



설정 SANtricity 11.6

NetApp
February 12, 2024

목차

- 설정 1
 - 경고 1
 - 시스템: 스토리지 배열 설정입니다 14
 - 시스템: iSCSI 설정 27
 - 시스템: NVMe 설정 39
 - 시스템: 추가 기능 46
 - 시스템: 보안 키 관리 50
 - 액세스 관리 64
 - 인증서 93

설정

경고

개념

알림의 작동 방식

알림은 스토리지 시스템에서 발생하는 중요한 이벤트를 관리자에게 알립니다. 알림은 이메일, SNMP 트랩 및 syslog를 통해 보낼 수 있습니다.

알림 프로세스는 다음과 같이 작동합니다.

1. 관리자는 System Manager에서 다음 경고 방법 중 하나 이상을 구성합니다.
 - * 이메일 * — 메시지가 이메일 주소로 전송됩니다.
 - SNMP * — SNMP 트랩이 SNMP 서버로 전송됩니다.
 - * Syslog * — 메시지가 syslog 서버로 전송됩니다.
2. 스토리지 배열의 이벤트 모니터가 문제를 감지하면 해당 문제에 대한 정보를 이벤트 로그에 기록합니다(* 메뉴: 지원 [이벤트 로그] * 에서 사용 가능). 예를 들어, 배터리 오류, 최적화에서 오프라인으로 이동하는 구성 요소 또는 컨트롤러의 중복 오류와 같은 이벤트가 문제에 포함될 수 있습니다.
3. 이벤트 모니터에서 이벤트가 "alertable"이라고 판단하면 구성된 경고 방법(e-메일, SNMP 및/또는 syslog)을 사용하여 알림을 보냅니다. 모든 중요 이벤트는 일부 경고 및 정보 이벤트와 함께 "alertable"으로 간주됩니다.

알림 구성

초기 설정 마법사(e-메일 알림만 해당) 또는 경고 페이지에서 경고를 구성할 수 있습니다. 현재 구성을 확인하려면 * 메뉴: 설정 [경고] * 로 이동하십시오.

경고 타일에는 다음 중 하나에 해당하는 경고 구성이 표시됩니다.

- 구성되지 않았습니다.
- 구성됨. 하나 이상의 경고 방법이 설정되었습니다. 구성된 경고 방법을 확인하려면 커서를 바둑판식으로 가져옵니다.

경고 정보

알림에는 다음과 같은 유형의 정보가 포함될 수 있습니다.

- 스토리지 배열의 이름입니다.
- 이벤트 로그 엔트리와 관련된 이벤트 오류 유형입니다.
- 이벤트가 발생한 날짜 및 시간입니다.
- 이벤트에 대한 간략한 설명입니다.



Syslog 알림은 RFC 3164 메시징 표준을 따릅니다.

경고 용어

알림 조건이 스토리지 어레이에 적용되는 방식에 대해 알아보십시오.

구성 요소	설명
이벤트 모니터	이벤트 모니터는 스토리지 시스템에 상주하며 백그라운드 작업으로 실행됩니다. 이벤트 모니터에서 스토리지 배열의 이상 징후를 감지하면 해당 문제에 대한 정보를 이벤트 로그에 기록합니다. 배터리 오류, 최적화에서 오프라인으로 이동하는 구성 요소 또는 컨트롤러의 중복 오류와 같은 문제가 포함될 수 있습니다. 이벤트 모니터에서 이벤트가 "alertable"이라고 판단하면 구성된 경고 방법(e-메일, SNMP 및/또는 syslog)을 사용하여 알림을 보냅니다. 모든 중요 이벤트는 일부 경고 및 정보 이벤트와 함께 "alertable"으로 간주됩니다.
메일 서버	메일 서버는 이메일 경고를 보내고 받는 데 사용됩니다. 서버는 SMTP(Simple Mail Transfer Protocol)를 사용합니다.
SNMP를 선택합니다	SNMP(Simple Network Management Protocol)는 IP 네트워크의 장치 간에 정보를 관리 및 공유하는 데 사용되는 인터넷 표준 프로토콜입니다.
SNMP 트랩	SNMP 트랩은 SNMP 서버로 전송되는 알림입니다. 트랩에는 스토리지 배열 관련 주요 문제에 대한 정보가 포함되어 있습니다.
SNMP 트랩 대상입니다	SNMP 트랩 대상은 SNMP 서비스를 실행하는 서버의 IPv4 또는 IPv6 주소입니다.
커뮤니티 이름입니다	커뮤니티 이름은 SNMP 환경에서 네트워크 서버의 암호 역할을 하는 문자열입니다.
MIB 파일	MIB(Management Information Base) 파일은 스토리지 어레이에서 모니터링 및 관리되는 데이터를 정의합니다. SNMP 서비스 응용 프로그램을 사용하여 서버에서 복사 및 컴파일해야 합니다. 이 MIB 파일은 지원 사이트의 System Manager 소프트웨어와 함께 사용할 수 있습니다.
MIB 변수	MIB(Management Information Base) 변수는 스토리지 배열 이름, 배열 위치 및 SNMP GetRequests에 대한 응답으로 연락 담당자 등의 값을 반환할 수 있습니다.
Syslog를 클릭합니다	Syslog는 네트워크 장치가 로깅 서버에 이벤트 메시지를 보내는 데 사용하는 프로토콜입니다.
UDP입니다	UDP(User Datagram Protocol)는 패킷 헤더에서 소스 및 대상 포트 번호를 지정하는 전송 계층 프로토콜입니다.

방법

이메일 알림을 관리합니다

메일 서버 및 받는 사람이 알림을 받도록 구성합니다

전자 메일 알림을 구성하려면 메일 서버 주소와 경고 받는 사람의 전자 메일 주소를 지정해야 합니다. 최대 20개의 이메일 주소가 허용됩니다.

시작하기 전에

- 메일 서버의 주소를 사용할 수 있어야 합니다. 주소는 IPv4 또는 IPv6 주소이거나 정규화된 도메인 이름일 수 있습니다.



정규화된 도메인 이름을 사용하려면 두 컨트롤러 모두에서 DNS 서버를 구성해야 합니다. 하드웨어 페이지에서 DNS 서버를 구성할 수 있습니다.

- 알림 발신자로 사용할 이메일 주소를 사용할 수 있어야 합니다. 경고 메시지의 "보낸 사람" 필드에 나타나는 주소입니다. SMTP 프로토콜에 보낸 사람 주소가 필요합니다. 이 주소가 없으면 오류 결과가 발생합니다.
- 알림 수신자의 이메일 주소를 사용할 수 있어야 합니다. 받는 사람은 일반적으로 네트워크 관리자 또는 스토리지 관리자의 주소입니다. 최대 20개의 이메일 주소를 입력할 수 있습니다.

이 작업에 대해

이 작업은 메일 서버를 구성하고, 보낸 사람과 받는 사람의 전자 메일 주소를 입력하고, 경고 페이지에서 입력한 모든 전자 메일 주소를 테스트하는 방법을 설명합니다.



초기 설정 마법사에서 이메일 알림을 구성할 수도 있습니다.

단계

1. 메뉴: 설정 [알림] * 을 선택합니다.
2. 이메일 * 탭을 선택합니다.

이메일 서버가 아직 구성되지 않은 경우 이메일 탭에 "메일 서버 구성"이 표시됩니다.

3. 메일 서버 구성 * 을 선택합니다.

메일 서버 구성 * 대화 상자가 열립니다.

4. 메일 서버 정보를 입력한 다음 * 저장 * 을 클릭합니다.

- * 메일 서버 주소 * — 메일 서버의 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소를 입력합니다.



정규화된 도메인 이름을 사용하려면 두 컨트롤러 모두에서 DNS 서버를 구성해야 합니다. 하드웨어 * 페이지에서 DNS 서버를 구성할 수 있습니다.

- * 이메일 발신자 주소 * — 이메일 발신자로 사용할 유효한 이메일 주소를 입력합니다. 이 주소는 전자 메일 메시지의 "보낸 사람" 필드에 나타납니다.
- * 전자 메일에 연락처 정보 포함 * — 경고 메시지에 보낸 사람의 연락처 정보를 포함하려면 이 옵션을 선택한 다음 이름과 전화 번호를 입력합니다. 저장 * 을 클릭하면 * 알림 * 페이지의 * 이메일 * 탭에 이메일 주소가 나타납니다.

5. 이메일 추가 * 를 선택합니다.

이메일 추가 대화 상자가 열립니다.

6. 경고 수신자에 대한 이메일 주소를 하나 이상 입력한 다음 * 추가 * 를 클릭합니다.

이메일 주소는 경고 페이지에 나타납니다.

7. 이메일 주소가 유효한지 확인하려면 * Test all email * 을 클릭하여 수신자에게 테스트 메시지를 보냅니다.

결과

e-메일 알림을 구성한 후 이벤트 모니터는 alertable 이벤트가 발생할 때마다 지정된 수신자에게 e-메일 메시지를 보냅니다.

알림에 대한 이메일 주소를 편집합니다

전자 메일 알림을 받는 사람의 전자 메일 주소를 변경할 수 있습니다.

시작하기 전에

편집하려는 이메일 주소는 경고 페이지의 이메일 탭에서 정의해야 합니다.

단계

1. 메뉴: 설정 [알림] * 을 선택합니다.
2. 이메일 * 탭을 선택합니다.
3. [전자 메일 주소] * 테이블에서 변경할 주소를 선택한 다음 맨 오른쪽에 있는 * 편집 * (연필) 아이콘을 클릭합니다.

행이 편집 가능한 필드가 됩니다.

4. 새 주소를 입력한 다음 * 저장 * (확인 표시) 아이콘을 클릭합니다.



변경 사항을 취소하려면 * Cancel * (X) 아이콘을 선택합니다.

결과

경고 페이지의 이메일 탭에는 업데이트된 이메일 주소가 표시됩니다.

알림에 대한 이메일 주소를 추가합니다

최대 20명의 전자 메일 알림을 받는 사람을 추가할 수 있습니다.

단계

1. 메뉴: 설정 [알림] * 을 선택합니다.
2. 이메일 * 탭을 선택합니다.
3. 이메일 추가 * 를 선택합니다.

이메일 추가 * 대화 상자가 열립니다.

4. 빈 필드에 새 이메일 주소를 입력합니다. 둘 이상의 주소를 추가하려면 * 다른 이메일 추가 * 를 선택하여 다른 필드를 엽니다.
5. 추가 * 를 클릭합니다.

결과

경고 * 페이지의 * 이메일 * 탭에 새 이메일 주소가 표시됩니다.

알림에 대한 메일 서버 또는 이메일 주소를 삭제합니다

이전에 정의한 메일 서버를 제거하여 알림이 더 이상 이메일 주소로 전송되지 않도록 하거나 개별 이메일 주소를 제거할 수 있습니다.

단계

1. 메뉴: 설정 [알림] * 을 선택합니다.
2. 이메일 * 탭을 선택합니다.
3. 테이블에서 다음 중 하나를 수행합니다.
 - 알림이 더 이상 전자 메일 주소로 전송되지 않도록 메일 서버를 제거하려면 메일 서버의 행을 선택합니다.
 - 알림이 더 이상 이 주소로 전송되지 않도록 전자 메일 주소를 제거하려면 삭제할 전자 메일 주소의 행을 선택합니다. 테이블 오른쪽 위에 있는 * Delete * (삭제 *) 버튼을 선택할 수 있습니다.
4. 삭제 * 를 클릭하고 작업을 확인합니다.

알림에 대한 메일 서버를 편집합니다

전자 메일 알림에 사용되는 메일 서버 주소 및 전자 메일 보낸 사람 주소를 변경할 수 있습니다.

시작하기 전에

변경하고 있는 메일 서버의 주소를 사용할 수 있어야 합니다. 주소는 IPv4 또는 IPv6 주소이거나 정규화된 도메인 이름일 수 있습니다.



정규화된 도메인 이름을 사용하려면 두 컨트롤러 모두에서 DNS 서버를 구성해야 합니다. 하드웨어 페이지에서 DNS 서버를 구성할 수 있습니다.

단계

1. 메뉴: 설정 [알림] * 을 선택합니다.
2. 이메일 * 탭을 선택합니다.
3. 메일 서버 구성 * 을 선택합니다.

메일 서버 구성 대화 상자가 열립니다.
4. 메일 서버 주소, 보낸 사람 정보 및 연락처 정보를 편집합니다.
 - * 메일 서버 주소 * — 메일 서버의 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소를 편집합니다.



정규화된 도메인 이름을 사용하려면 두 컨트롤러 모두에서 DNS 서버를 구성해야 합니다. 하드웨어 페이지에서 DNS 서버를 구성할 수 있습니다.

- e-메일 보낸 사람 주소 * — e-메일을 보낸 사람으로 사용할 e-메일 주소를 편집합니다. 이 주소는 전자 메일 메시지의 "보낸 사람" 필드에 나타납니다.
 - * 전자 메일에 연락처 정보 포함 * — 보낸 사람의 연락처 정보를 편집하려면 이 옵션을 선택한 다음 이름과 전화 번호를 편집합니다.
5. 저장 * 을 클릭합니다.

SNMP 경고를 관리합니다

SNMP 경고에 대한 커뮤니티 및 대상을 구성합니다

SNMP(Simple Network Management Protocol) 경고를 구성하려면 스토리지 배열의 이벤트 모니터에서 SNMP 트랩을 보낼 수 있는 서버를 하나 이상 식별해야 합니다. 구성에 서버의 커뮤니티 이름과 IP 주소가 필요합니다.

시작하기 전에

- 네트워크 서버는 SNMP 서비스 애플리케이션으로 구성되어야 합니다. 이벤트 모니터가 해당 주소로 트랩 메시지를 보낼 수 있도록 이 서버의 네트워크 주소(IPv4 또는 IPv6 주소)가 필요합니다. 둘 이상의 서버를 사용할 수 있습니다(최대 10대의 서버가 허용됨).
- 인쇄 가능한 ASCII 문자만 포함하는 커뮤니티 이름을 만들어야 합니다. 네트워크 서버의 암호 역할을 하는 문자열인 커뮤니티 이름은 일반적으로 네트워크 관리자가 만듭니다. 최대 256개의 커뮤니티를 만들 수 있습니다.
- MIB(Management Information Base) 파일이 SNMP 서비스 응용 프로그램을 사용하여 서버에서 복사 및 컴파일되었습니다. 이 MIB 파일은 모니터링 및 관리되는 데이터를 정의합니다.

MIB 파일이 없는 경우 NetApp Support 사이트에서 얻을 수 있습니다.

- 로 이동합니다 ["NetApp 지원"](#).
- Downloads * 를 클릭합니다.
- 소프트웨어 * 를 클릭합니다.
- 관리 소프트웨어(예: SANtricity 시스템 관리자)를 찾은 다음 오른쪽의 * Go! * 를 클릭합니다.
- 최신 버전에서 보기 및 다운로드를 클릭합니다.
- 페이지 하단의 * 계속 * 을 클릭합니다.
- EULA에 동의합니다.
- SNMP 트랩*에 대한 * MIB 파일이 표시될 때까지 아래로 스크롤한 다음 링크를 클릭하여 파일을 다운로드합니다.

이 작업에 대해

이 작업에서는 트랩 대상에 대한 SNMP 서버를 식별하고 구성을 테스트하는 방법을 설명합니다.

단계

1. 메뉴: 설정 [알림] * 을 선택합니다.
2. SNMP * 탭을 선택합니다.

커뮤니티가 아직 구성되지 않은 경우 SNMP 탭에 "커뮤니티 구성"이 표시됩니다.

3. 커뮤니티 구성 * 을 선택합니다.

커뮤니티 구성 * 대화 상자가 열립니다.

4. 커뮤니티 이름 * 필드에 네트워크 서버에 대한 커뮤니티 문자열을 하나 이상 입력한 다음 * 저장 * 을 클릭합니다.

경고 페이지에 "트랩 대상 추가"가 표시됩니다.

5. 트랩 대상 추가 * 를 선택합니다.

트랩 대상 추가 * 대화 상자가 열립니다.

6. 하나 이상의 트랩 대상을 입력하고 관련 커뮤니티 이름을 선택한 다음 * 추가 * 를 클릭합니다.

- * 트랩 대상 * — SNMP 서비스를 실행하는 서버의 IPv4 또는 IPv6 주소를 입력합니다.
- * 커뮤니티 이름 * — 드롭다운에서 이 트랩 대상에 대한 커뮤니티 이름을 선택합니다. (커뮤니티 이름을 하나만 정의한 경우 이 필드에 이름이 이미 표시됩니다.)
- * 인증 실패 트랩 전송 * — 인식되지 않는 커뮤니티 이름으로 인해 SNMP 요청이 거부될 때마다 트랩 대상에 알려려면 이 옵션(확인란)을 선택합니다. 추가 * 를 클릭하면 * 알림 * 페이지의 * SNMP * 탭에 트랩 대상 및 관련 커뮤니티 이름이 나타납니다.

7. 트랩이 유효한지 확인하려면 표에서 트랩 대상을 선택한 다음 * Test Trap Destination * 을 클릭하여 구성된 주소로 테스트 트랩을 보냅니다.

결과

이벤트 모니터는 alertable 이벤트가 발생할 때마다 SNMP 트랩을 서버로 전송합니다.

SNMP 트랩의 커뮤니티 이름을 편집합니다

SNMP 트랩의 커뮤니티 이름을 편집하고 다른 커뮤니티 이름을 SNMP 트랩 대상에 연결할 수도 있습니다.

시작하기 전에

인쇄 가능한 ASCII 문자만 포함하는 커뮤니티 이름을 만들어야 합니다. 네트워크 서버의 암호 역할을 하는 문자열인 커뮤니티 이름은 네트워크 관리자가 만듭니다.

단계

1. 메뉴: 설정 [알림] * 을 선택합니다.
2. SNMP * 탭을 선택합니다.

트랩 대상 및 커뮤니티 이름이 테이블에 나타납니다.

3. 다음과 같이 커뮤니티 이름을 편집합니다.

- 커뮤니티 이름을 편집하려면 * 커뮤니티 구성 * 을 선택합니다. 새 커뮤니티 이름을 입력한 다음 * 저장 * 을 클릭합니다. 커뮤니티 이름은 인쇄 가능한 ASCII 문자만 포함할 수 있습니다.
- 커뮤니티 이름을 새 트랩 대상에 연결하려면 테이블에서 커뮤니티 이름을 선택한 다음 맨 오른쪽에 있는 * 편집 * (연필) 아이콘을 클릭합니다. 커뮤니티 이름 드롭다운에서 SNMP 트랩 대상의 새 커뮤니티 이름을 선택한 다음 * 저장 * (확인 표시) 아이콘을 클릭합니다.



변경 사항을 취소하려면 * Cancel * (X) 아이콘을 선택합니다.

결과

Alerts * 페이지의 * SNMP * 탭에 업데이트된 커뮤니티가 표시됩니다.

SNMP 트랩에 대한 커뮤니티 이름을 추가합니다

SNMP 트랩에 대해 최대 256개의 커뮤니티 이름을 추가할 수 있습니다.

시작하기 전에

커뮤니티 이름을 만들어야 합니다. 네트워크 서버의 암호 역할을 하는 문자열인 커뮤니티 이름은 일반적으로 네트워크 관리자가 만듭니다. 인쇄 가능한 ASCII 문자만 포함됩니다.

단계

1. 메뉴: 설정 [알림] * 을 선택합니다.
2. SNMP * 탭을 선택합니다.

트랩 대상 및 커뮤니티 이름이 테이블에 나타납니다.

3. 커뮤니티 구성 * 을 선택합니다.

커뮤니티 구성 대화 상자가 열립니다.

4. 다른 커뮤니티 추가 * 를 선택합니다.
5. 새 커뮤니티 이름을 입력한 다음 * 저장 * 을 클릭합니다.

결과

새 커뮤니티 이름이 * Alerts * 페이지의 * SNMP * 탭에 나타납니다.

SNMP 트랩의 커뮤니티 이름을 제거합니다

SNMP 트랩의 커뮤니티 이름을 제거할 수 있습니다.

단계

1. 메뉴: 설정 [알림] * 을 선택합니다.
2. SNMP * 탭을 선택합니다.

트랩 대상 및 커뮤니티 이름이 경고 페이지에 나타납니다.

3. 커뮤니티 구성 * 을 선택합니다.

커뮤니티 구성 * 대화 상자가 열립니다.

4. 삭제할 커뮤니티 이름을 선택한 다음 오른쪽 끝에 있는 * 제거 * (X) 아이콘을 클릭합니다.

트랩 대상이 이 커뮤니티 이름과 연결된 경우 * 커뮤니티 제거 확인 * 대화 상자에 영향을 받는 트랩 대상 주소가 표시됩니다.

5. 작업을 확인한 다음 * 제거 * 를 클릭합니다.

결과

커뮤니티 이름 및 관련 트랩 대상이 * Alerts * 페이지에서 제거됩니다.

SNMP MIB 변수를 구성합니다

SNMP 알림의 경우 SNMP 트랩에 나타나는 MIB(Management Information Base) 변수를 선택적으로 구성할 수 있습니다. 이러한 변수는 스토리지 배열 이름, 배열 위치 및 담당자를 반환할 수 있습니다.

시작하기 전에

MIB 파일은 SNMP 서비스 응용 프로그램을 사용하여 서버에서 복사 및 컴파일해야 합니다.

MIB 파일이 없는 경우 다음과 같이 얻을 수 있습니다.

- 로 이동합니다 ["NetApp 지원"](#).
- Downloads * 를 클릭합니다.
- 소프트웨어 * 를 클릭합니다.
- 관리 소프트웨어(예: SANtricity 시스템 관리자)를 찾은 다음 오른쪽의 * Go! * 를 클릭합니다.
- 최신 버전에서 * 보기 및 다운로드 * 를 클릭합니다.
- 페이지 하단의 * 계속 * 을 클릭합니다.
- EULA에 동의합니다.
- SNMP 트랩*에 대한 * MIB 파일이 표시될 때까지 아래로 스크롤한 다음 링크를 클릭하여 파일을 다운로드합니다.

이 작업에 대해

이 작업에서는 SNMP 트랩에 대한 MIB 변수를 정의하는 방법에 대해 설명합니다. 이러한 변수는 SNMP GetRequests에 응답하여 다음 값을 반환할 수 있습니다.

- 'sysname'(스토리지 배열 이름)
- 'sysLocation'(스토리지 배열 위치)
- 'sysContact'(관리자 이름)

단계

1. 메뉴: 설정 [알림] * 을 선택합니다.
2. SNMP * 탭을 선택합니다.
3. SNMP MIB 변수 구성 * 을 선택합니다.

Configure SNMP MIB Variables(SNMP MIB 변수 구성) 대화 상자가 열립니다.

4. 다음 값 중 하나 이상을 입력한 다음 * 저장 * 을 클릭합니다.
 - * 이름 * — MIB 변수 "sysname"의 값입니다. 예를 들어 스토리지 배열의 이름을 입력합니다.
 - * Location * — MIB 변수 'sysLocation'의 값입니다. 예를 들어 스토리지 배열의 위치를 입력합니다.
 - * Contact * — MIB 변수 'sysContact'의 값입니다. 예를 들어 스토리지 시스템을 담당하는 관리자를 입력합니다.

결과

이러한 값은 스토리지 배열 경고에 대한 SNMP 트랩 메시지에 표시됩니다.

SNMP 트랩을 보내기 위해 최대 10대의 서버를 추가할 수 있습니다.

시작하기 전에

- 추가하려는 네트워크 서버는 SNMP 서비스 애플리케이션으로 구성되어야 합니다. 이벤트 모니터가 해당 주소로 트랩 메시지를 보낼 수 있도록 이 서버의 네트워크 주소(IPv4 또는 IPv6 주소)가 필요합니다. 둘 이상의 서버를 사용할 수 있습니다(최대 10대의 서버가 허용됨).
- 인쇄 가능한 ASCII 문자만 포함하는 커뮤니티 이름을 만들어야 합니다. 네트워크 서버의 암호 역할을 하는 문자열인 커뮤니티 이름은 일반적으로 네트워크 관리자가 만듭니다. 최대 256개의 커뮤니티를 만들 수 있습니다.
- MIB(Management Information Base) 파일이 SNMP 서비스 응용 프로그램을 사용하여 서버에서 복사 및 컴파일되었습니다. 이 MIB 파일은 모니터링 및 관리되는 데이터를 정의합니다.

MIB 파일이 없는 경우 NetApp Support 사이트에서 얻을 수 있습니다.

- 로 이동합니다 ["NetApp 지원"](#).
- Downloads * 를 클릭합니다.
- 소프트웨어 * 를 클릭합니다.
- 관리 소프트웨어(예: SANtricity 시스템 관리자)를 찾은 다음 오른쪽의 * Go! * 를 클릭합니다.
- 최신 버전에서 * 보기 및 다운로드 * 를 클릭합니다.
- 페이지 하단의 * 계속 * 을 클릭합니다.
- EULA에 동의합니다.
- SNMP 트랩*에 대한 * MIB 파일이 표시될 때까지 아래로 스크롤한 다음 링크를 클릭하여 파일을 다운로드합니다.

단계

1. 설정 * > * 알림 * 을 선택합니다.
2. SNMP * 탭을 선택합니다.

현재 정의된 트랩 대상이 테이블에 나타납니다.

3. Add Trap Desations * 를 선택합니다.

트랩 대상 추가 대화 상자가 열립니다.

4. 하나 이상의 트랩 대상을 입력하고 관련 커뮤니티 이름을 선택한 다음 * 추가 * 를 클릭합니다.
 - * 트랩 대상 * — SNMP 서비스를 실행하는 서버의 IPv4 또는 IPv6 주소를 입력합니다.
 - * 커뮤니티 이름 * — 드롭다운에서 이 트랩 대상에 대한 커뮤니티 이름을 선택합니다. (커뮤니티 이름을 하나만 정의한 경우 이 필드에 이름이 이미 표시됩니다.)
 - * 인증 실패 트랩 전송 * — 인식되지 않는 커뮤니티 이름으로 인해 SNMP 요청이 거부될 때마다 트랩 대상에 알려려면 이 옵션(확인란)을 선택합니다. 추가 * 를 클릭하면 트랩 대상 및 관련 커뮤니티 이름이 테이블에 나타납니다.
5. 트랩이 유효한지 확인하려면 표에서 트랩 대상을 선택한 다음 * Test Trap Destination * 을 클릭하여 구성된 주소로 테스트 트랩을 보냅니다.

결과

이벤트 모니터는 alertable 이벤트가 발생할 때마다 SNMP 트랩을 서버로 전송합니다.

트랩 대상을 삭제합니다

스토리지 배열의 이벤트 모니터가 더 이상 SNMP 트랩을 해당 주소로 보내지 않도록 트랩 대상 주소를 삭제할 수 있습니다.

단계

1. 메뉴: 설정 [알림] * 을 선택합니다.
2. SNMP * 탭을 선택합니다.

트랩 대상 주소가 테이블에 나타납니다.

3. 트랩 대상을 선택한 다음 페이지 오른쪽 위에 있는 * Delete * (삭제 *)를 클릭합니다.
4. 작업을 확인한 다음 * 삭제 * 를 클릭합니다.

대상 주소가 * Alerts * 페이지에 더 이상 나타나지 않습니다.

결과

삭제된 트랩 대상은 더 이상 스토리지 배열의 이벤트 모니터로부터 SNMP 트랩을 수신하지 않습니다.

syslog 알림을 관리합니다

경고에 대한 **syslog** 서버를 구성합니다

syslog 알림을 구성하려면 syslog 서버 주소와 UDP 포트를 입력해야 합니다. 최대 5개의 syslog 서버가 허용됩니다.

시작하기 전에

- syslog 서버 주소를 사용할 수 있어야 합니다. 이 주소는 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소일 수 있습니다.
- syslog 서버의 UDP 포트 번호를 사용할 수 있어야 합니다. 이 포트는 일반적으로 514입니다.

이 작업에 대해

이 작업은 syslog 서버의 주소와 포트를 입력한 다음 입력한 주소를 테스트하는 방법을 설명합니다.

단계

1. 메뉴: 설정 [알림] * 을 선택합니다.
2. Syslog * 탭을 선택합니다.

syslog 서버가 아직 정의되지 않은 경우 * Alerts * 페이지에 "Add Syslog Servers"가 표시됩니다.

3. Add Syslog Servers * 를 클릭합니다.

Add Syslog Server * 대화 상자가 열립니다.

4. 하나 이상의 syslog 서버에 대한 정보(최대 5개)를 입력한 다음 * 추가 * 를 클릭합니다.
 - * 서버 주소 * — 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소를 입력합니다.
 - * UDP 포트 * — 일반적으로 syslog에 대한 UDP 포트는 514입니다. 구성된 syslog 서버가 테이블에 표시됩니다.
5. 서버 주소로 테스트 알림을 보내려면 * 모든 Syslog 서버 테스트 * 를 선택합니다.

결과

이벤트 모니터는 경고 가능 이벤트가 발생할 때마다 syslog 서버에 경고를 보냅니다.

경고를 위해 **syslog** 서버를 편집합니다

syslog 알림을 수신하는 데 사용되는 서버 주소를 편집할 수 있습니다.

단계

1. 메뉴: 설정 [알림] * 을 선택합니다.
2. Syslog * 탭을 선택합니다.
3. 테이블에서 syslog 서버 주소를 선택한 다음 오른쪽 끝에 있는 * Edit * (연필) 아이콘을 클릭합니다.

행이 편집 가능한 필드가 됩니다.
4. 서버 주소와 UDP 포트 번호를 편집한 다음 * 저장 * (확인 표시) 아이콘을 클릭합니다.

결과

업데이트된 서버 주소가 테이블에 나타납니다.

경고에 대한 **syslog** 서버를 추가합니다

syslog 알림에 최대 5개의 서버를 추가할 수 있습니다.

시작하기 전에

- syslog 서버 주소를 사용할 수 있어야 합니다. 이 주소는 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소일 수 있습니다.
- syslog 서버의 UDP 포트 번호를 사용할 수 있어야 합니다. 이 포트는 일반적으로 514입니다.

단계

1. 메뉴: 설정 [알림] * 을 선택합니다.
2. Syslog * 탭을 선택합니다.
3. Add Syslog Servers * 를 선택합니다.

Add Syslog Server 대화 상자가 열립니다.
4. 다른 syslog 서버 추가 * 를 선택합니다.
5. syslog 서버에 대한 정보를 입력한 다음 * 추가 * 를 클릭합니다.
 - * Syslog Server Address * — 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소를 입력합니다.

- * UDP 포트 * — 일반적으로 syslog에 대한 UDP 포트는 514입니다.



최대 5개의 syslog 서버를 구성할 수 있습니다.

결과

syslog 서버 주소가 테이블에 나타납니다.

경고를 위해 **syslog** 서버를 삭제합니다

더 이상 경고를 받지 않도록 syslog 서버를 삭제할 수 있습니다.

단계

1. 메뉴: 설정 [알림] * 을 선택합니다.
2. Syslog * 탭을 선택합니다.
3. syslog 서버 주소를 선택한 다음 오른쪽 위에서 * 제거 * 를 클릭합니다.

Confirm Delete Syslog Server(Syslog 서버 삭제 확인) 대화 상자가 열립니다.

4. 작업을 확인한 다음 * 삭제 * 를 클릭합니다.

결과

제거한 서버는 더 이상 이벤트 모니터로부터 경고를 받지 않습니다.

FAQ 를 참조하십시오

경고가 비활성화되면 어떻게 합니까?

관리자가 스토리지 어레이에서 발생하는 중요한 이벤트에 대한 알림을 받도록 하려면 경고 방법을 구성해야 합니다.

SANtricity System Manager로 관리되는 스토리지 어레이의 경우 경고 페이지에서 경고를 구성합니다. 경고 알림은 이메일, SNMP 트랩 또는 syslog 메시지를 통해 보낼 수 있습니다. 또한 초기 설정 마법사에서 이메일 경고를 구성할 수도 있습니다.

SNMP 또는 **syslog** 알림을 구성하려면 어떻게 합니까?

e-메일 알림 외에도 SNMP(Simple Network Management Protocol) 트랩 또는 syslog 메시지를 통해 보낼 알림을 구성할 수 있습니다.

SNMP 또는 syslog 알림을 구성하려면 설정 [경고] 메뉴로 이동합니다.

타임스탬프가 스토리지와 알림 간에 일치하지 않는 이유는 무엇입니까?

스토리지 시스템에서 알림을 보낼 때 알림을 받는 타겟 서버 또는 호스트의 표준 시간대가 올바르지 않습니다. 대신 스토리지 배열은 로컬 시간(GMT)을 사용하여 경고 레코드에 사용되는 타임스탬프를 생성합니다. 따라서 스토리지 어레이의 타임스탬프와 알림을 수신하는 서버 또는 호스트의 일치하지 않는 부분이 표시될 수 있습니다.

스토리지 배열이 경고를 보낼 때 표준 시간대에 대해 올바르게 작동하지 않기 때문에 경고의 타임스탬프는 GMT-상대 시간이며 시간 영역 오프셋이 0입니다. 현지 시간대에 맞는 타임스탬프를 계산하려면 GMT에서 시간 오프셋을 결정한 다음 타임스탬프에서 해당 값을 더하거나 빼야 합니다.



이 문제를 방지하려면 스토리지 어레이 컨트롤러에서 NTP(네트워크 시간 프로토콜)를 구성합니다. NTP는 컨트롤러가 항상 올바른 시간에 동기화되도록 합니다.

시스템: 스토리지 배열 설정입니다

개념

캐시 설정 및 성능

캐시 메모리는 드라이브 미디어보다 액세스 시간이 빠른 컨트롤러의 임시 휘발성 저장 영역입니다.

캐싱을 사용하면 전반적인 I/O 성능을 다음과 같이 향상시킬 수 있습니다.

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

기본 캐시 설정은 대부분의 환경에 대한 요구 사항을 충족하지만 원하는 경우 변경할 수 있습니다.

스토리지 캐시 설정입니다

스토리지 배열의 모든 볼륨에 대해 시스템 페이지에서 다음 값을 지정할 수 있습니다.

- * 플러싱에 대한 시작 값 * — 캐시 플러시를 트리거하는 캐시에 기록되지 않은 데이터의 비율입니다(디스크에 쓰기). 캐시에 기록되지 않은 데이터의 지정된 시작 백분율이 있으면 플러시가 트리거됩니다. 기본적으로 컨트롤러는 캐시가 80% 찰 때 캐시를 플러시합니다.
- * 캐시 블록 크기 * — 캐시 관리를 위한 조직 단위인 각 캐시 블록의 최대 크기입니다. 캐시 블록 크기는 기본적으로 8KiB이지만 4, 8, 16 또는 32KiB로 설정할 수 있습니다. 가장 많이 사용되는 애플리케이션의 입출력 크기로 캐시 블록 크기를 설정하는 것이 좋습니다. 파일 시스템 또는 데이터베이스 애플리케이션은 일반적으로 더 작은 크기를 사용하며, 더 큰 크기는 대용량 데이터 전송이나 순차적 I/O가 필요한 애플리케이션에 적합합니다.

볼륨 캐시 설정입니다

스토리지 배열의 개별 볼륨의 경우 Volumes(볼륨) 페이지(메뉴: Storage(저장소) [Volumes](볼륨))에서 다음 값을 지정할 수 있습니다.

- * 읽기 캐싱 * — 읽기 캐시는 드라이브에서 읽은 데이터를 저장하는 버퍼입니다. 읽기 작업의 데이터가 이전 작업의 캐시에 이미 있을 수 있으므로 드라이브에 액세스할 필요가 없습니다. 데이터가 플러시될 때까지 읽기 캐시에 남아 있습니다.
 - * 동적 읽기 캐시 프리페치 * — 동적 캐시 읽기 프리페치를 사용하면 컨트롤러에서 드라이브에서 캐시로 데이터 블록을 읽는 동안 순차적 데이터 블록을 추가로 캐시에 복사할 수 있습니다. 이 캐싱은 향후 캐시에서 데이터 요청을 채울 수 있는 기회를 높여줍니다. 동적 캐시 읽기 프리페치는 순차적 I/O를 사용하는 멀티미디어 애플리케이션에 중요합니다. 캐시로 프리페치되는 데이터의 속도와 양은 호스트 읽기의 속도 및 요청 크기에

따라 자동으로 조정됩니다. 랜덤 액세스로 인해 데이터를 캐시로 프리페치하지 않습니다. 이 기능은 읽기 캐시를 사용하지 않는 경우 적용되지 않습니다.

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



◦ 데이터 손실 가능성 * — 배터리 없이 쓰기 캐싱 옵션을 활성화하고 보호를 위한 범용 전원 공급 장치가 없는 경우 데이터가 손실될 수 있습니다. 또한 컨트롤러 배터리가 없고 배터리 없이 쓰기 캐싱 옵션을 활성화하면 데이터가 손실될 수 있습니다.

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

자동 로드 밸런싱 개요

자동 로드 밸런싱은 시간이 지남에 따라 로드 변화에 동적으로 대응하고 볼륨 컨트롤러 소유권을 자동으로 조정하여 워크로드가 컨트롤러 간에 이동할 때 로드 불균형 문제를 해결함으로써 I/O 리소스 관리를 개선합니다.

각 컨트롤러의 워크로드는 지속적으로 모니터링되며 호스트에 설치된 다중 경로 드라이버의 협력을 통해 필요할 때마다 자동으로 균형을 맞출 수 있습니다. 컨트롤러 간에 워크로드가 자동으로 재조정되면 스토리지 관리자는 스토리지 어레이의 로드 변경을 수용하기 위해 볼륨 컨트롤러 소유권을 수동으로 조정해야 하는 부담을 덜 수 있습니다.

자동 로드 밸런싱이 활성화되면 다음 기능을 수행합니다.

- 컨트롤러 리소스 활용률을 자동으로 모니터링 및 균형 조정
- 필요한 경우 볼륨 컨트롤러 소유권을 자동으로 조정하여 호스트와 스토리지 어레이 간의 I/O 대역폭을 최적화합니다.

자동 로드 밸런싱 활성화 및 비활성화

자동 로드 밸런싱은 모든 스토리지 어레이에서 기본적으로 활성화됩니다.

다음과 같은 이유로 스토리지 어레이에서 자동 로드 밸런싱을 사용하지 않도록 설정할 수 있습니다.

- 워크로드의 균형을 맞추기 위해 특정 볼륨의 컨트롤러 소유권을 자동으로 변경하지 않으려는 경우
- 부하 분산이 의도적으로 설정된 고도로 조정된 환경에서 컨트롤러 간에 특정 분포를 이룰 수 있습니다.

자동 로드 밸런싱 기능을 지원하는 호스트 유형입니다

스토리지 어레이 레벨에서 자동 로드 밸런싱이 활성화되어 있더라도 호스트 또는 호스트 클러스터에 대해 선택하는 호스트 유형은 이 기능의 작동 방식에 직접적인 영향을 미칩니다.

여러 컨트롤러에 걸쳐 스토리지 어레이의 워크로드를 밸런싱할 때 자동 로드 밸런싱 기능은 두 컨트롤러가 액세스할 수 있고 자동 로드 밸런싱 기능을 지원할 수 있는 호스트 또는 호스트 클러스터에만 매핑된 볼륨을 이동하려고 시도합니다.

이렇게 하면 로드 밸런싱 프로세스로 인해 호스트가 볼륨에 액세스하지 못하게 됩니다. 하지만 자동 로드 밸런싱을 지원하지 않는 호스트에 매핑된 볼륨이 있으면 스토리지 시스템의 워크로드 균형 조정 기능에 영향을 줍니다. 자동 로드 균형 조정을 위해 다중 경로 드라이버는 TPGS를 지원해야 하며 호스트 유형은 다음 표에 포함되어야 합니다.



호스트 클러스터에서 자동 로드 밸런싱을 사용하려면 해당 그룹의 모든 호스트가 자동 로드 밸런싱을 지원할 수 있어야 합니다.

자동 로드 밸런싱을 지원하는 호스트 유형입니다	이 다중 경로 드라이버를 사용합니다
Windows 또는 Windows 클러스터형	NetApp E-Series DSM을 사용한 MPIO
Linux DM-MP(커널 3.10 이상)	'scsi_dh_ALUA' 디바이스 핸들러가 있는 DM-MP
VMware	VMW_SATP_ALUA 스토리지 어레이 유형 플러그인을 사용하는 NMP(Native Multipathing Plugin)



사소한 예외를 제외하고 자동 로드 밸런싱을 지원하지 않는 호스트 유형은 이 기능이 활성화되어 있는지 여부에 관계없이 계속 정상적으로 작동합니다. 한 가지 예외는 시스템에 페일오버가 있는 경우 데이터 경로가 반환될 때 스토리지 어레이가 매핑되지 않았거나 할당되지 않은 볼륨을 소유 컨트롤러로 다시 이동하는 것입니다. 비 자동 로드 밸런싱 호스트에 매핑되거나 할당된 볼륨은 이동되지 않습니다.

를 참조하십시오 **"상호 운용성 매트릭스 툴"** 특정 다중 경로 드라이버, OS 레벨 및 컨트롤러 드라이브 트레이 지원에 대한 호환성 정보

자동 로드 밸런싱 기능과 **OS** 호환성을 확인합니다

새(또는 기존) 시스템을 설정하기 전에 자동 로드 밸런싱 기능과 OS 호환성을 확인하십시오.

1. 로 이동합니다 **"상호 운용성 매트릭스 툴"** 솔루션을 찾고 지원을 확인합니다.

시스템에서 Red Hat Enterprise Linux 6 또는 SUSE Linux Enterprise Server 11을 실행하는 경우 기술 지원 부서에 문의하십시오.

2. '/etc/multipath.conf 파일'을 업데이트하고 구성합니다.
3. 해당 벤더 및 제품에 대해 "Stain_Attached_device_handler"와 "Detect_prio"가 모두 "yes"로 설정되어 있는지 확인하거나 기본 설정을 사용하십시오.

기본 호스트 운영 체제 유형입니다

호스트가 처음 접속될 때 스토리지 시스템에서 기본 호스트 유형을 사용합니다. 볼륨에 액세스할 때 스토리지 배열의 컨트롤러가 호스트의 운영 체제에서 작동하는 방식을 정의합니다. 접속된 호스트를 기준으로 스토리지 시스템의 작동 방식을 변경해야 하는 경우 호스트 유형을 변경할 수 있습니다.

일반적으로 호스트를 스토리지 어레이에 접속하거나 추가 호스트를 접속할 때 기본 호스트 유형을 변경합니다.

다음 지침을 염두에 두십시오.

- 스토리지 시스템에 접속하려는 모든 호스트의 운영 체제가 동일한 경우(호스트 환경 균질성) 호스트 유형을 운영 체제와 일치하도록 변경합니다.
- 스토리지 시스템에 접속하려는 운영 체제가 다른 호스트(이기종 호스트 환경)가 있는 경우 호스트 유형을 호스트 운영 체제의 대부분과 일치하도록 변경합니다.

예를 들어 8개의 서로 다른 호스트를 스토리지 배열에 연결하고 그 중 6개의 호스트가 Windows 운영 체제를 실행 중인 경우, Windows를 기본 호스트 운영 체제 유형으로 선택해야 합니다.

- 연결된 호스트의 대부분이 서로 다른 운영 체제를 사용하는 경우 호스트 유형을 공장 출하시 기본값으로 변경합니다.

예를 들어, 8개의 서로 다른 호스트를 스토리지 시스템에 접속하고 있고 이 중 2개의 호스트가 Windows 운영 체제를 실행 중인 경우 3개는 VMware 운영 체제를 실행하고, 또 다른 3개는 Linux 운영 체제를 실행하고 있으므로 기본 호스트 운영 체제 유형으로 공장 기본값을 선택해야 합니다.

방법

스토리지 배열 이름을 편집합니다

SANtricity 시스템 관리자의 제목 표시줄에 나타나는 스토리지 배열 이름을 변경할 수 있습니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. 일반 * 에서 * 이름: * 필드를 찾습니다.

스토리지 배열 이름이 정의되지 않은 경우 이 필드에는 "알 수 없음"이 표시됩니다.

3. 스토리지 배열 이름 옆에 있는 * Edit * (연필) 아이콘을 클릭합니다.

필드를 편집할 수 있게 됩니다.

4. 새 이름을 입력합니다.

이름에는 문자, 숫자 및 밑줄(_), 대시(-) 및 해시(#)를 사용할 수 있습니다. 이름에는 공백을 사용할 수 없습니다. 이름의 최대 길이는 30자입니다. 이름은 고유해야 합니다.

5. 저장 * (확인 표시) 아이콘을 클릭합니다.



변경하지 않고 편집 가능한 필드를 닫으려면 * Cancel * (X) 아이콘을 클릭합니다.

결과

새 이름이 SANtricity 시스템 관리자의 제목 표시줄에 나타납니다.

스토리지 배열 로케이터 표시등을 켭니다

캐비닛에서 스토리지 배열의 물리적 위치를 찾으려면 해당 로케이터(LED) 표시등을 켜면 됩니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. 일반 * 에서 * 스토리지 배열 로케이터 표시등 켜기 * 를 클릭합니다.

스토리지 배열 로케이터 표시등 켜기 * 대화 상자가 열리고 해당 스토리지 배열의 로케이터 표시등이 켜집니다.

3. 스토리지 배열을 물리적으로 찾았으면 대화 상자로 돌아가서 * 끄기 * 를 선택합니다.

결과

로케이터 표시등이 꺼지고 대화 상자가 닫힙니다.

스토리지 배열 클럭을 동기화합니다

NTP(네트워크 시간 프로토콜)가 활성화되지 않은 경우 컨트롤러의 시계를 수동으로 설정하여 관리 클라이언트(SANtricity 시스템 관리자에 액세스하는 브라우저를 실행하는 데 사용되는 시스템)와 동기화할 수 있습니다.

이 작업에 대해

동기화는 이벤트 로그의 이벤트 타임 스탬프가 호스트 로그 파일에 기록된 타임 스탬프와 일치하도록 합니다. 동기화 프로세스 중에도 컨트롤러는 사용 가능하고 정상적으로 작동합니다.



System Manager에서 NTP가 활성화되어 있는 경우 이 옵션을 사용하여 시계를 동기화하지 마십시오. 대신 NTP는 SNTP(Simple Network Time Protocol)를 사용하여 외부 호스트와 시계를 자동으로 동기화합니다.



동기화 후 성능 통계가 손실되거나 비뚤어지거나, 일정(ASUP, 스냅샷 등)이 영향을 받고, 로그 데이터의 타임스탬프가 비뚤어지는 것을 확인할 수 있습니다. NTP를 사용하면 이 문제가 방지됩니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. General * 에서 * Synchronize Storage Array Clocks * 를 클릭합니다.

스토리지 배열 시계 동기화 대화 상자가 열립니다. 컨트롤러 및 관리 클라이언트로 사용되는 컴퓨터의 현재 날짜 및 시간을 표시합니다.



단일 스토리지 어레이의 경우 하나의 컨트롤러만 표시됩니다.

3. 대화 상자에 표시된 시간이 일치하지 않으면 * Synchronize * 를 클릭합니다.

결과

동기화에 성공하면 이벤트 로그 및 호스트 로그에 대해 이벤트 타임 스탬프가 동일합니다.

스토리지 배열 구성을 저장합니다

스토리지 배열의 구성 정보를 스크립트 파일에 저장하여 동일한 구성으로 추가 스토리지 배열을 설정하는 시간을 절약할 수 있습니다.

시작하기 전에

스토리지 시스템에서 논리적 구성 설정을 변경하는 작업을 수행해서는 안 됩니다. 이러한 작업의 예로는 볼륨 생성 또는 삭제, 컨트롤러 펌웨어 다운로드, 핫 스페어 드라이브 할당 또는 수정, 볼륨 그룹에 용량(드라이브) 추가 등이 있습니다.

이 작업에 대해

스토리지 배열 구성을 저장하면 스토리지 배열에 대한 스토리지 배열 설정, 볼륨 구성, 호스트 구성 또는 호스트-볼륨 할당을 포함하는 CLI(Command Line Interface) 스크립트가 생성됩니다. 생성된 이 CLI 스크립트를 사용하여 정확히 동일한 하드웨어 구성을 가진 다른 스토리지 어레이로 구성을 복제할 수 있습니다.

그러나 재해 복구에 이 생성된 CLI 스크립트를 사용해서는 안 됩니다. 대신 시스템 복원을 수행하려면 수동으로 생성한 구성 데이터베이스 백업 파일을 사용하거나 기술 지원 부서에 문의하여 최신 자동 지원 데이터에서 이 데이터를 얻으십시오.

이 작업은 _ 이(가) 다음 설정을 저장하지 않습니다.

- 배터리 수명
- 컨트롤러 시간입니다
- NVSRAM(Nonvolatile Static Random Access Memory) 설정입니다
- 모든 프리미엄 기능
- 스토리지 배열 암호입니다
- 하드웨어 구성 요소의 작동 상태 및 상태입니다
- 볼륨 그룹의 작동 상태(최적 상태 제외) 및 상태입니다
- 미러링 및 볼륨 복사본과 같은 복사 서비스를 이용할 수 있습니다



• 응용 프로그램 오류 위험 * — 스토리지 배열에 논리 구성 설정을 변경할 작업이 진행 중인 경우에는 이 옵션을 사용하지 마십시오. 이러한 작업의 예로는 볼륨 생성 또는 삭제, 컨트롤러 펌웨어 다운로드, 핫 스페어 드라이브 할당 또는 수정, 볼륨 그룹에 용량(드라이브) 추가 등이 있습니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. 스토리지 배열 구성 저장 * 을 선택합니다.
3. 저장할 구성 항목을 선택합니다.

- * 스토리지 배열 설정 *
- * 볼륨 구성 *
- * 호스트 구성 *
- * 호스트-볼륨 할당 *



Host-to-volume Assignments * 항목을 선택하면 * Volume configuration * 항목과 * Host configuration * 항목도 기본적으로 선택됩니다. 볼륨 구성 * 및 * 호스트 구성 * 을 저장하지 않으면 * 호스트-볼륨 할당 * 을 저장할 수 없습니다.

4. 저장 * 을 클릭합니다.

이 파일은 브라우저의 다운로드 폴더에 'storage-array-configuration.cfg'라는 이름으로 저장됩니다.

작업을 마친 후

저장된 스토리지 배열 구성을 다른 스토리지 배열에 로드하려면 "-f" 옵션과 함께 SANtricity 명령줄 인터페이스 (SMcli)를 사용하여 ".cfg" 파일을 적용합니다.



Unified Manager 인터페이스를 사용하여 스토리지 어레이 구성을 다른 스토리지 어레이에 로드할 수도 있습니다(* 메뉴: 관리 [설정 가져오기] * 선택).

스토리지 배열 구성을 지웁니다

스토리지 배열에서 모든 풀, 볼륨 그룹, 볼륨, 호스트 정의 및 호스트 할당을 삭제하려면 구성 지우기 작업을 사용합니다.

시작하기 전에

- 스토리지 배열 구성을 지우기 전에 데이터를 백업합니다.

이 작업에 대해

스토리지 배열 구성 지우기 옵션에는 두 가지가 있습니다.

- * 볼륨 * — 일반적으로 볼륨 옵션을 사용하여 테스트 스토리지 어레이를 프로덕션 스토리지 어레이로 재구성할 수 있습니다. 예를 들어, 테스트용으로 스토리지 어레이를 구성한 다음 테스트를 마치면 테스트 구성을 제거하고 운영 환경에 맞게 스토리지 어레이를 설정할 수 있습니다.
- * 스토리지 배열 * — 일반적으로 스토리지 배열 옵션을 사용하여 스토리지 배열을 다른 부서 또는 그룹으로 이동할 수 있습니다. 예를 들어, 엔지니어링 팀에서 스토리지 어레이를 사용하고 있고 이제 엔지니어링 팀에서 새 스토리지 어레이를 가져오므로 현재 스토리지 어레이를 재구성할 관리 위치로 이동할 수 있습니다.

스토리지 배열 옵션은 일부 추가 설정을 삭제합니다.

	볼륨	스토리지
풀 및 볼륨 그룹을 삭제합니다	X	X
볼륨을 삭제합니다	X	X
호스트 및 호스트 클러스터를 삭제합니다	X	X
호스트 할당을 삭제합니다	X	X
스토리지 배열 이름을 삭제합니다		X
스토리지 캐시 설정을 기본값으로 재설정합니다		X



- 데이터 손실 위험 * — 이 작업은 스토리지 배열의 모든 데이터를 삭제합니다. (보안 지우지는 않습니다.) 이 작업을 시작한 후에는 취소할 수 없습니다. 기술 지원 부서에서 지시한 경우에만 이 작업을 수행하십시오.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. 스토리지 배열 구성 지우기 * 를 선택합니다.
3. 드롭다운 목록에서 * Volume * 또는 * Storage Array * 를 선택합니다.
4. * 선택 사항: * 데이터가 아닌 구성을 저장하려면 대화 상자의 링크를 사용합니다.
5. 작업을 수행할지 확인합니다.

결과

- 현재 구성이 삭제되어 스토리지 어레이의 기존 데이터가 모두 제거됩니다.
- 모든 드라이브가 할당되지 않았습니다.

로그인 배너를 구성합니다

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

이 작업에 대해

배너를 만들면 대화 상자의 로그인 화면 앞에 나타납니다.

단계

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

로그인 배너 구성 대화 상자가 열립니다.

3. 로그인 배너에 표시할 텍스트를 입력합니다.



HTML이나 다른 태그 태그를 서식 지정에 사용하지 마십시오.

4. 저장 * 을 클릭합니다.

결과

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

세션 시간 제한을 관리합니다

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

이 작업에 대해

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



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

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. General * 섹션에서 * Enable/Disable Session Timeout * 을 선택합니다.

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

3. 스피너 컨트롤을 사용하여 시간을 분 단위로 늘리거나 줄입니다.

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



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

4. 저장 * 을 클릭합니다.

스토리지 배열에 대한 캐시 설정을 변경합니다

스토리지 배열의 모든 볼륨에 대해 캐시 메모리 설정을 조정하여 플러싱과 블록 크기를 조정할 수 있습니다.

이 작업에 대해

캐시 메모리는 컨트롤러의 임시 휘발성 저장 공간으로, 드라이브 미디어보다 액세스 시간이 더 빠릅니다. 캐시 성능을 조정하려면 다음 설정을 조정할 수 있습니다.

캐시 설정	설명
요청 캐시 플러싱을 시작합니다	Start demand cache flashing은 캐시 플러시(디스크에 쓰기)를 트리거하는 캐시에 기록되지 않은 데이터의 비율을 지정합니다. 기본적으로 캐시 플러싱은 기록되지 않은 데이터가 80% 용량에 도달하면 시작됩니다. 쓰기 작업이 주로 수행되는 환경에서는 더 높은 비율이 적합하므로 새 쓰기 요청은 디스크로 이동할 필요 없이 캐시로 처리될 수 있습니다. 입출력 오류가 발생하는 환경(데이터 버스트 사용)에서 낮은 설정은 더 낮기 때문에 시스템이 데이터 버스트 사이에 캐시를 자주 플러시합니다. 그러나 시작 비율이 80%보다 낮으면 성능이 저하될 수 있습니다.
캐시 블록 크기	캐시 블록 크기는 각 캐시 블록의 최대 크기를 결정합니다. 이 크기는 캐시 관리를 위한 조직 단위입니다. 기본적으로 블록 크기는 32KiB입니다. System Manager에서는 캐시 블록 크기를 4, 8, 16 또는 32KiB로 설정할 수 있습니다. 애플리케이션은 스토리지 성능에 영향을 미치는 다양한 블록 크기를 사용합니다. 파일 시스템 또는 데이터베이스 애플리케이션에 적합한 크기는 더 작습니다. 더 큰 크기는 멀티미디어와 같이 순차적 I/O를 생성하는 응용 프로그램에 이상적입니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. 아래로 스크롤하여 * 추가 설정 * 을 찾은 다음 * 캐시 설정 변경 * 을 클릭합니다.

캐시 설정 변경 대화 상자가 열립니다.

3. 다음 값을 조정합니다.

- * 요청 캐시 플러싱 시작 * — 사용자 환경에서 사용되는 I/O에 적합한 비율을 선택합니다. 80% 미만의 값을 선택하면 성능이 저하될 수 있습니다.
- * 캐시 블록 크기 * — 응용 프로그램에 적합한 크기를 선택합니다.

4. 저장 * 을 클릭합니다.

호스트 연결 보고를 설정합니다

스토리지 어레이가 컨트롤러와 구성된 호스트 간의 연결을 지속적으로 모니터링하도록 호스트 연결 보고를 설정한 다음 연결이 중단되면 경고를 표시합니다. 이 기능은 기본적으로 활성화되어 있습니다.

이 작업에 대해

호스트 접속 보고 기능을 해제하면 시스템이 더 이상 스토리지 배열에 연결된 호스트의 접속 또는 다중 경로 드라이버 문제를 모니터링하지 않습니다.



호스트 연결 보고를 비활성화하면 컨트롤러 리소스 활용률을 모니터링 및 밸런싱하는 자동 로드 밸런싱도 비활성화됩니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.

2. 아래로 스크롤하여 * 추가 설정 * 을 선택한 다음 * 호스트 연결 보고 활성화/비활성화 * 를 클릭합니다.

이 옵션 아래의 텍스트는 현재 활성화 또는 비활성화 여부를 나타냅니다.

확인 대화 상자가 열립니다.

3. 계속하려면 * 예 * 를 클릭하십시오.

이 옵션을 선택하면 기능을 활성화/비활성화 상태로 전환할 수 있습니다.

자동 로드 밸런싱을 설정합니다

자동 로드 밸런싱 기능은 호스트로부터 들어오는 I/O 트래픽이 두 컨트롤러 간에 동적으로 관리 및 균형 조정되도록 합니다. 이 기능은 기본적으로 활성화되어 있지만 System Manager에서 비활성화할 수 있습니다.

이 작업에 대해

자동 로드 밸런싱이 활성화되면 다음 기능을 수행합니다.

- 컨트롤러 리소스 활용률을 자동으로 모니터링 및 균형 조정
- 필요한 경우 볼륨 컨트롤러 소유권을 자동으로 조정하여 호스트와 스토리지 어레이 간의 I/O 대역폭을 최적화합니다.

다음과 같은 이유로 스토리지 어레이에서 자동 로드 밸런싱을 사용하지 않도록 설정할 수 있습니다.

- 워크로드의 균형을 맞추기 위해 특정 볼륨의 컨트롤러 소유권을 자동으로 변경하지 않으려는 경우
- 부하 분산이 의도적으로 설정된 고도로 조정된 환경에서 컨트롤러 간에 특정 분포를 이룰 수 있습니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. 아래로 스크롤하여 * 추가 설정 * 을 선택한 다음 * 자동 로드 밸런싱 활성화/비활성화 * 를 클릭합니다.

이 옵션 아래의 텍스트는 기능이 현재 활성화되어 있는지 여부를 나타냅니다.

확인 대화 상자가 열립니다.

3. 계속하려면 * 예 * 를 클릭하여 확인하십시오.

이 옵션을 선택하면 기능을 활성화/비활성화 상태로 전환할 수 있습니다.



이 기능이 비활성화에서 사용으로 이동되면 호스트 연결 보고 기능도 자동으로 활성화됩니다.

기본 호스트 유형을 변경합니다

기본 호스트 운영 체제 변경 설정을 사용하여 스토리지 어레이 레벨에서 기본 호스트 유형을 변경합니다. 일반적으로 호스트를 스토리지 어레이에 접속하거나 추가 호스트를 접속할 때 기본 호스트 유형을 변경합니다.

이 작업에 대해

다음 지침을 염두에 두십시오.

- 스토리지 시스템에 접속하려는 모든 호스트의 운영 체제가 동일한 경우(호스트 환경 균질성) 호스트 유형을 운영 체제와 일치하도록 변경합니다.
- 스토리지 시스템에 접속하려는 운영 체제가 다른 호스트(이기종 호스트 환경)가 있는 경우 호스트 유형을 호스트 운영 체제의 대부분과 일치하도록 변경합니다.

예를 들어 8개의 서로 다른 호스트를 스토리지 배열에 연결하고 그 중 6개의 호스트가 Windows 운영 체제를 실행 중인 경우, Windows를 기본 호스트 운영 체제 유형으로 선택해야 합니다.

- 연결된 호스트의 대부분이 서로 다른 운영 체제를 사용하는 경우 호스트 유형을 공장 출하시 기본값으로 변경합니다.

예를 들어, 8개의 서로 다른 호스트를 스토리지 시스템에 접속하고 있고 이 중 2개의 호스트가 Windows 운영 체제를 실행 중인 경우 3개는 VMware 운영 체제를 실행하고, 또 다른 3개는 Linux 운영 체제를 실행하고 있으므로 기본 호스트 운영 체제 유형으로 공장 기본값을 선택해야 합니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. 아래로 스크롤하여 * 추가 설정 * 을 찾은 다음 * 기본 호스트 운영 체제 유형 변경 * 을 클릭합니다.
3. 기본값으로 사용할 호스트 운영 체제 유형을 선택합니다.
4. 변경 * 을 클릭합니다.

레거시 관리 인터페이스를 활성화 또는 비활성화합니다

스토리지 배열과 관리 클라이언트 간의 통신 방법인 레거시 관리 인터페이스(기호)를 설정하거나 해제할 수 있습니다.

이 작업에 대해

기본적으로 레거시 관리 인터페이스는 켜져 있습니다. 이 기능을 해제하면 스토리지 어레이와 관리 클라이언트에서 더욱 안전한 통신 방법(https를 통한 REST API)을 사용합니다. 그러나 특정 톨 및 작업이 비활성화된 경우 영향을 받을 수 있습니다.



EF600 스토리지 시스템의 경우 이 기능은 기본적으로 비활성화되어 있습니다.

이 설정은 다음과 같은 작업에 영향을 줍니다.

- * On * (기본값) — CLI 및 OCI 어댑터와 같은 다른 톨을 사용하여 미러링을 구성하는 데 필요한 설정입니다.
- * Off * — 스토리지 어레이와 관리 클라이언트 간 통신에서 기밀성을 강화하고 외부 도구에 액세스하는 데 필요한 설정입니다. LDAP(Directory Server)를 구성할 때 권장되는 설정입니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. 아래로 스크롤하여 * 추가 설정 * 을 선택한 다음 * 관리 인터페이스 변경 * 을 클릭합니다.
3. 대화 상자에서 * 예 * 를 클릭하여 계속합니다.

FAQ 를 참조하십시오

컨트롤러 캐시란 무엇입니까?

컨트롤러 캐시는 두 가지 유형의 I/O(I/O) 작업, 즉 컨트롤러 및 호스트 간, 컨트롤러 및 디스크 간 작업을 간소화하는 물리적 메모리 공간입니다.

읽기 및 쓰기 데이터 전송의 경우 호스트와 컨트롤러는 고속 연결을 통해 통신합니다. 그러나 디스크가 상대적으로 느린 장치이기 때문에 컨트롤러의 백엔드에서 디스크와의 통신이 느려집니다.

컨트롤러 캐시가 데이터를 수신하면 컨트롤러는 데이터가 현재 보유 중인 호스트 애플리케이션에 확인합니다. 이렇게 하면 호스트 애플리케이션이 I/O가 디스크에 기록될 때까지 기다릴 필요가 없습니다. 대신 응용 프로그램에서 작업을 계속할 수 있습니다. 또한 서버 애플리케이션에서 캐시된 데이터에 쉽게 액세스할 수 있으므로 데이터에 액세스하기 위해 디스크를 추가로 읽을 필요가 없습니다.

컨트롤러 캐시는 다음과 같은 여러 가지 방법으로 스토리지 어레이의 전반적인 성능에 영향을 줍니다.

- 캐시는 버퍼 역할을 하므로 호스트 및 디스크 데이터 전송을 동기화할 필요가 없습니다.
- 호스트의 읽기 또는 쓰기 작업에 대한 데이터가 이전 작업의 캐시에 있을 수 있으므로 디스크를 액세스할 필요가 없습니다.
- 쓰기 캐시를 사용하는 경우 이전 쓰기 작업의 데이터가 디스크에 기록되기 전에 호스트에서 후속 쓰기 명령을 전송할 수 있습니다.
- 캐시 프리페치가 설정된 경우 순차적 읽기 액세스가 최적화됩니다. 캐시 프리페치를 사용하면 디스크에서 데이터를 읽는 대신 캐시에서 데이터를 더 많이 찾을 수 있습니다.



- 데이터 손실 가능성 * — 배터리 없이 * 쓰기 캐싱 * 옵션을 활성화하고 보호를 위한 범용 전원 공급 장치가 없는 경우 데이터가 손실될 수 있습니다. 또한 컨트롤러 배터리가 없고 * 배터리 없이 쓰기 캐싱 * 옵션을 활성화하면 데이터가 손실될 수 있습니다.

캐시 플래싱이란 무엇입니까?

캐시에 기록되지 않은 데이터의 양이 특정 수준에 도달하면 컨트롤러는 캐시된 데이터를 드라이브에 주기적으로 씁니다. 이 쓰기 프로세스를 "플러시"라고 합니다.

컨트롤러는 캐시 플래싱에 두 가지 알고리즘(요구 기반 및 사용 기간 기반)을 사용합니다. 컨트롤러는 캐시된 데이터의 양이 캐시 플래시 임계값 아래로 떨어질 때까지 수요 기반 알고리즘을 사용합니다. 기본적으로 플러시는 캐시의 80%가 사용 중일 때 시작됩니다.

System Manager에서 "Start demand cache flashing" 임계값을 설정하여 사용자 환경에서 사용되는 입출력 유형을 가장 잘 지원할 수 있습니다. 주로 쓰기 작업을 수행하는 환경에서는 "Start demand cache flashing" 비율을 높게 설정하여 새 쓰기 요청을 디스크로 이동하지 않고 캐시로 처리할 수 있는 확률을 높여야 합니다. 백분을 설정은 더 많은 데이터가 캐시에 남아 있도록 캐시 플러시 수를 제한하여 캐시 적중률이 증가할 수 있습니다.

입출력 오류가 발생하는 환경(데이터 급증)에서는 낮은 캐시 플러시를 사용하여 시스템이 데이터 버스트 사이에 캐시를 자주 플러시할 수 있습니다. 다양한 부하를 처리하는 다양한 I/O 환경에서 또는 로드 유형을 알 수 없는 경우 임계값을 양호한 중간 지면으로 50%로 설정합니다. 시작 비율이 80%보다 낮은 경우 호스트 읽기에 필요한 데이터를 사용할 수 없기 때문에 성능이 저하될 수 있습니다. 낮은 비율을 선택하면 캐시 레벨을 유지하는 데 필요한 디스크 쓰기 수도 증가하여 시스템 오버헤드가 증가합니다.

연령 기반 알고리즘은 쓰기 데이터가 디스크에 플러시되기 전에 캐시에 남아 있을 수 있는 기간을 지정합니다. 컨트롤러는 캐시 플러시 임계값에 도달할 때까지 연령 기반 알고리즘을 사용합니다. 기본값은 10초이지만 이 기간은 비활성 기간 동안에만 계산됩니다. System Manager에서 플러시 타이밍을 수정할 수 없습니다. 대신 CLI(Command-Line Interface)에서 * 스토리지 배열 설정 * 명령을 사용해야 합니다.



- 데이터 손실 가능성 * — 배터리 없이 * 쓰기 캐싱 * 옵션을 활성화하고 보호를 위한 범용 전원 공급 장치가 없는 경우 데이터가 손실될 수 있습니다. 또한 컨트롤러 배터리가 없고 * 배터리 없이 쓰기 캐싱 * 옵션을 활성화하면 데이터가 손실될 수 있습니다.

캐시 블록 크기란 무엇입니까?

스토리지 시스템의 컨트롤러는 캐시를 "블록"으로 구성합니다. 이는 8, 16, 32KiB 크기의 메모리 청크입니다. 스토리지 시스템의 모든 볼륨이 동일한 캐시 공간을 공유하기 때문에 볼륨에 캐시 블록 크기가 하나만 있을 수 있습니다.

애플리케이션은 스토리지 성능에 영향을 미칠 수 있는 다양한 블록 크기를 사용합니다. 기본적으로 System Manager의 블록 크기는 32KiB이지만 값을 8, 16, 32KiB로 설정할 수 있습니다. 파일 시스템 또는 데이터베이스 애플리케이션에 적합한 크기는 더 작습니다. 크기가 클수록 대용량 데이터 전송, 순차 I/O 또는 멀티미디어와 같은 고대역폭이 필요한 응용 프로그램에 적합합니다.

스토리지 배열 클록은 언제 동기화해야 합니까?

System Manager에 표시되는 타임 스탬프가 관리 클라이언트(브라우저를 통해 System Manager에 액세스하는 컴퓨터)에 표시되는 타임 스탬프와 정렬되지 않은 경우 스토리지 어레이에서 컨트롤러 클록을 수동으로 동기화해야 합니다. 이 작업은 System Manager에서 NTP(네트워크 시간 프로토콜)가 활성화되지 않은 경우에만 필요합니다.



시계를 수동으로 동기화하는 대신 NTP 서버를 사용하는 것이 좋습니다. NTP는 SNTP(Simple Network Time Protocol)를 사용하여 외부 서버와 시계를 자동으로 동기화합니다.

시스템 페이지에서 사용할 수 있는 스토리지 배열 시계 동기화 대화 상자에서 동기화 상태를 확인할 수 있습니다. 대화 상자에 표시된 시간이 일치하지 않으면 동기화를 실행합니다. 이 대화 상자를 주기적으로 볼 수 있습니다. 이 대화 상자는 컨트롤러 시계의 시간 디스플레이가 서로 분리되어 더 이상 동기화되지 않았음을 나타냅니다.

호스트 연결 보고란 무엇입니까?

호스트 연결 보고가 설정되면 스토리지 어레이는 컨트롤러와 구성된 호스트 간의 연결을 지속적으로 모니터링한 다음 연결이 중단되면 경고를 표시합니다.

느슨하거나 손상되거나 누락된 케이블이 있거나 호스트에 다른 문제가 있는 경우 연결이 중단될 수 있습니다. 이러한 경우, 시스템이 Recovery Guru 메시지를 열 수 있습니다.

- * 호스트 중복성 손실* — 두 컨트롤러가 호스트와 통신할 수 없는 경우 열립니다.
- * 잘못된 호스트 유형* — 호스트 유형이 스토리지 배열에 잘못 지정되어 장애 조치 문제가 발생할 경우 열립니다.

컨트롤러를 재부팅하면 연결 시간 초과보다 오래 걸릴 수 있는 상황에서 호스트 연결 보고를 사용하지 않도록 설정할 수 있습니다. 이 기능을 사용하지 않도록 설정하면 복구 Gurus 메시지가 표시되지 않습니다.



호스트 연결 보고를 비활성화하면 컨트롤러 리소스 사용을 모니터링 및 밸런싱하는 자동 로드 밸런싱도 비활성화됩니다. 그러나 호스트 연결 보고를 다시 활성화하면 자동 로드 밸런싱 기능이 자동으로 다시 활성화되지 않습니다.

시스템: iSCSI 설정

개념

iSCSI 용어

iSCSI 용어가 스토리지 어레이에 어떻게 적용되는지 알아보십시오.

기간	설명
CHAP	CHAP(Challenge Handshake Authentication Protocol) 메시드는 초기 링크 중에 대상 및 이니시에이터의 ID를 확인합니다. 인증은 CHAPsecret이라는 공유 보안 키를 기반으로 합니다.
컨트롤러	컨트롤러는 보드, 펌웨어 및 소프트웨어로 구성됩니다. 드라이브를 제어하고 System Manager 기능을 구현합니다.
DHCP를 선택합니다	DHCP(Dynamic Host Configuration Protocol)는 IP 주소와 같은 네트워크 구성 매개 변수를 동적으로 배포하기 위해 IP(인터넷 프로토콜) 네트워크에서 사용되는 프로토콜입니다.

기간	설명
IB	IB(InfiniBand)는 고성능 서버와 스토리지 시스템 간의 데이터 전송을 위한 통신 표준입니다.
ICMP ping 응답	ICMP(Internet Control Message Protocol)는 네트워크 컴퓨터의 운영 체제에서 메시지를 보내는 데 사용되는 프로토콜입니다. ICMP 메시지는 호스트에 연결할 수 있는지 여부와 해당 호스트와 패킷을 주고 받는 데 걸리는 시간을 결정합니다.
IQN을 선택합니다	IQN(iSCSI Qualified Name) 식별자는 iSCSI 이니시에이터 또는 iSCSI 타겟의 고유한 이름입니다.
iSER	iSER(iSCSI Extensions for RDMA)은 InfiniBand 또는 이더넷과 같은 RDMA 전송을 통해 작동하는 iSCSI 프로토콜을 확장하는 프로토콜입니다.
iSNS를 선택합니다	iSNS(Internet Storage Name Service)는 TCP/IP 네트워크에서 iSCSI 및 Fibre Channel 디바이스를 자동으로 검색, 관리 및 구성할 수 있는 프로토콜입니다.
MAC 주소	MAC 주소(Media Access Control Identifier)는 동일한 물리적 전송 네트워크 인터페이스의 두 포트를 연결하는 별도의 논리 채널을 구분하기 위해 이더넷에서 사용됩니다.
관리 클라이언트	관리 클라이언트는 System Manager 액세스를 위해 브라우저가 설치된 컴퓨터입니다.
MTU	MTU(Maximum Transmission Unit)는 네트워크에서 전송할 수 있는 가장 큰 크기의 패킷 또는 프레임입니다.
RDMA 를 참조하십시오	RDMA(Remote Direct Memory Access)는 네트워크 컴퓨터가 두 컴퓨터의 운영 체제와 관계없이 주 메모리에서 데이터를 교환할 수 있도록 하는 기술입니다.
명명되지 않은 검색 세션	명명되지 않은 검색 세션 옵션이 활성화된 경우 iSCSI 초기자는 컨트롤러의 정보를 검색하기 위해 타겟 IQN을 지정할 필요가 없습니다.

방법

iSCSI 포트를 구성합니다

컨트롤러에 iSCSI 호스트 연결이 포함된 경우 시스템 페이지에서 iSCSI 포트 설정을 구성할 수 있습니다.

시작하기 전에

- 컨트롤러에 iSCSI 포트가 포함되어야 합니다. 그렇지 않으면 iSCSI 설정을 사용할 수 없습니다.
- 네트워크 속도(포트와 호스트 간의 데이터 전송 속도)를 알아야 합니다.



iSCSI 설정 및 기능은 스토리지 배열이 iSCSI를 지원하는 경우에만 나타납니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. iSCSI 설정 * 에서 * iSCSI 포트 구성 * 을 선택합니다.



iSCSI 포트 구성 * 옵션은 System Manager가 컨트롤러에서 iSCSI 포트를 감지한 경우에만 나타납니다.

3. 구성할 iSCSI 포트가 있는 컨트롤러를 선택합니다.
4. 드롭다운 목록에서 구성할 포트를 선택한 후 * 다음 * 을 클릭합니다.
5. 구성 포트 설정을 선택한 후 * 다음 * 을 클릭합니다.

모든 포트 설정을 보려면 대화 상자 오른쪽에 있는 * 추가 포트 설정 표시 * 링크를 클릭합니다.

필드 세부 정보

포트 설정	설명
IPv4 사용/IPv6 사용	<p>IPv4 및 IPv6 네트워크에 대한 지원을 활성화하려면 하나 또는 두 옵션을 모두 선택하십시오.</p> <p> 포트 액세스를 비활성화하려면 두 확인란을 모두 선택 취소합니다.</p>
TCP 수신 대기 포트(* 추가 포트 설정 표시 * 를 클릭하여 사용 가능)	<p>필요한 경우 새 포트 번호를 입력합니다.</p> <p>수신 대기 포트는 컨트롤러가 호스트 iSCSI 초기자의 iSCSI 로그인을 수신 대기하기 위해 사용하는 TCP 포트 번호입니다. 기본 수신 대기 포트는 3260입니다. 3260 또는 49152와 65535 사이의 값을 입력해야 합니다.</p>
MTU 크기(* 추가 포트 설정 표시 * 를 클릭하여 사용 가능)	<p>필요한 경우 MTU(Maximum Transmission Unit)에 대한 새 크기를 바이트 단위로 입력합니다.</p> <p>기본 MTU(Maximum Transmission Unit) 크기는 프레임당 1,500바이트입니다. 1500에서 9000 사이의 값을 입력해야 합니다.</p>
ICMP Ping 응답을 활성화합니다	<p>ICMP(Internet Control Message Protocol)를 활성화하려면 이 옵션을 선택합니다. 네트워크로 연결된 컴퓨터의 운영 체제는 이 프로토콜을 사용하여 메시지를 전송합니다. 이러한 ICMP 메시지는 호스트에 연결할 수 있는지 여부와 해당 호스트와 패킷을 주고 받는 데 걸리는 시간을 결정합니다.</p>

IPv4 사용 * 을 선택한 경우 * 다음 * 을 클릭하면 IPv4 설정을 선택할 수 있는 대화 상자가 열립니다. IPv6 사용 * 을 선택한 경우 * 다음 * 을 클릭하면 IPv6 설정을 선택할 수 있는 대화 상자가 열립니다. 두 옵션을 모두 선택한 경우 IPv4 설정에 대한 대화 상자가 먼저 열리고 * 다음 * 을 클릭하면 IPv6 설정에 대한 대화 상자가 열립니다.

6. IPv4 및/또는 IPv6 설정을 자동 또는 수동으로 구성합니다. 모든 포트 설정을 보려면 대화 상자 오른쪽에 있는 * 추가

설정 표시 * 링크를 클릭합니다.

필드 세부 정보

포트 설정	설명
자동으로 구성을 가져옵니다	구성을 자동으로 가져오려면 이 옵션을 선택합니다.
수동으로 정적 설정을 지정합니다	이 옵션을 선택한 다음 필드에 정적 주소를 입력합니다. (필요한 경우 주소를 잘라내어 필드에 붙여 넣을 수 있습니다.) IPv4의 경우 네트워크 서브넷 마스크 및 게이트웨이를 포함합니다. IPv6의 경우 라우팅 가능한 IP 주소와 라우터 IP 주소를 포함합니다.
VLAN 지원을 활성화합니다(* 추가 설정 표시 * 를 클릭하여 사용 가능).	VLAN을 활성화하고 해당 ID를 입력하려면 이 옵션을 선택합니다. VLAN은 동일한 스위치, 동일한 라우터 또는 둘 다에서 지원되는 다른 물리적 LAN(가상 LAN)과 물리적으로 분리된 것처럼 동작하는 논리 네트워크입니다.
이더넷 우선 순위 활성화(* 추가 설정 표시 * 를 클릭하여 사용 가능)	<p>네트워크 액세스 우선 순위를 결정하는 매개변수를 활성화하려면 이 옵션을 선택합니다. 슬라이더를 사용하여 1(최저)과 7(최고) 사이의 우선순위를 선택합니다.</p> <p>이더넷과 같은 공유 LAN(Local Area Network) 환경에서는 많은 스테이션이 네트워크 액세스에 대해 경합할 수 있습니다. 액세스는 선착순으로 제공됩니다. 두 스테이션이 동시에 네트워크에 액세스하려고 시도할 수 있으며, 이로 인해 두 스테이션이 다시 꺼졌다가 다시 시도하기 전에 대기하게 됩니다. 스위치 포트에 하나의 스테이션만 연결되어 있는 스위치 이더넷의 경우 이 프로세스가 최소화됩니다.</p>

7. 마침 * 을 클릭합니다.

iSCSI 인증을 구성합니다

iSCSI 네트워크의 보안을 강화하기 위해 컨트롤러(타겟)와 호스트(이니시에이터) 간에 인증을 설정할 수 있습니다. System Manager에서는 CHAP(Challenge Handshake Authentication Protocol) 방법을 사용하여 초기 링크 중에 대상 및 초기자의 ID를 확인합니다. 인증은 CHAPsecret이라는 공유 보안 키를 기반으로 합니다.

시작하기 전에

타겟(컨트롤러)에 대한 CHAP 암호를 설정하기 전이나 후에 이니시에이터(iSCSI 호스트)에 대한 CHAP 암호를 설정할 수 있습니다. 이 작업의 지침을 따르기 전에 호스트가 iSCSI 연결을 먼저 수행할 때까지 기다린 다음 개별 호스트에 CHAP 암호를 설정해야 합니다. 연결이 완료되면 호스트의 IQN 이름과 해당 CHAP 암호가 iSCSI 인증 대화 상자(이 작업에 설명되어 있음)에 나열되며, 수동으로 입력할 필요가 없습니다.

이 작업에 대해

다음 인증 방법 중 하나를 선택할 수 있습니다.

- * 단방향 인증 * — 컨트롤러가 iSCSI 호스트의 ID를 인증할 수 있도록 하려면 이 설정을 사용합니다(단방향 인증).
- * 양방향 인증 * — 컨트롤러와 iSCSI 호스트가 모두 인증(양방향 인증)을 수행할 수 있도록 하려면 이 설정을 사용합니다. 이 설정은 컨트롤러가 iSCSI 호스트의 ID를 인증할 수 있도록 하고, iSCSI 호스트가 컨트롤러의 ID를 인증할 수 있도록 하여 두 번째 수준의 보안을 제공합니다.



iSCSI 설정 및 기능은 스토리지 배열이 iSCSI를 지원하는 경우에만 설정 페이지에 표시됩니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. iSCSI 설정 * 에서 * 인증 구성 * 을 클릭합니다.

현재 설정된 방법을 보여 주는 * 인증 구성 * 대화 상자가 나타납니다. 또한 호스트에 CHAP 암호가 구성되어 있는지 여부도 표시됩니다.

3. 다음 중 하나를 선택합니다.
 - * 인증 없음 * — 컨트롤러가 iSCSI 호스트의 ID를 인증하지 않도록 하려면 이 옵션을 선택하고 * 마침 * 을 클릭합니다. 대화 상자가 닫히고 구성이 완료됩니다.
 - * 단방향 인증 * — 컨트롤러가 iSCSI 호스트의 ID를 인증할 수 있도록 하려면 이 옵션을 선택하고 * 다음 * 을 클릭하여 대상 CHAP 구성 대화 상자를 표시합니다.
 - * 양방향 인증 * — 컨트롤러와 iSCSI 호스트가 인증을 수행하도록 허용하려면 이 옵션을 선택하고 * 다음 * 을 클릭하여 대상 CHAP 구성 대화 상자를 표시합니다.
4. 단방향 또는 양방향 인증의 경우 컨트롤러의 CHAP 암호(타겟)를 입력하거나 확인합니다. CHAP 암호는 12자에서 57자 사이의 인쇄 가능한 ASCII 문자여야 합니다.



컨트롤러에 대한 CHAP 암호가 이전에 구성된 경우 필드의 문자가 마스킹됩니다. 필요한 경우 기존 문자를 바꿀 수 있습니다(새 문자는 마스킹되지 않음).

5. 다음 중 하나를 수행합니다.
 - one-way_authentication을 구성하는 경우 * Finish * 를 클릭합니다. 대화 상자가 닫히고 구성이 완료됩니다.
 - two-way_authentication을 구성하는 경우 * Next * 를 클릭하여 이니시에이터 CHAP 구성 대화 상자를 표시합니다.
6. 양방향 인증의 경우, 12-57자의 인쇄 가능한 ASCII 문자일 수 있는 iSCSI 호스트(이니시에이터)에 대한 CHAP 암호를 입력하거나 확인합니다. 특정 호스트에 대해 양방향 인증을 구성하지 않으려면 * Initiator CHAP Secret * 필드를 비워 둡니다.



호스트에 대한 CHAP 암호가 이전에 구성된 경우 필드의 문자가 마스킹됩니다. 필요한 경우 기존 문자를 바꿀 수 있습니다(새 문자는 마스킹되지 않음).

7. 마침 * 을 클릭합니다.

결과

인증을 지정하지 않은 경우, 컨트롤러와 iSCSI 호스트 간의 iSCSI 로그인 시퀀스 중에 인증이 발생합니다.

iSCSI 검색 설정을 활성화합니다

iSCSI 네트워크에서 스토리지 디바이스 검색과 관련된 설정을 설정할 수 있습니다. 대상 검색 설정을 사용하면 iSNS(Internet Storage Name Service) 프로토콜을 사용하여 스토리지 배열의 iSCSI 정보를 등록하고 명명되지 않은 검색 세션을 허용할지 여부를 결정할 수 있습니다.

시작하기 전에

iSNS 서버가 정적 IP 주소를 사용하는 경우 iSNS 등록에 해당 주소를 사용할 수 있어야 합니다. IPv4와 IPv6가 모두 지원됩니다.

이 작업에 대해

iSCSI 검색과 관련된 다음 설정을 활성화할 수 있습니다.

- * iSNS 서버를 사용하여 타겟을 등록합니다. * — 이 옵션을 설정하면 스토리지 어레이가 iSNS 서버의 iSCSI IQN(Qualified Name) 및 포트 정보를 등록합니다. 이 설정은 iSNS 검색을 허용하므로 이니시에이터는 iSNS 서버에서 IQN 및 포트 정보를 검색할 수 있습니다.
- * 이름 없는 검색 세션 활성화 * — 이름 없는 검색 세션이 활성화되면 이니시에이터(iSCSI 호스트)가 검색 유형 연결을 위한 로그인 시퀀스 중에 타겟(컨트롤러)의 IQN을 제공할 필요가 없습니다. 비활성화된 경우 호스트는 IQN을 제공하여 컨트롤러에 검색 세션을 설정해야 합니다. 하지만 정상(입출력 베어링) 세션에 대해서는 타겟 IQN이 항상 필요합니다. 이 설정을 비활성화하면 권한이 없는 iSCSI 호스트가 해당 IP 주소만 사용하여 컨트롤러에 연결하는 것을 방지할 수 있습니다.



iSCSI 설정 및 기능은 스토리지 배열이 iSCSI를 지원하는 경우에만 설정 페이지에 표시됩니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. iSCSI 설정 * 에서 * 대상 검색 설정 보기/편집 * 을 클릭합니다.

대상 검색 설정 * 대화 상자가 나타납니다. iSNS 서버 사용 *... 필드 아래에 컨트롤러가 이미 등록되어 있는지 여부를 나타내는 대화 상자가 나타납니다.

3. 컨트롤러를 등록하려면 * iSNS 서버를 사용하여 대상 등록 * 을 선택한 후 다음 중 하나를 선택합니다.
 - * DHCP 서버에서 자동으로 구성 가져오기 * — DHCP(Dynamic Host Configuration Protocol) 서버를 사용하여 iSNS 서버를 구성하려면 이 옵션을 선택합니다. 이 옵션을 사용하는 경우 컨트롤러의 모든 iSCSI 포트에서도 DHCP를 사용하도록 구성해야 합니다. 필요한 경우 컨트롤러 iSCSI 포트 설정을 업데이트하여 이 옵션을 활성화합니다.



DHCP 서버가 iSNS 서버 주소를 제공하려면 옵션 43--""공급업체 특정 정보"를 사용하도록 DHCP 서버를 구성해야 합니다. 이 옵션은 데이터 바이트 0xa-0xd(10-13)로 iSNS 서버 IPv4 주소를 포함해야 합니다.

- * 수동으로 정적 구성 지정 * — iSNS 서버의 정적 IP 주소를 입력하려면 이 옵션을 선택합니다. (필요한 경우 주소를 잘라내어 필드에 붙여 넣을 수 있습니다.) 필드에 IPv4 주소 또는 IPv6 주소를 입력합니다. 둘 다 구성된 경우 IPv4가 기본값입니다. 또한 TCP 수신 대기 포트를 입력합니다(기본값 3205를 사용하거나 49152와 65535 사이의 값을 입력합니다).
4. 스토리지 배열이 명명되지 않은 검색 세션에 참여할 수 있도록 하려면 * 명명되지 않은 검색 세션 활성화 * 를 선택합니다.
 - 이 옵션을 설정하면 컨트롤러의 정보를 검색하기 위해 타겟 IQN을 지정하는 데 iSCSI 이니시에이터가 필요하지

않습니다.

- 비활성화된 경우 이니시에이터가 타겟 IQN을 제공하지 않으면 검색 세션이 차단됩니다. 명명되지 않은 검색 세션을 비활성화하면 보안이 강화됩니다.

5. 저장 * 을 클릭합니다.

결과

System Manager에서 iSNS 서버에 컨트롤러를 등록하려고 하면 진행률 표시줄이 나타납니다. 이 프로세스는 최대 5분 정도 걸릴 수 있습니다.

iSCSI 통계 패키지를 봅니다

스토리지 배열에 대한 iSCSI 연결에 대한 데이터를 볼 수 있습니다.

이 작업에 대해

System Manager는 이러한 유형의 iSCSI 통계를 표시합니다. 모든 통계는 읽기 전용이며 설정할 수 없습니다.

- * 이더넷 MAC 통계 * — MAC(Media Access Control)에 대한 통계를 제공합니다. 또한 MAC는 실제 주소 또는 MAC 주소라는 주소 지정 메커니즘을 제공합니다. MAC 주소는 각 네트워크 어댑터에 할당된 고유한 주소입니다. MAC 주소는 하위 네트워크 내의 대상으로 데이터 패킷을 전송하는 데 도움이 됩니다.
- * 이더넷 TCP/IP 통계 * — TCP(Transmission Control Protocol) 및 IP(Internet Protocol)인 TCP/IP에 대한 통계를 제공합니다. TCP를 사용하면 네트워크로 연결된 호스트의 응용 프로그램이 서로 연결을 만들어 데이터를 패킷으로 교환할 수 있습니다. IP는 패킷 교환 방식의 네트워크를 통해 데이터를 전달하는 데이터 지향 프로토콜입니다. IPv4 통계 및 IPv6 통계는 별도로 표시됩니다.
- * 로컬 대상/초기자(프로토콜) 통계 * — iSCSI 대상에 대한 통계를 표시합니다. iSCSI 타겟은 해당 스토리지 미디어에 대한 블록 수준 액세스를 제공하고 비동기 미러링 작업에서 이니시에이터로 사용될 때 스토리지 배열에 대한 iSCSI 통계를 표시합니다.
- * DCBX 작업 상태 통계 * — 다양한 DCBX(Data Center Bridging Exchange) 기능의 작동 상태를 표시합니다.
- * LLDP TLV statistics * — LLDP(Link Layer Discovery Protocol) TLV(Type Length Value) 통계를 표시합니다.
- * DCBX TLV 통계 * — DCB(데이터 센터 브리징) 환경에서 스토리지 배열 호스트 포트를 식별하는 정보를 표시합니다. 이 정보는 식별 및 기능 목적으로 네트워크 피어와 공유됩니다.

각 통계를 원시 통계 또는 기준 통계로 볼 수 있습니다. 원시 통계는 컨트롤러가 시작된 이후 수집된 모든 통계입니다. 기준 통계는 기준 시간을 설정한 후 수집된 시점 통계입니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. iSCSI 통계 패키지 보기 * 를 선택합니다.
3. 탭을 클릭하여 다양한 통계 집합을 봅니다.
4. * 선택 사항: * 기준선을 설정하려면 * 새 기준선 설정 * 을 클릭합니다.

기준을 설정하면 통계 수집에 대한 새로운 시작 지점이 설정됩니다. 모든 iSCSI 통계에는 동일한 기준이 사용됩니다.

iSCSI 세션을 봅니다

스토리지 배열에 대한 iSCSI 연결에 대한 자세한 정보를 볼 수 있습니다. iSCSI 세션은 비동기 미러 관계의 호스트 또는 원격 스토리지 시스템에서 발생할 수 있습니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. iSCSI 세션 보기/종료 * 를 선택합니다.

현재 iSCSI 세션 목록이 나타납니다.

3. 특정 iSCSI 세션에 대한 추가 정보를 보려면 세션을 선택한 다음 * 세부 정보 보기 * 를 클릭합니다.

항목	설명
세션 식별자(SSID)	iSCSI 이니시에이터와 iSCSI 타겟 간의 세션을 식별하는 16진수 문자열입니다. SSID는 ISID와 TPGT로 구성됩니다.
이니시에이터 세션 ID(ISID)	세션 식별자의 이니시에이터 부분입니다. 초기자는 로그인 중에 ISID를 지정합니다.
대상 포털 그룹	iSCSI 타겟입니다.
대상 포털 그룹 태그(TPGT)	세션 식별자의 대상 부분. iSCSI 대상 포털 그룹의 16비트 숫자 식별자입니다.
이니시에이터 iSCSI 이름입니다	이니시에이터의 전 세계에서 고유한 이름입니다.
이니시에이터 iSCSI 레이블	System Manager에 설정된 사용자 레이블입니다.
이니시에이터 iSCSI 별칭입니다	iSCSI 노드와 연결할 수도 있는 이름입니다. 별칭을 사용하면 조직에서 사용자에게 친숙한 문자열을 iSCSI 이름과 연결할 수 있습니다. 그러나 별칭은 iSCSI 이름을 대체하는 것이 아닙니다. 이니시에이터 iSCSI 별칭은 호스트에서만 설정할 수 있고 System Manager에서는 설정할 수 없습니다
호스트	스토리지 배열에 입력 및 출력을 전송하는 서버입니다.
연결 ID(CID)	이니시에이터와 타겟 간의 세션 내 접속에 대한 고유한 이름입니다. 초기자는 이 ID를 생성하여 로그인 요청 중에 대상에 제공합니다. 연결이 닫히라는 로그아웃 중에도 연결 ID가 표시됩니다.
이더넷 포트 식별자입니다	연결과 관련된 컨트롤러 포트입니다.
이니시에이터 IP 주소입니다	이니시에이터의 IP 주소입니다.
협상된 로그인 매개 변수	iSCSI 세션 로그인 중에 트랜잭션되는 매개 변수입니다.
인증 방법	iSCSI 네트워크에 액세스할 사용자를 인증하는 기술입니다. 유효한 값은 * CHAP * 및 * 없음 * 입니다.
헤더 다이제스트 방법입니다	iSCSI 세션에 대해 가능한 헤더 값을 표시하는 기술입니다. HeaderDigest 및 DataDigest는 * None * 또는 * CRC32C * 일 수 있습니다. 두 가지 모두 기본값은 * 없음 * 입니다.

항목	설명
데이터 다이제스트 방법입니다	iSCSI 세션에 대해 가능한 데이터 값을 표시하는 기술입니다. HeaderDigest 및 DataDigest는 * None * 또는 * CRC32C * 일 수 있습니다. 두 가지 모두 기본값은 * 없음 * 입니다.
최대 연결 수	iSCSI 세션에 허용되는 최대 연결 수입니다. 최대 연결 수는 1 ~ 4입니다. 기본값은 * 1 * 입니다.
대상 별칭	대상과 연관된 레이블입니다.
이니시에이터 별칭입니다	이니시에이터와 연결된 레이블입니다.
대상 IP 주소입니다	iSCSI 세션의 타겟의 IP 주소입니다. DNS 이름은 지원되지 않습니다.
초기 R2T	초기 전송 준비 상태입니다. 상태는 * 예 * 또는 * 아니요 * 일 수 있습니다.
최대 버스트 길이	이 iSCSI 세션의 최대 SCSI 페이로드(바이트) 최대 버스트 길이는 512에서 262,144(256KB)입니다. 기본값은 * 262,144(256KB) * 입니다.
첫 번째 버스트 길이	이 iSCSI 세션에 대한 요청되지 않은 데이터의 SCSI 페이로드입니다. 첫 번째 버스트 길이는 512에서 131,072(128KB)일 수 있습니다. 기본값은 * 65,536(64KB) * 입니다.
기본 대기 시간입니다	연결 종료 또는 연결 재설정 후 연결을 시도하기 전에 대기하는 최소 시간(초)입니다. 기본 대기 시간은 0에서 3600 사이입니다. 기본값은 * 2 * 입니다.
기본 유지 시간	연결 종료 또는 연결 재설정 후에도 연결이 가능한 최대 시간(초)입니다. 기본 유지 시간은 0에서 3600 사이입니다. 기본값은 * 20 * 입니다.
최대 미결 R2T	이 iSCSI 세션에 대해 최대 "전송 준비 완료" 수입니다. 전송 준비 완료 최대 값은 1에서 16 사이의 값일 수 있습니다. 기본값은 * 1 * 입니다.
복구 수준 오류	이 iSCSI 세션에 대한 오류 복구 수준입니다. 오류 복구 레벨 값은 항상 * 0 * 으로 설정됩니다.
최대 수신 데이터 세그먼트 길이	이니시에이터 또는 타겟이 iSCSI PDU(페이로드 데이터 유닛)에서 수신할 수 있는 최대 데이터 양입니다.
대상 이름입니다	대상의 공식 이름(별칭 아님). 대상 이름(_iqn_format)입니다.
이니시에이터 이름입니다	이니시에이터의 공식 이름(별칭 아님) <i>iqn</i> 또는 <i>_eui_format</i> 을 사용하는 이니시에이터 이름입니다.

4. * 선택 사항: * 보고서를 파일에 저장하려면 * 저장 * 을 클릭합니다.

이 파일은 브라우저의 다운로드 폴더에 "iscsi-session-connections.txt"라는 파일 이름으로 저장됩니다.

iSCSI 세션을 종료합니다

더 이상 필요하지 않은 iSCSI 세션을 종료할 수 있습니다. iSCSI 세션은 비동기 미러 관계의 호스트 또는 원격 스토리지 시스템에서 발생할 수 있습니다.

이 작업에 대해

다음과 같은 이유로 iSCSI 세션을 종료할 수 있습니다.

- * 무단 액세스 * — iSCSI 초기자가 로그인되어 있고 액세스 권한이 없는 경우 iSCSI 세션을 종료하여 iSCSI 초기자를 스토리지 배열에서 강제로 끌 수 있습니다. 사용 가능한 인증 방법이 없으므로 iSCSI 초기자가 로그인할 수 있습니다.
- * 시스템 다운타임 * — 스토리지 배열을 중지시켜야 하고 iSCSI 초기자가 여전히 로그인 상태인 것을 볼 경우 iSCSI 세션을 종료하여 스토리지 배열에서 iSCSI 초기자를 가져올 수 있습니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. iSCSI 세션 보기/종료 * 를 선택합니다.

현재 iSCSI 세션 목록이 나타납니다.

3. 종료할 세션을 선택합니다
4. 세션 종료 * 를 클릭하고 작업을 수행할지 확인합니다.

InfiniBand 포트를 통해 iSER 구성

컨트롤러에 InfiniBand 포트를 통한 iSER이 포함된 경우 호스트에 대한 네트워크 연결을 구성할 수 있습니다.

시작하기 전에

- 컨트롤러에 InfiniBand 포트를 통한 iSER이 포함되어야 합니다. 그렇지 않으면 InfiniBand를 통한 iSER 설정을 System Manager에서 사용할 수 없습니다.
- 호스트 연결의 IP 주소를 알아야 합니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다
2. iSER over InfiniBand settings * 에서 * Configure iSER over InfiniBand ports * 를 선택합니다.
3. 구성하려는 InfiniBand 포트를 통해 iSER이 있는 컨트롤러를 클릭합니다. 다음 * 을 클릭합니다.
4. 드롭다운 목록에서 구성할 HIC 포트를 선택한 다음 호스트의 IP 주소를 입력합니다.
5. 마침 * 을 클릭합니다.
6. iSER을 InfiniBand 포트로 재설정하려면 * 예 * 를 클릭합니다.

InfiniBand 통계를 통해 iSER 보기

스토리지 어레이의 컨트롤러에 InfiniBand 포트를 통한 iSER이 포함된 경우 호스트 연결에 대한 데이터를 볼 수 있습니다.

이 작업에 대해

System Manager는 InfiniBand 통계를 통해 다음과 같은 유형의 iSER을 보여 줍니다. 모든 통계는 읽기 전용이며 설정할 수 없습니다.

- * 로컬 타겟(프로토콜) 통계 * — InfiniBand 타겟에 대한 iSER 통계를 제공하며, 이 통계는 스토리지 미디어에 대한 블록 레벨 액세스를 보여줍니다.
- InfiniBand 인터페이스 통계 * 를 통한 * iSER — InfiniBand 인터페이스의 모든 iSER 포트에 대한 통계를 제공하며, 여기에는 각 스위치 포트와 관련된 성능 통계 및 링크 오류 정보가 포함됩니다.

각 통계를 원시 통계 또는 기준 통계로 볼 수 있습니다. 원시 통계는 컨트롤러가 시작된 이후 수집된 모든 통계입니다. 기준 통계는 기준 시간을 설정한 후 수집된 시점 통계입니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. InfiniBand 통계 * 를 통해 iSER 보기 * 를 선택합니다.
3. 탭을 클릭하여 다양한 통계 집합을 봅니다.
4. * 선택 사항: * 기준선을 설정하려면 * 새 기준선 설정 * 을 클릭합니다.

기준을 설정하면 통계 수집에 대한 새로운 시작 지점이 설정됩니다. InfiniBand 통계에서 모든 iSER에 동일한 기준선이 사용됩니다.

FAQ 를 참조하십시오

등록을 위해 iSNS 서버를 사용하면 어떻게 됩니까?

iSNS(Internet Storage Name Service) 서버 정보를 사용하는 경우 iSNS 서버를 쿼리하여 타겟(컨트롤러)에서 정보를 검색하도록 호스트(이니시에이터)를 구성할 수 있습니다.

이 등록을 통해 iSNS 서버에 컨트롤러의 IQN(iSCSI Qualified Name) 및 포트 정보를 제공하고 이니시에이터(iSCSI 호스트)와 타겟(컨트롤러) 간의 쿼리를 허용합니다.

iSCSI에 대해 자동으로 지원되는 등록 방법은 무엇입니까?

iSCSI 구현에서는 iSNS(Internet Storage Name Service) 검색 방법이나 대상 보내기 명령을 사용할 수 있습니다.

iSNS 방법을 사용하면 이니시에이터(iSCSI 호스트)와 타겟(컨트롤러) 간에 iSNS 검색을 수행할 수 있습니다. iSNS 서버에 컨트롤러의 IQN(iSCSI Qualified Name) 및 포트 정보를 제공하기 위해 타겟 컨트롤러를 등록합니다.

iSNS를 구성하지 않으면 iSCSI 호스트가 iSCSI 검색 세션 중에 대상 보내기 명령을 전송할 수 있습니다. 이에 따라 컨트롤러는 포트 정보(예: 대상 IQN, 포트 IP 주소, 수신 포트 및 대상 포트 그룹)를 반환합니다. iSNS를 사용하는 경우 호스트 이니시에이터가 iSNS 서버에서 대상 IP를 검색할 수 있으므로 이 검색 방법은 필요하지 않습니다.

InfiniBand 통계를 통해 iSER을 어떻게 해석합니까?

View iSER over InfiniBand Statistics(InfiniBand를 통한 iSER 통계 보기) 대화 상자에는 로컬 타겟(프로토콜) 통계와 iSER over InfiniBand(IB) 인터페이스 통계가 표시됩니다. 모든 통계는 읽기 전용이며 설정할 수 없습니다.

- * 로컬 타겟(프로토콜) 통계 * — InfiniBand 타겟에 대한 iSER 통계를 제공하며, 이 통계는 스토리지 미디어에 대한 블록 레벨 액세스를 보여줍니다.
- InfiniBand 인터페이스 통계 * 를 통한 * iSER — InfiniBand 인터페이스의 InfiniBand 포트를 통해 모든 iSER에 대한 통계를 제공하며, 여기에는 각 스위치 포트와 관련된 성능 통계 및 링크 오류 정보가 포함됩니다.

각 통계를 원시 통계 또는 기준 통계로 볼 수 있습니다. 원시 통계는 컨트롤러가 시작된 이후 수집된 모든 통계입니다. 기준 통계는 기준 시간을 설정한 후 수집된 시점 통계입니다.

InfiniBand를 통해 iSER을 구성하거나 진단하려면 어떻게 해야 합니까?

다음 표에는 InfiniBand 세션을 통해 iSER을 구성 및 관리하는 데 사용할 수 있는 System Manager 기능이 나와 있습니다.



InfiniBand를 통한 iSER 설정은 스토리지 어레이의 컨트롤러에 InfiniBand 호스트 관리 포트를 통한 iSER이 포함된 경우에만 사용할 수 있습니다.

InfiniBand를 통해 iSER 구성 및 진단

조치	위치
InfiniBand 포트를 통해 iSER 구성	<ol style="list-style-type: none">1. 하드웨어 * 를 선택합니다.2. Show back of shelf * 를 선택합니다.3. 컨트롤러를 선택합니다.4. InfiniBand 포트를 통해 iSER 구성 * 을 선택합니다. <p>또는</p> <ol style="list-style-type: none">1. 메뉴: 설정 [시스템] * 을 선택합니다.2. InfiniBand 설정을 통해 * iSER * 로 스크롤한 다음 * InfiniBand 포트를 통해 iSER 구성 * 을 선택합니다.
InfiniBand 통계를 통해 iSER 보기	<ol style="list-style-type: none">1. 메뉴: 설정 [시스템] * 을 선택합니다.2. InfiniBand 설정 * 을 통해 * iSER로 스크롤한 다음 * InfiniBand 통계 * 를 통해 iSER 보기 * 를 선택합니다.

시스템: NVMe 설정

개념

NVMe 개요

일부 컨트롤러에는 패브릭을 통해 NVMe(비휘발성 메모리 익스프레스)를 구현하기 위한 포트가 포함되어 있습니다. NVMe를 사용하면 호스트와 스토리지 어레이 간에 고성능 통신이 가능합니다.

NVMe란 무엇입니까?

NVMe는 "비휘발성 메모리"를 나타내며 다양한 유형의 저장 장치에 사용되는 영구 메모리입니다. NVMe(NVM Express)는 NVM 장치와의 고성능 다중 대기열 통신을 위해 특별히 설계된 표준 인터페이스 또는 프로토콜입니다.

NVMe over Fabrics란?

NVMe over Fabrics (NVMe-oF)는 NVMe 메시지 기반 명령 및 데이터가 네트워크를 통해 호스트 컴퓨터와 스토리지 간에 전송되도록 하는 기술 사양입니다. Fabric을 사용하는 호스트에서 NVMe 스토리지 어레이(_subsystem)에 액세스할 수 있습니다. NVMe 명령은 호스트 측과 하위 시스템 측 모두에서 전송 추상화 계층에서 활성화 및 캡슐화됩니다. 이를 통해 고성능 NVMe 인터페이스 엔드 투 엔드를 호스트에서 스토리지로 확장하고 명령 세트를 표준화하여 단순화합니다.

NVMe-oF 스토리지는 호스트에 로컬 블록 스토리지 디바이스로 표시됩니다. 다른 블록 스토리지 디바이스와 마찬가지로 볼륨(namespace)을 파일 시스템에 마운트할 수 있습니다. REST API, SMCli 또는 SANtricity System Manager를 사용하여 필요에 따라 스토리지를 프로비저닝할 수 있습니다.

NVMe 적격 이름(NQN)이란 무엇입니까?

NVMe 정규화된 이름(NQN)은 원격 스토리지 타겟을 식별하는 데 사용됩니다. 스토리지 배열의 NVMe 정규화된 이름은 항상 서브시스템에 의해 할당되며 수정할 수 없습니다. 전체 어레이에 대해 하나의 NVMe 정규화된 이름만 있습니다. NVMe 적격 이름은 223자로 제한됩니다. iSCSI 정규화된 이름과 비교할 수 있습니다.

네임스페이스 및 네임스페이스 ID란 무엇입니까?

네임스페이스는 SCSI의 논리 유닛과 동일하며 어레이의 볼륨과 관련이 있습니다. NSCID(Namespace ID)는 SCSI의 LUN(Logical Unit Number)과 동일합니다. 네임스페이스 생성 시 NSID를 만들고 1에서 255 사이의 값으로 설정할 수 있습니다.

NVMe 컨트롤러란 무엇입니까?

호스트 이니시에이터에서 스토리지 시스템의 타겟으로 연결되는 경로를 나타내는 SCSI I_T Nexus와 마찬가지로, 호스트 연결 프로세스 중에 생성된 NVMe 컨트롤러는 스토리지 어레이의 네임스페이스와 호스트 간의 액세스 경로를 제공합니다. 호스트의 NQN 및 호스트 포트 식별자는 NVMe 컨트롤러를 고유하게 식별합니다. NVMe 컨트롤러는 단일 호스트에만 연결될 수 있지만 여러 네임스페이스에 액세스할 수 있습니다.

SANtricity System Manager를 사용하여 호스트에 대한 네임스페이스 ID를 설정하고 네임스페이스에 액세스할 수 있는 호스트를 구성할 수 있습니다. 그런 다음 NVMe 컨트롤러가 생성되면 NVMe 컨트롤러에서 액세스할 수 있는 네임스페이스 ID 목록을 생성하여 허용 가능한 연결을 구성하는 데 사용합니다.

NVMe 관련 용어

NVMe 용어가 스토리지 어레이에 어떻게 적용되는지 알아보십시오.

기간	설명
InfiniBand	IB(InfiniBand)는 고성능 서버와 스토리지 시스템 간의 데이터 전송을 위한 통신 표준입니다.
네임스페이스	네임스페이스는 블록 액세스를 위해 포맷된 NVM 스토리지입니다. 스토리지 배열의 볼륨과 관련된 SCSI의 논리 유닛과 유사합니다.
네임스페이스 ID입니다	네임스페이스 ID는 네임스페이스에 대한 NVMe 컨트롤러의 고유 식별자이며 1에서 255 사이의 값으로 설정할 수 있습니다. SCSI의 LUN(Logical Unit Number)과 유사합니다.
NQN	NVMe 정규화된 이름(NQN)은 원격 스토리지 대상(스토리지 어레이)을 식별하는 데 사용됩니다.
NVM	NVM(비휘발성 메모리)은 다양한 유형의 스토리지 장치에서 사용되는 영구 메모리입니다.
NVMe를 참조하십시오	NVMe(비휘발성 메모리 익스프레스)는 SSD 드라이브와 같은 플래시 기반 스토리지 장치를 위해 설계된 인터페이스입니다. NVMe는 이전 논리 장치 인터페이스와 비교하여 I/O 오버헤드를 줄이고 성능 개선을 포함합니다.
NVMe - oF	NVMe-oF(Non-Volatile Memory Express over Fabrics)는 NVMe 명령 및 데이터가 호스트와 스토리지 간의 네트워크를 통해 전송되도록 하는 사양입니다.
NVMe 컨트롤러	호스트 연결 프로세스 중에 NVMe 컨트롤러가 생성됩니다. 스토리지 배열의 네임스페이스와 호스트 간의 액세스 경로를 제공합니다.
NVMe 전담팀	큐는 NVMe 인터페이스를 통해 명령 및 메시지를 전달하는 데 사용됩니다.
NVMe 하위 시스템	NVMe 호스트 연결이 있는 스토리지 어레이
RDMA 를 참조하십시오	RDMA(Remote Direct Memory Access)를 사용하면 네트워크 인터페이스 카드(NIC) 하드웨어에 전송 프로토콜을 구현하여 서버 내외부로 데이터를 더욱 직접 이동할 수 있습니다.
RoCE	RoCE(RDMA over Converged Ethernet)는 이더넷 네트워크를 통한 RDMA(Remote Direct Memory Access)를 지원하는 네트워크 프로토콜입니다.
SSD를 지원합니다	SSD(Solid-State Disk)는 데이터를 영구적으로 저장하기 위해 솔리드 스테이트 메모리 (플래시)를 사용하는 데이터 스토리지 장치입니다. SSD는 기존의 하드 드라이브를 에뮬레이트하며 하드 드라이브에서 사용하는 것과 동일한 인터페이스로 사용할 수 있습니다.

방법

InfiniBand 포트를 통해 NVMe를 구성합니다

컨트롤러에 InfiniBand 연결을 통한 NVMe가 포함된 경우 시스템 페이지에서 NVMe 포트 설정을 구성할 수 있습니다.

시작하기 전에

- 컨트롤러에서 NVMe over InfiniBand 호스트 포트를 포함해야 합니다. 그렇지 않으면 System Manager에서 NVMe over InfiniBand 설정을 사용할 수 없습니다.
- 호스트 연결의 IP 주소를 알아야 합니다.



NVMe over InfiniBand 설정 및 기능은 스토리지 어레이 컨트롤러에 NVMe over InfiniBand 포트가 포함된 경우에만 표시됩니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. InfiniBand를 통한 NVMe 설정 * 에서 * InfiniBand 포트를 통한 NVMe 구성 * 을 선택합니다.
3. 구성할 NVMe over InfiniBand 포트가 있는 컨트롤러를 선택합니다. 다음 * 을 클릭합니다.
4. 드롭다운 목록에서 구성할 HIC 포트를 선택한 다음 IP 주소를 입력합니다.

200GB 사용 HIC를 포함하는 EF600 스토리지 어레이를 구성하는 경우 이 대화 상자에 물리적 포트(외부)용 IP 주소 필드와 가상 포트(내부)용 IP 주소 필드가 2개 표시됩니다. 두 포트에 대해 고유한 IP 주소를 할당해야 합니다. 이러한 설정을 통해 호스트는 각 포트 간에 경로를 설정하고 HIC는 최대 성능을 달성할 수 있습니다. IP 주소를 가상 포트에 할당하지 않으면 HIC는 약 절반 수준의 속도로 실행됩니다.

5. 마침 * 을 클릭합니다.
6. Yes * 를 클릭하여 NVMe over InfiniBand 포트를 재설정합니다.

NVMe over RoCE 포트를 구성합니다

컨트롤러에 NVMe over RoCE(RDMA over Converged Ethernet)에 대한 연결이 포함되어 있는 경우 시스템 페이지에서 NVMe 포트 설정을 구성할 수 있습니다.

시작하기 전에


- 컨트롤러에 NVMe over RoCE 호스트 포트가 포함되어야 합니다. 그렇지 않으면 System Manager에서 NVMe over RoCE 설정을 사용할 수 없습니다.
- 호스트 연결의 IP 주소를 알아야 합니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. NVMe over ROCE 설정 * 에서 * Configure NVMe over ROCE ports * 를 선택합니다.
3. 구성할 NVMe over RoCE 포트가 있는 컨트롤러를 선택합니다. 다음 * 을 클릭합니다.
4. 드롭다운 목록에서 구성할 HIC 포트를 선택합니다. 다음 * 을 클릭합니다.
5. 포트 설정을 구성합니다.

모든 포트 설정을 보려면 대화 상자 오른쪽에 있는 * 추가 포트 설정 표시 * 링크를 클릭합니다.

필드 세부 정보

포트 설정	설명
이더넷 포트 속도를 구성했습니다	포트에서 SFP의 속도 기능과 일치하는 속도를 선택합니다.
IPv4 사용/IPv6 사용	IPv4 및 IPv6 네트워크에 대한 지원을 활성화하려면 하나 또는 두 옵션을 모두 선택하십시오. <div>  <div>포트 액세스를 비활성화하려면 두 확인란을 모두 선택 취소합니다.</div> </div>
MTU 크기(* 추가 포트 설정 표시 * 를 클릭하여 사용 가능)	필요한 경우 MTU(Maximum Transmission Unit)에 대한 새 크기를 바이트 단위로 입력합니다. 기본 MTU(Maximum Transmission Unit) 크기는 프레임당 1,500바이트입니다. 1500에서 9000 사이의 값을 입력해야 합니다.

IPv4 사용 * 을 선택한 경우 * 다음 * 을 클릭하면 IPv4 설정을 선택할 수 있는 대화 상자가 열립니다. IPv6 사용 * 을 선택한 경우 * 다음 * 을 클릭하면 IPv6 설정을 선택할 수 있는 대화 상자가 열립니다. 두 옵션을 모두 선택한 경우 IPv4 설정에 대한 대화 상자가 먼저 열리고 * 다음 * 을 클릭하면 IPv6 설정에 대한 대화 상자가 열립니다.

1. IPv4 및/또는 IPv6 설정을 자동 또는 수동으로 구성합니다.

필드 세부 정보

포트 설정	설명
자동으로 구성을 가져옵니다	구성을 자동으로 가져오려면 이 옵션을 선택합니다.
수동으로 정적 설정을 지정합니다	이 옵션을 선택한 다음 필드에 정적 주소를 입력합니다. (필요한 경우 주소를 잘라내어 필드에 붙여 넣을 수 있습니다.) IPv4의 경우 네트워크 서브넷 마스크 및 게이트웨이를 포함합니다. IPv6의 경우 라우팅 가능한 IP 주소와 라우터 IP 주소를 포함합니다. 200GB 사용 HIC를 포함하는 EF600 스토리지 어레이를 구성하는 경우 이 대화 상자에 네트워크 매개 변수에 대한 두 개의 필드 세트가 물리적 포트(외부)에 대해, 가상 포트(내부)에 대해 하나씩 표시됩니다. 두 포트에 대해 고유한 매개 변수를 할당해야 합니다. 이러한 설정을 통해 호스트는 각 포트 간에 경로를 설정하고 HIC는 최대 성능을 달성할 수 있습니다. IP 주소를 가상 포트에 할당하지 않으면 HIC는 약 절반 수준의 속도로 실행됩니다.

2. 마침 * 을 클릭합니다.

NVMe over Fabrics 통계 보기

스토리지 어레이에 대한 NVMe over Fabrics 연결에 대한 데이터를 볼 수 있습니다.

이 작업에 대해

System Manager에는 이러한 유형의 NVMe over Fabrics 통계가 표시됩니다. 모든 통계는 읽기 전용이며 설정할 수 없습니다.

- * NVMe 하위 시스템 통계 * — NVMe 컨트롤러 및 해당 대기열에 대한 통계를 표시합니다. NVMe 컨트롤러는 스토리지 배열의 네임스페이스와 호스트 간의 액세스 경로를 제공합니다. 연결 실패, 재설정 및 종료 같은 항목에 대한 NVMe 하위 시스템 통계를 검토할 수 있습니다.
- RDMA 인터페이스 통계 * — RDMA 인터페이스의 모든 NVMe over Fabrics 포트에 대한 통계를 제공하며, 여기에는 각 스위치 포트에 연결된 성능 통계 및 링크 오류 정보가 포함됩니다. 이 탭은 NVMe over Fabrics 포트를 사용할 수 있을 때만 나타납니다.

각 통계를 원시 통계 또는 기준 통계로 볼 수 있습니다. 원시 통계는 컨트롤러가 시작된 이후 수집된 모든 통계입니다. 기준 통계는 기준 시간을 설정한 후 수집된 시점 통계입니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. View NVMe over Fabrics Statistics * 를 선택합니다.
3. * 선택 사항: * 기준선을 설정하려면 * 새 기준선 설정 * 을 클릭합니다.

기준을 설정하면 통계 수집에 대한 새로운 시작 지점이 설정됩니다. 모든 NVMe 통계에 동일한 기준선이 사용됩니다.

FAQ 를 참조하십시오

NVMe over Fabrics 통계를 어떻게 해석합니까?

NVMe over Fabrics 통계 보기 대화 상자에는 NVMe 하위 시스템과 RDMA 인터페이스에 대한 통계가 표시됩니다. 모든 통계는 읽기 전용이며 설정할 수 없습니다.

- * NVMe 하위 시스템 통계 * — NVMe 컨트롤러 및 해당 대기열에 대한 통계를 표시합니다. NVMe 컨트롤러는 스토리지 배열의 네임스페이스와 호스트 간의 액세스 경로를 제공합니다. 연결 실패, 재설정 및 종료 같은 항목에 대한 NVMe 하위 시스템 통계를 검토할 수 있습니다. 이러한 통계에 대한 자세한 내용을 보려면 * 표 제목에 대한 범례 보기 * 를 클릭하십시오.
- RDMA 인터페이스 통계 * — RDMA 인터페이스의 모든 NVMe over Fabrics 포트에 대한 통계를 제공하며, 여기에는 각 스위치 포트에 연결된 성능 통계 및 링크 오류 정보가 포함됩니다. 이 탭은 NVMe over Fabrics 포트를 사용할 수 있을 때만 나타납니다. 통계에 대한 자세한 내용을 보려면 * 표 제목에 대한 범례 보기 * 를 클릭합니다.

각 통계를 원시 통계 또는 기준 통계로 볼 수 있습니다. 원시 통계는 컨트롤러가 시작된 이후 수집된 모든 통계입니다. 기준 통계는 기준 시간을 설정한 후 수집된 시점 통계입니다.

InfiniBand를 통해 **NVMe**를 구성하거나 진단하려면 어떻게 해야 합니까?

다음 표에는 InfiniBand를 통해 NVMe를 구성하고 관리하는 데 사용할 수 있는 System Manager 기능이 나와 있습니다.



NVMe over InfiniBand 설정은 스토리지 어레이 컨트롤러에 NVMe over InfiniBand 포트가 포함된 경우에만 사용할 수 있습니다.

조치	위치
InfiniBand 포트를 통해 NVMe를 구성합니다	<ol style="list-style-type: none"> 1. 하드웨어 * 를 선택합니다. 2. Show back of shelf * 를 선택합니다. 3. 컨트롤러를 선택합니다. 4. Configure NVMe over InfiniBand ports * 를 선택합니다. <p>또는</p> <ol style="list-style-type: none"> 1. 메뉴: 설정 [시스템] * 을 선택합니다. 2. 아래로 스크롤하여 * NVMe over InfiniBand settings * 로 이동한 다음 * Configure NVMe over InfiniBand Ports * 를 선택합니다.
InfiniBand를 통한 NVMe 통계 보기	<ol style="list-style-type: none"> 1. 메뉴: 설정 [시스템] * 을 선택합니다. 2. 아래로 스크롤하여 * NVMe over InfiniBand settings * 를 선택한 다음 * View NVMe over Fabrics Statistics * 를 선택합니다.

NVMe over RoCE를 구성 또는 진단하려면 어떻게 해야 하나요?

하드웨어 및 설정 페이지에서 NVMe over RoCE를 구성 및 관리할 수 있습니다.



NVMe over RoCE 설정은 스토리지 어레이의 컨트롤러에 NVMe over RoCE 포트가 포함된 경우에만 사용할 수 있습니다.

NVMe over RoCE를 구성하고 진단합니다

조치	위치
NVMe over RoCE 포트를 구성합니다	<ol style="list-style-type: none"> 1. 하드웨어 * 를 선택합니다. 2. Show back of shelf * 를 선택합니다. 3. 컨트롤러를 선택합니다. 4. RoCE 포트를 통한 NVMe 구성 * 을 선택합니다. <p>또는</p> <ol style="list-style-type: none"> 1. 메뉴: 설정 [시스템] * 을 선택합니다. 2. 아래로 * NVMe over RoCE 설정 * 으로 스크롤한 다음 * Configure NVMe over RoCE Ports * 를 선택합니다.
NVMe over Fabrics 통계 보기	<ol style="list-style-type: none"> 1. 메뉴: 설정 [시스템] * 을 선택합니다. 2. 아래로 * NVMe over RoCE 설정 * 으로 스크롤한 다음 * NVMe over Fabrics 통계 보기 * 를 선택합니다.

하나의 물리적 포트에 대해 두 개의 IP 주소가 있는 이유는 무엇입니까?

EF600 스토리지 어레이에는 2개의 HIC, 즉 외부 스토리지와 내부 HIC를 각각 하나씩 포함할 수 있습니다.

이 구성에서는 외부 HIC를 내부 보조 HIC에 연결합니다. 외부 HIC에서 액세스할 수 있는 각 물리적 포트에는 내부 HIC에서 연결된 가상 포트가 있습니다.

최대 200GB 성능을 얻으려면 호스트가 각 포트에 연결을 설정할 수 있도록 물리적 포트와 가상 포트 모두에 대해 고유한 IP 주소를 할당해야 합니다. IP 주소를 가상 포트에 할당하지 않으면 HIC는 약 절반 수준의 속도로 실행됩니다.

물리적 포트 하나에 대해 두 개의 매개 변수 세트가 있는 이유는 무엇입니까?

EF600 스토리지 어레이에는 2개의 HIC, 즉 외부 스토리지와 내부 HIC를 각각 하나씩 포함할 수 있습니다.

이 구성에서는 외부 HIC를 내부 보조 HIC에 연결합니다. 외부 HIC에서 액세스할 수 있는 각 물리적 포트에는 내부 HIC에서 연결된 가상 포트가 있습니다.

최대 200GB 성능을 얻으려면 호스트가 각 포트에 대한 연결을 설정할 수 있도록 물리적 포트와 가상 포트 모두에 대해 매개 변수를 할당해야 합니다. 가상 포트에 매개 변수를 할당하지 않으면 HIC는 약 절반 수준의 속도로 실행됩니다.

시스템: 추가 기능

개념

애드온 기능의 작동 방식

추가 기능은 System Manager의 표준 구성에 포함되지 않은 기능으로, 활성화하려면 키가 필요할 수 있습니다. 애드온 기능은 단일 프리미엄 기능 또는 번들 기능 팩일 수 있습니다.

다음 단계에서는 프리미엄 기능 또는 기능 팩을 사용하는 방법을 개괄적으로 설명합니다.

1. 다음 정보를 얻습니다.
 - 설치할 기능의 스토리지 배열을 식별하는 새시 일련 번호 및 기능 활성화 식별자. 이러한 항목은 System Manager에서 사용할 수 있습니다.
 - 기능 활성화 코드 - 기능 구매 시 지원 사이트에서 사용할 수 있습니다.
2. 스토리지 공급업체에 문의하거나 프리미엄 기능 활성화 사이트에 액세스하여 기능 키를 얻습니다. 새시 일련 번호, 활성화 식별자 및 활성화를 위한 기능 코드를 제공합니다.
3. System Manager를 사용하여 기능 키 파일을 사용하여 프리미엄 기능 또는 기능 팩을 활성화합니다.

애드온 기능 용어

애드온 기능 조건이 스토리지 어레이에 적용되는 방식에 대해 알아보십시오.

기간	설명
기능 활성화 식별자	Feature Enable Identifier는 특정 스토리지 배열을 식별하는 고유한 문자열입니다. 이 식별자는 프리미엄 기능을 사용할 때 특정 스토리지 어레이에만 연결되도록 합니다. 이 문자열은 시스템 페이지의 추가 기능 아래에 표시됩니다.
피쳐 키 파일	기능 키 파일은 프리미엄 기능 또는 기능 팩의 잠금 해제 및 활성화를 위해 제공되는 파일입니다.
기능 팩	기능 팩은 스토리지 배열 속성을 변경하는 번들(예: 프로토콜을 Fibre Channel에서 iSCSI로 변경)입니다. 기능 팩을 사용하려면 특수 키가 필요합니다.
프리미엄 기능	프리미엄 기능은 추가 옵션으로, 이를 활성화하려면 키가 필요합니다. System Manager의 표준 구성에는 포함되어 있지 않습니다.

방법

기능 키 파일을 가져옵니다

스토리지 어레이에서 프리미엄 기능 또는 기능 팩을 활성화하려면 먼저 기능 키 파일을 구해야 합니다. 키는 하나의 스토리지 배열에만 연결됩니다.

이 작업에 대해

이 작업에서는 기능에 필요한 정보를 수집한 다음 기능 키 파일에 대한 요청을 보내는 방법을 설명합니다. 필수 정보는 다음과 같습니다.

- 새시 일련 번호입니다
- 기능 활성화 식별자
- 기능 활성화 코드

단계

1. System Manager에서 새시 일련 번호를 찾아 기록합니다. 지원 센터 타일에 마우스를 올려 놓으면 이 일련 번호를 볼 수 있습니다.
2. System Manager에서 Enable Identifier 기능을 찾습니다. 메뉴: 설정 [시스템] * 으로 이동한 다음 아래로 스크롤하여 * 추가 기능 * 으로 이동합니다. Feature Enable Identifier * 를 찾습니다. 기능 식별자 활성화 의 번호를 기록합니다.
3. 기능 활성화를 위한 코드를 찾아 기록합니다. 기능 팩의 경우 이 코드는 변환을 수행하기 위한 적절한 지침에 나와 있습니다.

NetApp 지침은 에서 확인할 수 있습니다 ["NetApp E-Series 시스템 설명서 센터 를 참조하십시오"](#).

프리미엄 기능의 경우 지원 사이트에서 다음과 같이 활성화 코드에 액세스할 수 있습니다.

- a. 에 로그인합니다 ["NetApp 지원"](#).
- b. 사용 중인 제품의 * 소프트웨어 라이선스 * 로 이동합니다.
- c. 스토리지 어레이 새시의 일련 번호를 입력하고 * Go * 를 클릭합니다.

- d. 라이선스 키 * 열에서 기능 활성화 코드를 찾습니다.
 - e. 원하는 기능에 대한 기능 활성화 코드를 기록합니다.
4. 새시 일련 번호, 활성화 식별자 및 기능 활성화를 위한 코드와 같은 정보를 사용하여 스토리지 공급업체에 이메일 또는 텍스트 문서를 보내 기능 키 파일을 요청합니다.
- 로 이동할 수도 있습니다 ["NetApp 라이선스 활성화: 스토리지 어레이 프리미엄 기능 활성화"](#) 및 필요한 정보를 입력하여 기능 팩 또는 기능 팩을 얻습니다. (이 사이트의 지침은 기능 팩이 아닌 프리미엄 기능에 대한 것입니다.)

작업을 마친 후

기능 키 파일이 있는 경우 프리미엄 기능 또는 기능 팩을 활성화할 수 있습니다.

프리미엄 기능 지원

프리미엄 기능은 활성화를 위한 키가 필요한 추가 옵션입니다.

시작하기 전에

- 기능 키를 받았습니다. 필요한 경우 기술 지원 부서에 키를 문의하십시오.
- 키 파일을 관리 클라이언트(System Manager 액세스를 위한 브라우저가 있는 시스템)에 로드했습니다.

이 작업에 대해

이 작업에서는 System Manager를 사용하여 프리미엄 기능을 활성화하는 방법을 설명합니다.



프리미엄 기능을 비활성화하려면 CLI(Command Line Interface)에서 Disable Storage Array feature 명령(`dissable storageArray(featurePack | feature=featureAttributeList)`)을 사용해야 합니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. 추가 기능 * 에서 * 프리미엄 기능 사용 * 을 선택합니다.

Premium 기능 사용 대화 상자가 열립니다.

3. 찾아보기 * 를 클릭한 다음 키 파일을 선택합니다.

대화 상자에 파일 이름이 표시됩니다.

4. 사용 * 을 클릭합니다.

기능 팩을 활성화합니다

기능 팩은 스토리지 배열 속성을 변경하는 번들(예: 프로토콜을 Fibre Channel에서 iSCSI로 변경)입니다. 기능 팩에는 지원을 위한 특수 키가 필요합니다.

시작하기 전에

- 변환을 수행하고 새 스토리지 배열 속성을 위한 시스템을 준비하기 위한 적절한 지침을 따랐습니다.



변환 지침은 에서 확인할 수 있습니다 ["NetApp E-Series 시스템 설명서 센터 를 참조하십시오"](#).

- 스토리지 배열이 오프라인이므로 호스트 또는 애플리케이션이 이를 액세스하지 않습니다.
- 모든 데이터가 백업됩니다.
- 기능 팩 파일을 받았습니다.

기능 팩 파일이 관리 클라이언트(System Manager 액세스를 위한 브라우저가 있는 시스템)에 로드됩니다.



다운타임 유지 관리 창을 예약하고 호스트와 컨트롤러 사이의 모든 I/O 작업을 중지해야 합니다. 또한 변환을 성공적으로 완료할 때까지 스토리지 배열의 데이터에 액세스할 수 없습니다.

이 작업에 대해

이 작업에서는 System Manager를 사용하여 기능 팩을 설정하는 방법에 대해 설명합니다. 작업을 마치면 스토리지 배열을 다시 시작해야 합니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. 추가 기능 * 아래에서 * 기능 팩 변경 * 을 선택합니다.
3. 찾아보기 * 를 클릭한 다음 키 파일을 선택합니다.

대화 상자에 파일 이름이 표시됩니다.

4. 필드에 * change * 를 입력합니다.
5. 변경 * 을 클릭합니다.

기능 팩 마이그레이션이 시작되고 컨트롤러가 재부팅됩니다. 기록되지 않은 캐시 데이터가 삭제되어 입출력 작업이 발생하지 않습니다. 두 컨트롤러가 자동으로 재부팅되므로 새로운 기능 팩이 적용됩니다. 재부팅이 완료되면 스토리지 배열이 응답 상태로 돌아갑니다.

CLI(Command Line Interface) 다운로드

System Manager에서 CLI(Command Line Interface) 패키지를 다운로드할 수 있습니다. CLI는 스토리지 시스템을 구성하고 모니터링하기 위한 텍스트 기반 방법을 제공합니다. https를 통해 통신하며 외부에서 설치된 관리 소프트웨어 패키지에서 사용할 수 있는 CLI와 동일한 구문을 사용합니다. CLI를 다운로드하는 데 키가 필요하지 않습니다.

시작하기 전에

- CLI 명령을 실행하려는 관리 시스템에서 Java Runtime Environment(JRE) 버전 8 이상을 사용할 수 있어야 합니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. 추가 기능 * 에서 * 명령줄 인터페이스 * 를 선택합니다.

ZIP 패키지가 브라우저로 다운로드됩니다.

3. ZIP 파일을 스토리지 배열에 대한 CLI 명령을 실행할 관리 시스템에 저장한 다음 파일의 압축을 풉니다.

이제 DOS C: 프롬프트와 같은 운영 체제 프롬프트에서 CLI 명령을 실행할 수 있습니다. CLI 명령 참조는 System Manager 사용자 인터페이스 오른쪽 위의 도움말 메뉴에서 사용할 수 있습니다.

시스템: 보안 키 관리

개념

드라이브 보안 기능의 작동 방식

드라이브 보안은 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브를 통해 추가 보안 계층을 제공하는 스토리지 어레이 기능입니다. 이러한 드라이브를 드라이브 보안 기능과 함께 사용하는 경우 데이터에 액세스하려면 보안 키가 필요합니다. 드라이브가 어레이에서 물리적으로 제거되면 다른 어레이에 설치될 때까지 작동할 수 없으며, 이때 올바른 보안 키가 제공될 때까지 보안 잠금 상태가 됩니다.

드라이브 보안을 구현하는 방법

드라이브 보안을 구현하려면 다음 단계를 수행하십시오.

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

드라이브 보안 작동 방식

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

드라이브 보안 기능은 보안 기능이 있는 드라이브를 통해 추가 보호 계층을 제공합니다. 드라이브 보안을 위해 이러한 드라이브의 볼륨 그룹 또는 풀을 선택한 경우 드라이브는 데이터에 대한 액세스를 허용하기 전에 보안 키를 찾습니다. 드라이브의 기존 데이터에 영향을 주지 않고 언제든지 풀 및 볼륨 그룹에 대해 드라이브 보안을 설정할 수 있습니다. 그러나 드라이브의 모든 데이터를 지우지 않으면 드라이브 보안을 비활성화할 수 없습니다.

스토리지 어레이 레벨에서 드라이브 보안이 작동하는 방식

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

보안 사용 드라이브가 스토리지 어레이에서 제거되어 다른 스토리지 배열에 다시 설치된 경우 드라이브는 보안 잠금 상태가 됩니다. 재배치된 드라이브는 데이터에 다시 액세스하기 전에 보안 키를 찾습니다. 데이터 잠금을 해제하려면 소스 스토리지 어레이에서 보안 키를 적용합니다. 잠금 해제 프로세스가 완료되면 다시 찾은 드라이브가 대상 스토리지 배열에 이미 저장된 보안 키를 사용하며 가져온 보안 키 파일이 더 이상 필요하지 않습니다.



내부 키 관리의 경우 실제 보안 키는 컨트롤러에 액세스할 수 없는 위치에 저장됩니다. 이 형식은 사람이 읽을 수 있는 형식도 아니며 사용자가 액세스할 수도 없습니다.

드라이브 보안이 볼륨 수준에서 작동하는 방식

보안 가능 드라이브에서 풀 또는 볼륨 그룹을 생성할 때 해당 풀 또는 볼륨 그룹에 대해 드라이브 보안을 설정할 수도 있습니다. Drive Security 옵션을 사용하면 드라이브 및 관련 볼륨 그룹과 풀의 보안이 `__enabled__`로 설정됩니다.

보안이 설정된 볼륨 그룹 및 풀을 생성하기 전에 다음 지침을 염두에 두십시오.

- 볼륨 그룹 및 풀은 전적으로 보안이 가능한 드라이브로 구성되어야 합니다. (FIPS 지원이 필요한 볼륨의 경우 FIPS 드라이브만 사용합니다. 볼륨 그룹 또는 풀에서 FIPS 및 FDE 드라이브를 혼합하면 모든 드라이브가 FDE 드라이브로 처리됩니다. 또한 FDE 드라이브는 All-FIPS 볼륨 그룹 또는 풀에서 스페어로 추가하거나 사용할 수 없습니다.)
- 볼륨 그룹 및 풀이 최적의 상태여야 합니다.

보안 키 관리의 작동 방식

드라이브 보안 기능을 구현하는 경우 FIPS 또는 FDE(Secure-Enabled Drive)에 데이터 액세스를 위한 보안 키가 필요합니다. 보안 키는 이러한 유형의 드라이브와 스토리지 배열의 컨트롤러 사이에서 공유되는 문자의 문자열입니다.

드라이브 전원을 켜다가 켜 때마다 보안 활성화 드라이브는 컨트롤러가 보안 키를 적용할 때까지 보안 잠금 상태로 변경됩니다. 스토리지 어레이에서 보안 지원 드라이브를 제거하면 드라이브의 데이터가 잠깁니다. 드라이브가 다른 스토리지 배열에 다시 설치되면 데이터를 다시 액세스할 수 있도록 하기 전에 보안 키를 찾습니다. 데이터의 잠금을 해제하려면 원래 보안 키를 적용해야 합니다.

다음 방법 중 하나를 사용하여 보안 키를 만들고 관리할 수 있습니다.

- 컨트롤러의 영구 메모리에서 내부 키 관리.
- 외부 키 관리 서버의 외부 키 관리.

내부 키 관리

내부 키는 컨트롤러의 영구 메모리에 유지됩니다. 내부 키 관리를 구현하려면 다음 단계를 수행하십시오.

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. 식별자 및 암호 구문을 정의하는 내부 보안 키를 만듭니다. 식별자는 보안 키와 연결된 문자열이며, 컨트롤러와 키에 연결된 모든 드라이브에 저장됩니다. 암호 구문은 백업을 위해 보안 키를 암호화하는 데 사용됩니다. 내부 키를 만들려면 * 메뉴: 설정 [시스템 > 보안 키 관리 > 내부 키 만들기] * 로 이동합니다.

보안 키는 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 키 관리를 구현하려면 다음 단계를 수행하십시오.


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. 스토리지 어레이와 키 관리 서버 간 인증을 위해 CSR(Client Certificate Signing Request)을 완료하고 다운로드합니다. 메뉴: 설정 [인증서 > 키 관리 > CSR 완료] * 로 이동합니다.
4. 다운로드한 CSR 파일을 사용하여 키 관리 서버에서 클라이언트 인증서를 생성하고 다운로드합니다.
5. 클라이언트 인증서와 키 관리 서버에 대한 인증서 사본을 로컬 호스트에서 사용할 수 있는지 확인합니다.
6. 키 관리 서버의 IP 주소와 KMIP 통신에 사용되는 포트 번호를 정의하는 데 사용되는 외부 키를 생성합니다. 이 프로세스 중에 인증서 파일도 로드합니다. 외부 키를 만들려면 * 메뉴: 설정 [시스템 > 보안 키 관리 > 외부 키 만들기] * 로 이동합니다.

입력한 자격 증명을 사용하여 시스템이 키 관리 서버에 연결됩니다. 그런 다음 보안이 설정된 볼륨 그룹 또는 풀을 생성하거나 기존 볼륨 그룹 및 풀에 대한 보안을 설정할 수 있습니다.

드라이브 보안 용어

드라이브 보안 조건이 스토리지 어레이에 적용되는 방식에 대해 알아보십시오.

기간	설명
드라이브 보안 기능	드라이브 보안은 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브를 통해 추가 보안 계층을 제공하는 스토리지 어레이 기능입니다. 이러한 드라이브를 드라이브 보안 기능과 함께 사용하는 경우 데이터에 액세스하려면 보안 키가 필요합니다. 드라이브가 어레이에서 물리적으로 제거되면 다른 어레이에 설치될 때까지 작동할 수 없으며, 이때 올바른 보안 키가 제공될 때까지 보안 잠금 상태가 됩니다.
FDE 드라이브	FDE(전체 디스크 암호화) 드라이브는 하드웨어 레벨의 디스크 드라이브에서 암호화를 수행합니다. 하드 드라이브에는 쓰기 중에 데이터를 암호화한 다음 읽기 중에 데이터를 해독하는 ASIC 칩이 포함되어 있습니다.
FIPS 드라이브	FIPS 드라이브는 FIPS(Federal Information Processing Standards) 140-2 레벨 2를 사용합니다. 이러한 드라이브는 강력한 암호화 알고리즘 및 방법을 보장하는 미국 정부 표준을 준수하는 FDE 드라이브입니다. FIPS 드라이브는 FDE 드라이브보다 보안 표준이 더 높습니다.
관리 클라이언트	System Manager 액세스를 위한 브라우저가 포함된 로컬 시스템(컴퓨터, 태블릿 등)

기간	설명
암호 구문	<p>암호 구문은 백업을 위해 보안 키를 암호화하는 데 사용됩니다. 드라이브 마이그레이션 또는 헤드 스위프의 결과로 백업된 보안 키를 가져올 때 보안 키를 암호화하는 데 사용된 것과 동일한 암호를 제공해야 합니다. 암호문은 8자에서 32자 사이여야 합니다.</p> <p> Drive Security의 암호는 스토리지 배열의 관리자 암호와 무관합니다.</p>
보안 지원 드라이브	<p>보안이 가능한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있으며, 이 드라이브는 쓰기 중에 데이터를 암호화하고 읽기 중에 데이터를 해독합니다. 이러한 드라이브는 드라이브 보안 기능을 사용하여 추가 보안을 위해 사용할 수 있으므로 보안 - 가능_으로 간주됩니다. 드라이브 보안 기능이 이러한 드라이브에 사용된 볼륨 그룹 및 풀에 대해 활성화된 경우 드라이브는 secure-_enabled_가 됩니다.</p>
보안 지원 드라이브	<p>보안 지원 드라이브는 드라이브 보안 기능과 함께 사용됩니다. 드라이브 보안 기능을 활성화한 다음 보안 -가능 드라이브의 풀 또는 볼륨 그룹에 드라이브 보안을 적용하면 드라이브는 보안- 사용 상태가 됩니다. 읽기 및 쓰기 액세스는 올바른 보안 키로 구성된 컨트롤러를 통해서만 사용할 수 있습니다. 이렇게 추가된 보안으로 인해 스토리지 어레이에서 물리적으로 제거된 드라이브의 데이터에 대한 무단 액세스가 방지됩니다.</p>
보안 키	<p>보안 키는 스토리지 어레이에서 보안 지원 드라이브와 컨트롤러 간에 공유되는 문자의 문자열입니다. 드라이브 전원을 켜다가 켜 때마다 보안 활성 드라이브는 컨트롤러가 보안 키를 적용할 때까지 보안 잠금 상태로 변경됩니다. 스토리지 어레이에서 보안 지원 드라이브를 제거하면 드라이브의 데이터가 잠깁니다. 드라이브가 다른 스토리지 배열에 다시 설치되면 데이터를 다시 액세스할 수 있도록 하기 전에 보안 키를 찾습니다. 데이터의 잠금을 해제하려면 원래 보안 키를 적용해야 합니다. 다음 방법 중 하나를 사용하여 보안 키를 만들고 관리할 수 있습니다.</p> <ul style="list-style-type: none"> • 내부 키 관리 — 컨트롤러의 영구 메모리에 보안 키를 만들고 관리합니다. • 외부 키 관리 — 외부 키 관리 서버에 보안 키를 만들고 유지 관리합니다.
보안 키 식별자입니다	<p>보안 키 식별자는 키를 생성하는 동안 보안 키와 연결된 문자열입니다. 식별자는 컨트롤러와 보안 키와 연결된 모든 드라이브에 저장됩니다.</p>

방법

내부 보안 키를 생성합니다

드라이브 보안 기능을 사용하려면 스토리지 어레이에서 컨트롤러와 보안 가능 드라이브에서 공유하는 내부 보안 키를 생성해야 합니다. 내부 키는 컨트롤러의 영구 메모리에 유지됩니다.

시작하기 전에

- 스토리지 배열에 보안 가능 드라이브가 설치되어 있어야 합니다. 이러한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있습니다.
- 드라이브 보안 기능을 활성화해야 합니다. 그렇지 않으면 이 작업 중에 보안 키를 만들 수 없음 대화 상자가 열립니다. 필요한 경우 스토리지 공급업체에 드라이브 보안 기능 활성화에 대한 지침을 문의하십시오.



FDE 및 FIPS 드라이브가 모두 스토리지 어레이에 설치된 경우 모두 동일한 보안 키를 공유합니다.

이 작업에 대해

이 작업에서는 내부 보안 키와 연결할 식별자와 암호를 정의합니다.



Drive Security의 암호는 스토리지 배열의 관리자 암호와 무관합니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.

2. 보안 키 관리 * 에서 * 내부 키 생성 * 을 선택합니다.

아직 보안 키를 생성하지 않은 경우 * 보안 키 생성 * 대화 상자가 열립니다.

3. 다음 필드에 정보를 입력합니다.

- * 보안 키 식별자 정의 * — 기본값(컨트롤러 펌웨어에 의해 생성되는 스토리지 배열 이름 및 타임 스탬프)을 그대로 사용하거나 값을 직접 입력할 수 있습니다. 공백, 구두점 또는 기호 없이 최대 189자의 영숫자 문자를 입력할 수 있습니다.



입력한 문자열의 양쪽 끝에 추가된 추가 문자가 자동으로 생성됩니다. 생성된 문자는 식별자가 고유한지 확인합니다.

- * 암호문 정의/암호문 다시 입력 * — 암호문을 입력하고 확인합니다. 값은 8자에서 32자 사이여야 하며 다음 각 문자를 포함해야 합니다.
 - 대문자(하나 이상) 암호는 대/소문자를 구분합니다.
 - 숫자(하나 이상)
 - !, *, @ (하나 이상)와 같은 영숫자 이외의 문자입니다.



나중에 사용할 수 있도록 항목을 기록해 두십시오. 스토리지 어레이에서 보안 지원 드라이브를 이동해야 하는 경우, 드라이브 데이터의 잠금을 해제하려면 식별자와 암호를 알아야 합니다.

4. Create * 를 클릭합니다.

보안 키는 컨트롤러에 액세스할 수 없는 위치에 저장됩니다. 실제 키와 함께 암호화된 키 파일이 브라우저에서 다운로드됩니다.



다운로드한 파일의 경로는 브라우저의 기본 다운로드 위치에 따라 다를 수 있습니다.

5. 키 식별자, 암호 및 다운로드한 키 파일의 위치를 기록한 다음 * 닫기 * 를 클릭합니다.

결과

이제 보안 설정된 볼륨 그룹 또는 풀을 생성하거나 기존 볼륨 그룹 및 풀에 대한 보안을 설정할 수 있습니다.



드라이브 전원을 켜다가 다시 켤 때마다 모든 보안 지원 드라이브는 보안 잠금 상태로 변경됩니다. 이 상태에서는 드라이브 초기화 중에 컨트롤러가 올바른 보안 키를 적용할 때까지 데이터에 액세스할 수 없습니다. 잠긴 드라이브를 물리적으로 제거하고 다른 시스템에 설치하는 경우 보안 잠금 상태는 데이터에 대한 무단 액세스를 방지합니다.

작업을 마친 후

키 파일이 손상되지 않도록 보안 키의 유효성을 검사해야 합니다.

외부 보안 키를 만듭니다

키 관리 서버에서 드라이브 보안 기능을 사용하려면 스토리지 어레이에서 키 관리 서버와 보안 가능 드라이브가 공유하는 외부 키를 만들어야 합니다.

시작하기 전에

- 스토리지에 보안 가능 드라이브가 설치되어 있어야 합니다. 이러한 드라이브는 FDE(전체 디스크 암호화) 드라이브 또는 FIPS(Federal Information Processing Standard) 드라이브일 수 있습니다.



FDE 및 FIPS 드라이브가 모두 스토리지 어레이에 설치된 경우 모두 동일한 보안 키를 공유합니다.

- 드라이브 보안 기능을 활성화해야 합니다. 그렇지 않으면 이 작업 중에 * 보안 키 생성 불가 * 대화 상자가 열립니다. 필요한 경우 스토리지 공급업체에 드라이브 보안 기능 활성화에 대한 지침을 문의하십시오.
- 로컬 호스트에서 클라이언트 및 서버 인증서를 사용할 수 있으므로 스토리지 시스템 및 키 관리 서버가 서로를 인증할 수 있습니다. 클라이언트 인증서는 컨트롤러의 유효성을 검사하는 반면 서버 인증서는 키 관리 서버의 유효성을 검사합니다.

이 작업에 대해

이 작업에서는 키 관리 서버의 IP 주소와 사용하는 포트 번호를 정의한 다음 외부 키 관리를 위해 인증서를 로드합니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. 보안 키 관리 * 에서 * 외부 키 생성 * 을 선택합니다.



현재 내부 키 관리가 구성되어 있으면 대화 상자가 열리고 외부 키 관리로 전환할지 확인하는 메시지가 표시됩니다.

외부 보안 키 만들기 * 대화 상자가 열립니다.

3. 키 서버에 연결 * 에서 다음 필드에 정보를 입력합니다.
 - * 키 관리 서버 주소 * — 키 관리에 사용되는 서버의 정규화된 도메인 이름 또는 IP 주소(IPv4 또는 IPv6)를 입력합니다.
 - * 키 관리 포트 번호 * — KMIP(Key Management Interoperability Protocol) 통신에 사용되는 포트 번호를 입력합니다. 키 관리 서버 통신에 사용되는 가장 일반적인 포트 번호는 5696입니다.
 - * 클라이언트 인증서 선택 * — 첫 번째 * 찾아보기 * 버튼을 클릭하여 스토리지 배열 컨트롤러의 인증서 파일을 선택합니다.
 - * 키 관리 서버의 서버 인증서 선택 * — 두 번째 * 찾아보기 * 버튼을 클릭하여 키 관리 서버의 인증서 파일을 선택합니다.
4. 다음 * 을 클릭합니다.
5. 생성/백업 키 * 에서 다음 필드에 정보를 입력합니다.
 - * 암호문 정의/암호문 다시 입력 * — 암호문을 입력하고 확인합니다. 값은 8자에서 32자 사이여야 하며 다음 각 문자를 포함해야 합니다.

- 대문자(하나 이상) 암호는 대/소문자를 구분합니다.
- 숫자(하나 이상)
- !, *, @ (하나 이상)와 같은 영숫자 이외의 문자입니다.



나중에 사용할 수 있도록 항목을 기록해 두십시오. 스토리지 어레이에서 보안 지원 드라이브를 이동해야 하는 경우, 드라이브 데이터를 잠금 해제하려면 암호를 알아야 합니다.

6. 마침 * 을 클릭합니다.

입력한 자격 증명을 사용하여 시스템이 키 관리 서버에 연결됩니다. 그런 다음 보안 키의 복사본이 로컬 시스템에 저장됩니다.



다운로드한 파일의 경로는 브라우저의 기본 다운로드 위치에 따라 다를 수 있습니다.

7. 다운로드한 키 파일의 위치와 암호를 기록한 다음 * 닫기 * 를 클릭합니다.

외부 키 관리를 위한 추가 링크가 포함된 다음 메시지가 페이지에 표시됩니다.

현재 키 관리 방식: 외부

8. 테스트 통신 * 을 선택하여 스토리지 어레이와 키 관리 서버 간의 연결을 테스트합니다.

대화 상자에 검사 결과가 표시됩니다.

결과

외부 키 관리를 사용하도록 설정하면 보안 설정된 볼륨 그룹 또는 풀을 생성하거나 기존 볼륨 그룹 및 풀에 대한 보안을 설정할 수 있습니다.



드라이브 전원을 켜다가 다시 켤 때마다 모든 보안 지원 드라이브는 보안 잠금 상태로 변경됩니다. 이 상태에서는 드라이브 초기화 중에 컨트롤러가 올바른 보안 키를 적용할 때까지 데이터에 액세스할 수 없습니다. 잠긴 드라이브를 물리적으로 제거하고 다른 시스템에 설치하는 경우 보안 잠금 상태는 데이터에 대한 무단 액세스를 방지합니다.

작업을 마친 후

- 키 파일이 손상되지 않도록 보안 키의 유효성을 검사해야 합니다.

보안 키를 변경합니다

언제든지 보안 키를 새 키로 바꿀 수 있습니다. 회사에서 보안 위반이 발생할 수 있으며 권한이 없는 사람이 드라이브의 데이터에 액세스하지 못하도록 하려면 보안 키를 변경해야 할 수 있습니다.

시작하기 전에

보안 키가 이미 있습니다.

이 작업에 대해

이 작업에서는 보안 키를 변경하고 새 키로 바꾸는 방법에 대해 설명합니다. 이 프로세스가 완료되면 이전 키가 무효화됩니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. 보안 키 관리 * 에서 * 키 변경 * 을 선택합니다.

보안 키 변경 대화 상자가 열립니다.

3. 다음 필드에 정보를 입력합니다.

- * 보안 키 식별자 정의 — * (내부 보안 키에만 해당) 기본값(컨트롤러 펌웨어에서 생성되는 스토리지 배열 이름 및 타임스탬프)을 그대로 사용하거나 값을 직접 입력합니다. 공백, 구두점 또는 기호 없이 최대 189자의 영숫자 문자를 입력할 수 있습니다.



추가 문자는 자동으로 생성되며 입력하는 문자열의 양쪽 끝에 추가됩니다. 생성된 문자는 식별자가 고유한지 확인하는 데 도움이 됩니다.

- * 암호문 정의/암호문 다시 입력 * — 이러한 각 필드에 암호문을 입력합니다. 값은 8자에서 32자 사이여야 하며 다음 각 문자를 포함해야 합니다.
 - 대문자(하나 이상) 암호는 대/소문자를 구분합니다.
 - 숫자(하나 이상)
 - !, *, @ (하나 이상)와 같은 영숫자 이외의 문자입니다.



나중에 사용할 수 있도록 항목을 기록해야 합니다. — 보안 설정 드라이브를 스토리지 배열에서 이동해야 하는 경우, 드라이브 데이터를 잠금 해제하려면 식별자와 암호를 알아야 합니다.

4. 변경 * 을 클릭합니다.

새 보안 키는 더 이상 유효하지 않은 이전 키를 덮어씁니다.



다운로드한 파일의 경로는 브라우저의 기본 다운로드 위치에 따라 다를 수 있습니다.

5. 키 식별자, 암호 및 다운로드한 키 파일의 위치를 기록한 다음 * 닫기 * 를 클릭합니다.

작업을 마친 후

키 파일이 손상되지 않도록 보안 키의 유효성을 검사해야 합니다.

외부에서 내부 키 관리로 전환합니다

외부 키 서버에서 스토리지 배열에 사용되는 내부 방법으로 Drive Security의 관리 방법을 변경할 수 있습니다. 그런 다음 외부 키 관리를 위해 이전에 정의된 보안 키를 내부 키 관리에 사용합니다.

시작하기 전에

외부 키가 생성되었습니다.

이 작업에 대해

이 작업에서는 외부 키 관리를 사용하지 않도록 설정하고 새 백업 복사본을 로컬 호스트에 다운로드합니다. 기존 키는 드라이브 보안에 계속 사용되지만 스토리지 시스템에서 내부적으로 관리됩니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. 보안 키 관리 * 에서 * 외부 키 관리 비활성화 * 를 선택합니다.

외부 키 관리 비활성화 * 대화 상자가 열립니다.

3. 암호 정의/암호 다시 입력 * 에서 키 백업에 대한 암호 구문을 입력하고 확인합니다. 값은 8자에서 32자 사이여야 하며 다음 각 문자를 포함해야 합니다.

- 대문자(하나 이상) 암호는 대/소문자를 구분합니다.
- 숫자(하나 이상)
- !, *, @ (하나 이상)와 같은 영숫자 이외의 문자입니다.



나중에 사용할 수 있도록 항목을 기록해 두십시오. _ 스토리지 어레이에서 보안 지원 드라이브를 이동해야 하는 경우, 드라이브 데이터의 잠금을 해제하려면 식별자와 암호를 알아야 합니다.

4. 비활성화 * 를 클릭합니다.

백업 키가 로컬 호스트에 다운로드됩니다.

5. 키 식별자, 암호 및 다운로드한 키 파일의 위치를 기록한 다음 * 닫기 * 를 클릭합니다.

결과

이제 드라이브 보안이 스토리지 어레이를 통해 내부적으로 관리됩니다.

작업을 마친 후

- 키 파일이 손상되지 않도록 보안 키의 유효성을 검사해야 합니다.

키 관리 서버 설정을 편집합니다

외부 키 관리를 구성한 경우 언제든지 키 관리 서버 설정을 보고 편집할 수 있습니다.

시작하기 전에

외부 키 관리를 구성해야 합니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. 보안 키 관리 * 에서 * 키 관리 서버 설정 보기/편집 * 을 선택합니다.
3. 다음 필드에서 정보를 편집합니다.

- * 키 관리 서버 주소 * — 키 관리에 사용되는 서버의 정규화된 도메인 이름 또는 IP 주소(IPv4 또는 IPv6)를 입력합니다.
- * KMIP 포트 번호 * — KMIP(Key Management Interoperability Protocol) 통신에 사용되는 포트 번호를 입력합니다.

4. 저장 * 을 클릭합니다.

보안 키를 백업합니다

보안 키를 만들거나 변경한 후에는 원본이 손상되는 경우에 대비하여 키 파일의 백업 복사본을 만들 수 있습니다.

시작하기 전에

- 보안 키가 이미 있습니다.

이 작업에 대해

이 작업에서는 이전에 만든 보안 키를 백업하는 방법에 대해 설명합니다. 이 절차를 수행하는 동안 백업에 대한 새 암호를 만듭니다. 이 암호문은 원래 키를 만들거나 마지막으로 변경할 때 사용한 암호문과 일치하지 않아도 됩니다. 암호는 생성 중인 백업에만 적용됩니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. 보안 키 관리 * 에서 * 백업 키 * 를 선택합니다.

보안 키 백업 대화 상자가 열립니다.

3. 암호 구문 정의/암호 구문 다시 입력 * 필드에 이 백업의 암호 구문을 입력하고 확인합니다.

값은 8자에서 32자 사이여야 하며 다음 각 문자를 포함해야 합니다.

- 대문자(하나 이상)
- 숫자(하나 이상)
- 영숫자 이외의 문자(예:!, *, @(하나 이상)



나중에 사용할 수 있도록 입력 내용을 기록해 두십시오. 이 보안 키의 백업에 액세스하려면 암호문이 필요합니다.

4. 백업 * 을 클릭합니다.

보안 키의 백업이 로컬 호스트에 다운로드되고 * 보안 키 백업 확인/기록 * 대화 상자가 열립니다.



다운로드한 보안 키 파일의 경로는 브라우저의 기본 다운로드 위치에 따라 다를 수 있습니다.

5. 암호를 안전한 위치에 기록한 다음 * 닫기 * 를 클릭합니다.

작업을 마친 후

백업 보안 키의 유효성을 확인해야 합니다.

보안 키를 확인합니다

보안 키가 손상되지 않았는지 확인하고 올바른 암호문이 있는지 확인할 수 있습니다.

시작하기 전에

보안 키가 생성되었습니다.

이 작업에 대해

이 작업에서는 이전에 만든 보안 키의 유효성을 검사하는 방법을 설명합니다. 이 단계는 키 파일이 손상되지 않고 암호 구문이 올바른지 확인하는 중요한 단계입니다. 이렇게 하면 보안 지원 드라이브를 한 스토리지 어레이에서 다른 스토리지 어레이로 이동하는 경우 나중에 드라이브 데이터에 액세스할 수 있습니다.

단계

1. 메뉴: 설정 [시스템] * 을 선택합니다.
2. 보안 키 관리 * 에서 * 키 확인 * 을 선택합니다.

보안 키 유효성 검사 * 대화 상자가 열립니다.

3. 찾아보기 * 를 클릭하고 키 파일(예: drivesecurity.slk)을 선택합니다.
4. 선택한 키와 관련된 암호를 입력합니다.

유효한 키 파일과 암호를 선택하면 * Validate * 버튼을 사용할 수 있게 됩니다.

5. Validate * 를 클릭합니다.

유효성 검사 결과가 대화 상자에 표시됩니다.

6. 결과에 "보안 키 유효성 확인 성공"이 표시되면 * 닫기 * 를 클릭합니다. 오류 메시지가 나타나면 대화 상자에 표시되는 권장 지침을 따릅니다.

보안 키를 사용하여 드라이브 잠금을 해제합니다

보안 설정 드라이브를 한 스토리지 어레이에서 다른 스토리지 어레이로 이동하는 경우 적절한 보안 키를 새 스토리지 어레이로 가져와야 합니다. 키를 가져오면 드라이브의 데이터가 잠금 해제됩니다.

시작하기 전에

- 드라이브를 이동하는 대상 스토리지 어레이에 이미 보안 키가 구성되어 있어야 합니다. 마이그레이션된 드라이브는 대상 스토리지 배열에 다시 연결됩니다.
- 잠금을 해제할 드라이브와 연결된 보안 키를 알아야 합니다.
- 보안 키 파일은 관리 클라이언트(System Manager 액세스에 사용되는 브라우저가 있는 시스템)에서 사용할 수 있습니다. 드라이브를 다른 시스템에서 관리하는 스토리지 어레이로 이동하는 경우 보안 키 파일을 해당 관리 클라이언트로 이동해야 합니다.

이 작업에 대해

이 작업은 스토리지 어레이에서 제거한 후 다른 스토리지 배열에 다시 설치한 보안 지원 드라이브에서 데이터의 잠금을 해제하는 방법을 설명합니다. 어레이가 드라이브를 검색하면 재배치된 드라이브에 대해 "Security Key Needed" 상태와 함께 "Needs Attention" 상태가 표시됩니다. 스토리지 배열에 보안 키를 가져와 드라이브 데이터의 잠금을 해제할 수 있습니다. 이 프로세스 중에 보안 키 파일을 선택하고 키에 대한 암호를 입력합니다.



암호 구문이 스토리지 배열의 관리자 암호와 같지 않습니다.

다른 보안 지원 드라이브가 새 스토리지 배열에 설치되어 있는 경우 가져오는 것과 다른 보안 키를 사용할 수 있습니다. 가져오기 프로세스 중에 이전 보안 키는 설치 중인 드라이브의 데이터 잠금을 해제하는 데만 사용됩니다. 잠금 해제 프로세스가 성공하면 새로 설치된 드라이브가 대상 스토리지 배열의 보안 키에 다시 입력됩니다.

단계

1. 설정 [시스템] 메뉴를 선택합니다.
2. 보안 키 관리 * 에서 * 보안 드라이브 잠금 해제 * 를 선택합니다.

보안 드라이브 잠금 해제 대화 상자가 열립니다. 보안 키가 필요한 모든 드라이브가 표에 나와 있습니다.

3. * 선택 사항: * 드라이브 번호 위로 마우스를 가져가면 드라이브 위치(셀프 번호 및 베이 번호)가 표시됩니다.
4. 찾아보기 * 를 클릭한 다음 잠금을 해제할 드라이브에 해당하는 보안 키 파일을 선택합니다.

선택한 키 파일이 대화 상자에 나타납니다.

5. 이 키 파일과 관련된 암호를 입력합니다.

입력한 문자는 마스크됩니다.

6. 잠금 해제 * 를 클릭합니다.

잠금 해제 작업이 성공하면 대화 상자에 "연결된 보안 드라이브가 잠금 해제되었습니다."라는 메시지가 표시됩니다.

결과

모든 드라이브가 잠겼다가 잠금 해제되면 스토리지 배열의 각 컨트롤러가 재부팅됩니다. 그러나 대상 스토리지 배열에 이미 일부 잠금 해제된 드라이브가 있는 경우 컨트롤러는 재부팅되지 않습니다.

FAQ 를 참조하십시오

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 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 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. 스토리지 어레이와 키 관리 서버 간 인증을 위해 CSR(Client Certificate Signing Request)을 완료하고 다운로드합니다. 메뉴: 설정 [인증서 > 키 관리 > CSR 완료] * 로 이동합니다.
4. 다운로드한 CSR 파일을 사용하여 키 관리 서버에서 클라이언트 인증서를 생성하고 다운로드합니다.
5. 클라이언트 인증서와 키 관리 서버에 대한 인증서 사본을 로컬 호스트에서 사용할 수 있는지 확인합니다.

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.

보안 키 정보를 기록하는 것이 중요한 이유는 무엇입니까?

보안 키 정보가 손실되고 백업이 없는 경우, 보안 지원 드라이브를 재배치하거나 컨트롤러를 업그레이드할 때 데이터가 손실될 수 있습니다. 드라이브에서 데이터를 잠금 해제하려면 보안 키가 필요합니다.

보안 키 식별자, 연결된 암호 구문 및 보안 키 파일이 저장된 로컬 호스트의 위치를 기록해야 합니다.

보안 키를 백업하기 전에 알아야 할 내용은 무엇입니까?

원래 보안 키가 손상되고 백업이 없는 경우, 한 스토리지 어레이에서 다른 스토리지 어레이로 마이그레이션할 경우 드라이브의 데이터에 액세스할 수 없게 됩니다.

보안 키를 백업하기 전에 다음 지침을 염두에 두십시오.

- 원본 키 파일의 보안 키 식별자 및 암호를 알고 있어야 합니다.



내부 키만 식별자를 사용합니다. 식별자를 만들면 추가 문자가 자동으로 생성되고 식별자 문자열의 양쪽 끝에 추가됩니다. 생성된 문자는 식별자가 고유한지 확인합니다.

- 백업에 대한 새 암호를 만듭니다. 이 암호문은 원래 키를 만들거나 마지막으로 변경할 때 사용한 암호문과 일치하지 않아도 됩니다. 암호는 생성 중인 백업에만 적용됩니다.



드라이브 보안의 암호를 스토리지 배열의 관리자 암호와 혼동해서는 안 됩니다. Drive Security의 암호 구문은 보안 키의 백업을 보호합니다. 관리자 암호를 사용하면 전체 스토리지 시스템이 무단으로 액세스하지 못하도록 보호할 수 있습니다.

- 백업 보안 키 파일이 관리 클라이언트에 다운로드됩니다. 다운로드한 파일의 경로는 브라우저의 기본 다운로드 위치에 따라 다를 수 있습니다. 보안 키 정보가 저장된 위치를 기록해 두십시오.

보안 드라이브를 잠금 해제하기 전에 알아야 할 사항은 무엇입니까?

새 스토리지 어레이로 마이그레이션된 보안 지원 드라이브에서 데이터의 잠금을 해제하려면 해당 보안 키를 가져와야 합니다.

보안 지원 드라이브를 잠금 해제하기 전에 다음 지침을 염두에 두십시오.

- 드라이브를 이동하는 대상 스토리지 어레이에 이미 보안 키가 있어야 합니다. 마이그레이션된 드라이브는 대상 스토리지 배열에 다시 연결됩니다.
- 마이그레이션하는 드라이브의 경우 보안 키 식별자와 보안 키 파일에 해당하는 암호 구문을 알고 있습니다.
- 보안 키 파일은 관리 클라이언트(System Manager 액세스에 사용되는 브라우저가 있는 시스템)에서 사용할 수 있습니다.
- 잠긴 NVMe 드라이브를 재설정하는 경우 드라이브의 보안 ID를 입력해야 합니다. 보안 ID를 찾으려면 드라이브를 물리적으로 제거하고 드라이브 레이블에서 PSID 문자열(최대 32자)을 찾아야 합니다. 작업을 시작하기 전에 드라이브를 다시 설치해야 합니다.

읽기/쓰기 접근성이란 무엇입니까?

드라이브 설정 창에는 드라이브 보안 속성에 대한 정보가 포함되어 있습니다. "읽기/쓰기 액세스 가능"은 드라이브의 데이터가 잠겨 있는지 여부를 표시하는 속성 중 하나입니다.

드라이브 보안 속성을 보려면 하드웨어 페이지로 이동합니다. 드라이브를 선택하고 * 설정 보기 * 를 클릭한 다음 * 추가 설정 표시 * 를 클릭합니다. 드라이브의 잠금이 해제될 때 페이지 하단에서 읽기/쓰기 액세스 가능 속성 값은 * 예 * 입니다. 읽기/쓰기 액세스 가능 속성 값은 드라이브가 잠겨 있을 때 * 아니오, 유효하지 않은 보안 키 * 입니다. 보안 키를 가져와 보안 드라이브의 잠금을 해제할 수 있습니다(설정 [시스템 > 보안 드라이브 잠금 해제] 메뉴로 이동).

보안 키 유효성 검사에 대해 알아야 할 내용은 무엇입니까?

보안 키를 만든 후에는 키 파일이 손상되지 않았는지 확인해야 합니다.

유효성 검사에 실패하면 다음을 수행합니다.

- 보안 키 식별자가 컨트롤러의 식별자와 일치하지 않는 경우 올바른 보안 키 파일을 찾은 다음 확인을 다시 시도하십시오.
- 컨트롤러가 유효성 검사를 위해 보안 키를 해독할 수 없는 경우 암호 구문을 잘못 입력했을 수 있습니다. 암호를 다시 확인하고 필요한 경우 다시 입력한 다음 확인을 다시 시도하십시오. 오류 메시지가 다시 나타나면 키 파일의 백업을 선택하고(있는 경우) 유효성 검사를 다시 시도하십시오.
- 여전히 보안 키의 유효성을 검사할 수 없는 경우 원본 파일이 손상되었을 수 있습니다. 키의 새 백업을 생성하고 해당 복사본을 확인합니다.

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.

액세스 관리

개념

액세스 관리 작동 방식

액세스 관리는 SANtricity 시스템 관리자에서 사용자 인증을 설정하는 방법입니다.

Access Management 구성 및 사용자 인증은 다음과 같이 작동합니다.

1. 관리자는 보안 관리자 권한이 포함된 사용자 프로필을 사용하여 System Manager에 로그인합니다.



처음 로그인하는 경우 사용자 이름 admin이 자동으로 표시되며 변경할 수 없습니다. admin 사용자는 시스템의 모든 기능에 액세스할 수 있습니다.

2. 관리자는 사용자 인터페이스에서 Access Management(액세스 관리)로 이동합니다. 스토리지 어레이는 RBAC(역할 기반 액세스 제어) 기능을 구현하는 로컬 사용자 역할을 사용하도록 사전 구성됩니다.
3. 관리자는 다음 인증 방법 중 하나 이상을 구성합니다.
 - * 로컬 사용자 역할 * — 스토리지 어레이에 적용된 RBAC 기능을 통해 인증이 관리됩니다. 로컬 사용자 역할에는 미리 정의된 사용자 프로필과 특정 액세스 권한이 있는 역할이 포함됩니다. 관리자는 이러한 로컬 사용자 역할을 단일 인증 방법으로 사용하거나 디렉터리 서비스와 함께 사용할 수 있습니다. 사용자 암호 설정 이외의 구성은 필요하지 않습니다.
 - * 디렉터리 서비스 * — 인증은 LDAP(Lightweight Directory Access Protocol) 서버 및 Microsoft의 Active Directory와 같은 디렉터리 서비스를 통해 관리됩니다. 관리자는 LDAP 서버에 연결한 다음 LDAP 사용자를 스토리지 배열에 포함된 로컬 사용자 역할에 매핑합니다.
 - * SAML * — 인증은 SAML(Security Assertion Markup Language) 2.0을 사용하여 ID 공급자(IDP)를 통해 관리됩니다. 관리자는 IdP 시스템과 스토리지 어레이 간의 통신을 설정한 다음 IdP 사용자를 스토리지 어레이에 포함된 로컬 사용자 역할에 매핑합니다.
4. 관리자는 사용자에게 System Manager에 대한 로그인 자격 증명을 제공합니다.
5. 사용자는 자격 증명을 입력하여 시스템에 로그인합니다.



SAML 및 SSO(Single Sign-On)로 인증이 관리되는 경우 시스템은 System Manager 로그인 대화 상자를 건너뛸 수 있습니다.

로그인 중에 시스템은 다음과 같은 백그라운드 작업을 수행합니다.

- 사용자 계정에 대해 사용자 이름과 암호를 인증합니다.
- 할당된 역할에 따라 사용자의 권한을 결정합니다.
- 사용자에게 사용자 인터페이스의 작업에 대한 액세스 권한을 제공합니다.
- 인터페이스의 오른쪽 위에 사용자 이름을 표시합니다.

System Manager에서 사용 가능한 작업

작업에 대한 액세스 권한은 사용자가 할당한 역할에 따라 다르며, 여기에는 다음이 포함됩니다.

- * 스토리지 관리자 * — 스토리지 객체(예: 볼륨 및 디스크 풀)에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
- * 보안 관리자 * — 액세스 관리, 인증서 관리, 감사 로그 관리 및 레거시 관리 인터페이스(기호)를 켜거나 끌 수 있는 기능의 보안 구성에 액세스합니다.
- * 지원 관리자 * — 스토리지 어레이의 모든 하드웨어 리소스, 장애 데이터, MEL 이벤트 및 컨트롤러 펌웨어 업그레이드에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
- * Monitor * — 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.

사용할 수 없는 작업은 회색으로 표시되거나 사용자 인터페이스에 표시되지 않습니다. 예를 들어 Monitor 역할을 가진 사용자는 볼륨에 대한 모든 정보를 볼 수 있지만 해당 볼륨을 수정하기 위한 기능에는 액세스할 수 없습니다. Copy Services * 및 * Add to Workload * 와 같은 기능에 대한 탭은 회색으로 표시되고 * View/Edit Settings * 만 사용할 수 있습니다.

SANtricity Unified Manager 및 SANtricity Storage Manager의 제한 사항

스토리지에 대해 SAML이 구성된 경우 사용자는 SANtricity Unified Manager 또는 SANtricity 스토리지 관리자 인터페이스에서 해당 스토리지에 대한 스토리지를 검색 또는 관리할 수 없습니다.

로컬 사용자 역할 및 디렉터리 서비스가 구성된 경우 사용자는 다음 기능을 수행하기 전에 자격 증명을 입력해야 합니다.

- 스토리지 배열의 이름을 바꿉니다
- 컨트롤러 펌웨어 업그레이드 중
- 스토리지 배열 구성을 로드하는 중입니다
- 스크립트 실행
- 사용하지 않는 세션이 시간 초과된 경우 활성 작업을 수행하려고 합니다

Access Management(액세스 관리) 용어

액세스 관리 용어가 스토리지 어레이에 어떻게 적용되는지 알아보십시오.

기간	설명
Active Directory를 클릭합니다	AD(Active Directory)는 Windows 도메인 네트워크에 LDAP를 사용하는 Microsoft 디렉터리 서비스입니다.
바인딩	바인딩 작업은 클라이언트를 디렉터리 서버에 인증하는 데 사용됩니다. 일반적으로 바인딩에는 계정 및 암호 자격 증명만 필요하지만 일부 서버에서는 익명 바인딩 작업을 허용합니다.
CA	CA(인증 기관)는 인터넷 보안을 위해 디지털 인증서라는 전자 문서를 발급하는 신뢰할 수 있는 엔터티입니다. 이러한 인증서는 클라이언트와 서버 간의 보안 연결을 허용하는 웹사이트 소유자를 식별합니다.

기간	설명
인증서	인증서는 보안 목적으로 사이트의 소유자를 식별하므로 공격자가 사이트를 가장할 수 없습니다. 인증서에는 사이트 소유자에 대한 정보와 이 정보를 인증(서명)한 신뢰할 수 있는 엔터티의 ID가 포함되어 있습니다.
IDP	IDP(Identity Provider)는 사용자의 자격 증명을 요청하고 해당 사용자가 성공적으로 인증되었는지 확인하는 데 사용되는 외부 시스템입니다. IDP는 다중 요소 인증을 제공하고 Active Directory와 같은 사용자 데이터베이스를 사용하도록 구성할 수 있습니다. 보안 팀은 IDP를 유지 관리할 책임이 있습니다.
LDAP를 지원합니다	LDAP(Lightweight Directory Access Protocol)는 분산 디렉터리 정보 서비스에 액세스하고 유지 관리하기 위한 애플리케이션 프로토콜입니다. 이 프로토콜을 사용하면 다양한 응용 프로그램 및 서비스를 LDAP 서버에 연결하여 사용자의 유효성을 검사할 수 있습니다.
RBAC	역할 기반 액세스 제어(RBAC)는 개별 사용자의 역할에 따라 컴퓨터 또는 네트워크 리소스에 대한 액세스를 제어하는 방법입니다. RBAC 제어는 스토리지 어레이에 적용되고 사전 정의된 역할을 포함합니다.
SAML	SAML(Security Assertion Markup Language)은 두 개체 간의 인증 및 승인을 위한 XML 기반 표준입니다. SAML을 사용하면 다중 요소 인증을 수행할 수 있습니다. 사용자는 ID를 입증하기 위해 두 개 이상의 항목(예: 암호 및 지문)을 제공해야 합니다. 스토리지에 포함된 SAML 기능은 ID 어설션, 인증 및 권한 부여에 대해 SAML2.0을 준수합니다.
SP	서비스 공급자(SP)는 사용자 인증 및 액세스를 제어하는 시스템입니다. SAML로 액세스 관리를 구성하면 스토리지 어레이가 ID Provider에서 인증을 요청하는 서비스 공급자 역할을 합니다.
SSO	SSO(Single Sign-On)는 하나의 로그인 자격 증명 세트로 여러 응용 프로그램에 액세스할 수 있는 인증 서비스입니다.

매핑된 역할에 대한 권한

스토리지 어레이에 적용된 RBAC(역할 기반 액세스 제어) 기능에는 하나 이상의 역할이 매핑된 사전 정의된 사용자 프로필이 포함됩니다. 각 역할에는 SANtricity 시스템 관리자의 작업에 액세스할 수 있는 권한이 포함되어 있습니다.

사용자 프로필 및 매핑된 역할은 System Manager의 사용자 인터페이스에서 * 메뉴: 설정 [액세스 관리 > 로컬 사용자 역할] * 에서 액세스할 수 있습니다.

역할은 다음과 같이 작업에 대한 사용자 액세스를 제공합니다.

- * 스토리지 관리자 * — 스토리지 객체(예: 볼륨 및 디스크 풀)에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
- * 보안 관리자 * — 액세스 관리, 인증서 관리, 감사 로그 관리 및 레거시 관리 인터페이스(기호)를 켜거나 끌 수 있는 기능의 보안 구성에 액세스합니다.

- * 지원 관리자 * — 스토리지 어레이의 모든 하드웨어 리소스, 장애 데이터, MEL 이벤트 및 컨트롤러 펌웨어 업그레이드에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
- * Monitor * — 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.

사용자에게 특정 작업에 대한 권한이 없는 경우 해당 작업은 회색으로 표시되거나 사용자 인터페이스에 표시되지 않습니다.

로컬 사용자 역할을 사용하여 액세스 관리

액세스 관리의 경우 관리자는 스토리지 어레이에 적용된 RBAC(역할 기반 액세스 제어) 기능을 사용할 수 있습니다. 이러한 기능을 "로컬 사용자 역할"이라고 합니다.

구성 워크플로우

로컬 사용자 역할은 스토리지에 대해 사전 구성됩니다. 로컬 사용자 역할을 인증에 사용하려면 관리자가 다음을 수행할 수 있습니다.

1. 관리자는 보안 관리자 권한이 포함된 사용자 프로필을 사용하여 SANtricity 시스템 관리자에 로그인합니다.



admin 사용자는 시스템의 모든 기능에 액세스할 수 있습니다.

2. 관리자는 사용자 프로파일을 검토합니다. 사용자 프로파일은 미리 정의되어 있으며 수정할 수 없습니다.
3. * 선택 사항: * 관리자가 각 사용자 프로파일에 대해 새 암호를 할당합니다.
4. 사용자는 할당된 자격 증명을 사용하여 시스템에 로그인합니다.

관리

인증에 로컬 사용자 역할만 사용하는 경우 관리자는 다음 관리 작업을 수행할 수 있습니다.

- 암호를 변경합니다.
- 암호의 최소 길이를 설정합니다.
- 사용자가 암호 없이 로그인할 수 있도록 허용합니다.

디렉토리 서비스를 통한 액세스 관리

액세스 관리의 경우 관리자는 LDAP(Lightweight Directory Access Protocol) 서버와 Microsoft의 Active Directory와 같은 디렉토리 서비스를 사용할 수 있습니다.

구성 워크플로우

네트워크에서 LDAP 서버 및 디렉토리 서비스를 사용하는 경우 구성은 다음과 같이 작동합니다.

1. 관리자는 보안 관리자 권한이 포함된 사용자 프로필을 사용하여 SANtricity 시스템 관리자에 로그인합니다.



admin 사용자는 시스템의 모든 기능에 액세스할 수 있습니다.

2. 관리자는 LDAP 서버에 대한 구성 설정을 입력합니다. 설정에는 도메인 이름, URL 및 바인딩 계정 정보가 포함됩니다.

3. LDAP 서버가 보안 프로토콜(LDAPS)을 사용하는 경우 관리자는 LDAP 서버와 스토리지 시스템 간의 인증을 위해 CA(인증 기관) 인증서 체인을 업로드합니다.
4. 서버 연결이 설정되면 관리자는 사용자 그룹을 스토리지 시스템의 역할에 매핑합니다. 이러한 역할은 미리 정의되어 있으며 수정할 수 없습니다.
5. 관리자는 LDAP 서버와 스토리지 시스템 간의 연결을 테스트합니다.
6. 사용자는 할당된 LDAP/Directory 서비스 자격 증명을 사용하여 시스템에 로그인합니다.

관리

인증을 위해 디렉터리 서비스를 사용하는 경우 관리자는 다음 관리 작업을 수행할 수 있습니다.

- 디렉토리 서버를 추가합니다.
- 디렉토리 서버 설정을 편집합니다.
- LDAP 사용자를 로컬 사용자 역할에 매핑합니다.
- 디렉토리 서버를 제거합니다.

SAML을 통한 액세스 관리

Access Management의 경우 관리자는 스토리지에 포함된 SAML(Security Assertion Markup Language) 2.0 기능을 사용할 수 있습니다.

구성 워크플로우

SAML 구성은 다음과 같이 작동합니다.

1. 관리자는 보안 관리자 권한이 포함된 사용자 프로필을 사용하여 System Manager에 로그인합니다.



"admin" 사용자는 System Manager의 모든 기능에 액세스할 수 있습니다.

2. 관리자는 액세스 관리 아래의 * SAML * 탭으로 이동합니다.
3. 관리자는 ID 공급자(IDP)와의 통신을 구성합니다. IDP는 사용자의 자격 증명을 요청하고 사용자가 성공적으로 인증되었는지 확인하는 데 사용되는 외부 시스템입니다. 스토리지 어레이와의 통신을 구성하기 위해 관리자는 IDP 시스템에서 IDP 메타데이터 파일을 다운로드한 다음 System Manager를 사용하여 파일을 스토리지 어레이에 업로드합니다.
4. 관리자는 서비스 공급자와 IDP 간의 신뢰 관계를 설정합니다. 서비스 공급자는 사용자 인증을 제어합니다. 이 경우 스토리지 배열의 컨트롤러는 서비스 공급자 역할을 합니다. 통신을 구성하기 위해 관리자는 System Manager를 사용하여 각 컨트롤러에 대한 서비스 공급자 메타데이터 파일을 내보냅니다. 그런 다음 관리자는 IDP 시스템에서 해당 메타데이터 파일을 IDP로 가져옵니다.



또한 관리자는 IDP가 인증 시 이름 ID를 반환하는 기능을 지원해야 합니다.

5. 관리자는 스토리지 어레이의 역할을 IDP에 정의된 사용자 속성에 매핑합니다. 이렇게 하려면 관리자가 System Manager를 사용하여 매핑을 생성합니다.
6. 관리자는 IDP URL에 대한 SSO 로그인을 테스트합니다. 이 테스트는 스토리지 배열 및 IDP가 통신할 수 있도록 보장합니다.



SAML이 활성화되면 사용자 인터페이스를 통해 이를 _비활성화할 수 없으며 IDP 설정을 편집할 수도 없습니다. SAML 구성을 비활성화하거나 편집해야 하는 경우 기술 지원 부서에 지원을 요청하십시오.

7. System Manager에서 관리자는 스토리지 배열에 대해 SAML을 활성화합니다.
8. 사용자는 SSO 자격 증명을 사용하여 시스템에 로그인합니다.

관리

인증을 위해 SAML을 사용하는 경우 관리자는 다음 관리 작업을 수행할 수 있습니다.

- 새 역할 매핑을 수정하거나 작성합니다
- 서비스 공급자 파일을 내보냅니다

액세스 제한

SAML이 활성화된 경우 사용자는 SANtricity Unified Manager 또는 SANtricity 스토리지 관리자 인터페이스에서 해당 스토리지에 대한 스토리지를 검색 또는 관리할 수 없습니다.

또한 다음 클라이언트는 스토리지 서비스 및 리소스에 액세스할 수 없습니다.

- 엔터프라이즈 관리 창(EMW)
- CLI(Command-Line Interface)
- SDK(소프트웨어 개발자 키트) 클라이언트
- 대역내 클라이언트
- HTTP 기본 인증 REST API 클라이언트
- 표준 REST API 끝점을 사용하여 로그인합니다

방법

로컬 사용자 역할을 봅니다

로컬 사용자 역할 탭에서 사용자 프로필의 매핑을 기본 역할에 표시할 수 있습니다. 이러한 매핑은 스토리지 어레이에서 적용되는 RBAC(역할 기반 액세스 제어)의 일부입니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.

이 작업에 대해

사용자 프로파일과 매핑은 변경할 수 없습니다. 암호만 수정할 수 있습니다.

단계

1. MENU: 설정 [Access Management] * 를 선택합니다.
2. 로컬 사용자 역할 * 탭을 선택합니다.

사용자 프로파일이 표에 표시됩니다.

- * 루트 관리자 * (admin) — 시스템의 모든 기능에 액세스할 수 있는 슈퍼 관리자. 이 사용자 프로파일에는 모든 역할이 포함되어 있습니다.
- * 스토리지 관리자 * (스토리지) — 모든 스토리지 프로비저닝을 담당하는 관리자. 이 사용자 프로파일에는 스토리지 관리자, 지원 관리자 및 모니터 역할이 포함됩니다.
- * 보안 관리자 * (보안) — 액세스 관리, 인증서 관리 및 보안 활성화 드라이브 기능을 비롯한 보안 구성을 담당하는 사용자입니다. 이 사용자 프로파일에는 보안 관리 및 모니터 역할이 포함되어 있습니다.
- * 지원 관리자 * (지원) — 하드웨어 리소스, 오류 데이터 및 펌웨어 업그레이드를 담당하는 사용자입니다. 이 사용자 프로파일에는 지원 관리자 및 모니터 역할이 포함되어 있습니다.
- * 모니터 * (모니터) — 시스템에 대한 읽기 전용 액세스 권한이 있는 사용자입니다. 이 사용자 프로파일에는 Monitor 역할만 포함됩니다.

암호를 변경합니다

Access Management에서 각 사용자 프로파일에 대한 사용자 암호를 변경할 수 있습니다.

시작하기 전에

- 루트 관리자 권한이 포함된 로컬 관리자로 로그인해야 합니다.
- 로컬 관리자 암호를 알아야 합니다.

이 작업에 대해

암호를 선택할 때는 다음 지침을 염두에 두십시오.

- 새 로컬 사용자 암호는 최소 암호(보기/편집 설정)에 대한 현재 설정을 충족하거나 초과해야 합니다.
- 암호는 대/소문자를 구분합니다.
- 후행 공백이 설정된 경우 암호에서 제거되지는 않습니다. 암호에 공백이 포함된 경우 해당 공백을 포함해야 합니다.
- 보안을 강화하려면 15자 이상의 영숫자 문자를 사용하고 암호를 자주 변경하십시오.



System Manager에서 암호를 변경하면 CLI(Command Line Interface)에서도 암호가 변경됩니다. 또한 암호를 변경하면 사용자의 활성 세션이 종료됩니다.

단계

1. MENU: 설정 [Access Management] * 를 선택합니다.
2. 로컬 사용자 역할 * 탭을 선택합니다.
3. 테이블에서 사용자를 선택합니다.

암호 변경 단추를 사용할 수 있게 됩니다.

4. 암호 변경 * 을 선택합니다.

암호 변경 대화 상자가 열립니다.

5. 로컬 사용자 암호에 대해 최소 암호 길이를 설정하지 않은 경우 선택한 사용자가 스토리지 배열에 액세스하기 위해 암호를 입력하도록 확인란을 선택한 다음 선택한 사용자의 새 암호를 입력할 수 있습니다.

6. 로컬 관리자 암호를 입력한 다음 * 변경 * 을 클릭합니다.

결과

사용자가 현재 로그인한 경우 암호 변경으로 인해 사용자의 활성 세션이 종료됩니다.

로컬 사용자 암호 설정을 변경합니다

스토리지 배열의 새 로컬 사용자 암호 또는 업데이트된 로컬 사용자 암호의 최소 길이를 설정할 수 있습니다. 또한 로컬 사용자가 암호를 입력하지 않고 스토리지 배열에 액세스하도록 허용할 수 있습니다.

시작하기 전에

- 루트 관리자 권한이 포함된 로컬 관리자로 로그인해야 합니다.

이 작업에 대해

로컬 사용자 암호의 최소 길이를 설정할 때는 다음 지침을 염두에 두십시오.

- 설정을 변경해도 기존 로컬 사용자 암호에는 영향을 주지 않습니다.
- 로컬 사용자 암호에 필요한 최소 길이 설정은 0자에서 30자 사이여야 합니다.
- 새 로컬 사용자 암호는 현재 최소 길이 설정을 충족하거나 초과해야 합니다.
- 로컬 사용자가 암호를 입력하지 않고 스토리지 배열에 액세스하도록 하려면 암호의 최소 길이를 설정하지 마십시오.

단계

1. MENU: 설정 [Access Management] * 를 선택합니다.
2. 로컬 사용자 역할 * 탭을 선택합니다.
3. 설정 보기/편집 * 버튼을 선택합니다.

로컬 사용자 암호 설정 * 대화 상자가 열립니다.

4. 다음 중 하나를 수행합니다.

- 로컬 사용자가 암호를 입력하지 않고 스토리지 배열에 액세스할 수 있도록 하려면 "모든 로컬 사용자 암호를 최소 이상으로 요구" 확인란의 선택을 취소합니다.
- 모든 로컬 사용자 암호에 대해 최소 암호 길이를 설정하려면 "모든 로컬 사용자 암호를 최소 이상으로 요구" 확인란을 선택한 다음 spinner 상자를 사용하여 모든 로컬 사용자 암호에 필요한 최소 길이를 설정합니다.

새 로컬 사용자 암호는 현재 설정을 충족하거나 초과해야 합니다.

5. 저장 * 을 클릭합니다.

디렉토리 서버를 추가합니다

액세스 관리에 대한 인증을 구성하려면 스토리지 어레이와 LDAP 서버 간의 통신을 설정한 다음 LDAP 사용자 그룹을 스토리지의 사전 정의된 역할에 매핑할 수 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이

나타나지 않습니다.

- 사용자 그룹은 디렉토리 서비스에 정의되어 있어야 합니다.
- 도메인 이름, 서버 URL, 그리고 선택적으로 바인딩 계정 사용자 이름 및 암호를 포함하여 LDAP 서버 자격 증명을 사용할 수 있어야 합니다.
- 보안 프로토콜을 사용하는 LDAPS 서버의 경우 로컬 시스템에 LDAP 서버의 인증서 체인을 설치해야 합니다.

이 작업에 대해

디렉토리 서버를 추가하는 과정은 2단계로 이루어집니다. 먼저 도메인 이름과 URL을 입력합니다. 서버에서 보안 프로토콜을 사용하는 경우 비표준 서명 기관에서 서명한 경우 인증을 위한 CA 인증서도 업로드해야 합니다. 바인딩 계정에 대한 자격 증명이 있는 경우 사용자 계정 이름 및 암호를 입력할 수도 있습니다. 그런 다음 LDAP 서버의 사용자 그룹을 스토리지의 사전 정의된 역할에 매핑합니다.



LDAP 서버를 추가하는 절차 중에는 레거시 관리 인터페이스가 비활성화됩니다. 기존 관리 인터페이스(symbol)는 스토리지 배열과 관리 클라이언트 간의 통신 방법입니다. 이 기능을 해제하면 스토리지 어레이와 관리 클라이언트에서 더욱 안전한 통신 방법(https를 통한 REST API)을 사용합니다.

단계

1. MENU: 설정 [Access Management] * 를 선택합니다.
2. 디렉터리 서비스 * 탭에서 * 디렉터리 서버 추가 * 를 선택합니다.

디렉토리 서버 추가 대화 상자가 열립니다.

3. 서버 설정 * 탭에서 LDAP 서버의 자격 증명을 입력합니다.

설정	설명
• 구성 설정 *	도메인
LDAP 서버의 도메인 이름을 입력합니다. 여러 도메인의 경우 쉼표로 구분된 목록에 도메인을 입력합니다. 도메인 이름은 로그인(<i>username@domain</i>)에서 인증할 디렉토리 서버를 지정하는 데 사용됩니다.	서버 URL
LDAP 서버에 액세스하기 위한 URL을 "LDAP[s]://*host*: *port*" 형식으로 입력합니다.	인증서 업로드(선택 사항)
<div data-bbox="245 1058 302 1115">  </div> <div data-bbox="358 915 480 1251"> <p>이 필드는 LDAPS 프로토콜이 위의 서버 URL 필드에 지정된 경우에만 나타납니다.</p> </div> <div data-bbox="212 1304 496 1535"> <p>찾아보기 * 를 클릭하고 업로드할 CA 인증서를 선택합니다. LDAP 서버를 인증하는 데 사용되는 신뢰할 수 있는 인증서 또는 인증서 체인입니다.</p> </div>	BIND ACCOUNT(선택 사항)

설정	설명
LDAP 서버에 대한 검색 쿼리 및 그룹 내에서 검색할 읽기 전용 사용자 계정을 입력합니다. LDAP 유형 형식으로 계정 이름을 입력합니다. 예를 들어 바인딩 사용자가 "bindacct"라고 하는 경우 "CN=bindacct, CN=Users, DC=CPoC, DC=local"과 같은 값을 입력할 수 있습니다.	바인딩 암호(선택 사항)
<div>  <div> <p>이 필드는 위에 바인딩 계정을 입력할 때 나타납니다.</p> </div> </div> <p>바인딩 계정의 암호를 입력합니다.</p>	추가하기 전에 서버 연결을 테스트합니다
스토리지 배열이 입력한 LDAP 서버 구성과 통신할 수 있는지 확인하려면 이 확인란을 선택합니다. 이 테스트는 대화 상자 하단의 * 추가 * 를 클릭하면 발생합니다. 이 확인란을 선택하고 테스트에 실패하면 구성이 추가되지 않습니다. 오류를 해결하거나 확인란을 선택 취소해야 테스트를 건너뛰고 구성을 추가할 수 있습니다.	<ul style="list-style-type: none"> 권한 설정**
검색 기준 DN	사용자를 검색할 LDAP 컨텍스트를 일반적으로 'CN=Users,DC=copc,DC=local' 형식으로 입력합니다.
사용자 이름 특성입니다	인증을 위해 사용자 ID에 바인딩된 특성을 입력합니다. 예를 들어, 'sAMAccountName'을 입력합니다.
그룹 속성	그룹 대 역할 매핑에 사용되는 사용자의 그룹 속성 목록을 입력합니다. 예를 들어, memberOf , managedObjects 등이 있습니다.

4. [역할 매핑]** 탭을 클릭합니다.

5. 미리 정의된 역할에 LDAP 그룹을 할당합니다. 그룹은 여러 개의 역할을 할당할 수 있습니다.

필드 세부 정보

설정	설명
• 매핑 *	그룹 DN
매핑할 LDAP 사용자 그룹의 그룹 DN(고유 이름)을 지정합니다.	역할



Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 사용자에게 대해서는 System Manager가 올바르게 작동하지 않습니다.

1. 필요한 경우 * 다른 매핑 추가 * 를 클릭하여 그룹 대 역할 매핑을 추가로 입력합니다.

2. 매핑을 마쳤으면 * 추가 * 를 클릭합니다.

시스템은 스토리지 시스템 및 LDAP 서버가 통신할 수 있도록 검증을 수행합니다. 오류 메시지가 나타나면 대화 상자에 입력한 자격 증명을 확인하고 필요한 경우 정보를 다시 입력합니다.

디렉토리 서버 설정 및 역할 매핑을 편집합니다

이전에 Access Management에서 디렉터리 서버를 구성한 경우 언제든지 해당 설정을 변경할 수 있습니다. 설정에는 서버 연결 정보와 그룹 대 역할 매핑이 포함됩니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로파일로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
- 디렉토리 서버를 정의해야 합니다.

단계

1. MENU: 설정 [Access Management] * 를 선택합니다.
2. 디렉터리 서비스 * 탭을 선택합니다.
3. 둘 이상의 서버가 정의된 경우 테이블에서 편집할 서버를 선택합니다.
4. 설정 보기/편집 * 을 선택합니다.

디렉터리 서버 설정 * 대화 상자가 열립니다.

5. 서버 설정 * 탭에서 원하는 설정을 변경합니다.

설정	설명
• 구성 설정 *	도메인
LDAP 서버의 도메인 이름입니다. 여러 도메인의 경우 쉼표로 구분된 목록에 도메인을 입력합니다. 도메인 이름은 로그인 (<i>username@domain</i>)에서 인증할 디렉토리 서버를 지정하는 데 사용됩니다.	서버 URL
LDAP 서버 액세스 URL은 "LDAP[s]:// * host *: * port *" 형식입니다.	BIND ACCOUNT(선택 사항)
LDAP 서버에 대한 검색 쿼리 및 그룹 내 검색을 위한 읽기 전용 사용자 계정입니다.	바인딩 암호(선택 사항)
바인딩 계정의 암호입니다. (이 필드는 바인딩 계정을 입력할 때 나타납니다.)	저장하기 전에 서버 연결을 테스트합니다
스토리지 배열이 LDAP 서버 구성과 통신할 수 있는지 확인합니다. 이 테스트는 대화 상자 아래쪽에 있는 * Save * 를 클릭하면 발생합니다. 이 확인란을 선택하고 검사에 실패하면 구성이 변경되지 않습니다. 오류를 해결하거나 확인란을 선택 취소해야 테스트를 건너뛰고 구성을 다시 편집할 수 있습니다.	• 권한 설정 *
검색 기준 DN	일반적으로 사용자를 검색할 LDAP 컨텍스트는 'CN=Users,DC=copc,DC=local' 형식입니다.
사용자 이름 특성입니다	인증을 위해 사용자 ID에 바인딩된 속성입니다. 예를 들어, 'sAMAccountName'을 입력합니다.
그룹 속성	그룹-역할 매핑에 사용되는 사용자의 그룹 속성 목록입니다. 예를 들어, memberOf , managedObjects 등이 있습니다.

6. 역할 매핑 * 탭에서 원하는 매핑을 변경합니다.

설정	설명
• 매핑 *	그룹 DN
매핑할 LDAP 사용자 그룹의 도메인 이름입니다.	역할



Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 사용자에게 대해서는 System Manager가 올바르게 작동하지 않습니다.

7. 필요한 경우 * 다른 매핑 추가 * 를 클릭하여 그룹 대 역할 매핑을 추가로 입력합니다.

8. 저장 * 을 클릭합니다.

결과

이 작업을 완료하면 활성 사용자 세션이 종료됩니다. 현재 사용자 세션만 유지됩니다.

디렉토리 서버를 제거합니다

디렉토리 서버와 스토리지 시스템 간의 접속을 끊는 경우 Access Management 페이지에서 서버 정보를 제거할 수 있습니다. 새 서버를 구성한 다음 이전 서버를 제거하려는 경우 이 작업을 수행할 수 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.

이 작업에 대해

이 작업을 완료하면 활성 사용자 세션이 종료됩니다. 현재 사용자 세션만 유지됩니다.

단계

1. MENU: 설정 [Access Management] * 를 선택합니다.
2. 디렉터리 서비스 * 탭을 선택합니다.
3. 목록에서 삭제할 디렉터리 서버를 선택합니다.
4. 제거 * 를 클릭합니다.

디렉터리 서버 제거 * 대화 상자가 열립니다.

5. 필드에 remove를 입력한 다음 * Remove * 를 클릭합니다.

디렉터리 서버 구성 설정, 권한 설정 및 역할 매핑이 제거됩니다. 사용자는 더 이상 이 서버의 자격 증명으로 로그인할 수 없습니다.

SAML을 구성합니다

액세스 관리에 대한 인증을 구성하려면 스토리지 어레이에 포함된 SAML(Security Assertion Markup Language) 기능을 사용할 수 있습니다. 이 구성은 ID 공급자와 스토리지 공급자 간의 연결을 설정합니다.

이 작업에 대해

IDP(Identity Provider)는 사용자의 자격 증명을 요청하고 해당 사용자가 성공적으로 인증되었는지 확인하는 데 사용되는 외부 시스템입니다. IDP는 다중 요소 인증을 제공하고 Active Directory와 같은 사용자 데이터베이스를 사용하도록 구성할 수 있습니다. 보안 팀은 IDP를 유지 관리할 책임이 있습니다. 서비스 공급자(SP)는 사용자 인증 및 액세스를 제어하는 시스템입니다. SAML로 액세스 관리를 구성하면 스토리지 어레이가 ID Provider에서 인증을 요청하는 서비스 공급자 역할을 합니다. IDP와 스토리지 어레이 간의 연결을 설정하려면 이 두 엔터티 간에 메타데이터 파일을 공유합니다. 다음으로 IDP 사용자 엔터티를 스토리지 어레이 역할에 매핑합니다. 마지막으로 SAML을 활성화하기 전에 연결 및 SSO 로그인을 테스트합니다.



- SAML 및 디렉토리 서비스 * 디렉터리 서비스가 인증 방법으로 구성되어 있을 때 SAML을 설정하면 SAML이 System Manager의 디렉터리 서비스를 대체합니다. 나중에 SAML을 사용하지 않도록 설정하면 Directory Services 구성이 이전 구성으로 돌아갑니다.



- 편집 및 비활성화 * SAML이 활성화되면 사용자 인터페이스를 통해 이를 _비활성화할 수 없으며 IDP 설정을 편집할 수도 없습니다. SAML 구성을 비활성화하거나 편집해야 하는 경우 기술 지원 부서에 지원을 요청하십시오.

SAML 인증 구성은 다단계 절차입니다.

1단계: IDP 메타데이터 파일을 업로드합니다

IDP 연결 정보를 스토리지 어레이에 제공하기 위해 IDP 메타데이터를 System Manager로 가져옵니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
- IDP 관리자가 IDP 시스템을 구성했습니다.
- IDP 관리자는 IDP가 인증 시 이름 ID를 반환하는 기능을 지원하도록 했습니다.
- 관리자는 NTP 서버를 통해 또는 컨트롤러 클럭 설정을 조정하여 IDP 서버 및 컨트롤러 클럭이 동기화되도록 했습니다.
- IDP 메타데이터 파일은 IDP 시스템에서 다운로드되며 System Manager 액세스에 사용되는 로컬 시스템에서 사용할 수 있습니다.

이 작업에 대해

이 작업에서는 IDP의 메타데이터 파일을 System Manager로 업로드합니다. IDP 시스템은 인증 요청을 올바른 URL로 리디렉션하고 받은 응답을 검증하려면 이 메타데이터가 필요합니다. 두 개의 컨트롤러가 있더라도 스토리지 어레이에 대해 하나의 메타데이터 파일만 업로드하면 됩니다.

단계

1. MENU: 설정 [Access Management] * 를 선택합니다.
2. SAML * 탭을 선택합니다.

구성 단계의 개요가 페이지에 표시됩니다.

3. IdP(ID 공급자 가져오기) 파일 * 링크를 클릭합니다.

ID 공급자 파일 가져오기 * 대화 상자가 열립니다.

4. 로컬 시스템에 복사한 IDP 메타데이터 파일을 선택하여 업로드하려면 * 찾아보기 * 를 클릭합니다.

파일을 선택하면 IDP 엔티티 ID가 표시됩니다.

5. 가져오기 * 를 클릭합니다.

2단계: 서비스 제공업체 파일 내보내기

IDP와 스토리지 어레이 간의 신뢰 관계를 설정하려면 서비스 공급자 메타데이터를 IDP로 가져옵니다.

시작하기 전에

- 스토리지 어레이에 있는 각 컨트롤러의 IP 주소 또는 도메인 이름을 알고 있습니다.

이 작업에 대해

이 작업에서는 컨트롤러에서 메타데이터를 내보냅니다(각 컨트롤러에 대해 파일 1개). IDP는 컨트롤러와 신뢰 관계를 설정하고 승인 요청을 처리하기 위해 이 메타데이터가 필요합니다. 이 파일에는 IDP가 서비스 공급자와 통신할 수 있도록 컨트롤러 도메인 이름 또는 IP 주소와 같은 정보가 포함되어 있습니다.

단계

1. Export Service Provider files *(서비스 제공자 파일 내보내기 *) 링크를 클릭합니다.

서비스 공급자 파일 내보내기 * 대화 상자가 열립니다.

2. 컨트롤러 A * 필드에 컨트롤러 IP 주소 또는 DNS 이름을 입력한 다음 * 내보내기 * 를 클릭하여 메타데이터 파일을 로컬 시스템에 저장합니다. 스토리지 배열에 두 개의 컨트롤러가 포함된 경우, * Controller B * 필드의 두 번째 컨트롤러에 대해 이 단계를 반복합니다.

내보내기 * 를 클릭하면 서비스 공급자 메타데이터가 로컬 시스템에 다운로드됩니다. 파일이 저장된 위치를 기록해 둡니다.

3. 로컬 시스템에서 내보낸 서비스 공급자 메타데이터 파일을 찾습니다.

각 컨트롤러마다 XML 형식의 파일이 하나씩 있습니다.

4. IDP 서버에서 서비스 공급자 메타데이터 파일을 가져와 트러스트 관계를 설정합니다. 파일을 직접 가져오거나 파일에서 컨트롤러 정보를 수동으로 입력할 수 있습니다.

3단계: 역할 매핑

사용자에게 System Manager에 대한 권한 부여 및 액세스 권한을 제공하려면 IDP 사용자 특성 및 그룹 멤버십을 스토리지 어레이의 사전 정의된 역할에 매핑해야 합니다.

시작하기 전에

- IDP 관리자가 IDP 시스템에서 사용자 속성 및 그룹 구성원을 구성했습니다.
- IDP 메타데이터 파일을 System Manager로 가져옵니다.

- 각 컨트롤러의 서비스 공급자 메타데이터 파일을 IDP 시스템으로 가져와 트러스트 관계를 확인합니다.

이 작업에 대해

이 작업에서는 System Manager를 사용하여 IDP 그룹을 로컬 사용자 역할에 매핑합니다.

단계

1. System Manager 역할 매핑 링크를 클릭합니다.

역할 매핑 대화 상자가 열립니다.

2. IDP 사용자 특성 및 그룹을 미리 정의된 역할에 할당합니다. 그룹은 여러 개의 역할을 할당할 수 있습니다.

필드 세부 정보

설정	설명
• 매핑 *	사용자 속성
매핑할 SAML 그룹의 속성(예: "구성원")을 지정합니다.	속성 값
매핑할 그룹의 속성 값을 지정합니다.	역할



Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 사용자에게 대해서는 System Manager가 올바르게 작동하지 않습니다.

3. 필요한 경우 * 다른 매핑 추가 * 를 클릭하여 그룹 대 역할 매핑을 추가로 입력합니다.



역할 매핑은 SAML이 활성화된 후에 수정할 수 있습니다.

4. 매핑을 마치면 * 저장 * 을 클릭합니다.

4단계: SSO 로그인을 테스트합니다

IDP 시스템 및 스토리지 어레이가 통신할 수 있도록 SSO 로그인을 선택적으로 테스트할 수 있습니다. 이 테스트는 SAML을 활성화하기 위한 마지막 단계에서도 수행됩니다.

시작하기 전에

- IDP 메타데이터 파일을 System Manager로 가져옵니다.
- 각 컨트롤러의 서비스 공급자 메타데이터 파일을 IDP 시스템으로 가져와 트러스트 관계를 확인합니다.

단계

1. Test SSO Login * 링크를 선택합니다.

SSO 자격 증명을 입력하기 위한 대화 상자가 열립니다.

2. 보안 관리자 권한과 모니터 권한이 모두 있는 사용자의 로그인 자격 증명을 입력합니다.

시스템에서 로그인을 테스트하는 동안 대화 상자가 열립니다.

3. 테스트 성공 메시지를 찾습니다. 테스트가 성공적으로 완료되면 SAML 활성화를 위한 다음 단계로 이동합니다.

테스트가 성공적으로 완료되지 않으면 추가 정보와 함께 오류 메시지가 나타납니다. 다음을 확인합니다.

- 사용자는 보안 관리자 및 모니터 권한이 있는 그룹에 속합니다.
- IDP 서버에 대해 업로드한 메타데이터가 정확합니다.
- SP 메타데이터 파일의 컨트롤러 주소가 올바릅니다.

5단계: SAML을 활성화합니다

마지막 단계는 SAML 사용자 인증을 활성화하는 것입니다.

시작하기 전에

- IDP 메타데이터 파일을 System Manager로 가져옵니다.
- 각 컨트롤러의 서비스 공급자 메타데이터 파일을 IDP 시스템으로 가져와 트러스트 관계를 확인합니다.
- 하나 이상의 Monitor 및 Security Admin 역할 매핑이 구성되어 있습니다.

이 작업에 대해

이 작업은 사용자 인증을 위해 SAML 구성을 완료하는 방법을 설명합니다. 이 프로세스 중에 SSO 로그인을 테스트하라는 메시지가 표시됩니다. SSO 로그인 테스트 프로세스는 이전 단계에서 설명합니다.



- 편집 및 비활성화 * SAML이 활성화되면 사용자 인터페이스를 통해 이를 _비활성화할 수 없으며 IDP 설정을 편집할 수도 없습니다. SAML 구성을 비활성화하거나 편집해야 하는 경우 기술 지원 부서에 지원을 요청하십시오.

단계

1. SAML * 탭에서 * SAML * 활성화 링크를 선택합니다.

SAML * 활성화 확인 대화 상자가 열립니다.

2. "enable"을 입력한 다음 * Enable * 을 클릭합니다.

3. SSO 로그인 테스트에 대한 사용자 자격 증명을 입력합니다.

결과

시스템에서 SAML을 활성화하면 모든 활성 세션이 종료되고 SAML을 통해 사용자 인증이 시작됩니다.

SAML 역할 매핑을 변경합니다

이전에 Access Management에 SAML을 구성한 경우 IDP 그룹과 스토리지 배열의 사전 정의된 역할 간의 역할 매핑을 변경할 수 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이

나타나지 않습니다.

- IDP 관리자가 IDP 시스템에서 사용자 속성 및 그룹 구성원을 구성했습니다.
- SAML이 구성 및 활성화되었습니다.

단계

1. MENU: 설정 [Access Management] * 를 선택합니다.
2. SAML * 탭을 선택합니다.
3. 역할 매핑 * 을 선택합니다.

역할 매핑 * 대화 상자가 열립니다.

4. IDP 사용자 특성 및 그룹을 미리 정의된 역할에 할당합니다. 그룹은 여러 개의 역할을 할당할 수 있습니다.



SAML이 활성화되어 있는 동안에는 권한을 제거하지 않도록 주의하십시오. 그렇지 않으면 System Manager에 액세스할 수 없게 됩니다.

필드 세부 정보

설정	설명
• 매핑 *	사용자 속성
매핑할 SAML 그룹의 속성(예: "구성원")을 지정합니다.	속성 값
매핑할 그룹의 속성 값을 지정합니다.	역할



Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 사용자에게 대해서는 System Manager가 올바르게 작동하지 않습니다.

1. * 선택 사항: * 다른 매핑 추가 * 를 클릭하여 추가 그룹-역할 매핑을 입력합니다.
2. 저장 * 을 클릭합니다.

결과

이 작업을 완료하면 활성 사용자 세션이 종료됩니다. 현재 사용자 세션만 유지됩니다.

SAML 서비스 공급자 파일을 내보냅니다

필요한 경우 스토리지 배열에 대한 서비스 공급자 메타데이터를 내보내고 해당 파일을 IdP(Identity Provider) 시스템으로 다시 가져올 수 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
- SAML이 구성 및 활성화되었습니다.

이 작업에 대해

이 작업에서는 컨트롤러에서 메타데이터를 내보냅니다(각 컨트롤러에 대해 파일 1개). IDP는 컨트롤러와 신뢰 관계를 설정하고 인증 요청을 처리하기 위해 이 메타데이터가 필요합니다. 이 파일에는 IDP가 요청을 보내는 데 사용할 수 있는 컨트롤러 도메인 이름 또는 IP 주소와 같은 정보가 포함되어 있습니다.

단계

1. MENU: 설정 [Access Management] * 를 선택합니다.
2. SAML * 탭을 선택합니다.
3. 내보내기 * 를 선택합니다.

서비스 공급자 파일 내보내기 * 대화 상자가 열립니다.

4. 각 컨트롤러에 대해 * Export * (내보내기 *)를 클릭하여 메타데이터 파일을 로컬 시스템에 저장합니다.



각 컨트롤러의 도메인 이름 필드는 읽기 전용입니다.

파일이 저장된 위치를 기록해 둡니다.

5. 로컬 시스템에서 내보낸 서비스 공급자 메타데이터 파일을 찾습니다.

각 컨트롤러마다 XML 형식의 파일이 하나씩 있습니다.

6. IDP 서버에서 서비스 공급자 메타데이터 파일을 가져옵니다. 파일을 직접 가져오거나 해당 파일에서 컨트롤러 정보를 수동으로 입력할 수 있습니다.
7. 닫기 * 를 클릭합니다.

감사 로그 활동을 봅니다

보안 관리자 권한이 있는 사용자는 감사 로그를 보고 사용자 작업, 인증 실패, 잘못된 로그인 시도 및 사용자 세션 수명을 모니터링할 수 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.

단계

1. MENU: 설정 [Access Management] * 를 선택합니다.
2. Audit Log(감사 로그) * 탭을 선택합니다.




감사 로그 작업은 다음과 같은 정보 열이 포함된 표 형식으로 표시됩니다.

- * 날짜/시간 * — 스토리지 배열이 이벤트를 감지한 때의 타임스탬프(GMT).
- * 사용자 이름 * — 이벤트와 연결된 사용자 이름입니다. 스토리지 시스템에서 인증되지 않은 작업의 경우

"N/A"가 사용자 이름으로 나타납니다. 인증되지 않은 작업은 내부 프록시 또는 다른 메커니즘에 의해 트리거될 수 있습니다.

- * 상태 코드 * — 작업의 HTTP 상태 코드(200, 400 등) 및 이벤트와 관련된 설명 텍스트입니다.
- * URL 액세스 * — 전체 URL(호스트 포함) 및 쿼리 문자열
- * 클라이언트 IP 주소 * — 이벤트와 연결된 클라이언트의 IP 주소입니다.
- * 소스 * — 이벤트와 연결된 로깅 소스로, System Manager, CLI, 웹 서비스 또는 지원 셸이 될 수 있습니다.

3. 감사 로그 페이지의 선택 항목을 사용하여 이벤트를 보고 관리할 수 있습니다.

선택	설명
이벤트 표시...	날짜 범위별로 표시되는 이벤트 제한(지난 24시간, 지난 7일, 지난 30일 또는 사용자 지정 날짜 범위)
필터	필드에 입력한 문자로 표시되는 이벤트를 제한합니다. 따옴표(" ")를 사용하여 정확히 일치하는 단어를 선택하거나, 또는 "를 입력하여 하나 이상의 단어를 반환하거나, 대시(--))를 입력하여 단어를 생략합니다.
새로 고침	페이지를 최신 이벤트로 업데이트하려면 * Refresh * 를 선택합니다.
설정 보기/편집	설정 보기/편집 * 을 선택하여 전체 로그 정책 및 기록할 작업 수준을 지정할 수 있는 대화 상자를 엽니다.
이벤트를 삭제합니다	페이지에서 이전 이벤트를 제거할 수 있는 대화 상자를 열려면 * 삭제 * 를 선택합니다.
열 표시/숨기기	<p>표시/숨기기 * 열 아이콘을 클릭합니다  테이블에 표시할 추가 열을 선택합니다. 추가 열은 다음과 같습니다.</p> <ul style="list-style-type: none"> • * Method * — HTTP 메서드(예: POST, GET, DELETE 등). • * CLI 명령 실행됨 * — Secure CLI 요청에 대해 실행되는 CLI 명령(문법) • * CLI return Status * — CLI 상태 코드 또는 클라이언트의 입력 파일 요청입니다. • * 기호 프로시저 * — 기호 프로시저가 실행됩니다. • * SSH 이벤트 유형 * — 로그인, 로그아웃 및 login_fail과 같은 SSH(Secure Shell) 이벤트 유형 • * SSH 세션 PID * — SSH 세션의 프로세스 ID 번호입니다. • * SSH 세션 지속 시간 * — 사용자가 로그인한 시간(초)입니다.
열 필터를 전환합니다	토글 * 아이콘을 클릭합니다  각 열의 필터링 필드를 엽니다. 열 필드에 문자를 입력하여 해당 문자로 표시되는 이벤트를 제한합니다. 필터링 필드를 닫으려면 아이콘을 다시 클릭합니다.
변경 내용을 취소합니다	실행 취소 * 아이콘을 클릭합니다  를 눌러 테이블을 기본 구성으로 되돌립니다.
내보내기	내보내기 * 를 클릭하여 테이블 데이터를 CSV(쉼표로 구분된 값) 파일에 저장합니다.

감사 로그 정책을 정의합니다

덮어쓰기 정책과 감사 로그에 기록된 이벤트 유형을 변경할 수 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.

이 작업에 대해



이 작업에서는 이전 이벤트를 덮어쓰는 정책과 이벤트 유형을 기록하는 정책을 비롯한 감사 로그 설정을 변경하는 방법에 대해 설명합니다.

단계

1. MENU: 설정 [Access Management] * 를 선택합니다.
2. 감사 로그 탭을 선택합니다.
3. 설정 보기/편집 * 을 선택합니다.

감사 로그 설정 * 대화 상자가 열립니다.

4. 기록된 이벤트 유형 또는 덮어쓰기 정책을 변경합니다.

설정	설명
정책 덮어쓰기	<p>최대 용량에 도달할 때 이전 이벤트를 덮어쓰는 정책을 결정합니다.</p> <ul style="list-style-type: none"> * 감사 로그가 가득 차면 감사 로그의 가장 오래된 이벤트를 덮어쓰도록 허용 * — 감사 로그가 50,000개 레코드에 도달할 때 이전 이벤트를 덮어씁니다. * * 감사 로그 이벤트를 수동으로 삭제해야 함 * — 이벤트가 자동으로 삭제되지 않도록 지정합니다. 대신 설정된 백분율로 임계값 경고가 표시됩니다. 이벤트는 수동으로 삭제해야 합니다. <div>  <p>덮어쓰기 정책을 사용하지 않도록 설정하고 감사 로그 항목이 최대 한도에 도달하면 보안 관리자 권한이 없는 사용자는 System Manager에 액세스할 수 없습니다. 보안 관리자 권한이 없는 사용자에게 대한 시스템 액세스를 복원하려면 보안 관리자 역할에 할당된 사용자가 이전 이벤트 레코드를 삭제해야 합니다.</p> </div> <div>  <p>감사 로그 보관을 위해 syslog 서버가 구성된 경우 덮어쓰기 정책은 적용되지 않습니다.</p> </div>
기록할 작업 수준입니다	<p>기록할 이벤트 유형을 결정합니다.</p> <ul style="list-style-type: none"> * 수정 이벤트만 기록 * — 사용자 작업이 시스템에서 변경을 수행하는 이벤트만 표시합니다. * * 모든 수정 및 읽기 전용 이벤트 기록 * — 정보를 읽거나 다운로드하는 사용자 작업을 포함한 모든 이벤트를 표시합니다.

5. 저장 * 을 클릭합니다.

감사 로그에서 이벤트를 삭제합니다

이전 이벤트의 감사 로그를 지울 수 있으므로 이벤트 검색을 보다 쉽게 관리할 수 있습니다. 삭제 시 이전 이벤트를 CSV(쉼표로 구분된 값) 파일에 저장할 수 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.

이 작업에 대해

이 작업에서는 감사 로그에서 이전 이벤트를 제거하는 방법에 대해 설명합니다.

단계

1. MENU: 설정 [Access Management] * 를 선택합니다.
2. Audit Log(감사 로그) * 탭을 선택합니다.

3. 삭제 * 를 선택합니다.

감사 로그 삭제 대화 상자가 열립니다.

4. 삭제할 가장 오래된 이벤트 수를 선택하거나 입력합니다.

5. 삭제된 이벤트를 CSV 파일로 내보내려면(권장) 확인란을 선택한 상태로 유지합니다. 다음 단계에서 * 삭제 * 를 클릭하면 파일 이름과 위치를 입력하라는 메시지가 표시됩니다. 그렇지 않으면 이벤트를 CSV 파일에 저장하지 않으려면 확인란을 클릭하여 선택을 취소합니다.

6. 삭제 * 를 클릭합니다.

확인 대화 상자가 열립니다.

7. 필드에 삭제 를 입력한 다음 * 삭제 * 를 클릭합니다.

가장 오래된 이벤트는 감사 로그 페이지에서 제거됩니다.

감사 로그를 위해 **syslog** 서버를 구성합니다

감사 로그를 외부 syslog 서버에 보관하려는 경우 해당 서버와 스토리지 시스템 간의 통신을 구성할 수 있습니다. 연결이 설정되면 감사 로그가 syslog 서버에 자동으로 저장됩니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
- syslog 서버 주소, 프로토콜 및 포트 번호를 사용할 수 있어야 합니다. 서버 주소는 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소일 수 있습니다.
- 서버에서 보안 프로토콜(예: TLS)을 사용하는 경우 로컬 시스템에서 인증 기관(CA) 인증서를 사용할 수 있어야 합니다. CA 인증서는 서버와 클라이언트 간의 보안 연결을 위해 웹 사이트 소유자를 식별합니다.

단계

1. MENU: 설정 [Access Management] * 를 선택합니다.

2. 감사 로그 * 탭에서 * Syslog 서버 구성 * 을 선택합니다.

Syslog 서버 구성 * 대화 상자가 열립니다.

3. 추가 * 를 클릭합니다.

Add Syslog Server * 대화 상자가 열립니다.

4. 서버에 대한 정보를 입력한 다음 * 추가 * 를 클릭합니다.

- * 서버 주소 * — 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소를 입력합니다.
- * 프로토콜 * — 드롭다운 목록에서 프로토콜을 선택합니다(예: TLS, UDP 또는 TCP).
- * 인증서 업로드(선택 사항) * — TLS 프로토콜을 선택했지만 아직 서명된 CA 인증서를 업로드하지 않은 경우 * 찾아보기 * 를 클릭하여 인증서 파일을 업로드합니다. 감사 로그는 신뢰할 수 있는 인증서가 없는 syslog 서버에 보관되지 않습니다.



나중에 인증서가 유효하지 않게 되면 TLS 핸드셰이크가 실패합니다. 따라서 오류 메시지가 감사 로그에 게시되고 메시지가 더 이상 syslog 서버로 전송되지 않습니다. 이 문제를 해결하려면 syslog 서버에서 인증서를 수정한 다음 * 메뉴로 이동하여 설정 [감사 로그 > Syslog 서버 구성 > 모두 테스트] * 를 선택해야 합니다.

- * Port * — syslog 수신기의 포트 번호를 입력합니다.

Add * 를 클릭하면 * Configure Syslog Servers * 대화 상자가 열리고 구성된 syslog 서버가 페이지에 표시됩니다.

5. 스토리지 배열과의 서버 연결을 테스트하려면 * Test All * 을 선택합니다.

결과

구성 후 모든 새 감사 로그가 syslog 서버로 전송됩니다. 이전 로그는 전송되지 않습니다.

감사 로그 레코드에 대한 **syslog** 서버 설정을 편집합니다

감사 로그 아카이빙에 사용되는 syslog 서버의 설정을 변경하고 서버에 대한 새 CA(인증 기관) 인증서를 업로드할 수도 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 Access Management 기능이 나타나지 않습니다.
- syslog 서버 주소, 프로토콜 및 포트 번호를 사용할 수 있어야 합니다. 서버 주소는 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소일 수 있습니다.
- 새 CA 인증서를 업로드하는 경우 로컬 시스템에서 인증서를 사용할 수 있어야 합니다.

단계

1. MENU: 설정 [Access Management] * 를 선택합니다.
2. 감사 로그 * 탭에서 * Syslog 서버 구성 * 을 선택합니다.

구성된 syslog 서버가 페이지에 표시됩니다.

3. 서버 정보를 편집하려면 서버 이름 오른쪽에 있는 * Edit * (연필) 아이콘을 선택한 후 다음 필드에서 원하는 대로 변경합니다.
 - * 서버 주소 * — 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소를 입력합니다.
 - * 프로토콜 * — 드롭다운 목록에서 프로토콜을 선택합니다(예: TLS, UDP 또는 TCP).
 - * Port * — syslog 수신기의 포트 번호를 입력합니다.
4. 프로토콜을 보안 TLS 프로토콜(UDP 또는 TCP)으로 변경한 경우 * 신뢰할 수 있는 인증서 가져오기 * 를 클릭하여 CA 인증서를 업로드합니다.
5. 스토리지 배열과의 새 연결을 테스트하려면 * Test All * 을 선택합니다.

결과

구성 후 모든 새 감사 로그가 syslog 서버로 전송됩니다. 이전 로그는 전송되지 않습니다.

FAQ 를 참조하십시오

로그인할 수 없는 이유는 무엇입니까?

System Manager에 로그인할 때 오류가 발생하면 다음과 같은 가능한 원인을 검토하십시오.

다음 이유 중 하나로 System Manager에 로그인 오류가 발생할 수 있습니다.

- 잘못된 사용자 이름 또는 암호를 입력했습니다.
- 권한이 부족합니다.
- 디렉토리 서버(구성된 경우)를 사용할 수 없습니다. 이 경우 로컬 사용자 역할로 로그인을 시도하십시오.
- 여러 번 로그인을 시도했으나 실패하여 잠금 모드가 시작되었습니다. 다시 로그인하려면 10분 정도 기다립니다.
- 잠금 조건이 트리거되었고 감사 로그가 꽉 찼을 수 있습니다. Access Management(액세스 관리)로 이동하여 감사 로그에서 이전 이벤트를 삭제합니다.
- SAML 인증이 활성화되었습니다. 로그인하려면 브라우저를 새로 고치십시오.

미러링 작업을 위해 원격 스토리지 어레이에 로그인 오류가 발생하는 원인은 다음과 같습니다.

- 잘못된 암호를 입력했습니다.
- 여러 번 로그인을 시도했으나 실패하여 잠금 모드가 시작되었습니다. 10분 정도 기다린 후 다시 로그인하십시오.
- 컨트롤러에 사용된 최대 클라이언트 연결 수에 도달했습니다. 여러 사용자 또는 클라이언트를 확인합니다.

디렉토리 서버를 추가하기 전에 알아야 할 사항은 무엇입니까?

Access Management에서 디렉터리 서버를 추가하기 전에 다음 요구 사항을 충족하는지 확인합니다.

- 사용자 그룹은 디렉토리 서비스에 정의되어 있어야 합니다.
- 도메인 이름, 서버 URL, 그리고 선택적으로 바인딩 계정 사용자 이름 및 암호를 포함하여 LDAP 서버 자격 증명을 사용할 수 있어야 합니다.
- 보안 프로토콜을 사용하는 LDAPS 서버의 경우 로컬 시스템에 LDAP 서버의 인증서 체인을 설치해야 합니다.

스토리지 어레이 역할에 매핑하는 방법에 대해 알아야 할 내용은 무엇입니까?

그룹을 역할에 매핑하기 전에 다음 지침을 검토하십시오.

스토리지 시스템의 내장 RBAC(역할 기반 액세스 제어) 기능에는 다음과 같은 역할이 포함됩니다.

- * 스토리지 관리자 * — 스토리지 객체(예: 볼륨 및 디스크 풀)에 대한 전체 읽기/쓰기 액세스이지만 보안 구성에 대한 액세스는 없습니다.
- * 보안 관리자 * — 액세스 관리, 인증서 관리, 감사 로그 관리 및 레거시 관리 인터페이스(기호)를 켜거나 끌 수 있는 기능의 보안 구성에 액세스합니다.
- * 지원 관리자 * — 스토리지 어레이의 모든 하드웨어 리소스, 장애 데이터, MEL 이벤트 및 컨트롤러 펌웨어 업그레이드에 액세스합니다. 스토리지 객체 또는 보안 구성에 대한 액세스 권한이 없습니다.
- * Monitor * — 모든 스토리지 객체에 대한 읽기 전용 액세스이지만 보안 구성에 대한 액세스는 없습니다.

LDAP(Lightweight Directory Access Protocol) 서버 및 디렉터리 서비스를 사용하는 경우 다음 사항을 확인하십시오.

- 관리자가 디렉터리 서비스에 사용자 그룹을 정의했습니다.
- LDAP 사용자 그룹의 그룹 도메인 이름을 알고 있습니다.
- Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 사용자에게 대해서는 System Manager가 올바르게 작동하지 않습니다.

SAML

스토리지 어레이에 포함된 SAML(Security Assertion Markup Language) 기능을 사용하는 경우 다음 사항을 확인하십시오.

- IDP(Identity Provider) 관리자가 IDP 시스템에서 사용자 속성 및 그룹 구성원을 구성했습니다.
- 그룹 구성원 이름을 알고 있습니다.
- Monitor 역할은 관리자를 포함한 모든 사용자에게 필요합니다. Monitor 역할이 없는 사용자에게 대해서는 System Manager가 올바르게 작동하지 않습니다.

이 변경의 영향을 받을 수 있는 외부 관리 도구는 무엇입니까?

관리 인터페이스 전환 또는 SAML 인증 방법 사용과 같이 System Manager에서 특정 변경 작업을 수행할 경우 일부 외부 도구와 기능의 사용이 제한될 수 있습니다.

관리 인터페이스

레거시 관리 인터페이스 설정이 활성화되어 있지 않으면 SANtricity SMI-S Provider 또는 OnCommand Insight(OCI)와 같은 기존 관리 인터페이스(기호)와 직접 통신하는 도구가 작동하지 않습니다. 또한 이 설정이 비활성화되어 있으면 레거시 CLI 명령을 사용하거나 미러링 작업을 수행할 수 없습니다.

자세한 내용은 기술 지원 부서에 문의하십시오.

SAML 인증

SAML이 활성화되면 다음 클라이언트가 스토리지 서비스 및 리소스에 액세스할 수 없습니다.

- 엔터프라이즈 관리 창(EMW)
- CLI(Command-Line Interface)
- SDK(소프트웨어 개발자 키트) 클라이언트
- 대역내 클라이언트
- HTTP 기본 인증 REST API 클라이언트
- 표준 REST API 끝점을 사용하여 로그인합니다

자세한 내용은 기술 지원 부서에 문의하십시오.

SAML을 구성 및 활성화하기 전에 알아야 할 내용은 무엇입니까?

인증을 위해 SAML(Security Assertion Markup Language) 기능을 구성 및 활성화하기 전에 다음 요구 사항을 충족하고 SAML 제한 사항을 이해해야 합니다.

요구 사항

시작하기 전에 다음 사항을 확인하십시오.

- ID 공급자(IDP)가 네트워크에 구성되어 있습니다. IDP는 사용자의 자격 증명을 요청하고 사용자가 성공적으로 인증되었는지 확인하는 데 사용되는 외부 시스템입니다. 보안 팀은 IDP를 유지 관리할 책임이 있습니다.
- IDP 관리자가 IDP 시스템에서 사용자 속성 및 그룹을 구성했습니다.
- IDP 관리자는 IDP가 인증 시 이름 ID를 반환하는 기능을 지원하도록 했습니다.
- 관리자는 NTP 서버를 통해 또는 컨트롤러 클럭 설정을 조정하여 IDP 서버 및 컨트롤러 클럭이 동기화되도록 했습니다.
- IDP 메타데이터 파일은 IDP 시스템에서 다운로드되며 System Manager 액세스에 사용되는 로컬 시스템에서 사용할 수 있습니다.
- 스토리지 어레이에 있는 각 컨트롤러의 IP 주소 또는 도메인 이름을 알고 있습니다.

제한 사항

위의 요구 사항 외에 다음과 같은 제한 사항을 이해해야 합니다.

- SAML이 활성화되면 사용자 인터페이스를 통해 이를 비활성화할 수 없으며 IDP 설정을 편집할 수도 없습니다. SAML 구성을 비활성화하거나 편집해야 하는 경우 기술 지원 부서에 지원을 요청하십시오. 최종 구성 단계에서 SAML을 활성화하기 전에 SSO 로그인을 테스트하는 것이 좋습니다. (SAML을 활성화하기 전에 SSO 로그인 테스트도 수행합니다.)
- 나중에 SAML을 사용하지 않도록 설정하면 이전 구성(로컬 사용자 역할 및/또는 디렉터리 서비스)이 자동으로 복원됩니다.
- 디렉터리 서비스가 현재 사용자 인증을 위해 구성된 경우 SAML은 해당 구성을 재정의합니다.
- SAML이 구성된 경우 다음 클라이언트가 스토리지 시스템 리소스에 액세스할 수 없습니다.
 - 엔터프라이즈 관리 창(EMW)
 - CLI(Command-Line Interface)
 - SDK(소프트웨어 개발자 키트) 클라이언트
 - 대역내 클라이언트
 - HTTP 기본 인증 REST API 클라이언트
 - 표준 REST API 끝점을 사용하여 로그인합니다

감사 로그에 기록되는 이벤트 유형은 무엇입니까?

감사 로그는 수정 이벤트 또는 수정 이벤트와 읽기 전용 이벤트를 모두 기록할 수 있습니다.

정책 설정에 따라 다음과 같은 유형의 이벤트가 표시됩니다.

- * 수정 이벤트 * — 시스템 변경(예: 스토리지 프로비저닝)이 포함된 System Manager 내 사용자 조치.

- * 수정 및 읽기 전용 이벤트 * — 볼륨 할당 보기와 같은 정보 보기 또는 다운로드와 관련된 이벤트뿐만 아니라 시스템에 대한 변경 사항을 포함하는 사용자 작업입니다.

syslog 서버를 구성하기 전에 알아야 할 내용은 무엇입니까?

외부 **syslog** 서버에 감사 로그를 보관할 수 있습니다.

syslog 서버를 구성하기 전에 다음 지침을 염두에 두십시오.

- 서버 주소, 프로토콜 및 포트 번호를 알고 있어야 합니다. 서버 주소는 정규화된 도메인 이름, IPv4 주소 또는 IPv6 주소일 수 있습니다.
- 서버에서 보안 프로토콜(예: TLS)을 사용하는 경우 로컬 시스템에서 인증 기관(CA) 인증서를 사용할 수 있어야 합니다. CA 인증서는 서버와 클라이언트 간의 보안 연결을 위해 웹 사이트 소유자를 식별합니다.
- 구성 후 모든 새 감사 로그가 **syslog** 서버로 전송됩니다. 이전 로그는 전송되지 않습니다.
- 덮어쓰기 정책 설정(* 보기/편집 설정 * 에서 사용 가능)은 **syslog** 서버 구성을 사용하여 로그를 관리하는 방법에 영향을 주지 않습니다.
- 감사 로그는 RFC 5424 메시징 형식을 따릅니다.

syslog 서버가 더 이상 감사 로그를 수신하지 않습니다. 어떻게 해야 합니까?

TLS 프로토콜을 사용하여 **syslog** 서버를 구성한 경우 어떤 이유로든 인증서가 유효하지 않으면 서버에서 메시지를 수신할 수 없습니다. 유효하지 않은 인증서에 대한 오류 메시지가 감사 로그에 게시됩니다.

이 문제를 해결하려면 먼저 **syslog** 서버의 인증서를 수정해야 합니다. 유효한 인증서 체인이 배치되면 * 메뉴: 설정 [감사 로그 > Syslog 서버 구성 > 모두 테스트] * 로 이동합니다.

인증서

개념

인증서 작동 방식

인증서는 인터넷 보안 통신을 위해 웹 사이트 및 서버와 같은 온라인 엔터티를 식별하는 디지털 파일입니다.

인증서는 웹 통신이 지정된 서버와 클라이언트 사이에서만 암호화된 형식으로 비공개로, 변경되지 않도록 합니다. **System Manager**를 사용하면 호스트 관리 시스템의 브라우저(클라이언트 역할)와 스토리지 시스템의 컨트롤러(서버 역할) 간에 인증서를 관리할 수 있습니다.

인증서는 신뢰할 수 있는 기관에서 서명할 수도 있고 자체 서명할 수도 있습니다. "서명"은 단순히 누군가가 소유자의 신원을 확인하고 자신의 장치를 신뢰할 수 있다는 것을 확인하는 것을 의미합니다. 스토리지 어레이에는 각 컨트롤러에서 자동으로 생성된 자체 서명 인증서가 함께 제공됩니다. 자체 서명된 인증서를 계속 사용하거나 컨트롤러와 호스트 시스템 간의 보다 안전한 연결을 위해 CA 서명 인증서를 얻을 수 있습니다.



CA 서명 인증서는 향상된 보안 보호 기능을 제공하지만(예: 중간 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 포함되어 있습니다. 루트는 특정 CA 조직을 식별합니다. 모든 네트워크 장치에 동일한 CA를 사용하는 경우 하나의 루트 인증서만 있으면 됩니다.
- 중급 — 루트에서 오프하는 것은 중간 인증서입니다. CA는 하나 이상의 중간 인증서를 발급하여 보호된 루트와 서버 인증서 간의 중간 역할을 수행합니다.
- 서버 — 체인 하단에 있는 서버 인증서는 웹 사이트 또는 기타 장치와 같은 특정 엔터티를 식별합니다. 스토리지 어레이의 각 컨트롤러에는 별도의 서버 인증서가 필요합니다.

자체 서명된 인증서

스토리지 어레이의 각 컨트롤러에는 사전 설치된 자체 서명된 인증서가 포함되어 있습니다. 자체 서명된 인증서는 타사 대신 개체 소유자가 유효성을 검사한다는 점을 제외하면 CA 서명 인증서와 비슷합니다. CA 서명 인증서와 마찬가지로 자체 서명된 인증서에는 자체 개인 키가 포함되어 있으며, 서버와 클라이언트 간의 HTTPS 연결을 통해 데이터가 암호화되고 전송되도록 합니다. 그러나 자체 서명된 인증서는 CA 서명 인증서와 동일한 신뢰 체인을 사용하지 않습니다.

자체 서명된 인증서는 브라우저에서 "신뢰할 수 있는" 인증서가 아닙니다. 자체 서명된 인증서만 포함된 웹 사이트에 연결할 때마다 브라우저에 경고 메시지가 표시됩니다. 웹 사이트로 이동할 수 있는 경고 메시지의 링크를 클릭해야 합니다. 이렇게 하면 자체 서명된 인증서를 기본적으로 수락하게 됩니다.

키 관리 서버에 사용되는 인증서

드라이브 보안 기능이 있는 외부 키 관리 서버를 사용하는 경우 해당 서버와 컨트롤러 간의 인증을 위한 인증서를 관리할 수도 있습니다.

인증서 용어

다음 용어는 인증서 관리에 적용됩니다.

기간	설명
CA	CA(인증 기관)는 인터넷 보안을 위해 디지털 인증서라는 전자 문서를 발급하는 신뢰할 수 있는 엔터티입니다. 이러한 인증서는 클라이언트와 서버 간의 보안 연결을 허용하는 웹사이트 소유자를 식별합니다.
CSR	CSR(인증서 서명 요청)은 신청자가 CA(인증 기관)로 보내는 메시지입니다. CSR은 CA가 인증서를 발급하는 데 필요한 정보를 확인합니다.
인증서	인증서는 보안 목적으로 사이트의 소유자를 식별하므로 공격자가 사이트를 가장할 수 없습니다. 인증서에는 사이트 소유자에 대한 정보와 이 정보를 인증(서명)한 신뢰할 수 있는 엔터티의 ID가 포함되어 있습니다.
인증서 체인	인증서에 보안 계층을 추가하는 파일의 계층 구조입니다. 일반적으로 체인은 계층 맨 위에 루트 인증서 하나, 중간 인증서 하나 이상 및 엔터티를 식별하는 서버 인증서를 포함합니다.
클라이언트 인증서	보안 키 관리를 위해 클라이언트 인증서는 스토리지 배열의 컨트롤러를 검증하므로 키 관리 서버가 해당 IP 주소를 신뢰할 수 있습니다.
중간 인증서	하나 이상의 중간 인증서가 인증서 체인의 루트에서 분기됩니다. CA는 하나 이상의 중간 인증서를 발급하여 보호된 루트와 서버 인증서 간의 중간 역할을 수행합니다.
키 관리 서버 인증서입니다	보안 키 관리를 위해 키 관리 서버 인증서는 서버의 유효성을 검사하므로 스토리지 배열이 해당 IP 주소를 신뢰할 수 있습니다.
키 저장소	키 저장소는 해당 공개 키 및 인증서와 함께 개인 키가 들어 있는 호스트 관리 시스템의 리포지토리입니다. 이러한 키와 인증서는 컨트롤러와 같은 사용자 고유의 엔터티를 식별합니다.
OCSP 서버	OCSP(Online Certificate Status Protocol) 서버는 CA(인증 기관)가 예약된 만료 날짜 이전에 인증서를 취소할지 여부를 확인한 다음 인증서가 해지되면 사용자가 서버에 액세스하지 못하도록 차단합니다.
루트 인증서입니다	루트 인증서는 인증서 체인의 계층 구조 맨 위에 있으며 다른 인증서에 서명하는 데 사용되는 개인 키를 포함합니다. 루트는 특정 CA 조직을 식별합니다. 모든 네트워크 장치에 동일한 CA를 사용하는 경우 하나의 루트 인증서만 있으면 됩니다.
서명된 인증서	CA(인증 기관)에서 유효성을 검사하는 인증서입니다. 이 데이터 파일에는 개인 키가 포함되어 있으며 HTTPS 연결을 통해 서버와 클라이언트 간에 암호화된 형식으로 데이터가 전송됩니다. 또한 서명된 인증서에는 개체 소유자(일반적으로 서버 또는 웹 사이트)에 대한 세부 정보와 문자와 숫자로 구성된 디지털 서명이 포함됩니다. 서명된 인증서는 신뢰 체인을 사용하므로 프로덕션 환경에서 가장 많이 사용됩니다. "CA 서명 인증서" 또는 "관리 인증서"라고도 합니다.
자체 서명된 인증서	자체 서명된 인증서는 해당 엔터티의 소유자에 의해 유효성이 검사됩니다. 이 데이터 파일에는 개인 키가 포함되어 있으며 HTTPS 연결을 통해 서버와 클라이언트 간에 암호화된 형식으로 데이터가 전송됩니다. 문자와 숫자로 구성된 디지털 서명도 포함되어 있습니다. 자체 서명된 인증서는 CA 서명 인증서와 동일한 신뢰 체인을 사용하지 않으므로 테스트 환경에서 가장 많이 사용됩니다. "사전 설치된" 인증서라고도 합니다.

기간	설명
서버 인증서	서버 인증서는 인증서 체인의 맨 아래에 있습니다. 웹 사이트 또는 기타 장치와 같은 특정 엔터티를 식별합니다. 스토리지 시스템의 각 컨트롤러에는 별도의 서버 인증서가 필요합니다.

방법

컨트롤러에 **CA** 서명 인증서를 사용합니다

컨트롤러와 System Manager 액세스에 사용되는 브라우저 간에 보안 통신을 위해 CA 서명 인증서를 얻을 수 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.

이 작업에 대해

CA 서명 인증서를 사용하는 것은 3단계 절차입니다.

1단계: 컨트롤러를 위해 **CSR**을 작성하여 제출합니다

먼저 스토리지 배열의 각 컨트롤러에 대해 CSR(인증서 서명 요청) 파일을 생성한 다음 CA(인증 기관)에 파일을 제출해야 합니다.

시작하기 전에

- 각 컨트롤러의 IP 주소 또는 DNS 이름을 알아야 합니다.

이 작업에 대해

CSR은 조직의 정보, 컨트롤러의 IP 주소 또는 DNS 이름 및 컨트롤러의 웹 서버를 식별하는 키 쌍에 대한 정보를 제공합니다. 이 작업 중에 스토리지 어레이에 하나의 컨트롤러만 있고 두 개의 컨트롤러가 있는 경우 두 개의 CSR 파일이 있는 경우 하나의 CSR 파일이 생성됩니다.



CA에 제출한 후 새 CSR을 생성하지 마십시오. CSR을 생성하면 시스템에서 개인 키 및 공개 키 쌍을 생성합니다. 공개 키는 CSR의 일부이며 개인 키는 키 저장소에 보관됩니다. 서명된 인증서를 받은 후 키 저장소로 가져오면 시스템에서는 개인 키와 공개 키가 모두 원래 쌍이 되도록 합니다. 따라서 CA에 CSR을 제출한 후 새 CSR을 생성해서는 안 됩니다. 이렇게 하면 컨트롤러가 새 키를 생성하고 CA로부터 받은 인증서는 작동하지 않습니다.

단계

1. 메뉴: 설정 [인증서] * 를 선택합니다.
2. 어레이 관리 * 탭에서 * CSR 완료 * 를 선택합니다.



두 번째 컨트롤러에 대해 자체 서명된 인증서를 수락하라는 대화 상자가 표시되면 * 자체 서명된 인증서 수락 * 을 클릭하여 계속 진행합니다.

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 * — 스토리지 배열 또는 비즈니스가 위치한 시/군/구.
- * 주/지역(선택 사항) * — 스토리지 배열 또는 비즈니스가 위치한 주 또는 지역입니다.
- * 국가 ISO 코드 * — 미국 등 해당 국가의 2자리 ISO(International Organization for Standardization) 코드입니다.



일부 필드는 컨트롤러의 IP 주소와 같은 적절한 정보로 미리 채워질 수 있습니다. 값이 올바르지 않다고 확신하지 않는 한 미리 채워진 값을 변경하지 마십시오. 예를 들어 CSR을 아직 완료하지 않은 경우 컨트롤러 IP 주소는 ""localhost""로 설정됩니다. 이 경우 "localhost"를 컨트롤러의 DNS 이름 또는 IP 주소로 변경해야 합니다.

4. 스토리지 어레이에서 컨트롤러 A에 대한 다음 정보를 확인하거나 입력합니다.

- * Controller a common name * — 컨트롤러 A의 IP 주소 또는 DNS 이름이 기본적으로 표시됩니다. 이 주소가 올바른지 확인합니다. 입력한 주소와 정확하게 일치해야 브라우저에서 System Manager에 액세스할 수 있습니다.
- * 컨트롤러 대체 IP 주소 * — 공통 이름이 IP 주소인 경우 컨트롤러 A에 대한 추가 IP 주소 또는 별칭을 선택적으로 입력할 수 있습니다 여러 항목의 경우 쉼표로 구분된 형식을 사용합니다.
- * 컨트롤러 A 대체 DNS 이름 * — 공통 이름이 DNS 이름이면 컨트롤러 A의 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. 스토리지 배열에 컨트롤러가 하나만 있는 경우 * Finish * (마침 *) 버튼을 사용할 수 있습니다. 스토리지 배열에 컨트롤러가 두 개 있는 경우 * Next * (다음 *) 버튼을 사용할 수 있습니다.



CSR 요청을 처음 생성할 때 * 이 단계 건너뛰기 * 링크를 클릭하지 마십시오. 이 링크는 오류 복구 상황에서 제공됩니다. 드문 경우지만 한 컨트롤러에서 CSR 요청이 실패할 수 있지만 다른 컨트롤러에서는 그렇지 않습니다. 이 링크를 사용하면 컨트롤러 A에서 CSR 요청을 생성하는 단계를 건너뛸 수 있습니다(이미 정의된 경우). 컨트롤러 B에서 CSR 요청을 다시 생성하기 위한 다음 단계를 계속 진행할 수 있습니다

5. 하나의 컨트롤러만 있는 경우 * 마침 * 을 클릭합니다. 두 개의 컨트롤러가 있는 경우 * 다음 * 을 클릭하여 컨트롤러 B에 대한 정보(위와 동일)를 입력한 다음 * 마침 * 을 클릭합니다.

단일 컨트롤러의 경우 하나의 CSR 파일이 로컬 시스템에 다운로드됩니다. 이중 컨트롤러의 경우 두 개의 CSR 파일이 다운로드됩니다. 다운로드의 폴더 위치는 브라우저에 따라 다릅니다.

6. 다운로드한 CSR 파일을 찾습니다. 폴더 위치는 브라우저에 따라 다릅니다.

7. CSR 파일을 CA에 제출하고 서명된 인증서를 PEM 형식으로 요청합니다.

8. CA가 인증서를 반환할 때까지 기다린 다음 로 이동합니다 **2단계: 컨트롤러의 서명된 인증서 가져오기.**

2단계: 컨트롤러의 서명된 인증서 가져오기

서명된 인증서를 받은 후에는 컨트롤러의 파일을 가져옵니다.

시작하기 전에

- CA가 서명된 인증서 파일을 반환했습니다.
- 파일은 로컬 시스템에서 사용할 수 있습니다.
- CA에서 체인 인증서(예: .p7b 파일)를 제공한 경우, 연결된 파일의 압축을 개별 파일(루트 인증서, 하나 이상의 중간 인증서, 컨트롤러를 식별하는 서버 인증서)에 풀어야 합니다. Windows 'certmgr' 유틸리티를 사용하여 파일의

압축을 풀 수 있습니다(마우스 오른쪽 버튼을 클릭하고 * MENU: 모든 작업 [내보내기] * 선택). 내보내기가 완료되면 체인의 각 인증서 파일에 대해 CER 파일이 표시됩니다.

이 작업에 대해

이 작업에서는 인증서 파일을 업로드하는 방법에 대해 설명합니다.

단계

1. 메뉴: 설정 [인증서] * 를 선택합니다.
2. Array Management * 탭에서 * Import * 를 선택합니다.

인증서 파일을 가져올 수 있는 대화 상자가 열립니다.

3. 찾아보기 * 버튼을 클릭하여 먼저 루트 및 중간 파일을 선택한 다음 컨트롤러의 각 서버 인증서를 선택합니다. 루트 파일과 중간 파일은 두 컨트롤러 모두에 대해 동일합니다. 서버 인증서만 각 컨트롤러에 대해 고유합니다.

파일 이름이 대화 상자에 표시됩니다.

4. 가져오기 * 를 클릭합니다.

파일이 업로드되고 검증됩니다.

결과

세션이 자동으로 종료됩니다. 인증서를 적용하려면 다시 로그인해야 합니다. 다시 로그인하면 새 CA 서명 인증서가 세션에 사용됩니다.

관리 인증서를 재설정합니다

CA 서명 인증서를 사용하는 것이 아니라 자체 서명된 인증서를 공장 출하시 설정된 인증서로 되돌릴 수 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.
- CA 서명 인증서는 이전에 가져와야 합니다.

이 작업에 대해

재설정 기능은 각 컨트롤러에서 현재 CA 서명 인증서 파일을 삭제합니다. 그런 다음 컨트롤러는 자체 서명 인증서를 사용하여 로 돌아갑니다.

단계

1. 메뉴: 설정 [인증서] * 를 선택합니다.
2. Array Management * 탭에서 * Reset * 을 선택합니다.

확인 * 관리 인증서 재설정 * 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

컨트롤러는 자체 서명된 인증서 사용으로 되돌아갑니다. 따라서 사용자가 세션에 대해 자체 서명된 인증서를 수동으로 수락하라는 메시지가 표시됩니다.

가져온 인증서 정보를 봅니다

인증서 페이지에서 인증서 유형, 발급 기관 및 스토리지 배열에 대한 유효한 인증서 날짜 범위를 볼 수 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.

단계

1. 설정 [인증서] 메뉴를 선택합니다.
2. 인증서에 대한 정보를 보려면 탭 중 하나를 선택합니다.

탭을 클릭합니다	설명
어레이 관리	루트 파일, 중간 파일 및 서버 파일을 포함하여 각 컨트롤러에 대해 가져온 CA 서명 인증서에 대한 정보를 봅니다.
신뢰성	컨트롤러에 대해 가져온 다른 모든 유형의 인증서에 대한 정보를 봅니다. 사용자가 설치한 인증서 또는 사전 설치된 인증서를 보려면 * 다음 인증서 표시 * 아래의 필터 필드를 사용하십시오. • * 사용자 설치 *. 컨트롤러가 서버 대신 클라이언트, LDAPS 인증서 및 Identity Federation 인증서 역할을 할 때 신뢰할 수 있는 인증서를 포함할 수 있도록 사용자가 스토리지 어레이에 업로드한 인증서입니다. • * 사전 설치됨 *. 스토리지 배열에 포함된 자체 서명된 인증서.
키 관리	외부 키 관리 서버에 대해 가져온 CA 서명 인증서에 대한 정보를 봅니다.

클라이언트로 작동할 때 컨트롤러의 인증서를 가져옵니다

네트워크 서버에 대한 신뢰 체인을 확인할 수 없기 때문에 컨트롤러가 연결을 거부하면 신뢰할 수 있는 탭에서 인증서를 가져올 수 있습니다. 그러면 컨트롤러(클라이언트 역할)가 해당 서버의 통신을 수락할 수 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.
- 인증서 파일이 로컬 시스템에 설치됩니다.

이 작업에 대해

다른 서버가 컨트롤러(예: TLS를 사용하는 LDAP 서버 또는 syslog 서버)에 접속하도록 허용하려면 신뢰할 수 있는

탭에서 인증서를 가져와야 할 수 있습니다.

단계

1. 메뉴: 설정 [인증서] * 를 선택합니다.
2. Trusted * (신뢰할 수 있는 *) 탭에서 * Import * (가져오기 *)를 선택합니다.

신뢰할 수 있는 인증서 파일을 가져올 수 있는 대화 상자가 열립니다.

3. 컨트롤러의 인증서 파일을 선택하려면 * 찾아보기 * 를 클릭합니다.

대화 상자에 파일 이름이 표시됩니다.

4. 가져오기 * 를 클릭합니다.

결과

파일이 업로드되고 검증됩니다.

인증서 해지 확인을 사용합니다

OCSP(Online Certificate Status Protocol) 서버가 비보안 연결을 만드는 사용자를 차단하도록 해지된 인증서를 자동으로 검사할 수 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.
- DNS 서버는 두 컨트롤러 모두에 구성되어 OCSP 서버에 정규화된 도메인 이름을 사용할 수 있습니다. 이 작업은 하드웨어 페이지에서 사용할 수 있습니다.
- 사용자 고유의 OCSP 서버를 지정하려면 해당 서버의 URL을 알아야 합니다.

이 작업에 대해

CA에서 인증서를 잘못 발급했거나 개인 키가 손상된 경우 자동 해지 확인을 사용하는 것이 좋습니다.

이 작업 중에 OCSP 서버를 구성하거나 인증서 파일에 지정된 서버를 사용할 수 있습니다. OCSP 서버는 CA가 예약된 만료 날짜 이전에 인증서를 취소할지 여부를 확인한 다음 인증서가 해지될 경우 사용자가 사이트에 액세스하지 못하도록 차단합니다.

단계

1. 메뉴: 설정 [인증서] * 를 선택합니다.
2. 신뢰할 수 있는 * 탭을 선택합니다.



키 관리 * 탭에서 해지 확인을 활성화할 수도 있습니다.

3. Uncommon Tasks * 를 클릭한 다음 드롭다운 메뉴에서 * Enable Revocation Checking * 을 선택합니다.
4. 해지 확인을 활성화하겠습니다 * 를 선택하면 확인란에 확인 표시가 나타나고 대화 상자에 추가 필드가 나타납니다.
5. OCSP 응답자 주소* 필드에 OCSP 응답자 서버의 URL을 선택적으로 입력할 수 있습니다. 주소를 입력하지 않으면 시스템에서 인증서 파일의 OCSP 서버 URL을 사용합니다.
6. Test Address * 를 클릭하여 시스템이 지정된 URL에 대한 연결을 열 수 있는지 확인합니다.

7. 저장 * 을 클릭합니다.

결과

스토리지 배열이 인증서가 해지된 서버에 연결을 시도하면 연결이 거부되고 이벤트가 기록됩니다.

신뢰할 수 있는 인증서를 삭제합니다

신뢰할 수 있는 탭에서 이전에 가져온 사용자 설치 인증서를 삭제할 수 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.
- 신뢰할 수 있는 인증서를 새 버전으로 업데이트하는 경우 이전 인증서를 삭제하기 전에 업데이트된 인증서를 가져와야 합니다.



대체 인증서를 가져오기 전에 컨트롤러 및 LDAP 서버와 같은 다른 서버를 인증하는 데 사용되는 인증서를 삭제하면 시스템에 대한 액세스가 끊어질 수 있습니다.

이 작업에 대해

이 작업은 사용자가 설치한 인증서를 삭제하는 방법을 설명합니다. 사전 설치된 자체 서명된 인증서는 삭제할 수 없습니다.

단계

1. 메뉴: 설정 [인증서] * 를 선택합니다.
2. 신뢰할 수 있는 * 탭을 선택합니다.

아래 표에는 스토리지 배열의 신뢰할 수 있는 인증서가 나와 있습니다.

3. 테이블에서 제거할 인증서를 선택합니다.
4. 클릭 * 메뉴: Uncommon Tasks [Delete] *

신뢰할 수 있는 인증서 삭제 확인 대화 상자가 열립니다.

5. 필드에 삭제 를 입력한 다음 * 삭제 * 를 클릭합니다.

키 관리 서버에서 인증에 **CA** 서명 인증서를 사용합니다

키 관리 서버와 스토리지 어레이 컨트롤러 간의 보안 통신을 위해 적절한 인증서 세트를 구성해야 합니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.

이 작업에 대해

컨트롤러와 키 관리 서버 간의 인증은 2단계 절차입니다.

1단계: 키 관리 서버를 사용하여 인증을 위해 **CSR**을 작성하여 제출합니다

먼저 CSR(인증서 서명 요청) 파일을 생성한 다음 CSR을 사용하여 키 관리 서버에서 신뢰할 수 있는 CA(인증 기관)로부터 서명된 클라이언트 인증서를 요청해야 합니다. 다운로드한 CSR 파일을 사용하여 키 관리 서버에서 클라이언트 인증서를 생성하고 다운로드할 수도 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.

이 작업에 대해

이 작업에서는 CSR 파일을 생성하는 방법을 설명합니다. 이 파일을 사용하여 키 관리 서버에서 신뢰할 수 있는 CA로부터 서명된 클라이언트 인증서를 요청할 수 있습니다. 클라이언트 인증서는 스토리지 어레이 컨트롤러의 유효성을 검사하므로 키 관리 서버가 KMIP(Key Management Interoperability Protocol) 요청을 신뢰할 수 있습니다. 이 작업을 수행하는 동안 조직에 대한 정보를 제공해야 합니다.

단계

1. 메뉴: 설정 [인증서] * 를 선택합니다.
2. 키 관리 * 탭에서 * CSR 완료 * 를 선택합니다.
3. 다음 정보를 입력합니다.
 - * 공통 이름 * — 인증서 파일에 표시될 스토리지 배열 이름과 같이 이 CSR을 식별하는 이름입니다.
 - * 조직 * — 회사 또는 조직의 전체 법적 이름. Inc. 또는 Corp.와 같은 접미사를 포함합니다
 - * 조직 단위(선택 사항) * — 인증서를 처리하는 조직의 사업부입니다.
 - * 시/군/구 * — 조직이 위치한 시/군/구.
 - * 시/도(선택 사항) * — 조직이 위치한 시/도 또는 지역입니다.
 - * 국가 ISO 코드 * — 귀하의 조직이 위치한 미국과 같은 두 자리 ISO(국제 표준화 기구) 코드입니다.
4. 다운로드 * 를 클릭합니다.

CSR 파일이 로컬 시스템에 저장됩니다.

5. 키 관리 서버에서 신뢰할 수 있는 CA로부터 서명된 클라이언트 인증서를 요청합니다.
6. 클라이언트 인증서가 있는 경우 로 이동합니다 [2단계: 키 관리 서버의 인증서를 가져옵니다](#).

2단계: 키 관리 서버의 인증서를 가져옵니다

다음 단계에서는 스토리지 어레이와 키 관리 서버 간에 인증을 위한 인증서를 가져옵니다. 인증서 유형에는 두 가지가 있습니다. 클라이언트 인증서는 스토리지 시스템의 컨트롤러를 검증하는 반면 키 관리 서버 인증서는 서버를 검증합니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.
- 서명된 클라이언트 인증서 파일이 있습니다(참조 [1단계: 키 관리 서버를 사용하여 인증을 위해 CSR을 작성하여 제출합니다](#)), 그리고 System Manager에 액세스하는 호스트에 해당 파일을 복사했습니다. 클라이언트 인증서는 스토리지 어레이 컨트롤러의 유효성을 검사하므로 키 관리 서버가 KMIP(Key Management Interoperability Protocol) 요청을 신뢰할 수 있습니다.
- 키 관리 서버에서 서버 인증서 파일을 검색한 다음 해당 파일을 System Manager에 액세스할 호스트에 복사해야 합니다. 키 관리 서버 인증서는 키 관리 서버의 유효성을 검사하므로 스토리지 배열이 해당 IP 주소를 신뢰할 수

있습니다.



서버 인증서에 대한 자세한 내용은 키 관리 서버 설명서를 참조하십시오.

이 작업에 대해

이 작업에서는 스토리지 컨트롤러 및 키 관리 서버 간에 인증을 위해 인증서 파일을 업로드하는 방법에 대해 설명합니다. 컨트롤러의 클라이언트 인증서 파일과 키 관리 서버의 서버 인증서 파일을 모두 로드해야 합니다.

단계

1. 메뉴: 설정 [인증서] * 를 선택합니다.
2. 키 관리 * 탭에서 * 가져오기 * 를 선택합니다.

인증서 파일을 가져올 수 있는 대화 상자가 열립니다.

3. Select client certificate * 옆에 있는 * Browse * 버튼을 클릭하여 스토리지 배열 컨트롤러의 클라이언트 인증서 파일을 선택합니다.

대화 상자에 파일 이름이 표시됩니다.

4. 키 관리 서버의 서버 인증서 선택 * 옆에 있는 * 찾아보기 * 버튼을 클릭하여 키 관리 서버의 서버 인증서 파일을 선택합니다.

대화 상자에 파일 이름이 표시됩니다.

5. 가져오기 * 를 클릭합니다.

파일이 업로드되고 검증됩니다.

키 관리 서버 인증서를 내보냅니다

키 관리 서버의 인증서를 로컬 컴퓨터에 저장할 수 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.
- 인증서를 이전에 가져와야 합니다.

단계

1. 메뉴: 설정 [인증서] * 를 선택합니다.
2. 키 관리 * 탭을 선택합니다.
3. 테이블에서 내보낼 인증서를 선택한 다음 * 내보내기 * 를 클릭합니다.

저장 대화 상자가 열립니다.

4. 파일 이름을 입력하고 * 저장 * 을 클릭합니다.

FAQ 를 참조하십시오

다른 컨트롤러에 액세스할 수 없음 대화 상자가 나타나는 이유는 무엇입니까?

인증서 가져오기 등의 CA 인증서와 관련된 특정 작업을 수행할 때 두 번째 컨트롤러에 대해 자체 서명된 인증서를 수락하라는 대화 상자가 나타날 수 있습니다.

두 개의 컨트롤러가 있는 스토리지 배열(이중 구성)에서 이 대화 상자는 SANtricity 시스템 관리자가 두 번째 컨트롤러와 통신할 수 없거나 브라우저가 특정 작업 중에 인증서를 수락할 수 없는 경우에 나타납니다.

이 대화 상자가 열리면 * 자체 서명된 인증서 수락 * 을 클릭하여 계속 진행합니다. 암호를 묻는 다른 대화 상자가 나타나면 System Manager 액세스에 사용되는 관리자 암호를 입력합니다.

이 대화 상자가 다시 나타나고 인증서 작업을 완료할 수 없는 경우 다음 절차 중 하나를 수행합니다.

- 다른 브라우저 유형을 사용하여 이 컨트롤러에 액세스하고, 인증서를 수락하고, 계속합니다.
- System Manager에서 두 번째 컨트롤러에 액세스하고, 자체 서명된 인증서를 수락한 다음 첫 번째 컨트롤러로 돌아가 계속합니다.

외부 키 관리를 위해 **System Manager**에 업로드해야 하는 인증서를 어떻게 알 수 있습니까?

외부 키 관리의 경우 두 엔터티가 서로 신뢰할 수 있도록 스토리지 배열과 키 관리 서버 간에 인증을 위해 두 가지 유형의 인증서를 가져옵니다.

클라이언트 인증서는 스토리지 어레이 컨트롤러의 유효성을 검사하므로 키 관리 서버가 KMIP(Key Management Interoperability Protocol) 요청을 신뢰할 수 있습니다. 클라이언트 인증서를 얻으려면 System Manager를 사용하여 스토리지 배열에 대한 CSR을 완료합니다. 그런 다음 CSR을 키 관리 서버에 업로드하고 여기서 클라이언트 인증서를 생성할 수 있습니다. 클라이언트 인증서가 있으면 해당 파일을 System Manager에 액세스할 호스트에 복사합니다.

키 관리 서버 인증서는 키 관리 서버의 유효성을 검사하므로 스토리지 배열이 해당 IP 주소를 신뢰할 수 있습니다. 키 관리 서버에서 서버 인증서 파일을 가져온 다음 System Manager에 액세스하는 호스트로 해당 파일을 복사합니다.

인증서 해지 확인에 대해 알아야 할 사항은 무엇입니까?

System Manager를 사용하면 인증서 해지 목록(CRL)을 업로드하는 대신 OCSP(온라인 인증서 상태 프로토콜) 서버를 사용하여 해지된 인증서를 확인할 수 있습니다.

해지된 인증서는 더 이상 신뢰할 수 없습니다. 인증서를 잘못 발급했거나 개인 키가 손상되었거나 식별된 엔터티가 정책 요구 사항을 준수하지 않은 경우와 같이 여러 가지 이유로 인증서가 해지될 수 있습니다.

시스템 관리자에서 OCSP 서버에 대한 연결을 설정한 후 스토리지 어레이는 AutoSupport 서버, EKMS(외부 키 관리 서버), LDAPS(Lightweight Directory Access Protocol over SSL) 서버 또는 Syslog 서버에 연결할 때마다 해지 확인을 수행합니다. 스토리지 배열은 이러한 서버의 인증서가 해지되지 않았는지 확인하기 위해 유효성을 검사합니다. 그런 다음 서버는 해당 인증서에 대해 "양호", "취소됨" 또는 "알 수 없음" 값을 반환합니다. 인증서가 해지되었거나 어레이가 OCSP 서버에 연결할 수 없는 경우 연결이 거부됩니다.



System Manager 또는 CLI(Command Line Interface)에서 OCSP 응답자 주소를 지정하면 인증서 파일에 있는 OCSP 주소가 재정의됩니다.

어떤 유형의 서버에 대해 해지 확인을 사용할 수 있습니까?

스토리지 시스템은 AutoSupport 서버, EKMS(외부 키 관리 서버), LDAPS(Lightweight Directory Access Protocol over SSL) 서버 또는 Syslog 서버에 연결할 때마다 해지 확인을 수행합니다.

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

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

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

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

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

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

상표 정보

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