인증서
SANtricity 11.6

NetApp
February 12, 2024

목차

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 Manager를 사용하면 호스트 관리 시스템의 브라우저(클라이언트 역할)와 스토리지 시스템의 컨트롤러(서버 역할) 간에 인증서를 관리할 수 있습니다.

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

> CA 서명 인증서는 향상된 보안 보호 기능을 제공하지만(예: 중간의 공격 방지) 대규모 네트워크를 사용하는 경우 비용이 많이 들 수 있습니다. 반면 자체 서명된 인증서는 보안성이 떨어지지만 무료입니다. 따라서 자체 서명된 인증서는 프로덕션 환경이 아닌 내부 테스트 환경에 가장 많이 사용됩니다.

서명된 인증서

서명된 인증서는 신뢰할 수 있는 타사 조직인 CA(인증 기관)에서 유효성을 검사합니다. 서명된 인증서에는 개체 소유자(일반적으로 서버 또는 웹 사이트)에 대한 세부 정보, 인증서 발급 및 만료 날짜, 엔터티에 대한 유효한 도메인 및 문자와 숫자로 구성된 디지털 서명이 포함됩니다.

브라우저를 열고 웹 주소를 입력하면 시스템은 백그라운드에서 인증서 확인 프로세스를 수행하여 유효한 CA 서명 인증서가 포함된 웹 사이트에 연결 중인지 확인합니다. 일반적으로 서명된 인증서로 보호되는 사이트에는 자물쇠 아이콘과 주소에 https 지정이 포함되어 있습니다. CA 서명 인증서가 없는 웹 사이트에 연결하려고 하면 브라우저에 사이트가 안전하지 않음을 알리는 경고가 표시됩니다.

CA는 응용 프로그램 프로세스 중에 ID를 확인하는 단계를 수행합니다. 등록된 회사에 이메일을 보내고, 회사 주소를 확인하고, HTTP 또는 DNS 확인을 수행할 수 있습니다. 응용 프로그램 프로세스가 완료되면 CA는 호스트 관리 시스템에 로드할 디지털 파일을 보냅니다. 일반적으로 이러한 파일에는 다음과 같은 신뢰 체인이 포함됩니다.

- 루트 — 계층 구조의 맨 위에 루트 인증서가 있으며, 이 인증서에는 다른 인증서에 서명하는 데 사용되는 개인 키가 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.

기간	설명
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.
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.

탭을 클릭합니다	설명
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 Manager에 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.