



인증서 SANtricity 11.5

NetApp
February 12, 2024

목차

인증서	1
개념	1
방법	2
FAQ 를 참조하십시오	10

인증서

개념

CA 인증서의 작동 방식

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.

브라우저를 열고 컨트롤러 관리 포트를 통해 System Manager에 연결하려고 하면 브라우저에서 스토리지 어레이의 컨트롤러가 신뢰할 수 있는 소스인지 확인합니다. 브라우저에서 컨트롤러에 대한 디지털 인증서를 찾을 수 없는 경우, 인식된 인증 기관이 인증서를 서명하지 않고 계속할 것인지 묻는 메시지가 표시됩니다. 이 경고를 더 이상 볼 수 없는 경우 CA로부터 서명된 디지털 인증서를 받아야 합니다.

드라이브 보안 기능이 있는 외부 키 관리 서버를 사용하는 경우 해당 서버와 컨트롤러 간 인증에 사용할 인증서를 생성하거나 스토리지 배열에서 자체 서명된 인증서를 수락할 수도 있습니다.

신뢰할 수 있는 기관에서 디지털 인증서를 사용하려면 다음 단계가 필요합니다.

1. 설정 [인증서] 메뉴로 이동합니다. 사용자 로그인에는 보안 관리자 권한이 포함되어야 합니다. 그렇지 않으면 * 인증서 * 가 페이지에 나타나지 않습니다.
2. 각 컨트롤러 또는 키 관리 서버에 대해 CSR(인증서 서명 요청)을 생성합니다.
3. CSR 파일을 CA로 보낸 다음 인증서를 보낼 때까지 기다립니다.
4. CA에서 신뢰할 수 있는(중간 및 루트) 인증서를 가져옵니다. 이러한 인증서는 CA 계층 구조에 대한 신뢰 지점을 설정합니다.
5. 각 컨트롤러 또는 키 관리 서버에 대해 서명된 관리 인증서를 가져옵니다.

인증서 용어

인증서 조건이 스토리지 어레이에 적용되는 방식에 대해 알아보십시오.

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.

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.
클라이언트 인증서	보안 키 관리를 위해 클라이언트 인증서는 스토리지 배열의 컨트롤러를 검증하므로 키 관리 서버가 해당 IP 주소를 신뢰할 수 있습니다.
키 관리 서버 인증서입니다	보안 키 관리를 위해 키 관리 서버 인증서는 서버의 유효성을 검사하므로 스토리지 배열이 해당 IP 주소를 신뢰할 수 있습니다.
관리 인증서	관리 인증서는 CA(인증 기관)에 의해 승인되며 웹 응용 프로그램에 대한 보안 액세스를 허용합니다. "서명된 인증서"라고도 합니다.
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.
자체 서명된 인증서	자체 서명된 인증서가 컨트롤러에 미리 로드됩니다. 사이트 연결이 자체 서명된 경우 웹 응용 프로그램으로 진행하기 전에 경고 메시지가 열립니다.
신뢰할 수 있는 인증서입니다	CA(인증 기관)의 신뢰할 수 있는 인증서는 인증서 계층 구조의 맨 위에 있는 알려진 인증서입니다. "루트 인증서"라고도 합니다.

방법

컨트롤러에 대한 **CA** 인증서 서명 요청(**CSR**)을 완료합니다

스토리지 배열 컨트롤러의 CA(인증 기관) 인증서를 받으려면 먼저 저장소 배열의 각 컨트롤러에 대해 CSR(인증서 서명 요청) 파일을 생성해야 합니다.

시작하기 전에

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

이 작업에 대해

이 작업에서는 컨트롤러에 대한 서명된 관리 인증서를 받기 위해 CA로 보내는 .csr 파일(인증서 서명 요청)을 생성하는 방법에 대해 설명합니다. 조직에 대한 정보와 컨트롤러의 IP 주소 또는 DNS 이름을 제공해야 합니다. 이 작업 중에 스토리지 어레이에 컨트롤러가 하나만 있고 컨트롤러가 두 개인 경우 .csr 파일이 두 개 있는 경우 .csr 파일이 하나 생성됩니다.

단계

1. 설정 [인증서] 메뉴를 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 올바르게 없다고 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 올바르게 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 심표로 구분된 형식을 사용합니다.
- * 컨트롤러 A 대체 DNS 이름 * — 공통 이름이 DNS 이름이면 컨트롤러 A의 추가 DNS 이름을 입력합니다 여러 항목의 경우 심표로 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 .csr 파일 하나가 로컬 시스템에 다운로드됩니다. 이중 컨트롤러의 경우 .csr 파일 두 개가 다운로드됩니다. 다운로드의 폴더 위치는 브라우저에 따라 다릅니다.

6. CA로 .csr 파일을 보냅니다.

작업을 마친 후

디지털 인증서를 받으면 CA가 보낸 적절한 인증서 파일을 가져옵니다.

컨트롤러의 신뢰할 수 있는 인증서를 가져옵니다

CA(인증 기관)로부터 디지털 인증서를 받은 후 컨트롤러의 인증서 체인(중간 및 루트)을 가져올 수 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.
- 인증서 서명 요청(.csr 파일)을 생성하여 CA로 보냈습니다.
- CA가 신뢰할 수 있는 인증서 파일을 반환했습니다.
- 인증서 파일이 로컬 시스템에 설치됩니다.

이 작업에 대해

이 작업에서는 스토리지 시스템의 컨트롤러에 대해 신뢰할 수 있는 인증서를 업로드하는 방법에 대해 설명합니다.

단계

1. 설정 [인증서] 메뉴를 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.

작업을 마친 후

관리 인증서를 가져옵니다.

컨트롤러의 관리 인증서를 가져옵니다

신뢰할 수 있는 인증서 체인을 가져온 후에는 스토리지 배열의 각 컨트롤러에 대한 서명된 관리 인증서 파일을 가져옵니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.
- 신뢰할 수 있는 인증서를 가져왔습니다.
- CA가 각 컨트롤러에 대한 관리 인증서 파일을 반환했습니다.
- 관리 인증서 파일은 로컬 시스템에서 사용할 수 있습니다.

이 작업에 대해

이 작업은 컨트롤러 인증을 위해 관리 인증서 파일을 업로드하는 방법을 설명합니다.

단계

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

인증서 파일을 가져올 수 있는 대화 상자가 열립니다.

3. 컨트롤러 A의 파일을 선택하려면 * 찾아보기 * 를 클릭합니다 두 개의 컨트롤러가 있는 경우 두 번째 * 찾아보기 * 버튼을 클릭하여 컨트롤러 B의 파일을 선택합니다

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.

가져온 인증서 정보를 봅니다

인증서 페이지에서 인증서 유형, 발급 기관 및 이전에 가져온 인증서의 유효한 날짜 범위를 볼 수 있습니다.

시작하기 전에

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

이 작업에 대해

이 작업에서는 사용자가 설치하거나 사전 설치한 인증서에 대한 정보를 보는 방법에 대해 설명합니다.

단계

1. 설정 [인증서] 메뉴를 선택합니다.
2. 탭 중 하나를 선택하여 컨트롤러의 관리 인증서, 신뢰할 수 있는 인증서 및 키 관리 서버의 인증서에 대한 정보를 봅니다.

탭을 클릭합니다	설명
어레이 관리	컨트롤러에 대해 가져온 모든 서버 인증서에 대한 정보를 봅니다.

탭을 클릭합니다	설명
신뢰성	컨트롤러에 대해 가져온 모든 신뢰할 수 있는(루트) 인증서에 대한 정보를 봅니다. 사용자가 설치한 인증서 또는 사전 설치된 인증서를 보려면 * 다음 인증서 표시 * 아래의 필터 필드를 사용하십시오. <ul style="list-style-type: none"> * 사용자 설치 *. 사용자가 스토리지 어레이에 업로드한 인증서(신뢰할 수 있는 인증서, LDAPS 인증서 및 ID 페더레이션 인증서 포함) * 사전 설치됨 *. 스토리지 배열에 포함된 인증서.
키 관리	외부 키 관리 서버에 대해 가져온 모든 관리(서명된) 인증서에 대한 정보를 봅니다.

신뢰할 수 있는 인증서를 삭제합니다

사용자가 가져온 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 스토리지 배열의 관리 인증서 또는 LDAP 서버를 인증하는 데 사용되는 인증서를 삭제하면 시스템에 대한 액세스가 끊어질 수 있습니다.

이 작업에 대해

이 작업은 사용자가 가져온 인증서를 삭제하는 방법을 설명합니다. 미리 정의된 인증서는 삭제할 수 없습니다.

단계

1. 설정 [인증서] 메뉴를 선택합니다.
2. 신뢰할 수 있는 * 탭을 선택합니다.

아래 표에는 스토리지 배열의 신뢰할 수 있는 인증서가 나와 있습니다.

3. 테이블에서 제거할 인증서를 선택합니다.
4. Uncommon Tasks[드문 작업][Delete] 메뉴를 클릭합니다.

신뢰할 수 있는 인증서 삭제 확인 대화 상자가 열립니다.

5. 필드에 삭제 를 입력한 다음 * 삭제 * 를 클릭합니다.

관리 인증서를 재설정합니다

스토리지 배열의 관리 인증서를 공장 자체 서명 상태로 되돌릴 수 있습니다.

시작하기 전에

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

- 인증서를 이전에 가져와야 합니다.

이 작업에 대해

스토리지 배열의 관리 인증서를 재설정하면 각 컨트롤러에서 현재 관리 인증서가 삭제됩니다. 인증서가 재설정된 후 컨트롤러는 자체 서명된 인증서를 사용하여 돌아갑니다.

단계

1. 설정 [인증서] 메뉴를 선택합니다.
2. Array Management * 탭에서 * Reset * 을 선택합니다.

관리 인증서 재설정 확인 * 대화 상자가 열립니다.

3. 필드에 reset을 입력하고 * Reset * 을 클릭합니다.

결과

브라우저를 새로 고친 후 컨트롤러는 자체 서명된 인증서 사용으로 돌아갑니다. 따라서 사용자가 세션에 대해 자체 서명된 인증서를 수동으로 수락하라는 메시지가 표시됩니다.

키 서버에 대한 **CA** 인증서 서명 요청(CSR)을 완료합니다

키 관리 서버에 대한 CA(인증 기관) 인증서를 받으려면 먼저 CSR(인증서 서명 요청) 파일을 생성해야 합니다.

시작하기 전에

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

이 작업에 대해

이 작업에서는 키 관리 서버에 대해 서명된 인증서를 받기 위해 CA로 보내는 .csr 파일(인증서 서명 요청)을 생성하는 방법에 대해 설명합니다. 이 작업을 수행하는 동안 조직에 대한 정보를 제공해야 합니다.

단계

1. 설정 [인증서] 메뉴를 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. CA로 .csr 파일을 보냅니다.

작업을 마친 후

키 관리 서버에서 클라이언트 및 서버 인증서를 가져오면 스토리지 배열 컨트롤러에서 인증을 위해 가져옵니다.

키 관리 서버 인증서를 가져옵니다

외부 키 관리의 경우 두 엔터티가 서로 신뢰할 수 있도록 스토리지 배열과 키 관리 서버 간에 인증을 위한 인증서를 가져옵니다. 인증서 유형에는 클라이언트 인증서가 컨트롤러를 검증하는 반면 키 관리 서버 인증서는 서버의 유효성을 검사하는 인증서 두 가지가 있습니다.

시작하기 전에

- 보안 관리자 권한이 포함된 사용자 프로필로 로그인해야 합니다. 그렇지 않으면 인증서 기능이 나타나지 않습니다.
- 스토리지 배열에 대해 클라이언트 인증서를 사용할 수 있습니다.



클라이언트 인증서는 스토리지 배열의 컨트롤러를 검증하므로 키 관리 서버가 해당 IP 주소를 신뢰할 수 있습니다. 클라이언트 인증서를 얻으려면 스토리지 배열에 대한 CSR을 완료한 다음 키 관리 서버에 업로드해야 합니다. 서버에서 클라이언트 인증서를 생성합니다.

- 키 관리 서버 인증서를 사용할 수 있습니다.



키 관리 서버 인증서는 서버의 유효성을 검사하므로 스토리지 배열은 해당 IP 주소를 신뢰할 수 있습니다. 키 관리 서버 인증서를 얻으려면 키 관리 서버에서 인증서를 생성해야 합니다.

이 작업에 대해

이 작업에서는 스토리지 컨트롤러 및 키 관리 서버 간에 인증을 위해 인증서 파일을 업로드하는 방법에 대해 설명합니다.

단계

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

인증서 파일을 가져올 수 있는 대화 상자가 열립니다.

3. 찾아보기 * 버튼을 클릭하여 파일을 선택합니다.

대화 상자에 파일 이름이 표시됩니다.

4. 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. 설정 [인증서] 메뉴를 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.

인증서 해지 확인을 사용합니다

OCSP(Online Certificate Status Protocol) 서버가 비보안 연결을 만드는 사용자를 차단하도록 해지된 인증서를 자동으로 검사할 수 있습니다. CA(인증 기관)가 인증서를 잘못 발급했거나 개인 키가 손상된 경우 자동 해지 확인을 사용하는 것이 좋습니다.

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

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. 설정 [인증서] 메뉴를 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.

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 Manager를 사용하여 두 번째 컨트롤러에 액세스하고, 자체 서명된 인증서를 수락한 다음 첫 번째 컨트롤러로 돌아가 계속합니다.

System Manager에 어떤 인증서를 업로드해야 하는지 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 배열의 컨트롤러를 검증하므로 키 관리 서버가 해당 IP 주소를 신뢰할 수 있습니다. 클라이언트 인증서를 얻으려면 스토리지 배열에 대한 CSR을 완료한 다음 키 관리 서버에 업로드해야 합니다. 서버에서 클라이언트 인증서를 생성한 다음 System Manager를 사용하여 인증서를 가져옵니다.

키 관리 서버 인증서는 키 관리 서버의 유효성을 검사하므로 스토리지 배열이 해당 IP 주소를 신뢰할 수 있습니다. 키 관리 서버 인증서를 얻으려면 키 관리 서버에서 인증서를 생성해야 합니다.

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.