보안 인증서 관리

Active IQ Unified Manager 9.12

NetApp
December 18, 2023

This PDF was generated from https://docs.netapp.com/ko-kr/active-iq-unified-manager-912/config/task_view_https_security_certificate_ocf.html on December 18, 2023. Always check docs.netapp.com for the latest.

목차

보안 인증서 관리

Unified Manager 서버에서 HTTPS를 구성하여 보안 연결을 통해 클러스터를 모니터링하고 관리할 수 있습니다.

HTTPS 보안 인증서 보기

HTTPS 인증서 세부 정보를 브라우저에서 검색된 인증서와 비교하여 브라우저가 Unified Manager에 암호화된 연결을 가로채 가로채지 않도록 할 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

인증서를 보면 다시 생성된 인증서의 내용을 확인하거나 Unified Manager에 액세스할 수 있는 주체 대체 이름(SAN)을 볼 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * HTTPS 인증서 * 를 클릭합니다.

   HTTPS 인증서는 페이지 맨 위에 표시됩니다

HTTPS 인증서 페이지에 표시된 것보다 보안 인증서에 대한 자세한 정보를 보려면 브라우저에서 연결 인증서를 볼 수 있습니다.

HTTPS 인증서 서명 요청을 다운로드하는 중입니다

서명할 인증 기관에 파일을 제공할 수 있도록 현재 HTTPS 보안 인증서에 대한 인증 서명 요청을 다운로드할 수 있습니다. CA 서명 인증서는 끼어들기 공격을 방지하고 자체 서명된 인증서보다 향상된 보안 보호를 제공합니다.

- 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * HTTPS 인증서 * 를 클릭합니다.
2. HTTPS 인증서 서명 요청 다운로드 * 를 클릭합니다.
3. 를 저장합니다 `<hostname>.csr` 파일.

서명하도록 인증 기관에 파일을 제공한 다음 서명된 인증서를 설치할 수 있습니다.

서명되고 반환된 HTTPS 인증서를 설치하는 중입니다

인증 기관이 서명하여 반환한 후에 보안 인증서를 업로드 및 설치할 수 있습니다. 업로드 및

설치하는 파일은 자체 서명된 기존 인증서의 서명된 버전이어야 합니다. CA 서명 인증서는 끼어들기 공격을 방지하고 자체 서명된 인증서보다 더 나은 보안 보호를 제공합니다.

- 필요한 것 *

다음 작업을 완료해야 합니다.

- 인증서 서명 요청 파일을 다운로드하고 인증 기관에서 서명했습니다
- 인증서 체인을 PEM 형식으로 저장했습니다
- 중간 인증서를 비롯하여 Unified Manager 서버 인증서에서 루트 서명 인증서까지 체인에 있는 모든 인증서가 포함됩니다

애플리케이션 관리자 역할이 있어야 합니다.

> CSR이 생성된 인증서의 유효 기간이 397일 이상인 경우 CA가 인증서를 서명 및 반환하기 전에 유효 기간을 397일로 줄입니다

단계

1. 왼쪽 탐색 창에서 * 일반 * > * HTTPS 인증서 * 를 클릭합니다.
2. HTTPS 인증서 설치 * 를 클릭합니다.
3. 표시되는 대화 상자에서 * 파일 선택… * 을 클릭하여 업로드할 파일을 찾습니다.
4. 파일을 선택한 다음 * 설치 * 를 클릭하여 파일을 설치합니다.

   자세한 내용은 을 참조하십시오 "외부 도구를 사용하여 생성된 HTTPS 인증서 설치".

인증서 체인의 예

다음 예제에서는 인증서 체인 파일이 표시되는 방법을 보여 줍니다.

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

외부 도구를 사용하여 생성된 **HTTPS** 인증서 설치

자체 서명 또는 CA 서명된 인증서를 설치할 수 있으며 OpenSSL, BoringSSL, LetsEncrypt와 같은 외부 도구를 사용하여 생성할 수 있습니다.

이러한 인증서는 외부에서 생성된 공개-개인 키 쌍이므로 인증서 체인과 함께 개인 키를 로드해야 합니다. 허용된 키 쌍 알고리즘은 "RSA"와 "EC"입니다. HTTPS 인증서 설치 * 옵션은 일반 섹션의 HTTPS 인증서 페이지에서 사용할 수 있습니다. 업로드하는 파일은 다음과 같은 입력 형식이어야 합니다.

1. Active IQ Unified Manager 호스트에 속한 서버의 개인 키입니다
2. 개인 키와 일치하는 서버의 인증서입니다
3. 위의 인증서에 서명하는 데 사용되는 루트까지 CA의 인증서가 반대입니다

EC 키 쌍을 사용하여 인증서를 로드하는 형식입니다

허용되는 곡선은 프리메256v1, 에코384r1입니다. 외부에서 생성된 EC 쌍이 있는 인증서 샘플:

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

RSA 키 쌍을 사용하여 인증서를 로드하는 형식입니다

호스트 인증서에 속하는 RSA 키 쌍에 허용되는 키 크기는 2048, 3072 및 4096입니다. 외부에서 생성된 * RSA 키 쌍이 포함된 인증서 *:

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

인증서가 업로드되면 Active IQ Unified Manager 인스턴스를 다시 시작하여 변경 내용을 적용해야 합니다.

외부에서 생성된 인증서를 업로드하는 동안 확인합니다

시스템은 외부 툴을 사용하여 생성된 인증서를 업로드하는 동안 검사를 수행합니다. 확인 중 하나라도 실패하면 인증서가 거부됩니다. 또한 제품 내에서 CSR에서 생성된 인증서 및 외부 도구를 사용하여 생성된 인증서에 대한 유효성 검사가 포함되어 있습니다.

- 입력의 개인 키는 입력의 호스트 인증서에 대해 유효성이 검사됩니다.
- 호스트 인증서의 CN(일반 이름)이 호스트의 FQDN에 대해 확인됩니다.
- 호스트 인증서의 CN(일반 이름)은 비어 있거나 비어 있어서는 안 되며 localhost로 설정해서는 안 됩니다.
- 유효 시작 날짜는 미래일 수 없으며 인증서의 유효 기간이 과거일 수 없습니다.
- 중간 CA 또는 CA가 있는 경우 인증서의 유효 시작 날짜는 미래일 수 없으며 유효 기간 만료 날짜는 과거일 수 없습니다.

> 입력의 개인 키는 암호화해서는 안 됩니다. 암호화된 개인 키가 있으면 시스템에서 거부됩니다.

예 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

예 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

예 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

인증서 관리에 대한 페이지 설명입니다

HTTPS 인증서 페이지를 사용하여 현재 보안 인증서를 보고 새 HTTPS 인증서를 생성할 수 있습니다.

HTTPS 인증서 페이지

HTTPS 인증서 페이지에서는 현재 보안 인증서를 보거나, 인증서 서명 요청을 다운로드하거나, 자체 서명된 새 HTTPS 인증서를 생성하거나, 새 HTTPS 인증서를 설치할 수 있습니다.

자체 서명된 새 HTTPS 인증서를 생성하지 않은 경우 이 페이지에 나타나는 인증서는 설치 중에 생성된 인증서입니다.

명령 버튼

명령 단추를 사용하여 다음 작업을 수행할 수 있습니다.

- * HTTPS 인증서 서명 요청 다운로드 *

  현재 설치된 HTTPS 인증서에 대한 인증 요청을 다운로드합니다. 브라우저에서 <hostname>.csr 파일을 저장하라는 메시지를 표시하면 서명할 인증 기관에 파일을 제공할 수 있습니다.

- * HTTPS 인증서 설치 *

  인증 기관이 서명하여 반환한 후에 보안 인증서를 업로드 및 설치할 수 있습니다. 관리 서버를 다시 시작한 후 새 인증서가 적용됩니다.

- * HTTPS 인증서 재생성 *

  현재 보안 인증서를 대체하는 자체 서명된 새 HTTPS 인증서를 생성할 수 있습니다. 새 인증서는 Unified Manager를 다시 시작한 후에 적용됩니다.

HTTPS 인증서 재생성 대화 상자

HTTPS 인증서 다시 생성 대화 상자에서는 보안 정보를 사용자 지정한 다음 해당 정보로 새 HTTPS 인증서를 생성할 수 있습니다.

현재 인증서 정보가 이 페이지에 나타납니다.

""현재 인증서 특성을 사용하여 재생성" 및 ""현재 인증서 특성 업데이트" 선택 항목을 사용하면 현재 정보로 인증서를 다시 생성하거나 새 정보로 인증서를 생성할 수 있습니다.

- * 일반 이름 *

  필수 요소입니다. 보안하려는 FQDN(정규화된 도메인 이름)입니다.

  Unified Manager 고가용성 구성에서 가상 IP 주소를 사용합니다.

- * 이메일 *

  선택 사항. 조직에 연락할 이메일 주소. 일반적으로 인증서 관리자 또는 IT 부서의 이메일 주소입니다.

- * 회사 *

  선택 사항. 일반적으로 회사의 통합 이름입니다.

- * 부서 *

  선택 사항. 회사의 부서 이름입니다.

- * 시 *

  선택 사항. 회사의 도시 위치입니다.

- * 시/도 *

  선택 사항. 회사의 시/도 위치(약어로 표시되지 않음)입니다.

- * 국가 *

  선택 사항. 회사의 국가 위치입니다. 이 코드는 일반적으로 해당 국가의 2자리 ISO 코드입니다.

- * 대체 이름 *

  필수 요소입니다. 기존 localhost 또는 기타 네트워크 주소 외에 이 서버에 액세스하는 데 사용할 수 있는 추가, 비기본 도메인 이름입니다. 각 대체 이름을 쉼표로 구분합니다.

  인증서의 대체 이름 필드에서 로컬 식별 정보를 제거하려면 "'로컬 식별 정보 제외(예: localhost)'" 확인란을 선택합니다. 이 확인란을 선택하면 필드에 입력한 항목만 대체 이름 필드에 사용됩니다. 공백으로 두면 결과 인증서에 대체 이름 필드가 전혀 없습니다.

- * 키 크기(키 알고리즘: RSA) *

  키 알고리즘은 RSA로 설정됩니다. 2048, 3072 또는 4096비트의 키 크기 중 하나를 선택할 수 있습니다. 기본 키

크기는 2048비트로 설정됩니다.

- * 유효 기간 *

  기본 유효 기간은 397일입니다. 이전 버전에서 업그레이드한 경우 이전 인증서 유효성이 변경되지 않은 상태로 표시될 수 있습니다.

자세한 내용은 을 참조하십시오 "HTTPS 인증서를 생성하는 중입니다".

저작권 정보

Copyright © 2023 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 라이센스와 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 라이센스도 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 라이센스를 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 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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