웹 서비스 관리
ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/ko-kr/ontap/system-admin/manage-web-services-concept.html on February 12, 2026. Always check docs.netapp.com for the latest.

목차

웹 서비스 관리

웹 서비스 관리 개요

클러스터 또는 SVM(Storage Virtual Machine)에 대한 웹 서비스를 설정 또는 해제하고, 웹 서비스 설정을 표시하고, 역할 사용자가 웹 서비스에 액세스할 수 있는지 여부를 제어할 수 있습니다.

다음과 같은 방법으로 클러스터 또는 SVM을 위한 웹 서비스를 관리할 수 있습니다.

- 특정 웹 서비스 활성화 또는 비활성화
- 웹 서비스에 대한 액세스가 암호화된 HTTP(SSL)로만 제한되는지 여부 지정
- 웹 서비스의 사용 가능 여부를 표시합니다
- 역할의 사용자가 웹 서비스에 액세스할 수 있도록 허용 또는 허용하지 않습니다
- 웹 서비스에 액세스할 수 있는 역할을 표시합니다

사용자가 웹 서비스에 액세스하려면 다음 조건을 모두 충족해야 합니다.

- 사용자를 인증해야 합니다.

  예를 들어 웹 서비스에서 사용자 이름과 암호를 묻는 메시지가 표시될 수 있습니다. 사용자의 응답은 유효한 계정과 일치해야 합니다.

- 사용자는 올바른 액세스 방법을 사용하여 설정해야 합니다.

  지정된 웹 서비스에 대해 올바른 액세스 방법을 사용하는 사용자에게만 인증이 성공합니다. ONTAP API 웹 서비스('ontapi')의 경우 사용자에게 "ontapi" 액세스 방법이 있어야 합니다. 다른 모든 웹 서비스의 경우 사용자는 http 액세스 방법을 가지고 있어야 합니다.

  를 사용합니다 `security login` 사용자의 액세스 방법 및 인증 방법을 관리하는 명령입니다.

- 사용자의 액세스 제어 역할을 허용하도록 웹 서비스를 구성해야 합니다.

  'vserver services web access' 명령을 사용하여 웹 서비스에 대한 역할의 액세스를 제어합니다.

방화벽이 설정된 경우 웹 서비스에 사용할 LIF의 방화벽 정책을 HTTP 또는 HTTPS를 허용하도록 설정해야 합니다.

웹 서비스 액세스에 HTTPS를 사용하는 경우, 웹 서비스를 제공하는 클러스터 또는 SVM에 SSL도 사용하도록 설정해야 하며 클러스터 또는 SVM에 대한 디지털 인증서를 제공해야 합니다.

ONTAP 웹 서비스에 대한 액세스 관리

웹 서비스는 사용자가 HTTP 또는 HTTPS를 사용하여 액세스할 수 있는 응용 프로그램입니다. 클러스터 관리자는 웹 프로토콜 엔진을 설정하고, SSL을 구성하고, 웹 서비스를 활성화하고, 역할의 사용자가 웹 서비스에 액세스할 수 있도록 할 수 있습니다.

ONTAP 9.6부터는 다음과 같은 웹 서비스가 지원됩니다.

- 서비스 프로세서 인프라('pi')

  이 서비스에서는 클러스터 관리 LIF 또는 노드 관리 LIF를 통해 노드의 로그, 코어 덤프 및 MIB 파일을 HTTP 또는 HTTPS 액세스에 사용할 수 있습니다. 기본 설정은 "사용"입니다.

  노드의 로그 파일이나 코어 덤프 파일에 액세스하라는 요청이 있을 경우 `spi` 웹 서비스는 파일이 있는 노드에서 다른 노드의 루트 볼륨으로의 마운트 지점을 자동으로 생성합니다. 마운트 지점을 수동으로 생성할 필요는 없습니다.

- ONTAP API('ontapi')

  이 서비스를 사용하면 ONTAP API를 실행하여 원격 프로그램으로 관리 기능을 실행할 수 있습니다. 기본 설정은 "사용"입니다.

  일부 외부 관리 도구에 이 서비스가 필요할 수 있습니다. 예를 들어, System Manager를 사용하는 경우 이 서비스를 활성 상태로 유지해야 합니다.

- Data ONTAP 디스커버리(disco)

  이 서비스를 사용하면 오프 박스 관리 애플리케이션이 네트워크에서 클러스터를 검색할 수 있습니다. 기본 설정은 "사용"입니다.

- 지원 진단('Support')

  이 서비스는 시스템의 특별 권한 환경에 대한 액세스를 제어하여 문제 분석 및 해결을 지원합니다. 기본 설정은 사용 안 함 입니다. 기술 지원 부서의 지시가 있을 때만 이 서비스를 활성화해야 합니다.

- System Manager('smmgr')

  이 서비스는 ONTAP에 포함된 System Manager의 가용성을 제어합니다. 기본 설정은 "사용"입니다. 이 서비스는 클러스터에서만 지원됩니다.

- 펌웨어 베이스보드 관리 컨트롤러(BMC) 업데이트('FW_BMC')

  이 서비스를 사용하여 BMC 펌웨어 파일을 다운로드할 수 있습니다. 기본 설정은 "사용"입니다.

- ONTAP 문서(dOCS)

  이 서비스를 통해 ONTAP 설명서에 액세스할 수 있습니다. 기본 설정은 "사용"입니다.

- ONTAP RESTful API(DOCS_API)

  이 서비스를 통해 ONTAP RESTful API 설명서에 액세스할 수 있습니다. 기본 설정은 "사용"입니다.

- 파일 업로드 및 다운로드('FUD')

  이 서비스는 파일 업로드 및 다운로드를 제공합니다. 기본 설정은 "사용"입니다.

- ONTAP 메시징('ontapmsg')

  이 서비스는 이벤트에 등록할 수 있는 게시 및 구독 인터페이스를 지원합니다. 기본 설정은 "사용"입니다.

- ONTAP 포털('포털')

  이 서비스는 게이트웨이를 가상 서버에 구현합니다. 기본 설정은 "사용"입니다.

- ONTAP Restful Interface(재차)

  이 서비스는 클러스터 인프라의 모든 요소를 원격으로 관리하는 데 사용되는 RESTful 인터페이스를 지원합니다. 기본 설정은 "사용"입니다.

- SAML(Security Assertion Markup Language) 서비스 공급자 지원(SAML)

  이 서비스는 SAML 서비스 공급자를 지원하는 리소스를 제공합니다. 기본 설정은 "사용"입니다.

- SAML 서비스 공급자(SML-SP)

  이 서비스는 SP 메타데이터 및 어설션 소비자 서비스와 같은 서비스를 서비스 공급자에게 제공합니다. 기본 설정은 "사용"입니다.

ONTAP 9.7부터는 다음과 같은 추가 서비스가 지원됩니다.

- 구성 백업 파일('백업')

  이 서비스를 사용하면 구성 백업 파일을 다운로드할 수 있습니다. 기본 설정은 "사용"입니다.

- ONTAP 보안('보안')

  이 서비스는 향상된 인증을 위해 CSRF 토큰 관리를 지원합니다. 기본 설정은 "사용"입니다.

ONTAP에서 웹 프로토콜 엔진을 관리합니다

웹 액세스가 허용되는지 여부와 사용할 수 있는 SSL 버전을 제어하도록 클러스터의 웹 프로토콜 엔진을 구성할 수 있습니다. 웹 프로토콜 엔진에 대한 구성 설정을 표시할 수도 있습니다.

다음과 같은 방법으로 클러스터 수준에서 웹 프로토콜 엔진을 관리할 수 있습니다.

- '-external' 파라미터를 가진 'system services web modify' 명령어를 이용하여 원격 클라이언트가 HTTP나 HTTPS를 이용하여 웹 서비스 컨텐츠에 액세스할 수 있는지 여부를 지정할 수 있다.
- '-supported-protocol' 파라미터를 가진 '보안 설정 수정' 명령어를 이용하여 SSLv3을 안전한 웹 액세스에 사용할지 여부를 지정할 수 있다. 기본적으로 SSLv3은 비활성화되어 있습니다. 전송 계층 보안 1.0(TLSv1.0)이 활성화되어 있으며 필요한 경우 비활성화할 수 있습니다.

  에 대한 자세한 내용은 `security config modify` "ONTAP 명령 참조입니다"을 참조하십시오.

- FIPS(Federal Information Processing Standard) 140-2 규정 준수 모드를 사용하여 클러스터 전체의 컨트롤 플레인 웹 서비스 인터페이스를 구현할 수 있습니다.

  기본적으로 FIPS 140-2 규정 준수 모드는 비활성화되어 있습니다.

  ◦ * FIPS 140-2 compliance mode 비활성화 시 * '보안 구성 수정' 명령에 대해 'is-FIPS-enabled' 매개 변수를 'true'로 설정한 다음 'security config show' 명령을 사용하여 온라인 상태를 확인하면 FIPS 140-2 compliance

모드를 사용할 수 있습니다.

◦ * FIPS 140-2 규정 준수 모드가 활성화된 경우 *

▪ ONTAP 9.11.1부터 TLSv1, TLSv1.1 및 SSLv3이 비활성화되고 TSLv1.2 및 TSLv1.3만 활성화됩니다. ONTAP 9 내부와 외부의 다른 시스템 및 통신에 영향을 줍니다. FIPS 140-2 규정 준수 모드를 활성화한 후 이후에 사용하지 않도록 설정하는 경우 TLSv1, TLSv1.1 및 SSLv3은 비활성화 상태로 유지됩니다. TLSv1.2 또는 TLSv1.3은 이전 구성에 따라 활성화된 상태로 유지됩니다.

▪ 9.11.1 이전의 ONTAP 버전에서는 TLSv1 및 SSLv3이 모두 사용되지 않고 TLSv1.1 및 TLSv1.2만 활성화됩니다. ONTAP를 사용하면 FIPS 140-2 규정 준수 모드가 활성화된 경우 TLSv1 및 SSLv3을 모두 사용할 수 없습니다. FIPS 140-2 규정 준수 모드를 활성화한 후 나중에 비활성화하면 TLSv1 및 SSLv3은 비활성화 상태로 유지되지만 TLSv1.2 또는 TLSv1.1 및 TLSv1.2는 이전 구성에 따라 모두 활성화됩니다.

- 'system security config show' 명령을 사용하여 클러스터 차원의 보안 구성을 표시할 수 있습니다.

에 대한 자세한 내용은 `security config show` "ONTAP 명령 참조입니다"을 참조하십시오.

방화벽이 설정된 경우 웹 서비스에 사용할 논리 인터페이스(LIF)의 방화벽 정책을 HTTP 또는 HTTPS 액세스를 허용하도록 설정해야 합니다.

웹 서비스 액세스에 HTTPS를 사용하는 경우, 웹 서비스를 제공하는 클러스터 또는 SVM(스토리지 가상 머신)에 SSL도 사용하도록 설정해야 하며 클러스터 또는 SVM에 디지털 인증서를 제공해야 합니다.

MetroCluster 구성에서는 클러스터의 웹 프로토콜 엔진에 대해 변경한 설정이 파트너 클러스터에 복제되지 않습니다.

웹 프로토콜 엔진을 관리하기 위한 **ONTAP** 명령

'system services web' 명령어를 이용하여 웹 프로토콜 엔진을 관리한다. '시스템 서비스 방화벽 정책 생성' 및 '네트워크 인터페이스 수정' 명령을 사용하여 웹 액세스 요청이 방화벽을 통과할 수 있도록 합니다.

원하는 작업	이 명령 사용...
클러스터 수준에서 웹 프로토콜 엔진을 구성합니다. • 클러스터에 대한 웹 프로토콜 엔진을 설정하거나 해제합니다 • 클러스터에 대해 SSLv3을 사용하거나 사용하지 않도록 설정합니다 • 보안 웹 서비스(HTTPS)를 위해 FIPS 140-2 규정 준수 활성화 또는 비활성화	'시스템 서비스 웹 수정
클러스터 수준에서 웹 프로토콜 엔진의 구성을 표시하고, 클러스터 전체에서 웹 프로토콜이 작동하는지 여부를 확인하고, FIPS 140-2 규정 준수를 활성화 및 온라인 상태로 표시합니다	'시스템 서비스 웹 쇼'
노드의 웹 프로토콜 엔진 구성 및 클러스터의 노드에 대한 웹 서비스 처리 작업을 표시합니다	'시스템 서비스 웹 노드 쇼'

원하는 작업	이 명령 사용...
방화벽 정책을 생성하거나 기존 방화벽 정책에 HTTP 또는 HTTPS 프로토콜 서비스를 추가하여 웹 액세스 요청이 방화벽을 통과할 수 있도록 합니다	'시스템 서비스 방화벽 정책 생성 service 매개 변수를 http 또는 https로 설정하면 웹 액세스 요청이 방화벽을 통과할 수 있습니다.
방화벽 정책을 LIF와 연결합니다	네트워크 인터페이스 수정 '-firewall-policy' 매개 변수를 사용하여 LIF의 방화벽 정책을 수정할 수 있습니다.

관련 정보

- "네트워크 인터페이스 수정"

ONTAP 웹 서비스에 대한 액세스 구성

웹 서비스에 대한 액세스를 구성하면 권한 있는 사용자가 HTTP 또는 HTTPS를 사용하여 클러스터의 서비스 콘텐츠 또는 SVM(스토리지 가상 머신)에 액세스할 수 있습니다.

단계

1. 방화벽이 설정된 경우 웹 서비스에 사용될 LIF의 방화벽 정책에 HTTP 또는 HTTPS 액세스가 설정되어 있는지 확인합니다.

   'system services firewall show' 명령을 사용하여 방화벽이 활성화되어 있는지 확인할 수 있습니다.

   a. 방화벽 정책에 HTTP 또는 HTTPS가 설정되어 있는지 확인하려면 'system services firewall policy show' 명령을 사용합니다.

      시스템 서비스 방화벽 정책의 '-service' 매개 변수를 'http' 또는 'https'로 설정하여 해당 정책이 웹 액세스를 지원할 수 있도록 합니다.

   b. HTTP 또는 HTTPS를 지원하는 방화벽 정책이 웹 서비스를 제공하는 LIF와 연결되어 있는지 확인하려면 '-firewall-policy' 매개 변수와 함께 'network interface show' 명령을 사용하십시오.

      에 대한 자세한 내용은 `network interface show` "ONTAP 명령 참조입니다"을 참조하십시오.

      'network interface modify' 명령을 '-firewall-policy' 매개 변수와 함께 사용하여 LIF에 방화벽 정책을 적용합니다.

   에 대한 자세한 내용은 `network interface modify` "ONTAP 명령 참조입니다"을 참조하십시오.

2. 클러스터 수준 웹 프로토콜 엔진을 구성하고 웹 서비스 콘텐츠를 액세스할 수 있도록 하려면 'system services web modify' 명령을 사용합니다.
3. 보안 웹 서비스(HTTPS)를 사용하려는 경우 '보안 SSL 수정' 명령을 사용하여 SSL을 활성화하고 클러스터 또는 SVM에 대한 디지털 인증서 정보를 제공합니다.

   에 대한 자세한 내용은 `security ssl modify` "ONTAP 명령 참조입니다"을 참조하십시오.

4. 클러스터 또는 SVM에 대한 웹 서비스를 활성화하려면 'vserver services web modify' 명령을 사용하십시오.

   클러스터 또는 SVM에 대해 활성화할 각 서비스에 대해 이 단계를 반복해야 합니다.

5. 클러스터 또는 SVM에서 웹 서비스에 액세스하는 역할을 승인하려면 'vserver services web access create' 명령을 사용하십시오.

   액세스 권한을 부여하는 역할이 이미 있어야 합니다. 'Security login role show' 명령어를 사용해 기존 역할을 표시하거나, 'ecurity login role create' 명령어를 사용해 새로운 역할을 생성할 수 있다.

   및 `security login role create` 에 대한 자세한 `security login role show` 내용은 을 "ONTAP 명령 참조입니다"참조하십시오.

6. 웹 서비스에 액세스할 수 있는 권한을 가진 역할의 경우, '보안 로그인 표시' 명령의 출력을 확인하여 사용자가 올바른 액세스 방법을 사용하도록 구성해야 합니다.

   ONTAP API 웹 서비스('ontapi')에 액세스하려면 사용자가 "ontapi" 액세스 방법으로 구성해야 합니다. 다른 모든 웹 서비스에 액세스하려면 사용자가 http 액세스 방법으로 구성되어야 합니다.

   에 대한 자세한 내용은 `security login show` "ONTAP 명령 참조입니다"을 참조하십시오.

   명령을 사용하여 `security login create` 사용자에 대한 액세스 방법을 추가합니다. 에 대한 자세한 내용은 `security login create` "ONTAP 명령 참조입니다"을 참조하십시오.

웹 서비스 관리를 위한 **ONTAP** 명령

'vserver services web' 명령을 사용하여 클러스터나 SVM(스토리지 가상 머신)의 웹 서비스 가용성을 관리할 수 있습니다. 'vserver services web access' 명령을 사용하여 웹 서비스에 대한 역할의 액세스를 제어합니다.

원하는 작업	이 명령 사용...
클러스터 또는 SVM을 위한 웹 서비스 구성: • 웹 서비스를 활성화 또는 비활성화합니다 • 웹 서비스에 액세스하는 데 HTTPS만 사용할 수 있는지 여부를 지정합니다	가상 서버 서비스 웹 수정
클러스터 또는 anSVM을 위한 웹 서비스의 구성 및 가용성을 표시합니다	가상 서버 서비스 웹 쇼
클러스터 또는 SVM에서 웹 서비스에 액세스하는 역할을 승인합니다	'vserver services web access create'
클러스터 또는 anSVM에서 웹 서비스에 액세스하도록 승인된 역할을 표시합니다	'vserver services web access show'

원하는 작업	이 명령 사용...
클러스터 또는 SVM에서 웹 서비스에 대한 역할 액세스 방지	'vserver services web access delete'(가상 서버 서비스 웹 액세스 삭제)

관련 정보

"ONTAP 명령 참조입니다"

ONTAP 노드의 마운트 포인트를 관리하기 위한 명령

'pi' 웹 서비스는 노드의 로그 파일 또는 코어 파일에 대한 액세스 요청이 있을 경우 한 노드에서 다른 노드의 루트 볼륨으로 마운트 지점을 자동으로 생성합니다. 마운트 지점을 수동으로 관리할 필요는 없지만 'system node root-mount' 명령을 사용하면 됩니다.

원하는 작업	이 명령 사용...
한 노드에서 다른 노드의 루트 볼륨으로 마운트 지점을 수동으로 생성합니다	'시스템 노드 root-mount create' 하나의 노드만 다른 노드로 존재할 수 있다.
마운트 지점이 생성된 시간과 현재 상태를 포함하여 클러스터의 노드에 기존 마운트 지점을 표시합니다	'system node root-mount show'
한 노드에서 다른 노드의 루트 볼륨으로 마운트 지점을 삭제하고 마운트 지점에 대한 연결을 강제로 닫습니다	'시스템 노드 root-mount delete

관련 정보

"ONTAP 명령 참조입니다"

ONTAP 에서 SSL 관리

를 사용합니다 `security ssl` 클러스터 또는 SVM(스토리지 가상 머신)에 대한 SSL 프로토콜을 관리하는 명령입니다. SSL 프로토콜은 디지털 인증서를 사용하여 웹 서버와 브라우저 간에 암호화된 연결을 설정함으로써 웹 액세스의 보안을 향상시킵니다.

다음과 같은 방법으로 클러스터 또는 SVM(스토리지 가상 머신)의 SSL을 관리할 수 있습니다.

- SSL 활성화
- 디지털 인증서를 생성 및 설치하고 이를 클러스터 또는 SVM과 연계합니다
- SSL이 활성화되었는지 여부를 확인하기 위해 SSL 구성을 표시하고, 사용 가능한 경우 SSL 인증서 이름을 표시합니다
- 웹 액세스 요청을 통과할 수 있도록 클러스터 또는 SVM에 대한 방화벽 정책 설정
- 사용할 수 있는 SSL 버전을 정의합니다
- 웹 서비스에 대한 HTTPS 요청에만 액세스를 제한합니다

SSL 관리를 위한 명령입니다

를 사용합니다 `security ssl` 클러스터 또는 SVM(스토리지 가상 머신)에 대한 SSL 프로토콜을 관리하는 명령입니다.

원하는 작업	이 명령 사용...
클러스터 또는 SVM에 SSL을 활성화하고 디지털 인증서를 연결합니다	보안 SSL 수정
클러스터 또는 SVM의 SSL 구성과 인증서 이름을 표시합니다	보안 SSL 쇼

및 `security ssl show` 에 대한 자세한 `security ssl modify` 내용은 을 "ONTAP 명령 참조입니다 "참조하십시오.

ONTAP 웹 서비스에 HSTS 사용

HTTP Strict Transport Security(HSTS)는 프로토콜 다운그레이드 공격 및 쿠키 하이재킹과 같은 중간자 공격으로부터 웹사이트를 보호하는 웹 보안 정책 메커니즘입니다. HSTS는 HTTPS 사용을 강제함으로써 사용자 브라우저와 서버 간의 모든 통신이 암호화되도록 보장합니다. ONTAP 9.17.1부터 ONTAP ONTAP 웹 서비스에 HTTPS 연결을 강제할 수 있습니다.

HSTS는 ONTAP 과 초기 보안 HTTPS 연결이 설정된 후에만 웹 브라우저에 의해 적용됩니다. 브라우저가 초기 보안 연결을 설정하지 않으면 HSTS가 적용되지 않습니다. HSTS 관리에 대한 자세한 내용은 브라우저 설명서를 참조하십시오.

이 작업에 대해

- 9.17.1 이상에서는 새로 설치된 ONTAP 클러스터에 대해 HSTS가 기본적으로 활성화되어 있습니다. 9.17.1로 업그레이드하면 HSTS가 기본적으로 활성화되지 않습니다. 업그레이드 후 HSTS를 활성화해야 합니다.
- HSTS는 모든 지원됩니다 "ONTAP 웹 서비스" .

시작하기 전에

- 다음 작업에는 고급 권한이 필요합니다.

HSTS 구성 표시

현재 HSTS 구성을 표시하여 활성화되어 있는지 확인하고 최대 연령 설정을 볼 수 있습니다.

단계

1. 사용하세요 `system services web show` HSTS 설정을 포함한 현재 웹 서비스 구성을 표시하는 명령:

```
cluster-1::system services web*> show

                    External Web Services: true
                                HTTP Port: 80
                               HTTPS Port: 443
                          Protocol Status: online
                       Per Address Limit: 80
                     Wait Queue Capacity: 192
                            HTTP Enabled: true
                  CSRF Protection Enabled: true
Maximum Number of Concurrent CSRF Tokens: 500
       CSRF Token Idle Timeout (Seconds): 900
   CSRF Token Absolute Timeout (Seconds): 0
          Allow Web Management via Cloud: true
Enforce Network Interface Service-Policy: -
                            HSTS Enabled: true
                  HSTS max age (Seconds): 63072000
```

HSTS를 활성화하고 최대 연령을 설정하세요

ONTAP 9.17.1부터 새 ONTAP 클러스터에서 HSTS가 기본적으로 활성화됩니다. 기존 클러스터를 9.17.1 이상으로 업그레이드하는 경우, HTTPS 사용을 강제하려면 클러스터에서 HSTS를 수동으로 활성화해야 합니다. HSTS를 활성화하고 최대 사용 기간을 설정할 수 있습니다. HSTS가 활성화된 경우 언제든지 최대 사용 기간을 변경할 수 있습니다. HSTS가 활성화되면 브라우저는 초기 보안 연결이 설정된 후에만 보안 연결을 적용하기 시작합니다.

단계

1. 사용하세요 `system services web modify` HSTS를 활성화하거나 최대 연령을 수정하는 명령:

```
system services web modify -hsts-enabled true -hsts-max-age <seconds>
```

`-hsts-max-age` 브라우저가 HTTPS를 강제 적용하는 기간을 초 단위로 지정합니다. 기본값은 63072000초(2년)입니다.

HSTS 비활성화

브라우저는 각 연결마다 HSTS 최대 사용 기간 설정을 저장하며, ONTAP 에서 HSTS가 비활성화된 경우에도 전체 기간 동안 HSTS를 계속 적용합니다. HSTS가 비활성화된 후 브라우저가 HSTS 적용을 중단하는 데는 설정된 최대 사용 기간까지 걸립니다. 이 기간 동안 보안 연결이 불가능해지면 HSTS를 적용하는 브라우저는 문제가 해결되거나 브라우저의 최대 사용 기간이 만료될 때까지 ONTAP 웹 서비스에 대한 액세스를 허용하지 않습니다.

단계

1. HSTS를 비활성화하려면 다음을 사용하세요. `system services web modify` 명령:

```
system services web modify -hsts-enabled false
```

관련 정보

"RFC 6797 - HTTP 엄격한 전송 보안(HSTS)"

ONTAP 웹 서비스 액세스 문제 해결

구성 오류로 인해 웹 서비스 액세스 문제가 발생합니다. LIF, 방화벽 정책, 웹 프로토콜 엔진, 웹 서비스, 디지털 인증서를 확인하여 오류를 해결할 수 있습니다. 사용자 액세스 권한이 모두 올바르게 구성되어 있습니다.

다음 표는 웹 서비스 구성 오류를 식별하고 해결하는 데 도움이 됩니다.

이 액세스 문제는...	이 구성 오류로 인해 발생합니다.	오류를 해결하려면...
웹 서비스에 액세스하려고 하면 웹 브라우저에서 "연결할 수 없음" 또는 "연결 실패" 오류가 반환됩니다.	LIF가 잘못 구성될 수 있습니다.	웹 서비스를 제공하는 LIF를 ping할 수 있는지 확인합니다. 명령을 사용하여 `network ping` LIF를 ping할 수 있습니다.
방화벽이 잘못 구성되었을 수 있습니다.	HTTP 또는 HTTPS를 지원하도록 방화벽 정책을 설정하고 웹 서비스를 제공하는 LIF에 정책이 할당되도록 합니다. '시스템 서비스 방화벽 정책' 명령을 사용하여 방화벽 정책을 관리합니다. 'network interface modify' 명령을 '-firewall-policy' 매개 변수와 함께 사용하여 정책을 LIF와 연결합니다.	웹 프로토콜 엔진이 비활성화되었을 수 있습니다.

이 액세스 문제는...	이 구성 오류로 인해 발생합니다.	오류를 해결하려면...
웹 서비스에 액세스할 수 있도록 웹 프로토콜 엔진이 활성화되어 있는지 확인합니다. '시스템 서비스 웹' 명령을 사용하여 클러스터의 웹 프로토콜 엔진을 관리합니다.	웹 서비스에 액세스하려고 하면 웹 브라우저에서 "찾을 수 없음" 오류가 반환됩니다.	웹 서비스가 비활성화되었을 수 있습니다.
액세스를 허용할 각 웹 서비스가 개별적으로 설정되어 있는지 확인합니다. 'vserver services web modify' 명령을 사용하여 액세스를 위한 웹 서비스를 활성화할 수 있습니다.	웹 브라우저가 사용자의 계정 이름 및 암호를 사용하여 웹 서비스에 로그인하지 못합니다.	사용자를 인증할 수 없거나, 액세스 방법이 올바르지 않거나, 사용자가 웹 서비스에 액세스할 수 있는 권한이 없습니다.
사용자 계정이 존재하고 올바른 액세스 방법 및 인증 방법으로 구성되었는지 확인합니다. 또한 사용자의 역할이 웹 서비스에 액세스할 수 있는 권한이 있는지 확인합니다. '보안 로그인' 명령어를 이용하여 사용자 계정과 접속 방법 및 인증 방식을 관리할 수 있다. ONTAP API 웹 서비스에 액세스하려면 "ontapi" 액세스 방법이 필요합니다. 다른 모든 웹 서비스에 액세스하려면 http 접근 방식이 필요합니다. 'vserver services web access' 명령을 사용하여 웹 서비스에 대한 역할의 액세스를 관리합니다.	HTTPS를 사용하여 웹 서비스에 연결하면 웹 브라우저에서 연결이 중단되었음을 나타냅니다.	웹 서비스를 제공하는 클러스터 또는 SVM(스토리지 가상 머신)에서 SSL을 사용하지 못할 수 있습니다.

이 액세스 문제는...	이 구성 오류로 인해 발생합니다.	오류를 해결하려면...
클러스터 또는 SVM에 SSL이 활성화되어 있고 디지털 인증서가 유효한지 확인합니다. 'Security SSL' 명령어를 이용하여 HTTP 서버의 SSL 설정을 관리하고 'Security certificate show' 명령어를 이용하여 디지털 인증서 정보를 출력한다.	HTTPS를 사용하여 웹 서비스에 연결하면 웹 브라우저에서 연결을 신뢰할 수 없음을 나타냅니다.	자체 서명된 디지털 인증서를 사용 중일 수 있습니다.

관련 정보

- "ONTAP 의 네트워크 구성에 대한 모범 사례는 무엇입니까?"
- "네트워크 Ping"
- "네트워크 인터페이스 수정"
- "보안 인증서 생성 - CSR"
- "보안 인증서 설치"
- "보안 인증서가 표시됩니다"
- "보안 SSL"

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 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.