인증 및 액세스 제어

ONTAP 9

NetApp
April 24, 2024

목차

인증 및 액세스 제어

인증 및 액세스 제어 개요

ONTAP 클러스터 인증과 ONTAP 웹 서비스에 대한 액세스 제어를 관리할 수 있습니다.

System Manager 또는 CLI를 사용하여 클러스터 및 스토리지에 대한 클라이언트 및 관리자 액세스를 제어하고 보호할 수 있습니다.

클래식 시스템 관리자(ONTAP 9.7 이전에서만 사용 가능)를 사용하는 경우 를 참조하십시오 "System Manager Classic(ONTAP 9.0 ~ 9.7)"

클라이언트 인증 및 권한 부여

ONTAP는 신뢰할 수 있는 소스로 ID를 확인하여 클라이언트 시스템과 사용자를 인증합니다. ONTAP는 사용자의 자격 증명을 파일 또는 디렉터리에 구성된 권한과 비교하여 사용자가 파일 또는 디렉터리에 액세스할 수 있도록 승인합니다.

관리자 인증 및 **RBAC**

관리자는 로컬 또는 원격 로그인 계정을 사용하여 클러스터 및 스토리지 VM에 대한 자체 인증을 수행합니다. 역할 기반 액세스 제어(RBAC)는 관리자가 액세스할 수 있는 명령을 결정합니다.

관리자 인증 및 **RBAC** 관리

CLI를 사용한 관리자 인증 및 **RBAC** 개요

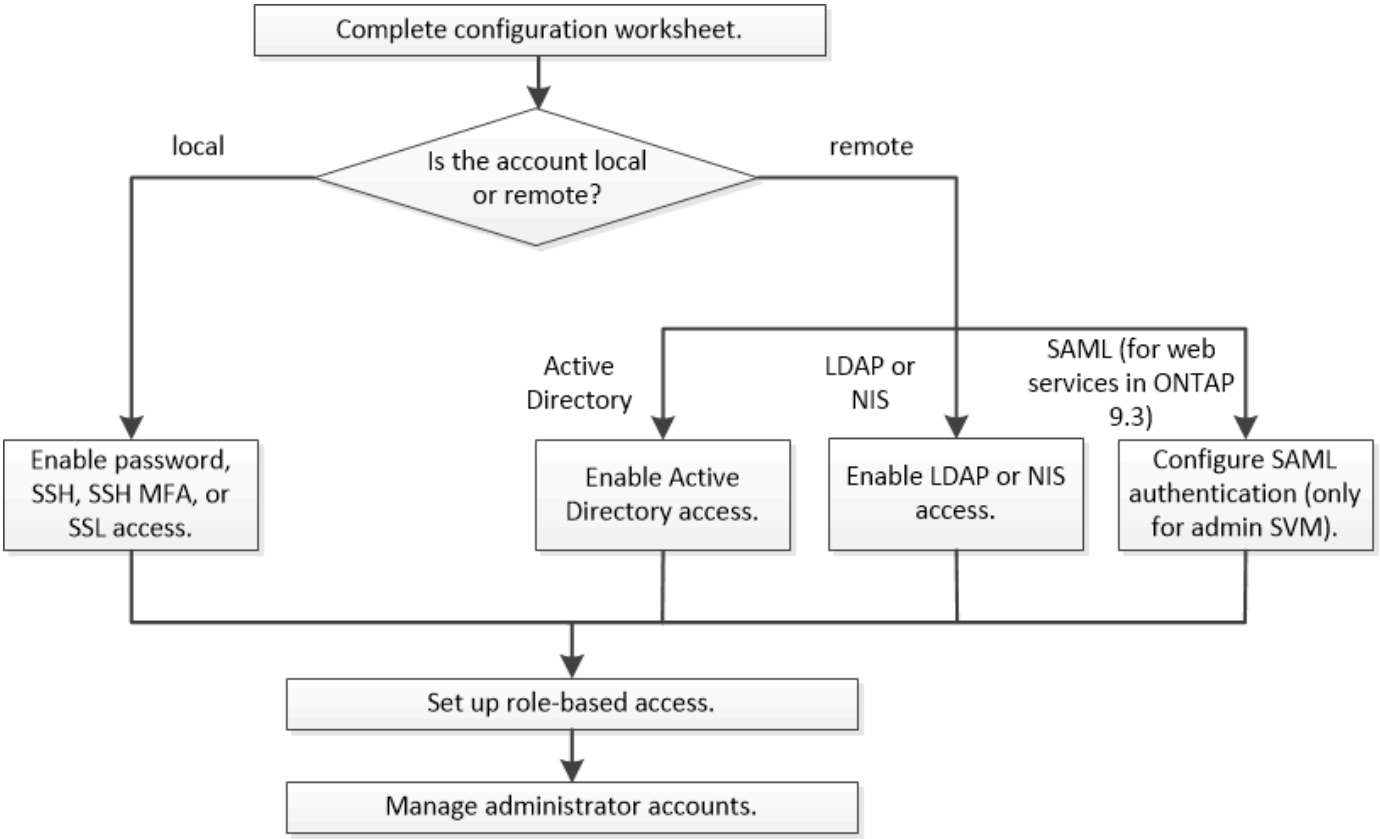
ONTAP 클러스터 관리자 및 SVM(스토리지 가상 시스템) 관리자의 로그인 계정을 활성화할 수 있습니다. 역할 기반 액세스 제어(RBAC)를 사용하여 관리자의 기능을 정의할 수도 있습니다.

다음과 같은 방법으로 로그인 계정 및 RBAC를 사용할 수 있습니다.

- System Manager나 자동화된 스크립팅 도구가 아니라 ONTAP CLI(Command-Line Interface)를 사용하려는 경우
- 사용 가능한 모든 옵션을 탐색하는 것이 아니라 모범 사례를 사용하려고 합니다.
- SNMP를 사용하여 클러스터에 대한 정보를 수집하지 않습니다.

관리자 인증 및 **RBAC** 워크플로

로컬 관리자 계정 또는 원격 관리자 계정에 대해 인증을 설정할 수 있습니다. 로컬 계정의 계정 정보는 스토리지 시스템에 있으며 원격 계정의 계정 정보는 다른 위치에 있습니다. 각 계정에는 미리 정의된 역할 또는 사용자 지정 역할이 있을 수 있습니다.



로컬 관리자 계정이 다음 유형의 인증을 통해 SVM(관리 스토리지 가상 시스템) 또는 데이터 SVM에 액세스할 수 있도록 설정할 수 있습니다.

- 암호
- SSH 공개 키
- SSL 인증서
- SSH 다단계 인증(MFA)

  ONTAP 9.3부터 암호 및 공개 키로 인증이 지원됩니다.

원격 관리자 계정에서 다음 인증 유형을 사용하여 관리 SVM 또는 데이터 SVM에 액세스할 수 있습니다.

- Active Directory를 클릭합니다
- SAML 인증(관리 SVM에만 해당)

  ONTAP 9.3부터 SAML(Security Assertion Markup Language) 인증은 서비스 프로세서 인프라, ONTAP API 또는 System Manager 웹 서비스를 사용하여 관리 SVM에 액세스하는 데 사용할 수 있습니다.

- ONTAP 9.4부터 SSH MFA를 LDAP 또는 NIS 서버의 원격 사용자에게 사용할 수 있습니다. nsswitch 및 공개 키를 사용한 인증이 지원됩니다.

관리자 인증 및 **RBAC** 구성을 위한 워크시트

로그인 계정을 생성하고 역할 기반 액세스 제어(RBAC)를 설정하기 전에 구성 워크시트의 각 항목에 대한 정보를 수집해야 합니다.

로그인 계정을 만들거나 수정합니다

이러한 값은 에 제공됩니다 `security login create` 스토리지 VM에 액세스하기 위해 로그인 계정을 설정할 때 명령을 실행합니다. 에 동일한 값을 제공합니다 `security login modify` 계정이 스토리지 VM에 액세스하는 방법을 수정할 때 명령입니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	계정이 액세스하는 스토리지 VM의 이름입니다. 기본값은 클러스터에 대한 admin 스토리지 VM의 이름입니다.	
'-user-or-group-name'입니다	계정의 사용자 이름 또는 그룹 이름입니다. 그룹 이름을 지정하면 그룹의 각 사용자에 액세스할 수 있습니다. 사용자 이름 또는 그룹 이름을 여러 응용 프로그램과 연결할 수 있습니다.	
'-응용 프로그램'	스토리지 VM에 액세스하는 데 사용되는 애플리케이션: • http입니다 • ontapi • 'NMP'입니다 • "쉬"	
'-AuthMethod'입니다	계정을 인증하는 데 사용되는 메소드: • SSL 인증서 인증용 인증서 • Active Directory 인증을 위한 "domain"입니다 • LDAP 또는 NIS 인증을 위한 nsswitch입니다 • 사용자 비밀번호 인증용 비밀번호 • 공개 키 인증을 위한 공개 키 • SNMP 커뮤니티 문자열을 위한 커뮤니티 • SNMP 사용자 보안 모델을 위한 USM • SAML(Security Assertion Markup Language) 인증 시 'AML	

'-remote-switch-ipaddress'	원격 스위치의 IP 주소입니다. 원격 스위치는 CSMM(Cluster Switch Health Monitor)에서 모니터링하는 클러스터 스위치이거나 MCC-HM(MetroCluster Health Monitor)에서 모니터링하는 FC(Fibre Channel) 스위치일 수 있습니다. 이 옵션은 애플리케이션이 NMP에 있고 인증 방법이 USM 일 때만 적용됩니다.	
'-역할'	계정에 할당된 액세스 제어 역할: • 클러스터(관리자 스토리지 VM)의 경우 기본값은 입니다 `admin`. • 데이터 스토리지 VM의 경우 기본값은 입니다 `vsadmin`.	
``논평’	(선택 사항) 계정에 대한 설명 텍스트입니다. 텍스트는 큰따옴표(")로 묶어야 합니다.	
'-is-ns-switch-group'	계정이 LDAP 그룹 계정인지 NIS 그룹 계정인지 여부('예' 또는 '아니요')	
두 번째 인증 방법	다단계 인증의 경우 두 번째 인증 방법: • "없음" 다단계 인증을 사용하지 않으면 기본값이 됩니다 • AuthMethod가 password 또는 nsswitch 일 때 공개 키 인증을 위한 공개 키 • 'AuthMethod’가 공개 키일 때 사용자 암호 인증을 위한 'password’입니다 • AuthMethod가 publickey 일 때 사용자 암호 인증을 위한 nsswitch 인증 순서는 항상 공개 키와 암호 순서로 표시됩니다.	

'-is-ldap-fastbind'	ONTAP 9.11.1부터 true로 설정하면 nsswitch 인증에 대한 LDAP 고속 바인딩이 설정됩니다. 기본값은 false 입니다. LDAP fast bind를 사용하려면 '-authentication-method' 값을 nsswitch로 설정해야 한다. "nsswitch 인증을 위한 LDAP fastbind에 대해 알아봅니다."	

Cisco Duo 보안 정보를 구성합니다

이러한 값은 에 제공됩니다 `security login duo create` 스토리지 VM에 대해 SSH 로그인으로 Cisco Duo 2단계 인증을 사용하도록 설정하는 명령입니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	Duo 인증 설정이 적용되는 스토리지 VM(ONTAP CLI에서 가상 서버라고도 함)	
`-integration-key`	Duo에 SSH 애플리케이션을 등록할 때 얻은 통합 키입니다.	
`-secret-key`	Duo에 SSH 애플리케이션을 등록할 때 얻은 비밀 키입니다.	
`-api-host`	Duo에 SSH 애플리케이션을 등록할 때 얻은 API 호스트 이름입니다. 예를 들면 다음과 같습니다. `api-<HOSTNAME>.duosecurity.com`	
`-fail-mode`	Duo 인증을 방해하는 서비스 또는 구성 오류 발생 시 실패합니다 `safe` (액세스 허용) 또는 `secure` (액세스 거부). 기본값은 입니다 `safe`즉, Duo API 서버에 액세스할 수 없는 등의 오류로 인해 Duo 인증이 실패할 경우 Duo 인증이 무시됩니다.	

`-http-proxy`	지정된 HTTP 프록시를 사용합니다. HTTP 프록시에 인증이 필요한 경우 프록시 URL에 자격 증명을 포함합니다. 예를 들면 다음과 같습니다. `http-proxy=http://username:password@proxy.example.org:8080`	
`-autopush`	둘 다 가능합니다 `true` 또는 `false`. 기본값은 입니다 `false`. If(경우 `true`, Duo는 푸시 로그인 요청을 사용자의 전화기로 자동으로 전송하여 푸시 기능을 사용할 수 없는 경우 전화 통화로 되돌립니다. 이렇게 하면 암호 인증이 효과적으로 비활성화됩니다. If(경우 `false`인증 방법을 선택하라는 메시지가 표시됩니다. 를 사용하여 구성 시 `autopush = true`, 설정하는 것이 좋습니다 `max-prompts = 1`.	
`-max-prompts`	사용자가 두 번째 요소로 인증하지 못하면 Duo는 사용자에게 다시 인증하라는 메시지를 표시합니다. 이 옵션은 액세스를 거부하기 전에 Duo가 표시하는 최대 프롬프트 수를 설정합니다. 이어야 합니다 `1`, `2`, 또는 `3`. 기본값은 입니다 `1`. 예를 들어, When `max-prompts = 1`, 사용자가 첫 번째 프롬프트에서 성공적으로 인증해야 하는 반면 IF `max-prompts = 2`초기 프롬프트에서 잘못된 정보를 입력하면 다시 인증하라는 메시지가 표시됩니다. 를 사용하여 구성 시 `autopush = true`, 설정하는 것이 좋습니다 `max-prompts = 1`. 최상의 경험을 위해 공개 키 인증만 있는 사용자는 항상 을(를) 가질 수 있습니다 `max-prompts` 를 로 설정합니다 `1`.	

`-enabled`	Duo 이중 인증을 활성화합니다. 를 로 설정합니다 `true` 기본적으로 사용됩니다. 활성화되면 구성된 매개변수에 따라 SSH 로그인 중에 Duo 이중 인증이 적용됩니다. Duo가 비활성화된 경우(로 설정 `false`), Duo 인증은 무시됩니다.	

사용자 지정 역할을 정의합니다

사용자 지정 역할을 정의할 때 이러한 값에 '보안 로그인 역할 생성' 명령을 제공합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	(선택 사항) 역할과 연결된 스토리지 VM(ONTAP CLI에서 가상 서버라고 함)의 이름입니다.	
'-역할'	역할의 이름입니다.	
'-cmddirname'입니다	역할이 액세스를 제공하는 명령 또는 명령 디렉토리입니다. 명령 하위 디렉터리 이름은 큰따옴표(")로 묶어야 합니다. 예를 들어 ""볼륨 스냅샷""을 입력합니다. 모든 명령 디렉토리를 지정하려면 'default'를 입력해야 합니다.	

'-액세스'	(선택 사항) 역할에 대한 액세스 수준입니다. 명령 디렉토리의 경우: • "없음"(사용자 지정 역할의 기본값)은 명령 디렉토리의 명령에 대한 액세스를 거부합니다 • '재만'은 명령 디렉토리와 하위 디렉토리에 있는 'show' 명령에 대한 액세스 권한을 부여합니다 • ALL은 명령 디렉토리와 하위 디렉토리에 있는 모든 명령에 대한 액세스 권한을 부여합니다 비내장 명령어 _ (create, modify, delete, sHow로 끝내지 않는 명령어): • "없음"(사용자 지정 역할의 기본값)은 명령에 대한 액세스를 거부합니다 • "재담만"은 적용할 수 없습니다 • 모두 명령을 사용할 수 있는 권한을 부여합니다 내장 명령에 대한 액세스를 부여하거나 거부하려면 명령 디렉터리를 지정해야 합니다.	
'-query'	(선택 사항) 명령 또는 명령 디렉터리의 명령에 대해 유효한 옵션 형식으로 지정된 액세스 수준을 필터링하는 데 사용되는 쿼리 개체입니다. 쿼리 개체는 큰따옴표 (")로 묶어야 합니다. 예를 들어, 명령 디렉토리가 "volume"이면 쿼리 객체 "-aggr0"은 "aggr0" 집합에만 액세스를 활성화합니다.	

공개 키를 사용자 계정에 연결합니다

SSH 공개 키를 사용자 계정에 연결할 때 이 값을 '보안 로그인 공개 키 생성' 명령과 함께 제공합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	(선택 사항) 계정이 액세스하는 스토리지 VM의 이름입니다.	

'-사용자 이름'	계정의 사용자 이름입니다. 기본값인 admin은 클러스터 관리자의 기본 이름입니다.	
``인덱스’	공개 키의 인덱스 번호입니다. 이 키가 계정에 대해 만들어진 첫 번째 키인 경우 기본값은 0이고, 그렇지 않은 경우 기본값은 해당 계정의 기존 인덱스 번호가 가장 높은 값보다 하나 더 큽니다.	
'-공개 키'	OpenSSH 공개 키입니다. 키를 큰따옴표(")로 묶어야 합니다.	
'-역할'	계정에 할당된 액세스 제어 역할입니다.	
``논평’	(선택 사항) 공개 키에 대한 설명 텍스트입니다. 텍스트는 큰따옴표(")로 묶어야 합니다.	
`-x509-certificate`	(선택 사항) ONTAP 9.13.1 부터는 SSH 공개 키와 X.509 인증서 연결을 관리할 수 있습니다. X.509 인증서를 SSH 공개 키와 연결하면 ONTAP는 SSH 로그인 시 이 인증서가 유효한지 확인합니다. 만료되었거나 해지된 경우 로그인이 허용되지 않고 연결된 SSH 공개 키가 비활성화됩니다. 가능한 값: • `install`: 지정된 PEM 인코딩된 X.509 인증서를 설치하고 SSH 공개 키와 연결합니다. 설치할 인증서의 전체 텍스트를 포함합니다. • `modify`: 기존 PEM 인코딩된 X.509 인증서를 지정된 인증서와 업데이트하고 SSH 공개 키에 연결합니다. 새 인증서의 전체 텍스트를 포함합니다. • `delete`: SSH 공개 키와 기존 X.509 인증서 연결을 제거합니다.	

CA 서명 서버 디지털 인증서를 설치합니다

이러한 값은 에 제공됩니다 `security certificate generate-csr` 스토리지 VM을 SSL 서버로 인증하는 데 사용할 디지털 인증서 서명 요청(CSR)을 생성하는 명령

필드에 입력합니다	설명	귀사의 가치
'-common-name'입니다	정규화된 도메인 이름(FQDN) 또는 사용자 지정 일반 이름인 인증서의 이름입니다.	
'-size'	개인 키의 비트 수입니다. 값이 클수록 키가 더 안전합니다. 기본값은 2048입니다. 가능한 값은 512, 1024, 1536, 2048입니다.	
``국가'	스토리지 VM의 국가로, 2자로 된 코드입니다. 기본값은 입니다 `US`. 코드 목록은 man 페이지를 참조하십시오.	
``상태''	스토리지 VM의 시/도입니다.	
``지역성''	스토리지 VM의 인접성	
``조직''	스토리지 VM의 조직입니다.	
``단위''	스토리지 VM 조직의 단위입니다.	
'-email-addr'	스토리지 VM에 대한 담당자 관리자의 e-메일 주소입니다.	
``해쉬-함수''	인증서 서명을 위한 암호화 해싱 기능 기본값은 'HA256'입니다. 가능한 값은 'HA1', 'HA256', 'MD5'입니다.	

이러한 값은 에 제공됩니다 `security certificate install` 클러스터 또는 스토리지 VM을 SSL 서버로 인증하는 데 사용할 CA 서명 디지털 인증서를 설치할 때 사용하는 명령입니다. 다음 표에는 계정 구성과 관련된 옵션만 나와 있습니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	인증서를 설치할 스토리지 VM의 이름입니다.	

``유형''	인증서 유형: • 서버 인증서 및 중간 인증서에 대한 서버 • SSL 클라이언트의 루트 CA의 공개 키 인증서에 대한 client-ca • ONTAP가 클라이언트인 SSL 서버의 루트 CA의 공개 키 인증서에 대한 서버-카 • SSL 클라이언트로서 ONTAP의 자체 서명 또는 CA 서명 디지털 인증서 및 개인 키용 '클라이언트'	

Active Directory 도메인 컨트롤러 액세스를 구성합니다

이러한 값은 에 제공됩니다 `security login domain-tunnel create` 데이터 스토리지 VM에 사용할 SMB 서버를 이미 구성한 상태에서 스토리지 VM을 게이트웨이로 구성하거나 클러스터에 대한 Active Directory 도메인 컨트롤러 액세스를 위해 _tunnel_을 구성하려는 경우에 명령을 실행합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	SMB 서버가 구성된 스토리지 VM의 이름입니다.	

이러한 값은 에 제공됩니다 `vserver active-directory create` SMB 서버를 구성하지 않은 상태에서 Active Directory 도메인에 스토리지 VM 컴퓨터 계정을 생성하려는 경우 명령

필드에 입력합니다	설명	귀사의 가치
'-vserver'	Active Directory 컴퓨터 계정을 생성할 스토리지 VM의 이름입니다.	
'-계정-이름'	컴퓨터 계정의 NetBIOS 이름입니다.	
``도메인’	FQDN(정규화된 도메인 이름)입니다.	
'-ou'	도메인의 조직 단위입니다. 기본값은 CN=Computers입니다. ONTAP는 이 값을 도메인 이름에 더하여 Active Directory 고유 이름을 생성합니다.	

LDAP 또는 **NIS** 서버 액세스를 구성합니다

이러한 값은 에 제공됩니다 `vserver services name-service ldap client create` 명령을 사용하여 스토리지 VM에 대한 LDAP 클라이언트 구성을 생성할 수 있습니다.

다음 표에는 계정 구성과 관련된 옵션만 나와 있습니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	클라이언트 구성에 대한 스토리지 VM의 이름입니다.	
'-client-config'입니다	클라이언트 구성의 이름입니다.	
'-LDAP-서버'	클라이언트가 연결되는 LDAP 서버의 IP 주소 및 호스트 이름을 쉼표로 구분하여 나열합니다.	
'-스키마'	클라이언트가 LDAP 쿼리를 만드는 데 사용하는 스키마입니다.	
'-use-start-tls'	클라이언트가 Start TLS를 사용하여 LDAP 서버와의 통신을 암호화하는지 여부("true" 또는 "false") TLS 시작은 데이터 스토리지 VM에 대한 액세스에만 지원됩니다. 관리자 스토리지 VM에 대한 액세스는 지원되지 않습니다.	

이러한 값은 에 제공됩니다 `vserver services name-service ldap create` LDAP 클라이언트 구성을 스토리지 VM에 연결하는 명령입니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	클라이언트 구성을 연결할 스토리지 VM의 이름입니다.	
'-client-config'입니다	클라이언트 구성의 이름입니다.	
'-client-enabled'	스토리지 VM이 LDAP 클라이언트 구성을 사용할 수 있는지 여부를 나타냅니다 (`true` 또는 `false`)를 클릭합니다.	

이러한 값은 에 제공됩니다 `vserver services name-service nis-domain create` 명령을 사용하여 스토리지 VM에 NIS 도메인 구성을 생성할 수 있습니다.

필드에 입력합니다	설명	귀사의 가치

'-vserver'	도메인 구성을 생성할 스토리지 VM의 이름입니다.	
``도메인’	도메인의 이름입니다.	
'-활성'	도메인이 활성 상태인지('true' 또는 'false') 여부	
'-서버'	• ONTAP 9.0, 9.1 *: 도메인 구성에 사용되는 NIS 서버의 IP 주소 목록을 쉼표로 구분하여 표시합니다.	
'-NIS-서버'	도메인 구성에 사용되는 NIS 서버의 IP 주소 및 호스트 이름을 쉼표로 구분된 목록입니다.	

이름 서비스 소스에 대한 조회 순서를 지정할 때 이러한 값을 'vserver services name-service ns-switch create' 명령과 함께 제공합니다.

필드에 입력합니다	설명	귀사의 가치
'-vserver'	이름 서비스 조회 순서를 구성할 스토리지 VM의 이름입니다.	
'-데이터베이스'	네임 서비스 데이터베이스: • 파일 및 DNS 이름 서비스를 위한 호스트 • 파일, LDAP, NIS 이름 서비스에 대한 그룹 • 파일, LDAP 및 NIS 이름 서비스의 'passwd' • 파일, LDAP 및 NIS 이름 서비스에 대한 넷그룹 • 파일 및 LDAP 이름 서비스에 대한 이름 맵	
``근원’’	쉼표로 구분된 목록에서 이름 서비스 소스를 조회하는 순서: • '파일' • 드문들 • "LDAP" • 국정원	

SAML 액세스를 구성합니다

ONTAP 9.3부터는 SAML 인증을 구성하기 위해 'Security SAML-SP create' 명령을 사용하여 이러한 값을 제공합니다.

필드에 입력합니다	설명	귀사의 가치
'-IDP-Uri'	IDP 메타데이터를 다운로드할 수 있는 IDP(Identity Provider) 호스트의 FTP 주소 또는 HTTP 주소입니다.	
``SP-HOST''	SAML 서비스 공급자 호스트(ONTAP 시스템)의 호스트 이름 또는 IP 주소입니다. 기본적으로 클러스터 관리 LIF의 IP 주소가 사용됩니다.	
`-cert-ca` 및 `-cert-serial`, 또는 `-cert-common-name`	서비스 공급자 호스트(ONTAP 시스템)의 서버 인증서 세부 정보입니다. 서비스 공급자의 CA(인증 기관)와 인증서의 일련 번호 또는 서버 인증서 공통 이름을 입력할 수 있습니다.	
'-verify-metadata-server'	IDP 메타데이터 서버의 ID를 검증해야 하는지 여부('true' 또는 'false'). 가장 좋은 방법은 이 값을 항상 TRUE로 설정하는 것입니다.	

로그인 계정을 만듭니다

로그인 계정 생성 개요

로컬 또는 원격 클러스터 및 SVM 관리자 계정을 활성화할 수 있습니다. 로컬 계정은 계정 정보, 공개 키 또는 보안 인증서가 스토리지 시스템에 상주하는 계정입니다. AD 계정 정보는 도메인 컨트롤러에 저장됩니다. LDAP 및 NIS 계정은 LDAP 및 NIS 서버에 상주합니다.

클러스터 및 **SVM** 관리자

클러스터 관리자는 _ 클러스터에 대한 admin SVM에 액세스합니다. 클러스터 설정 시 admin이라는 예약 이름의 클러스터 관리자와 SVM 관리자가 자동으로 생성됩니다.

기본 'admin' 역할을 가진 클러스터 관리자는 전체 클러스터와 리소스를 관리할 수 있습니다. 클러스터 관리자는 필요에 따라 서로 다른 역할을 가진 추가 클러스터 관리자를 생성할 수 있습니다.

SVM 관리자는 _ 데이터 SVM에 액세스합니다. 클러스터 관리자가 필요에 따라 데이터 SVM 및 SVM 관리자를 생성합니다.

SVM 관리자는 기본적으로 'vsadmin' 역할이 할당됩니다. 클러스터 관리자는 필요에 따라 SVM 관리자에게 다양한 역할을 할당할 수 있습니다.

명명 규칙

다음 일반 이름은 원격 클러스터 및 SVM 관리자 계정에 사용할 수 없습니다.

- "아담"
- "출력함"
- "CLI"
- "데몬"
- "FTP"
- "게임"
- "중지"
- "lp"
- "메일"
- "남자"
- "나루트"
- "NetApp"
- "뉴스"
- "없음"
- "연산자"
- "루트"
- "종료"
- "sshd"
- "동기화"
- "시스템"
- "우프"
- "www"

병합된 역할

동일한 사용자에 대해 여러 원격 계정을 사용하도록 설정하면 계정에 지정된 모든 역할의 조합이 사용자에게 할당됩니다. 즉, LDAP 또는 NIS 계정에 vsadmin 역할이 할당되고 같은 사용자의 AD 그룹 계정에 vsadmin-volume 역할이 할당되면 AD 사용자는 보다 포괄적인 vsadmin 기능으로 로그인합니다. 역할은 _ 병합 _ 이라고 합니다.

로컬 계정 액세스를 설정합니다

로컬 계정 액세스 개요를 활성화합니다

로컬 계정은 계정 정보, 공개 키 또는 보안 인증서가 스토리지 시스템에 상주하는 계정입니다. 'Security login create' 명령을 사용하여 로컬 계정에서 admin 또는 data SVM에 액세스할 수 있습니다.

암호 계정 액세스를 활성화합니다

'Security login create' 명령을 사용하면 관리자 계정에서 admin 또는 data SVM에 암호를 사용하여 액세스할 수 있습니다. 명령을 입력하면 암호를 묻는 메시지가 표시됩니다.

이 작업에 대해

로그인 계정에 할당할 액세스 제어 역할을 잘 모르는 경우 '보안 로그인 수정' 명령을 사용하여 나중에 역할을 추가할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 로컬 관리자 계정에서 암호를 사용하여 SVM에 액세스:

   security login create -vserver *SVM_name* -user-or-group-name *user_or_group_name* -application *application* -authmethod *authentication_method* -role *role* -comment *comment*

   전체 명령 구문은 을 참조하십시오 "워크시트".

   다음 명령을 사용하면 미리 정의된 백업 역할을 가진 클러스터 관리자 계정 admin1이 암호를 사용하여 SVM "engCluster"에 액세스할 수 있습니다. 명령을 입력하면 암호를 묻는 메시지가 표시됩니다.

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name
   admin1 -application ssh -authmethod password -role backup
   ```

SSH 공개 키 계정을 활성화합니다

'Security login create' 명령을 사용하면 관리자 계정이 SSH 공개 키로 admin 또는 data SVM에 액세스할 수 있습니다.

이 작업에 대해

- 계정이 SVM에 액세스하려면 먼저 공개 키를 계정에 연결해야 합니다.

  공개 키를 사용자 계정과 연결

  계정 액세스를 활성화하기 전이나 후에 이 작업을 수행할 수 있습니다.

- 로그인 계정에 할당할 액세스 제어 역할을 잘 모르는 경우 '보안 로그인 수정' 명령을 사용하여 나중에 역할을 추가할 수 있습니다.

클러스터에서 FIPS 모드를 활성화하려면 지원되는 키 알고리즘이 없는 기존 SSH 공개 키 계정을 지원되는 키 유형으로 재구성해야 합니다. FIPS를 사용하도록 설정하기 전에 계정을 다시 구성해야 하며 그렇지 않으면 관리자 인증이 실패합니다.

다음 표에는 ONTAP SSH 연결에 지원되는 호스트 키 유형 알고리즘이 나와 있습니다. 이러한 키 유형은 SSH 공개 인증 구성에 적용되지 않습니다.

ONTAP 릴리즈	FIPS 모드에서 지원되는 키 유형입니다	FIPS 이외의 모드에서 지원되는 키 유형입니다
9.11.1 이상	ECDSA-SHA2-nistp256	ECDSA-SHA2-nistp256+RSA-SHA2-512+RSA-SHA2-256+ssh-ed25519+ssh-dss+ssh-ssh-rsa
9.10.1 이하	ECDSA-SHA2-nistp256+ssh-ed25519	ECDSA-SHA2-nistp256+ssh-ed25519+ssh-dss+ssh-rsa

ONTAP 9.11.1부터 ssh-ed25519 호스트 키 알고리즘에 대한 지원이 제거되었습니다.

자세한 내용은 을 참조하십시오 "FIPS를 사용하여 네트워크 보안을 구성합니다".

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 로컬 관리자 계정이 SSH 공개 키를 사용하여 SVM에 액세스할 수 있도록 합니다.

   '보안 로그인 생성 - vserver_SVM_name_-user-or-group-name user_or_group_name-application_application_-AuthMethod_authentication_method_-role_role_-comment_comment_'

   전체 명령 구문은 을 참조하십시오 "워크시트".

   다음 명령을 실행하면 SSH 공개 키를 사용하여 SVM "engData1"에 액세스할 수 있도록 사전 정의된 "vsadmin-volume" 역할이 있는 SVM 관리자 계정의 vmadmin1이 활성화됩니다.

   ```
   cluster1::>security login create -vserver engData1 -user-or-group-name
   svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
   ```

작업을 마친 후

공개 키를 관리자 계정에 연결하지 않은 경우, 계정이 SVM에 액세스하려면 먼저 연결해야 합니다.

공개 키를 사용자 계정과 연결

다단계 인증**(MFA)** 계정 활성화

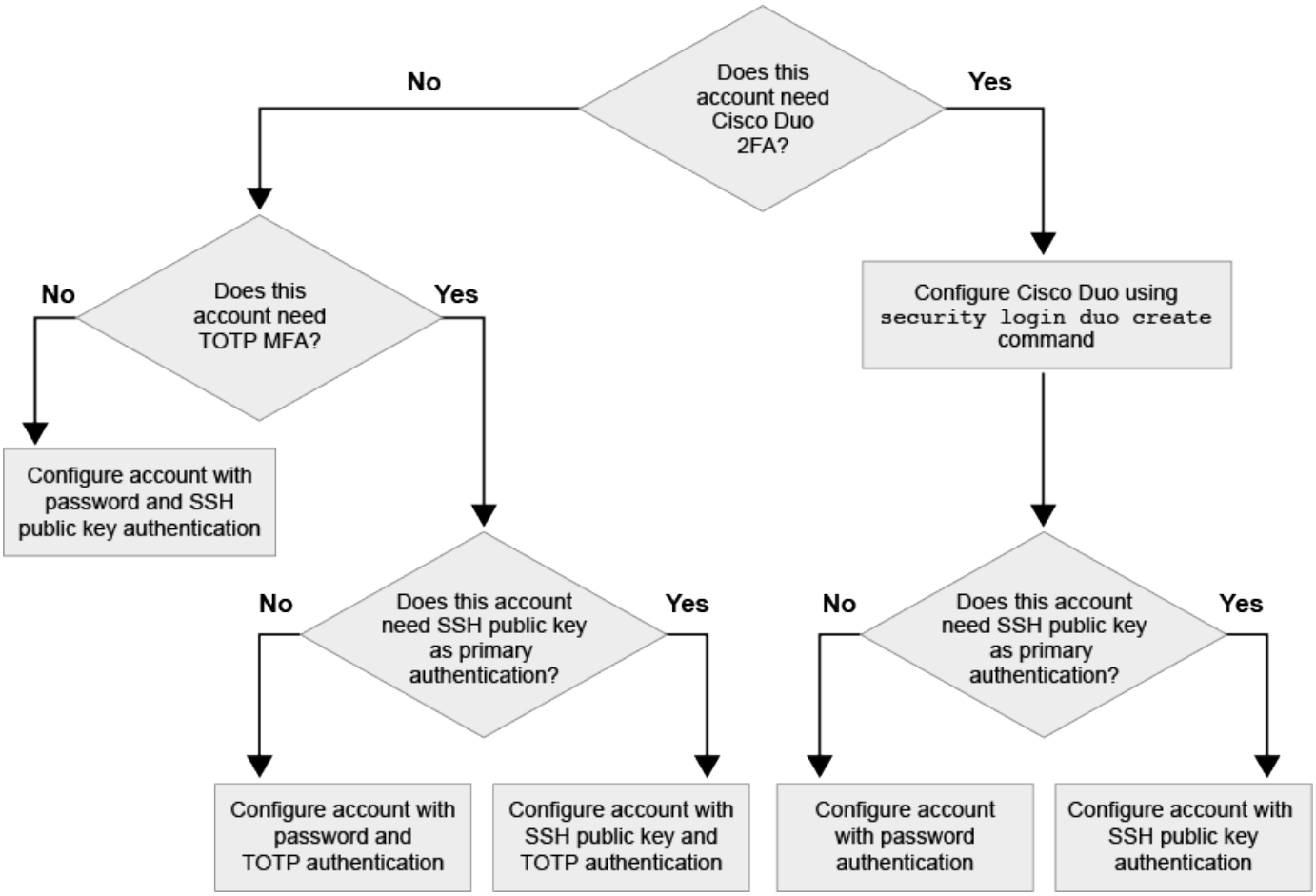
다단계 인증 개요

다단계 인증(MFA)을 사용하면 사용자에게 관리자 또는 데이터 스토리지 VM에 로그인하기 위한 두 가지 인증 방법을 제공하도록 요구하여 보안을 강화할 수 있습니다.

ONTAP 버전에 따라 다단계 인증을 위해 SSH 공개 키, 사용자 암호 및 시간 기반 TOTP(일회성 암호)를 함께 사용할 수 있습니다. Cisco Duo(ONTAP 9.14.1 이상)를 활성화 및 구성하면 모든 사용자에 대한 기존 방법을 보완하는 추가 인증 방법으로 사용됩니다.

다음으로 시작...	첫 번째 인증 방법입니다	두 번째 인증 방법입니다
ONTAP 9.14.1	SSH 공개 키	토TP
	사용자 암호	토TP
	SSH 공개 키	Cisco 듀오
	사용자 암호입니다	Cisco 듀오
ONTAP 9.13.1	SSH 공개 키	토TP
	사용자 암호입니다	토TP
ONTAP 9.3	SSH 공개 키	사용자 암호입니다

MFA가 구성된 경우 클러스터 관리자가 먼저 로컬 사용자 계정을 사용하도록 설정한 다음 로컬 사용자가 계정을 구성해야 합니다.



다단계 인증 을 활성화합니다

다단계 인증(MFA)을 사용하면 사용자가 admin 또는 data SVM에 로그인하기 위한 두 가지 인증 방법을 제공하도록 요구하여 보안을 강화할 수 있습니다.

이 작업에 대해

- 이 작업을 수행하려면 클러스터 관리자여야 합니다.

- 로그인 계정에 할당할 액세스 제어 역할을 잘 모르는 경우 '보안 로그인 수정' 명령을 사용하여 나중에 역할을 추가할 수 있습니다.

  "관리자에게 할당된 역할 수정"

- 인증을 위해 공개 키를 사용하는 경우, 계정이 SVM에 액세스하려면 먼저 공개 키를 계정에 연결해야 합니다.

  "공개 키를 사용자 계정에 연결합니다"

  계정 액세스를 활성화하기 전이나 후에 이 작업을 수행할 수 있습니다.

- ONTAP 9.12.1부터 FIDO2(Fast Identity Online) 또는 PIV(Personal Identity Verification) 인증 표준을 사용하여 SSH 클라이언트 MFA에 Yubikey 하드웨어 인증 장치를 사용할 수 있습니다.

SSH 공개 키 및 사용자 암호로 **MFA**를 사용하도록 설정합니다

ONTAP 9.3부터 클러스터 관리자는 SSH 공개 키 및 사용자 암호를 사용하여 MFA로 로그인하도록 로컬 사용자 계정을 설정할 수 있습니다.

1. SSH 공개 키 및 사용자 암호를 사용하여 로컬 사용자 계정에서 MFA를 사용하도록 설정합니다.

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_name> -application ssh -authentication-method <password|publickey>
   -role admin -second-authentication-method <password|publickey>
   ```

   다음 명령을 수행하려면 미리 정의된 "admin" 역할을 가진 SVM 관리자 계정 "admin2"가 SSH 공개 키와 사용자 암호를 사용하여 SVM "engData1"에 로그인해야 합니다.

   ```
   cluster-1::> security login create -vserver engData1 -user-or-group-name
   admin2 -application ssh -authentication-method publickey -role admin
   -second-authentication-method password

   Please enter a password for user 'admin2':
   Please enter it again:
   Warning: To use public-key authentication, you must create a public key
   for user "admin2".
   ```

TOTP로 **MFA**를 활성화합니다

ONTAP 9.13.1 부터는 로컬 사용자가 SSH 공개 키 또는 사용자 암호와 TOTP(Time-Based One-Time Password)를 사용하여 admin 또는 data SVM에 로그인하도록 하여 보안을 강화할 수 있습니다. TOTP로 MFA에 대해 계정을 활성화한 후 로컬 사용자는 에 로그인해야 합니다 "구성을 완료합니다".

TOTP는 현재 시간을 사용하여 1회 암호를 생성하는 컴퓨터 알고리즘입니다. TOTP를 사용하는 경우 SSH 공개 키 또는 사용자 암호 뒤에 항상 두 번째 인증 형태입니다.

시작하기 전에

이러한 작업을 수행하려면 스토리지 관리자여야 합니다.

단계

사용자 암호 또는 SSH 공개 키를 사용하여 MFA를 에 설정하고 TOTP를 두 번째 인증 방법으로 설정할 수 있습니다.

사용자 암호 및 **TOTP**로 **MFA**를 활성화합니다

1. 사용자 암호 및 TOTP를 사용하여 다단계 인증을 위한 사용자 계정을 활성화합니다.

   - 신규 사용자 계정의 경우 *

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   - 기존 사용자 계정의 경우 *

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

2. TOTP로 MFA가 활성화되었는지 확인합니다.

   ```
   security login show
   ```

SSH 공개 키 및 **TOTP**로 **MFA**를 활성화합니다

1. SSH 공개 키 및 TOTP를 사용하여 다단계 인증을 위한 사용자 계정을 활성화합니다.

   - 신규 사용자 계정의 경우 *

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role>
   -comment <comment>
   ```

   - 기존 사용자 계정의 경우 *

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

2. TOTP로 MFA가 활성화되었는지 확인합니다.

```
security login show
```

작업을 마친 후

- 공개 키를 관리자 계정에 연결하지 않은 경우, 계정이 SVM에 액세스하려면 먼저 연결해야 합니다.

  "공개 키를 사용자 계정과 연결"

- TOTP로 MFA 구성을 완료하려면 로컬 사용자가 로그인해야 합니다.

  "TOTP로 MFA에 대한 로컬 사용자 계정을 구성합니다"

관련 정보

에 대해 자세히 알아보십시오 "ONTAP 9의 다단계 인증(TR-4647)".

TOTP로 **MFA**에 대한 로컬 사용자 계정을 구성합니다

ONTAP 9.13.1 부터는 TOTP(Time-Based One-Time Password)를 사용하여 MFA(Multifactor Authentication)로 사용자 계정을 구성할 수 있습니다.

시작하기 전에

- 스토리지 관리자는 을(를) 사용해야 합니다 "TOTP로 MFA를 활성화합니다" 사용자 계정에 대한 두 번째 인증 방법입니다.
- 기본 사용자 계정 인증 방법은 사용자 암호 또는 공용 SSH 키여야 합니다.
- TOTP 앱이 스마트폰과 연동되도록 구성하고 TOTP 비밀 키를 만들어야 합니다.

  TOTP는 Google Authenticator와 같은 다양한 인증 앱에서 지원됩니다.

단계

1. 현재 인증 방법으로 사용자 계정에 로그인합니다.

   현재 인증 방법은 사용자 암호 또는 SSH 공개 키여야 합니다.

2. 계정에 TOTP 구성을 생성합니다.

   ```
   security login totp create -vserver "<svm_name>" -username
   "<account_username >"
   ```

3. TOTP 구성이 계정에서 활성화되어 있는지 확인합니다.

   ```
   security login totp show -vserver "<svm_name>" -username
   "<account_username>"
   ```

TOTP 비밀 키를 재설정합니다

계정 보안을 보호하려면 TOTP 비밀 키가 손상되었거나 손실된 경우 이를 비활성화하고 새 키를 만들어야 합니다.

키가 손상된 경우 **TOTP**를 재설정합니다

TOTP 비밀 키가 손상되었지만 여전히 액세스할 수 있는 경우 손상된 키를 제거하고 새 키를 만들 수 있습니다.

1. 사용자 암호 또는 SSH 공개 키 및 손상된 TOTP 비밀 키를 사용하여 사용자 계정에 로그인합니다.
2. 손상된 TOTP 암호 키를 제거합니다.

```
security login totp delete -vserver <svm_name> -username
<account_username>
```

3. 새 TOTP 암호 키 생성:

```
security login totp create -vserver <svm_name> -username
<account_username>
```

4. TOTP 구성이 계정에서 활성화되어 있는지 확인합니다.

```
security login totp show -vserver <svm_name> -username
<account_username>
```

키를 분실한 경우 **TOTP**를 재설정합니다

TOTP 암호 키가 분실된 경우 스토리지 관리자에게 문의하십시오 "키를 사용하지 않도록 설정합니다". 키를 비활성화한 후 첫 번째 인증 방법을 사용하여 새 TOTP에 로그인하고 구성할 수 있습니다.

시작하기 전에

TOTP 암호 키는 스토리지 관리자가 해제해야 합니다. 저장소 관리자 계정이 없는 경우 저장소 관리자에게 문의하여 키를 사용하지 않도록 설정합니다.

단계

1. 스토리지 관리자가 TOTP 암호를 비활성화한 후 기본 인증 방법을 사용하여 로컬 계정에 로그인합니다.
2. 새 TOTP 암호 키 생성:

```
security login totp create -vserver <svm_name> -username
<account_username >
```

3. TOTP 구성이 계정에서 활성화되어 있는지 확인합니다.

```
security login totp show -vserver <svm_name> -username
<account_username>
```

로컬 계정에 대해 **TOTP** 암호 키를 비활성화합니다

로컬 사용자의 TOTP(Time-based One-Time Password) 비밀 키를 분실한 경우 저장소 관리자가 손실된 키를 비활성화해야 새 TOTP 비밀 키를 생성할 수 있습니다.

이 작업에 대해

이 작업은 클러스터 관리자 계정에서만 수행할 수 있습니다.

단계

1. TOTP 암호 키 비활성화:

```
security login totp delete -vserver "<svm_name>" -username
"<account_username>"
```

SSL 인증서 계정을 활성화합니다

'보안 로그인 생성' 명령을 사용하면 관리자 계정이 SSL 인증서를 통해 관리자 또는 데이터 SVM에 액세스할 수 있습니다.

이 작업에 대해

- 계정이 SVM에 액세스하려면 CA 서명 서버 디지털 인증서를 설치해야 합니다.

  CA 서명 서버 인증서 생성 및 설치

  계정 액세스를 활성화하기 전이나 후에 이 작업을 수행할 수 있습니다.

- 로그인 계정에 할당할 액세스 제어 역할을 잘 모르는 경우 나중에 '보안 로그인 수정' 명령을 사용하여 역할을 추가할 수 있습니다.

  관리자에게 할당된 역할 수정

> 클러스터 관리자 계정의 경우 에서 인증서 인증이 지원됩니다 `http`, `ontapi`, 및 `rest` 응용 프로그램. SVM 관리자 계정의 경우 인증서 인증은 을 통해서만 지원됩니다 `ontapi` 및 `rest` 응용 프로그램.

단계

1. 로컬 관리자 계정이 SSL 인증서를 사용하여 SVM에 액세스할 수 있도록 지원:

   '보안 로그인 생성 - vserver SVM_name -user -or -group -name user_or_group_name -application application application -AuthMethod authentication_method -role role role-comment'

   전체 명령 구문은 을 참조하십시오 "ONTAP man 페이지를 릴리스별로 표시합니다".

다음 명령을 실행하면 SSL 디지털 인증서를 사용하여 SVM "engData2"에 액세스할 수 있는 기본 "vsadmin" 역할을 가진 SVM 관리자 계정 'vmadmin2'가 활성화됩니다.

```
cluster1::>security login create -vserver engData2 -user-or-group-name
svmadmin2 -application ontapi -authmethod cert
```

작업을 마친 후

CA 서명 서버 디지털 인증서를 설치하지 않은 경우 계정이 SVM에 액세스하려면 먼저 인증서를 설치해야 합니다.

CA 서명 서버 인증서 생성 및 설치

Active Directory 계정 액세스를 설정합니다

'보안 로그인 생성' 명령을 사용하여 AD(Active Directory) 사용자 또는 그룹 계정을 활성화하여 admin 또는 data SVM에 액세스할 수 있습니다. AD 그룹의 모든 사용자는 그룹에 할당된 역할을 통해 SVM에 액세스할 수 있습니다.

이 작업에 대해

- 계정이 SVM에 액세스하려면 먼저 클러스터 또는 SVM에 대한 AD 도메인 컨트롤러 액세스를 구성해야 합니다.

  Active Directory 도메인 컨트롤러 액세스 구성

  계정 액세스를 활성화하기 전이나 후에 이 작업을 수행할 수 있습니다.

- ONTAP 9.13.1 부터는 SSH 공개 키를 AD 사용자 암호와 함께 기본 또는 보조 인증 방법으로 사용할 수 있습니다.

  SSH 공개 키를 기본 인증으로 사용하도록 선택하면 AD 인증이 수행되지 않습니다.

- ONTAP 9.11.1부터 를 사용할 수 있습니다 "nsswitch 인증을 위한 LDAP 빠른 바인딩" AD LDAP 서버에서 지원하는 경우
- 로그인 계정에 할당할 액세스 제어 역할을 잘 모르는 경우 '보안 로그인 수정' 명령을 사용하여 나중에 역할을 추가할 수 있습니다.

  관리자에게 할당된 역할 수정

> AD 그룹 계정 액세스는 에서만 지원됩니다 `SSH`, `ontapi`, 및 `rest` 응용 프로그램. 다단계 인증에는 일반적으로 사용되는 SSH 공개 키 인증에서는 AD 그룹이 지원되지 않습니다.

시작하기 전에

- 클러스터 시간은 AD 도메인 컨트롤러에서 5분 이내에 에 동기화되어야 합니다.
- 이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. AD 사용자 또는 그룹 관리자 계정을 사용하여 SVM에 액세스:

   - AD 사용자용: *

ONTAP 버전	기본 인증	보조 인증	명령
9.13.1 이상	공개 키	없음	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role>`

9.13.1 이상	도메인	공개 키	• 신규 사용자용 *
			`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`
			• 기존 사용자의 경우 *
			`security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`

9.0 이상	도메인	없음	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

AD 그룹의 경우 *

ONTAP 버전입니다	기본 인증	보조 인증	명령
9.0 이상	도메인	없음	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

+
전체 명령 구문은 을 참조하십시오 "관리자 인증 및 RBAC 구성을 위한 워크시트"

작업을 마친 후

AD 도메인 컨트롤러를 클러스터 또는 SVM에 액세스하도록 구성하지 않은 경우 계정이 SVM에 액세스하려면 먼저 액세스 권한을 구성해야 합니다.

Active Directory 도메인 컨트롤러 액세스 구성

LDAP 또는 **NIS** 계정 액세스를 설정합니다

'Security login create' 명령을 사용하여 LDAP 또는 NIS 사용자 계정이 admin 또는 data SVM에 액세스할 수 있도록 설정할 수 있습니다. SVM에 대한 LDAP 또는 NIS 서버 액세스를 구성하지 않은 경우, 계정이 SVM에 액세스하려면 먼저 액세스 권한을 구성해야 합니다.

이 작업에 대해

- 그룹 계정은 지원되지 않습니다.
- 계정이 SVM에 액세스하려면 먼저 SVM에 대한 LDAP 또는 NIS 서버 액세스를 구성해야 합니다.

  LDAP 또는 NIS 서버 액세스를 구성합니다

  계정 액세스를 활성화하기 전이나 후에 이 작업을 수행할 수 있습니다.

- 로그인 계정에 할당할 액세스 제어 역할을 잘 모르는 경우 '보안 로그인 수정' 명령을 사용하여 나중에 역할을 추가할 수 있습니다.

  관리자에게 할당된 역할 수정

- ONTAP 9.4부터 LDAP 또는 NIS 서버를 통한 원격 사용자에 대해 MFA(Multifactor Authentication)가 지원됩니다.
- ONTAP 9.11.1부터 를 사용할 수 있습니다 "nsswitch 인증을 위한 LDAP 빠른 바인딩" LDAP 서버에서 지원하는 경우
- 알려진 LDAP 문제로 인해 LDAP 사용자 계정 정보 필드(예: "gecos", "userPassword" 등)에 ":"(콜론) 문자를 사용해서는 안 됩니다. 그렇지 않으면 해당 사용자에 대한 조회 작업이 실패합니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. LDAP 또는 NIS 사용자 또는 그룹 계정을 사용하여 SVM에 액세스:

   '보안 로그인 생성 - vserver SVM_name -user -or -group -name user_name -application application -AuthMethod nsswitch -role role -comment comment comment -is -ns -switch -group yes | no [-is -ldap -fastbind true]'를 참조하십시오

   전체 명령 구문은 을 참조하십시오 "워크시트".

   "로그인 계정 생성 또는 수정"

   다음 명령을 실행하면 미리 정의된 백업 역할을 사용하여 LDAP 또는 NIS 클러스터 관리자 계정 guest2가 SVM "engCluster"에 액세스할 수 있습니다.

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name
   guest2 -application ssh -authmethod nsswitch -role backup
   ```

2. LDAP 또는 NIS 사용자에 대해 MFA 로그인 활성화:

   "Security login modify -user -or -group -name rem_usr1 -application ssh-authentication -method nsswitch -role admin -is -ns -switch-group no-second-authentication-method publickey'

   인증 방법은 홍보 키로, 두 번째 인증 방식은 nsswitch로 지정할 수 있습니다.

   다음 예에서는 MFA 인증이 활성화되어 있는 것을 보여 줍니다.

   ```
   cluster-1::*> security login modify -user-or-group-name rem_usr2
   -application ssh -authentication-method nsswitch -vserver
   cluster-1 -second-authentication-method publickey"
   ```

작업을 마친 후

SVM에 대한 LDAP 또는 NIS 서버 액세스를 구성하지 않은 경우, 계정이 SVM에 액세스하려면 먼저 액세스 권한을 구성해야 합니다.

LDAP 또는 NIS 서버 액세스를 구성합니다

액세스 제어 역할을 관리합니다

액세스 제어 역할 관리 개요

관리자에게 할당된 역할에 따라 관리자가 액세스할 수 있는 명령이 결정됩니다. 관리자 계정을 만들 때 역할을 할당합니다. 필요에 따라 다른 역할을 할당하거나 사용자 지정 역할을 정의할 수 있습니다.

관리자에게 할당된 역할을 수정합니다

'security login modify' 명령을 사용하여 클러스터 또는 SVM 관리자 계정의 역할을 변경할 수 있습니다. 미리 정의된 역할 또는 사용자 지정 역할을 할당할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 클러스터 또는 SVM 관리자의 역할 변경:

   '보안 로그인 수정 - vserver SVM_name -user -or -group -name user_or_group_name -application application application -AuthMethod authentication_method -role role role-comment

   전체 명령 구문은 을 참조하십시오 "워크시트".

   "로그인 계정 생성 또는 수정"

   다음 명령을 실행하면 AD 클러스터 관리자 계정 DOMAIN1\guest1 의 역할이 미리 정의된 "재만" 역할로 변경됩니다.

   ```
   cluster1::>security login modify -vserver engCluster -user-or-group-name
   DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
   ```

   다음 명령을 실행하면 AD 그룹 계정 DOMAIN1\adgroup의 SVM 관리자 계정 역할이 사용자 지정 "vol_role" 역할로 변경됩니다.

   ```
   cluster1::>security login modify -vserver engData -user-or-group-name
   DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
   ```

사용자 지정 역할을 정의합니다

'Security login role create' 명령을 사용하여 사용자 지정 역할을 정의할 수 있습니다. 역할에 연결할 기능을 정확하게 조합하기 위해 필요한 만큼 명령을 실행할 수 있습니다.

이 작업에 대해

- 사전 정의되거나 사용자 지정되거나 관계 없이 역할은 ONTAP 명령 또는 명령 디렉터리에 대한 액세스를 허용하거나 거부합니다.

  명령 디렉토리(예: 볼륨)는 관련 명령 및 명령 하위 디렉토리 그룹입니다. 이 절차에서 설명한 경우를 제외하고 명령 디렉터리에 대한 액세스 권한을 부여하거나 거부하면 디렉터리 및 해당 하위 디렉터리의 각 명령에 대한 액세스 권한이 부여되거나 거부됩니다.

- 특정 명령 액세스 또는 하위 디렉토리 액세스는 상위 디렉토리 액세스보다 우선합니다.

  역할이 명령 디렉토리로 정의된 후 특정 명령이나 상위 디렉토리의 하위 디렉토리에 대해 다른 액세스 수준으로 다시 정의된 경우 명령 또는 하위 디렉토리에 지정된 액세스 수준이 상위 명령의 액세스 수준을 재정의합니다.

"admin" 클러스터 관리자만 사용할 수 있는 명령 또는 명령 디렉토리에 대한 액세스를 제공하는 SVM 관리자 역할을 할당할 수 없습니다. 예를 들어, 'security' 명령 디렉토리입니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 사용자 지정 역할 정의:

   'Security login role create -vserver SVM_name -role role -cmddirname command_or_directory_name -access access_level -query'

   전체 명령 구문은 을 참조하십시오 "워크시트".

   다음 명령을 실행하면 'volume' 명령 디렉토리의 명령에 대한 'vol_role' 역할이 전체 액세스되고 'volume snapshot' 하위 디렉토리의 명령에 대한 읽기 전용 액세스가 부여됩니다.

```
cluster1::>security login role create -role vol_role -cmddirname
"volume" -access all

cluster1::>security login role create -role vol_role -cmddirname "volume
snapshot" -access readonly
```

   다음 명령어를 통해 'storage' 명령 디렉토리의 명령에 대한 'vm_storage' 역할 읽기 전용 액세스, 'storage encryption' 하위 디렉토리의 명령에 대한 액세스 권한 없음, 'storage aggregate offline' 비내장 명령에 대한 전체 액세스 권한을 부여한다.

```
cluster1::>security login role create -role SVM_storage -cmddirname
"storage" -access readonly

cluster1::>security login role create -role SVM_storage -cmddirname
"storage encryption" -access none

cluster1::>security login role create -role SVM_storage -cmddirname
"storage aggregate plex offline" -access all
```

클러스터 관리자를 위한 사전 정의된 역할

클러스터 관리자를 위한 사전 정의된 역할은 대부분의 요구사항을 충족해야 합니다. 필요에 따라 사용자 지정 역할을 만들 수 있습니다. 기본적으로 클러스터 관리자에게는 미리 정의된 "admin" 역할이 할당됩니다.

다음 표에는 클러스터 관리자를 위한 사전 정의된 역할이 나와 있습니다.

이 역할은…	이 수준의 액세스 권한…	명령 또는 명령 디렉토리로 이동합니다

관리자	모두	모든 명령 디렉토리(기본값)
Admin-no-FSA(ONTAP 9.12.1부터 사용 가능)	읽기/쓰기	• 모든 명령 디렉토리(기본값) • `security login rest-role` • `security login role`
읽기 전용	• `security login rest-role create` • `security login rest-role delete` • `security login rest-role modify` • `security login rest-role show` • `security login role create` • `security login role create` • `security login role delete` • `security login role modify` • `security login role show` • `volume activity-tracking` • `volume analytics`	없음
`volume file show-disk-usage`	AutoSupport	모두
• '세트' • '시스템 노드 AutoSupport	없음	기타 모든 명령 디렉토리(기본값)
백업	모두	'vserver services ndmp'
읽기 전용	'볼륨'	없음
기타 모든 명령 디렉토리(기본값)	읽기 전용	모두

• '보안 로그인 비밀번호 사용자 계정 로컬 암호 및 키 정보 관리에만 사용됩니다 • '세트'	없음	'보안'
읽기 전용	기타 모든 명령 디렉토리(기본값)	없음

AutoSupport 역할은 AutoSupport OnDemand가 사용하는 미리 정의된 AutoSupport 계정에 할당됩니다. ONTAP에서는 AutoSupport 계정을 수정하거나 삭제할 수 없습니다. 또한 ONTAP에서는 다른 사용자 계정에 'AutoSupport' 역할을 할당할 수 없습니다.

SVM 관리자를 위한 사전 정의된 역할

SVM 관리자를 위한 사전 정의된 역할은 대부분의 요구사항을 충족해야 합니다. 필요에 따라 사용자 지정 역할을 만들 수 있습니다. 기본적으로 SVM 관리자는 사전 정의된 "vsadmin" 역할이 할당됩니다.

다음 표에는 SVM 관리자를 위한 사전 정의된 역할이 나와 있습니다.

역할 이름	제공합니다
vsadmin을 선택합니다	• 사용자 계정 로컬 암호 및 키 정보 관리 • 볼륨 이동을 제외한 볼륨 관리 • 할당량, Qtree, 스냅샷 복사본 및 파일 관리 • LUN 관리 • 권한 있는 삭제를 제외한 SnapLock 작업 수행 • 프로토콜 구성: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC 및 NVMe/TCP • 서비스 구성: DNS, LDAP 및 NIS • 작업 모니터링 • 네트워크 연결 및 네트워크 인터페이스 모니터링 • SVM 상태 모니터링

vsadmin - 볼륨	• 사용자 계정 로컬 암호 및 키 정보 관리 • 볼륨 이동을 포함한 볼륨 관리 • 할당량, Qtree, 스냅샷 복사본 및 파일 관리 • LUN 관리 • 프로토콜 구성: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC 및 NVMe/TCP • 서비스 구성: DNS, LDAP 및 NIS • 네트워크 인터페이스 모니터링 • SVM 상태 모니터링
vsadmin - 프로토콜	• 사용자 계정 로컬 암호 및 키 정보 관리 • 프로토콜 구성: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC 및 NVMe/TCP • 서비스 구성: DNS, LDAP 및 NIS • LUN 관리 • 네트워크 인터페이스 모니터링 • SVM 상태 모니터링
vsadmin - 백업	• 사용자 계정 로컬 암호 및 키 정보 관리 • NDMP 작업 관리 • 복구된 볼륨을 읽기/쓰기로 만듭니다 • SnapMirror 관계 및 Snapshot 복사본 관리 • 볼륨 및 네트워크 정보 보기
vsadmin - SnapLock	• 사용자 계정 로컬 암호 및 키 정보 관리 • 볼륨 이동을 제외한 볼륨 관리 • 할당량, Qtree, 스냅샷 복사본 및 파일 관리 • 권한 있는 삭제를 포함한 SnapLock 작업 수행 • 프로토콜 구성: NFS 및 SMB • 서비스 구성: DNS, LDAP 및 NIS • 작업 모니터링 • 네트워크 연결 및 네트워크 인터페이스 모니터링

vsadmin - 읽기 전용입니다	• 사용자 계정 로컬 암호 및 키 정보 관리 • SVM 상태 모니터링 • 네트워크 인터페이스 모니터링 • 볼륨 및 LUN 보기 • 서비스 및 프로토콜 보기

관리자 액세스 제어

관리자에게 할당된 역할에 따라 관리자가 System Manager에서 수행할 수 있는 기능이 결정됩니다. 클러스터 관리자 및 스토리지 VM 관리자를 위한 사전 정의된 역할은 System Manager에서 제공합니다. 관리자 계정을 만들 때 역할을 할당하거나 나중에 다른 역할을 할당할 수 있습니다.

계정 액세스를 설정한 방법에 따라 다음 중 하나를 수행해야 할 수 있습니다.

- 공개 키를 로컬 계정에 연결합니다.
- CA 서명 서버 디지털 인증서를 설치합니다.
- AD, LDAP 또는 NIS 액세스를 구성합니다.

계정 액세스를 활성화하기 전이나 후에 이러한 작업을 수행할 수 있습니다.

관리자에게 역할 할당

다음과 같이 관리자에게 역할을 할당합니다.

단계

1. 클러스터 > 설정 * 을 선택합니다.
2. 를 선택합니다 → 사용자 및 역할 * 옆에 있습니다.
3. 를 선택합니다 + Add 사용자 * 아래.
4. 사용자 이름을 지정하고 * 역할 * 의 드롭다운 메뉴에서 역할을 선택합니다.
5. 사용자의 로그인 방법 및 암호를 지정합니다.

관리자 역할 변경

다음과 같이 관리자의 역할을 변경합니다.

단계

1. 클러스터 > 설정 * 을 클릭합니다.
2. 역할을 변경할 사용자의 이름을 선택한 다음 을 클릭합니다 ⋮ 사용자 이름 옆에 표시됩니다.
3. 편집 * 을 클릭합니다.
4. 드롭다운 메뉴에서 * 역할 * 의 역할을 선택합니다.

관리자 계정을 관리합니다

관리자 계정 관리 개요

계정 액세스를 설정한 방법에 따라 공개 키를 로컬 계정에 연결하거나, CA 서명 서버 디지털 인증서를 설치하거나, AD, LDAP 또는 NIS 액세스를 구성해야 할 수 있습니다. 계정 액세스를 활성화하기 전이나 후에 이러한 모든 작업을 수행할 수 있습니다.

공개 키를 관리자 계정에 연결합니다

SSH 공개 키 인증의 경우 계정에서 SVM에 액세스할 수 있으려면 먼저 공개 키를 관리자 계정과 연결해야 합니다. 'Security login publickey create' 명령어를 이용하여 관리자 계정에 키를 연결할 수 있다.

이 작업에 대해

암호 및 SSH 공개 키로 SSH를 통해 계정을 인증하면 먼저 공개 키로 계정이 인증됩니다.

시작하기 전에

- SSH 키를 생성해야 합니다.
- 이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. 공개 키를 관리자 계정에 연결:

   '보안 로그인 공개 키 생성 - vserver_SVM_name_-username_user_name_-index_index_-publickey_certificate_-comment_comment_'

   전체 명령 구문은 에 대한 워크시트 참조를 참고하십시오 "공개 키를 사용자 계정과 연결".

2. 공개 키를 확인하여 변경 사항을 확인합니다.

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

예

다음 명령을 실행하면 공용 키가 SVM 관리자 계정에 연결됩니다 `svmadmin1` SVM을 위해 `engData1`. 공개 키에는 인덱스 번호 5가 할당됩니다.

```
cluster1::> security login publickey create -vserver engData1 -username
svmadmin1 -index 5 -publickey
"<key text>"
```

관리자 계정에 대한 **SSH** 공개 키와 **X.509** 인증서를 관리합니다

관리자 계정으로 SSH 인증 보안을 강화하기 위해 를 사용할 수 있습니다 `security login publickey` SSH 공개 키 및 X.509 인증서와의 연결을 관리하는 명령 집합입니다.

공개 키와 **X.509** 인증서를 관리자 계정에 연결합니다

ONTAP 9.13.1 부터는 X.509 인증서를 관리자 계정과 연결된 공개 키와 연결할 수 있습니다. 이렇게 하면 해당 계정에 대한 SSH 로그인 시 인증서 만료 또는 해지 확인을 추가로 보호할 수 있습니다.

이 작업에 대해

SSH 공개 키와 X.509 인증서를 모두 사용하여 SSH를 통해 계정을 인증하는 경우 ONTAP는 SSH 공개 키로 인증하기 전에 X.509 인증서의 유효성을 검사합니다. 인증서가 만료되거나 해지되면 SSH 로그인이 거부되고 공개 키는 자동으로 비활성화됩니다.

시작하기 전에

- 이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.
- SSH 키를 생성해야 합니다.
- X.509 인증서만 만료 여부를 확인해야 하는 경우 자체 서명된 인증서를 사용할 수 있습니다.
- X.509 인증서의 만료 및 해지 여부를 확인해야 하는 경우:
  - CA(인증 기관)로부터 인증서를 받아야 합니다.
  - 를 사용하여 인증서 체인(중간 및 루트 CA 인증서)을 설치해야 합니다 `security certificate install` 명령.
  - SSH용 OCSP를 활성화해야 합니다. 을 참조하십시오 "디지털 인증서가 OCSP를 사용하여 유효한지 확인합니다" 를 참조하십시오.

단계

1. 공개 키와 X.509 인증서를 관리자 계정에 연결합니다.

   `security login publickey create -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`* `-publickey` *`certificate`* `-x509-certificate install`

   전체 명령 구문은 에 대한 워크시트 참조를 참고하십시오 "공개 키를 사용자 계정과 연결".

2. 공개 키를 확인하여 변경 사항을 확인합니다.

   `security login publickey show -vserver` *`SVM_name`* `-username` *`user_name`* `-index` *`index`*

예

다음 명령을 실행하면 공용 키와 X.509 인증서가 SVM 관리자 계정에 연결됩니다 `svmadmin2` SVM을 위해 `engData2`. 공개 키에는 인덱스 번호 6이 할당됩니다.

```
cluster1::> security login publickey create -vserver engData2 -username
svmadmin2 -index 6 -publickey
"<key text>" -x509-certificate install
Please enter Certificate: Press <Enter> when done
<certificate text>
```

관리자 계정의 **SSH** 공개 키에서 인증서 연결을 제거합니다

공개 키를 유지하면서 계정의 SSH 공개 키에서 현재 인증서 연결을 제거할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. 관리자 계정에서 X.509 인증서 연결을 제거하고 기존 SSH 공개 키를 유지합니다.

   ```
   security login publickey modify -vserver SVM_name -username user_name -index
   index -x509-certificate delete
   ```

2. 공개 키를 확인하여 변경 사항을 확인합니다.

   ```
   security login publickey show -vserver SVM_name -username user_name -index
   index
   ```

예

다음 명령을 실행하면 SVM 관리자 계정에서 X.509 인증서 연결이 제거됩니다 `svmadmin2` SVM을 위해 `engData2` 인덱스 번호 6.

```
cluster1::> security login publickey modify -vserver engData2 -username
svmadmin2 -index 6 -x509-certificate delete
```

관리자 계정에서 공개 키 및 인증서 연결을 제거합니다

계정에서 현재 공개 키 및 인증서 구성을 제거할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. 관리자 계정에서 공개 키와 X.509 인증서 연결을 제거합니다.

   ```
   security login publickey delete -vserver SVM_name -username user_name -index
   index
   ```

2. 공개 키를 확인하여 변경 사항을 확인합니다.

   ```
   security login publickey show -vserver SVM_name -username user_name -index
   index
   ```

예

다음 명령을 실행하면 SVM 관리자 계정에서 공개 키와 X.509 인증서가 제거됩니다 `svmadmin3` SVM을 위해 `engData3` 인덱스 번호 7.

```
cluster1::> security login publickey delete -vserver engData3 -username
svmadmin3 -index 7
```

SSH 로그인에 **Cisco Duo 2FA**를 구성합니다

ONTAP 9.14.1부터 SSH 로그인 시 2FA(2단계 인증)에 Cisco Duo를 사용하도록 ONTAP를 구성할 수 있습니다. 클러스터 수준에서 Duo를 구성하면 기본적으로 모든 사용자 계정에 적용됩니다. 또는 스토리지 VM(이전에는 가상 머신이라고 함) 레벨에서 Duo를 구성할 수 있습니다. 이 경우 스토리지 VM의 사용자에게만 적용됩니다. Duo를 활성화하고 구성하면 모든 사용자에 대한 기존 방법을 보완하는 추가 인증 방법으로 사용됩니다.

SSH 로그인에 대해 Duo 인증을 사용하는 경우 사용자는 다음에 SSH를 사용하여 로그인할 때 장치를 등록해야 합니다. 등록 정보는 Cisco Duo를 참조하십시오 "등록 문서".

ONTAP 명령줄 인터페이스를 사용하여 Cisco Duo에서 다음 작업을 수행할 수 있습니다.

- Cisco Duo를 구성합니다
- Cisco Duo 구성을 변경합니다
- Cisco Duo 구성을 제거합니다
- Cisco Duo 구성을 봅니다
- Duo 그룹을 제거합니다
- Duo 그룹 보기
- 사용자를 위한 Duo 인증 우회

Cisco Duo를 구성합니다

를 사용하여 전체 클러스터 또는 특정 스토리지 VM(ONTAP CLI에서 가상 서버라고 함)에 대한 Cisco Duo 구성을 생성할 수 있습니다 `security login duo create` 명령. 이렇게 하면 이 클러스터 또는 스토리지 VM에 대한 SSH 로그인에 Cisco Duo가 활성화됩니다.

단계

1. Cisco Duo Admin Panel에 로그인합니다.
2. 애플리케이션 > UNIX 애플리케이션 * 으로 이동합니다.
3. 통합 키, 비밀 키 및 API 호스트 이름을 기록합니다.
4. SSH를 사용하여 ONTAP 계정에 로그인합니다.
5. 이 스토리지 VM에 대해 Cisco Duo 인증을 사용하도록 설정하고, 환경 정보를 괄호 안의 값으로 대체합니다.

```
security login duo create \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME>
```

이 명령의 필수 및 선택적 매개 변수에 대한 자세한 내용은 을 참조하십시오 "관리자 인증 및 RBAC 구성을 위한 워크시트".

Cisco Duo 구성을 변경합니다

Cisco Duo가 사용자를 인증하는 방법(예: 받은 인증 프롬프트 수 또는 사용된 HTTP 프록시)을 변경할 수 있습니다. 스토리지 VM(ONTAP CLI에서 가상 서버로 표시됨)에 대한 Cisco Duo 구성을 변경해야 하는 경우 를 사용할 수 있습니다 `security login duo modify` 명령.

단계

1. Cisco Duo Admin Panel에 로그인합니다.
2. 애플리케이션 > UNIX 애플리케이션 * 으로 이동합니다.
3. 통합 키, 비밀 키 및 API 호스트 이름을 기록합니다.
4. SSH를 사용하여 ONTAP 계정에 로그인합니다.
5. 이 스토리지 VM에 대한 Cisco Duo 구성을 변경하여 환경의 업데이트된 정보를 괄호 안의 값으로 대체합니다.

```
security login duo modify \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME> \
-pushinfo true|false \
-http-proxy <HTTP_PROXY_URL> \
-autopush true|false \
-prompts 1|2|3 \
-max-unenrolled-logins <NUM_LOGINS> \
-is-enabled true|false \
-fail-mode safe|secure
```

Cisco Duo 구성을 제거합니다

Cisco Duo 구성을 제거하면 SSH 사용자가 로그인할 때 Duo를 사용하여 인증할 필요가 없습니다. 스토리지 VM에 대한 Cisco Duo 구성(ONTAP CLI에서 가상 서버라고 함)을 제거하려면 을 사용합니다 `security login duo delete` 명령.

단계

1. SSH를 사용하여 ONTAP 계정에 로그인합니다.
2. 스토리지 VM 이름을 로 대체하여 이 스토리지 VM에 대한 Cisco Duo 구성을 제거합니다 `<STORAGE_VM_NAME>`:

```
security login duo delete  -vserver <STORAGE_VM_NAME>
```

이렇게 하면 이 스토리지 VM에 대한 Cisco Duo 구성이 영구적으로 삭제됩니다.

Cisco Duo 구성을 봅니다

를 사용하여 스토리지 VM(ONTAP CLI에서 가상 서버로 지칭)에 대한 기존 Cisco Duo 구성을 볼 수 있습니다 `security login duo show` 명령.

단계

1. SSH를 사용하여 ONTAP 계정에 로그인합니다.
2. 이 스토리지 VM에 대한 Cisco Duo 구성을 표시합니다. 필요한 경우 를 사용할 수 있습니다 `vserver` 스토리지 VM 이름을 로 대체하는 스토리지 VM을 지정하는 매개 변수입니다 `<STORAGE_VM_NAME>`:

```
security login duo show -vserver <STORAGE_VM_NAME>
```

다음과 유사한 출력이 표시됩니다.

```
Vserver: testcluster
Enabled: true

Status: ok
INTEGRATION-KEY: DI89811J9JWMJCCO7IOH
SKEY SHA Fingerprint:
b79ffa4b1c50b1c747fbacdb34g671d4814
API Host: api-host.duosecurity.com
Autopush: true
Push info: true
Failmode: safe
Http-proxy: 192.168.0.1:3128
Prompts: 1
Comments: -
```

Duo 그룹을 생성합니다

Cisco Duo에 특정 Active Directory, LDAP 또는 로컬 사용자 그룹의 사용자만 Duo 인증 프로세스에 포함하도록 지시할 수 있습니다. Duo 그룹을 생성하는 경우 해당 그룹의 사용자만 Duo 인증을 요구합니다. 를 사용하여 Duo 그룹을 만들 수 있습니다 `security login duo group create` 명령. 그룹을 생성할 때 필요에 따라 해당 그룹의 특정 사용자를 Duo 인증 프로세스에서 제외할 수 있습니다.

단계

1. SSH를 사용하여 ONTAP 계정에 로그인합니다.
2. 환경의 정보를 대괄호로 묶은 값으로 대체하여 Duo 그룹을 만듭니다. 를 생략할 경우 `-vserver` 매개 변수로, 그룹이 클러스터 레벨에서 생성됩니다.

```
security login duo group create -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -exclude-users <USER1, USER2>
```

Duo 그룹의 이름은 Active Directory, LDAP 또는 로컬 그룹과 일치해야 합니다. 옵션을 사용하여 지정하는 사용자입니다 `-exclude-users` 매개변수는 Duo 인증 프로세스에 포함되지 않습니다.

Duo 그룹 보기

를 사용하여 기존 Cisco Duo 그룹 항목을 볼 수 있습니다 `security login duo group show` 명령.

단계

1. SSH를 사용하여 ONTAP 계정에 로그인합니다.
2. 환경의 정보를 대괄호로 묶은 값으로 대체하여 Duo 그룹 항목을 표시합니다. 를 생략할 경우 `-vserver` 매개변수로, 그룹이 클러스터 레벨에 표시됩니다.

```
security login duo group show -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -exclude-users <USER1, USER2>
```

Duo 그룹의 이름은 Active Directory, LDAP 또는 로컬 그룹과 일치해야 합니다. 옵션을 사용하여 지정하는 사용자입니다 `-exclude-users` 매개 변수가 표시되지 않습니다.

Duo 그룹을 제거합니다

를 사용하여 Duo 그룹 항목을 제거할 수 있습니다 `security login duo group delete` 명령. 그룹을 제거하면 해당 그룹의 사용자가 Duo 인증 프로세스에 더 이상 포함되지 않습니다.

단계

1. SSH를 사용하여 ONTAP 계정에 로그인합니다.
2. Duo 그룹 항목을 제거하여 환경의 정보를 대괄호 안의 값으로 대체합니다. 를 생략할 경우 `-vserver` 매개 변수로, 그룹이 클러스터 레벨에서 제거됩니다.

```
security login duo group delete -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME>
```

Duo 그룹의 이름은 Active Directory, LDAP 또는 로컬 그룹과 일치해야 합니다.

사용자를 위한 **Duo** 인증 우회

Duo SSH 인증 프로세스에서 모든 사용자 또는 특정 사용자를 제외할 수 있습니다.

모든 **Duo** 사용자를 제외합니다

모든 사용자에 대해 Cisco Duo SSH 인증을 비활성화할 수 있습니다.

단계

1. SSH를 사용하여 ONTAP 계정에 로그인합니다.
2. SSH 사용자에 대해 Cisco Duo 인증을 사용하지 않도록 설정하고 SVM 이름을 로 바꿉니다 `<STORAGE_VM_NAME>`:

```
security login duo -vserver <STORAGE_VM_NAME> -is-duo-enabled-false
```

Duo 그룹 사용자를 제외합니다

Duo 그룹에 속한 특정 사용자를 Duo SSH 인증 프로세스에서 제외할 수 있습니다.

단계

1. SSH를 사용하여 ONTAP 계정에 로그인합니다.
2. 그룹의 특정 사용자에 대해 Cisco Duo 인증을 비활성화합니다. 제외할 그룹 이름 및 사용자 목록을 대괄호 안의 값으로 대체합니다.

   ```
   security login group modify -group-name <GROUP_NAME> -exclude-users
   <USER1, USER2>
   ```

   Duo 그룹의 이름은 Active Directory, LDAP 또는 로컬 그룹과 일치해야 합니다. 로 지정한 사용자 `-exclude -users` 매개변수는 Duo 인증 프로세스에 포함되지 않습니다.

로컬 Duo 사용자를 제외합니다

Cisco Duo Admin Panel을 사용하여 특정 로컬 사용자를 Duo 인증을 사용하지 않도록 제외할 수 있습니다. 자세한 내용은 를 참조하십시오 "Cisco Duo 설명서".

CA 서명 서버 인증서 개요 생성 및 설치

운영 시스템에서 클러스터 또는 SVM을 SSL 서버로 인증하는 데 사용할 CA 서명 디지털 인증서를 설치하는 것이 좋습니다. 'Security certificate generate -csr' 명령어를 이용하여 CSR(certificate signing request)과 'security certificate install' 명령어를 이용하여 인증 기관으로부터 받은 인증서를 설치할 수 있다.

인증서 서명 요청을 생성합니다

'Security certificate generate -csr' 명령을 사용하여 CSR(인증서 서명 요청)을 생성할 수 있습니다. 요청을 처리한 후 CA(인증 기관)에서 서명된 디지털 인증서를 보냅니다.

시작하기 전에

이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. CSR 생성:

   'Security certificate generate - csr -common -name FQDN_or_common_name - size 512 | 1024 | 1536 | 2048 - 국가-주-시/도-구/군-기관-조직-단위 장치-전자 메일_of_contact-hash-function SHA1 | SHA256 | MD5'

   다음 명령은 미국 캘리포니아주 서니베일에 위치한 'server1.companyname.com`" 사용자 정의 공통 이름을 가진 회사의 IT 부서의 '소프트웨어' 그룹에서 'sha256' 해시 기능에서 생성된 2048비트 개인 키로 CSR을 만듭니다. SVM 담당자 관리자의 이메일 주소는 ""web@example.com""입니다. 출력에 CSR과 개인 키가 표시됩니다.

CSR 생성 예

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California
-locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256

Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----


Private Key :
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----

Note: Please keep a copy of your certificate request and private key
for future reference.
```

2. CSR 출력에서 인증서 요청을 복사한 다음 전자 양식(예: 전자 메일)으로 신뢰할 수 있는 타사 CA로 보내 서명합니다.

   요청을 처리한 후 CA는 서명된 디지털 인증서를 보냅니다. 개인 키와 CA 서명 디지털 인증서의 복사본을 유지해야 합니다.

CA 서명 서버 인증서를 설치합니다

'보안 인증서 설치' 명령을 사용하여 SVM에 CA 서명 서버 인증서를 설치할 수 있습니다. ONTAP는 서버 인증서의 인증서 체인을 형성하는 CA(인증 기관) 루트 및 중간 인증서를 입력하라는 메시지를 표시합니다.

시작하기 전에

이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. CA 서명 서버 인증서 설치:

   ```
   security certificate install -vserver SVM_name -type certificate_type
   ```

   전체 명령 구문은 을 참조하십시오 "워크시트".

   > ONTAP 서버 인증서의 인증서 체인을 형성하는 CA 루트 및 중간 인증서를 입력하라는 메시지가 표시됩니다. 체인은 서버 인증서를 발급한 CA의 인증서로 시작되며 CA의 루트 인증서까지 범위가 될 수 있습니다. 누락된 중간 인증서는 서버 인증서 설치에 실패합니다.

   다음 명령을 실행하면 CA 서명 서버 인증서와 중간 인증서가 SVM ""engData2""에 설치됩니다.

CA 서명 서버 인증서 중간 인증서 설치 예

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTADEJMAcGA1UECxMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTADEJMAcGA1UECxMA
MQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAyXrK2sry
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLycsUdXA7hXhumHNpvF
C61X2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM7OtbUsgPKw+QCCh9dF1jmuQKeDr+wUMWknlDeGrfhILpzfJGHrLJ
z7UCIQDr8d3gOG71UyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuSl8U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEAr1mnrfYC8KwE9k7A0ylRzBLdUwK9
AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Jugckrbosd/lSd7nQIg
aEMAzt6qHHT4mndi8Bo8sDGedG2SKx6Qbn2IpuNZ7rc=
-----END RSA PRIVATE KEY-----

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIE+zCCBGSgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1Zh
bGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFRoZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECxMoR28gRGFkZHkgQ2xhc3MgMiBDZXJ0
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
```

```
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0
IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTk5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0IFZhbGlkYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENs
YXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDExhodHRw
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: n

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.
```

System Manager를 사용하여 인증서를 관리합니다

ONTAP 9.10.1부터 시스템 관리자를 사용하여 신뢰할 수 있는 인증서 기관, 클라이언트/서버 인증서 및 로컬(온보드) 인증서 기관을 관리할 수 있습니다.

System Manager를 사용하면 다른 응용 프로그램에서 받은 인증서를 관리할 수 있으므로 해당 응용 프로그램의 통신을 인증할 수 있습니다. 시스템을 다른 응용 프로그램에 식별하는 고유한 인증서를 관리할 수도 있습니다.

인증서 정보를 봅니다

System Manager를 사용하면 클러스터에 저장된 신뢰할 수 있는 인증서 기관, 클라이언트/서버 인증서 및 로컬 인증서 기관을 볼 수 있습니다.

단계

1. System Manager에서 * 클러스터 > 설정 * 을 선택합니다.
2. 보안 * 영역으로 스크롤합니다. 인증서 * 섹션에 다음 세부 정보가 표시됩니다.
   - 저장된 신뢰할 수 있는 인증 기관의 수입니다.
   - 저장된 클라이언트/서버 인증서 수
   - 저장된 로컬 인증 기관의 수입니다.
3. 인증서 범주에 대한 세부 정보를 보려면 번호를 선택하거나 을 선택합니다 → 모든 범주에 대한 정보가 포함된 * 인증서 * 페이지를 엽니다.
   이 목록에는 전체 클러스터에 대한 정보가 표시됩니다. 특정 스토리지 VM에 대한 정보만 표시하려면 다음 단계를 수행하십시오.
   a. 스토리지 > 스토리지 VM * 을 선택합니다.
   b. 스토리지 VM을 선택합니다.
   c. 설정 * 탭으로 전환합니다.

d. 인증서 * 섹션에 표시된 번호를 선택합니다.

다음 단계

- 인증서 * 페이지에서 을(를) 사용할 수 있습니다 인증서 서명 요청을 생성합니다.
- 인증서 정보는 세 개의 탭으로 구분됩니다. 각 범주마다 하나씩 있습니다. 각 탭에서 다음 작업을 수행할 수 있습니다.

이 탭에서…	다음 절차를 수행할 수 있습니다…
• 신뢰할 수 있는 인증 기관 *	• [install-trusted-cert] • 신뢰할 수 있는 인증 기관을 삭제합니다 • 신뢰할 수 있는 인증 기관을 갱신합니다
• 클라이언트/서버 인증서 *	• [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert]
• 로컬 인증 기관 *	• 새 로컬 인증 기관을 생성합니다 • 로컬 인증 기관을 사용하여 인증서에 서명합니다 • 로컬 인증 기관을 삭제합니다 • 로컬 인증 기관을 갱신합니다

인증서 서명 요청을 생성합니다

인증서 * 페이지의 아무 탭에서나 System Manager를 사용하여 CSR(인증서 서명 요청)을 생성할 수 있습니다. 개인 키와 해당하는 CSR이 생성되며, 이 키는 인증 기관을 통해 서명하여 공용 인증서를 생성할 수 있습니다.

단계

1. 인증서 * 페이지를 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. CSR 생성 * 을 선택합니다.
3. 주체 이름에 대한 정보를 입력합니다.
   a. 일반 이름 * 을 입력합니다.
   b. 국가 * 를 선택합니다.
   c. 조직 * 을 입력합니다.
   d. 조직 단위 * 를 입력합니다.
4. 기본값을 무시하려면 * 추가 옵션 * 을 선택하고 추가 정보를 제공합니다.

신뢰할 수 있는 인증 기관을 설치(추가)합니다

신뢰할 수 있는 인증 기관을 System Manager에 추가로 설치할 수 있습니다.

단계

1. 신뢰할 수 있는 인증 기관 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 를 선택합니다 + Add .
3. 신뢰할 수 있는 인증 기관 추가* 패널에서 다음을 수행하십시오.
   - 이름 * 을 입력합니다.
   - 범위 * 에서 스토리지 VM을 선택합니다.
   - 일반 이름 * 을 입력합니다.
   - 유형 * 을 선택합니다.
   - 인증서 세부 정보 * 를 입력하거나 가져옵니다.

신뢰할 수 있는 인증 기관을 삭제합니다

System Manager를 사용하면 신뢰할 수 있는 인증 기관을 삭제할 수 있습니다.

> ONTAP에 사전 설치된 신뢰할 수 있는 인증 기관은 삭제할 수 없습니다.

단계

1. 신뢰할 수 있는 인증 기관 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 신뢰할 수 있는 인증 기관의 이름을 선택합니다.
3. 를 선택합니다 ⋮ 이름 옆에 있는 * 삭제 * 를 선택합니다.

신뢰할 수 있는 인증 기관을 갱신합니다

System Manager를 사용하면 만료되었거나 곧 만료될 신뢰할 수 있는 인증 기관을 갱신할 수 있습니다.

단계

1. 신뢰할 수 있는 인증 기관 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 신뢰할 수 있는 인증 기관의 이름을 선택합니다.
3. 를 선택합니다 ⋮ 인증서 이름 옆에 * 갱신 * 을 입력합니다.

클라이언트/서버 인증서를 설치(추가)합니다

System Manager를 사용하면 추가 클라이언트/서버 인증서를 설치할 수 있습니다.

단계

1. 클라이언트/서버 인증서 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 를 선택합니다 + Add .
3. 클라이언트/서버 인증서 추가 * 패널에서 다음을 수행하십시오.
   - 인증서 이름 * 을 입력합니다.
   - 범위 * 에서 스토리지 VM을 선택합니다.
   - 일반 이름 * 을 입력합니다.

- 유형 * 을 선택합니다.
- 인증서 세부 정보 * 를 입력하거나 가져옵니다. 텍스트 파일에서 인증서 세부 정보를 작성하거나 복사하여 붙여 넣거나 * Import *(가져오기 *)를 클릭하여 인증서 파일에서 텍스트를 가져올 수 있습니다.
- 개인 키 * 를 입력합니다.
  텍스트 파일에서 개인 키를 작성하거나 복사하여 붙여 넣거나 * Import *(가져오기 *)를 클릭하여 개인 키 파일에서 텍스트를 가져올 수 있습니다.

자체 서명된 클라이언트/서버 인증서를 생성(추가)합니다

System Manager를 사용하면 자체 서명된 클라이언트/서버 인증서를 추가로 생성할 수 있습니다.

단계

1. 클라이언트/서버 인증서 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 선택 * + 자체 서명 인증서 생성 *.
3. 자체 서명된 인증서 생성 * 패널에서 다음을 수행합니다.
   - 인증서 이름 * 을 입력합니다.
   - 범위 * 에서 스토리지 VM을 선택합니다.
   - 일반 이름 * 을 입력합니다.
   - 유형 * 을 선택합니다.
   - 해시 함수 * 를 선택합니다.
   - 키 크기 * 를 선택합니다.
   - 스토리지 VM * 을 선택합니다.

클라이언트/서버 인증서를 삭제합니다

System Manager를 사용하면 클라이언트/서버 인증서를 삭제할 수 있습니다.

단계

1. 클라이언트/서버 인증서 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 클라이언트/서버 인증서의 이름을 선택합니다.
3. 를 선택합니다 ⋮ 이름 옆에 있는 * 삭제 * 를 클릭합니다.

클라이언트/서버 인증서를 갱신합니다

System Manager를 사용하면 만료되었거나 곧 만료될 클라이언트/서버 인증서를 갱신할 수 있습니다.

단계

1. 클라이언트/서버 인증서 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 클라이언트/서버 인증서의 이름을 선택합니다.
3. 를 선택합니다 ⋮ 이름 옆에 있는 * 갱신 * 을 클릭합니다.

새 로컬 인증 기관을 생성합니다

System Manager를 사용하여 새 로컬 인증 기관을 만들 수 있습니다.

단계

1. 로컬 인증 기관 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 를 선택합니다 + Add .
3. [로컬 인증 기관 추가]* 패널에서 다음 작업을 수행하십시오.
   - 이름 * 을 입력합니다.
   - 범위 * 에서 스토리지 VM을 선택합니다.
   - 일반 이름 * 을 입력합니다.
4. 기본값을 무시하려면 * 추가 옵션 * 을 선택하고 추가 정보를 제공합니다.

로컬 인증 기관을 사용하여 인증서에 서명합니다

System Manager에서 로컬 인증 기관을 사용하여 인증서에 서명할 수 있습니다.

단계

1. 로컬 인증 기관 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 로컬 인증 기관의 이름을 선택합니다.
3. 를 선택합니다 ⋮ 이름 옆에 * 인증서 서명 * 을 입력합니다.
4. 인증서 서명 요청 * 양식 을 작성합니다.
   - 인증서 서명 콘텐츠를 붙여 넣거나 * 가져오기 * 를 클릭하여 인증서 서명 요청 파일을 가져올 수 있습니다.
   - 인증서가 유효한 일 수를 지정합니다.

로컬 인증 기관을 삭제합니다

System Manager를 사용하면 로컬 인증 기관을 삭제할 수 있습니다.

단계

1. 로컬 인증 기관 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 로컬 인증 기관의 이름을 선택합니다.
3. 를 선택합니다 ⋮ 이름 옆에 * Delete * 를 클릭합니다.

로컬 인증 기관을 갱신합니다

System Manager를 사용하면 만료되었거나 곧 만료될 로컬 인증 기관을 갱신할 수 있습니다.

단계

1. 로컬 인증 기관 * 탭을 봅니다. 을 참조하십시오 인증서 정보를 봅니다.
2. 로컬 인증 기관의 이름을 선택합니다.
3. 를 선택합니다 ⋮ 이름 옆에 있는 * 갱신 * 을 클릭합니다.

Active Directory 도메인 컨트롤러 액세스 개요 구성

AD 계정이 SVM에 액세스하려면 먼저 클러스터 또는 SVM에 대한 AD 도메인 컨트롤러 액세스를 구성해야 합니다. 데이터 SVM을 위해 SMB 서버를 이미 구성한 경우, SVM을 클러스터에 대한 AD 액세스를 위한 게이트웨이 또는 _tunnel_로 구성할 수 있습니다. SMB 서버를 구성하지 않은 경우 AD 도메인에서 SVM에 대한 컴퓨터 계정을 생성할 수 있습니다.

ONTAP는 다음과 같은 도메인 컨트롤러 인증 서비스를 지원합니다.

- Kerberos
- LDAP를 지원합니다
- Netlogon
- 로컬 보안 기관(LSA)

ONTAP는 보안 Netlogon 연결을 위해 다음 세션 키 알고리즘을 지원합니다.

세션 키 알고리즘입니다	다음으로 시작…
HMAC-SHA256, AES(Advanced Encryption Standard) 기반 클러스터에서 ONTAP 9.9.1 이하를 실행하고 도메인 컨트롤러가 보안 Netlogon 서비스를 위해 AES를 적용하는 경우 연결이 실패합니다. 이 경우 ONTAP와의 강력한 키 연결을 허용하도록 도메인 컨트롤러를 다시 구성해야 합니다.	ONTAP 9.10.1
Des 및 HMAC-MD5(강력한 키가 설정된 경우)	모든 ONTAP 9 릴리스

Netlogon 보안 채널을 설정하는 동안 AES 세션 키를 사용하려면 SVM에서 AES가 활성화되어 있는지 확인해야 합니다.

- ONTAP 9.14.1부터 AES는 SVM을 생성할 때 기본적으로 사용하도록 설정되며, Netlogon 보안 채널 설정 중에 AES 세션 키를 사용하도록 SVM의 보안 설정을 수정할 필요가 없습니다.
- ONTAP 9.10.1~9.13.1에서는 SVM을 생성할 때 AES가 기본적으로 사용하지 않도록 설정됩니다. 다음 명령을 사용하여 AES를 사용하도록 설정해야 합니다.

```
cifs security modify -vserver vs1 -aes-enabled-for-netlogon-channel true
```

> ONTAP 9.14.1 이상으로 업그레이드할 때 이전 ONTAP 릴리즈와 함께 생성된 기존 SVM에 대한 AES 설정이 자동으로 변경되지 않습니다. 하지만 이러한 SVM에서 AES를 사용하도록 설정하려면 이 설정의 값을 업데이트해야 합니다.

인증 터널을 구성합니다

데이터 SVM을 위해 SMB 서버를 이미 구성한 경우 'security login domain-tunnel create' 명령을 사용하여 SVM을 게이트웨이로 구성하거나, AD에서 클러스터에 액세스하도록 _tunnel_을 사용할 수 있습니다.

시작하기 전에

- 데이터 SVM을 위해 SMB 서버를 구성해야 합니다.
- 클러스터의 admin SVM에 액세스하려면 AD 도메인 사용자 계정을 활성화해야 합니다.
- 이 작업을 수행하려면 클러스터 관리자여야 합니다.

ONTAP 9.10.1부터 AD 액세스를 위한 SVM 게이트웨이(도메인 터널)가 있는 경우 AD 도메인에서 NTLM을 비활성화한 경우 관리자 인증에 Kerberos를 사용할 수 있습니다. 이전 릴리즈에서는 SVM 게이트웨이에 대한 관리자 인증을 사용하여 Kerberos를 지원하지 않았습니다. 이 기능은 기본적으로 사용할 수 있으며 구성이 필요하지 않습니다.

> Kerberos 인증은 항상 먼저 시도됩니다. 오류가 발생하면 NTLM 인증이 시도됩니다.

단계

1. 클러스터에 대한 AD 도메인 컨트롤러 액세스를 위한 인증 터널로 SMB 지원 데이터 SVM 구성:

   `security login domain-tunnel create -vserver svm_name`

   전체 명령 구문은 을 참조하십시오 "워크시트".

   > 사용자가 인증을 받으려면 SVM이 실행 중이어야 합니다.

   다음 명령은 SMB 지원 데이터 SVM ""engData""를 인증 터널로 구성합니다.

   ```
   cluster1::>security login domain-tunnel create -vserver engData
   ```

도메인에서 **SVM** 컴퓨터 계정을 생성합니다

데이터 SVM용으로 SMB 서버를 구성하지 않은 경우 'vserver active-directory create' 명령을 사용하여 도메인의 SVM에 대한 컴퓨터 계정을 생성할 수 있습니다.

이 작업에 대해

'vserver active-directory create' 명령을 입력하면 도메인의 지정된 조직 단위에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 AD 사용자 계정에 대한 자격 증명을 제공하라는 메시지가 표시됩니다. 계정의 암호는 비워둘 수 없습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. AD 도메인에서 SVM을 위한 컴퓨터 계정을 생성합니다.

   'vserver active-directory create-vserver_SVM_name_-account-name_NetBIOS_account_name_-domain_domain_-ou_조직_unit_'

   전체 명령 구문은 을 참조하십시오 "워크시트".

   다음 명령을 실행하면 SVM ""engData"" 도메인인 ""example.com`""ADSERVER1""이라는 컴퓨터 계정이 생성됩니다. 명령을 입력한 후 AD 사용자 계정 자격 증명을 입력하라는 메시지가 표시됩니다.

```
cluster1::>vserver active-directory create -vserver engData -account
-name ADSERVER1 -domain example.com

In order to create an Active Directory machine account, you must supply
the name and password of a Windows account with sufficient privileges to
add computers to the "CN=Computers" container within the "example.com"
domain.

Enter the user name: Administrator

Enter the password:
```

LDAP 또는 **NIS** 서버 액세스 개요를 구성합니다

LDAP 또는 NIS 계정이 SVM에 액세스하려면 먼저 SVM에 대한 LDAP 또는 NIS 서버 액세스를 구성해야 합니다. 스위치 기능을 사용하면 LDAP 또는 NIS를 대체 이름 서비스 소스로 사용할 수 있습니다.

LDAP 서버 액세스를 구성합니다

LDAP 계정이 SVM에 액세스하려면 SVM에 대한 LDAP 서버 액세스를 구성해야 합니다. SVM에서 'vserver services name-service ldap client create' 명령을 사용하여 LDAP 클라이언트 구성을 생성할 수 있습니다. 그런 다음 "vserver services name-service ldap create" 명령을 사용하여 LDAP 클라이언트 구성을 SVM과 연결할 수 있습니다.

이 작업에 대해

대부분의 LDAP 서버는 ONTAP에서 제공하는 기본 스키마를 사용할 수 있습니다.

- MS-AD-BIS(대부분의 Windows 2012 이상 AD 서버에 대한 기본 스키마)
- AD-IDMU(Windows 2008, Windows 2016 이상 AD 서버)
- AD-SFU(Windows 2003 및 이전 AD 서버)
- RFC-2307(UNIX LDAP 서버)

그렇지 않으면 기본 스키마를 사용하는 것이 가장 좋습니다. 이 경우 기본 스키마를 복사하고 복사본을 수정하여 고유한 스키마를 만들 수 있습니다. 자세한 내용은 다음을 참조하십시오.

- "NFS 구성"
- "NetApp 기술 보고서 4835: ONTAP에서 LDAP를 구성하는 방법"

시작하기 전에

- 을(를) 설치해야 합니다 "CA 서명 서버 디지털 인증서" SVM에서.
- 이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. SVM에서 LDAP 클라이언트 구성을 생성합니다.

`vserver services name-service ldap client create -vserver SVM_name -client -config client_configuration -servers LDAP_server_IPs -schema schema -use -start-tls true|false`

> 시작 TLS는 데이터 SVM에 대한 액세스에만 지원됩니다. 관리 SVM에 대한 액세스는 지원되지 않습니다.

전체 명령 구문은 을 참조하십시오 "워크시트".

다음 명령을 실행하면 SVM ""engData""에 ""corp""라는 LDAP 클라이언트 구성이 생성됩니다. 클라이언트는 IP 주소 172.160.0.100 및 172.16.0.101을 사용하여 LDAP 서버에 익명 바인딩합니다. 클라이언트는 RFC-2307 스키마를 사용하여 LDAP 쿼리를 만듭니다. 클라이언트와 서버 간의 통신은 시작 TLS를 사용하여 암호화됩니다.

```
cluster1::> vserver services name-service ldap client create
-vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
-schema RFC-2307 -use-start-tls true
```

> ONTAP 9.2부터 -ldap-servers 필드가 -servers 필드를 대체합니다. 이 새 필드는 LDAP 서버의 호스트 이름 또는 IP 주소를 사용할 수 있습니다.

2. LDAP 클라이언트 구성을 SVM에 연결: `vserver services name-service ldap create -vserver SVM_name -client-config client_configuration -client-enabled true|false`

   전체 명령 구문은 을 참조하십시오 "워크시트".

   다음 명령은 LDAP 클라이언트 구성을 연결합니다 `corp` SVM을 사용합니다 `engData`및 는 SVM에서 LDAP 클라이언트를 활성화합니다.

```
cluster1::>vserver services name-service ldap create -vserver engData
-client-config corp -client-enabled true
```

> ONTAP 9.2부터 'vserver services name-service ldap create' 명령은 자동 구성 검증을 수행하고 ONTAP가 이름 서버에 연결할 수 없는 경우 오류 메시지를 보고합니다.

3. vserver services name-service ldap check 명령을 사용하여 이름 서버의 상태를 확인합니다.

   다음 명령을 실행하면 SVM vs0에서 LDAP 서버를 검증합니다.

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                |
| Client Configuration Name: c1                               |
| LDAP Status: up                                             |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                              |
```

이름 서비스 확인 명령은 ONTAP 9.2부터 사용할 수 있습니다.

NIS 서버 액세스를 구성합니다

NIS 계정이 SVM에 액세스하려면 먼저 SVM에 대한 NIS 서버 액세스를 구성해야 합니다. SVM에 NIS 도메인 구성을 생성하려면 'vserver services name-service nis-domain create' 명령을 사용할 수 있습니다.

이 작업에 대해

여러 NIS 도메인을 생성할 수 있습니다. NIS 도메인은 한 번에 하나만 '활성'으로 설정할 수 있습니다.

시작하기 전에

- SVM에서 NIS 도메인을 구성하기 전에 구성된 모든 서버를 사용할 수 있고 액세스할 수 있어야 합니다.
- 이 작업을 수행하려면 클러스터 또는 SVM 관리자여야 합니다.

단계

1. SVM에서 NIS 도메인 구성 생성:

   ```
   vserver services name-service nis-domain create -vserver SVM_name -domain
   client_configuration -active true|false -nis-servers NIS_server_IPs
   ```

   전체 명령 구문은 을 참조하십시오 "워크시트".

   > ONTAP 9.2부터, 필드 '-NIS-SERS'는 필드 '-SERVers'를 대체합니다. 이 새 필드는 NIS 서버의 호스트 이름 또는 IP 주소를 사용할 수 있습니다.

   다음 명령을 실행하면 SVM ""engData""에 NIS 도메인 구성이 생성됩니다. NIS 도메인입니다 `nisdomain` 생성 시 활성 상태이며 IP 주소 192.0.2.180을 사용하여 NIS 서버와 통신합니다.

   ```
   cluster1::>vserver services name-service nis-domain create
   -vserver engData -domain nisdomain -active true -nis-servers 192.0.2.180
   ```

네임 서비스 스위치를 생성합니다

이름 서비스 스위치 기능을 사용하면 LDAP 또는 NIS를 대체 이름 서비스 소스로 사용할 수 있습니다. 'vserver services name-service ns-switch modify' 명령을 사용하여 이름 서비스 소스의 조회 순서를 지정할 수 있습니다.

시작하기 전에

- LDAP 및 NIS 서버 액세스를 구성해야 합니다.
- 이 작업을 수행하려면 클러스터 관리자 또는 SVM 관리자여야 합니다.

단계

1. 이름 서비스 원본에 대한 조회 순서를 지정합니다.

   ```
   vserver services name-service ns-switch modify -vserver SVM_name -database
   name_service_switch_database -sources name_service_source_order
   ```

   전체 명령 구문은 을 참조하십시오 "워크시트".

다음 명령은 SVM ""engData""의 ""passwd"" 데이터베이스에 대한 LDAP 및 NIS 이름 서비스 소스의 조회 순서를 지정합니다.

```
cluster1::>vserver services name-service ns-switch
modify -vserver engData -database passwd -source files ldap,nis
```

관리자 암호를 변경합니다

처음 시스템에 로그인한 후 즉시 초기 암호를 변경해야 합니다. SVM 관리자는 '보안 로그인 비밀번호' 명령을 사용하여 비밀번호를 변경할 수 있습니다. 클러스터 관리자인 경우 '보안 로그인 암호' 명령을 사용하여 관리자 암호를 변경할 수 있습니다.

이 작업에 대해

새 암호는 다음 규칙을 준수해야 합니다.

- 사용자 이름은 포함할 수 없습니다
- 8자 이상이어야 합니다
- 하나 이상의 문자와 숫자를 포함해야 합니다
- 마지막 여섯 개의 암호와 같을 수 없습니다

> 를 사용할 수 있습니다 `security login role config modify` 지정된 역할과 연결된 계정의 암호 규칙을 수정하는 명령입니다. 자세한 내용은 를 참조하십시오 "명령 참조".

시작하기 전에

- 암호를 변경하려면 클러스터 또는 SVM 관리자여야 합니다.
- 다른 관리자의 암호를 변경하려면 클러스터 관리자여야 합니다.

단계

1. 관리자 암호 변경: `security login password -vserver` *`svm_name`* `-username` *`user_name`*

   다음 명령을 실행하면 SVM에 대한 관리자 admin의 암호(vs1.example.com``)가 변경됩니다. 현재 암호를 입력하라는 메시지가 표시되면 새 암호를 입력하고 다시 입력합니다.

   ```
   vs1.example.com::>security login password -vserver engData -username
   admin1
   Please enter your current password:
   Please enter a new password:
   Please enter it again:
   ```

관리자 계정 잠금 및 잠금 해제

'Security login lock' 명령어를 이용하여 관리자 계정을 잠그고, 'Security login unlock' 명령어를 이용하여 계정 잠금을 해제할 수 있다.

시작하기 전에

이러한 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 관리자 계정 잠금:

   'Security login lock - vserver SVM_name - username user_name

   다음 명령을 실행하면 SVM에 대한 관리자 계정 admin1이 잠깁니다. vs1.example.com``:

   ```
   cluster1::>security login lock -vserver engData -username admin1
   ```

2. 관리자 계정 잠금 해제:

   'Security login unlock - vserver SVM_name - username user_name'

   다음 명령을 실행하면 SVM에 대한 관리자 계정 admin1의 잠금이 해제됩니다. vs1.example.com``:

   ```
   cluster1::>security login unlock -vserver engData -username admin1
   ```

실패한 로그인 시도를 관리합니다

로그인 시도가 반복적으로 실패하면 침입자가 스토리지 시스템을 액세스하려고 시도하는 것을 나타내는 경우가 있습니다. 침입이 발생하지 않도록 여러 단계를 수행할 수 있습니다.

로그인 시도가 실패했음을 어떻게 알 수 있습니다

이벤트 관리 시스템(EMS)은 매 시간마다 로그인 실패 사실을 알립니다. 'audit.log' 파일에서 실패한 로그인 시도 기록을 찾을 수 있습니다.

반복 로그인 시도가 실패하면 어떻게 해야 합니까

단기적으로는 침입 방지를 위한 여러 단계를 수행할 수 있습니다.

- 암호는 최소 대문자, 소문자, 특수 문자 및/또는 숫자로 구성되어야 합니다
- 로그인 시도 실패 후 지연을 적용합니다
- 허용되는 로그인 시도 실패 횟수를 제한하고 지정된 시도 실패 횟수 이후에 사용자를 잠급니다
- 지정된 일 수 동안 비활성 상태인 계정을 만료 및 잠급니다

'Security login role config modify' 명령어를 사용해 이 작업을 수행할 수 있다.

장기적으로 다음과 같은 추가 단계를 수행할 수 있습니다.

- 새로 생성된 모든 SVM에 대해 로그인 시도 실패 횟수를 제한하려면 'security ssh modify' 명령을 사용합니다.
- 사용자에게 암호를 변경하도록 요구하여 기존 MD5 알고리즘 계정을 보다 안전한 SHA-512 알고리즘으로 마이그레이션합니다.

관리자 계정 암호에 **SHA-2**를 적용합니다

ONTAP 9.0 이전에 만든 관리자 계정은 암호를 수동으로 변경할 때까지 업그레이드 후 MD5 암호를 계속 사용합니다. MD5는 SHA-2보다 안전하지 않습니다. 따라서 업그레이드 후 MD5 계정 사용자에게 암호를 변경하여 기본 SHA-512 해시 기능을 사용하도록 해야 합니다.

이 작업에 대해

암호 해시 기능을 사용하면 다음을 수행할 수 있습니다.

- 지정된 해시 함수와 일치하는 사용자 계정을 표시합니다.
- 지정된 해시 기능(예: MD5)을 사용하는 계정을 만료하여 사용자가 다음 로그인 시 암호를 변경하도록 합니다.
- 암호가 지정된 해시 기능을 사용하는 계정을 잠급니다.
- ONTAP 9 이전 릴리즈로 되돌릴 때 이전 릴리즈에서 지원하는 MD5(해시 기능)와 호환되도록 클러스터 관리자의 자체 암호를 재설정합니다.

ONTAP는 NetApp Manageability SDK를 사용하여 해시된 SHA-2 암호만 허용합니다 (`security-login-create` 및 `security-login-modify-password`)를 클릭합니다.

단계

1. MD5 관리자 계정을 SHA-512 암호 해시 기능으로 마이그레이션합니다.
   a. MD5 관리자 계정 모두 만료: '보안 로그인 만료 - 암호 - vserver* - 사용자 이름* - 해시 - 기능 MD5'

      이렇게 하면 MD5 계정 사용자는 다음 로그인 시 암호를 변경해야 합니다.

   b. MD5 계정 사용자에게 콘솔 또는 SSH 세션을 통해 로그인하도록 요청합니다.

      계정이 만료되었음을 감지하고 사용자에게 암호를 변경하라는 메시지를 표시합니다. SHA-512는 변경된 암호에 기본적으로 사용됩니다.

2. 사용자가 로그인하지 않은 MD5 계정의 경우 일정 시간 내에 암호를 변경하려면 다음과 같이 계정 마이그레이션을 강제로 수행합니다.
   a. MD5 해시 기능(고급 권한 수준)을 계속 사용하는 계정 잠금: '보안 로그인 만료 - 암호 - vserver* - 사용자 이름 * - 해시 - 기능 md5 - 정수 후 잠금

      록애프터(lock-After)로 지정된 일 수가 지나면 MD5 계정에 액세스할 수 없습니다.

   b. 사용자가 암호를 변경할 준비가 되면 계정의 잠금을 해제합니다. `security login unlock -vserver svm_name -username user_name`
   c. 사용자가 콘솔 또는 SSH 세션을 통해 계정에 로그인하고 시스템에서 암호를 변경하도록 요청하는 경우 암호를 변경하도록 요청합니다.

파일 액세스 문제를 진단하고 해결합니다

단계

1. System Manager에서 * 스토리지 > 스토리지 VM * 을 선택합니다.
2. 추적을 수행할 스토리지 VM을 선택합니다.
3. 을 클릭합니다 ⋮ 추가 정보 *.

4. 추적 파일 액세스 * 를 클릭합니다.
5. 사용자 이름과 클라이언트 IP 주소를 입력한 다음 * 추적 시작 * 을 클릭합니다.

   추적 결과가 테이블에 표시됩니다. 이유 * 열은 파일에 액세스할 수 없는 이유를 제공합니다.

6. 을 클릭합니다 ⌄ 파일 액세스 권한을 보려면 결과 테이블의 왼쪽 열에 있습니다.

여러 관리자 검증 관리

다중 관리 검증 개요

ONTAP 9.11.1부터 MAV(Multi-admin verification)를 사용하여 볼륨 삭제 또는 스냅샷 복사본 삭제와 같은 특정 작업이 지정된 관리자의 승인 후에만 실행될 수 있는지 확인할 수 있습니다. 따라서 손상되거나 악의적이거나 경험이 부족한 관리자가 원치 않는 변경 또는 데이터 삭제를 방지할 수 있습니다.

다중 관리자 검증 구성은 다음과 같이 구성됩니다.

- "하나 이상의 관리자 승인 그룹을 생성합니다."
- "다중 관리 확인 기능 활성화."
- "규칙 추가 또는 수정"

초기 구성 후에는 MAV 승인 그룹(MAV 관리자)의 관리자만 이러한 요소를 수정할 수 있습니다.

다중 관리 검증이 활성화된 경우 모든 보호 작업을 완료하려면 다음 3단계를 수행해야 합니다.

- 사용자가 작업을 시작하면, 가 표시됩니다 "요청이 생성되었습니다."
- 실행하기 전에 최소 1개 이상 "MAV 관리자가 승인해야 합니다."
- 승인 시 사용자는 작업을 완료합니다.

멀티 관리 검증은 작업이 완료되기 전에 각 자동화 작업이 승인을 받아야 하기 때문에 대량 자동화가 필요한 볼륨 또는 워크플로우에서 사용할 수 없습니다. 자동화 및 MAV를 함께 사용하려면 특정 MAV 작업에 대한 쿼리를 사용하는 것이 좋습니다. 예를 들어, 자동화가 포함되지 않은 볼륨에만 볼륨 삭제 MAV 규칙을 적용하고 특정 명명 체계를 사용하여 해당 볼륨을 지정할 수 있습니다.

> MAV 관리자의 승인 없이 다중 관리 검증 기능을 사용하지 않도록 설정해야 하는 경우 NetApp Support에 다음 기술 자료 문서를 멘션하십시오. "MAV 관리자를 사용할 수 없는 경우 다중 관리 확인을 비활성화하는 방법".

다중 관리 확인 작동 방식

다중 관리 검증의 구성:

- 승인 및 거부권을 가진 하나 이상의 관리자 그룹.
- _rules table_의 보호된 작업 또는 명령 집합.
- 보호된 작업의 실행을 식별하고 제어하기 위한 _ 규칙 엔진 _.

역할 기반 액세스 제어(RBAC) 규칙 이후에 MAV 규칙을 평가합니다. 따라서 보호된 작업을 실행하거나 승인하는 관리자는 해당 작업에 대한 최소 RBAC 권한을 이미 가지고 있어야 합니다. "RBAC에 대해 자세히 알아보십시오."

시스템 정의 규칙

다중 관리 검증이 활성화된 경우 시스템 정의 규칙(_guard-rail_rules라고도 함)은 MAV 프로세스 자체를 회피하는 위험을 포함할 수 있는 일련의 MAV 작업을 설정합니다. 이러한 작업은 규칙 테이블에서 제거할 수 없습니다. MAV가 활성화되면 별표(*)로 지정된 작업은 실행 전에 하나 이상의 관리자가 승인해야 합니다. 단, * show * 명령은 예외입니다.

- `security multi-admin-verify modify` 작동 *

  다중 관리 검증 기능의 구성을 제어합니다.

- '보안 멀티 관리 - 승인그룹' 운영 여부 확인

  여러 관리자 확인 자격 증명을 사용하여 관리자 집합에서 구성원 자격을 제어합니다.

- '보안 멀티-관리-검증 규칙' 운영 *

  admin이 여러 개인 검증이 필요한 명령 세트 제어

- '보안 멀티-관리-검증 요청' 작업

  승인 프로세스를 제어합니다.

규칙으로 보호된 명령

시스템 정의 명령 외에도 멀티 관리 검증이 활성화된 경우 다음 명령은 기본적으로 보호되지만, 규칙을 수정하여 이러한 명령에 대한 보호를 제거할 수 있습니다.

- '보안 로그인 비밀번호
- 보안 로그인 잠금 해제
- '세트'

다음 명령은 ONTAP 9.11.1 이상 릴리스에서 보호할 수 있습니다.

'클러스터 피어 삭제' 이벤트 구성 수정 '보안 로그인 생성' '보안 로그인 삭제 보안 로그인 수정 '시스템 노드 실행 '시스템 노드 시스템 쉘' '볼륨 삭제' 볼륨 FlexCache 삭제	'볼륨 스냅샷 자동 삭제 수정' '볼륨 스냅샷 삭제' 볼륨 스냅샷 정책 추가 스케줄 볼륨 스냅샷 정책 생성 볼륨 스냅샷 정책 삭제 볼륨 스냅샷 정책 수정 볼륨 스냅샷 정책 수정 스케줄 볼륨 스냅샷 정책 제거 스케줄 '볼륨 스냅샷 복원' 'vserver peer delete

ONTAP 9.13.1부터 다음 명령을 보호할 수 있습니다.

- `volume snaplock modify`
- `security anti-ransomware volume attack clear-suspect`
- `security anti-ransomware volume disable`
- `security anti-ransomware volume pause`

ONTAP 9.14.1부터 다음 명령을 보호할 수 있습니다.

- `volume recovery-queue modify`
- `volume recovery-queue purge`
- `volume recovery-queue purge-all`
- `vserver modify`

여러 관리자의 승인 방식

보호된 작업이 MAV 보호 클러스터에 입력될 때마다 작업 실행 요청이 지정된 MAV 관리자 그룹으로 전송됩니다.

다음을 구성할 수 있습니다.

- MAV 그룹의 이름, 연락처 정보 및 관리자 수

  MAV 관리자는 클러스터 관리자 권한이 있는 RBAC 역할을 가지고 있어야 합니다.

- MAV 관리자 그룹 수
  - 각 보호된 작업 규칙에 대해 MAV 그룹이 할당됩니다.
  - 여러 MAV 그룹의 경우 지정된 규칙을 승인하는 MAV 그룹을 구성할 수 있습니다.

- 보호된 작업을 실행하는 데 필요한 MAV 승인 수입니다.
- MAV 관리자가 승인 요청에 응답해야 하는 _ 승인 만료 _ 기간.
- 요청 관리자가 작업을 완료해야 하는 _ 실행 expiry_period입니다.

이러한 매개 변수가 구성되면 이를 수정하려면 MAV 승인이 필요합니다.

MAV 관리자는 보호된 작업을 실행하기 위한 자체 요청을 승인할 수 없습니다. 즉,

- 관리자가 한 명 있는 클러스터에서는 MAV를 사용하지 않아야 합니다.
- MAV 그룹에 한 사람만 있는 경우 해당 MAV 관리자는 보호된 작업을 입력할 수 없습니다. 일반 관리자는 해당 작업을 입력해야 하며 MAV 관리자는 승인만 할 수 있습니다.
- MAV 관리자가 보호된 작업을 실행할 수 있도록 하려면 MAV 관리자 수가 필요한 승인 수보다 1개 이상 커야 합니다. 예를 들어 보호된 작업에 대해 두 번의 승인이 필요하고 MAV 관리자가 이를 실행하도록 하려면 MAV administrators 그룹에 세 명의 사용자가 있어야 합니다.

MAV 관리자는 전자 메일 알림(EMS 사용)으로 승인 요청을 받거나 요청 대기열을 쿼리할 수 있습니다. 요청을 받으면 다음 세 가지 작업 중 하나를 수행할 수 있습니다.

- 승인
- 거부(거부권)
- 무시(동작 없음)

다음과 같은 경우 전자 메일 알림이 MAV 규칙과 연결된 모든 승인자에게 전송됩니다.

- 요청이 생성됩니다.
- 요청이 승인되거나 거부되었습니다.
- 승인된 요청이 실행됩니다.

요청자가 작업에 대해 동일한 승인 그룹에 있는 경우 요청이 승인되면 이메일을 받게 됩니다.

- 참고:* 요청자는 승인 그룹에 있더라도 자신의 요청을 승인할 수 없습니다. 하지만 이메일 알림을 받을 수 있습니다. 승인 그룹에 없는 요청자(즉, MAV 관리자가 아닌)는 이메일 알림을 받지 않습니다.

보호된 작업 실행의 작동 방식

보호된 작업에 대해 실행이 승인되면 요청 사용자는 메시지가 표시될 때 작업을 계속합니다. 작업이 거부되면 요청 사용자는 계속하기 전에 요청을 삭제해야 합니다.

MAV 규칙은 RBAC 권한 이후에 평가됩니다. 따라서 작업 실행에 대한 충분한 RBAC 권한이 없는 사용자는 MAV 요청 프로세스를 시작할 수 없습니다.

관리자 승인 그룹을 관리합니다

MAV(Multi-admin verification)를 활성화하기 전에 승인 또는 거부권을 부여할 관리자가 하나 이상 포함된 관리자 승인 그룹을 만들어야 합니다. 다중 관리자 확인을 활성화한 경우 승인 그룹 구성원을 수정하려면 기존의 검증된 관리자 중 한 명의 승인이 필요합니다.

이 작업에 대해

기존 관리자를 MAV 그룹에 추가하거나 새 관리자를 만들 수 있습니다.

MAV 기능은 기존의 역할 기반 액세스 제어(RBAC) 설정을 그대로 사용합니다. 잠재적인 MAV 관리자는 MAV 관리자 그룹에 추가하기 전에 보호 작업을 실행할 수 있는 충분한 권한이 있어야 합니다. "RBAC에 대해 자세히 알아보십시오."

승인 요청이 보류 중이라는 것을 MAV 관리자에게 알리도록 MAV를 구성할 수 있습니다. 이렇게 하려면 이메일 알림(특히, 'Mail From' 및 'Mail Server' 매개 변수)을 구성하거나 이러한 매개 변수를 지워 알림을 비활성화해야 합니다. 이메일 알림이 없으면 MAV 관리자는 승인 대기열을 수동으로 확인해야 합니다.

System Manager 절차

처음으로 MAV 승인 그룹을 만들려면 System Manager 절차 - 를 참조하십시오 "다중 관리 검증을 활성화합니다."

기존 승인 그룹을 수정하거나 추가 승인 그룹을 만들려면:

1. 여러 관리자 검증을 받을 관리자 식별
   a. 클러스터 > 설정 * 을 클릭합니다
   b. 을 클릭합니다 → 사용자 및 역할 * 옆에 있습니다
   c. 을 클릭합니다 + Add 사용자 * 에서
   d. 필요에 따라 명단을 수정합니다.

      자세한 내용은 을 참조하십시오 "관리자 액세스 제어."

2. MAV 승인 그룹 생성 또는 수정:
   a. 클러스터 > 설정 * 을 클릭합니다
   b. 을 클릭합니다 → 보안 * 섹션의 * 다중 관리자 승인 * 옆에 있습니다. (이 표시됩니다 ⚙ MAV가 아직 구성되지 않은 경우 아이콘).
      - 이름: 그룹 이름을 입력합니다.
      - 승인자: 사용자 목록에서 승인자를 선택합니다.
      - 이메일 주소: 이메일 주소를 입력합니다.
      - Default group(기본 그룹): 그룹을 선택합니다.

MAV가 활성화되면 기존 구성을 편집하려면 MAV 승인이 필요합니다.

CLI 절차

1. 'Mail From' 및 'Mail Server' 매개 변수에 값이 설정되어 있는지 확인합니다. 입력:

   이벤트 구성 쇼

   디스플레이는 다음과 비슷해야 합니다.

```
cluster01::> event config show
                           Mail From:  admin@localhost
                         Mail Server:  localhost
                           Proxy URL:  -
                          Proxy User:  -
 Publish/Subscribe Messaging Enabled:  true
```

이러한 매개 변수를 구성하려면 다음을 입력합니다.

"이벤트 구성 수정-메일-보낸 사람_이메일_주소_-메일-서버_서버_이름_'

2. 여러 관리자 검증을 받을 관리자 식별

원하는 사항	이 명령을 입력합니다
현재 관리자를 표시합니다	'보안 로그인 쇼'
현재 관리자의 자격 증명을 수정합니다	'Security login modify_<parameters>_'
새 관리자 계정을 만듭니다	'Security login create-user-or-group-name_admin_name_-application ssh-authentication-method password

3. MAV 승인 그룹 생성:

   security multi-admin-verify approval-group create [-vserver *svm_name*] -name *group_name* -approvers *approver1*[,*approver2*…] [[-email *address1*], *address1*…]

   - '-vserver' - 이번 릴리즈에서는 관리 SVM만 지원됩니다.
   - '-name' - 최대 64자의 MAV 그룹 이름입니다.
   - '-승인자' - 하나 이상의 승인자 목록입니다.
   - '-email' - 요청을 작성, 승인, 거부하거나 실행할 때 통지되는 하나 이상의 이메일 주소입니다.
     - 예: * 다음 명령을 실행하면 멤버 2개와 관련 이메일 주소가 있는 MAV 그룹이 생성됩니다.

```
cluster-1::> security multi-admin-verify approval-group create -name
mav-grp1 -approvers pavan,julia -email pavan@myfirm.com,julia@myfirm.com
```

4. 그룹 생성 및 구성원 자격 확인:

   security multi-admin-verify approval-group show

   - 예: *

```
cluster-1::> security multi-admin-verify approval-group show
Vserver  Name        Approvers        Email
-------  ---------------- ------------------
------------------------------------------------------------
svm-1    mav-grp1   pavan,julia      email
pavan@myfirm.com,julia@myfirm.com
```

이 명령을 사용하여 초기 MAV 그룹 구성을 수정합니다.

- 참고: * 모두 실행 전에 MAV 관리자의 승인이 필요합니다.

원하는 사항	이 명령을 입력합니다
그룹 특성을 수정하거나 기존 구성원 정보를 수정합니다	'Security multi-admin - Verify approval-group modify[*parameters*]'
구성원을 추가 또는 제거합니다	'보안 다중 관리자 - 승인 확인 - 그룹 바꾸기[-vserver_svm_name_] - name_group_name_[-approver-to-add_approver1_[,*approver2*…]] [-approver-to-remove_approver1_[,*approver2*…]'
그룹을 삭제합니다	'보안 multi-admin-verify approval-group delete[-vserver_svm_name_]-name_group_name_'

다중 관리 확인을 활성화 및 비활성화합니다

MAV(Multi-admin verification)를 명시적으로 활성화해야 합니다. 다중 관리 확인을 사용하도록 설정한 후에는 MAV 승인 그룹(MAV 관리자)의 관리자가 이를 삭제해야 합니다.

이 작업에 대해

MAV가 활성화되면 MAV를 수정하거나 사용하지 않도록 하려면 MAV 관리자의 승인이 필요합니다.

> MAV 관리자의 승인 없이 다중 관리 검증 기능을 사용하지 않도록 설정해야 하는 경우 NetApp Support에 다음 기술 자료 문서를 멘션하십시오. "MAV 관리자를 사용할 수 없는 경우 다중 관리 확인을 비활성화하는 방법".

MAV를 사용하도록 설정하면 다음 매개 변수를 전역적으로 지정할 수 있습니다.

승인 그룹

글로벌 승인 그룹 목록 MAV 기능을 사용하려면 하나 이상의 그룹이 필요합니다.

> ARP(Autonomous 랜섬웨어Protection)와 함께 MAV를 사용하는 경우 ARP 일시 중지, 비활성화 및 의심되는 요청을 승인하는 신규 또는 기존 승인 그룹을 정의하십시오.

필수 승인자

보호된 작업을 실행하는 데 필요한 승인자 수입니다. 기본 및 최소 숫자는 1입니다.

> 필요한 승인자 수는 기본 승인 그룹의 총 고유 승인자 수보다 적어야 합니다.

승인 만료(시간, 분, 초)

MAV 관리자가 승인 요청에 응답해야 하는 기간. 기본값은 1시간(1시간)이고, 지원되는 최소 값은 1초(1초)이며, 지원되는 최대 값은 14일(14D)입니다.

실행 만료(시간, 분, 초)

요청 관리자가 완료해야 하는 기간:: 작업. 기본값은 1시간(1시간)이고, 지원되는 최소 값은 1초(1초)이며, 지원되는 최대 값은 14일(14D)입니다.

또한 특정 매개 변수에 대해 이러한 매개 변수를 재정의할 수도 있습니다 "작업 규칙."

System Manager 절차

1. 여러 관리자 검증을 받을 관리자 식별
   a. 클러스터 > 설정 * 을 클릭합니다
   b. 을 클릭합니다 → 사용자 및 역할 * 옆에 있습니다
   c. 을 클릭합니다 + Add 사용자 * 에서
   d. 필요에 따라 명단을 수정합니다.

      자세한 내용은 을 참조하십시오 "관리자 액세스 제어."

2. 하나 이상의 승인 그룹을 생성하고 하나 이상의 규칙을 추가하여 다중 관리 검증을 활성화합니다.
   a. 클러스터 > 설정 * 을 클릭합니다
   b. 을 클릭합니다 ⚙ 보안 * 섹션의 * 다중 관리자 승인 * 옆에 있습니다.
   c. 을 클릭합니다 + Add 하나 이상의 승인 그룹을 추가합니다.
      - 이름 - 그룹 이름을 입력합니다.
      - 승인자 - 사용자 목록에서 승인자를 선택합니다.
      - 이메일 주소 – 이메일 주소를 입력합니다.
      - Default group(기본 그룹) – 그룹을 선택합니다.
   d. 하나 이상의 규칙을 추가합니다.
      - 작업 - 목록에서 지원되는 명령을 선택합니다.
      - 쿼리 - 원하는 명령 옵션 및 값을 입력합니다.
      - 선택적 매개 변수입니다. 글로벌 설정을 적용하려면 비워 두거나 글로벌 설정을 재정의하기 위해 특정 규칙에 다른 값을 할당합니다.
        - 승인자 수가 필요합니다
        - 승인 그룹
   e. 기본값을 보거나 수정하려면 * 고급 설정 * 을 클릭합니다.

    - 필요한 승인자 수(기본값: 1)
    - 실행 요청 만료(기본값: 1시간)
    - 승인 요청 만료(기본값: 1시간)
    - 메일 서버 *
    - 발신 이메일 주소 *
        - 이렇게 하면 "알림 관리"에서 관리되는 이메일 설정이 업데이트됩니다. 아직 구성되지 않은 경우 설정하라는 메시지가 표시됩니다.

f. MAV 초기 구성을 완료하려면 * 활성화 * 를 클릭합니다.

초기 구성 후 현재 MAV 상태가 * Multi-Admin Approval * (다중 관리자 승인 *) 타일에 표시됩니다.

- 상태(활성화됨 또는 아님)
- 승인이 필요한 활성 작업
- 보류 중인 미결 요청 수입니다

를 클릭하여 기존 설정을 표시할 수 있습니다 →. 기존 구성을 편집하려면 MAV 승인이 필요합니다.

다중 관리 확인을 비활성화하려면:

1. 클러스터 > 설정 * 을 클릭합니다
2. 을 클릭합니다 ⚙ 보안 * 섹션의 * 다중 관리자 승인 * 옆에 있습니다.
3. 사용 전환 단추를 클릭합니다.

   이 작업을 완료하려면 MAV 승인이 필요합니다.

CLI 절차

CLI에서 MAV 기능을 활성화하기 전에 하나 이상의 기능이 있어야 합니다 "MAV 관리자 그룹" 이(가) 생성되어야 합니다.

원하는 사항	이 명령을 입력합니다
MAV 기능을 활성화합니다	'보안 multi-admin-verify modify-approval-group1_[,*group2*…] [-필수-승인자_nn_] - 활성화된 참 [-실행-만료 [*nn*h] [*nn*m] [*nn*s] [- 승인-만료 [*nn*h] [*nn*s] [*nn*s]] • 예 *: 다음 명령을 실행하면 1개의 승인 그룹, 2개의 필수 승인자 및 기본 만료 기간이 포함된 MAV가 활성화됩니다. `cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true` 최소 1개를 추가하여 초기 구성을 완료합니다 "작업 규칙."
MAV 구성 수정(MAV 승인 필요)	'보안 Multi-admin-Verify approval-group modify [-approval-group1_[,*group2*…] [-필수-승인자_nn_] [-실행-만료 [*nn*h] [*nn*m] [*nn*s] [- 승인-만료 [*nn*h] [*nn*s]]

MAV 기능을 확인합니다	'보안 멀티-관리-검증 쇼'
	
	• 예: *
	
	`cluster-1::> security multi-admin-verify show`
	`Is Required Execution`
	`Approval Approval`
	`Enabled Approvers Expiry Expiry`
	`Groups`
	`------- --------- ---------`
	`-------- ----------`
	`true 2 1h 1h`
	`mav-grp1`

MAV 기능 비활성화(MAV 승인 필요)	'보안 멀티-관리-검증 수정-사용 안 함

보호된 작업 규칙을 관리합니다

MAV(Multi-admin verification) 규칙을 만들어 승인이 필요한 작업을 지정합니다. 작업이 시작될 때마다 보호된 작업이 차단되고 승인 요청이 생성됩니다.

적절한 RBAC 기능이 있는 관리자가 MAV를 활성화하기 전에 규칙을 만들 수 있지만, M5V가 활성화되면 규칙 집합을

수정하려면 MAV 승인이 필요합니다.

작업당 하나의 MAV 규칙만 만들 수 있습니다. 예를 들어 여러 개를 만들 수 없습니다 `volume-snapshot-delete` 규칙. 원하는 규칙 제약 조건은 하나의 규칙 내에 포함되어야 합니다.

규칙으로 보호된 명령

ONTAP 9.11.1부터 다음 명령을 보호하는 규칙을 만들 수 있습니다.

'클러스터 피어 삭제'	'볼륨 스냅샷 자동 삭제 수정'
이벤트 구성 수정	'볼륨 스냅샷 삭제'
'보안 로그인 생성'	볼륨 스냅샷 정책 추가 스케줄
'보안 로그인 삭제	볼륨 스냅샷 정책 생성
보안 로그인 수정	볼륨 스냅샷 정책 삭제
'시스템 노드 실행	볼륨 스냅샷 정책 수정
'시스템 노드 시스템 쉘'	볼륨 스냅샷 정책 수정 스케줄
'볼륨 삭제'	볼륨 스냅샷 정책 제거 스케줄
볼륨 FlexCache 삭제	'볼륨 스냅샷 복원'
	'vserver peer delete

ONTAP 9.13.1부터 다음 명령을 보호하는 규칙을 만들 수 있습니다.

- `volume snaplock modify`
- `security anti-ransomware volume attack clear-suspect`
- `security anti-ransomware volume disable`
- `security anti-ransomware volume pause`

ONTAP 9.14.1부터 다음 명령을 보호하는 규칙을 만들 수 있습니다.

- `volume recovery-queue modify`
- `volume recovery-queue purge`
- `volume recovery-queue purge-all`
- `vserver modify`

MAV 시스템 기본 명령에 대한 규칙인 입니다 `security multi-admin-verify` "명령"변경할 수 없습니다.

시스템 정의 명령 외에도 멀티 관리 검증이 활성화된 경우 다음 명령은 기본적으로 보호되지만, 규칙을 수정하여 이러한 명령에 대한 보호를 제거할 수 있습니다.

- '보안 로그인 비밀번호
- 보안 로그인 잠금 해제
- '세트'

규칙 제약 조건

규칙을 만들 때 선택적으로 을 지정할 수 있습니다 `-query` 명령 기능의 하위 집합으로 요청을 제한하는 옵션입니다. 를 클릭합니다 `-query` 옵션을 사용하여 SVM, 볼륨, 스냅샷 이름과 같은 구성 요소를 제한할 수도 있습니다.

예를 들어 의 을 참조하십시오 `volume snapshot delete` 명령, `-query` 로 설정할 수 있습니다 `-snapshot !hourly*,!daily*,!weekly*`즉, 매시간, 일별 또는 주별 속성으로 접두사가 지정된 볼륨 스냅샷이 MAV 보호에서 제외됩니다.

```
smci-vsim20::> security multi-admin-verify rule show
                                              Required  Approval
Vserver Operation                             Approvers Groups
------- ------------------------------------- --------- -------------
vs01    volume snapshot delete                -         -
          Query: -snapshot !hourly*,!daily*,!weekly*
```

제외된 구성 요소는 MAV로 보호되지 않으므로 관리자가 삭제하거나 이름을 바꿀 수 있습니다.

기본적으로 규칙은 해당 을 지정합니다 `security multi-admin-verify request create` *"protected_operation"* 보호된 작업이 입력되면 명령이 자동으로 생성됩니다. 이 기본값을 수정하여 을 요구할 수 있습니다 `request create` 명령을 별도로 입력합니다.

기본적으로 규칙별 예외를 지정할 수 있지만 규칙은 다음과 같은 전역 MAV 설정을 상속합니다.

- 필요한 승인자 수
- 승인 그룹
- 승인 만료 기간
- 실행 만료 기간

System Manager 절차

보호된 작업 규칙을 처음으로 추가하려면 에 System Manager 절차를 참조하십시오 "다중 관리 검증을 활성화합니다."

기존 규칙 집합을 수정하려면 다음을 수행합니다.

1. 클러스터 > 설정 * 을 선택합니다.
2. 를 선택합니다 ⚙ 보안 * 섹션의 * 다중 관리자 승인 * 옆에 있습니다.
3. 를 선택합니다 + Add 규칙을 하나 이상 추가하려면 기존 규칙을 수정하거나 삭제할 수도 있습니다.
   - 작업 - 목록에서 지원되는 명령을 선택합니다.
   - 쿼리 - 원하는 명령 옵션 및 값을 입력합니다.

- 선택적 매개 변수 – 글로벌 설정을 적용하려면 비워 두거나 글로벌 설정을 재정의하기 위해 특정 규칙에 다른 값을 할당합니다.
  - 승인자 수가 필요합니다
  - 승인 그룹

CLI 절차

> 모든 '보안 멀티 관리-검증 규칙' 명령은 '보안 멀티-관리-검증 규칙 표시'를 제외하고 실행 전에 MAV 관리자의 승인이 필요합니다.

원하는 사항	이 명령을 입력합니다
규칙을 만듭니다	'Security multi-admin-verify rule create-operation_"protected_operation"*[-query_operation_subset*][*parameters*]'

현재 관리자의 자격 증명을 수정합니다	`security login modify <parameters>`
	• 예 *: 다음 규칙에 따라 루트 볼륨을 삭제해야 합니다.
	`security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"`

규칙을 수정합니다	'Security multi-admin-verify rule modify -operation_“protected_operation”*[_parameters*]'
규칙을 삭제합니다	'Security multi-admin - verify rule delete - operation_“protected_operation” _'
규칙 표시	'보안 멀티-관리-검증 규칙 표시'

명령 구문에 대한 자세한 내용은 보안 다중 관리 확인 규칙 man 페이지를 참조하십시오.

보호된 작업의 실행을 요청합니다

MAV(Multi-admin verification)를 사용하도록 설정된 클러스터에서 보호 작업 또는 명령을 시작하면 ONTAP가 자동으로 작업을 인터셉트하여 MAV 승인 그룹(MAV 관리자)의 한 명 이상의 관리자가 승인해야 하는 요청을 생성하도록 요청합니다. 또는 대화 상자 없이 MAV 요청을 만들 수 있습니다.

요청이 승인되면 쿼리에 응답하여 요청 만료 기간 내에 작업을 완료해야 합니다. 거부되거나 요청 또는 만료 기간이 초과된 경우 요청을 삭제하고 다시 제출해야 합니다.

MAV 기능은 기존 RBAC 설정을 그대로 사용합니다. 즉, 관리자 역할에 MAV 설정과 관계없이 보호된 작업을 실행할 수 있는 충분한 권한이 있어야 합니다. "RBAC에 대해 자세히 알아보십시오".

MAV 관리자인 경우 보호된 작업을 실행하기 위한 요청도 MAV 관리자의 승인을 받아야 합니다.

System Manager 절차

사용자가 메뉴 항목을 클릭하여 작업을 시작하고 작업을 보호하는 경우 승인 요청이 생성되고 다음과 유사한 알림이 사용자에게 표시됩니다.

```
Approval request to delete the volume was sent.
Track the request ID 356 from Events & Jobs > Multi-Admin Requests.
```

MAV가 활성화된 경우 사용자의 로그인 ID 및 MAV 역할(승인자 여부)에 따라 보류 중인 요청을 표시하는 * 다중 관리자 요청 * 창을 사용할 수 있습니다. 보류 중인 각 요청에 대해 다음 필드가 표시됩니다.

- 작동
- 색인(숫자)
- 상태(보류, 승인됨, 거부됨, 실행됨 또는 만료됨)

  한 승인자가 요청을 거부하면 추가 작업이 불가능합니다.

- 쿼리(요청된 작업의 매개 변수 또는 값)
- 사용자를 요청하는 중입니다
- 요청이 에 만료됩니다
- (수) 보류 중인 승인자
- (수) 잠재적 승인자

요청이 승인되면 요청 사용자는 만료 기간 내에 작업을 다시 시도할 수 있습니다.

사용자가 승인 없이 작업을 재시도하면 다음과 유사한 알림이 표시됩니다.

```
Request to perform delete operation is pending approval.
Retry the operation after request is approved.
```

CLI 절차

1. 보호된 작업을 직접 입력하거나 MAV 요청 명령을 사용합니다.
   - 예제 – 볼륨을 삭제하려면 다음 명령 중 하나를 입력합니다. *
     - '볼륨 삭제'

```
cluster-1::*> volume delete -volume vol1 -vserver vs0

Warning: This operation requires multi-admin verification. To
create a
         verification request use "security multi-admin-verify
request
         create".

         Would you like to create a request for this operation?
          {y|n}: y

Error: command failed: The security multi-admin-verify request
(index 3) is
       auto-generated and requires approval.
```

- 보안 다중 관리 - 확인 요청은 "볼륨 삭제"를 생성합니다

```
Error: command failed: The security multi-admin-verify request
(index 3)
       requires approval.
```

2. 요청의 상태를 확인하고 MAV 통지에 응답합니다.

   a. 요청이 승인되면 CLI 메시지에 응답하여 작업을 완료합니다.

      - 예: *

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: approved
Required Approvers: 1
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: admin2
       User Vetoed: -
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Info: Volume "vol1" in Vserver "vs0" will be marked as deleted and
placed in the volume recovery queue. The space used by the volume
will be recovered only after the retention period of 12 hours has
completed. To recover the space immediately, get the volume name
using (privilege:advanced) "volume recovery-queue show vol1_*" and
then "volume recovery-queue purge -vserver vs0 -volume <volume_name>"
command. To recover the volume use the (privilege:advanced) "volume
recovery-queue recover -vserver vs0       -volume <volume_name>"
command.

Warning: Are you sure you want to delete volume "vol1" in Vserver
"vs0" ?
{y|n}: y
```

b. 요청이 거부되거나 만료 기간이 지난 경우 요청을 삭제하고 다시 제출하거나 MAV 관리자에게 문의하십시오.

   - 예: *

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: vetoed
Required Approvers: 1
 Pending Approvers: 1
   Approval Expiry: 2/25/2022 14:38:47
  Execution Expiry: -
         Approvals: -
       User Vetoed: admin2
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:38:47
     Time Approved: -
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Error: command failed: The security multi-admin-verify request (index 3)
hasbeen vetoed. You must delete it and create a new verification
request.
To delete, run "security multi-admin-verify request delete 3".
```

보호된 작업 요청을 관리합니다

MAV 승인 그룹(MAV 관리자)의 관리자가 보류 중인 작업 실행 요청을 통지받으면 정해진 기간(승인 만료) 내에 승인 또는 거부 메시지로 응답해야 합니다. 충분한 수의 승인을 받지 못한 경우 요청자는 요청을 삭제하고 다른 요청을 해야 합니다.

이 작업에 대해

승인 요청은 인덱스 번호로 식별되며, 이 번호는 이메일 메시지와 요청 대기열의 디스플레이에 포함됩니다.

요청 대기열의 다음 정보를 표시할 수 있습니다.

작동
: 요청이 생성되는 보호된 작업입니다.

쿼리
: 사용자가 작업을 적용하려는 개체(또는 개체)입니다.

상태
: 요청의 현재 상태, 보류, 승인, 거부, 만료됨, 실행됨. 한 승인자가 요청을 거부하면 추가 작업이 불가능합니다.

필수 승인자

요청을 승인하는 데 필요한 MAV 관리자 수 사용자는 작업 규칙에 필요한 승인자 매개 변수를 설정할 수 있습니다. 사용자가 필수 승인자를 규칙에 설정하지 않으면 전역 설정의 필수 승인자가 적용됩니다.

보류 중인 승인자

요청을 승인하기 위해 승인 요청을 승인해야 하는 MAV 관리자 수.

승인 만료

MAV 관리자가 승인 요청에 응답해야 하는 기간. 권한이 있는 사용자는 작업 규칙에 대한 승인 만료 기간을 설정할 수 있습니다. 규칙에 대해 승인-만료가 설정되어 있지 않으면 전역 설정의 승인-만료가 적용됩니다.

실행 만료

요청 관리자가 작업을 완료해야 하는 기간. 권한이 있는 사용자는 작업 규칙에 대해 실행 만료 기간을 설정할 수 있습니다. 규칙에 대해 execution-expiry를 설정하지 않으면 전역 설정에서의 execution-expiry가 적용됩니다.

사용자가 승인했습니다

요청을 승인한 MAV 관리자

사용자가 거부했습니다

요청에 거부권을 행사한 MAV 관리자

스토리지 **VM(SVM)**

요청이 연결된 SVM 이 릴리즈에서는 admin SVM만 지원합니다.

사용자가 요청되었습니다

요청을 생성한 사용자의 사용자 이름입니다.

생성 시간

요청이 생성된 시간입니다.

시간이 승인되었습니다

요청 상태가 승인으로 변경된 시간입니다.

설명

요청과 관련된 모든 메모.

사용자 허용

요청이 승인된 보호된 작업을 수행하도록 허용된 사용자 목록입니다. '사용자 허용'이 비어 있으면 적절한 권한을 가진 모든 사용자가 작업을 수행할 수 있습니다.

1000개의 요청이 한계에 도달하거나 만료된 요청에 대해 만료된 시간이 8시간을 초과할 경우 만료되거나 실행된 모든 요청이 삭제됩니다. 거부된 요청은 만료됨으로 표시되면 삭제됩니다.

System Manager 절차

MAV 관리자는 승인 요청 세부 정보, 요청 만료 기간 및 요청을 승인 또는 거부할 수 있는 링크가 포함된 전자 메일 메시지를 수신합니다. 이메일의 링크를 클릭하여 승인 대화 상자에 액세스하거나 System Manager의 * 이벤트 및 작업 > 요청 * 으로 이동할 수 있습니다.

복수 관리자 확인이 활성화된 경우 사용자의 로그인 ID 및 MAV 역할(승인자 여부)을 기준으로 보류 중인 요청을 표시하는 * 요청 * 창을 사용할 수 있습니다.

- 작동
- 색인(숫자)
- 상태(보류, 승인됨, 거부됨, 실행됨 또는 만료됨)

  한 승인자가 요청을 거부하면 추가 작업이 불가능합니다.

- 쿼리(요청된 작업의 매개 변수 또는 값)
- 사용자를 요청하는 중입니다
- 요청이 에 만료됩니다
- (수) 보류 중인 승인자
- (수) 잠재적 승인자

MAV 관리자는 이 창에 개별 작업 또는 선택한 작업 그룹을 승인, 거부 또는 삭제할 수 있는 추가 컨트롤이 있습니다. 그러나 MAV 관리자가 요청 사용자인 경우 자신의 요청을 승인, 거부 또는 삭제할 수 없습니다.

CLI 절차

1. 대기 중인 요청을 이메일로 통지할 경우 요청의 인덱스 번호 및 승인 만료 기간을 기록합니다. 색인 번호는 아래에 언급된 * show * 또는 * show-pending * 옵션을 사용하여 표시할 수도 있습니다.
2. 요청을 승인 또는 거부하십시오.

원하는 사항	이 명령을 입력합니다
요청을 승인합니다	'보안 multi-admin-verify request approve_nn_'
요청을 거부하십시오	'보안 다수 관리 - 확인 요청 거부_nn_'
모든 요청, 보류 중인 요청 또는 단일 요청을 표시합니다	'보안 다중 관리 - 확인 요청{show
show-pending}[*nn*] {-fields_field1_[,*field2*…] [-instance]}' 대기열에 있는 모든 요청 또는 보류 중인 요청만 표시할 수 있습니다. 인덱스 번호를 입력하면 해당 에 대한 정보만 표시됩니다. 특정 필드('-fields' 매개 변수 사용) 또는 모든 필드('-instance' 매개 변수 사용)에 대한 정보를 표시할 수 있습니다.	요청을 삭제합니다

예**:**

다음 시퀀스는 MAV 관리자가 이미 하나의 승인이 있는 색인 번호 3의 요청 이메일을 받은 후에 요청을 승인합니다.

```
          cluster1::> security multi-admin-verify request show-pending
                                          Pending
Index Operation      Query State   Approvers Requestor
----- -------------- ----- ------- --------- ---------
    3 volume delete  -     pending 1         julia


cluster-1::> security multi-admin-verify request approve 3

cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -
             State: approved
Required Approvers: 2
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: mav-admin2
       User Vetoed: -
           Vserver: cluster-1
    User Requested: julia
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -
```

예:

다음 시퀀스는 MAV 관리자가 이미 하나의 승인이 있는 색인 번호 3의 요청 이메일을 받은 후에 요청을 거부한다.

```
      cluster1::> security multi-admin-verify request show-pending
                                      Pending
Index Operation      Query State   Approvers Requestor
----- -------------- ----- ------- --------- ---------
    3 volume delete  -     pending 1         pavan


cluster-1::> security multi-admin-verify request veto 3

cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -
             State: vetoed
Required Approvers: 2
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: mav-admin1
       User Vetoed: mav-admin2
           Vserver: cluster-1
    User Requested: pavan
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -
```

OAuth 2.0을 사용한 인증 및 권한 부여

ONTAP OAuth 2.0 구축 개요

ONTAP 9.14부터 OAuth 2.0(Open Authorization 2.0) 프레임워크를 사용하여 ONTAP 클러스터에 대한 액세스를 제어할 수 있습니다. 이 기능은 ONTAP CLI, System Manager, REST API를 포함한 모든 ONTAP 관리 인터페이스를 사용하여 구성할 수 있습니다. 그러나 OAuth 2.0 권한 부여 및 액세스 제어 결정은 클라이언트가 REST API를 사용하여 ONTAP에 액세스할 때만 적용할 수 있습니다.

> OAuth 2.0 지원은 ONTAP 9.14.0에서 처음 도입되었으며 사용 중인 ONTAP 릴리스에 따라 가용성이 달라집니다. 를 참조하십시오 "ONTAP 릴리즈 노트" 를 참조하십시오.

기능 및 이점

ONTAP와 함께 OAuth 2.0을 사용할 때의 주요 기능과 이점은 다음과 같습니다.

OAuth 2.0 표준을 지원합니다

OAuth 2.0은 업계 표준 인증 프레임워크입니다. 서명된 액세스 토큰을 사용하여 보호된 리소스에 대한 액세스를 제한하고 제어하는 데 사용됩니다. OAuth 2.0을 사용하면 다음과 같은 여러 이점이 있습니다.

- 권한 부여 구성에 대한 다양한 옵션
- 암호를 포함한 클라이언트 자격 증명을 공개하지 마십시오
- 토큰은 구성에 따라 만료되도록 설정할 수 있습니다
- REST API와 함께 사용하는 데 가장 적합합니다

널리 사용되는 여러 인증 서버를 사용하여 테스트했습니다

ONTAP 구현은 OAuth 2.0 호환 인증 서버와 호환되도록 설계되었습니다. 다음과 같은 일반적인 서버 또는 서비스를 사용하여 테스트되었습니다.

- Auth0
- ADFS(Active Directory Federation Service)
- 키클로크

여러 개의 동시 인증 서버 지원

단일 ONTAP 클러스터에 대해 최대 8개의 인증 서버를 정의할 수 있습니다. 따라서 다양한 보안 환경의 요구 사항을 충족할 수 있는 유연성을 제공합니다.

나머지 역할과의 통합

ONTAP 권한 부여 결정은 궁극적으로 사용자 또는 그룹에 할당된 REST 역할을 기반으로 합니다. 이러한 역할은 액세스 토큰에서 자체 포함된 범위 또는 Active Directory 또는 LDAP 그룹과 함께 로컬 ONTAP 정의를 기반으로 수행됩니다.

보낸 사람 제한 액세스 토큰을 사용하는 옵션입니다

클라이언트 인증을 강화하는 MTL(상호 전송 계층 보안)을 사용하도록 ONTAP 및 인증 서버를 구성할 수 있습니다. OAuth 2.0 액세스 토큰은 원래 발급된 클라이언트에서만 사용됩니다. 이 기능은 FAPI 및 MITRE에서 수립한 보안 권장 사항을 포함하여 몇 가지 일반적인 보안 권장 사항을 지원하고 그에 맞게 조정됩니다.

구현 및 구성

OAuth 2.0 구현 및 구성의 여러 측면을 개괄적으로 살펴보면 시작할 때 고려해야 할 사항이 있습니다.

ONTAP 내의 **OAuth 2.0** 엔티티

OAuth 2.0 권한 부여 프레임워크는 데이터 센터 또는 네트워크 내의 실제 요소 또는 가상 요소에 매핑할 수 있는 여러 엔터티를 정의합니다. OAuth 2.0 엔터티 및 ONTAP에 대한 적응은 아래 표에 나와 있습니다.

OAuth 2.0 엔티티	설명
리소스	내부 ONTAP 명령을 통해 ONTAP 리소스에 액세스하는 REST API 엔드포인트입니다.
리소스 소유자	보호된 리소스를 생성했거나 기본적으로 소유한 ONTAP 클러스터 사용자입니다.
리소스 서버	ONTAP 클러스터인 보호된 리소스의 호스트입니다.
클라이언트	리소스 소유자를 대신하거나 리소스 소유자의 권한이 있는 REST API 끝점에 대한 액세스를 요청하는 응용 프로그램입니다.

OAuth 2.0 엔티티	설명
인증 서버	일반적으로 액세스 토큰 발급 및 관리 정책 적용을 담당하는 전용 서버입니다.

핵심 **ONTAP** 구성

OAuth 2.0을 활성화하고 사용하려면 ONTAP 클러스터를 구성해야 합니다. 여기에는 인증 서버에 대한 연결 설정 및 필요한 ONTAP 인증 구성 정의가 포함됩니다. 다음과 같은 관리 인터페이스를 사용하여 이 구성을 수행할 수 있습니다.

- ONTAP 명령줄 인터페이스입니다
- 시스템 관리자
- ONTAP REST API를 참조하십시오

환경 및 지원 서비스

ONTAP 정의 외에 인증 서버도 구성해야 합니다. 그룹-역할 매핑을 사용하는 경우 Active Directory 그룹 또는 이에 상응하는 LDAP도 구성해야 합니다.

지원되는 **ONTAP** 클라이언트

ONTAP 9.14부터 REST API 클라이언트는 OAuth 2.0을 사용하여 ONTAP에 액세스할 수 있습니다. REST API 호출을 실행하기 전에 인증 서버에서 액세스 토큰을 얻어야 합니다. 그런 다음 클라이언트는 HTTP 승인 요청 헤더를 사용하여 이 토큰을 _bearer token_으로 ONTAP 클러스터에 전달합니다. 필요한 보안 수준에 따라 클라이언트에서 인증서를 만들고 설치하여 MTL을 기반으로 보낸 사람 제한 토큰을 사용할 수도 있습니다.

선택된 용어

ONTAP를 사용하여 OAuth 2.0 배포를 살펴보기 시작하면 몇 가지 용어를 익히는 것이 좋습니다. 을 참조하십시오 "추가 리소스" OAuth 2.0에 대한 자세한 내용을 보려면 링크를 클릭하십시오.

액세스 토큰

인증 서버에서 발급되고 OAuth 2.0 클라이언트 응용 프로그램에서 보호된 리소스에 대한 액세스를 요청하는 데 사용하는 토큰입니다.

JSON 웹 토큰

액세스 토큰을 포맷하는 데 사용되는 표준입니다. JSON은 OAuth 2.0 클레임을 세 개의 주요 섹션으로 정렬한 작은 형식으로 표현하는 데 사용됩니다.

보낸 사람 제한 액세스 토큰

MTL(상호 전송 계층 보안) 프로토콜을 기반으로 하는 선택적 기능입니다. 토큰에 추가 확인 클레임을 사용하면 액세스 토큰이 원래 발급된 클라이언트에서만 액세스 토큰을 사용할 수 있습니다.

JSON 웹 키 집합입니다

JWKS는 ONTAP에서 클라이언트가 제시한 JWT 토큰을 확인하기 위해 사용하는 공개 키 모음입니다. 키 세트는 일반적으로 전용 URI를 통해 인증 서버에서 사용할 수 있습니다.

범위

범위를 사용하면 ONTAP REST API와 같은 보호된 리소스에 대한 응용 프로그램의 액세스를 제한하거나 제어할 수 있습니다. 액세스 토큰은 문자열로 표시됩니다.

ONTAP REST 역할입니다

ONTAP 9.6에 도입된 REST 역할은 ONTAP RBAC 프레임워크의 핵심 부분입니다. 이러한 역할은 ONTAP에서 여전히 지원하는 이전의 기존 역할과 다릅니다. ONTAP의 OAuth 2.0 구현은 REST 역할만 지원합니다.

HTTP 권한 부여 헤더

REST API 호출의 일부로 클라이언트 및 관련 권한을 식별하기 위한 HTTP 요청에 포함된 헤더 인증 및 권한 부여가 수행되는 방법에 따라 몇 가지 기능 또는 구현이 가능합니다. ONTAP에 OAuth 2.0 액세스 토큰을 제시할 때 토큰은 *bearer token* 으로 식별됩니다.

HTTP 기본 인증

초기 HTTP 인증 기법은 여전히 ONTAP에서 지원됩니다. 일반 텍스트 자격 증명(사용자 이름 및 암호)은 콜론으로 연결되고 base64로 인코딩됩니다. 이 문자열은 승인 요청 헤더에 배치되고 서버로 전송됩니다.

파피

금융 업계를 위한 프로토콜, 데이터 스키마 및 보안 권장 사항을 제공하는 OpenID Foundation의 작업 그룹입니다. 이 API는 원래 금융 등급 API로 알려져 있었습니다.

마이터

미국 공군과 미국 정부에 기술 및 보안 지침을 제공하는 비영리 민간 회사입니다.

추가 리소스

몇 가지 추가 리소스가 아래에 제공됩니다. OAuth 2.0 및 관련 표준에 대한 자세한 내용을 보려면 이러한 사이트를 검토해야 합니다.

프로토콜 및 표준

- "RFC 6749: OAuth 2.0 인증 프레임워크"
- "RFC 7519: JSON 웹 토큰(JWT)"
- "RFC 7523: OAuth 2.0 클라이언트 인증 및 권한 부여에 대한 JSON 웹 토큰(JWT) 프로파일"
- "RFC 7662: OAuth 2.0 토큰 소개"
- "RFC 7800: JWT에 대한 소유 증명 키"
- "RFC 8705: OAuth 2.0 상호 TLS 클라이언트 인증 및 인증서 바인딩된 액세스 토큰"

조직

- "OpenID 파운데이션"
- "FAPI 작업 그룹"
- "마이터"
- "IANA-JWT의 약어입니다"

제품 및 서비스

- "Auth0"
- "ADFS 개요"
- "키클로크"

추가 도구 및 유틸리티

- "Auth0에 의한 JWT"
- "OpenSSL 을 참조하십시오"

NetApp 설명서 및 리소스

- "ONTAP 자동화" 문서화

개념

인증 서버 및 액세스 토큰

인증 서버는 OAuth 2.0 권한 부여 프레임워크 내에서 중앙 구성 요소로 몇 가지 중요한 기능을 수행합니다.

OAuth 2.0 인증 서버

권한 부여 서버는 주로 액세스 토큰을 만들고 서명합니다. 이러한 토큰에는 클라이언트 응용 프로그램이 보호된 리소스에 선택적으로 액세스할 수 있도록 하는 ID 및 권한 부여 정보가 포함되어 있습니다. 서버는 일반적으로 서로 격리되며 독립 실행형 전용 서버나 대규모 ID 및 액세스 관리 제품의 일부로 구현하는 등 여러 가지 방법으로 구현할 수 있습니다.

> 인증 서버에는 다른 용어를 사용할 수 있습니다. 특히 OAuth 2.0 기능이 보다 큰 ID 및 액세스 관리 제품 또는 솔루션 내에 패키지되어 있는 경우 더욱 그렇습니다. 예를 들어, * ID 공급자(IDP) * 라는 용어는 * 인증 서버 * 와 같은 의미로 사용되는 경우가 많습니다.

관리

권한 부여 서버는 액세스 토큰을 발급하는 것 외에도 일반적으로 웹 사용자 인터페이스를 통해 관련 관리 서비스를 제공합니다. 예를 들어 다음을 정의하고 관리할 수 있습니다.

- 사용자 및 사용자 인증
- 범위
- 테넌트 및 영역을 통한 관리 분리
- 정책 적용
- 다양한 외부 서비스에 연결
- 기타 ID 프로토콜(예: SAML) 지원

ONTAP는 OAuth 2.0 표준과 호환되는 인증 서버와 호환됩니다.

ONTAP로 정의

ONTAP에 하나 이상의 인증 서버를 정의해야 합니다. ONTAP는 각 서버와 안전하게 통신하여 토큰을 확인하고 클라이언트 응용 프로그램을 지원하는 기타 관련 작업을 수행합니다.

ONTAP 구성의 주요 측면은 다음과 같습니다. 도 참조하십시오 "OAuth 2.0 배포 시나리오" 를 참조하십시오.

액세스 토큰의 유효성 검사 방법 및 위치

액세스 토큰의 유효성을 검사하는 방법에는 두 가지가 있습니다.

- 로컬 검증

  ONTAP는 토큰을 발급한 인증 서버에서 제공한 정보를 기반으로 액세스 토큰의 유효성을 로컬로 검사할 수 있습니다. 인증 서버에서 검색된 정보는 ONTAP에 의해 캐시되고 정기적으로 새로 고쳐집니다.

- 원격 자기 주도

  또한 인증 서버에서 토큰의 유효성을 검사하기 위해 원격 검사를 사용할 수도 있습니다. introspection은 권한이 있는 사용자가 인증 서버에 액세스 토큰을 쿼리할 수 있도록 하는 프로토콜입니다. ONTAP는 액세스 토큰에서 특정 메타데이터를 추출하고 토큰의 유효성을 검사하는 방법을 제공합니다. ONTAP은 성능상의 이유로 일부 데이터를 캐싱합니다.

네트워크 위치

ONTAP가 방화벽 뒤에 있을 수 있습니다. 이 경우 프록시를 구성의 일부로 식별해야 합니다.

권한 부여 서버가 정의되는 방법

CLI, System Manager 또는 REST API를 포함한 관리 인터페이스를 사용하여 ONTAP에 권한 부여 서버를 정의할 수 있습니다. 예를 들어, CLI에서는 명령을 사용합니다 `security oauth2 client create`.

인증 서버 수입니다

단일 ONTAP 클러스터에 대해 최대 8개의 인증 서버를 정의할 수 있습니다. 발급사 또는 발급사/대상 그룹 클레임이 고유하면 동일한 인증 서버를 동일한 ONTAP 클러스터에 두 번 이상 정의할 수 있습니다. 예를 들어 Keycloak를 사용하면 다른 영역을 사용할 때 항상 이 경우가 발생합니다.

OAuth 2.0 액세스 토큰 사용

인증 서버에서 발급한 OAuth 2.0 액세스 토큰은 ONTAP에서 검증하고 REST API 클라이언트 요청에 대한 역할 기반 액세스 결정을 내리는 데 사용됩니다.

액세스 토큰을 가져오는 중입니다

REST API를 사용하는 ONTAP 클러스터에 정의된 인증 서버에서 액세스 토큰을 얻어야 합니다. 토큰을 얻으려면 인증 서버에 직접 연결해야 합니다.

> ONTAP는 액세스 토큰을 발급하거나 클라이언트에서 인증 서버로 요청을 리디렉션하지 않습니다.

토큰을 요청하는 방법은 다음과 같은 여러 요인에 따라 달라집니다.

- 인증 서버 및 구성 옵션
- OAuth 2.0 보조금 유형
- 요청을 발급하는 데 사용되는 클라이언트 또는 소프트웨어 도구입니다

허가 유형

A_GRANT_는 OAuth 2.0 액세스 토큰을 요청하고 수신하는 데 사용되는 네트워크 흐름 집합을 포함한 잘 정의된 프로세스입니다. 클라이언트, 환경 및 보안 요구 사항에 따라 여러 가지 다른 부여 형식을 사용할 수 있습니다. 인기 있는 보조금 유형 목록은 아래 표에 나와 있습니다.

허가 유형	설명
클라이언트 자격 증명입니다	ID 및 공유 암호 등 자격 증명만 사용하는 일반적인 부여 유형입니다. 클라이언트는 리소스 소유자와 밀접한 트러스트 관계를 갖는 것으로 간주됩니다.
암호	리소스 소유자 암호 자격 증명 부여 유형은 리소스 소유자가 클라이언트와 신뢰 관계가 설정된 경우에 사용할 수 있습니다. 레거시 HTTP 클라이언트를 OAuth 2.0으로 마이그레이션할 때도 유용합니다.
인증 코드	이는 기밀 클라이언트에 이상적인 보조금 유형이며 리디렉션 기반 흐름을 기반으로 합니다. 액세스 토큰을 가져오고 토큰을 새로 고치는 데 사용할 수 있습니다.

JWT 콘텐츠

OAuth 2.0 액세스 토큰은 JWT로 포맷됩니다. 콘텐츠는 사용자의 구성에 따라 인증 서버에서 만들어집니다. 그러나 토큰은 클라이언트 응용 프로그램에서 불투명합니다. 클라이언트는 토큰을 검사하거나 내용을 인식할 이유가 없습니다.

각 JWT 액세스 토큰에는 클레임 집합이 포함됩니다. 클레임은 권한 부여 서버의 관리 정의에 따라 발급자의 특성과 권한 부여를 설명합니다. 표준에 등록된 청구의 일부는 아래 표에 설명되어 있습니다. 모든 문자열은 대/소문자를 구분합니다.

청구	키워드	설명
발급사	아이에스에스주식회사	토큰을 발급한 보안 주체를 식별합니다. 신청 처리는 응용 프로그램에 따라 다릅니다.
제목	하위	토큰의 제목 또는 사용자입니다. 이름은 전역적으로 또는 로컬에서 고유하도록 범위가 지정됩니다.
대상	호주 달러	토큰을 받을 수신자입니다. 문자열 배열로 구현됩니다.
만료	만료	토큰이 만료되어 거부되어야 하는 시간입니다.

을 참조하십시오 "RFC 7519: JSON 웹 토큰" 를 참조하십시오.

ONTAP 클라이언트 인증 옵션

ONTAP 클라이언트 인증을 사용자 지정하는 데 사용할 수 있는 몇 가지 옵션이 있습니다. 권한 부여 결정은 궁극적으로 액세스 토큰에 포함되어 있거나 액세스 토큰에서 파생된 ONTAP REST 역할을 기반으로 합니다.

> 만 사용할 수 있습니다 "ONTAP REST 역할" OAuth 2.0에 대한 권한 부여를 구성하는 경우. 이전 ONTAP의 기존 역할은 지원되지 않습니다.

소개

ONTAP 내의 OAuth 2.0 구현은 유연하고 강력하도록 설계되어 ONTAP 환경을 보호하는 데 필요한 옵션을 제공합니다. 상위 수준에서는 ONTAP 클라이언트 권한 부여를 정의하기 위한 세 가지 주요 구성 범주가 있습니다. 이러한 구성 옵션은 함께 사용할 수 없습니다.

ONTAP는 사용자의 구성에 따라 가장 적합한 단일 옵션을 적용합니다. 을 참조하십시오 "ONTAP에서 액세스를 결정하는 방법" ONTAP에서 액세스 결정을 내리기 위해 구성 정의를 처리하는 방법에 대한 자세한 내용을 참조하십시오.

OAuth 2.0 독립형 범위

이러한 범위에는 각각 단일 문자열로 캡슐화된 하나 이상의 사용자 지정 REST 역할이 포함됩니다. ONTAP 역할 정의와는 독립적입니다. 인증 서버에서 이러한 범위 문자열을 정의해야 합니다.

로컬 **ONTAP** 관련 **REST** 역할 및 사용자

구성에 따라 로컬 ONTAP ID 정의를 사용하여 액세스 결정을 내릴 수 있습니다. 옵션은 다음과 같습니다.

- 단일 이름 REST 역할입니다
- 사용자 이름과 로컬 ONTAP 사용자를 일치시킵니다

명명된 역할의 범위 구문은 * ontap-role - * <URL-encoded-ONTAP-role-name>입니다. 예를 들어, 역할이 "admin"인 경우 범위 문자열은 "ontap-role-admin"이 됩니다.

Active Directory 또는 **LDAP** 그룹

로컬 ONTAP 정의를 검사했지만 액세스를 결정할 수 없는 경우 Active Directory("도메인") 또는 LDAP("nsswitch") 그룹이 사용됩니다. 그룹 정보는 다음 두 가지 방법 중 하나로 지정할 수 있습니다.

- OAuth 2.0 범위 문자열

  그룹 멤버십을 가진 사용자가 없는 경우 클라이언트 자격 증명 흐름을 사용하여 기밀 응용 프로그램을 지원합니다. 범위의 이름은 * ontap-group - * <URL-encoded-ONTAP-group-name>여야 합니다. 예를 들어 그룹이 "development"인 경우 범위 문자열은 "ontap-group-development"가 됩니다.

- "그룹" 요구 사항

  리소스 소유자(암호 부여) 흐름을 사용하여 ADFS에서 발급한 액세스 토큰에 사용됩니다.

자체 포함된 **OAuth 2.0** 범위

자체 포함 범위는 액세스 토큰으로 전달되는 문자열입니다. 각각은 완전한 사용자 지정 역할 정의이며 ONTAP에서 액세스 결정을 내리는 데 필요한 모든 것을 포함합니다. 범위는 ONTAP 자체 내에 정의된 모든 REST 역할과 별개입니다.

범위 문자열의 형식입니다

기본 수준에서 범위는 연속된 문자열로 표시되며 콜론으로 구분된 6개의 값으로 구성됩니다. 범위 문자열에 사용되는 매개 변수는 아래에 설명되어 있습니다.

ONTAP 리터럴

범위는 리터럴 값으로 시작해야 합니다 `ontap` 소문자로 입력합니다. ONTAP에만 해당하는 범위를 식별합니다.

클러스터

범위가 적용되는 ONTAP 클러스터를 정의합니다. 값은 다음과 같습니다.

- 클러스터 UUID

  단일 클러스터를 식별합니다.

- 별표(*)

범위가 모든 클러스터에 적용됨을 나타냅니다.

ONTAP CLI 명령을 사용할 수 있습니다 `cluster identity show` 클러스터의 UUID를 표시합니다. 지정하지 않으면 범위가 모든 클러스터에 적용됩니다.

역할

자체 포함된 범위에 포함된 REST 역할의 이름입니다. 이 값은 ONTAP에서 검사하거나 ONTAP에 정의된 기존 REST 역할과 일치하지 않습니다. 이 이름은 로깅에 사용됩니다.

액세스 수준

이 값은 범위에서 API 끝점을 사용할 때 클라이언트 응용 프로그램에 적용되는 액세스 수준을 나타냅니다. 아래 표에 설명된 대로 6개의 값이 있습니다.

액세스 수준	설명
없음	지정된 끝점에 대한 모든 액세스를 거부합니다.
읽기 전용	GET를 사용하여 읽기 액세스만 허용합니다.
read_create 를 참조하십시오	POST를 사용하여 새 리소스 인스턴스를 만들고 읽기 액세스를 허용합니다.
read_modify 를 참조하십시오	패치를 사용하여 기존 리소스를 업데이트할 수 있을 뿐 아니라 읽기 액세스를 허용합니다.
READ_CREATE_MODIFY 을 참조하십시오	삭제를 제외한 모든 액세스를 허용합니다. 허용되는 작업에는 GET(읽기), POST(작성) 및 패치(업데이트)가 포함됩니다.
모두	전체 액세스를 허용합니다.

SVM

클러스터 내 SVM의 이름이 범위에 적용됩니다. * 값(별표)을 사용하여 모든 SVM을 나타냅니다.

> 이 기능은 ONTAP 9.14.1에서 완벽하게 지원되지 않습니다. SVM 매개 변수를 무시하고 별표를 자리 표시자로 사용할 수 있습니다. 를 검토합니다 "ONTAP 릴리즈 노트" 향후 SVM 지원 확인

REST API URI입니다

리소스 또는 관련 리소스 집합에 대한 전체 또는 부분 경로입니다. 문자열은 로 시작해야 합니다 `/api`. 값을 지정하지 않으면 범위가 ONTAP 클러스터의 모든 API 끝점에 적용됩니다.

범위 예

다음은 자급식 범위의 몇 가지 예입니다.

ONTAP: *:joes-역할**: read_create_modify: *:/api/cluster**

이 역할에 할당된 사용자에게 에 대한 읽기, 생성 및 수정 액세스 권한을 제공합니다 `/cluster` 엔드포인트.

CLI 관리 도구

ONTAP는 자체 포함된 범위를 보다 쉽게 관리할 수 있도록 CLI 명령을 제공합니다 `security oauth2 scope` 입력 매개 변수를 기반으로 범위 문자열을 생성합니다.

명령을 입력합니다 `security oauth2 scope` 은 고객 입력에 따라 두 가지 사용 사례를 가지고 있습니다.

- 문자열 범위를 지정하는 CLI 매개 변수입니다

  이 버전의 명령을 사용하여 입력 매개 변수를 기반으로 범위 문자열을 생성할 수 있습니다.

- 문자열을 CLI 매개 변수로 지정합니다

  이 버전의 명령을 사용하여 입력 범위 문자열을 기반으로 명령 매개 변수를 생성할 수 있습니다.

예

다음 예제에서는 아래 명령 예제 다음에 포함된 출력으로 범위 문자열을 생성합니다. 이 정의는 모든 클러스터에 적용됩니다.

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

```
ontap:*:joes-role:readonly:*:/api/cluster
```

ONTAP에서 액세스를 결정하는 방법

OAuth 2.0을 올바르게 설계하고 구현하려면 ONTAP에서 클라이언트의 액세스 결정을 내리기 위해 인증 구성이 사용되는 방법을 이해해야 합니다.

1단계**:** 자체 포함 범위

액세스 토큰에 자체 포함된 범위가 포함되어 있는 경우 ONTAP에서는 해당 범위를 먼저 검사합니다. 자체 포함된 범위가 없는 경우 2단계로 이동합니다.

하나 이상의 자체 포함 범위가 있는 경우 ONTAP는 명시적 * allow * 또는 * deny * 결정을 내릴 수 있을 때까지 각 범위를 적용합니다. 명시적인 결정이 내려지면 처리가 종료됩니다.

ONTAP에서 명시적인 액세스 결정을 내릴 수 없는 경우 2단계를 계속 진행합니다.

2단계**:** 로컬 역할 플래그를 확인합니다

ONTAP는 플래그 값을 검사합니다 `use-local-roles-if-present`. 이 플래그의 값은 ONTAP로 정의된 각 인증 서버에 대해 별도로 설정됩니다.

- 값이 이면 `true` 3단계를 계속 진행합니다.
- 값이 이면 `false` 처리가 종료되고 액세스가 거부됩니다.

3단계**:** 이름이 지정된 **ONTAP REST** 역할입니다

액세스 토큰에 이름이 지정된 REST 역할이 포함된 경우 ONTAP는 해당 역할을 사용하여 액세스 결정을 내립니다. 이렇게 하면 항상 * allow * 또는 * deny * 결정이 되고 처리가 종료됩니다.

이름이 지정된 REST 역할이 없거나 역할을 찾을 수 없는 경우 4단계를 계속 진행하십시오.

단계 **4:** 로컬 **ONTAP** 사용자

액세스 토큰에서 사용자 이름을 추출하여 로컬 ONTAP 사용자와 일치시키려고 시도합니다.

로컬 ONTAP 사용자가 일치하는 경우 ONTAP는 사용자에게 정의된 역할을 사용하여 액세스 결정을 내립니다. 이로 인해 항상 * allow * 또는 * deny * 결정이 내려지고 처리가 종료됩니다.

로컬 ONTAP 사용자가 일치하지 않거나 액세스 토큰에 사용자 이름이 없는 경우 5단계를 계속 진행합니다.

5단계**:** 그룹**-**역할 매핑

액세스 토큰에서 그룹을 추출하고 그룹에 일치시키려고 시도합니다. 그룹은 Active Directory 또는 이에 상응하는 LDAP 서버를 사용하여 정의됩니다.

그룹 일치 항목이 있는 경우 ONTAP는 그룹에 대해 정의된 역할을 사용하여 액세스 결정을 내립니다. 이로 인해 항상 * allow * 또는 * deny * 결정이 내려지고 처리가 종료됩니다.

일치하는 그룹이 없거나 액세스 토큰에 그룹이 없으면 액세스가 거부되고 처리가 종료됩니다.

OAuth 2.0 배포 시나리오

ONTAP에 대한 인증 서버를 정의할 때 사용할 수 있는 몇 가지 구성 옵션이 있습니다. 이러한 옵션에 따라 배포 환경에 적합한 인증 서버를 만들 수 있습니다.

구성 매개 변수 요약

ONTAP에 대한 인증 서버를 정의할 때 사용할 수 있는 몇 가지 구성 매개 변수가 있습니다. 이러한 매개 변수는 일반적으로 모든 관리 인터페이스에서 지원됩니다.

매개 변수 이름은 ONTAP 관리 인터페이스에 따라 약간 다를 수 있습니다. 예를 들어, 원격 내부 조사를 구성할 때 끝점은 CLI 명령 매개 변수를 사용하여 식별됩니다 `-introspection-endpoint`. 그러나 System Manager의 경우, 해당 필드는 _ 인증 서버 토큰 내부 URI _ 입니다. 모든 ONTAP 관리 인터페이스를 수용할 수 있도록 매개 변수에 대한 일반적인 설명이 제공됩니다. 정확한 매개 변수 또는 필드는 컨텍스트에 따라 명확해야 합니다.

매개 변수	설명
이름	ONTAP에 알려진 인증 서버의 이름입니다.
응용 프로그램	정의가 적용되는 ONTAP 내부 응용 프로그램입니다. 이 값은 * http * 여야 합니다.
발급자 URI입니다	토큰을 발급하는 사이트 또는 조직을 식별하는 경로가 있는 FQDN입니다.
공급자 JWKS URI입니다	ONTAP가 액세스 토큰의 유효성을 검사하는 데 사용되는 JSON 웹 키 세트를 가져오는 경로 및 파일 이름의 FQDN입니다.
JWKS 새로 고침 간격입니다	ONTAP가 공급자 JWKS URI에서 인증서 정보를 새로 고치는 빈도를 결정하는 시간 간격입니다. 값은 ISO-8601 형식으로 지정됩니다.
성찰의 끝점입니다	ONTAP에서 자체 조사를 통해 원격 토큰 유효성 검사를 수행하는 데 사용하는 경로가 있는 FQDN입니다.
클라이언트 ID입니다	인증 서버에 정의된 클라이언트의 이름입니다. 이 값이 포함된 경우 인터페이스를 기반으로 연결된 클라이언트 암호도 제공해야 합니다.

매개 변수	설명
발신 프록시	이는 ONTAP가 방화벽 뒤에 있을 때 인증 서버에 대한 액세스를 제공하기 위한 것입니다. URI는 curl 형식이어야 합니다.
있는 경우 로컬 역할을 사용합니다	로컬 ONTAP 정의가 사용되는지 여부를 결정하는 부울 플래그(명명된 REST 역할 및 로컬 사용자 포함)
사용자 클레임을 제거합니다	ONTAP에서 로컬 사용자와 일치시키기 위해 사용하는 대체 이름입니다. 를 사용합니다 `sub` 로컬 사용자 이름과 일치하는 액세스 토큰의 필드입니다.

배포 시나리오

다음은 몇 가지 일반적인 배포 시나리오입니다. 토큰 유효성 검사는 ONTAP에서 로컬로 수행되는지 아니면 인증 서버에서 원격으로 수행되는지를 기준으로 구성됩니다. 각 시나리오에는 필요한 구성 옵션 목록이 포함되어 있습니다. 을 참조하십시오 "ONTAP에 OAuth 2.0 배포" 구성 명령의 예를 참조하십시오.

> 인증 서버를 정의한 후 ONTAP 관리 인터페이스를 통해 구성을 표시할 수 있습니다. 예를 들어, 명령을 사용합니다 `security oauth2 client show` ONTAP CLI 사용.

로컬 검증

다음 배포 시나리오는 토큰 유효성 검사를 로컬로 수행하는 ONTAP를 기반으로 합니다.

프록시 없이 자체 포함된 범위를 사용합니다

이것은 OAuth 2.0 자체 포함 범위만 사용하는 가장 간단한 배포입니다. 로컬 ONTAP ID 정의는 사용되지 않습니다. 다음 매개 변수를 포함해야 합니다.

- 이름
- 응용 프로그램(http)
- 공급자 JWKS URI입니다
- 발급자 URI입니다

또한 인증 서버에 범위를 추가해야 합니다.

프록시에 자체 포함된 범위를 사용합니다

이 배포 시나리오에서는 OAuth 2.0 자체 포함 범위를 사용합니다. 로컬 ONTAP ID 정의는 사용되지 않습니다. 하지만 인증 서버는 방화벽 뒤에 있으므로 프록시를 구성해야 합니다. 다음 매개 변수를 포함해야 합니다.

- 이름
- 응용 프로그램(http)
- 공급자 JWKS URI입니다
- 발신 프록시
- 발급자 URI입니다
- 대상

또한 인증 서버에 범위를 추가해야 합니다.

프록시에 로컬 사용자 역할 및 기본 사용자 이름 매핑을 사용합니다

이 배포 시나리오에서는 기본 이름 매핑과 함께 로컬 사용자 역할을 사용합니다. 원격 사용자 클레임은 기본값인 을 사용합니다 `sub` 액세스 토큰의 이 필드는 로컬 사용자 이름과 일치시키는 데 사용됩니다. 사용자 이름은 40자 이하여야 합니다. 인증 서버는 방화벽 뒤에 있으므로 프록시를 구성해야 합니다. 다음 매개 변수를 포함해야 합니다.

- 이름
- 응용 프로그램(http)
- 공급자 JWKS URI입니다
- 있는 경우 로컬 역할을 사용합니다 (`true`)
- 발신 프록시
- 발급사

로컬 사용자가 ONTAP로 정의되었는지 확인해야 합니다.

프록시를 사용하여 로컬 사용자 역할 및 대체 사용자 이름 매핑을 사용합니다

이 배포 시나리오에서는 로컬 ONTAP 사용자와 일치시키는 데 사용되는 대체 사용자 이름과 함께 로컬 사용자 역할을 사용합니다. 인증 서버는 방화벽 뒤에 있으므로 프록시를 구성해야 합니다. 다음 매개 변수를 포함해야 합니다.

- 이름
- 응용 프로그램(http)
- 공급자 JWKS URI입니다
- 있는 경우 로컬 역할을 사용합니다 (`true`)
- 원격 사용자 클레임
- 발신 프록시
- 발급자 URI입니다
- 대상

로컬 사용자가 ONTAP로 정의되었는지 확인해야 합니다.

원격 자기 주도

다음 배포 구성은 ONTAP를 기반으로 합니다. 이 구성은 자체 조사를 통해 토큰 유효성 검사를 원격으로 수행합니다.

프록시 없이 자체 포함된 범위를 사용합니다

OAuth 2.0 독립형 범위를 사용하여 간단하게 배포할 수 있습니다. ONTAP ID 정의는 사용되지 않습니다. 다음 매개 변수를 포함해야 합니다.

- 이름
- 응용 프로그램(http)
- 성찰의 끝점입니다
- 클라이언트 ID입니다
- 발급자 URI입니다

인증 서버에서 클라이언트 및 클라이언트 비밀은 물론 범위를 정의해야 합니다.

상호 **TLS**를 사용한 클라이언트 인증

보안 요구에 따라 강력한 클라이언트 인증을 구현하도록 MTL(Mutual TLS)을 선택적으로 구성할 수 있습니다. OAuth 2.0 배포의 일부로 ONTAP와 함께 사용할 경우 MTL은 액세스 토큰이 원래 발급된 클라이언트에서만 사용되도록 보장합니다.

상호 **TLS**와 **OAuth 2.0**

TLS(Transport Layer Security)는 두 애플리케이션(일반적으로 클라이언트 브라우저와 웹 서버)간에 보안 통신 채널을 설정하는 데 사용됩니다. 상호 TLS는 클라이언트 인증서를 통해 클라이언트를 강력하게 식별함으로써 이 기능을 확장합니다. OAuth 2.0이 있는 ONTAP 클러스터에서 사용할 경우 기본 MTL 기능은 보낸 사람 제한 액세스 토큰을 생성하고 사용하여 확장됩니다.

보낸 사람 제한 액세스 토큰은 원래 발급된 클라이언트에서만 사용할 수 있습니다. 이 기능을 지원하기 위해 새로운 확인 요청이 있습니다 (`cnf`)이 토큰에 삽입됩니다. 필드에 속성이 포함되어 있습니다 `x5t#S256` 액세스 토큰을 요청할 때 사용되는 클라이언트 인증서의 다이제스트가 들어 있습니다. 이 값은 토큰 유효성 검사의 일부로 ONTAP에서 확인합니다. 보낸 사람 제한이 없는 인증 서버에서 발급한 액세스 토큰에는 추가 확인 클레임이 포함되지 않습니다.

각 인증 서버에 대해 MTL을 별도로 사용하도록 ONTAP를 구성해야 합니다. 예를 들어, CLI 명령을 사용할 수 있습니다 `security oauth2 client` 매개 변수를 포함합니다 `use-mutual-tls` 아래 표와 같이 세 가지 값을 기반으로 MTL 처리를 제어합니다.

> 각 구성에서 ONTAP가 수행한 결과 및 작업은 구성 매개 변수 값과 액세스 토큰 및 클라이언트 인증서의 내용에 따라 달라집니다. 표의 매개 변수는 최소 값부터 최대 제한값까지 구성됩니다.

매개 변수	설명
없음	인증 서버에 대해 OAuth 2.0 상호 TLS 인증이 완전히 비활성화되었습니다. 토큰에 확인 클레임이 있거나 TLS 연결과 함께 클라이언트 인증서가 제공된 경우에도 ONTAP는 MTL 클라이언트 인증서 인증을 수행하지 않습니다.
요청	OAuth 2.0 상호 TLS 인증은 클라이언트가 보낸 사람 제한 액세스 토큰을 제공하는 경우 적용됩니다. 즉, MTL은 확인 요청(속성 포함)이 있는 경우에만 적용됩니다 `x5t#S256`)이 액세스 토큰에 있습니다. 기본 설정입니다.
필수 요소입니다	OAuth 2.0 상호 TLS 인증은 인증 서버에서 발급한 모든 액세스 토큰에 대해 적용됩니다. 따라서 모든 액세스 토큰은 sender-constraint여야 합니다. 액세스 토큰에 확인 클레임이 없거나 잘못된 클라이언트 인증서가 있는 경우 인증 및 REST API 요청이 실패합니다.

높은 수준의 구현 흐름

ONTAP 환경에서 OAuth 2.0과 함께 MTL을 사용할 때 적용되는 일반적인 단계는 다음과 같습니다. 을 참조하십시오 "RFC 8705: OAuth 2.0 상호 TLS 클라이언트 인증 및 인증서 바인딩된 액세스 토큰" 를 참조하십시오.

1단계**:** 클라이언트 인증서를 생성하고 설치합니다

클라이언트 ID 설정은 클라이언트 개인 키에 대한 지식을 입증하기 위한 것입니다. 해당 공개 키는 클라이언트에서 제공하는 서명된 X.509 인증서에 저장됩니다. 클라이언트 인증서 만들기와 관련된 단계는 다음과 같습니다.

1. 공개 및 개인 키 쌍을 생성합니다
2. 인증서 서명 요청을 만듭니다

3. CSR 파일을 잘 알려진 CA로 보냅니다
4. CA에서 요청을 확인하고 서명된 인증서를 발급합니다

일반적으로 클라이언트 인증서를 로컬 운영 체제에 설치하거나 curl과 같은 공통 유틸리티를 사용하여 직접 사용할 수 있습니다.

2단계**: MTL**을 사용하도록 **ONTAP**를 구성합니다

MTL을 사용하도록 ONTAP을 구성해야 합니다. 이 구성은 각 인증 서버에 대해 별도로 수행됩니다. 예를 들어, CLI를 사용하면 명령을 사용할 수 있습니다 `security oauth2 client` 선택적 매개 변수와 함께 사용됩니다 `use-mutual-tls`. 을 참조하십시오 "ONTAP에 OAuth 2.0 배포" 를 참조하십시오.

3단계**:** 클라이언트가 액세스 토큰을 요청합니다

클라이언트는 ONTAP로 구성된 인증 서버에서 액세스 토큰을 요청해야 합니다. 클라이언트 응용 프로그램은 1단계에서 생성하고 설치한 인증서가 있는 MTL을 사용해야 합니다.

4단계**:** 인증 서버가 액세스 토큰을 생성합니다

인증 서버는 클라이언트 요청을 확인하고 액세스 토큰을 생성합니다. 이 과정에서 클라이언트 인증서의 메시지 다이제스트가 생성되며, 이 다이제스트는 토큰에 확인 클레임(필드)으로 포함됩니다 `cnf`)를 클릭합니다.

5단계**:** 클라이언트 애플리케이션이 **ONTAP**에 액세스 토큰을 제공합니다

클라이언트 응용 프로그램은 ONTAP 클러스터에 REST API 호출을 수행하고 권한 부여 요청 헤더에 액세스 토큰을 * 베어러 토큰 * 으로 포함합니다. 클라이언트는 액세스 토큰을 요청하는 데 사용된 것과 동일한 인증서를 가진 MTL을 사용해야 합니다.

6단계**: ONTAP**는 클라이언트와 토큰을 확인합니다**.**

ONTAP는 MTL 처리의 일부로 사용되는 클라이언트 인증서뿐만 아니라 HTTP 요청으로 액세스 토큰을 받습니다. ONTAP는 먼저 액세스 토큰의 서명을 확인합니다. 구성에 따라 ONTAP는 클라이언트 인증서의 메시지 다이제스트를 생성하고 토큰의 확인 클레임 * CNF * 와 비교합니다. 두 값이 일치하면 ONTAP는 API 요청을 하는 클라이언트가 액세스 토큰이 원래 발급된 클라이언트와 동일하다는 것을 확인했습니다.

구성 및 배포

ONTAP와 함께 **OAuth 2.0**을 배포할 준비를 하십시오

ONTAP 환경에서 OAuth 2.0을 구성하기 전에 배포를 준비해야 합니다. 주요 작업과 결정에 대한 요약이 아래에 나와 있습니다. 섹션의 정렬은 일반적으로 따라야 할 순서에 맞춰집니다. 그러나 대부분의 배포에는 적용되지만 필요에 따라 환경에 맞게 조정해야 합니다. 공식 배포 계획을 작성하는 것도 고려해야 합니다.

> 사용자 환경에 따라 ONTAP에 정의된 인증 서버에 대한 구성을 선택할 수 있습니다. 여기에는 각 배포 유형에 대해 구체화해야 하는 매개 변수 값이 포함됩니다. 을 참조하십시오 "OAuth 2.0 배포 시나리오" 를 참조하십시오.

보호된 리소스 및 클라이언트 응용 프로그램

OAuth 2.0은 보호된 리소스에 대한 액세스를 제어하기 위한 권한 부여 프레임워크입니다. 이 점을 감안하면 모든 배포에서 중요한 첫 단계는 사용 가능한 리소스가 무엇이고 어떤 클라이언트가 액세스할 필요가 있는지 확인하는 것입니다.

클라이언트 애플리케이션을 식별합니다

REST API 호출을 실행할 때 OAuth 2.0을 사용할 클라이언트와 이들이 액세스해야 하는 API 엔드포인트를 결정해야 합니다.

기존 **ONTAP REST** 역할 및 로컬 사용자를 검토합니다

REST 역할 및 로컬 사용자를 포함하여 기존 ONTAP ID 정의를 검토해야 합니다. OAuth 2.0을 구성하는 방법에 따라 이러한 정의를 액세스 결정에 사용할 수 있습니다.

OAuth 2.0으로의 글로벌 전환

OAuth 2.0 인증을 점진적으로 구현할 수도 있지만 각 인증 서버에 대한 글로벌 플래그를 설정하여 모든 REST API 클라이언트를 OAuth 2.0으로 즉시 이동할 수도 있습니다. 따라서 자체 포함된 범위를 만들 필요 없이 기존 ONTAP 구성을 기반으로 액세스 결정을 내릴 수 있습니다.

인증 서버

권한 부여 서버는 액세스 토큰을 발행하고 관리 정책을 시행함으로써 OAuth 2.0 배포에서 중요한 역할을 수행합니다.

인증 서버를 선택하여 설치합니다

하나 이상의 인증 서버를 선택하여 설치해야 합니다. 범위를 정의하는 방법을 비롯하여 ID 공급자의 구성 옵션 및 절차를 숙지하는 것이 중요합니다.

인증 루트 **CA** 인증서를 설치해야 하는지 확인합니다

ONTAP는 인증 서버의 인증서를 사용하여 클라이언트가 제공하는 서명된 액세스 토큰의 유효성을 검사합니다. 이렇게 하려면 ONTAP에서 루트 CA 인증서와 모든 중간 인증서가 필요합니다. ONTAP와 함께 사전 설치되어 있을 수 있습니다. 그렇지 않은 경우 설치해야 합니다.

네트워크 위치 및 구성을 평가합니다

인증 서버가 방화벽 뒤에 있는 경우 프록시 서버를 사용하도록 ONTAP를 구성해야 합니다.

클라이언트 인증 및 권한 부여

클라이언트 인증 및 권한 부여에는 몇 가지 측면을 고려해야 합니다.

자체 포함된 범위 또는 로컬 **ONTAP ID** 정의

상위 수준에서는 권한 부여 서버에서 정의된 자체 포함 범위를 정의하거나 역할 및 사용자를 비롯한 기존 로컬 ONTAP ID 정의를 사용할 수 있습니다.

로컬 **ONTAP** 처리 옵션

ONTAP ID 정의를 사용하는 경우 다음을 포함하여 적용할 항목을 결정해야 합니다.

- 이름이 지정된 REST 역할입니다
- 로컬 사용자와 일치합니다
- Active Directory 또는 LDAP 그룹

로컬 검증 또는 원격 검사

액세스 토큰의 유효성을 ONTAP에서 로컬로 검사할지, 아니면 자체 검사를 통해 인증 서버에서 검사할지 결정해야 합니다. 또한 새로 고침 간격과 같이 고려해야 할 여러 관련 값도 있습니다.

보낸 사람 제한 액세스 토큰

높은 수준의 보안이 필요한 환경에서는 MTL을 기반으로 보내기 제한 액세스 토큰을 사용할 수 있습니다. 이렇게 하려면 각 클라이언트에 대한 인증서가 필요합니다.

관리 인터페이스

다음을 비롯한 모든 ONTAP 인터페이스를 통해 OAuth 2.0을 관리할 수 있습니다.

- 명령줄 인터페이스입니다
- 시스템 관리자
- REST API

클라이언트가 액세스 토큰을 요청하는 방법

클라이언트 응용 프로그램은 권한 부여 서버에서 직접 액세스 토큰을 요청해야 합니다. 허가 유형을 포함하여 이 작업을 수행하는 방법을 결정해야 합니다.

ONTAP를 구성합니다

몇 가지 ONTAP 구성 작업을 수행해야 합니다.

REST 역할 및 로컬 사용자를 정의합니다

인증 구성에 따라 로컬 ONTAP 식별 처리를 사용할 수 있습니다. 이 경우 REST 역할 및 사용자 정의를 검토하고 정의해야 합니다.

코어 구성

핵심 ONTAP 구성을 수행하는 데 필요한 주요 단계는 다음과 같습니다.

- 선택적으로 인증 서버의 인증서를 서명한 CA에 대한 루트 인증서(및 모든 중간 인증서)를 설치합니다.
- 인증 서버를 정의합니다.
- 클러스터에 대해 OAuth 2.0 처리를 활성화합니다.

ONTAP에 **OAuth 2.0** 배포

핵심 OAuth 2.0 기능을 배포하려면 세 가지 기본 단계가 필요합니다.

시작하기 전에

ONTAP를 구성하기 전에 OAuth 2.0 배포를 준비해야 합니다. 예를 들어 인증서의 서명 방법 및 방화벽 뒤에 있는지 등 인증 서버를 평가해야 합니다. 을 참조하십시오 "ONTAP와 함께 OAuth 2.0을 배포할 준비를 하십시오" 를 참조하십시오.

1단계**:** 인증 서버 인증서를 설치합니다

ONTAP에는 미리 설치된 루트 CA 인증서가 다수 포함되어 있습니다. 따라서 대부분의 경우 추가 구성 없이 ONTAP에서 인증 서버의 인증서를 즉시 인식합니다. 그러나 인증 서버 인증서 서명 방법에 따라 루트 CA 인증서와 중간 인증서를 설치해야 할 수도 있습니다.

필요한 경우 아래 제공된 지침에 따라 인증서를 설치합니다. 필요한 모든 인증서를 클러스터 수준에서 설치해야 합니다.

ONTAP 액세스 방법에 따라 올바른 절차를 선택합니다.

예 **1.** 단계

시스템 관리자

1. System Manager에서 * 클러스터 * > * 설정 * 을 선택합니다.
2. 아래로 스크롤하여 * 보안 * 섹션으로 이동합니다.
3. Certificates * 옆에 있는 * → * 를 클릭합니다.
4. 신뢰할 수 있는 인증 기관 * 탭에서 * 추가 * 를 클릭합니다.
5. 가져오기 * 를 클릭하고 인증서 파일을 선택합니다.
6. 사용자 환경에 대한 구성 매개 변수를 입력합니다.
7. 추가 * 를 클릭합니다.

CLI를 참조하십시오

1. 설치를 시작합니다.

   보안 인증서설치형 server-ca

2. 다음 콘솔 메시지를 찾습니다.

   ```
   Please enter Certificate: Press <Enter> when done
   ```

3. 텍스트 편집기로 인증서 파일을 엽니다.
4. 다음 행을 포함하여 전체 인증서를 복사합니다.

   ```
   -----BEGIN CERTIFICATE-----

   -----END CERTIFICATE-----
   ```

5. 명령 프롬프트 후 터미널에 인증서를 붙여 넣습니다.
6. Enter * 키를 눌러 설치를 완료합니다.
7. 다음 중 하나를 사용하여 인증서가 설치되었는지 확인합니다.

   ```
   security certificate show-user-installed

   security certificate show
   ```

2단계**:** 인증 서버를 구성합니다

ONTAP에 하나 이상의 인증 서버를 정의해야 합니다. 구성 및 배포 계획에 따라 매개 변수 값을 선택해야 합니다. 검토 "OAuth2 배포 시나리오" 구성에 필요한 정확한 매개 변수를 결정합니다.

> 권한 부여 서버 정의를 수정하려면 기존 정의를 삭제하고 새 정의를 만듭니다.

아래에 제공된 예는 의 첫 번째 간단한 배포 시나리오를 기반으로 합니다 "로컬 검증". 독립 실행형 범위는 프록시 없이 사용됩니다.

ONTAP 액세스 방법에 따라 올바른 절차를 선택합니다. CLI 절차에서는 명령을 실행하기 전에 교체해야 하는 기호 변수를 사용합니다.

예 **2.** 단계

시스템 관리자

1. System Manager에서 * 클러스터 * > * 설정 * 을 선택합니다.
2. 아래로 스크롤하여 * 보안 * 섹션으로 이동합니다.
3. OAuth 2.0 권한 부여 * 옆에 있는 * + * 를 클릭합니다.
4. 추가 옵션 * 을 선택합니다.
5. 다음과 같이 배포에 필요한 값을 제공합니다.
   - 이름
   - 응용 프로그램(http)
   - 공급자 JWKS URI입니다
   - 발급자 URI입니다
6. 추가 * 를 클릭합니다.

CLI를 참조하십시오

1. 정의를 다시 만듭니다.

```
security oauth2 client create -config-name <NAME> -provider-jwks-uri
<URI_JWKS> -application http -issuer <URI_ISSUER>
```

예를 들면 다음과 같습니다.

```
security oauth2 client create \
-config-name auth0 \
-provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-
realm/protocol/openid-connect/certs \
-application http \
-issuer https://superzap.dev.netapp.com:8443/realms/my-realm
```

3단계**: OAuth 2.0**을 활성화합니다

마지막 단계는 OAuth 2.0을 활성화하는 것입니다. ONTAP 클러스터에 대한 전역 설정입니다.

> ONTAP, 인증 서버 및 지원 서비스가 모두 올바르게 구성되었는지 확인하기 전까지는 OAuth 2.0 처리를 활성화하지 마십시오.

ONTAP 액세스 방법에 따라 올바른 절차를 선택합니다.

예 **3.** 단계

시스템 관리자

1. System Manager에서 * 클러스터 * > * 설정 * 을 선택합니다.
2. 아래로 스크롤하여 * 보안 섹션 * 을 찾습니다.
3. OAuth 2.0 권한 부여 * 옆에 있는 * → * 를 클릭합니다.
4. OAuth 2.0 권한 부여 * 를 활성화합니다.

CLI를 참조하십시오

1. OAuth 2.0 활성화:

   ```
   security oauth2 modify -enabled true
   ```

2. OAuth 2.0이 활성화되어 있는지 확인합니다.

   ```
   security oauth2 show
   Is OAuth 2.0 Enabled: true
   ```

OAuth 2.0을 사용하여 **REST API** 호출을 실행합니다

ONTAP의 OAuth 2.0 구현은 REST API 클라이언트 애플리케이션을 지원합니다. curl을 사용하여 간단한 REST API 호출을 실행하여 OAuth 2.0을 사용할 수 있습니다. 아래 예에서는 ONTAP 클러스터 버전을 검색합니다.

시작하기 전에

ONTAP 클러스터에 대해 OAuth 2.0 기능을 구성하고 사용하도록 설정해야 합니다. 여기에는 인증 서버 정의가 포함됩니다.

1단계**:** 액세스 토큰을 획득합니다

REST API 호출에 사용할 액세스 토큰을 얻어야 합니다. 토큰 요청은 ONTAP 외부에서 수행되며 정확한 절차는 인증 서버 및 해당 구성에 따라 다릅니다. 웹 브라우저, curl 명령 또는 프로그래밍 언어를 사용하여 토큰을 요청할 수 있습니다.

설명 목적으로 curl을 사용하여 Keycloak에서 액세스 토큰을 요청하는 방법에 대한 예가 아래에 나와 있습니다.

Keycloak 예

```
curl --request POST \
--location
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-
connect/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=dp-client-1' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'client_secret=5iTUf9QKLGxAoYa1iR33vlD5A2xq09V7'
```

반환된 토큰을 복사하여 저장해야 합니다.

2단계**: REST API** 호출을 실행합니다

유효한 액세스 토큰이 있으면 액세스 토큰과 함께 curl 명령을 사용하여 REST API 호출을 실행할 수 있습니다.

매개 변수 및 변수

컬링 예제의 두 변수는 아래 표에 설명되어 있습니다.

변수	설명
$FQDN_IP입니다	ONTAP 관리 LIF의 정규화된 도메인 이름 또는 IP 주소
$access_token입니다	인증 서버에서 발급한 OAuth 2.0 액세스 토큰

curl 예제를 실행하기 전에 먼저 Bash 셸 환경에서 이러한 변수를 설정해야 합니다. 예를 들어, Linux CLI에서 다음 명령을 입력하여 FQDN 변수를 설정하고 표시합니다.

```
FQDN_IP=172.14.31.224
echo $FQDN_IP
172.14.31.224
```

두 변수가 모두 로컬 Bash 셸에 정의되면 curl 명령을 복사하여 CLI에 붙여 넣을 수 있습니다. Enter * 키를 눌러 변수를 대체하고 명령을 실행합니다.

컬의 예

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster?fields=version" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $ACCESS_TOKEN"
```

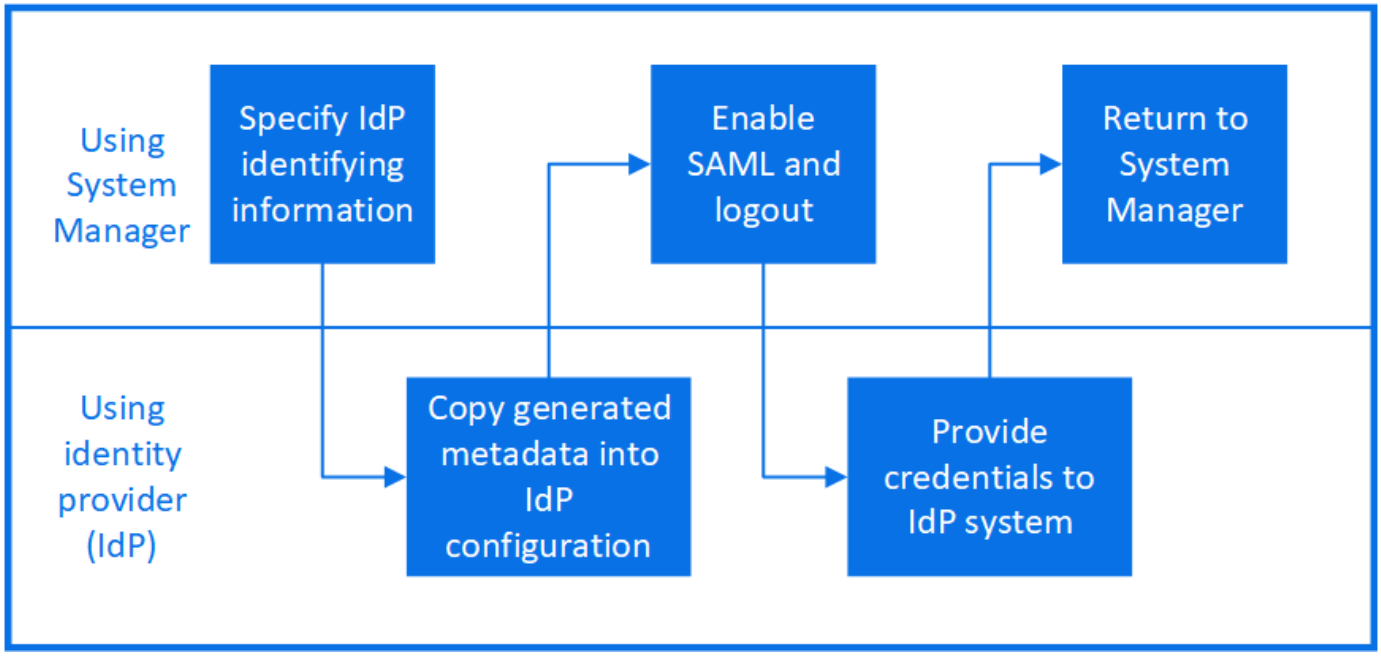
SAML 인증을 구성합니다

ONTAP 9.3부터 웹 서비스에 대한 SAML(Security Assertion Markup Language) 인증을 구성할 수 있습니다. SAML 인증이 구성 및 설정되면 사용자는 Active Directory 및 LDAP와 같은 디렉터리 서비스 공급자 대신 외부 ID 공급자(IDP)에 의해 인증됩니다.

SAML 인증을 활성화합니다

System Manager 또는 CLI를 사용하여 SAML 인증을 활성화하려면 다음 단계를 수행하십시오. 클러스터에서 ONTAP 9.7 이하를 실행 중인 경우에는 System Manager에서 따라야 하는 단계가 다릅니다. 시스템에서 사용할 수 있는 System Manager 온라인 도움말을 참조하십시오.

> SAML 인증을 활성화한 후에는 원격 사용자만 System Manager GUI에 액세스할 수 있습니다. SAML 인증이 활성화된 후에는 로컬 사용자가 System Manager GUI에 액세스할 수 없습니다.



시작하기 전에

- 원격 인증에 사용하려는 IDP를 구성해야 합니다.

  > 구성한 IDP에서 제공하는 설명서를 참조하십시오.

- IDP의 URI가 있어야 합니다.

이 작업에 대해

- SAML 인증은 'http' 및 'ontapi' 애플리케이션에만 적용됩니다.

  http와 ontapi 애플리케이션은 서비스 프로세서 인프라, ONTAP API, System Manager 등의 웹 서비스에서 사용됩니다.

- SAML 인증은 관리 SVM에 액세스하는 경우에만 적용됩니다.

다음 IdP는 System Manager에서 검증되었습니다.

- Active Directory 페더레이션 서비스
- Cisco Duo(다음 ONTAP 버전에서 검증:)
  - 9.7P21 이상 9.7 릴리즈(참조 "System Manager Classic 설명서")
  - 9.8P17 이상 9.8 릴리스
  - 9.9.1P13 이상 9.9 릴리스
  - 9.10.1P9 이상 9.10 릴리스
  - 9.11.1P4 이상 9.11 릴리즈
  - 9.12.1 이상 릴리즈
- 시바볼레스

환경에 따라 다음 단계를 수행하십시오.

예 **4.** 단계

시스템 관리자

1. 클러스터 > 설정 * 을 클릭합니다.
2. SAML 인증 * 옆에 있는 을 클릭합니다 ⚙.
3. SAML 인증 활성화 * 확인란이 선택되어 있는지 확인합니다.
4. IDP URI의 URL(포함)을 입력합니다 .
5. 필요한 경우 호스트 시스템 주소를 수정합니다.
6. 올바른 인증서가 사용되고 있는지 확인합니다.
   - 시스템이 "서버" 유형의 인증서를 하나만 사용하여 매핑된 경우 해당 인증서는 기본값으로 간주되어 표시되지 않습니다.
   - 시스템이 여러 인증서를 "서버" 유형으로 매핑한 경우 인증서 중 하나가 표시됩니다. 다른 인증서를 선택하려면 * 변경 * 을 클릭합니다.
7. 저장 * 을 클릭합니다. 확인 창에 메타데이터 정보가 표시되며, 이 정보는 클립보드에 자동으로 복사됩니다.
8. 지정한 IDP 시스템으로 이동하고 클립보드에서 메타데이터를 복사하여 시스템 메타데이터를 업데이트합니다.
9. System Manager의 확인 창으로 돌아가서 * 호스트 URI 또는 메타데이터 * 를 사용하여 IDP를 구성했는지 * 확인란을 선택합니다.
10. SAML 기반 인증을 활성화하려면 * 로그아웃 * 을 클릭합니다. IDP 시스템에 인증 화면이 표시됩니다.
11. IdP 시스템에서 SAML 기반 자격 증명을 입력합니다. 자격 증명이 확인되면 System Manager 홈 페이지로 이동합니다.

CLI를 참조하십시오

1. SAML 구성을 생성하여 ONTAP가 IDP 메타데이터에 액세스할 수 있도록 합니다.

   '* security SAML-SP create-IDP-Uri_IDP_Uri_-sp-host_ontap_host_name_ * '

   IDP_Uri는 IDP 메타데이터를 다운로드할 수 있는 IDP 호스트의 FTP 또는 HTTP 주소입니다.

   'ontap_host_name'은 SAML 서비스 공급자 호스트의 호스트 이름 또는 IP 주소이며, 이 경우 ONTAP 시스템입니다. 기본적으로 클러스터 관리 LIF의 IP 주소가 사용됩니다.

   ONTAP 서버 인증서 정보를 선택적으로 제공할 수 있습니다. 기본적으로 ONTAP 웹 서버 인증서 정보가 사용됩니다.

```
cluster_12::> security saml-sp create -idp-uri
https://example.url.net/idp/shibboleth

Warning: This restarts the web server. Any HTTP/S connections that
are active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 179] Job succeeded: Access the SAML SP metadata using the URL:
https://10.0.0.1/saml-sp/Metadata

Configure the IdP and Data ONTAP users for the same directory server
domain to ensure that users are the same for different
authentication methods. See the "security login show" command for
the Data ONTAP user configuration.
```

ONTAP 호스트 메타데이터에 액세스할 수 있는 URL이 표시됩니다.

2. IDP 호스트에서 ONTAP 호스트 메타데이터를 사용하여 IDP를 구성합니다.

   IDP 구성에 대한 자세한 내용은 IDP 설명서를 참조하십시오.

3. SAML 구성 활성화:

   '* security SAML-SP modify -is-enabled true*'

   'http' 또는 'ontapi' 애플리케이션에 액세스하는 기존 사용자는 자동으로 SAML 인증을 위해 구성됩니다.

4. SAML이 구성된 후 'http' 또는 'ontapi' 애플리케이션에 대한 사용자를 생성하려면 SAML을 새 사용자의 인증 방법으로 지정합니다.

   a. SAML 인증을 사용하여 새 사용자에 대한 로그인 방법을 생성합니다. + `* 보안 로그인 create-user-or-group-name_user_name_-application [http|ontapi] -authentication-method SAML-vserver_svm_name_ * '

      ```
      cluster_12::> security login create -user-or-group-name admin1
      -application http -authentication-method saml -vserver
      cluster_12
      ```

   b. 사용자 항목이 생성되었는지 확인합니다.

      '* 보안 로그인 쇼 * '

```
cluster_12::> security login show

Vserver: cluster_12

Second
User/Group                  Authentication                 Acct
Authentication
Name            Application Method        Role Name        Locked
Method
-------------- ----------- ------------- ---------------- ------
--------------
admin           console     password      admin            no
none
admin           http        password      admin            no
none
admin           http        saml          admin            -
none
admin           ontapi      password      admin            no
none
admin           ontapi      saml          admin            -
none
admin           service-processor
                            password      admin            no
none
admin           ssh         password      admin            no
none
admin1          http        password      backup           no
none
**admin1        http        saml          backup           -
none**
```

SAML 인증을 비활성화합니다

외부 ID 공급자(IDP)를 사용하여 웹 사용자 인증을 중지하려면 SAML 인증을 사용하지 않도록 설정할 수 있습니다. SAML 인증이 비활성화되면 Active Directory 및 LDAP와 같이 구성된 디렉터리 서비스 공급자가 인증에 사용됩니다.

환경에 따라 다음 단계를 수행하십시오.

예 **5.** 단계

시스템 관리자

1. 클러스터 > 설정 * 을 클릭합니다.
2. SAML Authentication * 에서 * Enabled * 토글 버튼을 클릭합니다.
3. *Optional*: 을(를) 클릭할 수도 있습니다 ⚙ SAML Authentication * 옆에 있는 * SAML Authentication * 확인란의 선택을 취소합니다.

CLI를 참조하십시오

1. SAML 인증 비활성화:

   '* security SAML-SP modify -is-enabled false * '

2. SAML 인증을 더 이상 사용하지 않거나 IDP를 수정하려는 경우 SAML 구성을 삭제합니다.

   '* 보안 SAML-SP 삭제 * '

SAML 구성 관련 문제를 해결합니다

SAML(Security Assertion Markup Language) 인증을 구성하지 못한 경우 SAML 구성이 실패한 각 노드를 수동으로 복구하고 장애를 복구할 수 있습니다. 복구 프로세스 중에 웹 서버가 다시 시작되고 활성 HTTP 연결 또는 HTTPS 연결이 중단됩니다.

이 작업에 대해

SAML 인증을 구성할 경우 ONTAP는 노드별로 SAML 구성을 적용합니다. SAML 인증을 설정하면 구성 문제가 있는 경우 ONTAP에서 자동으로 각 노드를 복구하려고 시도합니다. 노드에서 SAML 구성에 문제가 있는 경우 SAML 인증을 비활성화한 다음 SAML 인증을 다시 활성화할 수 있습니다. SAML 인증을 다시 설정한 후에도 하나 이상의 노드에 SAML 구성이 적용되지 않는 경우가 있을 수 있습니다. SAML 구성이 실패한 노드를 확인한 다음 해당 노드를 수동으로 복구할 수 있습니다.

단계

1. 고급 권한 레벨에 로그인합니다.

   ' * set-Privilege advanced * '

2. SAML 구성이 실패한 노드 식별:

   ' * security SAML-SP status show-instance * '

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                 Update Status: config-success
                Database Epoch: 9
   Database Transaction Count: 997
                    Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                          Node: node2
                 Update Status: config-failed
                Database Epoch: 9
   Database Transaction Count: 997
                    Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

3. 장애가 발생한 노드에서 SAML 구성을 복구합니다.

   '* security SAML-SP repair-node_node_name_ * '

```
cluster_12::*> security saml-sp repair -node node2

Warning: This restarts the web server. Any HTTP/S connections that are
active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 181] Job is running.
[Job 181] Job success.
```

   웹 서버가 다시 시작되고 활성화된 HTTP 연결 또는 HTTPS 연결이 모두 중단됩니다.

4. 모든 노드에서 SAML이 구성되었는지 확인합니다.

   ' * security SAML-SP status show-instance * '

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                 Update Status: config-success
                Database Epoch: 9
   Database Transaction Count: 997
                    Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                          Node: node2
                 Update Status: **config-success**
                Database Epoch: 9
   Database Transaction Count: 997
                    Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

관련 정보

"ONTAP 9 명령"

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.

웹 서비스에 대한 액세스를 관리합니다

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 파일 또는 코어 덤프 파일에 대한 액세스 요청이 있을 경우 'pi' 웹 서비스는 자동으로 노드에서 파일이 상주하는 다른 노드의 루트 볼륨으로 마운트 지점을 만듭니다. 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.

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.
- 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. TLSv.1 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.

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 엔진 관리를 위한 명령입니다

'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'
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.

웹 서비스에 대한 액세스를 구성합니다

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.

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

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.
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.

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.

   ⓘ '보안 로그인 생성' 명령을 사용하여 사용자의 액세스 방법을 추가합니다.

웹 서비스 관리를 위한 명령입니다

'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 9 명령"

노드의 마운트 지점을 관리하는 명령입니다

'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 9 명령"

SSL 관리

SSL 프로토콜은 웹 서버와 브라우저 간에 암호화된 연결을 설정하기 위해 디지털 인증서를 사용하여 웹 액세스의 보안을 개선합니다.

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

SVM(Cluster ora Storage Virtual Machine)의 SSL 프로토콜을 관리하려면 '보안 SSL' 명령을 사용합니다.

원하는 작업	이 명령 사용...
클러스터 oranSVM에 SSL을 활성화하고 디지털 인증서를 이 클러스터와 연결합니다	보안 SSL 수정
클러스터 oranSVM의 SSL 구성 및 인증서 이름을 표시합니다	보안 SSL 쇼

웹 서비스 액세스 문제를 해결합니다

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. LIF를 ping하는 데 'network ping' 명령을 사용합니다. 네트워크 구성에 대한 자세한 내용은 _Network Management Guide_를 참조하십시오.

이 액세스 문제는...	이 구성 오류로 인해 발생합니다.	오류를 해결하려면...
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.
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.

이 액세스 문제는...	이 구성 오류로 인해 발생합니다.	오류를 해결하려면...
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.
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.

인증서를 사용하여 원격 서버의 ID를 확인합니다

인증서 개요를 사용하여 원격 서버의 ID를 확인합니다

ONTAP는 보안 인증서 기능을 지원하여 원격 서버의 ID를 확인합니다.

ONTAP 소프트웨어는 다음과 같은 디지털 인증서 기능 및 프로토콜을 사용하여 보안 연결을 지원합니다.

- OCSP(온라인 인증서 상태 프로토콜)는 SSL 및 TLS(전송 계층 보안) 연결을 사용하여 ONTAP 서비스에서 디지털 인증서 요청 상태를 검증합니다. 이 기능은 기본적으로 비활성화되어 있습니다.
- 신뢰할 수 있는 루트 인증서의 기본 집합은 ONTAP 소프트웨어에 포함되어 있습니다.
- KMIP(Key Management Interoperability Protocol) 인증서를 통해 클러스터 및 KMIP 서버를 상호 인증할 수 있습니다.

디지털 인증서가 **OCSP**를 사용하여 유효한지 확인합니다

ONTAP 9.2부터 OCSP(온라인 인증서 상태 프로토콜)를 사용하면 ONTAP 응용 프로그램에서 TLS(전송 계층 보안) 통신을 사용하는 응용 프로그램이 OCSP가 활성화될 때 디지털 인증서 상태를 수신할 수 있습니다. 특정 애플리케이션에 대한 OCSP 인증서 상태 확인을 언제든지 활성화 또는 비활성화할 수 있습니다. 기본적으로 OCSP 인증서 상태 확인은 사용되지 않습니다.

필요한 것

이 작업을 수행하려면 고급 권한 수준 액세스 권한이 필요합니다.

이 작업에 대해

OCSP는 다음 애플리케이션을 지원합니다.

- AutoSupport
- EMS(이벤트 관리 시스템)
- TLS를 통한 LDAP
- 키 관리 상호 운용성 프로토콜(KMIP)
- 로깅 감사
- FabricPool
- SSH(ONTAP 9.13.1 로 시작)

단계

1. 권한 수준을 Advanced:'Set-Privilege advanced'로 설정합니다.
2. 특정 ONTAP 응용 프로그램에 대한 OCSP 인증서 상태 검사를 사용하거나 사용하지 않도록 설정하려면 적절한 명령을 사용합니다.

OCSP 인증서 상태를 통해 일부 응용 프로그램을 확인하려는 경우...	명령 사용...
활성화됨	`security config ocsp enable -app app name`
사용 안 함	`security config ocsp disable -app app name`

다음 명령을 실행하면 AutoSupport 및 EMS에 대한 OCSP 지원이 활성화됩니다.

```
cluster::*> security config ocsp enable -app asup,ems
```

OCSP가 활성화되면 애플리케이션은 다음 응답 중 하나를 수신합니다.

- 양호 - 인증서가 유효하며 통신이 진행됩니다.
- 해지 - 인증서는 발급 인증 기관에서 영구적으로 신뢰할 수 없는 것으로 간주되어 통신이 진행되지 않습니다.
- 알 수 없음 - 서버에 인증서에 대한 상태 정보가 없으며 통신이 진행되지 않습니다.
- OCSP 서버 정보가 인증서에 없습니다. 서버는 OCSP가 비활성화되어 TLS 통신을 계속하는 것처럼 작동하지만 상태 검사는 발생하지 않습니다.
- OCSP 서버의 응답이 없습니다. 응용 프로그램을 계속할 수 없습니다.

3. TLS 통신을 사용하는 모든 응용 프로그램에 대해 OCSP 인증서 상태 검사를 사용하거나 사용하지 않도록 설정하려면 적절한 명령을 사용합니다.

OCSP 인증서 상태가 모든 응용 프로그램의 상태를 확인하려는 경우...	명령 사용...
활성화됨	'보안 구성 OCSP 활성화 '-APP ALL'
사용 안 함	보안 구성 OCSP 비활성화 '-APP ALL'

이 옵션을 활성화하면 모든 응용 프로그램은 지정된 인증서가 양호, 취소 또는 알 수 없다는 서명된 응답을 받습니다. 인증서가 해지된 경우 응용 프로그램을 계속 진행할 수 없습니다. 애플리케이션이 OCSP 서버로부터 응답을 수신하지 못하거나 서버에 연결할 수 없는 경우 응용 프로그램을 계속 진행할 수 없습니다.

4. 'Security config OCSP show' 명령어를 사용하면 OCSP를 지원하는 모든 애플리케이션과 지원 상태를 확인할 수 있다.

```
cluster::*> security config ocsp show
         Application                        OCSP Enabled?
         --------------------               ---------------------
         autosupport                        false
         audit_log                          false
         fabricpool                         false
         ems                                false
         kmip                               false
         ldap_ad                            true
         ldap_nis_namemap                   true
         ssh                                true

         8 entries were displayed.
```

TLS 기반 응용 프로그램에 대한 기본 인증서를 봅니다

ONTAP 9.2부터 ONTAP는 TLS(전송 계층 보안)를 사용하는 ONTAP 응용 프로그램에 대해 신뢰할 수 있는 루트 인증서 기본 집합을 제공합니다.

필요한 것

기본 인증서는 생성 중 또는 ONTAP 9.2로 업그레이드 도중에만 관리 SVM에 설치됩니다.

이 작업에 대해

현재 클라이언트 역할을 하고 인증서 검증이 필요한 애플리케이션은 AutoSupport, EMS, LDAP, 감사 로깅, FabricPool입니다. 및 KMIP

인증서가 만료되면 사용자에게 인증서 삭제를 요청하는 EMS 메시지가 호출됩니다. 기본 인증서는 고급 권한 수준에서만 삭제할 수 있습니다.

> 기본 인증서를 삭제하면 일부 ONTAP 응용 프로그램이 예상대로 작동하지 않을 수 있습니다(예: AutoSupport 및 감사 로깅).

단계

1. security certificate show 명령을 사용하여 admin SVM에 설치된 기본 인증서를 볼 수 있습니다.

   '* security certificate show -vserver –type server-ca*'

```
fas2552-2n-abc-3::*> security certificate show -vserver fas2552-2n-abc-3
-type server-ca
Vserver    Serial Number   Common Name                             Type
---------- --------------- ---------------------------------------
------------
fas2552-2n-abc-3
           01              AAACertificateServices
server-ca
    Certificate Authority: AAA Certificate Services
          Expiration Date: Sun Dec 31 18:59:59 2028
```

클러스터와 KMIP 서버를 상호 인증합니다

클러스터 및 KMIP 서버 개요를 상호 인증

KMIP(Key Management Interoperability Protocol) 서버와 같은 외부 키 관리자를 함께 사용하면 키 관리자가 SSL을 통해 KMIP를 사용하여 클러스터와 통신할 수 있습니다. 애플리케이션 또는 특정 기능(예: 스토리지 암호화 기능)에서 보안 데이터 액세스를 제공하기 위해 보안 키가 필요한 경우 이 작업을 수행합니다.

클러스터에 대한 인증서 서명 요청을 생성합니다

보안 인증서 'generate-csr' 명령을 사용하여 인증서 서명 요청(CSR)을 생성할 수 있습니다. 요청을 처리한 후 CA(인증 기관)에서 서명된 디지털 인증서를 보냅니다.

필요한 것

이 작업을 수행하려면 클러스터 관리자 또는 SVM 관리자여야 합니다.

단계

1. CSR 생성:

   '* 보안 인증서 생성 - csr-common-name_FQDN_or_common_name_-size 512 | 1024 | 1536 | 2048-country_country_-state_-지역성_-organization_organization_-unit_unit_-email-addr_email_of_contact_-hash-function SHA1 | SHA256 | MD5*'

   전체 명령 구문은 man 페이지를 참조하십시오.

   다음 명령은 SHA256 해싱 기능에 의해 생성된 2,048비트 개인 키를 가진 CSR을 생성하고, 사용자 정의 공통 이름이 server1.companyname.com 인 회사의 IT 부서에서 사용하는 사용자 정의 공용 키가 미국 캘리포니아주 서니베일에 있습니다. SVM 연락처 관리자의 이메일 주소는 web@example.com 입니다. 출력에 CSR과 개인 키가 표시됩니다.

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.
```

2. CSR 출력에서 인증서 요청을 복사한 다음 전자 양식(예: 전자 메일)으로 신뢰할 수 있는 타사 CA로 보내 서명합니다.

   요청을 처리한 후 CA는 서명된 디지털 인증서를 보냅니다. 개인 키와 CA 서명 디지털 인증서의 복사본을 유지해야 합니다.

클러스터에 대한 **CA** 서명 서버 인증서를 설치합니다

SSL 서버에서 클러스터 또는 SVM(Storage Virtual Machine)을 SSL 클라이언트로 인증할 수 있도록 하려면 클러스터 또는 SVM에 클라이언트 유형과 함께 디지털 인증서를 설치합니다. 그런 다음 서버에 설치하기 위해 SSL 서버 관리자에게 클라이언트-CA 인증서를 제공합니다.

필요한 것

SSL 서버의 루트 인증서를 이미 클러스터 또는 SVM에 'server-ca' 인증서 유형으로 설치해야 합니다.

단계

1. 클라이언트 인증에 자체 서명된 디지털 인증서를 사용하려면 type client 매개 변수를 사용하여 Security certificate create 명령을 사용합니다.

2. 클라이언트 인증에 CA 서명 디지털 인증서를 사용하려면 다음 단계를 수행하십시오.

   a. 보안 인증서 'generate-csr' 명령을 사용하여 디지털 인증서 서명 요청(CSR)을 생성합니다.

      ONTAP는 인증서 요청과 개인 키가 포함된 CSR 출력을 표시하고 나중에 참조할 수 있도록 출력을 파일로 복사하도록 알려 줍니다.

   b. 전자 양식(예: 전자 메일)으로 CSR 출력에서 인증서 요청을 신뢰할 수 있는 CA로 보내 서명합니다.

      나중에 참조할 수 있도록 개인 키와 CA 서명 인증서의 복사본을 유지해야 합니다.

   요청을 처리한 후 CA는 서명된 디지털 인증서를 보냅니다.

   a. '-type client' 매개 변수와 함께 보안 인증서 설치 명령을 사용하여 CA 서명 인증서를 설치합니다.
   b. 메시지가 표시되면 인증서와 개인 키를 입력한 다음 * Enter * 키를 누릅니다.
   c. 메시지가 표시되면 추가 루트 또는 중간 인증서를 입력하고 * Enter * 를 누릅니다.

      신뢰할 수 있는 루트 CA에서 시작하고 사용자에게 발급된 SSL 인증서로 끝나는 인증서 체인이 중간 인증서를 누락하는 경우 클러스터나 SVM에 중간 인증서를 설치합니다. 중간 인증서는 최종 엔터티 서버 인증서를 발급하기 위해 신뢰할 수 있는 루트에서 발급하는 하위 인증서입니다. 그 결과 신뢰할 수 있는 루트 CA에서 시작하여 중간 인증서를 거쳐 사용자에게 발급된 SSL 인증서로 끝나는 인증서 체인이 만들어집니다.

3. 서버에 설치하기 위해 SSL 서버 관리자에게 클러스터 또는 SVM의 '클라이언트-CA' 인증서를 제공합니다.

   인스턴스, 클라이언트-CA 형식의 매개 변수를 가진 보안 인증서 표시 명령은 클라이언트-CA 인증서 정보를 표시합니다.

KMIP 서버용 CA 서명 클라이언트 인증서를 설치합니다

클라이언트 및 서버 CA 유형과 함께 KMIP(Key Management Interoperability Protocol)(-subtype KMIP-cert 매개 변수)의 인증서 하위 유형은 클러스터 및 KMIP 서버와 같은 외부 키 관리자를 상호 인증하는 데 인증서가 사용됨을 나타냅니다.

이 작업에 대해

KMIP 인증서를 설치하여 KMIP 서버를 클러스터에 대한 SSL 서버로 인증합니다.

단계

1. KMIP 서버용 KMIP 인증서를 설치하려면 '-type server-ca' 및 '-subtype KMIP-cert' 매개 변수와 함께 'Security certificate install' 명령을 사용하십시오.
2. 메시지가 표시되면 인증서를 입력한 다음 Enter 키를 누릅니다.

   ONTAP는 나중에 참조할 수 있도록 인증서 복사본을 보관하도록 알려 줍니다.

```
cluster1::> security certificate install -type server-ca -subtype kmip-
cert
-vserver cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/Er4wDQYJKoZIhvcNAQEFBQAwXzELMAkG
2JhucwNhkcV8sEVAbkSdjbCxlnRhLQ2pRdKkkirWmnWXbj9T/UWZYB2oK0z5XqcJ
2HUw19JlYD1n1khVdWk/kfVIC0dpImmClr7JyDiGSnoscxlIaU5rfGW/D/xwzoiQ
...
-----END CERTIFICATE-----


You should keep a copy of the CA-signed digital certificate for future
reference.

cluster1::>
```