



관리자 인증 및 **RBAC** 관리

ONTAP 9

NetApp
April 24, 2024

목차

관리자 인증 및 RBAC 관리	1
CLI를 사용한 관리자 인증 및 RBAC 개요	1
관리자 인증 및 RBAC 워크플로	1
관리자 인증 및 RBAC 구성을 위한 워크시트	2
로그인 계정을 만듭니다	13
액세스 제어 역할을 관리합니다	27
관리자 계정을 관리합니다	34
여러 관리자 검증 관리	58

관리자 인증 및 RBAC 관리

CLI를 사용한 관리자 인증 및 RBAC 개요

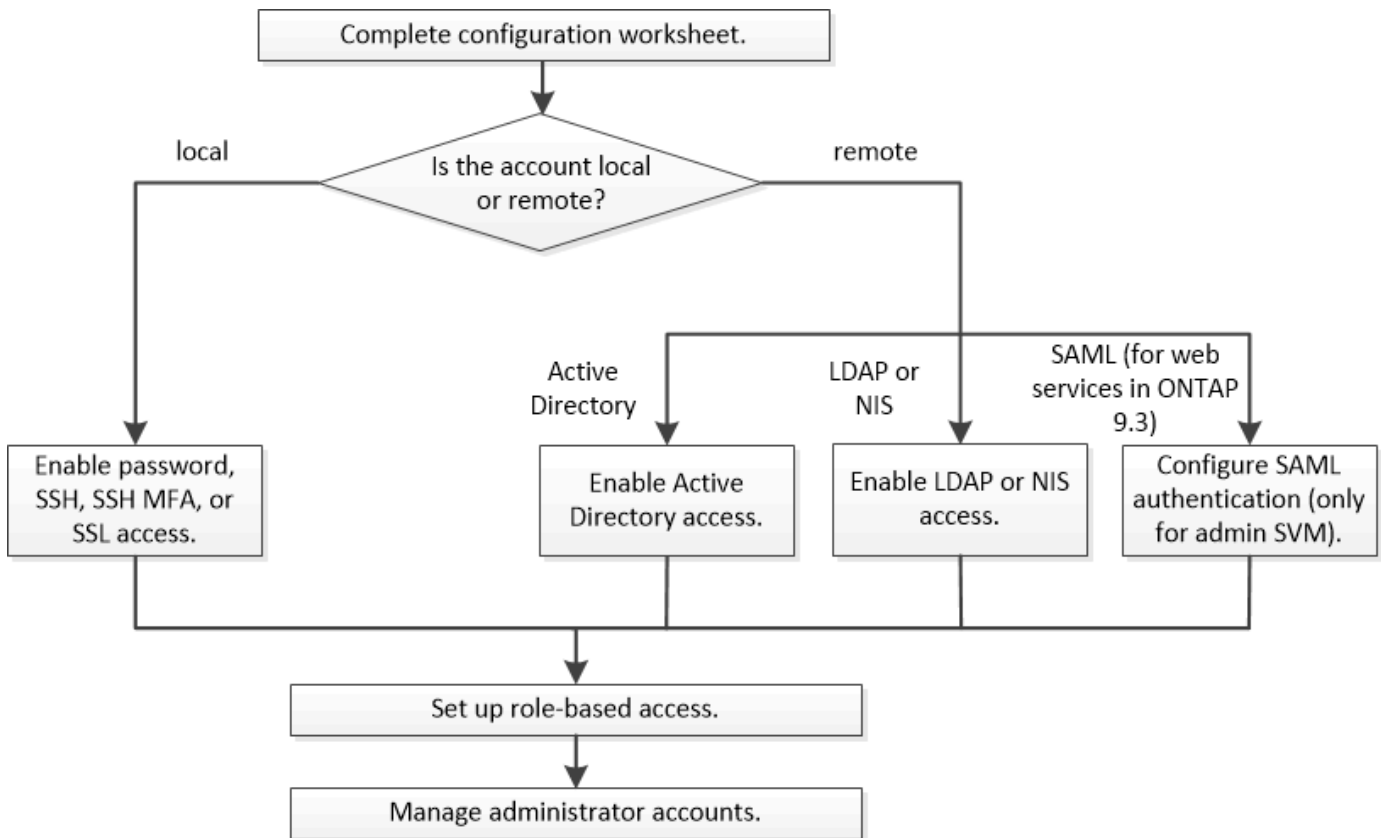
ONTAP 클러스터 관리자 및 SVM(스토리지 가상 시스템) 관리자의 로그인 계정을 활성화할 수 있습니다. 역할 기반 액세스 제어(RBAC)를 사용하여 관리자의 기능을 정의할 수도 있습니다.

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 사용자에게 액세스할 수 있습니다. 사용자 이름 또는 그룹 이름을 여러 응용 프로그램과 연결할 수 있습니다.	

'-응용 프로그램'	<p>스토리지 VM에 액세스하는 데 사용되는 애플리케이션:</p> <ul style="list-style-type: none"> • http입니다 • ontapi • 'NMP'입니다 • "쉬" 	
'-AuthMethod'입니다	<p>계정을 인증하는 데 사용되는 메소드:</p> <ul style="list-style-type: none"> • 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'	<p>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.</p>	
'-역할'	<p>계정에 할당된 액세스 제어 역할:</p> <ul style="list-style-type: none"> • 클러스터(관리자 스토리지 VM)의 경우 기본값은 admin. • 데이터 스토리지 VM의 경우 기본값은 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	<p>다단계 인증의 경우 두 번째 인증 방법:</p> <ul style="list-style-type: none"> • "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 <p>인증 순서는 항상 공개 키와 암호 순서로 표시됩니다.</p>	
'-is-ldap-fastbind'	<p>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."</p>	

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	<p>Duo에 SSH 애플리케이션을 등록할 때 얻은 API 호스트 이름입니다. 예를 들면 다음과 같습니다.</p> <pre>api- <HOSTNAME>.duosecurity.com</pre>	
-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	<p>지정된 HTTP 프록시를 사용합니다. HTTP 프록시에 인증이 필요한 경우 프록시 URL에 자격 증명을 포함합니다. 예를 들면 다음과 같습니다.</p> <pre>http- proxy=http://username :password@proxy.example.org:8080</pre>	
-autopush	<p>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.</p> <p>를 사용하여 구성 시 autopush = true, 설정하는 것이 좋습니다 max-prompts = 1.</p>	

-max-prompts	<p>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.</p> <p>예를 들어, When <code>max-prompts = 1</code>, 사용자가 첫 번째 프롬프트에서 성공적으로 인증해야 하는 반면 IF <code>'max-prompts = 2'</code> 초기 프롬프트에서 잘못된 정보를 입력하면 다시 인증하라는 메시지가 표시됩니다.</p> <p>를 사용하여 구성 시 <code>autopush = true</code>, 설정하는 것이 좋습니다 <code>max-prompts = 1</code>.</p> <p>최상의 경험을 위해 공개 키 인증만 있는 사용자는 항상 을(를) 가질 수 있습니다 <code>max-prompts</code> 를 로 설정합니다 1.</p>	
-enabled	<p>Duo 이중 인증을 활성화합니다. 를 로 설정합니다 <code>true</code> 기본적으로 사용됩니다. 활성화되면 구성된 매개 변수에 따라 SSH 로그인 중에 Duo 이중 인증이 적용됩니다. Duo가 비활성화된 경우(로 설정 <code>false</code>), Duo 인증은 무시됩니다.</p>	

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'	<p>(선택 사항) 역할에 대한 액세스 수준입니다. 명령 디렉토리의 경우:</p> <ul style="list-style-type: none"> • "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 <p>비내장 명령어 _ (create, modify, delete, sHow로 끝내지 않는 명령어):</p> <ul style="list-style-type: none"> • "없음"(사용자 지정 역할의 기본값)은 명령에 대한 액세스를 거부합니다 • "재담만"은 적용할 수 없습니다 • 모두 명령을 사용할 수 있는 권한을 부여합니다 <p>내장 명령에 대한 액세스를 부여하거나 거부하려면 명령 디렉토리를 지정해야 합니다.</p>	
'-query'	(선택 사항) 명령 또는 명령 디렉토리의 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 큼니다.	
'-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	<p>(선택 사항) ONTAP 9.13.1 부터는 SSH 공개 키와 X.509 인증서 연결을 관리할 수 있습니다.</p> <p>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:</p> <ul style="list-style-type: none"> • <code>install</code>: 지정된 PEM 인코딩된 X.509 인증서를 설치하고 SSH 공개 키와 연결합니다. 설치할 인증서의 전체 텍스트를 포함합니다. • <code>modify</code>: 기존 PEM 인코딩된 X.509 인증서를 지정된 인증서와 업데이트하고 SSH 공개 키에 연결합니다. 새 인증서의 전체 텍스트를 포함합니다. • <code>delete</code>: SSH 공개 키와 기존 X.509 인증서 연결을 제거합니다. 	

CA 서명 서버 디지털 인증서를 설치합니다

이러한 값은 예 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'	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 <code>us</code> 입니다. 코드 목록은 <code>man</code> 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 예 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''	<p>인증서 유형:</p> <ul style="list-style-type: none"> • 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 vservice 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 vservice 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 심표로 구분하여 나열합니다.	
'-스키마'	클라이언트가 LDAP 쿼리를 만드는 데 사용하는 스키마입니다.	
'-use-start-tls'	<div> <div>  </div> <div> <p>TLS 시작은 데이터 스토리지 VM에 대한 액세스에만 지원됩니다. 관리자 스토리지 VM에 대한 액세스는 지원되지 않습니다.</p> </div> </div>	

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'	<ul style="list-style-type: none"> • 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'	<p>네임 서비스 데이터베이스:</p> <ul style="list-style-type: none"> • 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"	<p>쉼표로 구분된 목록에서 이름 서비스 소스를 조회하는 순서:</p> <ul style="list-style-type: none"> • '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 사용자에게 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 vadmin1이 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

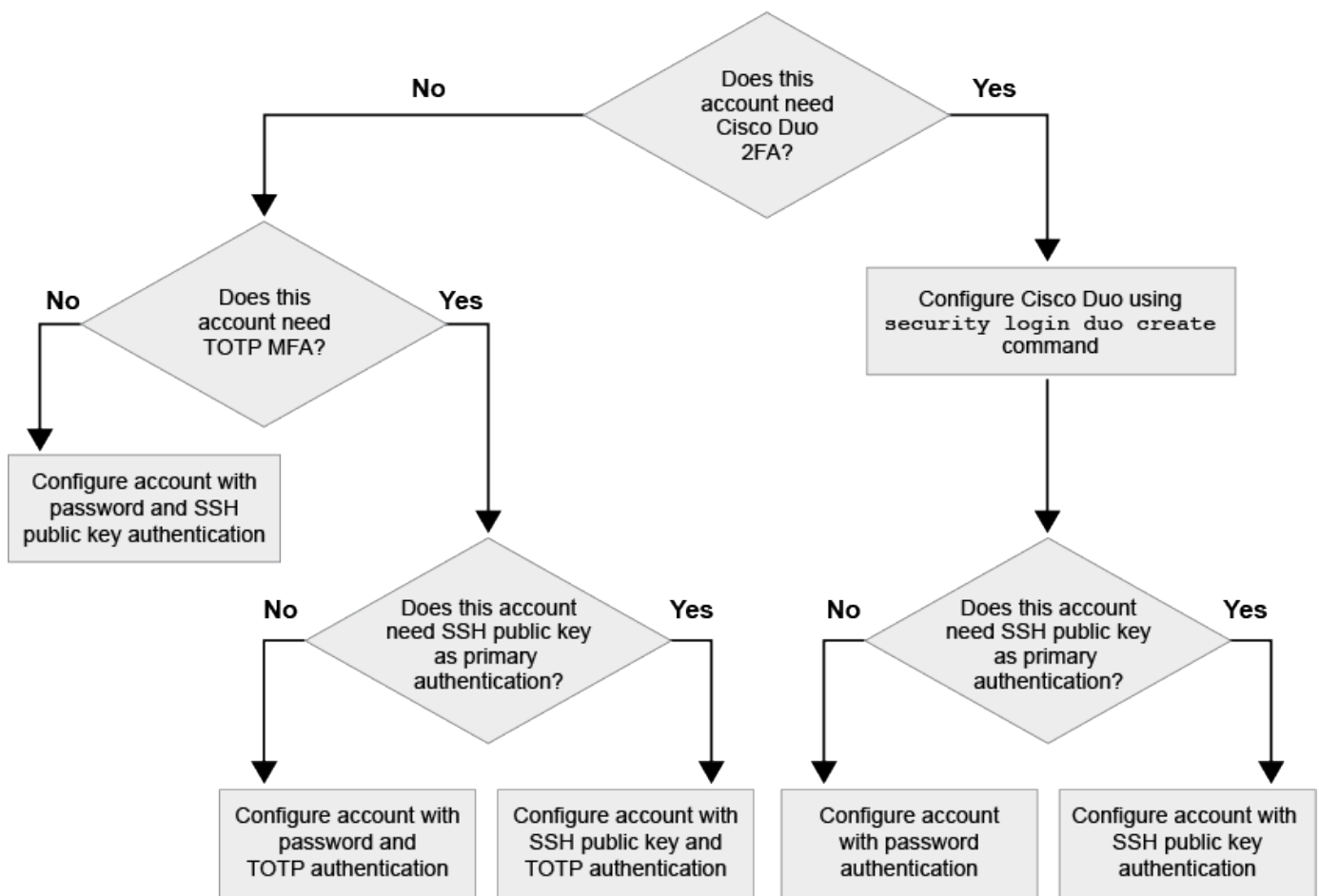
다단계 인증 개요

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 사용자에게 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	토평
	사용자 암호	토평
	SSH 공개 키	Cisco 듀오
	사용자 암호입니다	Cisco 듀오
ONTAP 9.13.1	SSH 공개 키	토평
	사용자 암호입니다	토평
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 MFA를 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 MFA를 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 MFA에 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 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	<pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role></pre>
9.13.1 이상	도메인	공개 키	<p>• 신규 사용자용 *</p> <pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role></pre> <p>• 기존 사용자의 경우 *</p> <pre>security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role></pre>
9.0 이상	도메인	없음	<pre>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]</pre>

AD 그룹의 경우 *

ONTAP 버전입니다	기본 인증	보조 인증	명령
9.0 이상	도메인	없음	<pre>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]</pre>

+ 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 사용자에게 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 사용자에게 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 사용자에게 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 "재판" 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 디렉터리 액세스는 상위 디렉터리 액세스보다 우선합니다.

역할이 명령 디렉터리로 정의된 후 특정 명령이나 상위 디렉터리의 하위 디렉터리에 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	<ul style="list-style-type: none"> • 모든 명령 디렉토리(기본값) • security login rest-role • security login role
읽기 전용	<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • '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
<ul style="list-style-type: none"> • '보안 로그인 비밀번호' <p>사용자 계정 로컬 암호 및 키 정보 관리에만 사용됩니다</p> <ul style="list-style-type: none"> • '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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 svadmin2 SVM을 위해 engData2. 공개 키에는 인덱스 번호 6이 할당됩니다.

```
cluster1::> security login publickey create -vserver engData2 -username svadmin2 -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 `svadmin2` SVM을 위해 `engData2` 인덱스 번호 6.

```
cluster1::> security login publickey modify -vserver engData2 -username  
svadmin2 -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 `svadmin3` SVM을 위해 `engData3` 인덱스 번호 7.

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

SSH 로그인에 Cisco Duo 2FA를 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 사용자에게 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 ["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 vservice 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 매개 변수로, 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 사용자에게 대해 Cisco Duo SSH 인증을 비활성화할 수 있습니다.

단계

1. SSH를 사용하여 ONTAP 계정에 로그인합니다.
2. SSH 사용자에게 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 사용자에게 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(certification 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-----

```
MIIBGjCBxQIBADBqMRQwEgYDVQQDEwtLEGFtcGxlLmNvbTELMakGA1UEBhMCVVMx
CTAHBgNVBAgTADAEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAStADEPMA0G
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApTlnzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3alwoUsb13wfEvQnHVFNCi
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBcWUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsfHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
```

Private Key :

-----BEGIN RSA PRIVATE KEY-----

```
MIIBOwIBAAJBAPXFanNoJApTlnzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3alwoUsb13wfEvQnHVFNCi2ninsJ8CAwEAAQJAWt2AO+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. ONTAP은 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.

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCA ZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMACGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTAD EJMACGA1UECXMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRh cHAuY29tMQswCQYDVQQG
EwJVUzEJMACGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTAD EJMACGA1UECXMAM
Q8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBI AkeA yXrK2sry
-----END CERTIFICATE-----
```

```
Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLyCsUdXA7hXhumHNpvF
C61X2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM70tbUsgPKw+QCCh9dF1jmuQKeDr+wUMWkn1DeGrfhILpzfJGHR LJ
z7UCIQDr8d3gOG71UyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuS18U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEArlmnrFYC8KwE9k7A0ylRzBLdUwK9
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+zCCBGsgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQA wgb s x JDAiBgNVBAcTG1Zh
bGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsT LFZhbGlDZXJ0IENsYXNzID IgUG9saWN5IFZhbGlkYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWewluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFroZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECXMOR28gRGFkZ HkgQ2xhc3MgMiBDZXJ0
-----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-----
```

```
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwbG9zJDAiBgNVBACzG1ZhbG1DZXJ0
IFZhbG1kYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTTFZhbG1DZXJ0IENsYXNzIDIGUG9saWN5IFZhbG1kYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQUDEXhodHRwOi8vd3d3LnZhbG1jZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDtk5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBACzG1ZhbG1DZXJ0IFZhbG1kYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTTFZhbG1DZXJ0IENs
YXNzIDIGUG9saWN5IFZhbG1kYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQUDEXhodHRw
-----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 수입입니다.
 - 저장된 클라이언트/서버 인증서 수
 - 저장된 로컬 인증 기관의 수입입니다.
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 *	<ul style="list-style-type: none">• [install-trusted-cert]• 신뢰할 수 있는 인증 기관을 삭제합니다• 신뢰할 수 있는 인증 기관을 갱신합니다
• 클라이언트/서버 인증서 *	<ul style="list-style-type: none">• [install-cs-cert]• [gen-cs-cert]• [delete-cs-cert]• [renew-cs-cert]
• 로컬 인증 기관 *	<ul style="list-style-type: none">• 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.

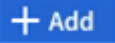
단계

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 .
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.

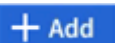
단계

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 .
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 .
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.

ONTAP은 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`의 `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.

- 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.

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

다음 명령을 실행하면 SVM `vs0`에서 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 하나

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. 추적할 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_rules`라고도 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'	'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 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.

다음은 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

- 클러스터 > 설정 * 을 클릭합니다
- 을 클릭합니다 → 사용자 및 역할 * 옆에 있습니다
- 을 클릭합니다 + Add 사용자 * 에서
- 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.

- 클러스터 > 설정 * 을 클릭합니다
- 을 클릭합니다 ⚙ 보안 * 섹션의 * 다중 관리자 승인 * 옆에 있습니다.
- 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.
- 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
- 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	<p>'보안 multi-admin-verify modify-approval-group1_[,group2...] [-필수-승인자_nn_] - 활성화된 참 [-실행-만료 [nnh] [nnm] [nns] [- 승인-만료 [nnh] [nns] [nns]]</p> <ul style="list-style-type: none"> 예 *: 다음 명령을 실행하면 1개의 승인 그룹, 2개의 필수 승인자 및 기본 만료 기간이 포함된 MAV가 활성화됩니다. <pre>cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true</pre> <p>최소 1개를 추가하여 초기 구성을 완료합니다 "작업 규칙."</p>
MAV 구성 수정(MAV 승인 필요)	'보안 Multi-admin-Verify approval-group modify [-approval-group1_[,group2...] [-필수-승인자_nn_] [-실행-만료 [nnh] [nnm] [nns] [- 승인-만료 [nnh] [nns]]
MAV 기능을 확인합니다	<p>'보안 멀티-관리-검증 쇼'</p> <ul style="list-style-type: none"> 예: * <pre>cluster-1::> security multi-admin-verify show Is Required Execution Approval Approval Enabled Approvers Expiry Expiry Groups ----- true 2 1h 1h mav-grp1</pre>
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-vsrm20::> 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 " <u>protected_operation</u> "[-query_operation_subsef][parameters]'
현재 관리자의 자격 증명을 수정합니다	security login modify <parameters> <ul style="list-style-type: none"> • 예 *: 다음 규칙에 따라 루트 볼륨을 삭제해야 합니다. <pre>security multi-admin-verify rule create-operation "volume delete" -query "-vserver vs0"</pre>
규칙을 수정합니다	'Security multi-admin-verify rule modify-operation " <u>protected_operation</u> "[parameters]'
규칙을 삭제합니다	'Security multi-admin - verify rule delete-operation " <u>protected_operation</u> " _'
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 voll -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 voll
    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 voll -vserver vs0
```

Info: Volume "voll" 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 voll_*" 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 "voll" 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 voll
    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 voll -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
```

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: -
```


저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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