



ONTAP 강화 지침

ONTAP 9

NetApp
July 18, 2024

목차

ONTAP 강화 지침	1
ONTAP 보안 강화 개요	1
ONTAP 이미지 검증	1
로컬 스토리지 관리자 계정	1
시스템 관리 방법	18
ONTAP 자율 랜섬웨어 방어	23
스토리지 관리 시스템 감사	24
스토리지 암호화	25
데이터 복제 암호화	28
전송 중인 IPsec 데이터 암호화	29
TLS 및 SSL 관리	30
CA 서명 디지털 인증서를 만듭니다	31
온라인 인증서 상태 프로토콜입니다	32
SSHv2 관리	32
NetApp AutoSupport를 참조하십시오	33
Network Time Protocol의 약어입니다	34
NAS 파일 시스템 로컬 계정(CIFS 작업 그룹)	34
NAS 파일 시스템 감사	35
CIFS SMB 서명 및 봉인을 구성하고 사용하도록 설정합니다	37
NFS 보안	37
Lightweight Directory Access Protocol 서명 및 봉인을 활성화합니다	39
NetApp FPolicy를 생성하여 사용합니다	40
LIF 보안	42
프로토콜 및 포트 보안	42
보안 리소스	46

ONTAP 강화 지침

ONTAP 보안 강화 개요

ONTAP에서 제공하는 제어 기능을 사용하면 업계 최고의 데이터 관리 소프트웨어인 ONTAP 스토리지 운영 체제를 강화할 수 있습니다. ONTAP의 지침 및 구성 설정을 사용하여 조직에서 정보 시스템의 기밀성, 무결성 및 가용성에 대해 규정된 보안 목표를 충족할 수 있도록 지원하십시오.

현재 위협 환경의 진화는 조직이 가장 중요한 자산인 데이터와 정보를 보호하기 위한 고유한 과제를 안고 있습니다. 우리가 직면하고 있는 지능적이고 동적인 위협과 취약성은 갈수록 정교해지고 있습니다. 잠재적 침입자의 측면에서 단독 처리 및 정찰 기법의 효과성이 높아짐에 따라 시스템 관리자는 사전에 데이터 및 정보의 보안을 다루어야 합니다.



2024년 7월부터 이전에 PDF로 게시된 기술 보고서의 콘텐츠가 ONTAP 제품 설명서와 통합되었습니다. 이제 ONTAP 보안 문서에는 ONTAP_에 대한 _TR-4569: 보안 강화 가이드의 내용이 포함되어 있습니다.

ONTAP 이미지 검증

ONTAP는 업그레이드 및 부팅 시 ONTAP 이미지가 유효한지 확인하는 메커니즘을 제공합니다.

이미지 검증 업그레이드

코드 서명을 활용하면 무중단 이미지 업데이트 또는 자동화된 무중단 이미지 업데이트, CLI 또는 ONTAP API를 통해 설치된 ONTAP 이미지가 NetApp에서 실제로 생성되며 무단 변경이 이뤄지지 않았는지 확인할 수 있습니다. 업그레이드 이미지 검증 기능은 ONTAP 9.3에 도입되었습니다.

이 기능은 ONTAP 업그레이드 또는 재버전에 대한 터치 없는 보안 향상 기능입니다. 사용자는 최상위 수준 "image.tgz" 서명을 선택적으로 확인하는 경우를 제외하고 다른 작업을 수행할 수 없습니다.

부팅 시간 이미지 검증

ONTAP 9.4부터는 UEFI(통합 확장 펌웨어 인터페이스) 보안 부팅이 NetApp AFF A800, AFF A220, FAS2750, FAS2720 시스템과 UEFI BIOS를 사용하는 후속 차세대 시스템에서 지원됩니다.

전원을 켜는 동안 부트로더는 로드된 각 모듈과 연결된 서명을 사용하여 보안 부팅 키의 화이트리스트 데이터베이스를 검증합니다. 각 모듈이 검증되고 로드된 후 부팅 프로세스는 ONTAP 초기화를 계속합니다. 모듈에 대한 서명 검증이 실패하면 시스템이 재부팅됩니다.



이러한 항목은 ONTAP 이미지 및 플랫폼 BIOS에 적용됩니다.

로컬 스토리지 관리자 계정

역할, 응용 프로그램 및 인증

ONTAP는 보안을 중시하는 기업에 다양한 로그인 응용 프로그램 및 방법을 통해 다양한

관리자에게 세분화된 액세스를 제공할 수 있는 기능을 제공합니다. 이를 통해 고객은 데이터 중심의 제로 트러스트 모델을 만들 수 있습니다.

다음은 관리자 및 스토리지 가상 머신 관리자가 사용할 수 있는 역할입니다. 로그인 응용 프로그램 방법과 로그인 인증 방법이 지정됩니다.

역할

사용자는 역할 기반 액세스 제어(RBAC)를 사용하여 직무 역할 및 기능에 필요한 시스템 및 옵션에만 액세스할 수 있습니다. ONTAP의 RBAC 솔루션은 사용자의 관리 액세스를 정의된 역할에 허용된 수준으로 제한하므로 관리자가 할당된 역할별로 사용자를 관리할 수 있습니다. ONTAP는 몇 가지 미리 정의된 역할을 제공합니다. 운영자와 관리자는 사용자 지정 액세스 제어 역할을 생성, 수정 또는 삭제할 수 있으며 특정 역할에 대한 계정 제한을 지정할 수 있습니다.

클러스터 관리자를 위한 사전 정의된 역할

이 역할은...	이 수준의 액세스 권한...	명령 또는 명령 디렉토리로 이동합니다
admin	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)
backup	모두	'vserver services ndmp'
읽기 전용	'볼륨'	없음
기타 모든 명령 디렉토리(기본값)	readonly	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.

스토리지 가상 머신(SVM) 관리자를 위한 사전 정의된 역할

역할 이름	제공합니다
vsadmin	<ul style="list-style-type: none"> • 사용자 계정 로컬 암호 및 키 정보를 관리합니다 • 볼륨 이동을 제외하고 볼륨을 관리합니다 • 할당량, Qtree, 스냅샷 복사본 및 파일을 관리합니다 • LUN 관리 • 권한 있는 삭제를 제외하고 SnapLock 작업을 수행합니다 • 프로토콜 구성: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC 및 NVMe/TCP • DNS, LDAP 및 NIS 서비스 구성 • 작업을 모니터링합니다 • 네트워크 연결 및 네트워크 인터페이스를 모니터링합니다 • SVM의 상태를 모니터링합니다
vsadmin-volume	<ul style="list-style-type: none"> • 사용자 계정 로컬 암호 및 키 정보를 관리합니다 • 볼륨 이동을 포함한 볼륨 관리 • 할당량, Qtree, 스냅샷 복사본 및 파일을 관리합니다 • LUN 관리 • 프로토콜 구성: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC 및 NVMe/TCP • DNS, LDAP 및 NIS 서비스 구성 • 네트워크 인터페이스를 모니터링합니다 • SVM의 상태를 모니터링합니다
vsadmin-protocol	<ul style="list-style-type: none"> • 사용자 계정 로컬 암호 및 키 정보를 관리합니다 • 프로토콜 구성: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC 및 NVMe/TCP • DNS, LDAP 및 NIS 서비스 구성 • LUN 관리 • 네트워크 인터페이스를 모니터링합니다 • SVM의 상태를 모니터링합니다

vsadmin-backup	<ul style="list-style-type: none"> • 사용자 계정 로컬 암호 및 키 정보를 관리합니다 • NDMP 작업을 관리합니다 • 복원된 볼륨을 읽기/쓰기로 만듭니다 • SnapMirror 관계 및 스냅샷 복사본 관리 • 볼륨 및 네트워크 정보를 봅니다
vsadmin-snaplock	<ul style="list-style-type: none"> • 사용자 계정 로컬 암호 및 키 정보를 관리합니다 • 볼륨 이동을 제외하고 볼륨을 관리합니다 • 할당량, Qtree, 스냅샷 복사본 및 파일을 관리합니다 • 권한 있는 삭제를 포함한 SnapLock 작업을 수행합니다 • 프로토콜 구성: NFS 및 SMB • DNS, LDAP 및 NIS 서비스 구성 • 작업을 모니터링합니다 • 네트워크 연결 및 네트워크 인터페이스를 모니터링합니다
vsadmin-readonly	<ul style="list-style-type: none"> • 사용자 계정 로컬 암호 및 키 정보를 관리합니다 • SVM의 상태를 모니터링합니다 • 네트워크 인터페이스를 모니터링합니다 • 볼륨 및 LUN 보기 • 서비스 및 프로토콜 보기

응용 프로그램 방법

응용 프로그램 메서드는 로그인 메서드의 액세스 유형을 지정합니다. 가능한 값에는 console, http, ontapi, rsh, snmp, service-processor, ssh, 및 `telnet`가 포함됩니다.

이 매개 변수를 설정하면 service-processor 사용자에게 서비스 프로세서에 대한 액세스 권한이 부여됩니다. 이 매개 변수를 로 설정할 service-processor -authentication-method 경우 서비스 프로세서가 암호 인증만 지원하므로 매개 변수를 로 설정해야 password 합니다. SVM 사용자 계정은 서비스 프로세서에 액세스할 수 없습니다. 따라서 이 매개 변수가 로 설정된 경우 연산자 및 관리자는 매개 변수를 사용할 수 -vserver `service-processor` 없습니다.

에 대한 액세스를 더 제한하려면 service-processor 명령을 system service-processor ssh add-allowed-addresses`사용하십시오. 명령을 `system service-processor api-service 사용하여 구성 및 인증서를 업데이트할 수 있습니다.

NetApp에서는 보안 원격 액세스를 위해 SSH(보안 셸)를 권장하므로 보안상의 이유로 Telnet 및 RSH(원격 셸)는 기본적으로 비활성화되어 있습니다. 텔넷 또는 RSH에 대한 요구 사항이나 고유한 요구 사항이 있는 경우 이를 활성화해야 합니다.

이 `security protocol modify` 명령은 RSH 및 Telnet의 기존 클러스터 전체 구성을 수정합니다. 활성화된 필드를 로 설정하여 클러스터에서 RSH 및 텔넷을 활성화합니다 `true`.

인증 방법

`authentication method` 매개 변수는 로그인에 사용되는 인증 방법을 지정합니다.

인증 방법	설명
<code>cert</code>	SSL 인증서 인증
<code>community</code>	SNMP 커뮤니티 문자열
<code>domain</code>	Active Directory 인증
<code>nsswitch</code>	LDAP 또는 NIS 인증
<code>password</code>	암호
<code>publickey</code>	공개 키 인증
<code>usm</code>	SNMP 사용자 보안 모델입니다



프로토콜 보안의 약점으로 인해 NIS를 사용하지 않는 것이 좋습니다.

ONTAP 9.3부터는 두 가지 인증 방법으로 로컬 SSH 계정에 대해 연결된 2단계 인증을 사용할 수 `admin publickey` 있습니다. 명령의 필드 외에 `-authentication-method security login`이라는 새 필드가 `-second -authentication-method` 추가되었습니다. 공개 키 또는 암호를 또는 로 지정할 수 `-authentication -method `second-authentication-method`` 있습니다. 그러나 SSH 인증 중에 순서는 부분 인증을 사용하는 공개 키와 전체 인증을 위한 암호 프롬프트가 차례로 표시됩니다.

```
[user@host01 ~]$ ssh ontap.netapp.local
Authenticated with partial success.
Password:
cluster1::>
```

ONTAP 9.4부터 를 `nsswitch` 와 함께 두 번째 인증 방법으로 사용할 수 ``publickey`` 있습니다.

ONTAP 9.12.1부터 FIDO2는 YubiKey 하드웨어 인증 장치 또는 기타 FIDO2 호환 장치를 사용하는 SSH 인증에도 사용할 수 있습니다.

ONTAP 9.13.1부터:

- `domain` 계정은 에서 두 번째 인증 방법으로 사용할 ``publickey`` 수 있습니다.
- 시간 기반 일회용 암호 (totp)는 현재 시간을 두 번째 인증 방법의 인증 요소 중 하나로 사용하는 알고리즘에 의해 생성된 임시 암호입니다.
- 공개 키 취소는 SSH 공개 키와 SSH 중에 만료/해지 여부를 확인하는 인증서를 통해 지원됩니다.

ONTAP System Manager, Active IQ Unified Manager, SSH를 위한 다단계 인증(MFA)에 대한 자세한 내용은 를 참조하십시오. "[TR-4647: ONTAP 9의 다단계 인증](#)"

기본 관리 계정

관리자 역할은 모든 응용 프로그램을 사용하여 액세스할 수 있으므로 관리자 계정을 제한해야 합니다. diag 계정은 시스템 쉘에 액세스할 수 있으며 기술 지원 부서의 문제 해결 작업을 수행하기 위한 목적으로만 예약되어야 합니다.

기본 관리 계정에는 및 의 두 admin `diag`가지가 있습니다.

고립된 계정은 권한 에스컬레이션을 비롯한 취약점을 유발하는 주요 보안 수단입니다. 이러한 계정은 사용자 계정 저장소에 남아 있는 불필요하고 사용되지 않는 계정입니다. 이러한 계정은 기본적으로 사용되지 않았거나 암호가 업데이트 또는 변경되지 않은 기본 계정입니다. 이 문제를 해결하기 위해 ONTAP에서는 계정 제거 및 이름 변경을 지원합니다.



ONTAP에서 기본 제공 계정을 제거하거나 이름을 바꿀 수 없습니다. 그러나 NetApp에서는 lock 명령을 사용하여 필요하지 않은 기본 제공 계정을 잠그는 것이 좋습니다.

분리된 계정은 중요한 보안 문제이지만 NetApp에서는 로컬 계정 리포지토리에서 계정을 제거할 경우의 영향을 테스트하는 것이 좋습니다.

로컬 계정을 나열합니다

로컬 계정을 나열하려면 security login show 명령을 실행합니다.

```
cluster1::*> security login show -vserver cluster1

Vserver: cluster1

          Authentication
User/Group Name  Application Method   Role Name   Acct   Is-Nsswitch
                  Locked   Group
-----
admin            console   password   admin   no     no
admin            http      password   admin   no     no
admin            ontapi    password   admin   no     no
admin            service-processor password admin   no     no
admin            ssh       password   admin   no     no
autosupport      console   password   autosupport no     no
6 entries were displayed.
```

기본 관리자 계정을 제거합니다

`admin`계정은 관리자 역할을 가지며 모든 응용 프로그램을 사용하여 액세스할 수 있습니다.

단계

1. 다른 관리자 수준 계정을 만듭니다.

기본 계정을 완전히 제거하려면 admin 먼저 로그인 응용 프로그램을 사용하는 다른 관리자 수준 계정을 만들어야 console 합니다.



이러한 변경을 수행하면 원하지 않는 결과가 발생할 수 있습니다. 항상 비운영 클러스터에서 솔루션의 보안 상태에 영향을 줄 수 있는 새 설정을 먼저 테스트하십시오.

예:

```
cluster1::*> security login create -user-or-group-name NewAdmin
-application console -authentication-method password -vserver cluster1
```

```
cluster1::*> security login show -vserver cluster1
```

```
Vserver: cluster1
```

		Authentication		Acct	Is-
Nsswitch					
User/Group Name	Application	Method	Role Name	Locked	Group
-----	-----	-----	-----	-----	-----
NewAdmin	console	password	admin	no	no
admin	console	password	admin	no	no
admin	http	password	admin	no	no
admin	ontapi	password	admin	no	no
admin	service-processor	password	admin	no	no
admin	ssh	password	admin	no	no
autosupport	console	password	autosupport	no	no

7 entries were displayed.

2. 새 관리자 계정을 만든 후 계정 로그인으로 해당 계정에 대한 액세스를 NewAdmin 테스트합니다. 로그인을 사용하여 NewAdmin 기본 또는 이전 admin 계정(예: , , 또는)과 동일한 로그인 응용 프로그램을 사용하도록 계정을 http ontapi service-processor `ssh`구성합니다. 이 단계를 통해 액세스 제어가 유지됩니다.

예:

```
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application ssh -authentication-method password
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application http -authentication-method password
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application ontapi -authentication-method password
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application service-processor -authentication-method password
```

3. 모든 기능을 테스트한 후 ONTAP에서 제거하기 전에 모든 응용 프로그램에 대해 admin 계정을 비활성화할 수 있습니다. 이 단계는 이전 관리 계정을 사용하는 반복 기능이 없는지 확인하기 위한 최종 테스트로 사용됩니다.

```
cluster1::*> security login lock -vserver cluster1 -user-or-group-name
admin -application *
```

4. 기본 admin 계정과 이 계정에 대한 모든 항목을 제거하려면 다음 명령을 실행합니다.

```
cluster1::*> security login delete -vserver cluster1 -user-or-group-name
admin -application *
cluster1::*> security login show -vserver cluster1
```

Vserver: cluster1

		Authentication		Acct	Is-
User/Group Name	Application	Method	Role Name	Locked	Group

NewAdmin	console	password	admin	no	no
NewAdmin	http	password	admin	no	no
NewAdmin	ontapi	password	admin	no	no
NewAdmin	service-processor	password	admin	no	no
NewAdmin	ssh	password	admin	no	no
autosupport	console	password	autosupport	no	no

7 entries were displayed.

진단(diag) 계정 암호를 설정합니다

라는 진단 계정이 diag 스토리지 시스템과 함께 제공됩니다. 계정을 사용하여 에서 문제 해결 작업을 수행할 수 diag systemshell` 있습니다. 이 `diag 계정은 권한이 있는 명령을 통해 시스템 셸에 액세스하는 데 사용할 수 있는 유일한 계정입니다. diag systemshell



시스템 셸 및 관련 diag 계정은 저수준 진단 목적으로 사용됩니다. 이러한 액세스 권한은 진단 권한 수준이 필요하며, 기술 지원 부서의 지침에 따라 문제 해결 작업을 수행할 수 있는 경우에만 사용됩니다. 계정과 은 일반 관리 목적으로 사용할 수 diag systemshell 없습니다.

시작하기 전에

에 액세스하기 전에 systemshell` 명령을 사용하여 계정 암호를 설정해야 `diag security login password 합니다. 강력한 암호 원칙을 사용하고 정기적으로 암호를 변경해야 diag 합니다.

단계

1. 계정 사용자 암호 설정 diag :

```

cluster1::> set -privilege diag

Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? \{y|n\}: y

cluster1::*> systemshell -node node-01
      (system node systemshell)
diag@node-01's password:

Warning: The system shell provides access to low-level
diagnostic tools that can cause irreparable damage to
the system if not used properly. Use this environment
only when directed to do so by support personnel.

node-01%

```

다중 관리 검증

ONTAP 9.11.1부터 MAV(다중 관리자 검증)를 사용하여 지정된 관리자의 승인 후에만 볼륨 또는 스냅샷 복사본 삭제 같은 특정 작업이 실행되도록 할 수 있습니다. 따라서 손상되거나 악의적이거나 경험이 부족한 관리자가 원치 않는 변경 또는 데이터 삭제를 방지할 수 있습니다.

MAV 구성은 다음과 같이 구성됩니다.

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

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

MAV가 활성화된 경우 모든 보호된 작업을 완료하려면 다음 세 단계를 수행해야 합니다.

1. 사용자가 작업을 시작하면 가 나타납니다 "요청이 생성되었습니다."
2. 이 명령을 실행하기 전에 필요한 개수 "MAV 관리자가 승인해야 합니다."
3. 승인 후 사용자가 작업을 완료합니다.

MAV는 자동화 작업이 완료되기 전에 승인이 필요하기 때문에 높은 자동화가 필요한 볼륨이나 워크플로에는 사용할 수 없습니다. 자동화와 MAV를 함께 사용하려는 경우 NetApp에서는 특정 MAV 작업에 대해 쿼리를 사용하는 것이 좋습니다. 예를 들어, 자동화가 관련되지 않은 볼륨에만 MAV 규칙을 적용할 수 volume delete 있으며 특정 명령 체계를 사용하여 해당 볼륨을 지정할 수 있습니다.

MAV에 대한 자세한 내용은 ["ONTAP 다중 관리자 인증 문서"](#)참조하십시오.

스냅샷 복사본 잠금

스냅샷 복사본 잠금은 볼륨 스냅샷 정책의 보존 기간 동안 수동으로 또는 자동으로 스냅샷 복사본을 지울 수 없는 SnapLock 기능입니다. 스냅샷 복사본 잠금의 목적은 악성 또는 신뢰할 수 없는 관리자가 1차 또는 2차 ONTAP 시스템에서 스냅샷을 삭제하지 못하도록 방지하는 것입니다.

스냅샷 복사본 잠금은 ONTAP 9.12.1에 도입되었습니다. 스냅샷 복사본 잠금은 무단 조작 방지 스냅샷 잠금이라고도 합니다. SnapLock 라이선스와 규정 준수 클록의 초기화가 필요하지만, 스냅샷 복사본 잠금은 SnapLock Compliance 또는 SnapLock Enterprise와 관련이 없습니다. SnapLock Enterprise에서와 같이 신뢰할 수 있는 스토리지 관리자는 없으며 SnapLock 규정 준수와 같이 기본 물리적 스토리지 인프라를 보호하지 않습니다. 이것은 보조 시스템에 Snapshot 복사본을 SnapVaulting에 비해 향상된 기능입니다. 기본 시스템에서 잠긴 스냅샷을 빠르게 복구하여 랜섬웨어에 의해 손상된 볼륨을 복원할 수 있습니다.

스냅샷 복사본 잠금에 대한 자세한 내용은 [를 참조하십시오 "ONTAP 설명서"](#).

인증서 기반 API 액세스를 설정합니다

REST API 또는 ONTAP에 대한 NetApp Manageability SDK API 액세스에 대한 사용자 ID 및 암호 인증 대신 인증서 기반 인증을 사용해야 합니다.



REST API에 대한 인증서 기반 인증 대신 사용 "[OAuth 2.0 토큰 기반 인증](#)")

이 단계에 설명된 대로 ONTAP에서 자체 서명된 인증서를 생성하고 설치할 수 있습니다.

단계

1. OpenSSL을 사용하여 다음 명령을 실행하여 인증서를 생성합니다.

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout test.key
-out test.pem \> -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=cert_user"
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'test.key'
```

이 명령은 라는 공용 인증서와 test.pem 라는 개인 키를 `key.out` 생성합니다. 일반 이름인 CN은 ONTAP 사용자 ID에 해당합니다.

2. 다음 명령을 실행하고 메시지가 표시되면 인증서의 내용을 붙여 넣어 ONTAP의 PEM(Privacy Enhanced mail) 형식으로 공용 인증서 내용을 설치합니다.

```
security certificate install -type client-ca -vserver cluster1

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

3. ONTAP를 활성화하여 SSL을 통한 클라이언트 액세스를 허용하고 API 액세스에 대한 사용자 ID를 정의합니다.

```
security ssl modify -vserver cluster1 -client-enabled true
security login create -user-or-group-name cert_user -application ontapi
-authmethod cert -role admin -vserver cluster1
```

다음 예에서는 사용자 ID가 `cert_user` 인증서 인증 API 액세스를 사용할 수 있게 되었습니다. ONTAP 버전을 표시하기 위해 사용하는 간단한 관리 SDK Python 스크립트는 `cert_user` 다음과 같습니다.

```
#!/usr/bin/python

import sys
sys.path.append("/home/admin/netapp-manageability-sdk-9.5/netapp-
manageability-sdk-9.5/lib/python/NetApp")
from NaServer import *

cluster = "cluster1"
transport = "HTTPS"
port = 443
style = "CERTIFICATE"
cert = "test.pem"
key = "test.key"

s = NaServer(cluster, 1, 30)
s.set_transport_type(transport)
s.set_port(port)
s.set_style(style)
s.set_server_cert_verification(0)
s.set_client_cert_and_key(cert, key)

api = NaElement("system-get-version")
output = s.invoke_elem(api)
if (output.results_status() == "failed"):
    r = output.results_reason()
    print("Failed: " + str(r))
    sys.exit(2)

ontap_version = output.child_get_string("version")
print ("V: " + ontap_version)
```

스크립트의 출력에 ONTAP 버전이 표시됩니다.

```
./version.py

V: NetApp Release 9.5RC1: Sat Nov 10 05:13:42 UTC 2018
```

4. ONTAP REST API를 사용하여 인증서 기반 인증을 수행하려면 다음 단계를 완료하십시오.

a. ONTAP에서 http 액세스에 대한 사용자 ID를 정의합니다.

```
security login create -user-or-group-name cert_user -application http
-authmethod cert -role admin -vserver cluster1
```

b. Linux 클라이언트에서 다음 명령을 실행하여 ONTAP 버전을 출력으로 생성합니다.

```
curl -k --cert-type PEM --cert ./test.pem --key-type PEM --key
./test.key -X GET "https://cluster1/api/cluster?fields=version"
{
  "version": {
    "full": "NetApp Release 9.7P1: Thu Feb 27 01:25:24 UTC 2020",
    "generation": 9,
    "major": 7,
    "minor": 0
  },
  "_links": {
    "self": {
      "href": "/api/cluster"
    }
  }
}
```

추가 정보

- ["ONTAP용 NetApp 관리 SDK를 사용한 인증서 기반 인증"..](#)

REST API에 대한 ONTAP OAuth 2.0 토큰 기반 인증

인증서 기반 인증 대신 REST API에 OAuth 2.0 토큰 기반 인증을 사용할 수 있습니다.

ONTAP 9.14.1부터 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 토큰은 사용자 계정 인증을 위한 암호를 대체합니다.

OAuth 2.0 사용에 대한 자세한 내용은 ["OAuth 2.0을 사용한 인증 및 권한 부여에 대한 ONTAP 문서"](#) 참조하십시오.

로그인 및 암호 매개 변수

효과적인 보안 체계는 확립된 조직 정책, 지침 및 조직에 적용되는 모든 거버넌스 또는 표준을 준수합니다. 이러한 요구 사항의 예로는 사용자 이름 수명, 암호 길이 요구 사항, 문자 요구 사항

및 이러한 계정의 저장 등이 있습니다. ONTAP 솔루션은 이러한 보안 구조를 처리하는 기능을 제공합니다.

새로운 로컬 계정 기능

거버넌스를 포함하여 조직의 사용자 계정 정책, 지침 또는 표준을 지원하기 위해 ONTAP에서 지원되는 기능은 다음과 같습니다.

- 최소 숫자, 소문자 또는 대문자를 사용하도록 암호 정책 구성
- 로그인 시도 실패 후 지연이 필요합니다
- 계정 비활성 한도 정의
- 사용자 계정 만료
- 암호 만료 경고 메시지 표시
- 잘못된 로그인에 대한 알림입니다



구성 가능한 설정은 보안 로그인 역할 config modify 명령을 사용하여 관리합니다.

SHA-512 지원

암호 보안을 강화하기 위해 ONTAP 9에서는 SHA-2 암호 해시 기능을 지원하며, 새로 생성되거나 변경된 암호를 해시하는 데 기본적으로 SHA-512를 사용합니다. 운영자와 관리자는 필요에 따라 계정을 만료하거나 잠글 수도 있습니다.

암호가 변경되지 않은 기존 ONTAP 9 사용자 계정은 ONTAP 9.0 이상으로 업그레이드한 후에도 MD5 해시 기능을 계속 사용합니다. 그러나 NetApp에서는 사용자가 암호를 변경하도록 하여 이러한 사용자 계정을 보다 안전한 SHA-512 솔루션으로 마이그레이션할 것을 적극 권장합니다.

암호 해시 기능을 사용하면 다음 작업을 수행할 수 있습니다.

- 지정된 해시 함수와 일치하는 사용자 계정 표시:

```
cluster1::*> security login show -user-or-group-name NewAdmin -fields
hash-function
vserver user-or-group-name application authentication-method hash-
function
-----
-----
cluster1 NewAdmin console password sha512
cluster1 NewAdmin ontapi password sha512
cluster1 NewAdmin ssh password sha512
```

- 지정된 해시 함수(예: MD5)를 사용하는 계정을 만료시켜 사용자가 다음 로그인 시 암호를 변경해야 합니다.


```
cluster1::*> security login expire-password -vserver * -username * -hash
-function md5
```

- 지정된 해시 함수를 사용하는 암호로 계정을 잠급니다.

```
cluster1::*> security login lock -vserver * -username * -hash-function
md5
```

클러스터의 관리 SVM에서 내부 사용자가 암호 해시 기능을 알 수 없습니다 `autosupport`. 이 문제는 외관상 문제입니다. 이 내부 사용자에게는 기본적으로 구성된 암호가 없으므로 해시 기능을 알 수 없습니다.

- 사용자의 암호 해시 기능을 보려면 `autosupport` 다음 명령을 실행합니다.

```
::> set advanced
::> security login show -user-or-group-name autosupport -instance

                Vserver: cluster1
User Name or Group Name: autosupport
        Application: console
        Authentication Method: password
Remote Switch IP Address: -
                Role Name: autosupport
        Account Locked: no
                Comment Text: -
        Whether Ns-switch Group: no
        Password Hash Function: unknown
Second Authentication Method2: none
```

- 암호 해시 기능(기본값: SHA512)을 설정하려면 다음 명령을 실행합니다.

```
::> security login password -username autosupport
```

암호가 무엇으로 설정되어 있는지는 중요하지 않습니다.

```
security login show -user-or-group-name autosupport -instance
```

```

Vserver: cluster1
User Name or Group Name: autosupport
Application: console
Authentication Method: password
Remote Switch IP Address: -
Role Name: autosupport
Account Locked: no
Comment Text: -
Whether Ns-switch Group: no
Password Hash Function: sha512
Second Authentication Method2: none

```

암호 매개 변수

ONTAP 솔루션은 조직 정책 요구 사항 및 지침을 다루고 지원하는 암호 매개 변수를 지원합니다.

속성	설명	기본값	범위
username-minlength	최소 사용자 이름 길이가 필요합니다	3	3-16 을 참조하십시오
username-alphanum	사용자 이름 영숫자	사용 안 함	활성화/비활성화
passwd-minlength	최소 암호 길이가 필요합니다	8	3-64 을 참조하십시오
passwd-alphanum	암호 영숫자	활성화됨	활성화/비활성화
passwd-min-special-chars	암호에 필요한 최소 특수 문자 수입니다	0	0-64 을 참조하십시오
passwd-expiry-time	암호 만료 시간(일)	무제한 - 암호가 만료되지 않습니다	0 - 무제한 0 = 지금 만료
require-initial-passwd-update	첫 번째 로그인 시 초기 암호 업데이트가 필요합니다	사용 안 함	활성화/비활성화 콘솔 또는 SSH를 통해 변경이 허용됩니다
max-failed-login-attempts	최대 시도 실패 횟수입니다	0, 계정을 잠그지 마십시오	-
lockout-duration	최대 잠금 기간(일)	기본값은 0입니다. 즉, 계정이 하루 동안 잠겨 있습니다	-
disallowed-reuse	마지막 N 암호를 허용하지 않습니다	6	최소값은 6입니다

속성	설명	기본값	범위
change-delay	암호 변경 간격(일)	0	-
delay-after-failed-login	로그인 시도 실패 후 지연(초)	4	-
passwd-min-lowercase-chars	암호에 필요한 최소 소문자 알파벳 문자 수입니다	0으로, 소문자가 필요하지 않습니다	0-64 을 참조하십시오
passwd-min-uppercase-chars	알파벳 대문자 최소 개수여야 합니다	0 - 대문자가 필요하지 않습니다	0-64 을 참조하십시오
passwd-min-digits	암호에 필요한 최소 자릿수입니다	0으로, 숫자가 필요하지 않습니다	0-64 을 참조하십시오
passwd-expiry-warn-time	암호 만료 전에 경고 메시지 표시(일)	Unlimited(무제한) - 암호 만료에 대해 경고하지 않습니다	0: 로그인할 때마다 암호 만료에 대해 사용자에게 경고합니다
account-expiry-time	계정이 N일 후에 만료됩니다	무제한. 즉, 계정이 만료되지 않습니다	계정 만료 시간은 계정 비활성 제한보다 커야 합니다
account-inactive-limit	계정 만료 전 최대 비활성 기간(일)	무제한 - 비활성 계정은 만료되지 않습니다	계정 비활성 한도는 계정 만료 시간보다 작아야 합니다

```

cluster1::*> security login role config show -vserver cluster1 -role admin

                                Vserver: cluster1
                                Role Name: admin
                                Minimum Username Length Required: 3
                                Username Alpha-Numeric: disabled
                                Minimum Password Length Required: 8
                                Password Alpha-Numeric: enabled
Minimum Number of Special Characters Required in the Password: 0
                                Password Expires In (Days): unlimited
                                Require Initial Password Update on First Login: disabled
                                Maximum Number of Failed Attempts: 0
                                Maximum Lockout Period (Days): 0
                                Disallow Last 'N' Passwords: 6
                                Delay Between Password Changes (Days): 0
                                Delay after Each Failed Login Attempt (Secs): 4
Minimum Number of Lowercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Uppercase Alphabetic Characters Required in the
Password: 0
Minimum Number of Digits Required in the Password: 0
Display Warning Message Days Prior to Password Expiry (Days): unlimited
                                Account Expires in (Days): unlimited
Maximum Duration of Inactivity before Account Expiration (Days): unlimited

```



9.14.1부터는 암호에 대한 복잡성과 잠금 규칙이 증가합니다. 이는 ONTAP의 신규 설치에만 적용됩니다.

시스템 관리 방법

이는 ONTAP 시스템 관리를 강화하는 중요한 매개 변수입니다.

명령줄 액세스

보안 솔루션을 유지 관리하려면 시스템에 대한 보안 액세스를 설정하는 것이 중요합니다. 가장 일반적인 명령줄 액세스 옵션은 SSH, Telnet 및 RSH입니다. 이 중에서 SSH는 원격 명령줄 액세스를 위한 가장 안전한 업계 표준 모범 사례입니다. NetApp에서는 ONTAP 솔루션에 대한 명령줄 액세스를 위해 SSH를 사용할 것을 적극 권장합니다.

SSH 구성

`security ssh show` 명령은 클러스터 및 SVM에 대한 SSH 키 교환 알고리즘, 암호, MAC 알고리즘의 구성을 보여줍니다. 키 교환 방법은 이러한 알고리즘과 암호를 사용하여 암호화 및 인증을 위해 1회성 세션 키가 생성되는 방법과 서버 인증이 수행되는 방법을 지정합니다.

```
cluster1::> security ssh show
```

Vserver	Ciphers	Key Exchange Algorithms	MAC Algorithms
nsadhanacluster-2	aes256-ctr, aes192-ctr, aes128-ctr	diffie-helman-group- exchange-sha256, ecdh-sha2-nistp384	hmac-sha2-256 hmac-sha2-512
vs0	aes128-gcm	curve25519-sha256	hmac-sha1
vs1	aes256-ctr, aes192-ctr, aes128-ctr, 3des-cbc, aes128-gcm	diffie-hellman-group- exchange-sha256 ecdh-sha2-nistp384 ecdh-sha2-nistp512	hmac-sha1-96 hmac-sha2-256 hmac-sha2-256- etm hmac-sha2-512

3 entries were displayed.

로그인 배너

조직은 로그인 배너를 사용하여 모든 운영자, 관리자, 범법자를 막론하고 모두에게 사용 약관을 제공하고 시스템에 액세스 할 수 있는 사람을 표시 할 수 있습니다. 이 접근 방식은 시스템 액세스 및 사용에 대한 기대치를 설정하는 데 유용합니다. `security login banner modify` 이 명령은 로그인 배너를 수정합니다. 로그인 배너는 SSH 및 콘솔 장치 로그인 프로세스 중 인증 단계 바로 앞에 표시됩니다. 다음 예에 표시된 대로 배너 텍스트는 큰 따옴표(" ")로 묶어야 합니다.

```
cluster1::> security login banner modify -vserver cluster1 -message
"Authorized users ONLY!"
```

로그인 배너 매개 변수

매개 변수	설명
vserver	이 매개 변수를 사용하여 수정된 배너가 있는 SVM을 지정합니다. 클러스터 관리자 SVM의 이름을 사용하여 클러스터 레벨 메시지를 수정하십시오. 클러스터 레벨 메시지는 메시지가 정의되지 않은 데이터 SVM에 대한 기본값으로 사용됩니다.

매개 변수	설명
message	<p>이 선택적 매개 변수는 로그인 배너 메시지를 지정하는 데 사용할 수 있습니다. 클러스터에 로그인 배너 메시지가 설정된 경우 클러스터 로그인 배너는 모든 데이터 SVM에서 사용됩니다. 데이터 SVM의 로그인 배너를 설정하면 클러스터 로그인 배너의 디스플레이가 재정의됩니다. 데이터 SVM 로그인 배너를 사용하여 클러스터 로그인 배너를 재설정하려면 이 매개 변수를 "-" 값과 함께 사용하십시오.</p> <p>이 매개 변수를 사용하는 경우 로그인 배너에 줄 바꿈(줄 끝 [EOL] 또는 줄 바꿈)을 포함할 수 없습니다. 새 줄이 있는 로그인 배너 메시지를 입력하려면 매개 변수를 지정하지 마십시오. 메시지를 대화형으로 입력하라는 메시지가 표시됩니다. 대화형으로 입력된 메시지에는 줄 바꿈을 포함할 수 있습니다.</p> <p>ASCII가 아닌 문자는 유니코드 UTF-8을 사용해야 합니다.</p>
uri	<p>`(ftp`</p>
http://(hostname	<p>IPv4`</p> <p>이 매개 변수를 사용하여 로그인 배너를 다운로드할 URI를 지정합니다.</p> <p>메시지의 길이는 2048바이트를 초과할 수 없습니다. 비 ASCII 문자는 유니코드 UTF-8로 제공되어야 합니다.</p>

오늘의 메시지

이 `security login motd modify` 명령은 MOTD(오늘의 메시지)를 업데이트합니다.

MOTD에는 클러스터 레벨 MOTD와 데이터 SVM 레벨 MOTD라는 두 가지 범주가 있습니다. 데이터 SVM의 클러스터 셸에 로그인하는 사용자는 클러스터 레벨 MOTD 다음에 해당 SVM에 대한 SVM 레벨 MOTD라는 두 가지 메시지를 볼 수 있습니다.

클러스터 관리자는 필요한 경우 각 SVM에서 개별적으로 클러스터 수준 MOTD를 사용하거나 사용하지 않도록 설정할 수 있습니다. 클러스터 관리자가 SVM에 대해 클러스터 레벨 MOTD를 사용하지 않도록 설정하면 SVM에 로그인한 사용자에게 클러스터 레벨 메시지가 표시되지 않습니다. 클러스터 관리자만 클러스터 레벨 메시지를 설정 또는 해제할 수 있습니다.

MOTD 매개 변수입니다	설명
SVM	이 매개변수를 사용하여 MOTD가 수정되는 SVM을 지정합니다. 클러스터 관리자 SVM의 이름을 사용하여 클러스터 레벨 메시지를 수정하십시오.

MOTD 매개 변수입니다	설명
메시지	<p>이 선택적 매개 변수는 메시지를 지정하는 데 사용할 수 있습니다. 이 매개변수를 사용하면 MOTD에 줄 바꿈을 포함할 수 없습니다. 매개 변수 이외의 매개 변수를 지정하지 <code>-vserver</code> 않으면 메시지를 대화형으로 입력하라는 메시지가 표시됩니다. 대화형으로 입력된 메시지에는 줄 바꿈을 포함할 수 있습니다. 비 ASCII 문자는 유니코드 UTF-8로 제공되어야 합니다. 메시지에는 다음과 같은 이스케이프 시퀀스를 사용하여 동적으로 생성된 콘텐츠가 포함될 수 있습니다.</p> <ul style="list-style-type: none"> • <code>\l</code> - 단일 백래시 문자 • <code>\b</code> - 출력 없음(Linux와의 호환성을 위해서만 지원됨) • <code>\C</code> - 클러스터 이름입니다 • <code>\d</code> - 로그인 노드에 설정된 현재 날짜입니다 • <code>\t</code> - 로그인 노드에 설정된 현재 시간입니다 • <code>\I</code> - 수신 LIF IP 주소(로그인용 콘솔 인쇄 <code>console</code>) • <code>\l</code> - 로그인 장치 이름(로그인을 위해 콘솔을 인쇄함 <code>console</code>) • <code>\L</code> - 클러스터의 모든 노드에서 사용자에게 대한 마지막 로그인입니다 • <code>\m</code> - 기계 아키텍처 • <code>\n</code> - 노드 또는 데이터 SVM 이름 • <code>\N</code> - 로그인한 사용자의 이름입니다 • <code>\o</code> - <code>\O</code>와 동일합니다 Linux 호환성을 위해 제공됩니다. • <code>\O</code> - 노드의 DNS 도메인 이름입니다. 출력은 네트워크 구성에 따라 달라지며 비어 있을 수 있습니다. • <code>\r</code> - 소프트웨어 릴리스 번호 • <code>\s</code> - 운영 체제 이름입니다 • <code>\u</code> - 로컬 노드의 활성 클러스터 셸 세션 수입니다. 클러스터 관리자의 경우: 모든 클러스터 셸 사용자. 데이터 SVM 관리자의 경우: 해당 데이터 SVM에 대한 액티브 세션만 지원됩니다. • <code>\U</code> - 와 같지만 <code>\u`</code> 또는 가 <code>`user users</code> 추가됩니다 • <code>\v</code> - 효과적인 클러스터 버전 문자열 • <code>\W</code> - 사용자가 로그인할 수 있도록 클러스터 전체에서 활성 세션 (<code>`who`</code> 사용)

ONTAP에서 오늘의 메시지를 구성하는 방법에 대한 자세한 내용은 ["오늘의 메시지에 대한 ONTAP 문서"](#).

CLI 세션 시간 초과

기본 CLI 세션 시간 초과는 30분입니다. 시간 초과는 부실 세션 및 세션 피기백킹을 방지하는 데 중요합니다.

명령을 사용하여 `system timeout show` 현재 CLI 세션 시간 초과를 봅니다. 시간 초과 값을 설정하려면 `system timeout modify -timeout <minutes>` 명령을 사용합니다.

NetApp ONTAP System Manager를 통한 웹 액세스

ONTAP 관리자가 클러스터를 액세스하고 관리하는 데 CLI 대신 그래픽 인터페이스를 사용하려는 경우 NetApp ONTAP System Manager를 사용하십시오. 기본적으로 활성화되며 브라우저를 통해 액세스할 수 있는 웹 서비스로 ONTAP에 포함되어 있습니다. DNS를 사용하는 경우 브라우저에서 호스트 이름을 가리키거나 를 통해 IPv4 또는 IPv6 주소를 `https://cluster-management-LIF` 지정합니다.

클러스터에서 자체 서명된 디지털 인증서를 사용하는 경우 브라우저에서 인증서를 신뢰할 수 없음을 나타내는 경고를 표시할 수 있습니다. 액세스를 계속할 위험을 인식하거나 서버 인증을 위해 클러스터에 CA(인증 기관) 서명 디지털 인증서를 설치할 수 있습니다.

ONTAP 9.3부터 SAML(Security Assertion Markup Language) 인증은 ONTAP System Manager의 옵션입니다.

ONTAP System Manager에 대한 SAML 인증

SAML 2.0은 타사 SAML 호환 ID 공급자(IDP)가 기업에서 선택한 IDP에 고유한 메커니즘을 사용하고 SSO(Single Sign-On)의 소스로 MFA를 수행할 수 있도록 하는 널리 채택된 업계 표준입니다.

SAML 사양에는 Principal, IDP 및 Service Provider의 세 가지 역할이 정의되어 있습니다. ONTAP 구현에서 주체는 클러스터 관리자가 ONTAP System Manager 또는 NetApp Active IQ Unified Manager를 통해 ONTAP에 액세스할 수 있도록 하는 것입니다. IDP는 타사 IDP 소프트웨어입니다. ONTAP 9.3부터 Microsoft ADFS(Active Directory Federated Services)와 오픈 소스 Shibboleth IDP가 지원됩니다. ONTAP 9.12.1부터 Cisco Duo는 IDP를 지원합니다. 서비스 공급자는 ONTAP에 내장된 SAML 기능으로, ONTAP System Manager 또는 Active IQ Unified Manager 웹 애플리케이션에서 사용됩니다.

SSH 2단계 구성 프로세스와 달리, SAML 인증이 활성화된 후 ONTAP System Manager 또는 ONTAP 서비스 프로세서 액세스에 모든 기존 관리자는 SAML IDP를 통해 인증해야 합니다. 클러스터 사용자 계정을 변경할 필요가 없습니다. SAML 인증이 활성화되면 및 응용 프로그램에 대한 관리자 역할이 있는 기존 사용자에게 의 새로운 인증 방법이 `saml http ontapi` 추가됩니다.

SAML 인증을 사용하도록 설정한 후 SAML IDP 액세스가 필요한 추가 새 계정을 ONTAP에서 관리자 역할 및 및 및 응용 프로그램에 대한 SAML 인증 방법으로 `http ontapi` 정의해야 합니다. 특정 시점에 SAML 인증이 비활성화된 경우 이러한 새 계정은 및 응용 프로그램에 대한 관리자 역할을 정의하고 로컬 ONTAP 인증을 위한 콘솔 응용 프로그램을 ONTAP 시스템 관리자에 추가해야 `password http ontapi` 합니다.

SAML IDP를 사용하도록 설정하면 IDP는 LDAP(Lightweight Directory Access Protocol), AD(Active Directory), Kerberos, 암호 등과 같이 IDP에 사용 가능한 방법을 사용하여 ONTAP 시스템 관리자 액세스에 대한 인증을 수행합니다. 사용 가능한 방법은 IDP에 고유합니다. ONTAP에 구성된 계정에는 IDP 인증 방법에 매핑되는 사용자 ID가 있어야 합니다.

NetApp에서 검증한 IDP는 Microsoft ADFS, Cisco Duo 및 오픈 소스 Shibboleth IDP입니다.

ONTAP 9.14.1부터 Cisco Duo를 SSH의 두 번째 인증 요소로 사용할 수 있습니다.

ONTAP System Manager, Active IQ Unified Manager 및 SSH를 위한 MFA에 대한 자세한 내용은 를 참조하십시오. "[TR-4647: ONTAP 9의 다단계 인증](#)"

ONTAP System Manager의 통찰력

ONTAP 9.11.1부터 ONTAP System Manager는 클러스터 관리자가 일상 작업을 간소화하는 데 도움이 되는 통찰력을 제공합니다. 보안 정보는 이 기술 보고서의 권장 사항을 기반으로 합니다.

보안 통찰력	결정
텔넷이 활성화되었습니다	보안 원격 액세스를 위해 SSH(Secure Shell)를 사용하는 것이 좋습니다.
원격 셸(RSH)이 활성화되었습니다	NetApp에서는 보안 원격 액세스에 SSH를 권장합니다.
AutoSupport가 안전하지 않은 프로토콜을 사용하고 있습니다	AutoSupport가 HTTPS 링크를 통해 전송되도록 구성되지 않았습니다.
로그인 배너가 클러스터 레벨의 클러스터에 구성되어 있지 않습니다	로그인 배너가 클러스터에 대해 구성되지 않은 경우 경고.
SSH가 안전하지 않은 암호를 사용하고 있습니다	SSH에서 안전하지 않은 암호를 사용하는 경우 경고
구성된 NTP 서버가 너무 적습니다	구성된 NTP 서버 수가 3개 미만인 경우 경고
기본 관리자 사용자가 잠기지 않았습니다	기본 관리 계정(admin 또는 diag)을 사용하여 System Manager에 로그인하지 않고 이러한 계정이 잠겨 있지 않은 경우 계정을 잠그는 것이 좋습니다.
랜섬웨어 방어 - 볼륨에 스냅샷 정책이 없습니다	하나 이상의 볼륨에 적절한 스냅샷 정책이 연결되어 있지 않습니다.
랜섬웨어 방어 - 스냅샷 자동 삭제를 사용하지 않습니다	스냅샷 자동 삭제는 하나 이상의 볼륨에 대해 설정되어 있습니다.
랜섬웨어 공격을 위해 볼륨을 모니터링하지 않고 있습니다	여러 볼륨에서 자율적 랜섬웨어 보호가 지원되지만 아직 구성되지 않았습니다.
SVM은 자율적 랜섬웨어 보호용으로 구성되지 않습니다	여러 SVM에서 자율적 랜섬웨어 보호가 지원되지만 아직 구성되지 않았습니다.
기본 FPolicy가 구성되지 않았습니다	NAS SVM에 FPolicy가 설정되지 않았습니다.
자율적 랜섬웨어 방어 활성화 모드를 활성화합니다	여러 볼륨이 학습 모드를 완료했으며 활성 모드를 켤 수 있습니다
글로벌 FIPS 140-2 규정 준수가 비활성화되었습니다	글로벌 FIPS 140-2 규정 준수는 사용되지 않습니다.
클러스터가 알림에 대해 구성되지 않았습니다	이메일, Webhook 또는 SNMP traps가 알림을 수신하도록 구성되지 않았습니다.

ONTAP System Manager 인사이트에 대한 자세한 내용은 ["ONTAP System Manager 인사이트 설명서"](#) 참조하십시오.

ONTAP 자율 랜섬웨어 방어

스토리지 워크로드 보안에 대한 사용자 행동 분석을 보완하기 위해 ONTAP 자율적 랜섬웨어 방어는 볼륨 워크로드와 엔트로피를 분석하여 랜섬웨어를 탐지하고 스냅샷을 생성하여 공격이 의심되면 관리자에게 알립니다.

NetApp Cloud Insights/Cloud Secure 및 NetApp FPolicy 파트너 에코시스템과 함께 외부 FPolicy 사용자 행동 분석(UBA)을 사용한 랜섬웨어 감지 및 예방과 더불어 ONTAP 9.10.1에는 자율적인 랜섬웨어 방어 기능이 도입되었습니다. ONTAP 자율적 랜섬웨어 방어는 볼륨 워크로드 활동과 데이터 엔트로피를 확인하여 랜섬웨어를 자동으로 탐지하는 내장 머신 러닝(ML) 기능을 사용합니다. UBA와 다른 활동을 모니터링하여 UBA에 없는 공격을 감지할 수 있습니다.

이 기능에 대한 자세한 내용은 [또는](#) 을 참조하십시오 ["TR-4572: 랜섬웨어용 NetApp 솔루션"](#) ["ONTAP 자율적 랜섬웨어"](#)

스토리지 관리 시스템 감사

ONTAP 이벤트를 원격 syslog 서버로 오프로드하여 이벤트 감사의 무결성을 보장합니다. 이 서버는 Splunk와 같은 보안 정보 이벤트 관리 시스템이 될 수 있습니다.

syslog를 보냅니다

로그 및 감사 정보는 지원 및 가용성의 관점에서 조직에 매우 중요합니다. 또한 로그(syslog) 및 감사 보고서/출력에 포함된 정보와 세부 정보는 일반적으로 민감한 특성입니다. 보안 제어 및 상태를 유지하려면 조직에서 로그 및 감사 데이터를 안전하게 관리해야 합니다.

syslog 정보의 오프로드는 침입의 범위 또는 설치 공간을 단일 시스템 또는 솔루션으로 제한하는 데 필요합니다. 따라서 syslog 정보를 안전한 스토리지 또는 보존 위치로 안전하게 오프로딩하는 것이 좋습니다.

로그 전달 대상을 생성합니다

명령을 사용하여 cluster log-forwarding create 원격 로깅을 위한 로그 전달 대상을 생성할 수 있습니다.

매개 변수

다음 매개 변수를 사용하여 cluster log-forwarding create 명령을 구성합니다.

- * 대상 호스트. * 이 이름은 로그를 전달할 서버의 호스트 이름 또는 IPv4 또는 IPv6 주소입니다.

```
-destination <Remote InetAddress>
```

- * 대상 포트. * 대상 서버가 수신 대기하는 포트입니다.

```
[-port <integer>]
```

- * 로그 전달 프로토콜. * 이 프로토콜은 메시지를 대상으로 보내는 데 사용됩니다.

```
[-protocol \{udp-unencrypted|tcp-unencrypted|tcp-encrypted}&#92;]
```

로그 전달 프로토콜은 다음 값 중 하나를 사용할 수 있습니다.

- udp-unencrypted.. 보안이 없는 사용자 데이터그램 프로토콜.
- tcp-unencrypted.. 보안 기능이 없는 TCP.
- tcp-encrypted.. TLS(Transport Layer Security)를 사용하는 TCP.
- * 대상 서버 ID를 확인하십시오. * 이 매개 변수를 true로 설정하면 해당 인증서의 유효성을 확인하여 로그 전달 대상의 ID를 확인합니다. 프로토콜 필드에서 값을 선택한 경우에만 이 값을 TRUE로 설정할 수 tcpencrypted 있습니다.

```
[-verify-server \{true|false\}]
```

- * Syslog 기능. * 이 값은 전달된 로그에 사용할 syslog 기능입니다.

```
[-facility <Syslog Facility>]
```

- * 연결 테스트를 건너뛰니다. * 일반적으로 이 `cluster log-forwarding create` 명령은 ICMP(Internet Control Message Protocol) ping을 보내 대상에 연결할 수 있는지 확인하고 도달할 수 없는 경우 실패합니다. 이 값을 설정하면 true Ping 검사를 무시하여 대상에 도달할 수 없을 때 구성할 수 있습니다.

```
[-force [true]]
```



NetApp에서는 명령을 사용하여 유형에 강제로 연결하는 것이 `cluster log-forwarding -tcp -encrypted` 좋습니다.

이벤트 알림

시스템에서 나가는 정보와 데이터의 보호는 시스템의 보안 상태를 유지하고 관리하는 데 있어 매우 중요합니다. ONTAP 솔루션에 의해 생성되는 이벤트는 솔루션이 마주치는 내용, 처리되는 정보 등에 대한 풍부한 정보를 제공합니다. 데이터가 활발하게 사용됨에 따라 데이터를 안전하게 관리하고 마이그레이션해야 할 필요성이 대두되었습니다.

이 `event notification create` 명령은 이벤트 필터로 정의된 일련의 이벤트에 대한 새 알림을 하나 이상의 알림 대상으로 보냅니다. 다음 예에서는 구성된 이벤트 알림 필터 및 대상을 표시하는 이벤트 알림 구성 및 `event notification show` 명령을 보여 줍니다.

```
cluster1::> event notification create -filter-name filter1 -destinations
email_dest,syslog_dest,snmp-traphost
```

```
cluster1::> event notification show
```

```
ID      Filter Name      Destinations
-----
1 filter1 email_dest, syslog_dest, snmp-traphost
```

스토리지 암호화

디스크 도난, 반환 또는 용도 변경 시 기밀 데이터를 보호하려면 하드웨어 기반 NetApp 스토리지 암호화나 소프트웨어 기반 NetApp 볼륨 암호화/NetApp 애그리게이트 암호화를 사용하십시오. 두 메커니즘 모두 FIPS-140-2 인증을 거쳤으며 소프트웨어 기반 메커니즘과 함께 하드웨어 기반 메커니즘을 사용할 경우 CSfC(Commercial Solutions for Classified) 프로그램에 적합합니다. 하드웨어 및 소프트웨어 계층 모두에서 저장된 비밀 데이터와 주요 기밀 데이터에 대한 보안 보호 기능이 강화됩니다.

유휴 데이터 암호화는 디스크 도난, 반환 또는 용도 변경이 발생할 경우 중요한 데이터를 보호하는 데 중요합니다.

ONTAP 9에는 세 가지 FIPS(Federal Information Processing Standard) 140-2를 준수하는 유휴 데이터 암호화 솔루션이 있습니다.

- NetApp Storage Encryption(NSE)은 자체 암호화 드라이브를 사용하는 하드웨어 솔루션입니다.
- NetApp Volume Encryption(NVE)은 각 볼륨의 고유 키를 사용하여 모든 드라이브 유형의 모든 데이터 볼륨을 암호화할 수 있는 소프트웨어 솔루션입니다.
- NetApp Aggregate Encryption(NAE)은 각 애그리게이트의 고유 키를 사용하여 활성화된 모든 드라이브 유형의 모든 데이터 볼륨을 암호화할 수 있는 소프트웨어 솔루션입니다.

NSE, NVE, NAE는 외부 키 관리 또는 온보드 키 관리자(OKM)를 사용할 수 있습니다. NSE, NVE, NAE를 사용할 경우 ONTAP 스토리지 효율성 기능에 영향을 미치지 않습니다. 하지만, NVE 볼륨은 애그리게이트 중복제거에서 제외됩니다. NAE 볼륨은 애그리게이트 중복제거가 사용되며 이를 통해 더 많은 이점을 누리고 있습니다.

OKM은 NSE, NVE, NAE와 함께 유휴 데이터를 위한 모든 구성요소가 완비된 암호화 솔루션을 제공합니다.

NVE, NAE 및 OKM은 ONTAP CryptoMod를 사용합니다. CryptoMod는 CMVP FIPS 140-2 검증 모듈 목록에 나열되어 있습니다. 을 "[FIPS 140-2 인증 #4144](#)"참조하십시오.

OKM 구성을 시작하려면 `security key-manager onboard enable` 명령을 사용합니다. 외부 키 관리 상호 운용성 프로토콜(KMIP) 키 관리자를 구성하려면 `security key-manager external enable` 명령을 사용하십시오. ONTAP 9.6부터 멀티 테넌시가 외부 키 관리자를 위해 지원됩니다. 매개 변수를 사용하여 `-vserver <vserver name>` 특정 SVM에 대한 외부 키 관리를 활성화합니다. 9.6 이전 버전에서는 `security key-manager setup` OKM과 외부 키 관리자를 모두 구성하기 위해 명령을 사용했습니다. 온보드 키 관리를 위해 이 구성은 운영자 또는 관리자에게 OKM 구성을 위한 암호 설정과 추가 매개 변수를 안내합니다.

구성의 일부가 다음 예에 나와 있습니다.

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.
```

Enter the following commands at any time
"help" or "?" if you want to have a question clarified,
"back" if you want to change your answers to previous questions, and
"exit" if you want to quit the key manager setup wizard. Any changes
you made before typing "exit" will be applied.

Restart the key manager setup wizard with "security key-manager setup". To
accept a default
or omit a question, do not enter a value.

Would you like to configure onboard key management? {yes, no} [yes]:
Enter the cluster-wide passphrase for onboard key management. To continue
the configuration, enter the passphrase, otherwise
type "exit":
Re-enter the cluster-wide passphrase:
After configuring onboard key management, save the encrypted configuration
data
in a safe location so that you can use it if you need to perform a manual
recovery
operation. To view the data, use the "security key-manager backup show"
command.

ONTAP 9.4부터는 `yes` 옵션을 사용하여 재부팅 후 사용자가 암호를 입력하도록 요구할 수 `-enable-cc-mode security key-manager setup` 있습니다. ONTAP 9.6 이상에서 명령 구문은 `security key-manager onboard enable -cc-mode-enabled yes`.

ONTAP 9.4부터 고급 권한의 기능을 사용하여 NVE 지원 볼륨에서 데이터를 중단 없이 "스크럽" 데이터를 사용할 수 `secure-purge` 있습니다. 암호화된 볼륨의 데이터를 스크리빙하면 물리적 미디어에서 데이터를 복구할 수 없습니다. 다음 명령을 실행하면 SVM VS1의 vol1에서 삭제된 파일이 안전하게 제거됩니다.

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume vol1
```

ONTAP 9.7부터 VE 라이선스가 설정되어 있고 OKM 또는 외부 키 관리자가 구성되어 있고 NSE가 사용되지 않는 경우 NAE와 NVE가 기본적으로 활성화됩니다. NAE 볼륨은 NAE 애그리게이트에 대해 기본적으로 생성되며, 비 NAE 애그리게이트에 NVE 볼륨이 기본적으로 생성됩니다. 다음 명령을 입력하여 이를 재정의할 수 있습니다.

```
cluster1::*> options -option-name
encryption.data_at_rest_encryption.disable_by_default true
```

ONTAP 9.6부터 SVM 범위를 사용하여 클러스터에 있는 데이터 SVM에 대한 외부 키 관리를 구성할 수 있습니다. 이는

각 테넌트가 데이터를 제공하기 위해 다른 SVM(또는 SVM 세트)을 사용하는 멀티테넌트 환경에 가장 적합합니다. 지정된 테넌트의 SVM 관리자만 해당 테넌트의 키에 액세스할 수 있습니다. 자세한 내용은 ONTAP 설명서의 을 ["ONTAP 9.6 이상에서 외부 키 관리를 활성화합니다"](#) 참조하십시오.

ONTAP 9.11.1부터는 SVM에서 기본 및 보조 키 서버를 지정하여 클러스터된 외부 키 관리 서버에 대한 연결을 구성할 수 있습니다. 자세한 내용은 ONTAP 설명서의 을 ["클러스터된 외부 키 서버를 구성합니다"](#) 참조하십시오.

ONTAP 9.13.1부터 시스템 관리자에서 외부 키 관리자 서버를 구성할 수 있습니다. 자세한 내용은 ONTAP 설명서의 을 ["외부 키 관리자를 관리합니다"](#) 참조하십시오.

데이터 복제 암호화

유휴 데이터의 암호화를 보완하기 위해 SnapMirror, SnapVault 또는 FlexCache에서 사전 공유 키와 TLS 1.2를 사용하여 클러스터 간 ONTAP 데이터 복제 트래픽을 암호화할 수 있습니다.

재해 복구, 캐싱 또는 백업을 위해 데이터를 복제할 때 ONTAP 클러스터 간에 유선으로 데이터를 전송하는 동안 해당 데이터를 보호해야 합니다. 이렇게 하면 전송 중일 때 기밀 데이터에 대한 악의적인 메시지 가로채기 공격을 방지할 수 있습니다.

ONTAP 9.6부터 클러스터 피어링 암호화는 SnapMirror, SnapVault, FlexCache 등과 같은 ONTAP 데이터 복제 기능을 위해 TLS 1.2 AES-256 GCM 암호화 지원을 제공합니다. 암호화는 두 클러스터 피어 간에 미리 공유된 키(PSK)를 통해 설정됩니다.

NSE, NVE, NAE와 같은 기술을 사용하여 유휴 데이터를 보호하는 고객은 ONTAP 9.6 이상으로 업그레이드하여 클러스터 피어링 암호화를 사용하여 엔드 투 엔드 데이터 암호화를 사용할 수도 있습니다.

클러스터 피어링은 클러스터 피어 간의 모든 데이터를 암호화합니다. 예를 들어, SnapMirror를 사용할 때 모든 피어링 정보와, 소스와 대상 클러스터 피어 간의 모든 SnapMirror 관계가 암호화됩니다. 클러스터 피어링 암호화가 활성화된 클러스터 피어 간에는 일반 텍스트 데이터를 보낼 수 없습니다.

ONTAP 9.6부터 새로운 클러스터 피어 관계는 기본적으로 암호화가 활성화되어 있습니다. ONTAP 9.6 이전에 생성된 클러스터 피어 관계의 암호화를 활성화하려면 소스 및 대상 클러스터를 9.6으로 업그레이드해야 합니다. 또한 클러스터 피어링 암호화를 사용하려면 명령을 사용하여 `cluster peer modify` 소스 및 대상 클러스터 피어를 모두 변경해야 합니다.

다음 예에 표시된 것처럼 ONTAP 9.6에서 클러스터 피어링 암호화를 사용하도록 기존 피어 관계를 변환할 수 있습니다.

On the Destination Cluster Peer

```
cluster2::> cluster peer modify cluster1 -auth-status-admin use-  
authentication -encryption-protocol-proposed tls-psk
```

When prompted enter a passphrase.

On the Source Cluster Peer

```
cluster1::> cluster peer modify cluster2 -auth-status-admin use-  
authentication -encryption-protocol-proposed tls-psk
```

When prompted enter the same passphrase you created in the previous step.

전송 중인 IPsec 데이터 암호화

데이터 복제 트래픽을 위해 NSE(NetApp Storage Encryption), NVE(NetApp Volume Encryption), CPE(클러스터 피어링 암호화)와 같은 유휴 데이터 암호화 기술을 사용하는 고객은 이제 ONTAP 9.8 이상으로 업그레이드하고 를 사용하여 하이브리드 멀티 클라우드 Data Fabric 전반에서 클라이언트와 스토리지 간에 엔드 투 엔드 암호화를 사용할 수 있습니다 IPsec을 선택합니다. IPsec은 NFS 또는 SMB/CIFS 암호화에 대한 대안을 제공하며 iSCSI 트래픽에 대한 전송 중인 유일한 암호화 옵션입니다.

경우에 따라 유선을 통해(또는 전송 중인) ONTAP SVM으로 전송되는 모든 클라이언트 데이터를 보호해야 할 필요가 있을 수 있습니다. 이렇게 하면 전송 중에 중요 데이터에 대한 재생 및 악의적인 메시지 가로채기 공격이 방지됩니다.

ONTAP 9.8부터 IPsec(인터넷 프로토콜 보안)은 클라이언트와 ONTAP SVM 간의 모든 IP 트래픽에 엔드 투 엔드 암호화 지원을 제공합니다. 모든 IP 트래픽에 대한 IPsec 데이터 암호화에는 NFS, iSCSI 및 SMB/CIFS 프로토콜이 포함됩니다. IPsec은 iSCSI 트래픽에 대해 전송 중인 유일한 암호화 옵션을 제공합니다.

유선을 통해 NFS 암호화를 제공하는 것은 IPsec의 주요 사용 사례 중 하나입니다. ONTAP 9.8 이전에는 NFS 유선 암호화 기능이 krb5p를 활용하여 전송 중인 NFS 데이터를 암호화하려면 Kerberos를 설정하고 구성해야 했습니다. 모든 고객 환경에서 이것이 항상 단순하거나 쉽게 달성되는 것은 아닙니다.

데이터 복제 트래픽을 위해 NSE(NetApp Storage Encryption), NVE(NetApp Volume Encryption), CPE(클러스터 피어링 암호화)와 같은 유휴 데이터 암호화 기술을 사용하는 고객은 이제 ONTAP 9.8 이상으로 업그레이드하고 를 사용하여 하이브리드 멀티 클라우드 Data Fabric 전반에서 클라이언트와 스토리지 간에 엔드 투 엔드 암호화를 사용할 수 있습니다 IPsec을 선택합니다.

IPSec은 IETF 표준입니다. ONTAP는 전송 모드에서 IPsec을 사용합니다. 또한 IPv4 또는 IPv6를 사용하여 클라이언트와 ONTAP 간의 키 자료를 협상하기 위해 사전 공유 키(PSK)를 사용하는 IKE(인터넷 키 교환) 프로토콜 버전 2를 활용합니다. 기본적으로 IPsec은 Suite-B AES-GCM 256비트 암호화를 사용합니다. 256비트 암호화를 지원하는 Suite-B AES-GMAC256 및 AES-CBC256도 지원됩니다.

클러스터에서 IPsec 기능을 활성화해야 하지만 SPD(보안 정책 데이터베이스) 항목을 사용하여 개별 SVM IP 주소에 적용됩니다. 정책(SPD) 항목에는 클라이언트 IP 주소(원격 IP 서브넷), SVM IP 주소(로컬 IP 서브넷), 사용할 암호화 암호 그룹 및 IKEv2를 통해 인증하고 IPsec 연결을 설정하는 데 필요한 사전 공유 암호(PSK)가 포함됩니다. 트래픽이 IPsec 연결을 통해 전달되기 전에 IPsec 정책 항목 외에 클라이언트가 동일한 정보(로컬 및 원격 IP, PSK 및 암호 그룹

)로 구성되어야 합니다. ONTAP 9.10.1부터 IPsec 인증서 인증 지원이 추가되었습니다. 이렇게 하면 IPsec 정책 제한이 제거되고 IPsec에 대한 Windows OS 지원이 활성화됩니다.

클라이언트와 SVM IP 주소 사이에 방화벽이 있는 경우 IKEv2 협상이 성공하고 IPsec 트래픽을 허용하려면 ESP 및 UDP(포트 500 및 4500) 프로토콜(인바운드(수신) 및 아웃바운드(송신) 모두 허용해야 합니다.

NetApp SnapMirror 및 클러스터 피어링 트래픽 암호화의 경우, 유선으로 전송되는 안전한 이동을 위해 IPsec보다 CPE(클러스터 피어링 암호화)를 사용하는 것이 좋습니다. CPE는 이러한 워크로드에 대해 IPsec보다 우수한 성능을 제공합니다. IPsec에 대한 라이선스가 필요하지 않으며 가져오기 또는 내보내기 제한이 없습니다.

다음 예에 표시된 것처럼 클러스터에서 IPsec을 활성화하고 단일 클라이언트 및 단일 SVM IP 주소에 대한 SPD 항목을 만들 수 있습니다.

```
On the Destination Cluster Peer
```

```
cluster1::> security ipsec config modify -is-enabled true
```

```
cluster1::> security ipsec policy create -vserver vs1 -name test34 -local  
-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
```

```
When prompted enter and confirm the pre shared secret (PSK).
```

TLS 및 SSL 관리

ONTAP 명령을 사용하여 매개 변수를 true로 설정하여 컨트롤 플레인 인터페이스에 대해 FIPS 140-2/3 준수 모드를 활성화할 수 is-fips-enabled security config modify 있습니다.

ONTAP 9부터는 클러스터 차원의 제어 평면 인터페이스를 위해 FIPS 140-2 규정 준수 모드를 활성화할 수 있습니다. 기본적으로 FIPS 140-2 전용 모드는 비활성화되어 있습니다. 명령에 대한 매개 변수를 로 설정하여 FIPS 140-2 규정 준수 모드를 사용하도록 설정할 수 is-fips-enabled true security config modify 있습니다. 그런 다음 를 사용하여 온라인 상태를 확인할 수 security config show command 있습니다.

FIPS 140-2 규정 준수를 활성화하면 TLSv1 및 SSLv3이 비활성화되고 TLSv1.1 및 TLSv1.2만 활성화됩니다. ONTAP는 FIPS 140-2 규정 준수를 사용하는 경우 TLSv1 및 SSLv3을 활성화하지 못하도록 합니다. FIPS 140-2를 활성화한 후 다시 비활성화하면 TLSv1 및 SSLv3은 사용 안 함으로 유지되지만 이전 구성에 따라 TLSv1.2 또는 TLSv1.1 및 TLSv1.2는 모두 사용 가능한 상태로 유지됩니다.

이 security config modify 명령은 기존 클러스터 차원의 보안 구성을 수정합니다. FIPS 호환 모드를 사용하도록 설정하면 클러스터에서 TLS 프로토콜만 자동으로 선택됩니다. -supported-protocols`FIPS 모드와 별개로 TLS 프로토콜을 포함하거나 제외하려면 매개 변수를 사용하십시오. 기본적으로 FIPS 모드는 비활성화되며 ONTAP는 TLSv1.2, TLSv1.1 및 TLSv1 프로토콜을 지원합니다.

이전 버전과의 호환성을 위해 ONTAP는 FIPS 모드가 비활성화된 경우 목록에 SSLv3 추가를 supported-protocols 지원합니다. 매개 변수를 사용하여 -supported-cipher-suites AES(Advanced Encryption Standard) 또는 AES 및 3DES 만 구성합니다. 또한!RC4를 지정하여 RC4와 같은 약한 암호를 비활성화할 수도 있습니다. 기본적으로 지원되는 암호화 설정은 ALL:!LOW:!aNULL:!EXP:!eNULL. 이 설정은 인증, 암호화 없음, 내보내기 없음 및 저암호화 암호화 암호 그룹을 제외한 프로토콜에 대해 지원되는 모든 암호화 그룹이 활성화됨을 의미합니다. 64비트 또는 56비트 암호화 알고리즘을 사용하는 제품군입니다.

선택한 해당 프로토콜에서 사용할 수 있는 암호 그룹을 선택합니다. 잘못된 구성으로 인해 일부 기능이 제대로 작동하지 않을 수 있습니다.

올바른 암호화 문자열 구문은 OpenSSL(OpenSSL 소프트웨어 재단에서 게시)의 페이지를 참조하십시오 **"암호입니다"**. ONTAP 9.9.1 이상 릴리스부터 보안 구성을 수정한 후 더 이상 모든 노드를 수동으로 재부팅할 필요가 없습니다.

FIPS 140-2 규정 준수를 활성화하면 ONTAP 9 내부 및 외부 시스템과 통신할 수 있습니다. NetApp에서는 콘솔 액세스 권한이 있는 비프로덕션 시스템에서 이러한 설정을 테스트하는 것이 좋습니다.



SSH를 사용하여 ONTAP 9를 관리하는 경우 OpenSSH 5.7 이상 클라이언트를 사용해야 합니다. SSH 클라이언트가 연결에 성공하려면 ECDSA(Elliptic Curve Digital Signature Algorithm) 공개 키 알고리즘과 협상해야 합니다.

TLS 1.2만 활성화하고 PFS(Perfect Forward Secrecy) 지원 암호화 제품군을 사용하면 TLS 보안을 더욱 강화할 수 있습니다. PFS는 TLS 1.2와 같은 암호화 프로토콜과 함께 사용할 경우 공격자가 클라이언트와 서버 간의 모든 네트워크 세션을 해독하지 못하도록 하는 키 교환 방법입니다. TLS 1.2 및 PFS 지원 암호 제품군만 활성화하려면 다음 예와 같이 고급 권한 수준에서 명령을 사용합니다 `security config modify`.



SSL 인터페이스 구성을 변경하기 전에 클라이언트가 ONTAP에 연결할 때 언급된 암호(DHE, ECDHE)를 지원해야 한다는 점을 기억해야 합니다. 그렇지 않으면 연결이 허용되지 않습니다.

```
cluster1::*> security config modify -interface SSL -supported-protocols
TLSv1.2 -supported-cipher-suites
PSK:DHE:ECDSA:!LOW:!aNULL:!EXP:!eNULL:!3DES:!kDH:!kECDH
```

`y` 각 프롬프트에 대해 확인합니다. PFS에 대한 자세한 내용은 [link:https://blog.netapp.com/protecting-your-data-perfect-forward-secrecy-pfs-with-netapp-ontap/](https://blog.netapp.com/protecting-your-data-perfect-forward-secrecy-pfs-with-netapp-ontap/) ["NetApp 블로그"] 참조하십시오.

ONTAP 9.11.1 및 TLS 1.3 지원부터 FIPS 140-3을 검증할 수 있습니다.



FIPS 구성은 ONTAP 및 플랫폼 BMC에 적용됩니다.

CA 서명 디지털 인증서를 만듭니다

대부분의 조직에서 ONTAP 웹 액세스용 자체 서명된 디지털 인증서는 InfoSec 정책을 준수하지 않습니다. 운영 시스템에서는 클러스터 또는 SVM을 SSL 서버로 인증하는 데 사용할 CA 서명 디지털 인증서를 설치하는 것이 NetApp 모범 사례입니다.

명령을 사용하여 CSR(인증서 서명 요청)을 생성하고 명령을 사용하여 CA에서 받은 인증서를 설치할 수 `security certificate generate-csr security certificate install` 있습니다.

단계

1. 조직의 CA에서 서명한 디지털 인증서를 만들려면 다음을 실행합니다.

- a. CSR을 생성합니다.
- b. 조직의 절차에 따라 조직의 CA에서 CSR을 사용하여 디지털 인증서를 요청합니다. 예를 들어 Microsoft Active Directory 인증서 서비스 웹 인터페이스를 사용하여 `로 <CA_server_name>/certsrv 이동하여 인증서를 요청합니다.`
- c. ONTAP에 디지털 인증서를 설치합니다.

온라인 인증서 상태 프로토콜입니다

OCSP(온라인 인증서 상태 프로토콜)를 사용하면 LDAP 또는 TLS와 같은 TLS 통신을 사용하는 ONTAP 애플리케이션이 OCSP가 설정된 경우 디지털 인증서 상태를 수신할 수 있습니다. 응용 프로그램에서 요청된 인증서가 양호하거나 해지되었거나 알 수 없음을 나타내는 서명된 응답을 받습니다.

OCSP를 사용하면 인증서 해지 목록(CRL) 없이도 디지털 인증서 상태를 확인할 수 있습니다.

기본적으로 OCSP 인증서 상태 확인은 사용되지 않습니다. 앱 이름은 , , , , , 로 설정할 수 있는 명령을 사용하여 쉘 수 `security config ocspl enable -app name` 있습니다. `autosupport audit_log fabricpool ems kmip ldap_ad ldap_nis_namemap, 또는 모두. 이 명령에는 advanced 권한 수준이 필요합니다.`

SSHv2 관리

이 `security ssh modify` 명령을 실행하면 클러스터에 대한 SSH 키 교환 알고리즘, 암호 또는 MAC 알고리즘의 기존 구성을 지정한 구성 설정으로 대체합니다.

NetApp에서 권장하는 사항은 다음과 같습니다.



- 사용자 세션에 암호를 사용합니다.
- 컴퓨터 액세스에 공개 키를 사용합니다.

지원되는 암호 및 키 교환

암호입니다	키 교환
AES256-CTR	Diffie-Hellman-group-exchange-SHA256(SHA-2)
AES192 - CTR	Diffie-Hellman-group-exchange-SHA1(SHA-1)
AES128-CTR	Diffie-Hellman-group14-SHA1(SHA-1)
AES256 - CBC	Diffie-Hellman-group1-SHA1(SHA-1)
AES192 - CBC	-
AES128 - CBC	-
AES128-GCM을 참조하십시오	-
AES256-GCM을 참조하십시오	-
3DES-CBC입니다	-

AES 및 3DES 대칭 암호화가 지원됩니다

ONTAP는 다음 유형의 AES 및 3DES 대칭 암호화(암호라고도 함)도 지원합니다.

- HMAC-SHA1
- HMAC-SHA1-96
- HMAC-MD5 를 참조하십시오
- HMAC-MD5-96
- HMAC-RIPEMD160
- umac-64 를 참조하십시오
- umac-64 를 참조하십시오
- umac-128
- HMAC-SHA2-256
- HMAC-SHA2-512
- HMAC-SHA1-ETM
- HMAC-SHA1-96-ETM
- HMAC-SHA2-256-ETM
- HMAC-SHA2-512-ETM
- HMAC-MD5-ETM의 약어입니다
- HMAC-MD5-96-ETM
- HMAC-RIPEMD160-ETM
- umac-64-ETM
- umac-128-ETM



SSH 관리 구성은 ONTAP 및 플랫폼 BMC에 적용됩니다.

NetApp AutoSupport를 참조하십시오

ONTAP의 AutoSupport 기능을 사용하면 시스템의 상태를 사전에 모니터링하고 메시지와 세부 정보를 NetApp 기술 지원, 조직의 내부 지원 팀 또는 지원 파트너에게 자동으로 보낼 수 있습니다. 기본적으로 스토리지 시스템을 처음 구성하면 NetApp 기술 지원에 보내는 AutoSupport 메시지가 사용하도록 설정됩니다. 또한 AutoSupport는 NetApp 기술 지원이 활성화된 후 24시간 후에 메시지를 보내기 시작합니다. 이 24시간 기간은 구성 가능합니다. 조직의 내부 지원 팀과의 통신을 활용하려면 메일 호스트 구성을 완료해야 합니다.

클러스터 관리자만 AutoSupport 관리(구성)를 수행할 수 있습니다. SVM 관리자는 AutoSupport에 액세스할 수 없습니다. AutoSupport 기능을 비활성화할 수 있습니다. 하지만 NetApp 스토리지 시스템에서 문제가 발생하는 경우 AutoSupport가 문제를 더 빠르게 식별하고 해결할 수 있도록 이 기능을 사용하도록 설정하는 것이 좋습니다. 기본적으로 시스템은 AutoSupport 정보를 수집하여 사용자가 AutoSupport를 사용하지 않도록 설정한 경우에도 로컬에 저장합니다.

다양한 메시지에 포함된 내용 및 다양한 유형의 메시지가 전송되는 위치를 비롯하여 AutoSupport 메시지에 대한 자세한

내용은 설명서를 참조하십시오. "[NetApp Active IQ 디지털 자문업체](#)"

AutoSupport 메시지에는 다음 항목을 포함하되 이에 국한되지 않는 중요한 데이터가 포함됩니다.

- 로그 파일
- 특정 하위 시스템과 관련된 상황에 맞는 데이터입니다
- 구성 및 상태 데이터
- 성능 데이터

AutoSupport는 전송 프로토콜을 위해 HTTPS, HTTP 및 SMTP를 지원합니다. AutoSupport 메시지는 기본적으로 민감하므로 NetApp 지원에 AutoSupport 메시지를 보낼 때 HTTPS를 기본 전송 프로토콜로 사용하는 것이 좋습니다.

또한 명령을 활용하여 `system node autosupport modify` AutoSupport 데이터의 타겟을 지정해야 합니다(예: NetApp 기술 지원, 조직의 내부 운영, 파트너). 이 명령을 사용하여 보낼 특정 AutoSupport 세부 정보(예: 성능 데이터, 로그 파일 등)를 지정할 수도 있습니다.

AutoSupport를 완전히 해제하려면 `system node autosupport modify -state disable` 명령을 사용합니다.

Network Time Protocol의 약어입니다

ONTAP를 사용하면 클러스터에서 시간대, 날짜 및 시간을 수동으로 설정할 수 있지만 적어도 3개의 외부 NTP 서버와 클러스터 시간을 동기화하도록 NTP(네트워크 시간 프로토콜) 서버를 구성해야 합니다.

클러스터 시간이 정확하지 않을 수 있습니다. ONTAP를 사용하면 클러스터에서 시간대, 날짜 및 시간을 수동으로 설정할 수 있지만 클러스터 시간을 외부 NTP 서버와 동기화하도록 NTP(네트워크 시간 프로토콜) 서버를 구성해야 합니다.

ONTAP 9.5부터 대칭 인증을 사용하여 NTP 서버를 구성할 수 있습니다.

명령을 사용하여 최대 10개의 외부 NTP 서버를 연결할 수 `cluster time-service ntp server create` 있습니다. 시간 서비스의 이중화 및 품질을 위해 최소 3개의 외부 NTP 서버를 클러스터에 연결해야 합니다.

ONTAP에서 NTP 구성에 대한 자세한 내용은 을 참조하십시오 "[클러스터 시간 관리\(클러스터 관리자만 해당\)](#)".

NAS 파일 시스템 로컬 계정(CIFS 작업 그룹)

워크그룹 클라이언트 인증은 기존의 도메인 인증 방식과 동일하게 ONTAP 솔루션에 추가적인 보안 계층을 제공합니다. 명령을 사용하면 `vserver cifs session show` IP 정보, 인증 메커니즘, 프로토콜 버전 및 인증 유형을 비롯한 다양한 상태 관련 세부 정보를 표시할 수 있습니다.

ONTAP 9부터 로컬로 정의된 사용자 및 그룹을 사용하여 서버에 인증하는 CIFS 클라이언트를 사용하여 작업 그룹에 CIFS 서버를 구성할 수 있습니다. 워크그룹 클라이언트 인증은 기존의 도메인 인증 방식과 동일하게 ONTAP 솔루션에 추가적인 보안 계층을 제공합니다. CIFS 서버를 구성하려면 명령을 사용합니다 `vserver cifs create`. CIFS 서버를 생성한 후에는 CIFS 도메인에 연결하거나 작업 그룹에 연결할 수 있습니다. 작업 그룹에 참여하려면 `-workgroup` 매개 변수를 사용합니다. 다음은 구성의 예입니다.

```
cluster1::> vservers cifs create -vservers vs1 -cifs-server CIFS_SERVER1
-workgroup Sales
```



작업 그룹 모드의 CIFS 서버는 Windows NT LAN Manager(NTLM) 인증만 지원하며 Kerberos 인증은 지원하지 않습니다.

NetApp은 NTLM 인증 기능을 CIFS 작업 그룹과 함께 사용하여 조직의 보안 상태를 유지할 것을 권장합니다. NetApp은 명령을 사용하여 CIFS 보안 상태를 검증하기 위해 IP 정보, 인증 메커니즘, 프로토콜 버전 및 인증 유형 등의 다양한 상태 관련 세부 정보를 표시할 것을 `vservers cifs session show` 권장합니다.

NAS 파일 시스템 감사

NAS 파일 시스템이 차지하는 공간 증가 오늘날의 위협 환경에서 감사 기능은 가시성을 지원하는 데 매우 중요합니다.

보안에는 검증이 필요합니다. ONTAP 9은 솔루션 전반에 걸쳐 향상된 감사 이벤트와 세부 정보를 제공합니다. NAS 파일 시스템은 오늘날의 위협 환경에서 차지하는 공간이 늘어나기 때문에 감사 기능은 가시성을 지원하는 데 매우 중요합니다. ONTAP 9의 감사 기능이 개선되었기 때문에 CIFS 감사 세부 정보가 그 어느 때보다 많이 제공됩니다. 생성된 이벤트로 다음을 비롯한 키 세부 정보가 기록됩니다.

- 파일, 폴더 및 공유 액세스
- 생성, 수정 또는 삭제된 파일
- 파일 읽기 액세스가 성공했습니다
- 파일 읽기 또는 쓰기 시도가 실패했습니다
- 폴더 권한 변경

감사 구성을 생성합니다

감사 이벤트를 생성하려면 CIFS 감사를 설정해야 합니다. 명령을 사용하여 `vservers audit create` 감사 구성을 생성합니다. 기본적으로 감사 로그는 크기에 따라 순환 방법을 사용합니다. Rotation Parameters(회전 매개변수) 필드에 지정된 경우 시간 기반 회전 옵션을 사용할 수 있습니다. 추가 로그 감사 회전 구성 세부 정보에는 회전 일정, 회전 제한, 주중 회전 날짜 및 회전 크기가 포함됩니다. 다음 텍스트는 12:30에 모든 요일에 대해 예약된 월별 시간 기반 순환을 사용하는 감사 구성을 보여 주는 예제 구성을 제공합니다.

```
cluster1::> vservers audit create -vservers vs1 -destination /audit_log
-rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule
-hour 12 -rotate-schedule-minute 30
```

CIFS 감사 이벤트입니다

CIFS 감사 이벤트는 다음과 같습니다.

- * File share *: CIFS 네트워크 공유가 추가, 수정 또는 삭제될 때 관련 명령을 사용하여 감사 이벤트를 `vservers cifs share` 생성합니다.

- * 감사 정책 변경 *: 감사 정책이 비활성화, 활성화 또는 수정된 경우 관련 명령을 사용하여 감사 이벤트를 `vserver audit` 생성합니다.
- * 사용자 계정 *: 로컬 CIFS 또는 UNIX 사용자가 생성 또는 삭제되거나, 로컬 사용자 계정이 활성화, 비활성화 또는 수정되거나, 암호가 재설정되거나 변경될 때 감사 이벤트를 생성합니다. 이 이벤트는 `vserver cifs users-and-groups local-group` 명령 또는 관련 `vserver services name-service unix-user` 명령을 사용합니다.
- * Security group *: 명령 또는 관련 명령을 사용하여 로컬 CIFS 또는 UNIX 보안 그룹을 생성하거나 삭제할 때 감사 이벤트를 `vserver cifs users-and-groups local-group vserver services name-service unix-group` 생성합니다.
- * 권한 부여 정책 변경 *: 명령을 사용하여 CIFS 사용자 또는 CIFS 그룹에 대한 권한이 부여되거나 취소될 때 감사 이벤트를 `vserver cifs users-and-groups privilege` 생성합니다.



이 기능은 시스템 감사 기능을 기반으로 합니다. 이 기능을 사용하면 관리자가 데이터 사용자의 관점에서 시스템에서 허용하고 수행하는 작업을 검토할 수 있습니다.

REST API가 NAS 감사에 미치는 영향

ONTAP에는 관리자 계정이 REST API를 사용하여 SMB/CIFS 또는 NFS 파일에 액세스하고 조작할 수 있는 기능이 포함되어 있습니다. REST API는 ONTAP 관리자만 실행할 수 있지만 REST API 명령은 시스템 NAS 감사 로그를 무시합니다. 또한 REST API를 사용할 때 ONTAP 관리자가 파일 권한을 무시할 수도 있습니다. 그러나 파일에 대한 REST API를 사용한 관리자의 작업은 시스템 명령 기록 로그에 기록됩니다.

액세스할 수 없는 **REST API** 역할을 생성합니다

REST를 통해 ONTAP 볼륨에 액세스할 수 없는 REST API 역할을 생성하여 ONTAP 관리자가 파일 액세스에 REST API를 사용하지 못하도록 할 수 있습니다. 이 역할을 프로비저닝하려면 다음 단계를 완료하십시오.

단계

1. 스토리지 볼륨에 대한 액세스 권한이 없지만 다른 모든 REST API 액세스가 가능한 새 REST 역할을 생성합니다.

```
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api/storage/volumes" -access none
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api" -access all
```

2. 이전 단계에서 만든 새 REST API 역할에 관리자 계정을 할당합니다.

```
cluster1::> security login modify -user-or-group-name user1 -application
http -authentication-method password -vserver cluster1 -role nofile
```



기본 제공 ONTAP 클러스터 관리자 계정에서 파일 액세스에 REST API를 사용하지 않으려면 먼저 해야 **"새 관리자 계정을 만들고 기본 제공 계정을 사용 안 함 또는 삭제합니다"**합니다.

CIFS SMB 서명 및 봉인을 구성하고 사용하도록 설정합니다

스토리지 시스템과 클라이언트 간의 트래픽이 재생 공격이나 메시지 가로채기 공격으로 인해 손상되지 않도록 하여 Data Fabric의 보안을 보호하는 SMB 서명을 구성하고 사용하도록 설정할 수 있습니다. SMB 서명은 SMB 메시지에 유효한 서명이 있는지 확인하여 보호합니다.

이 작업에 대해

파일 시스템 및 아키텍처의 일반적인 위협 벡터는 SMB 프로토콜에 있습니다. 이 문제를 해결하기 위해 ONTAP 9 솔루션은 업계 표준 SMB 서명 및 봉인을 사용합니다. SMB 서명을 활용하면 스토리지 시스템과 클라이언트 사이의 트래픽이 재생 공격이나 메시지 가로채기 공격으로 인해 손상되지 않도록 하여 Data Fabric의 보안을 보호할 수 있습니다. 이는 SMB 메시지에 포함되는 유효한 서명이 있는지 확인하는 것으로 간주됩니다.

SMB 서명은 성능을 위해 기본적으로 비활성화되어 있지만 NetApp에서는 이를 사용하도록 설정하는 것이 좋습니다. 또한 ONTAP 솔루션은 봉인이라고도 하는 SMB 암호화를 지원합니다. 이 접근 방식을 사용하면 공유별로 데이터를 안전하게 전송할 수 있습니다. 기본적으로 SMB 암호화는 비활성화되어 있습니다. 그러나 NetApp는 SMB 암호화를 활성화할 것을 권장합니다.

이제 SMB 2.0 이상에서 LDAP 서명 및 봉인이 지원됩니다. 서명(변조 방지)과 봉인(암호화)을 통해 SVM과 Active Directory 서버 간의 안전한 통신을 지원합니다. 이제 SMB 3.0 이상에서 AES 새 명령(Intel AES NI) 암호화가 지원됩니다. 더욱 개선된 AES 알고리즘인 Intel AES NI는 지원되는 프로세서 제품군에서 데이터 암호화의 성능을 높여 줍니다.

단계

1. SMB 서명을 구성하고 사용하도록 설정하려면 명령을 사용하고 `vserver cifs security modify` 매개 변수가 (으)로 설정되어 있는지 `-is-signing-required true` 확인하십시오. 다음 예제 구성을 참조하십시오.

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock  
-skew 3 -kerberos-ticket-age 8 -is-signing-required true
```

2. SMB 봉인 및 암호화를 구성하고 사용하도록 설정하려면 명령을 사용하여 `vserver cifs security modify` 매개 변수가 으로 설정되어 있는지 `-is-smb-encryption-required true` 확인하십시오. 다음 예제 구성을 참조하십시오.

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption  
-required true  
  
cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-  
encryption-required  
vserver is-smb-encryption-required  
-----  
vs1 true
```

NFS 보안

내보내기 규칙은 익스포트 정책의 기능 요소입니다. 내보내기 규칙은 클라이언트 액세스 요청을

처리하는 방법을 결정하기 위해 구성하는 특정 매개 변수와 볼륨에 대한 클라이언트 액세스 요청과 일치합니다. 클라이언트에 대한 액세스를 허용하려면 내보내기 정책에 하나 이상의 내보내기 규칙이 있어야 합니다. 익스포트 정책에 둘 이상의 규칙이 포함된 경우 규칙은 익스포트 정책에 표시되는 순서대로 처리됩니다.

액세스 제어는 안전한 태세를 유지하는 데 있어 핵심입니다. 따라서 ONTAP은 익스포트 정책 기능을 사용하여 특정 매개 변수와 일치하는 클라이언트에 대한 NFS 볼륨 액세스를 제한합니다. 익스포트 정책에는 각 클라이언트 액세스 요청을 처리하는 익스포트 규칙이 하나 이상 포함되어 있습니다. 익스포트 정책은 각 볼륨과 연결되어 볼륨에 대한 클라이언트 액세스를 구성합니다. 이 프로세스의 결과는 클라이언트가 볼륨에 대한 액세스 권한을 부여 또는 거부(권한 거부 메시지 포함)할지 여부를 결정합니다. 이 프로세스는 볼륨에 제공되는 액세스 레벨도 결정합니다.



클라이언트가 데이터에 액세스하려면 SVM에 익스포트 규칙이 있는 익스포트 정책이 있어야 합니다. SVM은 여러 익스포트 정책을 포함할 수 있습니다.

규칙 순서는 규칙 인덱스 번호로 지정됩니다. 규칙이 클라이언트와 일치하면 해당 규칙의 사용 권한이 사용되고 더 이상 규칙이 처리되지 않습니다. 일치하는 규칙이 없으면 클라이언트가 액세스가 거부됩니다.

내보내기 규칙은 다음 기준을 적용하여 클라이언트 액세스 권한을 결정합니다.

- 클라이언트에서 요청을 보내는 데 사용되는 파일 액세스 프로토콜(예: NFSv4 또는 SMB)
- 클라이언트 식별자(예: 호스트 이름 또는 IP 주소)
- 클라이언트가 인증하는 데 사용하는 보안 유형(예: Kerberos v5, NTLM 또는 AUTH_SYS)

규칙이 여러 조건을 지정하고 클라이언트가 하나 이상의 조건을 일치하지 않으면 규칙이 적용되지 않습니다.

익스포트 정책의 예로는 다음과 같은 매개 변수를 가진 익스포트 규칙이 있습니다.

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

보안 유형은 클라이언트가 받는 액세스 수준을 결정합니다. 세 가지 액세스 수준은 읽기 전용, 읽기/쓰기 및 수퍼유저입니다(사용자 ID가 있는 클라이언트의 경우 0). 보안 유형에 의해 결정되는 액세스 수준은 이 순서로 평가되므로 나열된 규칙을 준수해야 합니다.

내보내기 규칙의 액세스 수준 매개 변수에 대한 규칙입니다

클라이언트가 다음과 같은 액세스 수준을 얻을 수 있습니다	이러한 액세스 매개 변수는 클라이언트의 보안 유형과 일치해야 합니다
일반 사용자 읽기 전용	읽기 전용('rorule')
일반 사용자 읽기-쓰기	읽기 전용('rorule') 및 읽기/쓰기('rwrule')
고급 사용자 읽기 전용	읽기 전용('rorule') 및 '-superuser'
고급 사용자 읽기-쓰기	읽기 전용('rorule') 및 읽기/쓰기('rwrule') 및 '-superuser'


다음은 이러한 세 가지 액세스 매개 변수 각각에 대해 유효한 보안 유형입니다.

- 모두
- 없음
- 안 함

다음 보안 형식은 매개 변수와 함께 사용할 수 `-superuser` 없습니다.

- krb5
- NTLM입니다
- 시스템

매개 변수 결과에 액세스하기 위한 규칙입니다

클라이언트의 보안 유형....	그럼...
access 매개 변수에 지정된 보안 유형과 일치합니다.	클라이언트는 자체 사용자 ID를 사용하여 해당 수준에 대한 액세스를 받습니다.
지정된 보안 유형과 일치하지 않지만 access 매개 변수에 옵션이 포함되어 `none` 있습니다.	클라이언트는 해당 레벨에 대한 액세스 권한을 받고 매개 변수로 지정된 사용자 ID를 사용하여 익명 사용자를 <code>-anon</code> 받습니다.
지정된 보안 유형과 일치하지 않으며 access 매개 변수에 옵션이 포함되어 있지 `none` 않습니다.	클라이언트는 해당 레벨에 대한 액세스 권한을 받지 않습니다.
	 이 매개 변수는 지정되지 않은 경우에도 항상 없음이 포함되므로 이 제한은 매개 변수에 적용되지 <code>-superuser</code> 않습니다.

Kerberos 5 및 Krb5p

ONTAP 9부터 개인 정보 보호 서비스(krb5p)를 통한 Kerberos 5 인증이 지원됩니다. krb5p 인증 모드는 안전하며 체크섬을 사용하여 클라이언트와 서버 간의 모든 트래픽을 암호화하여 데이터 무단 변경 및 스누핑으로부터 보호합니다. ONTAP 솔루션은 Kerberos 128비트/256비트 AES 암호화를 지원합니다. 개인정보보호 서비스에는 수신 데이터의 무결성 확인, 사용자 인증, 전송 전 데이터 암호화가 포함됩니다.

krb5p 옵션은 암호화 옵션으로 설정된 내보내기 정책 기능에 가장 많이 있습니다. 다음 예와 같이 krb5p 인증 방법을 인증 매개 변수로 사용할 수 있습니다.

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
10.22.32.42 -volume flex_vol -authentication-method krb5p -protocol nfs3
-access- type read
```

Lightweight Directory Access Protocol 서명 및 봉인을 활성화합니다

서명과 봉인을 지원하여 LDAP 서버에 대한 쿼리에 대한 세션 보안을 활성화합니다. 이 접근

방식은 LDAP-over-TLS 세션 보안을 대체할 수 있습니다.

서명은 비밀 키 기술을 사용하여 LDAP 페이로드 데이터의 무결성을 확인합니다. 봉인은 LDAP 페이로드 데이터를 암호화하여 중요한 정보를 일반 텍스트로 전송하지 않도록 합니다. SVM의 세션 보안 설정은 LDAP 서버에서 사용할 수 있는 설정과 일치합니다. 기본적으로 LDAP 서명 및 봉인은 사용되지 않습니다.

단계

1. 이 기능을 활성화하려면 `vserver cifs security modify` 매개 변수를 사용하여 명령을 `session-security-for-ad-ldap` 실행합니다.

LDAP 보안 기능 옵션:

- * 없음 *: 기본값, 서명 또는 봉인 없음
- * 서명 *: LDAP 트래픽에 서명합니다
- * Seal *: LDAP 트래픽을 서명 및 암호화합니다



서명 및 봉인 매개변수는 누적되므로 서명 옵션을 사용할 경우 결과가 서명과 함께 LDAP입니다. 단, 쉘 옵션을 사용할 경우 결과는 표지와 쉘입니다. 또한 이 명령에 매개 변수를 지정하지 않으면 기본값은 none입니다.

다음은 구성의 예입니다.

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock  
-skew 3 -kerberos-ticket-age 8 -session-security-for-ad-ldap seal
```

NetApp FPolicy를 생성하여 사용합니다

ONTAP 솔루션의 인프라 구성요소인 FPolicy를 생성하여 파트너 애플리케이션이 파일 액세스 권한을 모니터링하고 설정할 수 있도록 합니다. 더욱 강력한 애플리케이션 중 하나는 하이브리드 클라우드 환경 전반에서 모든 기업 데이터 액세스에 대한 중앙 집중식 가시성과 제어를 제공하여 보안 및 규정 준수 목표를 달성하는 NetApp SaaS 애플리케이션인 스토리지 워크로드 보안입니다.

액세스 제어는 중요한 보안 개념입니다. 가시성과 파일 액세스 및 파일 작업에 대응하는 기능은 보안 태세를 유지하는 데 있어 아주 중요합니다. 가시성과 파일 액세스 제어를 제공하기 위해 ONTAP 솔루션은 NetApp FPolicy 기능을 사용합니다.

파일 유형에 따라 파일 정책을 설정할 수 있습니다. FPolicy는 스토리지 시스템이 개별 클라이언트 시스템에서 요청한 생성, 열기, 이름 변경, 삭제 등의 작업을 처리하는 방식을 결정합니다. ONTAP 9부터 FPolicy 파일 액세스 알림 프레임워크가 개선되어 필터링 제어 및 단기적인 네트워크 중단에 대비한 복원력을 갖추게 되었습니다.

단계

1. FPolicy 기능을 활용하려면 먼저 명령으로 FPolicy 정책을 생성해야 `vserver fpolicy policy create` 합니다.



또한 `-events` 가시성과 이벤트 수집에 FPolicy를 사용하는 경우 매개 변수를 사용하십시오. ONTAP에서 제공하는 추가 세분화 수준을 통해 필터링 및 사용자 이름 제어 수준까지 액세스할 수 있습니다. 사용자 이름으로 권한을 제어하고 액세스를 제어하려면 `-privilege-user-name` 매개 변수를 지정합니다.

다음 텍스트는 FPolicy 생성의 예를 제공합니다.

```
cluster1::> vserver fpolicy policy create -vserver vs1.example.com
-policy-name vs1_pol -events cserver_evt,vl1l -engine native -is
-mandatory true -allow-privileged-access no -is-passthrough-read-enabled
false
```

2. FPolicy 정책을 생성한 후에는 명령으로 정책을 활성화해야 `vserver fpolicy enable` 합니다. 또한 이 명령은 FPolicy 항목의 우선순위 또는 순서를 설정합니다.



FPolicy 시퀀스는 여러 정책이 동일한 파일 액세스 이벤트를 구독한 경우 액세스 허용 또는 거부 순서를 지시하기 때문에 중요합니다.

다음 텍스트는 FPolicy 정책을 설정하고 명령을 통해 구성을 검증하기 위한 샘플 구성을 `vserver fpolicy show` 제공합니다.

```
cluster1::> vserver fpolicy enable -vserver vs2.example.com -policy-name
vs2_pol -sequence-number 5

cluster1::> vserver fpolicy show
Vserver                Policy Name                Sequence  Status
Engine
-----
vs1.example.com        vs1_pol
vs2.example.com        vs2_pol
external
2 entries were displayed.
```

FPolicy 개선 사항

ONTAP 9에는 다음 섹션에서 설명하는 FPolicy 개선 사항이 포함되어 있습니다.

필터링 컨트롤

디렉터리 활동에 대한 알림을 제거하거나 제거하는 데 새 필터를 사용할 수 `SetAttr` 있습니다.

비동기식 복원력

비동기 모드에서 작동하는 FPolicy 서버에서 네트워크 중단이 발생하는 경우, 정전 중에 생성된 FPolicy 알림은

스토리지 노드에 저장됩니다. FPolicy 서버가 온라인 상태로 돌아오면 저장된 알림에 대한 알림이 표시되고 스토리지 노드에서 가져올 수 있습니다. 정전 중에 알림을 저장할 수 있는 시간은 최대 10분까지 구성할 수 있습니다.

LIF 보안

LIF는 역할, 홈 포트, 홈 노드, 페일오버할 포트 목록 및 방화벽 정책과 같은 관련 특성이 있는 IP 주소 또는 WWPN(Worldwide Port Name)입니다. 클러스터가 네트워크를 통해 통신을 주고받는 포트에 LIF를 구성할 수 있습니다. 각 LIF 역할의 보안 특성을 이해하는 것이 중요합니다.

LIF 역할

LIF 역할은 다음과 같습니다.

- * 데이터 LIF *: SVM에 연결된 LIF로 클라이언트와의 통신에 사용됩니다.
- * 클러스터 LIF *: 클러스터 내 노드 간에 클러스터 간 트래픽을 전달하는 데 사용되는 LIF.
- * 노드 관리 LIF *: 클러스터의 특정 노드를 관리하기 위한 전용 IP 주소를 제공하는 LIF입니다.
- * 클러스터 관리 LIF *: 전체 클러스터에 대한 단일 관리 인터페이스를 제공하는 LIF입니다.
- * Intercluster LIF *: 클러스터 간 통신, 백업 및 복제에 사용되는 LIF.

각 LIF 역할의 보안 특성입니다

	데이터 LIF	클러스터 LIF	노드 관리 LIF	클러스터 관리 LIF입니다	인터클러스터 LIF
프라이빗 IP 서브넷이 필요합니까?	아니요	예	아니요	아니요	아니요
보안 네트워크가 필요하십니까?	아니요	예	아니요	아니요	예
기본 방화벽 정책	매우 제한적입니다	완전히 열립니다	중간	중간	매우 제한적입니다
방화벽을 사용자 정의할 수 있습니까?	예	아니요	예	예	예



- 클러스터 LIF는 구성 가능한 방화벽 정책을 가지고 있지 않으며 완전히 열리기 때문에 격리된 보안 네트워크의 프라이빗 IP 서브넷에 있어야 합니다.
- 어떤 상황에서도 LIF 역할이 인터넷에 공개되어서는 안 됩니다.

LIF 보안에 대한 자세한 내용은 ["LIF의 방화벽 정책을 구성합니다"](#) 참조하십시오.

프로토콜 및 포트 보안

솔루션 강화에는 온박스 보안 작업 및 기능 외에도 오프 박스 보안 메커니즘도 포함되어야 합니다. 방화벽, IPS(침입 방지 시스템) 및 기타 보안 장치와 같은 추가 인프라 장치를 활용하여

ONTAP에 대한 액세스를 필터링하고 제한하는 것은 엄격한 보안 태세를 구축하고 유지하는 효과적인 방법입니다. 이 정보는 환경과 해당 리소스에 대한 액세스를 필터링하고 제한하기 위한 핵심 구성 요소입니다.

일반적으로 사용되는 프로토콜 및 포트

서비스	포트/프로토콜	설명
SSH	22/TCP	SSH 로그인
telnet	23/TCP	원격 로그인
Domain	53/TCP	도메인 이름 서버
HTTP	80/TCP 80/UDP입니다	HTTP
rpcbind	111/TCP 111/UDP	원격 프로시저 호출
NTP	123/UDP입니다	Network Time Protocol의 약어입니다
msrpc	135/UDP	Microsoft 원격 프로시저 호출
Netbios-name	137/TCP 137/UDP	NetBIOS 이름 서비스입니다
netbios-ssn	139/TCP 를 참조하십시오	NetBIOS 서비스 세션입니다
SNMP	161/UDP	SNMP를 선택합니다
HTTPS	443/TCP	보안 링크: http
microsoft-ds	445/TCP	Microsoft 디렉토리 서비스
IPsec	500/UDP입니다	인터넷 프로토콜 보안
mount	635/UDP	NFS 마운트
named	953/UDP	이름 데몬입니다
NFS	2049/UDP 2049/TCP	NFS 서버 데몬
nrv	2050/TCP	NetApp 원격 볼륨 프로토콜
iscsi	3260/TCP	iSCSI 타겟 포트입니다
Lockd	4045/TCP 4045/UDP	NFS 잠금 데몬
NFS	4046/TCP	NFS 마운트 프로토콜
acp-proto	4046/UDP	계정 프로토콜
rquotad	4049/UDP	NFS rquotad 프로토콜
krb524	4444/UDP	Kerberos 524
IPsec	4500/UDP입니다	인터넷 프로토콜 보안

서비스	포트/프로토콜	설명
acp	5125/UDP 5133/UDP 5144/TCP	디스크용 대체 제어 포트
Mdns	5353/UDP	멀티캐스트 DNS
HTTPS	5986/UDP	HTTPS 포트: 수신 이진 프로토콜
TELNET	8023/TCP입니다	노드 범위 텔넷
HTTPS	8443/TCP	링크를 통한 7MTT GUI 툴: HTTPS
RSH	8514/TCP입니다	노드 범위 RSH
KMIP	9877/TCP입니다	KMIP 클라이언트 포트(내부 로컬 호스트만 해당)
ndmp	10000/TCP	NDMP
cifs 증인 포트	40001/TCP	CIFS 감시 포트입니다
TLS	50000/TCP	전송 계층 보안
Iscsi	65200/TCP	iSCSI 포트입니다
SSH	65502/TCP입니다	보안 셸
vsun	65503/TCP입니다	vsun

NetApp 내부 포트

포트/프로토콜	설명
900	NetApp 클러스터 RPC
902	NetApp 클러스터 RPC
904	NetApp 클러스터 RPC
905	NetApp 클러스터 RPC
910	NetApp 클러스터 RPC
911	NetApp 클러스터 RPC
913	NetApp 클러스터 RPC
914	NetApp 클러스터 RPC
915	NetApp 클러스터 RPC
918	NetApp 클러스터 RPC
920	NetApp 클러스터 RPC
921)를 참조하십시오	NetApp 클러스터 RPC
924	NetApp 클러스터 RPC
925	NetApp 클러스터 RPC
927)를 참조하십시오	NetApp 클러스터 RPC
928	NetApp 클러스터 RPC

포트/프로토콜	설명
929)를 누릅니다	NetApp 클러스터 RPC
931	NetApp 클러스터 RPC
932	NetApp 클러스터 RPC
933	NetApp 클러스터 RPC
934	NetApp 클러스터 RPC
935	NetApp 클러스터 RPC
936	NetApp 클러스터 RPC
937	NetApp 클러스터 RPC
939	NetApp 클러스터 RPC
940	NetApp 클러스터 RPC
951을 참조하십시오	NetApp 클러스터 RPC
954를 참조하십시오	NetApp 클러스터 RPC
955	NetApp 클러스터 RPC
956을 참조하십시오	NetApp 클러스터 RPC
958	NetApp 클러스터 RPC
961	NetApp 클러스터 RPC
963	NetApp 클러스터 RPC
964	NetApp 클러스터 RPC
966	NetApp 클러스터 RPC
967	NetApp 클러스터 RPC
7810)를 참조하십시오	NetApp 클러스터 RPC
7811	NetApp 클러스터 RPC
7812)를 참조하십시오	NetApp 클러스터 RPC
7813)를 참조하십시오	NetApp 클러스터 RPC
7814)를 참조하십시오	NetApp 클러스터 RPC
7815)를 참조하십시오	NetApp 클러스터 RPC
7816	NetApp 클러스터 RPC
7817	NetApp 클러스터 RPC
7818)를 참조하십시오	NetApp 클러스터 RPC
7819)를 참조하십시오	NetApp 클러스터 RPC
7820)를 참조하십시오	NetApp 클러스터 RPC
7821)를 참조하십시오	NetApp 클러스터 RPC
7822)를 참조하십시오	NetApp 클러스터 RPC

포트/프로토콜	설명
7823)를 참조하십시오	NetApp 클러스터 RPC
7824)를 참조하십시오	NetApp 클러스터 RPC

보안 리소스

이 ONTAP 보안 설명서에 설명된 정보에 대한 자세한 내용은 다음 추가 정보 및 보안 개념을 참조하십시오.

취약성 및 사고 보고, NetApp 보안 응답 및 고객 기밀성에 대한 자세한 내용은 를 참조하십시오 ["NetApp 보안 포털"](#).

- ["ONTAP 9 릴리즈 노트"](#)
- ["ONTAP 9 명령 참조"](#)
- ["시스템 관리"](#)
- ["관리자 인증 및 RBAC"](#)
- ["NetApp 암호화"](#)
- ["TR-4647: ONTAP 9.3의 다단계 인증"](#)
- ["OpenSSL 암호화"](#)
- ["CryptoMod FIPS-140-2 레벨 1"](#)
- ["ONTAP용 NetApp 관리 SDK를 사용한 인증서 기반 인증"](#)
- ["네트워크 관리"](#)

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.