



NVE를 사용하여 볼륨 데이터 암호화 ONTAP 9

NetApp
July 11, 2025

목차

NVE를 사용하여 볼륨 데이터 암호화	1
NVE 개요를 사용하여 볼륨 데이터 암호화	1
ONTAP에서 VE 라이선스를 사용하여 애그리게이트 수준 암호화를 활성화합니다	1
ONTAP에서 새 볼륨에 대해 암호화를 활성화합니다	2
ONTAP에서 volume encryption conversion start 명령을 사용하여 기존 볼륨에서 암호화를 활성화합니다	4
기존 볼륨에 암호화를 설정합니다	5
볼륨 암호화 변환 시작 명령을 사용하여 기존 볼륨에서 암호화를 활성화합니다	5
볼륨 이동 시작 명령을 사용하여 기존 볼륨에서 암호화를 활성화합니다	7
SVM 루트 볼륨에 NetApp 볼륨 암호화를 구성합니다	9
노드 루트 볼륨 암호화를 설정합니다	10

NVE를 사용하여 볼륨 데이터 암호화

NVE 개요를 사용하여 볼륨 데이터 암호화

ONTAP 9.7부터는 VE 라이선스 및 온보드 키 또는 외부 키 관리 기능이 있는 경우 기본적으로 애그리게이트 및 볼륨 암호화가 활성화됩니다. ONTAP 9.6 이하 버전의 경우 새 볼륨 또는 기존 볼륨에서 암호화를 활성화할 수 있습니다. 볼륨 암호화를 활성화하려면 VE 라이선스를 설치하고 키 관리를 활성화해야 합니다. NVE는 FIPS-140-2 레벨 1을 준수합니다.

ONTAP에서 VE 라이선스를 사용하여 애그리게이트 수준 암호화를 활성화합니다

ONTAP 9.7부터 "VE 라이선스", 온보드 키 또는 외부 키 관리가 있는 경우 새로 생성된 애그리게이트와 볼륨은 기본적으로 암호화됩니다. ONTAP 9.6부터 애그리게이트 레벨 암호화를 사용하여 암호화할 볼륨에 포함된 애그리게이트에 키를 할당할 수 있습니다.

이 작업에 대해

인라인 또는 백그라운드 애그리게이트 레벨 중복제거를 수행하려는 경우 애그리게이트 레벨 암호화를 사용해야 합니다. 그 외에는 NVE에서 애그리게이트 레벨의 중복제거가 지원되지 않습니다.

애그리게이트 레벨 암호화를 위해 활성화된 애그리게이트를 *NAE aggregate*(NetApp 애그리게이트 암호화의 경우)라고 합니다. NAE 애그리게이트의 모든 볼륨은 NAE 또는 NVE 암호화로 암호화되어야 합니다. Aggregate 레벨의 암호화를 사용하면 Aggregate에서 생성한 볼륨이 NAE 암호화로 기본적으로 암호화됩니다. 대신 NVE 암호화를 사용하도록 기본값을 재정의할 수 있습니다.

NAE 애그리게이트에서는 일반 텍스트 볼륨이 지원되지 않습니다.

시작하기 전에

이 작업을 수행하려면 클러스터 관리자여야 합니다.

단계

1. 애그리게이트 레벨 암호화 활성화 또는 비활성화:

대상...	이 명령 사용...
ONTAP 9.7 이상을 사용하여 NAE 애그리게이트를 생성합니다	<code>storage aggregate create -aggregate aggregate_name -node node_name</code>
ONTAP 9.6으로 NAE 애그리게이트를 생성합니다	<code>storage aggregate create -aggregate aggregate_name -node node_name -encrypt-with -aggr-key true</code>
NAE가 아닌 집계로 NAE 집계를 변환합니다	<code>storage aggregate modify -aggregate aggregate_name -node node_name -encrypt-with -aggr-key true</code>

NAE 집계를 NAE가 아닌 집집합으로 변환합니다

```
storage aggregate modify -aggregate  
aggregate_name -node node_name -encrypt-with  
-aggr-key false
```

이 절차에서 설명하는 명령에 대한 자세한 내용은 ["ONTAP 명령 참조입니다"](#)참조하십시오.

다음 명령을 실행하면 "aggr1"에서 집계 수준 암호화가 활성화됩니다.

- ONTAP 9.7 이상:

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9.6 이하:

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with  
-aggr-key true
```

2. Aggregate가 암호화를 사용하도록 설정되어 있는지 확인합니다.

'스토리지 집계 표시 필드 암호화 - 집계 키 사용'

에 대한 자세한 내용은 `storage aggregate show` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

다음 명령을 실행하면 "aggr1"이 암호화에 대해 활성화되어 있는지 확인합니다.

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key  
aggregate          encrypt-aggr-key  
-----  
aggr0_vsim4        false  
aggr1               true  
2 entries were displayed.
```

작업을 마친 후

'volume create' 명령을 실행하여 암호화된 볼륨을 생성합니다.

KMIP 서버를 사용하여 노드의 암호화 키를 저장하는 경우, ONTAP는 볼륨을 암호화할 때 암호화 키를 서버에 자동으로 "푸시"(푸시)"합니다.

ONTAP에서 새 볼륨에 대해 암호화를 활성화합니다

'volume create' 명령을 사용하여 새 볼륨에서 암호화를 활성화할 수 있습니다.

이 작업에 대해

NVE(NetApp Volume Encryption)를 사용하여 볼륨을 암호화하고 ONTAP 9.6, NetApp Aggregate Encryption(NAE)로 시작할 수 있습니다. NAE와 NVE에 대한 자세한 내용은 [볼륨 암호화 개요](#).

이 절차에서 설명하는 명령에 대한 자세한 내용은 ["ONTAP 명령 참조입니다"](#)참조하십시오.

ONTAP에서 새 볼륨에 대한 암호화를 활성화하는 절차는 사용 중인 ONTAP 버전과 특정 구성에 따라 다릅니다.

- ONTAP 9.4부터 시작합니다(사용하는 경우) cc-mode Onboard Key Manager(온보드 키 관리자)를 설정할 때 로 생성한 볼륨입니다 volume create 명령은 사용자가 지정하든 관계없이 자동으로 암호화됩니다 -encrypt true.
- ONTAP 9.6 및 이전 버전에서는 을 사용해야 합니다 -encrypt true 와 함께 volume create 암호화를 활성화하는 명령(사용하지 않은 경우 cc-mode)를 클릭합니다.
- ONTAP 9.6에서 NAE 볼륨을 작성하려면 집계 수준에서 NAE를 활성화해야 합니다. 을 참조하십시오 [VE 라이선스로 애그리게이트 레벨 암호화를 설정합니다](#) 를 참조하십시오.
- ONTAP 9.7부터, "[VE 라이선스](#)"온보드 키 또는 외부 키 관리가 있는 경우 새로 생성된 볼륨이 기본적으로 암호화됩니다. 기본적으로 NAE 애그리게이트에서 생성된 새 볼륨은 NVE가 아닌 NAE 유형이 됩니다.
 - ONTAP 9.7 이상 릴리즈에서 추가하는 경우 -encrypt true 를 누릅니다 volume create NAE 애그리게이트에서 볼륨을 생성하는 명령은 볼륨에 NAE 대신 NVE 암호화가 있습니다. NAE 애그리게이트의 모든 볼륨은 NVE 또는 NAE로 암호화되어야 합니다.



NAE 애그리게이트에서는 일반 텍스트 볼륨이 지원되지 않습니다.

단계

1. 새 볼륨을 생성하고 볼륨에 암호화가 활성화되어 있는지 여부를 지정합니다. 새 볼륨이 NAE 애그리게이트에 있는 경우 기본적으로 볼륨은 다음 NAE 볼륨이 됩니다.

생성 방법...	이 명령 사용...
NAE 볼륨	<pre>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name</pre>
NVE 볼륨	<pre>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt true</pre> <p>를 누릅니다</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> <p>NAE가 지원되지 않는 ONTAP 9.6 및 이전 버전에서는 -encrypt true NVE를 사용하여 볼륨을 암호화하도록 지정합니다. NAE 애그리게이트에서 볼륨이 생성되는 ONTAP 9.7 이상에서는 -encrypt true 대신 NAE의 기본 암호화 유형을 재정의하여 NVE 볼륨을 생성합니다.</p> </div>
일반 텍스트 볼륨입니다	<pre>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt false</pre>

에 대한 자세한 내용은 volume create ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

2. 볼륨에 암호화가 설정되어 있는지 확인합니다.

볼륨 쇼는 암호화된 사실이다

에 대한 자세한 내용은 `volume show` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

결과

KMIP 서버를 사용하여 노드의 암호화 키를 저장하는 경우, ONTAP는 볼륨을 암호화할 때 암호화 키를 서버에 자동으로 "푸시" 합니다.

ONTAP에서 `volume encryption conversion start` 명령을 사용하여 기존 볼륨에서 암호화를 활성화합니다

ONTAP 9.3부터 볼륨을 다른 위치로 이동하지 않고도 "볼륨 암호화 변환 시작" 명령을 사용하여 기존 볼륨을 "제자리에" 암호화할 수 있습니다.

이 작업에 대해

변환 작업을 시작한 후에는 작업을 완료해야 합니다. 작업 중에 성능 문제가 발생하면 를 실행할 수 있습니다 `volume encryption conversion pause` 명령을 사용하여 작업을 일시 중지하고, 를 클릭합니다 `volume encryption conversion resume` 명령을 사용하여 작업을 재개합니다.

ONTAP 9.14.1부터 를 사용할 수 있습니다 `volume encryption conversion start` SVM 루트 볼륨에 대해 수행할 수 있습니다. 자세한 내용은 을 참조하십시오 [SVM 루트 볼륨에 NetApp 볼륨 암호화를 구성합니다](#).



를 사용할 수 없습니다 `volume encryption conversion start` SnapLock 볼륨을 변환합니다.

단계

1. 기존 볼륨에서 암호화 활성화:

```
volume encryption conversion start -vserver svm_name -volume volume_name
```

에 대한 자세한 내용은 `volume encryption conversion start` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

다음 명령을 실행하면 기존 볼륨의 암호화가 설정됩니다 `vol1`:

```
cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
```

시스템에서 볼륨에 대한 암호화 키를 생성합니다. 볼륨의 데이터가 암호화됩니다.

2. 변환 작업의 상태를 확인합니다.

볼륨 암호화 변환 표시

에 대한 자세한 내용은 `volume encryption conversion show` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

다음 명령을 실행하면 변환 작업의 상태가 표시됩니다.

```
cluster1::> volume encryption conversion show
```

Vserver	Volume	Start Time	Status
vs1	vol1	9/18/2017 17:51:41	Phase 2 of 2 is in progress.

3. 변환 작업이 완료되면 볼륨에 암호화가 활성화되어 있는지 확인합니다.

볼륨 쇼는 암호화된 사실이다

에 대한 자세한 내용은 `volume show -is-encrypted true` "ONTAP 명령 참조입니다"를 참조하십시오.

다음 명령을 실행하면 암호화된 볼륨이 'cluster1'에 표시됩니다.

```
cluster1::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
vs1	vol1	aggr2	online	RW	200GB	160.0GB	20%

결과

KMIP 서버를 사용하여 노드의 암호화 키를 저장하는 경우, 볼륨을 암호화할 때 ONTAP는 서버에 암호화 키를 자동으로 푸시합니다.

기존 볼륨에 암호화를 설정합니다

둘 중 하나를 사용할 수 있습니다 `volume move start` 또는 을 누릅니다 `volume encryption conversion start` 기존 볼륨에서 암호화를 활성화하는 명령입니다.

이 작업에 대해

당신은 사용할 수 있습니다 `volume encryption conversion start` 볼륨을 다른 위치로 이동하지 않고도 기존 볼륨의 암호화를 "현재 위치"에서 활성화하는 명령입니다. 또는 다음을 사용할 수 있습니다. `volume move start` 명령.

볼륨 암호화 변환 시작 명령을 사용하여 기존 볼륨에서 암호화를 활성화합니다

당신은 사용할 수 있습니다 `volume encryption conversion start` 볼륨을 다른 위치로 옮기지 않고도 기존 볼륨의 암호화를 "그대로" 활성화하는 명령입니다.

변환 작업을 시작한 후에는 작업을 완료해야 합니다. 작업 중에 성능 문제가 발생하면 를 실행할 수 있습니다 `volume encryption conversion pause` 명령을 사용하여 작업을 일시 중지하고, 를 클릭합니다 `volume encryption conversion resume` 명령을 사용하여 작업을 재개합니다.



를 사용할 수 없습니다 `volume encryption conversion start` SnapLock 볼륨을 변환합니다.

단계

1. 기존 볼륨에서 암호화 활성화:

'볼륨 암호화 변환 시작 - SVM_NAME - volume volume volume_name'

에 대한 자세한 내용은 `volume encryption conversion start` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 명령을 실행하면 기존 볼륨의 암호화가 설정됩니다 `vol1`:

```
cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
```

시스템에서 볼륨에 대한 암호화 키를 생성합니다. 볼륨의 데이터가 암호화됩니다.

2. 변환 작업의 상태를 확인합니다.

볼륨 암호화 변환 표시

에 대한 자세한 내용은 `volume encryption conversion show` "ONTAP 명령 참조입니다"을 참조하십시오.

다음 명령을 실행하면 변환 작업의 상태가 표시됩니다.

```
cluster1::> volume encryption conversion show
```

Vserver	Volume	Start Time	Status
vs1	vol1	9/18/2017 17:51:41	Phase 2 of 2 is in progress.

3. 변환 작업이 완료되면 볼륨이 암호화에 활성화되어 있는지 확인합니다.

볼륨 쇼는 암호화된 사실이다

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

다음 명령을 실행하면 암호화된 볼륨이 'cluster1'에 표시됩니다.

```
cluster1::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
vs1	vol1	aggr2	online	RW	200GB	160.0GB	20%

결과

KMIP 서버를 사용하여 노드의 암호화 키를 저장하는 경우, ONTAP는 볼륨을 암호화할 때 암호화 키를 서버에 자동으로

"푸시"(푸시)"합니다.

볼륨 이동 시작 명령을 사용하여 기존 볼륨에서 암호화를 활성화합니다

명령을 사용하여 기존 볼륨을 이동하여 암호화를 활성화할 수 `volume move start` 있습니다. 동일한 애그리게이트 또는 다른 애그리게이트를 사용할 수 있습니다.

이 작업에 대해

- ONTAP 9.8부터 볼륨 이동 시작을 사용하여 SnapLock 또는 FlexGroup 볼륨에서 암호화를 활성화할 수 있습니다.
- ONTAP 9.4부터 Onboard Key Manager를 설정할 때 ""cc-mode""를 활성화하면 "volume move start" 명령으로 생성한 볼륨이 자동으로 암호화됩니다. `-encrypt-destination true`는 지정하지 않아도 됩니다.
- ONTAP 9.6부터는 Aggregate 수준의 암호화를 사용하여 이동할 볼륨의 포함된 Aggregate에 키를 할당할 수 있습니다. 고유 키로 암호화된 볼륨을 `_NVE` 볼륨 `_` 이라고 합니다(NetApp 볼륨 암호화를 사용한다는 의미). 애그리게이트 레벨 키로 암호화된 볼륨을 `_NAE` 볼륨 `_` (NetApp 애그리게이트 암호화의 경우)이라고 합니다. NAE 애그리게이트에서는 일반 텍스트 볼륨이 지원되지 않습니다.
- ONTAP 9.14.1부터 NVE로 SVM 루트 볼륨을 암호화할 수 있습니다. 자세한 내용은 [을 참조하십시오 SVM 루트 볼륨에 NetApp 볼륨 암호화를 구성합니다.](#)

시작하기 전에

이 작업을 수행하려면 클러스터 관리자이거나 클러스터 관리자가 권한을 위임한 SVM 관리자여야 합니다.

"볼륨 이동 명령을 실행하는 위임 권한"

단계

1. 기존 볼륨을 이동하고 볼륨에 암호화가 활성화되어 있는지 여부를 지정합니다.

변환...	이 명령 사용...
NVE 볼륨에 대한 일반 텍스트 볼륨입니다	<code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination true</code>
NAE 볼륨에 대한 NVE 또는 일반 텍스트 볼륨(대상에 애그리게이트 레벨 암호화가 사용되는 것으로 가정)	<code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key true</code>
NVE 볼륨에 대한 NAE 볼륨	<code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key false</code>
Nae 볼륨을 일반 텍스트 볼륨으로	<code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false -encrypt-with-aggr-key false</code>

NVE 볼륨을 일반 텍스트 볼륨으로

```
volume move start -vserver SVM_name -volume  
volume_name -destination-aggregate aggregate_name  
-encrypt-destination false
```

에 대한 자세한 내용은 `volume move start` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

다음 명령을 실행하면 이름이 vol1인 일반 텍스트 볼륨이 NVE 볼륨으로 변환됩니다.

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination  
-aggregate aggr2 -encrypt-destination true
```

대상에서 애그리게이트 레벨 암호화를 사용하도록 설정한 경우 다음 명령을 실행하면 NVE 볼륨이나 일반 텍스트 볼륨 vol1이 NAE 볼륨으로 변환됩니다.

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination  
-aggregate aggr2 -encrypt-with-aggr-key true
```

다음 명령을 실행하면 이름이 vol2인 NAE 볼륨이 NVE 볼륨으로 변환됩니다.

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination  
-aggregate aggr2 -encrypt-with-aggr-key false
```

다음 명령을 실행하면 이름이 vol2인 NAE 볼륨이 일반 텍스트 볼륨으로 변환됩니다.

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination  
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

다음 명령을 실행하면 이름이 vol2인 NVE 볼륨이 일반 텍스트 볼륨으로 변환됩니다.

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination  
-aggregate aggr2 -encrypt-destination false
```

2. 클러스터 볼륨의 암호화 유형을 확인합니다.

'볼륨 표시 필드 암호화 - 없음|볼륨|집계'를 입력합니다

암호화 유형 필드는 ONTAP 9.6 이상에서 사용할 수 있습니다.

에 대한 자세한 내용은 `volume show` "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

다음 명령을 실행하면 'cluster2'의 볼륨 암호화 유형이 표시됩니다.

```
cluster2::> volume show -fields encryption-type
```

```
vserver  volume  encryption-type
-----  -
vs1      vol11    none
vs2      vol12    volume
vs3      vol13    aggregate
```

3. 볼륨에 암호화가 설정되어 있는지 확인합니다.

볼륨 쇼는 암호화된 사실이다

에 대한 자세한 내용은 `volume show` ["ONTAP 명령 참조입니다"](#)을 참조하십시오.

다음 명령을 실행하면 암호화된 볼륨이 'cluster2'에 표시됩니다.

```
cluster2::> volume show -is-encrypted true
```

```
Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-----  -
vs1      vol11    aggr2      online  RW   200GB  160.0GB  20%
```

결과

KMIP 서버를 사용하여 노드의 암호화 키를 저장하는 경우, 볼륨을 암호화할 때 ONTAP는 서버에 암호화 키를 자동으로 푸시합니다.

SVM 루트 볼륨에 NetApp 볼륨 암호화를 구성합니다

ONTAP 9.14.1부터 스토리지 VM(SVM) 루트 볼륨에서 NetApp 볼륨 암호화(NVE)를 활성화할 수 있습니다. NVE에서는 루트 볼륨을 고유 키로 암호화하여 SVM의 보안을 강화합니다.

이 작업에 대해

SVM 루트 볼륨의 NVE는 SVM이 생성된 후에만 활성화할 수 있습니다.

시작하기 전에

- SVM 루트 볼륨은 NetApp 애그리게이트 암호화(NAE)로 암호화된 애그리게이트에 있어서는 안 됩니다.
- Onboard Key Manager 또는 외부 키 관리자를 사용하여 암호화를 활성화해야 합니다.
- ONTAP 9.14.1 이상을 실행해야 합니다.
- NVE로 암호화된 루트 볼륨이 포함된 SVM을 마이그레이션하려면 마이그레이션이 완료된 후 SVM 루트 볼륨을 일반 텍스트 볼륨으로 변환한 다음 SVM 루트 볼륨을 다시 암호화해야 합니다.
 - SVM 마이그레이션의 타겟 Aggregate에서 NAE를 사용하는 경우 루트 볼륨은 기본적으로 NAE를 상속합니다.
- SVM이 SVM 재해 복구 관계에 있는 경우:

- 미러링된 SVM의 암호화 설정은 대상에 복사되지 않습니다. 소스 또는 대상에서 NVE를 활성화한 경우 미러링된 SVM 루트 볼륨에서 NVE를 별도로 활성화해야 합니다.
- 타겟 클러스터의 모든 애그리게이트가 NAE를 사용하는 경우 SVM 루트 볼륨은 NAE를 사용합니다.

단계

ONTAP CLI 또는 System Manager를 사용하여 SVM 루트 볼륨에서 NVE를 활성화할 수 있습니다.

CLI를 참조하십시오

제자리에서 SVM 루트 볼륨에서 NVE를 사용하거나 애그리게이트 간에 볼륨을 이동하여 활성화할 수 있습니다.

루트 볼륨을 제자리에서 암호화합니다

1. 루트 볼륨을 암호화된 볼륨으로 변환:

```
volume encryption conversion start -vserver svm_name -volume volume
```

2. 암호화가 성공했는지 확인합니다. 를 클릭합니다 volume show -encryption-type volume NVE를 사용하는 모든 볼륨의 목록을 표시합니다.

SVM 루트 볼륨을 이동하여 암호화

1. 볼륨 이동 시작:

```
volume move start -vserver svm_name -volume volume -destination-aggregate aggregate -encrypt-with-aggr-key false -encrypt-destination true
```

에 대한 자세한 내용은 volume move "[ONTAP 명령 참조입니다](#)"을 참조하십시오.

2. 를 확인합니다 volume move 에서 작업이 성공했습니다 volume move show 명령. 를 클릭합니다 volume show -encryption-type volume NVE를 사용하는 모든 볼륨의 목록을 표시합니다.

시스템 관리자

1. 스토리지> 볼륨 으로 이동합니다.
2. 암호화할 SVM 루트 볼륨의 이름 옆에 있는 **Edit** 를 선택합니다  .
3. 저장소 및 최적화 제목 아래에서 암호화 활성화 를 선택합니다.
4. 저장을 선택합니다.

노드 루트 볼륨 암호화를 설정합니다

ONTAP 9.8부터 NetApp 볼륨 암호화를 사용하여 노드의 루트 볼륨을 보호할 수 있습니다.



이 작업에 대해

이 절차는 노드 루트 볼륨에 적용됩니다. SVM 루트 볼륨에는 적용되지 않습니다. SVM 루트 볼륨은 애그리게이트 레벨 암호화 및 [ONTAP 9.14.1부터 NVE](#).

루트 볼륨 암호화가 시작되면 완료해야 합니다. 작업을 일시 중지할 수 없습니다. 암호화가 완료되면 루트 볼륨에 새 키를 할당할 수 없으며 보안 제거 작업을 수행할 수 없습니다.

시작하기 전에

- 시스템에서 HA 구성을 사용해야 합니다.
- 노드 루트 볼륨이 이미 생성되어 있어야 합니다.
- KMIP(Key Management Interoperability Protocol)를 사용하여 시스템에 온보드 키 관리자 또는 외부 키 관리 서버가 있어야 합니다.

단계

1. 루트 볼륨 암호화:

```
volume encryption conversion start -vserver SVM_name -volume root_vol_name
```

2. 변환 작업의 상태를 확인합니다.

볼륨 암호화 변환 표시

3. 변환 작업이 완료되면 볼륨이 암호화되었는지 확인합니다.

'볼륨 표시 필드'

다음은 암호화된 볼륨에 대한 출력 예입니다.

```
::> volume show -vserver xyz -volume vol0 -fields is-encrypted
vserver      volume is-encrypted
-----
xyz          vol0    true
```

저작권 정보

Copyright © 2025 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.