



6단계. 업그레이드를 완료합니다

Upgrade controllers

NetApp
July 05, 2024

목차

6단계. 업그레이드를 완료합니다	1
6단계 개요	1
KMIP 서버를 사용하여 인증 관리	1
새 컨트롤러가 올바르게 설정되었는지 확인합니다	1
새 컨트롤러 모듈에서 스토리지 암호화를 설정합니다	4
새 컨트롤러 모듈에 NetApp 볼륨 또는 애그리게이트 암호화를 설정합니다	5
기존 시스템을 폐기합니다	7
SnapMirror 작업을 재개합니다	7

6단계. 업그레이드를 완료합니다

6단계 개요

6단계 동안 새 노드가 올바르게 설정되었는지 확인하고, 새 노드가 암호화를 사용하도록 설정된 경우 스토리지 암호화 또는 NetApp 볼륨 암호화를 구성하고 설정합니다. 또한 이전 노드의 사용을 중지하고 SnapMirror 작업을 다시 시작해야 합니다.

단계

1. "KMIP 서버를 사용하여 인증 관리"
2. "새 컨트롤러가 올바르게 설정되었는지 확인합니다"
3. "새 컨트롤러 모듈에서 스토리지 암호화를 설정합니다"
4. "새 컨트롤러 모듈에 NetApp 볼륨 또는 애그리게이트 암호화를 설정합니다"
5. "기존 시스템을 폐기합니다"
6. "SnapMirror 작업을 재개합니다"

KMIP 서버를 사용하여 인증 관리

KMIP(Key Management Interoperability Protocol) 서버를 사용하여 인증 키를 관리할 수 있습니다.

단계

1. 새 컨트롤러 추가:

```
security key-manager external enable
```

2. 키 관리자 추가:

```
security key-manager external add-servers -key-servers  
key_management_server_ip_address
```

3. 키 관리 서버가 구성되어 있고 클러스터의 모든 노드에서 사용할 수 있는지 확인합니다.

```
security key-manager external show-status
```

4. 연결된 모든 키 관리 서버에서 새 노드로 인증 키를 복원합니다.

```
security key-manager external restore -node new_controller_name
```

새 컨트롤러가 올바르게 설정되었는지 확인합니다

올바른 설정을 확인하려면 HA 쌍을 활성화해야 합니다. 또한 노드 3과 노드 4가 서로의 스토리지에 액세스할 수 있고 클러스터의 다른 노드에 속하는 데이터 LIF가 소유하지 않는지 확인해야 합니다. 또한 노드 3이 노드 1의 애그리게이트를 소유하고 있고 노드 4가 노드 2의

애그리게이트를 소유하고 있으며, 두 노드의 볼륨이 온라인 상태인지 확인해야 합니다.

단계

1. 노드 2의 사후 검사를 수행한 후 노드 2 클러스터에 대한 스토리지 페일오버 및 클러스터 HA 쌍이 설정됩니다. 작업이 완료되면 두 노드가 완료된 것으로 표시되고 시스템에서 일부 정리 작업을 수행합니다.
2. 스토리지 페일오버가 설정되었는지 확인합니다.

```
storage failover show
```

다음 예에서는 스토리지 페일오버가 설정된 경우의 명령 출력을 보여 줍니다.

```
cluster::> storage failover show
                                Takeover
Node      Partner  Possible  State Description
-----  -
node3     node4    true      Connected to node4
node4     node3    true      Connected to node3
```

3. 다음 명령을 사용하여 출력을 검사하여 node3과 node4가 같은 클러스터에 속해 있는지 확인합니다.

```
cluster show
```

4. 다음 명령을 사용하여 출력을 검사하여 node3과 node4가 서로의 스토리지에 액세스할 수 있는지 확인합니다.

```
storage failover show -fields local-missing-disks, partner-missing-disks
```

5. 다음 명령을 사용하여 노드 3과 노드 4에서 클러스터의 다른 노드가 소유한 데이터 LIF를 확인하고 출력을 확인합니다.

```
network interface show
```

노드 3이나 노드 4에서 클러스터의 다른 노드가 소유한 데이터 LIF가 홈 소유자에게 있는 경우 데이터 LIF를 다음과 같이 되돌립니다.

```
network interface revert
```

6. 노드 3이 노드 1의 애그리게이트를 소유하고 있고 노드 4가 노드 2의 애그리게이트를 소유하고 있는지 확인합니다.

```
storage aggregate show -owner-name <node3>
```

```
storage aggregate show -owner-name <node4>
```

7. 볼륨이 오프라인 상태인지 확인합니다.

```
volume show -node <node3> -state offline
```

```
volume show -node <node4> -state offline
```

8. 오프라인 상태인 볼륨이 있으면 섹션에서 캡처한 오프라인 볼륨 목록과 비교합니다 **업그레이드할 노드를**

"준비합니다"을 사용하여 각 볼륨에 대해 다음 명령을 사용하여 필요에 따라 오프라인 볼륨을 온라인으로 전환합니다.

```
volume online -vserver <vserver_name> -volume <volume_name>
```

9. 각 노드에 대해 다음 명령을 사용하여 새 노드에 대한 새 라이선스를 설치합니다.

```
system license add -license-code <license_code,license_code,license_code...>
```

license-code 매개변수는 28개의 대문자 알파벳 문자 키 목록을 허용합니다. 한 번에 하나의 라이선스를 추가하거나 한 번에 여러 라이선스를 추가하여 각 라이선스 키를 심표로 분리할 수 있습니다.

10. 다음 명령 중 하나를 사용하여 원래 노드에서 이전 라이선스를 모두 제거합니다.

```
system license clean-up -unused -expired
```

```
system license delete -serial-number <node_serial_number> -package <licensable_package>
```

- 만료된 모든 라이선스 삭제:

```
system license clean-up -expired
```

- 사용하지 않는 모든 라이선스 삭제:

```
system license clean-up -unused
```

- 노드에서 다음 명령을 사용하여 클러스터에서 특정 라이선스를 삭제합니다.

```
system license delete -serial-number <node1_serial_number> -package *
```

```
system license delete -serial-number <node2_serial_number> -package *
```

다음 출력이 표시됩니다.

```
Warning: The following licenses will be removed:
<list of each installed package>
Do you want to continue? {y|n}: y
```

를 입력합니다 y 모든 패키지를 제거합니다.

11. 다음 명령을 사용하여 출력을 검사하여 라이선스가 올바르게 설치되었는지 확인합니다.

```
system license show
```

출력을 섹션에서 캡처한 출력과 비교할 수 있습니다 "**업그레이드할 노드를 준비합니다**".

12. 자체 암호화 드라이브가 구성에 사용되고 있고 변수를 (예: 의) 로 설정한 경우 `kmip.init.maxwait off` "**노드 4, 24단계를 설치 및 부팅합니다**" 변수를 설정 해제해야 합니다.

```
set diag; systemshell -node <node_name> -command sudo kenv -u -p
kmp.init.maxwait
```

13. [[13단계] 두 노드에서 다음 명령을 사용하여 SP를 구성합니다.

```
system service-processor network modify -node <node_name>
```

을 참조하십시오 ["참조"](#) SP 및 _ONTAP 9.8 명령에 대한 자세한 내용은 [_시스템 관리 참조_](#)에 대한 링크를 참조하십시오. 시스템에 대한 자세한 내용은 [수동 페이지 참조_](#)를 참조하십시오 `service-processor network modify` 명령.

14. 새 노드에서 스위치가 없는 클러스터를 설정하려면 [을 참조하십시오 "참조" _NetApp Support 사이트_](#)에 연결하고 스위치가 없는 2노드 클러스터로 전환 [_](#)의 지침을 따르십시오.

작업을 마친 후

노드 3과 노드 4에서 스토리지 암호화가 설정된 경우 섹션을 완료합니다 ["새 컨트롤러 모듈에서 스토리지 암호화를 설정합니다"](#). 그렇지 않으면 섹션을 완료합니다 ["기존 시스템을 폐기합니다"](#).

새 컨트롤러 모듈에서 스토리지 암호화를 설정합니다

교체된 컨트롤러 또는 새 컨트롤러의 HA 파트너가 Storage Encryption을 사용하는 경우, SSL 인증서 설치 및 키 관리 서버 설정을 포함하여 Storage Encryption에 대한 새 컨트롤러 모듈을 구성해야 합니다.

이 작업에 대해

이 절차에는 새 컨트롤러 모듈에서 수행되는 단계가 포함됩니다. 올바른 노드에 명령을 입력해야 합니다.

단계

1. 키 관리 서버를 계속 사용할 수 있는지, 해당 상태 및 인증 키 정보를 확인합니다.

```
security key-manager external show-status
```

```
security key-manager onboard show-backup
```

2. 이전 단계에 나열된 키 관리 서버를 새 컨트롤러의 키 관리 서버 목록에 추가합니다.

- a. 키 관리 서버를 추가합니다.

```
security key-manager external add-servers -key-servers
key_management_server_ip_address
```

- b. 나열된 각 키 관리 서버에 대해 이전 단계를 반복합니다. 최대 4개의 키 관리 서버를 연결할 수 있습니다.

- c. 키 관리 서버가 성공적으로 추가되었는지 확인합니다.

```
security key-manager external show
```

3. 새 컨트롤러 모듈에서 키 관리 설정 마법사를 실행하여 키 관리 서버를 설정하고 설치합니다.

기존 컨트롤러 모듈에 설치된 것과 동일한 키 관리 서버를 설치해야 합니다.

a. 새 노드에서 키 관리 서버 설정 마법사를 시작합니다.

```
security key-manager external enable
```

b. 마법사의 단계를 완료하여 키 관리 서버를 구성합니다.

4. 연결된 모든 키 관리 서버에서 새 노드로 인증 키 복원:

```
security key-manager external restore -node new_controller_name
```

새 컨트롤러 모듈에 **NetApp** 볼륨 또는 애그리게이트 암호화를 설정합니다

새 컨트롤러의 교체된 컨트롤러 또는 고가용성(HA) 파트너가 NetApp Volume Encryption(NVE) 또는 NetApp Aggregate Encryption(NAE)을 사용하는 경우, NVE 또는 NAE에 새 컨트롤러 모듈을 구성해야 합니다.

이 작업에 대해

이 절차에는 새 컨트롤러 모듈에서 수행되는 단계가 포함됩니다. 올바른 노드에 명령을 입력해야 합니다.

Onboard Key Manager(온보드 키 관리자)

Onboard Key Manager를 사용하여 NVE 또는 NAE를 구성합니다.

단계

1. 연결된 모든 키 관리 서버에서 새 노드로 인증 키 복원:

```
security key-manager onboard sync
```

외부 키 관리

External Key Management를 사용하여 NVE 또는 NAE를 구성합니다.

단계

1. 키 관리 서버를 계속 사용할 수 있는지, 해당 상태 및 인증 키 정보를 확인합니다.

```
security key-manager key query -node node
```

2. 이전 단계에 나열된 키 관리 서버를 새 컨트롤러의 키 관리 서버 목록에 추가합니다.

- a. 키 관리 서버를 추가합니다.

```
security key-manager external add-servers -key-servers  
key_management_server_ip_address
```

- b. 나열된 각 키 관리 서버에 대해 이전 단계를 반복합니다. 최대 4개의 키 관리 서버를 연결할 수 있습니다.
- c. 키 관리 서버가 성공적으로 추가되었는지 확인합니다.

```
security key-manager external show
```

3. 새 컨트롤러 모듈에서 키 관리 설정 마법사를 실행하여 키 관리 서버를 설정하고 설치합니다.

기존 컨트롤러 모듈에 설치된 것과 동일한 키 관리 서버를 설치해야 합니다.

- a. 새 노드에서 키 관리 서버 설정 마법사를 시작합니다.

```
security key-manager external enable
```

- b. 마법사의 단계를 완료하여 키 관리 서버를 구성합니다.

4. 연결된 모든 키 관리 서버에서 새 노드로 인증 키 복원:

```
security key-manager external restore
```

이 명령을 실행하면 OKM 암호가 필요합니다

자세한 내용은 기술 자료 문서를 참조하십시오 ["ONTAP 부팅 메뉴에서 외부 키 관리자 서버 구성을 복원하는 방법"](#).

작업을 마친 후

인증 키를 사용할 수 없거나 EKM 서버에 연결할 수 없어 볼륨이 오프라인 상태가 되었는지 확인합니다. 를 사용하여

해당 볼륨을 다시 온라인 상태로 전환합니다 `volume online` 명령.

기존 시스템을 폐기합니다

업그레이드한 후 NetApp Support 사이트를 통해 기존 시스템의 사용을 중단할 수 있습니다. 시스템을 폐기하면 NetApp이 시스템이 더 이상 작동하지 않으며 지원 데이터베이스에서 제거된다는 것을 알려줍니다.

단계

1. 을 참조하십시오 "참조" 를 눌러 _NetApp Support 사이트_에 연결하고 로그인합니다.
2. 메뉴에서 * 제품 > 내 제품 * 을 선택합니다.
3. 설치된 시스템 보기 * 페이지에서 시스템에 대한 정보를 표시하는 데 사용할 * 선택 기준 * 을 선택합니다.

다음 중 하나를 선택하여 시스템을 찾을 수 있습니다.

- 일련 번호(장치 뒷면에 있음)
- 내 위치의 일련 번호입니다

4. Go! * 를 선택합니다

표에는 일련 번호를 포함한 클러스터 정보가 표시됩니다.

5. 테이블에서 클러스터를 찾고 제품 도구 세트 드롭다운 메뉴에서 * 이 시스템 사용 중지 * 를 선택합니다.

SnapMirror 작업을 재개합니다

업그레이드하기 전에 중지된 SnapMirror 전송을 다시 시작하고 SnapMirror 관계를 다시 시작할 수 있습니다. 업그레이드가 완료된 후 업데이트가 일정에 따라 진행되고 있습니다.

단계

1. 대상에서 SnapMirror 상태를 확인합니다.

```
snapmirror show
```

2. SnapMirror 관계 재개:

```
snapmirror resume -destination-vserver vserver_name
```

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.