Red Hat Virtualization 4.4

재해 복구 가이드

재해 복구를 위해 Red Hat Virtualization 4.4 구성

Last Updated: 2022-06-26

Red Hat Virtualization 4.4 재해 복구 가이드

재해 복구를 위해 Red Hat Virtualization 4.4 구성

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

법적 공지

초록

재해 발생 시에도 환경이 계속 작동하도록 Red Hat Virtualization을 구성할 수 있습니다. 이 문서에서는 재해 복구를 위한 Red Hat Virtualization 환경을 구성하는 데 필요한 정보와 지침을 제공합니다.

차례

1장. 재해 복구 솔루션

Red Hat Virtualization은 사이트 중단 시 환경을 복구할 수 있도록 두 가지 유형의 재해 복구 솔루션을 지원합니다. 두 솔루션 모두 두 사이트를 지원하며 둘 다 복제 스토리지가 필요합니다.

Active-Active 재해 복구

이 솔루션은 확장 클러스터 구성을 사용하여 구현됩니다. 즉, 기본 및 보조 사이트에서 필요한 가상 시스템을 실행할 수 있는 호스트가 포함된 클러스터의 단일 RHV 환경이 있습니다. 가상 머신은 중단이 발생하는 경우 보조 사이트의 호스트로 자동으로 마이그레이션됩니다. 그러나 환경은 대기 시간 및 네트워킹 요구 사항을 충족해야 합니다. 자세한 내용은 Active-Active Overview 를 참조하십시오.

active-Passive 재해 복구

사이트 간 장애 조치라고도 하는 이 재해 복구 솔루션은 활성 기본 환경 및 패시브 보조 환경(백업) 환경의 두 가지 별도의 RHV 환경을 구성하여 구현됩니다. 사이트 간 페일오버 및 장애 조치(failback)는 수동으로 실행해야 하며 Ansible에서 관리합니다. 자세한 내용은 Active-Passive 개요 를 참조하십시오.

2장. ACTIVE-ACTIVE 재해 복구

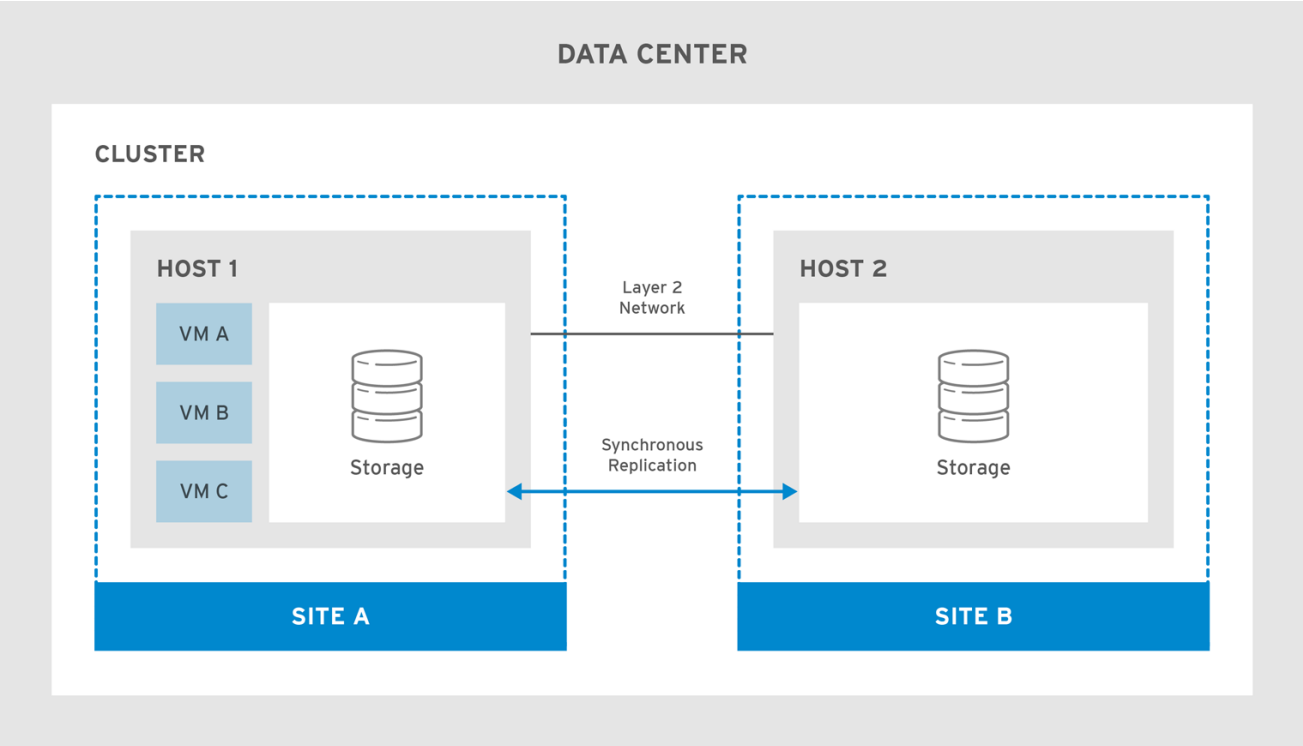
2.1. ACTIVE-ACTIVE 개요

액티브-액티브 재해 복구 장애 조치 구성은 두 개의 사이트에 걸쳐 있을 수 있습니다. 두 사이트 모두 활성화되어 있으며 기본 사이트를 사용할 수 없게 되면 Red Hat Virtualization 환경이 보조 사이트에서 계속 운영되어 비즈니스 연속성을 보장합니다.

액티브-액티브 장애 조치 구성에는 가상 시스템을 실행할 수 있는 호스트가 기본 사이트 및 보조 사이트 둘 다에 있는 확장 클러스터가 포함됩니다. 모든 호스트가 동일한 Red Hat Virtualization 클러스터에 속합니다.

이 구성을 사용하려면 두 사이트에서 쓰기 가능한 복제 스토리지가 필요하므로 가상 시스템이 두 사이트 간에 마이그레이션되고 두 사이트의 스토리지 모두에서 계속 실행될 수 있습니다.

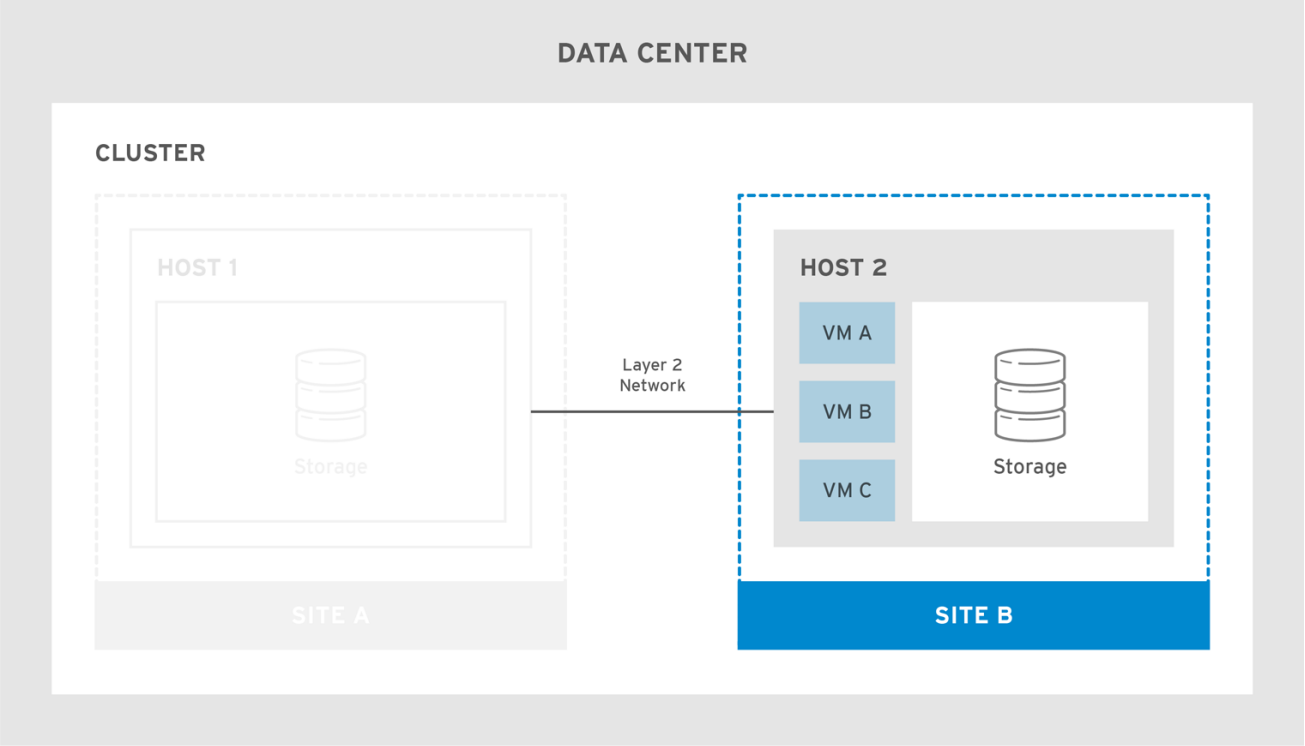
그림 2.1. 클러스터 설정 확장



RHV_460251_1017

기본 사이트를 사용할 수 없게 되면 가상 머신을 보조 사이트로 마이그레이션합니다. 사이트를 사용할 수 있게 되고 두 사이트 모두에서 스토리지가 복제되면 가상 머신은 기본 사이트로 자동으로 장애 복구됩니다.

그림 2.2. 실패한 Stretch 클러스터



중요

가상 머신 장애 조치 및 장애 조치(failback)가 작동하는지 확인하려면 다음을 수행합니다.

- 가상 시스템은 고가용성이 되도록 구성해야 하며, 각 가상 시스템에는 전원 관리 없이도 가상 시스템을 시작할 수 있도록 대상 스토리지 도메인에 리스가 있어야 합니다.
- 가상 시스템이 선택한 호스트에서만 시작되도록 소프트 적용 가상 시스템을 호스트 선호도에 구성해야 합니다.

자세한 내용은 가상 머신 *관리 가이드에서 가상 머신 고가용성으로 가동 시간 향상* 및 *선호도 그룹을 참조하십시오.*

확장형 클러스터 구성은 자체 호스팅 엔진 환경 또는 독립 실행형 관리자 환경을 사용하여 구현할 수 있습니다. 다양한 유형의 배포에 대한 자세한 내용은 *제품 가이드에서 Red Hat Virtualization Architecture 를 참조하십시오.*

2.2. 네트워크 고려 사항

클러스터의 모든 호스트는 L2 네트워크를 통해 동일한 브로드캐스트 도메인에 있어야 합니다. 따라서 두 사이트 간의 연결은 L2여야 합니다.

L2 네트워크의 사이트 간 최대 대기 시간 요구 사항은 두 설정에 따라 다릅니다. 독립 실행형 Manager 환경에는 최대 대기 시간이 100ms인 반면 셀프 호스트 엔진 환경에는 최대 7ms의 대기 시간이 필요합니다.

2.3. 스토리지 고려 사항

Red Hat Virtualization의 스토리지 도메인은 블록 장치(SAN, iSCSI 또는 FCP) 또는 파일 시스템(NAS - NFS, GlusterFS 또는 기타 POSIX 호환 파일 시스템)을 구성할 수 있습니다. Red Hat Virtualization 스토리지에 대한 자세한 내용은 *관리 가이드 의 스토리지를 참조하십시오*.

참고

GlusterFS 스토리지는 더 이상 사용되지 않으며 향후 릴리스에서 더 이상 지원되지 않습니다.

사이트에는 L2(공유 계층 2) 네트워크 연결이 있는 두 사이트에서 쓰기 가능한 동기 복제 스토리지가 필요합니다. 복제된 스토리지는 가상 시스템이 사이트 간에 마이그레이션하고 사이트의 스토리지에서 계속 실행되도록 하려면 필요합니다. Red Hat Enterprise Linux 7 이상에서 지원하는 모든 스토리지 복제 옵션을 확장 클러스터에서 사용할 수 있습니다.

중요

스토리지 벤더에서 권장하는 사용자 지정 다중 경로 구성이 있는 경우 SAN 벤더에 대한 다중 경로 구성 사용자 정의의 지침 및 중요한 제한 사항을 참조하십시오.

우선 순위를 가지도록 기본 사이트에 있는 호스트에서 SPM 역할을 설정합니다. 이 작업을 수행하려면 보조 사이트 호스트에서 SPM 우선 순위를 높은 수준으로 구성하고 SPM 우선 순위를 변경합니다. 기본 사이트 내의 네트워크 장치에 영향을 주는 기본 사이트 오류가 있는 경우, SPM 호스트의 펜싱 장치가 전원 손실과 같이 연결할 수 없게 되면 두 번째 사이트 내의 호스트가 SPM 역할을 넘겨받을 수 없습니다.

이러한 시나리오에서는 가상 시스템이 페일오버를 수행하지만, SPM 역할이 필요한 작업을 제 위치에 추가할 수 없으며, 새 디스크 추가, 기존 디스크 확장, 가상 시스템 내보내기 등의 작업을 실행할 수 없습니다.

전체 기능을 복원하려면 재해의 실제 특성을 감지하고 근본 원인을 수정하고 SPM 호스트를 재부팅한 후 SPM 호스트에 **대해 Confirm 'Host has been Rebooted**(다시 부팅 확인)를 선택합니다.

추가 리소스

관리 가이드에서 수동으로 무응답 호스트 분리 또는 격리 .

2.4. 자체 호스팅 엔진 STRETCH 클러스터 환경 구성

이 절차에서는 자체 호스팅 엔진 배포를 사용하여 확장 클러스터를 구성하는 방법을 설명합니다.

사전 요구 사항

- L2 네트워크 연결이 있는 두 사이트 모두에서 쓰기 가능한 스토리지 서버.
- 스토리지 복제를 위한 실시간 스토리지 복제 서비스.

제한

- 사이트 간 최대 7ms 대기 시간.

셀프 호스트 엔진 Stretch 클러스터 구성

1. 셀프 호스트 엔진 배포. 명령줄을 사용하여 자체 호스팅 엔진으로 Red Hat Virtualization 설치를 참조하십시오.

2. 각 사이트에 셀프 호스트 엔진 노드를 추가로 설치하고 클러스터에 추가합니다. *명령줄을 사용하여 Red Hat Virtualization을 자체 호스팅 엔진 엔진으로 설치할 때 Red Hat Virtualization Manager에 자체 호스팅 엔진 노드 추가*를 참조하십시오.

3. 선택적으로 추가 표준 호스트를 설치합니다. *명령줄 을 사용하여 Red Hat Virtualization을 자체 호스팅 엔진으로 설치할 때 Red Hat Virtualization Manager에 표준 호스트 추가*를 참조하십시오.

1. 보조 사이트에 있는 모든 호스트에서 SPM 우선 순위를 더 높게 구성하여 기본 사이트의 모든 호스트를 사용할 수 없는 경우에만 SPM이 발생하도록 합니다. *관리 가이드의 SPM 우선 순위를 참조하십시오.*

2. 고가용성으로 장애 조치해야 하는 모든 가상 시스템을 구성하고, 가상 시스템의 대상 스토리지 도메인에 임대가 있는지 확인합니다. 가상 머신 *관리 가이드에서 고가용성 가상 머신 구성 을 참조하십시오*.

3. 소프트 선호도를 호스팅하고 선호도 그룹에서 예상되는 동작을 정의하도록 가상 시스템을 구성합니다. 관리 가이드에서 *가상 머신 관리 가이드* 및 스케줄링 정책 의 유사성 그룹을 *참조하십시오.*

액티브-액티브 장애 조치는 기본 사이트의 호스트를 유지 관리 모드로 전환하여 수동으로 수행할 수 있습니다.

2.5. 독립 실행형 관리자 STRETCH 클러스터 환경 구성

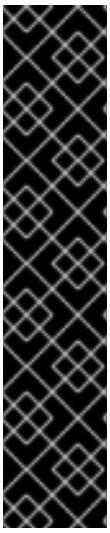
이 절차에서는 독립 실행형 관리자 배포를 사용하여 확장 클러스터를 구성하는 방법을 설명합니다.

사전 요구 사항

- L2 네트워크 연결이 있는 두 사이트 모두에서 쓰기 가능한 스토리지 서버.
- 스토리지 복제를 위한 실시간 스토리지 복제 서비스.

제한

- 사이트 간 최대 100ms 대기 시간.



중요

가상 머신은 사이트 간 장애 조치(failover) 및 장애 복구가 가능해야 합니다. 관리자로 관리자가 다운되면 가상 머신은 장애 조치(failover)되지 않습니다.

독립 실행형 관리자는 외부적으로 관리되는 경우에만 고가용성입니다. 예를 들면 다음과 같습니다.

- Red Hat의 고가용성 애드온 사용.
- 별도의 가상화 환경에서 고가용성 가상 시스템으로 사용.
- Red Hat Enterprise Linux Cluster Suite 사용.
- 배포할 수 있습니다.

절차

1. Red Hat Virtualization Manager 설치 및 구성. *로컬 데이터베이스가 있는 독립 실행형 관리자로 Red Hat Virtualization 설치를 참조하십시오*.

2. 각 사이트에 호스트를 설치하고 클러스터에 추가합니다. *로컬 데이터베이스가 있는 독립 실행형 관리자로 Red Hat Virtualization 설치에서 Red Hat Virtualization용 호스트 설치를 참조하십시오.*

1. 보조 사이트에 있는 모든 호스트에서 SPM 우선 순위를 더 높게 구성하여 기본 사이트의 모든 호스트를 사용할 수 없는 경우에만 SPM이 발생하도록 합니다. *관리 가이드의 SPM 우선 순위를 참조하십시오.*

2. 고가용성으로 장애 조치해야 하는 모든 가상 시스템을 구성하고, 가상 시스템의 대상 스토리지 도메인에 임대가 있는지 확인합니다. 가상 머신 *관리 가이드에서 고가용성 가상 머신 구성* 을 참조하십시오.

3. 소프트 선호도를 호스팅하고 선호도 그룹에서 예상되는 동작을 정의하도록 가상 시스템을 구성합니다. 관리 가이드에서 *가상 머신 관리 가이드* 및 스케줄링 정책 의 유사성 그룹을 *참조하십시오.*

액티브-액티브 장애 조치는 기본 사이트의 호스트를 유지 관리 모드로 전환하여 수동으로 수행할 수 있습니다.

3장. ACTIVE-PASSIVE 재해 복구

3.1. 액티브-패시브 개요

Red Hat Virtualization은 두 사이트를 포괄할 수 있는 액티브-패시브 재해 복구 솔루션을 지원합니다. 기본 사이트를 사용할 수 없게 되면 Red Hat Virtualization 환경에서 보조 사이트(백업) 사이트로 장애 조치해야 할 수 있습니다.

장애 조치는 다음과 같은 보조 사이트에서 Red Hat Virtualization 환경을 구성하여 수행할 수 있습니다.

- 활성 Red Hat Virtualization Manager.
- 데이터 센터 및 클러스터.
- 기본 사이트와 동일한 일반 연결이 있는 네트워크.
- 장애 조치 후 중요한 가상 시스템을 실행할 수 있는 활성 호스트.

중요

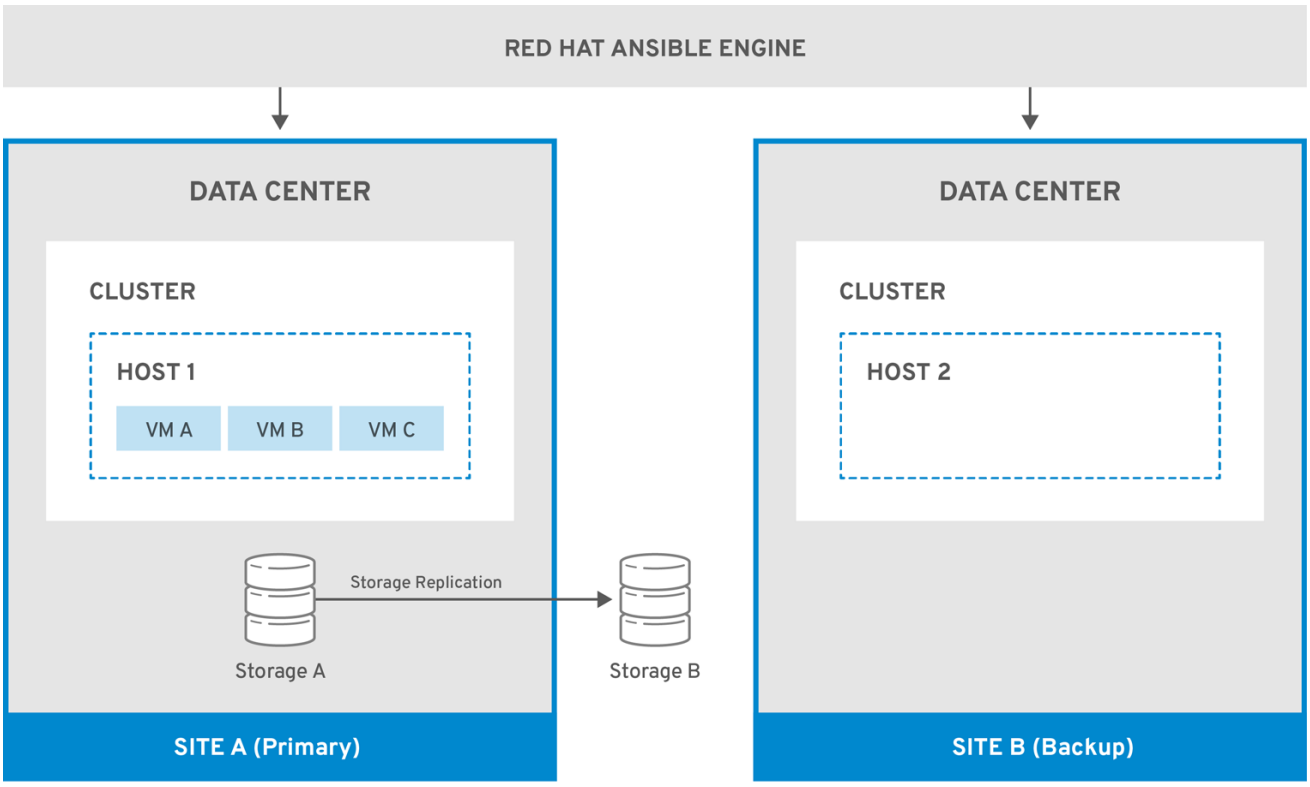
보조 환경에 가상 시스템에서 장애가 발생한 를 실행할 수 있는 충분한 리소스가 있는지, 기본 및 보조 환경에 동일한 Manager 버전, 데이터 센터 및 클러스터 호환성 수준, PostgreSQL 버전이 있는지 확인해야 합니다. 지원되는 최소 호환성 수준은 4.2입니다.

기본 사이트에 가상 머신 디스크와 템플릿이 포함된 스토리지 도메인을 복제해야 합니다. 이러한 복제된 스토리지 도메인은 보조 사이트에 연결할 수 없습니다.

장애 조치 및 장애 조치(failback) 프로세스를 수동으로 실행해야 합니다. 이렇게 하려면 사이트 간에 엔터티를 매핑하고 장애 조치(failover) 및 장애 조치(failback) 프로세스를 관리하는 Ansible 플레이북을 생성해야 합니다. 매핑 파일은 Red Hat Virtualization 구성 요소에 장애 조치(failover) 또는 대상 사이트에서 다시 실패한 Red Hat Virtualization 구성 요소를 지시합니다.

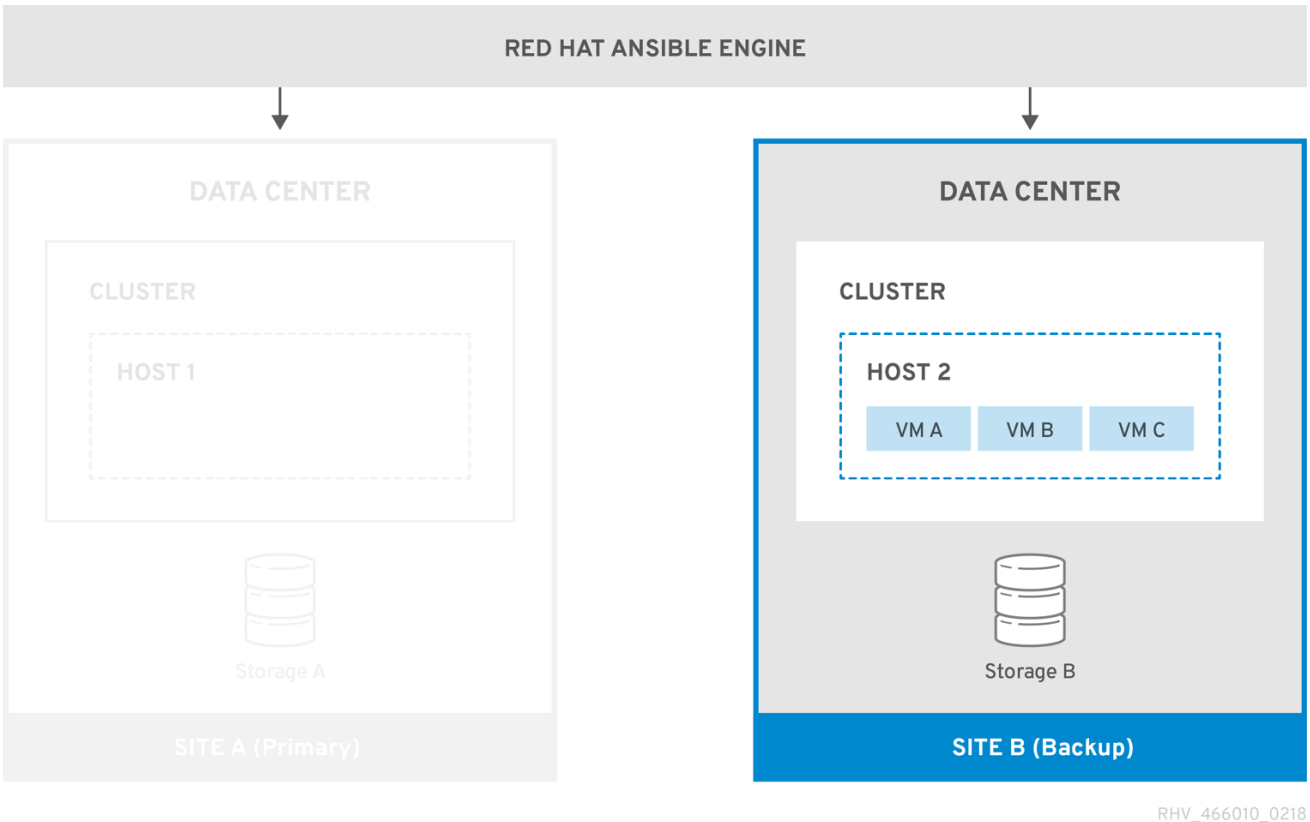
다음 다이어그램에서는 Red Hat Ansible Engine을 실행하는 시스템이 고가용성이며 **oVirt.disaster-recovery Ansible 역할, 구성된 플레이북 및 매핑 파일에 액세스할 수 있는 액티브-** 패시브 설정을 설명합니다. Site A에 가상 머신 디스크를 저장하는 스토리지 도메인이 복제됩니다. 사이트 B에는 가상 머신이나 연결된 스토리지 도메인이 없습니다.

그림 3.1. 액티브-패시브 구성



환경이 Site B로 실패하면 스토리지 도메인이 Site B의 데이터 센터에서 먼저 연결 및 활성화되고 가상 머신이 등록됩니다. 고가용성 가상 시스템은 먼저 페일오버됩니다.

그림 3.2. 백업 사이트로 장애 조치



다시 실행되는 경우 기본 사이트(A)로 다시 실패해야 합니다.

3.2. 네트워크 고려 사항

기본 사이트 및 보조 사이트에 동일한 일반 연결이 있는지 확인해야 합니다.

여러 네트워크 또는 여러 데이터 센터가 있는 경우 매핑 파일에 빈 네트워크 매핑을 사용하여 장애 조치 중 모든 엔터티가 대상에 등록하도록 해야 합니다. 자세한 내용은 파일 속성 매핑 을 참조하십시오.

3.3. 스토리지 고려 사항

Red Hat Virtualization의 스토리지 도메인은 블록 장치(SAN, iSCSI 또는 FCP) 또는 파일 시스템(NAS - NFS, GlusterFS 또는 기타 POSIX 호환 파일 시스템)을 구성할 수 있습니다. Red Hat Virtualization 스토리지에 대한 자세한 내용은 *관리 가이드 의 스토리지를 참조하십시오*.

참고

GlusterFS 스토리지는 더 이상 사용되지 않으며 향후 릴리스에서 더 이상 지원되지 않습니다.

중요

재해 복구를 위해 로컬 스토리지 도메인이 지원되지 않습니다.

기본 및 보조 스토리지 복제본이 필요합니다. 가상 시스템 디스크 또는 템플릿이 포함된 기본 스토리지 도메인의 블록 장치 또는 공유는 복제해야 합니다. 보조 스토리지는 데이터 센터에 연결할 수 없으며 장애 조치 중에 백업 사이트의 데이터 센터에 추가됩니다.

자체 호스팅 엔진을 사용하여 재해 복구를 구현하는 경우 스토리지 도메인이 실패하지 않으므로 Manager 가상 시스템에서 사용하는 스토리지 도메인에 가상 시스템 디스크가 포함되지 않도록 합니다.

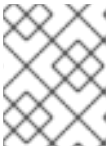
Red Hat Enterprise Linux 7 이상에서 지원하는 복제 옵션이 있는 모든 스토리지 솔루션을 사용할 수 있습니다.

3.4. 필요한 ANSIBLE 플레이북 생성

Ansible은 재해 복구 장애 조치 및 장애 복구 장애 조치(failback)를 시작하고 관리하는 데 사용됩니다. 이를 위해 Ansible 플레이북을 생성해야 합니다. Ansible 플레이북 생성에 대한 자세한 내용은 Ansible 설명서를 참조하십시오.

사전 요구 사항

- 기본 사이트에서 Red Hat Virtualization 환경 완벽하게 작동.
- 기본 환경과 동일한 데이터 센터 및 클러스터 호환성 수준이 있는 보조 사이트의 백업 환경. 백업 환경에는 다음이 있어야 합니다.
  - Red Hat Virtualization Manager.
  - 가상 시스템을 실행하고 복제된 스토리지 도메인에 연결할 수 있는 활성 호스트입니다.
  - 클러스터가 있는 데이터 센터.
  - 기본 사이트와 동일한 일반 연결이 있는 네트워크.
- 복제 스토리지. 자세한 내용은 스토리지 고려 사항을 참조하십시오.



참고

가상 머신 및 템플릿이 포함된 복제된 스토리지는 보조 사이트에 첨부해서는 안 됩니다.

- failover 및 failback을 자동화하는 고가용성 Red Hat Ansible Engine 시스템에 **oVirt.disaster-recovery** 패키지를 설치해야 합니다.
- Red Hat Ansible Engine을 실행하는 시스템은 SSH를 사용하여 기본 및 보조 사이트의 Manager에 연결할 수 있어야 합니다.

보조 사이트에서 선호도 그룹, 선호도 레이블, 사용자 등 기본 사이트에 있는 환경 속성을 생성하는 것도 좋습니다.

참고

Ansible 플레이북의 기본 동작은 **/usr/share/ansible/roles/oVirt.disaster-recovery/defaults/main.yml** 파일에서 구성할 수 있습니다.

다음 플레이북을 생성해야 합니다.

- 파일을 만들어 기본 및 보조 사이트에 엔터티를 매핑하는 플레이북입니다.
- 페일오버 플레이북.
- failback 플레이북입니다.

또한 실패하기 전에 기본 사이트를 정리하는 선택적 플레이북을 만들 수 있습니다.

장애 조치 및 장애 조치를 관리하는 Ansible 시스템에서 **/usr/share/ansible/roles/oVirt.disaster-recovery/** 에서 플레이북 및 관련 파일을 생성합니다. 관리할 수 있는 여러 개의 Ansible 시스템이 있는 경우 파일을 모든 Ansible에 복사해야 합니다.

Active-Passive 구성 테스트에서 하나 이상의 테스트 절차를 사용하여 구성을 테스트할 수 있습니다.

3.4.1. Ansible 작업의 **ovirt-dr** 스크립트

ovirt-dr 스크립트는 다음 Ansible 작업을 간소화합니다.

- 장애 조치 및 폴백을 위한 기본 및 보조 사이트의 **var** 매핑 파일 생성
- **var** 매핑 파일 검증
- 대상 사이트에서 장애 조치 실행
- 대상 사이트에서 소스 사이트로의 failback 실행

이 스크립트는 **/usr/share/ansible/roles/oVirt.disaster-recovery/files**에 있습니다.

사용법

```
# ./ovirt-dr generate/validate/failover/failback
            [--conf-file=dr.conf]
            [--log-file=ovirt-dr-log_number.log]
            [--log-level=DEBUG/INFO/WARNING/ERROR]
```

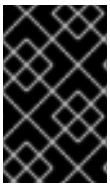
구성 파일 **/usr/share/ansible/roles/oVirt.disaster-recovery/files/dr.conf** 에서 스크립트 작업의 매개변수를 설정할 수 있습니다.

--conf-file 옵션을 사용하여 구성 파일의 위치를 변경할 수 있습니다.

--log-file 및 --log- level 옵션을 사용하여 로깅 세부 정보의 위치 및 수준을 설정할 수 있습니다.

3.4.2. 매핑 파일 생성을 위한 플레이북 생성

매핑 파일을 생성하는 데 사용되는 Ansible 플레이북은 타겟(기본) 사이트의 엔터티로 파일을 미리 채웁니다. 그런 다음 IP 주소, 클러스터, 선호도 그룹, 선호도 레이블, 외부 LUN 디스크, 권한 부여 도메인, 역할 및 vNIC 프로필과 같은 백업 사이트의 엔터티를 수동으로 추가해야 합니다.



중요

자체 호스팅 엔진의 스토리지 도메인에 가상 시스템 디스크가 있으면 매핑 파일 생성이 실패합니다. 또한 매핑 파일에는 실패하지 않아야 하기 때문에 이 스토리지 도메인의 속성이 포함되지 않습니다.

이 예제에서 Ansible 플레이북의 이름은 **dr-rhv-setup.yml** 이며 기본 사이트의 Manager 머신에서 실행됩니다.

절차

1. 매핑 파일을 생성하는 Ansible 플레이북을 생성합니다. 예를 들면 다음과 같습니다.

```
---
- name: Generate mapping
  hosts: localhost
  connection: local

  vars:
    site: https://example.engine.redhat.com/ovirt-engine/api
    username: admin@internal
    password: my_password
    ca: /etc/pki/ovirt-engine/ca.pem
    var_file: disaster_recovery_vars.yml

  roles:
    - oVirt.disaster-recovery
```

참고

보안을 강화하기 위해 a **.yml** 파일에서 Manager 암호를 암호화할 수 있습니다. 자세한 내용은 *관리 가이드에서* Ansible 역할을 사용하여 Red Hat Virtualization 구성 을 참조하십시오.

2. Ansible 명령을 실행하여 매핑 파일을 생성합니다. 기본 사이트의 구성은 미리 채워져 있습니다.

```
# ansible-playbook dr-rhv-setup.yml --tags "generate_mapping"
```

3. 매핑 파일(이 경우**disaster_recovery_vars.yml**)을 백업 사이트의 구성으로 구성합니다. 매핑 파일의 특성에 대한 자세한 내용은 매핑 속성 매핑을 참조하십시오.

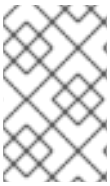
장애 조치 및 장애 조치(failback)를 수행할 수 있는 여러 Ansible 시스템이 있는 경우 매핑 파일을 모든 관련 시스템에 복사합니다.

3.4.3. Failover 및 Failback 플레이북 만들기

이를 플레이북에 추가해야 하므로 생성 및 구성한 매핑 파일이 있는지 확인합니다(이 경우 **disaster_recovery_vars.yml**).

기본 사이트 및 보조 사이트의 관리자 **암호를 저장하도록 암호 파일(예: password.yml**)을 정의할 수 있습니다. 예를 들면 다음과 같습니다.

```
---
# This file is in plain text, if you want to
# encrypt this file, please execute following command:
#
# $ ansible-vault encrypt passwords.yml
#
# It will ask you for a password, which you must then pass to
# ansible interactively when executing the playbook.
#
# $ ansible-playbook myplaybook.yml --ask-vault-pass
#
dr_sites_primary_password: primary_password
dr_sites_secondary_password: secondary_password
```



참고

보안을 강화하기 위해 암호 파일을 암호화할 수 있습니다. 그러나 플레이북을 실행할 때 **--ask-vault-pass** 매개변수를 사용해야 합니다. 자세한 내용은 관리 가이드에서 *Ansible 역할을 사용하여 Red Hat Virtualization 구성* 을 참조하십시오.

이 예제에서 장애 조치 및 장애 조치(failover)라는 Ansible 플레이북의 이름은 **dr-rhv-failover.yml** 및 **dr-rhv-failback.yml** 입니다.

환경을 장애 조치하기 위해 다음 Ansible 플레이북을 생성합니다.

```
---
- name: Failover RHV
  hosts: localhost
  connection: local
  vars:
    dr_target_host: secondary
    dr_source_map: primary
  vars_files:
    - disaster_recovery_vars.yml
    - passwords.yml
  roles:
    - oVirt.disaster-recovery
```

다음 Ansible 플레이북을 생성하여 환경에 장애 복구합니다.

```
---
- name: Failback RHV
  hosts: localhost
```

```
connection: local
vars:
  dr_target_host: primary
  dr_source_map: secondary
vars_files:
  - disaster_recovery_vars.yml
  - passwords.yml
roles:
  - oVirt.disaster-recovery
```

3.4.4. 기본 사이트 정리를 위한 플레이북 만들기

기본 사이트로 다시 실패하려면 먼저 기본 사이트를 가져올 모든 스토리지 도메인이 정리되었는지 확인해야 합니다. Manager에서 수동으로 이 작업을 수행하거나 선택적으로 Ansible 플레이북을 생성하여 수행할 수 있습니다.

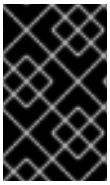
기본 사이트를 정리하는 Ansible 플레이북의 이름은 이 예에서 **dr-cleanup.yml** 이며 다른 Ansible 플레이북에서 생성한 매핑 파일을 사용합니다.

```
---
- name: clean RHV
  hosts: localhost
  connection: local
  vars:
    dr_source_map: primary
  vars_files:
    - disaster_recovery_vars.yml
  roles:
    - oVirt.disaster-recovery
```

3.5. 장애 조치(FAILOVER) 실행

사전 요구 사항

- 보조 사이트의 관리자와 호스트가 실행 중입니다.
- 복제 스토리지 도메인은 읽기/쓰기 모드입니다.
- 보조 사이트에 연결된 복제 스토리지 도메인이 없습니다.
- 필수 패키지 및 파일과 함께 기본 및 보조 사이트의 관리자에 SSH를 통해 연결할 수 있는 Red Hat Ansible Engine을 실행하는 시스템입니다.
  - **oVirt.disaster-recovery** 패키지.
  - 매핑 파일 및 필수 페일오버 플레이북입니다.



중요

Sanlock은 장애 조치 프로세스를 시작하기 전에 복제 스토리지 도메인의 모든 스토리지 잠금을 해제해야 합니다. 이러한 잠금은 재해 발생 후 약 80초 후에 자동으로 해제되어야 합니다.

이 예에서는 이전에 만든 **dr-rhv-failover.yml** 플레이북을 사용합니다.

절차

1. 다음 명령을 사용하여 장애 조치 플레이북을 실행합니다.

```
# ansible-playbook dr-rhv-failover.yml --tags "fail_over"
```

2. 기본 사이트가 활성화되면 다시 실패하기 전에 환경을 정리해야 합니다. 자세한 내용은 기본 사이트 정리를 참조하십시오.

3.6. 기본 사이트 정리

페일오버 후에는 기본 사이트에서 다시 실패하기 전에 환경을 정리해야 합니다.

- 기본 사이트의 모든 호스트를 재부팅합니다.
- 보조 사이트의 스토리지 도메인이 읽기/쓰기 모드이고 기본 사이트의 스토리지 도메인이 읽기 전용 상태인지 확인합니다.
- 보조 사이트의 스토리지 도메인에서 복제를 기본 사이트의 스토리지 도메인과 동기화합니다.
- 가져올 모든 스토리지 도메인의 기본 사이트를 정리합니다. 이 작업은 Manager에서 수동으로 수행하거나 Ansible 플레이북을 만들고 실행하여 수행할 수 있습니다. 수동 지침은 *관리 가이드*에서 스토리지 도메인 분리 또는 기본 사이트를 정리하여 Ansible 플레이북을 만드는 방법을 참조하십시오.

이 예에서는 이전에 만든 **dr-cleanup.yml** 플레이북을 사용하여 환경을 정리합니다.

절차

1. 다음 명령을 사용하여 기본 사이트를 정리합니다.

```
# ansible-playbook dr-cleanup.yml --tags "clean_engine"
```

2. 이제 환경을 기본 사이트로 장애 복구할 수 있습니다. 자세한 내용은 Failback 실행을 참조하십시오.

3.7. 실패 실행

장애 조치(failover)되면 기본 사이트로 장애 조치(failover)할 수 있으며 환경을 정리하는 데 필요한 단계를 수행한 경우 기본 사이트로 다시 실패할 수 있습니다.

사전 요구 사항

- 기본 사이트의 환경은 실행 중이고 정리되었으며 자세한 내용은 기본 사이트 정리를 참조하십시오.
- 보조 사이트의 환경이 실행 중이며 활성 스토리지 도메인이 있습니다.
- 필수 패키지 및 파일과 함께 기본 및 보조 사이트의 관리자에 SSH를 통해 연결할 수 있는 Red Hat Ansible Engine을 실행하는 시스템입니다.
  - **oVirt.disaster-recovery** 패키지.
  - 매핑 파일 및 필수 장애 복구 플레이북입니다.

이 예에서는 이전에 만든 **dr-rhv-failback.yml** 플레이북을 사용합니다.

절차

1. 다음 명령을 사용하여 failback 플레이북을 실행합니다.

```
# ansible-playbook dr-rhv-failback.yml --tags "fail_back"
```

2. 기본 스토리지 도메인에서 보조 스토리지 도메인으로 복제를 활성화합니다.

부록 A. 파일 속성 매핑

다음 테이블에서는 액티브-패시브 재해 복구 솔루션의 두 사이트 간에 장애 조치(failover)하는 데 사용되는 매핑 파일의 속성을 설명합니다.

표 A.1. 파일 속성 매핑

파일 섹션 매핑	설명
사이트 세부 정보	이러한 특성은 Manager 세부 정보를 기본 및 보조 사이트에 매핑합니다. 예를 들면 다음과 같습니다. dr_sites_primary_url: https://manager1.example.redhat.com/ovirt-engine/api dr_sites_primary_username: admin@internal dr_sites_primary_ca_file: /etc/pki/ovirt-engine/ca.pem # Please fill in the following properties for the secondary site: dr_sites_secondary_url: https://manager2.example.redhat.com/ovirt-engine/api dr_sites_secondary_username: admin@internal dr_sites_secondary_ca_file: /etc/pki/ovirt-engine/ca.pem

스토리지 도메인 세부 정보	이러한 특성은 기본 사이트와 보조 사이트 간에 스토리지 도메인 세부 정보를 매핑합니다. 예를 들면 다음과 같습니다.
	
	dr_import_storages:
	- dr_domain_type: nfs
	  dr_primary_name: DATA
	  dr_master_domain: True
	  dr_wipe_after_delete: False
	  dr_backup: False
	  dr_critical_space_action_blocker: 5
	  dr_warning_low_space: 10
	  dr_primary_dc_name: Default
	  dr_discard_after_delete: False
	  dr_primary_path: /storage/data
	  dr_primary_address: 10.64.100.xxx
	  # Fill in the empty properties related to the secondary site
	  dr_secondary_dc_name: Default
	  dr_secondary_path: /storage/data2
	  dr_secondary_address:10.64.90.xxx
	  dr_secondary_name: DATA

파일 섹션 매핑	설명
클러스터 세부 정보	이러한 특성은 기본 사이트와 보조 사이트 간에 클러스터 이름을 매핑합니다. 예를 들면 다음과 같습니다. dr_cluster_mappings: - primary_name: cluster_prod secondary_name: cluster_recovery - primary_name: fc_cluster secondary_name: recovery_fc_cluster
선호도 그룹 세부 정보	이러한 특성은 가상 머신이 속한 선호도 그룹을 매핑합니다. 예를 들면 다음과 같습니다. dr_affinity_group_mappings: - primary_name: affinity_prod secondary_name: affinity_recovery
유사성 레이블 세부 정보	이러한 특성은 가상 머신이 속한 선호도 레이블을 매핑합니다. 예를 들면 다음과 같습니다. dr_affinity_label_mappings: - primary_name: affinity_label_prod secondary_name: affinity_label_recovery
도메인 AAA 세부 정보	도메인 인증, 권한 부여 및 계정 지정(AAA) 속성은 기본 사이트 및 보조 사이트 간에 권한 부여 세부 정보를 매핑합니다. 예를 들면 다음과 같습니다. dr_domain_mappings: - primary_name: internal-authz secondary_name: recovery-authz - primary_name: external-authz secondary_name: recovery2-authz
역할 세부 정보	Role 속성은 특정 역할에 대한 매핑을 제공합니다. 예를 들어 가상 시스템이 **VmCreator** 역할을 가진 사용자에게 등록된 경우, 관리자가 장애 조치(failover)에서 동일한 사용자로 해당 가상 시스템의 권한을 등록하지만 다른 역할로 등록할 수 있습니다. 예를 들면 다음과 같습니다. dr_role_mappings: - primary_name: VmCreator Secondary_name: NewVmCreator

파일 섹션 매핑	설명
네트워크 세부 정보	네트워크 특성은 기본 사이트와 보조 사이트 간에 vNIC 세부 정보를 매핑합니다. 예를 들면 다음과 같습니다. dr_network_mappings: - primary_network_name: ovirtmgmt primary_profile_name: ovirtmgmt primary_profile_id: 0000000a-000a-000a-000a-000000000398 # Fill in the correlated vnic profile properties in the secondary site for profile 'ovirtmgmt' secondary_network_name: ovirtmgmt secondary_profile_name: ovirtmgmt secondary_profile_id: 0000000a-000a-000a-000a-000000000410 여러 네트워크 또는 여러 데이터 센터가 있는 경우 매핑 파일에 빈 네트워크 매핑을 사용하여 장애 조치 중 모든 엔터티가 대상에 등록하도록 해야 합니다. 예를 들면 다음과 같습니다. dr_network_mappings: # No mapping should be here

파일 섹션 매핑	설명
외부 LUN 디스크 세부 정보	외부 LUN 특성을 사용하면 장애 조치 및 장애 조치 후 가상 머신을 적절한 외부 LUN 디스크에 등록할 수 있습니다. 예를 들면 다음과 같습니다. dr_lun_mappings: - primary_logical_unit_id: 460014069b2be431c0fd46c4bdce29b66 primary_logical_unit_alias: Fedora_Disk primary_wipe_after_delete: False primary_shareable: False primary_logical_unit_description: 2b66 primary_storage_type: iscsi primary_logical_unit_address: 10.35.xx.xxx primary_logical_unit_port: 3260 primary_logical_unit_portal: 1 primary_logical_unit_target: iqn.2017-12.com.prod.example:444 secondary_storage_type: iscsi secondary_wipe_after_delete: False secondary_shareable: False secondary_logical_unit_id: 460014069b2be431c0fd46c4bdce29b66 secondary_logical_unit_address: 10.35.x.xxx secondary_logical_unit_port: 3260 secondary_logical_unit_portal: 1 secondary_logical_unit_target: iqn.2017-12.com.recovery.example:444

부록 B. ACTIVE-PASSIVE 구성 테스트

구성 후 재해 복구 솔루션을 테스트해야 합니다. 이 섹션에서는 액티브-패시브 재해 복구 구성을 테스트하는 여러 옵션을 제공합니다.

1. 기본 사이트가 활성화된 상태에서 기본 사이트의 스토리지 도메인에서 가상 머신을 방해하지 않고 페일오버를 테스트합니다. 장애 조치(failover) 테스트 를 참조하십시오.

2. 기본 사이트에 연결된 특정 스토리지 도메인을 사용하여 장애 조치 및 장애 조치를 테스트하므로 기본 사이트를 활성 상태로 유지할 수 있습니다. 장애 조치(failover) 및 Failback Test 를 참조하십시오.

3. 보조 사이트로 장애 조치(failover)를 수행하거나 기본 사이트의 예기치 않은 종료를 위해 유예 기간인 재해에 대한 장애 조치(failover) 및 장애 복구(failback)를 테스트합니다. 전체 장애 조치(failover) 및 Failback 테스트 참조.

중요

이러한 테스트를 실행하기 전에 액티브-패시브 구성을 구성하는 모든 단계를 완료했는지 확인합니다.

B.1. 중단된 페일오버 테스트

이 테스트에서는 기본 사이트 및 모든 스토리지 도메인을 활성 상태로 유지하여 사용자가 기본 사이트에서 계속 작업할 수 있는 장애 조치를 시뮬레이션합니다. 이 시나리오를 활성화하려면 기본 스토리지 도메인과 복제된(보조) 스토리지 도메인 간 복제를 비활성화해야 합니다. 이 테스트 중에 기본 사이트는 보조 사이트의 장애 조치 활동을 인식하지 못합니다.

이 테스트를 사용하면 장애 복구 기능을 테스트할 수 없습니다.

중요

장애 조치 후 프로덕션 작업이 수행되지 않는지 확인합니다. 예를 들어 이메일 시스템이 이메일을 실제 사용자에게 전송하지 않거나 다른 위치로 이메일을 리디렉션하지 않는지 확인합니다. 시스템이 다른 시스템을 직접 관리하는 데 사용되는 경우 시스템에 대한 액세스를 금지하거나 보조 사이트의 병렬 시스템에 액세스하는 것을 금지합니다.

무차별 장애 조치 테스트 수행:

1. 기본 스토리지 도메인과 복제된 스토리지 도메인 간에 스토리지 복제를 비활성화하고 복제된 모든 스토리지 도메인이 읽기/쓰기 모드인지 확인합니다.

2. 보조 사이트로 장애 조치하려면 명령을 실행합니다.

```
# ansible-playbook playbook --tags "fail_over"
```

   자세한 내용은 Failback 실행을 참조하십시오.

3. 모든 관련 스토리지 도메인, 가상 시스템 및 템플릿이 성공적으로 등록되어 실행 중인지 확인합니다.

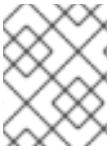
환경을 active-passive 상태로 복원합니다.

1. 보조 사이트에서 스토리지 도메인을 분리합니다.

2. 기본 스토리지 도메인과 보조 스토리지 도메인 간의 스토리지 복제를 활성화합니다.

B.2. 중단된 FAILOVER 및 FAILBACK 테스트

이 테스트에서는 장애 조치(failover) 및 장애 조치(failback)를 테스트하는 데 특별히 사용되는 테스트 가능한 스토리지 도메인을 정의해야 합니다. 복제된 스토리지를 보조 사이트에 연결할 수 있도록 이러한 스토리지 도메인을 복제해야 합니다. 이를 통해 사용자가 기본 사이트에서 계속 작업하는 동안 장애 조치(failover)를 테스트할 수 있습니다.



참고

기본 사이트에서 프로덕션에 사용되는 기본 스토리지 도메인에 영향을 주지 않고 오프라인일 수 있는 별도의 스토리지 서버에 테스트 가능한 스토리지 도메인을 정의해야 합니다.

환경 장애 조치, 환경 정리 및 장애 조치 수행에 대한 자세한 내용은 장애 조치(failover) 실행,기본 사이트 정리 및 Failback 실행을 참조하십시오.For more information about failing over the environment, cleaning the environment, cleaning the environment, and performing the failback, see Executing a Failover, Covering the Primary site , and Executing a Failback .

절차: 무차별 장애 조치 테스트:

1. 기본 사이트에서 테스트 스토리지 도메인을 중지합니다. 예를 들어 서버 호스트를 종료하거나 방화벽 규칙을 사용하여 차단하여 이 작업을 수행할 수 있습니다.
2. 테스트 가능한 스토리지 도메인 간에 스토리지 복제를 비활성화하고 테스트에 사용된 모든 복제된 스토리지 도메인이 읽기/쓰기 모드인지 확인합니다.
3. 테스트 기본 스토리지 도메인을 읽기 전용 모드에 배치합니다.
4. 보조 사이트로 장애 조치하려면 명령을 실행합니다.

```
# ansible-playbook playbook --tags "fail_over"
```

5. 모든 관련 스토리지 도메인, 가상 시스템 및 템플릿이 성공적으로 등록되어 실행 중인지 확인합니다.

절차: 중단 장애 복구 테스트*

1. 명령을 실행하여 기본 사이트를 정리하고 비활성 스토리지 도메인 및 관련 가상 머신 및 템플릿을 모두 제거합니다.

```
# ansible-playbook playbook --tags "clean_engine"
```

2. failback 명령을 실행합니다.

```
# ansible-playbook playbook --tags "fail_back"
```

3. 기본 스토리지 도메인에서 보조 스토리지 도메인으로 복제를 활성화합니다.
4. 모든 관련 스토리지 도메인, 가상 시스템 및 템플릿이 성공적으로 등록되어 실행 중인지 확인합니다.

B.3. 전체 장애 조치(FAILOVER) 및 FAILBACK 테스트

이 테스트는 기본 사이트와 보조 사이트 간에 전체 장애 조치(failover) 및 장애 조치(failback)를 수행합니다. 기본 사이트의 호스트를 종료하거나 방화벽 규칙을 추가하여 재해를 시뮬레이션하여 스토리지 도메인에 쓰기를 차단할 수 있습니다.

환경 장애 조치, 환경 정리 및 장애 조치 수행에 대한 자세한 내용은 장애 조치(failover) 실행,기본 사이트 정리 및 Failback 실행을 참조하십시오.For more information about failing over the environment, cleaning the environment, cleaning the environment, and performing the failback, see Executing a Failover, Covering the Primary site , and Executing a Failback .

절차: 장애 조치 테스트

1. 기본 스토리지 도메인과 복제된 스토리지 도메인 간에 스토리지 복제를 비활성화하고 복제된 모든 스토리지 도메인이 읽기/쓰기 모드로 되어 있는지 확인합니다.
2. 보조 사이트로 장애 조치하려면 명령을 실행합니다.

```
# ansible-playbook playbook --tags "fail_over"
```

3. 모든 관련 스토리지 도메인, 가상 시스템 및 템플릿이 성공적으로 등록되어 실행 중인지 확인합니다.

절차: 장애 복구 테스트

1. 보조 사이트의 스토리지 도메인과 기본 사이트의 스토리지 도메인 간 복제를 동기화합니다. 보조 사이트의 스토리지 도메인은 읽기/쓰기 모드여야 하며 기본 사이트의 스토리지 도메인은 읽기 전용 모드여야 합니다.
2. 명령을 실행하여 기본 사이트를 정리하고 비활성 스토리지 도메인 및 관련 가상 머신 및 템플릿을 모두 제거합니다.

```
# ansible-playbook playbook --tags "clean_engine"
```

3. failback 명령을 실행합니다.

```
# ansible-playbook playbook --tags "fail_back"
```

4. 기본 스토리지 도메인에서 보조 스토리지 도메인으로 복제를 활성화합니다.
5. 모든 관련 스토리지 도메인, 가상 시스템 및 템플릿이 성공적으로 등록되어 실행 중인지 확인합니다.

부록 C. 법적 공지