Red Hat Enterprise Linux 9

Identity Management를 통한 재해 복구 준비

IdM 환경에서 서버 및 데이터 손실 시나리오의 영향 완화

Last Updated: 2023-09-29

Red Hat Enterprise Linux 9 Identity Management를 통한 재해 복구 준비

IdM 환경에서 서버 및 데이터 손실 시나리오의 영향 완화

법적 공지

초록

예를 들어 하드웨어 오류로 인한 서버 및 데이터 손실 시나리오는 IT 환경에서 가장 큰 위험 요소입니다. Red Hat IdM(Identity Management) 토폴로지에서는 다른 서버와의 복제를 구성하고, VM(가상 머신) 스냅샷 및 IdM 백업을 사용하여 이러한 상황의 영향을 완화할 수 있습니다.

차례

보다 포괄적 수용을 위한 오픈 소스 용어 교체

Red Hat은 코드, 문서 및 웹 속성에서 문제가 있는 언어를 교체하기 위해 최선을 다하고 있습니다. 먼저 마스터(master), 슬레이브(slave), 블랙리스트(blacklist), 화이트리스트(whitelist) 등 네 가지 용어를 교체하고 있습니다. 이러한 변경 작업은 작업 범위가 크므로 향후 여러 릴리스에 걸쳐 점차 구현할 예정입니다. 자세한 내용은 CTO Chris Wright의 메시지 를 참조하십시오.

ID 관리에서 계획된 용어 교체는 다음과 같습니다.

- ***블록 목록*** 대체 *블랙리스트*
- ***허용 목록*** 대체 *허용 목록*
- ***보조*** 대체 *슬레이브*
- 컨텍스트에 따라 *마스터* 라는 단어가 보다 정확한 언어로 교체되고 있습니다.
  - ***IdM 서버*** 대체 *IdM 마스터*
  - ***CA 갱신 서버는*** *CA 갱신 마스터*로 대체
  - ***CRL 게시자 서버는*** *CRL master*를 대체합니다.
  - ***multi-supplier*** 는 *멀티 마스터*교체

RED HAT 문서에 관한 피드백 제공

문서에 대한 피드백에 감사드립니다. 어떻게 개선할 수 있는지 알려주십시오.

특정 문구에 대한 의견 제출

1. **Multi-page HTML** 형식으로 설명서를 보고 페이지가 완전히 로드된 후 오른쪽 상단 모서리에 **피드백** 버튼이 표시되는지 확인합니다.
2. 커서를 사용하여 주석 처리할 텍스트 부분을 강조 표시합니다.
3. 강조 표시된 텍스트 옆에 표시되는 **피드백 추가** 버튼을 클릭합니다.
4. 의견을 추가하고 **제출** 을 클릭합니다.

Jira를 통해 피드백 제출 (등록 필요)

1. Jira 웹 사이트에 로그인합니다.
2. 상단 탐색 모음에서 **생성** 을 클릭합니다.
3. **Summary** (요약) 필드에 설명 제목을 입력합니다.
4. **Description** (설명) 필드에 개선을 위한 제안을 입력합니다. 문서의 관련 부분에 대한 링크를 포함합니다.
5. 대화 상자 하단에서 **생성** 을 클릭합니다.

1장. IDM의 재해 복구 툴

좋은 재해 복구 전략은 다음과 같은 도구를 결합하여 가능한 한 빨리 데이터 손실을 최소화하여 재해에서 복구합니다.

복제

복제는 IdM 서버 간 데이터베이스 콘텐츠를 복사합니다. IdM 서버에 장애가 발생하면 나머지 서버 중 하나를 기반으로 새 복제본을 생성하여 손실된 서버를 교체할 수 있습니다.

VM(가상 머신) 스냅샷

스냅샷은 지정된 시점에서 사용 가능한 모든 디스크에 있는 VM의 운영 체제 및 애플리케이션에 대한 보기입니다. VM 스냅샷을 만든 후 이를 사용하여 VM 및 IdM 데이터를 이전 상태로 되돌릴 수 있습니다.

IdM 백업

ipa-backup 유틸리티를 사용하면 IdM 서버의 구성 파일 및 해당 데이터를 백업할 수 있습니다. 나중에 백업을 사용하여 IdM 서버를 이전 상태로 복원할 수 있습니다.

2장. IDM의 재해 시나리오

재해 시나리오에는 *서버 손실 및 데이터 손실* 의 두 가지 주요 클래스가 있습니다.

표 2.1. 서버 손실과 데이터 손실

재해 유형	원인 예	준비 방법
서버 손실: IdM 배포 하나 이상의 서버가 손실됩니다.	• 하드웨어 장애 조치	• 복제를 사용하여 서버 손실 준비
데이터 손실: 서버에서 IdM 데이터가 예기치 않게 수정되며 변경 사항이 다른 서버로 전파됩니다.	• 사용자가 실수로 데이터를 삭제 • 소프트웨어 버그 수정 데이터	• VM 스냅샷으로 데이터 손실 준비 • IdM 백업을 사용하여 데이터 손실 준비

3장. 복제를 사용하여 서버 손실 준비

다음 지침에 따라 서버 손실에 대응할 수 있는 복제 토폴로지를 설정합니다.

이 섹션에서는 다음 주제를 다룹니다.

- 토폴로지의 복제본 연결
- 복제본 토폴로지 예
- IdM CA 데이터 보호

3.1. 토폴로지에서 IDM 복제본 연결 지침

각 복제본을 두 개 이상의 다른 복제본에 연결

추가 복제 계약을 구성하면 설치한 초기 복제본과 첫 번째 서버뿐만 아니라 다른 복제본 간에도 정보가 복제됩니다.

복제본을 최대 4개의 다른 복제본에 연결(하드 요구 사항이 아님)

서버당 다수의 복제 계약이 큰 이점을 추가하지 않습니다. 수신 복제본은 한 번에 하나의 다른 복제본에서만 업데이트할 수 있으며 다른 복제 계약에서는 유휴 상태입니다. 복제본당 복제 계약 4개 이상은 일반적으로 리소스 낭비를 의미합니다.

참고

이 권장 사항은 인증서 복제 및 도메인 복제 계약에 모두 적용됩니다.

복제본당 복제 계약 4개 제한에는 두 가지 예외가 있습니다.

- 특정 복제본이 온라인 상태가 아닌 경우 장애 조치(failover) 경로가 필요합니다.
- 대규모 배포에서는 특정 노드 간에 직접 연결을 추가로 수행해야 합니다.

많은 수의 복제 계약을 구성하면 전체 성능에 부정적인 영향을 미칠 수 있습니다: 토폴로지의 여러 복제 계약이 업데이트를 전송하는 경우 특정 복제본은 들어오는 업데이트와 발신 업데이트 사이에 변경 로그 데이터베이스 파일에 대한 경합이 발생할 수 있습니다.Configuring a number of replication agreements can have a negative impact on overall performance: when multiple replication agreements in the topology are sending updates, certain replicas can experience a high contention on the changelog database file between the incoming updates and the outgoing updates.

복제본당 더 많은 복제 계약을 사용하려면 복제 문제 및 대기 시간이 발생하지 않아야 합니다. 그러나 많은 중간 노드 수와 많은 중간 노드 수로 인해 대기 시간 문제가 발생할 수 있습니다.

데이터 센터의 복제본을 서로 연결

이렇게 하면 데이터 센터 내에서 도메인 복제가 보장됩니다.

각 데이터 센터를 두 개 이상의 다른 데이터 센터에 연결

이렇게 하면 데이터 센터 간 도메인 복제가 보장됩니다.

최소 한 쌍의 복제 계약을 사용하여 데이터 센터 연결

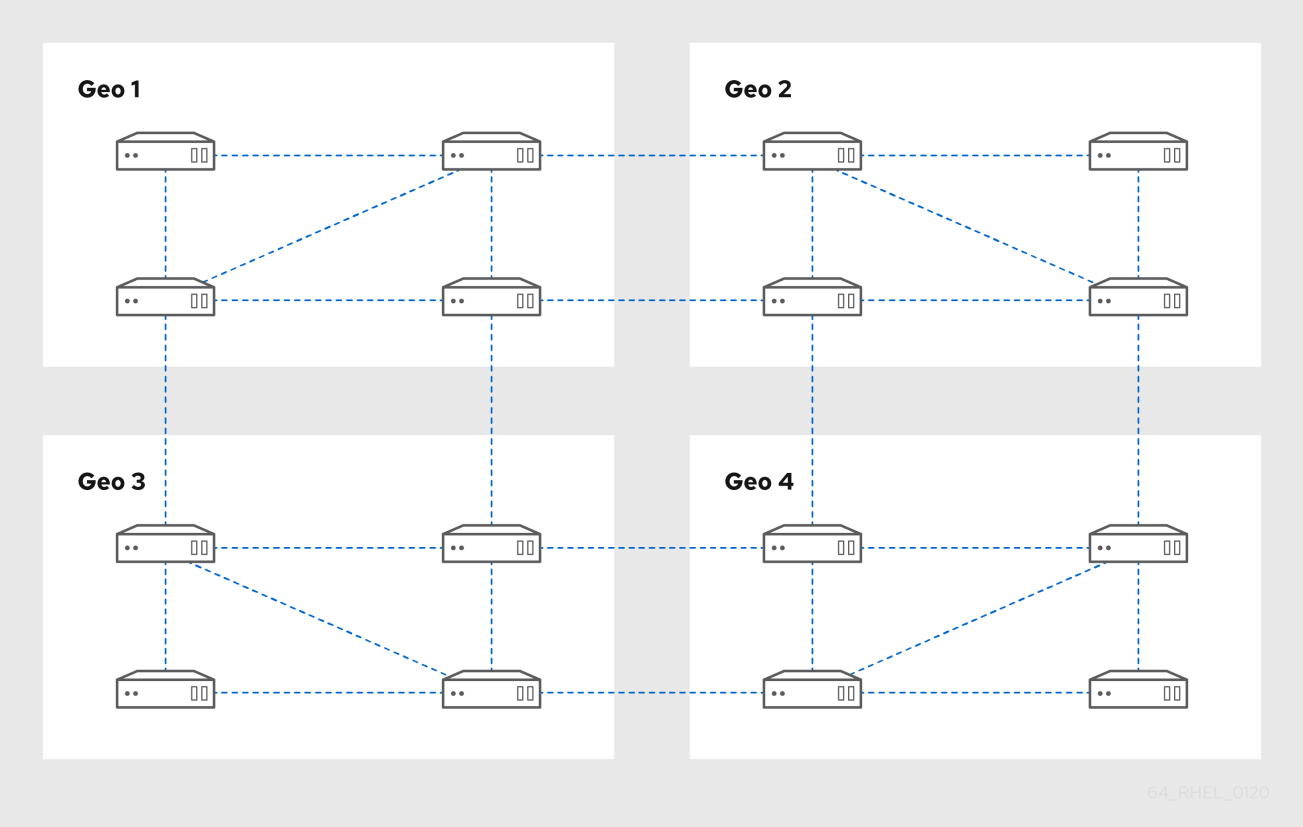
데이터 센터 A1에서 B1로의 복제 계약이 있는 경우 A2에서 B2로의 복제 계약을 통해 서버 중 하나가 다운된 경우 두 데이터 센터 간에 복제를 계속할 수 있습니다.

3.2. 복제본 토폴로지 예

아래 그림은 안정적인 토폴로지를 생성하기 위한 지침에 따라 IdM(Identity Management) 토폴로지의 예를 보여줍니다.

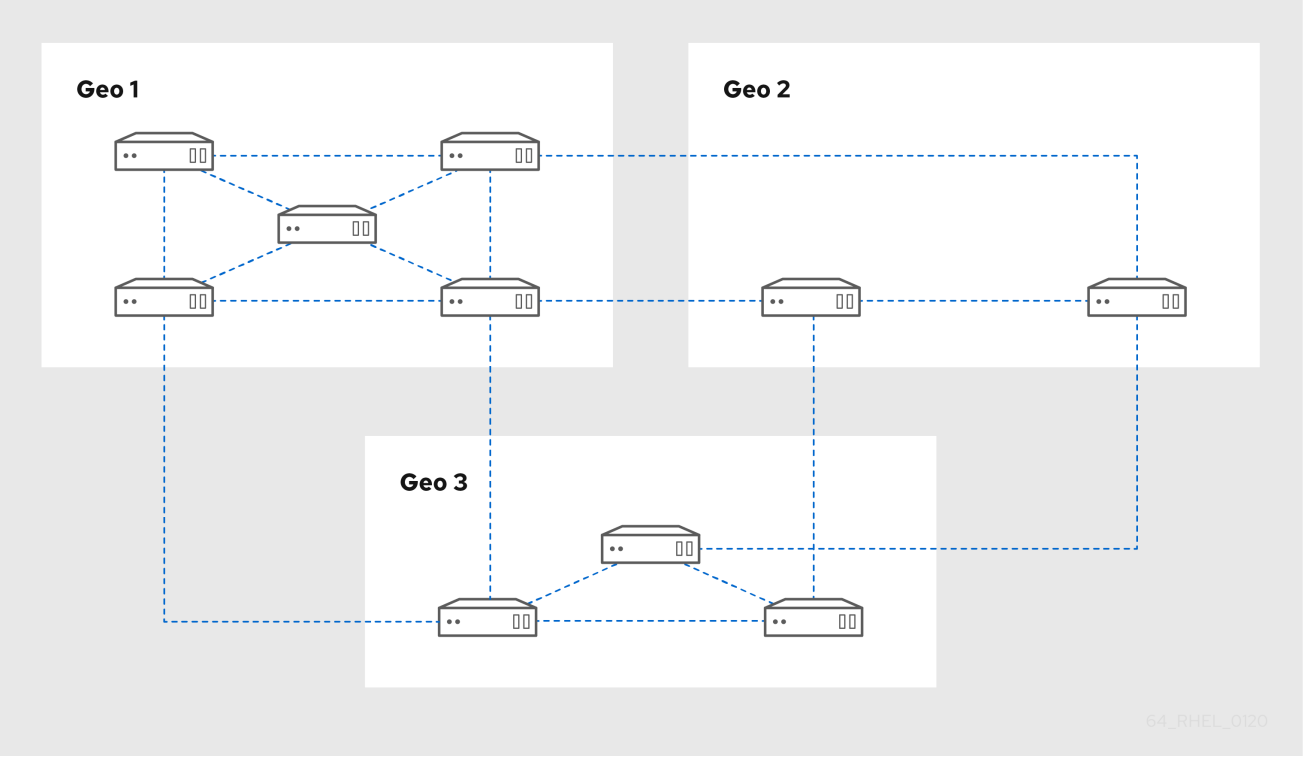
복제본 토폴로지 예 1 은 각각 4개의 서버가 있는 4개의 데이터 센터를 표시합니다. 서버는 복제 계약과 연결되어 있습니다.

그림 3.1. 복제본 토폴로지 예 1



복제본 토폴로지 예 2 는 각각 다른 서버 수가 있는 세 개의 데이터 센터를 보여줍니다. 서버는 복제 계약과 연결되어 있습니다.

그림 3.2. 복제본 토폴로지 예 2



3.3. IDM CA 데이터 보호

배포에 통합 IdM CA(인증 기관)가 포함된 경우 여러 CA 복제본을 설치하여 추가 CA 복제본을 생성할 수 있습니다.

절차

1. CA 서비스를 제공하도록 3개 이상의 복제본을 구성합니다.

   a. CA 서비스를 사용하여 새 복제본을 설치하려면 **--setup-ca** 옵션으로 **ipa-replica-install** 을 실행합니다.

   ```
   [root@server ~]# ipa-replica-install --setup-ca
   ```

   b. 기존 복제본에 CA 서비스를 설치하려면 **ipa-ca-install** 을 실행합니다.

   ```
   [root@replica ~]# ipa-ca-install
   ```

2. CA 복제본 간의 CA 복제 계약을 생성합니다.

```
[root@careplica1 ~]# ipa topologysegment-add
Suffix name: ca
Left node: ca-replica1.example.com
Right node: ca-replica2.example.com
Segment name [ca-replica1.example.com-to-ca-replica2.example.com]: new_segment
----------------------------
Added segment "new_segment"
----------------------------
  Segment name: new_segment
```

```
Left node: ca-replica1.example.com
Right node: ca-replica2.example.com
Connectivity: both
```

주의

하나의 서버만 CA 서비스를 제공하고 손상된 경우 전체 환경이 손실됩니다. IdM CA를 사용하는 경우 Red Hat은 CA 서비스가 설치된 복제본 3개 이상과 함께 CA 복제 계약을 사용하는 **것이 좋습니다**.

추가 리소스

- CA 서비스 계획.
- IdM 복제본 설치.
- 복제본 토폴로지 계획.

4장. VM 스냅샷으로 데이터 손실 준비

VM(가상 머신) 스냅샷은 IdM 서버의 전체 상태를 유지하기 때문에 데이터 복구 전략의 필수 구성 요소입니다.

- 운영 체제 소프트웨어 및 설정
- IdM 소프트웨어 및 설정
- IdM 고객 데이터

IdM CA(인증 기관) 복제본의 VM 스냅샷을 준비하면 재해 발생 후 전체 IdM 배포를 다시 빌드할 수 있습니다.

주의

환경에서 통합 CA를 사용하는 경우 인증서 데이터가 유지되지 않으므로 *CA가 없는* 복제본의 스냅샷은 배포를 다시 빌드하는 데 충분하지 않습니다.

마찬가지로, 환경에서 IdM KMS(Key recovery Authority)를 사용하는 경우 KRA 복제본의 스냅샷을 생성하거나 스토리지 키가 손실될 수 있습니다.

배포에 사용 중인 모든 IdM 서버 역할(CA, KRA, DNS)이 설치된 VM의 스냅샷을 생성하는 것이 좋습니다.

사전 요구 사항

- RHEL VM을 호스팅할 수 있는 하이퍼바이저입니다.

절차

1. VM 내에서 실행하도록 배포에 하나 이상의 **CA 복제본** 을 구성합니다.
   a. 환경에 IdM DNS 또는 KRA를 사용하는 경우 이 복제본에도 DNS 및 KRA 서비스를 설치하는 것이 좋습니다.
   b. 선택적으로 이 VM 복제본을 숨겨진 복제본 으로 구성합니다.
2. 정기적으로 이 VM을 종료하고 해당 VM의 전체 스냅샷을 종료한 후 다시 온라인 상태로 전환하므로 복제 업데이트가 계속 수신됩니다. VM이 숨겨진 복제본인 경우 이 프로세스 중에 IdM 클라이언트가 중단되지 않습니다.

추가 리소스

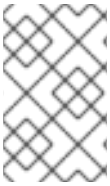
- Red Hat Enterprise Linux를 실행하도록 인증된 하이퍼바이저는 무엇입니까?
- 숨겨진 복제본 모드.

5장. IDM 백업을 사용하여 데이터 손실 준비

IdM은 백업 IdM 데이터에 **ipa-backup** 유틸리티를 제공하고 **ipa-restore** 유틸리티를 통해 해당 백업의 서버 및 데이터를 복원합니다.

이 섹션에서는 다음 주제를 다룹니다.

- IdM 백업 유형
- IdM 백업 파일의 이름 지정 규칙
- 백업 생성 시 고려 사항
- IdM 백업 생성
- GPG2-encrypted IdM 백업 생성
- GPG2 키 생성



참고

모든 서버 역할이 설치된 *숨겨진 복제본*, 특히 통합 IdM CA를 사용하는 경우 CA(인증 기관) 역할에 필요한 경우 백업을 자주 실행하는 것이 좋습니다. IdM 숨겨진 복제본 설치를 참조하십시오.

5.1. IDM 백업 유형

ipa-backup 유틸리티를 사용하면 다음 두 가지 유형의 백업을 생성할 수 있습니다.

전체 서버 백업

- IdM과 관련된 모든 서버 구성 파일과 LDAP Data Interchange Format(LDIF) 파일의 LDAP 데이터를 **포함합니다**.
- IdM 서비스는 **오프라인** 상태여야 합니다.
- IdM 배포를 처음부터 다시 빌드하는 데 **적합합니다**.

데이터 전용 백업

- LDIF 파일 및 복제 변경 로그에 LDAP 데이터가 **포함되어** 있습니다.
- IdM 서비스는 **온라인 또는 오프라인** 상태일 수 있습니다.
- IdM 데이터를 과거 상태로 복원하는 데 **적합합니다**.

5.2. IDM 백업 파일의 이름 지정 규칙

기본적으로 IdM은 백업을 **/var/lib/ipa/backup/** 디렉터리의 하위 디렉터리에 **.tar** 아카이브로 저장합니다.

아카이브 및 하위 디렉터리는 다음과 같은 명명 규칙을 따릅니다.

전체 서버 백업

ipa-full- < ***YEAR-MM-DD-HH-MM-SS>라는 디렉토리에 ipa- full*.tar** 이라는 아카이브로, 915 시간에 지정된 시간을 지정합니다.

```
[root@server ~]# ll /var/lib/ipa/backup/ipa-full-2021-01-29-12-11-46
total 3056
-rw-r--r--. 1 root root     158 Jan 29 12:11 header
-rw-r--r--. 1 root root 3121511 Jan 29 12:11 ipa-full.tar
```

데이터 전용 백업

ipa-data- < ***YEAR-MM-DD-HH-MM-SS>라는 디렉토리에 ipa- data*.tar** 이라는 아카이브로, 915 시간에 지정된 시간을 지정합니다.

```
[root@server ~]# ll /var/lib/ipa/backup/ipa-data-2021-01-29-12-14-23
total 1072
-rw-r--r--. 1 root root     158 Jan 29 12:14 header
-rw-r--r--. 1 root root 1090388 Jan 29 12:14 ipa-data.tar
```

참고

IdM 서버를 설치 제거해도 백업 파일이 자동으로 제거되지는 않습니다.

5.3. 백업 생성 시 고려 사항

ipa-backup 명령의 중요한 동작 및 제한 사항은 다음과 같습니다.

- 기본적으로 **ipa-backup** 유틸리티는 오프라인 모드로 실행되어 모든 IdM 서비스를 중지합니다. 백업이 완료된 후 유틸리티를 통해 IdM 서비스가 자동으로 다시 시작됩니다.
- 전체 서버 백업은 **항상** 오프라인으로 IdM 서비스를 실행해야 하지만 온라인 서비스에서 데이터 전용 백업을 수행할 수 있습니다.
- 기본적으로 **ipa-backup** 유틸리티는 **/var/lib/ipa/backup/** 디렉터리가 포함된 파일 시스템에 백업을 생성합니다. Red Hat은 IdM에서 사용하는 프로덕션 파일 시스템과 별도로 파일 시스템에 백업을 정기적으로 만들고 백업을 자리기 또는 광장 스토리지와 같은 고정된 매체로 보관하는 것이 좋습니다.
- 숨겨진 복제본에서 백업을 수행하는 것이 좋습니다. IdM 클라이언트에 영향을 주지 않고 숨겨진 복제본에서 IdM 서비스를 종료할 수 있습니다.
- **ipa-backup** 유틸리티는 CA(인증 기관), DNS(Domain Name System), Key recovery Agent(KRA)와 같이 IdM 클러스터에 사용된 모든 서비스가 백업을 실행하는 서버에 설치되어 있는지 확인합니다. 서버에 이러한 서비스가 설치되지 않은 경우 해당 호스트에서 가져온 백업으로 인해 전체 클러스터 복원에 충분하지 않기 때문에 **ipa-backup** 유틸리티가 경고로 종료됩니다.
  예를 들어 IdM 배포에서 통합 CA(인증 기관)를 사용하는 경우 비CA 복제본에서 백업 실행이 CA 데이터를 캡처하지 않습니다. **ipa-backup** 을 수행하는 복제본에 클러스터에 사용되는 모든 IdM 서비스가 있는지 확인하는 것이 좋습니다.

  ipa-backup --disable-role-check 명령을 사용하여 IdM 서버 역할 검사를 바이패스할 수 있지만, 결과적으로 백업에 IdM을 완전히 복원하는 데 필요한 모든 데이터가 포함되어 있지 않습니다.

5.4. IDM 백업 생성

ipa-backup 명령을 사용하여 오프라인 및 온라인 모드에서 전체 서버 및 데이터 전용 백업을 생성하려면 다음 절차를 따르십시오.

사전 요구 사항

- **ipa-backup** 유틸리티를 실행하려면 **루트** 권한이 있어야 합니다.

절차

- 오프라인 모드에서 전체 서버 백업을 생성하려면 추가 옵션 없이 **ipa-backup** 유틸리티를 사용하십시오.

```
[root@server ~]# ipa-backup
Preparing backup on server.example.com
Stopping IPA services
Backing up ipaca in EXAMPLE-COM to LDIF
Backing up userRoot in EXAMPLE-COM to LDIF
Backing up EXAMPLE-COM
Backing up files
Starting IPA service
Backed up to /var/lib/ipa/backup/ipa-full-2020-01-14-11-26-06
The ipa-backup command was successful
```

- 오프라인 데이터 전용 백업을 만들려면 **--data** 옵션을 지정합니다.

```
[root@server ~]# ipa-backup --data
```

- IdM 로그 파일이 포함된 전체 서버 백업을 생성하려면 **--logs** 옵션을 사용합니다.

```
[root@server ~]# ipa-backup --logs
```

- IdM 서비스가 실행되는 동안 데이터 전용 백업을 생성하려면 **--data** 및 **--online** 옵션을 둘 다 지정합니다.

```
[root@server ~]# ipa-backup --data --online
```

참고

/tmp 디렉터리의 공간이 충분하지 않아 백업이 실패하는 경우 **TMPDIR** 환경 변수를 사용하여 백업 프로세스에서 생성된 임시 파일의 대상을 변경합니다.

```
[root@server ~]# TMPDIR=/new/location ipa-backup
```

자세한 내용은 ipa-backup Command Fails to Finish 를 참조하십시오.

검증 단계

- 백업 디렉터리에는 백업이 포함된 아카이브가 포함되어 있습니다.

```
[root@server ~]# ls /var/lib/ipa/backup/ipa-full-2020-01-14-11-26-06
header  ipa-full.tar
```

5.5. GPG2-ENCRYPTED IDM 백업 생성

GPG(GNU Privacy guard) 암호화를 사용하여 암호화된 백업을 생성할 수 있습니다. 다음 절차에서는 IdM 백업을 생성하고 GPG2 키를 사용하여 암호화합니다.

사전 요구 사항

- GPG2 키를 생성했습니다. GPG2 키 생성을 참조하십시오.

절차

- **--gpg** 옵션을 지정하여 GPG 암호화 백업을 만듭니다.

```
[root@server ~]# ipa-backup --gpg
Preparing backup on server.example.com
Stopping IPA services
Backing up ipaca in EXAMPLE-COM to LDIF
Backing up userRoot in EXAMPLE-COM to LDIF
Backing up EXAMPLE-COM
Backing up files
Starting IPA service
Encrypting /var/lib/ipa/backup/ipa-full-2020-01-13-14-38-00/ipa-full.tar
Backed up to /var/lib/ipa/backup/ipa-full-2020-01-13-14-38-00
The ipa-backup command was successful
```

검증 단계

- 백업 디렉터리에 **.gpg** 파일 확장자로 암호화된 아카이브가 포함되어 있는지 확인합니다.

```
[root@server ~]# ls /var/lib/ipa/backup/ipa-full-2020-01-13-14-38-00
header  ipa-full.tar.gpg
```

추가 리소스

- 백업 생성.

5.6. GPG2 키 생성

다음 절차에서는 암호화 유틸리티에서 사용할 GPG2 키를 생성하는 방법을 설명합니다.

사전 요구 사항

- **root** 권한이 필요합니다.

절차

1. **pinentry** 유틸리티를 설치하고 구성합니다.

```
[root@server ~]# dnf install pinentry
[root@server ~]# mkdir ~/.gnupg -m 700
[root@server ~]# echo "pinentry-program /usr/bin/pinentry-curses" >> ~/.gnupg/gpg-agent.conf
```

2. 기본 세부 정보를 사용하여 GPG **키 쌍을 생성하는 데 사용되는 키 입력** 파일을 만듭니다. 예를 들어 다음과 같습니다.

```
[root@server ~]# cat >key-input <<EOF
%echo Generating a standard key
Key-Type: RSA
Key-Length: 2048
Name-Real: GPG User
Name-Comment: first key
Name-Email: root@example.com
Expire-Date: 0
%commit
%echo Finished creating standard key
EOF
```

3. *(선택 사항)* 기본적으로 GPG2는 해당 인증 키를 **~/.gnupg** 파일에 저장합니다. 사용자 지정 인증 키 위치를 사용하려면 **GNUPGHOME** 환경 변수를 루트에서만 액세스할 수 있는 디렉터리로 설정합니다.

```
[root@server ~]# export GNUPGHOME=/root/backup

[root@server ~]# mkdir -p $GNUPGHOME -m 700
```

4. 키 **입력 파일의 콘텐츠를 기반으로 새 GPG2 키를** 생성합니다.

```
[root@server ~]# gpg2 --batch --gen-key key-input
```

5. GPG2 키를 보호하려면 암호를 입력합니다. 이 암호를 사용하여 암호 해독을 위해 개인 키에 액세스합니다.

```
┌──────────────────────────────────────────────────────┐
│ Please enter the passphrase to                       │
│ protect your new key                                 │
│                                                      │
│ Passphrase: <passphrase>                             │
│                                                      │
│  <OK>                    <Cancel>                    │
└──────────────────────────────────────────────────────┘
```

6. 다시 입력하여 올바른 암호를 확인합니다.

```
┌──────────────────────────────────────────────────────┐
│ Please re-enter this passphrase                      │
│                                                      │
│ Passphrase: <passphrase>                             │
│                                                      │
│  <OK>                    <Cancel>                    │
└──────────────────────────────────────────────────────┘
```

7. 새 GPG2 키가 성공적으로 생성되었는지 확인합니다.

```
gpg: keybox '/root/backup/pubring.kbx' created
gpg: Generating a standard key
gpg: /root/backup/trustdb.gpg: trustdb created
```

```
gpg: key BF28FFA302EF4557 marked as ultimately trusted
gpg: directory '/root/backup/openpgp-revocs.d' created
gpg: revocation certificate stored as '/root/backup/openpgp-
revocs.d/8F6FCF10C80359D5A05AED67BF28FFA302EF4557.rev'
gpg: Finished creating standard key
```

검증 단계

- 서버에서 GPG 키를 나열합니다.

```
[root@server ~]# gpg2 --list-secret-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
/root/backup/pubring.kbx
------------------------
sec   rsa2048 2020-01-13 [SCEA]
      8F6FCF10C80359D5A05AED67BF28FFA302EF4557
uid           [ultimate] GPG User (first key) <root@example.com>
```

추가 리소스

- GNU 개인 정보 보호 기능

6장. ANSIBLE 플레이북을 사용하여 IDM 서버 백업

ipabackup Ansible 역할을 사용하여 IdM 서버 백업을 자동화하고 서버와 Ansible 컨트롤러 간에 백업 파일을 전송할 수 있습니다.

이 섹션에서는 다음 주제를 다룹니다.

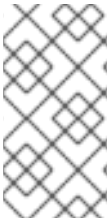
- IdM 관리를 위해 Ansible 제어 노드 준비
- Ansible을 사용하여 IdM 서버 백업 생성
- Ansible을 사용하여 Ansible 컨트롤러에 IdM 서버 백업 생성
- Ansible을 사용하여 IdM 서버의 백업을 Ansible 컨트롤러에 복사
- Ansible을 사용하여 Ansible 컨트롤러에서 IdM 서버로 IdM 서버 백업 복사
- Ansible을 사용하여 IdM 서버에서 백업 제거

6.1. IDM 관리를 위해 ANSIBLE 제어 노드 준비

Red Hat Ansible Engine으로 작업할 때 IdM(Identity Management)을 관리하는 시스템 관리자는 다음을 수행하는 것이 좋습니다.

- 홈 디렉터리에서 Ansible 플레이북 전용 하위 디렉터리를 생성합니다(예: **~/MyPlaybooks**).
- **/usr/share/doc/ansible-freeipa/*** 및 **/usr/share/doc/rhel-system-roles/*** 디렉터리 및 하위 디렉터리에서 **~/MyPlaybooks** 디렉터리에 복사 및 조정.
- 인벤토리 파일을 **~/MyPlaybook** 디렉터리에 포함합니다.

이 방법을 따라 모든 플레이북을 한 곳에서 찾을 수 있으며 루트 권한을 호출하지 않고 플레이북을 실행할 수 있습니다.



참고

ipaserver,**ipareplica**,**ipaclient**,**ipabackup**,**ipasmartcard_server** 및 **ipasmartcard_client** **ansible-freeipa** 역할을 실행하려면 관리형 노드에서만 **root** 권한이 필요합니다. 이러한 역할을 수행하려면 디렉터리 및 **dnf** 소프트웨어 패키지 관리자에 대한 액세스 권한이 필요합니다.

Ansible 플레이북을 저장하고 실행하는 데 사용할 수 있도록 **~/MyPlaybooks** 디렉터리를 생성하고 구성하려면 다음 절차를 따르십시오.

사전 요구 사항

- 관리형 노드 *server.idm.example.com* 및 *replica.idm.example.com* 에 IdM 서버를 설치했습니다.
- 제어 노드에서 직접 관리형 노드, *server.idm.example.com* 및 *replica.idm.example.com* 에 로그인할 수 있도록 DNS 및 네트워킹을 구성했습니다.
- IdM **관리자** 암호를 알고 있습니다.

절차

1. 홈 디렉터리에서 Ansible 구성 및 플레이북의 디렉터리를 생성합니다.

```
$ mkdir ~/MyPlaybooks/
```

2. **~/MyPlaybooks/** 디렉터리로 변경합니다.

```
$ cd ~/MyPlaybooks
```

3. 다음 콘텐츠를 사용하여 **~/MyPlaybooks/ansible.cfg** 파일을 생성합니다.

```
[defaults]
inventory = /home/your_username/MyPlaybooks/inventory

[privilege_escalation]
become=True
```

4. 다음 콘텐츠를 사용하여 **~/MyPlaybooks/inventory** 파일을 만듭니다.

```
[ipaserver]
server.idm.example.com

[ipareplicas]
replica1.idm.example.com
replica2.idm.example.com

[ipacluster:children]
ipaserver
ipareplicas

[ipacluster:vars]
ipaadmin_password=SomeADMINpassword

[ipaclients]
ipaclient1.example.com
ipaclient2.example.com

[ipaclients:vars]
ipaadmin_password=SomeADMINpassword
```

이 구성은 이러한 위치에 있는 호스트에 대해 **eu** 와 **us** 이라는 두 개의 호스트 그룹을 정의합니다. 또한 이 구성은 **eu** 및 **us** 그룹의 모든 호스트를 포함하는 **ipaserver** 호스트 그룹을 정의합니다.

5. [선택 사항] SSH 공개 및 개인 키를 생성합니다. 테스트 환경에서 액세스를 단순화하려면 개인 키에 암호를 설정하지 마십시오.

```
$ ssh-keygen
```

6. SSH 공개 키를 각 관리 노드의 IdM **관리자** 계정에 복사합니다.

```
$ ssh-copy-id admin@server.idm.example.com
$ ssh-copy-id admin@replica.idm.example.com
```

이러한 명령을 입력할 때 IdM **관리자** 암호를 입력해야 합니다.

추가 리소스

- Ansible 플레이북을 사용하여 Identity Management 서버 설치 .
- 인벤토리를 구축하는 방법.

6.2. ANSIBLE을 사용하여 IDM 서버 백업 생성

다음 절차에서는 Ansible 플레이북에서 ipabackup 역할을 사용하여 IdM 서버의 백업을 생성하고 IdM 서버에 저장하는 방법을 설명합니다.

사전 요구 사항

- 다음 요구 사항을 충족하도록 Ansible 제어 노드를 구성했습니다.
  - Ansible 버전 2.14 이상을 사용하고 있습니다.
  - Ansible 컨트롤러에 **ansible-freeipa** 패키지가 설치되어 있습니다.
  - 이 예제에서는 ***~/MyPlaybook/*** 디렉터리에서 IdM 서버의 FQDN(정규화된 도메인 이름)을 사용하여 Ansible 인벤토리 파일을 생성했다고 가정합니다.
  - 이 예제에서는 **secret.yml** Ansible 자격 증명 모음이 **ipaadmin_password** 를 저장한다고 가정합니다.

절차

1. **~/MyPlaybook/** 디렉터리로 이동합니다.

```
$ cd ~/MyPlaybooks/
```

2. **/usr/share/doc/ansible-freeipa/playbooks** 디렉터리에 있는 **backup-server.yml** 파일의 사본을 만듭니다.

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/backup-server.yml backup-my-server.yml
```

3. 편집할 **backup-my-server.yml** Ansible 플레이북 파일을 엽니다.
4. **hosts** 변수를 인벤토리 파일의 호스트 그룹으로 설정하여 파일을 조정합니다. 이 예에서는 **ipaserver** 호스트 그룹으로 설정합니다.

```
---
- name: Playbook to backup IPA server
  hosts: ipaserver
  become: true

  roles:
  - role: ipabackup
    state: present
```

5. 파일을 저장합니다.
6. 인벤토리 파일 및 플레이북 파일을 지정하여 Ansible 플레이북을 실행합니다.

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory
backup-my-server.yml
```

검증 단계

1. 백업한 IdM 서버에 로그인합니다.
2. 백업이 **/var/lib/ipa/backup** 디렉터리에 있는지 확인합니다.

```
[root@server ~]# ls /var/lib/ipa/backup/
ipa-full-2021-04-30-13-12-00
```

추가 리소스

- **ipabackup** 역할을 사용하는 샘플 Ansible Playbook은 다음을 참조하십시오.
  - **/usr/share/doc/ansible-freeipa/roles/ipabackup** 디렉토리의 **README.md** 파일입니다.
  - **/usr/share/doc/ansible-freeipa/playbooks/** 디렉토리

6.3. ANSIBLE을 사용하여 ANSIBLE 컨트롤러에 IDM 서버 백업 생성

다음 절차에서는 Ansible 플레이북에서 **ipabackup** 역할을 사용하여 IdM 서버의 백업을 생성하고 Ansible 컨트롤러에서 자동으로 전송하는 방법을 설명합니다. 백업 파일 이름은 IdM 서버의 호스트 이름으로 시작됩니다.

사전 요구 사항

- 다음 요구 사항을 충족하도록 Ansible 제어 노드를 구성했습니다.
  - Ansible 버전 2.14 이상을 사용하고 있습니다.
  - Ansible 컨트롤러에 **ansible-freeipa** 패키지가 설치되어 있습니다.
  - 이 예제에서는 ***~/MyPlaybook/*** 디렉터리에서 IdM 서버의 FQDN(정규화된 도메인 이름)을 사용하여 Ansible 인벤토리 파일을 생성했다고 가정합니다.
  - 이 예제에서는 **secret.yml** Ansible 자격 증명 모음이 **ipaadmin_password** 를 저장한다고 가정합니다.

절차

1. 백업을 저장하려면 Ansible 컨트롤러의 홈 디렉터리에 하위 디렉터리를 생성합니다.

```
$ mkdir ~/ipabackups
```

2. **~/MyPlaybook/** 디렉터리로 이동합니다.

```
$ cd ~/MyPlaybooks/
```

3. **/usr/share/doc/ansible-freeipa/playbooks** 디렉터리에 있는 **backup-server-to-controller.yml** 파일의 사본을 만듭니다.

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/backup-server-to-controller.yml backup-my-server-to-my-controller.yml
```

4. 편집할 **backup-my-server-to-my-controller.yml** 파일을 엽니다.
5. 다음 변수를 설정하여 파일을 조정합니다.
   a. **hosts** 변수를 인벤토리 파일의 호스트 그룹으로 설정합니다. 이 예에서는 **ipaserver** 호스트 그룹으로 설정합니다.
   b. *(선택 사항)* IdM 서버의 백업 사본을 유지하려면 다음 행의 주석을 제거하십시오.

```
# ipabackup_keep_on_server: yes
```

6. 기본적으로 백업은 Ansible 컨트롤러의 현재 작업 디렉터리에 저장됩니다. 1단계에서 만든 백업 디렉터리를 지정하려면 **ipabackup_controller_path** 변수를 추가하고 **/home/user/ipabackups** 디렉터리로 설정합니다.

```
---
- name: Playbook to backup IPA server to controller
  hosts: ipaserver
  become: true
  vars:
    ipabackup_to_controller: yes
    # ipabackup_keep_on_server: yes
    ipabackup_controller_path: /home/user/ipabackups

  roles:
  - role: ipabackup
    state: present
```

7. 파일을 저장합니다.
8. 인벤토리 파일 및 플레이북 파일을 지정하여 Ansible 플레이북을 실행합니다.

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory backup-my-server-to-my-controller.yml
```

검증 단계

- 백업이 Ansible 컨트롤러의 **/home/user/ipabackups** 디렉터리에 있는지 확인합니다.

```
[user@controller ~]$ ls /home/user/ipabackups
server.idm.example.com_ipa-full-2021-04-30-13-12-00
```

추가 리소스

- **ipabackup** 역할을 사용하는 샘플 Ansible Playbook은 다음을 참조하십시오.
  - **/usr/share/doc/ansible-freeipa/roles/ipabackup** 디렉토리의 **README.md** 파일입니다.
  - **/usr/share/doc/ansible-freeipa/playbooks/** 디렉토리

6.4. ANSIBLE을 사용하여 IDM 서버의 백업을 ANSIBLE 컨트롤러에 복사

다음 절차에서는 Ansible 플레이북을 사용하여 IdM 서버에서 Ansible 컨트롤러로 IdM 서버의 백업을 복사하는 방법을 설명합니다.

사전 요구 사항

- 다음 요구 사항을 충족하도록 Ansible 제어 노드를 구성했습니다.
  - Ansible 버전 2.14 이상을 사용하고 있습니다.
  - Ansible 컨트롤러에 **ansible-freeipa** 패키지가 설치되어 있습니다.
  - 이 예제에서는 ***~/MyPlaybook/*** 디렉터리에서 IdM 서버의 FQDN(정규화된 도메인 이름)을 사용하여 Ansible 인벤토리 파일을 생성했다고 가정합니다.
  - 이 예제에서는 **secret.yml** Ansible 자격 증명 모음이 **ipaadmin_password** 를 저장한다고 가정합니다.

절차

1. 백업을 저장하려면 Ansible 컨트롤러의 홈 디렉터리에 하위 디렉터리를 생성합니다.

```
$ mkdir ~/ipabackups
```

2. **~/MyPlaybook/** 디렉터리로 이동합니다.

```
$ cd ~/MyPlaybooks/
```

3. **/usr/share/doc/ansible-freeipa/playbooks** 디렉터리에 있는 **copy-backup-from-server.yml** 파일의 사본을 만듭니다.

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/copy-backup-from-server.yml copy-backup-from-my-server-to-my-controller.yml
```

4. 편집하려면 **copy-my-backup-from-my-server-to-my-controller.yml** 파일을 엽니다.

5. 다음 변수를 설정하여 파일을 조정합니다.

   a. **hosts** 변수를 인벤토리 파일의 호스트 그룹으로 설정합니다. 이 예에서는 **ipaserver** 호스트 그룹으로 설정합니다.

   b. **ipabackup_name** 변수를 Ansible 컨트롤러에 복사할 IdM 서버의 **ipabackup** 이름으로 설정합니다.

   c. 기본적으로 백업은 Ansible 컨트롤러의 현재 작업 디렉터리에 저장됩니다. 1단계에서 만든 디렉터리를 지정하려면 **ipabackup_controller_path** 변수를 추가하고 **/home/user/ipabackups** 디렉터리로 설정합니다.

```
---
- name: Playbook to copy backup from IPA server
  hosts: ipaserver
  become: true
  vars:
    ipabackup_name: ipa-full-2021-04-30-13-12-00
```

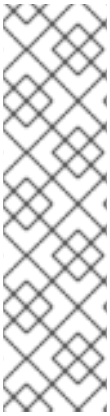
```
  ipabackup_to_controller: yes
  ipabackup_controller_path: /home/user/ipabackups

roles:
- role: ipabackup
  state: present
```

6. 파일을 저장합니다.

7. 인벤토리 파일 및 플레이북 파일을 지정하여 Ansible 플레이북을 실행합니다.

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory copy-backup-from-my-server-to-my-controller.yml
```



참고

모든 IdM 백업을 컨트롤러에 복사하려면 Ansible 플레이북의 **ipabackup_name** 변수를 **all**로 설정합니다.

```
vars:
  ipabackup_name: all
  ipabackup_to_controller: yes
```

예를 들어 **/usr/share/doc/ansible-freeipa/playbooks** 디렉터리의 **copy-all-backups-from-server.yml** Ansible 플레이북을 참조하십시오.

검증 단계

- 백업이 Ansible 컨트롤러의 **/home/user/ipabackups** 디렉터리에 있는지 확인합니다.

```
[user@controller ~]$ ls /home/user/ipabackups
server.idm.example.com_ipa-full-2021-04-30-13-12-00
```

추가 리소스

- **/usr/share/doc/ansible-freeipa/roles/ipabackup** 디렉토리의 **README.md** 파일입니다.
- **/usr/share/doc/ansible-freeipa/playbooks/** 디렉토리

6.5. ANSIBLE을 사용하여 ANSIBLE 컨트롤러에서 IDM 서버로 IDM 서버 백업 복사

다음 절차에서는 Ansible 플레이북을 사용하여 Ansible 컨트롤러에서 IdM 서버로 IdM 서버의 백업을 복사하는 방법을 설명합니다.

사전 요구 사항

- 다음 요구 사항을 충족하도록 Ansible 제어 노드를 구성했습니다.
  - Ansible 버전 2.14 이상을 사용하고 있습니다.
  - Ansible 컨트롤러에 **ansible-freeipa** 패키지가 설치되어 있습니다.

- 이 예제에서는 ***~/MyPlaybook/*** 디렉터리에서 IdM 서버의 FQDN(정규화된 도메인 이름)을 사용하여 Ansible 인벤토리 파일을 생성했다고 가정합니다.
- 이 예제에서는 **secret.yml** Ansible 자격 증명 모음이 **ipaadmin_password** 를 저장한다고 가정합니다.

절차

1. **~/MyPlaybook/** 디렉터리로 이동합니다.

```
$ cd ~/MyPlaybooks/
```

2. **/usr/share/doc/ansible-freeipa/playbooks** 디렉터리에 있는 **copy-backup-from-controller.yml** 파일의 사본을 만듭니다.

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/copy-backup-from-controller.yml copy-backup-from-my-controller-to-my-server.yml
```

3. 편집하려면 **copy-my-backup-from-my-controller-to-my-server.yml** 파일을 엽니다.
4. 다음 변수를 설정하여 파일을 조정합니다.
   a. **hosts** 변수를 인벤토리 파일의 호스트 그룹으로 설정합니다. 이 예에서는 **ipaserver** 호스트 그룹으로 설정합니다.
   b. **ipabackup_name** 변수를 IdM 서버에 복사할 Ansible 컨트롤러의 **ipabackup** 이름으로 설정합니다.

```
---
- name: Playbook to copy a backup from controller to the IPA server
  hosts: ipaserver
  become: true

  vars:
    ipabackup_name: server.idm.example.com_ipa-full-2021-04-30-13-12-00
    ipabackup_from_controller: yes

  roles:
  - role: ipabackup
    state: copied
```

5. 파일을 저장합니다.
6. 인벤토리 파일 및 플레이북 파일을 지정하여 Ansible 플레이북을 실행합니다.

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory copy-backup-from-my-controller-to-my-server.yml
```

추가 리소스

- **/usr/share/doc/ansible-freeipa/roles/ipabackup** 디렉토리의 **README.md** 파일입니다.
- **/usr/share/doc/ansible-freeipa/playbooks/** 디렉토리

6.6. ANSIBLE을 사용하여 IDM 서버에서 백업 제거

다음 절차에서는 Ansible 플레이북을 사용하여 IdM 서버에서 백업을 제거하는 방법을 설명합니다.

사전 요구 사항

- 다음 요구 사항을 충족하도록 Ansible 제어 노드를 구성했습니다.
  - Ansible 버전 2.14 이상을 사용하고 있습니다.
  - Ansible 컨트롤러에 **ansible-freeipa** 패키지가 설치되어 있습니다.
  - 이 예제에서는 ***~/MyPlaybook/*** 디렉터리에서 IdM 서버의 FQDN(정규화된 도메인 이름)을 사용하여 Ansible 인벤토리 파일을 생성했다고 가정합니다.
  - 이 예제에서는 **secret.yml** Ansible 자격 증명 모음이 **ipaadmin_password** 를 저장한다고 가정합니다.

절차

1. ~/MyPlaybook/ 디렉터리로 이동합니다.

```
$ cd ~/MyPlaybooks/
```

2. **/usr/share/doc/ansible-freeipa/playbooks** 디렉터리에 있는 **remove-backup-from-server.yml** 파일의 사본을 만듭니다.

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/remove-backup-from-server.yml remove-backup-from-my-server.yml
```

3. 편집할 **remove-backup-from-my-server.yml** 파일을 엽니다.
4. 다음 변수를 설정하여 파일을 조정합니다.
   a. **hosts** 변수를 인벤토리 파일의 호스트 그룹으로 설정합니다. 이 예에서는 **ipaserver** 호스트 그룹으로 설정합니다.
   b. IdM 서버에서 삭제하도록 **ipabackup_name** 변수를 **ipabackup** 으로 설정합니다.

```
---
- name: Playbook to remove backup from IPA server
  hosts: ipaserver
  become: true

  vars:
    ipabackup_name: ipa-full-2021-04-30-13-12-00

  roles:
  - role: ipabackup
    state: absent
```

5. 파일을 저장합니다.
6. 인벤토리 파일 및 플레이북 파일을 지정하여 Ansible 플레이북을 실행합니다.

```
$ ansible-playbook --vault-password-file=password_file -v -i ~/MyPlaybooks/inventory
remove-backup-from-my-server.yml
```

참고

IdM 서버에서 **모든** IdM 백업을 제거하려면 Ansible 플레이북의 **ipabackup_name** 변수를 **all** 로 설정합니다.

```
vars:
  ipabackup_name: all
```

예를 들어 **/usr/share/doc/ansible-freeipa/playbooks** 디렉터리의 **remove-all-backups-from-server.yml** Ansible 플레이북을 참조하십시오.

추가 리소스

- **/usr/share/doc/ansible-freeipa/roles/ipabackup** 디렉토리의 **README.md** 파일입니다.
- **/usr/share/doc/ansible-freeipa/playbooks/** 디렉토리