Red Hat Enterprise Linux 9

Identity Management를 사용하여 재해 복구 수행

서버 또는 데이터 손실 후 IdM 복구

Last Updated: 2024-05-02

Red Hat Enterprise Linux 9 Identity Management를 사용하여 재해 복구 수행

서버 또는 데이터 손실 후 IdM 복구

법적 공지

초록

예를 들어 하드웨어 오류로 인한 서버 및 데이터 손실 시나리오는 IT 환경에서 가장 큰 위험 요소입니다. Red Hat IdM(Identity Management) 환경에서 이러한 이벤트가 발생하는 경우 복구 프로세스는 문제 유형, IdM 토폴로지 및 이러한 상황을 완화하기 위해 수행된 작업에 따라 달라집니다. 예를 들어 IdM 복제 토폴로지에서 단일 서버와 여러 서버를 복구할 수 있으며 IdM 백업 및 스냅샷을 사용하여 데이터를 복구할 수 있습니다. 복구 중 또는 이후에 DNS 서버 및 Kerberos 구성과 같은 클라이언트 설정을 조정해야 할 수 있습니다.

차례

보다 포괄적 수용을 위한 오픈 소스 용어 교체

Red Hat은 코드, 문서, 웹 속성에서 문제가 있는 용어를 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.

RED HAT 문서에 관한 피드백 제공

문서에 대한 피드백에 감사드립니다. 어떻게 개선할 수 있는지 알려주십시오.

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 시나리오

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

표 1.1. 서버 손실과 데이터 손실

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

2장. 복제를 사용하여 단일 서버 복구

단일 서버가 심각하게 중단되거나 손실된 경우 복제본이 여러 개 있으면 대체 복제본을 생성하고 이전 수준의 중복성을 신속하게 복원할 수 있습니다.

IdM 토폴로지에 통합 CA(인증 기관)가 포함된 경우 손상된 복제본을 제거하고 교체하는 단계는 CA 갱신 서버 및 기타 복제본에 따라 다릅니다.

2.1. CA 갱신 서버 손실에서 복구

CA(인증 기관) 갱신 서버가 손실된 경우 먼저 다른 CA 복제본을 승격하여 CA 갱신 서버 역할을 충족한 다음 교체 CA 복제본을 배포해야 합니다.

사전 요구 사항

- 배포 시 IdM의 내부 인증 기관(CA)을 사용합니다.
- 환경의 다른 복제본에는 CA 서비스가 설치되어 있습니다.

주의

다음과 같은 경우 IdM 배포를 복구할 수 없습니다.

1. CA 갱신 서버가 손실되었습니다.
2. 다른 서버에는 CA가 설치되어 있지 않습니다.
3. CA 역할이 있는 복제본의 백업이 없습니다.
   인증서 데이터가 보호되도록 CA 역할이 있는 복제본에서 백업을 생성하는 것이 중요합니다. 백업에서 생성 및 복원하는 방법에 대한 자세한 내용은 IdM 백업을 사용하여 데이터 손실 준비를 참조하십시오.

절차

1. 환경의 다른 복제본에서 해당 환경의 다른 CA 복제본을 승격하여 새 CA 갱신 서버 역할을 합니다. IdM CA 갱신 서버 변경 및 재설정 을 참조하십시오.
2. 환경의 다른 복제본에서 손실된 CA 갱신 서버에 대한 복제 계약을 제거합니다. CLI를 사용하여 토폴로지에서 서버 제거를 참조하십시오.
3. 새 CA 복제본을 설치하여 손실된 CA 복제본을 교체합니다. CA를 사용하여 IdM 복제본 설치를 참조하십시오.
4. 복제 토폴로지의 변경 사항을 반영하도록 DNS를 업데이트합니다. IdM DNS를 사용하면 DNS 서비스 레코드가 자동으로 업데이트됩니다.
5. IdM 클라이언트가 IdM 서버에 연결할 수 있는지 확인합니다. 복구 중에 IdM 클라이언트 조정을 참조하십시오.

검증 단계

1. Kerberos ticket-Granting-Ticket를 IdM 사용자로 성공적으로 검색하여 새 복제본에서 Kerberos 서버를 테스트합니다.

```
[root@server ~]# kinit admin
Password for admin@EXAMPLE.COM:

[root@server ~]# klist
Ticket cache: KCM:0
Default principal: admin@EXAMPLE.COM

Valid starting       Expires              Service principal
10/31/2019 15:51:37  11/01/2019 15:51:02  HTTP/server.example.com@EXAMPLE.COM
10/31/2019 15:51:08  11/01/2019 15:51:02  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

2. 사용자 정보를 검색하여 Directory Server 및 SSSD 구성을 테스트합니다.

```
[root@server ~]# ipa user-show admin
  User login: admin
  Last name: Administrator
  Home directory: /home/admin
  Login shell: /bin/bash
  Principal alias: admin@EXAMPLE.COM
  UID: 1965200000
  GID: 1965200000
  Account disabled: False
  Password: True
  Member of groups: admins, trust admins
  Kerberos keys available: True
```

3. **ipa cert-show** 명령을 사용하여 CA 구성을 테스트합니다.

```
[root@server ~]# ipa cert-show 1
  Issuing CA: ipa
  Certificate: MIIEgjCCAuqgAwIBAgIjoSIP...
  Subject: CN=Certificate Authority,O=EXAMPLE.COM
  Issuer: CN=Certificate Authority,O=EXAMPLE.COM
  Not Before: Thu Oct 31 19:43:29 2019 UTC
  Not After: Mon Oct 31 19:43:29 2039 UTC
  Serial number: 1
  Serial number (hex): 0x1
  Revoked: False
```

추가 리소스

- IdM CA 갱신 서버 사용

2.2. 일반 복제본 손실에서 복구

CA(인증 기관) 갱신 서버가 아닌 복제본을 교체하려면 토폴로지에서 손실된 복제본을 제거하고 해당 위치에 새 복제본을 설치합니다.

사전 요구 사항

- CA 갱신 서버가 제대로 작동합니다. CA 갱신 서버가 손실된 경우 복구가 CA 갱신 서버 손실에서 참조하십시오.

절차

1. 손실된 서버에 대한 복제 계약 제거. IdM 서버 제거를 참조하십시오.
2. 원하는 서비스(CA, KRA, DNS)를 사용하여 새 복제본을 배포합니다. IdM 복제본 설치를 참조하십시오.
3. 복제 토폴로지의 변경 사항을 반영하도록 DNS를 업데이트합니다. IdM DNS를 사용하면 DNS 서비스 레코드가 자동으로 업데이트됩니다.
4. IdM 클라이언트가 IdM 서버에 연결할 수 있는지 확인합니다. 복구 중에 IdM 클라이언트 조정을 참조하십시오.

검증 단계

1. Kerberos ticket-Granting-Ticket를 IdM 사용자로 성공적으로 검색하여 새 복제본에서 Kerberos 서버를 테스트합니다.

```
[root@newreplica ~]# kinit admin
Password for admin@EXAMPLE.COM:

[root@newreplica ~]# klist
Ticket cache: KCM:0
Default principal: admin@EXAMPLE.COM

Valid starting       Expires              Service principal
10/31/2019 15:51:37  11/01/2019 15:51:02  HTTP/server.example.com@EXAMPLE.COM
10/31/2019 15:51:08  11/01/2019 15:51:02  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

2. 사용자 정보를 검색하여 새 복제본에서 Directory Server 및 SSSD 구성을 테스트합니다.

```
[root@newreplica ~]# ipa user-show admin
  User login: admin
  Last name: Administrator
  Home directory: /home/admin
  Login shell: /bin/bash
  Principal alias: admin@EXAMPLE.COM
  UID: 1965200000
  GID: 1965200000
  Account disabled: False
  Password: True
  Member of groups: admins, trust admins
  Kerberos keys available: True
```

3장. 복제를 사용하여 여러 서버 복구

여러 서버가 동시에 손실되는 경우 다음 5가지 시나리오 중 어느 것이 귀하의 상황에 적용되는지 확인하여 환경을 다시 빌드할 수 있는지 확인합니다.

3.1. CA가 없는 배포에서 여러 서버 손실에서 복구

CA가 없는 배포의 서버는 모두 동일하게 간주되므로 손실된 복제본을 임의의 순서로 제거하고 교체하여 환경을 다시 빌드할 수 있습니다.

사전 요구 사항

- 배포 시 외부 CA(인증 기관)를 사용합니다.

절차

- 복구가 일반 복제본 손실에서 참조하십시오.

3.2. CA 갱신 서버가 심각하지 않은 경우 여러 서버 손실에서 복구

CA 갱신 서버가 손상되지 않은 경우 다른 서버를 임의의 순서로 교체할 수 있습니다.

사전 요구 사항

- 배포에서 IdM 내부 인증 기관(CA)을 사용합니다.

절차

- 복구가 일반 복제본 손실에서 참조하십시오.

3.3. CA 갱신 서버 및 기타 서버 손실에서 복구

CA 갱신 서버 및 기타 서버가 손실되면 다른 복제본을 교체하기 전에 다른 CA 서버를 CA 갱신 서버 역할로 승격합니다.

사전 요구 사항

- 배포에서 IdM 내부 인증 기관(CA)을 사용합니다.
- 하나 이상의 CA 복제본이 손상되지 않습니다.

절차

1. 다른 CA 복제본을 승격하여 CA 갱신 서버 역할을 수행합니다. 복구가 CA 갱신 서버 손실에서 참조하십시오.
2. 손실된 다른 모든 복제본을 교체합니다. 복구가 일반 복제본 손실에서 참조하십시오.

3.4. 모든 CA 복제본 손실에서 복구

CA(인증 기관) 복제본이 없으면 IdM 환경에서 추가 복제본을 배포하고 자체적으로 다시 빌드할 수 있는 기능이 손실되었습니다.

사전 요구 사항

- 배포에서 IdM 내부 인증 기관(CA)을 사용합니다.

절차

- 이 상황은 완전한 손실입니다.

추가 리소스

- 전체 인프라 손실을 준비하려면 VM 스냅샷으로 데이터 손실 준비 .

3.5. 전체 인프라 손실에서 복구

모든 서버가 한 번에 손실되고 복원할 VM(가상 머신) 스냅샷 또는 데이터 백업이 없는 경우 이 상황을 복구할 수 없습니다.

절차

- 이 상황은 완전한 손실입니다.

추가 리소스

- VM 스냅샷으로 데이터 손실 준비 .

4장. VM 스냅샷을 사용하여 데이터 손실 복구

데이터 손실 이벤트가 발생하면 CA(인증 기관) 복제본의 VM(가상 머신) 스냅샷을 복원하여 손실된 데이터를 복구하거나 새 환경을 배포할 수 있습니다.

4.1. VM 스냅샷에서만 복구

재해가 모든 IdM 서버에 영향을 미치고 IdM CA 복제본 가상 머신(VM)의 스냅샷만 남은 경우 손실된 서버에 대한 모든 참조를 제거하고 새 복제본을 설치하여 배포를 다시 생성할 수 있습니다.

사전 요구 사항

- CA 복제본 VM의 VM 스냅샷을 준비했습니다. VM 스냅샷으로 데이터 손실 준비를 참조하십시오.

절차

1. CA 복제본 VM의 원하는 스냅샷을 부팅합니다.
2. 손실된 복제본에 대한 복제 계약을 제거합니다.

```
[root@server ~]# ipa server-del lost-server1.example.com
[root@server ~]# ipa server-del lost-server2.example.com
...
```

3. 두 번째 CA 복제본을 설치합니다. IdM 복제본 설치를 참조하십시오.
4. 이제 VM CA 복제본이 CA 갱신 서버입니다. Red Hat은 환경에서 다른 CA 복제본을 승격하여 CA 갱신 서버 역할을 하는 것이 좋습니다. IdM CA 갱신 서버 변경 및 재설정 을 참조하십시오.
5. 원하는 서비스(CA, DNS)를 사용하여 추가 복제본을 배포하여 원하는 복제본 토폴로지를 다시 생성합니다. IdM 복제본 설치를 참조하십시오.
6. 새 복제본 토폴로지를 반영하도록 DNS를 업데이트합니다. IdM DNS를 사용하면 DNS 서비스 레코드가 자동으로 업데이트됩니다.
7. IdM 클라이언트가 IdM 서버에 연결할 수 있는지 확인합니다. 복구 중에 IdM 클라이언트 조정을 참조하십시오.

검증 단계

1. Kerberos 티켓 통합 티켓을 IdM 사용자로 성공적으로 검색하여 모든 복제본에서 Kerberos 서버를 테스트합니다.

```
[root@server ~]# kinit admin
Password for admin@EXAMPLE.COM:

[root@server ~]# klist
Ticket cache: KCM:0
Default principal: admin@EXAMPLE.COM

Valid starting       Expires              Service principal
10/31/2019 15:51:37  11/01/2019 15:51:02  HTTP/server.example.com@EXAMPLE.COM
10/31/2019 15:51:08  11/01/2019 15:51:02  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

2. 사용자 정보를 검색하여 모든 복제본에서 Directory Server 및 SSSD 구성을 테스트합니다.

```
[root@server ~]# ipa user-show admin
  User login: admin
  Last name: Administrator
  Home directory: /home/admin
  Login shell: /bin/bash
  Principal alias: admin@EXAMPLE.COM
  UID: 1965200000
  GID: 1965200000
  Account disabled: False
  Password: True
  Member of groups: admins, trust admins
  Kerberos keys available: True
```

3. **ipa cert-show** 명령을 사용하여 모든 CA 복제본에서 CA 서버를 테스트합니다.

```
[root@server ~]# ipa cert-show 1
  Issuing CA: ipa
  Certificate: MIIEgjCCAuqgAwIBAgIjoSIP...
  Subject: CN=Certificate Authority,O=EXAMPLE.COM
  Issuer: CN=Certificate Authority,O=EXAMPLE.COM
  Not Before: Thu Oct 31 19:43:29 2019 UTC
  Not After: Mon Oct 31 19:43:29 2039 UTC
  Serial number: 1
  Serial number (hex): 0x1
  Revoked: False
```

추가 리소스

- 복제본 토폴로지 계획.

4.2. 부분적으로 작업 중인 환경에서 VM 스냅샷에서 복구

기타 기능이 제대로 작동하는 동안 일부 IdM 서버에 재해가 영향을 미치는 경우 VM(가상 머신) 스냅샷에서 캡처된 상태로 배포를 복원할 수 있습니다. 예를 들어 다른 복제본이 프로덕션 상태에 있는 동안 모든 CA(인증 기관) 복제본이 손실되는 경우 해당 환경으로 CA Replica을 다시 가져와야 합니다.

이 시나리오에서는 손실된 복제본에 대한 참조를 제거하고, 스냅샷에서 CA 복제본을 복원하고, 복제를 확인하고, 새 복제본을 배포합니다.

사전 요구 사항

- CA 복제본 VM의 VM 스냅샷을 준비했습니다. VM 스냅샷으로 데이터 손실 준비를 참조하십시오.

절차

1. 손실된 서버에 대한 모든 복제 계약을 제거합니다. IdM 서버 제거를 참조하십시오.
2. CA 복제본 VM의 원하는 스냅샷을 부팅합니다.
3. 복원된 서버와 손실된 서버 간의 복제 계약을 모두 제거합니다.

```
[root@restored-CA-replica ~]# ipa server-del lost-server1.example.com
[root@restored-CA-replica ~]# ipa server-del lost-server2.example.com
...
```

4. 복원된 서버에 아직 프로덕션 중인 서버에 복제 계약이 없는 경우 복원된 서버를 다른 서버와 연결하여 복원된 서버를 업데이트합니다.

```
[root@restored-CA-replica ~]# ipa topologysegment-add
Suffix name: domain
Left node: restored-CA-replica.example.com
Right node: server3.example.com
Segment name [restored-CA-replica.com-to-server3.example.com]: new_segment
--------------------------
Added segment "new_segment"
--------------------------
  Segment name: new_segment
  Left node: restored-CA-replica.example.com
  Right node: server3.example.com
  Connectivity: both
```

5. **/var/log/dirsrv/slapd-YOUR-INSTANCE/errors** 에서 Directory Server 오류 로그를 검토하여 스냅샷의 CA 복제본이 나머지 IdM 서버와 올바르게 동기화되는지 확인합니다.

6. 데이터베이스가 너무 오래되어 복원된 서버의 복제가 실패하면 복원된 서버를 다시 초기화합니다.If replication on the restored server fails because its database is too older, reinitialize the restored server.

```
[root@restored-CA-replica ~]# ipa-replica-manage re-initialize --from
server2.example.com
```

7. 복원된 서버의 데이터베이스가 올바르게 동기화된 경우 IdM 복제본 설치에 따라 원하는 서비스(CA, DNS)를 사용하여 추가 복제본 을 계속 배포합니다.

검증 단계

1. Kerberos 티켓 통합 티켓을 IdM 사용자로 성공적으로 검색하여 모든 복제본에서 Kerberos 서버를 테스트합니다.

```
[root@server ~]# kinit admin
Password for admin@EXAMPLE.COM:

[root@server ~]# klist
Ticket cache: KCM:0
Default principal: admin@EXAMPLE.COM

Valid starting       Expires              Service principal
10/31/2019 15:51:37  11/01/2019 15:51:02  HTTP/server.example.com@EXAMPLE.COM
10/31/2019 15:51:08  11/01/2019 15:51:02  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

2. 사용자 정보를 검색하여 모든 복제본에서 Directory Server 및 SSSD 구성을 테스트합니다.

```
[root@server ~]# ipa user-show admin
  User login: admin
  Last name: Administrator
```

```
Home directory: /home/admin
Login shell: /bin/bash
Principal alias: admin@EXAMPLE.COM
UID: 1965200000
GID: 1965200000
Account disabled: False
Password: True
Member of groups: admins, trust admins
Kerberos keys available: True
```

3. **ipa cert-show** 명령을 사용하여 모든 CA 복제본에서 CA 서버를 테스트합니다.

```
[root@server ~]# ipa cert-show 1
  Issuing CA: ipa
  Certificate: MIIEgjCCAuqgAwIBAgIjoSIP...
  Subject: CN=Certificate Authority,O=EXAMPLE.COM
  Issuer: CN=Certificate Authority,O=EXAMPLE.COM
  Not Before: Thu Oct 31 19:43:29 2019 UTC
  Not After: Mon Oct 31 19:43:29 2039 UTC
  Serial number: 1
  Serial number (hex): 0x1
  Revoked: False
```

추가 리소스

- VM 스냅샷에서 복구하여 새로운 IdM 환경을 구축합니다 .

4.3. VM 스냅샷에서 복구하여 새 IDM 환경 설정

복원된 VM(가상 머신) 스냅샷의 CA(인증 기관) 복제본이 다른 서버와 함께 복제할 수 없는 경우 VM 스냅샷에서 새 IdM 환경을 생성합니다.

새 IdM 환경을 설정하려면 VM 서버를 분리하고 추가 복제본을 생성한 다음 IdM 클라이언트를 새 환경으로 전환합니다.

사전 요구 사항

- CA 복제본 VM의 VM 스냅샷을 준비했습니다. VM 스냅샷으로 데이터 손실 준비를 참조하십시오.

절차

1. CA 복제본 VM의 원하는 스냅샷을 부팅합니다.
2. 모든 복제 토폴로지 세그먼트를 제거하여 현재 배포의 나머지 부분에서 복원된 서버를 분리합니다.
   a. 먼저 모든 **도메인** 복제 토폴로지 세그먼트를 표시합니다.

```
[root@restored-CA-replica ~]# ipa topologysegment-find
Suffix name: domain
------------------
8 segments matched
------------------
  Segment name: new_segment
```

```
  Left node: restored-CA-replica.example.com
  Right node: server2.example.com
  Connectivity: both

...

----------------------------
Number of entries returned 8
----------------------------
```

b. 다음으로 복원된 서버를 포함하는 모든 **도메인** 토폴로지 세그먼트를 삭제합니다.

```
[root@restored-CA-replica ~]# ipa topologysegment-del
Suffix name: domain
Segment name: new_segment
----------------------------
Deleted segment "new_segment"
----------------------------
```

c. 마지막으로 모든 **ca** 토폴로지 세그먼트를 사용하여 동일한 작업을 수행합니다.

```
[root@restored-CA-replica ~]# ipa topologysegment-find
Suffix name: ca
------------------
1 segments matched
------------------
  Segment name: ca_segment
  Left node: restored-CA-replica.example.com
  Right node: server4.example.com
  Connectivity: both
----------------------------
Number of entries returned 1
----------------------------

[root@restored-CA-replica ~]# ipa topologysegment-del
Suffix name: ca
Segment name: ca_segment
----------------------------
Deleted segment "ca_segment"
----------------------------
```

3. 복원된 서버에서 충분한 IdM 복제본을 설치하여 배포 로드를 처리합니다. 이제 두 개의 연결이 끊긴 IdM 배포가 병렬로 실행됩니다.

4. 새 IdM 복제본에 대한 하드 코딩 참조를 적용하여 IdM 클라이언트를 전환하여 새 배포를 사용합니다. 복구 중에 IdM 클라이언트 조정을 참조하십시오.

5. 이전 배포에서 IdM 서버를 중지하고 설치 제거합니다. IdM 서버 제거를 참조하십시오.

검증 단계

1. Kerberos 티켓 통합 티켓을 IdM 사용자로 성공적으로 검색하여 모든 새 복제본에서 Kerberos 서버를 테스트합니다.

```
[root@server ~]# kinit admin
```

```
Password for admin@EXAMPLE.COM:

[root@server ~]# klist
Ticket cache: KCM:0
Default principal: admin@EXAMPLE.COM

Valid starting       Expires              Service principal
10/31/2019 15:51:37  11/01/2019 15:51:02  HTTP/server.example.com@EXAMPLE.COM
10/31/2019 15:51:08  11/01/2019 15:51:02  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

2. 사용자 정보를 검색하여 모든 새 복제본에서 Directory Server 및 SSSD 구성을 테스트합니다.

```
[root@server ~]# ipa user-show admin
  User login: admin
  Last name: Administrator
  Home directory: /home/admin
  Login shell: /bin/bash
  Principal alias: admin@EXAMPLE.COM
  UID: 1965200000
  GID: 1965200000
  Account disabled: False
  Password: True
  Member of groups: admins, trust admins
  Kerberos keys available: True
```

3. **ipa cert-show** 명령을 사용하여 모든 새 CA 복제본에서 CA 서버를 테스트합니다.

```
[root@server ~]# ipa cert-show 1
  Issuing CA: ipa
  Certificate: MIIEgjCCAuqgAwIBAgIjoSIP...
  Subject: CN=Certificate Authority,O=EXAMPLE.COM
  Issuer: CN=Certificate Authority,O=EXAMPLE.COM
  Not Before: Thu Oct 31 19:43:29 2019 UTC
  Not After: Mon Oct 31 19:43:29 2039 UTC
  Serial number: 1
  Serial number (hex): 0x1
  Revoked: False
```

5장. IDM 백업을 사용하여 데이터 손실 복구

ipa-restore 유틸리티를 사용하여 IdM 서버를 IdM 백업에 캡처된 이전 상태로 복원할 수 있습니다.

5.1. IDM 백업에서 복원하는 경우

IdM 백업에서 복원하여 여러 재해 시나리오에 응답할 수 있습니다.

- **LDAP 콘텐츠의 바람직하지 않은 변경 사항이** 적용되었습니다. : Entries가 변경되거나 삭제되어 배포 전체에서 복제가 수행되었으며 이러한 변경 사항을 되돌리려고 합니다. 데이터 전용 백업을 복원하면 IdM 구성 자체에 영향을 주지 않고 LDAP 항목이 이전 상태로 반환됩니다.
- **Total Infrastructure Losss, or loss of all CA instances** 재해가 모든 인증 기관 복제본을 손상시키는 경우 추가 서버를 배포하여 다시 빌드할 수 있는 기능이 손실되었습니다. 이 경우 CA Replica의 백업을 복원하고 새 복제본을 빌드합니다.
- **격리된 서버의 업그레이드 실패**: 운영 체제가 계속 작동하지만 IdM 데이터는 손상되므로 IdM 시스템을 알려진 양호한 상태로 복원하려고 합니다. 기술 지원을 사용하여 문제를 진단하고 해결할 것을 권장합니다. 이러한 작업이 실패하면 전체 서버 백업에서 복원하십시오.

중요

하드웨어 또는 업그레이드 실패에 대한 기본 솔루션은 손실된 서버를 복제본에서 다시 빌드하는 것입니다. 자세한 내용은 복제가 있는 단일 서버 복구를 참조하십시오.

5.2. IDM 백업에서 복원할 때 고려 사항

ipa-backup 유틸리티를 사용하여 생성된 백업이 있는 경우 IdM 서버 또는 LDAP 콘텐츠를 백업이 수행될 때 있는 상태로 복원할 수 있습니다.

IdM 백업에서 복원하는 동안 고려해야 할 주요 사항은 다음과 같습니다.

- 백업이 원래 생성된 서버의 구성과 일치하는 서버에서 백업만 복원할 수 있습니다. 서버에는 다음이 **있어야 합니다**.
  - 동일한 호스트 이름
  - 동일한 IP 주소
  - IdM 소프트웨어의 동일한 버전
- 많은 중 하나의 IdM 서버가 복원되면 복원된 서버는 IdM의 유일한 정보 소스가 됩니다. 다른 모든 서버는 복원된 서버에서 다시 초기화 **해야 합니다**.
- 마지막 백업 이후에 생성된 데이터는 손실되므로 백업을 사용하지 말고 정상적인 시스템 유지 관리를 위해 백업 및 복원 솔루션을 사용하지 마십시오.
- 서버가 손실되면 백업에서 복원하지 않고 서버를 다시 설치하여 서버를 다시 설치하는 것이 좋습니다. 새 복제본을 생성하면 현재 작업 환경의 데이터가 유지됩니다. 자세한 내용은 복제를 사용하여 서버 손실 준비 항목을 참조하십시오.
- 백업 및 복원 기능은 명령줄에서만 관리할 수 있으며 IdM 웹 UI에서 사용할 수 없습니다.

- **/tmp** 또는 **/var/tmp** 디렉터리에 있는 백업 파일에서는 복원할 수 없습니다. IdM 디렉터리 서버는 PrivateTmp 디렉터리를 사용하며 운영 체제에서 일반적으로 사용할 수 있는 **/tmp** 또는 **/var/tmp** 디렉터리에 액세스할 수 없습니다.

작은 정보

백업에서 복원하려면 백업이 수행될 때 설치된 대상 호스트에 동일한 소프트웨어(RPM) 버전이 필요합니다. 이로 인해 Red Hat은 백업이 아닌 가상 머신 스냅샷에서 복원할 것을 권장합니다. 자세한 내용은 VM 스냅샷 복구에서 데이터 손실을 참조하십시오.

5.3. 백업에서 IDM 서버 복원

다음 절차에서는 IdM 백업에서 IdM 서버 또는 해당 LDAP 데이터를 복원하는 방법을 설명합니다.

그림 5.1. 이 예에서 사용되는 복제 토폴로지

표 5.1. 이 예제에서 사용되는 서버 이름 지정 규칙

서버 호스트 이름	함수
server1.example.com	백업에서 복원해야 하는 서버입니다.
caReplica2.example.com	**server1.example.com** 호스트에 연결된 CA(인증 기관) 복제본입니다.
replica3.example.com	**caReplica2.example.com** 호스트에 연결된 복제본입니다.

사전 요구 사항

- **ipa-backup** 유틸리티를 사용하여 IdM 서버의 전체 서버 또는 데이터 전용 백업을 생성했습니다. 백업 생성을 참조하십시오.
- 백업 파일은 **/tmp** 또는 **/var/tmp** 디렉토리에 없습니다.
- 전체 서버 백업에서 전체 서버 복원을 수행하기 전에 서버에서 IdM을 제거하고 이전과 동일한 서버 구성을 사용하여 IdM을 다시 설치합니다.

절차

1. **ipa-restore** 유틸리티를 사용하여 전체 서버 또는 데이터 전용 백업을 복원합니다.
   - 백업 디렉터리가 기본 **/var/lib/ipa/backup/** 위치에 있는 경우 디렉터리 이름만 입력합니다.

```
[root@server1 ~]# ipa-restore ipa-full-2020-01-14-12-02-32
```

- 백업 디렉터리가 기본 위치에 없는 경우 전체 경로를 입력합니다.

```
[root@server1 ~]# ipa-restore /mybackups/ipa-data-2020-02-01-05-30-00
```

참고

ipa-restore 유틸리티는 디렉터리에서 포함하는 백업 유형을 자동으로 감지하고 기본적으로 동일한 유형의 복원을 수행합니다. 전체 서버 백업에서 데이터 전용 복원을 수행하려면 **ipa-restore** 명령에 **--data** 옵션을 추가합니다.

```
[root@server1 ~]# ipa-restore --data ipa-full-2020-01-14-12-02-32
```

2. Directory Manager 암호를 입력합니다.

```
Directory Manager (existing master) password:
```

3. **yes** 를 입력하여 현재 데이터를 백업으로 덮어쓰는 것을 확인합니다.

```
Preparing restore from /var/lib/ipa/backup/ipa-full-2020-01-14-12-02-32 on
server1.example.com
Performing FULL restore from FULL backup
Temporary setting umask to 022
Restoring data will overwrite existing live data. Continue to restore? [no]: yes
```

4. **ipa-restore** 유틸리티는 사용 가능한 모든 서버에서 복제를 비활성화합니다.

```
Each master will individually need to be re-initialized or
re-created from this one. The replication agreements on
masters running IPA 3.1 or earlier will need to be manually
re-enabled. See the man page for details.
Disabling all replication.
Disabling replication agreement on server1.example.com to caReplica2.example.com
Disabling CA replication agreement on server1.example.com to caReplica2.example.com
Disabling replication agreement on caReplica2.example.com to server1.example.com
Disabling replication agreement on caReplica2.example.com to replica3.example.com
Disabling CA replication agreement on caReplica2.example.com to server1.example.com
Disabling replication agreement on replica3.example.com to caReplica2.example.com
```

그런 다음 유틸리티를 통해 IdM 서비스를 중지하고 백업을 복원한 다음 서비스를 다시 시작합니다.

```
Stopping IPA services
Systemwide CA database updated.
Restoring files
Systemwide CA database updated.
Restoring from userRoot in EXAMPLE-COM
Restoring from ipaca in EXAMPLE-COM
Restarting GSS-proxy
Starting IPA services
Restarting SSSD
Restarting oddjobd
Restoring umask to 18
The ipa-restore command was successful
```

-

5. 복원된 서버에 연결된 모든 복제본을 다시 초기화합니다.

   a. **도메인** 접미사의 모든 복제 토폴로지 세그먼트를 나열하고 복원된 서버와 관련된 토폴로지 세그먼트를 기록합니다.

   ```
   [root@server1 ~]# ipa topologysegment-find domain
   ------------------
   2 segments matched
   ------------------
     Segment name: server1.example.com-to-caReplica2.example.com
     Left node: server1.example.com
     Right node: caReplica2.example.com
     Connectivity: both

     Segment name: caReplica2.example.com-to-replica3.example.com
     Left node: caReplica2.example.com
     Right node: replica3.example.com
     Connectivity: both
   ----------------------------
   Number of entries returned 2
   ----------------------------
   ```

   b. 복원된 서버를 사용하여 모든 토폴로지 세그먼트에 대한 **도메인** 접미사를 다시 초기화합니다.
   이 예에서는 **server1** 의 데이터를 사용하여 **caReplica2** 의 다시 초기화를 수행합니다.

   ```
   [root@caReplica2 ~]# ipa-replica-manage re-initialize --from=server1.example.com
   Update in progress, 2 seconds elapsed
   Update succeeded
   ```

   c. 인증 기관 데이터로 이동하여 **ca** 접미사의 모든 복제 토폴로지 세그먼트를 나열합니다.

   ```
   [root@server1 ~]# ipa topologysegment-find ca
   -----------------
   1 segment matched
   -----------------
     Segment name: server1.example.com-to-caReplica2.example.com
     Left node: server1.example.com
     Right node: caReplica2.example.com
     Connectivity: both
   ----------------------------
   Number of entries returned 1
   ----------------------------
   ```

   d. 복원된 서버에 연결된 모든 CA 복제본을 다시 초기화합니다.
   이 예에서는 **server1** 의 데이터를 사용하여 **csreplica** 2의 re-initialization of **caReplica2** 를 수행합니다.

   ```
   [root@caReplica2 ~]# ipa-csreplica-manage re-initialize --
   from=server1.example.com
   Directory Manager password:

   Update in progress, 3 seconds elapsed
   Update succeeded
   ```

6. 복원된 **server1.example.com** 에서 데이터로 모든 서버가 업데이트될 때까지 복제 토폴로지를 계속하여 연속 복제본을 다시 시작합니다.
이 예제에서는 **caReplica2** 의 데이터가 포함된 **replica3** 에서 **도메인** 접미사만 다시 초기화해야 합니다.

```
[root@replica3 ~]# ipa-replica-manage re-initialize --from=caReplica2.example.com
Directory Manager password:

Update in progress, 3 seconds elapsed
Update succeeded
```

7. 잘못된 데이터로 인해 인증 문제를 방지하려면 모든 서버에서 SSSD의 캐시를 지우십시오.

   a. SSSD 서비스를 중지합니다.

   ```
   [root@server ~]# systemctl stop sssd
   ```

   b. SSSD에서 캐시된 모든 콘텐츠를 삭제합니다.

   ```
   [root@server ~]# sss_cache -E
   ```

   c. SSSD 서비스를 시작합니다.

   ```
   [root@server ~]# systemctl start sssd
   ```

   d. 서버를 재부팅합니다.

추가 리소스

- **ipa-restore(1)** 도움말 페이지는 복원 중에 복잡한 복제 시나리오를 처리하는 방법도 자세히 다룹니다.

5.4. 암호화된 백업에서 복원

이 절차에서는 암호화된 IdM 백업에서 IdM 서버를 복원합니다. **ipa-restore** 유틸리티는 IdM 백업이 암호화되었는지 자동으로 탐지하고 GPG2 루트 인증 키를 사용하여 복원합니다.

사전 요구 사항

- GPG 암호화 IdM 백업. 암호화된 IdM 백업 생성 을 참조하십시오.
- LDAP Directory Manager 암호
- GPG 키 생성 시 사용되는 암호

절차

1. GPG2 키를 생성할 때 사용자 정의 인증 키 위치를 사용한 경우 **$GNUPGHOME** 환경 변수가 해당 디렉터리로 설정되어 있는지 확인합니다. GPG2 키 생성을 참조하십시오.

```
[root@server ~]# echo $GNUPGHOME
/root/backup
```

2. **ipa-restore** 유틸리티를 백업 디렉터리 위치에 제공합니다.

```
[root@server ~]# ipa-restore ipa-full-2020-01-13-18-30-54
```

   a. Directory Manager 암호를 입력합니다.

```
Directory Manager (existing master) password:
```

   b. GPG 키를 생성할 때 사용한 암호를 입력합니다.

```
┌──────────────────────────────────────────────────────────────────────┐
│ Please enter the passphrase to unlock the OpenPGP secret key:        │
│ "GPG User (first key) <root@example.com>"                            │
│ 2048-bit RSA key, ID BF28FFA302EF4557,                               │
│ created 2020-01-13.                                                  │
│                                                                      │
│                                                                      │
│ Passphrase: <passphrase>                                             │
│                                                                      │
│       <OK>                          <Cancel>                         │
└──────────────────────────────────────────────────────────────────────┘
```

3. 복원된 서버에 연결된 모든 복제본을 다시 초기화합니다. 백업에서 IdM 서버 복원을 참조하십시오.

6장. ANSIBLE 플레이북을 사용하여 IDM 서버 복원

ipabackup Ansible 역할을 사용하면 백업에서 IdM 서버 복원을 자동화하고 서버와 Ansible 컨트롤러 간에 백업 파일을 전송할 수 있습니다.

이 섹션에서는 다음 주제를 다룹니다.

- IdM 관리를 위해 Ansible 제어 노드 준비
- Ansible을 사용하여 서버에 저장된 백업에서 IdM 서버 복원
- Ansible을 사용하여 Ansible 컨트롤러에 저장된 백업에서 IdM 서버 복원
- 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 서버에 저장된 백업에서 IDM 서버 복원

다음 절차에서는 Ansible 플레이북을 사용하여 해당 호스트에 저장된 백업에서 IdM 서버를 복원하는 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.
- **ansible-freeipa** 모듈이 실행되는 노드인 대상 노드는 IdM 도메인의 일부인 IdM 클라이언트, 서버 또는 복제본입니다.
- LDAP Directory Manager 암호를 알고 있습니다.

절차

1. **~/MyPlaybook/** 디렉터리로 이동합니다.

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

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

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

3. 편집할 **restore-my-server.yml** Ansible 플레이북 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 복원할 **ipabackup** 의 이름으로 설정합니다.
   c. **ipabackup_password** 변수를 LDAP Directory Manager 암호로 설정합니다.

```
---
- name: Playbook to restore an IPA server
  hosts: ipaserver
```

```
become: true

vars:
  ipabackup_name: ipa-full-2021-04-30-13-12-00
  ipabackup_password: <your_LDAP_DM_password>

roles:
- role: ipabackup
  state: restored
```

5. 파일을 저장합니다.

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

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

추가 리소스

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

6.3. ANSIBLE을 사용하여 ANSIBLE 컨트롤러에 저장된 백업에서 IDM 서버 복원

다음 절차에서는 Ansible 플레이북을 사용하여 Ansible 컨트롤러에 저장된 백업에서 IdM 서버를 복원하는 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.
- **ansible-freeipa** 모듈이 실행되는 노드인 대상 노드는 IdM 도메인의 일부인 IdM 클라이언트, 서버 또는 복제본입니다.
- LDAP Directory Manager 암호를 알고 있습니다.

절차

1. **~/MyPlaybook/** 디렉터리로 이동합니다.

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

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

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

3. 편집하려면 **restore-my-server-from-my-controller.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 복원할 **ipabackup** 의 이름으로 설정합니다.

   c. **ipabackup_password** 변수를 LDAP Directory Manager 암호로 설정합니다.

```
---
- name: Playbook to restore IPA server from controller
  hosts: ipaserver
  become: true

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

  roles:
  - role: ipabackup
    state: restored
```

5. 파일을 저장합니다.

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

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

추가 리소스

- **/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.

- **ansible-freeipa** 모듈이 실행되는 노드인 대상 노드는 IdM 도메인의 일부인 IdM 클라이언트, 서버 또는 복제본입니다.

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.
- **ansible-freeipa** 모듈이 실행되는 노드인 대상 노드는 IdM 도메인의 일부인 IdM 클라이언트, 서버 또는 복제본입니다.

절차

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.

- **ansible-freeipa** 모듈이 실행되는 노드인 대상 노드는 IdM 도메인의 일부인 IdM 클라이언트, 서버 또는 복제본입니다.

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

7장. 데이터 손실 관리

데이터 손실 이벤트에 대한 적절한 응답은 영향을 받는 복제본 수 및 손실된 데이터 유형에 따라 달라집니다.

7.1. 격리된 데이터 손실에 응답

데이터 손실 이벤트가 발생하면 즉시 영향을 받는 서버를 격리하여 데이터 손실을 최소화합니다. 그런 다음 환경의 영향을 받지 않는 나머지 환경에서 대체 복제본을 생성합니다.

사전 요구 사항

- 여러 복제본이 있는 강력한 IdM 복제 토폴로지입니다. 복제를 통한 서버 손실 준비를 참조하십시오.

절차

1. 데이터 손실을 복제하려면 복제 토폴로지 세그먼트를 제거하여 나머지 토폴로지에서 영향을 받는 모든 복제본의 연결을 끊습니다.

   a. 배포의 모든 **도메인** 복제 토폴로지 세그먼트를 표시합니다.

   ```
   [root@server ~]# ipa topologysegment-find
   Suffix name: domain
   ------------------
   8 segments matched
   ------------------
     Segment name: segment1
     Left node: server.example.com
     Right node: server2.example.com
     Connectivity: both

   ...

   ----------------------------
   Number of entries returned 8
   ----------------------------
   ```

   b. 영향을 받는 서버를 포함하는 모든 **도메인** 토폴로지 세그먼트를 삭제합니다.

   ```
   [root@server ~]# ipa topologysegment-del
   Suffix name: domain
   Segment name: segment1
   ----------------------------
   Deleted segment "segment1"
   ----------------------------
   ```

   c. 영향을 받는 서버를 포함하는 모든 **ca** 토폴로지 세그먼트에서 동일한 작업을 수행합니다.

   ```
   [root@server ~]# ipa topologysegment-find
   Suffix name: ca
   ------------------
   1 segments matched
   ------------------
   ```

```
  Segment name: ca_segment
  Left node: server.example.com
  Right node: server2.example.com
  Connectivity: both
----------------------------
Number of entries returned 1
----------------------------

[root@server ~]# ipa topologysegment-del
Suffix name: ca
Segment name: ca_segment
----------------------------
Deleted segment "ca_segment"
----------------------------
```

2. 데이터 손실의 영향을 받는 서버를 중단해야 합니다. 대체 복제본을 생성하려면 복제를 사용하여 여러 서버 복구를 참조하십시오.

7.2. 모든 서버간에 제한된 데이터 손실에 응답

데이터 손실 이벤트는 복제가 모든 서버에서 실수로 삭제되는 등 환경의 모든 복제본에 영향을 미칠 수 있습니다.A data loss event may affect all replicas in the environment, such as replication performing an accidental deletion between all servers. 데이터 손실이 알려지고 제한적이면 손실된 데이터를 수동으로 다시 추가합니다.

사전 요구 사항

- 손실된 데이터가 포함된 IdM 서버의 VM(가상 머신) 스냅샷 또는 IdM 백업입니다.

절차

1. 손실된 데이터를 검토해야 하는 경우 VM 스냅샷 또는 백업을 별도의 네트워크의 격리된 서버로 복원하십시오.
2. **ipa** 또는 **ldapadd** 명령을 사용하여 누락된 정보를 데이터베이스에 추가합니다.

추가 리소스

- VM 스냅샷을 사용하여 데이터 손실 복구 .
- IdM 백업 및 복원 .

7.3. 모든 서버간에 정의되지 않은 데이터 손실에 응답

데이터 손실이 심각하거나 정의되지 않은 경우 서버의 VM(가상 머신) 스냅샷에서 새 환경을 배포합니다.

사전 요구 사항

- VM(가상 머신) 스냅샷에는 손실된 데이터가 포함되어 있습니다.

절차

1. VM 스냅샷에서 알려진 양호한 상태로 IdM CA(인증 기관) 복제본을 복원하고 새 IdM 환경을 배포합니다. VM 스냅샷에서만 복구를 참조하십시오.

2. **ipa** 또는 **ldapadd** 명령을 사용하여 스냅샷을 만든 후 생성된 데이터를 추가합니다.

추가 리소스

- VM 스냅샷을 사용하여 데이터 손실 복구 .

8장. 복구 중 IDM 클라이언트 조정

IdM 서버를 복원하는 동안 복제본 토폴로지의 변경 사항을 반영하려면 IdM 클라이언트를 조정해야 할 수 있습니다.

절차

1. **DNS 설정 조정**:

   a. **/etc/hosts** 에 IdM 서버에 대한 참조가 포함되어 있는 경우 하드 코딩된 IP-hostname 매핑이 유효한지 확인하십시오.

   b. IdM 클라이언트가 이름 확인을 위해 IdM DNS를 사용하는 경우 **/etc/resolv.conf** 의 **nameserver** 항목이 DNS 서비스를 제공하는 IdM 복제본을 가리키는지 확인합니다.

2. **Kerberos 구성 조정**:

   a. 기본적으로 IdM 클라이언트는 Kerberos 서버의 DNS 서비스 레코드를 찾고 복제본 토폴로지의 변경 사항에 맞게 조정합니다.

   ```
   [root@client ~]# grep dns_lookup_kdc /etc/krb5.conf
     dns_lookup_kdc = true
   ```

   b. **/etc/krb5.conf** 에서 특정 IdM 서버를 사용하도록 IdM 클라이언트가 하드 코딩된 경우:

   ```
   [root@client ~]# grep dns_lookup_kdc /etc/krb5.conf
     dns_lookup_kdc = false
   ```

   /etc/krb5.conf 의 **kdc**,**master_kdc** 및 **admin_server** 항목이 제대로 작동하는 IdM 서버를 가리키는지 확인합니다.

   ```
   [realms]
    EXAMPLE.COM = {
     kdc = functional-server.example.com:88
     master_kdc = functional-server.example.com:88
     admin_server = functional-server.example.com:749
     default_domain = example.com
     pkinit_anchors = FILE:/var/lib/ipa-client/pki/kdc-ca-bundle.pem
     pkinit_pool = FILE:/var/lib/ipa-client/pki/ca-bundle.pem
    }
   ```

3. **SSSD 설정 조정**:

   a. 기본적으로 IdM 클라이언트는 LDAP 서버의 DNS 서비스 레코드를 살펴보고 복제본 토폴로지의 변경 사항에 맞게 조정합니다.

   ```
   [root@client ~]# grep ipa_server /etc/sssd/sssd.conf
   ipa_server = _srv_, functional-server.example.com
   ```

   b. IdM 클라이언트가 **/etc/sssd/sssd.conf** 에서 특정 IdM 서버를 사용하도록 하드 코딩된 경우 **ipa_server** 항목이 제대로 작동하는 IdM 서버를 가리키는지 확인하십시오.

   ```
   [root@client ~]# grep ipa_server /etc/sssd/sssd.conf
   ipa_server = functional-server.example.com
   ```

4. **SSSD의 캐시된 정보** 삭제:

   - SSSD 캐시에는 손실된 서버와 관련된 오래된 정보가 포함될 수 있습니다. 사용자에게 일관성 없는 인증 문제가 발생하는 경우 SSSD 캐시를 삭제합니다.

```
[root@client ~]# sss_cache -E
```

검증 단계

1. Kerberos ticket-Granting-Ticket를 IdM 사용자로 검색하여 Kerberos 구성을 확인합니다.

```
[root@client ~]# kinit admin
Password for admin@EXAMPLE.COM:

[root@client ~]# klist
Ticket cache: KCM:0
Default principal: admin@EXAMPLE.COM

Valid starting       Expires              Service principal
10/31/2019 18:44:58  11/25/2019 18:44:55  krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

2. IdM 사용자 정보를 검색하여 SSSD 구성을 확인합니다.

```
[root@client ~]# id admin
uid=1965200000(admin) gid=1965200000(admins) groups=1965200000(admins)
```