



Red Hat Enterprise Linux 9

Identity Management의 복제 관리

ID 관리 서버의 복제 토폴로지를 관리하는 가이드입니다.

Red Hat Enterprise Linux 9 Identity Management의 복제 관리

ID 관리 서버의 복제 토폴로지를 관리하는 가이드입니다.

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

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Managing_replication_in_Identity_Management.ent file |.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution-Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

초록

이 문서 컬렉션은 콘솔 및 WebUI에서 복제 계약을 설정하는 방법, Ansible을 사용하여 복제 토폴로지를 관리하는 방법, 숨겨진 복제본을 승격 및 시연하는 방법에 대한 지침을 제공합니다.

차례

보다 포괄적 수용을 위한 오픈 소스 용어 교체	3
RED HAT 문서에 관한 피드백 제공	4
1장. 복제 토폴로지 관리	5
1.1. 복제 계약, 토폴로지 접미사 및 토폴로지 세그먼트 설명	5
1.1.1. 복제 계약	5
1.1.2. 토폴로지 접미사	5
1.1.3. 토폴로지 세그먼트	6
1.2. 토폴로지 그래프를 사용하여 복제 토폴로지 관리	8
1.3. 웹 UI를 사용하여 두 서버 간 복제 설정	10
1.4. 웹 UI를 사용하여 두 서버 간 복제 중지	12
1.5. CLI를 사용하여 두 서버 간 복제 설정	13
1.6. CLI를 사용하여 두 서버 간 복제 중지	14
1.7. 웹 UI를 사용하여 토폴로지에서 서버 제거	15
1.8. CLI를 사용하여 토폴로지에서 서버 제거	16
1.9. 웹 UI를 사용하여 IDM 서버에서 서버 역할 보기	17
1.10. CLI를 사용하여 IDM 서버의 서버 역할 보기	17
1.11. 복제본을 CA 갱신 서버 및 CRL 게시자 서버로 승격	18
1.12. 숨겨진 복제본 검증 또는 승격	18
2장. ANSIBLE 플레이북을 사용하여 IDM을 관리하기 위한 환경 준비	20
3장. ANSIBLE을 사용하여 IDM의 복제 토폴로지 관리	22
3.1. ANSIBLE을 사용하여 IDM에 복제 계약이 있는지 확인	22
3.2. ANSIBLE을 사용하여 여러 IDM 복제본 간에 복제 계약이 존재하는지 확인	23
3.3. ANSIBLE을 사용하여 두 개의 복제본 간에 복제 계약이 있는지 확인합니다.	25
3.4. ANSIBLE을 사용하여 IDM에 토폴로지 접미사가 있는지 확인합니다.	27
3.5. ANSIBLE을 사용하여 IDM 복제본 다시 초기화	28
3.6. ANSIBLE을 사용하여 IDM에 복제 주석이 없는지 확인	30
3.7. 추가 리소스	32
4장. 숨겨진 복제본 검증 또는 승격	33
5장. 상태 점검을 사용하여 IDM 복제 확인	34
5.1. 복제 상태 테스트	34
5.2. HEALTHCHECK를 사용하여 복제 모니터링	34

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.

Identity Management에서 용어 교체는 다음과 같습니다.

- 블랙리스트를 **블록 목록**으로 대체
- 화이트리스트를 **허용 목록**으로 대체
- 슬레이브를 **보조**로 대체
- 컨텍스트에 따라 *마스터*라는 단어가 보다 정확한 용어로 교체되고 있습니다.
 - IdM 마스터를 **IdM 서버**로 대체
 - CA 갱신 마스터를 **CA 갱신 서버**로 대체
 - CRL 마스터를 **CRL 게시자 서버**로 대체
 - multi-master를 **multi-supplier**로 교체

RED HAT 문서에 관한 피드백 제공

문서 개선을 위한 의견을 보내 주십시오. Red Hat이 어떻게 이를 개선할 수 있는지 알려 주십시오.

- 특정 문구에 대한 간단한 의견 작성 방법은 다음과 같습니다.
 1. 문서가 *Multi-page HTML* 형식으로 표시되는지 확인합니다. 또한 문서 오른쪽 상단에 **피드백** 버튼이 있는지 확인합니다.
 2. 마우스 커서를 사용하여 주석 처리하려는 텍스트 부분을 강조 표시합니다.
 3. 강조 표시된 텍스트 아래에 표시되는 **피드백 추가** 팝업을 클릭합니다.
 4. 표시된 지침을 따릅니다.
- Bugzilla를 통해 피드백을 제출하려면 새 티켓을 생성하십시오.
 1. [Bugzilla](#) 웹 사이트로 이동하십시오.
 2. 구성 요소로 **문서**를 사용합니다.
 3. **설명** 필드에 문서 개선을 위한 제안 사항을 기입하십시오. 관련된 문서의 해당 부분 링크를 알려주십시오.
 4. **버그 제출**을 클릭합니다.

1장. 복제 토폴로지 관리

이 장에서는 IdM(Identity Management) 도메인에서 서버 간 복제를 관리하는 방법을 설명합니다.

추가 리소스

- [복제본 토폴로지 계획](#)

1.1. 복제 계약, 토폴로지 접미사 및 토폴로지 세그먼트 설명

복제본을 생성할 때 IdM(Identity Management)은 초기 서버와 복제본 간의 복제 계약을 생성합니다. 그런 다음 복제된 데이터는 토폴로지 접미사에 저장되고 두 개의 복제본이 접미사 사이에 복제 계약이 있는 경우 접미사는 토폴로지 세그먼트를 형성합니다. 이러한 개념은 다음 섹션에서 자세히 설명합니다.

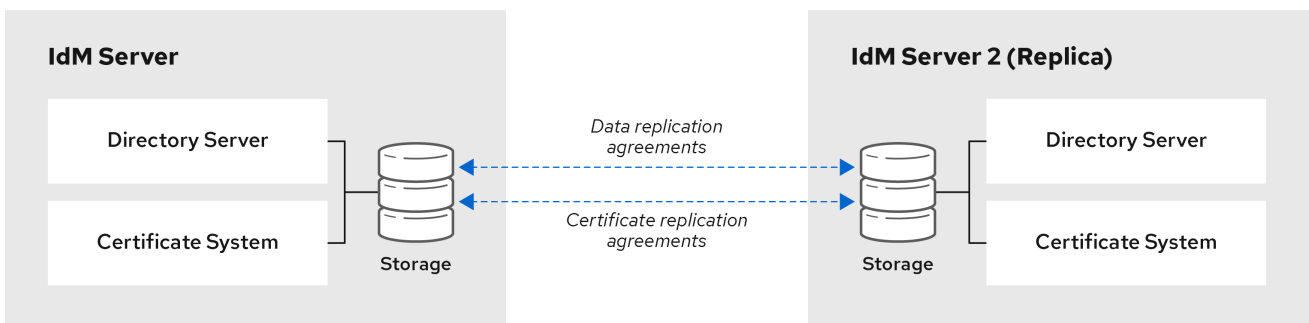
- [복제 계약](#)
- [토폴로지 접미사](#)
- [토폴로지 세그먼트](#)

1.1.1. 복제 계약

관리자가 기존 서버를 기반으로 복제본을 생성하면 IdM(Identity Management)은 초기 서버와 복제본 간의 복제 계약을 생성합니다. 복제 계약을 사용하면 두 서버 간에 데이터와 구성이 지속적으로 복제됩니다.

IdM은 여러 읽기/쓰기 복제본 복제를 사용합니다. 이 구성에서 복제 계약에 연결된 모든 복제본은 업데이트를 수신 및 제공하므로 공급업체 및 소비자 간주됩니다. 복제 계약서는 항상 양방향입니다.

그림 1.1. 서버 및 복제본 계약



64_RHEL_0120

IdM은 다음 두 가지 유형의 복제 계약을 사용합니다.

도메인 복제 계약

이러한 계약에서는 ID 정보를 복제합니다.

인증서 복제 계약

이러한 계약에서는 인증서 정보를 복제합니다.

두 복제 채널은 모두 독립적입니다. 두 서버에는 두 가지 유형의 복제 계약이 구성되어 있을 수 있습니다. 예를 들어 서버 A와 서버 B에 도메인 복제 계약만 구성되어 있는 경우 인증서 정보가 아닌 ID 정보만 복제됩니다.

1.1.2. 토폴로지 접미사

토폴로지 접미사는 복제된 데이터를 저장합니다. IdM은 **domain** 및 **ca**의 두 가지 유형의 토폴로지 접미사를 지원합니다. 각 접미사는 별도의 서버인 별도의 복제 토폴로지를 나타냅니다.

복제 계약이 구성되면 두 개의 다른 서버에 동일한 유형의 토폴로지 접미사가 사용됩니다.

domain suffix: dc=example,dc=com

domain suffix에는 모든 도메인 관련 데이터가 포함되어 있습니다.

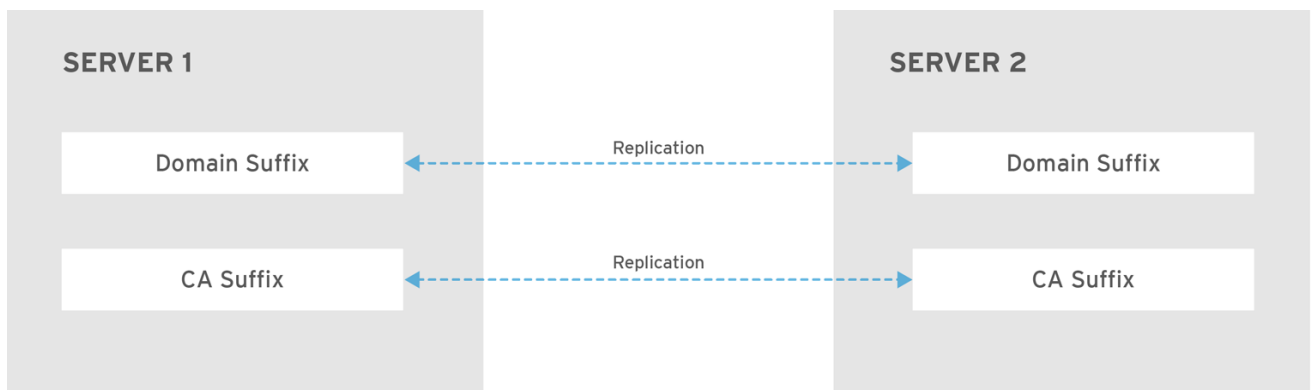
두 복제본의 **domain** 접미사 간 복제 계약이 있는 경우 사용자, 그룹 및 정책과 같은 디렉터리 데이터를 공유합니다.

ca suffix: o=ipaca

ca 접미사에는 인증서 시스템 구성 요소에 대한 데이터가 포함되어 있습니다. CA(인증 기관)가 설치된 서버에만 존재합니다.

두 복제본의 **ca** 접미사 간에 복제 계약이 있는 경우 인증서 데이터를 공유합니다.

그림 1.2. 토폴로지 접미사



RHEL_404973_0916

초기 토폴로지 복제 연결은 새 복제본을 설치할 때 **ipa-replica-install** 스크립트에서 두 서버 간에 설정됩니다.

예 1.1. 토폴로지 접미사 보기

ipa topologysuffix-find 명령은 토폴로지 접미사 목록을 표시합니다.

```

$ ipa topologysuffix-find
-----
2 topology suffixes matched
-----
Suffix name: ca
Managed LDAP suffix DN: o=ipaca

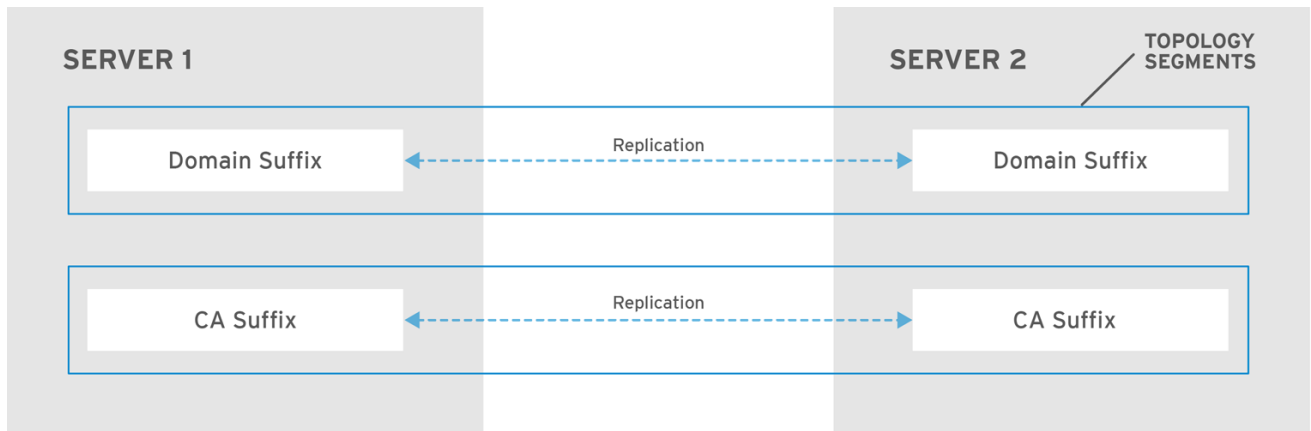
Suffix name: domain
Managed LDAP suffix DN: dc=example,dc=com
-----
Number of entries returned 2
-----
  
```

1.1.3. 토폴로지 세그먼트

두 복제본의 접미사 간에 복제 계약이 있는 경우 접미사는 *토폴로지 세그먼트*를 형성합니다. 각 토폴로지 세그먼트는 왼쪽 노드와 오른쪽 노드로 구성됩니다. 노드는 복제 계약에 조인된 서버를 나타냅니다.

IdM의 토폴로지 세그먼트는 항상 양방향입니다. 각 세그먼트는 서버 A에서 서버 B에, 서버 B에서 서버 A까지의 두 개의 복제 계약을 나타냅니다. 따라서 데이터는 두 가지 방향으로 복제됩니다.

그림 1.3. 토폴로지 세그먼트



RHEL_404973_0916

예 1.2. 토폴로지 세그먼트 보기

ipa topologysegment-find 명령은 도메인 또는 CA 접미사에 대해 구성된 현재 토폴로지 세그먼트를 표시합니다. 예를 들어 도메인 접미사의 경우:

```
$ ipa topologysegment-find
Suffix name: domain
-----
1 segment matched
-----
Segment name: server1.example.com-to-server2.example.com
Left node: server1.example.com
Right node: server2.example.com
Connectivity: both
-----
Number of entries returned 1
-----
```

이 예제에서 도메인 관련 데이터는 **server1.example.com**과 **server2.example.com**의 두 서버 간에만 복제됩니다.

특정 세그먼트에 대한 세부 정보만 표시하려면 **ipa topologysegment-show** 명령을 사용합니다.

```
$ ipa topologysegment-show
Suffix name: domain
Segment name: server1.example.com-to-server2.example.com
Segment name: server1.example.com-to-server2.example.com
Left node: server1.example.com
Right node: server2.example.com
Connectivity: both
```

1.2. 토폴로지 그래프를 사용하여 복제 토폴로지 관리

웹 UI의 토폴로지 그래프는 도메인의 서버 간 관계를 보여줍니다. 웹 UI를 사용하면 토폴로지의 표현을 조작하고 변환할 수 있습니다.

토폴로지 그래프 액세스

토폴로지 그래프에 액세스하려면 다음을 수행합니다.

1. IPA 서버 → 토폴로지 → 토폴로지 그래프를 선택합니다.
2. 그래프에 즉시 반영되지 않는 토폴로지를 변경하는 경우 **새로 고침**을 클릭합니다.

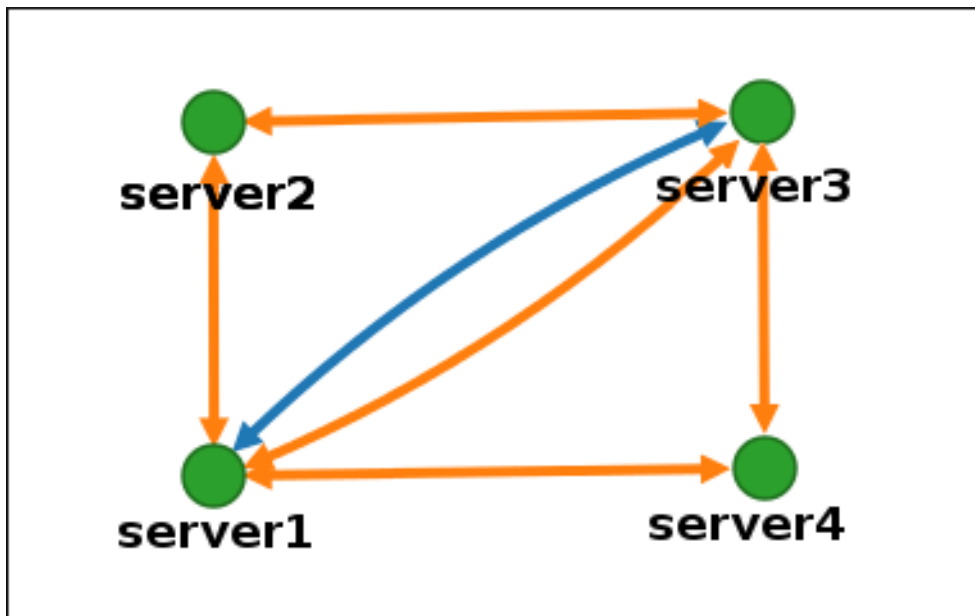
토폴로지 그래프 해석

도메인 복제 계약에 가입된 서버는 주황색 화살표로 연결됩니다. CA 복제 계약에 가입된 서버는 파란색 화살표로 연결됩니다.

토폴로지 그래프 예: 권장 토폴로지

아래 권장 토폴로지 예제에서는 4개의 서버에 대해 사용 가능한 권장 토폴로지 중 하나를 보여줍니다. 각 서버는 최소 두 개의 다른 서버에 연결되어 있고 두 개 이상의 서버는 CA 마스터입니다.

그림 1.4. 권장되는 토폴로지 예

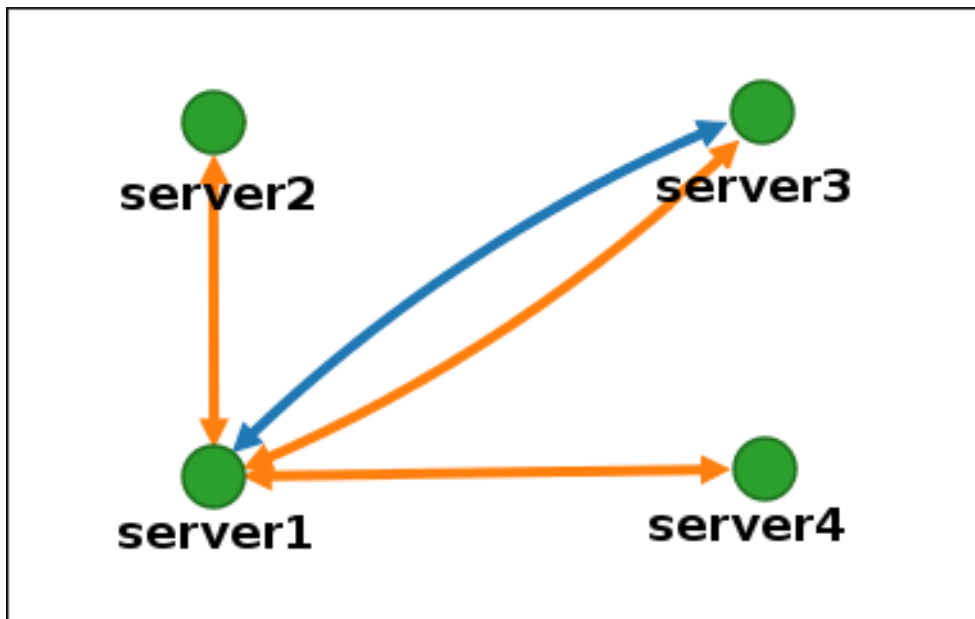


토폴로지 그래프 예: 디스크 토폴로지

아래 권장되지 않는 토폴로지 예에서 **server1**은 단일 장애 지점입니다. 다른 모든 서버는 이 서버와 복제 계약을 맺고 있지만 다른 서버와는 계약하지 않습니다. 따라서 **server1**이 실패하면 다른 모든 서버가 격리됩니다.

이와 같은 토폴로지를 생성하지 마십시오.

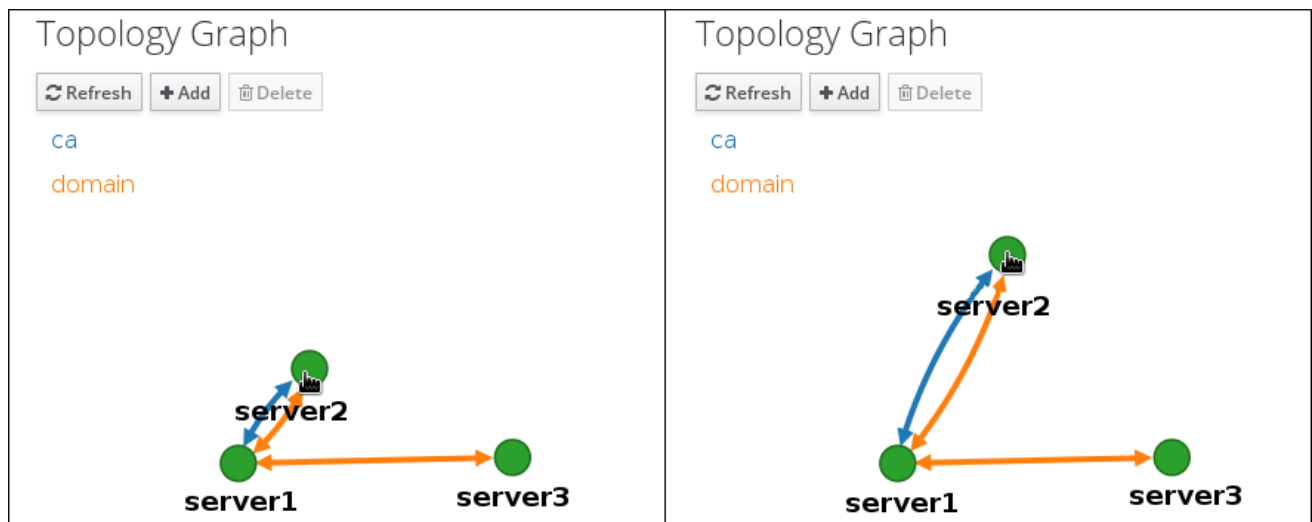
그림 1.5. 정지 토폴로지 예: Single Point of Failure



토폴로지 뷰 사용자 지정

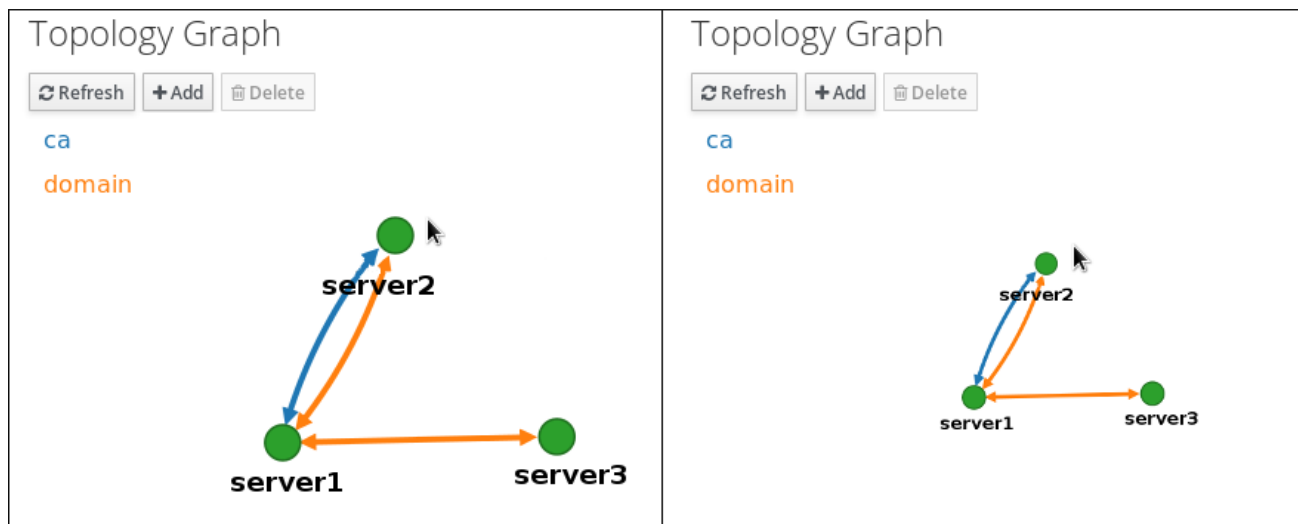
마우스를 드래그하여 개별 토폴로지 노드를 이동할 수 있습니다.

그림 1.6. 토폴로지 그래프 노드 이동



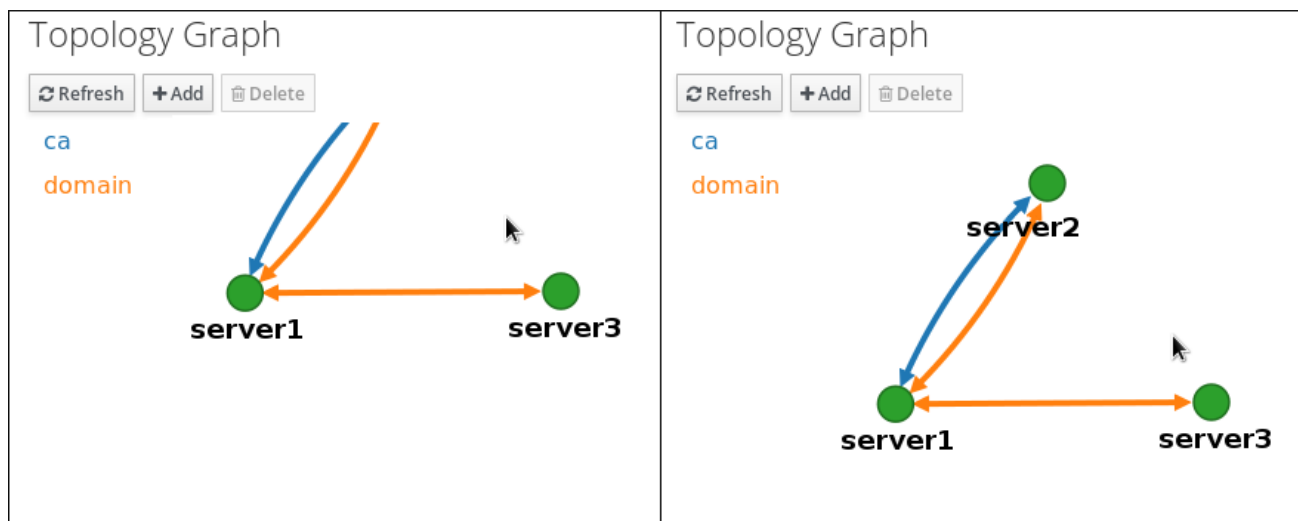
마우스 샵드를 사용하여 토폴로지 그래프를 확대하고 축소할 수 있습니다.

그림 1.7. 토폴로지 그래프 확대



왼쪽 마우스 버튼을 유지하여 토폴로지 그래프의 캔버스를 이동할 수 있습니다.

그림 1.8. 토폴로지 그래프 캔버스 이동



1.3. 웹 UI를 사용하여 두 서버 간 복제 설정

IdM(Identity Management)의 웹 인터페이스를 사용하여 두 서버를 선택하고 간에 새 복제 계약을 생성할 수 있습니다.

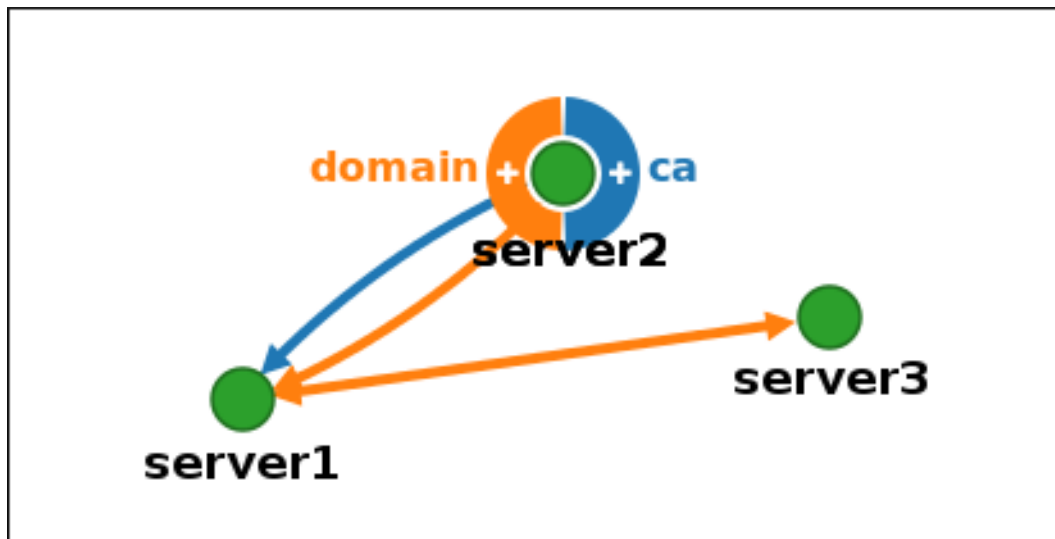
사전 요구 사항

- IdM 관리자 인증 정보가 있습니다.

절차

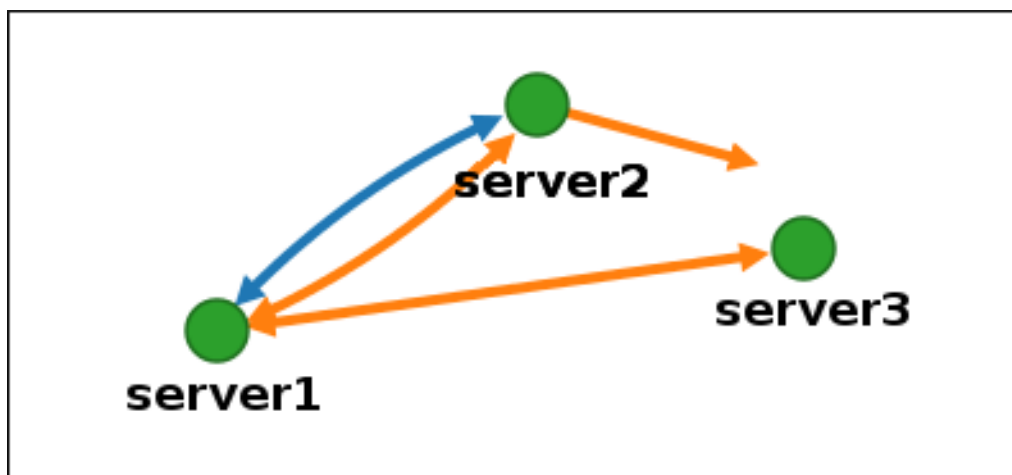
1. 토폴로지 그래프에서 서버 노드 중 하나에 마우스를 올려 놓습니다.

그림 1.9. 도메인 또는 CA 옵션



2. 생성할 토폴로지 세그먼트 유형에 따라 **도메인** 또는 원의 **ca** 부분을 클릭합니다.
3. 새 복제 계약을 나타내는 새 화살표가 마우스 포인터 아래에 표시됩니다. 마우스를 다른 서버 노드로 이동하여 클릭합니다.

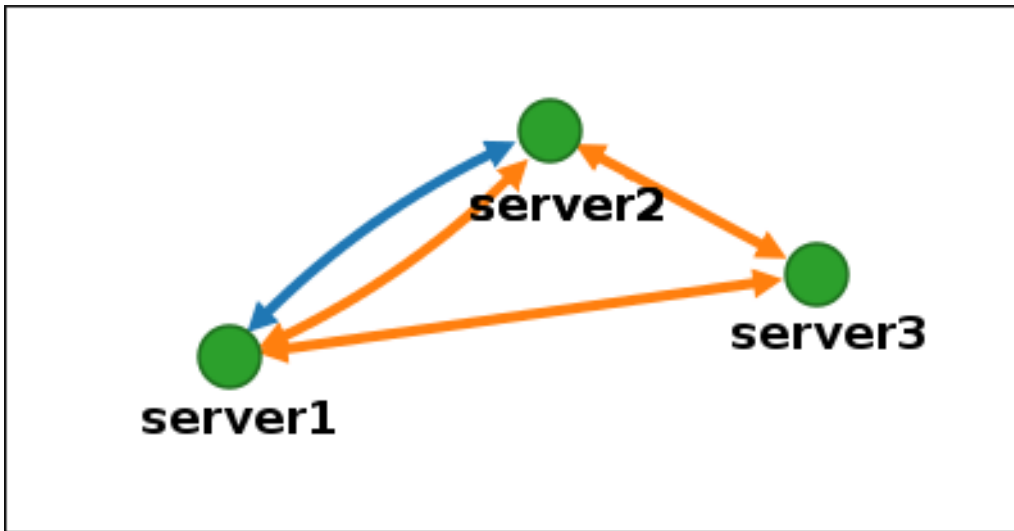
그림 1.10. 새 세그먼트 생성



4. 토폴로지 세그먼트 추가 창에서 **추가**를 클릭하여 새 세그먼트의 속성을 확인합니다.

두 서버 간의 새 토폴로지 세그먼트는 복제 계약에 조인합니다. 이제 토폴로지 그래프에서 업데이트된 복제 토폴로지를 표시합니다.

그림 1.11. 새 세그먼트 생성



1.4. 웹 UI를 사용하여 두 서버 간 복제 중지

IdM(Identity Management)의 웹 인터페이스를 사용하면 서버에서 복제 계약을 제거할 수 있습니다.

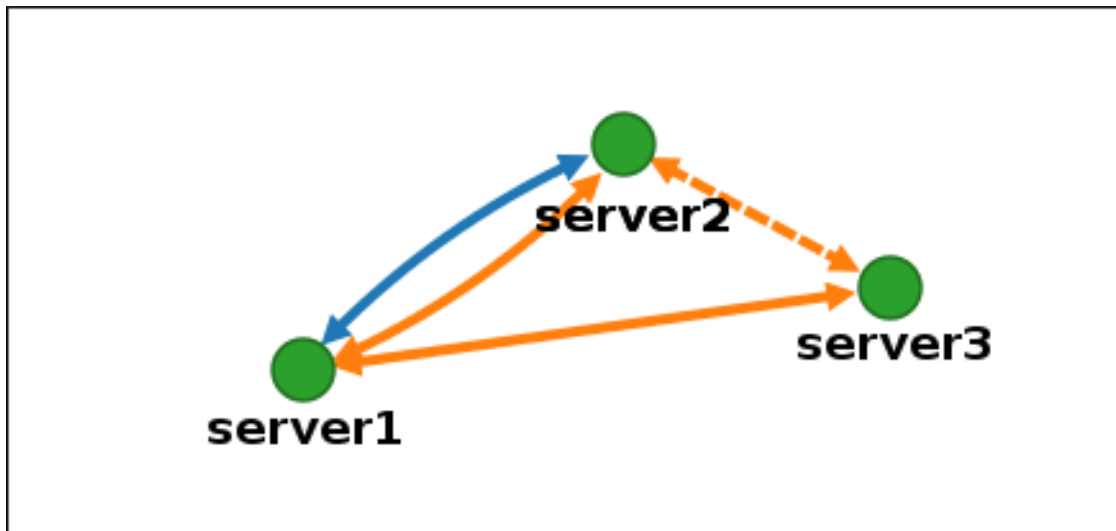
사전 요구 사항

- IdM 관리자 인증 정보가 있습니다.

절차

1. 제거할 복제 계약을 나타내는 화살표를 클릭합니다. 이것은 화살표를 강조합니다.

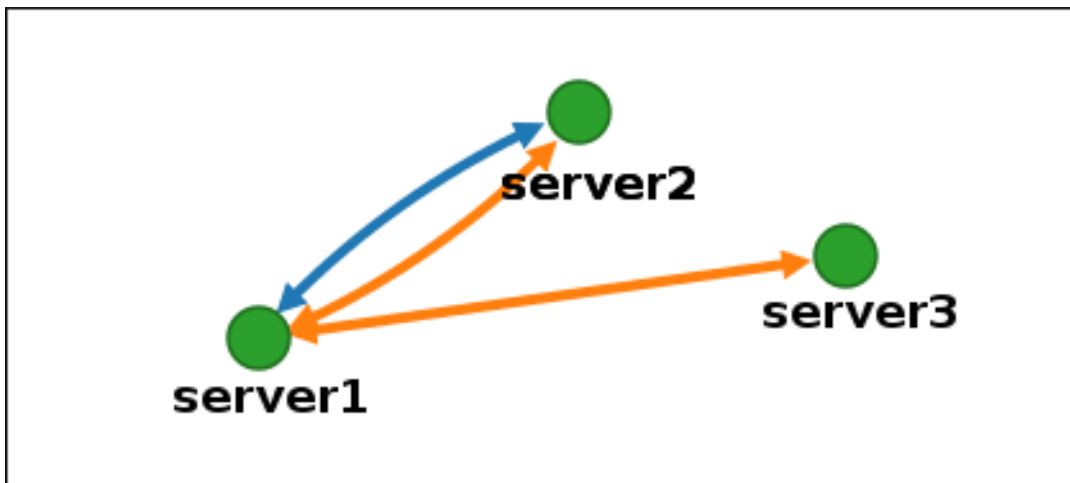
그림 1.12. 토폴로지 세그먼트가 강조 표시됨



2. 삭제를 클릭합니다.
3. 확인 창에서 확인을 클릭합니다.

IdM은 두 서버 간의 토폴로지 세그먼트를 제거하여 복제 계약을 삭제합니다. 이제 토폴로지 그래프에서 업데이트된 복제 토폴로지를 표시합니다.

그림 1.13. 토폴로지 세그먼트 삭제



1.5. CLI를 사용하여 두 서버 간 복제 설정

ipa topologysegment-add 명령을 사용하여 두 서버 간 복제 계약을 구성할 수 있습니다.

사전 요구 사항

- IdM 관리자 인증 정보가 있습니다.

절차

1. **ipa topologysegment-add** 명령을 사용하여 두 서버의 토폴로지 세그먼트를 생성합니다. 메시지가 표시되면 다음을 제공합니다.

- 필수 토폴로지 접미사: **domain** 또는 **ca**
- 두 서버를 나타내는 왼쪽 노드와 올바른 노드
- 필요에 따라 세그먼트에 대한 사용자 정의 이름
예를 들어 다음과 같습니다.

```

$ ipa topologysegment-add
Suffix name: domain
Left node: server1.example.com
Right node: server2.example.com
Segment name [server1.example.com-to-server2.example.com]: new_segment
-----
Added segment "new_segment"
-----
Segment name: new_segment
Left node: server1.example.com
Right node: server2.example.com
Connectivity: both
  
```

새 세그먼트를 추가하면 복제 계약의 서버에 연결됩니다.

2. **선택 사항:** **ipa topologysegment-show** 명령을 사용하여 새 세그먼트가 구성되었는지 확인합니다.

```

$ ipa topologysegment-show
  
```

```
Suffix name: domain
Segment name: new_segment
Segment name: new_segment
Left node: server1.example.com
Right node: server2.example.com
Connectivity: both
```

1.6. CLI를 사용하여 두 서버 간 복제 중지

ipa topology_segment-del 명령을 사용하여 명령줄에서 복제 계약을 종료할 수 있습니다.

사전 요구 사항

- IdM 관리자 인증 정보가 있습니다.

절차

1. 복제를 중지하려면 서버 간 해당 복제 세그먼트를 삭제해야 합니다. 이를 위해서는 세그먼트 이름을 알아야 합니다.
이름을 모르는 경우 **ipa topologysegment-find** 명령을 사용하여 모든 세그먼트를 표시하고 출력에서 필요한 세그먼트를 찾습니다. 메시지가 표시되면 필요한 토폴로지 접미사: **domain** 또는 **ca**를 입력합니다. 예를 들어 다음과 같습니다.

```
$ ipa topologysegment-find
Suffix name: domain
-----
8 segments matched
-----
Segment name: new_segment
Left node: server1.example.com
Right node: server2.example.com
Connectivity: both

...

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

2. **ipa topologysegment-del** 명령을 사용하여 두 서버에 연결된 토폴로지 세그먼트를 제거합니다.

```
$ ipa topologysegment-del
Suffix name: domain
Segment name: new_segment
-----
Deleted segment "new_segment"
-----
```

세그먼트를 삭제하면 복제 계약이 제거됩니다.

3. **선택 사항:** **ipa topologysegment-find** 명령을 사용하여 세그먼트가 더 이상 나열되지 않는지 확인합니다.

```
$ ipa topologysegment-find
```

Suffix name: *domain*

7 segments matched

Segment name: server2.example.com-to-server3.example.com

Left node: server2.example.com

Right node: server3.example.com

Connectivity: both

...

Number of entries returned 7

1.7. 웹 UI를 사용하여 토폴로지에서 서버 제거

IdM(Identity Management) 웹 인터페이스를 사용하여 토폴로지에서 서버를 제거할 수 있습니다.

사전 요구 사항

- IdM 관리자 인증 정보가 있습니다.
- 제거하려는 서버는 나머지 토폴로지를 사용하여 다른 서버를 연결하는 유일한 서버가 아닙니다. 이로 인해 다른 서버가 분리될 수 없습니다.
- 제거하려는 서버는 마지막 CA 또는 DNS 서버가 아닙니다.



주의

서버를 제거하는 것은 되돌릴 수 없는 작업입니다. 서버를 제거하면 토폴로지에 다시 도입할 수 있는 유일한 방법은 시스템에 새 복제본을 설치하는 것입니다.

절차

시스템에서 서버 구성 요소를 제거하지 않고 토폴로지에서 서버를 제거하려면 다음을 수행합니다.

1. IPA 서버 → 토폴로지 → IPA 서버를 선택합니다.
2. 삭제할 서버 이름을 클릭합니다.

그림 1.14. 서버 선택

IPA Servers				
Search			Refresh	
☐	Server name	Min domain level	Max domain level	Managed suffixes
☐	server1.example.com	0	1	domain, ca
☐	server2.example.com	0	1	domain
☐	server3.example.com	0	1	domain, ca
Showing 1 to 3 of 3 entries.				

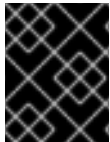
3. **Delete Server** (서버 삭제)를 클릭합니다.

1.8. CLI를 사용하여 토폴로지에서 서버 제거

명령줄 인터페이스를 사용하여 토폴로지에서 서버를 제거할 수 있습니다.

사전 요구 사항

- IdM 관리자 인증 정보가 있습니다.
- 제거하려는 서버는 나머지 토폴로지를 사용하여 다른 서버를 연결하는 유일한 서버가 아닙니다. 이로 인해 다른 서버가 분리되지 않습니다.
- 제거하려는 서버는 마지막 CA 또는 DNS 서버가 아닙니다.



중요

서버를 제거하는 것은 되돌릴 수 없는 작업입니다. 서버를 제거하면 토폴로지에 다시 도입할 수 있는 유일한 방법은 시스템에 새 복제본을 설치하는 것입니다.

절차

server1.example.com 을 제거하려면 다음을 수행합니다.

1. 다른 서버에서 **ipa server-del** 명령을 실행하여 **server1.example.com** 을 제거합니다. 이 명령은 서버를 가리키는 모든 토폴로지 세그먼트를 제거합니다.

```
[user@server2 ~]$ ipa server-del
Server name: server1.example.com
Removing server1.example.com from replication topology, please wait...
-----
Deleted IPA server "server1.example.com"
-----
```

2. **선택 사항:** **server1.example.com** 에서 **ipa server-install --uninstall** 명령을 실행하여 시스템에서 서버 구성 요소를 제거합니다.

```
[root@server1 ~]# ipa server-install --uninstall
```

1.9. 웹 UI를 사용하여 IDM 서버에서 서버 역할 보기

IdM 서버에 설치된 서비스를 기반으로 다양한 서버 역할을 수행할 수 있습니다. 예를 들어 다음과 같습니다.

- CA 서버
- DNS 서버
- KRA(Key recovery authority) 서버.

지원되는 서버 역할의 전체 목록은 IPA 서버 토폴로지 서버 역할을 참조하십시오.



참고

- 역할 status **absent** 는 토폴로지의 서버가 역할을 수행하지 않음을 의미합니다.
- 역할 상태가 활성화되어 있으면 토폴로지에서 하나 이상의 서버에서 역할을 수행하고 있습니다.

그림 1.15. 웹 UI에서 서버 역할

Server Roles		Refresh
Role name	Role status	
AD trust agent	absent	
AD trust controller	absent	
CA server	enabled	

1.10. CLI를 사용하여 IDM 서버의 서버 역할 보기

IdM 서버에 설치된 서비스를 기반으로 다양한 서버 역할을 수행할 수 있습니다. 예를 들어 다음과 같습니다.

- CA 서버
- DNS 서버
- KRA(Key recovery authority) 서버.

다음 명령을 사용하여 토폴로지에서 어떤 역할을 수행하는 서버를 볼 수 있습니다.

- **ipa config-show** 명령은 모든 CA 서버와 현재 CA 갱신 서버를 표시합니다.

```
$ ipa config-show
```

```
...
```

```
IPA masters: server1.example.com, server2.example.com, server3.example.com
```

```
IPA CA servers: server1.example.com, server2.example.com
```

```
IPA CA renewal master: server1.example.com
```

- **ipa server-show** 명령은 특정 서버에서 활성화된 역할 목록을 표시합니다. 예를 들어 *server.example.com* 에서 활성화된 역할 목록은 다음과 같습니다.

```
$ ipa server-show
Server name: server.example.com
...
Enabled server roles: CA server, DNS server, KRA server
```

- `ipa server-find --servrole` 은 특정 서버 역할이 활성화된 모든 서버를 검색합니다. 예를 들어 모든 CA 서버를 검색하려면 다음을 수행합니다.

```
$ ipa server-find --servrole "CA server"
-----
2 IPA servers matched
-----
Server name: server1.example.com
...
Server name: server2.example.com
...
-----
Number of entries returned 2
-----
```

1.11. 복제본을 CA 갱신 서버 및 CRL 게시자 서버로 승격

IdM 배포에서 포함된 CA(인증 기관)를 사용하는 경우 IdM CA 서버 중 하나가 CA 갱신 서버인 CA 하위 시스템 인증서 갱신을 관리하는 서버입니다. IdM CA 서버 중 하나는 인증서 해지 목록을 생성하는 서버인 IdM CRL 게시자 서버 역할을 합니다. 기본적으로 CA 갱신 서버 및 CRL 게시자 서버 역할은 시스템 관리자가 `ipa-server-install` 또는 `ipa-ca-install` 명령을 사용하여 CA 역할을 설치한 첫 번째 서버에 설치됩니다.

사전 요구 사항

- IdM 관리자 인증 정보가 있습니다.

1.12. 숨겨진 복제본 검증 또는 승격

절차

복제본이 설치되면 복제본이 숨겨지거나 표시되는지 여부를 구성할 수 있습니다.

숨겨진 복제본에 대한 자세한 내용은 [숨겨진 복제본 모드](#) 를 참조하십시오.

복제본이 CA 갱신 서버인 경우 이 복제본이 숨겨지기 전에 서비스를 다른 복제본으로 이동합니다.

자세한 내용은 을 참조하십시오.

절차

- 복제본을 숨기려면 다음을 입력합니다.

```
# ipa server-state replica.idm.example.com --state=hidden
```

또는 다음 명령을 사용하여 복제본을 볼 수도 있습니다.

```
# ipa server-state replica.idm.example.com --state=enabled
```

-

2장. ANSIBLE 플레이북을 사용하여 IDM을 관리하기 위한 환경 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 사용하면 모든 플레이북을 한 곳에서 찾을 수 있으며 루트 권한을 호출하지 않고도 플레이북을 실행할 수 있습니다.



참고

ipaserver, ipareplica, ipaclient 및 **ipabackup ansible-freeipa** 역할을 실행하려면 관리형 노드의 루트 권한만 있으면 됩니다. 이러한 역할에는 디렉터리 및 **dnf** 소프트웨어 패키지 관리자에 대한 권한이 있어야 합니다.

이 섹션에서는 ~/MyPlaybooks 디렉터리를 만들고 Ansible 플레이북을 저장하고 실행하는 데 사용할 수 있도록 구성하는 방법을 설명합니다.

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.

```
[eu]
```

```
server.idm.example.com
```

```
[us]
replica.idm.example.com
```

```
[ipaserver:children]
eu
us
```

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 실행하려면 IdM 관리자 암호를 입력해야 합니다.

추가 리소스

- [Ansible 플레이북을 사용하여 Identity Management 서버](#) 설치를 참조하십시오.
- [인벤토리를 구축하는 방법](#)을 참조하십시오.

3장. ANSIBLE을 사용하여 IDM의 복제 토폴로지 관리

여러 IdM(Identity Management) 서버를 유지 관리하고 중복을 위해 서버 손실을 완화하거나 방지하기 위해 서로 복제할 수 있습니다. 예를 들어, 한 서버가 실패하면 다른 서버에서 도메인에 서비스를 계속 제공합니다. 나머지 서버 중 하나를 기반으로 새 복제본을 생성하여 손실된 서버를 복구할 수도 있습니다.

IdM 서버에 저장된 데이터는 복제 계약을 기반으로 복제됩니다. 두 서버에 복제 계약이 구성된 경우 해당 데이터를 공유합니다. 복제된 데이터는 토폴로지 접미사에 저장됩니다. 두 복제본의 접미사 간에 복제 계약이 있는 경우 접미사는 토폴로지 세그먼트를 형성합니다.

이 장에서는 Red Hat Ansible Engine을 사용하여 IdM 복제 계약, 토폴로지 세그먼트 및 토폴로지 접미사를 관리하는 방법을 설명합니다. 이 장에는 다음 섹션이 포함되어 있습니다.

- [Ansible을 사용하여 IdM에 복제 계약이 있는지 확인](#)
- [Ansible을 사용하여 여러 IdM 복제본 간에 복제 계약이 존재하는지 확인](#)
- [Ansible을 사용하여 두 개의 복제본 간에 복제 계약이 있는지 확인합니다.](#)
- [Ansible을 사용하여 IdM에 토폴로지 접미사가 있는지 확인합니다.](#)
- [Ansible을 사용하여 IdM 복제본 다시 초기화](#)
- [Ansible을 사용하여 IdM에 복제 주석이 없는지 확인](#)

3.1. ANSIBLE을 사용하여 IDM에 복제 계약이 있는지 확인

IdM(Identity Management) 서버에 저장된 데이터는 복제 계약을 기반으로 복제됩니다. 두 서버에 복제 계약이 구성된 경우 해당 데이터가 공유됩니다. 복제 계약은 항상 서로 구분되며 데이터는 첫 번째 복제본에서 다른 복제본으로 복제되고 다른 복제본에서 첫 번째 복제본으로 복제됩니다.

이 섹션에서는 Ansible 플레이북을 사용하여 `server.idm.example.com` 과 `replica.idm.example.com` 간에 도메인 유형의 복제 계약이 있는지 확인하는 방법을 설명합니다.

사전 요구 사항

- 토폴로지의 복제본 연결에 나열된 IdM 토폴로지 설계에 대한 권장 사항을 이해해야 합니다
- IdM 관리자 암호를 알고 있습니다.
- 다음 요구 사항을 충족하는 Ansible 제어 노드를 구성했습니다.
 - Ansible 버전 2.8 이상을 사용하고 있습니다.
 - Ansible 컨트롤러에 [ansible-freeipa](#) 패키지를 설치했습니다.
 - `~/MyPlaybooks/` 디렉터리에 이러한 옵션을 구성하는 IdM 서버의 FQDN(정규화된 도메인 이름)을 사용하여 [Ansible 인벤토리 파일](#)을 생성했습니다.

절차

1. `~/MyPlaybooks/` 디렉터리로 이동합니다.

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

2. `/usr/share/doc/ansible-freeipa/playbooks/topology/` 디렉터리에 있는 `add-topologysegment.yml` Ansible 플레이북 파일을 복사합니다.

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/topology/add-topologysegment.yml
add-topologysegment-copy.yml
```

3. 편집할 `add-topologysegment-copy.yml` 파일을 엽니다.
4. `ipatopologysegment` 작업 섹션에서 다음 변수를 설정하여 파일을 조정합니다.
 - `ipaadmin_password` 변수를 IdM 관리자 의 암호로 설정합니다.
 - 추가할 세그먼트 유형에 따라 접미사 변수를 `domain` 또는 `ca` 로 설정합니다.
 - 왼쪽 변수를 복제 계약의 왼쪽 노드가 될 IdM 서버의 이름으로 설정합니다.
 - 올바른 변수를 복제 계약의 올바른 노드가 될 IdM 서버의 이름으로 설정합니다.
 - `state` 변수가 `present` 로 설정되어 있는지 확인합니다.

이는 현재 예제에서 수정된 Ansible 플레이북 파일입니다.

```
---
- name: Playbook to handle topologysegment
  hosts: ipaserver
  become: true

  tasks:
  - name: Add topology segment
    ipatopologysegment:
      ipaadmin_password: Secret123
      suffix: domain
      left: server.idm.example.com
      right: replica.idm.example.com
      state: present
```

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

```
$ ansible-playbook -v -i inventory add-topologysegment-copy.yml
```

추가 리소스

- [복제 계약](#), [Topology Suffixes](#), [Topology Segments](#)를 참조하십시오.
- `/usr/share/doc/ansible-freeipa/` 디렉터리에 있는 `README-topology.md` 파일을 참조하십시오.
- `/usr/share/doc/ansible-freeipa/playbooks/topology` 디렉터리에서 샘플 플레이북을 참조하십시오.

3.2. ANSIBLE을 사용하여 여러 IDM 복제본 간에 복제 계약이 존재하는지 확인

IdM(Identity Management) 서버에 저장된 데이터는 복제 계약을 기반으로 복제됩니다. 두 서버에 복제 계약이 구성된 경우 해당 데이터가 공유됩니다. 복제 계약은 항상 서로 구분되며 데이터는 첫 번째 복제본에서 다른 복제본으로 복제되고 다른 복제본에서 첫 번째 복제본으로 복제됩니다.

이 섹션에서는 IdM의 여러 복제본 쌍 간에 복제 계약이 있는지 확인하는 방법을 설명합니다.

사전 요구 사항

- 토폴로지의 [복제본](#) 연결에 나열된 IdM 토폴로지 설계에 대한 권장 사항을 이해하고 있는지 확인합니다.
- IdM 관리자 암호를 알고 있습니다.
- 다음 요구 사항을 충족하는 Ansible 제어 노드를 구성했습니다.
 - Ansible 버전 2.8 이상을 사용하고 있습니다.
 - Ansible 컨트롤러에 [ansible-freeipa](#) 패키지를 설치했습니다.
 - `~/MyPlaybooks/` 디렉터리에 이러한 옵션을 구성하는 IdM 서버의 FQDN(정규화된 도메인 이름)을 사용하여 [Ansible 인벤토리 파일](#)을 생성했습니다.

절차

1. `~/MyPlaybooks/` 디렉터리로 이동합니다.

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

2. `/usr/share/doc/ansible-freeipa/playbooks/topology/` 디렉터리에 있는 `add-topologysegments.yml` Ansible 플레이북 파일을 복사합니다.

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/topology/add-topologysegments.yml
add-topologysegments-copy.yml
```

3. 편집하기 위해 `add-topologysegments-copy.yml` 파일을 엽니다.

4. **vars** 섹션에서 다음 변수를 설정하여 파일을 조정합니다.

- `ipaadmin_password` 변수를 IdM 관리자 의 암호로 설정합니다.
- 모든 토폴로지 세그먼트에서 `ipatopology_segments` 섹션에 행을 추가하고 다음 변수를 설정합니다.
 - 추가할 세그먼트 유형에 따라 접미사 변수를 **domain** 또는 **ca** 로 설정합니다.
 - 왼쪽 변수를 복제 계약의 왼쪽 노드가 될 IdM 서버의 이름으로 설정합니다.
 - 올바른 변수를 복제 계약의 올바른 노드가 될 IdM 서버의 이름으로 설정합니다.

5. `add-topologysegments-copy.yml` 파일의 **tasks** 섹션에서 **state** 변수가 **present** 로 설정되어 있는지 확인합니다.

이는 현재 예제에서 수정된 Ansible 플레이북 파일입니다.

```
---
- name: Add topology segments
  hosts: ipaserver
```

```

become: true
gather_facts: false

vars:
  ipaadmin_password: Secret123
  ipatopology_segments:
    - {suffix: domain, left: replica1.idm.example.com , right: replica2.idm.example.com }
    - {suffix: domain, left: replica2.idm.example.com , right: replica3.idm.example.com }
    - {suffix: domain, left: replica3.idm.example.com , right: replica4.idm.example.com }
    - {suffix: domain+ca, left: replica4.idm.example.com , right:
      replica1.idm.example.com }

tasks:
  - name: Add topology segment
    ipatopologysegment:
      ipaadmin_password: "{{ ipaadmin_password }}"
      suffix: "{{ item.suffix }}"
      name: "{{ item.name | default(omit) }}"
      left: "{{ item.left }}"
      right: "{{ item.right }}"
      state: present
      #state: absent
      #state: checked
      #state: reinitialized
      loop: "{{ ipatopology_segments | default([]) }}"

```

6. 파일을 저장합니다.

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

```
$ ansible-playbook -v -i inventory add-topologysegments-copy.yml
```

추가 리소스

- 복제 계약, [Topology Suffixes](#), [Topology Segments](#)를 참조하십시오.
- `/usr/share/doc/ansible-freeipa/` 디렉토리에 있는 `README-topology.md` 파일을 참조하십시오.
- `/usr/share/doc/ansible-freeipa/playbooks/topology` 디렉토리에서 샘플 플레이북을 참조하십시오.

3.3. ANSIBLE을 사용하여 두 개의 복제본 간에 복제 계약이 있는지 확인합니다.

IdM(Identity Management) 서버에 저장된 데이터는 복제 계약을 기반으로 복제됩니다. 두 서버에 복제 계약이 구성된 경우 해당 데이터가 공유됩니다. 복제 계약은 항상 서로 구분되며 데이터는 첫 번째 복제본에서 다른 복제본으로 복제되고 다른 복제본에서 첫 번째 복제본으로 복제됩니다.

이 섹션에서는 IdM의 여러 복제본 쌍 간에 복제 계약이 존재하는지 확인하는 방법을 설명합니다.

사전 요구 사항

- 토폴로지의 [복제본 연결에 나열된 IdM\(Identity Management\) 토폴로지](#)를 설계하기 위한 권장 사항을 이해해야 합니다.

- IdM 관리자 암호를 알고 있습니다.
- 다음 요구 사항을 충족하는 Ansible 제어 노드를 구성했습니다.
 - Ansible 버전 2.8 이상을 사용하고 있습니다.
 - Ansible 컨트롤러에 [ansible-freeipa](#) 패키지를 설치했습니다.
 - `~/MyPlaybooks/` 디렉터리에 이러한 옵션을 구성하는 IdM 서버의 FQDN(정규화된 도메인 이름)을 사용하여 [Ansible 인벤토리 파일](#)을 생성했습니다.

절차

1. `~/MyPlaybooks/` 디렉터리로 이동합니다.

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

2. `/usr/share/doc/ansible-freeipa/playbooks/topology/` 디렉터리에 있는 `check-topology.yml` Ansible 플레이북 파일을 복사합니다.

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/topology/check-topologysegments.yml
check-topologysegments-copy.yml
```

3. 편집을 위해 `check-topologysegments-copy.yml` 파일을 엽니다.
4. **vars** 섹션에서 다음 변수를 설정하여 파일을 조정합니다.
 - `ipaadmin_password` 변수를 IdM 관리자 의 암호로 설정합니다.
 - 모든 토폴로지 세그먼트에서 `ipatopology_segments` 섹션에 행을 추가하고 다음 변수를 설정합니다.
 - 추가하는 세그먼트 유형에 따라 접미사 변수를 **domain** 또는 **ca** 로 설정합니다.
 - 왼쪽 변수를 복제 계약의 왼쪽 노드가 될 IdM 서버의 이름으로 설정합니다.
 - 올바른 변수를 복제 계약의 올바른 노드가 될 IdM 서버의 이름으로 설정합니다.
5. `check-topologysegments-copy.yml` 파일의 **tasks** 섹션에서 **state** 변수가 **present** 로 설정되어 있는지 확인합니다.
이는 현재 예제에서 수정된 Ansible 플레이북 파일입니다.

```
---
- name: Add topology segments
  hosts: ipaserver
  become: true
  gather_facts: false

  vars:
    ipaadmin_password: Secret123
    ipatopology_segments:
      - {suffix: domain, left: replica1.idm.example.com, right: replica2.idm.example.com }
      - {suffix: domain, left: replica2.idm.example.com , right: replica3.idm.example.com }
      - {suffix: domain, left: replica3.idm.example.com , right: replica4.idm.example.com }
      - {suffix: domain+ca, left: replica4.idm.example.com , right:
        replica1.idm.example.com }
```

```

tasks:
- name: Check topology segment
  ipatopologysegment:
    ipaadmin_password: "{{ ipaadmin_password }}"
    suffix: "{{ item.suffix }}"
    name: "{{ item.name | default(omit) }}"
    left: "{{ item.left }}"
    right: "{{ item.right }}"
    state: checked
    loop: "{{ ipatopology_segments | default([]) }}"

```

6. 파일을 저장합니다.

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

```
$ ansible-playbook -v -i inventory check-topologysegments-copy.yml
```

추가 리소스

- 토폴로지 계약, 접미사 및 세그먼트의 개념에 대한 자세한 내용은 [복제 계약](#), [Topology Suffixes](#), [Topology Segments](#).
- `/usr/share/doc/ansible-freeipa/` 디렉토리에 있는 `README-topology.md` 파일을 참조하십시오.
- `/usr/share/doc/ansible-freeipa/playbooks/topology` 디렉터리에서 샘플 플레이북을 참조하십시오.

3.4. ANSIBLE을 사용하여 IDM에 토폴로지 접미사가 있는지 확인합니다.

IdM(Identity Management)의 복제 계약 컨텍스트에서 토폴로지 접미사는 복제된 데이터를 저장합니다. IdM은 **domain** 및 **ca**의 두 가지 유형의 토폴로지 접미사를 지원합니다. 각 접미사는 별도의 백엔드인 별도의 복제 토폴로지를 나타냅니다. 복제 계약이 구성되면 두 개의 다른 서버에 동일한 유형의 토폴로지 접미사가 사용됩니다.

도메인 접미사에는 사용자, 그룹 및 정책과 같은 모든 도메인 관련 데이터가 포함됩니다. **ca** 접미사에는 인증서 시스템 구성 요소에 대한 데이터가 포함되어 있습니다. **CA**(인증 기관)가 설치된 서버에만 존재합니다.

이 섹션에서는 Ansible 플레이북을 사용하여 IdM에 토폴로지 접미사가 있는지 확인하는 방법을 설명합니다. 이 예제에서는 IdM에 도메인 접미사가 있는지 확인하는 방법을 설명합니다.

사전 요구 사항

- IdM 관리자 암호를 알고 있습니다.
- 다음 요구 사항을 충족하는 Ansible 제어 노드를 구성했습니다.
 - Ansible 버전 2.8 이상을 사용하고 있습니다.
 - Ansible 컨트롤러에 [ansible-freeipa](#) 패키지를 설치했습니다.
 - `~/MyPlaybooks/` 디렉터리에 이러한 옵션을 구성하는 IdM 서버의 FQDN(정규화된 도메인 이름)을 사용하여 [Ansible 인벤토리 파일](#)을 생성했습니다.

절차

1. `~/MyPlaybooks/` 디렉터리로 이동합니다.

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

2. `/usr/share/doc/ansible-freeipa/playbooks/topology/` 디렉터리에 있는 `verify-topologysuffix.yml` Ansible 플레이북 파일을 복사합니다.

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/topology/ verify-topologysuffix.yml
verify-topologysuffix-copy.yml
```

3. 편집할 `verify-topologysuffix-copy.yml` Ansible 플레이북 파일을 엽니다.

4. `ipatopologysuffix` 섹션에서 다음 변수를 설정하여 파일을 조정합니다.

- `ipaadmin_password` 변수를 IdM 관리자 의 암호로 설정합니다.
- 접미사 변수를 `domain` 으로 설정합니다. `ca` 접미사가 있는지 확인하는 경우 변수를 `ca` 로 설정합니다.
- `state` 변수가 검증 되도록 설정되어 있는지 확인합니다. 다른 옵션은 불가능합니다.

이는 현재 예제에서 수정된 Ansible 플레이북 파일입니다.

```
---
- name: Playbook to handle topologysuffix
  hosts: ipaserver
  become: true

  tasks:
    - name: Verify topology suffix
      ipatopologysuffix:
        ipaadmin_password: Secret123
        suffix: domain
        state: verified
```

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

```
$ ansible-playbook -v -i inventory verify-topologysuffix-copy.yml
```

추가 리소스

- [복제 계약](#), [Topology Suffixes](#), [Topology Segments](#)를 참조하십시오.
- `/usr/share/doc/ansible-freeipa/` 디렉터리에 있는 `README-topology.md` 파일을 참조하십시오.
- `/usr/share/doc/ansible-freeipa/playbooks/topology` 디렉터리에서 샘플 플레이북을 참조하십시오.

3.5. ANSIBLE을 사용하여 IDM 복제본 다시 초기화

복제본이 오랜 기간 동안 오프라인된 경우 또는 해당 데이터베이스가 손상된 경우 다시 초기화할 수 있습니다. 업데이트된 데이터 세트로 복제본을 새로 고칩니다. 예를 들어 백업에서 신뢰할 수 있는 복원이 필요한 경우 다시 초기화할 수 있습니다.



참고

복제 업데이트와 달리 복제본에서 변경된 항목만 서로 다시 보내면 전체 데이터베이스를 새로 고칩니다. In contrast to replication updates, during which replicas only send changed entries to each other, reinitialization refreshes the whole database.

명령을 실행하는 로컬 호스트는 reinitialized 복제본입니다. 데이터를 가져올 복제본을 지정하려면 **direction** 옵션을 사용합니다.

이 섹션에서는 Ansible 플레이북을 사용하여 server.idm.example.com 에서 replica.idm.example.com 에서 도메인 데이터를 다시 초기화하는 방법을 설명합니다.

사전 요구 사항

- IdM 관리자 암호를 알고 있습니다.
- 다음 요구 사항을 충족하는 Ansible 제어 노드를 구성했습니다.
 - Ansible 버전 2.8 이상을 사용하고 있습니다.
 - Ansible 컨트롤러에 [ansible-freeipa](#) 패키지를 설치했습니다.
 - ~/MyPlaybooks/ 디렉터리에 이러한 옵션을 구성하는 IdM 서버의 FQDN(정규화된 도메인 이름)을 사용하여 [Ansible 인벤토리 파일](#)을 생성했습니다.

절차

1. ~/MyPlaybooks/ 디렉터리로 이동합니다.

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

2. /usr/share/doc/ansible-freeipa/playbooks/topology/ 디렉터리에 있는 reinitialize-topologys.yml Ansible 플레이북 파일을 복사합니다.

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/topology/reinitialize-topologysegment.yml reinitialize-topologysegment-copy.yml
```

3. 편집할 reinitialize-topologysegment-copy.yml 파일을 엽니다.
4. ipatopologysegment 섹션에서 다음 변수를 설정하여 파일을 조정합니다.
 - ipadmin_password 변수를 IdM 관리자 의 암호로 설정합니다.
 - 접미사 변수를 domain 으로 설정합니다. ca 데이터를 다시 시작하는 경우 변수를 ca 로 설정합니다.
 - 왼쪽 변수를 복제 계약의 왼쪽 노드로 설정합니다.
 - 올바른 변수를 복제 계약의 올바른 노드로 설정합니다.

- **direction** 변수를 reinitializing 데이터의 방향으로 설정합니다. 왼쪽에서 오른쪽 방향은 데이터가 왼쪽 노드에서 오른쪽 노드로 전송됨을 의미합니다.
- **state** 변수가 다시 초기화 되도록 설정되어 있는지 확인합니다. 이는 현재 예제에서 수정된 Ansible 플레이북 파일입니다.

```
---
- name: Playbook to handle topologysegment
  hosts: ipaserver
  become: true

  tasks:
  - name: Reinitialize topology segment
    ipatopologysegment:
      ipaadmin_password: Secret123
      suffix: domain
      left: server.idm.example.com
      right: replica.idm.example.com
      direction: left-to-right
      state: reinitialized
```

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

```
$ ansible-playbook -v -i inventory reinitialize-topologysegment-copy.yml
```

추가 리소스

- 복제 계약, [Topology Suffixes](#), [Topology Segments](#)를 참조하십시오.
- `/usr/share/doc/ansible-freeipa/` 디렉토리에 있는 `README-topology.md` 파일을 참조하십시오.
- `/usr/share/doc/ansible-freeipa/playbooks/topology` 디렉토리에서 샘플 플레이북을 참조하십시오.

3.6. ANSIBLE을 사용하여 IDM에 복제 주석이 없는지 확인

IdM(Identity Management) 서버에 저장된 데이터는 복제 계약을 기반으로 복제됩니다. 두 서버에 복제 계약이 구성된 경우 해당 데이터가 공유됩니다. 복제 계약은 항상 서로 구분되며 데이터는 첫 번째 복제본에서 다른 복제본으로 복제되고 다른 복제본에서 첫 번째 복제본으로 복제됩니다.

이 섹션에서는 두 복제본 간의 복제 계약이 IdM에 없는지 확인하는 방법에 대해 설명합니다. 이 예제에서는 `replica01.idm.example.com` 과 `replica02.idm.example.com` IdM 서버 간에 도메인 유형의 복제 계약이 없는지 확인하는 방법을 설명합니다.

사전 요구 사항

- 토폴로지의 [복제본](#) 연결에 나열된 IdM 토폴로지 설계에 대한 권장 사항을 이해하고 있는지 확인합니다.
- IdM 관리자 암호를 알고 있습니다.
- 다음 요구 사항을 충족하는 Ansible 제어 노드를 구성했습니다.

- Ansible 버전 2.8 이상을 사용하고 있습니다.
- Ansible 컨트롤러에 **ansible-freeipa** 패키지를 설치했습니다.
- `~/MyPlaybooks/` 디렉터리에 이러한 옵션을 구성하는 IdM 서버의 FQDN(정규화된 도메인 이름)을 사용하여 **Ansible 인벤토리 파일**을 생성했습니다.

절차

1. `~/MyPlaybooks/` 디렉터리로 이동합니다.

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

2. `/usr/share/doc/ansible-freeipa/playbooks/topology/` 디렉터리에 있는 **delete-topologysegment.yml** Ansible 플레이북 파일을 복사합니다.

```
$ cp /usr/share/doc/ansible-freeipa/playbooks/topology/delete-topologysegment.yml
delete-topologysegment-copy.yml
```

3. 편집할 **delete-topologysegment-copy.yml** 파일을 엽니다.
4. **ipatopologysegment** 작업 섹션에서 다음 변수를 설정하여 파일을 조정합니다.
 - **ipaadmin_password** 변수를 IdM 관리자 의 암호로 설정합니다.
 - 접미사 변수를 **domain** 으로 설정합니다. 또는 왼쪽과 오른쪽 노드 간에 **ca** 데이터가 복제되지 않도록 하는 경우 변수를 **ca** 로 설정합니다.
 - 왼쪽 변수를 복제 계약의 왼쪽 노드인 IdM 서버의 이름으로 설정합니다.
 - 올바른 변수를 복제 계약의 올바른 노드인 IdM 서버의 이름으로 설정합니다.
 - **state** 변수가 **absent** 로 설정되어 있는지 확인합니다.

이는 현재 예제에서 수정된 Ansible 플레이북 파일입니다.

```
---
- name: Playbook to handle topologysegment
  hosts: ipaserver
  become: true

  tasks:
  - name: Delete topology segment
    ipatopologysegment:
      ipaadmin_password: Secret123
      suffix: domain
      left: replica01.idm.example.com
      right: replica02.idm.example.com:
      state: absent
```

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

```
$ ansible-playbook -v -i inventory delete-topologysegment-copy.yml
```

추가 리소스

- [복제 계약, Topology Suffixes, Topology Segments](#)를 참조하십시오.
- `/usr/share/doc/ansible-freeipa/` 디렉토리에 있는 **README-topology.md** 파일을 참조하십시오.
- `/usr/share/doc/ansible-freeipa/playbooks/topology` 디렉터리에서 샘플 플레이북을 참조하십시오.

3.7. 추가 리소스

- [복제본 토폴로지 계획](#)에서 참조하십시오.
- [IdM 복제본 설치](#)를 참조하십시오.

4장. 숨겨진 복제본 검증 또는 승격

복제본이 설치되면 복제본이 숨겨지거나 표시되는지 여부를 구성할 수 있습니다.

숨겨진 복제본에 대한 자세한 내용은 [숨겨진 복제본 모드](#) 를 참조하십시오.

복제본이 CA 갱신 서버인 경우 이 복제본이 숨겨지기 전에 서비스를 다른 복제본으로 이동합니다.

자세한 내용은 을 참조하십시오.

절차

- 복제본을 숨기려면 다음을 입력합니다.

```
# ipa server-state replica.idm.example.com --state=hidden
```

또는 다음 명령을 사용하여 복제본을 볼 수도 있습니다.

```
# ipa server-state replica.idm.example.com --state=enabled
```

5장. 상태 점검을 사용하여 IDM 복제 확인

이 섹션에서는 Healthcheck 툴을 사용하여 IdM(Identity Management) 복제를 테스트하는 방법을 설명합니다.

자세한 내용은 을 참조하십시오.

IdM의 상태 점검.

5.1. 복제 상태 테스트

Healthcheck 툴은 IdM(Identity Management) 토폴로지 구성을 테스트하고 복제 충돌 문제를 검색합니다.

모든 테스트를 나열하려면 `--list-sources` 옵션을 사용하여 `ipa-healthcheck` 을 실행합니다.

```
# ipa-healthcheck --list-sources
```

토폴로지 테스트는 `ipahealthcheck.ipa.topology` 및 `ipahealthcheck.ds.replication` 소스 아래에 배치됩니다.

IPATopologyDomainCheck

이 테스트에서는 다음을 검증합니다.

- 토폴로지의 연결이 끊어지지 않고 모든 서버 간에 복제 경로가 있습니다.
- 서버에 권장되는 복제 계약 수가 없는 경우.
테스트에 실패하면 테스트에서 연결 오류 또는 너무 많은 복제 계약과 같은 오류를 반환합니다.

테스트가 성공하면 테스트에서 구성된 도메인을 반환합니다.



참고

테스트는 도메인 및 ca 접미사 모두에 대해 `ipa topologysuffix-verify` 명령을 실행합니다(이 서버에 인증 기관을 구성하는 경우).

ReplicationConflictCheck

테스트에서는 LDAP 일치 (`&(!(!)=nsclass=nstombstone)(nsds5ReplConflict=*)`)의 항목을 검색합니다.



참고

문제를 확인하려고 할 때 모든 IdM 서버에서 이 테스트를 실행합니다.

5.2. HEALTHCHECK를 사용하여 복제 모니터링

이 섹션에서는 Healthcheck 도구를 사용하여 IdM(Identity Management) 복제 토폴로지 및 구성의 독립 실행형 수동 테스트를 설명합니다.

Healthcheck 툴에는 많은 테스트가 포함되어 있으므로 다음과 같이 결과를 단축할 수 있습니다.

- 복제 충돌 테스트: `--source=ipahealthcheck.ds.replication`

- 올바른 토폴로지 테스트: **--source=ipahealthcheck.ipa.topology**

사전 요구 사항

- 상태 점검 테스트는 root 사용자로 수행해야 합니다.

절차

- Healthcheck 복제 충돌 및 토폴로지 검사를 실행하려면 다음을 입력합니다.

```
# ipa-healthcheck --source=ipahealthcheck.ds.replication --
source=ipahealthcheck.ipa.topology
```

4 가지 다른 결과가 가능합니다:

- SUCCESS-testd가 성공적으로 통과되었습니다.

```
{
  "source": "ipahealthcheck.ipa.topology",
  "check": "IPATopologyDomainCheck",
  "result": "SUCCESS",
  "kw": {
    "suffix": "domain"
  }
}
```

- 경고: 테스트가 통과되었지만 문제가 있을 수 있습니다.
- ERROR-databind-test가 실패했습니다.

```
{
  "source": "ipahealthcheck.ipa.topology",
  "check": "IPATopologyDomainCheck",
  "result": "ERROR",
  "uuid": "d6ce3332-92da-423d-9818-e79f49ed321f",
  "when": "20191007115449Z",
  "duration": "0.005943",
  "kw": {
    "msg": "topologysuffix-verify domain failed, server2 is not connected
(server2_139664377356472 in MainThread)"
  }
}
```

- 테스트가 실패하고 IdM 서버 기능에 영향을 미칩니다.

추가 리소스

- **man ipa-healthcheck** 를 참조하십시오.