Red Hat Enterprise Linux 8

Identity Management에서 성능 튜닝

보다 나은 성능을 위해 Directory Server,ECDHE 및 SSSD와 같은 IdM 서비스 최적화

Last Updated: 2023-09-26

Red Hat Enterprise Linux 8 Identity Management에서 성능 튜닝

보다 나은 성능을 위해 Directory Server,ECDHE 및 SSSD와 같은 IdM 서비스 최적화

법적 공지

초록

Red Hat은 대부분의 배포에서 제대로 수행하기 위해 IdM(Identity Management)을 조정합니다. 그러나 특정 시나리오에서는 복제 계약, 디렉터리 서버, KDC(Kerberos Key Distribution Center) 또는 SSSD(System Security Services Daemon)와 같은 IdM 구성 요소를 조정하는 것이 유용할 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.

Identity Management에서 용어 교체는 다음과 같습니다.

- *블랙리스트*를 ***블록 목록***으로 대체
- *화이트리스트*를 ***허용 목록***으로 대체
- *슬레이브*를 ***보조***로 대체
- 컨텍스트에 따라 *마스터*라는 단어가 보다 정확한 용어로 교체되고 있습니다.
  - *IdM 마스터*를 ***IdM 서버***로 대체
  - *CA 갱신 마스터*를 ***CA 갱신 서버***로 대체
  - *CRL 마스터*를 ***CRL 게시자 서버***로 대체
  - *multi-master*를 ***multi-supplier***로 교체

RED HAT 문서에 관한 피드백 제공

문서 개선을 위한 의견에 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. **요약** 필드에 설명 제목을 입력합니다.
4. **설명** 필드에 개선을 위한 제안을 입력합니다. 문서의 관련 부분에 대한 링크를 포함합니다.
5. 대화 상자 하단에서 **생성** 을 클릭합니다.

1장. IDM 튜닝 시 중요한 고려 사항

ID 관리의 구성 요소 서비스는 대부분의 배포에 최적으로 작동하도록 조정됩니다. 시스템 관리자는 특정 환경의 요구에 맞게 IdM 서비스의 성능을 조정할 수 있습니다.

중요한 고려 사항

- 각 IdM 배포는 하드웨어, 소프트웨어, 네트워킹, 데이터, 워크로드 및 기타 여러 요인의 고유한 조합입니다. 하나의 환경에 도움이 되는 조정은 다른 환경에 해가 될 수 있습니다.
- 성능 튜닝은 반복적이고 실험적인 프로세스입니다. Red Hat은 한 번에 하나의 변수를 수정하고 환경에 미치는 영향을 모니터링할 것을 권장합니다. 하나의 변수로 원하는 결과를 얻은 후 다음 변수를 조정하면서 이전 조정의 성능을 계속 모니터링합니다.

2장. 하드웨어 권장 사항

RAM은 적절한 크기 조정에 가장 중요한 하드웨어 기능입니다. 시스템에 사용 가능한 RAM이 충분한지 확인합니다. 일반적인 RAM 요구 사항은 다음과 같습니다.

- 10,000명의 사용자 및 100개의 그룹: 최소 4GB의 RAM 및 4GB 스왑 공간
- 사용자 100,000명 및 50,000개 그룹의 경우: 최소 16GB의 RAM 및 4GB의 스왑 공간

대규모 배포의 경우 대부분의 데이터가 캐시에 저장되므로 디스크 공간을 늘리는 것보다 RAM을 늘리는 것이 더 효율적입니다. 일반적으로 RAM을 추가하면 캐싱으로 인해 대규모 배포를 위해 성능이 향상됩니다.

참고

기본 사용자 항목 또는 인증서가 있는 간단한 호스트 항목은 약 5-10 kB)입니다.

3장. IDM에서 페일오버, 로드 밸런싱 및 고가용성

IdM(Identity Management)에는 IdM 클라이언트에 대한 페일오버 메커니즘이 내장되어 있으며 IdM 서버의 부하 분산 및 고가용성 기능이 있습니다.

3.1. 클라이언트 측 장애 조치 기능

- 기본적으로 IdM 클라이언트의 **SSSD** 서비스는 DNS의 서비스(SRV) 리소스 레코드를 사용하여 연결할 최상의 IdM 서버를 자동으로 결정하도록 구성됩니다. 이 동작은 **/etc/sssd/sssd.conf** 파일의 **ipa_server** 매개변수에 있는 **_srv_** 옵션으로 제어됩니다.

```
[root@client ~]# cat /etc/sssd/sssd.conf

[domain/example.com]
id_provider = ipa
ipa_server = _srv_, server.example.com
...
```

  IdM 서버가 오프라인 상태가 되면 IdM 클라이언트의 SSSD 서비스가 자동으로 검색한 다른 IdM 서버에 연결됩니다.

- 성능상의 이유로 DNS 조회를 바이패스하려면 **ipa_server** 매개변수에서 **_srv_** 항목을 제거하고 클라이언트가 연결해야 하는 IdM 서버를 우선 순위로 지정합니다.

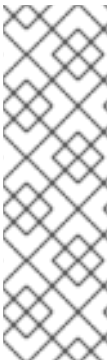
```
[root@client ~]# cat /etc/sssd/sssd.conf

[domain/example.com]
id_provider = ipa
ipa_server = server1.example.com, server2.example.com
...
```

3.2. 서버 측 로드 밸런싱 및 서비스 가용성

여러 IdM 복제본을 설치하여 IdM에서 로드 밸런싱 및 고가용성을 얻을 수 있습니다.

- 지리적으로 분산된 네트워크가 있는 경우 데이터 센터당 여러 IdM 복제본을 구성하여 IdM 클라이언트와 가장 가까운 액세스 가능 서버 간 경로를 단축할 수 있습니다.
- Red Hat은 최대 60개의 복제본이 있는 환경을 지원합니다.
- IdM 복제 메커니즘은 활성/활성 서비스 가용성을 제공합니다. 모든 IdM 복제본의 서비스를 동시에 쉽게 사용할 수 있습니다.



참고

Red Hat은 IdM 및 기타 로드 밸런싱 또는 HA(고가용성) 소프트웨어를 결합하는 것을 권장합니다.

많은 타사 고가용성 솔루션은 활성/수동 시나리오를 가정하고 IdM 가용성에 대한 불필요한 서비스가 중단됩니다. 다른 솔루션에서는 클러스터형 서비스당 가상 IP 또는 단일 호스트 이름을 사용합니다. 일반적으로 이러한 모든 방법은 IdM 솔루션에서 제공하는 서비스 가용성 유형과 제대로 작동하지 않습니다. 또한 Kerberos와 매우 부적절하게 통합되므로 전체 보안 및 배포의 안정성이 감소합니다.

4장. 복제본 토폴로지 최적화

강력한 복제본 토폴로지는 워크로드를 배포하고 복제 지연을 줄입니다. 다음 지침에 따라 복제본 토폴로지의 레이아웃을 최적화합니다.

4.1. 토폴로지에서 적절한 IDM 복제본 수를 결정하는 지침

각 데이터 센터에 두 개 이상의 복제본 설정(하드 요구 사항이 아님)

데이터센터는 예를 들어 주 사무실 또는 지리적 위치일 수 있습니다.

클라이언트 서비스를 제공하기에 충분한 수의 서버를 설정

하나의 IdM(Identity Management) 서버는 2000 - 3000 클라이언트에 서비스를 제공할 수 있습니다. 이 경우 클라이언트는 서버를 하루에 여러 번 쿼리하지만 예를 들어 1분마다 쿼리하지는 않습니다. 더 자주 쿼리를 예상하면 더 많은 서버를 계획할 수 있습니다.

충분한 수의 CA(인증 기관) 복제본 설정

CA 역할이 설치된 복제본만 인증서 데이터를 복제할 수 있습니다. IdM CA를 사용하는 경우 환경에 인증서 복제 계약이 있는 두 개 이상의 CA 복제본이 있는지 확인합니다.

단일 IdM 도메인에서 최대 60개의 복제본 설정

Red Hat은 최대 60개의 복제본이 있는 환경을 지원합니다.

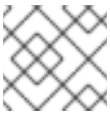
4.2. 토폴로지에서 IDM 복제본 연결 지침

각 복제본을 두 개 이상의 다른 복제본에 연결

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

복제본을 최대 4개의 다른 복제본에 연결(하드 요구 사항 아님)

서버당 다수의 복제 계약은 상당한 이점을 제공하지 않습니다. 수신 복제본은 한 번에 하나의 다른 복제본에서만 업데이트할 수 있으며 다른 복제 계약은 유휴 상태입니다. 복제본당 4개 이상의 복제 계약은 일반적으로 리소스를 낭비함을 의미합니다.



참고

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

복제본당 복제 계약 4개에 대한 두 가지 예외가 있습니다.

- 특정 복제본이 온라인 또는 응답하지 않는 경우 장애 조치 경로가 필요합니다.
- 대규모 배포에서 특정 노드 간 직접 링크를 추가로 연결하려고 합니다.

다수의 복제 계약을 구성하면 전반적인 성능에 부정적인 영향을 미칠 수 있습니다. 즉 토폴로지의 여러 복제 계약이 업데이트를 전송하는 경우 특정 복제본에서 들어오는 업데이트와 발신 업데이트 간에 changelog 데이터베이스 파일에 대한 높은 경합이 발생할 수 있습니다.

복제본당 더 많은 복제 계약을 사용하려면 복제 문제 및 대기 시간이 발생하지 않도록 합니다. 그러나 큰 거리와 높은 수의 중간 노드도 대기 시간 문제가 발생할 수 있습니다.

데이터 센터의 복제본을 서로 연결

이렇게 하면 데이터 센터 내의 도메인 복제가 가능합니다.

각 데이터 센터를 두 개 이상의 다른 데이터 센터에 연결

이렇게 하면 데이터 센터 간 도메인 복제가 가능합니다.

최소 한 쌍의 복제 계약을 사용하여 데이터 센터 연결

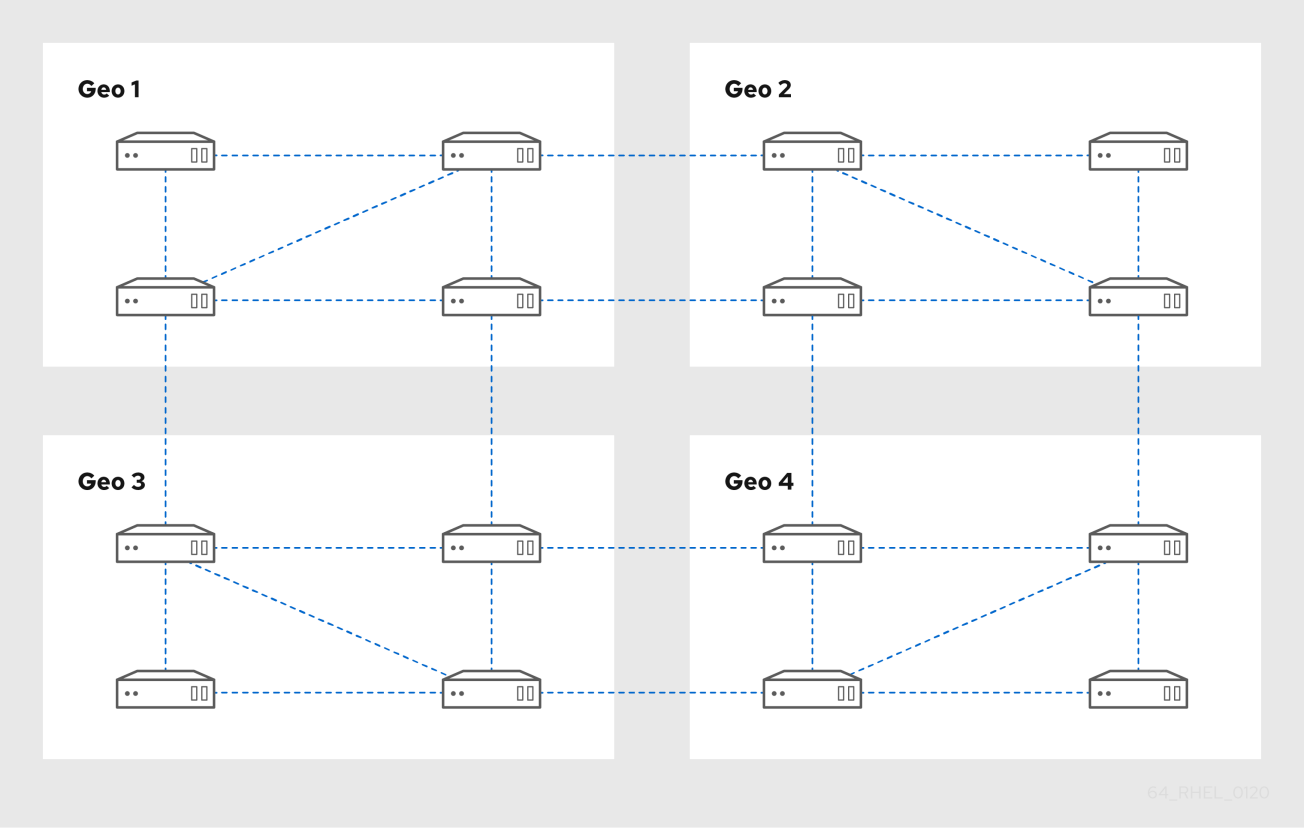
데이터 센터 A 및 B에 A1에서 B1로의 복제 계약이 있는 경우 A2에서 B2로 복제 계약을 보유하면 서버 중 하나가 다운된 경우 두 데이터 센터 간에 복제를 계속할 수 있습니다.

4.3. 복제본 토폴로지 예

아래 그림은 안정적인 토폴로지 생성 지침을 기반으로 IdM(Identity Management) 토폴로지의 예를 보여줍니다.

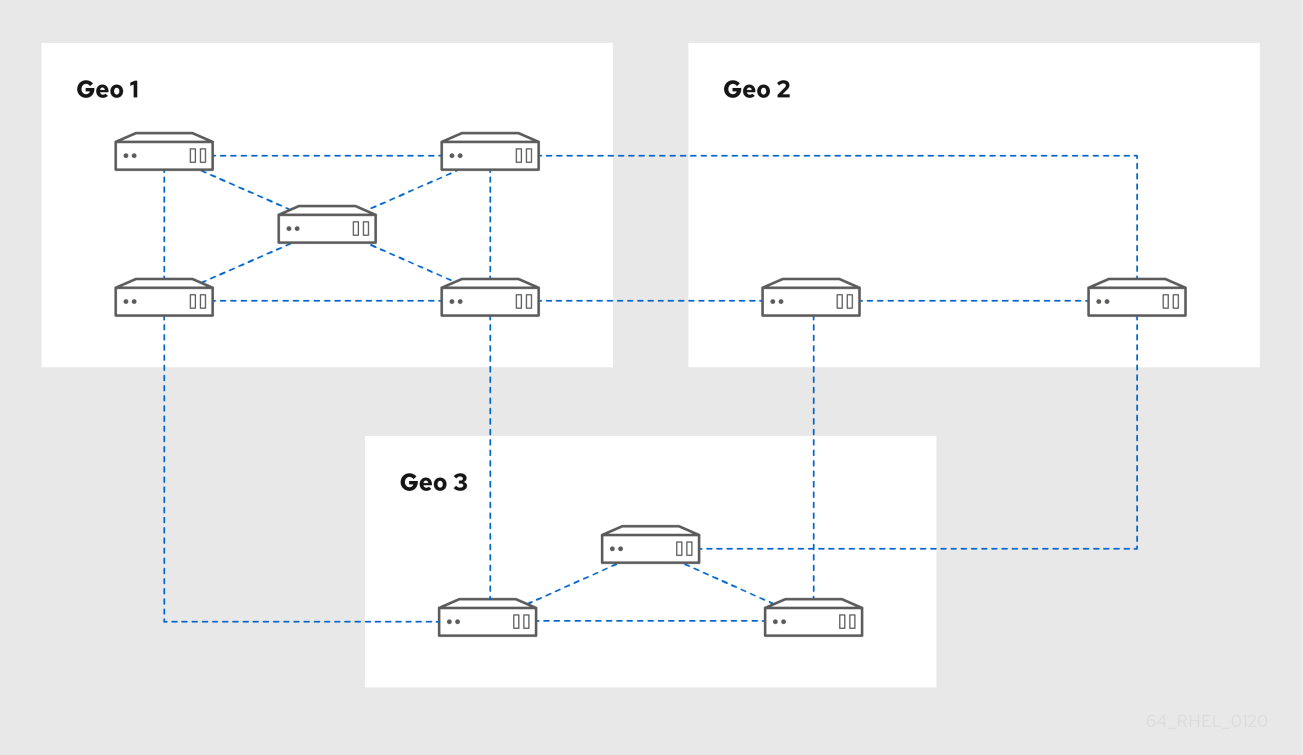
복제 토폴로지 예제 1 에는 각각 4개의 서버가 있는 데이터 센터 4개가 표시되어 있습니다. 서버는 복제 계약과 연결되어 있습니다.

그림 4.1. 복제본 토폴로지 예 1



복제 토폴로지 예제 2 는 각각 다른 수의 서버가 있는 3개의 데이터 센터를 보여줍니다. 서버는 복제 계약과 연결되어 있습니다.

그림 4.2. 복제본 토폴로지 예 2



4.4. 추가 리소스

- 복제본 토폴로지 계획.
- 복제 토폴로지 관리.

5장. 검색 크기 및 시간 제한 조정

IdM 사용자 목록을 요청하는 것과 같은 일부 쿼리는 매우 많은 항목을 반환할 수 있습니다. 이러한 검색 작업을 튜닝하면 **ipa user-find** 명령과 같은 **ipa *-find** 명령을 실행할 때와 웹 UI에 해당 목록을 표시할 때 전체 서버 성능을 향상시킬 수 있습니다.

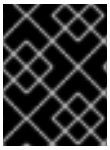
검색 크기 제한

클라이언트 CLI 또는 IdM 웹 UI에 액세스하는 브라우저에서 서버로 전송된 요청에 대해 반환된 최대 항목 수를 정의합니다.
기본값: 100개 항목.

검색 시간 제한

서버에서 검색이 실행될 때까지 대기하는 최대 시간(초)을 정의합니다. 검색이 이 제한에 도달하면 서버는 검색을 중지하고 해당 시간에 검색된 항목을 반환합니다.
기본값: 2초.

값을 **-1** 로 설정하면 검색 시 IdM에 제한이 적용되지 않습니다.



중요

검색 크기 또는 시간 제한을 너무 높게 설정하면 서버 성능에 부정적인 영향을 미칠 수 있습니다.

5.1. 명령줄에서 검색 크기 및 시간 제한 조정

다음 절차에서는 명령줄에서 검색 크기 및 시간 제한 조정에 대해 설명합니다.

- 전역적으로
- 특정 항목의 경우

절차

1. CLI에 현재 검색 시간 및 크기 제한을 표시하려면 **ipa config-show** 명령을 사용합니다.

```
$ ipa config-show

Search time limit: 2
Search size limit: 100
```

2. 모든 쿼리에 대해 **전역적으로** 제한을 조정하려면 **ipa config-mod** 명령을 사용하고 **--searchrecordslimit** 및 **--searchtimelimit** 옵션을 추가합니다. 예를 들면 다음과 같습니다.

```
$ ipa config-mod --searchrecordslimit=500 --searchtimelimit=5
```

3. 특정 쿼리에 대해서만 제한을 **일시적으로** 조정하려면 명령에 **--sizelimit** 또는 **--timelimit** 옵션을 추가합니다. 예를 들면 다음과 같습니다.

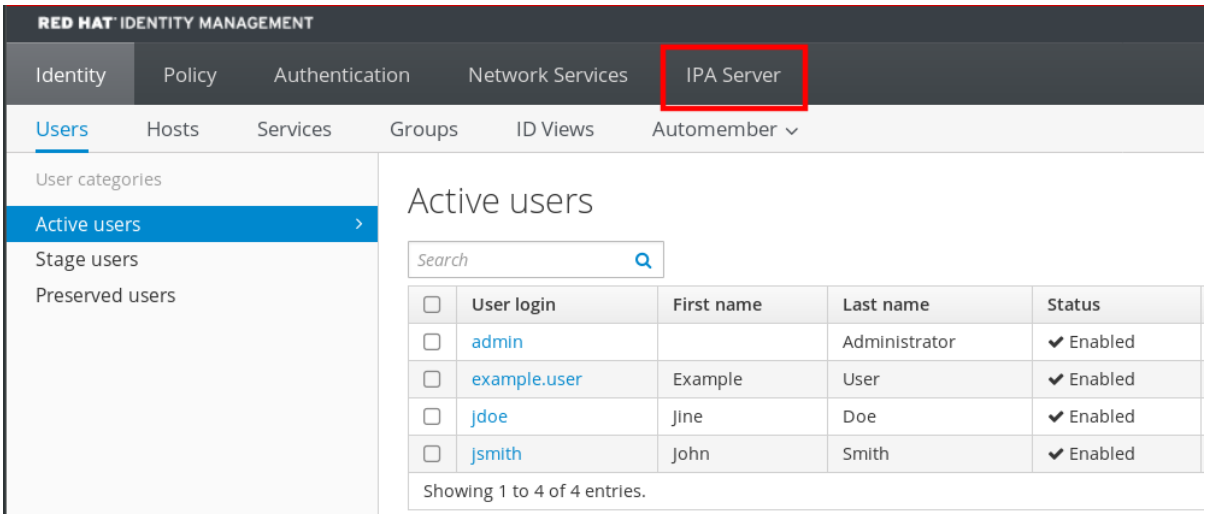
```
$ ipa user-find --sizelimit=200 --timelimit=120
```

5.2. 웹 UI에서 검색 크기 및 시간 제한 조정

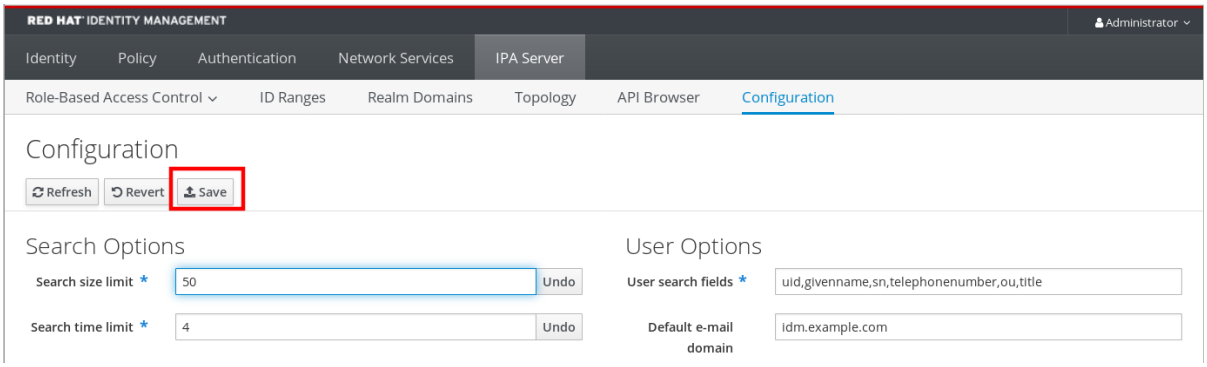
다음 절차에서는 IdM 웹 UI의 글로벌 검색 크기 및 시간 제한 조정에 대해 설명합니다.

절차

1. IdM 웹 UI에 로그인합니다.
2. **IPA Server** 를 클릭합니다.



3. **IPA Server** 탭에서 **Configuration** 을 클릭합니다.
4. **Search Options** (검색 옵션) 영역에 필요한 값을 설정합니다.
   기본값은 다음과 같습니다.
   - 검색 크기 제한: 100개 항목
   - 검색 시간 제한: 2초
5. 페이지 위쪽에서 **저장을** 클릭합니다.



6장. IDM DIRECTORY SERVER 성능 조정

Directory Server의 리소스 및 동작을 제어하는 LDAP 특성을 조정하여 ID 관리의 데이터베이스 성능을 조정할 수 있습니다.

Directory Server에서 **데이터를 캐시** 하는 방법을 조정하려면 다음 절차를 참조하십시오.

- 항목 캐시 크기 조정
- 데이터베이스 인덱스 캐시 크기 조정
- 입력 및 데이터베이스 캐시 자동 크기 조정 활성화
- DN 캐시 크기 조정
- 정규화된 DN 캐시 크기 조정

Directory Server의 **리소스 제한을** 조정하려면 다음 절차를 참조하십시오.

- 최대 메시지 크기 조정
- 최대 파일 설명자 수 조정
- 연결 백로그 크기 조정
- 최대 데이터베이스 잠금 수 조정

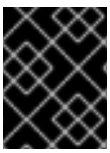
성능에 가장 큰 영향을 미치는 **타임아웃** 을 조정하려면 다음 절차를 참조하십시오.

- 입력/출력 블록 타임아웃 조정
- 유휴 연결 타임아웃 조정
- 복제 릴리스 타임아웃 조정

LDIF 파일에서 사용자 지정 Directory Server 설정을 사용하여 IdM 서버 또는 복제본을 설치하려면 다음 절차를 참조하십시오.

- LDIF 파일에서 사용자 지정 database-settings를 사용하여 IdM 서버 또는 복제본 설치

6.1. 항목 캐시 크기 조정



중요

성능을 최적화하기 위해 기본 제공 캐시 자동 크기 조정 기능을 사용하는 것이 좋습니다. 자동 튜닝된 값에서 의도적으로 벗어나야 하는 경우에만 이 값을 변경합니다.

nsslapd-cachememsize 속성은 항목 캐시에 사용 가능한 메모리 공간에 크기(바이트)를 지정합니다. 이 속성은 디렉토리 서버가 사용하는 물리적 RAM을 제어하는 데 가장 중요한 값 중 하나입니다.

항목 캐시 크기가 너무 작으면 **/var/log/dirsrv/slapd-*INSTANCE-NAME*/errors** 로그 파일에 Directory Server 오류 로그에 다음 오류가 표시될 수 있습니다.

> REASON: entry too large (*83886080* bytes) for the import buffer size (*67108864* bytes). **Try increasing nsslapd-cachememsize.**

Red Hat은 진입점 캐시와 데이터베이스 인덱스 항목 캐시를 메모리에 조정하는 것이 좋습니다.

기본값	**209715200** *(200 MiB)*
유효한 범위	**500000 - 18446744073709551615** *(500 kB - (2^{64}-1))*
DN 항목 위치	**cn=*database-name*,cn=ldbm database,cn=plugins,cn=config**

사전 요구 사항

- LDAP Directory Manager 암호

절차

1. 자동 캐시 튜닝을 비활성화합니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com
backend config set --cache-autosize=0
```

2. 데이터베이스 접미사와 해당 백엔드를 표시합니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com
backend suffix list
cn=changelog (changelog)
dc=example,dc=com (userroot)
o=ipaca (ipaca)
```

이 명령은 각 접미사 옆에 있는 백엔드 데이터베이스의 이름을 표시합니다. 다음 단계에서 접미사의 데이터베이스 이름을 사용합니다.

3. 데이터베이스의 항목 캐시 크기를 설정합니다. 이 예에서는 userroot 데이터베이스의 항목 캐시를 2GB로 설정합니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com
backend suffix set --cache-memsize=2147483648 userroot
```

4. Directory Server를 다시 시작합니다.

```
[root@server ~]# systemctl restart dirsrv.target
```

5. IdM 디렉터리 서버의 성능을 모니터링합니다. 바람직한 방식으로 변경되지 않으면 이 절차를 반복하고 **cache-memsize** 를 다른 값으로 조정하거나 캐시 자동 크기 조정을 다시 활성화합니다.

검증 단계

- **nsslapd-cachememsize** 특성 값을 표시하고 원하는 값으로 설정되어 있는지 확인합니다.

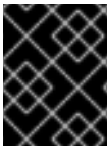
```
[root@server ~]# ldapsearch -D "cn=directory manager" -w DirectoryManagerPassword
-b "cn=userroot,cn=ldbm database,cn=plugins,cn=config" | grep nsslapd-
cachememsize
```

```
nsslapd-cachememsize: 2147483648
```

추가 리소스

- Directory Server 11 문서의 nsslapd-cachememsize
- 항목 및 데이터베이스 캐시 자동 크기 조정을 다시 활성화합니다 .

6.2. 데이터베이스 인덱스 캐시 크기 조정



중요

성능을 최적화하기 위해 기본 제공 캐시 자동 크기 조정 기능을 사용하는 것이 좋습니다. 자동 튜닝된 값에서 의도적으로 벗어나야 하는 경우에만 이 값을 변경합니다.

nsslapd-dbcachesize 속성은 데이터베이스 인덱스가 사용하는 메모리 양을 제어합니다. 이 캐시 크기는 입력 캐시 크기보다 Directory Server 성능에 미치는 영향은 적지만 항목 캐시 크기가 설정된 후 사용 가능한 RAM이 있는 경우 데이터베이스 캐시에 할당된 메모리 양을 늘리는 것이 좋습니다.

데이터베이스 캐시는 1.5GB RAM으로 제한됩니다. 높은 값은 성능을 향상시키지 않기 때문입니다.

기본값	**10000000** *(10MB)*
유효한 범위	**500000 - 1610611911** *(500 KB - 1.5GB)*
DN 항목 위치	**cn=config,cn=ldbm database,cn=plugins,cn=config**

사전 요구 사항

- LDAP Directory Manager 암호

절차

1. 자동 캐시 튜닝을 비활성화하고 데이터베이스 캐시 크기를 설정합니다. 이 예에서는 데이터베이스 캐시를 256MB로 설정합니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com
backend config set --cache-autosize=0 --dbcachesize=268435456
```

2. Directory Server를 다시 시작합니다.

```
[root@server ~]# systemctl restart dirsrv.target
```

3. IdM 디렉터리 서버의 성능을 모니터링합니다. 바람직한 방식으로 변경되지 않으면 이 절차를 반복하고 **dbcachesize** 를 다른 값으로 조정하거나 캐시 자동 크기 조정을 다시 활성화합니다.

검증 단계

- **nsslapd-dbcachesize** 특성 값을 표시하고 원하는 값으로 설정되어 있는지 확인합니다.

```
[root@server ~]# ldapsearch -D "cn=directory manager" -w DirectoryManagerPassword
-b "cn=config,cn=ldbm database,cn=plugins,cn=config" | grep nsslapd-dbcachesize
nsslapd-dbcachesize: 2147483648
```

추가 리소스

- Directory Server 11 문서의 nsslapd-dbcachesize
- 항목 및 데이터베이스 캐시 자동 크기 조정을 다시 활성화합니다 .

6.3. 데이터베이스 및 진입점 캐시 자동 크기 조정 활성화

중요

성능을 최적화하기 위해 기본 제공 캐시 자동 크기 조정 기능을 사용하는 것이 좋습니다. Red Hat은 캐시 크기를 수동으로 설정하는 것을 권장하지 않습니다.

기본적으로 IdM 디렉터리 서버는 데이터베이스 캐시 및 입력 캐시에 가장 적합한 크기를 자동으로 결정합니다. 사용 가능한 RAM의 일부를 제외하고 자동 크기 조정 세트를 설정하고 인스턴스가 시작될 때 서버의 하드웨어 리소스에 따라 두 캐시의 크기를 최적화합니다.

이 절차를 사용하여 사용자 정의 데이터베이스 캐시 및 항목 캐시 값을 취소하고 캐시 자동 크기 조정 기능을 기본값으로 복원합니다.

nsslapd-cache-autosize	이 설정은 데이터베이스 및 항목 캐시 자동 크기 조정을 위해 할당된 여유 RAM 양을 제어합니다. 값이 **0** 이면 자동 크기 조정이 비활성화됩니다.
기본값	**10** *(10 %의 무료 RAM)*
유효한 범위	**0 - 100**
DN 항목 위치	**cn=config,cn=ldbm database,cn=plugins,cn=config**

nsslapd-cache-autosize-split	이 값은 데이터베이스 캐시에 사용되는 **nsslapd-cache-autosize** 에 의해 결정된 사용 가능한 메모리의 백분율을 설정합니다. 나머지 백분율은 항목 캐시에 사용됩니다.
기본값	**25** *(데이터베이스 캐시의 경우 25%, 입력 캐시의 경우 60%)*
유효한 범위	**0 - 100**
DN 항목 위치	**cn=config,cn=ldbm database,cn=plugins,cn=config**

사전 요구 사항

- 이전에 데이터베이스 및 진입점 캐시 자동 튜닝을 비활성화했습니다.

절차

1. Directory Server를 중지합니다.

```
[root@server ~]# systemctl stop dirsrv.target
```

2. 추가로 수정하기 전에 **/etc/dirsrv/*slapd-instance_name*/dse.ldif** 파일을 백업하십시오.

```
[root@server ~]# *cp /etc/dirsrv/slapd-instance_name/dse.ldif \
    /etc/dirsrv/slapd-instance_name/dse.ldif.bak.$(date "+%F_%H-%M-%S")
```

3. **/etc/dirsrv/*slapd-instance_name*/dse.ldif** 파일을 편집합니다.

   a. 데이터베이스 및 항목 캐시에 사용할 사용 가능한 시스템 RAM의 백분율을 사용 가능한 RAM의 10%의 기본값인 10%로 다시 설정합니다.

   ```
   nsslapd-cache-autosize: 10
   ```

   b. 데이터베이스 캐시의 사용 가능한 시스템 RAM에서 사용된 백분율을 기본값인 25%로 설정합니다.

   ```
   nsslapd-cache-autosize-split: 25
   ```

4. 변경 사항을 **/etc/dirsrv/*slapd-instance_name*/dse.ldif** 파일에 저장합니다.

5. Directory Server를 시작합니다.

```
[root@server ~]# systemctl start dirsrv.target
```

검증 단계

- **nsslapd-cache-autosize** 및 **nsslapd-cache-autosize-split** 속성 값을 표시하고 원하는 값으로 설정되어 있는지 확인합니다.

```
[root@server ~]# ldapsearch -D "cn=directory manager" -w DirectoryManagerPassword
-b "cn=config,cn=ldbm database,cn=plugins,cn=config" | grep nsslapd-cache-autosize
nsslapd-cache-autosize: *10
nsslapd-cache-autosize-split: 25
```

추가 리소스

- Directory Server 11 문서의 nsslapd-cache-autosize

6.4. DN 캐시 크기 조정

중요

성능을 최적화하기 위해 기본 제공 캐시 자동 크기 조정 기능을 사용하는 것이 좋습니다. 자동 튜닝된 값에서 의도적으로 벗어나야 하는 경우에만 이 값을 변경합니다.

nsslapd-dncachememsize 속성은 Distinguished Names(DN) 캐시에 사용할 수 있는 메모리 공간에 크기(바이트)를 지정합니다. DN 캐시는 데이터베이스의 항목 캐시와 유사하지만 해당 표에서는 항목 ID와 DN 항목만 저장하므로 **이름 변경** 및 **moddn** 작업 시 더 빠르게 조회할 수 있습니다.

기본값	**10485760** *(10 MB)*
유효한 범위	**500000 - 18446744073709551615** *(500 kB - (2^{64}-1))*
DN 항목 위치	**cn=*database-name*,cn=ldbm database,cn=plugins,cn=config**

사전 요구 사항

- LDAP Directory Manager 암호

절차

1. *(선택 사항)* 데이터베이스 접미사와 해당 데이터베이스 이름을 표시합니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com
backend suffix list
dc=example,dc=com (userroot)
```

   이 명령은 각 접미사 옆에 있는 백엔드 데이터베이스의 이름을 표시합니다. 다음 단계에서 접미사의 데이터베이스 이름을 사용합니다.

2. 데이터베이스의 DN 캐시 크기를 설정합니다. 이 예에서는 DN 캐시를 20MB로 설정합니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com
backend suffix set --dncache-memsize=20971520 userroot
```

3. Directory Server를 다시 시작합니다.

```
[root@server ~]# systemctl restart dirsrv.target
```

4. IdM 디렉터리 서버의 성능을 모니터링합니다. 바람직한 방식으로 변경되지 않으면 이 절차를 반복하고 **dncache-memsize** 를 다른 값으로 조정하거나 기본값으로 10MB로 되돌립니다.

검증 단계

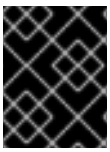
- **nsslapd-dncachememsize** 속성의 새 값을 표시하고 원하는 값으로 설정되어 있는지 확인합니다.

```
[root@server ~]# ldapsearch -D "cn=directory manager" -w DirectoryManagerPassword
-b "cn=userroot,cn=ldbm database,cn=plugins,cn=config" | grep nsslapd-
dncachememsize
nsslapd-dncachememsize: 20971520
```

추가 리소스

- Directory Server 11 문서의 nsslapd-dncachememsize

6.5. 정규화된 DN 캐시 크기 조정



중요

성능을 최적화하기 위해 기본 제공 캐시 자동 크기 조정 기능을 사용하는 것이 좋습니다. 자동 튜닝된 값에서 의도적으로 벗어나야 하는 경우에만 이 값을 변경합니다.

nsslapd-ndn-cache-max-size 속성은 정규화된 고유 이름(NDN)을 저장하는 캐시의 크기를 바이트 단위로 제어합니다. 이 값을 늘리면 더 자주 사용되는 DN이 메모리에 유지됩니다.

기본값	**20971520** *(20MB)*
유효한 범위	**0 - 2147483647**
DN 항목 위치	**cn=config**

사전 요구 사항

- LDAP Directory Manager 암호

절차

1. NDN 캐시가 활성화되어 있는지 확인합니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com config
get nsslapd-ndn-cache-enabled
Enter password for cn=Directory Manager on ldap://server.example.com:
nsslapd-ndn-cache-enabled: on
```

캐시가 **꺼져** 있으면 다음 명령을 사용하여 활성화합니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com config
replace nsslapd-ndn-cache-enabled=on
Enter password for cn=Directory Manager on ldap://server.example.com:
Successfully replaced "nsslapd-ndn-cache-enabled"
```

2. **nsslapd-ndn-cache-max-size** 매개변수의 현재 값을 검색하고 복원해야 하는 경우 조정하기 전에 기록해 둡니다. 메시지가 표시되면 Directory Manager 암호를 입력합니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com config
get nsslapd-ndn-cache-max-size
Enter password for cn=Directory Manager on ldap://server.example.com:
nsslapd-ndn-cache-max-size: 20971520
```

3. **nsslapd-ndn-cache-max-size** 특성 값을 수정합니다. 이 예에서는 값을 **41943040** (40MB)으로 늘립니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com config
replace nsslapd-ndn-cache-max-size=41943040
```

4. IdM 디렉터리 서버의 성능을 모니터링합니다. 바람직한 방식으로 변경되지 않으면 이 절차를 반복하고 **nsslapd-ndn-cache-max-size** 를 다른 값으로 조정하거나 캐시 자동 크기 조정을 다시 활성화합니다.

검증 단계

- **nsslapd-ndn-cache-max-size** 속성의 새 값을 표시하고 원하는 값으로 설정되어 있는지 확인합니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com config get nsslapd-ndn-cache-max-size
Enter password for cn=Directory Manager on ldap://server.example.com:
nsslapd-ndn-cache-max-size: 41943040
```

추가 리소스

- Directory Server 11 문서의 nsslapd-ndn-cache-max-size

6.6. 최대 메시지 크기 조정

nsslapd-maxbersize 속성은 들어오는 메시지 또는 LDAP 요청에 허용되는 최대 크기를 바이트 단위로 설정합니다. 요청 크기를 제한하면 일부 종류의 서비스 거부 공격을 방지할 수 있습니다.

최대 메시지 크기가 너무 작으면 **/var/log/dirsrv/slapd-*INSTANCE-NAME*/errors**:의 Directory Server 오류 로그에 다음 오류가 표시될 수 있습니다.

```
Incoming BER Element was too long, max allowable is 2097152 bytes. Change the nsslapd-maxbersize attribute in cn=config to increase.
```

제한은 LDAP 요청의 총 크기에 적용됩니다. 예를 들어, 요청이 항목을 추가하고 요청의 항목이 구성된 값 또는 기본값보다 큰 경우 add 요청이 거부됩니다. 그러나 제한은 복제 프로세스에는 적용되지 않습니다. 이 속성을 변경하기 전에 주의하십시오.

기본값	**2097152** *(2MB)*
유효한 범위	**0 - 2147483647** *(0 ~ 2GB)*
DN 항목 위치	**cn=config**

사전 요구 사항

- LDAP Directory Manager 암호

절차

1. **nsslapd-maxbersize** 매개변수의 현재 값을 검색하고 복원해야 하는 경우 조정하기 전에 기록해 둡니다. 메시지가 표시되면 Directory Manager 암호를 입력합니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com config get nsslapd-maxbersize
Enter password for cn=Directory Manager on ldap://server.example.com:
```

```
nsslapd-maxbersize: 2097152
```

2. **nsslapd-maxbersize** 특성 값을 수정합니다. 이 예에서는 값을 **4194304, 4** MB로 늘립니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com config
replace nsslapd-maxbersize=4194304
```

3. 구성을 변경하기 위해 Directory Manager로 인증합니다.

```
Enter password for cn=Directory Manager on ldap://server.example.com:
Successfully replaced "nsslapd-maxbersize"
```

4. IdM 디렉터리 서버의 성능을 모니터링합니다. 바람직한 방식으로 변경되지 않는 경우 이 절차를 반복하고 **nsslapd-maxbersize** 를 다른 값으로 조정하거나 기본값 **2097152** 로 돌아갑니다.

검증 단계

- **nsslapd-maxbersize** 특성 값을 표시하고 원하는 값으로 설정되어 있는지 확인합니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com config
get nsslapd-maxbersize
Enter password for cn=Directory Manager on ldap://server.example.com:
nsslapd-maxbersize: 4194304
```

추가 리소스

- Directory Server 11 문서의 nsslapd-maxbersize (최대 메시지 크기)

6.7. 최대 파일 설명자 수 조정

nsslapd-maxdescriptors 속성은 Directory Server에서 사용하는 최대 플랫폼 종속 수의 파일 설명자를 설정합니다. 파일 설명자는 클라이언트 연결, 로그 파일, 소켓 및 기타 리소스에 사용됩니다.

운영 체제가 **ns-slapd** 프로세스를 사용할 수 있는 총 파일 설명자 수보다 큰 **nsslapd-maxdescriptors** 값을 설정하면 Directory 서버에서 운영 체제를 최대 허용 가능한 값으로 쿼리한 다음 해당 값을 사용합니다.

기본값	**4096** 설명자
유효한 범위	**1 - 65535**
DN 항목 위치	**cn=config**

사전 요구 사항

- LDAP Directory Manager 암호

절차

1. **nsslapd-maxdescriptors** 매개변수의 현재 값을 검색하고 복원해야 하는 경우 조정하기 전에 기록해 둡니다. 메시지가 표시되면 Directory Manager 암호를 입력합니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com config
get nsslapd-maxdescriptors
Enter password for cn=Directory Manager on ldap://server.example.com:
nsslapd-maxdescriptors: 4096
```

2. **nsslapd-maxdescriptors** 속성 값을 수정합니다. 이 예에서는 값을 **8192** 로 늘립니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com config
replace nsslapd-maxdescriptors=8192
```

3. 구성을 변경하기 위해 Directory Manager로 인증합니다.

```
Enter password for cn=Directory Manager on ldap://server.example.com:
Successfully replaced "nsslapd-maxdescriptors"
```

4. IdM 디렉터리 서버의 성능을 모니터링합니다. 바람직한 방식으로 변경되지 않는 경우 이 절차를 반복하고 **nsslapd-maxdescriptors** 를 다른 값으로 조정하거나 기본값 **4096** 으로 돌아갑니다.

검증 단계

- **nsslapd-maxdescriptors** 속성 값을 표시하고 원하는 값으로 설정되어 있는지 확인합니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com config
get nsslapd-maxdescriptors
Enter password for cn=Directory Manager on ldap://server.example.com:
nsslapd-maxdescriptors: 8192
```

추가 리소스

- Directory Server 11 문서의 nsslapd-maxdescriptors (Maximum File Descriptors)

6.8. 연결 백로그 크기 조정

listen 서비스는 들어오는 연결을 수신하는 데 사용할 수 있는 소켓 수를 설정합니다. **nsslapd-listen-backlog-size** 값은 연결을 거부하기 전에 **sockfd** 소켓의 최대 대기열 길이를 설정합니다.

IdM 환경에서 많은 연결을 처리하는 경우 **nsslapd-listen-backlog-size** 값을 늘리는 것이 좋습니다.

기본값	**128** 개의 대기열 슬롯
유효한 범위	**0 - 9223372036854775807**
DN 항목 위치	**cn=config**

사전 요구 사항

- LDAP Directory Manager 암호

절차

1. **nsslapd-listen-backlog-size** 매개변수의 현재 값을 검색하고 복원해야 하는 경우 조정하기 전에 기록해 둡니다. 메시지가 표시되면 Directory Manager 암호를 입력합니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com config get nsslapd-listen-backlog-size
Enter password for cn=Directory Manager on ldap://server.example.com:
nsslapd-listen-backlog-size: 128
```

2. **nsslapd-listen-backlog-size** 특성 값을 수정합니다. 이 예에서는 값을 **192** 로 늘립니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com config replace nsslapd-listen-backlog-size=192
```

3. 구성을 변경하기 위해 Directory Manager로 인증합니다.

```
Enter password for cn=Directory Manager on ldap://server.example.com:
Successfully replaced "nsslapd-listen-backlog-size"
```

검증 단계

- **nsslapd-listen-backlog-size** 특성 값을 표시하고 원하는 값으로 설정되어 있는지 확인합니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com config get nsslapd-listen-backlog-size
Enter password for cn=Directory Manager on ldap://server.example.com:
nsslapd-listen-backlog-size: 192
```

추가 리소스

- Directory Server 11 문서의 nsslapd-listen-backlog-size

6.9. 최대 데이터베이스 잠금 수 조정

잠금 메커니즘은 동시에 실행할 수 있는 Directory Server 프로세스 복사본 수를 제어하고 **nsslapd-db-locks** 매개 변수는 최대 잠금 수를 설정합니다.

/var/log/dirsrv/slapd-*instance_name*/errors 로그 파일에 다음 오류 메시지가 표시되면 최대 잠금 수를 늘립니다.

```
libdb: Lock table is out of available locks
```

기본값	**50000** 잠금
유효한 범위	**0 - 2147483647**
DN 항목 위치	**cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config**

사전 요구 사항

- LDAP Directory Manager 암호

절차

1. **nsslapd-db-locks** 매개변수의 현재 값을 검색하고 복원해야 하는 경우 조정하기 전에 기록해 둡니다.

```
[root@server ~]# ldapsearch -D "cn=directory manager" -w DirectoryManagerPassword
-b "cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config" | grep nsslapd-db-
locks
nsslapd-db-locks: 50000
```

2. **locks** 속성의 값을 수정합니다. 이 예에서는 값을 **100000** 잠금으로 두 배로 늘립니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com
backend config set --locks=100000
```

3. 구성을 변경하기 위해 Directory Manager로 인증합니다.

```
Enter password for cn=Directory Manager on ldap://server.example.com:
Successfully updated database configuration
```

4. Directory Server를 다시 시작합니다.

```
[root@server ~]# systemctl restart dirsrv.target
```

검증 단계

- **nsslapd-db-locks** 속성 값을 표시하고 원하는 값으로 설정되어 있는지 확인합니다.

```
[root@server ~]# ldapsearch -D "cn=directory manager" -w DirectoryManagerPassword
-b "cn=bdb,cn=config,cn=ldbm database,cn=plugins,cn=config" | grep nsslapd-db-
locks
nsslapd-db-locks: 100000
```

추가 리소스

- Directory Server 11 문서의 nsslapd-db-locks

6.10. 입력/출력 블록 타임아웃 조정

nsslapd-ioblocktimeout 속성은 stalled LDAP 클라이언트에 대한 연결이 종료된 후 시간(밀리초)을 설정합니다. LDAP 클라이언트는 읽기 또는 쓰기 작업을 위해 I/O 진행을 수행하지 않은 경우 정지된 것으로 간주됩니다.

nsslapd-ioblocktimeout 속성 값을 줄이면 연결을 더 빨리 확보할 수 있습니다.

기본값	**10000** 밀리초
유효한 범위	**0 - 2147483647**
DN 항목 위치	**cn=config**

사전 요구 사항

- LDAP Directory Manager 암호

절차

1. **nsslapd-ioblocktimeout** 매개변수의 현재 값을 검색하고 복원해야 하는 경우 조정하기 전에 기록해 둡니다. 메시지가 표시되면 Directory Manager 암호를 입력합니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com config get nsslapd-ioblocktimeout
Enter password for cn=Directory Manager on ldap://server.example.com:
nsslapd-ioblocktimeout: 10000
```

2. **nsslapd-ioblocktimeout** 속성 값을 수정합니다. 이 예에서는 값을 **8000** 으로 줄입니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com config replace nsslapd-ioblocktimeout=8000
```

3. 구성을 변경하기 위해 Directory Manager로 인증합니다.

```
Enter password for cn=Directory Manager on ldap://server.example.com:
Successfully replaced "nsslapd-ioblocktimeout"
```

4. IdM 디렉터리 서버의 성능을 모니터링합니다. 바람직한 방식으로 변경되지 않으면 이 절차를 반복하고 **nsslapd-ioblocktimeout** 을 다른 값으로 조정하거나 기본값으로 **10000** 으로 돌아갑니다.

검증 단계

- **nsslapd-ioblocktimeout** 속성 값을 표시하고 원하는 값으로 설정되어 있는지 확인합니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com config get nsslapd-ioblocktimeout
Enter password for cn=Directory Manager on ldap://server.example.com:
nsslapd-idletimeout: 8000
```

추가 리소스

- Directory Server 11 문서의 nsslapd-ioblocktimeout (IO Block Time Out)

6.11. 유휴 연결 타임아웃 조정

nsslapd-idletimeout 속성은 IdM 서버에서 유휴 LDAP 클라이언트 연결을 닫는 시간(초)을 설정합니다. 값 **0** 은 서버가 유휴 연결을 종료하지 않음을 의미합니다.

Red Hat은 오래된 연결이 닫히도록 이 값을 조정할 것을 권장하지만 활성 연결은 조기에 닫히지 않습니다.

기본값	**3600** 초 *(1시간)*
유효한 범위	**0 - 2147483647**

DN 항목 위치	cn=config

사전 요구 사항

- LDAP Directory Manager 암호

절차

1. **nsslapd-idletimeout** 매개변수의 현재 값을 검색하고 복원해야 하는 경우 조정하기 전에 기록해 둡니다. 메시지가 표시되면 Directory Manager 암호를 입력합니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com config get nsslapd-idletimeout
Enter password for cn=Directory Manager on ldap://server.example.com:
nsslapd-idletimeout: 3600
```

2. **nsslapd-idletimeout** 속성 값을 수정합니다. 이 예에서는 값을 **1800** (30분)으로 줄입니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com config replace nsslapd-idletimeout=1800
```

3. 구성을 변경하기 위해 Directory Manager로 인증합니다.

```
Enter password for cn=Directory Manager on ldap://server.example.com:
Successfully replaced "nsslapd-idletimeout"
```

4. IdM 디렉터리 서버의 성능을 모니터링합니다. 바람직한 방식으로 변경되지 않는 경우 이 절차를 반복하고 **nsslapd-idletimeout** 을 다른 값으로 조정하거나 기본값 **3600** 으로 돌아갑니다.

검증 단계

- **nsslapd-idletimeout** 속성 값을 표시하고 원하는 값으로 설정되어 있는지 확인합니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com config get nsslapd-idletimeout
Enter password for cn=Directory Manager on ldap://server.example.com:
nsslapd-idletimeout: 3600
```

추가 리소스

- Directory Server 11 문서의 nsslapd-idletimeout (Default Idle Timeout)

6.12. 복제 릴리스 타임아웃 조정

IdM 복제본은 복제 세션 중에 다른 복제본이 있는 동안 전용 잠금됩니다. 일부 환경에서는 복제본이 오랫동안 잠기 때문에 대규모 업데이트 또는 네트워크 정체로 인해 복제 대기 시간이 증가합니다.

repl-release-timeout 매개변수를 조정하여 일정 시간 후에 복제본을 해제할 수 있습니다. Red Hat은 **30** 에서 **120** 사이에 이 값을 설정하는 것이 좋습니다.

- 값이 너무 낮게 설정되면 복제본이 지속적으로 서로 다시 업데이트되고 복제본이 더 큰 업데이트를 보낼 수 없습니다.

- 시간 초과가 길면 서버가 더 긴 시간 동안 복제본에 독점적으로 액세스하지만 값이 **120** 초 이상 지연되는 경우 트래픽이 많은 상황을 개선할 수 있습니다.

기본값	**60** 초
유효한 범위	**0 - 2147483647**
권장 범위	**30 - 120**

사전 요구 사항

- LDAP Directory Manager 암호

절차

1. 데이터베이스 접미사와 해당 백엔드를 표시합니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com
backend suffix list
cn=changelog (changelog)
dc=example,dc=com (userroot)
o=ipaca (ipaca)
```

   이 명령은 백엔드 데이터베이스의 이름을 접미사 옆에 표시합니다. 다음 단계에서 접미사 이름을 사용합니다.

2. 기본 userroot 데이터베이스의 **repl-release-timeout** 속성 값을 수정합니다. 이 예에서는 값을 **90** 초로 늘립니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com
replication set --suffix="dc=example,dc=com" --repl-release-timeout=90
```

3. 구성을 변경하기 위해 Directory Manager로 인증합니다.

```
Enter password for cn=Directory Manager on ldap://server.example.com:
Successfully replaced "repl-release-timeout"
```

4. (선택 사항) IdM 환경에서 IdM CA(인증 기관)를 사용하는 경우 CA 데이터베이스의 **repl-release-timeout** 속성 값을 수정할 수 있습니다. 이 예에서는 값을 **90** 초로 늘립니다.

```
[root@server ~]# dsconf -D "cn=Directory Manager" ldap://server.example.com replication
set --suffix="o=ipaca" --repl-release-timeout=90
Enter password for cn=Directory Manager on ldap://server.example.com:
Successfully replaced "repl-release-timeout"
```

5. Directory Server를 다시 시작합니다.

```
[root@server ~]# systemctl restart dirsrv.target
```

6. IdM 디렉터리 서버의 성능을 모니터링합니다. 바람직한 방식으로 변경되지 않으면 이 절차를 반복하고 **repl-release-timeout** 을 다른 값으로 조정하거나 기본값으로 **60** 초로 돌아갑니다.

검증 단계

- **nsds5ReplicaReleaseTimeout** 특성 값을 표시하고 원하는 값으로 설정되어 있는지 확인합니다.

```
[root@server ~]# ldapsearch -D "cn=directory manager" -w DirectoryManagerPassword
-b "cn=replica,cn=dc\3Dexample\2Cdc\3Dcom,cn=mapping tree,cn=config" | grep
nsds5ReplicaReleaseTimeout
nsds5ReplicaReleaseTimeout: 90
```

참고

이 예제의 접미사가 **dc=example,dc=com** 이지만 등호(**=**) 및 쉼표(**,**)를 **ldapsearch** 명령에서 이스케이프해야 합니다.

다음과 같은 이스케이프 문자를 사용하여 접미사 DN을 **cn=dc\3Dexample\2Cdc\3Dcom**으로 변환합니다.

- **\3D** replace **=**
- **\2C** 교체

추가 리소스

- Directory Server 11 문서의 nsDS5ReplicaReleaseTimeout

6.13. LDIF 파일에서 사용자 지정 데이터베이스 설정을 사용하여 IDM 서버 또는 복제본 설치

Directory Server 데이터베이스의 사용자 지정 설정을 사용하여 IdM 서버 및 IdM 복제본을 설치할 수 있습니다. 다음 절차에서는 데이터베이스 설정을 사용하여 LDIF(LDAP 데이터 상호 변경 형식) 파일을 생성하고 해당 설정을 IdM 서버 및 복제본 설치 명령에 전달하는 방법을 보여줍니다.

사전 요구 사항

- IdM 환경의 성능을 개선하는 사용자 정의 Directory Server 설정을 결정했습니다. IdM 디렉터리 서버 성능 조정을 참조하십시오.

절차

1. 사용자 지정 데이터베이스 설정으로 LDIF 형식으로 텍스트 파일을 만듭니다. 대시(-)를 사용하여 LDAP 특성을 별도로 수정합니다. 이 예에서는 유휴 시간 제한 및 최대 파일 설명자에 기본값이 아닌 값을 설정합니다.

```
dn: cn=config
changetype: modify
replace: nsslapd-idletimeout
nsslapd-idletimeout=1800
-
replace: nsslapd-maxdescriptors
nsslapd-maxdescriptors=8192
```

2. **--dirsrv-config-file** 매개변수를 사용하여 LDIF 파일을 설치 스크립트에 전달합니다.

   a. IdM 서버를 설치하려면 다음을 수행합니다.

```
# ipa-server-install --dirsrv-config-file filename.ldif
```

b. IdM 복제본을 설치하려면 다음을 수행합니다.

```
# ipa-replica-install --dirsrv-config-file filename.ldif
```

추가 리소스

- **ipa-server-install** 및 **ipa-replica-install** 명령 옵션

6.14. 추가 리소스

- 디렉터리 서버 11 성능 튜닝 가이드

7장. KDC의 성능 조정

다음 섹션에서는 사용자, 호스트 및 서비스를 인증하는 KDC(Kerberos Key Distribution Center)의 성능을 조정하는 방법을 설명합니다.

7.1. KDC 청취 대기열의 길이 조정

/var/kerberos/gradleb5kdc.conf 파일의 **[kdcdefaults]** 섹션에서 **kdc_tcp_listen_backlog** 옵션을 설정하여 KDC 데몬의 수신 대기열 길이의 크기를 조정할 수 있습니다. 일부 IdM 배포에서는 높은 수준의 Kerberos 트래픽이 발생하는 일부 IdM 배포에서는 기본값 **5** 가 너무 낮을 수 있지만 이 값을 너무 높은 성능이 저하됩니다.

기본값	**5**
유효한 범위	**1 - 10**

절차

1. 텍스트 편집기에서 **/var/kerberos/gradleb5kdc/kdc.conf** 파일을 엽니다.
2. TCP 수신 백 로그를 원하는 값 (예: **7)** 으로 설정합니다.

```
[kdcdefaults]
 ...
kdc_tcp_listen_backlog = 7
```

3. **/var/kerberos/gradleb5kdc/kdc.conf** 파일을 저장하고 닫습니다.
4. KDC를 다시 시작하여 새 설정을 로드합니다.

7.2. 영역당 KDC 동작 제어 옵션

각 Kerberos 영역의 사용자 계정을 잠금 및 잠금 해제하기 위해 KDC는 인증 성공 및 실패한 후 데이터베이스에 씁니다. **/etc/gradleb5.conf** 파일의 **[dbmodules]** 섹션에서 다음 옵션을 조정하면 KDC가 정보를 쓰는 빈도를 최소화하여 성능을 향상시킬 수 있습니다.

disable_last_success

true 로 설정하면 pre **authentication이 필요한 주요 항목의 마지막 성공적인 인증** 필드에 KDC 업데이트가 비활성화됩니다.

기본값	**false**
유효한 범위	**true** 또는 **false**

disable_lockout

true 로 설정하면 이 옵션은 **마지막 실패한 인증에 대한 KDC 업데이트를 억제하고 실패한 암호에서 preauthentication 이 필요한 보안 주체 항목의 필드를 시도합니다**. 이 플래그를 설정하면 성능이 향상될 수 있지만 계정 잠금을 비활성화하는 것은 보안 위험으로 간주될 수 있습니다.

기본값	**false**

유효한 범위	**true** 또는 **false**

추가 리소스

- 영역당 KDC 설정 조정

7.3. 영역당 KDC 설정 조정

이 절차에서는 Kerberos 영역별로 KDC 동작을 조정합니다.

절차

1. 텍스트 편집기에서 **/etc/gradleb5.conf** 파일을 엽니다.
2. **[dbmodules]** 섹션에서 옵션과 원하는 값을 지정하고 해당 Kerberos 영역에 지정합니다. 이 예제에서는 **EXAMPLE.COM** Kerberos 영역에 대해 **disable_last_success** 변수를 설정하고 있습니다.

```
[dbmodules]
   EXAMPLE.COM = {
      disable_last_success = true
   }
```

3. **/etc/gradleb5.conf** 파일을 저장하고 닫습니다.
4. KDC를 다시 시작하여 새 설정을 로드합니다.

추가 리소스

- 영역당 KDC 동작 제어 옵션

7.4. ECDHE 5KDC 프로세스 수 조정

KDC(Key Distribution Center)가 들어오는 연결을 처리하기 위해 시작하는 프로세스 수를 수동으로 조정하려면 다음 절차를 따르십시오.

기본적으로 IdM 설치 프로그램은 CPU 코어 수를 감지하고 **/etc/sysconfig/gradleb5kdc** 파일에 값을 입력합니다. 예를 들어 파일에는 다음 항목이 포함될 수 있습니다.

```
KRB5KDC_ARGS='-w 2'
[...]
```

이 예에서 **KRB5KDC_ARGS** 매개변수를 **-w 2** 로 설정하면 KDC는 기본 프로세스에서 들어오는 연결을 처리하기 위해 두 개의 별도의 프로세스를 시작합니다. 특히 요구 사항에 따라 가상 CPU 수를 쉽게 추가하거나 제거할 수 있는 가상 환경에서 이 값을 조정할 수 있습니다. 포트ECDHE에서 지속적으로 증가하는 TCP/IP 대기열로 인해 성능 문제 또는 IdM 서버가 응답하지 않도록 하려면 **KRB5KDC_ARGS** 매개변수를 더 높은 값으로 설정하여 더 많은 프로세스 수를 시뮬레이션합니다.

절차

1. 텍스트 편집기에서 **/etc/sysconfig/gradleb5kdc** 파일을 엽니다.

2. **KRB5KDC_ARGS** 매개변수의 값을 지정합니다. 이 예제에서는 프로세스 수를 10으로 설정하고 있습니다.

```
KRB5KDC_ARGS='-w 10'
[...]
```

3. **/etc/sysconfig/gradleb5kdc** 파일을 저장하고 종료합니다.

4. systemd 구성을 다시 로드합니다.

```
# systemctl daemon-reload
```

5. ECDHE **5kdc** 서비스를 다시 시작합니다.

```
# systemctl restart krb5kdc.service
```

참고

IdM 상태 점검 유틸리티를 사용하여 KDC가 최적의 작업자 프로세스 수를 사용하도록 구성되어 있는지 확인할 수 있습니다. IdM 상태 점검을 사용하여 KDC 작업자 프로세스의 최적 수 확인을 참조하십시오.

7.5. 추가 리소스

- MIT Kerberos 문서 - kdc.conf.

8장. 대규모 IDM-AD 신뢰 배포에 대한 SSSD 성능 튜닝

사용자 및 그룹 정보를 검색하는 것은 SSSD(System Security Services Daemon)에 대해 매우 데이터 집약적인 작업이며 특히 대규모 AD(Active Directory) 도메인에 대한 신뢰가 있는 IdM 배포입니다. SSSD가 ID 공급자에서 검색하는 정보와 기간을 조정하여 이 성능을 향상시킬 수 있습니다.

8.1. 대규모 IDM-AD 신뢰 배포를 위해 IDM 서버에서 SSSD 튜닝

이 절차에서는 IdM 서버의 SSSD 서비스 구성에 튜닝 옵션을 적용하여 대규모 AD 환경에서 정보를 검색할 때 응답 시간을 향상시킵니다.

사전 요구 사항

- **/etc/sssd/sssd.conf** 설정 파일을 편집하려면 **root** 권한이 필요합니다.

절차

1. 텍스트 편집기에서 **/etc/sssd/sssd.conf** 설정 파일을 엽니다.
2. Active Directory 도메인의 **[domain]** 섹션에 다음 옵션을 추가합니다. AD 도메인의 도메인 섹션이 아직 없는 경우 새로 생성합니다.

```
[domain/ad.example.com]
ignore_group_members = true
subdomain_inherit = ignore_group_members
...
```

3. 서버에 **/etc/sssd/sssd.conf** 파일을 저장하고 닫습니다.
4. SSSD 서비스를 다시 시작하여 구성 변경 사항을 로드합니다.

```
[root@client ~]# systemctl restart sssd
```

추가 리소스

- 대규모 IdM-AD 신뢰 배포를 위해 IdM 서버 및 클라이언트에서 SSSD 튜닝 옵션

8.2. IDM 서버의 IPA-EXTDOM 플러그인의 구성 시간 조정

IdM 클라이언트는 AD(Active Directory)에서 사용자와 그룹에 대한 정보를 직접 수신할 수 없으므로 IdM 서버는 **ipa-extdom** 플러그인을 사용하여 AD 사용자 및 그룹에 대한 정보를 수신하며 해당 정보가 요청 클라이언트로 전달됩니다.

ipa-extdom 플러그인은 AD 사용자에 대한 데이터에 대한 SSSD에 요청을 보냅니다. SSSD 캐시에 정보가 없는 경우 SSSD는 AD 도메인 컨트롤러(DC)에서 데이터를 요청합니다. 플러그인이 연결을 취소하고 호출자에게 시간 초과 오류를 반환하는 **ipa-extdom** 플러그인이 SSSD에서 응답을 대기하는 기간을 정의하는 구성 시간 값을 조정할 수 있습니다. 기본값은 10000밀리초(10초)입니다.

다음 예제에서는 구성 시간 제한을 20초(20000밀리초)로 조정합니다.

주의

구성 시간 제한을 조정할 때 주의하십시오.

- 500밀리초와 같이 값이 너무 작으면 SSSD에 응답할 시간이 충분하지 않을 수 있으며 요청은 항상 시간 초과를 반환합니다.
- 30000밀리초(30초)와 같이 너무 큰 값을 설정하면 단일 요청이 이 시간 동안 SSSD에 대한 연결을 차단할 수 있습니다. 한 번에 하나의 스레드만 SSSD에 연결할 수 있으므로 플러그인의 다른 모든 요청을 기다려야 합니다.
- IdM 클라이언트에서 보낸 요청이 여러 개 있는 경우 IdM 서버의 Directory Server에 대해 구성된 사용 가능한 모든 작업자를 차단할 수 있습니다. 그 결과 서버는 잠시 동안 어떤 종류의 요청에도 응답하지 못할 수 있습니다.

다음과 같은 경우 구성 시간 초과만 변경합니다.

- AD 사용자 및 그룹에 대한 정보를 요청할 때 자체 검색 타임아웃에 도달하기 전에 IdM 클라이언트가 시간 초과 오류를 자주 수신하는 경우 구성 시간 초과 값이 **너무 작아** 집니다.
- IdM 서버의 Directory Server가 잠긴 경우가 많으며 **pstack** 유틸리티에서 현재 많은 또는 모든 작업자가 **ipa-extdom** 요청을 처리하는 것으로 보고하는 경우 값은 **너무 큽니다**.

사전 요구 사항

- LDAP Directory Manager 암호

절차

- 다음 명령을 사용하여 구성 시간 제한을ECDHE밀리초로 조정합니다.

```
# ldapmodify -D "cn=directory manager" -W
dn: cn=ipa_extdom_extop,cn=plugins,cn=config
changetype: modify
replace: ipaExtdomMaxNssTimeout
ipaExtdomMaxNssTimeout: 20000
```

8.3. IDM 서버의 IPA-EXTDOM 플러그인의 최대 버퍼 크기 조정

IdM 클라이언트는 AD(Active Directory)에서 사용자와 그룹에 대한 정보를 직접 수신할 수 없으므로 IdM 서버는 **ipa-extdom** 플러그인을 사용하여 AD 사용자 및 그룹에 대한 정보를 수신하며 해당 정보가 요청 클라이언트로 전달됩니다.

SSSD가 수신하는 데이터를 저장할 수 있는 버퍼 크기를 조정하는 **ipa-extdom** 플러그인의 최대 버퍼 크기를 조정할 수 있습니다. 버퍼가 너무 작으면 SSSD에서 **ERANGE** 오류를 반환하고 플러그인이 더 큰 버퍼로 요청을 다시 시도합니다. 기본 버퍼 크기는 134217728 바이트(128MB)입니다.

다음 예제에서는 최대 버퍼 크기를 256MB(268435456바이트)로 조정합니다.

사전 요구 사항

- LDAP Directory Manager 암호

절차

- 다음 명령을 사용하여 최대 버퍼 크기를 268435456바이트로 설정합니다.

```
# ldapmodify -D "cn=directory manager" -W
dn: cn=ipa_extdom_extop,cn=plugins,cn=config
changetype: modify
replace: ipaExtdomMaxNssBufSize
ipaExtdomMaxNssBufSize: 268435456
```

8.4. IDM 서버에서 IPA-EXTDOM 플러그인의 최대 인스턴스 수 조정

IdM 클라이언트는 AD(Active Directory)에서 사용자와 그룹에 대한 정보를 직접 수신할 수 없으므로 IdM 서버는 **ipa-extdom** 플러그인을 사용하여 AD 사용자 및 그룹에 대한 정보를 수신한 다음 이 정보를 요청하는 클라이언트로 전달합니다.

기본적으로 **ipa-extdom** 플러그인은 LDAP 작업자 스레드의 최대 80%를 사용하여 IdM 클라이언트의 요청을 처리하도록 구성됩니다. IdM 클라이언트의 SSSD 서비스에서 AD 신뢰 사용자 및 그룹에 대한 많은 정보를 요청한 경우 이 작업으로 대부분의 LDAP 스레드를 사용하는 경우 LDAP 서비스가 중지될 수 있습니다. 이러한 문제가 발생하면 AD 도메인 **/var/log/sssd/sssd__your-ad-domain-name.com_.log** 에 대한 SSSD 로그 파일에 유사한 오류가 표시될 수 있습니다.

```
(2022-05-22  5:00:13): [be[ad.example.com]] [ipa_s2n_get_user_done] (0x0040): s2n exop request failed.
(2022-05-22  5:00:13): [be[ad.example.com]] [ipa_s2n_get_user_done] (0x0040): s2n exop request failed.
(2022-05-22  5:00:13): [be[ad.example.com]] [ipa_s2n_exop_done] (0x0040): ldap_extended_operation result: Server is busy(51), Too many extdom instances running.
```

ipaExtdomMaxInstances 옵션의 값을 설정하여 최대 **ipa-extdom** 인스턴스 수를 조정할 수 있습니다. 이 값은 0보다 크고 총 작업자 스레드 수보다 작아야 합니다.

사전 요구 사항

- LDAP Directory Manager 암호

절차

1. 총 작업자 스레드 수를 검색합니다.

```
# ldapsearch -xLLLD cn=directory\ manager -W -b cn=config -s base nsslapd-threadnumber
Enter LDAP Password:
dn: cn=config
nsslapd-threadnumber: 16
```

   즉, **ipaExtdomMaxInstances** 의 현재 값은 13입니다.

2. 최대 인스턴스 수를 조정합니다. 이 예에서는 값을 14로 변경합니다.

```
# ldapmodify -D "cn=directory manager" -W
```

```
dn: cn=ipa_extdom_extop,cn=plugins,cn=config
changetype: modify
replace: ipaExtdomMaxInstances
ipaExtdomMaxInstances: 14
```

3. IdM 디렉터리 서버의 성능을 모니터링하고 개선하지 않는 경우 이 절차를 반복하고 **ipaExtdomMaxInstances** 변수 값을 조정합니다.

8.5. 대규모 IDM-AD 신뢰 배포를 위해 IDM 클라이언트에서 SSSD 튜닝

이 절차에서는 IdM 클라이언트의 SSSD 서비스 구성에 튜닝 옵션을 적용하여 대규모 AD 환경에서 정보를 검색할 때 응답 시간을 개선합니다.

사전 요구 사항

- **/etc/sssd/sssd.conf** 설정 파일을 편집하려면 **root** 권한이 필요합니다.

절차

1. 캐시되지 않은 단일 로그인이 걸리는 시간(초)을 확인합니다.

   a. IdM 클라이언트 **client.example.com** 에서 SSSD 캐시를 지웁니다.

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

   b. **time** 명령을 사용하여 AD 사용자로 로그인하는 데 걸리는 시간을 측정합니다. 이 예에서는 IdM 클라이언트 **client.example.com** 에서 **ad.example.com** 도메인의 사용자 **ad-user** 와 동일한 호스트에 로그인합니다.

   ```
   [root@client ~]# time ssh ad-user@ad.example.com@client.example.com
   ```

   c. 가능한 한 빨리 암호를 입력합니다.

   ```
   Password:
   Last login: Sat Jan 23 06:29:54 2021 from 10.0.2.15
   [ad-user@ad.example.com@client ~]$
   ```

   d. 가능한 한 빨리 로그아웃하여 경과 시간을 표시합니다. 이 예에서는 캐시되지 않은 단일 로그인이 약 **9** 초가 걸립니다.

   ```
   [ad-user@ad.example.com@client /]$ exit
   logout
   Connection to client.example.com closed.

   real 0m8.755s
   user    0m0.017s
   sys     0m0.013s
   ```

2. 텍스트 편집기에서 **/etc/sssd/sssd.conf** 설정 파일을 엽니다.

3. Active Directory 도메인의 **[domain]** 섹션에 다음 옵션을 추가합니다. ECDHE **_id_timeout** 및 ECDHE **5_auth_timeout** 옵션을 캐시되지 않은 로그인이 걸리는 시간(초)으로 설정합니다. AD 도메인의 도메인 섹션이 아직 없는 경우 새로 생성합니다.

```
[domain/example.com/ad.example.com]
krb5_auth_timeout = 9
ldap_deref_threshold = 0
...
```

4. **[pam]** 섹션에 다음 옵션을 추가합니다.

```
[pam]
pam_id_timeout = 9
```

5. 서버에 **/etc/sssd/sssd.conf** 파일을 저장하고 닫습니다.

6. SSSD 서비스를 다시 시작하여 구성 변경 사항을 로드합니다.

```
[root@client ~]# systemctl restart sssd
```

추가 리소스

- 대규모 IdM-AD 신뢰 배포를 위해 IdM 서버 및 클라이언트에서 SSSD 튜닝 옵션

8.6. TMPFS에서 SSSD 캐시 마운트

SSSD(System Security Services Daemon)는 LDAP 오브젝트를 캐시에 지속적으로 씁니다. 이러한 내부 SSSD 트랜잭션은 디스크에 데이터를 쓰므로 RAM(Random-Access Memory)에서 읽고 쓰는 것보다 훨씬 느립니다.

이 성능을 개선하려면 RAM에 SSSD 캐시를 마운트합니다.

고려 사항

- SSSD 캐시가 RAM에 있는 경우 재부팅 후 캐시된 정보가 유지되지 않습니다.
- IdM 서버의 SSSD 인스턴스가 동일한 호스트의 Directory Server와의 연결이 끊어질 수 없으므로 IdM 서버에서 이러한 변경을 수행하는 것이 안전합니다.
- IdM 클라이언트에서 이 조정을 수행하고 IdM 서버에 대한 연결이 끊어지면 연결을 다시 설정할 때까지 사용자가 재부팅 후 인증할 수 없습니다.

사전 요구 사항

- **/etc/fstab** 구성 파일을 편집하려면 **root** 권한이 필요합니다.

절차

1. **tmpfs** 임시 파일 시스템을 생성합니다.

   a. RHEL 8.6 이상에서 SSSD 사용자가 **config.ldb** 파일에 소유하고 있는지 확인합니다.

```
# ls -al /var/lib/sss/db/config.ldb
-rw-------. 1 sssd sssd 1286144 Jun  8 16:41 /var/lib/sss/db/config.ldb
```

   이 경우 **/etc/fstab** 파일에 다음 항목을 한 줄로 추가합니다.

```
tmpfs /var/lib/sss/db/ tmpfs
size=300M,mode=0700,uid=sssd,gid=sssd,rootcontext=system_u:object_r:sssd_var_lib_
t:s0 0 0
```

b. RHEL 8 버전에서는 8.6 미만에서 **config.ldb** 파일은 **root** 사용자가 소유합니다.

```
# ls -al /var/lib/sss/db/config.ldb
-rw-------. 1 root root 1286144 Jun  8 14:15 /var/lib/sss/db/config.ldb
```

이 경우 **/etc/fstab** 파일에 다음 항목을 한 줄로 추가합니다.

```
tmpfs /var/lib/sss/db/ tmpfs
size=300M,mode=0700,rootcontext=system_u:object_r:sssd_var_lib_t:s0 0 0
```

이 예제에서는 300MB 캐시를 생성합니다. IdM 및 AD 디렉터리 크기에 따라 **size** 매개변수를 튜닝하고 10,000 LDAP 항목당 100MB를 추정합니다.

2. 새 SSSD 캐시 디렉터리를 마운트합니다.

```
[root@host ~]# mount /var/lib/sss/db/
```

3. 이 구성 변경 사항을 반영하려면 SSSD를 다시 시작합니다.

```
[root@host ~]# systemctl restart sssd
```

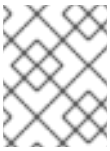
8.7. 대규모 IDM-AD 신뢰 배포를 위해 IDM 서버 및 클라이언트 튜닝을 위한 SSSD.CONF 의 옵션

/etc/sssd/sssd.conf 구성 파일에서 다음 옵션을 사용하여 IdM 서버 및 클라이언트의 SSSD 성능을 튜닝할 수 있습니다.

8.7.1. IdM 서버의 옵션 튜닝

ignore_group_members

그룹에 속한 모든 사용자와 달리 사용자가 속한 그룹을 아는 것은 사용자를 인증하고 승인할 때 중요합니다. **ignore_group_members** 가 **true** 로 설정된 경우 SSSD는 그룹 오브젝트에 대한 정보 자체만 검색하지 않고 해당 멤버가 아닌, 상당한 성능 향상을 제공합니다.



참고

id user@ad-domain.com 명령은 여전히 올바른 그룹 목록을 반환하지만 **getent 그룹 ad-group@ad-domain.com** 는 빈 목록을 반환합니다.

기본값	**false**
권장 값	**true**

참고

배포에 compat 트리가 있는 IdM 서버가 포함된 경우 이 옵션을 **true** 로 설정하지 않아야 합니다.

subdomain_inherit

subdomain_inherit 옵션을 사용하면 신뢰할 수 있는 AD 도메인 구성에 **ignore_group_members** 설정을 적용할 수 있습니다. **subdomain_inherit** 옵션에 나열된 설정은 main(IdM) 도메인과 AD 하위 도메인에 모두 적용됩니다.

기본값	**none**
권장 값	**subdomain_inherit = ignore_group_members**

8.7.2. IdM 클라이언트의 튜닝 옵션

pam_id_timeout

이 매개 변수는 ID 조회 중에 ID 공급자에 대한 과도한 왕복을 방지하기 위해 PAM 세션의 결과가 캐시되는 기간을 제어합니다. **5** 초의 기본값은 복잡한 그룹 멤버십이 IdM 서버 및 IdM 클라이언트 측에서 채워지는 환경에서 충분하지 않을 수 있습니다. CloudEvent_ **id_timeout** 을 캐시되지 않은 로그인에 걸리는 시간(초)으로 설정하는 것이 좋습니다.

기본값	**5**
권장 값	**캐시되지 않은 단일 로그인이 걸리는 시간(초)**

krb5_auth_timeout

increasing **ECDHE5_auth_timeout** 을 사용하면 사용자가 많은 그룹의 멤버인 환경에서 복잡한 그룹 정보를 처리할 수 있습니다. 이 값을 캐시되지 않은 로그인에 걸리는 시간(초)으로 설정하는 것이 좋습니다.

기본값	**6**
권장 값	**캐시되지 않은 단일 로그인이 걸리는 시간(초)**

ldap_deref_threshold

역참조 조회는 단일 LDAP 호출에서 모든 그룹 멤버를 가져오는 수단입니다. **ldap_deref_threshold** 값은 역참조 조회를 트리거하기 위해 내부 캐시에서 누락해야 하는 그룹 멤버 수를 지정합니다. 멤버가 더 적은 경우 개별적으로 조회됩니다. 역참조 조회는 대규모 환경에서 오랜 시간이 걸릴 수 있으며 성능이 저하될 수 있습니다. 역참조 조회를 비활성화하려면 이 옵션을 **0** 으로 설정합니다.

기본값	**10**
권장 값	**0**

8.8. 추가 리소스

- 대규모 IdM-AD 신뢰 배포를 위한 SSSD 성능 튜닝