Red Hat Enterprise Linux 8

IdM 상태 점검을 사용하여 IdM 환경 모니터링

상태 및 상태 점검 수행

Last Updated: 2023-09-22

Red Hat Enterprise Linux 8 IdM 상태 점검을 사용하여 IdM 환경 모니터링

상태 및 상태 점검 수행

법적 공지

초록

ipa-healthcheck 유틸리티는 관리자가 Red Hat IdM(Identity Management) 환경에서 문제를 감지하는 데 도움이 됩니다. 여기에는 IdM 서비스 상태 검사, 구성 파일 권한, 복제 상태 및 인증서 관련 문제가 포함됩니다.

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 계획된 용어 교체는 다음과 같습니다.

- ***차단 목록*** 대체 *블랙리스트*
- ***목록*** 교체 *허용 화이트리스트*
- ***2차*** 대체 *슬레이브*
- *master* 라는 단어는 컨텍스트에 따라 더 정확한 언어로 교체됩니다.
  - ***IdM 서버가*** *IdM 마스터*교체
  - ***CA 갱신 서버가*** *CA 갱신 마스터*교체
  - ***CRL 게시자 서버가*** *CRL 마스터*교체
  - ***멀티 공급자*** 대체 *멀티 마스터*

RED HAT 문서에 관한 피드백 제공

문서에 대한 피드백에 감사드립니다. 어떻게 개선할 수 있는지 알려주십시오.

특정 문구에 대한 의견 제출

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

Bugzilla를 통해 피드백 제출(등록 필요)

1. Bugzilla 웹 사이트에 로그인합니다.
2. **버전** 메뉴에서 올바른 버전을 선택합니다.
3. **Summary** (요약) 필드에 설명 제목을 입력합니다.
4. **Description** (설명) 필드에 개선을 위한 제안을 입력합니다. 문서의 관련 부분에 대한 링크를 포함합니다.
5. **Submit Bug**를 클릭하십시오.

1장. IDM 상태 점검 도구 설치 및 실행

IdM Healthcheck 툴과 설치 및 실행 방법에 대해 자세히 알아보십시오.

참고

- Healthcheck 도구는 RHEL 8.1 이상에서만 사용할 수 있습니다.

1.1. IDM의 상태 점검

IdM(Identity Management)의 상태 점검 도구는 IdM 환경의 상태에 영향을 줄 수 있는 문제를 찾는 데 도움이 됩니다.

참고

Healthcheck 도구는 Kerberos 인증 없이 사용할 수 있는 명령줄 도구입니다.

모듈은 서로 독립적입니다.

Healthcheck는 다음을 테스트하는 독립 모듈로 구성됩니다.

- 복제 문제
- 인증서 유효
- 인증 기관 인프라 문제
- IdM 및 Active Directory 신뢰 문제
- 올바른 파일 권한 및 소유권 설정

두 가지 출력 형식

Healthcheck는 output **-type 옵션을 사용하여 설정할 수 있는 다음 출력을** 생성합니다.

- **json**: JSON 형식의 머신에서 읽을 수 있는 출력 (기본값)
- **사람**: 사람이 읽을 수 있는 출력

output-file 옵션을 사용하여 다른 파일 대상을 지정할 수 있습니다.

결과

각 Healthcheck 모듈은 다음 결과 중 하나를 반환합니다.

성공
: 예상대로 구성됨

경고
: 오류는 아니지만 계속 감시하거나 평가할 수 있습니다.

ERROR
: 예상대로 구성되지 않음

심각
: 제대로 구성되지 않았습니다. 영향을 미칠 가능성이 높습니다.

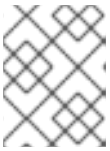
1.2. IDM 상태 점검 설치

IdM Healthcheck 툴을 설치하려면 다음 절차를 따르십시오.

절차

- **ipa-healthcheck** 패키지를 설치합니다.

```
[root@server ~]# yum install ipa-healthcheck
```



참고

RHEL 8.1 및 8.2 시스템에서 **yum install /usr/bin/ipa-healthcheck** 명령을 대신 사용합니다.

검증 단계

- **--failures-only** 옵션을 사용하여 **ipa-healthcheck** 가 오류만 보고하도록 합니다. IdM 설치는 **[]** 의 빈 결과를 반환합니다.

```
[root@server ~]# ipa-healthcheck --failures-only
[]
```

추가 리소스

- **ipa-healthcheck --help** 를 사용하여 지원되는 모든 인수를 확인합니다.

1.3. IDM 상태 점검 실행

상태 점검은 로그 회전을 사용하여 수동 또는 자동으로 실행할 수 있습니다.

사전 요구 사항

- Healthcheck 도구를 설치해야 합니다. IdM 상태 점검 설치를 참조하십시오.

절차

- 상태 점검을 수동으로 실행하려면 **ipa-healthcheck** 명령을 입력합니다.

```
[root@server ~]# ipa-healthcheck
```

추가 리소스

모든 옵션에 대해서는 **man ipa-healthcheck** 를 참조하십시오.

1.4. 로그 회전

로그 회전은 매일 새 로그 파일을 생성하고 파일은 날짜별로 구성됩니다. 로그 파일은 동일한 디렉터리에 저장되므로 날짜에 따라 특정 로그 파일을 선택할 수 있습니다.

순환은 최대 로그 파일 수가 구성되었음을 의미하며, 숫자가 초과된 경우 최신 파일이 다시 작성되고 가장 오래된 파일 이름을 바꿉니다. 예를 들어 순환 번호가 30인 경우 30초 로그 파일은 첫 번째(오래된) 로그 파일을 대체합니다.

로그 회전은 엄청난 로그 파일을 줄이고 이를 구성하므로 로그 분석에 도움이 될 수 있습니다.

1.5. IDM 상태 점검을 사용하여 로그 회전 구성

다음을 사용하여 로그 교체를 구성하려면 다음 절차를 따르십시오.

- **systemd** 타이머
- **crond** 서비스

systemd 타이머는 Healthcheck 도구를 정기적으로 실행하고 로그를 생성합니다. 기본값은 매일 4 a.m으로 설정됩니다.

crond 서비스는 로그 회전에 사용됩니다.

기본 로그 이름은 **healthcheck.log** 이고 순환된 로그는 **healthcheck.log-YYYMMDD** 형식을 사용합니다.

사전 요구 사항

- root로 명령을 실행해야 합니다.

절차

1. **systemd** 타이머를 활성화합니다.

```
# systemctl enable ipa-healthcheck.timer
Created symlink /etc/systemd/system/multi-user.target.wants/ipa-healthcheck.timer ->
/usr/lib/systemd/system/ipa-healthcheck.timer.
```

2. **systemd** 타이머를 시작합니다.

```
# systemctl start ipa-healthcheck.timer
```

3. **/etc/logrotate.d/ipahealthcheck** 파일을 열어 저장해야 하는 로그 수를 구성합니다.
   기본적으로 로그 회전은 30일 동안 설정됩니다.

4. **/etc/logrotate.d/ipahealthcheck** 파일에서 로그 경로를 구성합니다.
   기본적으로 로그는 **/var/log/ipa/healthcheck/** 디렉터리에 저장됩니다.

5. **/etc/logrotate.d/ipahealthcheck** 파일에서 로그 생성 시간을 구성합니다.
   기본적으로 로그는 오전 4시마다 생성됩니다.

6. 로그 회전을 사용하려면 **crond** 서비스가 활성화되어 실행 중인지 확인합니다.

```
# systemctl enable crond
# systemctl start crond
```

로그를 생성하려면 IPA 상태 점검 서비스를 시작합니다.

```
# systemctl start ipa-healthcheck
```

결과를 확인하려면 **/var/log/ipa/healthcheck/** 로 이동하여 로그가 올바르게 생성되었는지 확인합니다.

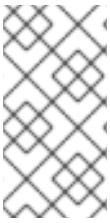
1.6. IDM 상태 점검 구성 변경

원하는 명령줄 옵션을 **/etc/ipahealthcheck/ipahealthcheck.conf** 파일에 추가하여 상태 점검 설정을 변경할 수 있습니다. 예를 들어 로그 교체를 구성하고 로그가 자동 분석에 적합한 형식으로 되어 있는지 확인하려고 하지만 새 타이머를 설정하지 않으려는 경우에 유용할 수 있습니다.

참고

이 상태 점검 기능은 RHEL 8.7 이상에서만 사용할 수 있습니다.

수정 후 Healthcheck가 생성하는 모든 로그는 새 설정을 따릅니다. 이러한 설정은 수동 상태 점검 실행에도 적용됩니다.



참고

Healthcheck를 수동으로 실행하는 경우 구성 파일의 설정이 명령줄에 지정된 옵션보다 우선합니다. 예를 들어 구성 파일에서 **output_type** 이 **human** 로 설정된 경우 명령줄에 **json** 을 지정하면 적용되지 않습니다. 구성 파일에 지정되지 않은 사용하는 명령줄 옵션이 정상적으로 적용됩니다.

추가 리소스

- IdM 상태 점검을 사용하여 로그 순환 구성

1.7. 출력 로그 형식을 변경하도록 HEALTHCHECK 구성

타이머가 이미 설정된 상태로 Healthcheck을 구성하려면 다음 절차를 따르십시오. 이 예제에서는 사용자가 읽을 수 있는 형식으로 로그를 생성하도록 상태 점검을 구성하고 오류만 아니라 성공적인 결과를 포함하도록 합니다.

사전 요구 사항

- 시스템에서 RHEL 8.7 이상을 실행하고 있습니다.
- **루트** 권한이 있어야 합니다.
- 이전에 타이머에서 로그 교체를 구성했습니다.

절차

1. 텍스트 편집기에서 **/etc/ipahealthcheck/ipahealthcheck.conf** 파일을 엽니다.
2. options **output_type=human** 및 **all=True** 를 **[default]** 섹션에 추가합니다.
3. 파일을 저장하고 닫습니다.

검증

1. Healthcheck를 수동으로 실행합니다.

```
# ipa-healthcheck
```

2. **/var/log/ipa/healthcheck/** 로 이동하여 로그가 올바른 형식으로 되어 있는지 확인합니다.

추가 리소스

- IdM 상태 점검을 사용하여 로그 순환 구성

1.8. 추가 리소스

- IdM 상태 점검 사용 예는 ID 관리 구성 및 관리 가이드의 다음 섹션을 참조하십시오.
  - 서비스 확인 중
  - IdM 및 AD 신뢰 구성 확인
  - 인증서 확인 중
  - 시스템 인증서 확인
  - 디스크 공간 확인 중
  - IdM 구성 파일의 권한 확인
  - 복제 확인 중
- 또한 단일 가이드로 구성된 해당 장을 확인할 수 있습니다. IdM 상태 점검을 사용하여 IdM 환경 모니터링

2장. IDM 상태 점검을 사용하여 서비스 확인

Healthcheck 툴을 사용하여 IdM(Identity Management) 서버에서 사용하는 서비스를 모니터링할 수 있습니다.

자세한 내용은 IdM의 상태 점검을 참조하십시오.

사전 요구 사항

- Healthcheck 도구는 RHEL 8.1 이상에서만 사용할 수 있습니다.

2.1. 서비스 상태 점검 테스트

상태 점검 도구에는 IdM 서비스가 실행 중이 아닌지 확인하는 테스트가 포함되어 있습니다. 이 테스트는 실행 중이지 않은 서비스가 다른 테스트에서 실패할 수 있기 때문에 중요합니다. 따라서 모든 서비스가 먼저 실행되고 있는지 확인합니다. 그런 다음 다른 모든 테스트 결과를 확인할 수 있습니다.

모든 서비스 테스트를 보려면 **--list -sources 옵션을 사용하여 ipa- healthcheck** 를 실행합니다.

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

ipahealthcheck.meta.services 소스에서 Healthcheck로 테스트된 모든 서비스를 찾을 수 있습니다.

- certmonger
- dirsrv
- gssproxy
- httpd
- ipa_custodia
- ipa_dnskeysyncd
- ipa_otpd
- kadmin
- krb5kdc
- 명명됨
- pki_tomcatd
- sssd

참고

문제를 발견하려고 할 때 모든 IdM 서버에서 이러한 테스트를 실행합니다.

2.2. 상태 점검을 사용하는 폴링 서비스

Healthcheck 툴을 사용하여 IdM(Identity Management) 서버에서 실행되는 서비스의 독립 실행형 수동 테스트를 실행하려면 다음 절차를 따르십시오.

Healthcheck 도구에는 다음을 사용하여 결과를 단축할 수 있는 많은 테스트가 포함되어 있습니다.

- 성공적인 모든 테스트 제외: **--failures-only**
- 서비스 테스트만 포함: **--source=ipahealthcheck.meta.services**

절차

- 경고, 오류 및 서비스와 관련된 중요한 문제를 사용하여 상태 점검을 실행하려면 다음을 입력합니다.

```
# ipa-healthcheck --source=ipahealthcheck.meta.services --failures-only
```

성공적인 테스트에 빈 괄호가 표시됩니다.

```
[ ]
```

서비스 중 하나가 실패하면 결과가 다음 예와 유사하게 표시됩니다.

```
{
  "source": "ipahealthcheck.meta.services",
  "check": "httpd",
  "result": "ERROR",
  "kw": {
    "status": false,
    "msg": "httpd: not running"
  }
}
```

추가 리소스

- **man ipa-healthcheck** 를 참조하십시오.

3장. IDM 상태 점검을 사용하여 디스크 공간 확인

Healthcheck 도구를 사용하여 Identity Management 서버의 사용 가능한 디스크 공간을 모니터링할 수 있습니다.

자세한 내용은 IdM의 상태 점검을 참조하십시오.

사전 요구 사항

- Healthcheck 도구는 RHEL 8.1 이상에서만 사용할 수 있습니다.

3.1. 디스크 공간 상태 점검 테스트

Healthcheck 도구에는 사용 가능한 디스크 공간을 확인하는 테스트가 포함되어 있습니다. 사용 가능한 디스크 공간이 충분하지 않으면 다음과 같은 문제가 발생할 수 있습니다.

- 로깅
- 실행
- 백업

테스트에서는 다음 경로를 확인합니다.

표 3.1. 테스트된 경로

테스트에서 확인한 경로	최소 디스크 공간(MB)
/var/lib/dirsrv/	1024
/var/lib/ipa/backup/	512
/var/log/	1024
var/log/audit/	512
/var/tmp/	512
/tmp/	512

모든 테스트를 나열하려면 **--list -sources 옵션을 사용하여 ipa- healthcheck** 를 실행합니다.

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

ipahealthcheck.system.filesystemspace 소스에서 파일 시스템 공간 점검 테스트를 찾을 수 있습니다.

FileSystemSpaceCheck

이 테스트에서는 다음과 같은 방법으로 사용 가능한 디스크 공간을 확인합니다.

- 필요한 최소 원시 가용 바이트.
- 백분율 - cinder 최소 사용 가능한 디스크 공간이 20%로 하드 코딩됩니다.

3.2. 상태 점검 도구를 사용하여 디스크 공간

Healthcheck 툴을 사용하여 IdM(Identity Management) 서버에서 사용 가능한 디스크 공간의 독립 실행형 수동 테스트를 실행하려면 다음 절차를 따르십시오.

Healthcheck에는 많은 테스트가 포함되어 있으므로 다음을 통해 결과를 좁힐 수 있습니다.

- 성공적인 모든 테스트 제외: **--failures-only**
- 공간 점검 테스트만 포함: **--source=ipahealthcheck.system.filesystemspace**

절차

- 경고, 오류 및 사용 가능한 디스크 공간과 관련된 중요한 문제를 사용하여 상태 점검을 실행하려면 다음을 입력합니다.

```
# ipa-healthcheck --source=ipahealthcheck.system.filesystemspace --failures-only
```

성공적인 테스트에 빈 괄호가 표시됩니다.

```
[]
```

예를 들어 실패한 테스트는 다음을 표시할 수 있습니다.

```
{
  "source": "ipahealthcheck.system.filesystemspace",
  "check": "FileSystemSpaceCheck",
  "result": "ERROR",
  "kw": {
    "msg": "/var/lib/dirsrv: free space under threshold: 0 MiB < 1024 MiB",
    "store": "/var/lib/dirsrv",
    "free_space": 0,
    "threshold": 1024
  }
}
```

실패한 테스트에서는 **/var/lib/dirsrv** 디렉터리에 공간이 부족했음을 알려줍니다.

추가 리소스

- **man ipa-healthcheck** 를 참조하십시오.

4장. HEALTHCHECK를 사용하여 IDM 구성 파일에 대한 권한 확인

Healthcheck 툴을 사용하여 IdM(Identity Management) 구성 파일을 테스트하는 방법에 대해 자세히 알아보십시오.

자세한 내용은 IdM의 상태 점검을 참조하십시오.

사전 요구 사항

- Healthcheck 도구는 RHEL 8.1 이상의 시스템에서만 사용할 수 있습니다.

4.1. 파일 권한 상태 점검 테스트

Healthcheck 툴은 IdM(Identity Management)에서 설치하거나 구성한 몇 가지 중요한 파일의 소유권 및 권한을 테스트합니다.

테스트된 파일의 소유권 또는 권한을 변경하면 테스트에서 **결과** 섹션에 경고를 반환합니다. 구성이 작동하지 않을 필요는 없지만 파일이 기본 구성과 다릅니다.

모든 테스트를 보려면 **--list -sources 옵션을 사용하여 ipa- healthcheck** 를 실행합니다.

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

ipahealthcheck.ipa.files 소스에서 파일 권한 테스트를 찾을 수 있습니다.

IPAFileNSSDBCheck

이 테스트는 389-ds NSS 데이터베이스와 CA(인증 기관) 데이터베이스를 확인합니다. 389-ds 데이터베이스는 **/etc/dirsrv/slapd-<dashed-REALM>** 에 있으며 CA 데이터베이스는 **/etc/pki/pki-tomcat/alias/** 에 있습니다.

IPAFileCheck

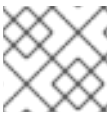
이 테스트에서는 다음 파일을 확인합니다.

- **/var/lib/ipa/ra-agent.{key|pem}**
- **/var/lib/ipa/certs/httpd.pem**
- **/var/lib/ipa/private/httpd.key**
- **/etc/httpd/alias/ipasession.key**
- **/etc/dirsrv/ds.keytab**
- **/etc/ipa/ca.crt**
- **/etc/ipa/custodia/server.keys**
  PKINIT가 활성화된 경우:
- **/var/lib/ipa/certs/kdc.pem**
- **/var/lib/ipa/private/kdc.key**
  DNS가 구성된 경우 다음을 수행합니다.
- **/etc/named.keytab**
- **/etc/ipa/dnssec/ipa-dnskeysyncd.keytab**

TomcatFileCheck

이 테스트에서는 CA가 구성된 경우 일부 tomcat 관련 파일을 확인합니다.

- **/etc/pki/pki-tomcat/password.conf**
- **/var/lib/pki/pki-tomcat/conf/ca/CS.cfg**
- **/etc/pki/pki-tomcat/server.xml**



참고

문제를 찾으려고 할 때 모든 IdM 서버에서 이러한 테스트를 실행합니다.

4.2. HEALTHCHECK를 사용하는 구성 파일

Healthcheck 툴을 사용하여 IdM(Identity Management) 서버의 구성 파일의 독립 실행형 수동 테스트를 실행하려면 다음 절차를 따르십시오.

Healthcheck 도구에는 많은 테스트가 포함되어 있습니다. 결과는 다음과 같이 좁힐 수 있습니다.

- 성공적인 모든 테스트 제외: **--failures-only**
- 소유권 및 권한 테스트만 포함: **--source=ipahealthcheck.ipa.files**

절차

1. 경고, 오류 및 심각한 문제만 표시하는 동시에 IdM 구성 파일 소유권 및 권한에 대해 상태 점검 테스트를 실행하려면 다음을 입력합니다.

```
# ipa-healthcheck --source=ipahealthcheck.ipa.files --failures-only
```

성공적인 테스트에 빈 괄호가 표시됩니다.

```
# ipa-healthcheck --source=ipahealthcheck.ipa.files --failures-only
[]
```

실패한 테스트에 다음 **경고** 와 유사한 결과가 표시됩니다.

```
{
  "source": "ipahealthcheck.ipa.files",
  "check": "IPAFileNSSDBCheck",
  "result": "WARNING",
  "kw": {
    "key": "_etc_dirsrv_slapd-EXAMPLE-TEST_pkcs11.txt_mode",
    "path": "/etc/dirsrv/slapd-EXAMPLE-TEST/pkcs11.txt",
    "type": "mode",
    "expected": "0640",
    "got": "0666",
    "msg": "Permissions of /etc/dirsrv/slapd-EXAMPLE-TEST/pkcs11.txt are 0666 and should be 0640"
  }
}
```

추가 리소스

- **man ipa-healthcheck** 를 참조하십시오.

5장. IDM 상태 점검을 사용하여 DNS 레코드 확인

Healthcheck 툴을 사용하여 IdM(Identity Management)에서 DNS 레코드 문제를 식별할 수 있습니다.

사전 요구 사항

- DNS 레코드 Healthcheck 툴은 RHEL 8.2 이상에서만 사용할 수 있습니다.

5.1. DNS 레코드 상태 점검 테스트

Healthcheck 도구에는 자동 검색에 필요한 예상 DNS 레코드를 확인할 수 있는지 확인하는 테스트가 포함되어 있습니다.

모든 테스트를 나열하려면 **--list -sources 옵션을 사용하여 ipa- healthcheck** 를 실행합니다.

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

ipahealthcheck.ipa.idns 소스에서 DNS 레코드 검사 테스트를 찾을 수 있습니다.

IPADNSSystemRecordsCheck

이 테스트에서는 **/etc/resolv.conf** 파일에 지정된 첫 번째 확인자를 사용하여 **ipa dns-update-system-records --dry-run** 명령에서 DNS 레코드를 확인합니다. IPA 서버에서 레코드가 테스트됩니다.

5.2. 상태 점검 툴을 사용하여 DNS 레코드 표시

Healthcheck 툴을 사용하여 IdM(Identity Management) 서버에서 DNS 레코드의 독립 실행형 수동 테스트를 실행하려면 다음 절차를 따르십시오.

Healthcheck 도구에는 많은 테스트가 포함되어 있습니다. **--source ipahealthcheck.ipa.idns** 옵션을 추가하여 DNS 레코드 테스트만 포함하여 결과를 줄일 수 있습니다.

사전 요구 사항

- **root** 사용자로 상태 점검 테스트를 수행해야 합니다.

절차

- DNS 레코드 확인을 실행하려면 다음을 입력합니다.

```
# ipa-healthcheck --source ipahealthcheck.ipa.idns
```

레코드를 확인할 수 있는 경우 테스트에서 **SUCCESS** 를 결과적으로 반환합니다.


```
{
    "source": "ipahealthcheck.ipa.idns",
    "check": "IPADNSSystemRecordsCheck",
    "result": "SUCCESS",
    "uuid": "eb7a3b68-f6b2-4631-af01-798cac0eb018",
    "when": "20200415143339Z",
    "duration": "0.210471",
    "kw": {
```

```
      "key": "_ldap._tcp.idm.example.com.:server1.idm.example.com."
    }
}
```

예를 **들어** 레코드 수가 예상 수와 일치하지 않는 경우 테스트에서 WARNING을 반환합니다.

```
{
    "source": "ipahealthcheck.ipa.idns",
    "check": "IPADNSSystemRecordsCheck",
    "result": "WARNING",
    "uuid": "972b7782-1616-48e0-bd5c-49a80c257895",
    "when": "20200409100614Z",
    "duration": "0.203049",
    "kw": {
      "msg": "Got {count} ipa-ca A records, expected {expected}",
      "count": 2,
      "expected": 1
    }
}
```

추가 리소스

- **man ipa-healthcheck** 를 참조하십시오.

6장. IDM HEALTHCHECK를 사용하여 최적의 KDC 작업자 프로세스 수 확인

IdM(Identity Management)의 상태 점검 툴을 사용하여 KDC(Kerberos Key Distribution Center)가 호스트의 CPU 코어 수와 같아야 하는 최적의 DestinationRule **5kdc** 작업자 프로세스를 사용하도록 구성되어 있는지 확인할 수 있습니다.

ipahealthcheck.ipa.kdc 소스에서 올바른 KDC 작업자 프로세스 수에 대한 테스트를 찾을 수 있습니다. 상태 점검 도구에는 많은 테스트가 포함되어 있으므로 **--source ipahealthcheck.ipa.kdc** 옵션을 추가하여 KDC 작업자 테스트만 포함하여 결과를 좁힐 수 있습니다.

사전 요구 사항

- KDC 작업자 프로세스 상태 점검 툴은 RHEL 8.7 이상에서만 사용할 수 있습니다.
- **root** 사용자로 상태 점검 테스트를 수행해야 합니다.

절차

- KDC 작업자 프로세스에 대한 검사를 실행하려면 다음을 입력합니다.

```
# ipa-healthcheck --source ipahealthcheck.ipa.kdc
```

KDC 작업자 프로세스의 수가 CPU 코어 수와 일치하는 경우 테스트에서 **SUCCESS** 를 결과를 반환합니다.

```
{
 "source": "ipahealthcheck.ipa.kdc",
 "check": "KDCWorkersCheck",
 "result": "SUCCESS",
 "uuid": "68f6e20a-0aa9-427d-8fdc-fbb8196d56cd",
 "when": "20230105162211Z",
 "duration": "0.000157",
 "kw": {
  "key": "workers"
 }
}
```

작업자 프로세스 수가 CPU 코어 수와 일치하지 않는 경우 테스트에서 **WARNING** 을 반환합니다. 다음 예에서는 코어가 2개인 호스트는 하나의 KDC 작업자 프로세스만 포함하도록 구성됩니다.

```
{
    "source": "ipahealthcheck.ipa.kdc",
    "check": "KDCWorkersCheck",
    "result": "WARNING",
    "uuid": "972b7782-1616-48e0-bd5c-49a80c257895",
    "when": "20230105122236Z",
    "duration": "0.203049",
    "kw": {
      "key": 'workers',
      "cpus": 2,
      "workers": 1,
      "expected": "The number of CPUs {cpus} does not match the number of workers
```

```
{workers} in {sysconfig}"
    }
}
```

이 테스트는 구성된 작업자가 없는 경우에도 **WARNING** 을 출력합니다. 다음 예에서 **KRB5KDC_ARGS** 변수는 **/etc/sysconfig/gradleb5kdc** 설정 파일에서 누락되었습니다.

```
 {
   "source": "ipahealthcheck.ipa.kdc",
   "check": "KDCWorkersCheck",
   "result": "WARNING",
   "uuid": "5d63ea86-67b9-4638-a41e-b71f4
56efed7",
   "when": "20230105162526Z",
   "duration": "0.000135",
   "kw": {
     "key": "workers",
     "sysconfig": "/etc/sysconfig/krb5kdc",
     "msg": "KRB5KDC_ARGS is not set in {sysconfig}"
   }
 }
```

추가 리소스

- **man ipa-healthcheck**

7장. 상태 점검을 사용하여 IDM 복제 확인

Healthcheck 툴을 사용하여 IdM(Identity Management) 복제를 테스트할 수 있습니다.

자세한 내용은 IdM의 상태 점검을 참조하십시오.

사전 요구 사항

- Healthcheck 도구는 RHEL 8.1 이상에서만 사용할 수 있습니다.

7.1. 복제 상태 점검 테스트

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

모든 테스트를 나열하려면 **--list -sources 옵션을 사용하여 ipa- healthcheck** 를 실행합니다.

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

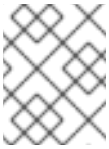
토폴로지 테스트는 **ipahealthcheck.ipa.topology 및 ipahealthcheck. ds.replication** 소스 아래에 배치됩니다.

IPATopologyDomainCheck

이 테스트는 다음을 확인합니다.

- 토폴로지 연결이 끊어지지 않고 모든 서버 간에 복제 경로가 있는지 여부.
- 서버에 권장되는 복제 계약 수 이상 없는 경우.
  테스트에 실패하면 테스트에서 연결 오류 또는 너무 많은 복제 계약과 같은 오류를 반환합니다.

  테스트가 성공하면 테스트에서 구성된 도메인을 반환합니다.

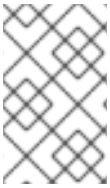


참고

테스트에서는 도메인 및 ca 접미사 모두에 대해 **ipa topologysuffix-verify** 명령을 실행합니다(이 서버에서 인증 기관이 구성되었다고 가정).

ReplicationConflictCheck

테스트에서 LDAP 일치 항목 검색(&(!(objectclass=nstombstone))(nsds5ReplConflict=*)).



참고

문제를 확인하려고 할 때 모든 IdM 서버에서 이러한 테스트를 실행합니다.

7.2. 상태 점검을 사용하여 복제 복제

Healthcheck 툴을 사용하여 IdM(Identity Management) 복제 토폴로지 및 구성을 독립 실행형 수동 테스트를 실행하려면 다음 절차를 따르십시오.

Healthcheck 도구에는 많은 테스트가 포함되어 있으므로 다음을 사용하여 결과를 단축할 수 있습니다.

- 복제 충돌 테스트**: --source=ipahealthcheck.ds.replication**
- 올바른 토폴로지 테스트**: --source=ipahealthcheck.ipa.topology**

사전 요구 사항

- **root** 사용자로 상태 점검 테스트를 수행해야 합니다.

절차

- 상태 점검 복제 충돌 및 토폴로지 검사를 실행하려면 다음을 입력합니다.

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

4가지 다른 결과가 가능합니다.

- **SUCCESSTI-**|테스트가 성공적으로 통과되었습니다.

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

- 경고 메세지**-** 테스트가 통과되었지만 문제가 있을 수 있습니다.
- 오류 메세지**-** 테스트에 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)"
  }
}
```

- **CRITICALTI-|테스트에 실패했습니다. IdM 서버 기능에 영향을 줍니다.**

추가 리소스

- **man ipa-healthcheck** 를 참조하십시오.

8장. IDM 상태 점검을 사용하여 IDM 및 AD 신뢰 구성 확인

Healthcheck 툴을 사용하여 IdM(Identity Management)의 IdM 및 Active Directory 신뢰 확인에 대해 자세히 알아보십시오.

사전 요구 사항

- Healthcheck 도구는 RHEL 8.1 이상에서만 사용할 수 있습니다.

8.1. IDM 및 AD 신뢰 상태 점검 테스트

Healthcheck 도구에는 IdM(Identity Management) 및 AD(Active Directory) 신뢰 상태를 테스트하기 위한 여러 테스트가 포함되어 있습니다.

모든 신뢰 테스트를 보려면 **--list -sources** 옵션을 사용하여 **ipa- healthcheck** 를 실행합니다.

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

ipahealthcheck.ipa.trust 소스에서 모든 테스트를 찾을 수 있습니다.

IPATrustAgentCheck

이 테스트에서는 시스템이 신뢰 에이전트로 구성된 경우 SSSD 구성을 확인합니다. **/etc/sssd/sssd.conf** 의 각 도메인에 대해 **id_provider=ipa** 는 **ipa_server_mode** 가 **True** 인지 확인합니다.

IPATrustDomainsCheck

이 테스트에서는 **sssctl** 도메인 목록의 도메인 목록을 IPA 도메인을 제외하고 **ipa trust-find** 의 도메인 목록과 비교하여 신뢰 도메인이 SSSD 도메인과 일치하는지 확인합니다.

IPATrustCatalogCheck

이 테스트에서는 AD 사용자 **Administrator@REALM** 이 해결됩니다. 그러면 **sssctl domain-status** 출력에서 AD Global 카탈로그 및 AD 도메인 컨트롤러 값이 채워집니다.

신뢰할 수 있는 각 도메인에 대해 SID + 500(관리자)의 id를 사용하여 사용자를 검색한 다음 **sssctl domain-status <domain> --active-server** 의 출력을 확인하여 도메인이 활성 상태인지 확인합니다.

IPAsidgenpluginCheck

이 테스트에서는 **IPA 389-ds** 인스턴스에서 **sidgen** 플러그인이 활성화되었는지 확인합니다. 또한 테스트에서는 **cn=plugins,cn=config** 의 **IPA SIDGEN** 및 **ipa-sidgen-task** 플러그인에 **nsslapd-pluginEnabled** 옵션이 포함되어 있는지 확인합니다.

IPATrustAgentMemberCheck

이 테스트에서는 현재 호스트가 **cn=adtrust** 에이전트인**cn=sysaccounts,cn=etc,SUFFIX** 의 멤버인지 확인합니다.

IPATrustControllerPrincipalCheck

이 테스트에서는 현재 호스트가 **cn=adtrust** 에이전트인**cn=sysaccounts,cn=etc,SUFFIX** 의 멤버인지 확인합니다.

IPATrustControllerServiceCheck

이 테스트에서는 **ipactl**에서 현재 호스트가 **ADTRUST** 서비스를 시작하는지 확인합니다.

IPATrustControllerConfCheck

이 테스트에서는 **net conf** 목록의 **passdb** 백엔드에 대해 **ldapi** 가 활성화되어 있는지 확인합니다.

IPATrustControllerGroupSIDCheck

이 테스트에서는 **admins** 그룹의 **SID**가 **512**(도메인 관리자 **RID**)로 끝나는지 확인합니다.

IPATrustPackageCheck

이 테스트에서는 신뢰 컨트롤러 및 **AD** 신뢰가 활성화되지 않은 경우 **trust-ad** 패키지가 설치되었는지 확인합니다.

참고

문제를 찾으려고 할 때 모든 **IdM** 서버에서 이러한 테스트를 실행합니다.

8.2. HEALTHCHECK 도구를 사용하여 신뢰를 건너뜁니다.

Healthcheck 툴을 사용하여 **IdM(Identity Management)** 및 **AD(Active Directory)** 신뢰 상태 점검의 독립 실행형 수동 테스트를 실행하려면 다음 절차를 따르십시오.

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

- 성공적인 모든 테스트 제외: **--failures-only**
- 신뢰 테스트만 포함: **--source=ipahealthcheck.ipa.trust**

절차

- 경고, 오류 및 중요한 문제로 인해 상태 점검을 실행하려면 다음을 입력합니다.

```
# ipa-healthcheck --source=ipahealthcheck.ipa.trust --failures-only
```

성공적인 테스트에 빈 괄호가 표시됩니다.

```
# ipa-healthcheck --source=ipahealthcheck.ipa.trust --failures-only
[]
```

추가 리소스

- **man ipa-healthcheck** 를 참조하십시오.

9장. IDM 상태 점검을 사용하여 시스템 인증서 확인

Healthcheck 툴을 사용하여 IdM(Identity Management)에서 시스템 인증서 문제 식별에 대해 자세히 알아보십시오.

자세한 내용은 IdM의 상태 점검을 참조하십시오.

사전 요구 사항

- Healthcheck 도구는 RHEL 8.1 이상에서만 사용할 수 있습니다.

9.1. 시스템 인증서 상태 점검 테스트

Healthcheck 도구에는 시스템 확인(DogTag) 인증서에 대한 여러 테스트가 포함되어 있습니다.

모든 테스트를 보려면 --list -sources 옵션을 사용하여 ipa- healthcheck 를 실행합니다.

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

ipahealthcheck.dogtag.ca 소스에서 모든 테스트를 찾을 수 있습니다.

DogtagCertsConfigCheck

이 테스트에서는 NSS 데이터베이스의 CA(Certificate Authority) 인증서를su .cfg 에 저장된 동일한 값과 비교합니다. 일치하지 않으면 CA가 시작되지 않습니다.

특히, 다음을 확인합니다.

- auditSigningCert cert-pki-ca against ca.audit_signing.cert
- ocspSigningCert cert-pki-ca against ca.ocsp_signing.cert
- caSigningCert cert-pki-ca against ca.signing.cert

- subsystemCert cert-pki-ca against ca.subsystem.cert
- ca.sslserver.cert에 대한 server-Cert cert-pki-ca

KRA(키 복구 권한)가 설치된 경우:

- transportCert cert-pki-kra against ca.connector.KRA.transportCert

DogtagCertsConnectivityCheck

이 테스트에서는 연결을 확인합니다. 이 테스트는 다음을 확인하는 **ipa cert-show 1** 명령과 동일합니다.

- Apache의 PKI 프록시 설정
- IdM에서 CA를 찾을 수 있음
- RA 에이전트 클라이언트 인증서
- 요청에 대한 CA 응답의 정확성

cert-show 를 실행하고 CA(인증서 또는 찾을 수 없음)에서 예상 결과를 가져올 수 있는지 확인하려고 하므로 테스트에서 **serial #1**을 사용하여 인증서를 점검합니다.

참고

문제를 찾으려고 할 때 모든 IdM 서버에서 이러한 테스트를 실행합니다.

9.2. HEALTHCHECK를 사용한 시스템 인증서

Healthcheck 툴을 사용하여 IdM(Identity Management) 인증서의 독립 실행형 수동 테스트를 실행하려면 다음 절차를 따르십시오.

상태 점검 도구에는 많은 테스트가 포함되어 있으므로 **DogTag** 테스트만 포함하여 결과를 좁힐 수 있습니다. **--source=ipahealthcheck.dogtag.ca**

절차

- **Healthcheck restricted**를 **DogTag** 인증서로 실행하려면 다음을 입력합니다.

```
# ipa-healthcheck --source=ipahealthcheck.dogtag.ca
```

성공적인 테스트의 예는 다음과 같습니다.

```
{
  "source: ipahealthcheck.dogtag.ca",
  "check: DogtagCertsConfigCheck",
  "result: SUCCESS",
  "uuid: 9b366200-9ec8-4bd9-bb5e-9a280c803a9c",
  "when: 20191008135826Z",
  "duration: 0.252280",
  "kw:" {
    "key": "Server-Cert cert-pki-ca",
    "configfile":  "/var/lib/pki/pki-tomcat/conf/ca/CS.cfg"
    }
}
```

실패한 테스트의 예는 다음과 같습니다.

```
{
  "source: ipahealthcheck.dogtag.ca",
  "check: DogtagCertsConfigCheck",
  "result: CRITICAL",
  "uuid: 59d66200-1447-4b3b-be01-89810c803a98",
  "when: 20191008135912Z",
  "duration: 0.002022",
  "kw:" {
    "exception": "NSDB /etc/pki/pki-tomcat/alias not initialized",
    }
}
```

추가 리소스

- **man ipa-healthcheck** 를 참조하십시오.

10장. IDM 상태 점검을 사용하여 인증서 확인

IdM(Identity Management)의 Healthcheck 툴을 이해하고 사용하여 certmonger 에서 유지 관리하는 IPA 인증서의 문제를 식별하는 방법에 대해 자세히 알아보십시오.

자세한 내용은 IdM의 상태 점검을 참조하십시오.

사전 요구 사항

- Healthcheck 도구는 RHEL 8.1 이상에서만 사용할 수 있습니다.

10.1. IDM 인증서 상태 점검 테스트

Healthcheck 도구에는 IdM(Identity Management)에서 certmonger가 유지 관리하는 인증서 상태를 확인하기 위한 여러 테스트가 포함되어 있습니다. certmonger에 대한 자세한 내용은 certmonger를 사용하여 서비스의 IdM 인증서 가져오기를 참조하십시오.

이 테스트 제품군은 만료, 검증, 신뢰 및 기타 문제를 확인합니다. 동일한 기본 문제에 대해 여러 오류가 발생할 수 있습니다.

모든 인증서 테스트를 보려면 --list -sources 옵션을 사용하여 ipa- healthcheck 를 실행합니다.

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

ipahealthcheck.ipa.certs 소스에서 모든 테스트를 찾을 수 있습니다.

IPACertmongerExpirationCheck

이 테스트에서는 certmonger 의 만료를 확인합니다.

오류가 보고되면 인증서가 만료됩니다.

경고가 나타나면 인증서가 곧 만료됩니다. 기본적으로 이 테스트는 인증서 만료일 전 28일 이내에 적용됩니다.

/etc/ipahealthcheck/ipahealthcheck.conf 파일에서 일 수를 구성할 수 있습니다. 파일을 열면 default 섹션에 있는 cert_expiration_days 옵션을 변경합니다.

참고

certmonger는 인증서 만료의 자체 보기를 로드하고 유지합니다. 이 검사는 디스크에 있는 인증서의 유효성을 검사하지 않습니다.

IPACertfileExpirationCheck

이 테스트에서는 인증서 파일 또는 NSS 데이터베이스를 열 수 없는지 확인합니다. 이 테스트도 만료를 확인합니다. 따라서 오류 또는 경고 출력에서 msg 특성을 주의 깊게 읽습니다. 메시지는 문제를 지정합니다.

참고

이 테스트는 디스크상의 인증서를 확인합니다. 인증서가 없으면 읽을 수 없음 등 별도의 오류도 발생할 수 있습니다.

IPACertNSSTrust

이 테스트는 NSS 데이터베이스에 저장된 인증서의 신뢰성을 비교합니다. NSS 데이터베이스에서 예상되는 추적된 인증서의 경우 신뢰는 예상 값과 일치하지 않는 경우 발생한 오류와 비교됩니다.

IPANSSChainValidation

이 테스트에서는 NSS 인증서의 인증서 체인의 유효성을 검사합니다. 테스트 실행: certutil -V -u V -e -d [dbdir] -n [nickname]

IPAOpenSSLChainValidation

이 테스트는 OpenSSL 인증서의 인증서 체인의 유효성을 검사합니다. 여기에서 NSS 검증 과 유사한 것은 OpenSSL 명령입니다.

```
openssl verify -verbose -show_chain -CAfile /etc/ipa/ca.crt [cert file]
```

IPARAAgent

이 테스트에서는 디스크의 인증서를 uid=ipara,ou=People,o=ipaca 의 LDAP에 있는 동등한 레코드와 비교합니다.

IPACertRevocation

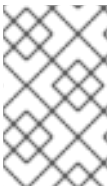
이 테스트에서는 **certmonger**를 사용하여 인증서가 취소되지 않았는지 확인합니다. 따라서 테스트는 **certmonger**에서만 유지 관리하는 인증서와 연결된 문제를 찾을 수 있습니다.

IPACertmongerCA

이 테스트는 **certmonger CA**(인증 기관) 구성을 확인합니다. **IdM**은 **CA** 없이 인증서를 발행할 수 없습니다.

certmonger는 일련의 **CA** 도우미를 유지 관리합니다. **IdM**에는 호스트 또는 서비스 인증서에 대해 호스트 또는 사용자 주체로 인증, **IdM**을 통한 인증서를 발행하는 **IPA**라는 **CA**가 있습니다.

CA 하위 시스템 인증서를 갱신 하는 **dogtag-ipa-ca-renew -agent** 및 **dogtag-ipa-ca-renew-agent-reuse**도 있습니다.



참고

문제를 확인하려고 할 때 모든 **IdM** 서버에서 이러한 테스트를 실행합니다.

10.2. 상태 점검 툴을 사용한 암호 인증서

Healthcheck 툴을 사용하여 **IdM(Identity Management)** 인증서 상태 점검의 독립 실행형 수동 테스트를 실행하려면 다음 절차를 따르십시오.

Healthcheck 도구에는 많은 테스트가 포함되어 있으므로 다음을 사용하여 결과를 단축할 수 있습니다.

- 성공적인 모든 테스트 제외: **--failures-only**
- 인증서 테스트만 포함: **--source=ipahealthcheck.ipa.certs**

사전 요구 사항

- **root** 사용자로 상태 점검 테스트를 수행해야 합니다.

절차

- 경고, 오류 및 인증서와 관련된 중요한 문제를 사용하여 상태 점검을 실행하려면 다음을 입력

합니다.

```
# ipa-healthcheck --source=ipahealthcheck.ipa.certs --failures-only
```

성공적인 테스트에 빈 괄호가 표시됩니다.

```
[]
```

실패한 테스트는 다음 출력을 보여줍니다.

```
{
  "source": "ipahealthcheck.ipa.certs",
  "check": "IPACertfileExpirationCheck",
  "result": "ERROR",
  "kw": {
    "key": 1234,
    "dbdir": "/path/to/nssdb",
    "error": [error],
    "msg": "Unable to open NSS database '/path/to/nssdb': [error]"
  }
}
```

이 IPACertfileExpirationCheck 테스트는 NSS 데이터베이스를 열 때 실패했습니다.

추가 리소스

- man ipa-healthcheck 를 참조하십시오.