

목차

RHV 4.x 인증서 갱신	3
이슈	3
RHV 인증서 갱신 (4.0에서 테스트 완료)	3
0. rhv-m 백업 (vm정상)	3
1. RHV-M에서 engine-setup으로 인증서 갱신 (vm정상)	3
2. RHV-M에서 /etc/hosts 에 호스트 등록 (vm정상)	3
3. RHV-M에서 singlehost.sh <호스트이름/IP> 실행 (vm정상)	3
4. 각 하이퍼바이저에서 vdsmd 데몬 재기동 (vm정상)	4
5. 호스트 한개부터 시작 (최소 한개의 호스트는 비워야 한다. VM을 종료한다.)	4
6. 서비스 확인	5
7. 매니저 정상 확인	5
장애처리	5
참조링크	5
추가정보	5

RHV 4.x 인증서 갱신

— 이강우 2023/05/28 13:14

이슈

```
sun.security.validator.ValidatorException: PKIX path validation failed:  
java.security.cert.CertPathValidatorException: validity check failed
```

RHV 인증서 갱신 (4.0에서 테스트 완료)

- 모든 호스트는 NTP동기화가 정상적으로 이루어져 있어야 함

0. rhv-m 백업 (vm정상)

```
engine-backup --scope=all --mode=backup --file=<BACKUP_FILE> --  
log=<LOG_FILE>
```

1. RHV-M에서 engine-setup으로 인증서 갱신 (vm정상)

Renew certificates? (Yes, No) [No]: yes선택

갱신후 매니저 화면 확인 매니저에서 호스트 정보 확인후 해당 내용 /etc/hosts에 등록(없을경우)

2. RHV-M에서 /etc/hosts 에 호스트 등록 (vm정상)

root 계정 디렉토리에 .ssh 폴더 존재 여부 확인 매니저에서 모든 호스트서버에 ssh root@host 접속 시도하여 접속여부 확인 (다음 단계의 스크립트 실행시 필요)

3. RHV-M에서 singlehost.sh <호스트이름/IP> 실행 (vm정상)

<https://access.redhat.com/sites/default/files/attachments/singlehost.sh> (

singlehost.zip

) 이름은 반드시 RHV-M 상에 등록된 이름/IP로 실행해야함

```
./singlehost.sh 10.33.4.11
```

4. 각 하이퍼바이저에서 vdsmd 데몬 재기동 (vm정상)

```
systemctl daemon-reload
systemctl restart vdsmd
```

호스트에서 : `systemctl restart vdsmd`

기다리면 hosts가 active로 올라옴 (약 10분)

- SPM까지 복구 되는거 확인 Contending → SPM으로 되어야 함(약 10분)
- 스토리지 도메인 정상 확인
- VM 콘솔 화면 확인

이 단계에서 VM Live migration실패 (이유: 호스트간 인증서가 예전 인증서로 기동되어있기 때문에 마이그레이션이 안됨) VM을 셧다운 → 기동 해도 마이그레이션 불가하므로 특별한 이유가 없다면 VM은 현상태 유지

libvirtd를 재기동하면 라이브마이그레이션도 가능 및 SPM이전도 가능해짐

```
# 이 작업은 아래 주의사항을 읽고 진행하도록 한다. VM이 강제종료될 수 있다.
$ systemctl restart libvirtd
# 또는 RHEV 3.x에서
$ vdsmd-tool service-restart libvirtd
```

주의 해야할것은 libvirtd를 재기동 할 경우 RHV 일부 버전에서는 버그로 인해 동작중인 VM이 강제 종료되는 경우가 있다. 따라서 이부분은 재량에 따라 진행하며 불가피한경우 이부분은 건너뛰고 최소한의 VM만 종료하여 다음 단계처럼 빈 호스트를 만들어 마이그레이션을 진행하도록 한다.

https://bugzilla.redhat.com/show_bug.cgi?id=1946697

https://bugzilla.redhat.com/show_bug.cgi?id=1836865

vdsmd를 재기동 했음에도 불구하고 매니저에서 호스트가 Up상태로 올라오지 않는다면 매니저의 ovirt-engine을 재시작 하거나 리부팅 해본다.

```
$ systemctl restart ovirt-engine
# 또는
$ sync; reboot
```

5. 호스트 한개부터 시작 (최소 한개의 호스트는 비워야 한다. VM을 종료한다.)

유지보수 모드 → 인증서 설치 → 리부팅 (최초 리부팅한 호스트를 SPM으로 지정)

이후 기존호스트 → 리부팅한 호스트로의 마이그레이션 정상 동작

6. 서비스 확인

마지막으로 매니저 서버 리부팅

7. 매니저 정상 확인

- 가급적 ISO Domain은 사용하지 않는다면 detach 해둔다.

장애처리

혹시라도 작업 이후 VM 리부팅 시에 부팅이 되지 않는 현상이 발생하면 아래 문서를 참고하도록 한다.
[Failed to mount /sysroot](#)

참조링크

- <https://access.redhat.com/solutions/6974830>
- <https://access.redhat.com/solutions/3532921>
- <https://access.redhat.com/solutions/6865861>
- <https://access.redhat.com/solutions/3329431>
- <https://access.redhat.com/solutions/4780411>

추가정보

인증서를 만료전에 강제로 갱신하는 방법

engine-setup 시 강제로 PKI Renew 하도록 하는 추가 설정파일 내용 engine-setup --config-append=renew.conf 와 같이 사용할 수 있다.

renew.conf 파일 내용

```
[environment:default]
OVESETUP_PKI/renew=bool:True
OVEHOST_PKI_GENERATENEW=bool:True
OVESETUP_RENEW_PKI=bool:True
OVESETUP_PKI_PRESERVE=bool:False
```

문제는 이 방법을 쓰더라도 CA파일은 날짜가 만료되지 않으면 갱신되지 않는다. 최상위 서명 기관인 CA(인증 기관)가 전혀 변경되지 않은 상태에서, 그 CA를 기반으로 개별 인증서들만 재발급(re-enroll)하는 것입니다.

결과적으로, 개별 인증서 파일의 타임스탬프는 바뀔 수 있지만, 인증서를 발급한 기관(Issuer)과 인증서 체인이 동일하기 때문에 openssl로 확인했을 때 일련번호(Serial Number)나 다른 중요한 내용이 바뀌지 않을 수 있습니다. 사용자가 보기에는 사실상 “갱신되지 않은 것”과 같은 결과가 나타나는 것입니다.

Last update:
2025/06/24
13:11

rhv_4.x 인
증서 갱신

https://atl.kr/dokuwiki/doku.php/rhv_4.x_%EC%9D%B8%EC%A6%9D%EC%84%9C_%EA%B0%B1%EC%8B%A0

따라서 전체 인증서를 만료되기 전에 새로 갱신하는 방법은 존재하지 않는다. 꼭 바꾸고 싶다면 백업/복구 방법으로 새로 설치를 하는 수밖에 없다.

From:

<https://atl.kr/dokuwiki/> - AllThatLinux!

Permanent link:

https://atl.kr/dokuwiki/doku.php/rhv_4.x_%EC%9D%B8%EC%A6%9D%EC%84%9C_%EA%B0%B1%EC%8B%A0

Last update: 2025/06/24 13:11

