목차

RHEV 2.2 인증서 만료 확인 및 갱신 3
인증서 확인 3
인증서 종류와 확인 6
RHEVM CA 7
FQDN 개인 인증서 7
레드햇 인증서 - 코드 서명 인증서 8
호스트 인증 9
참고사항 10

RHEV 2.2 인증서 만료 확인 및 갱신

— *이강우 2016/04/28 09:06*

RHEV 2.2 에서 사용되는 인증서는 3가지 종류가 있습니다.

1. RHEV-M CA 자체 서명 인증서
2. RHEV-M 개인 인증서
3. 코드 서명 인증서

CA인증서와 개인 인증서는 RHEV의 다른 구성 요소간 보안 통신을 위해 사용됩니다.

1. HTTPS를 통해 RHEV-M 및 사용자 / 관리자 포탈 사용
2. RHEV-M 내부 통신 - WCF를 통한 프론트/백 엔드간 통신
3. SSH를 통한 RHEV-M 과 Host간 통신

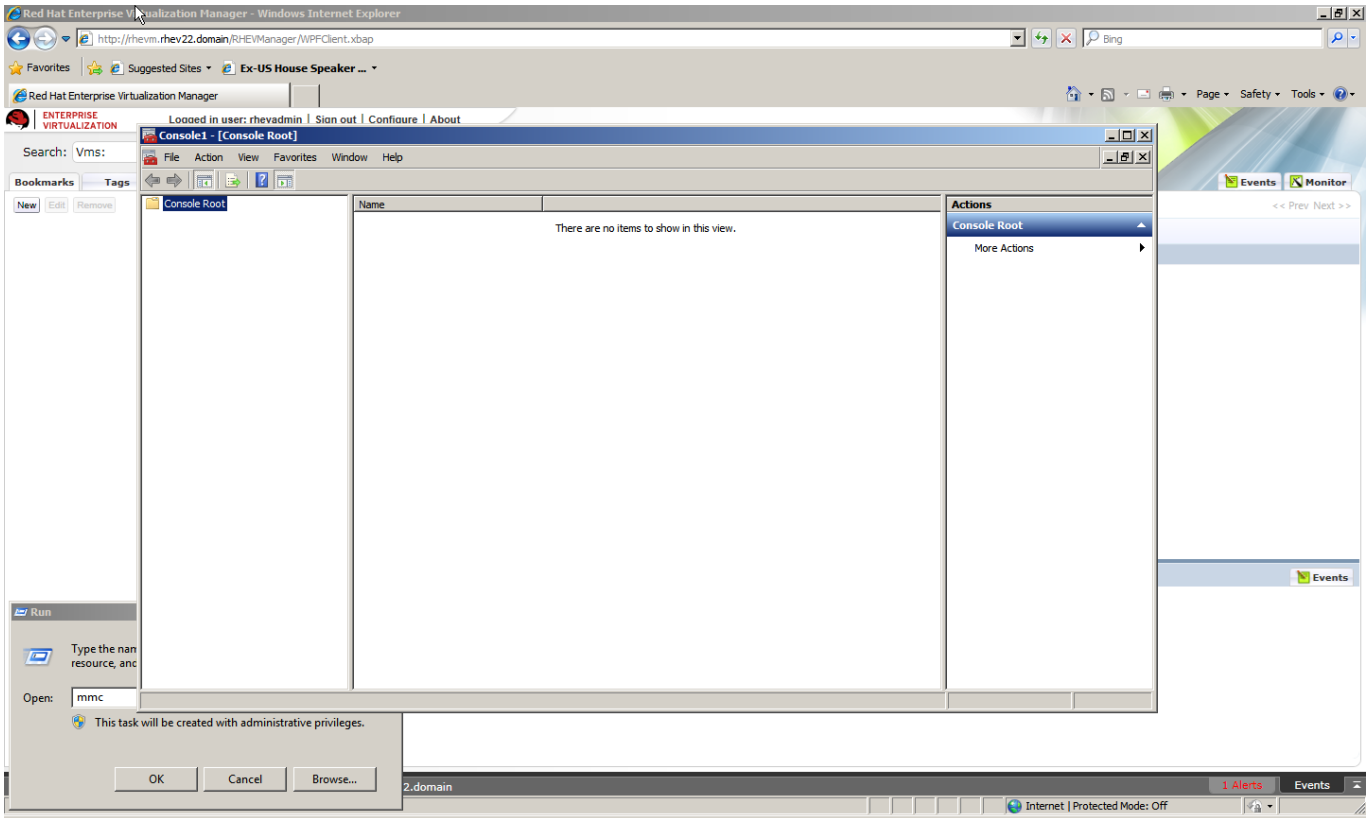
코드 서명 인증서는 클라이언트의 WPF실행에 필요한 인증서입니다. 관리포털 접속시 설치하는 WPF응용프로그램입니다. 일반적으로 클라이언트 PC에 설치되며 Verisign에 의해 서명되어집니다.

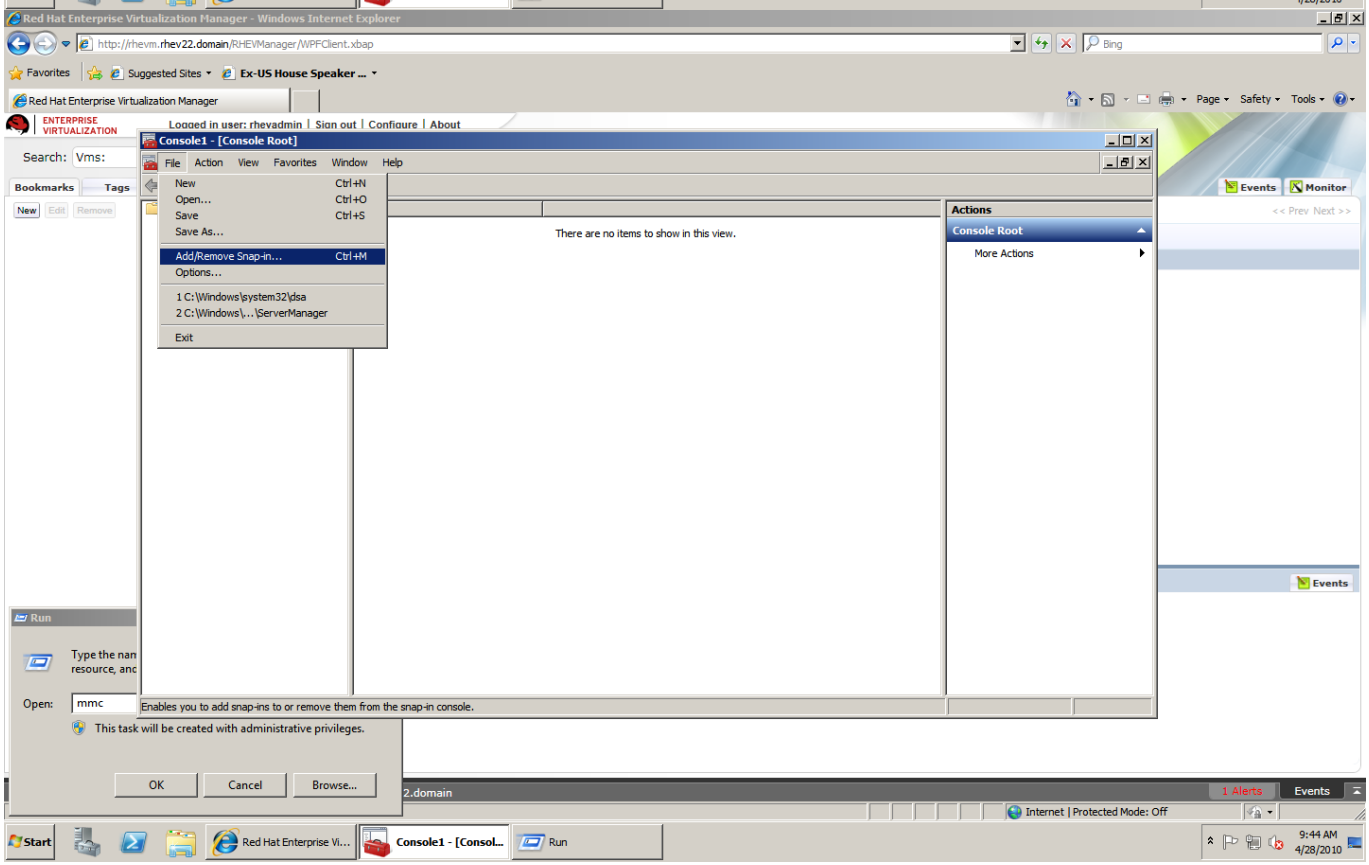
윈도우 OS에 대한 인증서는 다른 인증서 저장소에 구성되어 인증관리자 콘솔을 통해 접근 할 수 있습니다.

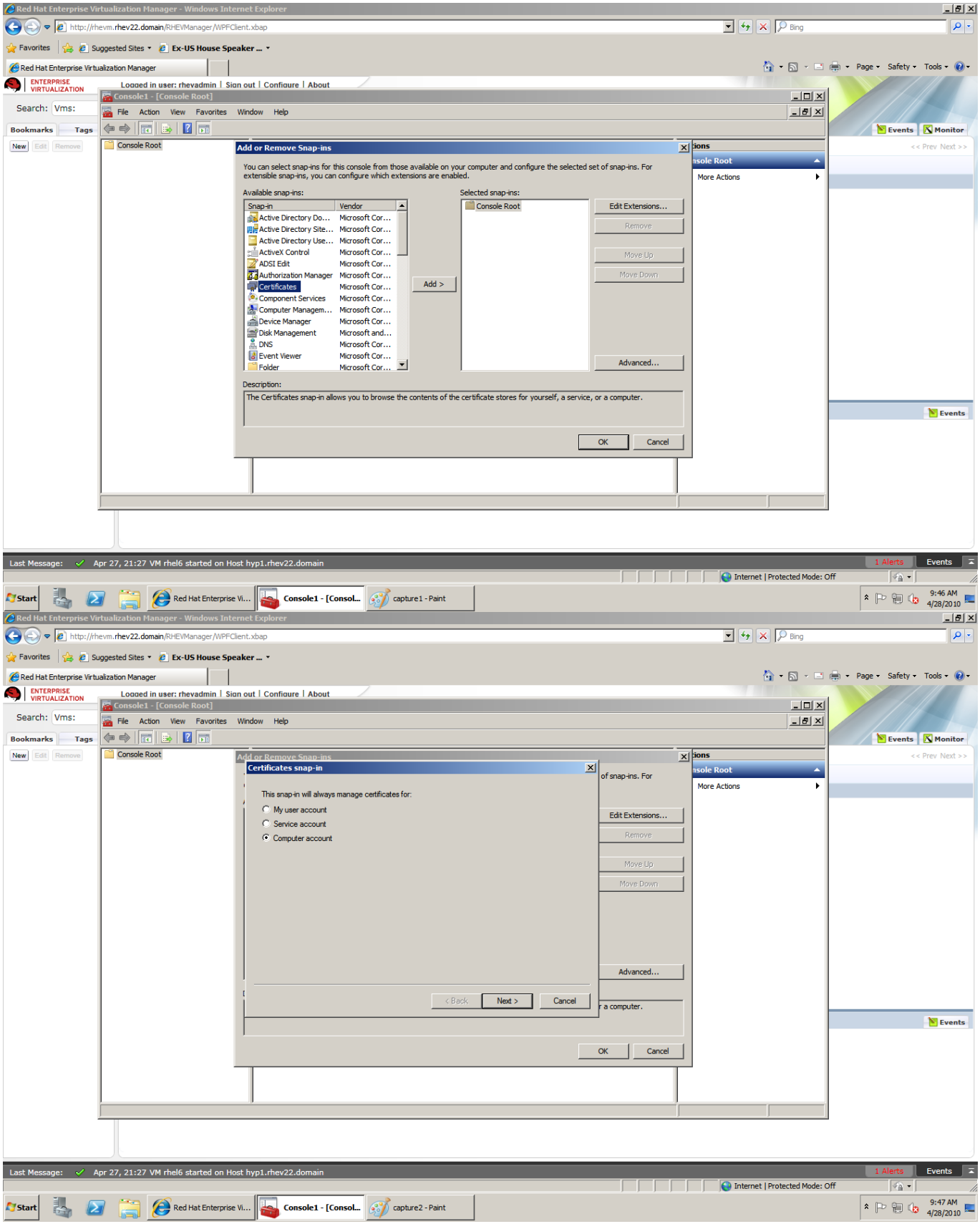
RHEV-M은 로컬 컴퓨터 계정에 모든 인증서를 설치 합니다.

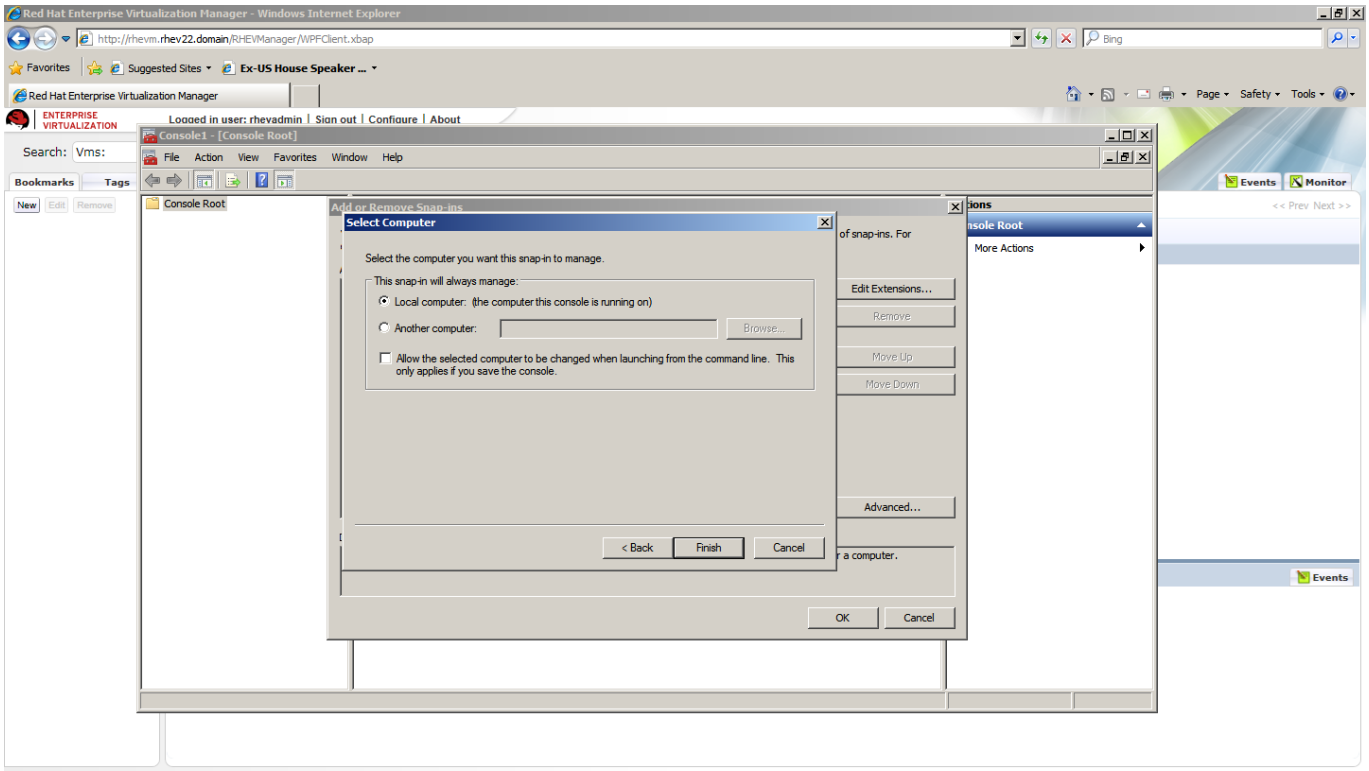
인증서 확인

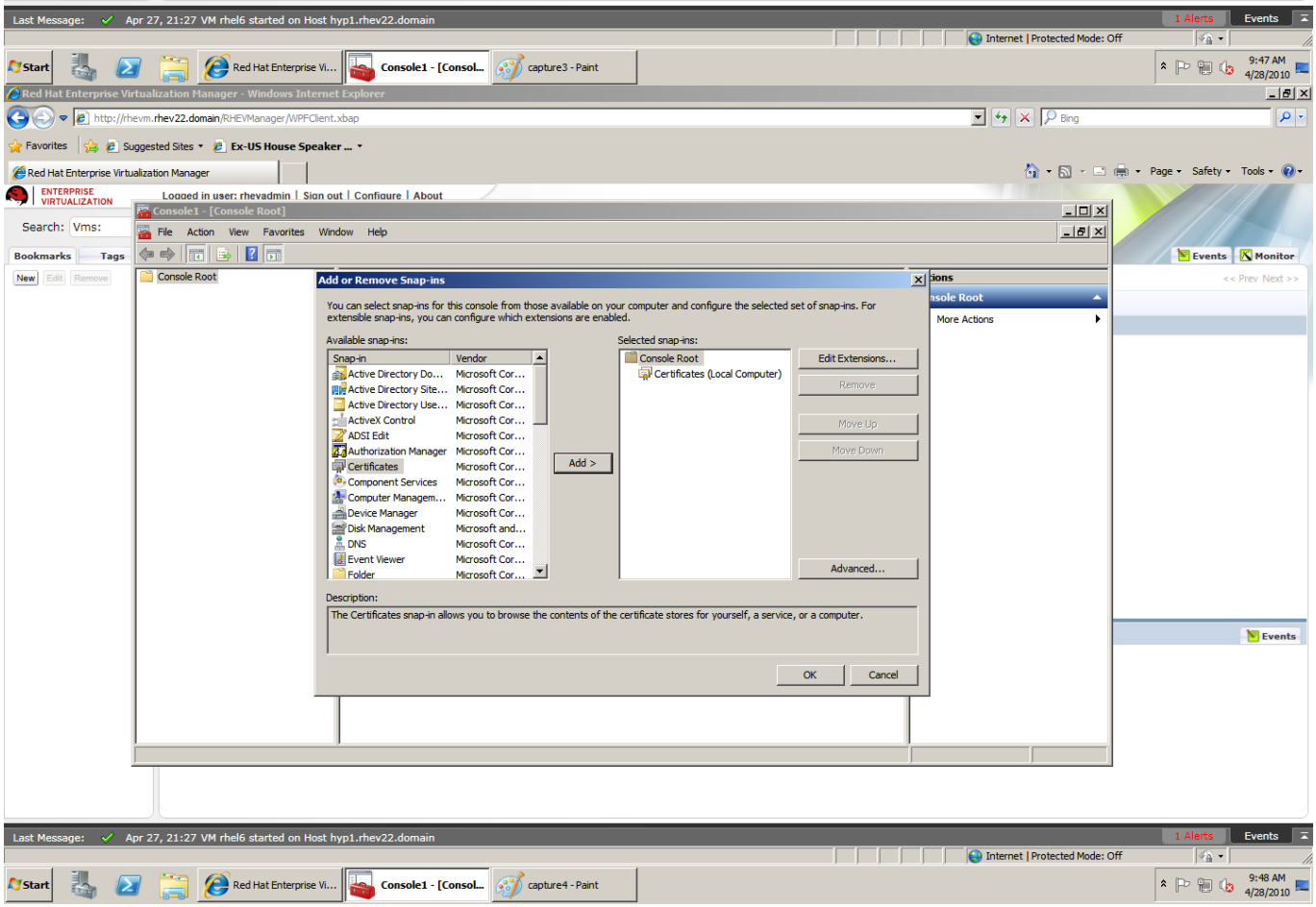
1. 실행 > MMC
2. 인증서 스냅인을 MMC에 추가
3. 스냅-IN→ 추가
4. 추가 / 제거 → 인증서 :
5. 컴퓨터 계정> 로컬 컴퓨터를 추가 → 확인


Red Hat Enterprise Virtualization Manager - Windows Internet Explorer
http://rhevm.rhev22.domain/RHEVManager/WPFClient.xbap
Console1 - [Console Root]
File Action View Favorites Window Help
Console Root
Name
There are no items to show in this view.
Actions
Console Root
More Actions
Run
Open: mmc
This task will be created with administrative privileges.
OK Cancel Browse...


Red Hat Enterprise Virtualization Manager - Windows Internet Explorer
http://rhevm.rhev22.domain/RHEVManager/WPFClient.xbap
Console1 - [Console Root]
File Action View Favorites Window Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\Windows\system32\dsa
2 C:\Windows\...\ServerManager
Exit
There are no items to show in this view.
Actions
Console Root
More Actions
Enables you to add snap-ins to or remove them from the snap-in console.
Run
Open: mmc
This task will be created with administrative privileges.
OK Cancel Browse...


Red Hat Enterprise Virtualization Manager - Windows Internet Explorer
Add or Remove Snap-ins
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.
Available snap-ins:
Selected snap-ins:
Console Root
Edit Extensions...
Remove
Move Up
Move Down
Add >
Advanced...
Description:
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.
OK
Cancel
Certificates snap-in
This snap-in will always manage certificates for:
My user account
Service account
Computer account
< Back
Next >
Cancel
Last Message: Apr 27, 21:27 VM rhel6 started on Host hyp1.rhev22.domain
Start
Console1 - [Consol...
capture1 - Paint
capture2 - Paint
9:46 AM
9:47 AM
4/28/2010





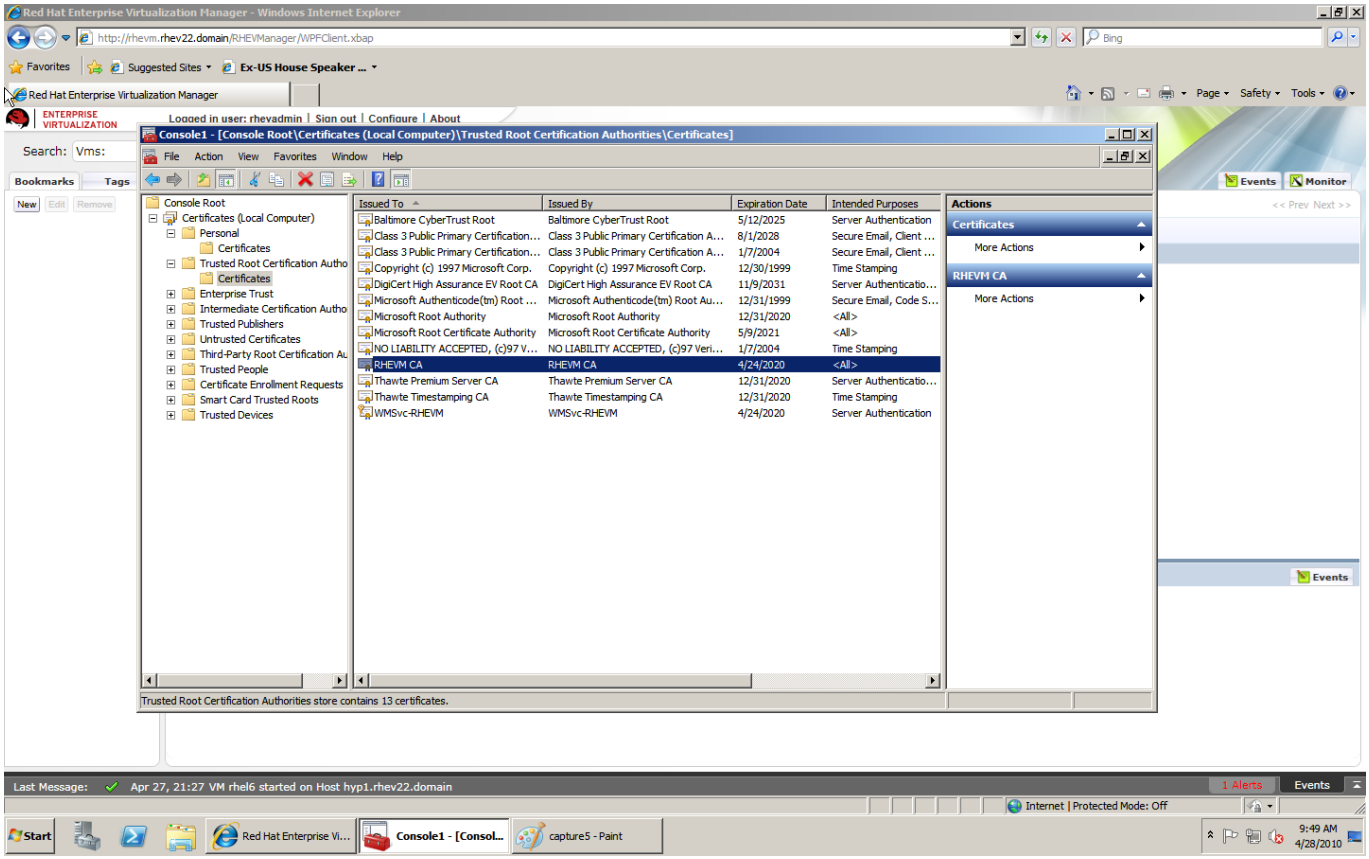
인증서 종류와 확인

인증서 종류는 아래와 같습니다.

RHEVM CA

이 RHEVM 공개 키와 인증서입니다. 그것은 자체 서명 된 RHEV-M 설치시 생성 한 다음 보안 통신을 제공하기위한 시스템의 다른 인증서에 서명하는 데 사용됩니다. 신뢰할 수있는 루트 인증 기관 저장소에 위치하고 있습니다.

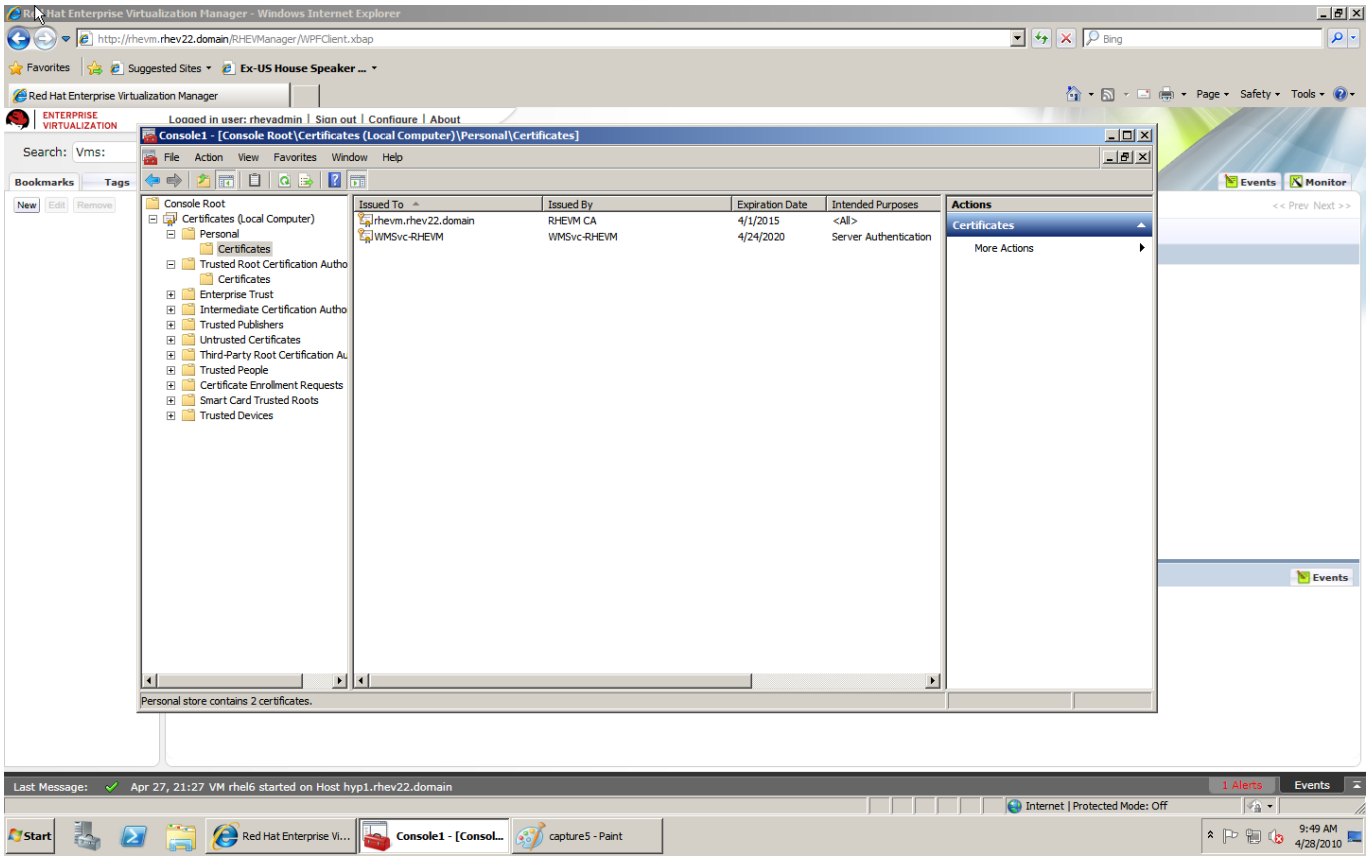
기본 유효기간은 설치 후 10년입니다.



FQDN 개인 인증서

이 RHEV-M 시스템의 개인 인증서로 RHEV-M를 설치하는 동안 만들었습니다. (그리고 다시 설치하는 경우마다 다시 생성합니다.) 그것은 이전과 동일한 설치 한 단계에서 생성 된 RHEV-M의 CA에 의해 서명됩니다. 개인 저장소에 위치하고 있습니다. 내부 RHEVM 구성 요소 간의 보안 통신 및 보안 HTTP를 통해 관리자 / 사용자 포털에 액세스하는 데 사용됩니다.

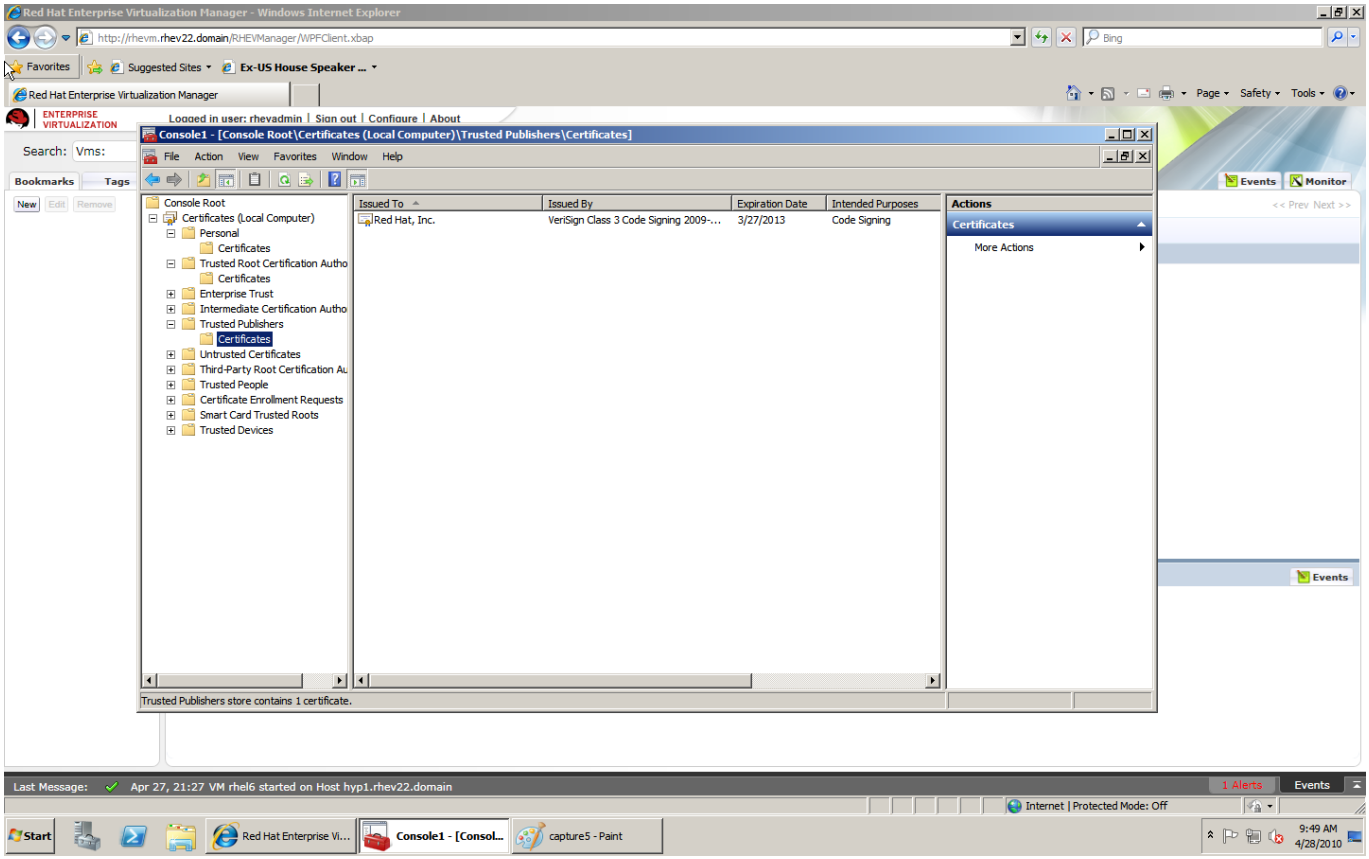
기본 유효기간은 설치 후 5년입니다.



레드햇 인증서 - 코드 서명 인증서

신뢰할 수있는 게시자 저장소에 위치하고 있습니다. 베리사인 클래스 3 코드 서명 CA에 의해 서명 WPF 응용 프로그램에 대한 완전 신뢰 요구 사항을 제공하기 위해 닷넷 코드를 서명하는 데 사용됩니다. 또한 RHEV-M 라이선스에 서명하는 데 사용.

기본 유효기간은 제품마다 고정되어있습니다. RHEV 2.x 설치시 제공되는 레드햇 인증서의 유효기간은 2013년 3월 27일까지입니다.



호스트 인증

각 호스트는 자신의 인증서를 생성하고 호스트 연결 절차의 일환으로 RHEV-M에 대한 서명 요청을 보냅니다. RHEV-M은 RHEVM CA와 호스트의 인증서에 서명하고 호스트로 다시 보냅니다. 그 후, 호스트 및 RHEV-M는 안전하게 통신 할 수있다.

호스트의 인증서 경로 : /var/vdsm/ts/certs # 공개 키

- cacert.pem # ca 인증서 기본 유효기간 10년
- vdsmcert.pem # vdsm 인증서 기본 유효기간 5년

유효기간 확인방법은 해당 pem파일을 열어보게 되면 확인이 가능합니다.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 3 (0x3)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=rhev22, CN=RHEVM CA
        Validity
            Not Before: Apr 26 21:02:52 2010 GMT
            Not After : Apr 27 04:02:53 2015 GMT
        Subject: O=rhev22, CN=192.168.0.141
        Subject Public Key Info:
```

/var/vdsm/ts/keys # 개인키

- vdsmkey.pem

참고사항

(!) 2.1 버전에서 사용하는 레드햇의 Inc 인증서 년 11 월에 만료 위해 2.2으로 업그레이드해야합니다 2.1 버전을 실행하는 2010 고객 관리 포털에 액세스 할 수 있습니다. 당신은 RHEV-M을 다시 설치하는 경우 (!), 그 기계에 대한 새 개인 인증서를 생성합니다. 이 서버에 연결된 모든 호스트 (제거하고 다시 추가) 다시 연결해야합니다 있도록, 새 인증서를 얻고 보안 통신을 가능하게합니다. 이 문서 RHEVM CA 와 레드햇, Inc의 인증서에 첨부. 그들은 RHEV 버전 2.2.4에 대한 유효 최대. 때를 사용 : 당신이 2.2.4을 실행하는 경우 어떤 이유로 당신은 당신의 인증서가 손상되었다. 그 사용 방법 : 관련 저장소로 가져옵니다.

- rhevm-ca.cer.zip
- redhatinc.cer.zip

From:
https://atl.kr/dokuwiki/ - **AllThatLinux!**

Permanent link:
https://atl.kr/dokuwiki/doku.php/rhev_2.2_%EC%9D%B8%EC%A6%9D%EC%84%9C_%EB%A7%8C%EB%A3%8C_%ED%99%95%EC%9D%B8_%EB%B0%8F_%EA%B0%B1%EC%8B%A0?rev=1461808797

Last update: **2016/04/28 01:59**