

Changing your host's network name and SSL certificate

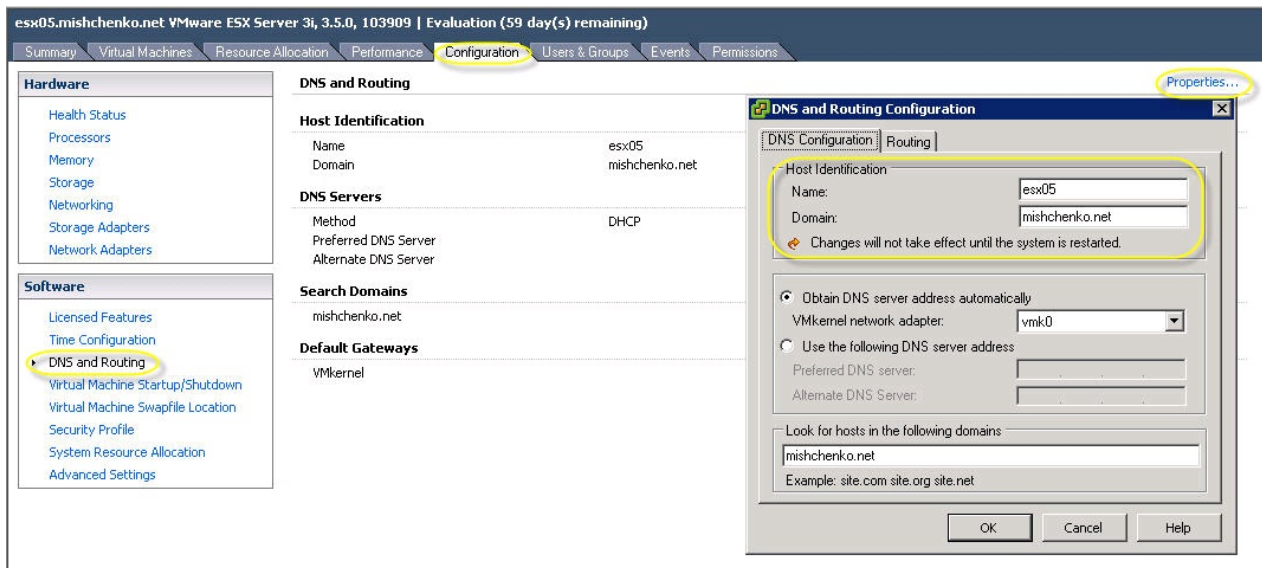
When you first install ESXi your host will be given a hostname of "localhost" and domain of "localdomain". You can change this at the console or with the VI client.

Using the Console

- 1) Press <F2> (Customize System)
- 2) Select Configure Management Network
- 3) Select DNS Configuration
- 4) Select the option "Use the following DNS server address and hostname"
- 5) In the hostname enter the hostname and domain for your host. Then press Enter.
- 6) Select Y (Yes) when prompted to save changes and restart the management network. The change will take place immediately.

Using the VI client

- 1) Go to Configuration tab and select DNS and Routing
- 2) Click on Properties to open the DNS and Routing Configuration screen
- 3) Enter the name and domain for your host and click OK.
- 4) Right click on the host and select Reboot.



Note: both these methods will update /etc/hosts on the ESXi host. Should you manually edit this file, it is important that you do not modify the line that consists of **127.0.0.1 localhost.localdomain localhost**.

Updating the SSL Certificate for your host

Should you change your host's hostname or domain after an install, the SSL certificate for the host will still be issued to localhost.localdomain. You can either regenerate a self-signed certificate for your ESXi host or replace the certificate from one generated by a certificate authority.

Regenerate your host's self-signed certificate

- 1) Access the console of ESXi. If you have not done that before, follow the first three steps on this [page](#).
- 2) Run the command `/sbin/create_certificates` as shown in the image below. This will replace both the private key and SSL certificate for the host. These files are located in /etc/vmware/ssl/
- 3) Enter the command `reboot` to restart the host. The certificate for the host will now reflect the hostname and domain changes that you have made.

```
WARNING - Tech Support Mode is not supported unless used in
consultation with VMware Tech Support. Tech Support Mode may be
disabled by an administrative user. Disabling requires a reboot of
the system. Please consult the ESX Server 3i Configuration Guide
for important additional information.

Password:

Tech Support Mode successfully accessed.
The time and date of this access have been sent to the system logs.

WARNING - Tech Support Mode is not supported unless used in
consultation with VMware Tech Support.

~ # /sbin/create_certificates
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to '/etc/vmware/ssl/rui.key'
-----
~ # ls -l /etc/vmware/ssl/
-r--r--r-- 1 root root 1229 Aug 9 15:15 rui.crt
-r----- 1 root root 891 Aug 9 15:15 rui.key
~ #
```

Replace the host's certificate with one generated by a certificate authority

The below steps used OpenSSL which can be downloaded from [here](#) and a Microsoft Windows 2003 Server Certificate Authority.

- 1) Download and install OpenSSL from the link provided. If you're using Linux, your host may already have the OpenSSL package. If you are using Windows, you may also need to download the Microsoft Visual C++ 2008 Redistributable [Package](#).
- 2) Generate a new private key with the command `openssl genrsa 1024 > rui.key`.

3) Create a new certificate request by running the command `openssl req -new -key rui.key > rui.csr`. A wizard will run and prompt you for information for the certificate request.

```
C:\OpenSSL\bin>openssl req -new -key rui.key > rui.csr
Loading 'screen' into random state - done
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value.
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CA
State or Province Name (full name) [Some-State]:BC
Locality Name (eg, city) []:Surrey
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Home
Organizational Unit Name (eg, section) []:Basement
Common Name (eg, YOUR name) []:esx05.mishchenko.net
Email Address []:daven@vm-help.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

C:\OpenSSL\bin>
```

- 4) Open the rui.csr file with a text editor and copy the contents. If using Windows, avoid using Notepad as it may insert extra characters into the copied text.
- 5) Open the certificate request page for your Windows 2003 CA server. This is typically `http://<hostname>/certsrv`.
- 6) Click on the "Request a Certificate" link followed by the "advanced certificated request" link on the Request a Certificate page.
- 7) Select the link "Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file."
- 8) On the certificate request page enter the text from the rui.csr file and change the Certificate Template to Web Server. Then click Submit.

Microsoft Certificate Services -- DC02

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or from external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	<pre>ogA+qvQyrtP5uJZp6SgKcY29T9tVcFMz+41XtEIH XMGjsVbqNNh5YnoMDyyC7eYkpSWkullIhwIDAQAB gYEAAzmPFU69jRldUvCzpHhz2v7uBJAQkp/dZpGy j69i+B5w1wc7GxiT4F4XvEeVlsaaKfKMOtn2YLP9 iA3n19gsfPD1gWrmjCdG5ZCUMLEjmlEIGlFGjbJM -----END CERTIFICATE REQUEST-----</pre>
Browse for a file to insert.	

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >

- 9) On the certificate issued page, select the "Based 64 encoded" option and then download the certificate to your PC
- 10) Run the command on the certificate that you downloaded: `openssl x509 -in certnew.cer -out esx.cer`.
- 11) Copy the private key and certificate to your ESXi host with the following RCLI commands
`vifs.pl -server esx05.mishchenko.net --put rui.key /host/ssl_key`
`vifs.pl -server esx05.mishchenko.net --put esx.cer /host/ssl_cert`
- 12) Restart the ESXi and verify that the certificate has been installed correctly. If there is a problem with the certificate, you may not be able to login to the host with the VI client. If that's the case, then run `/sbin/create_certificates` at the console and reboot the host.

Note: if you try to join your ESXi host to a vCenter server and get the error: "The SSL Certificate of the remote host could not be validated" you'll want to ensure that the root CA that issued the certificate is trusted by the vCenter host at the "Computer account" level and not just for "My user account".

[+] JVS 12-31-2008

Excellent howto, keep up the good work!

[+] MDW 01-07-2009

The put command does not change the file on my server. I looked at the syslog and see that the RCLI logged in but no commands were executed.

[+] Dave Mishchenko 01-07-2009

MDW, are you able to get files OK? Are you able to upload any files like esx.conf?

[+] MDW 02-13-2009

Sorry about the delay. I tried to modify and then upload motd and still see that I logged in, but the file has not changed.

[+] Dave Mishchenko 02-15-2009

The motd file is one you can download / upload with vifs.pl, but ESXi doesn't back up the file into state.tgz so any changes to the file would be lost when you reboot the host. If you want to permanently edit the file, then you would need to add it to oem.tgz.

[+] Gary 02-27-2009

I am getting "The SSL Certificate of the remote host could not be validated" after the vcenter fail to verify the authenticity of the esx host. I imported the root CA into the "Trusted Root Certification Authority" as "administrator. What do you mean by "computer account" and "my user account" level?

[-] [Dave Mishchenko](#) 02-28-2009

When you start MMC and then add the certificates snap-in you can specify that you will manage certificates for "My User Account", "Service Account" or "Computer Account". If you add the cert when you select My User Account it will only work for your account. To have the cert used for the vCenter server, you either have to select Service account (and then the vCenter service) or select Computer Account if the vCenter service uses the LocalSystem account. That way the vCenter service will have access to that root cert.

[-] Gary 03-02-2009

That worked. Thanks Dave. Initially, I followed the instruction in the VMware doc "replacing VC service cert." It said to just run certmgr.msc and import the Root CA. I guess that alone wasn't enough.

[-] Igor 04-28-2009

Hi Dave,

Thanks for excellent article. For my ESXi 3.5.0 update 4 host, I had to put the key and certificate files to /etc/vmware/ssl/ rui.key and rui.crt files; also, it's possible to save the certificate directly in Base64 encoding and don't use "openssl x509 -in certnew.cer -out esx.cer" (it may fail if there's certificate changing).

[-] [Wesley Darlington](#) 06-12-2009

On esxi 4.0.0 the script is /sbin/generate-certificates.sh (rather than /sbin/create_certificate ... note a hyphen rather than an underscore.)

[-] cookieme 07-30-2009

I have a standalone ESXi server. When I setup DNS similar to your config above, I cannot access my host via the vClient using esxi.mycompany.com. I do not have any DNS servers on this network, just the standalone ESXi host with three VMs. Can I solve this somehow?

[-] [Dave Mishchenko](#) 07-30-2009

If you don't have a DNS server then you could add the hostname and IP to your local hosts file.

[-] Vivek 09-06-2009

Can you please help me to update my ESX3.5i self signed certificates to 128 bit encryption

[-] [Dave Mishchenko](#) 09-07-2009

Vivek, your question would be best handled in the forum - <http://www.vm-help.com/forum/>. Could you include details about your CA server?

[-] Vivek 09-08-2009

I do not use a CA, i would like to upgrade the ESXi self-signed (no third party CA) certificate. Is it possible.

First of all i would like to know the current level of the encryption on the ESXi host (3.5.0 build 163429)

[-] Vivek 09-08-2009

I do not use a CA, i would like to upgrade the ESXi self-signed (no third party CA) certificate. Is it possible.

First of all i would like to know the current level of the encryption on the ESXi host (3.5.0 build 163429)

[-] [Maartycz](#) 10-22-2009

I found out that I can manually upload rui.key and rui.crt to /etc/vmware/ssl/ via scp or WinSCP. vifs.pl mentioned above does not work. After restart all works fine. Also make sure, you generate 1024 key not 512 it does not work.(if you are used to generate key via IIS)

[-] Derek 11-21-2009

I've modified your procedure for ESXi 4.0/U1 hosts. You can see the whole blog post here:

<http://derek858.blogspot.com/2009/11/vsphere-esxi-ssl-mystery-solved.html>

[-] udo 01-06-2010

i have ESXi 4.0 and the command /sbin/create_certificates does not work

Answer from ESXi /sbin/create_certificates: not found

Can you help?

[-] [Dave Mishchenko](#) 01-06-2010

For ESXi 4.0 look at /sbin/generate-certificates.sh

[-] udo 01-06-2010

Thank you thats working fine.

He will generate a 512 bit RSA pk -> ca.key and a 1024 bit pk -> rey.key

But there are Warning:

WARNING: Cant open config file: /etc/pki/tls/openssl.cnf

INSERT YOUR COMMENT - IF YOU HAVE A QUESTION PLEASE USE THE [FORUM](#)

Name (required)

Website (optional)

Email address (required - will not be displayed)

Comment (required)



Please enter code

Publish the Comment

Copyright © 2009 - Dave Mishchenko