

Trusted SSL certificates - request for ...



Guy Chapman 5 posts since

Jul 29, 2008

As I guess most of us will know, the default in VMware is to use self-certified certificates for the web interface. Best practice would be to replace these with trusted certificates either from your Active Directory certificate store, a valid certificate from a trusted vendor, or whatever other corporate certification authority you use.

;

Fixing the hosts is pretty straightforward, there is a great guide on the forums, but here are the steps (which assume that you have installed and configured OpenSSL)

;

This is my process, please peer review and comment.

Prerequisites

You will require a copy of OpenSSL, the open source SSL key generator. This can be downloaded from <http://www.openssl.org/> and the current version at time of writing is 0.9.8h. This is not the only tool available but it is the one on which VMware's documentation is based and it is supported by VMware.

;

The software must be installed and configured per the instructions on the website. It's not hard, and the documentation below also includes some help on this.

Background reading advised:

;

- VMware documentation on SSL certificate generation: http://www.vmware.com/pdf/vi_vcserver_certificates.pdf
- A thread in the VMware knowledge base: <http://communities.vmware.com/thread/88053?tstart=0>

;

Back up your certificates before you start. And back up your VCDB as well, just in case.

Creating the certificate request (CSR)

The CSR is created on the machine on which you installed OpenSSL. Note that if you use a Microsoft CA the key names and specifications differ between Microsoft's CA and OpenSSL. This is covered as necessary in the procedure.

;

Procedure:

1. Open a command window and change to the OpenSSL binary directory (default c:\OpenSSL\bin)
2. Check the settings in your local openssl config file. This is named openssl.cnf by default, you should copy it to openssl.cfg because Windows interprets .cnf as a SpeedDial shortcut; this is not fatal (you can still edit using notepad <path>\openssl.cnf) but it is a gotcha. It will save time if you add the basics to this file, such as the country code, email address and so on.
3. Create a new rui.key file as follows:
> openssl genrsa 1024 > rui.key
4. Generate a new certificate signing request at rui.csr as follows:
> openssl req -new -key rui.key > rui.csr -config openssl.cfg

The certificate request is now complete. You can open rui.csr in Notepad and copy the contents to the clipboard for the next stage.

;

If you want to place the files in another directory you can include the path (e.g. ../internal/rui.key) but you must use the Unix style forward slash not the Microsoft style backslash as the folder delimiter.

Microsoft specific information

If you use a Microsoft CA then you will probably need the following, which is taken from my MS CA:

1. Choose "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"
2. The certificate type is "Web Server (Exportable)"
3. When you download the certificate, make sure you choose the "base64 encoded" option (which is not the default)
4. I usually download both the certificate and the certificate chain

Generating the rui.pfx file

Save the certificates generated above, to the machine with OpenSSL, to the same folder as the rui.key and rui.csr files. Change the certificate name to rui.crt. Encode the certificate file as follows:

1. From the OpenSSL binary directory, run
`openssl pkcs12 -export -in rui.crt -inkey rui.key -name <common name of server> -out rui.pfx`
2. Note that you can use a relative path to use files in a different directory, as previously.

Installing the certificates

The files may now be copied to the server (VC or VM host). The default directories are (assuming the drive letter matches your ocnfig):

- For VirtualCenter: C:\Documents and Settings\All Users\Application Data\VMware\VMware VirtualCenter\SSL
- For ESX: etc/vmware/ssl/ - ensure you transfer in ASCII mode to convert Windows CR-LF terminators to Linux terminators, or the certificate will not work properly and you will be unable to attach to VC.
- For VMware Server: C:\Documents and Settings\All Users\Application Data\VMware\VMware Server\SSL

Remaining issues

Here's the biggie: when you replace the certificate on the VC server, you lose the virtual server connections. Experience to date indicates that if you reattach them, the VMs are fine, but I have only done this in the lab so have yet to run a structured test to check that all resource pools and folders remain intact with permissions unaffected.



[Steve Chambers](#) 213 posts since

May 31, 2008 1. **Re: Trusted SSL certificates - request for peer review** Nov 19, 2008 1:52 PM

I've posted an email internally @ VMware



[Steve Chambers](#) 213 posts since

May 31, 2008 2. **Re: Trusted SSL certificates - request for peer review** Nov 20, 2008 8:36 AM

Guy, When you finally create a proven practice doc out of this thread (Guy is getting peer review information from inside VMware) - we should link to these documents in the Resources section at the head of the doc:

Trusted SSL certificates - request for ...

;


Resources

- [Replacing VirtualCenter Server Certificates](#)
- [Enabling Server#Certificate Verification for Virtual Infrastructure Clients](#)
- [Replacing or Regenerating an SSL Certificate for the Management Interface](#)
- [Configuration Program vmware#config Might Set Incorrect Permissions on SSL Key Files](#)
- [Intermittent SSL Warnings Appear During Logoff](#)
- [Resetting the HTTP Session Timeout and Regenerating the SSL Certificate After Upgrading ESX Server](#)



[Rob Randell](#) 1 posts since

Jun 23, 2008 3. **Re: Trusted SSL certificates - request for peer review** Nov 21, 2008 3:12 PM

 in response to: [Steve Chambers](#)

I like it. Anything that can help here is a good thing as the current documentation has been considered lacking. Is there anyway to include screenshots in this? That would help to make the steps more clear I think.

;

BTW....here is the KB article for replacing VUM's SSL certs:

<http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&docType=kc&externalId=1004201388235>



[Steve Chambers](#) 213 posts since

May 31, 2008 4. **Re: Trusted SSL certificates - request for peer review** Nov 22, 2008 4:46 AM

It looks like Guy's original idea might be extended to VUM and Converter... suggestion: once this the proven practice for VC is done, someone can do the same for VUM and Converter? Perhaps those docs only need to be supplements (or even subsections) to the original VC doc?