Common Criteria Evaluated Configuration Guide for Citrix XenServer ® 6.0.2, Platinum Edition

Published Wednesday, 22 August 2012
3.0 Edition

Common Criteria Evaluated Configuration Guide for Citrix XenServer ® 6.0.2, Platinum Edition

Citrix, Inc.
851 West Cypress Creek Road
Fort Lauderdale, FL 33309
United States of America

Disclaimers

This document is furnished "AS IS." Citrix, Inc. disclaims all warranties regarding the contents of this document, including, but not limited to, implied warranties of merchantability and fitness for any particular purpose. This document may contain technical or other inaccuracies or typographical errors. Citrix, Inc. reserves the right to revise the information in this document at any time without notice. This document and the software described in this document constitute confidential information of Citrix, Inc. and its licensors, and are furnished under a license from Citrix, Inc.

Citrix Systems, Inc., the Citrix logo, Citrix XenServer and Citrix XenCenter are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the United States Patent and Trademark Office and in other countries. All other trademarks and registered trademarks are property of their respective owners.

Trademarks

Citrix®
XenServer ®
XenCenter ®

Published: 22 August 2012

Contents

Chapter 1. About this Guide

This Common Criteria Evaluated Configuration Guide for Citrix XenServer 6.0.2, Platinum Edition, describes the requirements and procedures for installing and configuring Citrix XenServer in accordance with the Common Criteria evaluated deployment.

If your security requirements and policies require you to deploy Citrix XenServer 6.0.2 to match the Common Criteria Target of Evaluation configuration, follow the procedures in this guide exactly.

Glossary

CA	X.509 Certification Authority, see RFC 5280
CC	Common Criteria
CLI	Command Line Interface
CN	Common Name, see RFC 5280
CSR	Certificate Signing Request, see PKCS#10
DNS	Domain Name System
EPT	Extended Page Tables
FQDN	Fully Qualified Domain Name
HCL	Hardware Compatibility List
IP	Internet Protocol
NFS	Network File System
NIC	Network Interface Controller
NTP	Network Time Protocol, see RFC 1305
PBD	Physical Block Device
PIF	Physical Interface
PXE	Preboot eXecution Environment
RPC	Remote Procedure Call
SAN	Subject Alternative Name, see RFC 5280
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SR	Storage Repository
ST	Security Target
SSL	Secure Socket Layer
UUID	Universally Unique Identifier

TOE	Target of Evaluation
VIF	Virtual Interface
VM	Virtual Machine
VT-x	Virtualization Technology for x86 Processors

References

[XS Install] *Citrix XenServer Installation Guide, 6.0*. 1.1 Edition.

[CTX LIC] *Citrix Licensing*. http://support.citrix.com/proddocs/topic/technologies/lic-library-node-wrapper.html .

[XS CC ST] *Common Criteria Security Target for Citrix XenServer ® 6.0.2, Platinum Edition CIN8-ST-0001*. Version 1.0.

[CC XS Admin] *Common Criteria Administrator's Guide for Citrix XenServer ® 6.0.2, Platinum Edition*. 1.0 Edition.

[XS Admin] *Citrix XenServer Administrator's Guide 6.0*. 1.1 Edition.

Chapter 2. Hardware

Important:

The hardware selected for use must be certified and supported for use with XenServer. Refer to the XenServer Hardware Compatibility List (*HCL*) at http://citrix.com/xenserver/cc-hcl for details. For Common Criteria purposes, the XenServer 6.0.2 HCL applies with the additional restriction that:

- Each server must contain at least 2 CPU cores.
- Only Intel 64-bit-capable CPUs with both VT-x and EPT capabilities are supported.
- Each server must contain at least 3 NICs.

2.1. Inventory

Servers
: At least 2, a maximum of 16, servers satisfying the limitations of the TOE as found in [XS CC ST].

Storage
: Network attached storage offering *NFS* storage, as defined in the TOE ([XS CC ST]).

Network
: Any network configuration within the limits of the TOE as found in [XS CC ST].

Note:

The host hardware configuration influences how the installed system will auto-configure. For the evaluated configuration, the hardware should be set up as follows:

- *NIC*0 - Management Network
- *NIC*1 - Storage Network
- *NIC*2 ... *NIC*N - One or more further *NIC*s must be added as required to create Guest Networks

2.2. Securing Hardware

The hardware must be secured as described in [XS CC ST] section Security Objectives for the Operational Environment, specifically OE.Secure_Resource, OE.Secure_Keys, OE.Separate_Networks.

Chapter 3. Software

The evaluated configuration as described in [XS CC ST] includes the XenCenter client as a management console, although XenCenter is not included in the TOE and is not relied upon to implement any security functions. When XenCenter is used as the client, the CC-specific version must be used (available on the CC ISO).

The standard version of XenCenter would provide notifications of updates that are not applicable to the XenServer CC version, which may cause an administrator to take it out of the Evaluated Configuration. The CC version of XenCenter does not provide these notifications. Users should monitor the Citrix Support site, http://support.citrix.com/6.0.2 [**URL to be confirmed**], for updates that are applicable specifically to the XenServer CC version.

3.1. Configuring XenCenter

The client used for the management of XenServer must verify presented SSL certificates.

To do this using Citrix XenCenter, execute the following procedure.

3.1.1. Initial Installation

Please refer to the steps in the section called “Installing XenCenter” ([XS Install]).

3.1.2. Post-Installation Configuration Procedures

1. On the **Tools** menu, select **Options**. This displays the Options dialog.
2. In the left hand pane, select **Security**.
3. Select the options **Warn me when a new SSL certificate is found** and **Warn me when an SSL certificate changes**.
4. Click **OK** to close the dialog.

> **Note:**
>
> If you use XenCenter for the Common Criteria configuration, it is possible to store your login credentials. The username and password for all managed servers can be stored between XenCenter sessions and used to automatically reconnect to them at the start of each new XenCenter session. To enable, in XenCenter on the “Tools” menu, select “Options”, then click “Save and Restore” and select the **Save and restore server connection state on startup** checkbox.
>
> In addition, when **Save and restore server connection state on startup** is enabled, you can protect the stored login credentials with a master password to ensure they remain secure. At the start of each session, you will be prompted to enter this master password before connections to your managed servers are automatically restored. To do this select the **Require a master** password checkbox.
>
> Administrators should follow their organization’s policies regarding storing passwords.

3.2. Configuring the Citrix License Server

The TOE as described in [XS CC ST] requires the use of a license server.

3.2.1. Initial Installation

For information on installing and configuring the Citrix License Server, please see [CTX LIC].

3.2.2. Post Installation Configuration Procedures

The evaluated configuration requires using the following ports:

Vendor Daemon Port	7279
License Server Manager Port	27000

3.3. Configuring Network Storage (NFS)

The evaluated configuration assumes that the *NFS* server uses the following standard ports:

RPC	111
NFS	2049
Lockd	26345
Statd	26346
Mountd	26347
Rquotad	26348

3.4. Configuring Network Time Protocol (NTP)

The evaluated configuration requires that the *NTP* server uses the standard port:

NTP	123

Chapter 4. Configuring a XenServer Host

This section describes the configuration steps that must be followed on each XenServer host.

Warning:

The evaluated configuration for a host will only be achieved once all of the following steps have been executed. The host *must not be made available for use* until the entire configuration has been completed.

Warning:

In the evaluated configuration, administrators must only use commands that are defined in the Common Criteria (CC) documentation, or in subsequent Citrix Knowledge Base articles that apply explicitly to the XenServer 6.0.2 CC configuration.

4.1. Before Installing XenServer

Before installing XenServer, verify the integrity of the downloaded ISO files by following the instructions in Chapter 1 of [del proc]

4.2. Installing XenServer

For the remainder of the installation procedure, refer to the steps in the section called “Installing the XenServer Host” ([XS Install]) and to [XS Admin], noting the following additional restrictions:

- Do not install any supplemental packs.
- Configure the host to use a static IP address.
- If your network does not have a DNS server, enter `127.0.0.1` when prompted for the IP address of a DNS server.

Note:

PXE booting XenServer installations, as described in Appendix C, *PXE Boot Installations* ([XS Install]) is not supported for the evaluated configuration.

4.3. Managing SSL Certificates

During XenServer host installation, a self-signed *SSL* certificate is installed. This must be replaced to fully comply with the requirements for a CC deployment as defined in [XS CC ST]. This section explains how to set up an SSL configuration. A configured X.509 Certification Authority (*CA*) is required for the steps in this section (see Appendix A, *Open SSL Configuration* for an example configuration suitable for use with OpenSSL).

Note:

When configuring a pool environment, these steps must be executed on all hosts.

4.3.1. Installing the Trusted CA Certificate

To Install the Trusted CA Certificate on a Host

1. Copy your trusted CA certificate to removable storage.
2. Mount the removable storage containing the certificate.
3. Install a CA certificate by entering the following commands on the host console.

```
# cd </path/to/directory/containing/certificate>
# xe pool-certificate-install filename=<ca_certificate_name.pem>
```

4. Unmount and remove the removable storage.

4.3.2. Generating Host Certificates

> **Note:**
>
> Keys used on the XenServer host must be generated in accordance with OE.Secure_Keys as defined in [XS CC ST].

When creating a Certificate Signing Request (*CSR*) it is also important to consider the following:

- Only a single Common Name (*CN*) entry is inspected during hostname validation.
- Only Subject Alternative Names (*SAN*) with type *DNS* are inspected during hostname validation.
- Hostname wildcards are not supported.
- The host IP address must be included in either CN or SAN.
- A Fully Qualified Domain Name (*FQDN*) can be provided in addition to the host IP address, however this is not essential.
- 127.0.0.1 must be included in either the CN or SAN.
- Allow a short period of time for xapi to be ready after performing `service xapi start`.

See Appendix A, *Open SSL Configuration* for an example using OpenSSL.

To Install the SSL Certificate on a Host

1. Copy your trusted CA certificate to removable storage.
2. Mount the removable storage media containing the certificate.
3. Enter the following commands on the host console:

```
# service xapi stop
# pkill stunnel
# cp /etc/xensource/xapi-ssl.pem /etc/xensource/orig-xapi-ssl.pem
# cp </path/to/new/cert.pem> /etc/xensource/xapi-ssl.pem
# service xapi start
```

4. Unmount and remove the removable storage.

4.4. Creating a XenServer Pool

XenServer resource pools can be created using either the XenCenter management console or the CLI. When you join a new host to a resource pool, the joining host synchronizes its local database with the pool-wide one, and inherits some settings from the pool. For more information on resource pools, refer to the chapter called "XenServer Hosts and Resource Pools" ([XS Admin]).

Before creating a XenServer Pool, choose one of the hosts to be the initial pool master. There are no special requirements for choosing the pool master. Once you have selected the pool master, join all the remaining hosts (which will be pool slaves) to the master using the following procedure.

To Join XenServer Host *slave1* to *master* Using CLI

1. Open a console on XenServer host *slave1*.
2. Configure the XenServer *slave1* host to act as a slave of Pool Master *master* by entering the following on the console:

```
xe pool-join master-address=<master-ip-address> master-username=root \
  master-password=<password>
```

The *`master-address`* must be set to the fully-qualified domain name or IP address of the XenServer host *master* and the *`password`* must be the password set when XenServer host *master* was installed.

To Name the Resource Pool

- By default, XenServer hosts belong to an unnamed pool. To name the resource pool, enter the following command:

```
# xe pool-list params=uuid minimal=true
<pool_uuid>
xe pool-param-set name-label=<"New Pool"> uuid=<pool_uuid>
```

4.5. Network Configuration

The TOE requires the use of separate networks for management, storage and guest traffic. Guests must only ever be connected to the Guest Networks. This ensures that proper separation is maintained and that VIFs are only created on the Guest Network. Under no circumstance must a Guest ever be connected to either the Management Network or the Storage Network. As dom0 does not need VIFs to access the Management and Storage networks, no VIFs should ever be defined for them. Refer to [CC XS Admin] for further information on configuring networking on XenServer and to the section Security Problem Definition in [XS CC ST], specifically A.Separate_Networks.

4.5.1. Configuring the Storage Network

> **Note:**
>
> The following steps for configuring the Storage Network must be performed on **ALL** hosts, including the Pool Master.

To configure the Storage Network:

1. Find the *UUID* of the host:

```
# xe host-list name-label=<host name> params=uuid
uuid ( RO): <host uuid>
```

2. Find the UUID of the *PIF* related to device `eth1` (*NIC1*) and the *UUID* of its network:

```
# xe pif-list device=eth1 host-uuid=<host uuid> params=uuid
uuid ( RO): <pif uuid>
```

3. Configure the Storage Network *IP* address:

```
# xe pif-reconfigure-ip uuid=<pif uuid> mode=static IP=<ip> netmask=<netmask>
```

4. Set the PIF to be permanently attached:

```
# xe pif-param-set uuid=<pif uuid> disallow-unplug=true
```

4.6. Storage Configuration

The TOE allows only two types of Storage Repository (SR): read-only ISO on NFS or VHD on NFS. For more information about ISO on NFS SRs, see Section 4.2.4, “ISO SRs” ([XS Admin]). For more information about VHD on NFS SRs, see Section 4.2.9, “NFS VHD SRs”([XS Admin]).

> **Note:**
>
> These steps must be executed *only* on the Pool Master's console.

4.6.1. Adding a VHD on NFS SR

1. To add a VHD on *NFS SR* at *<ip>*:*<path>* enter the following command:

```
# xe sr-create name-label="<name>" shared=true device-config:server=<ip> \
     device-config:serverpath=<path> type=nfs
```

This returns the *`sr-uuid`*.

2. Repeat the command for all subsequent *NFS SR*s that should be available to the pool.

4.6.2. Registering a Default SR

After adding all the *NFS SR*s, choose one *<sr-uuid>* and make it the default *SR*:

```
# xe pool-list params=uuid minimal=true
<pool_uuid>
# xe pool-param-set uuid=<pool_uuid> default-SR=<sr_uuid> \
     suspend-image-SR=<sr_uuid> crash-dump-SR=<sr_uuid>
```

4.6.3. Adding an ISO on NFS SR

1. To add an ISO on NFS SR at *<ip>*:*<path>* enter the following command:

   ```
   # xe sr-create name-label="<name>" shared=true type=iso \
       device-config:location=<ip:path> content-type=iso
   ```

   This returns the `sr-uuid`.

2. Repeat the command for all subsequent ISO on NFS SRs that should be available to the pool.

Appendix A. Open SSL Configuration

Following is an example of a configuration file for use with OpenSSL (version 1.0.0) that would create a *CSR* which satisfies the requirements XenServer has on certificates. Before using it, please ensure that this file complies with your organisational security policy.

Example A.1. OpenSSL Configuration

```
HOME        = .
oid_section = new_oids

[ new_oids ]

[ req ]
default_days       = 365
default_keyfile    = ./new_key.pem
default_bits       = 2048
distinguished_name = req_distinguished_name
encrypt_key        = no
string_mask        = nombstr
req_extensions     = v3_req

[ req_distinguished_name ]
CN           = 10.80.2.63
C            = GB
O            = MyFirm Ltd
OU           = Technical Support
emailAddress = my.email@address.myfirm.co.uk

[ v3_req ]
subjectAltName= @alt_names

[ alt_names ]
DNS.1 = 127.0.0.1
```

Appendix B. Firewall Configuration

By default, a restrictive firewall is configured during Common Criteria XenServer host installation. Details of the ports used can be found in the sections that follow.

B.1. Management Network Firewall

The ports that are used on the Management Network in the TOE as defined in [XS CC ST]:

Service	Port	Protocol	Direction
HTTPS	443	tcp	both
Ping	N/A	icmp (echo-request)	both
Licensing	7279	tcp	out
Licensing	27000	tcp	out
NTP	123	udp	out
DNS	53	tcp	out
DNS	53	udp	out

B.2. Storage Network Firewall

The ports that are used on the Storage Network in the TOE as defined in [XS CC ST]:

Service	Port	Protocol	Direction
Ping	N/A	icmp (echo-request)	both
DNS	53	tcp	out
DNS	53	udp	out
NFS	111	tcp & udp	out
NFS	2049	tcp & udp	out
NFS	26345-26348	tcp & udp	out

B.3. Guest Network Firewall

The Guest Network is solely used by the Guest VMs and the firewall does not require configuration.