Common Criteria Evaluated Configuration Guide for Citrix XenServer ® 7.1 LTSR Enterprise Edition

Published March 2019
1.0 Edition

Common Criteria Evaluated Configuration Guide for Citrix XenServer ® 7.1 LTSR Enterprise Edition

Version: 7.1

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, the Citrix logo, Citrix XenServer and Citrix XenCenter, and other trademarks appearing herein are the property of Citrix Systems, Inc, 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 ®

Contents

Chapter 1. Introduction

This *Common Criteria Evaluated Configuration Guide (CCECG) for Citrix XenServer 7.1 LTSR Enterprise Edition* describes the requirements and procedures for installing and configuring Citrix XenServer 7.1 LTSR Enterprise Edition in accordance with the Common Criteria evaluated deployment.

If your security requirements and policies require you to deploy Citrix XenServer 7.1 LTSR Enterprise Edition to match the Common Criteria Target of Evaluation configuration, follow the procedures in this guide.

The Common Criteria Evaluated Configuration Guide must be used in conjunction with the *XenServer 7.1 Administrator's Guide* [XS Admin]. In scenarios where *XS Admin* contains information that conflicts with information in this guide, you must use the information documented in this guide to maintain a XenServer host within the Common Criteria TOE.

> **Important:**
>
> Using features that are not part of the XenServer Common Criteria TOE or modifying any default settings that are not covered in the [CCECG] can take your deployment out of the evaluated configuration. For a list of features that are not included in the Common Criteria TOE, see Appendix A, *Features not Included in the Evaluated Configuration*.

1.1. Documentation

In addition to the CCECG, you must refer to the following documents for information when deploying XenServer in the TOE configuration.

- *Common Criteria Security Target for Citrix XenServer 7.1 LTSR Enterprise Edition* [XS CC ST] describes the TOE and details assumptions such as the physical environment used and associated roles. The [XS CC ST] also lists the major features of the TOE and the evaluation requirements.
- *Common Criteria Configuration Management for Citrix XenServer 7.1 LTSR Enterprise Edition* [XS CC CM] lists the configuration items and parts comprising Citrix XenServer 7.1 LTSR Enterprise Edition
- *Common Criteria Delivery Procedures Citrix XenServer 7.1 LTSR Enterprise Edition* [XS CC DP] contains information on how to download XenServer 7.1 LTSR Enterprise Edition and ensure the integrity and authenticity of the downloads.
- *XenServer 7.1 Administrator's Guide* [XS Admin] for in-depth information about XenServer deployment, including setting up storage, networking and pools.

  Note that in scenarios where *XS Admin* contains information that conflicts with information in this guide, you must use the information documented in this guide to maintain a XenServer host within the Common Criteria TOE.
- *XenServer 7.1 Installation* [XS Install] for information about installing XenServer and initial operation of XenServer and the XenCenter management console.
- *Citrix Licensing* [CTX LIC] for information about Licensing your XenServer hosts.

Common Criteria documents for *Citrix XenServer 7.1 LTSR Enterprise Edition* are available to download from the Citrix Common Criteria Certification Information page in the *Related Documents* section.

XenServer 7.1 LTSR Product documentation is available on the XenServer 7.1 LTSR product documentation page.

For information about licensing, see Citrix Licensing.

1.2. 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
OCF	Open Container Format
P2V	Physical-to-Virtual
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
SNMP	Simple Network Management Protocol
SR	Storage Repository
SR-IOV	Single Root I/O Virtualization
ST	Security Target
SSL	Secure Socket Layer
UUID	Universally Unique Identifier
TOE	Target of Evaluation
V2V	Virtual-to-Virutal
VIF	Virtual Interface
VM	Virtual Machine

VT-x	Virtualization Technology for x86 Processors

1.3. Documentation References

- [XS CC ST] - *Common Criteria Security Target for Citrix XenServer ® 7.1 LTSR Enterprise Edition CIN8-ST-0001*
- [XS CC DP] - *Common Criteria Delivery Procedures for Citrix XenServer ® 7.1 LTSR Enterprise Edition*
- [XS Install] - *Citrix XenServer 7.1 Installation Guide*
- [XS VM] - *Citrix XenServer 7.1 VM User's Guide*
- [XS Admin] - *Citrix XenServer 7.1 Administrator's Guide*
- [CTX LIC] - *Citrix Licensing*

Chapter 2. Hardware

Important:

The hardware selected for use must be certified and supported for use with XenServer. For Common Criteria purposes, the XenServer HCL applies with the additional restriction that:

- Each server must contain at least 2 CPU cores (Intel Xeon Processor E5 family).
- Only Intel 64-bit-capable CPUs with both VT-x and EPT capabilities are supported.
- Each server must contain at least 3 NICs.
- Customers must disable Simultaneous multithreading (SMT) or hyper-threading in XenServer. Hyper-threading is not supported in the CC evaluated configuration. For information about managing SMT (hyper-threading) in XenServer, see https://support.citrix.com/article/CTX237190.

2.1. Inventory

Storage

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

Network

Any network configuration within the limits of the TOE as defined 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] in the *Security Objectives for the Operational Environment* section. For specific details, refer to *OE.Secure_Resource, OE.Separate_Networks*.

Chapter 3. Software

The evaluated configuration as described in [XS CC ST] includes the XenCenter client as a management console. However, XenCenter is not included in the TOE and is not relied upon to implement any security functions.

> **Note:**
>
> When using XenCenter or an alternative XenAPI client, you must ensure that the usernames, passwords, and session tokens are handled in accordance with the industry best practices.

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. If you are using an alternative XenAPI client, ensure you have validated the SSL certificates.

3.1.1. Initial Installation

See the section *Installing XenCenter* in [XS Install] for instructions on installing XenCenter.

3.1.2. Post-Installation Configuration Procedures

1. In XenCenter, select **Tools** and then **Options**. This displays the Options dialog.
2. In the left hand pane, click **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**.

3.1.2.1. Storing your login credentials

If you use XenCenter for the Common Criteria configuration, it is possible to store your login credentials. The user name 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 this in XenCenter:

1. On the **Tools** menu, select **Options**. This displays the Options dialog.
2. In the left hand pane, click **Save and Restore**.
3. Select the **Save and restore server connection state on startup** check box.

   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.
4. To enable the master password, select the **Require a master password** check box.

> **Note:**
>
> You must follow your 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, see Citrix Licensing.

3.2.2. Post Installation Configuration Procedures

XenServer requires using the following ports:

Vendor Daemon Port	7279
License Server Manager Port	27000

3.3. Configuring Network Storage (NFS)

XenServer assumes that the *NFS* server uses the following standard ports:

RPC	111	TCP, UDP
NFS	2049	TCP, UDP
Lockd	4045	TCP, UDP
Statd	4047	TCP, UDP
Mountd	4046	TCP, UDP
Rquotad	4049	TCP, UDP

3.4. Configuring Network Time Protocol (NTP)

XenServer requires that the *NTP* server uses the standard port:

NTP	123	UDP

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 when 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 7.1 LTSR Enterprise Edition CC configuration.

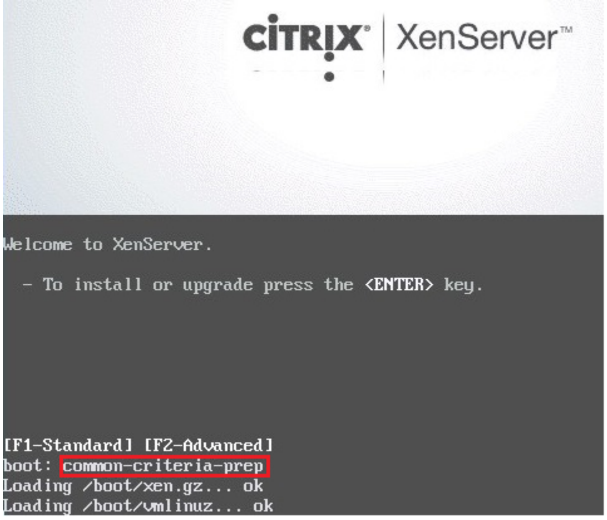
4.1. Before Installing XenServer

Before installing XenServer, verify the integrity of the downloaded ISO files by following the instructions in Chapter 1 of [XS CC DP]

4.2. Installing XenServer in CC Mode

For the remainder of the installation procedure, refer to the section *Installing the XenServer host* in [XS Install] and [XS Admin].

When you launch the XenServer installer, you must type **common-criteria-prep** at the boot prompt to install XenServer in the Common Criteria mode.



```
Welcome to XenServer.

  - To install or upgrade press the <ENTER> key.



[F1-Standard] [F2-Advanced]
boot: common-criteria-prep
Loading /boot/xen.gz... ok
Loading /boot/vmlinuz... ok
```

In addition, you must note the following restrictions to install XenServer in the common criteria mode:

- 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* in [XS Install] is not supported for the evaluated configuration.

4.3. Users on XenServer Hosts

After installation, only a single user account is available on the XenServer host `root`. As defined in the TOE in [XS CC ST], you must not create any other accounts on the XenServer host.

4.4. Network Configuration

Linux Bridge is the default network stack and the only supported network stack in the XenServer Common Criteria evaluated configuration.

The networks on the first three Network Interface Cards (PIFs 0, 1, and 2) are labelled **Management Network**, **Storage Network**, and **Guest Network** respectively. PIF 2 (for guest network 0) is configured **not** to have an IP address.

The TOE requires the use of separate networks for Management, Storage, and Guest traffic. To ensure that proper separation is maintained, VMs must only be placed on the Guest networks (that is, VIFs must only be created on a Guest network). You must not create any VIFs on the Storage or the Management network. That is, do not place any VMs on the Management or the Storage network .

A restrictive firewall is configured and enabled in dom0. As the dom0 does not require VIFs to access the Management Network or the Storage Network, you must not create any VIFs on the Storage or the Management network. That is, do not place any VMs on the Management or the Storage network.

Refer to [XS Admin] for further information on configuring networking on XenServer and to *A.Separate_Networks* in the section *Security Problem Definition* in [XS CC ST].

4.4.1. 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
   ```

4.5. Storage Configuration

The TOE allows VHD on NFS and local EXT3 SRs as defined in the [XS CC ST]. The writeable ISO storage repository falls outside of the TOE. For more information about *VHD on NFS SRs*, see the section *Storage Repository Formats* in [XS Admin].

> **Note:**
>
> You must execute these steps *only* on the Pool Master's console.

Local SRs are not created on installation. In a manual installation the user is no longer given the option. Note that removable SRs are not created on installation.

4.5.1. 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.

4.5.2. 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>
```

4.5.3. 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.

4.5.4. Probing an SR

The **sr-probe** command can be used in two ways:

- To identify unknown parameters for use in creating an SR.
- To return a list of existing SRs.

In both cases **sr-probe** works by specifying an SR type and one or more `device-config` parameters for that SR type. When an incomplete set of parameters is supplied, the **sr-probe** command returns an error message indicating parameters are missing and the possible options for the missing parameters. When a complete set of parameters is supplied a list of existing SRs is returned. All **sr-probe** output is returned as XML.

A known NFS server can be probed by specifying its name or IP address, and the set of NFS exported paths on the server will be returned. For example:

```
xe sr-probe type=nfs device-config:server=10.0.0.3

Error code: SR_BACKEND_FAILURE_101
Error parameters: , The request is missing the serverpath parameter, <?xml version="1.0"?>
<nfs-exports>
    <Export>
        <Target>
            10.0.0.3
        </Target>
        <Path>
            /vol/abc
        </Path>
        <Accesslist>
            (everyone)
        </Accesslist>
    </Export>
    <Export>
        <Target>
            10.0.0.3
        </Target>
        <Path>
            /vol/foo
        </Path>
        <Accesslist>
            (everyone)
        </Accesslist>
    </Export>
</nfs-exports>>
```

Probing the same server again, specifying both the name/IP address and the desired path, will return a list of the SRs that exist on that exported path, if any:

```
xe sr-probe type=nfs device-config:server=10.0.0.3 device-config:serverpath=/vol/abc

<?xml version="1.0"?>
<SRlist>
    <SR>
        <UUID>
            0aeb8aef-0bec-79dd-5ebd-c4565ec3dfd1
        </UUID>
    </SR>
    <SR>
        <UUID>
            713d1547-1870-45f5-365b-03cd9bf4f271
        </UUID>
    </SR>
</SRlist>
```

The following parameters can be probed for each supported SR type:

SR type	device-config parameter, in order of dependency	Can be probed?	Required for sr-create?
nfs	server	No	Yes
	serverpath	Yes	Yes

4.6. 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 C, *SSL Configuration* for an example configuration suitable for use with OpenSSL). Certificates with 2048-bit RSA keys are supported

> **Note:**
>
> When configuring a pool environment, the following steps must be executed on all hosts in the pool. Because XAPI is restarted during these configuration changes, perform them over a non-XAPI connection, such as the machine console.

4.6.1. 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.

4.6.2. 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*) you must consider the following:

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

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

To Install the SSL Certificate on a Host

1. Copy the SSL 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.

4.7. Creating a XenServer Resource 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, see *XenServer Hosts and Resource Pools* in [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. After you have selected the pool master, join all the remaining hosts (which will be pool members) to the pool using the following procedure.

To Join XenServer host *host1* to a resource pool using CLI

1. Open a console on *host1*.
2. Configure *host1* to join the pool by entering the following command 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

- XenServer hosts belong to an unnamed pool by default. 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>
```

4.8. Removing a XenServer Host from a Resource Pool

When a XenServer host is removed (*ejected*) from a pool, the machine is rebooted, reinitialized, and left in a state equivalent to that after a fresh installation.

To remove a host from a resource pool using the CLI

1. Open a console on any host in the pool.
2. Find the UUID of the host to be removed by running the command:

```
xe host-list
```

3. Eject the required host from the pool:

```
xe pool-eject host-uuid=<host_uuid>
```

4. You must then use a suitable tool to securely erase the contents of the hard disk.

4.9. Preparing a Pool of XenServer Hosts for Maintenance

Before performing maintenance operations on a XenServer host that is part of a resource pool, you should disable it. This prevents any VMs from being started on it. Move its VMs to another XenServer host in the pool by shutting them down, then starting them on another host.

> **Note:**
>
> Placing the master host into maintenance mode will result in the loss of the last 24 hours of Round Robin Database (RRD) updates for offline VMs. This is because the backup synchronization occurs every 24 hours.

> **Warning:**
>
> Citrix highly recommends rebooting all XenServer hosts prior to installing an update, then verifying their configuration. This is because some configuration changes only take effect

when a XenServer is rebooted, so the reboot may uncover configuration problems that would cause the update to fail.

To prepare a XenServer host in a pool for maintenance operations using the CLI

1. Run the command:

   ```
   xe host-disable uuid=<host_uuid>
   ```

   This will disable the XenServer host.
2. Shut down any VMs that are running on the host. If possible, restart the VMs on another host.
3. Perform the desired maintenance operation.
4. Once the maintenance operation is completed, enable the XenServer host:

   ```
   xe host-enable uuid=<host_uuid>
   ```
5. Restart any halted VMs.

4.10. Coping with Machine Failures

Warning:

After executing the command `xe host-forget`, you must use a suitable tool to erase the contents of hard disk of the XenServer host. After this, the XenServer host is left in a state where a fresh install can happen.

Warning:

When a non-fatal failure has occurred, the master must be power cycled before a new master is chosen. This is to ensure that there is no risk of disk corruption due to several instances of the same VM running at the same time.

Chapter 5. Creating VMs

This section contains notes on creating VMs which should be read in conjunction with [XS VM].

5.1. Types of Guests Supported

Only HVM (Windows and Linux) guests are supported for this Common Criteria evaluated configuration. PV guests are not included in the evaluated configuration under this Security Target.

> **Important:**
>
> Administrators must be careful when importing VMs and Virtual Appliances. You must verify that imported VMs do not take the XenServer hosts out of the evaluated configuration. (For example, a Virtual Appliance may contain a PV guest).

To check if there are any currently running PV guests, on the console of each XenServer host in the pool, run the following command:

```
for i in $(list_domains | grep -Ev '^ *0|^id|H$' | cut -f2 -d'|');   \
    do xe vm-list uuid=$i; done
```

To list all guests, both running and stopped, that will be PV when next booted. On the console of each XenServer host in the pool, run the following command:

```
xe vm-list HVM-boot-policy='BIOS order' | diff - <(xe vm-list is-control-domain=false)
```

5.2. Guest Security

The security of software running in a domU Guest (VM) remains the responsibility of the user and/or administrator of the guest (for example, to maintain appropriate patch states for software and virus protection within the domain).

5.3. SR-IOV

Although SR-IOV capable hardware may be used in the TOE (subject to it being supported in the Citrix XenServer Hardware Compatibility List), the SR-IOV specific functionality should not be enabled in a Common Criteria environment. To list any VMs that have SR-IOV configured, run the following bash script:

```
for vm in $(xe vm-list params=uuid | sed 's/^.*://'); do
xe vm-param-get uuid=$vm param-name=other-config param-key=pci 2>/dev/null  \
    && echo "FOUND A PCI SETTING for vm $vm" && echo
done
```

5.3.1. GPU Pass-through (and Virtual GPU)

GPU Pass through functionality, including any virtual GPU features must not be enabled in a Common Criteria environment. Run the `vgpu-list` command to confirm it is not enabled. This command returns an empty list if GPU Pass-thru is not enabled.

```
xe vgpu-list
```

5.4. Virtual Appliances

The following virtual appliances that are supplied with XenServer Enterprise Edition fall outside of the TOE as defined in [XS CC ST] and must not be installed or used within the evaluated configuration: Citrix License Server virtual appliance, Workload Balancing virtual appliance, XenServer Conversion Manager, and vSwitch Controller virtual appliance.

Chapter 6. VM Memory

The following sections contain information about viewing and updating the memory properties of a VM.

6.1. Display the Static Memory Properties of a VM

Perform the following steps to display the static memory properties of a VM:

1. Find the uuid of the required VM:

   ```
   xe vm-list
   ```

2. Note the uuid, then run the command **param-name=memory-static**:

   ```
   xe vm-param-get uuid=<uuid> param-name=memory-static-{min,max}
   ```

   For example, the following displays the static maximum memory properties for the VM with the uuid beginning ec77:

   ```
   xe vm-param-get uuid= \
       ec77a893-bff2-aa5c-7ef2-9c3acf0f83c0 \
       param-name=memory-static-max;
       268435456
   ```

   This shows that the static maximum memory for this VM is 268435456 bytes (256MB).

6.2. Display the Dynamic Memory Properties of a VM

To display the dynamic memory properties, follow the procedure as above but use the command **param-name=memory-dynamic**:

1. Find the uuid of the required VM:

   ```
   xe vm-list
   ```

2. Note the uuid, then run the command **param-name=memory-dynamic**:

   ```
   xe vm-param-get uuid=<uuid> param-name=memory-dynamic-{min,max}
   ```

   For example, the following displays the dynamic maximum memory properties for the VM with uuid beginning ec77

   ```
   xe vm-param-get uuid= \
       ec77a893-bff2-aa5c-7ef2-9c3acf0f83c0 \
       param-name=memory-dynamic-max;
       134217728
   ```

   This shows that the dynamic maximum memory for this VM is 134217728 bytes (128MB).

6.3. Updating Memory Properties

Warning:

In the Common Criteria configuration, Dynamic Memory Control (DMC) is outside of the TOE as defined in [XS CC ST] and, as such, care must be taken when altering VM memory settings. For more information, see XS Admin. In particular, you should always ensure the following constraint is maintained:

```
0 ≤ memory-static-min ≤ memory-dynamic-min = memory-dynamic-
max = memory-static-max
```

In the following command, 0 ≤ value1 ≤ value2.

Update all memory limits (static and dynamic) of a virtual machine:

```
xe vm-memory-limits-set \
    uuid=<uuid> \
    static-min=<value1> \
    static-max=<value2>
    dynamic-min=<value2> \
    dynamic-max=<value2>
```

> **Warning:**
>
> Citrix advises not to change the static minimum level *<value1>* in the command above, as this is set at the supported level per operating system. Refer to the memory constraints table in XS Admin for more information.

Chapter 7. Non-CC-certified Product Updates

Citrix will, from time to time, issue product updates which may correct flaws in the underlying software. Administrators should check with Citrix on a regular basis for these updates. Administrators may also opt to subscribe to proactive email alerts concerning product security vulnerabilities and their associated fixes. These alerts are sent out on a regular basis whenever new fixes are available. Administrators may contact and work with Citrix Support directly if they require additional support in obtaining and deploying any fix. More information about the email alerts system can be found at http://www.citrix.com.

In the event that an update is issued which corrects a critical flaw, but which has not yet been Common Criteria (CC) certified, the administrator should analyze the corrected flaw and the TOE's vulnerability to it when determining whether or not to install the non-CC certified update.

Appendix A. Features not Included in the Evaluated Configuration

Important:

The following table lists features that are NOT included in the CC evaluated configuration. Using any of the features listed below will take your XenServer deployment out of the evaluated configuration. For more information about the features included in the CC evaluated configuration, see [XS CC ST].

Feature
PV guests
Heterogeneous Resource Pools
Active Directory Integration
Role Based Access Control (RBAC)
Host UEFI Boot
SMB Storage
Software FCoE Storage
Software-boot-fromiSCSI
Intellicache
vSwitch
Live migration with XenMotion
Storage XenMotion
Live Memory Checkpoint (Snapshots)
Cross-Server Private Networks
Dynamic Memory Control (Ballooning)
High Availability
SNMP *
GPU pass-through
Disaster Recovery
Health Check
PVS Accelerator
Dynamic Workload Balancing & Audit Reporting (WLB)
Distributed Virtual Switch Controller (DVSC)

Feature
XenServer Conversion Manager
Docker Container Management
Direct Inspect APIs
GPU Virtualization
vGPU XenMotion
SMT (hyper-threading)

*In the common criteria evaluated configuration, SNMP is turned off and is further prevented by firewall rules used by dom0 when routing network packets.

Appendix B. Additional CC Configuration Information

B.1. P2V and V2V Tools

P2V and V2V tools and OCF support must not be enabled in the CC evaluated configuration.

B.2. Live Migration, XenMotion

The TOE as defined in [XS CCST] does not include live migration (XenMotion). It is not possible to disable this feature in XenServer and, therefore, it is necessary that everyone with administrator access to the XenServer pool is thus informed.

B.3. SNMP

By default, SNMP is not enabled in the Common Criteria configuration and must not be enabled.

B.4. Security

The pool secret is generated from `/dev/random` for maximum randomness.

The ssh daemon in dom0 is installed, but is not activated.

SSL certificate verification is activated.

Appendix C. SSL Configuration

C.1. OpenSSL Configuration

Following is an example of a configuration file for use with OpenSSL 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 C.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
DNS.2 = 10.80.2.63
```

Appendix D. 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.

D.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
SSH	22	TCP	out

D.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	4045 4046 4047 4049	TCP & UDP	out

D.3. Guest Network Firewall

The Guest Network is solely used by the VMs. Therefore, the firewall blocks any traffic to and from the XenServer host control domain.