Common Criteria Evaluated Configuration Guide for Citrix Hypervisor 8.2 Cumulative Update 1 Premium Edition [CH CCECG]

July 25, 2022

1.5 Edition

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 Hypervisor 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®
- Xen®
- XenCenter®

Table of contents

Introduction

This *Common Criteria Evaluated Configuration Guide (CCECG) for Citrix Hypervisor 8.2 Cumulative Update 1 Premium Edition* describes the requirements and procedures for installing and configuring Citrix Hypervisor 8.2 Cumulative Update 1 Premium Edition in accordance with the Common Criteria evaluated deployment.

If your security requirements and policies require you to deploy Citrix Hypervisor 8.2 Cumulative Update 1 Premium 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 *Citrix Hypervisor 8.2 Cumulative Update 1 product documentation*. Where the product documentation contains information that conflicts with the information in this guide, you must use the information documented in this guide to maintain a Citrix Hypervisor host within the Common Criteria TOE.

> **Important:**
>
> Using features that are not part of the Citrix Hypervisor Common Criteria TOE or modifying any default settings that are not covered in the Common Criteria Evaluated Configuration Guide can take your deployment out of the evaluated configuration. For a list of features that are not included in the Common Criteria TOE, see Features not included in the Evaluated Configuration.

Documentation

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

- *Common Criteria Security Target for Citrix Hypervisor 8.2 Cumulative Update 1 Premium Edition* [CH CC ST] describes the TOE and details assumptions such as the physical environment used and associated roles. The [CH CC ST] also lists the major features of the TOE and the evaluation requirements.
- *Common Criteria Configuration Management for Citrix Hypervisor 8.2 Cumulative Update 1 Premium Edition* [CH CC CM] lists the configuration items and parts comprising Citrix Hypervisor 8.2 Cumulative Update 1 Premium Edition
- *Common Criteria Delivery Procedures Citrix Hypervisor 8.2 Cumulative Update 1 Premium Edition* [CH CC DP] contains information on how to download Citrix Hypervisor 8.2 Cumulative Update 1 Premium Edition and ensure the integrity and authenticity of the downloads.
- *Citrix Hypervisor 8.2 Cumulative Update 1 product documentation* [CHPD] for in-depth information about Citrix Hypervisor deployment, including installation, licensing, initial operation, and setting up storage, networking, and pools.

  Where the product documentation conflicts with the information in this guide, use the information documented in this guide to maintain a Citrix Hypervisor server within the Common Criteria TOE.

Common Criteria documents for Citrix Hypervisor 8.2 Cumulative Update 1 Premium Edition are available to download from the Citrix Common Criteria Certification Information page in the *Related Documents* section.

Citrix Hypervisor 8.2 product documentation is available on the Citrix Hypervisor 8.2 Cumulative Update 1 product documentation page.

For information about licensing, see Citrix Licensing.

Glossary

Term	Definition
BIOS	Basic Input/Output System
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
EXT4	Fourth Extended Filesystem
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
RPC	Remote Procedure Call
SAN	Subject Alternative Name, see RFC 5280
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol

Term	Definition
SR	Storage Repository
SR-IOV	Single Root I/O Virtualization
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
UEFI	Unified Extensible Firmware Interface
UUID	Universally Unique Identifier
V2V	Virtual-to-Virtual
VIF	Virtual Interface
VM	Virtual Machine
VT-x	Virtualization Technology for x86 Processors

Documentation References

- [CH CC ST] - Common Criteria Security Target for Citrix Hypervisor 8.2 Cumulative Update 1 Premium Edition
- [CH CC CM] - Common Criteria Configuration Management for Citrix Hypervisor 8.2 Cumulative Update 1 Premium Edition
- [CH CC DP] - Common Criteria Delivery Procedures for Citrix Hypervisor 8.2 Cumulative Update 1 Premium Edition
- [CHPD] - Citrix Hypervisor 8.2 product documentation
- [CTX LIC] - Citrix Licensing

Hardware

Important:

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

- Only Intel 64-bit-capable CPUs with both VT-x and EPT capabilities are supported.
- Each server must contain at least 2 CPU cores from the 2nd Generation Intel® Xeon® Scalable Processors family (Intel Xeon 82xx/62xx/52xx/42xx/32xx).
- Your hardware must be in security support from your OEM.
- Each server must contain at least 3 network interfaces.
- Customers must disable Simultaneous multithreading (SMT) or hyper-threading in Citrix Hypervisor. Hyper-threading is not supported in the CC evaluated configuration. For information about managing SMT (hyper-threading) in Citrix Hypervisor, see https://support.citrix.com/article/CTX237190.

Inventory

- **Storage:** Network attached storage offering NFS storage, as defined in the TOE in [CH CC ST].
- **Network:** Any network configuration within the limits of the TOE as defined in [CH CC ST].

Note:

The host hardware configuration influences how the installed system auto-configures. 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

Securing Hardware

The hardware must be secured as described in [CH CC ST] in the *Security Objectives for the Operational Environment* section. For specific details, refer to *OE.Secure_Resource, OE.Separate_Networks*.

Software

The evaluated configuration as described in [CH 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 user names, passwords, and session tokens are handled in accordance with the industry best practices.

Configuring XenCenter

The client used to manage Citrix Hypervisor servers and pools must verify the presented TLS certificates.

To do this using Citrix XenCenter, complete the following procedure. If you are using an alternative XenAPI client, ensure you have validated the TLS certificates.

Initial Installation

For instructions on installing XenCenter, see the section *Installing XenCenter* in the Citrix Hypervisor 8.2 Cumulative Update 1 product documentation.

Post-Installation Configuration Procedures

1. In XenCenter, select **Tools** and then **Options**. This action displays the **Options** dialog.

2. In the left hand pane, click **Security**.

3. Select the options **Warn me when a new TLS certificate is found** and **Warn me when an TLS certificate changes**.

4. Click **OK**.

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 at the start of each new XenCenter session.

To enable credential storing in XenCenter:

1. On the **Tools** menu, select **Options**. This action 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.

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 are 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:**
>
> Follow your organization's policies regarding storing passwords.

Configuring the Citrix License Server

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

Initial Installation

For information on installing and configuring the Citrix License Server, see Citrix Licensing.

Post Installation Configuration Procedures

Citrix Hypervisor requires using the following ports:

Purpose	Port
Vendor Daemon Port	7279
License Server Manager Port	27000

Configuring Network Storage (NFS)

Citrix Hypervisor assumes that the NFS server uses the following standard ports:

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

Configuring Network Time Protocol (NTP)

Citrix Hypervisor requires that the *NTP* server uses the standard port:

Purpose	Port	UDP or TCP

Purpose	Port	UDP or TCP
NTP	123	UDP

Configuring a Citrix Hypervisor server

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

> **Warnings:**
>
> The evaluated configuration for a server is only achieved when all the following steps have been run. Do not use the server until the entire configuration has been completed.
>
> In the evaluated configuration, only use commands that are defined in the Common Criteria (CC) documentation or in Citrix Knowledge Base articles that apply explicitly to the Citrix Hypervisor 8.2 Cumulative Update 1 Premium Edition CC configuration.

Before installing Citrix Hypervisor

Before installing Citrix Hypervisor, verify the integrity of the downloaded ISO files by comparing the SHA-256 checksum of the downloaded file to the checksum listed on the Citrix Hypervisor download site.

On Linux, you can run the following command:

```
sha256sum <filename>
```

On Windows, you can run the following command:

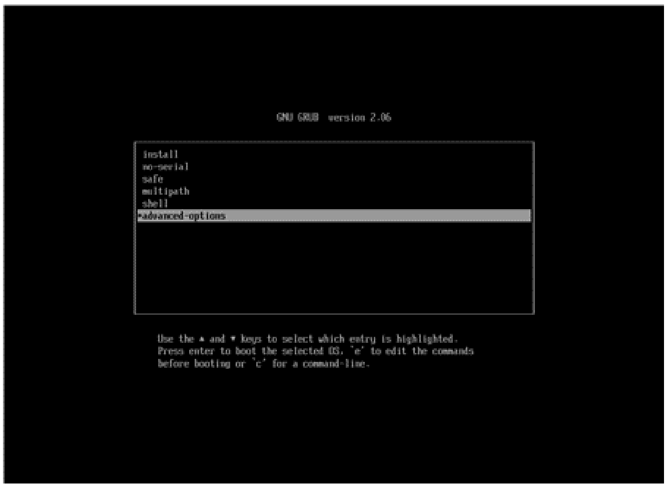
```
CertUtil -hashfile <filename> SHA256
```

Installing Citrix Hypervisor in CC mode

To run the evaluated configuration, you must install your Citrix Hypervisor servers in UEFI boot mode.

For the remainder of the installation procedure, refer to the *Install the Citrix Hypervisor Server* article in the Citrix Hypervisor 8.2 Cumulative Update 1 product documentation.

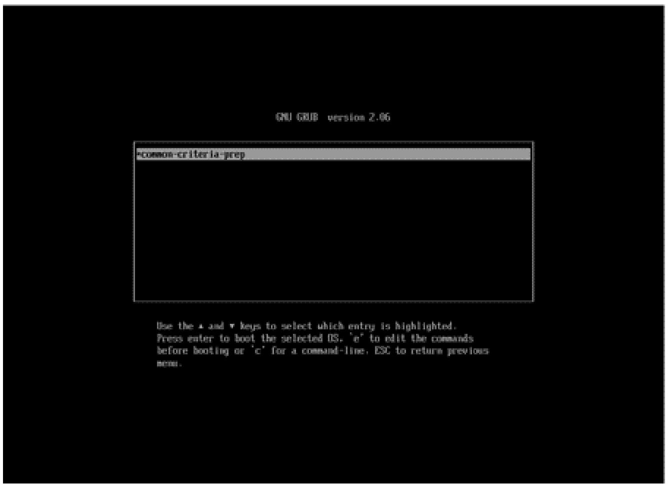
During the boot process (step 2 of the installation procedure), the GRUB menu displays for 5 seconds. On the GRUB menu, select **advanced-options > common-criteria-prep** to install Citrix Hypervisor in Common Criteria mode.



```
GNU GRUB  version 2.06

 install
 no-serial
 safe
 multipath
 shell
*advanced-options

  Use the ▲ and ▼ keys to select which entry is highlighted.
  Press enter to boot the selected OS, `e' to edit the commands
  before booting or `c' for a command-line.
```



```
GNU GRUB  version 2.06

*common-criteria-prep

  Use the ▲ and ▼ keys to select which entry is highlighted.
  Press enter to boot the selected OS, `e' to edit the commands
  before booting or `c' for a command-line. ESC to return previous
  menu.
```

In addition, you must note the following restrictions to install Citrix Hypervisor in 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.
- PXE booting your Citrix Hypervisor installation is not supported in the evaluated configuration.

As a result of restrictions enforced in common criteria mode, some of the options listed in the installation procedure in the *Install the Citrix Hypervisor Server* article are not available to you.

After you have installed Citrix Hypervisor 8.2 CU1 on your servers, you must also apply the following hotfixes to use the evaluated configuration:

- XS82ECU1001
- XS82ECU1002
- XS82ECU1003
- XS82ECU1005
- XS82ECU1006
- XS82ECU1007
- XS82ECU1010
- XS82ECU1012
- XS82ECU1014

In accordance with the flaw remediation process, Citrix might release additional hotfixes to address bugs or vulnerabilities. Only the hotfixes listed in the Common Criteria documentation are addressed by this evaluation.

We recommend that you apply all Citrix Hypervisor 8.2 CU 1 hotfixes to your hosts and pools that are running in common criteria mode. For more information, see Recommended Hotfixes for Citrix Hypervisor 8.2.

Users on Citrix Hypervisor servers

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

Network configuration

Linux bridge is the default network stack and the only supported network stack in the Citrix Hypervisor Common Criteria evaluated configuration.

The networks on the first three NICs (PIFs 0, 1, and 2) are labeled **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 VM traffic. To ensure that proper separation is maintained:

- Place your VMs only on the guest networks. Do not place any VMs on the management or the storage network.
- Only create VIFs on a guest network. Do not create any VIFs on the management or the storage network.

A restrictive firewall is configured and enabled in dom0. As 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.

Refer to Citrix Hypervisor 8.2 Cumulative Update 1 product documentation for further information on configuring networking and to **A.Separate_Networks** in the section **Security Problem Definition** in [CH CC ST].

Configuring the storage network

> **Note:**
>
> The following steps for configuring the storage network must be performed on all servers, 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
```

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

```
xe pif-list device=eth1 host-uuid=<host-uuid> params=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
```

Storage Configuration

The TOE allows NFS SRs and local EXT4 SRs as defined in the [CH CC ST]. The writeable ISO storage repository falls outside of the TOE. For more information about NFS SRs, see the Citrix Hypervisor 8.2 product documentation.

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

> **Note:**
>
> Complete these steps *only* on the pool master.

Creating an SR by using NFS storage

1. To add an 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 command returns the `sr-uuid`.

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

Registering a Default SR

After adding all the NFS SRs, choose one `sr-uuid` and make it the default SR:

1. Get the UUID of the pool:

   ```
   xe pool-list params=uuid minimal=true
   ```

2. Set the default SR for the pool:

   ```
   xe pool-param-set uuid=<pool-uuid> default-SR=<sr-uuid> \
       suspend-image-SR=<sr-uuid> crash-dump-SR=<sr-uuid>
   ```

Creating an ISO SR by using NFS storage

1. To add an ISO SR of type NFS 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 command returns the `sr-uuid`.

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

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 that 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 is returned. For example:

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

The output returned by the command is in the following format:

```
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, returns 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
```

The output returned by the command is in the following format:

```
<?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 NFS SRs:

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

Managing TLS Certificates

During Citrix Hypervisor host installation, a self-signed TLS certificate is installed. This certificate must be replaced to fully comply with the requirements for a CC deployment as defined in [CH CC ST]. This section explains how to set up a TLS configuration. A trusted X.509 Certification Authority (CA) is required for the steps in this section. For an example configuration suitable for use with OpenSSL, see the *TLS Configuration* section. Only certificates with 2048-bit RSA keys are supported.

Ensure that you install the trusted CA certificate and a server certificate on each Citrix Hypervisor server *before* joining the server to your pool.

Installing the Trusted CA Certificate

To install the trusted CA certificate on a server:

1. Copy your trusted CA certificate to removable storage.

2. Mount the removable storage containing the certificate.

3. In the server console, change to the directory containing the certificate.

4. Install the CA certificate by using the following command:

   ```
   xe pool-certificate-install filename=<ca-certificate-name>.pem
   ```

5. Unmount and remove the removable storage.

Generating server certificates

> **Note:**
>
> Keys used on the Citrix Hypervisor server must be generated in accordance with OE.Secure_Keys as defined in [CH 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.
- 127.0.0.1 must be included as a SAN.

For more information about TLS certificates for your Citrix Hypervisor server, see *Install a TLS certificate on your server* in the Citrix Hypervisor 8.2 Cumulative Update 1 product documentation.

For an example using OpenSSL, see the *TLS Configuration* section.

To install the TLS certificate on a server:

1. Copy the TLS certificate, private key, and certificate chain to removable storage.

2. Mount the removable storage media containing the certificate.

3. Enter the following command on the host console:

```
xe host-server-certificate-install certificate=<path-to-certificate-file> \
    private-key=<path-to-private-key> certificate-chain=<path-to-chain-file>
```

The `certificate-chain` parameter is optional.

4. Unmount and remove the removable storage.

Creating a Citrix Hypervisor resource pool

Citrix Hypervisor 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 *Hosts and resource pools* in the Citrix Hypervisor 8.2 Cumulative Update 1 product documentation.

Before creating a Citrix Hypervisor 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 a Citrix Hypervisor server `host1` to a resource pool using the xe 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 Citrix Hypervisor server `master`. The `password` must be the password set when the Citrix Hypervisor server `master` was installed.

Citrix Hypervisor hosts belong to an unnamed pool by default. To name the resource pool, enter the following commands:

1. Get the UUID of the pool:

   ```
   xe pool-list params=uuid minimal=true
   ```

2. Set the name of the pool:

   ```
   xe pool-param-set name-label="New Pool" uuid=<pool-uuid>
   ```

Removing a Citrix Hypervisor server from a resource pool

When a Citrix Hypervisor server is removed from a pool, the machine is rebooted, reinitialized, and left in a state equivalent to the state after a fresh installation.

To remove a host from a resource pool using the xe 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. Now use a suitable tool to securely erase the contents of the hard disk.

Preparing a pool of Citrix Hypervisor servers for maintenance

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

> **Note:**
>
> Placing the master host into maintenance mode results in the loss of the last 24 hours of Round Robin Database (RRD) updates for offline VMs. This behavior is because the backup synchronization occurs every 24 hours.
>
> Citrix highly recommends rebooting all Citrix Hypervisor hosts before installing an update, then verifying their configuration. Some configuration changes only take effect when a Citrix Hypervisor is rebooted, so a reboot can uncover configuration problems that would cause the update to fail.

To prepare a Citrix Hypervisor server in a pool for maintenance operations using the xe CLI

1. Run the command:

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

   This command disables the Citrix Hypervisor 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. After the maintenance operation is completed, enable the Citrix Hypervisor host:

```
xe host-enable uuid=<host-uuid>
```

5. Restart any halted VMs.

Coping with machine failures

> **Warning:**
>
> After running the command `xe host-forget`, use a suitable tool to erase the contents of the hard disk of the Citrix Hypervisor host. After you erase the hard disk, the Citrix Hypervisor host is left in a state where a fresh install can happen.
>
> When a non-fatal failure has occurred, the master must be power cycled before a new master is chosen. This action is to ensure that there is no risk of disk corruption due to several instances of the same VM running at the same time.

Creating VMs

This section contains notes on creating VMs. Read this information in conjunction with the *VMs* section of the Citrix Hypervisor 8.2 product documentation.

Types of VMs supported

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

> **Important:**
>
> Be careful when importing VMs and virtual appliances. Verify that imported VMs do not take the Citrix Hypervisor hosts out of the evaluated configuration. (For example, older virtual appliances might contain a PV guest).

VM security

The security of software running in a VM remains the responsibility of the user or administrator of the VM. For example, it is their responsibility to maintain appropriate patch states for software and virus protection within the domain.

SR-IOV

Although SR-IOV capable hardware (that is supported in the Hardware Compatibility List) can be used in the TOE, do not enable the SR-IOV specific functionality 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
```

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-through is not enabled.

```
xe vgpu-list
```

Virtual appliances

The following virtual appliances that are supplied with Citrix Hypervisor 8.2 Cumulative Update 1 Premium Edition fall outside of the TOE as defined in [CH CC ST]. Do not install or use these virtual appliances within the evaluated configuration:

- Citrix License Server virtual appliance
- Workload Balancing virtual appliance
- Citrix Hypervisor Conversion Manager virtual appliance

VM memory

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

Display the static memory properties of a VM

Complete 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=<vm-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
   ```

   The output from this example command is displayed in bytes:

   ```
   268435456
   ```

   The static maximum memory for this VM is 268435456 bytes (256 MB).

Display the dynamic memory properties of a VM

To display the dynamic memory properties, complete the following steps:

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=<vm-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
```

The output from this example command is displayed in bytes:

```
134217728
```

The dynamic maximum memory for this VM is 134217728 bytes (128 MB).

Updating memory properties

Warning:

In the Common Criteria configuration, dynamic memory control is outside of the TOE as defined in [CH CC ST]. As a result, take care when altering VM memory settings. For more information, see the Citrix Hypervisor 8.2 Cumulative Update 1 product documentation.

In particular, 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:

> Do not change the static minimum level `value1` in the preceding command, as this value is set at the supported level per operating system. For more information, see the memory constraints table in Citrix Hypervisor 8.2 product documentation.

Non-CC-certified product updates

From time to time, Citrix issues product updates which can correct flaws in the underlying software. Check with Citrix regularly for these updates. You can also opt to subscribe to email alerts concerning product security vulnerabilities and their associated fixes. These alerts are sent out regularly whenever new fixes are available. Contact Citrix Support directly if you require more support in obtaining and deploying any fix. More information about the email alerts system can be found at http://www.citrix.com.

If we issue an update that corrects a critical flaw, but the update is not yet CC certified, analyze the corrected flaw and the TOE's vulnerability to it when determining whether to install the non-CC certified update.

Features not included in the evaluated configuration

Important:

The following features are NOT included in the CC evaluated configuration. Using any of these features takes your Citrix Hypervisor deployment out of the evaluated configuration. For more information about the features included in the CC evaluated configuration, see [CH CC ST].

- Heterogeneous Resource Pools
- Active Directory Integration
- Role Based Access Control (RBAC)
- Host BIOS Boot
- SMB Storage
- Software FCoE Storage
- Software-boot-fromiSCSI
- IntelliCache
- vSwitch
- Live migration
- Storage live migration
- vGPU live migration
- Live Memory Checkpoint (Snapshots)
- Dynamic Memory Control (Ballooning)
- High Availability
- GPU Virtualization
- GPU pass-through
- Disaster Recovery
- Health Check
- PVS Accelerator
- Dynamic Workload Balancing & Audit Reporting (WLB)
- Citrix Hypervisor Conversion Manager
- Docker Container Management
- Direct Inspect APIs
- SMT (hyper-threading)
- SNMP

In the CC evaluated configuration, SNMP is turned off. The firewall rules used by dom0 when routing network packets also prevent the use of SNMP.

Additional CC configuration information

P2V and V2V Tools

Do not enable P2V and V2V tools and OCF support in the CC evaluated configuration.

Live migration

The TOE as defined in [CH CC ST] does not include live migration. It is not possible to disable this feature in Citrix Hypervisor. Ensure that everyone with administrator access to the Citrix Hypervisor pool is informed of this restriction.

SNMP

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

Security

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

TLS certificate verification is activated.

TLS Configuration

Following is an example of a configuration file for use with OpenSSL. This example creates a *CSR* that satisfies the requirements the Citrix Hypervisor server has for certificates. Before using it, ensure that this file complies with your organizational security policy.

Example:

```
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
```

Firewall configuration

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

Management network firewall

The ports that are used on the management network in the TOE as defined in [CH 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

Storage network firewall

The ports that are used on the storage network in the TOE as defined in [CH 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

Guest network firewall

The guest network is solely used by the VMs. Therefore, the firewall blocks any traffic to and from the Citrix Hypervisor server control domain.

Locations

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States

Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

Citrix Product Documentation | http://docs.citrix.com

July 25, 2022