Common Criteria Administrator's Guide for Citrix XenServer ® 6.0.2, Platinum Edition

Published Wednesday, 22 August 2012
3.0 Edition

Common Criteria Administrator's 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

Trademarks

Citrix®
XenServer ®
XenCenter ®

Published: 22 August 2012

CITRIX

Contents

Chapter 1. Document Overview

This document is a system administrator's guide to XenServer™ as it is to be used in the Common Criteria TOE. It is not a stand-alone document, but must be read together with [XS Admin].

The organization of this document mirrors that of [XS Admin]. The only addition is an appendix, Appendix B, *Common Criteria Related Information*, containing information specific to administrating a XenServer host in the Common Criteria evaluated configuration.

Where [XS Admin] contains information that conflicts with information in this document, it is the information in this document that should be used in order to maintain a XenServer host within the Common Criteria TOE.

> **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.

Bibliography

[XS CC ECG] *Common Criteria Evaluated Configuration Guide for Citrix XenServer ® 6.0.2, Platinum Edition*. 3.0.

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

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

[XS VM] *Citrix XenServer 6.0 Virtual Machine Installation Guide*. 1.0.

[XS XENAPI] *Citrix XenServer Management API*. API Revision 1.9.

Chapter 2. Managing Users

The information in this chapter is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

CITRIX

Chapter 3. XenServer Hosts and Resource Pools

Please see the corresponding section in [XS Admin].

3.1. Hosts and Resource Pools Overview

Please see the corresponding section in [XS Admin].

3.2. Requirements for Creating Resource Pools

Please see the corresponding section in [XS Admin].

3.3. Creating a Resource Pool

Please see the corresponding section in [XS Admin].

3.4. Creating Heterogeneous Resource Pools

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

3.5. Adding Shared Storage

Please see the corresponding section in [XS Admin].

> **Note:**
>
> This is limited to VHD on NFS in the Common Criteria configuration.

3.6. 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 zeroize the hard disk of the host that has been removed.

3.7. 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 XenServers 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 and restart them 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.

3.8. High Availability

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

3.9. Enabling HA on a XenServer Pool

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

3.10. Host Power On

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

CITRIX

Chapter 4. Storage

Please see the corresponding section in [XS Admin].

4.1. Storage Overview

Please see the corresponding section in [XS Admin].

4.2. Storage Repository Types

Please see the corresponding section in [XS Admin].

4.2.1. Local LVM

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

4.2.2. Local EXT3 VHD

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

4.2.3. udev

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

4.2.4. ISO

Please see the corresponding section in [XS Admin].

> **Note:**
>
> The writeable ISO storage repository falls outside of the TOE as defined in [XS CC ST].

4.2.5. Software iSCSI Support

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

4.2.6. Citrix StorageLink SRs

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

4.2.7. Managing Hardware Host Bus Adapters (HBAs)

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

4.2.8. LVM over iSCSI

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

4.2.9. NFS VHD

Please see the corresponding section in [XS Admin].

4.2.10. LVM over Hardware HBA

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

4.3. Storage Configuration

Please see the corresponding section in [XS Admin].

4.3.1. Creating Storage Repositories

Please see the corresponding section in [XS Admin].

4.3.2. Upgrading LVM Storage from XenServer 5.0 or Earlier

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

4.3.3. LVM Performance Considerations

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

4.3.4. Converting Between VDI Formats

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

4.3.5. 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

4.3.6. Storage Multipathing

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

4.3.7. MPP RDAC Driver Support for LSI Arrays.

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

4.4. Managing Storage Repositories

Please see the corresponding section in [XS Admin].

4.4.1. Destroying or Forgetting an SR

Please see the corresponding section in [XS Admin].

4.4.2. Introducing an SR

Please see the corresponding section in [XS Admin].

4.4.3. Resizing an SR

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

4.4.4. Converting Local Fibre Channel SRs to Shared SRs

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

4.4.5. Moving Virtual Disk Images (VDIs) Between SRs

Please see the corresponding section in [XS Admin].

4.4.6. Adjusting the Disk IO Scheduler

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

4.4.7. Automatically Reclaiming Space When Deleting Snapshots

Please see the corresponding section in [XS Admin].

4.5. Virtual Disk QoS Settings

Please see the corresponding section in [XS Admin].

CITRIX

Chapter 5. Configuring VM Memory

Please see the corresponding section in [XS Admin].

5.1. What is Dynamic Memory Control (DMC)?

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

5.2. xe CLI Commands

5.2.1. 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).

5.2.2. 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).

5.2.3. Updating Memory Properties

> **Warning:**
>
> In the Common Criteria configuration, 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 Section 5.1.6, “Supported Operating Systems” in [XS Admin] for more detail.

5.3. Workload Balancing Interaction

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

CITRIX

Chapter 6. Xen Memory Usage

When calculating the memory footprint of a Xen host there are two components that must be taken into consideration. First there is the memory consumed by the Xen hypervisor itself. Then there is the memory consumed by the *control domain* of the host. The control domain is a privileged VM that provides low-level services to other VMs, such as providing access to physical devices. It also runs the management tool stack.

The following fields on a VM define how much memory will be allocated. The default values shown are indicative of a machine with 8 GB of RAM:

name	default	description
memory-actual	789839872	The actual amount of memory current available for use by the VM *Read Only*
memory-target	789839872	The target amount of memory as set by using **xe vm-memory-target-set** *Read Only*
memory-static-max	789839872	The maximum possible physical memory Read Write when the VM is suspended; Read Only when the VM is running
memory-dynamic-max	789839872	The desired maximum memory to be made available Read Write
memory-dynamic-min	789839872	The desired minimum memory to be made available Read Write
memory-static-min	307232768	The minimum possible physical memory Read Write when the VM is suspended; Read Only when the VM is running
memory-overhead	15728640 (for example)	The memory overhead due to virtualization

Note:

The amount of memory reported in XenCenter on the **General** tab in the **Xen** field may exceed the values set using this mechanism. This is because the amount reported includes the memory used by the control domain, the hypervisor itself, and the crash kernel. The amount of memory used by the hypervisor will be larger for hosts with more memory.

To find out how much host memory is actually available to be assigned to VMs, get the value of the *memory-free* field of the host, then use the **vm-compute-maximum-memory** command to get the actual amount of free memory that can be allocated to the VM:

```
xe host-list uuid=<host_uuid> params=memory-free
xe vm-compute-maximum-memory vm=<vm_name> total=<host_memory_free_value>
```

CITRIX

Chapter 7. Networking

Please see the corresponding section in [XS Admin].

7.1. Networking Support

Please see the corresponding section in [XS Admin].

7.2. vSwitch Networks

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

7.3. XenServer Networking Overview

Please see the corresponding section in [XS Admin].

7.3.1. Network Objects

Please see the corresponding section in [XS Admin].

7.3.2. Networks

Please see the corresponding section in [XS Admin].

7.3.3. VLANs

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

7.3.4. NIC Bonds

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

7.3.5. Initial Networking Configuration

Please see the corresponding section in [XS CC ECG].

7.4. Managing Networking Configuration

Please see the corresponding section in [XS Admin].

7.4.1. Cross-Server Private Networks

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

7.4.2. Creating Networks in a Standalone Server

Please see the corresponding section in [XS Admin].

7.4.3. Creating Networks in Resource Pools

Please see the corresponding section in [XS Admin].

7.4.4. Creating VLANs

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

7.4.5. Creating NIC Bonds on a Standalone Host

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

7.4.6. Creating NIC Bonds in Resource Pools

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

7.4.7. Configuring a Dedicated Storage NIC

Please see the corresponding section in [XS Admin].

7.4.8. Using SR-IOV Enabled NICs

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

7.4.9. Controlling the Rate of Outgoing Data (QoS)

Please see the corresponding section in [XS Admin].

7.4.10. Changing Networking Configuration Options

Please see the corresponding section in [XS Admin].

7.5. Networking Troubleshooting

Please see the corresponding section in [XS Admin].

7.5.1. Diagnosing Network Corruption

Please see the corresponding section in [XS Admin].

7.5.2. Recovering from a Bad Network Configuration

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

CITRIX

Chapter 8. Disaster Recovery and Backup

Please see the corresponding section in [XS Admin].

8.1. Understanding XenServer DR

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

8.2. DR Infrastructure Requirements

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

8.3. Deployment Considerations

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

8.4. Enabling Disaster Recovery in XenCenter

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

8.5. Recovering VMs and vApps in the Event of Disaster (Failover)

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

8.6. Restoring VMs and vApps to the Primary Site After Disaster (Failback)

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

8.7. Test Failover

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

8.8. vApps

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

8.9. Backing Up and Restoring XenServer Hosts and VMs

Please see the corresponding section in [XS Admin].

8.10. VM Snapshots

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

8.11. VM Protection and Recovery

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

8.12. Coping with Machine Failures

Warning:

After executing the command `xe host-forget`, it is necessary to use a suitable tool to zeroise the 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 guest running at the same time.

Please see the corresponding section in [XS Admin].

Chapter 9. Monitoring and Managing XenServer

Please see the corresponding section in [XS Admin].

9.1. Alerts

Please see the corresponding section in [XS Admin].

9.1.1. Customizing Alerts

Please see the corresponding section in [XS Admin].

9.1.2. Configuring Email Alerts

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

9.2. Custom Fields and Tags

Please see the corresponding section in [XS Admin].

9.3. Custom Searches

Please see the corresponding section in [XS Admin].

9.4. Determining Throughput of Physical Bus Adapters

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

Chapter 10. Troubleshooting

Please see the corresponding section in [XS Admin].

10.1. XenServer Host Logs

Please see the corresponding section in [XS Admin].

10.1.1. Sending Host Log Messages to a Central Server

The information in this section is for a feature or aspect of XenServer that falls outside of the TOE as defined in [XS CC ST].

10.2. XenCenter Logs

Please see the corresponding section in [XS Admin].

10.3. Troubleshooting Connections between XenCenter and XenServer Host

Please see the corresponding section in [XS Admin].

Appendix A. Command Line Interface

Please see the corresponding section in [XS Admin].

A.1. Basic xe Syntax

Please see the corresponding section in [XS Admin].

A.2. Special Characters and Syntax

Please see the corresponding section in [XS Admin].

A.3. Command Types

Please see the corresponding section in [XS Admin].

A.4. xe Command Reference

Please see the corresponding section in [XS Admin].

> **Warning:**
>
> Some of the examples and the use of some of the commands described in this section, may take the host outside the evaluated configuration defined in [XS CC ST].

CITRIX

Appendix B. Common Criteria Related Information

B.1. Booting XenServer Hosts

The bootloader used on a XenServer host offers the user a choice of which kernel to boot, or to change the parameters passed to Xen and Linux. The user should *never* choose any kernel but the default one, nor change the boot parameters.

B.2. Network Forwarding

In order to ensure the separation between the three networks, network forwarding must be turned off on each XenServer host. Verify that network forwarding is off by entering the following commands:

```
sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 0
```

If network forwarding is on, disable it by entering the following commands:

```
sysctl -w net.ipv4.ip_forward=0
net.ipv4.ip_forward = 0
sed -i 's/net\.ipv4\.ip_forward.*/net.ipv4.ip_forward = 0/g'  \
  /etc/sysctl.conf
```

B.3. Notes on Creating VMs

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

B.3.1. Types of Guests Supported

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

> **Important:**
>
> Administrators should exercise caution when importing VMs and/or Virtual Appliances, and should 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)
```

B.3.2. Guest Security

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

B.3.3. 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
```

B.3.3.1. GPU Pass-thru

GPU Pass through 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
```

B.3.4. Virtual Appliances

The following virtual appliances that are supplied with XenServer Platinum 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, Web Self Service Virtual Appliance and vSwitch Controller Virtual Appliance.

B.4. Notes on Configuration

This section lists some Common Critera configuration topics which are not addressed in this document. See [XS CC ECG].

- Securing hardware
- Storage in Common Criteria configuration
- Networking in Common Critera configuration
- Firewall configuration
- Certificates

B.5. Users on XenServer Hosts

After installation, only a single user account is available on the XenServer host `root`. The TOE as defined in [XS CC ST] requires that no other accounts are created.

B.6. P2V and V2V Tools

P2V and V2V tools and OCF support must not be enabled in this configuration.

B.7. Live Migration, XenMotion

The TOE as defined in [XS CC ST] 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.8. SNMP

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

B.9. 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.

Administrators should check with Citrix on a regular basis for updates that are applicable specifically to the CC-certified version. For more information, see the "Software" section in [XS CC ECG].

Note:

Provisioning Services (virtual and physical servers) must not be installed in this configuration.

Note:

Lab Management and Stage Management must not be installed in this configuration.

CITRIX

Appendix C. Configuration differences between XenServer 6.0.2 and XenServer 6.0.2 Common Criteria Version

The XenServer 6.0.2 Common Criteria version incorporates all changes made by hotfixes released for XenServer 6.0.2 up to 7th July 2012. The hotfixes included are:

- Hotfix XS602E001
- Hotfix XS602E002
- Hotfix XS602E003
- Hotfix XS602E004
- Hotfix XS602E005

C.1. Networking

The Linux Bridge is the default networking stack, as vSwitch is excluded from the Evaluated Configuration.

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

A restrictive firewall is configured and enabled in dom0.

C.2. Storage

Local Storage Repositories (SR) are not created on installation. (In a manual installation the user is no longer given the option. When installing using an *answerfile*, any instruction to create a local SR is ignored.)

Removable SRs are not created on installation.

C.3. Hypervisor Restrictions

Xen is run with the cc-restrictions option. Therefore:

- Xen does not allow guests to use XATP+aliasing to free domain memory
- Unprivileged guests (i.e. not dom0) cannot use the grant table mechanism to access other guests' memory.
- The `guest_remove_page` function scrubs the page when memory is returned from a guest to Xen.
- Unprivileged guests (i.e. not dom0) cannot use the `XENMEM_exchange` operation to voluntarily return memory to Xen.

C.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.

C.5. Miscellaneous Changes

The dom0 kernel is run with the `xen_netback.netback_max_rx_protocol=0` option. (This is because version 1 of the protocol uses a receive-side copy mechanism.)

Dynamic memory control (memory ballooning) in dom0 is prevented by setting the memory target (and hence dynamic minimum and maximum) equal to the static maximum.

The version of XenCenter packaged with the CC variant of XenServer 6.0.2 does not notify users of available updates.

The file at `/etc/xensource-inventory` in dom0, contains the following line: `COMMON_CRITERIA='1'`