XenServer

Security Recommendations When Deploying XenServer

October 2023

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY

XenServer, a business unit of Cloud Software Group, is a trusted, competitively priced, and easy-to-use on-premises virtualization solution. For the last two decades, XenServer has enabled customers of all sizes to virtualize their workloads using the XenServer bare-metal hypervisor. Visit xenserver.com to see what XenServer can do for your business.

XenServer

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY

XenServer, a business unit of Cloud Software Group, is a trusted, competitively priced, and easy-to-use on-premises virtualization solution. For the last two decades, XenServer has enabled customers of all sizes to virtualize their workloads using the XenServer bare-metal hypervisor. Visit xenserver.com to see what XenServer can do for your business.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY

About

This guide helps you design security for a virtualized XenServer environment. It includes general best practices as well as information about the following:

- Protecting XenServer networks and storage
- Installing and deploying XenServer securely
- Configuring virtual machines
- Securing virtualized storage

The recommendations and guidance in this document are not intended to be exhaustive. Unless needed for clarity, this document does not provide detailed step-by-step procedures.

Applicable Versions

This guide applies to the following versions of XenServer:

- XenServer 8

Audience

Before reading this guide, you should have a basic knowledge of security, XenServer, and physical networking.

This guide has several audiences:

- Security specialists
- Systems architects
- Administrators

This guide assumes that you are familiar with basic XenServer concepts, including XenServer installation, XenCenter, resource pools, networking, and the pool coordinator (formerly pool master). You should also ensure that you are familiar with the release notes for the version of XenServer that you install.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY
XenServer, a business unit of Cloud Software Group, is a trusted, competitively priced, and easy-to-use on-premises virtualization solution. For the last two decades, XenServer has enabled customers of all sizes to virtualize their workloads using the XenServer bare-metal hypervisor. Visit xenserver.com to see what XenServer can do for your business.

XenServer

Finding Configuration Instructions

You can find configuration instructions in the following locations:

- XenServer product documentation. The XenServer 8 product documentation provides overview information and command-line based instructions.
- XenCenter product documentation. The XenCenter documentation provides UI-based step-by-step instructions using the XenCenter administration console. Users who are not comfortable with the XenServer xe commands, may prefer this option.

Terminology

- **Guest Network:** Guest networks carry VM traffic — the network traffic that originates or terminates from a virtual machine. These networks may also be referred to as VM networks.
- **Management Interface**: The management interface is a NIC (or a VLAN on a NIC) assigned an IP address that XenServer uses for its management network, including, but not limited to, traffic between hosts, between a host and Workload Balancing and for live migration. This is also the IP address to which management clients such as XenCenter will connect.
- **Hostile Traffic**: Any network traffic that could potentially violate the confidentiality, integrity, or availability of your network or its associated systems.
- **Control Domain**: A special-purpose domain (VM instance), based on a Linux kernel, that exists in a single instance on each XenServer host. The control domain is usually the only privileged domain (meaning that it can use privileged hypervisor calls, for example to map physical memory into and out of domains) on a XenServer host, and is thus the only domain that can control access to physical input/output resources directly and access the content of other domains (that is, Domain U). The control domain is also known as Domain 0 or “dom0”.
- **PV Drivers**: Drivers in a guest that accelerate storage and network data paths. These are treated as part of the guest operating system, use unprivileged XenServer interfaces, and are not involved in implementing XenServer security functions.
- **The management API**: The API for managing XenServer environments (that is, for remotely configuring and controlling domains running on hosts in a XenServer pool). The management API is sometimes referred to as “XenAPI.”

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY

Chapter 1: Introduction

In this chapter:

- An introduction to the guide
- An introduction to security in the cloud
- An approach for planning security in the layers of your virtual environment

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY

XenServer, a business unit of Cloud Software Group, is a trusted, competitively priced, and easy-to-use on-premises virtualization solution. For the last two decades, XenServer has enabled customers of all sizes to virtualize their workloads using the XenServer bare-metal hypervisor. Visit xenserver.com to see what XenServer can do for your business.

Introduction

The security requirements for your virtual environment depend on your organization's risk appetite and external factors such as regulation and compliance needs.

These requirements also depend on where your virtual environment is placed: within a co-location facility, within a private cloud, or hosted within your corporate network. Differing locations present different risk profiles. For example, a co-lo facility may present risks from other tenants but may be better resourced to provide dedicated, round-the-clock security monitoring. In contrast, in many enterprise environments internal threats may not be as significant. Consequently, efforts to secure internal guest networks may be a lower priority.

Many of the same security principles and techniques that apply to physical environments also apply to the virtual ones. Since the hypervisor is protecting every VM from every other VM, it is important that a hypervisor is designed with security from the ground up.

Approach

When planning a hypervisor environment, you need a particular focus on security design. This is because you not only have to protect the virtualization layer itself, but also the virtual machines running above. Both layers may be complex and large-scale with differing life-cycles and administrators. You need to meet not only your security expectations and governance, risk management, and compliance (GRC) needs but also those of the VMs running on your infrastructure. A large number of VM types, usages, and policies exacerbates the challenge.

In many deployments, different parts of the organization share services and may share computing resources. Separation between these groups must usually be achieved virtually rather physically. This use of virtualization should be secure by design.

Recommendation:

We recommend that you clearly understand and document:

- The traffic flow between different components, including hypervisors, switches, and guest traffic
- All components in the environment, including hypervisors, workloads, networks, management consoles, and physical hardware components
- Communications and data flows between hosts
- Any other potential communication channels for components, whether enabled or not
- What is expected not to change and what is expected to be reconfigured as differing organizational groups join, expand, shrink or leave
- RBAC roles and the individuals to whom they are assigned
- Any removable hardware components, such as USB drives and removable disk drives
- The details, including assigned IP addresses, of management interfaces and how they are physically configured to be on the network (switches, ports, and so on).

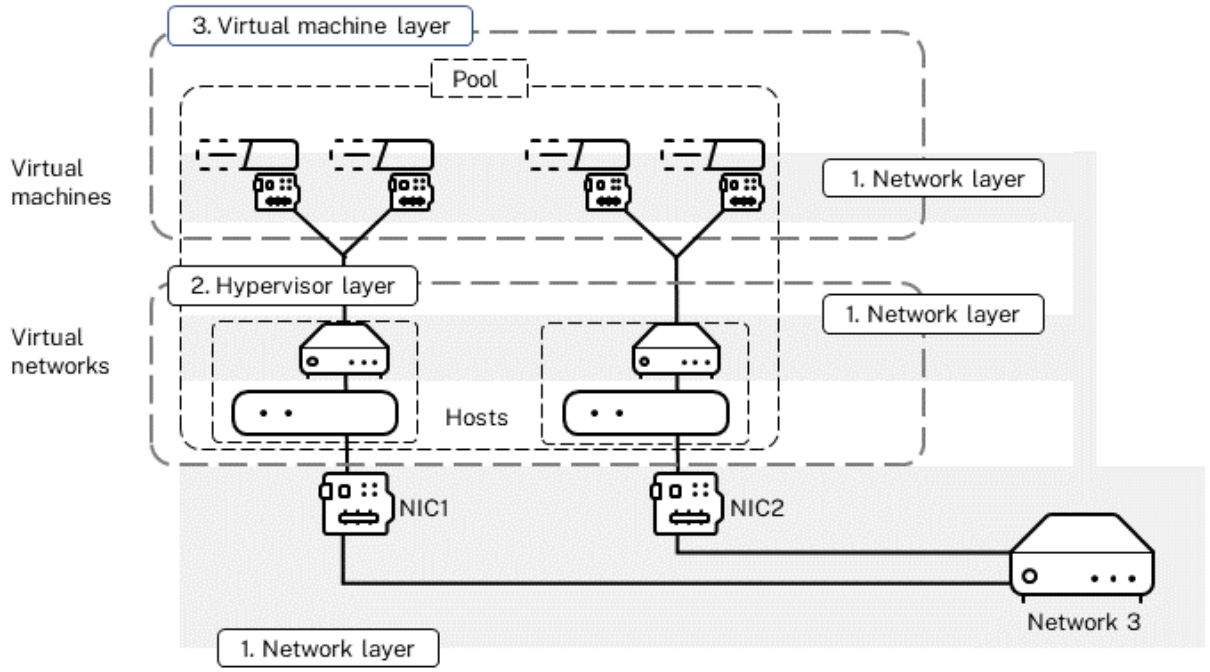
101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY

Planning Your Virtual Environment

Your virtual environment is structured as three layers, as shown in the diagram that follows:

1. Network layer, also including storage
2. Hypervisor (host) layer
3. Virtual machine (VM) layer

This document provides security guidance in corresponding chapters following this introductory chapter.



This illustration shows the different layers that people can secure in virtual environments, including the virtual machine layer, the hypervisor layer, and the network layer. The network layer, represented in gray, effectively straddles the hypervisor and virtual machine layers since there are networking aspects in all of these layers.

Many of the standard ways in which you secure physical environments apply to virtual environments. For example, it is possible to secure the virtual machine layer the same way as you normally secure an operating system, such as hardening Microsoft Windows.

Recommendation

We recommend that you secure guest operating systems in accordance with the standard practice of your organization's security policy.

We recommend that you secure networks in accordance with the standard practice of your organization's security policy. In particular, protect networking passwords, and also configure digital certificates accordingly.

We recommend that you manage access to the XenServer control domain carefully. The control domain provides administrative access to a pool and the VMs executing on it. The following chapters will provide you with recommendations on how to control users and isolate networks to restrict access.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY

Chapter 2: Protecting XenServer Networks and Storage

In this chapter:

- The importance of isolating the management network and separating XenServer networks
- How to separate XenServer networks
- XenServer firewall configuration and physical network security
- How to protect your storage network
- How to secure storage traffic.

In a XenServer environment, networking occurs not only on the physical level but also the logical level. From a network Layer 2 perspective, XenServer functions as a virtual network switch that can send traffic internally within the host (such as for private networks) and externally to the physical network.

Consequently, it is important that the XenServer environment is secured at all its levels: the virtual machine (guest) layer, the hypervisor layer, and the physical network layer, including storage networks.

Recommendation

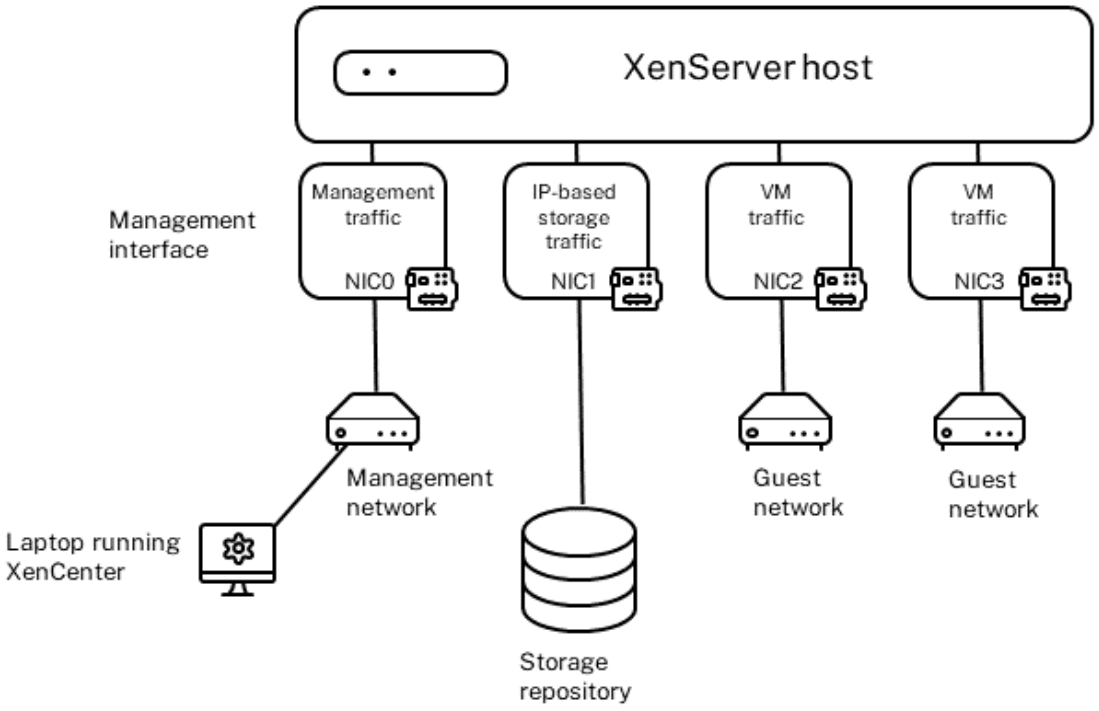
We recommend that you ensure that there is no data that crosses between networks, including the logical networks in the hypervisor layer.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY
XenServer, a business unit of Cloud Software Group, is a trusted, competitively priced, and easy-to-use on-premises virtualization solution. For the last two decades, XenServer has enabled customers of all sizes to virtualize their workloads using the XenServer bare-metal hypervisor. Visit xenserver.com to see what XenServer can do for your business.

Network Traffic Separation

XenServer has three distinct categories of network traffic in each pool: (a) management traffic, (b) storage traffic, and (c) VM (guest operating system) traffic. You can configure your XenServer hosts to send this traffic over separate or shared networks.

The following illustration provides an example of this separation where different classes of traffic use different physical NICs.



This illustration shows how NICs that are not designated for management or storage traffic only carry VM traffic.

- **Management Traffic**: XenServer uses the management network for XenServer management communications, including traffic between hosts, live migration, VM import and export, and resource pool metadata backups. The management network is the network connected to the NIC that is configured as the management interface. Management traffic does not include communications between guest virtual machines but does include traffic involving XenCenter, the administration console.

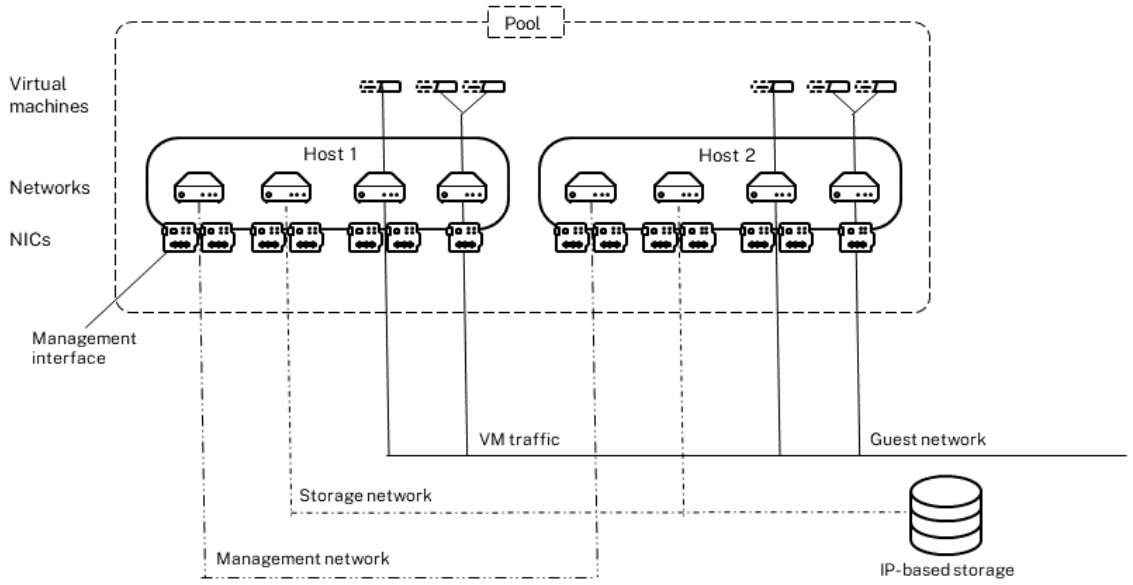
  XenServer installation creates the management network on each host and assigns it to a specific NIC that will function as the management interface. XenServer will allow you to use a single interface for all three types of traffic: management, storage and guest. However, this is not the most secure networking configuration, and we strongly recommend separating traffic as described throughout this section.

- **Storage Traffic**: The term storage traffic refers to Fibre Channel traffic and IP-based storage traffic, such as iSCSI software initiator traffic, NFS traffic, and SMBv3 traffic.

However, when this guide discusses placing storage traffic on its own network this specifically refers to iSCSI and NFS traffic. (Fibre Channel traffic is inherently on its own network.) Storage traffic is discussed in more detail throughout this section and in Protecting Virtualized Storage .

- **Guest Traffic**: Guest traffic refers to traffic being sent to or from guest virtual machines.

  Physical network separation provides additional security. The following illustration provides an example.



This illustration shows the management interface, the NIC used for management communications, and the management network. The management network is separated from the storage network and the guest network.

Recommendation:

We strongly recommend physically separating the management, storage, and guest networks through NICs, cables, switches, ports and network configuration as well as logically separating through configuration in XenServer. This includes ensuring that you do not unintentionally send guest traffic across the management network, as explained in the section that follows.

Ensuring Traffic is Separated

To understand how to separate traffic, it is important to understand how VMs communicate.

A VM can only use a NIC for guest traffic if it has a virtual network interface on the same network as the NIC.

Not all NICs have virtual network interfaces associated with them. If you do not configure a virtual network interface connecting to the management network, the management NIC becomes dedicated for management traffic. For example, in the previous illustration, there are NICs

connected to the management and storage networks that do not have corresponding virtual network interfaces.

The previous illustration depicts VMs that only have virtual network interfaces for the guest network. The VMs are not connected to the management or storage network: the VMs do not have virtual network interfaces that connect to those networks.

Recommendation:

We recommend that you isolate production networks from staging, testing and development networks.

Planning a Separate Storage Network

Recommendation

We recommend that you segregate traffic by configuring an additional storage interface(s) for IP-based storage traffic and configuring XenServer to access storage through that interface. (However, you must also then physically isolate the guest networks and configure virtual machines only to use those isolated networks). Note that additional interfaces are also known as secondary interfaces in some literature.

The overall process for creating a separate storage network is as follows:

1. Configuring physical network infrastructure so that different traffic is on different subnets.
2. Creating a storage interface to use the new network.

Consider configuring redundancy, either multipathing or bonding, during the above steps if desired.

Following the above process lets you establish separate networks for IP-based traffic provided that:

- You do not configure XenServer to use this network for any other purpose (for example, by connecting a virtual network interface to this network)
- The appropriate physical network configuration is in place

For example, to dedicate a NIC to storage traffic, the NIC, storage target, switch, and/or VLAN must be configured so that the target is only accessible over the assigned NIC.

To ensure that the storage traffic is separated from the management traffic, the storage network must be on a different subnet. The subnet for storage must be a separate IP subnet that is not “routable” from the management interface. If the physical or logical configuration does not enforce the traffic separation, then XenServer may direct storage traffic over the management interface after a host reboot, due to the order in which XenServer initializes NICs.

Planning a Separate Guest Network

Recommendation

We recommend that you configure all VMs to have guest networks only. VMs do not require access to storage and management networks as explained below.

Recommendation

We recommend that you configure your guest networks correctly so they do not unintentionally send traffic over the management and storage networks:

- Ensure the guest network is physically isolated from management and storage traffic. Connect the NIC that the VMs will use for guest traffic to a switch port that will be used for VM traffic only. This port must be physically isolated from the storage and management networks.
- Create a virtual network interface on the same network(s) as the NIC.
- Do not route any types of traffic, other than guest traffic, across that NIC.
- When you create VMs, if you configured the management interface on NIC 0, make sure that NIC 0 is not enabled in the VM wizard when you create the VM, as explained in the procedure that follows.

Alternative:

In situations where hosts only have one NIC dedicated to guest traffic, we recommend considering separating traffic into separate logical networks. For example, a common configuration is for an application server to manage "front-end" traffic (for example, to a web server) and "back-end" traffic (for example, to a database). This can be done using VLANs. A VLAN tags the Ethernet traffic separately but traffic still goes over the same physical NIC on the host.

Recommendation

We recommend that you do not assign the control domain an IP address for any network other than storage networks and the isolated management network.

Do not place guest VM traffic on any network that has a control domain IP address.

Recommendation

We recommend that, if you have a guest network that connects to a network that is not under your organizational control (such as the Internet), you make sure the local segment of the network is protected. Any unprotected network may be vulnerable to Level 2 network attacks, such as fake DHCP attacks, that must be performed from the same switch as the attack's target.

Recommendation

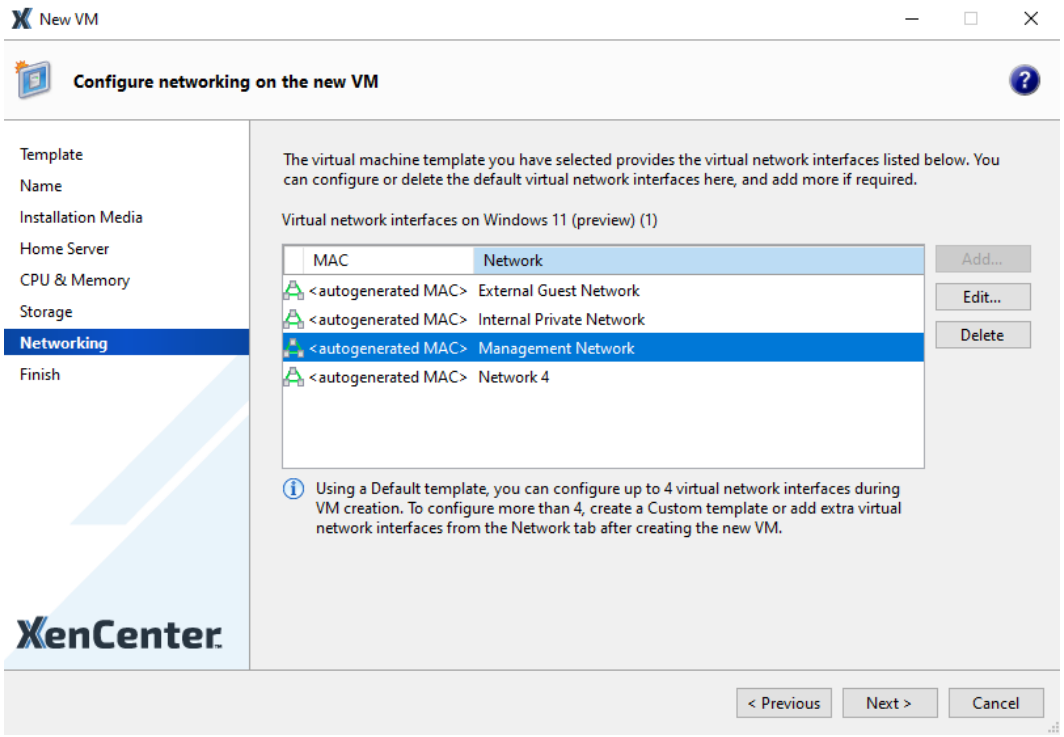
We recommend that, if you have some VMs that require Internet access and some that do not, you configure separate networks so that the VMs that do not require Internet access are not directly exposed to possible attacks from the Internet.

To configure VMs with guest networks only

Note: This procedure may be easier to perform if you change the names of the networks to assign them clear names as described in Naming Networks Clearly.

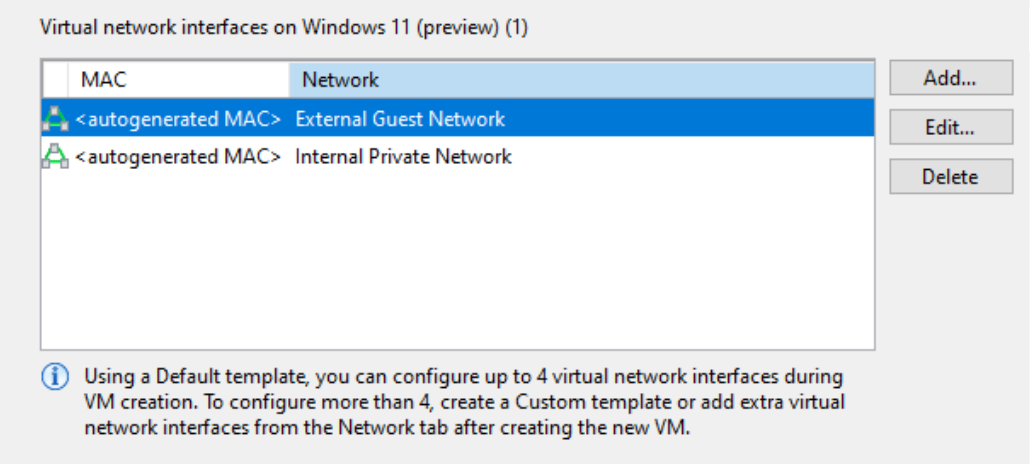
1. After launching the XenCenter **New VM** wizard (**VM> New VM**), follow the prompts until you reach the **Networking** page.

2. On the **Networking** page, remove all networks that the VM will not be using. Select the network to remove and click **Delete**.



By default, XenServer installation configures the management interface on Network 0, which is typically NIC0.

The resulting networks may look something like the following:



3. If necessary, click **Properties** to configure QoS settings or Virtual MAC addresses.

Important: Any virtual network interfaces that appear in this dialog box will be created as networks on the virtual machine.

Naming Networks Clearly

Recommendation

We recommend that you rename the default networks so they have clear names that are meaningful to your configuration to prevent inadvertently connecting a guest to a network to which it should not have access, such as the management network.

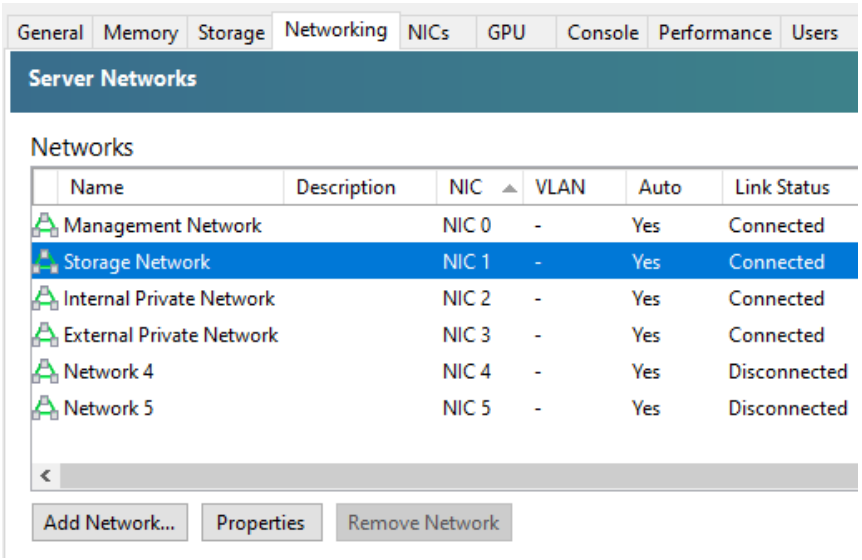
For example, change the default names XenServer assigns to NICs to ones that represent the functions they perform in your environment:

NIC	Network	Name
0	Network 0	Management Network
1	Network 1	Storage Network
2	Network 2	Internal Private Network
3	Network 3	External Guest Network

To change the names of networks

In the **Networking** tab in XenCenter, select the network and click **Properties**, as shown in the following screen capture:

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY



This screen capture displays the names of networks, which were changed from their default names for clarity. You can also add information about the network to the description column.

You can also change network names by running the following command:

```
# xe network-param-set uuid=<network uuid> name-label="<new network name>"
```

For example, to assign Network 1 the name “Storage Network” run:

```
# xe network-param-set uuid=213e396e-1e1f-0744-7a43-64c3e9dfd649 \
name-label="Storage Network"
```

Using the name-label parameter is the same as renaming the network in XenCenter.

Tip: To obtain the network UUID, run `xe network-list`.

Protecting the Management Network

Protecting the management network is important because this network can potentially provide access to all components connected to a host. Communication between XenServer 8 hosts and both XenCenter and other XenServer 8 hosts is over (encrypted) TLS connections to port 443. However, XenServer management functions listen on both port 80 (unencrypted) and port 443 (TLS encrypted) for management API requests. This allows interoperability with older versions of the product and other (e.g. third-party) products.

Recommendation

Unless you have third-party management API agents that are unable to use TLS, we recommend that you block access to port 80 with the CLI command

```
xe pool-param-set uuid=<pool uuid> https-only=true
```

If you need to reverse this command, for example if you need to migrate VMs to a XenServer 8 host from an earlier version of the product, you can do so the the CLI command

```
xe pool-param-set uuid=<pool uuid> https-only=false
```

It is possible to configure the management interface so that an IP address is not bound to it. However, this means that none of the management functions will work from outside the local console on the XenServer host. Be aware that in this configuration you cannot create resource pools, import/export VMs, or otherwise take advantage of features such as email alerting.

Configuring Switch Port Locking

In environments with untrusted guest VMs, it may be desirable to use security measures, such as spoofing protection, to reduce the ability of VMs to attack other virtual machines over the network.

Recommendation

We recommend that environments with potentially hostile or unknown guest traffic configure the XenServer switch-port locking feature:

We recommend using the switch-port locking feature to define specific IP addresses from which an individual VM is allowed to send traffic.

The XenServer switch-port locking feature lets you control traffic being sent from unknown, untrusted, or potentially hostile VMs by limiting their ability to pretend they have a MAC or IP address that was not assigned to them.

For more information, see the product documentation.

Recommendation

We recommend that environments that have both (a) VMs containing sensitive data and (b) untrusted VMs use the switch-port locking feature to prevent an untrusted VM from sending spoofed traffic to sensitive VMs.

The XenServer switch-port locking feature may assist in deployments that have a network architecture in which each VM has a public, Internet-connected IP address. For more information about switch-port locking, see the product documentation.

Securing the Physical Network

Recommendation

We recommend that you take precautions to ensure you do not inadvertently cable the management interface into the guest network. For example:

- We recommend consistently designating the same NICs for use with the same networks across all hosts in all pools.
- In environments with multiple pools, We recommend always designating specific ports for specific types of traffic and using these ports consistently. For example, across all pools always use the first network port for your management network, the second network port for your storage network, and so on.
- Where your organization does not already have cabling standards, We recommend that you consider labelling or color-coding cables to indicate their purpose.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY

Recommendation

We recommend that you erase all previous configurations when you reuse physical switches.

Previous passwords or configurations could potentially expose your environment to hostile entities or traffic. For example, somebody might have configured the switch to route traffic automatically to another site or network.

Recommendation

We recommend that you protect the physical location of the network, including the security of the physical area where the network is located.

Protecting Virtualized Storage

Data storage is considered to be virtualized when there is not a one-to-one relationship between the physical storage device and the resulting virtualized storage devices (or disks). For example, when one physical storage device is presented to users as one or more virtualized storage devices or conversely when multiple physical devices are presented as one virtual disk. While virtualizing data storage reduces the user's perception of complexity, it is important to ensure storage is virtualized securely.

For companies who want to secure and monitor their virtualized storage, it is worth noting that virtualized storage can reside in multiple physical locations simultaneously.

Recommendation

We recommend that you consider where all the physical drives being virtualized are located when determining the physical security of disks and you do not place disks in a location where they are physically at risk.

For example, if you add another SR because your original SR ran out of space and the new SR is in a different physical location (for example, on a server that might not be in the same machine room), ensure both locations are physically secure.

Dedicated storage NICs require an IP address that must be on a different IP subnet to the main administration interface. You can use XenCenter to dedicate a storage NIC and also to bond multiple NICs together for resilience.

Recommendation

We recommend isolating storage traffic from management traffic. If you are using IP-based storage devices, such as an NFS or iSCSI SR, the storage traffic also flows through the XenServer control domain.

Recommendation

We recommend that, where appropriate to the storage type, you configure target and host authentication. This helps protect your data if your storage network is exposed to other less trustworthy parts of your organization. Internal attacks on storage networks may enable hostile parties to intercept any data destined for storage. Such data ranges from data that could compromise the integrity of your virtual environment to sensitive data contained within the virtual machines.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY
XenServer, a business unit of Cloud Software Group, is a trusted, competitively priced, and easy-to-use on-premises virtualization solution. For the last two decades, XenServer has enabled customers of all sizes to virtualize their workloads using the XenServer bare-metal hypervisor. Visit xenserver.com to see what XenServer can do for your business.

NFS

A file-based NFS storage repository mounts the specified NFS repository on the control domain. Each SR is represented as a directory on the remote NFS server, with each virtual disk being a file in that directory stored in the VHD file format.

Recommendation

We recommend ensuring that, because the VHD is not an encrypted file format, only authorized XenServer hosts and authorized administrators can mount the file system. You can ensure only the correct XenServer hosts can mount the file system by limiting the export to specific IP addresses. Limiting export is typically done when setting up the NFS storage system.

Recommendation

We recommend ensuring that the storage interfaces of the remote storage device are not visible outside of the dedicated storage network.

Recommendation

We recommend enabling the NFSv4 AUTH_SYS host authentication.

iSCSI Software Initiator

In the case of iSCSI traffic, XenServer uses the software OpenISCSI initiator to connect to iSCSI targets.

If you are sharing your iSCSI storage network with other XenServer pools or non-XenServer systems, consider separating your iSCSI storage traffic with VLANs.

Recommendation

If you have multiple XenServer pools, We recommend that you do not share iSCSI storage networks between pools that have differing levels of trust. For example, a production server pool and a test server pool should not share a storage network.

Recommendation

We recommend that you configure CHAP target and host authentication unless you are using GFS2.

Fibre Channel

Recommendation

We recommend enabling LUN masking on your SAN to secure Fibre Channel traffic.

LUN masking is a way of configuring a LUN to only accept requests from specific HBAs so that a LUN is available to some hosts and not others. LUN masking shields LUNs from detection when a target is scanned. Depending on your HBA configuration, LUN masking may make it possible to control which hosts can access what volumes on a SAN. LUN masking lets you configure the exact LUNs that a specified host can detect.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY
XenServer, a business unit of Cloud Software Group, is a trusted, competitively priced, and easy-to-use on-premises virtualization solution. For the last two decades, XenServer has enabled customers of all sizes to virtualize their workloads using the XenServer bare-metal hypervisor. Visit xenserver.com to see what XenServer can do for your business.

Recommendation

We recommend creating zones in your SAN to separate and secure Fibre Channel traffic.

SAN zoning is a way to group Fibre Channel devices logically over the storage fabric's physical configuration. Consider implementing SAN zoning to separate storage traffic from more vulnerable servers (for example, Web servers or other servers with a lot of Internet traffic) from the storage traffic of other servers.

Zones effectively isolate devices in the zone from devices outside of the zone and prevent devices outside the zone from detecting devices in the zone. Because zoning is implemented in the fabric by the Fibre Channel switch, zoning can control traffic between devices and, in essence, provide a method of access control for SANs. Zones also provide security because zone traffic is isolated from traffic in other zones, which, in turn, limits the amount of traffic compromised in a successful attack.

SMB

If you are sharing your SMB storage network with other XenServer pools or non-XenServer systems, consider separating your SMB storage traffic with VLANs.

Recommendation

If you have multiple XenServer pools, We recommend that you do not share SMB storage networks between pools that have differing levels of trust. For example, a production server pool and a test server pool should not share a storage network.

Recommendation

We recommend that you configure SMB username/password host authentication.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY
XenServer, a business unit of Cloud Software Group, is a trusted, competitively priced, and easy-to-use on-premises virtualization solution. For the last two decades, XenServer has enabled customers of all sizes to virtualize their workloads using the XenServer bare-metal hypervisor. Visit xenserver.com to see what XenServer can do for your business.

Chapter 3: Protecting XenServer Hosts

In this chapter:

- Isolating sensitive VMs
- Securing the control domain
- Limiting access to physical hosts

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY

Isolating Sensitive VMs

When designing your virtual environment and determining what servers will host what workloads, consider which virtual machines are particularly sensitive.

Recommendation

We recommend that if you have VMs that are particularly sensitive, you consider putting them in a pool that is limited to specific administrators.

Recommendation

We also recommend using VLANs to isolate traffic for systems hosting sensitive data.

Recommendation

We recommend that, in environments with Workload Balancing enabled, if you have a host in a pool that has a different (even if higher) physical security level, you exclude such a host from Workload Balancing optimization and placement recommendations by using the Workload Balancing Exclude Hosts feature. When enabled, the Exclude Hosts feature excludes physical hosts from Workload Balancing optimization and placement recommendations, including Start On placement recommendations.

Securing the Control Domain

Each host in a pool has a control domain. 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 control domain contains the minimal functionality necessary to manage the host and is designed specifically for that purpose.

Recommendation

We strongly recommend that, to maintain the security, integrity and supportability of the control domain, you do not make any alterations to the control domain that we do not specifically recommend.

Recommendation

We recommend configuring a strong password for your control domain, track who has these passwords, and have a policy for changing both the pool secret and the root account passwords on control domains when individuals with access leave the organization.

For more information, see the product documentation for Managing your administrator password and Rotating your pool secret.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY
XenServer, a business unit of Cloud Software Group, is a trusted, competitively priced, and easy-to-use on-premises virtualization solution. For the last two decades, XenServer has enabled customers of all sizes to virtualize their workloads using the XenServer bare-metal hypervisor. Visit xenserver.com to see what XenServer can do for your business.

Designing Environments for Auditing

Recommendation

We recommend designing your environment with auditing in mind, including planning to enable Role Based Access Control (RBAC).

Enabling RBAC makes audit log data more meaningful since the transactions are logged with the associated user names.

Even if you do not wish your administrators to have different levels of access, RBAC allows you to audit which administrator performed which operation.

Recommendation

We recommend that you configure individual RBAC user accounts for each administrator to provide accountability.

XenServer provides support for running reports on administrative changes. These reports can be helpful for detecting changes made to your XenServer environment by administrators for either troubleshooting, or possibly auditing and compliance reasons.

Support for auditing is provided through the Workload Balancing component and its workload reports. Configuring support for auditing reports requires Active Directory and the following relatively simple tasks:

1. Adding the Active Directory accounts of the XenServer administrators to XenServer.
2. Configuring the XenServer Role Based Access Control (RBAC) feature and assigning roles to the XenServer user accounts. For information about RBAC, see the product documentation.
3. Deploying Workload Balancing, as described in the product documentation, so that you can run the Audit Trail History report. For more information about this report and what it contains, see the “Pool Audit Trail” information in the product documentation.

Depending on your need to demonstrate the compliance of your environment, you might want to take additional steps to secure the Workload Balancing database, which is where the audit-trail data is stored. Such steps might include limiting the access to the password or documenting procedures to show how the access is controlled.

Tracking Possibly Unauthorized Changes to Your Environment

When you need to track down the entry point of malware or another threat, it is essential to be able to review the sources of changes to your environment.

Recommendation

We recommend you require administrators to use their individual user accounts since it is easier to isolate the source of unauthorized administrative changes.

Not providing the root account password to administrators may assist in encouraging use of individual accounts.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY
XenServer, a business unit of Cloud Software Group, is a trusted, competitively priced, and easy-to-use on-premises virtualization solution. For the last two decades, XenServer has enabled customers of all sizes to virtualize their workloads using the XenServer bare-metal hypervisor. Visit xenserver.com to see what XenServer can do for your business.

Recommendation

We recommend enabling RBAC and Workload Balancing so you can use Workload Balancing to run the Audit Trail History Report.

The Audit Trail History Report lists administrative changes. For more information, see the product documentation.

Recommendation

We recommend setting all systems in a geographic region to use the same time source (for example, by using an NTP server).

When searching for events and changes across systems, it is extremely helpful if all of the systems through which you are searching are set to the same time. This makes it easier to use logs to correlate events across logs from different systems.

When reviewing changes, be aware of time zones and whether the particular log entry reflects local time or Coordinated Universal Time (UTC)/Greenwich Mean Time (GMT).

Enabling Audit Logging

Audit logging, which is the recording of specific administrative changes, is enabled by default in XenServer.

The XenServer audit log records any operation with side effects (successful or unsuccessful). This record includes the server name targeted by the action and the success or failure of the action. The audit log also records associated user names or, if RBAC is not enabled, the type of account association with the action.

Recommendation

To increase the security and availability of the contents of the audit log and reduce the risk of an attacker changing its contents, consider sending your audit log to a remote server, ideally one inaccessible to XenServer administrators.

Recommendation

We recommend both of the following:

- Remote servers for storing logs be managed by somebody with different operational role (for example, by somebody on a team that does not manage the XenServer hosts)
- Administrators with access to XenServer should not be granted permissions to modify or delete logs on the remote server

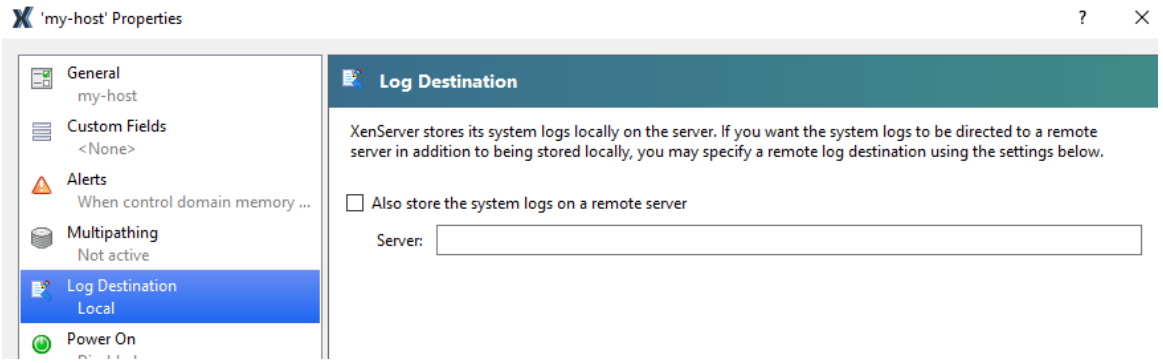
Recommendation

We recommend retaining audit logs in accordance with your organizational security policy.

To configure remote storage of system logs using XenCenter

1. In the XenCenter **Resource** pane, select the host, and click the **General** tab.
2. On the **General** tab, click the **Properties** button.

3. On the **Log Destination** page, select **Also store the system logs on a remote server** and enter the remote server where you want to save the logs.



It is important that the remote server where you are saving the audit log is connected to an NTP server. Even if an attacker, in an attempt to reduce detection, changes the time in the XenServer environment, the remotely saved logs will still reflect the correct system time.

Disabling Remote SSH Access

Recommendation

We recommend that customers who do not intend to use SSH access to the control domain disable SSH. Note that the console will still be available locally or through XenCenter.

To disable remote SSH access

1. In XenCenter, click the **Consol**e tab. Alternatively, you can go to the physical console.
2. At the command prompt, type `xsconsole`.
3. In the shell menu, scroll down to the **Remote Service Configuration** option and press **Enter**.
4. Select **Enable/Disable Remote Shell** and press **Enter**.
5. Enter your credentials and press **Enter**.
6. In the **Configure Remote Shell** options, select **Disable** and press **Enter**.
7. After a message appears stating configuration was successful, click **OK**.

Note: If you need to re-enable remote SSH access, repeat this procedure but select **Enable** in the **Configure Remote Shell** options.

XenCenter Security

If your version of XenCenter is not up to date, it will notify you that an update is available unless you have disabled that notification.

Recommendation

We recommend that you ensure that you are using the latest version of XenCenter.

XenCenter can store credentials for all the hosts it controls. (This option is configured in **Tools > Options > Save and Restore.**)

Recommendation

We recommend that you ensure that users only use the Save and Restore Service Connection State on Startup option if permitted by their organizational security policy. In particular, We do not recommend storing Active Directory credentials.

You can protect credentials stored by XenCenter by creating a main password. When enabled, XenCenter prompts users for a password to see any managed servers.

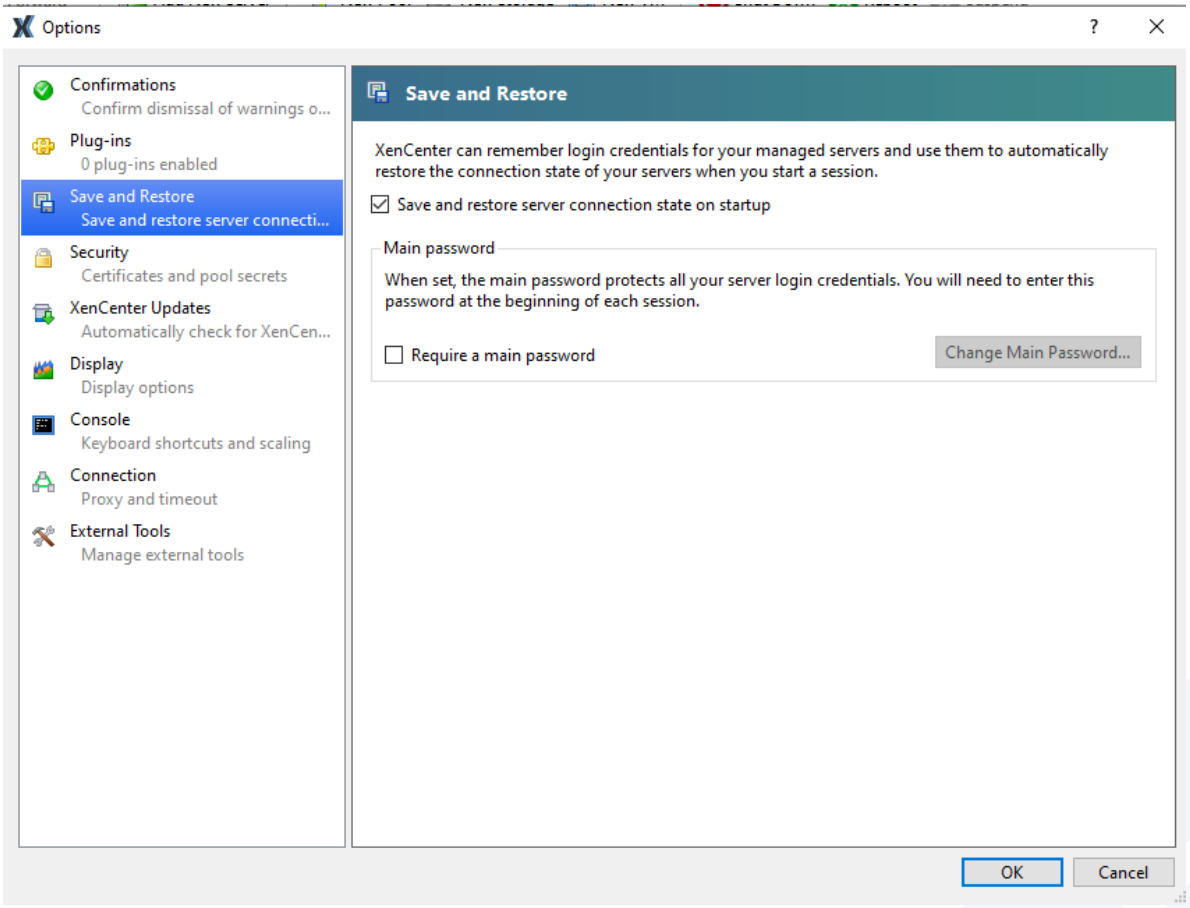
Recommendation

Where your organizational security policy permits XenCenter to store credentials, We recommend creating a main password for XenCenter to prevent unauthorized users from obtaining the credentials of managed XenServer hosts, for example if a laptop used to manage XenServer is stolen.

Recommendation

We recommend restricting physical access to XenCenter. For example, do not leave unauthorized people unattended with access to a logged in XenCenter console.

To set a main password



1. From the XenCenter **Tools** menu, click **Options** and then click the **Save and Restore** tab.
2. Ensure that the **Save and restore server connection state on startup** check box is selected.
3. Under **Main** password, select the **Require a main password** check box, then enter and confirm the password, and click **OK**. Remember that passwords are case-sensitive.

Naming Hosts Clearly

Recommendation

We recommend using meaningful naming conventions when assigning host names to prevent inadvertently configuring hosts in the same pool that should not be connected for security reasons.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY

- Choose a naming convention that has names that indicate physical security constraints (for example, the physical location).

Recommendation

We recommend that you ensure your host names have significance to your organization so as to avoid moving a VM to the wrong host.

Securing Physical Hosts

This section provides recommendations about limiting physical access to hosts and securing out-of band ("lights-out") management cards.

Limiting Physical Host Access

Recommendation

We recommend that you take steps to limit physical access to systems. In particular, as a number of different functions may be running in a virtual environment at a specific physical location, you should consider the number of functions that may be simultaneously compromised.

Securing Out-of-band Management Cards (Lights-out Management)

Recommendation

If you require support for hardware features that enable remote administration on the host (for example, Dell DRAC or HP iLO), ensure that access is secured in accordance with your organization's security policy for these features. Otherwise, disable these features.

Recommendation

We recommend that you consider the type of traffic (for example, untrusted guest VM traffic) on a network when considering enabling remote administration on an interface on that network.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY
XenServer, a business unit of Cloud Software Group, is a trusted, competitively priced, and easy-to-use on-premises virtualization solution. For the last two decades, XenServer has enabled customers of all sizes to virtualize their workloads using the XenServer bare-metal hypervisor. Visit xenserver.com to see what XenServer can do for your business.

Chapter 4: Protecting VMs

In this chapter:

- Securing virtual machines
- Mitigating abnormal loads (denial of service attacks)
- Securing resource pools
- Understanding how to use live migration in accordance with your security design

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY

Securing Virtual Machines

Recommendation

We recommend that you use the same practices that you would use to secure virtual machines that you would use to secure a physical server: in many ways, their security needs are comparable. This includes taking the same steps to secure the guest operating system as you would to secure the operating system on a physical machine.

- We recommend enabling all of the standard methods of protection on the virtual machines, including virus, spyware, and malware protection and operating-system level firewalls, if appropriate.
- We recommend checking that any virtual machines you start after a long period of dormancy have the latest updates to their anti-virus definitions and apply any relevant security patches.
- We recommend disabling any unnecessary system components at the guest level, including in the operating system that may provide an attack surface. For example, follow the operating system vendor's security guidance document.
- We recommend, to reduce the risk of omitting to set a secure configuration, using templates with the guest operating system installed and configured with security settings whenever you create a VM.
- We recommend creating a variety of templates that include not only the secured operating system but also any frequently deployed applications, such as Citrix Virtual Apps and Desktops (if applicable), that also have their security settings configured.

XenServer VM Tools

We recommend that customers have the latest version of XenServer VM Tools running on their guest virtual machines to ensure the best manageability. However, as the tools are running in the guest virtual machines and not in the control domain or the hypervisor, they do not present an additional threat to the XenServer installation. Information on applying updates for XenServer VM Tools can be found at Update XenServer VM Tools for Windows.

Secure boot

XenServer supports UEFI Secure Boot for Windows VMs. This blocks incorrect binaries from being executed within the guest as the OS is loaded and so helps to protect the guest VM.

Recommendation

We recommend that you consider enabling secure boot for your more sensitive VMs, taking into account whether VM OS has secure boot support.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY
XenServer, a business unit of Cloud Software Group, is a trusted, competitively priced, and easy-to-use on-premises virtualization solution. For the last two decades, XenServer has enabled customers of all sizes to virtualize their workloads using the XenServer bare-metal hypervisor. Visit xenserver.com to see what XenServer can do for your business.

Avoiding Resource Exhaustion During Abnormal System Load

Denial-of-service attacks (DoS attacks) are attempts to saturate a system's resources to suspend services of a host connected to the Internet. Often this is done by attempting to saturate the target system with external communication requests to the extent that the target cannot respond and becomes unavailable. Typical targets may include web sites associated with financial transactions, including banks, credit card, and ecommerce sites.

Recommendation

We recommend configuring sufficient CPU and memory resources to support the expected load of business critical VMs. There are two key principles to consider:

- Ensure that a VM is provisioned with sufficient virtual resources to carry out its expected workloads.
- Ensure that a VM is not overprovisioned so that in abnormal conditions it is not capable of consuming an unreasonable proportion of the host resources.

Recommendation

We recommend that you do not assign so much resource to one VM that, under its maximum load, it precludes other business-critical VMs from running.

Recommendation

We recommend that your configuration is sufficient to avoid the "domino" effect where the unavailability of one host or VM puts sufficient load on others that they in turn fail to be sufficiently responsive.

You can allocate CPU and initial memory resources to the new VM during VM creation or after the new VM is installed, if required. Specifically, you can allocate a number of virtual CPUs to a VM and set a priority for the VMs access to physical CPU resources on the host.

You can adjust the memory allocation either when a VM is created in the XenCenter **New VM** wizard, by changing it from the default, or after the new VM is created on the VM's **Memory** tab.

Naming and tagging VMs

Recommendation

If your organization does not have a policy on naming, we recommend naming VMs clearly using meaningful names.

For example, indicate specific properties of significant VMs (for example, "-HR-server" or "-finance-server").

Recommendation

We recommend tagging VMs to group VMs with similar characteristics. For example, tags of "migrateable" or "missioncritical" can then be used in XenCenter searches to reduce the risk of accidentally operating on the wrong VM.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY
XenServer, a business unit of Cloud Software Group, is a trusted, competitively priced, and easy-to-use on-premises virtualization solution. For the last two decades, XenServer has enabled customers of all sizes to virtualize their workloads using the XenServer bare-metal hypervisor. Visit xenserver.com to see what XenServer can do for your business.

Securing Resource Pools

When multiple hosts are grouped together in resource pools, the pool has a pool coordinator host that controls the other hosts. All management communication between pooled hosts is done over TLS; hosts authenticate using a randomly generated secret that is created when you form the pool.

Recommendation

We recommend physically isolating the management traffic and segregating it from other non management traffic.

However, if this is not possible, We recommend logically isolating the management traffic from other non-management traffic.

One method of logically isolating this management traffic is to use VLANs. You can configure your routers to tag all traffic from the management interfaces in the pool with a VLAN tag dedicated to this purpose.

If you decide to configure a VLAN for management traffic, be aware that remote clients such as XenCenter will need to connect to the management network VLAN.

Creating Pools

Consider the security requirements of the workloads you want to run on the pool.

Recommendation

We recommend, if workloads must be run on hosts that require a specific level of physical security, you consider creating pools that contain hosts in one physical location only. That is, do not design a pool that has hosts in one physical location that is less secure than another physical location.

Using Live Migration Features

When using live migration features, such as Workload Balancing and High Availability, it is important to be aware of the sensitivity of the data on the virtual machines. Live migration can potentially change:

- The host on which a VM resides
- The groupings of VMs on hosts

For example, if you enable automation in Workload Balancing so that it applies optimization recommendations automatically, it is possible for a VM to move to a host without you being aware of it. (In fact, this is the expected and desirable behavior of the feature.)

As a result of automation, if pools contain hosts in multiple physical locations, Workload Balancing could move a VM containing highly sensitive data to a host in a server room that is not physically secured to the required level.

Recommendation

We recommend, if you want to enable any live migration (for example, caused by Workload Balancing, High Availability or Rolling Pool Upgrade) features in the pool, ensure that all

workloads can be run securely on hosts in all of the physical locations the pool encompasses, including the physical security of the premises in which the hosts are located. See also Using Live Migration Features.

Also, be aware that features, such as Workload Balancing and High Availability, can change the host on which a VM resides.

Recommendation

We recommend using any of the following to address live-migration requirements:

- Designing pools from hosts that meet a common level of logical and physical security requirements
- Not enabling automation features in Workload Balancing
- Enabling automation in Workload Balancing, but excluding hosts from live migration

Recommendation

We recommend that, if you want to enable any live migration (Workload Balancing, High Availability) features in the pool, ensure that all workloads can be run securely on hosts on all of the physical locations the pool encompasses, including the physical security of the room in which the hosts are located.

Recommendation

We recommend, in some cases, excluding specific hosts from Workload Balancing if you want to ensure that specific workloads are never run on the same system. Likewise, you could run those workloads in different pools.

Features, such as Workload Balancing and High Availability, can change the host on which a VM resides.

Chapter 5: Deploying XenServer Hosts

In this chapter:

- An overview of preparing the host server.
- Guidance about installing XenServer in a secure manner so you do not inadvertently introduce vulnerabilities during installation
- Guidance to consider before deploying hosts.
- Information about creating secure templates.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY

Preparing the host server

It is important to ensure that, prior to installing XenServer, your hardware has been updated in accordance with your hardware vendor's recommendations.

Recommendation

We recommend that you apply all firmware (BIOS/UEFI) updates recommended by your hardware vendor prior to installing XenServer.

Recommendation

We recommend that you ascertain how your hardware vendor will inform you of future security and stability updates to their firmware.

Installing XenServer

When installing XenServer, it is important to be aware of best practices that can help ensure your deployment remains secure. These practices include:

- Checking the integrity of downloaded installation files.
- Waiting to connect (cable) hosts to physical networks until all hosts are configured. All of these considerations are described in more detail in the sections that follow.

Installation Media

It is important to ensure that the XenServer installation media you are using is a genuine copy from the XenServer downloads page.

Recommendation

We recommend the following for customers downloading XenServer installation media:

1. Downloading the XenServer installation files only from the secured xenserver.com site.
2. Before installing XenServer, check the integrity of the downloaded installation files. Verify the download against the secure checksum information on the XenServer download page. The checksum information lets you verify that the image you downloaded or obtained has not changed from the way in which we packaged it.

Checking the Integrity of Downloaded ISO Files

Recommendation

We recommend verifying the integrity of downloaded ISO files.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY
XenServer, a business unit of Cloud Software Group, is a trusted, competitively priced, and easy-to-use on-premises virtualization solution. For the last two decades, XenServer has enabled customers of all sizes to virtualize their workloads using the XenServer bare-metal hypervisor. Visit xenserver.com to see what XenServer can do for your business.

This section provides examples of how you can verify the integrity of downloaded ISO files for Windows and Linux. There are several different ways of accomplishing this task. The instructions are provided as an example.

To verify the integrity of the ISOs on Windows

1. At a Windows command line, type the following command:

```
certutil -hashfile XenServer8_YYYY-MM-DD.iso SHA256
```

2. Compare the checksum output to the checksum information on the XenServer download page.

   Note: It is important to compare the full length of the checksum and not just a few characters.

To verify the integrity of the ISOs on Linux

1. Log in, or open a console, to display a shell prompt.
2. At the prompt, type the following command:

```
% sha256sum XenServer8_YYYY-MM-DD.iso
```

3. Compare the checksum output to the checksum information on the XenServer download page.

Note: It is important to compare the full length of the checksum and not just a few characters.

Network installation

Recommendation

We recommend that if you are installing from a PXE boot server, you use a server that you trust.

In practice, this means that you should make sure that you connect to the PXE boot server over the management network and not the guest network. As previously discussed, this is to prevent a tenant PXE server with malicious XenServer installations from impersonating your PXE server.

Before Deploying Hosts

Before deploying a XenServer host or pool, we recommend performing both of the following:

- Verifying you configured your physical networks and VLANs as you expected
- Verifying the identity of a host

Recommendation

We recommend that before you put a pool into production, you double-check that your networks are configured and isolated as you expect. If you separated the different types of traffic from each other, check to make sure that you successfully isolated each traffic type.

For example, you might consider monitoring network traffic, examining network port activity lights (if present) and, if your network numbering and masking permits, trying to ping a device across networks.

You should check for isolation for each guest network, the management network and any IP-based storage networks.

Recommendation

We recommend that you do not cable the host, when installing XenServer, beyond connecting it to the management network – until you have all the host networks configured and the correct security policies in place.

Recommendation

We recommend that you ensure you have physically and logically isolated the management network through cabling and configuration before physically plugging the host in to the guest network where it may be exposed to potentially hostile traffic. This is particularly true in environments where the users and administrators of the guest VMs are unknown and may have malicious intent.

Recommendation

We recommend that, if you have a bare metal machine and you are booting it off the network using a boot server (for example, a PXE installation), take steps to validate the identity of the installation server before proceeding with installation.

This is particularly true in environments where a malicious guest VM could have a PXE server that you unwittingly connect to when performing installation.

- We recommend that you configure your host's BIOS to only use trusted network interfaces for PXE boot.

Adding Hosts to Pools

Recommendation

We recommend that you follow the previous advice when adding new hosts to an existing pool, with the following difference:

When adding hosts to a pool, do not connect to the guest networks until after:

1. You add the host to the pool
2. The pool coordinator is finished replicating the pool networks on the new host

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY

Creating Secure Templates

A template that was created with only one use case in mind might be re-used for many other VMs with differing security requirements.

Recommendation

We recommend that you take extra care when creating VMs for replication (as templates) to ensure that the configurations are suitable for all potential uses of the VM.

Recommendation

We recommend that you ensure that when you create templates, you do not unintentionally include data such as user accounts and data, in particular secrets such as SSH keys.

Recommendation

We recommend that templates are named so as to indicate their intended purpose (for example, to avoid using an experimental template for a production VM, specify “-test” as part of their name).

Recommendation

We recommend that if you are going to create VMs from a template, when you build your templates, you should make sure the template does not include any unnecessary or undesirable networks.

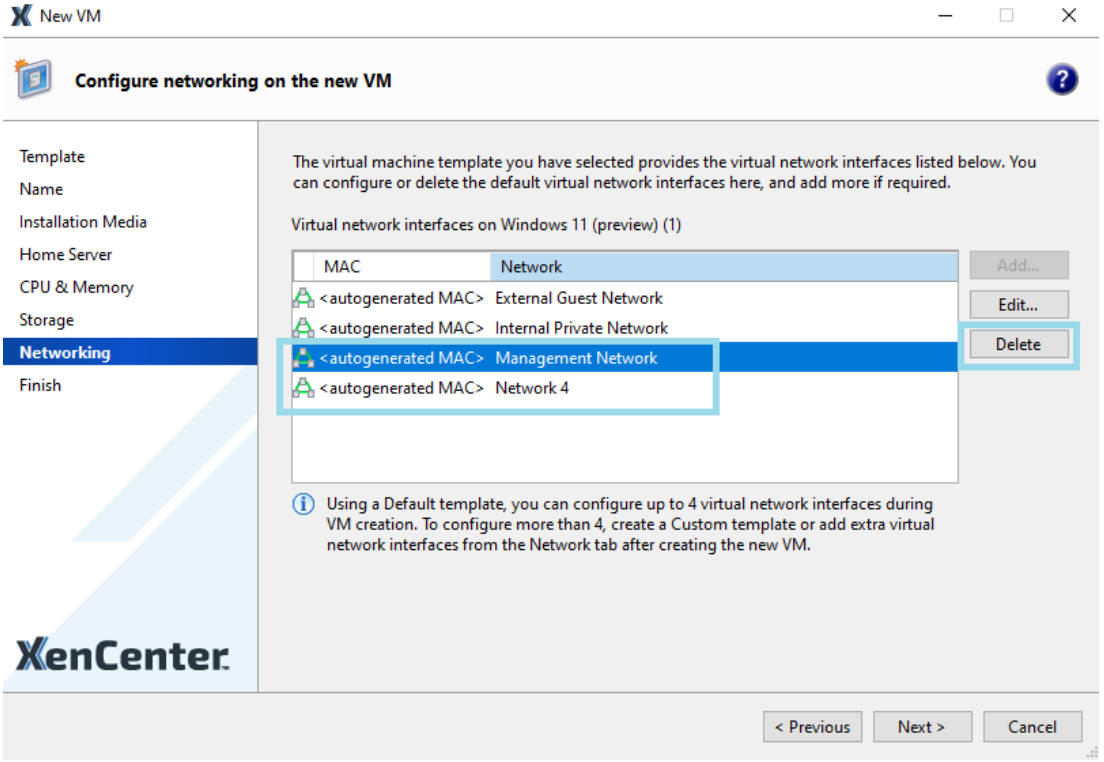
Recommendation

We recommend that you do not assign unnecessary network ports to each guest.

For example, when initially making the VM from which you want to generate the template, verify you do not create virtual network interfaces for all of the networks (NICs) available on your host.

The following image shows the screen where you can delete unnecessary network ports from VMs.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY
XenServer, a business unit of Cloud Software Group, is a trusted, competitively priced, and easy-to-use on-premises virtualization solution. For the last two decades, XenServer has enabled customers of all sizes to virtualize their workloads using the XenServer bare-metal hypervisor. Visit xenserver.com to see what XenServer can do for your business.



In the **Create New VM** wizard, when you are creating a new VM for use as a template, delete any unused networks to prevent the wizard from creating virtual network interfaces for them.

Recommendation

We recommend that you ensure that VM templates are considered as part of your organization's patching schedule.

Accessing XenServer Hosts and Using Certificates

Each XenServer host generates a set of random cryptographic key-pairs when it is installed. Each key-pair is split into two portions: a public key that is displayed to clients, and a private key that is only known to the host and can be used to prove that it is the owner of the public key.

The XenServer host generates two classes of keys: one for the Secure Shell (SSH) protocol and a second for the management API TLS network service. SSH is only used for advanced configuration of the control domain and should not be needed in normal use. The management API TLS communication path is used much more often (for example, by XenCenter).

The main use of these keys is to confirm that you are connecting to the correct host.

Adding Hosts to XenCenter Securely

Recommendation

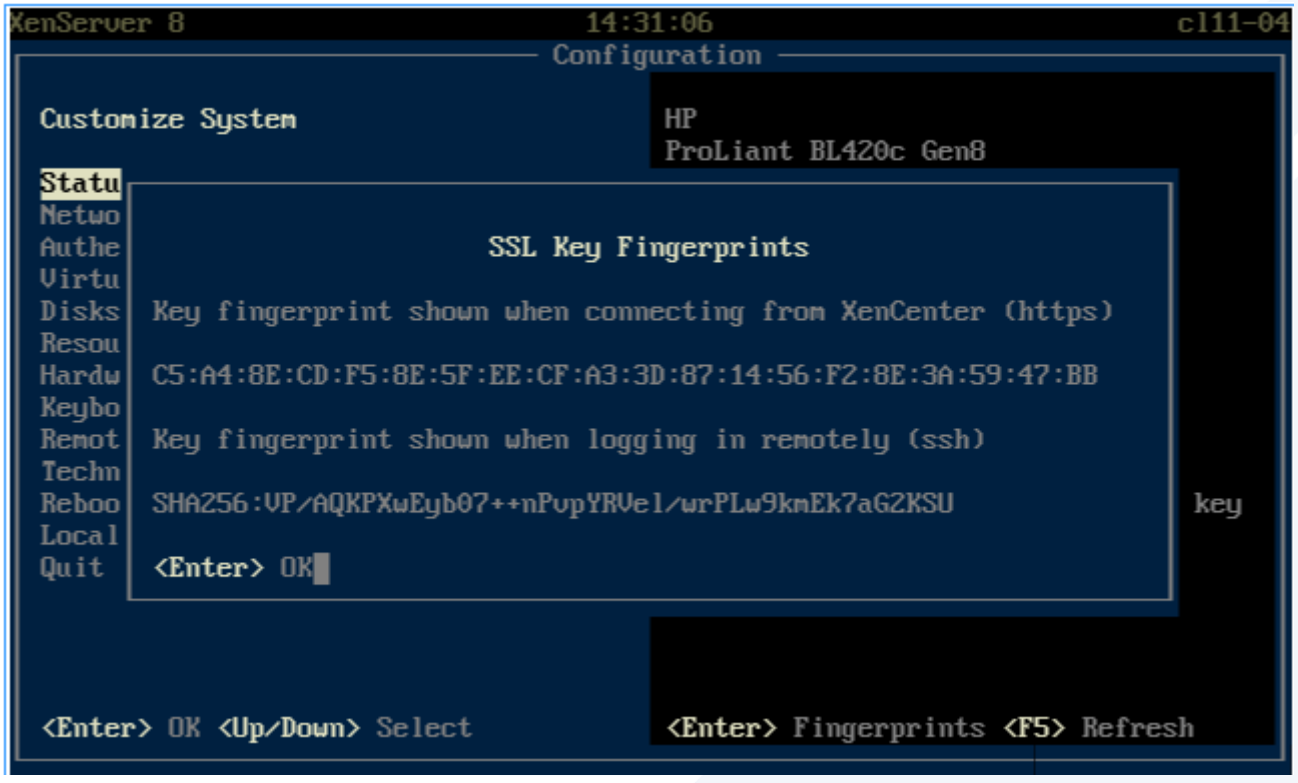
We recommend verifying that, when you add a host to XenCenter, the host you are adding is not being impersonated. Perform the steps in the procedure that follows to make sure you are not under a man-in-the-middle attack by an attacker trying to impersonate a XenServer host.

To verify you are not connecting to an impersonated host, obtain the TLS key for the host before adding the host to XenCenter. After noting the key, when you add the host to XenCenter, you can compare it to the key XenCenter displays when you add the host. After XenCenter connects to a host for the first time, XenCenter stores the TLS key and associates it with the host record. If the host key changes (for example, the host is upgraded or reinstalled), a warning appears showing the new host key.

Note: The terms thumbprint and fingerprint are used interchangeably throughout this section.

To obtain the TLS key fingerprint for a host

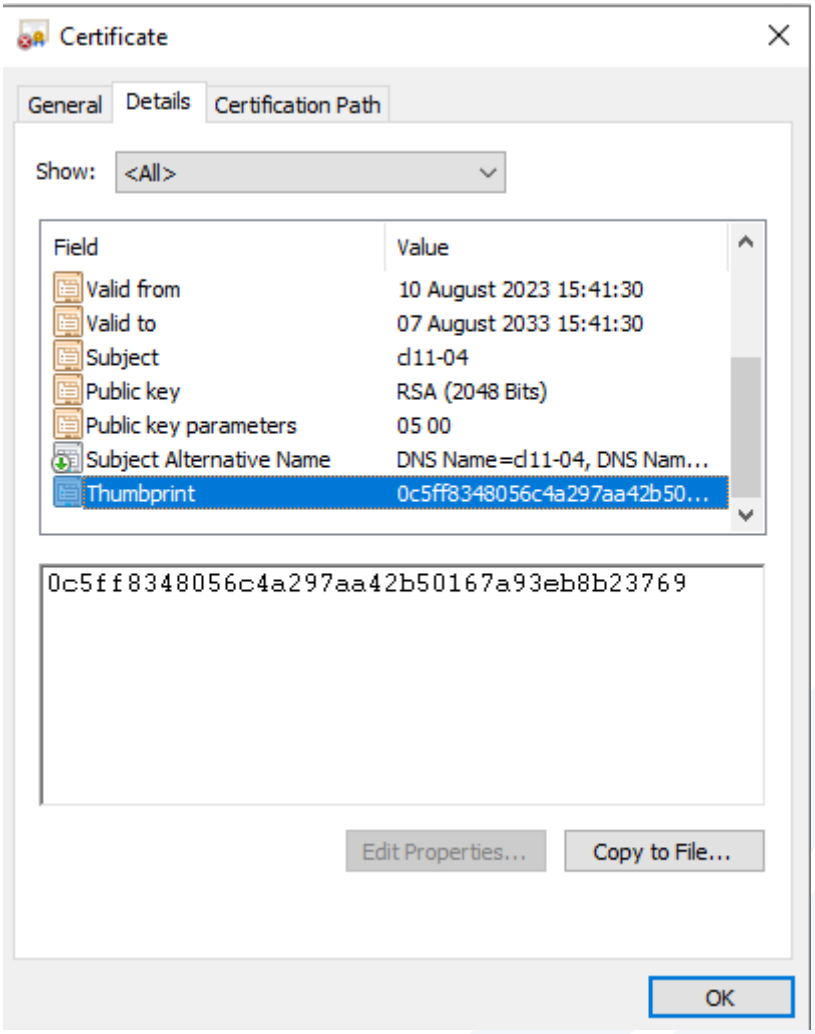
1. At the physical host, open the xsconsole by typing `xsconsole` at the command prompt.
2. Open the **Status Display**. Note the SSL Key Fingerprint for https that appears in the console.



101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY

To verify the host's identity when you add it to XenCenter

1. Add the host to XenCenter (**Server > Add**).
2. In the **New Security Certificate** dialog that appears, click **View Certificate**.
3. In the **Certificate** dialog that appears, click **Details**.
4. Scroll down to the **Thumbprint** field and select it.

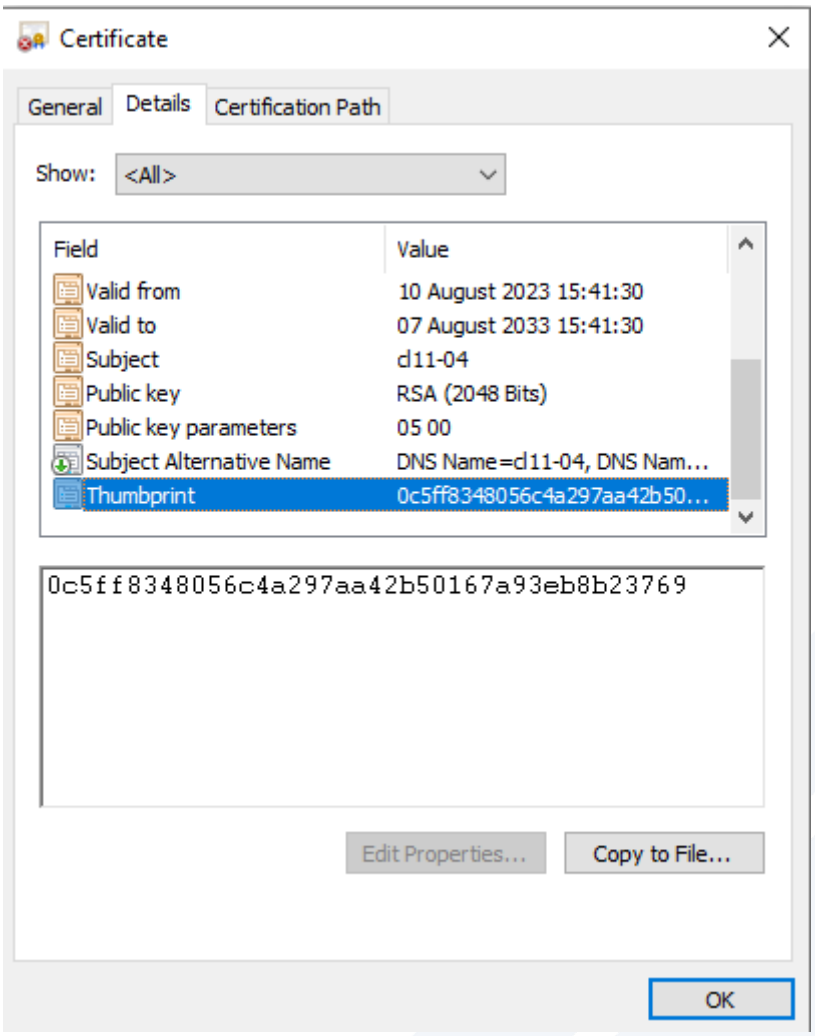


5. If desired, click **Copy to File** to copy the thumbprint to the clipboard.
6. If you copied the thumbprint, click **OK** to exit the dialog. The **New Security Certificate** dialog appears.
7. Compare the TLS key fingerprint XenCenter displays to the one you noted at the host console. If the two fingerprints do not match, click **Cancel** in the dialog box and investigate why the host XenCenter is connecting to is not the same host as the one you believe were adding.

Note: It is important to compare the full length of the fingerprint and not just a few characters.

To verify the TLS key fingerprint

1. In the **Security Certificate Changed** dialog, click **View Certificate**.
2. In the **Certificate** dialog box, click the **Details** tab.
3. Scroll down towards the bottom of the fields list and select the **Thumbprint** field.



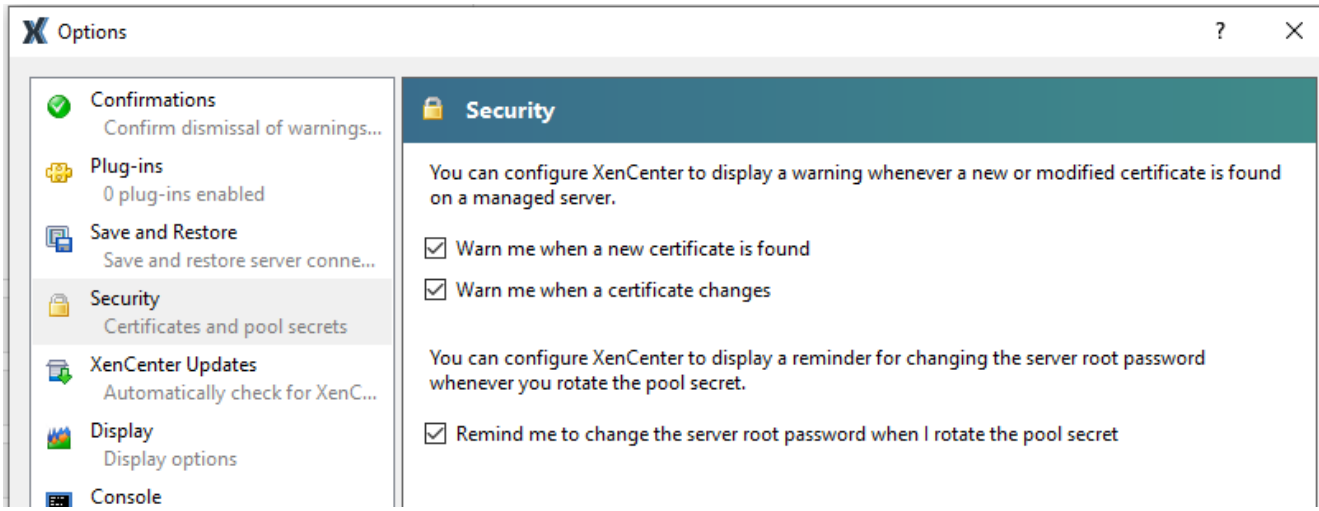
4. If desired, click **Copy to File** to copy the thumbprint to your clipboard.

To display a warning for new or modified TLS certificates on hosts

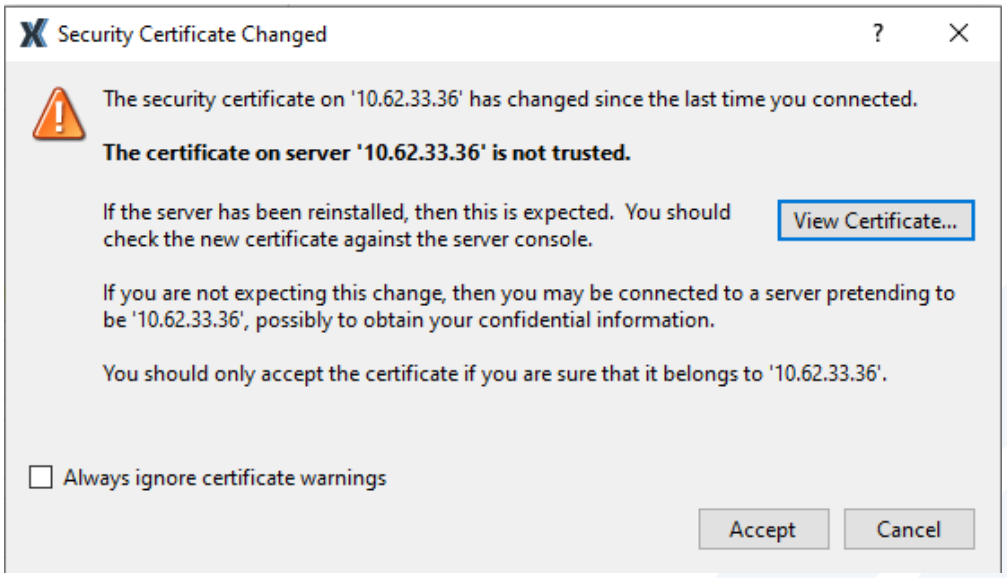
1. In XenCenter, in the **Tools** menu, select **Options**.

2. In the left-hand pane, select **Security**.

3. Select **Warn me when a new certificate is found** and **Warn me when a certificate changes.**



When a certificate changes, you see the following message:



Configuring Trusted Certificates for XenServer Hosts

Recommendation

We recommend replacing self-signed certificates with certificates from a trusted certificate authority to reduce the risk of malicious servers impersonating your hosts.

Recommendation

We recommend, for XenServer customers running Citrix Virtual Desktops workloads, using HTTPS to secure communication between Desktop Delivery Controller and XenServer. To

use HTTPS, you must replace the default TLS certificate installed with XenServer with one from a trusted certificate authority that is also trusted by the Desktop Delivery Controller.

For information about configuring XenServer certificates see the topic Install a TLS certificate on your server in the product documentation.

Decommissioning Systems

Decommissioned hosts may contain sensitive data on VMs.

Recommendation

We recommend completely erasing all data on local disks when decommissioning hosts containing sensitive data or that are part of highly secured environments.

Recommendation

We recommend that, when removing hosts, you also remove any access that has been granted by switches, storage backends etc. based on the removed host's MAC addresses or HBA identifiers.

Reusing Physical Servers

Recommendation

We recommend that you completely wipe and reimage hosts before reusing them in your environment; hosts may contain traces of sensitive data, passwords, or viruses.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY
XenServer, a business unit of Cloud Software Group, is a trusted, competitively priced, and easy-to-use on-premises virtualization solution. For the last two decades, XenServer has enabled customers of all sizes to virtualize their workloads using the XenServer bare-metal hypervisor. Visit xenserver.com to see what XenServer can do for your business.

Chapter 6: Managing XenServer VMs

In this chapter:

- Information about managing snapshots, backups, and archives.
- Information about managing dormant virtual machines.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY

Managing Snapshots, Backups, and Archives

Recommendation

We recommend that you consider if there is potentially sensitive data on the VM before configuring VM snapshots, backups, archives, or disaster recovery. Specifically, when you create the extra copy, be aware of the storage array's security level, physical security, and who can access it.

Recommendation

We recommend, if VM snapshots include sensitive data, applying the same level of security to all aspects of the archival or backup process as you would to the VM. For example, ensure the following are secured appropriately: the storage array for the snapshots or archives and the network used to send the archives.

Recommendation

We recommend, when configuring scheduled snapshots of VMs using the CLI or backed up VMs using Disaster Recovery, carefully reviewing the RBAC roles assigned to administrators. Be aware of which administrators may be able to access the snapshots and mirrored Disaster Recovery site.

- Any administrator assigned an RBAC role of Pool Admin, Pool Operator, or VM Power Admin can start a snapshot taken from any VM in the pool (for which they have that role).

Recommendation

We recommend, when backing up copies of VMs for storage, ensuring VMs containing sensitive information are backed up in a location with sufficient logical and physical security. In some cases, you may need to back up VMs containing sensitive data to a different location or configure different disaster recovery settings for sensitive VMs.

Scanning for Malware

Recommendation

We recommend avoiding simultaneous virus scans on VMs.

Running simultaneous security scans on multiple VMs on a host can cause unnecessary spikes in resource usage. Unlike physical servers that typically have excess resource capacity, hosts are often run at maximum VM density so unexpected processes can potentially cause overloads – especially if features like Workload Balancing, which can balance virtual-machine loads across hosts, are not configured.

We recommend that, if supported, you configure your virus scanner to scan VMs randomly or download updates to VMs at different times. Some anti-virus applications have virtualization-aware features to help mitigate these issues.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY
XenServer, a business unit of Cloud Software Group, is a trusted, competitively priced, and easy-to-use on-premises virtualization solution. For the last two decades, XenServer has enabled customers of all sizes to virtualize their workloads using the XenServer bare-metal hypervisor. Visit xenserver.com to see what XenServer can do for your business.

Managing Dormant Virtual Machines

Recommendation

We recommend deleting any dormant, inactive VMs or actively monitoring, managing, securing, and including them in update cycles. Otherwise, they may potentially provide easy access to the environment.

Recommendation

We recommend, when applying security updates, do not overlook VMs that are shut down or suspended. Failing to update any layer of software (for example, guest operating systems or workload applications), may leave security vulnerabilities and holes.

Dormant VMs should be tracked and included in all security policies and updates.

Consider the following:

- Dormant virtual machines may contain sensitive data, such as credit card transactions or employee social-security numbers.
- Dormant VMs may not be included in the latest access policies, may not have the latest virus software, and may be inadvertently omitted from monitoring and virus updates. Consequently, organizations may believe their environments are secure when in reality they are vulnerable to known threats, which they believe they addressed.

Recommendation

We recommend, depending on the risk profile of your environment (that is, if it has potentially dangerous or hostile traffic), if you must start a dormant VM that may be lacking significant security updates, start that VM on a network with restricted connectivity until the VM has a full complement of security updates.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY

Chapter 7: Managing XenServer Administrators

In this chapter:

- An overview of the XenServer role-based access functionality
- Recommendations for separating administrative responsibilities
- An overview of the XenServer Role Based Access Control (RBAC) functionality
- Definitions of the RBAC roles and permissions

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY

Separating Administrative Responsibilities

Recommendation

We recommend providing administrative access to XenServer through its Role Based Access Control (RBAC) feature. The RBAC feature lets you use the Active Directory accounts for administrators and assign levels of access to these accounts (through roles). Assigning role-based access lets you troubleshoot and monitor administrative activity through audit logging.

Ensuring each administrative tier is available only to appropriately authorized people helps avoid unintentional and intentional unauthorized changes, which can potentially affect the stability of physical hosts and VMs and the associated cost of resulting system outages.

If not in place already, consider separating administrative responsibilities for your virtualized environment, possibly based on the ones suggested by the predefined XenServer RBAC roles, and then defining which RBAC roles or people will be associated with which responsibilities.

The product documentation provides detailed information about configuring RBAC.

Recommendation

We recommend, before deploying RBAC, familiarizing yourself with the RBAC feature and understanding the division of responsibilities between the roles. Make sure you understand what tasks each role can perform and the data of which each role has visibility.

Do not assign roles solely based on their titles.

Recommendation

We recommend matching the assignment of roles to your organizational security policy.

Recommendation

We recommend carefully reviewing access policies and roles because access to the hypervisor can enable access to key infrastructure components, such as network switches and firewalls, as well as sensitive hosted applications and workloads.

Recommendation

We recommend, when making RBAC assignments, carefully reviewing the RBAC roles assigned to administrators in relation to the VM snapshots.

Any administrator assigned an RBAC role of Pool Admin, Pool Operator, or VM Power Admin can start a snapshot taken from any VM in the pool (for which they have that role).

Recommendation

When using RBAC, it is important to remember that a root account (that is, the local super-user account) still exists.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY
XenServer, a business unit of Cloud Software Group, is a trusted, competitively priced, and easy-to-use on-premises virtualization solution. For the last two decades, XenServer has enabled customers of all sizes to virtualize their workloads using the XenServer bare-metal hypervisor. Visit xenserver.com to see what XenServer can do for your business.

We recommend, in accordance with your organizational security policy, that you keep the root account password secure. You may want to store the root account password in a physically secure location with restricted access. (For example, you could store the root account password in safe or safety deposit box, where nobody has routine access, but a suitably authorized person could retrieve the password in the event of an emergency).

There are two approaches to implementing XenServer administrative accounts with RBAC:

- You could use the same account for XenServer administration as you use for other company activities (for example, email, network access, and so on). This is usually undesirable as it increases the opportunities for the account to become compromised and also increases the scope of potential impact if the account is compromised.
- You could create separate Active Directory accounts with a different user name solely for XenServer administration.

Recommendation

We recommend that when you implement RBAC you consult your organizational security policy to determine if you should create separate Active Directory accounts that are only used for XenServer administration. If you have don't have such a policy, We recommend that you create separate accounts for XenServer administration.

Recommendation

We recommend considering business continuity when using the RBAC feature.

Take steps to ensure that you can still access XenServer if the person assigned the Pool Admin role is no longer available. This might involve ensuring:

- More than one person is assigned an individual Pool Admin accounts
- The root account password is stored in a secure restricted location with protocols to access it in the event of an emergency in accordance with your organizational security policy

Recommendation

We recommend that when you implement RBAC in your environment you be aware that you are ultimately trusting the Active Directory administrator to control access to your environment.

- Whoever has the ability to control Active Directory accounts also has the ability to access those accounts and by extension access the XenServer environment
- The Active Directory administrator can inadvertently create a denial of service situation by unwittingly disabling accounts (for example, if the organizational security policy changes and the administrator changes the properties of the Active Directory accounts)

Consider how you will gain access to the XenServer environment if the Active Directory administrator inadvertently disables the XenServer Pool Admin account, and there is only one such account.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY
XenServer, a business unit of Cloud Software Group, is a trusted, competitively priced, and easy-to-use on-premises virtualization solution. For the last two decades, XenServer has enabled customers of all sizes to virtualize their workloads using the XenServer bare-metal hypervisor. Visit xenserver.com to see what XenServer can do for your business.

We recommend that you do not share RBAC accounts. If you do, your ability to trace the owner of changes in the audit log will be compromised.

Role Based Access Control (RBAC) Overview

XenServer's Role Based Access Control (RBAC) lets you assign predefined roles, or sets of XenServer permissions, to Active Directory users and groups. These permissions control the level of access XenServer users (that is, people administering XenServer) have to servers and pools: RBAC is configured and deployed at the pool level. Because users acquire permissions through their assigned role, you simply need to assign a role to a user or their group.

Using Active Directory accounts for XenServer user accounts, RBAC lets you restrict which operations different groups of users can perform which reduces the likelihood of inexperienced users making disastrous, accidental changes. Assigning RBAC roles also helps meet compliance requirements by preventing unauthorized changes to your resource pools. To facilitate compliance and auditing, RBAC also provides an Audit Log feature and its corresponding Workload Balancing Pool Audit Trail report.

RBAC depends on Active Directory for authentication services. Specifically, XenServer keeps a list of authorized users based on Active Directory user and group accounts. As a result, you must join the pool to the domain and add Active Directory accounts before you can assign roles.

Local Super-User

The local super-user, or root, is a special user account used for system administration and has all rights or permissions. In XenServer, the local super-user is the default account at installation. The local super-user is authenticated by XenServer and not an external authentication service. This means that if the external authentication service fails, the local super-user can still log in and manage the system. The local super-user can also access the XenServer physical server through SSH if SSH is enabled.

RBAC Roles

XenServer comes with six pre-established roles that are designed to align with different functions in an IT organization.

- **Pool Administrator (Pool Admin)**. This role is the most powerful role available. Pool Admins have full access to all XenServer features and settings. They can perform all operations, including role and user management. They can grant access to the XenServer console. As a best practice, We recommend assigning this role to an extremely limited number of users.

  Note: The local super user (root) always has the Pool Admin role. The Pool Admin role has the same permissions as the local root.

- **Pool Operator (Pool Operator)**. This role is designed to let the assignee manage pool-wide resources, including creating storage, managing servers, managing patches, and creating pools. Pool Operators can configure pool resources. They also have full access to the following features: High Availability (HA), Workload Balancing, and patch management. Pool Operators cannot add users or modify roles.

- **Virtual Machine Power Administrator (VM Power Admin)**. This role has full access to VM and Template management. They can choose where to start VMs. They have full access to the dynamic memory control features and the VM snapshot feature. In addition, they can set the Home Server and choose where to run workloads. Assigning this role grants the assignee sufficient permissions to provision virtual machines for VM Operator use.

- **Virtual Machine Administrator (VM Admin)**. This role can manage VMs and Templates and access the storage necessary to complete these tasks. However, this role relies on XenServer to choose where to run workloads and must use the settings in templates for dynamic memory control and the Home Server. (This role cannot access the dynamic memory control features, make snapshots, set the Home Server or choose where to run workloads.)

- **Virtual Machine Operator (VM Operator)**. This role can use the VMs in a pool and manage their basic lifecycle. VM Operators can interact with the VM consoles and start or stop VMs, provided sufficient hardware resources are available. Likewise, VM Operators can perform start and stop lifecycle operations. The VM Operator role cannot create or destroy VMs, alter VM properties, or server resources.

- **Read-only (Read Only)**. This role can only view resource pool and performance data.

  For information about the permissions associated with each role, see the product documentation.

Chapter 8: Monitoring for Security Updates

In this chapter:

- Information about monitoring for security updates to XenServer.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY

XenServer Security Updates

We continually release updates for the XenServer family of products, including updates that address security issues. We recommend that customers monitor the availability of new updates and apply them to their installations.

You can find information about whether there are pending updates for your systems on the XenCenter UI.

Recommendation

We recommend subscribing to XenServer Security Bulletins. These are listed at http://support.citrix.com/securitybulletins/ where the “My support alerts” option in the account pull-down lets you register to receive email alerts when we release security bulletins and updates. Alternatively, Atom and RSS feeds of security alerts are published at https://support.citrix.com/feeds.

Recommendation

We recommend selecting the Notifications tab in XenCenter when events are flagged and examining the relevant Alerts and Updates.

Recommendation

We recommend regularly applying any pending XenServer updates to your systems. However, we recommend expediting this when a security bulletin is published. After a security bulletin is published, the security vulnerability becomes publicly known. This principle also applies to any guest operating systems and any application workloads.

Many updates make use of XenServer’s Live Patching feature to minimize the disruption caused by updating.

Recommendation

When deploying updates, consider whether the updates make use of the Live Patch functionality and if that can expedite deployment.

Recommendation

We recommend following your hardware manufacturer’s guidance on applying any relevant firmware updates.

101 Cambridge Science Park, Milton Rd, Cambridge UK, CB4 0FY
XenServer, a business unit of Cloud Software Group, is a trusted, competitively priced, and easy-to-use on-premises virtualization solution. For the last two decades, XenServer has enabled customers of all sizes to virtualize their workloads using the XenServer bare-metal hypervisor. Visit xenserver.com to see what XenServer can do for your business.