ESXi 7.0 Build

Document for Telefonica UK

# Control Page

|  |  |
| --- | --- |
| **Control Information** | |
| Author / Editor | Sakthivel Rajendran |
| Document Name | ESXi 7.0 build document for Telefonica UK |
| Date | 05.12.2018 |
| Role | Senior Wintel administrator |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Change History Information** | | | | |
| Current Version | | 0.3 | | |
| **Version** | **Date** | **Changed By** | **Section** | **Changes** |
| 0.1 | 05.02.2018 | Sakthivel Rajendran | All | Draft version |
| 0.2 | 31.10.2019 | Subash Subbiah | Section 17 | updated CIS hardening details |
| 0.3 | 13.1.2023 | Vinoth | All | No Changes |
| 0.4 | 09.02.2023 | Samydurai | Summary | Standard build image privacy comments added in summary section |
| 0.5 |  |  |  |  |
| 1.0 |  |  |  |  |
| 1.1 |  |  |  |  |
| 1.2 |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **Related/Referenced Documents** | | |
| **Name** | **Description** | **Version** |
| ESXi Build Document  <https://groupshare.pri.o2.com/sites/cl/Network%20and%20Server%20Support%20Home%20Page/Shared%20Documents/Forms/AllItems.aspx?RootFolder=%2fsites%2fcl%2fNetwork%20and%20Server%20Support%20Home%20Page%2fShared%20Documents%2fBuild%20Documentation&FolderCTID=&View=%7b3786BD07%2d3C69%2d40BC%2d8BBE%2d5C8A9C4B11CE%7d> | ESXi 5.1 build design guide | 1.0 |
|  | Operational acceptance check list |  |
|  | TUK Security Standards Exception Form-2015 - VMWARE ESXi 5.5 |  |

|  |  |  |
| --- | --- | --- |
| **Distribution List** | | |
| **Name** | **Role** | **Representing** |
| Ifthar Ahmed | Telefonica IT E&D Architecture | Telefonica |
| Subash Subbiah | TCS Infrastructure Design | TCS |
| Williams Stephen | TCS Build Governance | TCS |

|  |  |  |  |
| --- | --- | --- | --- |
| **Distribution History** | | | |
| **Sent To** | **Sent By** | **Date** | **Version** |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Approval List** | | | |
| **Name** | **Role** | **Representing** | **Date** |
| Iain Radford | Telefonica IT E&D Architecture | Telefonica |  |
| Ifthar Ahmed | Telefonica IT E&D Architecture | Telefonica |  |
|  |  |  |  |

|  |  |
| --- | --- |
| **Annual Review** | |
| **Name** | **Date** |
|  |  |
|  |  |
|  |  |
|  |  |

# Summary

This document details the process to follow in order to build an ESXi server in accordance with best practice for acceptance onto the O2 CDN.

Golden images and build documents solely prepared for VMO2 purposes and should not be supplied outside of the VMO2 environment.

Any user access provision other than default common tool users always enabled based on respective design approval.

# Purpose

The purpose of this document is to provide a consistent and reliable mechanism for building servers in the O2 estate, based on the VMware ESXi platform. It will also document the post operating system procedures that must be followed in order to achieve a smooth transition into operational acceptance.

# Scope

The scope of this document includes the tasks required to successfully build an ESXi Server, installing additional Monitoring (SCOM) toolsets. It does not cover all the tasks required to successfully pass operational acceptance, such as the CIS and Qualys process for example.

# Relationship to Other Documents

This document is intrinsically linked to the Project Design Document and Operational Acceptance documentation. If a server is built using this build document, the Operational Acceptance process should be much improved for all parties.

It is also linked to documentation covering the processes of installing additional applications such patching and monitoring tools.

# Update Process

The process for updating this document is as follows:

* The document will be updated as requested
* The document will then be sent for internal review to those individuals in the distribution section at the top of this document
* Once review has been successfully completed, the new document will be published

# Build Process

This document specifies the configuration of any new server build within the estate but is only the first part of the server build process. The build process can be defined as follows:

## Deployment of build image

New physical ESXi host should be deployed using OEM Custom ISO. Should it be necessary to deploy a new build from OEM Custom ISO media then this document should be followed to produce a consistent build.

Ex.

DELL physical server – Dell custom ESXi image

HP Physical Server – HPE Custom ESXi Image

## Hardware Configuration

**Blade Server**:

* Apply the relevant firmware (so consistent with other nodes in the cluster).
* Configure the BIOS settings as per the design documentation.
* RAM tests the server (24 hours as a minimum).
* Configure Virtual Connect server profile
* Apply the host profile or do the configuration depending on cluster.
* Install ESXi as per build document

**Rack Server:**

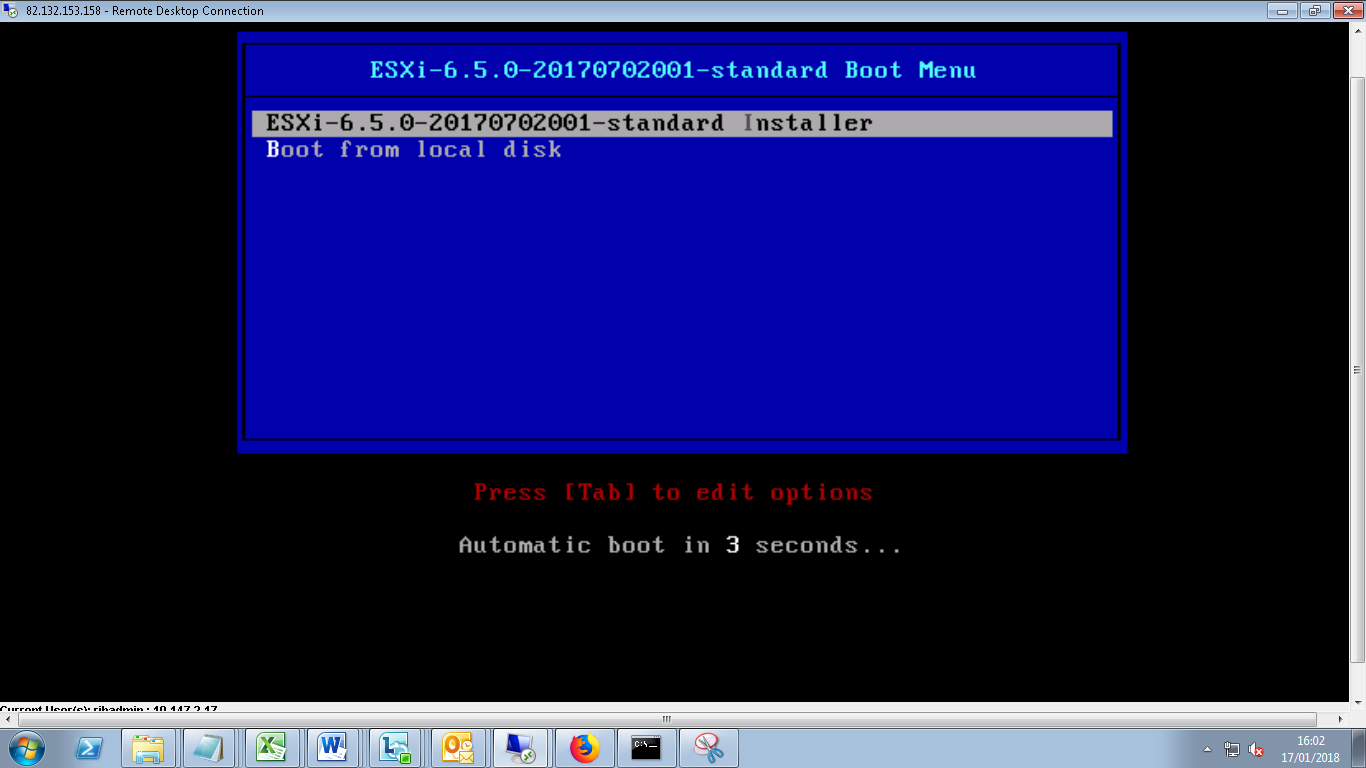
* Apply the relevant firmware (so consistent with other nodes in the cluster).
* All ESXi Hosts must have VT enabled from the BIOS.
* vmnic Detection order should be similar in all hosts.

## Disk Configuration

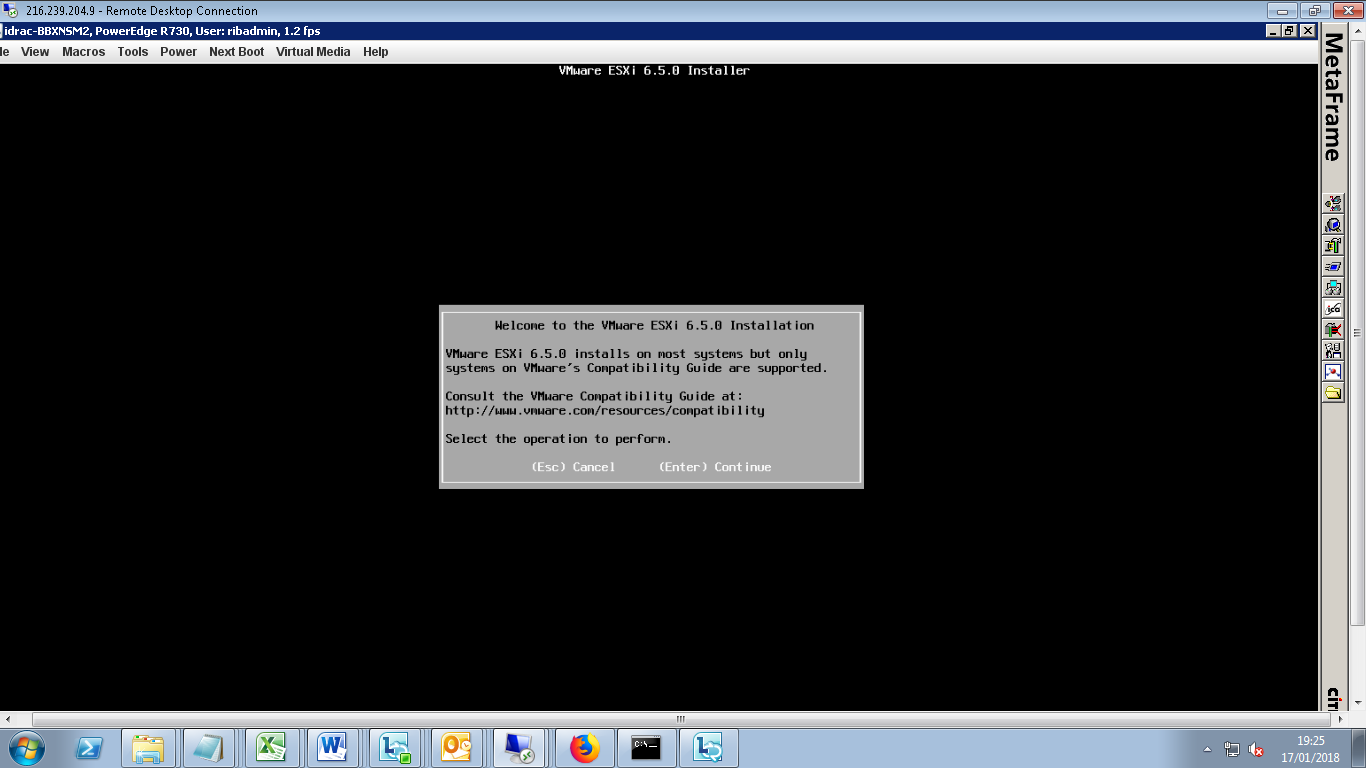
* + Local disk should be configured with RAID1 for installing Hypervisor VMware vSphere.

# Install ESXi

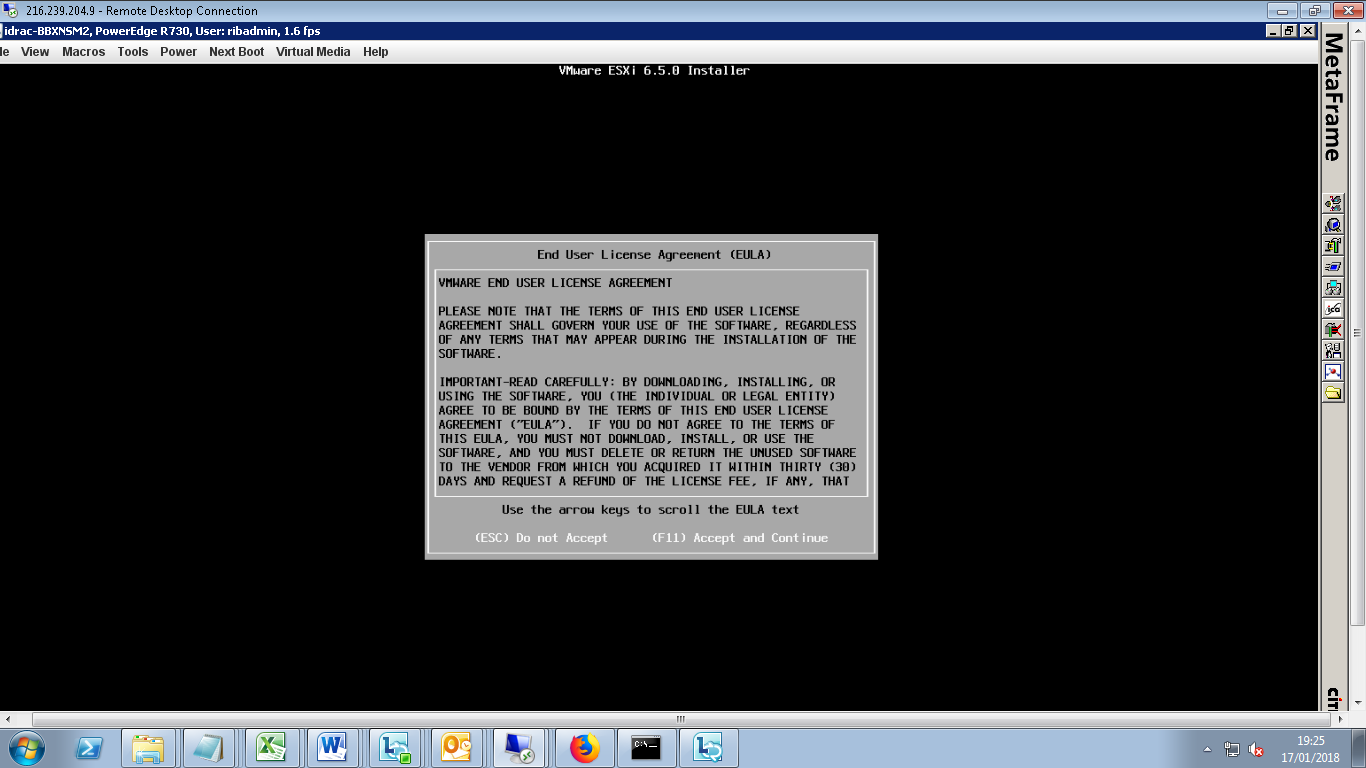
Connect to the ilo of the server and mount the relevant ISO Image. They will be stored in the software share in the VMware\vphere6.5 directory. Power on the server and boot from ISO.



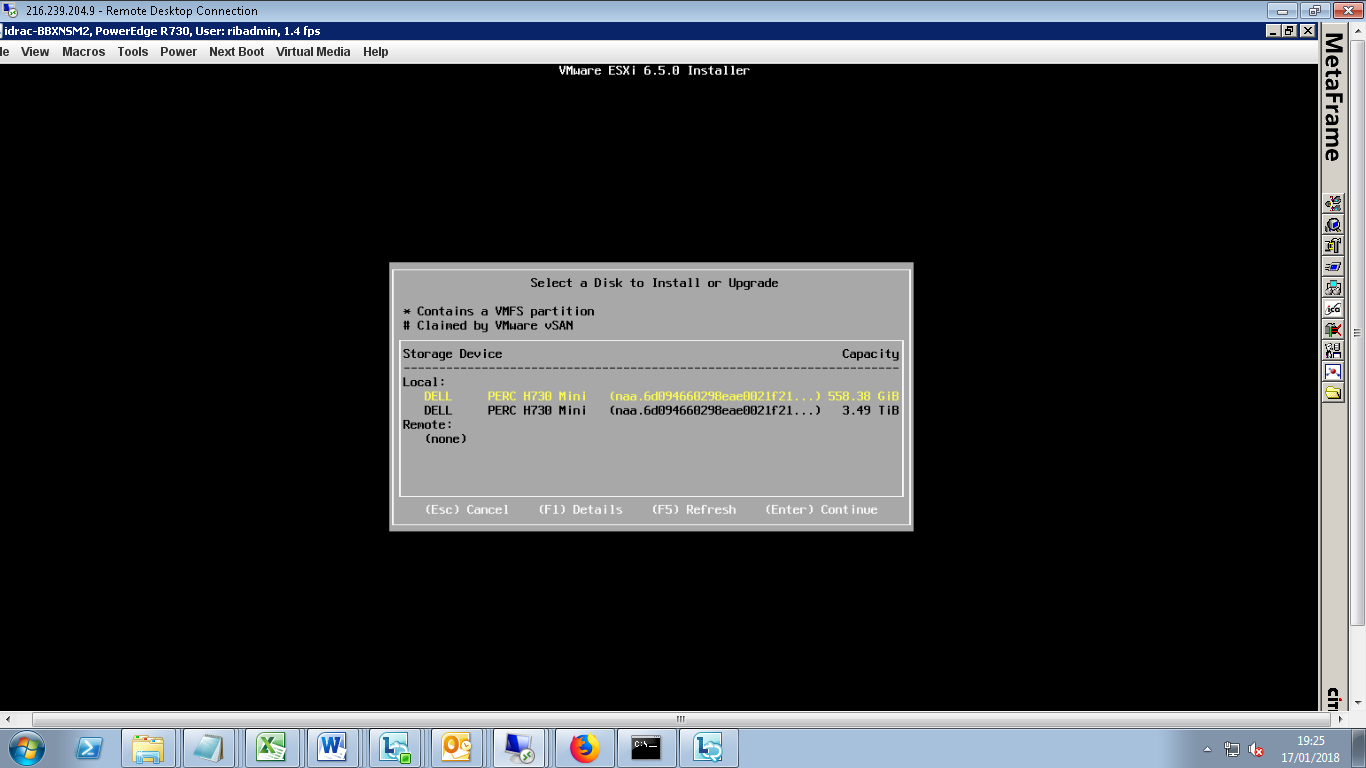
Press enter for the installer or allow it to automatically boot.



Press Enter to continue

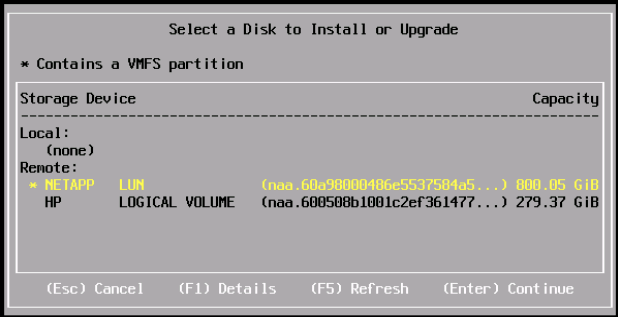


Press F11 to accept the agreement.



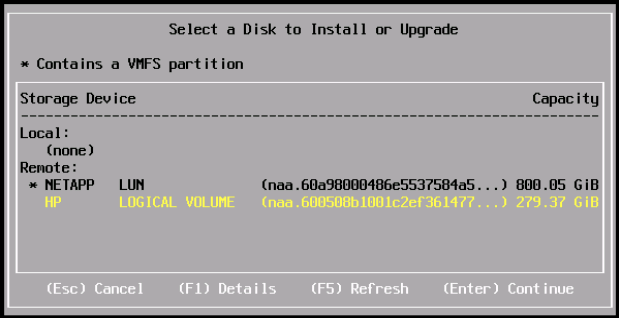
If the server has not been set up with access to LUNS the above should be seen. Press Enter to continue.

If this is a rebuild or LUNS have already been presented (i.e. SAN Zoning completed and iGroups mapped) then there will be more than one device listed:

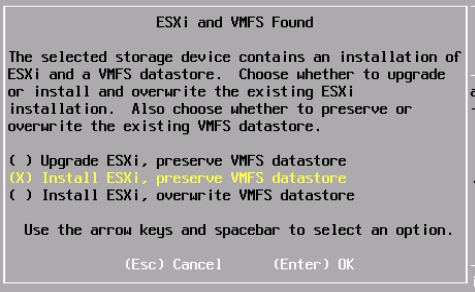


**WARNING:**  It is imperative that the correct device is selected. Although SAS drives are local they are detected by ESXi as Remote and hence will be listed with the NetApp LUNs. **If a NetApp LUN is selected you may overwrite a LUN with live VMs in it.**

Make sure the HP drive is selected and press Enter:

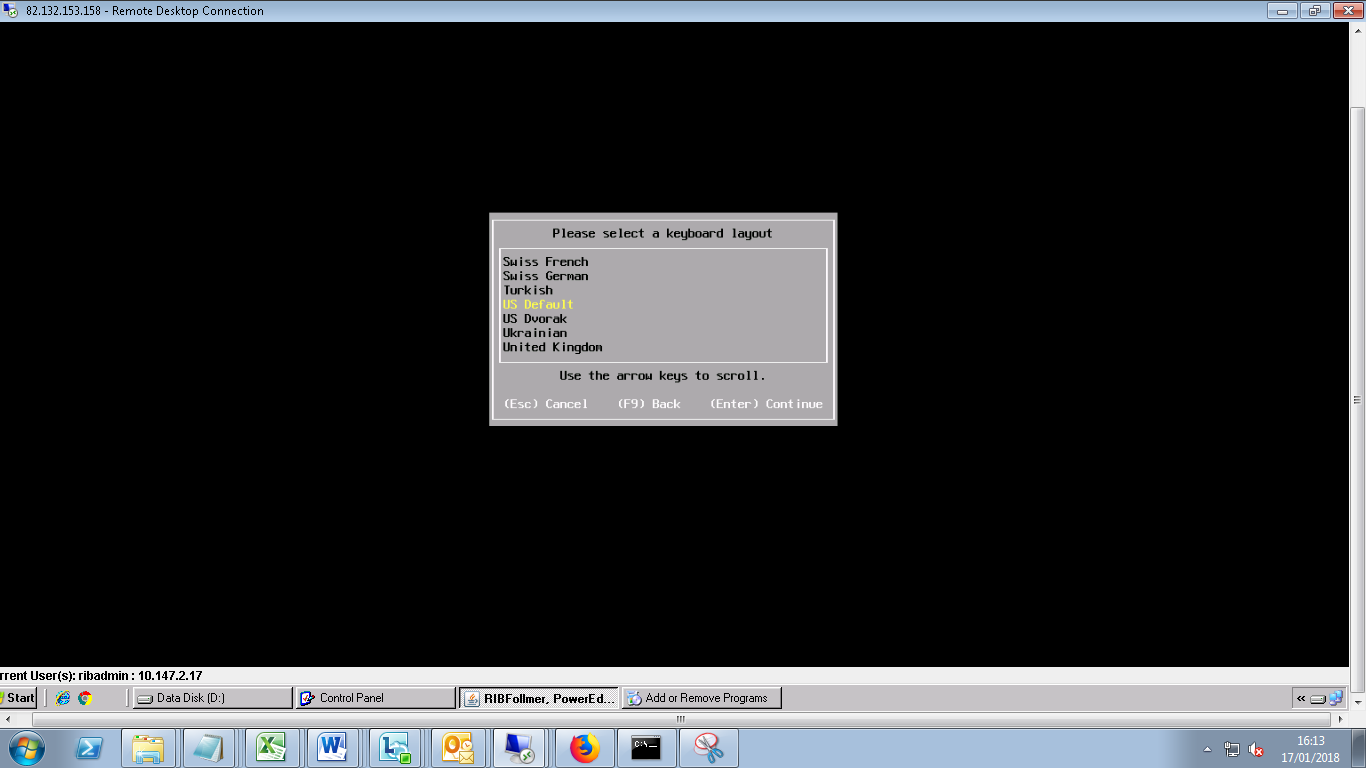


If this is a rebuild and you are installing a newer version of ESXi with one of the following depending if there’s a local VMFS datastore on the disk or not:

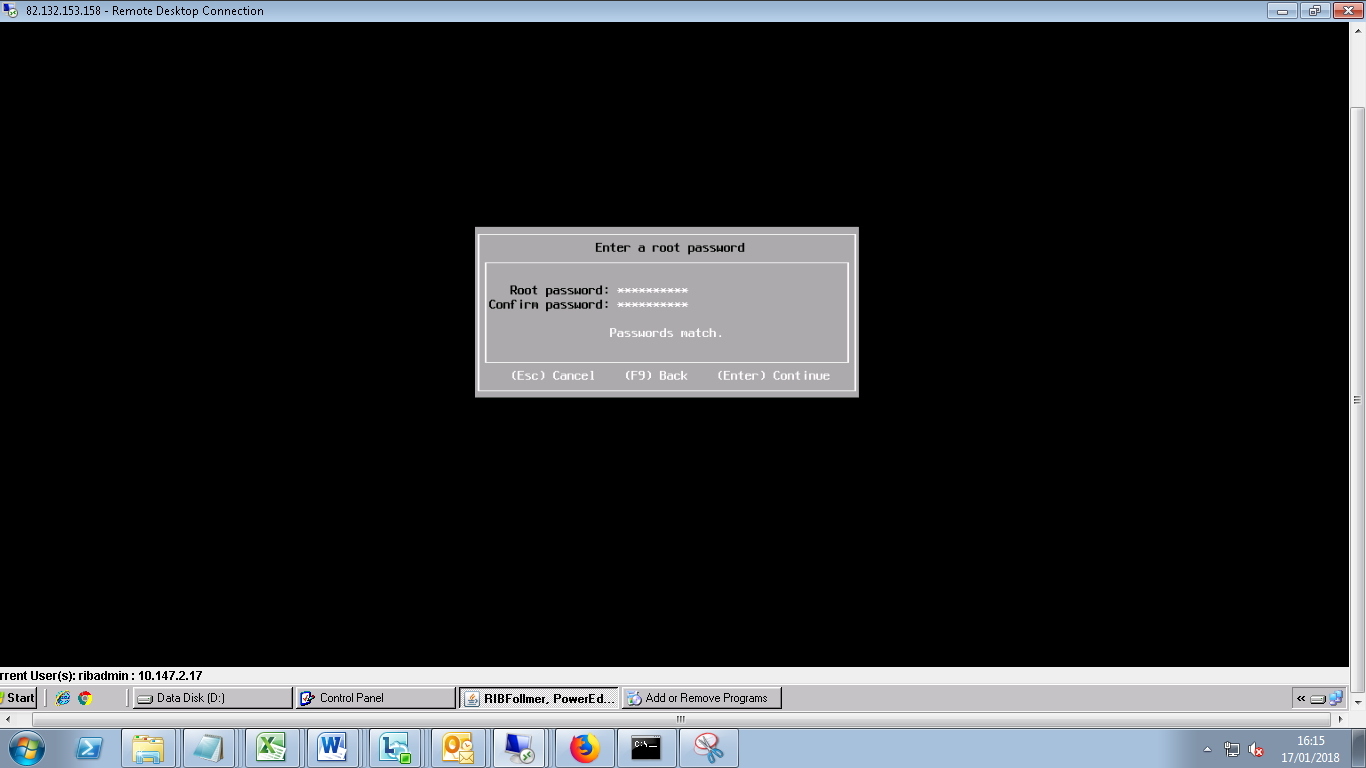




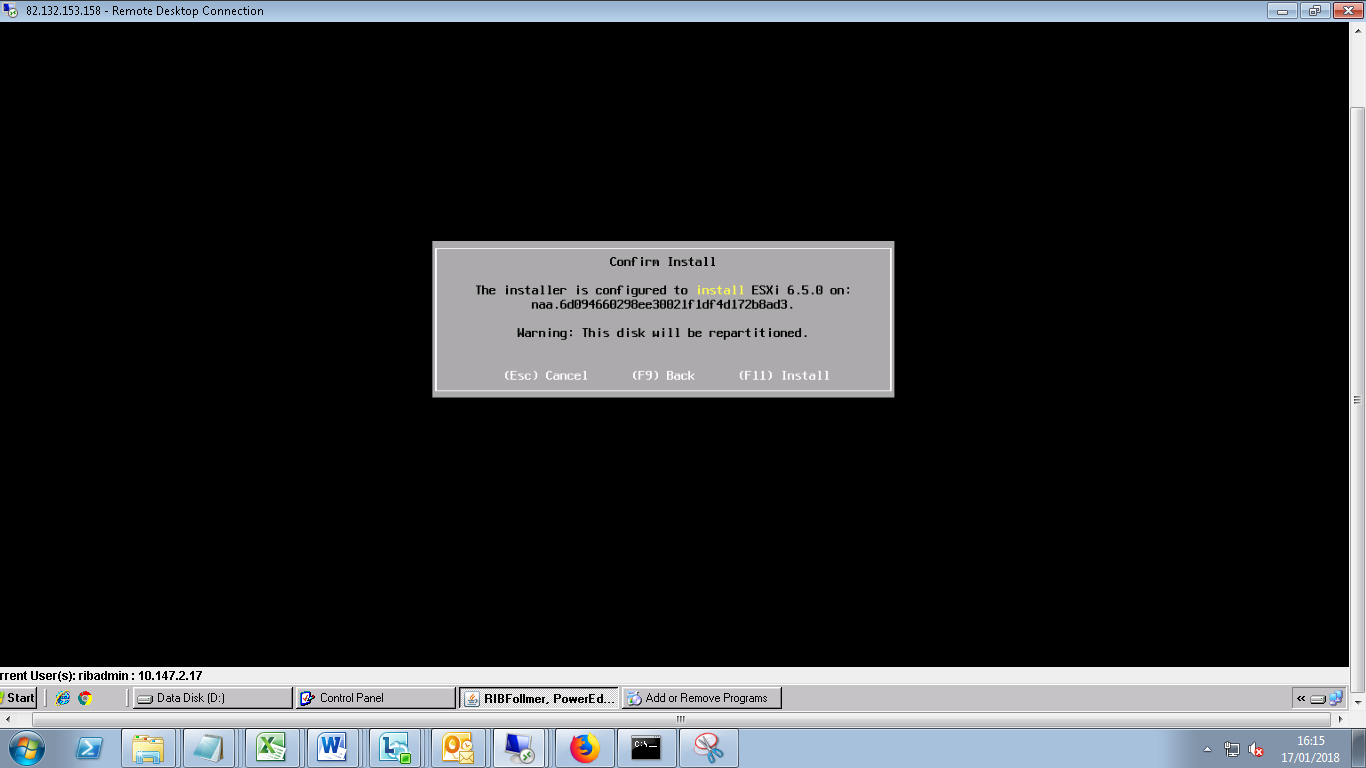
The recommended option is to do a fresh install of ESXi, preserving any local VMFS dataastores.



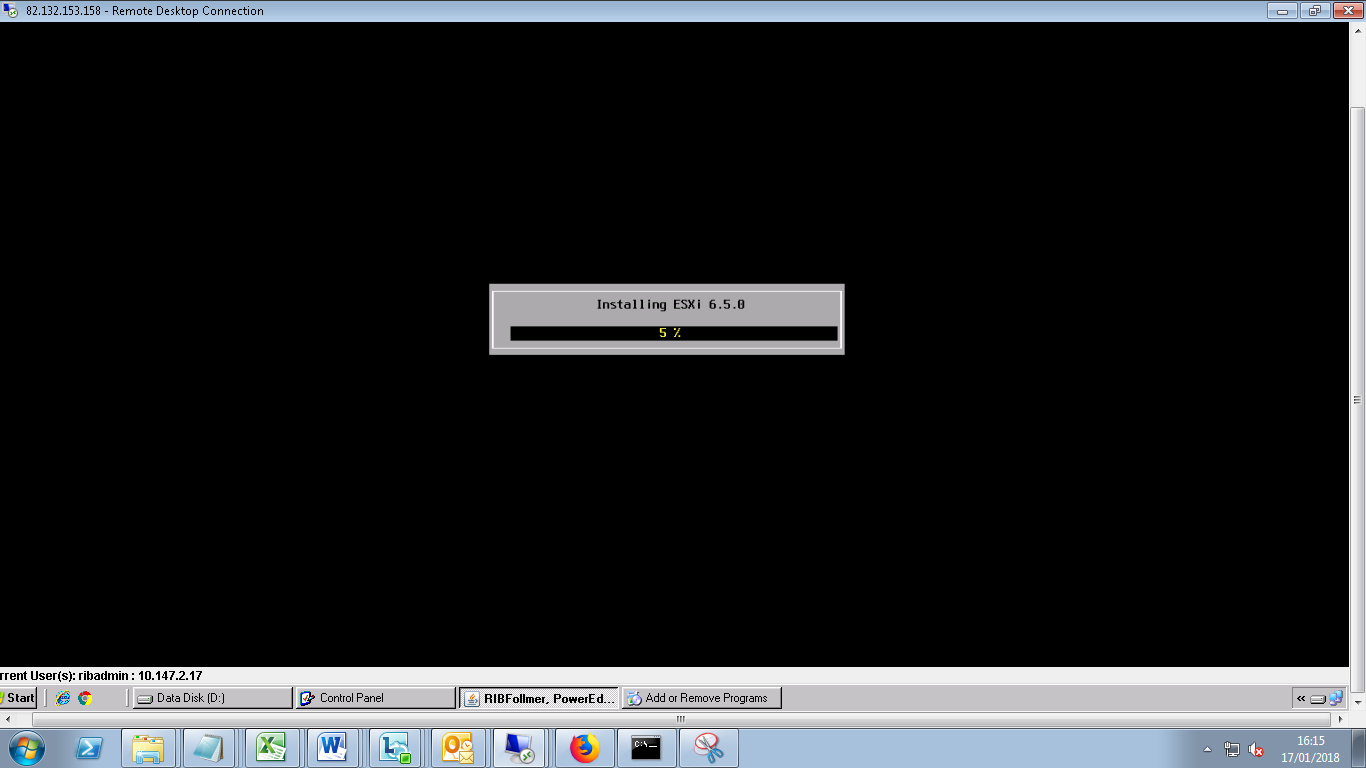
Select the United Kingdom Keyboard.



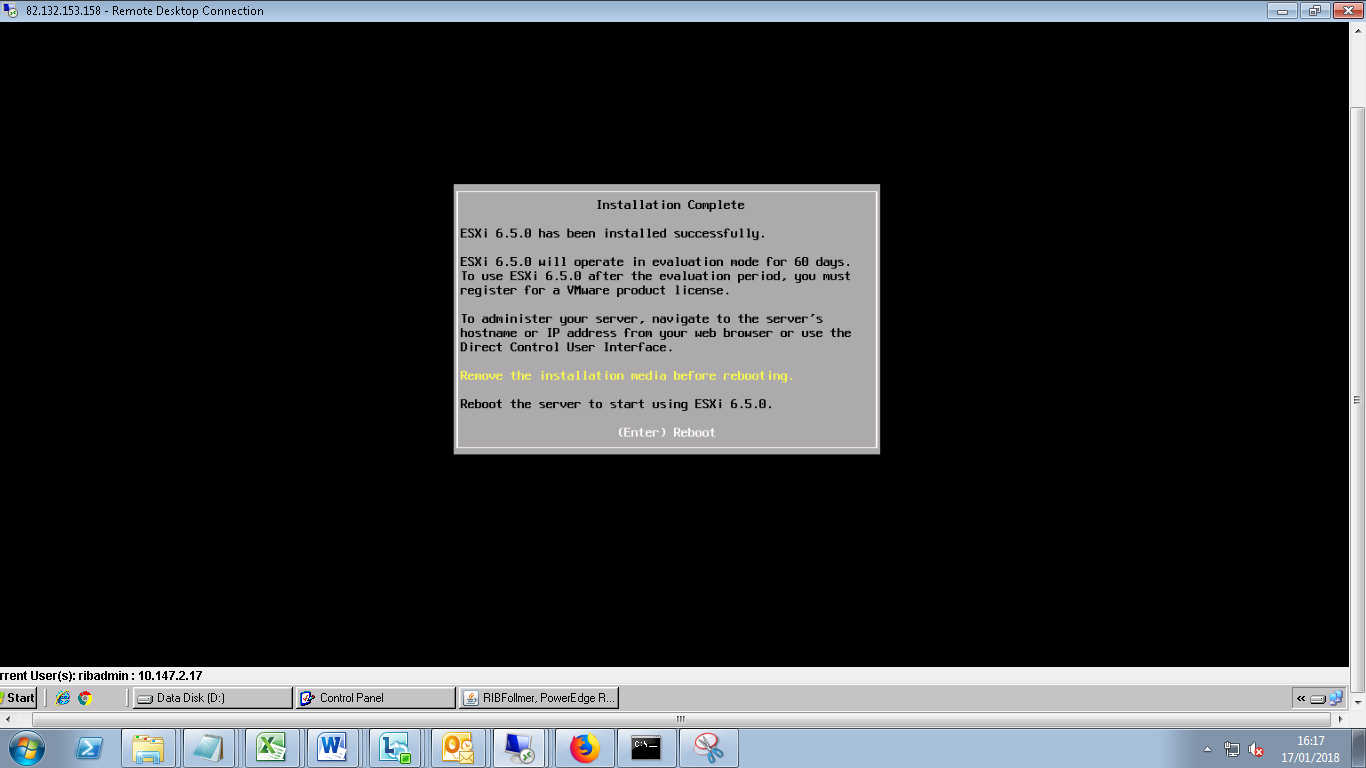
Enter the correct root password.

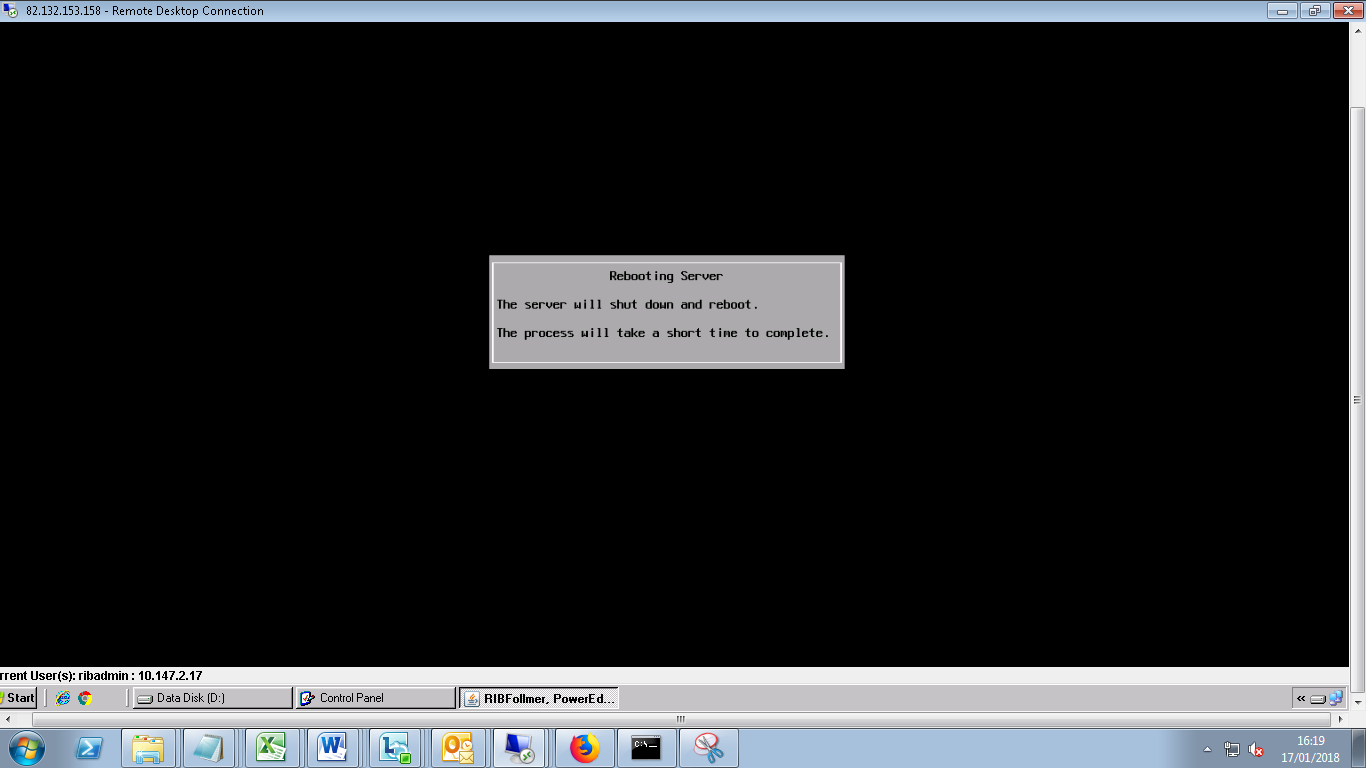


Press F11 to install ESXi.



The software will be installed.

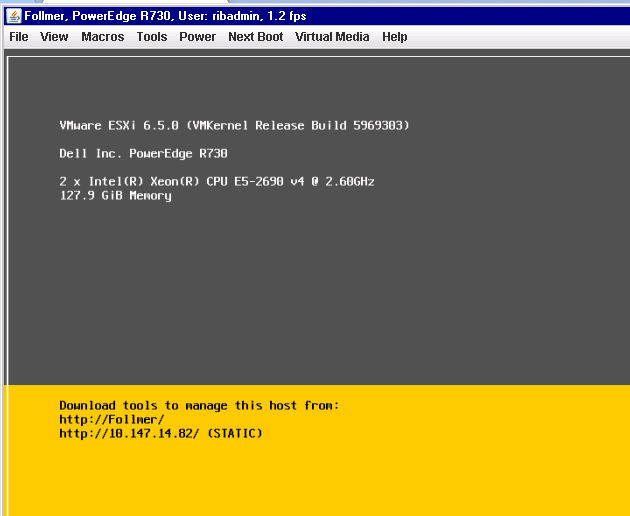




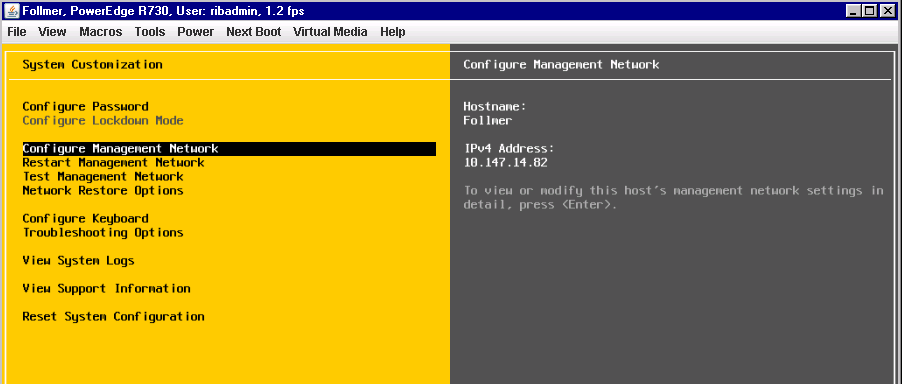
Once done dismount the ISO and reboot the server.

# Initial Configuration

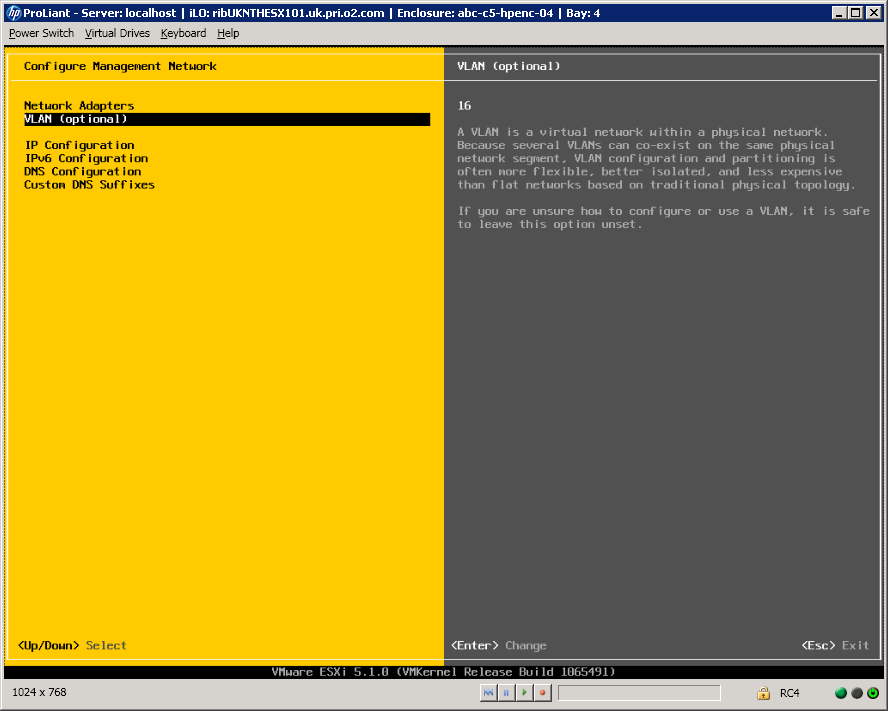
When the server reboots you will need to configure the basic information. The initial screen presented will be:



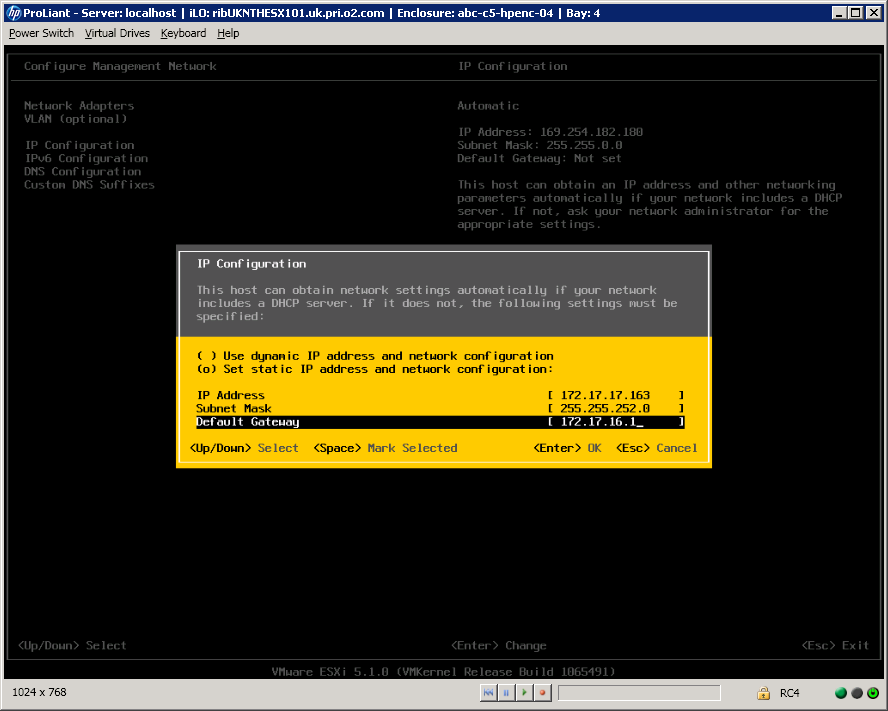
Press F2 to customise the system.



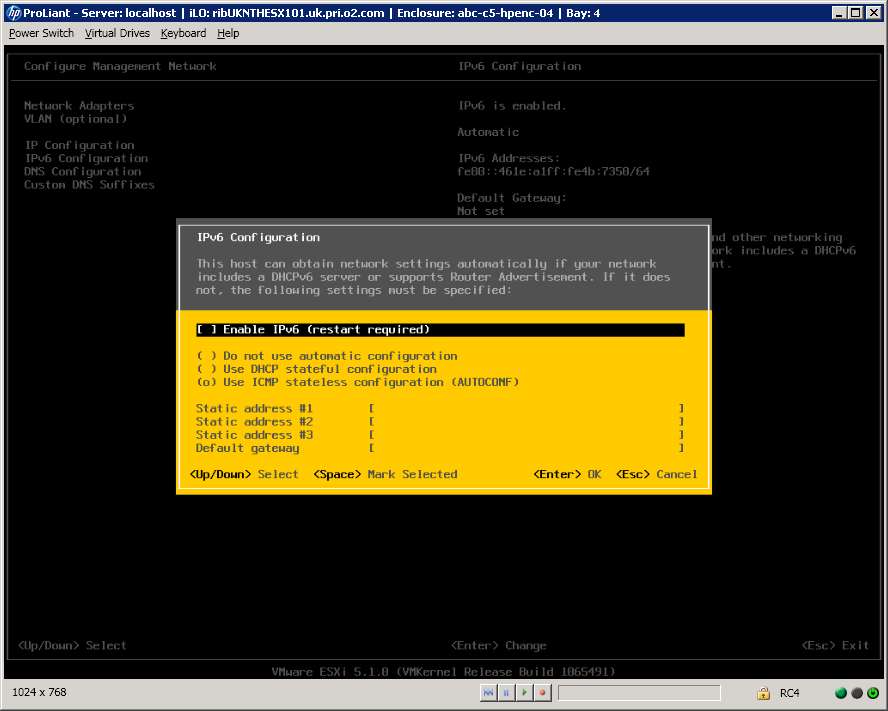
Firstly select Configure the Management Network.



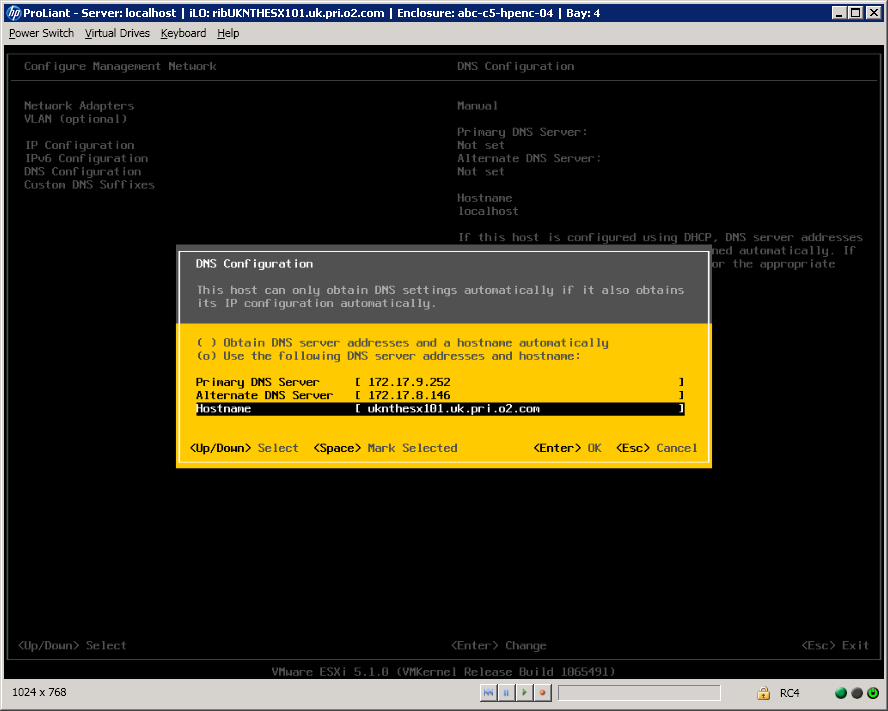
For Leeds ensure that vmnic0 or vmnic3 are selected under Network Adapters and that vLAN 16 is specified under the vLAN option.



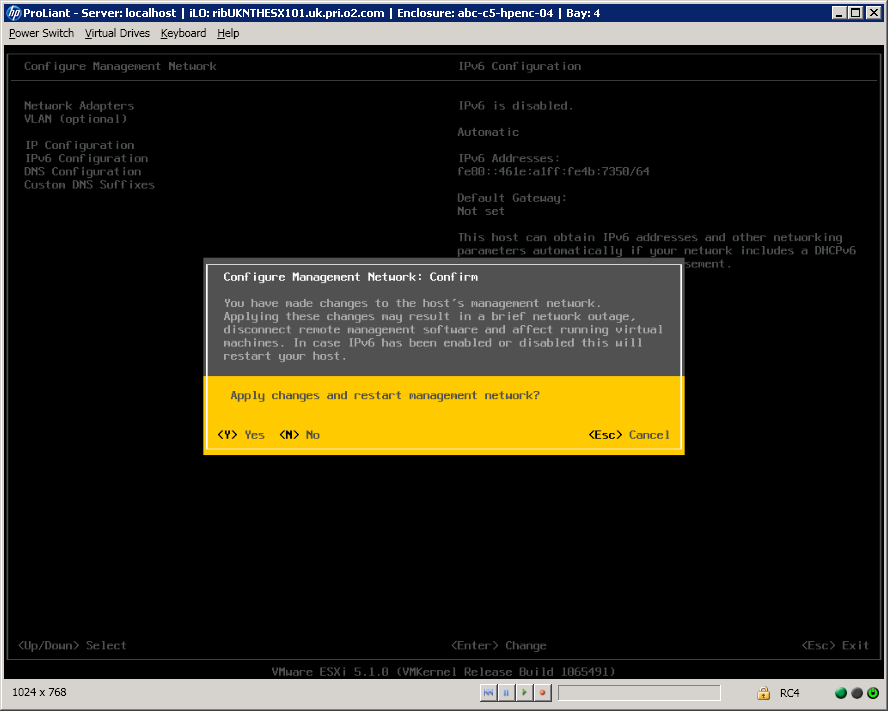
Specify the static IP address of the server, the subnet mask and the default gateway.



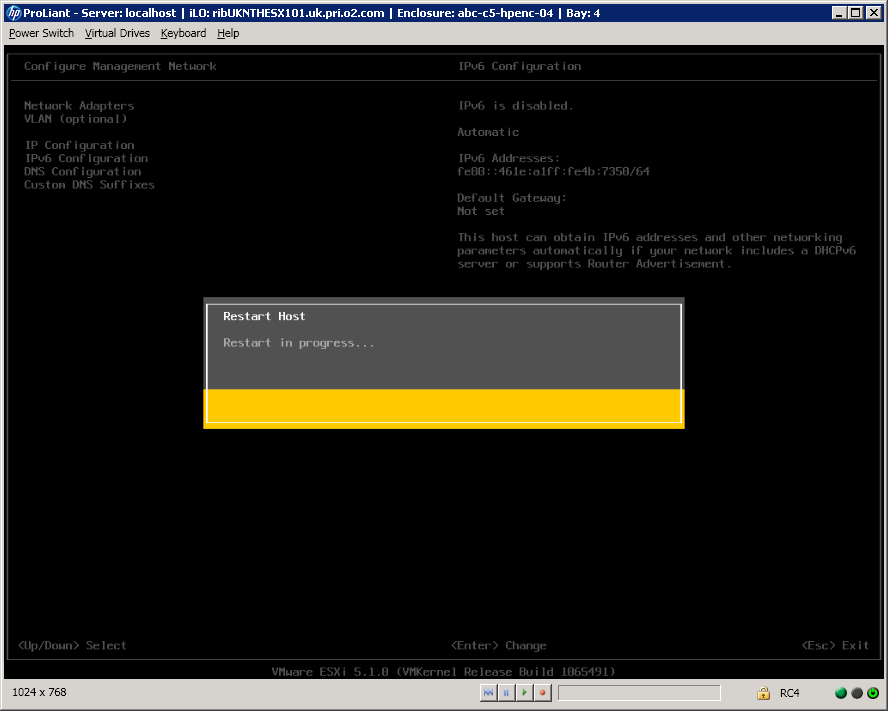
Disable IPv6 Support.



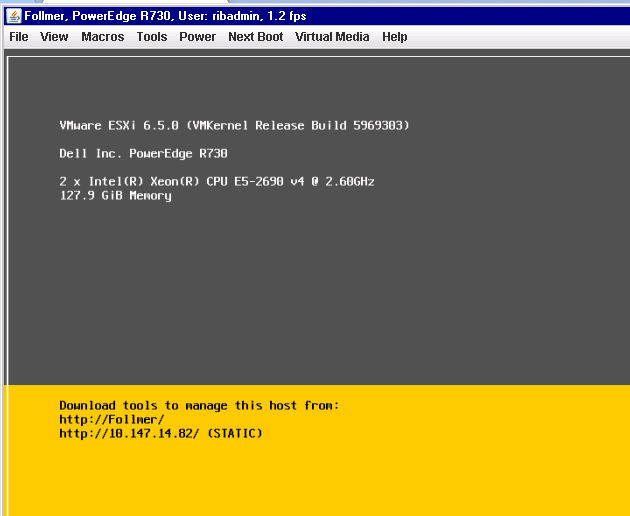
Specify the DNS and hostname information.



Apply the changes and restart the Management Network. As IPv6 has been disabled this will also cause the host to reboot (if it doesn’t reboot IPv6 has not been disabled properly).



The host will reboot.



When the reboot cycle has completed the correct IP information should be visible.

# VCenter Configuration

## Cluster settings:

Cluster setting such as HA, DRS and SDRS should be followed as per the iDLD.

# Network Connectivity

All ESXi host must have dual network connection for VMTraffic, vMotion, ESXi Mgmt.

## VSwitches:

Network should be configured with VMware teaming for ESXi Hosts. Two physical interfaces are teamed with vSwitch configuration within ESXi server in Active/Active mode. vSwitch uplink ports should be done as per design documents.

### Datastore

Datastores to be created as per iDLD and verify then following recommendation.

* Configure Active/Active multipath connection between the ESXi host and the Storage array.
* Round Robin Storage path Policy should be enabled from storage and ESXi host. .
* Storage Management Plug-In to be installed on VMware vCenter to access management capabilities from the VMware vCenter Server management console.

# Patch Management

* Patching of the VMWare ESXi hosts should be carried out based on existing cluster support model and life cycle management agreements.
* Patches should be applied by using VMware Update Manager to keep vSphere Hosts Up-To-Date.

### Time Server Details

The following table shows the Time Server details.

|  |  |
| --- | --- |
| Time / NTP Server details by IP | Time / NTP Server details by Name |
| 172.20.1.212, 172.20.1.213 and 172.20.1.217 | mnbas-vrs-1a, mnbas-vrs-1b and mnntm-vrs-1a |

## Governance Checks

Governance checks post build ensure that the ESXi host meets the build standard and any specific requirements of the iDLD before the host is handed over.

## Qualys / Tripwire Scan

All new ESXi host should have a Qualys or Tripwire scan to check for any vulnerabilities.

## CIS Scan

Latest CIS VMware ESXi 5.5 Benchmark should be used to do run the CIS report and all required CIS settings should be configured. Standard CIS exception from F&S approval in place for any additional CIS exception required then must obtain approval from F&S.

# User, Service Account and domain groups

* O2 UK Standard should be followed for creating users and groups.
* VCenter Single Sign-On (SSO) is already configured in existing vCenter UKMLWESX800.
* If users need a VM access via vSphere client, then access should be provided by using AD groups.

# Monitoring

* ESXi host monitoring should be done from SCOM via Veeam Management Pack.
* Ensure Veeam MP License must be installed and as per part of OA check the monitoring teams need to check that the server is correctly being monitored,

## Operational Acceptance

Once the host is ready for Go-Live the monitoring teams need to check that the host is correctly being monitored, there are no system alerts, no hardware failures. The host should have latest patches.

# User, Service Account and domain groups

* O2 UK Standard should be followed for creating users and groups.
* VCenter Single Sign-On (SSO) is already configured in existing vCenter UKMLWESX800.
* If users need a VM access via vSphere client, then access should be provided by using AD groups.

# Monitoring

* ESXi host monitoring should be done from SCOM via Veeam Management Pack.
* Ensure Veeam MP License must be installed and as per part of OA check the monitoring teams need to check that the server is correctly being monitored,

## Operational Acceptance

Once the host is ready for Go-Live the monitoring teams need to check that the host is correctly being monitored, there are no system alerts, no hardware failures. The host should have latest patches.

# CIS Hardening – Host Level:

* CIS hardening should be applied based on the project requirement.
* Below List of host and guest level CIS. From the attached Telefonica UK - CIS VMware ESXi 5.5 Configuration Standard Exception document shows the list of F&S approved CIS exception. Any new CIS exception needed then should be taken F&S approval.
* Most of the recommended hardening will be there by default and all default settings can be verified by taking the CIS report before applying the changes.

|  |  |  |
| --- | --- | --- |
| Benchmark Item | Remediation | Description |
| Configure NTP time synchronization | Description:   1. Perform the following: 2. Select the host. 3. Click "Manage" -> "Settings" -> "System" -> "Time Configuration". 4. Click the "Edit..." button. 5. Click on "Use Network Time Protocol". 6. Provide the name and / or IP of your NTP servers. Separate servers with commas. 7. If the NTP Service Status is "Stopped", click on "Start". 8. Change the start-up policy to "Start and stop with host". 9. Click "OK". | By ensuring that all systems use the same relative time source (including the relevant localization offset), and that the relative time source can be correlated to an agreed-upon time standard, you can make it simpler to track and correlate an intruder's actions when reviewing the relevant log files. Incorrect time settings can make it difficult to inspect and correlate log files to detect attacks and can make auditing inaccurate. |
| Disable ESXi Shell unless needed for diagnostics or troubleshooting | Perform the following:   1. From the vSphere web client select the host. 2. Select "Manage" -> "Settings" -> "System" -> "Security Profile". 3. Scroll down to "Services". 4. Click "Edit...". 5. Select "ESXi Shell". 6. Click "Stop". 7. Change the Startup Policy "Start and Stop Manually" 8. Click "OK | ESXi Shell is an interactive command line environment available from the Direct Console User Interface (DCUI) or remotely via SSH. Access to this mode requires the root password of the server. The ESXi Shell can be turned on and off for individual hosts. Activities performed from the ESXi Shell bypass vCenter RBAC and audit controls. The ESXi shell should only be turned on when needed to troubleshoot/resolve problems that cannot be fixed through the vSphere web client or vCLI/PowerCLI. You can use the vSphere Web Client to enable local and remote (SSH) access to the ESXi Shell and to set the idle timeout and availability timeout. |
| Disable SSH | Perform the following:   1. From the vSphere web client select the host. 2. Select "Manage" -> "Settings" -> "System" -> "Security Profile". 3. Scroll down to "Services". 4. Click "Edit...". 5. Select "SSH". 6. Click "Stop". 7. Change the Startup Policy "to Start and Stop Manually". 8. Click "OK". | Disable Secure Shell (SSH) for each ESXi host to prevent remote access to the ESXi shell. only enable if needed for troubleshooting or diagnostics |
| Enable lockdown mode to restrict remote access | From the vSphere web client:  1. Select the host ->Select "Manage" -> "Settings" -> "System" -> "Security Profile".   1. Scroll down to "Lockdown Mode". 2. Click "Edit...". 3. Select the "Enable Lockdown Mode" checkbox. 4. Click "OK". | Lockdown mode disables local access to the ESXi host. All management must be done from vCenter to ensure proper permissions and roles are being applied when using lockdown mode. |
| Ensure that the vSwitch Forged Transmits policy is set to reject | Remediation   1. In the vSphere Web Client, navigate to the host. 2. "Hosts and Clusters" -> "vCenter" -> host. 3. On the Manage tab, click Networking, and select Virtual switches. 4. Select a standard switch from the list and click the pencil icon to edit settings. 5. Select Security. 6. Set Forged transmits to "Reject". 7. Click "OK | Set the vSwitch Forged Transmits policy is set to reject for each vSwitch |
| Ensure that the vSwitch MAC Address Change policy is set to reject | 1. In the vSphere Web Client, navigate to the host. 2. "Hosts and Clusters" -> "vCenter" -> host. 3. On the Manage tab, click Networking, and select Virtual switches. 4. Select a standard switch from the list and click the pencil icon to edit settings. 5. Select Security. 6. Set MAC Address Changes to "Reject". 7. Click "OK". | Ensure that the MAC Address Change policy within the vSwitch is set to reject. |
| Ensure that the vSwitch Promiscuous Mode policy is set to reject | 1. In the vSphere Web Client, navigate to the host. 2. "Hosts and Clusters" -> "vCenter" -> host. 3. On the Manage tab, click Networking, and select Virtual switches. 4. Select a standard switch from the list and click the pencil icon to edit settings. 5. Select Security. 6. Set Promiscuous Mode to "Reject". 7. Click "OK". | Ensure that the Promiscuous Mode Policy within the vSwitch is set to reject |
| Configure the ESXi host firewall to restrict access to services running on the host | Perform the following from the vSphere web client:   1. Select the host 2. Go to "Manage" -> "Settings" -> "System" -> "Security Profile" 3. In the "Firewall" section select "Edit...". 4. For each enabled service, (e.g. ssh, vSphere Web Access, http client) provide a range of allowed IP addresses. 5. Click "Ok". | Below list of service must be enabled and provide the range of IP addresses from where these service access is required.  SSH  CIM Secure Server  vSphere client  CIM Server  NFS Client  NTP Client  NFC  vSphere HA  VMware vCenter agent  DNS client  vSphere web access  CIM SLP  SNMP Server  vMotion |

# CIS Hardening – Guest Level:

Below List of CIS hardening applied to VM. To implement the recommended configuration state, run the following PowerCLI command.

|  |  |  |
| --- | --- | --- |
| Benchmark Item | Remediation | Description |
| Disable Autologon | To implement the recommended configuration state, run the following PowerCLI command:  Get-VM | New-AdvancedSetting -Name "isolation.tools.ghi.autologon.disable" -value $true | Disable unneeded auto logon to reduce the potential for vulnerabilities |
| Disable BIOS BBS | Get-VM | New-AdvancedSetting -Name "isolation.bios.bbs.disable" -value $true | Disable BIOS BBS to reduce the potential for vulnerabilities. |
| Disable Guest Host Interaction Protocol Handler | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "isolation.tools.ghi.protocolhandler.info.disable" -value $true | Disable Guest Host Interaction Protocol Handle to reduce opportunity for vulnerabilities. |
| Disable Unity Taskbar | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "isolation.tools.unity.taskbar.disable" -value $true | Disable unexposed Unity Taskbar feature. |
| Disable Unity Active | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "isolation.tools.unityActive.disable" -value $True | Disable unexposed Unity Active feature. |
| Disable unexposed Unity Window Contents feature | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "isolation.tools.unity.windowContents.disable" -value $True | Disable unexposed Unity Window Contents feature. |
| Disable Unity Push Update | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "isolation.tools.unity.push.update.disable" -value $true | Disable unexposed Unity Push Update features |
| Disable Drag and Drop Version Get | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "isolation.tools.vmxDnDVersionGet.disable" -value $true | Disable unexposed Drag and Drop Version Get feature. |
| Disable Drag and Drop Version Set | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "isolation.tools.guestDnDVersionSet.disable" -value $true | Disable unexposed Drag and Drop Version Set feature. |
| Disable Shell Action | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "isolation.ghi.host.shellAction.disable" -value $true | Disable unexposed Shell Action feature |
| Disable Request Disk Topology | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "isolation.tools.dispTopoRequest.disable" -value $true | Disable unexposed Request Disk Topology feature |
| Disable Trash Folder State | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "isolation.tools.trashFolderState.disable" -value $true | Disable unexposed Trash Folder State feature |
| Disable Guest Host Interaction Tray Icon | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "isolation.tools.ghi.trayicon.disable" -value $true | Disable unexposed Guest Host Interaction Tray Icon feature. |
| Disable Unity | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "isolation.tools.unity.disable" -value $true | Disable unexposed Unity feature. |
| Disable Unity Interlock | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "isolation.tools.unityInterlockOperation.disable" -value $true | Disable unexposed Unity Interlock feature. Explicitly disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host |
| Disable GetCreds | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "isolation.tools.getCreds.disable" -value $true | Disable unexposed GetCreds feature. disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host |
| Disable Host Guest File System Server |  | Disable unexposed Host Guest File System Server.. Certain automated operations such as automated tools upgrades use a component into the hypervisor called Host Guest File System (HGFS) and an attacker could potentially use this to transfer files inside the guest OS. These VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. The code paths for these features are not implemented in ESXi. Explicitly disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host |
| Disable Guest Host Interaction Launch Menu | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "isolation.tools.ghi.launchmenu.change" -value $true | Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. The code paths for these features are not implemented in ESXi. Explicitly disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the hostfeature. |
| Disable memSchedFakeSampleStats | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "isolation.tools.memSchedFakeSampleStats.disable" -value $true | Some VMX parameters don't apply on vSphere because VMware virtual machines work on vSphere and hosted virtualization platforms such as Workstation and Fusion. The code paths for these features are not implemented in ESXi. Explicitly disabling these features reduces the potential for vulnerabilities because it reduces the number of ways in which a guest can affect the host. Note that these are referenced for organizations that insist any documented setting, regardless of whether it is implemented in code or not, must have a value. |
| Disable VM Console Copy operations | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "isolation.tools.copy.disable" -value $true | Copy and paste operations are disabled by default; however, by explicitly disabling this feature, it will enable audit controls to check that this setting is correct. |
| Disable VM Console Drag and Drop operations | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "isolation.tools.dnd.disable" -value $true | Copy and paste operations are disabled by default; however, by explicitly disabling this feature, it will enable audit controls to check that this setting is correct. |
| Disable VM Console and Paste GUI Options. | Rationale:Copy and paste operations are disabled by default; however, by explicitly disabling this feature, it will enable audit controls to check that this setting is correct. | Copy and paste operations are disabled by default; however, by explicitly disabling this feature, it will enable audit controls to check that this setting is correct. |
| Disable VM Console Paste operations | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "isolation.tools.paste.disable" -value $true | Copy and paste operations are disabled by default; however, by explicitly disabling this feature, it will enable audit controls to check that this setting is correct. |
| Control access to VM console via VNC protocol | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "RemoteDisplay.vnc.enabled" -value $false | The VM console enables you to connect to the console of a virtual machine, in effect seeing what a monitor on a physical server would show. This console is also available via the VNC protocol. Setting up this access also involves setting up firewall rules on each ESXi server the virtual machine will run on. |
| Disable VIX messages from the VM | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "isolation.tools.vixMessage.disable" -value $true | If you do not make use of custom VIX programming in your environment then you should disable this feature to reduce the potential for vulnerabilities. |
| Limit number of VM log files | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "log.keepOld" -value "10" | Configure VM settings to prevent uncontrolled logging |
| Do not send host information to guests | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "tools.guestlib.enableHostInfo" -value $false | Configure VMware Tools to disable host info from being sent to guests. |
| Limit VM log file size | # Add the setting to all VMs  Get-VM | New-AdvancedSetting -Name "log.rotateSize" -value "1024000" | Configure VM settings to prevent uncontrolled logging. Virtual machines write troubleshooting information into a virtual machine log file stored on the VMFS volume. Virtual machine users and processes can abuse logging either on purpose or inadvertently so that large amounts of data flood the log file. Over time, the log file can consume enough file system space to cause a denial of service. |