How to Configure vCenter Security Hardening Settings

First Published: 2018-10-31

Configure vCenter Security Hardening Settings

For the security hardening of vCenter, there are two additional parameters that must be configured manually in addition to the ones set via the automated script. For information on the automated script, see Automation Script for Setting STIG Parameters, on page 2.

To configure these two additional vCenter Security Hardening settings:

Procedure

Step 1 Set the `vpxd.hostPasswordLength` parameter to 32.

- The vpxuser password default length is 32 characters.
- The vpxuser password length must never be modified to less than the default length of 32 characters.
- From the vSphere Web Client, go to vCenter Inventory Lists >> vCenter Servers >> Select your vCenter Server >> Manage >> Settings >> **Advanced Settings**. Click **Edit** and edit the **config.vpxd.hostPasswordLength** setting to 32, or if the value does not exist, create it by entering the values in the **Key** and **Value** fields. Then click **Add**.
- If required, to change the password length policy, locate the vCenter Server configuration file "vpxd.cfg" on the system where vCenter Server is running and edit the `vpxd.hostPasswordLength` parameter.
- Restart the vCenter Server.

Step 2 Disable the vCenter Server Datastore browser.

- Stop the VirtualCenter Server service.
- Locate the vpxd.cfg file on the system where vCenter Server is running.
- Open the vpxd.cfg file using a text editor.
- Locate the <vpxd> and </vpxd> tags and add the following entry in tags, shown as follows:

```
<vpxd>
     <enableHttpDatastoreAccess>false</enableHttpDatastoreAccess>
</vpxd>
```

- Save the changes to the vpxd.cfg file.

- Start the VirtualCenter Server service.

Automation Script for Setting STIG Parameters

The STIG automation script for setting the STIG parameters for the Controller VMs, ESXi hosts, and vCenter in an HX Cluster can be executed either from the Controller VM or from a server with the following specification:

- Ubuntu Version: 16.04.4 LTS (Xenial Xerus)
- Python Version: 2.7.12
- Packages required: pyvmomi

The script, the configuration file, and log file are present on the controller VM at location: `/usr/share/springpath/storfs-misc/hx-scripts/`.

The file names are:

- `stig_security_settings.py`
- `stig_config.ini`

Note The preceding 2 files should be copied to the machine from where the script is to be executed.

To run the STIG automation script, enter:

```
python stig_security_settings.py
```

The following STIG parameters are set by the script:

- For ESXi hosts:

```
ESXiShellTimeOut:900DcuiTimeOut:900
DVFilterBindIpAddress:
BlockGuestBPDU:1
PasswordQualityControl:similar=deny retry=3 min=disabled,disabled,disabled,disabled,15
SyslogDir:[]/scratch/log
SyslogHost:udp://localhost
issue:This is a monitored system subject to Federal and International regulation.
Specific settings based on DISA STIGs have been implemented.
WelcomeMessage:This is a monitored system subject to Federal and International regulation.
 Specific settings based on DISA STIGs have been implemented.
AccountLockFailures:3
AccountUnlockTime:900
```

- For Controller VMs:

```
isolation.tools.hgfsServerSet.disable:true
RemoteDisplay.maxConnections:1
RemoteDisplay.vnc.enabled:false
isolation.device.connectable.disable:true
isolation.device.edit.disable:true
tools.guestlib.enableHostInfo:false
isolation.tools.copy.disable:true
isolation.tools.dnd.disable:true
```

```
isolation.tools.setGUIOptions.enable:false
isolation.tools.paste.disable:true
isolation.tools.ghi.autologon.disable:true
isolation.bios.bbs.disable:true
isolation.tools.getCreds.disable:true
isolation.tools.ghi.launchmenu.change:true
isolation.tools.memSchedFakeSampleStats.disable:true
isolation.tools.ghi.protocolhandler.info.disable:true
isolation.ghi.host.shellAction.disable:true
isolation.tools.dispTopoRequest.disable:true
isolation.tools.trashFolderState.disable:true
isolation.tools.ghi.trayicon.disable:true
isolation.tools.unity.disable:true
isolation.tools.unityInterlockOperation.disable:true
isolation.tools.unity.push.update.disable:true
isolation.tools.unity.taskbar.disable:true
isolation.tools.unityActive.disable:true
isolation.tools.unity.windowContents.disable:true
isolation.tools.vmxDnDVersionGet.disable:true
isolation.tools.guestDnDVersionSet.disable:true
isolation.tools.vixMessage.disable:true
isolation.tools.autoInstall.disable:true
tools.setinfo.sizeLimit:1048576
```

- For vCenter:

  ```
  config.nfc.useSSL:true
  ```

- For the ESXi Welcome message, the script is set to a default value.

To set the STIG parameters manually for security hardening, see the following sections:

- For ESXi hosts, see Set STIG Parameters for ESXi Hosts, on page 3.
- For Controller VMs, see Set STIG Parameters for Controller VMs, on page 5.
- For vCenter, see Set STIG Parameters for vCenter, on page 5.
- For the ESXi Welcome message, see Set ESXi Welcome Message, on page 6.

Note

1. When a HX cluster is expanded, the STIG settings do not automatically get applied to the newly added hosts and VMs. Either the script has be to run again or the settings have to applied manually.
2. Currently if user wants to reset the STIG settings, this has to be done manually.

Set STIG Parameters for ESXi Hosts

This procedure provides the instructions for manually setting the STIG parameters for ESXi hosts.

Warning

This causes the ESXi shell to be disabled after 900 seconds, which causes the HX upgrade to fail.

To manually set the STIG parameters for ESXi hosts:

Steps for vCenter Version 6.0 Using vSphere Web Client:

1. Browse to the host in the vSphere Web client inventory.
2. Click the Manage tab and click **Settings**.
3. Under System, select **Advanced System Settings**.
4. Select `UserVars.ESXiShellTimeOut` and click the Edit icon.
5. Enter the idle timeout setting.
6. Restart the SSH service for the timeout to take effect.
   a. Select the host.
   b. Click the Manage tab and click **Settings**.
   c. Under System, select **Security Profile**.
   d. In the Services section, click **Edit**.
   e. Select **SSH**.
   f. Click **Restart**.
   g. Click **OK**.
7. Click **OK**.

Steps for vCenter Version 6.5 Using vSphere Web Client:

1. Browse to the host in the vSphere Web Client inventory.
2. Click Configure.
3. Under System, select **Advanced System Settings**.
4. Select `UserVars.ESXiShellTimeOut` and click the Edit icon.
5. Enter the Value.
6. Restart the SSH service for the timeout to take effect.
   a. Select the host.
   b. Click the Manage tab and click **Settings**.
   c. Under System, select **Security Profile**.
   d. In the Services section, click **Edit**.
   e. Select **SSH**.
   f. Click **Restart**.
   g. Click **OK**.

Set STIG Parameters for Controller VMs

This procedure provides the instructions for setting the STIG parameters for Controller VMs:

Note It is recommended that you set this parameter for the VMs in the cluster one at a time. Each time after powering on the VM, wait for the cluster state to be healthy before proceeding to the next one.

Procedure

Step 1 To set the STIG parameters for vCenter version 6.0 using vSphere web client:

a. Log in to the vCenter Server system using the vSphere Client.

b. Select the virtual machine in the inventory.

c. Right click on the virtual machine > Power > Power off.

d. Select the Virtual Machine.

e. Right click and go to Edit Settings.

f. Select Virtual Hardware >> target hard disk and change the mode to Independent-persistent.

g. Right click the virtual machine > Power > Power on.

Step 2 To set the STIG parameters for vCenter version 6.5 using vSphere web client:

a. Log in to the vCenter Server system using the vSphere web client.

b. Select the virtual machine in the inventory.

c. Right click on the vitual machine > Power > Power off.

d. Select the Virtual Machine.

e. Right click and go to Edit Settings.

f. Select Virtual Hardware >> target hard disk and change the mode to Independent-persistent.

g. Right click on the virtual machine > Power > Power on.

Set STIG Parameters for vCenter

This procedure provides the instructions for setting the STIG parameters for vCenter:

Procedure

To set the STIG parameters for vCenter, see Configure vCenter Security Hardening Settings

Set ESXi Welcome Message

To manually set the ESXi Welcome message:

Procedure

Step 1 Using the vSphere Client, select the ESXi host in the Inventory.

Step 2 Click the **Configuration** tab.

Step 3 Click **Advanced Settings** under Software.

Step 4 Click **Annotations**.

Step 5 Enter the desired text in the Annotations.WelcomeMessage field.

Step 6 Click **OK**.

Or, you can use the following procedure:

a. Browse to the host in the vSphere Web Client inventory.

b. Click the Manage tab and click **Settings**.

c. Under System, select **Advanced System Settings**.

d. Select Annotations.WelcomeMessage and click the Edit icon.

e. Enter the desired text.

f. Click **OK**.

Note When a HX cluster is expanded, the STIG settings do not automatically get applied to the newly added hosts and VMs. Either the script has be to run again or the settings have to applied manually.

Currently if user wants to reset the STIG settings, it has to be done manually.

Communications, Services, Bias-free Language, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Bias-Free Language

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.