# Table of Contents

Lab Overview - HOL-1706-SDC-3 - Secure Your Software Defined Data Center ..........2  
Lab Guidance ........................................................................................................3  
Module 1 - Deploying The DISA STIG For ESXi Compliance and vCenter Two Factor Authentication (30 minutes) ........................................................................9  
  Introduction...........................................................................................................10  
  Deploy ESXi STIG for vSphere 6.0 ......................................................................12  
  vCenter Server Two-Factor Authentication .......................................................21  
  Conclusion ..........................................................................................................23  
Module 2 - Governance in a Secure World (45 minutes) .........................................25  
  Introduction.........................................................................................................26  
  Creating an Approval Policy in vRealize Automation .........................................27  
  Request to Destroy a Virtual Machine ..............................................................44  
  Manager Approval of the Request ....................................................................49  
  Conclusion ..........................................................................................................52  
Module 3 - Automating Password Complexity for ESXi Users (30 minutes) ...............54  
  Introduction.........................................................................................................55  
  Automate Password Complexity Policy ..............................................................56  
  Conclusion ..........................................................................................................63  
Module 4 - Forensic Security with vRealize Log Insight (30 minutes) .........................65  
  Introduction.........................................................................................................66  
  Perform Security Audit Actions .........................................................................67  
  Create Audit Query & Dashboard .....................................................................77  
  Analyze Linux Content Pack Security Dashboard ..........................................84  
  Conclusion ..........................................................................................................92
Lab Guidance

**NOTE:** It will take more than 90 minutes to complete this lab. You should expect to only finish 2-3 of the modules in one sitting. Modules are independent of each other, so you can start at the beginning of any module and proceed from there. Use the Table of Contents to access any module of your choosing, which can be accessed in the upper right-hand corner of the Lab Manual.

This lab contains four modules that focus on securing the vSphere infrastructure of the Software Defined Data Center. We will show administrators how they can leverage the features of core vSphere, CLI, vRealize Automation, and Log Insight to secure the SDDC.

Leveraging scripts, dashboards, certificate management and the worlds leading cloud management platforms, we will show vSphere administrators how to lower the amount of time they spend on securing the vSphere administrator, this will help IT organizations lower the overall operating expense associated with reducing security risk.

Lab Modules:

- **Module 1 - Deploying The DISA STIG For ESXi Compliance** (30 minutes, Beginner) From the Department of Defense to Financial Entities, the use of DISA Compliance standards is used across a broad set of industries. This lab will show vSphere administrators how to deploy the ESXi VIBS to ensure there ESXi hosts are in compliance with DISA standards.

- **Module 2 - Governance In a Secure World** (30 minutes, Intermediate) Have you ever hired a contract or temporary worker who has not yet passed your security process? How fantastic would it be to limit and govern the type of day two actions they perform on a virtual machine! In this module we will show cloud administrators, how they can leverage approvals in vRealize Automation, to limit day two actions for virtual machines users in vRA.

- **Module 3 - Automating Password Complexity for ESXi users** (30 minutes, Intermediate) 16 characters, dont use *, at least a number and a special character, but never $. Do these security compliance requirements drive you to drink? If so, this lab is for you! In this lab we will run a PowerCLI script that sets the password complexity rules for ESXi user across every host in your cluster.

- **Module 4 - Forensic Security with LogInsight** (30 minutes,Beginner) In prior versions of vSphere, the audit logs on vSphere hosts did not do a good job of identifying what user made a change. The change was recorded in vCenter, however ESXi logs would show vxpauser as the culprit. Leveraging vSphere 6 detailed logging capabilities and LogInsight, we will show administrators how to audit, who did what, on a particular ESXi host.
Lab Captains:

- **Module 1 - Ryan Cartwright** Senior Systems Engineer, USA. **Chris Saunders**, Staff Systems Engineer, USA
- **Module 2 - Ryan Cartwright** Senior Systems Engineer, USA. **Chris Saunders**, Staff Systems Engineer, USA
- **Module 3 - Ryan Cartwright** Senior Systems Engineer, USA. **Chris Saunders**, Staff Systems Engineer, USA
- **Module 4 - Ryan Cartwright** Senior Systems Engineer, USA. **Chris Saunders**, Staff Systems Engineer, USA

This lab manual can be downloaded from the Hands-on Labs Document site:


This lab may be available in other languages. To set your language preference and have a localized manual deployed with your lab, you may utilize this document to help guide you through the process:

Location of the Main Console

1. The area in the RED box contains the Main Console. The Lab Manual is on the tab to the Right of the Main Console.
2. A particular lab may have additional consoles found on separate tabs in the upper left. You will be directed to open another specific console if needed.
3. Your lab starts with 90 minutes on the timer. The lab can not be saved. All your work must be done during the lab session. But you can click the **EXTEND** to increase your time. If you are at a VMware event, you can extend your lab time twice, for up to 30 minutes. Each click gives you an additional 15 minutes. Outside of VMware events, you can extend your lab time up to 9 hours and 30 minutes. Each click gives you an additional hour.

Activation Prompt or Watermark

When you first start your lab, you may notice a watermark on the desktop indicating that Windows is not activated.

One of the major benefits of virtualization is that virtual machines can be moved and run on any platform. The Hands-on Labs utilizes this benefit and we are able to run the labs out of multiple datacenters. However, these datacenters may not have identical processors, which triggers a Microsoft activation check through the Internet.

Rest assured, VMware and the Hands-on Labs are in full compliance with Microsoft licensing requirements. The lab that you are using is a self-contained pod and does not have full access to the Internet, which is required for Windows to verify the activation.
Without full access to the Internet, this automated process fails and you see this watermark.

This cosmetic issue has no effect on your lab.

Alternate Methods of Keyboard Data Entry

During this module, you will input text into the Main Console. Besides directly typing it in, there are two very helpful methods of entering data which make it easier to enter complex data.

Click and Drag Lab Manual Content Into Console Active Window

You can also click and drag text and Command Line Interface (CLI) commands directly from the Lab Manual into the active window in the Main Console.

Accessing the Online International Keyboard

You can also use the Online International Keyboard found in the Main Console.
1. Click on the Keyboard Icon found on the Windows Quick Launch Task Bar.

Click once in active console window

In this example, you will use the Online Keyboard to enter the "@" sign used in email addresses. The "@" sign is Shift-2 on US keyboard layouts.

1. Click once in the active console window.
2. Click on the Shift key.

Click on the @ key

1. Click on the "@" key.

Notice the @ sign entered in the active console window.
Look at the lower right portion of the screen

Please check to see that your lab is finished all the startup routines and is ready for you to start. If you see anything other than "Ready", please wait a few minutes. If after 5 minutes you lab has not changed to "Ready", please ask for assistance.
Module 1 - Deploying The DISA STIG For ESXi Compliance and vCenter Two Factor Authentication (30 minutes)
Introduction

From the Department of Defense to Financial Entities, the use of DISA Compliance standards is used across a broad set of industries. This lab will show vSphere administrators how to deploy the ESXi VIBS to ensure there ESXi hosts are in compliance with DISA standards.

The DoD Security Technical Implementation Guide (‘STIG’) ESXi VIB is a Fling that provides a custom VMware-signed ESXi vSphere Installation Bundle (‘VIB’) to assist in remediating Defense Information Systems Agency STIG controls for ESXi. This VIB has been developed to help customers rapidly implement the more challenging aspects of the vSphere STIG. These include the fact that installation is time consuming and must be done manually on the ESXi hosts. In certain cases, it may require complex scripting, or even development of an in-house VIB that would not be officially digitally signed by VMware (and therefore would not be deployed as a normal patch would). The need for a VMware-signed VIB is due to the system level files that are to be replaced. These files cannot be modified at a community supported acceptance level. The use of the VMware-signed STIG VIB provides customers the following benefits:

- The ability to use vSphere Update Manager (‘VUM’) to quickly deploy the VIB to ESXi hosts (you cannot do this with a customer created VIB)
- The ability to use VUM to quickly check if all ESXi hosts have the STIG VIB installed and therefore are also in compliance
- No need to manually replace and copy files directly on each ESXi host in your environment
- No need to create complex shell scripts that run each time ESXi boots to re-apply settings

We will also show end users the new capability in vSphere 6 that meets another DISA requirement, two factor authentication into vCenter.
You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests—not for your personal benefit or privacy.
- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.
Deploy ESXi STIG for vSphere 6.0

For this lab we are installing VIBS on vSphere 6.0 and the VIBS have been pre-loaded into the environment. If you are going to deploy into your data center, then you need to adhere to the following requirements.

ESXi 5.x and 6.0 are supported but each have a different set of VIBs as the vSphere 5.0 and 6.0 STIGs have different requirements.

The following VIBs are provided for each ESXi version as follows:

ESXi 5.x
- dod-esxi5-stig-rd
- dod-esxi5-stig-re

ESXi 6.0
- dod-esxi6-stig-rd
- dod-esxi6-stig-re

The VIBS can be downloaded from here

Open WinSCP

1. Open WinSCP (click on the windows icon, then all programs)
Login Into esx-01a.corp.local

1. Click on "esx-01a.corp.local"
2. Click on "login"
Certificate Warning

1. Click Add

WARNING - POTENTIAL SECURITY BREACH!

The server’s host key does not match the one WinSCP has in cache. This means that either the server administrator has changed the host key, the server presents different key under certain circumstance, or you have actually connected to another computer pretending to be the server.

The new rsa2 key fingerprint is:

If you were expecting this change, trust the new key and want to continue connecting to the server, either press Update to update cache, or press Add to add the new key to the cache while keeping the old one(s). If you want to carry on connecting but without updating the cache, press Skip. If you want to abandon the connection completely, press Cancel. Pressing Cancel is the ONLY guaranteed safe choice.
Drag and Drop VIB to /root

1. Make sure you are in the folder "Desktop\Lab Files"
2. Click on "dod-esxi6-stig-rd-1.0.1.3210606.vib"
3. Ensure "/root" is selected in the right hand side
4. Drag and Drop the VIB to /root

The need for a VMware-signed VIB is due to the system level files that are to be replaced. These files cannot be modified at a community supported acceptance level.
Open Putty

1. Click on "Putty"
Login to esxi-01a.corp.local

1. Click on "esxi-01a.corp.local"
2. Click on "Load"
3. Click on "Open"
Install VIB

1. Type "pwd" to verify you are in the root or / directory

2. Type "ls"

3. Verify "dod-esxi6-stig-rd-1.0.1.3210606.vib" exists

4. Execute the command "esxcli software vib install -v /dod-esxi6-stig-rd-1.0.1.3210606.vib"

5. Verify the operation finished successfully

```
Using username "root".
Authenticating with public key "controlcenter" from agent
The time and date of this login have been sent to the system logs.

VMware offers supported, powerful system administration tools. Please see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the vSphere Security documentation for more information.

[root@esx-01a:~] pwd
/
[root@esx-01a:~] ls
altbootbank etc opt
bin lib proc
bootbank lib64 productLocker
bootpart.gz lcore.txt sbin
dev locker store

dod-esxi6-stig-rd-1.0.1.3210606.vib mbr
[root@esx-01a:~] esxcli software vib install -v /dod-esxi6-stig-rd-1.0.1.3210606.vib
Installation Result:
   Message: Operation finished successfully.
   Reboot Required: False
   VIBs Installed: VMware_bootbank_dod-esxi6-stig-rd-1.0.1-0.1.3210606
   VIBs Removed:
   VIBs Skipped:
[root@esx-01a:~]
```
Verify VIB is Installed

1. Execute the command "esxcli software vib list | grep "dod-esxi6-stig-rd"

2. The Result Should be the Same as the Screen Shot

Verify an Actual Change

1. Type "cat /etc/issue"

2. The Result Should be the DOD Banner

Alternative Install Methods

The DISA STIG VIB can also be deployed through VUM to make installation and compliance checking easier in large environments. Another alternative for installation is through PowerCLI.
vCenter Server Two-Factor Authentication

Two factor authentication (2FA) has become ubiquitous nowadays. For those of you still in the Dark Ages where you have your password written on a Post-It Note stuck to the bottom of your keyboard, 2FA is “something you have”, like a hardware or software token and “something you know” which would be a secret PIN.

vCenter Single Sign-On allows you to authenticate by using the name and password of a user in an identity source that is known to vCenter Single Sign-On, or using Windows session authentication for Active Directory identity sources. Starting with vSphere 6.0 Update 2, you can also authenticate by using a smart card (UPN-based Common Access Card or CAC), or by using an RSA SecurID token.

Two-Factor Authentication Methods

The two-factor authentication methods are often required by government agencies or large enterprises.

- Common Access Card (CAC) Authentication

CAC authentication allows access only to users who attach a physical card to the USB drive of the computer where they log in. If the PKI is deployed so that the smart card certificates are the only client certificates that are issued by the CA, then only smart card certificates are presented to the user. The user selects a certificate, and is then prompted for a PIN. Only users who have both the physical card and the PIN that matches the certificate can log in.

- RSA SecurID Authentication

For RSA SecureID authentication, your environment must include a correctly configured RSA Authentication Manager. If the Platform Services Controller is configured to point to the RSA server, and if RSA SecurID Authentication is enabled, users can then log in with their user name and token.

Note:

vCenter Single Sign-On supports only native SecurID, it does not support RADIUS authentication.
Quick Demo of vCenter Two Factor Authentication

Here’s a quick demo on how the user experience looks like. In the example we are using a Windows-based soft token assigned to administrator@demo.vmware.com. This user is in Active Directory. Note how the UI changes based on what authentication option we choose.
Conclusion

Congratulations on completing Module 1!

Keeping your ESXi hosts in compliance with recognized standards is key in reducing your overall security risk of the Software Defined Data Center.

In this module we took some time to see that we can leverage automation and STIG compliance VIBS to bring our ESXi hosts into STIG compliance.

We also covered the new feature in vSphere 6.0 that shows the capability to require users to leverage Two Factor Authentication for vCenter.

In Module 2, we will take a closer look at leveraging

For additional information from this module, visit the VMware blogs at https://blogs.vmware.com/vsphere/2016/01/making-security-easier-an-esxi-ling-for-us-federal-customers.html

Proceed to the next step, or select any module below which interests you most.

- **Module 2 - Governance In a Secure World** (30 minutes, Intermediate) Have you ever hired a contract or temporary worker who has not yet passed your security process? How fantastic would it be to limit and govern the type of day two actions they perform on a virtual machine! In this module we will show cloud administrators, how they can leverage approvals in vRealize Automation, to limit day two actions for virtual machines users in vRA.
- **Module 3 - Automating Password Complexity for ESXi users** (30 minutes, Intermediate) 16 characters, don't use *, at least a number and a special character, but never $. Do these security compliance requirments drive you to drink? If so, this lab is for you! In this lab we will run a PowerCLI script that sets the password complexity rules for ESXi user across every host in your cluster.
- **Module 4 - Forensic Security with LogInsight** (30 minutes, Beginning) In prior versions of vSphere, the audit logs on vSphere hosts did not do a good job of identifying what user made a change. The change was recoreded in vCenter, however ESXi logs would show vxpauser as the culprit. Leveraging vSphere 6 detailed logging capabilites and LogInsight, we will show administrators how to audit, who did what, on a paticular ESXi host.

**OPTIONAL: How to End the Lab**

You can now continue on to the next module by clicking forward, or use the Table of Contents to skip to another desired Module.

If you'd like to end your lab, click on the END button.
**Note:** If you end your lab, you will need to re-register for the lab in order to take any other modules.
Module 2 - Governance in a Secure World (45 minutes)
Introduction

This module shows how a vRealize Automation Tenant administrator can create an approval policy in vRealize Automation 7. This policy will be associated with a specific day 2 action. An offshore VI Administrator will request to destroy a linux Virtual Machine that is under his management. A notification will be sent to his manager that will allow them to either approve or reject the request to destroy the linux Virtual Machine.

This Module contains the following lessons:

- **vRealize Automation - Create an Approval Policy in vRealize Automation.** This lesson walks through creating an approval policy for destroying a Virtual Machine.
- **vRealize Automation - Request to Destroy a Virtual Machine.** This lesson walks through an administrator request to destroy a Virtual Machine based on an approval policy created in the prior lesson.
- **vRealize Automation - Manager Approval of the Request.** This lesson walks through a manager approving a request to destroy a Virtual Machine based on the request in the prior lesson.
Creating an Approval Policy in vRealize Automation

Approval policies are an out-of-the-box feature of vRealize Automation. It allows the business to create processes and policies for all kinds of reasons. The approval can be triggered before the machine is created (pre-approval) or after machine is created (post-approval). In this lab, we will walk through creating a post-approval policy.

Launch vRealize Automation

1. Launch vRealize Automation [https://vra-01a.corp.local/vcac](https://vra-01a.corp.local/vcac) from within Chrome or select vRealize Automation link from the Bookmarks toolbar.
Login to vRA with cloudadmin

Login to the console with the cloudadmin account.

1. Enter **cloudadmin** in the username field.
2. Enter **VMware1!** in the password field.
3. Click **Sign in**.

![Login to vRA](image)

Administration tab

1. Select the **Administration** tab.
Approval Policies

In this section, you will configure approval policies

Create a New Policy

1. Click **New** (green plus-sign).
Choose a Policy

You will be presented with the New Approval Policy pop up window.
Search for Destroy - Virtual Machine

1. Search for keyword "destroy" in the search box.
3. Click OK.
New Approval Policy Details

1. Enter "Destroy Virtual Machine Policy" in the Name field.
2. Change Status drop down and select **Active**.
3. Select **Post Approval** tab
4. Click the **green plus-sign** to create a New Level.
Configure the New Level Approval

In the next section, you will configure the New Level Approval.

![New Level Configuration Interface](image)

- **Level Information**
  - Name:
  - Description:

- **Approvers**:
  - Specific users and groups
  - Determine approvers from the request
  - Use event subscription

- **When approval is required**:
  - Always required
  - Required based on conditions

- **Search**:
  - No data selected
Level Information

1. Enter "Manager Approval" in the Name field.
2. Ensure "Always required" bullet is selected.

Approvers

1. Under Approvers, in the Search bar, enter "devmgr".
2. Press Enter on the keyboard to search.
3. Press Enter again to select Development Manager (devmgr@corp.local)
New Level Configuration Complete

1. Click **OK** button to complete the configuration of new level approvals.
Save New Approval Policy

1. Click **OK** to save the New Approval Policy.

Manage Approval Policies

You will now see the new Destroy Virtual Machine Policy in the Approval Policies screen.

Modify Entitlements

In the next section, you will modify entitlements.
Catalog Management

1. Click **Catalog Management**.
Entitlements

1. Click **Entitlements**.

![Entitlements Menu]

Edit Development Services Entitlement

1. Click on the **Development Services** entitlement hyperlink to edit.

![Entitlements Table]
Edit Entitlement

1. Click **Items & Approvals** tab.
Items & Approvals

1. Under the Entitled Actions section, use the scroll bar on the right to scroll down until you find Destroy (Virtual Machine).

Entitled Actions

1. Select the drop down arrow to Modify Policy.
Modify Policy

1. Select **Modify Policy**.

Apply this Policy

1. Select the **drop down arrow** next to Apply this policy:

Select Policy

1. Select **Destroy Virtual Machine Policy [Service Catalog - Resource Action Request - Destroy - Virtual Machine]**
Save Modify Policy

1. Click OK.

![Modify Policy dialog box]

Finish Editing Entitlement

1. Click Finish.

![Edit Entitlement dialog box]
Logout of the clouadmin Account

We will now logout of the clouadmin and log back in with the devuser account to destroy the CentOS Virtual Machine.

1. Click **Logout**.

Log Off Screen

1. Click **"Go back to login page"**. This will take you back to the login screen which will set you up for the next Chapter in the Module.
Request to Destroy a Virtual Machine

Login to vRA with devuser

Login to the vRealize Automation Console with the devuser account.

1. Enter **devuser** in the username field.
2. Enter **VMware1!** in the password field.
3. Click **Sign in**.

Internal Error

Note: You may see the following error appear when logging back in as devuser.

1. Click the X in the top right corner to close the error message.
Home Tab

When you first log into vRealize Automation with the devuser account, you will land on the Home tab. In the My Items section, the user can see the items under their management.

Note: The calendar may show a different calendar month depending what the actual date is when taking this lab.

1. Click CentOS 6.6-23714482 to open the Item Details.
Items Tab

1. Click **Destroy** under the Actions section of the Items tab.

   ![Screenshot of Items Tab]

   **Destroy CentOS**

   A popup window will appear to confirm if you wish to continue and destroy the CentOS Virtual Machine.

   1. Click **Submit**.

   ![Screenshot of Destroy CentOS]

   **Send Feedback**
Request Submission

On the next popup window, you will receive a notification that "The request has been submitted successfully."

1. Click **OK**.

Requests Tab

1. Click the **Requests** tab.

When you previously requested to Destroy the linux VM, you’ll notice the status almost immediately goes to “Pending Approval” within the Request tab.

Pending Approval

In the Requests tab, notice the recent request to Destroy the CentOS machine. Under the Status column, the status will say Pending Approval.

**Note:** The status change to Pending Approval may take a few moments or a page refresh to appear. Please continue to the next step.
Logout of the devuser Account

We will now logout of the devuser and log back in with the devmgr account to approve the pending approval request.

1. Click Logout.

Log Off Screen

1. Click Go back to login page button. This will take you back to the login screen which will set you up for the next Chapter in the Module.
Manager Approval of the Request

Approval policies also have the flexibility to configure accept/deny permissions for users/administrators in various setups. The permissions can be assigned to individual users or to a group of users. The two main setup options you can choose are:

- Anyone can approve: anyone in the given group of users can accept or deny. The first decision is the one that counts.
- All must approve: everyone in the given group of users (even when entering an active directory group) must accept/deny the approval.

Pending approvals can be seen from the Inbox within vRealize Automation or via email if notifications and the email server have been configured. In this section, we will use the Inbox.

Login to vRA with devmgr

Login to the vRealize Automation Console with the devmgr account.

1. Enter devmgr in the username field.
2. Enter VMware1! in the password field.
3. Click Sign in.
Home Tab

When you first log into vRealize Automation with the devmgr account, you will land on the Home tab. In the My Inbox section, the manager can see pending requests that need to be approved.

1. Click the **Item 1**.
Inbox Tab

Within the Inbox, you will see the request to destroy the CentOS Virtual Machine from devuser. A Justification is required, then the manager can Approve or Reject the request from devuser.

1. In the Justification input box, type **Approve**.
2. Click **Approve**.

Note: The devuser will now see this request with a status of "Successful" under their Requests tab.

Logout of the devmgr Account

1. Click **Logout**.

Summary

Approvals are going to be a necessary if your IaaS is going to be successful.

The module is now complete.
Conclusion

Congratulations on completing Module 2!

Providing Governance for sensitive systems for day two operations is a great tool to reduce the overall security risk of the Software Data Center.

In this module we took some time to see that we can leverage vRealize automation and approval policies to provide governance around deleting a sensitive virtual machine the SDDC.

In Module 3 we will show administrators how to automate the remediation of security policies on your ESXi hosts.

Proceed to the next step, or select any module below which interests you most.

- **Module 1 - Deploying The DISA STIG For ESXi Compliance** (30 minutes, Beginning) From the Department of Defense to Financial Entities, the use of DISA Compliance standards is used across a broad set of industries. This lab will show vSphere administrators how to deploy the ESXi VIBS to ensure these ESXi hosts are in compliance with DISA standards.
- **Module 3 - Automating Password Complexity for ESXi users** (30 minutes, Intermediate) 16 characters, don’t use *, at least a number and a special character, but never $. Do these security compliance requirements drive you to drink? If so, this lab is for you! In this lab we will run a PowerCLI script that sets the password complexity rules for ESXi user across every host in your cluster.
- **Module 4 - Forensic Security with LogInsight** (30 minutes, Beginning) In prior versions of vSphere, the audit logs on vSphere hosts did not do a good job of identifying what user made a change. The change was recorded in vCenter, however ESXi logs would show vxpauser as the culprit. Leveraging vSphere 6 detailed logging capabilities and LogInsight, we will show administrators how to audit, who did what, on a particular ESXi host.
OPTIONAL: How to End the Lab

You can now continue on to the next module by clicking forward, or use the Table of Contents to skip to another desired Module.

If you'd like to end your lab, click on the END button.

Note: If you end your lab, you will need to re-register for the lab in order to take any other modules.
Module 3 - Automating Password Complexity for ESXi Users (30 minutes)
Introduction

This article will show administrators how they can automate security policy on all of their ESXi hosts. This particular module will use as an example, setting password complexity for ESXi users. However the intent is to show how this method can be applied to all security policies an administrator would like to automate. So imagine you had one complete script that enforced all of the security guidelines for ESXi. On day zero of provisioning ESXi hosts, you would be in compliance. This will reduce the overall operating expense of securing the Software Defined Data Center.

This Module contains the following lessons:

- **PowerCLI - Automate Password Complexity** This lesson walks through executing a PowerCli script that sets password complexity policy on every ESXi host in your environment.

Script We will Execute

```powershell
#Set the Password Policy
$passwordpolicy = "retry=3 min=disabled,disabled,disabled,7,7"
#Get the list of connected ESXi hosts
$VMHosts = Get-VMHost | Where {$_._.ConnectionState -eq "Connected"}
#Loop through the lists of hosts and set the Advanced Setting
docht ($VMHost in $VMHosts)
    {
        Get-AdvancedSetting -Entity $VMHost -Name Security.PasswordQualityControl | Set-AdvancedSetting -Value $passwordpolicy -Confirm:$false
    }
```
Automate Password Complexity Policy

In this module administrators will leverage PowerCLI to automate password complexity. VMware vSphere PowerCLI provides an easy-to-use Windows PowerShell interface for command-line access to administration tasks or for creating executable scripts. You can read the documentation here


With VMware ESXi 6 the password policy is changed and require to use more complex passwords. The password policy in ESXi 6 has the following requirements:

• Passwords must contain characters from at least three character classes.
• Passwords containing characters from three character classes must be at least seven characters long.
• Passwords containing characters from all four character classes must be at least seven characters long.

An uppercase character that begins a password does not count toward the number of character classes used. A number that ends a password does not count toward the number of character classes used. The ESXi 5 default password policy has the following requirements:

• Passwords containing characters from one or two character classes must be at least eight characters long.
• Passwords containing characters from three character classes must be at least seven characters long.
• Passwords containing characters from all four character classes must be at least six characters long.

The default configuration is for ESXi 5 and ESXi 6 are:

ESXi 5: retry=3 min=8,8,8,7,6

ESXi 6: retry=3 min=disabled,disabled,disabled,7
Execute PowerCLI

1. Double Click on VMware vSphere PowerCLI Icon

![PowerCLI Icon](image)

Navigate to power shell script

1. Type the command "cd c:users\administrator\desktop"
2. Type the command cd "lab files"

![PowerCLI Console](image)

Search For Script

1. type the command "ls"
2. You should see the power shell script named "password.ps1"
This script contains the following code, which leverages the advanced ESXi settings to change the complexity. For ESXi hosts, you have to use a password with predefined requirements. You can change the required length and character class requirement or allow pass phrases using the Security.PasswordQualityControl advanced option.

#script begins here

Connect-VIServer -server vcsa-01a.corp.local -user administrator@vsphere.local -password VMware1!

#Set the Password Policy

$passwordpolicy = "retry=3 min=disabled,disabled,disabled,7,7"

#Get the list of connected ESXi hosts

$VMHosts = Get-VMHost | Where {$_-ConnectionState -eq "Connected"}

#Loop through the lists of hosts and set the Advanced Setting

foreach ($VMHost in $VMHosts) {

Get-AdvancedSetting -Entity $VMHost -Name Security.PasswordQualityControl |Set-AdvancedSetting -Value $passwordpolicy -Confirm:$false

}
Execute Script

1. type the command ".\passwd.ps1"

2. Notice how we set the password complexity value to "retry=3 min=disabled,disabled,disabled,7,7"

The following password candidates illustrate potential passwords if the option is set to retry=3 min=disabled,disabled,disabled,7,7

That means that passwords with one or two character classes and pass phrases are not allowed, as indicated by the first three disabled items. Passwords from three and four character classes require seven characters.
Verify Change on ESXi Host

1. Click on All Programs
2. Click On Putty to Open Putty
SSH to ESXi Host

1. Click on "esxi-01a.corp.local"
2. Click on "Load"
3. Click on "Open"
Verify Change Was Made

1. Type the command "cd /etc/pam.d"

2. type the command "cat passwd"

3. You should see your changes and the proper complexity settings loading with pam. Please feel free to repeat with esx-02a to see the change was made against multiple hosts.
Conclusion

Congratulations on completing Module 3!

Leveraging scripts to re-mediate security policies that our out of compliance is a key way to reduce the overall security risk of the Software Data Center and lower the associated operating expense of securing your systems.

In this module we took some time to see how we can leverage powerCLI to automate password complexity settings, this also can apply to a myriad of security settings.

In Module 3 we will show administrators how to automate the remediation of security policies on your ESXi hosts.

Proceed to the next step, or select any module below which interests you most.

- **Module 1 - Deploying The DISA STIG For ESXi Compliance** (30 minutes, Beginning) From the Department of Defense to Financial Entities, the use of DISA Compliance standards is used across a broad set of industries. This lab will show vSphere administrators how to deploy the ESXi VIBS to ensure there ESXi hosts are in compliance with DISA standards.

- **Module 2 - Governance In a Secure World** (30 minutes, Intermediate) Have you ever hired a contract or temporary worker who has not yet passed your security process? How fantastic would it be to limit and govern the type of day two actions they perform on a virtual machine! In this module we will show cloud administrators, how they can leverage approvals in vRealize Automation, to limit day two actions for virtual machines users in vRA.

- **Module 4 - Forensic Security with LogInsight** (30 minutes, Beginning) In prior versions of vSphere, the audit logs on vSphere hosts did not do a good job of identifying what user made a change. The change was recorded in vCenter, however ESXi logs would show vxpauser as the culprit. Leveraging vSphere 6 detailed logging capabilities and LogInsight, we will show administrators how to audit, who did what, on a particular ESXi host.
OPTIONAL: How to End the Lab

You can now continue on to the next module by clicking forward, or use the Table of Contents to skip to another desired Module.

If you'd like to end your lab, click on the END button.

**Note:** If you end your lab, you will need to re-register for the lab in order to take any other modules.
Module 4 - Forensic Security with vRealize Log Insight (30 minutes)
Introduction

This module shows how a vSphere administrator can use the new logging capabilities in vSphere 6.0 and vRealize Log Insight to show who actually did what, in vCenter. This module will also show how you can create a custom dashboard to give administrators a rapid view of whom rebooted a virtual machine as well as valid and unauthorized login attempt to ESXi. We also explore the security dashboards from the Linux Content Pack.

This Module contains the following lessons:

- **vRealize Log Insight - Perform Security Audit Actions.** This lesson walks through performing security audit actions by rebooting a virtual machine in vCenter as well as performing a valid and unauthorized login attempt to ESXi.
- **vRealize Log Insight - Create Audit Query & Custom Dashboard.** This lesson walks through creating a query that shows whom rebooted a virtual machine in vCenter as well as creating a custom dashboard based on that query.
- **vRealize Log Insight - Analyze Linux Content Pack Security Dashboard.** This lesson walks through analyzing a security dashboard from the Linux Content Pack.

The Problem In Prior Versions of vSphere

Prior to 6.0, actions taken at the vCenter level by a named user would show up in ESXi logs with the “vpuxuser” username.

- [user=vpuxuser]
- This made for difficult forensic tracking of user actions.

In 6.0, all actions taken at vCenter against an ESXi server now show up in the ESXi logs with the vCenter username

- [user=vpuxuser:CORP\Administrator]
Perform Security Audit Actions

Before we get started analyzing the data in vRealize Log Insight, we will need to perform some security audit actions to mimic events that may occur inside of your organization.

We will restart a virtual machine in vCenter as well as logging into ESXi as root and logging into ESXi as an unauthorized user. We will be using ESXi to showcase this functionality, but the systems could also be any Windows or Linux operating system in addition to storage and network devices. vRealize Log Insight can consume logs from anywhere!

Open Firefox

1. Click on Firefox in the windows task bar

Reboot a Machine In vCenter

The following steps will have you login to vCenter using the web client and restart the guest OS of a VM.
Login to vCenter

The following steps will be performed from within the vSphere Web Client.

1. Click on **vCenter - Region A** from the bookmarks tool bar
2. Click the **checkbox** that reads "Use Windows session authentication"
3. Click on **Login**

**Note:** If you take this Module before the other modules in this lab, then logging in my take a minute or two while vCenter loads.
Navigate to VM

1. Click on **Hosts and Clusters**
Reboot VM

1. Right click the VM called "app-01a"
2. Select **Power**
3. Select **Restart Guest OS**
Confirm Guest Restart

1. Click **Yes** to confirm guest restart

You are now done performing tasks inside of the vSphere Web Client. Keep Firefox open as you will need to use this to access vRealize Log Insight in the next lesson.

Login as root

The following steps will have you log in to an ESXi host as root with proper credentials to mimic a proper login.

Open Putty

1. Click the **putty icon** in the Windows Taskbar
Login to esx-01a.corp.local as root

We will now login to esx-01.corp.local as root using a saved session.

1. Double click **esx-01a.corp.local**
Root Authentication

You can now see the username "root" was automatically logged in to esx-01a.corp.local and authenticated with a public key.
New Session

We are finished with this session and need to open a new putty session.

1. To use the system menu of the application's icon, on the top left corner of the Putty window, click the icon and notice that a menu displays
2. Select New Session...

Login as admin

The following steps will have you log in to the same ESXi host as before with admin with invalid credentials to mimic a login attempt from an unauthorized user.
Connect to esx-01a.corp.local

1. Type `esx-01a.corp.local` in the Host Name field
2. Click Open
Access Denied - admin

We will now purposefully attempt to login as the admin account with a bad password.

1. Type admin next to "login as:" then press Enter on the keyboard
2. Type admin next to "Password:" then press Enter on the keyboard
3. Exit both of the Putty session's by selecting the red X in the top right corner of each window

Note: Access denied is the desired response after Step 2.

Putty Exit Confirmation

1. Click OK to confirm the exit of each Putty session
Create Audit Query & Dashboard

VMware vRealize Log Insight delivers heterogeneous and highly scalable log management with intuitive, actionable dashboards, sophisticated analytics and broad third party extensibility, providing deep operational visibility and faster troubleshooting.

**Intelligent and Extensible**

Integrates with vRealize Operations and many other vendors to provide proactive management capabilities to infrastructure and applications across physical, virtual and cloud environments.

**Highly Scalable**

Analyzes massive amounts of log data generated in dynamic, heterogeneous infrastructures in near real-time and applies sophisticated analytics to solve complex IT problems.

**Intuitive and Affordable**

Provides powerful built-in and customizable dashboards with easy to understand problem analysis and meaningful, actionable results with an unlimited-data pricing structure.

**Free Log Insight for vCenter**

For each instance of vCenter Server that you own or purchase you are entitled to a free 25 OSI license of vRealize Log Insight for vCenter.

https://www.vmware.com/products/vrealize-log-insight#sthash.fh9I8E7F.dpuf

**Open vRealize Log insight**

Let's access vRealize Log Insight

1. Click the **vRealize Log Insight** from the bookmark toolbar
Log in to vRealize Log Insight

Once the vRealize Log Insight login screen appears,

1. Enter the following credentials:
   - **User name:** admin
   - **Password:** VMware1!

   **Note:** The password field potentially will auto populate, this is normal.

2. Click **Login**

![Login Screen](image)

Dashboards General Overview

Note: We can safely ignore the 'Evaluation License' warning, as temporary license keys are applied for the life of each Hands On Lab.

1. **Content Packs.** This is the **General** content. You can click the drop down icon to see where this content pack resides compared to others.
2. **Dashboards.** This is a list of the dashboards available in the selected content pack. Here, the **Overview** dashboard is selected which is what we see in the main panel.
3. **Time Range.** Here you can set the data time range from 5 minutes - 48 hours, or a custom time range, for the selected dashboard.
4. **Filters.** Filters available to the selected dashboard are defined here, to focus the query only to relevant information.
5. **Widgets.** The main panel contains Widgets for the selected dashboard. Widgets are a representation of the data selected in the preceding areas, displayed using graphs, charts, figures, and more.
6. **Information.** For more information on each widget, hover the cursor over the widget and click on its Information icon.

---

**Interactive Analytics**

Interactive Analytics allows administrators and engineers to drill down into log messages, to determine problem areas, and to perform root cause analysis.

1. Click on **Interactive Analytics**
Create Query

**Note:** LogInsight provides suggested queries and phrases based on indexed log files when typing for each input.

1. In the query bar type "reboot"
2. Add a filter by clicking on the plus sign next to "Add Filter"
3. In the filter search for "text" select "contains" and type administrator
4. Change the time range from "Latest 5 minutes of data" to "Latest hour of data"
5. Click the **Magnifying glass** to search.

Here we can see that Administrator was the user that rebooted app-01a.
Create Dashboard Based On Query

Notice the circled results of the query shows that the Guest OS for app-01a was rebooted on esx-01a in ha-datacenter.

1. Click the "Add current query to dashboard" button

Save Dashboard

1. Type "Administrator Reboot Dashboard" in the Name field
2. Click Add
Navigate to Dashboards

1. Click **Dashboards** link at the top of the screen

![Dashboards Link](image1)

Navigate to My Dashboards

1. Click on **General** to bring up the list of dashboards
2. Click on **My Dashboards**

![My Dashboards](image2)

Administrator Reboot Dashboard

Here we can see the new widget called Administrator Reboot Dashboard that now exists in Dashboard 1. vRealize Log Insight users have the ability to create custom dashboards and queries for a variety of items based on their needs. The out of the box content packs provide an idea of some common scenarios, but think about what other dashboards might be important to you.

**Note:** The dashboard widget defaults to “Latest 5 minutes of data.” If you happen to take longer than 5 minutes, the dashboard may show no results so you may need to change the dashboard to “Last hour of Data” as highlighted above, then select **Update.**
In the next section, we will analyze a security dashboard of the Linux Content Pack.
Analyze Linux Content Pack Security Dashboard

The content pack for Linux provides you with information about key entities of any Linux operating system installation’s health using Log Insight’s ability to monitor filesystem logs.

There are 12 pre-defined Linux OS specific dashboards, with total of 45 extracted field for helping to visualize, analyze and take meaningful action on Linux OS log information. It provides:

- Security monitoring: Including SSH, su and sudo for auditing and incident management.
- System application events: Including Cron and NTP for daemon process monitoring.
- Email information: For Postfix and Sendmail making it possible to troubleshoot and manage mail servers.
- Syslog information: For Rsyslog and Syslog-NG making it possible to troubleshoot and manage third-party syslog agents.
Linux Content Pack

The Linux Content Pack has already been installed. Let's analyze some of its data based on the security audit actions we previously performed.

1. Click **General** content pack to present the available content packs that are currently installed
2. Select **Linux** content pack

This will open the Linux content pack and placed on the Security - Overview dashboard
Security - SSH Dashboard

We will select the Security - SSH dashboard and need to change the time range from "Latest 5 minutes of data" to "Latest hour of data" in order to capture the events that we previously initiated.

1. Click Security - SSH dashboard
2. Click the drop down for "Latest 5 minutes of data"
3. Select "Latest hour of data"

SSH events

Below is a brief summary of what's included on the Security - SSH dashboard that contains 4 widgets out of the box.

SSH events by source and destination - This widget can be helpful in tracking down user activity especially during security related incidents such as DDOS attacks.

SSH events by user - This widget shows frequent users attempting SSH attempts.

SSH events by status - This widget shows the status of the SSH operations. Note that multiple different types of failed messages exist though only a small number of successful messages exists.

SSH events by user and destination - This widget shows user SSH attempts per destination.
1. Hover over the **SSH events by status** widget until a toolbar appears, then click on the **magnifying glass** to open the widget's underlying query in Interactive Analytics.
Query in Interactive Analytics

Notice the query is already populated. This will now give you the ability to customize the chart type or constraints of the query if you wish to customize to suit your needs.

1. Return to the dashboards page by selecting back in the browser.
Microsoft - Windows Content Pack

1. Click Linux Dashboards to pull up a menu of the other Content Pack Dashboards
2. Select Microsoft - Windows

Review Microsoft - Windows Dashboards

There is also security related dashboards Microsoft - Windows content pack with Security related dashboards as well, but that is out of the scope for this current lab
Microsoft - Windows Content Pack

1. Click **Microsoft - Windows** Dashboards to pull up a menu of the other Content Pack Dashboards
2. Select **Microsoft - Active Directory**
Review Microsoft - Active Directory Dashboards

Additional security related dashboards Microsoft - Active Directory content pack with Security related dashboards as well, but that is out of the scope for this current lab.

We highly encourage you to take advantage of all of the content packs that are available which can help meet some of your security requirements. Only a small subset of content packs are installed in this lab.
Conclusion

Congratulations on completing Module 4!

Leveraging vRealize Log Insight to audit users to see whom did what, is a valuable solution for security administrators to analyze security incidents in the Software Defined Data Center.

In this module we took some time look at the new logging features in vSphere 6 as well as the Linux Content Pack. We were able to build out a helpful query to understand whom exactly rebooted a machine.

This is the last module, you can end your time or select any module below which interests you most.

- **Module 1 - Deploying The DISA STIG For ESXi Compliance** (30 minutes, Beginning) From the Department of Defense to Financial Entities, the use of DISA Compliance standards is used across a broad set of industries. This lab will show vSphere administrators how to deploy the ESXi VIBS to ensure there ESXi hosts are in compliance with DISA standards.

- **Module 2 - Governance In a Secure World** (30 minutes, Intermediate) Have you ever hired a contract or temporary worker who has not yet passed your security process? How fantastic would it be to limit and govern the type of day two actions they perform on a virtual machine! In this module we will show cloud administrators, how they can leverage approvals in vRealize Automation, to limit day two actions for virtual machines users in vRA.

- **Module 3 - Automating Password Complexity for ESXi users** (30 minutes, Intermediate) 16 characters, dont use *, at least a number and a special character, but never $. Do these security compliance requirements drive you to drink? If so, this lab is for you! In this lab we will run a PowerCLI script that sets the password complexity rules for ESXi user across every host in your cluster.

**OPTIONAL: How to End the Lab**

You can now continue on to the next module by clicking forward, or use the Table of Contents to skip to another desired Module.

If you’d like to end your lab, click on the **END** button.

**Note:** If you end your lab, you will need to re-register for the lab in order to take any other modules.
Conclusion

Thank you for participating in the VMware Hands-on Labs. Be sure to visit http://hol.vmware.com/ to continue your lab experience online.

Lab SKU: HOL-1706-SDC-3

Version: 20161024-125317