# Table of Contents

Lab Overview - HOL-1901-02-CMP - Optimize Performance and Assess vSphere Configuration and Compliance with vRealize Operations ................................................................. 2
  Lab Guidance ........................................................................................................ 3
Module 1 - Optimize Workloads Based on Business or Operational Intent with vRealize Operations (60 minutes) ........................................................................................................ 9
  Introduction .......................................................................................................... 10
  Log in to the vRealize Operations Live Instance .................................................... 11
  Optimize Performance based on Workload ............................................................. 15
  Optimize Placement based on vSphere Tags .......................................................... 37
  Automating Performance Optimization ................................................................ 53
  Conclusion ............................................................................................................. 61
Module 2 - Rightsize the Configuration of Oversized or Undersized VMs with vRealize Operations (45 minutes) ......................................................................................... 62
  Introduction .......................................................................................................... 63
  Log in to the vRealize Operations HVM instance .................................................... 64
  Optimize Performance Dashboard Overview .......................................................... 67
  Optimize Capacity - Reclaim Dashboard Overview ................................................ 76
  Using Views to Identify Undersized and Oversized VMs ......................................... 90
  Conclusion ............................................................................................................. 98
Module 3 - vSphere Optimization Recommendations with vRealize Operations (15 minutes) ......................................................................................................................... 99
  Introduction .......................................................................................................... 100
  Log in to the vRealize Operations HVM instance .................................................... 101
  Optimization Recommendations ............................................................................ 104
  Conclusion ............................................................................................................. 112
Module 4 - Assess vSphere Configuration with vRealize Operations (15 Minutes) ........ 113
  Introduction .......................................................................................................... 114
  Log in to the vRealize Operations HVM instance .................................................... 115
  Overview of Configuration Dashboards ................................................................... 118
  Conclusion ............................................................................................................. 132
Module 5 - Assess vSphere Compliance Against Standards with vRealize Operations (30 Minutes) ............................................................................................................. 133
  Introduction to vSphere Compliance ...................................................................... 134
  Log into the vRealize Operations Live Instance ..................................................... 135
  Ensuring Compliance of vSphere Objects .............................................................. 139
  Infrastructure Compliance With PCI and HIPAA Standards .................................. 157
  Conclusion ............................................................................................................. 175
Lab Overview - HOL-1901-02-CMP - Optimize Performance and Assess vSphere Configuration and Compliance with vRealize Operations
Lab Guidance

Note: It will take more than 90 minutes to complete all modules in this lab. You should expect to only finish 2-3 of the modules during your time unless you extend your session. The modules are independent of each other so you can start at the beginning of any module and proceed from there. You can use the Table of Contents to access any module of your choosing.

The Table of Contents can be accessed in the upper right-hand corner of the Lab Manual.

Using vRealize Operations, we are going to take you through the optimization content for a vSphere environment. The modules will take you through the assessment of vSphere performance, balancing workloads across clusters, right-sizing under-utilized and over-utilized virtual machines, and assessing the configuration of the vSphere environment and compliance with standards.

After completing the lab modules, you will be better prepared to navigate the vRealize Operations console when evaluating performance.

Lab Module List:

- **Module 1 - Optimize Workloads Based on Business or Operational Intent with vRealize Operations (60 minutes)**
- **Module 2 - Rightsize the Configuration of Oversized or Undersized VMs with vRealize Operations (45 minutes)**
- **Module 3 - vSphere Optimization Recommendations with vRealize Operations (15 minutes)**
- **Module 4 - Assess vSphere Configuration with vRealize Operations (15 minutes)**
- **Module 5 - Access vSphere Compliance Against Standards with vRealize Operations (30 minutes)**

Lab Captains:

- Modules 1-3 - Jack White, Cloud Management Specialist SE, USA - Ohio
- Module 4 - Jase Machado, Cloud Management Specialist SE, USA - California
- Module 5 - Michael Lapham, Cloud Management Specialist SE, USA - New Jersey

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

http://docs.hol.vmware.com
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.

**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.
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.

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 - Optimize Workloads Based on Business or Operational Intent with vRealize Operations (60 minutes)


Introduction

This Module will take us through Workload optimization.

In this module we will go through the following during the scenario:

- Configuring Workload Optimization
- Using Workload Optimization
- Manage Optimization Schedules
- Workload Automation Policy Settings
- View DRS Summary
- Optimize Schedules
- Optimize Placement
Log in to the vRealize Operations Live Instance

This lab environment is running three different instances of vRealize Operations and one instance of vRealize Log Insight. We have the different vRealize Operations instances in order to be able to work through different use cases that have unique requirements. The lab instances are as follows:

- Live Instance: Connected to the small running vSphere environment in the lab. There isn't a large inventory of objects in this instance but it allows us to interact with vCenter.
- Historical Instance: Running a 30-minute time loop of data that was captured in the past. This instance has a much larger inventory of objects but since it is not currently connected to a vCenter, we can't perform any actions here.
- Blue Medora Management Packs: Also running in historical mode, this instance has a large number of management packs from Blue Medora that allow us to see information from adjacent infrastructure (storage and physical servers) as well as operating system and application information.

In this lesson we will be using the Live Instance of vRealize Operations.

If you are already logged into the live (not historical) instance of vRealize Operations, click to skip ahead.

Open the Chrome Browser from Windows Quick Launch Task Bar

If your browser isn't already open, launch Google Chrome

1. Click the Chrome icon on the Windows Quick Launch Task Bar
Open the vRealize Operations - Live Instance Tab

The browser home page has links to the different instances of vRealize Operations that are running in the lab.

1. Click the **vRealize Operations - Live Instance** link to open the UI in a new browser tab
Log in to vRealize Operations

vRealize Operations is integrated with VMware Identity Manager which we will use for user authentication in this lab.

VMware Identity Manager should be pre-selected as the identity source. However, if it is not you will choose it.

Click the drop-down arrow

1. Select **VMware Identity Manager**
2. Click **REDIRECT** to take you to the user login page
VMware Identity Manager Login

The user and password information should already be filled out. However, if needed type them in.

USER: hol

PASSWORD: VMware1!

1. Click Sign in
Optimize Performance based on Workload

In this lesson we will work our way through Workload Optimization. We can view and manage DRS settings along with managing Workload Optimization. DRS (Distributed Resource Scheduler) is used to keep a cluster balanced based on workload. With Workload Optimization, it works to keep resources balanced across multiple clusters. When you're using vCenter Server 6.5 or newer, we have the ability to use Predictive DRS. With Predictive DRS, an hour before a workload occurs (based on historical trends), resources are moved to ensure better balance and better performance in the environment.

Go to Home

You should be on the 'Home' tab. If not:

1. Click on Home
Workload Optimization

In Optimize Performance:

1. Click **Workload Optimization**

Datacenter Selection

RegionA01 is not optimized

1. Click on **Not Optimized**
Optimization Recommendation

The first widget entitled ‘Optimization Recommendation’, the status is ‘Not Optimized’ and we’re given recommendations to set DRS to fully automated.

We require DRS to allow clusters to be more optimized. Workload Optimization can optimize across multiple clusters.

The widget below ‘Optimization Recommendation’ is where we can configure the DRS settings per cluster.
1. Just a note before going further. For the upcoming instructions, we may need to perform a refresh. Use the circular arrow as identified above to refresh the content on the display.

Clusters to configure
Scroll down to view the DRS settings.

Both clusters are configured to ‘Partial Automated’ with a Migration threshold set to ‘Default’

1. Expand the column if necessary to view the cluster name.

**Set DRS Automation**

![Set DRS Automation Diagram]

1. Select the first row for **RegionA01-COMP01**
2. Click on **SET DRS AUTOMATION**

**Automation Level**

![Automation Level Diagram]

In order to set the DRS automation level to Fully Automated:
1. Click the drop-down arrow and select **Fully Automated**
2. Click **BEGIN ACTION**

**Task ID**

You will see a pop up window with the Task ID. Your ID will be different than the one displayed.

1. Click on the task link.

**The Task**

You are now in the ‘Recent task’ view where you can inspect the process you just initiated. You should see that the task has completed and the result is a success. You may need to click on the refresh icon at the top right of the vRealize Operations
interface. You may need to refresh the browser to see the process update. Remember to use the circular arrow in the top-right corner of the display to refresh.

1. Once status shows completed
2. Click the vRealize Operations BACK button

Set DRS Automation

We need to set the second cluster's DRS Settings just like we did the first cluster.

1. Select the other cluster ‘RegionA01-COMP02’
2. Click SET DRS AUTOMATION as we did for the first cluster.
Adjust the DRS Settings

1. Change the Automation Level to 'Fully Automated'
2. Click BEGIN ACTION

Task ID

1. Click on the task id to ensure this completes successfully too.
Task Process

1. Once the task is completed (Refresh with the circular arrow in the top-right corner of the display)
2. Click the vRealize Operations **BACK** button.

Optimize Now

With both clusters set to ‘Fully Automated’ and ‘Default’ Migration threshold, the ‘Optimization Recommendation’ will let us know that we can optimize our Datacenter by moving workloads.
1. Click **OPTIMIZE NOW**

**Before and After**

The ‘Optimize Placement’ process will take a little bit of time. Allow it to complete. Once completed, you will see before and after results. Pay attention to the CPU and Memory workloads in the before and after values. This gives us an indication of the resource utilization once the optimization is complete.

In this screenshot, the memory is not balanced before the optimization. After the optimization is completed, memory will be more balanced between the two clusters.

**Note:** After we click NEXT, on the next screen we will review the data and then cancel to make some further changes.

1. Click **NEXT**
Review Moves

On the next screen, we see the moves that are about to happen. Before we make any changes, we are going to go back and change the Migration Threshold settings for DRS.

1. Click **CANCEL**.

Migration Threshold

For the previous setting, we are using the default migration threshold for DRS. Let's take a look at the results with a higher migration threshold setting. For the DRS Settings, change the Migration Threshold from ‘Default’ to ‘Aggressive’.

For each cluster listed, select one at a time and set the DRS Automation level.

1. Select one of the clusters
2. Click **SET DRS AUTOMATION**
You will repeat this process to set the automation level of the second cluster too.

**Most Aggressive Threshold**

1. Change the Migration Threshold to ‘**Most Aggressive**’
2. Click **BEGIN ACTION**.

**Another Task ID**

1. Review the task ID
Task Process

You may need to refresh the browser to see the process update.

1. Once Status shows **Completed**,  
2. Click the vRealize Operations **BACK** button.

**Remember to do the same settings for the other cluster.**

Once the second cluster is modified, watch the Task like we did earlier to confirm the process has completed. Again, use the circular arrow in the top-right to refresh the display.

**DRS Settings Updated**

The DRS setting for both clusters should match the graphic (Fully Automated and Most Aggressive):
Optimize Now

Now that both clusters are Fully Automated with a Most Aggressive Migration Threshold, we will run the optimization process.

1. Click **OPTIMIZE NOW**

Before and After

Examine the Before and After results. Notice our clusters are nearly the same as before.

Even though we have made changes to DRS, each cluster still has the same utilization. DRS is working within the cluster and not across multiple clusters. The settings we
have modified will ensure that each cluster will work to stay more balanced. With workload optimization, we will allow the virtual machines to be placed in different clusters allowing for better resource utilization.

1. Click **NEXT**

**Review Moves**

Examine the moves that will be performed if we accept the optimization settings. The moves depicted here will ensure the resource utilization of each cluster will be more optimized.

We need to cancel at this time for a couple of reasons. We want to view the impact on the cluster without making changes and we are going to go through some additional settings that require this lab to remain the way it is now.

1. Click **CANCEL**
In the center of the Workload Optimization screen, you will see ‘Placement Settings’

In ‘Placement Settings’ we can configure how placement occurs across multiple clusters. In this widget, we show three clusters. Above the clusters, we see the message ‘Utilization Objective: Balance.’ For the current setting, workload optimization will attempt to keep all clusters equally utilized. Also, notice in the upper right corner of the widget, you see ‘Tag Applied’ with a small circle to the left. We’ll discuss this in the settings.

1. Click **EDIT SETTINGS**
Policy Settings

In the ‘Workload Automation Policy Settings’ window, there are 3 categories:

- Workload Optimization
- Cluster Headroom
- Tag Based VM Placement

We will go through each of these settings. You may need to unlock the settings.

1. Click on the **lock icon** to toggle between locked and unlocked.

**Make sure each are unlocked.**
Workload Optimization

By sliding the workload Optimization setting to the right, we can configure workload placement to be more aggressive in its consolidation. This will place the workloads into as few clusters as possible.

Sliding the lever to the left will configure workload optimization to be more balanced. This will better ensure that each cluster in the selected datacenter has a more equal workload to the other clusters.

1. Slide the lever to the right to make a more consolidated configuration.
Cluster headroom can be configured to allow for a buffer in clusters. A zero setting tells the configuration to use all the resources in the cluster. Sliding the lever to the right will increase the amount of space to buffer.

1. Slide the lever to the center to create a 25% headroom.
2. Click SAVE
The workload optimization will run at the scheduled time for 10 consecutive days based on this configuration. It is possible to create symptoms that would trigger an alarm where workload optimization could be a recommended action.

In the ‘Optimization Recommendation’ widget:

1. Click ‘OPTIMIZE NOW’
Optimization

Based on our settings, we now have nothing to optimize. We configured the optimization to use 25% headroom in each cluster. We also made a change to put workload on the first cluster before placing workload on the second cluster. With the headroom configuration, the optimization process no longer recognizes any room to move resources between the clusters.

If there is any work to do, you will see the before and after recommendations screen. If the datacenter is balanced based on the settings, you will see that the selected containers cannot be improved.

It is possible to create custom Datacenters, assign selected clusters to that custom Datacenter and perform workload optimization specific to that object.

It is also possible to automate this process. To automate Workload Optimization. An alert can be created with symptoms that could trigger the rebalance action. The alert can be set to automated in the policy for the selected Datacenter or custom Datacenter.
HOL-1901-05-CMP Module 3 - Symptoms, recommendations and alerts covers the automation concept.

This is a very powerful and agile tool. The ability to have an environment where virtual machines can run where the resources exist. End users don't care where their resources come from. This gives an administrator the ability to fully utilize hosts and possibly remove under-utilized hosts from contracts or service.

Next we will look at Tag-based Optimization for Workloads.
Optimize Placement based on vSphere Tags

If you have been following the module in order, we just went through workload optimization as a basic level. In this lesson, we are going to continue the conversation and show how tags can aide in the placement of resources.

If you skipped the last lesson, it's okay. Stay with this lesson to see how tags can possibly improve the placement and management of resources.

With Workload Optimization, resources like CPU, Memory and Storage can be optimized across multiple clusters. We know that DRS will keep a cluster more balanced. Workload optimization takes an additional step to ensure multiple clusters are more optimized.
Go Home

Make sure we are on the home screen and navigate to Workload Optimization.

1. Click **HOME**
2. Click **Workload Optimization**
We need to make sure our placement settings are set back to their defaults.

1. Click **EDIT SETTINGS**
1. Set Workload Optimization to **Balance**
2. Set Cluster Headroom to **0%**
3. Click **SAVE**
Stop and Check

You should be looking at a screen that is similar to the one in the image.

From this perspective, we know that the first cluster is green for CPU and Memory workload. The second cluster is green for CPU Workload but red for Memory (indicating 100% or higher workload).

With Workload Optimization, we can move the virtual machines across clusters making sure they have enough resources to run efficiently.

With DRS, we can create affinity rules to ensure a VM is always run on a specific host. We can also use DRS to ensure a VM will never run on a host with anti-affinity rules. Some vendors license their products based on the host where their software runs. Another reason for keeping virtual machines on specific hosts may be compliance. As an administrator, you may want to keep storage tiers separated for performance as well.

With Workload Optimization, we can keep virtual machines pinned to selected hosts across multiple clusters. Now we give you the flexibility to keep clusters more balanced while you maintain license agreements or keep storage assigned for the correct use.
Open vCenter Server

1. Open a new tab in chrome
2. Click on the HTML5 Client Bookmark

**vCenter Server Authentication**

The User name and Password should be pre-filled. If not use the following:

- administrator@vsphere.local
- VMware1!

1. Click **Login**
View Tags

Once you are logged into vCenter server, we will examine some tags that we have already created for this exercise.

1. Click on **Menu**
2. Click **Tags & Custom Attributes**
Compliance Tags

For this lesson, we have already created four tags. You should see HIPAA and PCI for Compliance category. We also have the Performance Tier (PerfTier) category with tags Gold and Silver. For this lesson we are going to use the compliance tags.

Hosts

Navigate to the Hosts and Clusters section
1. Click on **Menu**
2. Click **Hosts and Clusters**

**Host Tags**

We have assigned tags to a couple of hosts. Here you will see the tags associated with the first host.

1. Click on **esx-01a.corp.local**
2. Scroll down and view the assigned tag of **HIPAA**
The other host

1. Click on **esx-04a.corp.local**
2. Scroll down and examine the **PCI** tag

We have two hosts with assigned tags. Let's take a look at the virtual machines for this lesson.

**First Tagged VM**
1. Click on the VM **app-01a**
2. Scroll down and view the assigned tag **HIPAA**

The Other VM Tagged

![Image of virtual machine with tags](image)

1. Click on **base-w12-01**
2. Examine the tag for **PCI**

We have two virtual machines that are tagged. When we run workload placement, we will make sure to include the tags as a priority. Let's go back to vRealize Operations.

Back to vROps

1. Click on the Chrome Tab **'Workload Optimization'**
Placement Settings

1. Click **EDIT SETTINGS**

Tag Based VM Placement
Using Tags, we can ensure VMs that are tagged will only be moved to hosts with matching tags. This is important for many reasons. Some vendors license their products based on the host their product runs on. For this lesson, we are going to prioritize our compliance tags

1. Enter the category ‘Compliance’
2. Enter the tag ‘HIPAA’
3. Click INCLUDE TAG

Another Tag

1. Enter the tag ‘Compliance’
2. Enter the tag ‘PCI’
3. Click INCLUDE TAG
Tag Priority

Under non-prioritized tags, we see the two tags just created.

1. Click ‘Enable Prioritization’
2. Drag PCI to the right to make it a priority (both tags will move as we are actually prioritizing compliance).
3. Click SAVE

Optimize Now

1. Click OPTIMIZE NOW
Optimize Placement

This process may take a minute or two. Let it complete.

Before and After

We can see the before and after results should we continue our optimization process. Notice the memory and CPU workloads on the two clusters. The second cluster is over 100% in the 'before' stage. In the 'after' stage, both clusters are below 100%. The first cluster will have a higher memory workload once the resources are moved.
1. Click **NEXT**

**Review Moves**

We see that the moves that would occur do not include the virtual machines with tags. Those resources were already on the hosts with the same tag. We have ensured they remain in place with the tag settings that we have implemented.

Feel free to play around with the tag settings. You may change the values in vCenter, assign new tags, etc. Keep in mind, changing a value in vCenter will require vRealize Operations to go through a collection cycle. The default settings for a collection cycle in vRealize Operations is 5 minutes.

**Lesson End**

Up to this point, we have gone through the process to configure workload placement. In our next lesson we will go through the process to automate this process.
Automating Performance Optimization

In this lesson, we will demonstrate the ability to automate performance optimization. We have the ability to run on a schedule as well as automating an action that is triggered through an alert process.

Home

Make sure we are on the home screen and navigate to Workload Optimization.

1. Click HOME
2. Click Workload Optimization
Schedule Optimization

1. Click **SCHEDULE**
Manage Rebalance Schedules

The first option to automate workload optimization is with a schedule. We will create a schedule with the following parameters:

1. Schedule Name: **Rebalance Daily**
2. Time Zone: **Host**
3. Recurrence: **Daily**
4. Start on: <Choose any time> / **Repeat every day**
5. Expire after **10** runs
6. Click **SAVE**

With these settings, the workload optimization will run for the next 10 days at the time specified. The settings for the optimization were completed in the previous lesson. Those settings will be applied for each of these runs.
Automation through alerts

1. Click Alerts
2. Expand Alert Settings

Alert Definitions

1. Click on Alert Definitions
2. Type 'Optimiz' and press enter

With the filter in place, we can see two predefined alerts that match. The first alert has an Object Type 'Custom Datacenter'. The second alert has an Object Type 'Datacenter'.

A Datacenter is learned from the registered vCenter Server. A Custom Datacenter is an object that can be created in vRealize Operations.
View the Alert Definition

1. With the first row selected, click the edit icon.
Symptoms in the Alert

Within vRealize Operations, there is a metric that is set when a Custom Datacenter or a Datacenter needs rebalanced. If that metric is true, the symptom we see in the alert definition will cause the alert to trigger. When the alert triggers, one or more recommendations will be given.

The Recommendations

You may need to scroll down in the window to get to the Recommendations.

We can see two recommendations for this alert. The first is a recommendation to 'Rebalance the container to optimize workload placement'. The recommendation has an associated action called 'Optimize Container'.

When an alert is triggered, an action associated to a recommendation will appear as a button or a link to the action. That is a manual process. We can automate that process.
by modifying the policy. We will go over that here in a quick way. If you would like a deeper dive into alerts, see module 1901-05 Module 3.

1. Click **CANCEL**

**Policies**

1. Click **Administration**
2. Click **Policies**

**Edit Policy**
1. Click **Policy Library**
2. Select the policy 'HOL Default Policy'
3. Click the edit icon

**Alert Settings**

![Edit Monitoring Policy](image)

1. Go to Section 6
2. Enter 'Custom Datacenter' in the Object Type field
3. Click the Automate drop-down selector

The default setting is disabled and inherited. We can set the option to enabled Local. When enabled, the alert will automatically start the associated action.

This can be a powerful option. Other alerts can be automated as well. Keep in mind, an automated action will run when the alert is triggered.

**Lesson End**

In this lesson we went through the process to automate the workload placement process. In the next lesson we'll take a look at enabling predictive DRS (pDRS).
Conclusion

This module covered the following scenario's.

- Configuring Workload Optimization
- Using Workload Optimization
- Manage Optimization Schedules
- Workload Automation Policy Settings
- View DRS Summary
- Optimize Schedules
- Optimize Placement

You've finished module 1

Congratulations on completing module 1.

If you are looking for additional information on vRealize Operations, you can start here: [https://www.vmware.com/products/vrealize-suite.html](https://www.vmware.com/products/vrealize-suite.html)

You may proceed to the next module by advancing to the next page. If you want to jump to a particular module, follow one of the links below.

- **Module 2 - Rightsize the Configuration of Oversized or Undersized VMs with vRealize Operations (45 minutes)**
- **Module 3 - vSphere Optimization Recommendations with vRealize Operations (15 minutes)**
- **Module 4 - Assess vSphere Configuration with vRealize Operations (15 minutes)**
- **Module 5 - Access vSphere Compliance Against Standards with vRealize Operations (30 minutes)**

Or if you want to end your lab,

1. Click on the **END** button at the top of the page.
Module 2 - Rightsize the Configuration of Oversized or Undersized VMs with vRealize Operations (45 minutes)
Introduction

This Module contains the following lessons:

- Optimize Capacity - Reclaim Dashboard Overview
- Using Views to identify Undersized and Oversized VMs
Log in to the vRealize Operations HVM instance

This lab environment is running three different instances of vRealize Operations and one instance of vRealize Log Insight. We have the different vRealize Operations instances in order to be able to work through different use cases that have unique requirements. The lab instances are as follows:

- Live Instance: Connected to the small running vSphere environment in the lab. There isn't a large inventory of objects in this instance but it allows us to interact with vCenter.
- Historical Instance: Running a 30-minute time loop of data that was captured in the past. This instance has a much larger inventory of objects but since it is not currently connected to a vCenter, we can't perform any actions here.
- Blue Medora Management Packs: Also running in historical mode, this instance has a large number of management packs from Blue Medora that allow us to see information from adjacent infrastructure (storage and physical servers) as well as operating system and application information.

In this lesson we will be using the Historical Instance of vRealize Operations.

If you are already logged into the historical (not live) instance of vRealize Operations, click here to skip ahead.

Open the Chrome Browser from Windows Quick Launch Task Bar

If your browser isn't already open, launch Google Chrome

1. Click the Chrome icon on the Windows Quick Launch Task Bar
Open the vRealize Operations - Historical Instance Tab

1. Click the **vRealize Operations - Historical Instance** link to open the UI in a new browser tab

The browser home page has links to the different instances of vRealize Operations that are running in the lab.
Log in to vRealize Operations

1. If Local Users is not the default, click the drop down as shown and click **Local Users**

Enter user credentials. Username is **admin** and password is **VMware1!**

2. Click **LOG IN**
Optimize Performance Dashboard
Overview

In this lesson, we are going to examine the 'Optimize Performance - Overview' dashboard.

The optimize performance dashboard gives us insight to the virtual machines that are undersized and oversized. We have the ability to take actions from this dashboard and resize resources that need it most.

Home Screen

![Home Screen Image]

You should be at the Home screen.

1. Click on Home if necessary
Navigate to the Optimize Performance Overview

1. Expand **Optimize Performance**
2. Click **Overview**
Optimize Performance

You will see a description at the top of the dashboard followed by a list of Undersized Virtual Machines and Oversized Virtual Machines. We can sort the data by clicking on column headers. We also see a summary for each Undersized and Oversized categories.

With Undersized resources, it's obvious that right-sizing them will allow them to perform better. With Oversized resources, it may not be as obvious that right-sizing them may improve their performance as well as the performance of other resources in the environment. When a VM is over allocated with CPUs, it can create contention and increased wait times for the hypervisor.
Sorting Undersized Resources

1. Click on the column 'Configured Memory (GB)\(^1\)' two times to ensure the largest configured machines are listed first (wait for the first click to complete before clicking the second time).

Selecting a Virtual Machine

At the top of the sorted list, you will see 'VMware-vRealize-Network-Insight-3.7.0.1519211678-platform - Canned demo.' You may need to expand the Name column to see the full name of the VM.

We can see the VM is configured with 32GB and vRealize Operations is recommending the VM needs 3GB more.
Selecting a Virtual Machine

1. Click the VM 'VMware-vRealize-Network-Insight-3.7.0.15192116778-platform - Canned demo'

Taking actions

1. Click on Actions
2. Click on Set Memory for VM
Action Settings

You will see 'New (MB)' column reflects the additional 3GB added to the configured 32768MB taking the value to 35840MB. We also can see that the VM is powered on. The next check box allows us to power off the VM followed by another check box to allows us to take a snapshot.

The power off option is there in the event the VM does not allow for hot add.

The snapshot option allows us to take a snapshot before any configuration changes occur.

1. Click CANCEL.

Back to the list
Navigate using the BACK button on the top left of the vRealize Operations Manager interface.

1. You'll need to Click **twice** on **BACK**

**Oversized VM List**

You should be seeing Undersized and Oversized page.

**Select an Oversized VM**

1. Scroll down to the 'Oversized Virtual Machines' list
   - In the list, we can see 'vrli-master3' is configured with 16 vCPU and vRealize Operations indicates 8 reclaimable vCPUs. We also show that the VM is configured with 32GB of memory with a reclaimable amount of 14GB. With both CPU and memory in mind, let's look at the VM.

2. Click on **vrli-master3**
Take actions on the VM

1. Click on **Actions**
2. Click **Set CPU Count for VM**

**Action Settings**

- Name: vri-master3
  - New CPU: 8
  - Current CPU: 16
  - Power State: Powered On
  - Power Off Allowed: False
  - Snapshot: None
  - Host: w2-mgmtspn-16.mgmt.local
  - Parent vCenter: None

[Image of action settings interface]
Just as we seen with the memory example above, we can set the recommended CPU count for the VM. We also see the power state and have the ability to power off the resource and take a snapshot if necessary.

1. Click **CANCEL**

**Lesson Completed**

You have concluded this section of the lab.

Thank you.
Optimize Capacity - Reclaim Dashboard Overview

Open Google Chrome

![Chrome Icon]

Open Google Chrome

Start vRealize Operations

<table>
<thead>
<tr>
<th>HOL-1901 Lab Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>vRealize Operations Manager – Live Instance</td>
</tr>
<tr>
<td>vRealize Operations Manager – Historical Instance</td>
</tr>
<tr>
<td>vRealize Operations Manager – Blue Medora Management Packs</td>
</tr>
<tr>
<td>vRealize Log Insight</td>
</tr>
</tbody>
</table>

1. Click on **vRealize Operations Manager - Historical Instance**
Authenticate

Log In
1. Local Users
2. Admin
3. VMware1!
4. Click **LOG IN**

Go to Home

1. You should be on the 'Home' tab. If not, click on 'Home'
Optimize Capacity

Under Optimize Capacity

1. Click **Reclaim**

**Configuration Options**

Out of the box, the Reclaim dashboard is configured to show costs associated with reclamation (Not available in vRealize Operations Manager Standard).

It is possible to disable the cost if wanted. We can also configure the time frame for assessing a VM Powered Off, Idle, or with old snapshots. We also show Oversized VMs in this area.

1. Click **the gear** to the right of ‘Reclaim’
Default Settings

The default settings are 7 days for evaluation of a VM’s status. Each item is also checked by default. We will visit these settings later.

1. Click **CANCEL**

Datacenter Selection

Each box on the screen represents a datacenter.

1. Click on **lab-dc**.
Reclamation Values

We now see the potential savings along with the number of VMs with reclaimable resources. To the right of that data, we also see a breakdown of the total capacity to be reclaimed. Scrolling down, we see the categories for the following:

- Powered Off VMs
- Idle VMs
- Snapshots
- Oversized VMs

Change Settings
1. Click **the gear** at the top of the dashboard and set the days to 30 for each category.

1. Click **SAVE**

Instead of considering 7 days of data, we have told vRealize Operations to consider 30 days. A VM that may appear Powered Off over the last 7 days may very well be powered On over a 30 day stretch. The same logic can apply to Idle VMs and Snapshots. A 10 day old snapshot is considered new in a 30 day configuration and therefore not selected as a potential cleanup for vRealize Operations.

**Cluster Reclamation**

To view virtual machines in each cluster for the selected datacenter, we can expand the context.

1. Expand **lab-ops** by clicking on the chevron (>")
Clean up snapshots

Scroll down to see the list of VMs.

The list of VMs is based on the Powered Off status.

1. Click on **Snapshots**
2. Expand **lab-ops** once again.

We see just a few VMs with old snapshots.

View some data

1. Select **IIS-WebApp1**

Above the list of clusters and virtual machines, ‘Delete Snapshot(s)’ and ‘Exclude VM(s)’ are now actionable.
Take an action

1. Click DELETE SNAPSHOT(S).

Action Summary

A pop-up window shows us the Savings and Disk Space that will be reclaimed when we delete the snapshot.

1. Click CANCEL
Oversized VMs

1. Click on **Oversized VMs**
2. Scroll down and make sure **lab-ops** is expanded.

Select All

We now see all the Virtual Machines in the selected cluster. We see the allocated resources and the reclaimable resources.

1. Click the **box left of 'VM Name'** to select all of the VMs.
Resize VM(s)

1. Click **RESIZE VM(S)**

Resize Summary

- You have selected 12 VMs to be resized, which will allow you to reclaim:
  - CPU: 24 vCPUs
  - Memory: 7 GB

I understand that workloads may be interrupted because some VMs must be restarted during the resize.
1. The pop-up window gives us a list of the changes and a summation of the reclamation.
   - It is possible to overwrite the suggested changes.

2. Click the pencil icon on the right most column for any VM in the list.
   - It's now possible to edit the memory size for the selected VM.

3. The pencil icon in the center of the table will allow you to change the vCPU count for the selected VM.

**Are You Sure**

![Image of a pop-up window indicating reclamation adjustments]

1. Below the reclamation summary, there is a safety switch that requires us to check the box to ensure we know we want to change the VMs. We are not going to change anything at this time.
2. Click **CANCEL**.
Exclude VM(s)

In addition to making changes to our resources, there are times when we need to exclude VMs from the rules. We provide for these exceptions with the ‘Exclude VM(s)’ button.

1. Click **EXCLUDE VM(S)**

**Confirmation**

The pop-up window gives us a warning message about what we are going to do.
1. Click **EXCLUDE VM(S)**

![Image of dashboard showing 79 VMs with reclaimable resources]

1. We've now excluded a view VMs that were once considered Oversized. Take note of the VMs with reclaimable resources.
   - Scroll to the bottom of the dashboard

2. Click ‘**SHOW EXCLUDED VMS**’

**Select All**

![Image of VM selection]

1. Select the **box to the left of 'VM Name'** to select all of the VMs
2. Click **INCLUDE VM(S)**
Updated Resources

![Reclaim Resources Dashboard]

Notice the change to the number of VMs with reclaimable resources. With vRealize Operations 6.7, there is not an associated cost with Oversized VMs. In this version of vRealize Operations, costs are based on utilization and not allocation.

Lesson End

This concludes the Optimize Capacity Reclaim dashboard lesson.

With this lesson, we have taken you through the process to identify virtual machines with an opportunity to reclaim resources. We have also shown that it is possible to exclude virtual machines from this task.

Thank You
Using Views to Identify Undersized and Oversized VMs

Open Google Chrome

Start vRealize Operations Manager

1. Click on vRealize Operations Manager - Historical Instance
Authenticate

Log In
1. Local Users
2. Admin
3. VMware1!
4. Click **LOG IN**

Go to Environment

1. Click **Environment**
Navigate to vSphere Hosts and Clusters

1. Click **vSphere Hosts and Clusters**

Select a vCenter Server

1. Expand **vSphere World**
2. Select **msbu-vc-east**
3. Click ‘more...’
View Details

1. Click ‘Details’
2. Enter ‘size’ in ‘All Filters’ and press the enter key on your keyboard

Undersized Virtual Machines

1. In the list of views, single click on Undersized Virtual Machines
Remediation

In the ‘Undersized Virtual Machines’ list, every VM managed by msbu-vc-east undersized is displayed. The reason for being undersized is either CPU, Memory or both.

Select the first three virtual machines. This is done by single clicking on the first VM, then hold down the shift key on the keyboard and single click on the last VM.

A gear in the toolbar above the VM list is now visible.

1. Click the gear icon

Select an Action

1. When the list is populated, click ‘Set CPU count and Memory for VM.’
Each VM that was selected is now listed in the pop-up window. Each has its suggested vCPU count and recommended memory. These number can be modified.

Use the TAB key to navigate through each item if you need to change values.

You will also have columns for Power Off Allowed and Snapshot. Clicking the Power Off Allowed tells the script to power down the VM during the resizing process. The Snapshot check box will tell the script to take a snapshot of the selected VM before making any changes.

1. Click **CANCEL**
View Oversized VMs

1. In the view list, single click **Oversized Virtual Machines**.

**Remediation**

Select any VM in the list with a single click

1. Click the gear icon in the toolbar above the listed VMs.
Take an Action

1. Click ‘Set CPU Count and Memory for VM’

Action Parameters

We see the same pop-up windows we seen for the undersized list, with the same capabilities.

1. Click CANCEL.

Lesson End
Conclusion

This Module was an introduction to the following topics:

- Optimize Capacity - Reclaim Dashboard Overview
- Using Views to identify Undersized and Oversized VMs

You've finished module 2

Congratulations on completing module 2.

If you are looking for additional information on vRealize Operations, you can start here: https://www.vmware.com/products/vrealize-suite.html

You may proceed to the next module by advancing to the next page. If you want to jump to a particular module, follow one of the links below.

- Module 1 - Optimize Workloads Based on Business or Operational Intent with vRealize Operations (60 minutes)
- Module 3 - vSphere Optimization Recommendations with vRealize Operations (15 minutes)
- Module 4 - Assess vSphere Configuration with vRealize Operations (15 minutes)
- Module 5 - Access vSphere Compliance Against Standards with vRealize Operations (30 minutes)

Or if you want to end your lab,

1. Click on the END button at the top of the page.
Module 3 - vSphere Optimization Recommendations with vRealize Operations (15 minutes)
Introduction

This Module contains the following lessons:

- Optimization Recommendations
  - We take you through the 'Recommended Actions' dashboard. This dashboard will allow an administrator to better optimize an environment.
Log in to the vRealize Operations HVM instance

This lab environment is running three different instances of vRealize Operations and one instance of vRealize Log Insight. We have the different vRealize Operations instances in order to be able to work through different use cases that have unique requirements. The lab instances are as follows:

- Live Instance: Connected to the small running vSphere environment in the lab. There isn't a large inventory of objects in this instance but it allows us to interact with vCenter.
- Historical Instance: Running a 30-minute time loop of data that was captured in the past. This instance has a much larger inventory of objects but since it is not currently connected to a vCenter, we can't perform any actions here.
- Blue Medora Management Packs: Also running in historical mode, this instance has a large number of management packs from Blue Medora that allow us to see information from adjacent infrastructure (storage and physical servers) as well as operating system and application information.

In this lesson we will be using the Historical Instance of vRealize Operations.

If you are already logged into the historical (not live) instance of vRealize Operations, click [here](#) to skip ahead.

Open the Chrome Browser from Windows Quick Launch Task Bar

1. Click the Chrome icon on the Windows Quick Launch Task Bar
Open the vRealize Operations - Historical Instance Tab

The browser home page has links to the different instances of vRealize Operations that are running in the lab.

1. Click the vRealize Operations - Historical Instance link to open the UI in a new browser tab
Log in to vRealize Operations

1. If Local Users is not the default, click the drop down as shown and click **Local Users**

Enter user credentials. Username is **admin** and password is **VMware1!**

2. Click **LOG IN**
Optimization Recommendations

The recommended actions dashboard provides us with the ability to see resources, related alerts, number of objects. The alerts are separated by Object Type as well as the badge type (Health, Risk and Efficiency). We will go through the process of selecting object types, examine the alerts and show how to take action on the alert.

Navigate to Home

![Image of the Home page in the Operations Manager dashboard]

Return to the Home page

1. click **Home**

Navigate to Recommended Actions

![Image of the recommended actions section in the Operations Manager dashboard]

1. Expand **Optimize Performance**
2. Click **Recommended Actions**
Select a vCenter Server

The 'Recommended Actions' content gives us a perspective through the environment. It can provide information on 'Health', 'Risk', and 'Efficiency' alerts. We'll explain those as we move through the content. At the top-left of the Recommended Actions screen, you will see the drop-down list for Scope.

By default, the scope is empty and everything is included.

To limit our scope:

1. click the drop-down list
2. select msbu-vc-lab

Health Alerts
On the top-right area of the dashboard, we see three small icons. The first one on the left is selected. We see that with the darker squared background on the image. The icon represents alerts that have been classified as Health. With 'Health' selected, we will see recommendations that are related to health.

To better explain this, when an alert is created in vRealize Operations, the alert and its symptom(s) are categorized as Health, Risk or Efficiency. For a deeper understanding on Alerts, please visit the Hands On Lab for 1901-05 Module 3.

We can see that there is a recommendation for the datacenter 'lab-dc.' This recommendation is based on the alert 'Datacenter performance can potentially be optimized in one or more clusters.'

**VM Recommendations**

![Virtual Machine Recommendations](image)

At the top of the dashboard, navigate to the Virtual Machine recommendations:

1. Click on the Greater than sign ('>') near the top-right side to scroll right
2. Click on Virtual Machine

We can see there is an alert for 'vrli-45-ss' for 'one or more virtual machine guest file systems are running out of disk space.'

Immediately we know the affected resource (vrli-45-ss) and the alert for that resource. When a Virtual Machine is running out of resources like disk space, we probably take this more serious than we would something like a snapshot. For this reason, something in the Health category may have more impact that the other alert categories.
VM Risks

On the top-right of the dashboard,

1. switch to Risk
2. add a filter for vrops-upuat-data (As you type the name, a pop-up will appear. Click on the VM name to finish selecting the appropriate resource)
3. select the VM in the drop-down list that appears as you type.

Taking Action

We should see an alert for 'Virtual machine is running on snapshots for more than 2 days.' You will see that this alert has an action that has been associated to it. A Virtual Machine with snapshots may not be as critical as a Virtual Machine running out of resources like we seen in the previous alert. For that reason, this alert has been classified as a risk.

1. Click the action icon
Action Settings

You will see a pop-up screen that allows us to run the action to 'Delete Unused Snapshots for VM.'

The Days Old column can be adjusted to find snapshots greater than X days. If you click the Next button, the script will search for snapshots X days and then give you an option to remove them. For now, we are going to cancel the process.

1. Click cancel to return to the recommended actions dashboard.

View Alert

1. Click the link for the alert.
Alert Action

You now see the alert in its entirety. Like all alerts, we see the cause, the recommendations, symptoms and other alert information.

In this particular alert, we see the 'run action' button.

1. Click on **RUN ACTION**

Action Settings
We see the same action as we seen previously. We simply took a different approach to get here.

1. Click CANCEL.

Back

1. Click the vRealize Operations BACK button.

Alert Management

You should be seeing the Virtual Machine section of the recommended actions. The filter we used has been cleaned up.

1. Click 'Risk' category.
2. Click on a row. (Click in the area to the right of the links. Be sure not to click one of the hyperlinks).

Alert Options

By choosing the row, we now have the options to cancel the alert and suspending the alert. If you cancel the alert and it’s still active, the alert will return on the next cycle. If you suspend the alert, it will be suspended for the minutes specified. After the specified time entered, the alert will become active again. Click on each of the icons to see the process if you like.

Lesson End
Conclusion

This Module introduced the following topics:

• Optimization Recommendations

You've finished Module 3

Congratulations on completing module 3.

If you are looking for additional information on vRealize Operations, you can start here: https://www.vmware.com/products/vrealize-suite.html

You may proceed to the next module by advancing to the next page. If you want to jump to a particular module, follow one of the links below.

• Module 1 - Optimize Workloads Based on Business or Operational Intent with vRealize Operations (60 minutes)
• Module 2 - Rightsize the Configuration of Oversized or Undersized VMs with vRealize Operations (45 minutes)
• Module 4 - Assess vSphere Configuration with vRealize Operations (15 minutes)
• Module 5 - Access vSphere Compliance Against Standards with vRealize Operations (30 minutes)

Or if you want to end your lab,

1. Click on the END button at the top of the page.
Module 4 - Assess vSphere Configuration with vRealize Operations (15 Minutes)
Introduction

In this module we will leverage vRealize Operations Dashboards to Assess the vSphere Configuration. Leveraging the 'Configuration and Compliance' dashboards, we will look for tailored configuration metrics that will help us quickly identify and major opportunities to correct certain infrastructure misconfigurations.
Log in to the vRealize Operations HVM instance

This lab environment is running three different instances of vRealize Operations and one instance of vRealize Log Insight. We have the different vRealize Operations instances in order to be able to work through different use cases that have unique requirements. The lab instances are as follows:

- Live Instance: Connected to the small running vSphere environment in the lab. There isn't a large inventory of objects in this instance but it allows us to interact with vCenter.
- Historical Instance: Running a 30-minute time loop of data that was captured in the past. This instance has a much larger inventory of objects but since it is not currently connected to a vCenter, we can't perform any actions here.
- Blue Medora Management Packs: Also running in historical mode, this instance has a large number of management packs from Blue Medora that allow us to see information from adjacent infrastructure (storage and physical servers) as well as operating system and application information.

In this lesson we will be using the Historical Instance of vRealize Operations.

If you are already logged into the historical (not live) instance of vRealize Operations, click here to skip ahead.

Open the Chrome Browser from Windows Quick Launch Task Bar

If your browser isn't already open, launch Google Chrome

1. Click the Chrome icon on the Windows Quick Launch Task Bar
Open the vRealize Operations - Historical Instance Tab

The browser home page has links to the different instances of vRealize Operations that are running in the lab.

1. Click the **vRealize Operations - Historical Instance** link to open the UI in a new browser tab
Log in to vRealize Operations

1. If Local Users is not the default, click the drop down as shown and click Local Users

Enter user credentials. Username is **admin** and password is **VMware1**!

2. Click **LOG IN**
Overview of Configuration Dashboards

In this lesson we will be reviewing the available Configuration dashboards to get a better understanding of how vRealize Operations provides quick and insightful views into important configuration elements of the environment.

Exploring the available Dashboards

Let's view the available configuration dashboards

1. Select **Home**
2. From the 'Manage Configuration' area, select **Cluster**
Cluster Configuration

At the cluster configuration dashboard we are presented with the most important configuration elements of information first. We have the ability to double click on cluster items within any field of this dashboard to get more details.

From the screenshot above we can see:

1. There are 14 vSphere Clusters where DRS Enabled = true
2. There is 1 vSphere Cluster where HA is NOT enabled. This might be something an admin might want to verify is properly configured.
3. All of our vSphere Clusters have vMotion enabled. Good thing!
Explore Widget Controls

Now let's explore what options we have to adjust some of these widgets. Let's start with the 'Is vMotion Enabled...' widget.

1. Place the cursor over the widget header to expose widget options
2. Select the pencil icon to edit the widget settings
Available Widget Options

We can see that there are a number of options within a widget that can be adjusted to present the data as desired. It also worth noting that not all widgets are created the same. The available widget options depend on the type of Configuration represented in the widget.
Adjust Widget Configuration Grouping

Now let's toggle some of the widget options.

1. Under the 'Group by' area, select the down arrow next to 'Then by', Scroll down to view more object types within the vCenter Adapter
2. Select **Datacenter**
3. Select **Save**
Review adjusted Widget view

By selecting a few tiles in the newly adjusted widget view, we can see that the tile objects are now grouped by 'Datacenter' as opposed to previously being sorted by vCenter Cluster.

1. Select tiles  
2. Note the Datacenter value

At this point we are done exploring the widget controls for this area of cluster configurations. Feel free to experiment with toggling other settings within this widget.
Navigate to Virtual Switch Configuration

Let's navigate to the Distributed Switch Configuration dashboard.

1. Click on All Dashboards near the middle of the screen.
2. Under 'Configuration & Compliance', choose Distributed Switch Configuration.

Distributed Virtual Switch Configuration

[Diagram showing Distributed Switch Configuration dashboard with options and information]
By selecting a Distributed switch we are able to see context sensitive information for the remaining fields in the dashboard.

1. Select the dVS **vds10g-west**
2. Note that the information regarding related ESX hosts and port groups dynamically updates

This dashboard can be especially useful to quickly identify very important configuration items such as NIC speeds, Hosts connected to a dVS, and the VMs connected to the selected switch.

**Navigate to Widget Options for Distributed Switch Configuration**

Now lets explore what options we have to adjust some of the data presented in the widget.

1. Place the cursor over the widget header to expose widget options
2. Select the pencil icon to edit the widget settings
Widget Options

We can see that we have options to adjust refresh rates, tags to filter on, and the ability to show more columns of information.

This step concludes digging into the details of widgets. For more information on vRealize Operations widgets please see the link:

Navigate to Host Configuration

1. Click on All Dashboards near the middle of the screen
2. Under 'Configuration & Compliance', choose Host Configuration

Host Configuration
From the Host Configuration dashboard we have the ability to quickly view any deviations in our host hardware or low level hypervisor configurations.

By default, Operations Manager receives very granular hardware information from vCenter as shown above. As an administrator you have the ability to toggle which specific hardware attributes are displayed within the Host Configuration Dashboard. It is also possible to add even more detailed vendor specific hardware information through the use of Blue Medora Management Packs.

For more information on popular management packs:

https://bluemedora.com/resources/data-sheets/

**Navigate to VM Configuration**

1. Click on **All Dashboards** near the middle of the screen
2. Under ‘Configuration & Compliance’, choose **VM Configuration**

Let's navigate to the VM Configuration dashboard.

1. Click on **All Dashboards** near the middle of the screen
2. Under 'Configuration & Compliance', choose **VM Configuration**
VM Configuration

From the Host Configuration Dashboard we are quickly greeted with top level configuration information related to "heavy hitter" VMs. Understanding if or how many VMs are using large chunks of resources is very important to ensure proper performance and infrastructure utilization.

Navigate to Security
Lets navigate to the Security Compliance dashboard.

1. Click on **All Dashboards** near the middle of the screen
2. Under 'Configuration & Compliance', choose **vSphere Security Compliance**

**Security Compliance**

The Security Compliance dashboard contains lots of information including compliance levels, risk violations, violation trending, and granular compliance views. Compliance is measured against VMware Security Best Practices.

Please note that security baselines are purely evaluating the low level hardware and hypervisor configurations for compliance with hardening guides.

For more information on what settings are being evaluated to determine security compliance, please see the following link:

VMware Published Security Hardening Guides

By expanding the Compliance Details for **vSphere Compliance** and **VM Compliance**, we are able to see a heat map view of compliance levels across the environment.

For more information about configuring security compliance baselines, please see the following links:

**Initial Configuration of Compliance rules**


**Configuring PCI and HIPAA baselines**

Conclusion

In this module we were able to leverage vRealize Operations Manager Configuration Dashboards to review various configuration elements of the environment. We believe these dashboards have been designed in a logical way that provides an intuitive view into analyzing configuration areas.

You've finished module 4

Congratulations on completing module 4.

If you are looking for additional information on vRealize Operations, you can start here: https://www.vmware.com/products/vrealize-suite.html

You may proceed to the next module by advancing to the next page. If you want to jump to a particular module, follow one of the links below.

- **Module 1 - Optimize Workloads Based on Business or Operational Intent with vRealize Operations (60 minutes)**
- **Module 2 - Rightsize the Configuration of Oversized or Undersized VMs with vRealize Operations (45 minutes)**
- **Module 3 - vSphere Optimization Recommendations with vRealize Operations (15 minutes)**
- **Module 5 - Access vSphere Compliance Against Standards with vRealize Operations (30 minutes)**

Or if you want to end your lab,

1. Click on the END button at the top of the page.
Module 5 - Assess vSphere Compliance Against Standards with vRealize Operations (30 Minutes)
Introduction to vSphere Compliance

As vSphere administrators, we are responsible for the configuration of the virtual environment. This responsibility includes the enforcement of all industry configuration standards used by your organization such as the vSphere Security Configuration Guide, regulatory standards such as PCI and HIPAA, and your organization's defined standards.

vRealize Operations uses Alert Definitions to continually monitor the configuration of the virtual environment, alert, and report on the compliance level for your entire infrastructure. Additionally, individual subsets of the infrastructure that you define through custom groups can be monitored.

The vSphere Security Configuration Guide, PCI, and HIPAA Alert Definitions are provided via the installation of Solutions or Management Packs and can be turned on or off, as a group or individually, for all or part of the managed environment. Custom standards can be built by the user as new symptoms and Alert Definitions.

vRealize Operations Compliance is used specifically to monitor the vCenter Server instances, hosts, virtual machines, distributed port groups, and distributed switches in your environment to ensure that the settings on your objects meet the defined standards.

vRealize Operations provides Alert Definitions for vSphere Security Configuration Guide versions 6.5, 6.0 and 5.5; these are pre-installed but not turned on by default. Additional standards (PCI and HIPAA) are downloaded via the VMware Marketplace and installed as a new solution by the administrator.


In this module, you will learn:

- How to ensure compliance of a vSphere environment
- How to customize a policy to enable vSphere Security Configuration Guide alerts
- Various methods to ensure that vSphere objects comply with the alert-based compliance rules
- Remediation of compliance issues and reviewing the results
- How install and configure industry standards (PCI and HIPAA Compliance) for monitoring a vSphere environment

It is important to understand that vSphere compliance monitoring is limited to the vSphere-based object types described above. **It does not monitor or provide alerts** on the configuration of other objects in your environment such as guest operating systems, databases, or applications.
Log Into the vRealize Operations Live Instance

This lab environment is running three different instances of vRealize Operations and one instance of vRealize Log Insight. We have the different vRealize Operations instances to enable working through different use cases with unique requirements. The lab instances are as follows:

- **Live Instance**: Connected to the small running vSphere environment in the lab. There isn't a large inventory of objects in this instance, but it allows us to interact with vCenter.
- **Historical Instance**: Running a 30-minute time loop of data that was captured in the past. This instance has a much larger inventory of objects, but since it is not currently connected to a vCenter, we can't perform any actions here.
- **Blue Medora Management Packs**: Also running in historical mode, this instance has a large number of management packs from Blue Medora that allow us to see information from adjacent infrastructures (storage and physical servers) as well as operating system and application information.

In this lesson, we will be using the Live Instance of vRealize Operations.

If you are already logged into the live (not historical) instance of vRealize Operations, click to skip ahead.

Open the Chrome Browser From Windows Quick Launch Task Bar

![Chrome icon on Windows Task Bar]

If your browser isn't already open, launch Google Chrome.

1. Click the **Chrome** icon on the Windows Quick Launch Task Bar.
Open the vRealize Operations - Live Instance Tab

The browser home page has links to the different instances of vRealize Operations running in the lab.

1. Click the vRealize Operations - Live Instance link to open the UI in a new browser tab.
Log Into vRealize Operations

vRealize Operations is integrated with VMware Identity Manager, which we will utilize for user authentication in this lab.

VMware Identity Manager should be pre-selected as the identity source. However, if it is not, you must select it.

Click the drop-down arrow.

1. Select **VMware Identity Manager**
2. Click **REDIRECT** to take you to the user login page
VMware Identity Manager Login

The user and password information should already be populated; if not, type them in.

USER: hol

PASSWORD: VMware1!

1. Click Sign in
Ensuring Compliance of vSphere Objects

The compliance alerts in vRealize Operations enable administrators to monitor vSphere objects for violations of specific standards. When a compliance alert is triggered, it is necessary to investigate and resolve the violation to ensure continued compliance with industry standards.

To enforce and report the compliance of vSphere objects, we must enable and configure the appropriate risk profile based on the importance of the managed object.

In this lesson, you will learn:

- How to enable Compliance Alert Definitions in the default policy
- How to use Compliance Dashboards to identify and resolve configuration issues in your environment
- How to run a Compliance Report on a vCenter Server instance
- How to view the symptom set in the Compliance Alert Definition

Navigate to vSphere Compliance

To begin working with Compliance Standards, access the vSphere Compliance page from the Quick Start page.

1. Click on vSphere Compliance.
Enable vSphere Compliance

Compliance Alerts can be enabled by either using the Monitoring Goals Wizard when configuring a new instance of the vSphere Solution, or by editing the active policy. In this lab, the solution is already installed, so we will be using the Policy Editor to enable a specific set of Compliance Alerts.

From the vSphere Compliance screen, using the Enable link will open the Policies page in vRealize Operations.

1. Click on **ENABLE** in the vSphere Security Configuration Guide tile.

Edit the Policy
The compliance functionality enables the Compliance Alerts that are installed with the Compliance Management Pack. These alerts are enabled in the policy or policies where you want to assess compliance.

1. Click the Policy Library tab.
2. Select HOL Default Policy.
3. Click the Pencil to edit the policy.

Enable the vSphere Security Configuration Guide Alerts

We need to choose the alerts that we want to enable. Note that in addition to the vSphere Security Compliance alerts that exist for hosts (vCenter, vSphere Distributed Virtual Switches, and vSphere Distributed Port Groups), there are three different alerts for virtual machines corresponding to the three risk profiles defined in the Compliance Guide. You will only want to enable the alert that corresponds to the risk profile you have chosen to implement in your environment. In this case, we will use risk profile 3, but not risk profiles 1 or 2.

Enable the five alerts of interest.

1. Click Alert / Symptom Definitions.
2. In the filter, type Security to show only those alerts which include that text.
3. Hover over and then drag the bar to enlarge the Name column so you can see more of the alert names.
4. Note that the state of all alerts is disabled through inheritance. This means that the parent (base) policy has these specific alerts disabled by default.
Enlarge the Alert Definitions Window

In order to see all of the alerts:

1. Click on the double up-arrow at the top of the Symptom Definitions window to shrink it.
2. Click, hold, and drag the bottom of the Alert Definitions window down to enlarge it.

Select and Enable the Alerts

The final step is to select those alerts you want to enable (including risk profile 3), and then set the state of those alerts to Enabled as follows:
1. Click the first alert, and then while holding down the Ctrl key on your keyboard, click all other alerts except risk profiles 1 and 2. This will select the five alerts you want to enable. DO NOT SELECT RISK PROFILES 1 OR 2 (they have symptom counts of 52 and 16)
2. With those alerts selected, click Actions.
3. Click State.
4. Click Enable.
5. Note that the state of these five alerts changes to Enabled (indicated by the green check mark) and that there is now a local override in this policy.

**Save the Policy**

1. Click **SAVE**.
Review the Compliance Status

The monitoring of vSphere Security Compliance is now enabled in your lab environment.

Note: As we have seen, the compliance assessments in vRealize Operations are driven by symptoms and alerts. One of the results of this is that compliance scores won't be immediately available once the alerts are enabled in the policy. You will have to wait for at least one collection/analytics cycle to complete. They default cycle frequency is 5 minutes. However, we have reduced that frequency in this lab environment. You still might have to wait a couple of minutes before the compliance score updates on this dashboard.

1. Click **Home**.
2. Click **vSphere Compliance**.

Initially, the compliance score will be 100, indicating that all rules are in compliance on all monitored objects. Within a few minutes, the conditions will be evaluated and your true compliance score will display, along with the quantity of each object type that is in or out of compliance. Once this occurs, you should see that 19 objects are compliant, but one host is out of compliance. You can view the alerts from this page, but we are going to explore some additional ways to view and assess compliance in the system before we dig in to resolve the issues.

3. Click the refresh button until the compliance dashboard shows one host out of compliance.
4. Note Host status
Viewing the Compliance Dashboard

Compliance Dashboards can also be used to access the current state.

1. Navigate to Dashboards tab.
2. Select the Getting Started dashboard.
3. Click on the Configuration and Compliance category.
4. Scroll down and click on VSPHERE HARDENING COMPLIANCE to open that dashboard.
Tracking your compliance trends over time can help you identify technical or process-related issues with how you deploy and/or manage workloads or infrastructure in your environment. Note that you are provided an overall percentage that represents how much of your environment is compliant, as well as the number of high-, medium-, and low-risk items, allowing you to prioritize remediation efforts. This Summary dashboard also provides a consolidated list of all vSphere Security Configuration Alerts for the relevant objects for which the policy has been applied.

To determine exactly what property on that host is in violation of the Security Guide:

1. Click the arrow to expand the list of alerts from Today.
2. To see the actual alert with the violating, click the link to the alert.
Here, we see that:

1. The alert is active on the esx-02a.corp.local host.
2. The violation is that the shell interactive timeout is not configured on this host.

vRealize Operations does not directly resolve these configuration issues. We will need to log into the vSphere client and configure a shell timeout value in order to address the issue.
Log Into the vSphere Client

To log into the vSphere Client:

1. Open a new browser tab.
2. Click the HTML5 Client shortcut.
3. Click Use Windows session authentication.
4. Click Login.

Select the Host
To select the host where the violation is occurring, either:

1. Select the **esx-02a.corp.local** host in the inventory

Or

1. In the search bar, type **esx**
2. From the list of matching names, select the **esx-02a.corp.local** host

**Open Advanced System Settings for the Host**

1. Click on the **Configure** tab.
2. Scroll down the list.
3. Select **Advanced System Settings**.
4. Click **EDIT**.
Update Timeout

To set the shell timeouts that are in violation of the security standard:

1. Scroll down the list of advanced system settings.
2. Change the value for `UserVarsESXiShellInteractiveTimeOut` from 0 to 60.
3. Change the value for `UserVarsESXiShellTimeOut` from 0 to 60.
4. Click **OK** to save the new values.
Verify the Results

To see if this fixes the violation in vRealize Operations, let's return to the Compliance screen.

1. Return to the vRealize Operations tab in your browser.
2. Click Home.
3. Click vSphere Compliance.
vSphere Compliance

Note that it may take a few minutes for the compliance information to come up. vRealize Operations assesses compliance conditions such as other alerts every five minutes by default.

1. All four hosts are now in compliance.
2. All vSphere objects are in compliance, and we have a compliance score of 100.

Good job! You discovered a compliance issue, resolved it in the vSphere client, and verified that the object is no longer out of compliance.
Compliance information can also be viewed and assessed using the Compliance tab on any vSphere object.

1. Click the magnifying glass to open the search bar (not shown here since the bar has been opened).
2. Type `esx` and select the `esx-02a.corp.local` host from the list to open the host's object pages.
1. Click on the **Compliance** tab for the host object.
2. Click on **All Rules**.
3. Note that the host has a compliance score of 100 because all 29 rules are in compliance (thanks to configuration changes that we just completed).
4. Here, you can also see a list of all 29 rules being evaluated.

If any rules were out of compliance, they would have been displayed on the Violated Rules tab.

Note that you can modify the list of rules or symptoms by editing the Compliance Alert definition in the Alerts section of the tool. You can also create additional rules in that area and assess them as part of the compliance checks.
Running a Compliance Report on a vCenter Server Instance

Compliance reports can be generated for all or individual vSphere objects in your environment. These reports can be scheduled, saved, and/or sent to the individuals responsible for compliance within your organization.

1. Click on the **Dashboards** tab.
2. Click on the **Reports** in the left menu.

Run Report

1. Click on the **Report Templates** tab if it is not selected yet.
2. In the filter box, type **compliance** and hit **ENTER**.
4. Click on the **Run Template** icon.
5. On the window that pops up, browse through the inventory and select the object type as **vSphere Hosts and Cluster**.
6. Select **vSphere World** and click **OK**.

**Run Report**

![Image of Report Interface]

Wait for a few seconds for the report to run, and then perform the following steps.

1. Click on **Generated Reports**.
2. For the Compliance Report - vSphere Security Configuration Guide - Noncompliance, click the **PDF** icon under Download.
3. Click **Save**.
4. Click on downloaded report to review.

The non-compliance report appears for the host; it includes the date and time of the report and identifies the user who ran it. The report displays the non-compliant rules that ran on the object and its descendants. In the report, you can see the status of the alert, the object name, and the type on which the alert triggered.
Infrastructure Compliance With PCI and HIPAA Standards

The PCI (Payment Card Industry) Security Standards address the growing threat to consumer payment information. Companies and organizations that accept, process, or receive payments should adopt it as soon as possible to prevent, detect, and respond to cyber attacks that can lead to breaches. The vRealize Operations Compliance Pack for PCI provides alerts, policies, and reports to validate the vSphere resources against PCI DSS 3.2 standards.

HIPAA (Health Insurance Portability and Accountability Act of 1996) provides data privacy and security provisions for safeguarding patients' medical information. The vRealize Operations Compliance Pack for HIPAA provides alerts, policies, and reports to validate the vSphere resources against HIPAA standards.

The configurations of the following resources are validated using this content:

- vCenter servers
- ESXi hosts
- Virtual machines
- Distributed port groups
- Distributed virtual switches

In this lesson, you will learn:

- How to configure the vRealize Compliance Pack for PCI DSS
- How to run and view compliance reports and dashboards for vSphere objects
Installing the PCI Solution

1. From the Quick Start page, click **vSphere Compliance**.

View the current status of applied standards.

Note that the vRealize Operations Compliance Pack for PCI DSS has already been downloaded to the Main Console server that you are logged into now. For this lab, you will be installing and enabling the PCI Compliance solution. By default, Compliance Alerts are not enabled in any polices, so you will need to enable the alerts for the vRealize Operations Manager policy(ies).

As with the vSphere Security Configuration Guide, the alerts will drive the PCI compliance reports, views, and dashboards within vRealize operations. Organizations subject to PCI or HIPAA regulations might have specific environments within their enterprises where they are handling the credit card information or patient data. In this case, they would want to add only the infrastructure that will be subject to the regulations into groups within vRealize Operations Manager, and then enable the Compliance Alerts only for those groups.

**Real World Prerequisites (this has been done for you)**
Remember, in your real world (your environment), you would first need to download the appropriate PAK file from the VMware Marketplace.

Installing the PCI Standards Solution

View the current status of applied standards (continued).

1. Click **Install** in the PCI status pane.
Install the PCI PAK File

Installing PCI PAK file

To install the alert definitions for PCI compliance, install the PAK file from the Administration tab.

1. Click the + to add a new solution.
Select the PAK File

Select the downloaded PAK file to install.

1. Click **Browse**.
2. Navigate to **Lab Files** from the desktop.
3. Select the **PCI version 1.0.1...** PAK file.
4. Click **Open**.
5. Click **UPLOAD** (not shown).
Install PAK File

Once the PAK file signature is verified and you see the green check mark, you can proceed with the install.

1. Note Status of file.
2. Click NEXT.
Accept the User License Agreement.

1. Click "I accept the terms of this agreement."
2. Click **NEXT**.
Finish Installation

1. Note Status and click **FINISH**.
Verify Installation

Review PAK file Installation.

1. Note that the PCI PAK file is now installed.

Enabling the New Alerts

Next, you will need to enable the PCI alerts that were installed as part of the solution installation in the previous steps.

1. Click Home.
2. Click **vSphere Compliance**.
3. Click **ENABLE** to be taken to the policy editor in order to modify the lab policy.

**Edit the Hands On Lab Policy**

To enable (or disable) alerts in vRealize Operations, the effective policy must be edited. You should be in the Policies section of the Administration tab.

1. Click on the **Policy Library** tab.
2. Click on the **HOL Default policy** from the list to select it.
3. Click on the **pencil icon** to edit the policy.
A policy in vRealize Operations Manager controls many aspects of how objects are analyzed. One of the policy categories is for enabling/disabling alerts and symptoms and overriding threshold values for numerical symptoms.

1. Click **6. Alert / Symptom Definitions** to select that policy section.

Because of the relatively low desktop resolution in the lab, it will be easier to see the important columns in the Alert table if we remove some of the unnecessary columns.

2. Toggle the switch to enable column visibility selection.
3. Click the boxes to de-select the **Actionable Definitions, Automate, and Adapter Type** columns.
4. Click **OK** to save the setting.
Search for PCI Alerts

Re-size the Alert Definitions section and the Name column width for better visibility, and then filter the list to show alert definitions.

1. Hover over the column separator until the cursor changes, then click and drag to the right so you can see the full names of the Alert Definitions.
2. Hover over the bottom edge of the Alert Definitions box until the cursor changes, then click and drag the edge down to show more rows in the table.
3. Type "pci" in the filter box and press the Enter key.

You will see a list of all alerts that contain "pci" in their names. All of the Alert Definitions were added by the PCI DSS Compliance Pack when it was installed during the lab configuration.
Select the PCI Alerts

1. Notice that all of the PCI DSS alerts are disabled, a state that is inherited from the parent policy.

To enable these alerts, you will need to first select all of them.

2. Click the first Alert Definition in the list.
3. While holding down the **Shift** key, click the last Alert Definition in the list.

Notice that the selected Alert Definition rows have a gray background, indicating that they are selected.

Enable the PCI DSS Alerts
With the alerts selected, they can be bulk-updated. To override the inherited state of these alerts:

1. Click Actions.
2. Click State.
3. Click Enable.
4. Notice that the State for each definition changes to enabled (green check mark) and shows that the state is overridden locally in this policy.

Viewing PCI Compliance From the vSphere Compliance Screen

Now that the alerts are enabled, we can return to the vSphere Compliance Screen to see an overall status.

Review PCI Status.

1. Click Home.
2. Click vSphere Compliance.
3. Note the the number of PCI security standards that are complaint and non-complaint to modify the lab policy.

Note: It may take a couple of minutes for the values to populate.

Non-Compliance Results From the Object Perspective

While you can view Alerts and Reports globally for all objects in your environment, each individual object allows you to view its own specific compliance details. In this next section we will look at non-compliance alerts from an individual host's perspective.
Navigate to the Alerts Tab

The Alerts tab is another way to filter and view alerts in vRealize Operations Manager.

1. Enter `pci` in the filter field and press the Enter key.
2. Expand the **ESXi Host is violating PCI DSS 3.2 Hardening Guide for vSphere** alert header.
3. Click on the alert triggered on esx-02a.corp.local.

View the Alert

Note the triggered symptoms for this alert. These are the configurations that are out of compliance for the PCI DSS standards.
1. Click any of the links for esx-02a.corp.local to navigate to that object's page

View Compliance Alerts on the Object Compliance Tab

![Image of Compliance tab with alerts and information]

Review PCI Violated Rules.

1. From the Object, select the Compliance tab.
2. Click on the PCI Security Standards Status Box.
3. Click on Active Directory Symptom.
4. View the information provided.

Running the PCI Non-Compliance Reports for vSphere Objects

Now that the alerts are enabled, we can also run the non-compliant reports to see which conditions are out of compliance.
Navigate to Dashboards

The non-compliance reports can be run at any level in the vSphere inventory hierarchy. We will use the top level so that the report picks up all vSphere objects in the environment. If you only want to run the reports against a specific cluster, you could select the cluster and then proceed with the next steps.

1. Click **Dashboards**.
2. Click **Reports**.
3. In the filter, type **pci** and press the **Enter** key.
4. Select the **PCI 3.2** report and then click the icon to run the report.
5. Select **vSphere Hosts and Clusters** in the drop down list.
6. Select **vSphere World**.
7. Click **OK**.
Wait For the Report Generation to Complete

It will take several seconds for the report to be generated.

1. Wait until you see a value in the Last run column
2. Click the Generated reports link to see a list of the instances the report has been run in the past (including the one you just ran).

Launch the PDF Report

Reports in vRealize Operations Manager can be configured to be generated in PDF and/or CSV format. The default is for both formats to be created.

To view a PDF version of the non-compliance report:

1. Click the PDF icon and open PDF.

View the Report

View the resulting PCI DSS non-compliance report for the lab environment. You will see some object types that don't have any entries (meaning that their configuration is compliant with the standards) and other objects that do have entries that detail the configuration(s) that are out of compliance.
Conclusion

Compliance is a critical concern for IT organizations. No one wants to see their organization’s name in the headlines connected to outages, security breaches, or stolen customer data. This lab was designed to help you understand how vRealize Operations can be part of an overall compliance monitoring strategy to mitigate that risk and provide a stable platform for your critical applications.

In this module, we learned how to enable, assess, and resolve compliance issues with our vSphere configuration.

You've Finished Module 5

Congratulations on completing Module 5.

If you are looking for additional information on vRealize Operations, visit https://www.vmware.com/products/vrealize-suite.html.

You may proceed to the next module by advancing to the next page. If you want to jump to a particular module, follow one of the links below.

- **Module 1 - Optimize Workloads Based on Business or Operational Intent with vRealize Operations (60 minutes)**
- **Module 2 - Rightsize the Configuration of Oversized or Undersized VMs with vRealize Operations (45 minutes)**
- **Module 3 - vSphere Optimization Recommendations with vRealize Operations (15 minutes)**
- **Module 4 - Assess vSphere Configuration with vRealize Operations (15 minutes)**

Or, if you want to end your lab:

1. Click the **END** button at the top of the page.
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-1901-02-CMP

Version: 20181104-102920