# Table of Contents

Lab Overview - HOL-1901-04-CMP - Troubleshooting, Remediation and Compliance with vRealize Operations ................................................................. 2  
Lab Guidance ........................................................................................................... 3  
Module 1 - Troubleshoot Infrastructure Issues Using Guided Workflows in vRealize Operations (30 minutes) ............................................................................. 9  
  Introduction ............................................................................................................ 10  
  Log in to the vRealize Operations HVM instance .................................................. 11  
  Overview of Guided Workflows ............................................................................ 14  
  Identify and Troubleshoot an infrastructure issue using a guided workflow .......... 18  
  Log in to the vRealize Operations Live Instance ................................................... 26  
  Identify Performance Issues with Dashboards ..................................................... 30  
  Remediately a Performance Issue ....................................................................... 36  
  Conclusion .............................................................................................................. 42  
Module 2 - Troubleshoot Issues Using Metrics and Logs Together with vRealize Operations and vRealize Log Insight (45 minutes) ................................................. 43  
  Introduction ............................................................................................................ 44  
  Log in to the vRealize Operations Live Instance ................................................... 45  
  Metrics and IIS example ....................................................................................... 48  
  Conclusion .............................................................................................................. 79  
Module 3 - Application and OS Monitoring Using the Endpoint Operations Feature of vRealize Operations (45 minutes) .............................................................. 80  
  Introduction ............................................................................................................ 81  
  Exploring Endpoint Operations ............................................................................ 83  
  Building an Application Dashboard ...................................................................... 94  
  Service Discovery Management Pack .................................................................. 101  
  Conclusion .............................................................................................................. 103  
Module 4 - Extending Monitoring Through The Stack - From Physical to Applications with Blue Medora Management Packs (45 minutes) ....................................................... 104  
  Introduction ............................................................................................................ 105  
  Log in to the vRealize Operations Blue Medora instance .................................... 106  
  Microsoft SQL Server Health .............................................................................. 109  
  Overall Application Health .................................................................................. 112  
  Cohesity Mission Critical Backup ........................................................................ 114  
  Conclusion .............................................................................................................. 117
Lab Overview - HOL-1901-04-CMP - Troubleshooting, Remediation and Compliance with vRealize Operations
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 during your time. 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.

The lab introduces vRealize Operations topics such as monitoring, troubleshooting, and creating dashboards. We will also introduce End Point Operations for the operating system and applications.

Lab Module List:

• **Module 1 - Troubleshoot Infrastructure Issues using Guided Workflows in vRealize Operations** (30 minutes) In this module we will troubleshoot common vSphere infrastructure performance issues leveraging guided workflows. We will explore the format and steps of guided workflows including the 'Troubleshoot vSAN' workflow to determine if any VM configurations may be impacting vSAN performance.

• **Module 2 - Troubleshoot Issues Using Metrics and Logs Together with vRealize Operations and vRealize Log Insight** (45 minutes) In this module you will troubleshoot an issue affecting the performance of a web server. The IIS server is experiencing high HTTP GET requests. Using vRealize Operations alerts and vRealize Log Insight you will be able to review the logs to determine what is occurring. Once a root cause is determined the information can be presented to the other teams for their review and fix the IIS server.

• **Module 3 - Application and OS Monitoring Using the Endpoint Operations Feature of vRealize Operations** (45 minutes) In this module, we will explore the Endpoint Operations (EPOps) adapter in vRealize Operations.

• **Module 4 - Extending Monitoring Through The Stack - From Physical to Applications with Blue Medora Management Packs** (45 minutes) Looks at the different dashboards and metrics offered with 3rd party management pack.

Lab Captains:

- Module 1 - Jase Machado, Cloud Management Specialist, Sacramento
- Module 2 - Tony Welsh, Cloud Management Specialist, San Diego
- Modules 3-4 - Josh Green, Site Reliability Engineer, Palo Alto

This lab manual can be downloaded from the Hands-on Labs Document site found here:
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 your lab has not changed to "Ready", please ask for assistance.
Module 1 - Troubleshoot Infrastructure Issues Using Guided Workflows in vRealize Operations (30 minutes)
Introduction

In this module we will troubleshoot common vSphere infrastructure performance issues leveraging guided workflows. We will explore the format and steps of guided workflows including the 'Troubleshoot vSAN' workflow to determine if any VM configurations may be impacting vSAN performance.

This Module contains the following lessons:

• Lesson 1: Overview of available vROps guided workflows
• Lesson 2: Identify and Troubleshoot an infrastructure issue using a guided workflow
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 Guided Workflows

In this lesson we will explore the many available guided workflows to help you quickly identify infrastructure issue remediation opportunities. We are going to be using the historical view mode instance of vRealize Operations Manager as it has recorded data from a larger environment where we will be better able to showcase the capabilities. This means that there are limited changes that can be made, so don't worry if you navigate off the path a little and encounter an error. You are welcome to come back and run through the lessons again using the live instance if you want to try making changes.

Finding the Dashboards and Guided Workflows

To get started we must first navigate to the guided workflows section of the dashboards.

1. Click on "Dashboards"
2. Click on "Performance Troubleshooting"
3. Scroll down to view all available Guided Performance Troubleshooting options
Investigate how a guided workflow works

1. Select the 'Troubleshoot a cluster' workflow.

Step-by-Step Guided Analysis

Let's navigate through the workflow steps..
1. Let's select the cluster "east-mgmt'.
2. Notice subsequent troubleshooting steps dynamically update the scope of the information they provide to reflect the highlighted infrastructure component.

**Navigate to a different Dashboard**

In this step we will navigate to the 'Troubleshoot a Datastore' dashboard.

1. In the upper center of the screen, select the arrow for 'All Dashboards'.
2. Navigate to 'Performance Troubleshooting', and then select 'Troubleshoot a Datastore'.
Not all workflows are the same

The arrangement and troubleshooting steps for a datastore are much different than troubleshooting a cluster.

1. We can see that the 'Troubleshoot a Datastore' workflow provides us a very nice graphical heat map of datastore performance. This makes it much easier to visualize an impacted datastore.
2. Alternatively we can manually select a datastore from the list or add a filter.
3. The context of subsequent troubleshooting steps adjusts dynamically to show relevant information.
4. Finally, let's return to the 'Getting Started' page.
Identify and Troubleshoot an infrastructure issue using a guided workflow

In this lesson we will explore using a guided workflow to investigate for any potential infrastructure issues. Guided workflows are able to correlate many related data points from the virtual infrastructure to make root cause identification much faster.

Select a Guided workflow to troubleshoot a potential VM storage issue

1. Select ‘Performance Troubleshooting’.
2. Select ‘Troubleshoot vSAN’.

In this lesson we will explore troubleshooting vSAN performance to determine if any VMs may be impacted by unknown configuration issues.
Search for vSAN cluster related alerts

By default the troubleshooting steps will display data related to the very first object selected in step 1. For the vSAN Cluster 'east-comp', we can see an alert for 'Virtual machine disk I/O write latency is high'.

1. Click the link.
Select the alert instance to inspect

We now can see the 2 instances of this alert. Let's dig into the alert for 'weblogic-01'.

1. On the row for the server 'weblogic-01'. Click 'View Details'

We are now warned that any unsaved data will be lost as we are navigating away from the dashboards into the alert details. This is ok, please proceed.
Reviewing Alert Details

From the Alerts view, we can see that we are provided with additional information on Actions, Recommendations, and links to view additional metrics. We also have the ability to quickly see what symptoms are contributing to the alert and what particular symptom metric is contributing to the alert.
Available Actions

If we expand the available Actions, we can see what options are available.

1. Click the down arrow by 'Actions'

For more information on vRealize Operations Manager Actions please see this link: https://docs.vmware.com/en/vRealize-Operations-Manager/6.7/com.vmware.vcom.core.doc/GUID-BCD1B7D8-6988-4F3A-A70E-BE46A660383B.html
Now that we have identified that the VM 'weblogic-01' is having some issues, we can look at the detailed Alerts, Symptoms, and various metrics that may be contributing or resulting from our issue.

1. First let's look into the Symptoms. Click the 'Symptoms' button.
Review Symptoms

By default the Symptoms are listed in order of criticality. We also have the ability to sort on 'Created On' date as well as the symptom type. From our initial view we can see there is a critical alert regarding 'Virtual machine memory demand exceeds configured memory', this appears to be a very obvious issue we can remediate.

1. Click on the symptom for 'Virtual machine memory demand exceeds configured memory..'.
We are now able to confirm that the VM is experiencing demand for memory beyond what it is configured for. The memory configuration appears to be impacting disk latency performance for this VM using vSAN. In a real world scenario this would be very helpful in finding root cause of performance issues when various tools and technologies are integrated in a complex way.

For additional information on troubleshooting vSAN with vRealize Operations Manager, please see the 'Management Pack for vSAN' on the VMware Solutions Exchange website at: https://marketplace.vmware.com/vsx/solutions/management-pack-for-vsan

It is beyond the scope of this module to perform any further troubleshooting of this particular workload. We believe this lesson demonstrated the dynamic and powerful ability of vROps to continually collect and aggregate information and provided guided performance troubleshooting workflows.
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
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
Identify Performance Issues with Dashboards

In this lesson we will leverage guided workflows to identify unknown configuration issues that may be leading to performance issues.

Explore Guided Workflows

1. Select 'Dashboards'
2. Select each of the boxes that represent the functional dashboard types.
3. Note the available dashboards to provide info on Overviews, Utilization, Troubleshooting, Optimize, and Assess

Let's view the available dashboards and guided workflows.
Dive in Performance Troubleshooting workflows

Under the Performance Troubleshooting dashboards, we have the ‘Guided Workflows’. These are special interactive and dynamic workflows that are able to help correlate related infrastructure alerts, symptoms, and configurations. We can see that there are guided workflows to troubleshoot the common vSphere infrastructure items.

1. Select ‘Performance and Troubleshooting’
2. Notice the available guided workflows
Navigate to Troubleshooting VM performance

Let's troubleshoot VM Performance issues.

1. Select the button for 'TROUBLESHOOT A VM'
We are now starting the 'Troubleshoot a VM' guided workflow. The very first step is to identify if any VMs have Active Alerts, we can also utilize filters to look for VMs meeting other criteria. From this view we can see that the VM 'base-w10' has an active alert. When this VM is highlighted in the first step, we can see that the other steps provide other relevant information related to that VM.

1. Select the VM 'base-w10'
2. Note the additional information about the highlighted VM
Viewing Active Alerts

By looking at step 3, we can see that there is an alert that this VM is running on an old snapshot. Specifically, this alert indicates that the snapshot is over 2 days old. Click on the alert to get more details.

1. Click the alert ‘Virtual machine is running on snapshots for more than 2 days’
Alert Details and Symptoms

The detailed view of the alert shows the symptoms of the alert. We can now see that the VM has a snapshot that is approximately 1.7GB and the snapshot is older than 2 days.
Remediate a Performance Issue

In this lesson we will explore using automated remediation actions to allow administrators to quickly resolve issues without having to log into other management consoles.
Exploring Recommendations and Automated Remediation Actions

By looking at the 'Recommendations' area of the alert, we are able to see that vRealize Operations Manager is making a number of recommendations to correct the alert. Some recommendations are pre-defined, human provided, or even automated. The predefined options will vary depending on the type of infrastructure component.
Run Action to Remediate

Among the available recommendations, certain recommendations are actionable. By selecting the run action button, we are able to initiate an automated process that will result in vRealize Operations Manager instructing vCenter to remove the snapshot in question.

1. Click the 'RUN ACTION' button.

For more information on configuring vRealize Operations Manager Actions, please see this link: https://docs.vmware.com/en/vRealize-Operations-Manager/6.7/com.vmware.vcom.core.doc/GUID-C279EDE7-0720-462B-9BB3-5D2D2003D626.html
Initiate Automated Snapshot Deletion

A list of available VMs with snapshots is returned. Since we only have this one VM with a snapshot it is already highlighted. Select the 'NEXT' button.
We are now presented with a list of available snapshots on the VM 'base-w10'. Since we only have one snapshot it is already highlighted, we can now hit 'BEGIN ACTION' to initiate the snapshot removal.

**Task Generated**

![Delete Unused Snapshots for VM](image)

The Task ID(s): tbc45fb8-dddd-4574-9b0c-7f067760afcc

Changes may take up to 5 minutes.

We are provided with a confirmation that our snapshot removal task has started and we are provided with the task ID and a link to monitor the progress. Let's click that task link to see monitor the progress.

Once the link brings us to the 'Recent Tasks' area of Administration, we can see the status. It will initially state 'In Progress'.

**Confirming Task Completion**

![Recent Tasks](image)

By clicking on the refresh, we will see the status change to 'Completed'.
Confirm Alert is cleared

If we now return to the 'Troubleshoot a VM' guided workflow, we will now see that the VM 'base-w10' no longer shows up as having an active alert.
Conclusion

In this module you were able to explore vRealize Operations dashboards and guided workflows to identify performance issues. We were able to learn how the guided workflows navigate and correlate related infrastructure components making problem identification very fast and intuitive. In addition to a guided process to help correlate log information and configurations, we were also presented with further resolution suggestions and options to fix the issues.

You've finished module 1

Congratulations on completing the module.

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

If you want to jump to a particular module, follow one of the links below.

- Module 2 - Troubleshoot Issues Using Metrics and Logs Together with vRealize Operations and vRealize Log Insight
- Module 3 - Application and OS Monitoring Using the Endpoint Operations Feature of vRealize Operations
- Module 4 - Extending Monitoring Through The Stack - From Physical to Applications with Blue Medora Management Packs

Or if you want to end your lab,

1. Click on the END button at the top of the page.
Module 2 - Troubleshoot Issues Using Metrics and Logs Together with vRealize Operations and vRealize Log Insight (45 minutes)
Introduction

In this module you will troubleshoot an issue affecting the performance of a web server. The IIS server is experiencing high HTTP GET requests and causes a service to stop. Using vRealize Operations alerts and vRealize Log Insight you will be able to review the metrics and logs to determine what is occurring. Once a root cause is determined the information can be presented to the other teams for their review and fix the IIS server.
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 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 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 Manager - Live Instance** link to open the UI in a new browser tab

Log into vRealize Operations

![Log into vRealize Operations](image-url)
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**
Metrics and IIS example

This module uses the live version of vRealize Operations.

Search for IIS Server

The WWW Service Site is running on a Windows 2012 server called "base-w12-01". The quickest way is to search for the VM.

1. Click on the magnifying glass in the upper right corner of vRealize Operations. This is the search icon as shown in the picture.
1. Type `base` to begin the filtering items and scroll down until you find the Virtual Machine "base-w12-01". You may need to scroll down in the list to find the Virtual Machines.
2. Click `base-w12-01`
1. Verify you are viewing the Summary page of the base-w12-01 VM.
2. If there were any alerts for the VM they would be listed in the highlighted area.

Next lets take a look at the IIS Default site running on Base-w12-01.
To review the IIS Default Site we need to view the Related Objects.

1. Click Related Objects which will expand the objects contained in the folder.
2. Click IIS WWW Service Site A Default Web Site will be listed.
3. Click Default Web Site You should be presented with the Summary page of "Default Web Site"
4. If there were any Alerts they would be listed in this area of the summary screen.
   In order for alerts to appear we must create alert symptom and alert definitions.
5. Sometimes creating a dashboard to use for monitoring several metrics is helpful. Click All Metrics to begin the process.
Create Metric Charts

Two metrics we want on this dashboard is Utilization - Total Get Requests per Minute and IIS Service Availability. First we need to add them to a metric graph.

1. Click the V symbol to expand the contents of All metrics.
2. Click the V symbol for UTILIZATION to expand this section
3. Double-Click Total Get Requests per Minute to add the metric to the chart.
4. Click the V symbol for AVAILABILITY to expand the section.
5. Double-Click Resource Availability to add the metric to the chart

Add CPU Usage to Chart
One more metric needs to be added to the chart and that is the CPU Demand for the base-w12-01 VM. To change focus to the VM properties.

1. Click **base-w12-01**. If the virtual machine base-w12-01 is not appearing click **BACK** to return to the previous page.
2. Click the **V** to expand the **Utilization** metric section
3. Double-Click **CPU Demand (%)**
4. We also want to change the timeframe of the chart to be the last hour. **Click the icon that looks like a calendar.**
5. Click the **V** and select the **Last Hour** timeframe.
6. Click **GO** to set the new timeframe.

**Graphs and Create Dashboard**

Now that you have the charts in the correct timeframe it is time to create a dashboard that can be used to monitor these metrics.

1. Click the icon as shown to **Generate Dashboard**
IIS Requests & Availability

1. Enter **IIS Requests & Availability** for the name of the Dashboard.
2. Click **OK** to save the name and then click **OK** for the notice the dashboard was created.

View Dashboard

1. Click **Dashboards**
2. Click the new Dashboard **IIS Requests & Availability**
3. Move your cursor to the upper right hand corner of the dashboard and click the **Eye Icon** to turn on the toolbar.
4. Click the **Pencil Icon** to edit the widget.
Edit Dashboard

Change the refresh content settings for the dashboard with the following:

1. Click the radio button to **Set Refresh Content to ON** and enter **30** seconds for the **Refresh Interval**.
2. Click **SAVE**

Now that the Dashboard is created we need to create Alert Symptoms and Definitions.
Alerts

1. Click **Alerts** to view the Alert Settings on the left window.

Create Symptom Definition

First we need to define the Symptom definition. Symptoms are conditions that indicate problems in your environment. Once the symptom is complete, it is added to an alert definition so you are notified of a problem when it occurs with your monitored objects.

1. Click the **V** to expand the Alert Settings menu.
2. Click **Symptom Definitions**
3. Click the **+** to create a new definition.
1. For the Base Object Type click the V to expand the adapter list.
2. Click the V for the EP Ops Adapter to expand the object types.
3. Scroll down until you find the WWW service and click IIS WWW Service
Configure WWW Symptom

1. Click the V to expand the UTILIZATION Metrics section.
2. Double-Click Total Get Requests per Minute.
3. Type WWW Service for the Symptom Name.
4. Click the drop down menu and set to Critical
5. Type 100 as the threshold for the GET requests.
6. Click the V to expand the Advanced Section.
7. Change the Wait Cycle time to 1.
8. Change the Cancel Cycle time to 2.
9. Click SAVE

Filter for WWW Symptom

vRealize Operations has many predefined symptoms so lets filter to the one we created.

1. Type www in the filter field and then Enter on the keyboard. The only item displayed should be the "WWW Service definition" we just created.
The next step is to create the alert definition.

**Alert Definition**

1. Click *Alert Definitions*
2. Click the + to create a new alert.
1. Type **WWW Alert** for the name of the new alert.
2. Click **2. Base Object Type**
vCenter Adapter

Our Base object will be the virtual machine.

1. Click the V to expand the adapter list.
2. Click the V vCenter Adapter to expand the objects.
3. Scroll down and click Virtual Machine
4. Click 3. Alert Impact
Alert Impact

Verify the section "3. Alert Impact" has the settings as shown.

1. Click 4. Add Symptom Definitions
Alert Symptom

We want the alert to be triggered on the virtual machine if symptom is active on descendants. We do this by selecting the **descendant** as the object defined within the alert.

1. Click **V** and click **Descendant** to change the Defined On from Self to Descendant.
2. Click the **V** to list the available adapters.
3. Click the **v EP Ops Adapter** to expand the list of objects.
4. Scroll down and click **IIS WWW Service**
1. Click and drag the **WWW Service** to the right and drop into the Symptoms section of the workspace.
2. Click the **V** next to Count and change to **Any**
3. Click **5. Add Recommendations**
Now you can create a new recommendation for the alert.

1. Click the + to add a new recommendation.
New Recommendation

1. Type *Additional Web Servers are needed for High HTTP Requests*
2. Click **SAVE**

Drag Recommendation
1. In the filter field type Additional web
2. Once visible click and drag Additional Web Services for high HTTP Requests to the Recommendation section.
3. Click SAVE to complete the Alert Definition.

Next is to check if the default web page displays.

**IIS Web Page**

1. Open a new tab in the browser and enter http://base-w12-01.corp.local to check that the web service is functional.
Dashboards

1. Click the **tab for vRealize Operations** to return to that page
2. Click **Dashboards** to return to the dashboards area.
3. Click the **IIS Requests and Availability** dashboard if it is not the current dashboard. Notice the high and low values for the utilization are 1. This number will increase to thousands of requests shortly.

URL Stress & Stop Service

You will use a PowerShell to start a utility called **URLSTRESS** which sends thousands of **GET requests to the IIS service running on** [http://base-w12-01.corp.local](http://base-w12-01.corp.local). After a couple minutes the GET Request graph will reflect these requests. Also the VM CPU will begin to climb. After 5 minutes the availability chart will reflect a crash of the IIS service. You will investigate the logs that show the loss of service and restart the service.

1. Double-Click the **URL Stress utility** on the desktop.
URL Stress Parameters

Use the following parameters for URL Stress to send multiple HTTP GET requests to base-w12-01

1. Type [http://base-w12-01] for the URL line.
2. Set the Threads to 100
3. Set the Repeat Count to 10000
4. Click Run You should then see the requests begin and the number of current failures will be 0 as long as the WWW service is running.

This will start generating a large number of HTTP GET requests to the IIS server.
1. This metric chart is showing the number of Get requests is jumping to over 100,000.
2. The middle chart is showing that the web server has stopped running and has 0 availability.
3. The bottom chart is showing that the CPU of base-w12-01 has jumped to 75% utilization and then started dropping down after the availability went to 0.
4. Click **BACK** to see the summary of base-w12-01.
1. Let's look at the Default web page for the alert. Click **Related Objects** to expand the objects if it is not already expanded.
2. Click **IIS WWW Service Site**
3. Click **Default Web Site**.
4. You should see an alert indicating the Default Web Site is not available.
5. Click **base-w12-01** to go back to the summary of the VM.

**Alert of base-w12-01**
1. Click **Summary** if not already there.
2. Click the alert **WWW Alert** to view more details about the alert

**Base-w12-01 Web site down**

![Image of a web page with a 403 error]

1. To check if the web page is running refresh the tab that was opened earlier to the address of the IIS server.

   http://base-w12-01.corp.local
Explanation of Alert

1. Notice this area contains the recommendations you entered earlier in the lab during the Alert definition section.
2. Let's review the logs that were sent to Log Insight for this outage. Click View Logs
Log Insight is launched within vRealize Operations. Note: You may have to login "Login Via SSO" if the message appears.

There are other event types as shown in Log Insight but we are only concerned about the second group.

1. Lets change the timeframe to the last hour by clicking **Custom time range** and changing it to **Lastest hour of data**.
2. Click **Expand** to see the event details.
Events Like This

There are still the other events cluttering the list. Let's add another filter. If you hover over the area to the left of the events, a menu will appear containing a Gear icon.

1. Click the **Gear Icon**
2. Click **Events Like This** to add a filter for only events related to WWW service.

Field Table
There should be 2 filters listed on the screen now. Log Insight also has the ability to view the events in different formats. One of them is viewing the individual fields that make up the event.

1. Click **Field Table** to see a different format.

There are many additional use cases and features to Log Insight. You will find more information in the HOL-1901-01-CMP lab.

Let’s start the WWW Service again.

2. Click **Summary** to return the base-w12-01 summary page.

**Start WWW Service**

To restart the services, minimize your browser and double-click the **WWW Service Start** icon on the desktop.

**IIS Service Restored**
After a few minutes you will see the charts reflect that the WWW service has been restarted.

1. This metric chart is showing the web server is running with availability of 100.
2. The middle chart is showing that the number of Get requests has dropped back to 0.
3. The bottom chart is showing that the CPU of base-w12-01 has gone back down to 3%.
4. Click BACK to see the summary of base-w12-01.

**Base Alert cleared**

Now that service has been restored to the WWW default service, the alert is cleared and the Health of base-w12-01 is back to green.

There are some dashboards which can be viewed regarding the IIS requests.
IIS Dashboard

1. Click **Logs** to return to Log Insight.
2. Click **Dashboards** in the Log Insight application.
3. Click **V** to expand the contents of **Microsoft - IIS** dashboards.
4. Scroll down to see additional contents of the dashboards. Maybe try some other dashboards to see what additional contents exist.

Module Clean Up

To cleanup the environment for the next module, close the browser and URL Stress program.
Conclusion

In this module you discovered a issue affecting the performance of a web server. The IIS server was experiencing high HTTP GET requests. Using vRealize Operations alerts and vRealize Log Insight you were able to review the logs and determine what was occurring. Once a root cause was determined the information was presented to the other teams for their review and fixed the IIS server service.

You've finished module 2

Congratulations on completing the module.

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

If you want to jump to a particular module, follow one of the links below.

• Module 1 - Troubleshoot Infrastructure Issues using Guided Workflows in vRealize Operations
• Module 3 - Application and OS Monitoring Using the Endpoint Operations Feature of vRealize Operations
• Module 4 - Extending Monitoring Through The Stack - From Physical to Applications with Blue Medora Management Packs

Or if you want to end your lab,

1. Click on the END button at the top of the page.
Module 3 - Application and OS Monitoring Using the Endpoint Operations Feature of vRealize Operations (45 minutes)
Introduction

In this module, we will explore the End Point Operations (EPOps) adapter in vRealize Operations.

As you may already know, the vCenter adapter for vRealize Operations allows you to perform detailed monitoring of all layers of your virtualization infrastructure including virtual machines, hosts, clusters, datastores and virtual networking. While it also offers some limited insight into the guest, such as disk space utilization, it lacks some of the operating system specific metrics.

This is where the End Point Operations adapter comes into play. The End Point Operations adapter works by utilizing a Java agent inside the guest OS that allows you to expose OS-specific metrics, such as OS CPU usage, memory usage and swapping.

Another very important feature of End Point Operations is that it doesn't have to run on a virtual machine. You can install the agent on physical hardware (as long at the OS is supported) and bring in physical machine performance metrics into the vRealize Operations single pane of glass.

How it works

vRealize Operations collects information about your virtual machines by querying vCenter via the API. When you install the Endpoint Operations adapter, you augment the data collected through vCenter with metrics from inside the OS.

This is done by installing an agent on the machine (virtual or physical). This Java agent probes the OS and hardware and sends data back to vRealize Operations. For operating systems running in a vSphere virtual machine, vRealize Operations links the VM object
to the operating system object so you can see them and build dashboards and alerts based on metrics and discovered properties from the vSphere layer as well as the OS layer.
Exploring Endpoint Operations

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 instance of vRealize Operations, click to skip ahead.

In this chapter, we are going to look closer at what the Endpoint Operations adapter offers and how to use it.

Check for Lab Readiness

Before we start the next section, please check to ensure the lab is ready. If it is not, you may need to wait a few minutes until the status shows the Lab is ready.

Log Into the Live Instance of vRealize Operations Manager

The lab environment includes three instances of vRealize Operations Manager. Two of the instances are configured to run in a special mode that allows them to replay
historically collected data. We will be using a live instance of vRealize Operations for this lab module.

Launch the Chrome Browser

To launch the Chrome browser:

1. Click the Chrome icon in the Windows taskbar.

Open the vRealize Operations UI

1. Click the Live vRealize Operations shortcut or vRealize Operations Manager - Live Instance hyperlink to open the vRealize Operations login page.
Select the Authentication Source

You will see different choices for an authentication source to log in to vRealize Operations. In our lab, we have configured the VMware Identity Manager to use Active Directory for authentication and have configured vRealize Operations Manager to use the VMware Identity Manager as an authentication source. This allows for a single sign on experience within the lab.

1. Click on the drop-down menu to expand it.
2. Select **VMware Identity Manager** as the authentication source.
3. Click on the **Redirect** Button.
Confirm the Credentials

The following account information should already be filled in. If not, type or select the following information (this is the Active Directory account we will be logging in as):

User name: hol
Password: VMware1!
Domain: corp.local

1. Verify that the information is already filled in.
2. Click the Sign in button.
Finding an Operating System Object

Let's find an operating system object that has an Endpoint Operations agent in it. We can explore more of the

1. Click on the Magnifying Glass to expand the search field at the top right corner, type **w12**.
2. From the list scroll down, select the **base-w12-01.corp.local** as shown in the screen shot.

You will be taken to the Summary page for the operating system object. Remember that everything here has been collected from or calculated based on information from the OS by the Endpoint Operations agent.
Locating the OS Relationships and Metrics

To see the relationships that have been automatically created by vRealize Operations Manager for this OS object,

1. Click the All Metrics Tab.
2. Click the Show Object Relationship Down Arrow.

Viewing the OS Relationships and Metrics

The top panel is a relationship tree showing the operating system object and it's parents and children.

1. This illustrates how vRealize Operations Manager automatically builds and maintains the relationship between the vCenter representation of the virtual machine and its OS.
2. Expand the **All Metrics -> UTILIZATION** categories and **double-click** on **Percent Used Memory (%)**.

A graph of the memory usages from the perspective of the OS should show up to the right of the list of metrics.

If you don't see a graph on the right, then double click on the Percent Used Memory (%) Metric again

**Adding Process Monitoring**

In addition to the standard OS metrics, such as CPU and Memory utilization, you can also monitor specific processes running on a machine. This will give you availability and utilization on a per-process level.

The processes you wish to monitor are selected using a simple query language. You can search using process name, program path, pid file, pid and a number of other criteria. In our example, we're going to look at the VM Tools process. We do that by matching anything that contains the string "vmtoolsd" in the process name. The "ct" operator in "State.Name.ct" stands for "contains". If you want an exact match, you would use "eq" (for "equals").

To add the process monitor:

1. Click the **Actions** drop-down.
2. Select **Monitor OS Object**
3. Select **Monitor Processes**. A dialog box should pop up.
Create a Process Monitor

We want to monitor the VM Tools process running in the Linux OS of the web-01a.corp.local VM. The process monitor query will look for a process whose name contains the string "vmtoolsd".

1. In the Display Name field, enter **VM Tools**.
2. In the process.query field, enter **State.Name.ct=vmtoolsd**.
3. Click **OK**.

The UI will update.

Expand the Relationship

1. Select **All Metrics**
2. Click the **drop down** to expose the relationships.

### The New Process Monitor

You will need to zoom in a little as there are many group policy settings that are also on this OS.

1. Select the base-w12-01.corp.local OS.
2. Select the new VM Tools process monitor object that you just defined.

Note that the health indicator for the process monitor object will be gray initially. This is because the agent hasn’t yet performed its first data collection on the object.
Viewing Metrics For a Process

It will take a few minutes for the metrics to be collected for the VM Tools process monitor we just set up. For now this is just to show you where it lives.

1. Click on the **Web Service Process** icon object to bring focus to that object.
2. You can tell which object is "in focus" because the object will have a circle around it.
3. Now the metrics and properties in the lower panel will be for the Web Service Process
Examining the Process Metrics

To see metrics specific to this process:

1. Select the **IIS WWW Service** icon.
2. In the metrics list on the left, expand the **All Metrics -> UTILIZATION** group and double-click on **Process Cpu Usage (%)**. You will see the graph on the right-hand side.

The graph you're looking at shows the CPU utilization of that IIS web service. You can also monitor other metrics or the process availability from here.

Lesson Completed

Congratulations In this lesson we explored Endpoint Operations, created a process monitor, and viewed the metrics for a new process.
Building an Application Dashboard

We will be using the live instance of vRealize Operations for this portion of the lab.

As the system administrator of a clandestine agency, you must monitor components in the Web, application, and database tiers of your environment that can affect the performance of the system. You build an application that groups related objects together in each tier. If a problem occurs with one of the objects, it is reflected in the application display and you can open a summary to investigate the source of the problem further.

Locating the Applications tab

1. Click on the Environments tab
2. Select the Applications tab
3. Click on the Plus Sign to start the creation process.

Select the type of application

1. Select the Basic radio button
2. Now click Ok
1. Lets change the default to something useful: **Field Readiness App**
We decide we don't need the network tier, so let's delete it.

1. Select the **Network tier**
2. And click the **Delete Tier** button
Selecting Objects

Application Management

1. Select the Tier Name you want to add objects too.
2. Filter for IIS WWW
3. Select the service and drag it to the Tier Objects window.

Repeat this for at least 3 objects in the Web tier as seen in the Tier Objects window.
DB Tier

Application Management

<table>
<thead>
<tr>
<th>Tiers</th>
<th>Tier Name</th>
<th>Objects Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>DB</td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>App</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

1. Select the DB Tier
2. Filter again for the Database Virtual Machine and drag it to the Tier Object
3. Do the same for App Tier using the app-01a VM

You can rename each of the Tier Name's if you want.
Looking at our new application Dashboard

1. Let's go back to the **Environment** tab
2. Then click on **Applications** tab
3. Now you can select our new Application dashboard, click on **Field Readiness App**

The new application appears in the list of applications on the Environment Overview Applications page. If any of the components in any of the tiers develops a problem, the application displays a yellow or red status.

You can also edit your application dashboard from here.

Overview of the field readiness App

1. You can see recommended actions here under each object and our 3 tier app.
2. Select All Metrics

Feel free to play around with this.

Show the relationship in our App dashboard

1. Click the drop down button here to show the Relationship

Mapped view for our Application dashboard

We can now see that the 3 tier application dashboard as an object and its dependencies.

1. Double click on the web virtual machine to see which objects we added in our web tier.

You can have fun in here adding new application dashboards and any object you want to see the results.

Conclusion

The application dashboard shows how the performance of one object affects other objects in the same application, and helps you to locate the source of a problem. For example, if you have an application that includes all the database, Web, and network servers that process sales data for your business, you see a yellow, orange, or red status if the application health is degrading. Starting with the application summary dashboard, you can investigate which server is causing or exhibiting the problem.
Service Discovery Management Pack

vRealize Operations Service Discovery Management Pack (SDMP) discovers all the services running in each VM and then builds a relationship or dependencies between services from different VMs, based on the network communication.

Note that SDMP does not use agents.

Locating the Service Discovery Dashboard

1. Select Dashboards
2. Click the dropdown for All Dashboards
3. Select the checkbox for Service Discovery
4. Now you see the list added to your navigation bar
1. Select Service Relationships from the navigation pane
2. Select a service. In this case let’s select Apache HTTP
3. Wait for the Connections from the Selected Service to populate and examine the connection there.
4. We can the properties for the selected service as well.
Conclusion

In this module, we have explored the Endpoint Operations functionality of vRealize Operations. We have covered the following main topics:

- Overview of the Endpoint Operations
- Drill-down into application dashboard creation and correlation of metrics in a 3rd tier application.

You've finished module 3

Congratulations on completing the module.

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

If you want to jump to a particular module, follow one of the links below.

- Module 1 - Troubleshoot Infrastructure Issues using Guided Workflows in vRealize Operations
- Module 2 - Troubleshoot Issues Using Metrics and Logs Together with vRealize Operations and vRealize Log Insight
- Module 4 - Extending Monitoring Through The Stack - From Physical to Applications with Blue Medora Management Packs

Or if you want to end your lab,

1. Click on the END button at the top of the page.
Module 4 - Extending Monitoring Through The Stack - From Physical to Applications with Blue Medora Management Packs (45 minutes)
Introduction

For most data center operations teams, it’s pretty hard to get a comprehensive view of what’s going on in their IT ecosystems. Virtualization and cloud service abstractions have made cross-platform relationships between different layers of the IT stack more complex. Heterogenous, hybrid environments are the norm which is why visibility is a major challenge facing operations teams today.

VMware provides the best-of breed operations management for vSphere with vRealize Operations Manager (vROPS). Blue Medora complements vRealize Operations Manager and extends it’s capabilities. In this module we will use the Blue Medora management packs to deliver a robust set of dashboards.

Management Packs

Management Packs extend the capabilities of vRealize Operations Manager to third-party products and technologies to enable end-to-end operations intelligence with data visualizations, dashboards, reports, alerts, and actions. A Management Pack can also be delivered in the form of an agent plugin, content pack or compliance pack that extend the power to hybrid and heterogeneous environments, providing comprehensive visibility in a single operations console across applications, compute, storage and network devices.

We will be using the Blue Medora link for this entire module located in the Chrome Browser
Log in to the vRealize Operations Blue Medora 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 Blue Medora Management Packs instance of vRealize Operations.

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 - Blue Medora Management Pack 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 Manager - Blue Medora Management Packs** 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**
Microsoft SQL Server Health

In this module, we are going to explore Database Monitoring. Keep in mind this is not live data we will be looking at, but historical data made specifically for this Hands On Lab.

We will be using the Blue Medora HVM for this Lesson.

Finding slow queries

1. Select Dashboard
2. Select All Dashboards
3. Select Microsoft SQL Server
4. Click Microsoft SQL Server Query Plan
During a recent mission a Spectre agent was unable to download data into his mobile device and was subsequently unable to complete the mission. We need to figure out why it was taking so long. Our NOC team received an alert, but didn’t mention it to any on-call engineers. The alert was for slow query times within a database.

1. You can select whichever database server you want to view and find the worse performer.
2. The average execution time is already sorted by longest query.
3. The query we are going to use to see what is taking so long
4. The actual query text itself right in the vROPS dashboard!

Scroll to the bottom of the vROPS dashboard for the next page.
Analyzing the query

As you are looking through any anomalies here you see that one nested loop is consuming 22% of the entire transaction. In this case, you are not a DBA and you are able to create a task for the DBA team to optimize this query so that this nested loop can be removed. The Agent stops by and thanks you for your quick find.

1. Find and hover over the **Nested Loops (Inner Join) Cost 22%**
2. You can see the operator cost here

**Time saved**

Thanks to your previous work installing this management pack and then using this out of the box dashboard you saved yourself and the company hours of work trying to find this anomaly. You can now show your DBA where you think the problem might be and you have proof.

**Conclusion**

This is a very short lesson. We are simply trying to show the power of adding management packs into vRealize Operations Manager and how useful it can be.
Overall Application Health

MSSQL workloads are hosted on VMware, Hyper-V, and Docker. IT Operations needs to see these workload’s KPI’s side by side.

In this lesson we are using the Blue Medora HVM.

MS SQL Heterogenous Infrastructure overview

1. Select the **Dashboards** tab
2. Scroll down and select **MS SQL Heterogenous Infrastructure overview**
KPI's side by side

1. Select any of the **Server Instances**
2. You can see with each Server Instance you select it shows a different **VM/Container List**

Here we can see relation between VMs and containers and their metrics. We can then see all the relevant metrics we need to zero in on an issue without spending time logging into each instance which can be time consuming. Feel free to play around with this dashboard.

**Conclusion**

Since this is not a live instance and the data here is static for lab use we are only looking at what the Blue Medora Management pack can give you.
Cohesity Mission Critical Backup

1. Select **Dashboards**
2. Hover over **Cohesity**
3. Select **Cohesity Protected VMs**

**Dive into the failing object**

We can see under the Topology Graph on the right that there are unhealthy objects for the backup job on MSSQLCluster.
1. Double Click on MSSQLCluster in the Topology Graph

Looking at the alert

1. Click on the Alert link: **Virtual machine disk I/O write latency is high**
Looking at the recommended actions

1. You can see the specific failure here. Bus-Sharing is causing the snapshot to fail.

Conclusion

Here we looked at a 3rd party backup solution that can be monitored with vRealize Operations and Blue Medora. vRealize Operations is a versatile tool that can use 3rd party management packs that make it a must-have for your IT organization.
Conclusion

In this lab we were able to see the value gained from installed 3rd party management packs in vRealize Operations. This can be a huge benefit for those that don't have the time to build out dashboards base don the technology used by your company.

You've finished module 4

Congratulations on completing the module.

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

If you want to jump to a particular module, follow one of the links below.

- **Module 1 - Troubleshoot Infrastructure Issues using Guided Workflows in vRealize Operations**
- **Module 2 - Troubleshoot Issues Using Metrics and Logs Together with vRealize Operations and vRealize Log Insight**
- **Module 3 - Application and OS Monitoring Using the Endpoint Operations Feature of vRealize Operations**

Or if you want to end your lab,

1. Click on 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-1901-04-CMP

Version: 20190914-210445