# Table of Contents

Lab Overview - HOL-1884-01-HBD - VMware Cloud Services - Getting Started ........... 2
  Lab Guidance .................................................................................................................. 3
  Student Check-In ............................................................................................................. 9
Module 1 - VMware Discovery (15 Minutes) ................................................................. 19
  VMware Discovery ........................................................................................................ 20
Module 2 - VMware Cost Insight (45 Minutes) ............................................................... 29
  VMware Cost Insight ................................................................................................. 30
Module 3 - VMware Network Insight (45 Minutes) ......................................................... 64
  VMware Network Insight and Configuration ............................................................. 65
  Micro-segmentation Planning ...................................................................................... 68
  360-degree network visibility and troubleshooting .................................................. 78
Module 4 - VMware Log Intelligence (30 Minutes) ......................................................... 87
  VMware Log Intelligence and Configuration ............................................................. 88
  Getting Data Into Log Intelligence - Data Collectors .............................................. 91
  VMware Log Intelligence UI Walkthrough .............................................................. 96
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.

This lab provides a look at VMware Cloud Services and the features that will allow you to get better insight into your current cloud usage.

Note: A My VMware user account is required to access this lab.

The Student Check-In chapter will cover the My VMware requirements and how to access Cloud Services.

Lab Module List:

- **Module 1 - VMware Discovery** (15 minutes) (Basic) The discovery service allows you to see all the VMs from your multiple cloud providers. This module will also look at some of the configuration needed to power VMware Cloud Services.
- **Module 2 - VMware Cost Insight** (15 minutes) (Basic) A look at costs associated per cloud provider as well as trending information.
- **Module 3 - VMware Network Insight and Configuration** (45 minutes) (Basic/Advanced) Micro-segmentation planning and 360-degree network visibility across clouds.
- **Module 4 - VMware Log Intelligence (30 Minutes) (Basic)** Getting data in to the Log Intelligence service and a quick walkthrough the UI

Lab Captains:

- Module 1 - Alex Fanous, Senior Systems Engineer, USA
- Module 2 - Brad Christian, Senior Systems Engineer, USA
- Module 3 - Brad Christian, Senior Systems Engineer, USA
- Module 4 - Chis McClanahan, Senior Technical Product Line Marketing Manager, USA

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

[http://docs.hol.vmware.com](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

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.
Student Check-In

This article will provide guidance on how to gain access to VMware Cloud Services. You will locate the Student Check-In page, search for your My VMware email address, validate and be redirected to the VMware Cloud Services Welcome page.

During this process you will receive an email invitation from VMware Cloud Services. **This email can be ignored & deleted.** Below are the steps to validate and gain access to the lab.

Only My VMware email addresses are granted access. See the Troubleshooting section below for common fixes.

**Open Student Check-In Web Page**

Open Chrome Browser

1. On top of browser click **Student Check-In**
2. This will navigate to https://checkin.hol.vmware.com
Search and Validate

1. Enter your My VMware email address
2. Click Search
3. Click to Validate

Access to Cloud Services will be granted and you will be redirected to the login page. An email confirming your access will also be sent. Please ignore & delete.

Click here if you need to reset your My VMware password.

If you DO NOT have a My VMware account follow these steps:
1. Register HERE (MUST use same email address used to log into Hands-on Labs).
2. END this lab.
3. Locate registration email on your device (PC/Mac/Phone) and complete validation.
4. START this lab again.

Your My VMware email address must match the email address you used to login to Hands-on Labs.

If your email address is returned AND it's the same as your My VMware email address, Click to Validate
**Click to Validate** will 1) grant you access to cloud services, 2) send you a confirmation email, 3) redirect you to the VMware Cloud Service sign-in page.

Visit the **Troubleshooting** section at the end of this module if help needed.

**VMware Cloud Services Sign-In**

1. Confirm your My VMware address is shown correctly
2. Click **NEXT**
If you are a VMware employee you will be redirected to Workspace ONE for password or RSA passcode.

1. Enter your My VMware password
2. Click **SIGN IN**

Click **Forgot Password** if your password needs to be reset. Access reset emails from your personal device.
Welcome to VMware Cloud Services

This is the Console landing page which provides navigation to any cloud services you have subscribed to.

In this lab, you will have access to VMware Cost Insight, VMware Discovery and VMware Network Insight. **Enjoy!**

When this lab ends another email is sent letting you know access has been removed. You can always take the lab again to regain access.
Troubleshooting

If your email address was not found with a running lab please review these options to resolve.

- The email address used to login to Hands-On labs must match your My VMware email address.
- Register a new My VMware account to match your email address used for Hands-On Labs login.
- After creating a new My VMware account return to Student Check-In and Search again.

Message after Click to Validate
After **Click to Validate** you are returned to the Student Check-In page with a highlighted message

Invalid Email address!

The searched email address was not found in My VMware.

You must create a new My VMware account that matches your Hands-on Labs email address. Click **Register here** and create a new account. Complete all required fields. Validate the new email address from your personal device. Return to **Student Check-In** and **Search** again.

Otherwise 1) End lab, 2) logout of Hands-on Labs catalog/station, 3) login with a My VMware email address that is registered with Hands-On Labs, 4) Enroll in lab again.

Your VMware profile is incomplete

Your My VMware email address was found but there are missing fields in the profile. Login to My VMware, Edit Profile and look for required fields that are missing information.

First Name, Last Name, Department, Job Role, Industry, Business Phone, Address, City, Zip Code and Country are mandatory fields.

Make sure to **SAVE** your profile before trying the **Click to Validate** again. Sometimes a few minutes is needed before profile changes are active.

Close and re-open Chrome browser if **Click to Validate** is returning same response after profile saved.

Not active

Your My VMware email address was found but you have not finished activating the account. Use your personal device and check for an email to activate the email address. **Click to Validate** again once activated.

Capacity Limits
If you searched for your email address and this response is returned please END your lab and try again later. Each student is assigned a cloud services organization (org). When your lab started all these orgs were in use.

A few additional options will be shown.

**Set Desktop Screen Resolution**

The VMware Cloud Services interface is better used at a higher resolution than the default 1024x768
1. Right click the desktop and select **Screen Resolution**.

![Screen Resolution](image1.png)

1. Choose a higher resolution like **1280 x 800**.

### Setting Default Organization

If you are already a VMware Cloud Services customer, it may be necessary to set a default organization.

1. Click the drop-down box in the top right navigation where your full name is listed.

![Set Default Organization](image2.png)

1. On the drop-down menu, click the **Set Default Organization** if seen on the menu.
2. Ensure HOL 1884 is selected.
1. To quickly move between the various VMware Cloud Services, use the navigation at the top right hand of the page by selecting the drop-down menu and select the appropriate service. This can useful for switching between modules.
Module 1 - VMware Discovery (15 Minutes)
VMware Discovery

What is VMware Discovery?

Key Benefits

Visibility across all clouds

Every cloud has a unique way of sharing data. VMware Discovery understands the intricacies of different public and private clouds and automates the tedious process of building those cloud integration points so that you can quickly gather the inventory data necessary for finding cloud insights.

Continuous and automated collection

Once configured, VMware Discovery continuously monitor different clouds for any changes in inventory. With Discovery, you will never lose sight of your cloud resources.

See your cloud the way you want!

VMware Discovery gives you the flexibility to organize cloud resources into custom groups so that you can think about your cloud inventory and associated insights in ways that mirror your business needs.
**Student Check-In**

Follow the Student Check-In process if you have not already received access to the Console Page.

Under VMware Discovery click **OPEN**

VMware Discovery is an automated cloud inventory detection system that brings together inventory information from multiple clouds and makes it easy to search and identify workloads. Using native cloud tags and properties that have already been defined, Discovery allows organization of cloud resources in ways that mirror business needs.
1. To quickly move between the various VMware Cloud Services, use the navigation at the top right hand of the page by selecting the drop-down menu and select the appropriate service. This can be useful for switching between modules.

2. Ensure **VMware Discovery** is selected.

## Resources

Take a moment to explore the **Summary** section.

1. Proceed by ensuring the **Resources** tab is selected.

This section of the interface displays the Cloud resources discovered by the service.

## Resources Details

<table>
<thead>
<tr>
<th>Name</th>
<th>Cloud</th>
<th>Type</th>
<th>Address</th>
<th>Tags</th>
<th>Account</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-JRA-web-dont-delete</td>
<td>Amazon Web Services</td>
<td>EC2 Instance</td>
<td></td>
<td></td>
<td>AWS Prod</td>
</tr>
<tr>
<td>2-JRA-database-dont-delete</td>
<td>Amazon Web Services</td>
<td>EC2 Instance</td>
<td></td>
<td></td>
<td>AWS Prod</td>
</tr>
<tr>
<td>625Mac-014</td>
<td>Amazon Web Services</td>
<td>EC2 Instance</td>
<td>52.58.54.229</td>
<td>Description=; VCAC Owner=<a href="mailto:Auto.admin@lqa.local">Auto.admin@lqa.local</a></td>
<td>AWS Prod</td>
</tr>
<tr>
<td>com.vmware.csp.component.cafe.container_catalogitem.type.registration.name.Compute__f-mcm542-460048844743</td>
<td>Amazon Web Services</td>
<td>EC2 Instance</td>
<td>52.90.202.251</td>
<td></td>
<td>AWS Prod</td>
</tr>
<tr>
<td>_com.vmware.csp.component.cafe.container_catalogitem.type.registration.name.Compute__f-mcm542-460048844743</td>
<td>Amazon Web Services</td>
<td>EC2 Instance</td>
<td>34.267.233.34</td>
<td></td>
<td>AWS Prod</td>
</tr>
<tr>
<td>ak-software</td>
<td>Amazon Web Services</td>
<td>EC2 Instance</td>
<td>54.147.19.239</td>
<td>Description=; VCAC Owner=<a href="mailto:Auto.admin@lqa.local">Auto.admin@lqa.local</a></td>
<td>AWS Prod</td>
</tr>
<tr>
<td>akO2</td>
<td>Amazon Web Services</td>
<td>EC2 Instance</td>
<td></td>
<td></td>
<td>AWS Prod</td>
</tr>
</tbody>
</table>
Observe the details provided by VMware Discovery

1. The name of the resource.
2. The Cloud where the resource is hosted.
3. The type of Cloud.
4. The address of the Cloud.
5. The tags associated with the resource.
6. The account used to connect to the Cloud.

Filter the Discovered Resources

The Filter is a powerful tool used to examine, group and ultimately report on cloud resources.

1. Click Filter... at the top of the page and select Cloud from the drop-down box.

1. Select Amazon Web Services from the drop-down menu and hit Enter.
All the machines discovered that are running in Amazon Web Services should be displayed. You should notice the item count change next to the **Resources** title.

These groups are dynamic and will automatically populate new VMs added through the cloud provider that match the search.

**Filter within the Discovered AWS Properties**

1. Click the green plus icon to add another filter.

1. Select **Name** in the Properties drop-down box.
1. Type *JIRA* to create a wildcard that includes all instances of the text JIRA, whether there is surrounding text or not.

2. Press the Enter key.

3. Hit the Escape key or click to the side to dismiss the next Add Filter... drop-down box.

The Filter should now show Cloud: Amazon Web Services and Name: *JIRA*.

Any virtual machine that is running inside Amazon Web Services with JIRA in the name should now be clearly visible.

1. Click the Create Group icon.

This will save the filter as a Resource Group for future use. Resource Groups can also be used the Cloud Costing Service to provide fine-grained cost analysis of cloud resources. We'll go into this in more detail in the next module.
Create Resource Group

1. Enter a name for the Resource Group in the **Group Name** field.
2. Type a short description for the Resource Group in the **Description** field.
3. Note the **Group Definition** created by the Filter in previous steps. Additional filters may be added and/or changed before committing.
4. Note how many results match the filter.
5. The group may be created or canceled. Click **Cancel**.
Working with Tags

1. For the tag data type `VCAC Owner=Auto.admin@sqa.local` and hit enter.
2. You will see the results update with a total items count refresh to the right of the Resources title.
3. Click Create Group.
Create Tagged Resource Group

1. Enter a name for the Resource Group in the Group Name field.
2. Type a short description for the Resource Group in the Description field.
3. Note the Group Definition created by the Filter in previous steps. Additional filters may be added and/or changed before committing.
4. Note how many results match the filter.
5. The group may be created or canceled. Click Cancel.
Module 2 - VMware Cost Insight (45 Minutes)
VMware Cost Insight

What is VMware Cost Insight?

VMware Cost Insight is a cost monitoring and optimization service for public and private clouds that helps IT analyze and track cloud spend, identify key cost drivers, find savings opportunities and communicate the cost of services to the business. Cost Insight provides granular visibility into cloud costs so that IT leaders can map investments to strategic business priorities and ensure cost transparency.

Key Benefits

Make intelligent business decisions

VMware Cost Insight provides IT granular cost visibility to precisely attribute costs to applications and LoB teams. With a better understanding of both total cloud costs and key drivers, IT leaders can map investments to strategic business priorities, ensure cost accountability and communicate the value of services delivered to the business.

Avoid blind spots  Monitor both public and private cloud costs

With significant IT investments and expenses incurred in both public and private clouds, you simply cannot overlook or underestimate cost of operations in any one of these clouds. Cost Insight provides comprehensive visibility necessary to monitor, compare and optimize all costs, whether public or private.

Lower your cloud spend
VMware Cost Insight helps quickly identify hidden cloud waste within both public and private clouds to lower public cloud costs and free up data center capacity.

**Student Check-In**

Follow the Student Check-In process if you have not already received access to the Console Page

Under VMware Cost Insight click **OPEN**

VMware Cost Insight can also be accessed from the My Services drop-down
Cost Insight Summary

1. Note the Cost Insight **Summary**, which gives a quick snapshot of costs for the month.

Expense Overview Description

1. At the top left of the Expense Overview section, click the Information icon and read the overview description.

Expense Overview

On the initial Dashboard, VMware Cost Insight shows costs over time. Each color signifies the cost data from different cloud services. The costs projection for the next month is also displayed.
1. Mouse over the chart to see costs for an individual day.
2. Note the projected costs in the light-shaded part of the chart, to the far right on the timeline. Note that projected costs size on the chart will vary depending on the day of the month.
3. Mouse over the items in the chart legend to highlight each service.
4. Click **Private Cloud Expense** in the chart legend to remove it from the chart. This will focus on the remaining expenses in the chart legend, in this case the **AWS Expense** and **Azure Expense**.
5. Click **Private Cloud Expense** again to return it to the view.

**Inventory Distribution Across Clouds**

The bottom left section shows **Inventory Distribution Across Clouds** from the different cloud services.

1. Click the Information icon and read the overview description.
2. Note the number of **Accounts Configured**.
3. Note the **Total Number of VMs Running**.
The bottom middle section shows **Most Expensive Groups** that are being monitored.

1. Click the info icon to read the description.
2. We can see that the **All AWS Machines** group is the most expensive.
Expense Distribution Across Clouds

The bottom right section shows Expense Distribution Across Clouds in a pie graph of costs per provider.

1. Click the Information icon and read the overview description.

Cost Analysis
Click the X to remove the current filter.

Click into the filter bar and select Group.

Select **All AWS Machines** and then click off of the area.

1. Click **Apply** and you will see the dashboard update.
2. You can also **export** out the details.

**Expense trend for the month**

This area show us the current trend for this group. Hovering over the graph will show you details for costs per day.
1. The bottom window shows you all the VMs in this group. You can browse through the multiple pages of responses.
2. Select any of the VMs will show us information specific to that VM.
Individual VM summary

Summary

1. The Current Month Expense
2. Project Expense for the Month
3. Total Instances
4. Graph of the Expense trend for the month.

Amazon Web Services Cloud Provider

The navigation items above the Summary allows viewing the cost information about a specific cloud provider.

1. Click AWS to see details about AWS expenses.
AWS Expense Summary

1. At the top left of the Expense Overview section, click the Information icon and read the overview description.

AWS - Most Expensive Accounts

The Most Expensive Accounts section shows the previous month, the month to date and projected monthly expenses for each account used in AWS.

1. Click the Information icon and read the overview description.
2. Mouse over each of the bars in the bar chart for details on each account.
3. Click View Details.

1. Note the Cost Trend Column.
2. Click << Back to AWS to return to the previous page.
The **Most Expensive Services** section shows the different services used in AWS and breaks down expenses by cost and percentage.

<table>
<thead>
<tr>
<th>Service</th>
<th>Cost</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC2</td>
<td>$7,108</td>
<td>88.95%</td>
</tr>
<tr>
<td>CloudWatch</td>
<td>$303</td>
<td>3.79%</td>
</tr>
<tr>
<td>RDS</td>
<td>$233</td>
<td>2.92%</td>
</tr>
<tr>
<td>KinesisAnalytics</td>
<td>$84</td>
<td>1.05%</td>
</tr>
<tr>
<td>others</td>
<td>$263</td>
<td>3.29%</td>
</tr>
</tbody>
</table>
1. Click **View Details**.

1. Note the number of services listed.
2. Click << Back to AWS to return to the previous page.

AWS - Most Expensive EC2 Regions

<table>
<thead>
<tr>
<th>Region</th>
<th>MTD Expense</th>
<th>Number of Instances</th>
<th>vs Previous Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>us-east-1</td>
<td>$2,850</td>
<td>83</td>
<td>N/A</td>
</tr>
<tr>
<td>eu-west-1</td>
<td>$770</td>
<td>21</td>
<td>N/A</td>
</tr>
<tr>
<td>us-west-1</td>
<td>$505</td>
<td>30</td>
<td>N/A</td>
</tr>
<tr>
<td>eu-central-1</td>
<td>$405</td>
<td>29</td>
<td>N/A</td>
</tr>
<tr>
<td>us-west-2</td>
<td>$255</td>
<td>11</td>
<td>N/A</td>
</tr>
</tbody>
</table>

1. For breakdowns by Most Expensive EC2 Regions, note the arrows in vs Previous Month that indicate geographical trends. Note that N/A will be displayed until enough time has passed to display a trend.
AWS - Most Expensive EC2 Instance Type

The **Most Expensive EC2 Instance Types** details expenses by the AWS type of workload.

1. Instance Type used.
2. Month To Date Expenses.
3. Number of Instances
4. Comparison to the previous month. Note that **N/A** will be displayed until enough time has passed to display a trend.

**Private Cloud Provider**

**Private Cloud** - Private Cloud is a logical name for a group of vCenter Servers, defined by the administrator. It enumerates the **Total Cost of ownership** as defined by server hardware, storage, licenses, etc.
Select Private Cloud Provider

The navigation items above the Summary allows viewing the cost information about a specific cloud provider.

1. Click **Private Cloud** to see details about **Private Cloud** expenses.

Private Cloud Expense Summary

The vCenter Servers are grouped under Private Cloud only if they are provided with the same Private Cloud name while adding a vCenter Server.

1. At the top left of the **Private Cloud Expense Summary** section, click the Information icon and read the overview description.
2. Click **Private Clouds Configured**.
All Private Clouds

1. Note the vCenter Servers listed as *Private Cloud Names*.
2. Click << Back to Private Clouds to return to the previous page.
Private Cloud Cost Drivers

The list of Cost Drivers used in the calculation of expenses is available in a separate section of the interface.

1. Click **Manage** on the left-side navigation bar to expose the sub-menu.
2. Click **Cost Drivers**.

**Cost Drivers Explanation**

Cost Insight uses a Reference database of industry standard expenses.

**Server Hardware**

A server price depends on many different factors including how many and what CPUs it has, how much RAM it has, what other components such as hard disks, network and storage cards it has, and so on. Servers come in different form (e.g. rack mounted, tower, blade, desktop), different size (it may fill 1 rack unit or many), different power
consumption, and come with or without OS installed. Server prices decline for a given model once its newer revision hits the market.

Cost Insight has a built-in mechanism to estimate current server price based on the configuration information provided by vCenter: Server Model (e.g. HP ProLiant DL380 G7, IBM System x3250 M4), number of CPUs, CPU Model (e.g. AMD 8224 SE, Intel Xeon E5-2665), and amount of RAM. This mechanism first estimates the original price that the server might have when it was released based on the price of this exact or similar configurations. Second, the mechanism applies a double declining balance depreciation method to estimate the current value of the server.

Moreover, Cost Insight provides a fallback method to estimate server price even where some or all server configuration details are missing. For example it can bring price estimate based on CPU model and number of CPUs for unknown or missing server model.

Storage

For the sake of storage cost estimation, Cost Insight works at the level of a datastore. For costing purposes either the datastore profile (e.g. Gold, Silver, Bronze) or datastore type (BLOCK_DEVICE, Fiber Channel, NAS, SAN, OTHER) information is used to calculate costs. These two data points come from vCenter. The Reference DB maintains benchmark rates for each of the available storage types. By default Cost Insight calculates storage costs automatically through multiplying these Reference DB rates by the volume of the datastore. Users can change these rates or switch to using profiles. The newer versions of vCenter (>= 5.5) doesn’t have profiles. In this case datastore tags are used for costing purpose. If there are multiple versions of vCenters, then profiles are used to calculate storage costs for older vCenters and for newer vCenters, tags are used for calculating storage costs. This explains the default mechanism of costing storage in Cost Insight. For datastores whose luns or shares details present in EMC SRM, we use the storage base rates derived in section Storage Base Rate Calculation for EMC Arrays for calculating storage costs. For datastores created through vSAN, vSAN Storage Base Rate Calculation section provides full details of storage base rate calculations.

Note: Datastore Rate/GB reflects fully loaded cost, i.e. it is not limited to HW but rather is inclusive of additional constraints such as facilities and labor related to storage

License

OS license and OS maintenance list prices are publically available from OS vendors (e.g. Microsoft, Red Hat, and SUSE). vCenter provides what OS runs on each VM, what server this VM runs on and how many sockets this physical server has. This information is sufficient for Cost Insight to be able to calculate OS license and OS maintenance cost. It first calculates costs per physical server and then allocates it to each VM.
As in a previous case with server hardware, Cost Insight correlates the list price based approach with how much customers had actually paid, again data collected into the Reference DB.

In many cases, an IT organization may have an Enterprise License Agreement (ELA) with an OS software vendor. Usually, ELAs allow unlimited use of OS software by the IT organization replacing the per-socket pricing. Therefore, for each OS type, Cost Insight allows to specify either per-socket price or overall organization wide ELA yearly cost. For the cost allocation purposes, ELA costs are still divided between physical servers based on the number of sockets on each server.

**Network**

For a given physical host, the network cost is estimated as a product of suggested price per network port and the number of ports on this host. The suggested numbers come from the Reference DB and distinguish between 1 GB network port and 10 GB network port.

As with OS license, Facilities and Labor, a user can enter the total monthly network cost instead of providing cost per network port.

**Maintenance of Server Hardware and OS**

Cost Insight allows defining the server hardware maintenance cost and OS license maintenance cost as a percentage of the procurement cost for the corresponding items. As with the cost drivers above, a user can change an automatically suggested value (again coming from the Reference DB) to what was actually paid.

**Labor**

To estimate labor cost in a fully automatic way, Cost Insight applies labor related ratios (i.e. admin hours/physical servers, admin hours/OS instances and admin hours/VMs) to the private cloud configuration information obtained through vCenter. This allows finding approximate number of man hours required to manage a given number of physical servers and VMs. Multiplying the number of man hours by benchmarked hourly rate in the given region and number of working hours per month results in a total labor cost. The hourly rate reflects fully loaded cost (rather than only the salary component).

Users can fine-tune these ratios or alternatively override them altogether by providing total monthly costs for each one of the labor categories—physical server, virtualization and OS administration.

Labor ratios and hourly rates are a part of the Reference DB.

**Facilities**

Facilities reflect the real estate costs, more specifically the cost of data center buildings or rent, power costs, cooling costs, racks, and associated facility management labor.
Cost Insight encapsulates all facility related costs except power into the *rent price per rack unit*. Power costs come from applying power rates (price/kWh) to power consumption measured in vCenter.

Both the price/rack unit and price/kWh metrics are a part of the Reference DB.

**Private Cloud Cost Drivers Details**

<table>
<thead>
<tr>
<th>Private Cloud Cost Driver</th>
<th>Expense to Reference</th>
<th>Monthly Expense</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Hardware</td>
<td>0.00%</td>
<td>$403.03</td>
</tr>
<tr>
<td>Storage</td>
<td>0.00%</td>
<td>$3,230.25</td>
</tr>
<tr>
<td>License</td>
<td>0.00%</td>
<td>$462.46</td>
</tr>
<tr>
<td>Maintenance</td>
<td>0.00%</td>
<td>$215.91</td>
</tr>
<tr>
<td>Labor</td>
<td>0.00%</td>
<td>$359.46</td>
</tr>
<tr>
<td>Network</td>
<td>0.00%</td>
<td>$720</td>
</tr>
<tr>
<td>Facilities</td>
<td>0.00%</td>
<td>$1,281.14</td>
</tr>
<tr>
<td>Total</td>
<td></td>
<td>$6,672.25</td>
</tr>
</tbody>
</table>

1. Note the listed **Cost Drivers**.
2. Click each of the **Private Cloud Cost Drivers** to examine details for each monthly expense.
3. Click **<< Back to Cost Drivers** to return to the previous page after examining each **Private Cloud Cost Drivers**.
4. Click **Dashboard**Use the browser back button to return to **Private Cloud** in the **Dashboard** section.

1. Click **Dashboard**.
2. Click **Private Cloud**.
On the **Daily Expense Trend**, Cost Insight shows costs over time. The costs projection for the next month is also displayed.

1. Mouse over the chart to see costs for an individual day.
2. Note the projected costs in the light-shaded part of the chart, to the far right of the timeline.
3. Mouse over the items in the chart legend to highlight each section.
4. Click **Private Cloud Projected Expense** in the chart legend to remove it from the chart. This will focus on the remaining expenses in the chart legend, in this case the **Private Cloud Expense**.
5. Click **Private Cloud Projected Expense** again to return it to view.
1. At the top left of the Expense Details section, click the Information icon and read the overview description.
Most Expensive Private Cloud

1. Click View Details.

Most Expensive Private Cloud Details

1. Note how Private Cloud Name maps to a vCenter Server.
2. Click the browser back button.
Most Expensive Clusters

1. Click View Details.

All Private Clouds Cluster

1. Note how the Total Cost is listed for each Cluster.
2. Click << Back To Private Clouds.
Managing Cost Insight

A number of management features are available in Cost Insight.

1. Click **Manage** on the left-side navigation bar to expose the sub-menu.
2. Click **Data Collector**.
Deploy a Cost Insight Data Collector

You must deploy at least one cost insight data collector to retrieve your private cloud data into VMware Cloud Services.

Perform the following steps:

1. Download the Cost Insight data collector installation file.

   ![Download]
   
   Version: 7.2.0.11876
   File size: 664 MB

2. Run the data collector installation file.

   VMware recommends you to deploy the data collector in close vicinity of the vCenter Servers.

   ![An outbound internet connection is required from VMware Cloud Services to the Data Collector.]

3. Generate a one-time token.

   You must use this token during deployment to configure the data collector. For multiple data collector deployment, you must generate a unique key for each deployment.

   ![Generate]

   Note: This key expires in 24 hours. You can regenerate a new key when required.

You must deploy at least one cost insight data collector to retrieve private cloud data into VMware Cloud Services.

1. Do **not** download the **Cost Insight Data Collector**.
2. Click the Information icon and read the overview description.

Manage Private Clouds
Note that the **Add vCenter** option will be greyed out if the Data Collector is not deployed first.

1. Click the Information icon next to **Manage Private Clouds** and read the overview description.
2. Click the **Add vCenter** button.
3. Note the required information to add a vCenter.
4. Click **Cancel**.
5. Click the Information icon next to **vCenter Server Status** and read the overview description.
6. Click the Information icon next to **Data Collector Status** and read the overview description.

**Manage Public Clouds**

1. Click **Manage** on the left-side navigation bar to expose the sub-menu if it is not visible.
2. Click **Public Cloud**.
Manage Public Cloud Accounts

1. Click **Add New**.
2. Note the current public cloud providers.
Manage Groups

1. Click **Manage** on the left-side navigation bar to expose the sub-menu if it is not visible.
2. Click **Groups**.
Resource Groups

The group expense value is the sum of virtual machine expenses. The expense of private cloud virtual machines is calculated based on their utilization and the expense of public cloud virtual machines is based on their Month-to-Date (MTD) expense.

Cost Savings

1. Click Cost Savings.

At the bottom of the page is a list of VMs that have a recommended action against them.

Please proceed to Module 3, which covers VMware Network Insight.
The Cost Savings section calculates savings potential.

1. Note the **Savings Potential** under Amazon Web Services.
2. Note the **Recommendations** under Amazon Web Services.
3. Click **View Details**.
Reclamation Opportunities for AWS

1. Note the **Current Month Savings Potential**.
2. Note the **Total VMs with Reclaimable Capacity**.
3. Click the **Export to CSV** button and view the output. This data can be easily used for reporting purposes. Close the document.

<table>
<thead>
<tr>
<th>Instance or EBS volume</th>
<th>AWS Account</th>
<th>Address</th>
<th>Region ID</th>
<th>Type</th>
<th>Recommended Action</th>
<th>Month To Date Expense ($)</th>
<th>Current Month Savings Potential ($)</th>
<th>Age of Recommendation (Days)</th>
<th>Remove Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ec2-a33c3 4001</td>
<td>AWS Dev</td>
<td>107.20.62.2 05</td>
<td>us-east-1</td>
<td>EC2</td>
<td>Power Off VM</td>
<td>$54.47</td>
<td>$39.34</td>
<td>24 Days</td>
<td></td>
</tr>
<tr>
<td>ec2-0ef55 b001</td>
<td>AWS Dev</td>
<td>54.242.43.1 64</td>
<td>us-east-1</td>
<td>EC2</td>
<td>Power Off VM</td>
<td>$54.21</td>
<td>$39.15</td>
<td>24 Days</td>
<td></td>
</tr>
<tr>
<td>ec2-c9ca6 8001</td>
<td>AWS Dev</td>
<td>54.91.182.14 9</td>
<td>us-east-1</td>
<td>EC2</td>
<td>Power Off VM</td>
<td>$53.95</td>
<td>$38.96</td>
<td>24 Days</td>
<td></td>
</tr>
<tr>
<td>Amazon-m cm737-415 32383675</td>
<td>AWS Dev</td>
<td>34.201.141.22</td>
<td>us-east-1</td>
<td>EC2</td>
<td>Power Off VM</td>
<td>$41.7</td>
<td>$30.12</td>
<td>24 Days</td>
<td></td>
</tr>
<tr>
<td>Narendra</td>
<td>AWS Prod</td>
<td>52.53.203.1 29</td>
<td>us-west-1</td>
<td>EC2</td>
<td>Power Off VM</td>
<td>$31.28</td>
<td>$22.59</td>
<td>24 Days</td>
<td></td>
</tr>
<tr>
<td>aw5-BG00 25</td>
<td>AWS Dev</td>
<td>52.59.141.2 0</td>
<td>eu-central-1</td>
<td>EC2</td>
<td>Power Off VM</td>
<td>$30.1</td>
<td>$21.74</td>
<td>24 Days</td>
<td></td>
</tr>
<tr>
<td>BusinessGr o0003</td>
<td>AWS Dev</td>
<td>54.167.188. 56</td>
<td>us-east-1</td>
<td>EC2</td>
<td>Power Off VM</td>
<td>$22.65</td>
<td>$16.36</td>
<td>4 Days</td>
<td></td>
</tr>
<tr>
<td>BusinessGr o0002</td>
<td>AWS Dev</td>
<td>54.237.44. 252</td>
<td>us-east-1</td>
<td>EC2</td>
<td>Power Off VM</td>
<td>$22.59</td>
<td>$16.31</td>
<td>2 Days</td>
<td></td>
</tr>
<tr>
<td>new-vipvrv fib-server</td>
<td>AWS Prod</td>
<td>35.161.233.1 73</td>
<td>us-west-2</td>
<td>EC2</td>
<td>Power Off VM</td>
<td>$21.59</td>
<td>$15.6</td>
<td>5 Days</td>
<td></td>
</tr>
<tr>
<td>JG-Lab3</td>
<td>AWS Dev</td>
<td>52.0.30.59</td>
<td>us-east-1</td>
<td>EC2</td>
<td>Power Off VM</td>
<td>$17.64</td>
<td>$12.74</td>
<td>0 Days</td>
<td></td>
</tr>
</tbody>
</table>

1 - 10 of 99 2 3
VMware Network Insight and Configuration

What is VMware Network Insight?

Key Benefits

**Comprehensive network visibility across public and private clouds**

VMware Network Insight is purpose-built for network virtualization and public cloud security. It provides complete network visibility into all application traffic, so that you can understand application dependencies, plan security and troubleshoot issues across AWS and VMware clouds.

**Get the most out of your investment in VMware NSX**

VMware Network Insight helps build your micro-segmentation strategy and delivers actionable recommendations for quickly deploying and getting value out of VMware NSX. With Network Insight, manage and troubleshoot NSX deployments at scale using standard networking knowledge without any additional training.

**Easy to use and scale**

VMware Network Insight is search driven. Simply type a network or security query in plain English language text to find deep insights. The service is agent-less, which makes it easy to maintain and scale as your cloud infrastructure grows over time.

**Deployment options Choice is yours!**

VMware is all about choice. If you prefer SaaS and want a consumption based model, you can use Network Insight as a service by requesting access today. If you want the flexibility of deploying Network Insight in your data center and prefer a perpetual licensing model, you can get the same functionality in the form of vRealize Network Insight.
VMware Network Insight is a network and security analysis service purpose-built for software-defined data centers and public clouds. VMware Network Insight provides comprehensive network visibility and granular understanding of traffic flows between applications to enable cloud security planning and network troubleshooting. Best practices checks, intuitive UI and search simplify NSX administration, making it easier for cloud administrators to manage and troubleshoot NSX deployments at scale.

Understand application dependencies and improve cloud security
Student Check-In

Follow the Student Check-In process if you do not already have access to the console.

Click **Open** on the **VMware Network Insight** section.

You can also access **VMware Network Insight** from My Services
Micro-segmentation Planning

VMware Network Insight can plan security in Amazon Web Services by VPC or tag. This example will demonstrate how to discover firewall rules for an Amazon VPC. An Amazon Virtual Private Cloud (Amazon VPC) provisions a virtual network in a logically isolated section of AWS.

VMware Network Insight - Navigation

1. "Home" - Use this to return to the original navigation and search screen.
2. Navigation Pane
3. Search Bar including time line
4. Detail and Information Pane
5. Pinboards

Plan Security

When the VMware Network Insight portal login completes, the first screen will show a search bar at the top

1. Mouse over the Time Icon, but don't click it. This allows a search within historical data.
2. Type Plan Security and press Enter.
Traffic Distribution

Note the Traffic Distribution (by Total Bytes) section. It is an easy way to see metrics about network traffic.

1. The sum of all traffic flows, with the percentage shown as East-West only traffic.
2. Switched Traffic requires switching, both Incoming and Outgoing.
3. The percentage of Routed traffic that is routed between the East-West ports.
4. Virtual machine to Virtual Machine traffic as a percentage of the sum of East-West.
5. Traffic observed between virtual machines on the same host.
6. Traffic that requires internet access.
Focus on the Left-hand side of the **Plan Security** page on the **Micro-Segments** pane. The Micro-Segments pane can be used to generate rules for import into firewalls like VMware NSX.

Note that segmenting flows can be achieved using views that focus on **VLAN/VXLAN, Application, Tier, Subnet, Folder, Cluster, VM, Port, Security Tag, Security Groups, IPSet or VPC.**
1. Mouse over the various network segments. Observe how traffic flows are highlighted.
2. Click the drop-down box and observe the various views that are possible.

**Plan Security for a Amazon Virtual Private Cloud (VPC)**

An Amazon Virtual Private Cloud (Amazon VPC) provisions a virtual network in a logically isolated section of AWS.

1. Mouse over the left side of the interface and click on **Plan Security**.
Plan Security VPC
1. Click the **Entity** drop-down box.
2. Click **VPC**.

1. Click the second drop-down box.
2. Type "ccio". This narrows the search to all VPCs that start with "ccio".
3. Click **ccio-east-00**.
4. Click **Analyze** when done.

Note that typing **plan AWS VPC 'ccio-east-00'** in the **Search Bar** would obtain the same results.
Plan AWS VPC 'ccio-east-00'

Now display the AWS VPC 'ccio-east-00' by VM.

1. Click **by VM** in the **by Security Group** drop-down box in the **Micro-Segments** pane.
Now the **AWS VPC 'ccio-east-00'** lists each of the VMs and shows flows between them.
Flows for VM App3

1. Click **App3**.
Services and Flows for App3

Explore the **Services in this group**, the **External Services Accessed** and **Recommend Firewall Rules**.

1. Click the number under **Recommend Firewall Rules**.
2. Scroll through the **Recommend Firewall Rules**.
3. Click the three dots and select **Export as CSV**.
4. Open the CSV file and observe the rules. These rules can easily be imported into a firewall system.
5. Close **Recommend Firewall Rules**.
360-degree network visibility and troubleshooting

Network Insight includes advanced analytics that collect and display configuration data from all the components involved in the overlay and underlay of the network. Data is collected in realtime. Network Insight can gather intelligence from the network and all the components involved in sending and receiving network traffic between two objects.

Network Insight presents this in a smart user interface, and makes problem determination and visibility of the firewall and network configurations very easy.

Path of Visibility

This Section will utilize the "Path and Topology" feature in Network Insight to get 360 degrees of visibility into the network. The "Path and Topology" view can also extend to hosts, L3 networks, security groups etc., but this section will focus on the path.

From the main console:

1. Mouse over the left side of the interface and click on Path and Topology.
2. Click Path.
Path - Select source

In the Path box:

1. For Source, click the Select VM/IP Address field and scroll to bca-client, the client for a business critical application. Alternatively, simply enter the first few letters of the VM name to shorten the selection.
2. Click bca-client to select it.
Path - Select destination

1. For Destination, click the Select VM/IP Address/Internet field and scroll to IIS-WebApp1. Alternatively, simply enter the first few letters of the VM name to shorten the selection.
2. Click IIS-WebApp1 to select it.
3. Click Submit.

Note that same search could been completed by typing out and selecting each word in the string `VM 'bca-client' to VM 'IIS-WebApp1'` in the main search bar and selecting each word as it auto-populated. As users gain proficiency with Network Insight, the search bar is often faster than using UI elements.
In the **VM Path Topology**, a trace route-like visual representation of the path is displayed.

Note that each object on the path can be hovered over for details.

1. Click on **bca-client**.
VM Path Topology Details

<table>
<thead>
<tr>
<th>bca-client</th>
<th>IP Address</th>
<th>Disks</th>
<th>Datastore</th>
<th>Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLANs 222</td>
<td>10.145.222.35</td>
<td>bca-client:Hard disk 1</td>
<td>ntp_east_sata_1000_03_nfs</td>
<td>w2-m-c364:mgmt.local</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager 10.145.220.10</td>
<td>Reserved CPU (MHz) 0</td>
<td>Reserved Memory (MB) 0</td>
<td>Power State On</td>
<td>Connection State Connected</td>
</tr>
<tr>
<td>CPUs 2</td>
<td>Memory (GB) 4</td>
<td>IP Set 10.145</td>
<td>Firewall Status Protected</td>
<td>VNC Count 1</td>
</tr>
<tr>
<td>Default Gateway 10.145.223.253</td>
<td>Default Gateway Router 10.156.96.180::default [1 more]</td>
<td>Default Gateway Router Int... Vlan222 [1 more]</td>
<td>Network Address 10.145.222.0/23</td>
<td>Disconnected VNIC Count 0</td>
</tr>
<tr>
<td>OS Microsoft Windows Server 2...</td>
<td>Resource Pool Resources</td>
<td>DVS vds10g-east</td>
<td>DVS vds10g-east-222-vmmnet</td>
<td>Tag Business Units Finance</td>
</tr>
</tbody>
</table>

1. Note how additional information is displayed such as settings, interfaces and the like.
2. Close the bca-client box.
3. Note that any device on the path can display errors for additional troubleshooting.
4. Click the double arrow Response button and observe how the flow is reversed.

Note that an exhaustive description of Network Insight's path capabilities is available in vRealize Network Insight HOL 18XX.
Network Insight has the capability to

From the main console:
1. Mouse over the left side of the interface and click on **Path and Topology**.
2. Click **VMware NSX Manager**.

In the **Topology - VMware NSX Manager** box:

1. For **VMware NSX Manager**, click the **Select VMware NSX Manager** field and click **10.140.44.10**.
2. Click **Submit**.
NSX Manager Topology Details

Note the various objects included in the topology diagram to the right.

1. Click **NSX Manager** for details on Services, Associated Entities, Backups and Events. Close the NSX Manager.
2. Explore the other related entities on the diagram.
NSX Manager Checklist Details

The **NSX Checklist Rules -All** is an easy place to ensure NSX is configured correctly.

1. Click the three dots.
2. Click **Maximize**.
3. The list can now be scrolled through. Mouse over each of the checklist **Rules**, note how the rules can be used to investigate errors impacting a NSX environment.

**Module Conclusion**

This concludes the Network Insight Module, Be sure to check out the extended Network Insight Lab **HOL-1828** to learn more.
VMware Log Intelligence and Configuration

What is VMware Log Intelligence?

Key Benefits

Log Intelligence offers unified visibility across private clouds and AWS, including VMware Cloud on AWS, to provide deep operational insights and faster root cause analysis. It adds structure to unstructured log data, provides rich dashboards and delivers innovative indexing and machine learning based intelligent grouping for faster troubleshooting.

Rapidly troubleshoot your SDDC

Quickly understand the health of an SDDC environment by identifying anomalies across infrastructure and applications. Out-of-the-box dashboards for VMware SDDC solutions such as vCenter, NSX, and vSAN as well as robust log aggregation and analytics accelerate troubleshooting.

Monitor and manage log data at scale

Log Intelligence ingests logs in a secure and efficient manner and delivers sophisticated analytics. Log Intelligence has enterprise-class scalability, designed to handle all kinds of machine generated data and delivers near real-time monitoring.

Support for VMware Cloud on AWS

Analyze VMware Cloud on AWS audit logs as well as vCenter logs with quick and easy integrations. Log Intelligence also offers AWS cloud native application troubleshooting support.
Student Check-In

Follow the Student Check-In process if you do not already have access to the console.

Click **Open** on the **VMware Log Intelligence** section.
You can also access **VMware Log Intelligence** from My Services
Getting Data Into Log Intelligence - Data Collectors

When starting with Log Intelligence you will deploy a data collector into your private datacenter. The Remote Data Collector (RDC) is used as a log stream proxy to encrypt and compress log data before sending it to the Log Intelligence service. For this lab an RDC has already been deployed so for this module we will walk-through the process of deploying an RDC but will not actually deploy one.

Introduction

1. From the Log Intelligence home screen click on the double chevron in the upper left corner to expand the navigation pane.
Navigate to Data Collector Screen

1. From the expanded navigation pane select Manage to expand the management options.
2. Select Data Collectors to switch to the Data Collector information screen.

Data Collectors Screen

The Data Collectors page shows a list of the RDCs which have been deployed and collecting data for your instance of Log Intelligence.

1. This is the name given when deploying the data collector
2. The status of the data collector. If the RDC has not sent data to the Log Intelligence service then there will be a yellow warning symbol versus the green check mark.
3. When available the IP address of the collector will be displayed.
4. Next is the date that the collector was deployed.
5. Click on the ADD NEW button.

**Setup RDC Screen**

---

This is the Data Collector Setup screen. This screen will walk you through the process of deploying the data collector in your private data center.

1. Step one provides three methods to download the OVA for deployment. There is a download button and a URL to use for automated deployments of the OVA. There is a button to download the AMI for AWS.
2. Step two is to deploy the OVA into your private cloud vSphere environment using the typical OVA deployment methods.
3. Step three provides you will a one time secret key that you will use during the OVA deployment. This key links the remote data collector with your Log Intelligence instance.
4. Step four is informational to let you know that the registration process of the data collector to your Log Intelligence instance can take a few minutes. Normally this
registration process should take no longer than 10 minutes. You will know the data collector is deployed when it shows up in the list of data collectors with a green check mark.

5. Click the NEXT button.

**Configure Forwarding**

This final screen in the remote data collector deployment process shows valuable information about traffic flow and configuring infrastructure to the Log Intelligence data collector.

1. This diagram shows the traffic flow from devices sending data to the remote data collector and which ports and protocols are accepted. It is also important to note that all data sent from the data collector to the Log Intelligence service is encrypted and compressed over port 443.

2. This list provides clickable links that will give you step by step instructions on pointing different infrastructure component logs to the remote data collector.

3. Click FINISH to complete the deployment process.

**Summary**

This concludes this lab module. In this module you walked through the process of deploying a remote data collector (RDC) into your private data center. The RDC is the appliance that proxies your log data stream into Log Intelligence for analytics.
In the next module you will get familiar with the user interface of Log Intelligence to see all the great capabilities of the solution.
VMware Log Intelligence UI Walkthrough

In this module we will walkthrough the user interface for Log Intelligence. After completing this module you will have the necessary understanding of all the features that make up the Log Intelligence solution.

Home Screen

Navigating Log Intelligence is very easy by using the navigation pane on the left side of the screen. We will be walking through the Home screen to start.

1. Select the Home screen from the navigation menu.
The first section of the Home screen we will focus on is the quick search bar. The quick search bar is an easy way to create text-based query against log in Log Intelligence. You can take anything from a host name to a general word and Log Intelligence will try to assist with the search with auto-complete assistance as well as show you the number of entries found matching your text search.

1. Enter the word "error" in the quick search bar to see what comes up from an auto-complete assistance. Feel free to try any other search words. Don't actually execute the search yet as we are going to look at more of the Home screen before moving on.
Next let's take a look at the Recent Alerts widget on the Home Screen.

1. The Recent Alerts widget will show you any alerts that have occurred in the last hour or day in your environment.
2. The MORE ALERTS link will take you to the full alerts screen in Log Intelligence. Don't click on that link as we will explore the Alerts screen later in the module.
Event Observation

The Event Observations widget is a collection of queries that VMware has put together to quickly see if there are any anomalies in the environment. If there is a large spike or dip in the number of events for one of the specific observations that graph will present itself at the top of this widget.

1. Click on the ALL OBSERVATIONS link to see all the queries Log Intelligence is currently observing.

All Observation Screen
The Event Observations screen populates with common queries that have seen spikes in the number of occurrences. Hovering your mouse over the charts will show the count of events at the given time. You can click on the name of any of the widgets to launch into the Log Explorer screen.

1. Click on the vSphere Errors widget title to continue to Log Explorer.

### Log Explorer

You are now in the Log Explorer screen of Log Intelligence. Because we clicked on the vSphere Errors widget from the Event Observations screen we are brought to Log Explorer in the context of the query that makes up that widget. This is just one example of the many advanced queries that are provided out-of-the-box in Log Intelligence. We will look at the list of those queries later in the walkthrough. For now let's clear this query and continue to get familiar with the Log Explorer screen.

Click on the CLEAR ALL link.

### Creating Queries in Log Explorer

1. Search for text in logs by entering information in the search bar.
2. Easily add filters to your search criteria.
3. Change the time frame of the query results from last 1 minute up to the last 48 hours.
4. You can also give a name to the query by selecting the pencil icon and entering a name.
Query Results in Log Explorer

1. A stream of detailed log data based on the query results.
2. The chart populates based on your query results. This chart is interactive and you can zoom into a specific time by clicking at the desired time.

Log Details

Clicking on the drop down chevron on one of the log entries with provide more details on the specific entry including fields that were extracted by Log Intelligence.

- Click on any of the log entries to see the details of the log.
Extracted Fields

The Fields area breaks down the indexed and content sections of the collection of logs as a result of the query. These fields are interactive and allow you to drill down to specific logs based on things like hostname for example.

Saving Queries

If you have the administrator role for Log Intelligence you will be able to save your created query as well as create alert definitions from the query.

1. Click on the three dot icon to bring up the drop down menu.
Accessing Saved Queries

This dropdown menu provides several other options that can be performed on your created query:

- Open Saved Query - This will take you to a list of all of the saved queries both out-of-the-box and user saved queries in Log Intelligence.
- Save As - If you have pulled up an existing query then modified it, you can use the save as option to give it a new name in the saved query inventory.
- Add to dashboard will create a widget on the dashboard screen. We will explore the dashboard screen later in this walkthrough.
- Edit Description - Allows you to edit the description of the saved query for easy consumption by other users.
- Delete - If an administrator, allows you to delete the query in context.

Click out of the menu area to close the dropdown.

PINBOARD

Let's take a look at the PINBOARD feature of Log Intelligence. The Pinboard is a great way to bring up several queries at the same time and compare them to each other. To show this capability we are going to create three queries to search for errors for three ESXi hosts in a cluster to see if any of the three host are seeing more errors than the others. This is a quick way to quickly pinpoint which host in a cluster might be having issues.

1. In the search bar type the word "error".
2. Add a filter with the following criteria: hostname, contains, w2-sm-c3b1
3. Select the last hour for the time range
4. Then select the eye glass icon to get the search results
5. Finally click on the icon that looks like a pin to add the query to the Pinboard.

**Pinned Query**

![Pinned Query Image]

You will see the query show up on the Pinboard.

1. Click outside the pinboard to temporarily close the Pinboard

We are now going to repeat the above steps two more times.

1. In the search bar type the word "error".
2. Add a filter with the following criteria: hostname, contains, w2-sm-c3b2
3. Select the last hour for the time range
4. Then select the eye glass icon to get the search results
5. Finally click on the icon that looks like a pin to add the query to the Pinboard

**Finally Query:**

1. In the search bar type the word "error".
2. Add a filter with the following criteria: hostname, contains, w2-sm-c3b3
3. Select the last hour for the time range
4. Then select the eye glass icon to get the search results
5. Finally click on the icon that looks like a pin to add the query to the Pinboard
Comparing Queries

You now can see that there are three queries on the pinboard. Let's compare these three queries.

1. Click on the compare button.

Comparing Queries Continued

You are now on the comparison screen where you can see and compare the queries that were on the Pinboard. In this example, again, we are looking at the three hosts in a
cluster to see which one is seeing more errors than the others to try to pinpoint which host might be causing issues.

Note: The Pinboard is not permanent. This means when you log out of your Log Intelligence sessions the Pinboard is cleared.

Navigating to Dashboard Screen

Click on the icon that looks like an odometer to continue the walkthrough to the Dashboard screen.

Dashboard Screen

The Dashboard screen is used to put interesting queries you would like to quickly be able to reference at any time. You must be an administrator to be able to add queries to
the dashboard. In this example the three host error queries you did previously have been pre-saved to the dashboard screen.

- You can modify the time range for all the queries on the dashboard.
- Plus, you can navigate back to Log Explorer in context of the specific query by clicking on the widget name.

Click on the navigation pane to expand it out. Then click on Recent Alerts.

1. Click on Recent Alerts.

**Recent Alerts**
The Recent Alerts screen provides a sequential list of all alerts that have triggered in Log Intelligence. List will go back as far as 30 days.

1. You can select the graph to show the last hour, day, or week.
2. The graph shows a line for each alert that was triggered in the selected time range. You can roll your mouse over the alerts to see more information on the alert.
3. This is the list of triggered alerts in the order in which they were triggered. It also includes the date and time the alert was triggered.
4. Click on the the dot icon to expand the options drop down.

**Alert Details**

1. Click on the Details link to open the alert details page.

**Alert Details Screen**

The Alert Details screen gives you all the pertinent information about the triggered alert.

1. Notifications - List all notifications that were sent when alert was triggered.
2. Description - The description given to the alert.
3. Query - The exact query that was used as the alert definition.
4. Triggers - A description of the criteria that triggered the alert.
5. Chart - A current chart depicting the query the alert is based on.
6. Results Pane - A current result of the query in realtime.

Click on Recent Alerts in the navigation pane to return to the Recent Alerts screen.

**Alert Definitions**

Again, click on the three dot icon next to one of the alerts in the alerts list.

1. Select Definition from the drop down options list.

**Alert Definitions Details**

You are now on the Alert Definition screen. Here you can see and edit the alert.

Note: Only a Log Intelligence Administrator role can edit alerts. Also out-of-the-box alerts cannot be edited but they can be cloned which we will discuss later in this module.

1. Notifications - Clicking the pencil icon, as an administrator, allows you to select what notifications will be send when this alert is triggered.
2. Description - The description of the alert.
3. Query - Clicking on pencil icon, as an administrator, allows you modify the query for the specific alert. **Note:** If there is no pencil then this alert is one of the many out-of-the-box alert definitions that comes with Log Intelligence and cannot be modified.
4. Trigger - Clicking on pencil icon, as an administrator, allows you modify the trigger for the specific alert. **Note:** If there is no pencil then this alert is one of the many out-of-the-box alert definitions that comes with Log Intelligence and cannot be modified.
5. Enabled - A slider to enable or disable the alert.
6. Chart and Query Result - This is a current chart and results list of the query.

Again, click on Recent Alerts from the navigation pane to return to the Recent Alerts screen.

**Query Option**

Again, click on the three dot icon next to one of the alerts in the alerts list.

1. The final option in the options menu is the Query link. This link will take you back to Log Explorer in context of the query that defines the alert you selected from the list. Feel free to click on query if you would like and explore the alert query and current results.
Alert Definitions List

From the navigation pane select Alert Definitions

1. Click Alert Definitions

Enabling Alerts

You are now on the Alert Definitions list screen. Here you can see the over 75 out-of-the-box alerts that come with Log Intelligence as well as any custom alerts defined by a Log Intelligence administrator. These out-of-the-box alerts cover VMware solutions such as vSphere, NSX, VSAN. More solutions are being added regularly.
1. You enable alerts individually or in batch by selecting the all checkbox or checking all the alerts you want enabled and then moving one of the sliders to enabled position.
2. If you are looking for a specific alert you can filter by typing part of the alert name in filter field. For example, typing SSH in the Filter field will list alerts that are specific to SSH.
3. Clicking on one of the three dot icons will bring up the edit link and take you to the Alert Definition edit screen which you saw earlier in this module.

Managing Notifications

In the final portion of the walkthrough we will look at the notification options that come with Log Intelligence.

1. From the navigation pane select Manage.
2. Then select Email Configuration.
Log Intelligence comes with a built-in SMTP server. You can use the built-in server or configure Log Intelligence to use your corporate SMTP service.

1. You can enter the necessary configuration for your corporate SMTP service.
2. Send a Test Email by clicking the **SEND TEST EMAIL** link and enter your email address to get a test email notification.
Webhooks

Let's at the second notification option in Log Intelligence.

1. From the navigation pane select Manage.
2. Then select Webhook Configuration.
Webhook Configuration

Webhook are a great way to integrate Log Intelligence with any other system in your infrastructure that can accept REST API calls. For example you may configure a webhook to work with vRealize Orchestrator to trigger a workflow action in the event that an alert in Log Intelligence is triggered.

1. Select NEW WEBHOOK link to create a new webhook and give it a unique name.
2. This where you enter the URL to the receiving systems REST API. This must be a FQDN and cannot currently be an IP address.
3. Select the format you want to send the payload in. Your choices are XML or JSON.
4. Enter any credentials that might be necessary to send data to receiving REST API.
5. The area is where you will put the payload information for the notification. This must be in the format you selected in step 3 (either XML or JSON).
6. Log Intelligence provides a set of dynamic values that that can be set in the payload.
   - resultURL - A link that will take you directly into Log Intelligence to the query that resulted in the triggered alert.
   - sourceInfo - This lets you know which instance of Log Intelligence triggered the alert.
   - name - The name of the alert that was triggered
   - description - The description of the alert that was triggered
   - triggeredAt - The exact time and date the alert was triggered

Using webhook can extend Log Intelligence to any system in your environment that can except REST API POST.
Summary

In this module you walked through the user interface for Log Intelligence. From the Home screen, to Log Explorer screen, to configuring alerts and notifications you can see that Log Intelligence is a simple way to aggregate all your SDDC logs into an easy to use and effortless log analytics SaaS solution.
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-1884-01-HBD

Version: 20180601-202952