HOL-2601-06-VCF-L

HANDS-ON LABS MANUAL - 2026

VMware Cloud Foundation 9.0 - Operations: Analyzing Logs, Metrics, and Network Flows

HOL-2601-06-VCF-L

vmware by Broadcom

Table of Contents

VMware Cloud Foundation 9.0 - Operations: Analyzing Logs, Metrics, and Network Flows (HOL-2601-06-VCF-L)

VMware Cloud Foundation Operations 9.0 provides you with some new ways on how to manage and compare logs, create log dashboards, create simple or complex search queries for metrics as well as explore and analyze network flows within a single console. In this lab you will learn how to use the new Analyze console which combines the view of VMware Cloud Foundation Operations for logs and VMware Cloud Foundation Operations for networks in one console.

Lab Guidance

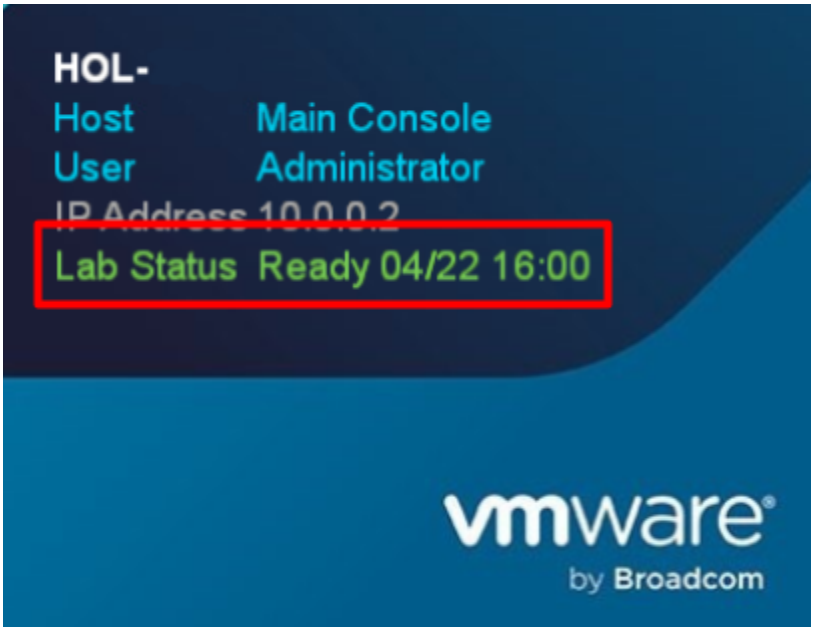
Welcome! This lab is available for you to repeat as many times as you want. Use the Table of Contents in the upper right-hand corner of the Lab Manual to jump ahead to any module.

Module	Title	Length	Level
1	Introduction to VCF Operations for log and VCF Operations for Networks	15 min	Beginner
2	Explore and Analyze Logs and build a Log Dashboard in VCF Operations	30 min	Intermediate
3	Explore and Analyze Object Metrics in VCF Operations	30 min	Intermediate
4	Explore and Analyze specific Flows in VCF Operations	30 min	Intermediate
5	Advanced Log Management in VCF Operations for Logs	30 min	Advanced

Lab Authors:
Fred Hofer, William De Marigny

First time using Hands-on Labs?

If this is your first time taking a lab you can review the VMware Learning Platform interface before proceeding.



The lab console will indicate when your lab has finished all the startup routines and is ready for you to start. If you see anything other than "Ready", please wait for the status to update. If after 5 minutes your lab has not changed to "Ready", please ask for assistance.

Module 1 - Introduction to VCF Operations for log and VCF Operations for Networks (15 minutes) Basic

VMware Cloud Foundation (VCF) Operations delivers enhanced observability and operational insights across your private cloud environment. Two key components—**VCF Operations for Logs** and **VCF Operations for Networks**—help administrators proactively monitor, troubleshoot, and optimize infrastructure performance.

VCF Operations for Logs provides centralized log aggregation, parsing, and analysis, allowing users to quickly identify anomalies and root causes across the VCF stack. It integrates with VCF Operations to offer powerful search capabilities, customizable dashboards, and intelligent alerting.

VCF Operations for Networks enhances visibility into the virtual and physical network fabric. It supports traffic flow analysis, network topology visualization, and performance diagnostics to ensure application connectivity and network health within the SDDC.

Together, these tools offer a unified operations experience that helps maintain stability, compliance, and efficiency in VCF environments.

Login to VCF Operations

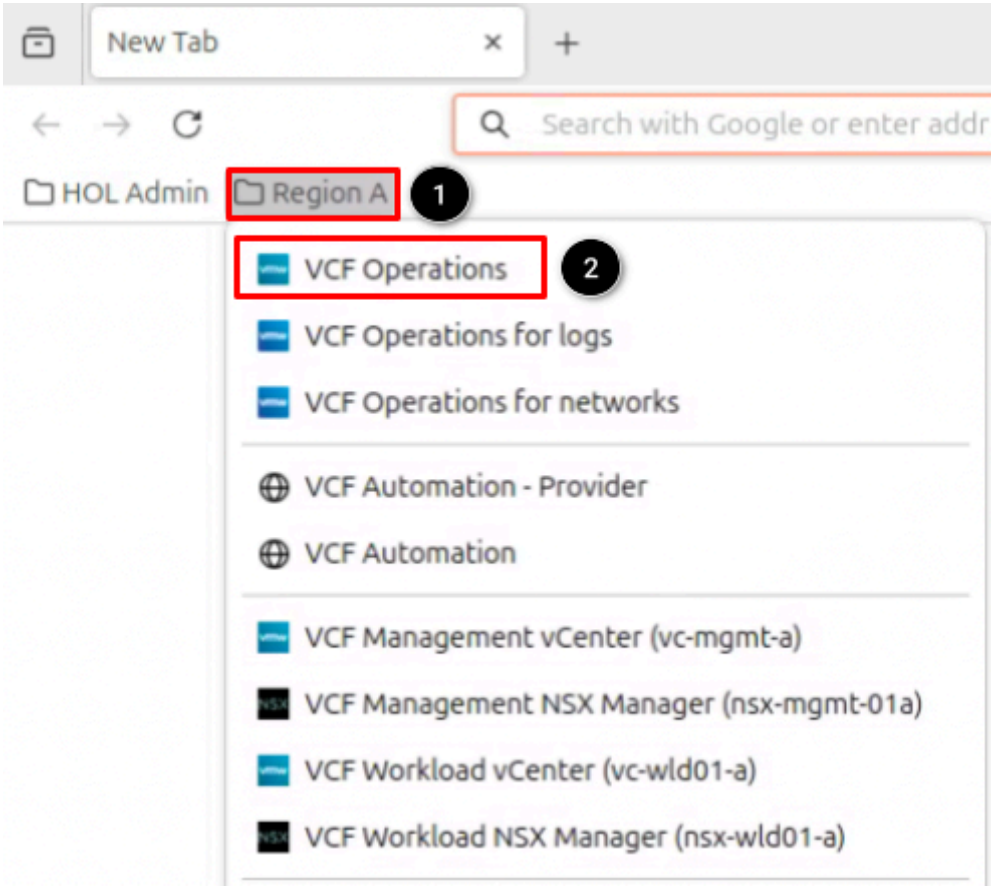
In the following few pages, we will walk through the process for logging in to VCF Operations.

Start Firefox

Open the Firefox Browser from the Linux Task Bar.

1. Click on the Firefox icon to open the browser.

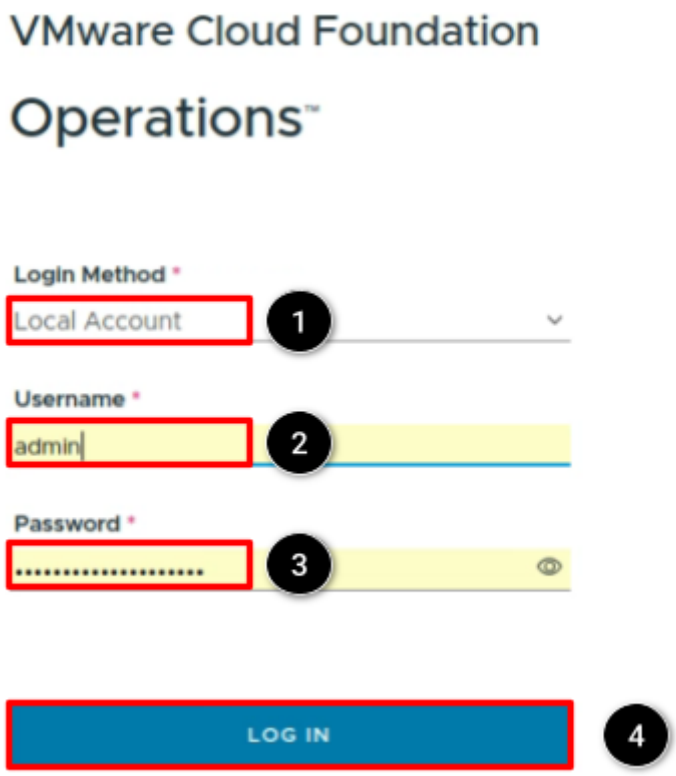
Open VCF Operations Console



Once Firefox has loaded:

1. Click on the **Region A** bookmark folder.
2. Click **VCF Operations**.

Login to VCF Operations Console

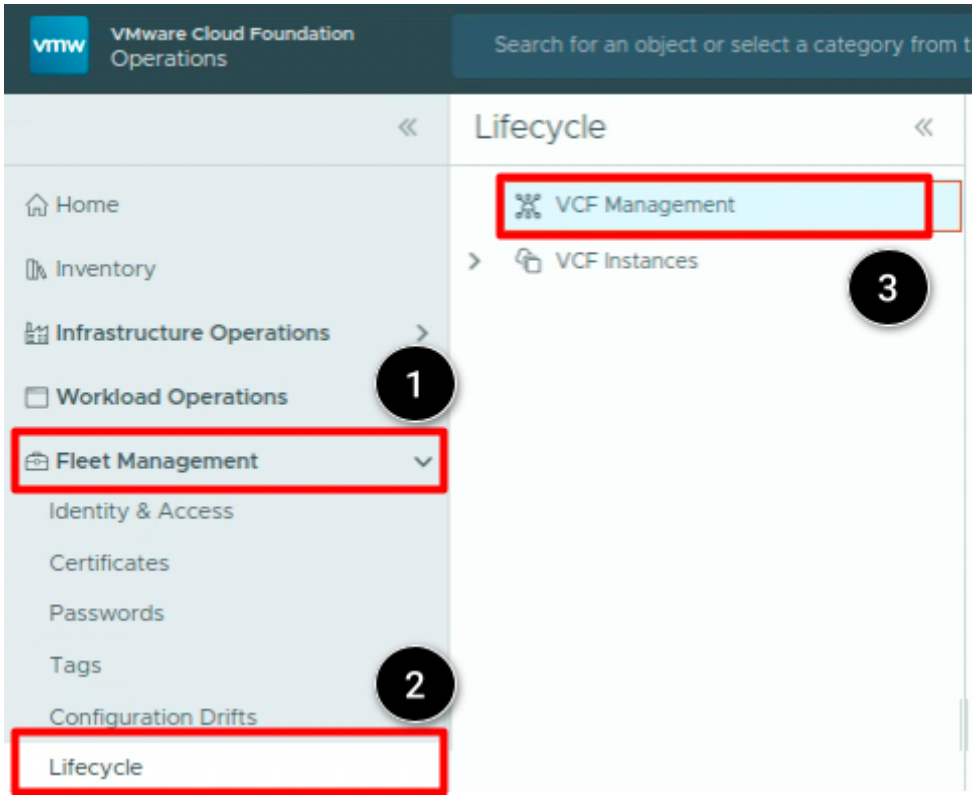


The credentials for **admin** should already be cached in the browser window.

At the VCF Operations login prompt, select the login method and type in the following user and password information:

1. At the Login Method dropdown, select **Local Account**.
2. At the username field, type **admin**.
3. At the password field, type **VMware123!VMware123!**
4. Click **LOG IN**.

Fleet Management - Lifecycle

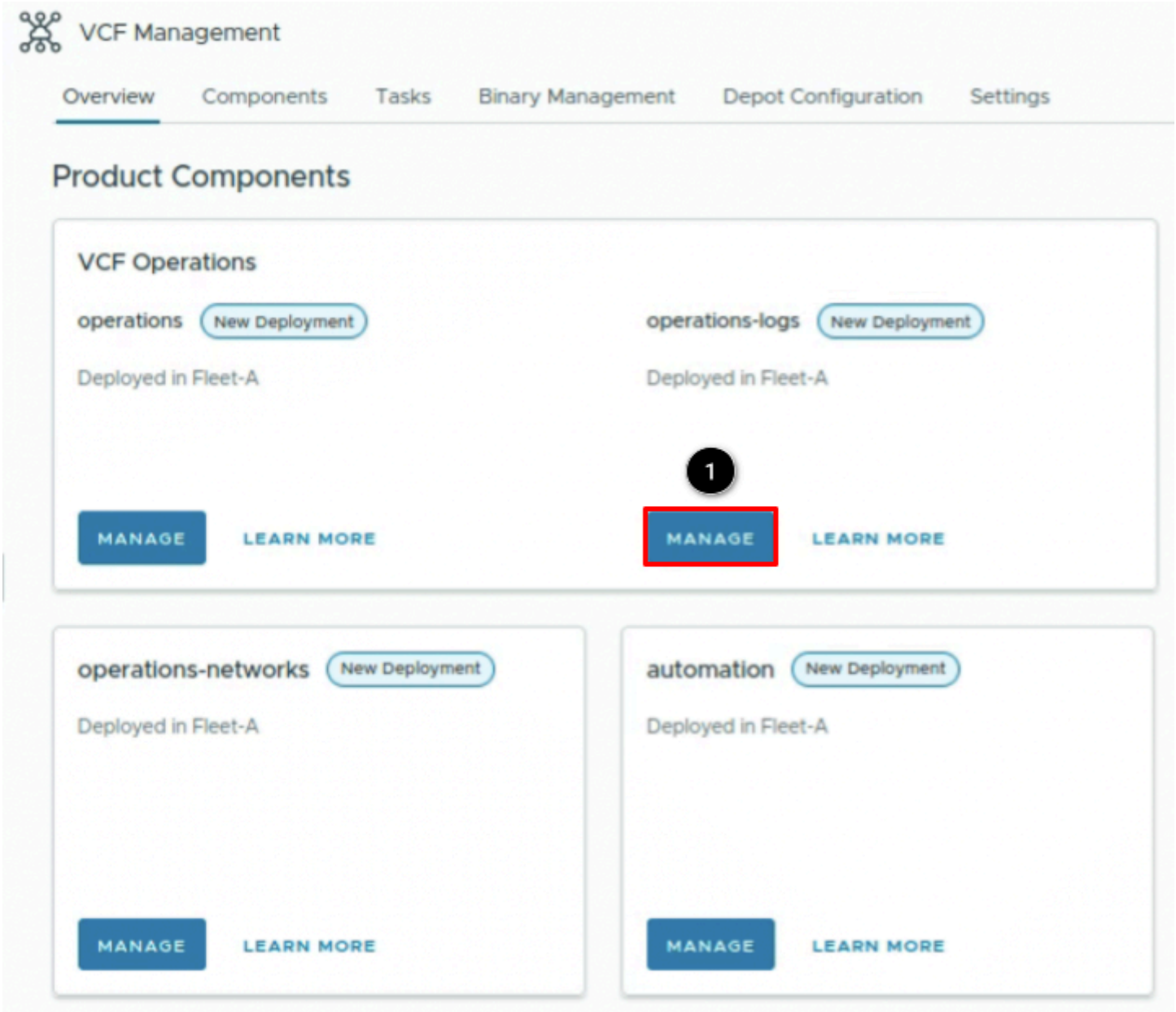


VMware Cloud Foundation (VCF) Operations is deployed automatically through the VCF Installer as part of the core platform. However, **VCF Operations for Logs** and **VCF Operations for Networks** are not included by default. These components must be **installed and configured separately** to enable advanced logging and network monitoring capabilities. Administrators can deploy them on-demand based on operational requirements.

After the login to VCF Operations follow these steps::

1. Click **Fleet Management**.
2. Click **Lifecycle**.
3. Click **VCF Management**.

VCF Management - Overview

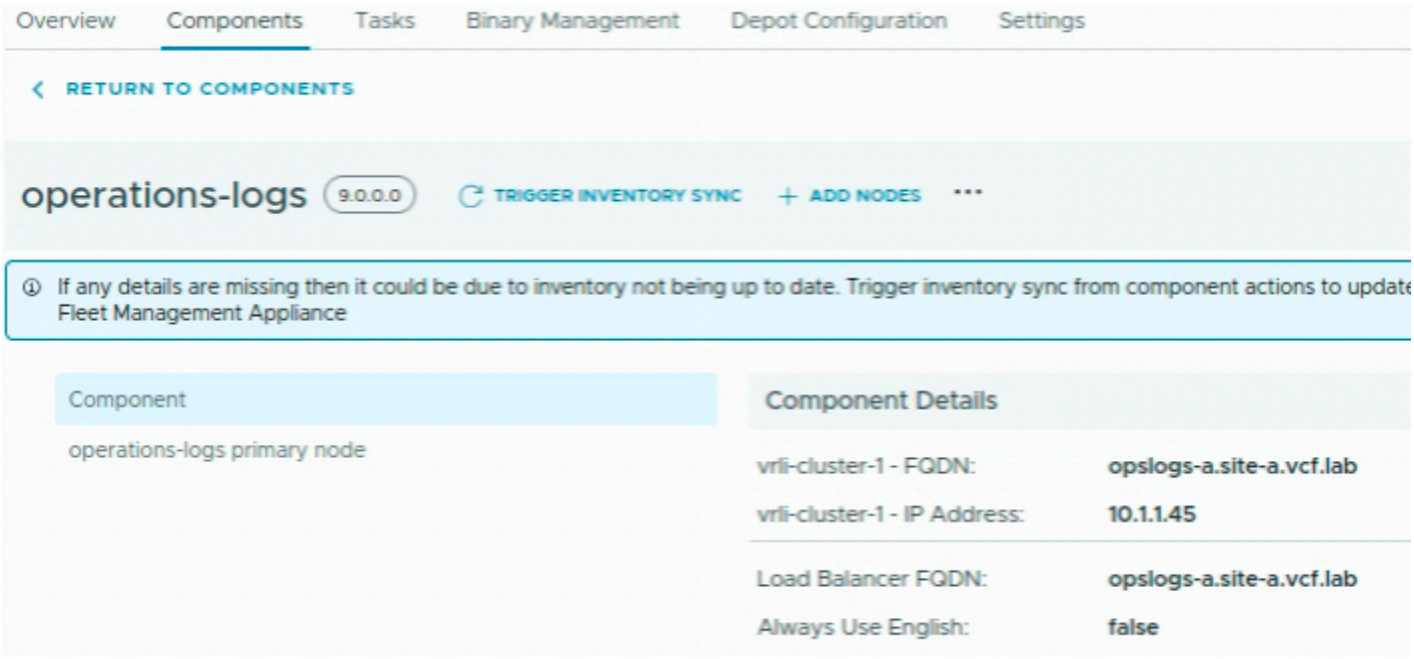


The **VCF Management Overview** page, displays all products available for deployment. Once the full VMware Cloud Foundation stack has been deployed, **VCF Operations** and **VCF Automation** are installed by default. In the lab environment, **VCF Operations for Logs** and **VCF Operations for Networks** have already been deployed as well—otherwise, there would be an **ADD** button instead of the **MANAGE** button.

To inspect the current configuration of e.g. VCF Operations for Logs follow this step:

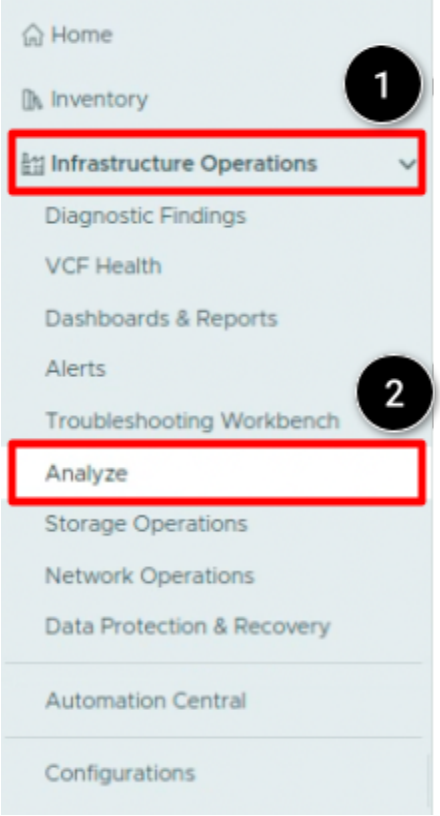
1. Click **Manage**.

VCF Management - Components



The component interface, presented in the familiar layout of the former Aria Suite Lifecycle, displays all configuration parameters defined during the initial deployment—such as FQDN, IP address, and others. As in previous versions, the deployment can be scaled up using the **three-dot menu** next to **ADD NODES**, or scaled out by adding additional nodes.

Infrastructure Operations - Analyze

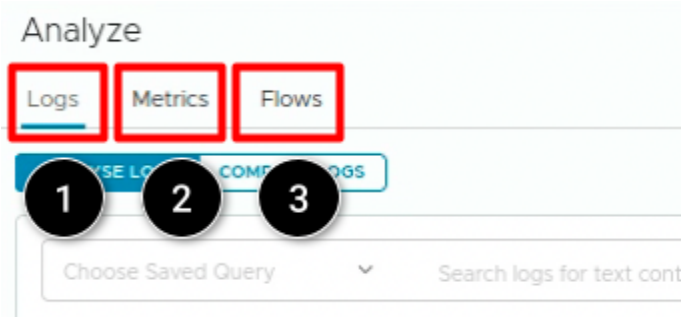


Many capabilities in **VCF Operations** become available only when **VCF Operations for Logs** and **VCF Operations for Networks** are deployed and properly configured. One of these capabilities is the new Analyze console.

To get there follow the following steps:

1. Click **Infrastructure Operations**.
2. Click **Analyze**.

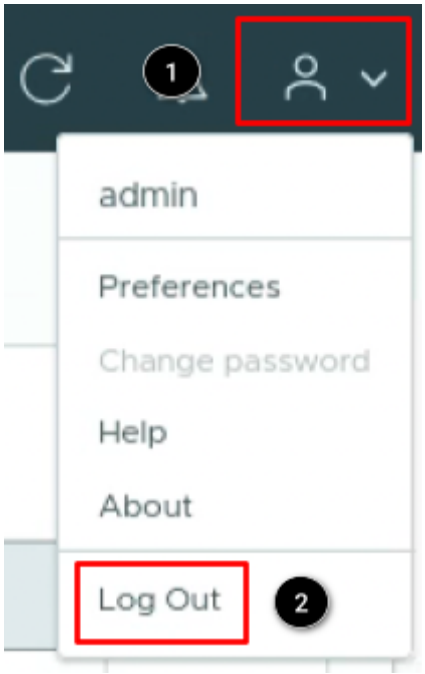
Analyze Console



The **Analyze** console contains three distinct tabs designed to support troubleshooting across various scenarios. Each of these tabs will be explored in greater detail in the upcoming modules.

1. **Logs**: Provides an integrated user experience for log analysis. (**Module 2** - Explore and Analyze Logs and build Log Dashboards in VCF Operations
2. **Metrics**: Provides an interface to analyze metrics and objects by creating a query. (**Module 3** - Explore and Analyze Object Metrics in VCF Operations)
3. **Flows**: Provides comprehensive visibility into network traffic patterns, performing analysis based on the entities, flows and time range. (**Module 4** - Explore and Analyze specific Flows in VCF Operations)

Logout



To Log out of VCF Operations:

1. Click the **User icon** to open the settings menu.
2. Click **Log Out**.

Conclusion

VCF Operations for Logs and **VCF Operations for Networks** are key components that must be deployed separately to fully leverage the capabilities of the VMware Cloud Foundation stack. Once deployed, they unlock additional functionality in VCF Operations—such as the **Analyze** console, which provides powerful tools for troubleshooting a wide range of scenarios.

From here you can:

- Take this quick survey to provide feedback about your experience with VCF 9.0
- Continue with the next lab module.
- Click [vlp:table-of-contents|Show Table of Contents] to jump to any module or lesson in this lab.
- End your lab and return in the future.

Module 2 - Explore and Analyze Logs and Build a Log Dashboard in VCF Operations (30 minutes) Intermediate

VMware Cloud Foundation Operations 9.0 provides an integrated user experience for log analysis. You can view and analyze logs from the VCF Operations console. The new centralized logs collection architecture provides the benefits of log collection across different VMware Cloud Foundation components, granular log configuration and cross data center log collection.

VCF Operations provides centralized management for log collection across all the VMware Cloud Foundation components. It also supports diagnostic and monitoring features that rely on these logs.

Login to VCF Operations

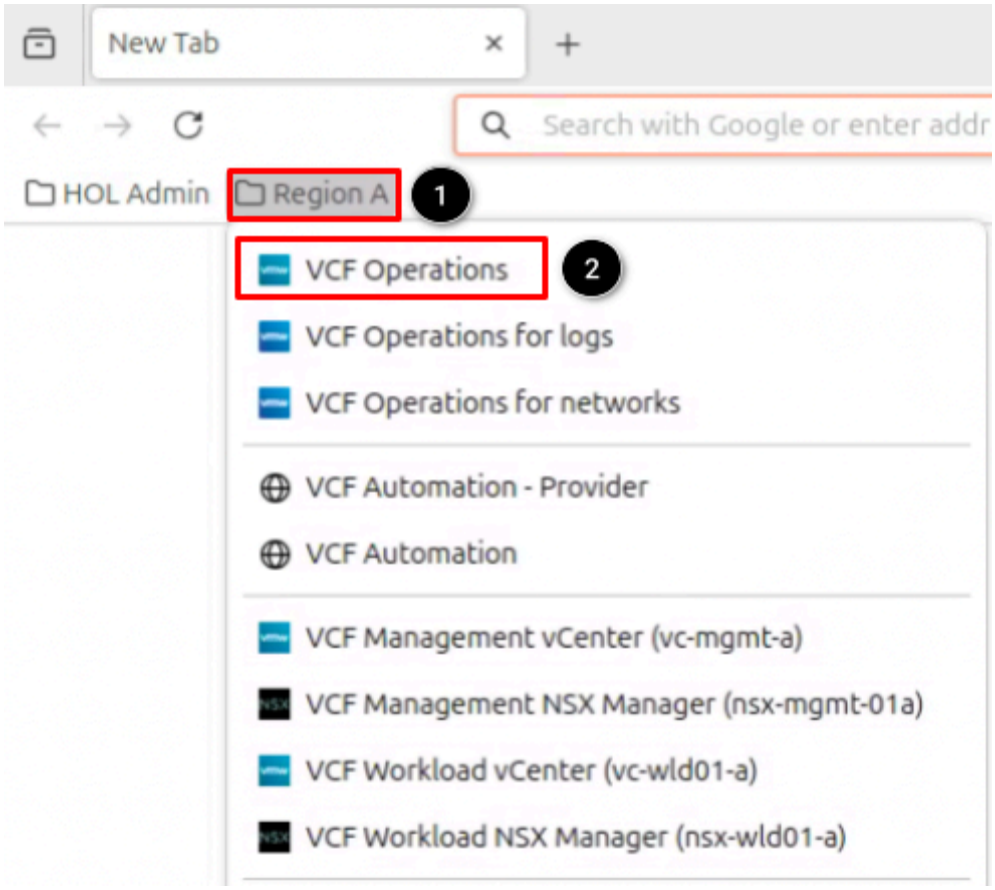
In the following few pages, we will walk through the process for logging in to VCF Operations.

Start Firefox

Open the Firefox Browser from the Linux Task Bar.

2. Click on the Firefox icon to open the browser.

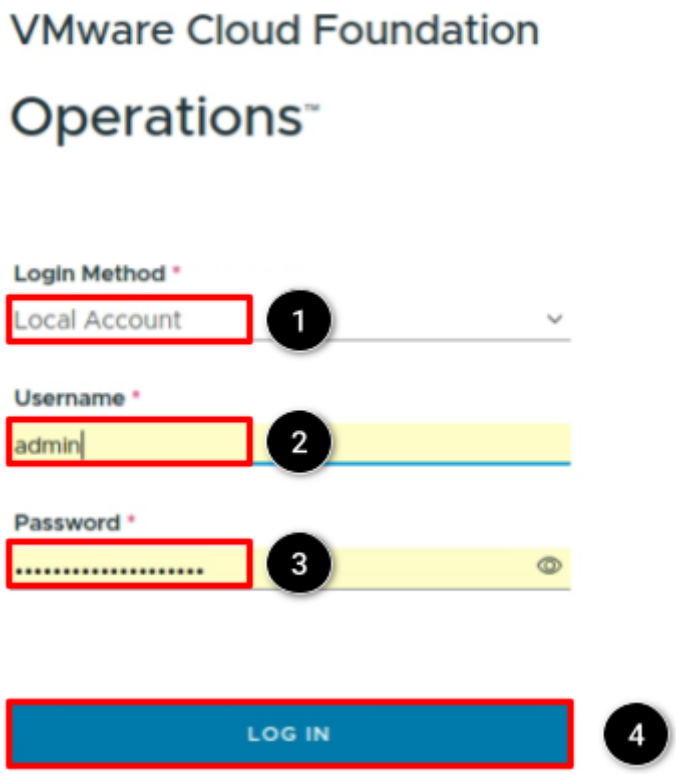
Open VCF Operations Console



Once Firefox has loaded:

3. Click on the **Region A** bookmark folder.
4. Click **VCF Operations**.

Login to VCF Operations Console



The credentials for **admin** should already be cached in the browser window.

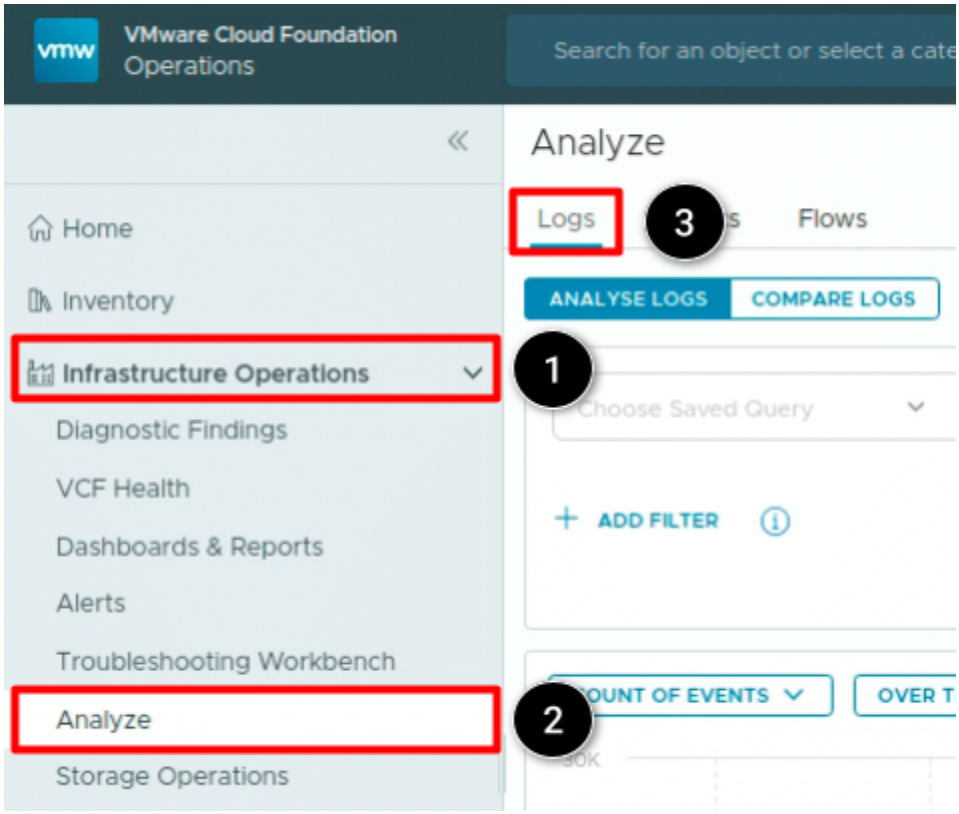
At the VCF Operations login prompt, select the login method and type in the following user and password information:

5. At the Login Method dropdown, select **Local Account**.
6. At the username field, type **admin**.
7. At the password field, type **VMware123!VMware123!**
8. Click **LOG IN**.

Viewing Logs, Queries and Fields

In this part of the module, we will show how the new Analyze Page for logs is working.

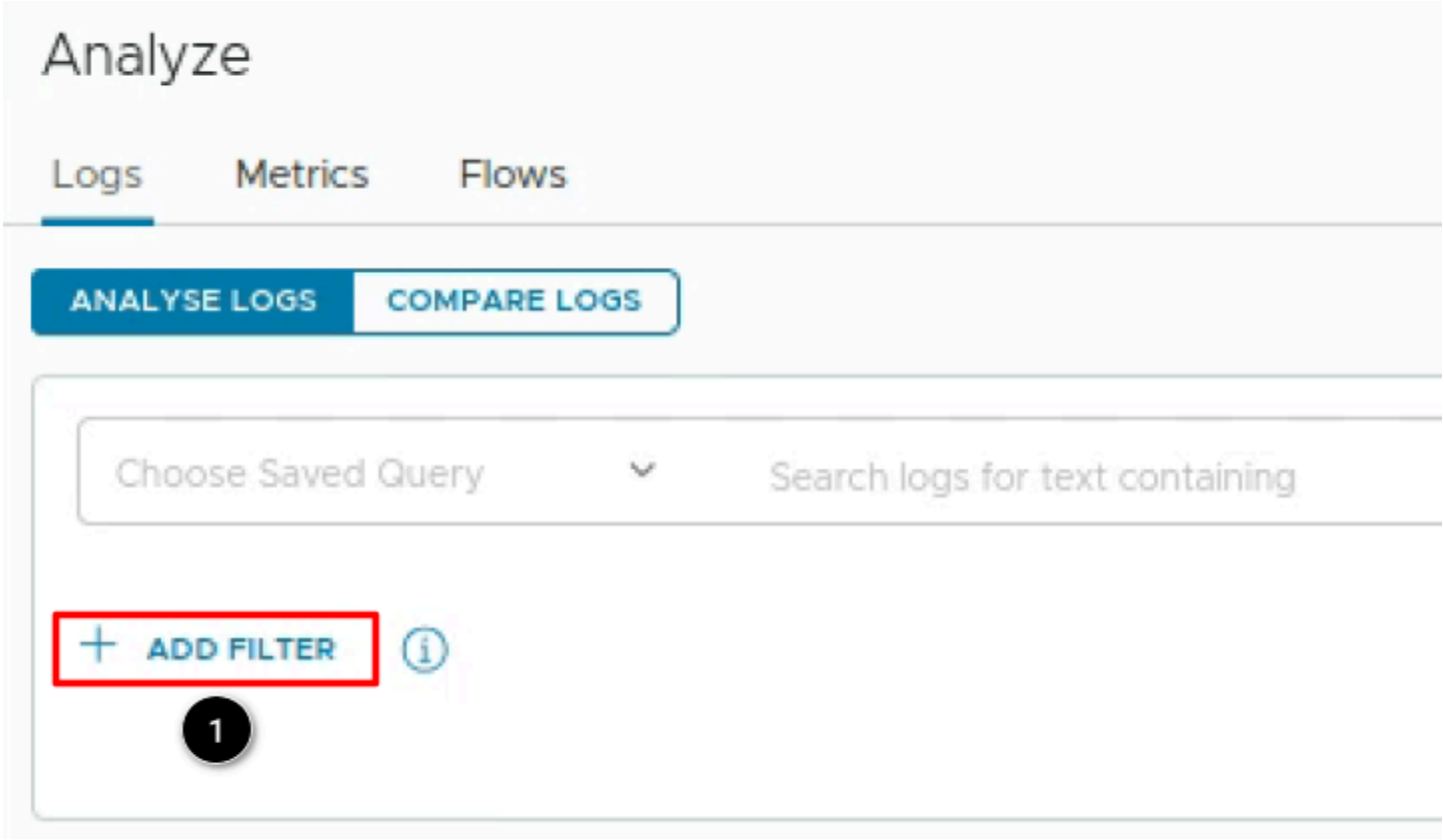
The Analyze Page



In the Logs tab of the Analyze page, we can search and filter log events, and create queries to extract events based on timestamp, text, source, and fields in log events. Besides presenting the log stream, VCF Operations presents charts of the query results.

1. From the left menu click **Infrastructure Operations**.
2. Select **Analyze**.
3. Click **Logs**.

Logs Filtering



1. Click **ADD FILTER** to start with filtering the logs.

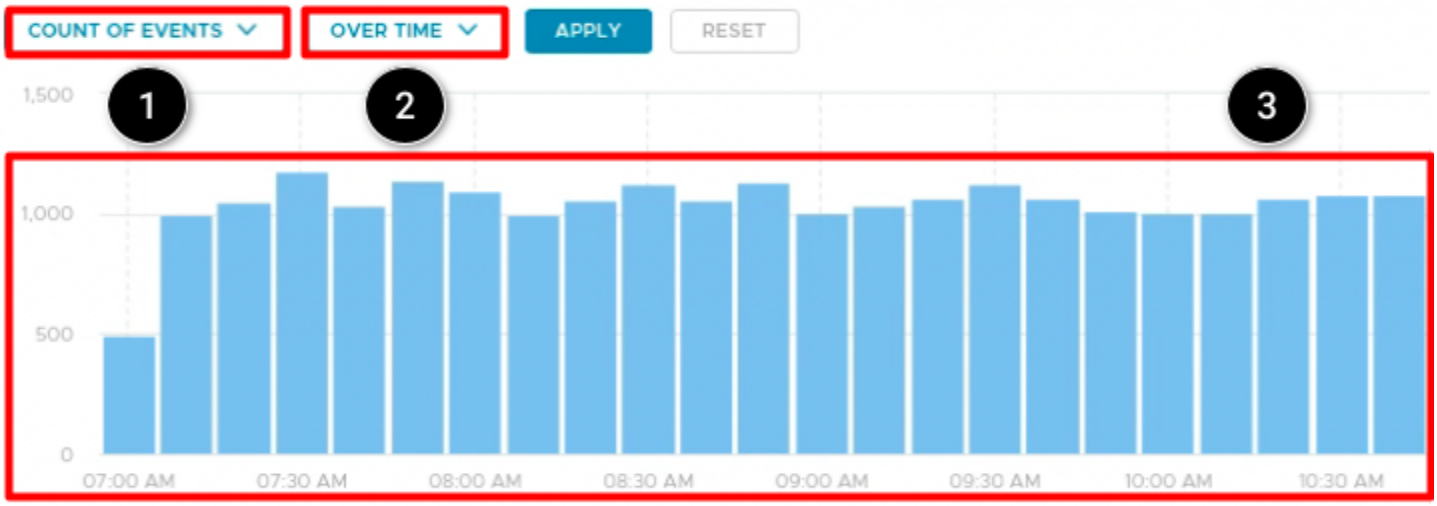
Create a Simple Log Filter

If you have previously used VCF Operations for Logs, the **Analyze - Logs** page will look familiar. In this exercise, we will create a basic log query that displays all logs containing the words "**error**" or "**failed**" in the log line, and where the hostname begins with "**esx**."

1. Define the first filter. Select "**text**" from the first drop-down, "**contains**" from the second drop-down and write **error**, press Enter, so that the first statement in the filter appears, write **failed** in the text field and press Enter again. Now we should see both expressions in the first filter.
2. Click **ADD FILTER**.

3. This will add a new filter with an AND clause, presented by the **All** selection. We do not change this setting, but we can see that there is also a Any option which is a logical OR.
4. Define the second filter. Select "**hostname**" from the first drop-down, "**Starts with**" from the second drop-down and write **esx** in the text field and press Enter.
5. Select **6h** as the timeline.
6. Click the **Search** icon.

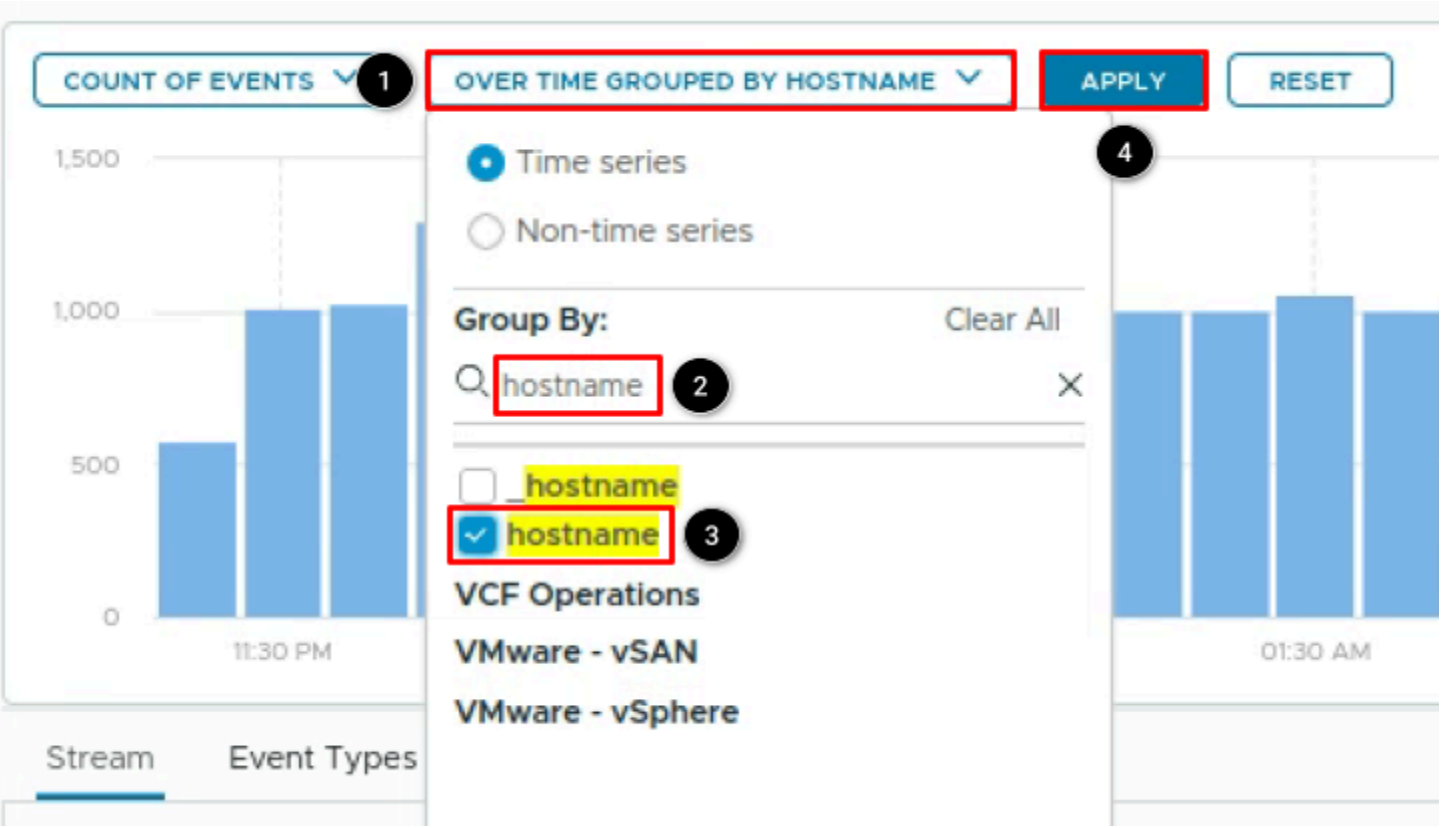
Log Filters Results



The result of the newly created filter should look similar to this.

1. Per default "**Count of Events**" is selected. This will count all findings based on the filter and display it as a column graphic.
2. Per default "**Over time**" is selected.
3. This is the actual result of the filter over 6 hours with a granularity of 10 minutes per column.

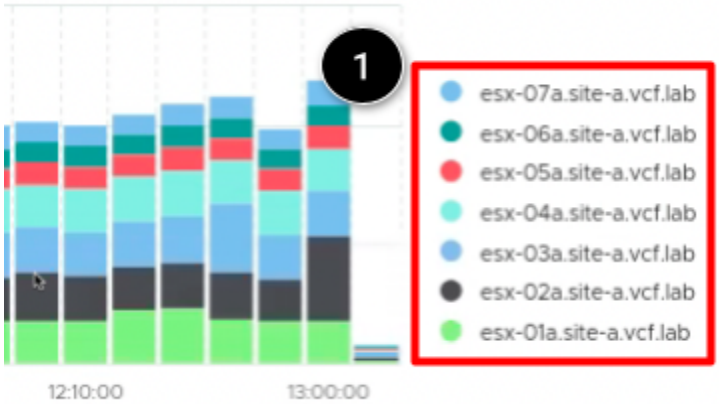
Tune Log Filter Output



To improve the graphical representation of the logs, adjust the log filter output to display the results per ESX host.

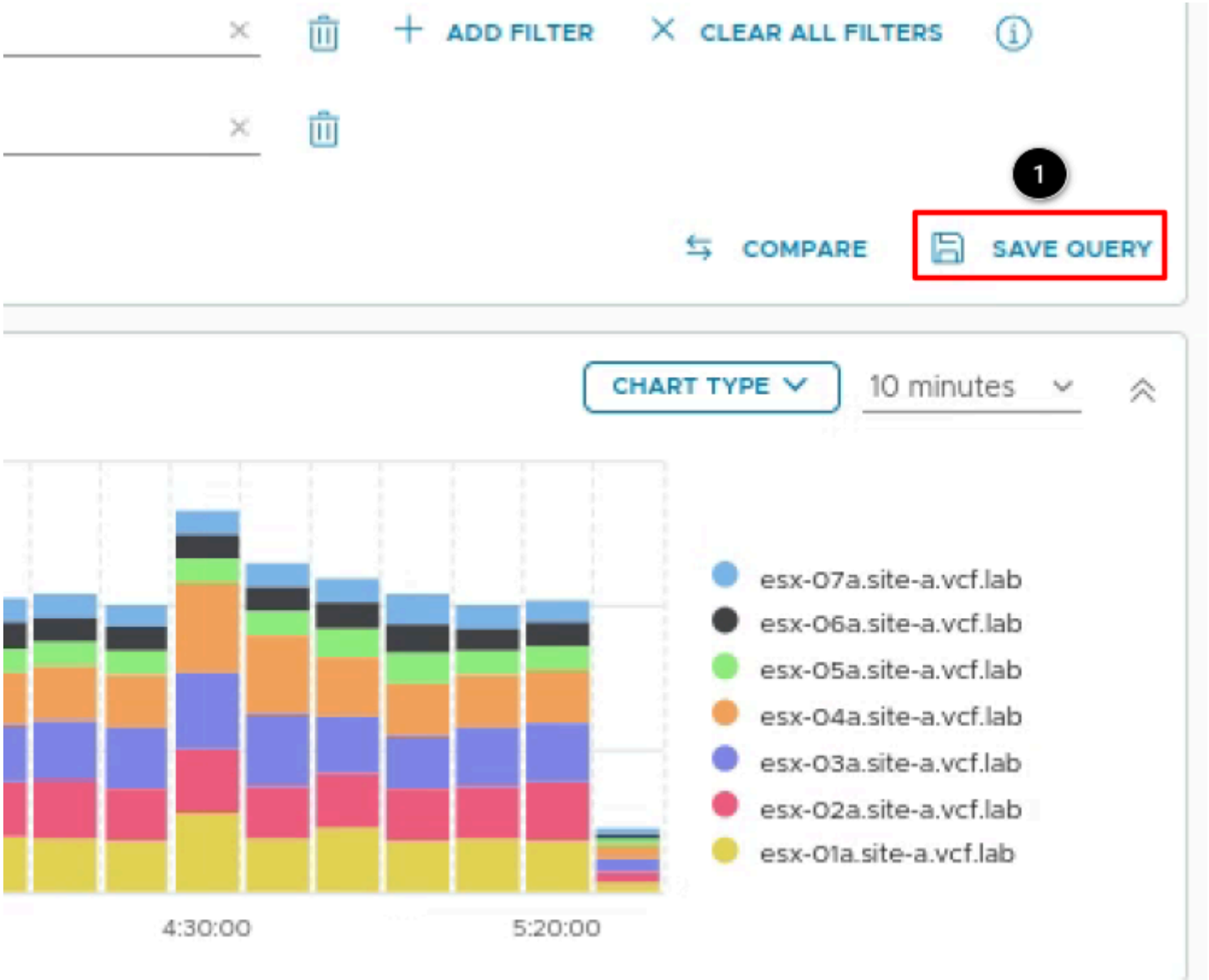
1. Click "**Over time**".
2. In the "**Group By**" search field enter **hostname**.
3. Check the box next to **hostname**.
4. Click **APPLY**.

Tuned Log Filter Results



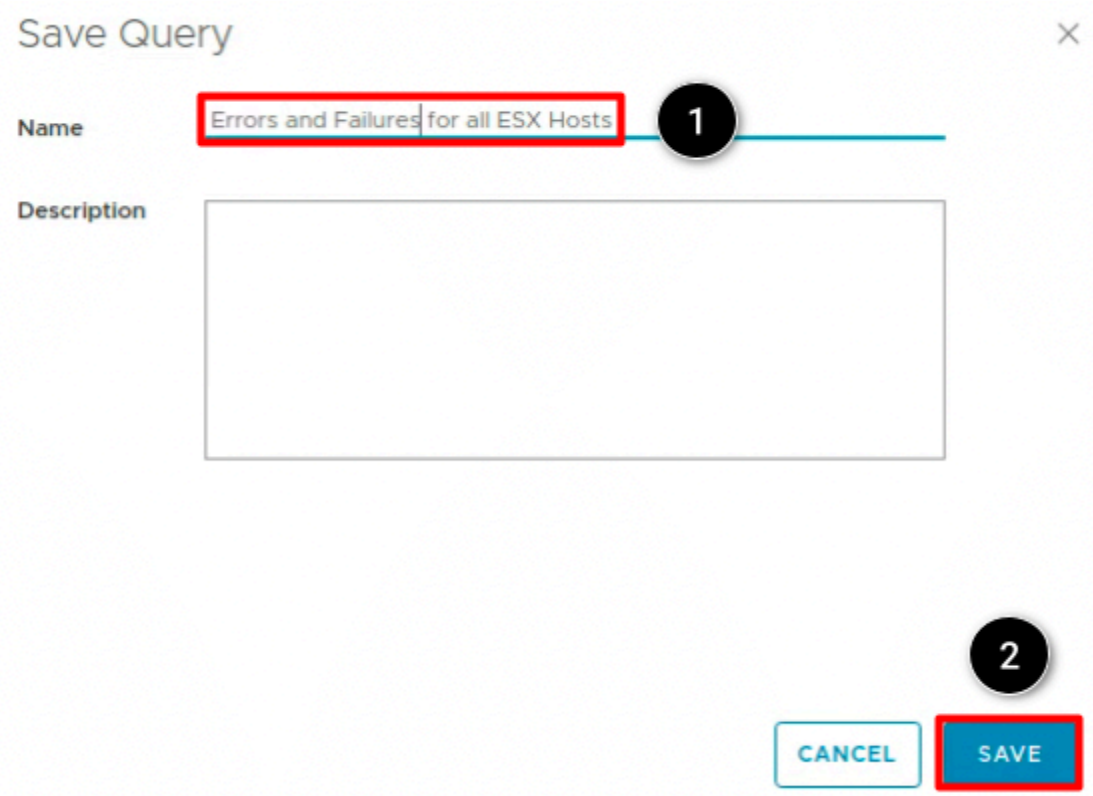
1. Instead of a column just showing aggregated events of logs we have now columns showing log events per ESX host. This can help to identify hosts that are generating a higher amount of logs maybe because of a problem.

Save the Log Query



1. Click on **SAVE QUERY**.

Save the Log Filter Query



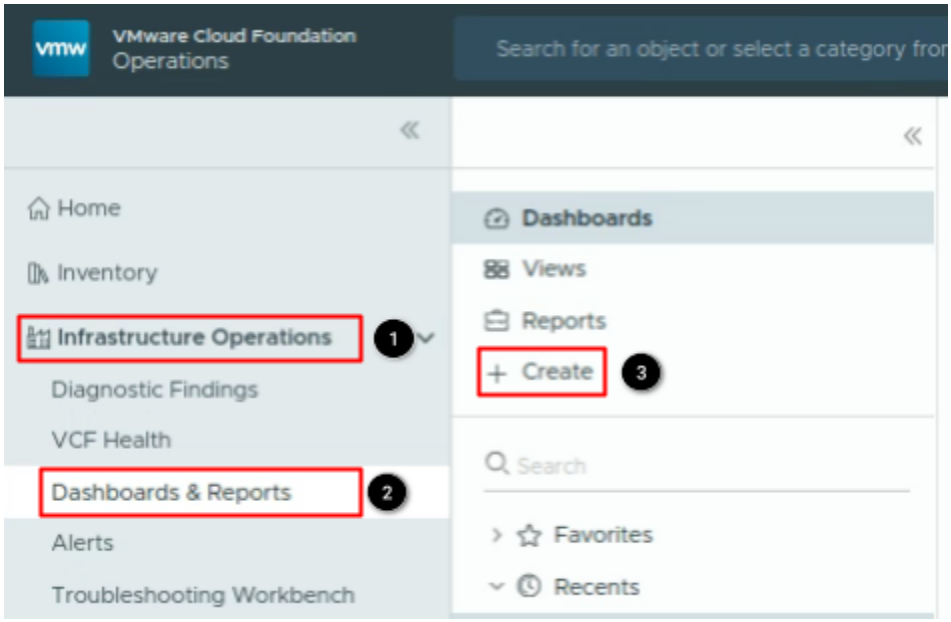
After completing your query, you can save it for future use, such as adding it to a dashboard.

1. Give the query a name: **Errors and Failures for all ESX hosts**
2. Click **SAVE**.

Build a Dashboard Using the Saved Log Filter

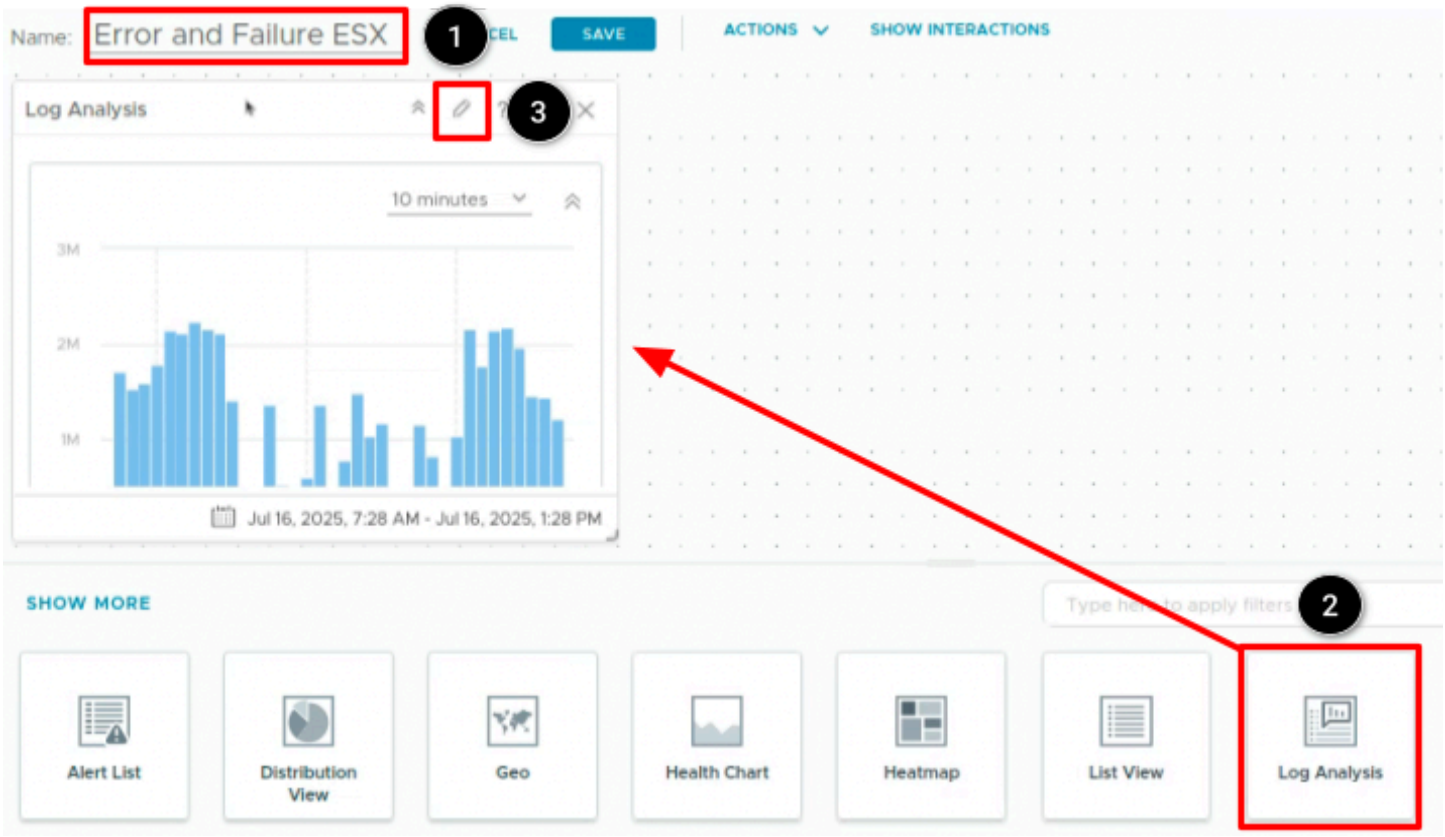
With targeted queries, admins quickly filter issues and spot trends. These saved queries power dashboards for real-time insights and faster troubleshooting. In VCF Operations 9.0 there are now VCF Operations for Logs dashboards integrated to have one console to see all important information.

Create a New Dashboard



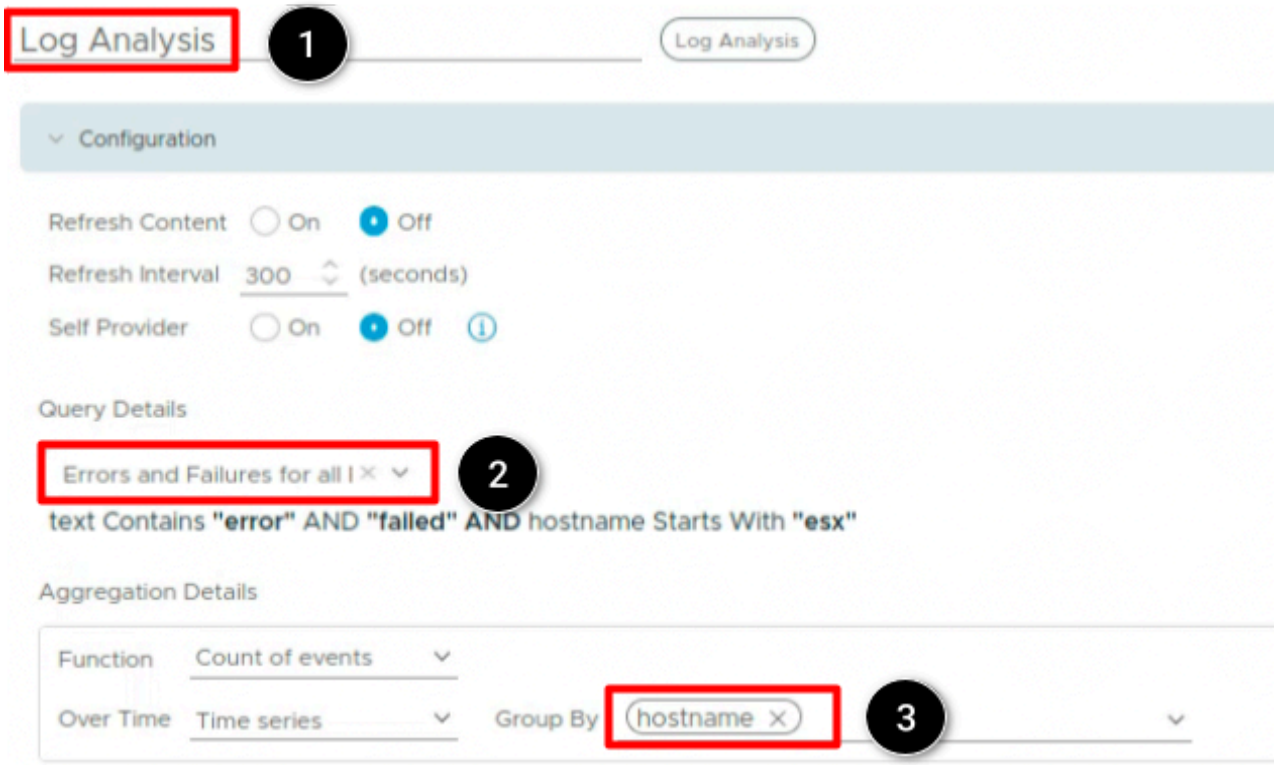
1. Click **Infrastructure Operations.**
2. Select **Dashboards & Reports**.
3. Click **Create**.

Add Log Analysis to the Dashboard



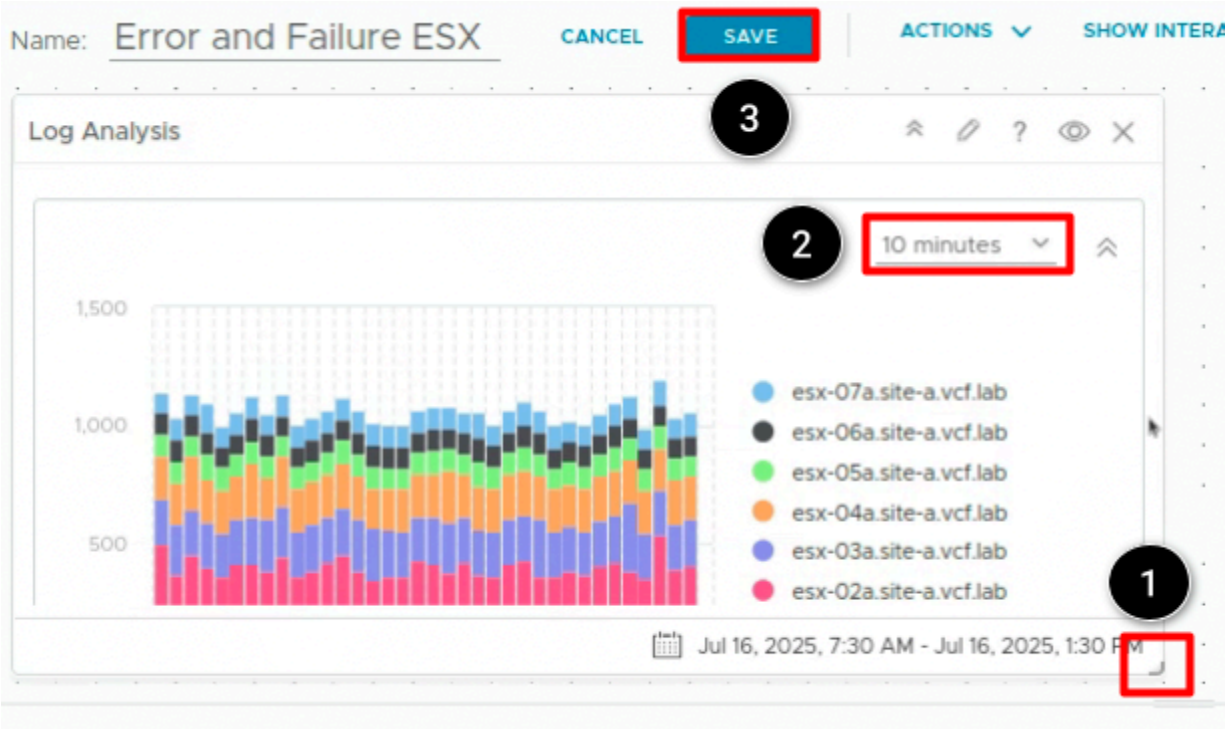
1. Give the new dashboard a name: **Error and Failure ESX**.
2. Drag and Drop the **Log Analysis** widget to a free dashboard area.
3. Hover with the mouse over the widget header and click the **pencil icon** to edit the widget.

Configure Log Analysis Widget



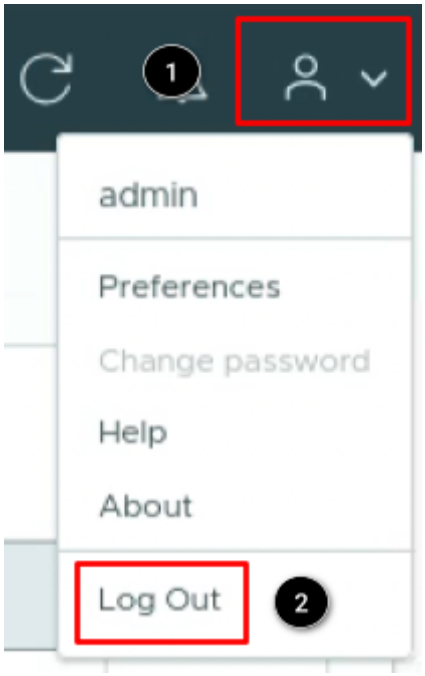
1. Give the widget a name. Here we will stay with the default name
2. In the query details dropdown select the saved query **Errors and Failures for all ESX hosts**.
3. In the "**Group By**" dropdown, select **hostname**.
4. (Not shown) Click **Save**.

Save the Dashboard



1. Use the mouse to scale the widget to the required size (simply click and drag it).
2. There are two time intervals we can select. Either **10 minutes** or **1 hour**. Depending on the interval we will see less or more columns. Select **10 minutes**.
3. Click **Save**.

Logout



To Log out of VCF Operations:

1. Click the **User icon** to open the settings menu.
2. Click **Log Out**.

Conclusion

This module offers a solid foundation for exploring, analyzing, and creating log dashboards within VCF Operations. It showcases how VCF Operations 9.0's new log standard and centralized collection architecture streamline log analysis. You have learned the steps for creating, tuning, and saving log filters, followed by the creation of a new dashboard.

From here you can:

- Take this quick survey to provide feedback about your experience with VCF 9.0
- Continue with the next lab module.
- Click [vlp:table-of-contents|Show Table of Contents] to jump to any module or lesson in this lab.
- End your lab and return in the future.

Module 3 - Explore and Analyze Object Metrics in VCF Operations (30 minutes) Intermediate

VMware Cloud Foundation Operations 9.0 provides an integrated user experience for search queries which will run across your entire deployment and find all types of objects based on the specified search terms used in a search query.

You can create a simple search query starting with a metric, property, or object type, or you can build a more complex query using different conditions to find all types of entities in VCF Operations.

Login to VCF Operations

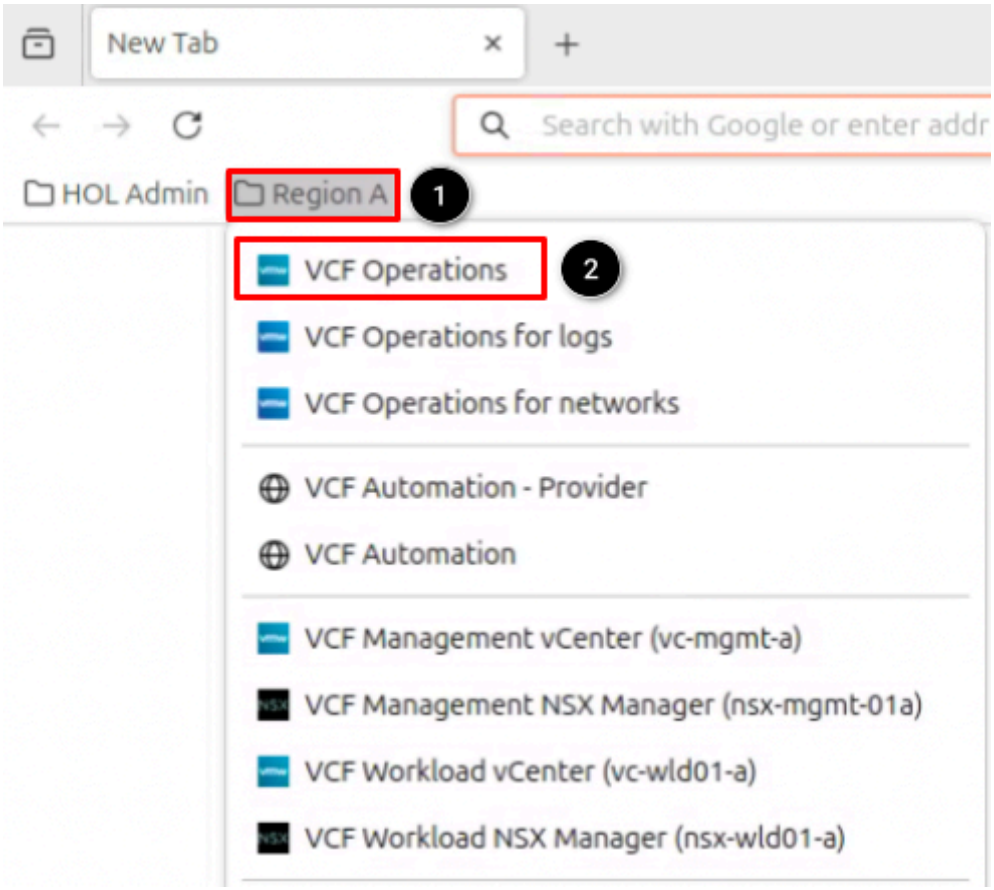
In the following few pages, we will walk through the process for logging in to VCF Operations.

Start Firefox

Open the Firefox Browser from the Linux Task Bar.

1. Click on the Firefox icon to open the browser.

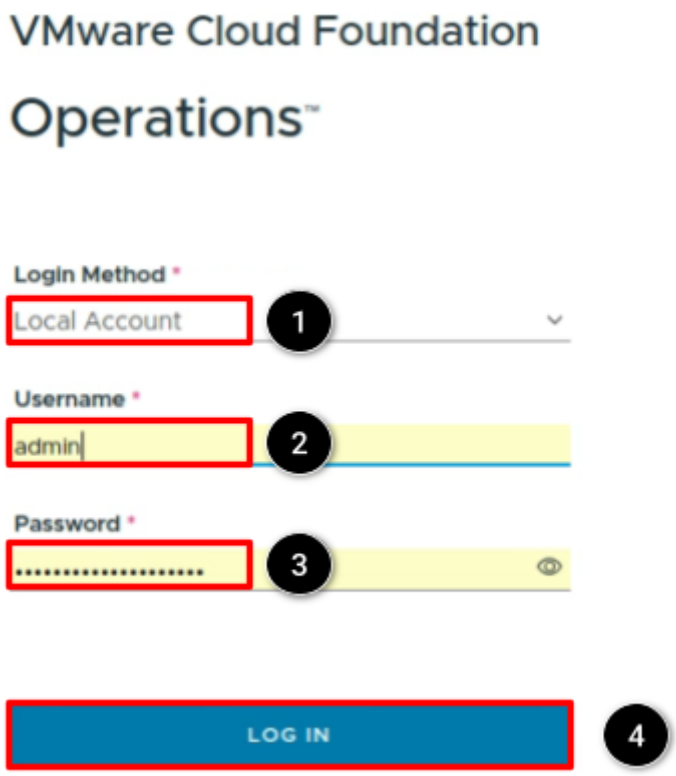
Open VCF Operations Console



Once Firefox has loaded:

1. Click on the **Region A** bookmark folder.
2. Click **VCF Operations**.

Login to VCF Operations Console



The credentials for **admin** should already be cached in the browser window.

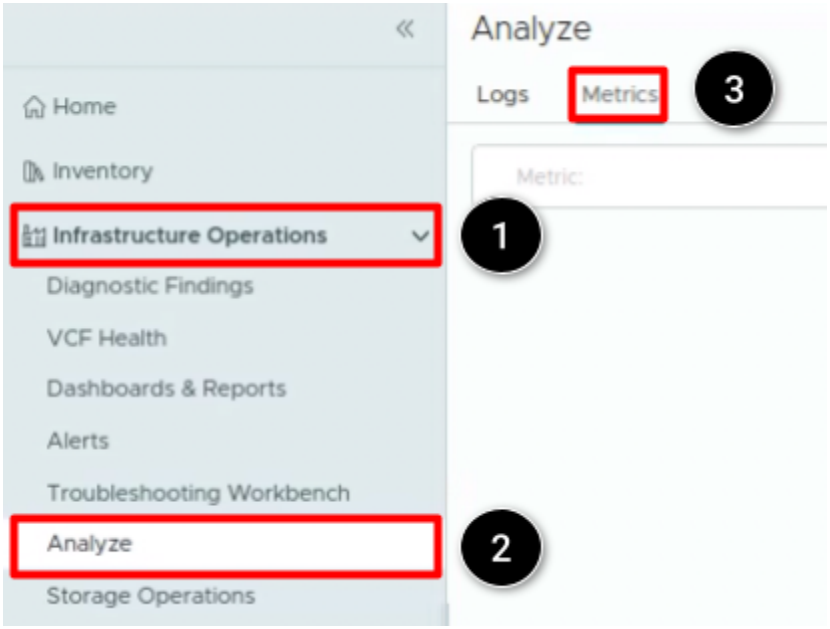
At the VCF Operations login prompt, select the login method and type in the following user and password information:

1. At the Login Method dropdown, select **Local Account**.
2. At the username field, type **admin**.
3. At the password field, type **VMware123!VMware123!**
4. Click **LOG IN**.

Create queries based on Objects, metrics and properties

In this part of the module, we will show how to utilize the new Analyze Page for metrics.

The Analyze Page



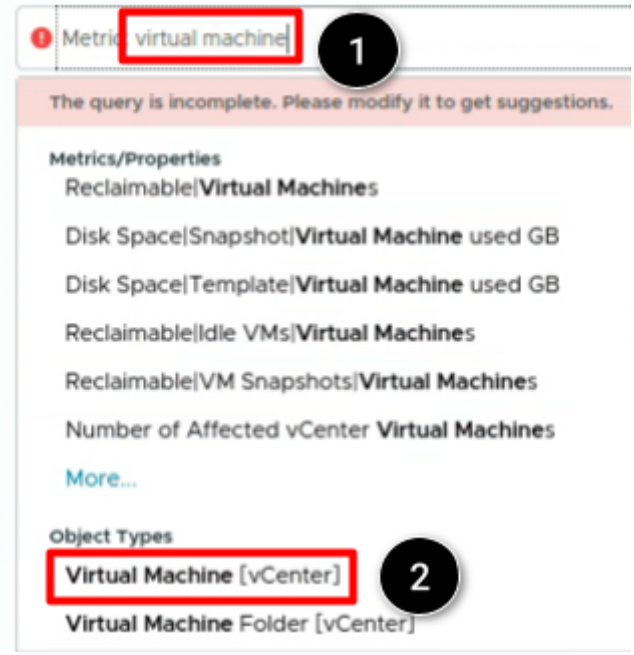
In the Metrics tab of the Analyze page, you can create queries to display, for example, all VMs with storage latency higher than 5ms. These query results can then be used for more detailed analysis or open one of these results in the Troubleshooting Workbench.

1. From the left menu click **Infrastructure Operations**.
2. Select **Analyze**.
3. Click **Metrics**.

Create a Simple Query

For our first query we will start easy. In the query we will search for every Virtual Machine that has **CPU usage (%) higher** than **15%**.

Select Object Type



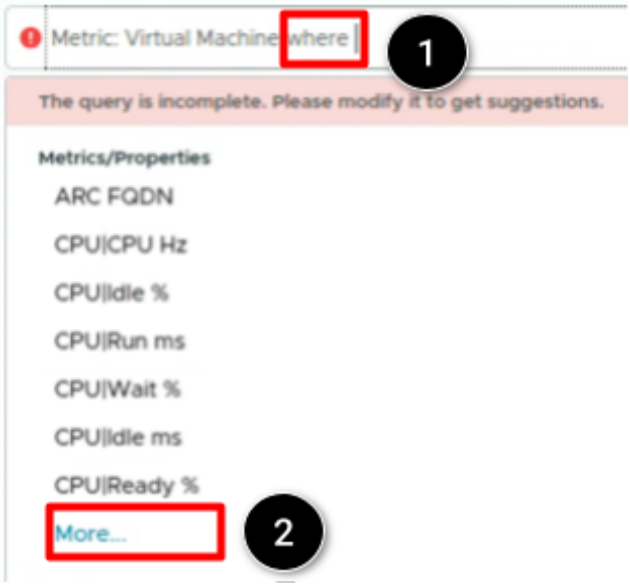
We now have 2 possibilities on how to create our simple query.

- Copy the following text and paste it in the search bar: **Virtual Machine where CPU|Usage % > 15 %**
- Click through the interactive search bar.

When we click the cursor in the search bar, a list of suggestions with the metric and property names and the object types appear. We can select a metric, property, or object type from this list. If we hover over the metric and property names we can view the name of the object types that the metric or property belongs to.

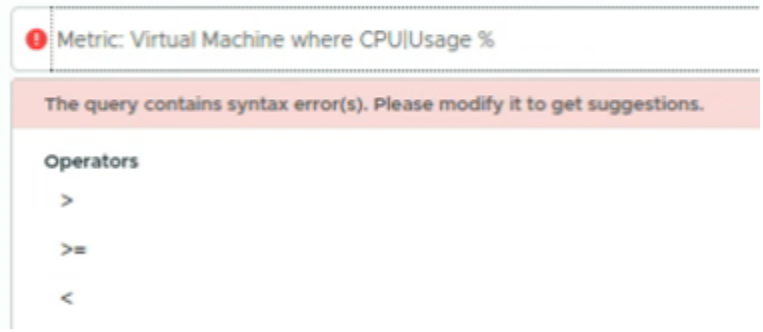
1. Enter **Virtual Machine** in the search bar.
2. Scroll down the list until you see **Virtual Machine [vCenter]** and click it.

Select Object Metric



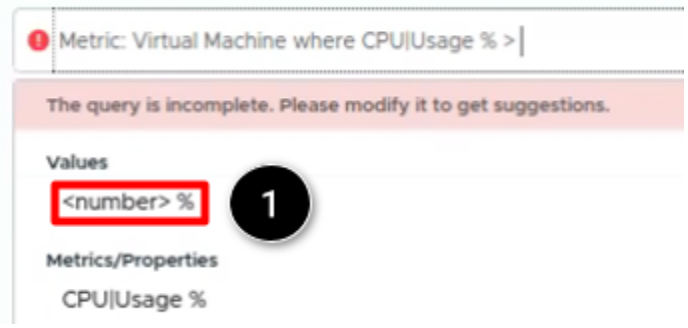
1. A "**where**" operator will be automatically appended to the Virtual Machine object.
2. Click "**More…**" to see additional metrics.
3. (**not shown**) Select **CPU|Usage %** to add it to the query.

Select Operator



1. Select the **">" (greater than sign)** as we want to have all VM greater than 15%.

Select value



1. Select **<number> %**. This will put a % sign at the end of the query and the cursor before it.

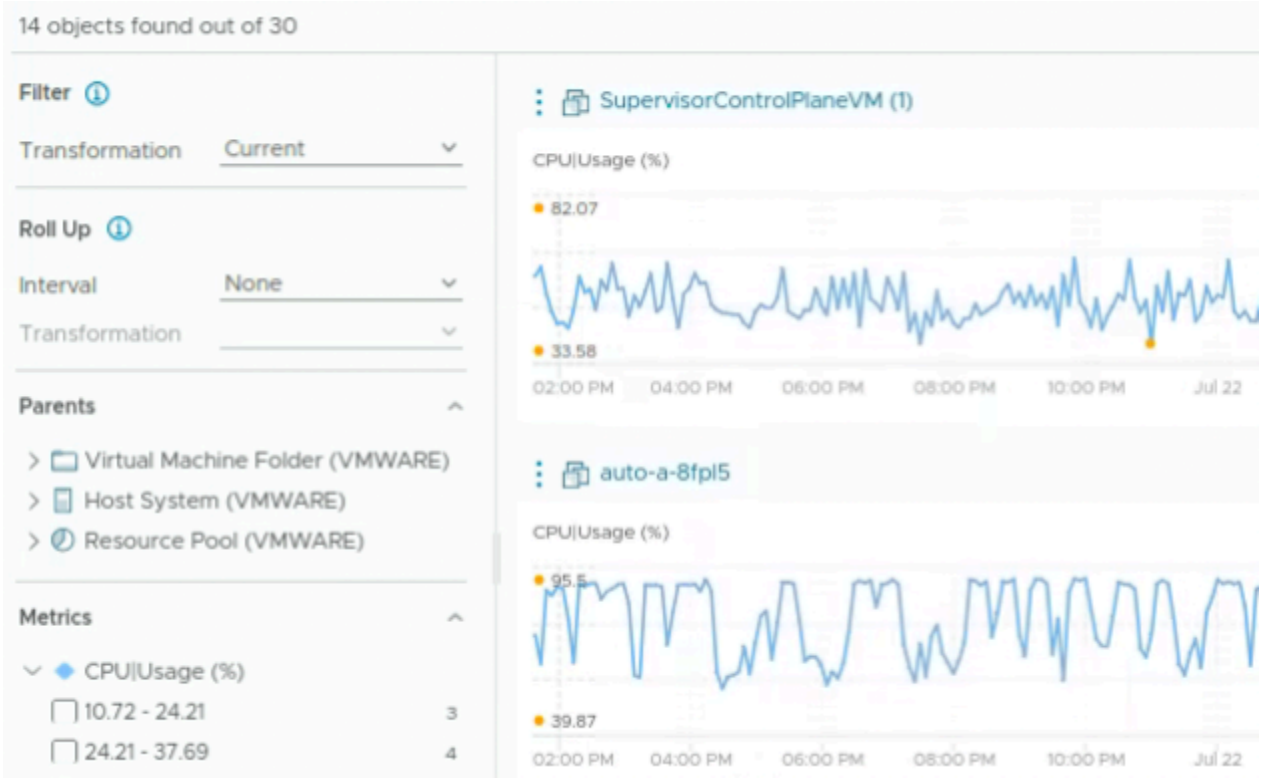
Enter the Value

1. Enter **15** as the value.
2. The red info bar should now change to a green info bar. This means the query is now complete.

Search the Query

1. Click the **magnifier icon** at the end of the search bar or **hit enter** to see the query results.

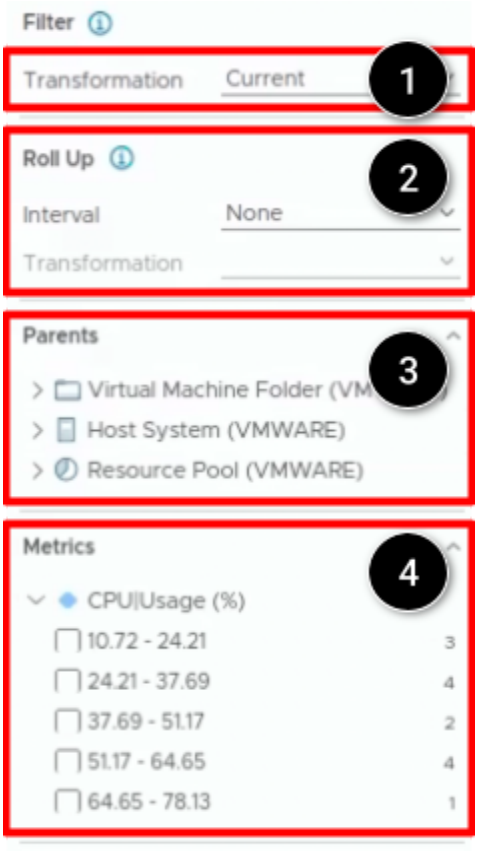
Simple Query Result



If the query is correct and we have Virtual Machines with CPU usage % of greater than 15 you should now see all of the VMs with this criteria. Note that the screenshot may differ from what we see in the HOL.

On rare occasions it can be that no VM is showing up in the results. If this happens please lower the value from 15% to 10% or even lower. This can happen from time to time depending on how busy the lab is.

Filter Explanation



Within the query results we also have additional filters we can use to further drill down what we really want to see.

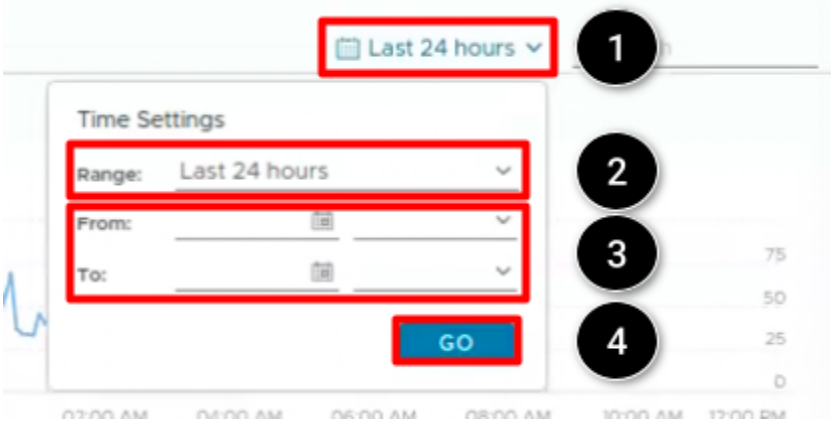
1. **Transformation:** The Transformation filter applies to the actual query and not the results as it applies to objects before the search query runs and cannot be used on the results. By default **Current** is the transformation. Other transformations are maximum, minimum, average, sum, first, last.

   Minimum. The minimum value of the metric over the selected time range.
   Maximum. The maximum value of the metric over the selected time range.
   Average. The mean of all the metric values over the selected time range.
   Sum. The sum of the metric values over the selected time range.
   First. The first metric value for the selected time range.
   Last. The last value of a metric within the selected time range.
   Current. The last available value of a metric if it was last updated not before five collection cycles were complete, otherwise, it is null.

2. **Roll Up:** The roll up filter is used to change data visualization based on the selected time interval and transformation. You can select one of the available options ranging from hour, day, week, month, quarter, or year. For example, if you select Hour as the interval and the Maximum as the transformation, then the system displays maximum values for each one-hour interval.

3. **Parents:** The parent objects grouped by type for the found objects that the metrics in the query belong to. You can use this option to further narrow down the results.
4. **Metrics:** Displays the metrics value distribution. The metric values are divided into 5 ranges and the number of objects which have the metric lying in that range is available.

Time Settings

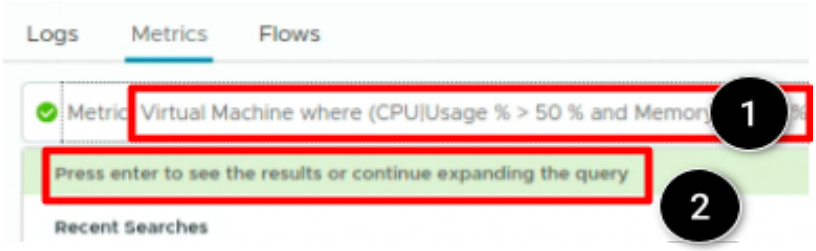


1. By default, all queries display data from the last 24 hours. To modify this, click on "Last 24 hours" to open the time settings menu.
2. **Range:** A variety of time ranges are available, such as the "**Last 1, 6, 12, or 24 hours**", as well as the "**Last 7 or 30 days**".
3. **Custom:** If none of the predefined ranges suit our needs, we can manually select specific dates and times instead.
4. Click **GO**.

Create a Complex Query

After we have created our first simple query it is time to start with a more complex query. In this query we will search for every Virtual Machine that has **CPU usage (%) higher** than **50%** and **Memory usage (%) higher** than **50%** and the **OS Name contains "Ubuntu"** in its name.

Copy and Paste the Complex Query



We now have again 2 possibilities on how to create our simple query.

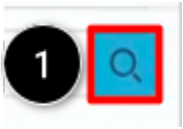
- Copy the following text and paste it in the search bar: **Virtual Machine where (CPU|Usage % > 15 % and Memory|Usage % > 15) and Summary|Guest Operating System|Guest OS from Tools contains 'Ubuntu'**
- Click through the interactive search bar.

For this query we go ahead and copy the mentioned text above and paste it into the search bar.

If you are using multiple metrics in one query be aware to set the parentheses correctly. Otherwise your query will give you different results.

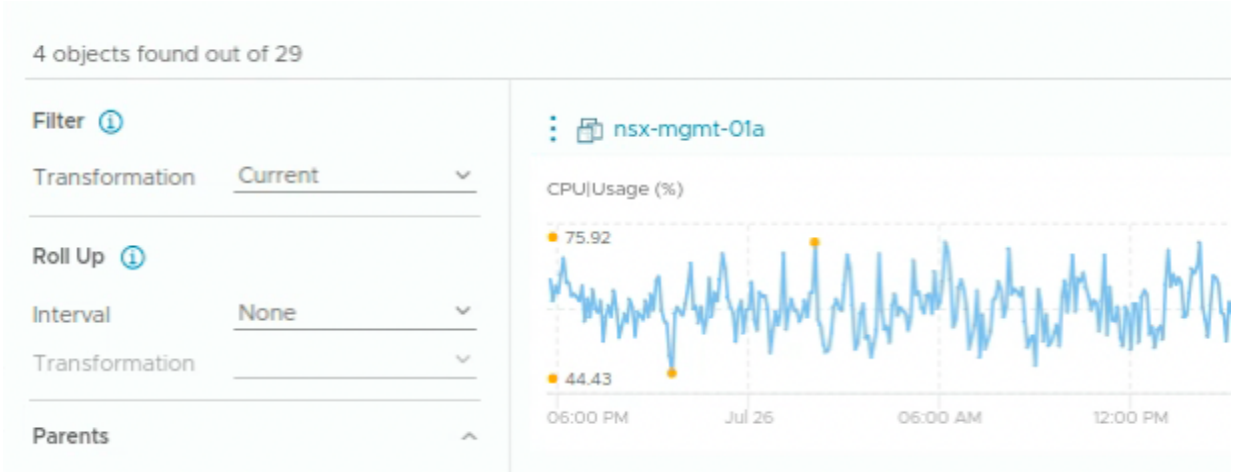
1. Copy **Virtual Machine where (CPU|Usage % > 15 % and Memory|Usage % > 15) and Summary|Guest Operating System|Guest OS from Tools contains 'Ubuntu'** and paste it into the search bar.
2. The info bar will show green when the query is correct.

Search the Query



1. Click the **magnifier icon** at the end of the search bar or **hit enter** to see the query results.

Complex Query Result



If the query is correct and we have Virtual Machines with all the requirements, you should now see all of the VMs with this criteria.

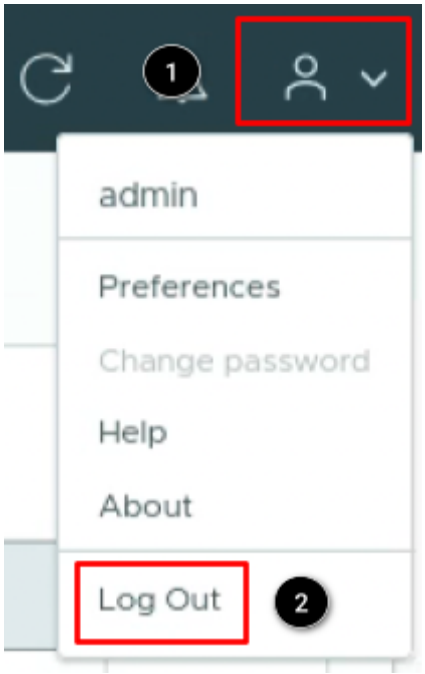
On rare occasions it can be that no VM is showing up in the results. If this happens please lower the value from 15% to 10% or even lower. This can happen from time to time depending on how busy the lab is.

Open Troubleshooting Workbench

1. Click the **three dots** next to the object you want to open the Troubleshooting Workbench.
2. Click **Troubleshoot**.

This will then redirect you to the **Troubleshooting Workbench**. How to use the Troubleshooting Workbench will be explained in LAB **VMware Cloud Foundation 9.0 - Operations: Troubleshooting the Private Cloud** (**HOL-2601-04-VCF-L**) - **Module 1** Introduction to the Troubleshooting Workbench.

Logout



To Log out of VCF Operations:

1. Click the **User icon** to open the settings menu.
2. Click **Log Out**.

Conclusion

Building queries to drill down into an existing problem is key when troubleshooting the full VCF stack. With the new **Analyze section** it is now easier to find this functionality. As we saw we can build all kinds of queries and only your imagination is the limit.

From here you can:

- Take this quick survey to provide feedback about your experience with VCF 9.0
- Continue with the next lab module.
- Click [vlp:table-of-contents|Show Table of Contents] to jump to any module or lesson in this lab.
- End your lab and return in the future.

Module 4 - Explore and Analyze Specific Flows in VCF Operations (30 min) Intermediate

Exploring and analyzing network flows provides rich context and information for modern private cloud administrators when working to troubleshoot performance, security and application problems. Normally a black box that requires the deployment of network taps and

extensive third party involvement, VMware vCloud Foundation Operations together with Network Operations provides a wealth of information and insight for administrators.

Let's take a look.

Login to VCF Operations

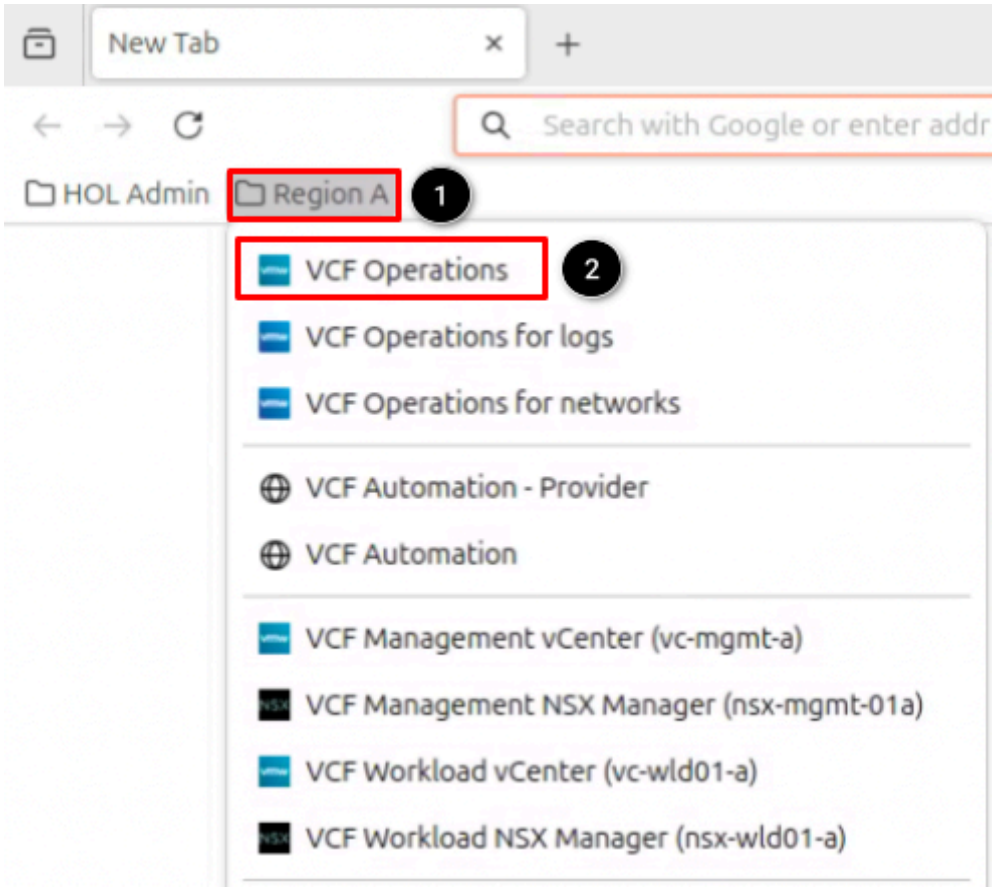
In the following few pages, we will walk through the process for logging in to VCF Operations.

Start Firefox

Open the Firefox Browser from the Linux Task Bar.

1. Click on the Firefox icon to open the browser.

Open VCF Operations Console

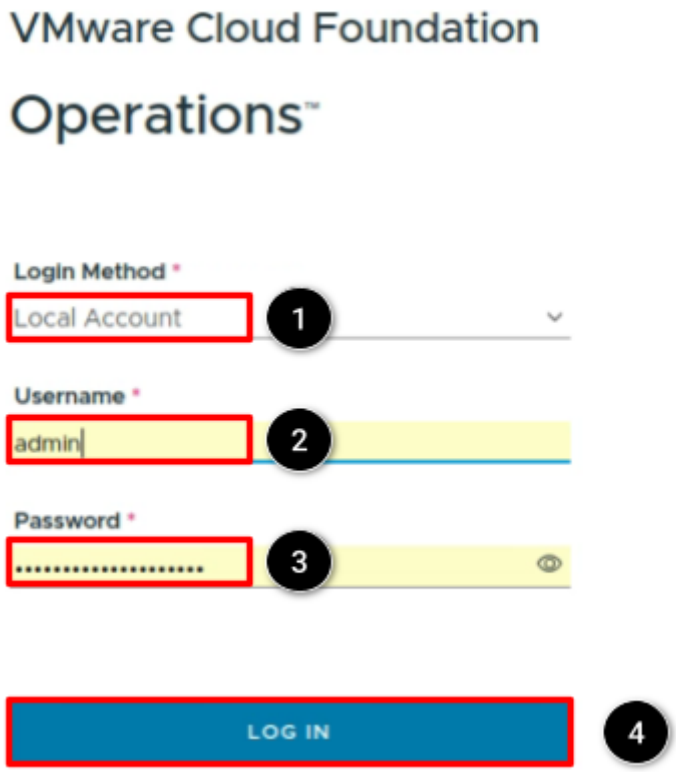


Once Firefox has loaded:

1. Click on the **Region A** bookmark folder.

2. Click **VCF Operations**.

Login to VCF Operations Console

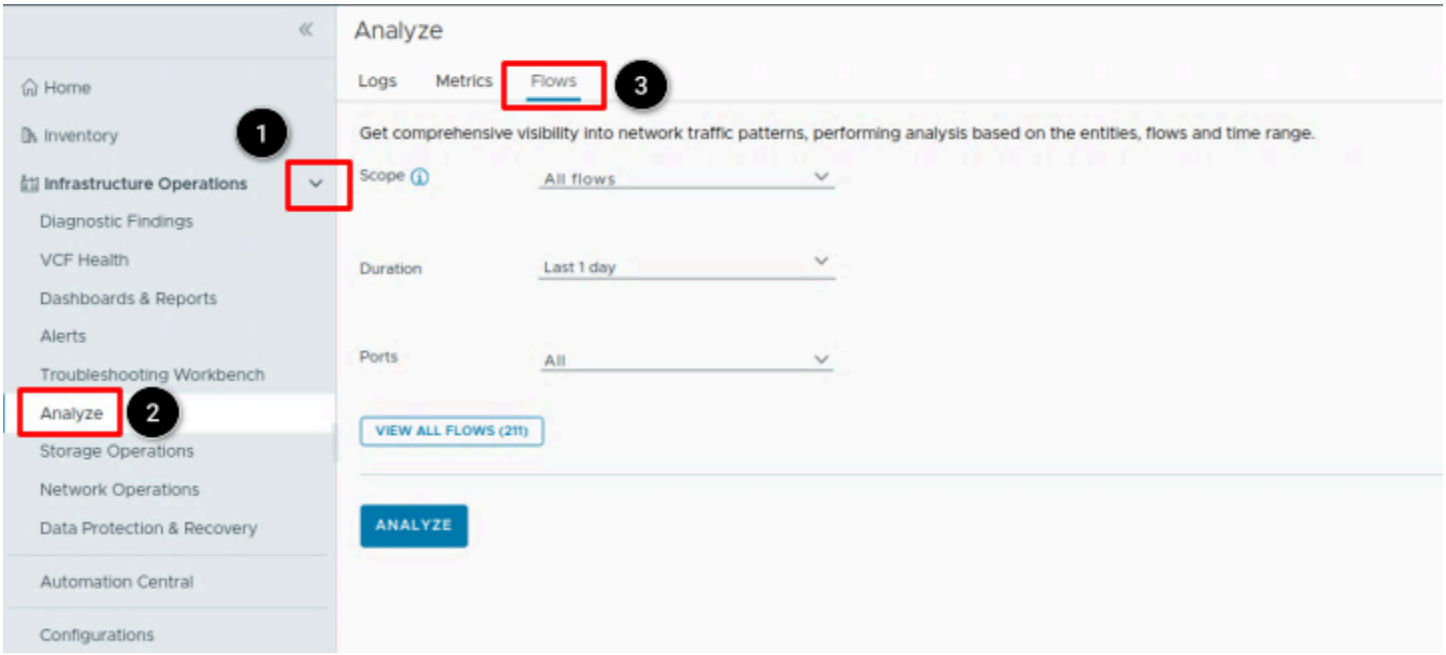


The credentials for **admin** should already be cached in the browser window.

At the VCF Operations login prompt, select the login method and type in the following user and password information:

1. At the Login Method dropdown, select **Local Account**.
2. At the username field, type **admin**.
3. At the password field, type **VMware123!VMware123!**
4. Click **LOG IN**.

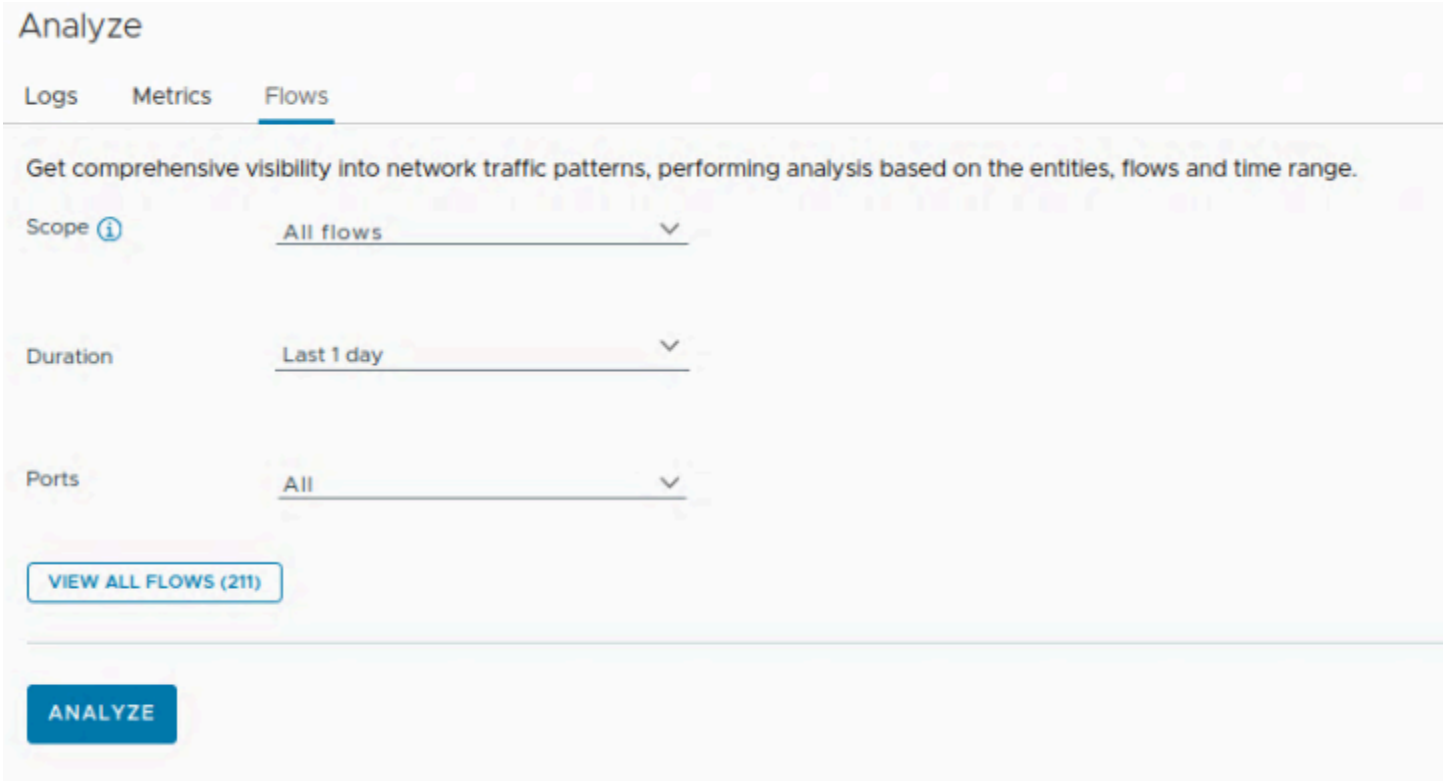
Navigate to Flow Analysis



VMware Cloud Foundation Operations contains many new features that assist administrators in their management and deployment of modern private cloud environments. One of these new features is the Analyze function within Infrastructure Operations. This new offering focuses on 3 main pillars, Logs, Metrics and Flows. Each of these pillars is built on what were previously separate products in the VMware portfolio, Aria Operations for Logs, Aria Operations and Aria Operations for Networks. We'll take a look at the experience for Network Flows in this module, Logs and Metrics are covered in other modules.

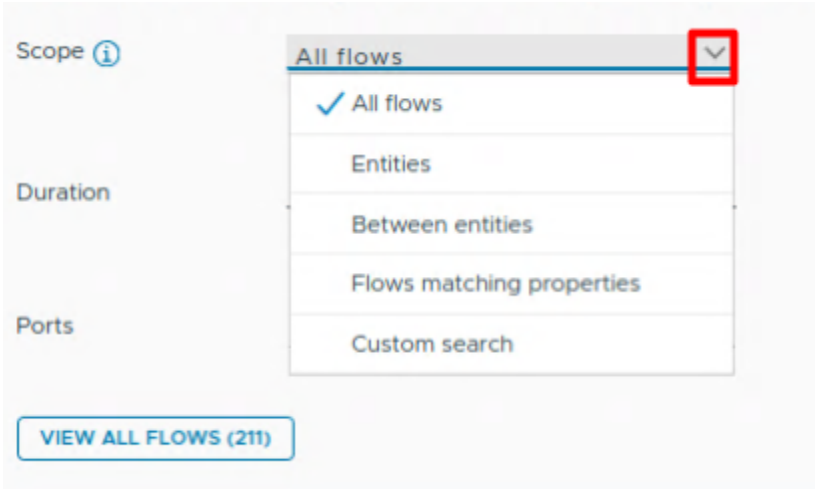
1. Locate **Infrastructure Operations** and **Click** the **Carrot** to expand the menu.
2. **Click** on **Analyze**.
3. **Click** on **Flows**.

Filtering Flows for Analysis



The first step in any analysis is to define the scope you wish to examine. Network Operations allows a user to specify the flow type, duration and ports. Once a user has defined these variables, they are able to view the flows that match the supplied criteria. Let's take a look at the options.

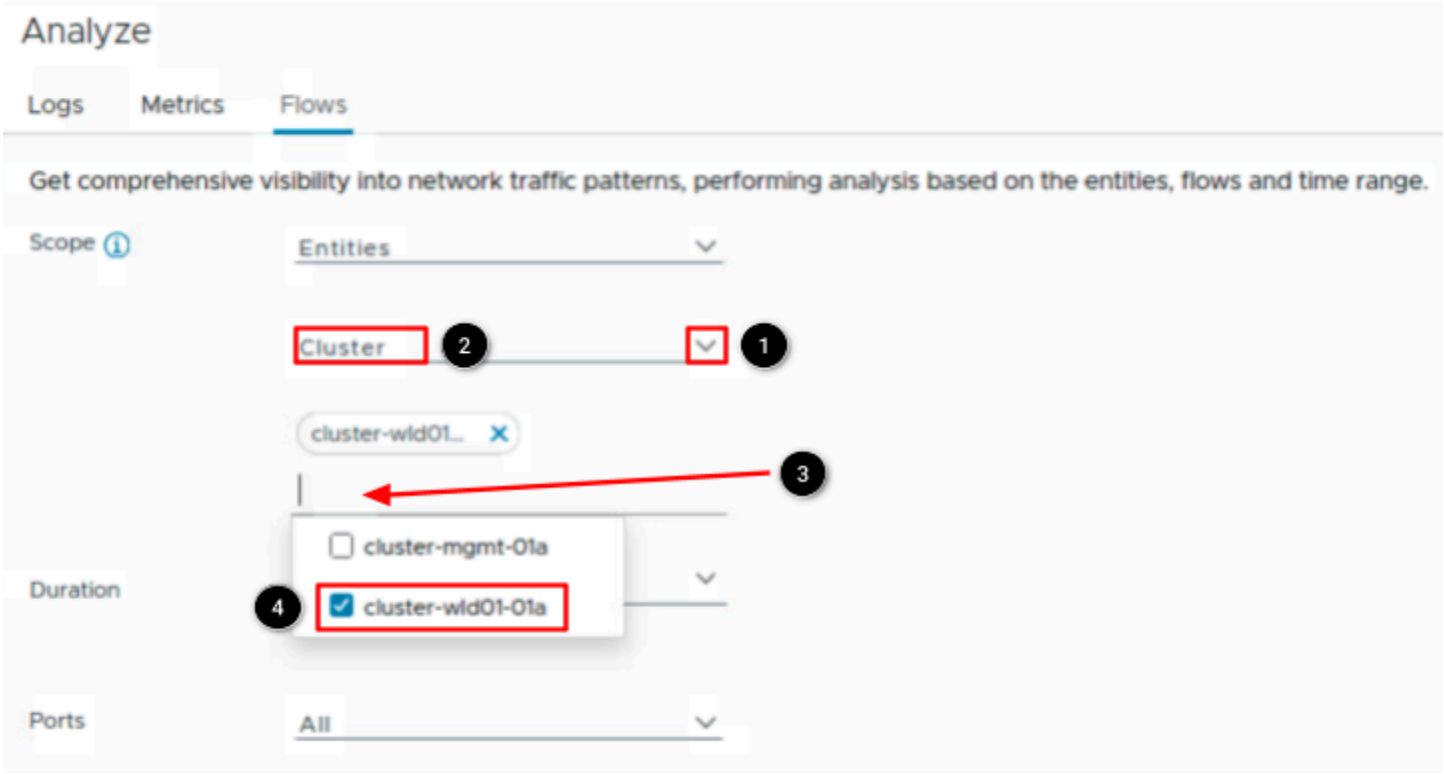
Filtering Scope for Analysis - All Flows



Network Operations presents multiple filtering options for users to choose from when defining the scope for analysis. The default option is to select All Flows, so there is nothing more to explore with this option, but others provide more capabilities. Let's take a look.

1. **Click** the **down carrot** to expand the dropdown menu.
2. Select **Entities**.

Filtering Scope for Analysis - Entities



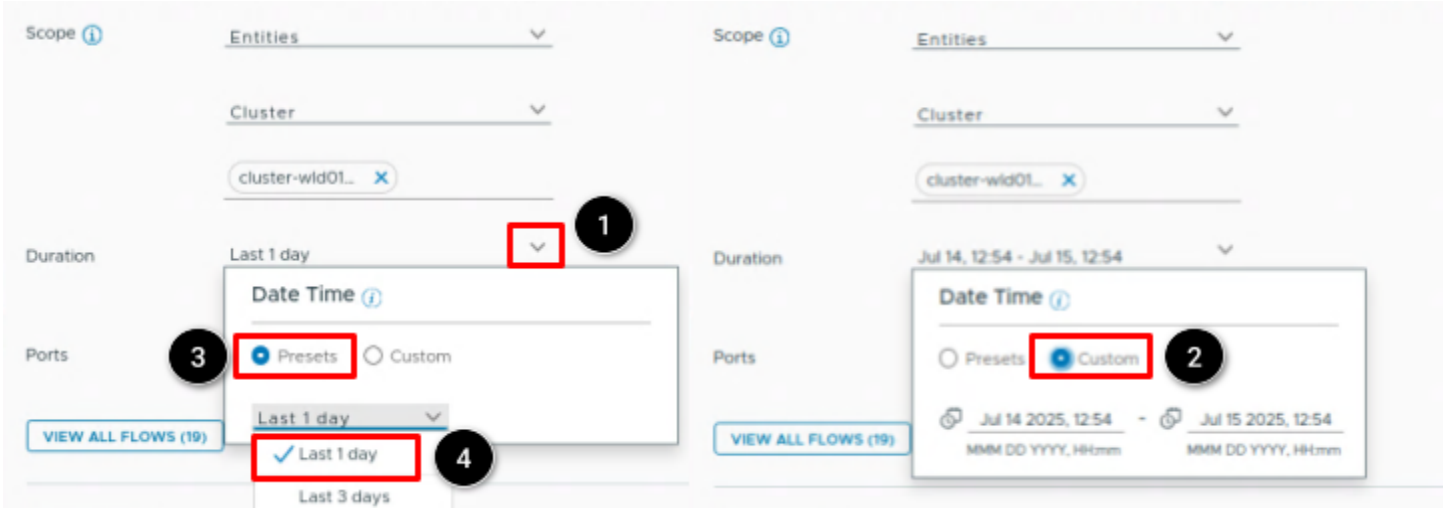
VMware Cloud Foundation Operations for Networks provides multiple logical grouping options for administrators to pick from. These include:

- **Application** - A grouping of Virtual Machines into discrete applications in Network Operations
- **Cluster** - A vSphere Cluster
- **Datacenter** - A vSphere Datacenter
- **Folder** - A vCenter folder containing Virtual Machines
- **Resource Pool** - A resource Pool containing vCenter resources
- **Security Group** - A NSX Group consisting of objects tagged with NSX Security Tags or manually defined
- **Security Tag** - A group of objects tagged with NSX Security Tags
- **Tier** - A grouping of Applications, Virtual Machines or other objects within Network Operations

For this example, let's select Cluster.

1. **Click** the **down carrot** to expand the Entities list.
2. **Click** on and select **Cluster**.
3. Click into the **search** field.
4. **Click** the **checkbox** next to **cluster-wld01-01a**.

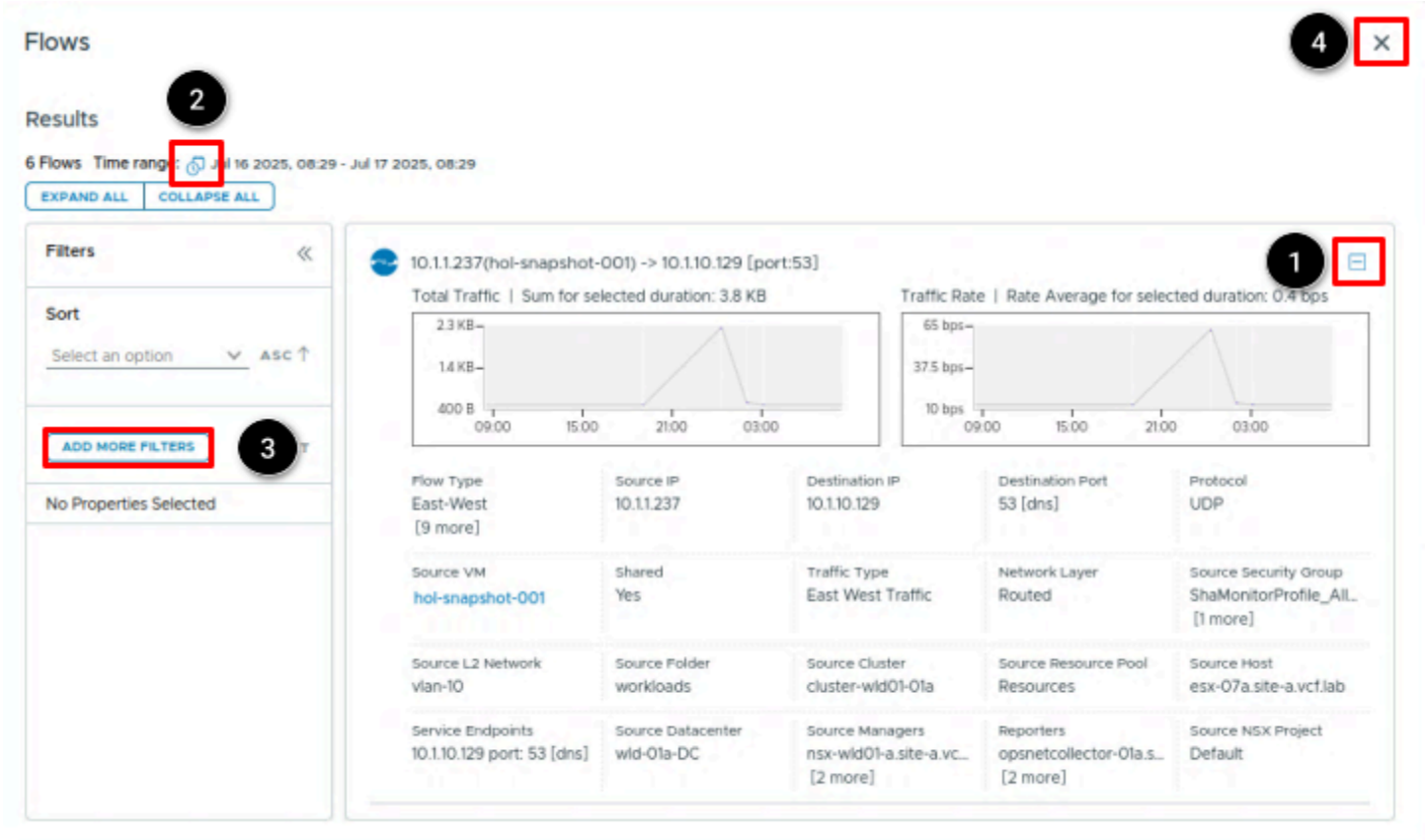
Filtering Scope for Analysis - Duration



Our next filtering step is to select our time range. Here I have combined 2 different screenshots for the sake of clarity. We can choose from a pre-defined time range or we can specify a custom range. This allows us to rewind back to a specific time when an event, outage or inquiry may originate from when we analyze flows.

1. **Click** the **down carrot** to open our Time Menu.
2. **Click** the **Custom radio button**.
3. **Click** the **Presets radio button**.
4. **Select Last 1 day**.
5. **Click View All Flows** (Not Shown)

Viewing Filtered Flows



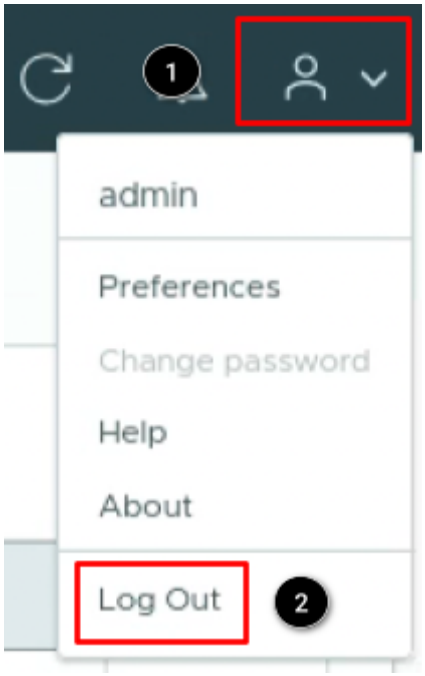
Here we see the results of our filtered query with the filtered flows broken down by unique sessions. Each session indicates the source, destination, port and protocol used. Each flow can be explored in further detail here by expanding the provided information, let's take a look.

1. **Click** the **+** sign to expand a given flow (your screen may have different flows).
2. **Optional**: Update the Time Range by **clicking** the **clock icon** and selecting the desired time range.
3. **Optional**: Add additional filters by **clicking Add More Filters**.
4. **Click** the **X** when you're done exploring flows.
5. **Click Analyze** when you return to the previous screen (not shown.)

Analyzing Flows

Content to be provided with additional POD work.

Logout



To Log out of VCF Operations:

1. Click the **User icon** to open the settings menu.
2. Click **Log Out**.

Conclusion

The new Network Operations dashboard gives administrators a quick overview of key information for both NSX and non-NSX networks. Showing objects and health relationships as well as network flows and traffic patterns, It serves as the primary starting point for monitoring and diagnosing network-related issues. In later modules, we will enable business applications with flows and network traffic summaries as well as overall NSX health summaries.

From here you can:

- Take this quick survey to provide feedback about your experience with VCF 9.0
- Continue with the next lab module.
- Click [vlp:table-of-contents|Show Table of Contents] to jump to any module or lesson in this lab.
- End your lab and return in the future.

Module 5 - Advanced Log Management in VCF Operations for Logs (30 minutes) Advanced

VMware Cloud Foundation (VCF) Operations for Logs gives administrators the ability to filter logs based on what is relevant to you, forward logs to another syslog system for further analytics and let you configure Index Partition to define different retention periods for different types of logs.

Login to VCF Operations for Logs

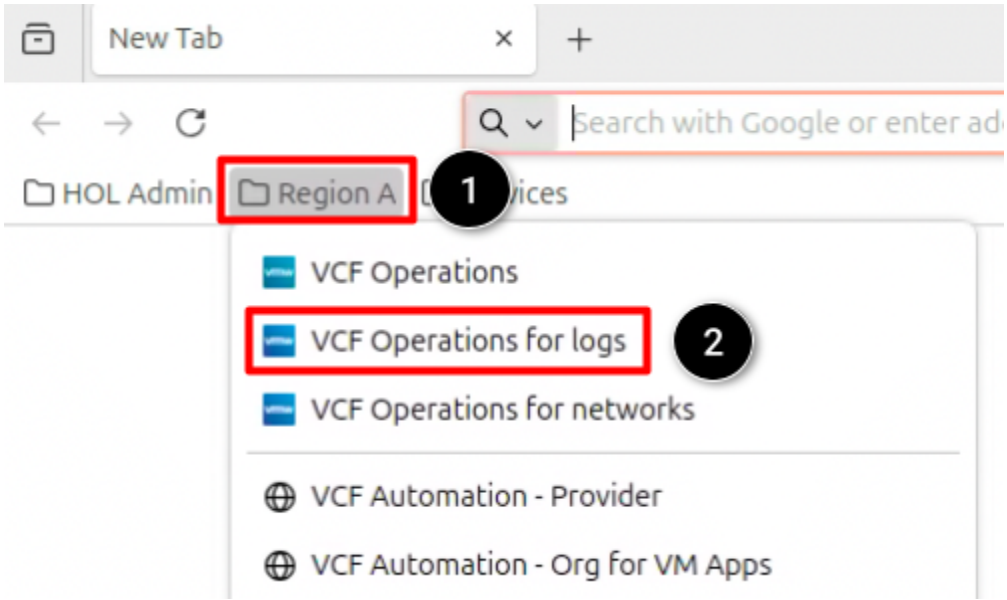
In the following few pages, we will walk through the process for logging in to VCF Operations for Logs.

Start Firefox

Open the Firefox Browser from the Linux Task Bar.

1. Click on the Firefox icon to open the browser.

Open VCF Operations for Logs Console



Once Firefox has loaded:

1. Click on the **Region A** bookmark folder.
2. Click **VCF Operations for Logs**.

Login to VCF Operations for Logs Console

The credentials for **admin** should already be cached in the browser window.

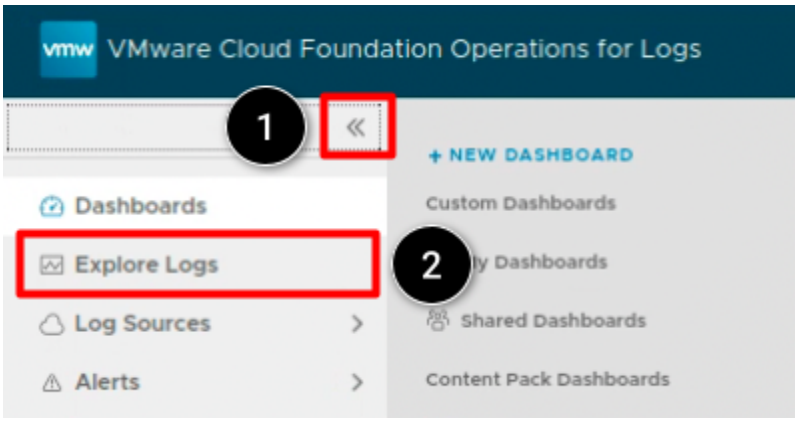
At the VCF Operations for Logs login prompt type in the following user and password information:

1. At the username field, type **admin**.
2. At the password field, type **VMware123!VMware123!**
3. Click **LOG IN**.

Configure Log Filtering

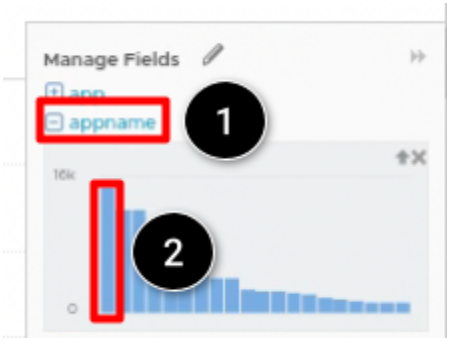
In this part of the module, we will show how to filter incoming logs based on a drop filter. When having a large amount of log source we will have some logs that are not relevant to us and therefore should not be ingested into VCF Operations for Logs.

Explore Logs



1. From the left menu click the **Collapse icon** to open the side menu and see the text of the icons.
2. Select **Explore Logs**.

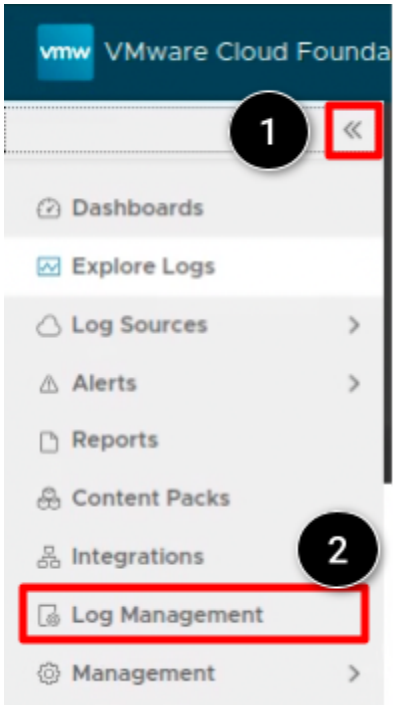
Explore Logs Overview



In the Explore Logs view you can see some bars that are much higher than the others. This means that in this time area more logs than usual were logged by VCF Operations for Logs.

1. In the **Manage Fields** section click on the "+" icon of the **appname** field.
2. **(Do not click)** You can see a bar that is higher than the others which means a lot of log entries from a specific **appname**. If you hover with the mouse over the bar you will see that the **appname** is **envoy-access**.

Go to Log Filtering

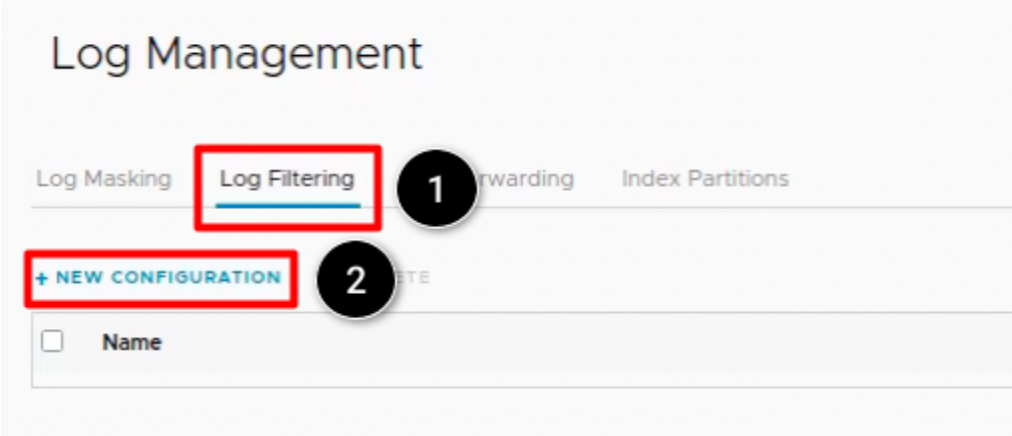


In our example the appname **envoy-access** is not relevant for our requirements. We will use Log Filtering to drop all logs that are coming from the appname **envoy-access**.

WARNING: This is just an example for this lesson. Please don't use this as an example for a real world environment. In a real world environment you would probably filter out different logs.

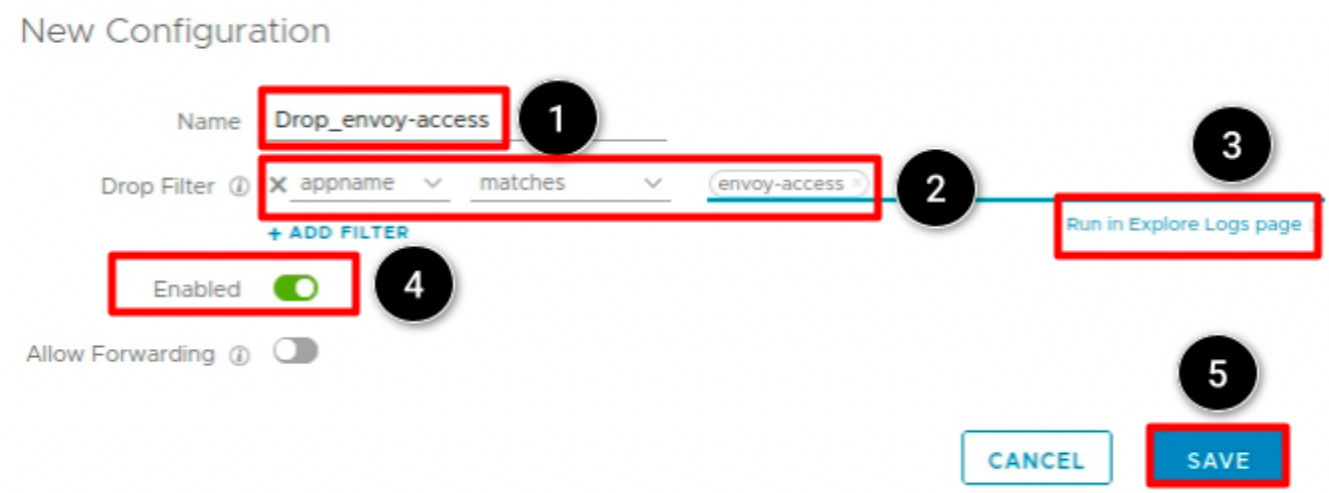
1. From the left menu click the **Collapse icon** to see the text of the icons.
2. Select **Log Management**.

Add Log Filtering configuration



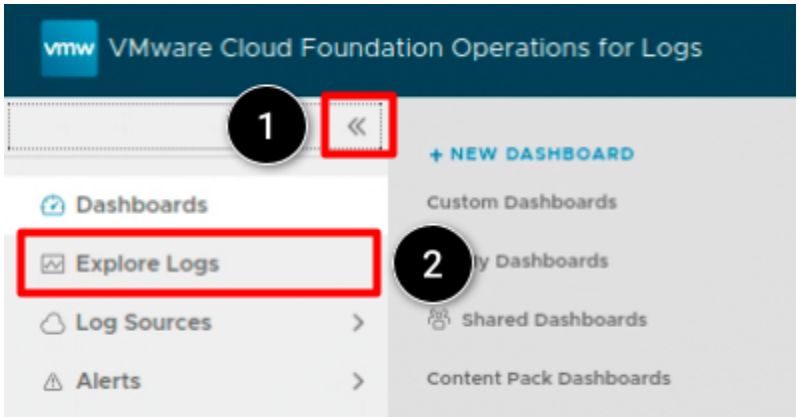
1. In Log Management click on **Log Filtering**.
2. Click on **New Configuration** to create a new Log Filtering rule.
3. **(not shown)** Also remember the time when you created this new rule so we can check in Explore Logs if it is working. You can find the time on top in the middle of the Ubuntu desktop.

Configure Log Filtering



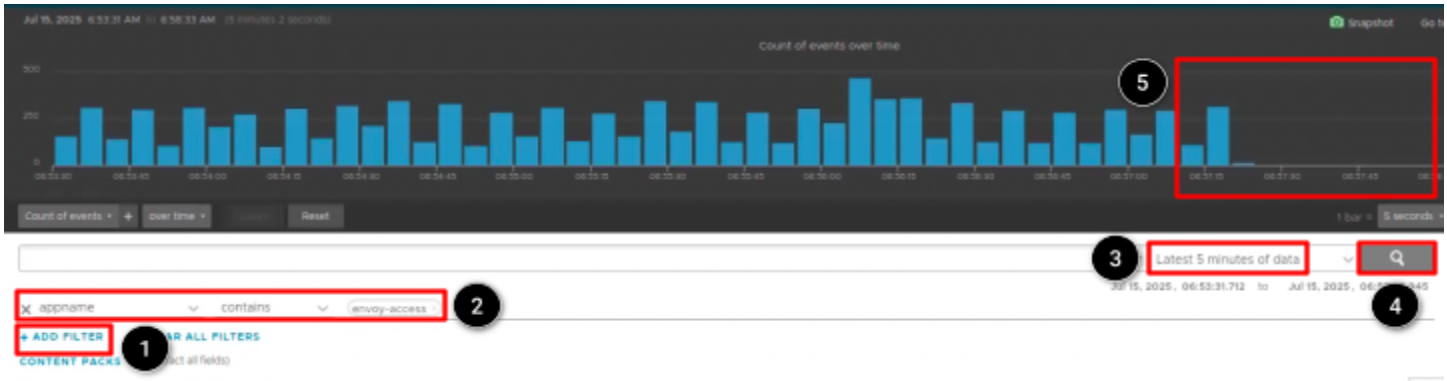
1. Give the rule a name: **Drop_envoy-access**
2. Define the drop filter. Select "**appname**" from the first drop-down, "**matches**" from the second drop-down and write **envoy-access** in the text field and press Enter or select the provided match.
3. You can use "**Run in Explore Logs page**" to see if your filter is correct.
4. Check if "**Enabled**" is on.
5. Click on "**Save**" to save your filter rule.

Go to Explore Logs



1. From the left menu click the **Collapse icon** to open the side menu and see the text of the icons.
2. Select **Explore Logs**.

Validate the Log Filter



1. In the **Explore Logs View**, click on "**Add Filter**" to add a new filter.
2. From the first drop-down select "**appname**" (you can also type appname to find it), from the second drop-down select "**contains**" and as text use **envoy-access** and press Enter or select the provided match from the drop down list.
3. Select "**Latest 5 minutes of data**"
4. Click on the magnifier symbol to start your search
5. You can see that after you enabled the Log Filter rule no new **envoy-access** entries will show up in the **Explore Logs view**.

Configure Log Forwarding

VCF Operations for Logs can be configured to forward incoming log events to a syslog or Ingestion API target.
Log forwarding can be used to send filtered or tagged logs to one or more remote destinations such as VCF Operations for Logs or syslog or both. Log forwarding can be used to support existing logging tools such as SIEM and to consolidate logging over different networks such as DMZ or WAN.

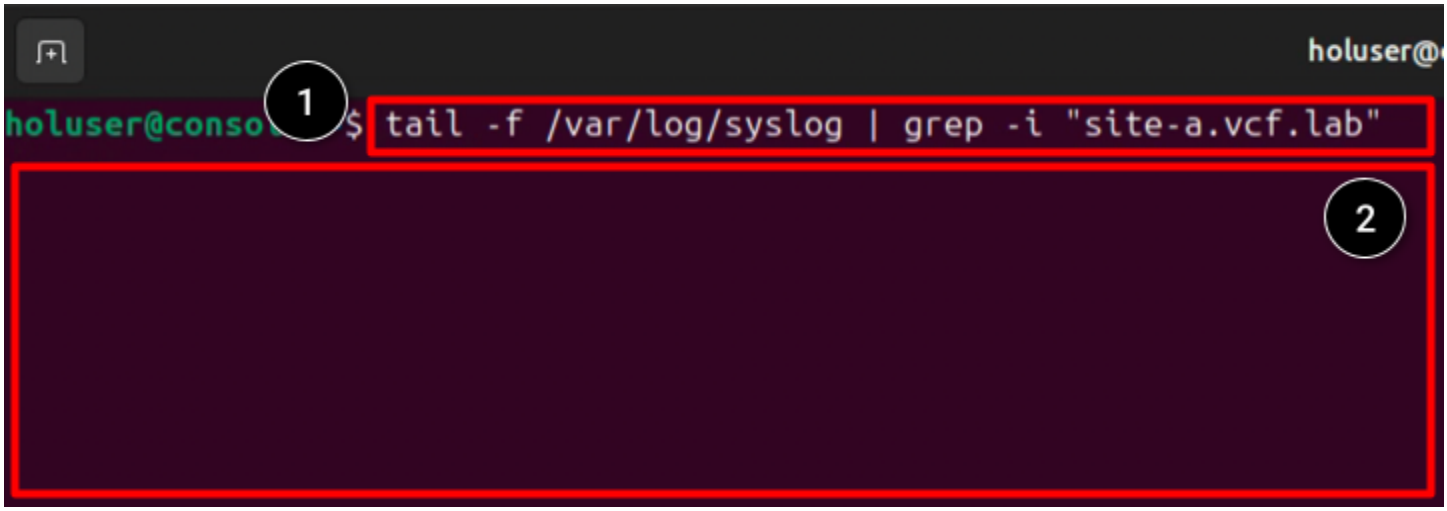
In this part of the module, we will show how to configure Log Forwarding to a different Syslog server.

Open Terminal

Open the Terminal from the Linux Task Bar.

1. Click on the **Terminal** icon.

Filter through local logs

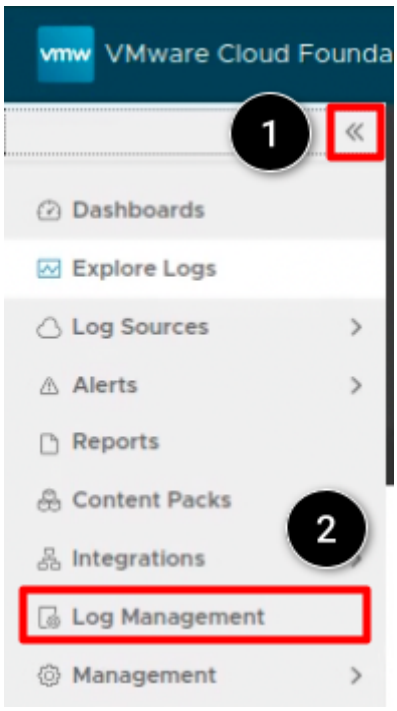


The Ubuntu Desktop we are currently connected to is functioning as a secondary syslog server, with the **rsyslog** service enabled on this VM. As there is no Graphical User Interface (GUI), we must utilize a terminal session and Linux commands to view incoming logs.

1. Use the Linux command **tail -f /var/log/syslog | grep -i "site-a.vcf.lab"**
2. As you can see, there is no entry coming up when using this command, as there is no forwarder configured yet.

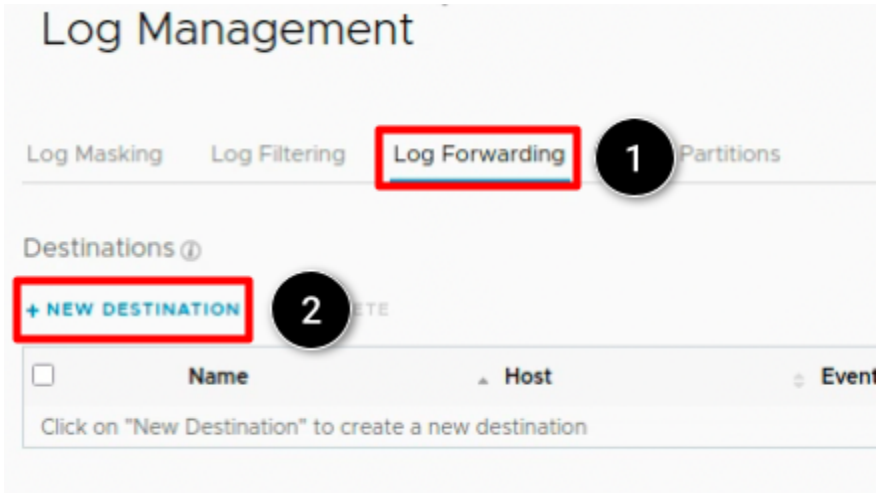
This command displays the end of the syslog file (**tail**), continuously updates with new input (**-f**), and filters for log entries containing "site-a.vcf.lab" (**grep**).

Go to Log Forwarding



1. From the left menu click the **Collapse icon** to see the text of the icons.
2. Select **Log Management**.

Add a New Log Forwarding Destination



1. In the Log Management View, click on "**Log Forwarding**".
2. Click on "**New Destination**" to create a new forwarding destination.

Configure the Log Forwarding Destination

1. Give the Destination a name: **Second-Syslog**
2. For the host use either FQDN or IP address: **10.1.10.130**
3. Select the protocol: **Syslog**
4. Select the transport: **UDP**
5. (Optional) Click **Test**. After a short period of time you should see a green text that starts with "**Test event sent...**". This shows that the destination syslog server is receiving information.
6. Click on "**Save**" to save the Log Forward Destination configuration.

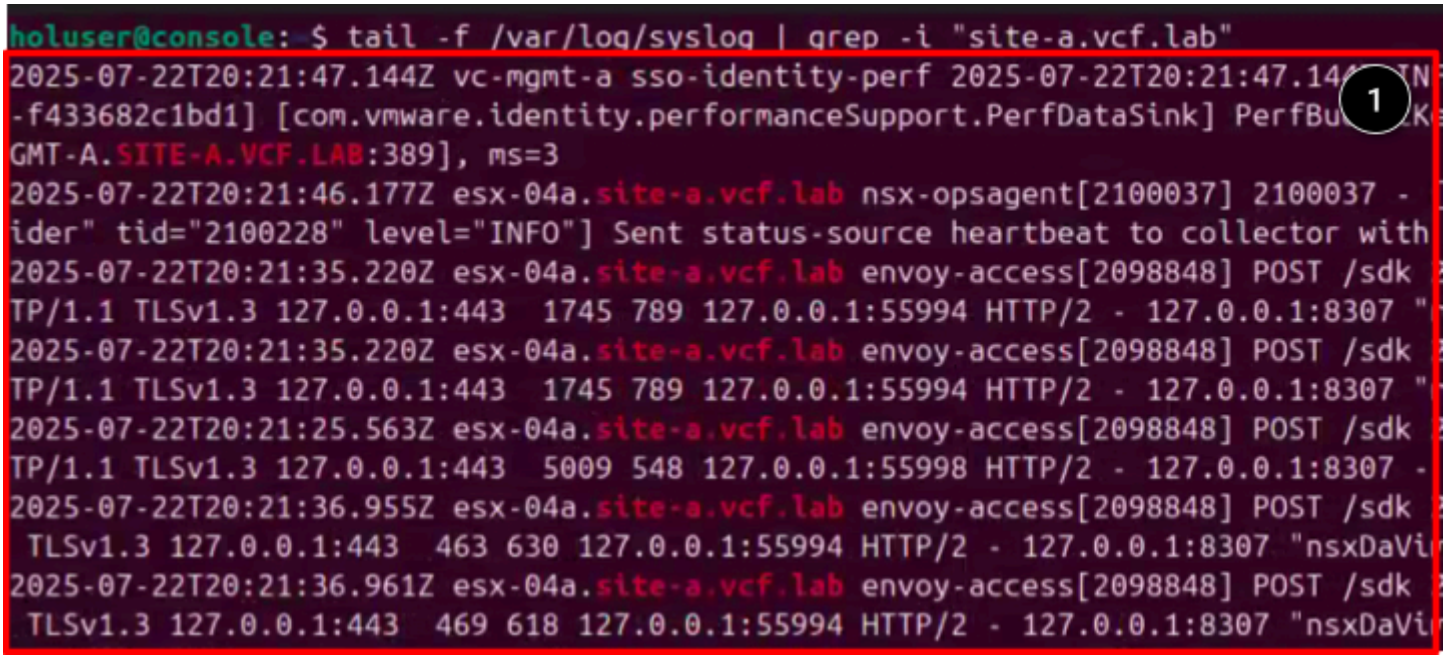
As a protocol we can choose between Ingestion API, Syslog and Raw.

When logs are forwarded using **Ingestion API**, the log's original source is preserved in the source field.

When logs are forwarded using **Syslog**, the log's original source is lost and the receiver can record the message's source as the VCF Operations for Logs forwarder's IP address or hostname.

When logs are forwarded using **Raw**, the behavior is similar to syslog, but syslog RFC-compliance is not ensured. RAW forwards a log exactly the way it is received, without a custom syslog header added by VCF Operations for Logs. The RAW protocol is useful for third-party destinations, because they expect syslog events in their original form.

Validate Log Forwarding



Go back to the Terminal.

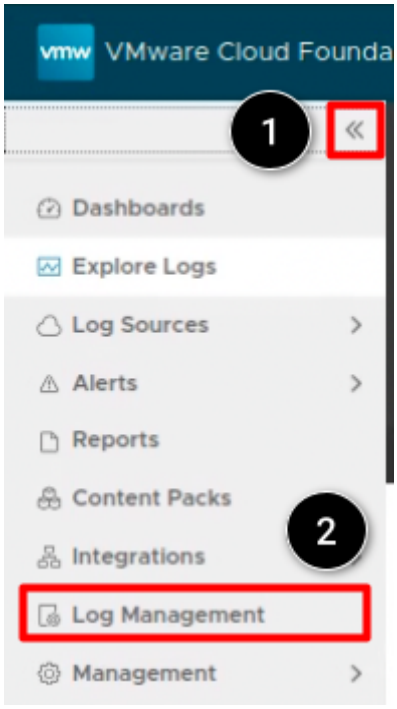
1. We can now see that we are receiving logs from VCF Operations for Logs.

Configure Index Partition

Index partitions let us define different retention periods for different types of logs. For example, logs with sensitive information might require a short retention period, such as five days which will help you save storage space. We can also archive the data in an index partition to an NFS mount, to retain the logs for an extended period.
In this part of the module, we will learn how to configure an Index Partition for specific logs and change the retention time for the partition.

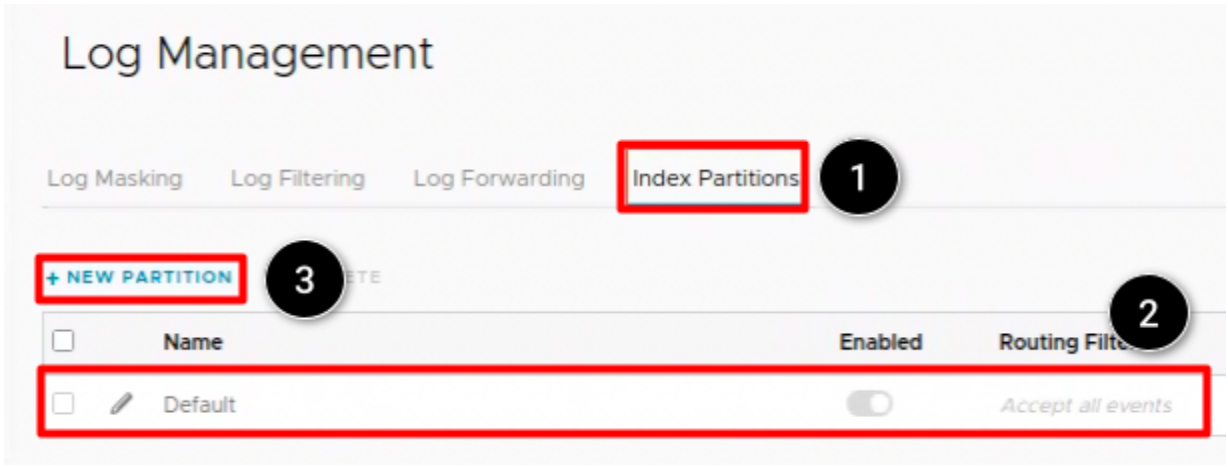
We can have a maximum of 10 index partitions.

Go to Index Partition



1. From the left menu click the **Collapse icon** to see the text of the icons.
2. Select **Log Management**.

Index Partitions Overview



1. In Log Management click on **Index Partitions**.
2. Per default there is an Index Partition named "**Default**" with a Routing Filter "**Accept all events**" and a Retention Period of "**Forever**". This means that this Index Partition has all log events in it and keeps it forever until there is not enough space left and the oldest entry gets deleted.
3. Click on "**New Partition**".

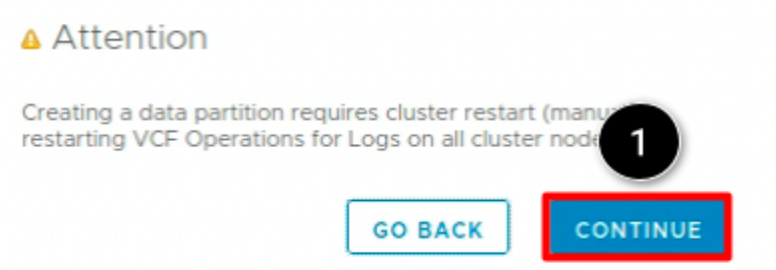
Add and Configure New Index Partition

In our example we will create an Index Partition that includes all ESX logs and has a retention time of 7 days.

This is just an example used here for demonstration purposes in the HOL environment. In a real world scenario you would probably use other filters, logs and partitions.

1. Give the Partition a name: **All-ESX-Logs**
2. Define the routing filter. Select **hostname** from the first drop-down (we can also type it in to find it faster), "starts with" from the second drop-down and write esxi in the text field.
3. We can use "**Run in Explore Logs page**" to validate if our filter is correct.
4. Define the "Retention Period": **7** days
5. **(Optional)** If there is a requirement to archive these logs, we could also configure an NFS share here. All log buckets that exceeds 500MB will be sealed, set to read-only and then will be moved to the NFS share.
6. Click on "**Save**" to save your Index Partition configuration.

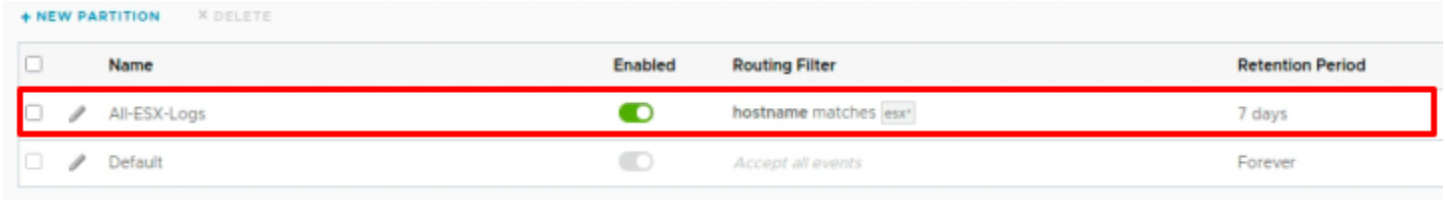
Finish Index Partition Configuration



After clicking on "**Save**" we will receive a warning Window. This means that we need to restart the VCF Operations for Logs cluster in order to make the Index Partition work. As this is a lab environment we **WILL NOT** restart the cluster as it will take a long time to restart it.

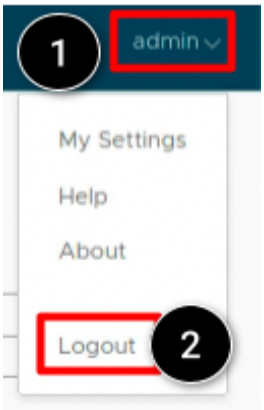
1. Click "**Continue**".

Validating the New Index Partition



We can see that the Index Partition was successfully created although it is not active yet.

Logout



To Log out of VCF Operations for Logs:

1. Click the **admin icon** to open the settings menu.
2. Click **Logout**.

Conclusion

In this module, we have reviewed how to create Log Filtering, Log Forwarding and Index Partitions.

From here you can:

- Take this quick survey to provide feedback about your experience with VCF 9.0
- Click [vlp:table-of-contents|Show Table of Contents] to jump to any module or lesson in this lab.
- End your lab and return in the future.

End of Lab Manual (06/25)

Copyright © 2025 Broadcom. All rights reserved.
The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, go to www.broadcom.com. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies. Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.
Item No: 51227-vcf-wp-hands-on-labs-manual-2025, Jan-25

vmware® by Broadcom