HOL-2601-11-VCF-L

HANDS-ON LABS MANUAL - 2026

Monitoring Private Cloud Infrastructure with VCF Health and Diagnostics Using VCF Operations

HOL-2601-11-VCF-L

vmware by Broadcom

Table of Contents

Monitoring Private Cloud Infrastructure with VCF Health and Diagnostics Using VCF Operations (HOL-2601-11-VCF-L)

Use this comprehensive guide to master the operational aspects of VMware Cloud Foundation 9.0. You'll gain hands-on experience with VCF Health and Diagnostics, learn to maximize value with VMware Aria Operations, monitor and analyze networks for improved application performance, and understand how to prevent issues by leveraging VCF Health. Discover how to effectively use Log Assist to streamline support and troubleshoot your VMware Cloud Foundation environment.

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	Using VCF Diagnostic Findings to Identify Issues in the Private Cloud	30 min	Intermediate
2	Using VCF Diagnostics Log Assist to Resolve Private Cloud Issues More Quickly	30 min	Beginner
3	Monitor Your Environment and Prevent Issues with VCF Health	30 min	Intermediate

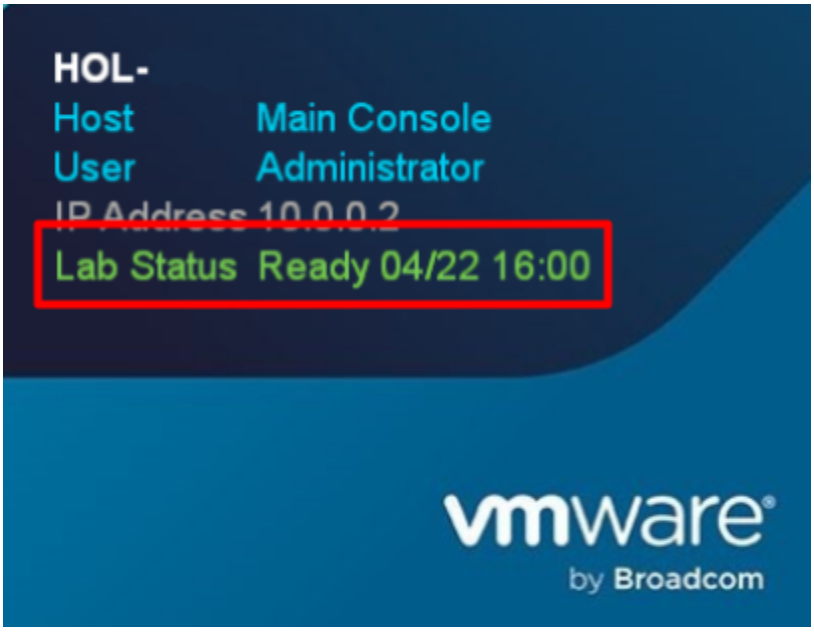
Lab Authors:
- Module 1 - Brock Peterson, Solutions Architect, USA and Shannon Fitzpatrick, Staff Technical Adoption Manager, USA
- Module 2 - Kelcey Lemon, Product Marketing Engineer, USA and Sorin Platon, Solution Specialist, Canada
- Module 3 - Brock Peterson, Solutions Architect, USA and Shannon Fitzpatrick, Staff Technical Adoption Manager, USA

Captain:
Shannon Fitzpatrick, Staff Technical Adoption Manager, USA

Lab Principals:
- Christopher Lewis, Lead VCF Specialist Solutions Architect, UK
- Katherine Skilling, Senior Architect, Professional Services, UK

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 - Using VCF Operations Diagnostic Findings (30 minutes) Intermediate

VMware Cloud Foundation (VCF) provides a unified and integrated platform that simplifies cloud management across compute, storage, and networking. In this module, we will review Diagnostic Findings and how it can help with Day 2 Operations by identifying potential problems and underlying issues in the VCF 9.0 environment.

Login to VCF Operations

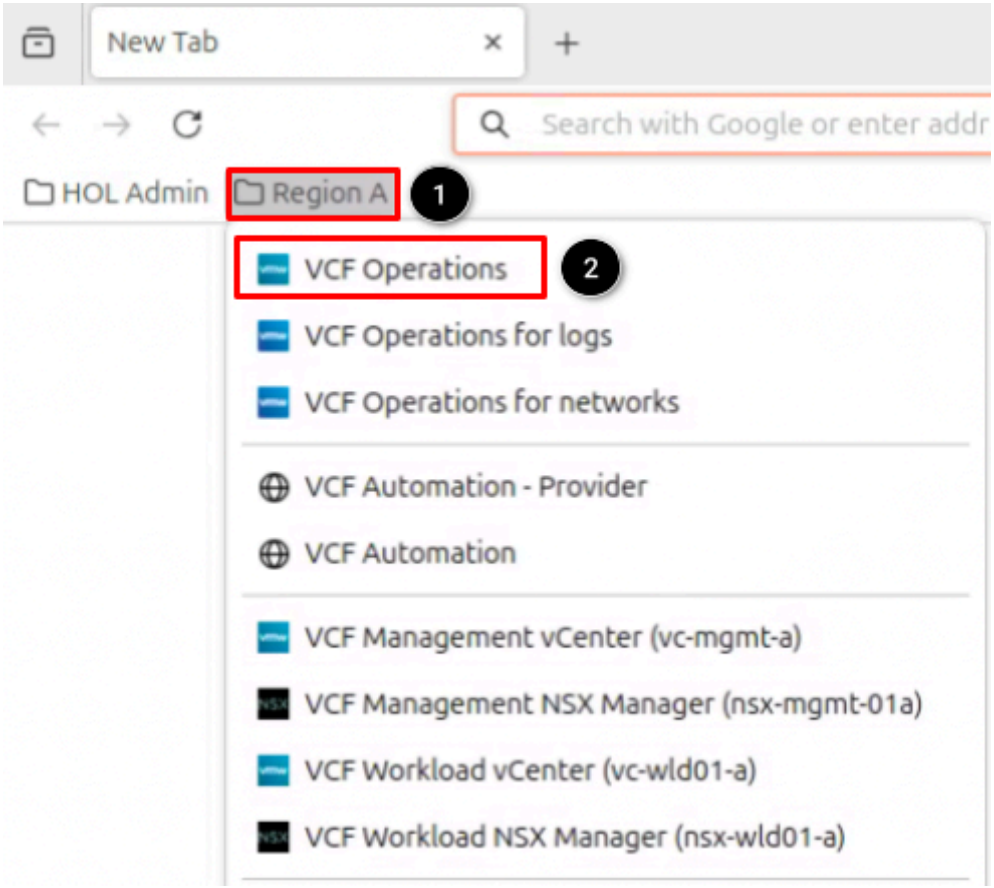
In the following few pages, we will walk through the process for logging in to VCF Operations.

Start Firefox

Open the Firefox Browser from the Linux Task Bar.

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

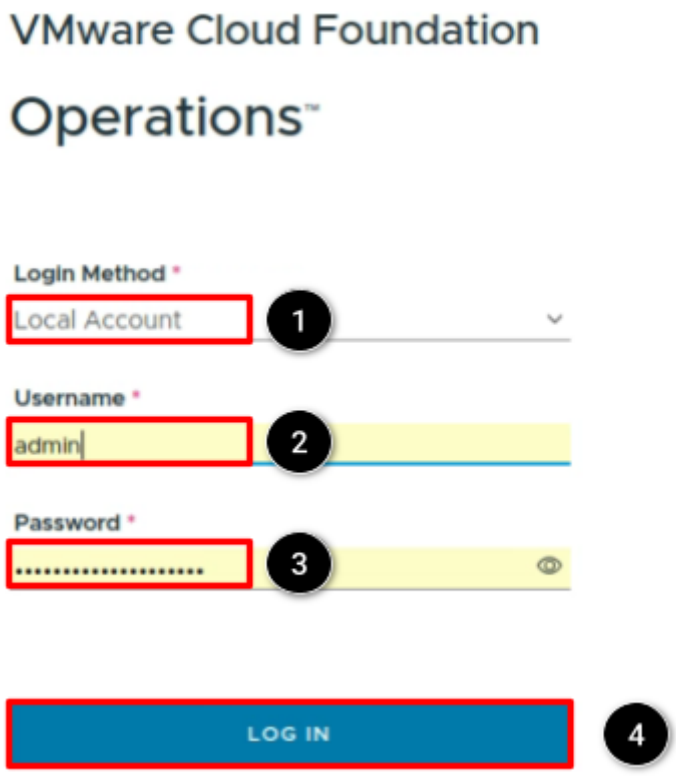
Open VCF Operations Console



Once Firefox has loaded:

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

Log In to VCF Operations



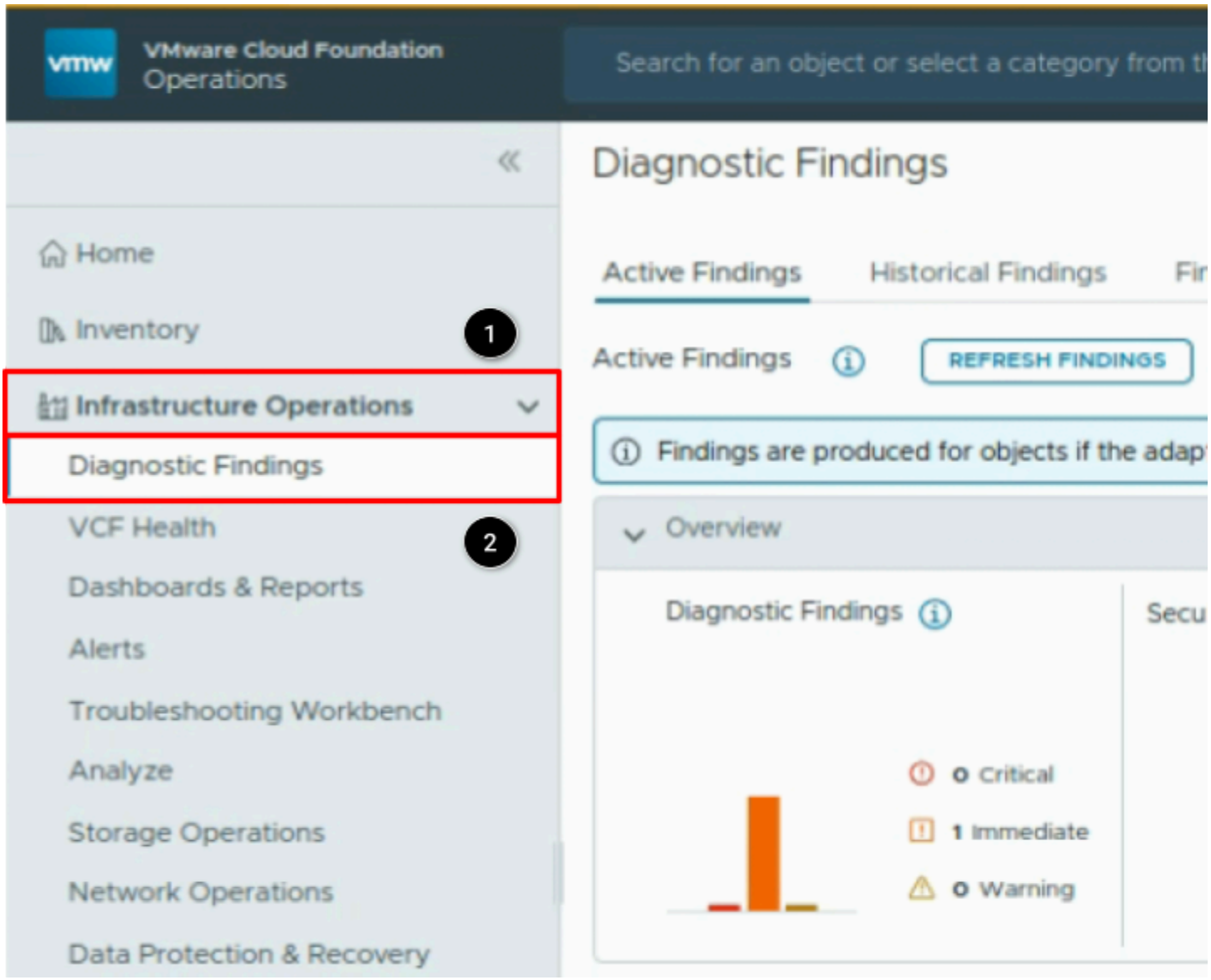
At the VCF Operations login prompt, select the login method and type in the following user and password information:

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**.

Troubleshooting the Private Cloud with Diagnostic Findings

Diagnostic Findings are derived from properties and product log data from vCenter, ESX, NSX, SDDC Manager, VCF Operations, vSAN, and VCF Automation. Using this collective data helps us identify potential problems and informs us about existing issues in our environment as well as provides steps to resolve them. Let's dig into this awesome tool and see how valuable it can be for Day 2 Operations.

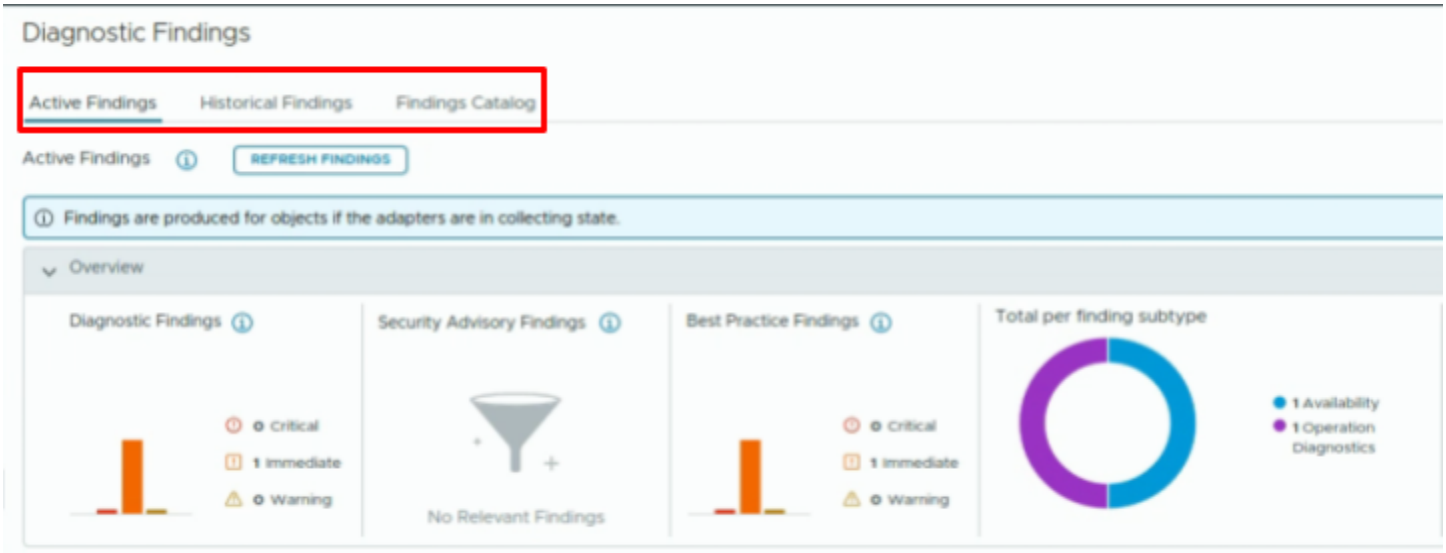
Access Diagnostic Findings



We access **Diagnostic Findings** by completing the following actions:

1. Select **Infrastructure Operations**.
2. Select **Diagnostic Findings**.

Diagnostic Findings Page - Overview

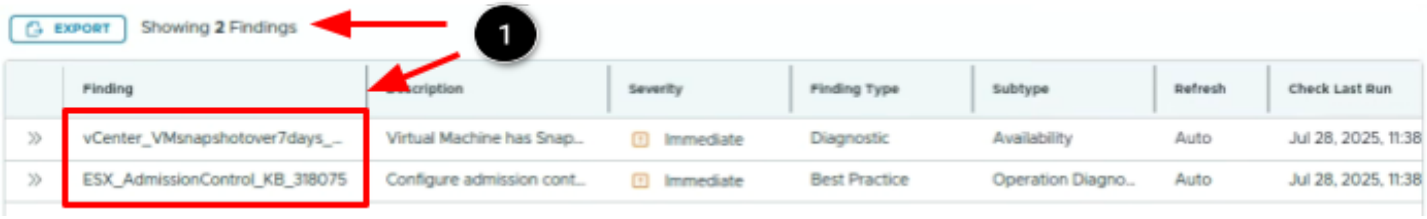


On the **Diagnostics Findings** page, we see the information is divided into three subcategory tabs to make it easier to locate what we need. The subcategories are:

- **Active Findings** – Findings currently found in the environment.
- **Historical Findings** – Findings previously found in the environment but no longer present.
- **Findings Catalog** – A catalog of all findings that are being searched for in the environment.

Note: The **Active Findings** tab is selected by default. Let's review a currently active finding in the lab environment.

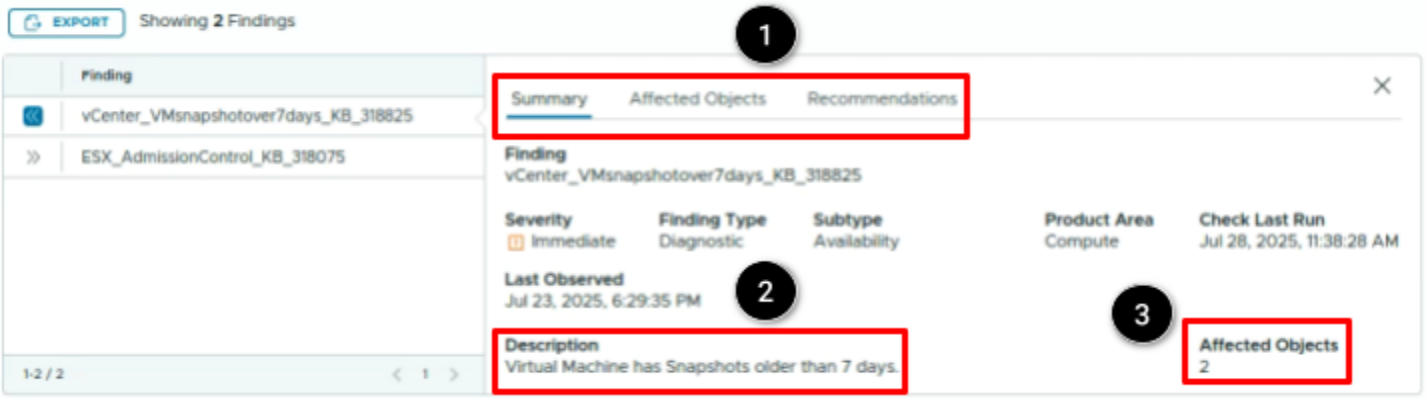
Active Findings List



In the lower right pane of the **Diagnostic Findings** page we start to see potential issues being identified. What is seen in the lab may differ from what is shown in the image, but the concepts and processes remain the same for any finding.

1. In the image, we see a total of **2 Findings** and see a brief overview in our list.
2. Click the **double arrow** icon next to one of the active findings (not shown). For this lab, we are focusing on the first finding, **vCenter_VMsnapshotover7days_KB_318825.**

Active Finding Summary

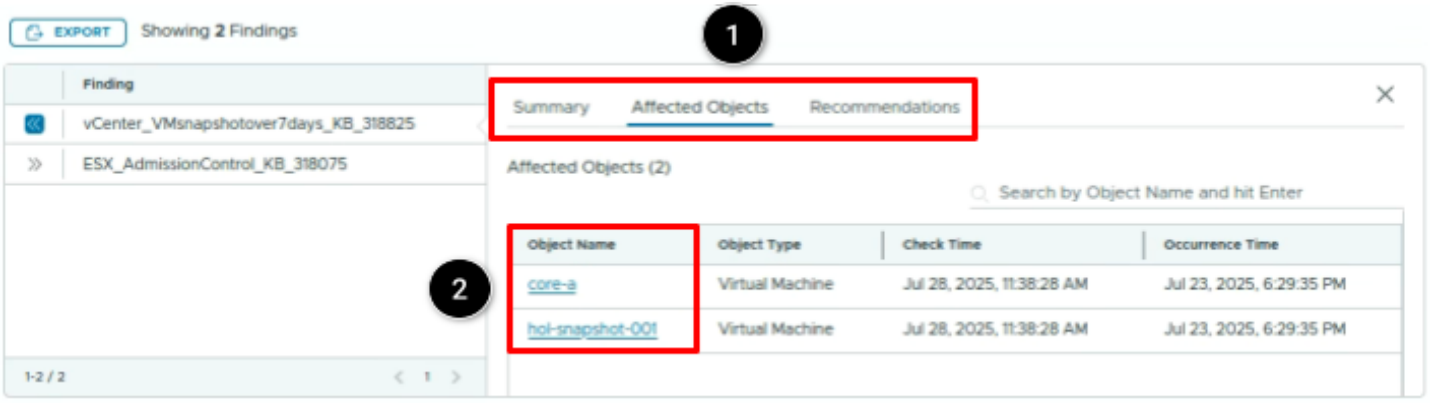


On the **Summary tab** of the Active Finding, we start to see some valuable information.

1. First, notice we are viewing the **Summary** of the finding as denoted by the blue underline bar.
2. The **Description** field is where we start learning the specifics of the finding. In the image example, we see this finding is for VMs running with snapshots older than 7 days.
3. Notice in the **Affected Objects** field that we have 2 objects in the environment impacted by this finding, meaning we have two VMs in our environment that have snapshots older than 7 days.

   Let's see which VMs are impacted by this finding by selecting the **Affected Objects** tab (shown in Step 1).

Active Finding Affected Objects

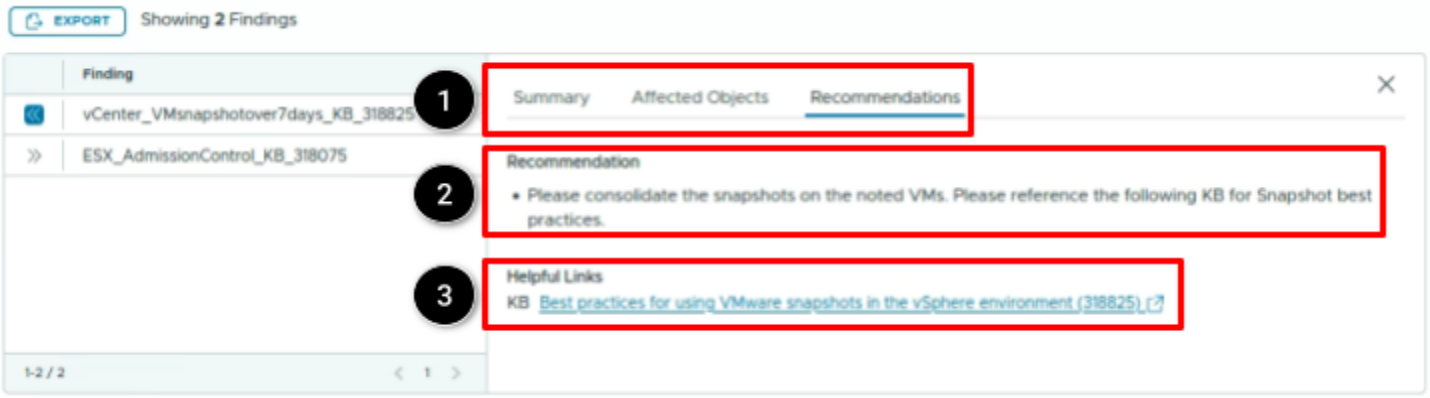


On the **Affected Objects tab** of the Active Finding, we see:

1. First, notice we are viewing **Affected Objects** of the finding as denoted by the blue underline bar.
2. The **Object Name Column** identifies the VMs impacted by this finding. In the image example, we see **core-a** and **hol-snapshot-001** are the VMs running with snapshots older than 7 days. **Note**: Clicking on either of the VM hyperlinks will take us to the Object Inventory for the chosen object. This is outside the scope of this lab, but feel free to research it further as time allows.

   Let's see the Recommendation on how to resolve this finding by selecting the **Recommendations** tab (shown in Step 1).

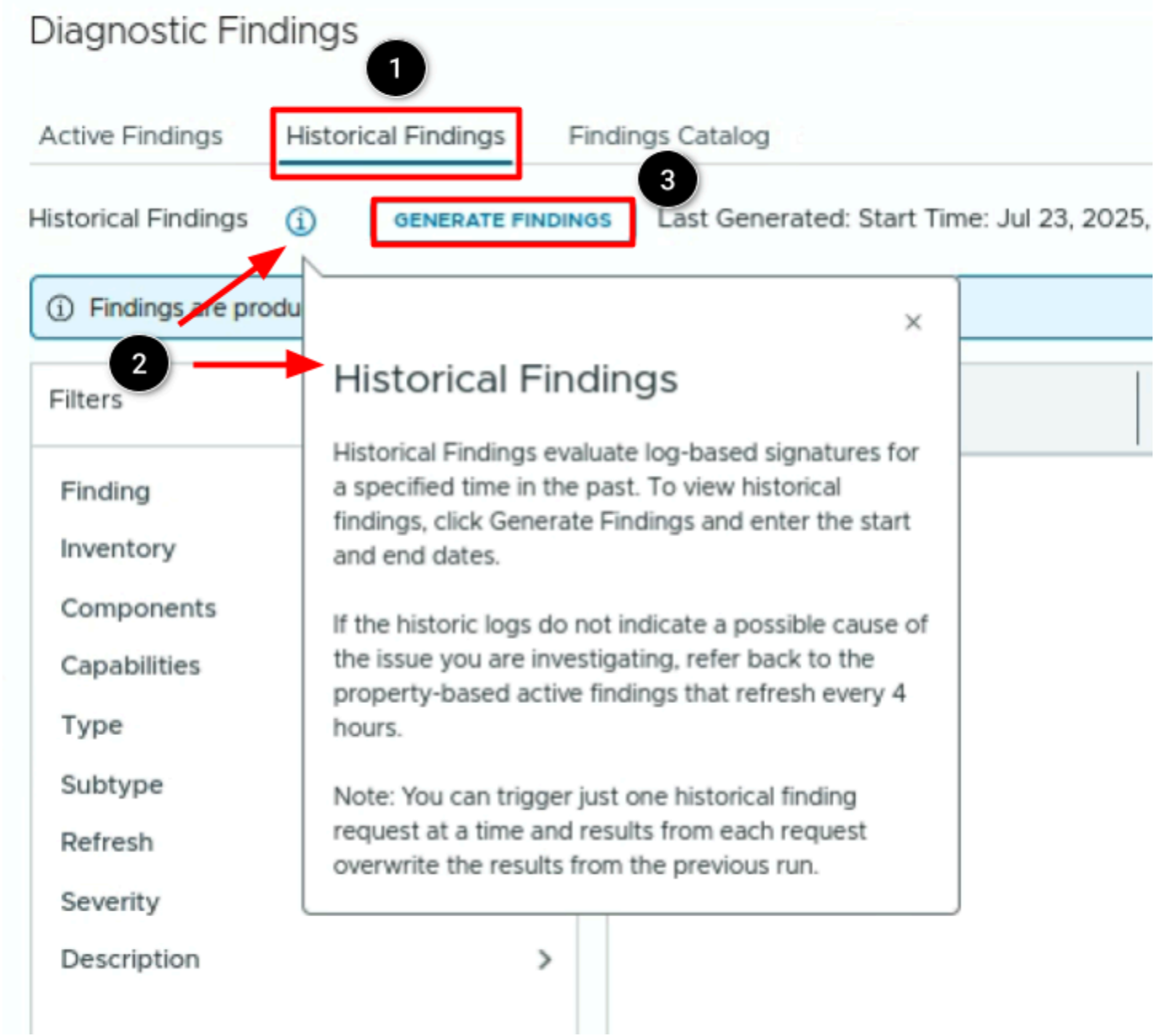
Active Finding Recommendations



On the **Recommendations tab** of the Active Finding, we see:

1. First, notice we are viewing **Recommendations** of the finding as denoted by the blue underline bar.
2. In the image example, we see the **Recommendation** is to consolidate the snapshot on the noted VMs.
3. We are also provided with a link in the **Helpful Links** section which takes us to an eternal KB article which discusses the Best Practices for using snapshots in a vSphere environment. (**Note**: The external link may not work in the lab due to the sandboxed environment). In a Production environment, these links can be a valuable resource for resolving the active findings we are researching.

Diagnostic Findings - Historical Findings

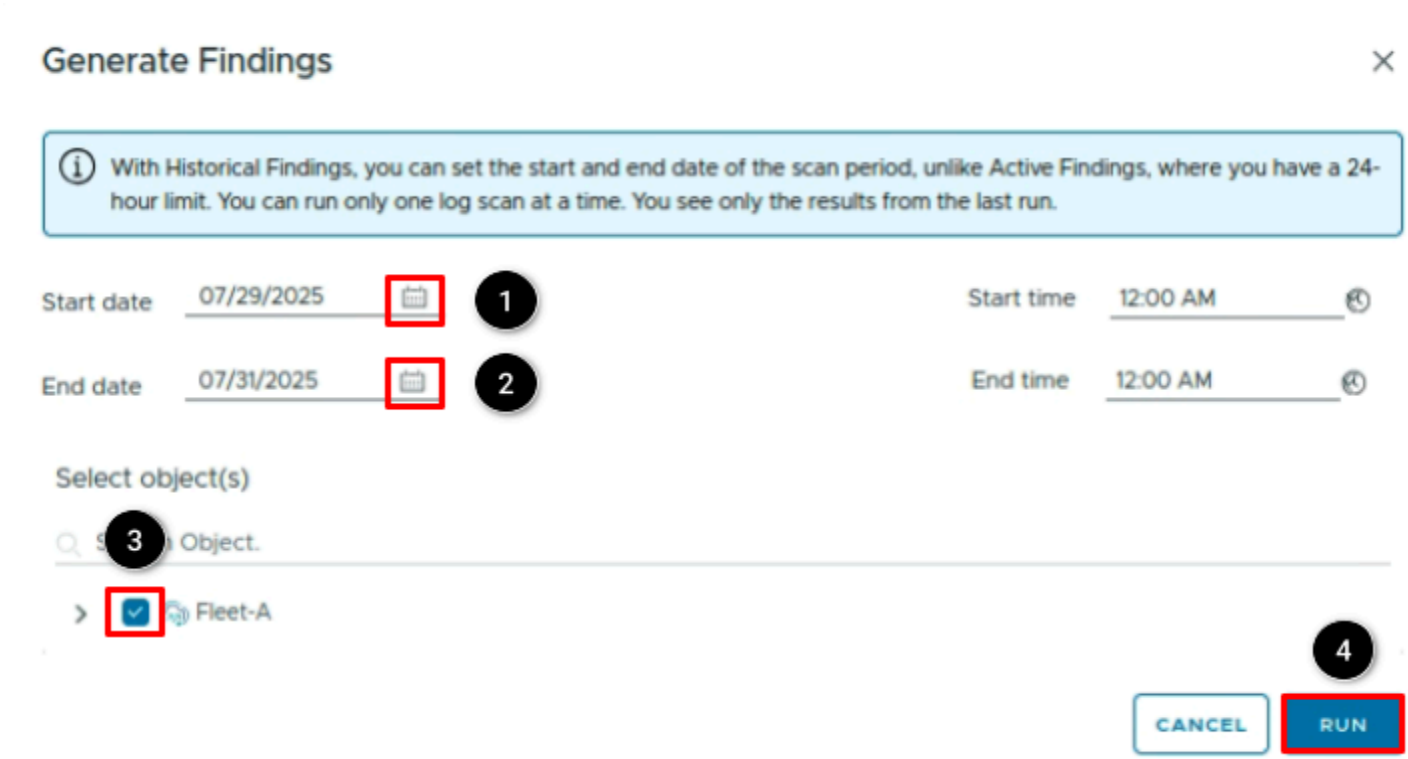


After completing our review of Active Findings, let's now focus on **Historical Findings**. Historical Findings are findings which have been observed in the environment during our designated review period. Let's see how to identify findings during the past 48 hours of the lab environment.

1. Click on the **Historical Findings** tab at the top of the Diagnostics Findings page.
2. (Optional) We can click on the **information icon** to learn more about Historical Findings.
3. Click **GENERATE FINDINGS**.

Note: The images throughout this section may not match what is seen in the lab due to the labs being “torn down and redeployed” on a regular basis. There may be more errors or no errors at the time of the lab; however, the concepts and actions taken will remain the same.

Generate Findings

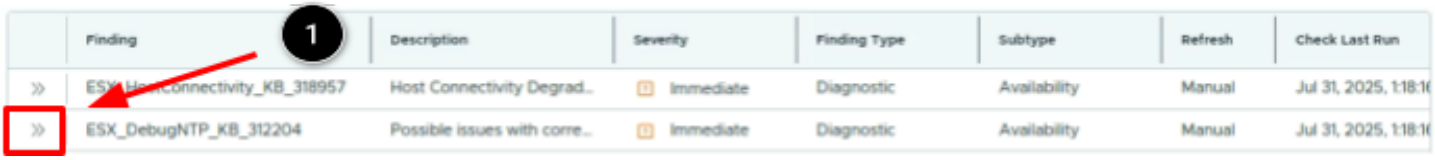


In order to view Historical Findings, we need to choose the dates and objects we want to review. These selections are made in the **Generate Findings** window.

1. In the **Start date** field, select the **calendar icon**. A separate calendar window will appear (not shown), and in this calendar select a day two days prior to the current date. (**Note**: Due to the limited lab resources, we can only pull log data from the previous 48 hours).
2. In the **End date** field, select the **calendar icon**. A separate calendar window will appear (not shown), and in this calendar select the current date.
3. We now want to select the **Object(s)** we want to pull historical data from. Our lab is small, so select **Fleet-A** (the entire available environment. In a large Production environment, we'd likely want to be more selective so as to keep our focus narrowed).
4. Click **RUN**.

Depending upon the current workload in the lab environment, this process may take several minutes. The process is tracked next to the **Generate Findings** button we clicked on earlier. Once the process is 100% completed, we should have some Historical Findings to review.

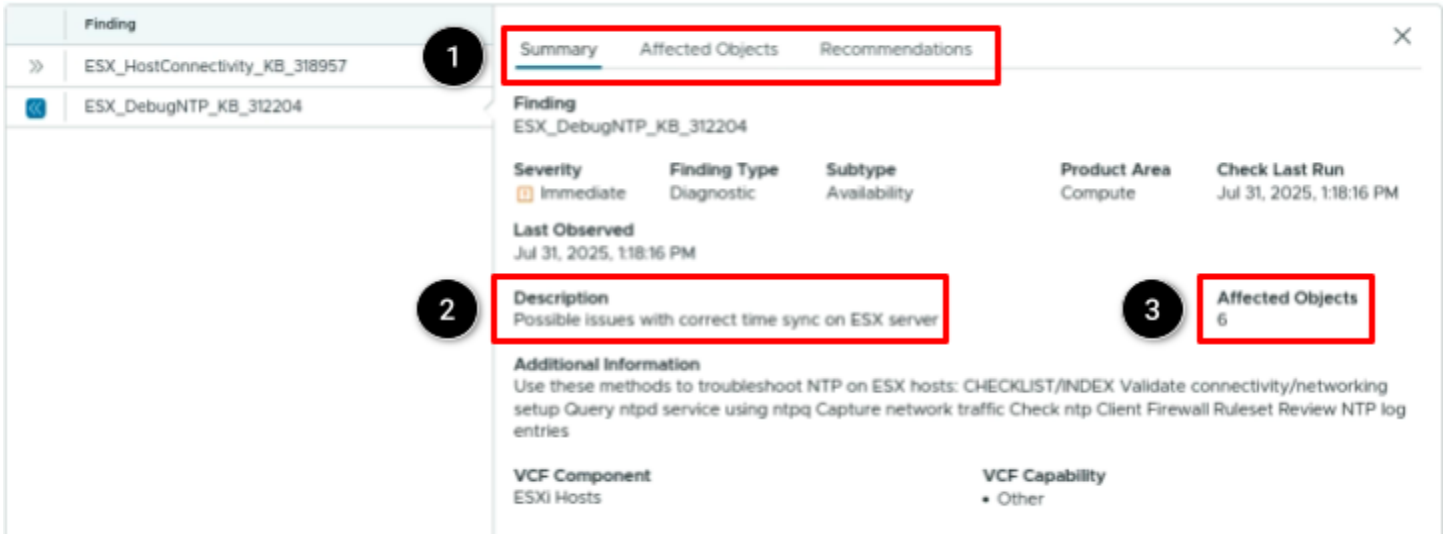
Historical Findings List



As with our previous discussion on Active Findings, we now see a list of Historical Findings. Let's review the options available in a specific finding.

1. Select the **double arrow icon** next to one of the identified findings. In our image, we selected the double arrows next to the second finding.

Historical Finding Summary

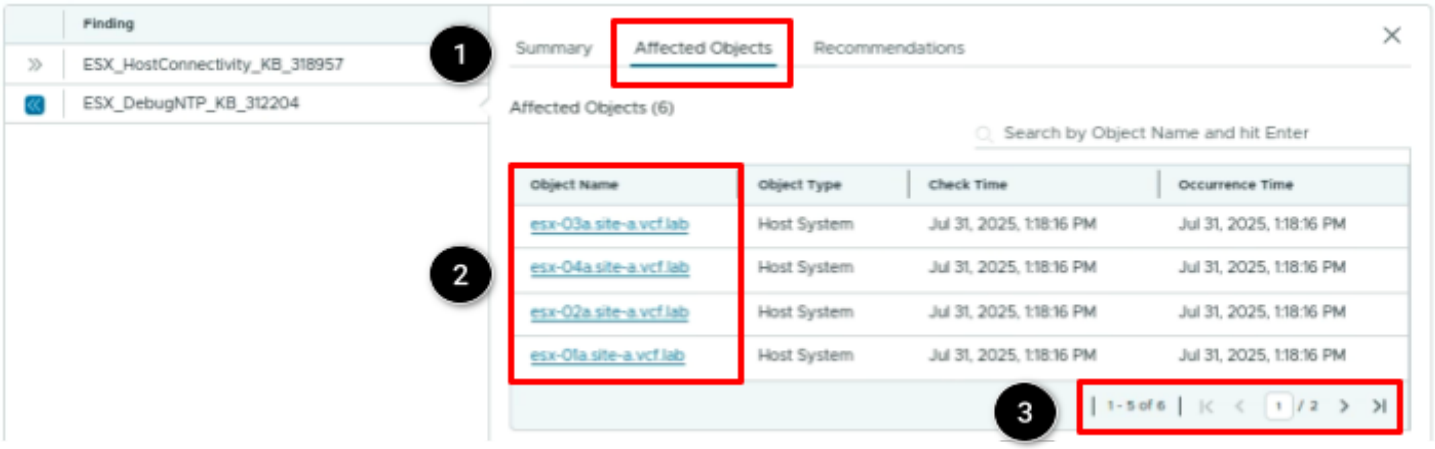


On the **Summary tab** of the chosen Historical Finding, we start to see some valuable information.

1. First, notice we are viewing the **Summary** of the finding as denoted by the blue underline bar.
2. The **Description** field is where we start learning the specifics of the finding. In the image example, we see this finding is for Possible issues with correct time sync on ESX server.
3. Notice in the image example, in the **Affected Objects** field we have 6 objects in the environment impacted by this finding, meaning we have six ESX Hosts in our environment that are having time sync issues (likely incorrect NTP settings or an inability to reach our configured NTP servers).

Let's see which ESX Hosts are impacted by this finding by selecting the **Affected Objects** tab (shown in Step 1).

Historical Finding Affected Objects

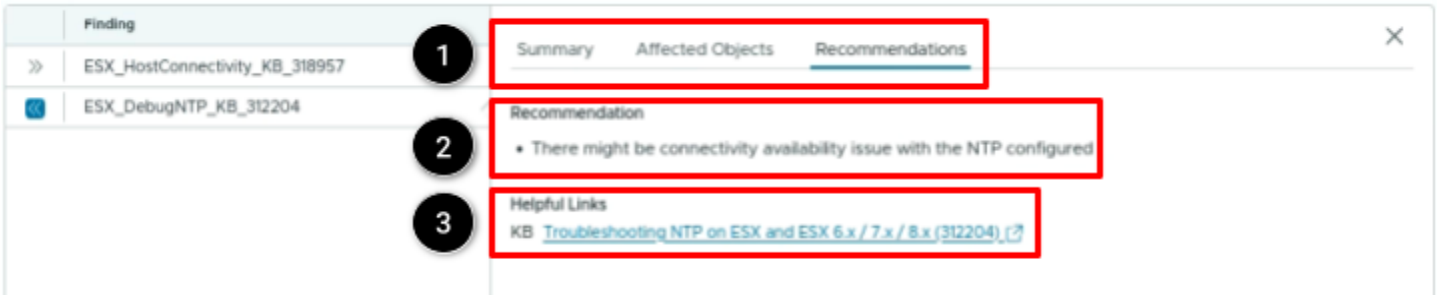


On the **Affected Objects tab** of the Historical Finding, we see:

1. First, notice we are viewing **Affected Objects** of the finding as denoted by the blue underline bar.
2. The **Object Name Column** identifies the ESX Hosts impacted by this finding. In the image example, we see four hosts in the immediate list that are having time sync issues. **Note**: Clicking on any of the Host hyperlinks will take us to the Object Inventory for the chosen object. This is outside the scope of this lab, but feel free to research it further as time allows.
3. Notice in the image example we are viewing 1-5 hosts out of 6 that are impacted by this finding. Our image shows 4, but we can use the sidebar (not show) to see the 5th host on this page. To see the 6th host impacted, click the **page over arrow**.

Let's see the Recommendation on how to resolve this finding by selecting the **Recommendations** tab (shown in Step 1).

Historical Finding Recommendations



On the **Recommendations tab** of the selected Historical Finding, we see:

1. First, notice we are viewing **Recommendations** of the finding as denoted by the blue underline bar.
2. In the image example, we see the **Recommendation** is there might be a connectivity availability issue with the NTP configured on the impacted ESX Hosts.
3. We are also provided with a link in the **Helpful Links** section which takes us to an eternal KB article which discusses how to Troubleshoot NTP on our Hosts. (**Note**: The external link may not work in the lab due to the sandboxed environment). In a Production environment, these links can be a valuable resource for resolving the active findings we are researching.

Conclusion

In this module, we reviewed how VMware Cloud Foundation (VCF) provides a unified and integrated platform that simplifies cloud management across compute, storage, and networking. We reviewed Diagnostic Findings and how it can help with Day 2 Operations by identifying potential problems and underlying issues in the VCF 9.0 environment.

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 - VCF Operations Diagnostics - Using Log Assist (30 minutes) Beginner

In VMware Cloud Foundation 9, a critical tool returns for assistance with Day 2 Operations in the form of **Log Assist**. Many customers likely remember this feature as part of Skyline Advisor before it was deprecated, but thankfully it has returned as a built-in component to VCF Operations Diagnostics.

As previous, Log Assist accelerates resolution of support cases, by providing the ability to generate log bundles and automatically attach property-based diagnostic findings data to the support case directly. Instead of this being done via a separate appliance and portal, as with Skyline Advisor, this functionality is now directly built into VCF. This feature does require external connectivity, which we do not have in the lab, thus this module is being provided as a recorded interactive simulation (iSIM) which will provide the ability to see and review the process in its entirety.

Login to VCF Operations

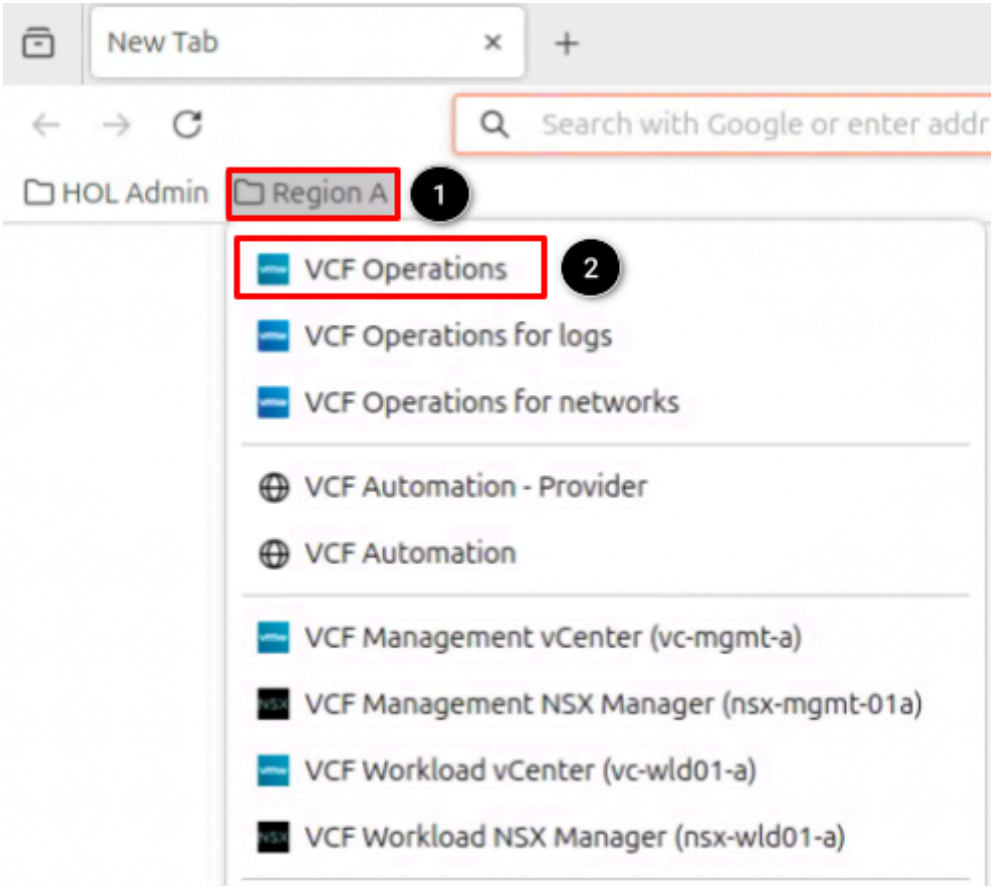
In the following few pages, we will walk through the process for logging in to VCF Operations.

Start Firefox

Open the Firefox Browser from the Linux Task Bar.

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

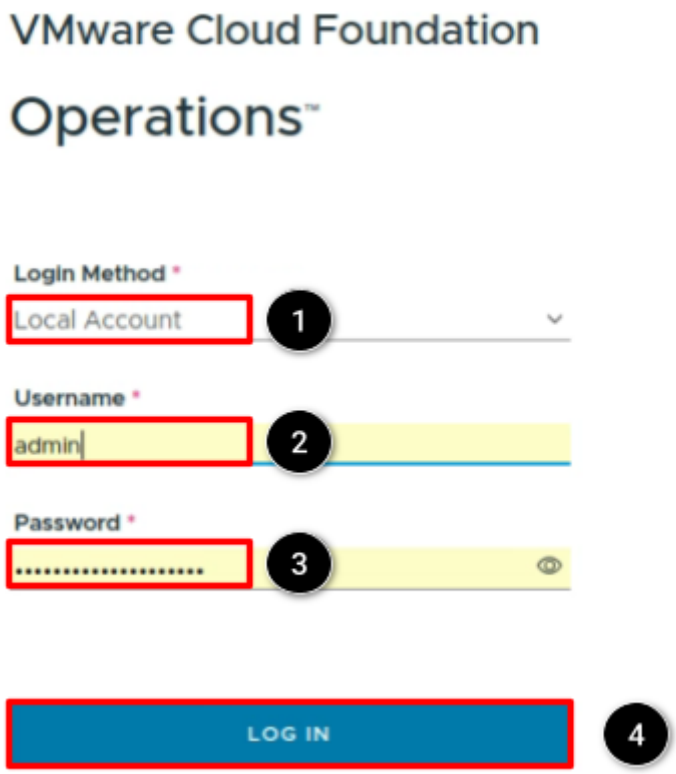
Open VCF Operations Console



Once Firefox has loaded:

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

Login to VCF Operations Console

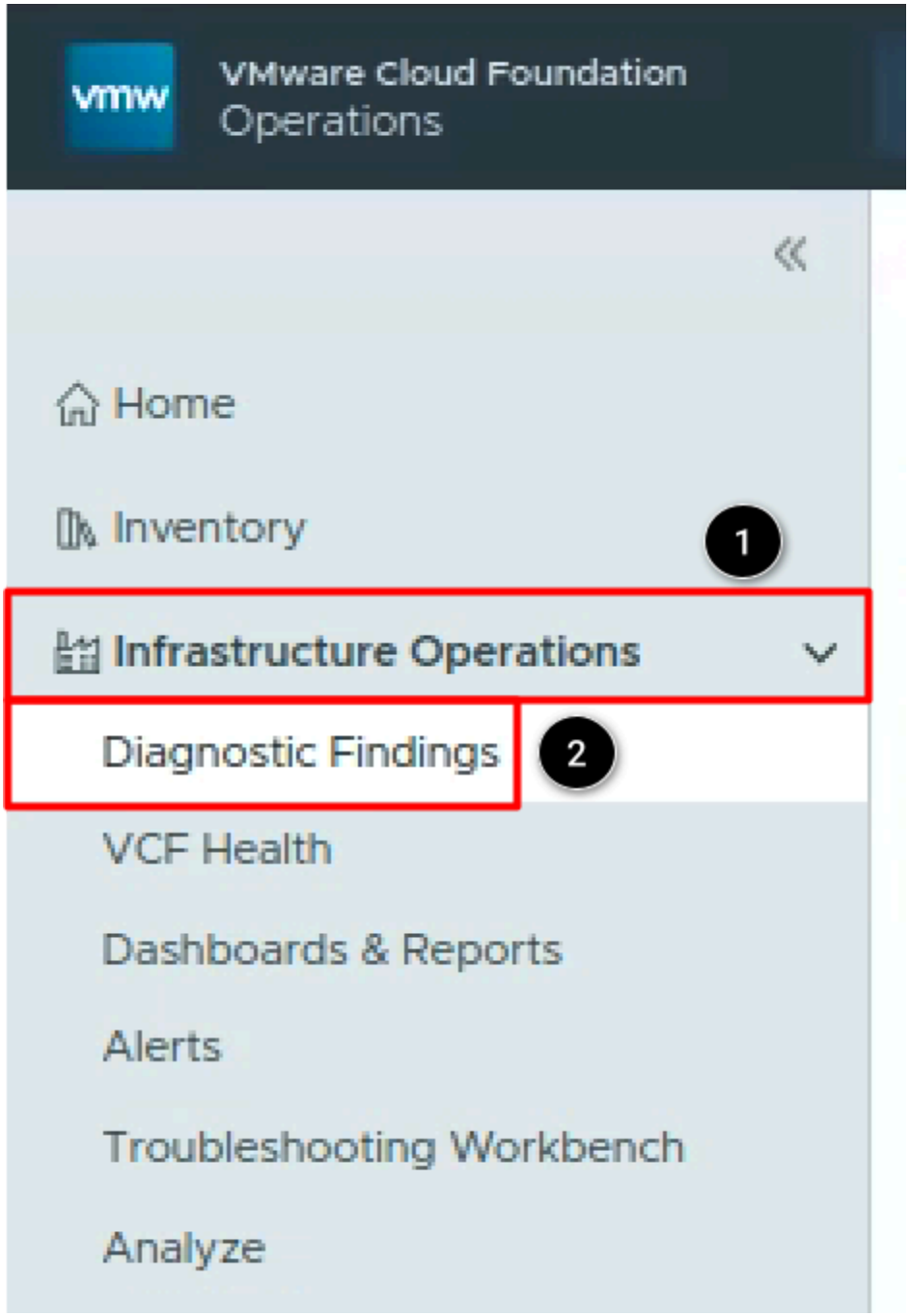


The credentials for **admin** should already be cached in the browser window.

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**.

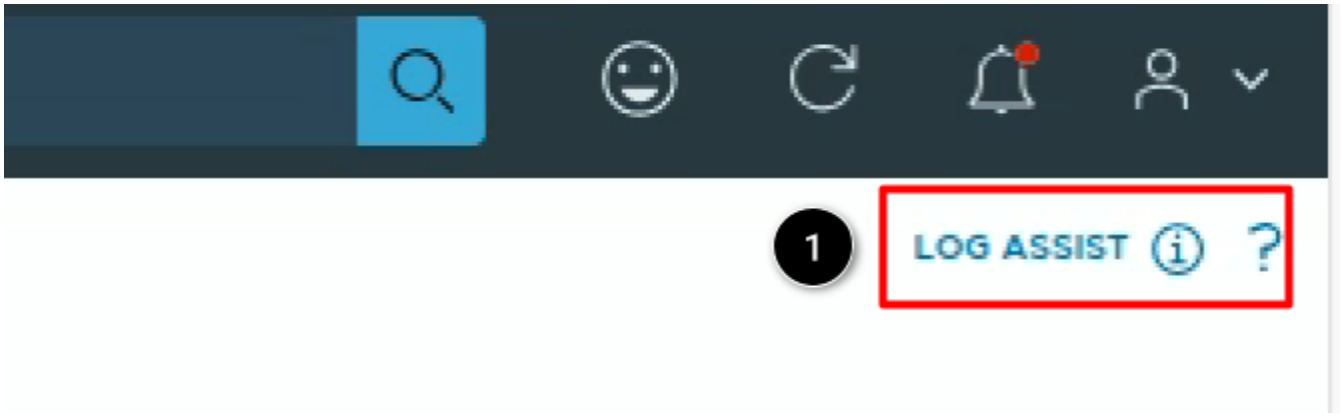
Access VCF Diagnostics



The **Log Assist** feature is a component of **VCF Diagnostic Findings**.

1. Click **Infrastructure Operations**.
2. Click **Diagnostic Findings**.

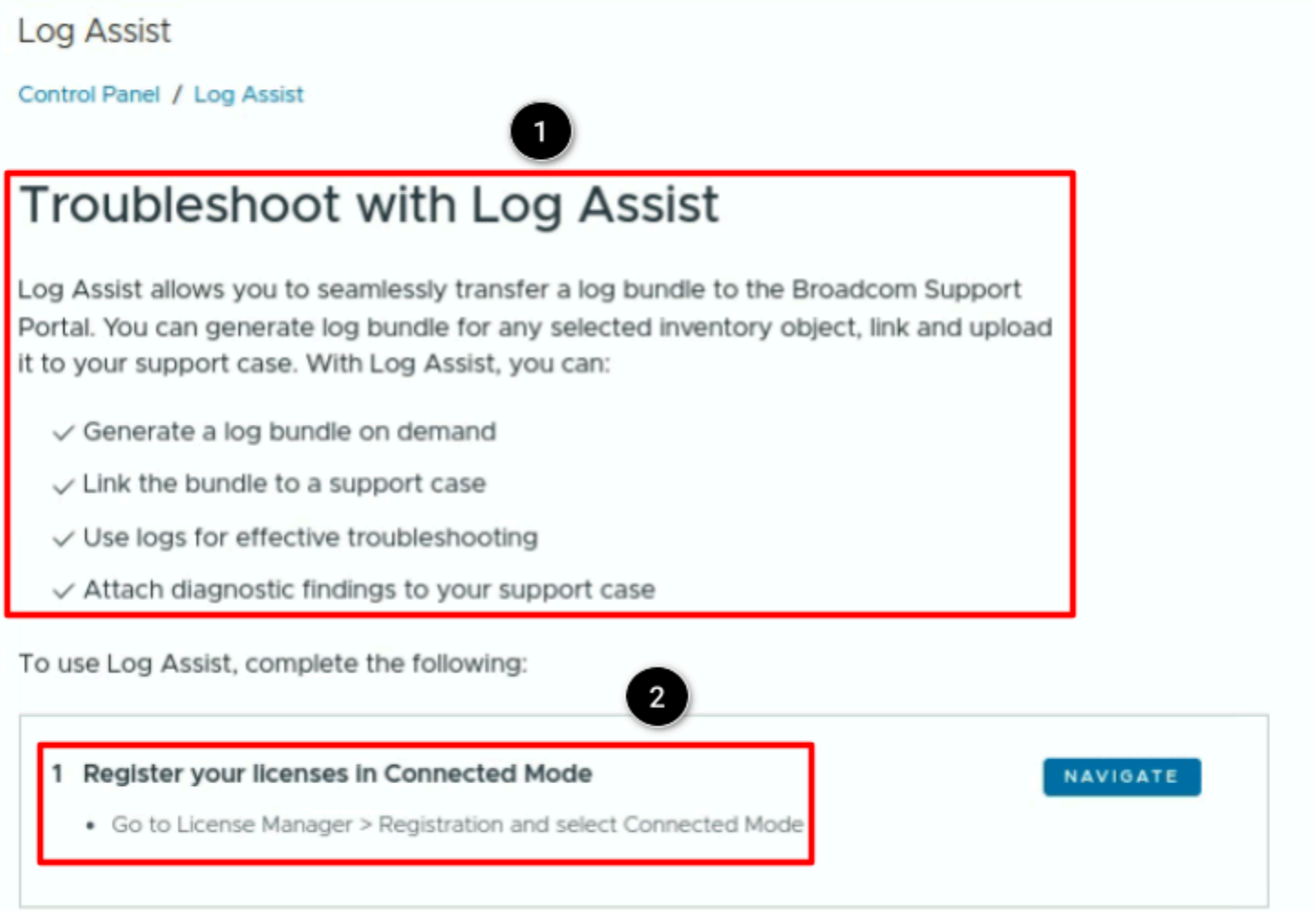
Access Log Assist



On the top right corner of the Diagnostics page there is a hyperlink to access **Log Assist**.

1. Click **LOG ASSIST**.

Log Assist Page

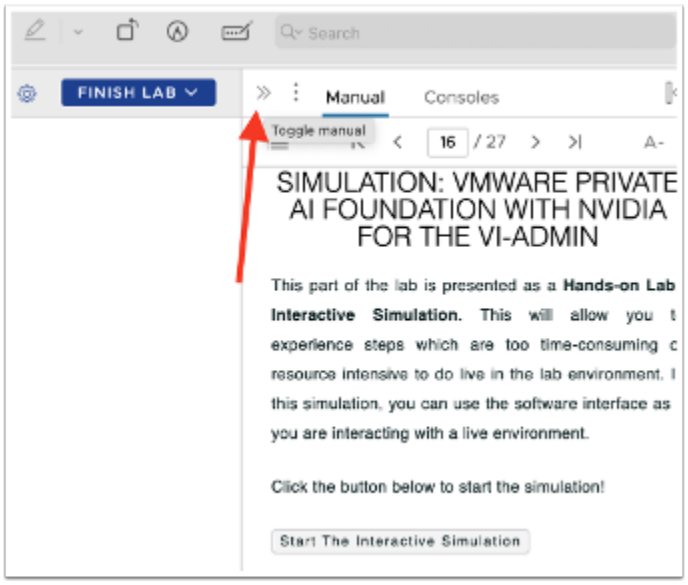


There are several steps which need to be completed in order to setup and configure **Log Assist** for use. While this configuration is outside the scope of this lab, the **Log Assist** page is where these tasks are performed.

1. As a point of reference, note what can be done with Log Assist in the **Troubleshoot with Log Assist** section.
2. Note that Log Assist requires **licenses in Connected Mode**. Connected Mode requires an Internet connection to obtain/maintain VCF subscription licenses. The lab is running in a Disconnected Mode state, thus why it has not been configured in this environment.
3. **Scroll down** to see additional requirements for setting up Log Assist (not shown).

Interactive Simulation – Log Assist

This part of the lab is presented as a Hands-on Labs Interactive Simulation. This will allow you to experience steps which are too time-consuming or resource intensive for the lab environment. In this simulation, you can use the software interface as if you are interacting with a live environment.
Click the button below to start the simulation!
[vlp:switch-console|HOL-2601-11-mod2_Diagnostic_Log_Assist|Start the Interactive Simulation]
You can hide the manual to use more of the screen for the simulation.



NOTE: When you have completed the simulation, click [vlp:switch-console|Console|Return to the Console] and continue with the lab.

Conclusion

In this lab, we noted how Log Assist no longer requires a separate appliance or portal, and how it is directly built into VMware Cloud Foundation 9 as part of VCF Diagnostics. We also reviewed an Interactive Simulation which showed how to use Log Assist to upload logs to Broadcom Support Cases.

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 - Monitor Your Environment and Prevent Issues with VCF Health (30 min) Advanced

Monitor, discover, and analyze the VCF environment to improve performance and availability. VCF Health in VMware Cloud Foundation Operations brings a level of visibility to your VCF environment generally, as well as insight into each component of VCF.

In this module we will examine the new VCF Health component in VMware Cloud Foundation Operations and how users can leverage it for visibility into VCF.

Login to VCF Operations

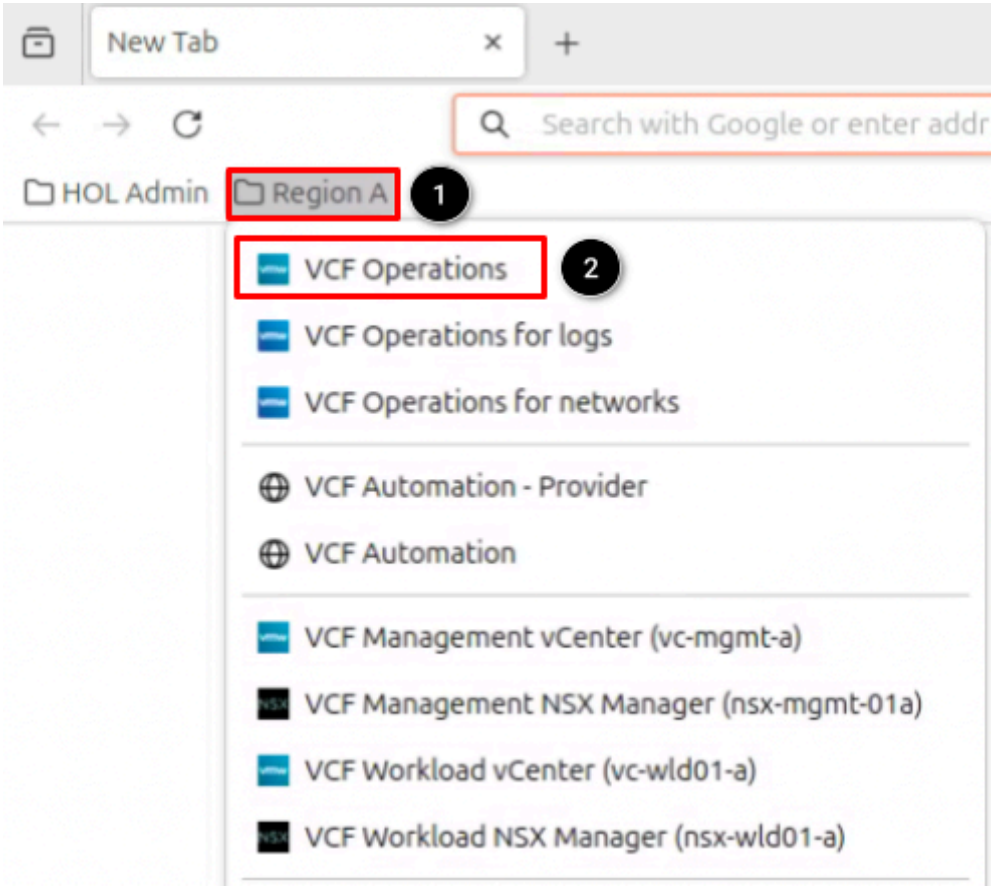
In the following few pages, we will walk through the process for logging in to VCF Operations.

Start Firefox

Open the Firefox Browser from the Linux Task Bar.

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

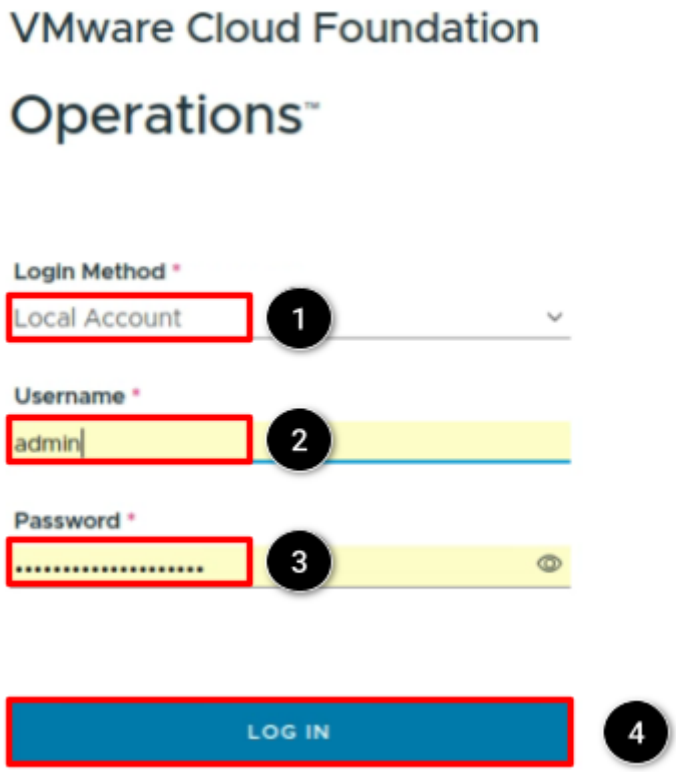
Open VCF Operations Console



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:

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**.

Introduction to VCF Health

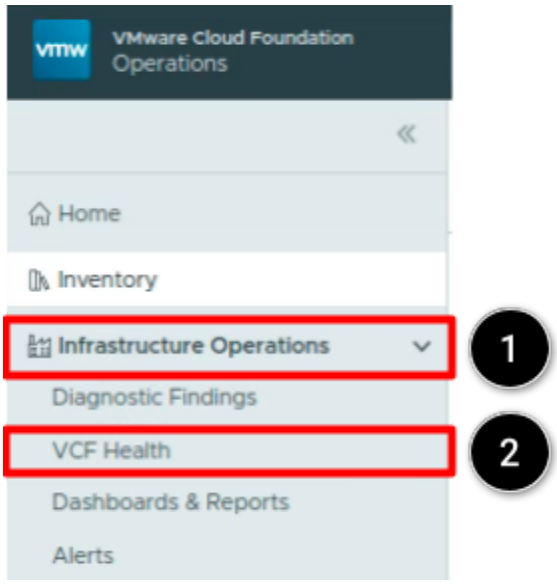
VCF Health for private cloud infrastructure administrators provides comprehensive oversight of the entire VCF stack, surpassing the functionalities of previous VMware products.

VCF Health offers two primary monitoring views: the Component View, which presents a holistic summary of all environmental objects, and the VCF View, which enables a detailed exploration from the management domain down to individual ESX hosts.

The screens within VCF Health are designed to assist with critical aspects of VMware Cloud Foundation platform setup and maintenance, drawing insights from support request data. This includes operational tasks such as configuring certificates, NTP synchronization, DNS reverse lookup, as well as tracking the performance of vCenter instances from an infrastructure perspective.

In this lab, we will show the two different VCF Health Views and how to dig deeper into identifying underlying issues in the lab environment. Due to the small scale of the lab and the minimal uptime, the manual images may differ from what is actually presented at the time of taking the lab, but it should provide enough information to help see the value of VCF Health and how it can help diagnose issues in Production environments.

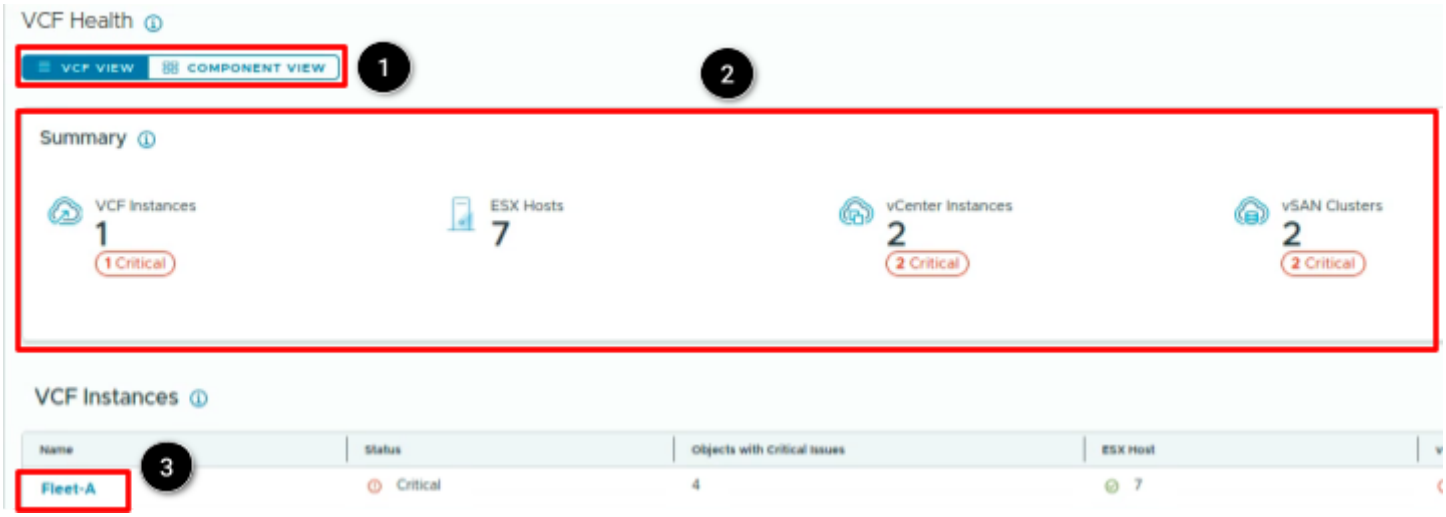
Access VCF Health



To access VCF Health:

1. Click on **Infrastructure Operations**.
2. Click on **VCF Health.**

VCF Health - VCF View

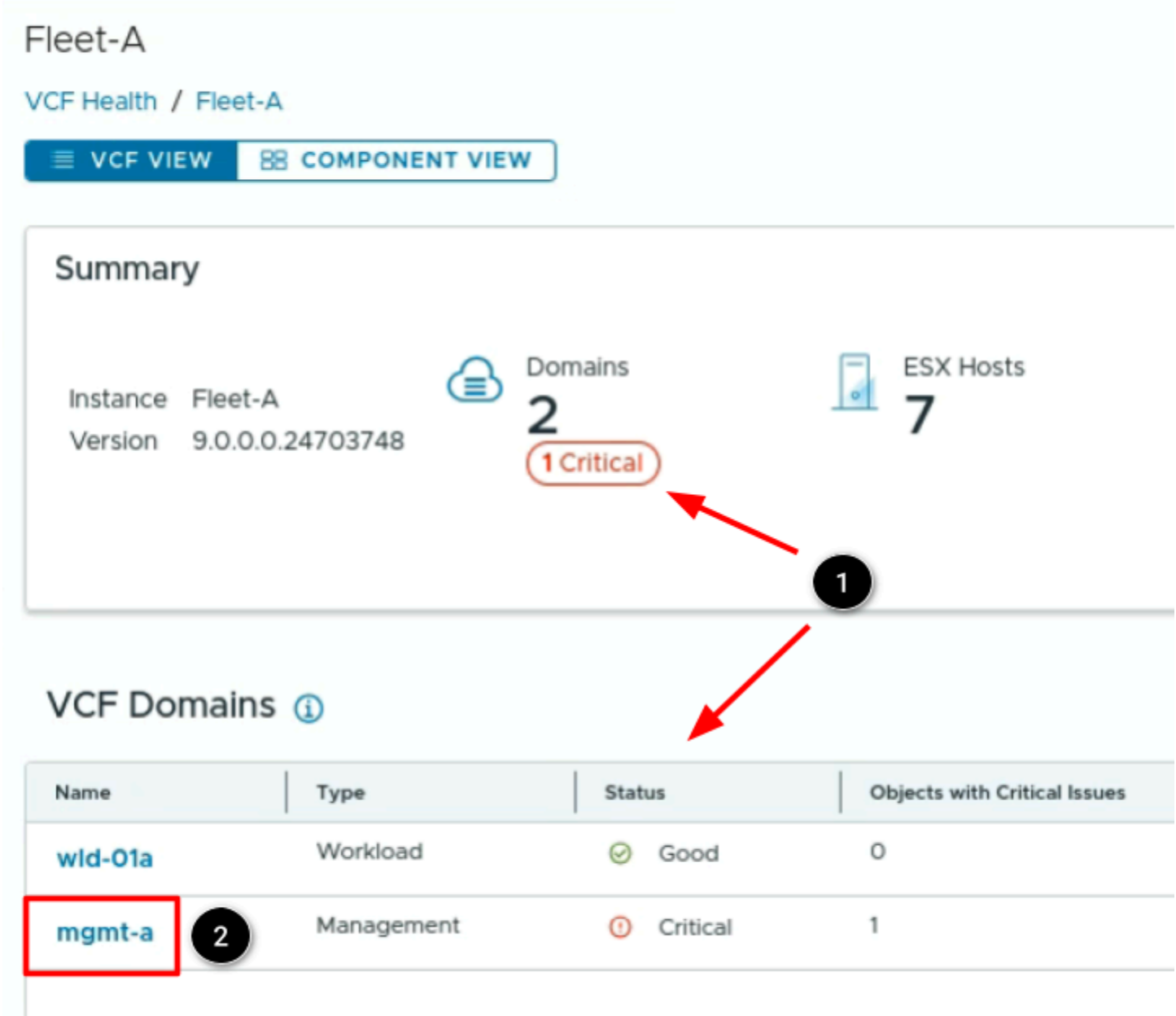


As mentioned previously, there are two Views available in VCF Health (VCF View and Component View). We will review both in this lab, but for now we will focus on the **VCF View**. Note that the errors displayed in the lab may differ from the one shown in the image.

1. Notice the **VCF View** is highlighted and is our default. The **VCF View** allows us to identify instances and domains where immediate attention is required. The **Component View** allows us to drill down into these specific issues and monitor for less important issues.
2. In the **Summary** section we see the different components that are being monitored. **Note:** The number of components and errors displayed in the lab may differ from the one shown in the image.
3. Let's start reviewing the health of our available VCF Instance. Select **Fleet-A**.

Note: The images throughout this section may not match what is seen in the lab due to the labs being "torn down and redeployed" on a regular basis. There may be more errors or no errors at the time of the lab; however, the concepts and actions taken will remain the same.

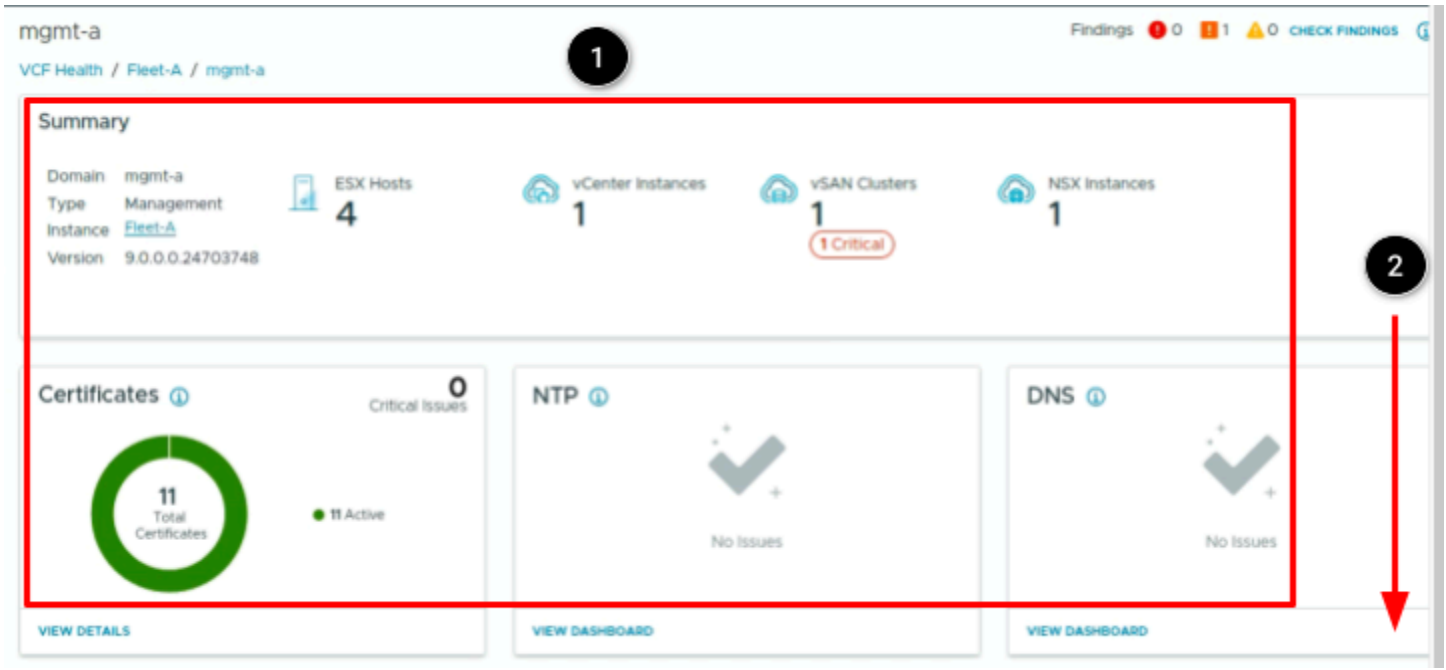
VCF Domains



In the lab, Fleet-A includes two VCF Domains (**wld-01a** and **mgmt-a**).

1. Notice in the image under Domains in the Summary section that we have 2 Domains and 1 has a Critical status (lab results may differ from image). We also see in the Status column of our VCF Domains the same information (2 Domains, 1 is Critical). Using the **VCF Domains** section, we easily identify that our **mgmt-a** domain is the one currently having issues.
2. Click **mgmt-a** to observe the VCF health details on this domain.

VCF Domain Health Overview

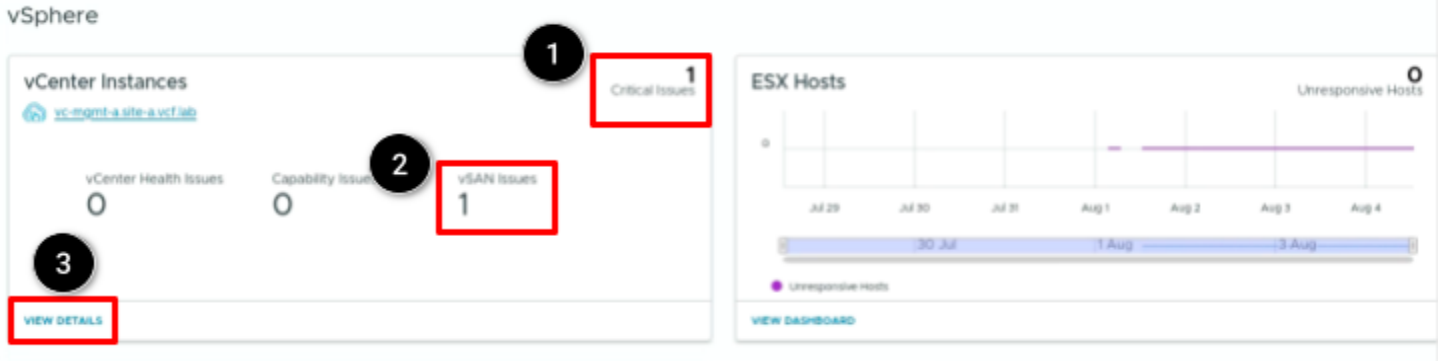


On the **mgmt-a** health page we see:

1. **Summary** – in this section, we see component totals for the **mgmt-a** VCF domain. In the image, we see a **vSAN Cluster** is reporting a critical alert. Other components in the image (Certificates, NTP, and DNS) are all reporting no issues.
2. **Scroll down** on this page to find the component that has triggered an alert.

Note: Each of the components on the page can be researched further as time allows in the lab. All components are covered in the *Monitoring Private Cloud Infrastructure With Diagnostic Findings and VCF Health* lab (2601-03), which provides a general overview of each. For this lab, we are focusing on troubleshooting an actual issue in the environment and thus why all components are not being reviewed.

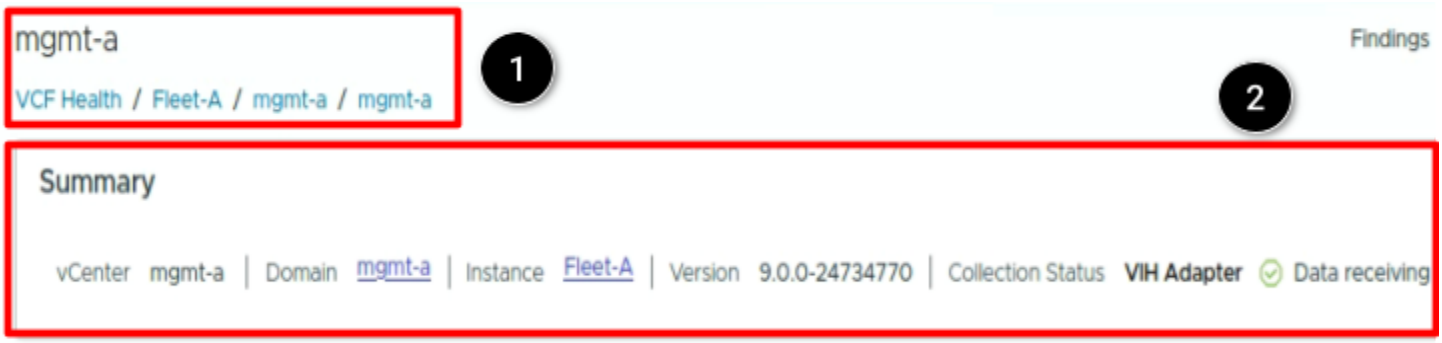
vSphere Health



Scrolling down farther, we see the **vSphere** section which shows the health of both **vCenter Instances** and **ESXi Hosts** that are part of the **mgmt-a** domain.

1. Notice we have **1 Critical Issue** in our **vCenter Instance**.
2. Specifically, we have **1 vSAN Issue** in the environment.
3. Let's dig deeper into this issue by clicking on **VIEW DETAILS**.

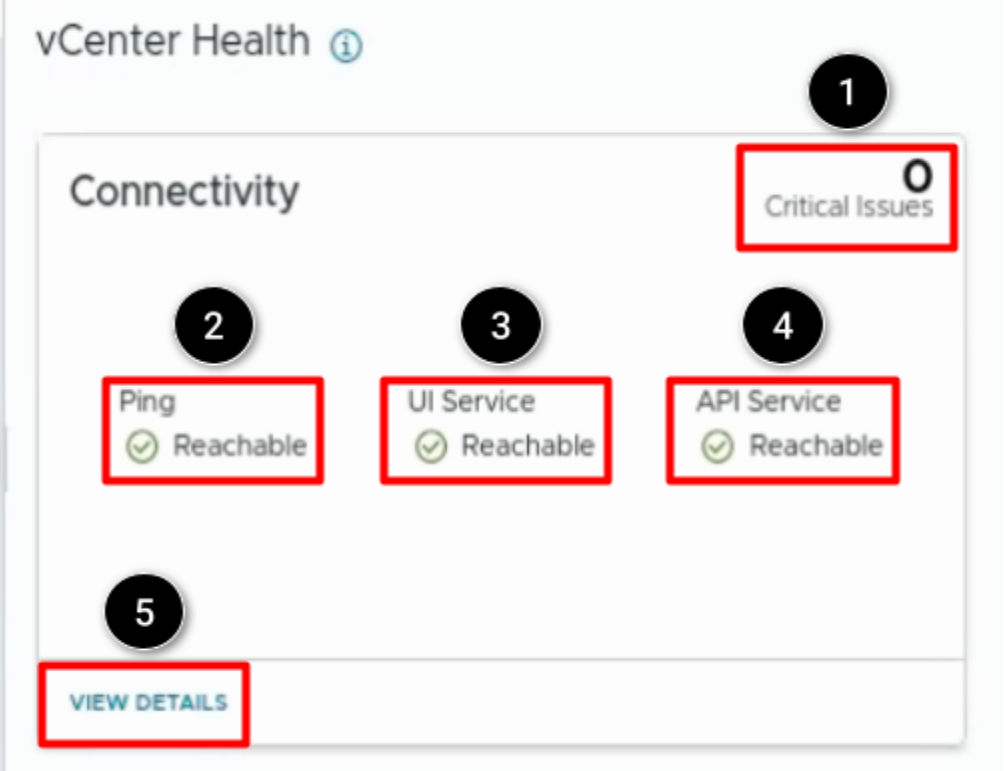
VCF Health Object Details Page



We are now on the VCF Health page for the specific object chosen. Over the next few pages, we'll review each of the components being shown on this page.

1. Note in the image we are viewing the **mgmt-a** object which is our vCenter appliance (lab vCenter name may differ).
2. In the **Summary** section, we see such items as the vCenter, Domain, Fleet, Version of VCF, and Collection Status for various adapters.

vCenter Health Connectivity



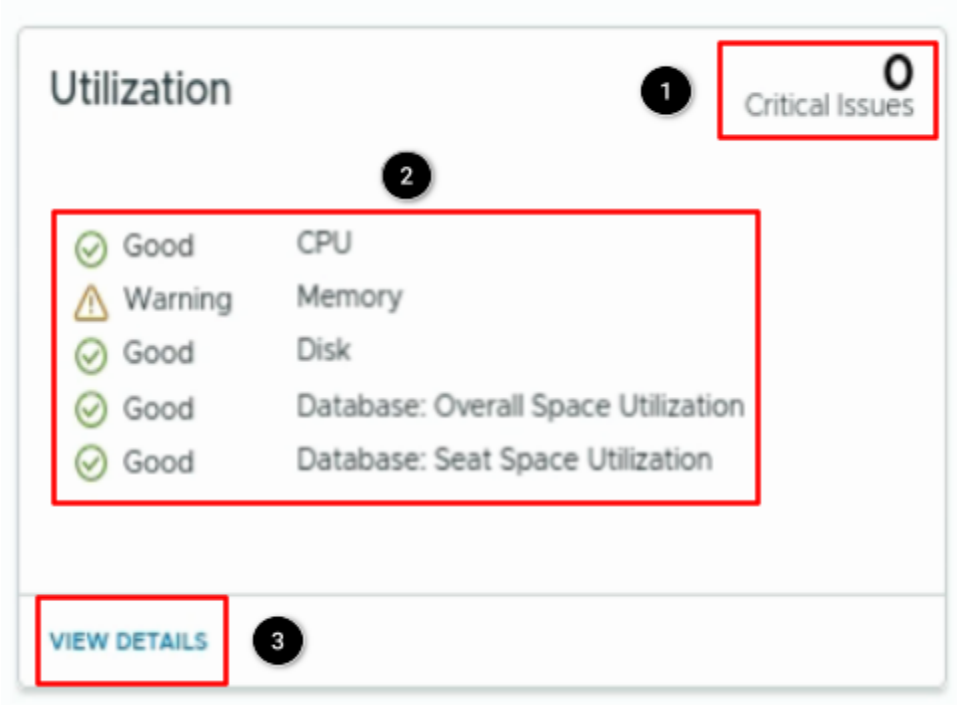
Next, we see **vCenter Health** which shows general vCenter Health: Connectivity, Utilization, Services, and more. As shown in the image, in the Connectivity tile we have the following.

1. There are **0 Critical Issues** in our vCenter.
2. **Ping Reachable** – the green checkmark indicates the vCenter is responding to ping.
3. **UI Service Reachable** – the green checkmark indicates the vCenter UI is available.
4. **API Service Reachable** – the green checkmark indicates the vCenter API is available.
5. Click **VIEW DETAILS** as this provides more details around Connectivity.

vCenter Health Connectivity Details

1. Notice we are in the **Connectivity** tab as denoted by the blue underline bar. Also, we see a quick glance of each service being monitored for Connectivity (Ping, UI Service, and API Service), and in the image we see all three are currently up and running.
2. **Ping** provides network availability of vCenter over the last 7 days – 1 indicates up, 0 indicates down. Note in the image the ping service was down (unavailable) for a period of time.
3. **UI Service** indicates availability of the vCenter UI – 1 indicates up, 0 indicates down. Notice in the lab manual image there was a loss of connectivity to the UI Service (likely during an upgrade and also corresponds to the missing pings noted above).
4. **Scroll down** and we'll also see the **API Service** (not shown in the image) which shows availability of vCenter API – 1 indicates up, 0 indicates down.
5. Click the **back arrow of the Internet Browser** to return to the VCF Health page (not shown).

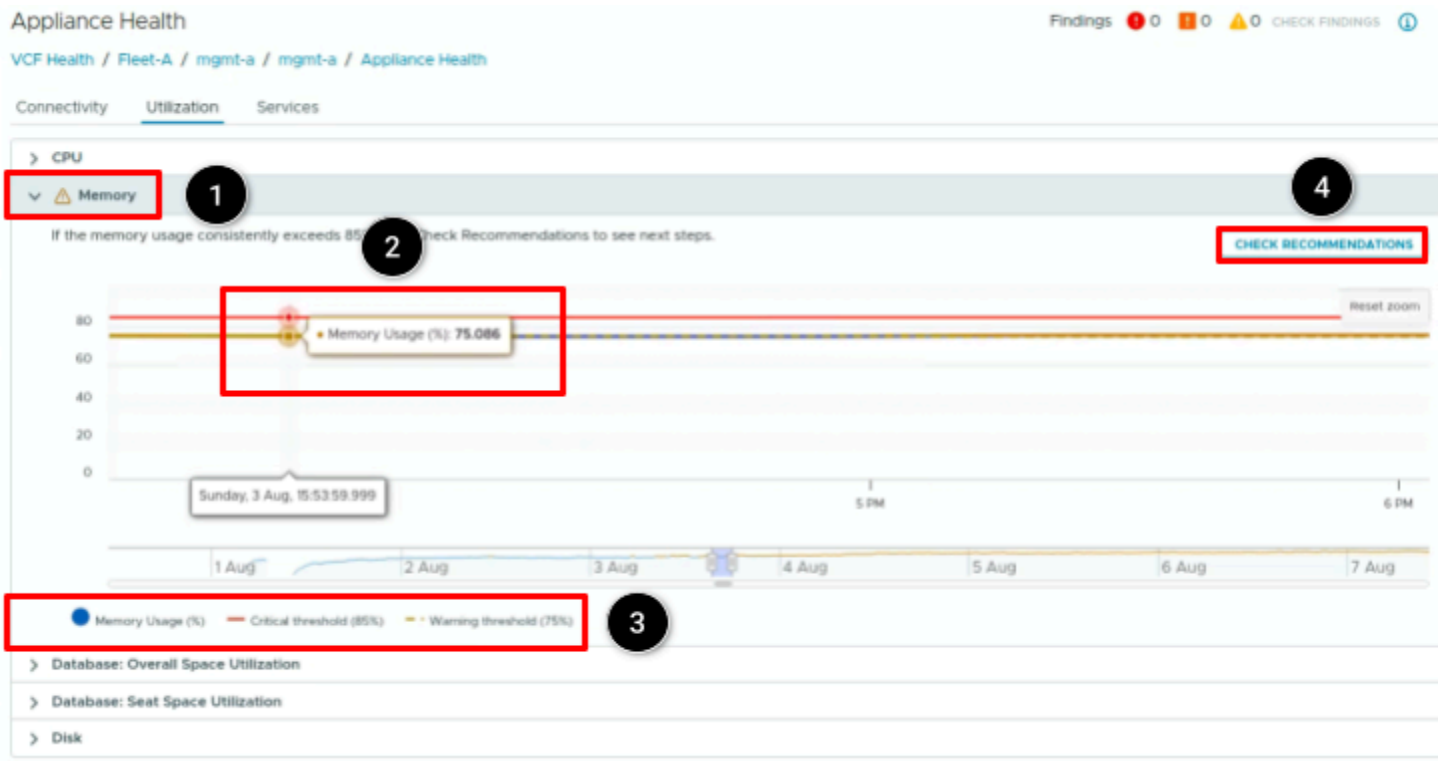
vCenter Health Utilization



The next tile under the vCenter Health section is **Utilization**.

1. **Critical Issues** shows any critical vCenter Utilization issues (if any).
2. The list of **CPU, Memory, Disk, and Database** shows any related utilization concerns. For instance, in the image we see a **Warning message** for the Memory on our vCenter.
3. Click **VIEW DETAILS** to see more details.

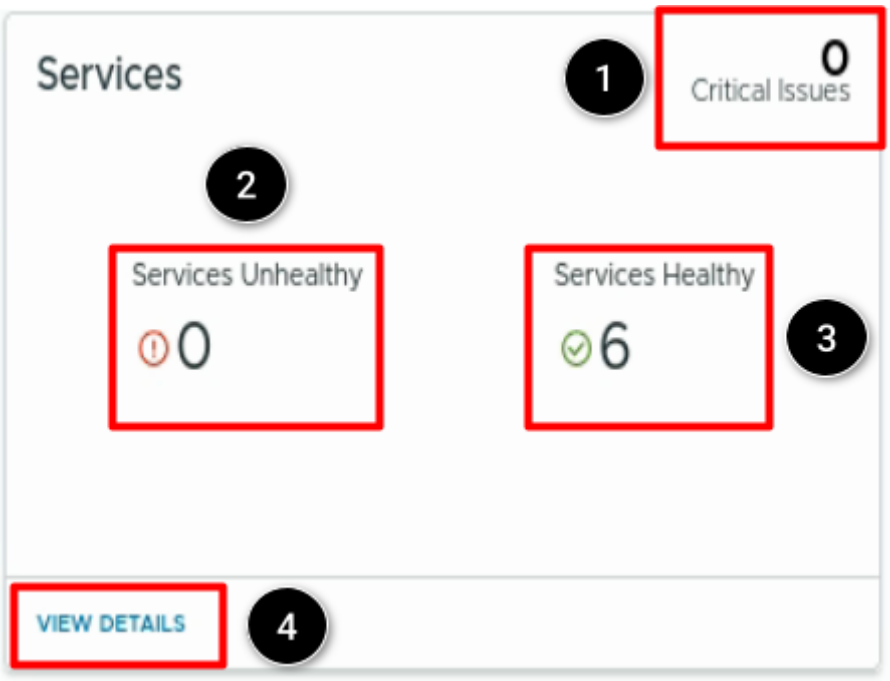
vCenter Health Utilization Details



We are now viewing the vCenter Appliance Health Utilization details. While we can see details on CPU, Memory, and Disk, let's focus on Memory which in the image example has a warning against it (may differ from the lab).

1. Expand the **Memory** section to see a graphical representation of the vCenter appliance memory usage over time.
2. Mouse over along the red line and we can see there are times when our **Memory Usage** exceeds 75% which is our configured threshold of when to trigger a Warning Alert.
3. Note the **Memory Usage Thresholds** for when alerts will be triggered.
4. Click **CHECK RECOMMENDATIONS** to see recommendations relative to the appliance resources shown here. Note: This opens a separate tab to an external KB article which may not work in the lab. Close the tab and return to VCF Health.
5. Click the **back arrow of the Internet Browser** to return to the VCF Health page (not shown).

vCenter Health Services

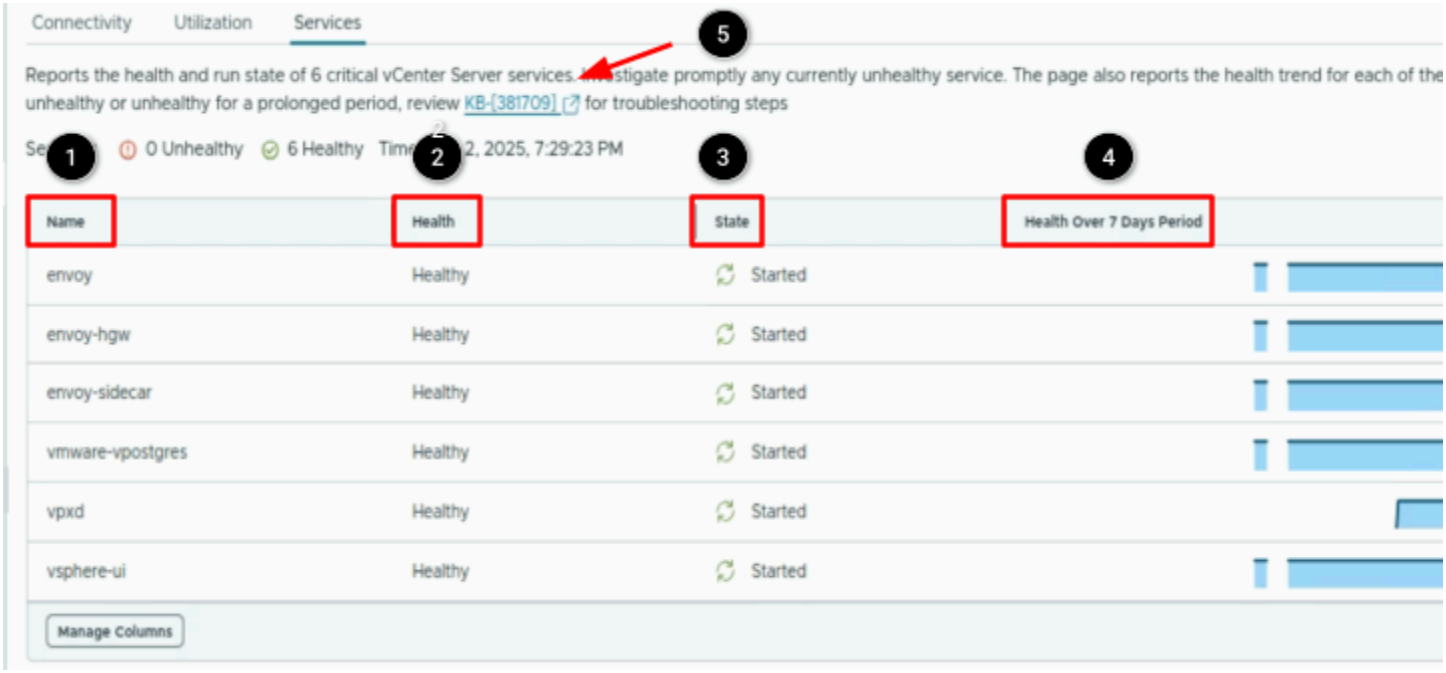


The next tile under the vCenter Health section is **Services**.

1. **Critical Issues** – denotes any critical issues for the Services in vCenter (if any).
2. **Services Unhealthy** – represents any unhealthy vCenter Services.
3. **Services Healthy –** shows the healthy vCenter Services being monitored. There are 6 total being monitored.
4. Click **VIEW DETAILS** which will provide more details around the 6 vCenter Services being monitored.

Note: The images throughout this section may not match what is seen in the lab due to the labs being "torn down and redeployed" on a regular basis. There may be more errors or no errors at the time of the lab; however, the concepts and actions taken will remain the same.

vCenter Health Services Details

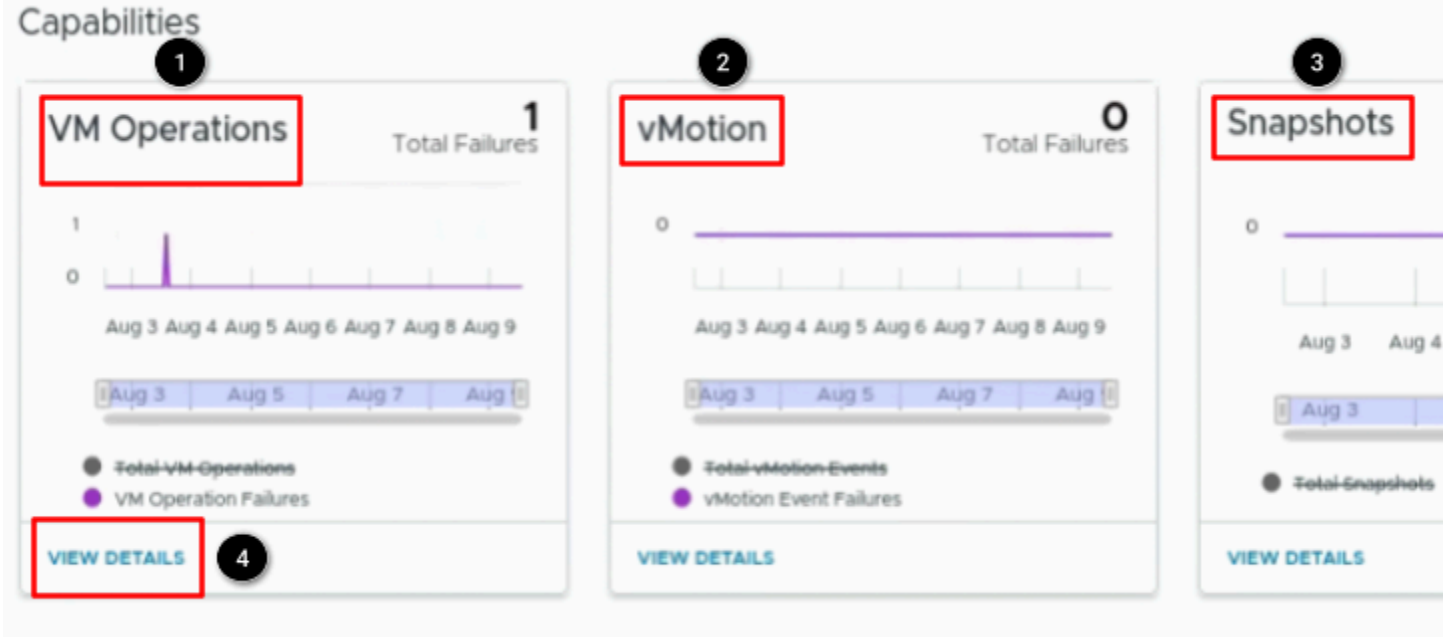


We are now viewing the health of the vCenter Appliance Services. Here we see:

1. **Name** – name of the vCenter Service being monitored.
2. **Health** – the health status of the vCenter Service.
3. **State** – the current state of the vCenter Service (Started or Not Started).
4. **Health Over 7 Days Period** – a graphical representation of the health of the vCenter Service over the last 7 days.
5. **KB-[381709]** is a link providing troubleshooting steps for vCenter Services via a KB (Note: This link may not work in the lab as it requires external connectivity).
6. Click the **back arrow of the Internet Browser** to return to the VCF Health page (not shown).

Note: The images throughout this section may not match what is seen in the lab due to the labs being "torn down and redeployed" on a regular basis. There may be more errors or no errors at the time of the lab; however, the concepts and actions taken will remain the same.

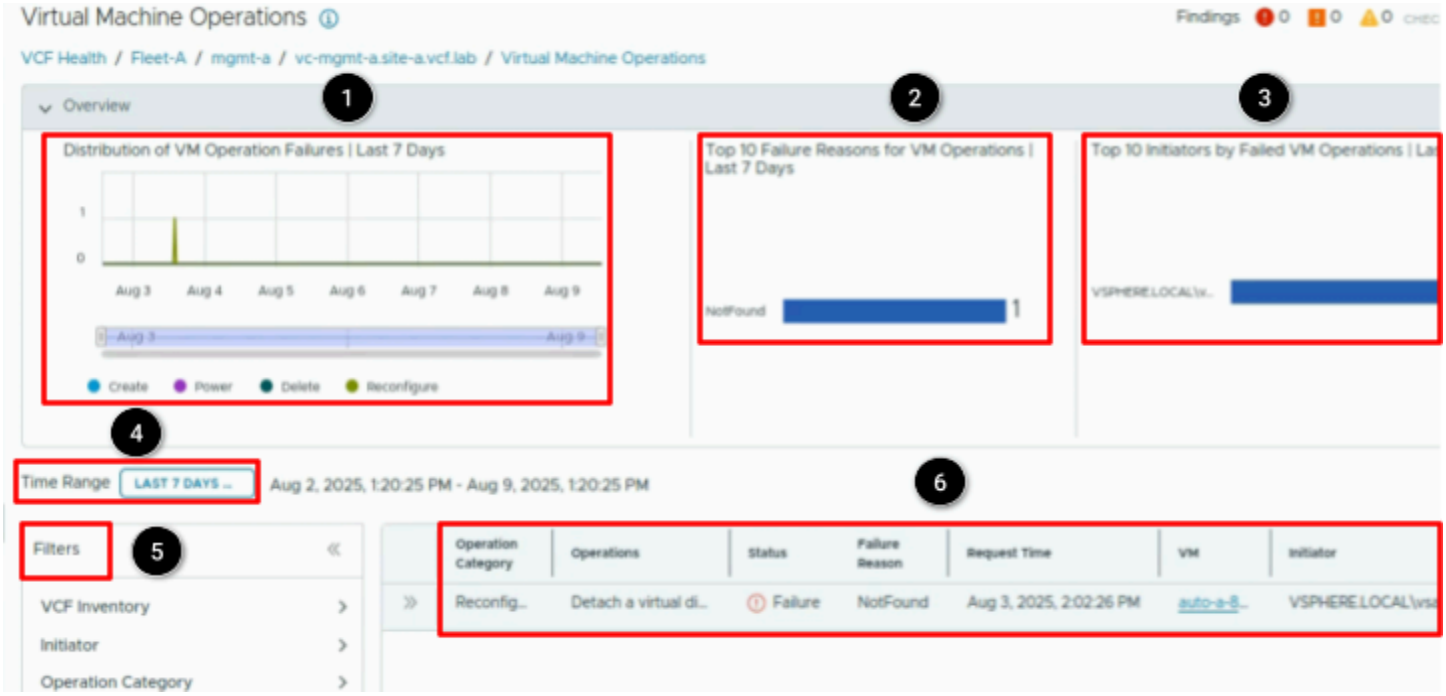
vCenter Health Capabilities VM Operations



Scrolling down further on the **VCF Health** page, we notice the **Capabilities** section and its tiles:

1. **VM Operations** – identifies all VM Operation Failures.
2. **vMotion** – identifies all vMotion Event failures.
3. **Snapshots** – identifies all failed snapshots, snapshots needing consolidation, and snapshots with long running consolidations.
4. Let's explore each of these Capabilities by first clicking **VIEW DETAILS** in the VM Operations tile.

vCenter Health Virtual Machine Operations

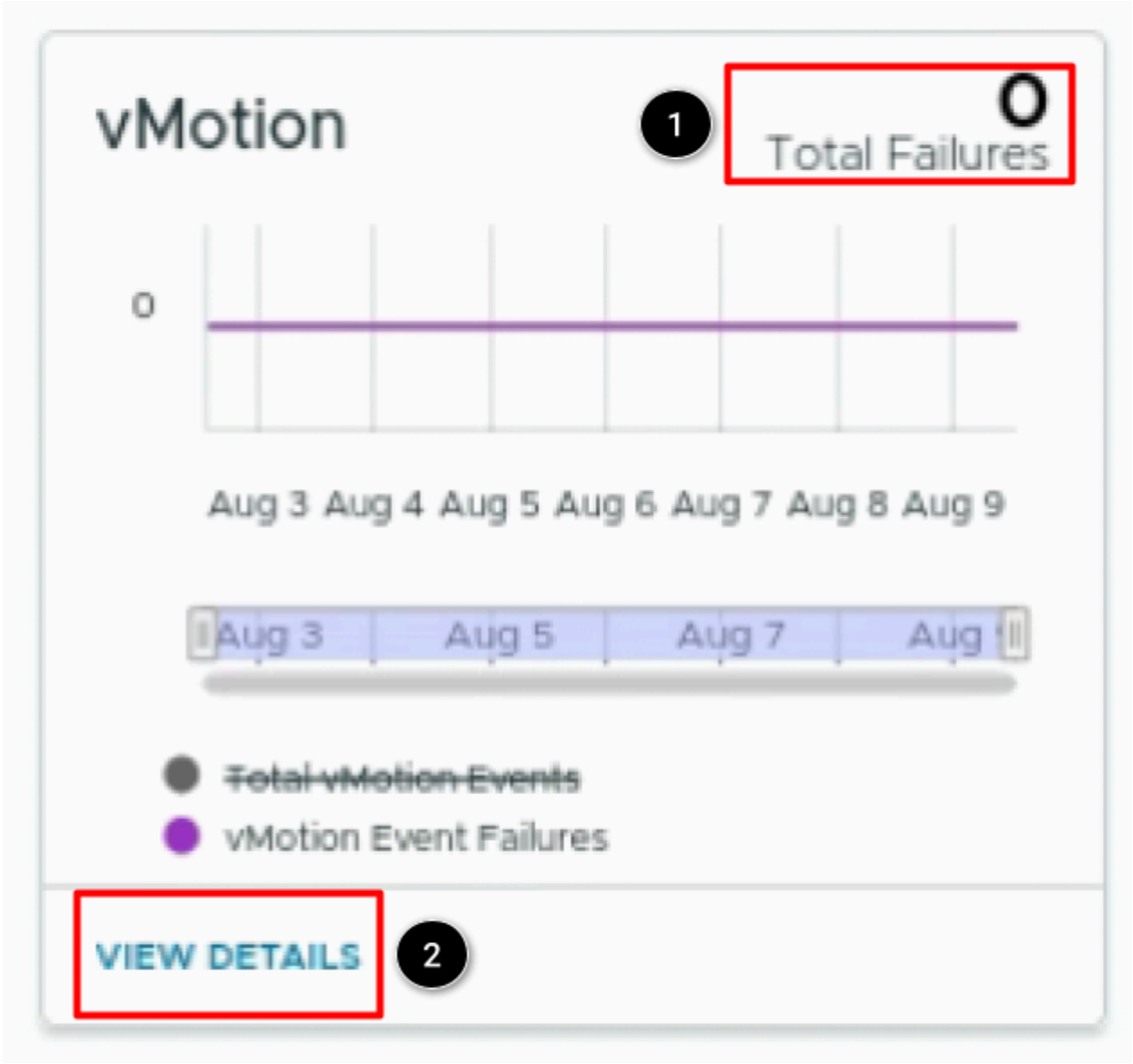


On the **Virtual Machine Operations** page, we see the following:

1. **Distribution of VM Operation Failures** – similar to the previous page, showing the VM Operation Failures over the last 7 days.
2. **Top 10 Failures Reasons for VM Operations** – top 10 most common VM Operation Failures over the past 7 days.
3. **Top 10 Initiators by Failed VM Operations** – top 10 most frequent initiators of VM Operations Failures over the past 7 days.
4. **Time Range** – time range to be displayed.
5. **Filters** – various filters to be used for details at right.
6. **Details** of the VM Operation Failure. If there is an item displayed, feel free to explore further using the **double arrow** icon next to the line item.
7. Click the **back arrow of the Internet Browser** to return to the VCF Health page (not shown).

Note: The images throughout this section may not match what is seen in the lab due to the labs being "torn down and redeployed" on a regular basis. There may be more errors or no errors at the time of the lab; however, the concepts and actions taken will remain the same.

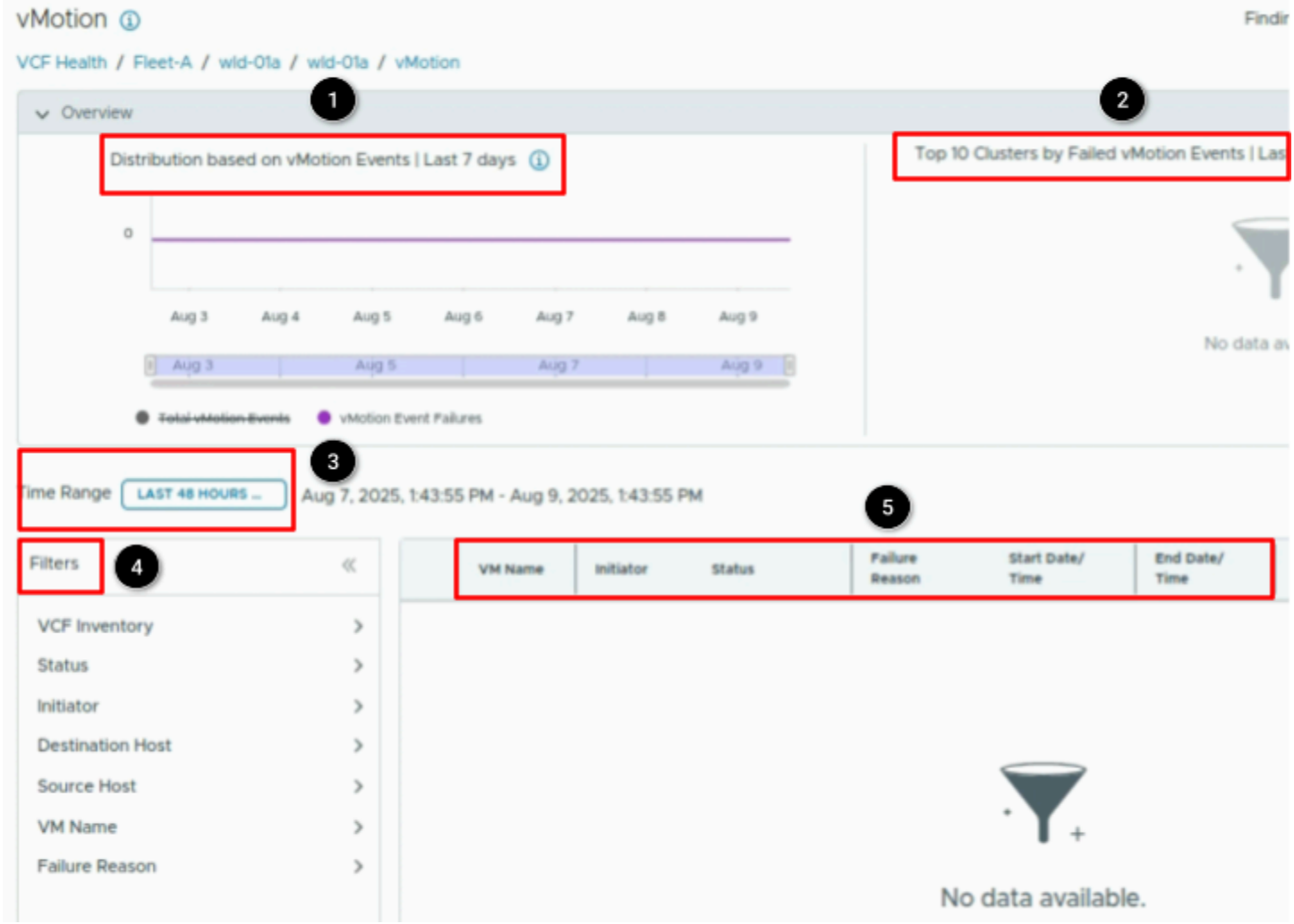
vCenter Health Capabilities vMotion



Returning to the **VCF Health** page, let's now review the **vMotion** tile.

1. **Total Failures** - total number of vMotion failures over the time period
2. Click **VIEW DETAILS** to see more information about vMotion failures.

vCenter Health Capabilities vMotion Details

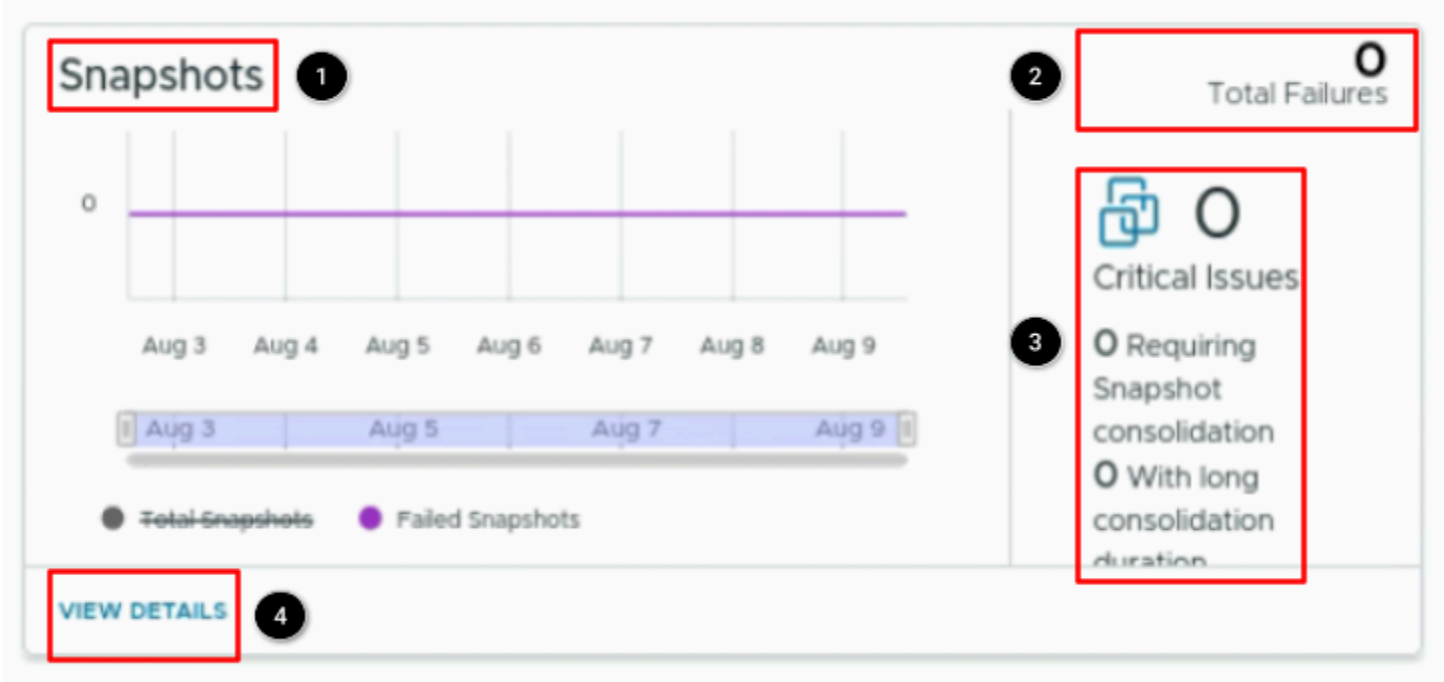


On the **vMotion** page, we see the following:

1. **Distribution based on vMotion Events** - graphical view of vMotion failures over the last 7 days.
2. **Top 10 Clusters by Failed vMotion Events** - top 10 Clusters with the most vMotion failures.
3. **Time Range** - time range for detailed data in the bottom charts.
4. **Filters** - filters to be used for detailed data in the right pane.
5. **Details of vMotion tasks and failures** – while there are likely no vMotion tasks or failures in the lab environment, notice the types of details if there were any. We would see which VM had a vMotion event (and if it was successful or failed), a reason for the failure (if applicable), when the vMotion process had started and ended, etc. With this information, we can easily follow up on vMotion--related failures across our entire environment.
6. Click the **back arrow of the Internet Browser** to return to the VCF Health page (not shown).

Note: The images throughout this section may not match what is seen in the lab due to the labs being "torn down and redeployed" on a regular basis. There may be more errors or no errors at the time of the lab; however, the concepts and actions taken will remain the same.

vCenter Health Capabilities Snapshots



Returning to the **VCF Health** page, let's now review the **Snapshots** tile.

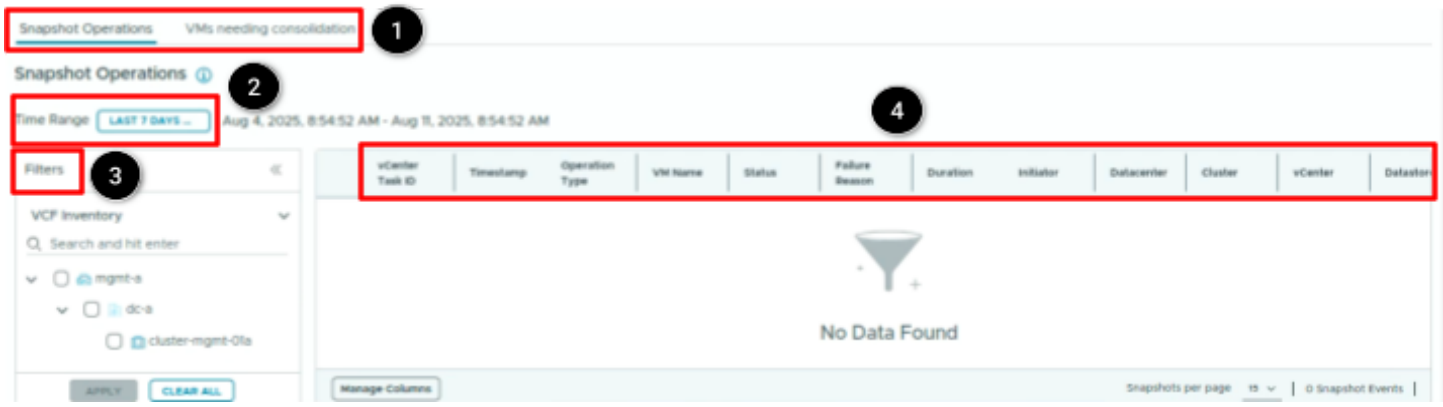
1. **Snapshots** – visual representation of Failed Snapshots over the last 7 days.
2. **Total Failures** – identifies the total failed Snapshots over the last 7 days.
3. **Critical Issues** – identifies critical issues, not necessarily Failed Snapshots. This section also identifies Snapshots requiring consolidation and Snapshot consolidations that are long running.
4. Click **VIEW DETAILS** to see more information about Snapshots.

vCenter Health Capabilities Snapshots Details

On the **Snapshots** page, in the **Overview** section we see the following:

1. **Distribution of Total and Failed Snapshots** – Graphical view of the last 7 days of total and failed snapshots in the environment.
2. **Top 10 VMs by Failed Snapshots** – top 10 VMs with failed Snapshots.
3. **Top 10 Initiators by Failed Snapshots** – top 10 initiators of failed Snapshots.
4. **Distribution based on deletion/consolidation time** – Snapshots taking the longest to delete/consolidate.
5. **Critical Issues** – Snapshots requiring consolidation and long running Snapshot consolidation jobs.
6. **Scroll down** to view the **Snapshot Operations** section.

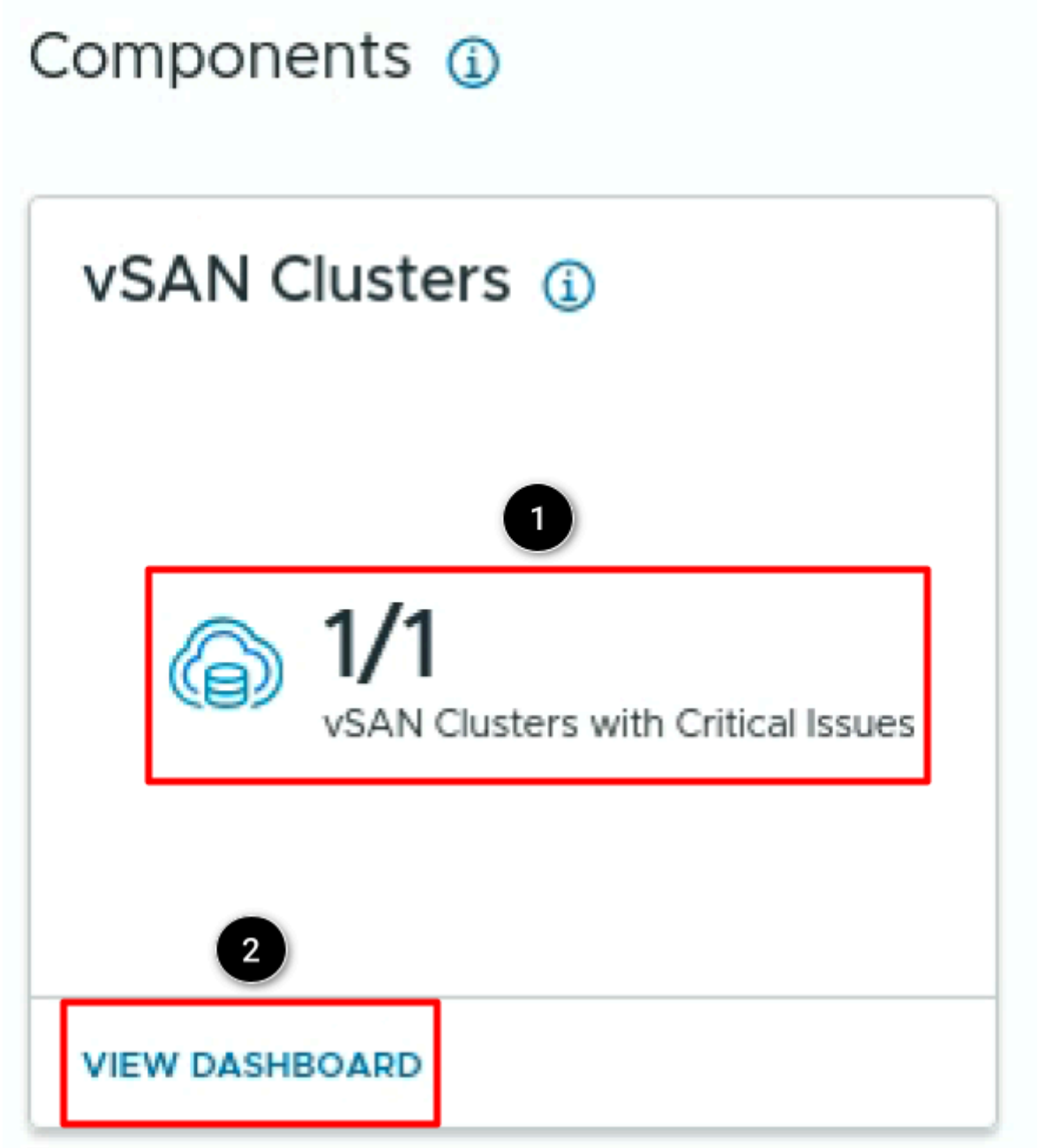
vCenter Health Capabilities Snapshots Details - Continued



On the **Snapshots** page, in the **Snapshot Operations** section we see the following:

1. Notice we are in the **Snapshot Operations** view and we can change to the **VMs needing consolidation** view if desired.
2. **Time Range** - time range for detailed data in the bottom charts.
3. **Filters** - filters to be used for detailed data in the right pane.
4. **Details of Snapshot tasks and failures** – while there are likely no Snapshot tasks or failures in the lab environment, notice the types of details if there were any. We would see which VM had a snapshot, if the snapshot was successful or had a failure, a reason for the failure (if applicable), how long the snapshot process took (duration), etc. With this information, we can easily follow up on Snapshot–related failures across our entire environment.
5. Click the **back arrow of the Internet Browser** to return to the VCF Health page (not shown).

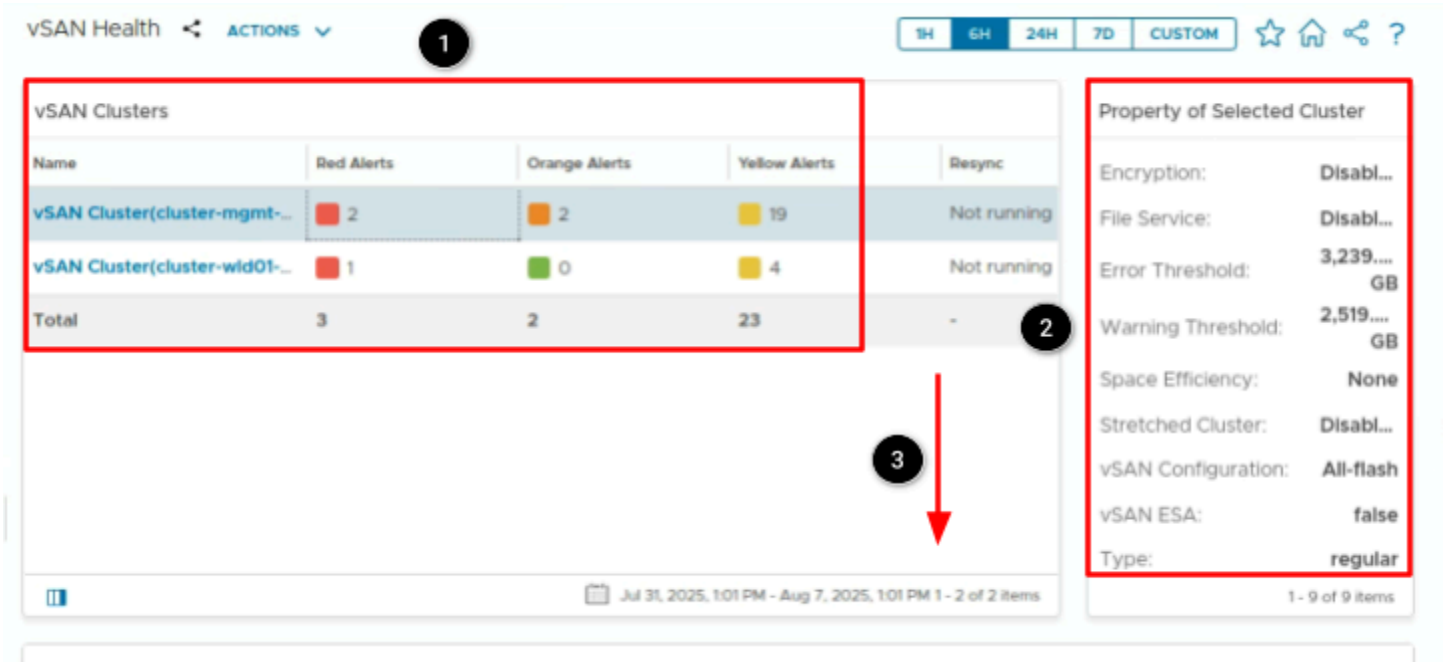
Components - vSAN Clusters



Scrolling down to the bottom of the **VCH Health** page for our vCenter, we see the **Components** section which includes the **vSAN Clusters** tile. This is tracking if the health score of a vSAN Cluster is below 60 or has critical alerts.

1. In the image, we see our environment is reporting a **vSAN Cluster with Critical Issues**.
2. Let's dig deeper into these issues by clicking **VIEW DASHBOARD**.

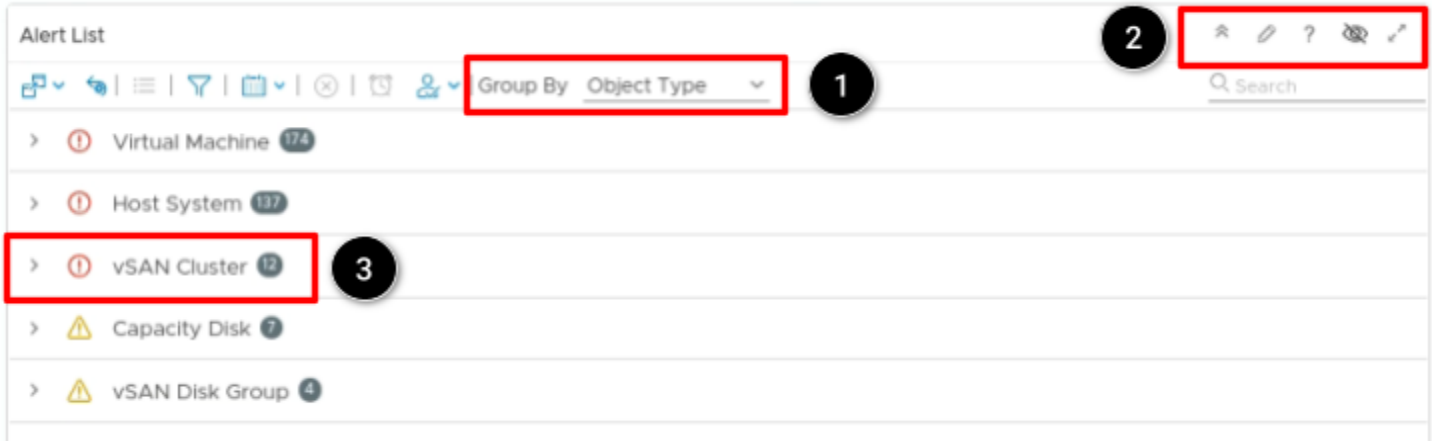
vSAN Health Dashboard Overview



We are now viewing the **vSAN Health Dashboard**. Here we see the following:

1. We see our **vSAN Clusters** and how many color-coded alerts each of them have.
2. Click on the first vSAN cluster line (somewhere next to one of the numbers in the columns, but not the hyperlinked object itself). Doing this will populate the **Property of Selected Cluster** widget we see on the right side.
3. Scroll down on the page to see the Alert List widget associated with vSAN Health.

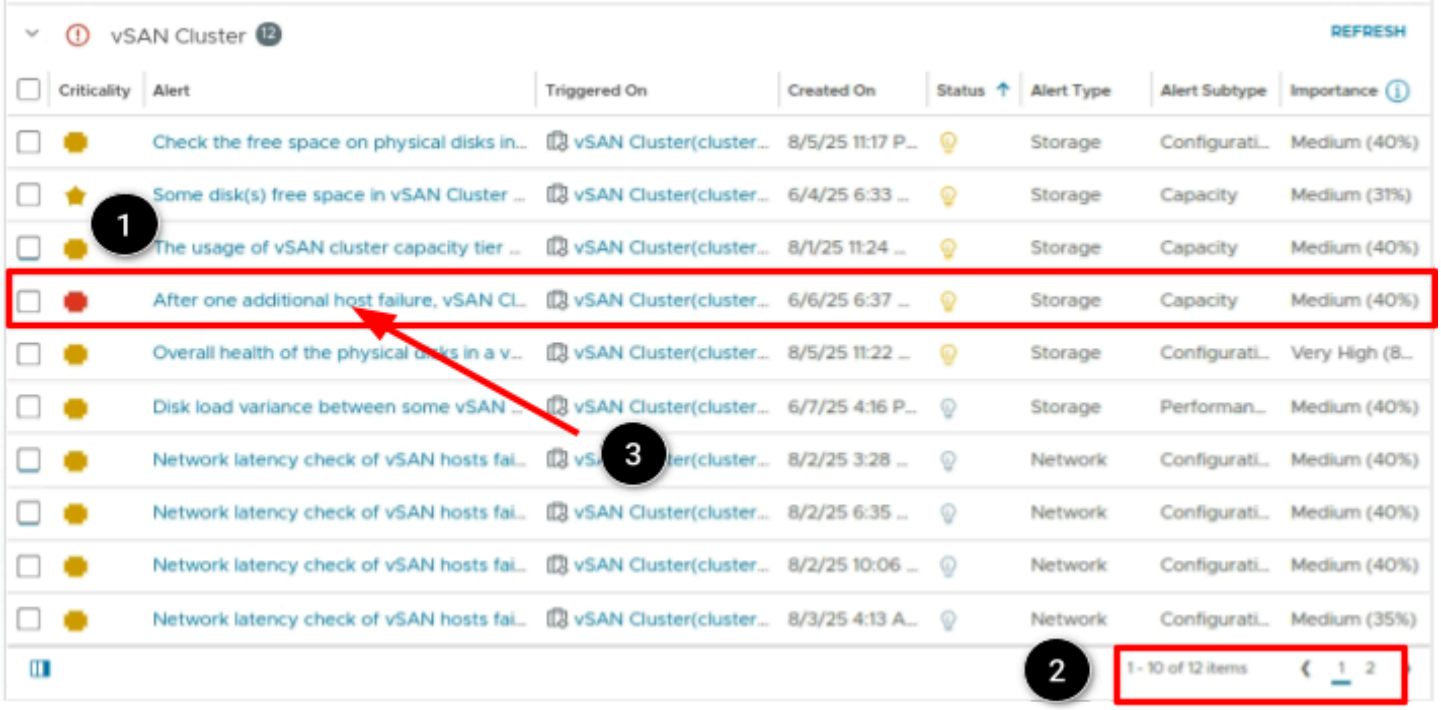
Alert List Widget



Throughout this lab, we've been walking through VCF Health to determine the actual vSAN cluster issue we have in our environment. With the **Alert List** widget, we can identify specific alerts/issues with the various objects in the environment.

1. Using the toolbar, change the **Group By** field to **Object Type**. We've been tracking a vSAN cluster issue, so we want to group all related alerts into this specific Object Type.
2. (Optional) – If the toolbar shown in the image (and used for Step 1) is not currently displayed, mouse over the top right corner and select the "eye icon" to unhide the toolbar.
3. Click the **down arrow** next to the **vSAN Cluster** Object Type to reveal all alerts in this category.

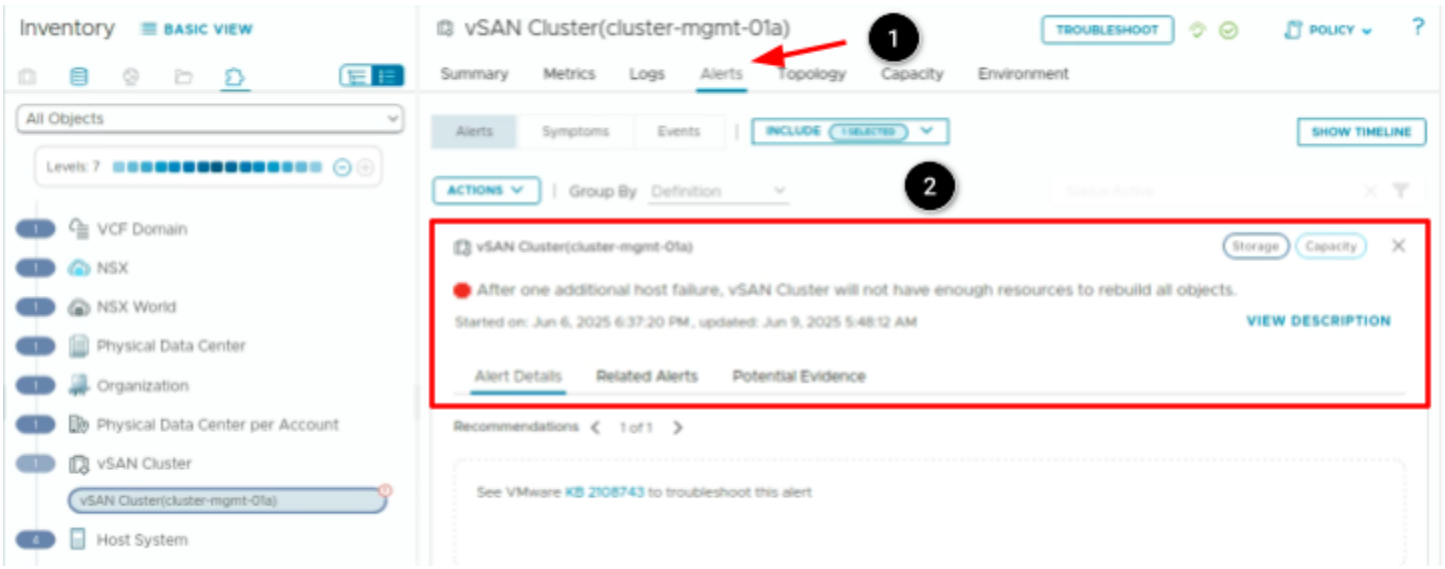
vSAN Cluster Alerts



Earlier in the lab, we saw notifications identifying one Critical issue on our vSAN Cluster. We are now looking at ALL alerts related to our vSAN Cluster Object Type and we see:

1. Notice the **Critical Alert** as identified by the **red icon**.
2. (Optional) If an Object Type has many alerts there may be multiple pages we could scroll through as shown here.
3. Click the hyperlink of the **Critical Alert**.

vSAN Cluster Object View

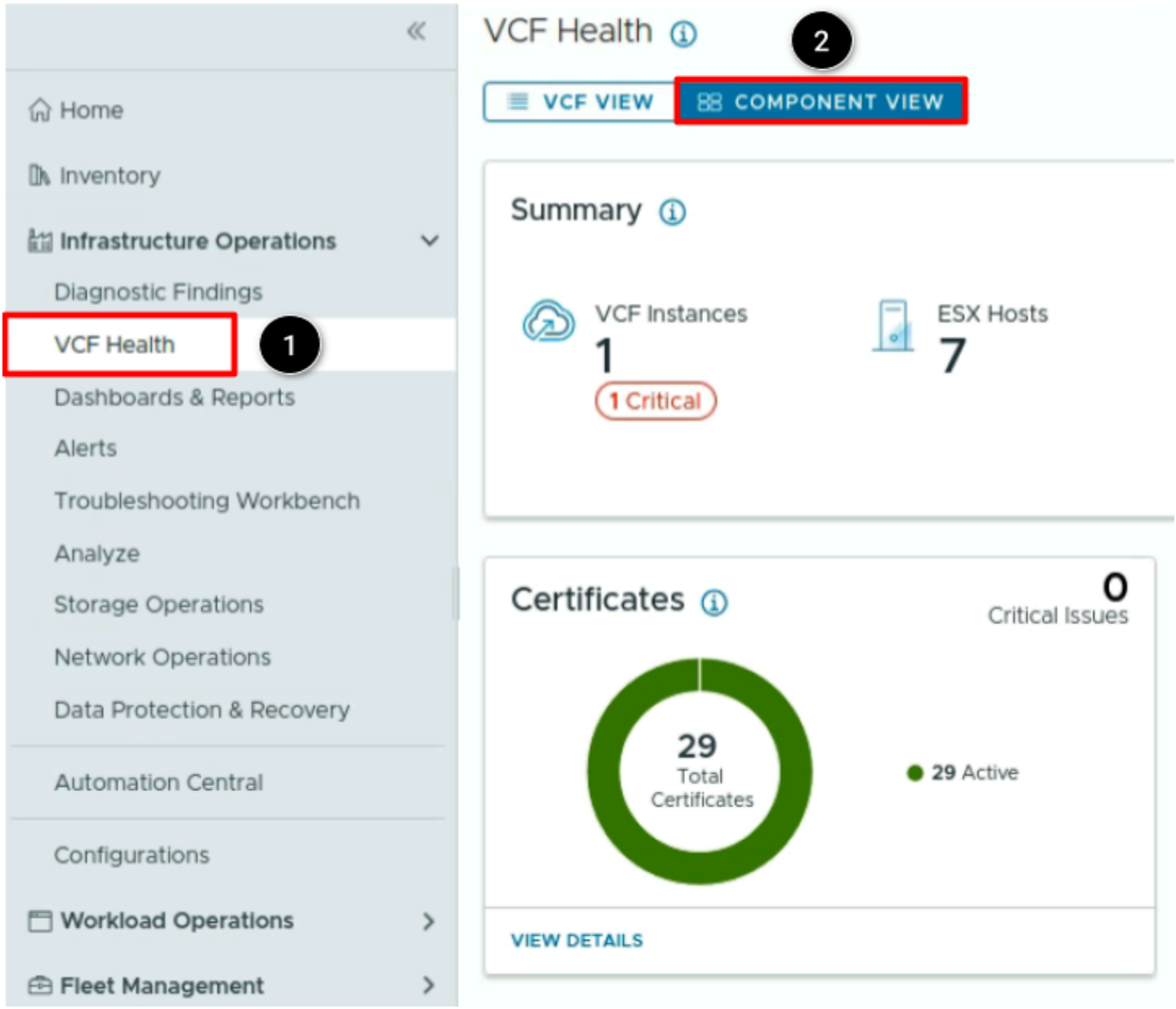


We are now viewing the details of the specific vSAN Cluster that is reporting a Critical Alert.

1. Notice we are viewing **Alerts** for this object as denoted with the blue line under the tab heading. Note: Though outside of this particular lab, there is a LOT of information in the Object View, so feel free to select the various tabs (Summary, Metrics, etc.) as time allows.
2. Here we see the **Alert Details** of the Critical Alert we've been researching. Notice it tells us "**After one additional host failure, vSAN Cluster will not have enough resources to rebuild all objects**." In a lab environment with minimal resources, that may be expected, but in a Production environment that would definitely be a critical alert and one that needs to be resolved immediately by adding more resources.

Congratulations! We've successfully used VCF Health (VCF View) to track down a Critical Alert in our environment. Let's now track the same issue through the VCF Health Component View.

VCF Health - Component View

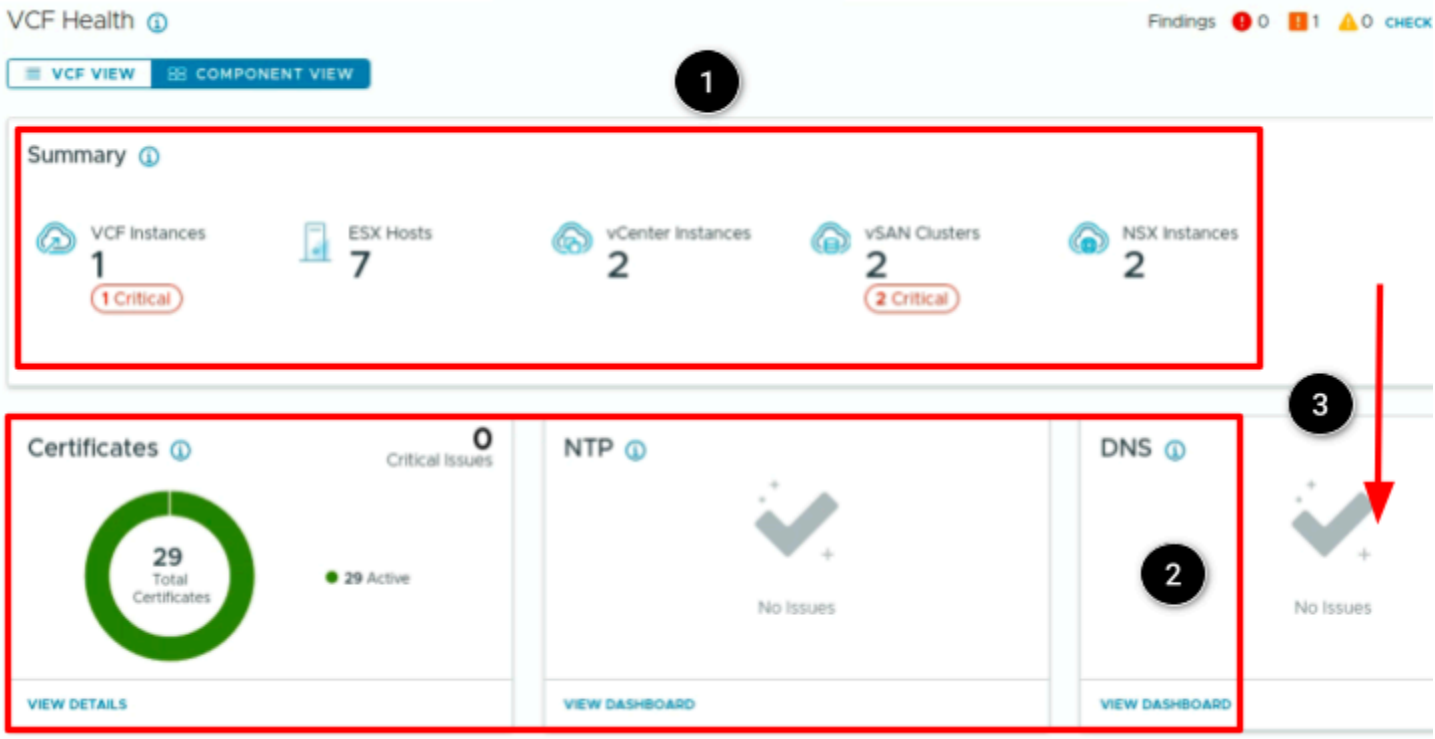


Let's restart our VCF Health view by doing the following:

1. Select **VCF Health** from the left menu.
2. Select the **COMPONENT VIEW** tab.

Note: The images throughout this section may not match what is seen in the lab due to the labs being "torn down and redeployed" on a regular basis. There may be more errors or no errors at the time of the lab; however, the concepts and actions taken will remain the same.

Component View Page

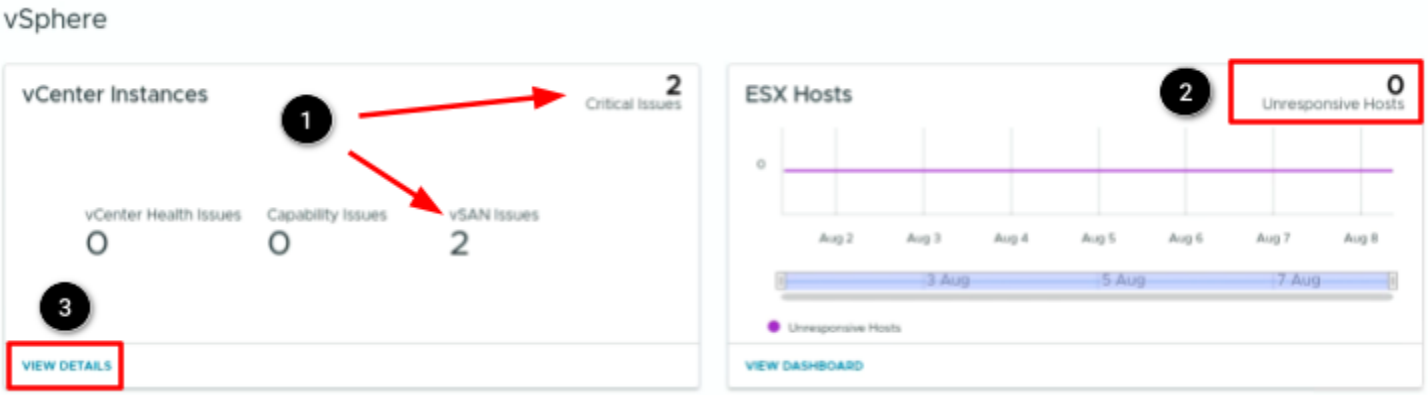


On the **Component View** Page, we see various tiles related to our environment.

1. **Summary** – Here we see a brief overview of our environment. Notice this is the same **Summary** View we saw in the VCF VIEW we discussed previously. In the image shown, we see there is 1 VCF Instance and 2 vSAN Clusters that have Critical Alerts in the environment. We will use VCF Health to track down those issues in this lab.
2. In this section, we see tiles related to **Certificates, NTP,** and **DNS**. These are currently showing no issues in the environment.
3. **Scroll down** to see more tiles related to VCF Health.

Note: Each of the components on the page can be researched further as time allows in the lab. All components are covered in the *Monitoring Private Cloud Infrastructure With Diagnostic Findings and VCF Health* lab (2601-03), which provides a general overview of each. For this lab, we are focusing on troubleshooting an actual issue in the environment and thus why all components are not being reviewed.

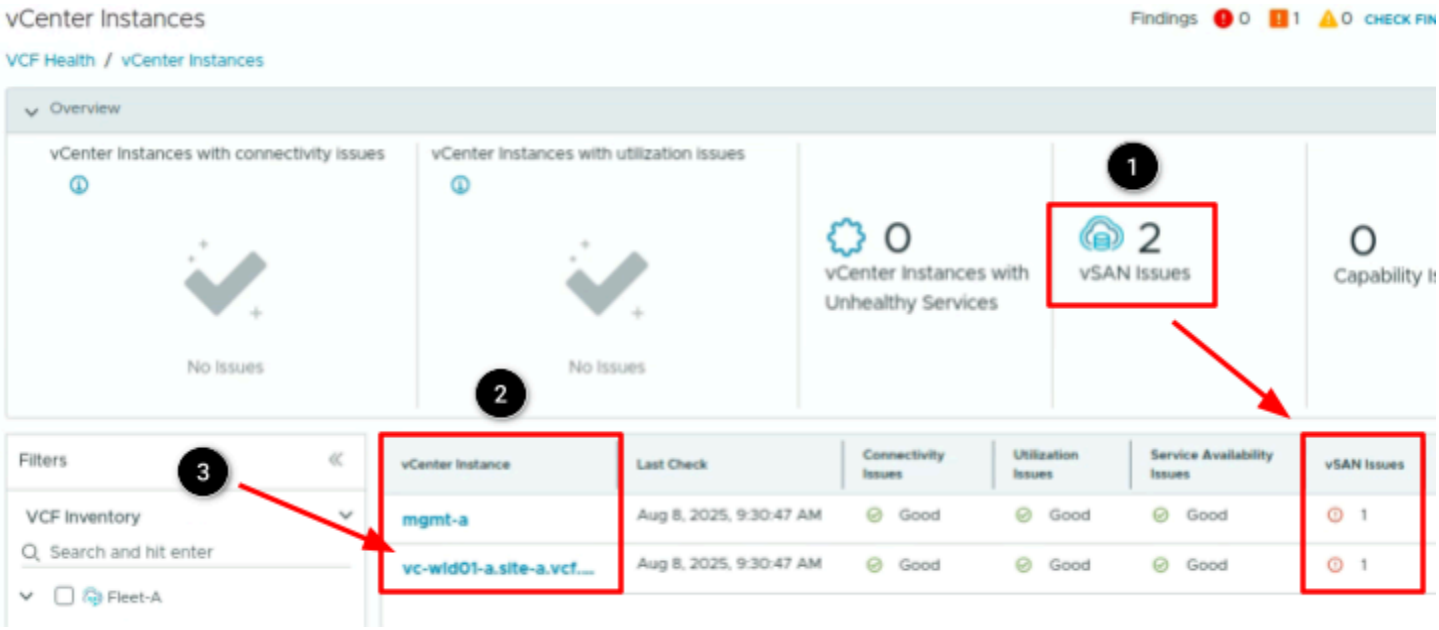
vSphere Health



In the **vSphere Health** section, we see health details on our vCenters and ESX Hosts in the environment.

1. Notice in the image (may differ from the lab) our **vCenter Instances** are reporting 2 Critical Issues and both are **vSAN Issues**.
2. In the image, there are **0 Unresponsive Hosts** in the environment, so we'll focus on the vSAN Issues that have been identified.
3. Click **VIEW DETAILS**

vCenter Instances



In the VCF Health view of our **vCenter Instances**, we see the following:

1. In the image, two **vSAN Issues** have been identified in the overall environment and this matches what we see in the **vSAN Issues** column.
2. We see these **vSAN Issues** have been identified in two of our vCenters as listed under the **vCenter Instance** column.

3. Previously in this lab, we focused on the health of the Management Cluster. This time, let's focus on the Workload Cluster in the environment. Click on the **vc-wld-a.site-a.vcf.lab** vCenter Instance hyperlink.

VCF Health Object Details Page

We are now on the VCF Health page for the specific object chosen. Over the next few pages, we'll review each of the components being shown on this page.

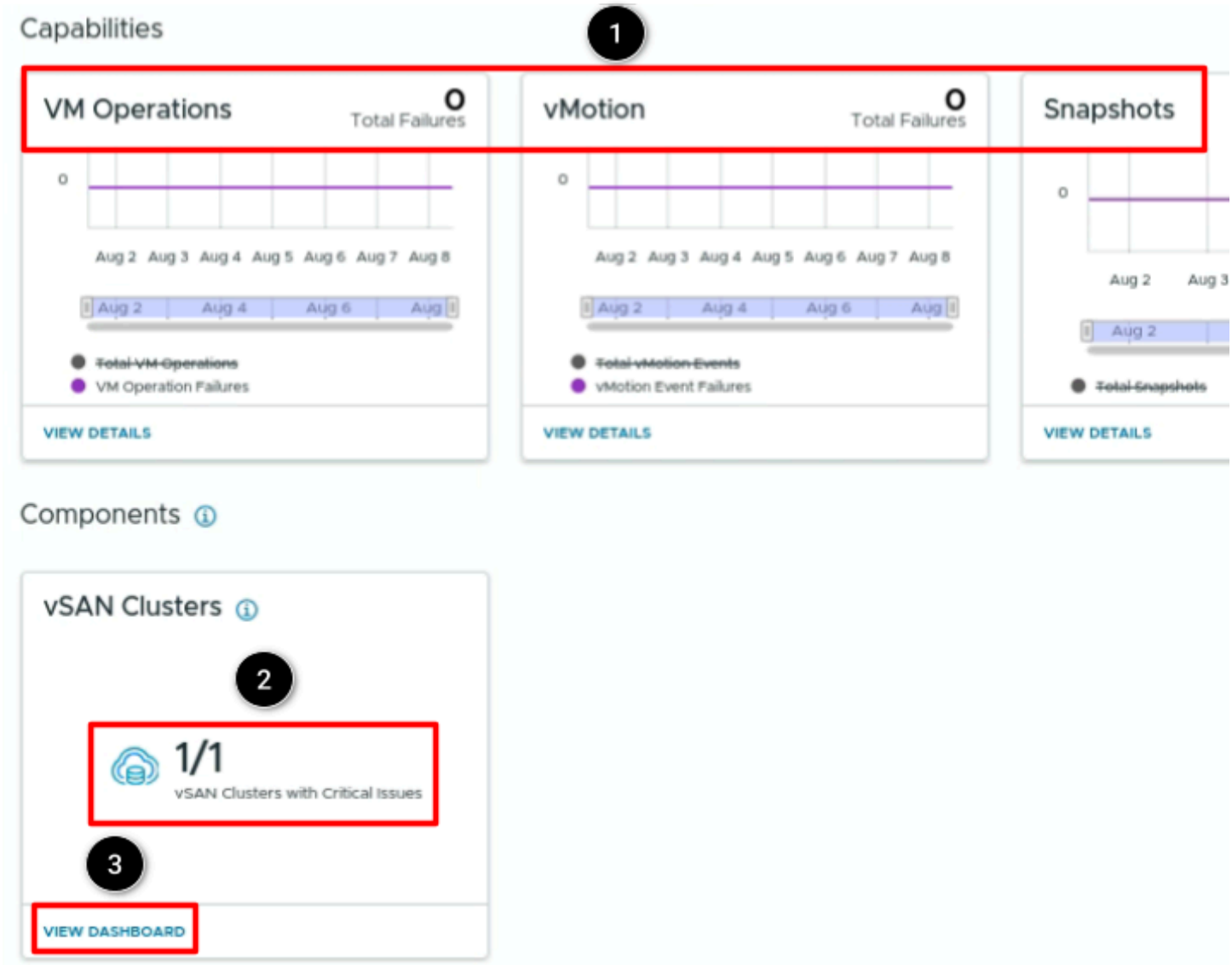
1. Note we are viewing the **vc-wld01-a.site-a.vcf.lab** object which is our vCenter appliance.
2. In the **Summary** section, we see such items as the Domain, Fleet, Version of VCF, and Collection Status for various adapters.

vCenter Health

The **Connectivity**, **Utilization**, and **Services** components were discussed previously in this lab, but we can briefly see in the image that all of them are healthy and no issues are identified (may differ from lab). Note: If any issues are revealed during the taking of the lab, feel free to click **VIEW DETAILS** on any of the impacted components as time allows. For now, let's continue moving forward in our task of troubleshooting vSAN issues.

1. **Scroll down** to view other components on the VCF Health page for this object.

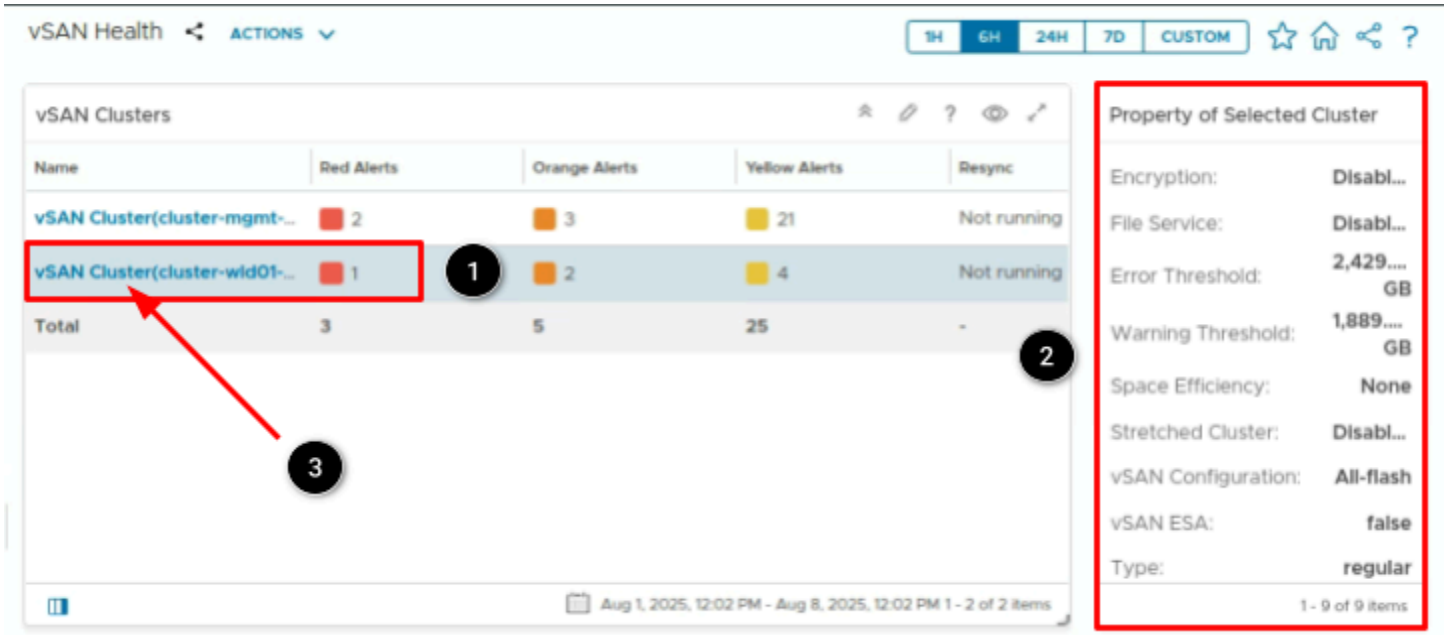
Capabilities and Components



Further down the **VCF Health** page for our vCenter, we see:

1. In the **Capabilities** section, we see the **VM Operations**, **vMotion**, and **Snapshots** tiles. These tiles were discussed previously in this lab and there are no issues identified in the image so we will move past these for now, but feel free to dig deeper into any of them as time allows.
2. In the **Components** section, in the image we see the **vSAN Clusters** tile and it is showing we have **1/1 vSAN Clusters with Critical Issues**. We want to review what issues have been identified.
3. Click **VIEW DASHBOARD**.

vSAN Health Dashboard

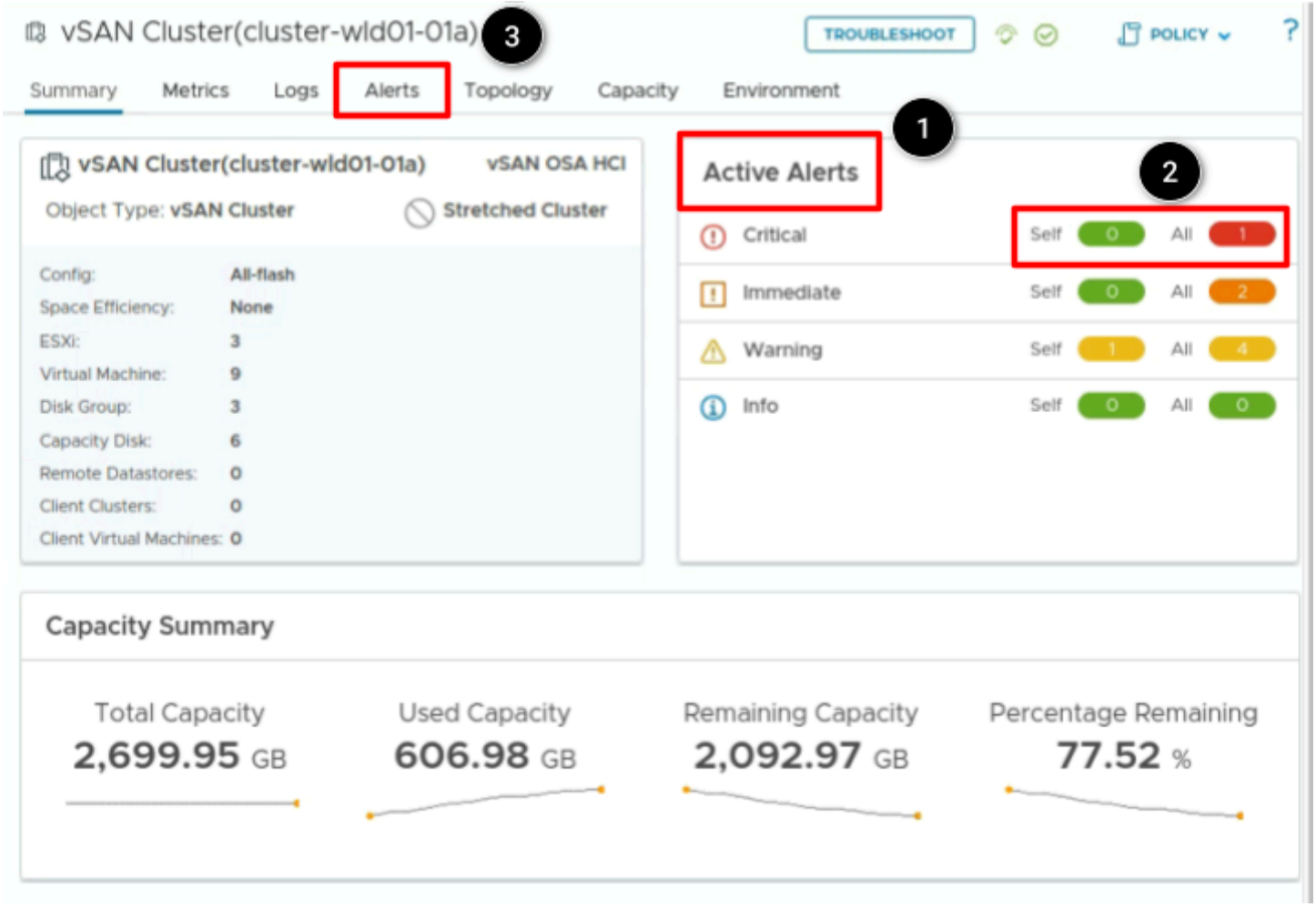


The **vSAN Health Dashboard** is the same one we've seen before when we went through the VCF Health View, so we are now beginning to see where the two views link us to the same underlying data.

1. Click on the **Workload vSAN cluster line** (not the hyperlink). Selecting this line populates the widget to the right.
2. Notice the **Property of Selected Cluster** widget is now populated with details for our Workload vSAN Cluster.
3. Click on **vSAN Cluster(cluster-wld01-01a)** (the actual hyperlink) to dig deeper into the specific object.

Note: The images throughout this section may not match what is seen in the lab due to the labs being "torn down and redeployed" on a regular basis. There may be more errors or no errors at the time of the lab; however, the concepts and actions taken will remain the same.

vSAN Cluster Object View

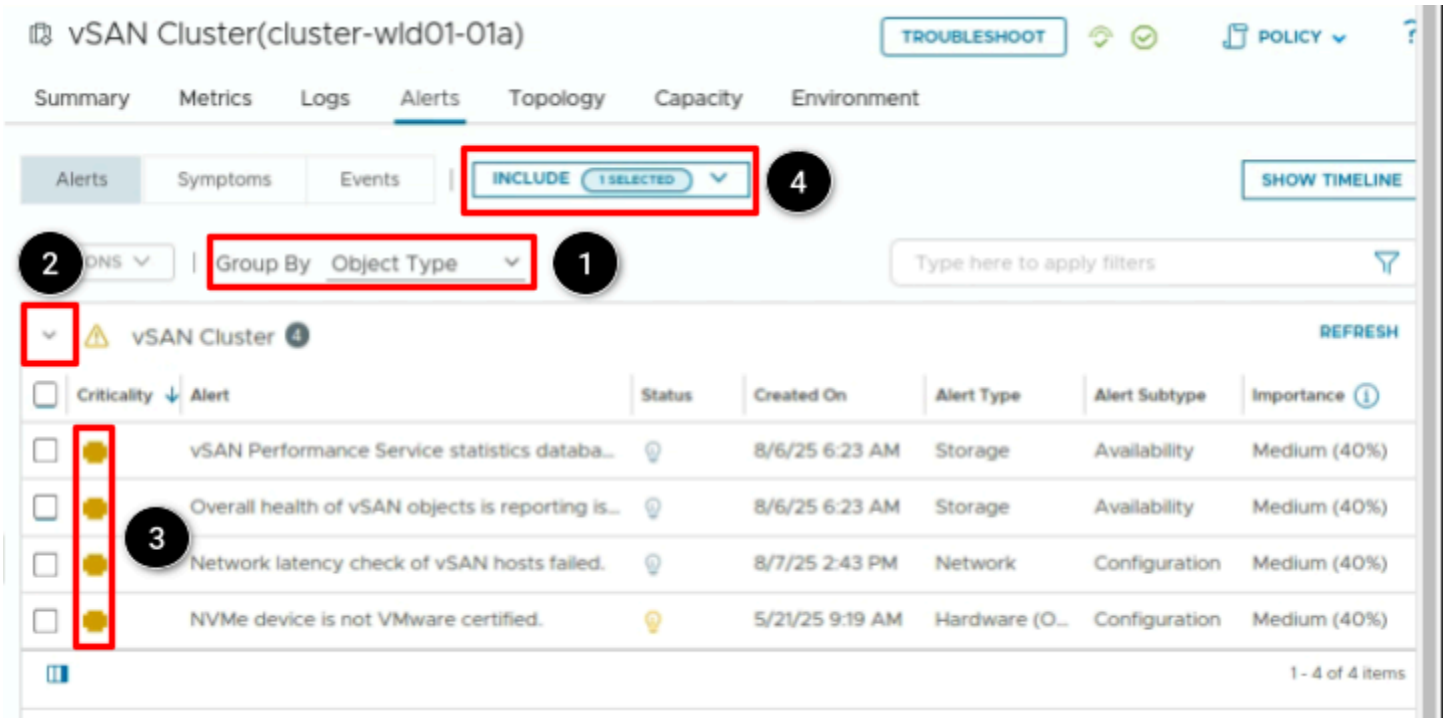


In the Object View of **vSAN Cluster(cluster-wld01-01a)** in the image notice the following:

1. Focus on the **Active Alerts** widget where we can see the various thresholds of alerts identified..
2. Notice the vSAN Cluster ("Self") does not have any Critical alerts, but there is a Critical alert in the "All" category. This means there is a Critical alert somewhere in the environment running on this particular vSAN Cluster. Let's track down this specific Critical alert. Note if there are no alerts at the time of the lab, follow along in the images provided to understand the steps and concepts.
3. Click on the **Alerts** tab.

Note: The images throughout this section may not match what is seen in the lab due to the labs being "torn down and redeployed" on a regular basis. There may be more errors or no errors at the time of the lab; however, the concepts and actions taken will remain the same.

vSAN Cluster Alerts

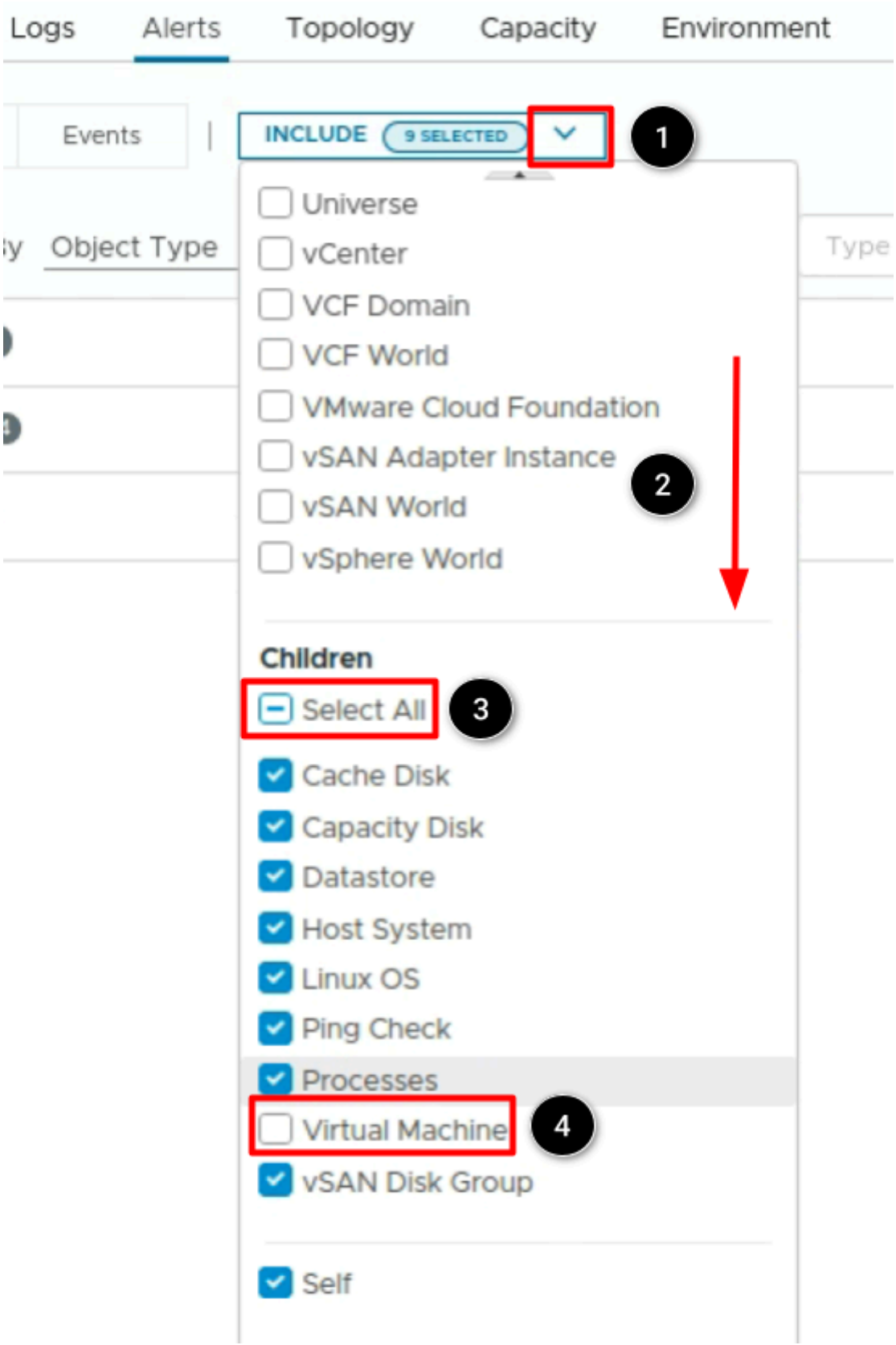


We are now in the **Alerts** for the vSAN Cluster. Our previous page image showed a Critical Alert on this vSAN Cluster, but where is it?

1. Make sure our **Group By** field is set to **Object Type**.
2. Click the **down arrow** next to the **vSAN Cluster** Object Type to show all alerts for this category.
3. Interesting. Note in the image showing current alerts that none are identified as Critical. This is because we are looking at only the vSAN Cluster itself rather than all components running on top of this vSAN.
4. Notice the **INCLUDE** field is set to only include alerts from only **1 Object** (which is the vSAN Cluster itself).

Note: The images throughout this section may not match what is seen in the lab due to the labs being "torn down and redeployed" on a regular basis. There may be more errors or no errors at the time of the lab; however, the concepts and actions taken will remain the same.

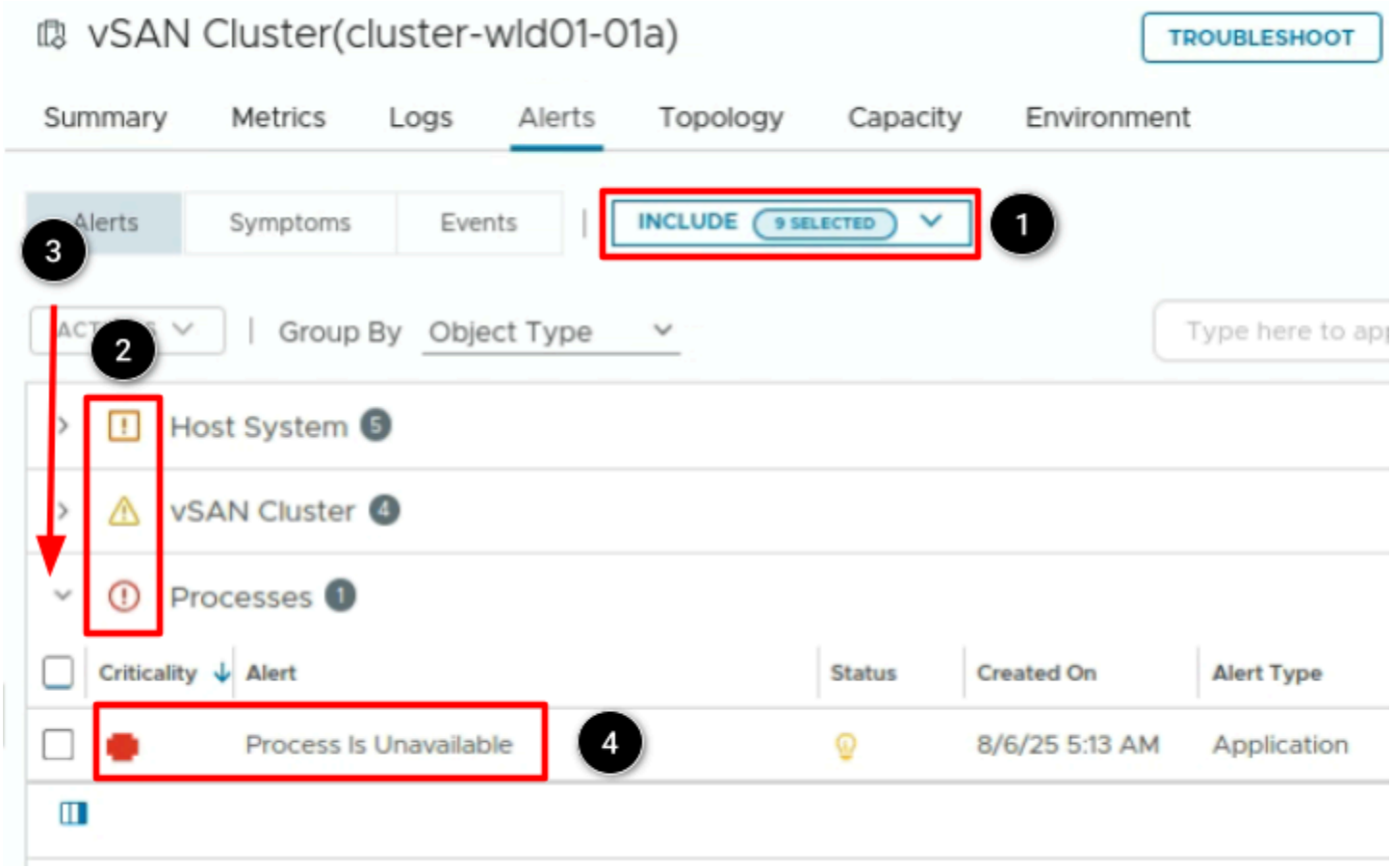
Include More Objects in the Alert View


Logs
Alerts
Topology
Capacity
Environment
Events
INCLUDE
9 SELECTED
1
Universe
vCenter
VCF Domain
VCF World
VMware Cloud Foundation
vSAN Adapter Instance
vSAN World
vSphere World
2
Object Type
Type
Children
Select All
3
Cache Disk
Capacity Disk
Datastore
Host System
Linux OS
Ping Check
Processes
Virtual Machine
4
vSAN Disk Group
Self

To add additional components to our **Alerts View**, do the following:

1. Click the **down arrow** in the **INCLUDE** field.
2. **Scroll down** to the **Children** section.
3. Click on **Select All** (we want to include the underlying **Children** components in our Alerts View).
4. Click on **Virtual Machine** to deselect it from the list (this will make our analysis for Critical alerts on the Infrastructure easier to review).
5. After selections have been made, click to the side of the box to close it (not shown).

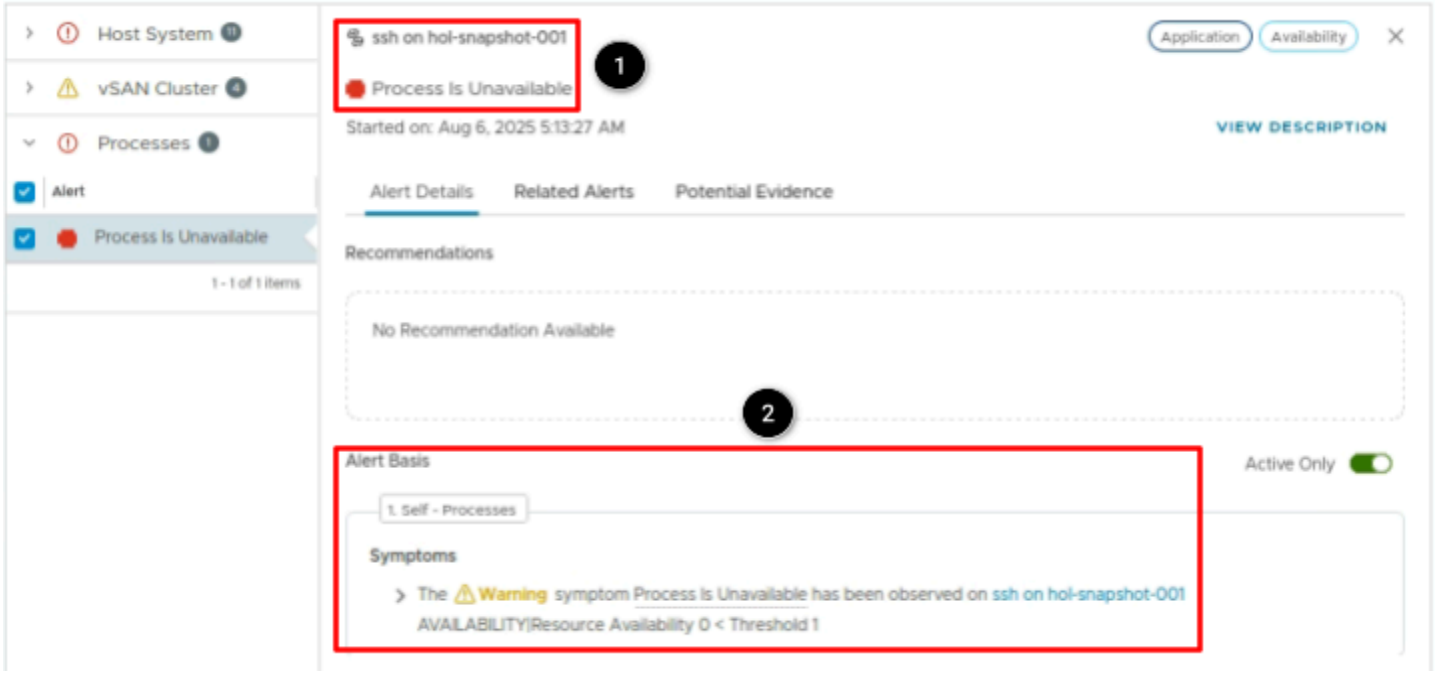
Critical Alert Identified



We are now viewing Alerts from the **vSAN Cluster** as well as underlying **Children** components.

1. Notice the **INCLUDE** field of the image now has 9 Object Types included rather than only 1 (may differ from the lab)..
2. In the image, based upon the **threshold icons** we see there is a **Critical Alert** in **Processes.**
3. Click the **down arrow** to expand the **Processes** Object Type. Note: If **Processes** are not showing in the list (due to no issues at the time of the lab), feel free to expand one of the other Object Types to reveal any alerts.
4. In the image, We see a **Critical Alert** which tells us a **Process is Unavailable**. Click on the Process alert (or any of the alerts at the time of the lab) to get more information.

Alert Details



For the **Process is Unavailable** Alert in the image, we now see the specific details.

1. Here we see the **SSH process on hol-snapshot-001** (one of our lab VMs) is unavailable.
2. In the **Alert Basis** we see more information and can see that the Symptom of a service not running is a **Warning**, but this Alert is configured to trigger as **Critical** if this symptom is found. As an additional FYI, the reason this alert triggered is because we enabled/configured Service Delivery in our VCF Operations instance, which tracks the state of services running on all VMs in the environment. From here, we could go review the VM and determine if this is a Service we want running.

Congratulations! We've successfully used VCF Health (Component View) to track down a Critical Alert in our environment.

Conclusion

In this lab, we were able to find and review Critical Alerts in our environment using VCF Health. We learned how to use both the VCF View and the Component View inside of VCF Health to track down these issues and determine if they required additional attention as an Administrator of our environment.

This was just a brief review of how to use VCF Health, but hopefully you now have the knowledge of how to use this powerful tool to easily identify issues and maintain the overall health of your environment(s).

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)

vmware® by Broadcom

Item No: 51227-vcf-wp-hands-on-labs-manual-2025, Jan-25