CyberSnap.io
Prerequisite Guide

Version 1.66



Jun 2026

CyberSnap Prerequisites

To ensure the correct operation of CyberSnap, certain prerequisites must be set up before installation.

Hardware and Software

CyberSnap server	Windows 2019/2022/2025 One server with 16 GB RAM, 4 CPUs, disk size 250 GB The latest VMware VM tools need to be installed on the server. The correct time zone should be set
Proxy server requirements for the CyberSnap ECE service	Windows 2022/2025 **The VMware SCSI Paravirtual controller must be used for virtual machine setup.** Add three additional VMware SCSI Paravirtual controllers, bringing the total number of SCSI Paravirtual controllers attached to the proxy server to four. One server with 20 GB RAM, 6 CPUs, disk size 250 GB The latest VMware VM tools need to be installed on the server. The correct time zone should be set
Supported Virtual Environment	VMware vCenter version 7 or above VMware ESXi version 7 or above
Windows credentials	The CyberSnap service should be configured to use the default Local System account
VMware Credentials	Dedicated VMware account that has full right in VMware vCenter
NetApp Credentials	Dedicated NetApp account that has full right in NetApp
Networking	Servers must have a single NIC and assign a static IP
Supported Browser	Google Chrome, Microsoft EDGE and Mozilla Firefox
UAC	Our best practice is to disable Users Access Control if possible

Firewall Setup

If your company enforces strict rules requiring all network segments to be configured with a firewall, the following ports will need to be enabled:

Source	Destination	Port	Type	Notes
CyberSnap	VMware vCenter	443	TCP	VMware default port
CyberSnap	ESXi(s)	443	TCP	ESXi default port
CyberSnap	NetApp	443	TCP	NetApp default port
CyberSnap	CyberSnap Proxy	5000	TCP	CyberSnap Proxy default port

All the ports listed are default ones. If you have customized your setup with different ports, you will need to define firewall rules for those specific ports.

Internet Access URL

S3 Backet

To automatically provide policy log files to CyberSnap Support, you must first enable HTTPS access to the AWS S3 CyberSnap bucket. This secure connection ensures that log files are transmitted safely and

efficiently. Each customer is assigned a dedicated folder for log file sharing. This design ensures strict access control and prevents any possibility of data exposure or leakage between different customers.

Once HTTPS access is configured, log file sharing can be activated from the Settings page within the CyberSnap Console. By default, this feature is disabled for security and privacy reasons and can only be enabled manually by the customer.

To enable the automatic upload of CyberSnap log files, the following URL must be accessible.

- https://cybersnap-customer-logs.s3.eu-west-1.amazonaws.com/

AI-Driven Cyber Findings Analysis

For advanced analysis of Cyber findings, CyberSnap integrates with an AI-based recommendation engine. This AI agent assists in interpreting scan results and provides actionable insights to enhance incident understanding and response.

To protect customer privacy and data integrity, CyberSnap does not upload or share any sensitive company information such as server names, IP addresses, usernames, or similar identifiers. Only non-sensitive metadata—such as the file name, triggered rule, and other relevant scan attributes—is transmitted to the AI agent. This ensures that the AI can perform an accurate contextual analysis without compromising data security.

The AI Analysis feature is enabled by default. However, to receive AI-generated recommendations, users must manually activate the process by clicking the AI button. For successful communication with the AI agent, the following URL must be accessible:

- https://ai.cybersnap.io

CyberSnap Git Repository Access

CyberSnap provides a dedicated Git repository that contains essential files maintained and updated by the CyberSnap team. To ensure your system receives the latest updates, the following URL must be accessible:

- https://bitbucket.org/cybersnap/

By default, CyberSnap automatically checks the Git repository each time a scan is initiated to verify whether new updates are available and download them if necessary. This ensures the system always operates with the most recent configurations and definitions.

NetApp ONTAP

To access CyberSnap capabilities, specific NetApp prerequisites must be fulfilled:

- Applied the FlexClone license
  - To successfully utilize the NetApp FlexClone license, a minimal amount of free space is required in the aggregate, depending on the size of your snapshot.
- NFS volumes, create a new export policy or update the existing NetApp ONTAP Export Policy to include all specified VMware ESXi hosts in the CyberSnap Policy.
- Ensure that an initiator group (igroup) is created for each ESXi host or cluster. This step is necessary for establishing connections between the ESXi hosts and the NetApp LUNs. (iSCSI/FC only)

    - *Note:* If INFRA scanning will be performed only using specific ESXi hosts, configure an igroup for each of those specific ESXi hosts.
- Set up snapshot policies on volumes that will be configured in CyberSnap.

AD Service Account

CyberSnap does not require a dedicated Windows account. Upon successful setup, the CyberSnap, CyberSnap Bridge, and ECE services are created on the CyberSnap servers, and the Local System account is configured for use by these services.

If your company policy restricts the use of the Local System account, you must create a service account with local administrator privileges on the CyberSnap server and assign it to the CyberSnap service. This service account can be either a local or domain account, depending on your company's policies.

Antivirus Prerequisites

An antivirus program running on CyberSnap servers may interfere with CyberSnap's operation by intercepting files that need to be scanned. To prevent conflicts in the scanning process, we recommend adding a folder exclusion:

CSI main server

- EXE Files:
    - C:\Program Files (x86)\CyberSnap.io\CyberSnap\web server\BridgeProxy.exe
    - C:\Program Files (x86)\CyberSnap.io\CyberSnap\web server\CyberSnap.API.exe
- PowerShell scripts:
    - Whole folder (all scripts): C:\Program Files (x86)\CyberSnap.io\CyberSnap\web server\scripts

CSI Proxy server

- Exclude folder:
    - C:\scan_folder
    - C:\Program Files\ECE Cyber Scan
- File
    - C:\Program Files\ECE Cyber Scan\ece_scan.exe
    - C:\Program Files\ECE Cyber Scan\ece_api.exe

Supported Virtual Machines

Depending on the policy type and the virtual machine's multiple-disk configuration, there are certain limitations in CyberSnap, which we list below:

- CyberSnap relies on NetApp snapshots to scan and validate virtual machines. Therefore, it is crucial that the virtual machine selected in the policy does not have multiple disks spread across different datastores. Such virtual machines will appear greyed out in the policy list, as this configuration is not supported by CyberSnap.
- The Cyber policy type does not support Linux virtual machines at the moment.

- The Infra policy type supports both Linux and Windows virtual machines.

Note: Virtual machines that use deprecated Windows dynamic volume types are not supported when configured with a Cyber policy type.

VMware vCenter – DRS

In a VMware vSphere environment, when working with clusters, you may have configured DRS (Distributed Resource Scheduler), which focuses on load balancing by automatically migrating VMs between hosts to optimize performance and resource usage.

Because CyberSnap scans VMDK disks attached to the Proxy server, it's essential to understand that migrating the server to a different host may disrupt the connection to the datastore, resulting in lost access to the attached VMDK disks.

To prevent this, create VM Override rules that disable VMware DRS for the CyberSnap Proxy virtual machine. This ensures that CyberSnap Proxy server remains connected to the dedicated datastore throughout the scanning process.

VMware vCenter – Clester Datastore Heartbeat

In VMware vSphere, HA (High Availability) datastore heartbeating provides a secondary communication mechanism between ESXi hosts when the management network becomes unavailable. By default, vSphere automatically selects accessible datastores for HA heartbeating.

During the CSI scanning process, datastores are temporarily attached to the vSphere environment to allow controlled access for analysis and validation operations. These attachments are transient by design and exist only for the duration of the scan.

During CSI scans, automatic datastore selection can cause operational issues. Datastores automatically selected for HA heartbeating may become locked by the VMware HA mechanism, preventing CSI from unmounting and removing the temporary datastores after the scan completes.

To avoid this condition, it is mandatory to disable automatic datastore selection and explicitly define which datastores are used for HA heartbeating.

Procedure:

Step 1: Select the Target Cluster

1. Log in to the vSphere Client.
2. Navigate to the desired cluster that will be used with CSI scanning.
3. Click Configure.

Step 2: Access vSphere HA Settings

1. Under Services, select vSphere Availability.
2. Click Edit (or Edit Cluster Settings).

Step 3: Disable Automatic Heartbeat Datastore Selection

1. In the vSphere HA settings window, expand Datastore Heartbeating.
2. Locate the Datastore Heartbeat option.
3. Change the selection from:
    - Automatically select datastores accessible from the hosts

to:

    - Use datastores only from the specified list

This change disables automatic datastore selection for HA heartbeating.

Step 4: Manually Select Heartbeat Datastores

1. After selecting Use datastores only from the specified list, click Browse.
2. Select one or more datastores to be used exclusively for HA heartbeating.

Best Practice:

    - VMware recommends selecting at least two shared datastores that are accessible by all hosts in the cluster.
3. Click OK to confirm the datastore selection.

Step 5: Save and Apply the Configuration

1. Click OK or Save to apply the cluster settings.
2. vSphere HA will automatically reconfigure the cluster.

Verification:

To confirm that automatic datastore selection is disabled:

1. Navigate to Cluster > Monitor > vSphere HA.
2. Select Heartbeat Datastores.
3. Verify that only the manually specified datastores are listed.

Result:

Automatic HA datastore selection is disabled, and vSphere HA uses only the explicitly defined datastores for heartbeating.

Summary:

By switching from automatic to manual HA datastore selection:

- Temporary datastores attached by CSI are not unintentionally used for HA heartbeating
- Datastore locks that prevent unmount or removal are avoided
- HA behavior becomes more predictable and aligned with CSI operational requirements

This configuration is essential for environments that rely on temporary datastore attachment during scanning or integrity verification workflows.

VMware vCenter – Backup and Snapshots

CyberSnap consists of two servers, each with a specific role. The CyberSnap main server will be configured with the CyberSnap Management Console, while the CyberSnap Proxy server will be responsible for scanning VMDKs from various source servers located on a NetApp volume defined in the policy.

Since certain VMware processes, such as backups and server snapshots, may be performed during the execution of the CyberSnap policy without CyberSnap being aware of them, we will provide guidelines on how to carry out these two specific tasks.

CyberSnap Console Server – Backup Application

Since the CyberSnap server will remain powered on during the backup process, the backup will be considered 'crash-consistent'. A crash consistent backup in VMware captures the state of a virtual machine (VM) at a specific point in time without shutting it down or coordinating with the applications inside. It includes all data that was in memory and on disk at the time of the snapshot, similar to a system crash or sudden power loss. While no data is lost from disk, data in memory or pending writes may not be preserved, so applications may require recovery steps on restart.

Because of “crash-consistent” nature backup can be taken during the policy running so when the server is restored by the backup application policy can be in error state. No issues are expected during the backup process, therefore, no specific measures need to be taken.

CyberSnap Console Server – VMware Snapshot

All the rules and measures mentioned in the previous paragraph are applied to the VMware Snapshot native process. We strongly suggest that before manually taking the snapshot, you validate that there are no policies or other running processes indicated in the CyberSnap console. This will help ensure the most accurate state for CyberSnap if you decide to revert the CyberSnap console server to the saved snapshot state.

CyberSnap Proxy Server – Backup Application

Since the CyberSnap Proxy server may be scanning during the backup process, this can cause the backup application to fail due to inaccessible VMDK disks that are under the control of CyberSnap.

Therefore, it is important to configure the backup application to include only the main OS disk, the disk used to set up the virtual machine and on which the ECE service is installed (typically named "Disk 0" in the VMware Console). All other disks must be excluded from the backup to avoid failures of backup and restores.

If your backup application doesn’t support this capability, you will need to define a time window during the day when no scanning processes are running on the CyberSnap Proxy Server. Then, schedule the backup to run during that time or perform a one-time manual backup while all policies on the CyberSnap Console Server are not in a 'running/scanning' state.

CyberSnap Proxy Server – VMware Snapshot

All the rules and measures mentioned in the previous paragraph also apply to the native VMware Snapshot process. We strongly recommend that, before manually taking a snapshot, you verify in the CyberSnap console that no policies are currently running. This is necessary to ensure that no VMDK disks from scanning servers are attached to the CyberSnap Proxy server during the manual VMware snapshot creation process.

VMware vCenter – Resource Pool

As part of the best practices, we suggest creating a dedicated Resource Pool for Infra policy types. By implementing Resource Pools, you can limit the resources available to CyberSnap in the VMware vSphere

environment while simultaneously allowing your production environment to utilize the maximum available resources.

Since Cyber Policy types works with VMDK disk files and this approach does not introduce additional impact to your VMware environment, except for the load on the CyberSnap server during scanning, we require configuring the Cyber Policy to the 'Target ESX' host in the policy settings and selecting the same VMware host where the Cyber Proxy server is located. If VMware DRS is enabled, ensure that VM Override rules disable DRS for the CyberSnap virtual machine.

To accommodate varying numbers of virtual machines with different RAM and CPU configurations, we suggest setting the following parameters for the CyberSnap Resource Pool:

Memory
Reservations: 20% of the total RAM limit
Limits: 50% of the total RAM

CPU
Reservation: 20% of the MAX Limit
Limits: 50% of the MAX Limit

Be aware that not all versions of VMware vSphere support Resource Pool feature, here is brief overview of versions:

- **vSphere Essentials**: Does not include the ability to create Resource Pools.
- **vSphere Essentials Plus**: Includes the ability to create Resource Pools, along with features like vMotion and High Availability.
- **vSphere Standard and above** (including vSphere Enterprise and Enterprise Plus): Also allow you to create Resource Pools and include additional features like Distributed Resource Scheduling (DRS), Storage DRS, and more.

In cases where you cannot use the Resource Pool feature due to license limitations, you will still be able to select hosts from VMware vCenter. We recommend upgrading your license to a level that supports the Resource Pool feature, as this will enable CyberSnap scans to run on a larger scale, with more servers simultaneously.

Regardless of whether you configure a Resource Pool in your environment or not, the virtual machine Overrides rule that disables DRS for the CyberSnap virtual machine must be configured if VMware DRS is enabled.

VMware vCenter – Customize Alarm Rules

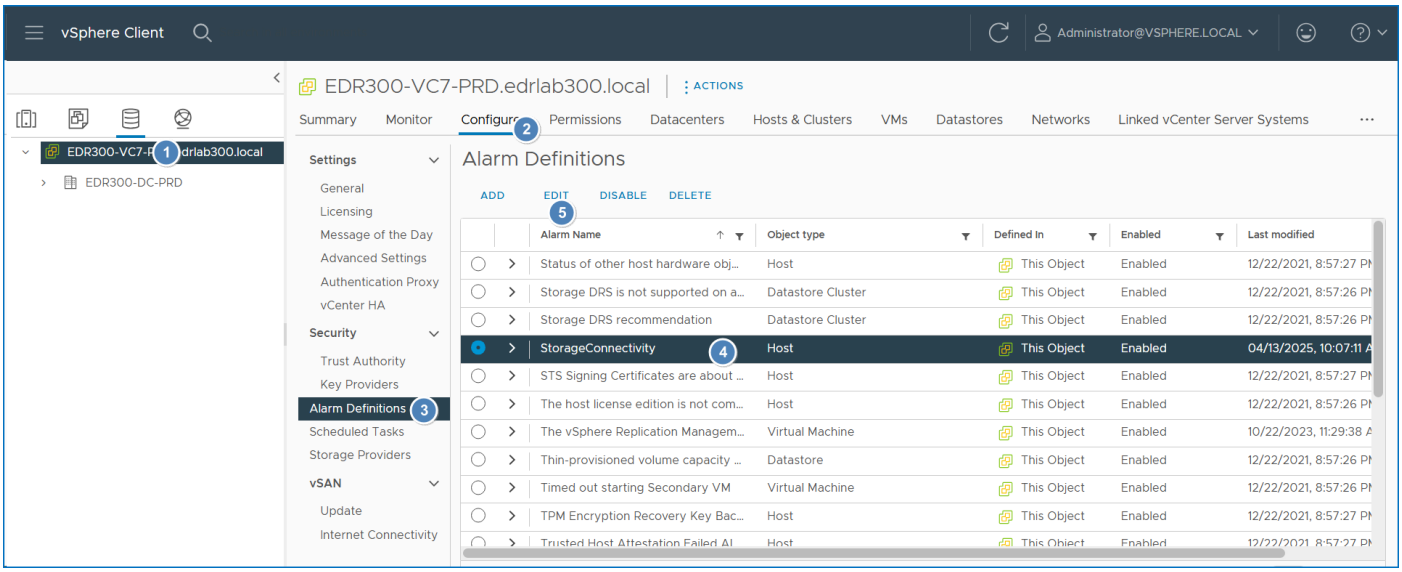
During CyberSnap operations, NetApp volumes will be connected and disconnected multiple times. If your environment includes alarms configured to trigger during this process, you may want to adjust them to prevent event generation and email notifications.

Fine tuning of Datastore Alarm definition

To avoid receiving emails when a Datastore is connected or disconnected by CyberSnap, you should add an additional filter in the current alarm definition. Once you modify the rule, it will ignore Datastore names that start with 'CSI', and no email will be sent.

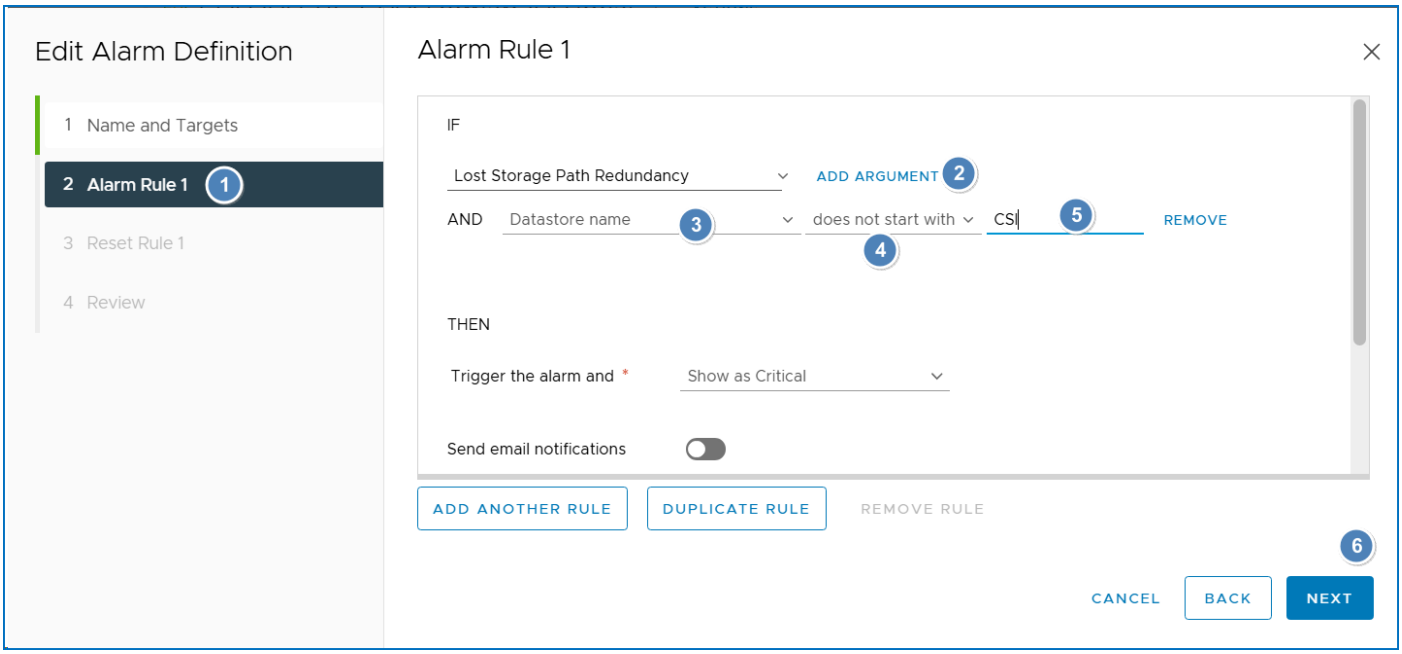
To modify an alarm definition, follow these steps:

1. Select the vCenter in the left pane.
2. In the right pane, click the Configuration tab.
3. From the list of options, select Alarm Definitions.
4. Choose the rule you previously created.
5. Click the Edit button.



When the rule is open:

1. Navigate to “Alarm Rule 1” in the Alarm Definition.
2. Click “Add Argument”. A new option will appear in the alarm definition.
3. For the filter, choose “Datastore name”.
4. Select “does not start with”.
5. Enter “CSI”.
6. Click “Next” until you reach the end of the rule definition, then click the “Save” button.

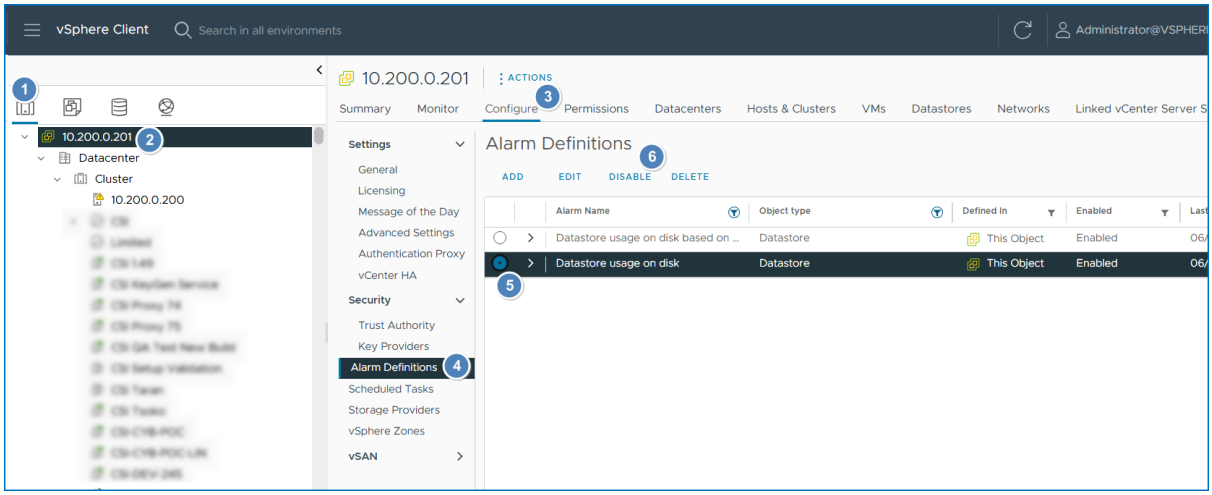


Reconfiguring Disk Usage Alarm in vSphere

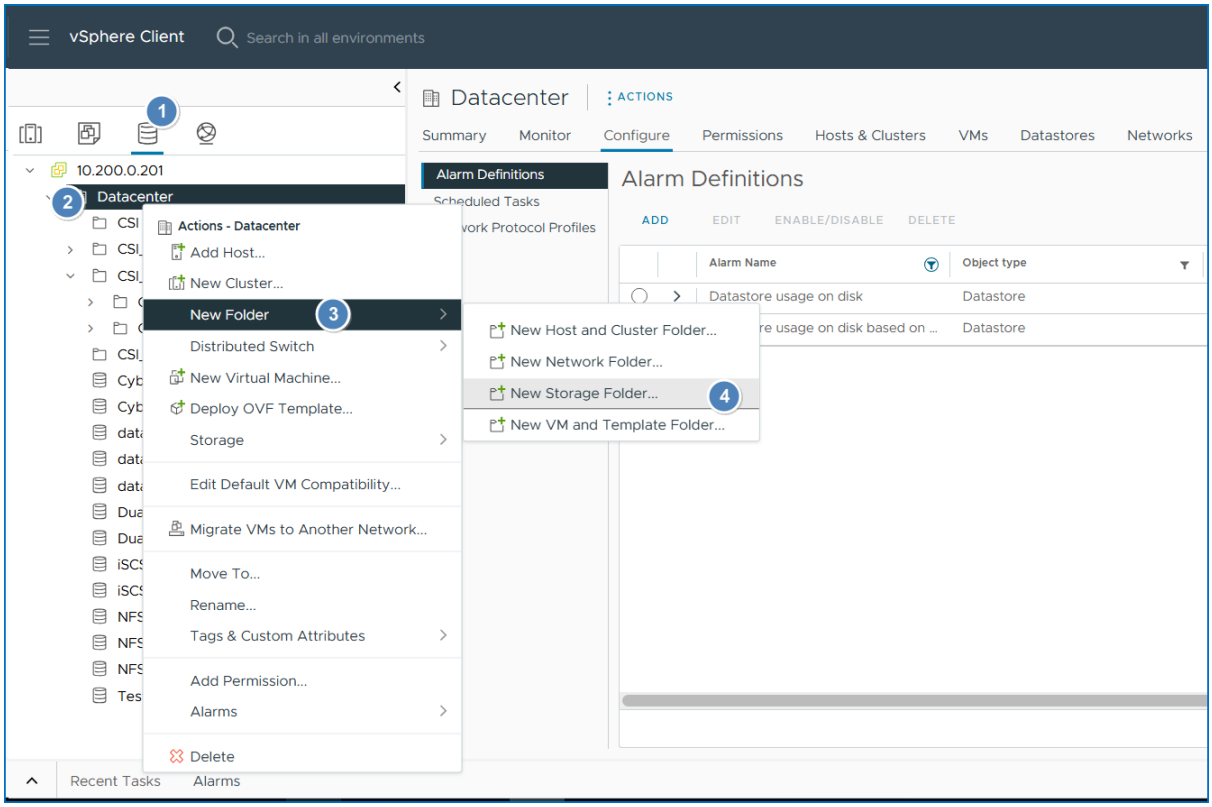
To prevent data stores created by CyberSnap from triggering the disk usage alarm, you should disable the default disk usage rule at the vCenter level and instead create a custom rule using the same metrics. This custom rule should only be applied to a specific folder, which you will need to create. Once the folder is in place and the custom rule is applied, move all production datastores into that folder.

Steps are:

- Disable the DiskUsage rule at the vSphere vCenter level

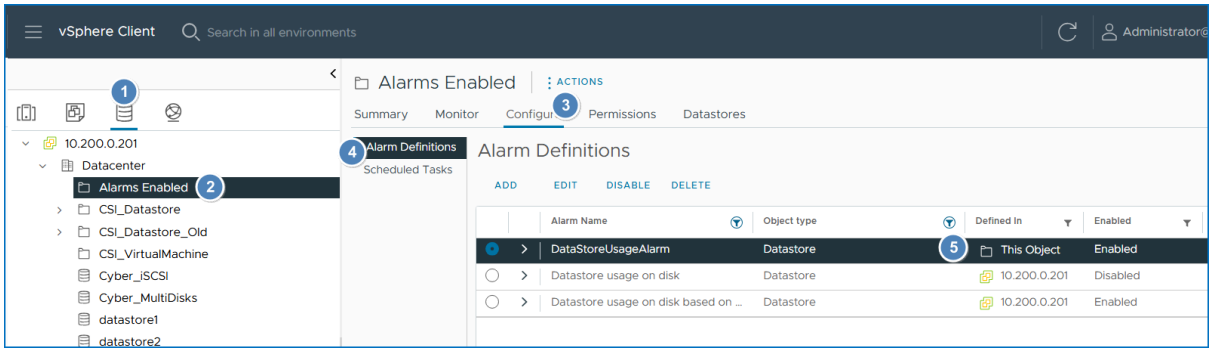


- Create folder in the datastore Inventory Tab named:
  - **Alarms Enabled**



- Select the folder you created in the previous step, then create a custom rule using the same metric details as the default DiskUsage rule.

Note: “Define In” must be “This Object” (e.g. folder that you select) in point 5.



- Now that the rule has been created and applied to the 'Alarms Enabled' folder, move all production datastores that need to be monitored into this folder.

