COHESITY

Version 4.2

October 2021

Cohesity ServiceNow Integration User Guide

ABSTRACT

The Cohesity ServiceNow (SNOW) plugin integrates ServiceNow with the Cohesity platform. The main goal of this plugin is to execute the workflows of Cohesity such as data protection, cloning, and recovery from ServiceNow. The SNOW plugin also lets you manage alerts using Webhooks, which is a common and an important part of IT Service Management (ITSM).

The Cohesity ServiceNow Integration User Guide describes the process of executing the Cohesity SNOW workflows.

Table of Contents

Figures

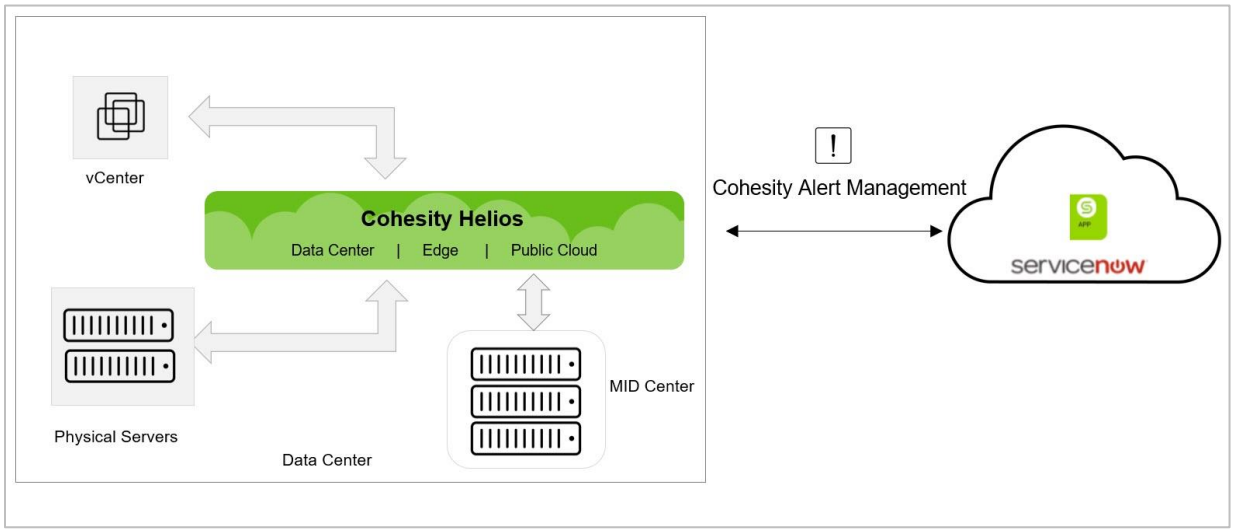
Tables

Introduction

The **Cohesity ServiceNow (SNOW)** plugin fetches data from Cohesity platform and facilitates performing various operations such as protecting, recovering, and cloning of VMs in ServiceNow using a secure network. See ServiceNow platform for details.

The following figure illustrates how Cohesity integrates with ServiceNow.

Figure 1: Cohesity Integration with ServiceNow



Cohesity integrates with ServiceNow through REST API to simplify data protection and data management on VMs including workflow automation, backup, and recovery.

Table 1: ServiceNow Interaction with Cohesity

MODULE	INTERACTION WITH COHESITY
vCenter	Once a vCenter is registered with Cohesity, all the resources available in the vCenter are populated to the Cohesity environment, which can then be backed up. The VMs can then be accessed by ServiceNow once the cluster where the VMs are present is registered.
Physical Server	These are the individual physical servers registered with Cohesity. Currently, you have an option to restore files and folders in the physical server that has been backed up.
MID Server	This acts as a medium between ServiceNow and Cohesity. That is, all the API calls are routed via the MID Server. For details, see MID Server Documentation.

Features

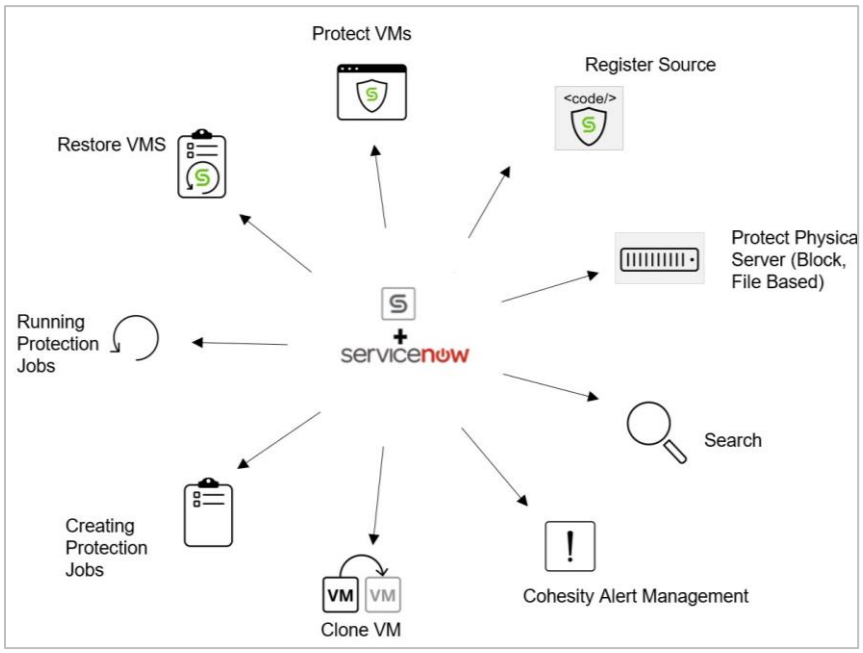
The Cohesity ServiceNow plugin offers the following features:

- Supports a multi-cluster environment
- Availability of Service Catalog with Protection Source, data protection, recovery, and clone workflows

NOTE: The workflows are supported for vCenter and physical sources.

- Option to register and unregister a vCenter and physical server
- Workflow management such as protect VMs, recover VMs, clone VMs, recover files and folders, and creating protection jobs
- Alert management through Webhooks

Figure 2: Cohesity ServiceNow Plugin Features



What's New

Latest Release: v4.1

This release 4.1 includes the following features:

Table 2: Release 4.1 Features

VERSION	WHAT'S NEW	REVISION DATE
v4.1	This release includes the following enhancements: • Option to schedule the recovery and clone workflow at a specific time slot • Optimization of the search files/folders results • Displaying the file size while restoring the file/folder • Resolving alerts through ServiceNow on a multi-node cluster environment • Few minor bug fixes	July 2020

Previous Releases

Table 3: Previous Releases Features

VERSION	WHAT'S NEW	REVISION DATE
v4.0	• Cohesity Alert Management through Webhook configuration • Simplified cluster synchronization and discovery processes • Service Catalog for workflow process	April 2020
v3.0	• Multi-cluster support • Registering/unregistering of protection sources • Simplified protection job creation process directly from	Nov 2019

VERSION	WHAT'S NEW	REVISION DATE
	ServiceNow which replaces the earlier process of creating it in the cluster and then syncing the jobs • Protection of Virtual Server • Protection of Physical host (block-based and file-based)	
v2.0	• Updated and modernized dashboard for the plugin and with few bug fixes	May 2019

Software Requirements

Table 4: Software Requirements

COHESITY SNOW PLUGIN VERSION	SERVICENOW RELEASE VERSION	COHESITY
4.1.0, 4.0.0	• New York, Madrid, and Orlando	6.3.x or higher
2.0.0, 3.0.0	• New York and Madrid	6.2.x or higher

NOTE:

- Alert management using Webhooks is supported in Cohesity cluster version 6.3.x or higher EXCEPT 6.5 and 6.5.1a.

Process Overview

The overall process of working with the SNOW plugin is as follows:

1. Install the SNOW plugin along with MID Server configuration.
2. Add ServiceNow users and assign to groups.
3. Run **Fix Scripts** if the application is upgraded to any new version from v2 or v1.
4. Configure Cohesity clusters in SNOW for:
   a) Discover of resources (vCenter and physical server)
   b) Webhook configuration
   c) Discovery and Webhook. See Cohesity ServiceNow Integration Install and Config Guide for details.
5. Execute workflows in SNOW as described in Cohesity SNOW Tasks.

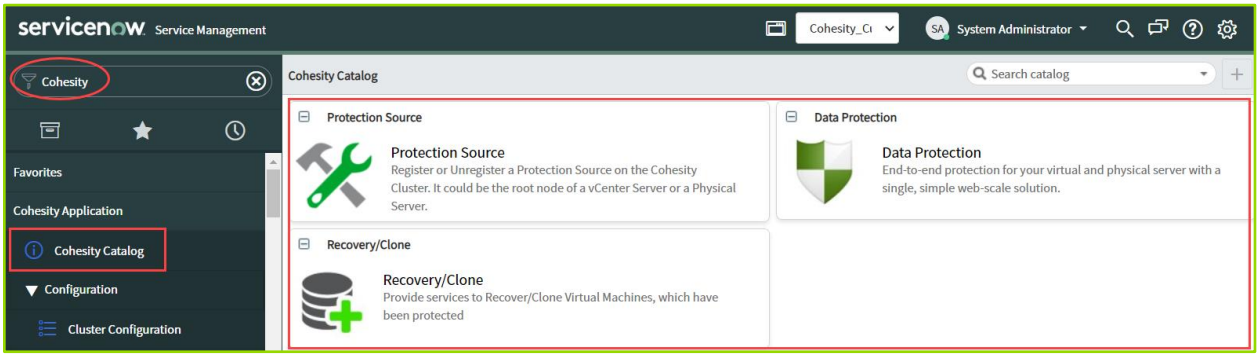
Cohesity SNOW Tasks

You can execute various Cohesity SNOW tasks such as registering a source, protecting VMs, physical servers, and other workflows using one of the following methods:

- Using Cohesity Catalog
- Using the UI options available in the respective ServiceNow database as explained in SNOW Workflows

Cohesity Catalog

Cohesity Catalog is a collection of services available such as Protection Source, Data Protection, and Recovery/Clone. To access this, type **Cohesity** in the search bar, and navigate to **Cohesity Application > Cohesity Catalog**.



Protection Source

You can register or unregister vCenter and physical servers using the **Protection Source** catalog as follows. The Protection Source can be the root node of a vCenter server or a physical server.

1. Type **Cohesity** in the search bar. Navigate to **Cohesity Application > Cohesity Catalog**.
2. Click **Protection Source**.
3. Select the environment category as **Physical Server** or **VMware**, based on the environment of source to be registered/unregistered.
4. Select the operation to be performed:
   - **VMware**: Register Source or Unregister Source
   - **Physical Server**: Register Source or Unregister Source

Data Protection

You can perform various operations such as create protection job, delete job, protect virtual machine, and unprotect virtual machine.

1. Type **Cohesity** in the search bar. Navigate to **Cohesity Application > Cohesity Catalog**.
2. Click **Data Protection**.
3. Select the environment category as **Physical Server** or **Virtual Server**.
4. Select the operation to be performed:
   - **Virtual Server**: Create New Protection Job, Delete Job, Protect Virtual Machine, or Unprotect Virtual Machine
   - **Physical Server**: Create New Protection Job or Delete Job

Recover/Clone

You can perform recovery or clone operations only on virtual machines.

1. Type **Cohesity** in the search bar. Navigate to **Cohesity Application > Cohesity Catalog**.
2. Click **Recovery/Clone**.
3. Select the operation to be performed:
   - Clone VM
   - Recover VM

SNOW Workflows

You can execute various SNOW workflows as described in the below procedures. After you execute a workflow, it will be sent as a request for approval or will be approved directly. This depends on the configurations enabled for approvals while configuring a cluster. See *Configure Cohesity clusters* in Cohesity ServiceNow Integration Install and Config Guide. Users belonging to a group with the necessary privileges to approve the requests can approve the SNOW execution requests.

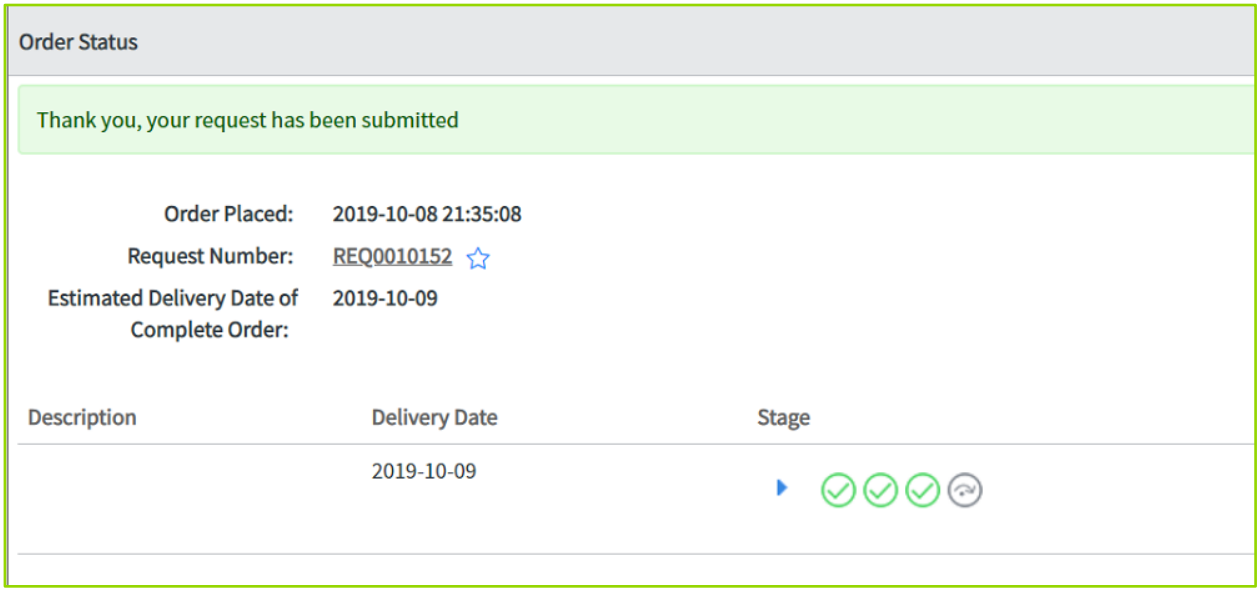
NOTE: Users associated with Cohesity Admin or Cohesity User group only will be able to perform the below tasks.

Register a Source

You can choose to register a cluster as a Hypervisor or physical server.

1. Type **Cohesity** in the search bar. Navigate to **Protection Source** > **Sources** and click **Register**.
2. Select the cluster to be registered from the drop-down list.

3. To register the cluster as a Hypervisor:
   1) Select **Hypervisor** as the Environment and **vCenter** as the Source Type.
   2) Enter the **Source Information** such as the Host IP address of the vCenter, Username and Password for authentication.
4. To register the cluster as a physical server:
   1) Select **Physical Server** as the Environment.
   2) Enter the **Source Information** such as the IP address of the physical server and Host Type of Windows/Linux.
5. Click **Order Now**.
6. A request is submitted for the catalog item.



7. To approve the request, log in to the instance using any of the users with Cohesity ProtectSource group. See Execute Approvals section for details.

Create Protection Jobs

You can choose to protect a vCenter or a physical server, which is block-based or file-based.

1. Type **Cohesity** in the search bar. Navigate to **Protection Jobs** > **Protection Jobs** and click **New Job**.
2. Make a selection to protect either a vCenter, physical server block-based, or file-based.

Protect a vCenter

1. Select the **Cluster**, enter a **Job Name**, and choose to protect **Virtual Server** from the drop-down.
2. Select the vCenter source and ESXI Host.

3. Choose the VMs to be protected by moving them from the left pane to the selected vms list on the right.
4. Select the **Policy** and **Storage Domain**.
5. Click **Order Now**.
   A request is submitted for the catalog item. If approval was enabled for this action in the configuration page, then the requested item will wait for approval from the user with the respective group (Cohesity ProtectVM).

Protect a Physical Server (Block-Based)

1. Select the **Cluster**, enter a **Job Name**, and choose to protect **Physical Server (Block-based)** from the drop-down.
2. Select the physical server IP, policy, and storage domain.
3. Click **Order Now**.
   A request is submitted for the catalog item.

Protect a Physical Server (File-Based)

1. Select the **Cluster**, enter a **Job Name**, and choose to protect **Physical Server (File-based)** from the drop-down.
2. Select the source IP, path of the file/folder to be protected, policy, and storage domain.
3. Click **Order Now**.
   A request is submitted for the catalog item.

Protect VM

1. Type **Cohesity** in the search bar. Navigate to **Virtual Machines** > **Virtual Machines List**.
2. Select one or more virtual machines which are in unprotected state and click **Protect**.
   The corresponding service catalog item page displays.
3. Select the protection job from the drop-down through which the virtual machines have to be protected. Click **Order Now**.
   A request is submitted for the catalog item. If approval was enabled for this action in the configuration page, then the requested item will wait for approval from the user with the respective group (Cohesity ProtectVM).
4. To approve the request, login to the instance using the credentials that belong to the Cohesity ProtectVM group. See Execute Approvals section for details.

NOTE:

- Only unprotected virtual machines can be selected for protection.
- You cannot select virtual machines from different clusters to protect at the same time.

Unprotect VM

1. Type **Cohesity** in the search bar. Navigate to **Virtual Machines** > **Virtual Machines List**.
2. Select a virtual machine and click **Unprotect**.

NOTE: Only one VM can be selected to unprotect at one instance. Selecting multiple VMs to unprotect displays an error.

3. On selecting the VM to unprotect, in the displayed prompt, click **OK**.
4. In the displayed catalog page, select the **Protection Job Name** from which the virtual machines have to be unprotected and click **Order Now**.
5. After submitting the catalog item, a request will be created for the catalog item. If the Approval is enabled for this action in the configuration page, then the requested item will wait for the approval from the user with respective group (Cohesity UnprotectVM).
6. To approve the request, login to the instance using any of the users with **Cohesity UnprotectVM** group membership. See Execute Approvals section for details.

Recover VM

1. Type **Cohesity** in the search bar. Navigate to **Recover** > **Recover VM**.
2. Select a virtual machine and click **Recover VM**.

Note: Only one VM can be selected at a time to be recovered. If multiple VMs are selected, an alert displays.

3. Select the **Recover Points** to indicate the time up to which the virtual machines have to be recovered.
4. To schedule the restore workflow, enable the option **Schedule the Restore,** and select the appropriate time slot in the **Scheduled Date** field.
5. To modify the recovered VM name or the recovery location, select **Change Recover Options**.
6. Click **Order Now**.
7. After submitting the catalog item, a request is created for the catalog item. If the approval is enabled for this action in the configuration page, then the requested item will wait for the approval from the user with respective group (Cohesity RecoverVM).
8. To approve the request, login to the instance using any of the users with Cohesity RecoverVM group membership. See Execute Approvals section for details.
9. Once the requested item is approved, it will call the corresponding REST client API to start the process for recovering the selected virtual machine in the Cohesity cluster and a status message displays.

Clone VM

1. Type **Cohesity** in the search bar. Navigate to **Clone** > **Clone VM**.
2. Select a virtual machine, and click **Clone VM**.

Note: Only one VM can be selected at a time. If multiple VMs are selected, the alert *Select only one VM at a time to Clone* displays.

3. To schedule the clone workflow, enable the option **Schedule the Cloning,** and select the appropriate time slot in the **Scheduled Date** field.
4. In the details page, select the Recover Points at which time the virtual machines have to be cloned. In case of changing the cloned VM name, select **Rename Clone VMs** as **Yes**. Select the Source, Resource Pool and View.
5. Click **Order Now**.
6. After submitting the catalog item, a request will be created for the catalog item. If the approval is enabled for this action in the configuration page, then the requested item will wait for the approval from the user with respective group (Cohesity CloneVM).
7. To approve the request, login to the instance using any of the users with Cohesity CloneVM group. See Execute Approvals section for details.
8. Once the requested item is approved, it will call the corresponding REST client API to start the process for cloning the selected virtual machine in the Cohesity cluster and the following status message displays.

Move VM

1. Type **Cohesity** in the search bar. Navigate to **Virtual Machines** > **Virtual Machines List**.
2. Select a virtual machine that is already ***Protected***, and in the Virtual Machines detail page, click **Move to another Protection job**.

Note: This option will not be available for virtual machines which are not protected.

3. In the **Move VM** page, the current protection job to which the selected VM is associated with displays. Select the **New Protection Job** to which the VM must be moved for protection. Click **Order Now**.
4. After submitting the catalog item, a request will be created for the catalog item. If the approval is enabled for this action in the configuration page, then the requested item will wait for the approval from the user with respective group (Cohesity MoveVM).
5. To approve the request, login to the instance using any of the users with Cohesity MoveVM group. See Execute Approvals section for details.
6. Once the requested item is approved, it will call the corresponding REST client API to start the process for moving the selected virtual machine in the Cohesity cluster and a success message displays accordingly.

Run Jobs

1. Type **Cohesity** in the search bar. Navigate to **Protection Jobs** > **Protection Jobs**.
2. Select the protection job to run and click **Run Job**.
   On running the job in SNOW, it will call the corresponding REST API to trigger the protection job in the respective Cohesity cluster.

Recover Files/Folders

You can either search for specific files/folders and then proceed to choose files/folders for recovery or directly click **Recover Files/Folders** option and then choose **files/folders for recovery**.

1. Type **Cohesity** in the search bar. Navigate to **Recover** > **Recover Files/Folders or Recover > Search Files/Folders**
2. Search for the specific file/folder you want to search in the Cohesity cluster and click **Search**.
   The corresponding files/folders based on the keyword match is populated.
3. Select the file/folder to be recovered and click **Recover Files or Folders**.

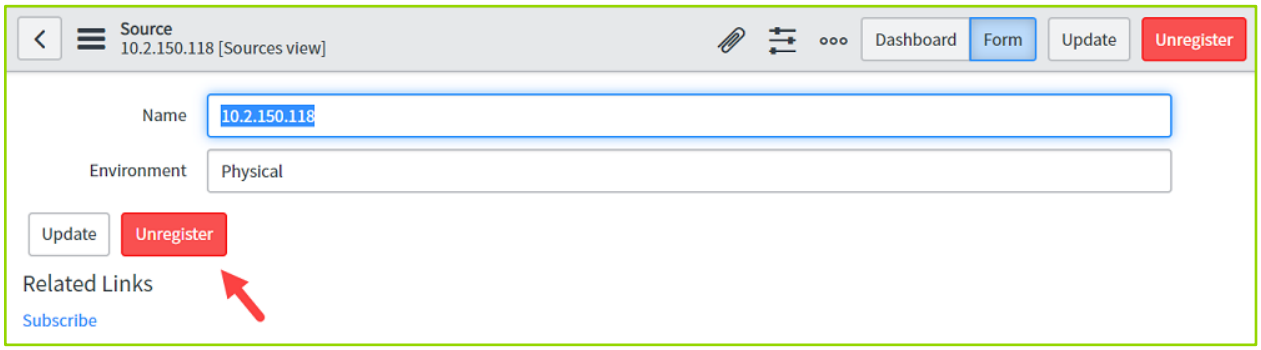
Note: Only one file/folder can be selected at a time. If multiple files/folders are selected, an alert displays.

4. Select the recovery points till at which the file/folder have to be recovered. If the file/folder has to be recovered to a different source, select the server name from the list and provide the username and password of the selected source. If the file has to be recovered to a different location, then select **Recover to original location** to **No** and provide the **Recover location**. Click **Order Now**.
5. To schedule the recovery of file/folders, enable the option **Schedule the Recovery,** and select the appropriate time slot in the **Scheduled Date** field.
6. After submitting the catalog item, a request is created for the catalog item. If the approval is enabled for this action in the configuration page, then the requested item will wait for the approval from the user with respective group (Cohesity RecoverFile).
7. To approve the request, login to the instance using any of the users with Cohesity RecoverFile group. See Execute Approvals section for details.
8. Once the requested item is approved, it will call the corresponding REST client API to start the process for recovering the selected file/folder in the Cohesity cluster and a success status message displays.

Unregister a Source

To unregister a source from the cluster and remove all the resources from the associated tables:

1. Type **Cohesity** in the search bar. Navigate to **Protection Source** > **Sources**.
2. Click on the source (VMware or physical server) that must be unregistered.
3. Click **Unregister**.



4. In the confirmation prompt, click **OK** to unregister.

Delete Protection Job

You can delete a previously protected vCenter or a physical server (file/block-based).

1. **Type Cohesity** in the search bar. Navigate to **Protection Jobs** > **Protection Jobs**.
2. Click the name of the job that you want to delete.
3. In the details page, click **Delete Job**.
4. In the confirmation prompt, click on the appropriate option depending on the requirement.

Approvals

As an admin, you must approve various requests for SNOW tasks such as protect VM, unprotect VM, clone VM, recover VM, and recover files and folders. To see the privileges associated with different groups, see *Privileges* in Cohesity ServiceNow Integration Install and Config Guide.

Procedure

1. Type **Cohesity** in the search bar and navigate to **Requested/Approvals** > **My Approvals**.
2. Click the appropriate record to approve a request.
3. Update the request by providing comments in the **Comments** field, and click **Approve/Reject**.
4. After the request is approved, you can view the updated data in the Cohesity platform.

Cohesity Alert Incident Management

Cohesity supports integration with ServiceNow to enable seamless translation of alerts to incident tickets in ServiceNow's incident management and IT service management system. The following Alert management methods are supported:

- Email-based alerts
- Webhooks

Alerts generated in Cohesity platform automatically trigger incidents in ServiceNow. On closing the incident, the alert is automatically resolved in Cohesity when you have configured the cluster with **Webhook** option.

When an alert is generated in Cohesity cluster, an incident is created for the alert in ServiceNow Incident database.

1. Type **Incident** in the search bar and navigate to **Incident** > **All**.
2. Select the incident to resolve that has been generated due to Cohesity Alert.
3. Select the **Caller** from the reference table.
4. Select the **Resolution Code** and provide the **Resolution notes** under the Resolution Information section.
5. Once all the required details are provided, click **Resolve**.
   On resolving the incident, it will call the corresponding REST client API to start the process for resolving the selected incident in the Cohesity cluster and display the status message of the resolution process.

Dashboard

Cohesity dashboard will be visible to those with the role **Cohesity Admin** or **Cohesity User** group. You can choose a cluster from the drop-down to display details specific to that cluster in the dashboard.

- **Protection Jobs Summary**: Type **Cohesity** in the search bar. Navigate to **Dashboard** > **Protection Jobs**.
  Protection Jobs
  - Errors: Total count of triggered job, that ends with Failed state
  - Warnings: Total count of triggered job, that ends with Warning
  - Success: Total count of triggered job, that ends with Success
  - Cancelled: Total count of triggered job, that has been cancelled
  - Running: Total count of triggered job, that are running
  - SLA Compliance: Total count of protection job, whose SLA is passed
  - Total Job runs: Donut chart that shows the count of triggered protection job's status
  - Job Runs (last 24 Hrs): Bar chart that shows the status of the protection job that has been triggered in last 24 hours
  - Job Details: Table that shows the available protection job in the Cohesity cluster

- **Virtual Machines Summary**: Type **Cohesity** in the search bar. Navigate to **Dashboard** > **Virtual Machines-Protection Summary**.
  - VM Protected—Bar chart that shows the count of the VM protected and unprotected
- **Storage Statistics Summary**: Type **Cohesity** in the search bar and select **Storage Stats**. This shows the storage consumption for a cluster.
- **Request and Approval**: Type **Cohesity** in the search bar and select **Request & Approval**. This dashboard displays any workflows execution requests for approvals and other related data.

Cohesity Logs for Troubleshooting

You can access the Cohesity Logs to analyze and debug the problems logged.
The Cohesity Logs can be accessed in the following ways:

- The logs can be seen under **Cohesity Application** > **Cohesity Logs** > **Cohesity Logs** in the ServiceNow instance.
- Navigate to the folder where the MID Server is installed/configured. The MID Server folder **agent/logs/agent0.log.0** file will be populated with debug logs in that location.

To enable the debug logs in MID Server:

1. Log in to the ServiceNow instance with system admin credentials.
2. Navigate to **MID Server** > **Servers**.
3. Select the MID Server in which debug log must be enabled.
4. Under the **Configuration Parameters** tab, click **New**.
5. Select the **Parameter Name** as '***debug.logging (Debug logging enable. Default: false)***' and set the Value as ***'true'***.
6. Click **Submit**.

Now, the MID Server logs will start to capture the debug logs.

The following failure modes are captured in the Cohesity application:

1. Case 1 : If credentials are not matching (may be invalid username/password combo)
   To resolve, you must update the configured cluster with valid username/password or domain details and retry.
2. Case 2: If the discovery of a configured cluster failed with '**Login Failed**' even if the credential of the cluster provided is correct.
   To resolve, restart the MID Server that has been assigned to the specified cluster and try to discover the cluster again.
3. Case 3: If http request is not correct
   This could happen if the cluster is not reachable or of if the cluster is down.
   To resolve, check the cluster status and restart accordingly.
4. Case 4: If MID Server is down or the MID Server is not able to reach the Cohesity environment. The error displayed is as follows:

   Error: 'Exception occured, com.glide.ecc.ECCResponseTimeoutException: No response for ECC message request with sysid=76bda8e32f7990102e12ae5df699b6cc after waiting for 30 seconds in ECC Queue'. This might be caused if the MID Server is down. Make sure whether the MID Server is up and running.
   To resolve, ensure that the MID Server is up and running.

Your Feedback

Was this document helpful? Send us your feedback!

ABOUT COHESITY

Cohesity radically simplifies data management. We make it easy to protect, manage, and derive value from data -- across the data center, edge, and cloud. We offer a full suite of services consolidated on one multicloud data platform: backup and recovery, disaster recovery, file and object services, dev/test, and data compliance, security, and analytics -- reducing complexity and eliminating mass data fragmentation. Cohesity can be delivered as a service, self-managed, or provided by a Cohesity-powered partner.

Visit our website and blog, follow us on Twitter and LinkedIn and like us on Facebook.