

IT Analytics Backup Manager Solution for ServiceNow Installation and Configuration Guide

Release 11.8

IT Analytics Backup Manager Solution for ServiceNow Installation and Configuration Guide

Last updated: 2026-08-12

Legal Notice

Copyright © 2026 Cohesity, Inc. All rights reserved.

© 2026 Cohesity, Inc. All Rights Reserved. Cohesity, the Cohesity Logo and other Cohesity Marks are trademarks of Cohesity, Inc. in the US and/or internationally. The information supplied herein is the confidential and proprietary information of Cohesity and may only be used (a) by the intended recipients and (b) in conjunction with validly licensed Cohesity software and services. Find the terms of Cohesity licenses at www.cohesity.com/agreements.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. COHESITY SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

- Go to [Cohesity Support](#), to search in our knowledge base; or contact us by phone - United States and Canada: 1-855-9CO-HESI (926-4374), option 2.
- Log in to the [Cohesity Support Portal](#) to create a new case.
- Click the (?) icon on the Cohesity UI and select Support Portal.

Support/Service Assistance

First, contact the Service Provider that you have contracted for service and support. If you work directly with Cohesity and have a product warranty/entitlement, repair pricing, or technical support-related question, see your options below:

- To find solutions to your product issues or for suggestions or best practices, visit the [Cohesity Knowledge Base](#).
- Log in to the [Cohesity Support Portal](#) to create a new case.
- To monitor your open cases, log in to the portal and click the **Cases** tab on the home page. This page should have all the case statuses and updates. You can also view individual case status.

Cohesity Software Running on Partner Hardware

For Cohesity software running on qualified third-party hardware, the following support workflow applies:

1. The customer may contact Cohesity Support first if the issue cannot be determined as a hardware issue.

Note: Cohesity cannot process hardware replacement requests for partner hardware.

2. Cohesity Support triages the issue. If it is a software issue, Cohesity Support continues to work on it.
3. If it is a hardware/firmware issue or is suspected to be a hardware/firmware issue, Cohesity provides information about the issue to the customer and requests that the customer open a support ticket with the appropriate partner.
4. If needed, Cohesity Support can join a three-way call with the partner and the customer.
5. The customer informs Cohesity Support on the progress of the partner's case.

Contents

Chapter 1	IT Analytics ServiceNow App Overview	6
	Backup Manager Overview	6
	Prerequisites	6
Chapter 2	Install and Configure	8
	Overview	8
	Initial Setup on IT Analytics Portal	8
	ServiceNow Configuration - Part One	11
	Step-1: Create MID server	11
	Step-2: Create a MID server user	12
	Step-3: Set MID server user role	13
	Step-4: Set the base URL	14
	Step-5: Configure the data source	16
	Step-6: Set REST API callback User and Password	20
	Step-7: Set REST message or HTTP method to use MID Server	21
	MID server installation on IT Analytics Portal server	22
	Step-1: Download a ServiceNow MID server	22
	Step-2: Install and configure ServiceNow MID server on your IT Analytics Portal server	24
	Step-3: Start the MID server service	26
	Step-4: Enable ServiceNow and data protection	27
	ServiceNow Configuration - Part Two	27
	Step-1: Validate the MID server	27
	Step-2: Set the schedule for the Import Set	28
Chapter 3	Test the IT Analytics ServiceNow App	29
	About Testing	29
	Test the IT Analytics ServiceNow App Configuration	29
	Test the IT Analytics ServiceNow App	36
Chapter 4	Troubleshooting	41
	About Troubleshooting	41
	Issue: Backup failures are not creating incidents in ServiceNow	41

data protection does not display any record	42
MID server registration with IT Analytics ServiceNow App fails	42

IT Analytics ServiceNow App Overview

This chapter includes the following topics:

- [Backup Manager Overview](#)
- [Prerequisites](#)

Backup Manager Overview

IT Analytics Protection Suite captures backup and data protection events from major backup vendors and provides one unified view of your enterprise data protection from a centralized portal. Backup operators are alerted about problems such as unprotected or under-protected clients and backup failures. Intelligent analytics provide proactive insights about clients at risk for RTO failure.

The IT Analytics ServiceNow App allows IT Analytics-detected backup issues to automatically create incidents in ServiceNow. Users in ServiceNow can see the key issue details such as client, policy, error number/message, and so on to quickly resolve the problem. Backup details, incident numbers, and status are automatically synchronized between the IT Analytics and ServiceNow applications to provide the full audit trail required for compliance.

This installation guide walks you through the steps you need to take within your ServiceNow application and the IT Analytics Portal to deploy and configure the IT Analytics ServiceNow App to integrate the two systems.

Prerequisites

- Previously installed and operational IT Analytics version 11.8 or later

- ServiceNow application (NewYork, Orlando, Paris, or later). See *ServiceNow Configurations* section in the *IT Analytics Certified Configurations Guide* for the most current supported versions.

Install and Configure

This chapter includes the following topics:

- [Overview](#)
- [Initial Setup on IT Analytics Portal](#)
- [ServiceNow Configuration - Part One](#)
- [MID server installation on IT Analytics Portal server](#)
- [ServiceNow Configuration - Part Two](#)

Overview

Installation and configuration requires coordination between the ServiceNow application and your IT Analytics environment. Alternate between the two applications to complete the installation. Certain operations require System Administrator privileges.

Initial Setup on IT Analytics Portal

The IT Analytics ServiceNow App makes REST API calls back to the IT Analytics Portal to update the jobs in the IT Analytics system with the ServiceNow Incident Status and Incident Number. This API call requires a valid user ID and password within the IT Analytics Portal. To set this up:

Create a user account

1. Create a new user account in the IT Analytics Portal and note the username and password. This new user does not require any specific privileges.

Veritas NetBackup™ IT Analytics

Inventory Reports Alerts Admin

Users and Privileges

Filter by User

Add User

Active: Yes Type: End User

Login* Password* Repeat password*

First name* Last name* Email*

Work phone Cell phone

Home Host group*

The license entitlement of the host group's domain will be available to the user.
Pick a host group from the list below:

- Aptare

OK Cancel Help Privacy Policy

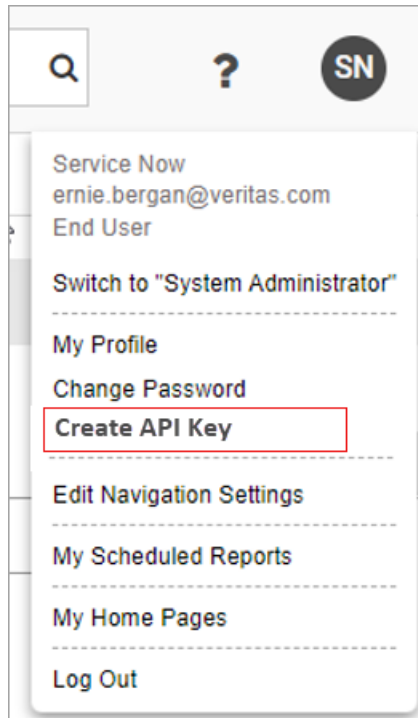
User Name	Home Group
1, Iberia	/Aptare/Iberia
2, Iberia	/Aptare/Paco
A, A	/Aptare
a, Himans	/Aptare
abuebid,	/Aptare
Accel, Ac	/Aptare
Adami, Me	/Aptare
ADMIN, IT	/Aptare/현대자동차그룹
Admin, RS	/Aptare
Ahlgim, M	/Aptare
Ahmad, In	/Aptare
Ajala, Afol	/Aptare
Akhand, T	/Aptare
Al Ahmad, Ibrahim	/Aptare
Al Ahmad, Shaban	/Aptare
Al Ahmad, Youssef	/Aptare

- Log into the IT Analytics Portal with this username/password and accept the EULA.

For details on how to create users, refer to the *IT Analytics User Guide* and search for *Creating Portal User Accounts*.

Authorize API Access

- 1 Log into IT Analytics Portal API interface as the user created above and authorize access.
- 2 Right-click on the initials of the ServiceNow account user in the upper right, then select the **Create API Key** option.



- 3 Save or note down the API key.

Add advanced parameter

- 1 Login as IT Analytics Portal administrator and go to **Admin > Advanced > System Configuration > Custom Parameters** and click **Add**.
- 2 Create a new custom parameter with **Custom Parameter Name** as **portal.legacy.restapi.allow** and **Custom Parameter Value** as **True**.
- 3 Remember to click **Save and Apply**.

ServiceNow Configuration - Part One

The first part of the ServiceNow configuration consists of the following steps:

1. [Step-1: Create MID server](#). Skip this step if you have an existing MID server.
2. [Step-2: Create a MID server user](#)
3. [Step-3: Set MID server user role](#)
4. [Step-4: Set the base URL](#)
5. [Step-5: Configure the data source](#)
6. [Step-6: Set REST API callback User and Password](#)
7. [Step-7: Set REST message or HTTP method to use MID Server](#)

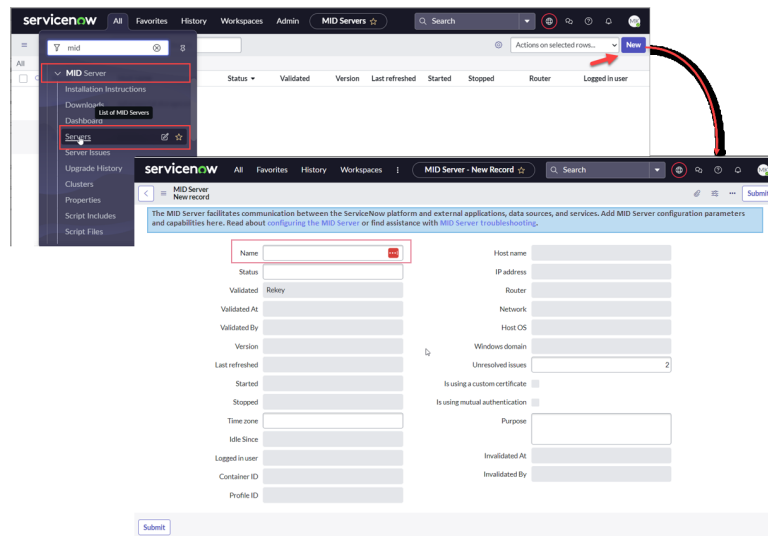
Step-1: Create MID server

You can skip this step if you already have an existing MID server.

Inside your IT Analytics ServiceNow App:

- 1 Create a new MID Server record using the **Filter Navigator** to search for **MID Server**.
- 2 Select **MID Server**.
- 3 Go to **MID Server > Servers**.
- 4 Click **New** to create a new MID Server record.
- 5 Enter the name of the new MID Server. For example: **NITAMID**.

Figure 2-1 Create MID Server

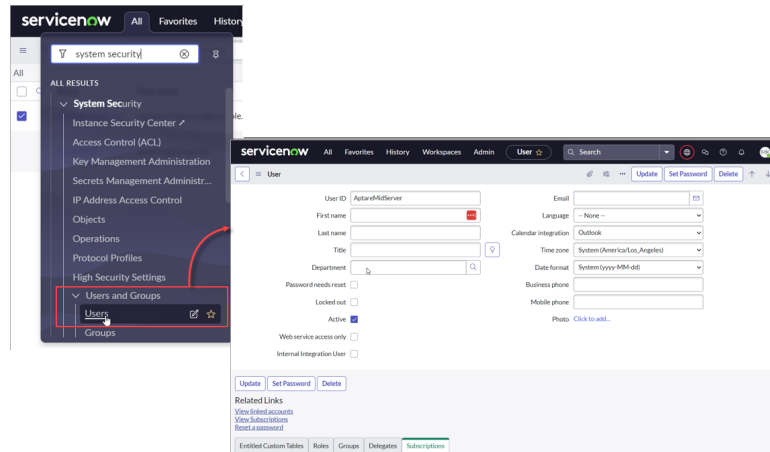


Step-2: Create a MID server user

Inside your IT Analytics ServiceNow App:

- 1** Use the **Filter Navigator** to search for **System Security**.
- 2** Select **Users and Groups** under **System Security**.
- 3** Select **Users**.
- 4** Select **New** to create new user and save the user ID and password for later use.

Figure 2-2 Create a MID Server user

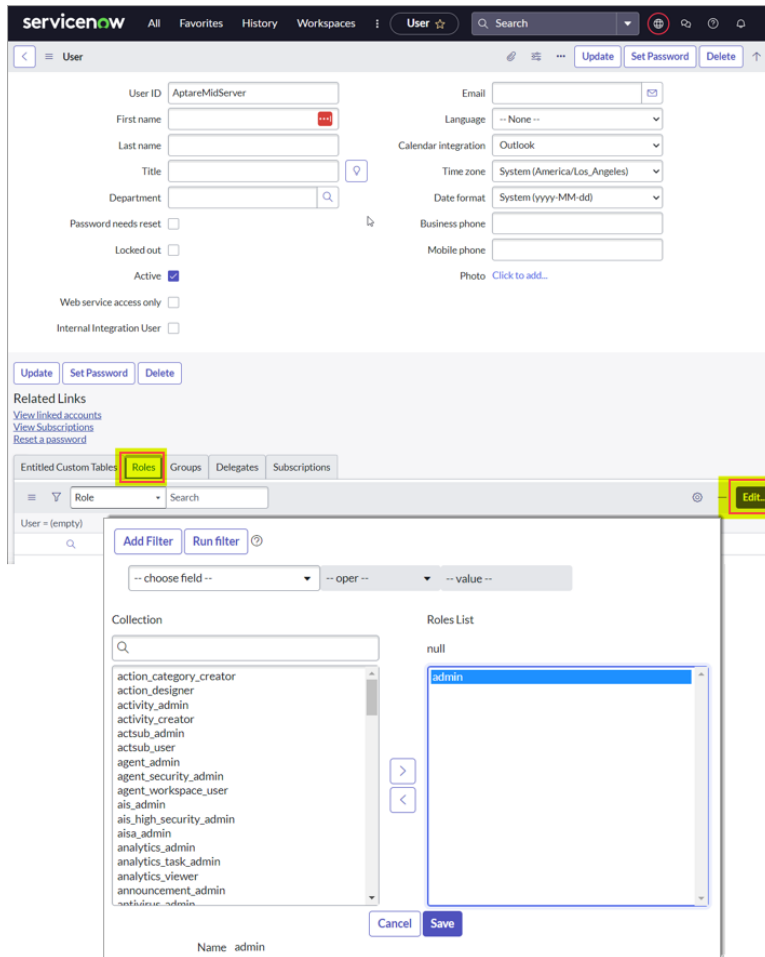


Step-3: Set MID server user role

Inside your IT Analytics ServiceNow App:

- 1 Select the user that you just created in the previous step.
- 2 Select **Roles** and click **Edit**.
- 3 Double-click **admin** to select the role and then click **Save**.

Figure 2-3 Set MID Server user role



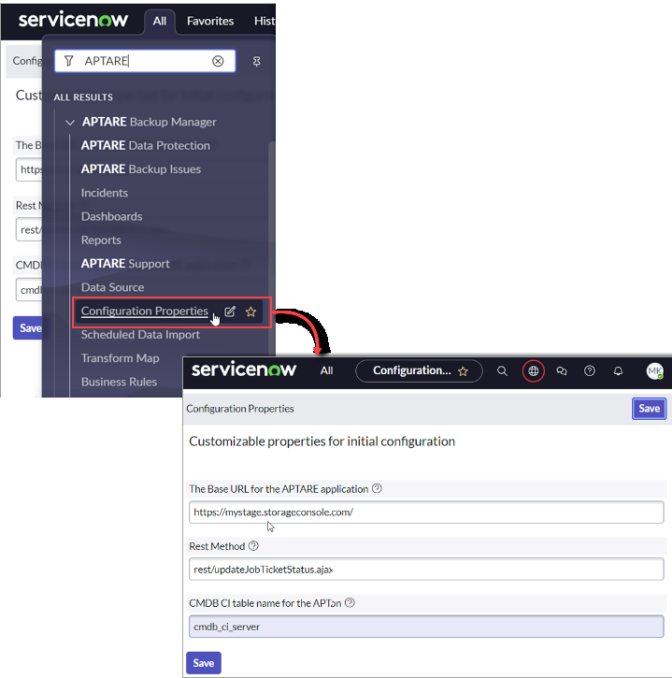
Step-4: Set the base URL

Inside your IT Analytics ServiceNow App:

- 1 User the **Filter Navigator** to search for **APTARE**.
- 2 Select **Configuration Properties**.
- 3 Set the value of **BaseURL** to the URL of the IT Analytics Portal instance.

For example: <https://itanalyticsportal.companydomain.com/>

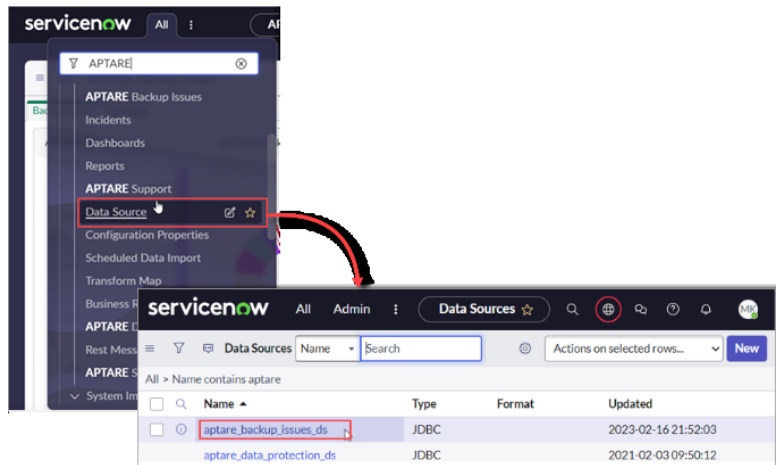
Figure 2-4 Set base URL



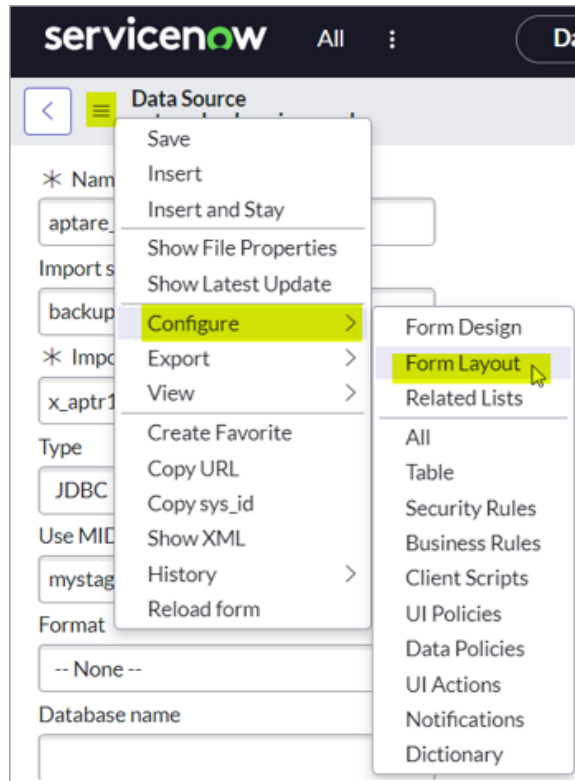
Step-5: Configure the data source

Inside your IT Analytics ServiceNow App:

- 1 Use the **Filter Navigator** to search for **APTARE**.
- 2 Select **Data Source**.



- 3 Select **aptare_backup_issues_ds** and click the link to open the dialog.
- 4 Configure the connection URL in the data source:
 - Click the **Additional Actions** menu link and select **Configure > Form Layout**.



- Double-click **Connection URL** to move it under Selected fields.

Configuring Data Source form

Available

- Delete Recovery->Initiating metadata
- Deleted Application File->Parent
- Deleted File Related->Parent
- Import Export Map->Data source
- Import Set->Data source
- Indicator->Data source
- OAuth OIDC Entity->Provision data source
- OAuth OIDC Entity->User Info Data source
- Robust Transformer
- Scheduled Data Import->Data source
- Transforms
- Updates
- Versions
- Connection URL**

Selected

- Password(scp_password)**
- CSV delimiter
- Private keyfile
- Use last run datetime
- Last run datetime
- Last run database field
- System keystore
- Request action
- Support pagination
- Limit
- Offset
- [- end_split -]
- Data Loader
- Parsing script

Cancel Save

Form view and section

View name: Default view

Section: Data Source

Create new field

Name:

Type: String

Field length: Small (40)

Add

Related Links

Show versions

- Enter the **Password** for the **Data Source**.
By default, this user or default schema is **portal** and click **Update**. This is the main user in the IT Analytics Oracle database.

The screenshot shows the ServiceNow 'Data Source' configuration page for 'aptare_backup_issues_ds'. The page is divided into two main sections: 'General' and 'Advanced'. The 'General' section includes fields for Name, Import set table label, Import set table name, Type, Use MID Server, Format, Database name, and Database port. The 'Advanced' section includes fields for Application, Username, Password, Server, Query, Query timeout, Connection timeout, Table name, Use last run datetime, Last run datetime, Last run database field, and Connection URL. The 'Use MID Server' field is set to 'mystagemidserver'. The 'Format' field is set to '-- None --'. The 'Password' field is masked with dots. The 'Server' field is set to '// :1521'. The 'Table name' field is set to 'apt_job_ticket'. The 'Last run datetime' field is set to '1676534421'. The 'Last run database field' field is set to 'MODIFIED_EPOCH_TIME'. The 'Connection URL' field is set to 'jdbc:oracle:thin:@// :1521/scdb'.

- In the **Use MID Server** section, select the MID Server that you created above.

- Add connection URL in this format:

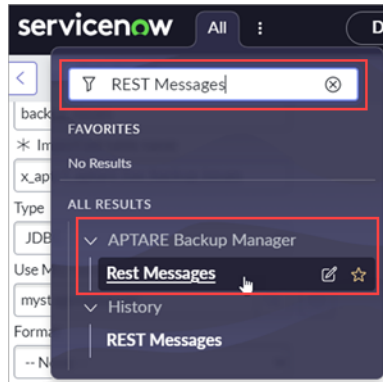
`jdbc:oracle:thin:@//IP_ADDRESS_OF_NITA_PORTAL_SERVER:1521/scdb`

- Repeat entries of the above fields for **aptare_dataprotection_ds**.

Step-6: Set REST API callback User and Password

Inside your IT Analytics ServiceNow App:

- 1 Use the **Filter Navigator** to search for **REST Messages**.

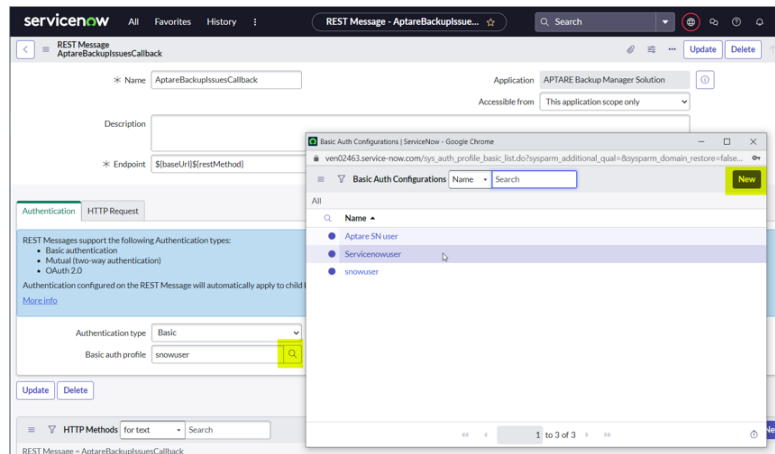


- 2 Select **AptareBackupIssuesCallback** and open the window.
- 3 In the **Basic auth profile**, click the search icon. A new window is displayed.



- 4 Click **New**. A secondary window is displayed.
- 5 Enter a **Username** and **Password**. This user must be the pre-created user with the IT Analytics system, created in the Initial Setup before.

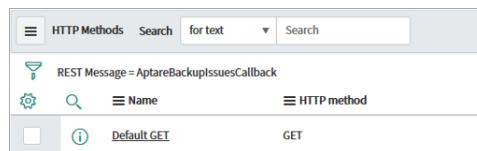
See “[Step-2: Create a MID server user](#)” on page 12.



Step-7: Set REST message or HTTP method to use MID Server

Inside your IT Analytics ServiceNow App:

- 1 Use the **Filter Navigator** to search for **REST Messages**.
- 2 Select **AptareBackupIssuesCallback**.
- 3 In the **REST Message** window, select the **Default GET** in the **HTTP Methods** section.



- 4 On the **HTTP Method** page, select the **HTTP Request** tab and enter the name of the MID Server that was created before.

- 5 Create an Authorization in the HTTP Headers area. Place the REST API key generated for the user in the **Value** field

MID server installation on IT Analytics Portal server

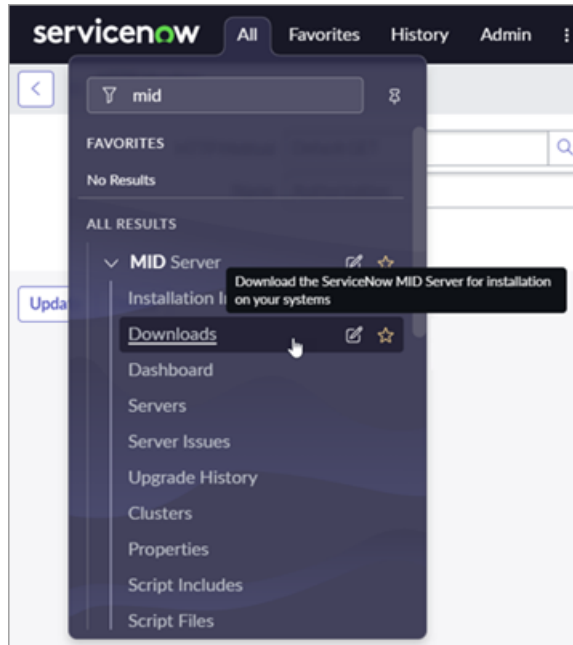
After you have completed the steps listed in [ServiceNow Configuration - Part One](#), complete the following steps. You can skip the first three steps if you already have an existing MID server.

1. [Step-1: Download a ServiceNow MID server](#)
2. [Step-2: Install and configure ServiceNow MID server on your IT Analytics Portal server](#)
3. [Step-3: Start the MID server service](#)
4. [Step-4: Enable ServiceNow and data protection](#)

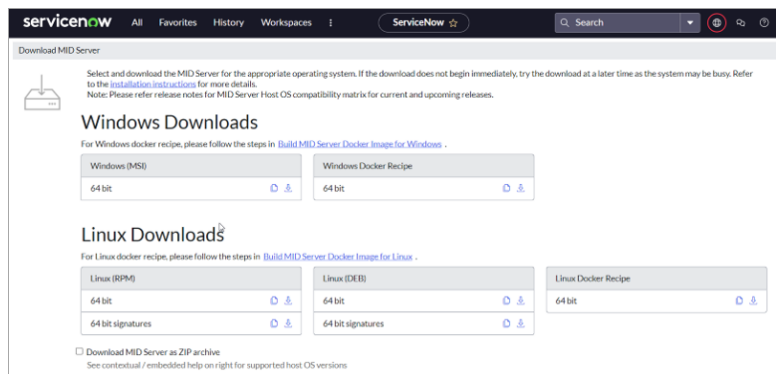
Step-1: Download a ServiceNow MID server

System Admin role is required to perform this step. Skip this step if you have an existing MID server.

- 1 Use the **Filter Navigator** to search for and select **MID Server** in the IT Analytics ServiceNow App.
- 2 Select **Downloads**.



- 3 Select the appropriate download binary to match your IT Analytics Portal server operating system.



Step-2: Install and configure ServiceNow MID server on your IT Analytics Portal server

Skip this step if you have an existing MID server.

Windows

On Windows, run the installer on your IT Analytics Portal server. You may want to create a new Windows account (for example: SVCNow) as a service user for the run.

Linux

- 1 Copy the downloaded MID sever files to the IT Analytics Portal server.
- 2 Create a folder under `temp` as `mid_server` where you will download the agent.

```
cd /opt/  
mkdir mid_server  
cd mid_server/
```

- 3 Use the `wget` command to download the binary link obtained from the procedure in Step-1.

```
wget https://install.service-now.com/glide/distribution/
```

- 4 Unzip the package after it is downloaded. You can see this folder after unzipping the package:

```
[root@ip-172-31-4-71 mid_server]# ll  
total 211356  
drwxr-xr-x 16 root root    4096 Feb 27 15:52 agent  
-rw-r--r--  1 root root 216422894 Jan  3 18:30 mid.kings
```

5 Get inside the folder to view its content.

```
[root@ip-172-31-4-71 agent]# ll
total 2908
drwxr-xr-x 3 root root 4096 Jan 3 09:57 bin
drwxr-xr-x 2 root root 4096 Dec 13 14:51 conf
-rw-rw-rw- 1 root root 7339 Feb 27 15:53 config.xml
drwxr-xr-x 2 root root 4096 Dec 13 14:51 etc
-rw-r--r-- 1 root root 18509 Dec 13 14:51 EULA.docx
drwxrwxrwx 2 root root 4096 Feb 27 15:52 lib
-rwxr-xr-x 1 root root 505 Dec 13 14:51 installer.bat
-rwxr-xr-x 1 root root 509 Dec 13 14:51 installer.sh
drwxr-xr-x 2 root root 4096 Jan 3 09:57 jetty
drwxr-xr-x 6 root root 4096 Jan 3 09:57 jre
drwxr-xr-x 2 root root 4096 Feb 27 15:53 keystore
drwxr-xr-x 4 root root 20480 Dec 13 14:51 lib
drwxrwxrwx 2 root root 4096 Feb 28 07:23 logs
drwxr-xr-x 2 root root 4096 Dec 13 14:51 midinstaller
drwxr-xr-x 4 root root 4096 Feb 27 16:54 package
drwxr-xr-x 2 root root 4096 Jan 3 10:01 properties
-rw-r--r-- 1 root root 19938 Dec 13 14:51 README.docx
drwxr-xr-x 5 root root 4096 Feb 27 15:52 scripts
-rw-r--r-- 1 root root 2786132 Dec 13 14:51 ServiceNow Open Source Disclosure 110217KMS0.pdf
-rwxr-xr-x 1 root root 17 Dec 13 14:51 start.bat
-rwxr-xr-x 1 root root 16 Dec 13 14:51 start.sh
-rwxr-xr-x 1 root root 16 Dec 13 14:51 stop.bat
-rwxr-xr-x 1 root root 15 Dec 13 14:51 stop.sh
drwxrwxrwx 7 root root 4096 Feb 28 07:23 tmp
-rw-r--r-- 1 root root 26235 Dec 13 14:51 wrapper-development-license-1.1.txt
-rw-r--r-- 1 root root 11952 Dec 13 14:51 wrapper-tsims-addendum-1.1.txt
```

Update the ServiceNow instance URL in this file and also the mid_server_user that you created during the ServiceNow

Logs

./start.sh to start the agent
./stop.sh to stop the agent

6 Configure the agent using config.xml file.

```
nano config.xml
<parameter name="url" value="https://example12345.service-now.com/">
<!-- If your ServiceNow instance has authentication enabled
(the normal case), set these parameters to define the
username and password the MID server will use to log into
the instance. -->
<parameter name="mid.instance.username" value="demo_mid_server"/>
<parameter name="mid.instance.password" secure="true" value=
"MyP@ssw0rd"/>
```

In the above agent configuration:

- `https://example12345.service-now.com/` is the URL of the ServiceNow instance.
- `mid.instance.username` is the MID server user created in [Step-2: Create a MID server user](#).
- `MyP@ssw0rd` is the password for the user. After entering the password for the first time, the agent encrypts it like this.
- `MyP@ssw0rd` is the initial true password entered in clear text. This password is encrypted in the next step below. After the services are started, the value in the XML is changed to the following:

```
<parameter name="mid.instance.password" secure="true" value=
"encrypted:sAM91EPasSw0rdOnly==" />
```

7 Save the file and start the server.

```
[root@ip-172-31-4-71 agent]# ./start.sh
Starting ServiceNow MID Server...
Waiting for ServiceNow MID Server....
running: PID: 3912
```

8 After your agent is correctly installed, go back to the ServiceNow instance and mark this step as complete.

Configure the MID Server on your IT Analytics Portal server

- 1 Go to the directory where MID Server is installed, `cd` to the agent irectory and edit `config.xml`.
- 2 Change the `config.xml` to set the user and password for the parameters `mid.instance.username` and `mid.instance.password`. Use the credentials set under [ServiceNow Configuration - Part One](#).
- 3 Change `config.xml` to set the MID Server name (`name="name" value=<MID server name>`) set under ServiceNow Configuration-Part One [Step-1: Create MID server](#).

Example:

```
<parameter name="mid.instance.username" value="NITAMidServer"/>
  <parameter encrypt="true" name="midinstance.password"
value="encripted:4x/MFMerZ3Cw2by+3FXCkQ==" />
<parameter name="name" value="aptmidwow"/>
```

Step-3: Start the MID server service

Skip this step if you have an existing MID server.

- Linux: Run:

```
$(base_install_dir/start.sh
```

execute `$(base_install_dir/agent/bin/mid.sh` (as root) to set up service to start on boot.

- Windows: Use services management console to start service.

Step-4: Enable ServiceNow and data protection

1. Compile user package for ServiceNow data protection:

- CD to /opt/aptare/database/stored_procedures.
- Back up the user_package.sql file.
- Copy user_package.sql from ../tools directory and overwrite file in ../stored_procedures directory.
- Compile the package using these commands at the sqlplus prompt.

```
su -aptare
sqlplus portal/portaluserpassword@scdb @/opt/aptare/database/
stored_procedures/user_package.sql
```

2. Set up the ServiceNow alert.

See *ServiceNow: Job Finalized Alert Rule* section in the *IT Analytics User Guide* for more information.

ServiceNow Configuration - Part Two

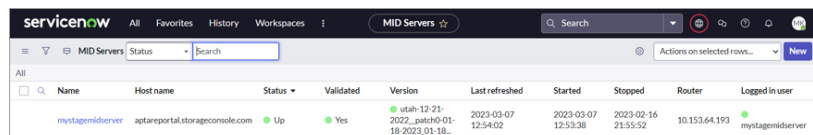
After completing ServiceNow configuration part one, and the steps in the IT Analytics Portal, finish the setup in your IT Analytics ServiceNow App.

1. [Step-1: Validate the MID server](#)
2. [Step-2: Set the schedule for the Import Set](#)

Step-1: Validate the MID server

You must have System Administrator privileges to perform these steps.

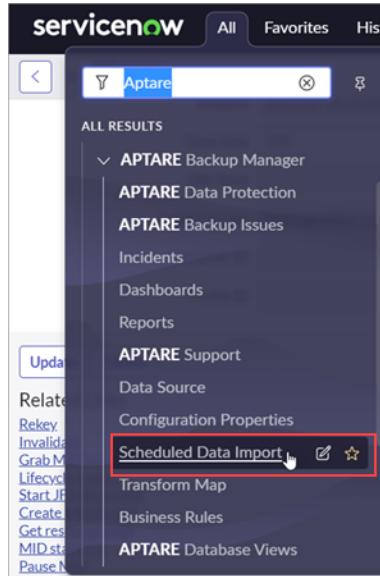
1. Use the **Filter Navigator** to search for the **MID Server**.
2. Select **MID Servers** under **MID Server Configuration**.
3. Open the MID server you created under [Step-1: Create MID server](#) of *Part One*.
4. Click the **Validate** link under **Related Links**.
5. Click **Restart MID** under **Related Links**.



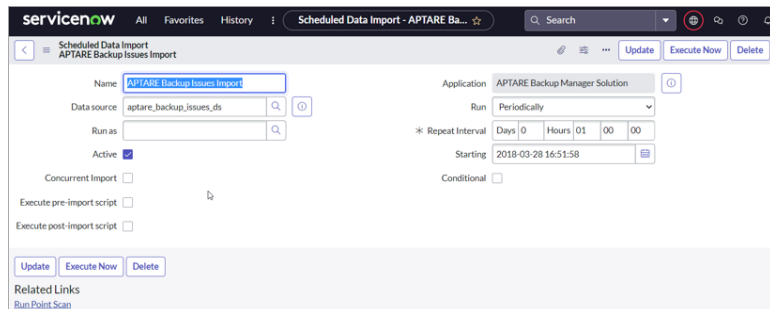
	Name	Host name	Status	Validated	Version	Last refreshed	Started	Stopped	Router	Logged in user
	mystagemidserver	aptareportal.storageconsole.com	Up	Yes	utah-12-21-2022_patch0-01-18-2023,01-18...	2023-03-07 12:54:02	2023-03-07 12:53:38	2023-03-16 21:55:52	10.153.64.193	mystagemidserver

Step-2: Set the schedule for the Import Set

1. Use the **Filter Navigator** to search for **Scheduled Data Import**.



2. Open **APTARE Backup Issues Import**.
3. Select the **Active** checkbox.
4. Set the **Repeat Interval** to the run frequency for the **Scheduled Data Import**. For example, if you set the frequency to **0 Days** and **1 Hour**, the IT Analytics Portal will be polled every hour to search for new job failures.



5. Repeat the above steps for **APTARE Data Protection Import**.

Test the IT Analytics ServiceNow App

This chapter includes the following topics:

- [About Testing](#)
- [Test the IT Analytics ServiceNow App Configuration](#)
- [Test the IT Analytics ServiceNow App](#)

About Testing

The testing procedures in this section help you to:

- [Test the IT Analytics ServiceNow App Configuration](#)
- [Test the IT Analytics ServiceNow App](#)

Test the IT Analytics ServiceNow App Configuration

Prerequisites

Prior to testing your configuration:

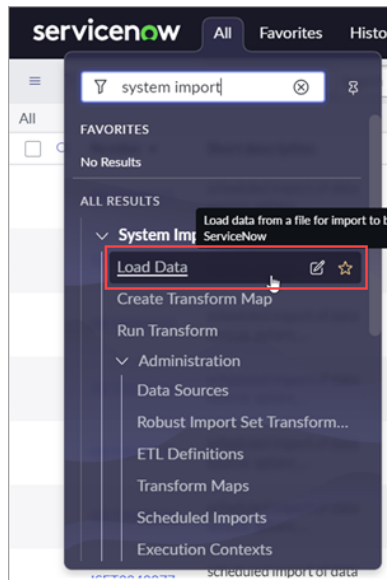
- Populate the table `apt_job_ticket` with test data for easy validation.
- After installation, the test data must appear in ServiceNow as a record under Backup Issues and Incidents.
- You must have System Administrator privileges to perform the testing.

Note: After the testing is complete, remember to clean up the test data.

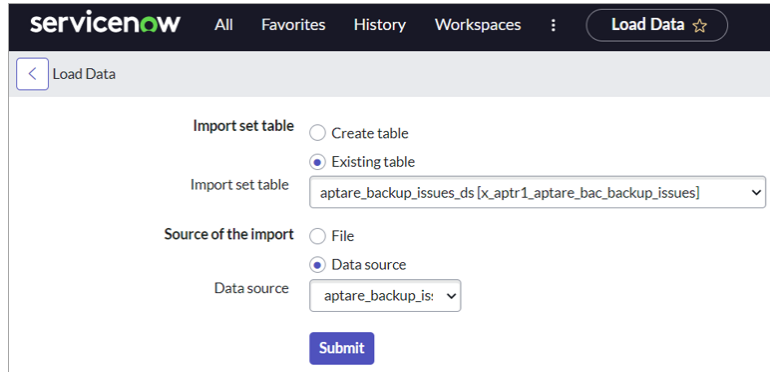
Test the configuration

To test the IT Analytics ServiceNow App configuration:

- 1 Use the **Filter Navigator** to search for **System Import Sets**.
- 2 Select **Load Data** and set **Import set table** as **Existing table** and in the drop down list set **aptare_backup_issues_ds**.

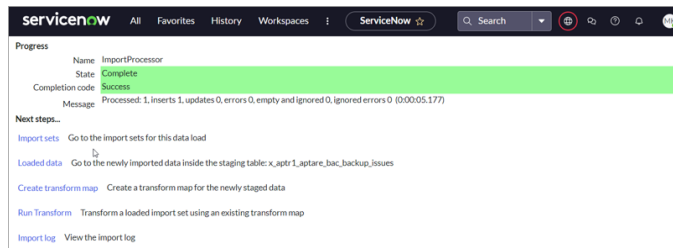


- 3 Set **Source of the Import** as **Data source** and from the **Data source** list, select **aptare_backup_issues_ds**.



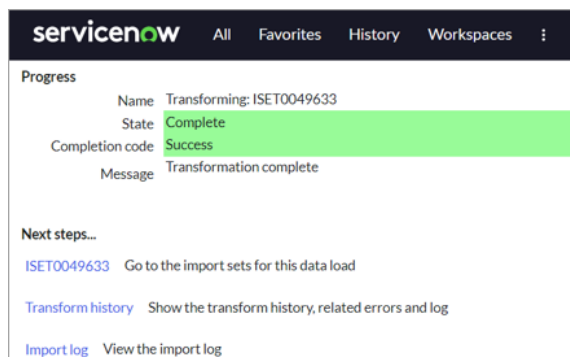
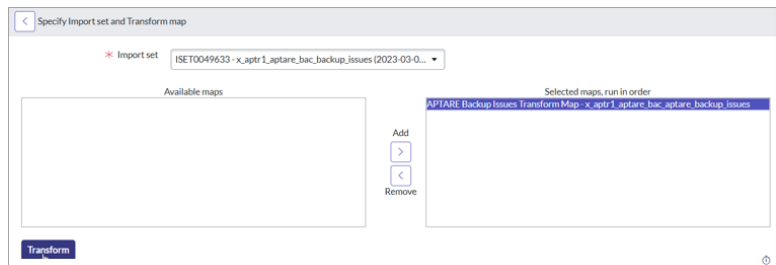
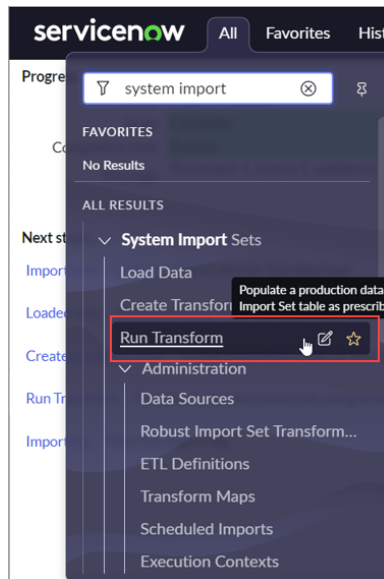
The screenshot shows the 'Load Data' configuration interface in ServiceNow. At the top, there's a navigation bar with 'All', 'Favorites', 'History', and 'Workspaces'. A 'Load Data' button with a star icon is on the right. Below the navigation bar, there's a 'Load Data' header with a back arrow. The main configuration area has three sections: 'Import set table' with radio buttons for 'Create table' and 'Existing table' (selected), a dropdown menu showing 'aptare_backup_issues_ds [x_aptr1_aptare_bac_backup_issues]', 'Source of the import' with radio buttons for 'File' and 'Data source' (selected), and a dropdown menu for 'Data source' showing 'aptare_backup_is:'. A blue 'Submit' button is at the bottom right.

- 4 Click **Submit**. Once the load data completes, the completion page displays a link to transform the imported data set.

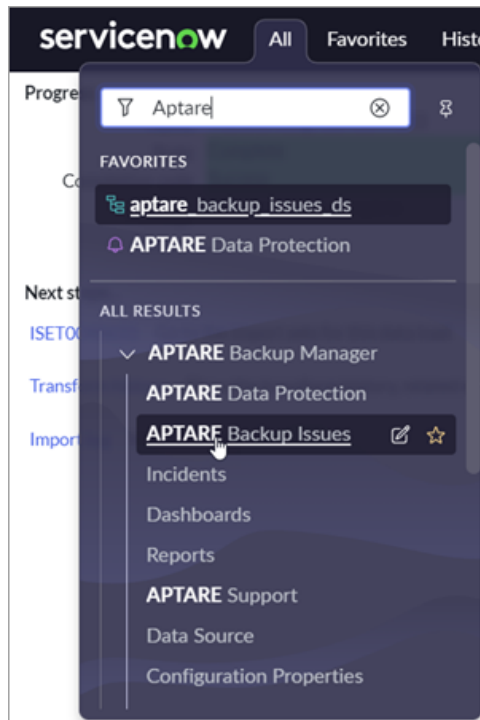


The screenshot shows the 'Progress' page for the 'ImportProcessor' in ServiceNow. The page has a dark header with 'ServiceNow' and a search bar. The main content area has a green progress bar with the following details: Name: ImportProcessor, State: Complete, Completion code: Success, and Message: Processed: 1, Inserts 1, updates 0, errors 0, empty and Ignored 0, Ignored errors 0 (0.00:05.177). Below the progress bar, there's a 'Next steps...' section with links: 'Import sets' (Go to the import sets for this data load), 'Loaded data' (Go to the newly imported data inside the staging table: x_aptr1_aptare_bac_backup_issues), 'Create transform map' (Create a transform map for the newly staged data), 'Run Transform' (Transform a loaded import set using an existing transform map), and 'Import log' (View the import log).

5 Select **Run Transform** under **System Import Sets**.



- 6 Use the **Filter Navigator** to search for **APTARE Backup Issues**.



- Select **APTARE Backup Issues** to view the contents of the table. This populated table validates dataflow to ServiceNow.

The screenshot shows the ServiceNow interface for the 'APTARE Backup Issues' table. The table has columns: Client Name, Server Name, Policy Name, Schedule Name, Product Name, Vendor Job ID, Vendor Status, Error Code, Error Message, and Job Start Date. Two rows are visible, both showing failed backup jobs.

Client Name	Server Name	Policy Name	Schedule Name	Product Name	Vendor Job ID	Vendor Status	Error Code	Error Message	Job Start Date
10.10.17.35	10.10.17.35	VMware backup job_periodic		NAKIVO Backup & Replication	VMware backup job_periodic	Failed	2	Failed	2023-12-11
10.10.17.35	10.10.17.35	VMware backup job_periodic		NAKIVO Backup & Replication	VMware backup job_periodic	Failed	2	Failed	2023-12-11

- Select and open a **APTARE Backup Issue**.
- Click the **Incident** tab.

The screenshot shows the 'APTARE Backup Issues - 57218385' form in ServiceNow. The form is divided into two main sections: 'Job Details' and 'Incident'. The 'Job Details' section contains fields for Client Name (10.10.17.35), Policy Name (VMware backup job, periodic), Product Name (NAKIVO Backup & Replication), Error Code (2), Client Name Aliases (10.10.17.35), Error Message (Failed), Notes (Backup failed. Please restart.), Server Name (10.10.17.35), Schedule Name, Vendor Status (Failed), Configuration Item, and IP Addresses (10.10.17.35). The 'Incident' section is currently empty, but the 'Incident' icon is highlighted in the Job Details section.

- Click the **Incident** icon to navigate to the incident and verify creation.

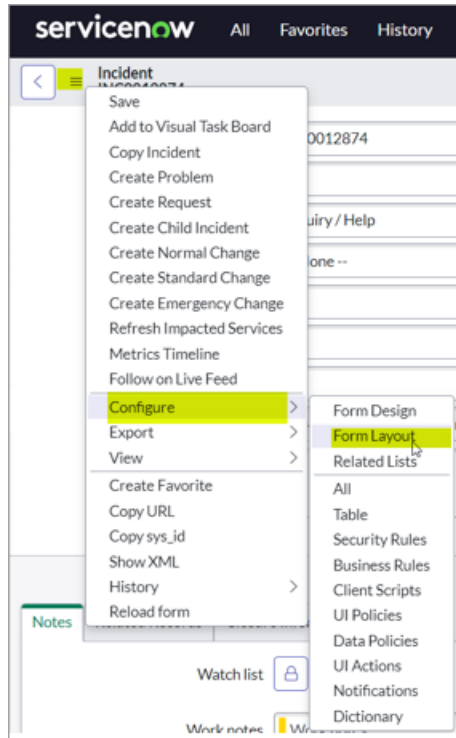
The screenshot shows the 'Incident' form in ServiceNow. The form is divided into two main sections: 'Job Details' and 'Incident'. The 'Job Details' section contains fields for Number (INC0012874), Channel (Phone), Caller, Category (Inquiry / Help), Subcategory, Business service, Service offering, Configuration item, Universal Request, Route reason, Short description (Backup failed. Please restart.), and Description. The 'Incident' section is currently empty, but the 'Incident' icon is highlighted in the Job Details section.

- Enable **Additional Fields** on the **Incident** screen. This is applicable only for APTARE issues. Skip this step for APTARE Data Protection.

By default, additional fields such as **Policy Name** and **Schedule Name** may not be enabled to be viewed on the **Incident** screen.

To enable these fields:

- Click the **Additional Actions** icon.
- Go to **Configure > Form Layout**.



- Find the **Policy Name** and **Schedule Name** fields from the list of fields under **Available** and move them to **Selected**.

The screenshot displays the ServiceNow Incident form for incident INC0010070. The form is in 'Portal view'. The 'Number' field is populated with 'INC0010070'. The 'Category' is 'Inquiry / Help'. The 'Subcategory' is 'None --'. The 'Business service' is 'Full'. The 'Service offering' is 'Full'. The 'Configuration item' is 'Full'. The 'Contact type' is 'Phone'. The 'State' is 'New'. The 'Backup Job ID' is '56398957'. The 'Catalog' is 'Full'. The 'Impact' is '3 - Low'. The 'Urgency' is '3 - Low'. The 'Priority' is '5 - Planning'. The 'Assignment group' is 'Full'. The 'Assigned to' is 'Full'. The 'Short description' is 'Backup failed. Please restart.' The 'Description' field is empty. The 'Policy Name' and 'Schedule Name' fields are highlighted in yellow, indicating they have been moved from the 'Available' list to the 'Selected' list.

- Click **Save**.
 The **Incident** screen must display the **Policy Name** and **Schedule Name** fields (as highlighted below) when you reopen the incident.

Test the IT Analytics ServiceNow App

You can perform a complete end-to-end test from your ServiceNow instance.

Objectives

This test confirms the following:

- IT Analytics is passing the Failed Backup jobs to ServiceNow.
- ServiceNow is opening incidents for the failed jobs passed to it by IT Analytics according to the ServiceNow Alert rules defined (if any) in the IT Analytics Portal.
- Any change made to the Incident State by changing the value of **State** from **New** to **Active**, the change is immediately propagated to IT Analytics.
- IT Analytics Data Protection dashboard displays backup data for Last Successful Backup by Server and Last Successful Full Backup by Server.

Prerequisites

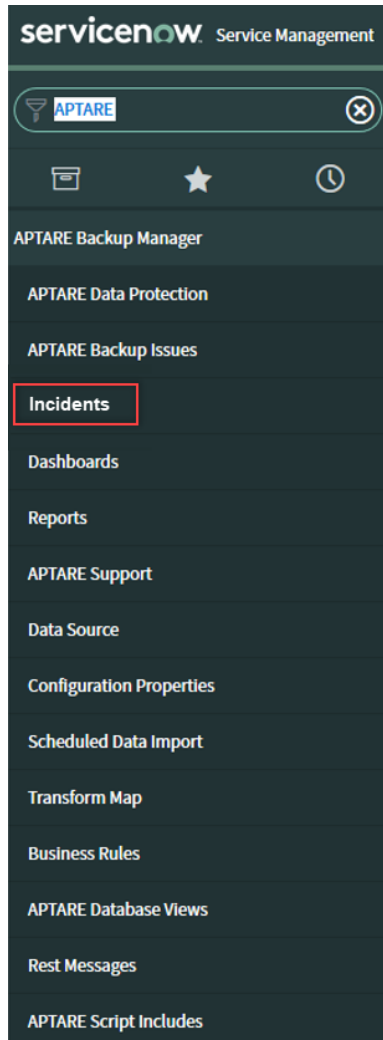
Verify the following before you proceed with the testing:

- IT Analytics Portal is installed, working, and accessible from a supported web browser.
- ServiceNow Job Finalized Alert is configured and enabled in the IT Analytics Portal. Alert can be configured with any rules according to your requirements.
- Backup Manager data collection is enabled in IT Analytics.
- IT Analytics user account is created to be used by the REST API from ServiceNow to IT Analytics Portal.
- IT Analytics ServiceNow App is downloaded and installed on your ServiceNow instance.
- If your ServiceNow instance does not have a MID server, create a new MID server. The MID server is used for communication between ServiceNow and IT Analytics Portal.
- New MID server user account is created, which is used to authenticate the MID server.
- The "Admin" role is granted to the new MID server user account.

Test the IT Analytics ServiceNow App

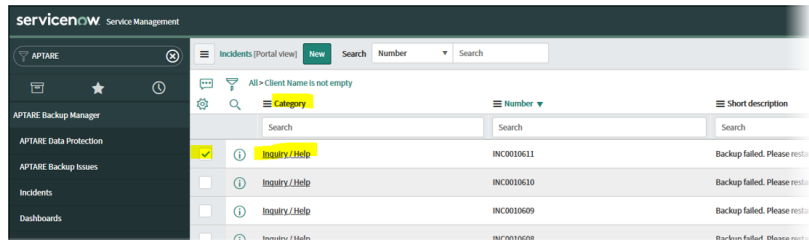
To test the IT Analytics ServiceNow App:

- 1 Login to your ServiceNow instance.
- 2 Search for the keyword **APTARE**.



- 3 Find and select **Incidents** and you can see the **Incidents** screen.

- 4 Select any incident from the list and click **Inquiry/Help** value displayed under the **Category** column.



This opens the **Incidents** screen that displays the incident details along with their current **State**, Backup Job ID, and some other information.

The screenshot shows the ServiceNow 'Incident' details view for INC0010611. The 'State' field is highlighted, and the 'Update' button is visible. The form contains various fields for incident details, including 'Number', 'Caller', 'Category', 'Subcategory', 'Business service', 'Service offering', 'Configuration item', 'Contact type', 'Phone', 'State', 'Backup Job ID', 'Policy Name', 'Schedule Name', 'Impact', 'Urgency', 'Priority', 'Assignment group', and 'Assigned to'. The 'Short description' field contains the text 'Backup failed. Please restart.'.

- 5 Change the value of **State** from **New** to **Active** by selecting an appropriate value from the drop down list.
- 6 Click **Update**.
- 7 Click **Inquiry/Help** under the **Category** field to reopen the incident.
- 8 Verify the new value **Active** in the **State** column.

- 9 In the **Backup Job ID** field, click **Review this Record**, which displays the **APTARE Backup Issues** screen, which contains the failed backup job details.

Backup Job ID: 56498990

APTARE Backup Issues Open Record

Client Name	[Redacted]	Server Name	[Redacted]
Policy Name	Catalog	Schedule Name	[Redacted]
Product Name	Veritas NetBackup	Vendor Status	Failed
Error Code	2	Configuration Item	[Redacted]
Client Name Aliases	[Redacted]	IP Addresses	[Redacted]

Error Message: None of the requested files were backed up. A backup or archive could not back up any of the files in the file list.

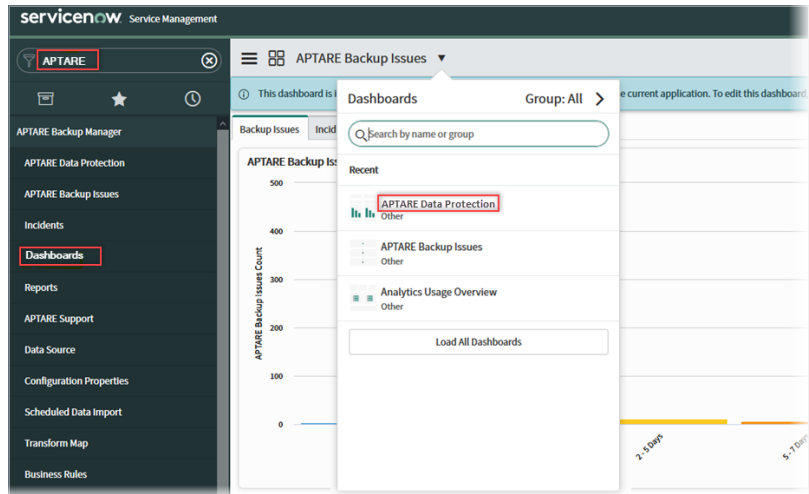
Notes: Backup failed. Please restart.

APTARE URL: https://mystage.storageconsole.com/portal/portal.login?drillDownId=jobId-56498990_productId-1

- 10 Click the **APTARE URL**. This should open the IT Analytics Portal.
- 11 Enter valid IT Analytics credentials and the portal must display the **Job Details** report. The ServiceNow **Incident Number** and its **State** are displayed under the **Notes** column on the report. You can enable notes using the menu invoked from the three vertical dots in the upper right corner.

2 Notes:		
Email	Date	Note
aptare	May 13, 2021 1:56:50 AM	ServiceNow Incident #: INC0010611 Incident State changed to: Active
aptare	May 12, 2021 7:52:09 AM	ServiceNow Incident #: INC0010611 Incident State: New

- 12 Select **Dashboards** and from **APTARE Backup Issues > Dashboards** list, select **APTARE Data Protection**.



- 13 Verify whether the dashboard displays **APTARE Last Successful backup by Server** and **APTARE Last Successful Full Backup by Server** data for your backup clients that are part of Backup Manager data collection.

Troubleshooting

This chapter includes the following topics:

- [About Troubleshooting](#)
- [Issue: Backup failures are not creating incidents in ServiceNow](#)
- [data protection does not display any record](#)
- [MID server registration with IT Analytics ServiceNow App fails](#)

About Troubleshooting

When troubleshooting the IT Analytics ServiceNow App, the first thing to determine is whether the issue is with the ServiceNow application or the IT Analytics Portal.

Issue: Backup failures are not creating incidents in ServiceNow

If backup failures are not creating incidents in ServiceNow, first check if those failures are being populated into the source table (`apt_job_ticket`) in the database.

- If the source table is not being populated, contact Cohesity Support to diagnose the problem.
- If job records are present, check if:
 - There were errors reported with connectivity/credentials for the MID Server.
 - The scheduled import is running.
 - The transform map had errors.

data protection does not display any record

If backup data protection does not show any records, confirm:

- user package is modified and compiled according to the above documentation.
- backup client host entry is present in the ServiceNow cmdb database. (Only the backup that has a matching entry in the ServiceNow cmdb are displayed with their last successful backups on the backup data protection ServiceNow screen.)
- ServiceNow cmdb has the entries for the backup client with the same name and IP address, and they exist in the backup manager.

MID server registration with IT Analytics ServiceNow App fails

If the MID server registration with IT Analytics ServiceNow App fails, refer to the logs from `/opt/midserver/agent/logs`.