COHESITY

Version 1.1
September 2019

One-Stop Alerts Management

Cohesity DataPlatform with ServiceNow Incident Management

Table of Contents

Figures

1 Introduction

Global data management goes beyond data protection features; seamless visibility into the data protection process is a key deliverable of a modern data protection solution. Cohesity DataPlatform supports integration with ServiceNow to enable seamless translation of alerts to incident tickets in ServiceNow's Incident Management and IT Service Management system. The result: streamlined and integrated global management.

ServiceNow states a benefit of Incident Management is the ability to restore normal service operations as quickly as possible while minimizing impact to business operations. Integrating with Incident Management ensures greater alert visibility and lowers friction in solving alerts. Enabling this integration requires a few configuration steps that are described in this paper.

1.1 Audience

This guide is targeted at ServiceNow and Cohesity DataPlatform operators and administrators for configuring more effective management of alerts from Cohesity DataPlatform. To reap the complete benefits of this guide, you must be familiar with the following domains:

- SMTP Server Settings
- The ServiceNow UI
- Cohesity DataPlatform

1.2 Supported Email Alert Scenarios

To facilitate the monitoring of data protection events, health, services, and alerts, Cohesity DataPlatform provides email alerts for several scenarios, including:

- Data protection events
- Threshold-based alerts
- State Change alerts
- Service Status alerts
- Hardware Alerts
- Software Alerts

For all alert scenarios that Cohesity DataPlatform supports, see Alerts Reference in the Cohesity DataPlatform online documentation.

1.3 Terminology

There are several terms that are important to understand as you learn about the integration with ServiceNow Incident Management. You can familiarize yourself with relevant Cohesity and ServiceNow terms here.

TERM	DEFINITION
Helios	Cohesity's SaaS-based secondary data and application management platform that enables comprehensive global monitoring and management of data, applications, and Clusters from a single interface.
Inbound Email Actions	A ServiceNow feature that enables you to define the actions an instance takes when receiving email.
Incident Ticket	An issue that can be logged, tracked and managed (marked as resolved) in ServiceNow Incident Management portal.
Alert	A notification by Cohesity DataPlatform that provides visibility to users in the event of data protection job failures, allowing a way to understand your infrastructure more effectively and respond to health events. Email alerts can be configured, as shown in this guide.

2 Integrate Cohesity DataPlatform and ServiceNow Incident Management

Whether from Helios or an individual instance of Cohesity DataPlatform (a cluster), alerts can be translated as tickets on ServiceNow's Incident Management portal.

Figure 1: ServiceNow Incident Management Integration with a Cohesity Helios

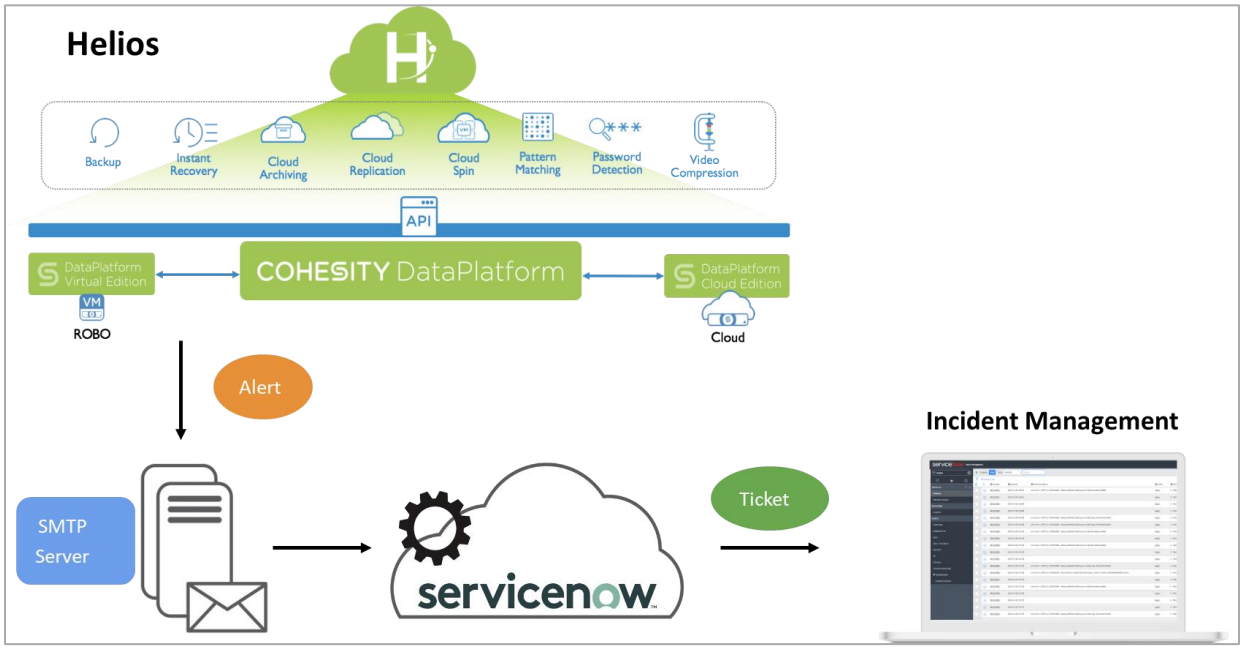
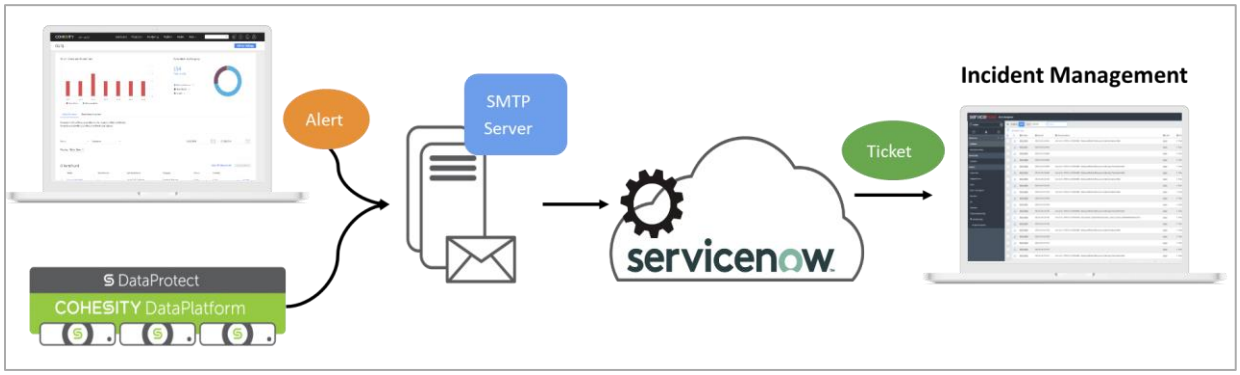


Figure 2: ServiceNow Incident Management Integration with a Cohesity DataPlatform Cluster



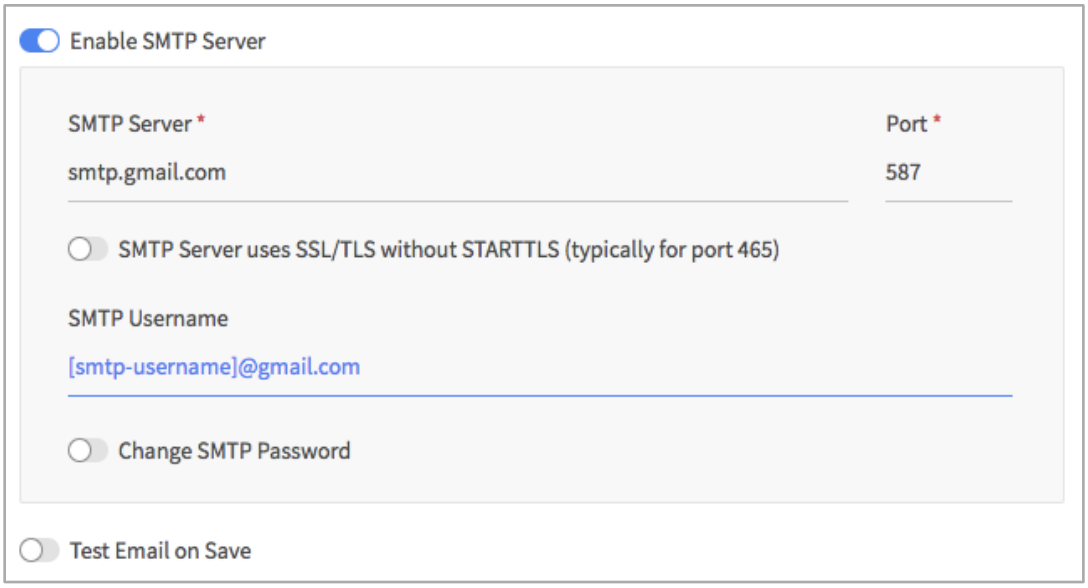
To integrate email-based alerts with ServiceNow's incident management portal:

- Configure SMTP for email on Cohesity DataPlatform.
- Set up a ServiceNow Instance as an Alert email recipient.
- Configure inbound actions on ServiceNow.

2.1 Configure SMTP for Email on Cohesity DataPlatform

1. Log in to Cohesity DataPlatform as admin.
2. Navigate to **Admin** > **Cluster Settings**.
3. Toggle **Enable SMTP Server**.
4. Contact your organization's IT department to understand recommended SMTP servers and server settings. In this paper, the Google SMTP service — and service settings — is used.

   Define the following:



   a. The **SMTP server**; in this paper, server smtp.gmail.com is used.
   b. The **SMTP server Port**; in this paper, Port 587 is used.
   c. The **SMTP Username**.
   d. The **SMTP Password**.

5. Enable **Test Email on Save** to verify inputted settings.
   a. Define the test recipient email.
6. Define the **System Admin Email Address**.
7. Choose **Save** to preserve changed SMTP settings under **Edit Cluster Settings**.

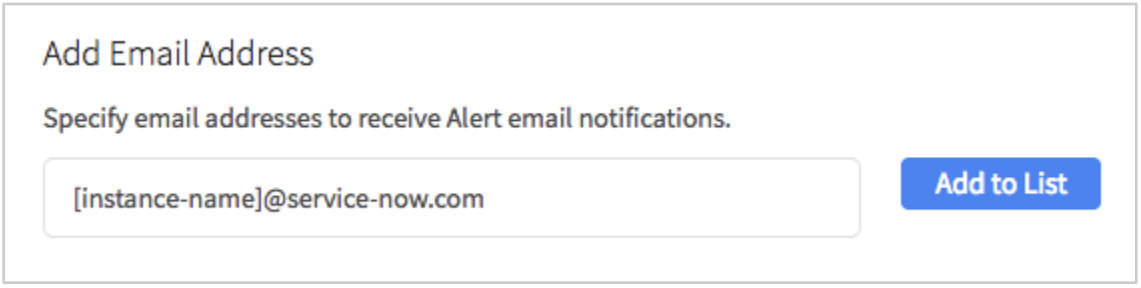
SMTP Security Troubleshooting

If unable to send emails, there may be a security or privilege issue on the SMTP server. Contact your IT administrator to verify full access to the SMTP server in use.

In case of Google's SMTP service, navigate to https://www.google.com/settings/security/lesssecureapps and enable **Turn on Access for Less Secure Apps**.

2.2 Set Up a ServiceNow Instance as an Alert Email Recipient

1. Log in to Cohesity DataPlatform and navigate to **Monitoring** > **Alerts**.
2. Under **Alert Settings**, specify the ServiceNow Instance as an email recipient.
   a. To send alerts to https://[**instance-name**].service-now.com/ use [**instance-name**]@service-now.com



   b. Click **Add to List**.

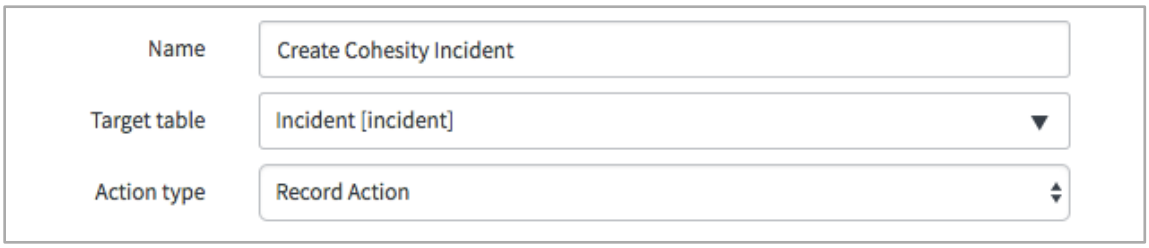
2.3 Configure Inbound Actions on ServiceNow

Now set up ServiceNow to receive alerts from Cohesity DataPlatform.

To configure Inbound Actions:

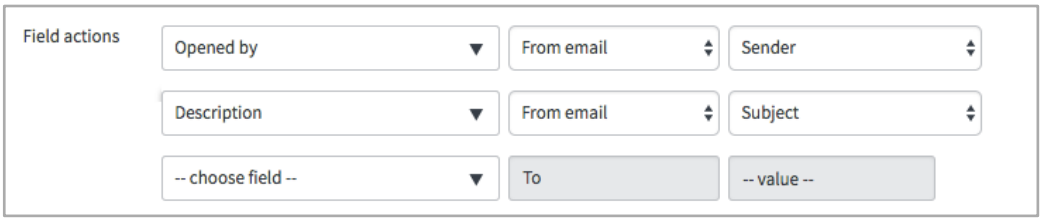
1. Navigate to your ServiceNow Instance via https://[**instance-name**].servicenow.com/.
2. Log in as **System Administrator** to your ServiceNow Instance.
3. On the left panel, navigate to **Inbound Actions** under **System Policy** > **Email**.

4. Choose **New** and enter the following information, naming the Inbound Action as desired:



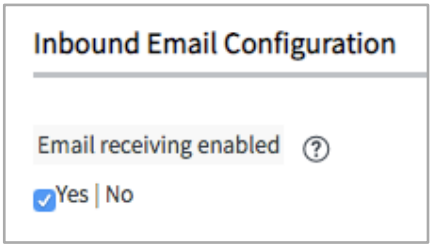
5. On the right-hand fields, verify **Application** is **Global** and **Active** is selected.

6. Under the **Inbound Actions** > **Actions tab**, select the following field actions, changing specific fields accordingly, to meet your environment needs:



These field actions allow the incident ticket parameters to be defined, including the priority of incoming email alerts, ticket assignees, and description of the incident ticket.

7. Under **System Properties** > **Email Properties**, select **Email receiving enabled**.



8. Under **System Properties** > **Email Properties**, define your organization's trusted domains, using the * character for all domains.

9. View Cohesity DataPlatform Alerts sent as emails on the ServiceNow Instance via **System Logs** > **Emails**, helping troubleshoot configuration or trusted domain challenges.
10. View Cohesity DataPlatform Alerts as Incident Tickets via **Service Desk** > **Incidents**.

NOTE: To learn more about configuring Inbound Actions, see the Inbound email actions ServiceNow article.

2.4 Example Workflow of Configured Incident Management System

Once your integration is complete, alerts begin appearing in your ServiceNow portal. For example, if a backup run in Cohesity DataPlatform fails:

1. Cohesity DataPlatform sends the *BackupJobFailed* email alert to ServiceNow Instance.
2. The email received by ServiceNow is then mapped as an incident.
3. The event on Cohesity DataPlatform is now manageable by Service Desk.

3 Use Webhooks to Configure Alerts Management

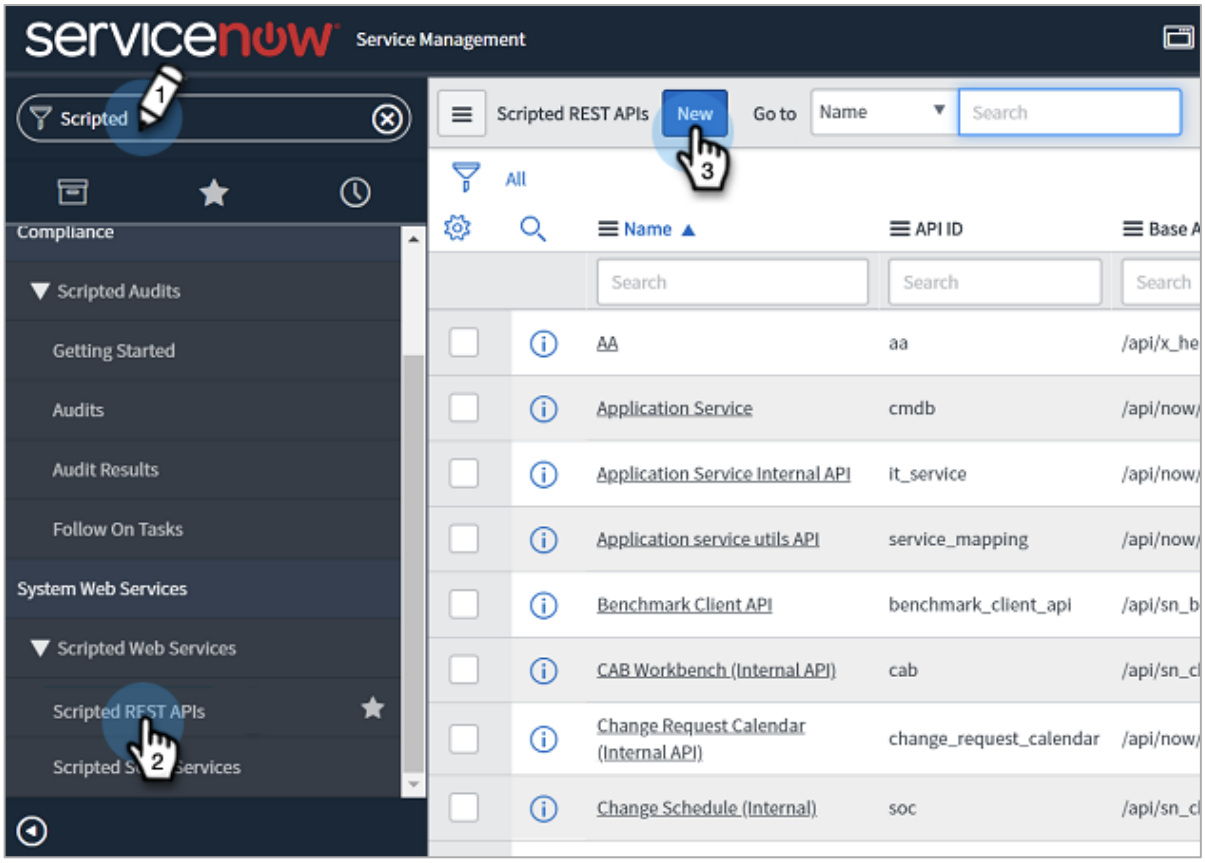
In addition to the existing integration of email-based alerts with ServiceNow, Cohesity has introduced a new method to enable the ServiceNow platform to receive alert notifications using Webhooks.

NOTE: This feature is supported on Cohesity clusters running version 6.2 and later.

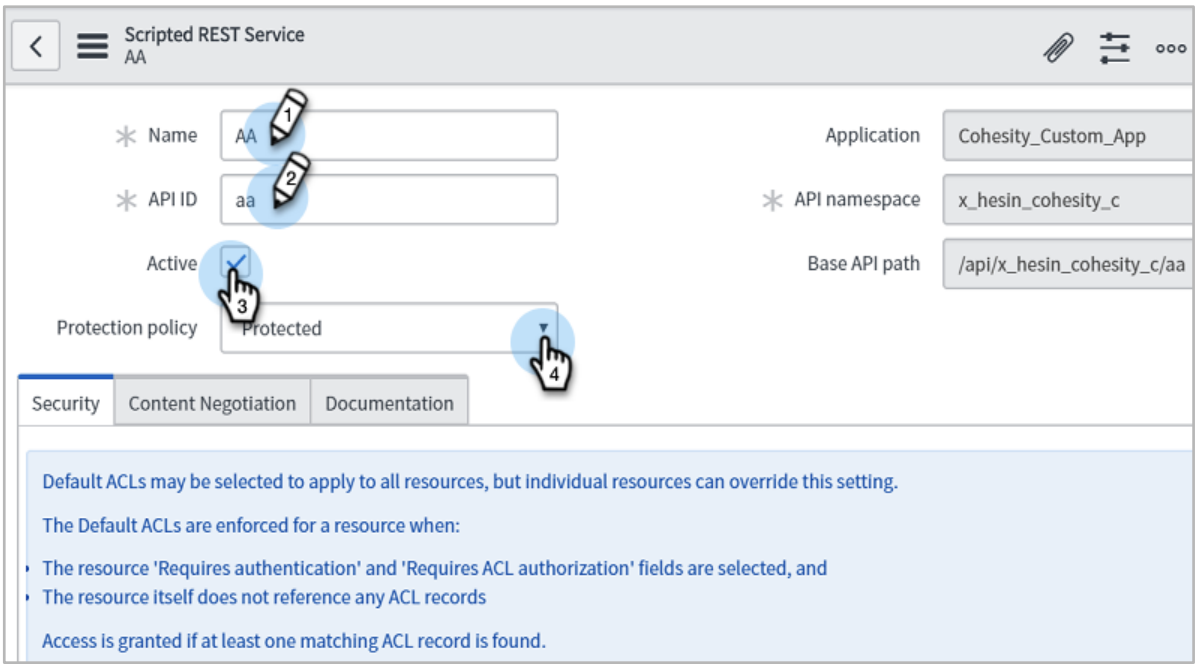
3.1 Create a REST API on ServiceNow

The first task is to create a new REST API that will enable Cohesity DataPlatform to send alerts to ServiceNow.

1. Log in to ServiceNow.
2. In the Search box, search for “Scripted REST APIs” and then, under **System Web Services**, click **Scripted REST APIs** and then **New**.

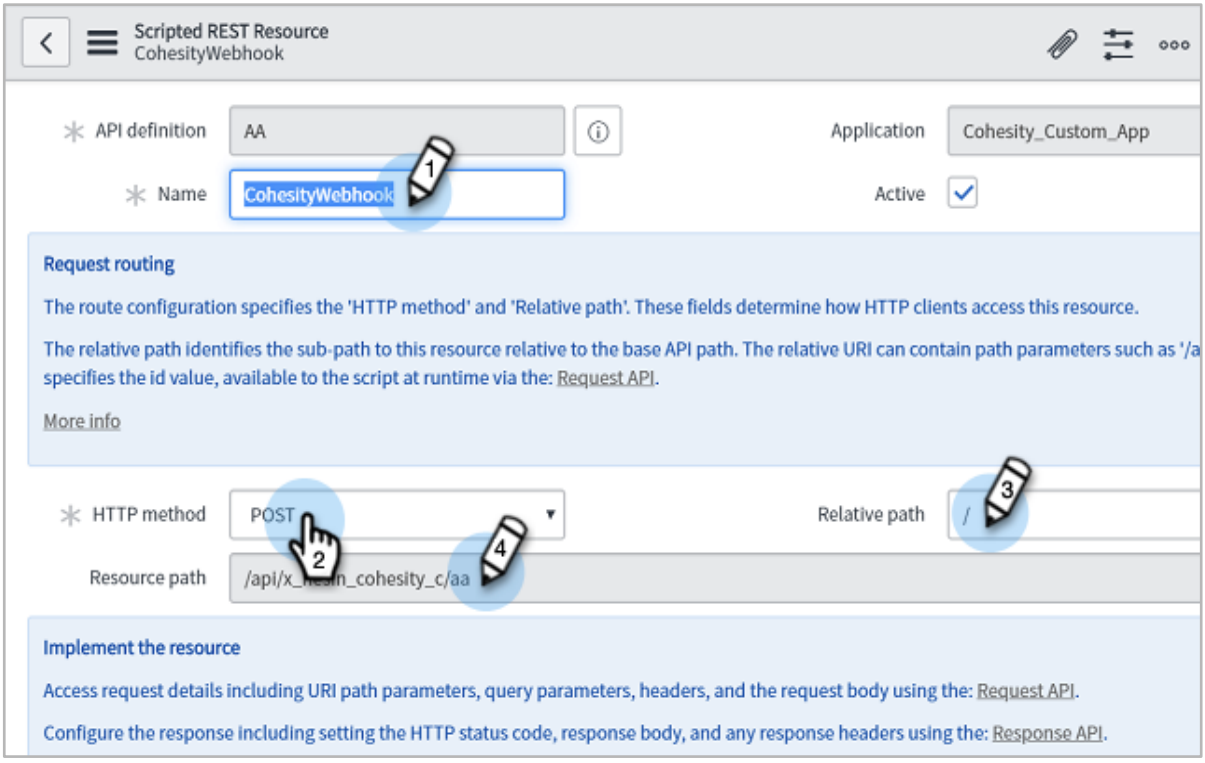


3. Enter the **Name**, **API ID**, select **Active**, and choose a **Protection policy**.



4. Scroll down and click **New**.

5. Enter the **Resource Name**, select **POST** as the **HTTP Method**, and provide the **Relative path** and the **Resource path**.



6. Scroll down to enter the script that enables ServiceNow to receive notifications from Cohesity Alerts Management. You can base your script on this sample but remember to make it specific to your environment.

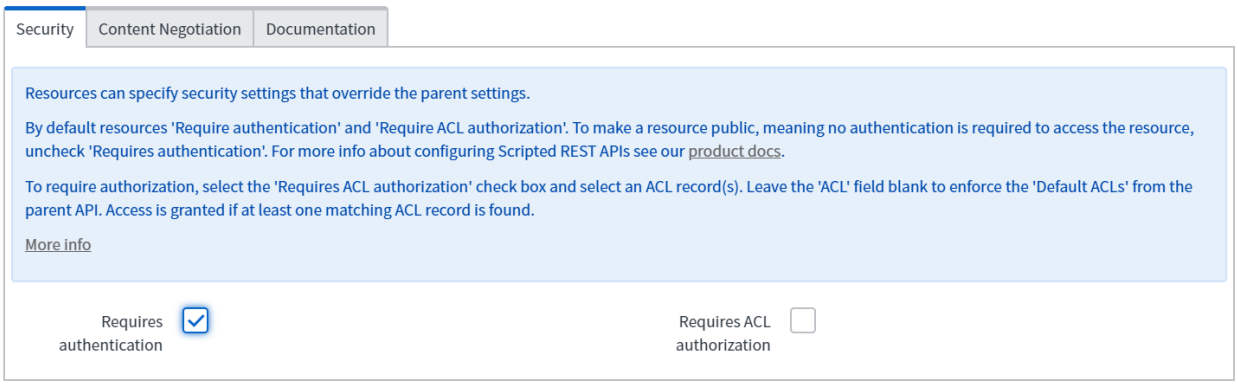
```
(function process(/*RESTAPIRequest*/ request, /*RESTAPIResponse*/ response) {
// implement resource here
//gs.info("Alert : " + request.body.dataString);

var parser = new global.JSON();
var alertRequest = parser.decode(request.body.dataString);
var priority = ['kCritical', 'kWarning', 'kInfo'];

//Alert info
var description = alertRequest.alertDescription;
var helpText = alertRequest.alertHelpText;
var alertUrl = alertRequest.alertUrl;
var reason = alertRequest.alertProperties.reason_string;
var nodeIp =  alertRequest.alertProperties.node_ip;
var descriptionString = description + '. ' + helpText + '\nAlert URL : ' +
alertUrl + '\nReason : ' + reason + '\nNode IP : ' + nodeIp;

var incidentDB = new GlideRecordSecure('incident');
incidentDB.initialize();
incidentDB.short_description = alertRequest.alertName;
incidentDB.description = descriptionString;
incidentDB.impact = 1;
incidentDB.urgency = Math.round(priority.indexOf(alertRequest.alertSeverity) + 1);
incidentDB.state = 3;
incidentDB.insert();
})(request, response);
```

7. To require authentication for the connection to ServiceNow, configure the settings under **Security**.



8. Click **Submit**.

NOTE: For more, see How to Integrate Webhooks Into ServiceNow.

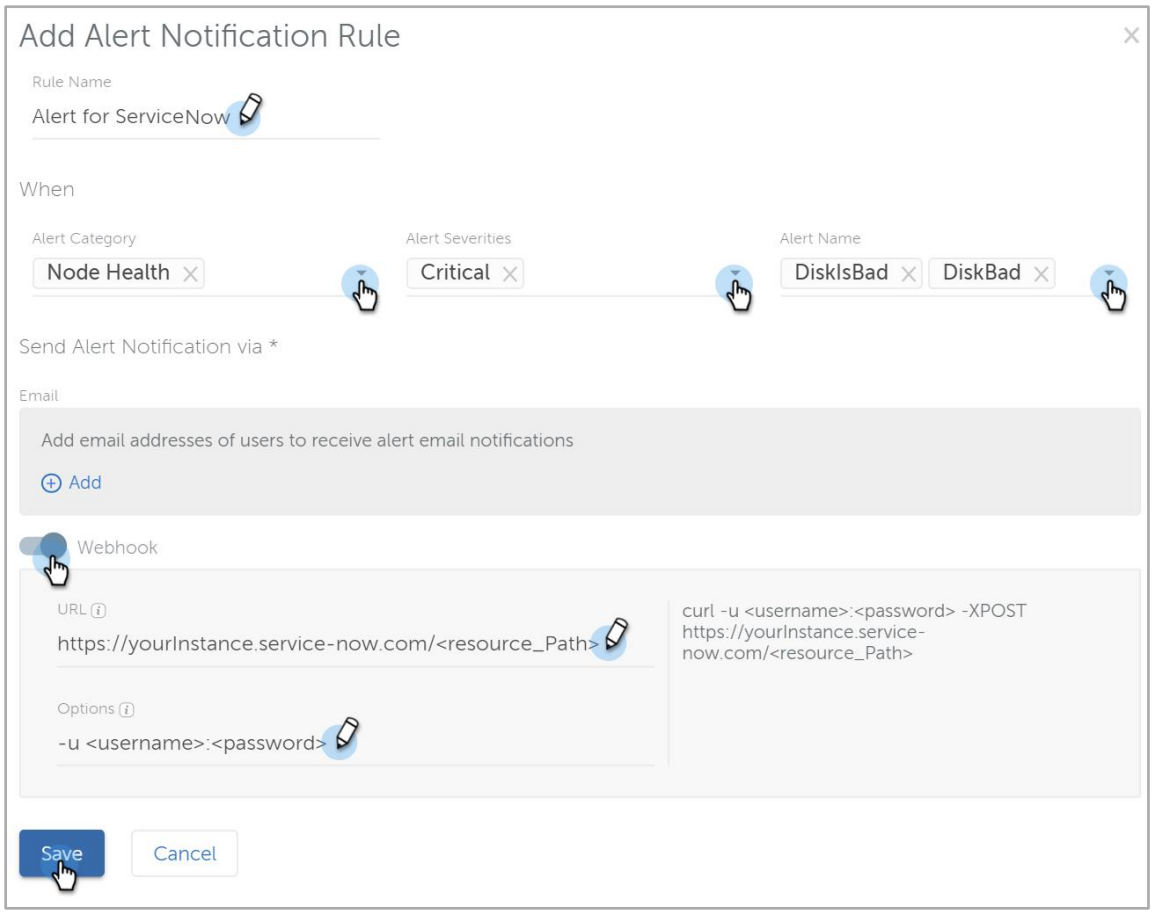
3.2 Connect Cohesity DataPlatform to ServiceNow

Now that you have created the ServiceNow REST API, you can use it to add an Alert Notification Rule to Cohesity DataPlatform.

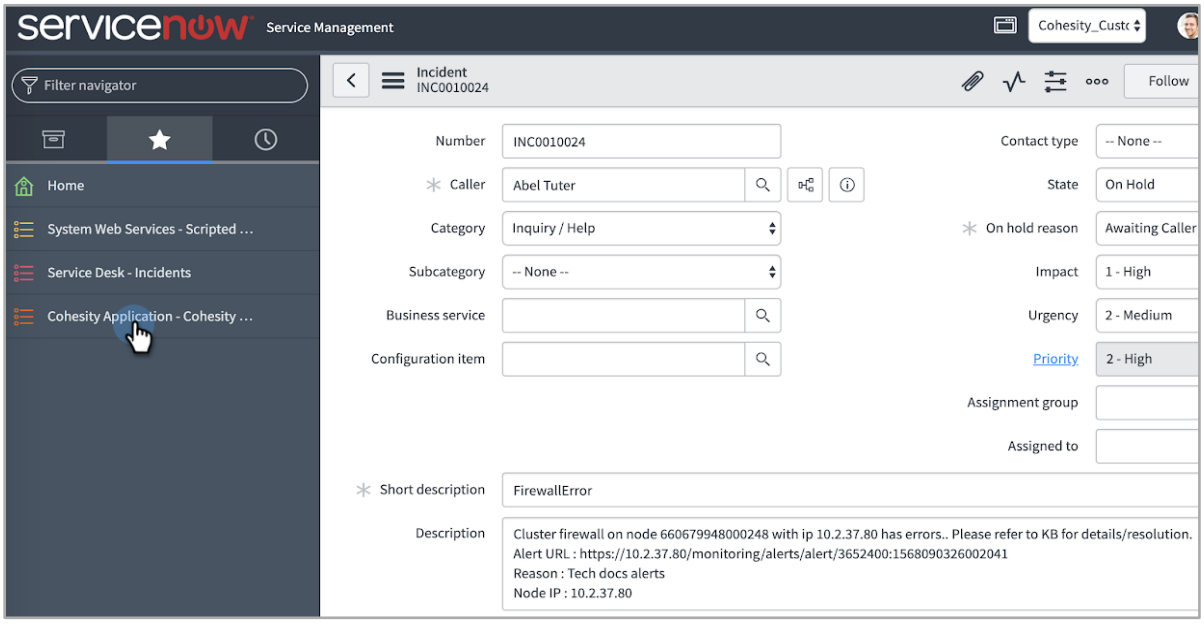
1. Log in to Cohesity DataPlatform as admin.
2. Navigate to **System** > **Alerts** and click the **Settings** tab.
3. Click **Add Alert Notification Rule**.
4. Enter the following details:
   a. Provide a **Rule Name**.
   b. Add an **Alert Category**, **Alert Severities**, and **Alert Name**.
   c. Toggle on **Webhook** under **Send Alert Notification via**.
   d. Enter the **ServiceNow URL** along with the **Resource Path** that allows Cohesity DataPlatform to establish a connection with ServiceNow. For example:

```
curl -u <username>:<password> -XPOST https://yourInstance.service-now.com/<resource_Path>
```

e. Finally, click **Save**.



Now, whenever an alert is generated by Cohesity DataPlatform, the incident is created in ServiceNow.



4 Cohesity DataPlatform and ServiceNow

Integrating ServiceNow with Cohesity DataPlatform advances agility, speed, and self-service. For more, see Automate and Integrate with APIs on our website.

5 About the Author

Srini Sekaran is a Technical Marketing Engineer at Cohesity. In his role, Srini focuses on virtualization and integrations with several solutions, understanding user needs and technical requirements.

6 Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.0	Feb 2019	Original Document
1.1	Sept 2019	Added Webhooks

7 Your Feedback

Was this document helpful? Send us your feedback!

ABOUT COHESITY

Cohesity makes your data work for you by consolidating secondary storage silos onto a hyperconverged, web-scale data platform that spans both private and public clouds. Enterprise customers begin by radically streamlining their backup and data protection, then converge file and object services, test/dev instances, and analytic functions to provide a global data store. Cohesity counts many Global 1000 companies and federal agencies among its rapidly growing customer base and was named to Forbes' "Next Billion-Dollar Startups 2017," LinkedIn's "Startups: The 50 Industry Disruptors You Need to Know Now," and CRN's "2017 Emerging Vendors in Storage" lists.

For more information, visit our website and blog, follow us on Twitter and LinkedIn and like us on Facebook.