

COHESITY

Version 1.1  
September 2019

# One-Stop Alerts Management

*Cohesity DataPlatform with ServiceNow  
Incident Management*



# Table of Contents

- 1 Introduction.....3
  - 1.1 Audience..... 3
  - 1.2 Supported Email Alert Scenarios..... 3
  - 1.3 Terminology..... 4
- 2 Integrate Cohesity DataPlatform and ServiceNow Incident Management .....5
  - 2.1 Configure SMTP for Email on Cohesity DataPlatform..... 6
  - 2.2 Set Up a ServiceNow Instance as an Alert Email Recipient..... 7
  - 2.3 Configure Inbound Actions on ServiceNow..... 7
  - 2.4 Example Workflow of Configured Incident Management System..... 9
- 3 Use Webhooks to Configure Alerts Management ..... 10
  - 3.1 Create a REST API on ServiceNow ..... 10
  - 3.2 Connect Cohesity DataPlatform to ServiceNow..... 13
- 4 Cohesity DataPlatform and ServiceNow ..... 15
- 5 About the Author ..... 16
- 6 Document Version History ..... 16
- 7 Your Feedback ..... 16

## Figures

- Figure 1: ServiceNow Incident Management Integration with a Cohesity Helios.....5
- Figure 2: ServiceNow Incident Management Integration with a Cohesity DataPlatform Cluster .....5

# 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
<b>Helios</b>	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.
<b>Inbound Email Actions</b>	A ServiceNow feature that enables you to define the actions an instance takes when receiving email.
<b>Incident Ticket</b>	An issue that can be logged, tracked and managed (marked as resolved) in ServiceNow Incident Management portal.
<b>Alert</b>	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

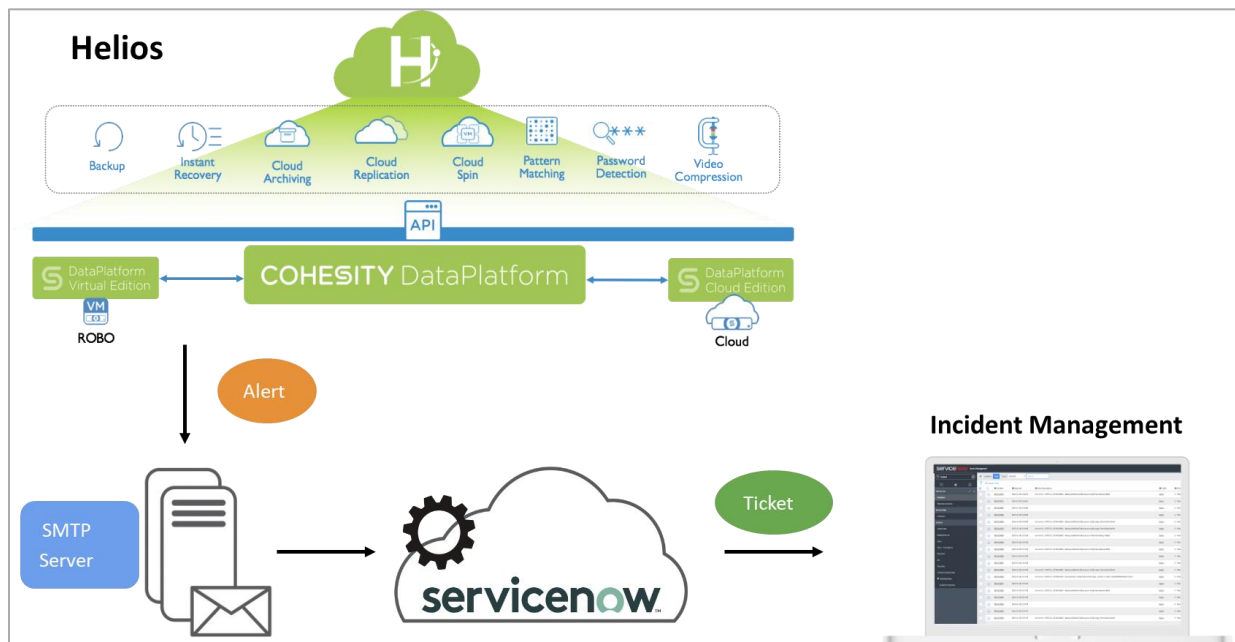
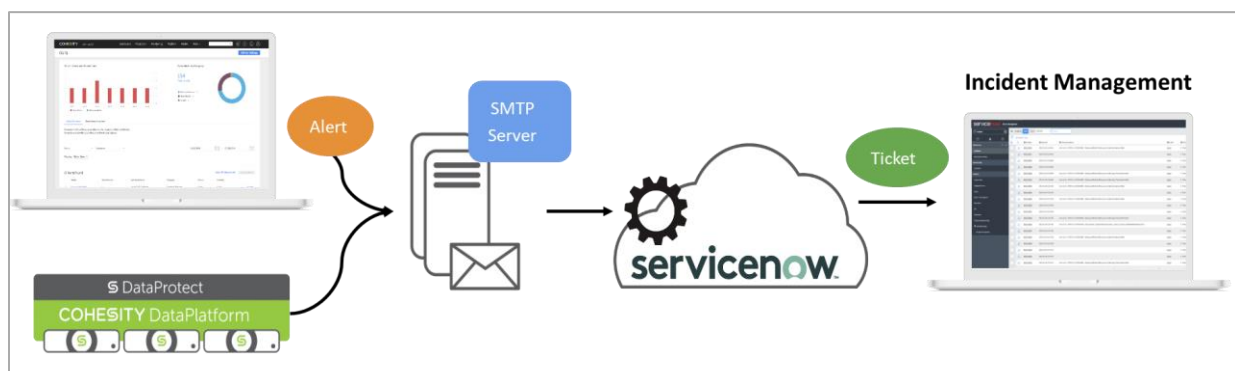


Figure 2: ServiceNow Incident Management Integration with a Cohesity DataPlatform Cluster



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:

Enable SMTP Server

SMTP Server *	Port *
smtp.gmail.com	587

SMTP Server uses SSL/TLS without STARTTLS (typically for port 465)

SMTP Username

[smtp-username]@gmail.com

Change SMTP Password

Test Email on Save

- 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**.

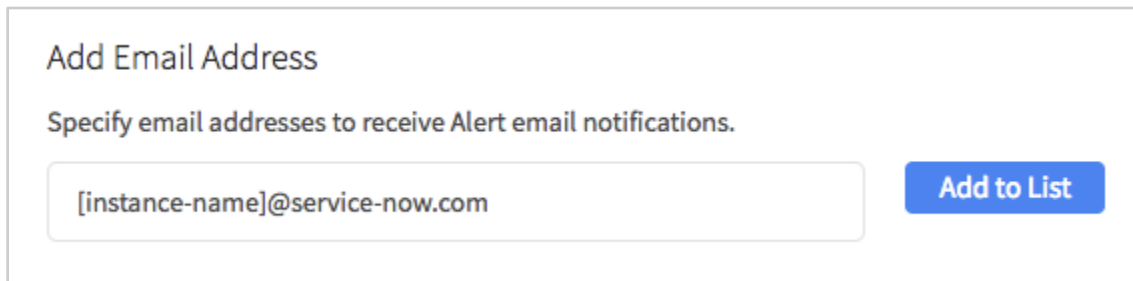
### SMTP Security Troubleshooting

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/](https://[instance-name].service-now.com/) use [\[instance-name\]@service-now.com](mailto:[instance-name]@service-now.com)



Add Email Address

Specify email addresses to receive Alert email notifications.

Add to List

- 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/](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**.

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

Name	<input type="text" value="Create Cohesity Incident"/>
Target table	<input type="text" value="Incident [incident]"/>
Action type	<input type="text" value="Record Action"/>

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

Application	<input type="text" value="Global"/>	<input type="button" value="i"/>
Active	<input checked="" type="checkbox"/>	
Stop processing	<input type="checkbox"/>	

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

Field actions	<input type="text" value="Opened by"/>	<input type="text" value="From email"/>	<input type="text" value="Sender"/>
	<input type="text" value="Description"/>	<input type="text" value="From email"/>	<input type="text" value="Subject"/>
	<input type="text" value="-- choose field --"/>	<input type="text" value="To"/>	<input type="text" value="-- value --"/>

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.

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

### Inbound Email Configuration

Email receiving enabled  ?

Yes | No

- Under **System Properties > Email Properties**, define your organization’s trusted domains, using the \* character for all domains.

Trust  domains when creating new users from incoming email (Ignore email from untrusted domains unless from an existing user; use \* 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

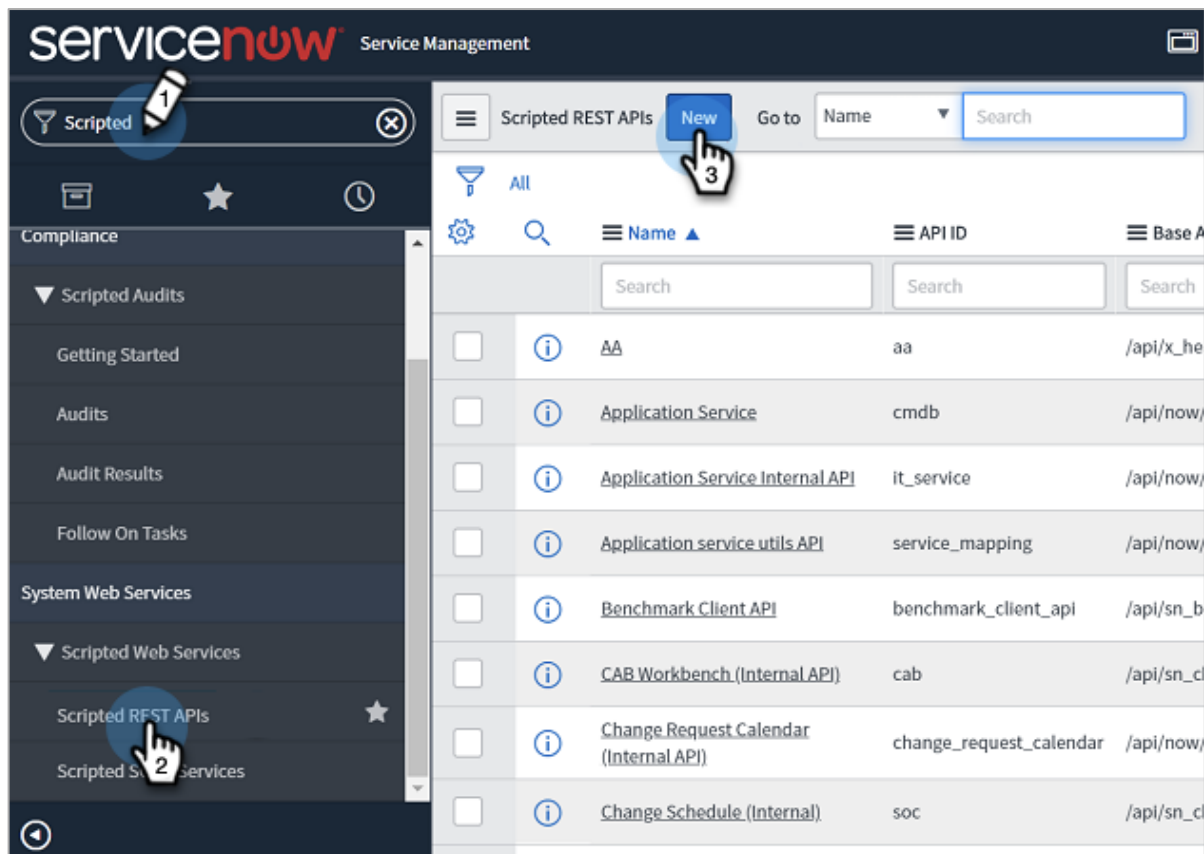
In addition to the existing integration of email-based alerts with ServiceNow, Cohesity has introduced a new method to enable the ServiceNow platform to receive alert notifications using Webhooks.

**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**.

Scripted REST Service  
AA

\* Name AA  
\* API ID aa  
Active   
Protection policy Protected

Application Cohesity\_Custom\_App  
\* API namespace x\_hesin\_cohesity\_c  
Base API path /api/x\_hesin\_cohesity\_c/aa

Security Content Negotiation Documentation

Default ACLs may be selected to apply to all resources, but individual resources can override this setting.

The Default ACLs are enforced for a resource when:

- The resource 'Requires authentication' and 'Requires ACL authorization' fields are selected, and
- The resource itself does not reference any ACL records

Access is granted if at least one matching ACL record is found.

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**.

Scripted REST Resource  
CohesityWebhook

\* API definition AA  
\* Name CohesityWebhook  
Application Cohesity\_Custom\_App  
Active

**Request routing**  
The route configuration specifies the 'HTTP method' and 'Relative path'. These fields determine how HTTP clients access this resource.  
The relative path identifies the sub-path to this resource relative to the base API path. The relative URI can contain path parameters such as '/a' specifies the id value, available to the script at runtime via the: [Request API](#).

[More info](#)

\* HTTP method POST  
Relative path /  
Resource path /api/x\_hesin\_cohesity\_c/aa

**Implement the resource**  
Access request details including URI path parameters, query parameters, headers, and the request body using the: [Request API](#).  
Configure the response including setting the HTTP status code, response body, and any response headers using the: [Response API](#).

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**.

Security
Content Negotiation
Documentation

Resources can specify security settings that override the parent settings.

By default resources 'Require authentication' and 'Require ACL authorization'. To make a resource public, meaning no authentication is required to access the resource, uncheck 'Requires authentication'. For more info about configuring Scripted REST APIs see our [product docs](#).

To require authorization, select the 'Requires ACL authorization' check box and select an ACL record(s). Leave the 'ACL' field blank to enforce the 'Default ACLs' from the parent API. Access is granted if at least one matching ACL record is found.

[More info](#)

Requires authentication

Requires ACL authorization

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**.

### Add Alert Notification Rule ✕

Rule Name  
Alert for ServiceNow

When

Alert Category: Node Health ✕

Alert Severities: Critical ✕

Alert Name: DiskBad ✕ DiskBad ✕

Send Alert Notification via \*

Email

Add email addresses of users to receive alert email notifications

[+ Add](#)

Webhook

URL   
[https://yourInstance.service-now.com/<resource\\_Path>](https://yourInstance.service-now.com/<resource_Path>)

Options   
 -u <username>:<password>

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

Save Cancel

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

The screenshot shows the ServiceNow interface for an incident. The left sidebar contains a filter navigator and a menu with items like 'Home', 'System Web Services - Scripted ...', 'Service Desk - Incidents', and 'Cohesity Application - Cohesity ...'. The main area displays the incident details for 'INC0010024'.

Number	INC0010024	Contact type	-- None --
* Caller	Abel Tuter	State	On Hold
Category	Inquiry / Help	* On hold reason	Awaiting Caller
Subcategory	-- None --	Impact	1 - High
Business service		Urgency	2 - Medium
Configuration item		Priority	2 - High
* Short description	FirewallError	Assignment group	
Description	Cluster firewall on node 660679948000248 with ip 10.2.37.80 has errors.. Please refer to KB for details/resolution. Alert URL : https://10.2.37.80/monitoring/alerts/alert/3652400:1568090326002041 Reason : Tech docs alerts Node IP : 10.2.37.80		

## 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](#).

© 2019. Cohesity, Inc.

*Cohesity, the Cohesity logo, SnapFS, SnapTree, SpanFS, and SpanOS, are registered trademarks, and DataPlatform, DataProtect, and Helios are trademarks of Cohesity, Inc. All rights reserved.*