COHESITY

Integrate IBM QRadar With Cohesity Data Cloud

Enhance visibility, investigation, and rapid response to all Cohesity cluster health and security alerts

Version 1.1

August 2025

ABSTRACT

The Cohesity Data Cloud provides cyber resilience with modern data security and management capabilities. Integrating it with a cloud-native SIEM/SOAR solution further enhances an organization's security operations by providing comprehensive visibility, automated incident response, and improved threat detection, resulting in a more robust and efficient security posture.

This guide explains how to integrate the IBM QRadar SIEM platform with Cohesity Data Cloud to enhance security visibility, investigate and respond rapidly to Cohesity cluster health and security alerts, and protect customer-critical data.

Table of Contents

List of Figures

Introduction

Ransomware attacks have increased exponentially, causing billions in losses, putting lives at risk, and damaging trust and reputations worldwide. As cybercriminals get more inventive, they're locking up production systems, destroying backups, and stealing sensitive data, leaving your enterprise with no option but to pay a ransom. Deploying a SIEM (Security Information and Event Management) system enhances the organization's security posture, streamlines compliance, and manages risks more effectively.

Defense in depth is the key to minimizing risk. An organization must have a backup system that reliably and securely makes continuous or frequent backups. The system must protect the organization from various attacks and immediately and safely put the data online at scale to support forensics and cyber recovery. Cohesity provides unique capabilities in these areas.

First, Cohesity gathers rich telemetry collected during backup and applies multiple machine-learning models and algorithms to identify anomalies in the backup data. If your other tools have failed to detect and block the attackers, this can be your first warning of trouble. For more information, refer to the Accelerate Anomaly Detection whitepaper.

Second, Cohesity takes a team sport approach to security, incorporating technologies from leading security vendors to help identify vulnerabilities in backed-up workloads and detect anomalous behavior and IOCs (Indicators of compromises). Cohesity also applies leading ML-driven classification technology that leverages Natural Language Processing (NLP) methods to automatically discover and classify large data sets by sensitivity at scale to help rapidly assess the impact of a ransomware attack.

By integrating with the IBM QRadar SIEM platform, Cohesity enhances your organization's ability to react quickly and coordinate. This solution tears down the silos between your IT and security operations teams to provide faster time for discovery, investigation, and recovery from ransomware attacks. The coupling of the Cohesity data security and management platform with IBM QRadar SIEM detects and aggregates anomaly events, delivering intelligent backup data security analytics to your enterprise. Integrating with QRadar SIEM centralizes various alerts—whether for maintenance, security, or compliance—into a single location, where they can be correlated with events from other log sources to support informed decision-making.

The integrated solution brings data-driven insights from your ITOps and SecOps organizations together, boosting the teamwork required to most effectively assess an attack's scope and quickly remediate the threat.

Cohesity and IBM QRadar Integration

Integrating the Cohesity Data Cloud with IBM QRadar gives organizations greater visibility into sensitive data and threats in your secondary data, faster threat detection, and comprehensive compliance support, essential in today's complex cybersecurity landscape.

Benefits

IBM QRadar collects, processes, aggregates, and stores data from various sources in real-time. It uses that data to manage network and data security by providing real-time information, monitoring, alerts, offenses, and responses to threats.

Here are some of the key benefits of integrating the Cohesity Data Cloud with IBM QRadar:

1. **Enhanced threat correlation:** Gain visibility into anomalous activities in your Cohesity backups—in all your self-managed clusters, whether on-premises or in the cloud and Cohesity-managed clusters. Consolidate threat data, including unusual backup patterns, indicators of compromise (IOCs), and the presence and movement of sensitive data into IBM QRadar SIEM to correlate events better and accelerate time-to-insights.
2. **Real-time monitoring of alerts**: Enables real-time analysis of alerts from Cohesity—from customer-managed clusters, whether on-premises or in the cloud, and Cohesity-managed Software as a Service (SaaS)—and other log sources in a single location. This allows security teams to better correlate hardware, software, data service, and maintenance alerts from Cohesity.
   Refer to the Alert Reference page on the Cohesity docs to get all the alerts that Cohesity can send to the QRadar SIEM.
3. **Ransomware detection**: Visibility across endpoints, application servers (on-premises and cloud), Cohesity clusters (on-premise or in the cloud), and network devices (firewalls) enables QRadar SIEM to detect ransomware behavior patterns across IT infrastructure and take proactive measures to mitigate the impact.
4. **Compliance**: Cohesity Data Cloud provides users with enhanced visibility into the sensitive data contained in their backups. By sending alerts about sensitive data to IBM QRadar SIEM and running SIEM log data through a compliance extension, customers can effectively manage complex compliance requirements, such as GDPR for EU member states.
5. **Streamlined IT and security collaboration** - The rapid transfer of data from Cohesity to IBM QRadar accelerates handoffs between your IT backup team and Security Operation Center (SOC) while giving both teams simultaneous access to alerts for faster threat detection.

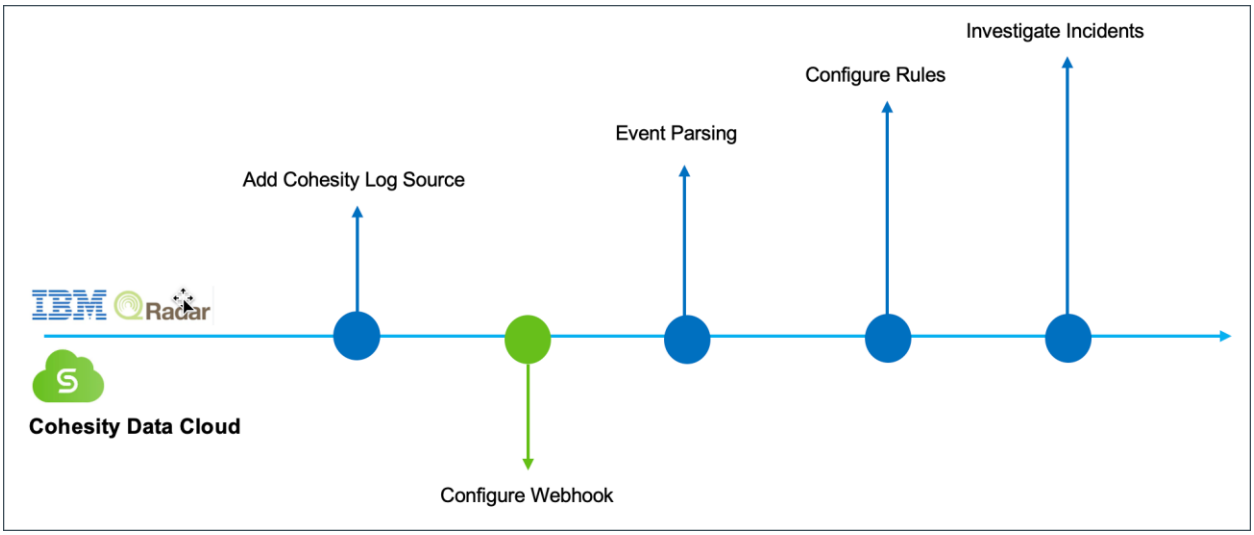
Components and Prerequisites

Components	Prerequisites
Cohesity Cluster (Self-Managed or Managed in Helios)	LTS version 6.8.1
IBM QRadar version	7.5 UP10
Security Alerts	Cluster claimed to Helios
Threat Detection Alerts	DataHawk ThreatProtection SKU
Data Classification Alerts	DataHawk DataClassification SKU

Solution Workflow

The Cohesity Data Cloud integration with IBM QRadar is a two-step process.

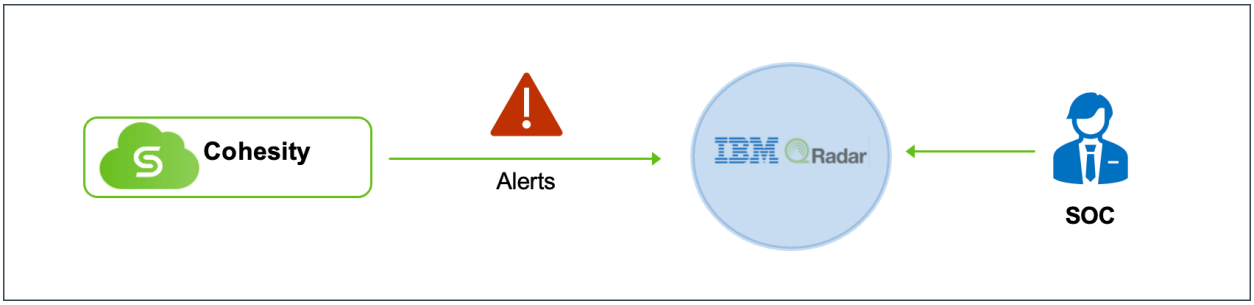
Figure 1: Configuration workflow



First, the Cohesity Data Cloud cluster is configured as a Log Source in QRadar to enable alert reception. Since QRadar doesn't automatically detect the Cohesity log source, it is added manually using the HTTP Receiver protocol. More details will be provided in the coming sections.

Next, a webhook is configured on the Cohesity Data Cloud to send alert notifications to IBM QRadar. This ensures the alert notifications are sent instantly when an event occurs, enabling real-time updates without the need for constant polling.

Figure 2: Solution Overview

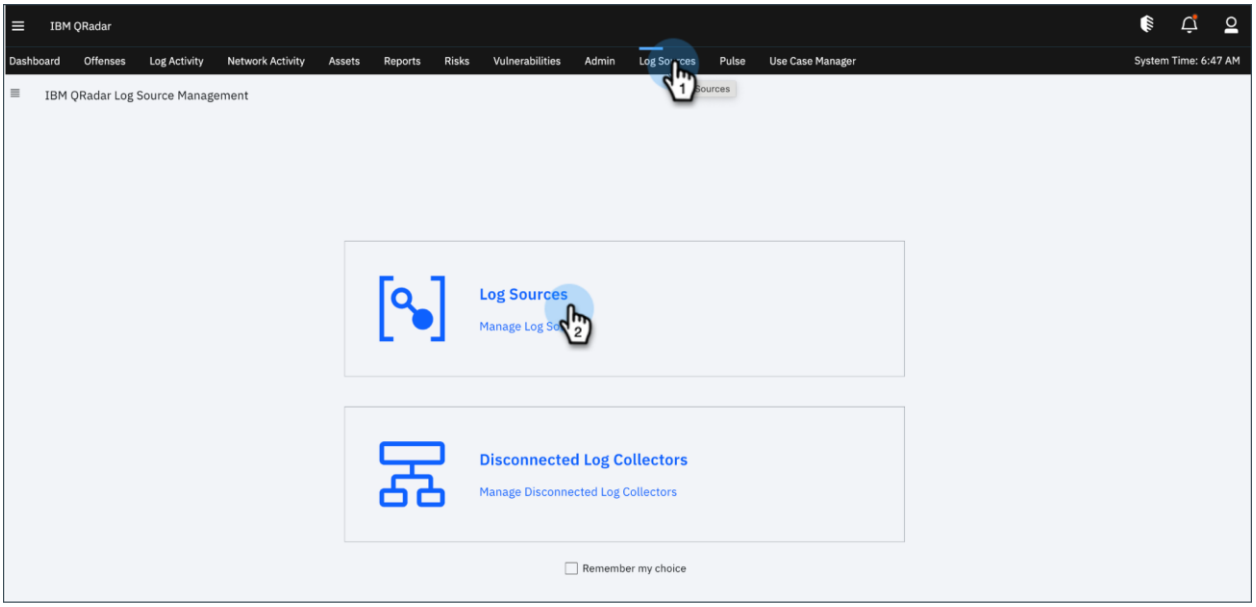


Configure Cohesity Log Source on IBM QRadar

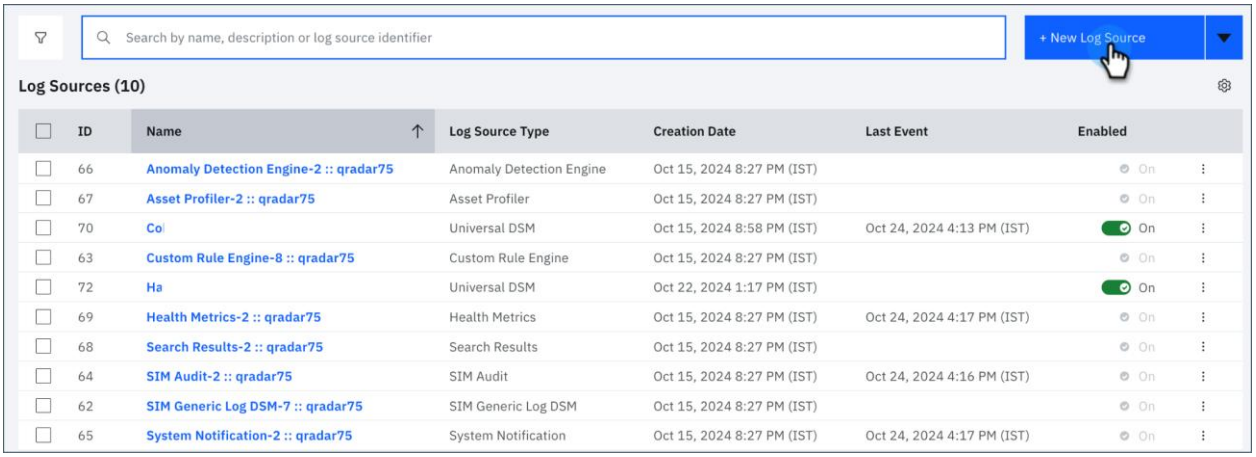
To receive alert notifications from the Cohesity source, a log source must be created on IBM QRadar.

Follow the steps below to add Cohesity Data Cloud Log source

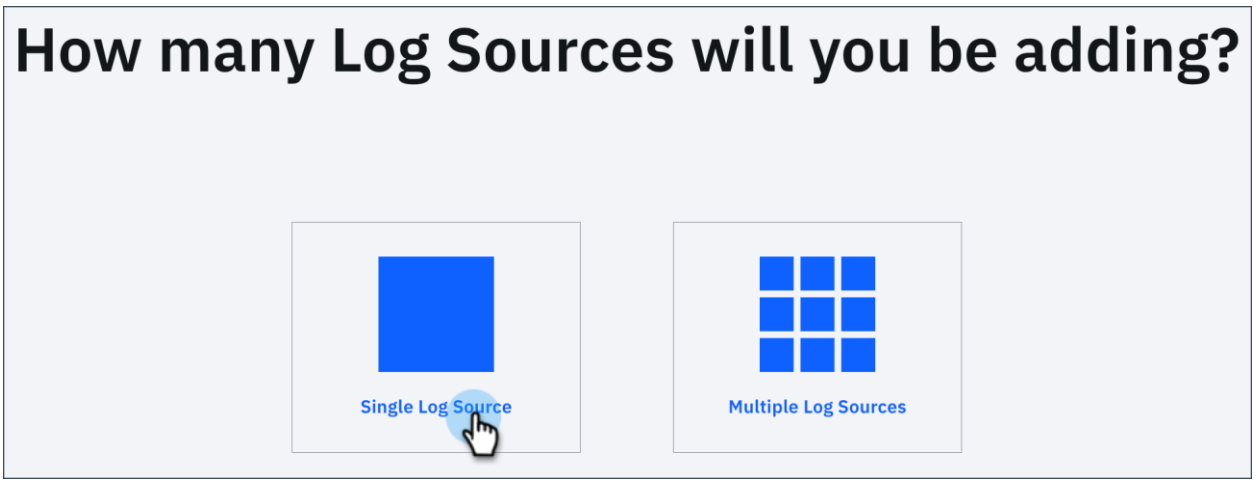
1. Log on to **QRadar**.
2. Click the **Admin** tab.
3. Click on **Log Sources** in the taskbar and select the **Log Sources** icon.



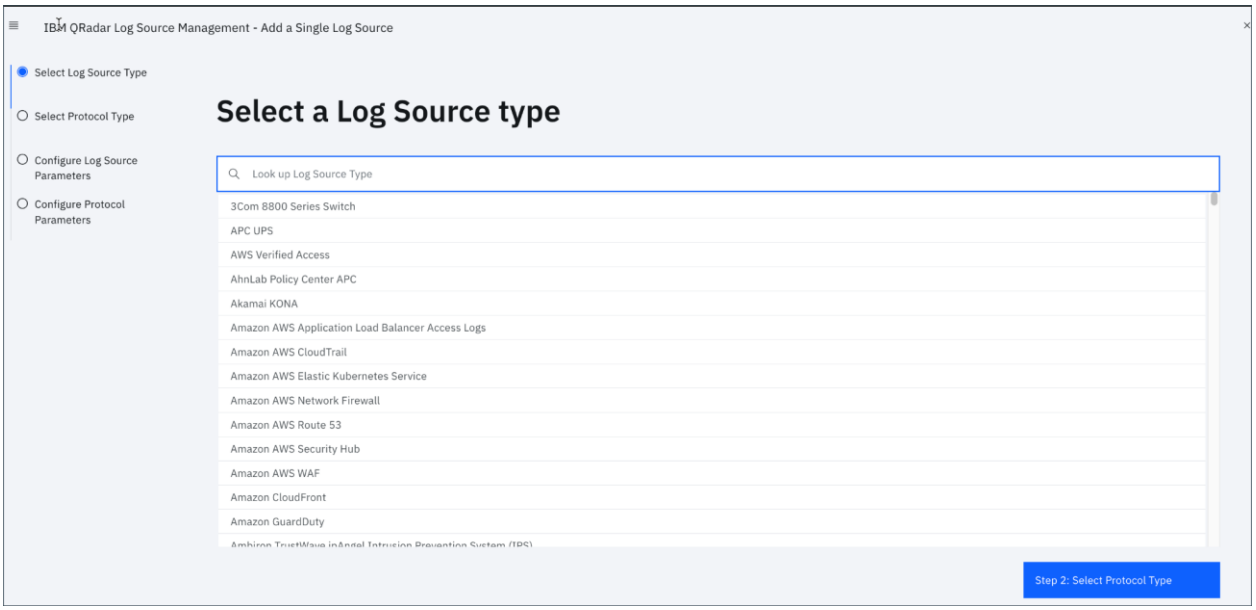
4. In the Log Sources screen, click on **+ New Log Source** to add a new log source.

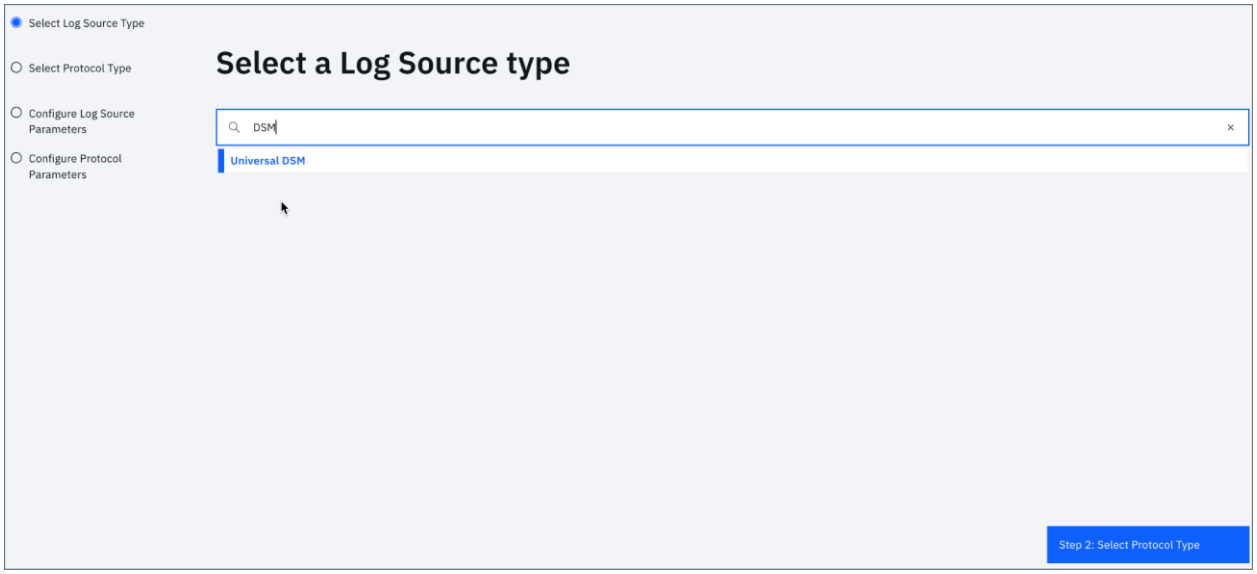


Depending on the requirement, you can connect a single or multiple log sources. In this setup, we will connect a single log source.

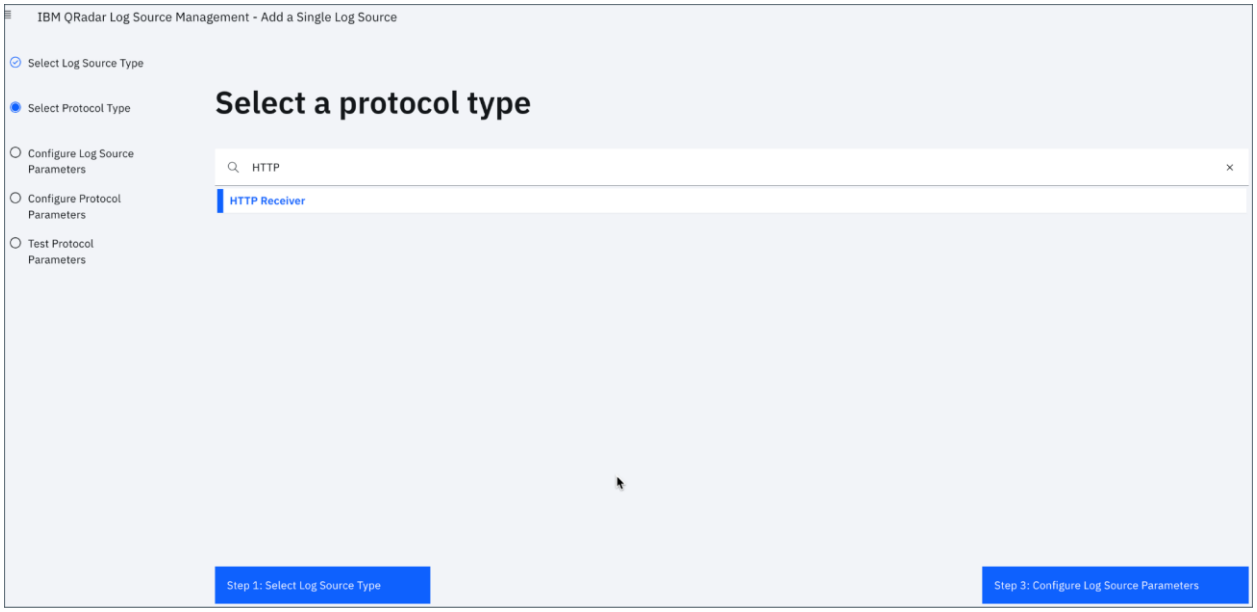


5. In the Add a Single Log Source wizard, select the log source type from the predefined list. For Cohesity integration, we will use the **Universal DSM**. Click Step 2.

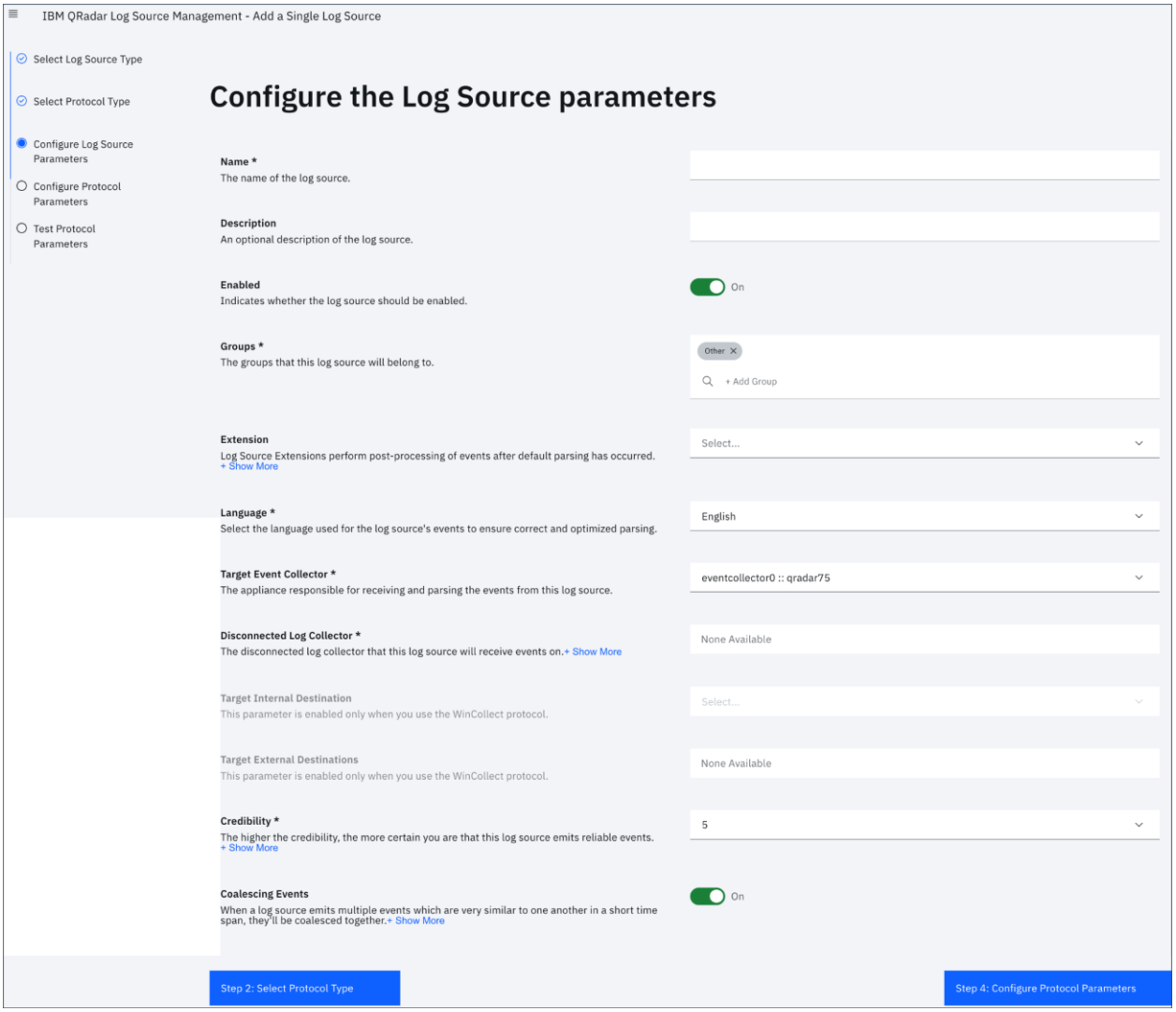




6. In the Select Protocol Type, choose **HTTP Receiver**. Click Step 3.



7. In the Configure Log Source parameters, enter the details of your log source, like name, description etc., and click Step 4.

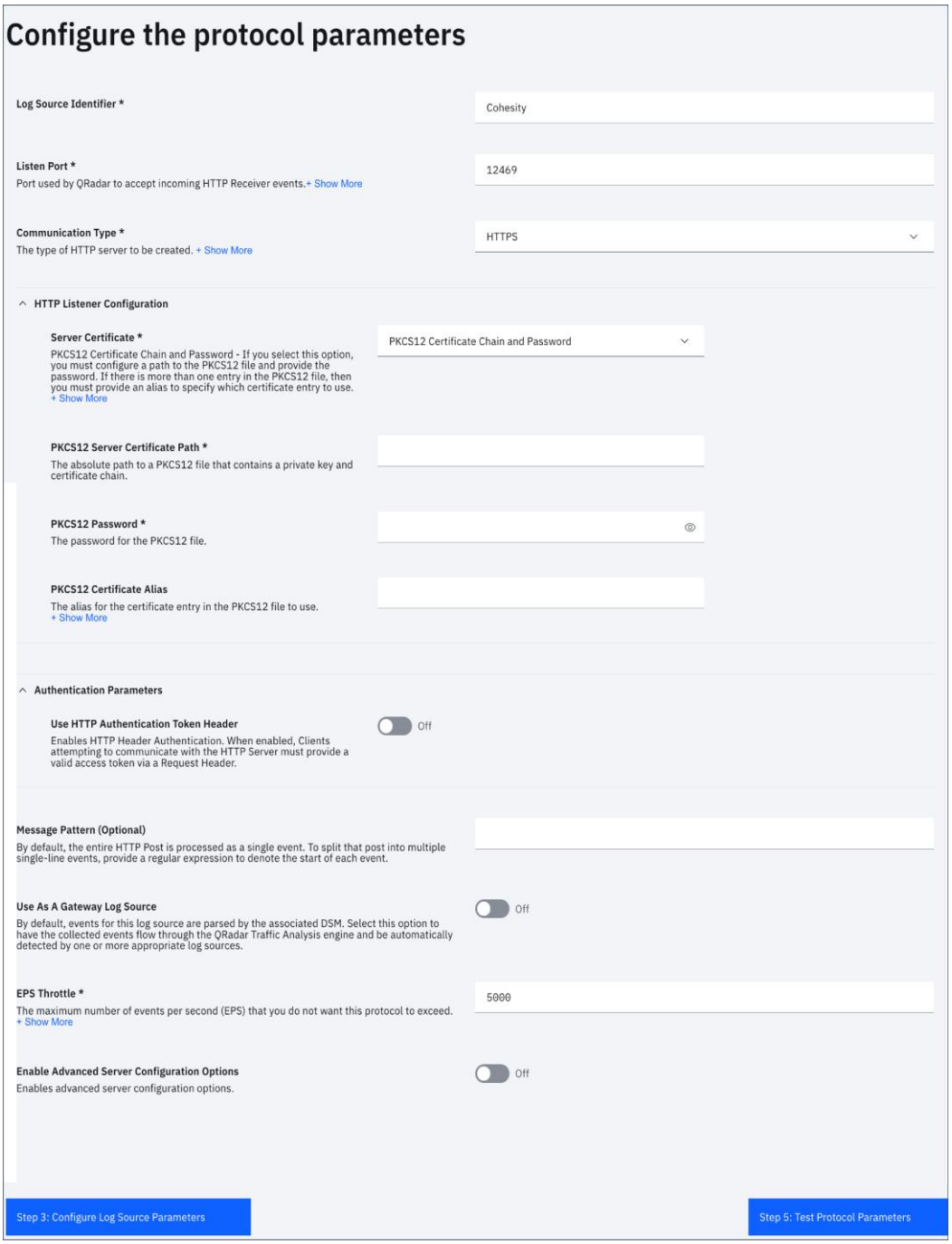


For more details on log source parameters, refer to IBM documentation.

8. Configure the protocol-specific parameters for your log source. In this example, we are configuring the **HTTP Receiver** protocol.

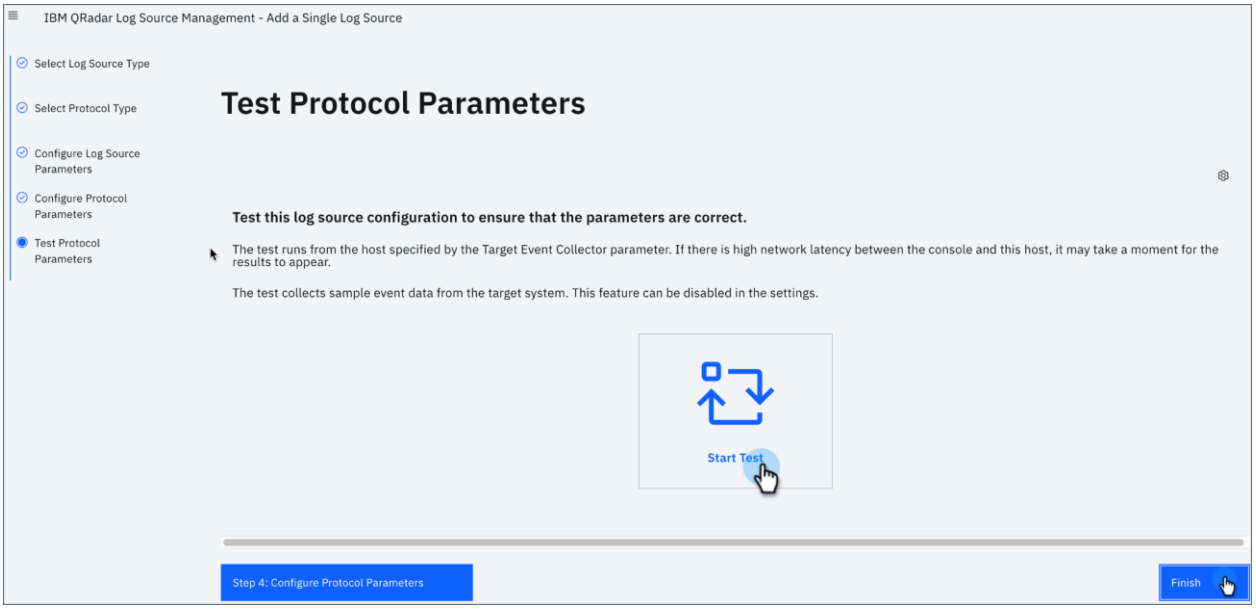
   IBM QRadar uses the **Lister Port** to accept incoming HTTP Receiver events. The default port is **12469**.

   You can choose the Communication Type to HTTP, HTTPs, or HTTPs with Mutual TLS. Secure communication is recommended.



Refer to IBM documentation for more details on configuring HTTP Receiver protocol. Click Step 5.

9. Click **Start Test** to test the protocol parameters and validate whether the port configured is open for listening. Click **Finish** to complete the Log source configuration.

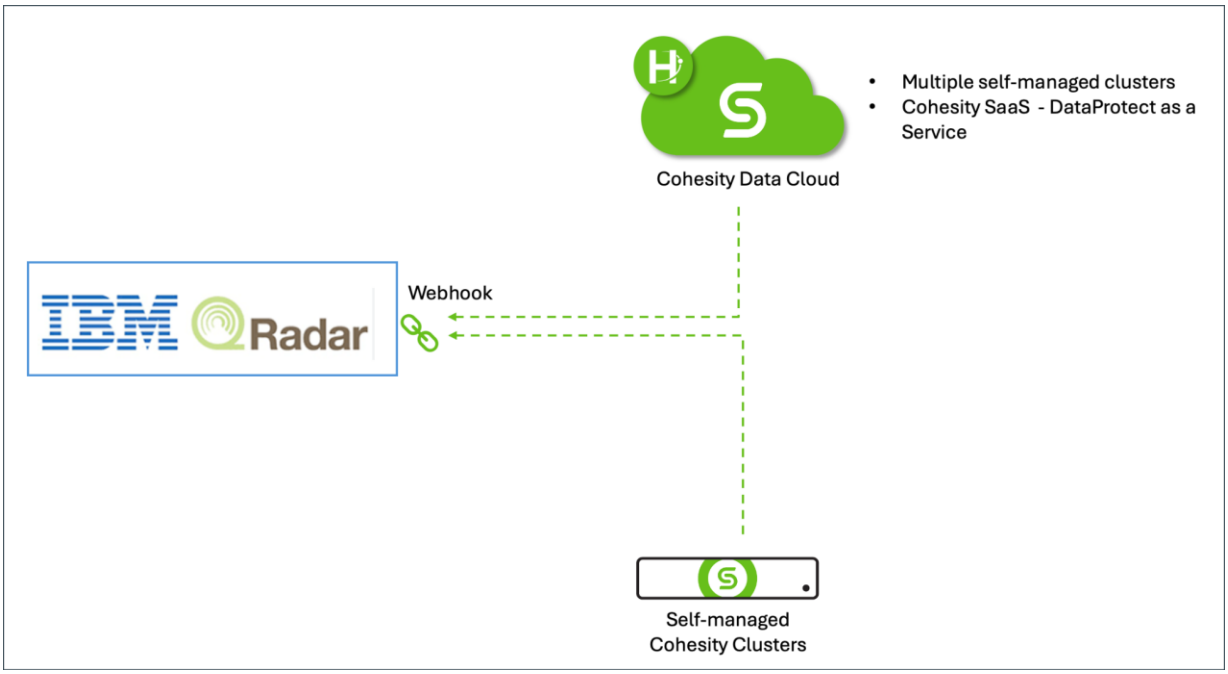


Configure Webhook on Cohesity

Alert notifications via webhooks can be configured on Cohesity in two ways:

1. At the Cluster Level - Configure alert notifications for a single cluster. These alerts capture cluster health-related issues (hardware, software, and maintenance) and the performance of data services.
2. Via Helios - Configure alerts for multiple clusters, including self-managed clusters (on-premises or in the cloud) and Cohesity-managed clusters for Cohesity SaaS offerings—DataProtect as a Service and DataHawk. These alerts capture cluster-level alerts described above and data security alerts on sensitive data and IOCs within Cohesity backups.

Figure 3: Cohesity Integration with IBM QRadar

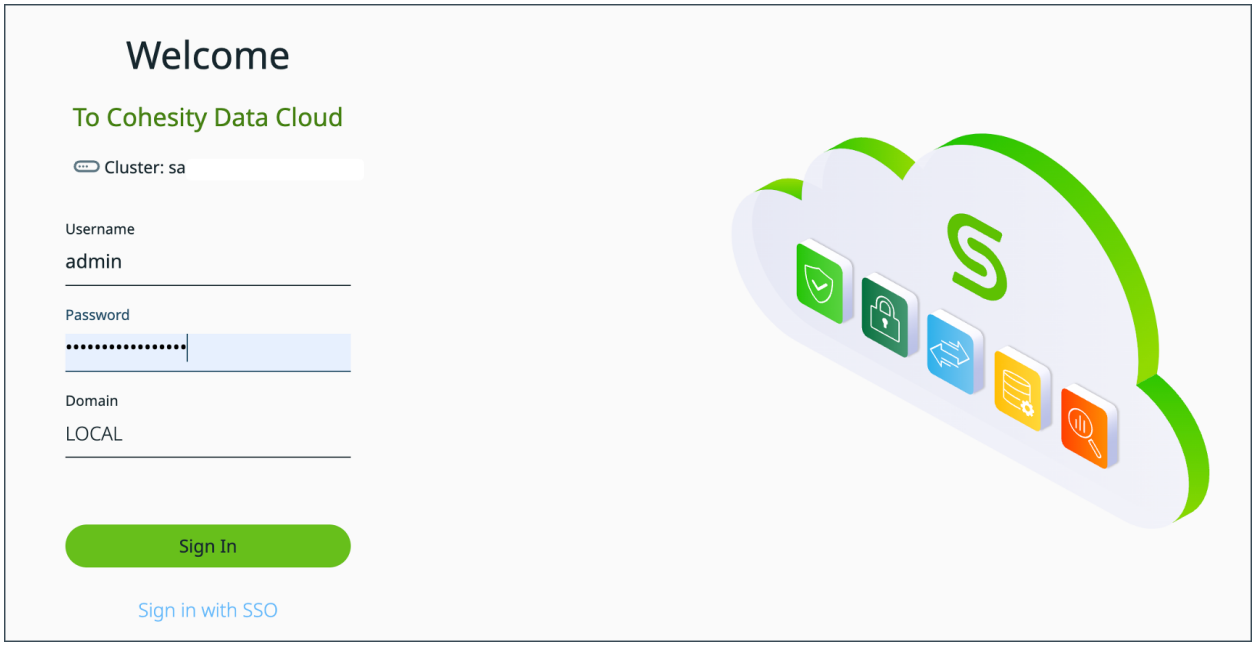


At The Cluster Level

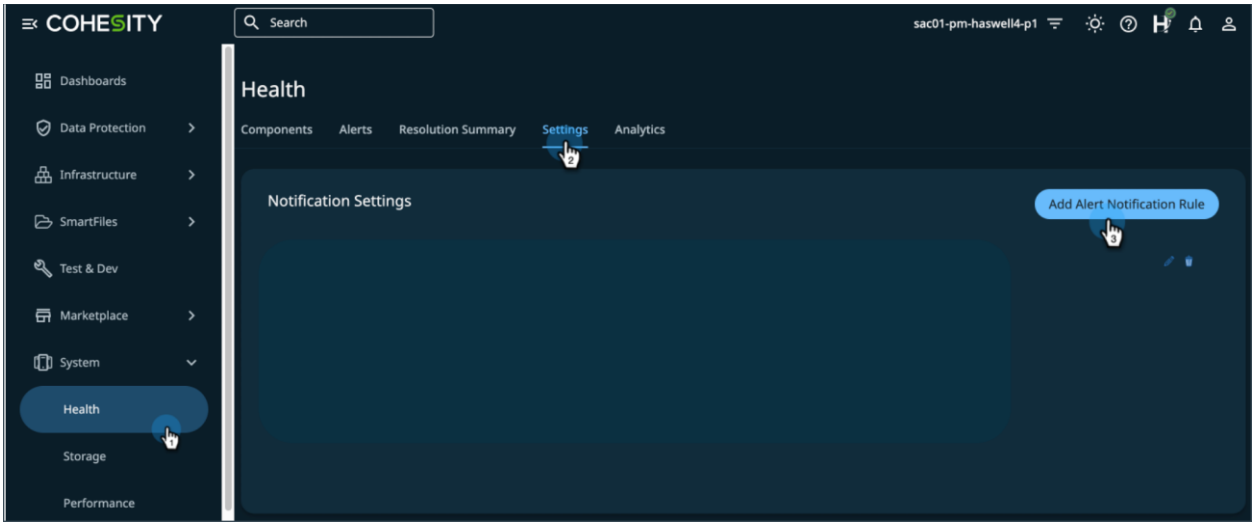
Cohesity leverages webhooks to send alert notifications to the QRadar SIEM appliance. These alert notifications are sent independently at the cluster level.

Follow the steps below to configure webhooks on the Cohesity on-premise cluster.

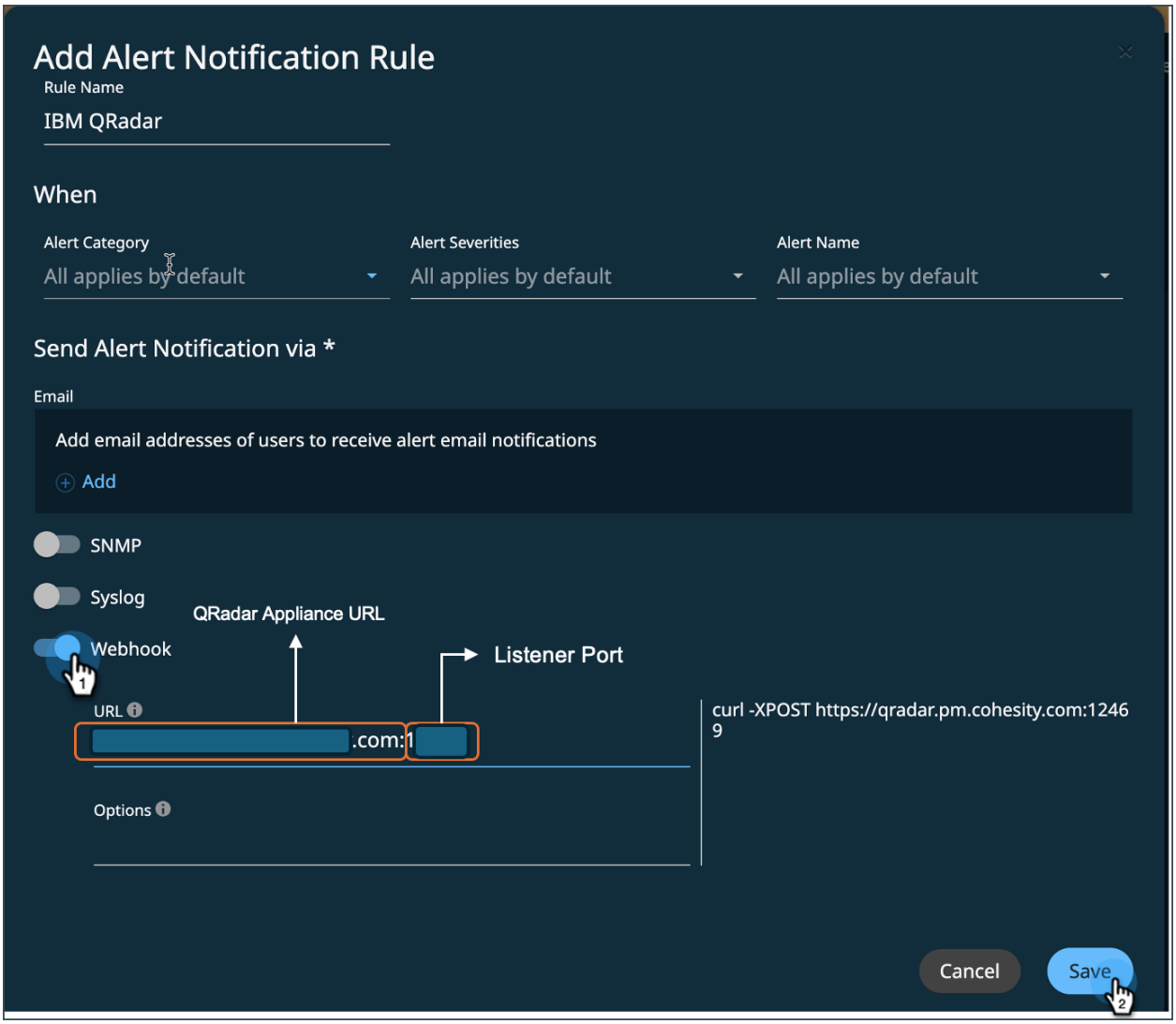
1. Log in to Cohesity self-managed cluster.



2. Navigate to **System** > **Health** and select the Alerts tab. The Alerts summary page is displayed.
3. Select the Settings tab, and click Add Alert Notification Rule.



4. In the **Alert Notification Rule** wizard, fill in the details to filter the alerts you want to send to the QRadar. By default, all are selected.
   Enable Webhook and enter the QRadar appliance URL and the listener port configured in the QRadar protocol parameters.



Refer to Cohesity docs for more details on configuring Webhooks for on-premise clusters.

Via Helios

Helios is a SaaS-based management platform that provides a single view and global management of all Cohesity clusters, whether on-premises, cloud, or Virtual Edition. Configuring alert notifications through webhooks on Helios allows for seamless transmission of cluster-level and security alerts. The security alerts can include threat detection, data classification, and anomaly detection.

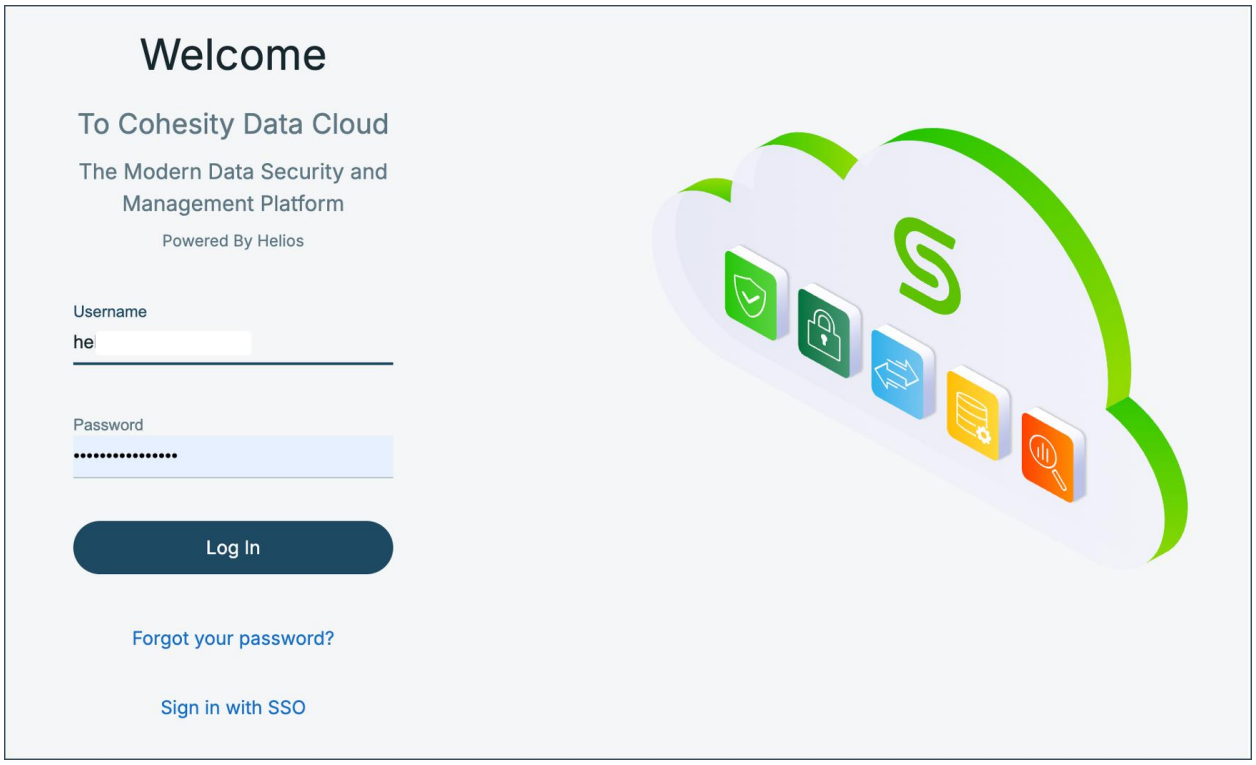
Under the Protection pillar of Helios, you can configure alert notifications for the following apps:

1. DataProtect - Offers a unified view and global management of all your Cohesity clusters—on-premises, in the cloud, or as Virtual Editions— regardless of the cluster size. You can easily connect your clusters to Helios and access them from anywhere using an internet connection and your Cohesity Support Portal credentials.
2. DataProtect as a Service - Cohesity's SaaS offering that protects your virtual and physical workloads, databases, and applications.

DataProtect

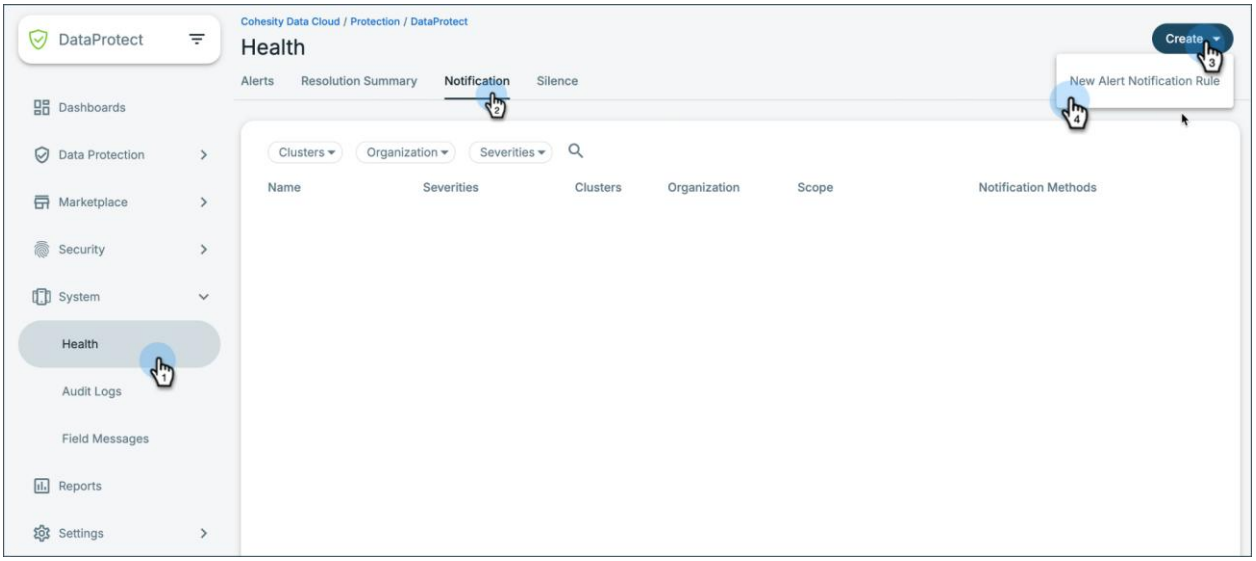
For clusters managed through Helios, follow the steps below to configure the webhooks to send alert notifications to the IBM QRadar.

1. Log in to Cohesity Helios.



2. Navigate to **Protection** > **Data Protect**.
3. Navigate to the **Health** > **Notification** tab.

4. Click **Create** > **New Alert Notification Rule**.



Refer to Cohesity docs for more details on configuring Webhooks for the Cohesity Data Cloud.

NOTE: Ensure connectivity from Helios to the IBM QRadar appliance. Alert notifications will not reach the QRadar SIEM if Helios cannot connect to the appliance.

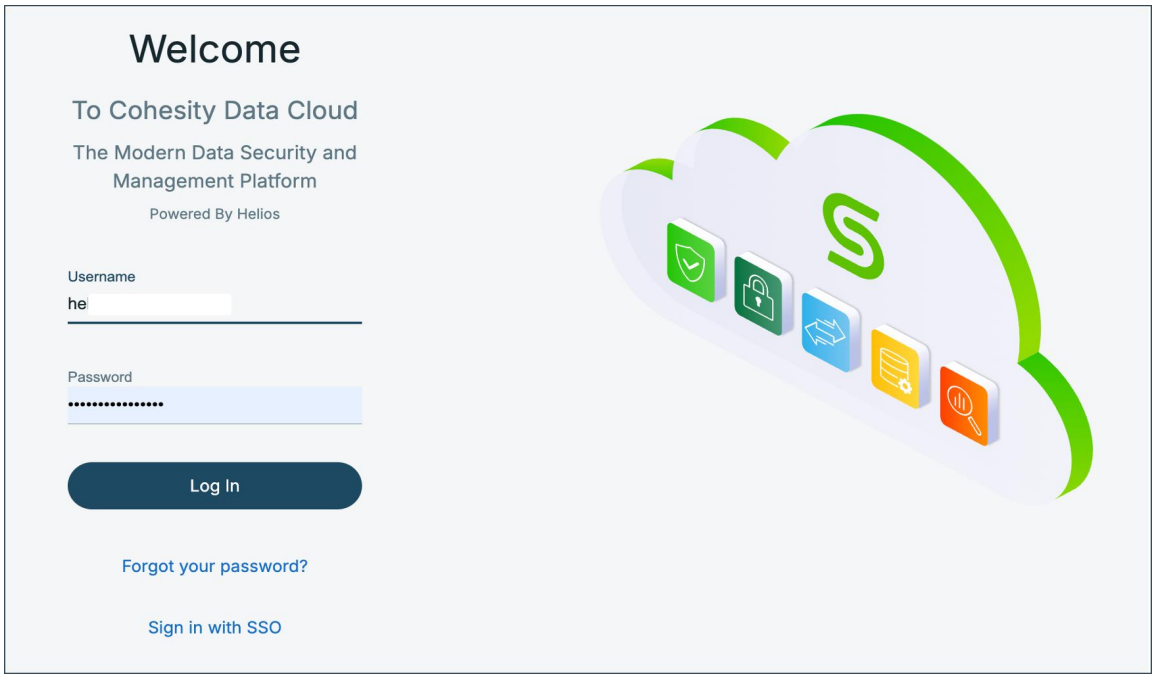
NOTE: DataHawk alerts are only available on Helios. To receive DataHawk alert notifications, configure webhooks on the Helios.

Cohesity DataProtect as a Service

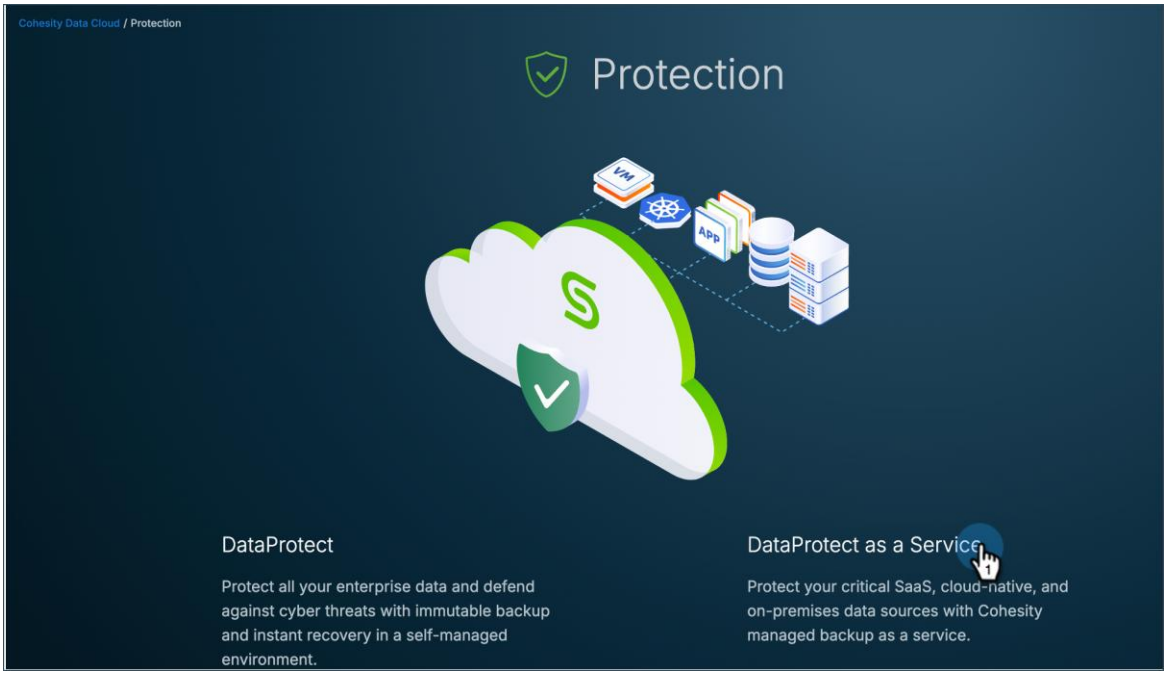
Alert notifications can be sent independently from Cohesity DataProtect as a Service.

Follow the steps below to configure webhooks on Cohesity Data Cloud DataProtect as a Service.

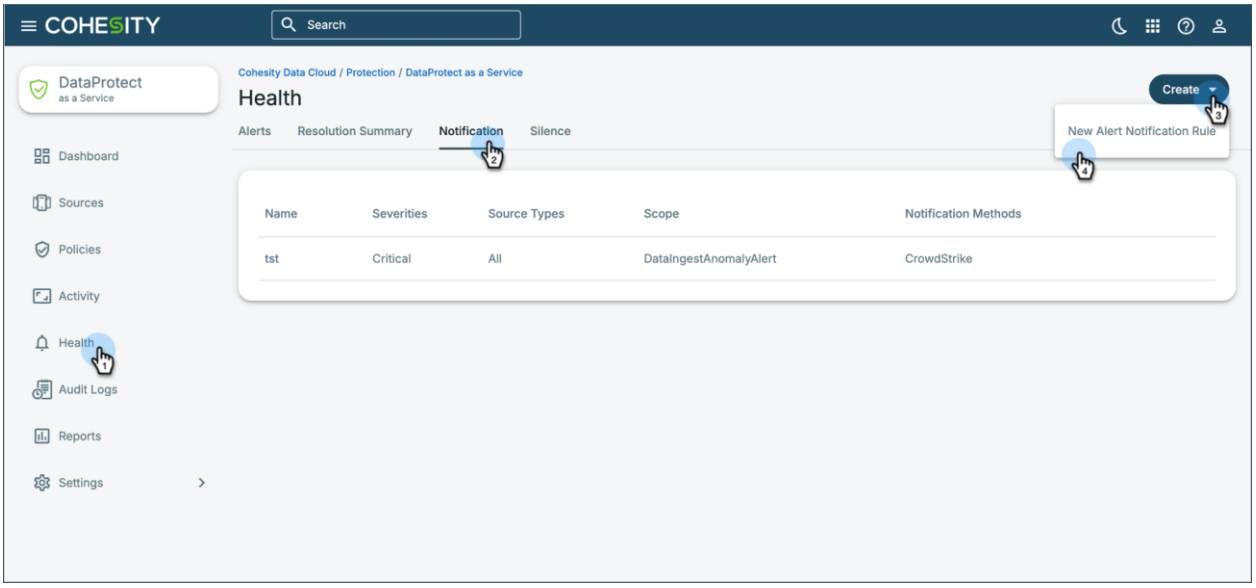
1. Log in to Cohesity Helios.



2. Navigate to **Protection** > **Data Protect as a Service**.



3. Navigate to the **Health** > **Notification** tab.
4. Click **Create** > **New Alert Notification Rule**.



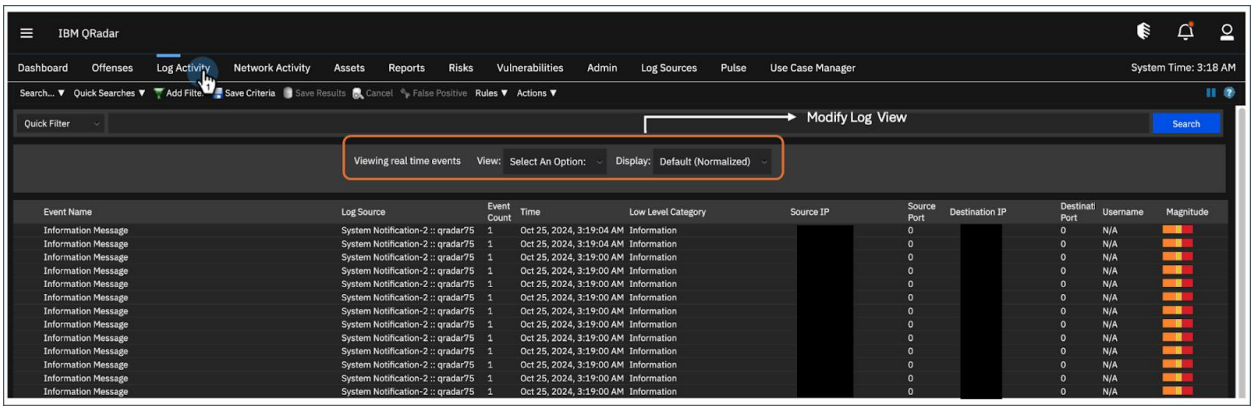
Refer to Cohesity docs for more details on configuring Webhooks for the Cohesity Data Cloud.

Manage Events on IBM QRadar

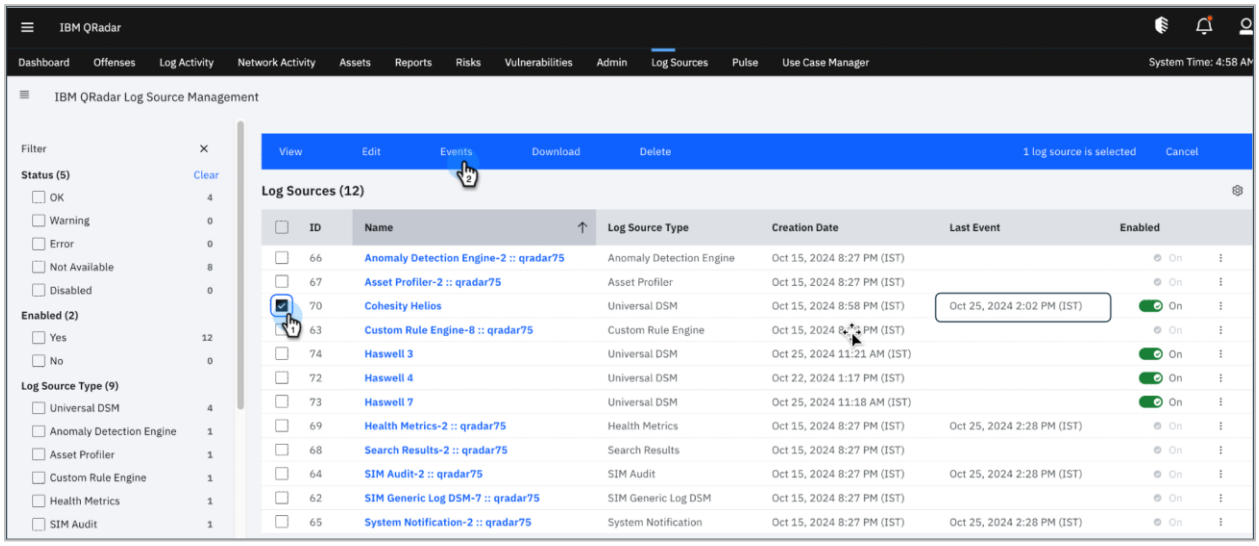
QRadar receives alerts from multiple log sources. Using the Log Activity tab, you can monitor and investigate log activity (events) in real-time or perform advanced searches.

To view the logs, click on **Log Activity** in the QRadar UI.

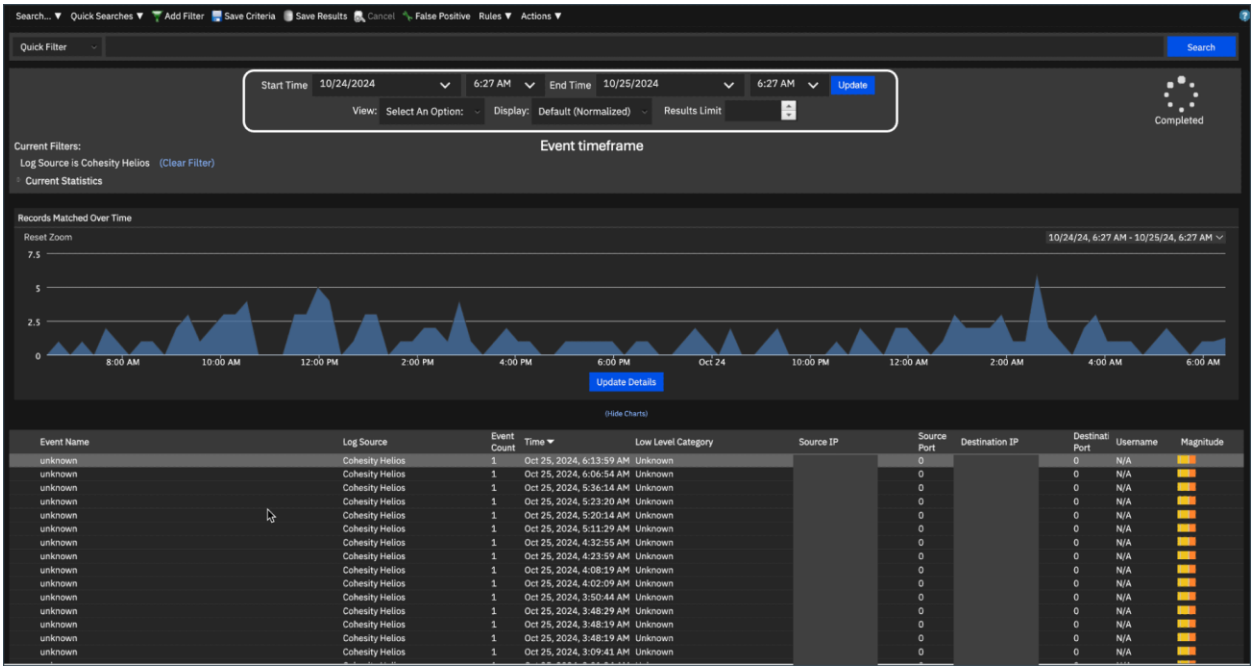
You can modify the view from real to a different time frame.



To view the events of a particular log source, be it Helios or a Cohesity on-premise cluster, go to Log Sources, select the Log source, and click on **Events** to view the events.



The events page displays all the events in the defined time frame.



Manage Events on DSM Editor

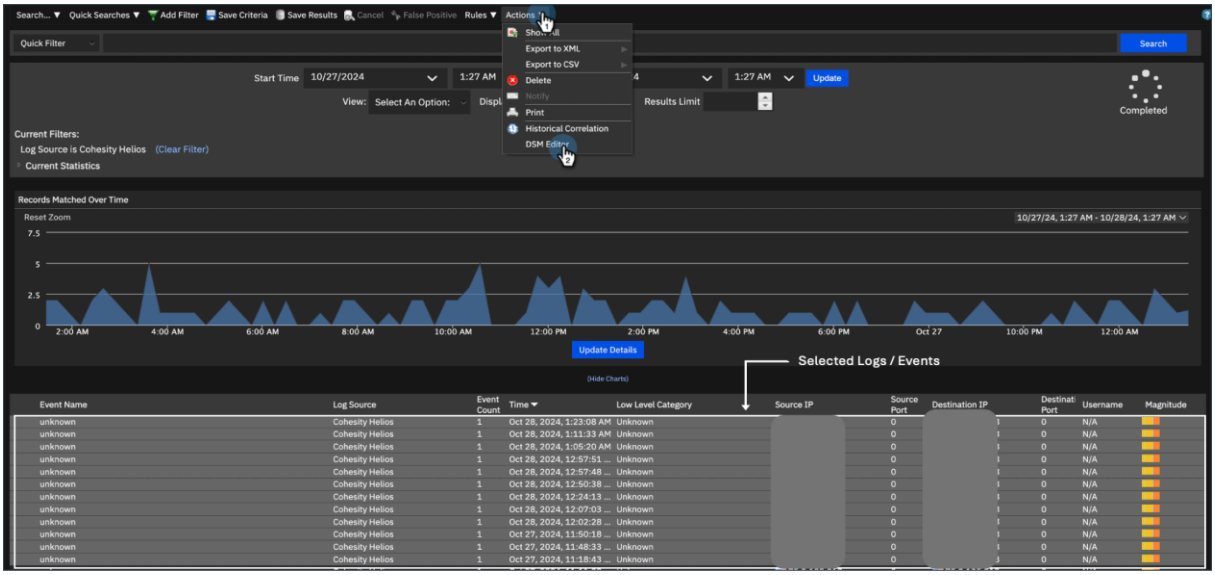
The DSM Editor provides different views of your data. The DSM Editor in IBM QRadar allows users to perform various tasks:

1. **Custom parsing**: Create custom parsers to get events into QRadar.
2. **Log source extensions**: Create log source extensions to get data into QRadar.
3. **Field extraction**: Extract fields from events.
4. **Custom properties**: Define custom properties for rules and search indexing.
5. **Event categorization**: Categorize events and store extra metadata.
6. **QID definitions**: Define new QID definitions.
7. **Log source types**: Create and configure custom log source types.

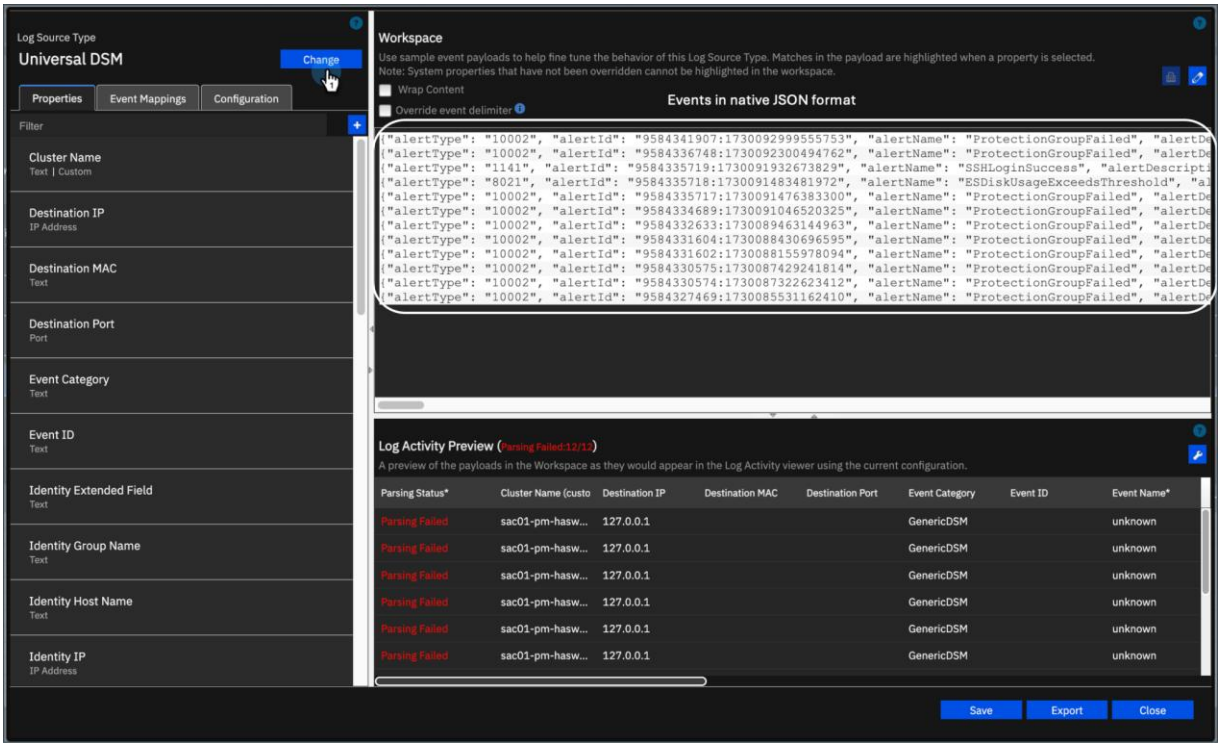
Configuring the DSM Editor

Let us configure the log source with the DSM editor and categorize the events and exact fields according to our requirements.

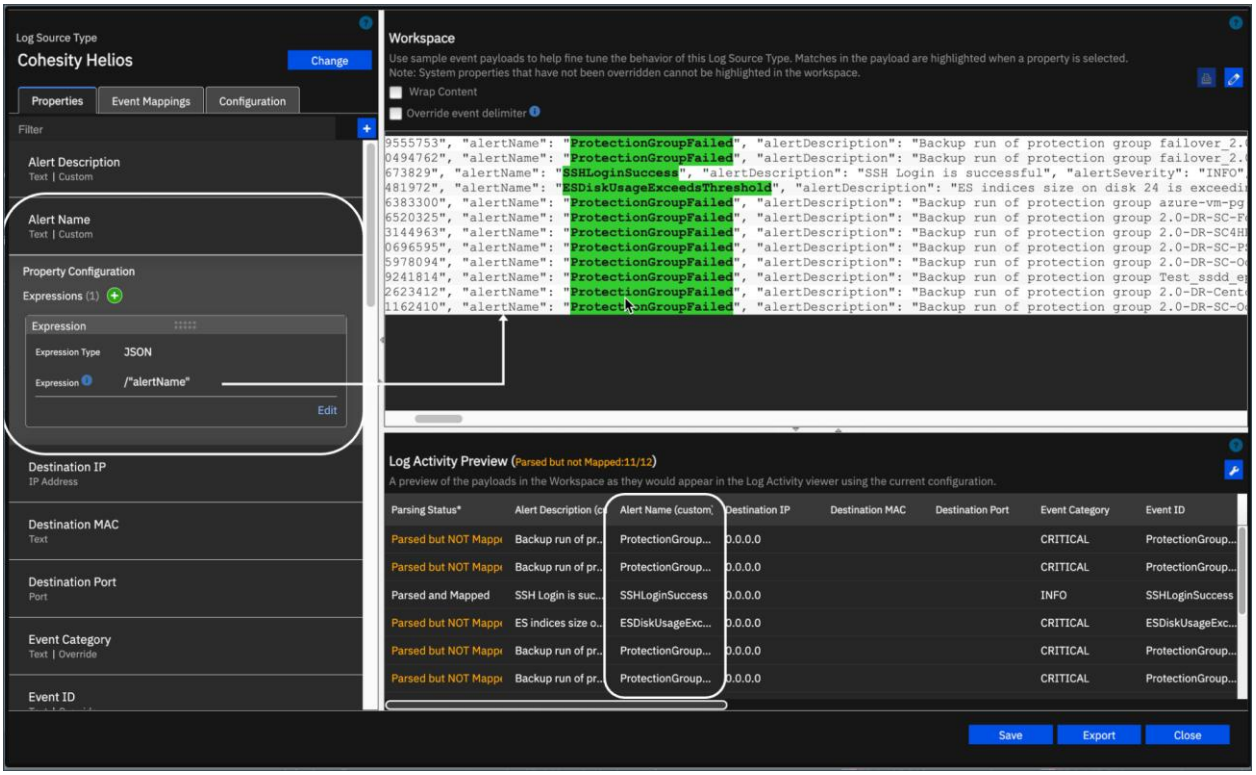
1. Log in to IBM QRadar and select your log source from the Log sources.
2. Select one or multiple events from the timeline and click on **DSM Editor** from the **Actions** dropdown.



3. In the DSM editor, change the log source to the desired log source, such as the Cohesity Helios or On-Premise cluster.

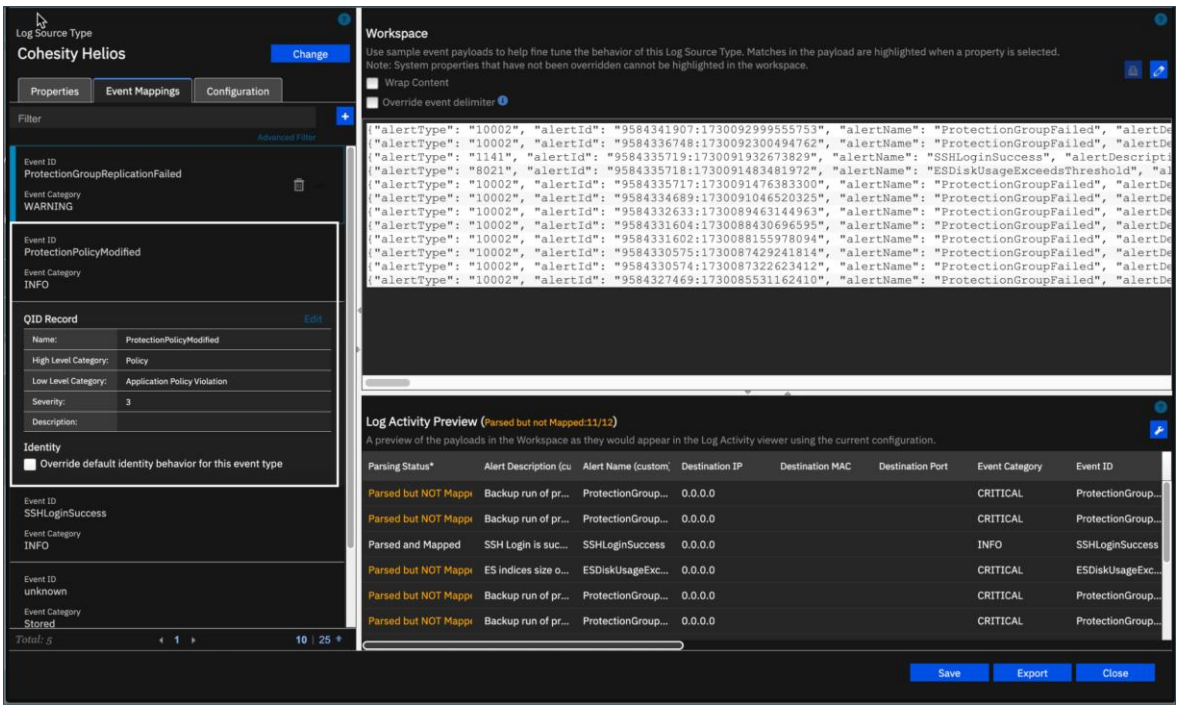


4. You can configure custom properties based on the nature of the alert and the payload. Create a custom property to extract data that IBM® QRadar® does not typically show from the event or flow payloads. In this example, we have created custom properties to extract the **Alert Name** and **Alert Description** from the event JSON. The custom properties are identified by the *custom* subtext and by *(custom)* in the Log Activity Preview.



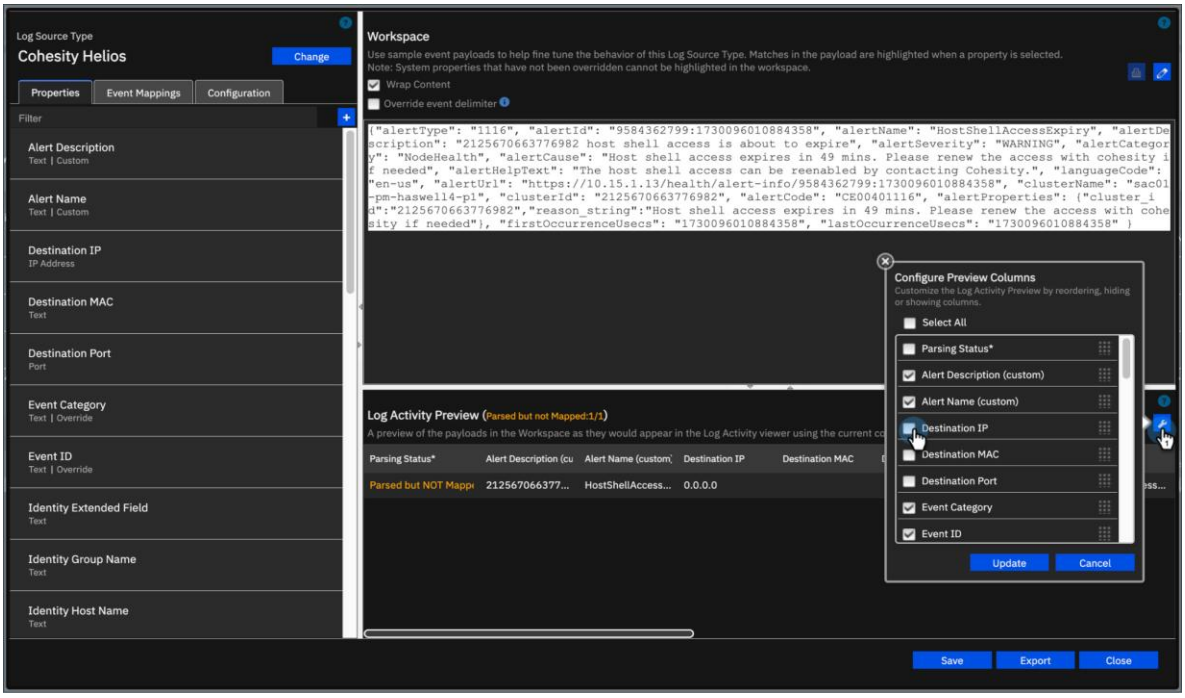
For more details on Custom Properties, refer to IBM documentation.

5. Further, you can map the events with category combinations in the QRadar system. An event mapping represents an association between an event ID and category combination and a QID record (referred to as event categorization).



For more details on Event Mapping, refer to IBM documentation.

6. You can further customize the **Log activity Preview** by configuring **Preview Columns.** Select the columns you find useful and want to display the information in, and click **update**.



7. Save the configuration.

Configuring Rules

IBM QRadar includes rules that detect various activities, generate data, and identify anomalies. You can also create your own rules to detect unusual activity.

For more information on configuring custom rules, refer to IBM documentation.

Appendix

IBM QRadar Overview

As the cost of a data breach rises and cyberattacks become increasingly sophisticated, the role of security operations center (SOC) analysts is more critical than ever. IBM QRadar SIEM is more than a tool; it is a teammate for SOC analysts—with advanced AI, powerful threat intelligence, and access to the latest detection content.

IBM QRadar SIEM uses multiple layers of AI and automation to enhance alert enrichment, threat prioritization, and incident correlation. It presents related alerts cohesively in a unified dashboard, reducing noise and saving time. QRadar SIEM helps maximize your security team's productivity by providing a unified experience across all SOC tools with integrated, advanced AI and automation capabilities.

To learn more about IBM QRadar capabilities, refer to IBM.com.

Cohesity Data Cloud Overview

Cohesity Data Cloud is a unified platform for securing, managing, and extracting value from your data, that reduces your attack surface, lowers costs, and minimizes risk. Cohesity Data Cloud is available as self-managed software and SaaS with rich features, including.

- **Modern Backup and Recovery**—The most comprehensive, modern, web-scale data management and backup and recovery solution to protect cloud-native, SaaS, and on-prem data at scale. You get instant recovery at scale and with direct metadata snapshots (so that each backup performs like a synthetic full), the ability to instantly put backed-up file shares online, and continuous data protection (CDP).
- **Traditional and Modern Workloads**—Support for VMs, databases, files, containers, cloud-native, SaaS, Storage, and traditional workloads.
- **Defend Against Ransomware Attacks**—Multilayered security architecture with Zero Trust Security, including granular RBAC, MFA, SSO, immutable snapshots, and ML-based ransomware attack detection. Protect and recover against ransomware with threat protection, cyber vaulting, and ML-powered data classification.
- **Threat Protection and Data Classification**—Highly curated and managed threat feeds, trained with ML, threat detection and response to your specific needs by augmenting the extensive library of over 200,000 behavioral patterns, create multiple YARA rules defining Indicators of Compromise (IOC), or import custom rules. Highly accurate NLP and ML-based engines classify sensitive data, automatically or on-demand, including personally identifiable information (PII), PCI, and HIPAA.
- **Global Search and Unified Management**—Reduce recovery point objectives to minutes by eliminating slow-to-access, chain-based backups. A single management platform offering multilayered security architecture, unifying operations with integrated solutions for backup, CDP, DR, search, ransomware attack detection, and vulnerability scanning into a single scalable environment.

- **Cloud Vault**—Cohesity FortKnox is a SaaS cyber vaulting and recovery solution that gives your data additional layers of managed security and protection against cybersecurity threats. To learn more, refer to Cohesity product documentation.
- **Cloud Archive**—Policy-based data archival to meet long-term data retention, compliance, and regulatory requirements.
- **Cohesity Cloud Services**—Cohesity-managed data security and management with SaaS that runs multiple cloud data services, including backup, cyber vaulting, threat defense, data classification, DR, and more on a single multi-cloud platform.
- **Cohesity Gaia**—Combines generative AI with your enterprise data. Unlock data insights by bringing retrieval augmented generation (RAG) AI and large language models (LLMs) to enterprise data within Cohesity. Ask natural language questions and get context-rich answers.
- **Business Continuity**—Simplify business continuity and disaster recovery with automated failover and failback orchestration for your mission-critical workloads. Get your critical applications online after a breach or outage through automated orchestration.
- **Security Integrations**—Cohesity integrates with leading perimeter and end-point security vendors, giving you greater visibility and actionable alerts in your Security Operations Center (SOC).
- **Deployment**—Software-defined solution for on-premises, public cloud, backup as a service, and edge sites.
- **API-first Extensibility**—Derive business insights with the Cohesity Marketplace partner ecosystem. Streamline operations and easily integrate on-prem and cloud environments with pre-built automated workflows and API integrations.

To learn more about how Cohesity provides **AI-powered data security and management**, refer to Cohesity.com.

Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Shashanka SR, Sr. Solutions Architect - Focuses on Security, Cohesity Gaia and GSI.

Other essential contributors included:

- Kamal Deka, Senior Product Manager at Cohesity. In his role, he focuses on Data Security (Threat Detection, Data Classification, Anomaly Detection).

Document Version History

VERSION	DATE	DOCUMENT HISTORY
1.1	Aug 2025	Republished with latest template
1.0	Nov 2024	First full release

ABOUT COHESITY

Cohesity is a leader in AI-powered data security and management. Aided by an extensive ecosystem of partners, Cohesity makes it easier to protect, manage, and get value from data – across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring for malicious behavior, and rapid recovery at scale. Cohesity solutions are delivered as a service, self-managed, or provided by a Cohesity-powered partner. Cohesity is headquartered in San Jose, CA, and is trusted by the world's largest enterprises, including six of the Fortune 10 and 44 of the Fortune 100.

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