

IBM® Storage

Cyber Resiliency with Splunk Enterprise and IBM FlashSystem Storage Safeguarded Copy with IBM Copy Services Manager

IBM Storage Team



© Copyright International Business Machines Corporation 2022.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About this document	1
Executive summary	2
Scope	3
Introduction	4
IBM FlashSystem Storage Safeguarded Copy function	4
IBM Copy Services Manager	4
Splunk Enterprise	5
Prerequisites	5
Solution overview	6
Control and data path use cases	7
Lab setup	7
Configuration and lab setup	8
Step 1: Configuring Splunk Enterprise	8
Step 2: Creating custom app config files in the Splunk Enterprise server	16
Step 3: Configuring IBM Copy Services Manager	22
Step 4: Configuring IBM FlashSystem Storage for Safeguarded Copy	24
Step 5: IBM FlashSystem Storage LUN that is mapped to a Windows server for a Microsoft SQL DB	27
Step 6: Use case for a brute force login attack on a Microsoft SQL server	28
Step 7: Validating Safeguarded Copy creation on IBM FlashSystem Storage	29
Summary	30
Authors	31
Resources	31
Notices	33
Trademarks	34
Terms and conditions for product documentation	35
Applicability	35
Commercial use	35
Rights	35
Privacy policy considerations	35



About this document

The focus of this document is to highlight early threat detection by using Splunk Enterprise and proactively start a cyber resilience workflow in response to a cyberattack or malicious user action. The workflow uses IBM® Copy Services Manager (IBM CSM) as orchestration software to invoke the IBM FlashSystem® storage Safeguarded Copy function, which creates an immutable copy of the data in an air-gapped form on the same IBM FlashSystem Storage for isolation and eventual quick recovery.

This document explains the steps that are required to enable and forward IBM FlashSystem audit logs and set a Splunk forwarder configuration to forward local event logs to Splunk Enterprise. This document also describes how to create various alerts in Splunk Enterprise to determine a threat, and configure and invoke an appropriate response to the detected threat in Splunk Enterprise. This document explains the lab setup configuration steps that are involved in configuring various components like Splunk Enterprise, Splunk Enterprise config files for custom apps, IBM CSM, and IBM FlashSystem Storage. The last steps in the lab setup section demonstrate the automated Safeguarded Copy creation and validation steps.

This document also describes brief steps for configuring various components and integrating them. This document demonstrates a use case for protecting a Microsoft SQL database (DB) volume that is created on IBM FlashSystem Storage. When a threat is detected on the Microsoft SQL DB volume, Safeguarded Copy starts on an IBM FlashSystem Storage volume. The Safeguarded Copy creates an immutable copy of the data, and the same data volume can be recovered or restored by using IBM CSM.

This publication does not describe the installation procedures for Splunk Enterprise, Splunk Forwarder for IBM CSM, the Microsoft SQL server, or the IBM FlashSystem Storage setup. It is assumed that the reader of the book has a basic understanding of system, Windows, and DB administration; storage administration; and has access to the required software and documentation that is used in this document.

Executive summary

The financial impact of cyberattacks continues to rise. Cyberattacks can happen in various ways. They can take the form of malware or ransomware that is targeted at stealing confidential data or holding valuable information for ransom. Sometimes these attacks are designed to destroy confidential data to cripple organizations. In many cases, these data breaches involve internal threat actors.

Traditional approaches to data protection work well for their intended purposes but are not adequate to protect against cyberattacks, which might encrypt or otherwise corrupt your data. Remote replication for disaster recovery replicates all changes including malicious ones to the remote copy. Recovery from a widespread attack by using data that is stored on offline media or the cloud might take too long. Large-scale recovery can take days to weeks, which lead to substantial downtime for businesses.

Detecting a threat before it starts can help speed recovery. Splunk Enterprise monitors activities for signs that might indicate the start of an attack, such as logins from unusual IP addresses or outside business hours. When threat detection and saved alerts occur, triggered conditions for Splunk Enterprise alerts and integration with IBM CSM can proactively invoke Safeguarded Copy to create a protected backup at the first sign of a threat.

The Safeguarded Copy function helps businesses recover quickly and safely from a cyberattack in minutes or hours. It creates multiple recovery points for a production volume. These recovery points are called Safeguarded Copy backups. The recovery data is not stored in separate regular volumes but in a storage space that is called Safeguarded Copy backup capacity, which creates a logical air gap. The backups are not directly accessible by a host. The data can be used only after a backup is recovered to a separate recovery volume.

In an attack, the orchestration software IBM CSM creates and identifies the best Safeguarded Copy backup to use, and it automates the process to restore or recover data to online volumes. Because a restore action uses the same snapshot technology, it is much faster than using offline copies or copies that are stored in the cloud.

Scope

The focus of this document is to showcase early threat detection on IBM FlashSystem Storage system and proactively invoke Safeguarded Copy to create an immutable backup at the first sign of a threat. The IBM CSM orchestration software interacts with IBM FlashSystem Storage to invoke a schedule task for a Safeguarded Copy backup. IBM CSM also is used for recovery or a restore of that backup.

As part of early threat detection, several alerts and saved alerts in Splunk Enterprise are shown. A sample Python script is provided that is used to invoke the Safeguarded Copy action.

Customers and readers are encouraged to create control path and data path use cases that are customized for Splunk Enterprise. They also should create custom response scripts and custom apps in Splunk Enterprise that are suited to their environment. The use cases, alerts, saved alerts, and Python script should be seen as templates or guides. They may not be used “as is” in a production environment.

The solution that is featured in this document is created by using Splunk Enterprise, IBM FlashSystem Storage, and IBM CSM. The IBM CSM Scheduled task feature is used to create the required workflow. The sample workflow that is explained is part of the solution, and it involves invoking Safeguarded Copy for the IBM FlashSystem Storage volume.

All the components that are described in this document, such as Splunk Enterprise, Splunk forwarder, IBM CSM, and the Microsoft SQL server are in the same network. More adequate network planning is required if these systems are in different segments.

For more information about Splunk Enterprise, Safeguarded Copy, IBM CSM, and IBM FlashSystem Storage, see “Resources” on page 31.

Introduction

Combining the capabilities of IBM FlashSystem Storage Safeguarded Copy, IBM CSM, and Splunk Enterprise enables enterprises to build comprehensive cyber resilience solutions that address the Protect and Recover and the Detect and Respond functions of the NIST framework. For more information, see [NIST Framework Documents](#).

Splunk Enterprise can log user activities in the access and audit logs, which contain all the storage object access information. To identify and detect potential malicious access or activities and check for compliance auditing, these access and audit logs must be integrated with the Splunk Enterprise and Security Information and Event Management (SIEM) solution.

IBM FlashSystem Storage Safeguarded Copy function

The Safeguarded Copy feature creates immutable backups that are not accessible by the host system, and it protects these backups from corruption that might happen in the production environment. A Safeguarded Copy schedule can be defined to create multiple backups regularly, such as hourly or daily.

Safeguarded Copy can create backups with more frequency and capacity compared to IBM FlashCopy® volumes. Creating Safeguarded Copy backups also has less of an impact than creating multiple target volumes by using FlashCopy.

The Safeguarded Copy function provides backup copies to recover data in case of logical corruption or destruction of primary data.

Safeguarded Copy uses a backup capacity, production volume, and recovery volume:

- ▶ Backup capacity can be created for any production volume. The size of the backup capacity depends on the frequency of the backups and the length of the duration that the backups must be retained.

The Safeguarded Copy session creates a consistency group across the source volumes to create a safeguarded backup, which stores the required data in the backup capacity.

- ▶ The production volume is the source volume for a Safeguarded Copy relationship. Depending on the specific client topology, this relationship might be a Metro Mirror, Global Mirror, or Global Mirror with change volume.
- ▶ A recovery volume is used to restore a backup copy for host access while production continues to run on the production volume. The recovery volume is the target volume for a Safeguarded Copy recovery, which enables a previous backup copy to be accessed by a host that is attached to this volume. The recovery volume is always thick-provisioned.

Management of the Safeguarded Copy is supported by IBM CSM 6.2.3 or later. The management software can create and recover backups and define policies for expiration.

IBM Copy Services Manager

IBM CSM controls copy services in storage environments. Copy services features are used by storage systems such as IBM Spectrum® Virtualize for Public Cloud (IBM SV4PC) to configure, manage, and monitor data-copy functions.

Copy services include FlashCopy, Metro Mirror, Global Mirror, and Metro/Global Mirror. IBM CSM runs on Windows, IBM AIX®, Linux, Linux on IBM zSystems, and IBM z/OS® operating systems. When it is running on z/OS, IBM CSM uses the Fibre Channel connection (IBM FICON®) to connect to and manage count key data (CKD) volumes.

The fully licensed version of IBM CSM provides all supported FlashCopy, Metro Mirror, Global Copy, Global Mirror, Metro/Global Mirror, and multi-target solutions.

IBM CSM provides a GUI, a command-line interface (CLI), and Representational State Transfer (RESTful) API for managing data replication and disaster recovery. Starting with IBM CSM 6.2.9, online help also integrates with the RESTful API.

Splunk Enterprise

Splunk Enterprise is a software product that enables you to search, analyze, and visualize the data that is gathered from the components of your IT infrastructure or business. Splunk Enterprise takes in data from websites, applications, sensors, devices, and so on. After you define the data source, Splunk Enterprise indexes the data stream and parses it into a series of individual events that you can view and search.

Most users connect to Splunk Enterprise with a web browser and use [Splunk Web](#) to administer their deployment; manage and create knowledge objects; run searches; and create pivots and reports. You also can use the CLI to administer your Splunk Enterprise deployment.

You can extend the Splunk Enterprise environment to fit the specific needs of your organization by using apps. An app is a collection of configurations, knowledge objects, views, and dashboards that run on the Splunk platform. A single Splunk Enterprise installation can run multiple apps simultaneously. You can browse available apps at [Splunkbase](#) or build your own apps at [Splunk Developer Program](#).

For more information about Splunk Enterprise, see [Splunk Enterprise Overview](#).

Prerequisites

This section outlines the prerequisites for the solution:

- ▶ IBM FlashSystem Storage administration skills with good understanding of Safeguarded Copy.
- ▶ IBM CSM 6.2.3 or later must be available and the IBM FlashSystem Storage must be registered in IBM CSM by using administrator privileges. For more information about IBM CSM document references, see “Resources” on page 31.
- ▶ A scheduled task must be defined inside IBM CSM. It must consist of various operations, depending on the functions that are used in the storage system. For example, when Copy Services such as Metro Mirror or Global Mirror are used, writes to target volumes must be suspended to achieve a consistent state before a Safeguarded Copy backup can be made.
- ▶ A Python script that initiates a Safeguarded Copy, which is available on [GitHub](#). Understanding the basic Python script and implementing the prerequisites are required for the script and automation.
- ▶ Make sure that the SafeGuarded pool virtual capacity is provisioned. To configure the SafeGuarded pool virtual capacity.
- ▶ Understanding IBM FlashSystem Storage is required for working with volumes and SafeGuarded pool capacity allotment.

- Make sure that Splunk Enterprise alerts and saved alerts are defined for the use case. In this case, we created rules for a specific case (a sample use case). Implement the alerts as needed for your requirements, such as brute force attack or a login failure for a DB user with an invalid password.
- Install Microsoft SQL 2019 on a Window host and configure users to access the DB. Restrict access to sensitive data table access as needed.

Solution overview

Organizations can face threats in multiple ways: compromised user credentials that are obtained through a spear-fishing attack; a rouge user within the organization; cyberattacks such as brute force attempts; and ransomware. Any of these threats poses grave risks to storage systems that are used for storing data.

To track admin actions, the solution implements various control path use cases. To track the application data changes, a data path use case is used.

A syslog configuration is created inside IBM FlashSystem Storage that allows forwarding of storage events to Splunk Enterprise and Splunk forwarder. The configuration is deployed on Windows along with local event configuration in Splunk Enterprise. Splunk Enterprise understands the events that are forwarded by IBM FlashSystem Storage, events that are forwarded from Splunk Forwarder, and local events from Windows and Microsoft SQL server. The Splunk Enterprise events are saved as alerts and categorized. The saved alerts are configured with custom action and triggered actions to create a saved alerts definition.

When the events classification completes and is saved as alerts, a Splunk Enterprise administrator can define several alerts to detect threats that are categorized under control and data path. When a threat is detected, a cyber resiliency response is invoked as a Python script that uses API commands to run a predefined IBM CSM scheduled task. The scheduled task feature of IBM CSM is used because it provides flexibility to run various operations, including conditional run times that are based on a certain state of a previously run command.

Figure 1 on page 7 represents the deployment overview of entire solution. Audit logs from IBM FlashSystem contain storage-related actions that were performed. To identify and detect potential malicious access and perform compliance auditing, these access logs must be integrated with the Splunk Enterprise and SIEM solution. Similarly, the application audit log events also are forwarded to Splunk Enterprise. The collected audit telemetry events are normalized and stored in a Splunk Enterprise DB. The preconfigured set of alerts analyses the normalized events for possible threat scenarios.

When a threat is detected, a cyber resilience workflow runs to create immutable Safeguarded Copy volumes in IBM FlashSystem Storage.

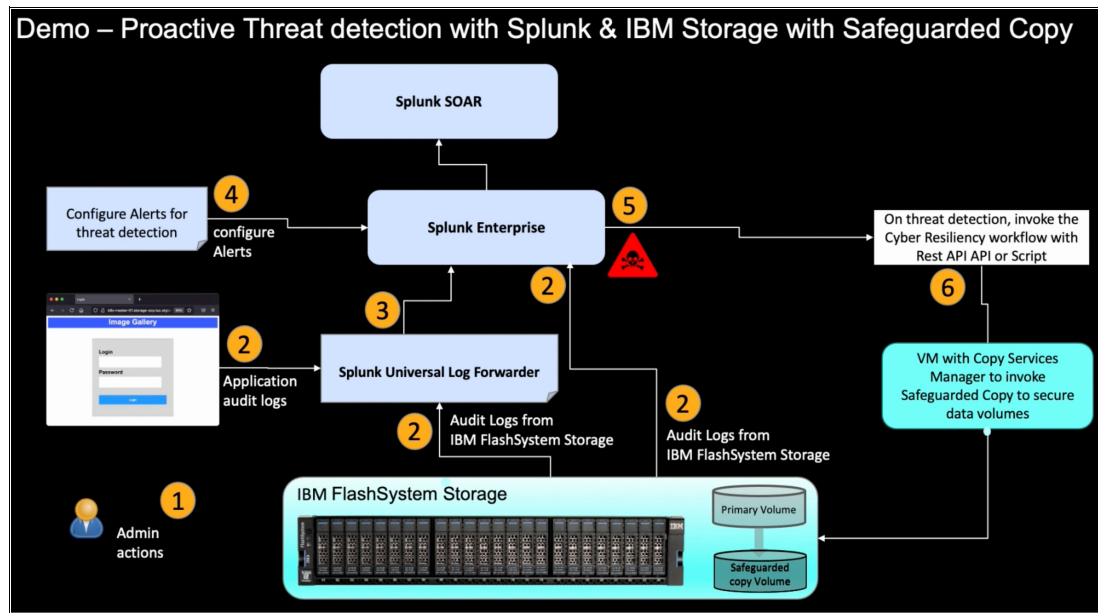


Figure 1 Deployment overview

Control and data path use cases

Sample control path use cases are listed in this section. This collection is not exhaustive, but it provides a general idea of threats. The security policy of an organization defines what a threat and its remediation should be.

- Log in to the DB and try to access the restricted tables. An event is generated for unauthorized access to DB tables. The event matches the saved alert criteria to invoke custom actions.

The DB user tries to access the data from the restricted tables. The DB user does not have access to the restricted tables, but they still try to access the data. This activity is an unauthorized one, so this type of activity should be detected and an alert should be generated to prevent any unauthorized access.

- Login failure for a DB user for an invalid password

This case is a classic one of compromised or shared credentials. This case also can be a user that uses a brute force attack to try to access the DB.

Lab setup

The lab setup that is described in this section briefly shows the configuration steps for various components like Splunk Enterprise, Splunk forwarder, IBM CSM, and Microsoft SQL server. For more information about product links and details configuration, see “Resources” on page 31.

Configuration and lab setup

To create the cyber resiliency solution by using Splunk Enterprise and IBM FlashSystem Storage Safeguarded Copy with IBM CSM, follow the steps in the subsections (“Step 1: Configuring Splunk Enterprise” on page 8 to “Step 7: Validating Safeguarded Copy creation on IBM FlashSystem Storage” on page 29) of this section.

Step 1: Configuring Splunk Enterprise

To configure Splunk Enterprise, complete the following steps:

1. Log in to the Splunk Enterprise portal with the username as admin and your password to configure and add data sources. Figure 2 shows the login window for Splunk Enterprise.

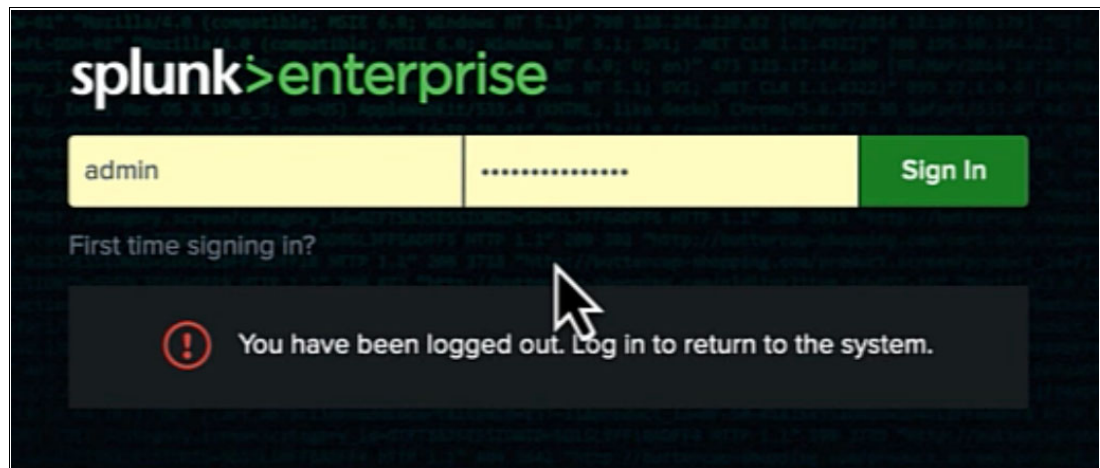


Figure 2 Splunk Enterprise login window

2. Select the data sources by clicking **Add Data**, as shown in Figure 3.

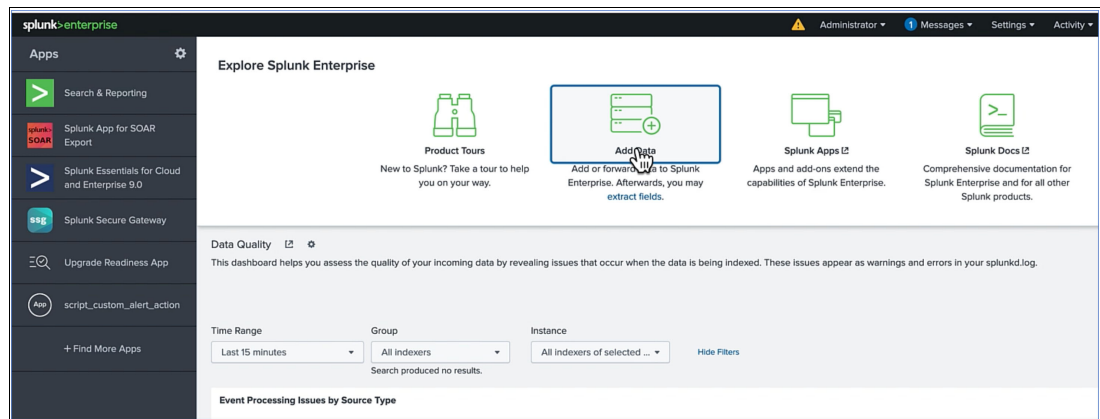


Figure 3 Adding data sources

3. Select the **TCP/UDP**, as shown in Figure 4 on page 9.

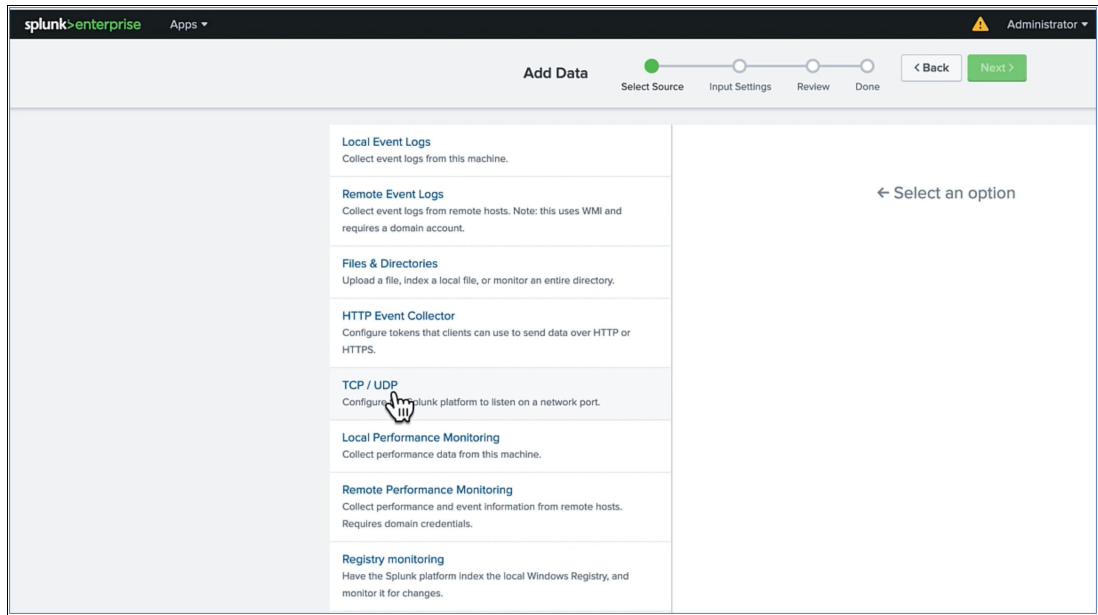


Figure 4 Adding TCP/UDP data sources

4. Add the source name and source type and click **Save**, as shown in Figure 5.

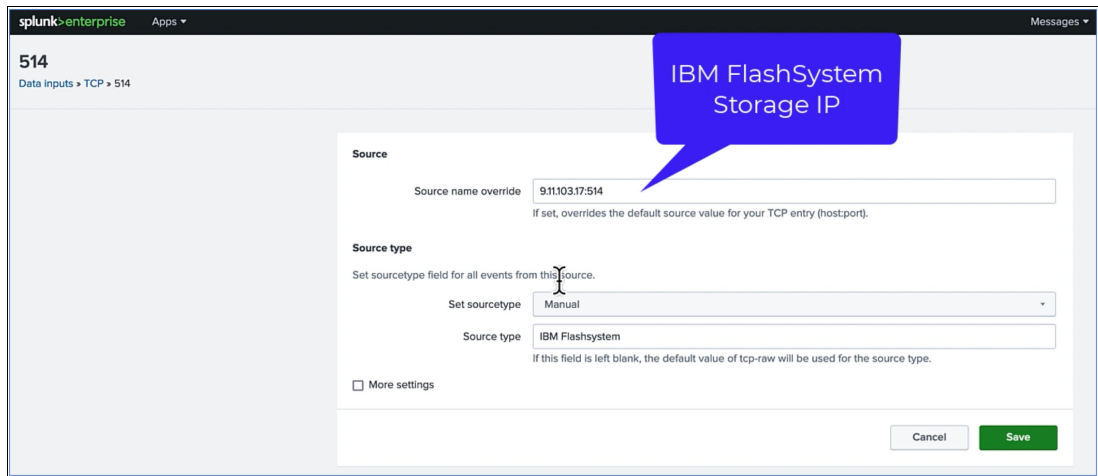


Figure 5 Adding a data source

5. Add another data source as local event log collection and click **Save**, as shown in Figure 6.

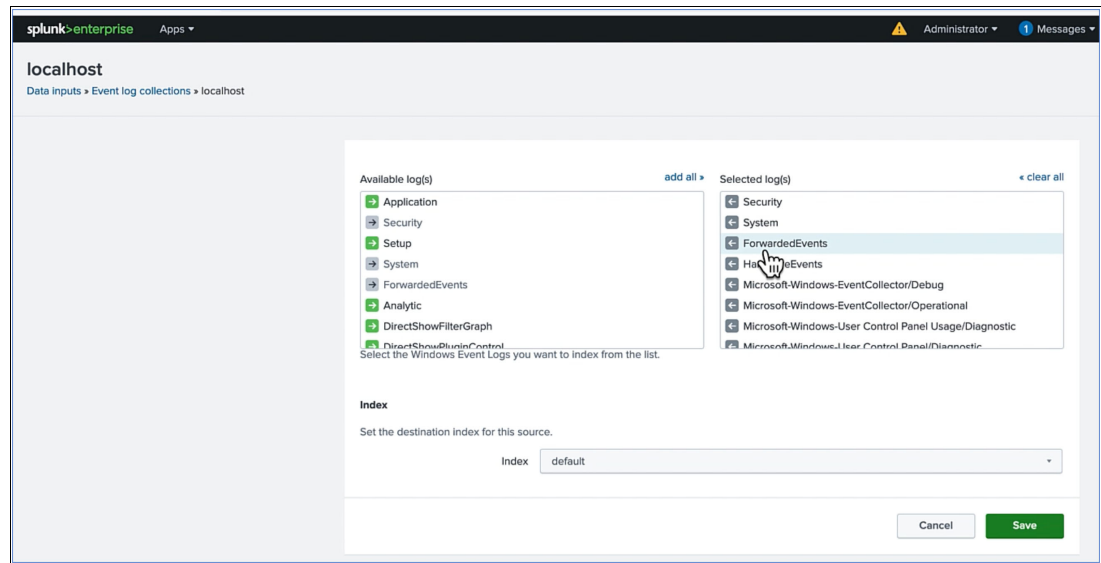


Figure 6 Data input settings

6. Go to the Forwarded inputs section and click **Windows Event Logs**, as shown in Figure 7.

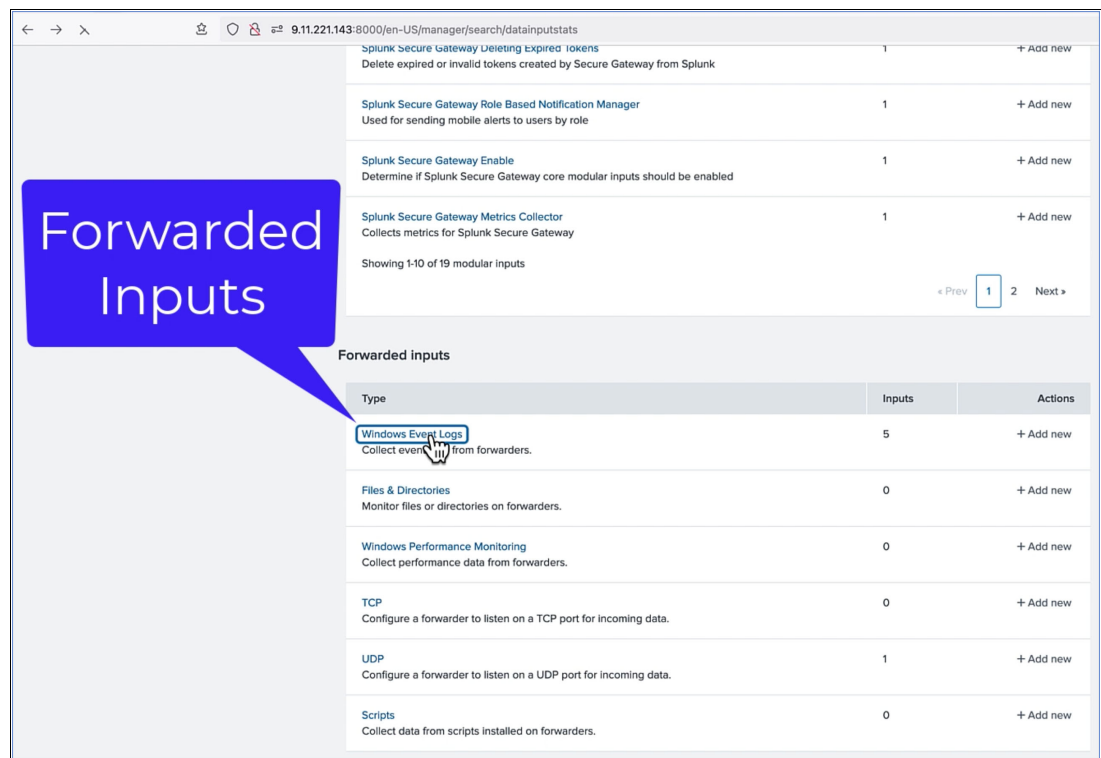


Figure 7 Windows Event Logs

7. Log in to the Microsoft SQL server and generate the log events for a failed login for a user so that the events can be configured as saved alerts in Splunk Enterprise, as shown in Figure 8 on page 11.

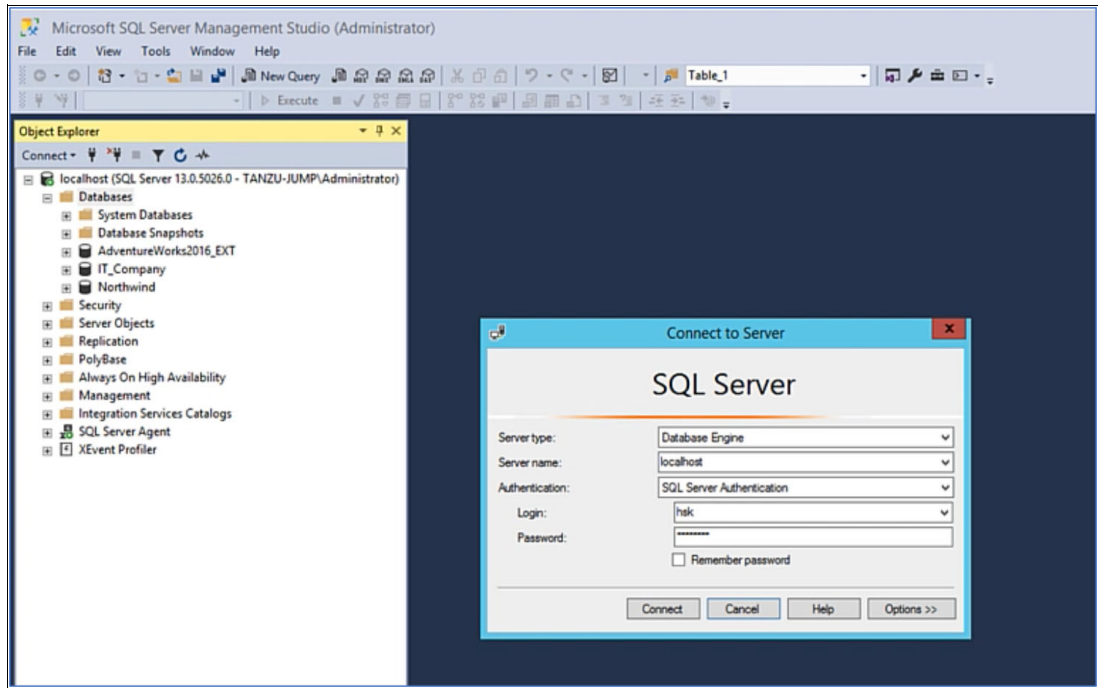


Figure 8 Microsoft SQL login for user

8. Add the search string as “failed login MSSQLSERVER” and search for these events. The search results display events for failed logins, as shown in Figure 9.

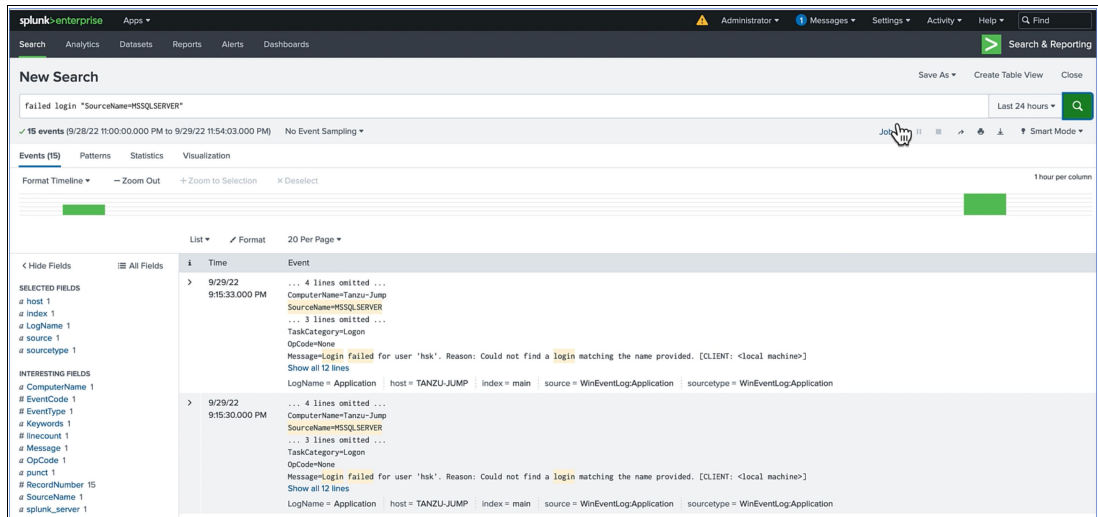


Figure 9 Failed login events for user

9. Select the event and click **Save As Alert**, as shown in Figure 10.

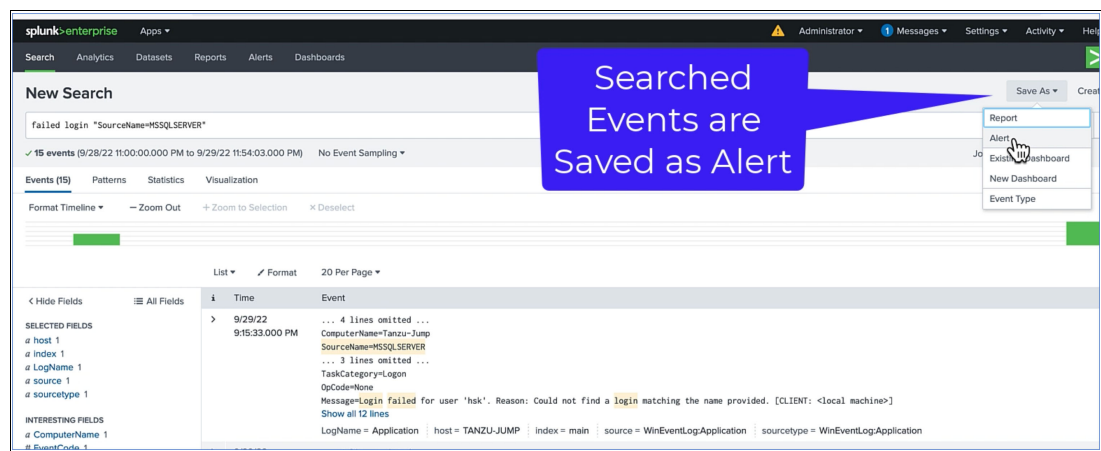


Figure 10 Search events are Saved As Alert

10.Add the description of the alert, alert type, and expiration in Settings. Add the trigger conditions and trigger actions and click **Save**, as shown in Figure 11.

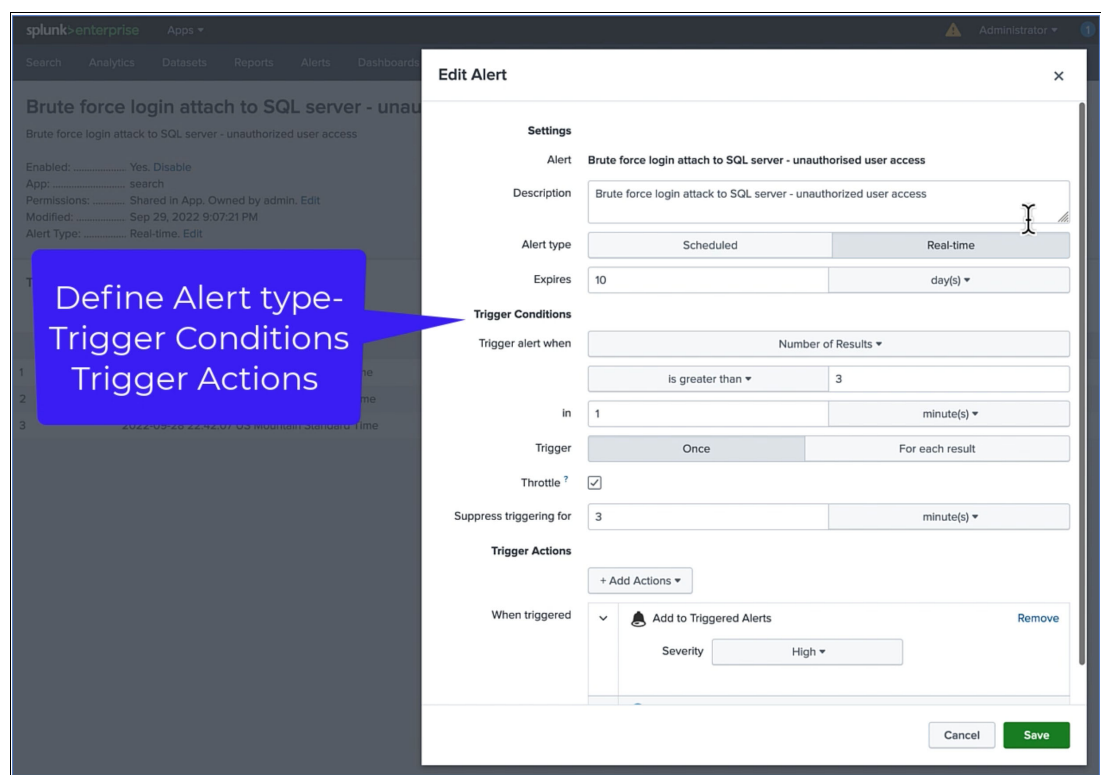


Figure 11 Configuring an alert

11.To a trigger action, go to the Trigger Actions section, click **Add Actions**, and select the relevant action from the drop-down menu, as shown in Figure 12 on page 13. In this example, we select **Scripted Custom Alert Action**, as shown in Figure 13 on page 13.

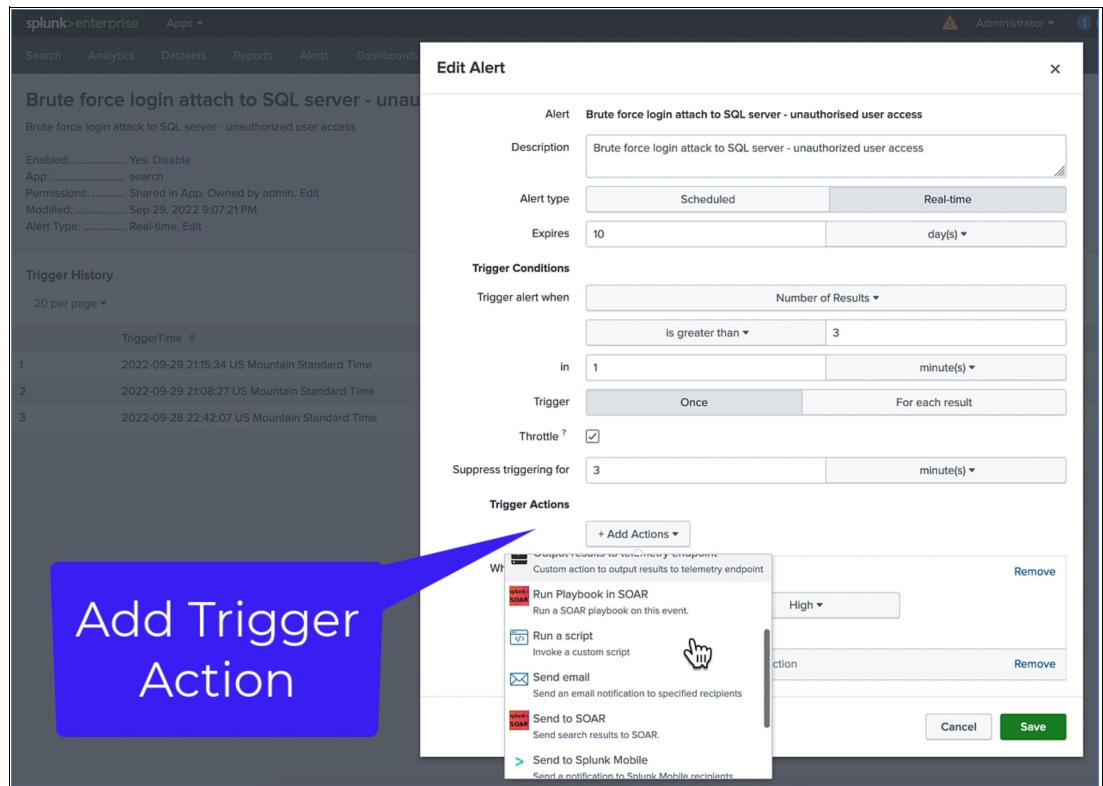


Figure 12 Adding trigger actions

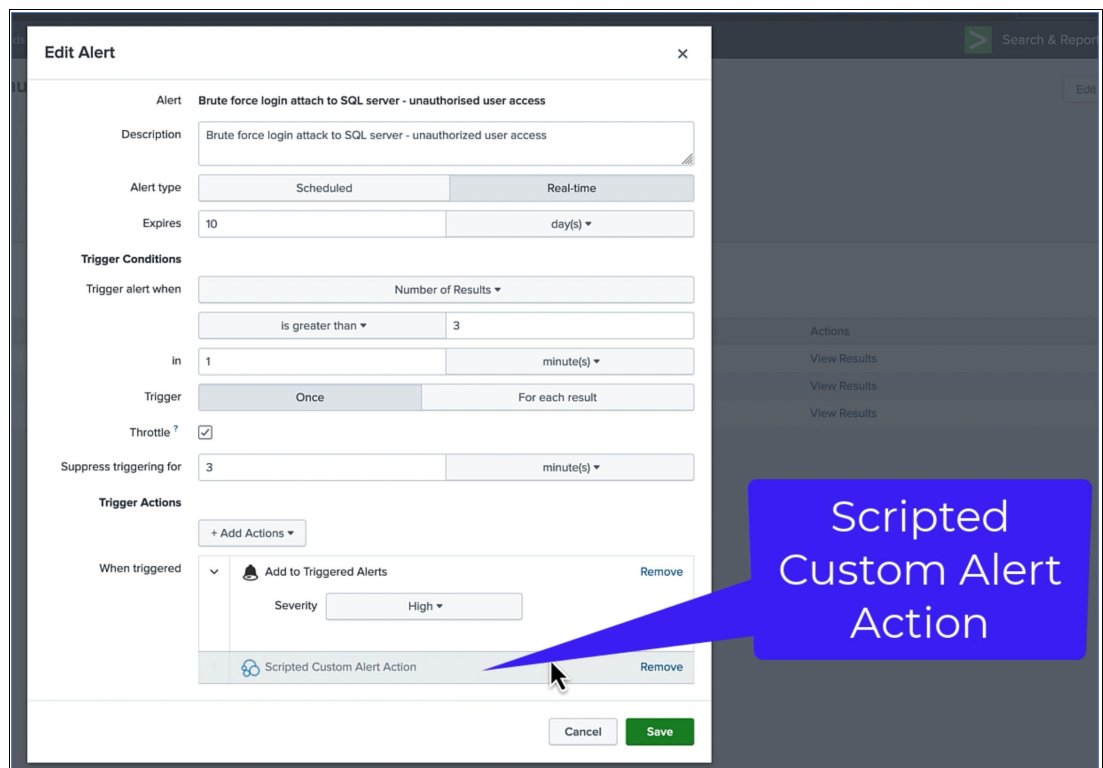


Figure 13 Adding a Scripted Custom Alert Action

12. Click **Manage Apps**, and then click **Create app** to create an app for the custom alert action, as shown in Figure 14. You must create this app first so that it is visible and can be selected in the **Add Actions** drop-down menu that is shown in Figure 13 on page 13.

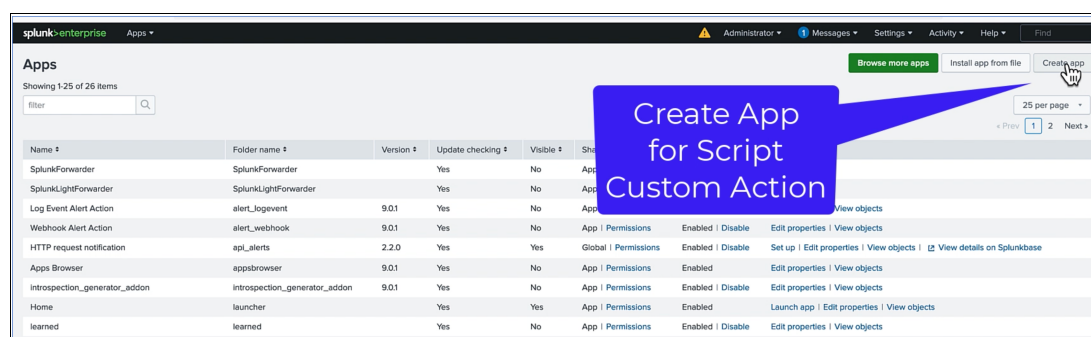


Figure 14 Creating an app for a custom alert action (1 of 2)

13. Create an app and complete the fields that are shown in Figure 15. Select a template and click **Save**, as shown in Figure 15.

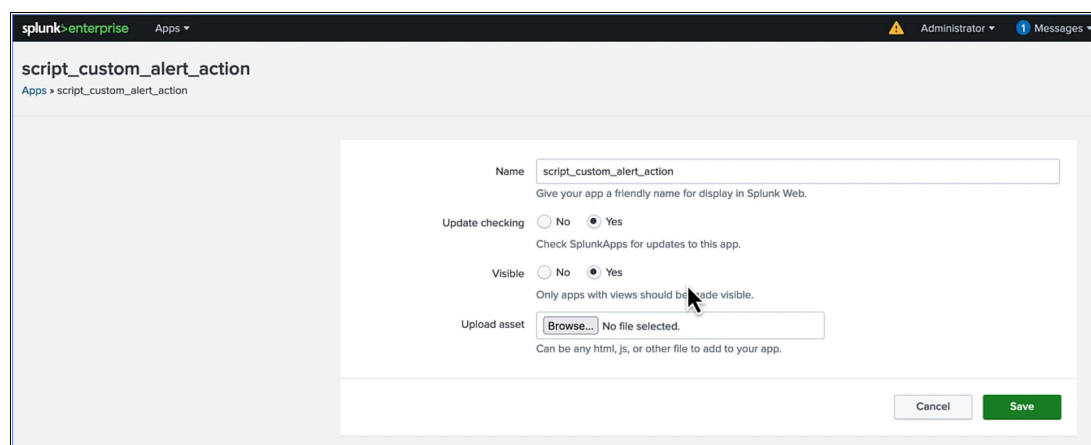


Figure 15 Creating an app for a custom alert action (2 of 2)

14. Click the **Apps** menu, and from the drop-down menu, click **Manage apps** and select the newly created app (script_custom_alert_action) from the list of apps. Click **Edit properties**, as shown in Figure 16.

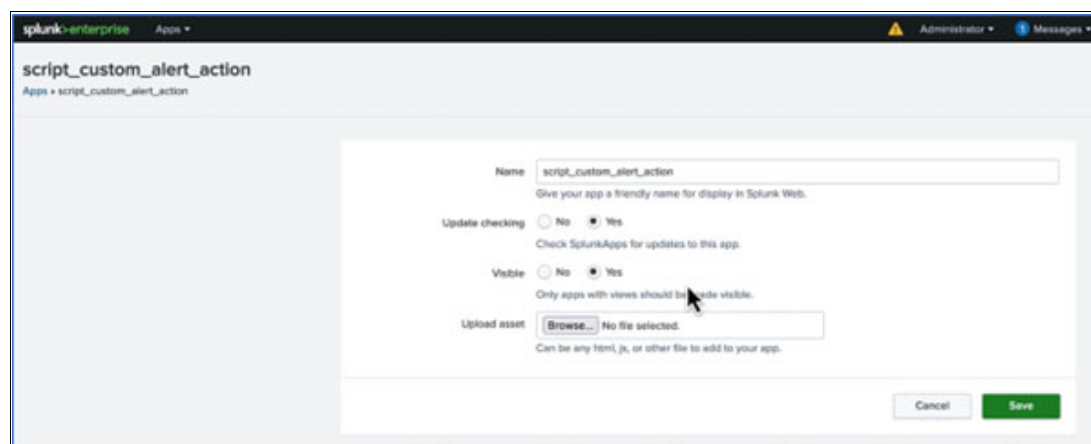


Figure 16 Editing properties for the script custom alert action app

15. Click the **Apps** menu, and from the drop-down menu, click **Manage apps** and select the newly created app (script_custom_alert_action) from the list of apps. Click **Permissions**, as shown in Figure 17.

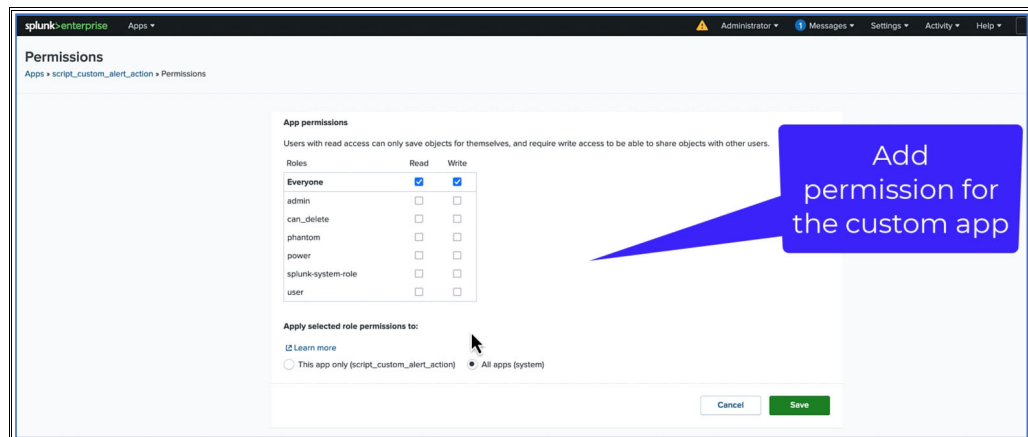


Figure 17 Adding permissions for the script custom alert action app

16. Click **Settings**, and from the drop-down menu, click **Alert Actions**. Go to the newly created app (script_custom_alert_action) and click **Permissions** to edit the permissions, as shown in Figure 18.

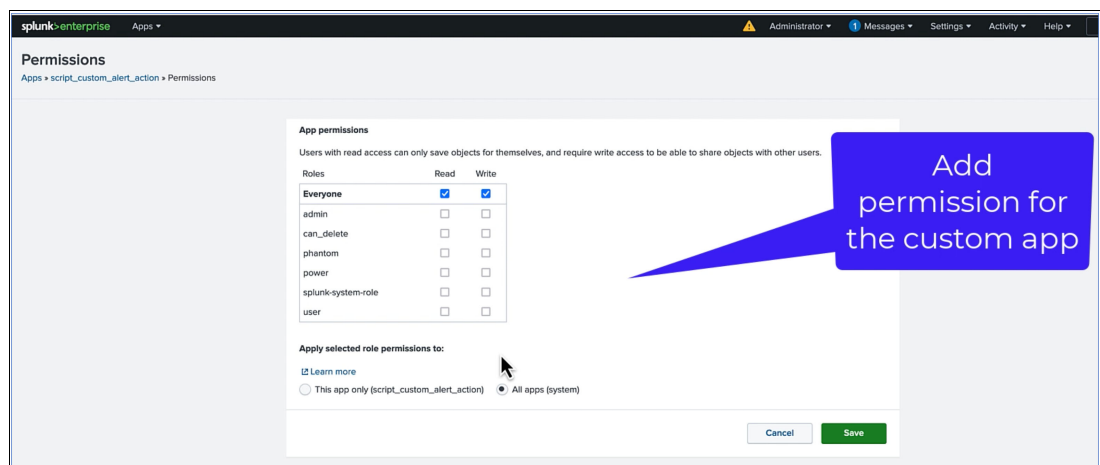


Figure 18 Adding permissions to the custom app

17. Select the new app from the **Apps** menu and add permissions, as shown in Figure 19.

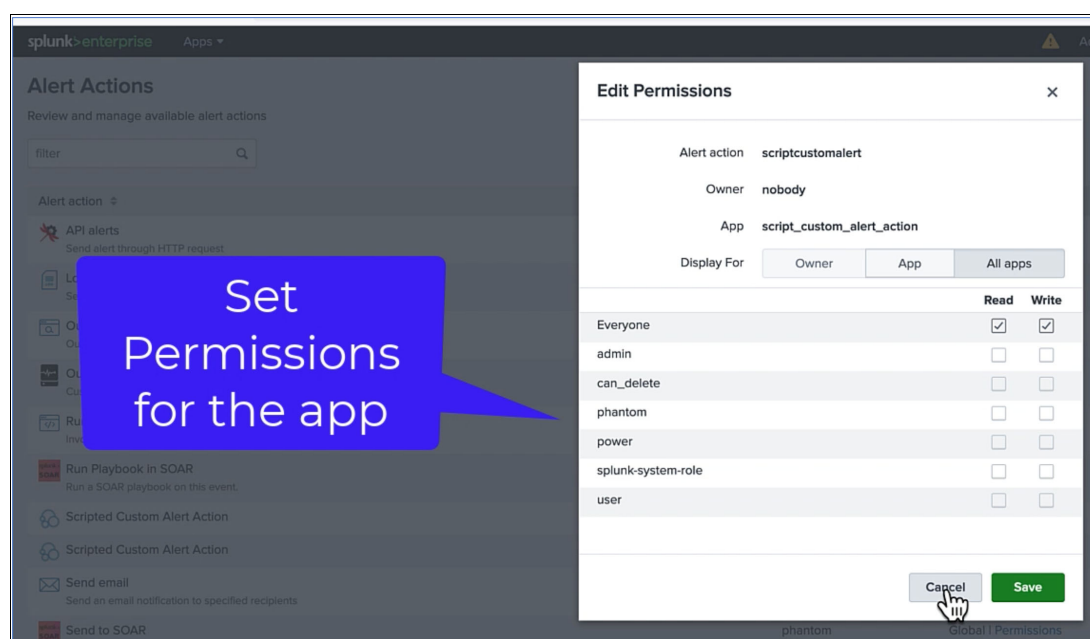


Figure 19 Adding permissions to the custom app (2 of 2)

Step 2: Creating custom app config files in the Splunk Enterprise server

Log in to the Windows server where Splunk Enterprise is installed and go to the `C:\Program Files\Splunk\etc\apps\scripts_custom_alert_action` directory. In that directory, create files for the custom alert action app. `Script_custom_alert_action` is the name of the app that we created for custom alert actions. For more information, see [Using custom alert actions](#).

Figure 20 on page 17 - Figure 27 on page 21 show the details for configuring the custom alert action app files.

Figure 20 and Figure 21 show the app directory structure and app components.

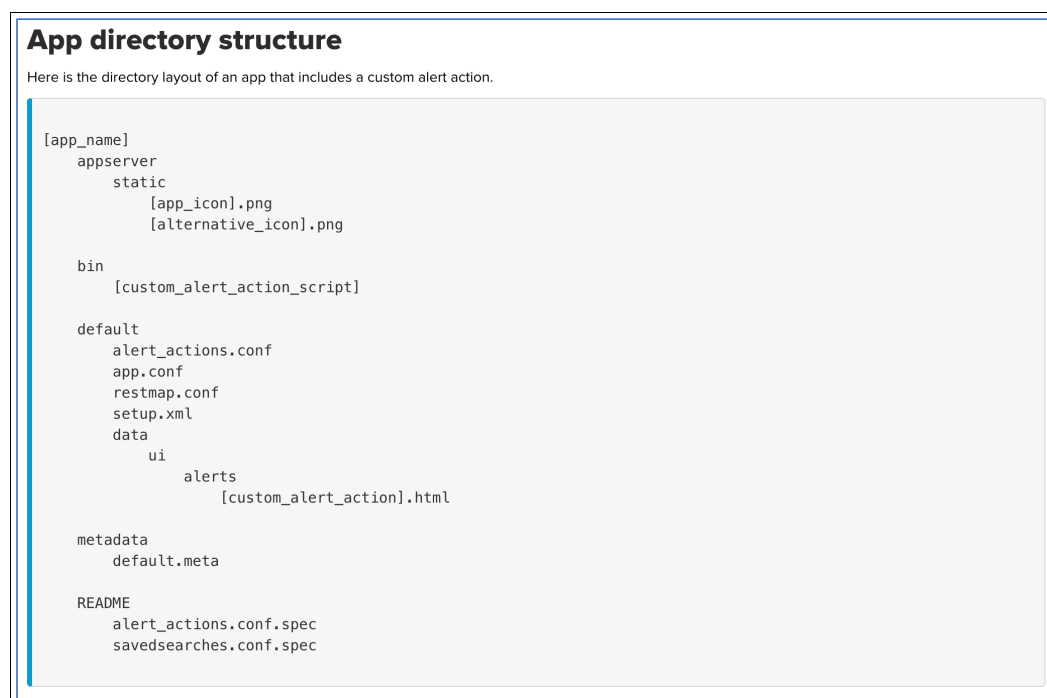


Figure 20 App directory structure for reference

App components			
This app directory has the following components.			
Component	File	Description	Required?
Logic	[custom_alert_action_script]	Alert action script or executable file	Yes
User interface	[custom_alert_action].html	HTML file defining the user interface for alert configuration	Yes
Alert action configuration	alert_actions.conf	Registers the custom alert action	Yes
Spec files	alert_actions.conf.spec	Declares alert action parameters	Optional
	savedsearches.conf.spec	Declares alert action parameters configured in the local savedsearches.conf file for the Splunk platform instance.	Optional
App configuration	app.conf	Defines app package and UI information	Yes
Icons	[app_icon].png	One or more icon image file(s)	Optional
Setup	setup.xml	Defines a UI for populating global settings at setup time	Optional
Validation	restmap.conf	Defines validation for parameters declared in savedsearches.conf	Optional
Access control metadata	default.meta	Defines alert action permission and scope	Optional

Figure 21 App components

The configurations files that are shown in Figure 22 - Figure 27 on page 21 are created for a custom alert action by using the App directory structure and App components that are shown in Figure 20 on page 17 and Figure 21 on page 17.

Figure 22 shows the alert configuration script or executable file.

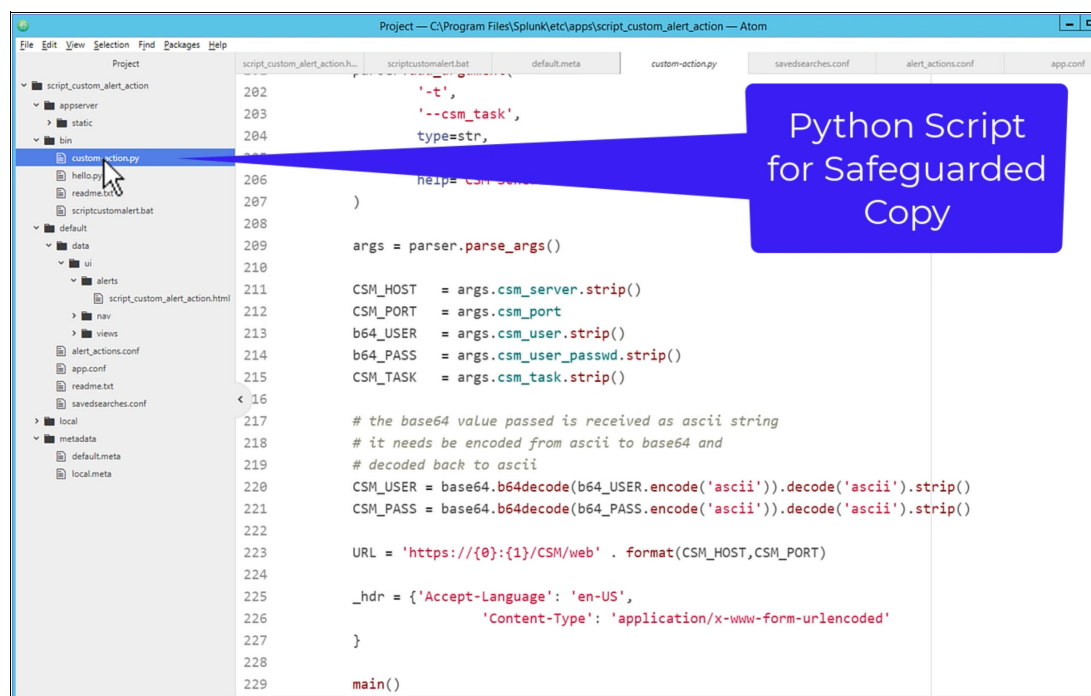


Figure 22 Python script for Safeguarded Copy

Figure 23 shows the Python script location on the GitHub site.

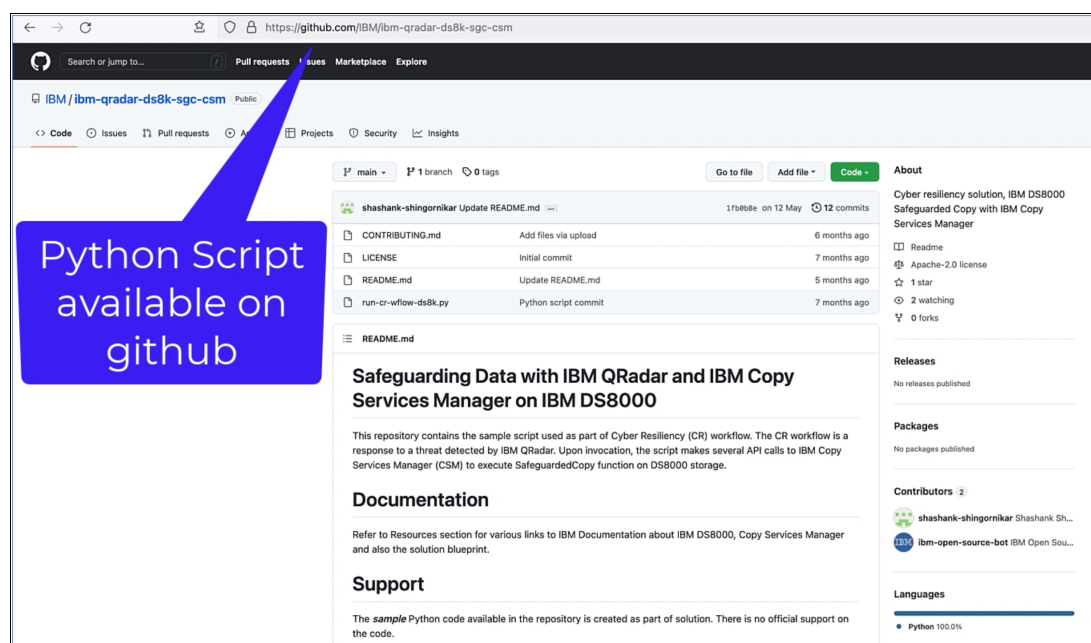


Figure 23 GitHub location for the Python script

Figure 24 on page 19 shows the alert action script or executable file.

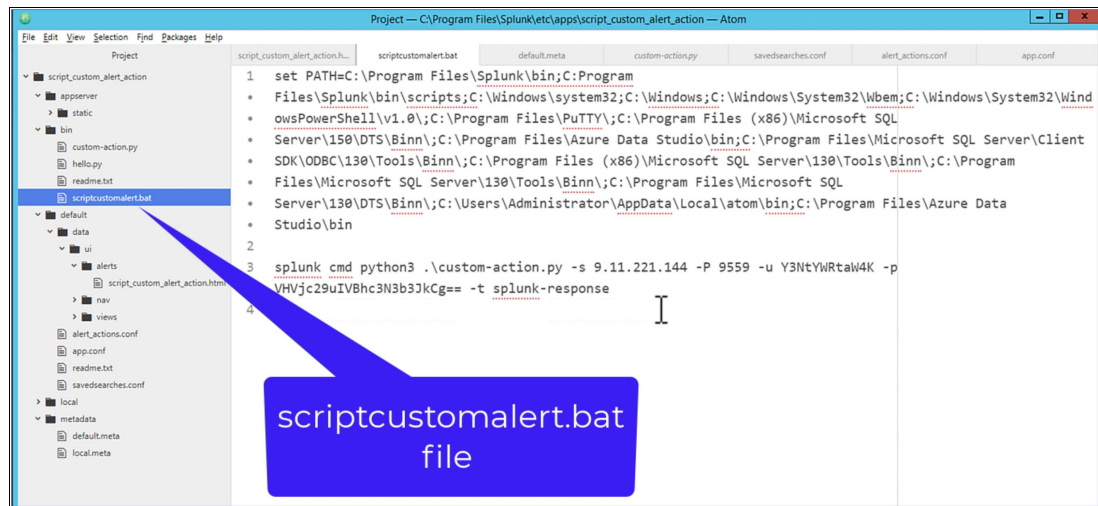


Figure 24 Files for custom alert actions (1 of 4)

Figure 25 shows the alert action configuration files.

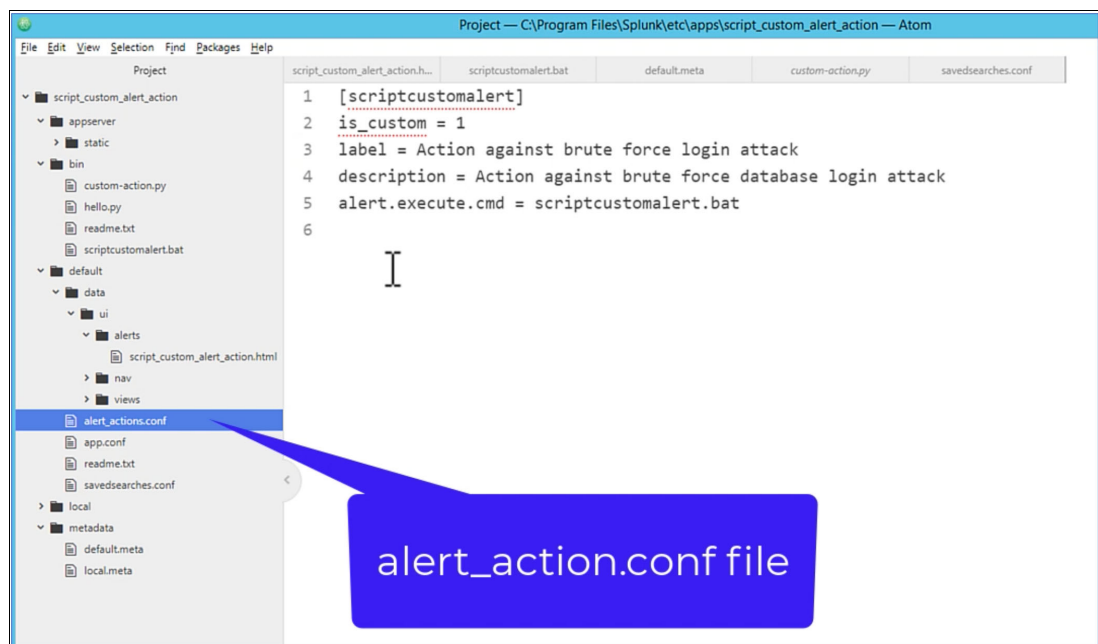


Figure 25 Files for custom alert actions (2 of 4)

Figure 26 defines the app package and UI information.

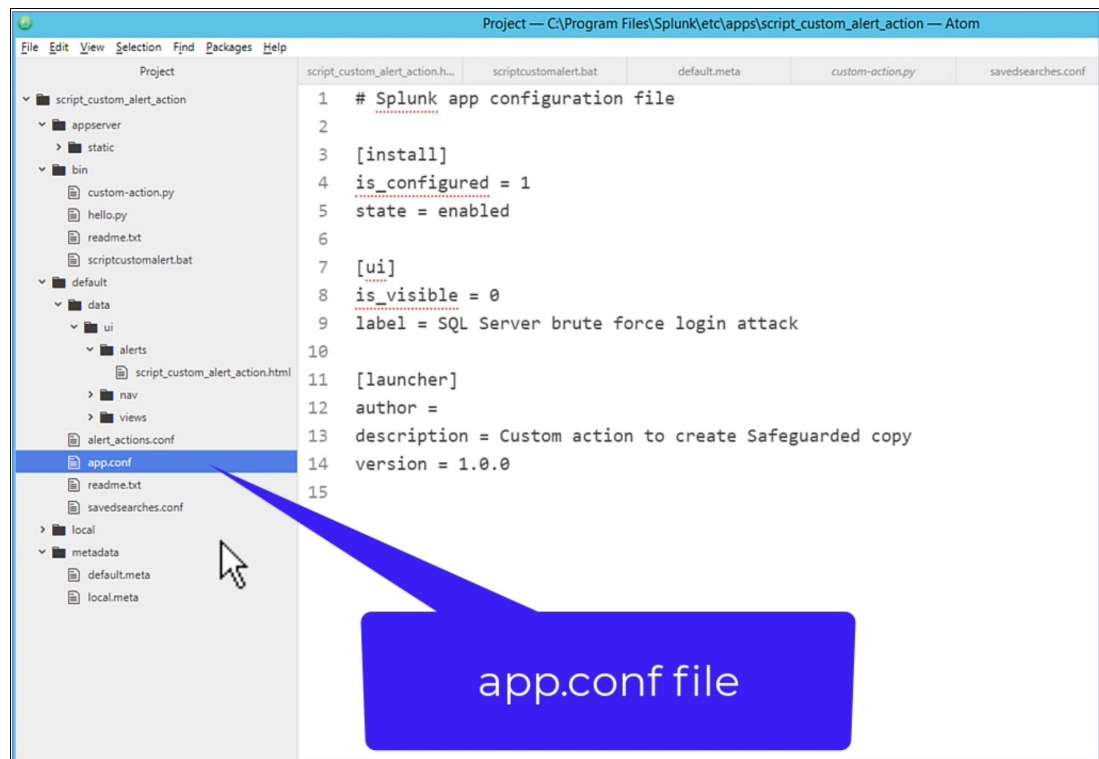


Figure 26 Files for custom alert actions (3 of 4)

Figure 27 declares the alert action parameters that are configured in the local `savedsearches.conf` file for the Splunk platform instance.

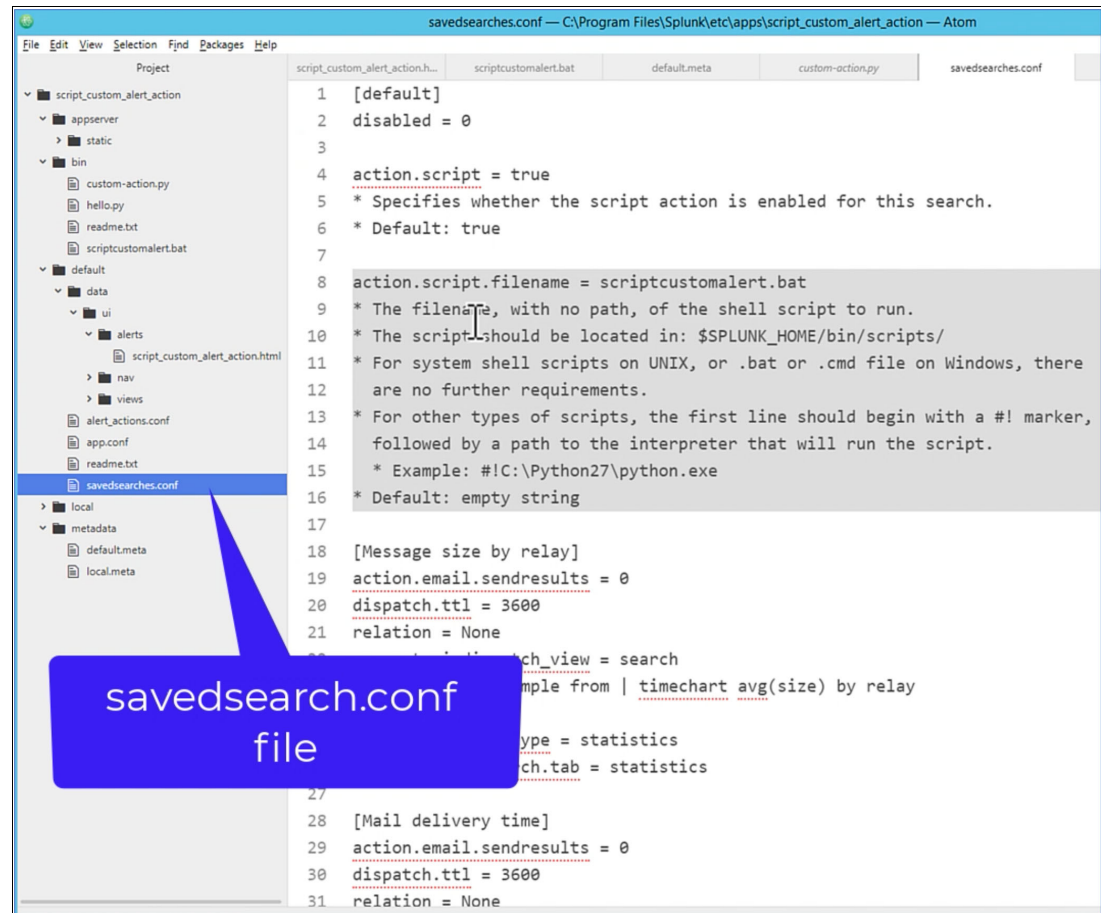


Figure 27 Files for custom alert actions (4 of 4)

Step 3: Configuring IBM Copy Services Manager

To configure IBM Copy Services Manager, complete the following steps:

1. Log in to IBM CSM and discover or create a session and schedule tasks, as shown in Figure 28 and Figure 29 on page 23. For more information about how to create a session, see [Creating volume groups and assigning source volumes](#).

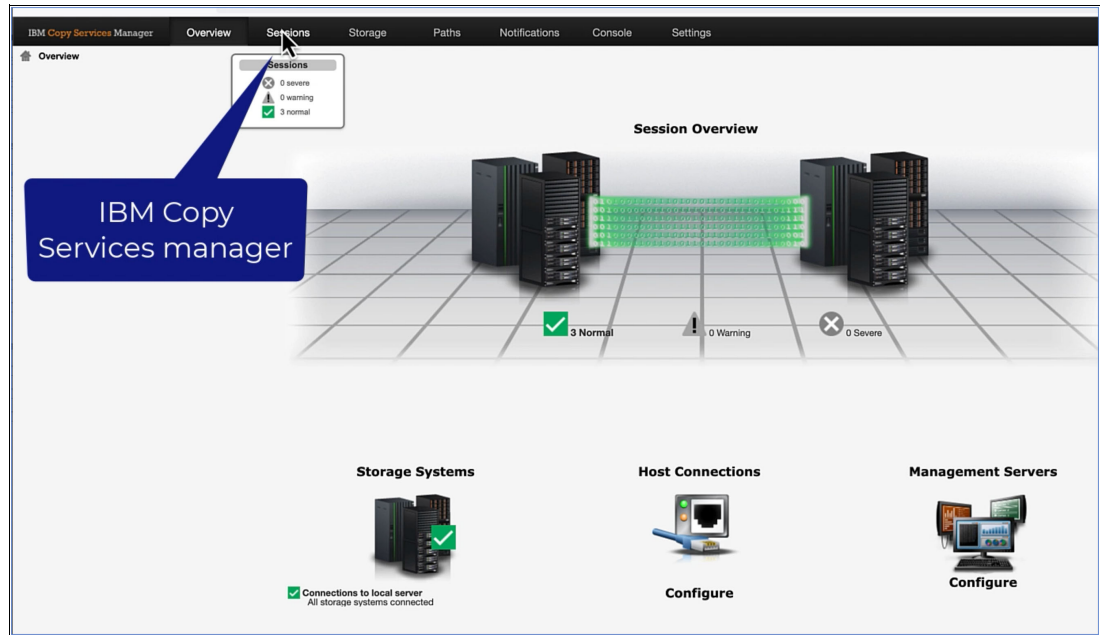


Figure 28 IBM CSM session

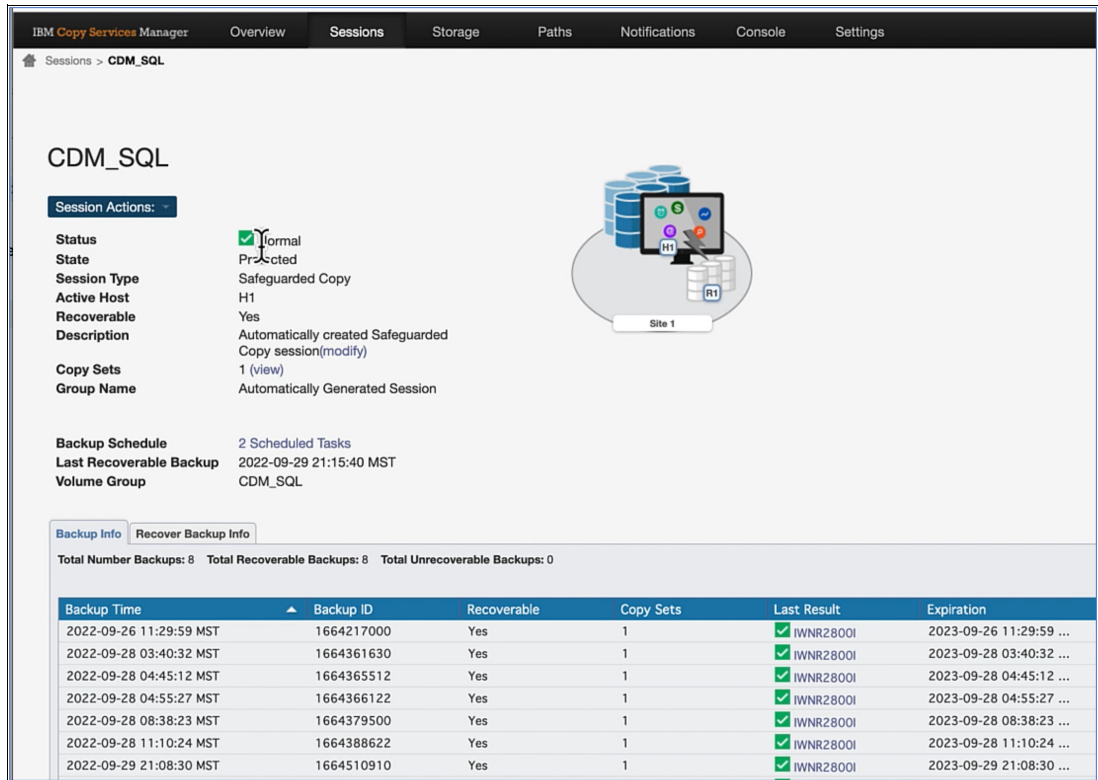


Figure 29 Session action

2. Create a schedule task in CMS, as shown in Figure 30. This schedule task is called by the Python script that is shown in Figure 22 on page 18. For more information about the Python script documentation and prerequisites, see [GitHub](#).

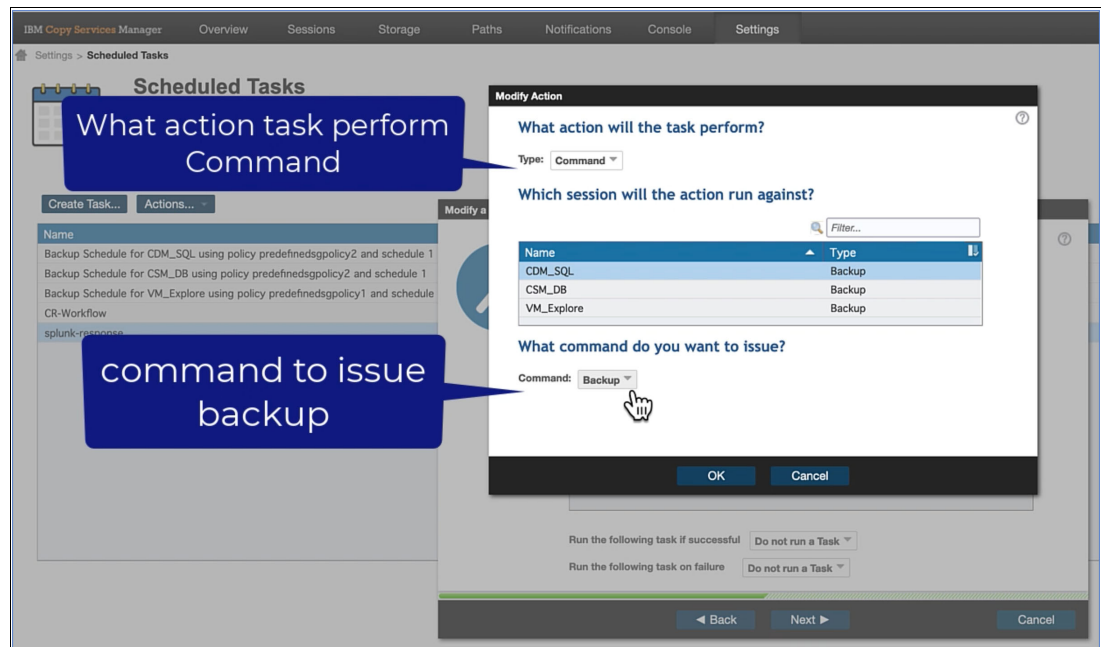


Figure 30 Schedule task details

splunk-response is the schedule task that is created with the affected session, as shown in Figure 31.

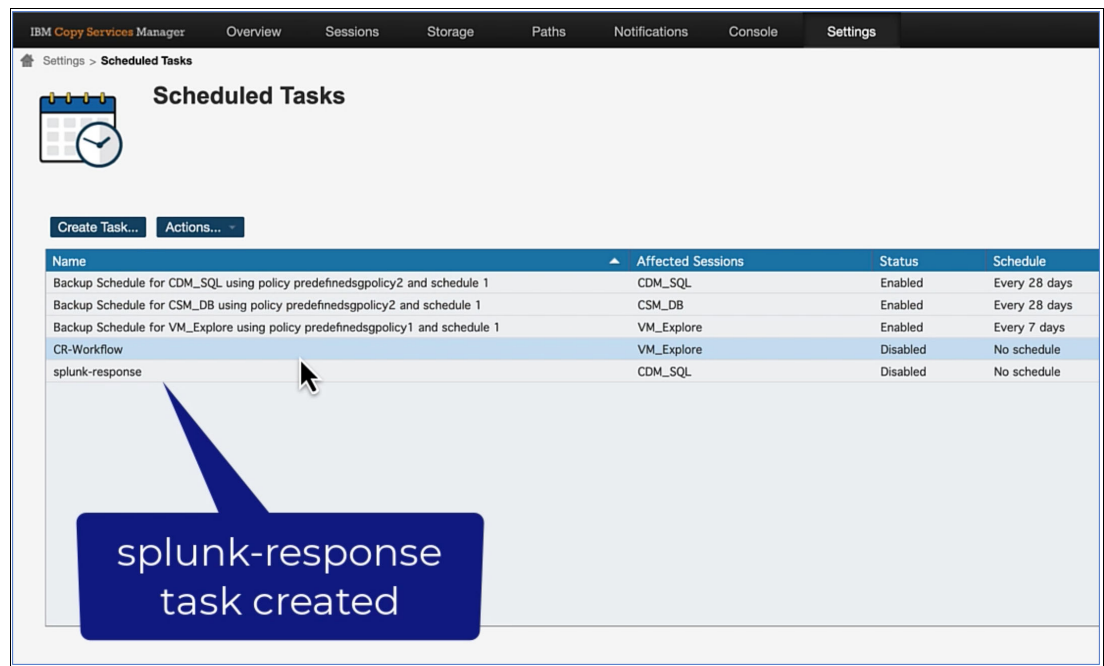


Figure 31 Created schedule task

Step 4: Configuring IBM FlashSystem Storage for Safeguarded Copy

To configure the IBM FlashSystem Storage for Safeguarded Copy, complete the following steps:

1. Log in to the IBM FlashSystem Storage, as shown in Figure 32.

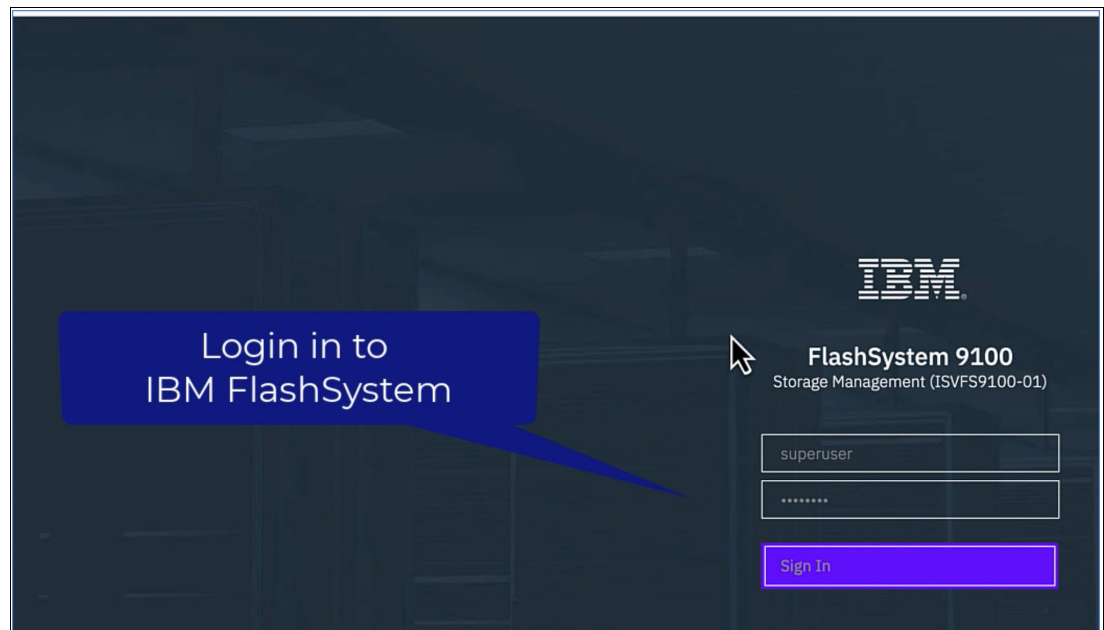


Figure 32 IBM FlashSystem Storage login

2. Create the Safeguarded pool and policy, as shown in Figure 33. For more information, see [Safeguarded Copy function](#).

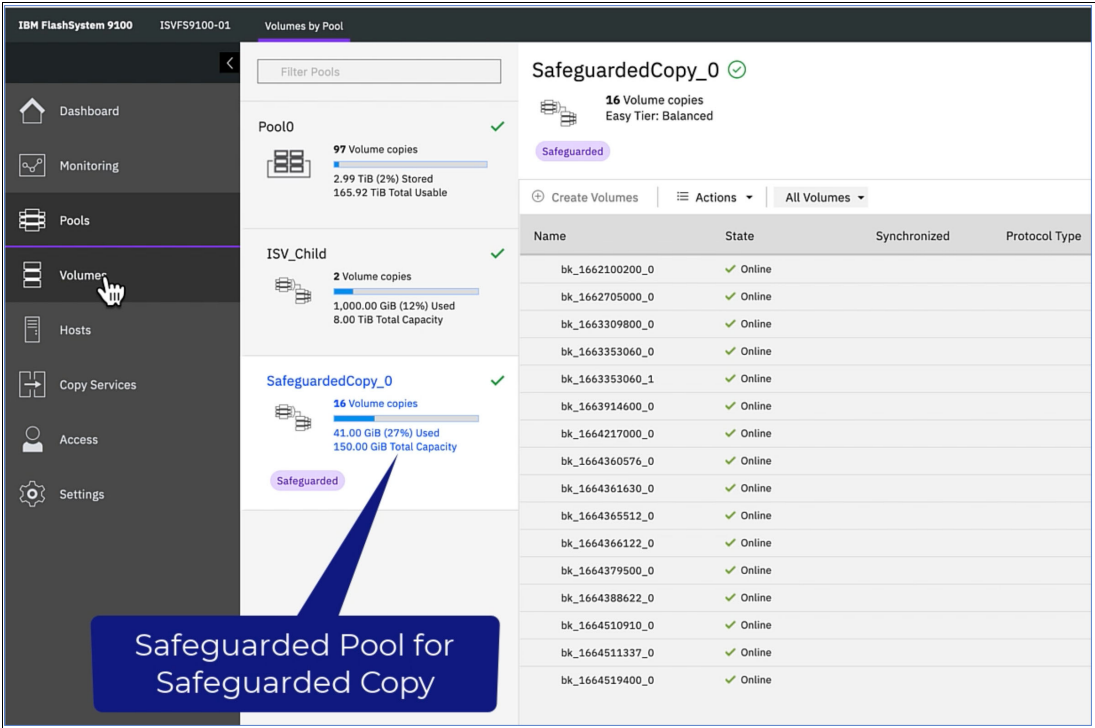


Figure 33 Safeguarded Copy pool

Figure 34 shows the storage volume that is mapped to the SQL server. The Safeguarded Copy is created for this storage volume.

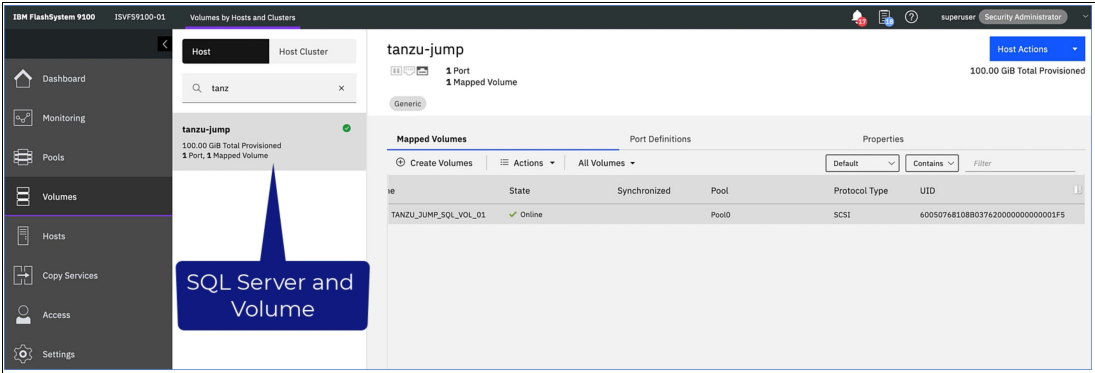


Figure 34 Volume that is mapped to the SQL server

Figure 35 shows the volume group for the storage volume that is mapped to the SQL server. The Safeguarded Copy is created for this storage volume.

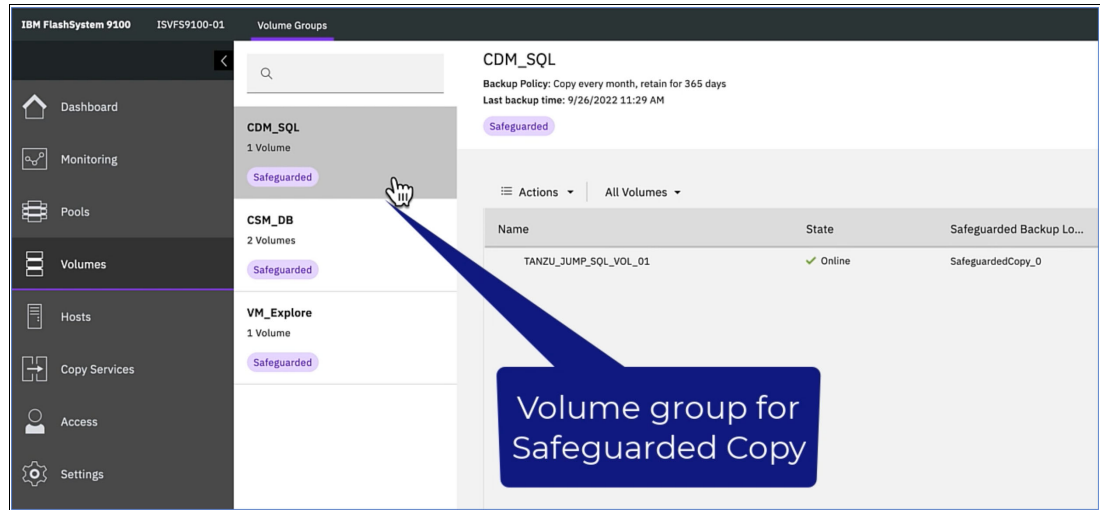


Figure 35 Volume group

- Figure 36 shows the syslog configuration of IBM FlashSystem Storage. To forward the storage logs to Splunk Enterprise, configure syslog forwarding (9.11.221.143 is the Splunk Enterprise IP address) for control path monitoring and threat detection.

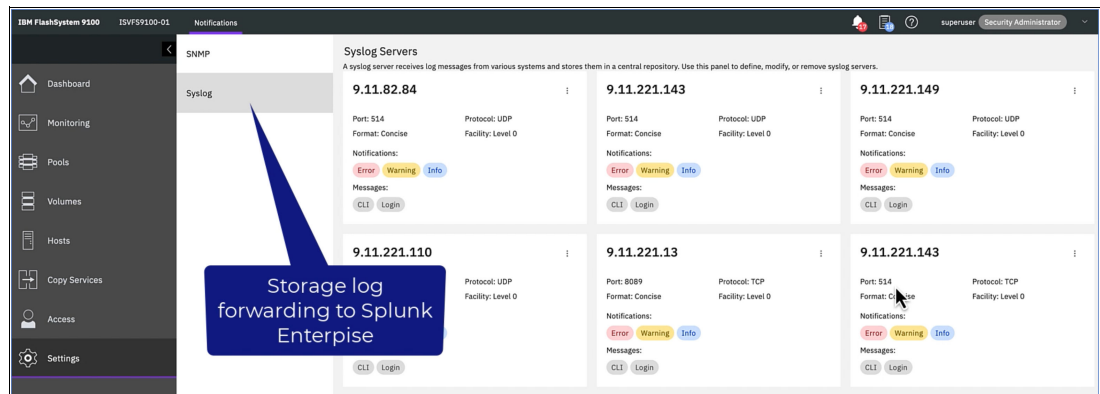


Figure 36 Syslog log forwarding

Step 5: IBM FlashSystem Storage LUN that is mapped to a Windows server for a Microsoft SQL DB

Figure 37 shows an IBM FlashSystem Storage LUN that is mapped to an SQL server. For more information about host and volume mappings, see [Host mapping](#).

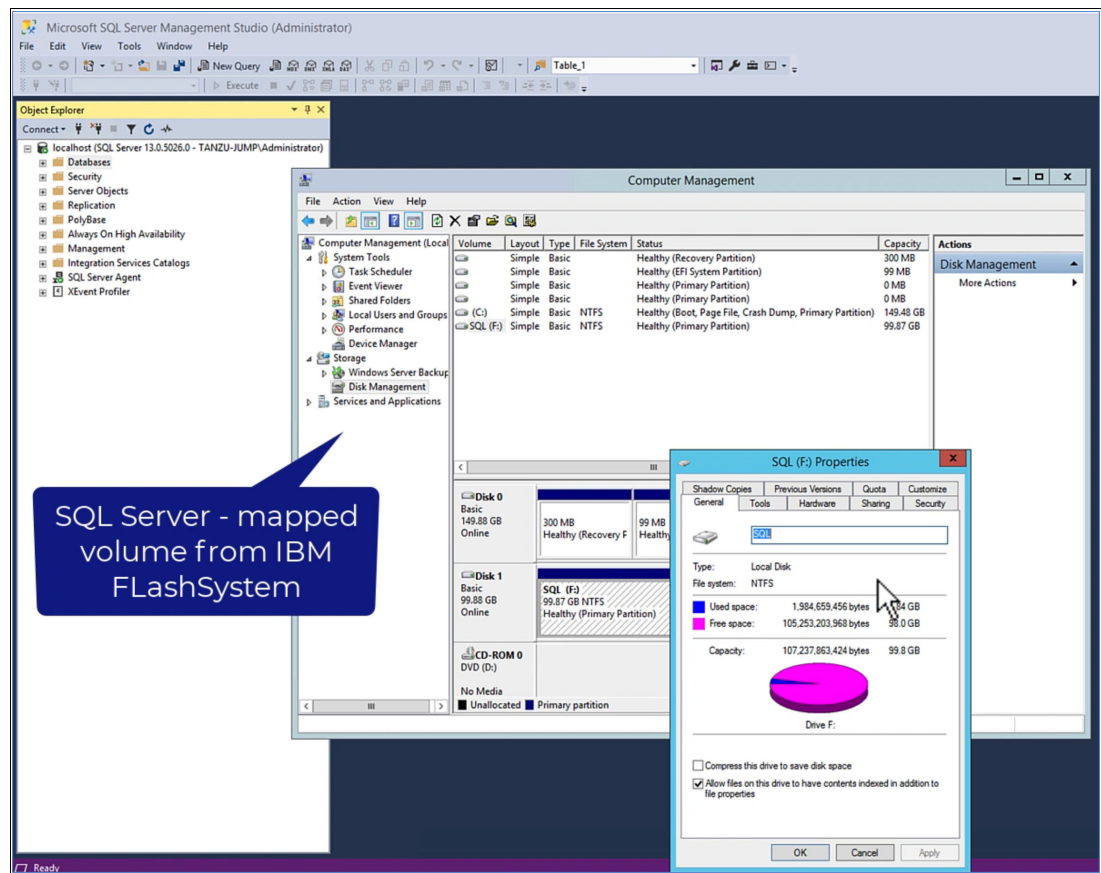


Figure 37 Storage LUN is mapped to the SQL server

Step 6: Use case for a brute force login attack on a Microsoft SQL server

Figure 38 shows the IBM CSM window and a Microsoft SQL server DB login action by a user who does not have access to the specified DB. This figure shows a simulation of a brute force login attack on the DB, where the user is trying to access the DB by using multiple login attempts. An alert and the SQL server logs are generated, and these logs are forwarded to Splunk Enterprise. Based on the logs and multiple login attempts by the user, the alert criteria is matched on the Splunk Enterprise. Based on the saved alerts definitions, the custom alert action is triggered to create a Safeguarded Copy in IBM FlashSystem Storage.

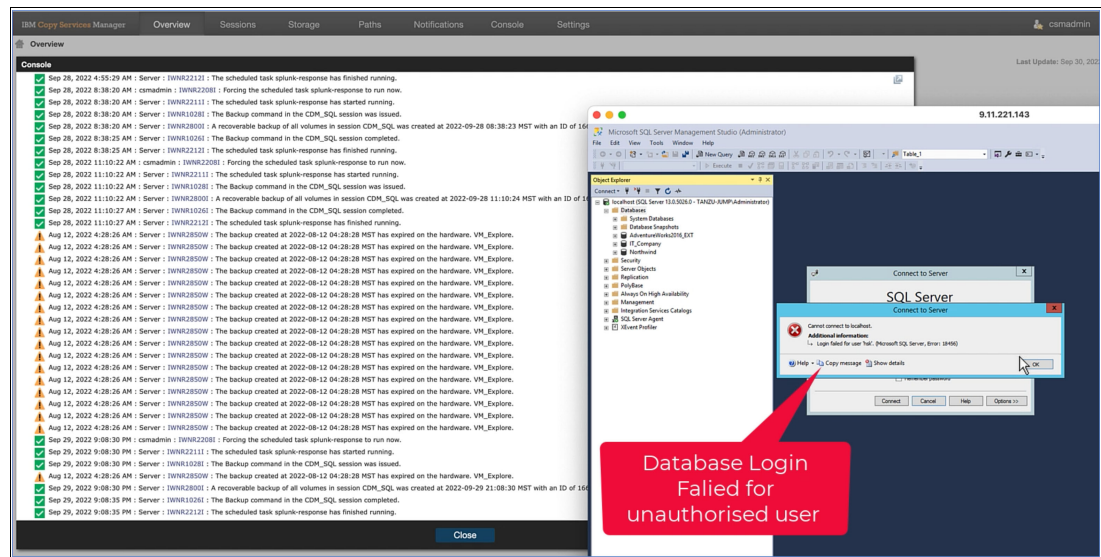


Figure 38 Brute force login attack simulation

With the automated response and configuration that is done by IBM CSM, the Safeguarded Copy is created in IBM FlashSystem Storage, as shown in Figure 39.

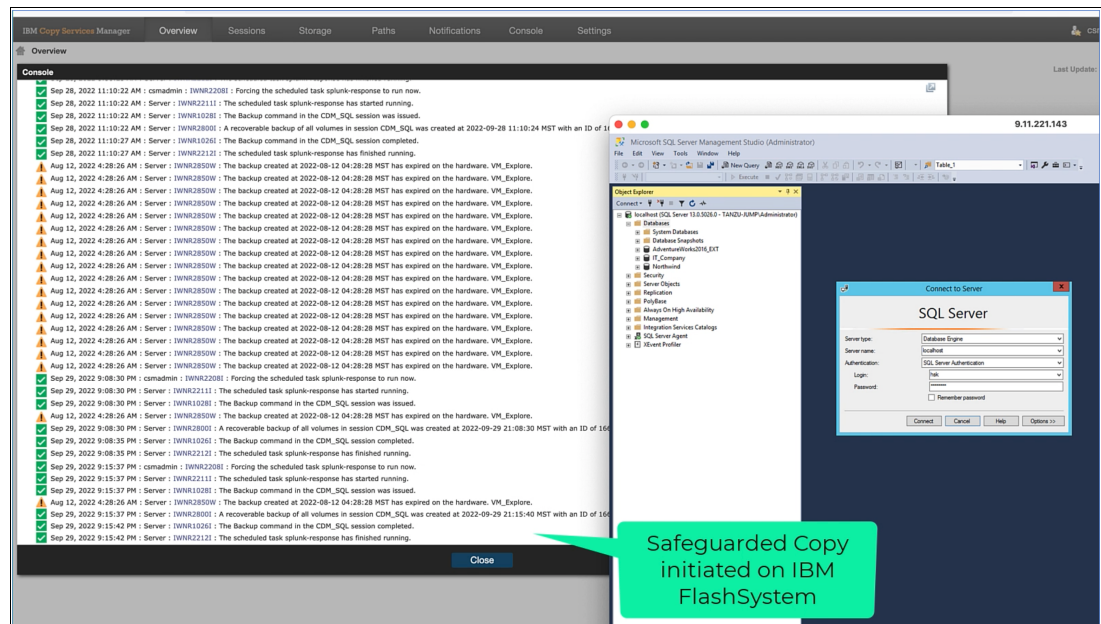
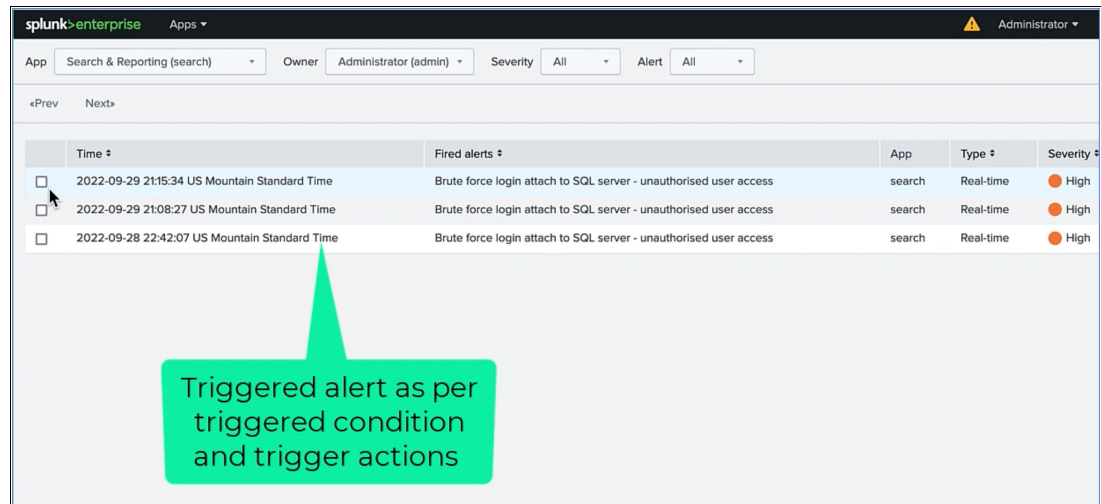


Figure 39 Safeguarded Copy created during a brute force login attack event

Step 7: Validating Safeguarded Copy creation on IBM FlashSystem Storage

Validate the Safeguarded Copy that is created in IBM FlashSystem Storage by completing the following steps:

1. Log in to Splunk Enterprise and check the triggered alerts during the period when the threat was detected. Figure 40 shows the triggered alert that was defined in the trigger conditions.

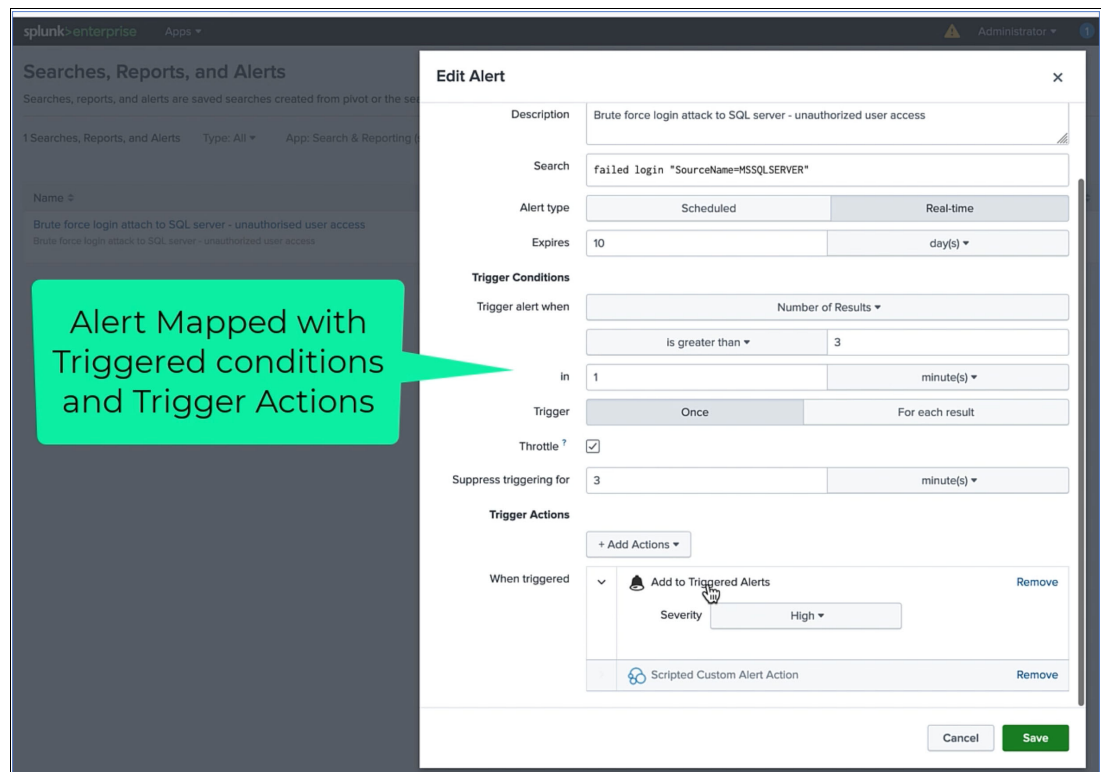


	Time	Fired alerts	App	Type	Severity
<input type="checkbox"/>	2022-09-29 21:15:34 US Mountain Standard Time	Brute force login attack to SQL server - unauthorised user access	search	Real-time	High
<input type="checkbox"/>	2022-09-29 21:08:27 US Mountain Standard Time	Brute force login attack to SQL server - unauthorised user access	search	Real-time	High
<input type="checkbox"/>	2022-09-28 22:42:07 US Mountain Standard Time	Brute force login attack to SQL server - unauthorised user access	search	Real-time	High

Triggered alert as per triggered condition and trigger actions

Figure 40 Triggered alerts

Figure 41 shows the alerts that are mapped with triggered conditions, and the trigger actions.



Edit Alert

Description: Brute force login attack to SQL server - unauthorized user access

Search: failed login "SourceName=MSSQLSERVER"

Alert type: ☐ Scheduled ☒ Real-time

Expires: 10 day(s)

Trigger Conditions

Trigger alert when: Number of Results

Is greater than: 3

in: 1 minute(s)

Trigger: ☐ Once ☒ For each result

Throttle: ☒

Suppress triggering for: 3 minute(s)

Trigger Actions

+ Add Actions

When triggered:

- ☒ Add to Triggered Alerts (Severity: High)
- ☐ Scripted Custom Alert Action

Buttons: Cancel, Save

Alert Mapped with Triggered conditions and Trigger Actions

Figure 41 Alert mapped with triggered actions

2. Safeguarded Copy creates a copy in IBM FlashSystem Storage, as shown in Figure 42.

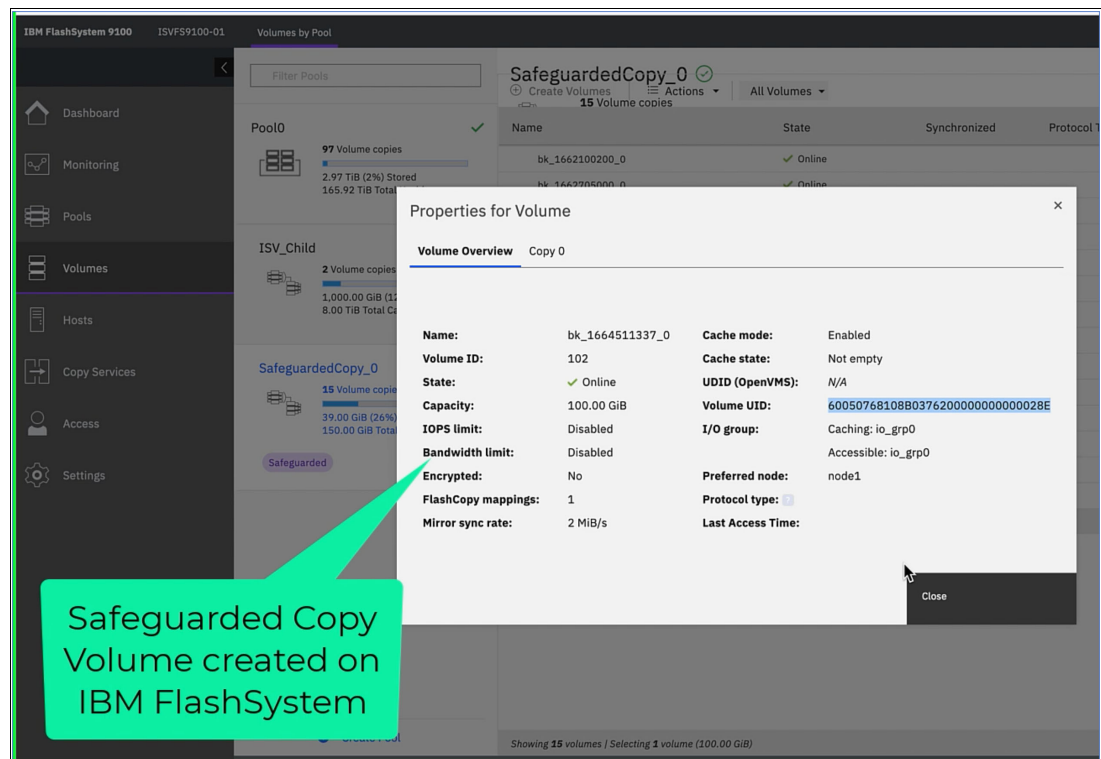


Figure 42 Safeguarded Copy was created during the brute force login attack event

Summary

The focus of this document is to highlight early threat detection by using Splunk Enterprise and proactively start a cyber resilience workflow in response to a cyberattack or malicious user action. The workflow uses IBM CSM as orchestration software to invoke the IBM FlashSystem Storage Safeguarded Copy function, which creates an immutable copy of the data in an air-gapped form on the same IBM FlashSystem Storage for isolation and eventual quick recovery.

This document explains the steps that are required to enable and forward IBM FlashSystem audit logs and set a Splunk forwarder configuration to forward local event logs to Splunk Enterprise. This document also describes how to create various alerts in Splunk Enterprise to determine a threat, and configure and invoke an appropriate response to the detected threat in Splunk Enterprise. This document explains the lab setup configuration steps that are involved in configuring various components like Splunk Enterprise, Splunk Enterprise config files for custom apps, IBM CSM, and IBM FlashSystem Storage. The last steps in the lab setup section demonstrate the automated Safeguarded Copy creation and validation steps.

This document also describes brief steps for configuring various components and integrating them. This document demonstrates a use case for protecting a Microsoft SQL DB volume that is created on IBM FlashSystem Storage. When a threat is detected on the Microsoft SQL DB volume, Safeguarded Copy starts on an IBM FlashSystem Storage volume. The Safeguarded Copy creates an immutable copy of the data, and the same data volume can be recovered or restored by using IBM CSM.

Authors

This blueprint guide was produced by a team of specialists from around the world working at IBM Redbooks, Poughkeepsie Center.

Hemant Kantak is a Storage Solutions Architect who has been with IBM Systems, ISDL Lab Pune, India for 11 years. He designs and deploys storage and backup solutions, and virtualization and cloud technologies solutions across various platforms, such as AWS, IBM Cloud®, and Microsoft Azure. He also works on enabling hybrid cloud solutions by using Red Hat OpenShift Container Platform, IBM Cloud Pak®, and VMware Solutions and Tanzu. As an IBM Systems TechU speaker, he demonstrates solutions to IBM clients and sales teams. He also writes blueprints and IBM Redbooks® publications.

Shashank Shingornikar is a Storage Solutions Architect who has been with IBM Systems, ISDL Lab Pune, India for over 12 years. He has worked extensively with IBM Storage products, such as IBM Spectrum Virtualize, IBM FlashSystem, and IBM Spectrum Scale to build solutions that combine Oracle and Red Hat OpenShift features. He is working on demonstrating cyber resilience solutions with IBM QRadar® and IBM Storage Systems. Before joining IBM, Shashank worked in The Netherlands on various high availability, disaster recovery, cluster, and replication solutions for DB technologies, such as Oracle, Microsoft SQL, and MySQL.

Thanks to the following person for their contributions to this project:

Douglas O'Flaherty

Principal Storage Sales Manager, Alliances and Solutions, IBM Technology, Worldwide

Resources

- ▶ *Cyber Resiliency Solution using IBM Spectrum Virtualize*, REDP-5657
- ▶ *IBM FlashSystem Safeguarded Copy Implementation Guide*, REDP-5654
- ▶ *Securing Data on Threat Detection by Using IBM Spectrum Scale and IBM QRadar: An Enhanced Cyber Resiliency Solution*, REDP-5560
- ▶ About Splunk Enterprise - Splunk Documentation
<https://docs.splunk.com/Documentation/Splunk/9.0.2/Overview/AboutSplunkEnterprise>
- ▶ GitHub link to download the script
<http://github.ibm.com/IBM/cyber-resiliency-solutions/ibm-qradar-ds8k-sgc-with-csm>
- ▶ IBM Copy Services Manager
<http://www.ibm.com/docs/en/csm>
- ▶ *IBM Copy Services Manager User's Guide*
<http://ibm.com/support/pages/system/files/inline-files/sc27854220.pdf>
- ▶ Scheduled Tasks in Copy Services Manager
<http://ibm.com/docs/en/csm/6.3.1?topic=replication-creating-scheduled-tasks>

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.


Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at <http://www.ibm.com/legal/copytrade.shtml>

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

AIX®
FICON®
FlashCopy®
IBM®

IBM Cloud®
IBM Cloud Pak®
IBM FlashSystem®
IBM Spectrum®

QRadar®
Redbooks®
Redbooks (logo) ®
z/OS®

The following terms are trademarks of other companies:

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Red Hat, OpenShift, are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

VMware, and the VMware logo are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

Other company, product, or service names may be trademarks or service marks of others.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at <http://www.ibm.com/privacy> and IBM's Online Privacy Statement at <http://www.ibm.com/privacy/details> in the section entitled "Cookies, Web Beacons and Other Technologies," and the "IBM Software Products and Software-as-a-Service Privacy Statement" at <http://www.ibm.com/software/info/product-privacy>.



© Copyright IBM Corporation

December 2022

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule
Contract with IBM Corp.



Please recycle

ISBN 0738460974

REDP-5701-00