

IBM® Storage

Enhanced Cyber Resilience Threat Detection with IBM FlashSystem Safeguarded Copy and IBM QRadar

IBM

© Copyright International Business Machines Corporation 2021.

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

Contents

Introduction	1
Executive summary	2
Scope	3
Introduction	3
Safeguarded Copy feature	3
IBM QRadar	4
Prerequisites	4
Solution overview	5
Control path use cases	6
Data path use case	7
Lab setup	7
Custom log source	11
IBM QRadar sample rules	21
Custom actions	30
Summary	43
Author	44
Acknowledgments	44
Appendix A	45
QRadar deployment model availability	45
Resources	46
Notices	49
Trademarks	50
Terms and conditions for product documentation	51
Applicability	51
Commercial use	51
Rights	51
Privacy policy considerations	51



Introduction

The focus of this document is to demonstrate an early threat detection by using IBM® QRadar® and the Safeguarded Copy feature that is available as part of IBM FlashSystem® and IBM SAN Volume Controller. Such early detection protects and quickly recovers the data if a cyberattack occurs.

This document describes integrating IBM FlashSystem audit logs with IBM QRadar, and the configuration steps for IBM FlashSystem and IBM QRadar. It also explains how to use the IBM QRadar's device support module (DSM) editor to normalize events and assign IBM QRadar identifier (QID) map to the events.

Post IBM QRadar configuration, we review configuring Safeguarded Copy on the application volumes by using volume groups and applying Safeguarded backup policies on the volume group.

Finally, we demonstrate the use of orchestration software IBM Copy Services Manager to start a recovery, restore operations for data restoration on online volumes, and start a backup of data volumes.

Executive summary

The financial effect of cyberattacks continues to rise. Cyberattacks can occur 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, the data breaches involve internal threat actors.

Traditional approaches to data protection work well for their intended purposes, but are inadequate to protect against cyberattacks, which can encrypt or otherwise corrupt your data. Remote replication for disaster recovery replicates all changes (malicious or not) to the remote copy.

Also, data that stored on offline media or the cloud can take too long to recover a widespread attack. Large-scale recovery can take anywhere between days to weeks, which can lead to substantial downtime for businesses.

The new Safeguarded Copy function for IBM FlashSystem and IBM SAN Volume Controller is designed to help businesses recover quickly and safely from a cyberattack, which helps reduce recovery to minutes or hours.

Safeguarded Copy automatically creates efficient immutable snapshots according to a schedule. These snapshots are stored specifically by the system and cannot be connected to servers, which creates a logical “air gap” from malware or other threats. They also cannot be changed and or deleted, except according to a planned schedule, which helps protect against errors or actions that are committed by staff.

Detecting a threat before it starts can help speed recovery even more.

IBM Security™ QRadar is a Security Information and Event Management (SIEM) and threat management system that monitors activities and looks for signs that can indicate the start of an attack, such as logins from unusual IP addresses or outside business hours.

Now, IBM QRadar can proactively start Safeguarded Copy to create a protected backup at the first sign of a threat.

If an attack occurs, IBM Copy Services Manager (the orchestration software) helps identify the best Safeguarded backup to use and automates the process to restore data to online volumes. Because a restore action uses the same snapshot technology, it is almost instant and much faster than the use offline copies or copies that are stored in the cloud.

Scope

The focus of this document is to describe how to proactively start Safeguarded Copy to create an immutable backup at the first sign of a threat that is detected by IBM QRadar. It also describes the use of Copy Services Manager orchestration software to recover or restore the backup.

As part of early threat detection, several rules are presented and a sample Python script is provided that was used to start the Safeguarded Copy process. The document also provides several sample control path and data path use cases.

Customers and readers are encouraged create control path and data path use cases, customized IBM QRadar rules, and custom response scripts that are best suited to their environment. The use cases, rules, and Python script are seen as templates and cannot be used as-is in an environment.

The solution that is featured in the document was created by using IBM QRadar release 7.4.2 and the Safeguarded Copy feature that was introduced in 8.4.2 software release for FlashSystem 5100, 5200, 7200, 9100/R, 9200/R, and IBM SAN Volume Controller.

For the restore or recovery of Safeguarded Copy volumes, Copy Services Manager software release 6.3.0 was used.

All components that are described in the document, such as IBM QRadar, IBM Copy Services Manager, and IBM FlashSystem are in same network segment. More network planning is required if these systems are in different networks.

For more information about IBM QRadar, Safeguarded Copy, and Copy Services Manager, see “Resources” on page 46.

Introduction

Combining the capabilities of IBM Safeguarded Copy and IBM QRadar enables enterprises to build comprehensive cyber resilience solutions. These solutions address the Protect, Recover, and Detect functions of the NIST framework.

IBM FlashSystem can log all administration activities in the access logs, which includes all storage objects access information. To identify and detect potential malicious access and for compliance auditing purposes, such access logs must be integrated with the SIEM solution.

By combining IBM FlashSystem administration access logs, application logs, network or server logs, and flow and packet data, IBM QRadar can provide 360 degree protection for the enterprise data.

Safeguarded Copy feature

The new Safeguarded Copy solution that is available with IBM Spectrum® Virtualize 8.4.2 software is the latest protection mechanism for data on IBM FlashSystem family and IBM SAN Volume Controller storage systems.

Similar to the IBM DS8000® Safeguarded Copy solution, Safeguarded Copy helps secure data to prevent it from being compromised (accidentally or deliberately) and allows for recovery from protected backups if a cyberattack occurs.

It also provides secure, point-in-time copies or snapshots of active production data that cannot be altered or deleted (immutable copies), and that can later be used for identification, repair, or replacement of data that was compromised by cyber or internal attack or corrupted by system failures or human error.

The safeguarded backups or copies of data are protected with extra security provided that is through unique user roles with dual management control (separation of duties).

The Safeguarded Copy solution on IBM® FlashSystem family and IBM SAN Volume Controller storage systems integrates with IBM Copy Services Manager software, starting with Copy Services Manager version 6.3.0.1, by using its automated, built-in copy and retention scheduling, testing, and ease of recovery capabilities. IBM Copy Services Manager also coordinates Safeguarded Copy function across multiple systems.

IBM QRadar

IBM QRadar is a leading SIEM solution that can monitor, inspect, detect, and derive insights for identifying potential threats to the data that is stored on IBM Spectrum Scale-managed systems. It is one of the most popular SIEM solutions on the market today.

The SIEM solution provides powerful cyber resilience and threat detection features, such as centralized visibility, flexible deployment, automated intelligence, machine learning, and proactive threat hunting.

The data management and storage features of IBM Spectrum Scale, combined with the log analysis, deep inspection, and detection of threats that are provided by IBM QRadar, offer an excellent platform for hosting unstructured business data, reducing the effect of cyber threats, and increasing cyber resilience.

IBM QRadar can detect malicious patterns by using several data sources and analysis tools and techniques, including access logs, heuristics, correlation with logs from other systems (such as network logs or server logs), network flow, and packet data, and even unknown threat vector detection by using IBM Watson for Security resources. Its open architecture enables third-party interoperability so that many solutions can be integrated, which makes it even more scalable and robust.

Prerequisites

This solution includes the following prerequisites:

- A user with Administrator privileges was created on the IBM FlashSystem® or centralized authentication, such as LDAP or Active Directory. This user can be used by QRadar® system to securely log on to storage system by using SSH to perform various actions. It is suggested that a qradaradmin user is created for this task.
- The public key from a user on IBM QRadar is added to the qradaradmin user that is defined on IBM FlashSystem to set up password less authentication between IBM QRadar and IBM FlashSystem.
- The private key of the same user from IBM QRadar is added to the /opt/qradar/bin/ca_jails/home/customactionuser/.ssh folder to authenticate qradaradmin user by using the public key that is shared with IBM FlashSystem.
- The firewall rules between IBM QRadar and IBM FlashSystem are adjusted to allow traffic on 514/tcp or 514/udp.

- To use IBM Copy Services Manager, a locally or externally identified user is required. The use of Copy Services Manager allows greater flexibility to recover or restore data from various backup sets. It offers great flexibility for Safeguarded Copy backup/restore management because Copy Service Manager can connect to multiple storage systems. CLI and GUI interfaces are available for Copy Services Manager.

This document does not discuss the installation and configuration of Copy Services Manager software. For more information, see “Resources” on page 46.

Solution overview

The solution that is presented in this publication is shown in Figure 1.

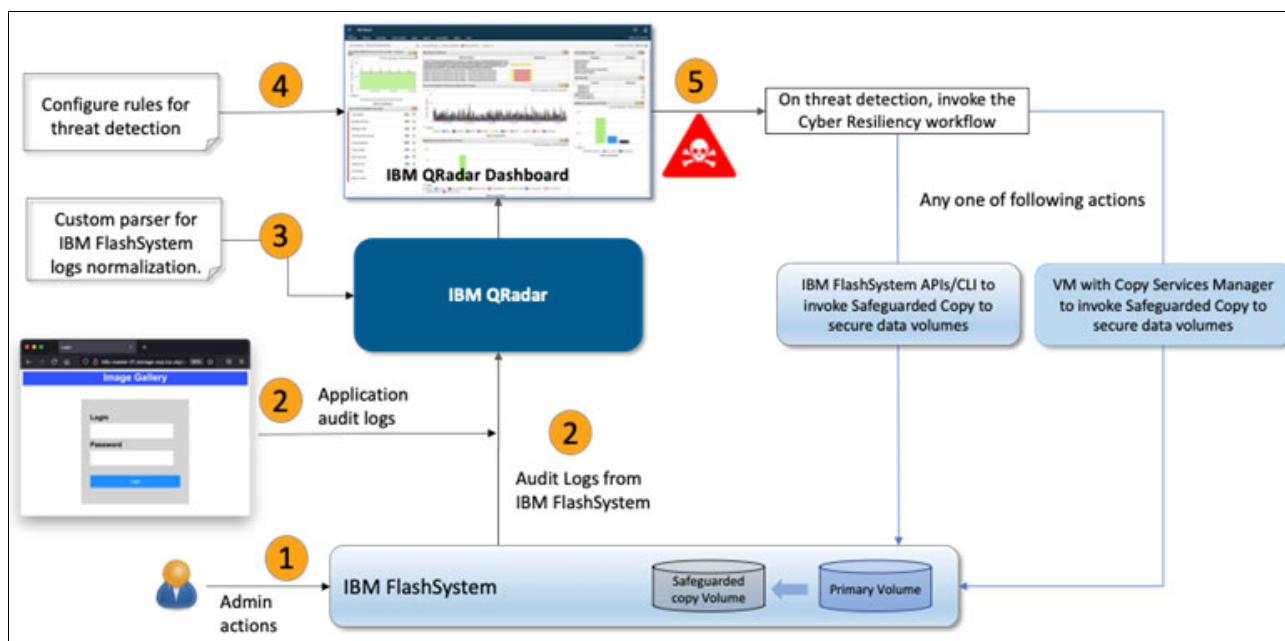


Figure 1 Solution overview

Organizations can face threats in many ways, such as compromised user credentials by using sphere fishing attack, or a rouge user within the organization cyberattacks, such as brute force attempts or ransomware. Any of these threats pose grave risks to storage systems that are used for storing the data.

For administrative tasks, IBM FlashSystem allows connectivity by using several methods, including as web login, command-line, or API calls. Every action from every connection is logged to IBM FlashSystems audit logs.

The IBM FlashSystem was configured to forward the audit logs to IBM QRadar by using the **mksyslogserver** command. By forwarding the audit log event, every administrative action is now logged and scrutinized for activities that are performed.

To simulate a brute force attack a 3-tier architecture application that involves a web server, an application and database server was created. The application was also configured to log actions by using the rsyslog Linux facility. The rsyslog configuration enables auditing of all events (application or user-related) that occur on the system

Various log sources were defined on IBM QRadar to classify all incoming events. To determine Control Path Events, a log source FS91K_Stoage_LS was used with the log source type as IBM SAN Volume Controller. To determine authentication-related events (GUI/CLI logins), a log source FS91K_Auth_LS was used with LinuxOS as the log source type. The storage system name acted as an identifier for every event that was generated on IBM.

The application events were forwarded by Linux rsyslog daemon running on the web server and the generated events were classified as Gallery-LS log source events. For more information about rsyslog daemon configuration, see “Appendix A” on page 45.

After the events are correctly classified based on the log sources, various rules were defined to filter events from each category. As part of rule definition, the response definition was also created ranging to register an offense to start Safeguarded Copy action by using custom actions. Python scripts were created and uploaded as Custom action.

To cover the control path actions and data path actions, the use cases that are described next were considered.

Control path use cases

In this section, thee control path uses cases are described.

Use case 1

In this use case, an attempt that was made by an administrator or lower role to delete the Safeguarded Copy (which is blocked and fails) raises an alert. Failed attempts to remove a volume are logged in the audit log.

Use case implementation

The volume ID of every Safeguarded Copy volume that was created was stored in the Safeguarded-Volumes Reference Set on IBM QRadar. The volume ID that is required in this case is always part of the Volume creation event that was sent from IBM FlashSystem. Similarly, an alert is generated when a user who is not from the designated Copy Services Manager user attempts to remove the Safeguarded Copy volume.

Use case 2

Administrator logins are detected outside business hours. Therefore, a Safeguarded Copy of important volumes can be generated, or the administrator user can be blocked.

Use case implementation

For more information about how this rule was created, see “IBM QRadar sample rules” on page 21.

Use case 3

The same FlashSystem administrator logged from a different location or IP address at the same time. Therefore, a Safeguarded Copy of important volumes can be generated or that administrator user can be blocked and forcefully logged out.

Use case implementation

For more information about how this rule was created, see “IBM QRadar sample rules” on page 21.

Data path use case

For the demonstration of data path use case, a simple 3-tier that is shown in Figure 2 was used. The application allows users to upload images upon successful login, and stores images on application server data volume.

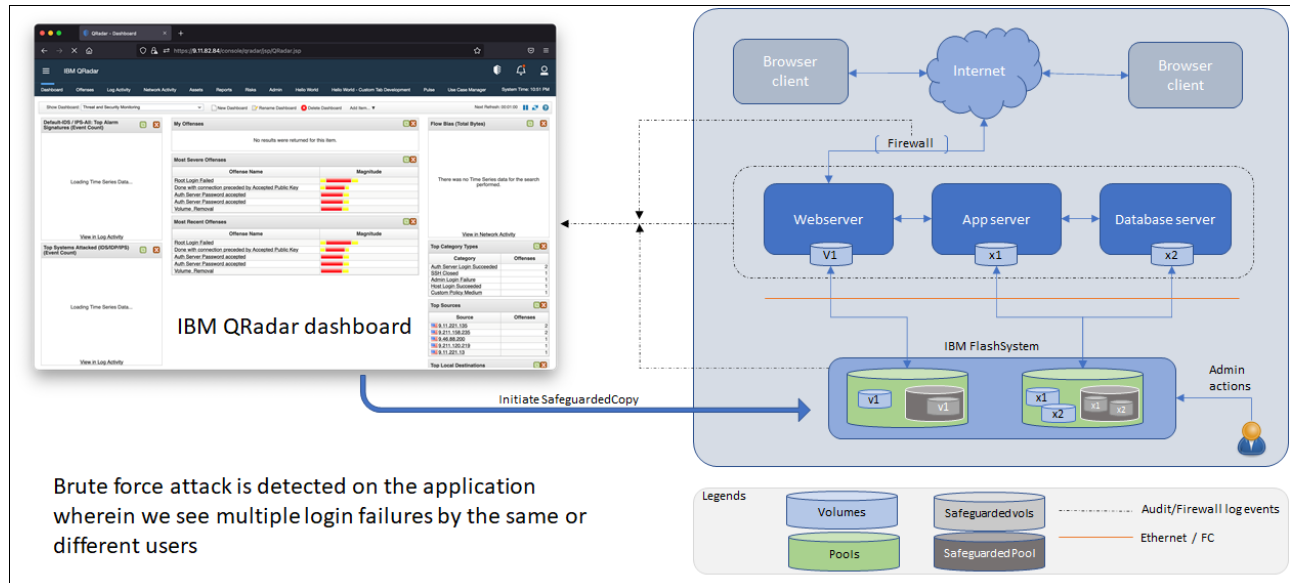


Figure 2 Sample application

To track user-specific images, a database table is maintained with an image ID for every user. When a threat is detected on the application, such as a brute force login, the failed login events are analyzed by IBM QRadar's rules engine, and then, it starts the Safeguarded Copy of the application and database volumes.

Lab setup

The data path use case that is shown in Figure 2 also shows the lab setup, on which the solution was created and tested.

Note: To run the CLI or GUI commands, log on to IBM FlashSystem as a superuser or a user with administrators privileges.

The following process was used to set up the lab:

1. Enable audit log forwarding from IBM FlashSystem to IBM QRadar by using the following CLI command:

```
mksyslogserver -name ibm-qradar-84 -ip 9.11.82.84 -error on -warning on -info on -audit on -protocol udp port 514
```

2. Enable the Safeguarded Copy feature on IBM FlashSystem by using the CLI or GUI:

- Using CLI: `mkmdiskgrp -parentmdiskgrp Pool0 -size 100 -unit gb -safeguarded`

Log on to IBM FlashSystem console and select **Pools** → **Create Child Pool**, as shown in Figure 3 on page 8. Enter a name for the child pool and then, select the **Safeguard** option.

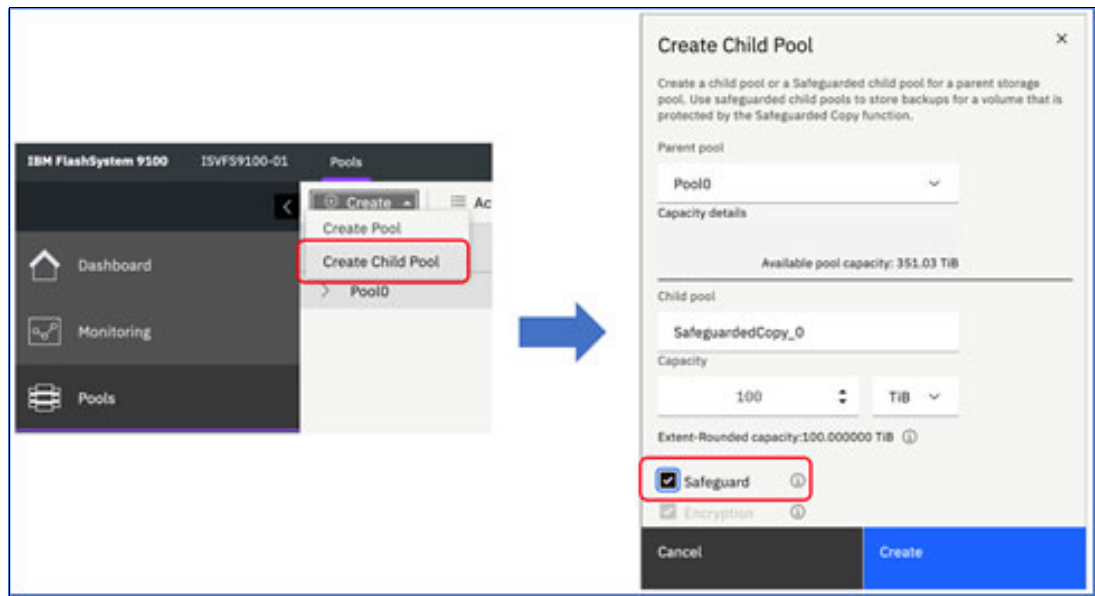


Figure 3 Creating Safeguarded Copy pool

3. Create a volume group:

- By using CLI: Create a volume group and assign a predefined Safeguarded policy 2:
`mkvolumegroup -name SafeguardedCopy_2 -safeguardedpolicy 2`
- By using GUI:
 - i. Create the Volume group, as shown in Figure 4. Then, choose the volumes to add to the volume group.

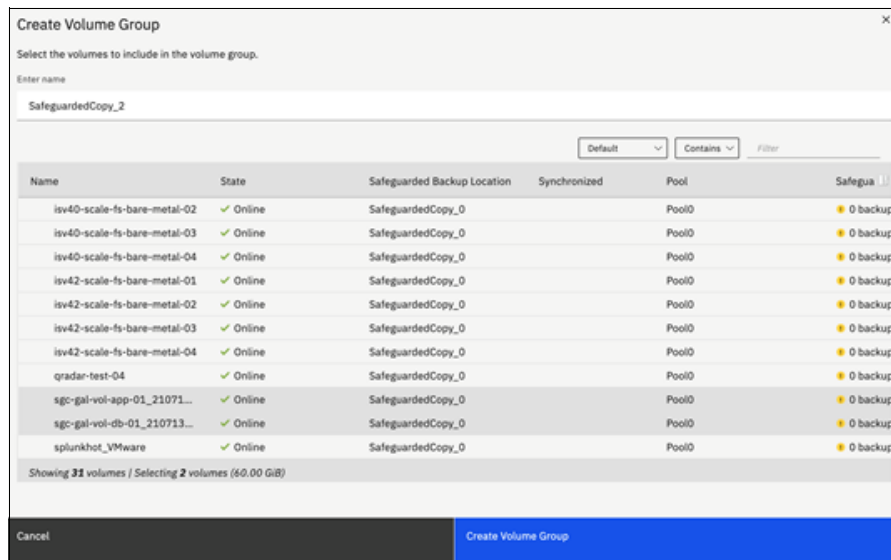
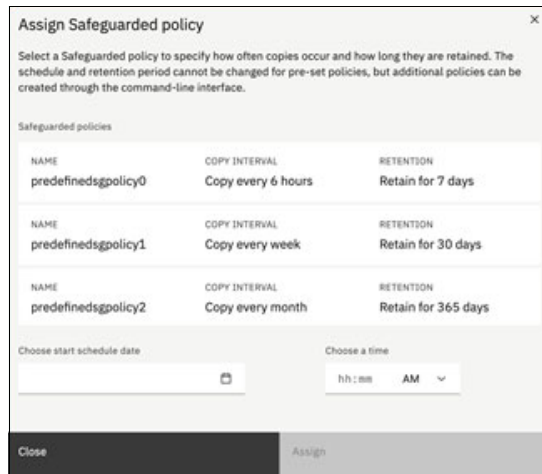


Figure 4 Creating a volume group

- ii. Assign the safeguarded policy to the volume group. The predefined policies are shown in Figure 5.



Assign Safeguarded policy

Select a Safeguarded policy to specify how often copies occur and how long they are retained. The schedule and retention period cannot be changed for pre-set policies, but additional policies can be created through the command-line interface.

Safeguarded policies

NAME	COPY INTERVAL	RETENTION
predefinedsgpolicy0	Copy every 6 hours	Retain for 7 days
predefinedsgpolicy1	Copy every week	Retain for 30 days
predefinedsgpolicy2	Copy every month	Retain for 365 days

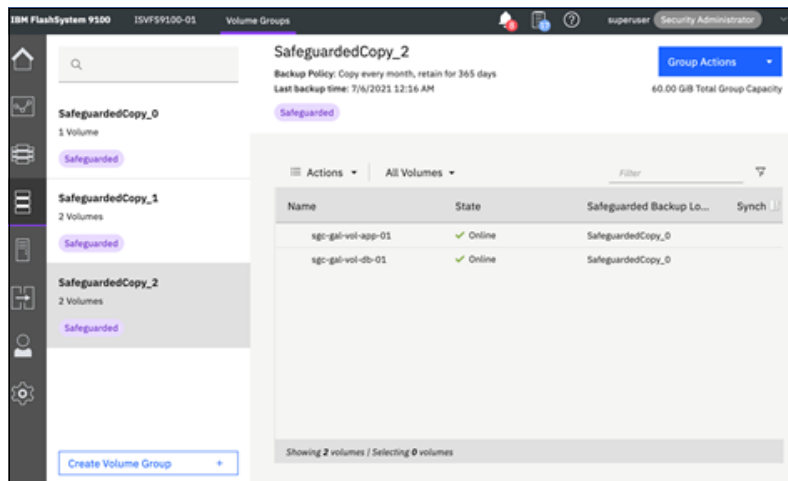
Choose start schedule date:

Choose a time: hh:mm AM

Close Assign

Figure 5 Assigning predefined Safeguarded policies volume group

- iii. Figure 6 shows the newly defined safeguarded copy volume group with a safeguard policy that is assigned to it. Two application volumes are also associated with the safeguarded copy volume group. The volume group name SafeguardedCopy_2 is used as parameter to the custom action that is defined in IBM QRadar.



IBM FlashSystem V100 ISVFS9100-01 Volume Groups

superuser Security Administrator

SafeguardedCopy_2

Backup Policy: Copy every month, retain for 365 days
Last backup time: 7/6/2021 12:16 AM
60.00 GiB Total Group Capacity

Safeguarded

Actions All Volumes Filter

Name	State	Safeguarded Backup Lo...	Synch
sgc-gal-vol-app-01	Online	SafeguardedCopy_0	
sgc-gal-vol-db-01	Online	SafeguardedCopy_0	

Showing 2 volumes / Selecting 0 volumes

Create Volume Group +

Figure 6 Volume group with Safeguarded copy policy assigned

4. Create the qradaradmin user with Administrator privileges:
 - By Using CLI:


```
mkuser -name qradaradmin -usergrp Administrator -password 'SuperLongPassword' -keyfile qradar-84-id_rsa.pub
```

- By using GUI (see Figure 7).

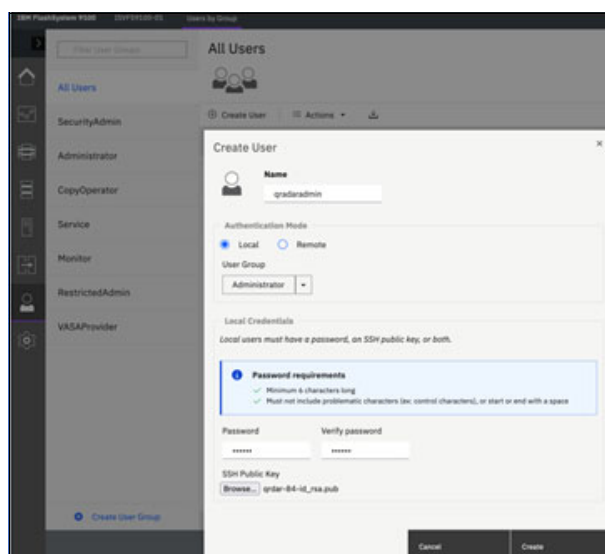


Figure 7 Creating local user qradaradmin on IBM FlashSystem

5. Copy the private key of IBM QRadar user to:

`/opt/qradar/bin/ca_jail/home/customactionuser/.ssh`

IBM QRadar creates a false root (chroot environment) to provide a pristine environment for user-provided scripts. In this case, as script uses SSH to log on to IBM FlashSystem as qradaradmin. When creating the qradaradmin user on IBM FlashSystem, a public key of root user was used. Therefore, root user's private key was copied to the ca_jails path, as shown in Figure 8.

```
[root@qradar /opt/qradar/bin/ca_jail/home/customactionuser/.ssh]# ls -la
total 16
drwx----- 2 customactionuser root          71 Jul  6 05:49 ./
drwxrwxr-x  3 customactionuser customactionuser 18 Jun 29 19:59 ../
-rw-----  1 customactionuser root           83 Jul  6 05:38 config
-rw-----  1 customactionuser root        3243 Jul  6 05:49 id_rsa
-rw-----  1 customactionuser root         756 Jul  6 05:55 id_rsa.pub
-rw-----  1 customactionuser root         531 Jul  6 01:39 known_hosts
```

Figure 8 .ssh folder path for customactionuser

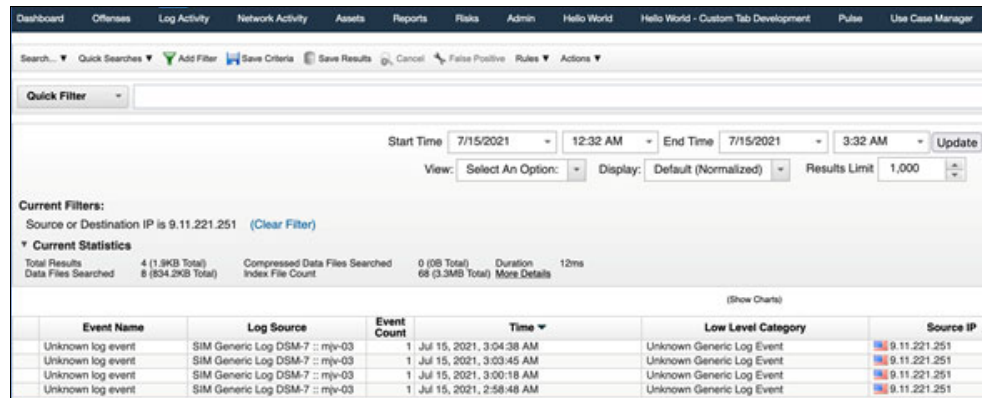
For more information about adding custom action scripts to IBM QRadar, see “Resources” on page 46.

6. Create custom log source types to normalize the audit log events that are received in QRadar into various log sources. For more information about how to normalize events by using regular expressions and assigning IBM QRadar identifier (QID) and create a custom log source, see “Custom log source” on page 11.
7. Define business-compliant rules. For more information, see “IBM QRadar sample rules” on page 21.
8. Upload the custom action script. For more information about how a custom action script is deployed in IBM QRadar, see “Custom actions” on page 30.
9. Generate a brute force attack on the web server to trigger multiple failure events.
10. Recover or restore storage volumes from the SafeguardedCopy backup by using the Copy Services Manager interface.

Custom log source

This section describes how to work with the audit events that are received from IBM FlashSystem.

When log forwarding is enabled on IBM FlashSystem by using `mksyslogserver`, IBM QRadar starts receiving the events. The received events are shown in the IBM QRadar's Log Activity window. IBM QRadar easily parses many types of log events and assigns the log source automatically. In specific cases, when IBM QRadar cannot automatically parse the event, the received event is listed as Unknown events, as shown in Figure 9.



The screenshot shows the IBM QRadar Log Activity window. At the top, there are tabs for Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Risks, Admin, Hello World, Hello World - Custom Tab Development, Pulse, and User Case Manager. Below the tabs is a search bar and a 'Quick Filter' dropdown. The main area displays event details for a specific time range (Start Time: 7/15/2021 12:32 AM, End Time: 7/15/2021 3:32 AM). The 'Current Filters' section shows 'Source or Destination IP is 9.11.221.251'. The 'Current Statistics' section shows 4 (1.9KB Total) Data Files Searched, 8 (834.2KB Total) Index File Count, 0 (0B Total) Compressed Data Files Searched, and 68 (3.3MB Total) Index File Count. The table below lists events with columns: Event Name, Log Source, Event Count, Time, Low Level Category, and Source IP.

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP
Unknown log event	SIM Generic Log DSM-7 : mpy-03	1	Jul 15, 2021, 3:04:38 AM	Unknown Generic Log Event	9.11.221.251
Unknown log event	SIM Generic Log DSM-7 : mpy-03	1	Jul 15, 2021, 3:03:45 AM	Unknown Generic Log Event	9.11.221.251
Unknown log event	SIM Generic Log DSM-7 : mpy-03	1	Jul 15, 2021, 3:00:18 AM	Unknown Generic Log Event	9.11.221.251
Unknown log event	SIM Generic Log DSM-7 : mpy-03	1	Jul 15, 2021, 2:58:48 AM	Unknown Generic Log Event	9.11.221.251

Figure 9 IBM QRadar Log Activity window

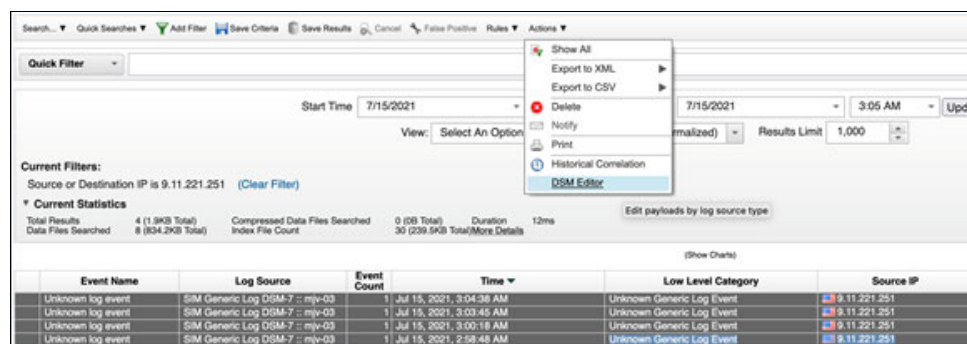
A sample event that was received from IBM FlashSystem is shown in Example 1.

Example 1 Sample event

```
<133>Jul 15 03:04:37 ISVFS9100-01 IBM2076[10405]: # timestamp = Thu Jul 15 03:04:37 2021 # cluster_user = superuser # source_panel = # target_panel = # ssh_ip_address = 9.211.91.228 # result = success # res_obj_id = none # command = svctask # action = rmvolume # action_cmd = rmvolume -gui 1471
```

Event normalization is required to create the rules definition that is based on the information that is contained in the payload. IBM QRadar's DSM module offers excellent flexibility to parse the events in many formats, including JSON or events with user-defined separator, as shown in Example 1.

Figure 10 shows the how to open a group of events in the DSM editor.



The screenshot shows the IBM QRadar Log Activity window with the 'DSM Editor' menu open. The menu options are: Show All, Export to XML, Export to CSV, Delete, Notify, Print, Historical Correlation, and DSM Editor. The 'DSM Editor' option is highlighted. The table below lists events with columns: Event Name, Log Source, Event Count, Time, Low Level Category, and Source IP.

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP
Unknown log event	SIM Generic Log DSM-7 : mpy-03	1	Jul 15, 2021, 3:04:38 AM	Unknown Generic Log Event	9.11.221.251
Unknown log event	SIM Generic Log DSM-7 : mpy-03	1	Jul 15, 2021, 3:03:45 AM	Unknown Generic Log Event	9.11.221.251
Unknown log event	SIM Generic Log DSM-7 : mpy-03	1	Jul 15, 2021, 3:00:18 AM	Unknown Generic Log Event	9.11.221.251
Unknown log event	SIM Generic Log DSM-7 : mpy-03	1	Jul 15, 2021, 2:58:48 AM	Unknown Generic Log Event	9.11.221.251

Figure 10 Opening multiple events with DSM editor

While opening the Unknown log events, IBM QRadar prompts the user to select a suitable Log Source Type. Many predefined log source types are available. Figure 11 shows **IBM SAN Volume Controller** is chosen as Log Source Type for the events.



Figure 11 Selecting the Log Source Type for events

When you select multiple events and choose **IBM SAN Volume Controller** as the Log Source Type, the DSM editor window looks the example that is shown in Figure 12.

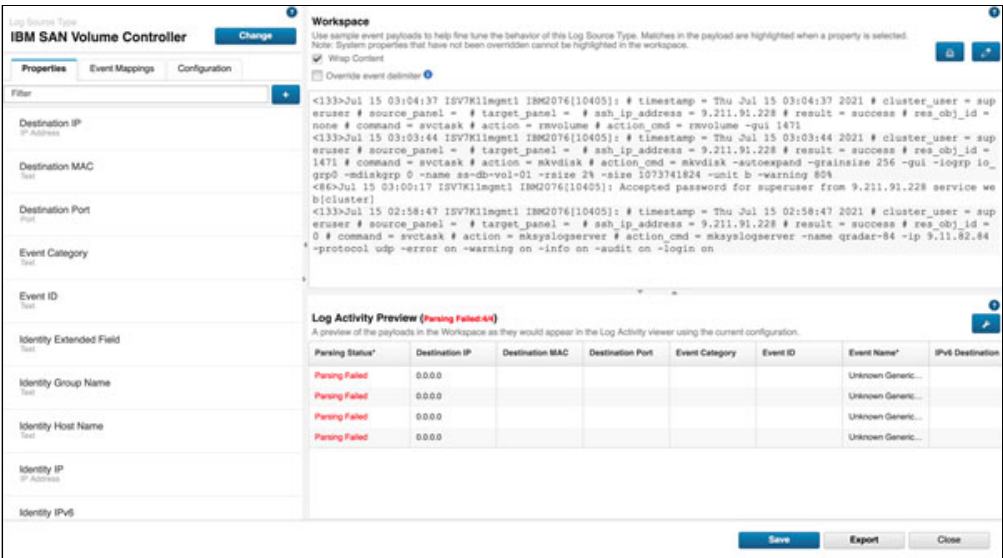


Figure 12 DSM Editor view with multiple non-parsed and non-mapped events

The Parsing failed status in Log Activity Preview window indicates, the IBM QRadar was unable to extract data for the event. In such cases, user intervention is required for providing the regular expressions to extract the required data values.

For more information about system- and custom-defined user extensions and how to match the required event values for those extensions, see Chapter 4, “Log source extensions”, in [IBM QRadar, DSM Configuration Guide](#).

It is also possible to select and open a single event in DSM editor, as shown in Figure 13. Also, a regular expression is shown to extract data for the Event ID property.

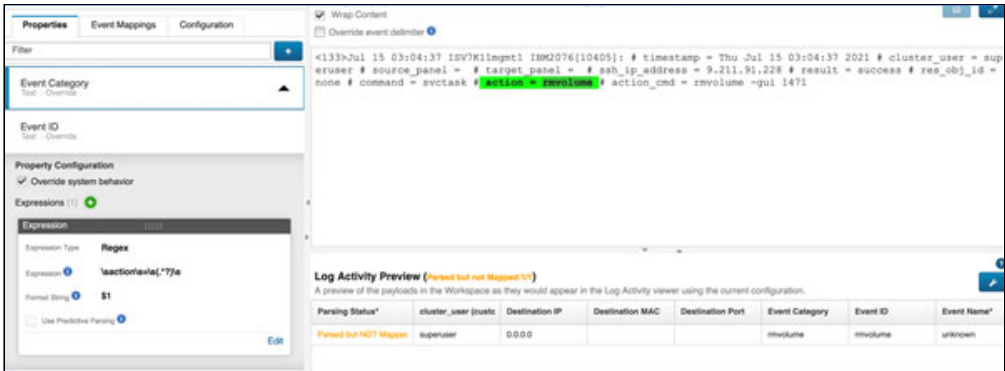


Figure 13 DSM editor with Single event parsed but not mapped to any QID

Event ID is a system property and it is populated automatically when QRadar can parse the event. In this case, the Event ID field is overridden to populate its value by using the user-defined regular expression.

While entering the regular expression, the matched part from the event is automatically highlighted in yellow. The green selection that is shown in Figure 13 indicates the successful match of event data by using the regular expression. Also, when the match is successful, data is seen in the Log Activity Preview window for the specific field.

It is possible to create a custom property to get a value for a specific field from the event. Clicking the [+] sign on event properties tab starts a wizard to help define custom property, as shown in Figure 14. The new custom property definition is started by clicking **Create New**.

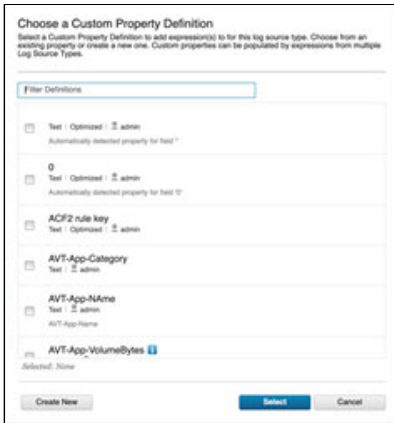


Figure 14 Custom property definition

When the event is received from IBM FlashSystem, the field cluster_user helps identify the user whose actions triggered the event.

Figure 15 shows the name, field type, and description that is chosen for the custom property. The Enable for use in Rules, Forwarding Profiles and Search Indexing option must be selected because this property is used later when the custom rules are defined.

Create a new Custom Property Definition
Create a new Custom Property Definition that can be expressed within one or more Log Source Type configurations.

Name: Field Type:

Description:

☒ Enable for use in Rules, Forwarding Profiles and Search Indexing ?

Figure 15 Creating a custom property definition

Clicking **Save** closes dialog box, and returns the control to Custom Property Definition window.

Choose **Select** to work with the cluster_user custom property in the DSM editor window.

Figure 16 shows the regular expression and the match for cluster_user custom property.

Properties | Event Mappings | Configuration

Filter:

Property Configuration

Expressions (1) ☒

Expression:

Expression Type:

Expression:

Capture Group:

Destination IP:

Destination MAC:

Log Activity Preview (Parsed but not Mapped 1/1)

A preview of the payloads in the Workspace as they would appear in the Log Activity viewer using the current configuration.

Parsing Status*	cluster_user (custo)	Destination IP	Destination MAC	Destination Port	Event Category	Event ID	Event Name*
Parsed but NOT Mapped	superuser	0.0.0.0			rmvolume	rmvolume	unknown

Figure 16 Regular expression and match for cluster_user property

As shown in the Log Activity Preview window in Figure 16, values for cluster_user, Event Category, and Event ID were extracted by providing correct regular expressions.

The properties that are defined to hold values that are matched from each type of audit events are listed in Table 1. The table contains System and Custom defined properties. The word *common* indicates that the property is used for multiple events. (The properties that were listed Table 1 were used for a custom log source FS91K_Storage_LS).

Table 1 System and Custom properties for Storage Events for FS91K_Storage_LS

Property name	Property type	Regular expression	Capture group	Storage event
Event ID	System, Common	\saction\s=\s(.*)\s	\$1	mkvolume
Event Category	System, Common	\saction_cmd\s=\smkvolume\s(.*)\s(SafeguardedCopy.*)\s	\$2	
Command	Custom	\saction_cmd\s=(.*)	1	
Command Origin	Custom	\s-gui\s	0	
Safeguarded Copy volume name	Custom	\s-name\s(bk_*)	1	
Result	Custom	\sresult\s=\s(.*)\s	1	
Safeguarded Copy Pool name	Custom	\saction_cmd\s=\smkvolume\s(.*)\s(SafeguardedCopy_d)\s	2	
SGC_BK_VOLID	Custom	\sres_obj_id\s=\s(.*)\s	1	
Username	Custom	\scluster_user\s=\s(.*)\s	\$1	
Volume_ID	Custom, Common	\d+\$	0	rmvolume

All login events to storage were assigned to FS91K_Auth_LS Log Source. These events are automatically parsed and required event categories were mapped by predefined LinuxOS Log Source Type.

The application-related events were assigned to Gallery_LS.

For every event that is received, the Event ID must have a value. When the event is not automatically parsed, this property must be overridden to match the required value from event as shown before.

After the required data from all events is correctly matched, QRadar attempts to assign a QRadar ID (QID). Every QID includes a description to help understand the event category.

For the automatically parsed events, QRadar automatically assigns the QID. For the manually parsed events, the QID must be assigned, which is done from DSM editor's Event Mappings tab.

As shown in Table 17, the Event ID and Event Category properties are populated with the value rmvolume.

Create a new Event Mapping

Enter an Event ID and Event Category combination to map to a QID record. A QID record allows a human-meaningful name and description to be associated with an event, as well as a Low Level Category and Severity value, which can in turn be used to trigger rules and building blocks.

Unknown Event Mappings

This table lists the Event ID/Event Category combinations that are parsed from events within the Workspace that do not currently have a corresponding Event Mapping. This table displays all Event Mappings that should be created for all events within the Workspace to parse successfully. Click on a row in this table to copy the Event ID and Event Category values into the corresponding text fields below.

Event ID	Event Category
rmvolume	rmvolume

Event ID

rmvolume

Event Category

rmvolume

QID Record

Choose QID...

Create

Close

Figure 17 Create a new Event Mapping window

Clicking **Choose QID** at the bottom of the window opens a dialog box in which the correct QID category can be selected (see Figure 18).

QID Records

Search for an existing QID record to assign, or create a new one.

High Level Category

Any

Low Level Category

Any

Log Source Type

Any

QIDName

Delete volume

Search

Search Results

Name	Severity	High Level Category	Low Level Category
Delete Volume	1	Audit	Delete Activity Attempted
Delete Volume - Client DryRun Operation The user has the required permissions, so the request would have succeeded, but	1	Audit	Read Activity Succeeded
Delete Volume - Client Invalid Volume NotFound Client Invalid Volume Not Found while Deleting the specified EBS volume	3	Audit	Delete Activity Failed
Delete Volume - Client Unauthorized Operation Unauthorized Operation when attempting to Delete the specified EBS volume	3	Audit	Delete Activity Failed
Delete Volume - Client Volume In Use Client Volume In Use while attempting operation Delete Volume: The specified Am	3	Audit	Delete Activity Failed
Delete Volume Containers Deletes an existing Volume Containers (8000 Series Only)	1	Audit	Delete Activity Succeeded

Total: 10 Selected: 1

Create New QID Record

Ok

Cancel

Figure 18 QID records

A QID can also be created from this window, if required. After the correct QID is located, it is then selected. The selected value then is assigned to Event, as shown in Figure 19.

Create a new Event Mapping

Enter an Event ID and Event Category combination to map to a QID record. A QID record allows a human-meaningful name and description to be associated with an event, as well as a Low Level Category and Severity value, which can in turn be used to trigger rules and building blocks.

Unknown Event Mappings

This table lists the Event ID/Event Category combinations that are parsed from events within the Workspace that do not currently have a corresponding Event Mapping. This table displays all Event Mappings that should be created for all events within the Workspace to parse successfully. Click on a row in this table to copy the Event ID and Event Category values into the corresponding text fields below.

Event ID	Event Category
rmvolume	rmvolume

Event ID

rmvolume

Event Category

rmvolume

QID Record

QID Record: Delete Volume

Create

Close

Figure 19 Event mapped to a QID

Now, the Event is correctly parsed and includes correct QID mapping. However, the existing events properties are not changed. It is still shown as an Unknown event. Any future events with a similar Event ID and Event Category are automatically assigned the same QID.

QRadar uses the QID information to coalesce events that belong to same category and displays a count that indicates how many times the event occurred, as shown in Figure 20.

	Event Name	Log Source	Event Count	Time	Low Level Category	Source IP
	Done with connection	LinuxServer@FS9100-01-Tucson	1	Jul 13, 2021, 8:28:26 PM	SSH Closed	9.11.82.84
	Done with connection	LinuxServer@FS9100-01-Tucson	1	Jul 13, 2021, 8:28:26 PM	SSH Closed	9.11.82.84
	PAM Session Closed	LinuxServer@FS9100-01-Tucson	1	Jul 13, 2021, 8:28:26 PM	Auth Server Session Closed	9.11.103.17
	Accepted Public Key	LinuxServer@FS9100-01-Tucson	1	Jul 13, 2021, 8:28:26 PM	Host Login Succeeded	9.11.82.84
	PAM Ssh User Impersonation	LinuxServer@FS9100-01-Tucson	1	Jul 13, 2021, 8:28:26 PM	Privilege Access	9.11.103.17
	PAM Unable to Resolve Sy...	LinuxServer@FS9100-01-Tucson	2	Jul 13, 2021, 8:28:19 PM	Error	9.11.103.17
	Unknown	FS91K_Storage_LS	2	Jul 13, 2021, 8:28:19 PM	Unknown	9.11.82.84
	Safeguarded_Volume_Cop...	FS91K_Storage_LS	1	Jul 13, 2021, 8:28:18 PM	Custom Policy High	9.11.82.84
	Unknown	FS91K_Storage_LS	1	Jul 13, 2021, 8:28:17 PM	Unknown	9.11.82.84
	PAM Session Closed	LinuxServer@FS9100-01-Tucson	7	Jul 13, 2021, 8:28:14 PM	Auth Server Session Closed	9.11.103.17
	Done with connection	LinuxServer@FS9100-01-Tucson	7	Jul 13, 2021, 8:28:14 PM	SSH Closed	9.11.82.84
	Done with connection	LinuxServer@FS9100-01-Tucson	7	Jul 13, 2021, 8:28:14 PM	SSH Closed	9.11.82.84
	Accepted Public Key	LinuxServer@FS9100-01-Tucson	7	Jul 13, 2021, 8:28:14 PM	Host Login Succeeded	9.11.82.84
	PAM Ssh User Impersonation	LinuxServer@FS9100-01-Tucson	7	Jul 13, 2021, 8:28:14 PM	Privilege Access	9.11.103.17
	PAM Unable to Resolve Sy...	LinuxServer@FS9100-01-Tucson	14	Jul 13, 2021, 8:28:14 PM	Error	9.11.103.17

Figure 20 QRadar log activity showing event coalescing

After event parsing and mapping is complete, a unique Log Source is defined to identify or filter events. This Log Source is also used when custom rules are defined in QRadar.

To define a new Log Source, from the Admin tab, select the **Log Source** option, as shown in Figure 21.

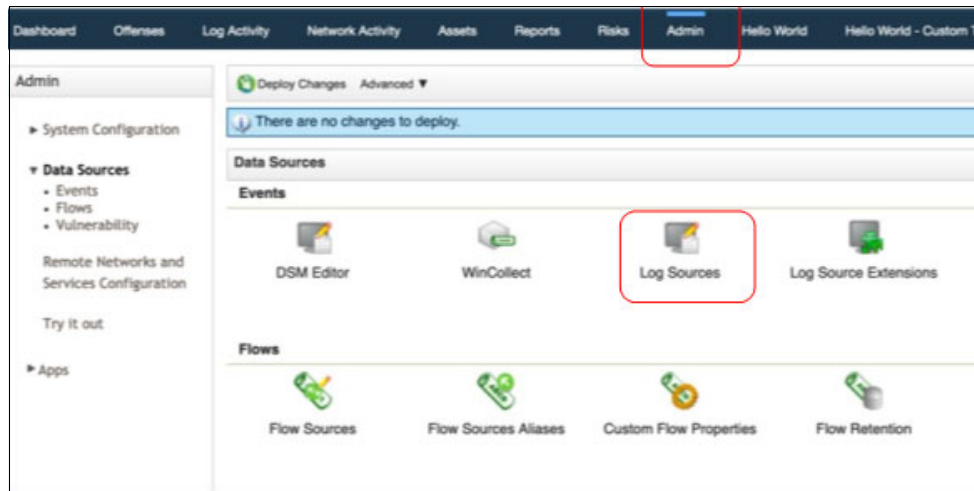


Figure 21 Log Source under Admin tab

The new Log Source wizard is started by clicking **New Log Source**, as shown in Figure 22.

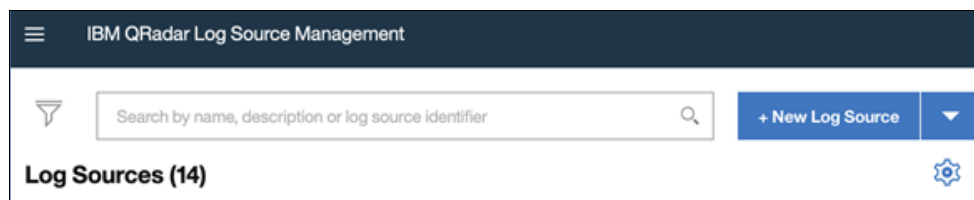


Figure 22 Creating a Log Source

Then, select **Single Log Source** in next window, as shown in Figure 23.

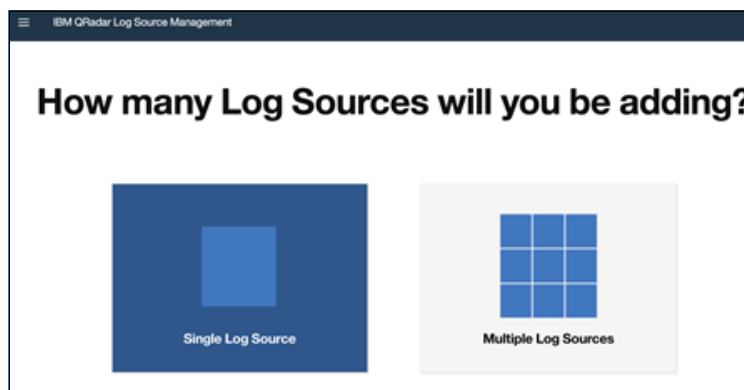


Figure 23 Intermediate step to indicate number of Log Sources

A wizard is started from where system-defined values were selected (see Figure 24).

The screenshot shows the 'Select a Log Source type' screen. On the left, a vertical sidebar contains four steps: 1. Select Log Source Type (highlighted with a blue circle), 2. Select Protocol Type, 3. Configure Log Source Parameters, and 4. Configure Protocol Parameters. The main area has a search bar with 'IBM SA' entered. Below the search bar, a single option 'IBM SAN Volume Controller' is listed and highlighted with a blue bar.

Figure 24 Log Source type selection

The next step involves choosing the Log Source (see Figure 25).

The screenshot shows the 'Select a protocol type' screen. The sidebar on the left now shows step 2 'Select Protocol Type' highlighted with a blue circle, while step 1 is marked with a green checkmark. The main area has a search bar labeled 'Look up Protocol Type'. Below it, two options are listed: 'Forwarded' and 'Syslog', with 'Syslog' highlighted by a blue bar. At the bottom, there is a checkbox for 'Show Undocumented Protocol Types' and two buttons: 'Step 1: Select Log Source Type' and 'Step 3: Configure Log Source Parameters'.

Figure 25 Choice of protocol

Then, the parameters for the Log Source are selected, as shown in Figure 26.

The screenshot shows the 'Configure the Log Source parameters' screen. The sidebar on the left shows step 3 'Configure Log Source Parameters' highlighted with a blue circle, while steps 1 and 2 are marked with green checkmarks. The main area contains several configuration fields: 'Name' (FSMK_Storage_13), 'Description' (Logsource for IBM FileSystemPRO), 'Enabled' (a toggle switch that is turned on), 'Groups' (Other), 'Extension' (IBMSANVolumeController_ext), 'Language' (English), and 'Target Event Collector' (eventcollector01-np-03). At the bottom, there are two buttons: 'Step 2: Select Protocol Type' and 'Step 4: Configure Protocol Parameters'.

Figure 26 Log Source parameters

The final step in the configuration process is to define the identifier for the events. The name of the storage system is listed here (see Figure 27).

The screenshot shows a configuration window titled "Configure the protocol parameters". On the left, a vertical list of steps is shown with checkmarks: "Select Log Source Type", "Select Protocol Type", "Configure Log Source Parameters", and "Configure Protocol Parameters" (which is highlighted with a blue circle). The main area contains two fields: "Log Source Identifier *" with the value "FS91K-03" and "Incoming Physical Encoding *" with a dropdown menu set to "UTF-8".

Figure 27 Log Source protocol parameters

The completed Log Source definition is shown in Figure 28.

The screenshot shows a "Log Source Summary" window. At the top, it displays the name "FS91K_Storage_LS" with a status of "OK" and a note "Last Updated 17 days ago". Below this, there are two tabs: "Overview" (selected) and "Protocol". The "Overview" tab shows a list of properties for the log source:

Property	Value
ID	214
Name	FS91K_Storage_LS
Description	Logsource for IBM FlashSystem 9100
Enabled	Yes
Log Source Type	FS91K_Storage_LS
Protocol Type	Syslog
Groups	Other
Extension	FS91KStorageLSCustom_ext
Language	English
Target Event Collector	eventcollector0 :: mjb-03
Disconnected Log Collector	Not Set
Credibility	5
Internal	No
Deployed	Yes
Coalescing Events	Yes

Figure 28 Completed Log Source

The custom log source definition is now complete. QRadar now has enough information to parse and map future events that are based on protocol parameters.

Definition or changes to a Log Source requires a Deployment task, as shown in the Admin tab (see Figure 29).

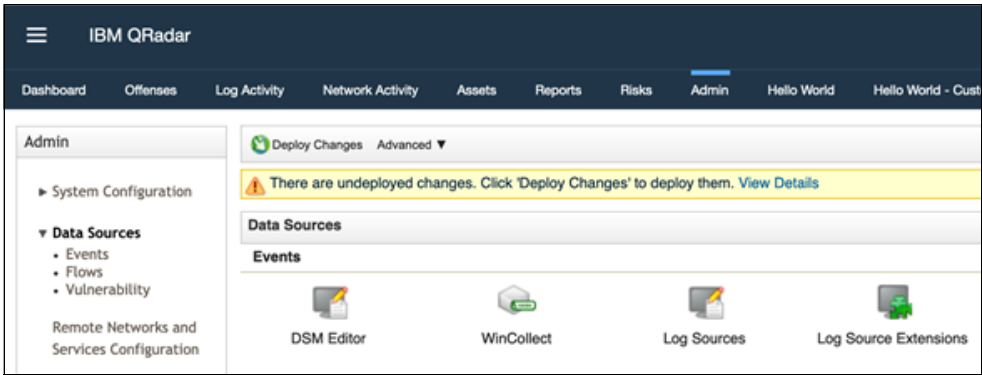


Figure 29 Deploying changes

IBM QRadar sample rules

This section explains the compliance rules that must be considered when IBM QRadar sample rules are created that deal with creating and removing SafeguardedCopy volumes from the storage system (see Figure 30).

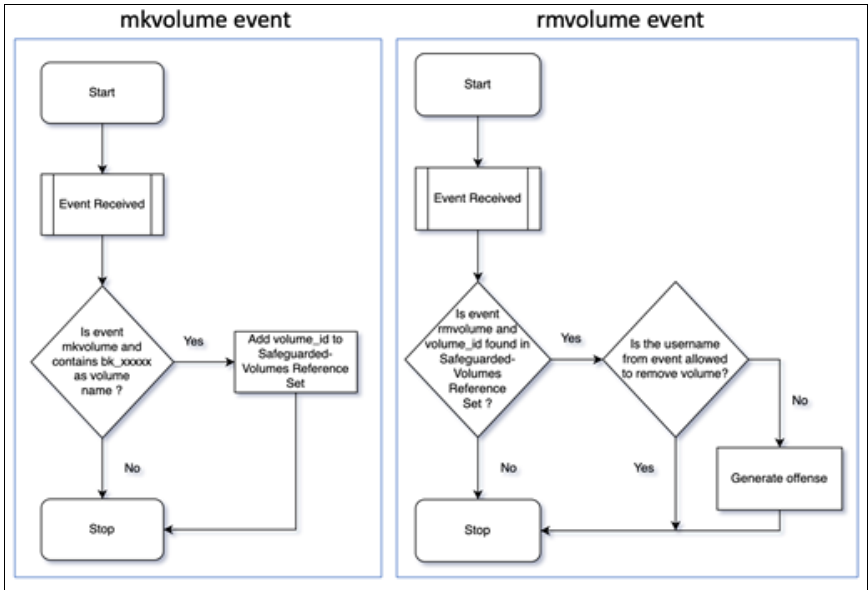


Figure 30 Sample compliance rules for creating and removing Safeguarded Copy volumes

To keep track of SafeguardedCopy volumes that were created on the storage system, a reference set was defined in IBM QRadar by clicking **Admin** → **Reference Set Management** → **Add Reference Set** (see Figure 31).

New Reference Collection

The following fields are required.

Name: SafeguardedCopy-Volumes

Type: AlphaNumeric

Time to Live of elements: (YY:MM.DD:hh:mm:ss)

☐ Since first seen
☐ Since last seen

☒ Lives Forever

When elements expire:

☒ Log each element in a separate log entry
☐ Log elements in one log entry
☐ Do not log elements

Create Cancel

Figure 31 Creating a reference set

The reference set is populated with volume_id custom property of the mkvolume event. The rules creation process is shown in Figure 32 - Figure 38 on page 25.

IBM QRadar

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Pulse Use Case Manager

Search... Quick Searches Add Filter Save Criteria Save Results Cancel False Positive Rules Actions

Advanced Search

Viewing real time

Current Filters:

Rules

- Add Anomaly Rule...
- Add Behavioral Rule...
- Add Threshold Rule...

Figure 32 Accessing predefined rules on IBM QRadar

Display: Rules Group: Rule and Building Block Groups Groups Actions Revert Rule Search Rules...

View the IBM App Exchange for more...

Rule Name	Group	Rule Category	Rule Type
All Exploits Beco...	Intrusion Detection	Custom Rule	Event
Anomaly: Excessi...	Recon	Custom Rule	Event
AssetExclusion: E...	Asset Reconciliati...	Custom Rule	Event
AssetExclusion: E...	Asset Reconciliati...	Custom Rule	Event
AssetExclusion: E...	Asset Reconciliati...	Custom Rule	Event
AssetExclusion: E...	Asset Reconciliati...	Custom Rule	Event
AssetExclusion: E...	Asset Reconciliati...	Custom Rule	Event
AssetExclusion: E...	Asset Reconciliati...	Custom Rule	Event
AssetExclusion: E...	Asset Reconciliati...	Custom Rule	Event

New Event Rule

- New Flow Rule
- New Common Rule
- New Offense Rule
- Enable/Disable
- Duplicate
- Open
- Delete
- Assign Groups
- Historical Correlation

Figure 33 Creating an event rule

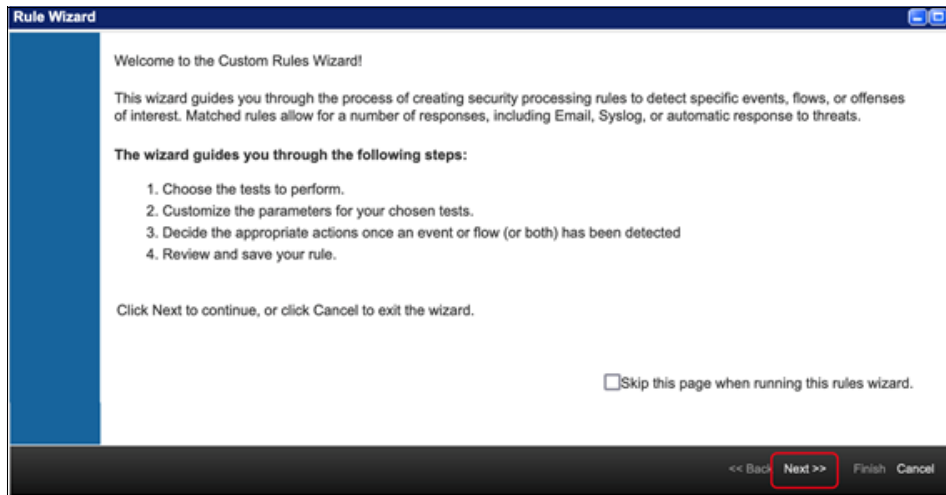


Figure 34 Wizard Welcome window

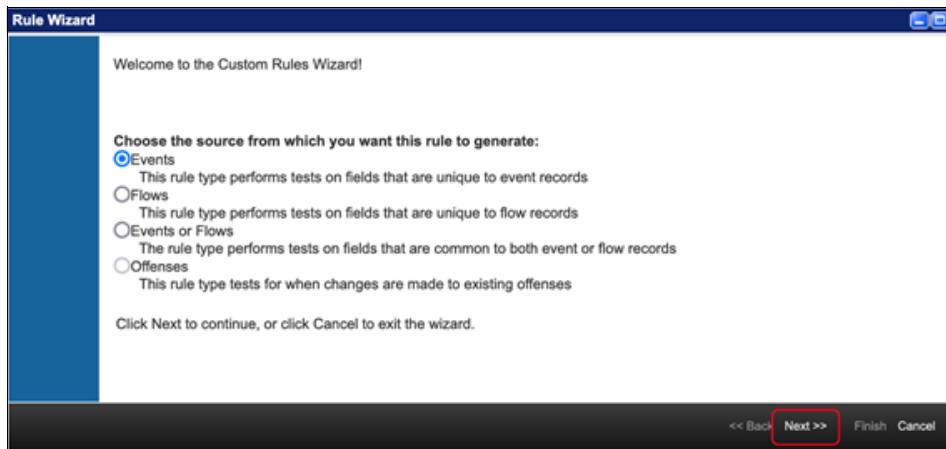


Figure 35 Choosing source for rule

Rule Wizard

Rule Wizard: Rule Test Stack Editor

Which tests do you wish to perform on incoming events?

Test Group: **All** Export as Building Block

Type to filter

- when the local network is one of the following networks
- when the destination network is one of the following networks
- when the IP protocol is one of the following protocols
- when the Event Payload contains this string**
- when the source port is one of the following ports
- when the destination port is one of the following ports
- when the local port is one of the following ports
- when the remote port is one of the following ports
- when the source IP is one of the following IP addresses
- when the destination IP is one of the following IP addresses

Rule (Click on an underlined value to edit it)
Invalid tests are highlighted and must be fixed before rule can be saved.

Apply Add-SafeguardedCopyVolume-To-Ref-Set on events which are detected by the **Local** system

- and when the event(s) were detected by one or more of E591K_Storage_LIS
- and when the event QID is one of the following (88750207) Create Volume
- and when the Event Payload contains bk_

Please select any groups you would like this rule to be a member of:

- ☐ Recon
- ☐ Response
- ☒ **SafeguardedCopy**
- ☐ Suspicious
- ☐ System

Notes (Enter your notes about this rule)

The rule attempts to detect "Create Volume" QID and volume name that begins with "bk_" from the event payload

<< Back Next >> **Finish** Cancel

Figure 36 Rule Test Stack Editor window

Rule Wizard

Choose the action(s) to take when an event occurs that triggers this rule

☐ Severity Set to 0

☒ Credibility Increase by 3

☐ Relevance Set to 0

☐ Ensure the detected event is part of an offense

☒ Annotate event

Enter annotation for this event: **Safeguarded-Volume-C**

☐ Bypass further rule correlation event

Rule Response

Choose the response(s) to make when an event triggers this rule

☐ Dispatch New Event

☐ Email

☐ Send to Local Syslog

☐ Send to Forwarding Destinations

☐ Notify

☒ Add to a Reference Set

Add the **volume_id (custom)** of the event or flow payload to the Reference Set:

SafeguardedCopy-Volumes - AlphaNumeric

☐ Add to Reference Data

☐ Remove from a Reference Set

☐ Remove from Reference Data

☐ Trigger Scan

☐ Execute Custom Action

Response Limiter

Use this section to configure the frequency with which you want this rule response to respond

☐ Respond no more than 1 time(s) per 30 minute(s) per Rule

<< Back **Next** >> Finish Cancel

Figure 37 Rule Response section

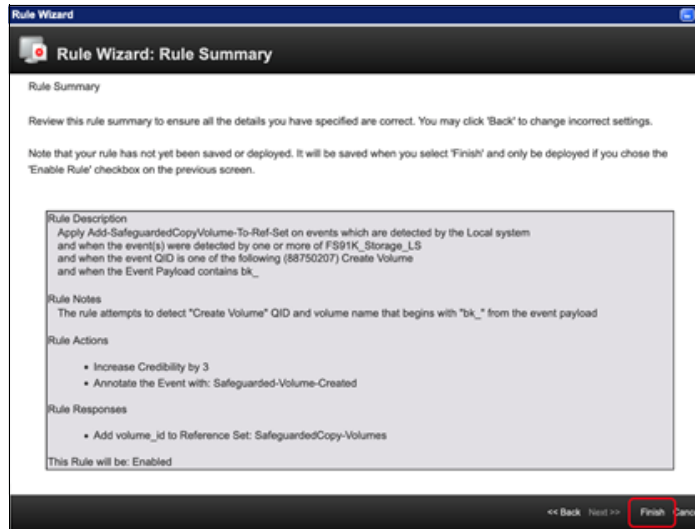


Figure 38 Rule Summary window

The rule is run for every event that matches Create Volume QID and contains bk_ text as part of event payload. Upon running, it adds the value of volume_id custom property to SafeguardedCopy-Volume reference set that was defined.

Similarly, when a SafeguardedCopy volume removal event is detected, the user that triggered the event is crosschecked against users that allowed the delete action on the storage. An offense is generated when the unauthorized users are attempting volume removal.

When the same action is run by an authorized user, no offense is generated. In both cases, the volume_id that is added by AddSafeguardedCopyVolume-To-Ref-Set rule is removed from SafeguardedCopy-Reference Set.

Notice that a custom property `rmvolume_id` is defined for the `rmvolume` event that holds the value of the volume that is being deleted. The rule's summary is shown in Figure 39.

Rule Description

Apply Remove-SafeguardedCopy-Volume-From-Ref-Set on events which are detected by the Local system
and when the events were detected by one or more of FS91K_Storage_LS
and when the event QID is one of the following (105255068) Delete volume
and when any of `rmvolume_id` (custom) are contained in any of SafeguardedCopy-Volumes - AlphaNumeric
and NOT when any of `cluster_user` are contained in any of SafeguardedCopy-Volume-Admins

Rule Actions

Set Severity to 6
Set Credibility to 6

Rule Responses

Remove `rmvolume_id` from Reference Set: SafeguardedCopy-Volumes

This Rule will be: Enabled

Figure 39 Remove `volume_id` from `SafeguardedCopy-Volumes` Reference Set

Figure 40 shows the `SafeguardCopy-Volumes` Reference Set that is defined in IBM QRadar.

Reference Set: SafeguardedCopy-Volumes			
<div>ContentReferences</div> <div> <div>AddDeleteDelete ListedImportExport</div> <div>Add new search criteria...</div> </div>			
Value	Origin	Time to Live	Date Last Seen
63	Add-SafeguardedCopyVolume-To-Ref-Set		Jul 14, 2021, 6:26:38 AM
64	Add-SafeguardedCopyVolume-To-Ref-Set		Jul 14, 2021, 6:26:38 AM
61	Add-SafeguardedCopyVolume-To-Ref-Set		Jul 14, 2021, 6:17:38 AM
62	Add-SafeguardedCopyVolume-To-Ref-Set		Jul 14, 2021, 6:17:38 AM
57	Add-SafeguardedCopyVolume-To-Ref-Set		Jul 13, 2021, 9:21:37 PM
58	Add-SafeguardedCopyVolume-To-Ref-Set		Jul 13, 2021, 9:21:37 PM
56	Add-SafeguardedCopyVolume-To-Ref-Set		Jul 13, 2021, 8:47:37 PM
55	Add-SafeguardedCopyVolume-To-Ref-Set		Jul 13, 2021, 8:45:37 PM

Figure 40 Safeguarded Copy `volume_id`'s Reference Set

Sample rules to capture control path actions

Figure 41 shows a rule to manage administrator logins that are detected outside of business hours.

Rule Description

Apply Admin-logins-outside-business-hours on events, which are detected by the Local system

and when the events were detected by one or more of FS91K_Auth_LS

and when the events occur between 00:00 and 06:00

and when the event category for the event is one of the following Authentication.Auth Server Login Succeeded, Authentication.Admin Login Attempt, Authentication.Host Login Succeeded

and when any of Username are contained in any of StorageAdmins - AlphaNumeric

Rule Notes

Admin logins detected outside office hours or odd hours

Rule Actions

Set Severity to 5

Set Credibility to 5

Annotate the Event with: Admin-login-outside-business-hours

This Rule will be: Enabled

Figure 41 Rule: Administrator logins detected outside business hours

Figure 42 shows a rule that manages when the same user logs on from multiple locations or IP addresses.

Rule Description

Apply Same-User-Multi-IP-Logins on events, which are detected by the Local system and when the events were detected by one or more of FS91K_Auth_LS and when the event QID is one of the following (11750041) Auth Server Login Succeeded, (11750336) Host Login Succeeded and when at least 2 events are seen with the same Username and different Source IP in 5 minutes

Rule Notes

The rule attempts to detect multiple logins by same username but from different IP addresses in 5 minutes

Rule Actions

Set Severity to 5

Set Credibility to 4

Force the detected Event to create a NEW offense, select the offense using Source IP

Annotate this offense with: Same user login from multiple locations

Annotate the Event with: Same user logged from multiple locations

This Rule will be: Enabled

Figure 42 Rule: Same user logged on from multiple locations or IP addresses

Sample rule to capture data path actions

Figure 43 shows a rule that applies multi-app login failures for a single username.

Rule Description

Apply Multiple App Login Failures for Single Username on events which are detected by the Local system

and when the event QID is one of the following (50253724) Login failed via web

and when at least 10 events are seen with the same Username in 5 minutes

and when the event(s) were detected by one or more of Gallery-LS

Rule Notes

Reports authentication failures for the same username

Rule Actions

Force the detected Event to create a NEW offense, select the offense using Username

Annotate this offense with: Multiple Login Failures for the Same User

Rule Responses

Dispatch New Event:

- Event Name: Multiple Login Failures for the Same User
- Event Description: Detected multiple (10) authentication failures for the same user name in a 5 minute period.
- Severity: 4 Credibility: 7 Relevance: 7
- High-Level Category: Authentication
- Low-Level Category: User Login Failure
- Force the dispatched event to create a NEW offense, select the offense using Username

Execute Custom Action

Rule Limiter

Respond no more than 3 times per 30 minutes per Rule

This Rule will be: Enabled

Figure 43 Rule: Multi-app login failure for single username

Custom actions

To add a custom action to IBM QRadar, choose the **Admin** option from the menu bar, and then, select **Custom Actions** in the **Data Sources** section, as shown in Figure 44. Then, click **Add** in the Custom Actions window.

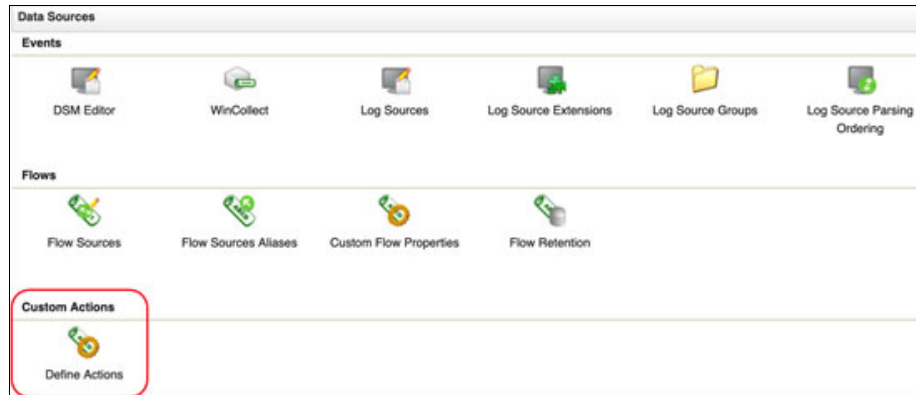


Figure 44 Custom actions

Define the Custom Action, as shown in Figure 45. A Fixed property or Network Event property also can be added. The Network Event property also can be a value that is extracted from an event.

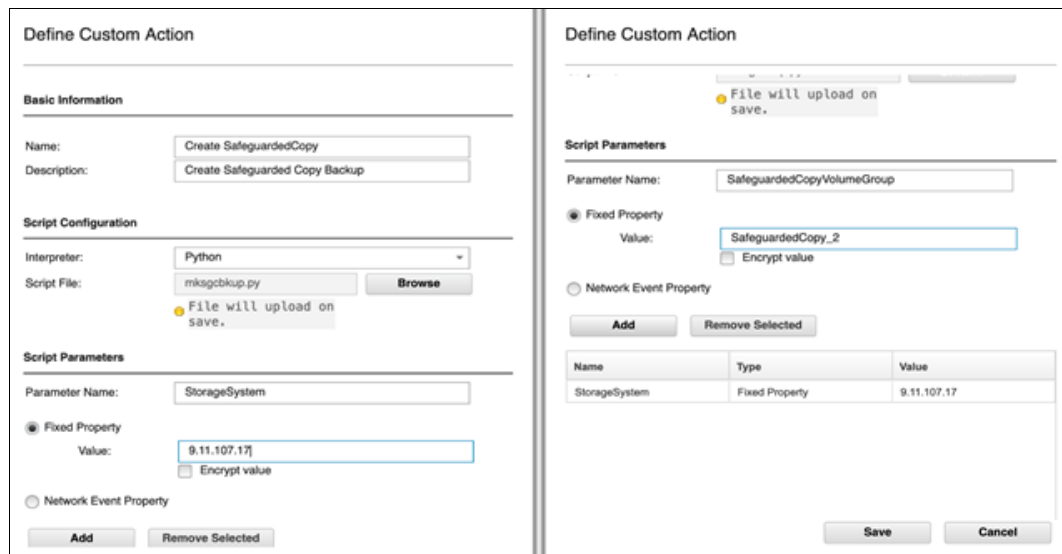


Figure 45 Defining custom action with parameters

Example 2 shows the sample Python script to start the Safeguarded Copy action.

Note: The script that is shown in Example 2 is provided as a sample reference and used for demonstration purposes. Customers can modify it based on their needs.

Example 2 Sample Python Script

```
#!/usr/bin/env python3

import os
import re
import sys
import subprocess
import datetime

def usage():

    msg = """
    Usage: {0} <storage_system> <volume_group_name>

    where
        storage_system = storage system FQDN or IP address
        volume_group_name = volume group on which safeguardedbackup policy has been
        applied (case sensitive)

    eg. {0} "9.199.142.39" "SafeguardedCopy_0"

    NOTE: Unset the simulation variable if the script has been exeuted in
    simulation mode before.

    ** simulation mode execution is possible with following conditions

    1. export simulation=True

    2. execute following command on svc/flashsystem and capture the output in
    lsmdisk_detail.csv file

        ssh user@SVC_SYSTEM "for x in \$(lsmdiskgrp -delim , | grep -v ^id | cut -d
        , -f 1); do lsmdiskgrp -delim , \$x; done" > lsmdiskgrp_detail.csv

    3. execute following command on svc/flashsystem and capture the output in
    lsvdisk_detail.csv file

        ssh user@SVC_SYSTEM "for x in \$(lsvdisk -delim , | grep -v id | grep -v bk_
        | cut -d , -f 27); do lsvdisk -bytes -delim , \$x; done" > lsvdisk_detail.csv

    4. execute following command on svc/flashsystem and capture the output in
    lsfcmaps.csv file

        ssh user@SVC_SYSTEM "lsfcmap -delim , | grep -v ^id" > lsfcmaps.csv

    Once all the csv files are created, re-run the python script.
```

To get an accurate simulation refresh all the CSV files with latest data by executing above commands on storage.

```
"""

print( msg . format(sys.argv[0]) )

sys.exit( 1 )

def runCli( cli_cmd ):
    """
        Purpose: This function runs the cli command on SVC system using SSH
                 a passwordless authentication must be available

        Parameters:
            - IN
              1. cli command to run
            - OUT
              1. output of cli command
    """

    global svc_system, remote_usr

    lst_cmd = []
    lst_cmd.append( 'ssh' )
    lst_cmd.append( '-o StrictHostKeyChecking=no' )
    lst_cmd.append( remote_usr + "@" + svc_system )
    lst_cmd.append( cli_cmd )

    try:
        # Command execution using subprocess
        stdout = subprocess.check_output( lst_cmd,
                                         universal_newlines = True,
                                         shell = False )

        if stdout != None:
            return stdout

    except KeyboardInterrupt:
        print( "User abort ..\n" )
        sys.exit( 1 )

    except subprocess.CalledProcessError:
        print( "Error connecting to remote host !! aborting !!! \n")
        sys.exit( 1 )

def getSafeguardedPoolName( all_mdisk ):
    """
        Purpose: This function is used to get the safeguarded pool from list of
        pools defined.
                 As soon as first safeguarded pool is found it is returned.

        Parameters:
```

```

- IN
    1. Comma delimited detailed output of all mdisks available on system

- OUT
    1. string value containing name of the safeguarded pool
"""

for line in all_mdisk.strip().split("\n"):

    if line != None:

        try:

            key = line.split(",")[0]
            val = line.split(",")[1]

            if key == 'name':

                sgc_pool_name = val

            if key == 'safeguarded' and val == 'yes':

                return sgc_pool_name

        except IndexError:
            pass

    return None

def getVdisksPerVolGroup( all_vdisks, vol_group, sgc_pool_name ):
    """
    Purpose: This function is used to generate a mkvolume command for each
    volume
            from the given volume group.

    Parameters:

    - IN
        1. all_vdisks : Comma delimited detailed output of all vdisks
        available on system
        2. vol_group   : Volume Group
        3. sgc_pool_name : The SafeguardedCopy Pool defined on the system.
    This is different
            than volume group definition with similar name.

    - OUT
        1. dictionary : Containing following record.

            { "vol_id" : "mkvol cmd" }

            vol_id      : contains the volume currently part of
            volume group.
            mkvol cmd   : contains the cli command to create backup
            volume with same
    """

```

```

                                characteristics as vol_id
"""

vols = {}
volgrp_matched = False
ctr = 0

for line in all_vdisks.strip().split("\n"):

    if line != None:

        try:

            key = line.split(",")[0]
            val = line.split(",")[1]

            if key == 'id' :

                vol_id = val

            elif key == 'IO_group_id' :

                iogrp = val

            elif key == 'capacity' :

                size = val

            elif key == 'volume_group_name' and val == vol_group :

                volgrp_matched = True

            elif key == 'preferred_node_id' :

                pref_node = val

            if volgrp_matched :

                epoch = datetime.datetime.now().strftime('%s')
                bk_vol_name = 'bk_' + str(epoch) + '_' + str(ctr)
                mkvol = '-pool {0} -iogrp {1} -size {2} -unit b -preferrednode
{3} -name {4}' . format(sgc_pool_name, iogrp, size, pref_node, bk_vol_name)

                vols[vol_id] = mkvol
                ctr += 1

                volgrp_matched = False

            elif key == 'safeguarded_mdisk_grp_name' :

                vol_id = ""
                iogrp = ""
                size = ""
                volgrp_matched = False
                pref_node = ""

```

```

        except IndexError:
            pass

    print("\nFound {0} volumes protected with volume group {1}\n" .
format(ctr,vol_group) )

    return vols

def getNextFcMap( all_fcmaps ):
    """
    Purpose: This function returns a string value
             containing next fcconsistency group name

    Prameters:

    - IN
      1. Comma separated lines with newline

    - OUT
      String containing fcconsistency group name
    """

    # loop thorough all_fcmaps ouput
    for line in all_fcmaps.strip().split("\n"):

        # skip the header line
        if re.search('^id', line):
            next
        else:
            fcmap_id = line.split(",")[0]# get fcmap_id
            fcmap_name = line.split(",")[1]# get fcmap_name

    return 'fcmap' + str(int(fcmap_id) + 1 )# return last fcmap_id + 1

def runSGCbackup( vdisks_per_volgroup, next_fcmap ):
    """
    Purpose      : This function triggers a series of cli commands
                   as part of safeguarded backup
    Parameters :
    - IN
      1. vdisk_per_vol_group - dictionary containing vol_id
         and mkvolume command
      2. next_vcmap - string containing fcconsistency group name
    """

    global simulation

    # Step 1 : Create a FCConcistency Group
    #          This is done once per entire SGC execution

    fcconsistgrp_name = 'qradar-' + next_fcmap
    mkfcconsistgrp_cmd = 'svctask mkfcconsistgrp -name ' + fcconsistgrp_name

```

```

print( "Step 1 : Creating Flashcopy Consistency group : {0} " .
format(fcconsistgrp_name) )

if not simulation:
    runCli( mkfcconsistgrp_cmd )
else:
    print( 'Simulating command => {0} \n' . format(mkfcconsistgrp_cmd) )
    print( '-' * 30 )
    print( '\n')

# Step 2 : Create a backup volume per source vdisk

bk_vol_id = 9999# initialize with simulation value
copyrate = 0# initialize copyrate to 0

startfcconsistgrp_cmd = 'svctask startfcconsistgrp -prep -retentiondays 15 ' +
fcconsistgrp_name

for vol_id in vdisks_per_volgroup :

    # generate command to create a single volume
    mkvol_cmd = 'svctask mkvolume ' + vdisks_per_volgroup[vol_id]

    if not simulation:

        print( "Step 2 : Creating backup volume ")
        output = runCli( mkvol_cmd )

        # From above output retrieve the volume_id of the newly created volume
        for line in output.strip().split("\n"):
            x = line.split(" ")[2].replace('[','').replace(']',',')

        # overwrite the simulation value with actual output
        bk_vol_id = x

        print( "Backup volume created id = {0} " . format(bk_vol_id) )

        # Step 3 : Create a FCmap command per source & target volume
        # note : copyrate hardcoded to 10.

        mkfcmap_cmd = ( 'svctask mkfcmap -source {0} -target {1} -consistgrp {2}
-coprate {3} ' \
            . format( vol_id, bk_vol_id, fcconsistgrp_name, copyrate ) )

        print( "Step 3 : Creating fcmap per source [{0}] and target [{1}] volume
" . format(vol_id,bk_vol_id) )
        runCli( mkfcmap_cmd )

    else:

        print( "Step 2 : Creating backup volume ")
        print( 'Simulating command => {0} \n' . format(mkvol_cmd) )

```



```

        mkfcmap_cmd = ( 'svctask mkfcmap -source {0} -target {1} -consistgrp {2}
-copyrate {3} ' \
        . format( vol_id, bk_vol_id, fcconsistgrp_name, copyrate ) )

        print( "Step 3 : Creating fcmap per source [{0}] and target [{1}] volume
" . format(vol_id,bk_vol_id) )
        print( 'Simulating command => {0} \n' . format(mkfcmap_cmd) )

        print( "Step 4: Starting copy sequence per volume using {0} flashcopy
consistency group" . format(fcconsistgrp_name) )

        if not simulation:
            runCli( startfcconsistgrp_cmd )
        else:
            print( 'Simulating command => {0} \n' . format(startfcconsistgrp_cmd) )
            print( '-' * 30 )
            print( '\n')

def loadData( csvfile ):
    """
        Purpose: This function loads the output from lsvdisk/lsmdisk commands to
        simulate
                backup when the script is executed in simulation mode

        Parameters:

            - IN : csvfile from svc/flashsystem with vdisk/mdisk output
            - OUT: loaded file contents in a string variable
    """

    try:

        print("Loading {0} for simulation" . format(csvfile) )

        f = open(csvfile,'r')
        data = f.read()
        f.close()

    except FileNotFoundError:

        print("\n\tError !! Unable to load {0} for simulation \n" . format(csvfile))
        print("\n\tcheck script usage for running simulation" . format(csvfile))

    return data

def main():

    global vol_group, simulation

    # Note : the script considers FIRST child pool found in
    #         lsmdiskgrp output defined as safeguarded=yes
    #         even if multiple pools are defined, they are ignored.
    #         also, the free capacity from the pool is not considered

```

```

#         before creating target volumes.

lsmdiskgrp_cmd = 'for x in $(lsmdiskgrp -delim , | grep -v ^id | cut -d , -f
1); do lsmdiskgrp -delim , $x; done'
lsvdisk_cmd = 'for x in $(lsvdisk -bytes -delim , | grep -v id | grep -v bk_ |
cut -d , -f 27); do lsvdisk -bytes -delim , $x; done'
lsfcmap_cmd = 'lsfcmap -delim , | grep -v ^id'

# Step 1 :
# - Get the first safeguard pool defined on the system
# - Get all the vdisks defined on the system
# - Get all the fcmaps defined on the system

if not simulation:

    # Step 0 : get the pools defined on the system
    all_mdisk = runCli( lsmdiskgrp_cmd )

    # Step 1 : get detailed properties of all volumes from the system
    all_vdisks = runCli( lsvdisk_cmd )

    # Step 3 : get the fcmap information from the system
    all_fcmaps = runCli( lsfcmap_cmd )

else:# we are in simulation mode

    # load the csv files captured before.
    all_mdisk = loadData("lsmdiskgrp_detail.csv")
    all_vdisks = loadData("lsvdisk_detail.csv")
    all_fcmaps = loadData("lsfcmaps.csv")

    # get the child pool name with safeguard=yes property
    sgc_pool_name = getSafeguardedPoolName( all_mdisk )

    # Abort execution if no safeguard pool is found
    if sgc_pool_name == None:

        print("Abort !! No SafeguardedCopy pool has been defined ")
        sys.exit(1)

    # Step 2 : Filter only vdisks configured with volume group with
    #         SafeguardedCopy policy

    # get list of vdisks belonging to the volume group we want to backup
    vdisks_per_volgroup = getVdisksPerVolGroup( all_vdisks, vol_group,
sgc_pool_name )

    # Abort if no vdisks are found for given group
    # possible cause:
    # - wrong volume_group_name
    # - vdisks not yet part of volume group

    if not vdisks_per_volgroup:
        print("Abort !! No volumes are protected with volume group {0}\n" .
format(vol_group) )

```

```

        sys.exit(1)

    # Step 3 : Generate the next FCMAP information used for SGC
    # get the next fcmmap
    next_fcmap = getNextFcMap( all_fcmaps )

    # Step 4 : Run backup for each volume we have safeguarded in
    #           the given volumegroup

    runSGCbackup( vdisks_per_volgroup, next_fcmap )

if __name__ == '__main__':

    argc = len(sys.argv) - 1

    if argc < 2 or sys.argv[1] == '-h':
        usage()

    svc_system = sys.argv[1]# svc_system FQDN/IP
    vol_group   = sys.argv[2]# volume group to backup

    remote_usr = 'qradaradmin'# QRadar user defined on SVC
                    # with Securityadmin / Administrator role

    try:
        simulation = os.environ['simulation']
    except KeyError:
        simulation = False

    if simulation:
        print(" *** Simulation {0} *** " . format(simulation) )

    main()

# function call order and parameters
# main()
# - all_mdisk = runCli( lsmdiskgrp_cmd )
# - all_vdisks = runCli( lsvdisk_cmd )
# - all_fcmaps = runCli( lsfcmap_cmd )
# - sgc_pool_name = getSafeguardedPoolName( all_mdisk )
# - vdisks_per_volgroup = getVdisksPerVolGroup( all_vdisks, vol_group,
sgc_pool_name )
# - next_fcmap = getNextFcMap( all_fcmaps )
# - runSGCbackup( vdisks_per_volgroup, next_fcmap )
# - runCli( mkfcconsistgrp_cmd )
# - runCli( mkvol_cmd )
# - runCli( mkfcmap_cmd )
# - runCli( startfcconsistgrp_cmd )

```

Brute force login attack generation

This section describes how the attack that was used in our lab was created on the application to simulate brute force login attempts.

Example 3 shows a sample script that was used to generate false logins for the applications. The script performs a POST operation with username and password fields that are populated with false data. When the login fails, a Login failed via web event is generated and sent to IBM QRadar. All the Login failed via web events were tagged with the Gallery keyword to uniquely identify them.

Example 3 Brute force login attack

```
for(( x=1; x<=15; x++))
do
    curl -d "user=hsk${x}&pass=pass0rd${x}" -X POST -H "Content-Type:
application/x-www-form-urlencoded"
http://k8s-master-01:8080/qr-gallery/php/auth.php
    sleep 5
done
```

The series of Login failed via web events that are received by IBM QRadar act as a trigger for running the multi-app-login-failure rule. This rule, in turn, starts the predefined custom action msgsgcbkup.py script. The script logs on to the IBM FlashSystem and runs a series of operations to generate a Safeguarded Copy. This execution flow is shown in Figure 46 and Figure 47 on page 41.

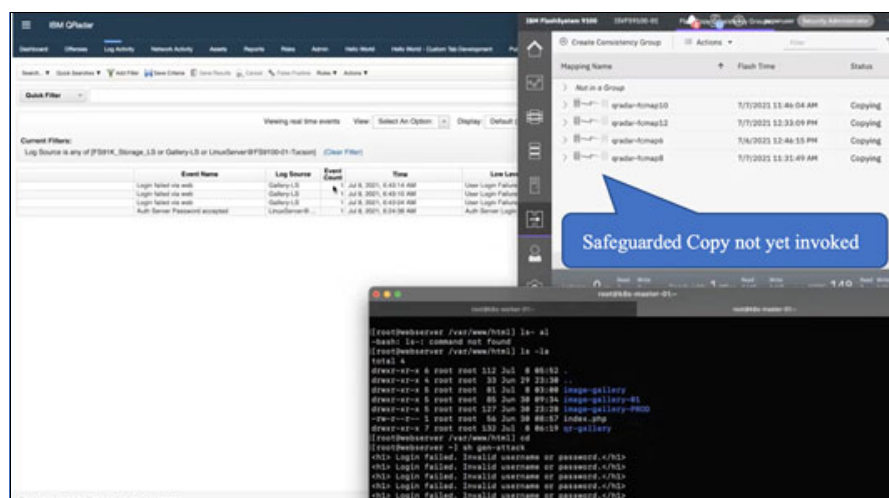


Figure 46 Brute force login attack in progress

A local storage user or a centralized user must be available for connection to the storage system. For our lab setup, a local storage user, csmadmin, was used for authentication, as shown in Figure 48.

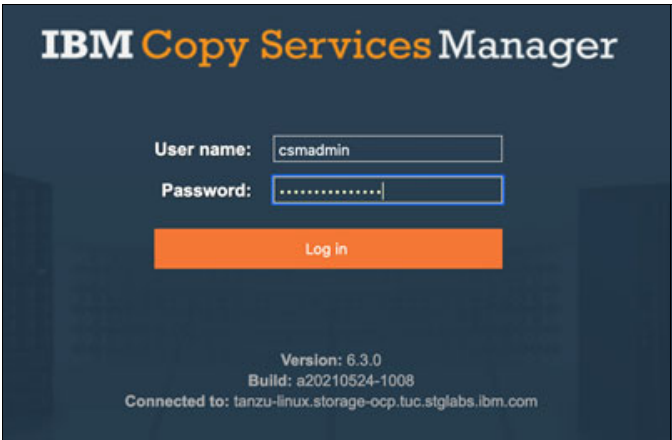


Figure 48 Copy Service Manager login window

Figure 49 shows the FlashSystem that was registered in Copy Services Manager.

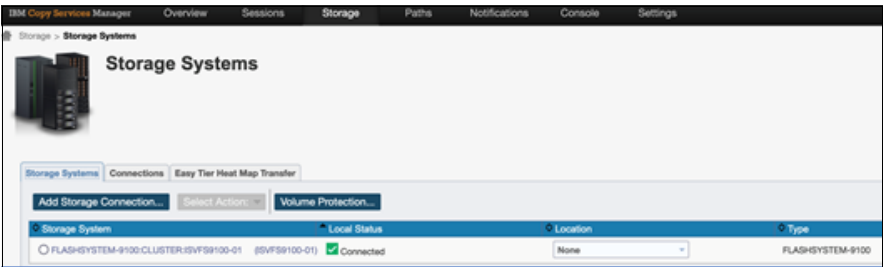


Figure 49 Storage system registered in Copy Service Manager

For the Copy Services Manager, an active session with storage system is required to start a backup, restore, or recover, as shown in Figure 50.

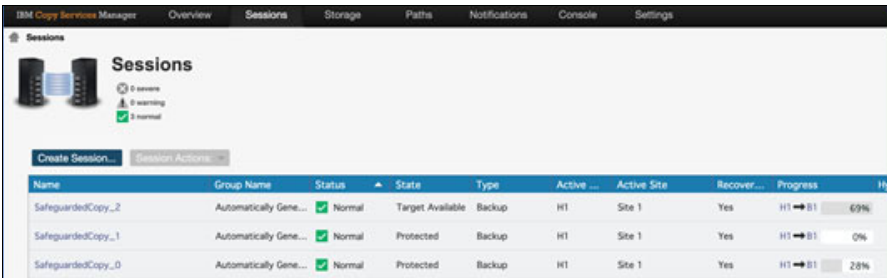


Figure 50 Session details in Copy Services Manager

A list of backups that are available for restoring or recovering can be obtained by selecting one of the sessions that are listed, as shown in Figure 51.

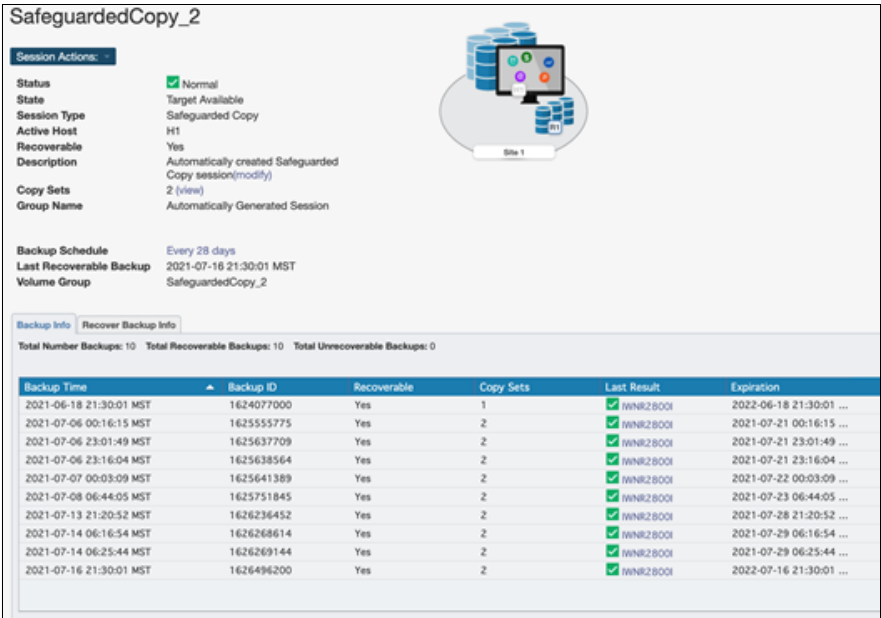


Figure 51 List of backups available for a specific session

The recovery or restore operation is possible on backup sets that are listed with a Yes value in the Recoverable column. The Recover Backup Info tab lists all the backups that were restored or recovered, as shown in Figure 52.

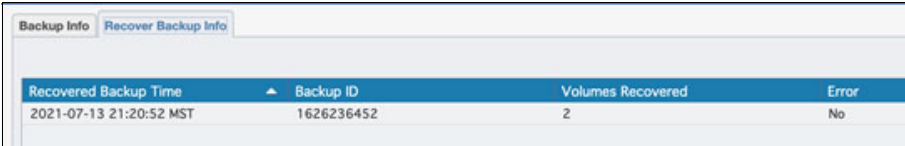


Figure 52 Recover Backup Info tab view

Summary

The solution that is described in this paper shows the integration of IBM QRadar and IBM FlashSystem SafeguardedCopy feature. This integration helps with early threat detection and creating an instantaneous immutable copy of a single volume or group of volumes.

IBM QRadar can receive events from various sources, normalizes them, and uses the data from these events to run various rules to detect any type of anomaly. The rules also are used to trigger a wanted response on the detected threat.

The IBM FlashSystem Safeguarded Copy feature is used to create immutable copies of volumes that are based on a defined safeguarded policy or in an ad hoc manner.

The solution that is described in this paper also shows control and data path use cases and the rules that are associated with them.

The paper also describes the configuration steps to enable IBM FlashSystem Safeguarded Copy feature, event processing in IBM QRadar, and the use of Copy Services Manager to restore or recover the wanted volumes.

The other artifacts that are provided in this paper, such as Python script or IBM QRadar sample rules, were tested in the IBM Lab. No guarantee is given that these artifacts work as when they are deployed in customer environment. Readers are encouraged to create their own response scripts or rules by reviewing the samples scripts and rules that are provided in this paper.

Author

Shashank Shingornikar is a Storage Solutions Architect with IBM Systems, ISDL Lab Pune, India, for the past 12 years. He has worked extensively with IBM Storage products, such as IBM Spectrum Virtualize, IBM FlashSystems, and IBM Spectrum Scale building solutions that combine Oracle and Redhat OpenShift features. Currently, 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 database technologies, such as Oracle, MSSQL, and MySQL.

Acknowledgments

The author wishes to thank the following people for their support in the production of this publication:

Oiza Dorgu
Yves Santos
Julio Cesar Hearnandez
Sandeep Patil
Pradip A. Waykos
Hemant Kantak
Hemanand Gadgil
Chris Daniel
Ajinkya Nanavati
Mandar Vaidya

IBM Systems

Sridhar Muppidi
Adam Frank
Boudhayan Chakrabarty
Ashish M Kothekar
Praphullachandra Mujumdar
Prateek Jain

IBM Security

Appendix A

This section describes the configuration that was created for rsyslog daemon on the web server.

A configuration file that is specific to the application was created in the /etc/rsyslog.d folder with the configuration options that are shown in Figure 53 (the rsyslog version that was used for the configuration was rsyslog-8.24.0-57).

```
[root@webserver /etc/rsyslog.d] cat qr-gallery.conf
# -- for safeguarded copy

module(load="imfile" PollingInterval="5")

if $syslogfacility-text == 'local0' and $msg contains 'gal' then
/var/log/gallery_error.log

input(type="imfile"
      File="/var/log/gallery_error.log"
      Tag="gal"
      Severity="error"
      Facility="local4")

local0.* action(type="omfwd" target="9.11.82.84" port="514" protocol="tcp")
```

Figure 53 rsyslog version rsyslog-8.24.0-57 is used

QRadar deployment model availability

Table 2 lists hardware and software configurations for the IBM QRadar based on capacity requirements.

Table 2 Hardware and software configurations

Size	MT/M	Appliance (All-in)	Characteristics
Small (Maximum EPS 5,000)	4563-Q3E	3105	Storage: 6 TB, Memory: 64 Gb (4x 16 Gb), Emulex 16 Gb FC
Medium (Maximum 15,000)	4563-Q4A	3129	Storage: 59 TB, Memory: 64 Gb (4x 256 Gb), Emulex 16 Gb FC
Large (Maximum 30,000)	4654-Q4B	3148	Storage: 12 TB, Memory: 128 Gb (4x 256 Gb), Emulex 16 Gb FC

Resources

For more information, see the following resources:

- Configuring User Roles on IBM FlashSystem:
<http://www.ibm.com/docs/en/flashsystem-9x00/8.4.0?topic=overview-user-roles>
- Adding custom actions to IBM QRadar:
<http://www.ibm.com/docs/en/qsip/7.4?topic=tasks-adding-custom-actions>
- IBM Copy Services Manager:
<https://www.ibm.com/docs/en/csm>

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.

Redbooks (logo) ®
DS8000®
IBM®

IBM FlashSystem®
IBM Security™
IBM Spectrum®

IBM Watson®
QRadar®

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.

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

August 2021

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



Please recycle

ISBN 0738459941

REDP-5655-00