IBM® Storage

Proactive Early Threat Detection and Securing Oracle Database with IBM QRadar, IBM Security Guardium Database Protection, and IBM Copy Services Manager by using IBM FlashSystem Safeguarded Copy

IBM Storage Team

Contents

About this document

This IBM® blueprint publication focuses on early threat detection within a database environment by using IBM Security® Guardium® Data Protection and IBM QRadar® . It also highlights how to proactively start a cyber resilience workflow in response to a cyberattack or potential malicious user actions.

The workflow that is presented here uses IBM Copy Services Manager as orchestration software to start IBM FlashSystem® Safeguarded Copy functions. The Safeguarded Copy creates an immutable copy of the data in an air-gapped form on the same IBM FlashSystem for isolation and eventual quick recovery.

This document describes how to enable and forward Oracle database user activities (by using IBM Security Guardium Data Protection) and IBM FlashSystem audit logs by using IBM FlashSystem to IBM QRadar.

This document also describes how to create various rules to determine a threat, and configure and launch a suitable response to the detected threat in IBM QRadar.

The document also outlines the steps that are involved to create a Scheduled Task by using IBM Copy Services Manager with various actions.

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.

IBM Security Guardium Data Protection offers solutions to protect sensitive and regulated data by continuously monitoring the data activity and accelerating compliance reporting that supports a zero trust approach to data management across environments, lifecycles, and platforms.

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

IBM QRadar is a security information and event management (SIEM) and threat management system that monitors activities while looking for signs that might indicate the start of an attack, such as logins from unusual IP addresses or outside business hours.

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

The IBM FlashSystem Safeguarded Copy function helps businesses recover quickly and safely from a cyberattack, which helps reduce recovery to minutes or hours. It also 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.

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

Scope

The focus of this document is to showcase the early threat detection in the form of potential malicious user actions, and database administrator's actions on Oracle database by using IBM Security Guardium Data Protection. The database host uses storage that is mapped from IBM FlashSystem.

When potential malicious database activities are detected by IBM Security Guardium Data Protection, IBM FlashSystem storage audit events are forwarded to IBM QRadar by using the preconfigured rules in IBM QRadar. The event data is analyzed to not only detect a potential threat, but also to proactively start Safeguarded Copy to create an immutable backup.

The IBM Copy Services Manager scheduled task function starts a predefined scheduled task with many actions. Although not covered here, IBM Copy Services Manager also can be used to recover or restore the backup by using only a few steps.

As part of early threat detection, several rules are described in this publication. Also, a sample Python script is used to start the Safeguarded Copy action that is provided. This document also explains several sample control path and data path use cases.

Customers are encouraged to create control path and data path use cases, customized IBM Security Guardium Data Protection policies, IBM QRadar rules, and custom response scripts that are best-suited to their environment.

Although the use cases, rules, and Python script from this publication can be seen as templates, they cannot be used in a real-world environment.

The solution that is featured in this document is created by using the following products:

- IBM Security Guardium Data Protection 11.4
- IBM QRadar release 7.4.2
- IBM FlashSystem 7.4.x
- BM Copy Services Manager 6.3

IBM Copy Services Manager Scheduled task sample workflow also is explained as part of the solution, which includes the following process:

1. Copying or mirroring of volumes is suspended.
2. The user waits for a confirmation of that suspension.
3. Safeguarded Copy is started.
4. Copying or mirroring of the volumes resumes.

Note: All components that are described in this blueprint, such as, IBM Security Guardium Data Protection, IBM QRadar, IBM Copy Services Manager, and IBM FlashSystem are in same network segment. Suitable network planning is required if these systems are in different network.

For more information about IBM QRadar, IBM FlashSystem, Safeguarded Copy, IBM Copy Services Manager, and IBM Security Guardium Data Protection, see "Resources" on page 38.

Introduction

Combining the capabilities of IBM FlashSystem Safeguarded Copy and IBM QRadar, IBM Security Guardium Data Protection enables enterprises to build comprehensive cyber resilience solutions that address the protect and recover functions of the NIST framework and the detect and respond function.

IBM FlashSystem can log all administrative activities in the access logs, which have all of the 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.

IBM QRadar can provide full protection to the enterprise data by combining IBM FlashSystem administration access logs, application logs, network or server logs, flow, packet data, and database events that are forwarded by IBM Security Guardium Data Protection.

IBM FlashSystem Safeguarded Copy function

The IBM FlashSystem Safeguarded Copy feature creates safeguarded backups that are not accessible by the host system. It also protects these backups from corruption that can occur 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 backups also affects performance less than the multiple target volumes that are created by IBM FlashCopy.

Note: The Safeguarded source volume cannot be removed before the Safeguarded backups are deleted.

The Safeguarded Copy function provides backup copies to recover data if a logical corruption occurs or primary data is destroyed.

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 duration that 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 is a Metro Mirror, Global Mirror, or IBM z/OS® Global Mirror primary or secondary volume, or a simplex 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 typically is thin-provisioned; however, it does not have to be thin-provisioned.

Managing Safeguarded Copy is supported by Copy Services Manager 6.2.3 or later. The management software helps to create and recover backups and define policies for expiration.

IBM Security Guardium Data Protection

IBM Security Guardium Data Protection empowers security teams to safeguard sensitive data through discovery and classification, data activity monitoring, vulnerability assessments, and advanced threat detection. These features extend comprehensive data protection across heterogeneous environments, including databases, data warehouses, mainframes, file systems, file shares, cloud, and big data platforms.

IBM Security Guardium Data Protection continuously monitors all data access operations in real time to detect unauthorized actions that are based on detailed context; that is, the “who, what, where, when, and how” of each data access. It reacts automatically to help prevent unauthorized or suspicious activities by privileged insiders and potential hackers.

IBM Security Guardium Data Protection security suite provides the following capabilities to commission a successful data security strategy:

- Session-level policy (SLP):
  - Improved performance because validation occurs at the beginning of sniffer processing, which decreases the load on the data-security policy (DSP). SLPs are evaluated before DSP policies.
  - Earlier evaluation of SLPs allows you to detect a user’s suspicious behavior and alert you about security incidents before a connection is created.
  - Extended set of criteria and actions that are not available in a DSP.
  - An SLP has connection metadata available (as encryption types and an admin session) that is not available in a DSP and not passed to a DSP.
  - Default SLP templates on Guardium:
    - Security anomalies
    - Security incidents: administrative users and applications
    - Security incidents: all users
    - Security incidents: credential stuffing attack
    - Security incidents: repeated failed logins or possible denial of service attack
  - Blocking with an SLP: The main difference between blocking that is configured in a DSP and in an SLP is that an SLP allows you to terminate a connection attempt before a connection is established. DSP can terminate only after the first query within a session.

Figure 1 illustrates blocking by using an SLP.

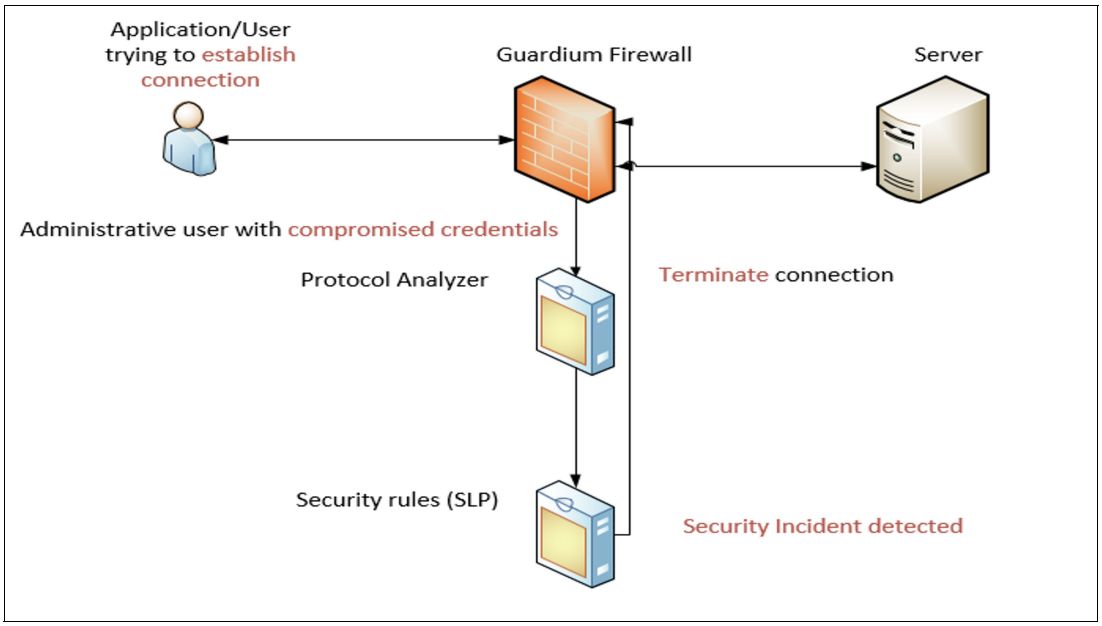

Figure 1 Blocking by using an SLP

- Real-time trust evaluation: The Real-time Trust Evaluator (RTTE) evaluates the application connections that are monitored by Guardium. Connections are classified as ‘untrusted’, ‘evaluated’, or ‘trusted’. Trust scores (0 - 100) are assigned to each classified connection. Connections that are not classified as trusted or untrusted are classified as evaluated.

  The trust evaluator release consists of three main modules:

  – *Security incident policies* that detect denial-of-service attacks, credential-stuffing attacks, password-spraying attacks, and connection authentication vulnerabilities, which means the offending connection can be terminated before it physically establishes, and the result of the connection check will be unknown.

  – *Probabilistic engine* (probability engine), which is based on a Bayesian machine learning model. This model requires a long training period. The training status is displayed in the user interface so that you can follow it.

  – *Anomaly detection*, which is based on a special machine learning model. Visually, anomaly detection is represented as a list of anomaly conditions. This model requires a short training period, and the training status is not displayed.

Figure 2 on page 7 shows the RTTE architecture.

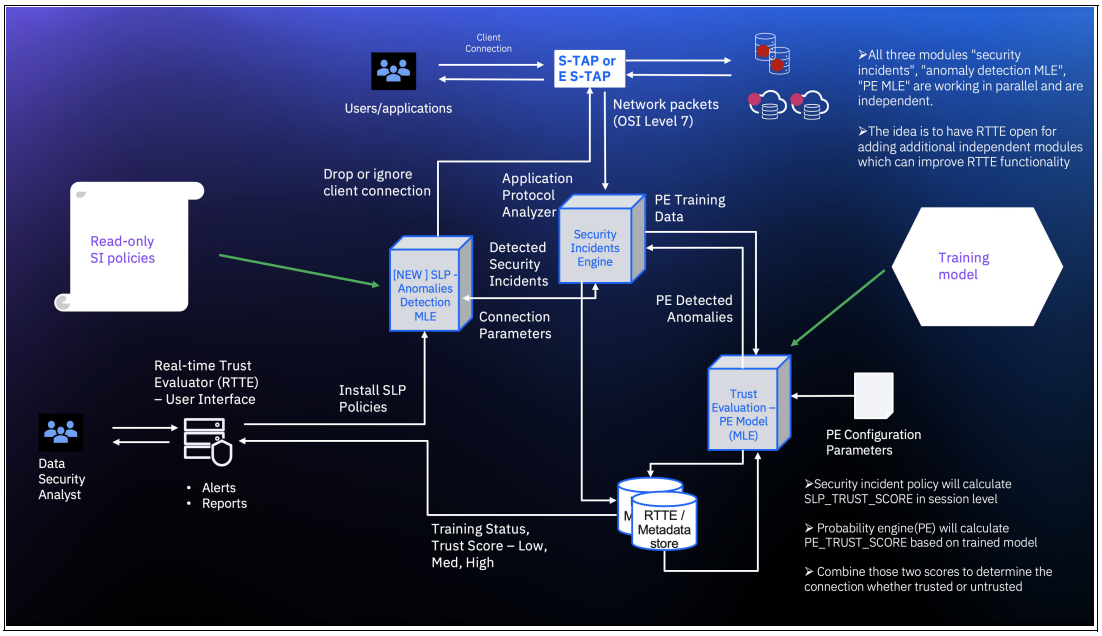

Figure 2 RTTE architecture

- Real-time sensitive object identification: Real-time identification of sensitive objects in the response data of the monitored data source.
- Redaction capabilities: Selectively mask portions of a query's output, which also is referred to as *data scrubbing*. This capability is essential to protecting sensitive data from unauthorized access.
- Blocking capability: Provides extra layer of protection for sensitive information. This feature enables fine-grained access control for the insiders to ensure that zero data leakage occurs.
- Adaptive policy rules: Can be tailored per business, compliance, or regulatory requirements.

IBM Copy Service Manager

IBM Copy Services Manager controls copy services in storage environments. *Copy services* are features that are used by storage systems (such as IBM FlashSystem) to configure, manage, and monitor data-copy functions.

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

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

IBM Copy Services Manager provides a GUI, a command-line interface (CLI), and Representational State Transfer (RESTful) API for managing data replication and disaster recovery.

Staring with IBM Copy Services Manager 6.3, the online help also integrates with the RESTful API.

IBM QRadar Security Intelligence Platform

IBM QRadar Security Intelligence Platform products provide a unified architecture for integrating security information and event management (SIEM), log management, anomaly detection, incident forensics, and configuration and vulnerability management.

It is one of the most popular SIEM solutions on the market today. It provides powerful cyber resilience and threat detection features, such as centralized visibility, flexible deployment, automated intelligence, machine learning, and proactive threat hunting.

IBM QRadar can detect malicious patterns by using various 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. Its open architecture enables third-party interoperability so that many solutions can be integrated, which makes it even more scalable and robust.

To apply the security and compliance policies, IBM QRadar administrators can perform following tasks:

- Search event data by using specific criteria and display events that match the search criteria in a results list. The columns of event data can be selected, organized, and grouped.
- Visually monitor and investigate flow data in real time, or perform advanced searches to filter the displayed flows. The flow information can be viewed to determine how and what network traffic is communicated.
- View all of the learned assets or search for specific assets in the environment.
- Investigate offenses, source, and destination IP addresses, network behaviors, and anomalies in the network.
- Edit, create, schedule, and distribute default or custom reports.

Prerequisites

The following prerequisites must be met for the solution:

- The firewall rules between IBM QRadar and IBM FlashSystem storage are adjusted to allow traffic on 514/TCP or 514/UDP. Also, the firewall rules are adjusted to allow traffic between IBM QRadar host and IBM Copy Services Manager on port TCP/9595.

  Note: IBM QRadar accepts incoming events on TCP/UDP protocol on port 514. The choice of protocol that is used for communication depends on organization's guidelines.

- IBM Security Guardium Data Protection is installed and configured to send events to IBM QRadar in Log Event Extended Format (LEEF) format. The events are sent to IBM QRadar by using Syslog protocol.
- A Policy configuration is available that consists of various rules that are aimed to capture any specific database action.

- A running Oracle database instance is available. For this solution, Oracle 19c single instance database was used. For more information about supported databases, see the IBM Security Guardium Data Protection documentation.
- IBM Copy Services Manager 6.3 or later is available and the IBM FlashSystem storage is registered in IBM Copy Services Manager by using administrator privileges. For more information, see “Resources” on page 38.
- A scheduled task is defined in IBM Copy Services Manager that consists of various operations, depending on the functions that are used in the storage system. For example, when copy services are used, such as Metro Mirror or Global Mirror, writes to target volumes must be suspended to achieve a consistent state before a Safeguarded Copy backup can be made.
- The safeguarded virtual capacity is provisioned. For more information about configuring safeguarded virtual capacity, see “Resources” on page 38.
- The recovery volume is configured before the safeguarded backup copy session is created in IBM Copy Services Manager.
- Understand IBM FlashSystem storage for working with volumes and safeguarded virtual capacity allotment.

Solution overview

Data is the most important asset of any company. It empowers businesses to make decisions. These decisions determine the future of the business and eventually the organization.

Organizations can face various threats, including the following examples:

- A rogue user within the organization
- Cyberattacks that result in compromised user credentials by using spear fishing attacks
- Brute force attempts
- Ransomware

All of these threats pose grave risks to storage systems that are used for storing the data.

To track the administrative action, the solution implements various control path use cases. To track the changes from application data, a data path use case is described here.

A syslog configuration is created in IBM FlashSystem that allows forwarding of storage events to IBM QRadar. IBM QRadar understands the authorization events that are forwarded by IBM FlashSystem and categorizes them correctly. Other storage-specific events must be mapped to the correct IBM QRadar identifier (QID) for storage-specific operation categorization.

After the events classification is completed, the IBM QRadar administrator can define several rules to detect threats that are categorized under the control and data path. Upon threat detection, a cyber resiliency response is started in the form a Python script that uses API commands to run a predefined IBM Copy Services Manager scheduled task.

The scheduled task feature of IBM Copy Services Manager is chosen because it provides flexibility to run various operations, including conditional execution that is based on specific states of the previously run command.

Figure 3 shows an overview of the solution.

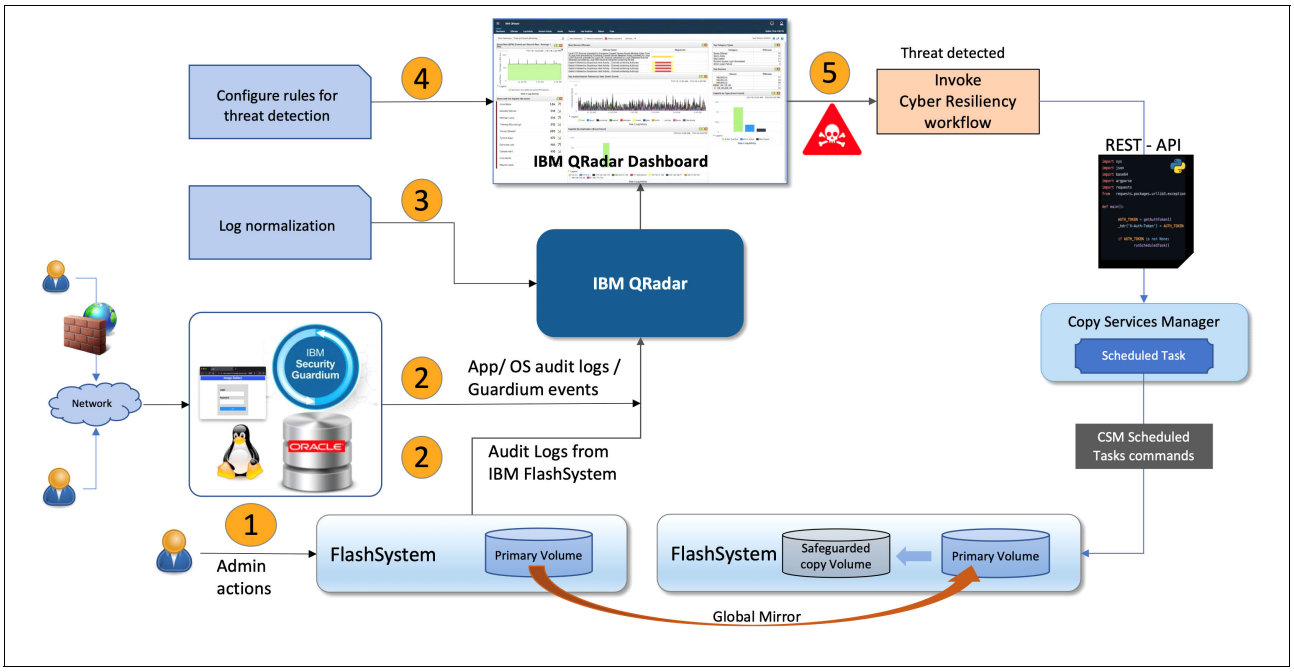

Figure 3 Solution overview

Control path use cases

The sample control path use cases include the following examples. This list by no means is an exhaustive collection, but it generalizes the idea of a threat. Ultimately, the security policy of the organization defines a threat:

- Storage administrator logins that are detected outside of business hours.

  Administrators must always log on to the system to solve an issue. But, what if an administrator is logging on to a system that does not have any open incident tickets? How can this login action be justified? More importantly, how can this action be tracked?

- A database SYS user is logged on from multiple locations or IP addresses at the same time.

  This use case is a classic example of compromised or shared credentials. A legitimate user might be oblivious of the second sessions activity under same login. Moreover, how can the remote SYS logins can be justified? What if one the session is malicious?

- Operating system logins activity.

  Tracking operating system login activity is a major task. Running commands, such as **`unmap`**, can result in dangerous consequences. It can easily go undetected and cause logical corruption on the storage volumes by overwriting the data that is in the volumes.

- Additional control path use cases that Guardium can handle.
  - Not a secure program (uses a plain password).
  - The administrator uses a weak password.
  - The administrative session is not encrypted.
  - Suspicious administrative activity.
  - The program uses a prohibited command.

Data path use case

Figure 4 shows a typical 3-tier application infrastructure with IBM QRadar monitoring telemetry from all of the sources within the environment.

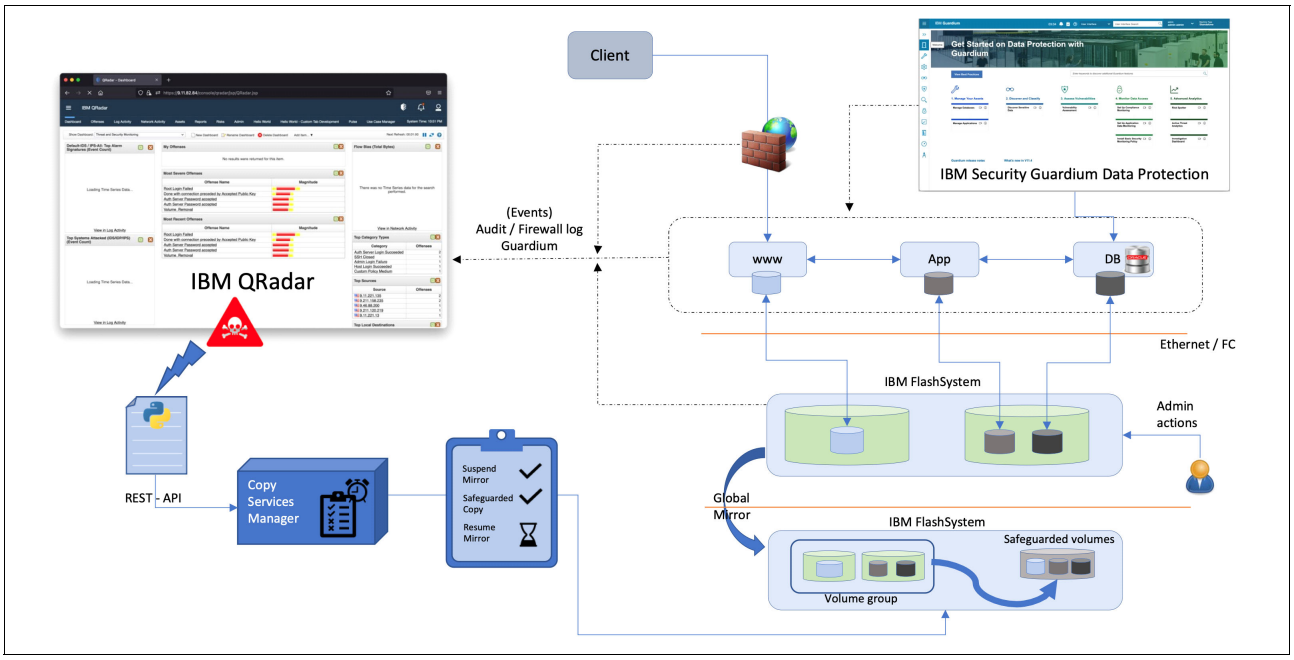

Figure 4 Sample application infrastructure

The addition of IBM Security Guardium Data Protection data protection helps track activities from the Oracle database. Also, the audit log events from hosts web, application, and database tier are used to determine anomalies or threats.

For this solution, several use cases were tracked, such as a brute force login, multiple and remote sys logins, user access to sensitive tables. The events that were captured by IBM Security Guardium Data Protection were sent to IBM QRadar to analyze the threat conditions. The cyber resiliency workflow was started IBM Copy Services Manager scheduled task to create Safeguarded Copy backups by suspending Global Mirror and restarting copy session post backup.

Additional data path use cases

Here are some additional data path use cases:

- A possibly compromised user because of a plain password
- Repeated failed login per SERVER_IP and user
- Too many failed logins from the same program and different DB users
- Password spraying attacks
- Unauthorized access detection
- Credential-stuffing attack
- Repeated failed logins per CLIENT_IP and user.
- Repeated failed logins per ANALYZED_CLIENT_IP and user
- Too many DB users connecting from same client IP address per period
- Too many DB users connecting from same ANALYZED client IP address per period

- Session or response data exfiltration
- Denial of service attack

Lab setup

The lab setup was created by using VMware ESXi that hosts the database server virtual machine. The storage volumes were mapped to ESXi host by using Fibre Channel and a single data store was created. Multiple VMware virtual disks were created in data stores and were mapped to Linux VM as virtual disk devices to store database files, redo logs, and flash the recovery area.

IBM Security Guardium Data Protection data protection appliance was deployed and the Oracle database was registered for monitoring. Also, syslog server in IBM Security Guardium Data Protection was configured to forward the events to IBM QRadar in LEEF format.

A database workload simulator was run on the Linux host to maintain write activity on the primary volumes. The block changes that were induced by writes on primary site traveled downstream with Global Mirror relationship.

Also, audit logging was enabled on both storage systems by using syslog setup. Because IBM QRadar understands the syslog event format, it automatically creates a LinuxServer type log source and the storage events are categorized.

For more information about sample regular expressions that were used to extract various properties from IBM QRadar Event payload to create custom properties to categorize the data, see “Appendix B: Sample regular expressions” on page 37.

Various components that were used in the sample setup are described next.

IBM FlashSystem

On IBM FlashSystem 9100, a Safeguarded Copy child pool was created under the parent pool. The shield icon that is next to the child pool’s name indicates that the child pool is the safeguarded pool (see Figure 5).

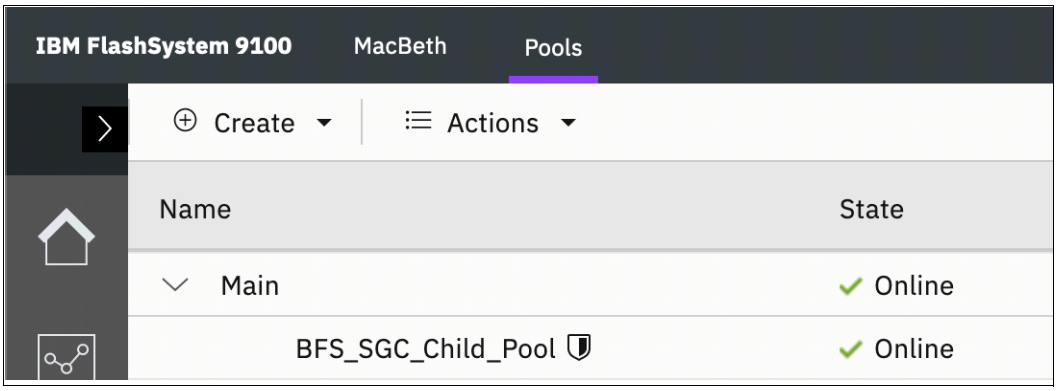

Figure 5 Child pool configured with Safeguarded properties

To make the immutable backups of the database volumes, a volume group was created. A Safeguarded policy also was created and the database volumes were added to the volume group (see Figure 6).

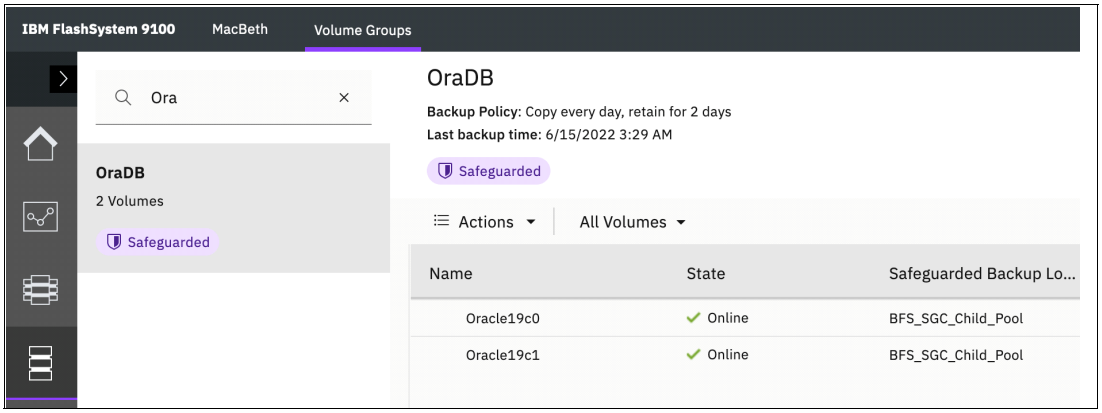

Figure 6 Volume group with Safeguarded copy policy

The volume group with associated safeguarded policies is recognized by IBM Copy Services Manager and a Safeguarded Copy session is automatically created by IBM Copy Services Manager.

For this setup (although not required by the solution), a Remote Copy (Global Mirror) relationship of the database volumes was configured (see Figure 7).

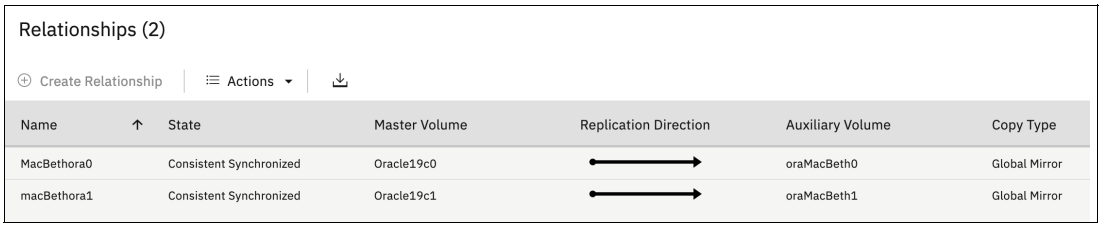

Figure 7 Remote copy relationship for database volumes (Global Mirror)

The remote copy session was introduced to closely simulate a production environment with storage replication. The decision to perform the Safeguarded Copy is largely dependent on the service level agreements (SLA) and compliance policies of the organization.

The solution shows making a Safeguarded Copy on the target storage system that is configured with Global Mirror replication.

Setting up audit log forwarding on IBM FlashSystem

To enable audit log forwarding from IBM FlashSystem to IBM QRadar, complete the following steps:

1. Log in to the FlashSystem GUI.
2. Select **Settings** → **Notifications**, and then click **Add Syslog Server**.

3. Enter the IP address of IBM QRadar host. Choose the facility as required.

   The syslog server that is configured in our lab is shown in Figure 8.

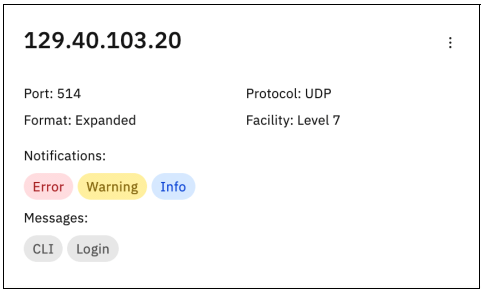

Figure 8 Syslog server configuration on IBM FlashSystem

IBM Security Guardium Data Protection

For the lab setup, IBM Security Guardium Data Protection Release 11.4 was used. This section describes two primary actions that were performed on the IBM Security Guardium Data Protection appliance.

Syslog configuration for IBM Security Guardium Data Protection

The Syslog configuration was created to forward all facilities and all priorities to IBM QRadar. Complete the following steps to configure Syslog:

1. Log on to the IBM Security Guardium Data Protection appliance and run the following commands to view the syslog servers that are configured and to configure syslog shipping to IBM QRadar:
   - View the current remote log store:

     ```
     cli> show remotelog
     ```

   - Ship IBM Security Guardium Data Protection application logs by using default port 514 and all priorities to IBM QRadar:

     ```
     cli> store remote log add daemon.all 129.40.103.20 udp
     ```

For more information about the use of different priorities of Syslog in IBM Security Guardium Data Protection, see “Resources” on page 38.

The IBM QRadar installation immediately supports Syslog messages from IBM Security Guardium Data Protection by using a DSM plug-in. No extra work in IBM QRadar is required for configuring the Log source for IBM Security Guardium Data Protection events.

Using IBM Security Guardium Data Protection policy builder for data

IBM Security Guardium Data Protection policies for data allow defining security policies with various rules. The Cybersecurity policy that is defined in IBM Security Guardium Data Protection is shown here.

Complete the following steps:

1. Log in to IBM Security Guardium Data Protection with user that has permissions to build security policies.
2. Start the Policy Builder for data from the dashboard post login (see Figure 9 on page 15).

Figure 9 Starting policy builder for data from user interface

The location path also shows the menu navigation options.

3. On the Securities Policies window, click **+** to start the policy creation wizard. The Create New Policy window opens (see Figure 10).

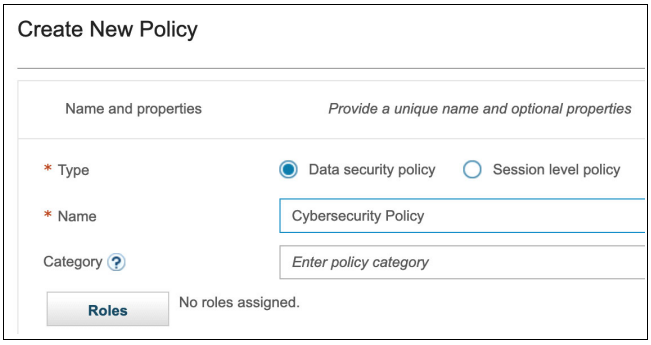

Figure 10 Create New Policy window

4. Click the **Rules** option to expand the view (see Figure 11).

Figure 11 Expanded Rules option window

5. In the expended windows of the Rules option, click **+** to start a new rule definition (see Figure 12).

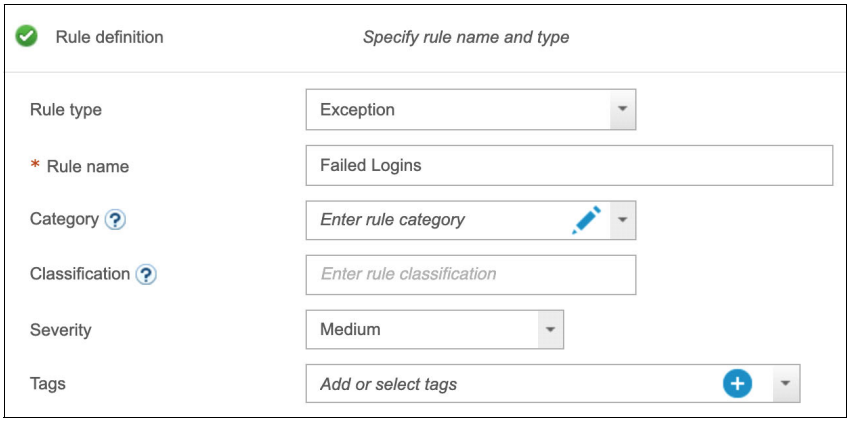

Figure 12 Rule definition window

6. Click **Rule criteria** to expand the section to enter various criteria for the rule (see Figure 13).

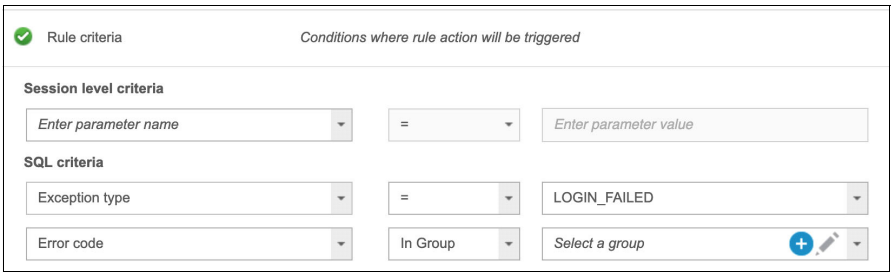

Figure 13 Step 4: Rule criteria window

An In Group expression is used when the rules criteria are defined, which allows defining a list. The list is created from the Select a group combination box by clicking the (**+**) option.

To check invalid for failed logins, a DB Error Codes group type was defined (see Figure 25 on page 22).

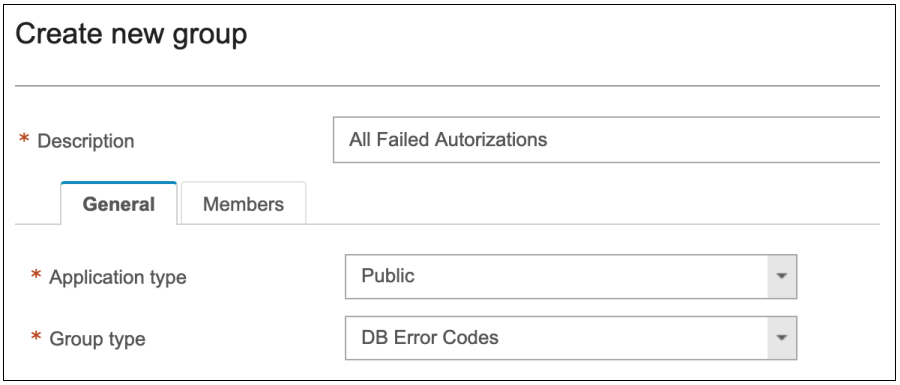

Figure 14 Optional list definition containing multiple values

7. On the **Members** tab, database error codes that are related to failed or invalid logins are defined. Use the Alias column to define an error message that identifies specific codes that are listed in the Member column (see Figure 15).

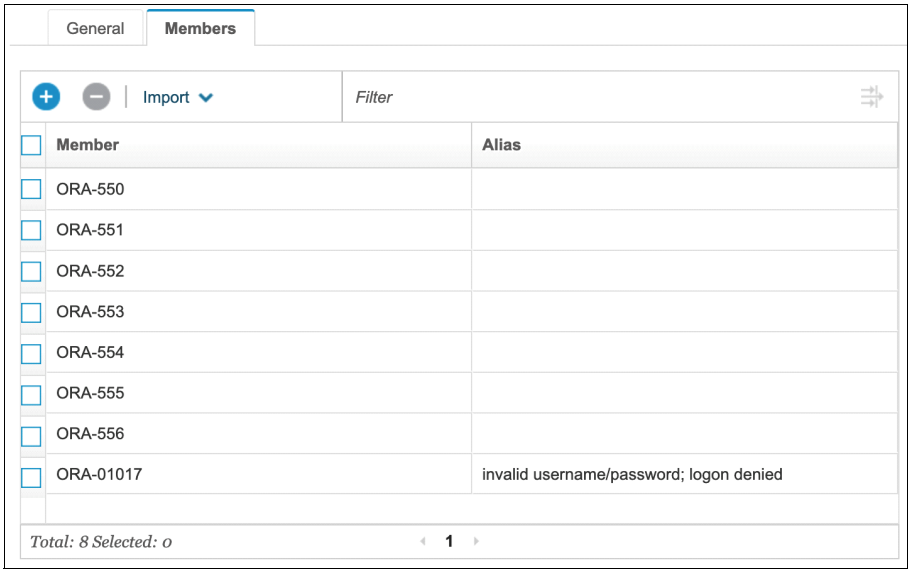

Figure 15 Optional list definition with various values and aliases

The Rule criteria section definition is complete (see Figure 16) after the All failed Authorization list that contains various database error codes is created and selected.

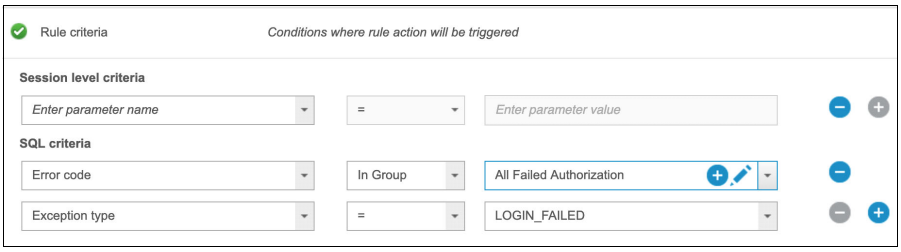

Figure 16 Completed Rules criteria section

8. Click **Rule action** to define the actions to take when the rule conditions are matched. Multiple actions can be defined (see Figure 17).

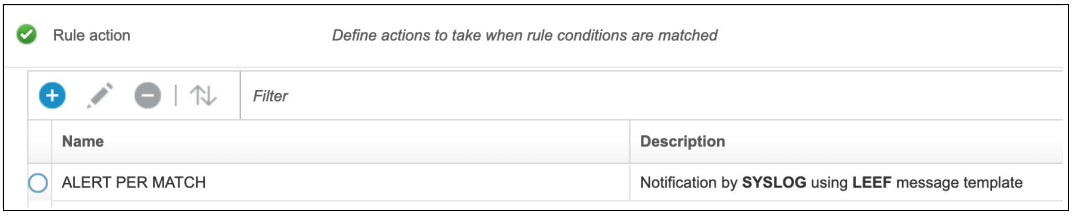

Figure 17 Step 5: Rule action definition

A completed policy with single rule is shown in Figure 18.

Figure 18 Policy definition with single rule

To demonstrate various use cases, multiple rules were added in the lab environment. A complete policy definition with various rules is shown in Figure 19.

Figure 19 Completed Cybersecurity policy with multiple rules

The completed policy must be installed or reinstalled when changes are made so that it becomes active (see Figure 20).

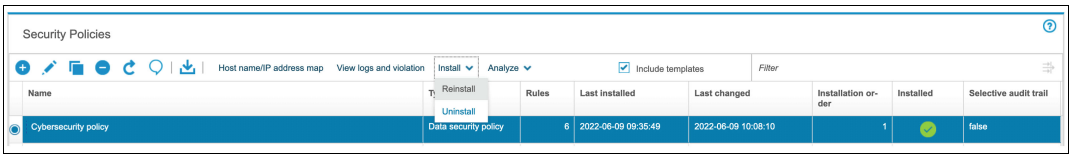

Figure 20 Installing or reinstalling a policy to make changes active

Figure 21 shows the list of session-level rules that can be leveraged to create custom rules according to your business requirements.

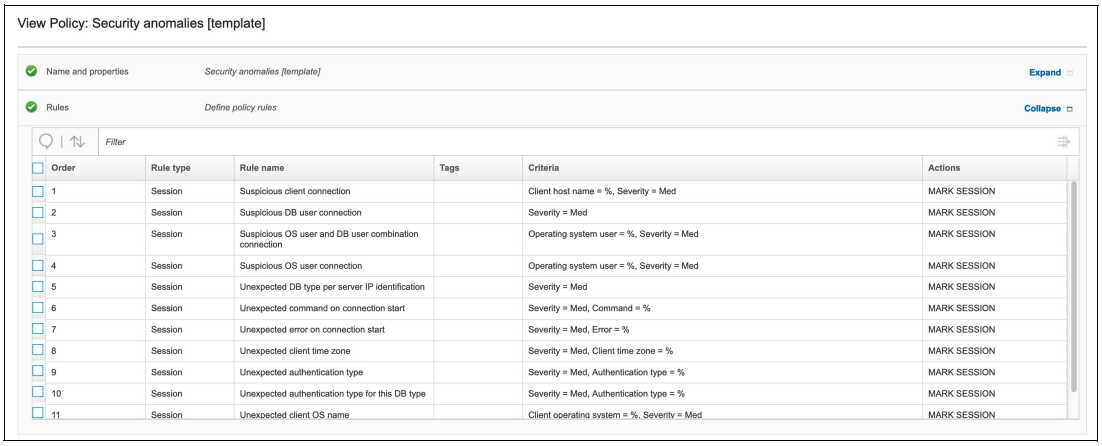

Figure 21 Security anomalies

IBM Copy Services Manager

IBM Copy Services Manager was used to define the Global Mirror replication between the lab hosts. Also, an ad hoc scheduled task was defined to perform multiple actions, such as suspending the Global Mirror copy services session, starting the Safeguarded Copy backup, and resuming the copy services post backup.

Scheduled tasks, sessions, and copy sets are described in this section.

Scheduled tasks

Starting with Copy Services Manager Version 6.2.1, you can use a GUI wizard to schedule tasks. As of this writing, tasks can be scheduled only against sessions. The scheduled tasks can consist of one or more actions, including issuing commands and waiting for states.

The Wait for State action ensures that the next action in the list does not occur until the session is in the correct state. The list of actions that you create in the wizard occur sequentially. Therefore, the Wait for State action delays the next action in the task from running until the specified state is reached. The task fails if the state is not reached.

Session

A *session* completes a specific type of data replication for a specific set of volumes. During data replication, data is copied from a source volume to one or more target volumes, depending on the session type. The source volume and target volumes that contain copies of the same data are collectively referred to as a *copy set*. A session can contain one or more copy sets.

Sessions are referred to as single-target or multi-target:

- With single-target sessions, the source volume site can have only one target site. Data replication occurs from the source to the target.
- With multi-target sessions, the source volume site can have multiple target sites. Data replication can occur from the source to an individual target or to all targets simultaneously.

Copy sets

During the data replication process, data is copied from a source volume to one or more target volumes, depending on the session type. The source volume and target volumes that contain copies of the same data are collectively referred to as a copy set.

The number of volumes in the copy set and the role that each volume plays is determined by the session type that is associated with the session to which the copy set belongs.

For more information, see *IBM Copy Services Manager 6.3 User's Guide*.

Creating Global Mirror session in IBM Copy Services Manager

To introduce the copy services, a single direction Global Mirror session was created between IBM Storwize® V7000 (primary storage) and IBM FlashSystem 9100 (auxiliary storage). The IBM Copy Services Manager GUI wizard was used to create the mirroring session.

Complete the following steps to create the Global Mirror session:

1. Click **Sessions**, and then click **Create Session** and choose or enter the suitable information in the corresponding fields (see Figure 22).

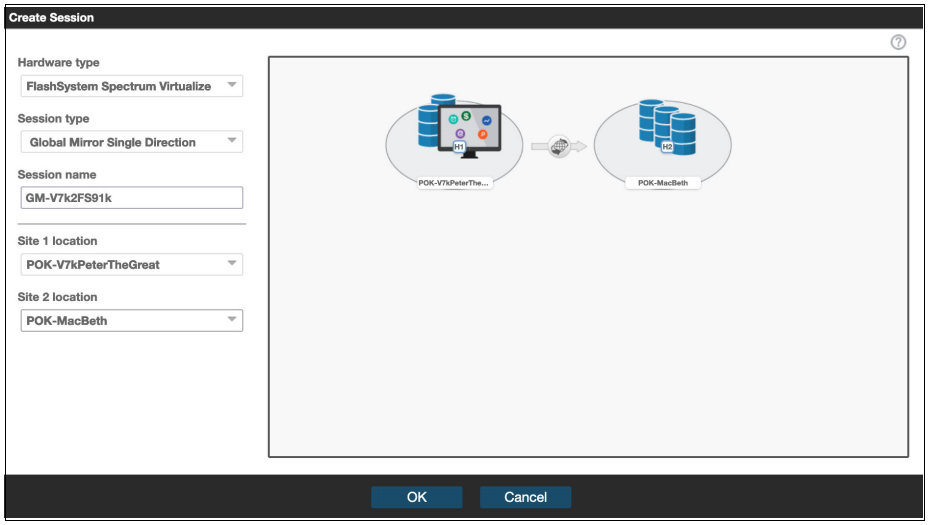

Figure 22 Creating a Global Mirror session

2. IBM Copy Services Manager responds when the session is created. Then, add the copy sets and storage volumes.
3. Click the newly created session, and then click **Session Actions**. Then, from the View/Modify menu, choose **Add copy sets**.
4. IBM Copy Services Manager starts the Add Copy Sets wizard. Select the Host1 storage system, I/O group, and volume from their respective drop-down menus (see Figure 23).

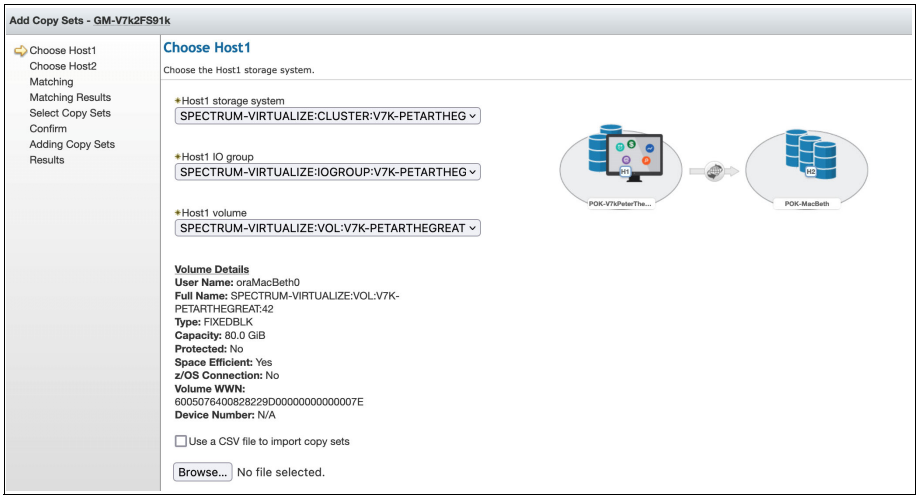

Figure 23 Choose Host1 window

5. Select the Host2 storage system, I/O group, and volume from their respective drop-down menus (see Figure 24).

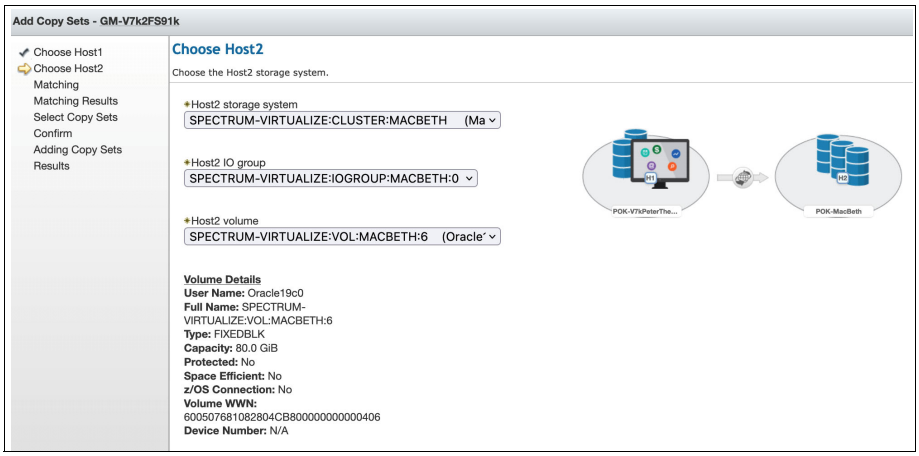

Figure 24 Choose Host2 window

6. IBM Copy Services Manager matches the volumes from both systems and shows the result in the next window. Confirm the volume, and then click **Next**.

   If the selected volume is part of another session, the wizard returns a warning to flag issue.

7. Click **Finish** after the validation warning (if any) is displayed to close the wizard.
8. Repeat this process to add all of the required volumes.
9. Start the mirroring process. Select the session, and then select **Commands** → **Session Actions**. Then, click **Start**.

The initial sync takes some time. After the sync is complete, the session state changes from `Inactive` to `Normal`.

Creating a scheduled task in IBM Copy Services Manager

Complete the following steps to create a scheduled task in IBM Copy Services Manager:

1. Log in to IBM Copy Services Manager and **Settings** → **Scheduled Tasks**, and then click **Create Task** to start the wizard.
2. Enter a name and description for the task, and then click **Next**.
3. Choose the **No Schedule** option in the How often do you want the task to run? window. Click **Next**.
4. In the “What action would you like to perform?” window, click **Add Action**.
5. In the **Type** drop-down menu, select the **Command** option, and then select the Copy Services session name.

6. Select the **Suspend** option from the **Command** drop-down menu, and then click **OK** (see Figure 25).

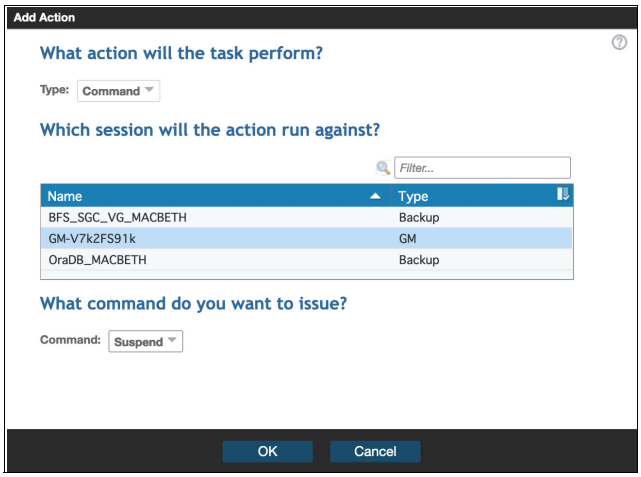

Figure 25 Selecting the Suspend command option

7. Click **Add Action** again and select the **Wait for State** option from the **Type** drop-down menu. Then, select the same **Session Name** from Step 5, select the **Suspended** option from the **State** drop-down menu. Then, enter a timeout value in minutes in the Time field and click **OK** (see Figure 26).

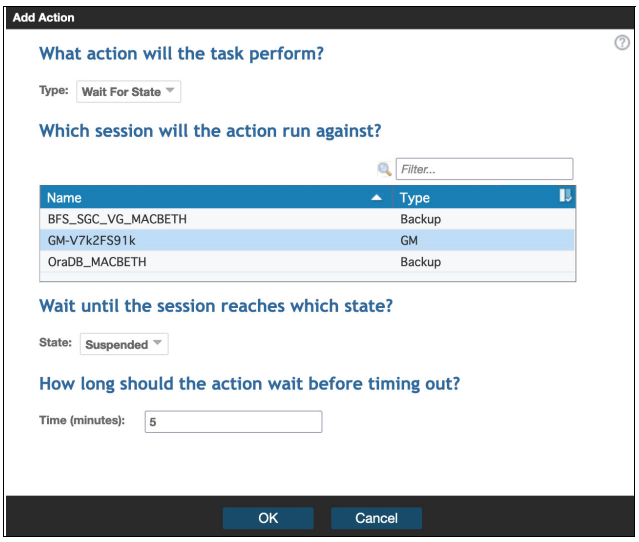

Figure 26 Entering a timeout value

8. Click **Add Action** again and select the **Backup** option from the **Type** drop-down menu. Then, select the **Safeguarded Copy** session name and click **OK** (see Figure 27).

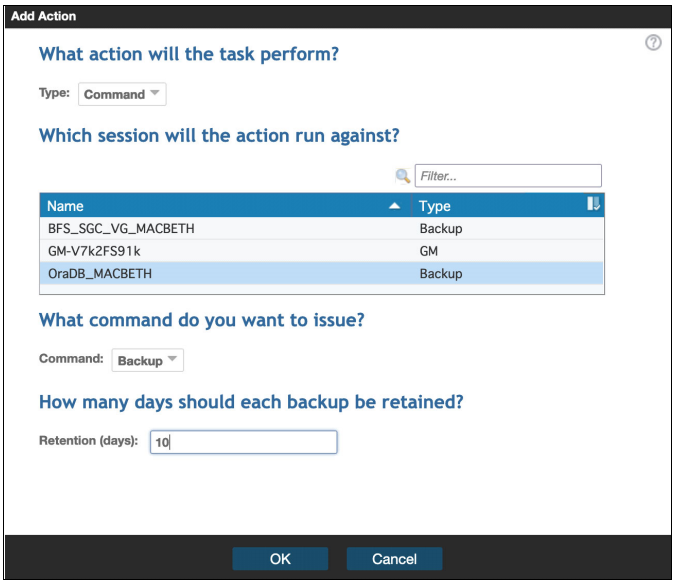

Figure 27 Selecting a Safeguard Copy session name

9. Click **Add Action** again and select the **Command** option from **Type** drop-down menu. Then, select **Copy Services session** and select the **Start** option from the **Command** drop-down menu (see Figure 28).

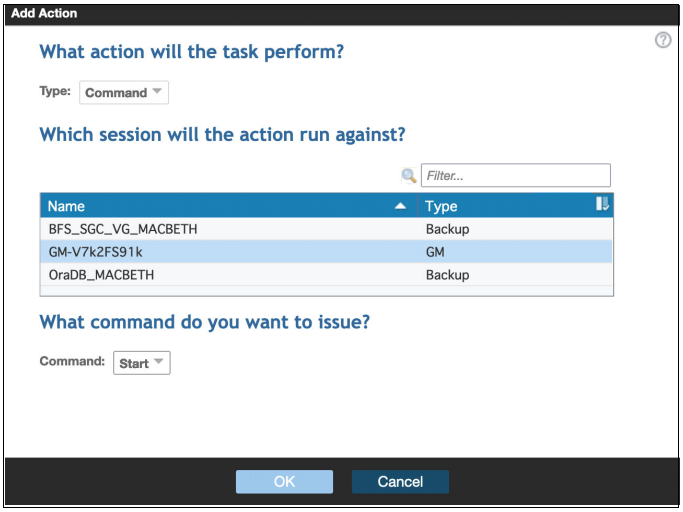

Figure 28 Selecting the Start option

10. The scheduled tasks actions definition is now complete. Leave the default settings of other values in the window (see Figure 29).

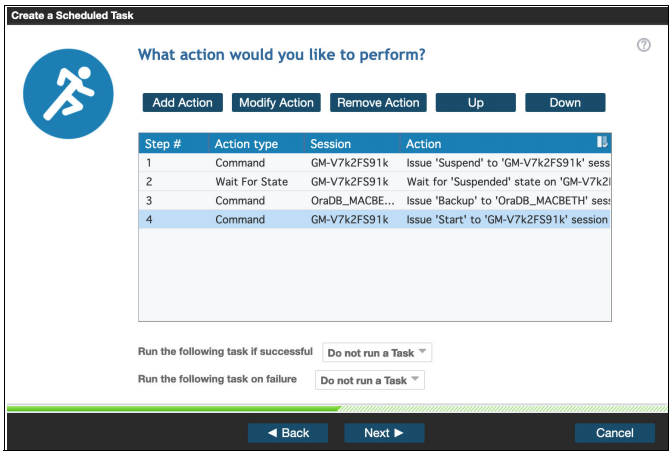

Figure 29 Selecting an action to perform

The last window in the wizard is summary of the scheduled tasks (see Figure 30).

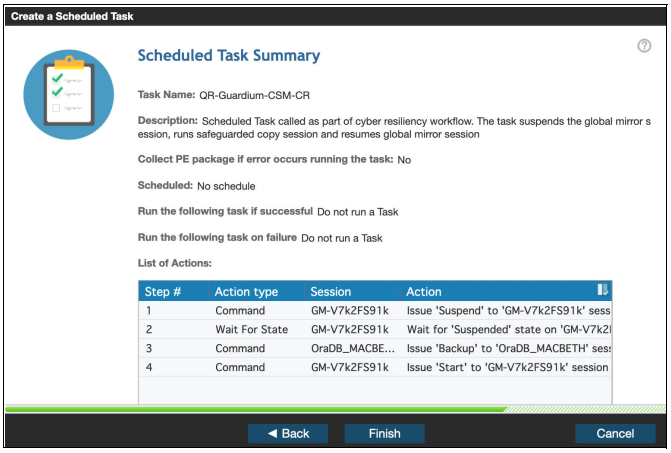

Figure 30 Scheduled Task Summary

11. Review the actions and click **Finish** to complete the scheduled task creation wizard.

IBM Copy Services Manager sessions for Copy Services and Safeguarded Copy are now configured.

Threat detection by using IBM QRadar

Threats are detected by the rules engine in IBM QRadar. The rules engine applies various conditions on the normalized events to determine the threat.

After the threat is detected, its severity can be determined, and a response can be generated that is based on properties that are extracted from the events. In addition to the response, the IBM QRadar administrator can choose to raise an offense.

The sample configuration of a custom action that is defined in IBM QRadar is shown Figure 31.

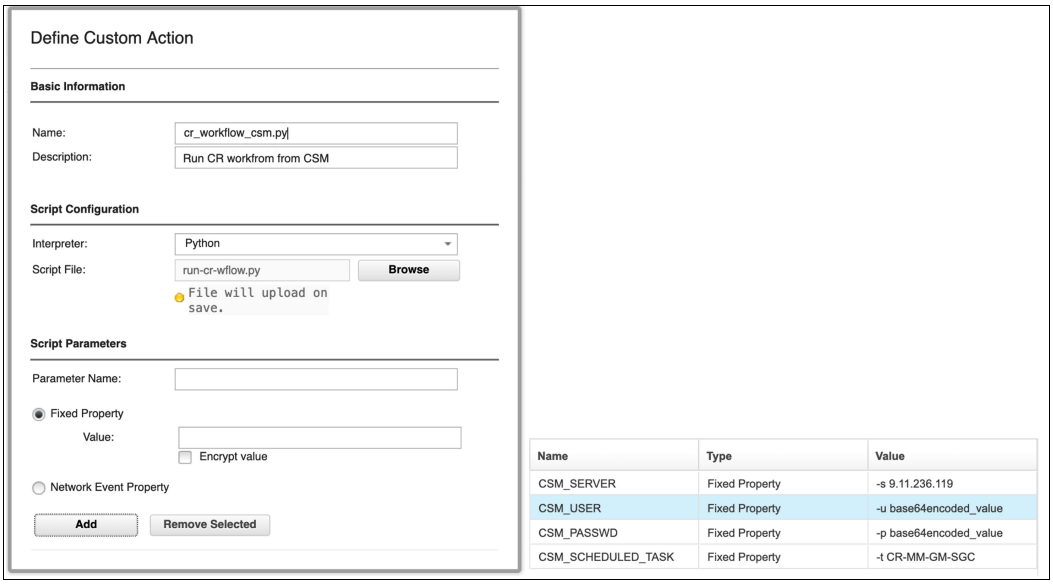

Figure 31 Custom action definition

Complete the following steps to define a custom action:

1. Log in to IBM QRadar by using administrator's privileges. Click the **Admin** tab, and then select **Custom Actions** → **Define Actions**. Then, click **Add**.
2. Define a custom action as shown in Figure 31. Notice that IBM Copy Services Manager_USER and IBM Copy Services Manager_PASSWD parameters are base64 encoded strings.
3. Click **OK** to save the changes and acknowledge the dialog box to deploy the script.
4. Back in the **Admin** tab, notice the messages about undeployed changes (see Figure 32). Click **Deploy Changes** to deploy the changes.

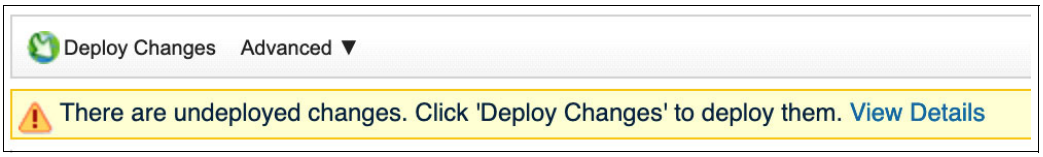

Figure 32 Deploying changes post custom action definition

5. From the **Admin** tab, click **Reference Set Management**. Then, click **Add** to create a reference set. Name the reference set as `Authorized Users`, and then click **Create**.

   This Authorized Users reference set contains a list of database users who are authorized to perform drop action on the database, such as drop table or drop view.
6. Locate and double-click the Authorized Users reference set. Click the **Import** option and provide a file that contains list of database users that are allowed the drop table or drop view action with one username that is written per line.
7. Click the **Log Activity** tab and click the **Rules** drop-down menu. Select the **Rules** option. Click **Next** in the Custom Rule wizard welcome window. The sample rule that is displayed is based on a drop table event that is captured by IBM Security Guardium Data Protection and forwarded to IBM QRadar.
8. Select **Events** as the Source to generate the rule, and then click **Next**.

9. The Rules Test Stack Editor window opens. Use the event matches criteria to filter the rules and click the green (**+**) icon to add the first rule. The bold words act as hyperlinks to select suitable properties (see Figure 33).

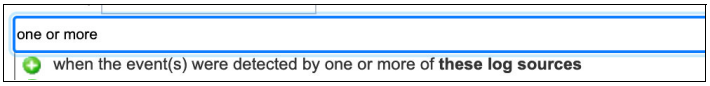

Figure 33 Filtering event rule

10. Click these log sources to select the property and search for Guardium word. Select the **LinuxServer@Guardium** value from the search results, and then click **Add+**. Click **Submit** (see Figure 34).

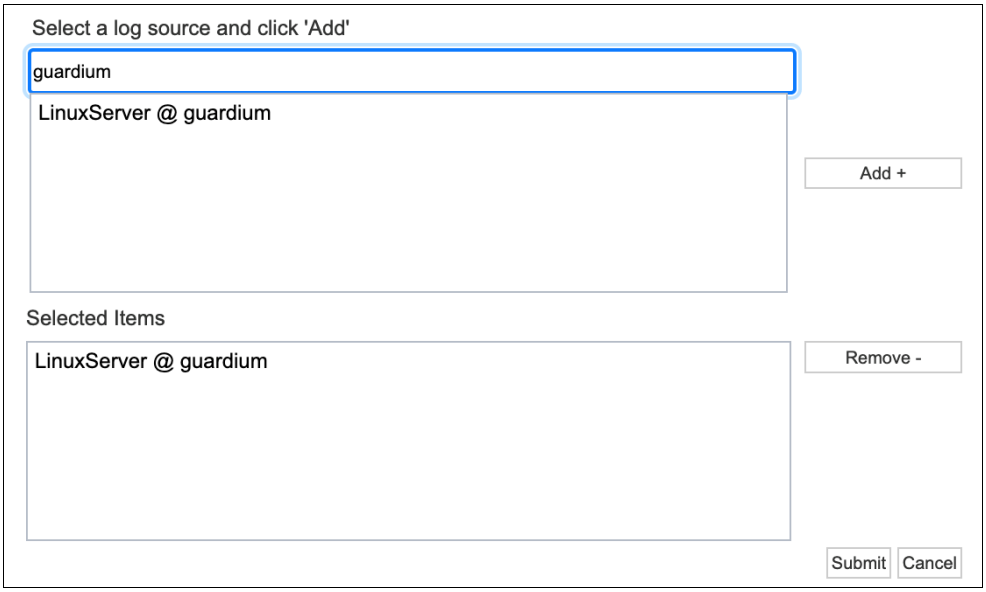

Figure 34 Property value search and selection

11. Use the filter text and add the next rule (see Figure 35).

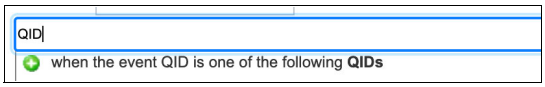

Figure 35 Filter text to select rule

12. Click **QIDs** and enter `Highly restricted data accessed` in the QID/Name field, and then click **Search**.
13. Select the matching QID value from Matching QIDs list, and then click **Add+**.
14. Use the filter text and add the next rule (see Figure 36).

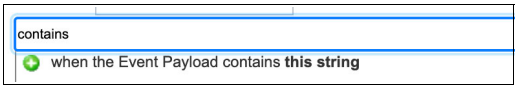

Figure 36 Filter text to select rule

15. Click this string and enter `sha.abc` as the property value (in this example, `abc` is a test table in the `sha` schema).
16. Repeat the process of using of the search filter and adding another rule entry. Then, update this string property value by using the drop-down menu.

17. Use the filter text and add the next rule (see Figure 37).

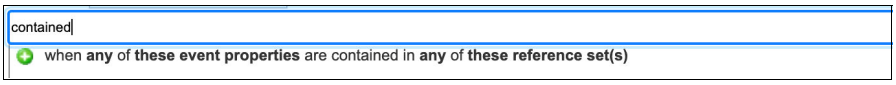

Figure 37 Filter text to select rule

Complete the following steps:

a. Click **and** to change the condition to `and NOT`.

b. Click **these event properties** and search and select the **Username** property value.

c. Click **these reference set(s)** and search and select the **Authorized Users** property value.

After all the property values are updated, the completed rule looks like the example that is shown in Figure 38.

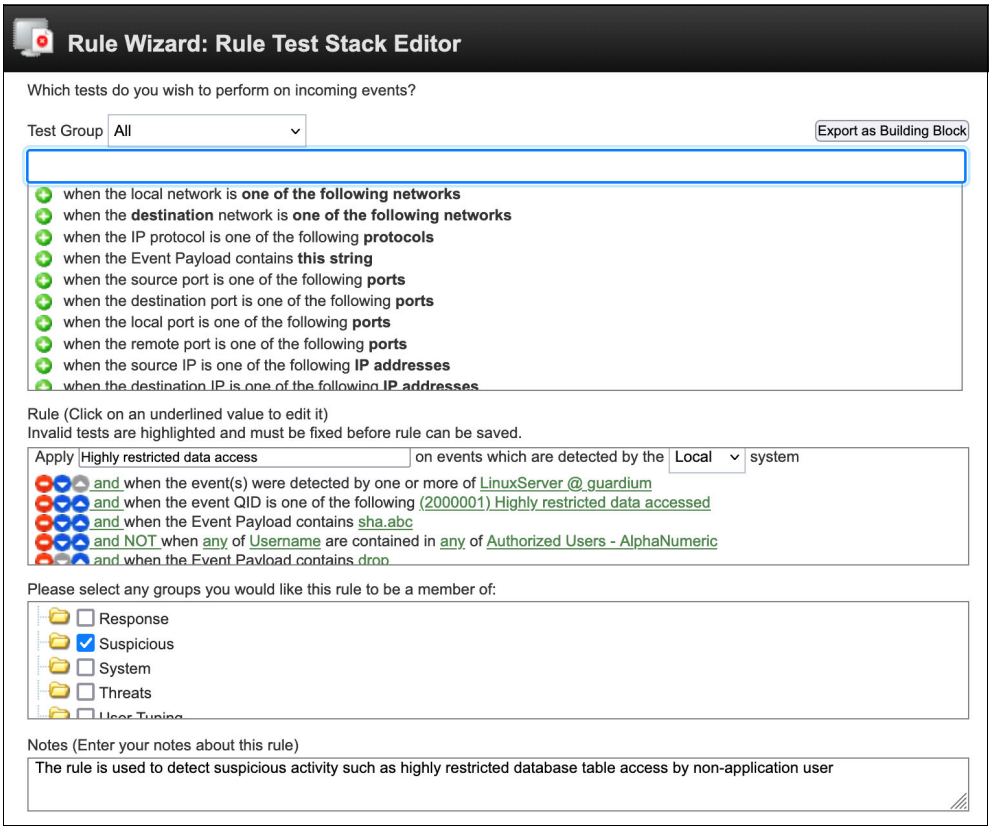

Figure 38 Rule that is defined by selecting the appropriate property values

Now, the rule also is given a name for identifying its purpose and a group is chosen for which this rule can become a member.

In our example, the rule was made part of the Suspicious group for rule categorization. Also, the notes that describe the purpose of the rule are provided for future reference.

18. Click **Next** to open the Rule Response window, which is divided into the following sections:

   – Rule Action

     Under the Rule action section, configure the Severity, Credibility, and Relevance properties to determine the suitability of the event. Use the Annotate even field to provide specific annotations to the event (see Figure 39).

Figure 39 Configuring Rule Action

   – Rule Response

     This section allows configuring a rule's response, such as the use of a property to base the offense on and the execution of custom action. It also allows configuring a new event with a user-defined name and description to indicate that the rule was triggered.

     For example, when checking for a brute force login, the event property Username is used to identify the offending user. Therefore, when an offense is generated, an event is dispatched, the offense is based on Username, and a predefined user action is run (see Figure 40).

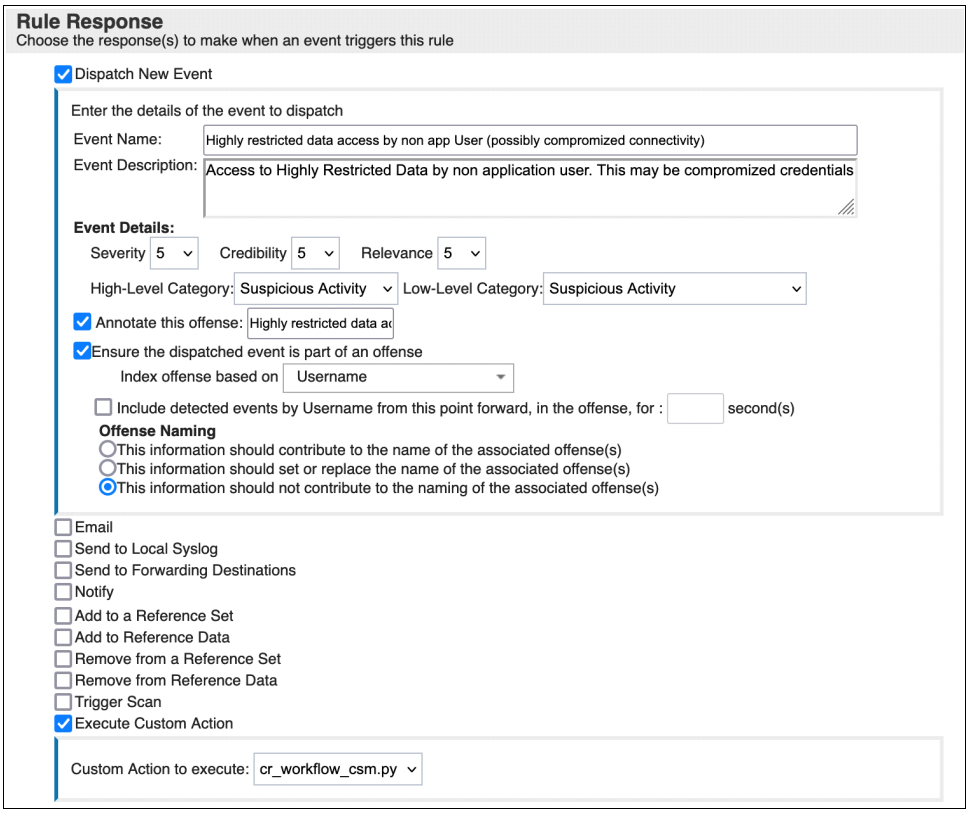

Figure 40 Configuring Rule Response

– Response Limiter

As the name suggests, this parameter limits the response by the rule. In this example, the rule response was set to single execution for every 30 minutes (see Figure 41).

Figure 41 Rule Response Limiter and Rule State

– Enable Rule

Multiple rules can be configured for testing different conditions to detect the threat. A single rule can be enabled by using this property (see Figure 41).

19. The final window of the Rule wizard shows the summary of the rule that was created (see Figure 42).

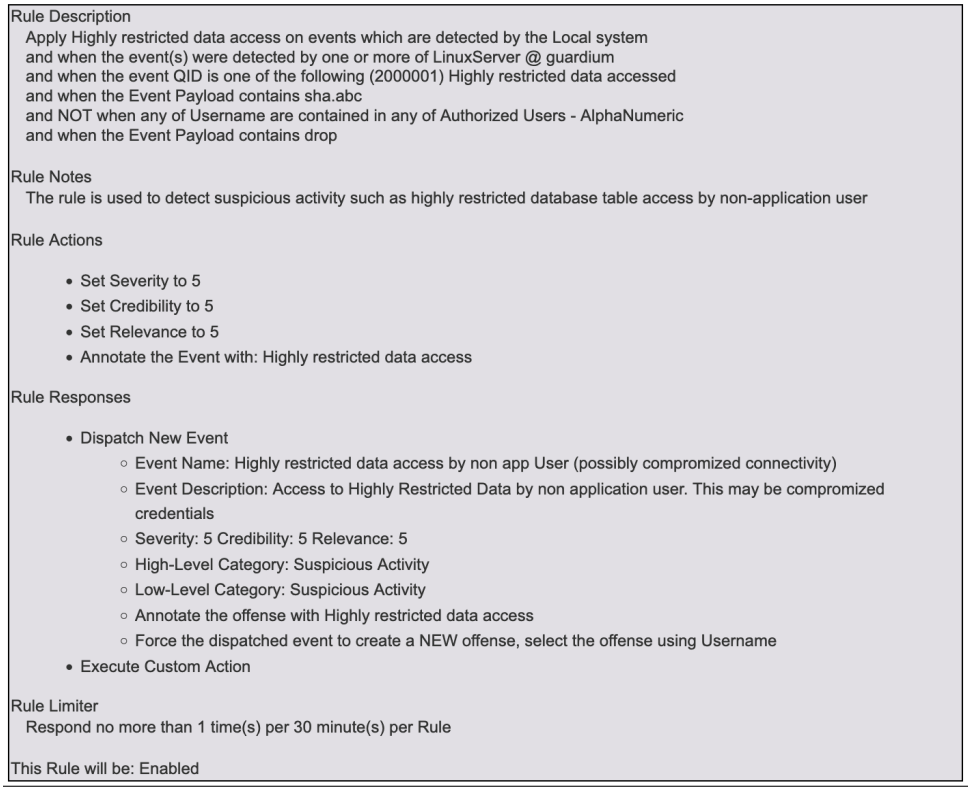

Figure 42 Rule Summary window

Validate the selection that was made and click **Finish** to save the rule and close the wizard.

Other rule summaries

The following rules also can be defined in IBM QRadar to work with events that are received from IBM Security Guardium Data Protection:

- IBM QRadar rule to detect SYS login failures (see Figure 43).

Rule Description
Apply Multiple login failures for SYS user on events which are detected by the Local system
and when an event matches any of the following BB:CategoryDefinition: Authentication Failures
and when at least 5 events are seen with the same Username in 1 minutes
and when the Event Payload contains SYS
and when the Event Payload contains LOGIN_FAILED

Rule Notes
Possible brute force login attack on database with SYS user

Rule Actions

- Set Severity to 3
- Set Credibility to 3
- Set Relevance to 3
- Force the detected Event to create a NEW offense, select the offense using Username
  - Annotate this offense with: Brute force SYS logins detected
- Annotate the Event with: Brute force SYS logins detected

Rule Responses

- Dispatch New Event
  - Event Name: Possible brute force login attack on database to guess SYS credentials
  - Event Description: Detected multiple (5) authentication failures for the same user name in a 1 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

This Rule will be: Enabled

Figure 43 Repeated SYS login failures

- IBM QRadar rule to detect Sensitive Object Access (see Figure 44).

Rule Description
Apply Sensitive Object Access on events which are detected by the Local system
and when the event(s) were detected by one or more of LinuxServer @ guardium
and when the event QID is one of the following (64250080) Select Commands, non App User, Sensitive Objects - Log Full Details

Rule Notes
The rule is used to detect suspicious activity such as sensitive database table access by non-application user

Rule Actions

- Set Severity to 5
- Set Credibility to 5
- Set Relevance to 5
- Annotate the Event with: Sensitive object access by non app User

Rule Responses

- Dispatch New Event
  - Event Name: Sensitive object access by non app User (possibly compromized connectivity)
  - Event Description: Access to sensitive object by non application user. This may be compromized credentials
  - Severity: 5 Credibility: 5 Relevance: 5
  - High-Level Category: Suspicious Activity
  - Low-Level Category: Suspicious Activity
  - Annotate the offense with Sensitive object access by non app User (possibly compromized connectivity)
  - Force the dispatched event to create a NEW offense, select the offense using Source IP

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

This Rule will be: Enabled

Figure 44 The same administrator logs in from multiple locations

- Blocking data access for a specific user at the database level by using IBM Security Guardium Data Protection (see Figure 45).

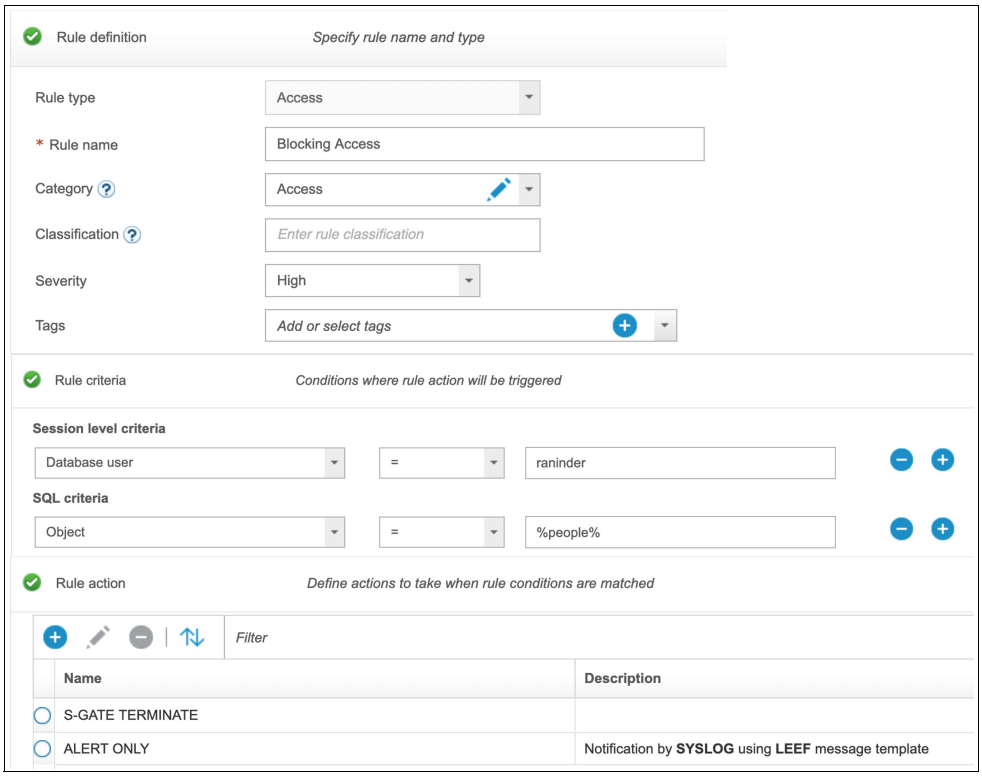

Figure 45 IBM Security Guardium Data Protection rule definition to block data access for a user

- Tracking privilege escalation at the database level by using IBM Security Guardium Data Protection (see Figure 46).

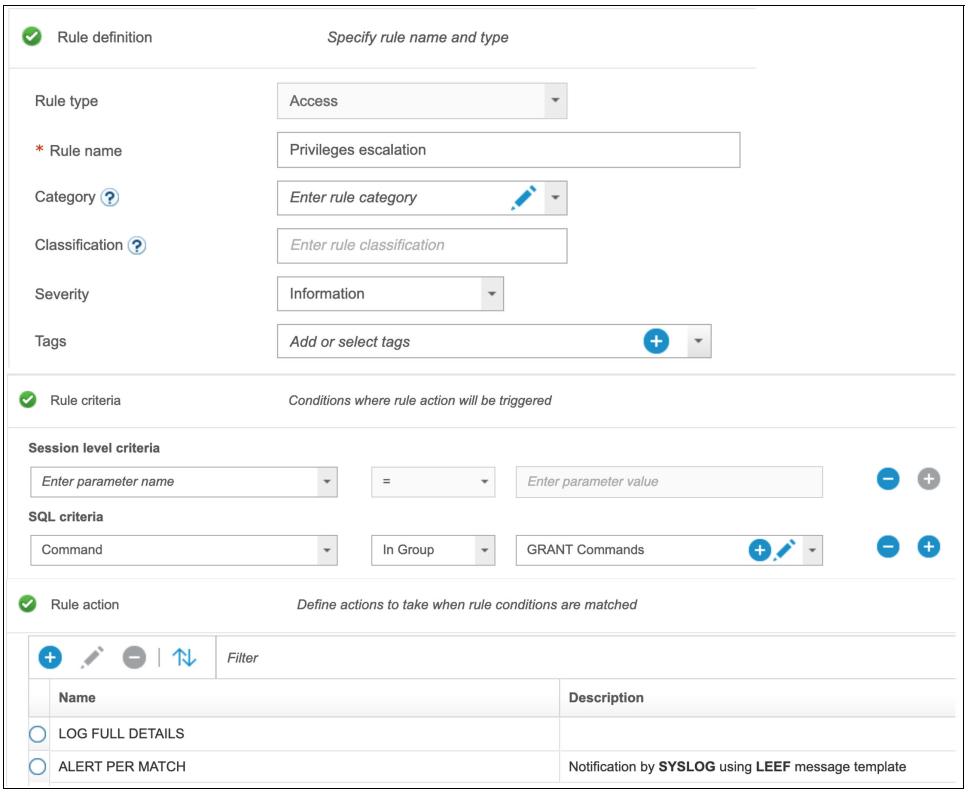

Figure 46 IBM Security Guardium Data Protection rule to track database privileges escalation

- Tracking storage administrator logins outside of business hours (see Figure 47).

Rule Description
Apply Storage admin login outside business hours on events which are detected by the Local system
and when the event(s) were detected by one or more of LinuxServer @ V7k-PetarTheGreat
and when the event QID is one of the following (4750001) Auth Server Password accepted
and when the event(s) occur between 00:00 and 06:00

Rule Notes
Storage admin login detection outside business hours

Rule Actions

- Set Severity to 4
- Set Credibility to 4
- Set Relevance to 5
- Annotate the Event with: Admin login detected outside business hours

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

This Rule will be: Enabled

Figure 47 Rule to detect an admin storage login outside business hours

Brute force login attack on a database or operating system

In this section, we discuss the issue of simultaneous SYS user logins from multiple remote locations.

The Oracle database parameter `remote_login_passwordfile` includes the default value of Exclusive. This value allows for the possibility for a SYS user login remotely.

Attackers can take advantage of this setting to impersonate the SYS user by attempting remote logins. One way to prevent this issue is to set the value `None` for parameter `remote_login_passwordfile`. This setting forces database administers to connect to the remote database host by using terminal emulator software.

To further secure Oracle user account on the system, DBAs must log on with own user account, and then use the sudo function to change to an Oracle user. As part of the lab testing, we used both methods to track the user access to the database.

Although this process might seem a bit cumbersome, these practices provide better protections.

To track the operating system audit activities on the Linux host, a rsyslog package was installed and configuration file (`qr_forward.conf`) was created in `/etc/rsyslog.d`. For more information about the contents of the `qr_forward.conf` file, see “Appendix A: Configuration for rsyslog daemon” on page 36.

A brute force login attack on the database host was generated by using SSH. Multiple failed SSH logins were recorded by the audit log. Those events were then forwarded to IBM QRadar by using the rsyslog daemon configuration.

IBM QRadar administrators use the following events to define rule conditions to identify threats and run the predefined custom user action:

- Database audit log events that were generated and forwarded by IBM Security Guardium Data Protection
- Operating system events that were forwarded by rsyslog on database host
- Control path events that were generated from storage system

The GitHub repository shows a sample python script that is registered as part of the custom user action. The script makes API calls to IBM Copy Services Manager to run the predefined Scheduled Task with different actions, as described in “Creating a scheduled task in IBM Copy Services Manager” on page 21.

The brute force login case that is described here represents threat detection from the operating system environment. Similarly, the use of IBM Security Guardium Data Protection rules engine to detect threats to the database by user actions and access can be tracked and prevented.

These events can be categorized and threat detection rules can be defined based on the security compliance matrix that is defined by the organization.

Summary

The solution that is described in this IBM blueprint publication shows the integration of IBM Security Guardium Data Protection, IBM FlashSystem, and IBM QRadar to perform early threat detection on database host operating systems, databases, and IBM FlashSystem storage.

When a threat is detected, a cyber resiliency workflow is triggered. This workflow is used to run a predefined scheduled task in IBM Copy Services Manager to perform required actions. Then, these actions start Safeguarded Copy to create an immutable copy of the data.

The solution that is presented here can be used as template to categorize the events that are received from IBM Security Guardium Data Protection, IBM FlashSystem storage, and the database host. Based on the events that are received, threat detection rules can be defined that confirm to security standards that are defined by organization's compliance matrix.

The sample Python script shows how to use the API interface of IBM Copy Services Manager to perform specific tasks.

Authors

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

Shashank Shingornikar is a Storage Solutions Architect 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, building solutions that combine Oracle and Red Hat 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.

Raninder Ravi Bhandari has over 14 years of experience with IBM Security Guardium Data Protection and is working as Product Manager in GSI Product management team. He has vast experience in development of innovative Data Protection Policies regarding business and compliance requirements (PCI-DSS, GDPR, and SOX). Raninder also has expertise in providing cost-effective, yet best in class DAM Architecture and advance Guardium implementations, such as blocking, redaction, query rewrite, discovery, classification, and vulnerability management.

Acknowledgment

The authors want to thank Andrew Greenfield, of IBM Systems, for his valuable contributions and support on this project.

Appendix A: Configuration for rsyslog daemon

This section describes the configuration that was created for rsyslog daemon on the Linux host that simulates database workload.

A configuration file that is specific to the application was created in `/etc/rsyslog.d` with the configuration options that are shown in Figure 48.

```
# Config files to forward events to QRadar
# QRadar host: 9.11.221.149, port: 514, TCP

#/var/log/audit/audit.log

module(load="imfile" PollingInterval="5")
input(type="imfile"
      File="/var/log/audit/audit.log"
      Tag="AUDIT"
      Severity="error"
      Facility="local4"
)

input(type="imfile"
      File="/var/log/secure"
      Tag="AUTH"
      Severity="error"
      Facility="local4"
)

local4.* action(type="omfwd" target="9.11.221.149" port="514" protocol="tcp")
```

Figure 48 Application-specific configuration file

The rsyslog is available as part of Red Hat 7.9 repository that was used for the configuration.

Appendix B: Sample regular expressions

The sample regular expressions that are used to extract specific value from the IBM QRadar event payload are listed in Table 1.

Table 1 Sample regular expressions that are used to extract specific value

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	
Sgc_volname	Custom	`\s-name\s(bk_.*)`	1	
Result	Custom	`#\sresult\s=\s(.*?)\s`	1	
Sgc_bkp_volid	Custom	`#\sres_obj_id\s=\s(.*?)\s`	1	
Username	Custom	`\scluster_user\s=\s(.*?)\s`	$1	
Volume_ID	Custom, Common	`\d+$`	0	Rmvolume
Username	Custom	`\scluster_user\s=\s(.*?)\s`	$1	Login
Command Origin	Custom	`\s-gui|\sservice\sweb\s`	0	Login

Resources

For more information about the topics that are discussed in this publication, see the following resources:

- Download the GitHub script:

  http://www.github.ibm.com/IBM/ibm-qradar-ds8k-sgc-with-csm

- IBM Copy Services Manager:

  http://www.ibm.com/docs/en/csm

- *IBM Copy Services Manager User's Guide*, found at:

  http://www.ibm.com/support/pages/system/files/inline-files/sc27854220.pdf

- *Enhanced Cyber Resilience Threat Detection with IBM FlashSystem Safeguarded Copy and IBM QRadar*, REDP-5655

- IBM QRadar:

  http://www.ibm.com/docs/en/qsip

- IBM QRadar and IBM Security Guardium Data Protection integration:

  http://www.ibm.com/docs/en/guardium/11.4?topic=integration-qradar-guardium

- IBM Security Guardium:

  http://www.ibm.com/docs/en/guardium/11.4

- Shipping Guardium Syslog to a remote server:

  http://www.ibm.com/support/pages/shipping-guardium-syslog-remote-server

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®	IBM®	QRadar®
FICON®	IBM FlashSystem®	Redbooks (logo) ®
FlashCopy®	IBM Security®	Storwize®
Guardium®	IBM Spectrum®	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.

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

OpenShift, Red Hat, 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.

March 2023

Please recycle

ISBN 0738461059

REDP-5686-01