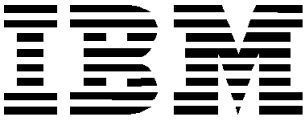
IBM® Storage

Cyber Resiliency with IBM QRadar and IBM Spectrum Virtualize for Public Cloud on Azure with IBM Copy Services Manager for Safeguarded Copy



About this document

The focus of this Blueprint publication is to highlight the early threat detection capabilities of IBM® QRadar® and to show how to proactively start a cyber-resilience workflow in response to a cyberattack or malicious user actions.

The workflow uses IBM's Copy Services Manager as orchestration software to start IBM Spectrum Virtualize for Public Cloud (SV4PC) Safeguarded Copy functions. The IBM SV4PC Safeguarded Copy function creates an immutable copy of the data in an air-gapped form on the same IBM SV4PC on Azure for isolation and eventual quick recovery.

This document describes the steps that are involved to enable and forward IBM SV4PC audit logs to IBM QRadar. It also describes how to create various rules to determine a threat, and configure and start a suitable response to the detected threat in IBM QRadar. This document also explains how to register a storage system and create a scheduled task by using IBM Copy Services Manager.

Finally, this document also describes deploying IBM QRadar and SV4PC on Azure. A use case for protecting the MS SQL database (DB) volume that was created on IBM SV4PC is included. Upon threat detection on a database volume, Safeguarded Copy is started for IBM SV4PC volume. The Safeguarded Copy creates an immutable copy of the data. The same data volume can be recovered or restored by using IBM's Copy Services Manager.

Executive summary

The financial effects of cyberattacks continue 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, it is observed that the data breaches involve internal threat actors.

Traditional approaches to data protection work well for their intended purposes, but are not adequate to protect against cyberattacks, which might encrypt or otherwise corrupt your data.

Remote replication for disaster recovery replicates all changes (malicious or not) to the remote copy. Data that is stored on offline media or the cloud can take too long to recover from a widespread attack. Large-scale recovery can take anywhere from days to weeks, which can lead to substantial downtime for businesses.

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 might 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.

The Safeguarded Copy function helps businesses recover quickly and safely from a cyberattack, helping reduce recovery to minutes or hours. It creates multiple recovery points for a production volume. These recovery points are called *Safeguarded Copy backups*.

The recovery data is not stored in separate regular volumes, but in a storage space that is called Safeguarded Copy backup capacity, which creates a logical air gap. The backups are not directly accessible by a host. The data can be used only after a backup is recovered to a separate recovery volume.

If an attack occurs, the orchestration software, IBM Copy Services Manager, helps create and identify the best Safeguarded Copy backup to use and automates the process to restore or recover data to online volumes. Because a restore action uses the same snapshot technology, it is almost instant and 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 on IBM SV4PC storage system and proactively start Safeguarded Copy to create an immutable backup at the first sign of a threat. IBM Copy Services Manager orchestration software is used to interact with IBM SV4PC system to start a schedule task for Safeguarded Copy backup, and to recover or restore that backup.

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

Customers are readers are encouraged to create a control path and data path use cases, customized IBM QRadar rules, and custom response scripts that are best suited to their environment. Consider the use cases, rules, and Python script as templates or guides that might not be used in a real-world, production environment as presented here.

The solution that is featured in the document is created by using IBM QRadar release 7.3.x, IBM's Azure SV4PC, and IBM's Copy Services Manager 6.3. IBM's Copy Services Manager Scheduled task feature is heavily relied upon to create the required workflow. The sample workflow that is explained as part of the solution involves starting Safeguarded Copy for IBM SV4PC volume.

All components that are described in this document, such as IBM QRadar, IBM Copy Services Manager, and IBM SV4PC are in the same Azure Resource Group. More adequate network planning is required if these systems are in different resource groups.

For more information about resources on IBM QRadar, Safeguarded Copy and Copy Services Manager, IBM SV4PC on Azure, see "Resources" on page 49.

Introduction

Combining the capabilities of IBM SV4PC Safeguarded Copy and IBM QRadar 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. For more information, see this NIST web page.

IBM SV4PC can log administrative activities in the access or audit logs, which include all storage objects access information. To identify and detect potential malicious access or activities and for compliance-auditing purposes, such access or audit logs must be integrated with the SIEM solution.

By combining IBM SV4PC administration access, audit logs, application logs, network and server logs, flow and packet data, IBM QRadar can provide complete protection to the entire data space and reduce attacks vectors.

IBM SV4PC Safeguarded Copy function

The Safeguarded Copy feature creates immutable backups that are not accessible by the host system and 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 in comparison to IBM FlashCopy® volumes. Creating Safeguarded Copy backups also has less performance impact than the multiple target volumes that are created by IBM FlashCopy.

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

Safeguarded Copy uses a backup capacity, production volume, and recovery volume. Consider the following points:

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

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

IBM Copy Services Manager

IBM Copy Services Manager controls copy services in storage environments. Copy services features are used by storage systems, such as IBM SV4PC, 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 the following operating systems:

- Windows
- IBM AIX®
- Linux
- Linux on IBM Z®
- IBM z/OS® operating systems

When it is running on z/OS, IBM Copy Services Manager uses the IBM Fibre Channel connection (IMB 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 graphical user interface (GUI), a command-line interface (CLI), and Representational State Transfer (RESTful) API possibility for managing Data Replication and Disaster Recovery.

Staring with IBM Copy Services Manager v6.2.9, the online help also integrates with the RESTful API.

IBM QRadar

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 several data sources and analysis tools and techniques, including access logs, heuristics, correlation with logs from other systems (such as network logs, database audit 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. Select, organize, and group the columns of event data.
- Visually monitor and investigate flow data in real time, or perform advanced searches to filter the displayed flows. View flow information to determine how and what network traffic is communicated.
- View all of the learned assets or search for specific assets in your environment.

- Investigate offenses, source and destination IP addresses, network behaviors, and anomalies on your network.
- Edit, create, schedule, and distribute default or custom reports.

Prerequisites

This section outlines the following prerequisites for the solution that is presented in this Blueprint:

- Azure administration skills with good understanding of Azure resource groups, Azure networking and deployments, and role bases access for the users on Azure.
- The firewall rules between IBM QRadar and IBM SV4PC 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 and udp protocol on port 514. The choice of protocol that is used for communication depends on an organization's guidelines.

- IBM Copy Services Manager 6.2.3 or later is available and the IBM SV4PC storage is registered in IBM Copy Services Manager by using administrator privileges (see "Resources" on page 49).
- A scheduled task must be defined inside 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 (such as metro or global mirror are used), writes to target volumes must be suspended to achieve a consistent state before a Safeguarded Copy backup can be made.
- Safeguarded virtual capacity is provisioned. For more information about configuring safeguarded virtual capacity, see "Resources" on page 49.
- An understanding of IBM SV4PC storage for working with volumes and safeguarded pool capacity allotment.
- IBM QRadar rules are defined for the use case. In this example, we created rules for two specific use cases:
  - Log in to the database and attempt to access the restricted tables. An offense likely is generated for unauthorized access to database tables.
  - In a brute force attack, a login failure occurs for the database user who attempts to use an invalid password.
- MS SQL 2019 is installed on a Windows host and users are configured to access the database, and restrict access to database users for sensitive data table access as demonstrated in the use case demonstration.
- IBM QRadar WinCollect is installed. Administrators can use WinCollect to forward Windows-based events for IBM QRadar SIEM administrators. For more information, see "Resources" on page 49.

Solution overview

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

To track administrator's actions, the solution implements various control path use cases. Also, a data path use case is discussed in which changes in application data are tracked.

A syslog configuration is created inside IBM SV4PC that allows forwarding of storage events to IBM QRadar. IBM QRadar understands the authorization events that are forwarded by IBM SV4PC and categorizes them correctly. Other storage-specific events must be mapped to correct IBM QRadar identifier (QID) for storage-specific operation categorization.

After the events classification is completed, an 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 of 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 as it provides flexibility to run various operations, including conditional execution based on certain state of previously run command.

An overview of solution is shown in Figure 1.

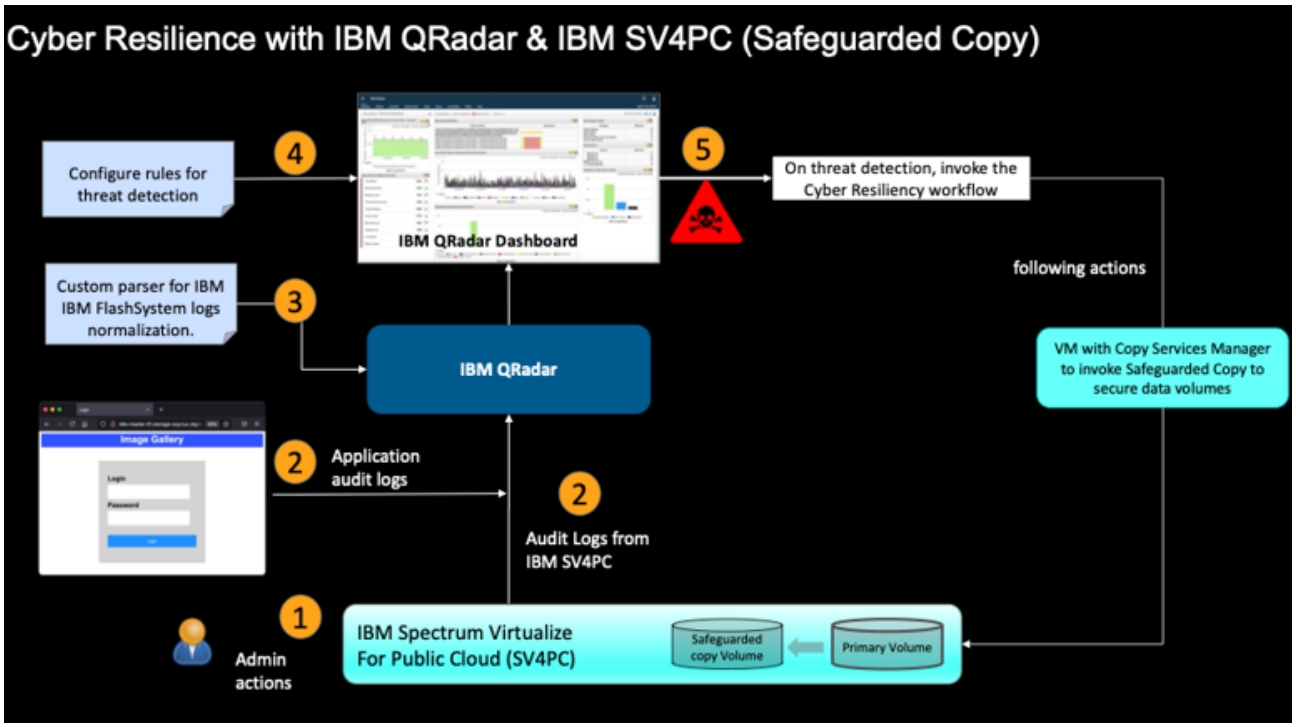


Figure 1 Solution overview

Control and data path use cases

The following sample control path use cases are presented in this document:

- An unauthorized user attempts to log in to the database and access data that is in restricted tables. An offense likely is generated to prevent any unauthorized access.
- A log in failure occurs when a database user attempts to use an invalid password. This use case is an example of when compromised or shared credentials are used. This example also can be considered a brute force attack when the user attempts to access the database.

These use cases are by no means is an exhaustive list of the types of cyberthreats that organizations face; rather, they are intended to provide general threat examples. Ultimately, cyberthreats are defined by the security policy of the organization.

Use case representation

Figure 2 shows a typical 3-tier application infrastructure with IBM QRadar monitoring telemetry from all the sources within the environment.

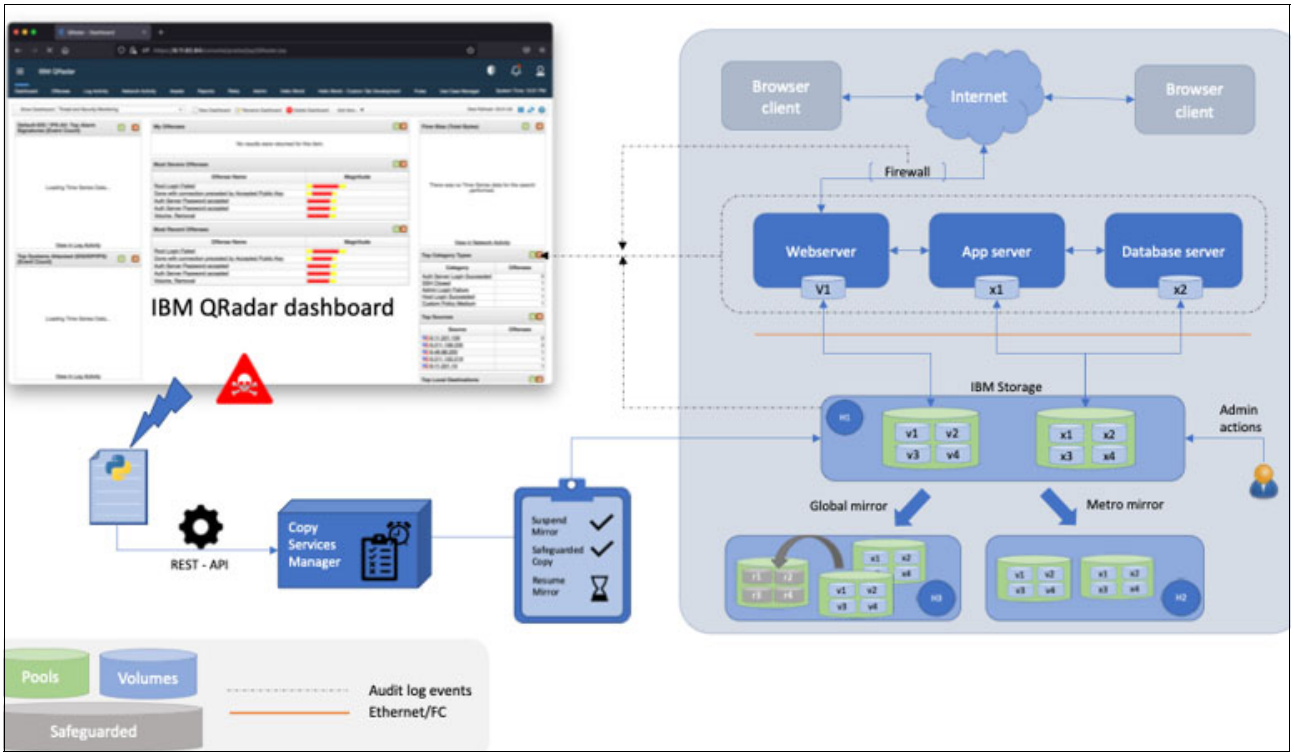


Figure 2 Sample application infrastructure

The audit log events from the host, web, application, and database tier can be used to determine a brute force attack threat.

For this solution, the brute force login on the database server was attempted. The failed logins triggered events inside IBM QRadar to activate the threat conditions. Then, the cyber-resiliency workflow starts an IBM Copy Services Manager scheduled task to create Safeguarded Copy backup by suspending Global Mirror. The copy session also is restarted post Safeguarded Copy backup.

Lab setup

This section explains the lab setup that was used.

Deployment overview

The deployment of various components on Azure for the entire solution is shown in Figure 3.

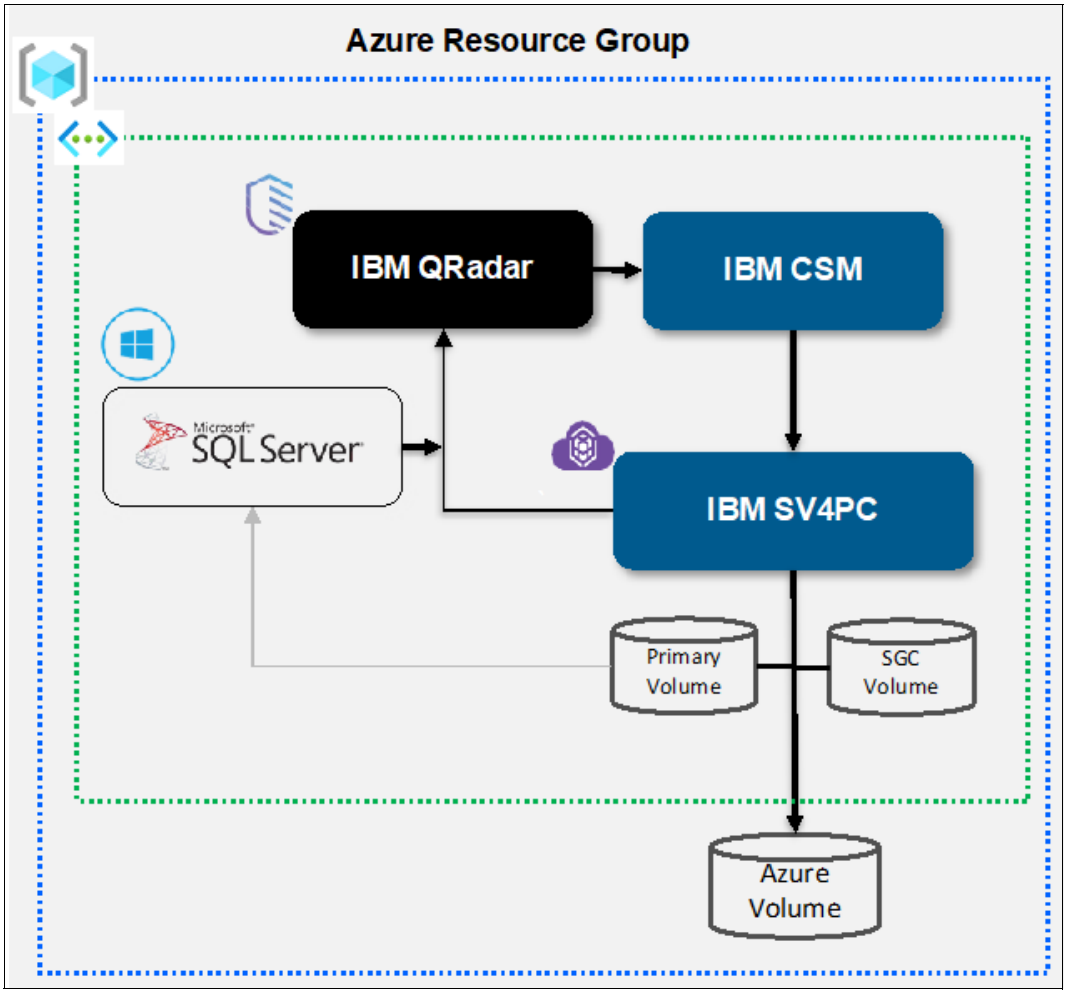


Figure 3 Deployment overview for entire solution

The configuration consisted of IBM QRadar, IBM Copy Services Manager, IBM SV4PC, and Microsoft's SQL Server that are deployed in the same Azure Resource Group within the same Azure region (see Figure 3).

The post deployment status of Azure virtual machines (VMs) in the resource group is shown (see Figure 4).

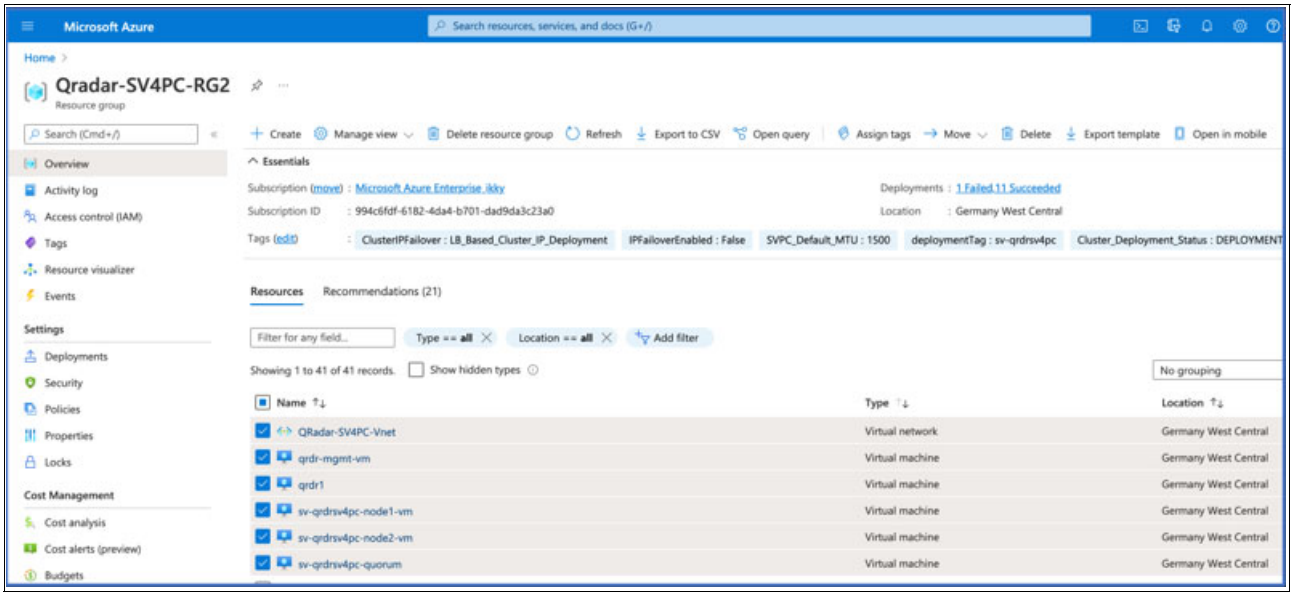


Figure 4 Virtual machines deployed in the resource group

The IBM SV4PC storage was configured with a Safeguarded pool and volumes, as shown in Figure 5.

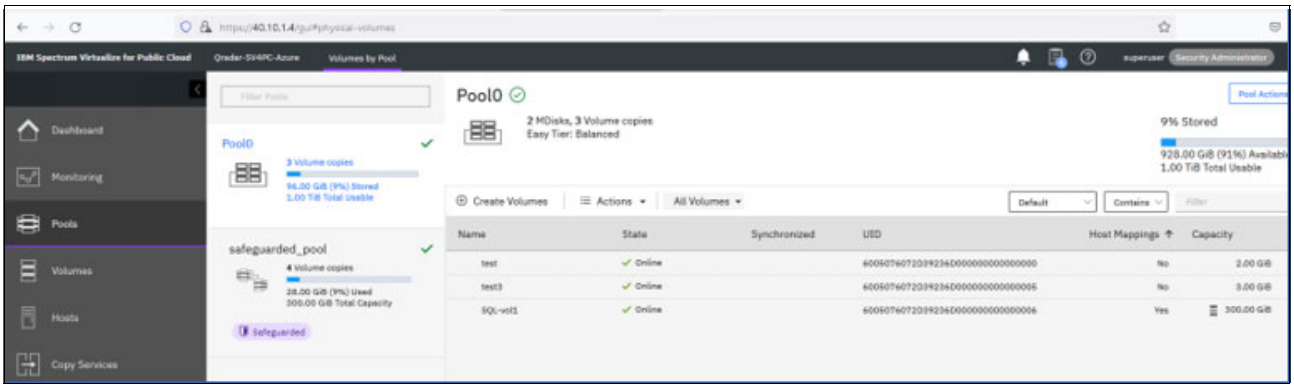


Figure 5 Safeguarded copy pool and capacity

The IBM Copy Services Manager software was installed on the Windows 2019 VM that was deployed inside the Azure resource group (see Figure 6).

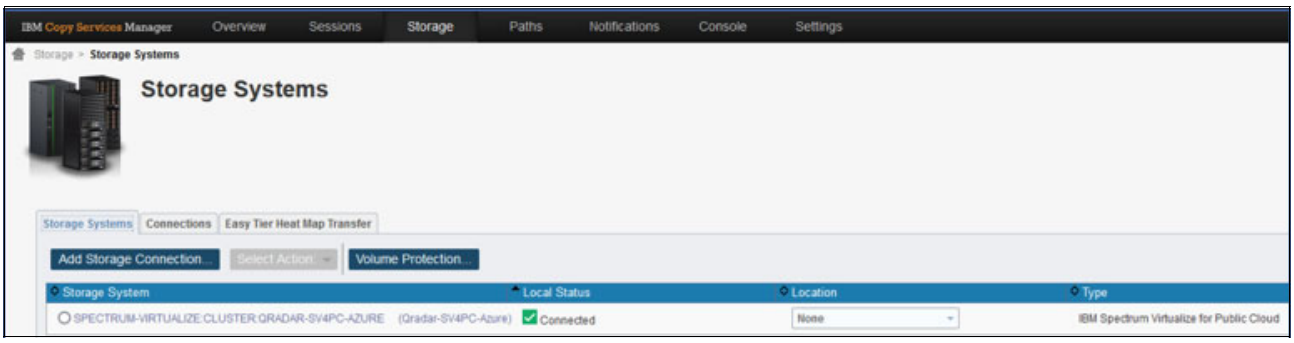


Figure 6 IBM Copy Services Manager host with IBM SV4PC storage connection added

Microsoft's SQL 2019 was deployed on an Azure Windows 2019 VM, where the volumes from IBM SV4PC storage are connected by using iSCSI. Various database user activities were started as a sample threat for use cases to access the Microsoft SQL database to maintain write activity on the primary volumes.

Audit logging was enabled on IBM SV4PC systems by using a syslog setup. IBM QRadar understands the syslog event format, it then automatically creates a LinuxServer type log source and the events are categorized. This categorization was changed for storage-specific actions.

Deploying IBM QRadar on Azure

Complete the following steps to deploy IBM QRadar on Azure:

1. Log in to `https://portal.azure.com/#home` with your username and password.
2. In the search bar, search for **Marketplace**. Then, search for "IBM QRadar" and select **IBM QRadar SIEM v7.3.x (BYOL)**, as shown in Figure 7.

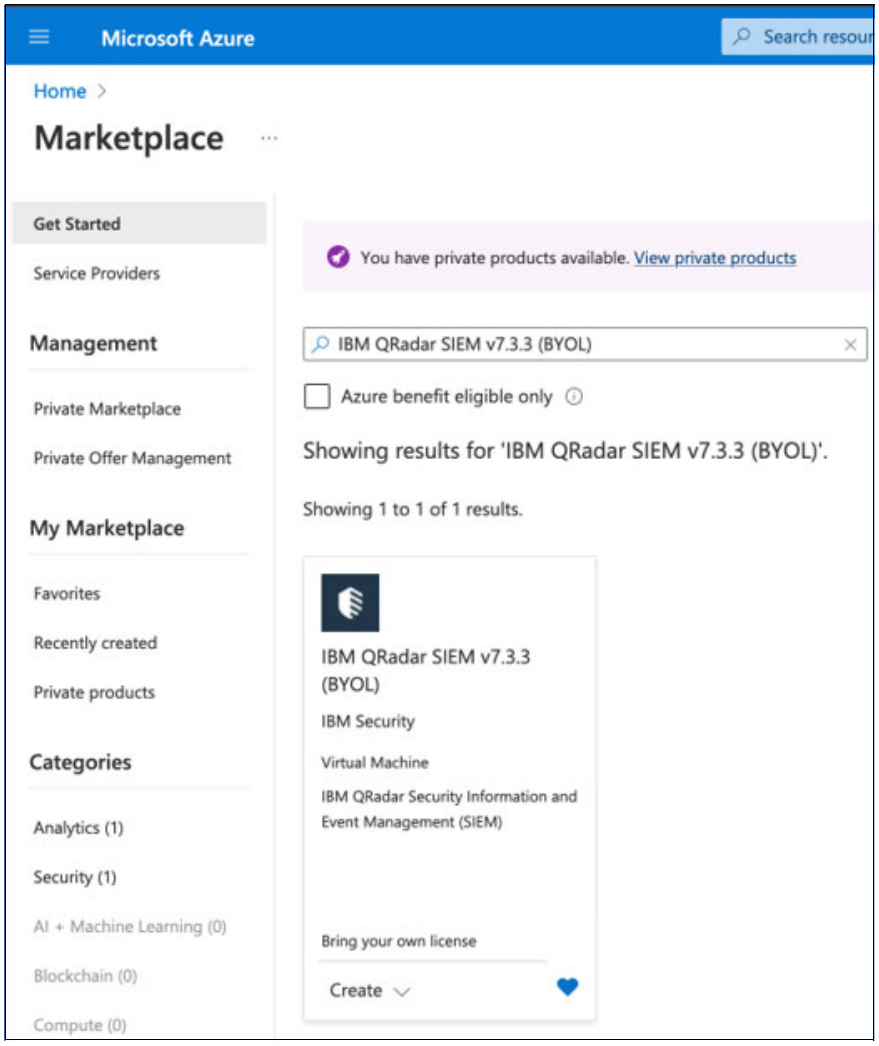


Figure 7 IBM QRadar SIEM v7.3.3 (BYOL)

For more information, see this hIBM Documentation web page.

3. Select the **IBM QRadar SIEM v7.3.3(BYOL)** plan and then, click Create (see Figure 8).

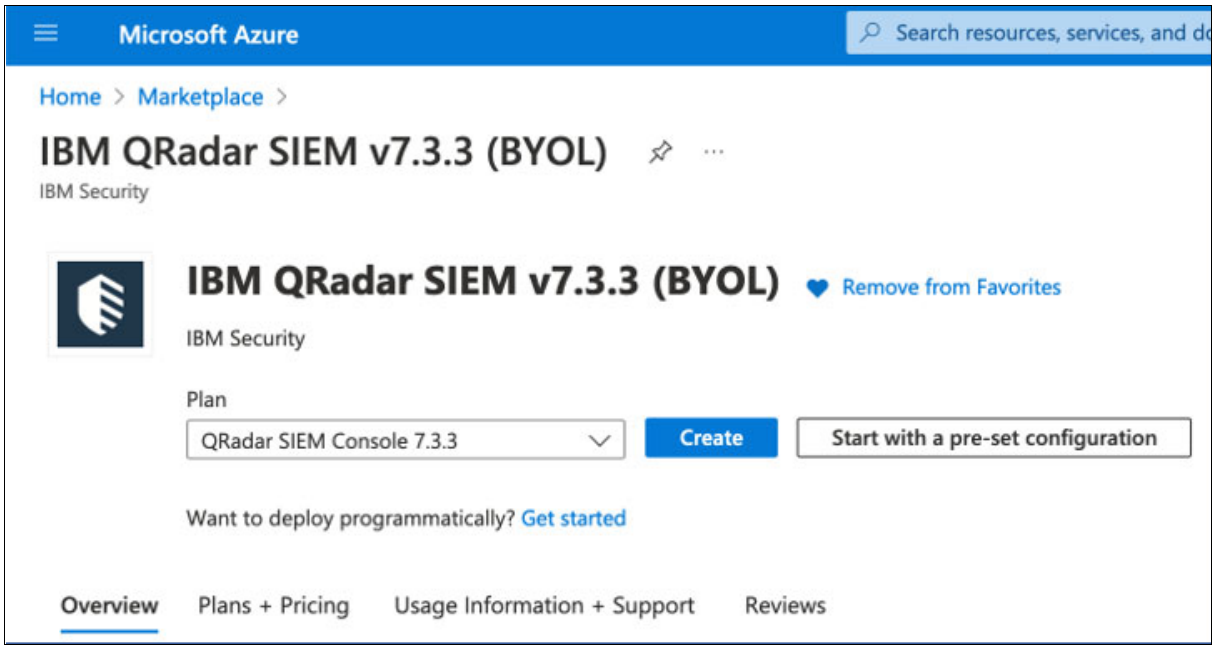


Figure 8 Selecting plan

4. Complete the following steps to configure the virtual machine settings (see Figure 9 - Figure 11 on page 14):
   a. Select an existing resource group or create a resource group.
   b. Enter the virtual machine name.
   c. Select **Region**.
   d. Choose an SSH public key or Password.
   e. Set the Public inbound ports to **Allow** selected ports.
   f. Set the Select inbound ports to **SSH (22)** and **HTTPS (443)**.

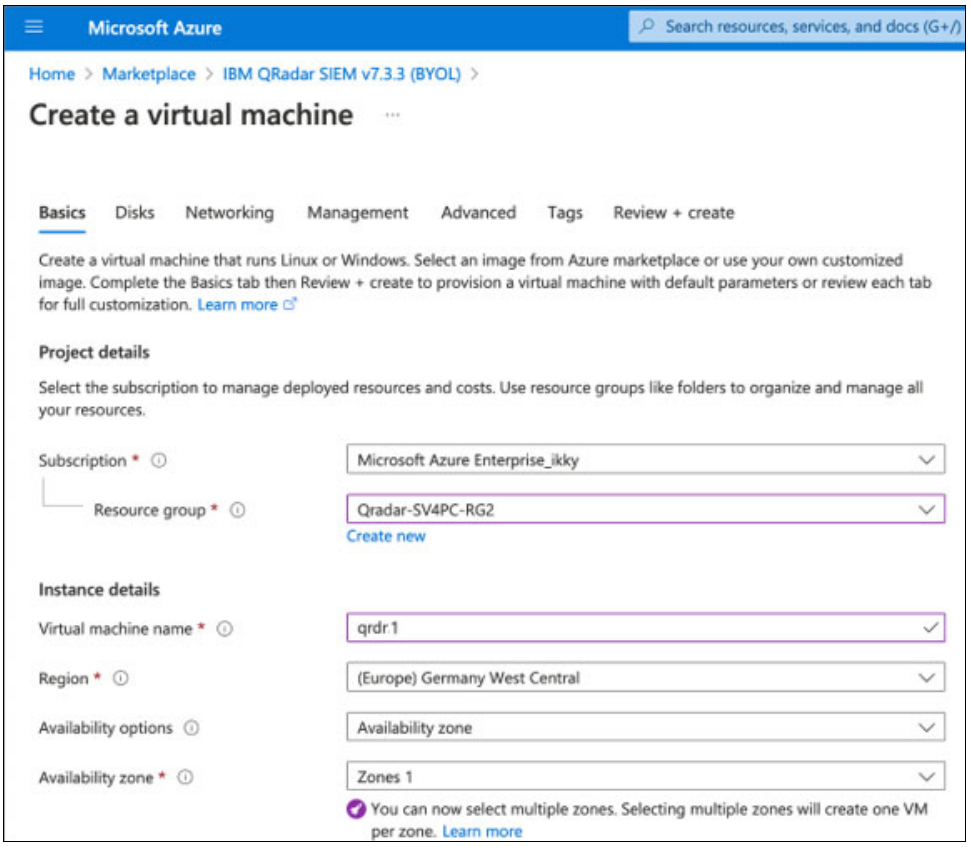


Figure 9 Basic, configure VM settings

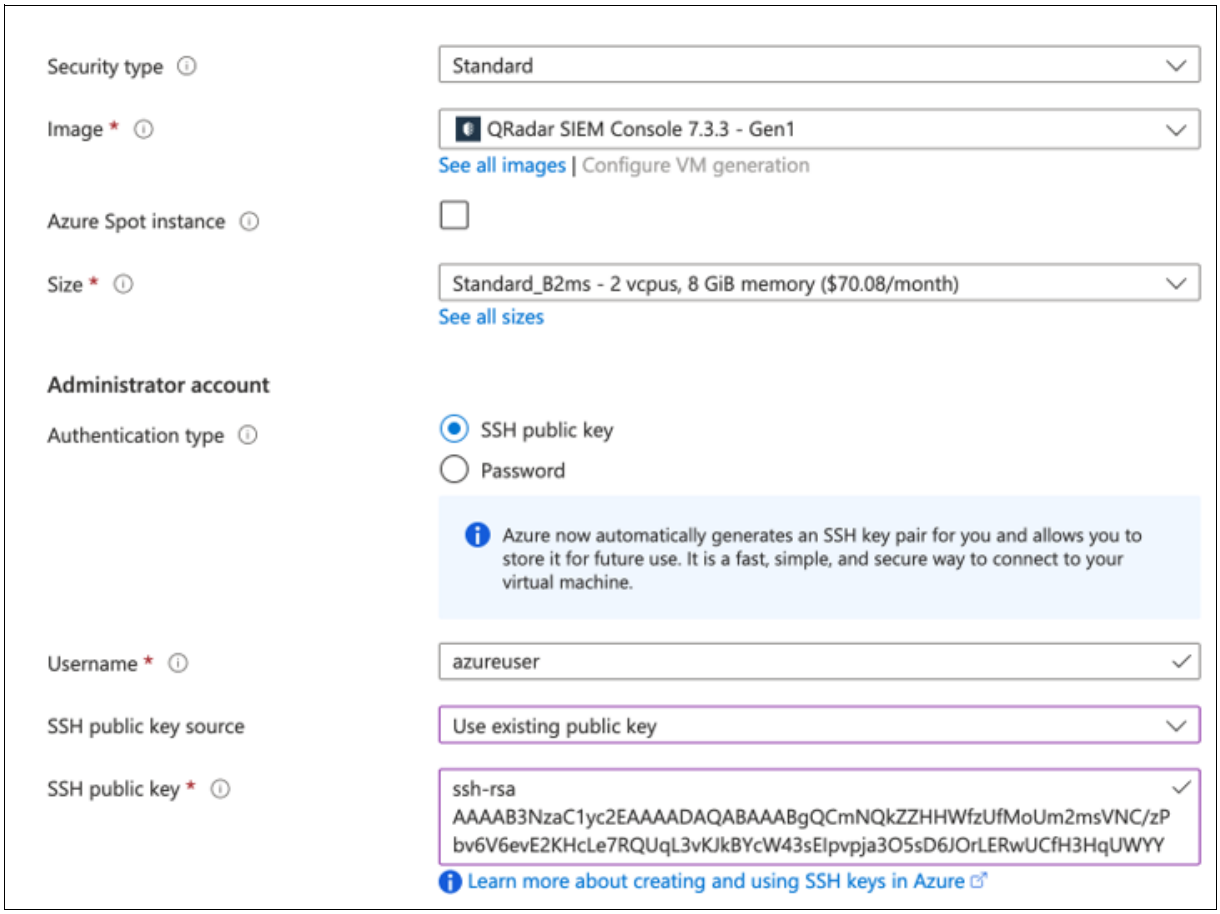


Figure 10 Basic, configure VM settings

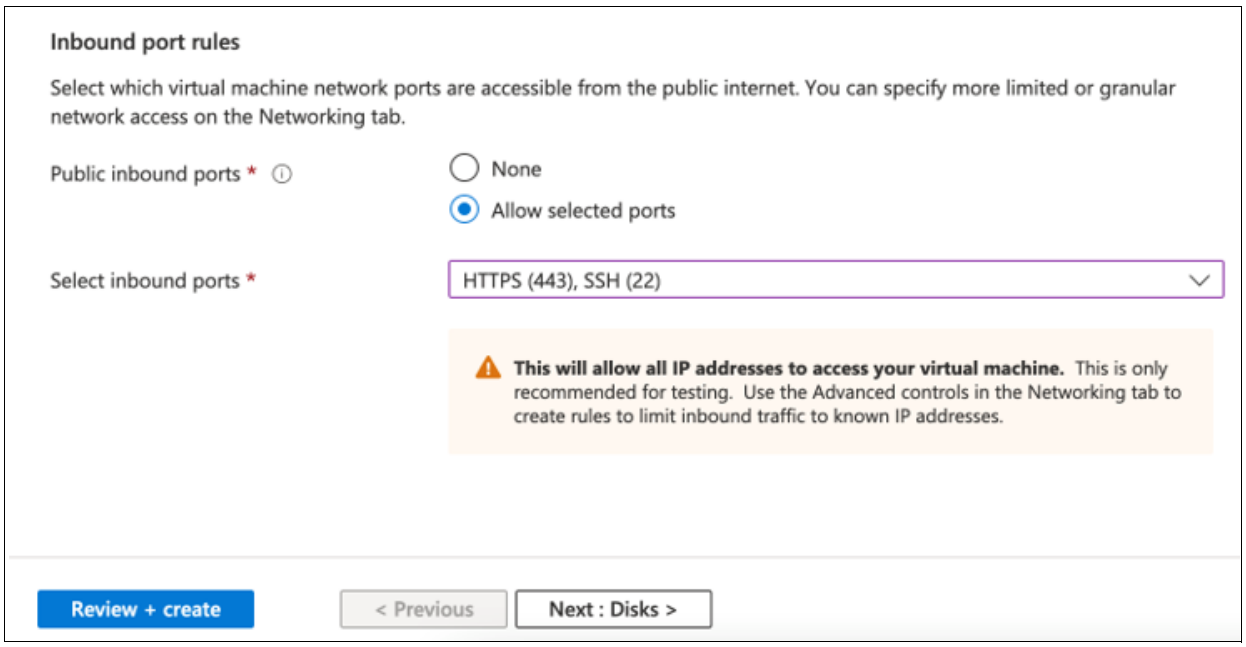


Figure 11 Basic, configure VM settings

5. Click **Next**: **Disks >**. Select the required disks from the drop-down menu. Click **Next**.
6. Click **Next: Networking >** and enter the network details (see Figure 12 and Figure 13 on page 16).

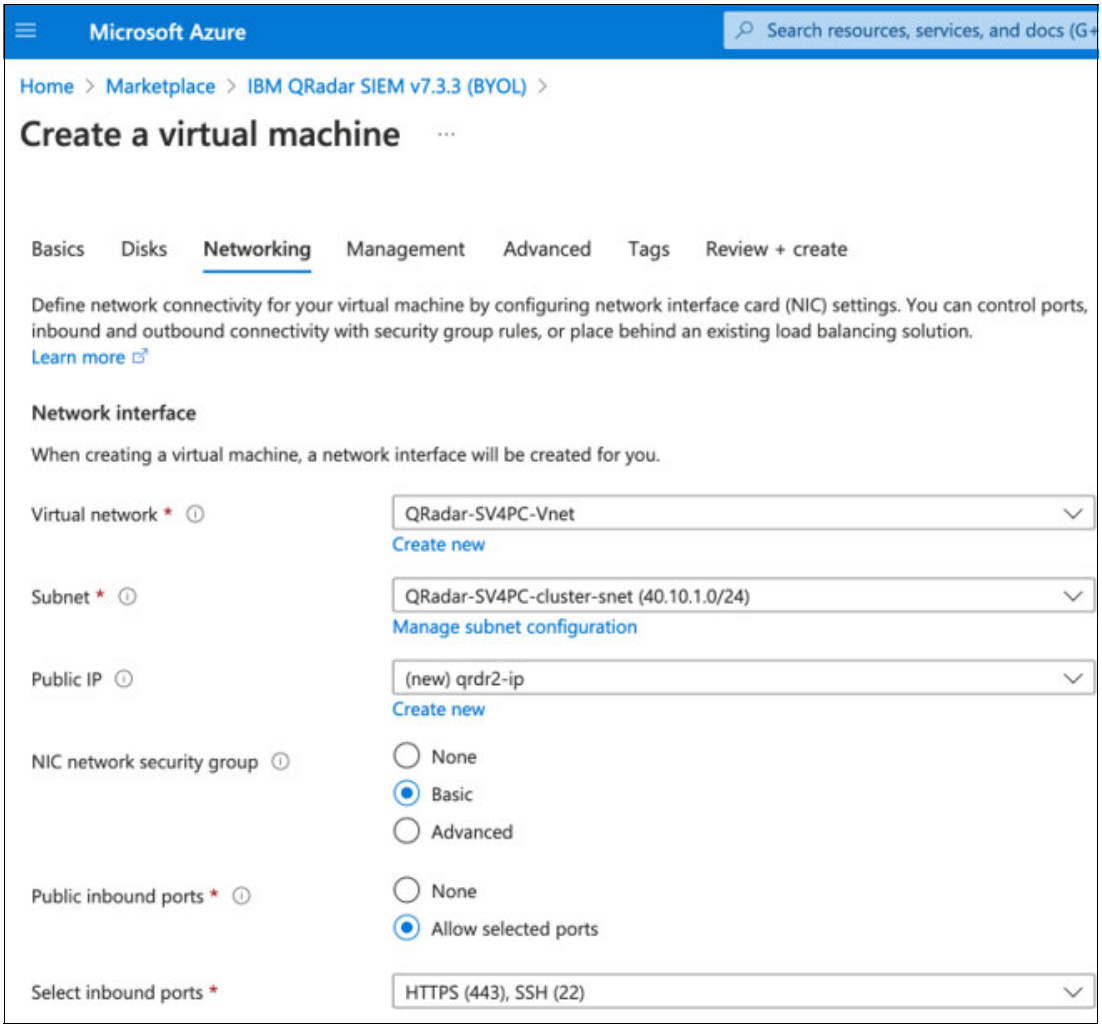


Figure 12 Networking, configure VM settings

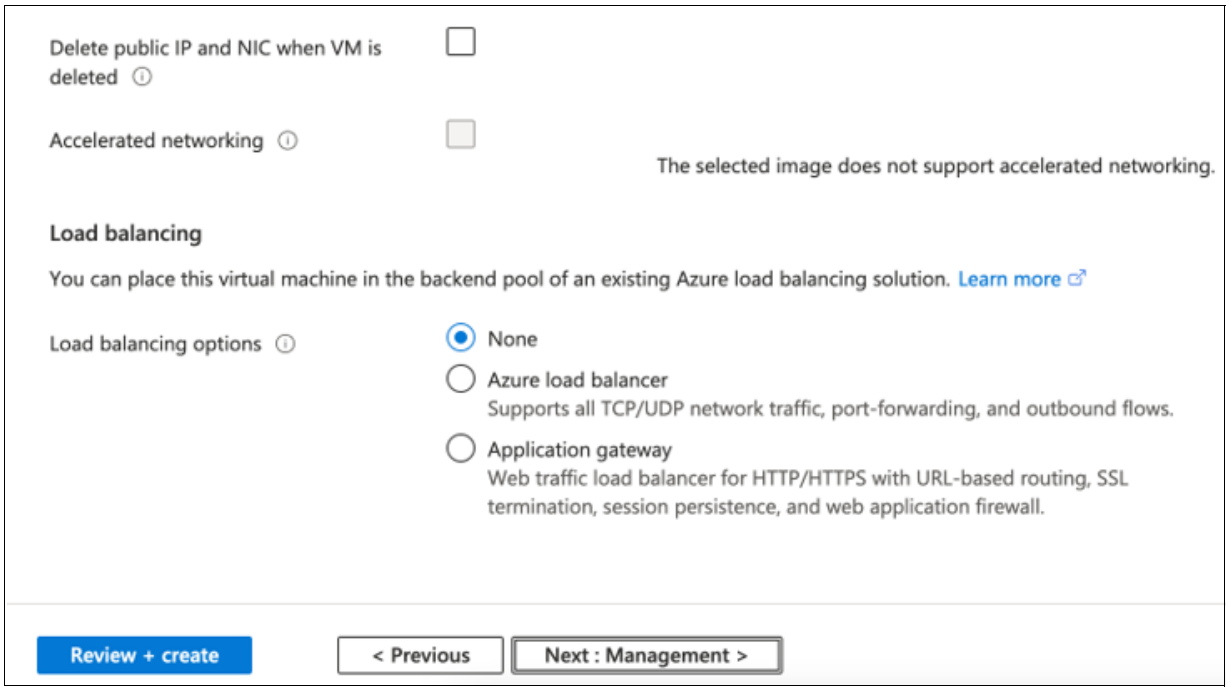


Figure 13 Networking, configure VM settings

7. Click **Next**: **Management >** and then, select the wanted options.
8. Click **Next**: **Advanced >** and then, select the wanted options.
9. Click **Next**: **Tags >**and then, enter the wanted name as a tag.

10. Click **Next: Review + Create >**. Based on the information that was entered, the review results are displayed as validation passed (see Figure 14).

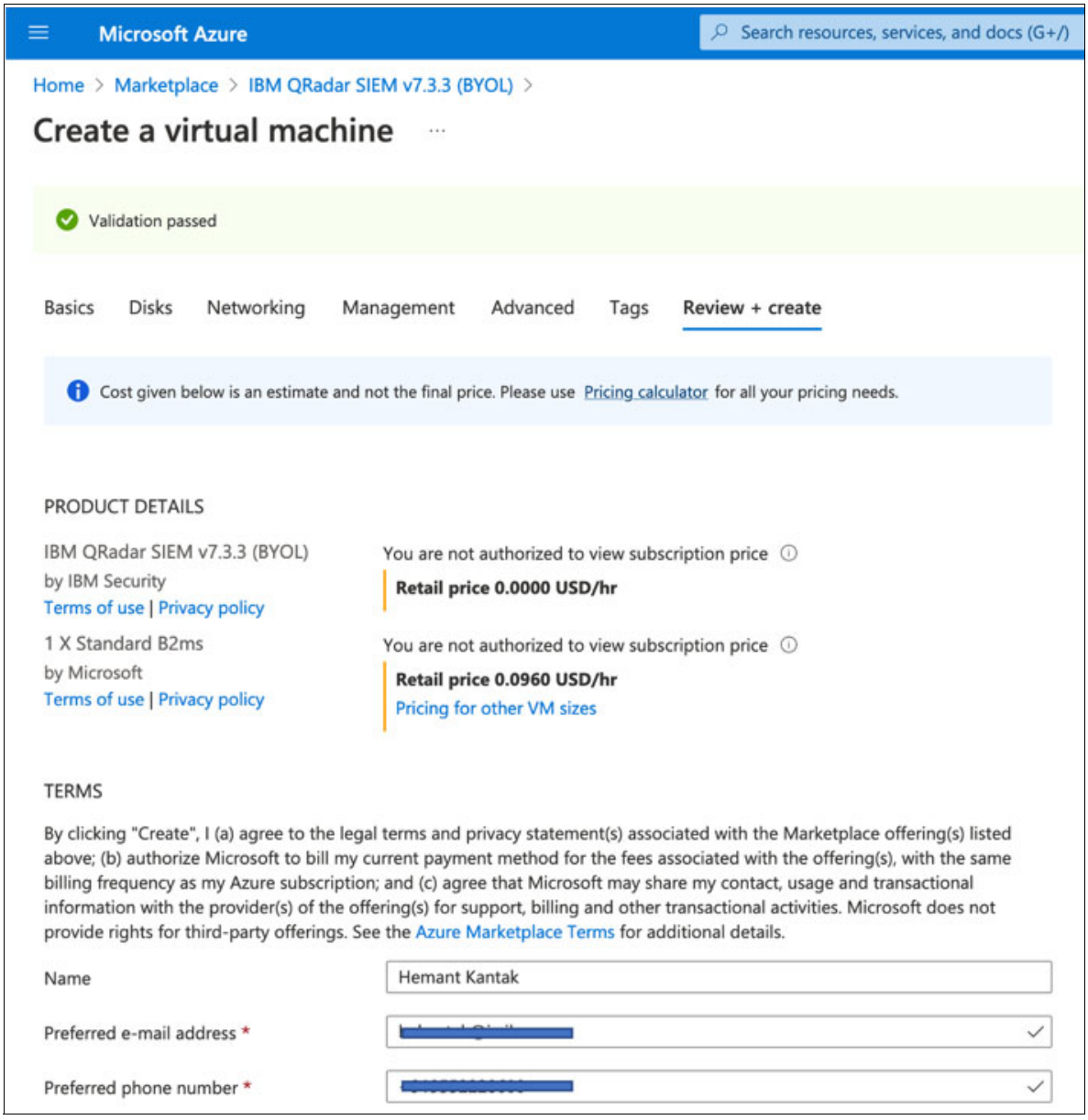


Figure 14 Review + Create, configure VM settings

11. Click **Create**. The deployment starts. Check the status of deployment and wait for the deployment to complete. Post deployment, check the assigned IP address to the IBM QRadar VM.

Upon logging in to IBM QRadar console with the username admin and your password, the dashboard page is displayed (see Figure 15).

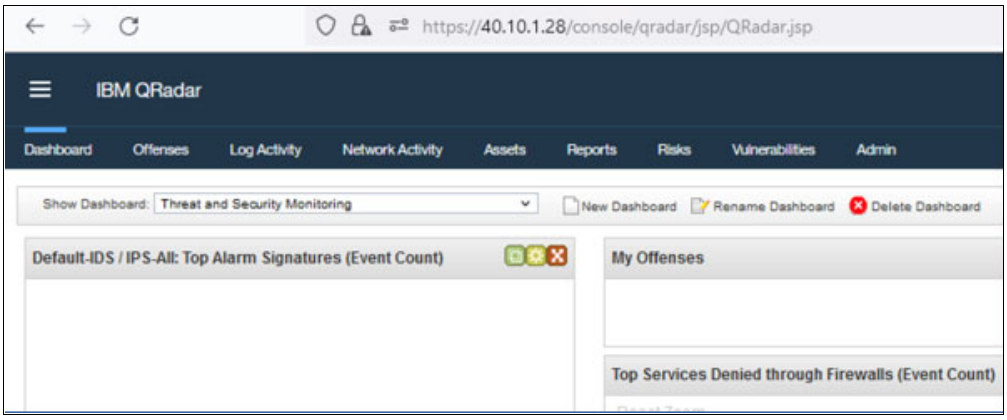


Figure 15 IBM QRadar console

Deploying IBM SV4PC on Azure

Complete the following steps to deploy IBM SV4PC on Azure:

1. Log in to `https://portal.azure.com/#home` with your username and password
2. In the search bar, search for “Marketplace”. Then, search for and select **IBM Spectrum Virtualize for Public Cloud**. Figure 15 - Figure 23 on page 24 shows the lab setup deployment steps.

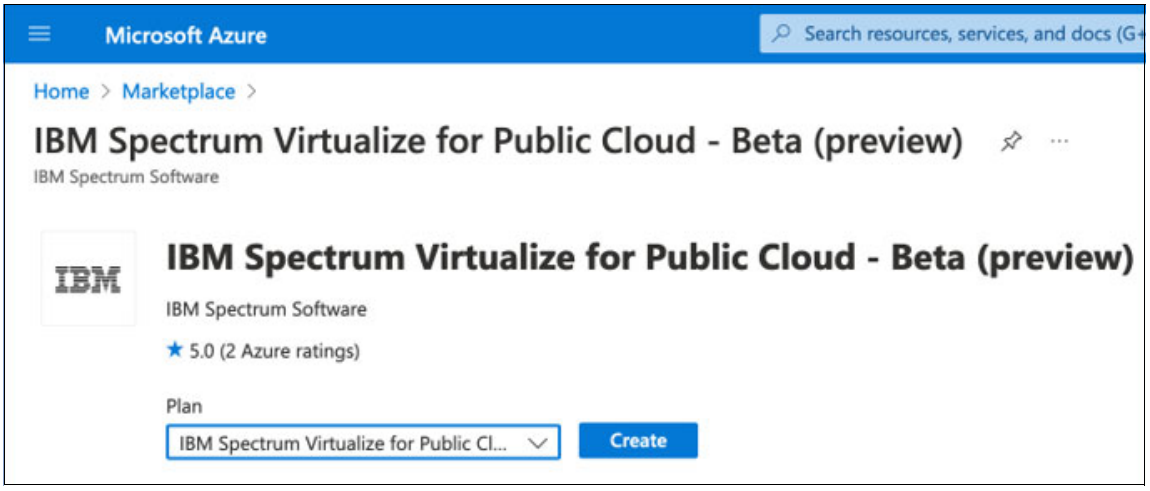


Figure 16 IBM Spectrum Virtualize for Public Cloud

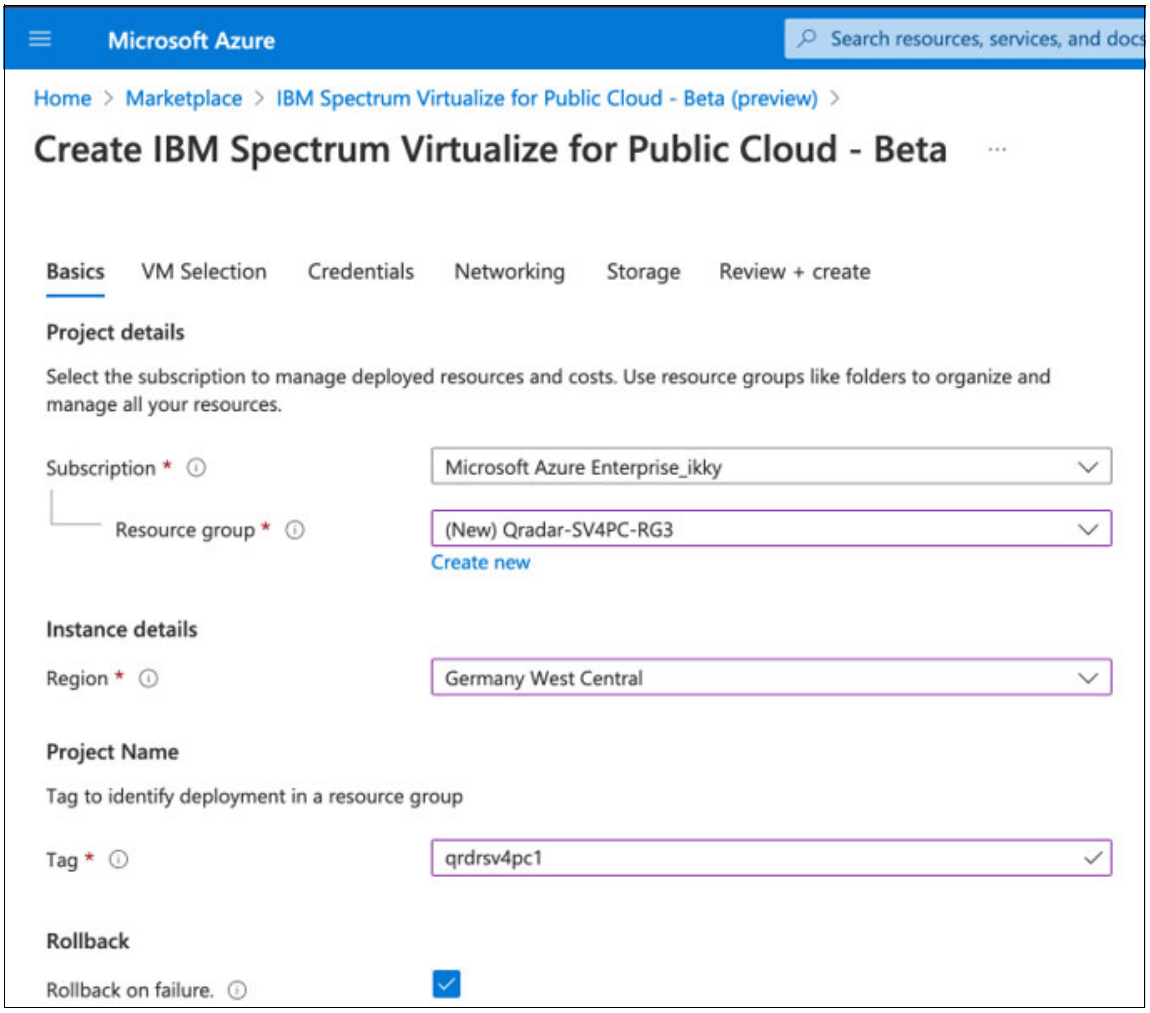


Figure 17 Create IBM Spectrum Virtualize for Public Cloud

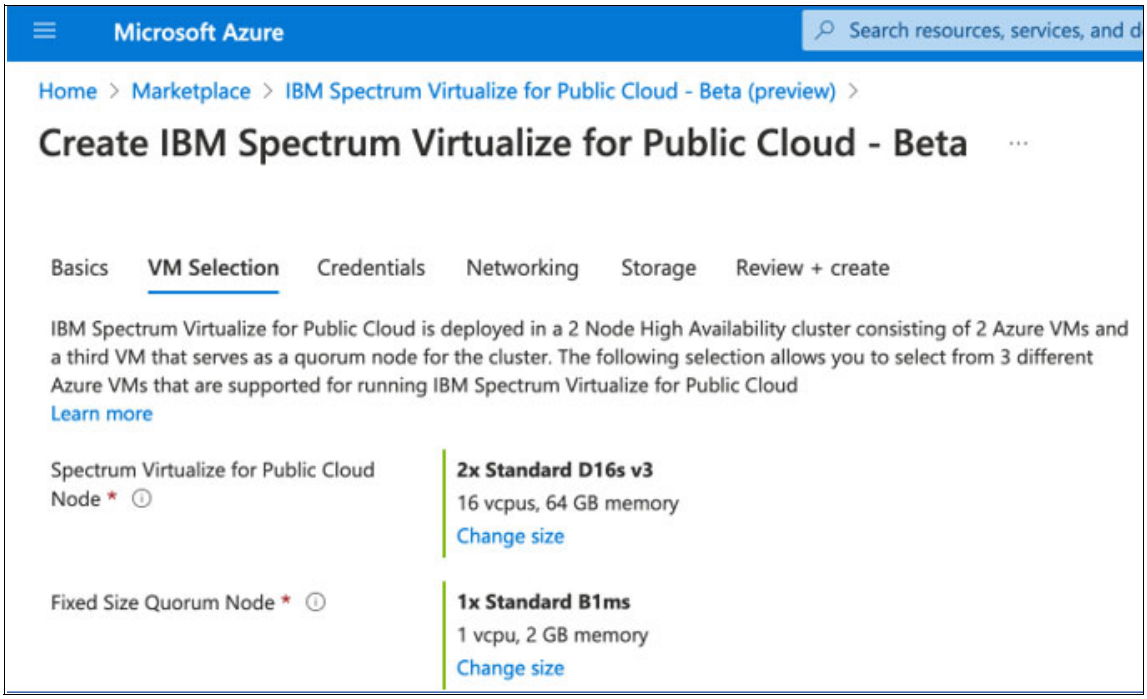


Figure 18 VM selection, IBM Spectrum Virtualize for Public Cloud

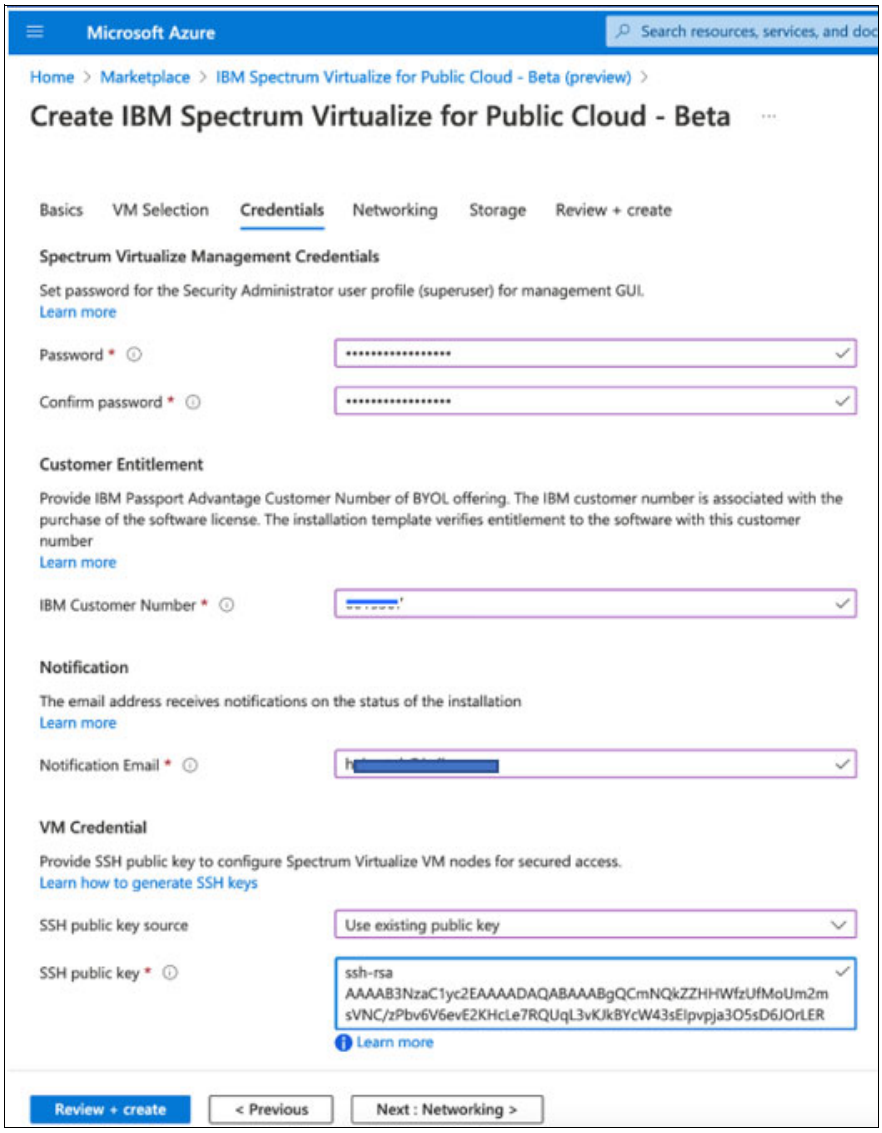


Figure 19 Credentials, IBM Spectrum Virtualize for Public Cloud

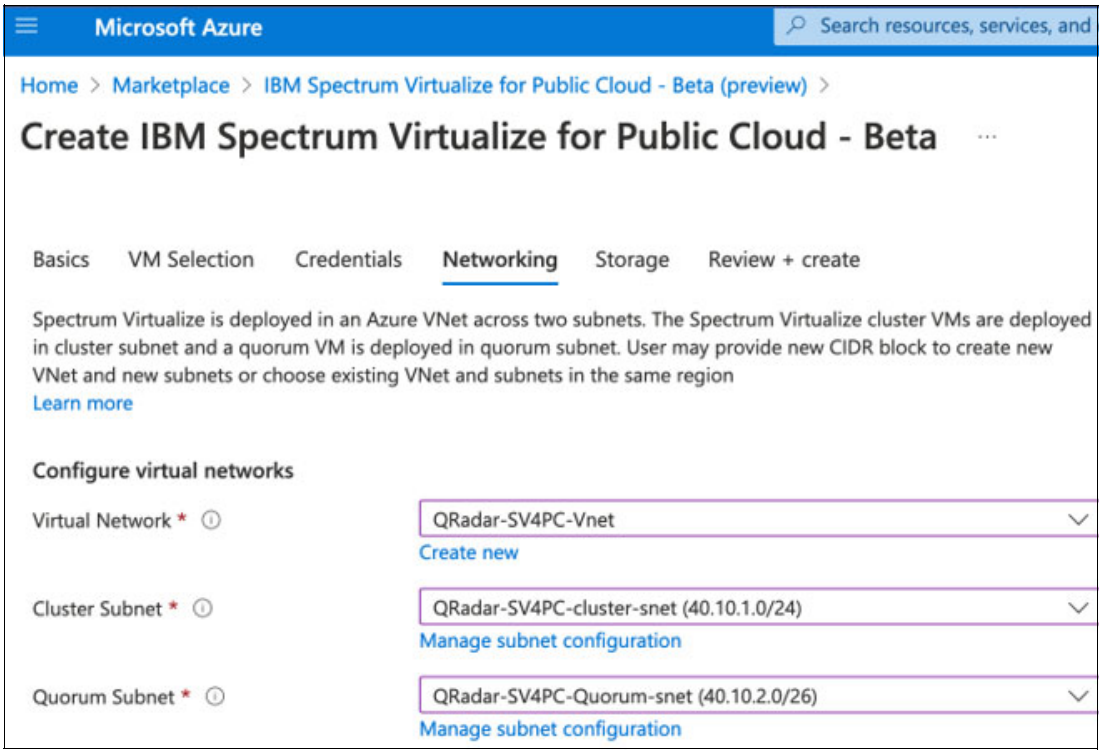


Figure 20 Networking items for IBM Spectrum Virtualize for Public Cloud

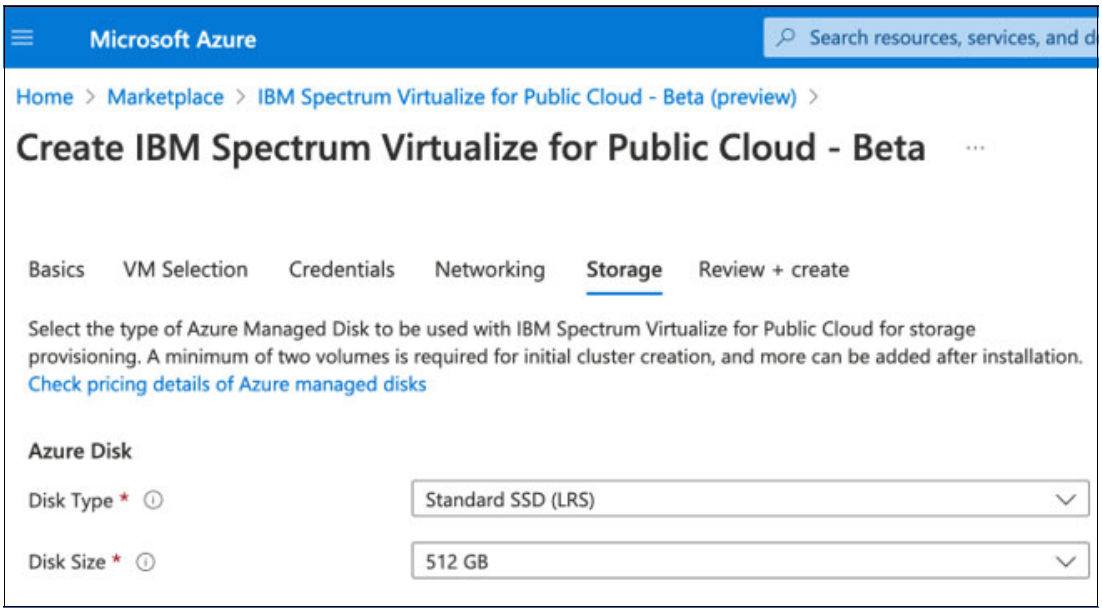


Figure 21 Azure Storage selection for IBM Spectrum Virtualize for Public cloud

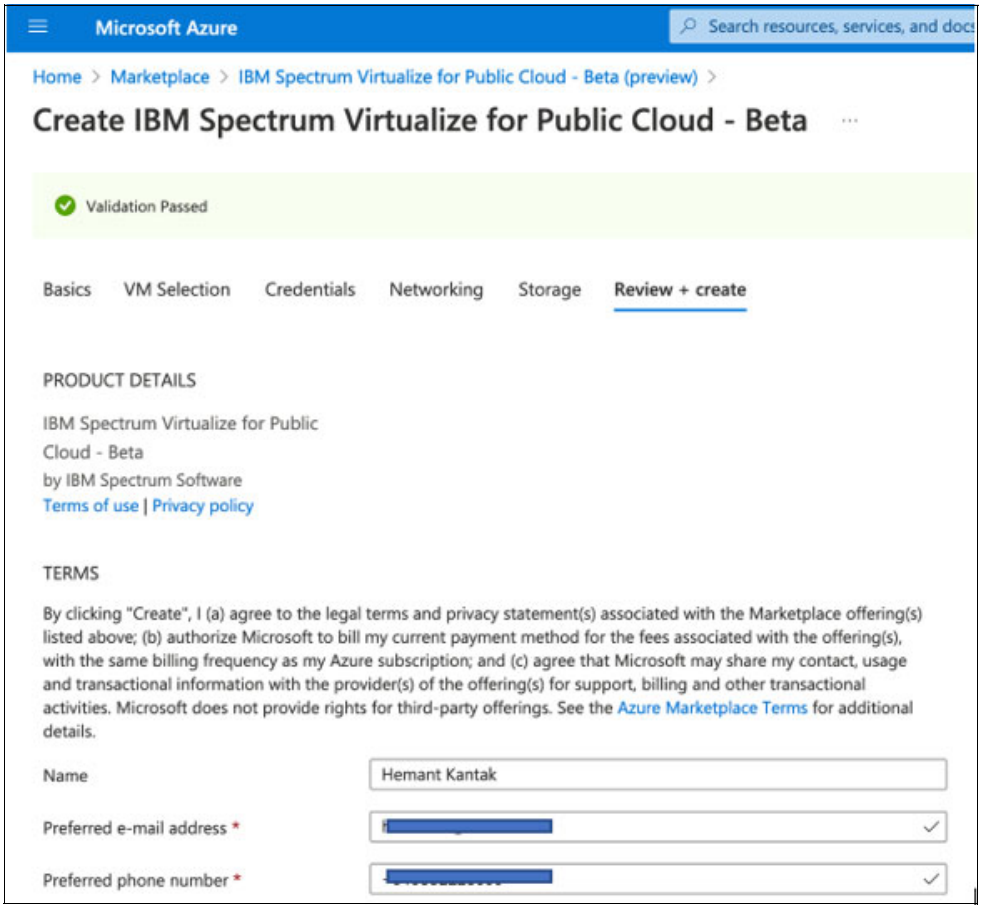


Figure 22 Review + Create, IBM Spectrum Virtualize for Public Cloud

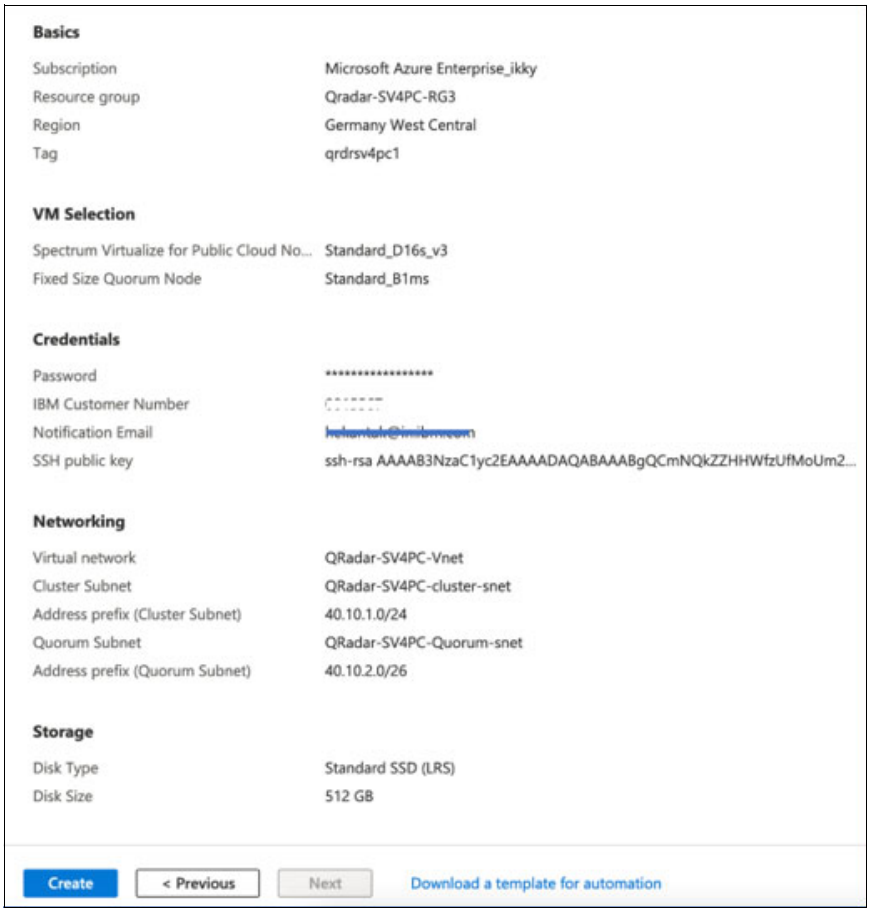


Figure 23 Create IBM Spectrum Virtualize for Public Cloud

Setting up audit log forwarding from IBM SV4PC

Complete the following steps to enable audit log forwarding from IBM SV4PC to IBM QRadar:

1. Log in to the SV4PC GUI as `superuser`.
2. Click **Settings** → **Notifications** → **Syslog** and then, select **Create Syslog Server**.
3. Enter the IP address of IBM QRadar host (do not change the default value for the port). The Syslog is configured for lab setup (see Figure 24).

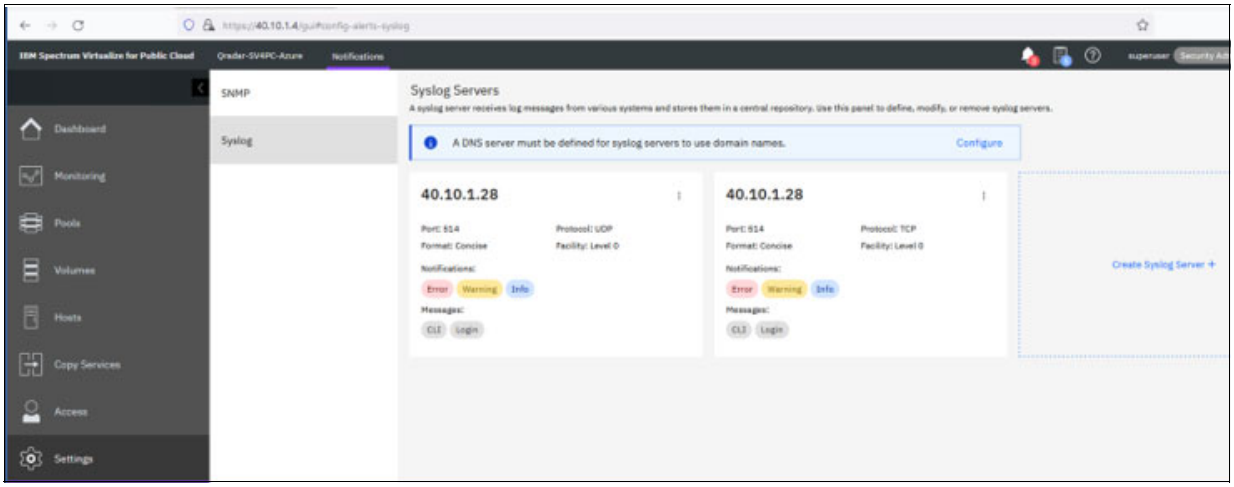


Figure 24 Setting up Syslog audit logging for IBM SV4PC

The syslog events that are forwarded by IBM SV4PC are understood by IBM QRadar as Linux events and a Log source is automatically defined. Although this setup works for most of the login and operating system operations, the storage-specific events need other categorization, as described next.

Working with IBM QRadar Events

This section describes how to use the Device Support Module (DSM) editor to correctly categorize the storage-related actions events that are incorrectly mapped as Linux events. Also, after an event mapping is created, subsequent events are mapped correctly. The process must be repeated for every storage event you want to monitor.

Under IBM QRadar's Log Activity tab, select the events from Action drop-down menu that must be categorized. Then, select the **DSM Editor** option (see Figure 25).

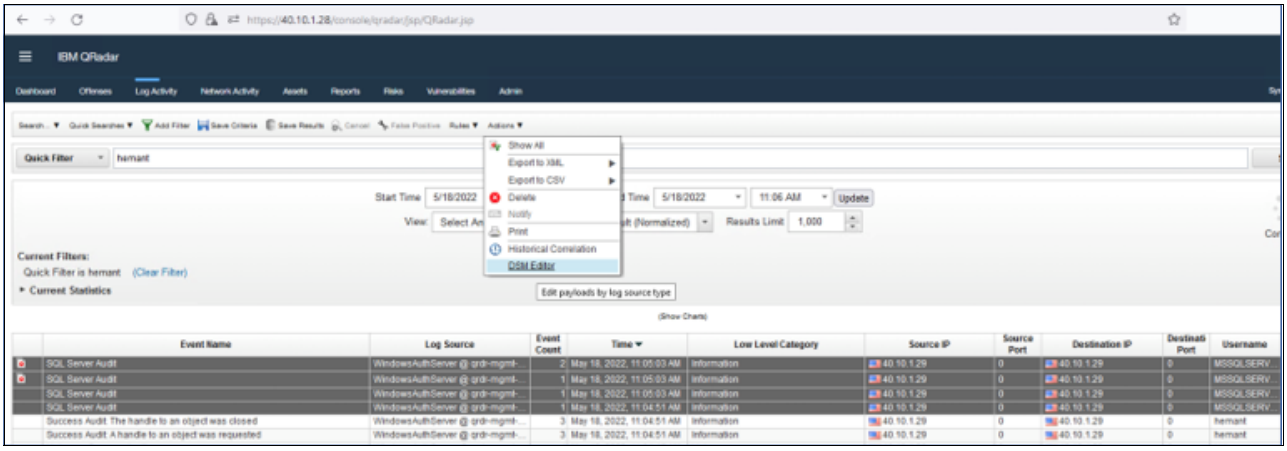


Figure 25 Opening events in DSM editor

The DSM editor shows the selected sample events that were generated for the SQL server audit action (see Figure 26).

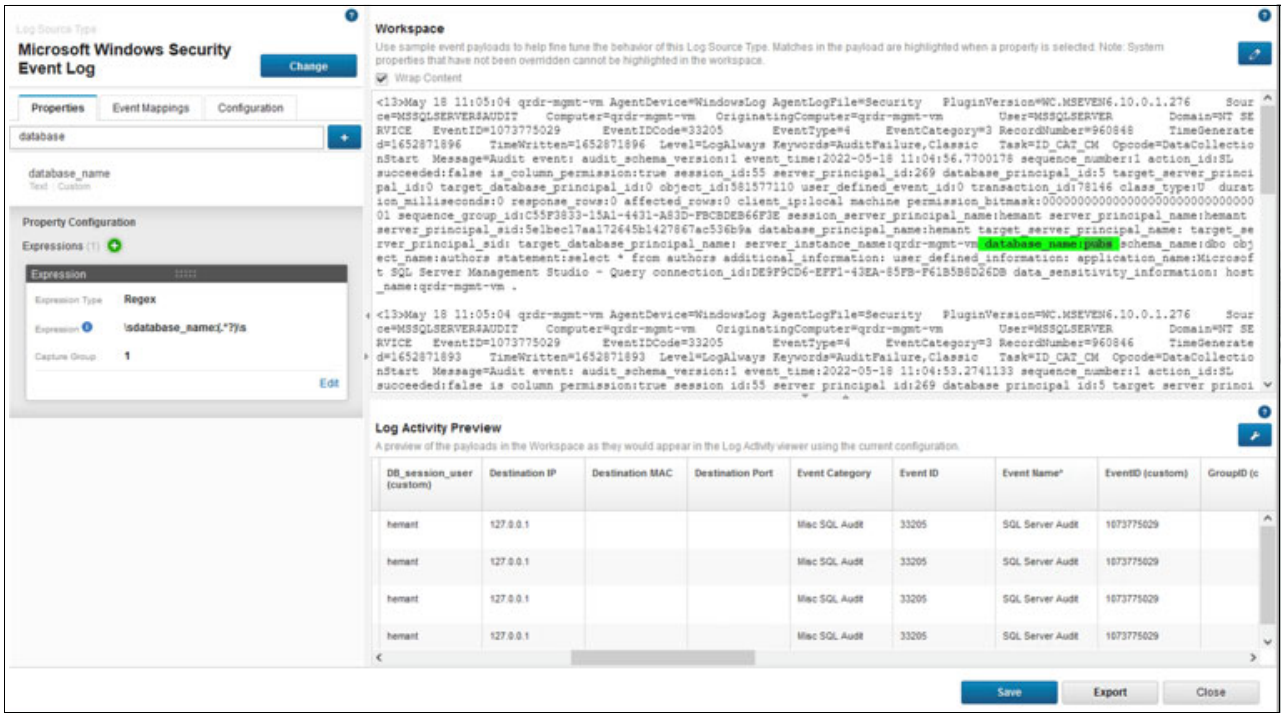


Figure 26 Sample audit event

Complete the following steps to correctly parse the event:

1. In the Log Source Type window on the Properties tab, click the blue **+** button to create a custom property definition and then, enter the regular expression. Repeat this step for each property definition that is to be parsed. It is possible to provide multiple criteria for a property to extract specific value from the event (see Figure 27).

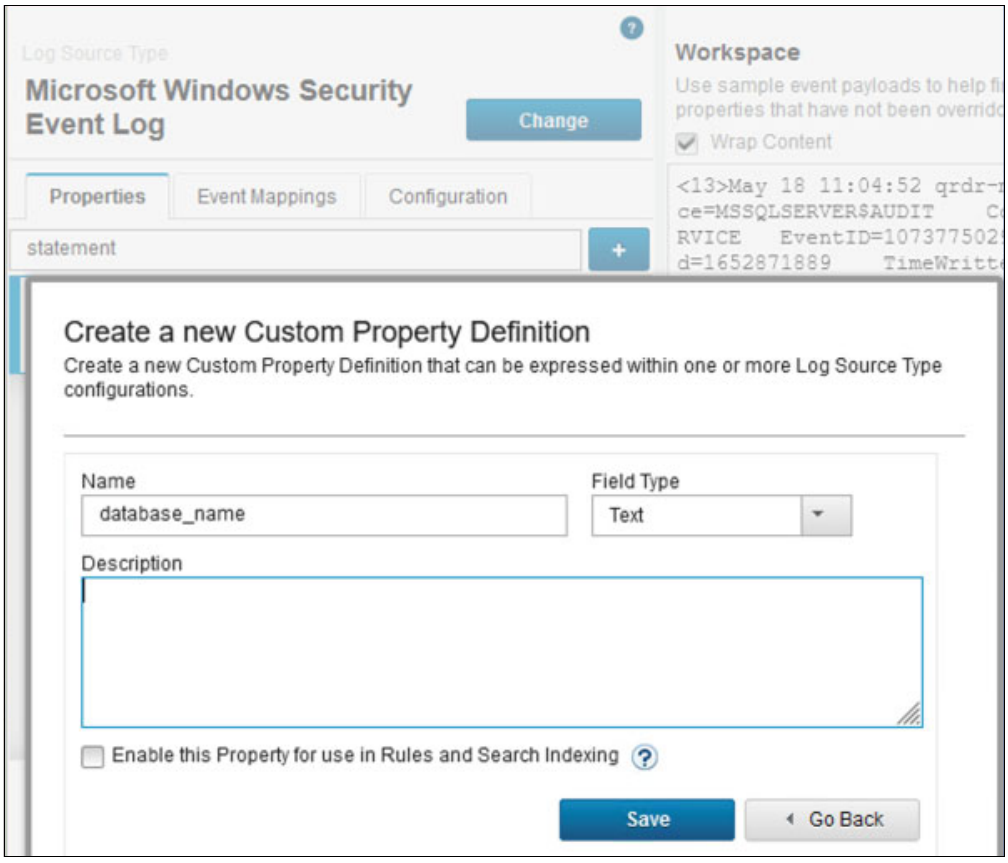


Figure 27 Regular expression for Event ID and Event Category

2. Update the custom property with the required regular expression (see Figure 28).

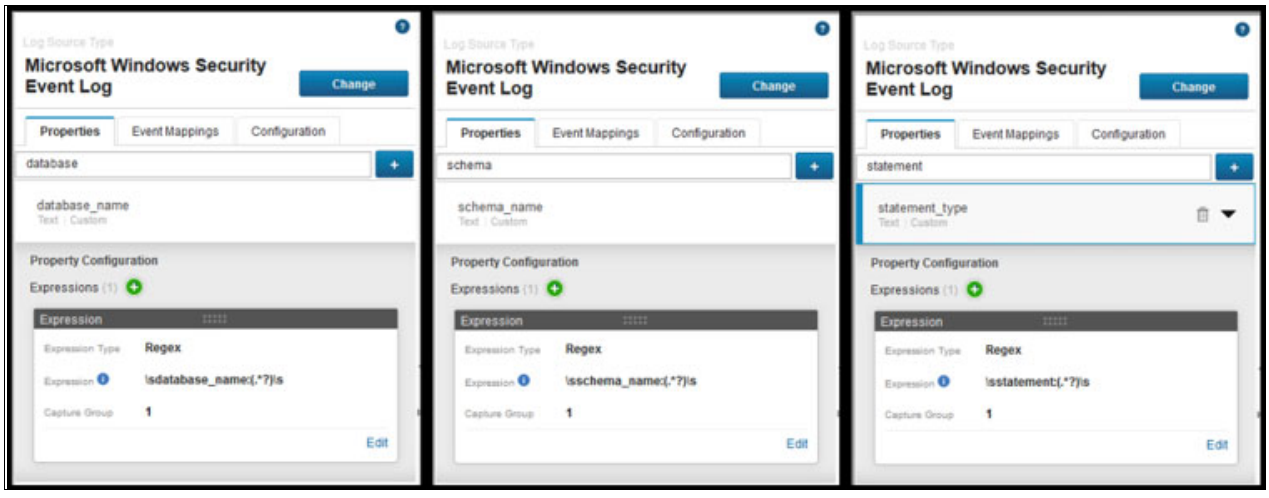


Figure 28 Regex for custom properties, event mapping

3. Click **Save**.

IBM Copy Services Manager

This section describes the Copy Services sessions setup between IBM SV4PC and IBM Copy Services Manager. For more information, see IBM Copy Services Manager User's Guide in “Resources” on page 49.

IBM Copy Services Manager includes the following key features:

- Scheduled Tasks

  Starting with Copy Services Manager Version 6.2.1, you can use a GUI wizard to schedule tasks. Currently, tasks can be scheduled against sessions only. 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; that is, one after the other. 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.

  For more information about other actions possible with Scheduled Tasks, see “Resources” on page 49.

- 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 in the following terms:

  - Single-target: The source volume site can have only one target site. Data Replication occurs from the source to the target.
  - Multi-target: 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.

  In our demo, the session type is “backup”, which is automatically detected for the safeguarded copy function.

- Copy sets

  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 the lab setup, we deployed IBM Copy Services Manager on a Windows 2019 server.

To ensure communication between IBM SV4PC storage and IBM Copy Services Manager, log in to IBM Copy Services Manager and then, click **Settings** → **Server Properties** → **Edit** and add the parameters in the server properties file (see Figure 29).

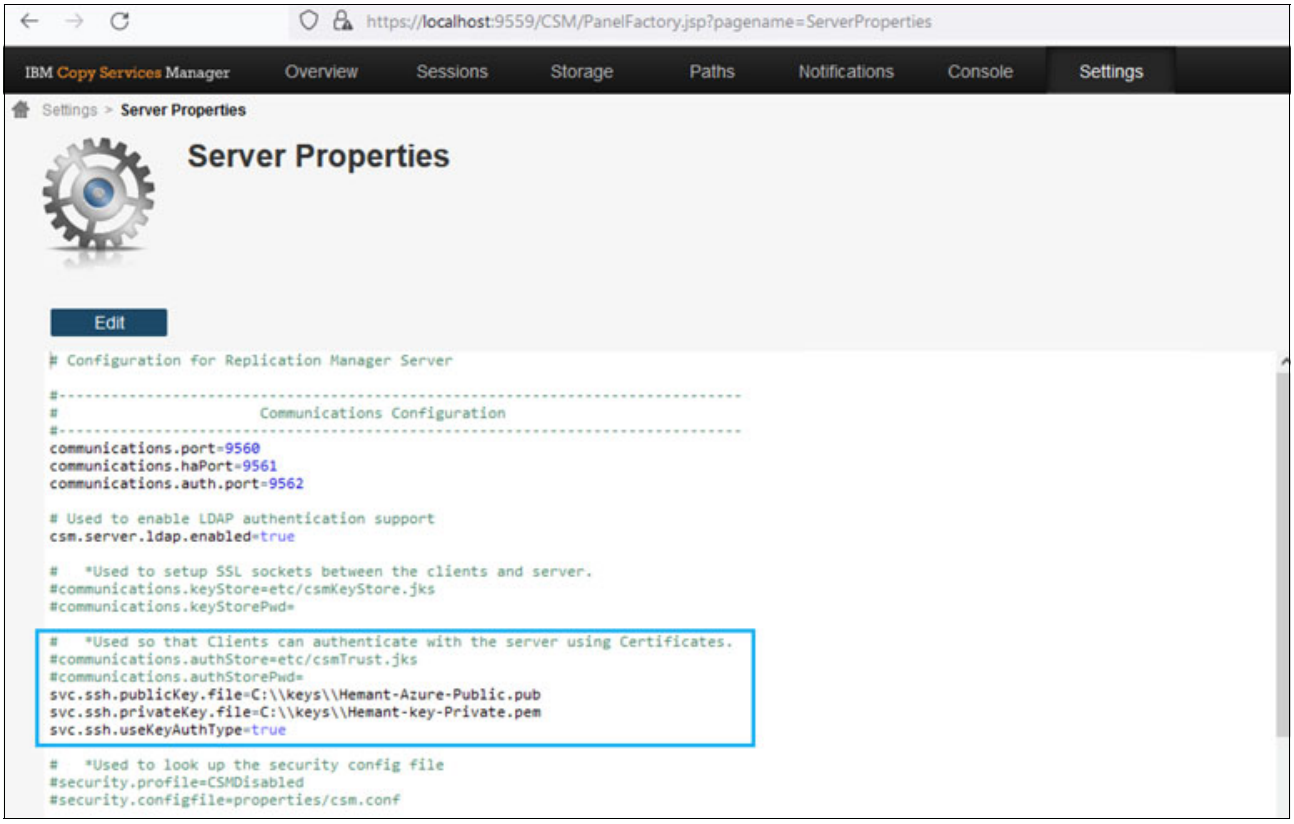


Figure 29 Copy Services Manager server property file for SSH Public Key for IBM QRadar

Creating a Safeguarded Copy session in Copy Services Manager

For the lab setup, Group Name (Automatically Generated Session) was chosen for the configuration, with the Safeguarded Copy and the session type is Backup.

Sessions are automatically detected for the Safeguarded Copy function in IBM Copy Services Manager (see Figure 30).

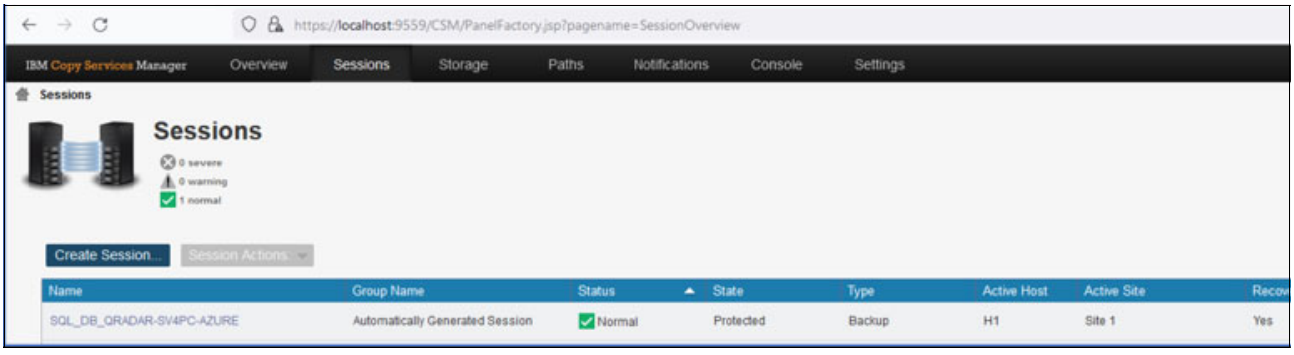


Figure 30 Session name and type for Safeguarded Copy

Creating a Scheduled Task to issue Safeguarded Copy backup in Copy Services Manager

Complete the following steps to create a scheduled task to issue Safeguard Copy backup in Copy Services Manager:

1. Log in to Copy Services Manager and click **Settings**. Then, select **Scheduled Tasks** from the drop-down menu. Click **Create Task** to start the task creation wizard.
2. Enter a suitable name and description for the task and then, click **Next**.
3. Select the **No Schedule** option in “How often do you want the task to run” window and then, click **Next**.
4. Click **Add Action** in the What action would you like to perform? window.
5. Select the **Command** option in the Type combination box and then select, **Copy Services session** name and the **Backup** option from the Command combination box. Click **OK** (see Figure 31).

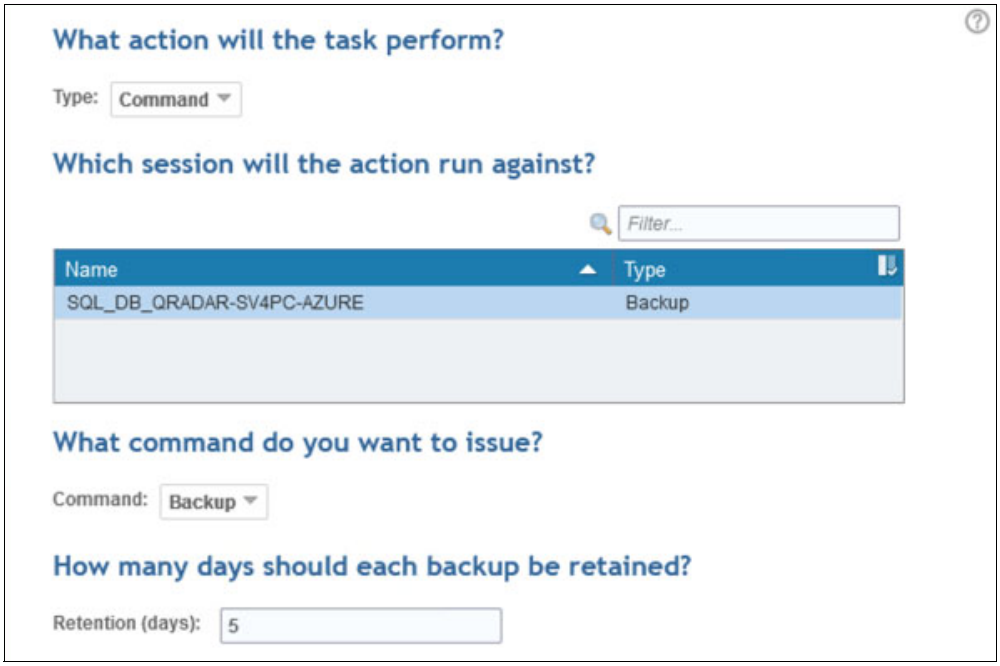


Figure 31 Scheduled Task Actions (step 1)

The last window in the wizard is the Scheduled Task Summary window of the scheduled task (see Figure 32).

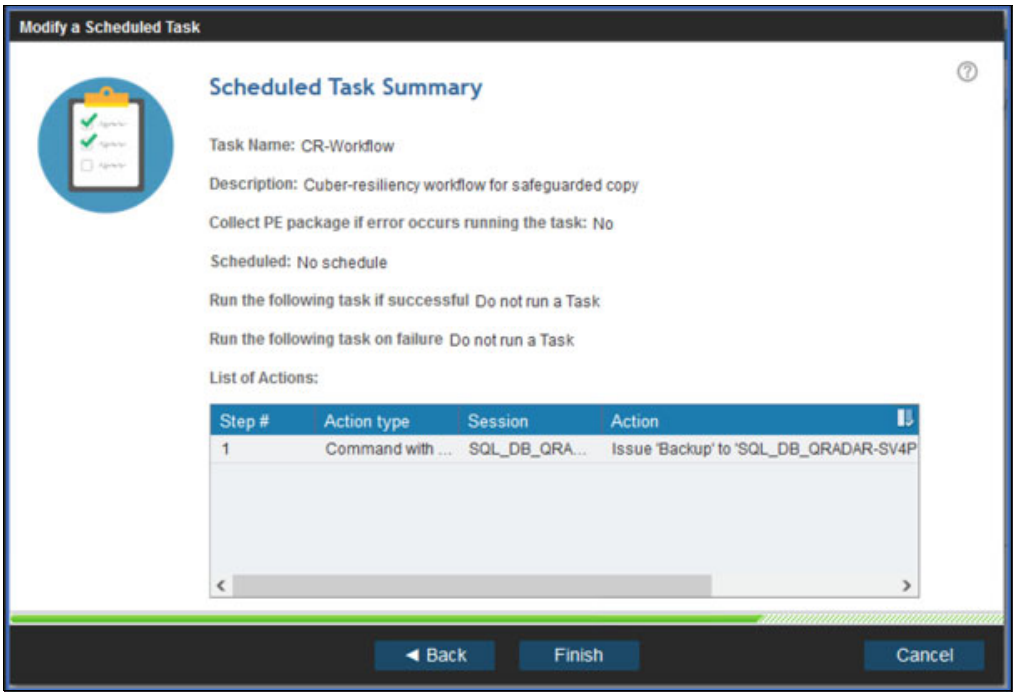


Figure 32 Scheduled Task Summary window

6. Review the actions and then, click **Finish** to complete the scheduled task creation wizard.

Threat detection in IBM QRadar

Threats are detected by the rules engine inside IBM QRadar. This rules engine applies various conditions to the normalized events to determine any threat.

After a threat is detected, its severity can be determined and a response can be generated that is based properties that are extracted from the source events.

In addition to the response, the IBM QRadar administrator can choose to raise an offense. The sample rule configuration that is used to determine the threat of a brute force login attack is described next.

Complete the following steps to build a cyber-resiliency workflow in IBM QRadar:

1. Log in to IBM QRadar with administrator's privileges. Click the **Admin** tab and then, click **Custom Actions** → **Define Actions** and then, click **Add** to define the custom action.
2. Define a custom action as shown in Figure 33. Notice that the `Copy Services Manager_USER` and `Copy Services Manager_PASSWD` parameters are base64-encoded strings.

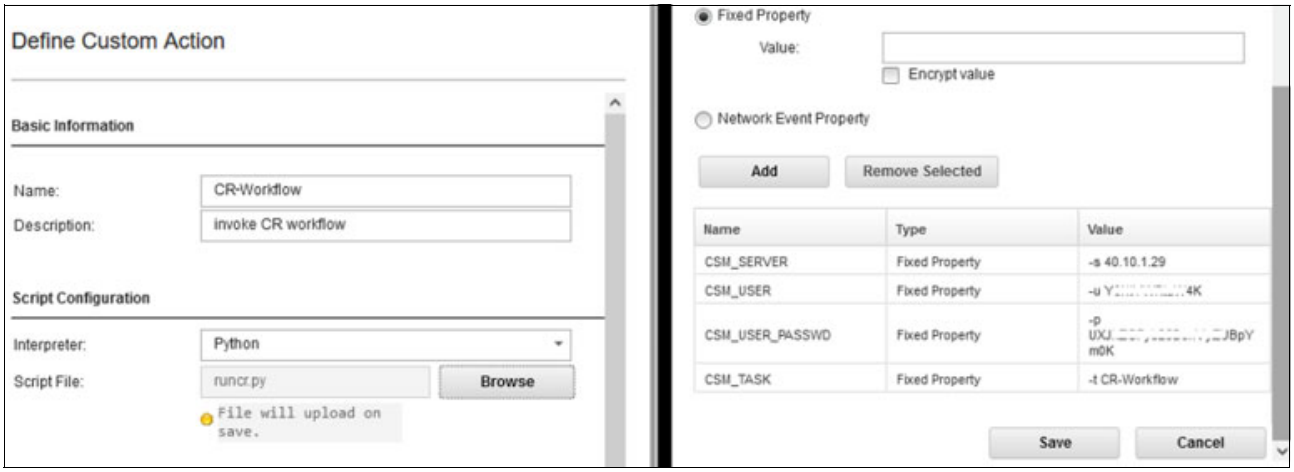


Figure 33 Custom action definition

> **Note:** The sample Python script is available on GitHub. For more information, see "Resources" on page 49.

3. Click **OK** to save the changes and acknowledge the dialog box to deploy the script.
4. Return to the Admin tab and notice the message regarding undeployed changes. Click **Deploy Changes** to deploy the changes that were made (see Figure 34).

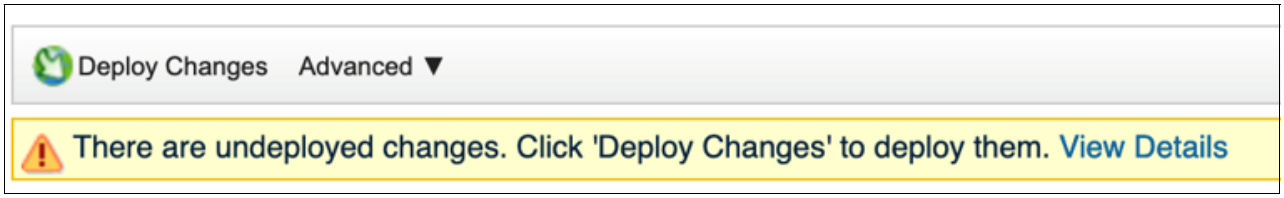


Figure 34 Deploy changes post custom action definition

5. Click the **Log Activity** tab and then, click the **Rules** drop down menu and select the **Rules** option. Click **Next** in the Custom Rule Wizard welcome window.

6. Select the **Action** drop-down menu to create the New Events rule radio button as the Source to generate the rule (see Figure 35).

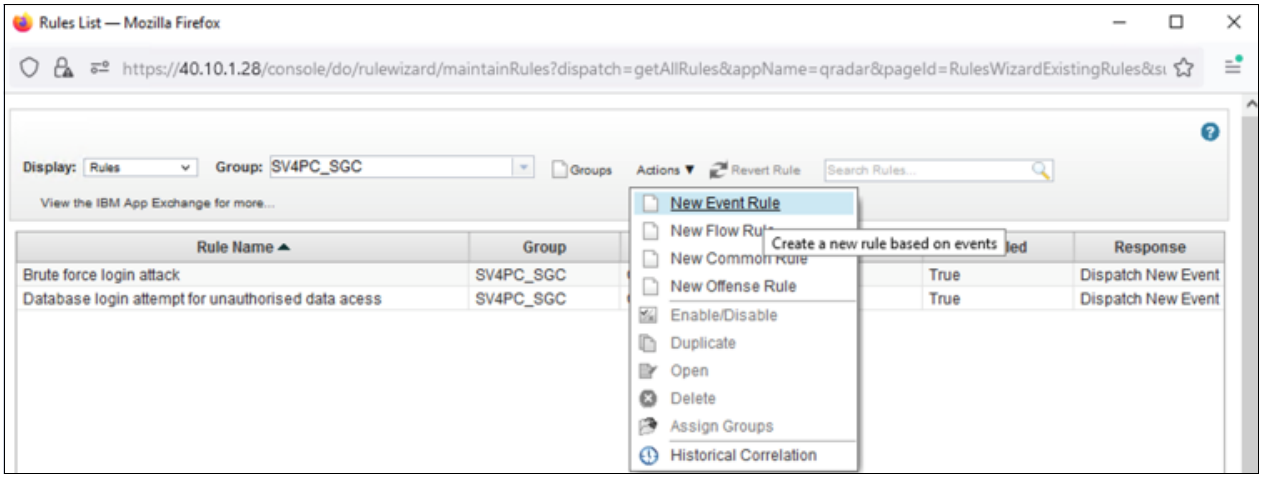


Figure 35 Creating a rule

7.Rules Test Stack Editor window, use the log source criteria to filter the rules and click the green (**+**) icon to add the first rule. The bold text act as hyperlinks for selecting the suitable properties (see Figure 36).

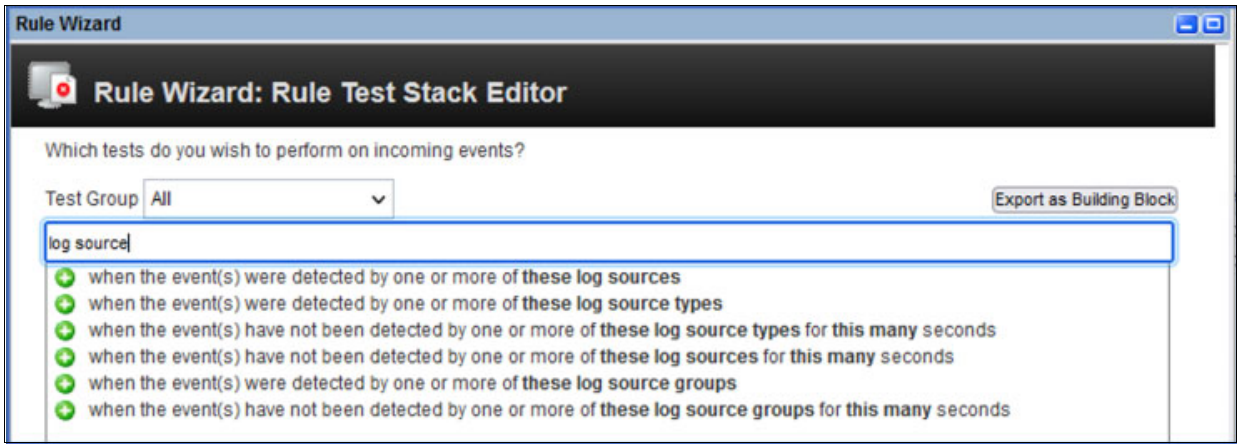


Figure 36 Filtering log source

7. Click the log sources and choose the log source that was automatically defined by IBM QRadar for the Linux host.

8. Click **Rules** to select the property. Search for at least this many events and select the green (**+**) icon to add the second rule (see Figure 37).

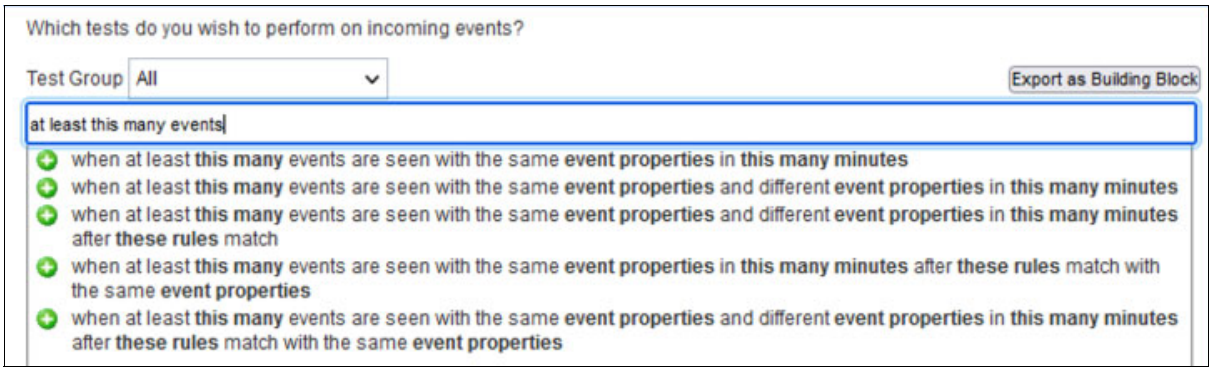


Figure 37 Filtering this many events

Make the following property value selections:

- Click **This many** and enter 5.
- Click **Event Properties** and choose **Username**.
- Click **This many minutes** and choose **3 minutes**.

9. Use the filter text and add the next rule (see Figure 38).

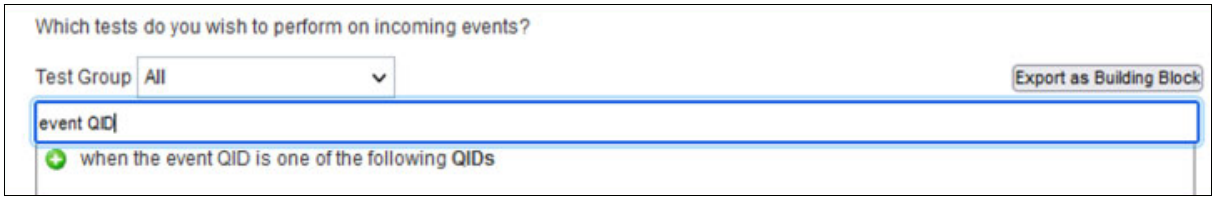


Figure 38 filtering for event QID

After all of the property values are updated, the completed rule looks similar to the example that is shown in Figure 39.

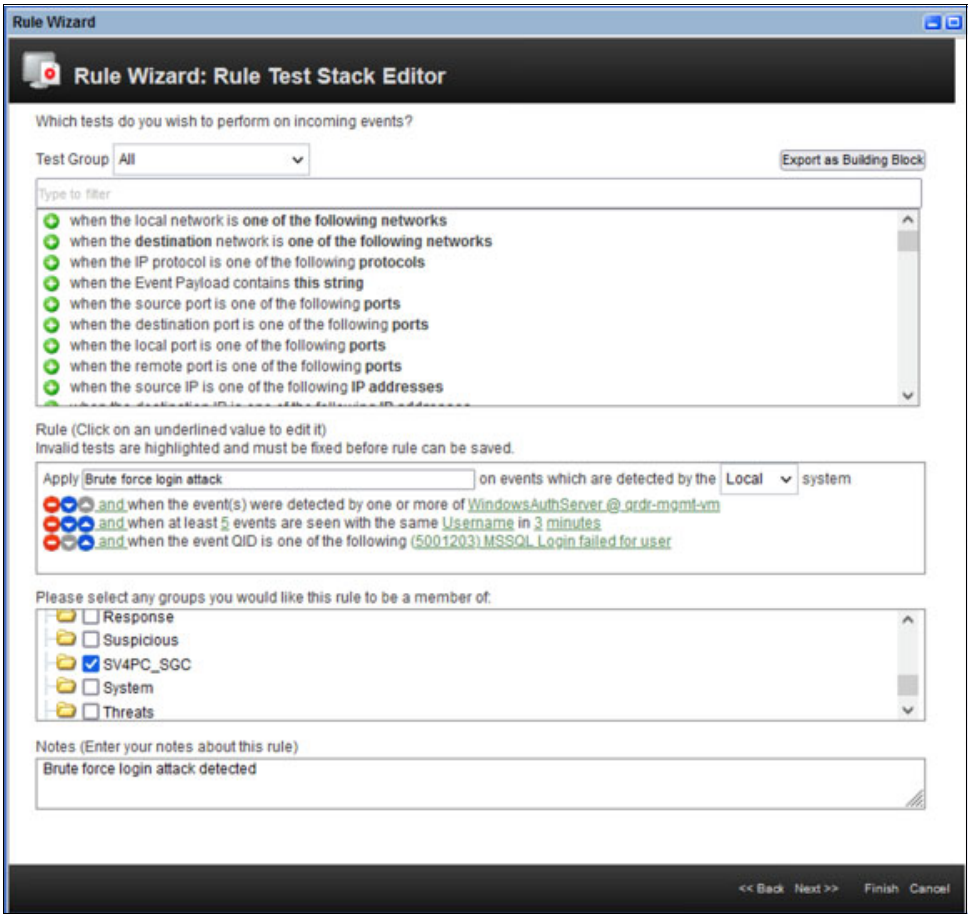


Figure 39 Rule that is defined by selecting appropriate property values

The rule also is assigned a name for identifying its purpose and a group is chosen of which this rule is to become a member.

In our lab setup, the rule was made part of the group `SV4PC_SGC` (for rule categorization). Of the three groups that were available, the `SV4PC_SGC` group name was custom created. Also, the notes that describe the purpose of the rule are provided for future reference.

10. Click **Next** to configure the Rule Response window, which is divided in the following sections:
    - Rule Action

      Various properties are configured in this section. An offense is also generated when the rule is triggered, and the property Username is used to identify the offending user who is attempting the brute force login (see Figure 40).

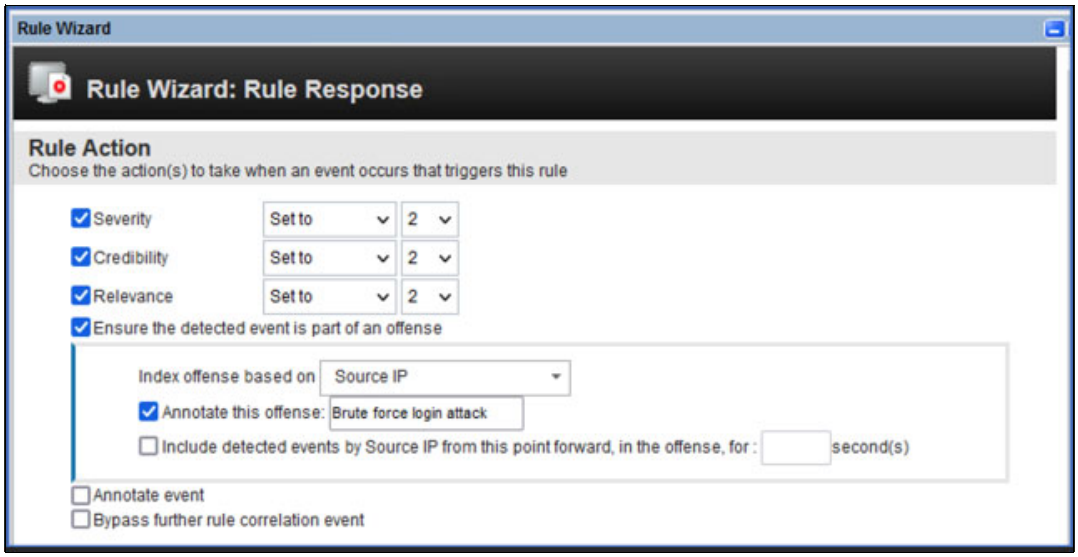


Figure 40 Configuring Rule Action

- Rule Response

  A new event is generated with a specific name and description to indicate that the rule was triggered. In this section, the custom action is also chosen in response to a detected threat (see Figure 41).

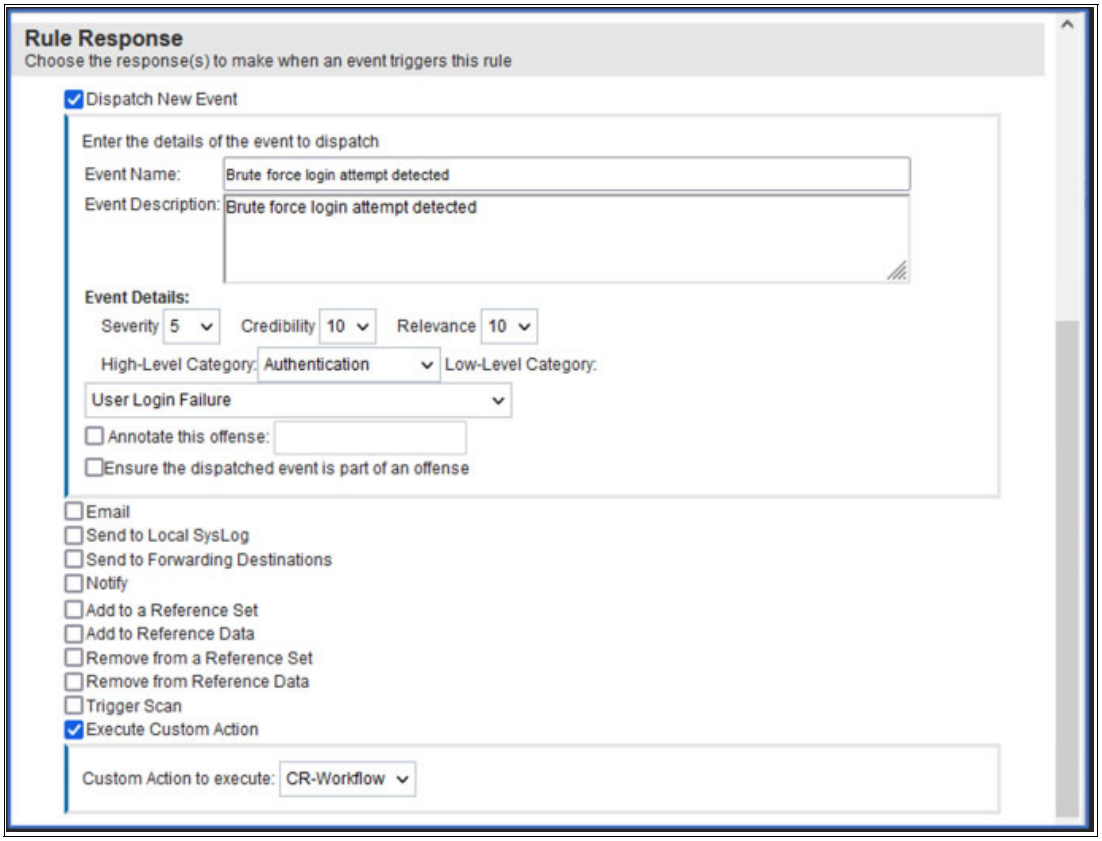


Figure 41 Configuring Rule Response

- Response Limiter

  This parameter limits the response by the rule. In this example, the rule response is set to single execution for every 30 minutes (see Figure 42).

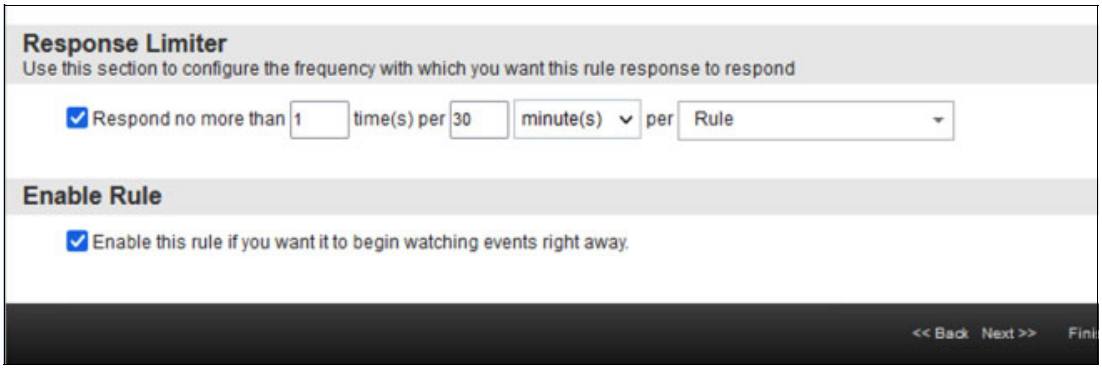


Figure 42 Rule Response Limiter and Rule State

- Enable Rule

  Multiple rules can be configured for testing different conditions to detect the threat, and a single rule can be enabled by using this property (see Figure 42).

11. The final window of the Rule Wizard shows the summary of the rule that was created. Validate the selection that is made and click **Finish** to save the rule and close the wizard (see Figure 43).

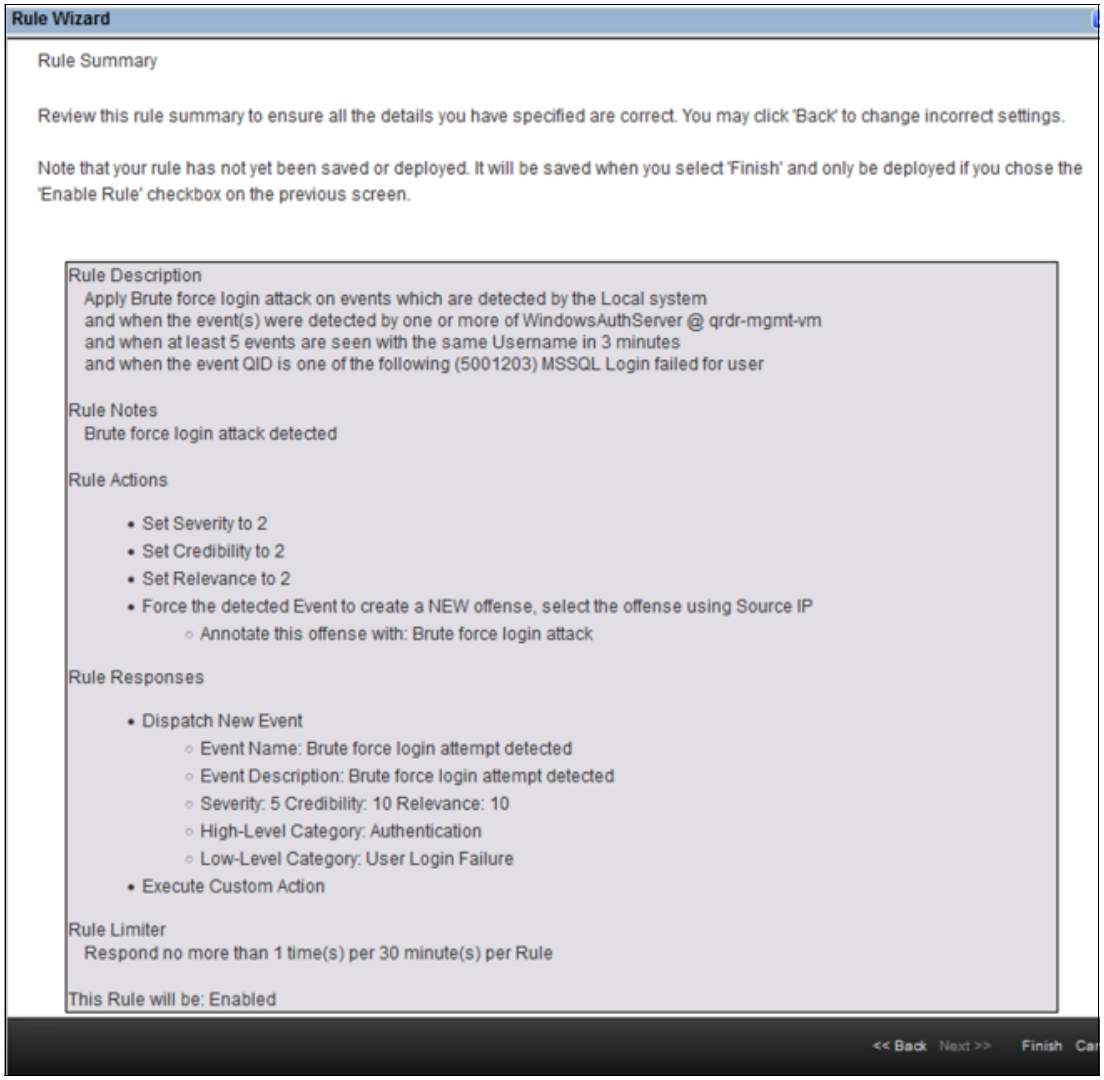


Figure 43 Rule Summary

Demonstration: Brute force login attack

This section demonstrates a brute force login attack scenario, Figure 44 shows the IBM QRadar console logs and SQL server connection in which the user attempts to log in by using an invalid password.

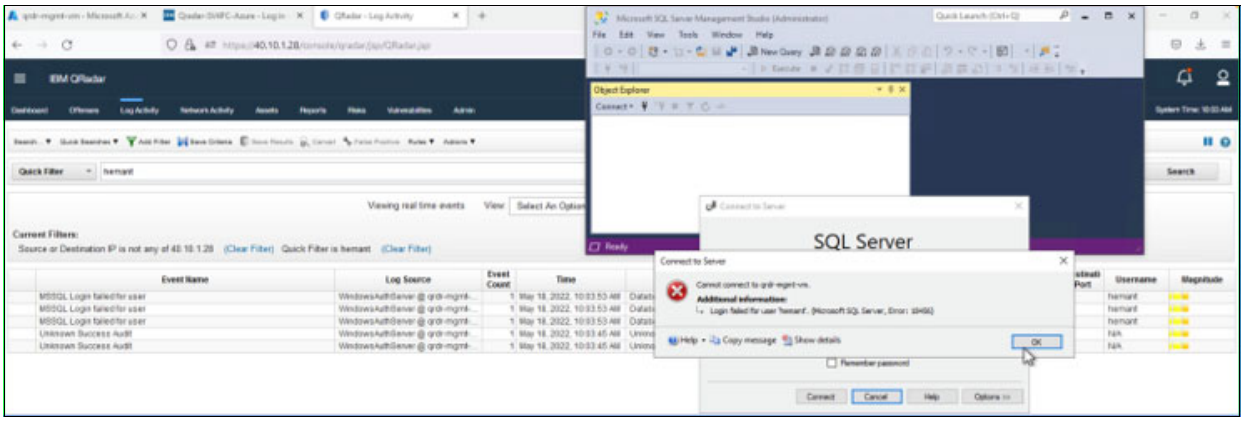


Figure 44 IBM QRadar console with MSSQL login failed events

Here, a brute force attach is depicted. Figure 44 also shows the events that are received from SQL server DB in the IBM QRadar log activity tab.

From the IBM QRadar console window, the database user attempts to log in by using invalid password. IBM QRadar monitors events. Based on the defined rules, it runs custom actions that were defined, including the Safeguarded copy. This Safeguarded copy is started inside IBM SV4PC by using IBM Copy Services Manager (see Figure 44).

After the audit log events reach IBM QRadar, the rules engine identifies the threat based on the rule conditions that were defined. Then, it runs the predefined custom user action, including the Python script that was 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 to issue Safeguarded Copy backup in Copy Services Manager” on page 30.

The brute force login case that is described here shows a threat detection from a database user environment. Similarly, by using the audit logging from other applications (for example, database or http), the syslog configuration can be extended to send application-specific events to IBM QRadar.

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

The IBM QRadar console events and IBM Copy Services Manager console events for the safeguarded copy-initiated events are shown in Figure 45 and Figure 46.

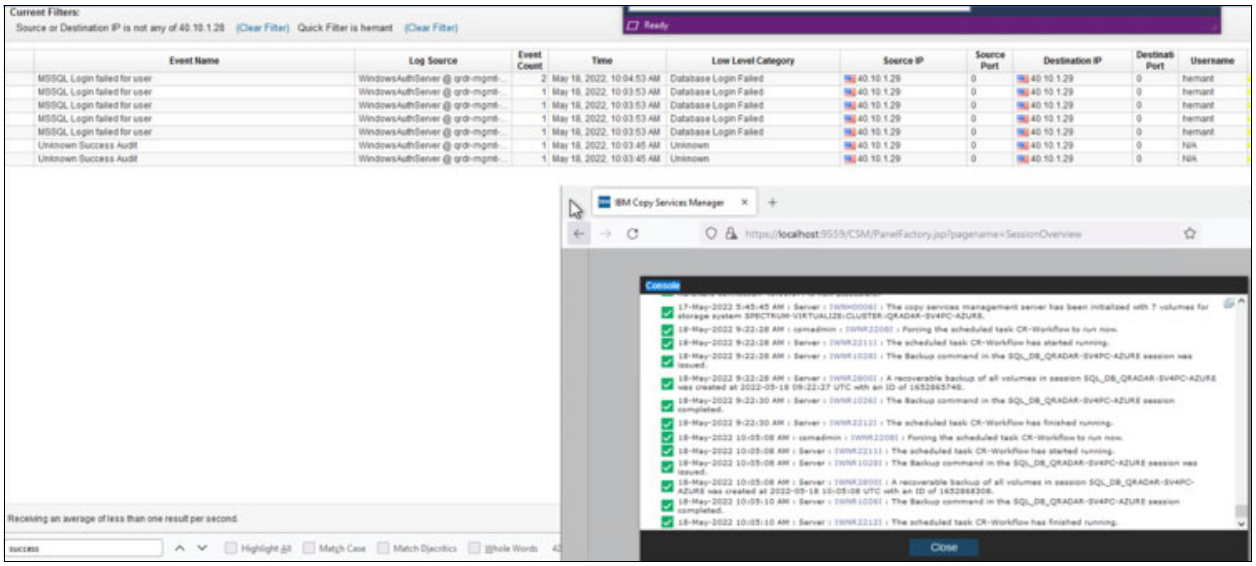


Figure 45 IBM QRadar console events and IBM Copy Services Manager console events

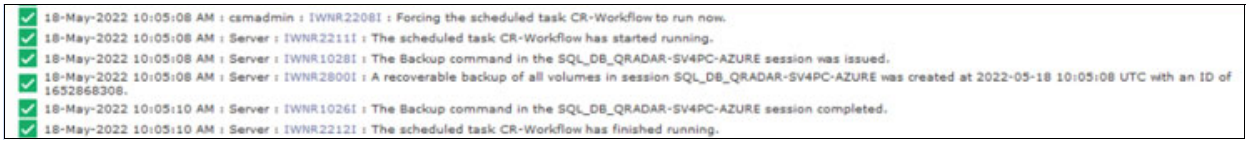


Figure 46 IBM Copy Services Manager Console Events for Safeguarded copy

The Safeguarded Copy that was created on IBM SV4PC is shown in Figure 47.

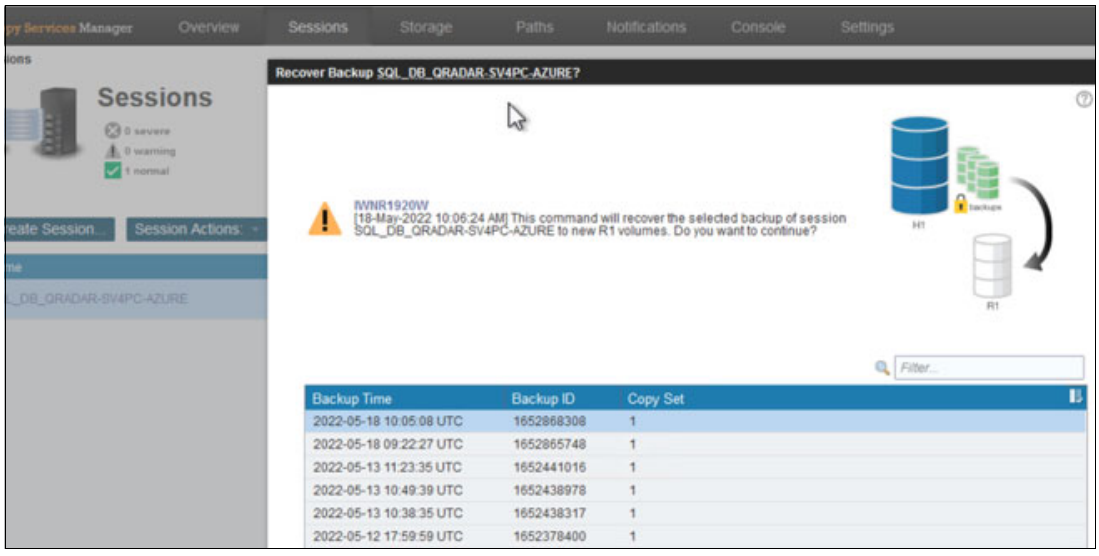


Figure 47 Backup ID, IBM Copy Services Manager

The Safeguarded Copy volume details in IBM SV4PC are shown in Figure 48.

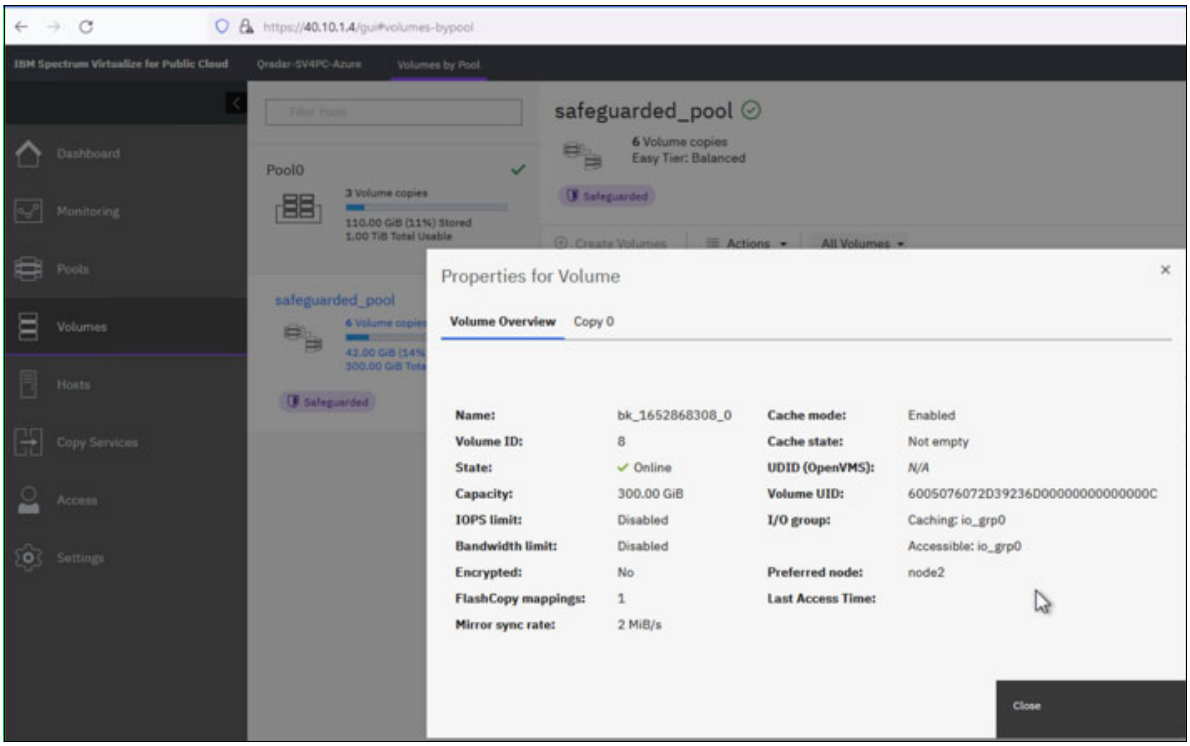


Figure 48 Safeguarded Copy created in IBM SV4PC

Sensitive data table access rule

This section provides the summary of the rules that were defined in IBM QRadar to cover data path use cases that are discussed in this publication.

The rule definition for sensitive data table access by a user who does not have access to table is shown in Figure 49.

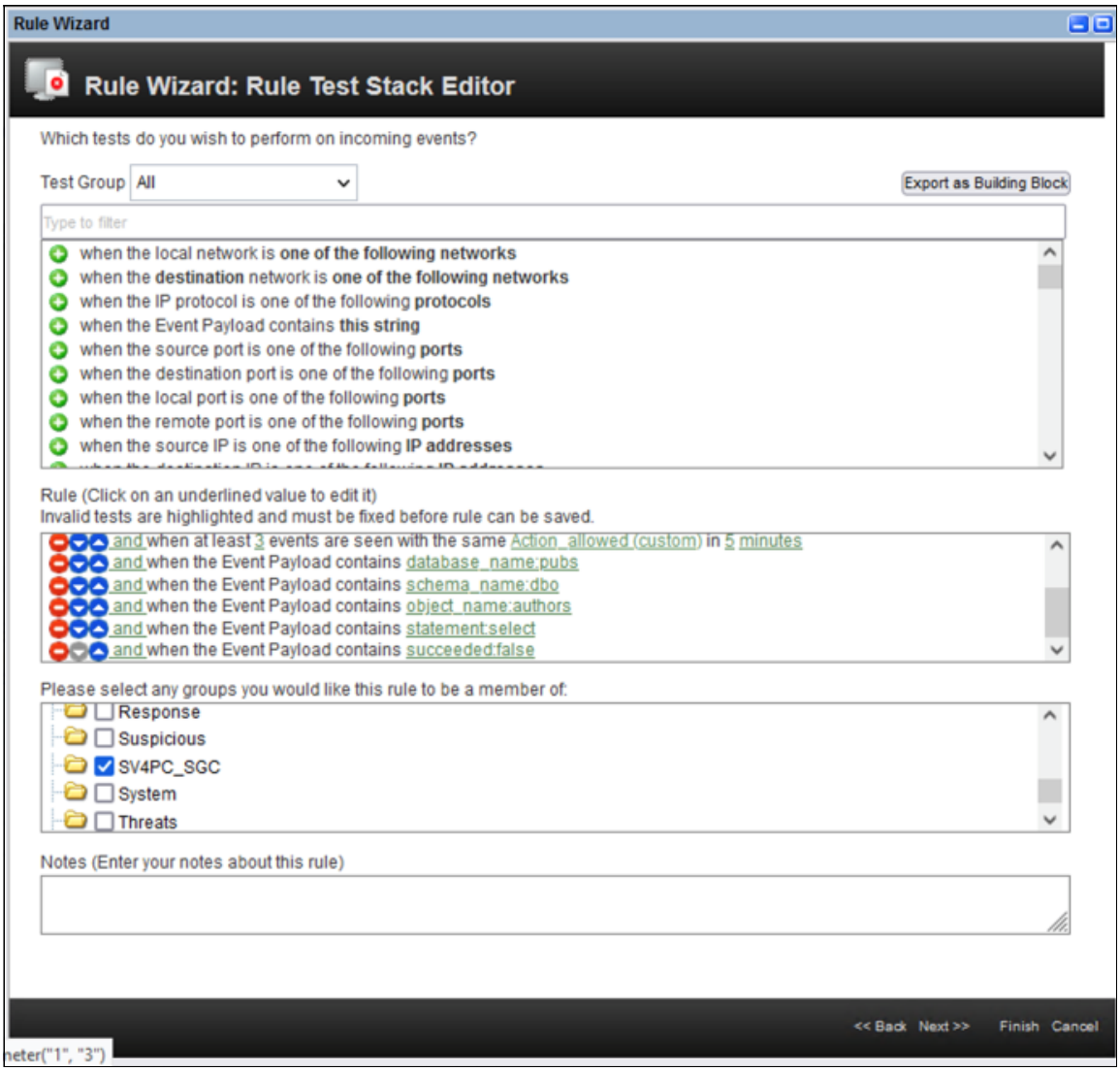


Figure 49 Rule definition for sensitive data table access by a user

The Rule Action window is shown in Figure 50.

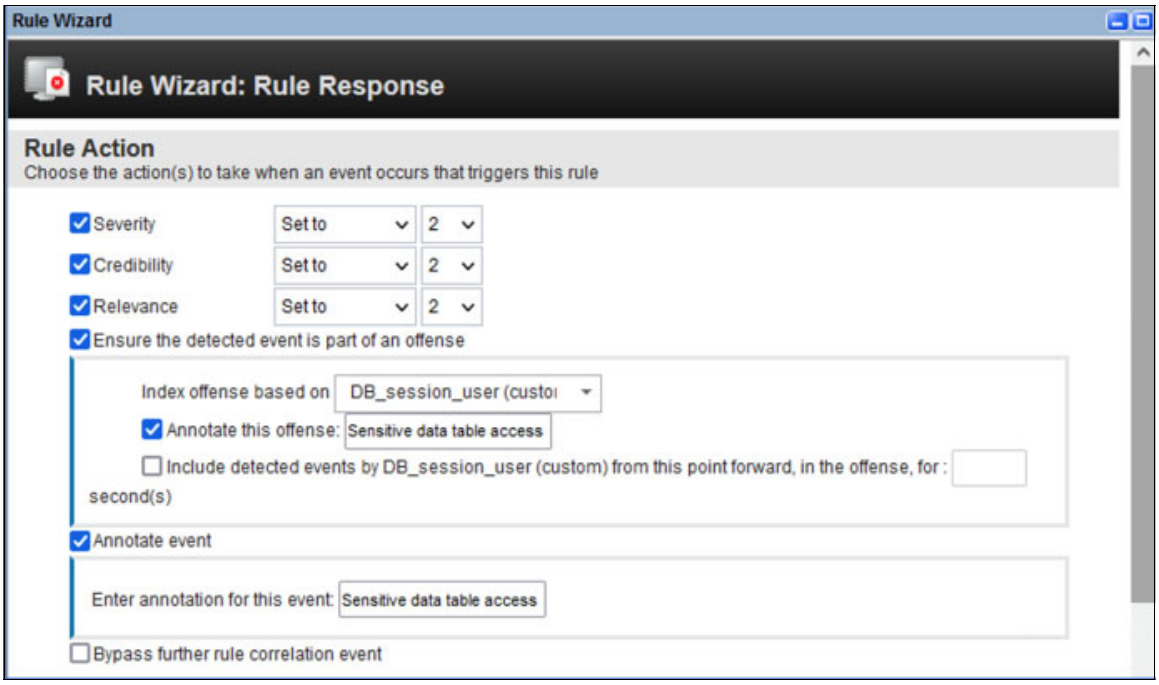


Figure 50 Database rule action

The Rule Response window is shown in Figure 51.

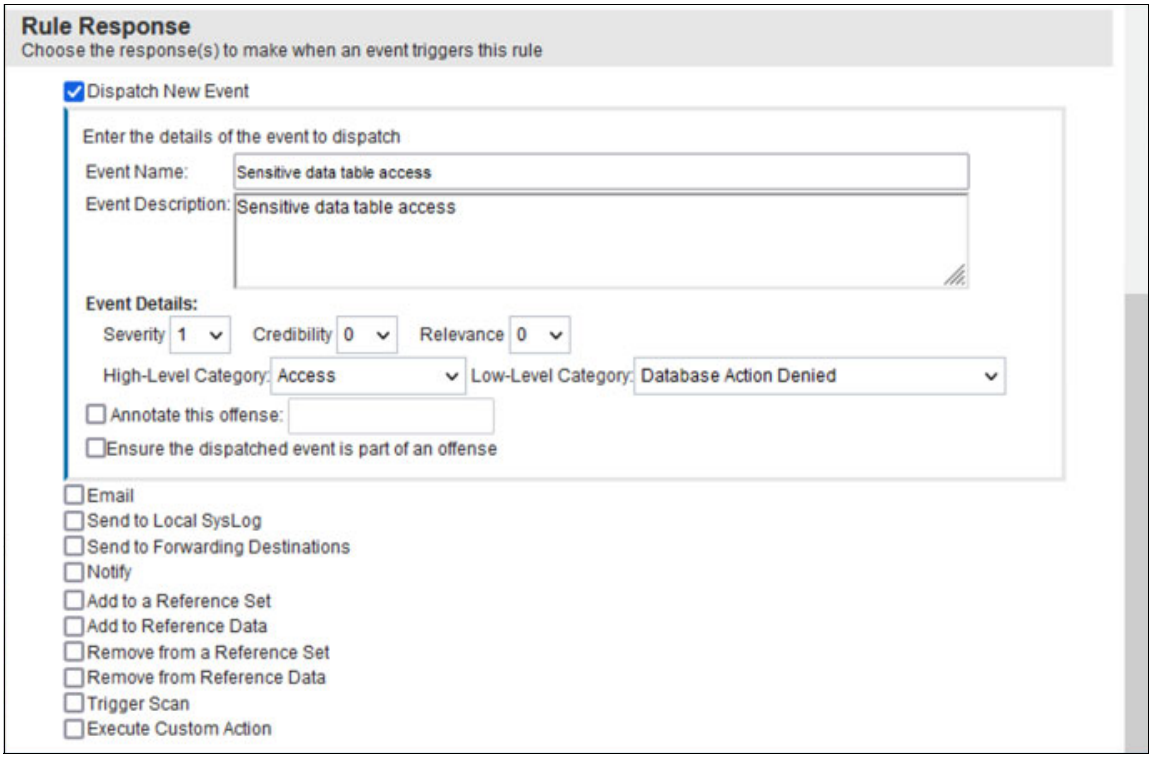


Figure 51 Rule response

The Rule Summary window is shown in Figure 52.

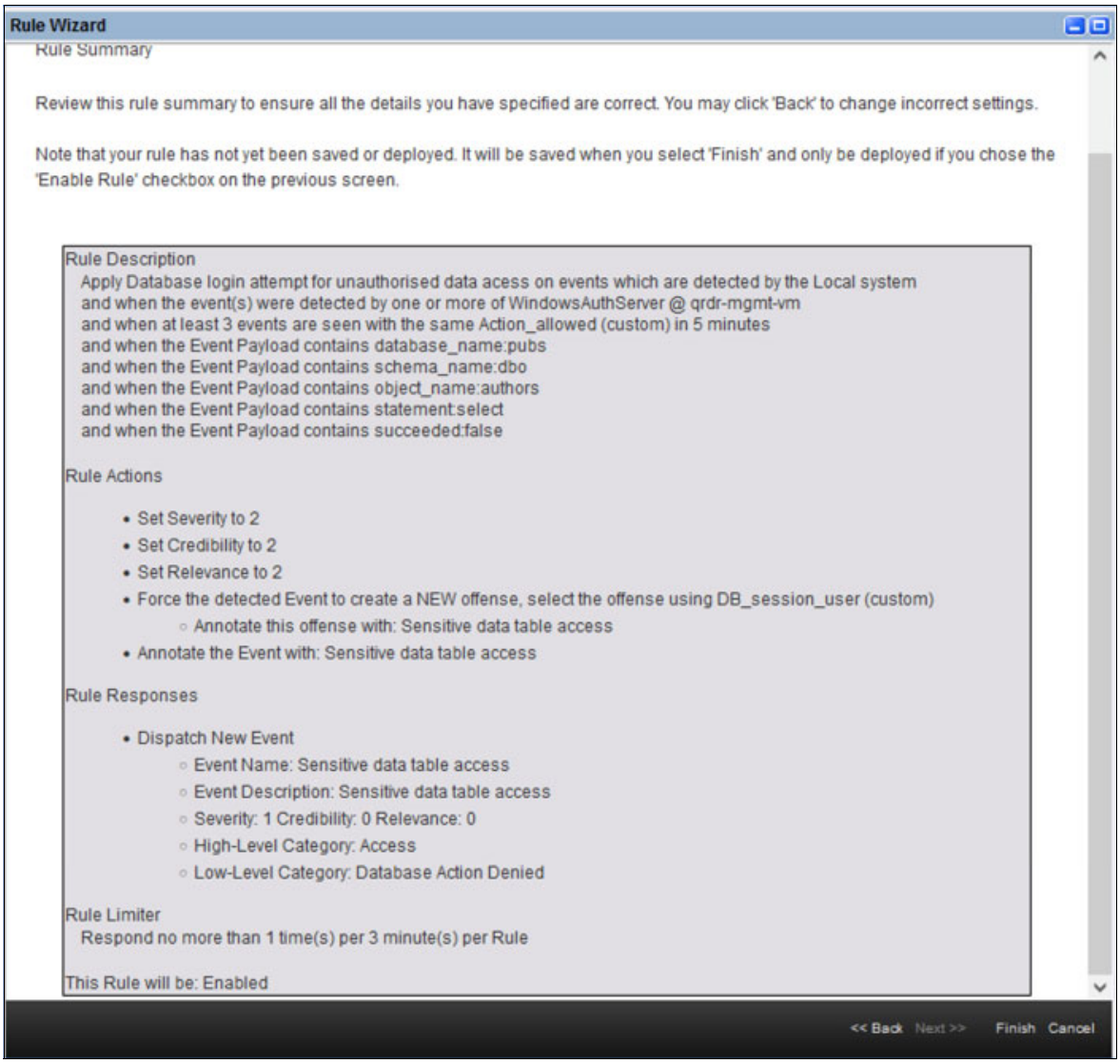


Figure 52 Rule summary, sensitive data table access by a user

Demonstration: Sensitive data table access to generate an offense

This section demonstrates the sensitive data table access scenario. Figure 53 shows the IBM QRadar console log activity and SQL server management studio.

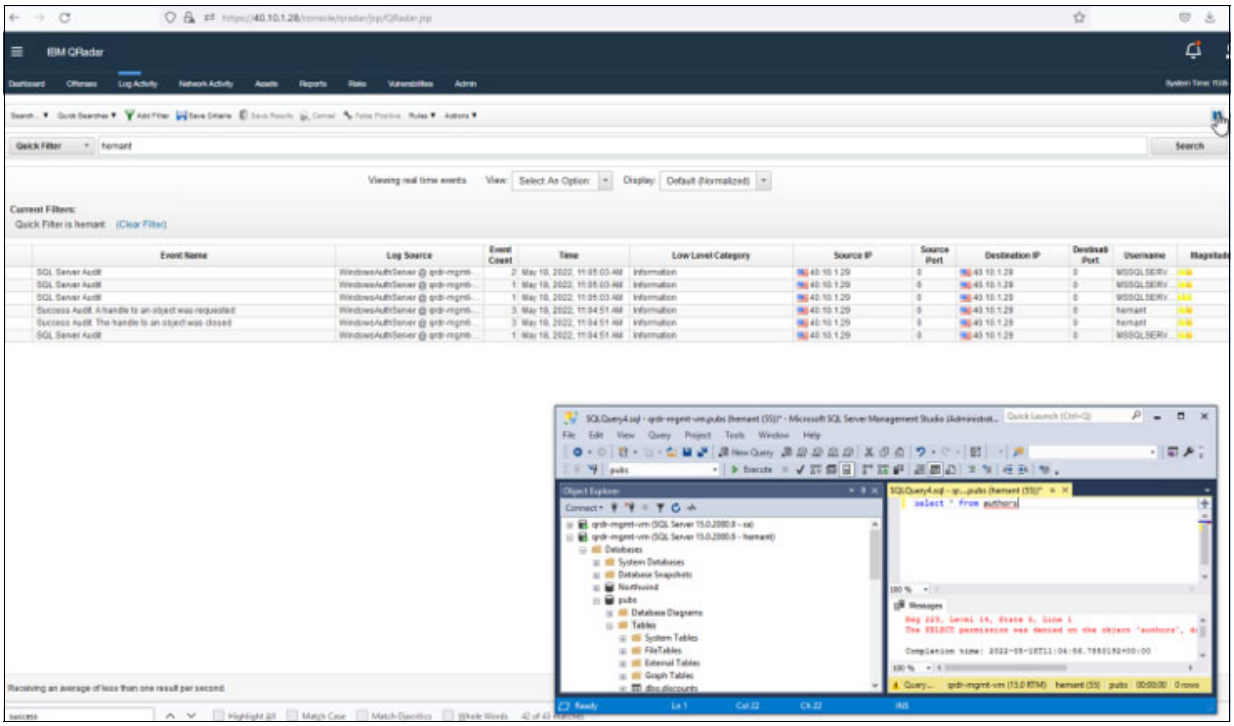


Figure 53 IBM QRadar events for sensitive data table access

In this scenario, the user attempts to access the tables by using the select query on the database table, with no access rights.

The IBM QRadar console window shows the detected SQL audit log events when the select query was run on the database table to which the user does not have access (see Figure 53).

The IBM QRadar event payload and rule that is defined for the event is displayed (see Figure 54).

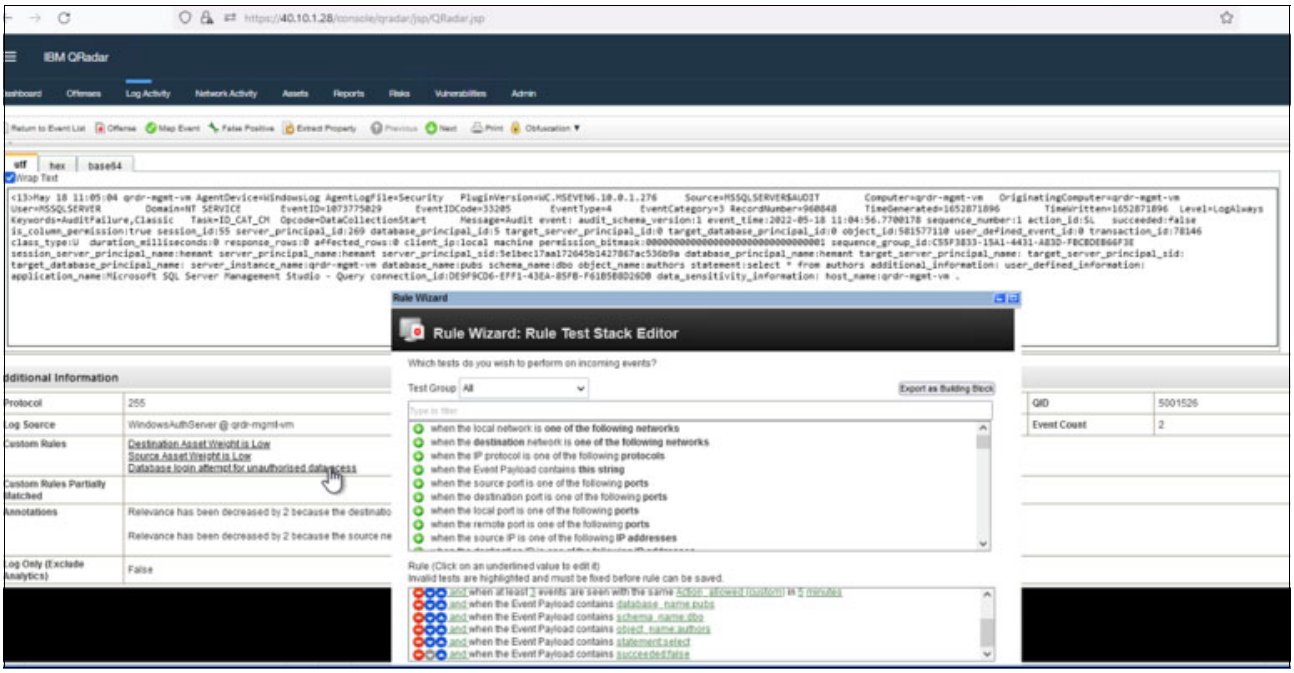


Figure 54 IBM QRadar event payload and rule that is triggered for the sensitive database event

An offense is generated for sensitive data table access (see Figure 55).

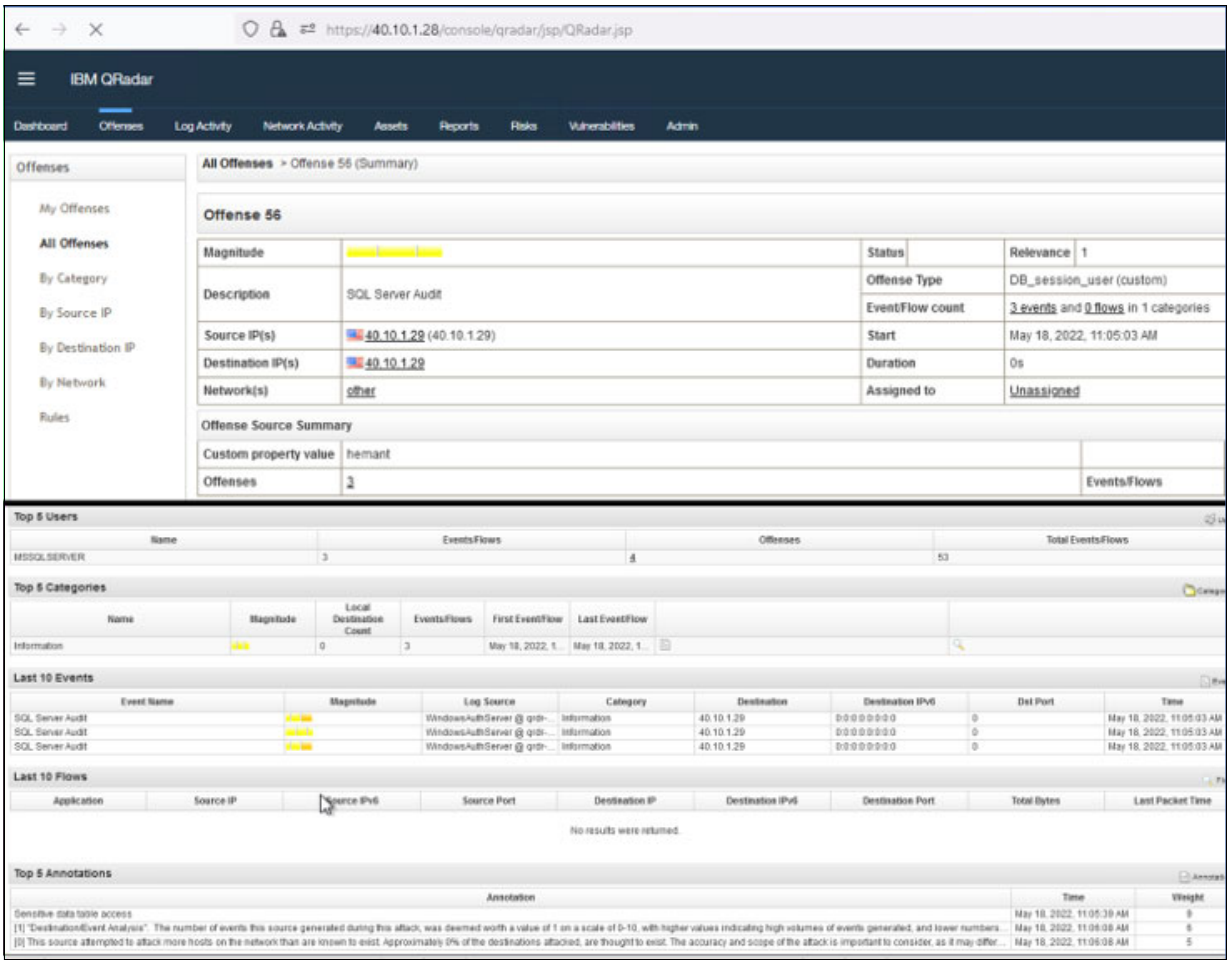


Figure 55 Offense generated for sensitive data table access

Summary

The solution that described in this Blueprint shows the integration of IBM QRadar for early threat detection for IBM SV4PC storage and a database that is running on a host.

After a threat is detected, IBM QRadar's cyber-resiliency workflow is triggered. The workflow is used to run a defined scheduled task in IBM Copy Services Manager. This task performs the required actions, including IBM SV4PC Safeguarded Copy, to create an immutable copy of the data.

The solution can be used as template to categorize the events that are received from the IBM SV4PC storage system and database host. Based on the events that are received, threat detection rules can be defined that conform with security standards that defined by the organization's compliance matrix.

Finally, the sample Python script shows how to use the API interface of IBM Copy Services Manager to perform a specific task.

Authors

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

Shashank Shingornikaris 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 to build 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 HA/DR/Cluster/Replication solutions for database technologies, such as Oracle, MSSQL, and MySQL.

Hemant Kantak is a Storage Solutions Architect with IBM Systems, ISDL Lab Pune, India, for the past 11 years in IBM. He designs and deploys storage and backup, virtualization, and cloud technology solutions across various platforms, including AWS, IBM Cloud®, and Microsoft Azure. He also enables hybrid cloud solutions, with Red Hat OpenShift Container Platform, IBM Cloud Paks, and VMware Solutions/Tanzu. As an IBM Systems TechU speaker, he demonstrates solutions to IBM clients and sales teams, and writes various Blueprints and IBM Redbooks® publications.

Thanks to **Michelle Tidwell**, IBM Storage, Program Director, IBM Spectrum Virtualize, Hybrid Cloud Product Management, for their contributions to this project.

Resources

For more information, see the following resources:

- Cyber Resiliency Solution using IBM Spectrum Virtualize:

  http://www.redbooks.ibm.com/abstracts/redp5657.html
- IBM FlashSystem Safeguarded Copy Implementation Guide:

  http://www.redbooks.ibm.com/abstracts/redp5654.html
- IBM QRadar:

  http://www.ibm.com/docs/en/qsip
- IBM Copy Services Manager:

  http://www.ibm.com/docs/en/csm
- IBM Copy Services Manager User's Guide:

  http://www.ibm.com/support/pages/system/files/inline-files/sc27854220.pdf
- Scheduled Tasks in Copy Services Manager:

  http://www.ibm.com/docs/en/csm/6.3.1?topic=replication-creating-scheduled-tasks
- Securing Data on Threat Detection by Using IBM Spectrum Scale and IBM QRadar: An Enhanced Cyber Resiliency Solution:

  http://www.redbooks.ibm.com/abstracts/redp5560.html?Open
- GitHub link to download the script:

  http://www.github.ibm.com/IBM/cyber-resiliency-solutions/ibm-qradar-ds8k-sgc-with-csm
- IBM WinCollect agent for QRadar:

  https://www.ibm.com/community/qradar/home/wincollect/

Notices

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

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

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

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

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

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

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

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

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

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

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

COPYRIGHT LICENSE:

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

Trademarks

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

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

AIX®
FICON®
FlashCopy®
IBM®
IBM Cloud®
IBM FlashSystem®
IBM Security™
IBM Spectrum®
IBM Z®
QRadar®
Redbooks®
Redbooks (logo)  ®
z/OS®

The following terms are trademarks of other companies:

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

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

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

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.

July 2022

Please recycle

ISBN 0738460621

REDP-5685-00