

Securing Data on Threat Detection by Using IBM Spectrum Scale and IBM QRadar

An Enhanced Cyber Resiliency Solution

Boudhayan Chakrabarty

Sandeep R Patil

Shashank Shingornikar

Ashish Kothekar

Praphullachandra Mujumdar

Smita Raut

Digvijay Ukirde



 **Security**

Storage

In partnership with
IBM Academy of Technology



Securing Data on Threat Detection by Using IBM Spectrum Scale and IBM QRadar

Having appropriate storage for hosting business-critical data and advanced Security Information and Event Management (SIEM) software for deep inspection, detection, and prioritization of threats has become a necessity for any business. This IBM® Redpaper publication explains how the storage features of IBM Spectrum® Scale, when combined with the log analysis, deep inspection, and detection of threats that are provided by IBM QRadar®, help reduce the impact of incidents on business data. Such integration provides an excellent platform for hosting unstructured business data that is subject to regulatory compliance requirements.

This paper describes how IBM Spectrum Scale File Audit Logging can be integrated with IBM QRadar. Using IBM QRadar, an administrator can monitor, inspect, detect, and derive insights for identifying potential threats to the data that is stored on IBM Spectrum Scale. When the threats are identified, you can quickly act on them to mitigate or reduce the impact of incidents. We further demonstrate how the threat detection by IBM QRadar can proactively trigger data snapshots or cyber resiliency workflow in IBM Spectrum Scale to protect the data during threat.

This third edition has added “Ransomware threat detection” on page 42 where we discuss a Ransomware attack scenario within an environment to leverage IBM Spectrum Scale File Audit logs integration with IBM QRadar.

This paper is intended for chief technology officers, solution engineers, security architects, and systems administrators.

Note: This paper assumes a basic understanding of IBM Spectrum Scale and IBM QRadar and their administration.

Introduction to IBM Spectrum Scale

IBM Spectrum Scale is a proven, scalable, high-performance file system that is suitable for various use cases. It provides world-class storage management with extreme scalability, flash accelerated performance, and automatic storage tiering capabilities. IBM Spectrum Scale reduces storage costs while improving security and management efficiency in cloud, big data, and analytics environments. IBM Spectrum Scale provides the following benefits:

- ▶ Virtually limitless scaling to nine quintillion files with yottabytes of data.
- ▶ High performance and simultaneous access to a common set of shared data.
- ▶ Integrated information lifecycle management (ILM) functions to automatically move data between storage tiers that include flash, disk, tape, and object storage (in public and private cloud environments). This function can dramatically reduce operational costs because fewer administrators can manage larger storage infrastructures.
- ▶ Software-defined storage that you use to build your infrastructure solution with the following characteristics:
 - Easy to scale with relatively inexpensive commodity hardware while maintaining world-class storage management capabilities.
 - Deployable on IBM Cloud® and Amazon Web Services (AWS) cloud platforms.
 - A cross-platform solution is available on IBM AIX®, Linux, and Windows server nodes, or a mix of all three. IBM Spectrum Scale is also available for IBM Z®.
- ▶ Available as the IBM Elastic Storage® Server (IBM ESS) pre-packaged storage solution with declustered RAID included.
- ▶ Global data access across geographic distances and unreliable WAN connections.
- ▶ Multi-site support by connecting a local IBM Spectrum Scale cluster to remote clusters to provide greater administrative flexibility and control.
- ▶ Proven reliability across multiple sites, with support for concurrent hardware and software upgrades.
- ▶ State-of-the-art protocol access methods for managing files and objects under the same global namespace, which makes more efficient use of storage space and avoids data islands. The supported protocols include NFS, SMB, POSIX, OpenStack Swift, and Amazon Simple Storage Service (S3).
- ▶ Seamless integration for Hadoop applications by using the Hadoop Distributed File System (HDFS) Transparency feature.
- ▶ Proven security features to ensure data privacy, authenticity, and auditability.
- ▶ File-level encryption for data at rest and secure erase.
- ▶ Policy-driven compression to reduce the size of data at rest and increase storage efficiency.
- ▶ Can be used as persistent storage for containers via Kubernetes CSI interface.
- ▶ Includes GUI to simplify storage administration tasks and monitor many aspects of the system.
- ▶ Includes container native flavor called IBM Spectrum Scale Container Native Storage Access (CNSA).

Figure 1 shows an overview of IBM Spectrum Scale.

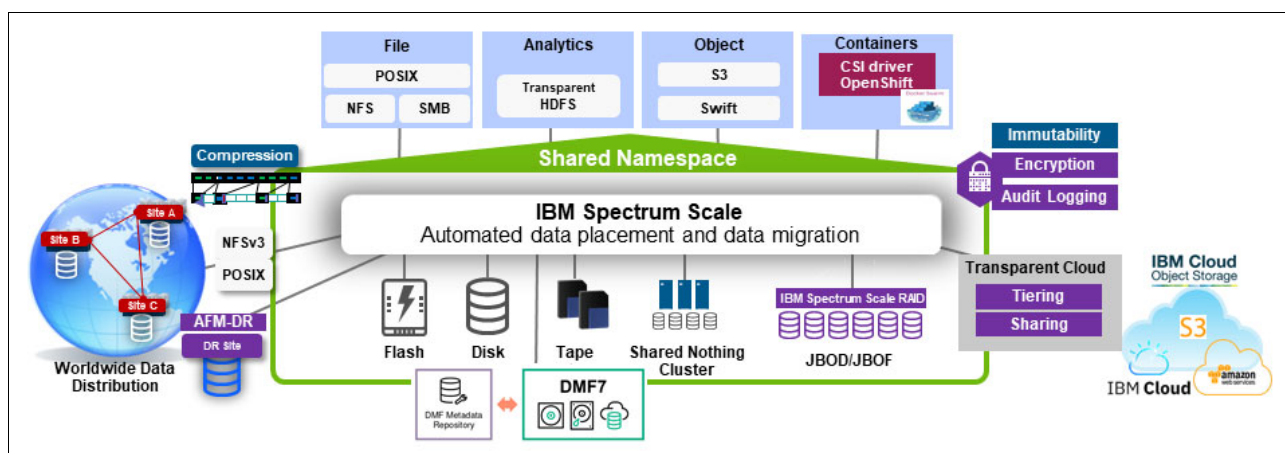


Figure 1 IBM Spectrum Scale overview

IBM Spectrum Scale is especially used in high-performance and computationally demanding environments across different branches, including banking, financial, healthcare, oil and gas, and automotive industries.

Note: IBM Spectrum Scale is available as a no-cost try and buy trial version that runs in a virtual environment. The trial version includes a fully preconfigured IBM Spectrum Scale instance in a virtual machine (VM), based on IBM Spectrum Scale V5.0. It can be downloaded from [IBM Spectrum Scale - Overview](#).

Introduction to IBM QRadar

In cybersecurity, SIEM is considered a series of technologies in charge of providing analysis, threat mitigation, and logging of security events across a determined network. SIEM provides a general view of all technical infrastructure, with specific data of security events, and the mitigation of any security threat vectors that are found in the environment.

SIEM includes several functions, such as Security Information Management (SIM) and Security Event Management (SEM), combined into a single solution. To better understand SIEM, think of a solution that gathers data from security sources for analyzing, correlating, and acting upon possible threats.

SIEM management offers various functions in the following areas:

- ▶ Event and log collection
- ▶ Rule correlation
- ▶ Log source management
- ▶ Adaptability
- ▶ Data normalization and registry
- ▶ Reports and Compliance

This solution tries to solve scenarios where people cannot analyze advanced threats by using the normal monitoring tools (on a general level), by using a business technical infrastructure, and by unifying all the elements. These elements are typically agents in a hierarchical model that gather events from endpoints, servers, and network equipment. IBM QRadar® provides third-party interoperability so that many solutions can be integrated, which makes this product scalable and more robust.

IBM QRadar is one of the most popular SIEM solutions in the market today. IBM QRadar helps you quickly uncover existing and potential threats through its advanced analytics capabilities. It provides many features, such as centralized visibility, flexible deployment, automated intelligence, machine learning, pro-active threat hunting, and much more.

Figure 2 gives a high-level overview of IBM QRadar Security Intelligence Platform coverage.

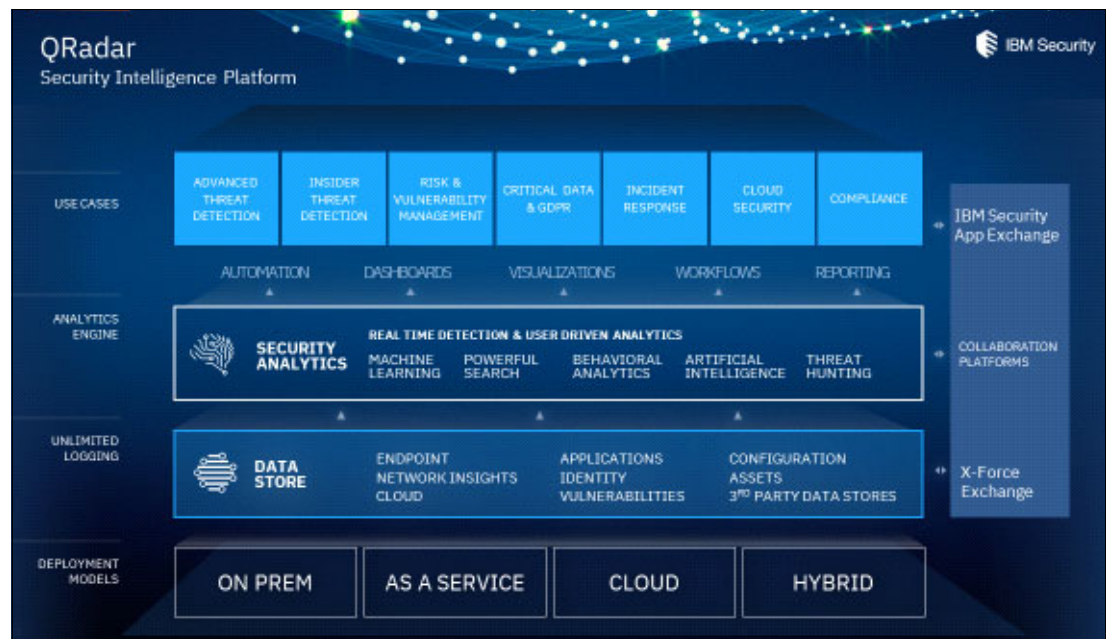


Figure 2 Overview of IBM QRadar Security Intelligence Platform

With thorough functionality, IBM QRadar collects events from different assets that are present in the environment, even picking up raw packets of data from the network for correlation. Furthermore, it provides session rebuilding capabilities for forensic analysis. IBM QRadar also integrates with IBM Watson® for Cyber Security and multiple other third-party security feeds, which helps you orchestrate responses to unknown threat vectors.

Figure 3 on page 5 shows how IBM QRadar compiles data from extensive data sources and then applies correlation and deep inspection to derive exceptionally accurate and actionable insights.

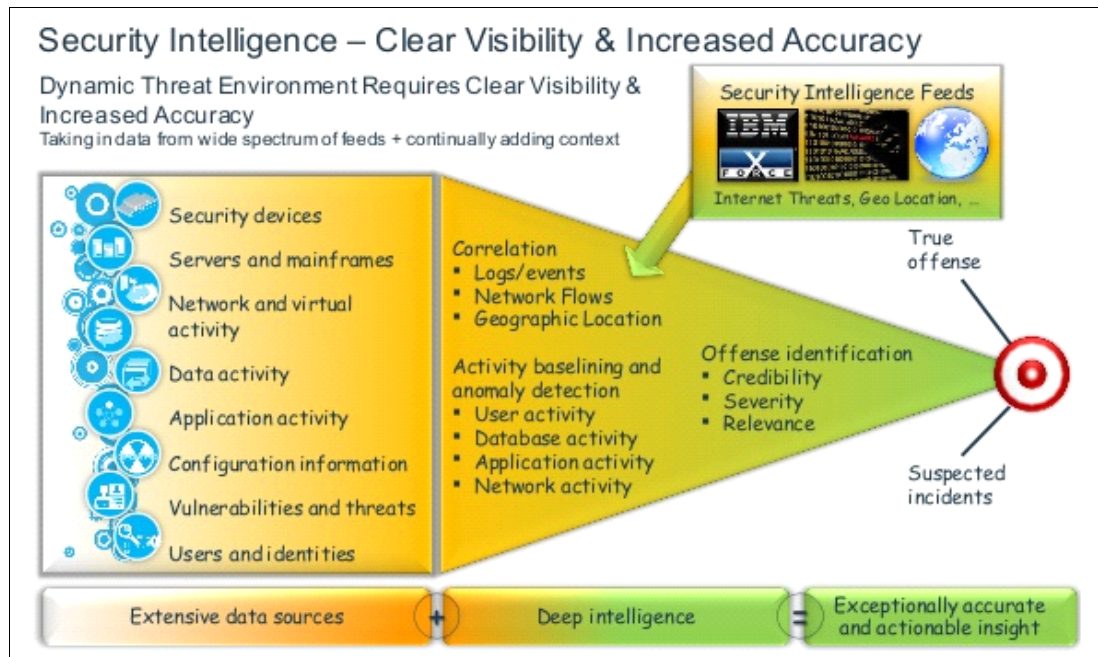


Figure 3 IBM QRadar Security Intelligence approach

For more information about IBM QRadar, see “References” on page 60.

IBM QRadar with IBM Spectrum Scale: Identifying threats to data and acting on potential incidents

Data is the “new oil”, and protection of data against cyberthreats is one of the key challenges that many organizations are facing. In a data-centric security paradigm, protection of actual data is of paramount importance, so you need security capabilities on underlying storage systems, such as secure data at rest, secure data in motion, role-based access control for administration, access control lists (ACLs), and antivirus support to ensure that the data is constantly secured and protected against malicious users.

IBM Spectrum Scale is a state-of-the-art, highly scalable file solution with security features that ensure the required protection for your data. One such capability is IBM Spectrum Scale File Audit Logging that, when enabled, logs all of the file access to the file system with the required audit information.

To identify and detect potential malicious data access, and for compliance auditing purposes, you must have such file audit logs integrated with the SIEM solution. This capability is provided by IBM QRadar, to which the IBM Spectrum Scale file access logs can be securely directed. In addition, IBM QRadar can detect malicious patterns based on the following information:

- ▶ Access logs
- ▶ Heuristics
- ▶ Correlation with logs from other systems (such as network logs or server logs)
- ▶ Flow and packet data
- ▶ Unknown threat vector detection by using IBM Watson

The subsequent sections demonstrate the integration of IBM QRadar and IBM Spectrum Scale, which is set up in the following manner:

- ▶ Unstructured data is in an IBM Spectrum Scale file system.
- ▶ IBM Spectrum Scale File Audit Logging is enabled for the file system hosting the data.
- ▶ The IBM Spectrum Scale server is configured to relay the file audit log message to IBM QRadar.
- ▶ IBM QRadar is configured in the same network to receive logs on the `rsyslog` port.
- ▶ IBM QRadar is configured with the required file parsing rules to interpret the semantics of IBM Spectrum Scale file audit logs.
- ▶ IBM QRadar is configured with sample rules (as manifestation) to identify potential threats (based on analyzing IBM Spectrum Scale file audit logs) and generate insights and alerts for the system administrator to act on.

Note: The purpose of this demonstration is to show IBM QRadar integration, and the value that it can deliver to secure the data that is hosted on IBM Spectrum Scale by using the IBM Spectrum Scale File Audit Logging feature. Actual deployments can use this demonstration as a sample illustration to configure and design solutions for cybersecurity of their data that is hosted over IBM Spectrum Scale according to their business needs.

In addition, the solution can be extended to include IBM Spectrum Scale administration command logging, which requires further customization that is not covered in this paper.

Environment

As shown in Figure 4 on page 7, an IBM Spectrum Scale cluster is configured with a file system hosting business data that is accessed by the users (in this example, through the IBM Spectrum Scale POSIX interface). IBM QRadar is installed on a separate, dedicated system that is configured to accept log messages by using the `rsyslog` protocol.

IBM Spectrum Scale is configured and enabled for file audit logging for the file system, which generates file access audit logs that are stored on a dedicated and immutable IBM Spectrum Scale file set. A dedicated IBM Spectrum Scale client node, which is a part of the IBM Spectrum Scale network, is configured to forward the IBM Spectrum Scale file audit logs to IBM QRadar.

IBM QRadar is configured with parsing logic to interpret the log format, parse the logs, and persistently store the logs. When the logs are in IBM QRadar, the security officer or administrator can set various rules, map log relationships, and so on to detect potential malicious data access. As sample manifestations, we set IBM QRadar rules on a user file access pattern, and generate incidents if that pattern violates business policies.

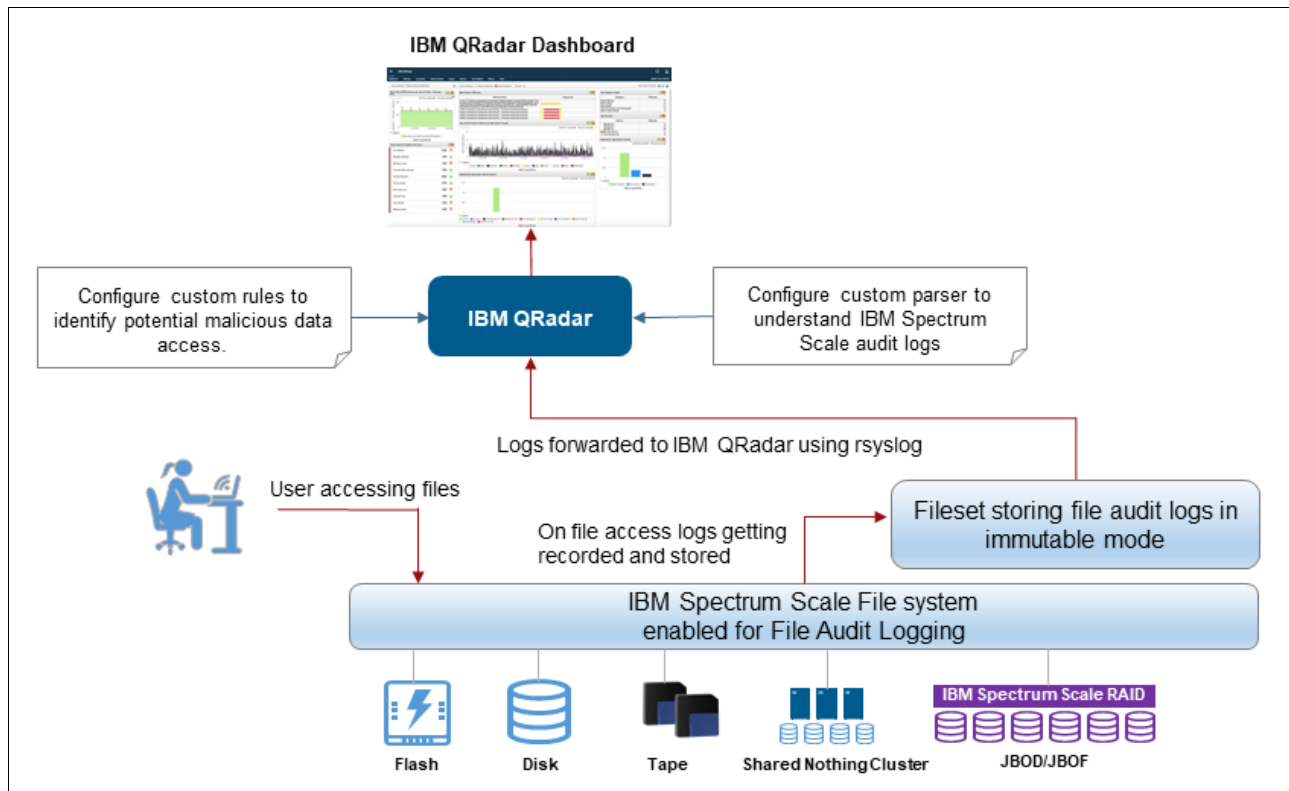


Figure 4 High-level setup: IBM Spectrum Scale and IBM QRadar for storing and analyzing file audit logs

Setup

The IBM Spectrum Scale V5.0.3 cluster that is used for this demonstration was configured on three nodes running Red Hat Enterprise Linux 7.5. The IBM Spectrum Scale file system is mounted on `/gpfs/fs1`, with the file audit logs on `/gpfs/fs1/fa1`. The IBM QRadar V7.3.2 appliance is installed in the same network. The VM3 node is configured with `rsyslog` to forward the logs to IBM QRadar.

Figure 5 shows the test setup that is used for this demonstration.

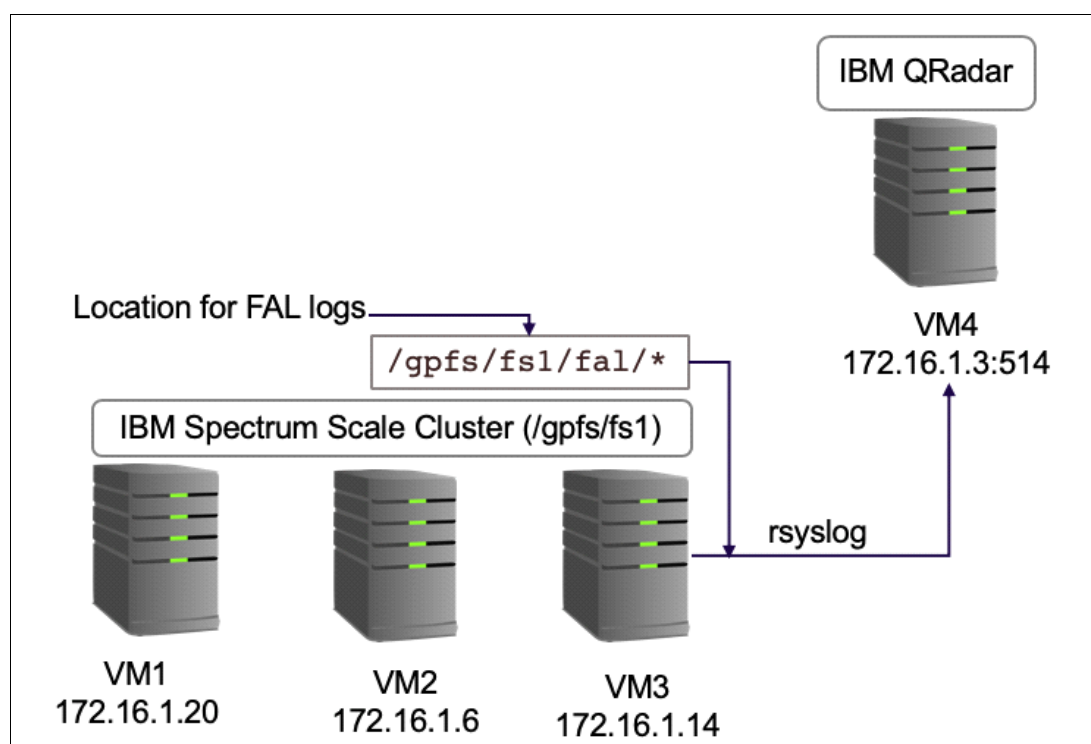


Figure 5 Test setup: IBM Spectrum Scale integrated with IBM QRadar

IBM Spectrum Scale cluster configuration

In this example, we installed and configured a three-node IBM Spectrum Scale cluster. Example 1 shows the details of the cluster.

Example 1 IBM Spectrum Scale cluster details

```
root@host-172-16-1-20 ~]# mmlscluster
```

GPFS cluster information

=====

```
GPFS cluster name:      cluster1.spectrum
GPFS cluster id:        9364683939971205925
GPFS UID domain:        cluster1.spectrum
Remote shell command:   /usr/bin/ssh
Remote file copy command: /usr/bin/scp
Repository type:        CCR
```

Node	Daemon node name	IP address	Admin node name	Designation
1	vm-1	172.16.1.20	vm-1	quorum
2	vm-2	172.16.1.6	vm-2	quorum-manager
3	vm-3	172.16.1.14	vm-3	quorum-manager

```
[root@host-172-16-1-20 ~]# mmlsfs fs1 -T --file-audit-log
```

flag	value	description
--file-audit-log	No	File Audit Logging enabled?
-T	/gpfs/fs1	Default mount point

Configuring IBM Spectrum Scale File Audit Logging

To configure IBM Spectrum Scale File Audit Logging, complete the following steps:

1. Ensure that File Audit Logging is installed on the cluster either by using the **install** toolkit or manually by installing packages. The demonstration setup uses Red Hat Enterprise Linux nodes, and the following packages were installed:

- gpfs.kafka-5.0*.rpm
- gpfs.librdkafka-5.0*.rpm

2. Enable the message queue (required by the IBM Spectrum Scale File Audit Logging feature) on all three nodes by using the **mmmsgqueue** command:

```
[root@host-172-16-1-20 ~]# mmmsgqueue enable -N vm-1,vm-2,vm-3
```

Example 2 shows the status of the nodes.

Example 2 Node status

[root@host-172-16-1-20 ~]# mmmsgqueue status -N vm-1,vm-2,vm-3				
Node	Contains	Broker	Contains	
Zookeeper				
Name	Broker	Status	Zookeeper	Status
vm-1	yes	good	yes	good
vm-2	yes	good	yes	good
vm-3	yes	good	yes	good

3. Enable File Audit Logging by using the **mmaudit** command for a file system (fs1 in our example). Also, specify the file set where the audit logs are directed (fal in our example), as shown in Example 3.

Example 3 Enabling File Audit Logging

[root@host-172-16-1-20 ~]# mmaudit fs1 enable --log-fileset fal				
File audit logging status can be viewed as:				
[root@host-172-16-1-20 ~]# mmaudit all list				
Audit	Cluster	Fileset	Fileset	Retention
Device	ID	Device	Name	(Days)
fs1	9364683939971205925	fs1	fal	365

The previous steps ensure that all File Audit Logging events are logged under the fal file set. The contents of this file set and the layout of directory structure are explained in the following section. It is vital to understand this layout because it helps to define the Regular Expressions (regex) rules in the rsyslog configuration that are required to forward the logs to IBM QRadar.

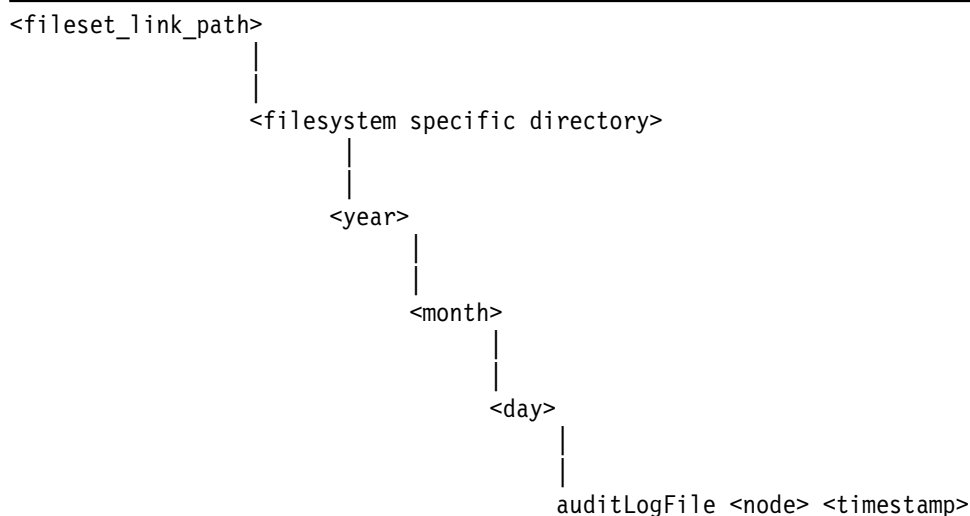
Note: From IBM Spectrum Scale 5.1.0 onwards, the need for Kafka configuration is not required. Refer to IBM Spectrum Scale 5.1 for [Configuring file audit logging](#).

Understanding File Audit Logging: Log file layout and log entries

File Audit Logging creates a directory per file system inside the file set that is assigned for hosting the audit logs. Inside this directory, there are subdirectories that are created for year, and then for month and day.

The overall directory structure looks like Example 4.

Example 4 Directory example that is created by File Audit Logging



In the demonstration setup file, audit logging created the SpectrumScale_150_9364683939971205925_2_FSYS_fs1_audit directory under the fal file set.

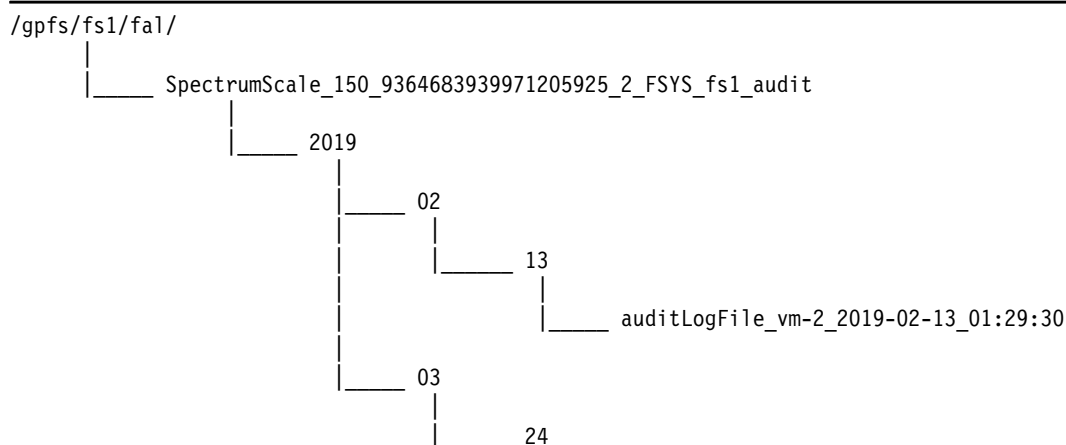
Example 5 shows the directory structure from the demonstration setup.

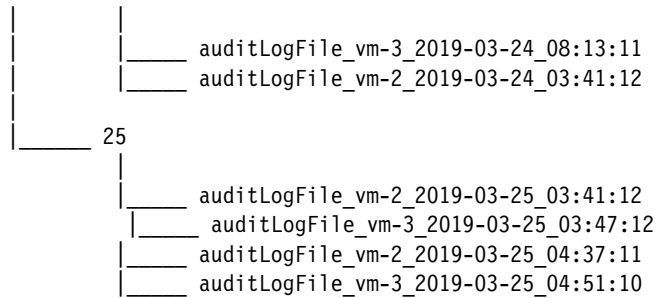
Example 5 Demonstration setup directory

```
[root@host-172-16-1-20 ~]# mmfsfilesset fs1 fal
File sets in file system 'fs1':
Name           Status    Path
fal            Linked   /gpfs/fs1/fal
[root@host-172-16-1-20 ~]#
```

Example 6 shows the directory structure in the file set link path.

Example 6 Directory structure in the file set link path





Audit events are logged in these auditLogFiles in a predefined JSON format. Example 7 shows a sample logged event in JSON format that is generated for each file access.

Example 7 Sample logged event in JSON format that is generated for each file access

```

{ "LWE_JSON": "0.0.1",
  "path": "/gpfs/fs1/anotherdir2/copyfile2452",
  "oldPath": null,
  "clusterName": "cluster1.spectrum",
  "nodeName": "vm-3",
  "nfsClientIp": "",
  "fsName": "fs1",
  "event": "CREATE",
  "inode": "8815",
  "linkCount": "1",
  "openFlags": "0",
  "poolName": "system",
  "fileSize": "0",
  "ownerUserId": "0",
  "ownerGroupId": "0",
  "atime": "2019-03-25_12:42:21+0530",
  "ctime": "2019-03-25_12:42:21+0530",
  "eventTime": "2019-03-25_12:42:21+0530",
  "clientUserId": "0",
  "clientGroupId": "0",
  "processId": "20000",
  "permissions": "200100644",
  "acls": null,
  "xattrs": null,
  "subEvent": "NONE" }
  
```

In Example 7, the following variables are defined:

path	Path of the file on which I/O is performed.
clusterName	Name of the cluster where the event was generated.
nodeName	Node on which the event was generated.
event	Type of event that was generated, for example, CREATE, DESTROY, OPEN, CLOSE, or XATTRCHANGE.
fileSize	Size of the file.
clientUserId	User ID (UID) of the process performing the operation on the file.
clientGroupId	Group ID (GID) of the process performing the operation on the file.

For more information about this format and an explanation of the other fields, see the IBM Spectrum Scale [JSON attributes in file audit logging](#).

Sending File Audit Logging events to IBM QRadar

IBM QRadar supports different mechanisms to direct events and logs towards it, and one of them is `rsyslog`. In this demonstration, we send events from an IBM Spectrum Scale node to IBM QRadar by using `rsyslog` remote forwarding.

The `rsyslog` *must* be configured to send all logs across *all* subdirectories within the auditing file set. To create a rule by using regex, you must upgrade `rsyslog` to Version 8 or later, which supports regex. Red Hat Enterprise Linux 7.5 systems that were used for the setup by default contain `rsyslog` V7.

To upgrade to Version 8, complete the following steps:

1. Choose an IBM Spectrum Scale client node (VM3 in our example) and upgrade to `rsyslog` V8 by using a V8 stable repository, as shown in Example 8.

Example 8 A Version 8 stable repository

```
cd /etc/yum.repos.d
wget http://rpms.adiscon.com/v8-stable/rsyslog.repo
Edit syslog.conf and change the below parameter-
baseurl=http://rpms.adiscon.com/v8-stable/epel-7/$basearch
yum update rsyslog
```

Note: At the time of writing, `rsyslog` V7 did not support a regex-based directory hierarchy, so `rsyslog` V8 was required.

2. After `rsyslog` is upgraded, edit the `/etc/rsyslog.conf` file to contain the statements that are shown in Example 9.

Example 9 Including the statements in this example in file /etc/rsyslog.conf

```
$ModLoad imfile
# Forward all the file audit directories by appropriately setting InputFileName
value
$InputFileName /gpfs/fs1/fal/SpectrumScale_*/**/*/*/*auditLogFile*
# Use InputFileTag to tag all the audit messages being forwarded by rsyslog
$InputFileTag fal
# Set InputFileStateFile with a unique pre-fix that is required by rsyslog
$InputFileStateFile stat-fal
#Set InputFileFacility to local4 which is then forwarded by rsyslog to IBM
QRadar. Set this according to your requirements.
$InputFileFacility local4
# Set InputRunFileMonitor to forward from local facility to IBM QRadar system.
$InputRunFileMonitor
local4.* @@172.16.1.3:514
#QRadar IP = 172.16.1.3
```

For more information about `rsyslog` configuration, see the `rsyslog` man page.

Here are some important notes:

- ▶ The `rsyslog` section that is shown in Example 9 on page 12 must be added for every file system that is configured to be audited. We have only one section because in this demonstration we are auditing only one file system.
- ▶ The `rsyslog` configuration must be done only on one IBM Spectrum Scale node where the IBM Spectrum Scale file system is mounted to avoid sending duplicate entries to IBM QRadar from multiple nodes.
- ▶ If there is a failure of a node where `rsyslog` is configured, the `rsyslog` configuration must be manually done on another node so that another node takes over the task of forwarding events to IBM QRadar. This task can be automated by practitioners per their needs.
- ▶ `Rsyslog` forwards file audit logs only from the time that it is configured and started. Existing file audit logs that might already be present are not forwarded.
- ▶ In the current setup, `rsyslog` is not configured with Transport Layer Security (TLS). You can configure `rsyslog` with TLS for secure data in flight.

Note: There are two methods to forward IBM Spectrum Scale 5.1 (or previous version) File Audit Log using `rsyslog`:

1. Set SELinux to permissive mode on the node the user will use for `rsyslog` forwarding.
2. Disable SELinux on the node the user will use for `rsyslog` forwarding.

For more updated information on forwarding semantics and rules using `rsyslog` refer to the latest [rsyslog documentation](#).

Configuring IBM QRadar for IBM Spectrum Scale file audit log events

When IBM Spectrum Scale is configured to send the events to IBM QRadar, log on to the IBM QRadar system. You already installed and configured an IBM QRadar software appliance running on VM4, as shown in Figure 5 on page 8. In the IBM QRadar GUI, from the **Log Activity** tab, filter the events based on the IP address of the IBM Spectrum Scale log source. You see the events with status “Unknown/Unparsed”, as shown in Figure 6.

Current Filters:						
Source IP is 172.16.1.3 (Clear Filter)						
	Event Name	Log Source	Event Count	Time	Low Level Category	Source IP
	Unknown log event	SIM Generic Log D...	1	Jun 3, 2019, 2:19:25 PM	Unknown Generic L...	172.16.1.3
	Unknown log event	SIM Generic Log D...	1	Jun 3, 2019, 2:19:25 PM	Unknown Generic L...	172.16.1.3
	Unknown log event	SIM Generic Log D...	1	Jun 3, 2019, 2:19:25 PM	Unknown Generic L...	172.16.1.3
	Unknown log event	SIM Generic Log D...	1	Jun 3, 2019, 2:19:25 PM	Unknown Generic L...	172.16.1.3
	Unknown log event	SIM Generic Log D...	1	Jun 3, 2019, 2:19:25 PM	Unknown Generic L...	172.16.1.3
	Unknown log event	SIM Generic Log D...	1	Jun 3, 2019, 2:19:25 PM	Unknown Generic L...	172.16.1.3
	Unknown log event	SIM Generic Log D...	1	Jun 3, 2019, 2:19:25 PM	Unknown Generic L...	172.16.1.3
	Unknown log event	SIM Generic Log D...	1	Jun 3, 2019, 2:19:25 PM	Unknown Generic L...	172.16.1.3
	Unknown log event	SIM Generic Log D...	1	Jun 3, 2019, 2:19:25 PM	Unknown Generic L...	172.16.1.3
	Unknown log event	SIM Generic Log D...	1	Jun 3, 2019, 2:19:25 PM	Unknown Generic L...	172.16.1.3
	Unknown log event	SIM Generic Log D...	1	Jun 3, 2019, 2:19:25 PM	Unknown Generic L...	172.16.1.3

Figure 6 IBM QRadar log activity to filter events on IP address

The payloads of the events being relayed by IBM Spectrum Scale to IBM QRadar look similar to the ones that are shown in the following examples.

Example 10 shows the event payload 1 sample.

Example 10 Event payload 1 sample

```
<166>Jun 10 10:15:43 scalegui fal {"LWE_JSON": "0.0.1", "path": "/ibm/fs1/demodata/dir9/file7", "oldPath": null,
"clusterName": "srCluster.kub-1", "nodeName": "scalegui", "nfsClientIp": "", "fsName": "fs1", "event": "OPEN", "inode":
"46446", "linkCount": "1", "openFlags": "0", "poolName": "system", "fileSize": "0", "ownerUserId": "27", "ownerGroupId":
"0", "atime": "2019-06-10_10:15:39+0530", "ctime": "2019-06-10_10:15:39+0530", "eventTime": "2019-06-10_10:15:39+0530",
"clientUserId": "0", "clientGroupId": "0", "processId": "19543", "permissions": "200100644", "acls": null, "xattrs":
null, "subEvent": "NONE" }
```

Example 11 shows the event payload 2 sample.

Example 11 Event payload 2 sample

```
<166>Jun 10 10:15:43 scalegui fal {"LWE_JSON": "0.0.1", "path": "/ibm/fs1/demodata/dir9/file7", "oldPath": null,
"clusterName": "srCluster.kub-1", "nodeName": "scalegui", "nfsClientIp": "", "fsName": "fs1", "event": "ACLCHANGE",
"inode": "46446", "linkCount": "1", "openFlags": "0", "poolName": "system", "fileSize": "0", "ownerUserId": "27",
"ownerGroupId": "0", "atime": "2019-06-10_10:15:39+0530", "ctime": "2019-06-10_10:15:39+0530", "eventTime":
"2019-06-10_10:15:39+0530", "clientUserId": "0", "clientGroupId": "0", "processId": "19543", "permissions": "200100755",
"acls": null, "xattrs": null, "subEvent": "NONE" }
```

Example 12 shows the event payload 3 sample.

Example 12 Event payload 3 sample

```
<166>Jun 10 10:15:43 scalegui fal {"LWE_JSON": "0.0.1", "path": "/ibm/fs1/demodata/dir8/file_2", "oldPath":
"/ibm/fs1/demodata/dir8/file2", "clusterName": "srCluster.kub-1", "nodeName": "scalegui", "nfsClientIp": "", "fsName":
"fs1", "event": "RENAME", "inode": "92226", "linkCount": "1", "openFlags": "0", "poolName": "system", "fileSize": "0",
"ownerUserId": "0", "ownerGroupId": "0", "atime": "2019-06-10_10:15:38+0530", "ctime": "2019-06-10_10:15:38+0530",
"eventTime": "2019-06-10_10:15:38+0530", "clientUserId": "0", "clientGroupId": "0", "processId": "19511", "permissions":
"200100644", "acls": null, "xattrs": null, "subEvent": "NONE" }
```

The next action is to create the parsing logic or DSM for this log source. This task can be done by using the DSM Editor. For more information about the DSM Editor, see “References” on page 60.

1. From the **Log Activity** tab, select **Actions** → **DSM Editor**. To use the DSM Editor, you must first select a few “Unknown log event” items from the log activity tab, as shown in Figure 7.

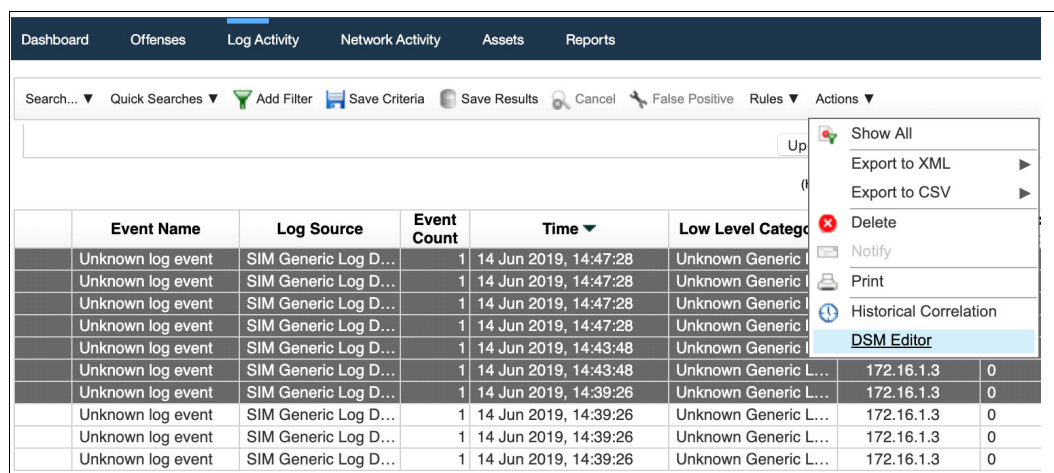


Figure 7 IBM QRadar DSM editor for creating parsing logic

After opening DSM Editor, you must create the Log Source Type.

2. Click **Create New**, as shown in Figure 8.

Select Log Source Type
Choose an existing Log Source Type to modify, or create a new Log Source Type

Filter

- 3Com 8800 Series Switch
- AhnLab Policy Center APC
- Akamai KONA
- Amazon AWS CloudTrail
- Ambiron TrustWave ipAngel Intrusion Prevention System (IPS)

Create New Select Cancel

Figure 8 IBM QRadar DSM Editor: Creating a Log Source Type

3. Enter the Log Source Type Name “Spectrum_LogSource” and click **Save**, which creates a new Log Source Type.
4. Next, from the list of Log Source Types, select the newly created Log Source Type “Spectrum_LogSource”, as shown in Figure 9.

Select Log Source Type
Choose an existing Log Source Type to modify, or create a new Log Source Type

Spec

- Spectrum_LogSource
- Trend Micro Deep Discovery Email Inspector
- Trend Micro Deep Discovery Inspector

Figure 9 IBM QRadar DSM Editor: Selecting the newly created Log Source Type

The following attributes from IBM Spectrum Scale events are considered for parsing in this document:

- ▶ event
- ▶ Log Source Time
- ▶ clientId
- ▶ clientGroupId
- ▶ clusterName

- ▶ nodeName
- ▶ openFlags
- ▶ path

Of course, more attributes can also be parsed, depending on the security administrator's needs. For all of the previous attributes, you must create a custom property for each identified attribute. Without modification, IBM QRadar provides a list of default properties that are used to extract data from events or flow payloads, such as Source IP, Destination IP, and Ports.

Some event sources (IBM Spectrum Scale file audit logs in this context) send unique information that is not normalized. You must create Custom Extract Properties (CEPs) of such information from the event payload post, which you can then use in your Rules, Searches, Reports, and so on.

Here are the CEPs that you extract from the payload of the events:

- ▶ event = Event ID
- ▶ Log Source Time = Log Source Time
- ▶ clientId = Spectrum_clientUserId
- ▶ clientGroupId = Spectrum_GroupId
- ▶ clusterName = Spectrum_clusterName
- ▶ nodeName = Spectrum_NodeName
- ▶ openFlags = Spectrum_openFlags
- ▶ path = Spectrum_Path

Note: The default properties Event ID and Log Source Time can be used, but for all other attributes, you must create CEPs.

To add new custom properties, select the **Plus (+)** button from the **Properties** tab under the "Spectrum_LogSource" type, as shown in Figure 10.



Figure 10 IBM QRadar: Adding new customer properties

The following steps demonstrate an example of creating a CEP for the node attribute:

1. Add the name for the new custom property, for example, "Spectrum_nodeName".
2. Select the **Text** Field Type.
3. Add a **Description**.
4. Make sure to select the **Enable this Property for use in Rules and Search Indexing** check box.
5. Click **Save**, as shown in Figure 11 on page 17.

Create a new Custom Property Definition

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

Name

Field Type

Text

Description
Node name from Spectrum device.

☒ Enable this Property for use in Rules and Search Indexing [?](#)

Save

Go Back

Figure 11 IBM QRadar: Creating a customer property

Follow these same steps to create the CEPs for all of the rest of the attributes.

When done, the next step is to add the Regular Expressions (regex) for these attributes so that they can be parsed. Complete the following steps:

1. From the **Properties** tab, select **Event ID** and add "Regex" to parse the attribute, as shown in Figure 12.

Log Source Type

Spectrum_LogSource

Change

Properties

Event Mappings

Configuration

Filter

+

Event ID
Text | Override

Property Configuration
☒ Override system behavior

Expressions (1)

+

Expression

Expression Type

Regex

Expression

"event": "(.*)"

Format String

\$1

Edit

Figure 12 IBM QRadar: Creating regex for event CEP

Note that the following regex are samples, and you can create better optimized regex for these properties.

2. Set the regex as shown in Figure 12 on page 17 to Figure 19 on page 21:
 - a. The event = eventId (Figure 12 on page 17)
 - b. The eventTime = Log Source Time (Figure 13)

Log Source Time
Date | Override

Property Configuration

☒ Override system behavior

Expressions (1) +

Expression	
Expression Type	Regex
Expression	"eventTime": "(.*)"
Format String	\$1
Date Format	yyyy-MM-dd_HH:mm:ss

[Edit](#)

Figure 13 IBM QRadar: Creating regex for Log Source Time CEP

- c. The clientId = Spectrum_clientUserId (Figure 14)

Spectrum_clientUserId
Text | Custom

Property Configuration

Expressions (1) +

Expression	
Expression Type	Regex
Expression	"clientId": "(.*)"
Capture Group	1

[Edit](#)

Figure 14 IBM QRadar: Creating regex for clientId CEP

- d. The clientGroupId = Spectrum_GroupId (Figure 15 on page 19)

Spectrum_GroupId
Text | Custom

Property Configuration

Expressions (1)

Expression	
Expression Type	Regex
Expression	"clientId": "(.*?)"
Capture Group	1

Edit

Figure 15 IBM QRadar: Creating regex for clientId CEP

- e. The clusterName = Spectrum_clusterName (Figure 16)

Spectrum_clusterName
Text | Custom

Property Configuration

Expressions (1)

Expression	
Expression Type	Regex
Expression	"clusterName": "(.*?)"
Capture Group	1

Edit

Figure 16 IBM QRadar: Creating regex for clusterName CEP

- f. The nodeName = Spectrum_NodeName (Figure 17)

The screenshot shows the 'Spectrum_NodeName' configuration page in IBM QRadar. The page has a header with the name 'Spectrum_NodeName' and a sub-header 'Text | Custom'. Below this is a 'Property Configuration' section. Under 'Expressions (1)', there is a green plus icon and a table. The table has a dark header row labeled 'Expression'. The first row of the table has 'Expression Type' set to 'Regex'. The second row has 'Expression' set to '"nodeName": "(.*)"' and 'Capture Group' set to '1'. An 'Edit' button is located at the bottom right of the table.

Expression	
Expression Type	Regex
Expression	"nodeName": "(.)"
Capture Group	1

Figure 17 IBM QRadar: Creating regex for nodeName CEP

- g. The openFlags = Spectrum_openFlags (Figure 18)

The screenshot shows the 'Spectrum_openFlags' configuration page in IBM QRadar. The page has a header with the name 'Spectrum_openFlags' and a sub-header 'Text | Custom'. Below this is a 'Property Configuration' section. Under 'Expressions (1)', there is a green plus icon and a table. The table has a dark header row labeled 'Expression'. The first row of the table has 'Expression Type' set to 'Regex'. The second row has 'Expression' set to '"openFlags": "(.)"' and 'Capture Group' set to '1'. An 'Edit' button is located at the bottom right of the table.

Expression	
Expression Type	Regex
Expression	"openFlags": "(.)"
Capture Group	1

Figure 18 IBM QRadar: Creating regex for openFlags CEP

h. The path = Spectrum_Path (Figure 19)

Spectrum_Path	
Text Custom	
Property Configuration	
Expressions (1) +	
Expression	
Expression Type	Regex
Expression	"path": "(.*)"
Capture Group	1
Edit	

Figure 19 IBM QRadar: Creating regex for path CEP

Important: Do not forget to click **Save** after making these changes.

Now, you map the events and create the IBM QRadar Identifier (QID).

A *QID* is a numeric representation of a specific event. The QID identifies the following items:

- ▶ Event name
- ▶ Event category
- ▶ Event severity
- ▶ Event description

Event categories are used to group incoming events for processing by IBM QRadar. All generated events are aggregated into *high-level* and *low-level* categories. Each high-level category contains low-level categories and an associated severity level. IBM QRadar provides the `qidmap_cli.sh` built-in utility to map the events categories. For more information about this script, see “References” on page 60.

Note: For any new event type, you must add a custom property, a regex, and then map the event category.

Here are the event categories that we concentrate on in this document:

- ▶ RENAME
- ▶ OPEN
- ▶ UNLINK
- ▶ CLOSE
- ▶ XATTRCHANGE

- ▶ CREATE
- ▶ ACLCHANGE
- ▶ RMDIR
- ▶ DESTROY

On the IBM QRadar All In One (AIO) Console in a distributed deployment, run the following commands to create and map the QIDs:

1. Here is the command for the QID mapping for the RENAME event (renaming a file) mapping to the low-level category Successful File Modification:

```
# /opt/qradar/bin/ qidmap_cli.sh -c --qname Rename_File --qdescription "attempt to rename the file" --severity 3 --lowlevelcategoryid 8014
```

2. Here is the command for the QID mapping for the OPEN event (opening file) mapping to the low-level category Successful File Modification:

```
# / opt/qradar/bin/ qidmap_cli.sh -c --qname Open_File --qdescription "attempt to open the file" --severity 3 --lowlevelcategoryid 8014
```

3. Here is the command for the QID mapping for the UNLINK event (moving file) mapping to the low-level category Successful File Modification:

```
# / opt/qradar/bin/ qidmap_cli.sh -c --qname Move_File --qdescription "attempt to move the file" --severity 2 --lowlevelcategoryid 8014
```

4. Here is the command for the QID mapping for the CLOSE event (closing file) mapping to the low-level category Successful File Modification:

```
# / opt/qradar/bin/ qidmap_cli.sh -c --qname Close_File --qdescription "attempt to close the file" --severity 3 --lowlevelcategoryid 8014
```

5. Here is the command for the QID mapping for the XATTRCHANGE event (modifying attributes of file) mapping to the low-level category Successful File Modification:

```
# / opt/qradar/bin/ qidmap_cli.sh -c --qname Modify_Attribute --qdescription "attempt to modify the attributes of file" --severity 2 --lowlevelcategoryid 8014
```

6. Here is the command for the QID mapping for the CREATE event (creating file) mapping to the low-level category File Created:

```
# / opt/qradar/bin/ qidmap_cli.sh -c --qname Create_File --qdescription "attempt to create the file" --severity 1 --lowlevelcategoryid 8028
```

7. Here is the command for the QID mapping for the ACLCHANGE event (changing file permissions) mapping to the low-level category Failed File Modification:

```
# / opt/qradar/bin/ qidmap_cli.sh -c --qname ChangeFile_Permissions --qdescription "attempt to change permissions of the file" --severity 1 --lowlevelcategoryid 8021
```

8. Here is the command for the QID mapping for the RMDIR event (removing directory) mapping to the low-level category Failed File Modification:

```
# / opt/qradar/bin/ qidmap_cli.sh -c --qname Remove_directory --qdescription "attempt to remove directory" --severity 1 --lowlevelcategoryid 8021
```


When you are done with QID creation, create the Log Source for IBM Spectrum Scale by completing the following steps:

1. Go to the **Admin** tab and select **Data Sources** → **Log Sources** → **Add**.
2. Configure the Log Source, which is shown in Figure 20, with the following details:
 - Log Source Name: Add the name for the log source as “Spectrum_Demo”.
 - Log Source Description: Add a description for the log source.
 - Log Source Type: Select **Spectrum_LogSource** from the drop-down menu.
 - Protocol Configuration: Syslog.
 - Log Source Identifier: The host name or IP address for the IBM Spectrum device.
3. Select the **Enabled** check box and accept the default value for **Credibility**.
4. Target Event Collector: Set the event collector over which the events are collected as shown in Figure 20.
5. You may clear or select **Coalescing Events**. Keep the default payload encoding.
6. Select **Store Event Payload**.
7. Log Source Extension: Select the one that was created, as shown in Figure 20.
8. Click **Save**.

Log Source Description	Spectrum Demo Log S
Log Source Type	Spectrum_LogSource
Protocol Configuration	Syslog
Log Source Identifier	scalegui
Enabled	<input checked="" type="checkbox"/>
Credibility	5
Target Event Collector	eventcollector0 :: vm09
Coalescing Events	<input type="checkbox"/>
Incoming Payload Encoding	UTF-8
Store Event Payload	<input checked="" type="checkbox"/>
Log Source Extension	SpectrumLogSourceCustom_ext

Figure 20 IBM QRadar: Creating the log source for the IBM Spectrum Scale logs

Note: A deployment is required after you create the log source.

After creating the log source and generating QIDs, map the events. If you do not map the events, they are categorized as “Unknown Generic Log Event”.

Complete the following steps:

1. As shown in Figure 21, from the **Log Activity** tab, click **Events generated from IBM Spectrum Scale** and then select **Log Activity** → **Map Event**.

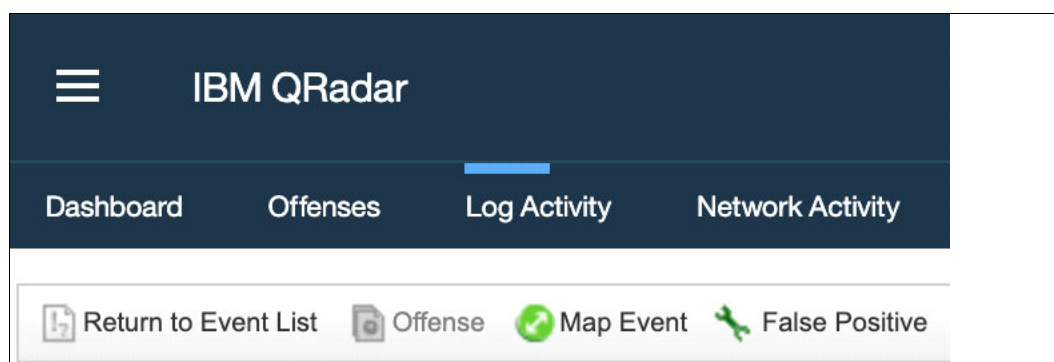


Figure 21 IBM QRadar: Selecting Map Event for QID mapping with events

2. From the **QID/Name** list that is shown in Figure 22, select the relevant QID.
For example, for the OPEN event ID, select the **Open_File** QID, and for CLOSE, select the **Close_File** QID.

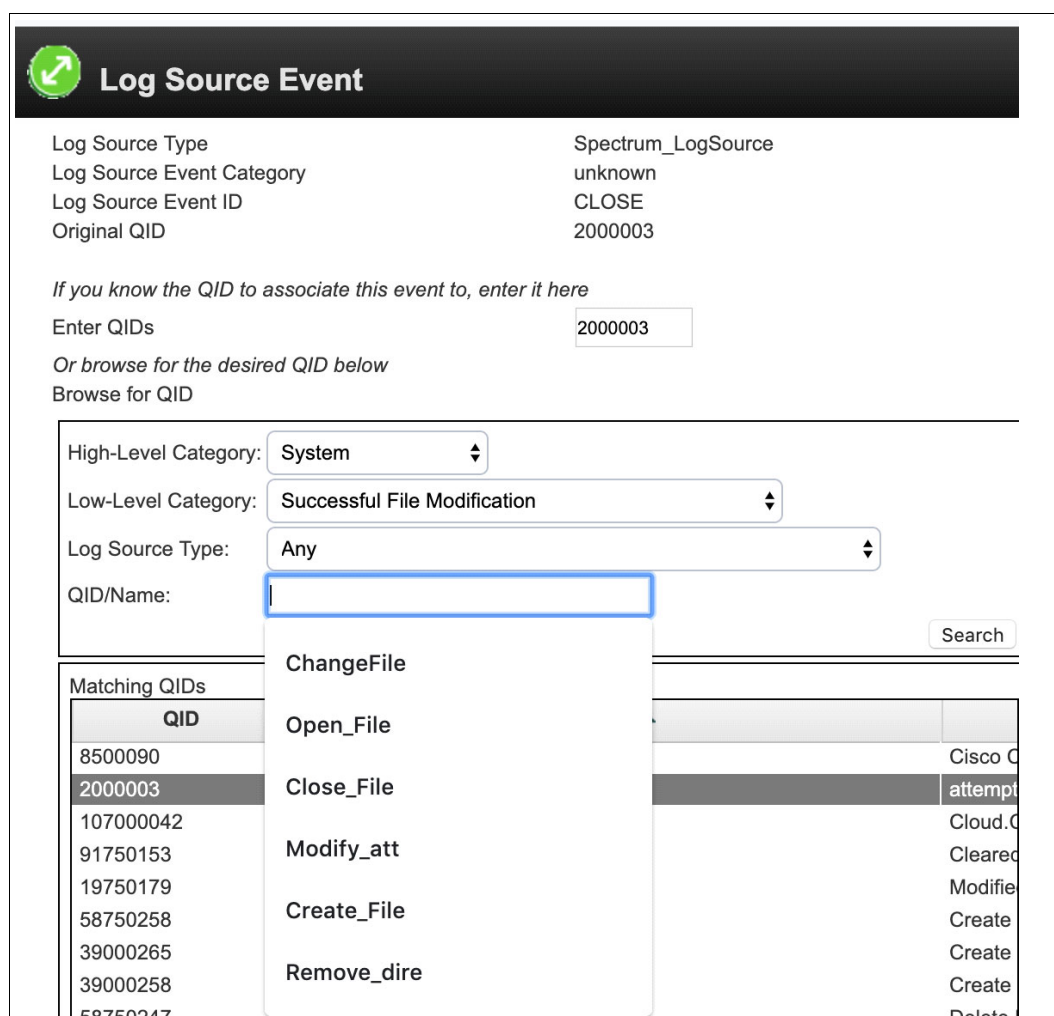


Figure 22 IBM QRadar: Mapping QIDs

3. Click **OK** to save the changes. Select the remaining events one by one and map their QIDs.

The events are parsed properly for the IBM Spectrum Scale log source, as shown in Figure 23.

Dashboard Offenses Log Activity Network Activity Assets Reports						
Search... ▾ Quick Searches ▾ Add Filter Save Criteria Save Results Cancel False Positive Rules ▾ Actions ▾						
Update Details						
(Hide Charts)						
	Event Name	Log Source	Event Count	Time ▾	Low Level Category	Source IP
	Open_File	Spectrum_Demo	1	10 Jun 2019, 10:15:09	Successful File Mod...	172.16.1.3
	ChangeFile_Permis...	Spectrum_Demo	1	10 Jun 2019, 10:15:09	Failed File Modificat...	172.16.1.3
	Close_File	Spectrum_Demo	1	10 Jun 2019, 10:15:09	Successful File Mod...	172.16.1.3
	Modify_Attribute	Spectrum_Demo	1	10 Jun 2019, 10:15:09	Successful File Mod...	172.16.1.3
	Open_File	Spectrum_Demo	1	10 Jun 2019, 10:15:09	Successful File Mod...	172.16.1.3
	Modify_Attribute	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Close_File	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Move_File	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Move_File	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Rename_File	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Modify_Attribute	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Modify_Attribute	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Close_File	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Open_File	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Open_File	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Modify_Attribute	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Close_File	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Modify_Attribute	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Create_File	Spectrum_Demo	1	10 Jun 2019, 10:15:08	File Created	172.16.1.3
	Remove_directory	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Failed File Modificat...	172.16.1.3

Figure 23 IBM QRadar: Parsing the output for the IBM Spectrum Scale log source

Creating the rules in IBM QRadar

After the events are parsed properly by IBM QRadar, then you create the correlation rules that are based on your business use cases. The number of rules that can be created to take advantage of this integration is infinite. However, the following sections include a few rules that you can create in IBM QRadar to see the benefit of this integration.

You can use the following sample manifestations to create your own use cases for this integration. All the following rules can be created by selecting **Offenses** → **Rules** → **Actions** → **New Event Rule** in IBM QRadar, to which the IBM Spectrum Scale log source is sending its events.

Rule 1

Here we describe the objective, descriptions, and definitions of the rule:

Objective of the Rule Detect any file accesses outside of business hours.

Description of the Rule This Rule detects any file accesses that are done outside of Business Hours and generates an Offense for each such activity. In this rule, you look for any event from the IBM Spectrum Log Source with a QID that relates to opening files (Open File), and whether this event comes in after 6:30 PM and before 9 AM (non-business hours).

If such an event is detected, this rule generates an Offense and increases the Severity, Relevance, and Credibility (SRC) values by 2. Therefore, the Magnitude value of the offense that it generates is relatively higher.

Rule definition

Figure 24 shows the rule definition of Rule 1.

Note: In the rule that is shown in Figure 24, combining the condition of generating event after 18:30 and before 09:00 requires IBM QRadar building blocks, which are used by an advanced IBM QRadar administrator. The other way to achieve the same result is to write two separate rules: One rule for “after 18:30” hours (which covers the incidences 18:30 - 00:00 hours), and another rule for “before 09:00” hours (which covers the incidences 00:00 - 09:00 hours). For more information see [IBM QRadar building blocks](#).

Rule Wizard

Rule Wizard: Rule Test Stack Editor

Which tests do you wish to perform on incoming events?

Test Group All ▼
Export as Building

Type to filter

+ when the local network is **one of the following networks**

+ when the **destination** network is **one of the following networks**

+ when the IP protocol is one of the following **protocols**

+ when the Event Payload contains **this string**

+ when the source port is one of the following **ports**

+ when the destination port is one of the following **ports**

+ when the local port is one of the following **ports**

+ when the remote port is one of the following **ports**

+ when the source IP is one of the following **IP addresses**

+ when the destination IP is one of the following **IP addresses**

+ when the local IP is one of the following **IP addresses**

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

Apply OutOfOfficeHours on events which are detected by the Local ▼ system

and when the event(s) were detected by one or more of [Spectrum Demo](#)

and when the event QID is one of the following [\(2000002\) Open File](#)

and when the event(s) occur [after 18:30](#)

and when the event(s) occur [before 09:00](#)

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

☐ Anomaly

☐ Asset Reconciliation Exclusion

☐ Authentication

☐ Botnet

☐ Category Definitions

Figure 24 IBM QRadar: Rule definition for Rule 1

Rule Response

Figure 25 shows the options for the **Rule Action** and the **Rule Response**.

Rule Wizard

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

☒ Severity

Increase by

▼

 2

▼

☒ Credibility

Increase by

▼

 2

▼

☒ Relevance

Increase by

▼

 2

▼

☒ Ensure the detected event is part of an offense

Index offense based on

Username

 ▼

☒ Annotate this offense:

User Access post office hou

☐ Include detected events by Username from this point forward, in the offense, for : second(s)

☐ Annotate event

☐ Drop the detected event

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

☐ Dispatch New Event

☐ Email

☐ Send to Local SysLog

☐ Send to Forwarding Destinations

☐ Notify

☐ Add to a Reference Set

☐ Add to Reference Data

☐ Remove from a Reference Set

☐ Remove from Reference Data

☐ Execute Custom Action

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

☐ Respond no more than time(s) per second(s) ▼ per

Rule

 ▼

Enable Rule

☒ Enable this rule if you want it to begin watching events right away.

Figure 25 IBM QRadar: Rule Action and Rule Response for Rule 1

Rule Summary page

Figure 26 describes the **Rule Summary** for Rule 1.

Rule Summary

Review this rule summary to ensure all the details you have specified are correct. You may click 'Back' to change incorrect settings.

Note that your rule has not yet been saved or deployed. It will be saved when you select 'Finish' and only be deployed if you chose the 'Enable Rule' checkbox on the previous screen.

Rule Description

Apply OutOfOfficeHours on events which are detected by the Local system and when the event(s) were detected by one or more of Spectrum_Demo and when the event QID is one of the following (2000002) Open_File and when the event(s) occur after 18:30 and when the event(s) occur before 09:00

Rule Actions

- Increase Severity by 2
- Increase Credibility by 2
- Increase Relevance by 2
- Force the detected Event to create a NEW offense, select the offense using Username
 - Annotate this offense with: User Access post office hours

This Rule will be: Enabled

Figure 26 IBM QRadar: Rule Summary for Rule 1

When this rule is applied, IBM QRadar starts monitoring the rule conditions, and an offense is generated whenever any user accesses any files on IBM Spectrum Scale after office hours.

Rule 2

Here we describe the objective, descriptions, and definitions of the rule:

Objective of the Rule Detect any Risky User accessing any file on the IBM Spectrum Scale cluster during non-business hours.

Description of the Rule This Rule builds on the previous rule and takes advantage of the User Behavior Analytics (UBA) capabilities of IBM QRadar. It demonstrates the correlation capabilities across the different components of IBM QRadar. UBA, based on user activities, maintains a list of the most risky Users in the organization, which is done by using a combination of IBM Sense events and UBA Rules (for more information, see “References” on page 60). You use this list of Risky Users in this Rule.

Note that from the IBM Spectrum Scale payload that you extract the clientUserId, which is the User ID that is associated with the User who ran the activity.

While configuring UBA, you can map this clientUserId with the existing Users that UBA detected by selecting **Uba Settings** → **User Coalescing**. In this way, the numeric values of clientUserId are mapped to actual Usernames, which are then used in this Use Case.

In the Rule, you detect events from the IBM Spectrum Scale Log Source that are related to Open Files. If these two conditions match, you then match whether the User who is opening the file is a Risky User, and if the destination IP address (where the destination IP address in this example is the IP address of the IBM Spectrum Scale node from where the file is being accessed) is for one of the Critical Assets.

The last check in the rule is to see whether this activity is done after Business Hours. As a response to the Rule, you generate an Offense and Dispatch a new Event. This new Event is picked up by UBA and used to increase the Risk Score of this specific User. In this way, you are taking data from the UBA component of IBM QRadar and feeding back data to it.

Rule definition

Figure 27 shows the rule definition of Rule 2.

Rule Wizard

Which tests do you wish to perform on incoming events?

Test Group: All Export as Building Block

Type to filter

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

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

Apply HighRiskUser- OffBusinessHoursAccess on events which are detected by the Local system

- and when the event(s) were detected by one or more of Spectrum Demo
- and when the event QID is one of the following (2000001) Open File
- and when any of Username are contained in any of UBA : High Risk Users - AlphaNumeric (Ignore Case)
- and when any of Destination IP are contained in any of Critical Assets - IP
- and when the event(s) occur after 18:30
- and when the event(s) occur before 09:00

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

- ☐ Anomaly
- ☐ Asset Reconciliation Exclusion
- ☐ Authentication
- ☐ Botnet
- ☐ Category Definitions

Notes (Enter your notes about this rule)

Detects when a Risky User accesses any file on a critical server after Office Hours.

Performance Analysis

This rule has not yet had a detailed analysis.

Figure 27 IBM QRadar: Rule definition for Rule 2

Rule Response

Figure 28 shows the options for the **Rule Action** and **Rule Response**.

Rule Wizard

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

☐ Severity Set to 0
☐ Credibility Set to 0
☐ Relevance Set to 0
☒ Ensure the detected event is part of an offense
Index offense based on Source IP
☒ Annotate this offense: Risky User accessing files
☐ Include detected events by Source IP from this point forward, in the offense, for : second(s)
☐ Annotate event
☐ Drop the detected event

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

☒ Dispatch New Event
Enter the details of the event to dispatch
Event Name: UBA : High Risk User Access to Critical Asset
Event Description: senseValue=15
Event Details:
Severity 10 Credibility 10 Relevance 10
High-Level Category: Sense Low-Level Category: User Access
☐ Annotate this offense:
☐ Ensure the dispatched event is part of an offense
☐ Email
☐ Send to Local SysLog
☐ Send to Forwarding Destinations
☐ Notify
☐ Add to a Reference Set
☐ Add to Reference Data
☐ Remove from a Reference Set
☐ Remove from Reference Data
☐ Trigger Scan
☐ Execute Custom Action

Response Limiter
Use this section to configure the frequency with which you want this rule response to respond
☒ Respond no more than 1 time(s) per 30 minute(s) per Username

Enable Rule
☒ Enable this rule if you want it to begin watching events right away.

Figure 28 IBM QRadar: Rule Action and Rule Response for Rule 2

Rule Summary page

Figure 29 describes the Rule Summary for Rule 2.

Rule Summary
Review this rule summary to ensure all the details you have specified are correct. You may click 'Back' to change incorrect settings.
Note that your rule has not yet been saved or deployed. It will be saved when you select 'Finish' and only be deployed if you chose the 'Enable Rule' checkbox on the previous screen.
<div><div>Rule Description</div><div>Apply HighRiskUser- OffBusinessHoursAccess on events which are detected by the Local system and when the event(s) were detected by one or more of Spectrum_Demo and when the event QID is one of the following (2000001) Open_File and when any of Username are contained in any of UBA : High Risk Users - AlphaNumeric (Ignore Case) and when any of Destination IP are contained in any of Critical Assets - IP and when the event(s) occur after 18:30 and when the event(s) occur before 09:00</div></div> <div><div>Rule Notes</div><div>Detects when a Risky User accesses any file on a critical server after Office Hours.</div></div> <div><div>Rule Actions</div><div><ul style="list-style-type: none">Force the detected Event to create a NEW offense, select the offense using Source IP<ul style="list-style-type: none">Annotate this offense with: Risky User accessing files on a critical server after Office Hours</div></div> <div><div>Rule Responses</div><div><ul style="list-style-type: none">Dispatch New Event<ul style="list-style-type: none">Event Name: UBA : High Risk User Access to Critical AssetEvent Description: senseValue=15Severity: 10 Credibility: 10 Relevance: 10High-Level Category: SenseLow-Level Category: User Access</div></div> <div><div>Rule Limiter</div><div>Respond no more than 1 time(s) per 30 minute(s) per Username</div></div> <div><div>This Rule will be: Enabled</div></div>

Figure 29 IBM QRadar: Rule Summary for Rule 2

Rule 3

Here we describe the objective, descriptions, and definitions of the rule:

Objective of the Rule

To detect file access by the same user from different geographies within 1 hour.

Description of the Rule

This Rule detects any user who opens any file from one county or geography and then accesses the file from another geography within 1 hour. It is not physically possible to open a file remotely from one geography and then travel to another geography and then access the file remotely from that new geography within 1 hour.

This Rule reflects a scenario of shared User IDs or compromised User IDs. This rule also covers scenarios in which a user opens a file from one geography (or a system with a unique IP address that maps to a certain geography) and then modifies another file from another geography (or another system with another unique IP address that maps to another geography) within 1 hour.

To implement this use case, you use the Building Blocks capability of IBM QRadar. You create two Building Blocks: **BB: File Open** and **BB: File Modify**.

Note: For the mentioned IBM Spectrum Scale setup, this example is hypothetical. In this setup, the systems are within the same LAN, but this rule illustrates the possibilities of what you can achieve by using IBM QRadar. For example, within the mentioned IBM Spectrum Scale cluster, if a file is accessed by the same user but from different nodes (where nodes are uniquely identified by IP address) and within a certain period, this event can be flagged by IBM QRadar.

This capability helps in organizations where an IBM Spectrum Scale cluster is deployed in such a way that an organization's department systems are separated based on IP addresses. In such cases, you can define an IP address range per department in IBM QRadar, and implement the same scenario explained previously, which is at a country or geography level.

Rule definition

Complete the following steps:

1. For **BB: File Open**, check whether the Events are from the IBM Spectrum Log Source, and whether the QID relates to someone opening a file, as shown in Figure 30.

Rule Wizard

Rule Wizard: Rule Test Stack Editor

Which tests do you wish to perform on incoming events?

Test Group:

Type to filter

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

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

Apply on events which are detected by the system

☐ and when the event(s) were detected by one or more of Spectrum Demo

☐ and when the event QID is one of the following (2000002) Open File


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

- ☐ Anomaly
- ☐ Asset Reconciliation Exclusion
- ☐ Authentication
- ☐ Botnet
- ☐ Category Definitions

Figure 30 IBM QRadar: Creating a Building Block to check whether the QID in the event maps to File Open

- For **BB: File Modify**, check whether the Events are from the IBM Spectrum Log Source, and whether the QID is related to any of the File modifications-related QIDs, as shown in Figure 31.

Rule Wizard


Rule Wizard: Rule Test Stack Editor

Which tests do you wish to perform on incoming events?

Test Group All

Type to filter

+

 when the local network is **one of the following networks**

+

 when the **destination** network is **one of the following networks**

+

 when the IP protocol is one of the following **protocols**

+

 when the Event Payload contains **this string**

+

 when the source port is one of the following **ports**

+

 when the destination port is one of the following **ports**

+

 when the local port is one of the following **ports**

+

 when the remote port is one of the following **ports**

+

 when the source IP is one of the following **IP addresses**

+

 when the destination IP is one of the following **IP addresses**

+

 when the local IP is one of the following **IP addresses**

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

Apply BB:File Modify on events which are detected by the Local system

and when the event(s) were detected by one or more of Spectrum Demo
and when the event QID is one of the following (2000004) Modify Attribute, (2000006) ChangeFile Permissions, (2000001) Rename File

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

Anomaly

Asset Reconciliation Exclusion

Authentication

Botnet

Category Definitions

Figure 31 IBM QRadar: Creating a Building Block to check whether the QID in the event maps to File Modify

- Create the Rule to check whether the two Building Blocks match within 1 hour for the same User ID from different countries. In our case, the CEP that is named `Spectrum_clientUserID` that you created previously, which contains the User ID of the user, is used in this rule to match whether it is the same user or a different user.

Rule Response

Figure 32 shows the options for the Rule Action and Rule Response.

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

☒Severity

Increase by

5

☒Credibility

Increase by

5

☒Relevance

Increase by

5

☒Ensure the detected event is part of an offense

Index offense based on

Source IP

☒Annotate this offense: File access from multiple co

☐Include detected events by Source IP from this point forward, in the offense, for : second(s)

☐Annotate event

☐Drop the detected event

Rule Response
Choose the response(s) to make when an event triggers this rule☐Dispatch New Event☐Email☐Send to Local SysLog☐Send to Forwarding Destinations☐Notify☐Add to a Reference Set☐Add to Reference Data☐Remove from a Reference Set☐Remove from Reference Data☐Execute Custom Action**Response Limiter**
Use this section to configure the frequency with which you want this rule to respond☐Respond no more than time(s) per second(s) per Rule**Enable Rule**☒Enable this rule if you want it to begin watching events right away.

Figure 32 IBM QRadar: Rule Action and Rule Response for Rule 3

This Rule Response generates an Offense and increases the SRC values by 5. Therefore, the Magnitude value of the Offense that it generates is relatively higher (where the magnitude of the value determines the severity of the offense).

Rule Summary page

Figure 33 describes the Rule Summary for Rule 3.

Rule Summary

Review this rule summary to ensure all the details you have specified are correct. You may click 'Back' to change incorrect settings.

Note that your rule has not yet been saved or deployed. It will be saved when you select 'Finish' and only be deployed if you chose the 'Enable Rule' checkbox on the previous screen.

Rule Description

Apply Geographic location change on events which are detected by the Local system and when BB:File open, BB:File Modify match at least 2 times with the same Spectrum_clientUserId (custom) and different Source Geographic Country/Region in 1 hour(s)

Rule Actions

- Increase Severity by 5
- Increase Credibility by 5
- Increase Relevance by 5
- Force the detected Event to create a NEW offense, select the offense using Source IP
 - Annotate this offense with: File access from multiple countries by the same user

This Rule will be: Enabled

Figure 33 IBM QRadar: Rule Summary for Rule 3

You can tune any of the rules and modify the Rule Responses to better fit your environment and requirements.

Note: Starting with IBM Spectrum Scale 5.1.0, file access denied events (ACCESS_DENIED event) are also recorded in file audit logs which can be used to create a new set of threat rules like flagging an alert if there is a continuous access denied event for a certain set of files which could hint at a brute force like attack on data access.

IBM QRadar with IBM Spectrum Scale: Proactively trigger a Data Protection/Cyber Resiliency workflow on threat detection

So far, the paper has described on how to integrate an IBM Spectrum Scale file audit log and IBM QRadar to alert on potential threats to the data that is hosted on IBM Spectrum Scale. In this section, we take the solution to the next level. When IBM QRadar detects a threat, it raises an alert and communicates with IBM Spectrum Scale to protect the data under threat. There can be various methods to protect the data under threat. One of the most useful methods is to take snapshot of the data at the storage level. Taking the snapshot of the data generates a read-only copy (copy on write) of the data so that administrators can roll back to the previous version if required.

There are various use cases where this solution can be useful. Here are two such use cases:

1. **Cyber Resiliency:** This solution enhances the existing IBM Spectrum Scale Cyber Resiliency solution (see *Cyber Resiliency Solution for IBM Spectrum Scale*, REDP-5559) by integrating it into the threat detection in the “Detect” phase of the National Institution of Standards and Technology (NIST) security framework.
2. **Business Policy on Data access by employees or applications:** The solution can detect violations of business policies around data access and provide proactive data protection through data snapshots. In this section, we build a solution on this use case.

Figure 34 shows the high-level view of the solution of how to achieve proactive data protection on threat detection. It shows that IBM Spectrum Scale File Audit Logging is configured to forward its logs to IBM QRadar. IBM QRadar is configured to continuously monitor and correlate the logs to identify threats in real time. IBM QRadar is uploaded with a custom script that automatically invokes the snapshots or a Cyber Resiliency workflow on IBM Spectrum Scale when a threat is detected.

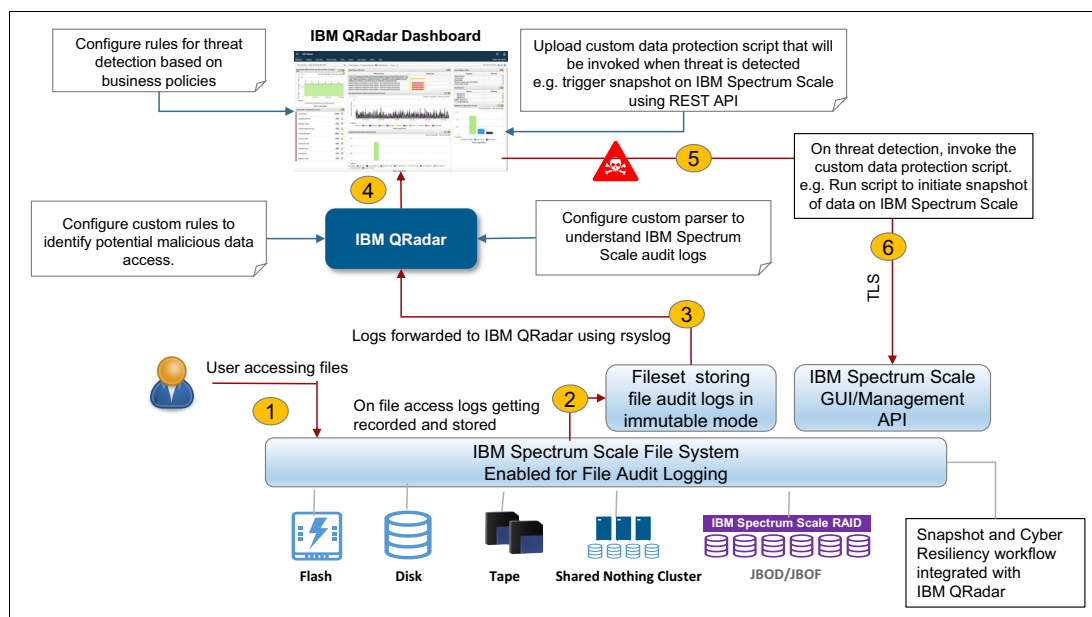


Figure 34 High-level view of solution for data protection on threat detection

Before you proceed, you must understand some basic concepts of snapshots and the APIs of IBM Spectrum Scale.

IBM Spectrum Scale snapshots

A snapshot of an entire GPFS file system can be created to preserve the contents of the file system at a single point. Snapshots of a file system are read-only; changes can be made only to the active (that is, normal non-snapshot) files and directories. Snapshots also provide an online backup capability for easy recovery from problems, such as accidental or intentional deletion of a file, and comparison with older versions of a file. Therefore, using a snapshot to safeguard a version of data when a potential threat is detected is one possible way to lessen the impact of data loss or data tampering by the threat agent. For more information, see IBM Spectrum Scale [Snapshots](#).

IBM Spectrum Scale management API

The IBM Spectrum Scale management API is a REST-style interface for managing IBM Spectrum Scale cluster resources. With the IBM Spectrum Scale management API, you can develop scripts to automate labor-intensive cluster management tasks or use them to integrate and create solutions.

The IBM Spectrum Scale management API consists of an API to securely initiate the snapshot of the file system or file sets through programming modules that we use in this solution. For more information, see [IBM Spectrum Scale management API](#).

Program for initiating snapshots by using the IBM Spectrum Scale REST API

“Appendix A: Custom script to take a snapshot” on page 51 shows a sample Python program that uses the IBM Spectrum Scale management API to initiate snapshots on the IBM Spectrum Scale file system or file set. This program serves as a custom script that must be configured with IBM QRadar. You may modify the program to suit your needs.

IBM QRadar custom script

With IBM QRadar, administrators can invoke a custom script and pass data to a script that is based on a rule response.

IBM QRadar allows *custom* actions to select or define the value that is passed to the custom script and run the resulting action. The use of these custom scripts is structured. There are three options for scripting: Bash, Perl, and Python. Custom actions are run in a *jailshell* to protect your data from a possible exploit from IBM QRadar.

The custom script must be uploaded into IBM QRadar by using the **Define Actions** icon in the **Admin** tab of the IBM QRadar GUI. The script is created by using a standard editor and saved to the location on the local drive that is used to access IBM QRadar before uploading it onto IBM QRadar.

After the script is created, click the **Define Actions** icon to show a list of existing scripts. Click **Add** in the menu bar, and in the window that opens, enter a name and description and the script interpreter, and then choose the custom script by clicking **Browse** and selecting the file name.

Creating a custom action script

This section explains how to create custom action scripts that can be associated with QRadar events.

Complete the following steps:

1. Create a file with a .py, .sh, or .pl extension.
2. In the IBM QRadar GUI, open **Admin settings**.
3. Click the navigation menu, and then click **Admin** to open the **Admin** tab.
4. Under **Custom Actions**, click **Define Actions**.
5. To upload your scripts, click **Add**.
6. Under **Basic Information**, type a name for the custom action.
7. Scroll down to **Script configuration** and select **Interpreter: Bash, python, perl**.
8. Click **Browse** and find the file that you created in step 1.
9. Scroll to the bottom of the Define Custom Action window and click **Save**.
10. Click **Deploy Changes**.

Testing the custom action script

Verify that the test file is created or updated either by using the **Test Execution** function in the Define Actions window or by confirming that the Custom Rule has been triggered.

To test the script by using the Test Execution, complete the following steps:

1. Open the **Admin settings**, and in the IBM QRadar GUI, click the navigation menu, and then click **Admin** to open the **Admin** tab.
2. Scroll down to **Custom Actions**.
3. Click **Define Actions**.
4. Highlight the test script.
5. Click **Test Execution** → **Execute**.

The screenshot displays the 'Test Custom Action Execution' window. It contains two parameter sections: 'password' and 'device'. Each section has a 'Parameter Type' dropdown set to 'Fixed Property' and a 'Parameter Value' text box. For 'password', the value is 'Passw0rd'. For 'device', the value is 'fs1'. Below these is the 'Test Execution' section, which shows a 'Result' of 'Execution Successful' with a green checkmark icon, and a 'Snapshot successful' message. The 'Output' section is empty. At the bottom, there are 'Execute' and 'Close' buttons.

Figure 35 Testing the custom action script

Results: Test Execution should be successful

In the “Testing the custom action script” example, on successful execution of the custom script a snapshot is created on IBM Spectrum Scale, which you can verify on the IBM Spectrum Scale GUI. After the script is verified, the custom script is ready to be associated with IBM QRadar events.

Editing the custom action script

If you need to edit the custom action script (for example, the password that is associated with the script must be updated), complete the following steps:

1. Open the **Admin settings**, and in the IBM QRadar GUI, click the navigation menu, and then click **Admin** to open the **Admin** tab.
2. Scroll down to **Custom Actions**.
3. Click **Define Actions**.

4. Highlight the test script.
5. Click **Edit** to alter the required parameters and click **Save**.
6. Test the modified script by clicking **Test Execution**.

Deleting custom action scripts

If you need to delete the custom action script, complete the following steps.

1. Open the **Admin settings**, and in the IBM QRadar GUI, click the navigation menu, and then click **Admin** to open the **Admin** tab.
2. Scroll down to **Custom Actions**.
3. Click **Define Actions**.
4. Highlight the test script.
5. Click **Delete** and click **OK**.

Editing a custom rule to run the custom action script

Now that you have the custom script ready, you can associate the script with the specific IBM QRadar rule response, which triggers this script when the specific event is triggered by the rule. To associate the custom script-specific rule, complete the following steps:

1. Log in to the IBM QRadar UI.
2. Click the **Offense** tab and then click **Rules**.
3. Locate or create a custom rule in the Rule wizard.
4. Edit the Rule to add the host IP and a criteria, such as successful login.
5. Click **Next** to configure the Rule Responses.
6. Select the **Execute Custom Action** check box.
7. Click the newly created custom action script in the **Custom Action to execute** drop-down menu, as shown in Figure 36.

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

☐ Dispatch New Event
☐ Email
☐ Send to Local SysLog
☐ Send to Forwarding Destinations
☐ Notify
☐ Add to a Reference Set
☐ Add to Reference Data
☐ Remove from a Reference Set
☐ Remove from Reference Data
☐ Trigger Scan
☒ Execute Custom Action

Custom Action to execute: Working_Spectrum_script

Figure 36 Rule Response for running the custom script

Sample use case

According to the business policy, users (especially risky users) are not supposed to access data that is hosted on IBM Spectrum Scale during non-business hours. If they do, the solution is required to generate an alert and safeguard the data on IBM Spectrum Scale so that the data can be recovered if any changes are made. These actions are two of the many manifestations for which you can create a solution by using IBM QRadar and IBM Spectrum Scale for proactive safeguarding of data on threats alerts. Another manifestation is to trigger a Cyber Resiliency workflow to take a backup when a threat is detected, which you can set up by creating another Rule.

Description of the Rule This Rule is an extension to “Rule 2” on page 28 where IBM QRadar detects the threat and invokes data protection scripts that safeguard the data on IBM Spectrum Scale.

The only change that you do is to include the custom script under the Rule Response section that is shown in Figure 37.

Objective of the Rule Detect any Risky User that accesses any file on the IBM Spectrum Scale cluster during non-business hours *and* generate an event to notify IBM Spectrum Scale to take a snapshot of the file system.

This Rule is an extension to “Rule 2” on page 28, where IBM QRadar must detect the threat and invoke data protection scripts that safeguard the data on IBM Spectrum Scale.

The only change that you must do is to include the custom script that you created in “Creating a custom action script” on page 37 is shown in the **Rule Response** section in Figure 37.

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

☒ Dispatch New Event

Enter the details of the event to dispatch

Event Name: UBA : High Risk User Access to Critical Asset

Event Description: senseValue=15

Event Details:

Severity: 10 ▾ Credibility: 10 ▾ Relevance: 10 ▾

High-Level Category: Sense ▾ Low-Level Category: User Access

☐ Annotate this offense:

☐ Ensure the dispatched event is part of an offense

☐ Email

☐ Send to Local SysLog

☐ Send to Forwarding Destinations

☐ Notify

☐ Add to a Reference Set

☐ Add to Reference Data

☐ Remove from a Reference Set

☐ Remove from Reference Data

☐ Trigger Scan

☒ Execute Custom Action

Custom Action to execute: Working_Spectrum_script ▾

Figure 37 Rule Response with the custom script that dispatches a new event

Note: If you are not using IBM QRadar Building Blocks to create a single rule that generates an event after 18:30 and before 09:00, which is typically done by an advanced IBM QRadar administrator, and have written two separate rules, then you must associate the custom script to both of these rules:

- ▶ Rule for “after 18:30” hours (which covers the incidents 18:30 - 00:00 hours)
- ▶ Rule for “before 09:00” hours (which covers the incidents 18:30 - 00:00 hours)

As shown in Figure 37 on page 40, you enabled the **Execute Custom Action** option and selected the script that you created in “Creating a custom action script” on page 37 from the drop-down menu.

This Rule now detects any risky user access of any files on the IBM Spectrum Scale cluster outside of business hours. If any such access occurs, the Rule generates an Offense and dispatches a new Event. This Event is picked up by UBA and used to increase the Risk Score of this specific User. In this way, you are taking data from the UBA component of IBM QRadar and feeding data to it. Then, the Rule takes a snapshot of the file system to maintain a copy of the file system before the User makes any malicious changes. An IBM Spectrum Scale admin can list snapshots that were taken proactively in the IBM Spectrum Scale GUI (see Figure 38) to make any necessary decisions.

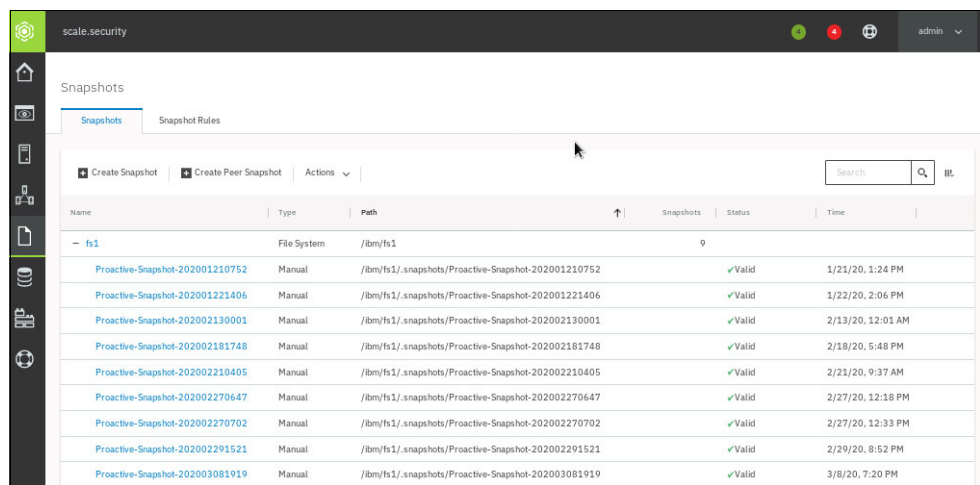


Figure 38 IBM Spectrum Scale GUI showing the list of file system snapshots

Similar changes in the Rule Response can be set for the other two use cases that are described in “Creating the rules in IBM QRadar” on page 25. You can also create your own set of rules for specific use cases and use the script in “Appendix A: Custom script to take a snapshot” on page 51 to automate the snapshot capability on an IBM Spectrum Scale cluster whenever IBM QRadar detects any security breaches.

Make sure that IBM QRadar does not continually trigger the custom script for a potential threat, but instead limit or throttle the script for a period. Otherwise, you get multiple snapshots of the file system in a short period, which impacts the overall system. To ensure this action, use the **Response Limiter** option that is present in the Rule Response window, as shown in Figure 39.

Response Limiter

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

☒ Respond no more than
 time(s) per
 hour(s)

▼

 per

Figure 39 Response Limiter

The Response Limiter must be set for all the different use cases. Using the settings in Figure 39 means that the snapshot script runs once every 9 hours for every risky User who accesses or modifies the file system outside of business hours. In this example, we selected 9 hours to exclude normal business hours. However, you can change these settings to meet the requirements of different customer environments.

Note: Ensure that a best practice for taking IBM Spectrum Scale snapshots is included in the solution. Taking frequent snapshots impacts the overall performance of the IBM Spectrum Scale system. Setting the Response Limiter is an important step of this solution, and only one snapshot should be triggered every day.

Note: The password of the IBM Spectrum Scale administrator account that is used to generate snapshots on threat detection must be periodically changed according to the organization's password policies. When the password is changed, update the IBM QRadar custom scripts to update the password in them, or the IBM QRadar scripts to take snapshots will not work.

Important: The solution does *not* guarantee a foolproof data protection or safeguarding. There might be instances where the data is changed or deleted before the data snapshot is initiated by IBM QRadar or before it was successfully taken by IBM Spectrum Scale system. Practitioners must evaluate the benefits to their business needs and the risks.

Ransomware threat detection

Having understood how IBM QRadar is helping to detect malicious user activity, we now discuss a Ransomware attack scenario within an environment, where we continue to leverage IBM Spectrum Scale File Audit logs integration with IBM QRadar.

Note: The solution presented here is not a replacement for any endpoint protection security software (Antivirus/Antimalware). Also, the method mentioned is not a guarantee to safeguard from ransomware, but an additional provision complementing an existing mechanism to protect the data against ransomware.

In this use case, IBM Spectrum Scale is enabled with SMB protocol (via the IBM Spectrum Scale protocol nodes) so the Windows clients can mount a network share to work/store the data. In this example, one of the Windows clients has a ransomware infection, and the ransomware is also scanning the network locations to spread the infection.

To illustrate the use case, an isolated environment was created in the lab. Figure 40 on page 43 represents the lab setup created for the ransomware simulation.

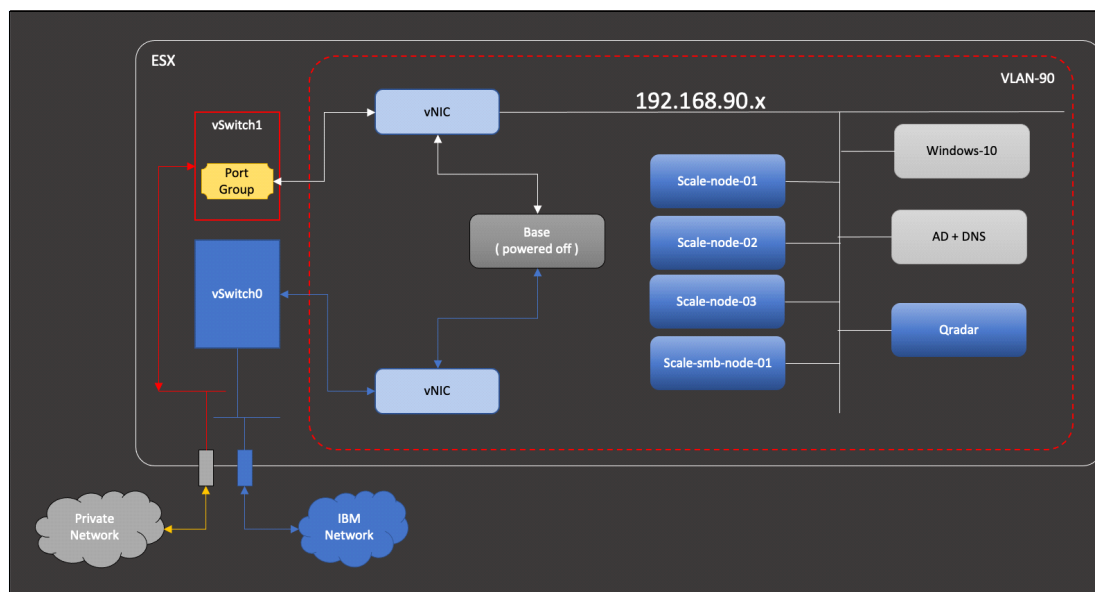


Figure 40 Lab setup for Ransomware simulation

The setup consisted of:

- ▶ A four node IBM Spectrum Scale cluster (version 5.1.0.2) of which 3 nodes were designated as NSD servers and 1 node created as a protocol node running SMB service
- ▶ Creating an Active directory server for network wide authentication and also for designating SMB export owners on the IBM Spectrum Scale cluster
- ▶ Installing a single Windows 10 system and using a client to mount the SMB export
- ▶ Creating a directory structure to keep approximately 90 test files of various types such as documents, spreadsheets, presentations, images, and PDFs

Due to the nature of the testing, the entire setup was isolated in a virtual LAN. The entire simulation was carried out by logging on to virtual machines using ESXi console. Client side caching (csc) policy was disabled on the SMB export to facilitate audit logging every time the file is accessed from the export. A Rsyslog configuration was created to forward the audit logging events to QRadar.

Note: Starting with IBM Spectrum Scale 5.1.0, changes are made when enabling to audit logging. The audit logging no longer uses the Kafka message queues.

Example 13 shows the command used to enable file audit logging.

Example 13 Enabling audit

```
mmaudit gpfs0 enable
```

Note: Before enabling file audit logging, SELinux must be disabled or set to permissive mode.

For the detection of ransomware, the file extension and associated file input output (I/O) changes recorded in file audit logs were considered before acting on the events. A ransomware attack study indicates that when the file is infected with ransomware, more often than not its extension is changed. This is done so that the ransomware can skip the infected files. While few ransomware add an extension to the files, others simply rename them.

A set of known ransomware extensions were loaded as reference sets in IBM QRadar (7.4.2) against each file extension in order to be compared. Refer to “Appendix D: Sample list of known ransomware file extensions” on page 54 for the sample set of file extensions used.

The reference set of file extensions was created by selecting **Reference Set Management** from the **Admin** tab section of IBM QRadar, as shown in Figure 41.

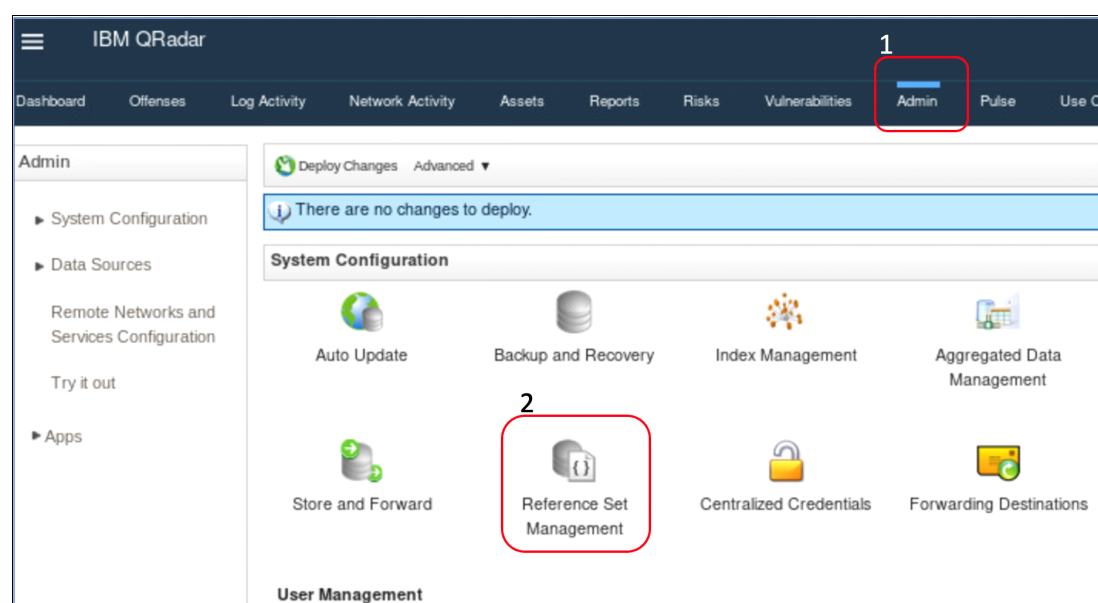
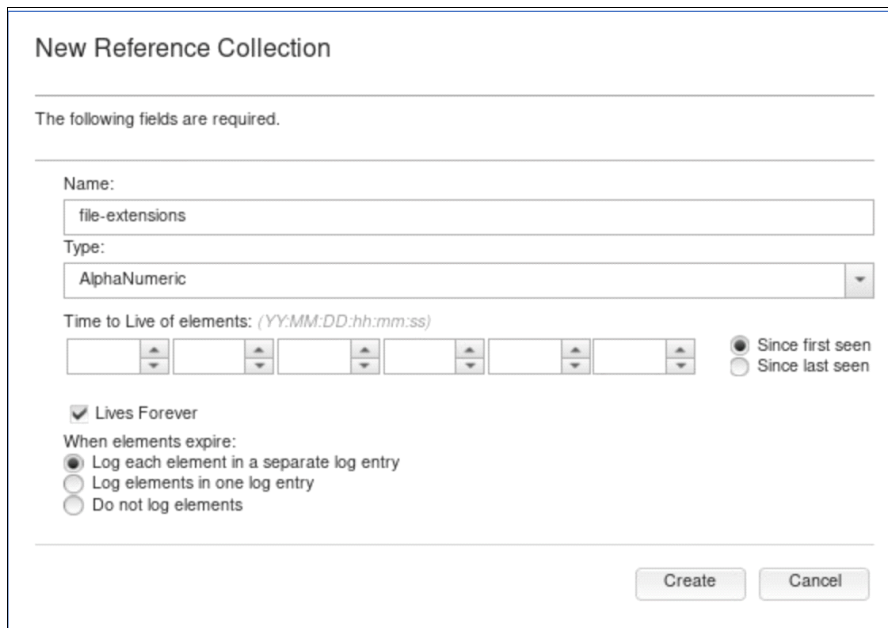


Figure 41 Menu path for Reference set management

A new reference set collection is created as shown in Figure 42 on page 45.



New Reference Collection

The following fields are required.

Name:

Type:

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

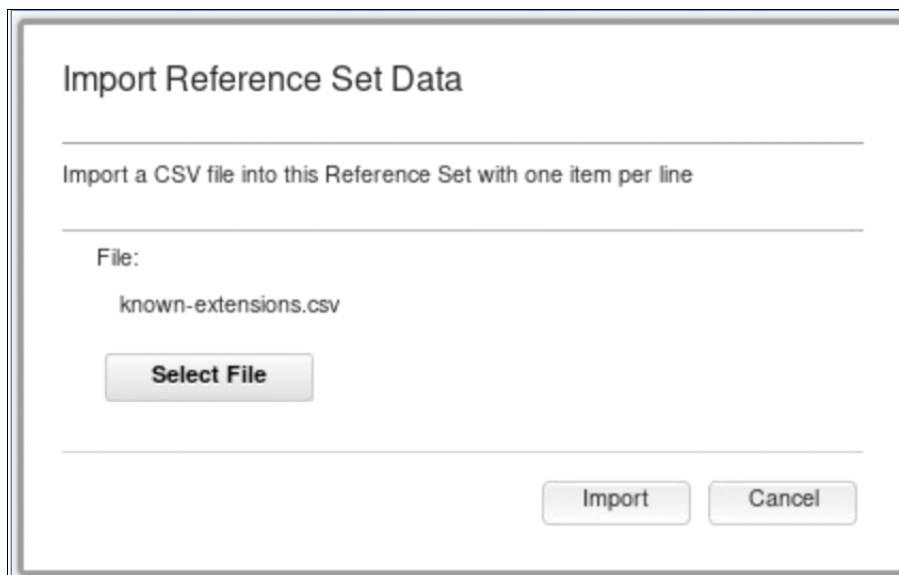
☒ Since first seen
☐ Since last seen

☒ Lives Forever

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

Figure 42 Menu path for Reference set management

It is possible to define specific file extensions or load a text file containing a single extension per line. This extension file was imported using the import screen, as shown in Figure 43.



Import Reference Set Data

Import a CSV file into this Reference Set with one item per line

File:
 known-extensions.csv

Figure 43 Importing csv file containing known ransomware extensions

All the imported extensions are now part of the file-extensions reference set, as shown in Figure 44.

Reference Set: file-extensions

Content

References

Add

Delete

Delete Listed

Import

Export

Add new search criteria...

Value	Origin	Time to Live	Date Last Seen
lovewindows	admin		Jun 4, 2021, 2:01:15 PM
paymts	admin		Jun 4, 2021, 2:01:15 PM
vindows	admin		Jun 4, 2021, 2:01:15 PM
VforVendetta	admin		Jun 4, 2021, 2:01:15 PM
odin	admin		Jun 4, 2021, 2:01:15 PM
ppr	admin		Jun 4, 2021, 2:01:15 PM
damage	admin		Jun 4, 2021, 2:01:15 PM
spora	admin		Jun 4, 2021, 2:01:15 PM
zorro	admin		Jun 4, 2021, 2:01:15 PM
rdm	admin		Jun 4, 2021, 2:01:15 PM
paym	admin		Jun 4, 2021, 2:01:15 PM
MRCR1	admin		Jun 4, 2021, 2:01:15 PM

Figure 44 Reference set with imported extensions

With IBM QRadar configuration completed, the ransomware simulation was started on the Windows client. On the IBM Spectrum Scale, as file auditing is configured, the access to every file is logged as an audit event. Based on the audit events generated for various infections examined in a lab environment, more commonly the following event pattern emerged.

- ▶ A new file is created with the same name and extension with an added extension or a file is created with an arbitrary name and an extension. This action generates a CREATE event.
- ▶ A CREATE event is followed by an OPEN event on the file.
- ▶ A CLOSE event is observed on the OPEN file.
- ▶ A set of OPEN / CLOSE / RENAME events was seen when the source file was infected without creating a new file. The RENAME event renames the file to the same name with an extension added or an entirely different filename and extension.

The above scenario narrowed down the set of CREATE/OPEN/CLOSE/RENAME events and single or double file extension.

Based on this information, IBM QRadar rules were written (see Figure 45) to act on the incoming audit event. The following section gives details on each rule and the number of infections observed during the ransomware simulation run.

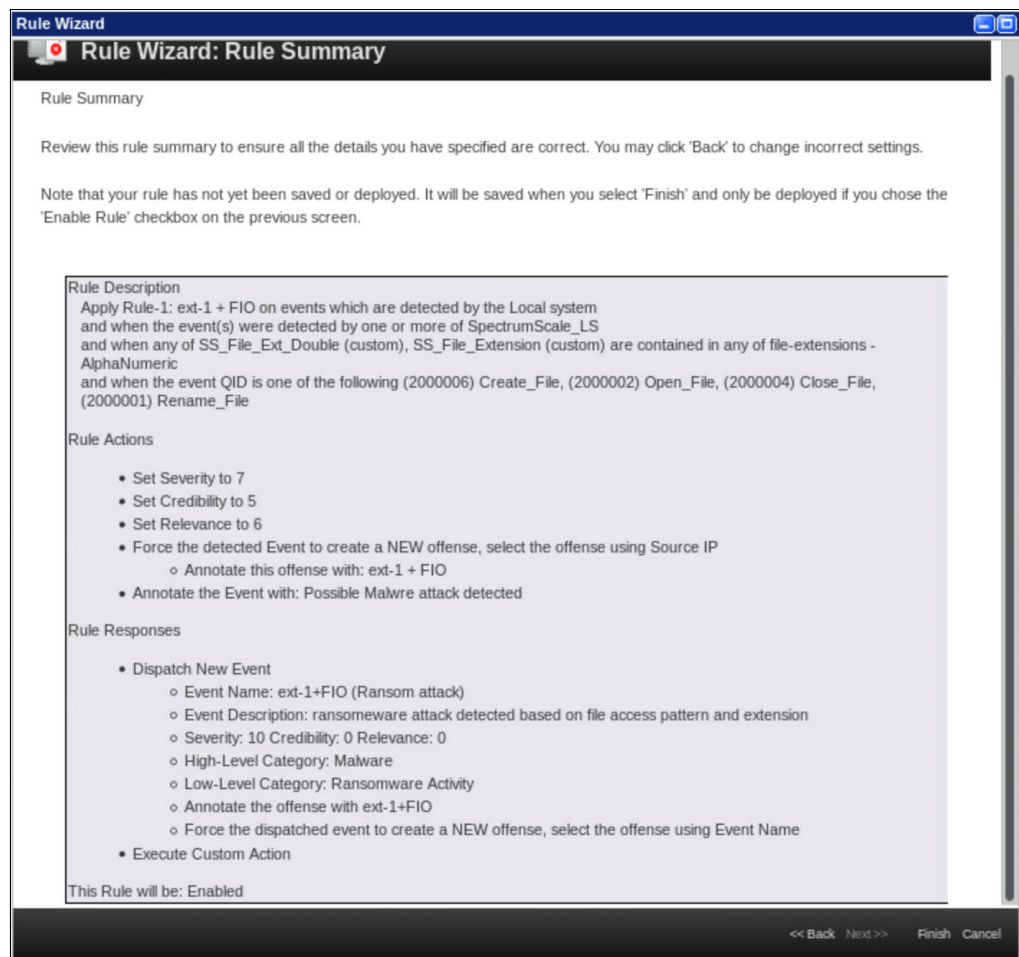


Figure 45 Sample rule based on the file extension and File I/O event

This rule resulted in 2 file system snapshots on IBM Spectrum Scale during the simulation run as a result of the configured custom action. The analysis of both snapshots (Figure 46 and Figure 47) showed the following results.

Although only a one-minute interval exists between 2 snapshots, we see a considerable change in the number of infected files in the later snapshot. The charts below show the number of infected files against each test directory's total number of files. During the simulation run, it is observed that the tests run in parallel, and do not follow the sequence. So when the first snapshot occurs, there could be cases that some tests were not started.

The initial snapshot itself highlights the importance of early threat detection and response. Comparison of two snapshots (Figure 46 and Figure 47) shows that even though the first snapshot could not save all the files, it still managed to save a considerable number of files, thereby reducing the time for restoring these files from backup.

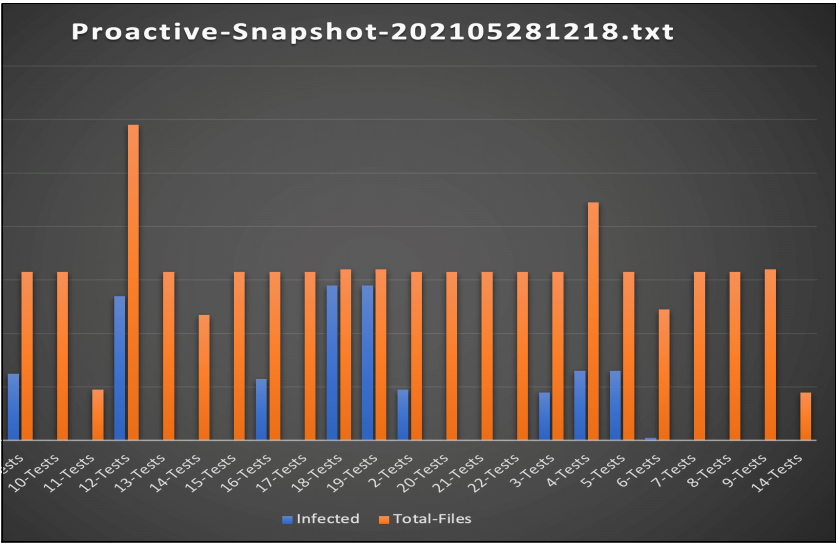


Figure 46 IBM Spectrum Scale snapshot 1

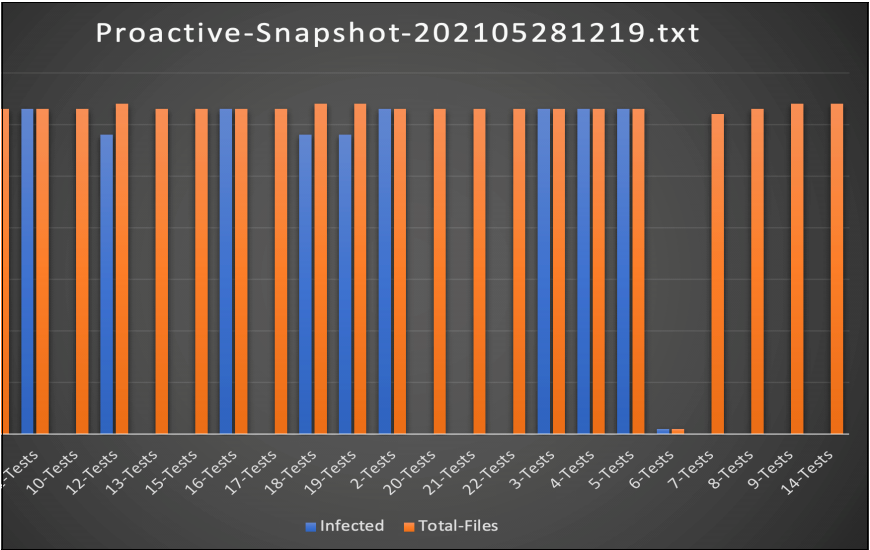


Figure 47 IBM Spectrum Scale snapshot 2

More sample rules are listed in “Appendix B: Sample IBM QRadar rules based on file access pattern or file extensions” on page 52. These rules can act as templates upon which more enrichments can be added by the organization security team.

In addition to the extension check described above, an additional check based on Linux *file* utility can also be added to the custom action to reduce *false positives*. The **file** command tests each argument in an attempt to classify it. There are three sets of tests performed in this order: file system tests, magic tests, and language tests. The first test that succeeds causes the file type to be printed. However, the **file** command cannot categorize certain valid binary files such as certificates. As the contents from such files cannot be understood, they are shown as data. Such behavior can lead to false positives or incorrect classification. A sample output of **file** command on several files is shown in Example 14.

Example 14 Sample output of file command on several files

```
[root@scale-node-01 TestData]# file *
CNSA Install Procedure.txt:      ASCII text
CP4MCMRoadmapVision2020.pptx:    Microsoft PowerPoint 2007+
DSC_9174.JPG:                    JPEG image data, EXIF standard
FOSDEM2021-COSI-CSI-RedHat.pdf:  PDF document, version 1.6
Huzefa.mp4:                      ISO Media, MPEG v4 system, version 2
IBM-COS-Deployment-Steps.pptx:    Microsoft PowerPoint 2007+
IMG_20170905_185208325.jpg:      JPEG image data, JFIF standard 1.01
IMG_2064.JPG:                    JPEG image data, EXIF standard 2.21
Kaustubh.mp4:                    ISO Media, MPEG v4 system, version 2
Kedar.mp4:                       ISO Media, MPEG v4 system, version 2
Mandar.mp4:                      ISO Media, MPEG v4 system, version 2
OpenWorld-2017-Collage.jpg:      JPEG image data, JFIF standard 1.01
Prashant.mp4:                    ISO Media, MPEG v4 system, version 2
ReeteshSurjani[11_0].docx:       Microsoft Word 2007+
Roadmap-2020.xlsx:              Microsoft Excel 2007+
Rsync Process - Jazz Cash.docx:  Microsoft Word 2007+
Sandeep-P.mp4:                  ISO Media, MPEG v4 system, version 2
ShashankKumar[10_0] (1).docx:    Microsoft Word 2007+
Social MediaApps Usage.docx:    Microsoft Word 2007+
Spectrum_Scale-HEPIX_V1a.pdf:    PDF document, version 1.4
Workout at home.pdf:            PDF document, version 1.3
abc.pdf:                        PDF document, version 1.4
cos.pptx:                       Microsoft PowerPoint 2007+
docu1.docx:                     Microsoft Word 2007+
docu2.docx:                     Microsoft Word 2007+
docu3.docx:                     Microsoft Word 2007+
hours.xlsx:                     Microsoft Excel 2007+
im10.png:                       PNG image data, 280 x 280, 8-bit/color RGBA,
non-interlaced
im11.png:                       PNG image data, 280 x 280, 8-bit/color RGBA,
non-interlaced
im12.png:                       PNG image data, 280 x 280, 8-bit/color RGBA,
non-interlaced
image (1).png:                  PNG image data, 1157 x 907, 8-bit/color RGBA,
non-interlaced
image.png:                      PNG image data, 985 x 33, 8-bit/color RGBA,
non-interlaced
pict10.jpg:                     JPEG image data, JFIF standard 1.01
pict11.jpg:                     JPEG image data, JFIF standard 1.01
pict12.jpg:                     JPEG image data, JFIF standard 1.01
pict20.jpg:                     JPEG image data, JFIF standard 1.01
pict21.jpg:                     JPEG image data, JFIF standard 1.01
pict22.jpg:                     JPEG image data, JFIF standard 1.01
pict30.jpg:                     JPEG image data, JFIF standard 1.01
```

pict31.jpg:	JPEG image data, JFIF standard 1.01
pict32.jpg:	JPEG image data, JFIF standard 1.01
voting.docs:	Microsoft Word 2007+

“Appendix C: Sample script for basic check on file type” on page 53 shows the code snippet that can be added to the existing “proactive_snapshot.py” in order to perform an additional check using the **file** command.

Note: If you plan to use **file** command, SSH access is required for the IBM Spectrum Scale cluster and the SSH user must have correct permissions to read the file from specific fileset/file system.

Supported platforms

This solution is applicable to all supported platforms by IBM Spectrum Scale where IBM File Audit logging is supported. This includes IBM Spectrum Scale on x86 architecture and IBM Power systems.

Conclusion

This paper demonstrated the integration of IBM Spectrum Scale File Audit Logs with IBM QRadar and described how they can be used for threat detection and prevention to safeguard the data that is hosted on an IBM Spectrum Scale system. An integrated deployment helps security administrators to correlate file access logs with other logs and events. These events from other network devices, servers, and applications assist security officers to discover potential threat vectors and take the required mitigation actions.

Overall, this function improves the cybersecurity posture of the deployment. In addition, consolidating audit logs in a centralized SIEM, such as IBM QRadar, helps security auditors ensure and validate business compliance to various applicable regulations.

The examples in this paper were simplified to provide a better understanding of using log analysis and the correlation of events and network flows for actionable intelligence. With these tools, threat detection can be much more advanced to suit your business requirements and audit requirements. In addition, you can identify potential threats, including complex, low, and slow cyberattacks or malicious use.

Notice: Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation (GDPR) and other compliances. Clients are solely responsible for obtaining the advice of competent legal counsel. This advice should include the identification and interpretation of any relevant laws and regulations that may affect the clients’ business, and any actions that the clients might need to take to comply with such laws and regulations.

The products, services, and other capabilities that are described here are not suitable for all client situations and might have restricted availability. IBM does not provide legal, accounting, or auditing advice, or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation or full proof against cyber threats.

Appendix A: Custom script to take a snapshot

Example 15 is a sample Python script that uses the IBM Spectrum Scale REST API to take a snapshot of a file system.

Example 15 Sample Python script that uses the IBM Spectrum Scale REST API to take a file system snapshot

```
# This script takes four arguments to take a file system snapshot:
# endpoint = IP address of remote IBM Spectrum Scale server.
# username = user name of remote IBM Spectrum Scale server.
# password = Password of remote IBM Spectrum Scale server.
# device = file system name of remote IBM Spectrum Scale server.
# For example:
# $ python proactive_snapshot.py <IP address of the Spectrum Scale Admin node> <admin_user> <password> <filesystem name>

import argparse
import json
import requests
import time
import urllib3
urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

def main():
    parser = argparse.ArgumentParser(description='Request proactive snapshot.')
    parser.add_argument("endpoint", action="store", help="Endpoint Name")
    parser.add_argument("username", action="store", help="User Name")
    parser.add_argument("password", action="store", help="Password")
    parser.add_argument("device", action="store", help="Device Name")

    args = parser.parse_args()

    endpoint = args.endpoint
    username = args.username
    password = args.password
    device = args.device

    url = ("/".join([endpoint, "scalemgmt", "v2", "filesystems", device,
                    "snapshots"]))
    headers = {'content-type': 'application/json'}
    snapshot_name = "Proactive-Snapshot-" + time.strftime('%Y%m%d%H%M')
    payload = {'snapshotName': snapshot_name}
    json_data = json.dumps(payload)

    response = None
    try:
        response = requests.post(url, auth=(username, password), verify=False,
                                data=json_data, headers=headers)
        if response.status_code == 202:
            print('Snapshot successful')
        else:
            print('Snapshot unsuccessful')
            print(response.status_code)
            print(response.content)
            print(response)
    except Exception as e:
        print('Something went wrong. Last Command: '
              'requests.post({0}, auth=({1}, {2}), verify=False, '
              'data=json.dumps(json_data), '
              'headers={3})'.format(url, username, password, headers))
        print(e)

if __name__ == "__main__":
    main()
```

Note: This script is provided as a sample. Customers are expected to create a script that meets their requirements.

Appendix B: Sample IBM QRadar rules based on file access pattern or file extensions

This appendix describes sample IBM QRadar rules that are based on file access patterns or file extensions. The following rules are based on conditions that are met:

► Apply Rule-2

SQ_Locky on events that are detected by the Local system when:

- The events were detected by one or more of SpectrumScale_LS.
- The event QID is one of the following items:
 - (58750276) Rename/Move Location
 - (2000006) Create_File
 - (2000002) Open_File
 - (2000004) Close_File
 - (39000456) Delete File(s)
 - (2000008) Remove_directory
- At least 50 events are seen with the same SS_Inode (custom) in 1 minute.

► Apply Rule-3

ext-2 on events that are detected by the Local system when:

- The events were detected by one or more of SpectrumScale_LS.
- The event QID is one of the following items:
 - (2000006) Create_File
 - (2000002) Open_File
 - (2000004) Close_File
 - (39000468) Delete File(s)
 - (2000001) Rename_File
- Any of SS_File_Extension (custom) or SS_File_Ext_Double (custom) are contained in any of file-extensions - AlphaNumeric.
- At least three events are seen with the same SS_Inode (custom) in 1 minute.

► Apply Rule-4

ext-3 on events that are detected by the Local system and when:

- The events were detected by one or more of SpectrumScale_LS.
- Any of SS_File_Extension (custom) or SS_File_Ext_Double (custom) are contained in any of file-extensions - AlphaNumeric.
- At least three events are seen with the same SS_File_Ext_Double (custom) or SS_File_Extension (custom) in 1 minute.

Appendix C: Sample script for basic check on file type

This code snippet performs a basic check by using the `file` command to determine the file type. The following function (Example 16) can be added to the existing `proactive_snapshot.py` script that is shown in this paper. The function is invoked by passing a single argument containing a full path to a file. The function uses the `subprocess` module to run the `file` command on the argument file. The resulting output is separated by using the Python-provided `split` function. The resulting `filetype` contains only two values: data or known file type. The known file types are described in Example 13 on page 43. When the `filetype` is seen as data, the function returns a true value.

Example 16 Basic check by using the file command to determine the file type

```
def isdataFileType( argfile ):
    """
        This function is written to check whether the output of the file command is "data"

        Input Parameters:
            1. argfile - This argument contains the full path of file on Spectrum Scale
export

        Return values:
            - boolean True/False depending on whether the output contains "data" keyword
    """
    1stCmd = []

    1stCmd.append("/usr/bin/file")
    1stCmd.append(argfile)

    output = subprocess.Popen( 1stCmd,
                               shell = False,
                               stdout = subprocess.PIPE,
                               stderr = subprocess.PIPE )

    stdout,stderr = output.communicate()

    if stderr != "":
        print("Error occured !!\nDetails:\n{0}" . format(stderr) )
        sys.exit(1)

    if stdout != "":

        lines = stdout.strip().split("\n")
        line = stdout.strip()

        filename,filetype = line.split(":")

        if filetype.strip() == 'data':
            print("Possible infection detected !!")
            return True
        else:
            print("{0}".format(line))
            return False
```

When the result of the function is combined with the I/O pattern and extension rule that is defined in QRadar, the file can now be identified as a ransomware infected object with relatively increased confidence, which reduces false positives.

Note: Using the `file` command is an incremental improvement over the above solution.

Appendix D: Sample list of known ransomware file extensions

Table 1 shows both ransomware extensions and their descriptions. The team loaded only the extension part of the table into QRadar.

Note: This is a indicative, but not comprehensive, list. There might be many variants of ransomware whose extensions are not listed below or work in a manner where no extension is created.

Table 1 Ransomware extensions considered

Extension	Description
micro	TeslaCrypt 3.0 ransomware encrypted data
zepto	Locky ransomware affected data
locky	Locky ransomware affected data
cerber	Cerber ransomware affected data
cerber3	Cerber 3 ransomware affected data
cryp1	CryptXXX ransomware affected data
mole	CryptoMix (variant) ransomware affected data
onion	Dharma ransomware affected data
axx	AxCrypt encrypted data
osiris	Locky (variant) ransomware affected data
crypz	CryptXXX ransomware affected data
crypt	Scatter ransomware affected data
locked	Various ransomware affected data
odin	Locky ransomware affected file
ccc	TeslaCrypt or Cryptowall encrypted data
cerber2	Cerber 2 ransomware affected file
sage	Sage ransomware affected data
globe	Globe ransomware affected file
exx	Alpha Crypt encrypted file
good	Scatter ransomware affected file
wallet	Globe 3 (variant) ransomware affected file
1txt	Enigma ransomware affected file
decrypt2017	Globe 3 ransomware affected file
encrypt	Alpha ransomware affected file

Extension	Description
eZZ	Alpha Crypt virus encrypted data
zzzzz	Locky ransomware affected file
MERRY	Merry X-Mas ransomware affected file
enciphered	Malware (ransomware) encoded file
r5a	7ev3n ransomware affected file
aesir	Locky ransomware affected file
ecc	Cryptolocker or TeslaCrypt virus encrypted file
enigma	Covertion ransomware affected file
cryptowall	Encrypted file by Cryptowall ransomware
encrypted	Various ransomware affected file
loli	LOLI RanSomeWare ransomware affected file
breaking_bad	Files1147@gmail(.)com ransomware affected file
coded	Anubis ransomware affected file
ha3	EI-Polocker affected file
damage	Damage ransomware affected file
wcry	WannaCry ransomware affected file
lol!	GPCode ransomware affected file
cryptolocker	CryptoLocker encrypted file
dharma	CrySiS ransomware affected file
MRCR1	Merry X-Mas ransomware affected file
sexy	PayDay ransomware affected files
crjoker	CryptoJoker ransomware affected file
fantom	Fantom ransomware affected file
keybtc@inbox_com	KeyBTC ransomware affected file
rrk	Radamant v2 ransomware affected file
legion	Legion ransomware affected file
kratos	KratosCrypt ransomware affected file
LeChiffre	LeChiffre ransomware affected file
kraken	Rakhni ransomware affected file
zcrypt	ZCRYPT ransomware affected file
maya	HiddenTear (variant) ransomware affected file
enc	TorrentLocker ransomware affected file
file0locked	Evil ransomware affected file
crinf	DecryptorMax or CryptInfinite ransomware affected file

Extension	Description
serp	Serpent (variant) ransomware affected file
potato	Potato ransomware affected file
ytbl	Troldesh (variant) ransomware affected file
surprise	Surprise ransomware affected file
angelamerkel	Angela Merkel ransomware affected file
Windows10	Shade ransomware affected file
lesli	CryptoMix ransomware affected file
serpent	Serpent ransomware affected file
PEGS1	Merry X-Mas ransomware affected file
dale	Chip ransomware affected file
pdcr	PadCrypt Ransomware script
zzz	TeslaCrypt ransomware encrypted file
xyz	TeslaCrypt ransomware encrypted file
1cbu1	Princess Locker ransomware affected file
venusf	Venus Locker ransomware affected file
coverton	Coverton ransomware affected file
thor	Locky ransomware affected file
rnsmr	Gremit ransomware affected file
evillock	Evil-JS (variant) ransomware affected file
R16m01d05	Ransomware affected data
wflx	WildFire ransomware affected file
nuclear55	Nuke ransomware affected file
darkness	Rakhni ransomware affected file
encl	FileLocker ransomware affected file
rekt	HiddenTear (variant) ransomware affected file
kernel_time	KeRanger OS X ransomware
zyklon	ZYKLON ransomware affected file
Dexter	Troldesh (variant) ransomware affected file
locklock	LockLock ransomware affected file
cry	CryLocker ransomware affected file
VforVendetta	Samsam (variant) ransomware affected file
btc	Jigsaw Ransomware affected file
raid10	Globe [variant] ransomware affected file
dCrypt	DummyLocker ransomware affected file

Extension	Description
zorro	Zorro ransomware affected file
AngleWare	HiddenTear/MafiaWare (variant) ransomware affected file
EnCiPhErEd	Xorist Ransomware affected file
purge	Globe ransomware affected file
realfs0ciety@sigaint.org.fs0ciety	FSociety ransomware affected file
shit	Locky ransomware affected file
atlas	Atlas ransomware affected file
exotic	Exotic ransomware affected file
crypted	Nemucod ransomware affected file
padcrypt	PadCrypt ransomware affected file
xxx	TeslaCrypt 3.0 ransomware encrypted file
hush	Jigsaw ransomware affected file
bin	Alpha/Alfa ransomware affected file
vbransom	VBRansom 7 ransomware affected file
RMCM1	Merry X-Mas ransomware affected file
cryeye	DoubleLocker ransomware affected data
unavailable	AI-Namrood ransomware affected file
braincrypt	Braincrypt ransomware affected file
fucked	Manifestus ransomware affected file
crypte	Jigsaw (variant) ransomware affected file
_AiraCropEncrypted	AiraCrop Ransomware affected file
stn	Satan ransomware affected file
paym	Jigsaw Ransomware affected file
spora	Spora ransomware affected file
dll	FSociety ransomware affected file
RARE1	Merry X-Mas ransomware affected file
alcatraz	Alcatraz Locker ransomware affected file
pzdc	Scatter ransomware affected file
aaa	TeslaCrypt ransomware encrypted file
ttt	TeslaCrypt 3.0 ransomware encrypted file
odcodc	ODCODC ransomware affected file
vvv	TeslaCrypt 3.0 ransomware encrypted file
ruby	Ruby ransomware affected file
pays	Jigsaw Ransomware affected file

Extension	Description
comrade	Comrade ransomware affected file
enc	Cryptorium ransomware affected file
abc	TeslaCrypt ransomware encrypted file
xxx	help_dcfile ransomware affected file
antihacker2017	Xorist (variant) Ransomware affected file
herbst	Herbst ransomware affected file
szf	SZFLocker ransomware affected file
rekt	RektLocker ransomware affected file
bript	BadEncryptor ransomware affected file
crptrgr	CryptoRoger ransomware affected file
kkk	Jigsaw Ransomware affected file
rdm	Radamant ransomware affected file
BarRax	BarRax (HiddenTear variant) ransomware affected file
vindows	Vindows Locker ransomware affected file
helpmeencedfiles	Samas/SamSam ransomware affected file
hnumkhotep	Globe 3 ransomware affected file
CCCRRRPPP	Unlock92 ransomware affected file
kyra	Globe ransomware affected file
fun	Jigsaw Ransomware affected file
rip	KillLocker ransomware affected file
73i87A	Xorist Ransomware affected file
bitstak	Bitstak ransomware affected file
kernel_complete	KeRanger OS X ransomware file
payrms	Jigsaw Ransomware affected file
a5zfn	Alma Locker ransomware affected file
perl	Bart ransomware affected file
noproblemwedecfiles	Samas/SamSam ransomware affected file
lcked	Jigsaw (variant) ransomware affected file
p5tkjw	Xorist Ransomware affected file
paymst	Jigsaw Ransomware affected file
magic	Magic ransomware affected file
payms	Jigsaw Ransomware affected file
d4nk	PyL33T ransomware affected file
SecureCrypted	Apocalypse ransomware affected file

Extension	Description
paymts	Jigsaw Ransomware affected file
kostya	Kostya ransomware affected file
lovewindows	Globe (variant) ransomware affected file
madebyadam	Roga ransomware affected file
powerfulldecrypt	Samas/SamSam ransomware affected file
gefickt	Jigsaw (variant) ransomware affected file
kernel_pid	KeRanger OS X ransomware file
ifuckedyou	SerbRansom ransomware affected file
grt	Karmen HiddenTear (variant) ransomware affected file
conficker	Conficker ransomware affected file
edgel	EdgeLocker ransomware affected file
PoAr2w	Xorist Ransomware affected file
oops	Marlboro ransomware affected file
adk	Angry Duck ransomware affected file
encrypted	KeRanger OS X or Donald Trum ransomware affected file
Whereisyourfiles	Samas/SamSam ransomware affected file
czvxce	Coverton ransomware affected file
theworldisyours	Samas/SamSam ransomware affected file
info	PizzaCrypts Ransomware affected file
razy	Razy ransomware affected file
rmd	Zeta ransomware affected file
fun	Jigsaw (variant) ransomware affected file
kimcilware	KimcilWare ransomware affected file
paymrss	DXXD ransomware affected file
pec	PEC 2017 ransomware affected file
rokku	Rokku ransomware affected file
lock93	Lock93 ransomware affected file
vxlock	vxLock ransomware affected file
pubg	PUBG ransomware affected data
wk	WeakCryptor
exe	Virlock variant ransomware
ppr	Strong Cryptor Net
ksr	Strong Cryptor Fast
ark	Strong Cryptor

Extension	Description
art	Streamer
xapgdof	Slow Cryptor

References

- ▶ Bolstering Cyber Resiliency with threat detection
<https://www.ibm.com/downloads/cas/V0J907RG>
- ▶ IBM QRadar: DSM Editor overview
<https://www.ibm.com/docs/en/qsip/7.4?topic=qradar-dsm-editor-overview>
- ▶ IBM QRadar: QID map overview (`qidmap_cli.sh` script)
<https://www.ibm.com/docs/en/qsip/7.4?topic=configuration-qid-map-overview>
- ▶ IBM QRadar Security Intelligence Platform documentation
<https://www.ibm.com/docs/en/qsip>
- ▶ IBM QRadar SIEM 7.4.3 documentation
https://www.ibm.com/docs/en/qsip/7.4?topic=SS42VS_7.4/com.ibm.qradar.doc/c_qradar_pdfs.html
- ▶ IBM QRadar Tuning Guide
https://www.ibm.com/docs/en/SS42VS_7.4/pdf/b_qradar_tuning_guide.pdf
- ▶ IBM QRadar: User Behavior Analytics (UBA)
<https://exchange.xforce.ibmcloud.com/hub/extension/IBMQRadar:UserBehaviorAnalytics>
- ▶ IBM QRadar white paper
<https://www.ibm.com/downloads/cas/G6E26E3J>
- ▶ *IBM Spectrum Scale Functionality to Support GDPR Requirements*, REDP-5489
- ▶ IBM Spectrum Scale on IBM Documentation
<https://www.ibm.com/docs/en/spectrum-scale>
- ▶ *IBM Spectrum Scale and IBM StoredIQ: Identifying and securing your business data to support regulatory requirements*, REDP-5525
- ▶ *IBM Spectrum Scale Immutability Introduction, Configuration Guidance, and Use Cases*, REDP-5507
- ▶ *IBM Spectrum Scale Security*, REDP-5426
- ▶ Red Hat Enterprise Linux: Basic Configuration of Rsyslog
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/deployment_guide/s1-basic_configuration_of_rsyslog
- ▶ Rsyslog documentation
<https://www.rsyslog.com/doc/master/index.html>

Authors

This paper was produced by a team of specialists from around the world.

Boudhayan Chakrabarty (Bob) is a SIEM Specialist at IBM India Software Labs, specializing in Security Intelligence and Compliance. With more than 11 years of practical experience with different Security Operations Center (SOC) and SIEM solutions, he has been the author of many white papers and IBM Redbooks® publications. He has also been conducting training and webcasts in this field. He has contributed to many international deployments, from the RFP phase, the Proof of Concept phase, and to the ultimate deployment for and training of the customer. He has designed architectures for different customer SOC centers by using IBM solutions, and is a subject matter expert for (SME) for Security Intelligence and Compliance.

Sandeep R Patil is a Senior Technical Staff Member who works as a Storage Architect with IBM System Labs. He has over 18 years of product architecture and design experience. Sandeep is an IBM Master Inventor, an IBM developerWorks® Master Author, and a member of the IBM® Academy of Technology. Sandeep holds a Bachelor of Engineering (Computer Science) degree from the University of Pune, India.

Shashank Shingornikar is a Storage Solutions Architect with IBM Systems, ISDL Lab Pune, India, for the past 12+ years. He has worked extensively with IBM Storage products such as Spectrum Virtualize / FlashSystems, Spectrum Scale building solutions combining Oracle, Red Hat OpenShift features. Currently he is working on demonstrating Cyber resilience solutions with IBM QRadar and IBM Storage Systems. Before joining IBM, Shashank has worked in The Netherlands on various HA/DR/Cluster/Replication solutions for database technologies such as Oracle / MSSQL / MySQL.

Ashish Kothekar is a Cybersecurity Consultant with IBM. He has worked on Monitoring and Intrusion Prevention solutions and is working on SIEM and SOAR solutions. He has been actively involved in deploying, upgrading, and managing SIEM and SOAR solutions for customers in the Asia Pacific region. He is an active speaker and has presented various security topics as part of the University Initiative by IBM.

Praphullachandra Mujumdar is a Security Specialist at IBM India Software Labs. With 14 years of experience in the IBM Security™ Domain, he has worked with different solutions, including IBM Security Federated Identity Manager and IBM Security Access Manager solutions for e-business. His knowledge extends from Identity and Access Management Solutions to SIEM solutions. He provides technical support to customers worldwide, and has delivered multiple webcasts in the SIEM domain.

Smita Raut is an Advisory Software Engineer with IBM Storage Labs in Pune, India. She works with the IBM Spectrum® Scale development team on object protocol support. In her 6 years with IBM, she has worked on various products, such as IBM Scale Out Network Attached Storage and IBM V7000 Unified. She has an overall industry experience of 15 years with organizations, such as Persistent Systems, TIBCO Inc., and BMC Software.

Digvijay Ukirde is a Software Developer with IBM Storage Labs in Pune, India. He has been working with IBM for the last 5 years on IBM Spectrum Scale. He specializes in DevOps solutions for storage components for private and public clouds. Digvijay holds a Master in Technology (Computer Science) from Mumbai University.

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

Larry Coyne
IBM Redbooks, Tucson Center

Vincent Hsu, Julio Cesar Hernandez, Erin Farr, Helen C Fischer, Pushkaraj B Thorat, Mandar J Vaidya, John Olson, Luis I Teran
IBM Systems

Sridhar Muppidi, Adam Frank, Prateek Jain, Shreya Mishra, Sheona Sinha
IBM Security

Now you can become a published author, too

Here's an opportunity to spotlight your skills, grow your career, and become a published author, all at the same time. Join an IBM Redbooks residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run 2 - 6 weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online:

ibm.com/redbooks/residencies.html

Stay connected to IBM Redbooks

- ▶ Look for us on LinkedIn:
<http://www.linkedin.com/groups?home=&gid=2130806>
- ▶ Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:
<https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm>
- ▶ Stay current on recent Redbooks publications with RSS Feeds:
<http://www.redbooks.ibm.com/rss.html>

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®
developerWorks®
IBM®
IBM Cloud®

IBM Elastic Storage®
IBM Security™
IBM Spectrum®
IBM Watson®

IBM Z®
QRadar®
Redbooks®
Redbooks (logo) ®

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.

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



REDP-5560-02

ISBN 073846001x

Printed in U.S.A.

Get connected

