

IBM® Storage

Securing IBM Spectrum Scale with IBM QRadar and IBM Cloud Pak for Security

IBM Storage Team



© Copyright International Business Machines Corporation 2021.

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

Contents

About this document	1
Executive summary	2
Scope	3
Use case	4
Tracking an internal threat actor	4
Origin of malware	4
Unified Data Foundation overview	5
Lab architecture	6
Lab setup	7
Configuring LDAP for CP4S users	7
Configuring domain name for CP4S	8
Configuring required TLS certificates for CP4S	9
Configuring CP4S on IBM Spectrum SCALE CNSA, StorageClass	10
Deploying CP4S 1.7	11
Configuring the identity provider (LDAP) with CP4S	13
Configuring QRadar with LDAP	16
Integrating IBM CP4S with IBM QRadar	18
Integrating IBM CP4S with IBM QRadar, Proxy	22
Enabling IBM Spectrum Scale logs forwarding	23
Configuring IBM Spectrum Scale log source in QRadar	24
Configuring IBM QRadar SOAR Plugin	31
Defining a reference set in QRadar	32
Defining rules in QRadar	34
Demonstration use case	37
Summary	40
Appendix A	40
Appendix B	41
About the author	43
Acknowledgments	43
Notices	45
Trademarks	46
Terms and conditions for product documentation	47
Applicability	47
Commercial use	47
Rights	47
Privacy policy considerations	47



About this document

Cyberattacks are likely to remain a significant risk for the foreseeable future. Attacks on organizations can be external and internal. Investing in technology and processes to prevent these cyberattacks is the highest priority for these organizations. Organizations need well-designed procedures and processes to recover from attacks.

The focus of this document is to demonstrate how the IBM® Unified Data Foundation (UDF) infrastructure plays an important role in delivering the persistence storage (PV) to containerized applications, such as IBM Cloud® Pak for Security (CP4S), with IBM Spectrum® Scale Container Native Storage Access (CNSA) that is deployed with IBM Spectrum scale CSI driver and IBM FlashSystem® storage with IBM Block storage driver with CSI driver. Also demonstrated is how this UDF infrastructure can be used as a preferred storage class to create back-end persistent storage for CP4S deployments.

We also highlight how the file I/O events are captured in IBM QRadar® and offenses are generated based on predefined rules. After the offenses are generated, we show how the cases are automatically generated in IBM Cloud Pak® for Security by using the IBM QRadar SOAR Plugin, with a manually automated method to log a case in IBM Cloud Pak for Security.

This document also describes the processes that are required for the configuration and integration of the components in this solution, such as:

- Integration of IBM Spectrum Scale with QRadar
- QRadar integration with IBM Cloud Pak for Security
- Integration of the IBM QRadar SOAR Plugin to generate automated cases in CP4S.

Finally, this document shows the use of IBM Spectrum Scale CNSA and IBM FlashSystem storage that uses IBM block CSI driver to provision persistent volumes for CP4S deployment. All models of IBM FlashSystem family are supported by this document, including:

- FlashSystem 9100 and 9200
- FlashSystem 7200 and FlashSystem 5000 models
- FlashSystem 5200
- IBM SAN Volume Controller
- All storage that is running IBM Spectrum Virtualize software

For more information about supported models, see the following resources:

- [This GitHub web page](#)
- [IBM Spectrum Scale Container Native Storage Access 5.1.0.3](#)
- [IBM Documentation](#)

Executive summary

With IBM Hybrid Cloud and AI solutions, the new generation of hybrid cloud enables you to build and manage applications or solutions across any cloud with a common platform. At IBM, the foundation of this approach is Red Hat OpenShift, which is the market-leading hybrid cloud container platform.

IBM also offers IBM Cloud Pak solutions, which are an AI-infused software portfolio that runs on Red Hat OpenShift. On the Red Hat Hybrid Cloud Platform, IBM delivers a set of six IBM Cloud Paks that each deliver a set of unified, domain-specific software capabilities.

IBM Cloud Pak for Security provides a platform to quickly integrate your security tools and generate deeper insights into threats across hybrid, multi-load environments.

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

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. When this capability is enabled, all of the file access to the file system is logged with the required audit information.

In this solution guide, we integrated, qualified, and documented a step-by-step approach for IBM FlashSystem storage, IBM Spectrum Scale CNSA, IBM Spectrum Scale cluster, and QRadar with CP4S.

By using these products, we built a cyber resiliency solution that demonstrates early threat detection for modification of data that is hosted on IBM Spectrum Scale FlashSystems by internal threat actors or a malware attack.

Scope

The scope of this document is to use IBM FlashSystem storage and IBM Spectrum Scale CNSA storage class as the storage persistence volumes requirement for a CP4S application in the Red Hat OpenShift container platform.

The document focuses on how to provision persistence storage from IBM Spectrum Scale CNSA or IBM Storage Block CSI by using “StorageClass” for CP4S application.

Also discussed is how to configure prerequisites for CP4S application deployment and configure a connector for QRadar to fetch data from connectors to CP4S applications.

Finally, this document describes how the file I/O events are captured in QRadar and offenses are generated based on defined rules. As a prerequisite, IBM Spectrum Scale file auditing must be enabled so that the file I/O audit events are generated. The setup also requires rsyslog to be configured to forward the events to QRadar.

This document does *not* discuss the installation of the following products:

- IBM Spectrum Scale CNSA
- IBM storage block CSI driver
- OCP
- QRadar

It is assumed that the reader has a basic understanding of Red Hat OpenShift, IBM Spectrum Scale, IBM QRadar, IBM Cloud Pak for Security, and LDAP.

All the steps that are described in this document are specific to demonstrating the use case and set up that was done in our lab and are restricted to the demonstration set-up. You might need to design your own example per your requirements.

Use case

The sample use case in this section is demonstrated as part of Cyber Resiliency workflow.

Tracking an internal threat actor

Although suitable permissions are defined at storage system, nothing stops a curious user or a threat actor from accessing the data that is available on the system, irrespective of access level.

Write permissions might be prohibited in specific cases, but users might still be able to view the contents of the file. Such incidents can result in stealing the information from the system.

To track such activities, the Spectrum Scale audit logging feature is an invaluable tool. By combining the audit logging capabilities of Spectrum Scale with IBM QRadar, a sophisticated monitoring mechanism can be set up to trace the threat actors.

Origin of malware

The nature of the malware or ransomware infection is to make the data inaccessible to the user for financial gains. After the infection begins, it rapidly spreads across the system to corrupt as many files as it can find.

Here too, by combining the file auditing capabilities of IBM Spectrum Scale and IBM QRadar, the malware or ransomware activity can be detected by analyzing the audit events. After such infection is detected, a file system-level snapshot can be started to protect the maximum amount of data, which limits the effect of infection by quickly restoring the infected files.

This sample use case can be further extended based on the organizations needs.

IBM Cloud Pak for Security provides sophisticated integration with AD/LDAP and provides the means to run automated workflow execution by using Ansible automation. This automation helps isolate and evict the device in question to curtail the spread of infection.

IBM QRadar also can run custom actions to facilitate response in automated manner.

Unified Data Foundation overview

IBM UDF is a reference architecture and framework (see Figure 1) that accelerates the adoption of hybrid cloud and AI platforms by providing a container-native or container-ready data service or foundation. This foundation is based on IBM and Red Hat software-defined storage tools and solutions

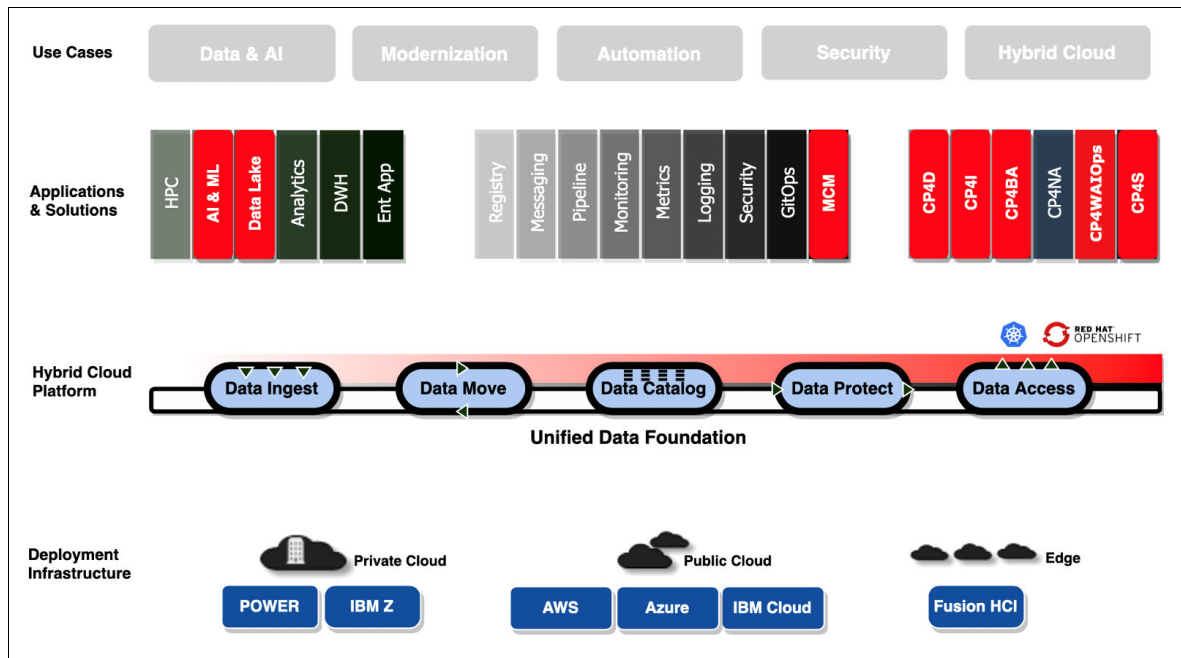


Figure 1 UDF reference architecture and framework

The use cases that are shown at the top of Figure 1 can be implemented by (but not limited to) applications and solutions that are shown in Figure 1. The data needs of these applications and solutions are catered by the Unified Data Foundation layer by using various functions, such as ingest, move, catalog, protect, and access. These UDF functions play a vital role as the application deployment can be a public or hybrid cloud model.

Lab architecture

As shown in Figure 2, the lab setup is orchestrated in an VMware environment with Red Hat Red Hat OpenShift 4.6 installed with the IPI method. It is assumed that Red Hat OpenShift 4.6+ with three master nodes and five CoreOS worker nodes is installed. For more information about prerequisites, see this [IBM Documentation web page](#).

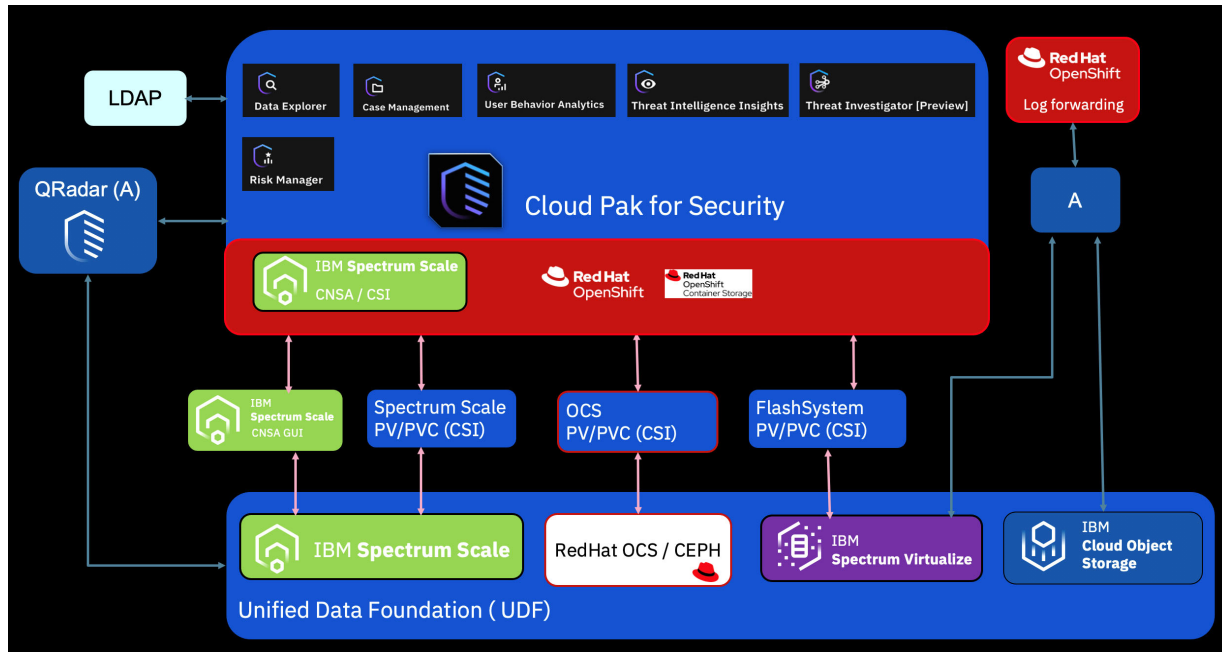


Figure 2 Lab setup

Ensure that you can access a DNS server (or can request a DNS server) to update the application domain name configuration that is required for CP4S. For more information, see this [IBM Documentation web page](#).

In this lab setup, the architecture shows that CP4S is deployed on the IBM® Spectrum Scale CNSA storage class.

Ensure that you can access an LDAP to configure users and groups and integrate LDAP with CP4S. In our lab setup, we used OpenLDAP to integrate with CP4S.

QRadar is used as the data source for CP4S. QRadar also features the log-source that was created for IBM FlashSystem and IBM Spectrum Scale.

Similarly, IBM Spectrum Scale auditing is enabled. How the file I/O events are captured in QRadar and offenses are generated based on defined rules is described. After the offenses are generated, we see how the cases are automatically generated in IBM Cloud® Pak for Security by using the QRadar SOAR Plugin.

With this lab setup, we demonstrate the deployment of CP4S with IBM block storage or IBM Spectrum Scale CNSA storage class. We also provide UDF services to the IBM Cloud Paks.

Lab setup

The document assumes that the following components are installed and configured per best practices:

- Red Hat OpenShift container platform 4.6 + with three master nodes and five CoreOS worker nodes
- IBM QRadar 7.4 + with IBM QRadar SOAR plug-in
- LDAP server (we used Open LDAP)
- IBM Spectrum Scale CNSA cluster with storage class
- IBM Spectrum Scale CNSA cluster with audit enabled
- Red Hat OpenShift client: oc binary
- Package deployment client: helm3
- CP4S configuration client: cloudctl

More domain names cases-rest and cases-stomp are required for working with case management application in CP4S. For more information about the resolution of the domain names, see “Configuring domain name for CP4S” on page 8.

Configuring LDAP for CP4S users

To configure the cpsadmin user in OpenLDAP, which used for logging on to the CP4S application domain, create the cpsadmin group first and then, create the cpsadmin user (see Figure 3).

The screenshot displays two side-by-side configuration windows for LDAP.
Step 1: Add User Group
- **Group name ***: cpsamin
- **Description**: Group for Cloud Pak for Security Admin User
- **Group Type**: Non-POSIX, External, ☒ POSIX
- **GID**: (empty field)
- *** Required field**: indicated by an asterisk next to the group name field.
- **Buttons**: Add, Add and Add Another, Add and Edit, Cancel.
Step 2: Add User
- **User login**: cpsadmin
- **First name ***: cpsadmin
- **Last name ***: cpsadmin
- **Class**: (empty field)
- **No private group**: ☐
- **GID**: 199000049 (dropdown menu)
- **New Password**: (masked with dots)
- **Verify Password**: (masked with dots)
- *** Required field**: indicated by an asterisk next to the first and last name fields.
- **Buttons**: Add, Add and Add Another, Add and Edit, Cancel.

Figure 3 Creating cpsadmin group and cpsadmin user

Configuring domain name for CP4S

This section describes the domain name registration process for CP4S in the DNS configuration in which OCP is hosted. In this lab setup, OCP is deployed by using the IPI method on VMware.

Figure 4 shows the fully qualified domain name (FQDN) use for CP4S. The domain name that is listed here must be resolved when the dnsname lookup is performed. Also, domain names for cases-rest and cases-stomp are registered for the same IP.

```
[root@cluster3-inf bin]#  
[root@cluster3-inf bin]# nslookup cp4s.apps.cluster3.storage-ocp.tuc.stglabs.ibm.com.  
Server:          9.11.221.254  
Address:         9.11.221.254#53  
  
Name:   cp4s.apps.cluster3.storage-ocp.tuc.stglabs.ibm.com  
Address: 9.11.221.36  
  
[root@cluster3-inf bin]# nslookup cases-rest.apps.cluster3.storage-ocp.tuc.stglabs.ibm.com.  
Server:          9.11.221.254  
Address:         9.11.221.254#53  
  
Name:   cases-rest.apps.cluster3.storage-ocp.tuc.stglabs.ibm.com  
Address: 9.11.221.36  
  
[root@cluster3-inf bin]# nslookup cases-stomp.apps.cluster3.storage-ocp.tuc.stglabs.ibm.com.  
Server:          9.11.221.254  
Address:         9.11.221.254#53  
  
Name:   cases-stomp.apps.cluster3.storage-ocp.tuc.stglabs.ibm.com  
Address: 9.11.221.36
```

Figure 4 Fully Qualified Domain Name for CP4S domain

Figure 5 shows the reverse lookup of the FQDN configured for CP4S. Notice the extra domain names (cases-rest and cases-stomp) also are resolved to same IP address.

```
[root@cluster3-inf bin]# nslookup 9.11.221.36  
36.221.11.9.in-addr.arpa    name = cases-rest.apps.cluster3.storage-ocp.tuc.stglabs.ibm.com.  
36.221.11.9.in-addr.arpa    name = apps.cluster3.storage-ocp.tuc.stglabs.ibm.com.  
36.221.11.9.in-addr.arpa    name = cases-stomp.apps.cluster3.storage-ocp.tuc.stglabs.ibm.com.
```

Figure 5 Reverse lookup for CP4S FQDN

Configuring required TLS certificates for CP4S

Complete the following steps to configure the TLS certificates. This sample is a TLS certificate that we created by using openssl that was specific to our CP4S domain (for more information, see this [IBM Documentation web page](#)):

1. Optionally export the SUBJ field that is used when creating the certificate:

```
[root@cluster3-inf] export SUBJ="/CN=cp4s.apps.cluster3.storage-ocp.tuc.stglabs.ibm.com"
```

2. Create the openssl.cfg file (see Figure 6).

```
[root@cluster3-inf TLS]# cat openssl.cfg
[ req ]
distinguished_name = req_distinguished_name
[ req_distinguished_name ]
commonName          = cp4s.apps.cluster3.storage-ocp.tuc.stglabs.ibm.com
commonName_max      = 64
[ v3_ca ]
basicConstraints = critical,CA:TRUE
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer:always
```

Figure 6 Configuring TLS certificate in .cfg file

3. Create a ca.key file:

```
[root@cluster3-inf] openssl genrsa -out ca.key 4096
```

4. Run the **openssl** command to create the required certificate by using the openssl.cfg configuration file and the ca.key file that were generated in step 2 and step 3:

```
[root@cluster3-inf] openssl -req x509 -new -nodes -key ca.key -sha256 -day 390
-config openssl.cfg -extensions v3_ca -subj "${SUBJ}" -out ca.crt
```

5. Create another configuration file (for example, step2-openssl.cfg), as shown in Figure 7.

```
[root@cluster3-inf TLS]# cat step2-openssl.cfg
[req]
req_extensions = req_ext
x509_extensions = usr_cert
distinguished_name = req_name
[ req_name ]
commonName = cp4s.apps.cluster3.storage-ocp.tuc.stglabs.ibm.com
[ usr_cert ]
basicConstraints=CA:FALSE
nsCertType = server
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer
subjectAltName = DNS:cp4s.apps.cluster3.storage-ocp.tuc.stglabs.ibm.com
[ req_ext ]
subjectAltName = DNS:cp4s.apps.cluster3.storage-ocp.tuc.stglabs.ibm.com

[root@cluster3-inf TLS]#

[root@cluster3-inf TLS]# cp step2-openssl.cfg openssl.cfg
cp: overwrite 'openssl.cfg'? y
```

Figure 7 Configure TLS certificate ca.crt file

6. Generate a `tls.key` and PEM formatted `tls.csr`:

```
openssl -req -nodes -newkey rsa:2048 -keyout tls.key -outform PEM -out tls.csr  
-subj ${SUBJ}" \ -config step2-openssl.cfg
```

7. Generate the TLS certificate:

```
openssl -req x509 -sha256 -in tls.csr -out tls.crt.tmp -CA ca.crt -Cakey ca.key  
-CAcreateserial -CAserial ca.serial -days 398 -extensions usr_cert -extfile  
step2-openssl.cfg
```

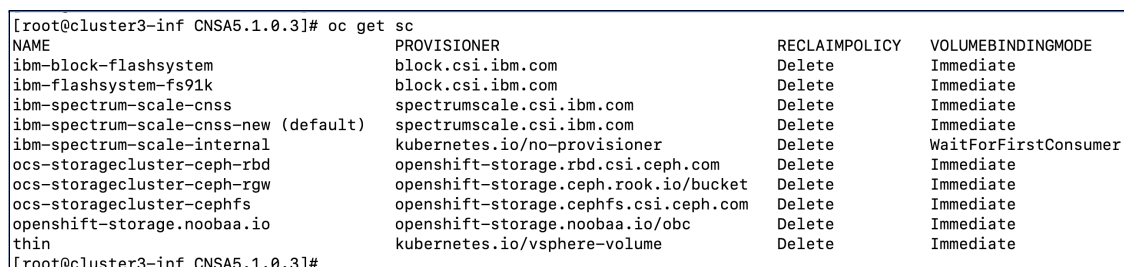
The TLS certificate and domains are used in the `values.conf` file, as listed in “Appendix A” on page 40 and are used while installing CP4S.

Configuring CP4S on IBM Spectrum SCALE CNSA, StorageClass

This section describes installing CP4S 1.7 on the CNSA storage class. It is assumed that required domains (for example, `values.conf`) are now created.

Verify that the CNSA storage cluster and storage class are available and created per the guidelines that are described at this [IBM Documentation web page](#).

Figure 8 shows the CNSA storage class `ibm-spectrum-scale-cnss-new` (default) that is used during the CP4S deployment process.



NAME	PROVISIONER	RECLAIMPOLICY	VOLUMEBINDINGMODE
ibm-block-flashsystem	block.csi.ibm.com	Delete	Immediate
ibm-flashsystem-fs91k	block.csi.ibm.com	Delete	Immediate
ibm-spectrum-scale-cnss	spectrumscale.csi.ibm.com	Delete	Immediate
ibm-spectrum-scale-cnss-new (default)	spectrumscale.csi.ibm.com	Delete	Immediate
ibm-spectrum-scale-internal	kubernetes.io/no-provisioner	Delete	WaitForFirstConsumer
ocs-storagecluster-ceph-rbd	openshift-storage.rbd.csi.ceph.com	Delete	Immediate
ocs-storagecluster-ceph-rgw	openshift-storage.ceph.rook.io/bucket	Delete	Immediate
ocs-storagecluster-cephfs	openshift-storage.cephfs.csi.ceph.com	Delete	Immediate
openshift-storage.noobaa.io	openshift-storage.noobaa.io/obc	Delete	Immediate
thin	kubernetes.io/vsphere-volume	Delete	Immediate

Figure 8 `ibm-spectrum-scale-cnss-new` (default) storage class for CNSA

Confirm that the following prerequisites are met:

- Domain name and TLS certificate Domain name and TLS certificate are created.
- `entitledRegistryUsername` and `entitledRegistryPassword` are updated in the `values.conf` file
- All other required parameters are populated in `values.conf` (see “Appendix B” on page 41)
- Check prerequisites at this [IBM Documentation web page](#) to download `oc`, `helm3`, and `cloudctl` binaries

Deploying CP4S 1.7

Complete the following steps to deploy CP4S 1.7:

1. Run the following **cloudctl** command, which downloads the required package archive for the CP4S installation. Extract the downloaded archive by using **tar** command. The command snippet shows execution of both commands in single operation:

```
# cloudctl case save -t 1 --case
https://github.com/IBM/cloud-pak/raw/master/repo/case/ibm-cp-security-1.0.17.tgz
z --outputdir /root/cp4s1.7/ && tar -xf
/root/cp4s1.7/ibm-cp-security-1.0.17.tgz
```

The extracted package creates the structure that is shown in Figure 9.

```
[root@cluster3-inf cp4s1.7]# ls
TLS/
charts/
ibm-auditlogging-1.4.1-charts.csv
ibm-auditlogging-1.4.1-images.csv
ibm-auditlogging-1.4.1.tgz
ibm-cert-manager-1.3.0-charts.csv
ibm-cert-manager-1.3.0-images.csv
ibm-cert-manager-1.3.0.tgz
ibm-cloud-databases-redis-1.2.3-charts.csv
ibm-cloud-databases-redis-1.2.3-images.csv
ibm-cloud-databases-redis-1.2.3.tgz
ibm-couchdb-1.0.8-charts.csv
ibm-couchdb-1.0.8-images.csv
ibm-couchdb-1.0.8.tgz
ibm-cp-common-services-1.3.4-charts.csv
ibm-cp-common-services-1.3.4-images.csv
ibm-cp-common-services-1.3.4.tgz
ibm-cp-security/
ibm-cp-security-1.0.17-charts.csv
ibm-cp-security-1.0.17-images.csv
ibm-cp-security-1.0.17.tgz
ibm-cs-commonui-1.5.3-charts.csv
ibm-cs-commonui-1.5.3-images.csv
ibm-cs-commonui-1.5.3.tgz
ibm-cs-healthcheck-1.3.1-charts.csv
ibm-cs-healthcheck-1.3.1-images.csv
ibm-cs-healthcheck-1.3.1.tgz
ibm-cs-iam-1.3.2-charts.csv
ibm-cs-iam-1.3.2-images.csv
ibm-cs-iam-1.3.2.tgz
ibm-cs-mongodb-1.3.2-charts.csv
ibm-cs-mongodb-1.3.2-images.csv
ibm-cs-mongodb-1.3.2.tgz
ibm-cs-monitoring-1.3.2-charts.csv
ibm-cs-monitoring-1.3.2-images.csv
ibm-cs-monitoring-1.3.2.tgz
ibm-events-operator-3.7.1-charts.csv
ibm-events-operator-3.7.1-images.csv
ibm-events-operator-3.7.1.tgz
ibm-licensing-1.4.2-charts.csv
ibm-licensing-1.4.2-images.csv
ibm-licensing-1.4.2.tgz
ibm-management-ingress-1.3.2-charts.csv
ibm-management-ingress-1.3.2-images.csv
ibm-management-ingress-1.3.2.tgz
ibm-platform-api-operator-1.3.1-charts.csv
ibm-platform-api-operator-1.3.1-images.csv
ibm-platform-api-operator-1.3.1.tgz
ibm-zen-1.0.4-charts.csv
ibm-zen-1.0.4-images.csv
ibm-zen-1.0.4.tgz
```

Figure 9 File structure created for cp4s

2. Log in to the Red Hat OpenShift cluster (see Figure 10).

```
[root@cluster3-inf cp4s1.7]# oc login
Authentication required for https://api.cluster3.storage-ocp.tuc.stglabs.ibm.com:6443 (openshift)
Username: kubeadmin
Password:
Login successful.

You have access to 81 projects, the list has been suppressed. You can list all projects with ' projects'

Using project "cp4s".
[root@cluster3-inf cp4s1.7]#
```

Figure 10 Log in to OCP cluster with kubeadmin

3. Update the values.conf file and run the **cloudctl** command with the installation parameter:

```
# cloudctl case launch -t 1 --case ibm-cp-security --namespace cp4s --inventory
installProduct --action install --args "--license accept --helm3
/usr/local/bin/helm3 --inputDir /root/cp4s1.7"
```

Note: The deployment process takes approximately 90 minutes to complete.

After the deployment is complete, the output that is shown in Figure 11 is displayed. Any other log files that are generated during the installation are found in the /tmp directory.

```
iscstrust.isc.ibm.com/arangodb-iscstrust has been completed at "2021-07-01T03:53:45Z"
iscstrust.isc.ibm.com/cp4s-cs-ca has been completed at "2021-07-01T03:53:45Z"
iscstrust.isc.ibm.com/cp4s-default-ca has been completed at "2021-07-01T03:46:08Z"
iscstrust.isc.ibm.com/isc-ingress-default-secret-11289 has been completed at "2021-07-01T03:44:41Z"
etcd.isc.ibm.com/default has been completed at "2021-07-01T05:44:04Z"
minio.isc.ibm.com/ow-minio has been completed at "2021-07-01T03:46:08Z"
elastic.isc.ibm.com/isc-tis-elastic has been completed at "2021-07-01T03:46:08Z"
appentitlements.entitlements.extensions.platform.cp4s.ibm.com/app-car has status Warning at 2021-07-01T06:21:19
appentitlements.entitlements.extensions.platform.cp4s.ibm.com/app-car-connector-config has been completed at 2021-07-01T06:21:19
appentitlements.entitlements.extensions.platform.cp4s.ibm.com/app-cases has been completed at 2021-07-01T06:21:19
appentitlements.entitlements.extensions.platform.cp4s.ibm.com/app-de has status Warning at 2021-07-01T06:21:19
appentitlements.entitlements.extensions.platform.cp4s.ibm.com/app-insiderthreat has been completed at 2021-07-01T06:21:19
appentitlements.entitlements.extensions.platform.cp4s.ibm.com/app-licensing has been completed at 2021-07-01T06:21:19
appentitlements.entitlements.extensions.platform.cp4s.ibm.com/app-platform has been completed at 2021-07-01T06:21:19
appentitlements.entitlements.extensions.platform.cp4s.ibm.com/app-platform-uds has been completed at 2021-07-01T06:21:19
appentitlements.entitlements.extensions.platform.cp4s.ibm.com/app-pulsedashboard has been completed at 2021-07-01T06:21:19
appentitlements.entitlements.extensions.platform.cp4s.ibm.com/app-qproxy has been completed at 2021-07-01T06:21:19
appentitlements.entitlements.extensions.platform.cp4s.ibm.com/app-service-provider has been completed at 2021-07-01T06:21:19
appentitlements.entitlements.extensions.platform.cp4s.ibm.com/app-soar has been completed at 2021-07-01T06:21:19
appentitlements.entitlements.extensions.platform.cp4s.ibm.com/app-threat-inv has been completed at 2021-07-01T06:21:19
appentitlements.entitlements.extensions.platform.cp4s.ibm.com/app-tii has been completed at 2021-07-01T06:21:19
appentitlements.entitlements.extensions.platform.cp4s.ibm.com/app-udi-changelog-cronjob has been completed at 2021-07-01T06:21:19
appentitlements.entitlements.extensions.platform.cp4s.ibm.com/app-udi-encryption-cronjob has been completed at 2021-07-01T06:21:19
appentitlements.entitlements.extensions.platform.cp4s.ibm.com/app-usermanagement has been completed at 2021-07-01T06:21:19
appentitlements.entitlements.extensions.platform.cp4s.ibm.com/atk-entitlement has status Warning at 2021-07-01T06:21:19
appentitlements.entitlements.extensions.platform.cp4s.ibm.com/idrmapp has been completed at 2021-07-01T06:21:19
appentitlements.entitlements.extensions.platform.cp4s.ibm.com/tiicoordinator has been completed at 2021-07-01T06:21:19
appentitlements.entitlements.extensions.platform.cp4s.ibm.com/tiscoordinator has been completed at 2021-07-01T06:21:19
cases.isc.ibm.com/cases has been completed at "2021-07-01T03:47:28Z"
postgresoperator.isc.ibm.com/crunchy-pgo has been completed at "2021-07-01T03:47:36Z"
rabbitmq.isc.ibm.com/udi-rabbit has been completed at "2021-07-01T03:46:08Z"
The following pods are in pending state and should be in running state shortly:
idrm-ingestion-6c57956d6b-mt4qd          0/1   ContainerCreating   0    4s
idrm-ingestion-7c6d76d8d7-547vj        0/1   ContainerCreating   0    4s
The following pods are in error state:
idrm-postgres-5c9z6                    0/1   Error               0    134m
idrm-postgres-p46sx                    0/1   Error               0    166m
Problems in deployments replicas:
idrmapp: expect 3 pods have upodate 1
idrm-ingestion: expect 3 pods have upodate
isc-cases-postgres: expect 1 pods have upodate
isc-drm-postgres: expect 1 pods have upodate
[Progress: ##### | Step 5 of 5, Task Completed: Post-Install-Validation]

[?] CASE launch script completed successfully
OK
[root@cluster3-inf cp4s1.7] #
```

Figure 11 Successful completion of CP4S deployment

4. Run the following command to retrieve the foundational services URL:

```
[root@cluster3-inf cp4s1.7]# oc get routes cp-console -n ibm-common-services -o jsonpath='{.spec.host}' | awk '{print $1}'
cp-console.apps.cluster3.storage-ocp.tuc.stglabs.ibm.com
```

5. Run the following command to retrieve the foundational services admin username:

```
[root@cluster3-inf cp4s1.7]# oc get secret platform-auth-idp-credentials -o jsonpath='{.data.admin_username}' -n ibm-common-services | base64 -d | awk '{print $1}'
admin
```

6. Use the output from steps 5 and 6 to retrieve the console login URL, username, and password. This information also is available in the installation log file that is found in the /tmp directory.

Configuring the identity provider (LDAP) with CP4S

Complete the following steps to configure the identity provider when you log in to CP4S for the first time:

1. Figure 12 shows the first-time login window in CP4S. Click **Manage identity provider**.

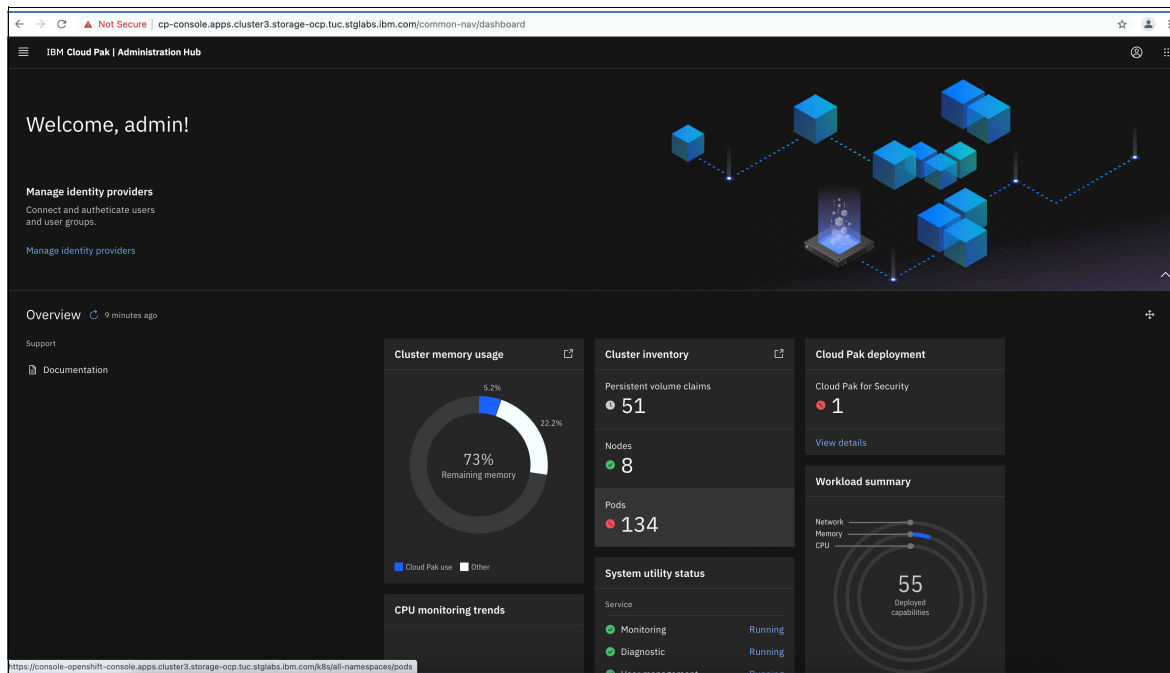


Figure 12 First-time login to the Common Service console

2. Click **Create connection** to configure the LDAP connection (see Figure 13).

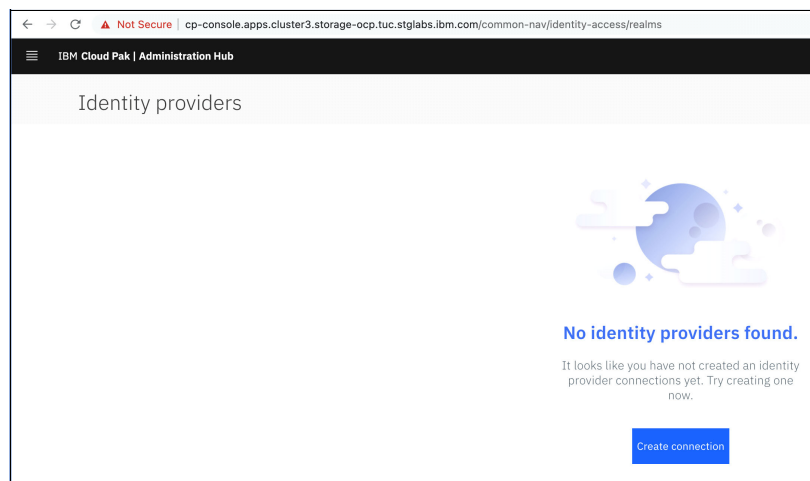


Figure 13 Configuring the identity provided LDAP

3. Enter the LDAP connection details as shown in Figure 14.

The screenshot shows the 'Add LDAP connection' form in the IBM Cloud Pak Administration Hub. The form is divided into three sections: 1. LDAP connection, 2. LDAP authentication, and 3. LDAP server. In the first section, the 'Connection name' is 'tuc_ldap' and the 'Server type' is 'Custom'. In the second section, the 'Base DN' is 'cn=accounts,dc=storage-ocp,dc=tuc,dc=stglabs.ibm.com', the 'Bind DN' is 'uid=admin,cn=users,cn=accounts,dc=storage-ocp,dc=tuc,dc=stglabs.ibm.com', and the 'Bind DN password' is masked with dots. In the third section, the 'URL' is 'ldap://ldap.storage-ocp.tuc.stglabs.ibm.com:389/cn=users,cn=accounts,dc=storage-ocp,dc=tuc,dc=stglabs.ibm.com?uid'. A 'Test connection' button is visible at the bottom right.

Figure 14 Creating LDAP connection with CP4S

Click **Test Connection** to test the connection to the LDAP server. Make sure that the result is successful. If the result is not successful, check the LDAP connectivity between LDAP server and CP4S, and re-check the parameters that were set in the Add LDAP connection (see Figure 14).

4. Log in to your CP4S application console URL by using the `cpsadmin` user that is configured in LDAP. Make sure to change the authentication type to LDAP at the login window (see Figure 15).

The screenshot shows the login page of the IBM Cloud Pak Administration Hub. The page has a dark background with a light blue illustration of people and network nodes on the left. On the right, there is a login form titled 'Log in to IBM Cloud Pak | Administration Hub'. The form asks for 'Username' and 'Password'. The 'Username' field contains 'cpsadmin' and the 'Password' field is masked with dots. There is a 'Log in' button and a link to 'Change your authentication type'.

Figure 15 Log in with LDAP user `cpsadmin`

Upon successful login, the CP4S dashboard is displayed (see Figure 16).

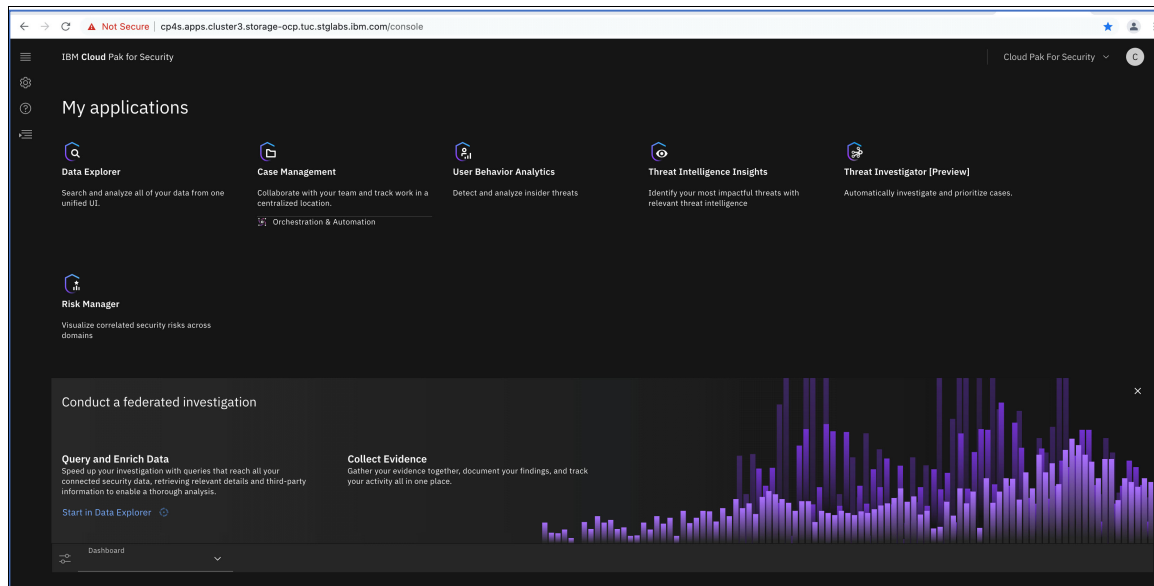


Figure 16 Successful log in to CP4S application by using the cpsadmin user

Configuring QRadar with LDAP

Complete the following steps to integrate IBM QRadar with LDAP:

1. Log in to the QRadar and select the **Admin** tab. Then, select **Authentication**. The Edit LDAP Repository window opens (see Figure 17).

The screenshot shows the 'Authentication Module Settings' window with the 'Edit LDAP Repository' tab selected. The left sidebar shows 'Authentication' and 'Repository Configuration' sections. The main content area is titled 'Edit LDAP Repository' and contains two sections: 'Basic Configuration' and 'Connection Settings'.

Basic Configuration

Repository ID	sha_ldap
Server URL	ldap://ldap.storage-ocp.tuc.stglabs.ibm.
SSL Connection	false
TLS Authentication	false
Search Entire Base	false
LDAP User Field	uid
User Base DN	cn=users,cn=accounts,dc=storage-ocp,dc=st
Referral	ignore

Connection Settings

☐ Anonymous Bind

☒ Authenticated Bind

Enter your authentication details below.

Login DN	uid=admin,cn=users,cn=accounts,dc=st
Password	*****

Buttons: Test Connection, Save, Cancel, Save Authentication Module

Figure 17 LDAP connection with QRadar

2. Scroll down and enter Group Base DN in the Group Member field (see Figure 18).

The screenshot shows the 'Authentication Module Settings' window with the 'Edit LDAP Repository' dialog open. The 'How to Authorize' section has three radio buttons: 'Local', 'User Attributes', and 'Group Based'. 'Group Based' is selected. Below it, the 'Group Base DN' field contains the text 'cn=groups,cn=accounts,dc=storage-ocf'. The 'Query Limit Enabled' checkbox is checked, and the 'Query Result Limit' is set to '1000'. In the 'By Member' section, the 'Group Member Field' is set to 'member'. There are also empty fields for 'Group Member Field' and 'Group Query Field' under the 'By Query' section. At the bottom of the dialog are 'Load Groups', 'Save', and 'Cancel' buttons. The background shows the 'Authentication Module Settings' page with a sidebar and a top navigation bar.

Figure 18 Completing the Group Member field

- Continue to scroll down and then, click **Load Groups** to populate the user roles and provide permissions (see Figure 19).

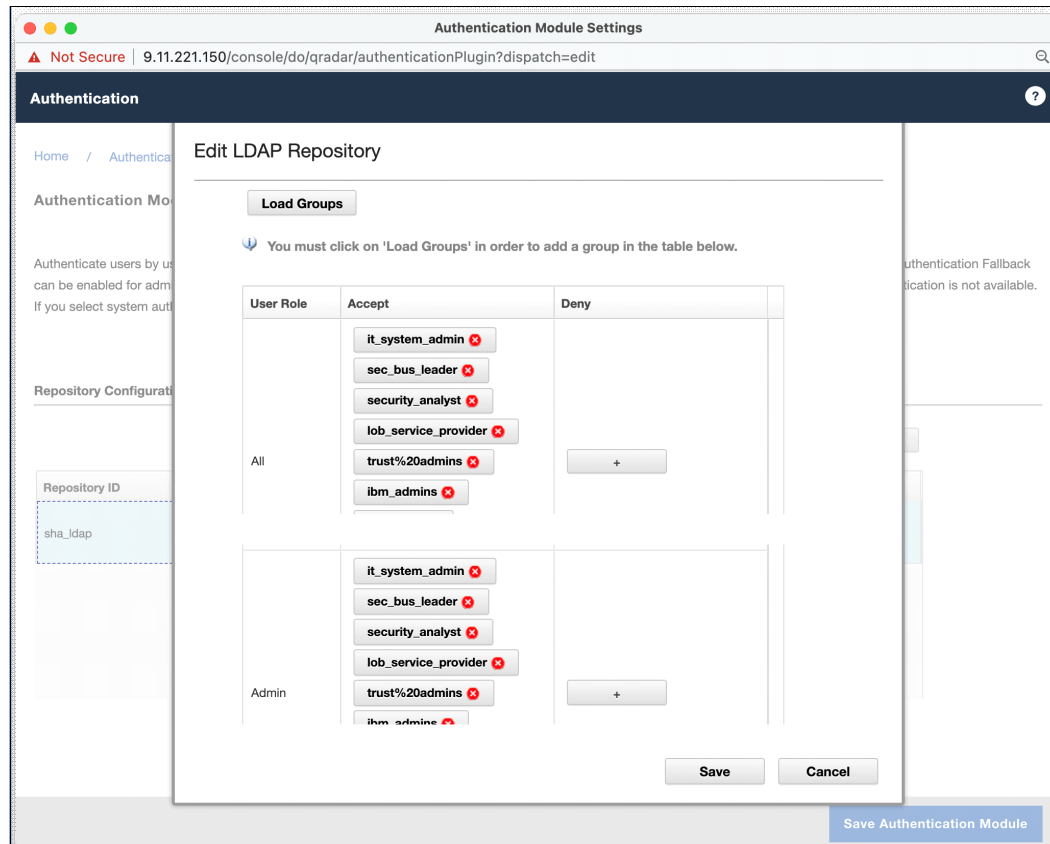


Figure 19 Populating the user roles and providing permissions

Integrating IBM CP4S with IBM QRadar

Complete the following steps to integrate IBM CP4S with IBM QRadar:

- Log in to the QRadar console and select the **Admin** tab. Then, select **Authorized Services** (see Figure 20).

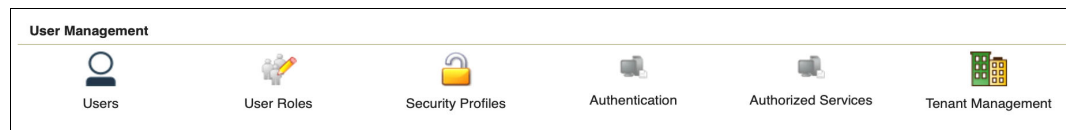


Figure 20 Select authorized services

- Create an authorized service name and token (see Figure 21), which is the same service and token that is to be used to configure QRadar connector from the CP4S console.

Add Authorized Service Delete Authorized Service Edit Authorized Service Name Selected Token:None						
Service Name	Authorized By	Authentication Token	User Role	Security Profile	Created	Expires
Qradar-tucson-for-cp4s-service	admin	50fd4de1-694e-4a26-a7a9-38cb005593b8	All	Admin	Jun 22, 2021, 8:36:08 ...	Permanent
qradar-service1	admin	706188cc-fd91-433a-96c8-8fd3b005b896	Admin	Admin	Jun 22, 2021, 8:42:52 ...	Permanent
service1	admin	54f4159d-45e5-41bb-a5f9-b081c651ecc8	qradaruser1	qradarsec1	Jun 22, 2021, 1:58:55 ...	Permanent

Figure 21 Creating authorized service and token

3. Log in to [CP4S application](#) and console by using the cpsadmin user. Click **Connections** → **Data sources**. Click the **Data sources** option and then, click **Connect a data source** (see Figure 22).

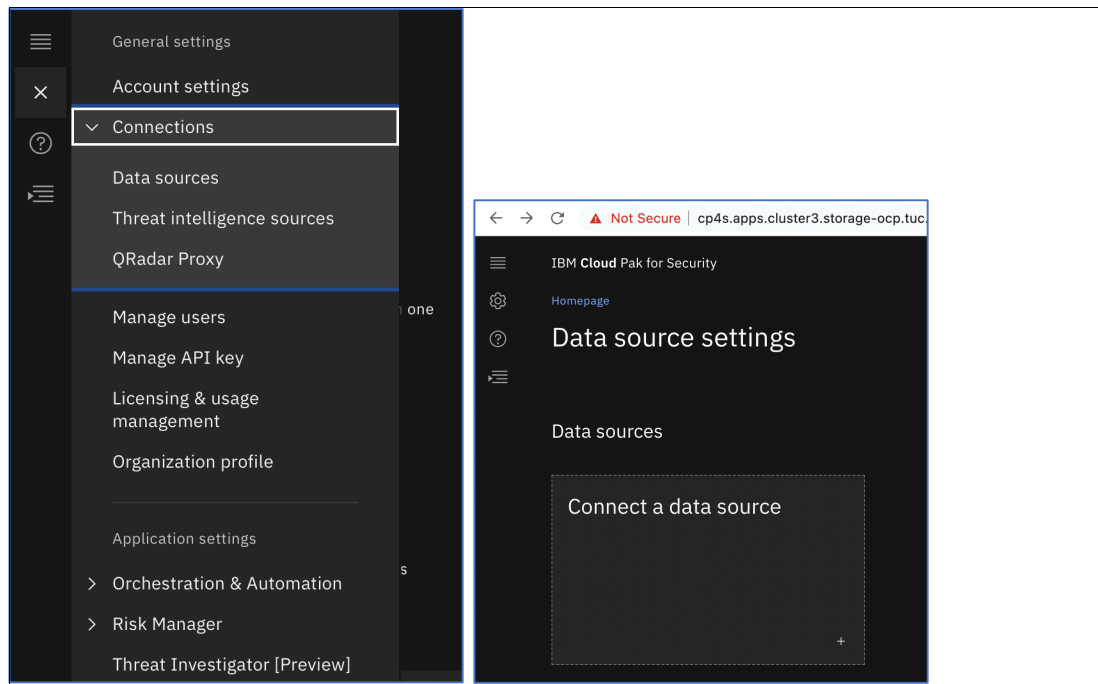


Figure 22 Creating a QRadar data source connection

4. Click **IBM QRadar** and **IBM QRadar On Cloud** (see Figure 23).

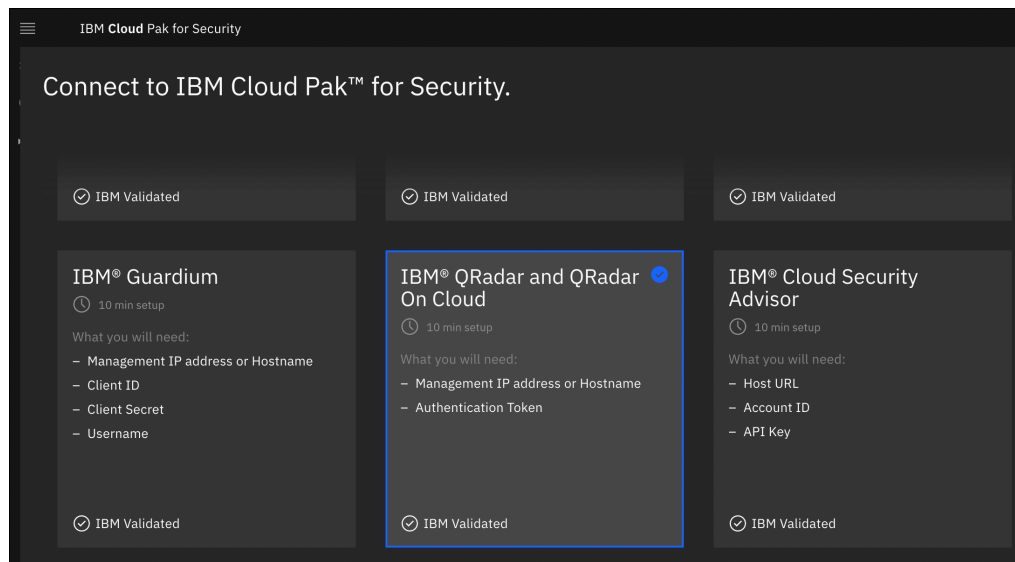


Figure 23 Creating data source connection

5. Enter the needed connection details (see Figure 24, which shows a sample lab configuration).

The screenshot shows the 'Connection details' configuration window in the IBM Cloud Pak for Security interface. On the left is a sidebar with a menu containing 'Connect to IBM® QRadar and QRadar On Cloud', 'Connection details' (selected), 'Query Parameters', 'Certificate', and 'Configurations'. The main area is titled 'Connection details' and includes a subtitle 'Define the general details to allow IBM Cloud Pak™ for Security to connect to the Data Source. Need additional help?'. It contains four input fields: 'Data source name' with the value 'Tucson-Qradar', 'Data source description' with the value 'Tucson-Qradar for CP4S 1.7', 'Management IP address or Hostname' with the value '9.11.221.150', and 'Host Port' with the value '443'. Below the 'Management IP address or Hostname' field is the text 'Specify the QRadar management IP address or Hostname.', and below the 'Host Port' field is the text 'Specify the associated port number of the data source.'

Figure 24 Entering the connection details

6. Continue to scroll down in the same window to complete the Query Parameters and Configurations sections (see Figure 25).

The screenshot shows the 'Query Parameters' and 'Configurations' sections of the configuration window. The 'Query Parameters' section on the left has the subtitle 'Set the parameters to control the behavior of the search query on the Data Source.' and contains four settings, each with a description and a numeric input field: 'Concurrent Search Limit' (4), 'Query Search Timeout Limit' (30), 'Result Size Limit' (10000), and 'Query Time Range' (5). The 'Configurations' section on the right has the subtitle 'Add and manage your Data Source configurations below. Most Data Sources require at least one configuration in order to connect.' and shows a table with one configuration: 'qradar-service1'. Above the table is the user 'cpsadmin cpsadmin' with an 'Edit access' link. Below the table is an 'Authentication Token' field with a 'Reset value' link. At the bottom are 'Cancel' and 'Save' buttons.

Figure 25 Completing the Query Parameters and Configurations sections

Optionally, add the certificate information (see Figure 26).

Connection Certificate (Optional)

This step can be safely skipped if the data source is using a certificate signed by a trusted certification authority (for example, not self-signed).

If the decoded certificate shows the Common Name as localhost.localdomain or your local domain, then it is a self-signed certificate. Otherwise, it is most likely a publicly signed certificate.

QRadar® 7.3.1 is configured with a self-signed Security Sockets Layer (SSL) certificate that is available in `/etc/httpd/conf/certs/cert.cert`.

QRadar® 7.3.2 root CA certificate can be downloaded from `http://<qradar_host_ip>:9381/vault-qrd_ca.pem` and the intermediate CA certificate from `http://<qradar_host_ip>:9381/vault-qrd_ca_int.pem`. Copy and paste both of these into the certificate section.

Server name indicator

Add a server name indicator

If your hostname or IP address does not match the common name you will need to supply a Server Name Indicator (SNI). This is used to allow a separate hostname to be provided to the TLS handshake of the resource connection.

IBM QRadar Certificate

Paste your certificate

Figure 26 Entering the IBM QRadar certificate

After the connection is created, a green dot and the word “Connected” are displayed, which indicates that the connection was successful (see Figure 27).

IBM Cloud Pak for Security

Homepage

Data source settings

Data sources

Connect a data source

+

Tucson-Qradar

Tucson-Qradar for CP4S 1.7

● Connected

Figure 27 Successful connection with QRadar

Integrating IBM CP4S with IBM QRadar, Proxy

As described in “Integrating IBM CP4S with IBM QRadar” on page 18, log in to the CP4S application and select **Connections** → **QRadar Proxy**. Enter the necessary information and create the connections.

Note: The connection is not shown as connected unless you log in by using the correct user (in our example, qradaruser1) in the QRadar console and accept the license (see Figure 28).

IBM Cloud Pak for Security

Homepage

QRadar Proxy

IBM QRadar

- Connection Details
- Authentication Token
- Certificate

Status for QRadar APIs
● Connected

Status for QRadar apps
● Connected

Last updated
10/08/2021, 16:45:54

Management IP address or hostname
Specify the QRadar management IP address or hostname.

qradar.storage-ocp.tuc.stglabs.ibm.com

Host Port
Specify the associated port number of the data source.

443

Authentication Token

Enter your IBM QRadar authentication token for REST API connectivity, such as for dashboards with content from IBM QRadar.

Authentication Token
The authentication token is also referred to as the SEC token.

.....

Enter a username and password to access supported apps in the IBM QRadar deployment.

Username
The username used to log in to the console.

qradaruser1

Password
The password used to log in to the console.

.....

IBM QRadar Connection Certificate (Optional)

Figure 28 QRadar proxy

Enabling IBM Spectrum Scale logs forwarding

Complete the following steps to enable audit logging and audit log events forwarding by using Rsyslog:

1. Log in to the IBM Spectrum Scale node and enable auditing on the file system (see Figure 29):

```
# mmaudit enable gpfs0
```

[root@udf-scale-01 ~]# mmaudit all list				
Audit Device	Cluster ID	Audit Fileset Name	Retention (Days)	Audit Type (Possible Filesets)
gpfs0	15195828851629006512	.audit_log	365	FSYS
[root@udf-scale-01 ~]# █				

Figure 29 Enabling audit on the file system

The audit log file structure is shown in Figure 30.

```
[root@udf-scale-01 .audit_log]# tree .
.
├── SpectrumScale_150_15195828851629006512_1627039168_FSYS_gpfs0_audit
│   ├── 2021
│   │   └── 07
│   │       └── 23
│   │           └── auditLogFile_udf-scale-01_2021-07-23_04:21:20
│   └── auditLogFile.latest_udf-scale-01 -> /ibm/gpfs0/.audit_log/SpectrumScale_150_15195828851629006512_1627039168_FSYS_gpfs0_audit/2021/07/23/auditLogFile_udf-scale-01_2021-07-23_04:21:20
4 directories, 2 files
[root@udf-scale-01 .audit_log]# █
```

Figure 30 Audit log file structure

2. Create a file for rsyslog to forward the log to QRadar system (see Figure 31).

```
[root@udf-scale-01 rsyslog.d]# cat qradar-forward.conf
# forward scale audit logs to IBM QRadar 9.11.221.150

module(load="imfile" PollingInterval="5")
input(type="imfile"
      File="/ibm/gpfs0/.audit_log/SpectrumScale_150_15195828851629006512_1627039168_FSYS_gpfs0_audit/auditLogFile.latest_udf-scale-01"
      Tag="fal"
      Severity="error"
      Facility="local4")
local4.* action(type="omfwd" target="9.11.221.150" port="514" protocol="tcp")
[root@udf-scale-01 rsyslog.d]# █
```

Figure 31 Creating a file for rsyslog

3. Run the **systemctl restart rsyslog** command to restart the rsyslog daemon process.
4. Confirm no errors are reported by the rsyslog daemon by running the **systemctl status rsyslog -l** command.

Configuring IBM Spectrum Scale log source in QRadar

Complete the following steps to configure the IBM Spectrum Scale log source in QRadar:

1. Log in to the QRadar console and confirm that the audit events are from Spectrum Scale are visible in QRadar. Various time-based filters can be applied to narrow the time for which events viewing (see Figure 32).

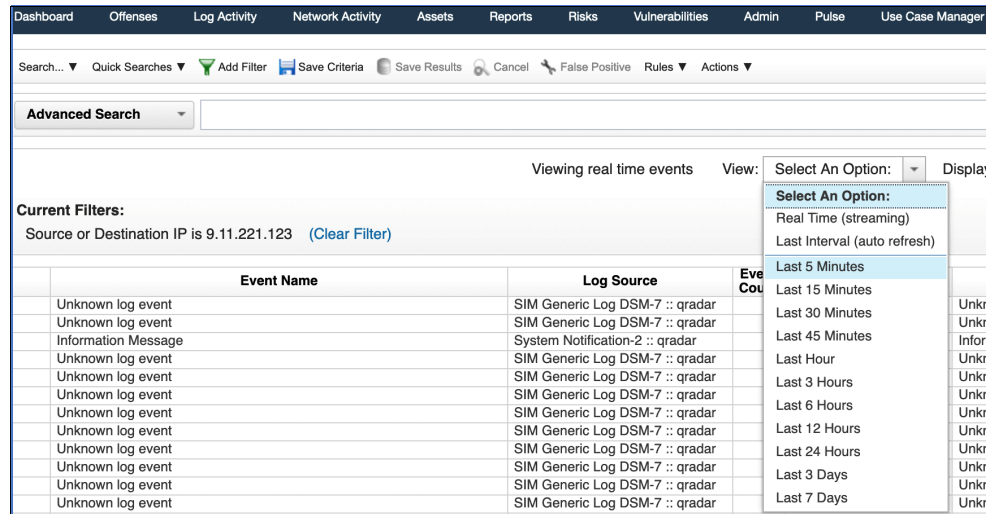


Figure 32 Applying time-based filters

2. Currently, QRadar does not support Spectrum Scale event normalization by extracting the data from the received audit log event. The data from these events must be manually configured by using DSM editor (see Figure 33).

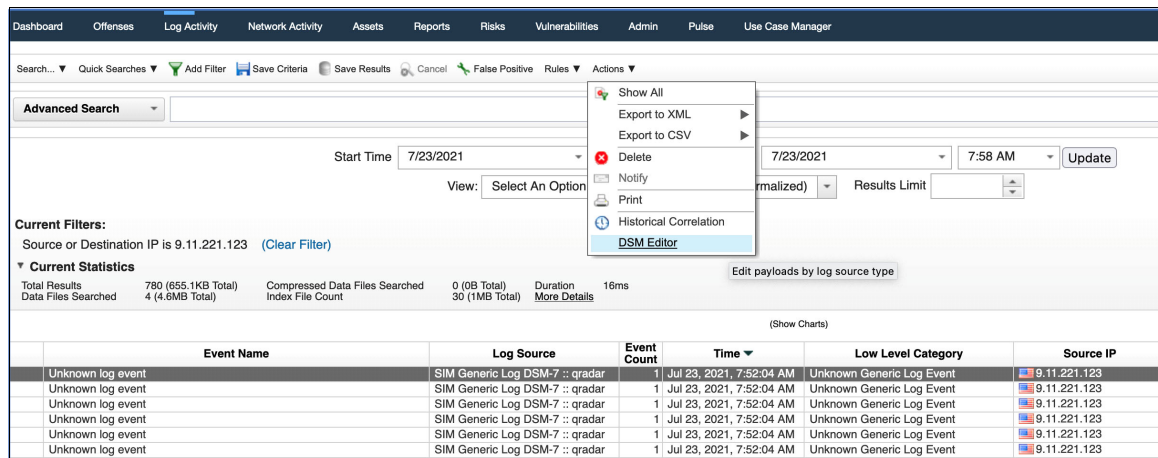


Figure 33 Selecting the DSM Editor option

3. Create an empty log source type by clicking **Create** (see Figure 3).

The figure consists of two screenshots of a web interface for selecting log source types.

Top Screenshot: The dialog is titled "Select Log Source Type" with the subtitle "Choose an existing Log Source Type to modify, or create a new Log Source Type". It features a "Filter" input field and a list of existing log source types: "3Com 8800 Series Switch", "AhnLab Policy Center APC", "Akamai KONA", "Amazon AWS Application Load Balancer Access Logs", and "Amazon AWS CloudTrail". At the bottom, there are three buttons: "Create New", "Select", and "Cancel".

Bottom Screenshot: This dialog is also titled "Select Log Source Type" with the same subtitle. It shows the "Create New" form. There is a label "Log Source Type Name" above an input field containing the text "IBM Spectrum Scale". At the bottom, there are two buttons: "Save" and "Go Back".

Figure 34 Creating a log source type

The DSM editor window now shows a three-pane view that includes the log source properties, raw event data, and log activity preview (see Figure 35).

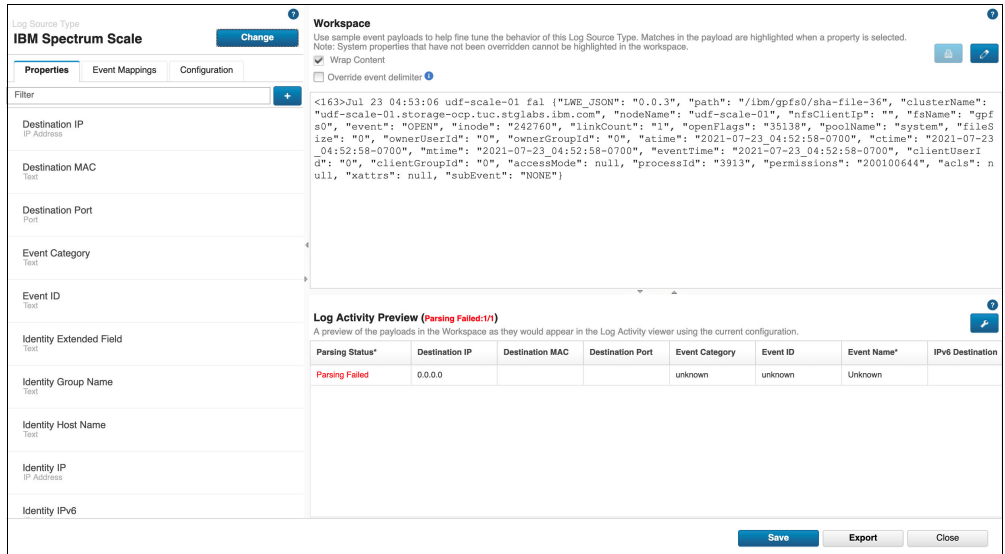


Figure 35 DSM Editor window

- Click and expand the **Event ID** property in the **Properties** window and enter the regular expression to extract data from the “event” field (see Figure 36).

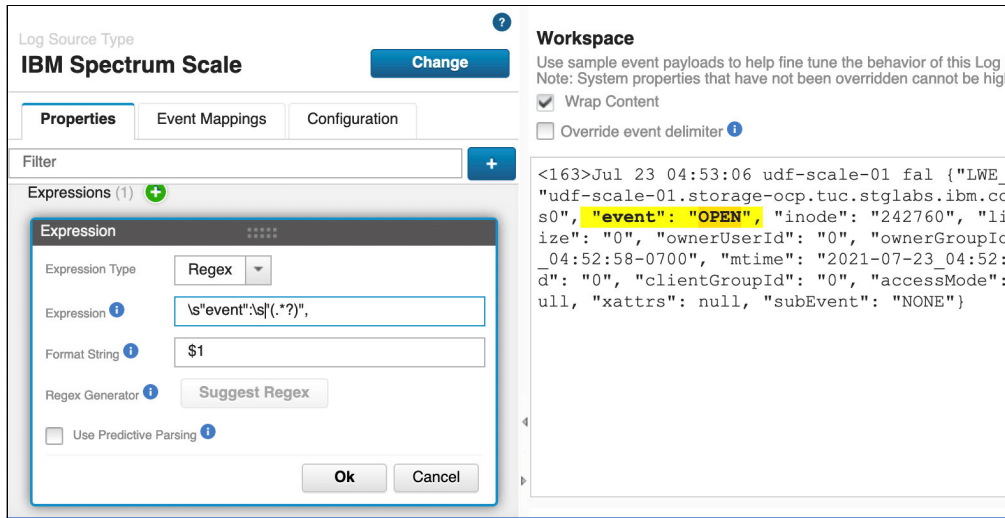


Figure 36 Regular expression to extract data from event field

The correct regular expression is highlighted in green (see Figure 37) for the text match found in the event data. The event is still shown as Parsed but *not* Mapped in the Log Activity preview window.

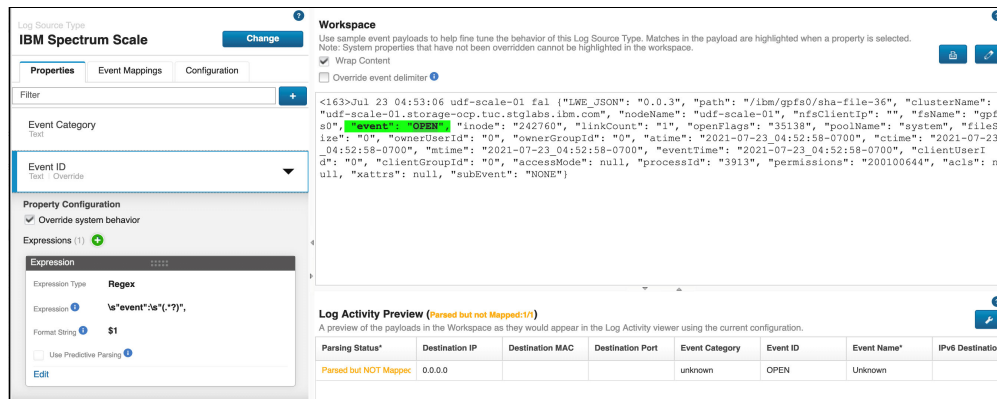


Figure 37 Correct regular expression highlighted

- Click **Choose QID** to create an event mapping, which maps the parsed event (see Figure 38).

Create a new Event Mapping

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

Unknown Event Mappings

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

Event ID	Event Category
OPEN	OPEN

Event ID i

OPEN

Event Category i

OPEN

QID Record
[Choose QID...](#)

Create **Close**

Figure 38 Log source configuration

In the QID Records window, various filters can be applied to narrow down the matching category that belong to the QID/Name (see Figure 39).

QID Records

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

High Level Category

Any

Low Level Category

Any

Log Source Type

Any

QID/Name

File Open

Search

Search Results

Name	Severity	High Level Category	Low Level Category
File Open A file was opened	2	System	Information
File Open A file was opened	2	System	Information
File Open A file was opened	2	System	Information
File Open Failed File open operation failed.	7	System	Error
File Open Failure Cannot open file for redirection.	3	Audit	File Access Failure

Total: 38 Selected: 1

1 2 3 4

10 | 25 | 50

Create New QID Record

Ok

Cancel

Figure 39 Selecting the suitable QID record

Selecting the suitable QID record completes the QID mapping and the event status is changed to Parsed and Mapped in the Log Activity Preview window (see Figure 40).

Log Source Type

IBM Spectrum Scale

Change

Properties Event Mappings Configuration

Filter

clusterName

Property Configuration

Expressions (1)

Expression

Expression Type

Regex

Expression

clusterName=.(.*?)

Capture Group

1

Edit

Destination IP

IP Address

Destination MAC

Workspace

Use sample event payloads to help fine tune the behavior of this Log Source Type. Matches in the payload are highlighted when a property is selected.

Note: System properties that have not been overridden cannot be highlighted in the workspace.

☒ Wrap Content

☐ Override event delimiter

<163>Jul 23 04:53:06 udf-scale-01 fal {"LWE_JSON": "0.0.3", "path": "/ibm/gpfs0/sha-file-36", "clusterName": "udf-scale-01.storage-ocp.tuc.stglabs.ibm.com", "nodeName": "udf-scale-01", "nfsClientIp": "", "fsName": "gpfs0", "event": "OPEN", "inode": "242760", "linkCount": "1", "openFlags": "35138", "poolName": "system", "fileSize": "0", "ownerUserId": "0", "ownerGroupId": "0", "atime": "2021-07-23 04:52:58-0700", "mtime": "2021-07-23 04:52:58-0700", "ctime": "2021-07-23 04:52:58-0700", "clientGroupId": "0", "accessMode": null, "processId": "3913", "permissions": "200100644", "acls": null, "xattrs": null, "subEvent": "NONE"}

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

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

Parsing Status	clusterName (custc)	Destination IP	Destination MAC	Destination Port	Event Category	Event ID	Event Name
Parsed but NOT Mapped	udf-scale-01.stora...	0.0.0.0			OPEN	OPEN	Unknown

Figure 40 Parsed and mapped event

Note: In the post QID-mapping process that is described here, the Save button must be clicked to save all the changes to be made to the newly created log source type.

6. To map the subsequent events that are received by QRadar, a new Log Source must be defined. This definition is done by clicking the **Admin** tab, and selecting **Log Sources** application under Data Sources (see Figure 41).

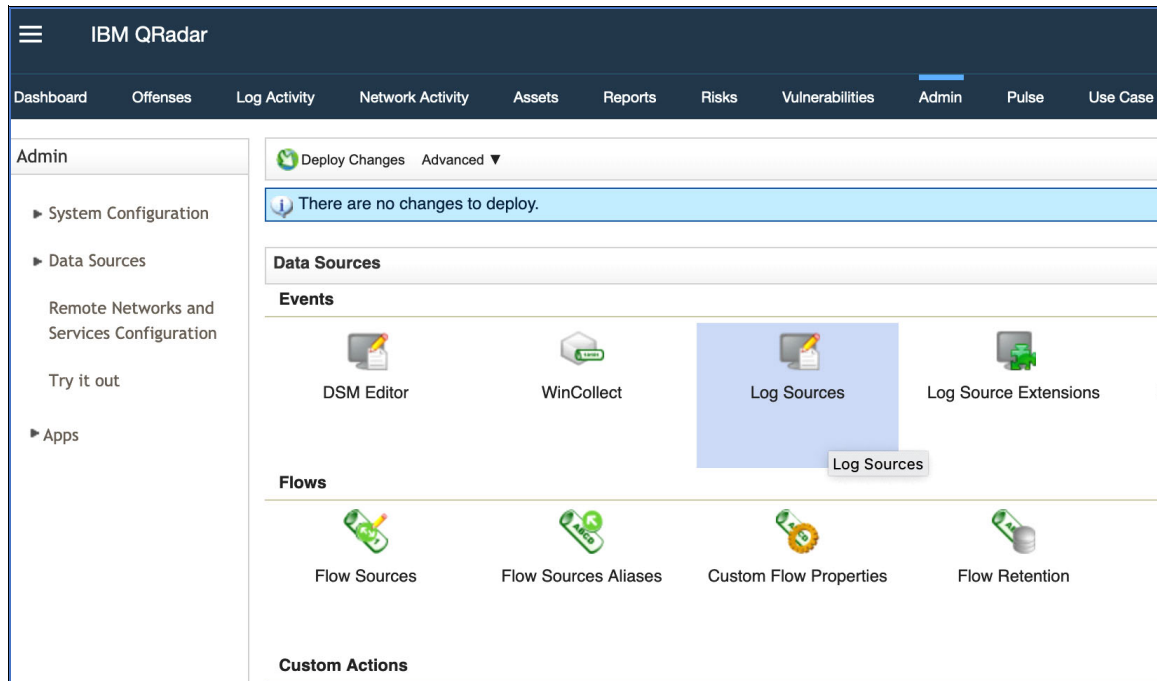


Figure 41 Log sources application

7. A new log source definition window opens. Start the new log source addition wizard by clicking **Add new log source** (see Figure 42).

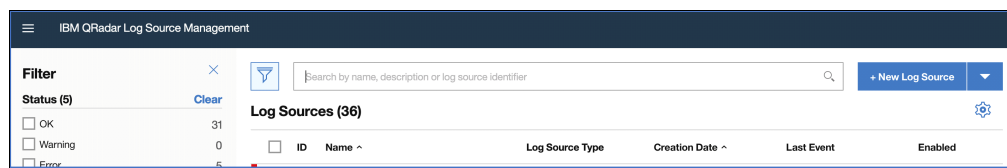



Figure 42 Defining new log source

The completed log source wizard summary is shown in Figure 43.

Log Source Summary



Spectrum-Scale-Log-Source

IBM Spectrum Scale

Status: Not Available

udf-scale-01

Last Updated in 3 hours

Initializing TCP syslog listener for port 514

Overview

Protocol

ID	162
Name	Spectrum-Scale-Log-Source
Description	IBM Spectrum Scale Log Source
Enabled	Yes
Log Source Type	IBM Spectrum Scale
Protocol Type	Syslog
Groups	Other
Extension	IBMSpectrumScaleCustom_ext
Language	English
Target Event Collector	eventcollector0 :: qradar
Disconnected Log Collector	Not Set
Credibility	5
Internal	No
Deployed	No
Coalescing Events	Yes

Figure 43 Log Source summary window

Configuring IBM QRadar SOAR Plugin

Complete the following steps to configure the IBM QRadar SOAR Plugin:

1. Download the IBM QRadar SOAR Plugin file to your local machine from [this web page](#).
2. Log in to QRadar console. Click **Extension management** → **Add** and then, enter any necessary information. Click **Install** (see Figure 44).

IBM QRadar SOAR Plugin

By: IBM SOAR

The extension has been installed successfully. Please review the install summary:

This extension contains one or more applications. In order for all new user interface elements to appear and function correctly, it is necessary to refresh your browser. It may also be necessary to clear your browser cache.

Custom Applications (1)	
IBM QRadar SOAR Plugin	INSTALL

Figure 44 SOAR Plugin window

3. Select the **Admin** tab and then, click **Apps** → **IBM QRadar SOAR Plugin** and configure the plug-in by using the provided information and click **Verify and Configure** (see Figure 45). For more information about editing the configuration file, see [IBM Documentation](#)).

IBM SOAR

QRadar Plugin

Application Access

QRadar Destination Name:

Authorized Service Token:

SOAR Server URL:

CP4S mode ☒

CP4S Connection Parameters

URL prefix
STOMP Host
STOMP Port

Authentication method:
Click to select

API key

Username/Password

API Key ID:

API Key Secret:

Multiple Organization Support:
☐

Organization Name:

SOAR Timeout (seconds):

Connect securely:
☐

Enable Configuring SOAR
☒

Need to configure a proxy?
☐

Proxy settings

Host

Port

User

Password

Cancel

Verify and Configure

Save

Connection and Configuration Verified Successfully!

Figure 45 SOAR plug-in

- To automate the process that creates cases in CP4S, configure the escalation rule in the Escalation tab of IBM QRadar SOAR Plugin (see Figure 46).

Figure 46 SOAR plug-in: Escalation rule

Defining a reference set in QRadar

Complete the following steps to configure a reference set in IBM QRadar:

- Log in to QRadar and click the **Admin** tab. Select **Reference set** and then, click **Add**. Add a new Alphanumeric reference type that is called Confidential items (see Figure 47).

Name	Type	Number of Elements	Associated Rules
UBA - Current Abridged ML Tracked Users	Alphanumeric (Ignore Case)	41	0
UBA : Multiple VPN Accounts Logged In from Single IP	IP	0	2
Asset Reconciliation NetBIOS Blacklist	Alphanumeric (Ignore Case)	0	3
Web Servers	IP	0	0
Asset Reconciliation IPv4 Whitelist	IP	0	0
Confidential Items	Alphanumeric	2	1

Figure 47 Reference set management

2. Double-click the newly defined reference set and click **Add** to add a single entry, or choose **Import** to import a text file that contains a list of entries that are defined as one record per line (see Figure 48).

⚠ Not Secure | 9.11.221.150/console/referenceSet/jsp/ReferenceSetDetails.jsp?rsId=77&name=Confidential Items

Reference Set: Confidential Items

Content

References

📄 Add

✖ Delete

✖ Delete Listed

📄 Import

📄 Export

Add new search criteria...

Value	Origin	Time to Live	Date Last Seen
confidential.txt	admin		11 Aug 2021, 07:38:46

Figure 48 Reference set Confidential items

Defining rules in QRadar

QRadar provides a flexible rules wizard that is used to incorporate various conditions that are suitable for a user's needs.

Complete the following steps to define rules that cater to tracking users actions to confidential items, files, or locations that are defined on the system:

1. Log in to QRadar and click the **Log Activities** tab; then, click the **Rules** drop-down to start the Rules wizard. Various condition choices are displayed that are selected by clicking the green button in front of the rule and by choosing the suitable attribute for the rule (see Figure 49).

The screenshot shows the 'Rule Wizard: Rule Test Stack Editor' window. At the top, it asks 'Which tests do you wish to perform on incoming events?'. Below this is a 'Test Group' dropdown set to 'All' and an 'Export as Building Block' button. A list of test conditions is shown, each with a green plus icon and a description: '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', and 'when the destination IP is one of the following IP addresses'. Below the list, it says 'Rule (Click on an underlined value to edit it)' and 'Invalid tests are highlighted and must be fixed before rule can be saved.' The rule is defined as: 'Apply Multiple File I/O events on events which are detected by the Local system and when the event(s) were detected by one or more of Spectrum-Scale-Log-Source request and when the event QID is one of the following (39000447) Change file attributes request, (39000257) Change file attributes request and when any of File_Name (custom) are contained in any of Confidential Items - AlphaNumeric'. Below the rule definition, it asks 'Please select any groups you would like this rule to be a member of:' and shows a list of groups: Anomaly (checked), Asset Reconciliation Exclusion, Authentication, Botnet, and Category Definitions. At the bottom, there is a 'Notes' section with the text 'Multiple file I/O events detected in short span'. The bottom of the window has navigation buttons: '<< Back', 'Next >>', 'Finish', and 'Cancel'.

Figure 49 New rule definition

The selection dialog box that appears when event QID attribute selection is chosen is shown in Figure 50.

Browse or Search for QIDs below. Select the desired QIDs and click 'Add'

High-Level Category: Any ▼
Low-Level Category: Any ▼
Log Source Type: Any ▼
QID/Name: change file attribute request

Search

Matching QIDs

QID	Name	Description ▲	Severity
39000447	Change file attributes request	Change file attributes request	1
39000257	Change file attributes request	Change file attributes request	1
20264588	CentOS.Security.Update.Firefox.CES...	Mozilla Firefox is a free and open source[8] we...	3
20257804	Mozilla.Thunderbird.SeaMonkey.Firefo...	Mozilla Firefox is a free and open source[8] we...	9
20267269	Red.Hat.Update.for.Firefox.RHSA-200...	Mozilla Firefox is a free and open source[8] we...	3
20264587	CentOS.Security.Update.Thunderbird....	Mozilla Thunderbird is a free, open source, cro...	3
4251740	FTP:CHMOD-OVERFLOW	Numerous FTP servers suffer from overflow v...	4
20264586	CentOS.Security.Update.SeaMonkey....	SeaMonkey is a free and open source cross-pl...	3
20271353	Oracle.Enterprise.Linux.Update.for.CU...	The Common UNIX Printing System (CUPS) p...	3

Figure 50 QID

The dialog box with various event properties when the File name attribute is chosen for the rule attribute is shown in Figure 51.

Not Secure | 9.11.221.150/console/do/rulewizard/customizeConditionParamet...

Select an event property and click 'Add'

Type to filter
(custom)
0 (custom)
ACF2 rule key (custom)
Access allowed (custom)
Access intent (custom)
Accesses (custom)

Add +

Selected Items

File_Name (custom)

Remove -

Submit Cancel

Figure 51 Event property

2. Upon choosing the suitable attributes per rule, click **Next** in the rule definition window to open the Rules Response section. Here, various response attributes, including the Offense definition, are configured (see Figure 2).

Rule Wizard

Rule Wizard: Rule Response

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

☒ Severity Set to 4

☒ Credibility Set to 3

☒ Relevance Set to 3

☒ Ensure the detected event is part of an offense

Index offense based on ownerUserId (custom)

☒ Annotate this offense: Multi file IO detected on

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

☒ Annotate event

Enter annotation for this event: multi-file-io

☐ Bypass further rule correlation event

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

☐ Dispatch New Event

☐ Email

☐ Send to Local Syslog

☐ Send to Forwarding Destinations

☐ Notify

☐ Add to a Reference Set

☐ Add 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

<< Back Next >> Finish Cancel

Figure 52 Selecting the rule response attributes

3. After all of the required attributes are set for the rule, click **Next** to display the Rule Summary page. This page describes the rule definition (see Figure 53).

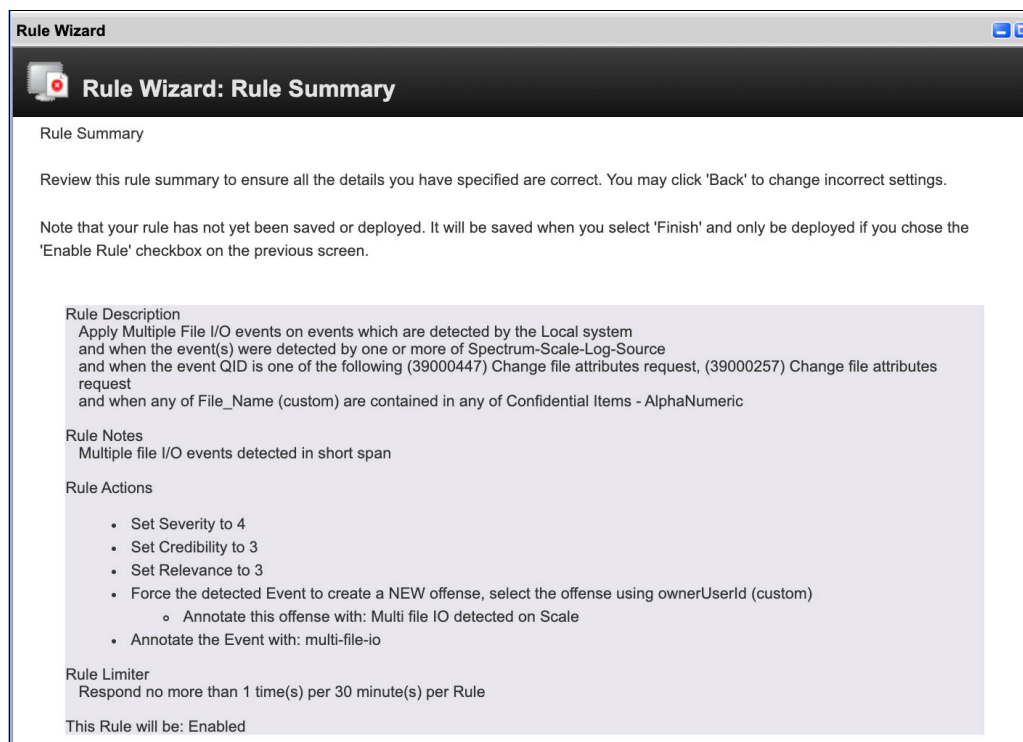


Figure 53 Rule Summary window

Demonstration use case

This demonstration shows how the file I/O events are captured in QRadar and offenses are generated based on predefined rules.

After the offenses are generated, we see how the Cases are automatically generated in Cloud Pak for Security by using the QRadar SOAR plug-in.

Complete the following steps:

1. With all the configuration tasks complete, log in to IBM Spectrum Scale node and attempt to update the `confidential.txt` file. This file is defined in QRadar's Reference set and is monitored for user actions against it (see Figure 54 on page 38).

```

hemantkantak@hemants-MacBook-Pro ~ %
hemantkantak@hemants-MacBook-Pro ~ %
hemantkantak@hemants-MacBook-Pro ~ % ssh hekantak@9.11.221.123
Warning: Permanently added '9.11.221.123' (ECDSA) to the list of known hosts.
Last login: Mon Aug 23 11:07:55 2021 from 9.79.188.143

[hekantak@udf-scale-01 ~]$
[hekantak@udf-scale-01 ~]$ cd /ibm/gpfs0/confidential/
[hekantak@udf-scale-01 confidential]$
[hekantak@udf-scale-01 confidential]$
[hekantak@udf-scale-01 confidential]$ ls -l
total 3
-rw-r--rw- 1 root root 66 Aug 23 01:05 Frank-Lee-2.txt
-rw-r--rw- 1 root root 140 Aug 23 01:05 Frank-lee.txt
-rw-r--r-- 1 root root 220 Aug 23 10:58 confidential.txt
-rw-r--r-- 1 root root 110 Aug 23 11:09 hsk
-rw-rw-r-- 1 sha sha 45 Aug 13 07:50 sha.txt
[hekantak@udf-scale-01 confidential]$
[hekantak@udf-scale-01 confidential]$ id
uid=1002(hekantak) gid=1002(hekantak) groups=1002(hekantak),10(wheel),1004(udf)
[hekantak@udf-scale-01 confidential]$
[hekantak@udf-scale-01 confidential]$ ls -ld /ibm/gpfs0/confidential/
drwxrwxr-x 2 root udf 4096 Aug 23 11:09 /ibm/gpfs0/confidential/
[hekantak@udf-scale-01 confidential]$
[hekantak@udf-scale-01 confidential]$

```

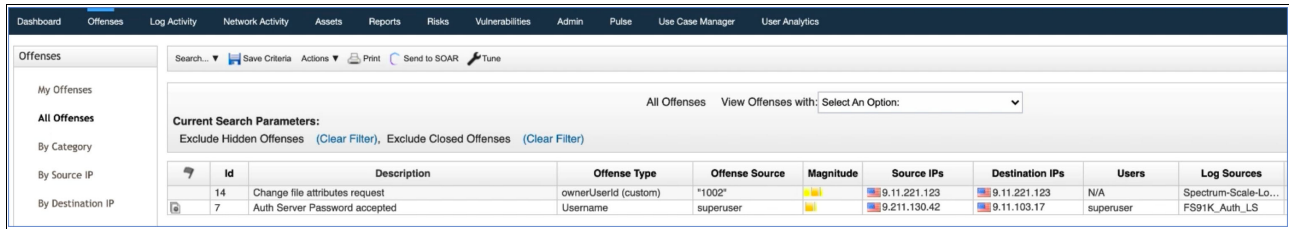
Figure 54 Scale node, update file

As the confidential file is being modified, IBM Spectrum Scale audit events track the I/O activity and generate audit events that are forwarded to IBM QRadar. These events can be seen under QRadar's Log Activity tab (see Figure 55).

viewing real time events view: Select An Option: Display: Default (Normalized)									
Current Filters: Log Source is any of [Linux @ Scale or Spectrum-Scale-Log-Source] (Clear Filter)									
Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Username
File Close	Spectrum-Scale-Log-Source	16	23 Aug 2021, 14:25:51	Information	9.11.221.123	0	9.11.221.123	0	N/A
File Open	Spectrum-Scale-Log-Source	14	23 Aug 2021, 14:25:51	Information	9.11.221.123	0	9.11.221.123	0	N/A
Access Denied	Spectrum-Scale-Log-Source	3	23 Aug 2021, 14:25:51	Access Denied	9.11.221.123	0	9.11.221.123	0	N/A
Change file attributes request	Spectrum-Scale-Log-Source	3	23 Aug 2021, 14:25:51	Successful File Modification	9.11.221.123	0	9.11.221.123	0	N/A
Delete File(s)	Spectrum-Scale-Log-Source	8	23 Aug 2021, 14:25:51	File Deleted	hemantkantak - hekantak@udf-scale-01/ibm/gpfs0/confidential - ssh h...				
File Created	Spectrum-Scale-Log-Source	6	23 Aug 2021, 14:25:51	File Created					
Change file attributes request	Spectrum-Scale-Log-Source	1	23 Aug 2021, 14:25:51	Successful File Modification	ibm/gpfs0/confidential - ssh 9.11.221.11		..ntial - ssh hekantak@9.11.221.123		
Change file attributes request	Spectrum-Scale-Log-Source	1	23 Aug 2021, 14:25:51	Successful File Modification					
Access Denied	Spectrum-Scale-Log-Source	1	23 Aug 2021, 14:25:51	Access Denied	wheel),1004(udf)				
ACL Updated	Spectrum-Scale-Log-Source	1	23 Aug 2021, 14:25:51	Update Activity Attempt	[hekantak@udf-scale-01 confidential]\$				
ACL Updated	Spectrum-Scale-Log-Source	1	23 Aug 2021, 14:25:51	Update Activity Attempt	[hekantak@udf-scale-01 confidential]\$ ls -ld /ibm/gpfs0/confide				
File Close	Spectrum-Scale-Log-Source	4	23 Aug 2021, 14:25:05	Information	ntial/				
File Created	Spectrum-Scale-Log-Source	3	23 Aug 2021, 14:25:05	File Created	drwxrwxr-x 2 root udf 4096 Aug 23 11:09 /ibm/gpfs0/confidential				
File Open	Spectrum-Scale-Log-Source	5	23 Aug 2021, 14:25:05	Information	[hekantak@udf-scale-01 confidential]\$				
Delete File(s)	Spectrum-Scale-Log-Source	1	23 Aug 2021, 14:25:05	File Deleted	[hekantak@udf-scale-01 confidential]\$				
File Created	Spectrum-Scale-Log-Source	1	23 Aug 2021, 14:25:05	File Created	[hekantak@udf-scale-01 confidential]\$				
Delete File(s)	Spectrum-Scale-Log-Source	1	23 Aug 2021, 14:25:05	File Deleted	[hekantak@udf-scale-01 confidential]\$ ls -l				
File Close	Spectrum-Scale-Log-Source	57	23 Aug 2021, 14:24:55	Information	total 3				
Delete File(s)	Spectrum-Scale-Log-Source	1	23 Aug 2021, 14:25:05	File Deleted	-rw-r--rw- 1 root root 66 Aug 23 01:05 Frank-Lee-2.txt				
File Created	Spectrum-Scale-Log-Source	1	23 Aug 2021, 14:25:05	File Created	-rw-r--rw- 1 root root 140 Aug 23 01:05 Frank-lee.txt				
File Open	Spectrum-Scale-Log-Source	58	23 Aug 2021, 14:24:55	Information	-rw-r--r-- 1 root root 220 Aug 23 10:58 confidential.txt				
File Created	Spectrum-Scale-Log-Source	1	23 Aug 2021, 14:25:00	File Created	-rw-r--r-- 1 root root 110 Aug 23 11:09 hsk				
Access Denied	Spectrum-Scale-Log-Source	1	23 Aug 2021, 14:25:00	Access Denied	-rw-rw-r-- 1 sha sha 45 Aug 13 07:50 sha.txt				
Access Denied	Spectrum-Scale-Log-Source	1	23 Aug 2021, 14:25:00	Access Denied	[hekantak@udf-scale-01 confidential]\$ vi confidential.txt				
File Open	Spectrum-Scale-Log-Source	1	23 Aug 2021, 14:24:55	Information	[hekantak@udf-scale-01 confidential]\$				
File Close	Spectrum-Scale-Log-Source	1	23 Aug 2021, 14:24:55	Information	[hekantak@udf-scale-01 confidential]\$ ls -l				
File Open	Spectrum-Scale-Log-Source	1	23 Aug 2021, 14:24:55	Information	total 3				
File Close	Spectrum-Scale-Log-Source	1	23 Aug 2021, 14:24:50	Information	-rw-r--rw- 1 root root 66 Aug 23 01:05 Frank-Lee-2.txt				
File Open	Spectrum-Scale-Log-Source	1	23 Aug 2021, 14:24:50	Information	-rw-r--rw- 1 root root 140 Aug 23 01:05 Frank-lee.txt				
File Close	Spectrum-Scale-Log-Source	1	23 Aug 2021, 14:24:50	Information	-rw-r--r-- 1 hekantak hekantak 138 Aug 23 11:27 confidential.tx				
File Open	Spectrum-Scale-Log-Source	1	23 Aug 2021, 14:24:50	Information	t				
					-rw-r--r-- 1 root root 110 Aug 23 11:09 hsk				
					-rw-rw-r-- 1 sha sha 45 Aug 13 07:50 sha.txt				
					[hekantak@udf-scale-01 confidential]\$				

Figure 55 Scale audit events

QRadar's rules act on the received audit event and an offense is generated when events are found that match the predefined rule (see Figure 56).



	Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destination IPs	Users	Log Sources
	14	Change file attributes request	ownerUserId (custom)	"1002"	1	9.11.221.123	9.11.221.123	N/A	Spectrum-Scale-Lo...
	7	Auth Server Password accepted	Username	superuser	1	9.211.130.42	9.11.103.17	superuser	FS91K_Auth_LS

Figure 56 Offenses in QRadar

2. Click **Send to SOAR**. The SOAR plug-in seamlessly sends the required event data to CP4S to create a case (see Figure 57).

Note: If you set the escalation rule in the IBM QRadar SOAR Plugin configuration, no manual intervention is needed to generate a case in CP4S. The required event data is automatically sent to CP4S.

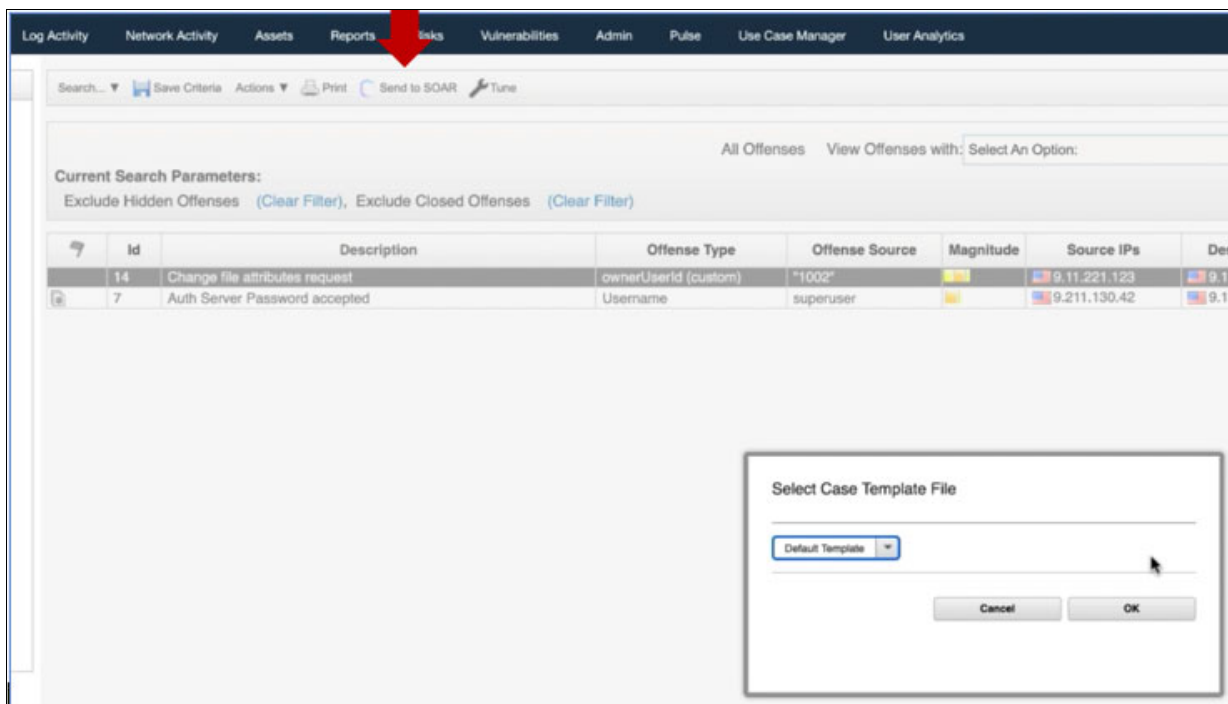
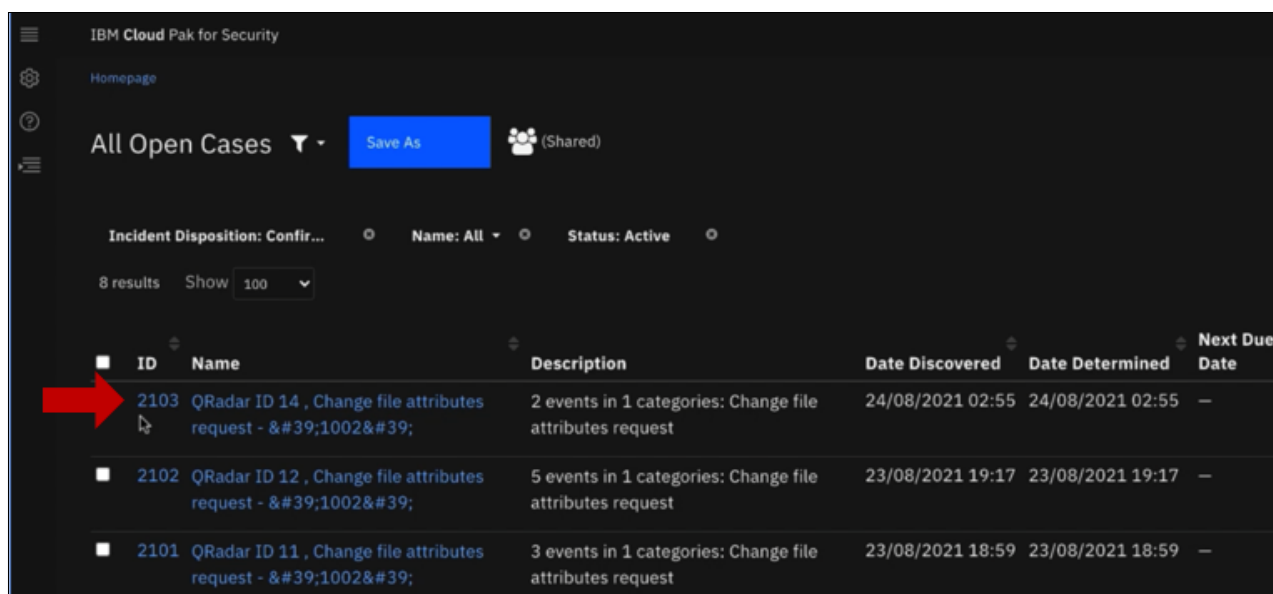


Figure 57 Sending event data to CP4S

Figure 58 shows the received event data and the Case that is generated against the same.



The screenshot shows the 'All Open Cases' page in IBM Cloud Pak for Security. It includes a sidebar with navigation icons, a header with 'All Open Cases' and a 'Save As' button, and a filter bar with 'Incident Disposition: Confir...', 'Name: All', and 'Status: Active'. Below the filter bar, it says '8 results' and 'Show 100'. The main content is a table with columns: ID, Name, Description, Date Discovered, Date Determined, and Next Due Date. A red arrow points to the first row, which has ID 2103 and a description starting with 'QRadar ID 14, Change file attributes request'.

ID	Name	Description	Date Discovered	Date Determined	Next Due Date
2103	QRadar ID 14, Change file attributes request - '1002'	2 events in 1 categories: Change file attributes request	24/08/2021 02:55	24/08/2021 02:55	—
2102	QRadar ID 12, Change file attributes request - '1002'	5 events in 1 categories: Change file attributes request	23/08/2021 19:17	23/08/2021 19:17	—
2101	QRadar ID 11, Change file attributes request - '1002'	3 events in 1 categories: Change file attributes request	23/08/2021 18:59	23/08/2021 18:59	—

Figure 58 Open Cases in CP4S

Summary

In this blueprint, we demonstrated the use of UDF infrastructure and UDF services for IBM Cloud Pak®. We also described integrating each of the components that are involved to prepare a solution for a Cyber Resiliency solution for the UDF infrastructure devices.

The combination IBM Spectrum Scale, IBM Cloud Pak for Security, and IBM QRadar integrated IBM QRadar SOAR Plugin for automating cases in CP4S 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. With the solutions and integrations that are listed “Appendix A”, we can also take advantage of the SOAR Platform (CP4S) with CP4S.

Appendix A

For more information, see the following publications:

- *Securing Data on Threat Detection Using IBM Spectrum Scale and IBM QRadar: An Enhanced Cyber Resiliency Solution*, [REDP-5560](#)
- *Enhanced Cyber Resilience Threat Detection with IBM FlashSystem Safeguarded Copy and IBM QRadar*, [REDP-5655](#)
- *Cyber Resiliency Solution using IBM Spectrum Virtualize*, [REDP-5657](#)

Appendix B

A sample values.conf file is shown in Figure 59.

```
[root@cluster3-inf cp4s1.7]# cat
./ibm-cp-security/inventory/installProduct/files/values.conf

# Admin User ID (Required): The user that is to be assigned as an Administrator in the
# default account after the installation. The user must exist in an LDAP directory that
# will be connected to Foundational Services after deployment.
adminUserId="cpsadmin"

# Cluster type (Required) should be one of the following: i.e. "aws", "ibmcloud",
# "azure", "ocp". This is a mandatory value, If not set it will be "ocp" by default.
cloudType="ocp"

# Block storage (Required), see more details
# https://www.ibm.com/support/knowledgecenter/en/SSTDPP_1.7.0/docs/security-pak/persistent
# _storage.html
storageClass="ibm-spectrum-scale-cnss-new"

# Entitled by default (Required)
registryType="entitled"

# Only Required for online install
entitledRegistryUrl="cp.icr.io"

# Only Required for online install
entitledRegistryPassword="YOUR-ENTITLED-REGISTRY-PASSWORD-HERE"

# Only Required for online install
entitledRegistryUsername="cp"

# Only required for offline/airgap install
localDockerRegistry=""

# Only required for offline/airgap install
localDockerRegistryUsername=""

# Only required for offline/airgap install
localDockerRegistryPassword=""

# CP4S FQDN domain (Optional: Not required if your cloudType is set to "ibmcloud" or
# "aws")
cp4sapplicationDomain="cp4s.apps.cluster3.storage-ocp.tuc.stglabs.ibm.com"

# e.g ./path-to-cert/cert.crt (Optional: Not required if you are using ibmcloud or aws).
# See more details:
# https://www.ibm.com/support/knowledgecenter/en/SSTDPP_1.7.0/docs/security-pak/tls_certs.
# html.
cp4sdomainCertificatePath="/root/cp4s1.7/TLS/tls.crt"
```

```

# Path to domain certificate key ./path-to-key/cert.key (Optional: Not required if you
using ibmcloud or aws). See more at
https://www.ibm.com/support/knowledgecenter/en/SSTDPP_1.7.0/docs/security-pak/tls_certs.
html.
cp4sdomainCertificateKeyPath="/root/cp4s1.7/TLS/tls.key"

# Path to custom ca cert e.g <path-to-cert>/ca.crt (Only required if using custom/self
signed certificate and optional on ibmcloud or aws). See more at
https://www.ibm.com/support/knowledgecenter/en/SSTDPP_1.7.0/docs/security-pak/tls_certs.
html.
cp4scustomcaFilepath="/root/cp4s1.7/TLS/ca.crt"

# Set image pullpolicy e.g Always,IfNotPresent, default is Always (Required)
cp4simagePullPolicy="Always"

# Set to "true" to enable Openshift authentication (Optional). Only supported for ROKS
clusters, for more details, see
https://www.ibm.com/support/knowledgecenter/en/SSHKN6/iam/3.x.x/roks_config.html
cp4sOpenshiftAuthentication="false"

# Default Account name, default is "Cloud Pak For Security" (Optional)
defaultAccountName="Cloud Pak For Security"

# set to "true" to enable CSA Adapter (Optional), see
https://www.ibm.com/support/knowledgecenter/en/SSTDPP_1.7.0/docs/scp-core/csa-adapter-ca
ses.html for more details
enableCloudSecurityAdvisor="false"

# Set storage fs group. Default is 26 (Optional)
storageClassFsGroup="26"

# Set storage class supplemental groups (Optional)
storageClassSupplementalGroups="ibm-spectrum-scale-cnss-new"

# Set seperate storageclass for backup (Optional)
backupStorageClass="ibm-spectrum-scale-cnss-new"

# Set custom storage size for backup, default is 100Gi (Optional)
backupStorageSize="100Gi"

```

Figure 59 Sample values.conf file

About the author

Hemant Kantak has been a Storage Solutions Architect with IBM Systems, ISDL Lab Pune, India, for over 10 years. He has worked extensively with IBM Storage products, such as Spectrum Virtualize, IBM FlashSystem®, IBM DS8k, IBM A9K, IBM Spectrum® Scale, and Red Hat OpenShift features. Currently, he is working on demonstrating Hybrid Cloud Solutions for Data and AI and Security solutions with IBM QRadar® and IBM Storage Suite for Cloud Paks. Before joining IBM, Hemant worked with Oracle India Ltd. (Sun Microsystems India), as a lead for enterprise accounts to manage the account's systems, storage, and solution portfolios.

Acknowledgments

The author wishes to thank the following people for their contributions to this project:

Frank Lee
IBM, DE

Matt Levan
IBM, Technical Offering Manager

Shashank Shingornikar
IBM, Solution Architect - Storage

Sandeep Patil
IBM, STSM, Storage CTO Office

Douglas O'Flaherty
Global Ecosystem Leader, IBM Storage

David Druker
IBM, Security Digital Technical Engagement

Notices

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

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

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

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

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

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

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

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

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

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

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

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


COPYRIGHT LICENSE:

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

Trademarks

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

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

Redbooks (logo) ®

IBM®

IBM Cloud®

IBM Cloud Pak®

IBM FlashSystem®

IBM Spectrum®

QRadar®

The following terms are trademarks of other companies:

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

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

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

Terms and conditions for product documentation

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

Applicability

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

Commercial use

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

Rights

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

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

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

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

Privacy policy considerations

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

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

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

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



© Copyright IBM Corporation

December 2021

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



Please recycle

ISBN 0738460141

REDP-5666-00