IBM Storage Defender Data Management Service

User's Guide

Note:

Before you use this information and the product it supports, read the information in “Notices” on page 125.

August 2024 edition

This edition applies to IBM Storage Defender Data Management Service and to all subsequent releases and modifications until otherwise indicated in new editions:

- IBM Storage Defender ordered through Passport Advantage® (product number 5900-AXW)
- IBM Storage Defender Data Management Service ordered through AAS (product number 5900-AY6)

© Copyright International Business Machines Corporation 2023, 2024.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About this publication

This publication provides overview, planning, installation, and user instructions for IBM Storage Defender Data Management Service.

© Copyright IBM Corp. 2023, 2024

Chapter 1. About IBM Storage Defender Data Management Service

IBM Storage Defender Data Management Service is a SaaS-based management platform that provides a single view and global management of all your IBM Storage Defender Data Protect clusters, whether on-premises, cloud or Virtual Edition, regardless of cluster size. You can quickly connect clusters to Data Management and then access them from anywhere using an internet connection and your IBMid credentials.

Data Management provides you with the following features:

Multi-cluster management
Actively manage all your clusters, including multi-cluster monitoring and reporting, from a single dashboard.

Global actionable search
Search across clusters and take action directly from the search results page. For example, search for all unprotected VMs and create jobs to protect them.

SmartAssist
Automatically schedule and orchestrate jobs and workloads to help meet SLAs. Get recommendations based on capacity forecasting and disk failure prediction. View important Data Management field notices.

Security tools
Detect threats and other anomalies across clusters with the unified Alerts page.

Changes that you make directly to the cluster while using Data Management might not appear in the Data Management Dashboard for fifteen minutes.

In Data Management, the data and metadata are secured by using different services based on the use case.

Prerequisites

- To sign in to IBM Storage Defender Data Management Service, you must have an IBMid.
- Data Management supports all supported Data Protect cluster versions, see IBM Storage Defender: Data Protect support information.
- To connect a cluster version to Data Management, additional configuration might be required. In some cases, Data Management determines that an external cluster is running inside the Data Management network based on DNS information it receives, and incorrectly configures an internal Data Management connection. To work around this issue, you might need to download and run a script.

What Next?

The following sections help you to get started with IBM Storage Defender Data Management Service:

- Managing Cluster Connections
- Logging in to IBM Storage Defender
  - Managing users
  - Managing roles

© Copyright IBM Corp. 2023, 2024

Chapter 2. Managing IBM Storage Protect connections

Connecting an IBM Storage Protect server to Data Management

Connecting an existing IBM Storage Protect server to IBM Storage Defender Data Management Service (Data Management) allows you to manage IBM Storage Protect server backups from Data Management along with your other clusters.

About this task

To connect or "claim" an IBM Storage Protect server, complete the procedure to download and install the IBM® Storage Defender® connection agent. Install the IBM Storage Defender connection agent on the IBM Storage Protect server that you are claiming or on another system that has network connectivity to the IBM Storage Protect server. The system where you install the agent must meet the following requirements:

- Must be running on a supported operating system:
  - Red Hat® Enterprise Linux® x86_64, version 8.7 or later RHEL 8 fix packs
  - SUSE Linux Enterprise Server x86_64, version 15.0 or later SLES 15 fix packs
- The IBM Storage Protect server that you are claiming must be running IBM Storage Protect 8.1.18 or later versions.
- Must be able to connect with IBM Storage Defender directly or through an HTTPS proxy.

Procedure

1. From the hamburger icon on IBM Storage Defender , click **Data Management** then click **Connection agents**. The **Connections agents** page is displayed.

   Important: To register an IBM Storage Protect server by using the Defender connection agent, your Data Management user account must have **Admin** role privileges.
2. Click **Download agent** to download the Defender connection agent file to the `Downloads` directory on your local system.
3. To install the Defender connection agent, complete the following steps:
   a) Extract the file that you downloaded in step “2” on page 3 by issuing the following command from the terminal:

   ```
   tar -xvf defender-agent-filename-tar.gz
   ```

   Where **`defender-agent-filename-tar.gz`** is the name of the downloaded file.

   b) Run the following installation script as sudo by specifying a local user account:

   ```
   sudo ./install-eagle-agent.sh -u <user>
   ```

   Where, *<user>* is the name of an existing user account on your local system that will be used to run the Defender connection agent after the agent is installed. Designate a user account that does not have administrator rights for the local system. After the Defender connection agent is installed, the agent will always run as the specified user.

© Copyright IBM Corp. 2023, 2024

Note: To specify that the Defender connection agent must use an HTTPS proxy to connect to Data Management, specify the **--proxy** parameter on the installation script by issuing the following command:

```
sudo ./install-eagle-agent.sh -u user --proxy <https://address:port>
```

4. Register the IBM Storage Protect server with Data Management by issuing the following dcli server register command.

   Remember: Run **dcli** commands by using the local user account that you specified in step "3.b" on page 3.

   ```
   /opt/ibm/defender/bin/dcli server register -a <admin_name> -p <password> -d
   <server_ip_address> -o <port> -n <server_nickname> -t <truststore_password>
   ```

   Where

   - *<admin_name>* is the IBM Storage Protect server administrator name that is used to authorize the server registration to Data Management.
   - *<password>* is the IBM Storage Protect server administrator password.
   - *<server_ip_address>* is the IP address or hostname for the IBM Storage Protect server.
   - *<port>* is the IBM Storage Protect server port number.
   - *<server_nickname>* is a user-specified nickname for the IBM Storage Protect server that will be displayed in Data Management.
   - *<truststore_password>* is the truststore password.

   Example: `/opt/ibm/defender/bin/dcli server register -a adminA -p myp@ssword -d server1.mycity.mycompany.com -o 1500 -n server1 -t secretpassword`

   Note: After you register the server with Data Management, a new administrator who is named *ibm-eagle-agent-admin* is created on the IBM Storage Protect server. This new administrator account has a low level of system privilege and is used by the IBM Storage Defender eagle agent service to retrieve information from the IBM Storage Protect server.

5. Connect the registered IBM Storage Protect server to Data Management by completing the steps to claim the server:

   a) From the IBM Storage Defender page, click **All Clusters** and navigate to **Settings > Access Management**.

   b) On the **Access Management** page. select the **Tokens** tab.

   c) Click the **Create** button in the upper right corner of the screen.

      The **Create Token** pop-up window appears with the two following input fields:

      - Name – The Name field is the name of this token. It can be any name you like, for example: SP Server Armonk 001.
      - Type – Change this from DataProtect to IBM Storage Protect. Then click **Create** , which creates a token.

   d) Before closing the **Create Token** window, copy the token by selecting the copy icon.

   e) Register the claim by issuing the "dcli claim register" on page 11 command from the terminal, paste the token from previous step:

      ```
      /opt/ibm/defender/bin/dcli claim register --token token-copied-from-previous-step
      ```

6. Start the Defender connection agent by issuing the **eagle-agent start** command:

   ```
   /opt/ibm/defender/bin/dcli eagle-agent start
   ```

7. To verify that the IBM Storage Protect server was successfully connected, launch Data Management and navigate to **All Clusters > Settings > Clusters**. The **Cluster Management** page is displayed.

If the cluster connection was successful, the **Connection** column displays a ✓ **Connected** status for the cluster.

Shows up under "cluster management"

Updating the Defender connection agent

You can update an existing IBM Storage Defender connection agent that is being used to manage the IBM Storage Protect server backups from IBM Storage Defender Data Management Service.

Before you begin

A Defender connection agent must have already been installed and configured to connect the IBM Storage Protect server to IBM Storage Defender Data Management Service (Data Management) before you can use this procedure to update the agent. If you are connecting the server to Data Management for the first time, see Connecting an IBM Storage Protect server to Data Management.

Procedure

1. On the IBM Storage Defender menu bar, click **Connection agents**. The **Connections agents** page is displayed.
2. Click **Download agent** to download the Defender connection agent file to the `Downloads` directory on your local system.
3. To install the Defender connection agent, complete the following steps:

   a) Extract the file that you downloaded in step "2" on page 5 by issuing the following command from the terminal:

   ```
   tar -xvf defender-agent-filename-tar.gz
   ```

   Where `defender-agent-filename-tar.gz` is the name of the downloaded file.

   b) Run the following installation script as sudo by specifying a local user account:

   ```
   sudo ./install-eagle-agent.sh -u <user>
   ```

   Where, *<user>* is the name of an existing user account on your local system that will be used to run the Defender connection agent after the agent is installed. Designate a user account that does not have administrator rights for the local system. After the Defender connection agent is installed, the agent will always run as the specified user.

   Note: To specify that the Defender connection agent must use an HTTPS proxy to connect to Data Management, specify the **--proxy** parameter on the installation script by issuing the following command:

   ```
   sudo ./install-eagle-agent.sh -u user --proxy <https://address:port>
   ```

Unregistering an IBM Storage Protect server

If an IBM Storage Protect server is no longer in use or no longer needs to be managed, you can unregister the IBM Storage Protect server from the IBM Storage Defender Data Management Service (Data Management). Unregistering an existing IBM Storage Protect server from Data Management removes management of IBM Storage Protect server backups from Data Management. When you unregister the IBM Storage Protect server, the IBM Storage Protect server is no longer be managed with your other clusters.

Before you begin

The IBM Storage Defender eagle agent service is used to send and receive data between the IBM Storage Protect server and Data Management. Before you unregister a cluster, you can stop the eagle agent that is running in the background by completing the following steps:

1. Stop the eagle-agent by issuing the dcli eagle-agent stop command.
2. Delete the claim to your IBM Storage Protect server by issuing the dcli claim delete command.
3. Delete the registration of the IBM Storage Protect server by issuing the dcli server delete command.
4. Follow the procedure to unregister the cluster in Data Management.

Procedure

1. Log in to IBM Storage Defender and from the **IBM Storage Defender** menu, navigate to **Data Management > Overview > Launch Data management**.
2. Click on the cluster's drop-down menu in the left side panel and select **All Clusters** for a view of all clusters.
3. Click **Settings > Clusters**. The **Cluster Management** page is displayed.
4. From the list of available clusters, click the ⋮ icon for the IBM Storage Protect server that you want to unregister from Data Management.
5. Select the **Unregister** option.

   The **Unregister** window is displayed along with the following message:

   ```
   Are you sure you want to unregister the cluster(s) from Data Management?
   ```
6. Click **Unregister**.
7. Verify that the IBM Storage Protect server is removed from the list of clusters. It might take a few moments for the table to update.

Removing the IBM Storage Protect server connection agent

Disconnecting an existing IBM Storage Protect server from IBM Storage Defender Data Management Service (Data Management) removes management of IBM Storage Protect server backups from Data Management. The IBM Storage Protect server will no longer be managed with your other clusters.

Before you begin

This task assumes that you have access to the **`install-eagle-agent.sh`** script to remove the eagle agent from the system. The script is contained within the `defender-agent-filename-tar.gz` compressed archive file. See "Connecting an IBM Storage Protect server to Data Management" on page 3 for information on how to download this package.

Procedure

1. Log in to the operating system terminal of the IBM Storage Protect server system with the non-root local user account that is used to run the IBM Storage Defender connection agent.
2. Run the following script by using the **`dcli claim delete`** command to delete the current claim to Data Management after completing the following steps:

   a) Connect to IBM Storage Defender Data Management Service with a user that has the Super Admin role.

   b) From the IBM Storage Defender Data Management Service, select **All Clusters** and select **Settings > Access Management**.

   c) Select the **API Key** tab.

d) Select the **Add API Key** box in the upper right corner of the screen. The **Add API Key** input window appears with the **Name** field. The **Name** field is the name of the key. The key can be any name that you like, for example: SP Server Armonk 001. Click **Save** to create the key.

e) Before closing the **API Key Details** window, copy the key by selecting the **Copy API Key Token** icon.

f) Delete the claim by issuing the **dcli claim delete** command from the terminal, and paste the token from previous step by issuing the following command:

```
/opt/ibm/defender/bin/dcli claim delete --<apiKey key-copied-from-previous-step>
```

3. Run the following script by using the **dcli server delete** command to delete the registration of the IBM Storage Protect server:

```
/opt/ibm/defender/bin/dcli server delete
```

4. Run the following script by using the **dcli eagle-agent stop** command to stop the eagle agent process:

```
/opt/ibm/defender/bin/dcli eagle-agent stop
```

5. Optionally, the eagle agent service can be removed by running the **install-eagle-agent.sh** script with the **--remove** option. This script is contained within the `defender-agent-filename-tar.gz` compressed archive that is downloaded from IBM Storage Defender Data Management. Run the following script as sudo from the directory where this script is located:

```
sudo ./install-eagle-agent.sh --remove
```

Troubleshooting connection issues

An IBM Storage Protect server that is being managed by the IBM Storage Defender Data Management Service (Data Management) maintains connectivity to Data Management by using the eagle agent service that is running alongside the IBM Storage Protect server on the same host system. Data is periodically collected by the eagle agent service from the IBM Storage Protect server that uses the *ibm-eagle-agent-admin* administrator that was created with the **dcli server register** command during initial setup. This data is then processed and sent to Data Management.

The following listed issues are possible sources of connectivity issues with the architecture:

- The host system where the IBM Storage Protect server is running is down or inaccessible over the network by Data Management
- The IBM Storage Protect server is down or not accepting TCP/IP connections
- The eagle agent service is not running on the host system
- "The claim to Data Management is not available" on page 9

For these and other connectivity issues, log files for the eagle agent service can be found on the IBM Storage Protect host system in the following directories:

`/opt/ibm/defender/logs/`

`/opt/ibm/defender/wlp/usr/servers/defaultServer/logs/`

Additionally, the following **systemctl** command can help indicate the status of eagle agent components on the system:

```
systemctl status liberty@defaultServer.service
```

The log files that are contained in these directories and also in the output of the **systemctl** command should be provided to IBM Support for continued problem determination and resolution.

The host system where the IBM Storage Protect server is running is down or inaccessible

If the host system where the IBM Storage Protect server and eagle agent service are running is down or inaccessible over the Ethernet (TCP/IP) network, then Data Management is unable to communicate with and manage the system.

Procedure

1. Verify that the host system is powered on.
2. Check whether the host system can be reached over the network, which is used for connectivity to Data Management. For example, you can attempt to ping or SSH to the system.

The IBM Storage Protect server is down or not accepting TCP/IP connections

If the IBM Storage Protect server is down, halted, or unable to accept new TCP/IP connections, then the eagle agent service running on the host system will be unable to query the IBM Storage Protect server for data. Also the eagle agent service will be unable to send data to Data Management.

Procedure

1. Check to see whether the IBM Storage Protect server process is running on the host system. If the server process is not running, then start the IBM Storage Protect server.
2. Check to see whether it is possible to connect to the IBM Storage Protect server. For example, use the `dsmadmc` or `dsmc` client applications to connect to the IBM Storage Protect server.

The eagle agent service is not running on the host system

If the eagle agent service is not running on the host system where the IBM Storage Protect is running, then no monitoring and management of the IBM Storage Protect server by Data Management can take place.

Procedure

1. Login to the operating system terminal of the IBM Storage Protect server system with the non-root local user account that is used to run the IBM Storage Defender connection agent.
2. Run the **`dcli eagle-agent query`** command to query the status of the eagle agent service:

   ```
   /opt/ibm/defender/bin/dcli eagle-agent query
   ```

   Verify that the output shows the existence of a running process with a process ID (PID). For example, the following output shows a running process with PID 4111327:

   ```
   Query IBM Storage Protect Eagle-Agent
   =====================================
   Successful
   Claim ID: 1
   pid : 4111327
   Start : Tue Jan 23 14:06:38 MST 2024
   ```

   If the eagle agent service is not running, the following message should be displayed in the output:

   ```
   Query IBM Storage Protect Eagle-Agent
   =====================================
   The specified object was not found.
   ```

3. If the eagle agent service is not running, attempt to start it with the **`dcli eagle-agent start`** command:

   ```
   /opt/ibm/defender/bin/dcli eagle-agent start
   ```

4. Repeat step 2 to verify that the eagle agent service is running.

The claim to Data Management is not available

If the IBM Storage Protect server is not actively claimed to Data Management, then it will not be present in the list of managed clusters.

About this task

The claims might not have been created, might have been deleted, or might have been directed to the wrong tenant. This might occur due to the following reasons:

- The IBM Storage Protect server was never claimed to Data Management.
- The IBM Storage Protect server's claim to Data Management was deleted and/or the server was unregistered from Data Management.
- The IBM Storage Protect server's claim was to a different tenant within Data Management.

Procedure

1. If the IBM Storage Protect server was never claimed to Data Management, then follow the steps in the "Connecting an IBM Storage Protect server to Data Management" on page 3 section to connect the server to Data Management.

   a. Check for the existence of the **`/opt/ibm/defender/bin/dcli`** application on the IBM Storage Protect host system to verify that the connection agent has been installed.

   b. Login to the operating system terminal of the IBM Storage Protect server system with the non-root local user account that is used to run the Defender connection agent.

   c. Run the **`dcli claim query`** command to check for the existence of a claim to Data Management:

   ```
   /opt/ibm/defender/bin/dcli claim query
   ```

2. If the IBM Storage Protect server's claim to Data Management was deleted or removed, either due to an **Unregister** from the Data Management clusters view or with a **`dcli claim delete`**, then it is necessary to re-connect the IBM Storage Protect server to Data Management. This is also true in the case of the IBM Storage Protect server being claimed to another tenant.

   a. Follow the steps in the "Unregistering an IBM Storage Protect server" on page 5 section to ensure that any previous instance of the monitored IBM Storage Protect server is removed from Data Management.

   b. Follow the steps in the "Connecting an IBM Storage Protect server to Data Management" on page 3 section to reconnect the server to Data Management (for the correct tenant).

Command line reference for IBM Storage Defender connection agent

Use commands to manage claims for the IBM Storage Defender connection agent.

The IBM Storage Defender connection agent command-line interface (CLI) is a utility that is used to connect or "claim" an IBM Storage Protect server to IBM Storage Defender Data Management Service. When you download the Storage Defender *connection agent* from Data Management, the command-line utility is included in the download file.

Tip: To connect an IBM Storage Protect server to Data Management, you must first install the Defender connection agent on the IBM Storage Protect server, register the server with Data Management, and use the CLI to start a claim. For more information about connecting a server, see "Connecting an IBM Storage Protect server to Data Management" on page 3.

dcli

The **dcli** command starts the IBM Storage Defender command-line interface (CLI).

The IBM Storage Defender command-line interface (CLI) is a utility that is used to register an IBM Storage Protect server to an IBM Storage Defender Data Management Service. For more information about registering a server, see "Connecting an IBM Storage Protect server to Data Management" on page 3.

dcli claim

Use the **dcli claim** commands to register, query, or delete a claim for a registered IBM Storage Protect server.

dcli claim delete

Use this command to delete an existing claim for an IBM Storage Protect server.

Parameters

-i | --id ***claim_id***
Specifies ID of the claim. The default value is 1.

-a | --apiKey ***apiKey_id***
Specifies the API Key generated by the UI.

-h | --help
Displays help information for the command.

Example: Delete a claim

Delete a claim with a claim ID of 1.

```
dcli claim delete -i 1 -a 1ea2b61f-3d5a-4363-543c-d47e2812cf15
```

Related commands

Table 1. Commands related to ***dcli claim delete***

Command	Description
dcli claim query	Queries a claim for the IBM Storage Protect server.

dcli claim query

Use this command to return information about a claim post for an IBM Storage Protect server to Data Management.

Parameters

-i | --id ***claim_id***
Specifies the claim ID for a registered IBM Storage Protect server. The default value is 1.

-h | --help
Displays help information for the command.

Example: Display help topics

Display information about a claim that has an ID of "1".

```
dcli claim query 1
```

Related commands

Table 2. Commands related to ***`dcli claim query`***

Command	Description
“dcli claim register” on page 11	Starts a claim for an IBM Storage Protect Server.
“dcli claim delete” on page 10	Deletes a claim for an IBM Storage Protect Server.

dcli claim register

Use this command to register a Data Management claim for an IBM Storage Protect server.

Tip: Before you issue the **`dcli claim register`** command, you must register the IBM Storage Protect server by using the “dcli server register” on page 15 command.

Parameters

`-i | --id`
Specifies the server ID for a registered IBM Storage Protect server. The default value is 1.

`-t | --token`
Specifies the token that is created from the IBM Storage Defender page for this cluster.

`-h | --help`
Displays help information for the command.

Example: Register a claim

Register a claim that has a registered IBM Storage Protect server ID of "1".

```
dcli claim register -i 1 -t
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc3MiOiJIZWxpb3MiLCJleHAiOjE3MDg5NjIxOTcsIm5iZiI6MTcwODk
2MTI5NywiaWF0IjoxNzA4OTYxMjk3LCJqdGkiOiI4ZmNlNTUwOS1kOGE4LTRlMTUtOGJkZS1kN2FkZDQ4NjIyNmMiLCJhc3N
ldF90eXBlIjo3LCJzZl9hY2NvdW50X2lkIjoiMDAxN0EwMDAwMHlqSEZnUUFNIiwiaGVsaW9zX3VybCI6Imh0dHBzOi8vdXN
lYS1zYW5kYm94LnN0b3JhZ2UtZGVmZW5kZXIuaWJtLmNvbSIsImhlbGlvc19kYXRhX3VybCI6InVzZWEtc2FuZGJveC1kYXR
hLnN0b3JhZ2UtZGVmZW5kZXIuaWJtLmNvbTo0NDMiLCJzZmRjX2NpZCI6IjNNVkc5M01HeTlWOGhGOU02VU9tU3BZRnNIZUw
wVl81bG42Lmljc2VsMzZ4TnF4ZHF2Y01OZmNMQV8zTWNJZ0o0YTFOOFBVdlloYktmUXNad2lJcnkiLCJzc29fdXJsIjoiaHR
0cHM6Ly9jb2hlc2l0eS0tYXF1YS5zYW5kYm94Lm15LnNpdGUuY29tL3N1cHBvcnQifQ.RQ3rIIE7kSO3_PQ4plEkHYpQAm05
24tsh9MZHQXbJlA
```

```
Register Claim
==============
Successful
Claim ID : 1
SP ID    : 1
Name     : server1
TimeStamp: Thu Feb 29 07:02:08 MST 2024
URL      : https://usea-prod.storage-defender.ibm.com
```

Field descriptions

Claim ID
The ID for claim.

SP ID
The ID for the IBM Storage Protect server.

Name
The user-specified nickname for the IBM Storage Protect server.

Timestamp
The date and time that the IBM Storage Protect server was registered.

URL
The address of the Data Management environment to which the IBM Storage Protect server is registered.

Related commands

Table 3. Commands related to ***`dcli claim register`***

Command	Description
dcli server register	Registers an IBM Storage Protect server.

dcli eagle-agent

Use the **`dcli eagle-agent`** commands to start, stop, or determine the status of the eagle agent.

After you connect an IBM Storage Protect server to Data Management by using the Defender connection agent, the IBM Storage Defender eagle agent service is used to send and receive data between the IBM Storage Protect server and Data Management.

dcli eagle-agent query

Use this command to query the status of the eagle agent.

Parameters

`-h | --help`
Displays help information for the command.

Example: Query the status of the eagle agent

```
dcli eagle-agent query
```

Related commands

Table 4. Commands related to ***`dcli eagle-agent query`***

Command	Description
"dcli eagle-agent start" on page 12	Starts the eagle agent.
"dcli eagle-agent stop" on page 13	Stops the eagle agent.

dcli eagle-agent start

Use this command to start the eagle agent.

Parameters

`-h | --help`
Displays help information for the command.

Example: Start of the eagle agent

```
dcli eagle-agent start
```

Related commands

Table 5. Commands related to ***`dcli eagle-agent start`***

Command	Description
"dcli eagle-agent query" on page 12	Query the status of the eagle agent.

Command	Description
“dcli eagle-agent stop” on page 13	Stops the eagle agent.

Table 5. Commands related to ***dcli eagle-agent start*** *(continued)*

dcli eagle-agent stop

Use this command to stop the eagle agent.

Parameters

-h | --help
Displays help information for the command.

Example: Stop the eagle agent

```
dcli eagle-agent stop
```

Related commands

Table 6. Commands related to ***dcli eagle-agent stop***

Command	Description
“dcli eagle-agent query” on page 12	Query the status of the eagle agent.
“dcli eagle-agent start” on page 12	Starts the eagle agent.

dcli server

Use the **dcli server** commands to manage registration of an IBM Storage Protect server to Data Management.

dcli server delete

Use this command to delete the registration of an IBM Storage Protect server.

When you issue the **dcli server delete** command, the registration for an IBM Storage Protect server is deleted. The administrative user that is named *ibm-eagle-agent-admin* is also deleted from the IBM Storage Protect server.

Parameters

-i | --id *server_id*
Specifies the ID for the registered IBM Storage Protect server. The default value 1.

-a | --admin *admin_name*
(Required) Specifies the IBM Storage Protect server administrator name that can authorize deletion of the server registration with Data Management.

-p | --password *admin_password*
Specifies the IBM Storage Protect server administrator password.

-t | --truststore-password *truststore_password*
Specifies the truststore password.

-m | --prompt-password
Specifies whether to prompt for the IBM Storage Protect server administrator password from the command-line.

-d | --address *ip_address*
Specifies the IP address or hostname for the IBM Storage Protect server.

-o | --port*port_number*
Specifies the port number for the IBM Storage Protect server. The default value is 1500.

-y | --yes
Specifies "yes" for all yes/no prompts that are displayed when the command runs.

-h | --help
Displays help information for the command.

Example: Delete a server

Delete an IBM Storage Protect server by specifying admin "harry" and password "secret".

```
dcli server delete -admin harry -password secret
```

Related commands

Table 7. Commands related to ***dcli server delete***

Command	Description
dcli	Registers an IBM Storage Protect server.
dcli server query	Displays information about a registered IBM Storage Protect server.

dcli server query

Use this command to display information about a registered IBM Storage Protect server.

Parameters

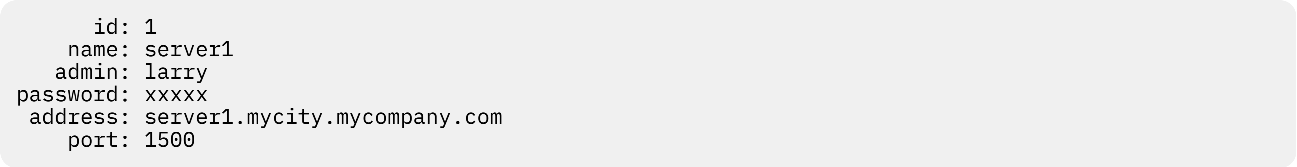
-i | --id *server_id*
Specifies the ID for the registered IBM Storage Protect server. The default value 1.

-h | --help
Displays help information for the command.

Example: Query a server

Display information about an IBM Storage Protect server.

```
dcli server query
```



```
      id: 1
    name: server1
   admin: larry
password: xxxxx
 address: server1.mycity.mycompany.com
    port: 1500
```

Field descriptions

id
The ID for the IBM Storage Protect server.

name
The user-specified nickname for the IBM Storage Protect server.

admin
The new administrative user named *ibm-eagle-agent-admin* that is created on the IBM Storage Protect server after the **dcli server register** command runs.

password:
Specifies the password for the IBM Storage Protect server administrator.

address:
Specifies the IP address for the IBM Storage Protect server.

port:
Specifies the port number for the IBM Storage Protect server.

Related commands

Table 8. Commands related to ***`dcli server query`***

Command	Description
dcli	Registers an IBM Storage Protect server.
dcli server update	dcli server update

dcli server register

Use this command to register an IBM Storage Protect server to IBM Storage Defender Data Management Service.

The **`dcli server register`** command is used for the initial registration of an existing IBM Storage Protect server to Data Management. For more information, see "Connecting an IBM Storage Protect server to Data Management" on page 3.

Parameters

`-a | --admin` ***admin_name***
(Required) Specifies the IBM Storage Protect server administrator name that is used to authorize the server registration to Data Management. The administrator must have system privilege on the IBM Storage Protect server.

`-p | --password` ***admin_password***
Specifies the IBM Storage Protect server administrator password.

`-m | --prompt-password`
Specifies whether to prompt for the IBM Storage Protect server administrator password from the command-line.

`-d | --address` ***ip_address***
(Required) Specifies the IP address or hostname for the IBM Storage Protect server.

`-o | --port`***port_number***
Specifies the port number for the IBM Storage Protect server. The default value is 1500.

`-n | --name` ***server_nickname***
(Required) Specifies a user-specified nickname for the IBM Storage Protect server that will be displayed in Data Management.

`-t | --truststore-password` ***truststore_password***
Specifies the truststore password.

`-c | --oc-url` ***operations_center_url***
Specifies the IP address or hostname for the registered IBM Storage Protect Operations Center.

`-y | --yes`
Specifies "yes" for all yes/no prompts that are displayed when the command runs.

`-h | --help`
Displays help information for the command.

Example: Register a server

Register an IBM Storage Protect server by specifying server name "server1" at address "server1.mycity.mycompany.com" and port "1500". Specify admin "Larry", password "myp@ssword", and truststore password "secretpassword".

```
dcli server register --address server1.mycity.mycompany.com --port 1500 --name server1 --admin
larry -password myp@ssword --truststore-password secretpassword
```

```
Register Server
===============
Successful
       id: 1
     name: server1
    admin: larry
  address: server1.mycity.mycompany.com
     port: 1500
clusterID: 8094343462909
timestamp: Mon May 15 12:04:09 EDT 2023
```

Field descriptions

ID
The ID for the IBM Storage Protect server.

Name
The user-specified nickname for the IBM Storage Protect server.

Admin
The new administrative user named *ibm-eagle-agent-admin* that is created on the IBM Storage Protect server after the **`dcli server register`** command runs.

Address
The IP address or hostname for the IBM Storage Protect server.

Port
The port number for the IBM Storage Protect server.

ClusterID
The cluster ID number that is assigned to the IBM Storage Protect server.

Timestamp
The date and time that the IBM Storage Protect server was registered.

Related commands

Table 9. Commands related to ***`dcli server register`***

Command	Description
dcli	Starts the IBM Storage Defender command-line interface (CLI).
dcli server delete	Deletes a registered IBM Storage Protect server.
dcli server query	Displays information about a registered IBM Storage Protect server.
dcli server register	Registers an IBM Storage Protect server.
dcli server update	Updates an IBM Storage Protect server registration.
dcli server updateuser	Updates an IBM Storage Protect server user.

dcli server update

Use this command to update the registration for an IBM Storage Protect server.

The **`dcli server update`** command is used to update the address, port, or name of an IBM Storage Protect server that is registered to Data Management.

Parameters

`-i | --id` ***server_id***
Specifies the ID for the registered IBM Storage Protect server. The default value 1.

`-d | --address` ***ip_address***
Specifies the IP address or hostname for the IBM Storage Protect server.

`-o | --port`***port_number***
Specifies the port number for the IBM Storage Protect server. The default value is 1500.

`-n | --name` ***server_nickname***
(Required) Specifies a user-specified nickname for the IBM Storage Protect server that will be displayed in Data Management.

`-c | --oc-url` ***operations_center_url***
Specifies the IP address or hostname for the registered IBM Storage Protect Operations Center.

`-h | --help`
Displays help information for the command.

Example: Update a server

Update a registered IBM Storage Protect server to use port "1500".

```
dcli server update -port 1500
```

Related commands

Table 10. Commands related to ***`dcli server update`***

Command	Description
dcli	Registers an IBM Storage Protect server.
dcli server query	Displays information about a registered IBM Storage Protect server.

dcli server updateuser

Use this command to update the user for a registered IBM Storage Protect server.

Parameters

`-i | --id` ***server_id***
Specifies the ID for the registered IBM Storage Protect server. The default value 1.

`-a | --admin` ***admin_name***
(Required) Specifies the IBM Storage Protect server administrator name.

`-p | --password` ***admin_password***
Specifies the IBM Storage Protect server administrator password.

`-m | --prompt-password`
Specifies whether to prompt for the IBM Storage Protect server administrator password from the command-line.

`-t | --truststore-password` ***truststore_password***
Specifies the truststore password.

-y | --yes
Specifies "yes" for all yes/no prompts that are displayed when the command runs.

-h | --help
Displays help information for the command.

Example: Update the user for a registered server

Update the IBM Storage Protect server administrator named "Harry", and specify a password of "secret".

```
dcli server updateuser -a harry -p secret
```

Related commands

Table 11. Commands related to ***dcli server updateuser***

Command	Description
dcli	Registers an IBM Storage Protect server.

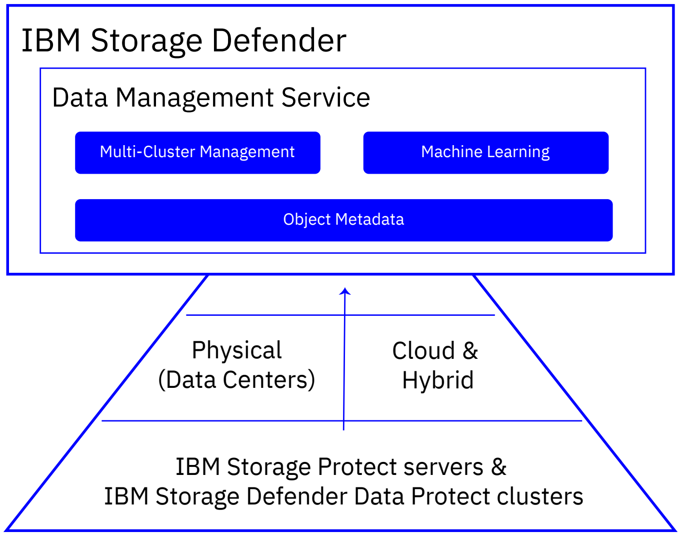
Chapter 3. Managing IBM Storage Defender Data Protect connections

To manage your clusters in Data Management, you must follow the steps to connect your clusters to Data Management. You must use the login credentials for the *cluster management account*, which are the credentials that were originally used to register with IBM Storage Defender. After your clusters are connected, Data Management starts monitoring your clusters to detect ransomware attacks. For more information, see Detect Ransomware Attacks.

Note: To connect a cluster to Data Management, additional configuration might be required. In some cases, Data Management determines that an external cluster is running inside the Data Management network based on DNS information it receives, and incorrectly configures an internal Data Management connection. To work around this issue, you might need to download and run a script.

IBM Storage Defender Data Management Service provides multi-cluster management of your Data Protect clusters along with your IBM Storage Protect servers. By registering or claiming Data Protect clusters and IBM Storage Protect servers to Data Management, you can easily view the overall health of your environment and manage your backup operations. Machine learning is applied to assist with detecting issues, monitoring the health of your environment, and alerting you about potential issues.

The following image shows clusters and IBM Storage Protect servers that are connected to Data Management:



Connecting a cluster to Data Management

Before you begin

Before you can log in to the cluster for the first time, you must define and create the cluster in IBM Storage Defender Data Protect.

To complete this procedure, you must use the login credentials for the *cluster management account*, which are the credentials that were originally used to register with IBM Storage Defender.

About this task

Connecting a cluster to Data Management is also referred to as a *claim*. A *claim* is the process of defining a cluster to Data Management.

© Copyright IBM Corp. 2023, 2024

Procedure

To connect a cluster to Data Management, complete the following steps:

Important: When you create a new Data Protect cluster, you will not be able to view and manage the cluster in IBM Storage Defender Data Management Service until you complete the steps in this procedure.

1. After you initiate the Data Protect cluster creation process, wait until the cluster login page is available. Click the URL that is displayed on the **Cluster Setup Status** page, but do not log in.
2. Before you log in, claim the required cluster by completing one of the following procedures:

   - To claim the Cohesity Data Protect 7.1.1 or later cluster by using token-based claim, complete the following steps:

     a. Log in to Data Management and navigate to **All Clusters > Settings > Access Management**.

     b. Click the **Tokens** tab.

     c. Click the **Create** button in the upper right corner of the screen.

        On the **Create Token** window, specify any name in the **Name** field for the token that you are generating. For the **Type** field, select **Cohesity** from the drop-down. Then select **Create**, which creates the token.

        Before closing the **Create Token** window, copy the token by selecting the copy icon.

     d. Download `iris_cli` to a Mac, Linux, or the system that includes Windows subsystem for Linux.

        Note: This step is not required for Cohesity Data Protect 7.2 and later versions.

        To download `iris_cli` for Mac, you can download `iris_cli` from the https://*CLUSTERIP*/files/bin/cli/darwin-x86_64/iris_cli. For Linux or the system that includes Windows subsystem for Linux, the `iris_cli` can be downloaded from https://*CLUSTERIP*/files/bin/cli/linux-x86_64/iris_cli.

        where in the URLs, you must replace CLUSTERIP with the TCP/IP address of one of the cluster nodes to download `iris_cli`.

        And then, run the **`iris_cli`** command against the Cohesity Data Protect cluster to enable token-based claim feature flag:

        ```
        iris_cli -server CLUSTERIP cluster update-feature-flag feature-flag-
        name=heliosTokenClaimEnabled is-approved=true is-ui-feature=true reason="Use token
        based claim"
        ```

     e. Sign in to Cohesity Data Protect cluster

     f. Click the H icon on the navigation menu.

     g. Paste the Token key that is created in step 2.c., then click **Connect** button.

     h. To verify that the cluster was successfully connected, log in to Data Management and navigate to **All Clusters > Settings > Clusters**. The Cluster Management page is displayed.

        If the cluster connection is successful, the Connection column displays the Connected status with green checkmark icon for the cluster.

   - To associate any cluster older than Cohesity Data Protect 7.1.1 with Data Management, you must run the `claim_to_ibm` script by completing these steps:

     a. Download the `claim_to_ibm.tar` script from IBM Documentation by right-clicking claim_to_ibm.tar and saving it to the `Downloads` directory on your local system.

        Note: The `claim_to_ibm.sh` script runs on Linux, Mac OS X, and Windows Subsystem for Linux. This script uses cURL, which is an open source REST command-line tool that can be downloaded from the internet at no cost.

     b. Install `cURL`. To check whether `cURL` is already installed, issue the command `curl -V` from the terminal. If a version number is returned, `cURL` is already installed.

c. Extract the `claim_to_ibm.tar` file that you downloaded in step 2.a. by issuing the following command from the terminal:

```
tar xvf claim_to_ibm.tar
```

d. Run the `claim_to_ibm.sh` script by issuing the following command from the terminal:

```
./claim_to_ibm.sh -s=cluster_ip_address
```

where `cluster_ip_address` is the IP address for the cluster.

Example:

```
./claim_to_ibm.sh -s=mycluster.mycompany.com
```

Tip: If you previously logged in to the cluster and changed the default password, use the **-p** parameter to specify your updated password.

Example:

```
./claim_to_ibm.sh -s=mycluster.mycompany.com -p=NewPassword
```

where `NewPassword` is your updated password.

e. When the script is run, a cluster URL is displayed.

3. From a web browser, open the cluster URL and refresh the page.

   - If you previously logged in to the cluster URL and you already changed the default password, complete the following steps:

     a. Sign in to the cluster by entering your credentials.

     b. Click the H icon on the navigation menu and then click **Register with Helios**.

     c. On the **Helios** page, click the **Connect to Helios** toggle to **Enable** a connection.

     d. Skip to step "4" on page 21.

   - If this is your first time signing in, complete the following steps:

     a. Sign in by using the default credentials:

        - **Username:** admin
        - **Password:** admin

     b. Review and accept the **End User License Agreement**.

     c. From the **Cluster Management** page, select **Manage in Helios SaaS** and click **Connect to Helios**.

     d. From the **License** page, select **Full Access Permissions**, and click **Continue**.

     e. Continue to step "4" on page 21.

4. From the **Cohesity Support Portal** page, click **MyCohesity Login**. Specify the login credentials for the *cluster management account*.

   Important: To log in and associate a cluster with Data Management, you must specify the *cluster management account* credentials that were originally used to register with IBM Storage Defender. You cannot connect a cluster to Data Management by using any other credentials.

5. You are prompted to change the default password.

   The **Summary** page for the Data Protect cluster is displayed.

6. To verify that the cluster was successfully connected, log in to Data Management and click **Settings** > **Clusters**. The **Cluster Management** page is displayed.

   If the cluster connection was successful, the **Connection** column displays a **Connected** ✓ status for the cluster.

7. Repeat this procedure on each cluster that you want connected to Data Management.

Disconnecting a cluster

Procedure

1. Log in to the Data Protect cluster that you want to disconnect from Data Management.

   Important: To log in to Data Management, you must specify the *cluster management account* credentials that were originally used to register with IBM Storage Defender. You cannot log in to a Data Protect cluster by using any other credentials.

2. In the Data Protect dashboard, as a user with administrative privileges, click the H icon on the navigation menu and click **Manage Connection**.
3. **Connect to Helios**—Turn off the **Enable** toggle.

   Access to the cluster in Data Management is immediately disabled.

Unregistering a cluster

If a cluster is no longer in use, you can unregister the cluster from Data Management.

Procedure

1. Log in to IBM Storage Defender and from the **IBM Storage Defender** menu, navigate to **Data Management > Overview > Launch Data management**.
2. Click on the cluster's drop-down menu in the left side panel and select **All Clusters** for a view of all clusters.
3. Click **Settings** > **Clusters**.

   The **Cluster Management** page is displayed.
4. From the list of available clusters, click the ⋮ icon for the cluster that you want to unregister from Data Management.
5. Select the **Unregister** option. The **Unregister** window is displayed, along with the following message:

   "Are you sure you want to unregister the clusters from Data Management?"
6. Click **Unregister**.

Troubleshooting connection issues

The Data Management icon on the navigation menu of the Data Management dashboard contains a red triangle ⚠ if there is an issue with Data Management. Click the icon and then select **View alert details**. The **Alerts** page opens and lists one or more alerts for Data Management issues. Click the alert link for more detailed information.

Note: When you upgrade the software for a single node cluster, the cluster temporarily disconnects from Data Management to apply the software update. While the software update is in progress, Data Management reports an error for the cluster. When the software update is complete, the cluster reconnects to Data Management and resumes to normal status after several minutes.

If you experience issues while connecting to Data Management, clear your browser cache and try reloading the page again.

Chapter 4. Getting started

- By default, the Data Management Dashboard provides a consolidated view of all your Data Management enabled clusters.
- To switch between all clusters and a single cluster, click **All Clusters** from the navigation menu.
- The items in the navigation menu can change depending on whether **All Clusters** or a single cluster is selected. For example, the **Infrastructure** menu option is only available if a single cluster is selected.
- The **Settings** icon ⚙ provides several administrative functions, such as cluster upgrades, access management, licensing, and cloud deployment.
- The help icon ? in the dashboard menu displays information appropriate to the current cluster, based on the software version that is running on the cluster.

Consumption tile

The Consumption tile now presents aggregated data from both IBM Storage Defender Data Protect and IBM Storage Protect clusters that are claimed and managed through IBM Storage Defender Data Management Service (Data Management Service).

To view the consumption tile, login to the Data Management Service and click **Launch Data management > Summary**.

The Consumption tile displays the current data that is consumed and the space that is saved by using data deduplication and data compression.

The tile displays the following details:

- Logical Data — The combined total of data in the objects that are protected.
- Total — The total physical capacity of all storage devices after subtracting the space reserved for software operations.
- Available — The amount of space still available on the cluster(s).
- Reduction — The ratio of Logical Data to Storage Consumed. This reflects all operations that are performed on source data, which includes snapshotting, change tracking and ingest, data deduplication, data compression, and data resiliency.

Chapter 5. Reporting

IBM provides one-stop-shop reporting on IBM Storage Defender Data Management Service. You have an aggregated view of your IBM deployment regardless of the use case, workload, or deployment type (on-premises, consumed as an IBM-hosted service, or a combination).

The built-in reports are designed to address your most common use cases and are available for immediate use. You can view an overall summary of your data protection jobs and storage systems, or you can analyze data at the granular level by using powerful filtering options. You can filter, schedule, email, and download reports.

Note: If you log in to Data Management by using SSO and your user account is not available on the **Access Management** page, then you cannot schedule reports.

The report that you schedule or download inherits the filters that you applied.

Viewing reports

View reports in Data Management to help you analyze and improve user experience.

Procedure

To view a report in Data Management, follow the procedure:

1. Log in to Data Management.
2. Click **All Clusters** from the navigation menu.
3. From the navigation menu, click **Reporting**.

   By default, the **Library** tab is displayed.
4. Click a report card. For more information, see Choose a Report Type.

   Each report helps you view, visualize, and analyze data. The following table describes the key features of Data Management reports:

Name	Description
Filters	Each report provides various filters that help you pare down the report until it shows only the data that you want in the report. The filter options change depending on the type of report. For more information, see Filter Report Data.
Glance bar	The glance bar provides a summary of the report for the time period that you specify in the filter.
Charts	Each report includes charts that provide a graphical representation of data.
Data table	The Data table in the report provides deeper insights to help you analyze the data. You can customize the columns in the table. For more information, see Customize Table Columns.

© Copyright IBM Corp. 2023, 2024

Name	Description
Common tasks	You can complete the following tasks: a. Download Reports b. Schedule Reports c. Manage Scheduled Reports d. Reset to Default View

Choosing a report type

Choose a report type to help you identify information that you need.

Currently, 15 built-in reports are available in IBM Storage Defender Data Management Service:

- Failures
- Protected Objects
- Protected / Unprotected Objects
- Protection Activities
- Protection Group Summary
- Protection Runs
- Recovery
- System Connections
- System Protection
- Storage Consumption by System
- Storage Consumption by Protection Groups
- Storage Consumption by Objects
- Storage Consumption by Storage Domains
- Storage Consumption by Views
- Data Transferred to External Targets

Filtering report data

Reporting in Data Management provides a comprehensive view of the data under management.

You have full control over the data that you choose to include and view in your reports. Use the filters to pare down your report until it shows only the data that you want in the report. The filter options change depending on the type of report.

Customizing table columns

Each report in Data Management provides comprehensive data. In each report, data is displayed in a tabular format. You can add and remove columns from the **Data** table. The changes that you make to columns in a table persist until you change them again or until you restore the report to the default view.

Procedure

To customize table columns, complete the following steps:

1. Launch Data Management.
2. Select **All Clusters** from the navigation menu.
3. Click **Reporting**.
4. Click a report card.

5. From the table, click the **Settings** ⚙ icon.
    - To add a column, enable the toggle.
    - To remove a column, disable the toggle.

Downloading reports

Download reports in different file formats from the Data Management reports page.

On any report, click the **Download** icon ⇩ and select one of the following file formats: PDF, Excel, or CSV.

The report in the selected file format gets downloaded to your system.

Note: The time taken to generate a report depends on multiple factors such as the number of clusters selected, other filters applied on the report, and the amount of data. If the report is large, it might take a few moments to download the report.

Scheduling reports

You can schedule reports to run at periodic intervals. After you select a report and filter the scope, you can schedule the report to run and send an email to recipients at specified times.

Before you begin

Important:

- SSO users can view and download reports. To schedule reports, SSO users must be explicitly added in Data Management. For more information about explicitly adding users, see Managing users.
- If the report is too large, the email contains a download link instead of an attachment.
- The columns that are included in the scheduled report are the columns available in the default view. If you customized the table, those changes are not reflected in the scheduled report.

Procedure

1. Log in to Data Management.
2. Click **All Clusters** from the navigation menu.
3. Click **Reporting**. By default, the **Library** tab is displayed.
4. Click a report card. For more information, see Choose a Report Type.
5. Click **Schedule**.

    Note: If the SSO user is not explicitly added in Data Management, the **Schedule** button is not displayed.

    The **Schedule Report** window is displayed.
6. Configure the following details in the **Schedule Report** window:

    Schedule Name
    Enter a name for your report.

    Schedule
    Choose the frequency and the time at which to run the report.

    Recipients
    Enter the email address of the recipient. You can enter multiple email addresses.

    Email Subject
    Enter a subject line for the email.

    Format
    Select the formats. The recipients receive the report in the format that you select.
7. Click **Schedule**.

The recipients receive a new email with the updated report on the schedule that you selected. See your scheduled reports under the **Scheduled** tab on the **Reporting** page.

Managing scheduled reports

You can view and manage the scheduled reports in Data Management.

About this task

You can complete the following tasks from the **Scheduled** tab:

- Instantly run a report
- Pause a report
- Modify the settings of a report
- Delete a report

Note: Users with the **Super Admin** role can view and manage all scheduled reports in the same Data Management account.

Procedure

1. Login to Data Management.
2. Click **All Clusters** from the navigation menu.
3. Click **Reporting**.
4. Click the **Scheduled** tab.
5. Hover over a report and click the **Actions** menu (⋮):
   - Select **Run Now** to instantly run and email the report.
   - Select **Pause** to pause the schedule.
   - Select **Edit** to modify the settings of a scheduled report. Update the settings as necessary and click **Schedule**.
   - Select **Delete** to delete a scheduled report. To confirm the deletion, you must click **Delete**.

Resetting reports to the default view

After you filter a report or customize table columns, you can reset the report to the default view.

To switch to the default Data Management reports page view, click **Restore to default display** icon 🗎. The page refreshes and reverts to the default view.

Reporting APIs

The IBM Storage Defender Data Management Service architecture is API driven. You can programmatically interface with the Data Management Reporting service.

For more information about using Data Management Reporting APIs, click the Help Center icon ? from the menu and select **Get REST APIs**.

Failures

The **Failures** report provides a summary and list of objects that had one or more backup run failures. It also helps you identify consecutive failures in the last three backups, and breaks down the failed objects by object type.

Example use case: Which object do I have no successful backup of in the last week?

Filter Report Data

The report supports multiple filters to pare down the data that you want to view in the report:

- **System**—Select all clusters to include.
- **Source**—Select all the sources to include.
- **Type**—Choose the types of objects to include — such as Generic NAS, Isilon, NetApp, Physical, Pure, VMware.
- **Time Range**—Set the time period for your report.
- **Object**—Enter an object name to filter by object name.

Glance Bar

The glance bar provides a summary of the report for the specified period:

- **Total Sources**—The total number of sources.
- **Total Objects**—The total number of objects.
- **Failed Objects**—The total number of objects that experienced one or more backup run failures during the specified date range.
- **Without Snapshots**—The total number of objects without any snapshots.

Charts

The report includes the following two charts:

- **Failures in Last 3 Backups**
- **Success and Failed Objects by Object Type**

Report Data

The following table describes the data that is displayed in the **Data** table. Use the search bar to filter the data by object name, source, system name, or policy.

You can add or remove columns. For more information, see Customize table columns. The data that is displayed in the **Policy** and **System** columns are from the last backup run of the object in the specified time period.

Column Name	**Description**
Object Name	The name of the object.
Source	The hostname or IP address of the registered source.
System	The name of the cluster on which the protection job was run.
Policy	The protection policy associated with the Protection Group.
Last Failed Run	The date and time at which the last backup run failed.
Failed Backups	The total number of backup runs that failed.
Failures in Last 3 Backups	The total number of failures in the last three backups.
Last Fail Reason	The reason for the failure of the last backup.

Protected objects

The **Protected Objects** report provides a summary and list of all protected objects that had a backup run. You can view the backup status and the objects with an active snapshot.

Example use case: Do I have a good backup of my VM in the last month?

Filter Report Data

The report supports multiple filters to pare down the data that you want to view in the report:

- **System**—Select all clusters to include.
- **Source**—Select all the sources to include.
- **Type**—Choose the types of objects to include — Generic NAS, Isilon, NetApp, Physical, Pure, VMware, and so on.
- **Backup Status**—Filter by objects with successful backups or unsuccessful backups.
- **Last Run Status**—Filter by the status of the most recent protection run — Canceled, Failed, Running, Success, and/or Warning.
- **Time Range**—Set the time period for your report.

  If you set a time period, the report displays all objects that had a backup run during the selected time period. If an object is no longer protected, the report would still display data if the object had a backup run during the selected time period. If an object is protected and if it did not have a backup run during the selected time period, the report does not display the data specific to this object.
- **Object**—Enter an object name to filter by the name of the object.
- **Organization**—Choose one or more organizations to see the report data specific to the selected organizations.

Glance Bar

The glance bar provides a summary of the report for the specified period:

- **Success Rate**—**Without Successful Backup** / **Total Objects**.
- **Total Objects**—The total number of objects.
- **With Successful Backup**—The total number of objects that have one or more successful backups.
- **Without Successful Backup**—The total number of objects that did not have any successful protection runs.
- **With Snapshots**—The total number of objects with snapshots retained. This number can differ from the earlier “With Successful Backups”, for example, all backups fail for an object during the selected date range but the object still has actively retained snapshots from earlier backups (that occurred before the selected date range).
- **Without Snapshots**—The total number of objects without snapshots.

Charts

The report includes the following two charts:

- **Protected Objects by Type**
- **Object Protection by Type**

Report Data

The following table describes the data displayed in the **Data** table. Use the search bar to filter the data by object name, system name, source, or policy.

You can add or remove columns. For more information, see Customize table columns.

Column Name	Description
Object Name	The name of the protected object.
Source	The hostname or IP address of the registered source.
Policy	The protection policy associated with the latest run of the object.
Last Run	The date and time at which the last backup for the object ran.
Last Successful Backup	The date and time at which the last successful backup for the object ran.
Active Snapshots	The total number of active snapshots for the object.
Successful Backups	The total number of successful backups for the object.
Unsuccessful Backups	The total number of unsuccessful backups for the object.
System	The name of the cluster on which the object had the latest run.

Protected or unprotected objects

The **Protected / Unprotected Objects** report provides a summary and list of objects along with their protection status.

You can identify objects that are not associated with a Protection Group. The report does not contain data about IBM views.

Example use case: Are all the objects in my vCenter protected?

Filter Report Data

The report supports multiple filters to pare down the data that you want to view in the report:

- **System**—Select all clusters to include.
- **Source**—Select all the sources to include.
- **Type**—Choose the types of objects to include — Generic NAS, Isilon, NetApp, Physical, Pure, VMware, and so on.
- **Protection Status**—Filter by object protection status — Protected or Unprotected.
- **Object**—Enter an object name to filter by the name of the object.
- **Organization**—Choose one or more organizations to see the report data specific to the selected organizations.

Glance Bar

The glance bar provides a summary of the report for the specified period:

- **Protected Objects**—The percentage of **Protected Objects** to **Total Objects**.
- **Total Sources**—The total number of sources.
- **Total Objects**—The total number of objects.
- **Protected Objects**—The total number of protected objects.

- **Unprotected Objects**—The total number of unprotected objects.

Charts

The report includes the following two charts:

- **Protection Status by Type**
- **Unprotected Objects by Source**

Report Data

The following table describes the data displayed in the **Data** table. Use the search bar to filter the data by object name, protection status, source, or system name.

You can add or remove columns. For more information, see Customize table columns.

Column Name	Description
Object Name	The name of the object.
Protection Status	The protection status of the object.
Source	The name of the registered source.
System	The name of the cluster on which the object is registered.
Logical Data	The combined total of data in the objects that are protected by Data Management. These metrics are different depending on workload type. • VMs—The data size reported by VMware is the provisioned amount, not the actual data residing in the VM. For example, if a VM is provisioned for 1 TB but contains only 100 GB of data, VMware reports it as 1 TB. • All Other Workloads—The data size reported is the actual front end data residing on the server. If a server with 1 TB capacity contains 100 GB of data, the server reports 100 GB. Data Management does not include unprotected objects in these metrics. Currently, the logical data value shown on the Data Management Dashboard is a sum of the logical data values captured across all the protection runs. For instance, if the source has 100 GB of logical data, and assuming it remains at 100 GB for the first 10 protection runs, Data Management would report, after 10 runs, the Logical Data to be 1000 GB (1 TB).
Organization	The name specified for the organization when added to the cluster.

Protection Activities

The **Protection Activities** report displays a summary and list of all the protection activities. The report displays details about all the archival, backup, and replication activities per object per run. The report provides a breakdown of the statuses of all protection activities and the status of these activities based on the object type.

Example use case: How many backup activities met the SLA?

Filter Report Data

The report supports multiple filters to pare down the data that you want to view in the report:

- **System**—Select all clusters to include.
- **Organization**–Choose one or more organizations to see the report data specific to the selected organizations.
- **Type**—Choose the types of objects to include — Generic NAS, Isilon, NetApp, Physical, Pure, VMware, and so on.
- **Run Status**—Filter by status of the protection run — **Canceled**, **Failed**, **Running**, **Success**, and/or **Warning**.
- **SLA Status**—Filter by status of the SLA — Met or Missed.

Note: SLA is applicable only for backup runs. If you filter the data by **SLA Status**, only backup runs are listed.

- **Activity Type**—Filter by activity type — Archive, Backup, and/or Replication.

Note: The report displays data specific to replication runs only if Data Management manages both primary and secondary clusters.

- **Time Range**—Set the time period for your report.

Glance Bar

The glance bar provides a summary of the report for the specified period:

- **Success Rate—Total Successful /Total Runs.**
- **Total Runs**—The total number of protection runs.
- **Total Successful**—The total number of successful runs.
- **Success**—The total number of protection runs with status Success.
- **Warning**—The total number of protection runs with status Warning.
- **Failed**—The total number of protection runs with status Failed.
- **Canceled**—The total number of protection runs with status Canceled.
- **Running**—The total number of protection runs with status Running.
- **SLA Met**—The total number of protection runs that met SLA.
- **SLA Missed**—The total number of protection runs that missed SLA.

Charts

The report includes the following two charts:

- **Run Status by Activity Type**
- **Run Status by Type**

Report Data

The following table describes the data that is displayed in the **Data** table. Use the search bar to filter the data by protection group name, policy, system name, activity type, target, or SLA.

Note: You can add or remove columns. For more information, see Customize table columns.

Column Name	Description
Start Time	The date and time at which the recovery task started.
Duration	The time taken by the recovery task.
End Time	The date and time at which the backup run ended.
Group Name	The name of the Protection Group
Policy	The protection policy associated with the Protection Group.
System	The name of the cluster on which the recovery task was run.
Activity Type	The type of protection activity such as archival, backup, or replication
Target	The target on which the data is archived or replicated.
SLA	Indicates whether the backup run met or missed the SLA **Note:** SLA is not applicable for archival and replication activities.
Data Read	Size of the set of protected objects as read by IBM Storage Defender for a single backup run. This number is a per protection run statistic and is not additive across backup runs. **Note:** Data Read is applicable only for the activity type 'Backup'.
Data Written	Data written on the IBM Storage Defender platform after the unique logical data has been reduced by data deduplication and data compression. **Note:** • This number reflects unique data that is written before resiliency operations. • l Data Written is applicable only for the activity type 'Backup'.
Organization	The name specified for the organization when added to the cluster.

Note: Logical Data Transferred and Physical Data Transferred are applicable only for the activity types 'Archival' and 'Replication'.

Protection Group Summary

The **Protection Group Summary** report provides a summary and list of all Protection Groups that had a backup run. You can view the Protection Groups with successful and unsuccessful backups.

Example use case: Do I have a good backup of the Protection Group in the past 24 hours?

Filter Report Data

The report supports multiple filters to pare down the data that you want to view in the report:

- **System**—Select all clusters to include
- **Source**—Select all the sources to include
- **Type**—Choose the types of objects to include — Generic NAS, Isilon, NetApp, Physical, Pure, VMware, and so on.
- **Backup Status**—Filter by Protection Groups with successful backups or unsuccessful backups
- **Run Status**—Filter by status of the protection run — Canceled, Failed, Running, Success, and/or Warning.
- **SLA Status**—Filter by status of the SLA — Met or Missed.
- **Time Range**—Set the time period for your report.
- **Organization**—Choose one or more organizations to see the report data specific to the selected organizations

Glance Bar

The glance bar provides a summary of the report for the specified period:

- **Success Rate—Protection Groups with Successful Backups /Total Protection Groups.**
- **Total Protection Groups**—The total number of Protection Groups.
- **Protection Groups with Successful Backups**—The total number of Protection Groups with successful backups.
- **Protection Groups with No Successful Backups**—The total number of Protection Groups with unsuccessful backups.
- **SLA Met**—The total number of Protection Groups that met SLA.
- **SLA Missed**—The total number of Protection Groups that missed SLA.

Charts

The report includes the following two charts:

- **Protection Groups by Type**
- **Group Protection by Type**

Report Data

The following table describes the data displayed in the **Data** table. Use the search bar to filter the data by protection group name, system name, policy, or SLA.

Note: You can add or remove columns. For more information, see Customize table columns.

Column Name	Description
Protection Group	The name of the Protection Group.
Source	The source that is protected by this Protection Group.
System	The name of the cluster on which the Protection Group was created.
Policy	The protection policy associated with the Protection Group.
Last Run	The date and time at which the last backup for the Protection Group ran.

Column Name	Description
Successful Backups	The total number of successful backups for the Protection Group.
Unsuccessful Backups	The total number of unsuccessful backups for the Protection Group.
Success Rate	Indicates the success rate of the backups for the Protection Group.
SLA	Indicates whether the last run of the Protection Group during the specified period met or missed the SLA.
Organization	The name specified for the organization when added to the cluster.

Protection Runs

The **Protection Runs** report provides a summary and list of all backup activities per object per run. You can view the summary and success rate of protection runs. You can also view the snapshot status of the protection run.

Example use case: How many failed protection runs did I have in the last week?

Filter Report Data

The report supports multiple filters to pare down the data that you want to view in the report:

- **System**—Select all clusters to include.
- **Source**—Select all the sources to include.
- **Type**—Choose the types of objects to include — Generic NAS, Isilon, NetApp, Physical, Pure, VMware, and so on.
- **Run Status**—Filter by the status of the protection run — Canceled, Failed, Running, Success, and/or Warning.
- **Snapshot Status**—Filter by the status of the snapshot — Active or Expired.
- **Time Range**—Set the time period for your report.
- **Organization**—Choose one or more organizations to see the report data specific to the selected organizations.

Glance Bar

The glance bar provides a summary of the report for the specified period:

- **Success Rate—Total Successful /Total Runs.**
- **Total Runs**—The total number of protection runs.
- **Total Successful**—The total number of successful runs.
- **Success**—The total number of protection runs with status Success.
- **Warning**—The total number of protection runs with status Warning.
- **Failed**—The total number of protection runs with status Failed.
- **Canceled**—The total number of protection runs with status Canceled.
- **Running**—The total number of protection runs with status Running
- **SLA Met**—The total number of protection runs that met SLA.
- **SLA Missed**—The total number of protection runs that missed SLA.

Charts

The report includes the following two charts:

- **Run Status by Policy**
- **Run Status by Type**

Report Data

The following table describes the data displayed in the **Data** table. Use the search bar to filter the data by object name, source, policy, system name, or snapshot status.

Note: You can add or remove columns. For more information, see Customize table columns.

Column Name	Description
Start Time	The date and time at which the protection run started.
End Time	The date and time at which the protection run was completed.
Object Name	The name of the protected object.
Source	The hostname or IP address of the registered source.
Policy	The protection policy associated with the protection run for the corresponding object.
System	The name of the cluster on which the object had a protection run.
Snapshot Status	The status of the snapshot.
Duration	The time taken by the protection run.
Logical Data	The combined total of data in the objects that are protected by Data Management. These metrics are different depending on workload type. • **VMs**—The data size reported by VMware is the provisioned amount, not the actual data residing in the VM. For example, if a VM is provisioned for 1 TB but contains only 100 GB of data, VMware reports it as 1 TB. • **All Other Workloads**—The data size reported is the actual front end data residing on the server. If a server with 1 TB capacity contains 100GB of data, the server reports 100 GB **Note:** Data Management does not include unprotected objects in these metrics. Currently, the logical data value shown on the Data Management Dashboard is a sum of the logical data values captured across all the protection runs. For instance, if the source has 100 GB of logical data, and assuming it remains at 100 GB for the first 10 protection runs, Data Management would report, after 10 runs, the Logical Data to be 1000 GB (1 TB).

Column Name	Description
Data Read	Size of the set of protected objects as read by Data Management for a single backup run. This number is a per protection run statistic and is not additive across backup runs.
Data Written	Data written on the Data Management platform after the unique logical data has been reduced by data deduplication and data compression. **Note:** This number reflects unique data written, before resiliency operations.
Organization	The name specified for the organization when added to the cluster.

Recovery

The **Recovery** report provides a summary and list of all the clone and recovery tasks that were executed. It also provides other details such as the time taken for the operation and status of the operation.

Note: If a Data Management view is unprotected, the report does not display data about clone view operations.

Example use case: How many recovery tasks failed in the last week?

Filter Report Data

The report supports multiple filters to pare down the data that you want to view in the report:

- **System**—Select all clusters to include.
- **Source**—Select all the sources to include.
- **Organization**–Choose one or more organizations to see the report data specific to the selected organizations.
- **Type**—Choose the types of objects to include — Generic NAS, Isilon, NetApp, Physical, Pure, VMware, and so on.
- **Status**—Filter by the status of the recovery task — Canceled, Failed, Running, Success, and/or Warning.
- **Time Range**—Set the time period for your report.
- **Object**—Enter an object name to filter by the name of the object.

Glance Bar

The glance bar provides a summary of the report for the specified period.

Chart

The report includes the **Recovery Status by Type** chart.

Report Data

The following table describes the data displayed in the **Data** table. Use the search bar to filter the data by object name, source, system name, task name, or username.

Note: You can add or remove columns. For more information, see Customize table columns.

Column Name	Description
Start Time	The date and time at which the recovery task started.
Object Name	The name of the object.
Source	The hostname or IP address of the registered source.
System	The name of the cluster on which the recovery task was run.
Recovery Point	The date and time of the backup run from which the object was recovered.
Duration	The time taken by the recovery task.
Task Name	The name of the recovery task.
Username	The name of the user who initiated the recovery.
Organization	The name specified for the organization when added to the cluster.

System Connections

The **System Connections** report provides an overview of the clusters connected to Data Management and the connectivity status of each cluster.

Example use case: How many clusters were disconnected from Data Management in the last week?

Note: This report is only available for cluster and service provider administrators, and Data Management users who have access to **All Organizations**. It is not available for organization or tenant administrators and the users in organizations.

Filter report data

The report supports multiple filters to pare down the data that you want to view in the report:

- **System**—Select all clusters to include.
- **Organization** – Choose one or more organizations to see the report data specific to the selected organizations.
- **Connection Status**—Filter by connectivity status — Connected or Disconnected.
- **Time Range**—Set the time period for your report.

Glance Bar

The glance bar provides a summary of the report for the specified period:

- **Connectivity Rate**—The percentage of **Connected** to **Systems**.
- **Systems**—The total number of clusters.
- **Connected**—The total number of clusters connected to Data Management.
- **Disconnected**—The total number of clusters disconnected from Data Management

Report Data

The following table describes the data displayed in the **Data** table. Use the search bar to filter the data by system name or connection status.

Note: You can add or remove columns. For more information, see Customize table columns.

Column Name	Description
System Name	The name of the cluster.
Connection Status	The current cluster connection status.
Total Disconnected Time	The total time for which the cluster was disconnected from Data Management during the specified period.
Disconnection Time Percentage	The percentage of time for which the cluster remained disconnected.
Disconnections	The total number of times the cluster was disconnected.
Most Recent Disconnection	The data and time of the most recent disconnection.
Organization	The name specified for the organization when added to the cluster.

System Protection

The **System Protection** report displays a summary and list of all the protection activities performed on the clusters connected to Data Management. The report details all the archival, backup, replication, and cloud vault activities.

Filter Report Data

The report supports multiple filters to pare down the data you want to view in the report:

- **System**—Select all clusters to include.
- **Activity Type**—Choose the types of activity to include — Archive, Backup, Cloud Vault, and Replication.
- **Time Range**—Set the time period for your report.

Glance Bar

The glance bar provides a summary of the report for the specified period:

- **Connectivity Rate**—The percentage of **Connected** to **Systems**.
- **Systems**—The total number of clusters.
- **Connected**—The total number of clusters connected to Data Management
- **Disconnected**—The total number of clusters disconnected from Data Management.

Charts

- **Protection Runs by Activity Type**
- **Run Status by Activity Type**

Report Data

The following table describes the data displayed in the **Data** table. Use the search bar to filter the data by the cluster name.

Note: You can add or remove columns. For more information, see Customize table columns.

Column Name	Description
System Name	The name of the cluster on which the protection activities are run.
Activity Type	The type of protection activity, such as archival, backup, replication, or cloud vault, that is run on the cluster.
Total Runs	The total number of protection activities runs on the cluster.
Success Rate	The percentage rate of the successful protection activity runs on the cluster. The success rate is calculated as follows: Success Rate =[The number of runs with status Success + The number of runs with status Warning / The total number of protection activities runs on the cluster (Total Runs)] * 100.
Success	The number of protection activities with the status Success on the cluster.
Warning	The number of protection activities with the status Warning on the cluster.
Failed	The number of protection activities with the status Failed on the cluster.
Canceled	The number of protection activities with the status Canceled on the cluster.
Skipped	The number of protection activities with status Skipped on the cluster.
Running	The number of protection activities with status Running on the cluster.

Storage Consumption by System

The **Storage Consumption by System** report provides a summary and break down of storage statistics by cluster. It includes details such as total capacity, storage consumed, and daily growth rate.

Important: The Data Protect cluster must be running at a supported version, see IBM Storage Defender: Data Protect support information.

Example use case: What is the storage usage trend in the last month?

Note: This report is only available for cluster and service provider administrators, and Data Management users who have access to **All Organizations**. It is not available for organization or tenant administrators and the users in organizations.

Filter Report Data

The report supports the **System** and **Time Range** filters that allow you to pare down the data by cluster for the specified time period. Select all cluster(s) to include and set the time period.

- **System**—Select all cluster(s) to include.
- **Organization**–Choose one or more organizations to see the report data specific to the selected organizations.
- **Time Range**—Set the time period for your report.

Glance Bar

The glance bar provides a summary of the report for the specified period.

Chart

The report includes the **Usage Trend** chart.

Report Data

The following table describes the data displayed in the **Data** table. Use the search bar to filter the data by system name.

Note: You can add or remove columns. For more information, see Customize table columns.

Column Name	**Description**
System Name	The name of the cluster.
Organization	The name specified for the organization when added to the cluster.
Total Capacity	The total physical capacity of all storage devices after subtracting the space reserved for Data Management software operations.
Usage Percentage	The percentage of storage consumed by the cluster versus the total capacity.
Data Ingested & Retained	The size of the source data is initially full, plus incremental across retained snapshots, as of the end date in the selected date range. **Note:** This is before deduplication, compression, or resiliency. **Note:** If the original initial full has expired from the retention window, this metric does still include a virtual initial full in that the size of the source data on the first day of the retention window is included in this
Data Ingested &Retained Growth	The increase in source data is initially full, plus incremental across retained snapshots, over the selected date range.
Data Ingested &Retained Daily Growth Rate	The rate of increase in source data is initially full, plus incremental across retained snapshots, over the selected date range.
Data Ingested & Retained Daily Growth Percentage	The rate of increase in source data is initially full, plus incremental across retained snapshots, in percentage, over the selected date range.
Data Reduction	This equals the Source Data Retained /Storage Consumed for Retained Data, as of the end date in the selected date range.
Deduplication Ratio	The reduction of storage required that is produced by data deduplication, the process of eliminating excess copies of data (at the file or block level) to significantly decrease storage capacity requirements.

Column Name	Description
Compression Ratio	The reduction of storage required that is produced by data compression, the process of modifying, encoding, or converting the bits structure of data in such a way that it consumes less storage space.
Storage Consumed for Retained Data	The size of Data Management storage consumed for all retained snapshots, after reductions for deduplication and compression, excluding resiliency, as of the end date in the selected date range.
Storage Consumed for Retained Data Growth	The increase in Data Management storage consumed for all retained snapshots, after reductions for deduplication and compression, excluding resiliency, over the selected date range.
Storage Consumed for Retained Data Daily Growth Rate	The rate of increase in Data Management storage consumed for all retained snapshots, after reductions for deduplication and compression, excluding resiliency, over the selected date range.
Storage Consumed for Retained Data Daily Growth Percentage	The rate of increase in Data Management storage consumed for all retained snapshots, after reductions for deduplication and compression, excluding resiliency, in percentage, over the selected date range.
Resiliency Impact	The size of additional Data Management storage consumed for resiliency (such as RF2 or Erasure Coding). It does not include uncollected garbage nor metadata.
Storage Consumed with Resiliency	The size of Data Management storage consumed for all retained snapshots, calculated after reductions for deduplication and compression, and including inflation for resiliency, as of the end date in the selected date range.
Storage Consumed with Resiliency Growth	The growth of Data Management storage consumed for all retained snapshots, calculated after reductions for deduplication and compression, and inflation for resiliency, over the selected date range.
Storage Consumed with Resiliency Daily Growth Rate	The rate of increase in Data Management storage consumed, over the selected date range.
Storage Consumed with Resiliency Daily Growth Percentage	The rate of increase in Data Management storage consumed, in percentage, over the selected date range.

Storage Consumption by Protection Groups

The **Storage Consumption by Protection Groups** report provides a summary and break down of statistics about the Protection Groups that are consuming the most disk space on the Data Protect cluster. This report provides statistics for all types of objects that are protected by Protection Groups.

The Data Protect cluster must be running at a supported version, see IBM Storage Defender: Data Protect support information.

Example use case: Which organization is consuming the most storage?

Filter Report Data

The report supports multiple filters to pare down the data that you want to view in the report:

- **System**—Select all clusters to include.
- **Source**—Select all the sources to include.
- **Group Type**—Choose the types of objects to include — Generic NAS, Isilon, NetApp, Physical, Pure, VMware, and so on.
- **Time Range**—Set the time period for your report.
- **Organization**–Choose one or more organizations to see the report data specific to the selected organizations.

Glance Bar

The glance bar provides a summary of the report for the specified period.

Chart

The report includes the **Storage Consumed with Resiliency by Type** and **Source Data Storage Efficiency by Type** charts.

Report Data

The following table describes the data displayed in the **Data** table. Use the search bar to filter the data by storage domain.

Note: You can add or remove columns. For more information, see Customize table columns.

Column Name	**Description**
Protection Group	The name of the Protection Group.
Source	The hostname or IP address of the registered source.
Policy	The protection policy associated with the Protection Group.
System	The cluster name or AWS region for backup data.
Organization	The name specified for the organization when added to the cluster.
Data Ingested & Retained	The size of the source data is initially full, plus incremental across retained snapshots, as of the end date in the selected date range. Note that this is before deduplication, compression, or resiliency. **Note:** If the original initially full has expired from the retention window, this metric does still include a virtual initial full in that the size of the source data on the first day of the retention window is included in this metric.
Data Ingested & Retained Growth	The increase in source data is initially full, plus incremental across retained snapshots, over the selected date range.

Column Name	Description
Data Ingested & Retained Daily Growth Rate	The rate of increase in source data is initially full, plus incremental across retained snapshots, over the selected date range.
Data Ingested & Retained Daily Growth Percentage	The rate of increase in source data is initially full, plus incremental across retained snapshots, in percentage, over the selected date range.
Data Reduction	This equals the Source Data Retained /Storage Consumed for Retained Data, as of the end date in the selected date range.
Deduplication Ratio	The reduction of storage required that is produced by data deduplication, the process of eliminating excess copies of data (at the file or block level) to significantly decrease storage capacity requirements.
Compression Ratio	The reduction of storage required that is produced by data compression, the process of modifying, encoding, or converting the bits structure of data in such a way that it consumes less storage space.
Storage Consumed for Retained Data	The size of Data Management storage consumed for all retained snapshots, after reductions for deduplication and compression, excluding resiliency, as of the end date in the selected date range.
Storage Consumed for Retained Data Growth	The increase in Data Management storage consumed for all retained snapshots, after reductions for deduplication and compression, excluding resiliency, over the selected date range.
Storage Consumed for Retained Data Daily Growth Rate	The rate of increase in Data Management storage consumed for all retained snapshots, after reductions for deduplication and compression, excluding resiliency, over the selected date range.
Storage Consumed for Retained Data Daily Growth Percentage	The rate of increase in Data Management storage consumed for all retained snapshots, after reductions for deduplication and compression, excluding resiliency, in percentage, over the selected date range.
Resiliency Impact	The size of additional Data Management storage consumed for resiliency (such as RF2 or Erasure Coding). It does not include uncollected garbage nor metadata.
Storage Consumed with Resiliency	The size of Data Management storage consumed for all retained snapshots, calculated after reductions for deduplication and compression, and including inflation for resiliency, as of the end date in the selected date range.

Column Name	Description
Storage Consumed with Resiliency Growth	The growth of Data Management storage consumed for all retained snapshots, calculated after reductions for deduplication and compression, and inflation for resiliency, over the selected date range.
Storage Consumed with Resiliency Daily Growth Rate	The rate of increase in Data Management storage consumed, over the selected date range.
Storage Consumed with Resiliency Daily Growth Percentage	The rate of increase in Data Management storage consumed, in percentage, over the selected date range.

Storage Consumption by Object

The **Storage Consumption by Objects** report provides a summary and break down of the objects that are consuming the most disk space on the Data Protect cluster.

The Data Protect cluster must be running at a supported version, see IBM Storage Defender: Data Protect support information.

Example use case: Which object is consuming the most disk space in the last 24 hours?

Filter Report Data

The report supports multiple filters to pare down the data that you want to view in the report:

- **System**—Select all clusters to include.
- **Source**—Select all the sources to include.
- **Object Type**—Choose the types of objects to include — Generic NAS, Isilon, NetApp, Physical, Pure, VMware, and so on.
- **Time Range**—Set the time period for your report.
- **Object**—Enter an object name to filter by the name of the object.
- **Organization**–Choose one or more organizations to see the report data specific to the selected organizations.

Glance Bar

The glance bar provides a summary of the report for the specified period.

Chart

The report includes the **Total Change by Type** chart.

Report Data

The following table describes the data displayed in the **Data** table. Use the search bar to filter the data by object name, source, or system name.

Note: You can add or remove columns. For more information, see Customize table columns.

Column Name	Description
Object Name	The name of the Protection Group.
System	The cluster name or AWS region for backup data.

Column Name	Description
Source	The hostname or IP address of the registered source.
Organization	The name specified for the organization when added to the cluster.
Snapshots	Total number of snapshots.
Logical Data	• For Data Protection, it is the combined total of data in the objects that are protected by Data Management. • For Smart Files, it is the size of total unique logical data of active filesystem as residing on Data Management.
Data Read	The size of the set of protected objects as read by Data Management for a single backup run. This number is a per protection run statistic and is not additive across backup runs.
Data Written	Data written on the Data Management platform after the unique logical data has been reduced by data deduplication and data compression. **Note:** This number reflects unique data written, before resiliency operations.
Daily Change Rate	The change rate of Data Read for the time period set in the filter.

Storage Consumption by Storage Domains

The **Storage Consumption by Storage Domains** report provides a summary and break down of storage domains consuming the most storage.

The Data Protect cluster must be running at a supported version, see IBM Storage Defender: Data Protect support information.

Example use case: Which storage domain is consuming the most storage?

Filter Report Data

The report supports multiple filters to pare down the data that you want to view in the report:

- **System**—Select all clusters to include.
- **Time Range**—Set the time period for your report.
- **Organization**–Choose one or more organizations to see the report data specific to the selected organizations.

Glance Bar

The glance bar provides a summary of the report for the specified period.

Report Data

The following table describes the data displayed in the **Data** table. Use the search bar to filter the data by storage domain.

Note: You can add or remove columns. For more information, see Customize table columns.

Column Name	Description
Storage Domain	The name of the storage domain.
System	The cluster name or AWS region for backup data.
Organization	The name specified for the organization when added to the cluster.
Data Ingested & Retained	The size of the source data is initially full, plus incremental across retained snapshots, as of the end date in the selected date range. Note that this is before deduplication, compression, or resiliency. **Note:** If the original initial full has expired from the retention window, this metric does still include a virtual initial full in that the size of the source data on the first day of the retention window is included in this metric.
Data Ingested &Retained Growth	The increase in source data is initially full, plus incremental across retained snapshots, over the selected date range.
Data Ingested &Retained Daily Growth Rate	The rate of increase in source data is initially full, plus incremental across retained snapshots, over the selected date range.
Data Ingested & Retained Daily Growth Percentage	The rate of increase in source data is initially full, plus incremental across retained snapshots, in percentage, over the selected date range.
Data Reduction	This equals the Source Data Retained /Storage Consumed for Retained Data, as of the end date in the selected date range.
Deduplication Ratio	The reduction of storage required that is produced by data deduplication, the process of eliminating excess copies of data (at the file or block level) to significantly decrease storage capacity requirements.
Compression Ratio	The reduction of storage required that is produced by data compression, the process of modifying, encoding, or converting the bits structure of data in such a way that it consumes less storage space.
Storage Consumed for Retained Data	The size of Data Management storage consumed for all retained snapshots, after reductions for deduplication and compression, excluding resiliency, as of the end date in the selected date range.
Storage Consumed for Retained Data Growth	The increase in Data Management storage consumed for all retained snapshots, after reductions for deduplication and compression, excluding resiliency, over the selected date range.
Resiliency Impact	The size of additional Data Management storage consumed for resiliency (such as RF2 or Erasure Coding). It does not include uncollected garbage nor metadata.

Column Name	Description
Storage Consumed with Resiliency	The size of Data Management storage consumed for all retained snapshots, calculated after reductions for deduplication and compression, and including inflation for resiliency, as of the end date in the selected date range.
Storage Consumed with Resiliency Growth	The growth of Data Management storage consumed for all retained snapshots, calculated after reductions for deduplication and compression, and inflation for resiliency, over the selected date range.
Resiliency Impact	The size of additional Data Management storage consumed for resiliency (such as RF2 or Erasure Coding). It does not include uncollected garbage nor metadata.
Storage Consumed with Resiliency	The size of Data Management storage consumed for all retained snapshots, calculated after reductions for deduplication and compression, and including inflation for resiliency, as of the end date in the selected date range.
Storage Consumed with Resiliency Growth	The growth of Data Management storage consumed for all retained snapshots, calculated after reductions for deduplication and compression, and inflation for resiliency, over the selected date range.
Storage Consumed with Resiliency Daily Growth Rate	The rate of increase in Data Management storage consumed, over the selected date range.
Storage Consumed with Resiliency Daily Growth Percentage	The rate of increase in Data Management storage consumed, in percentage, over the selected date range.

Storage Consumption by Views

The **Storage Consumption by Views** report provides a summary and break down of views that are consuming the most storage.

The cluster must be running at a supported version, see IBM Storage Defender: Data Protect support information.

Example use case: Which view is consuming the most storage in the past 24 hours?

Filter Report Data

The report supports multiple filters to pare down the data that you want to view in the report:

- **System**—Select all clusters to include
- **Organization**–Choose one or more organizations to see the report data specific to the selected organizations.
- **Time Range**—Set the time period for your report.

Glance Bar

The glance bar provides a summary of the report for the specified period.

Report Data

The following table describes the data displayed in the **Data** table. Use the search bar to filter the data by view name or system name.

Note: You can add or remove columns. For more information, see Customize table columns.

Column Name	**Description**
View Name	Displays the name of the view and storage domain.
Organization	The name specified for the organization when added to the cluster.
System	The cluster name or AWS region for backup data.
Data Ingested & Retained	The size of the source data is initially full, plus incremental across retained snapshots, as of the end date in the selected date range. Note that this is before deduplication, compression, or resiliency. **Note:** If the original initial full has expired from the retention window, this metric does still include a virtual initial full in that the size of the source data on the first day of the retention window is included in this metric.
Data Ingested & Retained Growth	The increase in source data is initially full, plus incremental across retained snapshots, over the selected date range.
Data Ingested & Retained Daily Growth Rate	The rate of increase in source data is initially full, plus incremental across retained snapshots, over the selected date range.
Data Ingested & Retained Daily Growth Percentage	The rate of increase in source data is initially full, plus incremental across retained snapshots, in percentage, over the selected date range.
Data Reduction	This equals the Source Data Retained / Storage Consumed for Retained Data, as of the end date in the selected date range.
Deduplication Ratio	The reduction of storage required that is produced by data deduplication, the process of eliminating excess copies of data (at the file or block level) to significantly decrease storage capacity requirements.
Compression Ratio	The reduction of storage required that is produced by data compression, the process of modifying, encoding, or converting the bits structure of data in such a way that it consumes less storage space.
Storage Consumed for Retained Data	The size of Data Management storage consumed for all retained snapshots, after reductions for deduplication and compression, excluding resiliency, as of the end date in the selected date range.

Column Name	Description
Storage Consumed for Retained Data Growth	The increase in Data Management storage consumed for all retained snapshots, after reductions for deduplication and compression, excluding resiliency, over the selected date range.
Storage Consumed for Retained Data Daily Growth Rate	The rate of increase in Data Management storage consumed for all retained snapshots, after reductions for deduplication and compression, excluding resiliency, over the selected date range.
Storage Consumed for Retained Data Daily Growth Percentage	The rate of increase in Data Management storage consumed for all retained snapshots, after reductions for deduplication and compression, excluding resiliency, in percentage, over the selected date range.
Resiliency Impact	The size of additional Data Management storage consumed for resiliency (such as RF2 or Erasure Coding). It does not include uncollected garbage nor metadata.
Storage Consumed with Resiliency	The size of Data Management storage consumed for all retained snapshots, calculated after reductions for deduplication and compression, and including inflation for resiliency, as of the end date in the selected date range.
Storage Consumed with Resiliency Growth	The growth of Data Management storage consumed for all retained snapshots, calculated after reductions for deduplication and compression, and inflation for resiliency, over the selected date range.
Storage Consumed with Resiliency Daily Growth Rate	The rate of increase in Data Management storage consumed, over the selected date range.
Storage Consumed with Resiliency Daily Growth Percentage	The rate of increase in Data Management storage consumed, in percentage, over the selected date range.

Data Transferred to External Targets

The **Data Transferred to External Targets** report provides statistics about the data that is transferred to External Targets for archiving Snapshots created by Protection Groups, and moving cold data from the Data Protect cluster to Cloud Tier.

The Data Protect cluster must be at version 7.0.1 or later.

Filter Report Data

The report supports multiple filters to pare down the data that you want to view in the report:

- **System**—Select all clusters to include.
- **Target Type**—Select the target type.
- **Target Name**—Select the target name.
- **Managed by**—Select to filter the External Targets based on whether customers or Data Management manages them.
- **Time Range**—Set the time period for your report.

Glance Bar

The glance bar provides a summary of the report for the specified period.

Chart

The report includes the **External Storage Consumption Trend** chart.

Report Data

The following table describes the data displayed in the **Data** table. Use the search bar to filter the data by target name.

Note: You can add or remove columns. For more information, see Customize table columns.

Column Name	Description
Target Name	The target name.
System	The cluster name or AWS region for backup data.
Data Transferred	The size of the data transferred over the network to the External Target over the selected date range.
Cumulative Data Transferred	The size of all data transferred over the network to the External Target, from initial transfer to the end date in the selected date range.
External Storage Consumed for Retained Data	The size of External Target storage consumed for all retained snapshots, after reductions for deduplication and compression, excluding resiliency, as of the end date in the selected date range.
External Storage Consumed for Retained Data Growth	The growth of External Storage Consumed for Retained Data, over the selected date range.
External Storage Consumed for Retained Data Daily Growth Rate	The daily average growth of External Storage Consumed for Retained Data, over the selected date range.

Chapter 6. Cluster management

The following topics provide essential information about cluster management:

- Upgrading clusters
- Globally search clusters and take action
- Viewing aggregated alerts

Upgrading clusters

Cluster upgrades bring your cluster up to the current maintenance level.

Before you begin

Before you can upgrade a Data Protect cluster, download the upgrade package file that you want to install. Upgrade package files are labeled with component name *Defender ClustSW Upgrade Package*. For information, see Download Information: IBM Storage Defender 2.x.

About this task

Important: Upgrade package files must be installed from the Data Protect management interface.

Alternatively, you can upgrade clusters from Data Management, but to do so, you must host the upgrade file on your own web server. By hosting the upgrade file on your own web server, you have the option to upgrade individual clusters from the **Cluster Management** page in Data Management or from the Data Protect management interface. For information, see Upgrading clusters from Data Management.

Note: The cluster upgrade process is nondisruptive. The upgrade is initiated on a single node in the cluster, and all remaining nodes in the cluster are then updated automatically. You do not need to take your cluster offline during the upgrade process unless your cluster configuration does not allow for a single node to be taken offline.

Procedure

To upgrade a cluster, complete the following steps:

1. Log in to the Data Protect management interface, and specify the login credentials for a cluster admin user.
2. Navigate to **Settings** > **Software Update**.
3. Click the **Upgrade** tab.
4. Click **Get New Package** and select **Upload a package file**.
5. Click **Select File** and browse to the upgrade file location.
6. Click **Upload and Upgrade**. The upgrade process starts.
7. Repeat this procedure for each cluster that you want to upgrade.

Upgrading clusters from Data Management

You can upgrade individual clusters from the **Cluster Management** page in Data Management.

Before you begin

For information about setting up access to Data Management, see Manage Cluster Connections.

Cluster upgrades bring your cluster up to the current maintenance level. Before you can upgrade a cluster, download the upgrade package file that you want to install. Upgrade package files are labeled with

© Copyright IBM Corp. 2023, 2024

component name *Defender ClustSW Upgrade Package*. For information, see Download Information: IBM Storage Defender 2.x.

To upgrade clusters from Data Management, you must host the upgrade file on your own web server. By hosting the upgrade file on your own web server, you have the option to upgrade individual clusters from the **Cluster Management** page in Data Management or from the Data Protect management interface. For information about uploading cluster upgrade files from the Data Protect management interface, see Upgrading clusters.

Tip: A user with Upgrade Cluster privilege can upgrade the cluster.

Procedure

To upgrade a cluster, complete the following steps:

1. Click **All Clusters** from the navigation menu, and select the individual cluster that you want to upgrade.
2. Click **Settings** > **Upgrade**.
3. Click the **Upgrade** tab.
4. Click the **Get New Package** button.
5. Select **Provide download URL**, and specify the URL for the upgrade package location.
6. Click **Download and Upgrade**.

   Note: The **Download and update** selection is only available when you are viewing the settings for an individual cluster.
7. Repeat this procedure for each cluster that you want to upgrade.

Updating cluster location

You can update a cluster location on the **Cluster Management** page.

Procedure

To update a cluster location, complete the following steps:

1. Click **Settings** > **Clusters**. The **Cluster Management** page is displayed.
2. Click the ⋮ icon for the required cluster.
3. Select the **Update Location** option. The **Change Cluster Location** window is displayed.
4. Enter the new cluster location and click **Update**. To update the locations of multiple clusters, select multiple clusters and click the **Update Location** button.

Unregistering a cluster

You can unregister a cluster from Data Management that is no longer needed to manage your data.

Before you begin

The IBM Storage Defender eagle agent service is used to send and receive data between the IBM Storage Protect server and Data Management. Before you unregister a cluster, you can stop the eagle agent that is running in the background by completing the following steps:

1. Stop the eagle-agent by issuing the dcli eagle-agent stop command.
2. Delete the claim to your IBM Storage Protect server by issuing the dcli claim delete command.
3. Delete the registration of the IBM Storage Protect server by issuing the dcli server delete command.
4. Follow the procedure to unregister the cluster in Data Management.

Procedure

To unregister a cluster, complete the following steps:

1. Click **Settings** > **Clusters**. The **Cluster Management page** is displayed.
2. From the list of available clusters, click the ⋮ icon for the cluster that you want to unregister from Data Management.
3. Select the **Unregister** option. The **Unregister** window is displayed, along with the following message: "Are you sure you want to unregister the clusters from Data Management?"
4. Click **Unregister**.

   Tip: To unregister multiple clusters, you can select multiple clusters and click **Unregister**.

Globally search clusters and take action

From Data Management, you can search across all your Data Management-enabled clusters for objects, such as VMs, storage volumes and databases. You can refine the search results and then act on the objects.

From the search results page, you can find and protect unprotected objects, investigate failed Protection Groups, or recover or clone snapshots. The actions launch the familiar IBM workflow pages, in addition to that you have information with the help icon ? to look in each page if you need.

Example: Find and protect

The following procedure is the example for demonstrating how to find unprotected VMs and protect them by creating a Protection Group.

Procedure

1. In the search bar, type `vm` and press enter. You can search for any partial name or type an asterisk * wildcard. The **Search** page is displayed with a list of objects that contain `vm` in the name.
2. Optionally, refine the list by selecting check boxes from the menu options.
   a. Under **Status**, select the **Unprotected** checkbox.
   b. Under **Type**, select the **Virtual Machines** checkbox. More options are displayed based on the infrastructure that you select.
   c. Under **Virtual Machines**, select the **VMware** checkbox.

   The list of objects is automatically updated to display only unprotected VMware VMs.
3. Select a VM in the center of the page. Details about the VM are displayed on the right side of the page.
4. Click **Protect**.
5. Select **Protection Group** and click **New Job**.
6. The **New Job** page is displayed and you can create a job to protect the VM.
7. When you are finished configuring the **Protection Group**, click **Protect** to create the job and return to the **Search** page.

Example: Clone or recover a snapshot

The following procedure is the example for demonstrating how to clone or recover a snapshot that was previously created by a **Protection Group**.

Procedure

To clone or recover a snapshot, complete the following steps:

1. In the search bar, type a partial job name or `*` and press enter. The Search page is displayed with a list of objects.
2. Select the **Protected** checkbox in the left pane.
3. Select a job from the center pane. Details about the job are displayed in the right pane.

4. Click the actions icon in the right pane and select **Clone** or **Recover**. You can also drill down to details about the job and its policy.
5. Depending on which action you click, the **Clone** or **Recover** page is displayed.
6. When you are finished configuring the clone or recovery options, click **Finish** to run the task and return to the Search page.

Aggregated alerts

The Data Management cluster creates an alert when a potential problem is found or when a threshold has been exceeded on a cluster. The alerts are aggregated from all clusters into a unified Alerts page.

Procedure

To manage the alerts for all Data Management-enabled clusters, complete the following steps:

1. Click **All Clusters** from the navigation menu.
2. Select **System** > **Health** > **Alerts**.
3. Note the **Cluster** column in the **Alerts** page.
4. Click an alert name to drill down to detailed information, including the cause of the alert.

   Important:

   - Detailed alert information for the IBM Storage Protect server is displayed in the language that is set for the IBM Storage Protect server. For languages other than English, the text might not display properly unless a language encoded in UTF-8 is set for the IBM Storage Protect server. For more information about language support selection, see Server language locales in the IBM Storage Protect documentation.
   - Marking an IBM Storage Protect server alert as **Resolved** in Data Management does not change the alert status on the IBM Storage Protect server. To change the status of an alert to resolved both on the IBM Storage Protect server *and* in Data Management, update the alert status to **Closed** on the IBM Storage Protect server by using either the command line or the Operations Center.

Chapter 7. Smart Assist

The following topics provide essential information about SmartAssist:

- Cluster Capacity Prediction
- Field Messages
- Simulations

Cluster Capacity Prediction

You can use the Data Management capacity prediction feature to determine when a cluster might run out of space. The prediction is based on the last 12 weeks of storage activity on the cluster.

Procedure

To use the capacity prediction feature, complete the following steps:

1. From the dashboard, select a single cluster from the **All Clusters** navigation menu.
2. Select **Settings** > **Summary**.
3. The Capacity Prediction chart is displayed at the bottom of the **Summary** tab (only if you have selected a single cluster).

   Today's date is represented by the vertical line. Actual capacity utilization appears to the left of the vertical line, which is shown as a solid blue line. Predicted capacity utilization appears to the right, shown as a dotted blue line.
4. Drag the mouse across the blue line to display the amount of used space and the predicted amount of utilization at a date in the future.

   The horizontal lines near the top of the chart show the total cluster capacity and the capacity at 80% and 90% utilization.

   Tip: The cluster issues the following alerts:

   - Alert CE00316002 when the capacity is at 90% utilization (critical).
   - Alert CE00502121 when the capacity is at 80% utilization (warning).
5. If the chart indicates that the cluster might run out of space soon, consider taking the following actions to add or reclaim capacity:

   - Add more nodes to the cluster.
   - Clean up snapshots that are no longer required.
   - Archive snapshots to an External Target.
   - Configure Cloud Tier to hold rarely used data.
   - Change Storage Domains to use Erasure Coding (capacity utilization will be reduced over time).

Field Messages

By default, IBM pushes important messages to Data Management, such as field notices, maintenance windows and release notes.

About this task

You can view recent field messages by clicking the notifications icon from the menu.

Procedure

To view a customizable list of field messages:

© Copyright IBM Corp. 2023, 2024

1. In the dashboard, select **System** > **Field Messages**.
2. Optionally, you can search for any text in the message, use the **Type** drop down to filter the list by message type, and specify a date range for when messages were received.
3. The messages that meet the search, filter and date criteria are listed.
4. Click a message to display the message content.
5. Click **Close** to close the message.

Simulations

IBM Storage Defender Data Management Service introduces a predict and plan model with the capability of making predictions on cluster utilization and storage consumption based on historical usage, workloads, and user specified what-if scenarios.

This capability enables system administrators to plan ahead and make decisions about procurement of new nodes, addition of new workloads, optimization of existing workloads and so on. This feature enables you to simulate scenarios for a set of user selected clusters and time periods.

From the **Simulation** dashboard, we can analyze and predict:

- Cluster usage and if it exceeds the capacity at a given point in time.
- Number of clusters that might exceed 80% or 90% of the cluster capacity.

Note:

- For simulation, the cluster must be claimed to Data Management for at least 24 hours.
- **Simulation** is available only in an **All-Clusters** view. If you have selected a specific cluster, then **Simulation** is not available.
- Depending on the role assigned, you are able to either only view simulations or manage simulation activities such as create, edit, and delete simulation. Example: A user with Super admin role may be able to view and manage simulations, but a user with Viewer role may be able to only view them.

Supported Software

The Simulations feature is supported on all supported Data Protect cluster versions, see IBM Storage Defender: Data Protect support information.

Adding a new simulation

You can add a new simulation from the **Simulation** dashboard to analyze and predict the cluster usage and capacity.

Procedure

To add a new simulation, complete the procedure:

1. From the dashboard, navigate to **System** > **Simulation**.

   The **Simulation** page displays.
2. Click + to create a new simulation.
3. Enter a relevant **Simulation Name** and provide a date until when this simulation will be active in the **Simulation Until Date** field.

   Note:

   - You can select a date from the current date up to a date within six months from the current date.
   - The Simulation Until Date must be always greater than the start date of any event.
4. Click **Add** to select an event from the drop-down list to be simulated.

   For details to add an event, see “Adding a protection group” on page 59, “Adding a node” on page 59, “Editing the storage domain” on page 60, and “Removing a protection group” on page 60.

You can create multiple events in this simulation page.

Note: The following options in the Add simulation list are currently unavailable:

- Add View
- Edit Policy
- Edit Protection Group

5. Click **Run**.

   After a successful run, the simulation is populated in the **Simulation** dashboard.

   Note:

   - If the simulation fails, the data is not populated and a “Failed” status is displayed. You have an option to rerun the simulation. Currently, a failed simulation cannot be edited before re-run.
   - While the simulation execution is in progress, users can navigate out of the simulations interface and revisit the simulation page later.

Adding a protection group

You can add a protection group from the **Add Simulation** page.

Procedure

To add a protection group, complete the procedure:

1. In the **Add Simulation** page, click **Add** > **Add Protection Group**.
2. Enter the start date to initiate the simulation for this event.
3. Select a cluster from the drop down.
4. Select the storage domain for the selected cluster.
5. Choose a workload and the initial size.
6. Select the **Data Reduction Ratio**, which is a combination of dedupe ratio and compression, and **Daily Change Rate**.

   Note: The above values are populated based on the workload that you choose. You can further refine these ratios if required. For example, if you select a VMware workload, the initial data reduction ratio is populated as 4X with a daily change rate of 2%.
7. Select an appropriate policy.

Adding a node

You can add a node from the **Add Simulation** page.

Procedure

To add a node, complete the procedure:

1. In the **Add Simulation** page, click **Add** > **Add Node**.
2. Enter the start date to initiate the simulation for this event.
3. Select a cluster from the drop down.
4. Select a model for this node.
5. Confirm the number of nodes.

   If you have multiple models to be selected, click + to add a new node and model.

Editing the storage domain

You can edit the storage domain from the **Add Simulation** page.

Procedure

To edit the storage domain, complete the procedure:

1. In the **Add Simulation** page, click **Add** > **Edit Storage Domain**.
2. Enter the start date to initiate the simulation for this event.
3. Select a cluster from the drop down.
4. Select the storage domain for the selected cluster and choose the resilience factor.

   Notes:

   - The resiliency indicates a prefix and suffix used. The prefix such as "1d:1n" is the resiliency value and represents the number of disks and nodes (1Disk:1Node) whose failure can be tolerated. The suffix such as "3 Nodes" represents the minimum number of nodes that are required for this EC/RF to be applicable.
   - The **Deduplication** and **Compression** options are not supported in this release.

Removing a protection group

You can remove a protection group from the **Add Simulation** page.

Procedure

To remove a protection group, complete the procedure:

1. In the **Add Simulation** page, click **Add** > **Remove Protection Group**.
2. Enter the start date to initiate the simulation for this event.
3. Select a cluster from the drop down.
4. Select the Protection Group.
5. Choose a workload and the initial size.
6. Under **Manage Snapshots**, choose to either delete all the old snapshots now or remove old snapshots per policy.

Editing a simulation

You can edit a simulation from the **Simulation** dashboard.

Procedure

To edit a simulation, complete the procedure:

1. From the **Simulation** dashboard, click an existing simulation.
2. Click 🔧 next to the simulation.
3. In the **Edit** panel, modify the simulation details or add new events based on the requirement.
4. Click **Run** to execute the newly modified simulation.

Deleting a simulation

To delete the simulation from the **Simulation** dashboard, click delete.

Limitations

The simulation is not available for Data Management - Premises Edition app.

Chapter 8. Compliance and Security

The following topics provide information about licensing and security using IBM Storage Defender Data Management Service:

- Data Management Licensing
- Compliance and Certifications
- Detect Ransomware attacks
- Security Advisor
- Audit Logs

Licensing

The IBM Storage Defender Data Management Service Licensing system helps customers and partners ensure that Data Management software is being used in accordance with the terms and conditions of the license and the usage is in compliance with the entitlement. The Data Management licensing model gives the flexibility to use certain features or services of the Data Management software, depending on which licenses the customer is entitled to.

All Data Protect clusters must be licensed. License usage is metered on each Data Protect cluster and the usage is aggregated in Data Management. Alerts are triggered or GUI notifications are displayed in one of the following scenarios:

- License usage violation—If the aggregate metered usage is nearing the entitlement or is exceeded the entitlement
- A cluster is set up without a license
- Clusters are not reporting their usage information to Data Management
- The license file on a particular cluster is expired or is about to expire

You must set up licensing on the Data Protect cluster. For more information on setting up licensing on each cluster, follow the instructions below.

You can monitor the license usage and view entitlement details in Data Management. For more information, see View License Usage and Entitlements.

License Modes

Licensing Data Management is possible only for Connected Sites-cluster as described in the following table.

Data Protect Cluster State	How Licensing Works	How Audits are Conducted
Connected Sites-cluster remains connected with Data Management always. All usage data is automatically shared with Data Management.	License is automatically generated in Data Management. The license is then reflected in the connected cluster automatically. Any manual intervention of operations is not needed. For more information, see Manage in Data Management SaaS.	Audit reports are automatically uploaded to Data Management daily. **Note:** The audit report contains details such as cluster ID, timestamp, license usage data, and entitlements.

© Copyright IBM Corp. 2023, 2024

License SKUs

New Service SKUs — Data Management software is packaged as services that can be run on any supported Data Protect cluster. Data Management supports the following service SKUs:

- IBM Storage Defender Data Protect
- IBM Storage Defender Replica

Viewing license usage and entitlements

The **License** page displays license usage details and entitlements across all registered clusters. You can get a good insight into the overall license usage and estimate your license needs. From the **License** page, you can:

- Filter by license status—Active or expired
- Drill down and view additional information about a particular license

If you have any entitlements or usage on your clusters, the license type is displayed on the **License** page. You can view the usage details, entitlements, and the total number of clusters.

To view the overall license usage:

1. Log in to Data Management.
2. Select **All Clusters** from the navigation menu.
3. Navigate to **Settings** > **License**.

   The **License** page displays a summary of the entitlements and usage across all clusters.

Viewing usage by license type

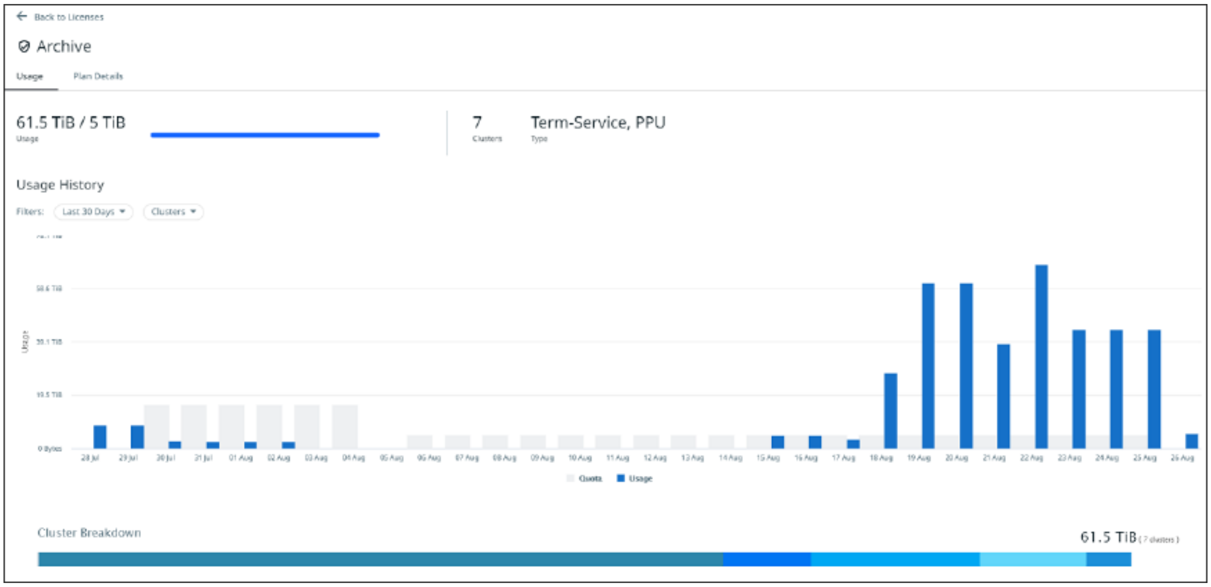
Procedure

From the **License** page, you can drill down and view usage and plan details of a particular license.

To view usage and plan details for a particular license:

1. Launch Data Management.
2. Select **All Clusters** from the navigation menu.
3. Navigate to **Settings** > **License**.
4. Click on a license to drill down. For example, **Archive**.
5. By default, the **Usage** tab is displayed. You can view the following details:

   - Current® usage across clusters out of the entitled capacity. As illustrated in the following image, 61.5 TiB is used across 7 clusters out of 5 TiB of entitled capacity.



Back to Licenses

Archive

Usage Plan Details

61.5 TiB / 5 TiB
Usage

7
Clusters

Term-Service, PPU
Type

Usage History

Filters: Last 30 Days ▾ Clusters ▾

Cluster Breakdown

61.5 TiB (7 clusters)

- License type.
- Cluster usage data for last 30 days.
- Cluster usage data for last 12 months.
- Current cluster usage distribution. You can also filter by cluster.

6. Click the **Plan Details** tab to view the following:

   - **Product Information**

     Link to the data sheet. Currently, data sheet is available only for Data Protect and Smart Files services.
   - **Purchase History**

     Displays the entitled capacity, expiration date, and details of the SKU.

About license usage warning

The **License** page displays a warning message if your licenses need to be renewed. If you exceed your license entitlement, a warning message is displayed on the license tile. To renew the license, contact your IBM sales representative.

Managing clusters in Data Management SaaS

If you want the cluster to remain connected with Data Management and automatically synchronize operations such as downloading audit reports, uploading license files, and so on, select the **SaaS** option when you set up the cluster.

Connecting with Data Management

If you are setting up the cluster for the first time or if you upgraded your cluster to a newer version, you must first establish the connection of your cluster with Data Management depending on your business requirement.

Procedure

If the connection with Data Management is not established previously from your cluster, complete the following steps:

1. On the Data Protect cluster GUI, click H > **Manage Connections**.

2. Turn on the Connect to Data Management toggle to automatically synchronize your cluster with Data Management.

   Once connected, the icon is displayed with a green tick ✓.

To connect your cluster with Data Management:

3. Log in to your cluster.
4. Read the **EULA License Agreement** and click **Agree**.
5. Click **Manage in Data Management SaaS** and then on **Connect to Data Management SaaS**.
6. On the **Connect with Data Management page**, select the appropriate access permission—**Full Access** or **View Only** and click **Continue**.
7. You will be redirected to the Data Management login page. Enter valid Data Management credentials and click **Connect** to establish connection with Data Management.

   The cluster is connected to Data Management successfully.

Automatic synchronization of license usage

For connected sites, since the clusters are connected with IBM Storage Defender Data Management Service, all operations such as generating the license file in Data Management, downloading the license file on the cluster, and uploading this license file in Data Management are all performed automatically. No manual intervention is required. You can access the License page on Data Management to check the license usage against the purchased entitlement.

Managing licenses on clusters

If you are unable to share cluster management information with Data Management SaaS or if you cannot connect your cluster to the internet for security reasons, you can consider keeping your cluster disconnected from Data Management. Data Management provides the following options:

- Connect to Data Management only for licensing purposes only—Only license usage information is transferred over the internet to Data Management. No other information is sent over the internet.
- Manually license your cluster—Every 180 days, you must manually download the audit report from the Data Protect cluster, upload the audit report on Data Management, generate the new license file on Data Management, and upload the new license file on the Data Protect cluster.

Note: If the Data Protect cluster is disconnected from Data Management, the License About To Expire alert is triggered when the license is about to expire.

Managing licenses

You can manage licenses from the Data Protect cluster.

Procedure

To manage licenses from the Data Protect cluster, complete the procedure:

1. Log in to the Data Protect cluster.
2. Read the **EULA License Agreement** and click **Agree**.
3. Click **Manage on Cluster** and then on **Connect to Cluster**.
4. On the **License page**, select one of the following licensing modes: **Data Management Smart Licensing**, **Manual Licensing** , and **Dark Site**.

   To manage the licenses later, select **Skip licensing at this time**. For details on how to configure the license at a later point in time, see "Configuring the license after cluster creation" on page 67.

Smart licensing

You can configure the Data Management for smart licensing. Only the licensing information is shared with Data Management.

Before you begin

When you select Data Management Smart Licensing at step 2 in Manage Licenses in the Data Protect cluster, the **Management Options** page is displayed.

Procedure

Perform the following steps on the **Management Options** page to configure Data Management smart licensing:

1. On the **Management Options** page, select the **Connect to Data Management only for licensing** option.
2. Click **Continue**.

   You will be redirected to the Data Management page to enter credentials to log in.
3. Click **Connect** to establish the connection with Data Management.

   Only the licensing information is shared with Data Management.

Manual licensing

You can manage licenses by **Manual Licensing** in the Data Protect cluster.

Before you begin

In step “4” on page 64 of the “Managing licenses” on page 64 topic, when you select **Manual Licensing**, the **Licensing Steps** page is displayed.

Procedure

Perform the following steps to configure Manual Licensing:

1. On the **Licensing Steps** dialog box, click **Download License Usage Report**.

   The License Usage Report file is downloaded to your local.
2. To upload the Audit Report:

   a. Log in to Data Management and navigate to **Settings** > **License**.

      The license summary of all clusters connected to Data Management is displayed.

   b. Click **Upload Audit Report**.

   c. In the **Upload Audit Report** dialog box, upload the Audit Report downloaded at step 1.

   d. Click **Submit**.
3. To generate the License File:

   a. Log in to your Data Protect cluster and navigate to **Settings** > **License**. On the **Licensing Steps** page, select **Copy Cluster ID**.

   b. Log in to Data Management and click **Generate License File**.

      The **Generate License File** dialog box appears and prompts for the Cluster ID.

   c. Paste the Cluster ID copied in Step 3 (a) and click **Generate**.

      The License File is downloaded to your local.
4. To upload the License File, complete the following steps:

   a. Log in to your Data Protect cluster and navigate to **Settings** > **License**.

   b. On the **Licensing Steps** page, click **Select File**.

c. Browse to select the License File that is downloaded at Step 3 c and click **Upload**.

You must download the audit report from the Data Protect cluster and upload it on Data Management every 180 days. The audit report contains details such as cluster ID, timestamp, license usage data, and entitlements.

Smart licensing and Manual licensing issues

The following table lists some of the notifications that occur for sites that are not connected to IBM Storage Defender Data Management Service:

Notification	Scenario	Steps to Resolve
Unregistered cluster	The cluster has not been registered with Data Management within 30 days of creation.	1. Go to Data Management and enter your cluster ID. 2. After the license file is downloaded, upload the license file on your cluster, and click **Submit**. The following message is displayed: `License file uploaded successfully.`
Cluster pending audit report upload	The audit report has not been uploaded within 90 days from the last upload.	Generate a new audit report: 1. Download the audit report from your cluster. 2. Log in to Data Management and upload the audit report.

Dark site issues

If the license activation was unsuccessful for a dark site, see the following points that are listed for possible corrective actions:

- **Invalid cluster ID**
  Confirm the cluster ID for which you generated the license key. Reconfirm if you applied the same cluster ID when you generated the license key. Otherwise, generate the license again by using the correct cluster ID.
- **License key expired**
  If the license key is expired, you must generate the license key again. The validity of the license key is 30 days from the time of license generation. You can also confirm if the cluster node time is not more than 30 days from the Data Management time.
- **Invalid license key**
  If the license key is invalid, reconfirm the correct license key and enter it correctly.

Dark site

To set up a cluster as a dark site, you must contact your IBM support representative and submit a request. If your request is approved, the license key is displayed in Data Management.

Copying the license key

You can copy the license key that is displayed in Data Management.

Procedure

To copy the license key from Data Management, complete the procedure:

1. Log in to Data Management and navigate to **Settings** > **License**.

   The alpha-numeric license key is displayed in the **License** page.
2. Copy the license key.

Copying the license key on your cluster

You can copy the license key on your cluster that is displayed in Data Management.

Procedure

If you selected Dark Sites at Step 2 in Manage Licenses in the Data Management Cluster, the **Licensing Steps** page is displayed.

1. Log in to your cluster.
2. Select **Settings** > **License**.
3. On the **Licensing Steps** page, paste the license key that is copied from Data Management, and click **Upload**.

   The "License Activated" message will display. This message indicates that the license is activated on that cluster.

Configuring the license after cluster creation

Before you configure the license for your Data Protect cluster, refer “License Modes” on page 61 to learn about the licensing modes and choose a licensing mode that is suitable for your business requirement and then configure the license.

Choosing a licensing mode after cluster creation

To configure the license, you can choose a licensing mode after cluster creation.

Procedure

If you chose the **Skip License** option when you created the cluster (at step 3 when you Choose the Licensing Mode), complete the following steps to configure licensing for your Data Protect cluster:

1. Log in to your Data Protect cluster.
2. From the menu, select **Settings** > **License**.

   If the license is not configured, the **License** page displays the *Configure License* link and the number of days within which you must configure the license. License must be configured within 180 days of creating the cluster.
3. To configure the license, click **Configure License**.
4. In the floating menu that appears, select one of the following modes and click **Apply**:

   - Data Management Smart Licensing
   - Manual Licensing
   - Dark Site

   Follow the procedures to configure a license mode.

Configuring smart licensing mode

After you chose smart licensing mode after cluster creation, you can configure the licensing mode.

Procedure

To configure Data Management smart licensing, complete the following steps:

1. Follow the steps in the Choose a Licensing Mode after Cluster Creation section and select Data Management Smart Licensing as the licensing mode.
2. From the **Management Options** page, select the **Connect to Data Management only for licensing** option.
3. Click **Continue**.

   You are redirected to the Data Management page to enter credentials to log in.
4. Click **Connect** to establish the connection with Data Management.

   Only the licensing information is shared with Data Management.

Configuring manual licensing mode

After you chose manual licensing mode after cluster creation, you can configure the licensing mode.

Before you begin

Configuring the Manual Licensing Mode requires you to download the License Usage Report from the Data Protect cluster and upload it to Data Management. Also generate the License File in Data Management and upload it to the Data Protect cluster. As these steps require switching between the Data Protect cluster and Data Management, it is preferred that you remain logged in to both the Data Protect cluster and Data Management until you complete the Manual License configuration.

Procedure

Perform the following steps to configure Manual Licensing:

1. Follow the steps in the Choose a Licensing Mode after Cluster Creation section and select Manual Licensing as the Licensing Mode.
2. On the **Licensing Steps** dialog box, click **Download License Usage Report**.

   The License Usage Report file or the Audit Report is downloaded to your local. The Audit Report contains details such as cluster ID, timestamp, license usage data, and entitlements.
3. To upload the Audit Report, complete the following steps:

   a. Log in to Data Management and navigate to **Settings** > **License**. The license summary of all clusters connected to Data Management is displayed.

   b. Click **Upload Audit Report**.

   c. In the **Upload Audit Report** dialog box, upload the Audit Report downloaded at step 2.

   d. Click **Submit**.
4. To generate the License File, complete the following steps:

   a. From your Data Protect cluster, navigate to **Settings** > **License**. On the **Licensing Steps** page, select **Copy Cluster ID**.

   b. From Data Management, click **Generate License File**.

      The **Generate License File** dialog box appears and prompts for the Cluster ID.

   c. Paste the Cluster ID copied in Step 4 (a) and click **Generate**.

      The License File is downloaded to your local system.
5. To upload the License File, complete the following steps:

   a. From your Data Protect cluster, navigate to **Settings** > **License**.

b. On the **Licensing Steps** page, click **Select File**.

c. Browse to select the License File downloaded at Step 4 (c) and click **Upload**.

What to do next

After Manual Licensing is configured, you must download the audit report from the Data Protect cluster and upload it on Data Management every 180 days.

Configuring dark site mode

After you chose dark site mode after cluster creation, you can configure the licensing mode.

Before you begin

To set up a cluster as a dark site, you must contact your IBM sales representative and submit a request. If your request is approved, the license key is displayed in Data Management.

Procedure

To setup the dark site mode, complete the following steps:

1. Follow the steps in the Choose a Licensing Mode after Cluster Creation section and select **Dark Site** as the Licensing Mode.
2. To copy the license key from Data Management, complete the following steps:
   a. Log in to Data Management and navigate to **Settings** > **License**. The alpha-numeric license key is displayed in the License page.
   b. Copy the License key.
3. Log in to your Data Protect cluster.
4. Select **Settings** > **License**
5. On the **Licensing Steps** page, paste the license key that is copied from Data Management, and click **Upload**. The message License Activated will display. This message indicates that the license is activated on that cluster.

Detecting ransomware attacks

Ransomware can take over enterprise data and threaten to publish it or block access to it until a ransom is paid. Backups, once considered defense against ransomware, are now a prime target for ransomware that destroys shadow data copies and restore point data.

IBM Storage Defender Data Management Service uses machine learning algorithms to continuously monitor changes in the backup data ingestion rate for your organization. If the rate is out of the normal range—based on daily and historical rates—Data Management flags it as a potential ransomware attack and alerts both your IT administrators and the Data Management platform support team. Administrators can then perform rapid restores from the last healthy snapshot to recover VMs, files, and application objects.

Prerequisites

Ensure the following prerequisites are met to detect, flag, and alert ransomware attacks in Data Management.

- The Data Protect cluster version must be running at a supported version, see IBM Storage Defender: Data Protect support information.
- Data Protect cluster managed through Data Management.
- Indexing must be enabled on the protection group.

Supported Workloads

The following table lists the workloads and the backup type for each workload that supports anomaly detection.

Source Type		Supported Backup Type	Affected Files List
Virtual Machines	Acropolis (AHV)	Block-based	Not supported
	AWS VMs	• Data Management Protection Service • Native Snapshot	Not supported
	AzureVMs	• Data Management Protection Service • Native Snapshot	Not supported
	Hyper-V	File-based	Supported
	VMware	Block-based	Supported
	KVM	Block-based	Not supported
Databases	Microsoft SQL Server	Block-based	Not supported
NAS	PureStorage FlashBlade	File-based	Supported
	GenericNAS	File-based	Not supported
	Isilon	File-based	Supported
	NetApp	File-based	Supported
Physical Servers	Physical	• Block-based • File-based	Supported
Applications	Active Directory	Block-based	Not supported
	MS Exchange Server	Block-based	Not supported
SAN	Pure	Block-based	Supported
Views	Data Management View	File-based	Supported

Viewing affected objects

You can view the affected objects in the Data Management Dashboard.

Procedure

To view the affected objects, complete the following steps:

1. In the Data Management Dashboard, select **All Clusters** from the navigation menu.
2. Click **Dashboards**

3. Select **Security** from the drop-down list.
4. Click the **Anti-ransomware** tab.

   The anomaly alerts appear under the **Anti-ransomware** tab in the Security dashboard.

   The **System with Affected Objects** section displays a map with all the clusters that have an anomaly. Clusters with an anomaly are indicated in red on the map. Hover on the legends in the map to analyze the anomalous occurrences. It also shows the:

   - Total number of affected sources
   - Total number of affected protections
   - Total number of affected systems
   - Total number of anomalous snapshots
   - Date and time of the first and latest detected snapshots

   The **Objects with Anomalous Snapshots** section displays a list of objects with anomalous snapshots along with the object name, latest anomalous snapshot, anomaly strength, source, and system name.

   You can filter the object type using the **Object Type** filter.

   You can customize the time frame by selecting **Last Day**, **Last Week**, **Last Month**, or **Last Quarter**.

   For more information, see Anomalous Object Details.

Configuring tags and notifications thresholds

Use the anomalous object settings to configure the notification threshold, add a tag name, and allow restore of tagged snapshots. You can access the **Settings** page either by clicking **Settings** in the **Anti-ransomware** tab (appears if there are no anomalies present during the selected time frame) or by clicking (⚙) in the **Objects with Anomalous Snapshots** section.

Configuring anomaly strength threshold

Anomaly strength threshold is a prediction setting that helps you to identify unusual change rates in the backup data. Data Management uses machine learning algorithms to continuously monitor backups for any anomaly. If an anomaly is detected, an anomaly alert is generated. All anomaly alerts have an associated anomaly strength with a numeric value between 0 to 100. The anomaly strength is a measure of the confidence of anomaly prediction. The Data Management dashboard triggers an email notification regarding the alert only if the anomaly alert has an anomaly strength greater than the anomaly strength threshold set by the user. By default, the anomaly strength is 70%. You can add or edit the email address to which you want to receive the ransomware alert. For more information, see Manage Alert Notifications Rule.

For example, set the Anomaly Strength Threshold to 50%, any alert with an anomaly strength higher than 50 will trigger an email notification. Email notifications are not sent if the detected anomaly strength is less than or equal to 50%.

To configure the notifications threshold, complete the following steps:

1. In the **Objects with Anomalous Snapshots** section, click ⚙.
2. Use the slider to increase or decrease the anomaly strength.
3. Click **Save**.

   Note: The lesser the anomaly strength, the more email notifications are triggered.

Adding a tag name

A tag name can be applied to an anomalous snapshot. By default, the tag name for snapshots is added automatically if the snapshot has an anomaly strength that is greater than the defined threshold. The tag name appears next to the anomalous snapshot in the **Objects with Anomalous Snapshots** section. The default tag name is **Blocked**. You can edit the default tag name and add a new tag name.

Complete the following steps to edit or add a tag name:

1. In the **Objects with Anomalous Snapshots** section, click ⚠.
2. In the **Tag Name** field, enter the tag name.
3. Click **Save**.

Blocking restores of tagged snapshots

Tagged snapshots are snapshots that have an anomaly strength above the defined threshold. You can block the restore of tagged snapshots. This is an optional setting and by default the **Block recoveries from tagged snapshots** checkbox is clear.

To block a tagged snapshot from restore, complete the following steps:

1. In the **Objects with Anomalous Snapshots** section, click ⚙.
2. Select the **Block recoveries from tagged snapshots** checkbox.
3. Click **Save**.

Anomalous object details

The **Anomalous object details** page provides information about the specific cluster with anomaly snapshots, anomaly strength, source, system name, the total number of files added or modified and the total number of files detected with an anomaly.

From the list of anomalous objects, click the link of any object to view more details. The snapshots are displayed on a graph. The y-axis shows the file size and the x-axis shows the time.

The legends on the graph indicate the following categories of snapshots:

- Red – Anomalous snapshot.
- Blue – Clean snapshot.
- Green – Latest clean snapshot.

Hover on each snapshot on the graph to view more details of the snapshots.

Add Object to Recover

Click **Add Object to Recover** to recover an anomalous object. For more information, see Recover Objects.

Ignore Anomaly

Click **Ignore Anomaly** if you do not want email notifications for the anomalous snapshot for 30 days. Data Management continues to evaluate the protection runs but does not trigger an alert for 30 days or until the anomaly strength is more than the anomaly strength of the ignored alert.

Snapshots

The Snapshot tab lists all the anomalous snapshots, clean snapshots, latest clean snapshots, tagged and untagged snapshots. You can filter the list by using the Tag and Type filters.

Following are the available options in the **Tag** filter:

Tagged:

Lists only the anomalous snapshots that have a tag name.

Untagged:

List only the anomalous snapshots that do not have a tag name.

The available options in the **Type** filter are:

Anomalous Snapshot:
Lists only the anomalous snapshots.

Clean Snapshot:
List only the clean snapshots.

Tagging one or more anomalous snapshots

By default, Data Management adds the tag name for snapshots that have an anomaly strength above the defined threshold. You can manually tag an anomalous snapshot.

Before you begin

Note: Only users with the **Enable or disable snapshot tagging feature** privilege can add or remove a tag.

Procedure

To manually tag anomalous snapshots, complete the following steps:

1. In the Data Management Dashboard, select **All Clusters** from the navigation menu.
2. Select **Security** from the drop-down list.
3. Click the **Anti-ransomware** tab.
4. In the **Objects with Anomalous Snapshots** section, click the anomalous objects that need a tag in the list.
5. Click the **Snapshots** tab.
6. From the snapshots list, select one or more snapshots checkbox for which you want to add a tag.
7. Click **Apply Tag**.

   Note: The tag name that appears for the anomalous snapshot is the name in the **Tag Name** field in **Settings**.
8. Click **Confirm**.

Removing tags from one or more anomalous snapshots

Procedure

You can manually remove the tag from an anomalous snapshot.

Note: Only users with the **Enable or disable snapshot tagging feature** privilege can add or remove a tag.

To manually tag anomalous snapshots, complete the following steps:

1. In the Data Management Dashboard, select **All Clusters** from the navigation menu.
2. From the drop-down, select **Security**.
3. Click the **Anti-ransomware** tab.
4. In the **Objects with Anomalous Snapshots** section, click the anomalous objects that needs a tag in the list.
5. Click the **Snapshots** tab.
6. From the snapshots list, select one or more snapshots checkbox for which you want to add a tag.
7. Click **Remove Tag**.
8. Click **Confirm**.

Affected files

The **Affected Files** tab shows the list of files that have changed between the clean snapshots and anomalous snapshots. It also shows if the file is added, modified, or deleted under the **Changed Type** column.

The **Affected Files** tab shows the anomalous snapshots for the following workloads only:

Source Type		**Supported Backup Type**
Virtual machines	VMware	Block-based
	Hyper-V	File-based
Physical servers	Physical	• Block-based • File-based
SAN	Pure	Block-based
NAS	NetApp	File-based
	Isilon	File-based

Recovering deleted files

You can recover a file from the list of files that are changed between the clean snapshot and the anomalous snapshot.

Procedure

To recover a deleted file, complete the following steps:

1. In the Data Management dashboard, select **All Clusters** from the navigation menu.
2. Select **Security**, from the drop-down.
3. In the **Objects with Anomalous Snapshots** section, click the object.
4. Click the **Affected Files** tab.
5. Hover over the file that you want to restore, click the Actions menu (⋮) and then click **Recover**.

Downloading files

You can download a file from the list of files that are changed between the clean snapshot and the anomalous snapshot.

Procedure

To download the affected file, complete the following steps:

1. From the Data Management dashboard, select **All Clusters** from the navigation menu.
2. Click **Security**.
3. In the **Objects with Anomalous Snapshots** section, click the object.
4. Click **Affected Files** tab.
5. Hover over the file you want to restore, click the Actions menu ⋮ and then click **Download File**.

Recovering objects

You can recover one or more anomalous objects from the Data Management dashboard.

Before you begin

Note: Only users with the **Restore from tagged snapshots** privilege can restore tagged snapshots.

Procedure

To recover objects, complete the following steps:

1. In the Data Management Dashboard, select **All Clusters** from the navigation menu.
2. Select **Security**, from the drop-down list.
3. In the **Objects with Anomalous Snapshots** section, click the object.
4. In the **Objects with Anomalous Snapshots** section, select the checkbox for the objects you want to recover or on the anomalous objects details page, click **Add Object to Recover**. The object is selected for recovery and redirects you back to the **Anti-ransomware** page.
5. Click **Recover**. The **Review Bulk Recovery** page appears. By default, the latest clean snapshot is selected for recovery.
6. Select **Custom** to choose a different recovery point and click icon ✎ to change the recovery point.
7. Click **Recover** to complete the recovery operation.

Managing alert notification rules

You can add or edit or delete the email address to which you want to receive the notifications.

Adding alert notification rules

You can add alert notification rules for the email address.

Procedure

To add an alert notification rule, complete the following steps:

1. Navigate to **System** > **Health** and click the **Notifications** tab.
2. Click **Create** > **New Alert Notification Rule**.

   The **Create Alert Notification Rule** page is displayed.
3. In the **Notification Name** field, specify a name.
4. From the **Alert Source** drop-down, select one or all clusters.
5. From the **Alert Severity** drop-down, select one or all severity.
6. From the **Alert Type** drop-down, select **Maintenance**.
7. From the **Alert Category** drop-down, select **Security**.
8. From the **Alert Name** drop-down, select **Data Ingest Anomaly Alert**.
9. Under **Create Notifications via**:

   a. Select the **Email** check box.

   b. Under **Email**, complete the following steps:

      i) Select **To** and type an email address or distribution list of the recipients to whom you plan to send the email notification.

      ii) Select **CC** and type an email address or distribution list of the recipients to whom you plan to send a copy of the email notification.

      iii) Click the add icon ⊕ to add more recipients. Click the delete 🗑 icon to delete recipients.
10. Click **Create**.

Results

The new alert notification rule appears in the **Notifications** tab.

Editing alert notification rules

You can edit an alert notification rule to add or remove the email address.

Procedure

To edit an alert notification rule, complete the following steps:

1. Navigate to **System** > **Health** and click the **Notifications** tab.
2. Click the edit icon ✏ .

   The **Edit Alert Notification Rule** page is displayed.
3. Add or remove the email address.
4. Click **Save**.

Results

The updated alert notification rule is applied from the next alert that is triggered.

Deleting alert notification rules

You can delete an alert notification rule from the **Notifications** tab.

Procedure

To delete an alert notification rule, complete the following steps:

1. Navigate to **System** > **Health** and click the **Notifications** tab.
2. Click the delete 🗑 icon for the alert notification that you plan to delete.

   The **Delete Notification** page is displayed.
3. Click **Delete**.

Results

The alert notification rule is removed from the **Notifications** tab.

Viewing the alert

You can view the alert in **Data Ingest Anomaly Alert**.

Before you begin

The ransomware Alert is CE01516011 Data Ingest Anomaly Alert.

Procedure

To view the alert, complete the following steps:

1. Navigate to **All Clusters** from the navigation menu.
2. Navigate to **System** > **Health**.

   The list of all alerts is displayed on the **Health** page.
3. From the **Category** drop-down, select **Security**, and click **Apply**.
4. Locate the alert that is named **Data Ingest Anomaly Alert**.
5. Click **Data Ingest Anomaly Alert** to view the details for this alert such as Alert Code, Severity, Type, Category, and Status along with the description and cause of the alert.

Frequently Asked Questions

1. Are all anomalous snapshots tagged?

   No, all snapshots are not tagged. Only snapshots with anomaly strength more than the defined threshold are tagged with a specific name.

2. Will the tag name automatically update if I change the existing tag name?

   Yes. All the existing snapshots with the previous label will be relabeled with the new tag name. Also, all new anomalous snapshots with anomaly strength more than the threshold will be tagged with the new tag name.

3. Are snapshot tags available on on-prem Data Management dashboard?

   No, anomalous snapshot tags are not available on on-prem Data Management dashboard. Snapshots are not blocked from recovery on on-prem cluster.

4. Does tagged snapshots prevent future backups?

   No, anomalous snapshot tags do not prevent future backups of the same job or the same entity.

5. Is blocking of tagged snapshot recovery also prevented in screens other than Data Management Security Dashboard?

   Yes, it is blocked from all the screens in the Data Management Dashboard. Even pass-through cluster screens will have tagged snapshot blocked.

6. Can all users restore from tagged snapshots?

   No, only users with the **Restore from tagged snapshots privilege** can restore from tagged snapshots

7. Can all users add or remove tags from snapshots?

   No, only users with the **Enable or disable snapshot tagging feature** privilege can add or remove a tag.

8. Do all users have the **Settings** icon in the **Objects with Anomalous Snapshots** section?

   No, only users with administrative privileges have the Settings icon ⚙ in the **Objects with Anomalous Snapshots** section.

9. Can a user log in to the Data Management Dashboard and restore a snapshot that is tagged in Data Management?

   Yes, users can log in to the Data Management Dashboard and restore a snapshot that is tagged in Data Management.

   Workaround: To prevent users from directly restoring tagged snapshots from the Data Management dashboard, you must assign specific roles to users that do not have permission to restore. For example, the **Viewer** role.

10. Are all ransomware alerts (CE01516011) triggered because of anomalous snapshots?

    No, all alerts triggered may not be because of anomalous snapshots. There might be some false positives.

    For example, if there is a sudden rise in the data ingestion rate that might be out of the normal range - based on daily and historical rates, Data Management might consider it as a potential ransomware attack. The alert helps the IT administrators and the IBM support team to administer the issue and if required perform a restore from the healthy snapshot.

Quorum approvals

Quorum approval on Data Management is an authorization model. The quorum approval ensures that a predefined quorum of approvers must approve sensitive or privileged operations that are requested by Data Management before those operations are run.

Quorum approvals help you eliminate the risk associated with a unitary, highly privileged administrator - specifically to prevent a rogue, poorly trained, or compromised administrator from performing sensitive or privileged operations on the Data Management platform without authorization or oversight.

In Data Management, you can define a group of users called a quorum group who can decide to approve whether defined operations initiated by a Data Management user are allowed to be run or not.

Note: Only Data Management users and persistent SSO users are supported for a quorum group.

How do quorum approvals work?

After you create a quorum group in Data Management, any operation that is controlled by the quorum group requires approval from the group's users or approvers for execution. In other words, after a Data Management user initiates an operation that is covered by a quorum group, it will not run immediately. Instead, a request for approval of that operation is sent to the approvers in the quorum group, where the approvers are asked to either approve or reject the request. It is also possible that approvers fail to act on a request on time.

Quorum-protected operations run when the approval request receives the minimum number of approvals that are configured in the quorum group. This might be as few as a single approval or as much as unanimous approval, which can be every approver that is defined in the quorum group must approve. When the requested operation reaches the approval threshold that is defined in the quorum group (within a defined time limit), the requested operation is run immediately.

Similarly, it is possible that enough approvers will explicitly reject a requested operation, and then it is no longer possible to reach the minimum approval threshold. In that case, the operation will be rejected and set to not run.

It is also possible that some approvers fail to act, where the approvers neither approve nor reject a requested operation within the time limit that is defined in the quorum group. In that case, the operation will be auto-approved or auto-denied after the time limit that is set in the approval workflow settings of the quorum group.

Considerations

Before you start running operations by using quorum approvals, ensure that you understand the following considerations:

- The operations under quorum approval have a delay in execution. This delay is because the operation runs only when a sufficient number of approvals are received from approvers as defined in the quorum group or the operation falls back to auto-approval after a time limit defined in the quorum group. Hence, the users initiating an operation under quorum must wait for the operation's approval prior to its execution.
- Only one operation of each operation type is queued for quorum approval at any given time. For example, suppose a request to add a new user is awaiting quorum approval. In that case, any other requests to add new users are not accepted until the existing add user operation is approved or denied.
- Quorum approval is complementary to, but different from RBAC. Quorum approvers who are approving an operation request need not be granted an RBAC role with permission to initiate the operation. RBAC only enforces who can initiate an operation, not who can approve it.
- Quorum supports Data Protect cluster and Data Management operations. The operations can be granular to the API endpoint level. For information about using Data Management Reporting APIs, click the Help Center icon ? on the menu bar and select **Get REST APIs**.
- Operations under quorum execute in the order that they are approved, not the order they were initiated.
- Only the user who initiated the operation under quorum can withdraw the request. An admin cannot withdraw the pending request.
- The quorum approval process is now enhanced to manage scenarios where a quorum member initiates a quorum-protected operation. When a quorum member initiates a quorum-protected operation, the request is auto-approved for the requester. The other members in the quorum group must approve the request for the quorum- protected operation to execute.

  For example,

In a quorum group with 3 members, with the approval quorum set to **At least 2**, if a member in the quorum group initiates the request to execute a quorum-protected operation, then one of the members apart from the requester must approve the request.

Best practices

When you implement quorum, the following best practices are helpful to streamline operations:

- Use the predefined templates to identify the sensitive or privileged operations that should be included in a quorum group. Unless instructed by IBM support, do not attempt to select individual operations in a quorum group manually from the List view.
- Implement quorum groups with a small number of sensitive or privileged operations in a specific operational area of the Data Management platform. As your organization's quorum gets familiar with reviewing and approving requested operations, slowly expand quorum approval to other operations.
- It is better to maintain multiple quorum groups for different operational areas (for example, access management, network configuration, data protection settings, and so on.) versus a single quorum group covering every possible sensitive or privileged operation. This allows different approvers and approval thresholds to be defined for different types of operations.
- Add at least two or more users to the quorum group. Quorum groups with many possible approvers and the lowest possible approval threshold (based on your organization's security policy) will be the most operationally efficient and resilient.
- Identify the minimum number of approvers based on your organization's security policy. Adding more approvers than a minimum necessary approvers might further delay the execution of operations.
- Avoid configuring quorum groups that require unanimous approval. If a single approver fails to respond on time, the operation may be delayed or not run.
- Actively maintain quorum groups. Periodically review the lists of approvers and adjust as needed, especially to remove users no longer responsible for approving operations on the Data Management platform.
- Quorum groups can get into a deadlock scenario when a sufficient number of quorum members are unavailable to make a Quorum decision, whether permanently or temporarily. The deadlock scenario arises as the quorum group cannot be modified without quorum approval from the members. Also, the operations that are secured by the quorum group cannot be run.

  The following are examples of the Quorum deadlock scenarios:

Number of Members in the Quorum Group	Number of Approvers in the Quorum Group	Minimum Number of Unavailable Members for the Deadlock to Happen
2	2	1
3	2	2
3	3	1
4	2	3

  To resolve the Quorum deadlock scenario, contact IBM support.
- **Recommendation:** Use the defined number of members that is **n/2+1**, where **n** is the total number of members in the quorum group for quorum approvals.

Quorum dashboard

The quorum dashboard lists the quorum requests and the quorum groups. To view the quorum dashboard, navigate to **Security** > **Quorum**.

The **Quorum** page consists of the following tabs:

- Pending Requests
- My Requests
- All Requests
- Groups

Pending requests

The **Pending Requests** tab lists all the pending requests for logged-in user’s approval.

Suppose that the logged-in user is part of the quorum group and initiates a quorum-protected operation. In that case, the operation is not listed for approval in the **Pending Requests** for the logged-in user.

The tab provides the following details:

Details	Description
Operation	Details of the operation for quorum approval.
Your Decision	The current status of your approval.
Operation Target	The target on which the requested operation would be performed.
Requester	The user who has requested the quorum approval for the operation.
Expires on	The expiry date and time of the request.

My requests

The **My Requests** tab lists all the requests that you have initiated for quorum approval.

The tab provides the following details:

Details	Description
Operation	Details of the operation for quorum approval
Quorum Decision	The current status of the approval
Operation Target	The target on which the requested operation would be performed.
Request on	The date and time when the request was initiated.
Expires on	The expiry date and time of the request.

All requests

The **All Requests** tab lists all the requests that have been initiated for quorum approval.

The tab provides the following details:

Details	Description
Operation	Details of the operation for quorum approval.
Quorum Decision	The current status of the quorum approval.
Your Decision	The current status of your approval.
Operation Target	The target on which the requested operation would be performed.

Details	Description
Requester	The user who has requested the quorum approval for the operation.
Request on	The date and time when the request was initiated.
Expires on	The expiry date and time of the request.

Group

The **Groups** tab lists all quorum groups that are created in Data Management. Use the **Groups** tab to create a new quorum group or manage existing quorum groups.

The tab provides the following details:

Details	Description
Name	The name of the quorum group.
Status	The status of the quorum group.
Approvers	The details of the approvers in the quorum group.
Operations	The number of operations protected by the quorum group.
Operation Target	The target on which the requested operation would be performed.

Creating a quorum group

Before you create a quorum group, ensure that you review the considerations and best practices for using quorum in Data Management.

Before you begin

Important: A quorum group can be created only by a user with a **Super Admin** role.

Procedure

To create a quorum group, complete the procedure:

1. In the Data Management dashboard, navigate to **Security** > **Quorum** and select the **Groups** tab.
2. In the **Groups** tab, click **Create Group** to open the **Create Quorum Group** page.
3. In the **Group Details** section, enter a **Name** for the group, select the **Operation Target**, and provide a brief **Description** for the group.

   Note: By default, Data Management is selected as the **Operation Target**. If you plan to configure the quorum group for only Data Management operations, you can skip selecting the **Operation Target**.
4. Click the **Operations** section and select any of the following operation templates as per your requirement, for a detailed list of operations that are provided in the respective operation templates, see "Supported operations" on page 82.

   Note: The **Templates** tab used to select the operation templates is disabled. Instead, use the **List** tab to search and add the operation that you want the quorum group to govern.

Template	Description
Cluster Management	Includes all the operations that are related to Data Management cluster administration and security settings.

Template	Description
Storage Management	Includes all the operations that are related to storage domain, view, and external target management.
Data Protection	Includes all the operations that are related to data protection.
Networking Management	Includes all the Data Protect cluster network settings and management operations.

Click **List** and search and add the operation that you want the quorum group to govern using the **Search** bar. You can use the available filters to narrow your search.

5. Click the **Approvers** section and complete the following steps:

   a. Select the **Members** for the quorum group from the drop-down list.

      Note: The users that you select as **Members** of the quorum group must be assigned the **Viewer** role at a minimum. Also, you can add a user with a **Custom** role to the quorum group as approvers.

   b. For the **Approval quorum**, select **All members** or **At least**.

      - If you select **All members**, the operation that is protected by the quorum requires approval from all the members in the quorum group.

   c. The unanimous **All members** approval is not a recommended best practice.

      - If you select **At least** and define the **number of members**, then the operation that is protected by the quorum requires approval from only the defined number of members.
      - **Recommendation:** The minimum supported number of members (**At least**) is **2**, and the maximum is the number of members in the quorum group. Use the defined number of members that is **n/2+1**, where **n** is the total number of members in the quorum group.

6. In **Approval Workflow**, add the configuration to auto approve or deny the request after the request expires.
7. Click **Create**.

Supported operations

The following table lists the Data Management operations in the Cluster Management operation template:

Operation Template	Operation Category	Operation Description
Cluster Management	Tenant	Enable Data Management for a tenant.
	Data Protect clusters	Specifies the request to upgrade clusters from Data Management. Specifies the request to unregister clusters on Data Management

Supported cluster operations

The following table lists the various cluster operations in the respective operation templates:

Operation Template	Operation Category	Operation Description
Cluster Management	Key Management System	Update KMS.
		Delete KMS.
		Add KMS.
	Network Reset	Set or cancel cluster reset state. This operation is a destructive operation.
	Active Directory	Update the machine accounts of an Active Directory.
		Update the list of trusted domains to be ignored during trusted domain discovery of an Active Directory.
		Update the Preferred Domain Controllers.
	Platform	Assimilate disks.
		Mark the disk for removal.
		Update the racks.
		Update cluster UI configuration.
		Mark the node for removal.
		Create racks.
	Support Channel	Update the support channel configuration.
	Security	Update cluster security settings.
	Clusters	Remove a node from a Data Management cluster.
	Syslog	Update a Syslog server by ID.
		Remove Syslog server by ID.
	Anti virus Service Group	Delete an anti virus service group corresponding to the specified anti virus service group ID.
		Update an anti virus service group.
	KMS Configuration	Delete a KMS configuration for a provided ID. Update KMS configurations in the cluster.
	Remote Cluster	Delete a remote cluster registration connection.
	Principals	Update the Linux user password.

Operation Template	Operation Category	Operation Description
Networking Management	Vlan	Remove the specified VLAN from the Data Management cluster.
		Update a specific VLAN of the Data Management cluster.
		Creates a VLAN of the Data Management cluster.
	IPMI	Update the cluster IPMI user information.
		Update the cluster IPMI network information.
	Platform	Update Host Mappings.
	Clusters	Update the external Client subnet of the cluster.
	Firewall	Update the cluster firewall.
	Route	Create a Static Route on the Data Management cluster.
		Delete a Static Route on the Data Management cluster.

Operation Template	Operation Category	Operation Description
Storage Management	External Target	Create an External Target.
		Delete an External Target.
		Update an External Target.
		Update External Target Settings.
	Storage Domain	Delete a Storage Domain.
		Create CAD Storage Domains.
		Update a Storage Domain.
	View Boxes	Update a Domain (View Box).
	Remote Storage	Register Remote Storage.
		Update Remote Storage Configuration.
	Principals	Reset the S3 secret access key for the specified user on the Data Management cluster.
	View	Update a View Template.
		Delete a View Template.
		Update a View.

Operation Template	Operation Category	Operation Description
Data Protection	Protection Runs	Update how long Protection Job runs and their snapshots are retained on the Data Management cluster.
		Cancel a Protection Job run.
	Object	Cancel object runs.
	Protection Sources	Unregister a previously registered Protection Source.
	Policy	Update a Protection Policy.
		Delete a Protection Policy.
	Protection Group	Perform an action like pause, resume, active, or deactivate on all specified Protection Groups.
		Update runs for a particular Protection Group.
		Delete a Protection Group.
		Action son a protection group run.
		Update a Protection Group.

Managing quorum groups

In IBM Storage Defender Data Management Service, a quorum group configuration includes operation target, operations, approval quorum, and approval workflow. You can modify the existing quorum groups based on your requirement.

Important:

- An existing quorum group can modified by only the quorum member in the group. Also, the operation requires quorum approval.
- You cannot modify the quorum group if there are pending requests for the operations that are controlled by the quorum group.
- Quorum groups can get into a deadlock scenario when a sufficient number of quorum members are unavailable to make a Quorum decision, whether permanently or temporarily. The deadlock scenario arises as the quorum group cannot be modified without quorum approval from the members. Also, the operations that are secured by the quorum group cannot be run.

The following are examples of the Quorum deadlock scenarios:

Number of Members in the Quorum Group	Number of Approvers in the Quorum Group	Minimum Number of Unavailable Members for the Deadlock to Happen
2	2	1
3	2	2
3	3	1

Number of Members in the Quorum Group	Number of Approvers in the Quorum Group	Minimum Number of Unavailable Members for the Deadlock to Happen
4	2	3

To resolve the Quorum deadlock scenario, contact IBM support.

Adding new operation targets

You can add new operation targets to the existing quorum group.

Procedure

To add new operation targets to the quorum group, complete the following steps:

1. In the Data Management Dashboard, navigate to **Security** > **Quorum** and select the **Groups** tab.
2. Find the quorum group that you need in the **Groups** tab and click the **Edit** icon on that row to open the **Edit Quorum Group** page.
3. Under the **Group Details** section, select the **Operation Target** from the drop-down list that you plan to add to the quorum group configuration.
4. Click **Save**.

Removing operation targets

You can remove operation targets from the existing quorum group.

Before you begin

Note: An existing quorum group can be modified only by the quorum member in the group. Also, the operation requires quorum approval.

If you have pending requests for the operations that are controlled by the quorum group, you cannot modify the quorum group.

Procedure

To add new operation targets to the quorum group:

1. In the Data Management dashboard, navigate to **Security** > **Quorum** and select the **Groups** tab.
2. Find the quorum group that you need in the **Groups** tab and click the **Edit** icon on that row to open the **Edit Quorum Group** page.
3. Under the **Group Details** section, deselect the **Operation Target** from the drop- down list that you plan to remove from the quorum group configuration.
4. Click **Save**.

Adding new operations

You can add new operations to the existing quorum group for quorum approval.

Note: An existing quorum group can be modified by the quorum member in the group. Also, the operation requires quorum approval.

If you have pending requests for the operations that are controlled by the quorum group, you cannot modify the quorum group. To add new operations to the quorum group, complete the following steps:

1. In the Data Management Dashboard, navigate to **Security** > **Quorum** and select the **Groups** tab.
2. Find the quorum group that you need in the **Groups** tab and click the **Edit** icon on that row to open the **Edit Quorum Group** page.

3. Click the **Operations** section and add any of the following operation templates as per your requirement, for a detailed list of operations that are provided in the respective operation templates, see "Supported operations" on page 82.

Template	**Description**
Cluster Management	Includes all the operations that are related to Data Protect cluster administration and security settings.
Access Management	Includes all the operations that are related to user management, Identity Provider settings, authentication, and access control.
Storage Management	Includes all the operations that are related to storage domain, view, and external target management.
Data Protection	Includes all the operations that are related to data protection.
Networking Management	Includes all the Data Protect cluster network settings and management operations.

Removing operations

You can remove the operations that you specified in your existing quorum group for quorum approval.

Before you begin

Note: An existing quorum group can be modified only by the quorum member in the group. Also, the operation requires quorum approval.

If you have pending requests for the operations that are controlled by the quorum group, you cannot modify the quorum group.

Procedure

To remove operations from the quorum group configuration, complete the following steps:

1. In the Data Management Dashboard, navigate to **Security** > **Quorum** and select the **Groups** tab.
2. Find the quorum group that you need in the **Groups** tab and click the **Edit** icon on that row to open the **Edit Quorum Group** page.
3. Click the **Operations** section and deselect the operation(s) that you plan to remove from the quorum group configuration.
4. Click **Save**.

Adding new quorum approvers

You can add new quorum approvers to the quorum group configuration.

Before you begin

Note: An existing quorum group can be modified only by the quorum member in the group. Also, the operation requires quorum approval.

If you have pending requests for the operations that are controlled by the quorum group, you cannot modify the quorum group.

Procedure

To add new quorum approvers to the quorum group, complete the following steps:

1. In the Data Management Dashboard, navigate to **Security** > **Quorum** and select the **Groups** tab.
2. Find the quorum group that you need in the **Groups** tab and click the **Edit** icon on that row to open the **Edit Quorum Group** page.
3. Click the **Approvers** section and select the **Members** for the quorum group from the drop-down list.
4. Click **Save**.

Removing quorum approvers

You can remove quorum approvers from the quorum group configuration.

Before you begin

Note: An existing quorum group can be modified only by the quorum member in the group. Also, the operation requires quorum approval.

If you have pending requests for the operations that are controlled by the quorum group, you cannot modify the quorum group.

Procedure

To remove quorum approvers from the quorum group, complete the following steps:

1. In the Data Management Dashboard, navigate to **Security** > **Quorum** and select the **Groups** tab.
2. Find the quorum group that you need in the **Groups** tab and click the **Edit** icon on that row to open the **Edit Quorum Group** page.
3. Click the **Approvers** section and deselect the **Members** from the list whom you plan to remove from the quorum group configuration.

   Note: Ensure that you have at least two or more members in the quorum group.
4. Click **Save**.

Modifying the approval quorum

You can modify the Approval Quorum settings that you configured on the quorum group.

Before you begin

Note: An existing quorum group can be modified only by the quorum member in the group. The operation requires quorum approval.

If you have pending requests for the operations that are controlled by the quorum group, you cannot modify the quorum group.

Procedure

To modify the Approval Quorum settings, complete the following steps:

1. In the Data Management Dashboard, navigate to **Security** > **Quorum** and select the **Groups** tab.
2. Find the quorum group that you need in the **Groups** tab and click the **Edit** icon on that row to open the **Edit Quorum Group** page.
3. Click the **Approvers** section and in **Approval quorum**, select **All members** or **At least**
   a) If you select **All members**, the operation that is protected by the quorum requires approval from all the members in the quorum group.
   b) If you select **At least** and define the **number of members**, then the operation that is protected by the quorum requires approval from only the defined number of members.

4. Click **Save**.

Modifying the approval workflow

You can modify the Approval Workflow settings that you configured on the quorum group.

Before you begin

Note: An existing quorum group can be modified only by the quorum member in the group. The operation requires quorum approval.

If you have pending requests for the operations that are controlled by the quorum group, you cannot modify the quorum group.

Procedure

To modify the Approval Workflow, complete the following steps:

1. In the Data Management Dashboard, navigate to **Security** > **Quorum** and select the **Groups** tab.
2. Find the quorum group that you need in the **Groups** tab and click the **Edit** icon on that row to open the **Edit Quorum Group** page.
3. Click the **Approvers** section and in **Approval Workflow**, based on your requirement, modify the configuration to auto approve or deny the request after the
4. Click **Save**.

Deleting a quorum group

You can delete a quorum group from Data Management.

Before you begin

Note: A quorum group can be deleted only by a quorum member in the group. The operation requires quorum approval.

A quorum group cannot be deleted if there are pending requests for the operations controlled by the quorum group.

Procedure

To delete a quorum group, complete the following steps:

1. In the Data Management dashboard, navigate to **Security** > **Quorum** and select the **Groups** tab.
2. Find the quorum group you need in the **Groups** tab and click the **Delete** icon on that row to delete the quorum group.

Disabling a quorum group

You can disable a quorum group from Data Management.

Before you begin

Note: A quorum group can be disabled only by a quorum member in the group. The operation requires quorum approval.

If you have pending requests for the operations that are controlled by the quorum group, you cannot disable a quorum group.

Procedure

To disable a quorum group, complete the following steps:

1. In the Data Management dashboard, navigate to **Security** > **Quorum** and select the **Groups** tab.
2. Find the quorum group that you need in the **Groups** tab and click the **Disable** icon on that row to disable the quorum group.

Approving or decline a quorum request

In Data Management, when a user initiates a quorum-protected operation, an email notification is sent to all the approvers in the respective quorum group. The operation requires approvals from the quorum approvers to run.

About this task

Quorum approvers can approve or decline the quorum requests from the "Pending requests" on page 80 tab in the Quorum Dashboard. After the quorum request is approved per the conditions that are defined in the quorum group configuration, the operations run immediately.

Procedure

To approve or deny a quorum request, complete the following steps:

1. In the Data Management Dashboard, navigate to **Security**> **Quorum** and select the **Pending Requests** tab.
2. Click the quorum request to open the request details page.
3. Review the quorum request details on the page and click **Approve** or **Decline**.

Security advisor

The **Security Advisor** enables the option for you to view the security posture of your organization and provides actionable insights so that you can modify the security settings based on your needs. To view the Security Dashboard, navigate to **Security** > **Security Advisor**.

The **Security Advisor** page consists of the following tabs:

- Scores
- Security Rules
- Scan Results

The scores, icons, and other information that is provided by the **Security Advisor** indicate how your organization's security deployment and configuration compares with the minimum preferred practices. These practices are designed to supplement (but are not a substitute for) a robust and comprehensive information security program that is managed by your organization's designated experts.

Scores

The **Scores** tab provides a global view of the security posture across all clusters. You can perform the following tasks:

- Initiate a scan
- View all issues
- Filter by score, cluster, or region

Performing a scan

You can perform a scan to see global view of the security posture across all clusters.

Procedure

To perform a scan, complete the following steps:

1. In the Data Management Dashboard, navigate to **Security** > **Security Advisor**. By default, the Scores tab is displayed.
2. Click **PerformScan**.
3. In the **PerformScan** window, click the checkbox to select clusters. You can select a single cluster or multiple clusters.
4. Click **PerformScan**.

Scores table

The following details are displayed in the **Scores** table:

- **Security Score**—Displays the score and the icon. The score is categorized as follows:
  - Less than 70—High risk
  - 70 to 90—Moderate risk
  - Greater than 90—Low risk
  - **Region**—Region of the clusters. For example, Europe.
- **Clusters**—Clusters that are included as part of the scan.
- **Rule**—Name of the security rule.
- **Last Scan**—Date and time at which the last scan was performed.

Security rules

The **Security Rules** dashboard provides an overall summary of the rules and clusters. By default, a security rule is configured, but you can edit the rule and update the definition.

Editing the default rule

You can edit the default rule and update the definition of the rule.

Procedure

To edit the default rule, complete the following steps:

1. In the **Security Rules** dashboard, hover over the rule and click ⋮ .
2. Click **Edit**.
3. On the **Edit Rule** page, you can complete the following actions:
   - Update the name of the rule
   - Update the definition
4. Click **Save**.

Security rules dashboard

The following details are displayed in the **Security Rules** dashboard:

- Number of rules that are configured
- Total number of protected clusters
- Total number of out of rule clusters
- Total number of out of rule clusters
  - Name of the rule
  - Strength of the definition
  - Total number of protected clusters
  - Total number of out of rule clusters

Viewing definition and cluster strength

You can view the definition and cluster strength from the Data Management Dashboard.

Procedure

To view the definition and cluster strength, complete the following steps:

1. In the Data Management Dashboard, navigate to **Security** > **Security Advisor** .
2. Click the **Security Rules** tab.
3. Click on a security rule.
4. By default, the tab appears and the following details are displayed:
   - Security percentage of the definition
   - Strength of the definition
   - **Access Control** criteria:
     - Check whether the external syslog server is configured
     - Check if NTP authentication is configured
     - Support channel status
     - Check whether sudo access for the support user is disabled
   - **Configuration** criteria:
     a. Check if External KMS is configured
     b. Check whether the login banner is enabled
     c. Check whether the audit log retention period is greater than 180 days
     d. Check if SNMPv3 is configured
     e. Check whether filer logs are enabled and the retention period is greater than 180 days
     f. Check whether Two-factor authentication is enabled
   - **Smart Files** criteria:
     a. Check whether Global Allowlist is disabled
     b. Check whether SMB authentication is enabled
5. Click the **Clusters** tab to view the following details:
   - Percentage of out of rule clusters
   - Total number of out of rule clusters
   - Total number of protected clusters
   - Cluster name and the corresponding strength

Viewing scan results

The **Scan Results** page provides a list of scan results and enables option for you to drill down further to view the issues. You can narrow down the results by using the **Date Range** filter.

Procedure

To view the scan results, complete the following steps:

1. In the Data Management Dashboard, navigate to **Security** > **Security Advisor** > **Scan Results**.
2. Use the **Date Range** filter, select one of the following options, and click **Apply**:
   - Today
   - Yesterday
   - Last 7 Days

- Last 30 Days
- Custom—Select the dates from the date picker

The scan results are displayed and you can view the following details:

- Name of the scan
- Security score
- Total number of clusters
- Total issues
- Date and time at which the last scan was performed

3. Click on a scan result to view the issues corresponding to the scan.

Global map view

The **Security Advisor** feature provides a Global Map view, which is a pictorial representation of the clusters and the security score. You can click on a region and navigate to the **Scores** tab on the **Security Advisor** page.

Procedure

To view the Global Map dashboard, complete the following steps:

1. In the Data Management dashboard, navigate to **Dashboards**.
2. Select **Security** from the drop-down list.
3. Click the **Security Advisor** tab.

Audit logs

An audit log describes audit information for events that are generated on the clusters that are managed on Data Management. They can be system events such as errors or an audit trail of:

- Read or write actions that are performed by the users on the clusters.
- Login and logout actions that are performed by the users on Data Management.

You can view these audit logs and also download them for further analysis purposes.

Configuring the audit log settings

By default, audit logs are enabled on Data Management. You can configure the following setting based on your requirement:

- Log retention period.
- Capture read logs of specific user roles on the Data Protect clusters.

Setting log retention period for audit logs

You can set the retention period for audit logs. When you set a retention period, the logs are retained on Data Management until the retention period ends.

Before you begin

Note: The default retention period is 300 days.

Procedure

To set a retention period for audit logs, complete the following steps:

1. Navigate to **System> Audit Logs> Settings**.

2. In the **Settings** tab, click the pencil icon for the **Log Retention Period** option, type the wanted number, and select retention period (Days, Weeks, Months, or Years). The Log Retention Period is displayed in days as Data Management converts weeks, months, or years into days.
3. Click **Save**.

Specifying user roles for read logs

You can configure Data Management to capture read logs of specific user roles on the Data Protect clusters.

Procedure

To specify user roles for read logs, complete the following steps:

1. Navigate to **System** > **Audit Logs** > **Settings**.
2. In the **Settings** tab, click the pencil icon for the **Logs for Read Actions** option.
3. For the drop-down list, select the **Role**. Click the plus **(+)** icon to add multiple roles.
4. Click **Save**.

Viewing audit logs

On the Data Management dashboard, you can view the audit logs for the **System > Audit Logs** page. The **Audit Logs** page lists the following information that is logged by the Data Protect clusters or Data Management:

- Time
- User
- Action

Note: By default, only the write actions that are performed by the users on the clusters are displayed on the **Audit Logs** page. To view the read actions, use the available filter. For more information, see "Filters" on page 95.

Filters

You can use the following available filters to narrow down the audit logs based on your requirement:

Filter	Purpose
Date Range	Filter the audit logs based on the selected time window.
System	Filter the audit logs based on the cluster or Data Management.
Users	View the audit trails of a specific user.
Category	Filter the audit logs based on the predefined categories.
Action	Filter the audit logs based on the read or write actions that are performed by the users on the Data Protect clusters managed in Data Management.

Chapter 9. Data Platform for cloud

The following topics help you deploy Cloud Edition clusters by using IBM Storage Defender Data Management Service:

- Deploy Cloud Edition AWS by using Data Management
- Deploy Cloud Edition Azure by using Data Management
- Deploy Cloud Edition GCP by using Data Management

Deploy cloud edition AWS by using IBM Storage Defender Data Management Service

Cloud Edition for AWS is a cluster that is deployed in AWS. Use IBM Storage Defender Data Management Service to deploy a Cloud Edition AWS cluster in approximately 20 minutes, provided you have completed the prerequisites that are listed below. You can setup some AWS infrastructure, then in Data Management you can create a deployment job that provisions the cluster in AWS.

Prerequisites

Before you deploy the Cloud Edition cluster, you must meet the following requirements:

- You must have an AWS IAM user account that is attached to an IAM policy. The IAM policy grants permissions to create the cluster (the permissions are provided later in this document and while creating the deployment job). For more information, see Create a Policy and Create an IAM User.
- You must have the access key (the access key ID and secret access key combination) for the AWS user account. The access key is used only during deployment; it is not saved in Data Management.
- You must have an AWS VPC (Virtual Public Cloud) and a subnet.

  Select a VPC and subnet when you create the deployment job. The subnet must be able to reach the AWS Systems Manager because cluster deployment creates EC2 instances and then uses the SSM Agent to create the cluster. For more information, see Interface VPC Endpoint or Internet Access in the AWS documentation.
- During the deployment process, you have an opportunity to select an existing AWS EC2-VPC security group or create a new one. If you create a new one, it will automatically contain rules that open the ports that are required for cross-node communication within the cluster. If you use an existing security group, ensure that the correct ports are open.
- The AWS `m5.4xlarge` instance type is used for node instances in the cluster. Ensure that the limit for the instance type is large enough to create a cluster. The default limit is 0.

Verifying limits for node instances

You can increase the following AWS limits before deploying the Cloud Edition cluster. The limits are per region. Verify the limits in the region where the cluster is set to deploy.

Before you begin

Running On-Demand EC2 instances: This limit is for all types of EC2 instances in the region. The limit must be large enough to accommodate the node instances and any other instances in the region.

Procedure

To verify and increase the limits, complete the following steps:

1. Log in to the **Amazon AWS** console and select **EC2**. The EC2 Dashboard appears.

© Copyright IBM Corp. 2023, 2024

2. In the left frame of the EC2 dashboard, select **Limits**.
3. Scroll down and find the limits. If the current limit for either of the above is too low, click **Request limit increase**.
4. Complete the form and click **Submit**.

Creating a policy

You can create a policy for the deployed Cloud Edition AWS in Data Management.

Procedure

1. Log in to the Amazon AWS console by using your AWS account credentials. The AWS credentials that you specify must have admin privileges.
2. From the menu bar, select **Services**.
3. Under **Security, Identity & Compliance**, select **IAM**.
4. Click **Policies**.
5. Click **Create policy**.
6. From the **Create policy** page, select the **JSON** tab.
7. Delete the default JSON code.
8. Copy the following JSON code:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action":[
                "iam:ListAttachedUserPolicies",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListGroupsForUser",
                "iam:ListUsers",
                "iam:GetUser",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:CreateRole",
                "iam:AttachRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:DetachRolePolicy",
                "iam:ListPolicies",
                "iam:GetRole",
                "iam:DeleteRole",
                "iam:CreateInstanceProfile",
                "iam:PassRole",
                "iam:DeleteInstanceProfile",
                "iam:GetInstanceProfile",
                "iam:TagRole",
                "cloudformation:UpdateStack",
                "cloudformation:ListStackResources",
                "cloudformation:CreateStack",
                "cloudformation:GetTemplate",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:ValidateTemplate",
                "cloudformation:DescribeStackEvents",
                "ec2:DescribeInstances",
                "ec2:DeleteTags",
                "ec2:DescribeRegions",
                "ec2:DeleteVolume",
                "ec2:DescribeNetworkInterfaces",
                "ec2:StartInstances",
                "ec2:DescribeVolumes",
                "ec2:AttachVolume",
                "ec2:DescribeInstanceStatus",
                "ec2:DetachVolume",
                "ec2:DetachNetworkInterface",
                "ec2:TerminateInstances",
                "ec2:ModifyVolumeAttribute",
                "ec2:CreateTags",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DeleteNetworkInterface",
                "ec2:RunInstances",
                "ec2:StopInstances",
                "ec2:CreateVolume",
                "ec2:CreateNetworkInterface",
                "ec2:AttachNetworkInterface",
                "ec2:DescribeSubnets",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:DescribeAvailabilityZones",
                "ec2:CreateSecurityGroup",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcs",
                "ec2:DeleteSecurityGroup",
                "ssm:SendCOmmand",
                "ssm:GetCommandInvocation",
                "s3:CreateBucket",
                "s3:GetObject",
                "s3:PutObject",
                "s3:DeleteObject",
                "s3:DeleteBucket",
                "s3:PutBucketPubicAccessBlock"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "VisualEditor0"

        }
    ]
}
```

9. Paste the JSON code from the previous step.
10. Click **Review policy**.
11. In the Name field, enter a name for this policy, such as `storagedefenderCEPolicy` and click **Create policy**.
12. Enter a name, such as `storagedefenderCEPolicy`, and an optional description for the policy and click **Create policy**.

Creating an IAM user

You can create an IAM user for the deployed Cloud Edition AWS in Data Management.

Procedure

1. Log in to the **Amazon AWS console** by using your AWS account with admin privileges.
2. In the upper left of the menu bar, select **Services**.
3. Under **Security, Identity & Compliance**, select **IAM**.
4. In the left frame, click **Users**.
5. Click **Add users**.
6. In the User name field, enter a user name such as IBMCE.
7. For **Access type**, select **Programmatic access** and click **Next:Permissions**.
8. Click **Attach existing policies directly**, then search for the name of the policy you created previously and select that policy.

   Note: Attaching the AWS permissions are required for a fresh deployment of the Cloud Edition or for a node that is being added to an existing cluster. When the Cloud Edition is deployed, the IAM permissions are not required and can be removed.
9. Click **Next:Tags**.
10. Optionally, enter tags for the policy and then click **Next:Review**.
11. In the **Secret access key** column, click **Show**.
12. Copy and paste the **Access key ID** and the **Secret access key** in to a text file to use later when you are deploying the cluster.
13. Click **Close**.

Configuring VPC, VPN access, and security

Configure networking and security in AWS before deploying the Cloud Edition AWS cluster. Use the VPC wizard in the Amazon VPC console to create the VPC (Virtual Public Cloud) and the VPN connection as described in the following sections.

Before you begin

Note: Configuring a VPN is needed only if you want to setup replication between an on-premises cluster and a Cloud Edition cluster.

Before you configure, complete one of the following actions:

- If an internal NTP server is not available, create a VPC with private and public subnets. See Public and Private Subnets and AWS Managed VPN Access.
- If an internal NTP server is available, create a VPC with a private subnet. See Private Only Subnet and AWS Managed VPN Access.

Public and Private Subnets and AWS Managed VPN Access

If an internal NTP server is not available, create a VPC with private and public subnets. For detailed instructions, see Scenario 3: VPC with Public and Private Subnets and AWS Managed VPN Access in the AWS documentation.

Use the following guidelines when you create the VPC and subnets.

Procedure

1. Determine the IPv4 CIDR block to use for the VPC. Cloud Edition for AWS supports only IPv4 addressing. Amazon recommends specifying a CIDR block from the private (non-publicly routable) IP address ranges as specified in `RFC 1918`.
2. Use the VPC wizard to create a private subnet in your VPC. Provide the IP address for the VMs that house the IBM nodes in this subnet.
3. Use the VPC wizard to create a public subnet in your VPC. If you do not specify a public subnet, you must have an internal NTP server in your corporate network (data center).
   a. While creating a customer gateway, **choose the static routing option** and specify a static internet routable address for your organization.
   b. While creating a VPN connection between the virtual private gateway and the customer gateway, **choose the static routing option.**
4. Use the VPC wizard to create a VPN connection between the VPC and your corporate network (datacenter).
5. Use the VPC wizard to create an internet gateway (`igw-<id>`) and update the public route table. For more information, see Routing in the AWS documentation.
6. Create a NAT gateway and deploy it in this public subnet. A NAT gateway allows instances in the subnet to access the internet but any instance in the internet cannot access any instance in the subnet.
7. Use the VPC wizard to create a virtual private gateway (`vgw-<id>`) and update the private route table. For more information, see Routing in the AWS documentation.
8. If you do not already have one, create an AWS security group for EC2-VPC. Open all ports on the security group because services on a cluster node must communicate with other cluster nodes. For more information, see Security Groups for EC2-VPC in the AWS documentation.
9. If you do not already have a security key pair, create one.
   a. Log in to the Amazon AWS console and select **EC2**. The **EC2 Dashboard** displays.
   b. In the left frame, under NETWORK & SECURITY, select **Key Pairs**.
   c. Click **Create Key Pair**. For more information, see Amazon EC2 Key Pairs in the AWS documentation.

Private Only Subnet and AWS Managed VPN Access

Use the following guidelines when you create the VPC and subnets.

a. Determine the IPv4 CIDR block to use for the VPC. Cloud Edition for AWS only supports IPv4 addressing. Amazon recommends specifying a CIDR block from the private (non-publicly routable) IP address ranges as specified in **RFC 1918**.
b. Use the VPC wizard to create a private subnet in your VPC. Provide the IP address for the VMs that house the Data Management nodes in this subnet.
c. Update the private route table. For more information, see Routing in the AWS documentation.
d. Use the VPC wizard to create a virtual private gateway (`vgw-<id>`) and update the private route table.

For more information, see Routing in the AWS documentation.

Deploying the cloud edition cluster

If you already set up the prerequisite AWS user account, access key, policy and security group, it takes approximately 15 to 20 minutes to deploy a Cloud Edition cluster.

Procedure

1. In Data Management, select **Settings > Data Platform for Cloud**.

   Note: Ensure that you are in the main Data Management and the dashboard displays a summary of **All Clusters**.
2. Click **Deploy** and select **AWS**.

   A **Deployment Checklist** window appears. Read through the details and click **Close**.
3. Provide the following information:
   - **Deployment Job Name:** Enter a name for this deployment job.
   - **Access Key ID:** Enter the access key ID for the AWS IAM user account that is used for deploying the cluster.
   - **Secret Access Key:** Enter the secret access key for AWS IAM user account.
   - **Region:** Select the AWS Region that you want the Cloud Edition cluster to run in.
4. The **Cloud Network Details** page provides drop-down lists of VPC, zone, security group, and subnet based on the AWS credentials you provided in the previous step.

   Select the components that you want to use for the Cloud Edition cluster.

   You can select an existing security group or create a new one. If you create a new one, it automatically contains rules that open the ports that are needed for cross-node communication within the cluster. If you use an existing security group, ensure that the correct ports are open.

   To create a security group, select **New Security Group** from the drop-down and click **Continue**.
5. Provide the following information:
   - **Cluster Name:** The name of the cluster. Specify a name up to 63 alphanumeric characters such as IBM1MyCompany. Hyphens are allowed but cannot be the first or last character. This name is the name of the cluster as displayed in the IBM UI and the IBM CLI.
   - **Node Size:** Select the size for each node.

     If you select **XLarge**, Cloud Tier is used to move cold data from the cluster to an existing S3 bucket. Provide the bucket name, region, access key ID, and secret access ID for the bucket. Data Management registers the bucket as an external target on the cluster and enable Cloud Tier for the DefaultStorageDomain.
   - **Number of Nodes:** Specify how many nodes to add to the cluster. For a production cluster, at least 3 nodes are needed. However, for test or demonstration purposes, you can select 1 or 2 nodes. The cluster does not allow node failures.

- **DNS Servers:** The IP addresses of the Domain Name System (DNS) servers that the Data Management cluster must use. Separate multiple IPs with commas. Ensure that the Active Directory DNS IP address (if applicable) is listed first. Verify that the specified DNS server can resolve the NTP servers and other entities in the system.
- **NTP Servers:** Specify NTP servers. IBM suggests to use the external Google Public Network Time Protocol (NTP) server and specify multiple servers (`time1.google.com, time2.google.com, time3.google.com, time4.google.com`). Avoid by using the `pool.ntp.org` or `time.nist.org` NTP servers, as sometimes they are not available and their IP addresses tend to change. If using an internal NTP server, use only one server (and no external servers). Specify the IP address or the Fully Qualified Domain Name of the NTP server(s). The cluster uses the specified NTP server to synchronize the time on all nodes in the cluster. Also, toggle **Use Authentication**

Key to secure the communication between the NTP server and the cluster. In the **Key ID** field, enter the Key ID that is associated with the SHA-1 key and in the **Key** field, enter the SHA-1 key. Only SHA-1 Keys are supported.

- **Domain Names:** The domain names for the cluster.
- **Cluster Encryption:** The cluster supports AES256 software encryption. If wanted, enable encryption to encrypt all the data that is to be stored on the cluster. After a cluster has been created, cluster-level encryption is not editable, however, you can enable encryption at the Storage Domain level.

6. Click **Deploy**.

   The process of deploying the cluster into the AWS account begins. A message indicates deployment initiation and the cluster name is displayed in the list of Cloud Editions.

   Tip: You can cancel the deployment at any time by clicking the **X** next to the cluster name.
7. Monitor the deployment progress. Click the expand icon next to deployment name for a scrollable list of tasks.

   Tip: You can also monitor the deployment progress in the AWS Console. Go to **Services > CloudFormation > Stacks** and click on the deployment name in the stack list. For example, the stack name for the deployment in this example might look like demo cluster-2EUUWD94Y0FKBD.
8. Wait a few minutes and then scroll the task list to step **5. Execute Commands** and copy the node IP address. You need the address to set up the cluster.

Changing the default admin password

After the Cloud Edition cluster is successfully deployed, log in to the cluster and change the default `admin` password.

Procedure

1. Open a browser window and paste the node IP address that you copied previously into the address bar and press enter.
2. When the cluster login page appears, log in using the default System Admin account called `admin` and the default password, `administrator`.
3. Accept the license agreement. Then you are asked to validate the license either by connecting to Data Management or deploying On Prem and providing the license key.
4. When prompted, accept the EULA and apply the license key that is provided by IBM.
5. In the **Change Password** dialog box, enter and confirm the new password for the System Admin account. The minimum length of the password must be 8 characters.

   You can now start to use the cluster.

   For page-specific help in the cluster, click the help icon in the menu.

Connecting the cloud edition cluster

Connect the cluster to IBM Storage Defender Data Management Service, which allows the cloud edition cluster to be managed from Data Management. For instructions, see "Connecting a cluster to Data Management" on page 19.

Deleting a cloud edition AWS cluster

You can permanently delete the Cloud Edition cluster from AWS. The access key ID and secret access key are required to delete the cluster.

Before you begin

Important: All data on the cluster will be deleted. The delete operation is irreversible.

Procedure

1. In the Data Management, select **Settings > Data Platform for Cloud**.
2. Find the Cloud Edition that you want to delete and click the delete icon.
3. Respond to the confirmation prompt.
4. Provide the access key information.
5. Click **Delete**.

Deploying cloud edition Azure by using IBM Storage Defender Data Management Service

Cloud Edition Azure is a cluster that is deployed in Azure. Use IBM Storage Defender Data Management Service to deploy a Cloud Edition Azure cluster in less time, provided you have the completed the prerequisites. Using Azure infrastructure, you can create a deployment job in Data Management that provisions and creates the cluster in Azure.

Creating a service principal

Before you can create a Cloud Edition cluster, you must create a service principal in Microsoft Azure by using your Azure account.

Before you begin

This procedure must be done only once for a single Azure account. For more information and detailed instructions, see Creating a Service Principal in the Azure documentation. Ensure that your Azure account has adequate Active Directory permissions to register an application.

Procedure

1. Log in to the Microsoft Azure Portal.
2. Select **Azure Active Directory > App registrations**.
3. Click **New registration**.
4. Provide a name for the application. Select a supported account type, which determines who can use the application. Under **Redirect URI**, select Web for the type of application you want to create. Enter the URI where the access token is sent to and then click **Register**.

   The Azure AD application and service principal are created.

Creating a custom role for the application

The built-in roles (except the Owner role) for Azure resources do not meet the requirements for deploying a Cloud Edition cluster. Therefore, you must create custom roles to meet the requirements.

Procedure

To create custom roles to meet the requirements, complete the following steps:

1. Download and install `Azure CLI` on your machine.
2. Copy the following JSON code to a JSON file and replace the following values: name, description, and subscription ID with relevant name, description, and Azure subscription ID in which the cluster is to be deployed.

   ```
   { "Name": "<Name of Role>", "Description": "<Description for role>", "IsCustom": true,
   Deploy Cloud Edition Azure Using Helios Create a Service Principal
   Project Aqua User Guide 353
   "Actions": [ "Microsoft.Authorization/locks/write", "Microsoft.Compute/disks/
   write", "Microsoft.Compute/locations/runCommands/read", "Microsoft.Compute/virtualMachines/
   deallocate/action", "Microsoft.Compute/virtualMachines/read", "Microsoft.Compute/
   virtualMachines/runCommand/action", "Microsoft.Compute/virtualMachines/start/action",
   "Microsoft.Compute/virtualMachines/write", "Microsoft.Network/networkInterfaces/join/
   action", "Microsoft.Network/networkInterfaces/read", "Microsoft.Network/networkInterfaces/
   write", "Microsoft.Network/networkSecurityGroups/join/action", "Microsoft.Network/
   networkSecurityGroups/read", "Microsoft.Network/networkSecurityGroups/write",
   "Microsoft.Network/virtualNetworks/read", "Microsoft.Network/virtualNetworks/subnets/join/
   action", "Microsoft.Resources/deployments/read", "Microsoft.Resources/deployments/
   validate/action", "Microsoft.Resources/deployments/write", "Microsoft.Resources/
   subscriptions/resourcegroups/delete", "Microsoft.Resources/subscriptions/resourcegroups/
   read", "Microsoft.Resources/subscriptions/resourcegroups/write", "Microsoft.Storage/
   storageAccounts/blobServices/containers/write", "Microsoft.Storage/storageAccounts/delete",
   "Microsoft.Storage/storageAccounts/listKeys/action", "Microsoft.Storage/storageAccounts/
   read", "Microsoft.Storage/storageAccounts/write" ], "DataActions": [], "NotDataActions": [],
   "AssignableScopes": [ "/subscriptions/<subscriptionID>" ] }
   ```

3. Run the following command:

   ```
   az role definition create --role-definition @<name_of_json_file>.json
   ```

   Assign the application to a role:

   To access resources in your subscription, you must assign the application to the custom role you created.

   a. Log in to Microsoft Azure Portal.

   b. Navigate to the subscription that is to be used to create the cluster.

   c. Select **Access control (IAM) > Add role assignment**.

      Note: The permissions are required for a fresh deployment of the Cloud Edition or for adding a new node to an existing cluster. When the Cloud Edition is deployed, the permissions are not required. The role can be disassociated from the application when the Cloud Edition is deployed.

   d. Select the custom role that you created for the application, and then click **Save**.

Deploying cloud edition Azure

If you already set up the prerequisite for Azure, it takes about 30 to 45 minutes to deploy a Cloud Edition cluster.

Procedure

1. In the Data Management, select **Settings > Data Platform for Cloud**.
2. Click **Deploy** and select **Azure**.
3. In the **Deploy IBM Azure** page, provide a deployment name of your choice in the **Cloud Edition Name** field.
4. Provide the following information:

- **Subscription ID:** Specify the subscription ID for the subscription used to store the resources of the cluster. Log in to the Azure portal. From the side panel, click **Subscriptions**. Copy the SUBSCRIPTION ID from the table. You obtain this value during the process of creating a service principal.
- **Application ID:** Specify the application ID assigned by Azure during the process of creating a service principal. For instructions, see Get application ID and authentication key in the Microsoft Azure documentation. You obtain this value during the process of creating a service principal.
- **Application Key:** Specify the application key generated by Azure during the service principal creation process that is used for authentication. For instructions, see Get application ID and authentication key in the Microsoft Azure documentation. You obtain this value during the process of creating a service principal.
- **Tenant ID:** Specify the unique Tenant ID assigned by Azure. For instructions, see Get tenant ID in the Microsoft Azure documentation. You obtain this value during the process of creating a service principal.

5. Click **Verify** and then provide the following cloud environment details:
   - **Region:** Select an Azure region from the drop-down list.
   - **Compute Resource Group:** Select a compute resource group available in the drop-down list or create a new compute resource group in Azure.
   - **Storage Resource Group:** Select a storage resource group available in the drop-down list or create a new storage resource group in Azure.
   - **Virtual Network:** From the drop-down list, select a virtual network available in the selected region.
   - **Subnet:** Select the subnet range within your selected virtual network.
   - **Security Group:** Select a security group available in the drop-down list or create a new security group in Azure to filter traffic to and from resources.
   - **Tags:** Provide a tag value for this deployment.
6. Click **Continue** and provide the following cloud details:
   - **Cluster Name**: Specify a name for the cluster. Only alphanumeric characters and hyphens are allowed. A hyphen cannot be the first or last character. Length cannot exceed 32 characters. No other characters are allowed.
   - **Node Size**: Select the size for each node in the cluster:
     - **Small**: 2 TB HDD and 1.6 TB SSD per node.
     - **Medium**: 6 TB HDD and 1.6 TB SSD per node.
     - **Large**: 12 TB HDD and 1.6 TB SSD per node.
     - **XLarge**: 12 TB HDD, 2 TB SSD and up to 36 TB of Azure Hot Blob storage per node. The XLarge nodes are supported on cluster version 6.5.1 and later.

       Create a storage account and a storage container in the same Azure region as IBM for Cloud. The storage account must be exclusive for IBM use.

       Note: To avoid egress charges while you transfer data between IBM and Azure storage, IBM recommends you to use Private Endpoints for Azure Storage. For more information, see Private Endpoints in the Microsoft Azure documentation.
   - **Number of Nodes**: Specify how many nodes to add to the cluster. For a production cluster, at least 3 nodes are required. However, for test or demonstration purposes, you can select 1 or 2 nodes. The cluster does not allow node failures.

     If you select **XLarge**, the following properties must be configured for the storage account that will be used for cold data moved from the cluster. Data Management registers the account as an external target on the cluster and enable Cloud Tier for the Default Storage Domain.

     - Storage Container Name: The storage container name.
     - Storage Account Name: The storage account name.

  - Storage Access Key: - The access key for the Azure storage account.
- **Fault Tolerance**: Enable this option to tolerate the failure of a single node. This option is available only if the cluster has three or more nodes.
- **DNS Servers**: Specify the IP addresses of the Domain Name System (DNS) servers that the cluster should use. Separate multiple IPs with commas. Ensure the Active Directory DNS IP address (if applicable) is listed first. Verify that the NTP servers and other entities in the system can be resolved by the specified DNS server.
- **NTP Servers**: Specify NTP servers. IBM suggests that use the external Google Public Network Time Protocol (NTP) server and specify multiple servers (`time1.google.com, time2.google.com, time3.google.com, time4.google.com`). If using an internal NTP server, use only one server (and no external servers). Specify the IP address or the Fully Qualified Domain Name of the NTP servers. The cluster uses the specified NTP server to synchronize the time on all nodes in the cluster.
- **Domain Names**: Specify the fully qualified domain name for the cluster.
- **Cluster Encryption**: The cluster supports AES256 software encryption. If wanted, enable encryption to encrypt all the data that is to be stored on the cluster. After a cluster has been created, cluster-level encryption is not editable, however, you can enable encryption at the Storage Domain level. You can also enable encryption while creating a Storage Domain. After a Storage Domain has been created, Storage Domain-level encryption is not editable.

7. Click **Deploy**.
8. (Optional) Also, in the email notification window, you can enter more email IDs to receive notification of successful deployment. By default a confirmation email is sent to your SFDC email ID.

   The process of deploying the cluster into the Azure account begins. A message indicates deployment initiation and the cluster name is displayed in the list of Cloud Edition.

   ⚠ **Warning:** For Azure Cloud Edition Cluster, ensure that the Host caching option for all cluster node disks is set to None to avoid potential data loss.

   Tip: You can cancel the deployment at any time by clicking the **X** next to the cluster name.

Changing the default admin password

After the Cloud Edition cluster is successfully deployed, log in to the cluster and change the default `admin` password.

Procedure

1. Open a browser and enter one of the node IPs.
2. When the cluster login page appears, log in using the default System Admin account called `admin` and the default password, `administrator`.
3. Accept the license agreement. Then you are asked to validate the license either by connecting to Data Management or deploying On Prem and providing the license key. IBM Support portal credentials are required.
4. When prompted, accept the EULA and apply the license key that is provided by IBM.
5. In the **Change Password** dialog box, enter and confirm the new password for the System Admin account. The minimum length of the password must be 8 characters.

   You can now start to use the cluster.

   Tip: For page-specific help in the cluster, click the help icon from the navigation menu.

Connecting the cloud edition cluster

Optionally, you can connect the cluster to IBM Storage Defender Data Management Service and then manage it from there.

Login to the Cloud Edition cluster and click the H icon in the menu bar, and then click **Enable**.

Deleting a cloud edition Azure cluster

You can permanently delete the Cloud Edition cluster from Azure. The access key ID and secret access key are required to delete the cluster.

Before you begin

Important: All data on the cluster will be deleted. The delete operation is irreversible.

Procedure

1. In Data Management, select **Settings > Data Platform for Cloud**.
2. Find the Cloud Edition that you want to delete and click the delete icon.
3. Respond to the confirmation prompt.
4. Provide the access key information.
5. Click **Delete**.

Deploying cloud edition GCP by using IBM Storage Defender Data Management Service

Cloud Edition GCP is a cluster that is deployed in Google Cloud Platform. Use IBM Storage Defender Data Management Service to deploy a Cloud Edition GCP cluster in less time, provided that you have completed the prerequisites. You can create a deployment job in Data Management that creates the cluster in your GCP environment.

Prerequisites

- Make sure that you have access to a GCP account with billing configured and a GCP project for deploying the IBM VM instances. For more information, see Creating and Managing GCP Projects in the GCP documentation.
- Enable the following APIs in the GCP Project in which Cloud Edition is to be deployed:
  - Compute Engine API
  - Cloud Resource Manager API
  - Serverless VPC Access API
  - Cloud Functions API
  - Cloud Build API

  For more information, see Enabling an API in your GCP project in the GCP documentation.

Verifying resource quotas

Verify that your GCP project has the resource quotas that are required to support the node VMs that make up the Data Management cluster. The required resource quota depends on the number of nodes that you plan on adding to your cluster.

Cloud Edition GCP supports one or more nodes. The node capacity can be small, medium, or large. The only difference is the HDD capacity:

Resource Per Node	Resource Type	Small	Medium	Large	Next-Gen
Storage - HDD for Data	pd-standard	2 TB	6 TB	12 TB	2 TB
Machine	n1-standard-16	16virtual CPUs			32vCPU

Resource Per Node	Resource Type	Small	Medium	Large	Next-Gen
Storage - Boot Disk	pd-standard	62 GB			120 GB
Storage - SSD for Metadata	pd-ssd	1.638 TB			

In the **Google Cloud Platform console** under **IAM & admin > Quotas**, verify that the resource quotas of the resources are large enough to accommodate the size of the planned cluster in your region.

Configuring a VPC network

Configure networking and security in GCP before you deploy the cluster Cloud Edition in GCP. Create a new or use an existing Virtual Private Cloud (VPC) network. You can create a new subnet in the region you want to deploy Cloud Edition or use an existing subnet. For more information, see Virtual Private Cloud (VPC) Network Overview in the GCP documentation.

You can also deploy a Cloud Edition in a Shared VPC. For more information, see Shared VPC overview in the GCP documentation.

Configuring firewall rules in the VPC network

The Cloud Edition cluster requires the rules to allow network traffic for cluster operations.

Before you begin

Verify that firewall rules exist (or create new ones) for your VPC network that allow network traffic over the protocols and ports that are specified in "Ingress firewall ports" on page 108 and "Egress firewall rules" on page 109.

If you use an existing security group, ensure that the correct ports are open.

Before creating firewall rules, read Firewall Rules Overview in the GCP documentation.

Procedure

To verify or create a Firewall Rule, complete the following steps:

1. Log in to **Google Cloud Platform console** with an account that has been granted the IAM roles that are required to create IBM nodes (instances).
2. From the menu bar drop-down, select your project where the IBM VMs will be created.
3. From the Menu icon, select **NETWORKING > VPC network > Firewalls rules**.
4. If a firewall rule (listed in "Ingress firewall ports" on page 108 and "Egress firewall rules" on page 109) does not already exist, create a new firewall rule by clicking **CREATE FIREWALL RULE**.
5. Create firewall rules by using the following information and the information in "Ingress firewall ports" on page 108 and "Egress firewall rules" on page 109.
   - **Action on match:** `allow`.
   - **Priority:** Your choice.
   - **Target:** Apply to all targets and target tags, or optionally filter by network tags or service account.
6. Click **Create**.
7. Repeat for the rows in the tables ("Ingress firewall ports" on page 108 and "Egress firewall rules" on page 109).

Ingress firewall ports

Select the **Ingress** tab.

Name	Subnets	Protocol and Port
http	Typically open to all subnets. Optional. Typically filtered by subnets that need access to the Control VM or the cluster.	`tcp:80`
https		`tcp:443`
icmp		`icmp`
inside-cluster		`all` - **Recommendation:** Open all the ports for traffic between the nodes of the Data Protect cluster.
nfs		`tcp:2049`
nfs-portmap		`tcp:111`
rdp		`tcp:3389` Needed for remote desktop.
replication		`tcp:11111, tcp:20000, tcp:22222, tcp:23456,tcp:25999, tcp:50051`. These ports are required for successful communication between clusters.
smb		`tcp:445`
ssh		`tcp:22`

Egress firewall rules

Select the **Egress** tab.

Name	Subnets	Protocol and Port
icmp-egress	Typically open to all subnets. `0.0.0.0/0`	`icmp`
nfs-egress	Optional - Typically filtered by subnets that need access to the Control VM or the Data Protect cluster.	`tcp:2049`
nfs-portmap-egress		`tcp:111`
smb-egress		`tcp:445`

Creating a serverless VPC connector

To create an IBM Cloud® Edition in a VPC network, there needs to be a Serverless VPC connector present in that VPC network. For details and instructions on how to create a Serverless VPC connector, see Serverless VPC Details in the GCP documentation.

- The VPC connector does not have to be in the same location as the region in which the cluster is to be deployed. For example, you can use a VPC connector that is created in `us- central1` to deploy a cluster in `us-west1`.
- The VPC connector must be created in the region that supports cloud functions.
- Ensure that the firewall rules do not block traffic between the IP range of the VPC connector and the subnet in which the cluster is to be deployed.
- The VPC connector can be deleted when the cluster is successfully deployed.

Creating and copying a GCP service account key

You can create and copy a GCP service account key from the Google Cloud Platform console.

Procedure

To create and copy a GCP service account key, complete the following steps:

1. Log in to the Google Cloud Platform console.
2. From the menu bar drop-down, select your project where the IBM Cloud Edition is to be created.
3. From the Menu icon, select **IAM& admin > Service accounts**.

   The Compute Engine default service account is listed.
4. Browse for a Google service account (in the gserviceacount.com domain) and under **Options**, select the more icon, then select **Create key**.
5. Under key type, select **JSON** and click **CREATE**.
6. Record the path where JSON key file is downloaded. You have to upload this file while deploying Cloud Edition GCP in Data Management.

Assigning the custom role to the service account

You can assign the custom role to the service account from the Google Cloud Platform console.

Procedure

1. Log in to Google Cloud Platform console.
2. From the menu bar drop-down, select your project where the IBM VMs are to be created.
3. Select **Your project**, open the **IAM & Admin** page and click **IAM**.
4. Identify the service account to which you want to add the custom role.
   - If the service account is not on the members list, then there will not be any roles that are assigned to it. To add the Service account, click **Add** and enter the email address of the service account.
   - If the service account is already on the members list, it has existing roles. Click the **Edit** icon on that service account to add more roles to it.
5. Search for the role **IBMCECreatorRole**.
6. Click **Add** or **Save** to apply the roles to the service account.

Granting access to the Google cloud functions service agent

After enabling the Serverless VPC Access API and Cloud Functions API, go to the **IAM & admin > IAM** section of the project in which Cloud Edition will be deployed and search for `gcf`.

Enable the **Include Google Provided Role Grants** checkbox to view the `gcf-adminrobot.iam.gserviceaccount` account.

You will see a new service account, for example, `service-15714958XXXX@gcf-admin-robot.iam.gserviceaccount.com`, which has the Cloud Functions Service Agent role assigned.

Grant these additional roles: Viewer and Compute Network User.

Note: When deploying Cloud Edition in a Shared VPC environment, you must grant the role Cloud Functions Service Agent to the service account in both the host project of the network that the cluster is being deployed in and in the service project.

Deploying cloud edition

If you already set up the prerequisites for Cloud Edition GCP, it takes about 30 to 45 minutes to deploy a Cloud Edition cluster.

Procedure

1. In Data Management, select **Settings > Data Platform for Cloud**.
2. Click **Deploy** and select **GCP**.

   The **Deployment Checklist** window appears.
3. Upload the Service Account Key file by either dropping the file in the Service Account JSON key file drop box or by clicking **Choose a file**.
4. Click **Verify**.

   The **Cloud Environment Details** page appears.
5. Provide the information that is specified in the following table, and then click **Continue**.

Cloud environment details	
Field	**Description**
Project ID	From the drop-down list, select the project in which the Cloud Edition needs to be deployed.
Region	From the drop-down list, select the GCP region where the IBM cluster Cloud Edition GCP runs, for example: `us-west1`. For more information about GCP Regions, see Regions and Zones in the GCP documentation.
Zone	From the drop-down list, select the GCP zone where the Data Management cluster Cloud Edition GCP runs, for example: `us-west1-b`. For more information about GCP Zones, see Regions and Zones in the GCP documentation.
VPC	From the drop-down list, select the VPC network that the Cloud Edition instances must use.
Subnet	From the drop-down list, select a subnet in the chosen VPC that the GCP instances(nodes) of the IBM cluster must use.
VPC Connector	From the drop-down list, select the VPC connector to be used to deploy the Cloud Edition.
Network Tag	Provide network tag names in a comma-separated list. These network tags are added to the node instances and allow you to make firewall rules and routes applicable to specific VM instances. Ensure that the network tags: • are limited to 63 characters • have only lowercase letters, numbers, and dashes • start and end with a lowercase letter
Label	Provide key value pairs to be added to the node instances. For more information, see Labeling Resources in the GCP documentation.

6. In the **Cloud Details** page, provide the details that are listed in the following table, and then click **Deploy**:

Cloud details	
Field	**Description**
Cluster Name	Specify the name of the cluster. The cluster name requirements are: • Must start with lowercase letters. • Must be of at least 42 characters long with a combination of lowercase letters, numbers, or hyphens. • Must not end with a hyphen. Example: `storagedefender1mycompany-5896548855-qwerty632105` This is the name of the cluster as displayed in the IBM UI and the IBM CLI.
Cluster Image	From the drop-down list, select the version of the IBM Cloud Edition you want to deploy.
Node Size	Select the size for each node: • Small: Each node has one 1.6 TB SSD and one HDD with 2 TB. • Medium: Each node has one 1.6 TB SSD and three HDDs with 2 TB each. • Large: Each node has one 1.6 TB SSD and six HDDs with 2 TB each.
Number of Nodes	Specify how many nodes to add to the cluster. For a production, at least 3 nodes are required. However, for test or demonstration purposes, you can select 1 or 2 nodes. The cluster will not allow node failures.
Fault Tolerance	Enable this option to tolerate the failure of a single node. This option is available only if the cluster has three or more nodes.
DNS Servers	Specify the IP address of the Domain Name System (DNS) servers that the IBM cluster should use and press Enter. You can specify multiple DNS Servers.

Cloud details *(continued)*	
Field	**Description**
NTP Servers	Specify the NTP server name and press Enter. You can specify multiple NTP Server names. IBM suggests to use the external Google Public Network Time Protocol (NTP) server and specify multiple servers (`time1.google.com, time2.google.com, time3.google.com,time4.google.com`). Avoid to use the `pool.ntp.org` or `time.nist.org` NTP servers, as they are sometimes unavailable and their IP addresses tend to change. If using an internal NTP server, use only one server (and no external servers). Specify the IP address or the Fully Qualified Domain Name of the NTP server(s). The cluster uses the specified NTP server to synchronize the time on all nodes in the cluster.
Domain Names	Specify the fully qualified domain name for the IBM cluster and press Enter. You can specify multiple domain names.
Cluster Encryption	The cluster supports AES256 software encryption. If wanted, enable encryption to encrypt all the data that is to be stored on the cluster. After a cluster is created, cluster-level encryption is not editable, however, you can enable encryption at the Storage Domain level. You can also enable encryption while creating a Storage Domain. After a Storage Domain has been created, Storage Domain-level encryption is not editable.

The process of deploying the cluster into the GCP account begins. A message indicates deployment initiation and the cluster name is displayed in the list of Cloud Edition.

Tip: You can cancel the deployment at any time by clicking the **X** next to the cluster name.

Chapter 10. Alerts

IBM Storage Defender Data Management Service displays all the alerts that are triggered on the clusters managed on Data Management. The cluster creates an alert for various reasons:

- It finds a potential problem or when it exceeds the defined threshold.
- A Protection Group is configured to trigger an alert indicating the success or failure of the job.

Each alert has a severity rating that indicates the seriousness of the problem:

- Critical – Immediate action is required because it detects a severe problem that might be imminent or major functionality is not working, such as a missing VM backup.
- Warning – Action is required, but the affected functionality is still working, such as the restore task failed due to some external target connectivity and/or credentials issues.
- Informational – Immediate action is not required, and the alert provides an informational message.

For a listing of the Alerts created by the clusters, see "Alert references" on page 121.

Viewing the alert on Data Management Service

From Data Management, you view the alerts that are triggered by a cluster, or all the clusters managed on Data Management.

Procedure

1. To view the alerts triggered by a cluster:
   a. Login to the Data Management Service.
   b. Navigate to a cluster from Data Management.
   c. Click **System > Health**, and then select **Alerts**.
2. To view the alerts that are triggered by all the clusters managed on Data Management:
   a. Log in to the Data Management Service. The **All Clusters** context is displayed.
   b. Click **System > Health** and, then select **Alerts**.

Analyzing the Alert

You can click on an alert from the **Alerts** tab and view the alert details on the **Details for <Alert_Name>** page.

The **Details for <Alert_Name>** page includes a timeline view showing the date and time the alert was triggered. The page also provides the following details of the alert:

Details	Description
Alert Code	The alert code. You can click on the alert code for detailed information about the alert.
Severity	The severity rating of the alert.
Type	The alert type. It defines the IBM Storage Defender Data Management Service component that triggered the alert.
Category	The alert category.

© Copyright IBM Corp. 2023, 2024

Details	Description
Status	The status of the alert. It can be Active, Resolved, or Note.
Description	A brief description of the problem that triggered the alert.
Cause	A brief description of the cause of the problem.

Alert Notification

You can configure general alert email notifications or enable webhooks for alert notifications in the **Health > Notification** tab. For more information, see "Configuring alert notification settings" on page 116.

Configuring alert notification settings

You can configure general alert notification rules from the **Health** page in the **Notification** tab. You can configure email and webhook as the notification output for the alert notification.

Creating an alert notification rule for email notifications

You can add different alert notification rules that send emails based on the alert categories, severities, and names.

Procedure

To create an alert notification rule for email notifications, complete the following steps:

1. Navigate to the **System > Health > Notification** tab.
2. Click **Create > New Alert Notification Rule**.
3. In the **Create Alert Notification Rule** dialog, perform the following:

   a. Enter a unique Notification Name for the alert notification rule.

   b. In the **Notification Filters** section, select the filter based on your requirements:

   Note: The alert notification is sent when an alert matches the combination of the filter settings you have configured.

Filter	Description
Clusters	Select one or more clusters from the drop-down. Otherwise, any cluster will trigger the rule.
Alert Severity	Select one or more severities from the drop-down. Otherwise, all alerts with any severity will trigger the rule.
Alert Type	Select one or more alert types from the drop-down. Otherwise, all alerts of any alert type will trigger the rule.
Alert Category	Select one or more categories from the drop-down. Otherwise, all alerts in any category will trigger the rule.
Alert Name	Select one or more names from the drop-down. Otherwise, any Alert name will trigger the rule. If you selected any categories, the list includes only alerts in those categories.

c. In the Notification Frequency section, select the frequency of the alert notification:

- Real-time
- Every 6 hours
- Every 24 hours

d. In the **Notification Method** section, select **Email**. Choose one of the options from the drop-down based on your requirement:

Options	Description
To	Type an email address or distribution list of the recipients to whom you plan to send the email notification.
CC	Type an email address or distribution list of the recipients to whom you plan to send a copy of the email notification.

Click **+** to add multiple email addresses based on your requirements.

e. Click **Create**.

Create alert notification rule for webhooks notification

Webhooks are HTTP callbacks that are usually triggered by some event. Webhooks are configured on one website, and when an event occurs on this website, an HTTP request is made to the configured URL, which invokes an action on the other website.

Before you begin

You can enable webhooks for cluster alerts by creating an alert notification rule. When the alert is triggered and meets the criteria in the rule, the cluster sends an HTTP request to the specified website. Your application can interpret the request. For example, the webhook might notify the website about a critical protection run alert, and your application might open a trouble ticket to track the problem.

Procedure

To create an alert notification rule for Webhook notifications, complete the following steps:

1. Navigate to the **System > Health > Notification** tab.
2. Click **Create > New Alert Notification Rule**.
3. In the **Create Alert Notification Rule** dialog, perform the following:

a. Enter a unique Notification Name for the alert notification rule.

b. In the **Notification Filters** section, select the filter based on your requirements:

Filter	Description
Clusters	Select one or more clusters from the drop-down. Otherwise, any cluster will trigger the rule.
Alert Severity	Select one or more severities from the drop-down. Otherwise, all alerts with any severity will trigger the rule.
Alert Type	Select one or more alert types from the drop-down. Otherwise, all alerts of any alert type will trigger the rule.

Filter	Description
Alert Category	Select one or more categories from the drop-down. Otherwise, all alerts in any category will trigger the rule.
Alert Name	Select one or more names from the drop-down. Otherwise, any Alert name will trigger the rule. If you selected any categories, the list includes only alerts in those categories.

c. In the **Notification Frequency** section, select the frequency of the alert notification:

- Real-time
- Every 6 hours
- Every 24 hours

d. In the Notification Method section, select Webhook, and provide the URL and cURL options.

Note: Ensure that the Webhook configuration follows the rfc3986 standards.

e. Click **Create**.

Alert request

When an alert is triggered, a sample payload, as shown below, will be available at the configured URL:

Request:

```
https://test-service-now.com/api/dms_webhook
```

The Payload sent to the above URL:

```
{
"receiver": "00101000005nBps_test1",
"status": "firing",
"alerts": [
{
"status": "firing",
"labels": {
"account_id": "00101000005nBps",
"alert_category": "BackupRestore",
"alert_code": "CE00610005",
"alert_id": "10534",
"alert_state": "Open",
"alert_type_bucket": "DataService",
"alert_type_id": "10005",
"alertname": "ProtectedObjectFailed",
"cluster_id": "1609127048663690",
"cluster_id_str": "4327092961767844",
"cluster_name": "DPCluster",
"failure_reason": "Testing DP alerts raise.",
"first_occurrence_usecs": "1682699539084721",
"hidden_from_user": "false",
"job_id": "18211",
"job_name": "Test12",
"job_type": "kOracle",
"matchedTags": "WorkloadSource_kOracle",
"object_id": "181",
"object_name" : "obj181",
"run_id": "182",
"run_start_time": "2023.02.07 11:21:00 Pacific Time",
"run_url": "https://test.com",
"severity": "Critical",
"tenant_id": "d520840916/",
"type": "kOracle"
},
"annotations": {
"cause": "Testing DP alerts raise..",
"description": "Backup of obj181 that is part of protection group Test12 of
type kOracle failed with error Testing DP alerts raise",
"help": "Please refer to KB for details/resolution.",
"occurrence": "Start at 2023-04-28 16:32:19.084721 +0000 UTC, total 1 time."
},
"startsAt": "2023-04-28T16:32:19.084721Z",
"endsAt": "0001-01-01T00:00:00Z",
"generatorURL": "",
"fingerprint": "bfef9abae71570f0"
}
],
"groupLabels": {
"account_id": "00101000005nBps",
"alertname": "ProtectedObjectFailed",
"severity": "Critical"
},
"commonLabels": {
"account_id": "00101000005nBps",
"alert_category": "BackupRestore",
"alert_code": "CE00610005",
"alert_state": "Open",
"alert_type_bucket": "DataService",
"alert_type_id": "10005",
"alertname": "ProtectedObjectFailed",
"cluster_id": "1609127048663690",
"cluster_id_str": "4327092961767844",
"cluster_name": "DPCluster",
"failed_objects": "obj181",
"failure_reason": "Testing DP alerts raise.",
"hidden_from_user": "false",
"job_id": "18211",
"job_type": "kOracle",
"matchedTags": "WorkloadSource_kOracle",
"run_start_time": "2023.02.07 11:21:00 Pacific Time",
"run_url": "https://test.com",
"severity": "Critical",
"tenant_id": "d520840916/",
"type": "kOracle"
},
"commonAnnotations": {
"help": "Please refer to KB for details/resolution."
},
"externalURL": "https://helios-dev3-internal.cohesitycloud.co/alertmanagerd1",
"version": "4",
"groupKey": "{}/{account_id=\"00101000005nBps\",alertname=~\"^(?:ProtectedObjectFailed)$\",
hidden_from_user=\"false\",matchedTags=~\"^(?:.*WorkloadSource_
kOracle.*)$\",tenant_id=\"d520840916/\"}:{account_
id=\"00101000005nBps\", alertname=\"ProtectedObjectFailed\", severity=\"
Critical\"}",
"truncatedAlerts": 0
}
```

Silencing alert notifications

Sometimes, it makes sense to silence alert notifications, such as during maintenance or testing windows.

About this task

You can silence alerts that match the rules you define in the **Silence** tab. Optionally, you can silence alerts for specific periods that you define. Once silenced, alerts are triggered and displayed on the **Alerts** page, but email or Webhook notifications are not sent.

Procedure

To create an alert silence rule, complete the following steps:

1. Navigate to the **System > Health > Silence** tab.
2. Click **Create > New Alert Silence Rule**.
3. In the **Create Alert Silence Rule** dialog, perform the following:
    a. Enter a **Silence Name** for this alert silence rule and provide the Reason why you are creating the alert silence rule.
    b. In the **Silence Filters** section, select the filters based on your requirements:

Filter	Description
Clusters	Select one or more clusters from the drop-down for which you want the alerts silenced.
Alert Severity	Select one or more severities from the drop-down you want to silence.
Alert Type	Select one or more alert types from the drop-down you want to silence.
Alert Category	Select one or more categories from the drop-down you want to silence.
Alert Name	Select one or more names from the drop-down you want to silence.
Source Type	Select one or more sources from the drop-down for which you want the alerts silenced.

c. In the **Time Range** section, select a date in the **Start Date** and **End Date** fields to set the period within which the alert notifications must be silenced.

d. Enable **Suppress** if you do not want the alert to persist and appear on the **Alerts** page.

e. Click **Create**.

Resolving alerts

In case you are aware of the problem and confirm that the issue has been resolved, or if the issue does not require further attention from the **Alerts** tab, you can manually resolve those alert(s). You can either create a new resolution of the alert(s) or attach an existing resolution to the alert(s).

Creating a new resolution

Procedure

To create a new resolution, complete the following steps:

1. In the Alerts tab, select an alert or multiple alerts you plan to resolve and click **Resolve Selected Alerts**.
2. In the **Resolution** dialog, do the following:

   a. Select **Create new resolution**.

   b. In the **Resolution Summary** field, add a resolution summary for the alert.

   c. In the **Resolution Description** field, add a brief description of the resolution.

   d. Click **Resolve**.

Results

The resolution is added to the selected alerts, and the alert(s) status is marked as **Resolved**.

Attaching an existing resolution

Procedure

To attach an existing resolution to the alert(s), complete the following steps:

1. In the **Alerts** tab, select an alert or multiple alerts you plan to resolve and click **Resolve Selected Alerts**.

2. In the **Resolution** dialog, do the following:
    a. Select **Associate with existing resolution**.
    b. From the **Resolution Summary** drop-down, you can search and select the resolution that you plan to attach to the alert.
    c. Click **Resolve**.

Results

The existing resolution is attached to the selected alerts, and the alert(s) status is marked as **Resolved**.

Resolving an alert in the Details for any Alert Name page

Once you have reviewed the alert, you can resolve the alert using the page's **Resolution** section. You can create a new alert resolution or attach an existing one in the **Resolution** section.

- To create a new resolution:
    1. In the **Resolution** section, select **Create new resolution**.
    2. In the **Resolution Summary** field, add a resolution summary for the alert.
    3. In the **Resolution Description** field, add a brief description of the resolution.
    4. Click **Resolve**.
- To attach an existing resolution:
    1. In the **Resolution** section, select **Associate with existing resolution**.
    2. From the **Resolution Summary** drop-down, you can search and select the resolution that you plan to attach to the alert.
    3. Click **Resolve**.

Alert references

For details on the alerts triggered by the clusters managed on Data Management, see the following documentation references for the respective IBM Storage Defender Data Management Service cluster version:

- IBM Storage Protect – Messages, return codes, and error codes
- IBM Storage Defender Data Protect:
    1. Click on **Reference Information** for the Data Protect version that you use.
    2. You will be redirected to a index page.
    3. On this index page click on the **Alerts** link to download the complete reference of alerts in xlsx format.

  For more information, see IBM Storage Defender Data Protect.

Appendix A. Accessibility features for IBM Storage Defender

Accessibility features assist users who have a disability, such as restricted mobility or limited vision, to use information technology content successfully.

Overview

IBM Storage Defender includes the following major accessibility features:

- Keyboard-only operation
- Operations that use a screen reader

IBM Storage Defender uses the latest W3C Standard, WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/), to ensure compliance with US Section 508 and Web Content Accessibility Guidelines (WCAG) 2.2 (www.w3.org/TR/WCAG20/). To take advantage of accessibility features, use the latest release of your screen reader and the latest web browser that is supported by the product.

The product documentation in IBM Storage Defender is enabled for accessibility.

Keyboard navigation

This product uses standard navigation keys.

Interface information

User interfaces do not have content that flashes 2 - 55 times per second.

Web user interfaces rely on cascading style sheets to render content properly and to provide a usable experience. The application provides an equivalent way for low-vision users to use system display settings, including high-contrast mode. You can control font size by using the device or web browser settings.

Web user interfaces include WAI-ARIA navigational landmarks that you can use to quickly navigate to functional areas in the application.

Vendor software

IBM Storage Defender includes certain vendor software that is not covered under the IBM license agreement. IBM makes no representation about the accessibility features of these products. Contact the vendor for accessibility information about its products.

Related accessibility information

In addition to standard IBM help desk and support websites, IBM has a TTY telephone service for use by deaf or hard of hearing customers to access sales and support services:

TTY service
800-IBM-3383 (800-426-3383)
(within North America)

For more information about the commitment that IBM has to accessibility, see IBM Accessibility (www.ibm.com/able).

© Copyright IBM Corp. 2023, 2024

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

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

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 supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

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

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

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.

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 the names and addresses used by an actual business enterprise 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.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., 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 www.ibm.com/legal/copytrade.shtml.

Adobe is a registered trademark of Adobe Systems Incorporated in the United States, and/or other countries.

Linear Tape-Open, LTO, and Ultrium are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Intel and Itanium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

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

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

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.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

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.

Product Number: 5900-AXW5900-AY6