

# IBM Storage Defender Data Resiliency Service

## *User's Guide*



**Note:**

Before you use this information and the product it supports, read the information in [“Notices” on page 69.](#)

**August 2024 edition**

This edition applies to IBM Storage Defender Data Resiliency 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 Resiliency 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

<b>About this publication.....</b>	<b>V</b>
<b>Chapter 1. Data Resiliency concepts.....</b>	<b>1</b>
Threat detection.....	2
IBM Storage Defender sensor.....	2
IBM Storage FlashSystem threat detection.....	3
Recovery group.....	4
Recovery test and recovery.....	5
<b>Chapter 2. Data Resiliency dashboard.....</b>	<b>9</b>
<b>Chapter 3. Recovery groups.....</b>	<b>11</b>
Creating a recovery group.....	11
Recovery group details.....	11
Open case.....	12
Overview.....	13
Protection.....	13
Detection.....	16
Resources.....	17
Notification.....	18
History.....	19
<b>Chapter 4. Profiles.....</b>	<b>21</b>
Governance profiles.....	21
Adding a governance profile.....	21
Reviewing a governance profile.....	22
Editing a governance profile.....	23
Removing a governance profile.....	23
Clean Room profiles.....	23
Adding a clean room profile.....	26
Reviewing a clean room profile.....	28
Editing a clean room profile.....	28
Removing a clean room profile.....	28
<b>Chapter 5. Resources.....</b>	<b>29</b>
Adding a connection manager.....	29
Reviewing available resources.....	29
Reviewing connections.....	29
Reviewing the connection managers.....	30
<b>Chapter 6. Integrations.....</b>	<b>33</b>
Integrating Data Resiliency to QRadar SIEM.....	33
Enabling email notification.....	35
<b>Chapter 7. IBM Storage Defender Connection Manager.....</b>	<b>37</b>
Connecting Data Resiliency to on-premises resources.....	37
Logging in to the user interface.....	39
Managing a Connection Manager profile.....	39
Connecting to data sources, recovery locations, and sensors.....	40

Data sources.....	40
Recovery locations.....	42
Sensor control nodes.....	43
Access.....	51
Roles in IBM Storage Defender Connection Manager.....	51
Users.....	51
User roles required to connect with IBM Storage FlashSystem.....	53
User rights required to connect with IBM Storage Defender Data Protect.....	53
User rights required to connect with VMware vCenter.....	53
Settings.....	53
Updating the name of the Connection Manager.....	53
Updating the Connection token of the Connection Manager.....	53
Downloading support logs.....	54
Upgrading Connection Manager.....	54
Backing up and restoring Connection Manager.....	55
Troubleshooting Connection Manager issues.....	57
Resolving an IBM Storage Defender sensor uninstallation failure.....	57
Appendix: Inventory metadata that is collected from Data Resiliency.....	58
<b>Chapter 8. Licensing.....</b>	<b>63</b>
<b>Appendix A. Accessibility.....</b>	<b>67</b>
<b>Notices.....</b>	<b>69</b>

## About this publication

---

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



---

# Chapter 1. Data Resiliency concepts

IBM Storage Defender Data Resiliency Service (DRS) introduces several new concepts. With these concepts you can plan, secure, test, and recover the data that you declare is most important to you.

## Recovery Group

Data Resiliency introduces the concept of recovery groups. You can organize collections of important resources into a recovery group. Review the [Recovery Group](#) topic to learn more and how they are used by Data Resiliency.

## Recovery Test and Recovery

Data Resiliency service introduces the concept of recovery and recovery testing. Recovery groups can be periodically tested to ensure that the viable recovery points that are needed are available. And if necessary, a recovery group can be used to recover the assigned resources when a cyber event occurs. Review the [“Recovery test and recovery” on page 5](#) topic to learn more about how recovery groups can be tested and used for recovery.

Recovery groups are assigned a protection level, which specifies the user's preferences for the number of recovery points that are needed and how frequently validation occurs. Additionally, recovery groups are assigned a clean room profile, which defines a user's preferences for running a recovery or a recovery test.

## Connection Manager

Data Resiliency introduces an agent that runs in your data center. This agent is responsible for connecting to your primary and secondary data sources for collecting information about them. The data stays only in your data center. The information that is collected by the Connection Manager is used to help you define plan, test, secure, and recover your data.

## Threat detection

**Defender® Sensor:** IBM Storage Defender provides malware sensors that can be deployed to virtual machines (VMs). These sensors perform near real-time monitoring and detection of malware for supported workloads. This information is sent to IBM Storage Defender Data Resiliency Service and used to help you understand when and where you might be encountering a cyber event that helps you to take action.

**IBM Storage FlashSystem threat detection:** The integration between IBM Storage Defender and IBM Storage FlashSystem allows the Data Resiliency service to access the information reported from the FlashCore Modules. The FlashCore Module sensors perform inline monitoring or operations on storage block level. The combination of anomaly detection on application level using the Defender sensors and on block level using the FlashCore Modules data increases the ability to detect malicious operations quickly.

## Governance Profile

IBM Storage Defender Data Resiliency Service allows you to assign data to governance profiles. These governance profiles provide criteria that IBM Storage Defender uses to evaluate your readiness to recover from a cyber event. These governance profiles include criteria for the number of recovery points that need to be available for a primary workload and how frequently the recovery snapshots need to be tested.

## Clean Room Profile

IBM Storage Defender Data Resiliency Service allows you to create recovery preferences. Data that is important to you is defined in a recovery group, which is assigned to a clean room profile. The clean room profile provides information about how to test a workload and recovery preferences for that workload.

## Recovery Plan

The recovery plan defines the lifecycle of a recovery group in Data Resiliency. The recovery plan is a virtual concept that is created automatically when a recovery group is created. For each resource in the recovery group, the engine behind the recovery plan compares the existing backup copies and the existing backup policies with the protection level that is assigned to the recovery group. Depending on the result of the comparison, the recovery plan informs the user about compliance or recommends

change that can help to achieve compliance. The recovery plan has a built-in scheduling concept that is used to perform automated recovery tests of a specific recovery group.

## Threat detection

IBM Storage Defender can detect operational threats on your production data.

You can use threat detection for the following system level detections:

- Detection on the file system level that is using IBM Storage Defender Sensor technology.
- Detection on the storage block level that is using IBM Storage FlashCore Module technology and statistical analysis to identify threat patterns.

### IBM Storage Defender sensor

IBM Storage Defender sensors implement a real time detection mechanism for anomalous operations on file system objects.

IBM Storage Defender sensors are part of the IBM Storage Defender product. You can deploy sensors on virtual machines that are part of recovery groups. When the sensors are deployed, the sensors automatically sent metadata to the IBM Storage Defender Data Resiliency Service.

On a high level, the workflow can be described as shown in the following image:

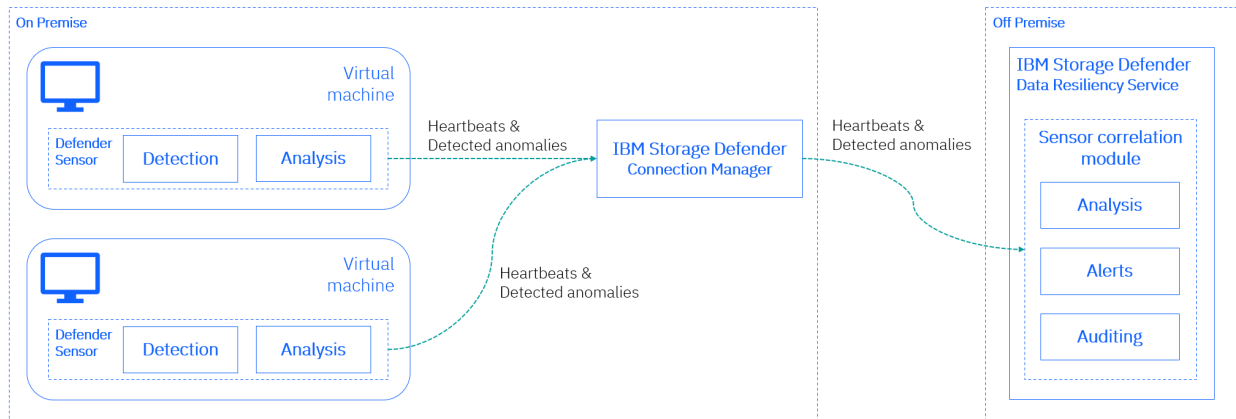


Figure 1. IBM Storage Defender Sensor workflow

#### IBM Storage Defender sensor operation on premises

1. When installed, the sensors use file system and operating system interfaces to collect information about operations on file system objects.
2. While collecting this information, sensors analyze this information to identify anomalies for operations on file system objects.
3. Frequently, heartbeat information is sent to the IBM Storage Defender Connection Manager to signalize that the sensor is active.
4. When anomalies are detected, the related information is sent to the IBM Storage Defender Connection Manager. A single Connection Manager can have many sensors that report data to it.

#### IBM Storage Defender sensor operation off premises

1. The IBM Storage Defender Connection Manager reports the sensor data that is collected on premises to the IBM Storage Defender Data Resiliency Service.
2. The Data Resiliency Service correlates the information with recovery groups in your tenant.
3. When sensor heartbeat information is missing or when an anomaly is detected for file system object data operations, a case is opened for the related recovery group.
4. Depending on your notification settings, you are notified about the new case.



## IBM Storage FlashSystem threat detection

IBM Storage FlashSystem threat detection is designed to provide resilient data storage in the event of a cyberattack. IBM Storage FlashSystem offers new smart technology that is enabled by FCM4 and designed to continuously monitor statistics gathered from every I/O. IBM Storage FlashSystem uses machine learning models to detect anomalies like ransomware in less than a minute, which helps ensure that your business is protected before a cyberattack.

IBM Storage Defender Data Resiliency Service integrates with IBM Storage Insights Pro and IBM FlashCore Module to enable inline data anomaly detection on storage block level.

**Note:** If you register the IBM Storage FlashSystem with IBM Storage Defender and you register the IBM Storage FlashSystem with IBM Storage Insights Pro, the threat detection is enabled automatically.

### IBM FlashCore Modules

IBM FlashCore Modules (FCM) are a family of high-performance flash drives in a standard 2.5", 15 mm form factor. The IBM FlashCore Module design uses the NVMe protocol, a PCIe Gen3/Gen4 U.2 interface, and high-speed NAND memory to provide high throughput and IOPS with consistent and predictable latency. Furthermore, IBM FlashCore Modules in version 4 implement an anomaly detection for operations on storage block level.

### IBM Storage Insights Pro

IBM Storage Insights Pro is a powerful cloud-based management platform that empowers businesses to proactively manage, monitor, and optimize their storage infrastructure in addition to network and host servers by using advanced AIOps features. Your ability to identify ransomware threats on storage systems is advanced with the AI-based ransomware threat detection. This feature adds an extra layer of detection that is designed for IBM® Storage Virtualize storage systems.

The following image describes the high-level integration between the products.

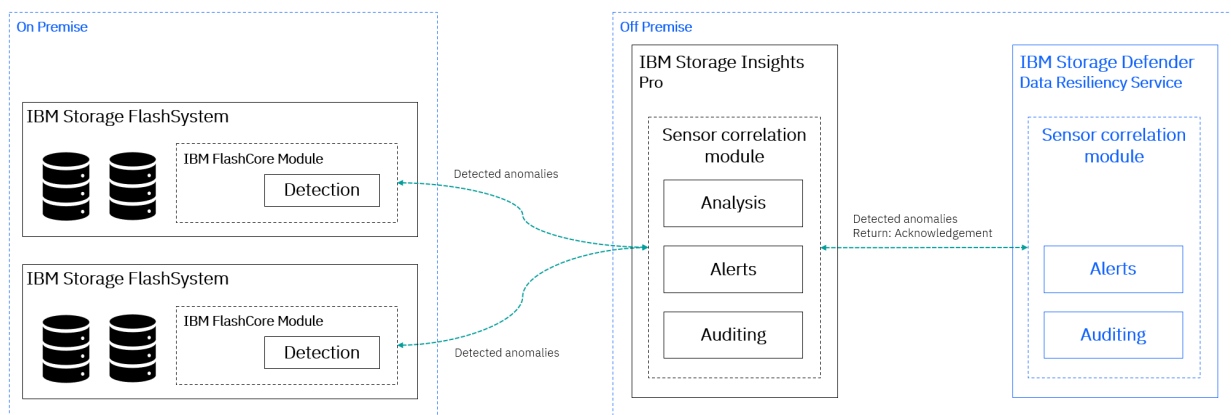


Figure 2. IBM Storage Defender integration with IBM FlashCore Module work flow

### Working principle of the IBM Storage Defender integration with IBM FlashCore Module

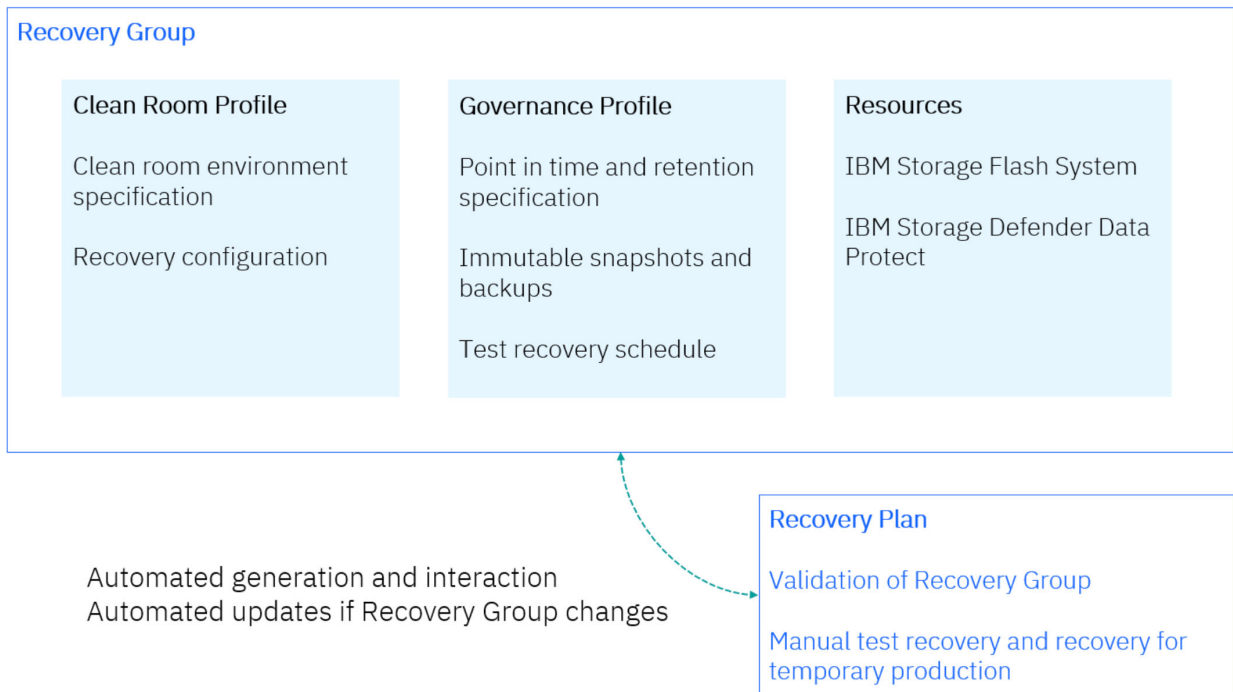
1. IBM FlashCore Module version 4 technology is built in the IBM Storage FlashSystem that is used.
2. The IBM Storage FlashSystem is registered in IBM Storage Insights Pro. When the system is registered, the IBM FlashCore Module starts reporting the detected anomalies to your IBM Storage Insights Pro tenant.
3. IBM Storage Insights Pro correlates the data from multiple IBM FlashCore Modules and analyzes the data.
4. The IBM Storage FlashSystem needs to be registered in IBM Storage Defender Data Resiliency Service. This registration is done in the user interface of Connection Manager.
5. The IBM Storage Insights Pro communicates with Data Resiliency Service. The data that is related to your IBM Storage FlashSystem is sent to the Data Resiliency Service.

6. IBM Storage Defender correlates the information that is received from the storage system to recovery groups.
7. When the IBM FlashCore Module detects an anomaly for block level data operations, a case is opened for the related recovery group.
8. Depending on your notification settings you are notified about the new case.

For more information about integrating IBM Storage Defender with IBM Storage FlashSystem as a data source, see [“Adding data sources” on page 40](#).

## Recovery group

You can use IBM Storage Defender to prioritize which data is important to you. To prioritize the data, you must assign storage resources to a recovery group, which is assigned to a governance profile and clean room profile.



A recovery group is a collection of related storage resources that are used to represent an important application or service in your environment. It is important to consider that a resource group meets the following characteristics:

1. There is a relationship between the resources that are assigned to the recovery group. For example, if a billing application your enterprise relies upon is based on 4 virtual machines (VMs), those 4 VMs should be assigned to the same recovery group.
2. The resources assigned to a recovery group need to be protected together (data protection snapshots should be made with the same frequency and retained for the same duration).

**Tip:** If IBM Storage Defender Data Protect is being used in your environment, then it is recommended that the VMs for a recovery group are assigned to the same policy and protection group in the IBM Storage Defender Data Protect Cluster. With this type of setup, the backups for the VMs are managed with the same retention, version policies, and the backups are performed at the same time from the association in the same protection group.

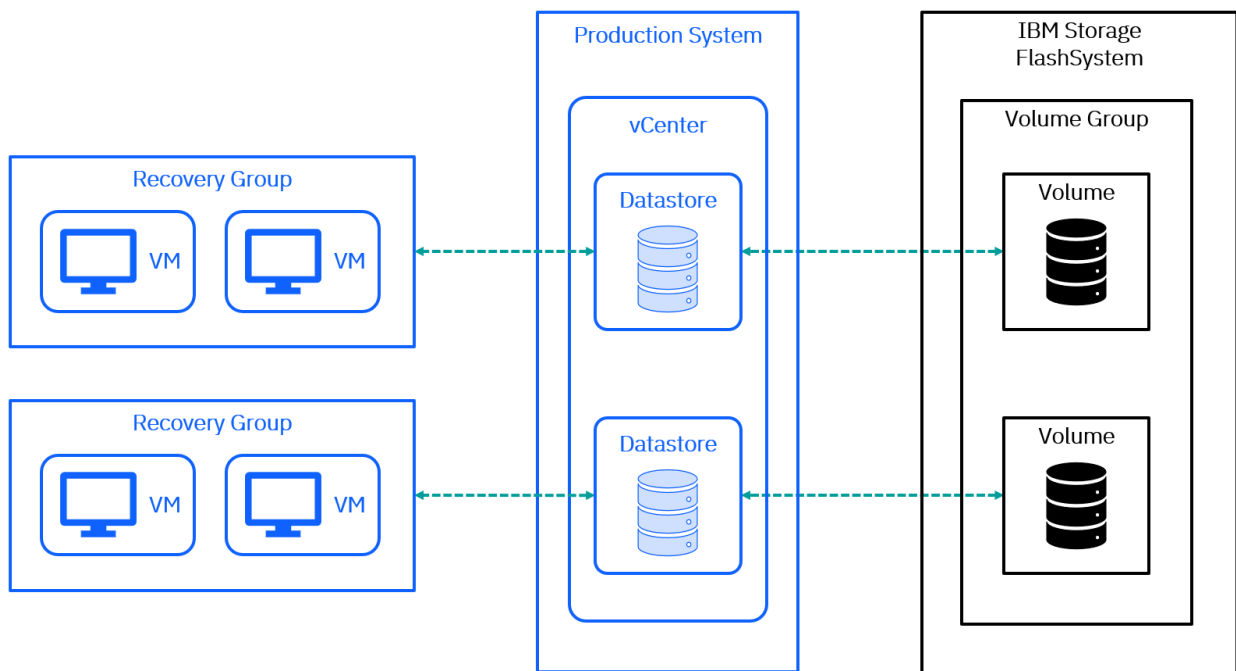
3. If a recovery is needed for the resources that are assigned to this recovery group, they should all be recovered together by using snapshots from the same point in time.

You can use IBM Storage Defender Data Resiliency Service to create recovery groups. The recovery group is evaluated when it is created to determine whether there are corresponding secondary resources such as data protection backups or snapshots available.

For example, if a recovery group is assigned with VM1, VM2, VM3, and VM4. Then IBM Storage Defender Data Resiliency Service determines whether it can find backup snapshots for these VMs in the secondary data sources in the same location (data center). If IBM Storage Defender Data Resiliency Service is able to correlate the primary and secondary VMs, it proceeds to test the recovery group based on the policy and clean room profile settings.

### Recovery Group and IBM Storage FlashSystem Volume Groups

Typically a datastore in a vCenter relates to a single volume in the IBM Storage FlashSystem. Multiple of such single volumes can be combined in the same volume group of IBM Storage FlashSystem. IBM Storage Defender Data Resiliency Service supports Recovery Groups that contain virtual machines, where the virtual machines belong to the same datastore in the vCenter and a single volume in the IBM Storage FlashSystem volume group. The following image illustrates a typical setup of a Recovery Group that contains virtual machines that belong to the same vCenter. The image also illustrates that the datastore in vCenter uses a single volume that is part of a volume group in IBM Storage FlashSystem.



## Recovery test and recovery

Data Resiliency Service introduces the concept of recovery tests. Recovery tests for recovery points that were detected from IBM Storage Defender can be performed at any time. The test frequency can be observed automatically by using the governance profile settings.

### Recovery Test

The Data Resiliency Service provides testing of recovery points for a recovery group. Testing of recovery points for a recovery group can be done when the status for the group is **Ready**. The testing of recovery points for a recovery group establishes the recovery plan, which is used if needed, in response to the occurrence of a cyber event.

The recovery plan for a recovery group has one of the following status values:

- **No Plan:** A recovery group is in **Draft** status and is not complete, so no recovery plan is created.
- **Ready:** A recovery group is complete, created a recovery plan, successfully tested, and validated one or more recovery points.
- **Test in Progress:** A recovery point for a recovery group is identified and being tested. If successful, the recovery plan status promotes to **Ready**. And if unsuccessful, the recovery plan status demotes to **At risk**.

- **At Risk:** A recovery group is complete and has a recovery plan. However, the recovery plan is at risk because it has no tested and validated recovery points. Some possible reasons that a recovery plan may not be able to test and validate a recovery point are: incomplete or missing backup (snapshots) for the assigned resources, the test is failed, or the recovery location is offline or unreachable.

To understand more about how recovery plans are managed for recovery groups, consider the following:

- **Creation of the test and recovery point:** In this step, the recovery point for the recovery group is created and listed in the recovery plan details section. The status of the recovery point is set to **Test in progress**.
- **Validation of the backup policy and of existing recovery points:** The recovery manager validates the backup policy and the existing recovery points against the governance profile. In addition, the governance profile that is assigned to the recovery group is compared with the recovery points that exist in the data protection solution that is used for each resource in the recovery group. When this verification step is passed the test recovery is initiated. When the verification step fails the status of the recovery point is updated from **Test in progress** to **At risk**. The status **At risk** of a recovery point can have multiple reasons.

For example,

- The backup policy that is used for the resources that does not meet the governance profile settings of the recovery group.
- The recent backup operations of the resources failed and no recovery point is available for some of the resources so that the governance profile cannot be met.

Any information that causes a recovery point to be in status **At risk** is added to the log of the recovery plan and displayed in the user interface.

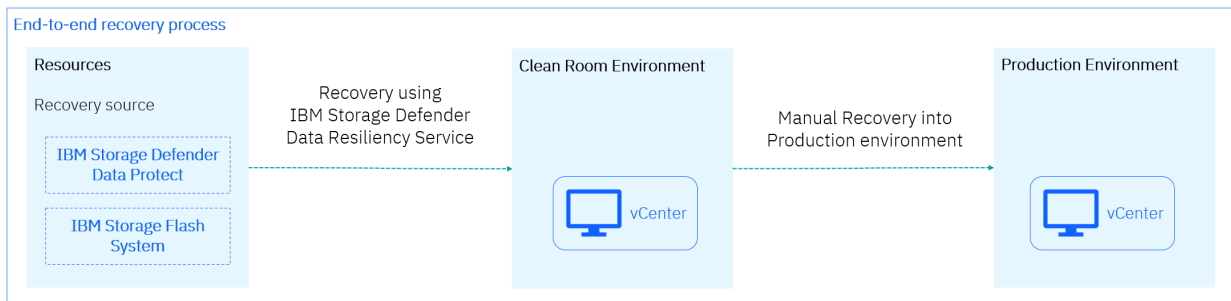
- **Test recovery and result verification:** In this step the virtual machines that belong to the recovery group are recovered by using the information that is stored in the clean room profile that is associated with the recovery group. Depending on the configuration of the clean room profile, the virtual machines are started and connected to the defined network or not. When the test recovery is finished successfully the status of the recovery point will be updated from **Test in progress** to **Awaiting validation**. To validate a recovery point, see [“Initiate the validation of a recovery point” on page 15](#). The result of the validation can be that you decide that the recovery was successful or not. As part of the validation process you can assign one of these options to the recovery point. Depending on the decision that you make the status of the recovery point will be updated from **Awaiting validation** to **Validated** or **Not valid**. The recovery points are kept in the history of the recovery group until the recovery window that is defined in the associated governance profile is exceeded.

The **Manual recovery test:** This is an ad hoc operation that can be performed at any time for a given recovery group. The manual recovery test follows the same steps as the orchestrated recovery test. You can initiate the manual recovery test by using the vertical ellipsis menu of an existing recovery point and selecting Test recovery point.

## Recovery

**Note:** IBM Storage Defender Data Resiliency Service does not support the recovery directly back to production. To ensure IBM Storage Defender does not interfere with any forensic analysis that may be required in the production environment, the recovery can go to a test environment or a specific recovery environment only. The final step to promote the recovered resources back into the production environment must be a manual step.

Example: For vCenter, the production vCenter URL must not be used in any of the Clean Room Profiles.



The recovery group option that is called **Activate recovery plan** describes the actual recovery of resources that are associated with a recovery group. This **Activate recovery plan** option uses an existing and valid recovery point to recover your application after a cyber attack or disaster. In contrast to the manual recovery test, the activate recovery plan process provides the flexibility to specify a new clean room profile for the given recovery point. With this option, you can use a dedicated recovery environment to test the recovery point again and prepare a recovery point for a downstream promotion into your production environment.



---

## Chapter 2. Data Resiliency dashboard

The dashboard provides you with a high-level overview on the existing recovery groups that you have created before. It also provides you with a summary of the connected resources like virtual machines, data sources, recovery locations, and connection managers. In addition, the dashboard provides you with the license usage overview in terms of used recovery groups from your assigned pool.

To access the dashboard, log in to the Recovery Service and click the **Dashboard** button.





---

## Chapter 3. Recovery groups

The recovery group is a concept for virtual inventory grouping in Data Resiliency.

### Creating a recovery group

---

Create a recovery group in Data Resiliency to add resources and clean room profiles to test and run the recovery schedules.

#### Procedure

To create a recovery group, complete the following steps:

1. On the Data Resiliency home page, click **Recovery Groups**.
2. On the **Recovery Groups** page, click the **Create group** button. The **Create recovery group** page appears.
3. Specify a name for the recovery group, and then click **Next**.

**Tip:** Use a name that indicates the application you want to address with the recovery group.

4. Review the governance profile page and click one of the defined governance profiles to make a selection. After choosing a governance profile, click **Next**.

**Note:** If you are not ready to assign a governance profile to your recovery group in this step, you can choose a governance profile later. In this case, the recovery group will be set to draft.

5. Click one of the connected and inventoried vCenters.

**Tip:**

If you have connected a new vCenter recently, it may not yet be fully inventoried. You can check later and complete this step.

If you have many vCenters connected to Data Resiliency you can use the **Search** function to find the vCenter.

6. Select the virtual machines that you want to add to the recovery group, and then click **Next**.

**Tip:** If you have many virtual machines in the selected vCenter, you can use the **Search** function to find the virtual machines.

7. Review the clean room profiles and click one of the configured clean room profiles, and then click **Create**.

**Note:** If you do not have a clean room profile that is configured, you can configure and assign it to the recovery group later.

#### What to do next

To view the details of a recovery group, complete the following steps:

1. On the Data Resiliency home page, click **Recovery Groups**.
2. Review the list of available recovery groups.

**Tip:** If you have many recovery groups in the list, you can use the Search function to find the right ones by name.

### Recovery group details

---

The recovery group dashboard provides you with all information needed for a quick review of the recovery group. The dashboard shows you the current state of the recovery plan and the progress on potential test recovery processes that are ongoing. If you are missing a verification step of a former test recovery, this

information is displayed here as well. The dashboard also includes a high-level listing of resources like protected virtual machines, connected vCenters, and IBM Storage Defender connection managers. For each of the resources the dashboard will indicate the health status. In addition to the recovery plan and resources information the dashboard includes a listing of IBM Storage Defender sensors that are installed on virtual machines that belong to the recovery group.

**To review the Recovery group dashboard to see information about one recovery group, complete the following steps:**

1. On the Data Resiliency home page, click **Recovery Groups**.
2. From the list of recovery groups, click the row in the table for the one you are interested in.
3. On the recovery group's details page, go to the navigation menu and click **Overview**.

## Open case

The Open case dashboard appears automatically when IBM Storage Defender detects an event for the recovery group.

**To view the open case dashboard for a recovery group, complete the following steps:**

1. On the Data Resiliency home page, click **Recovery Groups**.
2. From the list of recovery groups, click the row in the table for the recovery group that you are interested in.
3. On the recovery group's Overview dashboard, go to the navigation menu and click **Open case**.

### Review the overall number of events

In the **Case summary** tile, you can review the overall number of events registered for the recovery groups. Furthermore, you can review the time when the event was received the first time.

### Review the affected resources from the event

In the **Resource impact summary** tile, you can review which resources are affected from the event. The tile provides you with information about the Data sources, the list of affected virtual machines, the number of files affected, and the storage resources that are affected from the event.

### Review the list of events detected for the recovery group

In the **Timeline** tile, you can review the list of events detected for the recovery group. You can filter the list and you can review details for the events.

**To filter the event for different event types, complete the following steps:**

1. On the **Timeline** tile, click the drop-down menu for **Events**.
2. From the drop-down menu, select either **All events**, **Possible malware events**, or **Missed heartbeat**.

**To filter the event for different event sources, complete the following steps:**

1. On the **Timeline** tile, click the drop-down menu for Sources.
2. From the drop-down menu, select either **All sources**, **FCM anomaly detection**, or **Defender sensors**.

### Review details of the event

To review details of the event, click on **View sensor logs**.

### Close the open case

When the case or event has been resolved or determined, you can close the case. To close the case, click **Actions** and from the drop-down menu, select **Close case**.

### Activate Recovery Plan

If there is an anomaly detected, the separate **Activate Recovery Plan** button is enabled to click on the dashboard. If you want to activate a recovery plan as a preventive measure, click **Actions** and from the drop-down menu, select **Activate Recovery Plan**.

## Overview

The recovery plan dashboard shows you the current state of the recovery plan and the progress on potential test recovery processes that are running. If you are missing a verification step of a former test recovery, that information is displayed here as well. The dashboard also includes an overview on the clean room profile that is used for the recovery group. Also in the dashboard, you can edit the clean room profile association, assign a different clean room profile, manage Defender sensors, and view status of IBM Storage FlashSystem ransomware detection if applicable.

In addition, the recovery plan dashboard shows the governance profile that is assigned to the recovery group. And in the dashboard, you can edit the governance profile association and assign a different governance profile. Also, the list of existing recovery points for the recovery group are listed on the dashboard and ad hoc operations are allowed such as validating or activating a recovery point.

On the dashboard, you can complete the following actions:

### Rename a recovery group

To rename a recovery group, complete the following steps:

1. On the Overview dashboard, go to the **Actions** drop down button and select **Rename**.
2. In the pop-up window, enter a new name for the recovery group.
3. In the pop-up window, click the **Save** button.

### Archive a recovery group

To archive a recovery group, complete the following steps:

1. On the Overview dashboard, go to the **Actions** drop down button and select **Archive**.
2. In the pop-up window, confirm that you want to archive the recovery group.
3. In the pop-up window, click the **Archive** button.

### Assign a new clean room profile to a recovery group

To assign a new clean room profile to a recovery group, complete the following steps:

1. On the Recovery plan dashboard, go to the clean room profile section and click the pen symbol.
2. In the pop-up window, review the list of available clean room profiles and select the clean room profile that you want to associate with the recovery group.
3. In the pop-up window, click the **Save** button.

### Assign a new governance profile to a recovery group

To assign a new governance profile to a recovery group, complete the following steps:

1. On the **Recovery plan** dashboard, go to the governance profile section and click the pen symbol.
2. In the pop-up window, review the list of available governance profiles and select the governance profile that you want to associate with the recovery group.
3. In the pop-up window, click the **Save** button.

**Note:** Updating the governance profile of a recovery group causes a new validation of the recovery plan. A recovery plan that was valid before, can become invalid or vice versa.

## Protection

The Protection tab provides you with a detailed view on the available recovery points for the recovery group. Furthermore, it provides you with the capability to run a test recovery using a specific recovery point or to activate a recovery plan for a recovery.

## Assign a new clean room profile to a recovery group

To assign a new clean room profile to a recovery group, complete the following steps:

1. On the Recovery plan dashboard, go to the clean room profile section and click the pen symbol.
2. In the pop-up window, review the list of available clean room profiles and select the clean room profile that you want to associate with the recovery group.
3. In the pop-up window, click the **Save** button.

## Assign a new governance profile to a recovery group

To assign a new governance profile to a recovery group, complete the following steps:

1. On the **Recovery plan** dashboard, go to the governance profile section and click the pen symbol.
2. In the pop-up window, review the list of available governance profiles and select the governance profile that you want to associate with the recovery group.
3. In the pop-up window, click the **Save** button.

**Note:** Updating the governance profile of a recovery group causes a new validation of the recovery plan. A recovery plan that was valid before, can become invalid or vice versa.

## Initiate the test of a recovery point

If you test a recovery point, a test recovery of the recovery group is initiated.

To initiate the test of a recovery point, complete the following steps:

1. On the **Recovery plan** dashboard, go to the **Recovery Points** section.
2. Scroll the list to the recovery point of interest.

**Note:** You can use the search bar to search for a specific time or filter the list for specific states of a recovery plan.

3. Open the context menu in the right side and select **Test recovery point**.
4. Review the planned recovery process.
5. Click the **Recover** button.
6. After the recovery is finished, the recovery point used changes the status to **Awaiting validation**. You can perform a validation of the recovery point now.

## Initiate the activation of a recovery point

If you activate a recovery point, a test recovery of the recovery group is initiated.

To initiate the activation of a recovery point, complete the following steps:

1. On the **Recovery plan** dashboard, go to the **Recovery Points** section.
2. Scroll the list to the recovery point of interest.

**Note:** You can use the search bar to search for a specific time or filter the list for specific states of a recovery plan.

3. Open the context menu in the right side and select **Activate recovery point**. This action opens a pop-up window.
4. In the pop-up window, select a recovery point that you want to activate.
5. Click the **Next** button.
6. Select a clean room profile that you want to use for the recovery.
7. Click the **Next** button.
8. Review the planned recovery process.
9. Click the **Recover** button.

**Note:** If you select offline recovery, the button is called Download plan.

10. After the recovery is finished, the recovery point used changes the status to **Awaiting validation**. You can perform a validation of the recovery point now.

## Initiate the validation of a recovery point

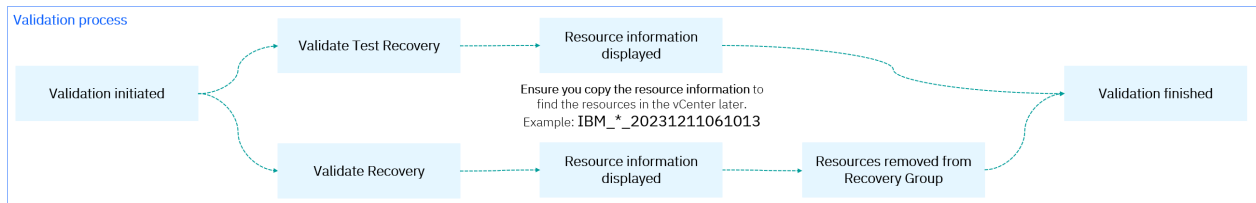
If you validate a recovery point after the manual test recovery or the manual activate recovery process, the recovery point is marked with the result. This information helps you when you want to use the recovery point for a recovery later.

The validation process implements two options:

- The validation after the manual test recovery – This process will not change the resources of the Recovery Group, but will mark the recovery point for you to simplify later to find a valid recovery point.
- The validation after the activate recovery point process – In this process IBM Storage Defender Data Resiliency Service assumes that the former resources are no longer usable and removes it from the Recovery Group. You can add the new resources that exist after the recovery to the Recovery Group after the validation.

**Note:** Ensure that you copy the resource information that is displayed as part of the validation process. You will need this information to find the recovered resources in the vCenter for renaming or removal.

The following figure illustrates the validation process:



To initiate the validation of a recovery point after **manual test recovery**, complete the following steps:

1. On the **Recovery Plan** dashboard, go to the **Recovery Points** section.
2. Choose the recovery point of interest from the list.

**Tip:** You can use the search bar to search for a specific time or filter the list for specific states of a recovery plan.

3. Open the context menu from the panel in the right side and select **Validate**. This action opens a pop-up window.
4. In the pop-up window, select the **Test Only** button.
5. In the next step, you can specify if the recovery point is valid or not valid.

**Note:** Ensure that you copy the resource information.

6. Click the **Yes** button to confirm the recovery point is valid.
7. After the validation is finished, the recovery point will be in the **Valid** or **Not valid** status.

**Note:** IBM Storage Defender Data Resiliency Service does not remove the recovered resources from the vCenter automatically. To remove the resources from the vCenter, see section **Clean up vCenter after Recovery** below.

To initiate the validation of a recovery point after **activate recovery plan**, complete the following steps:

1. On the **Recovery Plan** dashboard, go to the **Recovery Points** section.
2. Choose the recovery point of interest from the list.

**Note:** You can use the search bar to search for a specific time or filter the list for specific states of a recovery plan.

3. Open the context menu from the panel in the right side and select **Validate**. This action opens a pop-up window.

4. In the pop-up window, select the **Recovery Plan** button.
5. In the next step, you can specify if the recovery point is valid or not valid.

**Note:** Ensure that you copy the resource information.

6. Click the **Yes** button to confirm the recovery point is valid.
7. After the validation is finished, the recovery point will be in the **Valid** or **Not valid** status.

**Note:** If you have defined that the recover point is valid, the original resources are removed from the Recovery Group. Optionally, you can rename the recovered resources in the vCenter that you used for the recovery. You can add the recovered resources to the same Recovery Group again.

## Clean up after Safeguarded Copy recovery

If you initiate the clean up after Safeguarded Copy recovery the virtual machines created for the recovery, the datastore, and the clone created on the IBM Storage FlashSystem is cleaned up automatically.

To initiate the clean up of a recovery point, complete the following steps:

1. steps to be added - Dominic

## Clean up vCenter after Recovery

**To locate the recovered virtual machine in the vCenter, complete the following steps:**

1. Log in to the vCenter that was defined in the clean room profile. The clean room profile is the one that is used for the Recovery Group that is activated.
2. In the Search bar, enter the date by when the Recovery Plan is activated in the format: YYYYMMDD.
  - a. The vCenter user interface lists all the virtual machines that have the date in the name.
  - b. The virtual machines that were recovered with the Data Resiliency Service uses the original virtual machine's name with the prefix IBM\_ and the postfix \_YYYYMMDDhhmmss.
3. Identify one of the virtual machines that belong to the Recovery Group that is recovered. Click on this virtual machine.
  - a. The vCenter user interface opens the browser view of the folder structure that contains the virtual machine that you identified.
  - b. The folders are created automatically when the recovery of the Recovery Group is performed.
  - c. Each folder contains all the virtual machines that are part of the Recovery Group.

**To cleanup the recovered virtual machines in the vCenter, complete the following steps:**

1. Locate the recovered virtual machines.
2. Shutdown the virtual machines that you want to remove from the vCenter.
3. Use the vCenter functionality to remove the virtual machines from the vCenter.
4. If you remove all virtual machines from the containing folder, you can remove the folder from the vCenter by using the vCenter functionality.

## Detection

The **Detection** dashboard is dedicated to the information provided by the IBM Storage Defender sensor suite and its current configuration. On the **Detection** dashboard, you can review events from the IBM Storage Defender sensors, IBM Storage FlashSystem, and view detailed log information to understand why an alert was generated. You can also review the current state of the existing IBM Storage Defender sensor installations and IBM Storage FlashSystem.

**To view the Detection dashboard for a recovery group, complete the following steps:**

1. On the Data Resiliency home page, click **Recovery Groups**.

2. From the list of recovery groups, click the row in the table for the recovery group that you are interested in.
3. On the recovery group's Overview dashboard, go to the navigation menu and click **Detection**.

**To review the events from the defender sensors, complete the following steps:**

1. On the **Detection** dashboard, go to the **Detection events** section.
2. Events can be viewed in the included table with the following columns:
  - Time – shows the time when an event is generated from a connected source.
  - Source – shows the connected source type that generated the event.

**Tip:** Clicking the down arrow shows the reporting sensors. For heartbeat summary events, the sensors are divided into active heartbeats and missing heartbeats. Missing heartbeats might indicate an issue with the underlying system.
  - Event – shows the type of event.

**Tip:** For Potential threat events, you can click the Eye symbol to view the full log generated by the sensor.
3. You can scroll through the list to view the events in chronological order, or use the Search option to find specific events.

**To review the list of virtual machines in the recovery group along with its FQDN and OS, complete the following steps:**

1. Click **Manage** on the **Defender sensors** tile.

**Note:** If you have not installed any sensor previously, you will see the **Get started** button on the **Defender sensors** tile.
2. Review the list of virtual machines in this recovery group along with their FQDN and operating system.

**Tip:** IBM Storage Defender sensors are supported on the following operating systems:

  - RHEL 9.0 or later version
  - SUSE 15 SP5 and later version
  - Ubuntu 24.04 LTS and later version
3. You can download this list by selecting **Download**, for your reference during Ansible configuration.
4. To close the window, click **X**.

**To review detailed documentation related to Ansible playbooks and IBM Storage Defender sensors, complete the following steps:**

1. Click **Manage** on the **Defender sensors** tile.
2. Click the **Learn more** link.

## Resources

Compared to the recovery group overview dashboard, the resources dashboard provides detailed insights on the resources settings and status. On this dashboard, you can review a current list of resources associated with the recovery group and see details for each resource such as the related vCenter, virtual machine network settings, and virtual machine storage that is used. Also, you can remove a resource from the recovery group and add new resources to the recovery group.

**To review the Recovery group dashboard to see information about one recovery group, complete the following steps:**

1. On the Data Resiliency home page, click **Recovery Groups**.
2. From the list of recovery groups, click on the Eye symbol for the recovery group that you are interested in.
3. On the Recovery group overview dashboard, go to the navigation menu and click **Resources**.

**To review resources details, complete the following steps:**

1. In the list of virtual machines on the resource page, scroll to the virtual machine of interest.  
**Tip:** Use the search bar to search a specific name or wildcard.
2. From the list of virtual machines, click on the Eye symbol for the virtual machines that you are interested in. This opens a pop-up window.
3. In the pop-up window, you can review virtual machine's specific information such as VM name, power state, vCenter details, VM folder path, and VM storage details as well as VM network details.  
In addition, you can review IBM Storage Defender specific information such as the last inventory time and the unique identifier of the resource in Defender.
4. After you have finished reviewing details, close the pop-up window by clicking the **X** button.

**To add virtual machine resources to the recovery group, complete the following steps:**

1. Click the **Add Resources** button. This opens a pop-up window.
2. In the list of connected vCenters, select the one that you are interested in.  
**Note:** All virtual machines assigned to a resource group must be located in the same vCenter.
3. Click the square button in the list of inventoried virtual machines to select the virtual machine or multiple virtual machines that you want to add to the recovery group.  
**Tip:** Use the search bar to search a specific name or wildcard.
4. Click the **Add** button to add the resources to the recovery group.  
**Tip:** A pop-up message will indicate if the resources were added to the recovery group.

**To remove virtual machine resources from the recovery group, complete the following steps:**

1. In the list of virtual machines, click on the square button to select the virtual machine that you want to remove from the resource group.  
**Tip:**
  - Use the search bar to search a specific name or wildcard.
  - Click the square button in the headline of the table to select multiple virtual machines.
2. Click the **Remove** button.

## Notification

In the Notification dashboard, you can add recipients to receive the notifications that are generated from the Data Resiliency service.

To add recipients for the notifications, complete the following steps:

1. On the Data Resiliency home page, click **Recovery Groups**.
2. From the list of recovery groups, click on the Eye symbol for the recovery group that you are interested in.
3. On the Recovery group overview dashboard, go to the navigation menu and click **Notification**.
4. On the Notification dashboard, enter the email ID of a recipient in **Email notification recipient** and press Enter.

Optionally, enter additional email addresses to invite multiple users. Press Enter after each email address.

**Note:** All the added recipients will be notified when a case is opened for the Recovery Group on any of the following events:

- Missing heartbeat message from sensor
- Anomaly detected on VM
- Possible threat detected on VM



## History

In the **History** section, you can see a log for each update that was done for the recovery group.

To review the recovery group's **History** dashboard and to see a log of all changes that were made to the recovery group, complete the following steps:

**Note:** The history includes the creation and any updates of the recovery group. The validation of an activated recovery plan process removes resources from the Recovery Group. After a validation of a recovery, you can find the list of resources that were assigned to the Recovery Group before you validated the recovery.

1. On the Data Resiliency home page, click **Recovery Groups**.
2. From the list of recovery groups, click on the Eye symbol for the one you are interested in.
3. On the recovery group's **Overview** dashboard, click the **History** section.

Find more details about the update that was done by clicking the arrow button for a point in time in the log.



## Chapter 4. Profiles

The governance and clean room profiles help to configure recovery objectives of recovery groups and recovery target environments.

### Governance profiles

The governance profiles complement the recovery group with recovery objectives. The recovery objectives are the preset point in time for the recovery points and the preset minimum retention time for the recovery points. Also, in the governance profile you can specify a threshold time that can be elapsed until the next recovery test to be performed for the recovery group. The recovery objectives can be defined for IBM Storage FlashSystem and IBM Storage Defender Data Protect independently.

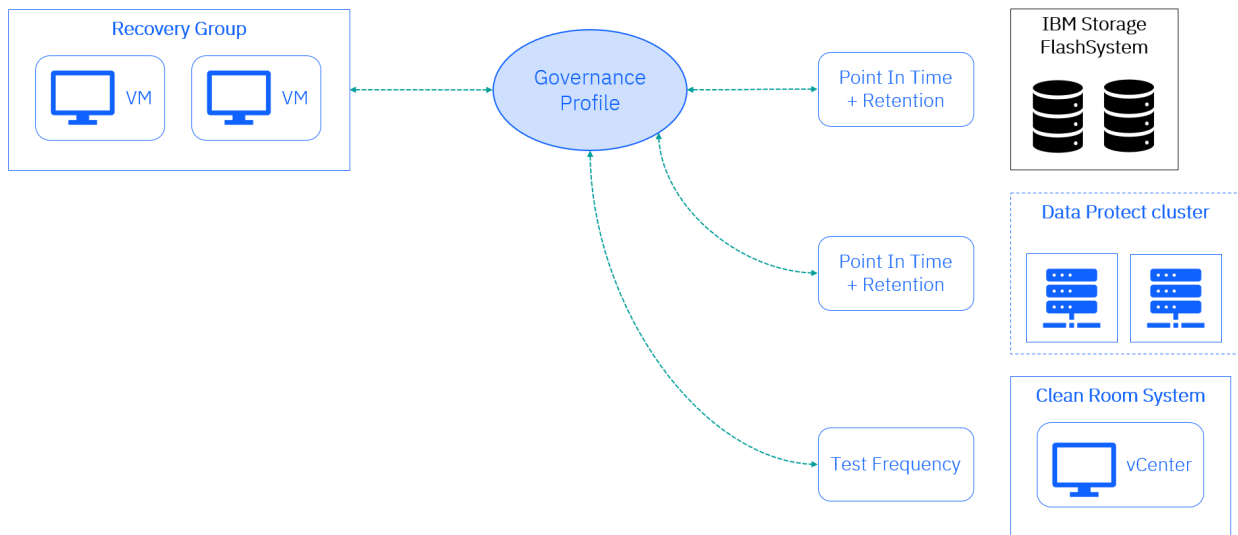


Figure 3. Recovery objectives configured in the governance profile

The governance profile definition allows one of the following three use case definitions:

- Observation of the recovery objectives for IBM Storage FlashSystem recovery points (safeguarded snapshot copies).
- Observation of the recovery objectives for IBM Storage Defender Data Protect recovery points.
- Observation of both the recovery objectives for IBM Storage FlashSystem recovery points and IBM Storage Defender Data Protect recovery points

The test frequency objective is optional for all use cases.

On the **Profiles** page, you can add, edit, or delete a governance profile by using the options in the **Governance** tab.

### Adding a governance profile

A governance profile defines the point in time and retention of recovery points. It complements the recovery group with recovery objectives. . To create one or multiple governance profiles, complete the following procedure.

#### Procedure

To add a governance profile, complete the following steps:

1. On the Data Resiliency home page, click **Profiles > Governance**.

2. To add a governance profile, click **Create Profile**. This action opens the **Create governance profile** window.
3. On the **Create governance profile** window, under the **Details** tab, enter the details for the following fields:

**Name**

Specify the name for a governance profile.

**Description**

Description of the governance profile

4. Click **Next**. Under the **Immutable snapshots** tab, you can select thresholds for immutable snapshot recovery points.

**Point in time**

- a. Select the checkbox to enable the point in time verification.
- b. Select a time unit from the drop-down list.
- c. Use the plus or minus buttons to increase or decrease the value or enter an integer value into the input box.

**Retention**

- a. Select the checkbox to enable the retention time verification.
- b. Select a time unit from the drop-down list.
- c. Use the plus or minus buttons to increase or decrease the value or enter an integer value into the input box.

5. Click **Next**. Under the **Backups** tab, you can select thresholds for backup copy recovery points.

**Point in time**

- a. Select the checkbox to enable the point in time verification.
- b. Select a time unit from the drop-down list.
- c. Use the plus or minus buttons to increase or decrease the value or enter an integer value into the input box.

**Retention**

- a. Check the checkbox to enable the retention time verification.
- b. Select a time unit from the drop-down list.
- c. Use the plus or minus buttons to increase or decrease the value or enter an integer value into the input box.

6. Click **Next**. Under the **Recovery testing** tab, you can select the threshold for recovery testing.

**Frequency**

- a. Select the checkbox to enable the test frequency verification.
- b. Use the plus or minus buttons to increase or decrease the value or enter an integer value into the input box. The value that you select or enter is the time unit in Days.

7. Click **Create** to create a governance profile with the specified values. The governance profile is created under the **Governance** tab.

## Reviewing a governance profile

You can review a governance profile to see all the settings of the governance profile.

### Procedure

To review a governance profile, complete the following steps:

1. On the Data Resiliency home page, click **Profiles > Governance**.

2. In the list of governance profiles on the **Profiles** page, scroll to the governance profile of interest.

**Tip:** Optionally, use the search bar to search a specific name or wildcard.

3. Click the table expand icon.
4. In the expanded table row, you can review all the settings of the governance profile.
5. Click the table expand icon to close the review.

## Editing a governance profile


You can edit a governance profile to update the specified values of the governance profile.

### Procedure

To edit a governance profile, complete the following steps:

1. On the Data Resiliency home page, click **Profiles > Governance**.
2. In the list of governance profiles on the **Profiles** page, scroll to the governance profile of interest.

**Tip:** Optionally, use the search bar to search a specific name or wildcard.

3. Click the overflow menu icon (  ) and select **Edit**.
4. In the sliding window, you can modify all the settings of the governance profile.

**Note:** Updates to the governance profile impacts the recovery groups that are associated with the governance profile.

5. Click **Save** to save the changes or click **Cancel** to continue with the former settings.

## Removing a governance profile


You can remove a governance profile if you no longer need a governance profile to manage resources. Removing or deleting a governance profile that is associated with any recovery groups is not possible. To delete a governance profile, you need to edit the associated recovery groups and remove all the governance profile assignments.

### Procedure

To remove a governance profile, complete the following steps:

1. On the Data Resiliency home page, click **Profiles > Governance**.
2. In the list of governance profiles on the **Profiles** page, scroll to the governance profile of interest.

**Tip:** Optionally, use the search bar to search a specific name or wildcard.

3. Click the overflow menu icon (  ) and select **Delete**.
4. To confirm the deletion of the governance profile, click **Delete** in the pop-up window.

**Note:** The deletion of a governance profile affects all recovery groups that are associated with the governance profile. If the governance profile is assigned to recovery groups, the deletion fails.

5. To cancel the deletion operation, click **Cancel**.

## Clean Room profiles

The clean room profiles connect the recovery groups that belong to resources in the production environment with resources and configuration that is defined in IBM Storage Defender Data Resiliency Service. The connected resources are IBM Storage FlashSystem, IBM Storage Defender Data Protect, and the clean room environment. The related configuration defines how IBM Storage Defender behaves for a recovery.

The following image illustrates the logical connection between the different components.

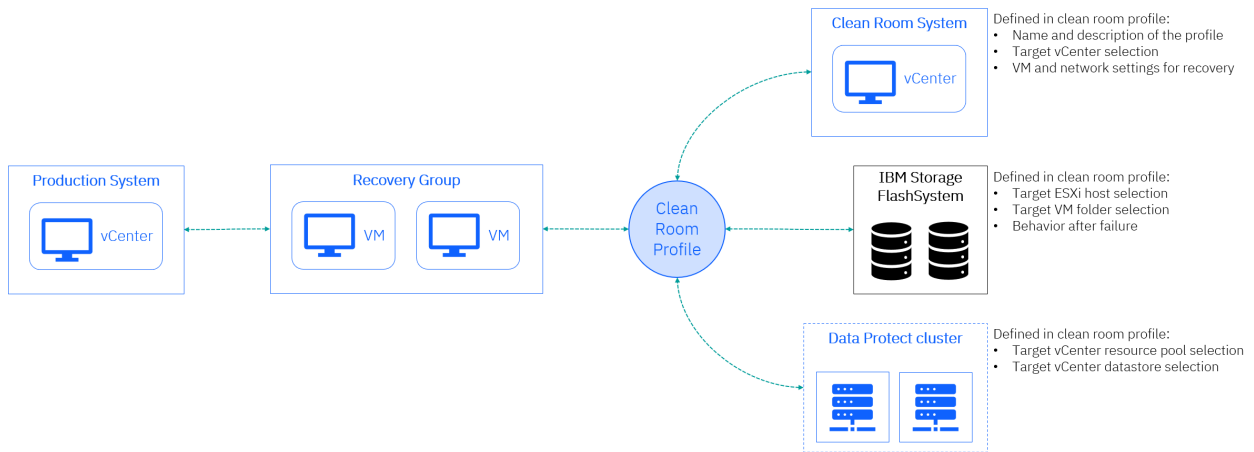


Figure 4. The role of the clean room profile in IBM Storage Defender.

To ensure the successful recovery of the recovery group that is assigned to the specific clean room profile, configuration requirements must be met. The configuration of a clean room profile allows the usage of the profile for one of the following three different use cases:

1. Recovery from IBM Storage FlashSystem safeguarded snapshots.
2. Recovery from IBM Storage Defender Data Protect backup copies.
3. Recovery from both IBM Storage FlashSystem safeguarded snapshots and IBM Storage Defender Data Protect backup copies.

**Important:** If the following requirements are not met, the recovery of the virtual machines that belong to the specific recovery group fails for clean room recoveries.

- Requirements for the recovery from IBM Storage FlashSystem
- Requirements for the recovery from IBM Storage Defender Data Protect
- Requirements for the recovery from IBM Storage FlashSystem and IBM Storage Defender Data Protect using the same clean room profile

In addition to the conceptual dependencies between the clean room profile and other IBM Storage Defender components you must consider that the same clean room profile can be reused for different recovery groups. What must be considered in such a case is that the different recovery groups may have different requirements for the recovery. Especially, when you recover from IBM Storage FlashSystem, the requirements for network infrastructure, mapping of volumes, or SAN zoning may be different. Therefore, it may be beneficial to implement multiple clean room profiles with different configurations to provide you with more flexibility for the recovery scenarios that you want to implement for different recovery groups. The following image illustrates the logical connection between the different components.

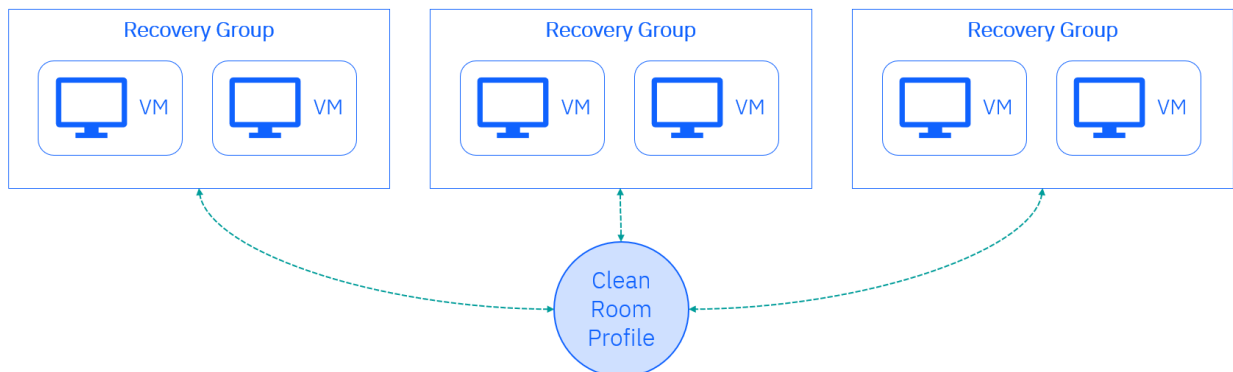


Figure 5. Reuse of the same clean room profile for multiple recovery groups

## Requirements for the recovery from IBM Storage FlashSystem

- **Network Infrastructure:** The physical and logical network infrastructure must be implemented that connects the IBM Storage FlashSystem, the production vSphere cluster, and the clean room vSphere cluster. Depending on the usage of iSCSI or Fibre Channel (FC), the environment implies Ethernet or SAN infrastructure.
- **Network Adapter:** The ESXi host systems that are used for the implementation of the clean room environment must have FC or iSCSI network adapters configured.
- **Map Volumes:** The IBM Storage FlashSystem must be configured to map the ESXi hosts. Also, the following requirements must be met:
  - A host cluster in the clean room vSphere cluster must contain host definitions for every ESXi host.
  - FC or iSCSI port definitions on IBM Storage FlashSystem must match the storage adapters on the vSphere hosts.
- **SAN Zoning:** The SAN zoning must be configured to connect the ESXi hosts and IBM Storage FlashSystem ports when the Fibre Channel protocol is used.

For the illustration of the required connectivity, see the following image.

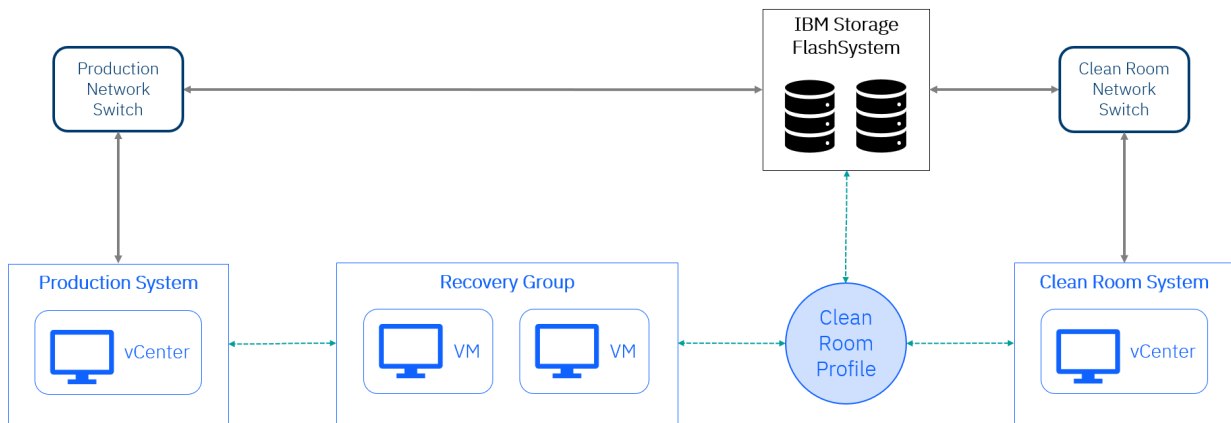


Figure 6. Illustration of the physical and logical configuration for IBM Storage FlashSystem recovery.

## Requirements for the recovery from IBM Storage Defender Data Protect

- **Network Infrastructure:** The physical and logical Ethernet network infrastructure must be implemented that connects the IBM Storage FlashSystem, the production vSphere cluster, and the clean room vSphere cluster.
- **Data Protect Configuration:** Both the production vCenter and the clean room vCenter must be registered in IBM Storage Defender Data Protect as data protection sources.

For the illustration of the required connectivity, see the following image.

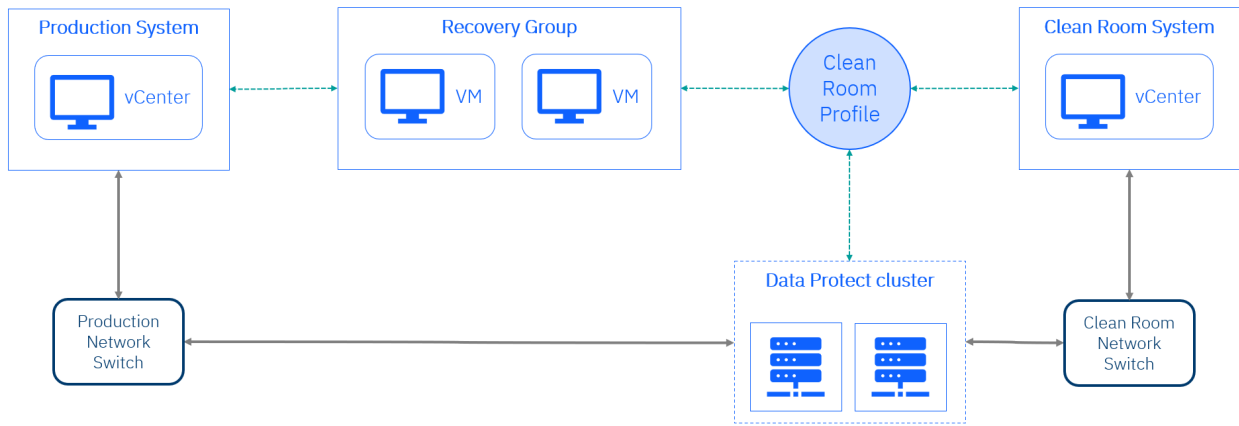


Figure 7. Illustration of the physical and logical configuration for IBM Storage Defender Data Protect recovery.

## Requirements for the recovery from IBM Storage FlashSystem and IBM Storage Defender Data Protect using the same clean room profile

**Important:** All the above requirements must be met for the recovery from both IBM Storage FlashSystem and IBM Storage Defender Data Protect.

On the **Profiles** page, you can add, edit, or delete a clean room profile by using the options in the **Clean room** tab.

## Adding a clean room profile

A clean room profile defines the target environment that can be used for recovery tests or for manual recoveries. To create one or multiple clean room profiles, complete the following procedure.

### Procedure

To add a clean room profile, complete the following steps:

1. On the Data Resiliency home page, click **Profiles > Clean room**.
2. To add a clean room profile, click **Create profile**. This action opens the **Clean room profile** window.
3. On the **Create clean room profile** window, under the **Details** tab, enter the details for the following fields:

#### Profile name

Specify the name for a clean room profile. The profile name must be unique in the context of the IBM Storage Defender tenant.

#### Description (optional)

You can provide description of the clean room profile. Use a description that is verbose enough to help you later to identify what is the intention of the profile specification and what use cases you want to implement by using the clean room profile.

4. Click **Next**. Under the **Clean room settings** tab, you can enter the clean room location and recovery preferences. The settings under this tab are global in the context of the profile and influences the recovery from IBM Storage FlashSystem and IBM Storage Defender Data Protect.

#### Clean room location

Select a location from the drop-down list to restore the data store. The list contains the vCenters that are connected to Data Resiliency. The vCenter you specify will be used as the clean room target vCenter for a recovery using this clean room profile.



### **Power state**

Toggle the **Power state** slider to switch on to allow Data Resiliency to start the virtual machine after recovery has finished.

### **Attach to network**

Toggle the **Attach to network** slider to enable network-specific settings in the profile management.

### **VM Network**

Select the virtual network from the drop-down list that can be used to attach network. When the recovery is finished, the specified network will be used for a potential network connection.

### **Start connection to the network**

Toggle the slider to specify if Data Resiliency should connect the virtual machine to the selected network after recovery and start.

### **Preserve MAC address**

Toggle the slider to specify if Data Resiliency must preserve the existing MAC address for the virtual machine or not when recovering the virtual machine and connecting to a network.

5. Click **Next**. Under the **Immutable snapshot recovery** tab, you can enter recovery preferences when recovering from immutable snapshots with IBM Storage FlashSystem.

### **Recovery setting**

Toggle the slider to switch on when you plan to recover from immutable snapshots by using this clean room profile

### **ESXi host**

Select the ESXi host from the drop-down list that can be used for the clean room profile. The cloned IBM Storage FlashSystem volume will be mapped to this host.

### **vCenter folder**

Select the vCenter VM folder from the drop-down list that can be used for the clean room profile. The virtual machines that reside on the cloned IBM Storage FlashSystem volume will be recovered into this VM folder.

### **Clean up on failure**

Toggle the slider to switch on if you want to enable the automated cleanup of the infrastructure that was created from IBM Storage Defender for the recovery. The cleanup takes place when the recovery fails.

6. Click **Next**. Under the **Backup recovery** tab, you can enter recovery preferences when recovering from IBM Storage Defender Data Protect.

### **Recovery settings**

Toggle the slider to switch on when you plan to recover from backup.

### **Data Protect resource pool**

Select the vSphere resource pool from the drop-down list that can be used for recovery. The default resource pool on each vCenter is the pool that is called Resources. In addition, you can have other resource pools that you have created in your vCenter. All available resource pools can be used for the recovery.

### **vCenter datastore**

Select the vCenter datastore from the drop-down list that can be used for recovery.

7. Click **Create** to create a clean room profile with the specified values. The clean room profile is created under the **Clean room** tab.


## Reviewing a clean room profile

### Procedure

To review a clean room profile, complete the following steps:

1. On the Data Resiliency home page, click **Profiles > Clean room**.
2. In the list of clean room profiles on the resource page, scroll to the clean room profile of interest.

**Tip:** Use the search bar to search a specific name or wildcard.

3. Click the overflow menu icon (  ) and select **View details**.
4. In the sliding window, you can review all the settings of the clean room profile.
5. Click the **X** button to close the review.

## Editing a clean room profile


You can edit a clean room profile to update the specified values of the clean room profile.

### Procedure

To edit a clean room profile, complete the following steps:

1. On the Data Resiliency home page, click **Profiles > Clean Room**.
2. In the list of clean room profiles on the resource page, scroll to the clean room profile of interest.

**Tip:** The search input allows searching a specific name or wildcard.

3. Click the overflow menu icon (  ) and select **Edit**.
4. In the sliding window, you can modify all the settings of the clean room profile.

**Note:** Updating the clean room profile impacts the recovery groups that are associated with the clean room profile. Automated test recoveries might behave differently after the clean room profile is modified.

5. Navigate to the end of the wizard and click **Save** to save the changes. Optionally, click **Cancel** at any time during the wizard to continue with the former settings.

## Removing a clean room profile


You can remove a clean room profile if you no longer need a clean room profile to manage resources.

### Procedure

To remove a clean room profile, complete the following steps:

1. On the Data Resiliency home page, click **Profiles > Clean room**.
2. In the list of clean room profiles on the resource page, scroll to the clean room profile of interest.

**Tip:** The search input allows searching a specific name or wildcard.

3. Click the overflow menu icon (  ) and select **Delete profile**.  
If the clean room profile is assigned to one or more recovery groups a pop-up window appears informing you about this. Click **X** to confirm and close the pop-up window.

---

## Chapter 5. Resources

The resources section in Data Resiliency helps you create connection managers, define and manage clean room profiles, and view the added resources.

### Adding a connection manager

---

To add more resources in Data Resiliency, you must add a connection manager to connect multiple locations.

#### Procedure

To add a connection manager, complete the following steps:

1. On the Data Resiliency home page, click **Resources**.
2. Click the **Actions** button. This action opens a context menu. In the context menu, complete the following steps:
  - a. Click **Download Connection Manager**. This action starts to download the OVA file that contains the Connection Manager software to your configured local download folder.
  - b. Click **Generate Connection Token**. This action generates a unique connection token that you can use to connect the installed Connection Manager to Data Resiliency later in the process. Save the token.
3. Follow the steps that are documented in [“Connecting Data Resiliency to on-premises resources” on page 37](#) to complete the setup.

### Reviewing available resources

---

You can review resources that are added in Data Resiliency from the **Resources** page.

#### Procedure

To review available resources, complete the following steps:

1. On the Data Resiliency home page, click **Resources > Available resources**.
2. In the list of available resources on the **Resources** page, scroll to the resource of interest.
3. Alternatively, use the search option to reduce the list to a specific group of resources.
  - a. In the search field, enter a resource name or partial resource name.
  - b. Click **Done** to apply the search.

### Reviewing connections

---

On the **Connections** page, you can review data sources and recovery locations that are available.

#### Reviewing data sources

To review available data sources, complete the following steps:

1. On the Data Resiliency home page, click **Resources > Connections**.
2. In the list of available data sources on the **Connections** page, scroll to the data source of interest.
3. Alternatively, use the search option to reduce the list to a specific group of data sources.
  - a. In the Search field, enter a data source name or partial data source name.
  - b. The list of data sources is adjusted and reduced automatically.

Alternatively, use the following filter options to reduce the list to a specific group of connection. In the Search field, click the filter button on the right side. The filter options are cumulative.

#### **Status**

1. Click on the drop-down list icon to open the list or options.
2. Click the square button to select the Success option.

#### **Type**

1. Click on the drop-down list icon to open the list or options.
2. Click the square button to select one option. The options are Data Protect, IBM FlashSystem, or VMware.

#### **Connection Manager**

1. Click on the drop-down list icon to open the list or options.
2. Click the square button to select one option. The options list is the list of connection manager systems connected to Data Resiliency.

Click **Done** to apply the filter settings.

### **Reviewing recovery locations**

To review available recovery locations, complete the following steps:

1. On the Data Resiliency home page, click **Resources > Connections**.
2. In the list of available recovery locations on the connections page, scroll to the recovery location of interest.
3. Alternatively, use the search option to reduce the list to a specific group of recovery locations
  - a. In the Search field, enter a recovery location name or partial recovery location name.
  - b. The list is adjusted automatically.

Alternatively, use the following filter options to reduce the list to a specific group of connections. In the Search field, click the filter button on the right side. The filter options are cumulative.

#### **Status**

1. Click on the drop-down list icon to open the list or options.
2. Click the square button to select the Success option.

#### **Type**

1. Click on the drop-down list icon to open the list or options.
2. Click the square button to select one option. The options are Data Protect, IBM FlashSystem, or VMware.

#### **Connection Manager**

1. Click on the drop-down list icon to open the list or options.
2. Click the square button to select one option. The options list is the list of connection manager systems connected to Data Resiliency.

Click **Done** to apply the filter settings.

## **Reviewing the connection managers**

---

### **Procedure**

To review the available connection managers, complete the following steps:

1. On the Data Resiliency home page, click **Resources > Connection Manager**.

2. In the list of available locations on the **Connection Manager** page, scroll to the location of interest.
3. Alternatively, use the search option to reduce the list to a specific group of locations.
  - a. In the Search field, enter a location name or partial location name.
  - b. The list is adjusted and reduced automatically.



---

## Chapter 6. Integrations

The integrations section in Data Resiliency helps you to integrate various capabilities.

By using the integrations, administrators can add or remove various integration tools, such as QRadar SIEM and enable or disable email notifications. To add or remove tools, click **Data Resiliency > Integrations** on the IBM Storage Defender Data Resiliency home page.

**Important:** IBM Security QRadar SIEM and Email notifications are not available with the trial plan. Contact sales if you wish to utilize these features.

### Value-add of IBM Storage Defender integration

- Empower security analysts to view storage related incidents on their existing Security Operation Center (SOC) dashboard.
- Ensure that the incidents are more actively monitored as compared to the IBM Storage Defender UI.

The following IBM Storage Defender events are sent to QRadar:

- Alerts for any threats received from IBM Storage Defender sensor.
- Events such as missed heartbeat from IBM Storage Defender sensor.

---

## Integrating Data Resiliency to QRadar SIEM

You can integrate QRadar SIEM to detect, analyze, and respond to security threats before they harm business operations. Integrating IBM Storage Defender Data Resiliency Service with QRadar SIEM helps you to improve the coverage of your organization's cybersecurity.

- Refer to the link to download QRadar extension from IBM Security App Exchange portal:

[IBM Security APP Exchange](#)

- Refer to the link for QRadar extension guide:

[QRadar Extension User Guide](#)

Complete the following steps to connect Data Resiliency to QRadar.

1. Login to IBM Storage Defender console.
2. Click the hamburger menu on the upper-left of the page.
3. Click **Data Resiliency > Integrations**.
4. Click the IBM Security QRadar SIEM.
5. Click **Add connection**.
6. Specify the SIEM host and TCP port for the connection to IBM Storage Defender and the associated Connection Manager.

**Note:** Select a TCP port in the range between 0 to 65535, except for port 5000, which is not allowed.

Wait for few minutes to get the connection added. On successful connection, the status becomes active.

**Note:** When a Connection Manager is already associated with a QRadar SIEM host, users are not allowed to use the same Connection Manager to add another SIEM host. In that case, use a different Connection Manager.

**Note:** When a virtual machine does not have an IP address, then the source IP address of an event in QRadar is assigned the IP address of Connection Manager, which was previously added as a log source. If a virtual machine does not have a hostname associated, the dvc field in the event payload maps to the Name of the virtual machine.

## Actions for IBM Storage Defender events

### Steps for a potential threat:

1. Login to IBM Storage Defender console.
2. On the Data Resiliency home page, click **Recovery Groups**.
3. Select the recovery group from which you received the SIEM event.
4. On the **Recovery Group Protection** dashboard, complete the following steps:
  - a. Select the appropriate recovery point and click **Activate recovery plan** if required.
  - b. Select the clean room profile that you want to use.
  - c. Click **Done**.
  - d. Wait for the recovery to complete.
  - e. Validate the resources are working as expected and then use the recovery point for production restore.

### Steps for a missed heartbeat:

1. Login to IBM Storage Defender console.
2. On the Data Resiliency home page, click **Recovery Groups**.
3. Select the recovery group from which you received the SIEM event.
4. Go to **Open case** tab. View the virtual machine hostname for the **Missed heartbeat** event in the **Timeline** section.
5. Login to the virtual machine that has the missed heartbeat event, and run the following command to verify that the sensor is working properly:

```
systemctl status defender-sensor
```

A sample output of the command is shown as follows:

```
defender-sensor.service - IBM Storage Defender Sensor service
  Loaded: loaded (/usr/lib/systemd/system/defender-sensor.service; enabled; preset:
disabled)
  Active: active (running) since Wed 2024-05-15 17:42:44 MST; 3h 47min ago
    Main PID: 1326 (defender-sensor)
      Tasks: 3 (limit: 48928)
     Memory: 291.9M
        CPU: 50.419s
    CGroup: /system.slice/defender-sensor.service
            └─1326 /usr/bin/bash /usr/bin/defender-sensor
              └─1327 /opt/ibm/defender/venv/bin/python3 -m espial.monitor

May 15 17:42:44 skrill-vm7.storage.tucson.ibm.com systemd[1]: Starting IBM Storage Defender
Sensor service...
May 15 17:42:44 skrill-vm7.storage.tucson.ibm.com systemd[1]: Started IBM Storage Defender
Sensor service.
May 15 17:42:50 skrill-vm7.storage.tucson.ibm.com defender-sensor[1327]: 2024-05-15
17:42:50,098 INFO: Starting version 2.0.4-1713905626
May 15 17:42:50 skrill-vm7.storage.tucson.ibm.com defender-sensor[1327]: 2024-05-15
17:42:50,142 INFO: Config file: /etc/opt/ibm/defender/defender-sensor.conf
May 15 17:42:50 skrill-vm7.storage.tucson.ibm.com defender-sensor[1327]: 2024-05-15
17:42:50,533 INFO: Configured file systems: ['all']
May 15 17:42:50 skrill-vm7.storage.tucson.ibm.com defender-sensor[1327]: 2024-05-15
17:42:50,534 INFO: Discovered file systems: ['/', '/boot', '/boot/efi', '/data', '/home>
May 15 17:42:50 skrill-vm7.storage.tucson.ibm.com defender-sensor[1327]: 2024-05-15
17:42:50,534 INFO: File systems to monitor: ['/', '/boot', '/boot/efi', '/data', '/home>
May 15 17:42:50 skrill-vm7.storage.tucson.ibm.com defender-sensor[1327]: 2024-05-15
17:42:50,535 INFO: Monitoring file systems: ['/', '/boot', '/boot/efi', '/data', '/home>
May 15 17:42:51 skrill-vm7.storage.tucson.ibm.com defender-sensor[1327]: 2024-05-15
17:42:51,093 INFO: Authenticating to server
May 15 17:42:52 skrill-vm7.storage.tucson.ibm.com defender-sensor[1327]: 2024-05-15
17:42:52,521 INFO: Initialization complete
```



## Enabling email notification

---

Enable users to add email recipients for event notification for each recovery group.

**Tip:** If the option is enabled, all recipients mentioned in the recovery group are notified about IBM Storage Defender case open events. When this option is not enabled, no recipient is notified, even if recipients are present in the recovery group.

For more information, see [Notification](#).



---

## Chapter 7. IBM Storage Defender Connection Manager

From Data Resiliency, the IBM Storage Defender Connection Manager (Connection Manager) is used to connect your local primary and secondary data environment and your Data Protect cluster to Data Resiliency.

Connection Manager is used to access your local environment and to do inventory operations and also to do test recovery and recovery operations by using Data Resiliency.

The Connection Manager is provided in OVA format and can be deployed in your local VMware vCenter. Inside the Connection Manager, Red Hat® Enterprise Linux® is used as the operating system. The Connection Manager software was built to require less configuration to become active and get connected to your local resources and the IBM Storage Defender Data Resiliency Service that runs in the cloud.

---

### Connecting Data Resiliency to on-premises resources

By downloading and installing Connection Manager, you can connect Data Resiliency to your on-premises resources.

#### Before you begin

Download the Connection Manager by completing the following steps:

1. Log in to IBM Storage Defender.
2. Click the hamburger menu on the upper left corner of the page.
3. Click **Data Resiliency > Resources**.
4. Click the drop-down menu on the upper right corner of the page.
5. Click **Download Connection Manager**. This action starts the download of the OVA file that contains the Connection Manager software to your configured local download folder.
6. Click **Generate Connection Token**. This action generates a unique connection token, that token you can use to connect the installed Connection Manager to Data Resiliency later in the process. Save the token.

**Note:** The generated connection token is valid only for 30 minutes. If you do not have time to download and deploy the OVA software before the token expires, you must generate the token again.

#### Considerations

Consider the following points listed when deploying multiple Connection Managers:

**Tip:** Typically, only one Connection Manager should be deployed at each physical location. Data sources must be registered to the Connection Manager, which is local to the same physical location.

- All related data sources that belong to a particular recovery group must be registered to the same Connection Manager (VMware vCenter, IBM Storage FlashSystem, IBM Storage Defender Data Protect, and recovery locations).
- If you register the relevant data sources to a different Connection Manager, the restore to a clean room operation can result in issues such as failures.
- When upgrading a Connection Manager, use the specified backup and restore methods to retain the registered data sources. For more information, see [“Backing up and restoring Connection Manager” on page 55](#).
- If a Connection Manager is completely destroyed and there is no backup to restore, some of the dependencies in recovery groups will be lost. In such a case you are required to archive the recovery group and re-create the recovery group. And then, complete the deployment of a Connection Manager to register the same data sources that belongs to the recovery group.

## Procedure

To connect Data Resiliency to on-premises resources, complete the following procedure:

1. To ensure the OVA that you deploy is a recognized trusted source, download and install the certificate chain by completing the following steps:
  - a) Extract the root certificate directly from DigiCert. The DigiCert Trusted Root G4 certificate can be used to validate the OVA code signed image.
  - b) Download the DigiCert Trusted Root G4 certificate in .pem format at <https://cacerts.digicert.com/DigiCertTrustedRootG4.crt.pem>.
  - c) Install the certificate chain into your VMware vCenter Certificate Management.
  - d) Log in to the vCenter by using the VMware administrator account.
  - e) Navigate to **Administration > Certificate Management**.
  - f) Locate Trusted Root Certificates and click the **Add** link to add the downloaded certificate.
  - g) After the certificate is added, you can import the IBM Storage Defender Connection Manager OVA.
2. Install the Connection Manager by completing the following steps:
  - a) Store the Connection Manager OVA file on a shared folder that can be read from your vCenter.
  - b) Log in to your vCenter and create a new virtual machine by using the OVA file.
  - c) While creating the virtual machine, follow the setup instructions of the vCenter to configure the network settings for the Connection Manager.
3. Update the default SSH password of the Connection Manager.
  - a) Log in to the newly created Connection Manager virtual machine by using SSH.
  - b) The default username is **defender** and the default password is **IbmStorage**.
  - c) Update the default password.
  - d) Log out.
4. Connect the Connection Manager to Data Resiliency by completing the following steps:
  - a) Navigate to the user interface of the Connection Manager through `https://<host name used for the OVA deployment>/`.
  - b) Enter a name for the Connection Manager. This name is used to identify the connection manager location in your IBM Storage Defender account.

**Tip:** You can change the name later.
  - c) Click **Continue**.
  - d) Enter the **Connection Token** for the Connection Manager. This token is the token that you generated in the Data Resiliency interface [step](#).

**Note:** The generated connection token is valid only for 30 minutes. If you do not have time to download and deploy the OVA software before the token expires, you must generate the token again.
  - e) Click **Connect account**.
  - f) In the user interface of the Connection Manager, enter the username and the initial password for the first user in the appropriate input fields.

**Tip:** You can use a functional user for this operation to ensure that the administration of the Connection Manager is not bound to a personal user in your company.
  - g) Either capture the presented QR code or cut and paste the 32-character alphanumeric code into your authenticator app to setup 2-factor authentication.
  - h) Follow the instructions in your authenticator app and enter the 6 digit code from the app into Connection Manager.
5. Allow the Connection Manager to automatically updating the **Connection Certificate** by completing the following step:

- a) Log out of the user interface.
- b) Wait 5 minutes.
- c) Log in to the user interface.

**Note:** This step is required for a newly deployed Connection Manager either for a new setup or a replacement of an existing Connection Manager . If the Connection Certificate is not updated, the installation or uninstallation of the sensor control node by using IBM Storage Defender Data Resiliency Service internal control node will fail.

## Logging in to the user interface

---

You can log in to the user interface of the Connection Manager to complete the operations such as manage your profile, data sources, recovery locations, and change settings.

### Procedure

To log in to the user interface of the Connection Manager, complete the following steps:

1. Navigate to the user interface of the Connection Manager through `https://<host name used for the OVA deployment>/`.
2. Enter the username and password.
3. Click **Log in** to proceed.

**Note:** If you are logging in for the first time, enable two-factor authentication by either capturing the QR code or cut and paste the 32-character alphanumeric code into your authenticator app.

4. Follow the instructions in your authenticator app and enter the 6 digit code from the app into Connection Manager.

## Managing a Connection Manager profile

---

In the Connection Manager user interface, you can view the profile, update the profile details, and manage password for the Connection Manager profile.

Log in to the Connection Manager that you want to manage. For login information, see [“Logging in to the user interface” on page 39](#).

On the home page of the Connection Manager, click on the profile icon to see the following options in the drop-down list:

- [“Profile” on page 39](#)
- [“Update password” on page 39](#)
- [“Log out” on page 39](#)

### Profile

In the **Profile** pop-up window, you can view your basic information and credentials for the Connection Manager.

### Update password

In the **Update password** pop-up window, you can update your password. To update your password, you must specify the current password and then specify the new password that you want to set.

### Log out

When you have made updates and saved the changes in the profile, you can log out from the user interface by clicking the **Log out** option.

## Connecting to data sources, recovery locations, and sensors

---

IBM Storage Defender can connect to different types of data sources and recovery locations. The data sources and recovery location that you connect to the IBM Storage Defender Connection Manager is inventoried automatically. Sensors observe the systems on which they are installed and can detect cyberattacks like ransomware attacks in real time, and sends you the alert messages.

### Data sources

IBM Storage Defender can connect to different data sources like data protection solutions and hypervisors. The resource that you connect to the IBM Storage Defender Connection Manager is inventoried automatically. The inventory metadata is transferred to the IBM Storage Defender Data Resiliency Service.

Review [“Appendix: Inventory metadata that is collected from Data Resiliency”](#) on page 58 to understand what metadata is collected from your environment. In general, all metadata that is collected is always encrypted while processing, transit, and also at rest.

### Adding data sources

You can add different data sources to IBM Storage Defender Connection Manager to help you define, plan, test, secure, and recover your data using the IBM Storage Defender Data Resiliency Service.

To add data sources, complete the following steps:

1. Log in to the connection manager of interest.
2. On the home page of the Connection Manager, click **Connections**.
3. Click **Data Sources**.
4. Click **Add connection**.
5. In the drop-down list, select **Data source**. This operation opens a dialog.

**Tip:** If no data source was added to the list of connections, You can click **Add a data source** in the data sources table. This operation opens a dialog.

6. In the dialog, select the type of data source that you want to add. You can select any of the following data source types:

- IBM FlashSystem

**Note:** You must integrate IBM Storage Defender with IBM Storage FlashSystem for threat detection and automatically reporting alerts to IBM Storage Defender. To integrate IBM Storage Defender with IBM Storage FlashSystem, see [“Integrating IBM Storage Defender with IBM Storage FlashSystem”](#) on page 41.

- IBM Storage Defender Data Protect
- VMware vCenter

7. Click **Next**.

8. Add the IP address or the fully qualifying domain name (FQDN) of the resource that you want to connect.

9. Click **Next**. IBM Storage Defender Connection Manager connects to the resource, downloads the certificate, and displays the certificate details in the user interface.

10. Click **Next**.

**Note:** If you click **Next**, you confirm that the certificate that was downloaded from IBM Storage Defender Connection Manager is trusted.

11. Add the username and password of the cluster that you want to use to connect to the resource.

**Note:** If the cluster account is MFA enabled, then you need to log in with an API key. To get an API key, complete the following steps:

- a. On the cluster's home page, navigate to **Settings**.
  - b. Select **Access Management** and then **API Keys**.
  - c. Copy the API key and paste it in the login page.
12. Click **Add** to connect the resource.

## Integrating IBM Storage Defender with IBM Storage FlashSystem

1. Register the IBM Storage FlashSystem with IBM Storage Defender Data Resiliency Service. This registration is done in the Connection Manager user interface.
2. Register the IBM Storage FlashSystem with IBM Storage Insights Pro. When the system is registered, the IBM FlashCore Module starts reporting the detected anomalies to your IBM Storage Insights Pro tenant.

**Note:** IBM FlashCore Module version 4 technology is built in the IBM Storage FlashSystem that is used. IBM Storage Insights Pro correlates the data from multiple IBM FlashCore Modules and analyzes the data.

3. Go to IBM Storage Insights Pro and acknowledge the connection. For more information, see [Acknowledging recommended actions in IBM Storage Insights Pro documentation](#).

For more information about working principle of the IBM Storage Defender integration with IBM FlashCore Module, see [“IBM Storage FlashSystem threat detection” on page 3](#).

## Editing data sources

### Procedure

To edit data sources, complete the following steps:

1. Log in to the Connection Manager of interest.
2. On the home page of the Connection Manager, click **Connections**.
3. Click **Data Sources**.
4. In the data sources table, scroll to the data source of interest.

**Tip:** If you have many entries in the list, you can use the filter options in the table to find a data source with a specific status or a specific type.

5. Click the overflow menu.
6. In the pop-up menu, click **Edit**. This operation opens a dialog.
7. In the dialog, you can update the username and password that is used for the connection.
8. Click **Save** to save the changes.

## Removing data sources

### Procedure

To remove data sources, complete the following steps:

1. Log in to the Connection Manager of interest.
2. On the home page of the Connection Manager, click **Connections**.
3. Click **Data Sources**.
4. In the data sources table, scroll to the data source of interest.

**Tip:** If you have many entries in the list, you can use the filter options in the table to find a data source with a specific status or a specific type.

5. Click the overflow menu.
6. In the pop-up menu, click **Remove**. This operation opens a dialog.

7. Click **Remove** to confirm that you want to remove the connection.

**Note:** Removing a connection prevents the Data Resiliency Service from using it as a data source. This action affects the recovery plan of any recovery group that currently uses resources from the data source that you disconnect.

## Recovery locations

IBM Storage Defender can connect to different recovery locations like hypervisors. The recovery location that you connect to the IBM Storage Defender Connection Manager is inventoried automatically. The inventory metadata is transferred to the IBM Storage Defender Data Resiliency Service.

Review [“Appendix: Inventory metadata that is collected from Data Resiliency”](#) on page 58 to understand what metadata is collected from your environment. In general, all metadata that is collected is always encrypted while processing, transit, and also at rest.

**Note:** You must not use the production environment as a recovery location. A recovery or test recovery back to your production environment might interfere with forensic analysis in your environment.

## Adding recovery locations

### Procedure

To add recovery locations, complete the following steps:

1. Log in to the Connection Manager of interest.
2. On the home page of the Connection Manager, click **Connections**.
3. Click the **Add connection** drop-down.
4. Select **Recovery location** from the drop-down list. This operation opens a dialog box.

**Tip:** If no recovery location was added to the list of connections, you can click **Add recovery location** in the empty recovery location table. This operation opens a dialog.

5. In the dialog box, add the IP address or the fully qualifying domain name (FQDN) of the recovery location that you want to connect.
6. Click **Next**. IBM Storage Defender Connection Manager connects to the resource, downloads the certificate, and displays the certificate details in the user interface.
7. Click **Next**.

**Note:** If you click **Next**, you confirm that the certificate that was downloaded from IBM Storage Defender Connection Manager is trusted.

8. Add the username and password of the identity that you want to use to connect to the recovery location.
9. Click **Add** to connect the resource.

## Editing recovery locations

### Procedure

To edit recovery locations, complete the following steps:

1. Log in to the connection manager of interest.
2. On the home page of the Connection Manager, click **Connections > Recovery Locations**.
3. In the Recovery Locations table, scroll to the recovery location of interest.

**Tip:** If you have many entries in the list, you can use the filter options in the table to find a recovery location with a specific status or a specific type.

4. Click the overflow menu.
5. In the pop-up menu, click **Edit**. This action opens a dialog box.



6. In the dialog box, you can update the name of the connection. Also, you can update the username and password that is used for the connection.
7. Click **Save** to save the changes.

## Removing recovery locations

### Procedure

To remove recovery locations, complete the following steps:

1. Log in to the Connection Manager of interest.
2. On the home page of the Connection Manager, navigate to **Connections > Recovery Locations**.
3. In the Recovery Locations table, scroll to the recovery location of interest.

**Tip:** If you have many entries in the list, you can use the filter options in the table to find a recovery location with a specific status or a specific type.

4. Click the overflow menu.
5. In the pop-up menu, click **Remove**. This action opens a dialog box.
6. Click **Remove** to confirm that you want to remove the connection.

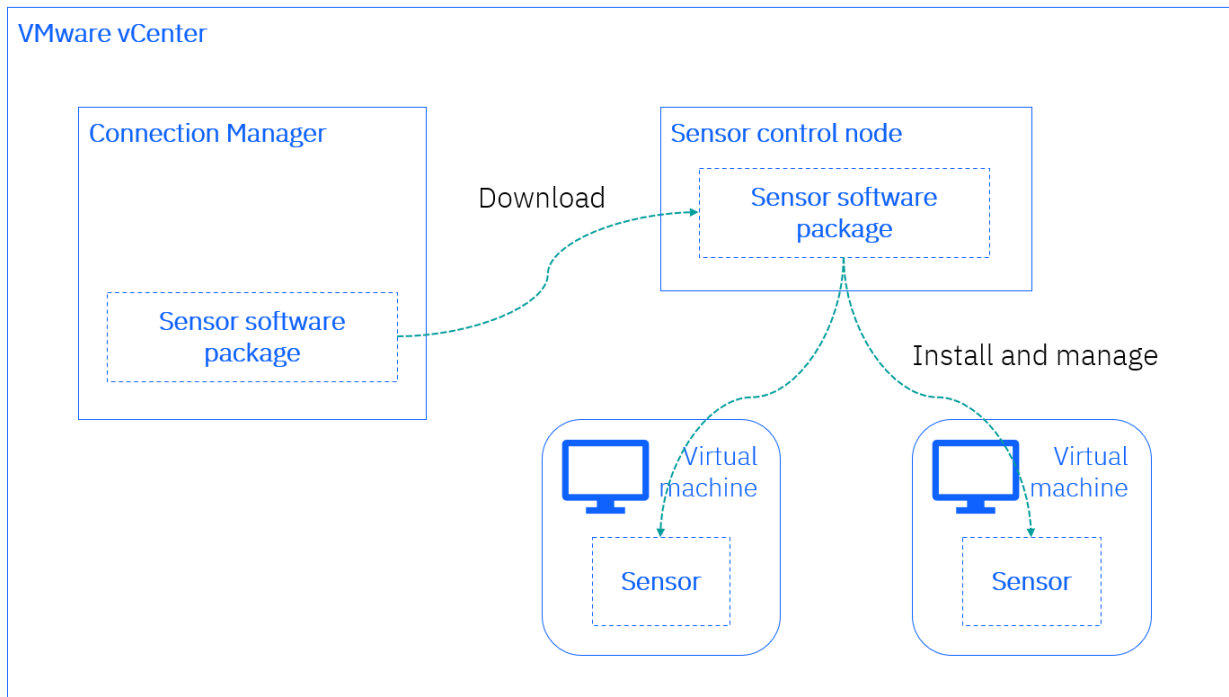
**Note:** Removing a connection prevents the Data Resiliency service from using it as a recovery location. This action affects the recovery plan of any recovery group that currently uses resources from the data source that you disconnect. The result is that no scheduled or manual recovery tests can be processed.

## Sensor control nodes

IBM Storage Defender implements the concept of sensor control nodes. The sensor control nodes are used to host the sensor management systems. The sensor management systems are used for sensors that get installed on resources like virtual machines.

The sensor control node hosts the sensor software and distributes it to the virtual machines that have the sensor installed. These sensors observe the systems that they are installed on and can detect cyberattacks like ransomware attacks in real time. When the sensor detects cyberattacks, the sensor alerts you by sending messages to the on-premises Connection Manager and IBM Storage Defender Data Resiliency Service.

The following drawing illustrates the sensor control architecture:



## Requirements for IBM Storage Defender sensor control node

IBM Storage Defender Sensor control node requires the following software:

### Ansible Playbook Software

- Ensure the availability of Ansible playbook software (command: **ansible-playbook**).
- Ansible collection `Community.General` should be installed.

### Red Hat Enterprise Linux Server 9

The control node should be running on Red Hat Enterprise Linux Server 9.

## Installing the sensor control software

### Before you begin

**Tip:** To review the system requirements, see [“Requirements for IBM Storage Defender sensor control node”](#) on page 44.

Download the IBM Storage Defender sensor control software by completing the following steps:

1. Log in to the system that you want to use as a sensor control node.
2. From that system, log in to the Connection Manager of interest.
3. On the home page of the Connection Manager, click **Connections**.
4. Click **Sensor control nodes**.
5. Click **Download package**.

### Procedure

Install the sensor control software on the sensor control node by completing the following steps:

1. Log in to the system that you want to use as a sensor control node.
2. Copy the sensor download package to a working directory.

3. Unpack the .tar software package that you downloaded.
4. In the newly created directory, run the **setup.sh** shell script.

The script requires the following input values:

**Hostname**

FQDN of the Connection Manager.

**Username**

Define a username that is to be used to register IBM Storage Defender sensors that are installed on virtual machines for the sensor control node.

**Password**

Define a password that is related to the username.

**Vault password**

The username and password that is defined before is stored and encrypted in a local Ansible vault. This password is used to protect the access to the vault.

## What to do next

Register a sensor control node. For more information, see [“Adding a sensor control node” on page 45.](#)

## Adding a sensor control node

### Before you begin

**Note:** Before you can register the sensor control node, you must install the sensor control software on the sensor control node. For more information, see [“Installing the sensor control software” on page 44.](#)

### Procedure

To add a sensor control node to the Connection Manager, complete the following steps:

1. Log in to the Connection Manager of interest.
2. On the home page of the Connection Manager, click **Connections**.
3. Click **Sensor control nodes**.
4. Click **Add control node**. This action opens a dialog box.
5. In the dialog box, enter the FQDN of the sensor control node.
6. Click **Next**
7. Enter the username that is defined when you installed the sensor control software on the sensor control node.

**Important:** Multiple sensor control nodes can use the same username and password for sensor installation or registration. In this case, only one control node needs to be added through the steps listed above. If you attempt to add more than one control node using the same username, the following error will occur in the UI:

Error getting source native ID: User name already in use. Please select a different user name.

8. Enter the password of the user.
9. Click **Add**.

## Removing a sensor control node

### Procedure

To remove a sensor control node from the Connection Manager, complete the following steps:

1. Log in to the Connection Manager of interest.

2. On the home page of the Connection Manager, click **Connections > Sensor control nodes**.
3. In the table that lists all the sensor control nodes, scroll to the sensor control node of interest.
4. In the row of the sensor control node, click the overflow menu, and then click **Remove**. This action opens a dialog box.
5. In the dialog box, click **Remove** to confirm that you want to remove the sensor control node from the Connection Manager.

**Note:** The operation does not remove the sensor control software from the sensor control node.

## Requirements for IBM Storage Defender sensors

Before proceeding to install and register IBM Storage Defender Sensor, ensure that your system meets the following requirements in terms of supported operating systems and necessary software packages:

### Supported Operating Systems

IBM Storage Defender Sensor is compatible with the following operating systems:

- Red Hat Enterprise Linux Server 9
- SUSE Linux Enterprise Server 15 SP5
- Ubuntu 24.04 LTS

### Requirements for IBM Storage Defender sensor node

#### Red Hat Enterprise Linux Server 9

Required packages:

- bash
- kernel 5.9 or later version
- libgomp
- python3

#### SUSE Linux Enterprise Server 15 SP5

Required packages:

- bash
- kernel 5.9 or later version
- libgomp1
- python311

**Note:** To install python311, the Python3 module must be enabled. For details on enabling modules, refer to the SUSE Linux Enterprise Server documentation.

#### Ubuntu 24.04 LTS

Required packages:

- bash
- libgomp1
- linux-image-generic 5.9 or later version
- python3

## Installing an IBM Storage Defender sensor

You can install an IBM Storage Defender sensor on one or multiple systems by using UI or CLI. The sensors observe the systems that they are installed on and can detect cyberattacks like ransomware attacks in real time.

## ***Installing an IBM Storage Defender sensor by using UI***

You can install the sensor on one or multiple systems directly in IBM Storage Defender UI.

### **Before you begin**

#### **Note:**

- To review the system requirements, see [“Requirements for IBM Storage Defender sensors” on page 46](#).
- The procedure that is described in this topic is not applicable for external sensor control nodes. You must add only an internal sensor control node with the following procedure: [“Adding a sensor control node” on page 45](#).

### **Procedure**

To install an IBM Storage Defender sensor on one or multiple systems, complete the following steps:

1. Log in to IBM Storage Defender.
2. Click the hamburger menu on the upper left corner of the page.
3. Click **Data Resiliency > Recovery Groups**.
4. From the list of recovery groups, click the row in the table for the recovery group that you are interested in.
5. In the **Overview** panel, navigate to the **Defender sensors** tile and click the **Get started** button.

**Note:** If you have previously installed sensors, you will see the **Manage** button on the **Defender sensors** tile.

6. On the **Manage sensors** pop-up window, select one or multiple VMs to add sensors by clicking the checkbox.

#### **Note:**

- The Connection Manager uses FQDNs of the VMs for sensor installation or uninstallation operations. Therefore the IBM Storage Defender sensor installation UI does not allow the selection of the following VMs:

- VMs with no FQDN
- VMs with localhost set as the FQDN
- VMs with identical FQDNs

Any changes on the VMs network configurations will be reflected in the UI after the next automatic or manually-triggered inventory scan. The automatic inventory scan interval is one hour.

- Sensors are supported only for VMs that are running on the following operating systems:

- RHEL 9.0 or later version
- SUSE 15 SP5 and later version
- Ubuntu 24.04 LTS and later version

7. Click **Add sensor +** in the title bar.
8. Enter either a username and password, or the SSH key to access the virtual machine.

**Note:** All the selected VMs must have the same login credentials.

9. Press **Add Sensor** to submit the installation request.
10. The state of selected VMs will change to **Installing** before showing the final result of the installation.

**Note:** Monitor the Notification menu to check for completed or failed notifications for each sensor. If the status is TIMEOUT, the installation request was accepted but did respond for 15 minutes. For the FAILED status, check the detailed error message in the notification.

## Results

After you finish the installation, the sensor automatically starts to monitor file access activities on the system. When the sensor detects any abnormal access patterns that resemble ransomware attacks, the sensor sends alert messages to the on-premises Connection Manager. The Connection Manager then forwards these alerts to the IBM Storage Defender Data Resiliency Service (DRS) through a secure connection. Also, the sensor sends heartbeat messages to the DRS through the Connection Manager periodically to indicate that the sensor is running normally.

## Installing an IBM Storage Defender sensor by using CLI

You can install an IBM Storage Defender sensor on one or multiple systems by using UI or CLI. The sensors observe the systems that they are installed on and can detect cyberattacks like ransomware attacks in real time.

## Before you begin

**Note:** To review the system requirements, see [“Requirements for IBM Storage Defender sensors” on page 46.](#)

## Procedure

To install an IBM Storage Defender sensor on one or multiple systems, complete the following steps:

1. Log in to the system that you use as a sensor control node.
2. Switch to the working directory of the sensor control software.

**Remember:** This directory is the same directory that you specified to download and install the sensor control software.

3. Create an inventory file that contains the FQDN of all systems that you want to equip with a sensor.
  - a) Edit the `/etc/ansible/hosts` file.

**Tip:** You can use a different file to build the inventory. If you use a different file for the inventory, specify the argument `-i /your-directory/your-file` in the **ansible-playbook** command in the next step.

- b) Add the FQDN of all systems that you want to equip. Add one per line under the tag `[defender_sensor_hosts]`.

**Tip:** Use the following template (in INI format) that includes the FQDNs of the IBM Storage Defender sensor hosts in the `/etc/ansible/hosts` file or alternative Ansible hosts inventory file.

```
[defender_sensor_hosts]
<FQDN1>
<FQDN2>
<FQDN3>

[defender_sensor_hosts:vars]
ansible_ssh_common_args='-o StrictHostKeyChecking=no'
ansible_connection=ssh
ansible_ssh_pass=<ssh password>
ansible_ssh_user=<ssh username>
```

**Tip:** If you are using an existing inventory file in YAML format, you can extend the inventory file by adding a `defender_sensor_hosts` group.

```

all:
  vars:
    ansible_connection: ssh
    ansible_ssh_user: <ssh username>
    ansible_ssh_pass: <ssh password>
    ansible_ssh_common_args: '-o StrictHostKeyChecking=no'
  children:
    defender_sensor_hosts:
      hosts:
        <FQDN1>:
        <FQDN2>:
        <FQDN3>:

```

4. Run the **ansible-playbook sensor\_install.yml --ask-vault-pass [-i <path\_to\_alternative\_inventory\_file>]** command. Press return.
5. Enter the Ansible vault password that you defined when you installed the sensor control node software, and then press return.

**Note:** If you want to prevent saving passwords in the hosts file, you can use the arguments **--ask-pass --ask-become-pass** to provide the SSH password and sudo password while running the **ansible-playbook** command.

## Results

After you finish the installation, the sensor automatically starts to monitor file access activities on the system. The sensor sends alert messages to the on-premises Connection Manager when it detects any abnormal access patterns that resemble ransomware attacks. The Connection Manager then forwards these alerts to the IBM Storage Defender Data Resiliency Service (DRS) through a secure connection. Additionally, the sensor also sends heartbeat messages to the DRS through the Connection Manager periodically to indicate that the sensor is running normally.

## Uninstalling an IBM Storage Defender sensor

You can uninstall an IBM Storage Defender sensor from one or multiple systems by using UI or CLI.

### *Uninstalling an IBM Storage Defender sensor by using UI*

You can uninstall the sensor on one or multiple systems directly in IBM Storage Defender UI.

## Before you begin

**Note:** To review the system requirements, see [“Requirements for IBM Storage Defender sensors” on page 46.](#)

## Procedure

To uninstall an IBM Storage Defender sensor on one or multiple systems, complete the following steps:


1. Log in to IBM Storage Defender.
2. Click the hamburger menu on the upper left corner of the page.
3. Click **Data Resiliency > Recovery Groups**.
4. From the list of recovery groups, click the row in the table for the recovery group that you are interested in.
5. On the recovery group's **Overview** dashboard, in the **Defender Sensors** tile, click **Manage**.
6. Select one or multiple VMs by clicking the check box for which you want to remove the sensors.

**Note:** The Connection Manager uses FQDNs of the VMs for sensor installation or uninstallation operations. Therefore the IBM Storage Defender sensor uninstallation UI does not allow the selection of the following VMs:

- VMs with no FQDN
- VMs with localhost set as the FQDN

- VMs with identical FQDNs

Any changes on the VMs network configurations will be reflected in the UI after the next automatic or manually-triggered inventory scan. The automatic inventory scan interval is one hour.

7. Click the **Remove Sensor**  button in the title bar.
8. Enter either a username and password, or the SSH key to access the virtual machine.

**Note:** All selected VMs must have the same login credentials.

9. Click **Remove Sensor** to submit the uninstall request.
10. Check the state of VMs that change to **Uninstalling**.

**Tip:** Monitor the Notification menu to check for completed or failed notifications for each sensor. If the status is TIMEOUT, the uninstallation request was accepted but did not respond for 15 minutes. For the FAILED status, check the detailed error message in the notification.

**Important:** If you are trying to uninstall a sensor that belongs to a Connection Manager that is destroyed or not properly backed up and restored during a Connection Manager OVA upgrade, the sensor uninstallation fails. For troubleshooting such a sensor uninstallation, see [“Resolving an IBM Storage Defender sensor uninstallation failure”](#) on page 57.

## Results

After you finish the uninstallation, the IBM Storage Defender sensor service is uninstalled from the selected VMs.

### *Uninstalling an IBM Storage Defender sensor by using CLI*

You can uninstall an IBM Storage Defender sensor from one or multiple systems by using UI or CLI.

## Procedure

To uninstall a defender sensor from a system, complete the following steps:

1. Log in to the sensor control node.
2. Create an inventory file that contains the FQDN or IP address of all systems that you want to equip with a sensor.
3. Edit the `/etc/ansible/hosts` file.

**Tip:** You can use a different file to build the inventory. If you use a different file for the inventory, specify the argument **-i /your-directory/your-file** in the **ansible-playbook** command in the next step.

4. Add the FQDN or IP address of all systems that you want to equip. Add one per line under the tag `[defender_sensor_hosts]`.
5. Run the **ansible-playbook sensor\_uninstall.yml --ask-vault-pass [-i <path\_to\_alternative\_inventory\_file>]** command. Press return.
6. Enter the Ansible® vault password.

**Important:** If you are trying to uninstall a sensor that belongs to a Connection Manager that is destroyed or not properly backed up and restored during a Connection Manager OVA upgrade, the sensor uninstallation fails. For troubleshooting such a sensor uninstallation, see [“Resolving an IBM Storage Defender sensor uninstallation failure”](#) on page 57.

## Unregistering IBM Storage Defender sensor

Typically an IBM Storage Defender sensor is uninstalled from a system by using the IBM Storage Defender sensor uninstall procedure. There might be edge cases in the management of the environment that



causes an IBM Storage Defender sensor to be uninstalled from a system, but still be registered at the sensor control node.

## About this task

**Note:** The lightweight command-line JSON processor **jq** must be installed on the sensor control node to complete the procedure.

## Procedure

To unregister a defender sensor from a sensor control node, complete the following steps:

1. Log in to the sensor control node.
2. Create an inventory file that contains the FQDN or IP address of all systems that you want to equip with a sensor.
3. Edit the `/etc/ansible/hosts` file.

**Note:** You can use a different file to build the inventory. If you use a different file for the inventory, specify the argument `-i /your-directory/your-file` in the **ansible-playbook** command in the next step.

4. Add the FQDN or IP address of all systems that you want to equip. Add one per line under the tag `[defender_sensor_hosts]`.
5. Run the **ansible-playbook sensor\_unregister.yml --ask-vault-pass [-i <path to alternative inventory file>]** command. Press return.
6. Enter the Ansible vault password.

## Access

---

## Roles in IBM Storage Defender Connection Manager

You have the following roles that you can assign to the users in IBM Storage Defender Connection Manager:

- Administrator: As an administrator, you can complete all actions, which also include assigning access to other users.
- Operator: As an operator, you can manage data sources and recovery locations.
- Viewer: As a viewer, you can view the Connection Manager, but cannot modify it.

## Users

### Adding a user to the Connection Manager

#### Procedure

To add a user to the Connection Manager, complete the following steps:

1. Log in to the Connection Manager of your interest.
2. On home page of the Connection Manager, click **Access**.
3. Click the **Add users** button. This action opens a dialog box.
4. In the **Username** field, add the email address of a user that you want to add.

**Tip:** To add more than one user at the same time, click the **Add more users** button. This action creates more **Username** fields that you can use to enter more users.

5. Select a Connection Manager role for the user or group of users.

For more information about the roles, see [“Roles in IBM Storage Defender Connection Manager”](#) on page 51.

6. In the **Initial password** field, set an initial password for the user.
7. Click the **Add users** button to complete the procedure.

**Tip:** In the list of users, your own user is marked with the **Self** tag.

## Editing the role of a user in the Connection Manager

### Procedure

To edit the role of a user in the Connection Manager, complete the following steps:

1. Log in to the Connection Manager of your interest.
2. On the home page of the Connection Manager, click **Access**.
3. Click the overflow menu.
4. In the pop-up menu, click **Edit role**. This action opens a dialog.
5. Click the radio button for the role that you want to assign to the user.
6. Click the **Save** button to finish the process.

## Removing a user from the Connection Manager

### Procedure

To remove a user from the Connection Manager, complete the following steps:

1. Log in to the Connection Manager of your interest.
2. On the home page of the Connection Manager, click **Access**.
3. Click the overflow menu.
4. In the pop-up menu, click **Remove user**. This action opens a dialog box.
5. In the dialog box, click the **Remove** button to confirm the removal of the user.

## Resetting the password of a user in the Connection Manager

### Procedure

To reset the password of a user in the Connection Manager, complete the following steps:

1. Log in to the Connection Manager of your interest.
2. On the home page of the Connection Manager, click **Access**.
3. Click the overflow menu.
4. In the pop-up menu, click **Reset password**.

## Resetting multifactor authentication of a user in the Connection Manager

### Procedure

To reset two-factor authentication of a user in the Connection Manager, complete the following steps:

1. Log in to the Connection Manager of your interest.
2. On the home page of the Connection Manager, click **Access**.
3. Click the overflow menu.
4. In the pop-up menu, click **Reset two-factor authentication**

## User roles required to connect with IBM Storage FlashSystem

To connect with IBM Storage FlashSystem, you must have either the **Security Administrator** role or **Administrator** role that is assigned to your user ID. Either of these roles provides you the permission to complete recovery operations.

## User rights required to connect with IBM Storage Defender Data Protect

To connect with IBM Storage Defender Data Protect, the **Operator** role must be assigned to the user ID. The Operator role gives the permission to the user to read all objects and metadata in IBM Storage Defender Data Protect. Also, the role gives the permission to the user to complete recovery operations.

## User rights required to connect with VMware vCenter

### Global permissions must be set to Read Only role

Users with the Read Only role for an object are allowed to view the state of the object and details about the object. For example, users with this role can view virtual machine, host, and resource pool attributes, but cannot view the remote console for a host. All actions through the menus and toolbars are not allowed.

### Propagate to children must be selected

You can assign a global permission at the root object level with **Propagate to children** selected in the vCenter identity management.

## Settings

---

## Updating the name of the Connection Manager

### Procedure

To update the name of the Connection Manager, complete the following steps:

1. Login to the Connection Manager of interest.
2. On the Connection Manager home page, click **Settings**.
3. Click the pencil button beside the Connection Manager name. This action opens a pop-up window.
4. In the **Connection Manager location** field, enter the new name.
5. Click the **Save** button to complete the process.

## Updating the Connection token of the Connection Manager

### Procedure

To update the Connection token of the Connection Manager, complete the following steps:

1. Log in to the Connection Manager of your interest.
2. On the Connection Manager home page, click **Settings**.
3. Click **Update Connection Token**. This action will open a pop-up window.
4. In the **Defender Connection Token** field, enter the new connection token.
5. Click the **Update** button to complete the process.

## Downloading support logs

You can collect the logs about your Connection Manager that might be required by IBM Support to troubleshoot or resolve issues.

### About this task

These logs should only be collected when requested by an IBM service representative and shared only with the requested representative.

### Procedure

To download logs, complete the following steps:

1. Login to the Connection Manager of interest.
2. On the Connection Manager home page, click **Settings**.
3. Click the **Download logs** button.
4. The log bundle is named as `connection-manager-logs.zip` and will be downloaded to your browser's default Download location.

## Upgrading Connection Manager

---

You can manage and protect your on-premises resources by connecting Data Resiliency to on-premises resources.

### Before you begin

Download the Connection Manager by completing the following steps:

1. Log in to IBM Storage Defender.
2. Click the hamburger menu on the upper left corner of the page.
3. Click **Data Resiliency > Resources**.
4. Click the drop-down menu on the upper right corner of the page.
5. Click **Download Connection Manager**. This action starts the download of the OVA file that contains the Connection Manager software to your configured local download folder.

### Procedure

To connect Data Resiliency to on-premises resources, complete the following procedure:

1. Back up the current Connection Manager information by using the `dabackup.sh` bash script. For more information, see [“Backing up Connection Manager” on page 55](#).
2. To ensure the OVA that you downloaded and planned to deploy is a recognized trusted source, download and install the certificate chain by completing the following steps:
  - a) Extract the root certificate directly from DigiCert. The DigiCert Trusted Root G4 certificate can be used to validate the OVA code signed image.
  - b) Download the DigiCert Trusted Root G4 certificate in .pem format at <https://cacerts.digicert.com/DigiCertTrustedRootG4.crt.pem>.
  - c) Install the certificate chain into your VMware vCenter Certificate Management.
  - d) Log in to the vCenter by using the VMware administrator account.
  - e) Navigate to **Administration > Certificate Management**.
  - f) Locate Trusted Root Certificates and click the **Add** link to add the downloaded certificate.
  - g) After the certificate is added, you can import the IBM Storage Defender Connection Manager OVA.
3. Install the Connection Manager by completing the following steps:
  - a) Store the Connection Manager OVA file on a shared folder that can be read from your vCenter.

- b) Log in to your vCenter and create a new virtual machine by using the OVA file.
  - c) While creating the virtual machine, follow the setup instructions of the vCenter to configure the network settings for the Connection Manager.
- Note:** The FQDN of an existing IBM Storage Defender Connection Manager cannot be changed. Use the same FQDN that is used earlier.
4. Update the default SSH password of the Connection Manager.
    - a) Log in to the newly created Connection Manager virtual machine by using SSH.
    - b) The default username is `defender` and the default password is `IbmStorage`.
    - c) Update the default password.
    - d) Log out.
  5. After you have redeployed the new Connection Manager, copy the backup file that is generated by the **dabackup.sh** script on the new Connection Manager. To restore the information from the previous Connection Manager, run the following bash script by specifying the **backupfile** parameter:

```
/opt/ibm/defender/bin/darestore.sh
```

Use the **sudo** command to run the script as the root privileges are required to run the script. When the Connection Manager is successfully restored, you can log in to your Connection Manager again.

#### Syntax

- `darestore.sh`
- `darestore.sh <backupfile>`
- `darestore.sh <backupfile> <password>`
- `darestore.sh --help`

#### Parameters

##### **backupfile**

Specifies the backup file to restore. The backup file must be a backup file that is generated by the **dabackup.sh** script. This parameter is optional. The user is prompted for a backupfile if it is not provided. If the backupfile is not provided at the prompt, the restore fails.

**Note:** The backup file format that is generated from the Connection Manager is `tar.gz`. If the backup file is generated from the older Connection Manager, the backup file format is `zip`. The restore operation supports both the file formats.

##### **password**

Specifies the password for the backup file. This parameter is optional. The user is prompted for a password if it is not provided. If the password is not provided at the prompt, the backup fails.

##### **--help**

Displays help information and exits.

## Backing up and restoring Connection Manager

---

When you redeploy the OVA software for a Connection Manager, you lose existing data such as database and other configuration information. To prevent losing this information, you can back up the current information by using the **dabackup.sh** bash script and store the backup file on another machine. When a new OVA is deployed, you can use the **darestore.sh** bash script with the saved backup file to restore the needed information for the redeployed OVA.

### Backing up Connection Manager

Use the **dabackup.sh** bash script to create the backup. This script is located in the `/opt/ibm/defender/bin` directory. Use the **sudo** command to run the script, as root user privileges are required to run the script. The **dabackup.sh** script will package the files that are needed for restore into a single output file and then will encrypt and password protect it. The name of the backup file is

in the following format: defender-agent-backup-YYYY.MM.DD\_HH.MM.SS.tar.gz. For example, defender-agent-backup-2024.02.01\_18.38.04.tar.gz. The backup file must be moved from the cluster and stored in a safe location. You will need this file to restore your Connection Manager.

### Syntax

- dabackup.sh
- dabackup.sh <path>
- dbbackup.sh <path> <password>
- dabackup.sh --help

### Parameters

#### path

Specifies the location to store the backup file. The path parameter is optional. The user is prompted for a path if it is not provided. If the path is not provided at the prompt, the backup file is written to the current working directory.

#### password

Specifies the password for the backup file. The password parameter is optional. The user is prompted for a password if it is not provided. If the password is not provided at the prompt, the backup fails. Save this password as it will be needed during restore.

#### --help

Displays help information and exits.

### Example: Backing up Connection Manager

```
[defender@defender6 ~]$ sudo /opt/ibm/defender/bin/dabackup.sh
Enter location to store the backup file: /home/defender/backup
=> Validating path /home/defender/backup..
Enter password to protect the backup file:
=> Backing up mariadb..
=> Backing up defender agent core files..
=> Backing up defender agent certificate files..
=> Backing up files to /home/defender/backup/defender-agent-backup-2024.07.03_11.30.41.tar.gz
Defender Agent has been successfully backed up to /home/defender/backup/defender-agent-
backup-2024.07.03_11.30.41.tar.gz.
=> Deleting /root/dabackup..
```

### Restoring Connection Manager

Before you begin with restore procedure, you must deploy the connection manager by completing the steps (1) to (5) in [“Connecting Data Resiliency to on-premises resources”](#) on page 37 in section **Before you begin**. Also, complete the steps (1) to (3) in section **Procedure**.

After you have redeployed the new Connection Manager, copy the backup file that is generated by the **dabackup.sh** script to the new Connection Manager. To restore the information from the previous Connection Manager, run the following bash script by specifying the **backupfile** parameter:

```
/opt/ibm/defender/bin/darestore.sh
```

Use the **sudo** command to run the script, as root user privileges are required to run the script.

#### Note:

- When you redeploy or upgrade the Connection Manager, you don't need to generate a connection token. For more information, see [“Upgrading Connection Manager”](#) on page 54.
- If the backup of a Connection Manager is being restored to a new OVA or a different Connection Manager than the one that was backed up from, then complete the following steps to allow the new Connection Manager to automatically update its connection certificate:
  1. Log out of the user interface.
  2. Wait for 5 minutes.

3. Log in to the user interface.

When the Connection Manager is successfully restored, you can log in to your Connection Manager again.

### Syntax

- `darestore.sh`
- `darestore.sh <backupfile>`
- `darestore.sh <backupfile> <password>`
- `darestore.sh --help`

### Parameters

#### backupfile

Specifies the backup file to restore. The backup file must be a file that is generated by the **dabackup.sh** script. This parameter is optional. The user is prompted for a backupfile if it is not provided. If the backupfile is not provided at the prompt, the restore fails.

**Note:** The backup file format that is generated from the Connection Manager is `tar.gz`. If the backup file is generated from the older Connection Manager, the backup file format is `zip`. The restore operation supports both the file formats.

#### password

Specifies the password for the backup file. This parameter is optional. The user is prompted for a password if it is not provided. If the password is not provided at the prompt, the backup fails.

#### --help

Displays help information and exits.

### Example: Restoring Connection Manager

```
[defender@defender6 ~]$ sudo /opt/ibm/defender/bin/darestore.sh
Enter the backup file to restore: /home/defender/defender-agent-
backup-2024.02.08_13.40.46.tar.gz
Enter password for the backup file:
=> Unzipping files to /root/dabackup..
=> Restoring defender agent core files..
=> Restoring mariadb..
=> Restarting defender-agent-db pod..
=> Restoring defender agent certificate files..
=> Restarting defender-agent-core pod..
=> Restarting defender-agent-espial pod..
=> Deleting /root/dabackup..
Defender Agent has been successfully restored.
```

## Troubleshooting Connection Manager issues

When working with Connection Manager, you might experience problems specific to the sensors. This might lead you to resolve the issues with involved procedures.

### Resolving an IBM Storage Defender sensor uninstallation failure

Uninstalling a IBM Storage Defender sensor might fail if the sensor is registered to a Connection Manager that is destroyed or not properly backed up and restored during a Connection Manager OVA upgrade. The sensor might show as installed in the UI, but an uninstall job fails and the UI continues to show the sensor as Installed.

To complete the sensor uninstallation in this situation and allow other sensors that were previously installed/registered to be uninstalled/unregistered, complete the following steps:

1. Back up the current Connection Manager using the `dabackup.sh` script.
2. Restore the Connection Manager from the backup file that is obtained in the [step 1](#) by using `darestore.sh` script. This restore operation triggers the Connection Manager to restore the sensor

registration data from the IBM Storage Defender Data Resiliency Service. This step may take several minutes to complete.

3. Uninstall IBM Storage Defender sensor with the instructions provided in [“Uninstalling an IBM Storage Defender sensor”](#) on page 49. You might need to retry if the restore of the sensor registration data in the [step 2](#) is not finished.

### For an External-control-node user

An external-control-node user might see that the sensor unregistration task fails during the execution of the `sensor_uninstall.yml` playbook.

If a Connection Manager is destroyed or not properly backed up and restored during a Connection Manager OVA upgrade, the external sensor control node registration data might be lost. In this case, the user needs to reregister the sensor control node through Connection Manager UI. The sensor administrator user ID and password that are associated with the external control node need to match the ones used on the corresponding external control node, which are provided through the `setup.sh` script in the top directory of the `defender-sensor-ansible.tar` file. These precautionary steps must be taken before running the `sensor_install.yml` or `sensor_uninstall.yml` playbooks.

## Appendix: Inventory metadata that is collected from Data Resiliency

---

IBM Storage Defender Data Resiliency Service collects metadata from the connected sources. This metadata can include settings that you configured on your VMware vCenter or IBM Storage Defender Data Protect cluster. It can also include names that you defined for resources like virtual machines or backup policies. The following lists provide you with detailed insights on what data is collected.

**Note:** At any time, the data that is collected from the connected sources is encrypted. This action is true for data in transit and data at rest.

### Metadata that is collected from IBM Storage Defender Data Protect

#### Policies:

- Source name (vCenter)
- Days to keep
- ID
- Name
- Retries
- Retry interval
- Incremental schedule policy
  - Backup interval
  - Periodicity
- Extended retention policies
  - Data lock configuration
    - Days to keep
    - Worm retention type
  - Days to keep
  - Multiplier
  - Periodicity

#### Protection groups:



- Description
- Environment
- ID
- Last modified time
- Name
- Number protected objects
- Policy ID
- Priority
- QoS policy
- SLA
  - Backup type
  - SLA minutes
- Start time
  - Hour
  - Minute
  - Time zone
- Storage domain ID
- VMware parameters
  - Index excludes path list
  - Index includes path list
- Objects
  - ID
  - Name

**vCenter information:**

- Name
- Protected objects
  - Environment
  - ID
  - Name
  - Parent ID
  - Protection groups
  - UUID
  - Versions
    - ID
    - Protection group ID
    - Start time
- vCenter information
  - Data stores
    - Name
    - ID
    - Parent ID
  - Network entities

- Name
- ID
- Parent ID
- Resource pools
  - Name
  - ID
  - Parent ID

## **Metadata that is collected from VMware vCenter**

### **Folders:**

- Name
- ID
- Tag

### **Disks:**

- Serial
- Name
- ID

### **Hosts:**

- Disks
  - LUN
  - Name
  - ID
  - Adapter ID
  - Target
  - Host
    - ID
    - Storage adapter
    - Tags

### **Volumes:**

- Size
- Name
- Disk ID
- ID
- Used
- Tags

### **VMs:**

- Hostname
- UUID
- Volumes
- Data center
- Configuration path
- OS name

- Folder path
- Power® state
- Network name
- Network ID
- Mac address

**Cluster:**

- Name
- ID
- Tags

**Views:**

- Parent
- Child
  - Parent
  - Child
  - Name
  - ID
  - Type
- Name
- ID
- Type

**Metadata that is collected from IBM Storage FlashSystem**

**Volumes:**

- ID
- UUID
- Name
- Size
- Volume Group ID
- Volume Group Name
- Snapshot Policy ID

**Volume Groups:**

- ID
- Name

**Host Clusters:**

- ID
- Name

**Hosts:**

- ID
- Name
- Node Identifiers (IQN or WWN)
- Host Cluster ID
- Mapped Volumes ID

- IO Group IDs
- IO Group Names

**Storage Pools:**

- ID
- Name
- Volume IDs
- Total Capacity
- Free Capacity

**Snapshots:**

- ID
- Name
- Volume ID
- Volume Name
- Created Time
- Expiration Time
- Volume Group ID
- Safeguarded (boolean)

**System:**

- Cluster ID
- Name
- Model Number
- Serial Number

**Snapshot Policies:**

- ID
- Name
- Type
- Start Time
- Retention Days
- Interval
- Interval Unit

## Chapter 8. Licensing

The IBM Storage Defender Data Resiliency Service (Data Resiliency Service) has the following two tiers of licensing: Trial and Essential.

The Trial service is valid for 60 days after activation. This Trial service gives you enough capability to learn about the Data Resiliency Service. To get access to the Trial service, you can choose one of the following two methods:

- If you are already registered with IBM Storage Defender Data Management Service (Data Management Service), you can select the Data Resiliency tile from the Dashboard, which directs you to fill out a form.
- If you are not registered with Data Management Service, you can directly go to the following URL to fill out the form: <https://www.ibm.com/account/reg/signup?formid=urx-52559>.

When you fill out the form, the information is sent to the IBM Storage Defender SRE team, who provision a Trial service. You will receive the IBM Documentation URL and login credentials in the email ID that you have specified in the form. You can use the same login credentials to log in to the service.

IBM Storage Defender  
Start your 60-day trial.

Connect primary and secondary storage  
Provides a complete view across primary and secondary storage to help keep your organization resilient.

Bridge organization silos  
Connect your Security and Storage teams with a common understanding of how to work together to remediate an event.

Get back to production quickly, effectively, and safely  
Quickly identify and validate the most recently recovery points free from anomalies.

Making the tool work for you  
In channel support and online material is available to help users set up and optimize their use of Storage Defender.

Create an IBMid  
Already have an IBM account? [Log in](#)

Account information

Business email <sup>ⓘ</sup>  
defender.developer

Password  
\*\*\*\*\*

Your email address will become your IBMid, which you'll use to log into IBM.com.

First name  
Last name

Country or region of residence  
United States of America

State or province  
New York

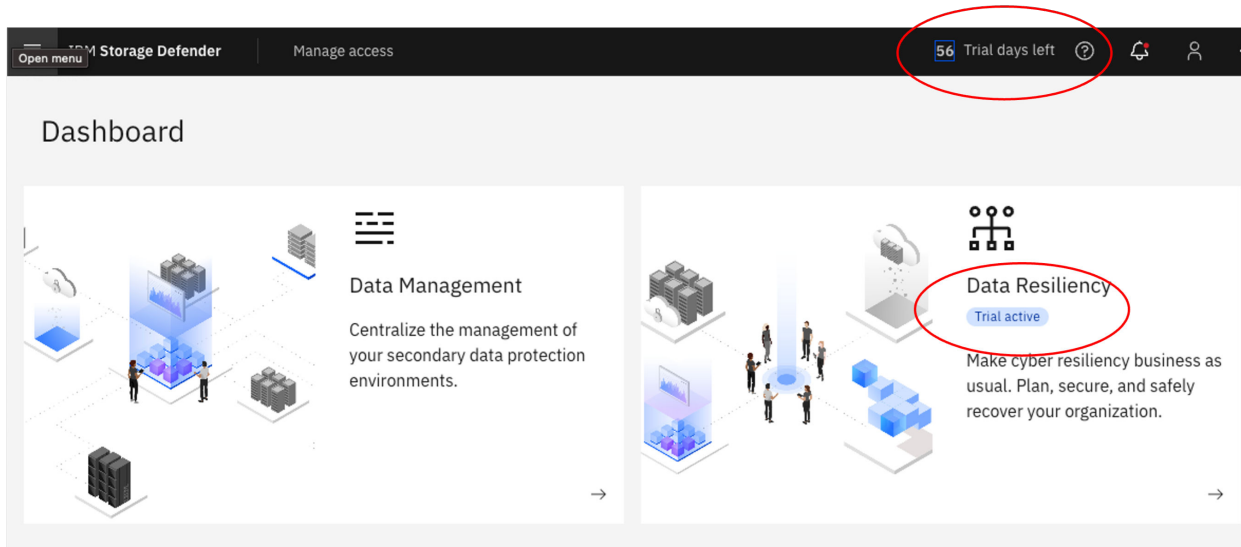
During the trial, we may share guidance on which features to explore. We may also reach out to you to check in on your progress and follow up after the trial is over. By participating in the trial, you agree to the [IBM Privacy Statement](#).

Next

Additional information

Verify email

On the top of the Dashboard screen, you can see the number of days remaining in the Trial service, and on the Data Resiliency tile, you can see **Trial active**.



This Trial service is a fully functional service, where you can implement an end-to-end deployment. But you must know that this Trial service is valid for the limited amount of time that you can use without purchase.

After you have tried IBM Storage Defender and if you want to use the paid version of the service, you can contact your IBM sales team to purchase this product. To contact IBM Sales team, you can click **Trial Days Left**, which pops up a window where you can find a email ID to contact IBM Sales. In the process of the purchase, the IBM Storage Defender SRE team is notified that the Trial service is required to be converted to the paid service.

The initial paid service is referred to as Essential, and the Essential service has the following extra functional advantages than the Trial service.

Function	Trial (Free for 60 days)	Essential (Paid tier)
Notification	Notification with the UI	Notification with the UI
	-	Notification outside the UI with SIEM
	-	Notification with email
Detection	IBM Storage Defender Sensor on RHEL 9	IBM Storage Defender sensors on RHEL 9, SLES, Ubuntu
	-	IBM FlashCore Module (FCM) hardware sensor
Cleanroom	Private Cleanroom	Private Cleanroom
Recovery	Recovery points up to 60 days in the past in IBM Storage FlashSystem and IBM Storage Defender Data Protect	All recovery points that exist in IBM Storage FlashSystem and IBM Storage Defender Data Protect

In the Trial service, you are allowed to use the user interface (UI) to operate the environment. In the Essential service, though you can use the UI, you do not have to be logged in to get notifications for any alerts or messages. Because IBM Storage Defender sends you messages and alerts to your email ID, which indicates that you should log in to the UI for further analysis.

If you are using QRadar to monitor your security environment, IBM Storage Defender Essential service has an integration that allows it to share information with QRadar when issues occur.

IBM Storage Defender sensors comes with the RHEL 9 kernel extension in the Trial version, and in the Essential service the sensor comes also with SLES and Ubuntu.

In the Trial environment, the IBM Storage Defender SRE team can gather information about recovery points only up to 60 days.





---

# 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/](http://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/](http://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 \(www.ibm.com/able\)](http://www.ibm.com/able).



## 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](http://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](http://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: