

Ransomware Detection powered by CyberSense®

v8.15.2515

Backup, Restore, and Recovery Guide

Provides information about the backup, restore, and recovery functions used with Ransomware Detection configuration files, indexes, databases, log files, and license files.

© 2023, 2026 Hitachi Vantara. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including copying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Vantara LLC (collectively "Hitachi"). Licensee may make copies of the Materials provided that any such copy is: (i) created as an essential step in utilization of the Software as licensed and is used in no other manner; or (ii) used for archival purposes. Licensee may not make any other copies of the Materials. "Materials" mean text, data, photographs, graphics, audio, video and documents.

Hitachi reserves the right to make changes to this Material at any time without notice and assumes no responsibility for its use. The Materials contain the most current information available at the time of publication.

Some of the features described in the Materials might not be currently available. Refer to the most recent product announcement for information about feature and product availability, or contact Hitachi Vantara LLC at https://support.hitachivantara.com/en_us/contact-us.html.

Notice: Hitachi products and services can be ordered only under the terms and conditions of the applicable Hitachi agreements. The use of Hitachi products is governed by the terms of your agreements with Hitachi Vantara LLC.

By using this software, you agree that you are responsible for:

- 1) Acquiring the relevant consents as may be required under local privacy laws or otherwise from authorized employees and other individuals; and
- 2) Verifying that your data continues to be held, retrieved, deleted, or otherwise processed in accordance with relevant laws.

Notice on Export Controls. The technical data and technology inherent in this Document may be subject to U.S. export control laws, including the U.S. Export Administration Act and its associated regulations, and may be subject to export or import regulations in other countries. Reader agrees to comply strictly with all such regulations and acknowledges that Reader has the responsibility to obtain licenses to export, re-export, or import the Document and any Compliant Products.

Hitachi and Lumada are trademarks or registered trademarks of Hitachi, Ltd., in the United States and other countries.

AIX, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, FlashCopy, GDPS, HyperSwap, IBM, OS/390, PowerHA, PowerPC, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z14, z15, z16, z/VM, and z/VSE are registered trademarks or trademarks of International Business Machines Corporation.

Active Directory, ActiveX, Bing, Excel, Hyper-V, Internet Explorer, the Internet Explorer logo, Microsoft, Microsoft Edge, the Microsoft corporate logo, the Microsoft Edge logo, MS-DOS, Outlook, PowerPoint, SharePoint, Silverlight, SmartScreen, SQL Server, Visual Basic, Visual C++, Visual Studio, Windows, the Windows logo, Windows Azure, Windows PowerShell, Windows Server, the Windows start button, and Windows Vista are registered trademarks or trademarks of Microsoft Corporation. Microsoft product screen shots are reprinted with permission from Microsoft Corporation.

All other trademarks, service marks, and company names in this document or website are properties of their respective owners.

Copyright and license information for third-party and open source software used in Hitachi Vantara products can be found in the product documentation, at <https://www.hitachivantara.com/en-us/company/legal.html>.

Contents

Chapter 1. Backup, Restore, and Recovery Introduction.....	5
Overview.....	7
Chapter 2. Using the CLI tools.....	9
Taking a backup of Ransomware Detection data.....	9
Restoring a backup of Ransomware Detection data.....	9
Recovering a backup of Ransomware Detection data.....	10
Chapter 3. Backing up Ransomware Detection data.....	11
Setting up the backup application.....	12
Installing the client software.....	12
Adding scripts and defining jobs.....	13
Using Dell PPDM.....	13
Using Dell NetWorker.....	13
Using Dell Avamar.....	14
Using Commvault Backup & Recovery.....	14
Using Cohesity NetBackup.....	15
Using IBM Storage Protect.....	15
Running the backup.....	17
Viewing the backup details.....	18
Chapter 4. Restoring backups.....	19
Restoring a backup (general process).....	20
Restoring a NetWorker backup.....	21
Chapter 5. Recovering backups.....	23
Recovering a backup.....	24
Appendix A. Migrating an engine to new hardware.....	25
Migrating an engine.....	25

Chapter 1. Backup, Restore, and Recovery

Introduction

This guide provides information about backup, restore, and recovery of your Ransomware Detection configuration files, indexes, databases, log files, and license files. You do this using either the command line interface (CLI) or commonly used third-party commercial backup and restore software, with the final recovery phase accomplished through the Ransomware Detection User Interface (UI).

Important:

The system backup procedures are intended to provide disaster recovery to restore an engine back to the state it was in at the time of the backup. Please be aware of the following:

- You may not be able to restart jobs that were running at the time of the backup, such as indexing; you may need to run a new job after restoring the system.
- The intent of the Restore/Recovery procedure is to apply the restored data onto a newly installed Ransomware Detection system, the same version of the Ransomware Detection software as was previously running. This ensures the integrity of all data and services. With a new install of the Ransomware Detection software, the Ransomware Detection system will not have any configuration data until recovery completes.

However, if you make configuration changes (such as by creating and running jobs) prior to a restore or recovery, files such as database files or log files may be out of sync after the restoration.

- When configuring the backup server, be sure to allow "dynamic" files. This means that regardless of your server's terminology for this functionality, you want it to ignore file contents and size changes during the backup.

In addition to the CLI, the currently supported backup applications that you can use for the backup and restore procedures include:

- Dell PowerProtect Data Manager® (PPDM)
- Dell NetWorker®

- Dell Avamar®
- Commvault Backup & Recovery
- Cohesity NetBackup® (NBU)
- IBM Storage Protect®

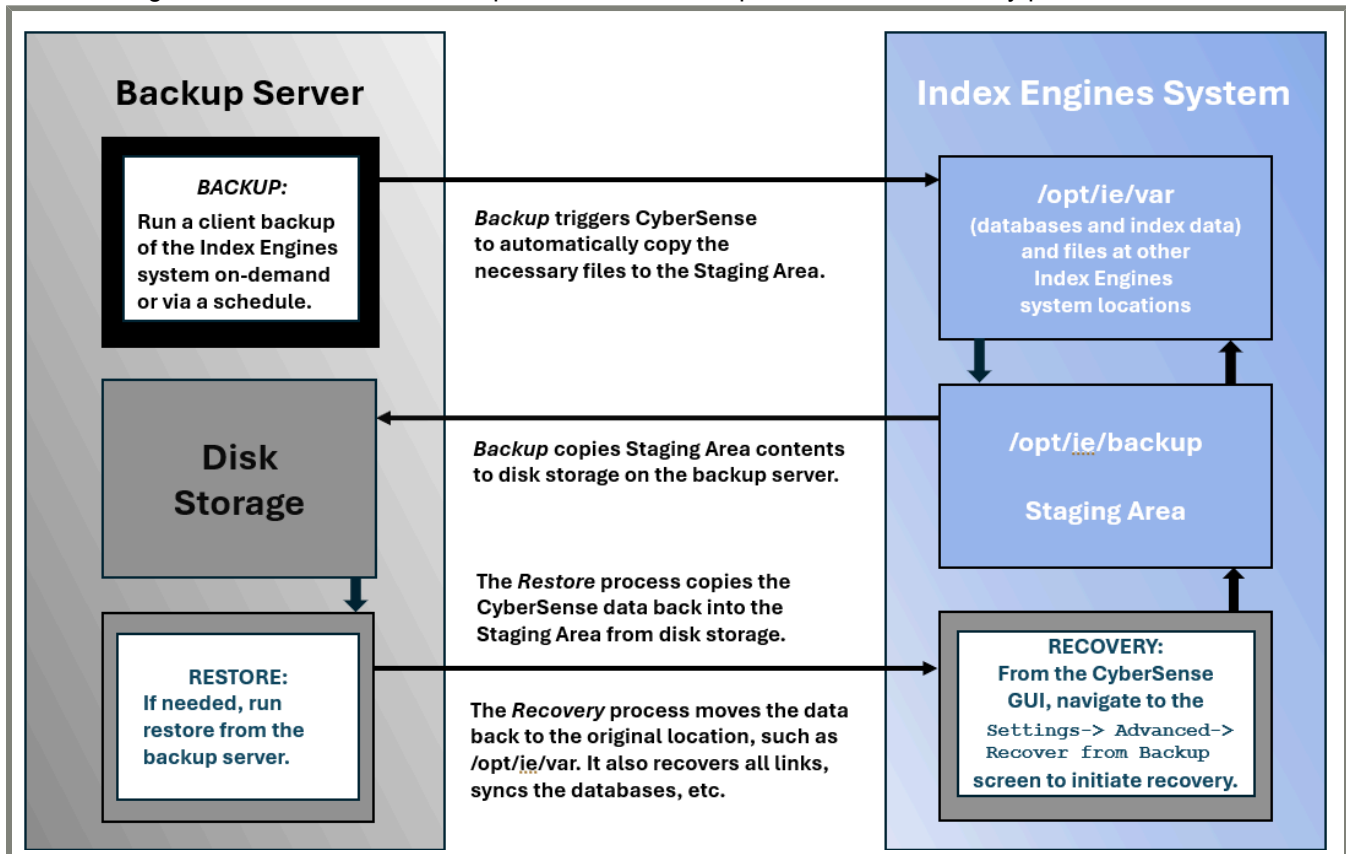
Many other backup applications may work—both free and proprietary—although other products have not yet been tested with our software.

Overview

On the Ransomware Detection server, the Ransomware Detection software creates a directory for staging the data for the backup/restore procedures. The staging area includes the backup and restore locations, which are the same. The backup directory is the location where Ransomware Detection puts the data to be backed up by the backup application. The restore directory is where the backup application puts the files to be recovered. Sometimes these directories are on different systems. Please note the following:

- **BACKUP:** Use the directory `/opt/ie/backup` as the location to store the Ransomware Detection backup.
 - You must set up your backup server tool to back up `/opt/ie/backup` on the Ransomware Detection client.
 - To periodically run backups, select full backup or select an incremental backup choice.
- **RESTORE:** When a restore is needed, initiate a restore to the `/opt/ie/backup` directory from the backup server.
- **RECOVERY:** When the restore completes, use the Ransomware Detection UI to perform a recovery. This moves the files and database contents back to the correct system locations. See [Recovering backups \(on page 23\)](#) for more information.

The following illustration summarizes the process of the backup, restore, and recovery procedures.



Chapter 2. Using the CLI tools

As an alternative to using third-party backup applications, use CLI tools for:

- [Taking a backup of Ransomware Detection data \(on page 9\)](#)
- [Restoring a backup of Ransomware Detection data \(on page 9\)](#)
- [Recovering a backup of Ransomware Detection data \(on page 10\)](#)

Taking a backup of Ransomware Detection data

Use the CLI on a Ransomware Detection server to manually create a backup.

To take a backup of Ransomware Detection data:

1. Log in to the server as the `root` user.
2. Run the following command to create the backup in the default directory of `/opt/ie/backup`:

```
/opt/ie/bin/ie_app_backup
```

A log of the backup process can be found at `/var/log/ie_backup`.

The resulting backup directory can now be copied to some other storage or to backup media.

Restoring a backup of Ransomware Detection data

Use the CLI to manually restore the Ransomware Detection system configuration, database, and index data to your target Ransomware Detection server.



Important: The Ransomware Detection software version on the target Ransomware Detection server where the restore is to be done **must** be the same as the version from which the backup was taken.

To restore a backup of Ransomware Detection data on the target Ransomware Detection server:

1. Stop or cancel any indexing jobs that may still be running.
2. Log in to the target Ransomware Detection server as the `root` user.
3. Copy the backup directory and its entire contents to the same path from which it was taken onto the target Ransomware Detection server.

Recovering a backup of Ransomware Detection data

Use the CLI to manually recover the backup.



Important: If you are recovering the backup to a new server that has a different MAC address than the one from which the backup was taken, you will need to create a support case with Hitachi Vantara Support Connect at <https://support.hitachivantara.com>. Request the required override key needed to allow licensing to be valid; include the MAC address from the original server and that of the new server on that request. The Hitachi Vantara support team will provide the override key.

To recover a backup of Ransomware Detection data:

1. Run the following command using the provided override key if you are recovering to a new server with a different MAC address as described in the note above:

```
setdbenv engine id_override <override_key>
```

2. Run the following command to restore from the default directory of `/opt/ie/backup`:

```
/opt/ie/bin/restore_from_backup -s
```

A log of the recover process can be found at `var/log/ie_backup/recovery.<timestamp>`.

The files from the source backup are removed upon successful recovery.

Chapter 3. Backing up Ransomware Detection data

You can use third-party software to back up your Ransomware Detection configuration files. The following supported third-party applications can be used for backup, restore, and recovery operations:

- Dell PowerProtect Data Manager® (PPDM)
- Dell NetWorker®
- Dell Avamar®
- Commvault Backup & Recovery®
- Cohesity NetBackup® (NBU)
- IBM Storage Protect®

Regardless of the chosen backup application, the process steps listed below are similar:

1. Install the client application on the Ransomware Detection server.
2. Use the default location, `/opt/ie/backup`, for the backup directory.



Note: The default location of `/opt/ie/backup` must be used in order to restore and recover the files.

3. Configure the backup client to access the Ransomware Detection scripts.
4. If necessary, define a backup job on the backup client application.
5. Run a backup job.

This section is set up to walk you through completing a backup job.



Note: Refer to your backup application's documentation when you need details that pertain to your specific backup application.

Setting up the backup application

The first step in backing up your files is to install the backup client software on the Ransomware Detection server. Next, you must configure this client software to access the Ransomware Detection scripts. If necessary, you then define a backup job in the backup tool, and, finally, run the backup job.

At this point, decide what kind of backup that you want performed. You can do either a full or incremental backup. Most large components of previously backed-up segments will not change even when new data is indexed, so it's reasonable to use incremental backups as part of your strategy.

Keep in mind that your backup software may have timer or timeout values that affect how long a client data preparation program or data transfer can run. If so, then allow enough time for the Ransomware Detection server to stage and transfer data for backup. The total time depends on the amount of indexed data and the network speed.

Installing the client software

These steps are dependent on the chosen backup client application. Refer to the documentation for the specific application to install it correctly.

This client-side software is installed on the Ransomware Detection server.

To install the client software on the Ransomware Detection server:

1. Install an appropriate Linux version of the backup client software on Ransomware Detection — it must be compatible with the backup application. For example, if you are using NetBackup server software, then install the NetBackup client software.
2. On your Ransomware Detection server, create the `/opt/ie/backup` directory.

Adding scripts and defining jobs

How the pre- and post-backup scripts are added to the backup application is software dependent. The sections below explain how to access the Ransomware Detection scripts and define a backup job on the client software.

These scripts use utility programs that save Ransomware Detection data in the backup staging area. These programs are executed by the backup server when a backup job runs. When the backup tool runs a scheduled backup, the Ransomware Detection pre- and post-backup scripts create a staging area in the `/opt/ie/backup` directory for the data on the client system. This staging area contains the databases, configuration files, and indexes to be backed up.

Using Dell PPDM

If you use Dell PPDM as your backup application, some steps are done on the Ransomware Detection server and others are done on the PPDM server.



Note: The agent service on your Ransomware Detection server is installed on Linux in the `/opt/dpsapps/agent.svc/` location.

To use PPDM:

1. Check to ensure that the PPDM client software is running on the Ransomware Detection server by running the command:

```
/ppdm_install_location/register.sh --status
```

2. Register the PPDM client software with the PPDM server by running the command:

```
/ppdm_install_location/register.sh --ppdmServer=<PPDM_SERVER_IP>
```

3. On the Ransomware Detection server, run the `ppdm_pre` script from `/opt/ie/bin` directory.
4. On the PPDM server, create protection policies to back up the Ransomware Detection directory `/opt/ie/backup` (or a different directory if you created one). Select **Full** backups or **Synthetic Full** backups as appropriate. Exclude directories that are not required in the backup.
5. On the Ransomware Detection server, run the `ppdm_post` script from `/opt/ie/bin` directory.

Using Dell NetWorker

If you use Dell NetWorker as your backup application, some steps are done on the Ransomware Detection server and others are done on the NetWorker server.

To use NetWorker:

1. On the NetWorker server, create a UNIX directive as below. Then, configure the Ransomware Detection server client to use that directive, which allows the backups to proceed even if files change during the backup process.

```
<<lopt/ie>>  
  
+logasm: *
```

2. In the **Backup command** field on the **Client Properties** window, enter `nsr` or `save`. Also enter the script name `nsr_pre_script` in the **Pre Command** and `nsr_post_script` in the **Post Command** fields.
3. On the Ransomware Detection server, place the following scripts in `/usr/bin`:
 - `nsr_pre_script`
 - `nsr_post_script`
4. Return to the NetWorker server and in the **Monitoring > Groups** section run the backup.

Using Dell Avamar

If you use Dell Avamar as your backup application, some steps are done on the Ransomware Detection server and others are done on the Avamar server.

To use Avamar:

1. Create the backup policy for the Ransomware Detection server on the Avamar server and define a dataset to back up the directory `/opt/ie/backup`.
2. On the Ransomware Detection server, place the following scripts from `/opt/ie/bin` directory to `/usr/local/avamar/etc/scripts` directory:
 - `avamar_pre`
 - `avamar_post`
3. Define a schedule and the retention plan for the backup policy, and then enable the schedule. During definition of a schedule, under **Dataset**, enable **Show Advanced Options** and select the following files.
 - In **Pre-Script > Run user-defined script at beginning of backup**, select `avamar_pre`.
 - In **Post-Script > Run user-defined script at end of backup**, select `avamar_post`.

Using Commvault Backup & Recovery

If you use Commvault Backup & Recovery as your backup application, the steps are performed on the Backup & Recovery server.

To use Backup & Recovery:

1. On the Backup & Recovery server, set up a schedule for backup of `/opt/ie/backup` (or an alternate if you choose to use one). This can be on-demand or time based. Choose **Full** or **Incremental**, based on local policy.
2. Implement pre- and post-backup scripting by placing the paths to the following programs as indicated by the Backup & Recovery software.

```
PreScan Process: /opt/ie/bin/commvault_pre  
PostBackup Process: /opt/ie/bin/commvault_post
```

3. Configure the backup software to all "dynamic" files. This is so the server will ignore files that change during the backup process. Also make sure backing up subdirectories is enabled and configured.

Using Cohesity NetBackup

If you use Cohesity NetBackup as your backup application, some steps are done on the Ransomware Detection server and others are done on the NetBackup server.

To use NetBackup:

1. On your Ransomware Detection server, in the NetBackup client install area, create symbolic links in the appropriate path for the `bpstart_notify` and `bpend_notify` scripts. For example, if the NetBackup client software was installed in `/usr/opensv/netbackup`, then the links can be made as shown below. The Ransomware Detection software provides initial versions of `bpstart_notify` and `bpend_notify`.

```
ln -s /opt/ie/bin/bpstart_notify /usr/opensv/netbackup/bin/bpstart_notify  
ln -s /opt/ie/bin/bpend_notify /usr/opensv/netbackup/bin/bpend_notify
```

2. Check to ensure that the NetBackup client software is running on the Ransomware Detection server. One way to start the NetBackup client software is with a command such as:

```
service netbackup start
```

3. On the NetBackup server, configure a policy to back up the Ransomware Detection directory `/opt/ie/backup` (or a different directory if you created one). Select **Full** backups or **Incremental** backups as appropriate.

Using IBM Storage Protect

If you use IBM Storage Protect as your backup application, some steps are done on the Ransomware Detection server and others are done on the Storage Protect server.



Note: By default, the Storage Protect client software is usually installed on Linux systems in `/opt/tivoli/tsm`. Implement pre- and post-backup scripting by placing the path to a program or script in the file `/opt/tivoli/tsm/client/ba/bin/dsm.sys`. Ransomware Detection provides utility programs to save data to the staging area. These programs are executed by the backup server when a backup job runs. The paths are identified in `dsm.sys`.

To use Storage Protect:

1. On the Ransomware Detection server, add the following lines to `dsm.sys`:

```
PRESCHEDULECMD /opt/ie/bin/tsm_presched
POSTSCHEDULECMD /opt/ie/bin/tsm_postsched
```

The files `/opt/ie/bin/tsm_presched` and `/opt/ie/bin/tsm_postsched` already exist on the Ransomware Detection system.

2. On the Storage Protect server, update the copy group for the policy domain, policy set, and management class that the client belongs to as follows:

```
Copy Serialization: Dynamic
```

3. Define a scheduled job to back up the client directory `/opt/ie/backup` (or the alternate directory if you created one). Select **Full** backups or **Incremental** backups as appropriate.



Note:

- You may need to specify `/opt/ie/backup/` as the backup "object" in order to back up the subdirectories.
- Storage Protect is sensitive to a trailing `/` or `/*` when requiring subdirectories. You can also specify `-subdir=yes` in the options list to enable the subdirectory backup.

Example:

```
UPDATE SCHEDULE dir2lto Backup_S SVM3 type=client action=incremental
objects='/opt/ie/backup/*' options=-subdir=yes startdate=TODAY starttime=NOW dayofweek=any
```

Running the backup

Now that the backup application is set up to call the pre- and post-backup scripts and, if necessary, make any changes needed for the backup job, it is time to run the backup job on your client software.

Run the defined backup job according to your backup application. Refer to your backup application's documentation for complete instructions.

Viewing the backup details

Note the following details about the backup process:

- After the backup software tool completes a successful backup, all of the data is automatically removed from the `/opt/ie/backup` staging area; only a README file remains in the `/opt/ie/backup` directory. The README file provides the following information:

```
The files/directories listed below are removed after a successful backup to
a supported server completes. This prevents a later restore operation from
intermixing restored indexing data with previously saved backup data.
```

```
backup_fmt_version
backup_version cmvbackup.log (Commvault only)
config_save.gz
dir_ul.txt
file_ul.txt
mac_addr
nsrbackup.log (NetWorker only)
stage/
tsmbackup.log (Storage Protect only)
```

- You can view the backup logs here: `/var/log/ie_backup`

Chapter 4. Restoring backups

When you restore a backup job, the files are restored to their original location of `/opt/ie/backup`. The process is the same for the NetBackup, Storage Protect, Commvault, PPDm, and Avamar applications. The process differs slightly for the NetWorker application.

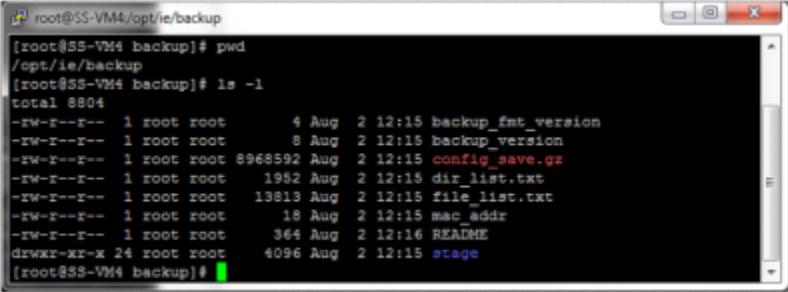
The process is a simple one — the files are first restored using the backup application, and then the restore process verifies that the files are in the correct location.

The final step is recovering the files, which is detailed in [Recovering backups \(on page 23\)](#).

Restoring a backup (general process)

To restore a backup:

1. In the backup application's UI, select the Ransomware Detection backup, and restore it to its original location: `/opt/ie/backup`. If the backup application asks about overwriting files that already exist in the restore directory, you can respond affirmatively.
2. On the Ransomware Detection server, verify that the files shown below were restored.



```
root@SS-VM4:/opt/ie/backup
[root@SS-VM4 backup]# pwd
/opt/ie/backup
[root@SS-VM4 backup]# ls -l
total 8804
-rw-r--r-- 1 root root    4 Aug 2 12:15 backup_fmt_version
-rw-r--r-- 1 root root    8 Aug 2 12:15 backup_version
-rw-r--r-- 1 root root 8968592 Aug 2 12:15 config_save.gz
-rw-r--r-- 1 root root  1952 Aug 2 12:15 dir_list.txt
-rw-r--r-- 1 root root 13813 Aug 2 12:15 file_list.txt
-rw-r--r-- 1 root root   18 Aug 2 12:15 mac_addr
-rw-r--r-- 1 root root   364 Aug 2 12:16 README
drwxr-xr-x 24 root root 4096 Aug 2 12:15 stage
[root@SS-VM4 backup]#
```

3. Then, proceed to the system recovery steps. See [Recovering backups \(on page 23\)](#) for more information.

Restoring a NetWorker backup

To restore a NetWorker backup:

1. In the NetWorker application's UI, select the backup or SSID you want to restore using one of the following commands:

```
recover -s <mediaserver> -c <client> -a <directory>
```

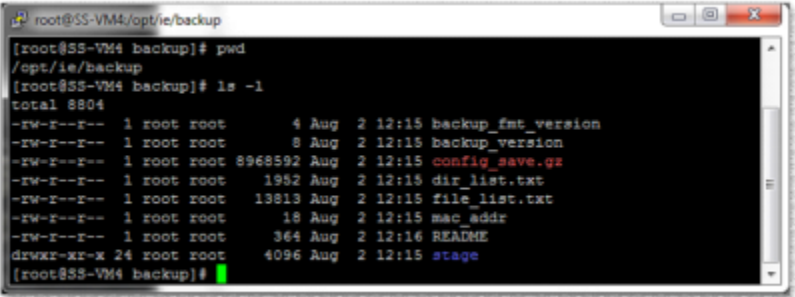
or

```
recover -s <mediaserver> -S <ssid> -d <directory>
```

Example:

```
recover -s tsm-mediaserver.quest.com -c ss-vm3 -a /opt/ie/backup
```

2. On the Ransomware Detection server, verify that the files shown below were restored.



```
root@SS-VM4:/opt/ie/backup
[root@SS-VM4 backup]# pwd
/opt/ie/backup
[root@SS-VM4 backup]# ls -l
total 8804
-rw-r--r-- 1 root root    4 Aug 2 12:15 backup_fmt_version
-rw-r--r-- 1 root root    8 Aug 2 12:15 backup_version
-rw-r--r-- 1 root root 8968592 Aug 2 12:15 config_save.gz
-rw-r--r-- 1 root root   1952 Aug 2 12:15 dir_list.txt
-rw-r--r-- 1 root root  13813 Aug 2 12:15 file_list.txt
-rw-r--r-- 1 root root    18 Aug 2 12:15 mac_addr
-rw-r--r-- 1 root root   364 Aug 2 12:16 README
drwxr-xr-x 24 root root  4096 Aug 2 12:15 stage
[root@SS-VM4 backup]#
```

3. Then, proceed to the system recovery steps. See [Recovering backups \(on page 23\)](#) for more information.

Chapter 5. Recovering backups

At this point in the process, your files have been backed up using a third-party backup tool and restored to the target Ransomware Detection server, which must have the same Ransomware Detection software installed.

The process is completed in the Ransomware Detection UI and recovers the Ransomware Detection configuration, database, and index data. Before beginning the recovery process, review the following information.

**Note:**

Requirements for a successful recovery:

- Stop or cancel any indexing or querying jobs before attempting a recovery. Otherwise, the recovery procedure will stop all Ransomware Detection services and any running jobs, which may have a negative impact.
- The installed Ransomware Detection software version must be the same that was used when creating the backup.
- The restore from the backup server must have successfully completed, with the backed-up files now residing on the client system with the Ransomware Detection software.
- Ransomware Detection servers depend on the ability to resolve hostnames to IP addresses. The recommended and typical way to accomplish this is to use the Domain Name System (DNS). If, however, you are not using DNS, then the `/etc/hosts` file on each engine must have the hostnames and/or IP addresses.

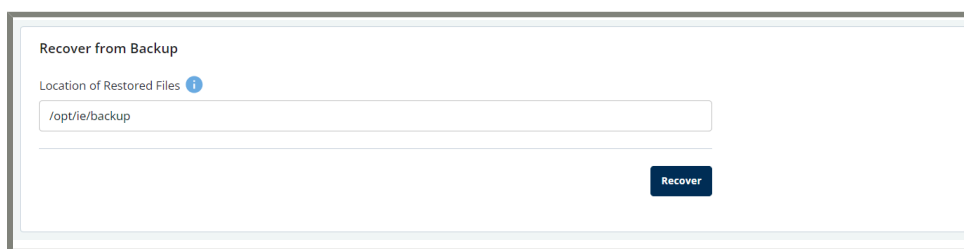


Important: If you are recovering the backup to a new server that has a different MAC address than the one from which the backup was taken, you will need to create a support case on Hitachi Vantara Support Connect at <https://support.hitachivantara.com>. Request the required override key needed to allow licensing to be valid; include the MAC address from the original server and that of the new server on that request. The Hitachi Vantara support team will provide the override key.

Recovering a backup

Once you restore a backup image to `/opt/ie/backup` using a backup tool, open the Ransomware Detection UI to recover the Ransomware Detection system configuration, database, and index data.

1. Open a web browser and sign in to the Ransomware Detection UI. In the **URL** field, use **https://** and type the hostname (preferred) or IP address of the host where the Ransomware Detection server is installed. The **Log In** page opens.
2. Type the administrator credentials and then select **Log In**.
3. Go to the **Settings > Advanced > Recover from Backup** page and type the path where the backup file was restored to. The path to use is `/opt/ie/backup`.



4. Select **Recover**.

The recovery scripts stop all Ransomware Detection services before the recovery begins and restart the services when recovery completes.

The scripts and programs check various conditions and report successes or failures. Possible errors may include the following:

- Cannot locate backup directory.
 - Expected files do not exist in the backup directory.
 - The software version file is missing.
 - The running system has an older version of software than the version on which the backup image was made.
 - Same-file-system requirement failed.
 - The backup image was already used for recovery (moving segments modifies the backup image during recovery).
5. Once recovery successfully completes, sign out and reboot the Ransomware Detection server.
 6. Sign back in. After a successful recovery, the files in the `/opt/ie/backup` directory are automatically removed. You can view the recovery log, which is located in `/var/log/ie_backup/recovery.<timestamp>`.

Appendix A. Migrating an engine to new hardware

The process of migrating an engine from one bare metal machine to another is similar to the backup, restore, and recovery process. The engine on the new hardware will be in the same state as it was on the original host hardware. The additional step in this migration process is to make the new hardware look like the old hardware using a key received from your support organization.

Migrating an engine

To migrate a Ransomware Detection server to a new server:



Note: To receive an override key, open a case with your support organization. Use the returned key as the value for the `<override_key>` field in step [4 \(on page 25\)](#).

1. Make a backup of the original Ransomware Detection server. See [Backing up Ransomware Detection data \(on page 11\)](#) for complete instructions.
2. Shut down the original Ransomware Detection server.
3. Change the host name on the new Ransomware Detection server to the host name of the original Ransomware Detection server.
4. On the new Ransomware Detection server, run:

```
setdbenv engine id_override <override_key>
```

Where `<override_key>` is the key you received from your support organization.

5. On the new Ransomware Detection server, restore the backup. See [Restoring backups \(on page 19\)](#) for complete instructions.
6. On the new Ransomware Detection server, run again:

```
setdbenv engine id_override <override_key>
```

7. On the new Ransomware Detection server, recover the files as described in [Recovering backups \(on page 23\)](#).

Hitachi Vantara

Corporate Headquarters 2535 Augustine Drive
Santa Clara, CA 95054 USA www.HitachiVantara.com community.HitachiVantara.com

Regional Contact Information

Americas: +1 866 374 5822 or info@hitachivantara.com

Europe, Middle East and Africa: +44 (0) 1753 618000 or info.emea@hitachivantara.com

Asia Pacific: +852 3189 7900 or info.marketing.apac@hitachivantara.com

