

HITACHI

Ransomware Detection powered by CyberSense®: Backup and Restore with HDPS

MK-26RDCS006-00

Hitachi Vantara

© Hitachi Vantara LLC 2026. All Rights Reserved.

Table of Contents

Notices and Disclaimer	2
About This Document	3
Intended Audience.....	3
Value Proposition	3
Document Revisions	3
Comments.....	3
Overview.....	4
Test Environment.....	4
Key Components.....	4
Prerequisites.....	4
Hardware	5
Software	5
Test Scenarios.....	5
Validation Results.....	6
File-level Backup and Restore	6
Server-level Backup and Restore.....	7
Summary	15

Notices and Disclaimer

© 2026 Hitachi Vantara LLC. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for commercial purposes without the express written permission of Hitachi, Ltd., or Hitachi Vantara (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 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.

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 to access relevant data; and
- 2) Verifying that 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.

EXPORT CONTROLS - Licensee will comply fully with all applicable export laws and regulations of the United States and other countries, and Licensee shall not export, or allow the export or re-export of, the Software, API, or Materials in violation of any such laws or regulations. By downloading or using the Software, API, or Materials, Licensee agrees to the foregoing and represents and warrants that Licensee is not located in, under the control of, or a national or resident of any embargoed or restricted country.

Hitachi is a registered trademark of Hitachi, Ltd., in the United States and other countries.

AIX, AS/400e, DB2, Domino, DS6000, DS8000, Enterprise Storage Server, eServer, FICON, Flash Copy, IBM, Lotus, MVS, OS/390, PowerPC, RS6000, S/390, System z9, System z10, Tivoli, z/OS, z9, z10, z13, z/VM, BCPii™ 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, the Microsoft Corporate 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 web site are properties of their respective owners.

RDC® is a registered trademark of Index Engines, Inc.

About This Document

This document describes how Ransomware Detection powered by CyberSense® (RDC) configurations are backed up and restored using Hitachi Data Protection Suite (HDPS). All procedures documented here are performed exclusively in a non-production laboratory environment.

- Ransomware Detection powered by CyberSense is an AI-powered data indexing and analytics engine. It recognizes patterns of change in data to confirm its integrity, and it detects ransomware corruption within immutable snapshots. RDC creates Thin Image Advanced Safe Snaps using policies and scans these snapshots to identify ransomware corruption in block data, enabling intelligent and rapid recovery.
- Hitachi Thin Image Advanced (TIA) is a highly efficient and advanced snapshot technology offered by Hitachi Vantara for its storage systems such as the Hitachi Virtual Storage Platform One Block (VSP One Block) series. It enables you to create nearly instant, point-in-time copies of your data volumes without duplicating all the data.
- Hitachi Data Protection Suite is a modern and unified solution that facilitates the backup, recovery, and management of enterprise and application data. It integrates seamlessly with Hitachi's processing and storage solutions to provide effective data protection and long-term data retention.
- Hitachi Virtual Storage Platform One Object is Hitachi Vantara's next-generation, S3-compatible object storage solution. It's engineered to operate on-premises with cloud-native capabilities such as in-place analytics and metadata-rich services. Designed atop Kubernetes, this platform deploys containerized services seamlessly, enabling scalable, intelligent, multi-petabyte storage for structured, semi-structured, and unstructured data.

Intended Audience

This document is intended for the following professionals:

- Cybersecurity Analysts: To understand how RDC detects data corruption (for example, ransomware infections) and how immutable snapshots prevent reinfection during and after the recovery process.
- Backup and Recovery Administrators: To learn the detailed procedures for restoring data, managing the snapshot lifecycle, and using verification reports to validate data integrity before bringing systems back online.
- Storage Administrators: To gain insights into configuring, managing, and monitoring Thin Image Advanced immutable snapshots, and integrating the storage system with RDC and Ansible for a unified recovery workflow.

Value Proposition

Backing up and restoring RDC configurations using Hitachi Data Protection Suite ensures resilient, automated, and secure protection of critical system configurations. By leveraging HDPS advanced features – such as file-level granularity, server-level recovery via 1-Touch, and script-driven automation – organizations can:

- Minimize downtime with fast, reliable recovery of RDC configurations and policies.
- Ensure compliance and audit readiness through consistent backup practices.
- Reduce operational risk by safeguarding against configuration loss or corruption.
- Simplify disaster recovery with centralized management and seamless integration into existing HDPS infrastructure.

This solution empowers IT teams to maintain RDC integrity and continuity with minimal manual intervention.

Document Revisions

Revision Number	Date	Details
v1.0	April 2026	Initial release

Comments

Send any comments on this document to Docs-Feedback@hitachivantara.com. Include the document title, including the revision level, and refer to specific sections and paragraphs whenever possible. All comments become the property of Hitachi Vantara LLC.

Thank you.

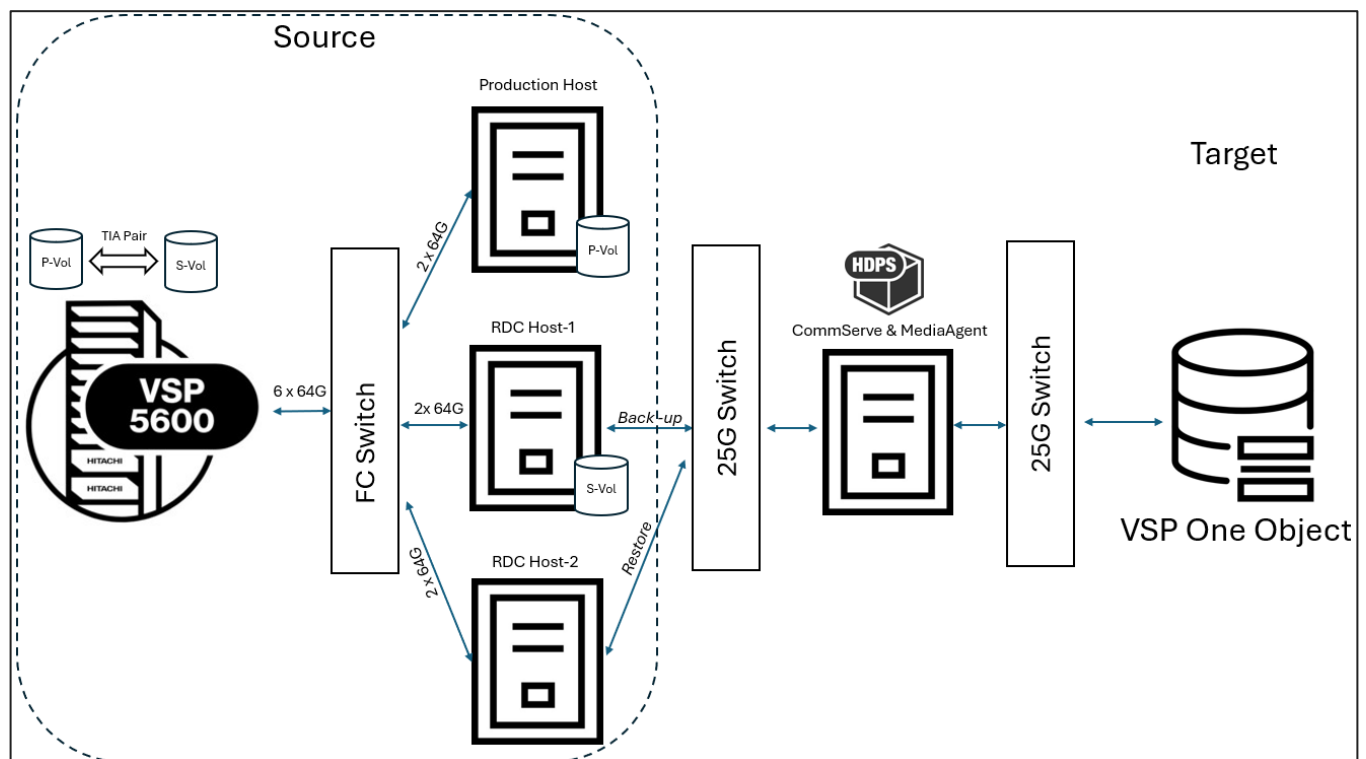
Overview

Ransomware Detection powered by CyberSense (RDC) leverages Hitachi Data Protection Suite (HDPS) to ensure reliable and secure backup and restoration of its configuration data. This process supports both **file-level** and **server-level** operations, providing flexibility and resilience in data protection.

HDPS integrates seamlessly with RDC, automating backup schedules, ensuring data integrity, and enabling quick recovery with minimal downtime. This implementation enhances operational continuity and safeguards critical configuration data against loss or corruption.

VSP One Object as a backup target enhances data security with its immutability and object lock features. Write-Once, Read-Many (WORM) ensures that once backup objects are written, they cannot be altered or deleted for a specified retention period, providing protection against ransomware, insider threats, and operational errors by making backups tamper-proof.

Test Environment



Key Components

- **RDC Configuration** – This includes system settings, policies, and operational data that must be preserved and restored.
- **HDPS** - The core data protection platform that manages backup and restore operations, including key configuration components like Subclient policies, PreScan and PostProcess scripts, and 1-Touch recovery feature for Server-level backup.
- **VSP One Object** - A dedicated, immutable backup target with object-lock capabilities for securely storing backup data.

Prerequisites

- RDC must be properly configured and operational.
- HDPS Media Agent and CommServe servers must be fully set up and accessible.
- A designated VSP One Object environment must be configured and available.

Hardware

Item	Description	Quantity
Physical Server	Hitachi Advanced Server HA820G2; 2 x Intel Xeon Silver 4310 (12C, 2.10Ghz); 128 GB RAM; 2 x SN1700E 64Gb 4p FC HBA	2
Physical Server	Hitachi Advanced Server HA820G3; 2x Intel Xeon Gold 5218 (16C, 2.3Ghz); 192 GB RAM; 2 x SN1700E 64Gb 4p FC HBA	2
Physical Server	Hitachi Advanced Server HA810; 2x Intel Xeon Silver 4410Y (12C, 2Ghz); 128 GB RAM; 2 x Emulex LPe35003-M2 32Gb 4p FC HBA	1
25G NICs	Broadcom P225p NetXtreme-E Dual port 10Gb/25Gb Ethernet PCIe Adapter - NIC	3
Physical Storage	Hitachi VSP 5600-2N	1
Ethernet Switch	Cisco93180YC-FX	1
FC Switch	Brocade G720	1

Table 1 lists the hardware used for testing.

NOTE: The testing was conducted in a non-production, laboratory environment using the hardware listed. This specific hardware is not mandatory, and any equivalent hardware can be used to implement the solution.

Software

Item	Version	Quantity
Physical Server	RHEL 9.4	4
Physical Server	Windows 2022	1
Physical Storage	Microcode: SVOS 9.8.7	1
HDPS	11.36	N/A
RDC	8.12.1-1.6	N/A

Table 2 lists the software used for testing.

Test Scenarios

Test	Description	Success Criteria
File-level backup and restore	RDC configuration files are backed up and restored via HDPS.	All the policies and the DB file must be intact after successful restore.
Server-level backup and restore	RDC server is backed up and restored via HDPS.	The entire server configuration must be intact after successful restore.

Table 3 lists the test scenarios performed in the validation.

Validation Results

Ransomware Detection powered by CyberSense configurations are backed up (at the file and server level) and restored successfully using Hitachi Data Protection Suite (HDPS).

File-level Backup and Restore

Individual RDC configuration files can be selectively backed up and restored without affecting the entire system. This capability is useful for recovering specific files, such as the Cyber Recovery Database, which contains the critical RDC information.

Backup

1. Login via SSH to the RDC host and verify that the `backup` directory exists in the `/opt/ie` path on the host. If it does not exist, create the directory.
2. Create a new Subclient in HDPS for the backup process; specifying the content path as `/opt/ie/backup/**`.
3. Assign the PreScan and PostProcess scripts to this Subclient as specified in the [Ransomware Detection powered by CyberSense Backup Restore and Recovery Guide](#).
4. Once the backup is complete, verify the contents of the `/opt/ie/backup` directory. It should contain a README file listing all the backed-up files:

```
[root@CyberSense-host1-93165 ie_backup]# cd /opt/ie/backup/
[root@CyberSense-host1-93165 backup]# ll
total 4
-rw-rw-r-- 1 root root 382 Sep 29 12:21 README
[root@CyberSense-host1-93165 backup]#
[root@CyberSense-host1-93165 backup]#
[root@CyberSense-host1-93165 backup]# more README
The files/directories listed below are removed whenever a successful backup
or restore from a supported server completes. This is to prevent a later restore
operation from intermixing restored indexing data with previously saved backup data.

  backup_fmt_version
  backup_version
  cmvbackup.log
  config_save.gz
  dir_list.txt
  file_list.txt
  mac_addr
  stage/
```

5. Navigate to the `crdb` file located at `/opt/ie/var/crdb` and note the size of the file.

Restore

1. Login via SSH to the RDC host and verify the file restoration by removing the `crdb` file located at `/opt/ie/var/crdb`.

```

root@CyberSense-host1-93165 backup]# cd /opt/ie/var/crdb/
root@CyberSense-host1-93165 crdb]# ll
total 2188
-rw-r--r-- 1 root root 258048 Oct  9 04:02 crdb
-rw----- 1 root root 266240 Sep 24 02:07 crdb.1
-rw----- 1 root root 110592 Jun 27 02:07 crdb.10
-rw----- 1 root root 94208 Jun 26 02:07 crdb.11
-rw----- 1 root root 90112 Jun  5 08:07 crdb.12
-rw----- 1 root root 253952 Sep 23 02:07 crdb.2
-rw----- 1 root root 229376 Sep 11 02:07 crdb.3
-rw----- 1 root root 110592 Sep  9 02:07 crdb.4
-rw----- 1 root root 110592 Sep  5 02:07 crdb.5
-rw----- 1 root root 110592 Sep  4 02:07 crdb.6
-rw----- 1 root root 110592 Sep  3 02:07 crdb.7
-rw----- 1 root root 90112 Aug 29 02:07 crdb.8
-rw----- 1 root root 139264 Jul  3 02:07 crdb.9
-rw----- 1 root root 266240 Sep 29 02:07 crdb.latest
root@CyberSense-host1-93165 crdb]#
root@CyberSense-host1-93165 crdb]#
root@CyberSense-host1-93165 crdb]#
root@CyberSense-host1-93165 crdb]# rm -rf crdb
root@CyberSense-host1-93165 crdb]# cd
root@CyberSense-host1-93165 ~]#
root@CyberSense-host1-93165 ~]#
root@CyberSense-host1-93165 ~]# cd /opt/ie/var/crdb/
root@CyberSense-host1-93165 crdb]# ll
total 1936
-rw----- 1 root root 266240 Sep 24 02:07 crdb.1
-rw----- 1 root root 110592 Jun 27 02:07 crdb.10
-rw----- 1 root root 94208 Jun 26 02:07 crdb.11
-rw----- 1 root root 90112 Jun  5 08:07 crdb.12
-rw----- 1 root root 253952 Sep 23 02:07 crdb.2
-rw----- 1 root root 229376 Sep 11 02:07 crdb.3
-rw----- 1 root root 110592 Sep  9 02:07 crdb.4
-rw----- 1 root root 110592 Sep  5 02:07 crdb.5
-rw----- 1 root root 110592 Sep  4 02:07 crdb.6
-rw----- 1 root root 110592 Sep  3 02:07 crdb.7
-rw----- 1 root root 90112 Aug 29 02:07 crdb.8
-rw----- 1 root root 139264 Jul  3 02:07 crdb.9
-rw----- 1 root root 266240 Sep 29 02:07 crdb.latest

```

- Run the `cd '/'` command and navigate to the root directory after the file is removed.
- Initiate the restore process in HDPS for the specified Subclient, enable the **Impersonate User** option, and provide the root user credentials.
- After a successful restore, inspect the `/opt/ie/backup` directory. The restored files should be visible:

```

root@CyberSense-host1-93165 ~]# cd /opt/ie/backup/
root@CyberSense-host1-93165 backup]# ll
total 7172
-rw-rw-r-- 1 root root      4 Oct  9 05:12 backup_fmt_version
-rw-rw-r-- 1 root root     11 Oct  9 05:12 backup_version
-rw-rw-r-- 1 root root   5027 Oct  9 05:12 cmvbackup.log
-rw-rw-r-- 1 root root 7275626 Oct  9 05:12 config_save.gz
-rw-rw-r-- 1 root root   2988 Oct  9 05:12 dir_list.txt
-rw-rw-r-- 1 root root  27503 Oct  9 05:12 file_list.txt
-rw-rw-r-- 1 root root     18 Oct  9 05:12 mac_addr
-rw-rw-r-- 1 root root    382 Oct  9 05:13 README
lrwxr-xr-x 32 root root   4096 Oct  9 05:12 stage

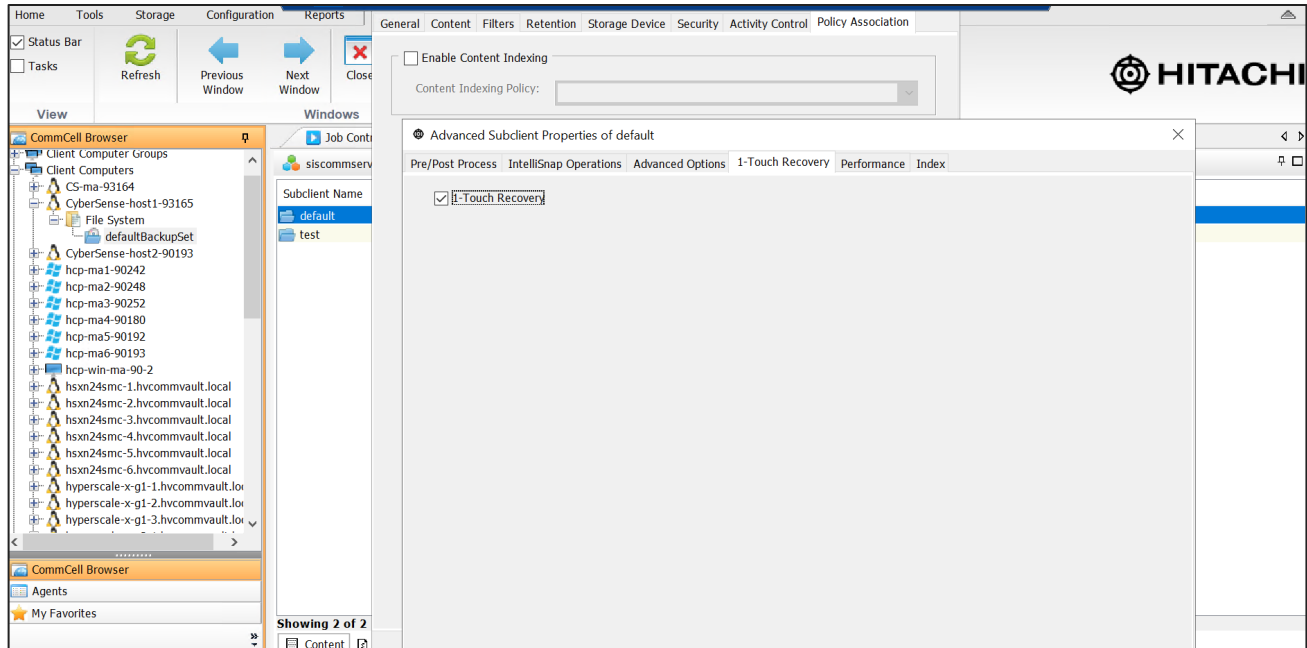
```

- Navigate to the RDC UI and initiate the 'Recover from Backup' operation. When prompted, specify the backup directory path as `/opt/ie/backup`.
- Upon completion of the recovery process, log out of the RDC UI and log back in to verify that the RDC configuration, defined policies, and the `crdb` file located at `/opt/ie/var/crdb` are successfully restored with the original size.

Server-level Backup and Restore

A complete snapshot of the RDC server, including all configuration files and system states, can be backed up and restored. This is ideal for disaster recovery scenarios or full-system migrations. The '1-Touch' feature in HDPS enables automated, bare-metal recovery by capturing a complete image of the server, including the operating system, applications, and configurations, allowing for efficient server-level backup and restoration.

- Login to the HDPS Commcell Console. To facilitate server-level backup and restoration, enable the 1-Touch recovery feature. In the **Commcell Browser**, navigate to **Client Computers > RDC host-1 > defaultBackupSet > Right-click on default subclient > Advanced Settings > 1-Touch Recovery** tab.



2. Initiate the backup operation. The job will run as a '1-Touch Backup'.

Notes:

- To initiate 1-Touch recovery, download the appropriate 1-Touch ISO image corresponding to your HDPS version from the CommVault Store.
 - To bypass DNS resolution during the recovery process, utilize IP addresses consistently and define a custom network topology. Prior to configuring the topology, ensure that client computer groups are created, including entries for the client, infrastructure components, and gateway (proxy) systems.
3. For BIOS boot type, the 1-Touch ISO can be directly attached and booted onto the target Bare Metal server. However, for the UEFI/EFI boot type, the target server must have the OS and HDPS software installed as a prerequisite.
 4. After the OS and HDPS software installation is completed on the target server, follow the steps below:
 - a) Navigate to the following directory - `/opt/hds/iDataAgent/systemrecovery`
 - b) Run the following command to create the single-stage ISO - `./create_1tchbootcd.sh -v 2 -m 0 -s <Client_Name> -c <CommServe_FQDN> -u admin -i <Instance_ID> -n <1-TouchISO_directory>`
 - c) After the successful creation of the single-stage ISO of the backed-up machine, use the ISO to boot the target machine for the recovery process to begin.

The steps to run '1-Touch' recovery are outlined as follows:

1. Begin the '1-Touch' recovery.

```
Linux 1-Touch LiveCD

To start the 1-Touch recovery type default and press <return>.

Available boot options:

    default    - 1-Touch recovery
    serial     - 1-Touch recovery serial console enabled
boot:
Loading vmlinuz... ok
Loading initrd.img..._
```

2. Select the **Interactive** option.

```
No response file detected
Do you want to specify a location ?

[Ok][Interactive][Select Location]
```

- Assign a new IPv4 address to the bare-metal server for post-recovery usage; which ensures it resides within the same gateway network as the backed-up server.

Installation Steps

- 1. Network Config**
2. Client Config
3. COMMServe Config
4. Firewall Config
5. Silent Install
6. Job Selection
7. Initrd recreation

Configure the NICs needed to communicate with the CS and MA

Interface	Bond nic (opt.)	Bond opts (opt.)
eth0		
IP Address		MAC
172.23.91.199		00:50:56:ac:3e:44
Netmask		<input type="checkbox"/> Use Dhcp
255.255.248.0		<input type="checkbox"/> Host Name for this NI
Gateway		HostName
172.23.88.1		
ULAN ID (optional)		Additional route commands

DNS Settings

Search Suffix	Name Server2
Name Server1	Name Server3

[Help for this step] [Prev] [Next]

- Specify the name of the backed-up source server, the target recovery server (after enabling the 'Clone client with a new name' option), and the associated Client Group name.

Installation Steps

1. Network Config
- 2. Client Config**
3. COMMServe Config
4. Firewall Config
5. Silent Install
6. Job Selection

Configure client details and ensure that the hostname specified resolves to this host

Backed up Client Name:
 CyberSense-host1-93165

Current Client Hostname
 (Arrow keys to select or type in other):

Clone client with new name

New Client Name:
 1TouchUM

Is a Metallic client

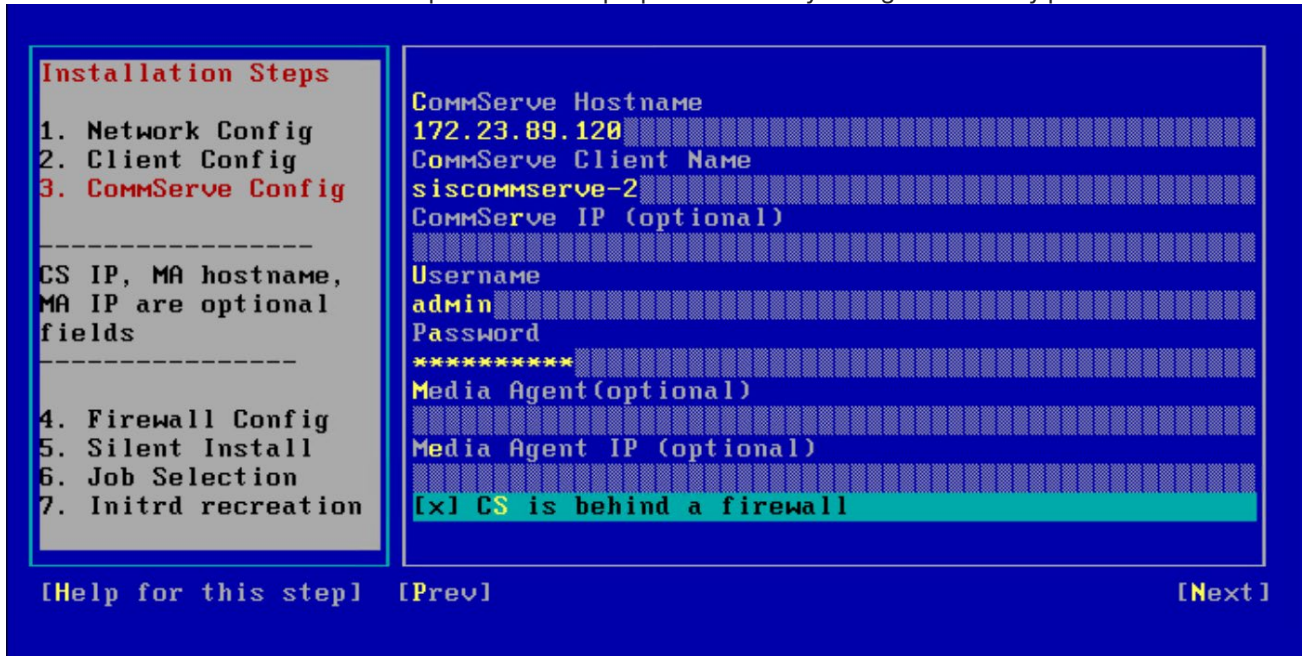
Advanced options (optional)

Client Group Name:
 1T-client

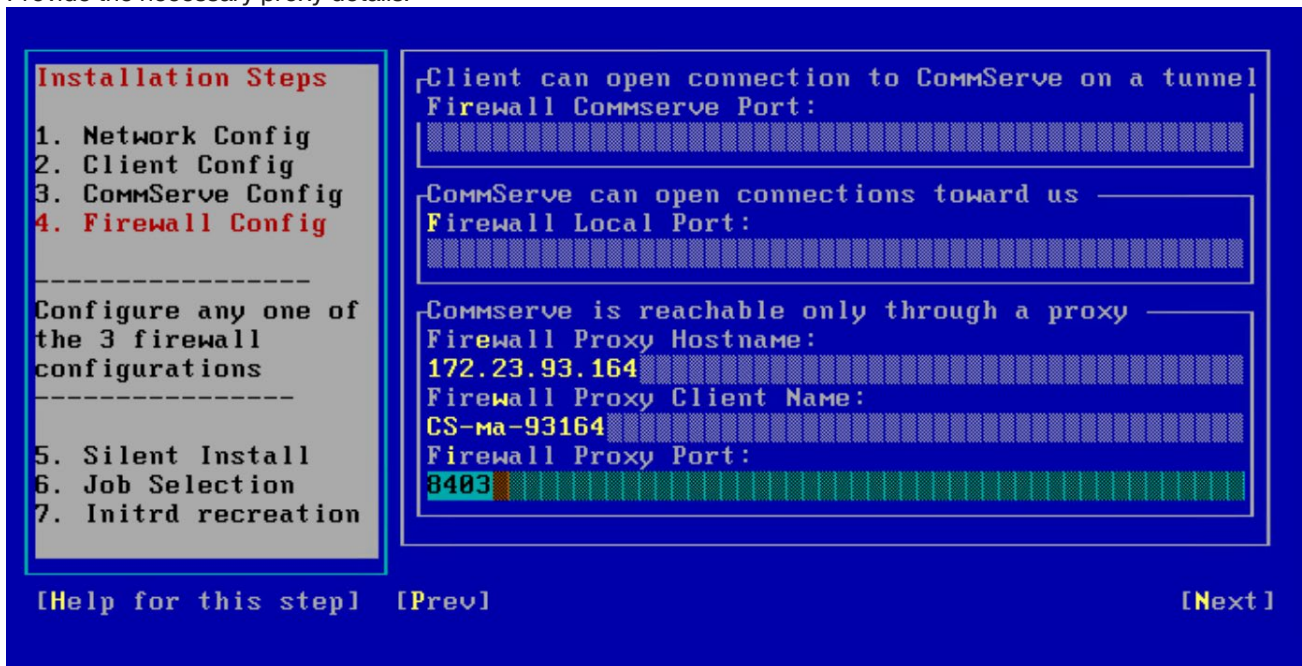
Restore Copy Precedence Number:

[Help for this step] [Prev] [Next]

- Provide the IP address, display name, and authentication credentials for the CommServe server. Additionally, enable the 'CommServe is behind a firewall' option to ensure proper connectivity during the recovery process.



- Provide the necessary proxy details.



Following this step, the installation process will commence. Upon completion, the system will automatically detect the '1-Touch Backup' job and run the corresponding restore operation.

Installation Steps

1. Network Config
2. Client Config
3. COMMserve Config
4. Firewall Config
5. Silent Install
6. Job Selection

Based on the job selected, a restore from point-in-time will be initiated

7. Initrd recreation

BackupSet Name
defaultBackupSet ▾

Select a job to restore system state
[kernel, network, storage ...]

Job Id	Start Date	Start Time	End Date	End Time
9320	2025-08-21	04:54:52	2025-08-21	05:02:42
9306	2025-07-23	06:02:33	2025-07-23	06:42:49

Select a file restore job

Job Id	Start Date	Start Time	End Date	End Time
9320	2025-08-21	04:54:52	2025-08-21	05:02:42
9308	2025-07-23	07:16:28	2025-07-23	07:20:50

[Help for this step]
[Prev]
[Next]

Installation Steps

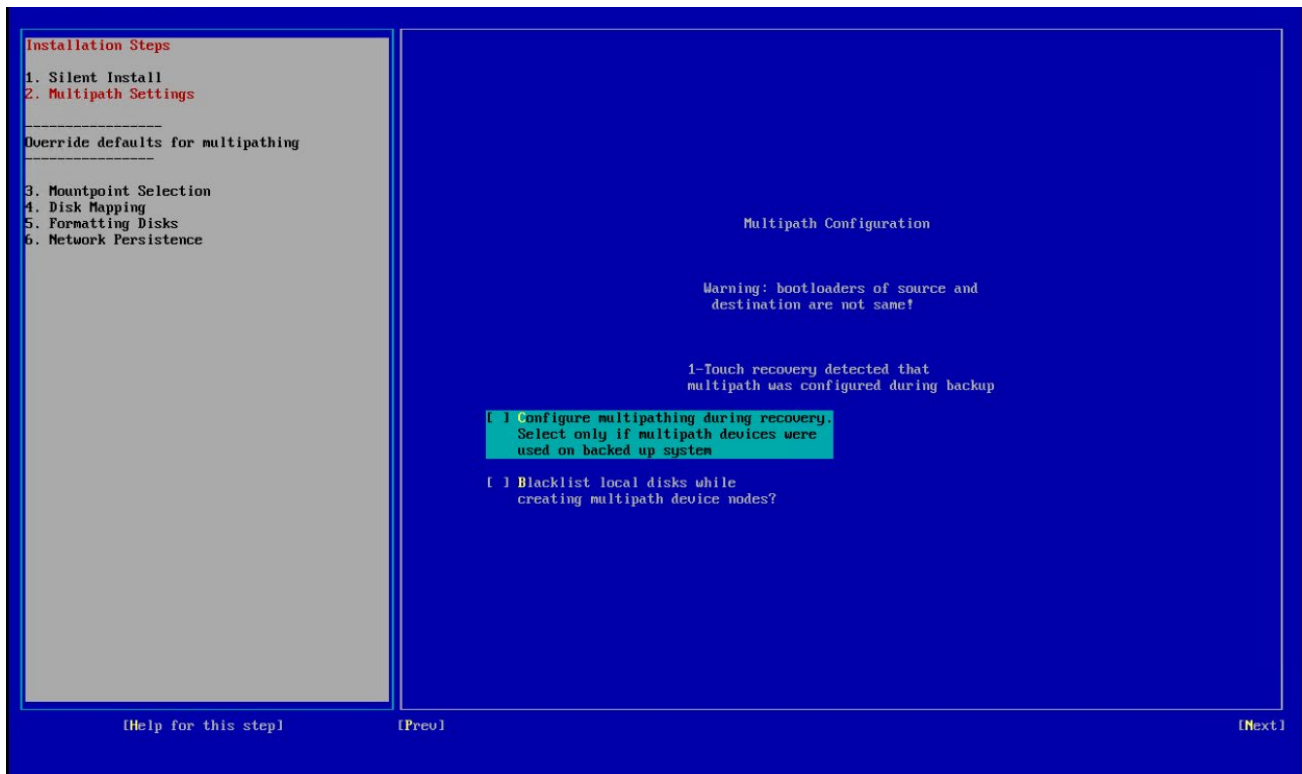
1. Network Config
2. Client Config
3. COMMserve Config
4. Firewall Config
5. Silent Install
6. Job Selection
7. Initrd recreation

Recreate the restored initrd and prepare stage-2 (you will see a reboot)

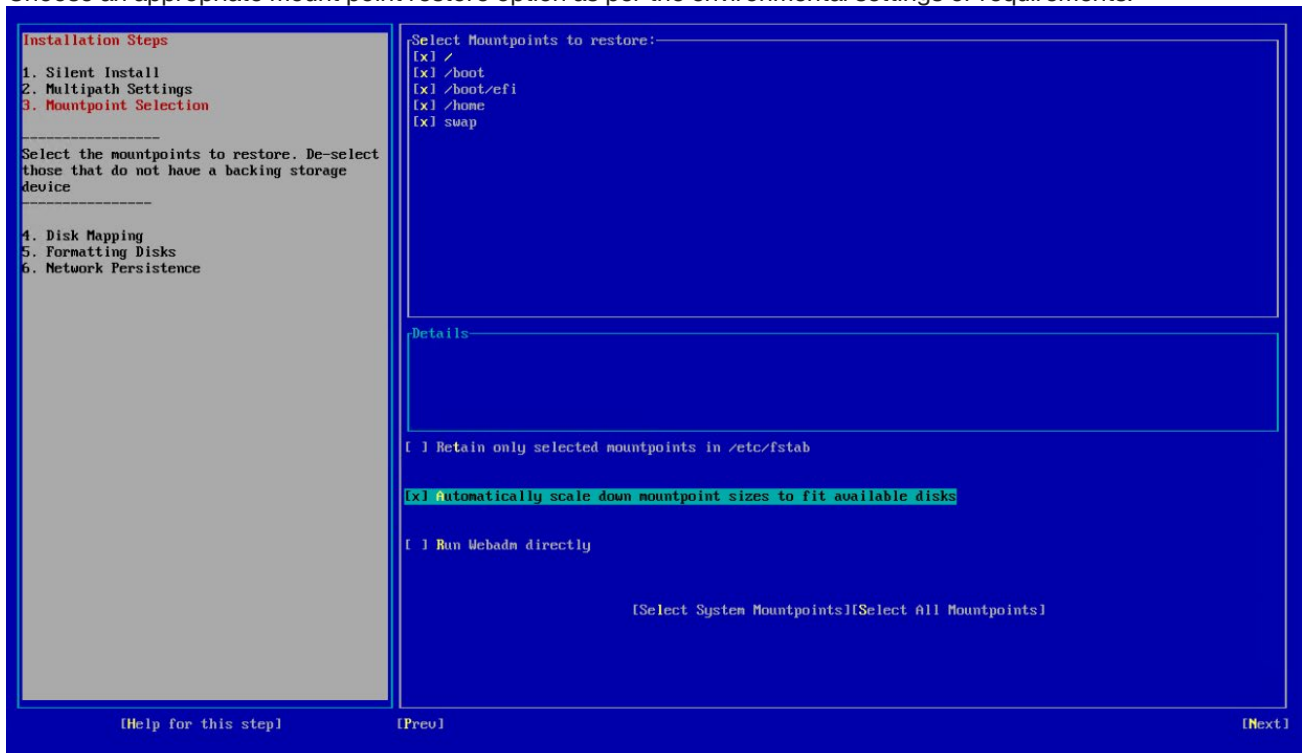
Booting the restored kernel ...

[Help for this step]
[Prev]
[Next]

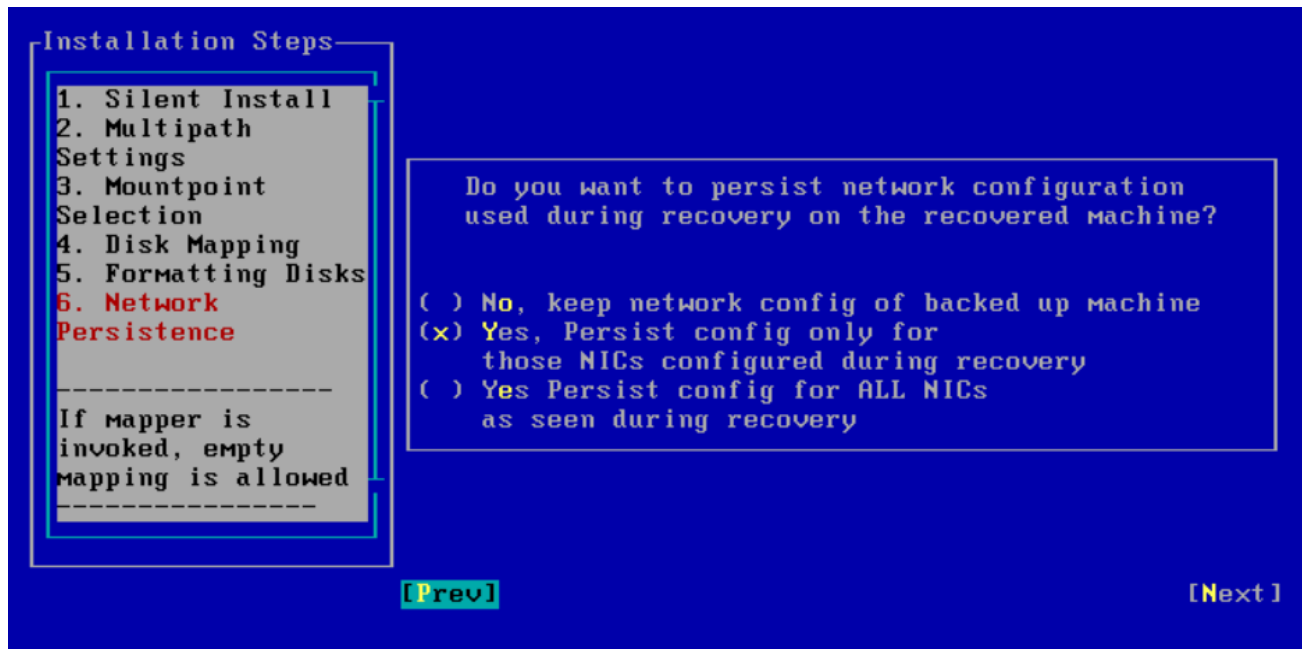
7. Select the appropriate multipathing configuration option (if applicable).



8. Choose an appropriate mount point restore option as per the environmental settings or requirements.



9. Choose an appropriate option for restoring the server's network settings, as per the environmental settings or requirements.



10. Once the 1-Touch recovery is successfully completed, 'ssh' into the target Linux machine and check if all the services are up and running, using the command 'dservice status all'.
11. Use the newly assigned IP of the target server to browse the RDC UI, and verify that all RDC configurations are intact.

Summary

The Ransomware Protection powered by CyberSense: Backup and Restore with HDPS solution is designed to preserve critical RDC configurations, including settings, policies, and analytics, ensuring continuity and disaster recovery readiness. It enables rapid restoration of functionality after system failures or cyber incidents, minimizing downtime and enhancing operational resilience. By guaranteeing consistent configurations across environments, it simplifies recovery processes, reduces manual effort, and mitigates human error. Additionally, it strengthens security by safeguarding configuration data against ransomware or unauthorized changes, delivering a reliable and efficient approach to maintaining system integrity.