TROUBLESHOOTING GUIDE

HYCU Data Protection for Enterprise Clouds v4.7.1

April 2023

HYCU®

Legal notices

Copyright notice

Trademarks

HYCU logos, names, trademarks and/or service marks and combinations thereof are the property of HYCU or its affiliates. Other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

Acropolis and Nutanix are trademarks of Nutanix, Inc. in the United States and/or other jurisdictions.

Amazon Web Services, AWS, and Amazon S3 are trademarks of Amazon.com, Inc. or its affiliates.

Azure®, Microsoft®, Microsoft Edge™, and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Dell Technologies, Dell and other trademarks are trademarks of Dell Inc. or its subsidiaries.

GCP™, Google Cloud Platform™, and Google Cloud Storage™ are trademarks of Google LLC.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Red Hat Enterprise Linux is a registered trademark of Red Hat, Inc. or its subsidiaries in the United States and other countries.

VMware ESXi™, VMware Tools™, VMware vCenter Server®, VMware vSAN™ ,VMware vSphere®, VMware vSphere® Data Protection™, VMware vSphere® Virtual Volumes™, and VMware vSphere® Web Client are registered trademarks or trademarks of VMware, Inc. and its subsidiaries in the United States and other jurisdictions.

NetApp®, NetApp Keystone® , and ONTAP® are trademarks of NetApp, Inc. and are registered in the United States and/or other jurisdictions.

Disclaimer

The details and descriptions contained in this document are believed to have been accurate and up to date at the time the document was written. The information contained

in this document is subject to change without notice.

HYCU provides this material "as is" and makes no warranty of any kind, expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. HYCU shall not be liable for errors and omissions contained herein. In no event shall HYCU be liable for any direct, indirect, consequential, punitive, special or incidental damages, including, without limitation, damages for loss and profits, loss of anticipated savings, business interruption, or loss of information arising out of the use or inability to use this document, or any action taken based on the information contained herein, even if it has been advised of the possibility of such damages, whether based on warranty, contract, or any other legal theory.

The only warranties for HYCU products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty.

Notice

This document is provided in connection with HYCU products. HYCU may have copyright, patents, patent applications, trademark, or other intellectual property rights covering the subject matter of this document.

Except as expressly provided in any written license agreement from HYCU, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property on HYCU products. Use of underlying HYCU product(s) is governed by their respective Software License and Support Terms.

Important: Please read Software License and Support Terms before using the accompanying software product(s).

HYCU
www.hycu.com

Contents

Chapter 1

About HYCU troubleshooting

This guide is designed to help you define the cause and the workaround for any problem that you may encounter when working with HYCU. It provides a list of most common problems and a set of questions that may help you solve a problem on your own. If the information in this guide does not address your particular situation and the problem still persists, this guide will help you determine what information you need to collect before submitting it to HYCU Customer Support for analysis.

When solving a problem, use the following approach:

1. Check if your problem is described in "Known problems and solutions" on page 9 and apply the recommended solution.
2. If you cannot find the problem in the list of known problems, try to solve it on your own.

   When solving a problem on your own, you first need to identify the cause of the problem, collect and analyze all available information about it, and then solve the problem. Answering the following questions may help you to solve your problem:

   a. Is your system up to date?

      Make sure that you apply the most recent updates to your operating system and the most recent HYCU patch because it may contain a software update that solves your problem. In addition, for information about supported environments and compatibility with other products, see the *HYCU Compatibility Matrix*.

   b. Have you made sure that the following does not apply to your problem?

      - You are not running into last-minute limitations and known problems that are described in the *HYCU Release Notes* or Knowledge base.
      - You have the appropriate prerequisite software installed and configured according to the instructions in the *HYCU User Guide*.

   c. Do you receive any errors?

      You can view all events that occurred in your environment in the Events panel. In addition, you can track jobs that are running in your environment and get an insight into the specific job status. For this purpose, use the Jobs panel. For detailed information about events and jobs, see the *HYCU User Guide*.

   d. Can you find information about your problem in log files?

For details about the log files, see "HYCU log files" on page 38.

e. Is your problem related to any third-party hardware or software?

Contact the respective vendor for support.

3. If the problem still persists, contact HYCU Customer Support.

It is recommended that you collect and send the following information to HYCU Customer Support:

- Description of your environment
- Description of your problem
- Log files
- Results of any testing you have done (if available)

The following flowchart shows the major steps of the troubleshooting process:

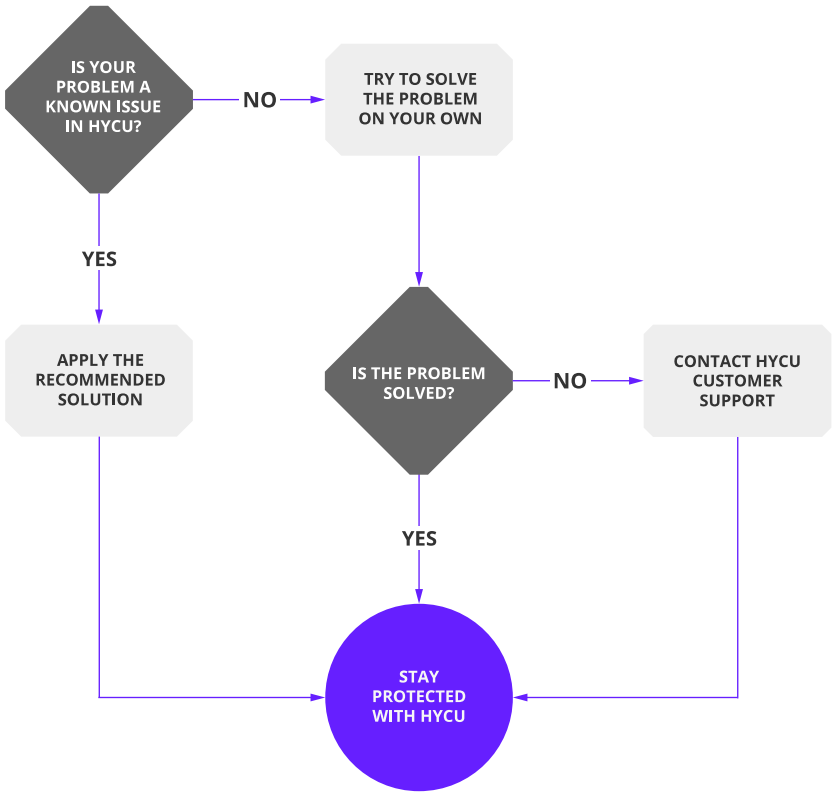

Figure 1–1: Major steps of the troubleshooting process

Chapter 2

Known problems and solutions

When using HYCU, you can encounter some problems and limitations. After you identify the most probable area where the problem originates, search for your problem and its solution. Depending on the area of troubleshooting, see one of the following sections:

Deployment and upgrade problems

This section contains information about troubleshooting deployment and upgrade problems.

For detailed information about deploying the HYCU virtual appliance or upgrading HYCU, see the *HYCU User Guide*.

HYCU web user interface is not accessible after deployment

Problem

After deploying the HYCU virtual appliance, you cannot access the HYCU web user interface.

Cause

There are several potential causes why this problem occurs.

Solution

To solve this problem, do the following:

1. Try to connect to the HYCU web user interface by entering the HYCU URL in a web browser: `https://<IPAddress>:<Port>`. The default port is 8443.

   By doing so, you eliminate your host name not being properly resolved as the cause of the problem.
2. Check your firewall settings to make sure that your firewall allows you to connect to the HYCU URL.
3. Check your browser proxy settings to make sure they do not cause a connection problem.
4. Try to connect to the HYCU web user interface from different virtual machines in your Nutanix environment.
5. If your problem still persists, check the HYCU application server (the Grizzly server) by connecting to the HYCU backup controller virtual machine by using SSH. The default SSH credentials are:

   User name: **hycu**

   Password: **hycu/4u**

   For detailed information about accessing the HYCU backup controller virtual machine by using SSH, see the *HYCU User Guide*.

   After you connect to the HYCU backup controller virtual machine by using SSH, do the following:

   a. Check that the HYCU application server is responding locally:

      ```
      wget --no-check-certificate http://127.0.0.1:8443/rest/v1.0/api-docs -O -
      ```

      The HYCU application server is always listening on port 8443, even if HYCU uses a different external port.

      If the HYCU application server is responding, check the Apache web server.

   b. Check the IP address that HYCU is using:

      ```
      ip address list
      ```

The following is an example of the output:

Example

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_
fast state UP ql en 1000
    link/ether 50:6b:8d:40:e8:b4 brd ff:ff:ff:ff:ff:ff
    inet 10.17.63.199/16 brd 10.17.255.255 scope global eth0
      valid_lft forever preferred_lft forever
```

c. Check the IP address and the port on which the Apache web server is listening:

```
sudo /usr/bin/netstat -nap | grep httpd | grep LISTEN
```

The Apache web server should be listening on the IP address from step 5b, for example:

```
tcp 0 0 10.17.63.199:8443 0.0.0.0:* LISTEN 13687/httpd
```

d. Check if the Apache web server responds locally:

```
wget --no-check-certificate
https://<IPFromStep5b>:<PortFromStep5c>/rest/v1.0/api-docs -O -
```

For example:

```
wget --no-check-certificate
https://10.17.63.199:8443/rest/v1.0/api-docs -O -
```

If HYCU responds locally on the correct IP address, double-check steps 1–4.

If you want to edit the virtual machine network configuration, see the *HYCU User Guide*.

Software upgrade drop-down list is empty

Problem

When trying to upgrade HYCU, the drop-down list of available versions to which you could upgrade HYCU is empty.

Cause

HYCU cannot find an adequate HYCU image in your Nutanix image configuration repository.

Solution

To solve this problem, make sure that when uploading the HYCU virtual appliance image to a Nutanix cluster, you enter the HYCU image name in the format that corresponds to that of the HYCU virtual machine disk image name. For details about uploading the HYCU virtual appliance image, see the *HYCU User Guide*.

Upgrading HYCU fails

Problem

When performing a HYCU upgrade, the upgrade fails.

Cause

There are several potential causes why this problem occurs.

Solution

To solve this problem, follow these steps:

1. Revert the HYCU backup controller to a previous snapshot:
   a. Log on to the Nutanix Prism web console by using your Nutanix logon credentials.
   b. In the menu bar, click **Home**, and then select **VM**.
   c. Click the **Table** tab, and then, from the list of virtual machines, select the HYCU backup controller virtual machine.
   d. Click **VM Snapshots**, and then select the preferred snapshot and click **Restore**.
   e. Click **Power on** to turn on the HYCU backup controller virtual machine.
2. Retry upgrading HYCU.

Logging settings change after upgrading HYCU

Problem

After performing an upgrade, the values of the customized logging settings change to the default ones.

Cause

During the HYCU upgrade, the `logging.properties` file containing the logging settings is overwritten.

Solution

Set up HYCU logging again according to the needs of your data protection environment.

Time zone of the HYCU backup controller in a vSphere environment is not set properly

Problem

The HYCU backup controller does not use the time zone as configured on the vCenter Server.

Solution

If the time zone is properly set on the vCenter Server and the synchronization fails, you can set the time zone using the `vsphere.bc.timezone` configuration setting. For details on how to customize HYCU configuration settings, see the *HYCU User Guide*.

Nutanix REST API v3 problems

This section contains information about troubleshooting Nutanix REST API v3 problems.

Nutanix REST API v3 is not accessible

Problem

When adding a Nutanix cluster to HYCU, the following warning message appears:

```
REST API V3 is not available on the cluster.
```

Cause

HYCU uses REST API v3 for its operations, but this REST API is not active on the Nutanix cluster.

Solution

Make sure REST API v3 is running. To check that it is running, go to the following webpage:

`https://<NutanixCluster>:<NutanixPort>/api/nutanix/v3/api_explorer/index.html`

If REST API v3 is not running, see Nutanix documentation as a reference for further troubleshooting.

Nutanix REST API v3 authentication error

Problem

When adding a Nutanix cluster to HYCU, the following warning message appears:

```
Failed to connect to Nutanix cluster: (401) Unauthorized
```

Cause

The specified password is wrong or the user account that you use to add a Nutanix cluster does not have the required REST API v3 permissions.

Solution

Specify the correct password or the user account that has access to REST API v3 granted.

Keep in mind that REST API v3 can be accessed by:

- Built-in Nutanix Prism admin account

  When specifying the admin user, make sure to use lowercase. Otherwise, REST API v3 cannot be accessed.

- Active Directory user

  To grant a user REST API v3 access to an Active Directory account, do the following:

  1. Link the Nutanix cluster with the Active Directory.
  2. Map the Active Directory account to the Cluster Admin role.
  3. Through the Prism self-service portal, assign SSP administrator privileges to the user.

  For details about the Prism web console, see Nutanix documentation.

Storage problems

This section contains information about troubleshooting storage problems.

Storage containers cannot be mounted when adding a Nutanix cluster

Problem

When adding a Nutanix cluster to HYCU, one of the storage containers cannot be added.

Cause

One of the storage containers has a storage container-level allowlist set that overrides the global allowlist for this storage container.

Solution

HYCU works also if one of the storage containers is not added, but does not list virtual machines that have disks residing on inaccessible storage containers. Therefore, to solve this problem, add HYCU to the container-level allowlist, or remove the container-level allowlist so that the storage container inherits the global allowlist.

Potentially incorrect conclusion about iSCSI target free space due to enabled compression

Problem

If compression is enabled on the storage container that contains your iSCSI target, this might lead to an incorrect conclusion about the actual amount of free space on the target.

Solution

Check the actual amount of free space on the iSCSI target. Keep in mind that compression is enabled only at the storage container level and this does not affect the data size of your iSCSI target, which is represented as a volume group in the storage container. If there is free space on the storage container, you can extend your iSCSI target by either adding a new disk or increasing the size of the existing disks.

For details on how to add a new disk, see Nutanix documentation. For details on how to increase an iSCSI target, see the *HYCU User Guide*.

Network problems

This section contains information about troubleshooting network problems.

NTP synchronization cannot be performed

Problem

Due to NTP synchronization not being performed successfully, the following problems may occur:

- NTP synchronization warning messages appear in the log file.
- The system time on the HYCU backup controller virtual machine is not correct.
- The start and end time of tasks are not correct.

Cause

By default, the HYCU backup controller uses the CentOS NTP servers to synchronize the system time. In some cases, these servers may not be available.

Solution

Add the source where the HYCU backup controller resides to HYCU. By doing so, the HYCU backup controller retrieves the NTP servers from the source and uses them instead of the default ones. For details on how to add a source, see the *HYCU User Guide*.

If the issue persists, check the NTP server settings on the Nutanix cluster. For details, see Nutanix documentation.

Connectivity problems after defining custom network settings

Problem

After editing the HYCU network settings by using the HYCU web user interface, you cannot access HYCU. The problem may occur after changing the main network, upgrading HYCU to a new version, or restoring the HYCU backup controller.

Cause

Network settings are not defined correctly.

Solution

Access the HYCU backup controller virtual machine by using SSH and define the correct network settings. To do so, follow these steps:

1. Open a remote session to the HYCU backup controller virtual machine:

   ```
   ssh hycu@<HYCUBackupControllerIPAddress>
   ```

   When requested, enter the password for the `hycu` user.

2. Open the `ifcfg-mainnetwork.template` file located at `/opt/grizzly/misc/`, and then follow the instructions provided in this document. Make sure to run the specified commands as the root user or by using sudo.

   > ⚠ Important If you have set up HYCU to use multiple networks, make sure to repeat this procedure for each network adapter separately.

Data protection problems

This section contains information about troubleshooting data protection problems.

Application discovery fails on a Windows virtual machine

Problem

After the application discovery is completed, the following error message appears when you hover over the virtual machine row:

```
Discovery failed. Connection error occurred. Please verify virtual
machine's WinRM configuration and accessibility.
```

Cause

There are several potential causes why this problem occurs.

Solution

Before you start solving this problem, do the following:

- Open a remote session to the HYCU backup controller virtual machine and make sure you can ping the virtual machine on which the application is running.
- Make sure you can access the HYCU web user interface from the virtual machine. In a supported browser, enter the following URL:

  ```
  https://<HYCUServer>:8443
  ```

In this instance, <*HYCUServer*> is the HYCU backup controller IP address or host name (for example, `https://hycu.example.com:8443`).

If you cannot access the HYCU web user interface, see "HYCU web user interface is not accessible after deployment" on page 9.

> **Caution** Because this is a case of troubleshooting a third-party problem, keep in mind that the following instructions do not intend to replace instructions in the official Microsoft documentation. Therefore, it is highly recommended to check the Microsoft documentation for any updates.

To solve this problem, open a PowerShell console as an administrator, and then do the following:

1. Make sure that you have PowerShell version 3.0 or later installed. To determine the current version of PowerShell, run the following command:

   ```
   $PSVersionTable
   ```

2. Enable PowerShell script execution. Make sure that PowerShell script execution is not restricted on hosts to be managed. To determine the current execution policy, run the following command:

   ```
   Get-ExecutionPolicy
   ```

   If this command returns Restricted, you will not be able to run scripts. Change the policy to **RemoteSigned** (recommended) or **Unrestricted** by running the following command:

   ```
   Set-ExecutionPolicy {RemoteSigned | Unrestricted}
   ```

3. If you are using a local built-in administrator account, application discovery should work out-of-the-box on Windows Server 2012 and newer releases of Windows Server. On all other supported operating systems, run the following command to configure them to receive remote commands (with the `-Force` option to suppress all user prompts):

   ```
   Enable-PSRemoting -Force
   ```

   If the problem persists, go to the next steps.

4. Verify that WinRM is configured properly:

   a. Verify that the WinRM service is running. To check that the WinRM service is running on the local virtual machine, run the following command:

      ```
      Test-WSMan
      ```

      The following example is a sample output of the `Test-WSMan` command if the WinRM service is running on the local virtual machine:

Example

```
> Test-WSMan
wsmid :
http://schemas.dmtf.org/wbem/wsman/identity/1/wsmanidentity.xsd
ProtocolVersion : http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd
ProductVendor : Microsoft Corporation
ProductVersion : OS: 0.0.0 SP: 0.0 Stack: 3.0
```

If the WinRM service is not running on the local virtual machine, an error message is displayed.

b. Verify that a WinRM listener is configured:

To list all WinRM listeners, run the following command:

```
winrm enumerate winrm/config/listener
```

If this command does not return any output, WinRM is not configured properly. In this case, you can use the following command to automatically configure a listener:

```
winrm quickconfig
```

c. Make sure that WinRM communication is not blocked by a firewall or an antivirus program.

5. Make sure that WinRM access to the user account is granted and the user account is a member of the virtual machine's local Administrators group.

Exchange Server discovery, backup, or restore fails

Problem

A file-level restore fails with the `Unable to connect to the remote server` message.

Cause

During a file-level restore, HYCU cannot use the Windows Remote Management (WinRM) service to download the HYCU restore script from the HYCU virtual machine and execute it on the client virtual machine to restore individual files or folders.

Solution

Make sure that access from the client virtual machine to HYCU is not disabled by a firewall rule. To do so, open a web browser on the Windows client virtual machine and try to access the HYCU web user interface. If there is a problem with the firewall, this attempt will fail, and you must therefore configure the firewall rules to allow access to HYCU.

File-level restore fails with "Unable to connect to the remote server"

Problem

Discovering, backing up, or restoring the Exchange Server applications may fail due to insufficient permissions on Exchange Server.

Cause

If the default Organization Management role group permissions have been changed, they may be insufficient to perform some or all of the following operations with the Exchange Server application: discovery, backup, restore.

Solution

To solve this problem, make sure that the following permissions are enabled in the Organization Management role group: Audit Logs, Compliance Admin, Database Availability Groups, Database Copies, Databases, Disaster Recovery, Distribution Groups, ExchangeCrossServiceIntegration, Information Rights Management, Legal Hold, Mail Enabled Public Folders, Mail Recipient Creation, Mail Recipients, Mail Tips, Mailbox Import Export, Mailbox Search, Message Tracking, Monitoring, Move Mailboxes, MyBaseOptions, MyContactInformation, MyMailboxDelegation, MyName, MyProfileInformation, MyRetentionPolicies, MyTextMessaging, MyVoiceMail, Organization Configuration, Public Folders, Retention Management, Role Management, Security Group Creation and Membership, Support Diagnostics, UM Mailboxes, UnScoped Role, Management, User Options, View-Only Audit Logs, View-Only Configuration, View-Only Recipients.

HYCU fails to perform application-consistent backups from the Virtual Machines panel

Problem

Hovering over the virtual machine row or checking its backup status shows Consistency as crash consistent.

Cause

When you perform backups from the Applications panel, application consistency is ensured by HYCU. However, when you perform backups from the Virtual Machines panel, VSS-based application consistency is achieved by using Nutanix Guest Tools (NGT). Therefore, not having NGT installed and configured on the client virtual machine causes this problem.

Solution

Make sure that the NGT software bundle is properly installed on the client virtual machine. For detailed information about installing, configuring, and troubleshooting NGT, see Nutanix documentation.

Policy cannot be assigned to both a virtual machine and one or more applications running on it

Problem

If you try to simultaneously assign the policy to a virtual machine and one or more applications running on it, the following warning message is displayed:

```
Policy is assigned to virtual machine hosting that application already.
```

Cause

The policy cannot be assigned to both the virtual machine and one or more applications running on it at the same time. Because there is no need to back up the same data twice, the policy can be assigned only to the virtual machine or one or more applications.

Solution

When application discovery is completed, it is recommended that you protect your applications from the HYCU Applications panel. When starting a backup from the HYCU Applications panel, HYCU ensures application consistency and no additional tools need to be installed on the client virtual machine. The same backup will also protect the entire virtual machine that will be visible and restorable from the HYCU Virtual Machines panel.

Backup of file shares to a cloud target fails

Problem

Backing up, copying, or archiving the file share data to a cloud target fails.

Cause

A problem may occur if the names of files, directories, or alternate data streams on the file share contain characters other than the Unicode Basic Multilingual Plane (BMP).

Solution

To solve this problem, make sure that the file system item names on the file share contain only Unicode BMP characters, and then run the backup again.

Antivirus software may recognize HYCU as a threat

Problem

When you perform an application backup or restore, or a file-level restore, some antivirus software may recognize HYCU binaries and data files as a threat.

Cause

HYCU may upload several binaries and data files to the virtual machine. These files are related to the application backup and restore, as well as the file-level restore, and may be treated as a threat by some antivirus software.

Solution

To solve this problem, add the *%ProgramData%*\HYCU folder that contains the uploaded binary files to your antivirus exception list.

Backup fails after restoring a virtual machine in a ROBO environment

Problem

After restoring a virtual machine to its original location in a ROBO environment, the virtual machine backup fails.

Cause

When you restore the virtual machine to its original location, new disk identifiers are generated for the virtual machine. However, because the last available snapshot created during the backup of this virtual machine still has the old disk identifiers, an identifier mismatch occurs and therefore the backup fails.

Solution

After you restore the virtual machine, remove it from the protection domain on the Nutanix cluster, and then add it again to the same protection domain.

Mounting a snapshot for a virtual machine fails

Problem

Mounting a snapshot for a virtual machine fails, resulting in no access to data included in the snapshot.

Solution

To solve this problem, in the `config.properties` file, set the `imagemounter.alwaysinspect` configuration setting to **true**. For details on how to customize HYCU configuration settings, see the *HYCU User Guide*.

Mounting some file systems fails

Problem

Mounting some file systems fails, resulting in not all file systems being visible in the file system hierarchy.

Solution

To solve this problem, in the `config.properties` file, set the `imagemounter.alwaysinspect` configuration setting to **true**. For details on how to customize HYCU configuration settings, see the *HYCU User Guide*.

Virtual machine on a Nutanix ESXi cluster does not boot after a restore

Problem

After you restore a virtual machine on a Nutanix ESXi cluster, the virtual machine does not boot.

Cause

There are several potential causes why this problem occurs (for example, the virtual machine was created by using the vSphere (Web) Client).

Solution

To solve this problem, do the following:

> ⚠ Important You can use either the vSphere Web Client or the vSphere Client as the interface for performing the required steps. As an example, you are guided through the steps that you must perform if you are using the vSphere Web Client.

- If the type of controller on the restored virtual machine is not the same as it was on the original virtual machine, do the following:
  1. Log on to the vSphere Web Client.
  2. Click the **VMs** tab, and then right-click the restored virtual machine and select **Edit Settings**.
  3. On the Virtual Hardware tab, modify the controller settings so that they match the ones on the original virtual machine.
- If the virtual machine uses UEFI firmware, you may need to select the boot file manually. In this case, do the following:
  1. Log on to the vSphere Web Client.
  2. Access the EFI Boot Manager menu, and then do the following:

a. Select the **Enter setup** option.
b. Enter the boot maintenance manager by selecting **Boot option maintenance menu**.
c. Use the **Boot from a File** option to browse for a boot file.
d. Find a device whose name contains the GPT string that represents the boot partition, and then press **Enter** to open it.
e. Navigate to the EFI boot file that you can find at the following location:
   - Windows: `\EFI\Microsoft\Boot\bootmgrfw.efi`
   - Linux: `/EFI/<OSName>/grubx64.efi`
f. Press **Enter** to resume booting.

Linux virtual machines with attached volume groups boot to emergency mode after the restore

Problem

Linux virtual machines with attached volume groups cannot reboot after a restore and go to emergency mode.

Cause

During the reboot process, the virtual machine operating system cannot find some filesystems defined in `/etc/fstab` because these filesystems failed to mount.

Solution

To solve this problem, make sure that all virtual disks belonging to attached volume groups are mounted. For instructions on how to do this, see Linux documentation.

Restoring multiple Exchange Server databases or mailboxes and/or public folders fails

Problem

When restoring multiple databases or mailboxes and/or public folders at the same time, the restore fails.

Solution

To solve this problem, restore the databases or mailboxes and/or public folders one by one.

Problems with protecting virtual machines with more than 15 disks

Problem

When using the default UML mode for the image mounter backend during the backup of virtual machines with more than 15 disks, the backup fails with the following error message:

```
Too many drives have been added, the current backend only supports 15
drives.
```

Cause

The image mounter backend is preset to the UML mode that supports only 15 drives.

Solution

To solve this problem, set the image mounter backend to the direct mode that supports 255 drives. To do so, in the `config.properties` file, set the `imagemounter.backend` configuration setting to `direct`. For details on how to customize HYCU configuration settings, see the *HYCU User Guide*.

Volume group files not available for a restore

Problem

When restoring individual files, the list of files that are available for a restore does not include volume group files although there are volume groups attached to the virtual machine.

Solution

To solve this problem, make sure the `imagemounter.alwaysinspect` configuration setting is set to `true`. For details on how to customize HYCU configuration settings, see the *HYCU User Guide*.

Virtual machine backup fails on a Nutanix ESXi cluster

Problem

When backing up a virtual machine on a Nutanix ESXi cluster, the backup job fails with the following error message:

```
An unexpected error has occurred during execution of job {UUID}
CreateSnapshotTask.
Hypervisor 'ServerName' returned error: The vCenter snapshot associated
with this VM should not exist if you want to proceed with the VM backup.
```

Cause

The virtual machine you are backing up contains one or more snapshots that were created on the vCenter Server to which the Nutanix ESXi cluster is registered.

Solution

To solve this problem, remove all vCenter snapshots associated with the virtual machine you are backing up.

> **Caution** When removing the snapshots, be aware that some of them may be related to the backup jobs of some other applications.

Delays in establishing an SSH connection to Linux systems

Problem

Because establishing an SSH connection to Linux systems is very slow, an `SSH_MSG_UNIMPLEMENTED` error message is displayed, indicating a significant delay in sshd authentication.

Solution

To solve this problem, do one of the following:

- On the SSH server, set the `UseDNS` option to `no` in the `sshd_config file`.
- Increase the value of the `ssh.transport.timeout` configuration setting in the HYCU `config.properties` file. The default timeout (in seconds) used when connecting to the SSH server is 30 seconds. For details on how to customize HYCU configuration settings, see the *HYCU User Guide*.

Application discovery fails due to the Windows Management Instrumentation service not being enabled on the VM

Problem

Application discovery fails with the following error message in the job report:

```
The service cannot be started, either because it is disabled or because it has no enabled devices.
```

Cause

The Windows Management Instrumentation service is not enabled on the virtual machine.

Solution

To solve this problem, make sure remote management is enabled on the virtual machine and the Windows Management Instrumentation service is started and running.

PROTECTED application status changes to PROTECTED_DELETED after removing a source

Problem

If you remove a source from HYCU while the status of the applications is PROTECTED, the status of these applications and the virtual machines on which they are running is changed to PROTECTED_DELETED. If you again add the same source to HYCU, the status of the virtual machines is automatically changed to PROTECTED during synchronization, whereas the status of the applications stays PROTECTED_DELETED, which prevents applications from being protected.

Solution

To solve this problem, run application discovery again. After you do so, the status of the applications is changed to PROTECTED, which allows applications to be protected.

Backups fail for vSphere virtual machines hosted on an NFS datastore

Problem

If your virtual machines are hosted on an NFS datastore, backups fail due to Changed Block Tracking (CBT) issues.

Solution

To solve this problem, follow these steps:

1. Make sure no backups are running.
2. Pause all the HYCU backup controller activities:
   a. In the HYCU web user interface, click ⚙ **Administration**, and then select **Power Options**.
   b. In the Power Options dialog box, select **Suspend**, and then click **Save**.
3. In the HYCU `config.properties` file, set the `vsphere.cbt.backup.entire.disk.enable` configuration setting to `true`. For details on how to customize HYCU configuration settings, see the *HYCU User Guide*.

Nutanix Prism issues volume group space usage warnings

Problem

When running a health check, Nutanix Prism issues warnings about space usage for the volume groups related to HYCU. For example: `WARN: Volume Group hycu-vg-80135991687442 space usage (87 %) above 75 %`

Cause

The space usage of disks in the volume group exceeds 75% of the total capacity of all disks in the volume group. This occurs during a HYCU backup of a virtual machine with disks that are over 75% full, because HYCU creates a snapshot volume group which contains these disks. The warning is displayed as long as this snapshot volume group is present.

Solution

You can safely ignore such warnings, because they do not affect the backup process and the virtual machine protection. To prevent these warnings from being issued, increase the threshold value in the Volume Group Space Usage Exceeded alert policy or enable automatic alert resolution. For details on how to do this, see Nutanix documentation.

Virtual machine backup includes unrelated volume groups

Problem

When you are backing up a virtual machine on which application discovery has been performed, volume groups that are not attached to the virtual machine are also included in the backup.

Cause

The probable cause for this problem is that the virtual machine has been cloned, but its IQN has not been modified and is therefore the same as the one of the original virtual machine.

Solution

To solve this problem, modify the IQN of the cloned virtual machine.

After restoring the HYCU backup controller, the status of the last internal backup job is Error

Problem

After you restore the HYCU backup controller, the status of the last internal backup job shown for the restored HYCU backup controller virtual machine is Error.

Solution

You can safely ignore this error status.

Backups of virtual machines fail occasionally

Problem

When backing up virtual machines, backups fail at various points of the backup process. In the HYCU system logs, iSCSI connection issues are logged.

Cause

The probable cause for this problem is connection issues, one of them being improperly configured HYCU network connections (for example, your HYCU backup controller is not on the same VLAN as the Nutanix Controller virtual machines).

Solution

Set the HYCU VLAN to the proper one by using the Nutanix Prism web console. For details on how to do this, see Nutanix documentation.

If you need a separate VLAN to access the HYCU web user interface, add a secondary NIC and a secondary network device to HYCU. For details on how to do this, see the *HYCU User Guide*.

Size of incremental backups of a Windows physical machine is larger than expected

Problem

The size of the incremental backups of a Windows physical machine can be significantly larger than expected considering I/O load since the last backup.

Solution

To solve this problem, do the following:

- Make sure that defragmentation does not occur in the interval between incremental backups. Because defragmentation moves blocks across a volume, on heavily fragmented volumes, the defragmentation process can have a significant effect on the

size of incremental backups.

- Under some circumstances, blocks allocated for the VSS snapshot storage area are collected during an incremental backup. In this case:
  1. View the limit of the allocated, used, and maximum VSS snapshot storage area by running the `vssadmin list shadowstorage` command.
  2. Limit the effect on incremental backups by setting the maximum size for the VSS snapshot storage area for every volume (by default, it is unlimited and the system can allocate a significant amount of blocks for it). To manage the VSS snapshot storage area, use the `vssadmin list/add/delete shadowstorage` commands.

     > Note When setting the maximum VSS storage area size, consider the amount of write I/O to a volume during the snapshot lifetime. If there is not enough space in the snapshot storage while the snapshot is in use, reading data from the snapshot will fail, which will result in a failed backup.

"Aged third-party backup snapshots present" alert is issued in the Nutanix Prism web console for Nutanix ESXi clusters

Problem

The following alert is issued in the Nutanix Prism web console for the snapshots that are created by HYCU:

```
Aged third-party backup snapshots present
```

Cause

HYCU automatically creates a snapshot every time you restore data from a restore point that does not contain the Snapshot tier itself and keeps it for the time period specified in the RPO setting increased by 24 hours. This results in HYCU requiring less time to perform a subsequent restore. Such snapshots are then displayed in the Nutanix Prism web console as volume groups and, by default, an alert is issued if they are present there for more than seven days.

Solution

You can safely ignore these alerts. However, if you do not plan to use such a restore point for restoring data, you can at any time mark it as expired and prevent this information from appearing in the Nutanix Prism web console. For details on how to do this, see the *HYCU User Guide*.

Virtual machine discovery job completes with a warning message indicating an issue with obtaining the iSCSI IQN

Problem

The virtual machine discovery job completes with a warning message indicating an issue with obtaining the iSCSI IQN of the Windows virtual machine. Because of this, HYCU cannot perform a restore of individual files with improved performance.

Cause

One of the potential causes is that the WMI repository is corrupted.

Solution

To solve this problem, from the command prompt, run the following commands:

1. `winmgmt /salvagerepository` to rebuild the repository.
2. `winmgmt /verifyrepository` to verify that the repository was rebuilt successfully.

For details on how to rebuild the WMI repository, see Microsoft documentation.

Nutanix Prism issues a warning about the backup schedule not being configured properly

Problem

On a Nutanix ESXi cluster, a warning is issued due to no schedules being attached to a HYCU protection domain (the backup schedule is not configured properly).

Solution

To solve this problem, do the following:

1. Suspend all HYCU activities. For details, see the *HYCU User Guide*.
2. Delete the HYCU protection domain. For details, see Nutanix documentation.
3. Resume the HYCU activities. For details, see the *HYCU User Guide*.

> **Note** If such a protection domain is required later for data protection purposes, HYCU will recreate it automatically.

Auditing system alerts issued for SMB targets

Problem

The auditing system alerts you about the potential violations of your system security due to anonymous login attempts on your SMB target.

Cause

As part of the ransomware protection feature, HYCU is by default configured to use an anonymous login to check if public access is enabled for an SMB target that will be used as a location for storing the data.

Solution

Disable the public access check for the affected SMB target. To do so, set the `target.ransomware.prevention.check` configuration setting to `false`. For details on how to customize HYCU configuration settings, see the *HYCU User Guide*.

> ⚠ Important By disabling the public access check, you disable the ransomware protection feature provided by HYCU that helps you to detect if public access is enabled for your SMB targets. In this case, HYCU stops issuing warning messages to notify you to adjust the security settings to restrict access to data.

Backup of an SQL Server application fails

Problem

The backup of an SQL Server application fails and the following message is displayed in the `hycuvdi` logs:

```
Cannot create worker thread.
```

Cause

The backup fails because not enough SQL Server worker threads can be created.

Solution

To solve this problem, in SQL Server, increase the value of the `max worker threads` option to a value that equals the sum of the number of the databases in the SQL Server instance multiplied by three and the default number of threads.

Several data protection actions fail on Windows due to the misconfigured PowerShell plugin

Problem

For Windows, discovering applications, restoring applications and individual files, as well as backing up physical machines fail with the following error:

```
Action CREATE failed: Unable to load assembly "-" specified in
"InitializationParameters" section
```

Cause

The PowerShell plugin configuration contains invalid values, which is commonly caused by a mistyped `Set-PSSessionConfiguration` command.

Solution

To solve this problem, you must first remove the invalid values, and then restart the WinRM service. To do so, on your Windows virtual machine, launch an administrative PowerShell prompt, and then run the following commands:

```
Remove-Item -Path wsman:\localhost\plugin\microsoft.powershell\
InitializationParameters\assemblyname
```

```
Remove-Item -Path wsman:\localhost\plugin\microsoft.powershell\
InitializationParameters\pssessionconfigurationtypename
```

```
Restart-Service winrm
```

Backup or archiving task of an Azure Government virtual machine fails with timeout

Problem

A backup or an archiving task of an Azure Government virtual machine fails with the following error message:

```
An error occurred while backing up disk 'DiskName' to target 'TargetName':
java.io.IOException: Reached max number of retries for blob download
request (3)
```

Cause

In some cases, the default number (3) of blob download requests HYCU sends to Azure Government is insufficient, or the time interval between retries is too short to successfully complete the task.

Solution

To solve this problem, in the `config.properties` file, adjust the `target.azure.retry.limit` configuration setting to increase the number of retries, or the `target.azure.retry.after.mseconds` configuration setting to increase the time interval between retries. For details on how to customize HYCU configuration settings, see the *HYCU User Guide*.

Application discovery fails when using WinRM with HTTPS

Problem

Discovering applications running on a Windows virtual machine fails with a Wrong credentials error message if the virtual machine is assigned WinRM credentials that use HTTPS. The same credentials work through WinRM using HTTP.

Cause

The HYCU NTLM client used for NTLM authentication with Windows virtual machines does not support channel binding. If the Windows virtual machine is configured with the `CbtHardeningLevel` setting set to `Strict`, NTLM authentication over HTTPS will fail.

This setting can be checked by running the following command in the PowerShell prompt on the Windows virtual machine:

```
Get-Item
Microsoft.WSMan.Management\WSMan::localhost\Service\Auth\CbtHardeningLevel
```

Solution

To solve this problem, set the `CbtHardeningLevel` setting to `Relaxed`. Depending on how this setting is applied, do one of the following:

- *Directly on the virtual machine:* Run the following command in the PowerShell prompt on the Windows virtual machine:

  ```
  Set-Item
  Microsoft.WSMan.Management\WSMan::localhost\Service\Auth\CbtHardeningLevel
  Relaxed
  ```

- *By using Group Policy:* Override the `CbtHardeningLevel` setting to `Relaxed` for the affected Windows virtual machine.

Errors are reported during generic file share backup

Problem

When protected files stored on a generic file server are changed during the backup (when a file is added, deleted, or modified), the backup job report includes errors stating that the backup was only partially successful.

Cause

Generic file servers do not support snapshots. If users change any of the protected files during the backup, this might affect the backup process outcome.

These are the most probable cases of data changes and their effect on the backup:

- If new files are added during the backup, the newly added files are not backed up immediately, but during the next incremental backup.
- If existing files are deleted during the backup, the backup job reports partial success.
- If files are changed after cataloging and before the backup, the backup result depends on the final data size:
  - If the data size remains unchanged, the data is successfully backed up.
  - If the data size changes, the backup job reports partial success.

- If existing files are changed during the backup, the backed up data may be inconsistent or only partially backed up.

Solution

If you store the protected file shares on a generic file server, avoid making any actions to the files during the backups.

Policy cannot be assigned to an SQL Server instance after the upgrade

Problem

After upgrading HYCU, a policy cannot be assigned to an already discovered SQL Server instance that is part of an Always On Availability Group.

Solution

To solve this problem, reassign credentials to the SQL Server instance.

Virtual machine running on a Nutanix ESXi cluster cannot be restored after the upgrade

Problem

After upgrading HYCU, a virtual machine running on a Nutanix ESXi cluster cannot be restored.

Solution

To solve this problem, make sure the storage container to which you want to restore data is mounted on ESXi hosts. For details on how to mount the storage container on the hosts, see Nutanix documentation.

Web user interface problems

This section contains information about troubleshooting HYCU web user interface problems.

Slow HYCU web user interface response

Problem

When using an AWS S3/Compatible or Azure target for storing your protected data, the HYCU web user interface is slow to respond if multiple concurrent backup jobs are running.

Solution

To solve this problem, do the following:

1. Add more CPU cores to the HYCU backup controller (at least one CPU core per concurrent backup job, in addition to the minimum number of 4 CPU cores required for HYCU).
2. Reduce the number of concurrent I/O requests by editing the value of the `backup.restore.cloud.num.of.io.requests` configuration setting in the HYCU `config.properties` file. The default value is 8 and it is recommended that the value you set for this configuration setting never exceeds the default value.

   For details on how to customize the HYCU configuration settings, see the *HYCU User Guide*.

Authentication problems

This section contains information about troubleshooting authentication problems.

Registering a FIDO authenticator fails due to IP configuration issues

Problem

When registering a FIDO authenticator, the process fails with the following error:

```
FIDO is not configured correctly. Contact system administrator.
```

```
Reverse lookup of IP doesn't work.
```

The most probable cause is that the hostname is not properly resolved by the DNS.

Solution

To solve this problem, set the value for the configuration setting `fido.rp.id` to the fully qualified domain name of the backup controller.

For details on how to customize the HYCU configuration settings, see the *HYCU User Guide*.

Browser URL mismatch is reported when using a FIDO authenticator

Problem

When registering a FIDO authenticator or when you log on to HYCU, the process fails with the following error:

```
Browser's URL doesn't match backup controller's FIDO relying party ID!
```

The most probable cause is that you did not enter a fully qualified domain name when logging on to HYCU.

Solution

To solve this problem, use a fully qualified domain name of the HYCU server when entering the URL in the browser.

After entering the wrong credentials, logging on to the HYCU backup controller fails when the correct credentials are provided

Problem

After you enter a wrong user name or password several times when logging on to the HYCU backup controller, you cannot log on to the HYCU backup controller with the correct credentials.

Cause

By default, after three failed log on attempts, you are prevented from logging on to the HYCU backup controller for 15 minutes.

Solution

Wait until the end of the required lock period.

> **Note** If required, you can adjust the default lock interval and the maximum number of failed log on attempts by setting the following variables:
> `login.lock.interval.minutes`
> `login.max.failed.count`
>
> For detailed information about customizing HYCU configuration settings, see the *HYCU User Guide*.

After entering the wrong credentials, adding a Nutanix Files server fails when the correct credentials are provided

Problem

After you enter the wrong user name or password several times when adding a Nutanix Files server, the connection fails when you enter the correct credentials.

Cause

After several failed attempts to provide the correct credentials, services may prevent you from trying again for a certain period for security reasons.

Solution

Wait until the lock period expires before you try again.

> Note The duration of the period during which you are prevented from providing credentials depends on your Nutanix Files settings. For details, see Nutanix documentation.

Chapter 3

Solving problems on your own

If you cannot find your problem described in the list of known issues with HYCU, many times you can identify the cause of the problem and solve the problem on your own. For example, you can do this by verifying that your system is up to date, checking error messages, viewing log files, and so on.

HYCU log files

If you encounter a problem when using HYCU, the information in log files can help you determine the symptom of the problem.

> Accessing the Logging dialog box
>
> To access the Logging dialog box, click ⚙ **Administration**, and then select **Logging**.

In the Logging dialog box, you can do the following:

- Download and view the existing log file by clicking **Get logs**.

  You download log files with the level that was specified at the time they were recorded. If logging is not set up, the log files are downloaded with the default settings. The changed logging level is applied only to the log files that are recorded after you save new logging settings.

  After you extract the `zip` file, check the log files at the following location:

  `/opt/grizzly/logs/`

- *Only if Sharing telemetry data with HYCU is enabled.* Send the existing log file to HYCU Customer Support by clicking **Send logs**.

  You send log files with the level that was specified at the time they were recorded. If logging is not set up, the log files are uploaded with the default settings. The changed logging level is applied only to the log files that are recorded after you save new logging settings.

- Set up logging. To do so, follow these steps:
  1. Specify values for the following logging settings:

Logging setting	Description
Maximum log file size (MiB)	The maximum size of a log file. The default log file size is 10 MiB, whereas the maximum log file size is 10 GiB.
Number of log files	The number of log files. The default number is 9.
Level	The following logging levels are available: ◦ `Informational` (default): Informational messages about the operation of HYCU are recorded to log files. ◦ `Detailed`: All activity is recorded to log files.
Outbound REST call level *(Available only if the Detailed logging level is selected.)*	The following levels are available: ◦ `Off` (default): Outbound REST call logs are not recorded to log files. ◦ `Informational`: Informational messages about the operations related to outbound REST calls are recorded to log files. ◦ `Detailed`: All activity related to outbound REST calls is recorded to log files.
Inbound REST call level *(Available only if the Detailed logging level is selected.)*	The following levels are available: ◦ `Off` (default): Inbound REST call logs are not recorded to log files. ◦ `Informational`: Informational messages about operations related to inbound REST calls are recorded to log files. ◦ `Detailed`: All activity related to inbound REST calls is recorded to log files.

  2. Use the **Keep settings after upgrade** switch if you want the custom logging settings to remain the same after you upgrade HYCU. As you usually set logging for troubleshooting purposes and do not need the same logging level for regular use of the product, by default, this switch is turned off.
  3. Click **Save**.

     > Note Keep in mind that the changed logging level is applied only to the log files that are recorded after you save new logging settings.

In addition, you can find the HYCU command-line user interface (hyCLI) log files at `.Hycu/log` under your home directory.

Provide feedback

For any suggestions and comments regarding this product or its documentation, send us an e-mail to:

info@hycu.com

We will be glad to hear from you!

www.hycu.com

HYCU®