Release 10.1.1-3 | Version 3.05042018



UNITRENDS

Provide feedback

Copyright

Copyright © 2018 Unitrends Incorporated. All rights reserved.

Content in this publication is copyright material and may not be copied or duplicated in any form without prior written permission from Unitrends, Inc ("Unitrends"). This information is subject to change without notice and does not represent a commitment on the part of Unitrends.

The software described in this publication is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of the license agreement. See the End User License Agreement before using the software.

The software described contains certain open source components that are copyrighted. For open source licenses, see the UnitrendsOpen Source Compliance section of the product Administrator Guide.

Because of the nature of this material, numerous hardware and software products are mentioned by name. In most, if not all, cases these product names are claimed as trademarks by the companies that manufacture the products. It is not our intent to claim these names or trademarks as our own.

The following applies to U.S. Government End Users: The Software and Documentation are "Commercial Items," as that term is defined at 48 C.F.R.2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R.12.212 or 48 C.F.R.227.7202, as applicable. Consistent with 48 C.F.R.12.212 or 48 C.F.R.227.7202 1 through 227.7202 4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Unpublished rights reserved under the copyright laws of the United States. Unitrends agrees to comply with all applicable equal opportunity laws including, if appropriate, the provisions of Executive Order 11246, as amended, Section 402 of the Vietnam Era Veterans Readjustment Assistance Act of 1974 (38 USC 4212), and Section 503 of the Rehabilitation Act of 1973, as amended, and the regulations at 41 CFR Parts 60 1 through 60 60, 60 250, and 60 741. The affirmative action clause and regulations contained in the preceding sentence shall be incorporated by reference.

The following applies to all contracts and subcontracts governed by the Rights in Technical Data and Computer Software Clause of the United States Department of Defense Federal Acquisition Regulations Supplement:

RESTRICTED RIGHTS LEGEND: USE, DUPLICATION OR DISCLOSURE BY THE UNITED STATES GOVERNMENT IS SUBJECT TO RESTRICTIONS AS SET FORTH IN SUBDIVISION (C)(1)(II) OF THE RIGHTS AND TECHNICAL DATA AND COMPUTER SOFTWARE CLAUSE AT DFAR 252 227 7013. UNITRENDS CORPORATION IS THE CONTRACTOR AND IS LOCATED AT 200 WHEELER ROAD, NORTH TOWER, 2ND FLOOR, BURLINGTON, MASSACHUSETTS 01803.

Unitrends, Inc 200 Wheeler Road North Tower, 2nd Floor Burlington, MA 01803, USA Phone: 1.866.359.5411



Contents

Chapter 1: Introduction
Chapter 2: Getting Started with AHV Protection
Requirements and considerations for AHV protection
AHV best practices and considerations
General AHV requirements
Hot backup copy limitation12
Install the 10.1.1-3 release
Add the Nutanix AHV host cluster
Run AHV backups
Next Steps
Chapter 3: Recovering AHV Backups
Recovering an AHV VM
Recovering files from a host-level backup of a Windows AHV VM
Windows prerequisites and considerations
Windows file-level recovery41
Step 1: Create the recovery object41
Step 2: Recover files43
Step 3: Remove the recovery object from the appliance51
Recovering files from a host-level backup of a Linux AHV VM52
Linux prerequisites and considerations52
Linux file-level recovery
Step 1: Create the recovery object54
Step 2: Recover files
Step 3: Remove the recovery object from the appliance
Chapter 4: Managing AHV Hosts and Virtual Machines65
Chapter 5: Working with Custom Filters in the Backup Catalog71

This page is intentionally left blank.

Chapter 1: Introduction

Release 10.1.1-3 introduces host-level protection of Acropolis Hypervisor (AHV) virtual machines. With hostlevel protection, virtual machines are backed up by leveraging AHV snapshots. Simply add the AHV host cluster to the Unitrends appliance. All VMs are automatically discovered and you can select them for protection. For details on installing this release, see "Getting Started with AHV Protection" on page 7.

In addition to AHV protection, this release includes:

- An updated Unitrends Windows agent. If you are protecting Windows machines by running asset-level backups, install this new agent after you upgrade the Unitrends appliance. For details, see "To install the 10.1.1-3 Windows agent" on page 17.
- A new custom filters feature you can use to quickly filter the backups and backup copies that display in the Backup Catalog. See "Working with Custom Filters in the Backup Catalog" on page 71 for details.
- New filter fields on the Jobs tabs. Enter text in these fields to filter the jobs that display.
- Fixes for customer-discovered issues. For details on issues that were resolved in this release, see the 10.1.1-3 Release Notes.

This page is intentionally left blank.



Chapter 2: Getting Started with AHV Protection

To start protecting your AHV virtual machines with the 10.1.1-3 release:

- **Step 1:** Review the "Requirements and considerations for AHV protection"
- Step 2: Review the "Getting Started with AHV Protection"
- **Step 3:** "Install the 10.1.1-3 release" on page 13
- Step 4: "Add the Nutanix AHV host cluster" on page 20
- Step 5: "Run AHV backups" on page 22

Requirements and considerations for AHV protection

Review the information in these topics before implementing AHV host-level protection:

- "AHV best practices and considerations"
- "General AHV requirements" on page 8
- "Hot backup copy limitation" on page 12

AHV best practices and considerations

Follow these best practices to protect your AHV virtual machines:

- Adhere to Nutanix best practices.
- Full and incremental backups are supported for AHV VMs.
- A new full backup is required if the VM configuration has changed since the last backup. This includes any configuration changes made to a VM through the hypervisor, such as creating or deleting a snapshot, or adding a new disk.

If the VM configuration has changed since the last backup, the next incremental fails. After this failure, the appliance promotes the next scheduled backup to a full (or displays a message indicating a full is required if an on-demand incremental is attempted). Once a full backup succeeds, subsequent incrementals run as scheduled.

- Due to a Nutanix limitation, Unitrends AHV snapshots do not display in the Nutanix AHV hypervisor. Note the following:
 - The first time a VM is backed up, the job creates a new snapshot of the AHV VM that remains with the VM after the job completes. During subsequent backups, the job creates a new snapshot of the AHV

7

VM, performs the backup, then removes either the previous snapshot (if the job was successful) or the current snapshot (if the job failed). If a job ends ungracefully (such as due to a power outage) the unneeded snapshot may remain on the hypervisor. A Unitrends cleanup process runs hourly to check for and remove any unneeded snapshots.

- If you are no longer protecting a VM on this Unitrends appliance, any leftover snapshot that has not been removed will remain on the hypervisor. This applies even if you begin protecting the VM with another Unitrends appliance. If you are no longer protecting a VM with the original Unitrends appliance, contact Support for assistance removing any unneeded snapshots.
- In some cases, you may want or need to protect VMs by using asset-level backups. To protect a VM with both host-level and asset-level (agent-based) backups, ensure that the VM's host-level and asset-level jobs do not overlap. Running both simultaneously may lead to undesirable results.

General AHV requirements

The following requirements must be met for host-level protection of AHV virtual machines.

ltem	Description
Unitrends appliance	The Unitrends appliance must be running version 10.1.1-3. After you install the 10.1.1-3 version, you must enable the AHV feature as described in step 9 on page 15 in the "To install release 10.1.1-3 on a Unitrends appliance" procedure.
	The Unitrends appliance must be running an Enterprise or Enterprise Plus license.
Nutanix AHV host cluster version	The AHV host must be running Acropolis Operating System (AOS) version 5.1.4 or higher.



Release 10.1.1-3 | April 2018

ltem	Description
AHV host account privileges	While adding the AHV cluster to the Unitrends appliance (described in "Add the Nutanix AHV host cluster" on page 20), you must enter the username and password credentials of one of the following AHV cluster accounts:
	• The Nutanix cluster admin account – You must use this account if the AHV cluster is not configured to use directory services authentication and the cluster is running a pre- 5.5 AOS release. Other user accounts with full administrative privileges are not supported.
	• Any local Nutanix cluster account that has been assigned the user admin or cluster admin role – Use a local account with either of these roles if the AHV cluster is not configured to use directory services authentication and the cluster is running AOS release 5.5.
	• An LDAP user that has the cluster admin role – Use this account if your AHV cluster is configured to use directory services authentication. See these topics for additional requirements: "Requirements for directory services authentication in AOS 5.1" or "Requirements for directory services authentication in AOS 5.5".
	Requirements for directory services authentication in AOS 5.1
	These additional requirements apply to Nutanix AHV clusters running in AOS 5.1 that are configured to use directory services authentication:
	• Set up authentication (as described in this Nutanix document: <u>Configuring</u> <u>Authentication</u>) to use these settings:
	 In the Directory List add a new directory of type Active Directory and connection LDAP. For the Directory URL, specify Idap://<ip-address>:<port></port></ip-address>
	- Create a role mapping for the LDAP user and assign the cluster admin role.
	 In the self service portal (SSP), set or update the SSP administrators to the user@domain. Use fully qualified domain names.
	 SSP will need to query the active directory for details of users. Ideally a service account with no time limit should be used. This account must have privileges for listing the users in the Directory server.
	• While adding the AHV cluster to the Unitrends appliance (described in "Add the Nutanix AHV host cluster" on page 20), you must specify a domain in addition to the username. The username and domain are case sensitive. Be sure to match the case that was entered in the self service portal (SSP). In the Username field, enter the username and

ltem	Description
	domain in this format: user@domain. For example, jalvarez@unitrends.com
	Requirements for directory services authentication in AOS 5.5
	These additional requirements apply to Nutanix AHV clusters running in AOS 5.5 that are configured to use directory services authentication:
	 Set up authentication (as described in this Nutanix document: <u>Configuring</u> <u>Authentication</u>) to use these settings:
	 In the Directory List add a new directory of type Active Directory and connection LDAP. For the Directory URL, specify Idap://<ip-address>:<port></port></ip-address>
	- Create a role mapping for the LDAP user and assign the cluster admin role.
	 While adding the AHV cluster to the Unitrends appliance (described in "Add the Nutanix AHV host cluster" on page 20), you must specify a domain in addition to the username. In the Username field, enter the username and domain in this format: user@domain. For example, jalvarez@unitrends.com

Chapter 2: Getting Started with AHV Protection Provide feedback



Release 10.1.1-3 | April 2018

ltem	Description
iSCSI target access	 AHV backup and recovery jobs access the AHV host over the iSCSI protocol. Ensure the following: The Unitrends appliance is able to connect to the iSCSI targets on the Nutanix storage LAN. iSCSI Data Services are configured for the Nutanix AHV cluster. To configure this setting: In the Nutanix Prism interface, select Cluster Details from the Options menu. Enter the iSCSI Data Services IP address.
	S CICK SAVE. Nutanix01 Home
Virtual machine storage	 The following requirements apply to virtual machine storage: Virtual machine storage must be disk storage allocated on a storage container. VM disks that are attached to a Volume Group are not included in the backup. Host-level protection is not supported for independent and pass-through disks. To protect these disks, you must install a Unitrends agent and use asset-level backups instead.

11

ltem	Description
Virtual machine configuration	The following VM configuration requirements must be met for Unitrends host-level protection:
	• Nutanix recommends installing Nutanix Guest Tools (NGT) in the guest operating system to ensure file system and application consistency.
	 NGT tools must be installed and running to enable application consistent quiesce. If NGT is not running, crash consistent quiesce is used. For details, see this Nutanix document: <u>Nutanix Guest Tools</u>.
	 For Windows guests, Nutanix recommends installing VirtIO drivers for enhanced performance and stability. For details, see this Nutanix document: <u>Nutanix Virtio for</u> <u>Windows</u>.
Virtualized Active Directory servers	To ensure database consistency, you must set up the virtualized Active Directory (AD) server in accordance with Microsoft best practices. If all Microsoft considerations are not addressed, backup and restore of the virtual machine may yield undesired results. If you prefer not to research these best practices, install the agent on the VM and protect it as you would a physical server (leveraging Microsoft's VSS writers).
Distributed File System environments	Distributed File System (DFS) Namespaces and DFS Replication offer high-available access to geographically dispersed files. Because of the replication and syncing operations in DFS environments, you must set up the virtual machine in accordance with Microsoft best practices to ensure database consistency. If all Microsoft considerations are not addressed, backup and restore of the virtual machine may yield undesired results. If you prefer not to research these best practices, install the agent on the VM and protect it as you would a physical server (leveraging Microsoft's VSS writers).

Hot backup copy limitation

Backup copy to the Unitrends Cloud is not supported. If desired, you can set up hot backup copy to your own Unitrends target appliance. To do this, first install the 10.1.1-3 release on the target appliance.

Notes:

- Backup copy to the Unitrends Cloud will be supported in a future release.
- If you are copying non-AHV backups to the Unitrends Cloud, those copies can continue after you upgrade the source appliance to release 10.1.1-3. Do not attempt to copy AHV backups. If you attempt to copy an AHV backup to the Cloud, the job fails and the appliance attempts to retry the failed job indefinitely, which encumbers the hot copy job queue.

Install the 10.1.1-3 release

Use these procedures to upgrade your appliances and protected Windows assets to release 10.1.1-3. Upgrade the Unitrends appliance before you upgrade the agent on its protected Windows assets.

- "To install release 10.1.1-3 on a Unitrends appliance"
- "To install the 10.1.1-3 Windows agent" on page 17

To install release 10.1.1-3 on a Unitrends appliance

Use the following steps to install the 10.1.1-3 release on your Unitrends appliance:

Note: If you will be copying AHV backups to a Unitrends appliance target, use this procedure to upgrade the target appliance before you upgrade the source backup appliance.

 Open a Firefox or Chrome browser and connect to the appliance UI by entering: https://<appliancelPaddress>/ui/. For example:

New Tab	×	+		-		×
https://10.10.10.1/ui/		▼ → Q Search	☆ 自	+	â	≡
Share Browser WebEx+						

2 Log in as a user with administrative privileges.

192. 100.20.214 - Dashboard	× +		
← → ♂ ଢ	① ♣ https://191 101 101 11/ui/#/	😨 🚖 🗍 🛛 Conne	ect to appliance UI 🔥 🔲 😑
UNITREN	JDS		
Unitrend	ls Recovery Series	root	
2	Enter user name and password. User must have superuser or administrator privileges		
		Keep me logged in	Log In -3
Support Documentation Contact Us			unitrends.com

3 Click the gear icon and select **Check for Updates**.



4 A list of available updates displays. Click **Apply Update** to begin the installation.

	Updates				?
	APPLIANCE	UPDATE INFORMATION	VERSION		
	Dominique-313	Update Available(488.68 MB)	10.1.1-1.201802130123.CentOS6	Apply Update	View Detail:
<					>
			Click to install		Close

5 For some appliances, software maintenance is required with the update. If so, you see this message and the update will take some extra time:

Note: If you do not see this message, maintenance has already been performed on the appliance.

Confirmation ?
 To optimize system performance, this appliance needs a software maintenance task that is run on the appliance during the update. The estimated runtime for this task is 30 minutes. If it takes longer than 30 minutes the task will be ended. Is it OK to proceed with the update now?
To continue with the update, press Confirm. To quit, press Cancel.
Confirm Cancel
Do one of the following:

- Click **Confirm** to continue with the update.
- Click **Cancel** to quit. (You can then install the update at another time.)
- 6 During the upgrade, you see status messages as packages are installed. If you have trouble with the installation, see "Troubleshooting the appliance upgrade" for tips.
- 7 After the installation completes, clear your browser cache, then close the browser.

Note: If you receive a message indicating that you need to reboot the appliance to take advantage of the new kernel installed during the upgrade, you can either reboot now or reboot at a later time.

Release 10.1.1-3 | April 2018

If you reboot now, do the browser steps above after the appliance boots. (If you do not receive this message, the kernel was not updated and a reboot is not required.)

- 8 Open the browser and log back in to the appliance UI.
- 9 Enable the AHV feature in the appliance UI by doing these steps:
 - On the **Configure > Appliances** page, select the appliance and click **Edit**.



• Click Advanced and select General Configuration.

		Users	Date Time	License	Backup Copy	Advanced	U
NCRYPTION SET	TINGS						
🗹 Enable End	ryption						
Current Passpl	hrase						
Change Pa	ssphrase						
New Passphra	ise						
Confirm New I	Passphrase						
Save Master K	ley File						
Save Master K	key File						
Save Master K AN DIRECT DET/	ley File AILS	lost	Port	Target	LUN	١	
AN DIRECT DET/	AILS	lost	Port	Target	LUN	N	
AN DIRECT DET/	AILS	lost	Port	Target	LUN	u .	

- Enter **ahv** in the Name field, then click the **showAHV** row.
- Enter **true** in the Value field, then click **Save**.

• Click **Close** to exit.

General Configuration	n (Advanced)			?
Section 🔺	Name ahv	Enter ahv ×	Value	
СМС	showAHV	2 Select row	false	^
fileDedup	enableInlir	neDedupAHV	Yes	
	Edit Settings (Advanc	ed)	Ø	
	Section	CMC		
	Name	showAHV		
	Description	If true, allow adding Nutanix Al-	IV assets for protection.	
	Value 😮	true	ue	
			Save Cancel	×
			5 0.	se

- **10** Log out of the appliance UI, then log back in. The AHV feature is now enabled. Continue to one of the following:
 - "To install the 10.1.1-3 Windows agent" on page 17 if you are protecting Windows assets with agentbased backups.
 - "Add the Nutanix AHV host cluster" on page 20 if you do not need to install the 10.1.1-3 Windows agent on any protected assets.

Troubleshooting the appliance upgrade

In rare instances, your first attempt to update the Unitrends appliance might not be successful. See the following table for a description of upgrade issues and steps you can take to resolve them:

lssue	Next steps
The update times out because some of the packages did not install.	If the installation stops and you receive a message stating a package did not install successfully, in most instances you can resolve the issue by clicking the refresh arrows and attempting the update again. If necessary you can repeat this multiple times until the update completes. See <u>KB 3402</u> for more information.

Release 10.1.1-3 | April 2018

lssue	Next steps
The appliance is unable to download the update packages.	The appliance cannot reach the FTP or HTTP site - If you receive a message stating that the appliance is unable to download packages, this is the most likely cause. The FTP or HTTP site might be blocked by a firewall or some other restriction might be preventing you from reaching the site. To resolve this issue, you can download the update packages from the site you are not currently using (such as downloading from the HTTP site if you are currently using the FTP site, or vice-versa). For procedures, see KB 3401.
An error message displays stating that the managing system must be updated.	To update the appliance, you must first update any other appliances that are managing it. Verify that any backup copy target appliance and any other managing appliances are running the latest release. Upgrade these appliances as needed. You can then upgrade any appliances that they are managing.
No data displays in the UI after installing appliance updates.	 To resolve this issue: Clear your browser cache, then close the browser. Open the browser and log back in to continue working with your appliance.

To install the 10.1.1-3 Windows agent

After upgrading your appliance, upgrade the agent software on any Windows assets that you are protecting with asset-level (agent-based) backups. It is best practice to upgrade agents to the latest release to take advantage of performance enhancements and fixes.

Note: The Windows agent is not used for host-level backups of AHV virtual machines. You do not need to install this agent on AHV VMs that you are protecting with host-level backups.

Before upgrading or installing the Windows agent, the following requirements must be met:

- You must be the user administrator to install or upgrade the Windows agent.
- Volume Snapshot Service (VSS) Exchange Writer is required for the Exchange agent.
- VSS SQL Writer is required for the SQL Server agent.
- VSS Hyper-V Writer is required for the Hyper-V agent.

Follow these steps to install or upgrade the Windows agent:

- 1 Log in to the Windows asset as a user that has full access to all files and folders on the system (i.e., local administrator).
- 2 Access the MSI installer on the Unitrends appliance by entering \\<*ApplianceIP*>\windows_agents in the Windows File Explorer:



- 3 Download one of these agent MSI files:
 - Unitrends_Agentx64.msi for 64-bit Windows assets
 - Unitrends_Agentx86.msi for 32-bit Windows assets
- 4 Double-click the MSI file to launch the installer. Click **Next**.



5 Select an installation directory and click **Next**.

The default directory is *C*:*\PCBP*. To install in another location (folder or volume), click **Browse** or manually enter the directory path.

Notes:

- Approximately 1100MB of temporary installation space is required on volume C:, regardless of where the software is ultimately installed.
- If you do NOT install to *C:\PCBP*, the installation does not include the Hyper-V CBT component. If you are running Hyper-V host-level backups and want to use this driver, you must install to the default location.

🖟 Unitrends Agent 10.1.0-2.020	092018_64 bit —		×
Select Installation F	older		
	The installer will install Unitrends Agent 10.1.0-2.0 bit to the following folder. To install in this folder, click "Next". To install to a folder, enter it below or click "Browse".	12092018_64 a different	-
Select installation directory	Eolder: C:\PCBP\	Browse	_
		Next >	

- 6 Click **Next** to begin the installation process (or click **Back** to review or modify data). The installation can be interrupted at any time by clicking **Cancel**.
 - **Note:** If a firewall is enabled on the Windows asset, the installer automatically opens Port 1743 and creates the necessary firewall exceptions.



7 The agent is installed. Click **Done** to exit the installer.

Add the Nutanix AHV host cluster

To protect VMs hosted in a Nutanix Acropolis Hypervisor (AHV) environment, you must add the AHV host cluster to the Unitrends appliance as a virtual host asset. Once the AHV host is added, all VMs on that host are automatically discovered and can be selected for protection.

To add a virtual host asset

Use this procedure to add the AHV host cluster.

- 1 Select Configure > Protected Assets.
- 2 Click Add > Virtual Host.



- 3 Enter the following in the Add Virtual Host dialog:
 - Hypervisor Select Nutanix-AHV in the list.
 - Host name Enter a unique name to identify the AHV cluster. This is the display name used by the appliance UI and does not need to match the actual hostname of the AHV cluster.
 - IP Address Enter the Nutanix cluster virtual IP address. This is a highly-available IP address used to reach the management services running on the Nutanix AHV cluster.
 - Username and Password:
 - For Nutanix AHV clusters that are NOT configured to use directory services authentication and are running a pre-5.5 AOS release, enter the credentials of the Nutanix **cluster admin** user account. You must use the **cluster admin** account. Other users with administrative privileges are not supported.

Δ

- For Nutanix AHV clusters that are NOT configured to use directory services authentication and are running AOS release 5.5, enter the credentials of any local Nutanix cluster account that has been assigned the **cluster admin** or **user admin** role.
- For Nutanix AHV clusters that are configured to use directory services authentication, enter the credentials of an LDAP user that has the **cluster admin** role. You must specify a domain in addition to the username. For AOS 5.1, the username and domain are case sensitive and you must match the case that was entered in the self service portal (SSP).

In the Username field, enter the username and domain in this format: *user@domain*. For example, **jalvarez@unitrends.com**. (For configuration requirements, see "Requirements for directory services authentication in AOS 5.1" on page 9 or "Requirements for directory services authentication in AOS 5.5" on page 10.)

DETAILS	1 Select
Hypervisor	Nutanix AHV Nutanix-AHV
Appliance	Dominique-313
Host name	nutanix-01 — 2 Enter host name
IP Address	19: 10 — 3 Enter cluster IP
CREDENTIALS	
Username	admin
Password	4 Enter credentials

Note: If you receive a credential error, see "Getting Started with AHV Protection" on page 7 for steps to resolve.

The host asset is added to the appliance. To start protecting the hosted VMs, see "Run AHV backups".



UNITRENDS

Appliances Protected Assets	Copied Ass	jets					
View:Table 💌 DisplayAll 🔻 😝 A	dd 🔻	Manage Credentials	6 Manage Global VM Set	ttings	🕞 Update Ag	ent 🔻 🗹 Edit 🔕 R	emove
NAME	ADDRESS	DESCRIPTION	CREDENTIALS	RETENTION	ENCRYPTED	AGENT VERSION	APPLIANCE
BURDCESX14.unitrends.com	10 100 112	VMware Host	(Unnamed)				Dominique-31
🔲 📱 CentOS6-rpm	10 49	Linux Al-	IV host is added	None	No	10.0.0-2.20170625_2204	Dominique-31
🔲 🖩 nutanix-01	19	AHV Host	nutanix-01-New-Credential	None	No	5.1.0.1	Dominique-313
□ 🖥 W2260		Windows 10	None	None	No	10.0.0-3	Dominique-313

Run AHV backups

To run backups of hosted AHV VMs, you can create backup jobs manually or create an SLA policy. For a comparison of these methods, see <u>Backup Administration and Procedures</u> in the <u>Administrator Guide for</u> Recovery Series and Unitrends Backup.

See the following procedures to create AHV backup jobs:

- "To create a backup job for Nutanix AHV assets" on page 22 Use to manually create a backup job.
- "To create an SLA policy for AHV assets" on page 29 Use to create an SLA policy. The appliance
 automatically creates the backup and backup copy jobs needed for the RPO and retention settings you
 specify in the policy.

To create a backup job for Nutanix AHV assets

Notes:

- An AHV asset can be assigned either to one manually created backup schedule or to one SLA policy (to ensure that the VM exists in only one backup schedule).
- To access newly added virtual machines, sync inventory before creating your job by clicking the **Gear** icon in the upper-right of the UI and selecting **Inventory Sync**.



1 Select Jobs > Active Jobs > Create Job > Backup.



Release 10.1.1-3 | April 2018



- 2 Select Nutanix AHV in the What do you want to backup? list.
- 3 In the Inventory tree, expand the AHV host cluster, then check boxes to select virtual machines to protect. Selected VMs display in the Job Inventory Settings area.
 - To locate an asset by name, use the **Search** field below.
 - To quickly select all hosted VMs, click the host checkbox.
 - To select one VM, click its checkbox.

Release 10.1.1-3 | April 2018

Create Backup Job	G
Job Name Backup Job	
1. Select Items 2. Define Job Settings	0
appliance What do you want to backup? Nutanix AHV	Name Protection Rules
UUB_118	pm-ubuntu 🖉 Edit
III myAHV	W2012R2251
AHV host cluster	pm-ubuntu-2
LindaT3_restore	4
	(Optional) Edit settings
× pm-ubuntu-2-restore-php	(optional) Ear sortings
select VMs	
🔲 🗙 pm-ubuntu-2-restore-php29c	
m District Provide American Science Provide Am	
x pm-ubuntu-2_restore0119_1427	
m when the store photon in	
m 🖾 🗙 pm-ubuntu-restore27 🗸 🗸	,
< >>	5 (Optional)
pm Q &	
(Optional) Enter search text	Auto-include new VMs
	6 Next Save Cancel

- 4 (Optional) Edit Job Inventory Settings to exclude VM disks from backup:
 - Locate the VM in the Job Inventory Settings list.
 - Click **Edit** to specify disks to exclude.
 - Click **Save** to retain any changes.

- 5 (Optional) Check the **Auto-include new VMs** box to automatically add newly discovered VMs to the schedule.
- 6 Click **Next**.
- 7 Select **Now** or **Create a Schedule** to specify when you want this job to run. If you create a schedule, enter a unique job name.
- 8 Set remaining Job Details and Options:

Chapter 2: Getting Started with AHV Protection Provide feedback

Note: Critical system volumes are required to recover the entire virtual machine. Use care when omitting disks from backup.

Release 10.1.1-3 | April 2018

b Name AHV incremen	tal			
Select Items 2. Defi	ne Job Settings			
JOB DETAIL		OPTIONS		
Select when to run this job:	O Now	Backup Target	Internal	
Select the backup mode:	Incremental Forever	🗌 Verify Backups 😧		
		Include job results in t	the Job Report	
Start Date:	1/23/2018	Include job failures in	the Failure Report	
ncremental Backup	Every SUN MON TUE WED THU FRI SAT			
Start Time	03:00 am			
Recurs every:	1 🗘 Hour(s) 🗸 Until 11:59 pm			

- In most cases, the standard backup modes can be used to create the schedule.
- If you need more granularity, choose the **Custom** mode and do these steps to create a custom backup calendar:
 - Click the calendar icon.

te Backup Job				
ob Name Backup Job				
Select Items 2. Defin	ne Job Settings			
JOB DETAIL		OPTIONS		
Select when to run this job:	O Now	Backup Target	Internal	\sim
Select the backup mode:	Custom	Select Custom ackups 📀		
		Include job results i	n the Job Report	
Calendar Contents.	NO CAIENDAR EXISTS	Include job failures	in the Failure Report	
	Click to Edit:			
	$\overline{\mathbf{U}}$			

- In the Calendar dialog, select a backup mode in the Backups area and drag it to a day on the calendar. (You cannot drag to a day in the past.)



- In the Add Backup dialog, modify settings and click **Save**.

- Repeat these steps to add other modes to the calendar.



Release 10.1.1-3 | April 2018

lendar							
Backups 😮	March 2018			month day		to	day <
Full	Sun	Mon	Tue	Wed	Thu	Fri	Sat
Incremental	25	26	27	28		1 2	
				Add Bac	:kup		0
Drag ba	ackup to calendar	5	6	Туре		Incremental ~]
				Start Da	ate:	03/09/2018	
	n	12	13	Start Tir	me	10:00 pm	
		Enter details	2	Rec	urrence:	Daily ~	
	18	19	20	0	Every Day		
					Every Week	day	
	25	26	27	0	Every Week	end Day	
	1	2	2			3 Save	Cancel
	1	2	5	•			

- Click **Save** to save the settings and close the Calendar dialog.



Release 10.1.1-3 | April 2018

	March 20	10		day			
Full	Sun	Mon	Tue	Wed	Thu	Fri	Sat
scremental	2	26	27	28	1	2	
		4 5	6	7	8	9 10p Incremental	
		11 12	13 10p Incremental	14 10p Incremental	15 10p incremental	16 10p incremental	4a Full
ckups display on the	e calendar						
		19 Incremental	20 10p Incremental	21 10p Incremental	10p Incremental	23 10p Incremental	4a Full
	2	25 26	27	28	29	30	
		10p Incremental	10p Incremental	10p Incremental	10p Incremental	10p Incremental	4a Full
		1 2 10p Incremental	3 10p incremental	4 10p Incremental	5 10p Incremental	6 10p incremental	4a Full

- Click **Save** to save the schedule.

Select Items 2 Def	ine Joh Settings			
JOB DETAIL	ine Job Settings			
Select when to run this job:	O Now	Backup Target	Internal	\sim
Select the backup mode:	Custom ~	Verify Backups 💡		
Calendar Contents:	Full Backup at 04:00 am, Recurring: weekly, Day(s): SA,Incremental Backup at 10:00 pm, Benuring: daily, Day(s): MO TI UNE TH FR	 Include job results in Include job failures in 	the Job Report the Failure Report	
are added	** Please save the job to save calendar changes.			
				Niek to

9 Click Save.

Chapter 2: Getting Started with AHV Protection Provide feedback

- **10** Click **OK** to close the Success message.
 - If you created a schedule, the job runs at the date and times you specified.
 - If you chose Now, the job queues immediately. Click **Active Jobs** to view the running job.

To create an SLA policy for AHV assets

Notes:

- An AHV asset can be assigned either to one SLA policy or to one manually created backup schedule (to ensure that the VM exists in only one backup schedule).
- The policy can contain VMs that are managed by a single AHV cluster.
- A VM can be assigned to only one hot backup copy schedule. The policy does not create a hot backup copy schedule if any of its VMs exist in another hot backup copy schedule.
- To access newly added virtual machines, sync inventory before creating your job by clicking the **Gear** icon in the upper-right of the UI and selecting **Inventory Sync**.

UNITREN		оот 🦓 🦓
DASHBOARD	BACKUP SUMMARY	INVENTORY SYNC
PROTECT	0 Errors	SET LANGUAGE (EN) Not Protected

1 Select Jobs > SLA Policies > Create Policy.



- 2 Select AHV Assets in the What do you want to protect? list.
- 3 In the Inventory tree, expand the AHV host cluster and check boxes to select virtual machines to protect. Selected VMs display in the Job Inventory Settings area.
 - To locate an asset by name, use the **Search** field below.
 - To protect all VMs, select the AHV host.
- 4 (Optional) Edit Job Inventory Settings to exclude VM disks from backup:

- Locate the VM in the Job Inventory Settings list.
- Click **Edit** to specify disks to exclude.
- Click **Save** to retain any changes.

Note: To recover the entire virtual machine requires critical system volumes. Use care when omitting disks from backup.

5 Click Next.

SLA Policy Na	ame SLA Policy		SLA Policy	Description (Optiona	il)	
1. Select Items	2. Define Policy Options					
INVENTORY			JOB INVENTORY SETT	INGS		
What do you w	ant to protect? AHV Assets	~	Name	Protection Rules		
	Dominique-313		doc-W2012R2		Edit	^
	Linux Servers		doc-ubuntu	4 (Optional) Edit setting	IS Ø Edit	
····· 🔽	nutanix01					
	.QA - Mark - Large VM					
	.QA - Mark - Source			A		
<u>م</u>	🛛 🗙 .QA - Mark - Target			Assets in the policy are listed h	ere	
k hoxes	🛛 🗙 .QA - Mark - VM Synthesis Te					
elect	Doc-UB					
ets for	🛛 🗙 doc-ubuntu					
policy	doc-W2012R2					
	LindaT3					
	LindaT3_restore					
	🛛 🗙 pm-ubuntu					
<	> pm-ubuntu-10					
doc	Q 🛛 📢 🕨 3 Matches					
						~

6 Define the remaining Policy Options, then click **Save**.

Policy Options are described in the following table:

SLA policy setting	Description
SLA Policy Name	Enter a unique name for the policy.
SLA Policy Description	(Optional) Enter a short description of the policy.

Release 10.1.1-3 | April 2018

SLA policy setting	Description
RPO of	Recovery Point Objective – The maximum interval of time between backups (the maximum threshold of data loss tolerated by your business continuity plan). Determines how often backups will run.
	Enter the number of hours or minutes to define the RPO interval.
Show Backup Window	 Check this box to view and/or edit the following: First Full Date – Date when the policy's first full backups will run. (Applies to assets that do not yet have a successful full backup.) First Full Time – Time when the policy's first full backups will run. (Applies to assets that do not yet have a successful full backup.) Backup Between – Hours of the day when backups will be taken.
Copy backups to the Hot Backup Copy Target	 Check this box to copy backups to your hot backup copy target. Supported only when a Unitrends appliance has been added as a backup copy target. (Hot copy to the Unitrends Cloud is not supported for the 10.1.1-3 release.) For details on adding a Unitrends appliance target, see these topics in the Administrator Guide for Recovery Series and Unitrends Backup: Backup copy targets to add the target. (Before adding the target, be sure to install the 10.1.1-3 release on the target appliance as described in "To install release 10.1.1-3 on a Unitrends appliance" on page 13.) Managing SLA Policies to start copying backups to the target you added by editing the SLA policy.
Copy backups daily to the Cold Backup Copy Target	 Check this box to copy backups to your cold backup copy target. Supported only when a cold backup copy target has been added to the backup appliance. Supported for these types of cold targets only: third-party cloud, NAS, or iSCSI. If multiple cold targets exist, the policy copies to the one that was added first. To copy to a different cold target, manually create a backup copy job instead, as described in <u>Creating backup copy jobs</u>. To add a cold target to the backup appliance, see <u>Backup copy targets</u>.

31

Release 10.1.1-3 | April 2018

UNITRENDS

SLA policy setting	Description
Cold Backup Copy Retention Days	Check this box to specify the length of time a copy must be retained before it can be deleted. To define the retention period, enter a number and select Days, Weeks, Months, or Years. For example, enter 2 and select Weeks to retain copies for 2 weeks.
Encrypt Cold Backup Copies	Check this box to encrypt cold backup copies. (Encryption must also be configured on the appliance. For details, see <i>Encryption</i> in <u>Appliance settings</u> .
	Note: If the backup copy target device is configured for encryption, copies are encrypted regardless of this setting.
Keep backups for <i>N</i> days	Number of days backups must be retained. Backups that are younger than <i>N</i> days are not purged for any reason, including at the expense of new, incoming backups.
Warn when less than <i>N</i> days of backups remain	Use this option to receive an email notification if this asset has less than <i>N</i> days of backups stored on the appliance.
Delete backups after <i>N</i> days	Number of days after which the appliance will delete backups.

ate SLA Policy		
SLA Policy Name AHV SLA Policy	SLA Policy Description	AHV policy
. Select Items 2. Define Policy Options Enter a unique	ue name	
	BACKUP RETENTION 🔺 —	
RPO of 12 Development Hour(s)	Keep backups for	14 🚖 days.
☑ Show Backup Window Edit settings First Full Date 2/5/2018	☑ Warn when less than	14 🔹 days of
First Full Time 03:00 am Backup Between 12:00 am And 11:59 pm 2	Delete backups after	backups remain.
BACKUP COPIES A Hot Backup Copy Target has not been configured		
Copy backups daily to the Cold Backup Copy Target 🔮		
Cold Backup Copy Retention Days 14 🖕 Days 🗸		
Encrypt Cold Backup Copies 📀		3
		Previous Save Cancel

7 The appliance creates the policy and related jobs. Click **Close** to close the status message.

Release 10.1.1-3 | April 2018

	Job Name	~	Job Type	~	Message	~	
0	_SLA:AHV SLA Policy (Backup)		Backup		Job created		^
	SLA:ALIV SLA Policy (Cold)		Cold Backup (onv	lob created		

The policy displays on the SLA Policies tab:

Active Jobs Job Ma	nager Recent Jobs	Recent System Jobs	SLA Policies Jobs Cale	ndar	
Create Policy	w Details	Delete			
NAME	✓ RPO		* RETENTION	~ APPLIANCE	~
AHV SLA Policy	12 Hours		Min 14, Max 21, Hold 14 Days	Dominique-313	

Jobs display on the Job Manager tab and are named with the prefix _SLA:

A	ctive Jobs	Job Manage	۶r	Recent Jo	bs Rece	nt Syste	m Jobs	SLA Po	licies	Jobs Cale	ndar		
+ (
	NAME	~	STATUS	~	TYPE	~	SCHEDULE	~	LAST RUN	~	NEXT RU	N ~	APPLIANCE
	_SLA:AHV SLA P	olicy (Backup)	🖌 Idle		Backup		Incremental: S	Sun-Sat e	Never		02/05/2	018 12:00:00	Dominique-313
	_SLA:AHV SLA P	olicy (Cold)	🧹 Idle		Backup Copy		Backup Copy:	Sun-Sat	Never		02/06/2	018 03:00:00	Dominique-313

Next Steps

UNITRENDS

Once you have created AHV backup jobs, you can opt to do any of the following:

- Create a backup copy job to copy AHV backups to a secondary target. The 10.1.1-3 release supports the following:
 - Hot backup copy to another Unitrends appliance. (The target appliance must be running release 10.1.1-3. Upgrade the target before copying AHV backups.)
 - Cold backup copy to these devices: eSATA, USB, tape, third-party cloud, attached disk, NAS, and SAN.

For details, see these topics in the Administrator Guide for Recovery Series and Unitrends Backup:

- Backup copy targets to add the target.

- <u>Creating backup copy jobs</u> to start copying backups to the target you added. (If you created an SLA policy, edit the policy to add the backup copy job instead. For details, see <u>Managing SLA</u> <u>Policies</u>.)
- Edit AHV host and VM settings. For details, see "Managing AHV Hosts and Virtual Machines" on page 65.
 - **Note:** AHV backups are run using the default quiesce setting of the backup appliance. To modify this setting, see <u>Quiesce settings for host-level backups</u> in the <u>Administrator Guide for Recovery</u> <u>Series and Unitrends Backup</u>.
- Recover entire VMs or files from AHV backups. For details, see "Recovering AHV Backups" on page 35.



Chapter 3: Recovering AHV Backups

Unitrends provides a variety of methods for recovering host-level backups of AHV virtual machines. You can recover entire virtual machines or selected files from backup. See these procedures for details:

- "Recovering an AHV VM"
- "Recovering files from a host-level backup of a Windows AHV VM" on page 39
- "Recovering files from a host-level backup of a Linux AHV VM" on page 52

Notes:

This guide includes procedures run from the backup appliance using host-level backups or imported backup copies. For additional procedures, see these topics in the <u>Administrator Guide for Recovery Series</u> and <u>Unitrends Backup</u>:

- <u>Recovering Backup Copies</u>
- <u>Recovering Host-level Backups</u>

Recovering an AHV VM

Use this procedure to recover an entire AHV virtual machine.

1 Select **Recover** and click the **Backup Catalog** tab.

(Optional) Use Filter Backups to the right to customize the backups that display. (For details, see "Working with Custom Filters in the Backup Catalog" on page 71.)



Release 10.1.1-3 | April 2018

U		NDS			L ROOT	**	<u> </u>
믱	DASHBOARD	Backup Catalog 2 File Level	Recovery In	Istant Recovery Replic	as 3	(Option) Modify settings a Or	nal) and click Filter
		Q Search Files 🗮 Recover	cover Files 🕥 Inst	ant Recovery O Import to	o Source 🔦 Hold 🗰	De Select a filter f	from the list de Filter
	PROTECT	8	APPLIANCE	HOST	APPLICATION MODE	FILTER BACKUPS	
_		CentOS5_rpm_4_250	Dominique-313	BL bm	VMware	Asset Name	
	RECOVER	🕨 📄 🚆 CentOS6-rpm	Dominique-313	CentOS6-rpm	Agent-Based	Appliance	Dominique-313 V
		CentOS6_rpm	Dominique-313	Bbm	VMware	Host	All
	JOBS	doc-ubuntu	Dominique-313	nutanix01	AHV	Application	
		doc-W2012R2	Dominique-313	nutanix01	AHV	Application	All
ш	REPORTS	doc-Windows-7_6_DB	Dominique-313	BI	VMware	Mode	All
		doc-Windows-8	Dominique-313	doc-Windows-8	Agent-Based	From	02/03/2018
\$	CONFIGURE	doc-WinVista_214_DB	Dominique-313	B	VMware	То	02/09/2018
		DocNode1	Dominique-313	BU tom	VMware	Held (0
	4	DocNode2	Dominique-313	BUDDOCCUT om	VMware		-
		▶ 🗌 🚆 HVSVR2008R2	Dominique-313	HVSVR2008R2	Agent-Based		
		▶ 🗌 🚾 UB_4_206	Dominique-313	B	VMware	Туре	Backup ^ Imported Backup
		Unitrends_doc-Windows-8	Dominique-313	BUTTE COOL COM	VMware		Backup Copy (Cold) Backup Copy (Hot)
		▶ 🗌 🗙 W2012R2-pm-2	Dominique-313	nutanix01	AHV		
		▶ 🗌 🚆 W2260	Dominique-313	W2260	Agent-Based		Clear
						MANAGE FILTERS	
						Select Filter	Backups last 7 d
						Artel	Eave Doleta
						Add	Save

- 2 Expand the VM asset and select one of the following to use for the recovery:
 - A host-level backup.
 - An imported host-level backup copy. (To import a backup copy, see <u>To import a cold backup copy</u> or <u>To import a hot backup copy</u> in the <u>Administrator Guide for Recovery Series and Unitrends Backup</u>.
- 3 Click **Recover**.

Backup Catalog	File Level Recovery	Insta	nt Recovery	Re	plicas	
Q Search Files	cover 3 Recover Files	🏵 Instant F	Recovery	o Impo	ort to Source	🛧 Hold
8			APPLIANCE		HOST	
► 🗌 🚾 CentOS5_rp	om_4_250		Dominique-313		Bl	om
🕨 🔲 🧮 CentOS6-rp	m		Dominique-313		CentOS6-rpn	n
CentOS6_rp	om		Dominique-313		В	om om
▶ 🗆 🗙 do 🗋 ntu			Dominique-313		nutanix01	
▼ □ × doc-W2012	R2		Dominique-313		nutanix01	
2 2 2 2	/06/2018 04:14:08 pm (Warnin	ig)	Dominique-313		nutanix01	
🔽 🗆 💽 🔺 02	/06/2018 12:00:55 am (Warnin	g)	Dominique-313		nutanix01	

4 Select these Recovery Options:


Release 10.1.1-3 | April 2018

Recovery Options	Description
Target Location	Select the AHV host where the VM will be recovered.
Target Storage	Select a storage container.
Recover excluded disk metadata	(Optional) Check this box to recover the metadata for disks that were excluded from the backup.

5 Click **Next**.

Create Recover Job				0
Job Name On-Demand			Asset Name: Backup Details:	doc-W2012R2 Full 02/06/2018 04:14:08 pm
1. Define Recovery Options	2. Summary		Size:	9756 MB
RECOVERY OPTIONS				
Target Location	nutanix01	~	Select targe	et AHV cluster
Target Storage	default-container-82835 (674 GB free)	~	and s	torage
Recover excluded disk meta	adata? 🕐			
2 (Optional) Ct	heck to include metadata			
			3	Next Cancel

A summary of the selected recovery options display.

- 6 (Optional) Modify the VM Name by clicking it in the Assets to Recover list and entering a new name.
- 7 Click **Save**. The job is queued immediately.

Create Reco	over Job				?
Job Name	On-Demand				I
1. Define F	Recovery Options	2. Summary			
ASSETST	O RECOVER				
VM NAME		TARGET HOST	TARGET STORAGE		
doc-W2012	R2_restore	^ዎ nutanix01 ካ	default-container-82835		^
1	(Optional)	Edit VM Name			~
				2	
			Previous	Save Canc	el

8 Click **OK** to close the Information message.



9 To view job progress, select **Jobs > Active Jobs**. Select the job and click **View Details**.

UNITE		3					L F	ROOT	°o (9	A0
	Activ	e Jobs	Job Manager	Recent Jobs	Recent System J	obs SL	A Policies	Jobs Calen	dar		
-	🕂 Crea	te Job 🔻	E View Details	4 🗉 Pause 🔇	Cancel						
PROTECT	JOB NAME	. ~	ASSET	✓ STATUS ✓	TYPE/MODE ~	STARTED -	Y PROGRESS	~	DURATION ~	APPLIANCE	~
	On-Dema	nd 🚬 👝	doc-W2012R2	X Connecting	K restore: Restore			0%		Dominique-313	
		3	Select job								
🛱 ЈОВЗ 🥤	JOBID	APPL	ICATION	HOST/SERVER	MESSAGE						
	11637	AHV		nutanix01	Sending data to nutan	iix01					

Recovery is complete when the job status changes to Success:

Active	Jobs	Job Manager	Recent Jobs	Recent System	Jobs	SLA Policies	Jobs Calendar			¢
+ Creat	Create Job V Hide Details									
JOB NAME	¥ ¥	ASSET ~	STATUS ~	TYPE/MODE ~	STARTED	• •	PROGRESS ~	DURATION	APPLIANCE Y	≡
On-Deman	nd o	doc-W2012R2	Success	K restore: Restore	02/09/20	018 01:20:55 pm	1	oc	Dominique-313	^
	Recovery is complete									
JOBID	APPLICATIO	N HOST/SERVE	R			MESSAGE	_			
11637	AHV	nutanix01				Task completed				

10 After the recovery job completes, go to the hypervisor and power on the recovered virtual machine.

nutanix01 VM	- ↓ - 🍣	· 🔔 2	• •	•	N				(ຊ ? ∝	\$ ~	Admin 🚨 ~
Overview · Table										+ Crea		
VM						nclude Cont	roller VMs · 1–1	0 of 50 (filtered f	írom 53) · < 🖒	· 🕸 🗸 · 🛛 sea	arch in tabl	e Q
 VM NAME 	HOST	IP ADDRESSES	CORES	MEMORY	STORAGE	CPU USAGE	CONTROLLER READ IOPS	CONTROLLER WRITE IOPS	CONTROLLER IO BANDWIDTH	CONTROLLER AVG	BACKUP .	FLASH MODE
 .QA - Mark - Large VM _restore 	NTNX-175M6D 120075-B	192.168	1	2 GiB	1.46 TiB / 3.13 TiB	1.67%	0	0	0 KBps	0.7 ms	i Yes	No
doc-W2012R2_restore			2	4 GiB	9.19 GiB / 70 GiB	0%	-		-		- Yes	No
LindaT3	Select the reco	vered VM	1	1 GiB	- / 0 GiB	0%	0	2 0	0 KBps	0 ms	Yes	No
Summary > doc-W2012R2	_restore		Manage	e Guest Tools	·휜 Launch Conso	le Pov	ver on Tak	e Snapshot	Migrate Paus	e Clone	🖋 Update	X Delete

11 Modify VM settings and backup schedules as needed.



- A recovered VM may not have the same network settings as the original. Check network settings and modify if needed.
- The recovered VM has the same username/password credentials as the original VM. Access the VM and verify that it is functioning as expected in production.
- Create or edit backup schedules to begin protecting the recovered VM.

Notes:

- Windows server VMs In rare instances, after a restore is performed for a Windows server VM, a disk
 may be inaccessible because it has been placed in an offline state. To bring disks into an online state,
 login to the VM, go to Disk Management, right-click on the offline disk, and select **Online** from the
 drop-down menu.
- Debian VMs In some instances, Gnome might not start after a Debian VM is recovered. You can
 resolve this issue by rebooting the VM or restarting Gnome from the console. To access the console,
 enter Ct/+Alt+F1 and log in as root. Then run startx.

Recovering files from a host-level backup of a Windows AHV VM

Use the procedures in this section to recover Windows files.

Windows prerequisites and considerations

The following requirements and considerations apply to recovering files from a host-level backup or host-level backup copy of a Windows VM:

Prerequisite or consideration	Description					
Supported recovery methods	To recover files from a host-level backup or copy, the appliance creates a recovery object that contains the backup's files. For some Windows VMs, this object is also exposed as a CIFS (Samba) share and/or an iSCSI LUN on the backup appliance. After you create the recovery object, you will view it on the File Level Recovery tab to see whether the CIFS and iSCSI options are available.					
	You can recover files from this object in several ways. Options include:					
	• Browse the recovery object and download selected files to a <i>.zip</i> file. This is the simplest method.					
	• Mount the CIFS share on a recovery target machine. From the target machine, select files to recover.					
	• Mount the iSCSI LUN on a recovery target machine. From the target machine, select files to recover. (You must use an iSCSI LUN in some cases. For details, see "When to use an iSCSI LUN" on page 40.)					
Recovery target requirements	The target can be configured with basic, GUID Partition Table (GPT), or dynamic disks. All configured disks must have unique names.					
When to use	You must recover by mounting the iSCSI LUN to perform the following tasks:					
an iSCSI LUN	• Recover access control information on files and folders.					
	Recover New Technology File System (NTFS) encrypted files.					
	Recover Resilient File System (ReFS) files.					
	• Recover files on dynamic disks. If the dynamic volumes are still in use on the original VM, you must mount the recovery object on a different machine.					
	Note: For the recovery, iSCSI disks are writable and a 1 GB write limit is enforced. Errors display on the recovery target machine if more than 1 GB is required. In this case, you cannot recover by using iSCSI. Recover files by downloading to a <i>.zip</i> file or by mounting the CIFS share, or perform a VM recovery.					



Windows file-level recovery

Use the following procedures to recover files from a backup or imported backup copy of a Windows VM. Before you start, be sure all requirements in "Windows prerequisites and considerations" on page 39 have been met.

- "Step 1: Create the recovery object"
- "Step 2: Recover files" on page 43
- "Step 3: Remove the recovery object from the appliance" on page 51

Step 1: Create the recovery object

Note: If a previously-created recovery object is still mounted for the VM, you must remove it before creating a new one.

- 1 Log in to the backup appliance.
- 2 Select **Recover** and click the **Backup Catalog** tab.

(Optional) Use Filter Backups to the right to customize the backups that display. (For details, see "Working with Custom Filters in the Backup Catalog" on page 71.)

3 Expand the VM asset and select the backup or imported backup copy from which you want to recover files.

(To import a backup copy, see <u>To import a cold backup copy</u> or <u>To import a hot backup copy</u> in the Administrator Guide for Recovery Series and Unitrends Backup.)

4 Click Recover Files.

Image: Second Secon								
Backup Catalog 2 File Lavel Recovery Instant Recovery Replicas Coplional) Coplional) Coplional) Coplional) Coplional) Coplional) Coplional) Coplional) Coplianal	UNITRE	NDS					°o	<u>a</u> <u>^0</u>
	DASHBOARD	Backup Catalog 2 File Level Recovery	Instant Recovery	Replicas			3 Modify s	(Optional) settings and click Filter Or
Image: Protect Image: CentCOSS_rpm, 4_250 Dominique-313 BufDcEDDMinuteWands.com VMware Asset Name Aspet Name Image: CentCOSS_rpm, 4_250 Dominique-313 BufDcEDDMinuteWands.com VMware Applance Applance Dominique-313 Image: CentCOSS-rpm Applance Applance Dominique-313 Image: CentCOSS-rpm Applance Dominique-313 Image: CentCOSS-rpm Applance Applance Applance Dominique-313 Image: CentCOSS-rpm Applance Ap		Q Search Files 📕 Recover 🖹 Recover Files 5	instant Recovery	🕤 Import to Source 🔦 Hold	Delete		Selec	t a filter from the list
Image: Sector	PROTECT	8 B	APPLIANCE	HOST	APPLICATION	MODE	FILTER BACKUPS	
RECOVER 	- 4	CentOS5_rpm_4_250	Dominique-313	Build according to the second scom	VMware		Asset Name	
I Control C	RECOVER	Final CentOS6-rpm	Dominique-313	CentOS6-rpm	Agent-Based		Appliance	Dominique-313 V
i j OBS i k docubuntu Dominique-313 nutanix01 AHV Application All i k docubuntu Dominique-313 nutanix01 AHV Full Mode All i k docubuntus Dominique-313 nutanix01 AHV Full Mode All i k docubuntus Dominique-313 nutanix01 AHV Full Form 02/03/2018 i k docubuntus Dominique-313 nutanix01 AHV Full Form 02/03/2018 i k docubuntus Dominique-313 Blace Mode All i k docubuntus Dominique-313 Blace Mode Internet i k docubuntus Domi	-	🕨 🔲 🚾 CentOS6_rpm	Dominique-313	BUPD crow in .com	VMware		Host	All
Image: Section of the sectin of the section of the section of the sect	JOBS	doc-ubuntu	Dominique-313	e-313 nutanix01 AHV			Application	
Image: A construction Image: A construction Dominique-313 nutanix01 AHV Full Mode All Expand asset and select backup Image: A construction Dominique-313 nutanix01 AHV Full From 02/03/2018 Image: A construction 02/09/2018 Image: A construction Image: A con		🔽 🗆 🗙 doc-W2012R2	Dominique-313	nutanix01	AHV		Application	All
Image: Stand asset and select backup Image: Stand asset and select backup <td><u>и</u> R4 хтз</td> <td>D2/06/2018 04:14:08 pm (Warning)</td> <td>Dominique-313</td> <td>nutanix01</td> <td>AHV</td> <td>Full</td> <td>Mode</td> <td>All</td>	<u>и</u> R4 хтз	D2/06/2018 04:14:08 pm (Warning)	Dominique-313	nutanix01	AHV	Full	Mode	All
Land select backup 	Expand asset	🗆 💽 🔺 02/06/2018 12:00:55 am (Warning)	Dominique-313	nutanix01	AHV	Full	From	02/03/2018
backup 	and select	doc-Windows-7_6_DB	Dominique-313	B S.com	VMware		То	02/09/2018
A Dominique-313 BURELLEMMENTALIZION VMware Agent-Based Dominique-313 BURELLEMMENTALIZION VMware Dominique-314 MUZELLEMMENTALIZION VMWare Dominique-315 MUZELLEMMENTALIZION VMWare Dominique-315 BURELLEMMENTALIZION VMWare Dominique-316 MUZELLEMMENTALIZION VMWare Dominique-317 MUZELLEMMENTALIZION VMWARE Dominique-318 MUZELLEMMENTALIZION VMWARE DOMINIQUE VMUZELLEMMENTALIZION VMUZELLE	backup	doc-Windows-8	Dominique-313	doc-Windows-8	Agent-Based		Held	0
Image: Second	÷	doc-WinVista_214_DB	Dominique-313	BURcom	VMware			
Image: Section of the section of th		DocNode1	Dominique-313	Bl :om	VMware		Successes	
Image: HVSVR2008R2 Dominique-313 HVSVR2008R2 Agent-Based Backup Copy (Cold) Backup Copy (Cold) Backup Copy (Hol) Image: Im		DocNode2	Dominique-313	B	VMware		Туре	Backup ^
Image: W184_206 Dominique-313 BUID C00104 with with with with with with with with		▶ □ ■ HVSVR2008R2	Dominique-313	HVSVR2008R2	Agent-Based			Backup Copy (Cold) Backup Copy (Hot)
Image: Select Filter Dominique-313 Deminique-313 Deminique-313 Deminique-313 Manage Filter Image: Select Filter Dominique-313 Inutanix01 AHV Manage Filters Image: Select Filter Image: Select Filter Dominique-313 W2260 Agent-Based Select Filter		▶ □ <u>₩</u> UB_4_206	Dominique-313	Butto cool in tunibundum	VMware			
W2012R2-pm-2 Dominique-313 nutanix01 AHV MANAGE FILTERS @ Image: W2260 Dominique-313 W2260 Agent-Based Select Filter Backups last 7 da v		Unitrends_doc-Windows-8	Dominique-313	B	VMware			Clear Filter
▶ 🗋 🗮 W2260 Dominique-313 W2260 Agent-Based Select Filter Backups last 7 da 🗸		▶ 🗌 🗙 W2012R2-pm-2	Dominique-313	nutanix01	AHV		MANAGE FILTERS	
		▶ 🔲 🚆 W2260	Dominique-313	W2260	Agent-Based		Select Filter	Backups last 7 da

5 Click **Confirm** to continue. The appliance creates the recovery object.

Note: If you receive an error on a Unitrends Backup appliance while creating the recovery object, increase the memory allocation for the Unitrends Backup VM by using the host that manages it.



6 Click View FLR.



Proceed to "Step 2: Recover files".



Step 2: Recover files

View the recovery object on the File Level Recovery tab to see which recovery options are supported for the VM you selected. Use one of the following procedures to recover files.

- "To recover files by browsing and downloading to a .zip file"
- "To recover files by mounting the CIFS share" on page 45
- "To recover files by mounting the iSCSI LUN" on page 47

To recover files by browsing and downloading to a .zip file

1 On the **File Level Recovery** tab, locate the recovery object.

Recovery objects display on the tab with the following details: the name of the VM asset for which the object was created, the status of the object, the date and time it was created, the length of time it has existed on the appliance, and whether it can be accessed through iSCSI or CIFS.

2 Select the recovery object and click **Browse/Download**.

Ur	NITRE	NDS				°o	0	¥0
	DASHBOARD	Backup Catalog	File Level Recovery	Instant Recovery	Replicas			
		Show Details	Browse/Download 2 Rem	ove				
	PROTECT	NAME		STATUS	STARTED	DURATION	iSCSI	CIFS
-	1—	doc-W2012R2		Available	02/09/2018 03:29:23 pm	00:01:22	Yes	Yes
- P	RECOVER							

3 In the File Browser, select or drag files and/or directories to recover.

Note: Softlinks (also called *symbolic links*) are excluded from download. If you select a directory that contains files and softlinks, only the files are downloaded.

4 Click **Download**.



Download

Cancel

ect a file to restore.	Add to selected files list	
Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files Image: Select files	yolume1/PCBP/Logs.dir/BPNETD_0.log/ volume1/PCBP/Logs.dir/BPNETD_1.log/ volume1/PCBP/Logs.dir/BPNETD_2.log/ volume1/PCBP/Logs.dir/BPNETD_2.log/	~
	File Selector 4	

5 Click **Confirm** to download the selected files to a *.zip* file. The *.zip* file is downloaded to your browser's default location.

Conf	irmation		?		
✓	Do you wish to download the selected files?				
		Confirm	Cancel		

Notes:

- Volumes are assigned numbers during recovery that do not necessarily match the numbers from the original disks.
- The duration of the download is impacted by various factors, such as the size of the files, bandwidth, and download speed.
- Persistent browser and UI sessions are required to create the *.zip* file in the browser's default download location. If you close the browser or UI session during the recovery, do one of the following:
 - For downloads that are 500MB or smaller, you must run a new job.
 - For downloads that are greater then 500MB, access the recovered files in the source appliance's
 //downloads directory by entering <SourceApplianceIP>//downloads in an Internet browser. Do not
 download these files until you see the Unitrends-Restore.zip file. While the recovery is in progress,

Release 10.1.1-3 | April 2018

you see files in this directory, but the download is not complete until the *.zip* file has been created. (Recoveries are automatically removed from the */downloads* directory after 72 hours.)

6 When the download completes, the *Unitrends-Restore.zip* file displays in the browser. Select whether to open or save the file.

Opening Unitrends-R	estore.zip	\times							
You have chosen to	open:								
🔢 Unitrends-Re	store.zip								
which is: Compressed (zipped) Folder (2.1 KB)									
from: blob:	from: blob:								
What should Firefo	What should Firefox do with this file?								
Open with	Windows Explorer (default)								
○ <u>S</u> ave File									
Do this <u>a</u> uto	matically for files like this from now on.								
	Cancel								

7 Access the recovered files in the download location and move them to another location on the local machine.



Image: Image	Compr	essed Folder Tools Extract	Logs.	dir Acces	ss and copy recove	ered files to	another lo	cation	- 🗆	× ~ (?)
\leftarrow \rightarrow \checkmark \uparrow \frown \checkmark Users \Rightarrow DBA	RRE~1 ⇒	AppData → Local	> Ter	mp → Unitrends-R	estore-1.zip → volume	1 → PCBP →	Logs.dir 🗸	Ö Sea	rch Logs.dir	2
E Pictures	* ^	Name	~	Туре	Compressed size	Password	Size	Ratio	Date modif	ïed
recover-asset		BPNETD_0.1	og	Text Document	1 KB	No	1 KE	60%	12/2/2017 1	1:27 PM
🔤 Satori Admin Guide		BPNETD_1.1	og	Text Document	1 KB	No	1 KB	60%	1/18/2018 2	2:52 PM
SLA		BPNETD_2.1	og	Text Document	1 KB	No	1 KE	60%	1/23/2018	7:12 PM

Proceed to "Step 3: Remove the recovery object from the appliance" on page 51.

To recover files by mounting the CIFS share

1 Select **Recover** and click the **File Level Recovery** tab.

Recovery objects display with the following details: the name of the VM asset for which the object was created, the status of the object, the date and time it was created, the length of time it has existed on the appliance, and whether it can be accessed through iSCSI or CIFS.

2 Select the recovery object and click **Show Details**.

UNITRE	NDS		L ROOT	°o	0	A 0
DA SHBOARD	Bac Catalog	File Level Recovery	Instant Recover	ry Replicas		
•	Show Details 😽 E	Browse/Download	Remove			
PROTECT	NAME	STATUS	STARTED	DURATION	iSCSI	CIFS
_ 0_	→ 🗹 🗙 doc-W2012R2	Available	02/12/2018 10:26:01 am	00:00:24	Yes	Yes
RECOVER						

3 Note the CIFS path that displays in the File Level Recovery Details window. You will need this path to mount the CIFS share on the target machine.

File Level Reco	overy Details
Name:	doc-W2012R2 (AHV VM)
Host/Server:	nutanix01
Created:	02/12/2018 10:26:01 am
Appliance:	Dominique-313
CIFS Path:	\\192.161111111111111111111111111111111111
iSCSI (Windows):	On the machine to which you want to restore files, use the Windows ISCSI Initiator. The iSCSI target identifier includes the VM name at the end (e.g.iqn.1995-21.com.unitrends.dpu:ftr.89fb.VMNAME).
	For details, see Recovering files using iSCSI on windows.
iSCSI (Linux):	Login to server or VM to which you want to copy files and download and run the script located at 19 4/iscsi_fir.
Messages:	None
	Close

- 4 Log in to the recovery target workstation.
- 5 Enter the CIFS path into a file browser on the recovery target.

🖳 I 🔲	-			Search Tools	flr177	-	\times
File	Home	Share	View	Search			~ 🕐
$\leftarrow \rightarrow$	× ↑ [\\192.16	5 ∎\f	ilr177 — E	Enter CIFS path 🗸 🗿 🛛 Search flr17	77	Ą

6 Browse the share to locate the files you want to recover.

Notes:

• Volumes are assigned numbers during recovery that do not necessarily match the numbers from the original disks.

• The Windows file explorer contains a setting to hide protected/system files. Turn off this setting to access all files.

🚽 📙 🖛 flr177	Expand directories to acc	ess recovered files	– 🗆 ×
File Home Sh	are View		~ 🕐
← → * ↑ ↓ >	Network > 192.16 14 > flr	177 > ~ ඊ	Search flr177 🔎
at Ouish server	^ Name	Date modified	Туре
	volume5		File folder
Desktop	Volume3		File folder
👆 Downloads	× volume2	1/23/2018 7:37 AM	File folder
🔮 Documents	* volume1	1/18/2018 4:13 PM	File folder
Pictures	🖈 🔡 🚽 volume0	10/11/2017 5:15 AM	File folder
Navigating_ui			
recover_vm			

- 7 Move selected files to another location on the local machine.
- 8 Disconnect the network share by right-clicking the share and selecting **Disconnect**.
- 9 Proceed to "Step 3: Remove the recovery object from the appliance" on page 51.

To recover files by mounting the iSCSI LUN

- 1 Log in to the recovery target.
- 2 Launch the iSCSI Initiator from Administrative Tools in the Control Panel.



3 In the Target field, enter the appliance IP address and click Quick Connect....

The **Discovered targets** field populates with a list of iSCSI LUN targets.

argets	Discovery	Favorite Targets	Volumes and Devices	RADIUS	Configuration
Quick C	Connect				
To disc	over and log	g on to a target usir	ig a basic connection, t	ype the IP	address or 🦰
DNS na	ame of the t	arget and then click	Quick Connect.		2
					_
Target	: 192	. 168 4		Qu	uick Connect
Diama					
DISCOVE	ered targets			_	
					Refresh
		Enter english			

- 4 Select the iSCSI target from the list.
- **5** The iSCSI target is discovered and connected to the local machine. Click **Done**.

Quick Conne	ect
Targets that are available for connection at the I provided are listed below. If multiple targets are to each target individually. Connections made here will be added to the list o to restore them will be made every time this comp	P address or DNS name that you available, you need to connect f Favorite Targets and an attempt juter restarts.
Discovered targets Name	Status
iqn.1995-11.com.unitrends.dpu:fir.aef1.	Connected
Progress report	
Login Succeeded.	

6 On the Volumes and Devices tab, click **Auto Configure** to map drives from the iSCSI target to the local machine (or map them manually if you prefer).

Note: Volumes are assigned letters during recovery that do not necessarily match the letters from the original disks.



Chapter 3: Recovering AHV Backups Provide feedback



Release 10.1.1-3 | April 2018

		ISCS	si initiat	or Propert	ies		
argets	Discovery	Favorite T) Volu	mes and Devic	es RAD	IUS Co	onfiguration
If a pro the list l configur This will for use the Fav	gram or serv below, or dia e all availab bind the vol by the prog orite Target	vice uses a parti ck Auto Configu le devices. lume or device s ram or service. s List.	icular volu re to have so that on This is on	me or device, e the iSCSI init system restar ly effective if	add that iator serv t it is more the associ	volume c ice autor e readily ated tar	or device to matically available get is on
Volume	List:						
Volum	e/mount poi	nt/device					
\\?\Vo	lume{2c088	94d-bf0d-49ab-	b71a-ec2	35611eede}\			
E:\ F:\				3			
H:\		Volumes	are ma	pped to t	he loca	l mac	hine
Configu	matically cor re.	nfigure all availa	ble device	es, click Auto	2	Auto	o Configure
To auto Configu To add	matically cor re. a specific de	nfigure all availa vice, click Add.	able device	es, click Auto	2	Auto	O Configure Add
To auto Configu To add To remo Remove	matically con re. a specific de ive a device	nfigure all availa evice, click Add. , select the dev	able device	en dick	2	Auto	Add
To auto Configu To add To remo Remove To imme	matically con re. a specific de we a device diately remo	nfigure all availa vice, click Add. , select the dev	ible device ice and th click Clear	en dick Auto	2	Auto	Add Remove
To auto Configu To add To remo Remove To imme <u>More a</u>	matically cor re. a specific de we a device diately remo sout Volume	nfigure all availa vice, click Add. , select the dev ove all devices,	ible device rice and th click Clear	en dick Auto en dick	2	F	Add Remove

7 Access the files under the mapped drives and move them to another location on the local machine.

Note: The Windows file explorer contains a setting to hide protected/system files. Turn off this setting to access all files.



Release 10.1.1-3 | April 2018



8 Use the iSCSI Initiator to disconnect from the LUN.



Release 10.1.1-3 | April 2018

		iSC	SI Ini	tiator l	Prope	rties				ľ
argets Disc	covery	Favorite Tar	gets	Volumes	and Dev	vices R	ADIUS	Con	figuration	
To discover DNS name o	and log of the tar	on to a targe get and the	et using n click (a basic Quick Cor	connecti inect.	ion, type	e the IP	addre	SS OF	
Target:							Q	uick Co	onnect	
Discovered t	targets							Def	rech	
Name						St	atus	Kei	rearr	1
iqn. 1995-1	l1.com.u	nitrends.dpu	ı:fir.aef	f1.		C	onnecte	ed		
To connect of click Connect To complete	using ad ct. ely discor	vanced optio	ons, sel	ect a tan	get and	then		Con	nect	
then click Dis For target p	propertie	t. s, including o	onfigur	ation	ssions	.,		Prope	rties	
Disc	connec	t From Al		ione						
			1 5633	NONS		lect		Devi	ces	
The total nu Disconnect	umber o t from al	f active ses I sessions b	sions is y clicki	: 1. ng Yes.		lect		Devi	ces	
The total nu Disconnect	umber o	f active ses I sessions b Yes	sions is y clicki	i 1. ng Yes. No		lect	Cance	Devia	ces Appl	y
The total nu Disconnect	umber o	f active ses I sessions b Yes iSC	sions is y clicki	i 1. ng Yes. No	Proper	lect	Cance	Devi	ces Appl	y
The total nu Disconnect	umber of t from al	f active ses I sessions b Yes iSC Favorite Tai	sions is y clicki	i 1. ng Yes. No tiator I	Proper	lect rties	Cance	Devis l	Appl figuration	y
The total ni Disconnect 2 	umber of t from all covery ect and log of the tar	I sessions b Yes iSC Favorite Ta on to a targ rget and the	sions is y clicki SI Ini rgets n dick (i 1. ng Yes. No tiator I Volumes g a basic Quick Cor	Proper and Dev connection	rties vices F	Cance ADIUS e the IF	Devia	Appl figuration ass or	y
The total nu Disconnect 2 	covery ect and log of the tar	f active ses I sessions b Yes iSC Favorite Tai on to a targ get and the	sions is y clicki SI Ini rgets et using	tiator I Volumes a basic Quick Cor	Proper and Dev connect	rties rices F	Cance ADIUS e the IF	Devia	Appl figuration ass or	y
The total nu Disconnect	covery ect and log of the tai	f active ses I sessions b Yes iSC Favorite Tai on to a targ get and the	sions is y clicki	tiator l Volumes	Proper and Dev connect.	lect rites rices F ion, type	Cance ADIUS a the IF	Devia	Appl figuration iss or ponnect	y
The total nu Disconnect 2 2 argets Disc Quick Conne To discover DNS name o Target: Discovered to Name	covery covery and log	f active ses I sessions b Yes iSC Favorite Tai on to a targ get and the	sions is y clicki SSI Ini rgets et using n dick C	i 1. ng Yes. No Volumes g a basic	Proper and Dev connect.	rties rties inces inon, type Si	Cance ADIUS e the IF	Devia	Appl figuration iss or onnect	y

9 Proceed to "Step 3: Remove the recovery object from the appliance".

Step 3: Remove the recovery object from the appliance

To ensure optimal performance, remove the recovery object from the appliance.

WARNING! If you mounted the CIFS share or iSCSI LUN, be sure to unmount it from the target before you remove the recovery object. Removing the recovery object while the target is still connected causes undesired results and errors on the target machine.

To remove a file-level recovery object

1 Select **Recover** and click the **File Level Recovery** tab.

- **2** Select the recovery object.
- 3 Click **Remove**.

UNITRE	NDS	2		ô	0	A 0
	Backup Catalog	File Level Recovery	Instant Recovery	Replicas		
0	Show Details	rowse/Download	Remove 4			
	NAME	STATUS	STARTED	DURATION	iSCSI	CIFS
-	🗹 🗙 doc-W2012R2	Available	02/09/2018 03:29:23 pm	02:19:18	Yes	Yes
RECOVER	3					

4 Click **Confirm** to continue. The object is removed and no longer displays on the File Level Recovery tab.

Confirm FLR Dele	etion				
Are you sure you want to delete this FLR Object?					
		Confirm	Cancel		
Backup Catalog	File Level Recovery	Instant Recovery	Replicas		
Show Details	Browse/Download	à			
NAME	STATUS	STARTED	DURATION	iSCSI	CIFS
	The FLR object i	s removed			

Recovering files from a host-level backup of a Linux AHV VM

Use the procedures in this section to recover Linux files.

Linux prerequisites and considerations

The following requirements and considerations apply to recovering files from a host-level backup or host-level backup copy of a Linux AHV VM:



Release 10.1.1-3 | April 2018

Prerequisite or consideration	Description
Supported recovery methods	To recover files from a host-level backup or copy, the appliance creates a recovery object that contains the backup's files. For some Linux VMs, this object is also exposed as a CIFS (Samba) share and/or an iSCSI LUN on the backup appliance. After you create the recovery object, you will view it on the File Level Recovery tab to see whether the CIFS and iSCSI options are available.
	You can recover files from this object in several ways. Options include:
	• Browse the recovery object and download selected files to a <i>.zip</i> file. This is the simplest method.
	• Mount the CIFS share on a recovery target machine. From the target machine, select files to recover.
	• Mount the iSCSI LUN on a recovery target machine. From the target machine, select files to recover.
Configuration of the	These requirements apply to the original Linux VM whose backup or backup copy will be used for the recovery:
protected Linux VM	• Software RAID (mdraid) configurations are not supported. If the VM is configured with software raid, you cannot recover files. Recover the entire VM instead, as described in "Recovering an AHV VM" on page 35.
	• For NTFS, FAT32, ext2, ext3, ext4, or xfs Linux file systems, you can recover by downloading to a <i>.zip</i> file or by mounting the CIFS share.
	• For other file systems, including Linux mounted volumes, you must mount the iSCSI LUN to access and recover files. For iSCSI requirements, see "Requirements for recovery by mounting the iSCSI LUN".
Requirements for recovery by	To recover by mounting the iSCSI LUN, the following prerequisites and considerations apply:
mounting the	• The iscsi-initiator-utils package must be installed on the recovery target.
	• For the recovery, iSCSI disks are writable and a 1 GB write limit is enforced. Errors display on the recovery target machine if more than 1 GB is required. In this case, you must recover the entire VM instead.

Linux file-level recovery

Use the following procedures to recover files from a backup, imported backup copy, or hot backup copy of a Linux VM. Before you start, be sure all requirements in "Linux prerequisites and considerations" on page 52 have been met.

- "Step 1: Create the recovery object"
- "Step 2: Recover files" on page 56
- "Step 3: Remove the recovery object from the appliance" on page 62

Step 1: Create the recovery object

Note: If a previously-created recovery object is still mounted for the VM, you must remove it before creating a new one.

- 1 Log in to the backup appliance.
- 2 Select **Recover** and click the **Backup Catalog** tab.

(Optional) Use Filter Backups to the right to customize the backups that display. (For details, see "Working with Custom Filters in the Backup Catalog" on page 71.)

3 Expand the VM asset and select the backup or imported backup copy from which you want to recover files.

(To import a backup copy, see <u>To import a cold backup copy</u> or <u>To import a hot backup copy</u> in the Administrator Guide for Recovery Series and Unitrends Backup.)

4 Click Recover Files.



Release 10.1.1-3 | April 2018

UNITRE	INDS					*o	
DASHBOARD	Backup Catalog 2 File Level Recovery	Instant Recovery	Replicas			3 Modify	settings and click Filter
	Q Search Files 📕 Recover 📑 Recover Files 5	Instant Recovery	🕤 Import to Source 🔦 Hold	🛅 Delete		Sele	ct a filter from the list
PROTECT	8 B	APPLIANCE	HOST	APPLICATION	MODE	FILTER BACKUPS	
_	▶ 🔲 페 CentOS5_rpm_4_250	Dominique-313	B om	VMware		Asset Name	
RECOVER	▶ 🗋 🗮 CentOS6-rpm	Dominique-313	CentOS6-rpm	Agent-Based		Appliance	Dominique-313
	CentOS6_rpm	Dominique-313	BLpm	VMware		Host	All
JOBS	y 🗆 🗙 doc-ubuntu	Dominique-313	nutanix01	AHV		Application	
4	🔽 💽 🔦 02/06/2018 04:13:56 pm (Warning)	Dominique-313	nutanix01	AHV	Full	Application	All
Expand asset	🗆 💽 🔦 02/06/2018 12:00:43 am (Warning)	Dominique-313	nutanix01	AHV	Incremental	Mode	All
and select	doc-Windows-8	Dominique-313	doc-Windows-8	Agent-Based		From	02/03/2018
backup	▶ □ m doc-WinVista_214_DB	Dominique-313	Bl m	VMware		То	02/09/2018
	DocNode1	Dominique-313	Bom	VMware		Held	0
•	DocNode2	Dominique-313	BL	VMware		_	Ĩ
	▶ 🔲 🚆 HVSVR2008R2	Dominique-313	HVSVR2008R2	Agent-Based		Successes	
	▶ □ 🔟 UB_4_206	Dominique-313	Billing	VMware		Туре	Backup ^
	Unitrends_doc-Windows-8	Dominique-313	Bl	VMware			Backup Copy (Cold) Backup Copy (Hot)
	▶ 🗌 🗙 W2012R2-pm-2	Dominique-313	nutanix01	AHV			
	▶ 🗋 🚆 W2260	Dominique-313	W2260	Agent-Based			Clear
						MANAGE FILTERS	
						Select Filter	Backups last 7 da
						Add	Save Delete

5 Click **Confirm** to continue. The appliance creates the recovery object.

Note: If you receive an error on a Unitrends Backup appliance while creating the recovery object, increase the memory allocation for the Unitrends Backup VM by using the host that manages it.



6 Click View FLR.

Notice		
File level recovery job successfully started.		
	View ELR	ОК

Proceed to "Step 2: Recover files".



Step 2: Recover files

Use one of the following procedures to recover files.

- "To recover files by browsing and downloading to a .zip file"
- "To recover files by mounting the CIFS share" on page 58
- "To recover files to a Linux machine by mounting the iSCSI LUN" on page 60

To recover files by browsing and downloading to a .zip file

1 On the **File Level Recovery** tab, locate the recovery object.

Recovery objects display on the tab with the following details: the name of the VM asset for which the object was created, the status of the object, the date and time it was created, the length of time it has existed on the appliance, and whether it can be accessed through iSCSI or CIFS.

2 Select the recovery object and click **Browse/Download**.

UNITRE	NDS			°o 😯	A0
DA SHBOARD	Backup Catalog File Level Recovery	Instant Recovery	Replicas		
-	Show Details Show Details	nove			
PROTECT	NAME	STATUS	STARTED	DURATION	ISCSI CIFS
_ 0	🗹 🗙 doc-ubuntu	Available	02/12/2018 01:59:32 pm	00:00:08	Yes Yes
RECOVER	□ X doc-W2012R2	Available	02/12/2018 10:26:01 am	03:33:39	Yes Yes

3 In the File Browser, select or drag files and/or directories to recover.

Note: Softlinks (also called *symbolic links*) are excluded from download. If you select a directory that contains files and softlinks, only the files are downloaded.

4 Click **Download**.



Release 10.1.1-3 | April 2018

elect a file to restore.	Add to selected files list	
Select files image: select files image: select files image: select files	volume4/hi2.bd/ volume4/hie1/ volume4/file2/	~
		File Selected:3

5 Click **Confirm** to download the selected files to a *.zip* file. The *.zip* file is downloaded to your browser's default location.

Con	irmation		?
~	Do you wish to download the selected files?		
		Confirm	Cancel

Notes:

- Volumes are assigned numbers during recovery that do not necessarily match the numbers from the original disks.
- The duration of the download is impacted by various factors, such as the size of the files, bandwidth, and download speed.
- Persistent browser and UI sessions are required to create the *.zip* file in the browser's default download location. If you close the browser or UI session during the recovery, do one of the following:
 - For downloads that are 500MB or smaller, you must run a new job.
 - For downloads that are greater then 500MB, access the recovered files in the source appliance's /downloads directory by entering <SourceApplianceIP>/downloads in an Internet browser. Do not download these files until you see the Unitrends-Restore.zip file. While the recovery is in progress, you see files in this directory, but the download is not complete until

the *.zip* file has been created. (Recoveries are automatically removed from the */downloads* directory after 72 hours.)

6 When the download completes, the *Unitrends-Restore.zip* file displays in the browser. Select whether to open or save the file.

Opening Unitrends-Restore.zip								
You have chosen to open:								
Unitrends-Restore.zip								
which is: zip Archive (24.0 MB)								
from: blob:								
What should Firefox do with this file?								
<u>O</u> pen with 7-Zip File Manager (default)								
Do this <u>a</u> utomatically for files like this from now on.								
OK Cancel								

7 Access the recovered files in the download location and move them to another location on the local machine.

Note: The Windows file explorer contains a setting to hide protected/system files. Turn off this setting to access all files.

<mark>.</mark> <mark>.</mark> , .			Compressed	Folder Tools	volume4	-		\times		
File Home SI	hare	View	Extr	ract				~ (
\leftarrow \rightarrow \checkmark \land AppData \rightarrow Local \rightarrow Temp \rightarrow Unitrends-Restore-2.zip \rightarrow volume4 \checkmark \circlearrowright										
🔹 Ouick access		^ Na	ame	Туре		Compressed size	3 iten	าร		
Desktop	*] file1	File		75 KB				
Downloads	*		file2 hi2.txt	File Text D	ocument	75 KB 1 KB				
🗄 Documents	*									
Pictures	*		Access a	ind copy re	ecovered files to	another location				
Navigating_ui										

Proceed to "Step 3: Remove the recovery object from the appliance" on page 62.

To recover files by mounting the CIFS share

1 Select **Recover** and click the **File Level Recovery** tab.

Recovery objects display with the following details: the name of the VM asset for which the object was created, the status of the object, the date and time it was created, the length of time it has existed on the appliance, and whether it can be accessed through iSCSI or CIFS.

2 Select the recovery object and click **Show Details**.

U		NDS		L ROOT	°o	Ø		A 0
88	DASHBOARD	Backup Catalog	File Level Recovery	1 2 Instant Recovery	Replic	as		
0		Show Details 4 B	rowse/Download	Remove				
	PROTECT	NAME	STATUS	STARTED	DURATION	iSCSI	CIFS	
-		🔽 🗙 doc-ubuntu	Available	02/12/2018 01:59:32 pm	80:00:00	Yes	Yes	
K	RECOVER	🗌 🗙 doc-W2012R2	Available	02/12/2018 10:26:01 am	03:33:39	Yes	Yes	

3 Note the CIFS path that displays in the File Level Recovery Details window. You will need this path to mount the CIFS share on the target machine.

File Level Recovery Details								
Name:	doc-ubuntu (AHV VM)							
Host/Server:	nutanix01							
Created:	02/12/2018 01:59:32 pm							
Appliance:	Dominique-313							
CIFS Path:	\\194\ftr171							
iSCSI (Windows)	On the machine to which you want to restore files, use the Windows ISCSI Initiator. The ISCSI target identifier includes the VM name at the end (e.g.iqn.1995-21.com.unitrends.dpu:fir.89fb.VMNAME).							
	For details, see Recovering files using iSCSI on windows.							
iSCSI (Linux):	Login to server or VM to which you want to copy files and download and run the script located at 19/iscsi_flr.							
Messages:	None							
	Close							

- 4 Log in to the recovery target workstation.
- 5 Enter the CIFS path into a file browser on the recovery target.

	↓ volur	me4	Compressed Fo		-		\times	
File	Home	Share	View	Extract				~ 🕐
$\leftarrow \rightarrow$	· ↑	\\192.	4\fl	r171	Enter	CIFS	path	P

6 Browse the share to locate the files you want to recover.

Note: Volumes are assigned numbers during recovery that do not necessarily match the numbers from the original disks.

Home Sr	nare v	lew				
→ * ↑	Network	> 192.168.20.214 >	flr171 ⇒		✓ ♂ Search flr171	
📃 Desktop	* ^	Name	Date modified	Туре	volume4	
🖊 Downloads	*	volume0	10/9/2017 10:44 PM	File folder	File folder	
Documents	*	volume1	10/10/2017 4:18 PM	File folder		
Pictures	*	🔍 volume4	10/9/2017 10:44 PM	File folder		
Navigating ui						

- 7 Move selected files to another location on the local machine.
- 8 Disconnect the network share by right-clicking the share and selecting **Disconnect**.
- **9** Proceed to "Step 3: Remove the recovery object from the appliance" on page 51.

To recover files to a Linux machine by mounting the iSCSI LUN

Use these steps to mount the iSCSI LUN to the target machine and copy the files.

1 In the appliance UI, select **Recover** and click the **File Level Recovery** tab.

Recovery objects display with the following details: the name of the VM asset for which the object was created, the status of the object, the date and time it was created, the length of time it has existed on the appliance, and whether it can be accessed through iSCSI or CIFS.

2 Select the recovery object and click **Show Details**.

UNITRE	NDS		👤 ROOT	°o	0		A 0
	Backup Catalog	File Level Recover	y 2 Instant Recovery	Replic	cas		
0	Show Details 4	Browse/Download	Remove				
PROTECT	NAME	STATUS	STARTED	DURATION	iSCSI	CIFS	
	🔽 🗙 doc-ubuntu	Available	02/12/2018 01:59:32 pm	80:00:00	Yes	Yes	
RECOVER	🗌 🗙 doc-W2012R2	Available	02/12/2018 10:26:01 am	03:33:39	Yes	Yes	

3 Note the full path of the iSCSI mount point directory that displays in the File Level Recovery Details window. You will need this path to mount the iSCSI object on the target machine. The mount point is normally: /iscsi_flr.



Release 10.1.1-3 | April 2018

File Level Reco	overy Details								
Name:	oc-ubuntu (AHV VM)								
Host/Server:	utanix01								
Created:)2/12/2018 01:59:32 pm								
Appliance:	Dominique-313								
CIFS Path:	\\19								
iSCSI (Windows):	On the machine to which you want to restore files, use the Windows ISCSI Initiator. The iSCSI target identifier includes the VM name at the end (e.g:iqn.1995-21.com.unitrends.dpu.flr.89fb.VMNAME).								
	For details, see Recovering files using iSCSI on windows.								
iSCSI (Linux):	Login to server or VM to which you want to copy files and download and run the script located at 19_1100_000_ /iscsi_fr.								
Messages:	None Note the iSCSI mount point, which is normally /iscsi_flr								
	Close								

- 4 Log in to the recovery target.
- **5** Enter the following command to change to the */tmp* directory:

	# cd /tmp
6	Run the following command to copy the <i>iscsi_flr</i> script from the backup appliance:
	# wget http:// <appliance ip="">/iscsi_flr</appliance>
7	After the script downloads, add the execute permission:
	# chmod +x iscsi_flr
8	Run the following command to mount the recovery object:
	# ./iscsi_flr mount
9	Enter the appliance IP address:
	# Enter address of the Unitrends backup system: <appliance ip=""></appliance>
10	Enter the full path of the mount point directory. The full path is likely: /iscsi flr. This procedure uses

10 Enter the full path of the mount point directory. The full path is likely: /iscsi_flr. This procedure uses /iscsi_flr as an example. Be sure to enter the actual mount point that was displayed in the appliance UI.

Enter mount point directory (full path): /iscsi_flr

11 Discovered iSCSI targets display. Choose the target that contains the appliance IP by entering its number. In this example, session 1 is the appliance target:



12 Change to the mount point directory to access the files. For example:



- 13 Move selected files to another location on the local machine.
- **14** Run the following command from the */tmp* directory to disconnect from the LUN:

./iscsi_flr unmount

15 Proceed to "Step 3: Remove the recovery object from the appliance".

Step 3: Remove the recovery object from the appliance

To ensure optimal performance, remove the recovery object from the appliance.

WARNING! If you recovered by mounting a LUN, be sure to unmount the LUN from the target before you remove the recovery object. Removing the recovery object while the target is still connected causes undesired results and errors on the target machine.

To remove a file-level recovery object

- 1 Select **Recover** and click the **File Level Recovery** tab.
- 2 Select the object to remove from the appliance.
- 3 Click Remove.



4 Click **Confirm** to continue. The object is removed and no longer displays on the File Level Recovery tab.

Confirm FLR Deletion					
Are you sure you want to delete this FLR Object?					
	Confirm	Cancel			
Backup Catalog File Level Recovery	Instant Recovery	Replicas			
Show Details 🚯 Browse/Download 🍡 Remo	ove				
NAME	STATUS	STARTED	DURATION	iSCSI	CIFS
□ × doc-W2012R2	Available	02/12/2018 10:26:01 am	03:33:39	Yes	Yes
The FLR ojbect is r	emoved				

This page is intentionally left blank.



Chapter 4: Managing AHV Hosts and Virtual Machines

Once you have added the AHV host, you can modify AHV host and VM settings, and remove the AHV host if you no longer want to protect its hosted VMs with this Unitrends appliance. See these procedures for details:

- "To edit a virtual host asset"
- "To upgrade a virtual host" on page 66
- "Removing a virtual host asset" on page 67
- "To edit a virtual machine asset" on page 68

To edit a virtual host asset

- **Note:** Because each asset can have only one retention policy, you cannot edit an asset's retention settings if the asset has been added to an SLA policy. For more on SLA policies, see <u>Backup Administration and</u> <u>Procedures</u> in the <u>Administrator Guide for Recovery Series and Unitrends Backup</u>.
- 1 Select Configure > Protected Assets.
- 2 Select the AHV host asset.
- 3 Click Edit.

U	NITRE	NDS						°o 0°	∆ 0
믱	DASHBOARD	Appliances Protected Assets	Copied Ass	ets					
_		🔡 View:Table 💌 DisplayAll 🔻 🚱 A	dd 🔻 🗹	Manage Credentials	Manage Global VM Sett	ings	Update Age	ent 🔹 🗹 Edit	4 Remove
	PROTECT	NAME	ADDRESS	DESCRIPTION	CREDENTIALS	RETENTION	ENCRYPTED	AGENT VERSION	APPLIANCE
		HVSVR2008R2	10	Windows 2008 R2	None	None	No	9.2.0-0	Dominique-313
	RECOVER	📄 🕨 🗧 localhost.localdomain	10 101 200 22	VMware Host	(Unnamed)				Dominique-313
	3	🕂 🕞 nutanix-01	192.100.171.2.10	AHV Host	nutanix-01-New-Credential	None	No	5.1.0.1	Dominique-313
	JOBS	🗌 🖥 W2260		Windows 10	None	None	No	10.0.0-3	Dominique-313
щ	REPORTS								
₽	CONFIGURE								

4 Modify settings and click **Save**.

Release 10.1.1-3 | April 2018

	Edit Virtual Host		0
	Edit settings for nutar	nix-01.	
	Hypervisor	Nutanix-AHV	~ 0
/	Appliance	Dominique-313	\sim
/	Host name	nutanix-01	Ø
/	IP Address	19	0
	Cheberrines		
	Username	root	Ø
Edit settings	Password	•••••	0
	- QUIESCE		
\backslash	Quiesce Settings	Keep Existing Quiesce Setting	ngs 😧
		Overwrite this hypervisor's \	VMs to Crash Consistent 🛛 😢
		Overwrite this hypervisor's \	VMs to Application Consistent 🛛 🛛
\		ENTION	
\	Retention settings will be overwritten.	are applied to all VMs associated wit	th this virtual host. Existing retention settings
	Retention Policy	None	🥝 🎄 Manage Retention
			2 Save Cancel

For details on these settings, see the following topics in the <u>Administrator Guide for Recovery Series and</u> <u>Unitrends Backup</u>:

- Managing asset credentials
- Managing retention settings
- Quiesce settings for host-level backups
- To manage global quiesce settings
- <u>To apply a quiesce setting to one host's VMs</u>

To upgrade a virtual host

Unitrends recommends upgrading virtual hosts to the latest supported version. Refer to the Nutanix documentation for instructions on upgrading. Note the following when upgrading:

- Your Unitrends appliance continues to protect the host with existing schedules as long as the IP address remains unchanged.
- If you change the IP address during the upgrade, update this setting in the appliance UI as described in "To edit a virtual host asset" on page 65. Existing schedules can then continue to protect the host's VMs.
- If VMs are added or removed on the host during the upgrade, refresh the VMs on the appliance to reflect the changes by selecting the **Options** icon in the top-right and clicking **Inventory Sync**.

UNITREN	••••••••••••••••••••••••••••••••••••••	
DASHBOARD	BACKUP SUMMARY	LINVENTORY SYNC (LAST: 11/13/2017 08:00:01 PM, SYNC FAIL
0	0	SET LANGUAGE (EN)
PROTECT	Errors	Not Protected

Removing a virtual host asset

CAUTION! When a virtual host is removed, all backups of its VMs are also deleted. Please use caution when removing a virtual host asset.

Use this procedure to remove a Nutanix AHV cluster from the Unitrends appliance. When you remove a virtual host, all backups of its VMs are also deleted.

To remove a virtual host asset

- 1 Select Configure > Protected Assets.
- 2 Select the AHV virtual host.
- 3 Click **Remove**.
- 4 Check the I understand... box and click **Remove Asset and Delete Backups**.

U	NITRE	NDS					°o	0	A 0
88	DASHBOARD	Appliances Protected Assets 2	Copied Assets						
•		View:Table 💌 DisplayAll 🔻 🚱 Add 🔻	Manag	ge Credentials 🛛 🚷 Ma	nage Global VM Set	tings	Update Agent	• Edit	Remove 4
	PROTECT	NAME	ADDRESS	DESCRIPTION	CREDENTIALS	RETENTION	ENCRYPTED	AGENT VERSION	APPLIANCE
		🔎 🕨 闘 nutanix01		AHV Host	nutanix01				Dominique-313
	RECOVER	3 🗆 🖥 doc-Windows-8	1	Confirm Asset R	emoval				0
		🕒 🖥 doc-Windows-8-2	1 4	Are you sure want	t to delete asset nut	tanix01?			
	JOBS	□ ► 🖥 HVSVR2008R2	10 8	When an accet is	removed all of its I	backupe are de	alatad (backup c	onios are not deleter	n.
_				Wilen all asset is	renioved, all of its i	Jackups are ut	eleted (backup ci	spies are not deleted	iy.
щ	REPORTS			I understand t	hat removing this a	sset will also c	lelete all of its ba	ckups.	
				5		6	Remove Asse	et And Delete Backup	Cancel
\$	CONFIGURE	0				U			

5 The host is removed. Click **OK** to close the Information message.

Note: If you are no longer protecting hosted VMs with this Unitrends appliance, contact Support for assistance removing any unneeded snapshots.



To edit a virtual machine asset

- **Note:** Because each asset can have only one retention policy, you cannot edit an asset's retention settings if the asset has been added to an SLA policy. For more on SLA policies, see <u>Backup Administration and</u> <u>Procedures</u> in the <u>Administrator Guide for Recovery Series and Unitrends Backup</u>.
- 1 Select **Configure > Protected Assets**.
- 2 Click to expand the VM's virtual host to display its VMs.
- **3** Select the VM and click **Edit**.

U	NITRE	NDS							°c	o 0	A 0
88	DASHBOARD	Appliance	Protected	Assets 2 Co	pied Assets						
Д	PROTECT	View:Ta	ble 💌 DisplayAll	Add •	Manage Cree	dentials 🚷 Man	age Global VM Settings	O Update	Agent 🔻 丨	Edit 5 Remove	
,	PROTECT	NAME 👻			ADDRESS	DESCRIPTION	CREDENTIALS	RETENTION	ENCRYPTED	AGENT VERSION	APPLIANCE
	DEADVED	🗆 🖁 V	N2260 3 Expa	and host		Windows 10	None	None	No	10.0.0-3	Dominique-313
	RECOVER		🔢 nutanix-01		190	AHV Host	nutanix-01-New-Credential	None	No	5.1.0.1	Dominique-313
			× .DS-Test			AHV:VM	N/A	None	No	None	Dominique-313
	JOBS		X .QA - Mark - Applic	cation Consistent Tes	t - 2	AHV:VM	N/A	None	No	None	Dominique-313
_	4 Select	t VM	× .QA Very Small Te	est VM :)		AHV:VM	N/A	None	No	None	Dominique-313
ш	REPORTS		× Doc-UB			AHV:VM	N/A	None	No	None	Dominique-313
_			× doc-ubuntu			AHV:VM	N/A	None	No	None	Dominique-313
₽.	CONFIGURE	1) 🖻	× doc-W2012R2			AHV:VM	N/A	None	No	None	Dominique-313
			× doc-W2012R2_res	store		AHV:VM	N/A	None	No	None	Dominique-313

4 Modify settings and click **Save**.

For details on these settings, see the following topics in the <u>Administrator Guide for Recovery Series and</u> <u>Unitrends Backup</u>:

- Encrypting backups
- Managing asset credentials
- Managing retention settings
- Quiesce settings for host-level backups

Release 10.1.1-3 | April 2018

Edit Assets			0
Edit settings of AHV:V	/M - doc-W2012R2		
DETAILS			
Appliance	Dominique-313	\checkmark	\mathbf{A}
Virtual Host	nutanix-01		
Encrypt Backups			
Credentials	None	🗸 🔇 🐐 Manage Credentials	
QUIESCE			Edit settings as needed.
Quiesce Settings	Crash Consistent 2		
	Application Consistent		
			/
Retention Policy	None	🛿 🏘 Manage Retention	
		2 Save Can	cel



This page is intentionally left blank.



Chapter 5: Working with Custom Filters in the Backup Catalog

The Backup Catalog lists the appliance's backups and backup copies, and contains buttons used for recovery and other management tasks. Release 10.1.1-3 introduces a new custom filters feature you can use to quickly change the backups and/or copies that display on this tab.

Upon accessing the Backup Catalog tab, the default filter displays associated backups and/or backup copies.

U	NITRE	NDS					°o	<u>ର ₄</u> ତ
믱	DASHBOARD	Backup Catalog 2 File Level Recovery Insta	int Recovery	Replicas			3 Modify	(Optional) y settings and click Filter
		Q Search Files 📕 Recover 🖹 Recover Files 🕅 Instant	Recovery	Import to Source 🔦 Hold	Delete		Sel	Or ect a filter from the list
	PROTECT	日 國 Name of the protected asset	APPLIANCE	HOST	APPLICATION	MODE	FILTER BACKUPS	
			Akshitha100	VCSA-127-New VMware	VMware	^	Asset Name	
	RECOVER	🕨 🛌 🔤 AppAware_Win2008R2-	Akshitha100	10	VMware		Appliance	All 🗸
ے		Farm	Akshitha100	SP2013 Application	SharePoint 2013		Host	All
	JOBS	guestdb	Akshitha100	Oracle Server	SQL Server 2014		Application	AI
		HVSVR2008R2	Akshitha100	HVSVR2008R2	Agent-Based		Mode	
ш	REPORTS	Mailbox Database Hover over	Akshitha100	Exchange 2010	Exchange 2010		-	
		►	Akshitha100	EDC_Node3C2	SQL Server 2014		From	07/02/2017
\	CONFIGURE	View details	Akshitha100	EDC_Node0SOI	SQL Server 2014		То	10/27/2017
	•	09/27/2017 03:02:00 and	Akshitha100	EDC_Node0 instance	SQL Server 2014	Differential	Held	0
	4	09/23/2017 03:02:12 am Size: 5 MB	Akshitha100	EDC_Node0	SQL Server 2014	Differential	C Surcossos	
Exp	pand asset	09/22/2017 03:03:30 am Storage: Internal	Akshitha100	EDC_Node0	SQL Server 2014	Differential	[♥] Soccesses	
to	view and	09/21/2017 03:02:10 am	Akshitha100	EDC_Node0	SQL Server 2014	Differential	Туре	Backup Imported Backup
- 50	oor buonup	09/20/2017 03:02:41 am	Akshitha100	EDC_Node0 Hyper-V	SQL Server 2014	Full		Backup Copy (Cold) Backup Copy (Hot)
		Small_Meaningless_VM	Akshitha100	UXTeam host	Hyper-V 2008 R2	mode		Clear
		Stars	Akshitha100	EDC_Node3C2	SQL Server 2014			
		ui-pc21014	Akshitha100	ui-pc21014 based	Agent-Based		MANAGE FILTERS	0
		W2K8SQL2K8	Akshitha100	UXTeam asset	Hyper-V 2008 R2	*	Select Filter	Today

To change the backups and copies that display, you can modify settings manually or apply a custom filter. See these topics for details:

- "To modify the display manually"
- "To add a filter" on page 72
- "To apply a filter" on page 74
- "To assign a default filter" on page 75
- "To edit a filter" on page 76
- "To delete a filter" on page 77

To modify the display manually

1 Modify the values in the Filter Backups fields.

- 72
- 2 Click **Filter** to apply the new settings.

Backup Catalog File Level	Recovery Inst	ant Recovery Replicas		
Search Files Recover Re	ecover Files 🕥 Instant	Recovery Import to Source	e 🛧 Hold 🛅 Delete	💋 Hide Fit
P 🛱	APPLIANCE	HOST	APPLICATION MODE	FILTER BACKUPS
CentOS6-rpm	Dominique-313	CentOS6-rpm	Agent-Based	Asset Name
doc-Windows-8	Dominique-313	doc-Windows-8	Agent-Based	Appliance Dominique-313
DocNode1	Dominique-313	Eom	VMware	Host All
□ ■ W2260	Dominique-313	W2260	Agent-Based	Application All
3	Filter settings are a	applied to the display		Mode Full
		Modify filter settings		From 10/01/2017
				To 02/06/2018
				Held
				Successes
				Type Backup Backup Copy (Cold) Backup Copy (Hot)
				Clear Filter
				Select Filter Today ~
				Add Save Delete

To add a filter

1 In the Manage Filters area, click **Add**.



- 2 Enter the following:
 - A unique name.
 - (Optional) Check **Set as default** to automatically load this filter.
- 3 Click Save.


Release 10.1.1-3 | April 2018

Add Filter		1 Enter name	?
Filter Name	Cold c	opy 7 days	
Set as default	2	(Optional) Check box to load by default	
Appliance	Load L	ocal Only	
Days Range	1		
Types	backup	p,imported	
	3	- Save Cancel	

4 The new filter is selected in the Select Filter list. Modify settings in the filter fields as needed, then click **Save**.

FILTER BACKUPS		
Asset Name		
Appliance	Dominique-313	
Host	All	
Application	All	
Mode	All	
From	01/31/2018	
То	02/06/2018	
Held	0	Modify settings
Successes		
Туре	Backup Imported Backup Backup Copy (Cold) Backup Copy (Hot)	
	Clear Filter	New filter is selected in the list
MANAGE FILTERS		
Select Filter	Cold copy 7 days 2 Add Save Delete	

5 Review settings and click **Save** to exit.



UNITRENDS

Release 10.1.1-3 | April 2018

Edit Filter	0	
Filter Name	Cold copy 7 days	
Set as default FILTER INFORMATION		1
Appliance	Load Local Only	Review
Days Range	7	setungs
Types	cold copy	
	2 Save Cancel	
MANAGE FILTERS		
Select Filter	Today	~
	Today Backups last 7 days Cold copy 7 days Filte	er is added

To apply a filter

Apply a custom filter by selecting it in the **Select Filter** list.



Release 10.1.1-3 | April 2018

Backup Catalog	File Level Recovery	Instant Recovery	Replicas				
Search Files Reco	over 🖹 Recover Files 💱) Instant Recovery	Import to So	ource 🛧 Hold	d Delete	Þ	Hide Filte
5 8	APPLIANCE	HOST	APPLICATION	MODE	FILTER BACKUPS		
doc-ubuntu	Dominique-313	nutanix01	AHV		Asset Name		
doc-W2012R2	2 Dominique-313	nutanix01	AHV		Appliance	Dominique-313	~
	2 Filter settings are	applied to the disp	lay		Host	All	~
					Application	All	~
					Mode	All	~
					From	01/31/2018	
					То	02/06/2018	
					Held	0	
					Successes		
					Туре	Backup Imported Backup Backup Copy (Co Backup Copy (Ho	Id) t) v
						Clear	Filter
					MANAGE FILTERS		
					Select Filter	Cold copy 7 day	s
					Add	Save D	elete

To assign a default filter

Upon accessing the Backup Catalog tab, the default filter is automatically applied, and backups and/or backup copies that meet the filter criteria display. The appliance's default filter displays today's backups and imported backup copies. To assign a different default filter, do one of the following:

- Add a new custom filter. In the Add Filter dialog, check the **Set as default** box. For details, see "To add a filter" on page 72.
- Make an existing filter the new default by using these steps:

Note: If you have already assigned a default filter and want to change your selection, simply check the **Set as default** box while creating a new filter or modifying an existing filter. This clears the **Set as default** checkbox of the previous default filter.

1 Select the filter and click **Save**.

UNITRENDS

Release 10.1.1-3 | April 2018

		💋 Hide Filter	
FILTER BACKUPS			
Asset Name			
Appliance	Dominique-313	~	
Host	All	~	
Application	All	\sim	
Mode	All	\sim	
From	01/31/2018		
То	02/06/2018		
Held	0		
Successes			
Туре	Backup Imported Backup	^	
	Backup Copy (Cold) Backup Copy (Hot)	~	
	Clear	Filter	
MANAGE FILTERS)	2	1
Select Filter	Backups last 7 days	~	Select the
	Add Save	Delete	from the I

2 Check the **Set as default** box, then click **Save**.

Edit Filter	
Filter Name	Backups last 7 days
Appliance	Load Local Only
Days Range	7
Types	backup, imported
	2 Save Cancel

To edit a filter

- 1 Select the filter.
- 2 Modify settings in the filter fields as needed, then click **Save**.

Release 10.1.1-3 | April 2018

FILTER BACKUPS		
Asset Name		
Appliance	Dominique-313	~
Host	All	~
Application	All	~
Mode	All	~
From	01/24/2018	
То	02/06/2018	
Held	0	Modify settings
Successes		
Туре	Backup Imported Backup Backup Copy (Cold)	
	Backup Copy (Hot)	v /
	Clear F	itter Select the filter
MANAGE FILTERS	3	
Select Filter	Backups last 7 days	
	Add Save Del	ete

3 Review settings, modify name (optional), check the **Set as default** box (optional), then click **Save**.



To delete a filter

UNITRENDS

1 Select the filter, then click **Delete**.



2 Click **Delete Filter** to confirm.

Chapter 5: Working with Custom Filters in the Backup Catalog Provide feedback

Release 10.1.1-3 | April 2018

Confirm Filter Removal				
Are you sure want to delete the catalog filter Cold copy 7 days?				
	Delete Filter Cancel			
MANAGE FILTERS	Filter is removed from the list			
Select Filter	Today 🗸			
	Today			
	Backups last 7 days			

UNITRENDS