AHV Protection Guide

User Guide | April 2018

AHV Protection Guide

Release 10.1.1-3 | Version 3.05042018

Provide feedback

UNITRENDS

Copyright

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

Contents

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 host-level 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

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.

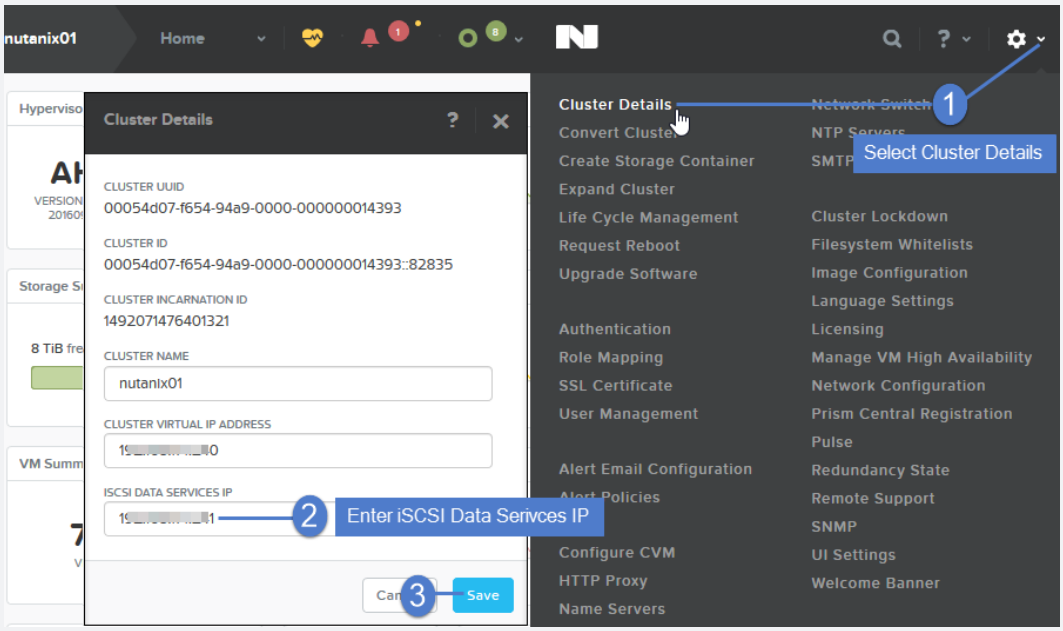
General AHV requirements

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

Item	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.

Item	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: Configuring Authentication) to use these settings: – In the Directory List add a new directory of type **Active Directory** and connection **LDAP**. For the Directory URL, specify **ldap://<ip-address>:<port>** – 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

Item	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: Configuring Authentication) to use these settings: – In the Directory List add a new directory of type **Active Directory** and connection **LDAP**. For the Directory URL, specify **ldap://<ip-address>:<port>** – 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**

Item	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: 1 In the Nutanix Prism interface, select **Cluster Details** from the Options menu. 2 Enter the iSCSI Data Services IP address. 3 Click **Save**. 
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.

Item	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: Nutanix Guest Tools. • For Windows guests, Nutanix recommends installing VirtIO drivers for enhanced performance and stability. For details, see this Nutanix document: Nutanix Virtio for Windows.
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.

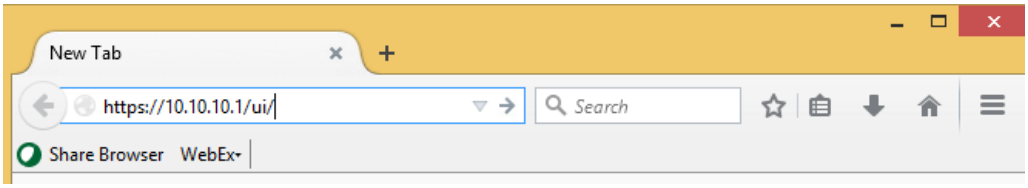
- "To install release 10.1.1-3 on a Unitrends appliance"
- "To install the 10.1.1-3 Windows agent" on page 17

To install release 10.1.1-3 on a Unitrends appliance

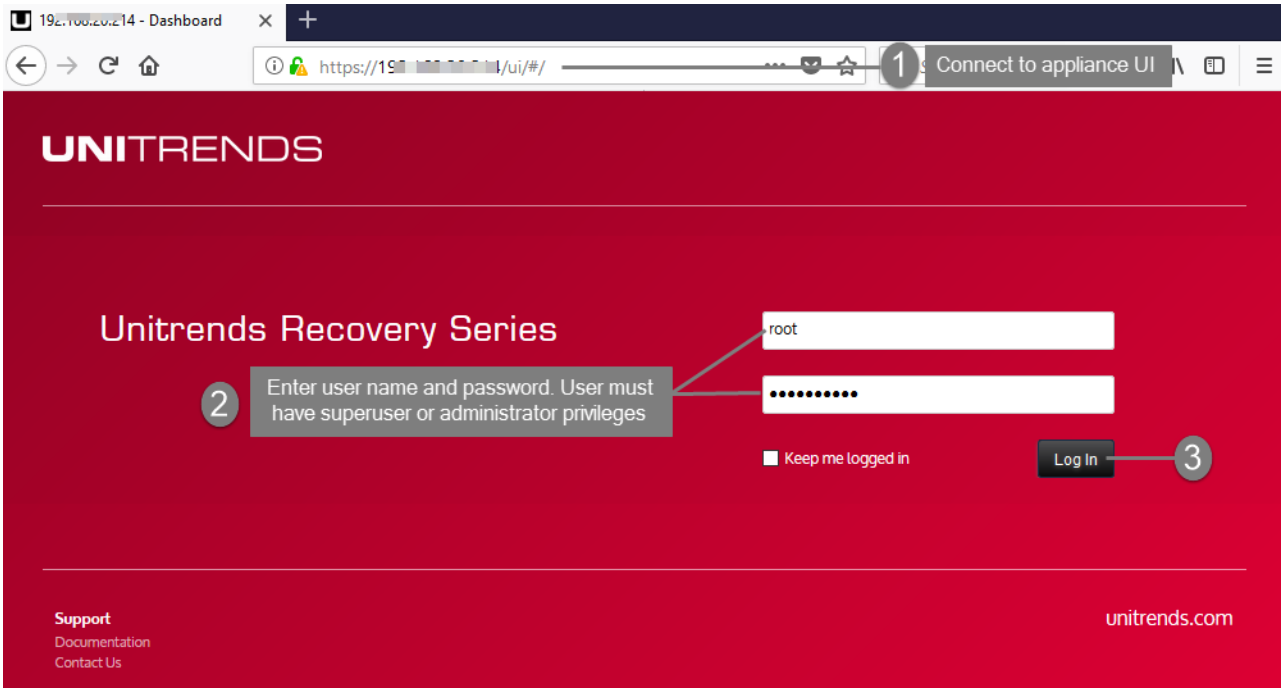
Use the following steps to install the 10.1.1-3 release on your Unitrends appliance:

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.

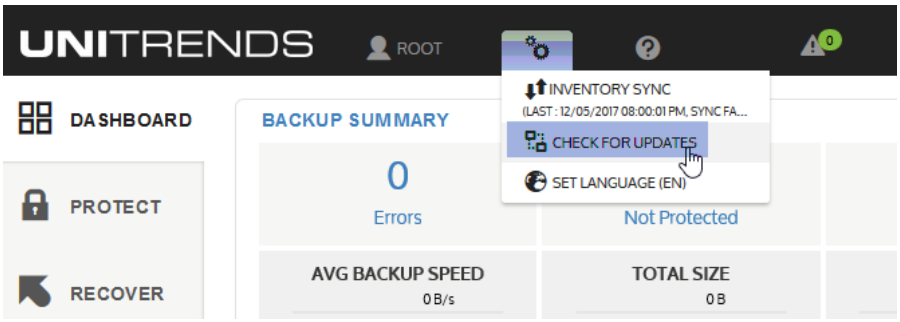
1 Open a Firefox or Chrome browser and connect to the appliance UI by entering: ***https://<applianceIPaddress>/ui/***. For example:



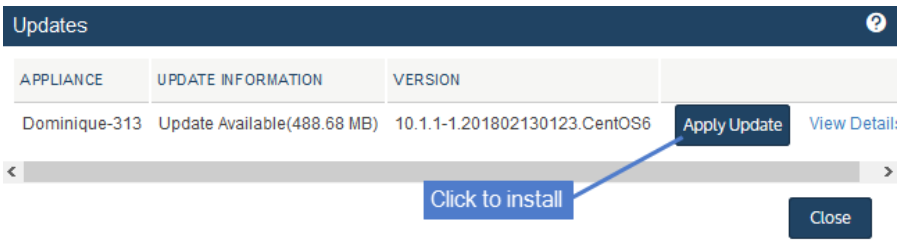
2 Log in as a user with administrative privileges.



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

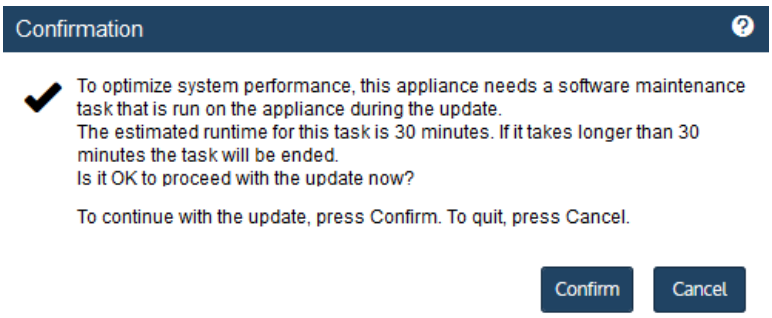


4 A list of available updates displays. Click **Apply Update** to begin the installation.



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.



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.

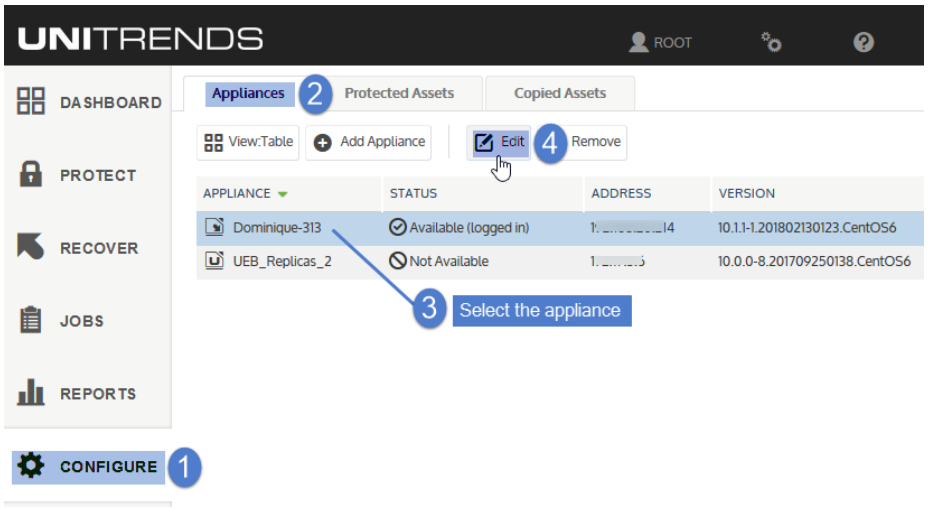
Note: If you receive a message indicating that you need to reboot the appliance to take advantage of the new kernel installed during the upgrade, you can either reboot now or reboot at a later time.

> 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.)

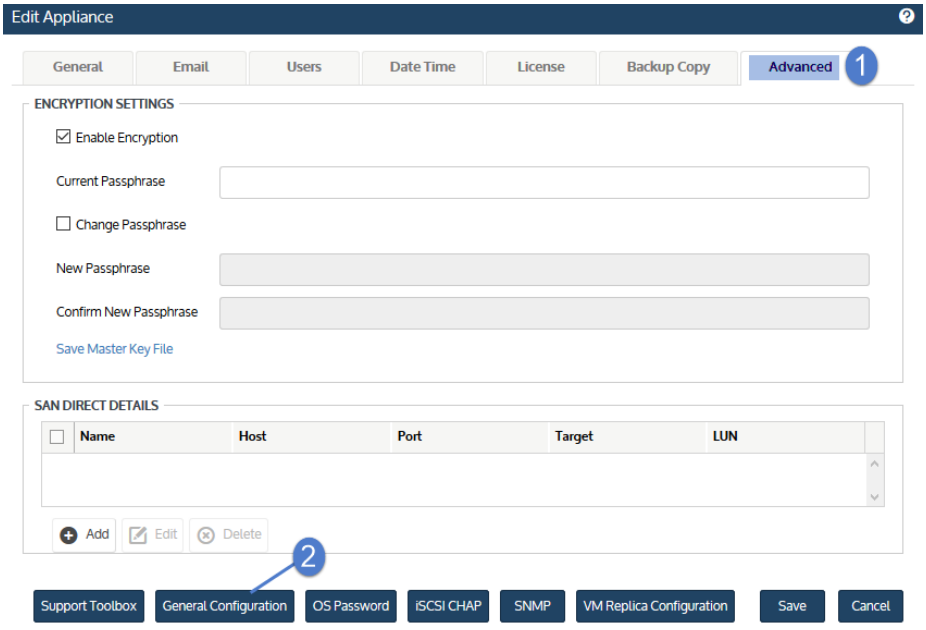
8 Open the browser and log back in to the appliance UI.

9 Enable the AHV feature in the appliance UI by doing these steps:

- On the **Configure > Appliances** page, select the appliance and click **Edit**.

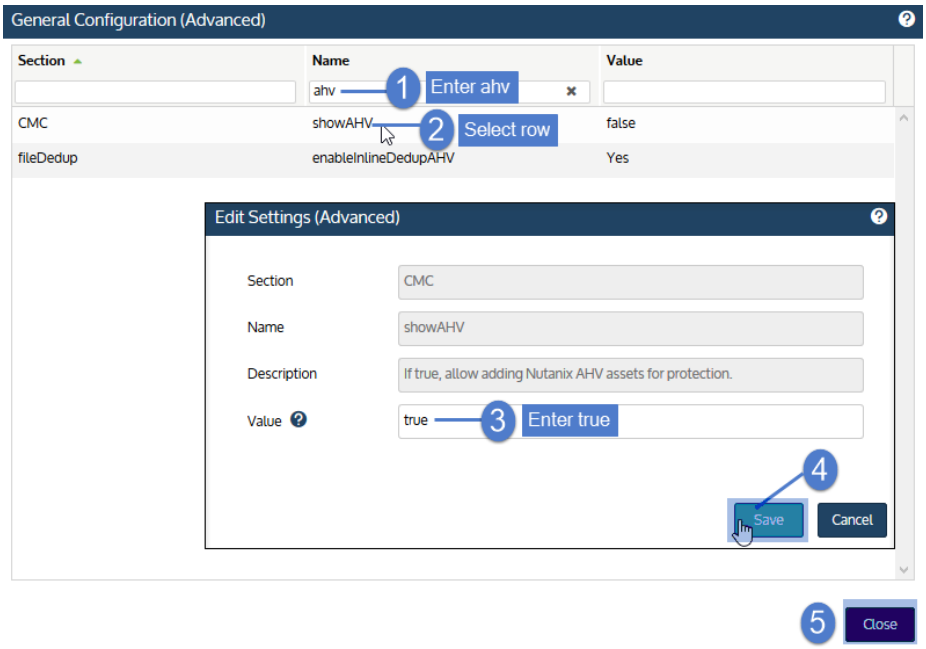


- Click **Advanced** and select **General Configuration**.



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

- Click **Close** to exit.



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 agent-based 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:

Issue	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 KB 3402 for more information.

Issue	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: 1 Clear your browser cache, then close the browser. 2 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.

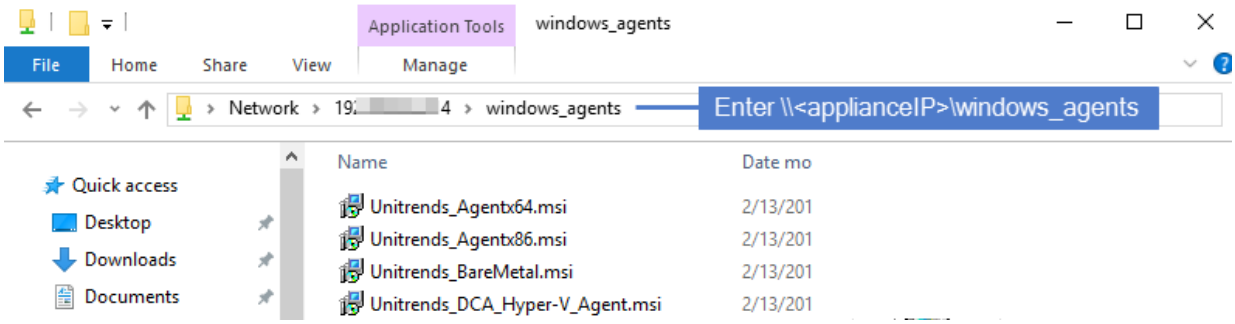
Note: The Windows agent is not used for host-level backups of AHV virtual machines. You do not need to install this agent on AHV VMs that you are protecting with host-level backups.

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

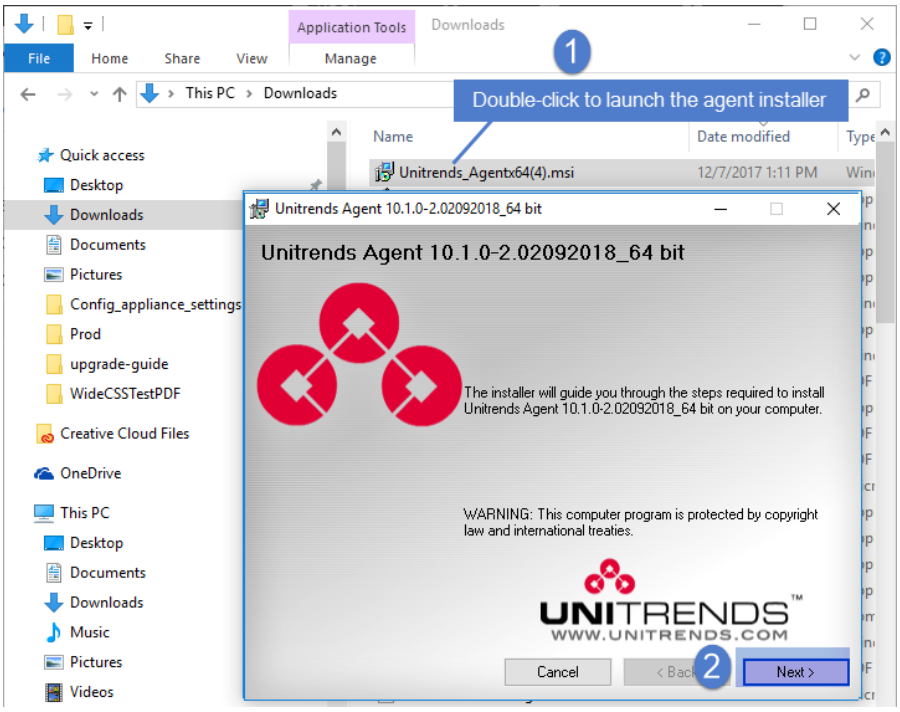
- You must be the user administrator to install or upgrade the Windows agent.
- Volume Snapshot Service (VSS) Exchange Writer is required for the Exchange agent.
- VSS SQL Writer is required for the SQL Server agent.
- VSS Hyper-V Writer is required for the Hyper-V agent.

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**.

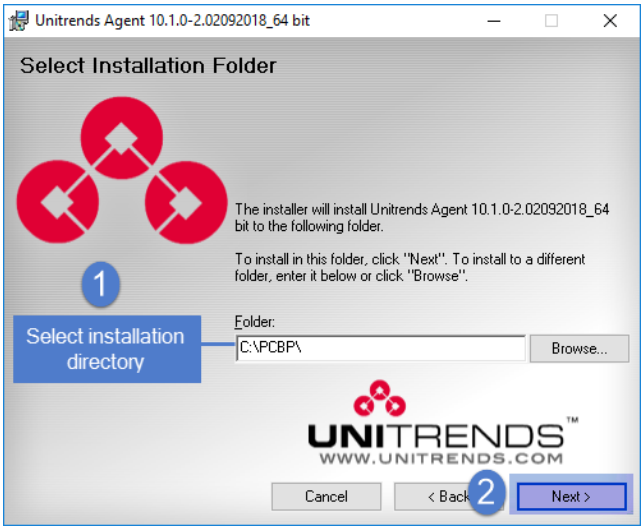


5. Select an installation directory and click **Next**.

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

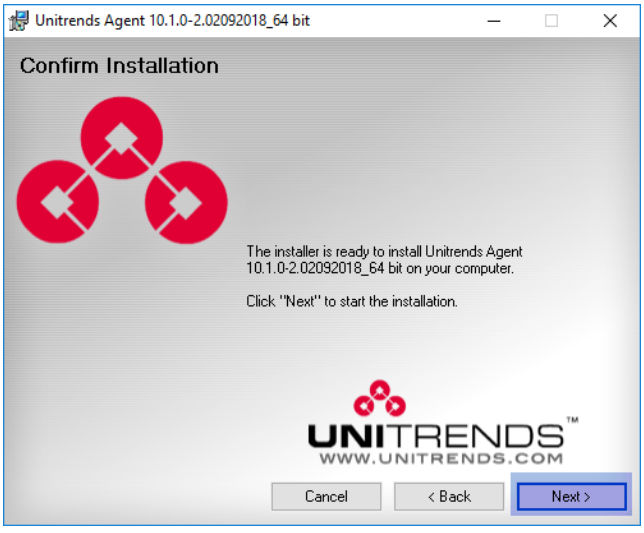
Notes:

- 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.



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

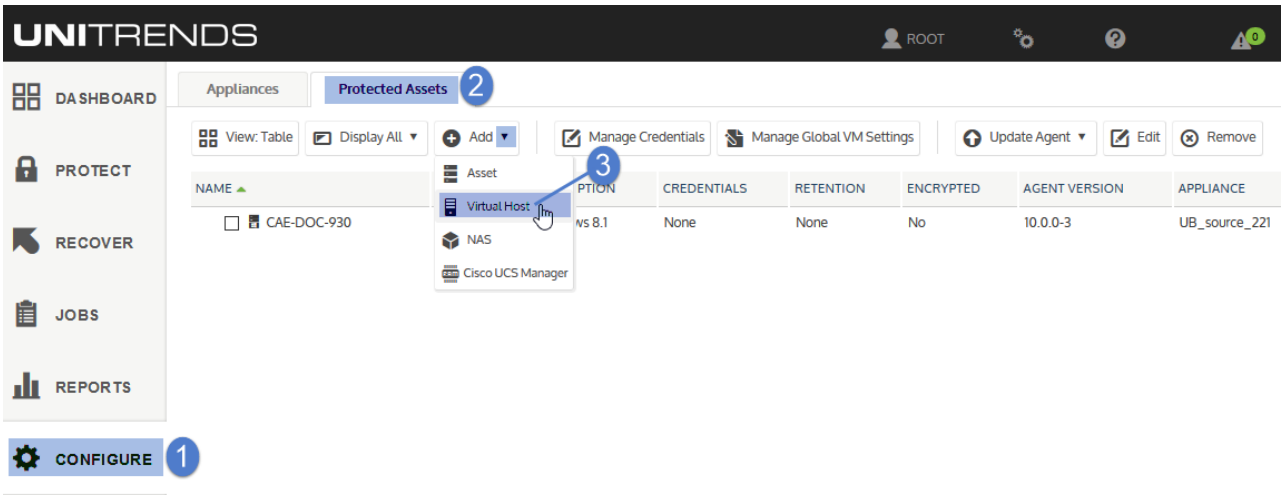
To protect VMs hosted in a Nutanix Acropolis Hypervisor (AHV) environment, you must add the AHV host cluster to the Unitrends appliance as a virtual host asset. Once the AHV host is added, all VMs on that host are automatically discovered and can be selected for protection.

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**.



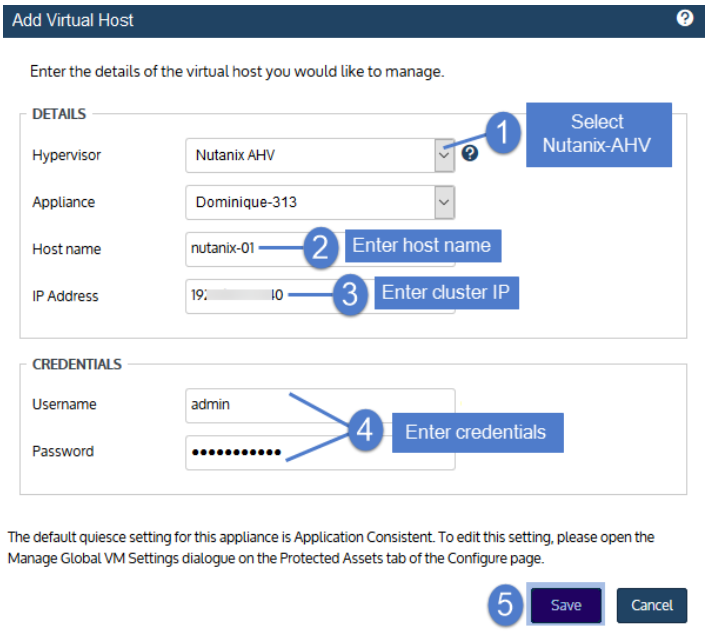
3 Enter the following in the Add Virtual Host dialog:

- 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.

- 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).

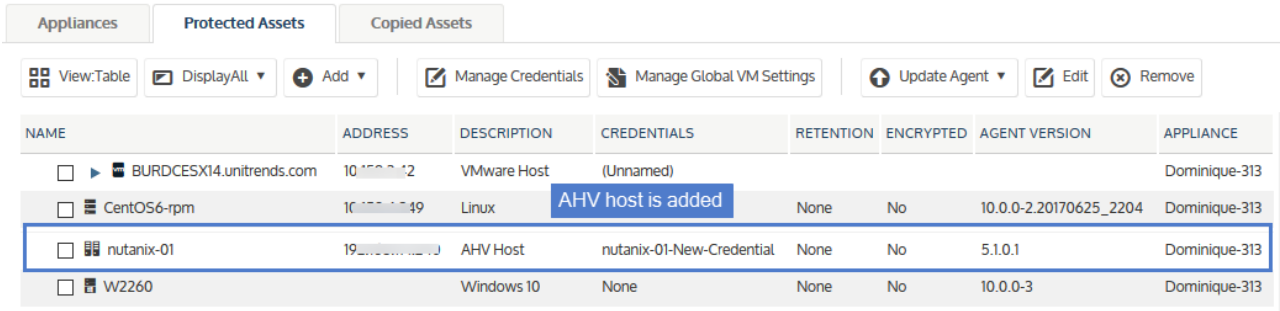
  In the Username field, enter the username and domain in this format: *user@domain*. For example, **jalvarez@unitrends.com**. (For configuration requirements, see "Requirements for directory services authentication in AOS 5.1" on page 9 or "Requirements for directory services authentication in AOS 5.5"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

4 Click **Save**.



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".



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 Backup Administration and Procedures in the Administrator Guide for Recovery Series and Unitrends Backup.

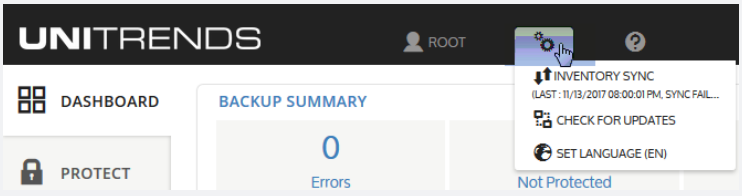
See the following procedures to create AHV backup jobs:

- "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.

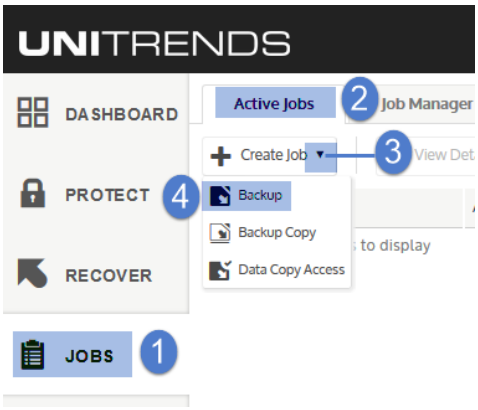
To create a backup job for Nutanix AHV assets

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**.



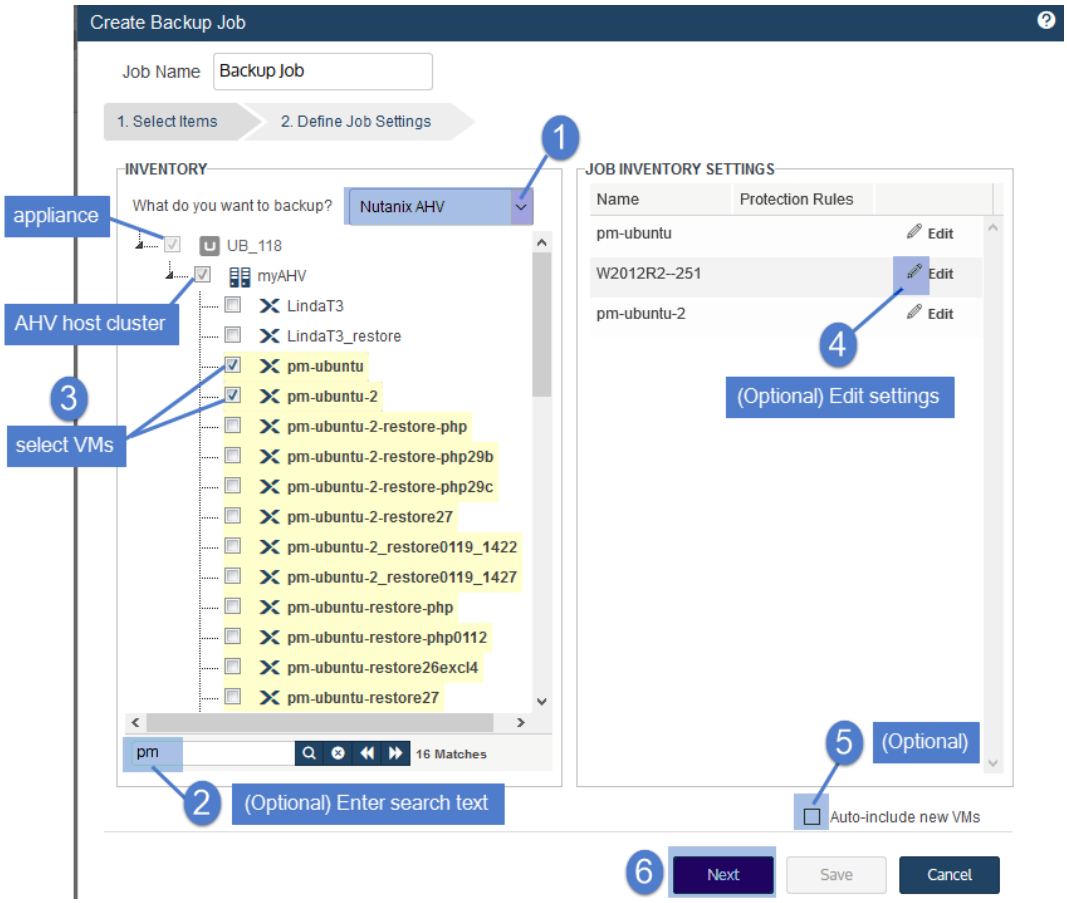
1 Select **Jobs > Active Jobs > Create Job > Backup**.



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.



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.

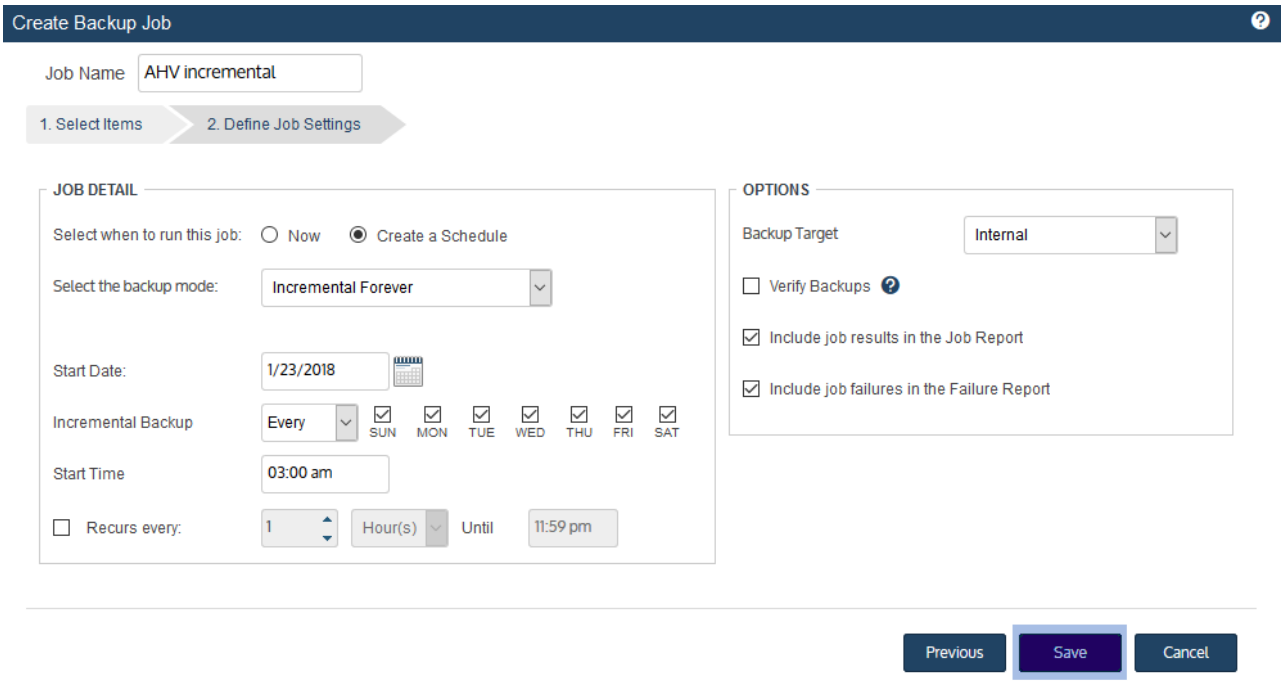
Note: Critical system volumes are required to recover the entire virtual machine. Use care when omitting disks from backup.

5 (Optional) Check the **Auto-include new VMs** box to automatically add newly discovered VMs to the schedule.

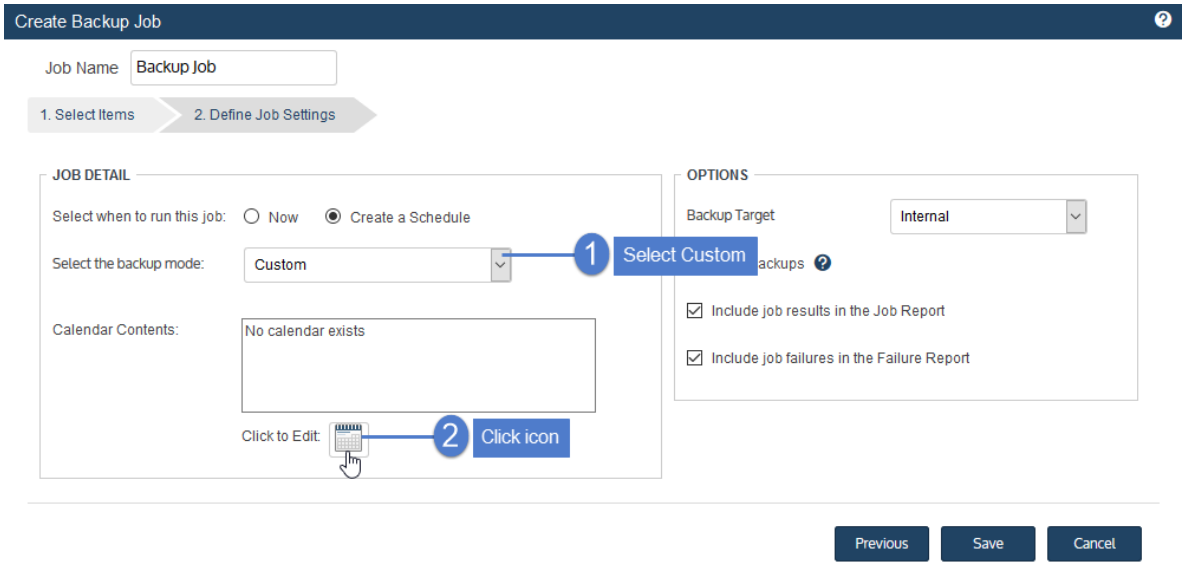
6 Click **Next**.

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:

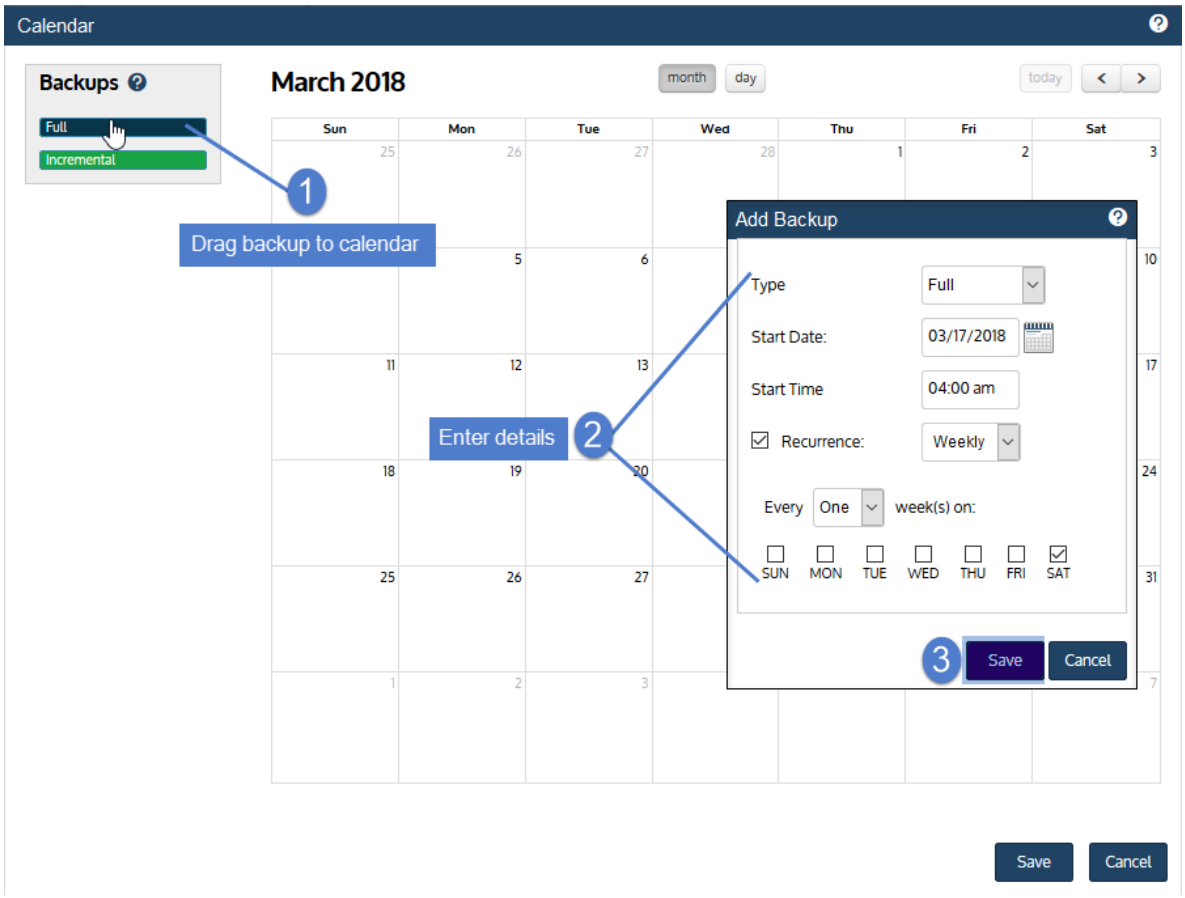


- In most cases, the standard backup modes can be used to create the schedule.
- If you need more granularity, choose the **Custom** mode and do these steps to create a custom backup calendar:
  - Click the calendar icon.

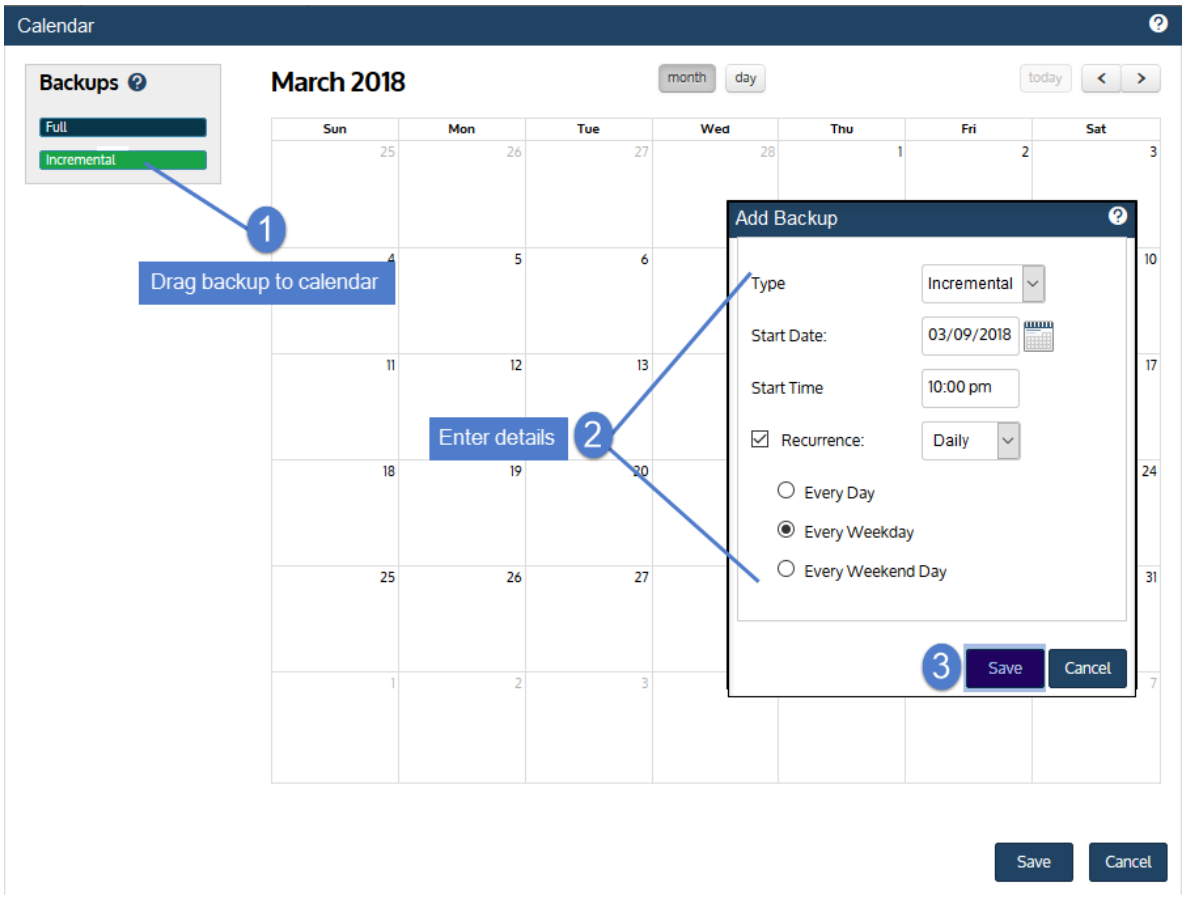


  - In the Calendar dialog, select a backup mode in the Backups area and drag it to a day on the calendar. (You cannot drag to a day in the past.)

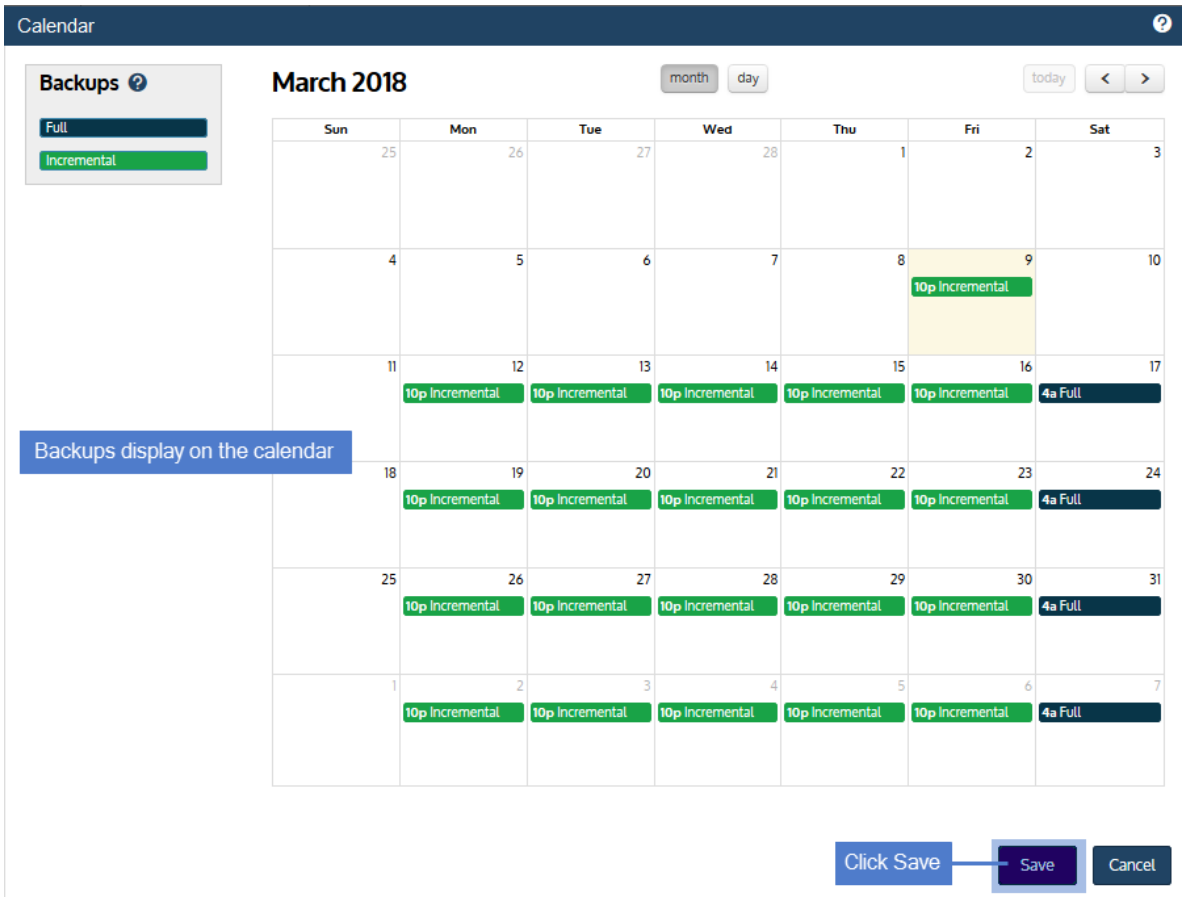
- In the Add Backup dialog, modify settings and click **Save**.



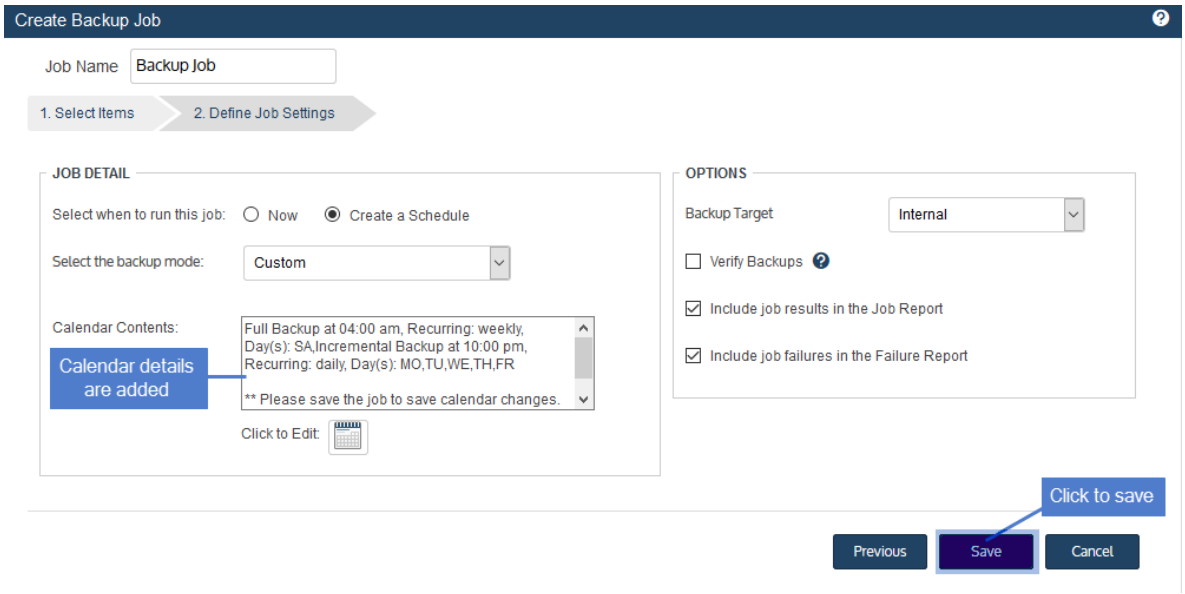
- Repeat these steps to add other modes to the calendar.



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



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



9 Click **Save**.

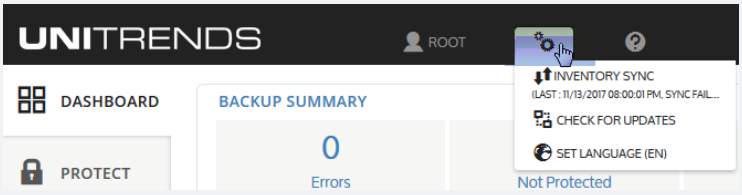
10 Click **OK** to close the Success message.

- 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.

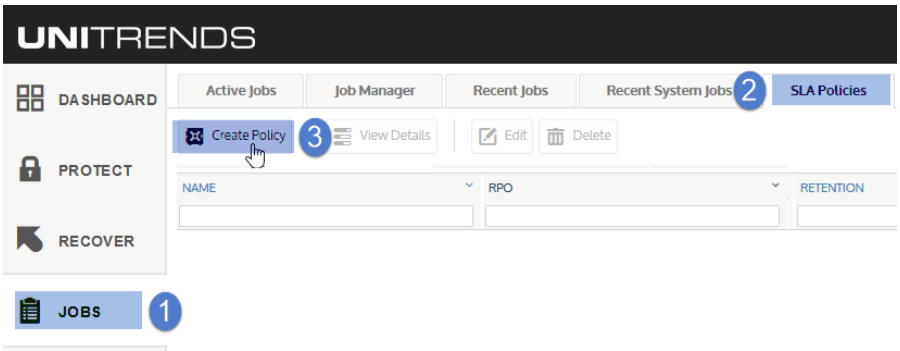
To create an SLA policy for AHV assets

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**.



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.

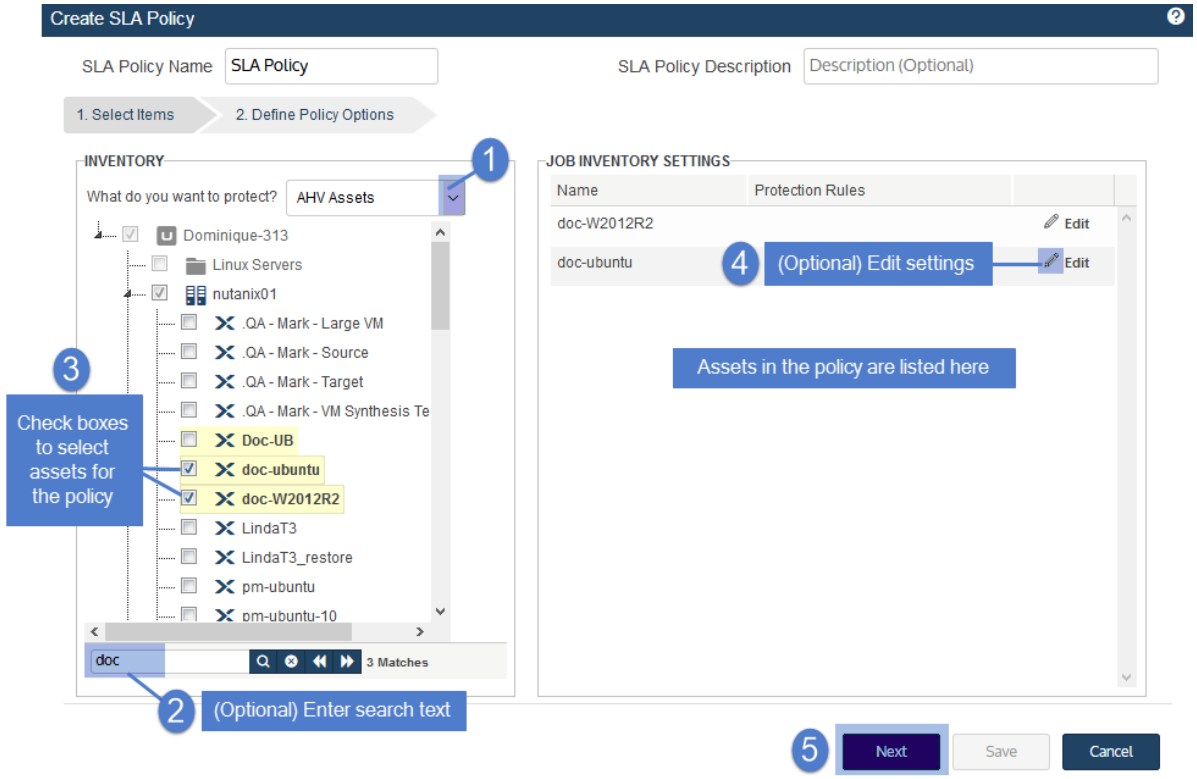
- To locate an asset by name, use the **Search** field below.
- To protect all VMs, select the AHV host.

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**.



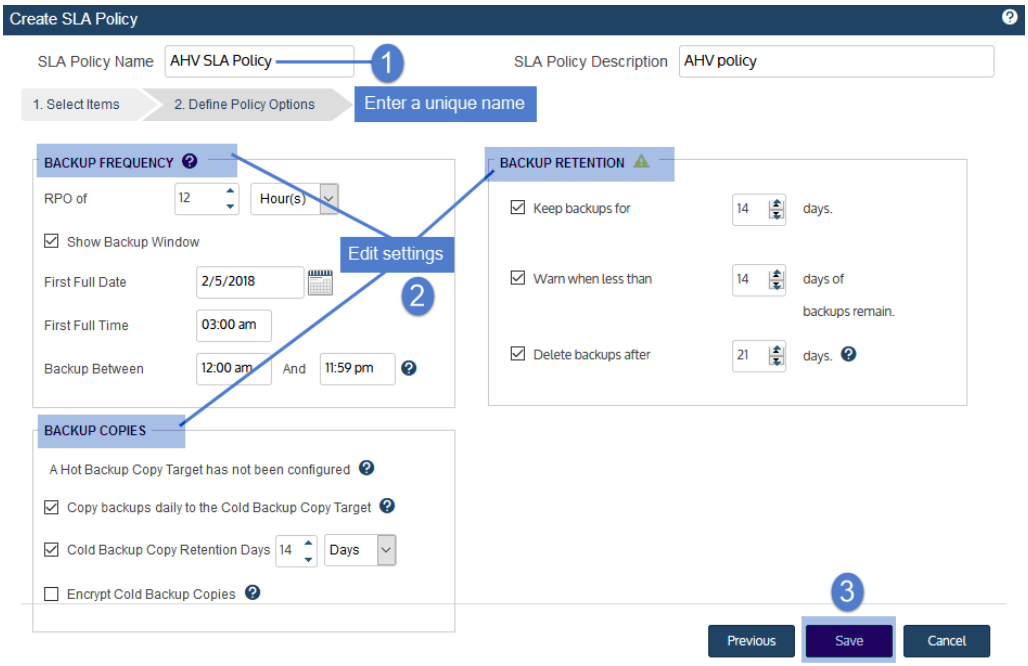
6 Define the remaining Policy Options, then click **Save**.

Policy Options are described in the following table:

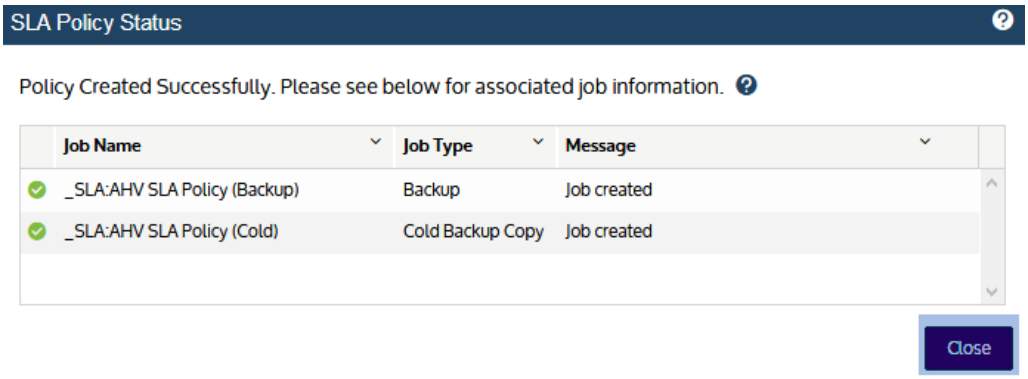
SLA policy setting	Description
SLA Policy Name	Enter a unique name for the policy.
SLA Policy Description	(Optional) Enter a short description of the policy.

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 Creating backup copy jobs. • To add a cold target to the backup appliance, see Backup copy targets.

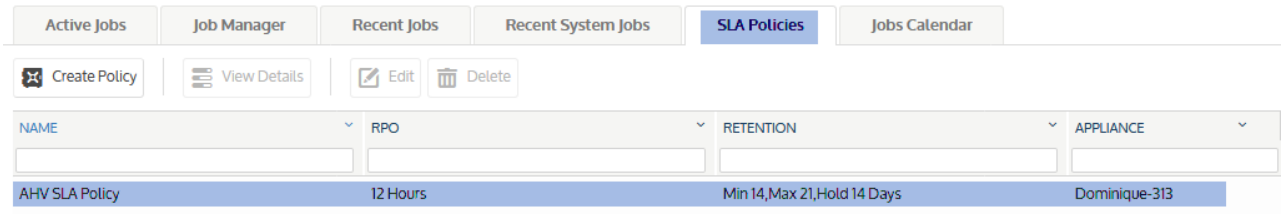
SLA policy setting	Description
Cold Backup Copy Retention Days	Check this box to specify the length of time a copy must be retained before it can be deleted. To define the retention period, enter a number and select Days, Weeks, Months, or Years. For example, enter **2** and select **Weeks** to retain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



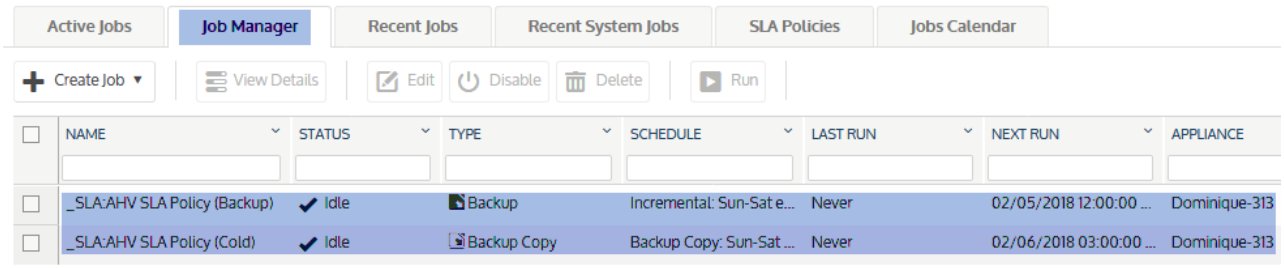
7 The appliance creates the policy and related jobs. Click **Close** to close the status message.



The policy displays on the SLA Policies tab:



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



Next Steps

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.

  - Creating backup copy jobs 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 Managing SLA Policies.)

- 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 Quiesce settings for host-level backups in the Administrator Guide for Recovery Series and Unitrends Backup.

- 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 Administrator Guide for Recovery Series and Unitrends Backup:

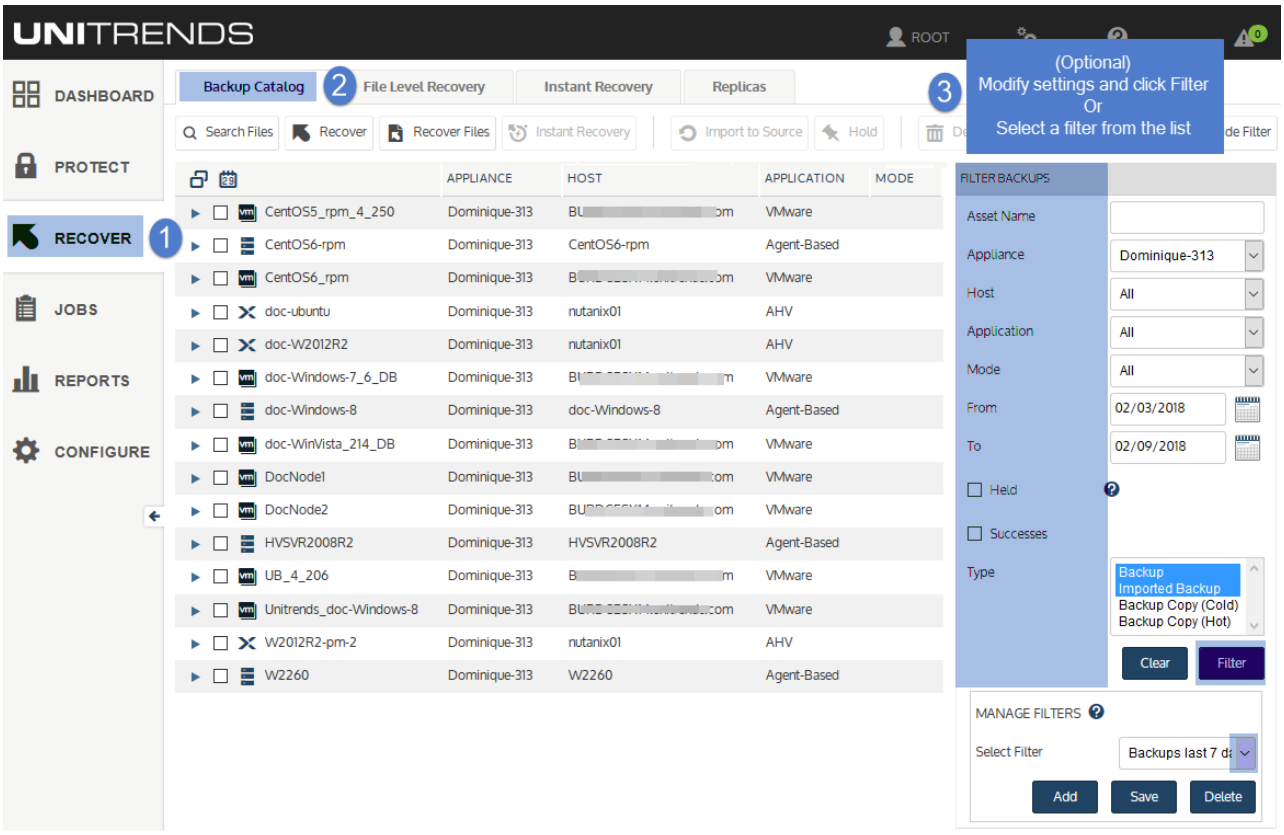
- Recovering Backup Copies
- Recovering Host-level Backups

Recovering an AHV VM

Use this procedure to recover an entire AHV virtual machine.

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

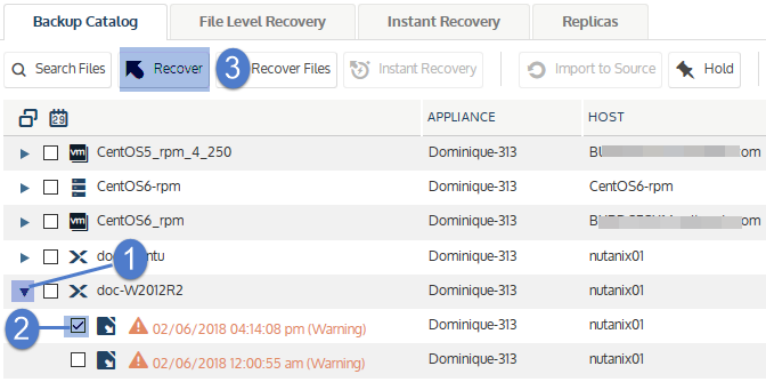
(Optional) Use Filter Backups to the right to customize the backups that display. (For details, see "Working with Custom Filters in the Backup Catalog" on page 71.)



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 To import a cold backup copy or To import a hot backup copy in the Administrator Guide for Recovery Series and Unitrends Backup.

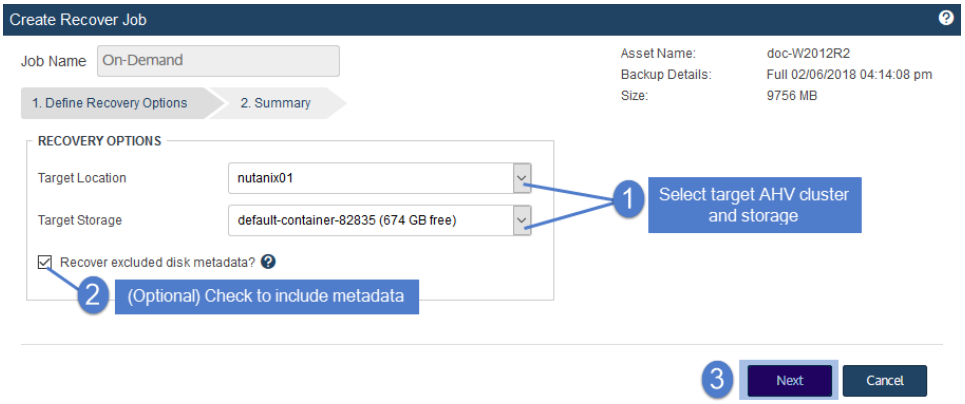
3 Click **Recover**.



4 Select these Recovery Options:

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.

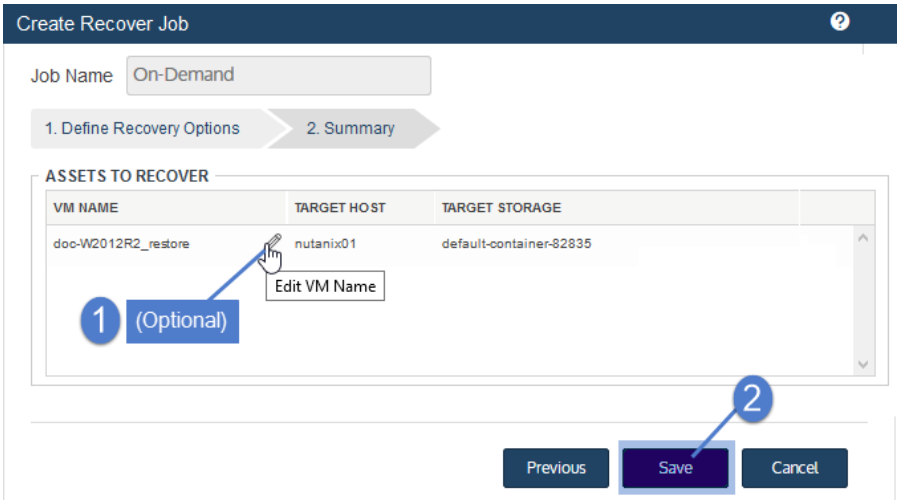
5 Click **Next**.



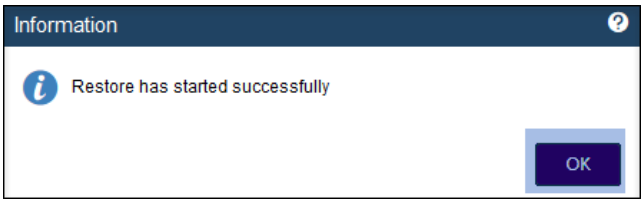
A summary of the selected recovery options display.

6 (Optional) Modify the VM Name by clicking it in the Assets to Recover list and entering a new name.

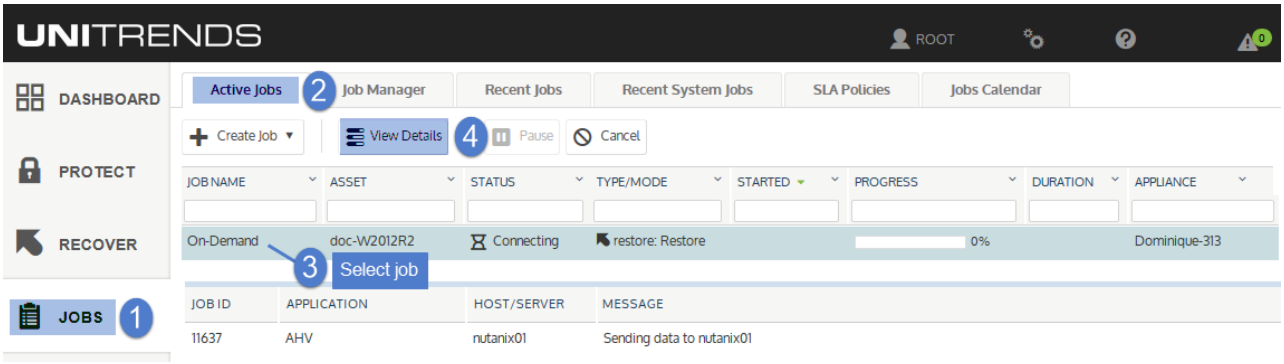
7 Click **Save**. The job is queued immediately.



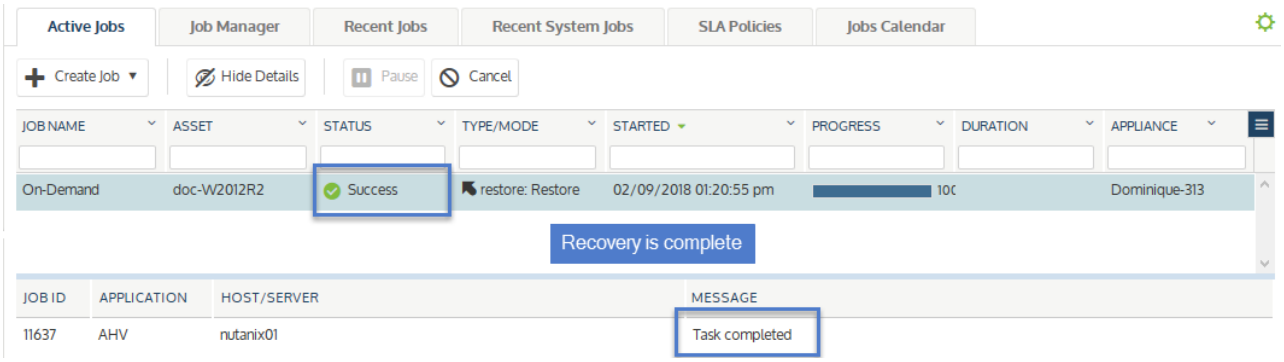
8 Click **OK** to close the Information message.



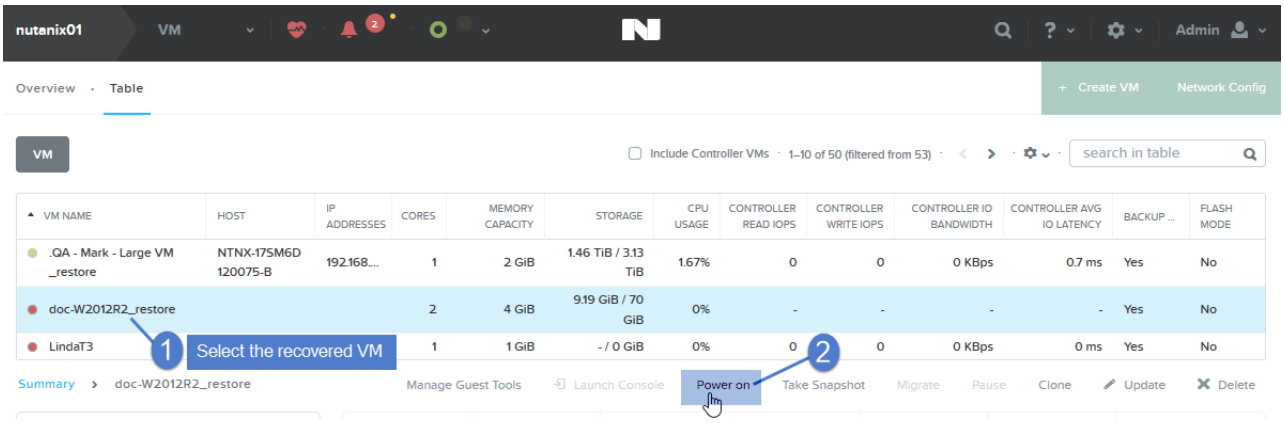
9 To view job progress, select **Jobs > Active Jobs**. Select the job and click **View Details**.



Recovery is complete when the job status changes to Success:



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



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 *Ctl+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 *.zip* 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 an iSCSI LUN	You must recover by mounting the iSCSI LUN to perform the following tasks: • 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 *.zip* 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

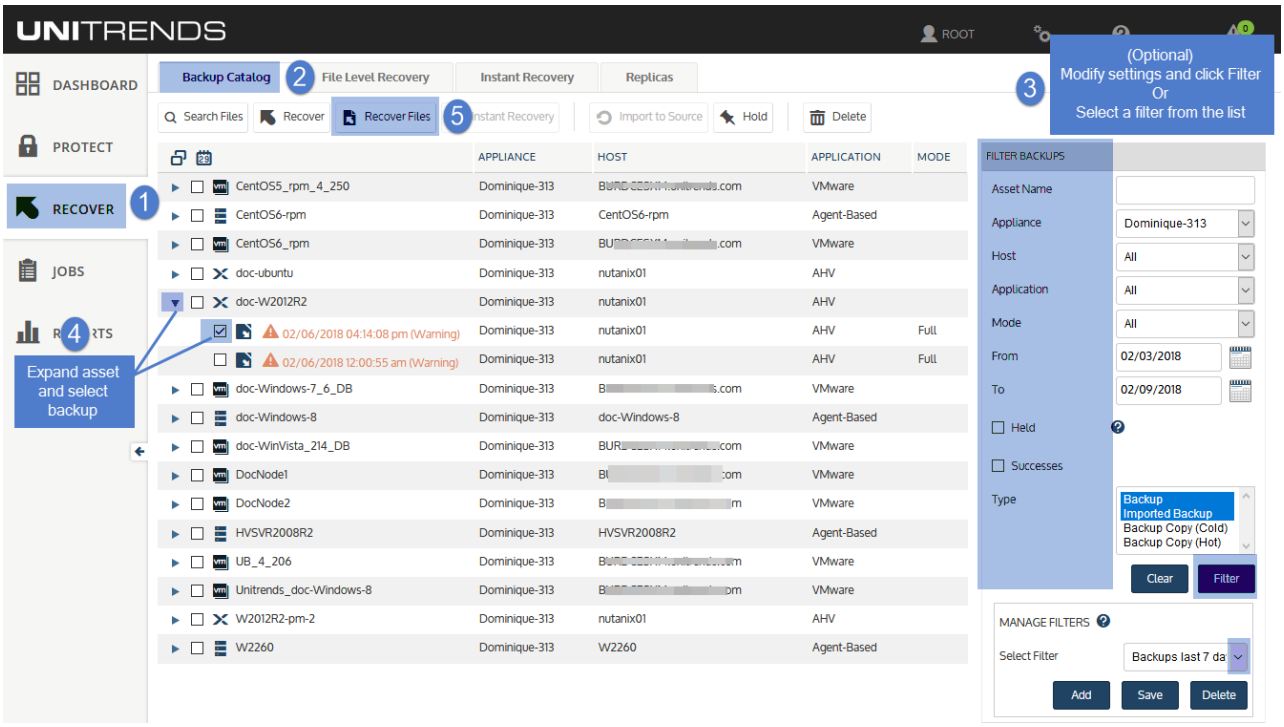
Step 1: Create the recovery object

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.

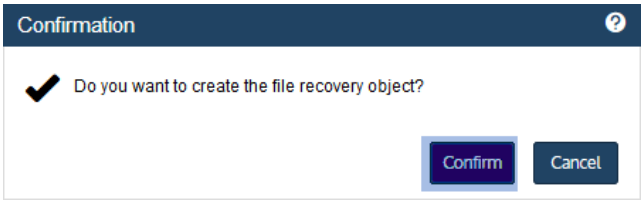
   (Optional) Use Filter Backups to the right to customize the backups that display. (For details, see "Working with Custom Filters in the Backup Catalog" on page 71.)
3. Expand the VM asset and select the backup or imported backup copy from which you want to recover files.

   (To import a backup copy, see To import a cold backup copy or To import a hot backup copy in the Administrator Guide for Recovery Series and Unitrends Backup.)
4. Click **Recover Files**.

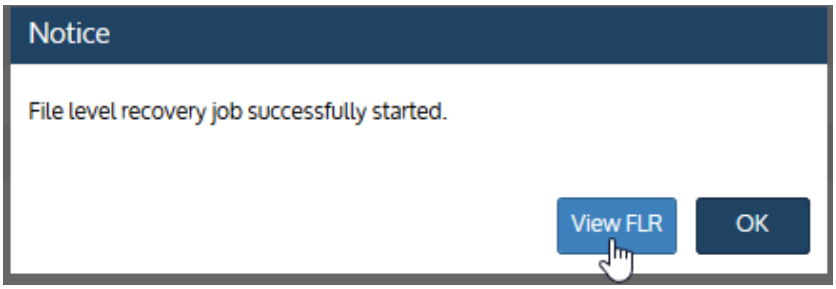


5 Click **Confirm** to continue. The appliance creates the recovery object.

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.

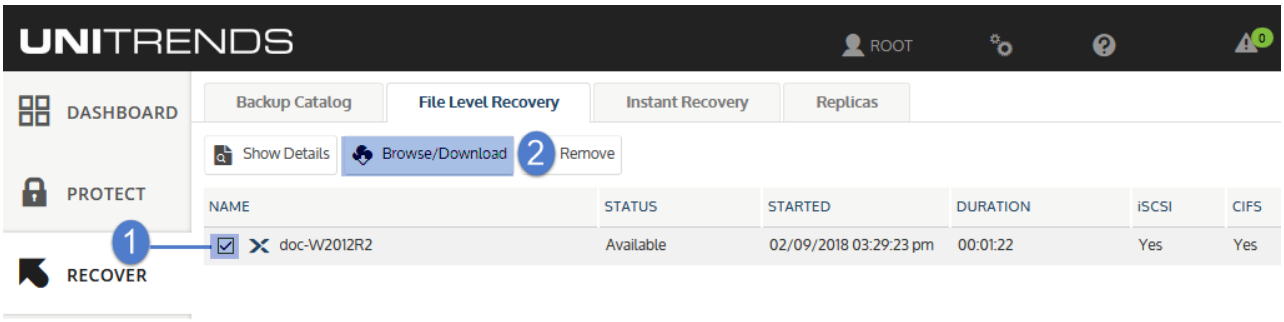
- "To recover files by browsing and downloading to a .zip file"
- "To recover files by mounting the CIFS share" on page 45
- "To recover files by mounting the iSCSI LUN" on page 47

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.

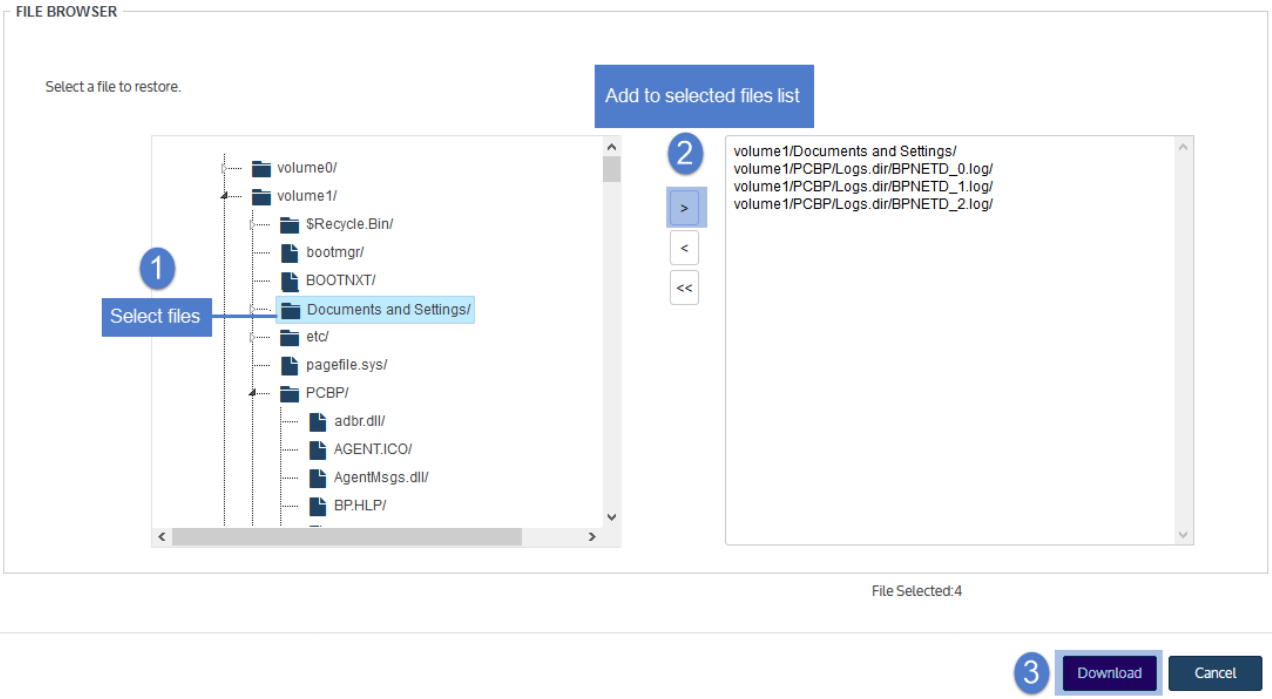
2 Select the recovery object and click **Browse/Download**.



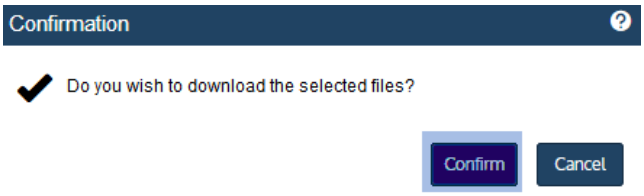
3 In the File Browser, select or drag files and/or directories to recover.

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**.



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

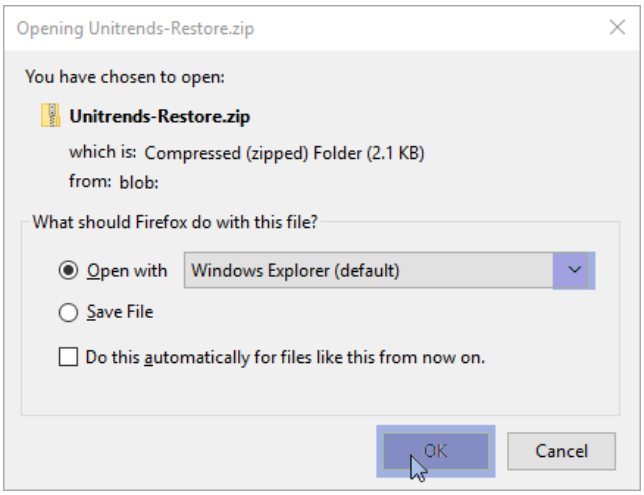


Notes:

- 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,

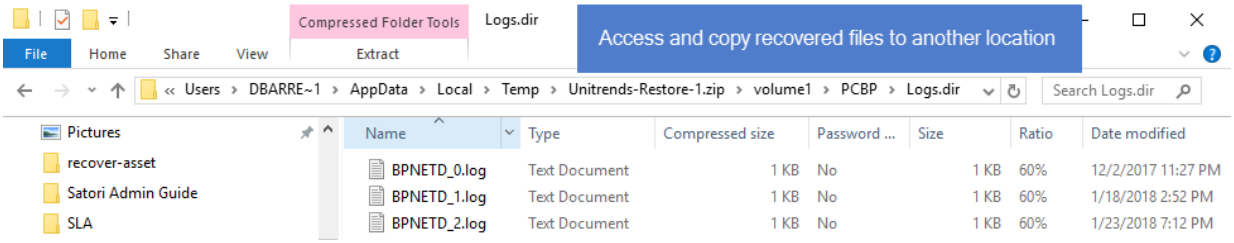
you see files in this directory, but the download is not complete until the *.zip* file has been created. (Recoveries are automatically removed from the */downloads* directory after 72 hours.)

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



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.



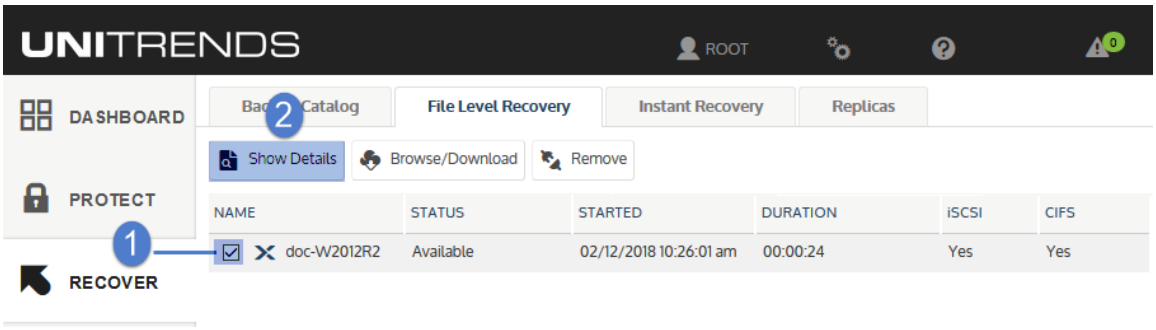
Proceed to "Step 3: Remove the recovery object from the appliance" on page 51.

To recover files by mounting the CIFS share

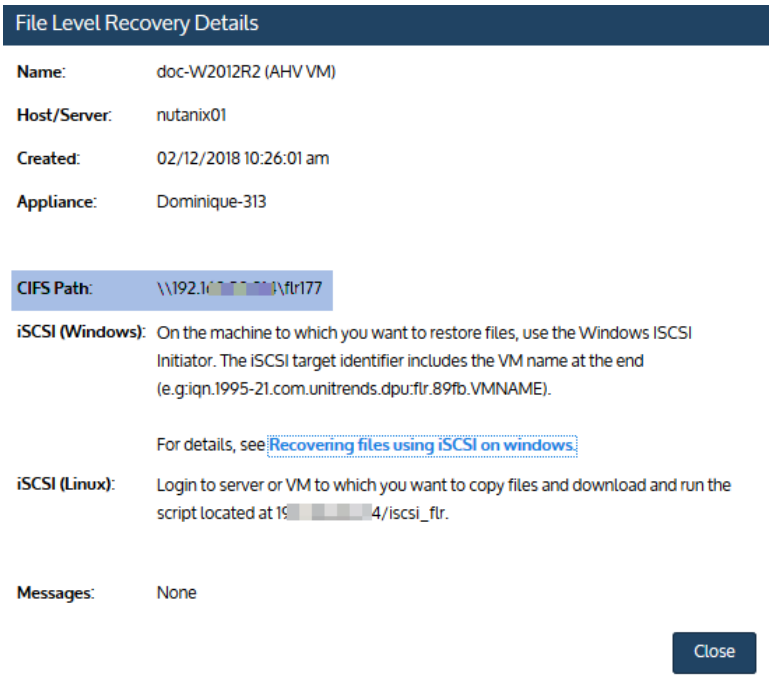
1 Select **Recover** and click the **File Level Recovery** tab.

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**.



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.



4 Log in to the recovery target workstation.

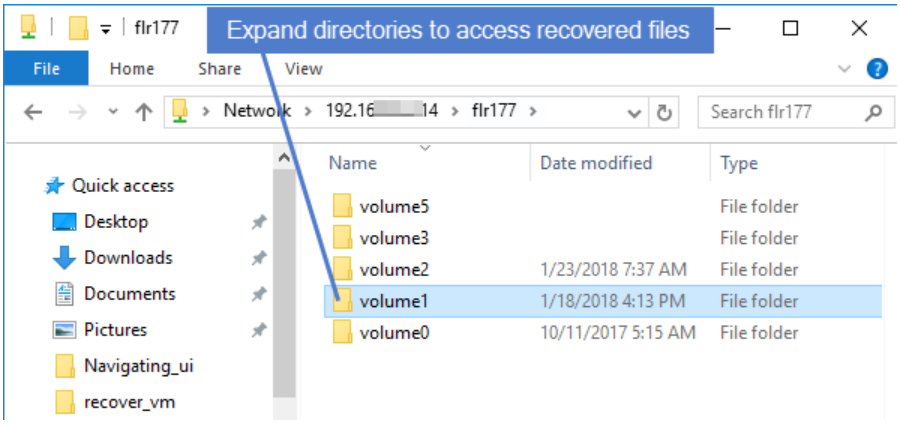
5 Enter the CIFS path into a file browser on the recovery target.

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.



7 Move selected files to another location on the local machine.

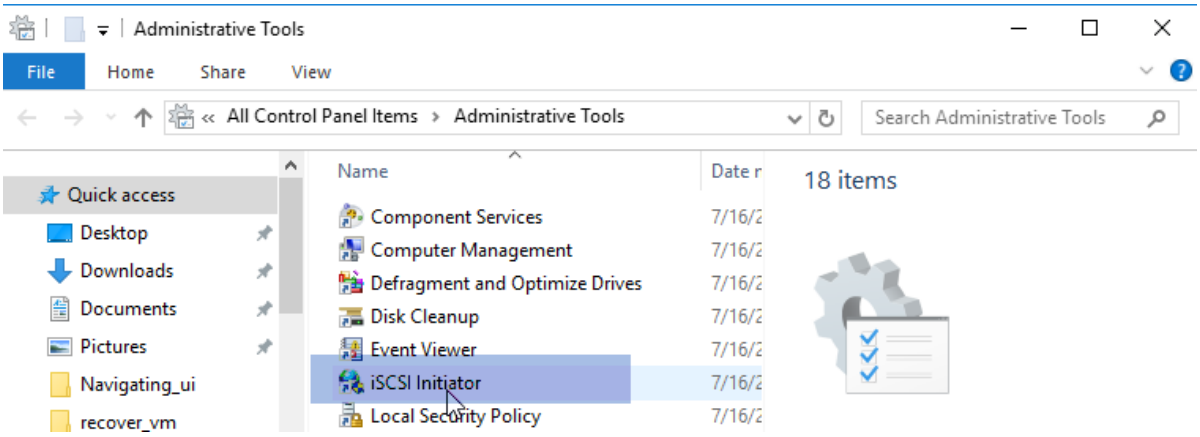
8 Disconnect the network share by right-clicking the share and selecting **Disconnect**.

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

To recover files by mounting the iSCSI LUN

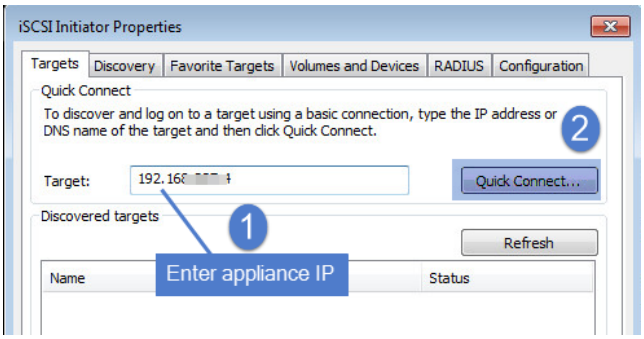
1 Log in to the recovery target.

2 Launch the iSCSI Initiator from **Administrative Tools** in the **Control Panel**.



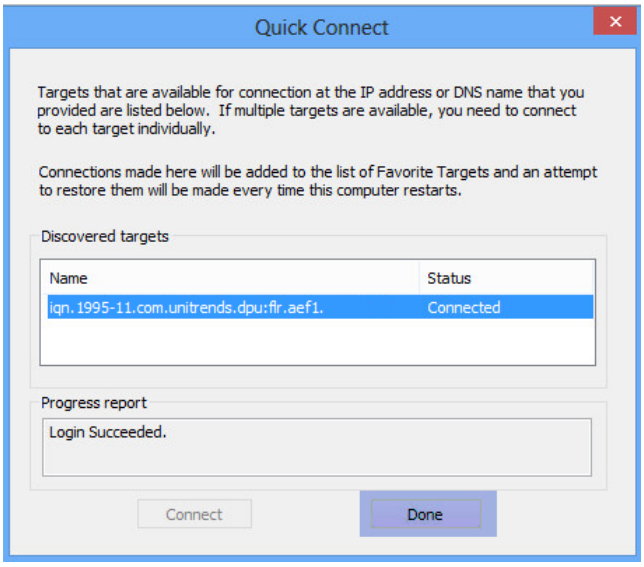
3 In the **Target** field, enter the appliance IP address and click **Quick Connect...**.

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



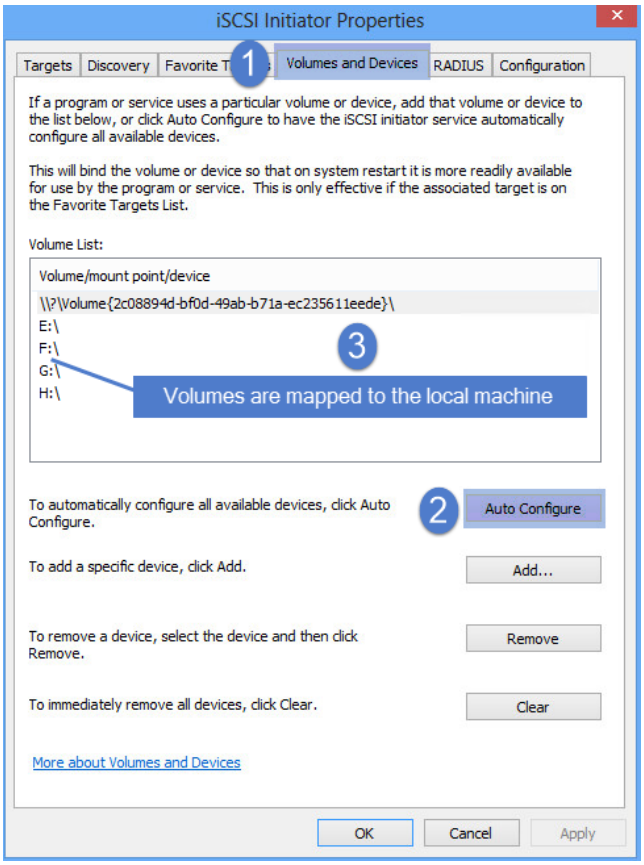
4 Select the iSCSI target from the list.

5 The iSCSI target is discovered and connected to the local machine. Click **Done**.



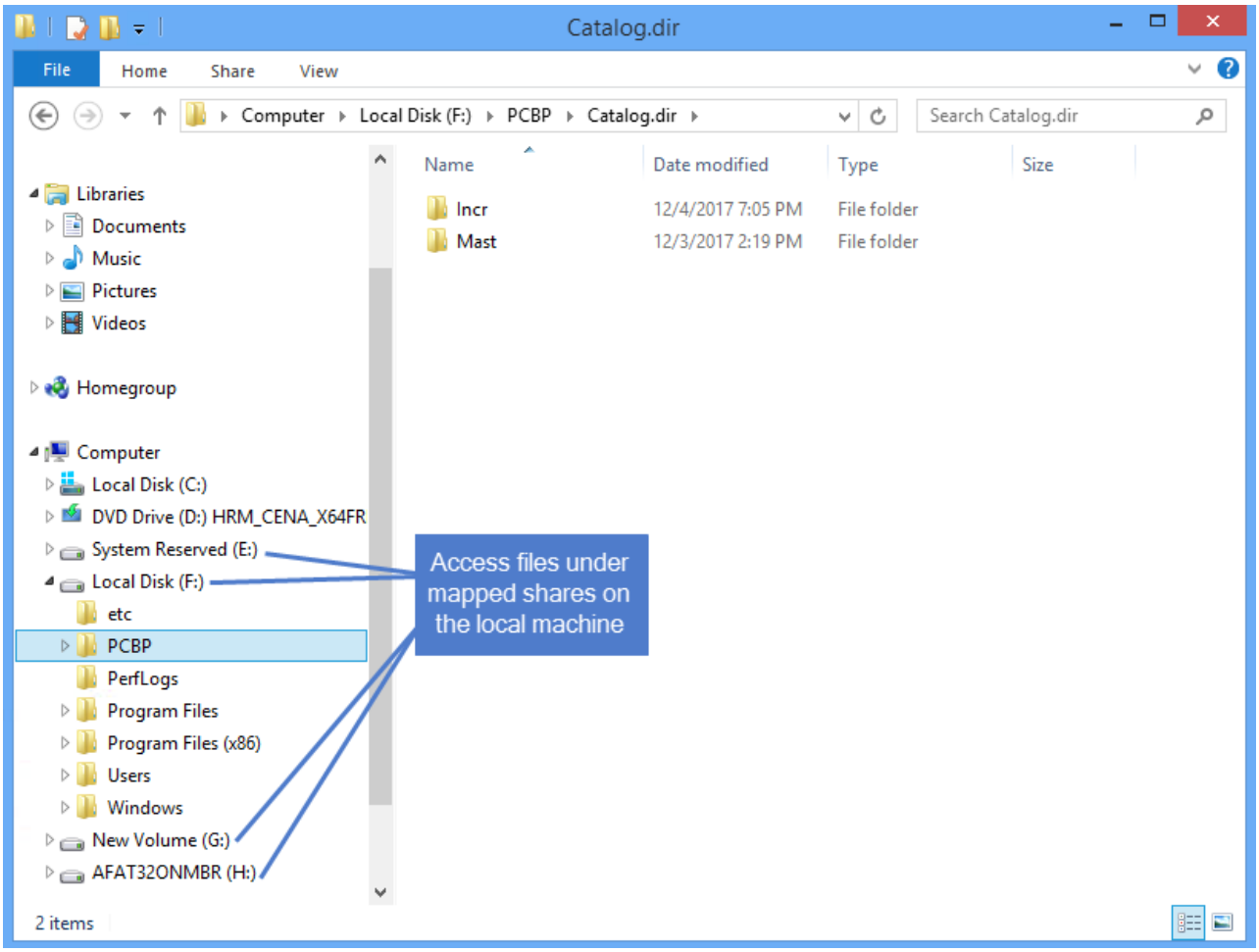
6 On the Volumes and Devices tab, click **Auto Configure** to map drives from the iSCSI target to the local machine (or map them manually if you prefer).

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

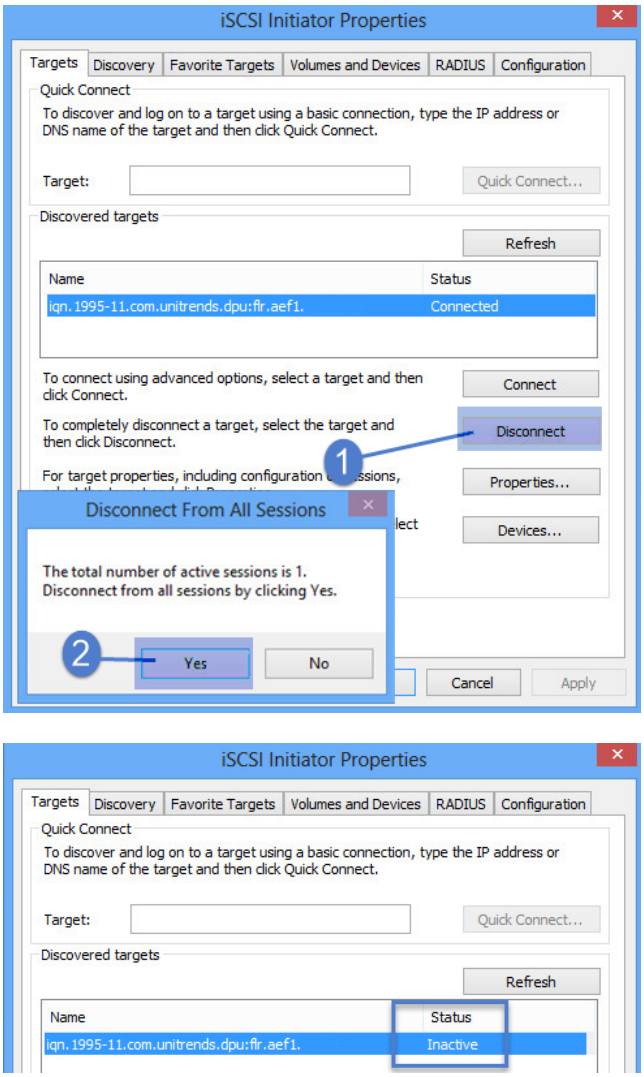


7 Access the files under the mapped drives and move them to another location on the local machine.

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



8 Use the iSCSI Initiator to disconnect from the LUN.



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.

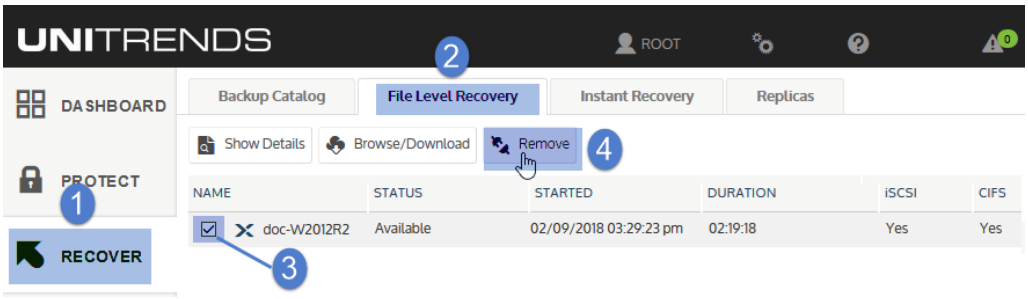
WARNING! If you mounted the CIFS share or iSCSI LUN, be sure to unmount it from the target before you remove the recovery object. Removing the recovery object while the target is still connected causes undesired results and errors on the target machine.

To remove a file-level recovery object

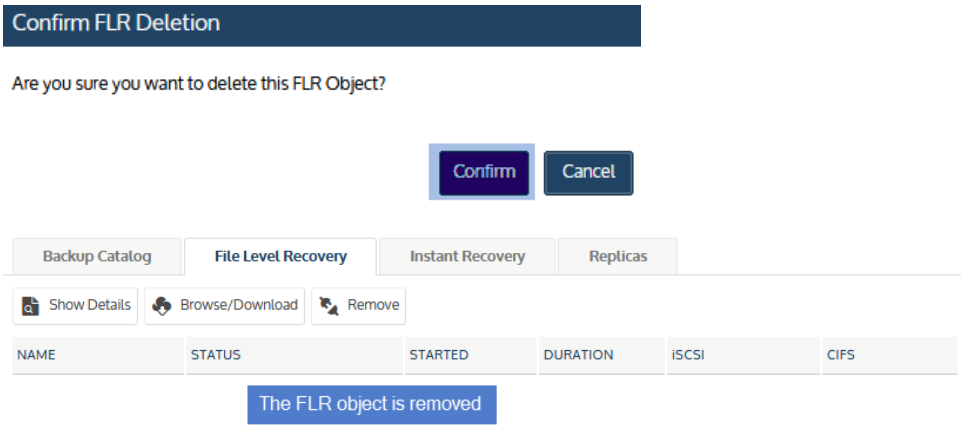
1 Select **Recover** and click the **File Level Recovery** tab.

2 Select the recovery object.

3 Click **Remove**.



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



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:

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 *.zip* 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 protected Linux VM	These requirements apply to the original Linux VM whose backup or backup copy will be used for the recovery: • 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 *.zip* 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 mounting the iSCSI LUN	To recover by mounting the iSCSI LUN, the following prerequisites and considerations apply: • 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

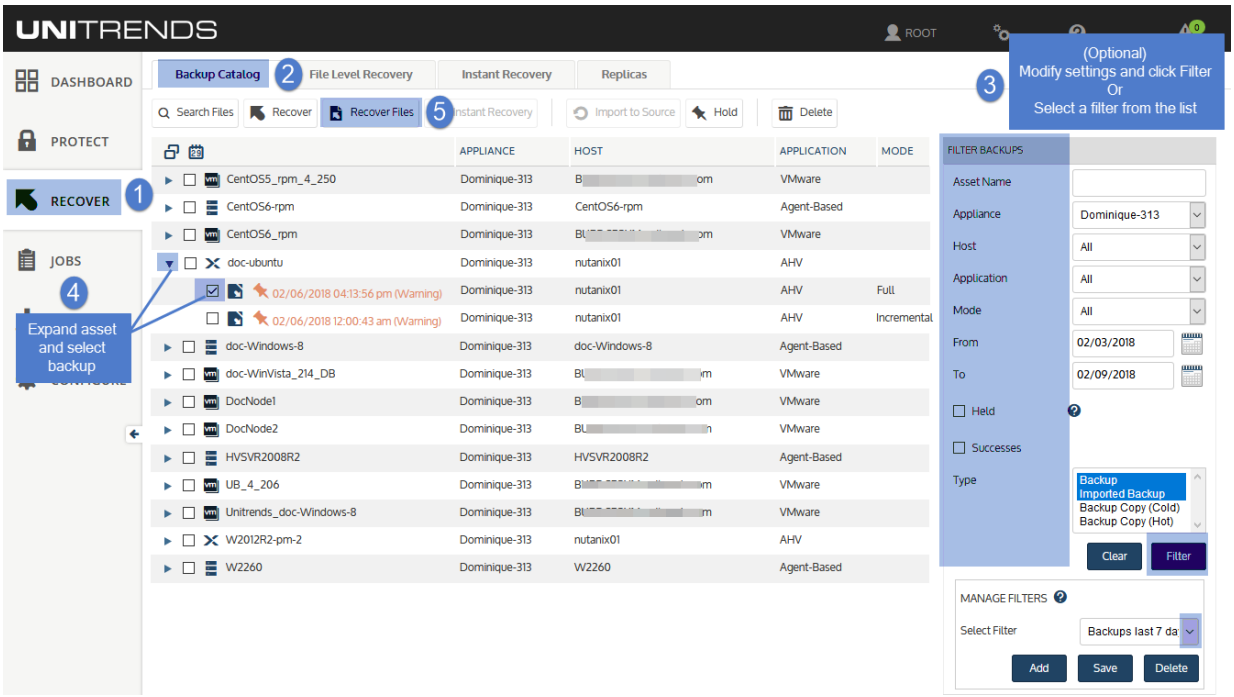
Step 1: Create the recovery object

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.

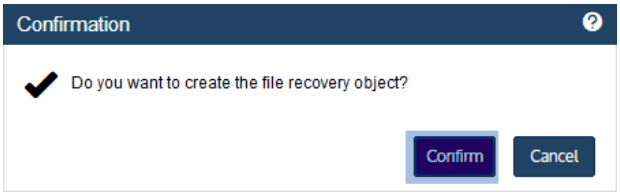
   (Optional) Use Filter Backups to the right to customize the backups that display. (For details, see "Working with Custom Filters in the Backup Catalog" on page 71.)
3. Expand the VM asset and select the backup or imported backup copy from which you want to recover files.

   (To import a backup copy, see To import a cold backup copy or To import a hot backup copy in the Administrator Guide for Recovery Series and Unitrends Backup.)
4. Click **Recover Files**.

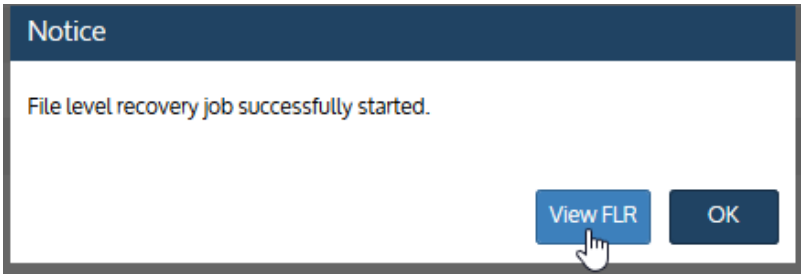


5 Click **Confirm** to continue. The appliance creates the recovery object.

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

Use one of the following procedures to recover files.

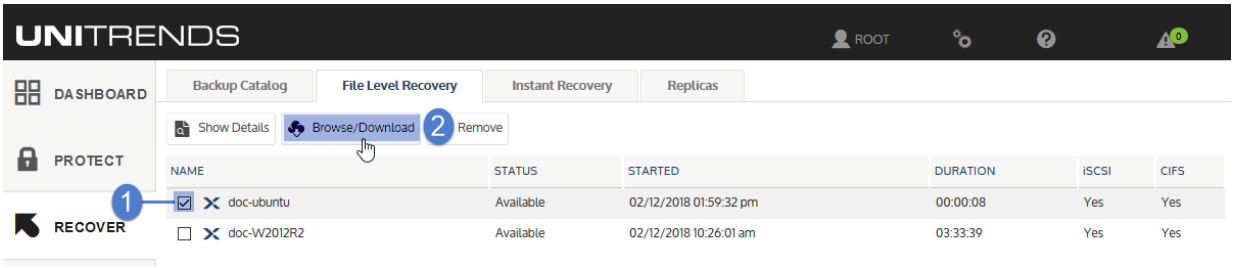
- "To recover files by browsing and downloading to a .zip file"
- "To recover files by mounting the CIFS share" on page 58
- "To recover files to a Linux machine by mounting the iSCSI LUN" on page 60

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.

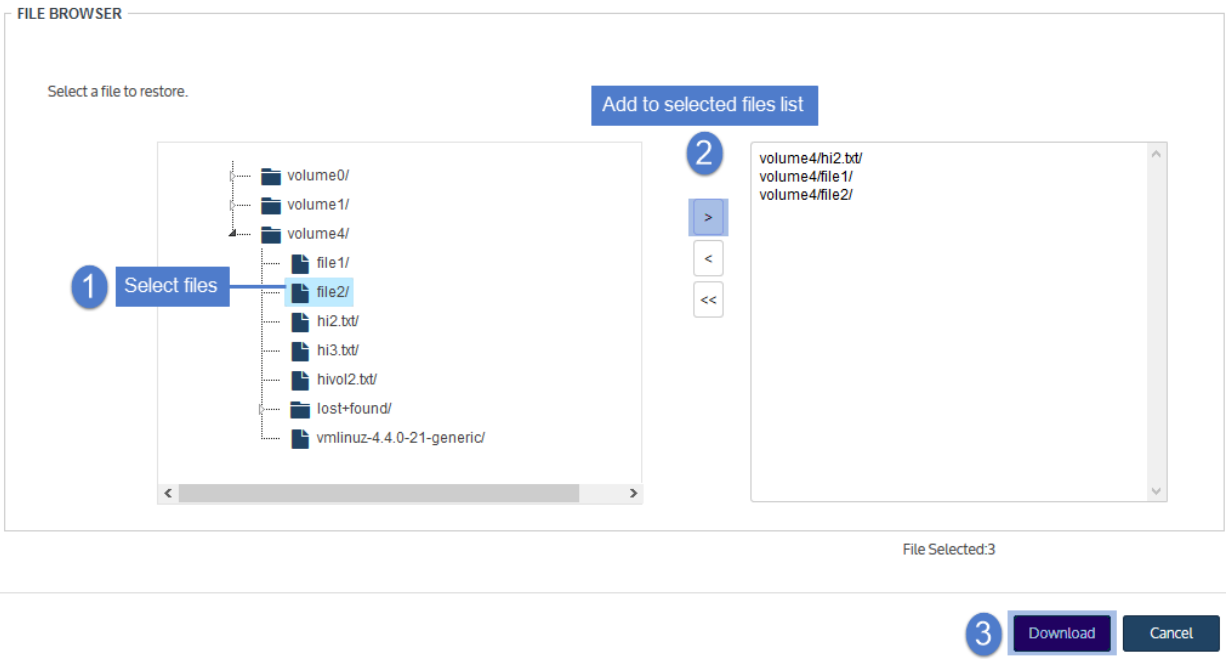
2 Select the recovery object and click **Browse/Download**.



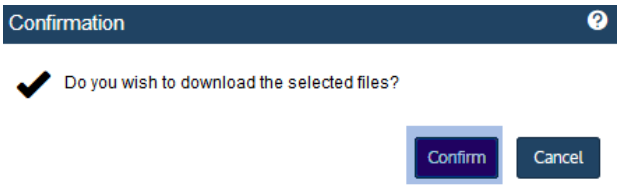
3 In the File Browser, select or drag files and/or directories to recover.

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**.



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

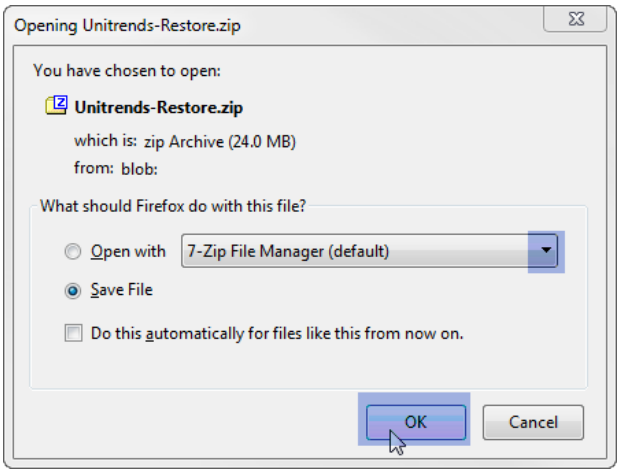


Notes:

- 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

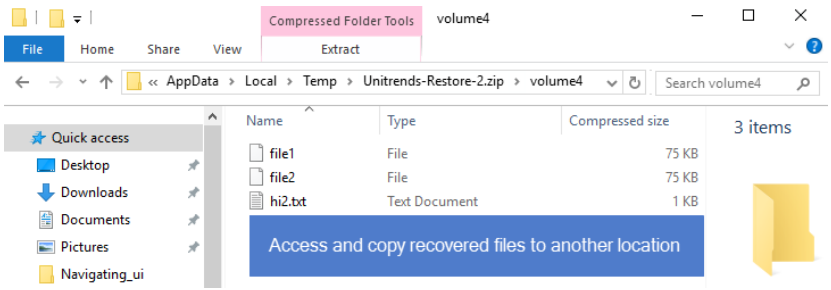
the *.zip* file has been created. (Recoveries are automatically removed from the */downloads* directory after 72 hours.)

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



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.



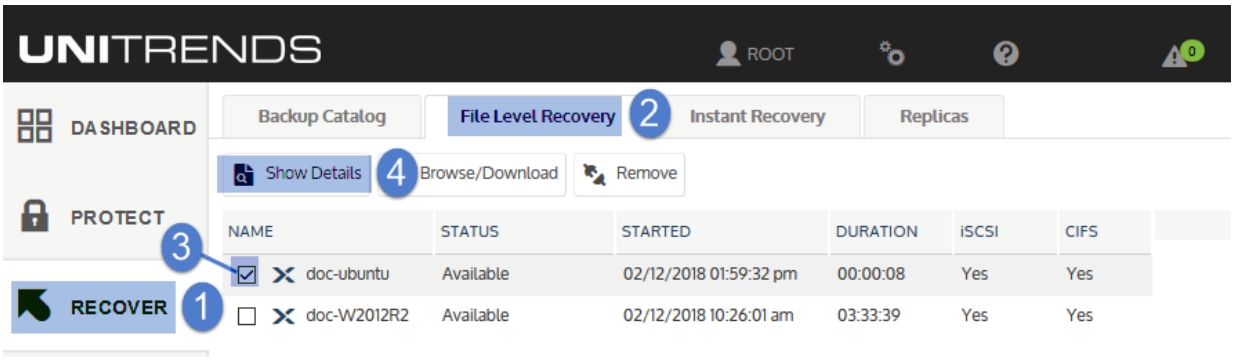
Proceed to "Step 3: Remove the recovery object from the appliance" on page 62.

To recover files by mounting the CIFS share

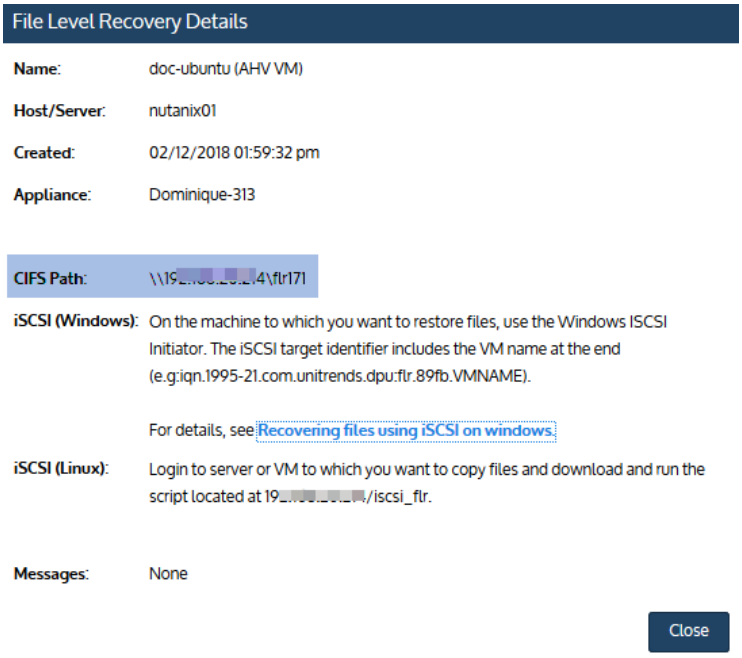
1 Select **Recover** and click the **File Level Recovery** tab.

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**.

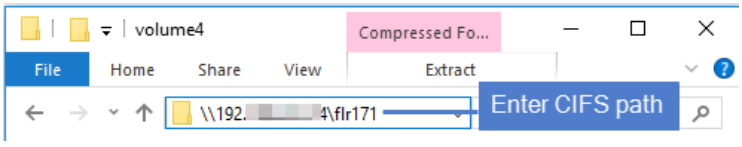


3 Note the CIFS path that displays in the File Level Recovery Details window. You will need this path to mount the CIFS share on the target machine.



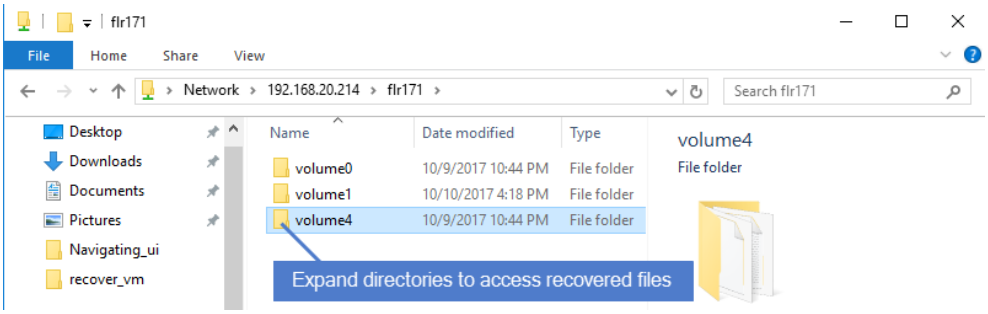
4 Log in to the recovery target workstation.

5 Enter the CIFS path into a file browser on the recovery target.



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.



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.

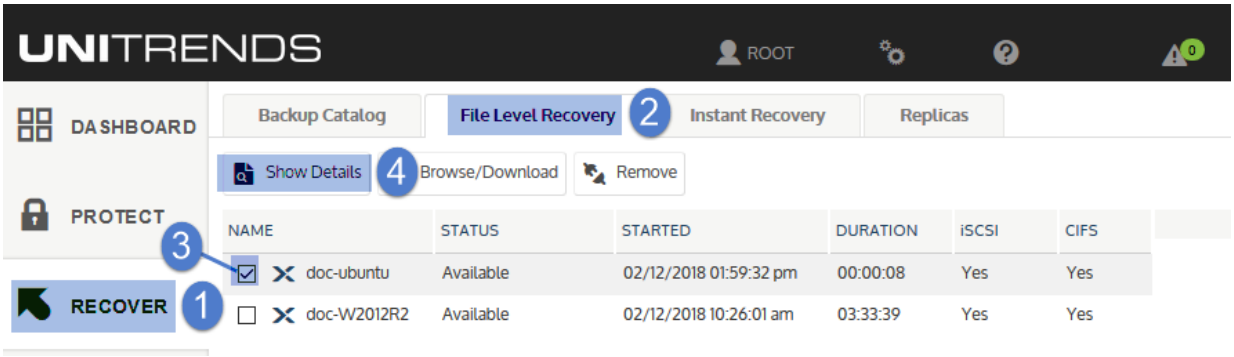
To recover files to a Linux machine by mounting the iSCSI LUN

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

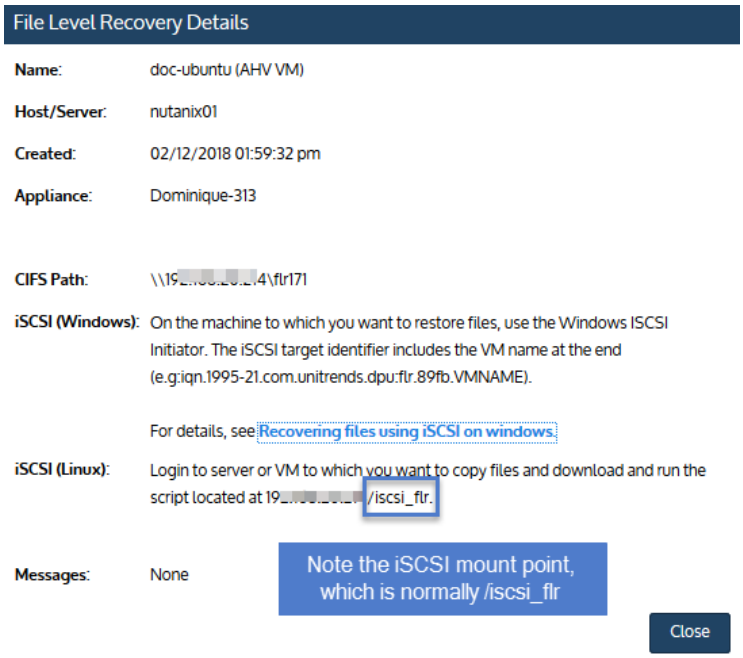
1 In the appliance UI, select **Recover** and click the **File Level Recovery** tab.

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**.



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.



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 *iscsi_flr* script from the backup appliance:

```
# wget http://<appliance IP>/iscsi_flr
```

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
```

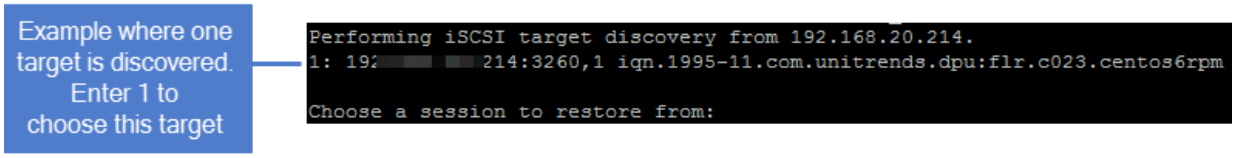
9 Enter the appliance IP address:

```
# Enter address of the Unitrends backup system: <appliance IP>
```

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:




```
# Choose a session to restore from: <SessionNumber>
```

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

```
#  cd /iscsi_flr
```

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.

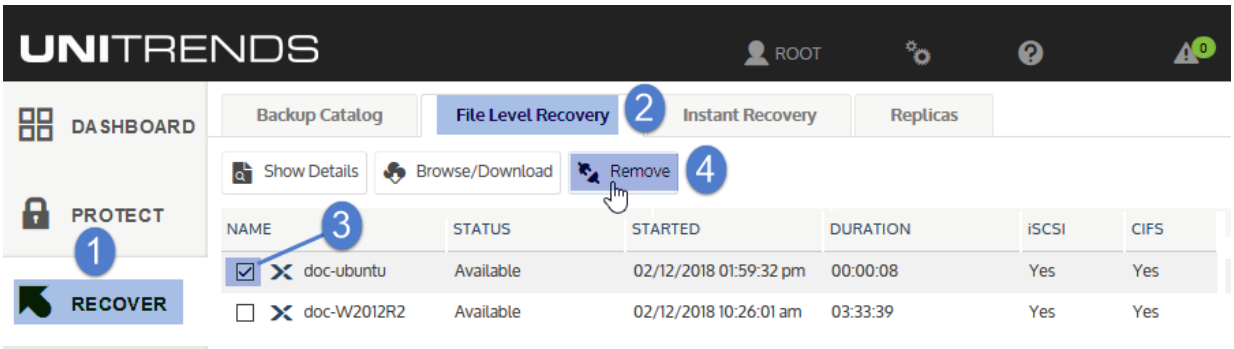
WARNING! If you recovered by mounting a LUN, be sure to unmount the LUN from the target before you remove the recovery object. Removing the recovery object while the target is still connected causes undesired results and errors on the target machine.

To remove a file-level recovery object

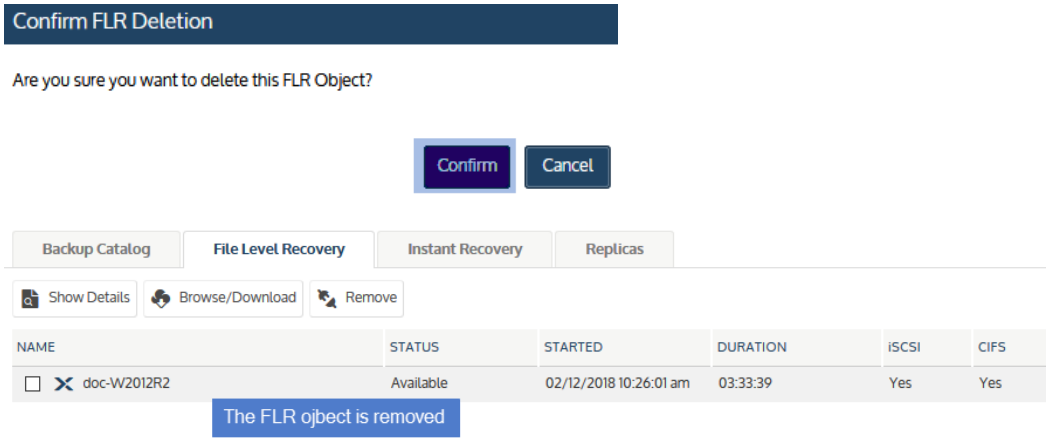
1 Select **Recover** and click the **File Level Recovery** tab.

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.



This page is intentionally left blank.

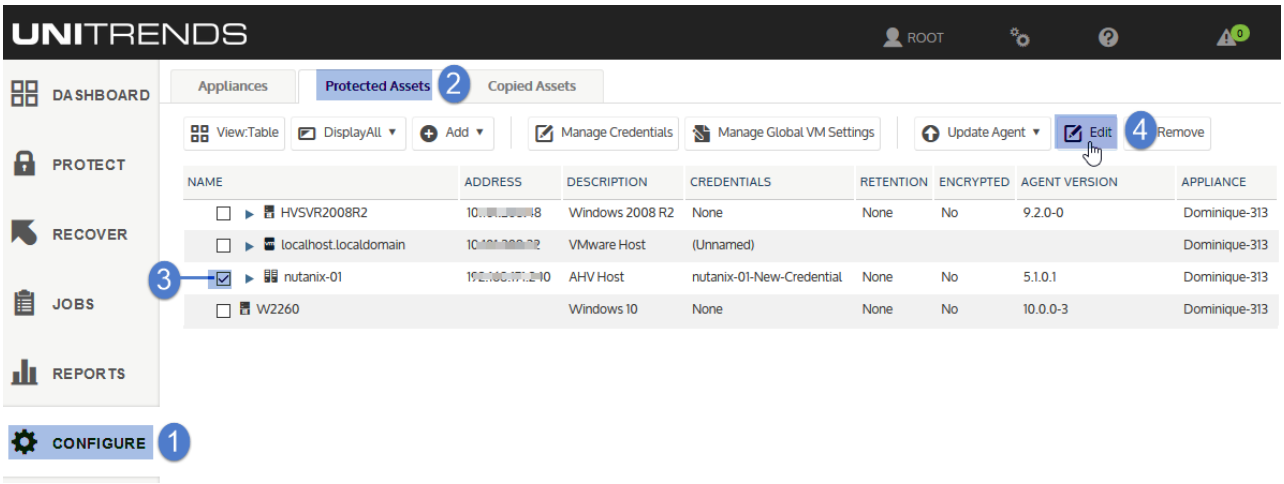
Chapter 4: Managing AHV Hosts and Virtual Machines

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:

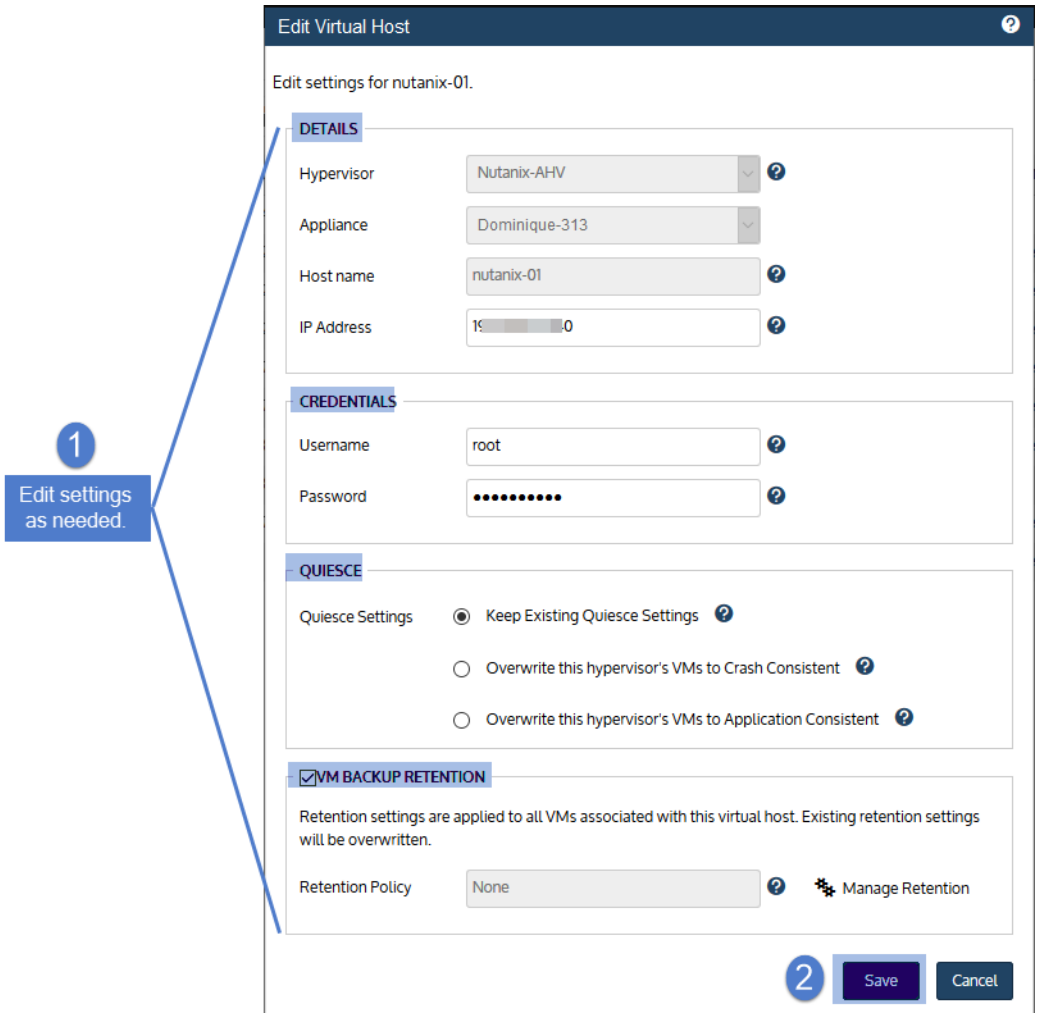
To edit a virtual host asset

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 Backup Administration and Procedures in the Administrator Guide for Recovery Series and Unitrends Backup.

1. Select **Configure > Protected Assets**.
2. Select the AHV host asset.
3. Click **Edit**.



4. Modify settings and click **Save**.



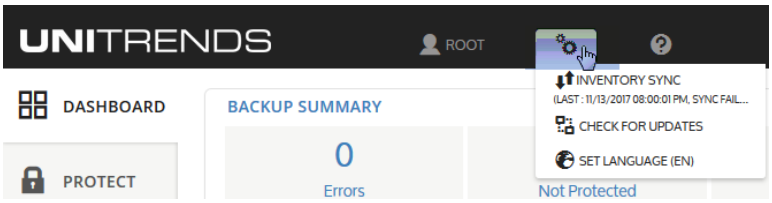
For details on these settings, see the following topics in the Administrator Guide for Recovery Series and Unitrends Backup:

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

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**.



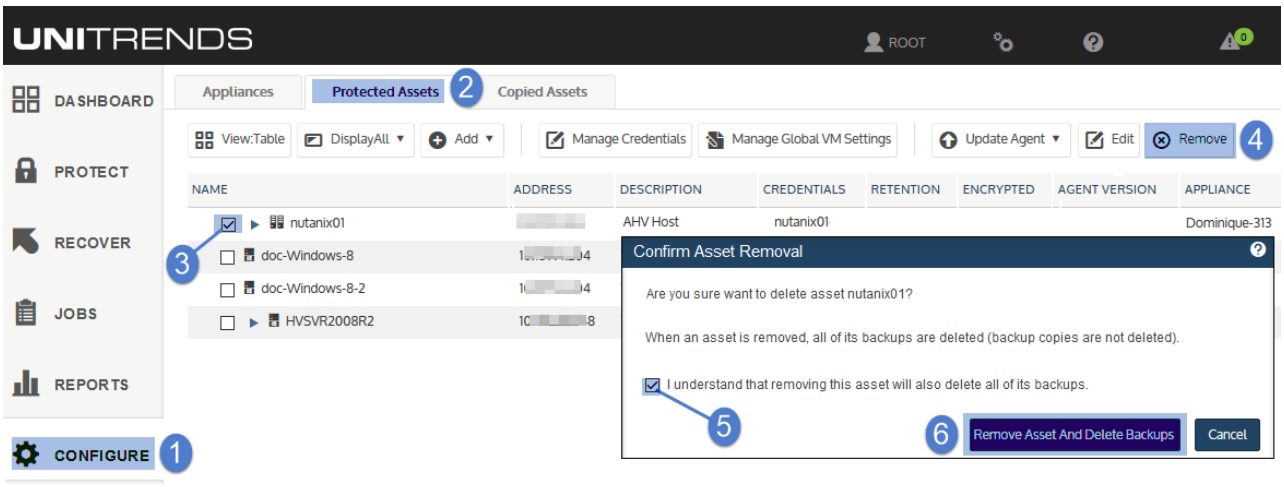
Removing a virtual host asset

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.

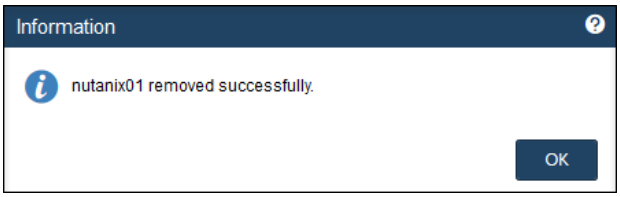
To remove a virtual host asset

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**.



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

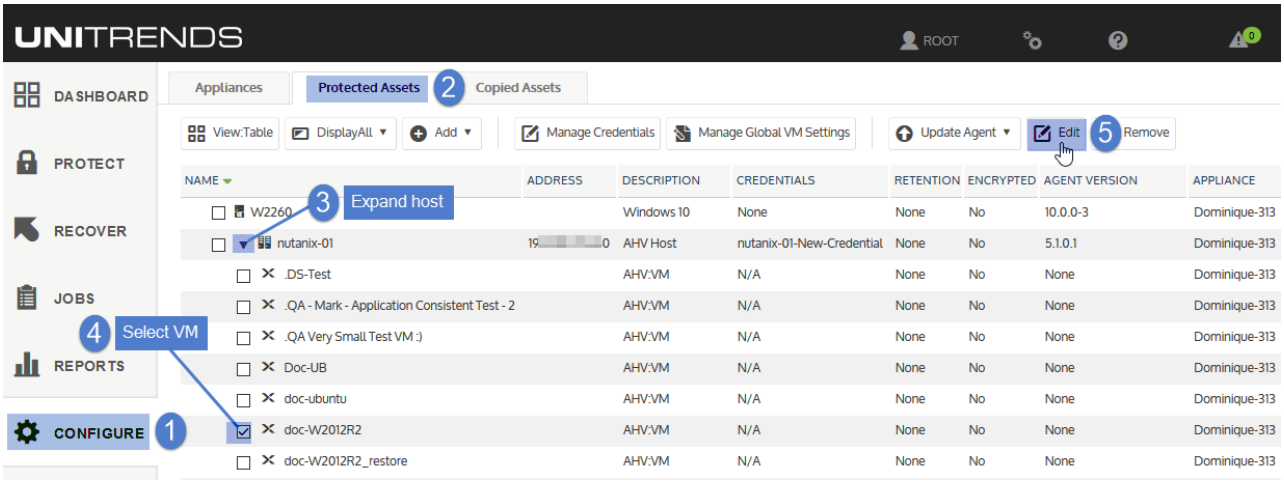
Note: If you are no longer protecting hosted VMs with this Unitrends appliance, contact Support for assistance removing any unneeded snapshots.



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 Backup Administration and Procedures in the Administrator Guide for Recovery Series and Unitrends Backup.

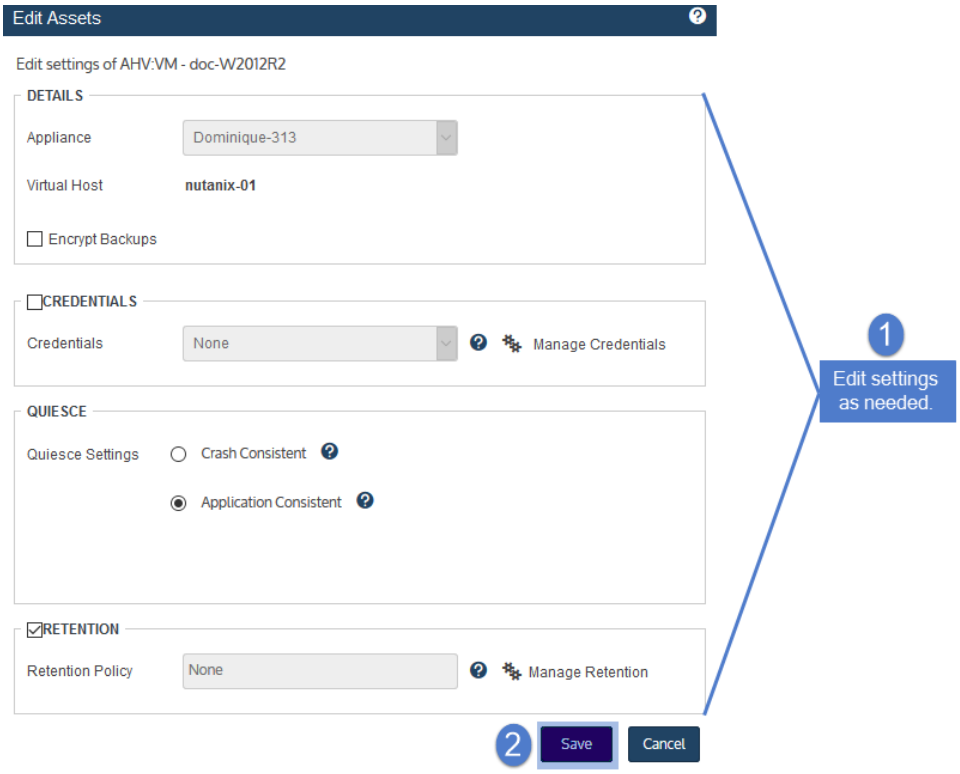
1. Select **Configure > Protected Assets**.
2. Click to expand the VM's virtual host to display its VMs.
3. Select the VM and click **Edit**.



4. Modify settings and click **Save**.

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

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

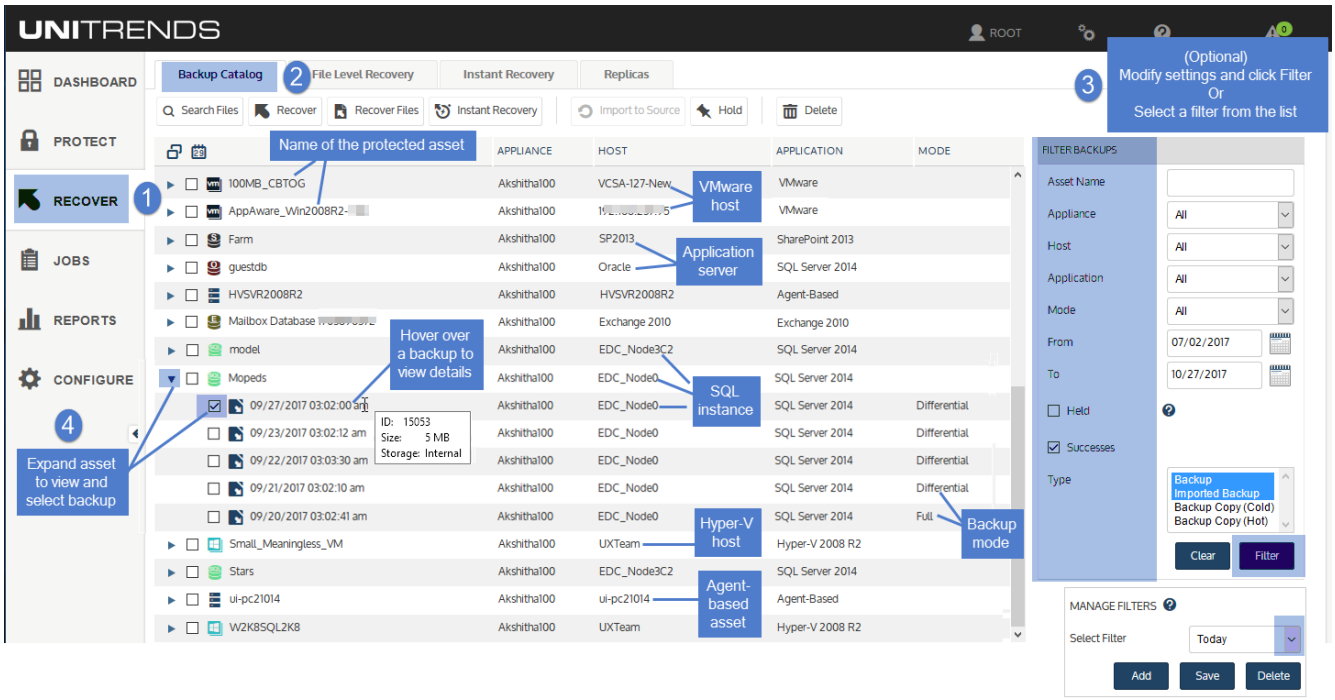

Edit Assets
Edit settings of AHV:VM - doc-W2012R2
DETAILS
Appliance
Dominique-313
Virtual Host
nutanix-01
Encrypt Backups
CREDENTIALS
Credentials
None
Manage Credentials
QUIESCE
Quiesce Settings
Crash Consistent
Application Consistent
RETENTION
Retention Policy
None
Manage Retention
1
Edit settings as needed.
2
Save
Cancel

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.



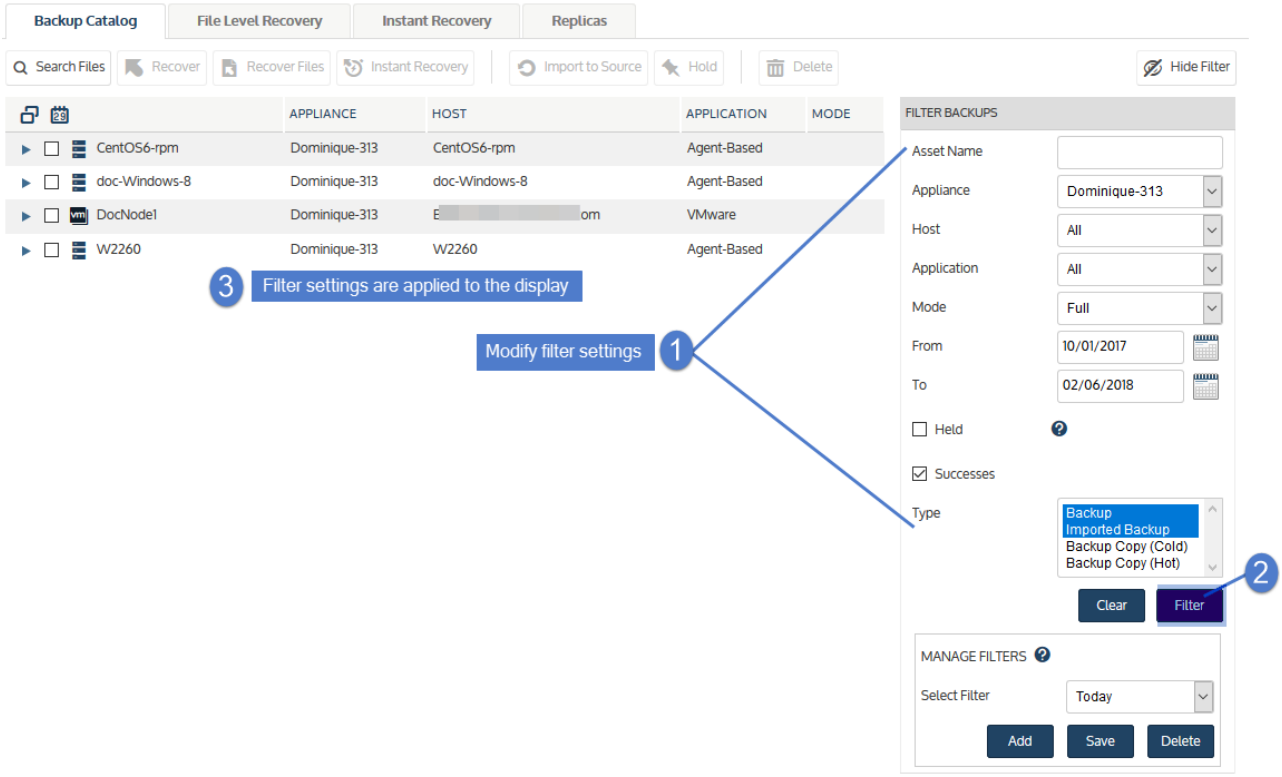
To change the backups and copies that display, you can modify settings manually or apply a custom filter. See these topics for details:

- "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

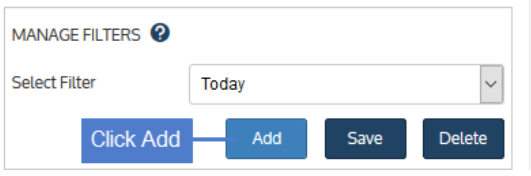
1 Modify the values in the Filter Backups fields.

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



To add a filter

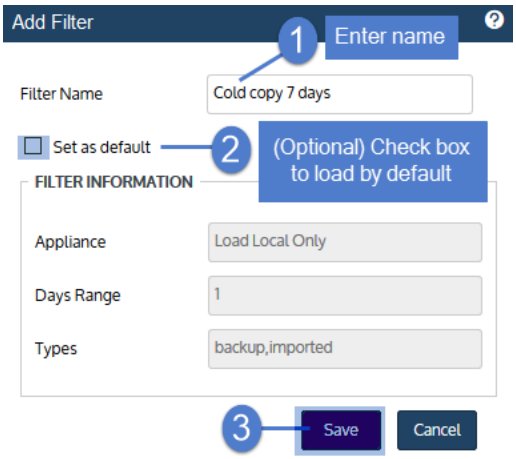
1 In the Manage Filters area, click **Add**.



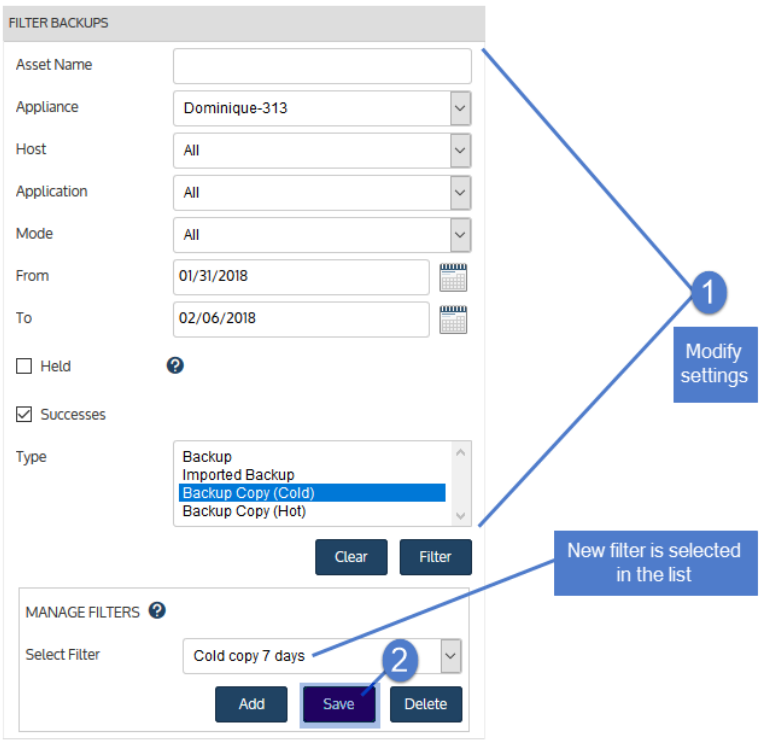
2 Enter the following:

- A unique name.
- (Optional) Check **Set as default** to automatically load this filter.

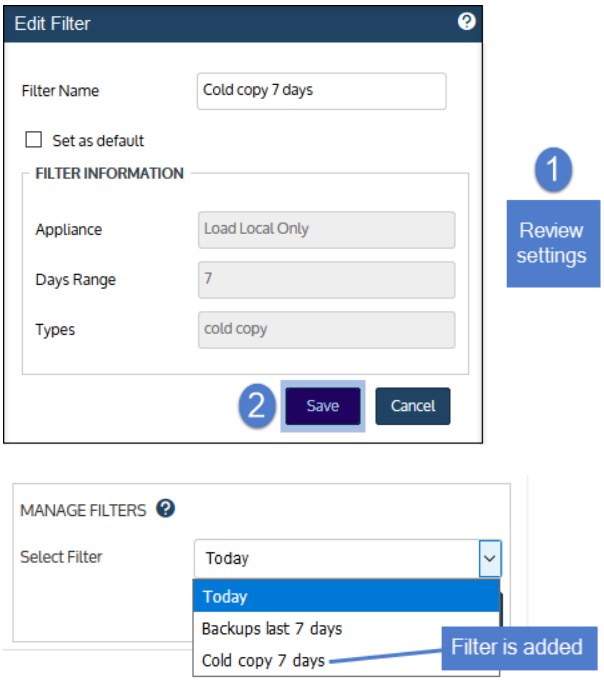
3 Click **Save**.



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

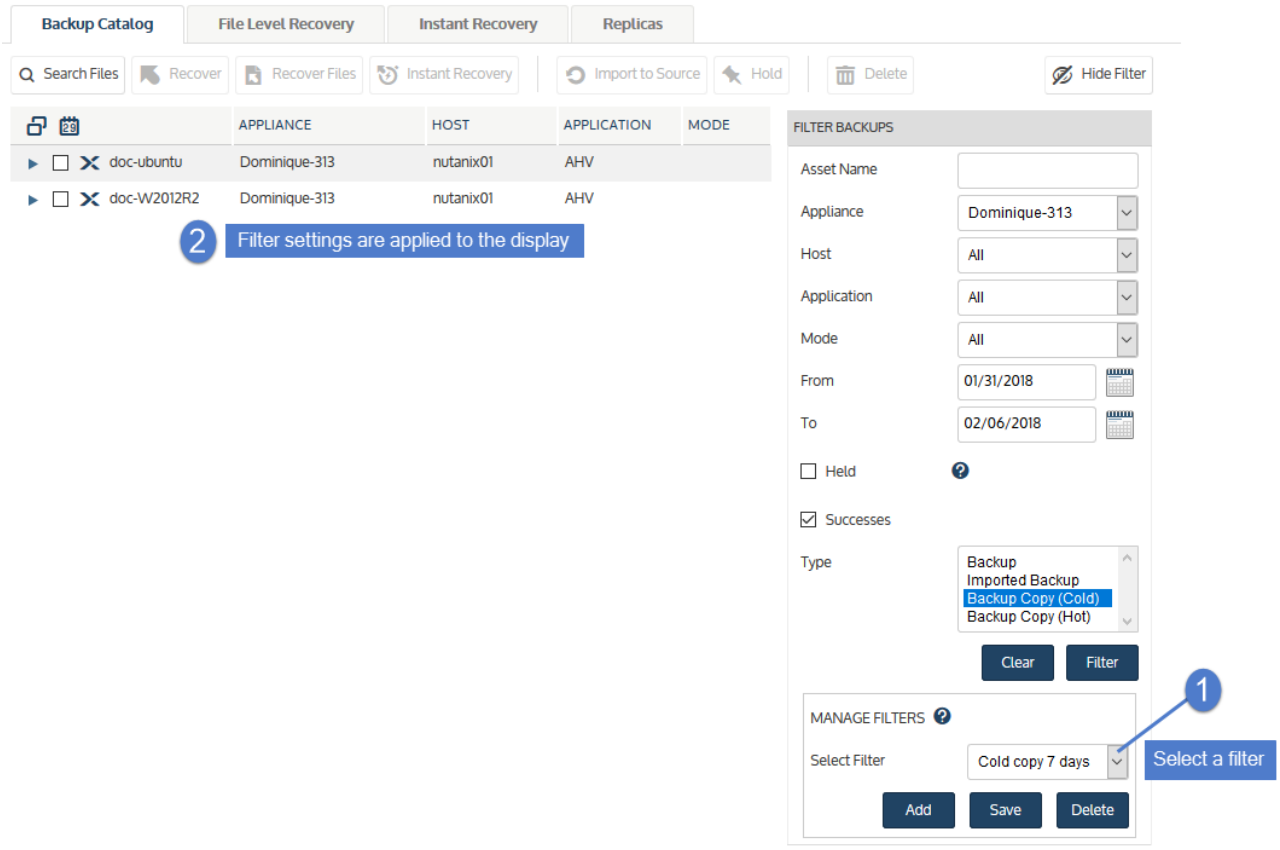


5 Review settings and click **Save** to exit.



To apply a filter

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



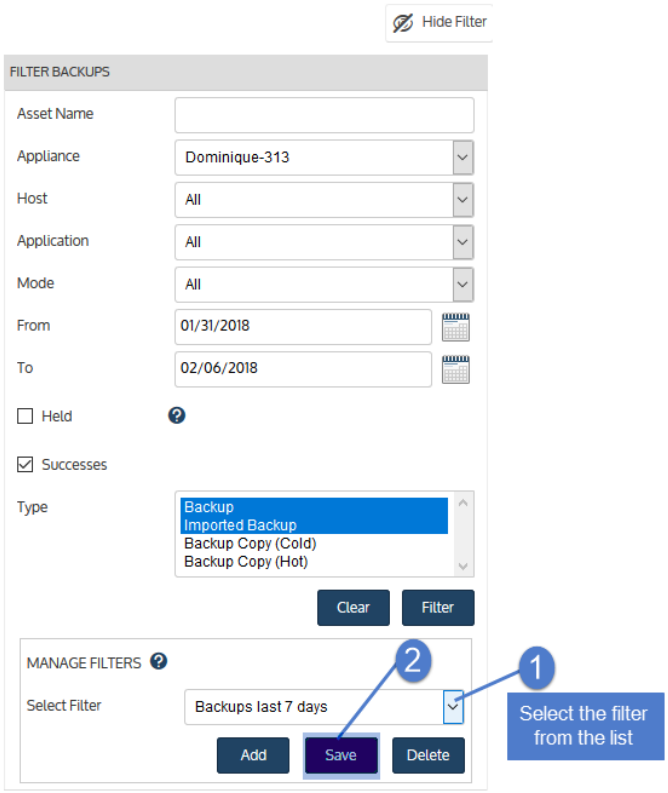
To assign a default filter

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:

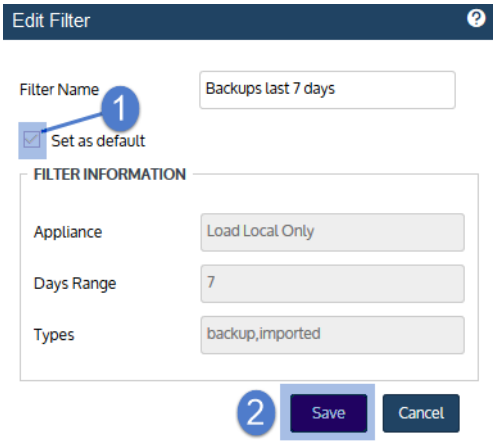
- Add a new custom filter. In the Add Filter dialog, check the **Set as default** box. For details, see "To add a filter" on page 72.
- Make an existing filter the new default by using these steps:

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**.



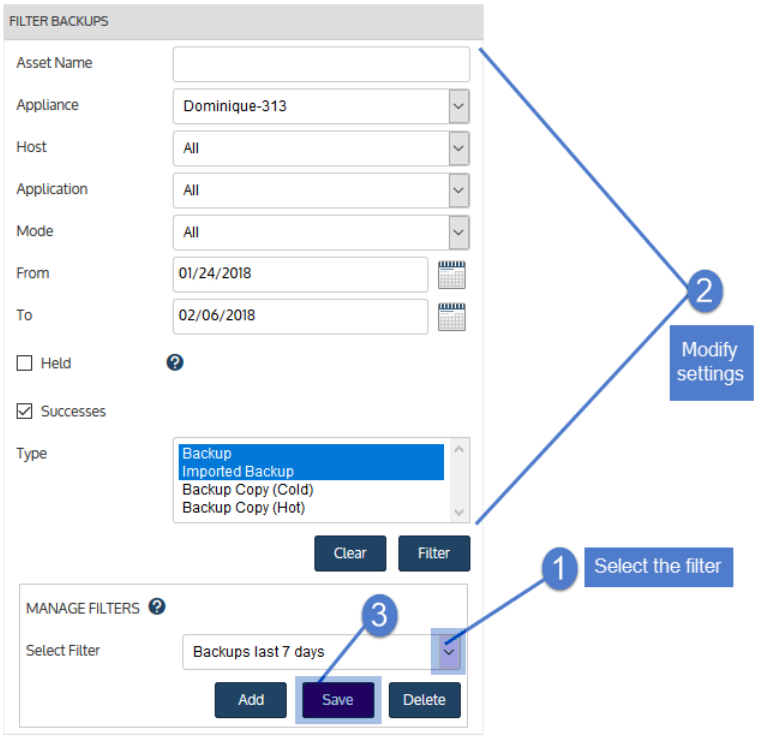
2 Check the **Set as default** box, then click **Save**.



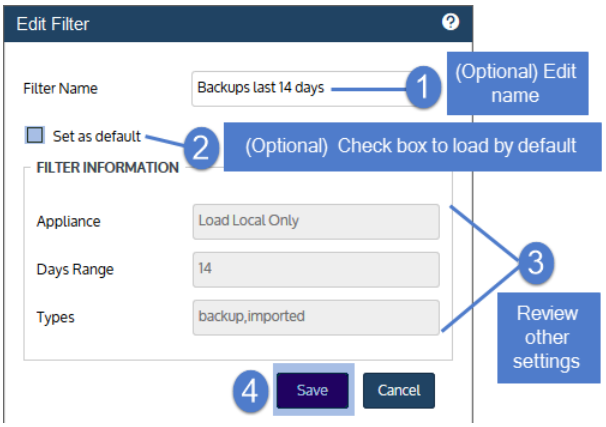
To edit a filter

1 Select the filter.

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

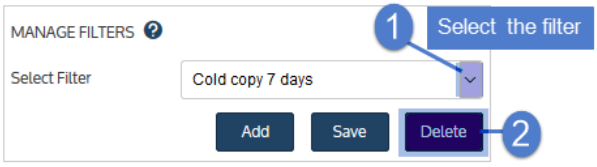


3 Review settings, modify name (optional), check the **Set as default** box (optional), then click **Save**.

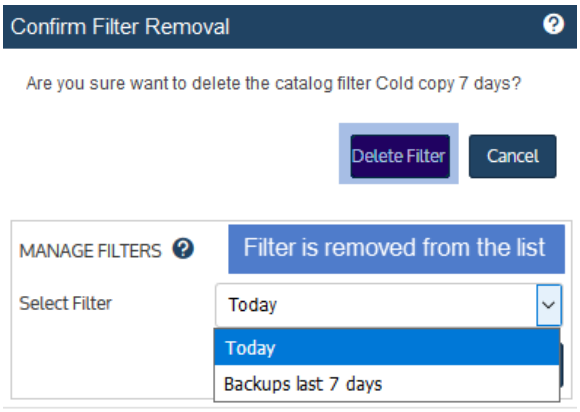


To delete a filter

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



2 Click **Delete Filter** to confirm.


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