

# Disaster Recovery

## Introduction

Protecting an organization's data and IT infrastructure has never been more important. This document describes the steps the Unitrends customer needs to take when planning and implementing a disaster recovery strategy. This strategy includes decisions that are best made long before a failure occurs.

An effective disaster recovery strategy consists of four aspects:

- ▶ The decision to archive or vault
- ▶ Preparation
- ▶ Restoring to a physical or virtual appliance
- ▶ Restoring backup data to clients

## Archive or Vault

Unitrends offers disaster recovery with both on-premise archiving and off-premise electronic vaulting.

Choosing which to use will be based on your particular needs, but the most effective disaster recovery strategy will be one in which these choices have been made well in advance.

Archiving is accomplished by storing backups, onsite, to a Unitrends appliance (which may be supplemented by third-party external storage devices), while vaulting involves block-level, in-flight deduplication of backups to an off-site location (also referred to as the disaster recovery site) in which a vault has been configured. Vaulting may be used alone for disaster recovery, or, in conjunction with archiving.

Archiving onsite to a Unitrends appliance offers a fuller level of retention, while vaulting may provide a higher level of reliability, since the data is transmitted to a location that is geographically distant to the disaster.

Successful recovery from a disaster using Unitrends' appliance solution requires that vaulting and/or archiving has been previously configured and implemented.

## Preparation

In the case of a disaster recovery event, the administrator will need a *fresh* appliance to which data may be restored. Depending on the business impacts of being *down* in the event of a true disaster, end-users may choose to:

Rely on their Platinum maintenance contract to deliver a replacement appliance to their disaster recovery site (shipped next business day)  
Purchase a replacement chassis at the time of the disaster under Silver and Gold maintenance contracts and wait 2 weeks (Silver) or 3-5 business days (Gold) for delivery of a new appliance to their disaster recovery site  
Purchase a standby, spare appliance chassis from Unitrends to have onsite in their disaster recovery center for the ultimate recovery scenario.

Next, to prepare your disaster recovery strategy, keep the following in mind:

Archive data at regular intervals and store disks in a safe location. (Archive to disk is not available for SFF-RecoveryOS).

Vault data directly to an off-site appliance at regular intervals.

**Step 1:** A complete disaster recovery strategy must include a record of certain information. You will need this information to restore protected systems in the event of disaster. Once the Unitrends appliance has been configured and the appropriate clients registered, the following information should be recorded and saved in such a way it can be accessed in the event of a system failure.

Asset #: \_\_\_\_\_

Software Serial #: \_\_\_\_\_

User String: \_\_\_\_\_

Feature String \_\_\_\_\_

License Key: \_\_\_\_\_

Note: License information can be found by accessing **Configure > License** on the user interface (RRC).

**Step 2:** Decide whether backups will be archived or vaulted.

**Step 3:** Setting up the Unitrends appliance for either Vaulting or Archiving. Depending on the type of protection you settle on, see the *Archiving* or the *Vaulting* sections for more information.

**Step 4:** Determine which clients will be protected. The steps for registering clients are covered in the *Client Registration* chapter.

**Step 5:** The creation of Bare Metal media for each of the registered clients. It is typically recommended that every client have a crash recovery media created as soon as it is set up, and then Bare Metal backups should be performed on a monthly basis, or, whenever major hardware or software changes are made to the client. For detailed information on this procedure, see the Bare Metal Boot CD chapter in the *Appliance and Agents User Manual*.

**Step 6:** Create schedules for running your desired backups. Go to the *Backups and Schedules* chapter of the *Appliance and Agents User Manual* to see detailed instructions for setting up backup schedules.

## Restoring the Appliance

We all hope it never happens, but if it does, the above preparation will leave you in the best possible position. This next part of the Disaster Recovery strategy involves the actual *recovery*. This is the information you will need to keep in mind if you find yourself having to restore your protected systems.

The following sections provide disaster recovery instructions for specific scenarios:

- ▶ Restoring a backup appliance
- ▶ Corrupted backup device
- ▶ Corrupted RAID
- ▶ Corrupt Internal Drive

### Scenario 1: Restoring A Backup Appliance

The following requirements are applicable whether you are restoring to a physical or virtual appliance. Additional requirements for restoring to a virtual appliance follow this section.

The original appliance being restored can be running any previous version of Unitrends' software. It is possible to restore to an appliance older than version 6.0.0 from a v6.0.0 Vault. However, the version of the new backup Appliance has to be of a same or newer version than the original appliance.

A *fresh* appliance to restore to. This can either be a new or a reimaged appliance. If you need to reimage an appliance for this process, contact your authorized Unitrends partner or Unitrends Support for additional details before proceeding.

It is recommended that the new appliance is assigned the same hostname as the original appliance.

When performing Disaster Recovery from an external storage like SAN/NAS/ internal data store that was previously configured as an archive device, the same storage should be added to the appliance by using the Storage Configuration (by navigating to Configuration > Storage). The purpose of the storage should be set as *Archive*.

**IMPORTANT !** If a storage device will be set up on the new appliance, it must be done prior to the restore process.

Disaster Recovery (**Tools > Disaster Recovery**) should be started by selecting the Vault in the navigation pane if restoring from a Vault. Similarly, Disaster Recovery (**Tools > Disaster Recovery**) should be started by selecting the Appliance in the navigation pane if restoring from an archive media.

The target appliance can be set up with additional storage devices that will house restored backups. This has to be done prior to the restore process. See section titled, "Storage Setup" below for additional details.

When using external storage or alternate storage, the target appliance must grant management privileges to the vault by:

- ▶ logging into the user interface (RRC) of the target appliance;
- ▶ navigating to **Configure > DPUs**; and
- ▶ clicking on **Allow Remote Management** on lower left side of the window.

When restoring from a vault, it is recommended that the target appliance and the vault be placed on an isolated network. This will help to ensure the integrity of the appliance during the restore process. For optimal results, it is recommended to use a cross-over cable to connect the target appliance to the vault.

## Scenario 2: Recovering From A Corrupt Backup Device

The following steps describe the recommended approach for recovering a DPU from a corrupted backup device. Examining the system logs to determine disk failure:

```
var/log/messages or  
  
/var/log/syslog
```

In the event of a single disk failure:

- ▶ Determine the failed disk drive by executing the appropriate disk controller command or by launching the disk controller tools (this can also be performed in BIOS):

```
tw_cli info <controller> [3ware-based appliances] or  
  
cat /proc/mdstat [for desktops and 1U appliances]
```

- ▶ Insert the new disk drive. Ideally, the new drive should be the same size, type and model as the original drive.
- ▶ Once the new drive is inserted, the rebuild process should begin automatically. If it does not, use the 3ware utility (for rack-mount units), or the `rebuild_disk` script (desktops and 1U appliances) to add the drive and launch the rebuild process.
- ▶ When the new device has been rebuilt successfully, it is ready for use.

## Scenario 3: Recovering From A Corrupt RAID

The following steps describe the recommended approach for recovering a DPU from a corrupted RAID. Examine the system logs (`/var/log/messages` or `/var/log/syslog`) to

determine if the disks on the disk controller are failing. If the failing disks are located on a controller that is failing, installing new disks on the failing controller will not solve the problem. This scenario assumes that the corrupted RAID is a result of multiple failed disks.

- ▶ Determine the failed disks by executing the appropriate disk controller commands or by launching the 3Ware utility (this can also be performed in BIOS):

```
tw_cli info <controller> [for 3ware-based appliances] or  
cat /proc/mdstat [desktops and 1U appliances]
```

- ▶ Insert the new disk drives. Ideally, the new disks should be the same size, type and model as the original disks.
- ▶ Once the new disks have been inserted, the rebuild process should begin automatically. If it does not, use the 3Ware utility (for rack-mount units), or the `rebuild_disk` script (desktops and 1U appliances) to add the drives and launch the rebuild process.
- ▶ When the new device has been rebuilt successfully, create a new Unitrends Postgres database with the following command:

```
/usr/bp/bin/setup_postgresql.sh create
```

- ▶ Perform Disaster Recovery from Vault or Archive. (See above for Disaster Recovery instructions).

If applicable, apply the manual steps following Disaster Recovery (see above for details).

## Scenario 4: Recovering A Corrupt Internal Drive

The following steps describe the recommended approach for recovering the system root drive on a Recovery-720 or Recovery-730.

- ▶ To determine which internal drive failed, view the alerts on the status window of the Web-based user interface. You may also view the contents of `/proc/mdstat`.
- ▶ If the drive is offline, bring the drive online and run the script

```
/usr/bp/bin/rebuild_disk.
```

- ▶ If the drive is corrupt, insert a new disk drive. The new disk drive must be the same size as the original disk drive.

- ▶ Once the new disk drive has been inserted, the rebuild process should begin automatically. If it does not, use the `/usr/bp/bin/rebuild_disk` script to format the new drive.

## Additional Requirements For Restoring To A Virtual Appliance

- ▶ Disaster Recovery to a virtual appliance from a vault or archive media requires all appliances to be running version 6.0.0 (or higher) of Unitrends' software.
- ▶ When restoring to a virtual appliance or to a new storage device on the target, the storage device must be set up prior to the restoration process.
- ▶ When restoring from a vault, the target appliance should grant management privileges to the Vault. To do so, login to the *Rapid Recovery Console* (RRC) of the target appliance, navigate to **Configure > DPUs**. Click on **Allow Remote Management** at the left bottom.

## Storage Setup

When restoring to a vRecovery appliance, also called the vRecovery Target appliance, it is required to be configured with storage devices to which data would be restored. Backup devices should be created on the target appliance prior to the restore. Storage can be internal data stores or external storages like SAN (connected via iSCSI or Fiber Channel) or NAS.

The recovery process will not attempt to connect to any storage, therefore, make the connection prior to beginning the restore. Depending on the amount of data that has to be restored to the appliance, the set up could vary. In all cases, if storage is directly added to the virtual appliance it cannot be packaged into an Open Virtualization Format (OVF), therefore external storage needs to be added as a data store to the ESX server hosting the virtual appliance.

Next, a virtual disk must be added to the virtual DPU using the designation of **Added Internal**. Set the purpose to **Backups** by clicking on **Configure > Storage**.

The following scenarios are possible, depending on the size of vaulted data:

Data less than 2TB - One virtual disk needs to be created on the data store housing the external storage.

Data greater than 2TB, no client greater than 2TB: Appropriate number of virtual disks need to be created with none greater than 2TB. The recovered system cannot be directly packaged into an Open Virtualization Format (OVF).

Data greater than 2TB, at least one client greater than 2TB: A floating storage device needs to be used to house client data greater than 2TB. This is required because the recovered

system cannot be directly packaged into an Open Virtualization Format (OVF). This device is directly connected to the target appliance and backup devices are added on this storage. This device has to be NAS only.

After storage devices are added to the target appliance, management privileges need to be granted to the vault, by navigating to **Configure > DPUs**.

## Disaster Recovery From Vault

- ▶ Log into the user interface (RRC) where the backups are vaulted. (By default: username: root and password: unitrends1)
- ▶ Select the appropriate vault in the Navigation pane.
- ▶ Click **Tools** in the user interface (RRC) menu bar.
- ▶ Click **Disaster Recovery**
- ▶ Select the Backup Appliance from the drop-down list. This is the name of the appliance being restored.
- ▶ Enter the IP address of the target appliance. This is the location to which the vaulted backups will be restored. If this is the original appliance, the default IP address that appears in this field should be used. If restoring to an alternate appliance, enter the new IP address. Note: If alternate storage is configured on the target management privileges it should be granted to the vault.
- ▶ If restoring to a virtual appliance or alternate storage, click **Select Target Storage**. Answer **Yes** to the question *Do you wish to get the list of devices defined on the new appliance?* The option to select the device for each client will be shown adjacent to the client.
- ▶ In the Select Clients table, select the client(s) and the devices to which those clients will be restored.
- ▶ Once the Disaster Recovery confirmation window opens, confirm the operation by placing a checkmark by the statement, *I understand the database and hosts file will be overwritten, and all existing backups on all devices will be deleted*, and click **Confirm**.
- ▶ If encryption was enabled on the original appliance you will be prompted to turn on encryption on the target appliance. For this, open the user interface (RRC) of the target appliance in a new browser window. Click **Tools > Encryption Manager**. Turn off encryption and restart it. You will require your master passkey to enable encryption.

- ▶ To check the status of the restore, select the vault again in the Navigation pane click **Tools > Job Status**
- ▶ Details from the latest recovery operation for each appliance recovered from the vault can be viewed in the Disaster Recovery log found in the General Support Toolbox.

## Automatic Disaster Recovery from Vault

An automated Disaster Recovery from vault operation may be performed on a regular basis. A key component of configuring this automated process involves the creation of a unique *profile*. A profile consists of information identifying the appliance being restored, the target IP address, clients and devices to be recovered, the start date and time, and the frequency with which the recovery will be performed.

### Create And Save An Automatic Disaster Recovery Profile

To set up the profile, perform the following steps from the Vault's user interface (RRC).

- ▶ In the **Disaster Recovery** pane, select the target appliance.
- ▶ Enter the IP address.
- ▶ Click Check for Automatic Disaster Recovery Profile.
- ▶ Assuming a profile does not already exist, check the box labeled, **Save Auto Disaster Recovery Profile** when it appears under the client table.
- ▶ Select the clients and devices to be recovered.
- ▶ Click **Confirm**.
- ▶ Once the **Disaster Recovery Profile Options** screen appears, select the start date and time and whether or not the system should check for encryption. Note: it is recommended this option be set to **YES**. If any backups on the vaulted appliance are encrypted, skipping this process will cause the Auto Disaster Recovery to fail. Additionally, it is recommended that a persistent passphrase be set for encryption.
- ▶ Once the profile options are set, click **Confirm**.
- ▶ When the **Disaster Recovery Profile Selections** detail screen opens, confirm the settings are correct. To make changes to the profile, click **Cancel**. Otherwise, click **Save** to proceed.

## View An Automatic Disaster Recovery Profile

To view an automatic disaster recovery profile:

- ▶ Select the appliance from the drop-down box.
- ▶ If the IP address of the target appliance is known, change the default IP address shown.
- ▶ Click **Check For Automatic Disaster Profile**
- ▶ If a profile exists for the given IP address, a **View Profile** option is shown.
- ▶ Click on **View Profile** to see the profile selections.

Saved profiles may be checked anytime by selecting an appliance from the drop-down box, and then entering the IP address. Clicking **Check for Profile** will display profiles if profiles exist. Clicking on View Profile will display the profile settings, where profiles may be removed. Existing profiles cannot be modified. To change a profile, you must remove the profile and create a new profile with your changes.

## Remove An Automatic Disaster Recovery Profile

In order to remove an automatic disaster recovery profile, first View the existing automatic disaster recovery profile (as discussed in previous paragraph) and click **Remove Profile**.

## Change, Stop or Suspend An Automatic Disaster Recovery Profile

An automatic disaster recovery profile cannot be changed or updated, but a new one can be created in its place. You will need to remove an existing automatic disaster recovery profile and then create and save a new one.

Once created, a profile cannot be stopped or suspended for a temporary period of time. It must be removed and recreated when required.

## Disaster Recovery from Archive

- ▶ Log into the appliance user interface (RRC).
- ▶ Select the appliance in the user interface (RRC) Navigation pane click **Tools** on the user interface (RRC) main menu.
- ▶ Click **Disaster Recovery**.
- ▶ Click **Scan for Archive Media**. External archive devices should be connected prior to attempting the restore.

- ▶ In the Select Media drop-down list, select the desired type of media device.
- ▶ If restoring to a virtual appliance or external storage, you may choose to replace storage by answering **YES** to the question *Media has been mounted. Would you like to use the storage (D2D) devices configured on the new appliance?*
- ▶ If YES is selected, the select **Target Storage** option will appear.
- ▶ If encryption was enabled on the original appliance you will be prompted to turn on encryption on the target appliance. For this, open the user interface (RRC) of the target appliance in a new browser window. Click **Tools > Encryption Manager**. Turn off encryption and restart it. You will require your master passkey to enable encryption.
- ▶ A list of clients will be populated. Note: the list of clients is populated only after the state restore is complete. Select the desired client(s) to restore and the devices to which the client backups will be restored to.
- ▶ Once the Disaster Recovery confirmation window opens, confirm the operation by placing a checkmark by the statement, *I understand the database and hosts file will be overwritten, and all existing backups on all devices will be deleted*, and click **Confirm**.

**NOTE:** If restoring to an alternate appliance, it might be necessary to change the hostname of the newly-restored appliance. The hostname will be that of the original while the IP address will be that of the new target appliance. They can be changed appropriately using the Configure>Network>Hosts interface after the restore is complete.

## Post-Recovery Considerations

The appliance's configuration information will be recovered when the Appliance state data has been restored. However, depending on the setup, additional steps may need to be performed in order to complete the Disaster Recovery operation.

- ▶ If required, re-configure the network with the new IP address. On the user interface (RRC) go to **Configure > Network > Ethernet** (eth0). Enter the new IP address and gateway as required. Select **Confirm**.
- ▶ If required, change the hostname via the user interface (RRC)
- ▶ Make sure vaulting is turned off if changing the hostname.
- ▶ Reconfigure the Appliance for synchronization via the user interface (RRC)
- ▶ Because synchronization is disabled during the restore process, ensure that the system is set to vault. On the user interface (RRC) go to **Configure > Vaulting Process > Connection Options** and **Vaulting Control > Resume Vaulting**

- ▶ If Microsoft Exchange CEP backups have been restored, change the login information for the workspace. Modifications to the workspace can be performed via the Exchange Web Admin application.
- ▶ Change owner and group of Exchange workspace on samba share to nobody. Use the following command for this:

```
chown -R <owner>:<group><workspace_path>
```

```
Example: chown -R nobody:nobody <workspace_path>
```

Also change the permissions to 777.

- ▶ If bonding was in use it will need to be reconfigured after the restore process is completed because it does NOT get restored.

Once the Appliance has been restored, individual clients can be restored using the user interface (RRC). See the section on **Managing Clients** for details on restoring individual clients.

## Restoring Backup Data to the Clients

Now that the Backup Appliance has been restored, restoring the clients can begin. Backups should be restored in the following order:

Bare Metal Backups

File Level Backups (Masters, Differentials or Incrementals)

Application Backups

### Bare Metal Basic Steps

Boot the client from the Bare Metal Media.

Restore the Bare Metal backup to the client. See the Bare Metal chapter for detailed instructions.

Reboot the client.

Restore the last incremental backup that was performed after the last master backup to the client. This may not be necessary if no incrementals have been done since the last master.

### File Level & Application Restore Basic Steps

To begin the restore process, log into the Appliance user interface (RRC) and select the appropriate client from the Navigation pane:

With the client selected in the Navigation pane, click **Restore**.

In the Restore pane, select the date from which the backup will be restored by clicking on the appropriate date in the **Recovery Point Day** calendar.

Select the appropriate time of day from which to restore a backup. The selection of this time can be made from either the available list of times in the **Recovery Point Times** table or by simply clicking on available wedges of time that appear on the 24-hour circle.

The command button for this operation changes depending on the type of restore. For file-level restores (as depicted in the above example) the user will click the **Restore** to initiate the restore process. For VM backups the user will click **Restore Files**, and **Restore Items** for Exchange backups.

In the **Restore from Backup of Client** pane, select individual files and applications to be restored, or place a checkmark by the client itself to perform a full restore.

If desired, change the **File Exclusion** options or the **Advanced Execution** options by clicking on the links at the bottom of the pane. Otherwise, click on **Restore**.

Note: for more information on configuring these options, see the **Restore File Exclusion Options** and **Advanced Execution Options for Restore** sections in the *Restore Procedures* chapter.

The Restore Progress bar will display the status of the restore and will indicate when it is complete.