Advanced Backup

⚠ This topic only applies to **Armor Complete** users.

⚠ To fully use this screen, you must have the following permissions assigned to your account:

- Read Advanced Backup Plans
- Read Advanced Backup
- Read Advanced Backup Vms
- Write Advanced Backup
- Create Advanced Backup Policy
- Read Advanced Backup Policy
- Read Advanced Backup Snapshots
- Refresh Advanced Backup Snapshots
- Remove Advanced Backup
- Request Advanced Backup Restore
- Update Advanced Backup Policy
- Commit Advanced Backup Restore
- Refresh Advanced Backup Snaphots
- Restore from Backup

Overview

⚠ Currently, **Advanced Backup** from Rubrik is available in the DFW01 (Dallas) and PHX01 (Phoenix) environments.

If you use the London (LHR01), Amsterdam (AMS01), or Singapore (SIN01) data centers, then you can use the Backup & Recovery add-on product from R1 Soft. To learn more, see Backup & Recovery.

⚠ This feature will eventually replace the snapshots service that is offered by default with Armor Complete.

You can use the **Advanced Backup** add-on product to take backups of your virtual machines. (These backups are also known as a snapshot.) In the event of data loss, you can use these snapshots to restore your virtual machine to a previous state. These snapshots will be stored with Armor, based on the retention configurations you create in the backup policy.

At a high-level, to use **Advanced Backup**, you must:

- Create a backup policy
- (Optional) Download and install the Rubrik agent
  - To restore specific files or folders, you must download and install the agent.
- Assign a policy to a virtual machine or fileset configuration

⚠ For **Advanced Backup**, there is a cost associated with the amount of data that you backup.

Armor offers two types of backups:

Type of Backup	Description	Additional Information
Virtual Machine	This backup restores your entire virtual machine.	Add Advanced Backup to restore a virtual machine
Fileset	This backup restores specific files or folders, not the entire virtual machine. When you create a policy, you can configure which files to include (and exclude) from the snapshot.	Add Advanced Backup for your filesets

Access the Advanced Backup screen

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.

2. Click **Advanced Backup**.

VM Protection

Column	Description
VM Name	This column displays the name of the virtual machine that is subscribed to **Advanced Backup**.
Location	This column displays the data center where the virtual machine is located (and where the backup will take place).
Policy Name	This column displays the descriptive name of the policy that is assigned to a virtual machine.
Last Backup	This column displays the last time Armor took a snapshot of your environment.
Storage Used	This column displays the amount of memory already collected.
Agent Status	This column displays if the agent is **Connected** or **Disconnected**.

Fileset Protection

Column	Description
VM Name	This column displays the name of the virtual machine that is subscribed to **Advanced Backup**.
Location	This column displays the data center where the virtual machine is located (and where the backup will take place).
Fileset Name	This column displays the assigned fileset grouping that will be backed-up.
Policy Name	This column displays the corresponding policy. This policy configures how often a backup will take and for how long that backup will be retained.
Storage Used	This column displays how much space has been used to store the backups. ⚠ For **Advanced Backup**, there is a cost associated with the amount of data that you backup.
Status	This column displays if the agent is **Connected** or **Disconnected**.

Filesets

Column	Description
Name	This column displays the name of the fileset group.
Location	This column displays the data center where the virtual machine is located (and where the backup will take place).
OS Family	This column displays the type of virtual machine.
Includes	This column displays the files that are included in the backup.
Excludes	This column displays the files that are not included in the backup.
Do Not Exclude	This column displays the files that have been configured to specifically be included in the backup.

Policies

Column	Description
Policy Name	This column displays the descriptive name of the policy that is assigned to a virtual machine.
Location	This column displays the data center where the virtual machine is located (and where the backup will take place).
Replication	This column displays if the policy has enabled the off-site replication feature.
Type	This column displays the type of protection (**Fileset Protection** or **VM Protection**) that the corresponding policy provides.

Assets Protected	This column displays the name of the virtual machine that contains the assigned policy.
Default Indicator	This column indicates if the corresponding policy is a default policy. With a default policy, when you create a new virtual machine in the same data center, this policy will be displayed, and you can quickly add the policy to the virtual machine.

Restore Logs

Column	Description
Event	This column displays a completed action. You can use this information to view the progression of a restoration. ⚠ When you restore a virtual machine from a virtual machine restoration, you will see: • Retrieving Snapshot • Committing to snapshot ⚠ When you restore a fileset from a virtual machine restoration, you will see: • Restoring Vm File from Snapshot ⚠ When you restore a fileset from a fileset restoration, you will see: • Restoring files
Message	This column describes a completed action, including the corresponding virtual machine or filesets.
Start Time	The date and time when this action began to take place.
End Time	The date and time when this action ended.
Status	This column describes the status of the action taking place, which can result in **success**, **in-progress**, or **failure**.
Snapshot Date	This column displays the date and time that the snapshot was taken.

Add Advanced Backup for virtual machine restoration

You can use these instructions to create and store snapshots of your virtual machine.

⚠ To simply create a backup of specific files or folders, see Add Advanced Backup for your filesets.

To enable backup on your virtual machine, you must:

- Create a policy
- (Optional) Download and install the Rubrik agent
- Assign a policy to a virtual machine

⚠ You must use an existing virtual machine. To create a virtual machine, see Virtual Machines.

⚠ A newly created virtual machine may not appear immediately in this screen. You may need to wait an hour before a newly created virtual machine appears.

To properly backup SQL databases, before you create a backup policy, Armor recommends that you separately create a backup of the database, and then place that backup in the server to be backed-up.

Step 1: Create a backup policy

You must create a policy to configure how often to take a backup and how long to keep a backup.

By default, times are based on your web browser's configured time zone.

The location of your virtual machine does not relate to the time zone used in this feature.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **Advanced Backup**.
3. Click **Policies**.
4. Click plus (+) icon.
5. In **Policy Name**, enter a descriptive name.
6. In **Location**, select the data center where the virtual machine is located (and where the backup will take place).
7. In **Type**, select **VM Protection**.
8. Next to **Backup Schedule**, under **Take Snapshots (Frequency)**, enter how often Armor should take a snapshot. And then directly across, under **Keep Snapshots (Retention)**, enter how long Armor should keep this snapshot.
    - You must enter your time configurations in the same row.
        - For example, to take a snapshot every week and to keep that snapshot for six months, under **Take Snapshots (Frequency)**, in **Every (Days)**, enter **7**, and then directly across, under **Keep Snapshots (Retention)**, in **For (Days)**, enter **182**.
    - You can create a maximum of four **Frequency** and **Retention** settings.
    - The minimum retention period is 3 days.
    - Additionally, you must create a policy that takes place once per day. You must enter a time in hours.
        - For example, to take a snapshot every two hours and to keep that snapshot for three days, under **Take Snapshots (Frequency)**, in **Every (Hours)**, enter **2**, and then directly across, under **Keep Snapshots (Retention)**, in **For (Days)**, enter **3**.
9. (Optional) In **Snapshot Window**, configure the time frame for when your scheduled snapshots should take place. By default, Rubrik will determine when the scheduled snapshots will take place; however, with this option, you have the ability to configure a specific time frame for when the scheduled snapshots will take place. This option can be useful if you want to perform snapshots during a period of low traffic.
10. Next to **First Full Window**, configure the time frame for when the first full snapshot should take place.
    - Armor recommends that you configure a time when your environment experiences low traffic, low transaction volume, or low changes.
    - By default, times are based on your web browser's configured time zone.
    - After the first full snapshot is complete, the configuration you created under **Take Snapshots (Frequency)** and **Take Snapshots Between** will be implemented.
        - For example, next to **First Full Window**, if you configure an initial time frame of Sunday 12 AM to Sunday 6 AM, then your first full snapshot will take place at any time during this time frame. After the first full snapshot is complete, then the time frame configured in **Take Snapshots (Frequency)** and **Take Snapshots Between** will begin. If the first snapshot completes at Sunday at 5 AM, and your policy includes a snapshot every 4 hours, then the next snapshot will take place at 9 AM, and then again at 1 PM.
11. Click **Create Policy**.

(Optional) Step 2: Download the Rubrik agent

To perform a full virtual machine restoration, you do not need to download and install the agent. However, if you download and install the agent, then you will have the ability to perform a separate fileset restoration.

You must download an agent for every data center you use.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **Advanced Backup**.
3. Click **VM Protection**.
4. Hover over the (+) icon, and then click the **Download Rubrik Agent** icon.
5. Select the data center where the virtual machine lives.
    - This must be the same data center that you selected in **Step 1: Create a policy**.
6. Select the operating system for the desired virtual machine.
7. Download and install the installer package onto your server.

Operating system	Step 1: Download the agent	Step 2: Install the agent

Windows	Download and install the installer package in AMP, or run the command below.
	
	⚠ The following command uses the DFW01 data center.
	
	Be sure to replace DFW01 with your desired data center.
	
	`$AllProtocols = [System.Net.SecurityProtocolType]'Tls11,Tls12'`
	`[System.Net.ServicePointManager]::SecurityProtocol = $AllProtocols`
	`Invoke-WebRequest https://get.core.armor.com/backup/DFW01/RubrikBackupService.zip -OutFile .\RubrikBackupService.zip`
	`Add-Type -assembly "System.IO.Compression.FileSystem"`
	`[IO.Compression.ZipFile]::ExtractToDirectory((Get-ChildItem .\RubrikBackupService.zip).FullName, (Get-Item -Path ".\").Fullname + "\RubrikBackupService").\RubrikBackupService\RubrikBackupService.msi /qn`
		Not applicable

CentOS	Download the installer package in AMP, or run the command below. ⚠ The following command uses the DFW01 data center. Be sure to replace DFW01 with your desired data center. `sudo wget https://get.core.armor.com/backup/DFW01/rubrik-agent.x86_64.rpm`	Run the following command: `sudo rpm -i rubrik-agent.x86_64.rpm`
Ubuntu	Download the installer package in AMP, or run the command below. ⚠ The following command uses the DFW01 data center. Be sure to replace DFW01 with your desired data center. `sudo wget https://get.core.armor.com/backup/DFW01/rubrik-agent.x86_64.deb`	Run the following command: `sudo dpkg -i rubrik-agent.x86_64.deb`
Red Hat Enterprise Linux	Download the installer package in AMP, or run the command below. ⚠ The following command uses the DFW01 data center. Be sure to replace DFW01 with your desired data center. `sudo wget https://get.core.armor.com/backup/DFW01/rubrik-agent.x86_64.rpm`	Run the following command: `sudo rpm -i rubrik-agent.x86_64.rpm`

Step 3: Assign a policy

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **Advanced Backup**.
3. In **VM Protection**, hover over the (+) icon.
4. Click the **Add VM Protection** icon.
5. For **Select A Location**, select the data center where the desired virtual machine lives.
    - This must be the same data center that you selected in **Step 1: Create a policy**.
6. In **Select Your VM(S**), mark the desired virtual machine (or machines).
    - This table will only list virtual machines that do not have an assigned policy. To assign a different policy to a virtual machine, see Replace an existing policy for a virtual machine.
    - A newly created virtual machine may not appear immediately in this list. You may need to wait an hour before a newly created virtual machine appears.

7. In **Select A Policy**, select the newly created policy.
    - You can only select a policy that was created for the same location as the selected virtual machine.
    - You can only select a virtual machine-specific policy; you cannot select a fileset-specific policy.
8. Create **Configure Backup**.
    - This action will populate the table in the **VM Protection** section of the **Advanced Backup** screen.

Restore a virtual machine from a virtual machine snapshot

If your virtual machine is running in a corrupt state, or if you notice data loss, then you may choose to restore that virtual machine to one of your retained backups.

During a restoration, you may experience intermittent issues in your environment. As a result, Armor recommends that you restore a virtual machine from a backup during a period of low traffic.

Once the restoration process has started, you will not be able to rollback your virtual machine.

1. In the Armor Management Portal, in the left-side navigation, click **Infrastructure**.
2. Click **Advanced Backup**.
3. In **VM Protection**, locate and hover over the desired virtual machine.
4. Click the vertical ellipses.
5. Click **Refresh Available Backups**.
    - This action ensures that AMP lists the latest retained backup.
6. Hover over the desired virtual machine again, and then click the vertical ellipses.
7. Click **Restore from Backup**.
8. Locate the desired snapshot, and then click the corresponding vertical ellipses.
9. Click **Restore**
10. Click **Restore** again.
    - Once the restoration has started, you will not be able to rollback your virtual machine.
    - If you are not satisfied with the selected snapshot, you can select a different snapshot in a later step.
    - Once the restoration is complete, the **Status** column for the corresponding virtual machine will display **Pending Commit**.
        - During a **Pending Commit** status, the virtual machine will operate in a transitional storage environment. The virtual machine is fully operational; however, during this time, storage performance may not run in an optimal state.
11. Hover over the desired virtual machine, and then click the vertical ellipses.
12. Click **Commit to Snapshot**.
    - This action will cause your data to move from the transitional storage environment to the production storage environment where storage performance will return to the appropriate storage tier. At this point, the status will display as **Restore Successful**.
    - Storage performance will be impacted during this commit process, so you may want to perform this step at a time during periods of low anticipated traffic.
    - You can still make changes to your environment before and after you click **Confirm Snapshots**. Rubrik will create a separate file (or files) to accommodate any changes made during the final restoration process.
    - In the event that you do not commit, the virtual machine will be auto-committed after 72 hours.
    - If you want to select a different snapshot, from the vertical ellipses, select **Choose Different Snapshot**.
13. Click **OK**.
14. In the **VM Protection** section, review the **Status** column to view the status of your restoration.
    - Additionally, you can access the **Restore Logs** section to view the progression of a restoration.

After you begin the restoration process, you can still cancel the restoration.

Before the snapshot reaches the **Pending Customer Commit** status, you can cancel a restoration. (You can use the **Review Logs** section to view the status of the restoration.)

1. In the Armor Management Portal, in the left-side navigation, click **Infrastructure**.
2. Click **Advanced Backup**.
3. In **VM Protection**, locate and hover over the desired virtual machine.
4. Click the vertical ellipses.
5. Click **Cancel VM restore**.
6. Click **Continue**.

Restore a fileset from a virtual machine snapshot

You can use these instructions to restore a fileset from a virtual machine snapshot.

You cannot use these instructions to restore a fileset from a filest snapshot.

To restore a fileset from a fileset snapshot, see Restore a fileset from a snapshot.

⚠ To restore a fileset from a virtual machine snapshot, you must have the Rubrik agent installed in the corresponding data center.

1. In the Armor Management Portal, in the left-side navigation, click **Infrastructure**.
2. Click **Advanced Backup**.
3. In **VM Protection**, locate and hover over the desired virtual machine.
4. Click the vertical ellipses.
5. Click **Register Rubrik Agent**.
6. Review the **Agent Status** column to display **Installed**.
7. Click the vertical ellipses, and then select **Refresh From Available Backups**.
8. Click the vertical ellipses, and then select **Restore From Backup**.
9. Locate the desired snapshot, and then click the vertical ellipses
10. Click **Browse**.
11. Navigate to the specific file or folder to restore.
    - You can also navigate to a high-level folder.
12. Hover over, and then click the vertical ellipses.
13. Click **Restore**.
14. There are two types of restorations.
    - **Option 1**: Mark **Overwrite Original** to replace your existing files with the restored files.
    - **Option 2**: Mark **Restore to Separate Folder** to place the restored files in a separate location. This option will not replace your existing files. You can use this option to verify specific files before you remove the original files.
        - In **Folder Name**, enter a valid file path to place the restored files.
15. Click **Restore**.
16. To review the status of the restoration, in the top menu, click **Restore Logs**.

Add Advanced Backup for fileset restoration

You can use these instructions to retain snapshots of specific files, and not of your entire virtual machine.

⚠ To properly backup SQL databases, before you create a backup policy, Armor recommends that you separately create a backup of the database, and then place that backup in the server to be backed-up.

Step 1: Create a policy

You must create a policy to configure often to take a backup and how long to keep a backup.

⚠ By default, times are based on your web browser's configured time zone.

The location of your virtual machine does not relate to the time zone used in this feature.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **Advanced Backup**.
3. Click **Policies**.
4. Click plus (+) icon.
5. In **Policy Name**, enter a descriptive name.
6. In **Location**, select the data center where the virtual machine is located (and where the backup will take place).
7. In **Type**, select **Fileset Protection.**
8. Next to **Backup Schedule**, under **Take Snapshots (Frequency)**, enter how often Armor should take a snapshot. And then directly across, under **Keep Snapshots (Retention)**, enter how long Armor should keep this snapshot.
    - You must enter your time configurations in the same row.
        - For example, to take a snapshot every week and to keep that snapshot for six months, under **Take Snapshots (Frequency)**, in **Every (Days)**, enter **7**, and then directly across, under **Keep Snapshots (Retention)**, in **For (Days)**, enter **182**.
    - You can create a maximum of four **Frequency** and **Retention** settings.
    - The minimum retention period is 3 days.
    - Additionally, you must create a policy that takes place once per day. You must enter a time in hours.
        - For example, to take a snapshot every two hours and to keep that snapshot for three days, under **Take Snapshots (Frequency)**, in **Every (Hours)**, enter **2**, and then directly across, under **Keep Snapshots (Retention)**, in **For (Days)**, enter **3**.
9. (Optional) To enable off-site replication, for **Replication**, mark **On**.
    - Select a **Location**.
    - Configure a time for retention.
    - This time cannot be larger than the time configured for local retention.
    - This feature stores copies of your snapshots in another physical location, which you can retrieve in case the copies in your local machine are not accessible or usable.
    - There is a cost associated with this feature.
10. (Optional) In **Snapshot Window**, configure the time frame for when your scheduled snapshots should take place. By default, Rubrik will determine when the scheduled snapshots will take place; however, with this option, you have the ability to configure a specific time frame for when the scheduled snapshots will take place. This option can be useful if you want to perform snapshots during a period of low traffic.
11. Under **First Full Window**, configure the time frame for when the first full snapshot should take place.
    - Armor recommends that you configure a time when your environment experiences low traffic, low transaction volume, or less frequent changes.
    - By default, times are based on your web browser's configured time zone.

- After the first full snapshot is complete, the configuration you created under **Take Snapshots (Frequency)** and **Take Snapshots Between** will be implemented.
    - For example, under **First full Window**, if you configure an initial time frame of Sunday 12 AM to Sunday 6 AM, then your first full snapshot will take place at any time during this time frame. After the first full snapshot is complete, then the time frame configured in **Take Snapshots (Frequency)** and **Take Snapshots Between** will begin. If the first snapshot completes at Sunday at 5 AM, and your policy includes a snapshot every 4 hours, then the next snapshot will take place at 9 AM, and then again at 1 PM.

12. Click **Create Policy**.

Step 2: Create a fileset

In this step, you will specify the specific folders or files to include (and exclude) from a snapshot.

You can use an asterisk to replace a single folder name in a file path. For example, you can enter **C:*\Microsoft Office**, which is the same as **C:\Program Files\Microsoft Office**.

You can enter two asterisks (**) to replace multiple folder names in a file path.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **Advanced Backup**.
3. Click **Filesets**.
4. Click the plus (+) icon.
5. In **Fileset Name**, enter a descriptive name.
6. In **Location**, select the data center where your virtual machine lives.
    - You must use the same data center that you configured in **Step 1: Create a policy**.
7. In **OS Family**, select the type of virtual machine.
8. Under **Rules**:
    - In **Include**, enter the files to include in the backup.
    - In **Exclude**, enter the files to exclude from the backup.
    - In **Do Not Exclude**, enter the files to overwrite the information in the **Exclude** field.
        - For example, you can configure the backup to exclude every image file; however, you can specify a specific image file to be included in the backup.
9. Click **Create Fileset**.

Step 3: Download the Rubrik agent

> ⚠ You must download an agent for every data center you use.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **Advanced Backup**.
3. Click **Fileset Protection**.
4. Hover over the (+) icon, and then click the **Download Rubrik Agent** icon.
5. Select the data center where the virtual machine lives.
    - You must use the same data center that you configured in **Step 1: Create a policy**.
6. Select the operating system for the desired virtual machine.
7. Download and install the installer package onto your server.

Operating system	Step 1: Download the agent	Step 2: Install the agent

Windows	Download and install the installer package in AMP, or run the command below.
	
	⚠ The following command uses the DFW01 data center.
	
	Be sure to replace DFW01 with your desired data center.
	
	`Invoke-WebRequest https://get.core.armor.com/backup/DFW01 /RubrikBackupService.zip -OutFile .\RubrikBackupService.zip`
	`Add-Type -assembly "System.IO.Compression.FileSystem" [IO.Compression.ZipFile]::ExtractToDirectory((Get-ChildItem .\RubrikBackupService.zip).FullName, (Get-Item -Path ".\"). Fullname + "\RubrikBackupService")`
	`.\RubrikBackupService\RubrikBackupService.msi /qn`
		Not applicable

CentOS	Download the installer package in AMP, or run the command below. ⚠ The following command uses the DFW01 data center. Be sure to replace DFW01 with your desired data center. `sudo wget https://get.core.armor.com/backup/DFW01/rubrik-agent.x86_64.rpm`	Run the following command: `sudo rpm -i rubrik-agent.x86_64.rpm`
Ubuntu	Download the installer package in AMP, or run the command below. ⚠ The following command uses the DFW01 data center. Be sure to replace DFW01 with your desired data center. `sudo wget https://get.core.armor.com/backup/DFW01/rubrik-agent.x86_64.deb`	Run the following command: `sudo dpkg -i rubrik-agent.x86_64.deb`
Red Hat Enterprise Linux	Download the installer package in AMP, or run the command below. ⚠ The following command uses the DFW01 data center. Be sure to replace DFW01 with your desired data center. `sudo wget https://get.core.armor.com/backup/DFW01/rubrik-agent.x86_64.rpm`	Run the following command: `sudo rpm -i rubrik-agent.x86_64.rpm`

Step 4: Assign a fileset policy to a virtual machine

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **Advanced Backup**.
3. Click **Fileset Protection**.
4. Hover over the plus (+) icon, and then click the **Add Fileset Protection** icon.
5. Select the desired virtual machine, and then click **Configure Backup**.
    - A newly created virtual machine may not appear immediately in this list. You may need to wait an hour before a newly created virtual machine appears.
6. Select the desired fileset and policy, and then click **Add**.

Restore a fileset from a fileset snapshot

⚠ During a restoration, you may experience intermittent issues in your environment. As a result, Armor recommends that you perform a restoration during a period of low traffic.

1. In the Armor Management Portal, in the left-side navigation, click **Infrastructure**.
2. Click **Advanced Backup**.
3. In **Fileset Protection**, locate and hover over the desired fileset.
4. Click the vertical ellipses.
5. Click **Restore from Backup**.
6. Locate and hover over the desired snapshot.
7. Click the vertical ellipses, and then click **Browse**.
8. Navigate to the specific file or folder to restore.
    - You can also navigate to a high-level folder.
9. Hover over, and then click the vertical ellipses.
10. Click **Restore**.
11. There are two types of restorations.
    - **Option 1**: Mark **Overwrite Original** to replace your existing files with the restored files.
    - **Option 2**: Mark **Restore to Separate Folder** to place the restored files in a separate location. This option will not replace your existing files. You can use this option to verify specific files before you remove the original files.

        - In **Folder Name**, enter a valid file path to place the restored files.
12. (Optional) Slide **Continue on restore errors** to avoid a possible interruption or cancelation of the restoration.
    - If you activate this option, then in the event a file cannot be restored, the system will continue to try to restore all other selected files.
    - If you do not activate this option, then in the event a file cannot be restored, the system will not attempt to restore additional files. Files that were previously restored will remain.
13. Click **Restore**.
14. To review the status of the restoration, in the top menu, click **Restore Logs**.

Edit an existing policy

⚠ Before you update an existing policy, consider that:

- You cannot update the location of an existing policy.
- If you update the **Snapshot Window** for an existing policy and there is a virtual machine already assigned to the policy, then the virtual machine will not experience another first full snapshot.
- Existing snapshots for the virtual machine will remain stored with Armor.
- If you decrease the **Retention** rate, then older snapshots will be removed in accordance with the updated policy. For example, if you lower the retention rate from 14 days to 10 days, then backups older than 10 days will be removed.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **Advanced Backup**.
3. Click **Policies**.
4. Locate and hover over the desired policy.
5. Click the vertical ellipses.
6. Click **Edit**.
7. Make your desired changes, and then click **Update Policy**.

Replace an existing policy for a virtual machine

You can use these instructions to replace one existing policy with another existing policy for a virtual machine.

⚠ Before you begin, consider that:

- When you replace a policy, the virtual machine will not experience another first full snapshot.
- Existing snapshots for the virtual machine will remain stored with Armor.
- If you replace a policy that has a different **Retention** rate, then older snapshots will be removed in accordance with the updated policy. For example, if the newly assigned policy has a retention rate of 10 days whereas the previously assigned policy had a retention rate of 14 days, then backups older than 10 days will be removed.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **Advanced Backup**.
3. In **VM Protection**, locate and hover over the desired virtual machine.
4. Click the vertical ellipses.
5. Click **Assign New Policy**.
6. Under **Policy**, select an existing policy to use.
7. Click **Update Policy**.
    - Policy changes will not affect existing backups unless the **Retention** rate is decreased. In this case, older snapshots will be removed in accordance with the updated policy. For example, if you lower the retention rate from 14 days to 10 days, then backups older than 10 days will be removed.

Delete a policy

You cannot delete a policy that is assigned to a virtual machine. As a result, you must first unassign a policy from a virtual machine.

⚠ You can skip **Step 1: Unassign a policy** if:

- You have already unassigned a policy from a virtual machine.
- You have never assigned a policy to a virtual machine.
- You want to delete a fileset protection policy.

Step 1: Unassign a policy

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **Advanced Backup**.
3. In **VM Protection**, locate and hover over the desired virtual machine.
4. Click the vertical ellipses.

5. Click **Assign New Policy**.
6. Under **Policy**, select an existing policy to use.
7. Click **Update Policy**.

Step 2: Delete an unassigned policy

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **Advanced Backup**.
3. Click **Policies**.
4. Locate and hover over the desired policy.
5. Click the vertical ellipses.
6. Click **Delete**.
7. Click **OK**.

Remove Advanced Backup from a virtual machine

You can use these instructions to remove the **Advanced Backup** add-on product from a virtual machine.

When you remove **Advanced Backup**:

- A snapshot will no longer be taken of the virtual machine.
- Snapshots of the virtual machine will no longer be available.

> ⚠ This action will not delete the policy associated with the virtual machine. The policy will still be available in the **Policies** section of the **Advanced Backup** screen.

> ⚠ Based on when you remove this feature, you may receive a charge for the service on your next invoice.

1. In the Armor Management Portal (AMP), in the left-side navigation, click **Infrastructure**.
2. Click **Advanced Backup**.
3. Locate and hover over the desired virtual machine.
4. Click the vertical ellipses.
5. Click **Remove from Backup**.
6. Click **OK**.

Troubleshooting

If you cannot access or update the **Advanced Backup** screen, consider that:

- You do not have permissions to view this add-on product.
  - You must have the following permissions to fully use the **Advanced Backup** add-on product. Contact your account administrator to enable these permissions. (If you are an account administrator, then to update your permissions, see Roles and Permissions (Armor Complete)).
    - Read Advanced Backup Plans
    - Read Advanced Backup
    - Read Advanced Backup Vms
    - Write Advanced Backup
    - Create Advanced Backup Policy
    - Read Advanced Backup Policy
    - Read Advanced Backup Snapshots
    - Refresh Advanced Backup Snapshots
    - Remove Advanced Backup
    - Request Advanced Backup Restore
    - Update Advanced Backup Policy
    - Commit Advanced Backup Restore
    - Refresh Advanced Backup Snaphots
    - Restore from Backup

For Vormetric users:

As a Vormetric user, how should I configure my files for Advanced Backup?

You must update the encryption policy to allow the Rubrik agent to access your files and directories.

You can give Rubrik read-only permissions or read and decrypt permissions.

If you allow read-only permissions, then the files will be backed up in an encrypted format; however, the Vormetric DSM, agent, and keys will need to be available in order to access the recovered, encrypted data. As a result, these files will have a higher change rate.

If you give Rubrik read and decrypt permissions, then the unencrypted files will be encrypted when they are transmitted to the backup appliance and platform. During this time, the content can potentially be recovered by Armor in an unencrypted format, which may not meet your desired security practices or compliance requirements.

During a file backup, if some files are missing, will I see an error message?

The Rubrik agent silently skips any files that it cannot access and continues with the backup. As a result, Rubrik does not generate any kind of error message.

To correct, this, please update the file system permissions, or the encryption policy, so that the Rubrik agent can access these files.

Related Documentation

- Armor Marketplace
- Firewall Rules
- Install SSL VPN Client for Ubuntu 16.x
- Install SSL VPN Client for Ubuntu 18.x
- IP Address
- Virtual Machines
- Workloads