Quest

Rapid Recovery 6.1.2

Replication Target for Microsoft Azure

Table of Contents

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Introduction to Rapid Recovery Replication Target for Microsoft Azure

Welcome to the *Rapid Recovery Replication Target for Microsoft Azure Setup Guide*.

Topics include:

- About this guide
- Working with Microsoft Azure
- Accessing your virtual machine from your Azure account
- Exploring your Rapid Recovery Replication Target VM desktop

About this guide

This document is for Microsoft Azure users who want to replicate on-premise backups from a Rapid Recovery version 6.x Core to the cloud, taking advantage of the simplicity, security and redundancy offered by Azure, Microsoft's cloud computing platform.

This document assumes the following:

- **You are a Rapid Recovery Core 6.x user.**

  This document assumes that you use (or plan to use) Rapid Recovery Core 6.x software to provide backup, replication and recovery solutions for your enterprise.
  For more information about Quest Rapid Recovery, please visit http://quest.com/products/rapid-recovery/.

- **You have a subscription to Microsoft Azure.**

  For more information about the Azure cloud platform, or to sign up, see http://azure.microsoft.com/en-us/.

- **You created (or plan to create) a VM on Azure to use as your replication target.**

  From the Azure Marketplace gallery, you can select a pre-configured virtual machine to add to your account by searching for Rapid Recovery Replication Target VM in Azure. Add this VM to your Azure account as a prerequisite.
  For more information, see About creating Azure virtual machines for replication target.

- **You know how to use Microsoft Azure.**

  Microsoft has substantial documentation on using Azure available in its documentation center. For more information, see Microsoft Azure documentation.

- **You know how to attach an empty disk to an Azure VM.**

  As part of setting up a VM to replicate from your source Core, you must have dedicated storage in your Azure account that is associated with your replication target VM. For more information, see Adding storage to your Azure VM.

This setup guide includes the following sections:

- Introduction to Rapid Recovery Replication Target for Microsoft Azure. This section includes conceptual information about the Azure replication target. It includes links to prerequisite tasks you must accomplish on the Microsoft Azure platform, and includes links to resources. It also describes how to access your VM once it is created, and describes the desktop of a newly created replication target VM.
- Upgrading from AppAssure 5.4.3 Replication Target. If you are upgrading your Azure replication target virtual machine (VM) from AppAssure 5.4.3 to Rapid Recovery 6.x, there are special considerations addressed in this section. If not upgrading, skip this section.
- Setting up your replication target VM. Setup is simple and quick; all steps should take less than half an hour. This section describes how to set up your new or updated replication target on Azure. Included are directions for adding storage volumes, running the included configuration utility, and disabling Compatibility View in Internet Explorer.
- Understanding licensing. Once your Core on the Azure VM is configured, you must register a software license. This section includes information about Rapid Recovery licenses, how to activate your license, and references to relevant documentation and resources.
- Considerations for seeding data to your target Core. This section outlines the process of seeding data from your source Core to your replicated Core. It describes steps specific for your replication target on Azure, and references other relevant content about replication.

Working with Microsoft Azure

Microsoft Azure is a subscription-based cloud computing platform. The following information is provided to Rapid Recovery customers to facilitate using Azure with our product.

Topics include:

- Azure interface disclaimer
- About creating Azure virtual machines for replication target
- Microsoft Azure documentation

Azure interface disclaimer

The Microsoft Azure interface is subject to change.

The information provided in this document relating to steps required in Azure were current as of the date of publication. This information is provided as a service to our customers to assist them with Azure prerequisites.

However, when working with Azure, be aware that specific steps, URLs or even the Azure interface may change at any time, which is beyond our control.

If you are having difficulty performing any steps related to your Azure account, please seek the advice of a Microsoft Azure representative.

About creating Azure virtual machines for replication target

To use Azure as a replication target for your on-premise Core, you must first create a pre-configured VM in your Azure account. To do this, log into your Azure account, and search the Azure Marketplace for the **Rapid**

Recovery Replication Target VM in Azure product. Select it and then create the VM in your Azure account. This process uses Azure Resource Manager to provision virtual machines and storage.

NOTE: Specific steps to create the VM on the Azure marketplace are not included in this document, because the Azure interface can change. For the procedure to create this VM (current as of the date of publication), see the Rapid Recovery knowledge base article 197356, "How to Create a virtual machine to use for Rapid Recovery Replication Target VM in Azure." For assistance with purchasing the VM from the Azure marketplace, please consult the Azure documentation or contact Azure technical support.

The VM you create for replication of your Rapid Recovery Core in the Azure cloud is pre-configured with specific attributes. For example:

- The VM created when you select this product from the Azure marketplace contains desktop shortcuts and configuration scripts referenced frequently in this document.

  For more information, see Exploring your Rapid Recovery Replication Target VM desktop.
- Rapid Recovery Cores require robust Microsoft Windows servers such as the Windows Server 2012 R2, which is the default OS for your VM.
- Specific ports (8006, 8007, 8009, 80, 81) are open on the VM by design for necessary network operations including replication, license management, and so on.
- Azure offers specific configurations to support your applications. These include a specific number of processors, RAM, and disk size. The minimum recommended configuration for replication to your Azure VM is D3. The replication needs of most enterprises are served by D3, D4, and D14. It is never bad to use VM configurations with more resources.

For more information on Azure configurations and pricing, see the virtual machines pricing page on the Azure website. For links to other useful references on Microsoft websites, see .

An earlier edition of this Setup Guide described how to set up an existing Microsoft Azure VM for use as a replication target for an AppAssure 5.4.3 Core. For that edition and other AppAssure documentation, please see https://support.quest.com/appassure/5.4.3/release-notes-guides.

Microsoft Azure documentation

Microsoft has substantial documentation on using Azure available in its documentation center.

For information on creating an Azure account, spinning up a VM for use with a Rapid Recovery or AppAssure Core, adding a storage account, and more, see the Microsoft documentation at https://azure.microsoft.com/en-us/documentation.

For example, for information on provisioning or managing Windows VMs, see https://azure.microsoft.com/en-us/documentation/services/virtual-machines/windows/.

For online videos about using Azure, see http://azure.microsoft.com/en-us/get-started/.

NOTE: The Azure website uses language and country codes for its web addresses, which affect display of the content. For example, `https://azure.microsoft.com/[country-code]/[destination]/`.

NOTE: The URLs for Azure used throughout this document include the country code for English in the United States. For other languages, based on the settings on your computer and the content Microsoft offers, URLs may differ based on these codes.

Relevant Microsoft links

Some relevant articles on Microsoft websites are listed below:

- Azure login page (US)
- Microsoft Azure home page
- Microsoft documentation center
- Windows virtual machines documentation
- Videos: Get started with Azure
- Azure Virtual machines pricing
- Azure services by region
- About Azure storage accounts
- Creating a storage account on Azure
- How to attach a data disk to a Windows VM in the Azure portal
- Use the Microsoft Azure Import/Export Service to Transfer Data to Blob Storage
- Import/Export Pricing
- Storage: Import/Export Hard Disk Drives to Windows Azure (blog post)

Accessing your virtual machine from your Azure account

This procedure assumes that you have a Microsoft Azure account, and that you have already created a Rapid Recovery Replication Target VM in your Azure account.

Azure login requires JavaScript. You may need to enable JavaScript or otherwise adjust security settings in the browser accordingly. For more information, consult your systems administrator.

Optionally, for a newly provisioned VM, you may want to disable the Compatibility View in the Internet Explorer web browser settings. For more information, see Disabling Compatibility View in Internet Explorer.

Follow this procedure to access your Rapid Recovery Replication Target VM.

1. Log in to your Azure account as described in the following steps.

   NOTE: While the precise steps, URL, or the user interface for logging into Azure may change, the main purpose of this step is to log into your Microsoft account to view your Azure account.

   a. From a web browser, enter the Azure login URL.

   The format for this web address is `https://azure.microsoft.com/[country-code]/account/`.

   For example, in the United States, go to https://azure.microsoft.com/en-us/account/.

   The Manage your Azure Account page appears.

   b. Click **Azure portal**.

   You are redirected to a Microsoft Azure login page.

   c. In the username text box, enter your email address or phone number associated with your Microsoft account.

   d. In the password field, enter your Microsoft password.

e. Click **Sign in**.

2. If you are prompted to allow Azure.com to use additional storage on your computer, select **Yes**.

   Your initial Azure VM only has enough space for the operating system. Confirming this prompt lets you extend storage on the VM. For example, it lets you run a script on your VM to configure Rapid Recovery Core, including the creation of a repository as the storage location to store your replicated recovery points from your source Core.

3. In the Azure dashboard, from the left navigation menu, click **Virtual machines** to open the **Virtual machines** page.
4. In the list of virtual machines, click the name for your Rapid Recovery replication target VM.
5. In the details pane for the selected VM, note the public internet protocol (IP) address or domain name system (DNS) name label.

   For example, `ReplicationVM1.cloudapp.net`.

6. You can open the VM in a new browser window, by entering into your browser location field the URL in format: `https://<IP or DNS>:8006`, where the <IP or DNS> parameter is the IP address or DNS name shown in your Azure account, and 8006 is the port.

   Using the previous example, your VM URL is `https://ReplicationVM1.cloudapp.net:8006`.

   Your replication target VM appears.

7. If you see a **Windows Security** prompt, select an appropriate certificate, and continue to the website.

Exploring your Rapid Recovery Replication Target VM desktop

This topic describes the items you see on the Rapid Recovery Replication Target VM before and after setup.

1. Click the **X** in the top right of the Server Manager window to close Server Manager.

   Your Rapid Recovery virtual machine uses the Windows Server 2012 R2 operating system. Each time a virtual or physical machine using this OS starts, Windows opens the Server Manager utility.

2. Note the **Configure Rapid Recovery Replication Target for Azure** shortcut on the desktop.

   Double-clicking this shortcut launches a script to configure your Core, or to format virtual disks for your Core. Before launching, you must first select the appropriate storage in your Azure account. For more information, see Adding storage to your Azure VM.

   For more information about running the configuration script, see Running the Core configuration script from the VM desktop.

   NOTE: If you add storage from the Azure Marketplace and attach it to your VM prior to running this script, the virtual disk is automatically configured as the destination for your Rapid Recovery repository. You can also run the script again any time you attach additional storage, to format the disk and add it as a repository storage location.

3. Note the **Rapid Recovery License Portal** shortcut on the desktop.

   Double-clicking this shortcut opens the Rapid Recovery License Portal in your web browser, where you can manage Rapid Recovery licenses. Each Core must be registered with the license portal.

   This license portal was previously known as the AppAssure License Portal. If you already have a license portal account you have used for AppAssure, use that account information. Previous license portal users do not need to register a new account for Rapid Recovery.

   Information about licenses is located in the Rapid Recovery License Portal 6.1 User Guide.

4. Note the **Quest Software Support** shortcut. Double-click this shortcut to view technical product documentation on the Quest Support website.

The Support portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the Support portal provides direct access to product support engineers through an online Service Request system.

5. Note the **Rapid Recovery 30-day trial key.lic** file on the desktop.

   This file is the temporary 30-day license for your Rapid Recovery Core. You can import this license file the first time you start the Core. For more information about licenses, see Understanding licensing. For instructions on activating a license, see Activating your Rapid Recovery license.

6. Note the **Rapid Recovery Documentation** shortcut. Double-click this shortcut to view technical product documentation on the Quest Support website.

   Documentation for Quest Rapid Recovery products is hosted on the Quest Support portal at https://support.quest.com/rapid-recovery/technical-documents.

7. After you have run the configuration script for the first time, you see a **Core Console** shortcut on the desktop.

   Double-clicking this shortcut opens the Rapid Recovery Core Console. You can use the configured Rapid Recovery Core as a replication target. This Azure VM serves as the destination, or target Core, to host machines replicated from any Rapid Recovery source Core.

   The first time you open the Core Console, you will be prompted to associate a license key. You can use the temporary key on the desktop, or obtain a perpetual license from Quest and enter that information.

Next steps

- Your Azure VM is considered a self-managed target Core. For more information about using Rapid Recovery version 6.1.x, including setting up replication targets, see the *Rapid Recovery User Guide,* particularly the topic Replicating to a self-managed target core.
- Information about licenses is located in the Rapid Recovery License Portal 6.1 User Guide.

Upgrading from AppAssure 5.4.3 Replication Target

This section applies only to users of AppAssure version 5.4.3 Replication Target for Microsoft Azure. If you are not upgrading an Azure VM from AppAssure version 5.4.3 to Rapid Recovery 6.x, proceed to the topic Setting up your replication target VM.

CAUTION: AppAssure version 5.4.3 includes localization to the following languages: Chinese (simplified), French, Korean, German, Japanese, Portuguese (Brazil), and Spanish (international).

CAUTION: Rapid Recovery release 6.0.1, including the Core Console and the PowerShell module, is available in English only. If running a 5.4.3 Core in other languages, Quest recommends upgrading directly to Rapid Recovery release 6.0.2 or 6.1.x. These releases (in addition to English) are also localized in the same 7 languages.

CAUTION: If you have a VM on Azure that is a replication target for your AppAssure 5.4.3 Core, and you want to upgrade your on-premises Core to Rapid Recovery 6.x, you must upgrade your target Core before your source Core.

Topics include:

- Archiving the repository
- Upgrading your target Core on the Azure VM
- Updating the configuration script on the Azure VM
- Running the updated configuration script on the Azure VM
- Upgrading any other target Cores
- Upgrading source Cores that replicate to your Azure VM

Archiving the repository

Keep the following points in mind regarding archiving the target Core repository.

NOTE: Since this topic addresses updating an AppAssure version 5.4.3 Core, references first link to the *AppAssure User Guide* for release 5.4.3 (revision B).

- While some users may choose not to archive due to time or resource constraints, Quest recommends archiving as a best practice.
- Quest recommends archiving to a data store in Azure. However, you can archive to any other location.
- Be advised that Microsoft charges fees when data is transmitted from Azure to another source.
- For detailed instructions on archiving, see Creating an archive in the *AppAssure User Guide*. When following those steps, please note:
  - A one-time archive is appropriate in this situation.
  - To archive to your Azure account, you must add the credentials for connecting to your Azure account to your Core.

For more information on performing this task in AppAssure Core version 5.4.3, see Adding a cloud account.
For more information on performing this task in Rapid Recovery Core version 6.0.1, see the *Rapid Recovery User Guide* topic Adding a cloud account.

- After adding your Azure cloud account, when selecting a location to archive in the Core Console, select the Cloud option.
- When defining options for the one-time archive, note that Microsoft Azure cloud archives are automatically divided into 200 GB segments.
- For best results, select the **Build recovery points chains (fix orphans)** option for your archive.

- For more information on archiving in AppAssure Core version 5.4.3, see the *AppAssure User Guide*, especially the topics Retention and archiving, Understanding archives and Creating an archive.
- For more information on archiving in Rapid Recovery Core version 6.0.1, see the *Rapid Recovery User Guide*, especially the topics Retention and archiving, Understanding archives and Creating an archive.

Upgrading your target Core on the Azure VM

You must have credentials for the Rapid Recovery License Portal to download the Rapid Recovery Core installer.

Following are general steps for upgrading your target Core.

For detailed information about upgrading a Core installation, see the *Rapid Recovery Installation and Upgrade Guide*.

1. From your Azure VM, log in to the license portal at https://licenseportal.com, and navigate to the **Downloads** page.
2. In the Windows-Based Applications area of the **Downloads** page, scroll down to the row in the table labeled **Core Installer**. In the last column, click **Download**.

   NOTE: Do not use the Core Web Installer.

   The executable Core installer file downloads to the location specified.
3. Right-click on the Core installer and select **Run as administrator**.

Updating the configuration script on the Azure VM

You must have an AppAssure version 5.4.3 Core on an Azure VM that you want to update to Rapid Recovery 6.x.

This task requires that the original configuration script resides on the desktop. If you moved the configuration script, return it to the desktop before performing this procedure.

You must have credentials for the Rapid Recovery License Portal to download the updater script used in this procedure.

If you already have an Azure replication target VM for use with an AppAssure 5.4.3 Core, use this procedure to you can update the configuration script. Thereafter, running the configuration script installs the Rapid Recovery 6.x Core and configures any disks you have attached to the VM as DVM repository storage locations on the Core.

1. From your Azure VM, log in to the license portal at https://licenseportal.com, and navigate to the **Downloads** page.
2. In the Windows-Based Applications area of the **Downloads** page, scroll down to row in the table labeled **Azure Replication Target Configuration Utility Updater**. In the last column, click **Download**.

   A compressed file named `RR_Azure_Rep_TGT_Config_Util_Updater.zip` downloads to the location specified.
3. Right-click on the compressed update utility file, select **Extract All**, accept the default settings, and then click **Extract**.

   The decompressed folder RR_Azure_Rep_TGT_Config_Util_Updater saves to the desktop. In the folder, an executable file, RR_Azure_Rep_TGT_Config_Util_Updater.exe, appears.
4. Right-click on the executable utility file, and select **Run as administrator**.
5. In the **WinRAR self-extracting archive** dialog box, leave the default destination folder (typically `C:\Program Files\AppRecovery\Core\PowerShellScripts\VM_FTBU`), accept the default settings, and then click **Install**.
6. If you are prompted to replace any existing files, follow the process indicated to confirm replacement for all files.

   A Windows PowerShell script starts. Several windows may appear as the script runs.
7. If you are prompted to accept an execution policy change, follow the process indicated to confirm the change.

   The window closes and the script completes.

   Parameters in the configuration script on your Azure VM desktop are now updated to use the appropriate values.

   A 30-day license key for the Rapid Recovery Core appears on the desktop.
8. Optionally, close unneeded open windows.
9. Optionally, move or archive the license key for the previous version so you will not confuse the two keys.

Next steps

Use the new license key when first starting your Cores. You must obtain a long-term license to continue using the Core. For more information about licenses, see Understanding licensing. For instructions on activating a license, see Activating your Rapid Recovery license.

Running the updated configuration script on the Azure VM

After you have run the update script, you can run the configuration script to update your Core configuration. You can also run the updated configuration script after you attach additional storage to the Azure VM, which adds the storage volume as another storage location in your DVM repository.

For more information, see the topic Running the Core configuration script from the VM desktop.

Upgrading any other target Cores

Best practice is to upgrade all target Cores before updating the source Core.

If you have target Cores other than your Azure VM target, update those Cores before updating the source Core.

For information on upgrading the Core software, see the *Quest Data Protection* | *Rapid Recovery Installation and Upgrade Guide*, including the parent topic Upgrading to Rapid Recovery and all of its sub-topics.

For more information on best practices for upgrading, including upgrading when using replication, see the *Quest Data Protection* | *Rapid Recovery Installation and Upgrade Guide* topic Upgrading factors to consider.

Upgrading source Cores that replicate to your Azure VM

Best practice is to upgrade all target Cores before updating the source Core. For more information on best practices, see the *Rapid Recovery Installation and Upgrade Guide* topic Upgrading factors to consider.

After upgrading your target Cores on the Azure VM, you can upgrade your source Cores that replicate to Azure.

For information on upgrading the Core software, see the *Rapid Recovery Installation and Upgrade Guide*, including the parent topic Upgrading to Rapid Recovery and all its sub-topics.

Setting up your replication target VM

This section describes the tasks required to set up your replication target virtual machine on Azure.

Topics include:

- Adding storage to your Azure VM
- Running the Core configuration script from the VM desktop
- Disabling Compatibility View in Internet Explorer

Adding storage to your Azure VM

This procedure assumes that you have a Microsoft Azure account, and that you have already created a Rapid Recovery replication target VM in your Azure account.

When you create a virtual machine from the Azure Marketplace, the VM includes only the amount of memory reserved for the operating system. From your Azure account, you must attach at least one additional data disk to your replication target VM.

CAUTION: The current maximum storage size for any single disk that can be purchased from the Marketplace is 1023GB (for practical purposes, in this document we refer to this as 1TB). For best results, it is recommended that you add storage disks for working with Rapid Recovery replication target in 1TB increments. If you need more storage for your replicated target Core, you can attach additional 1TB disks to your Azure VM.

You can add storage to your Azure VM before you set up Rapid Recovery replication target, or any time afterward. Quest recommends adding storage first, for the sake of simplicity. If you add storage before setting up your replication target Core using the configuration script, the repository is automatically defined as the storage location for your repository.

If you attach storage to your VM after the Core is configured, you can run the configuration script again to automatically associate that storage with your repository. Alternatively, you can add a new storage location to an existing Rapid Recovery DVM repository from the Core Console GUI on your VM. For more information, see the *Rapid Recovery User Guide* topic Adding a storage location to an existing repository.

NOTE: While the precise steps or the user interface for adding storage to your Azure VM may change, the main purpose of this step is to attach at least one data disk to your replication target VM. You can also search for relevant articles in the Azure documentation center. For example, see How to attach a data disk to a Windows VM in the Azure portal.

Perform the following procedure in your Azure account to attach storage to the replication target VM.

1. Log into your Azure VM.
2. In the Azure dashboard, from the left navigation menu, click **Virtual machines**.

   The **Virtual machines** page appears.
3. In the list of virtual machines, click the name for your replication target VM.

Two more panes appear. The first shows details for the selected VM, and the second pane shows settings for the VM.

4. In the **Settings** pane, click **Disks**.

   The **Disks** pane expands.

5. In the **Disks** pane, from the top menu, select **Attach new**.

   The **Attach new disk** pane appears.

6. Enter values as described in the following table to specify storage disk attributes.

Option	Description
Name	Type an appropriate name for your storage disk. For example, type ReplicationVM1_StorageVolume1.
Type	Select the appropriate disk type. Standard disks use standard magnetic disks. Premium (SSD) disks use solid state drives and have low latency. Quest recommends using premium disks on Azure for high transfer rates or frequent replication.
Size (GiB)	Enter the appropriate disk size. Quest strongly recommends using a 1023GB disk (the current maximum for Azure). **NOTE:** When you run the configuration utility (described in the topic Running the Core configuration script from the VM desktop), any empty storage disks that you attached to your Azure VM are automatically added to your Core as a DVM repository. If multiple disks are attached, each is configured as a separate storage location in the DVM repository. If you want to add more than one storage disk at the outset, add them all before running the configuration script. **NOTE:** If you add more storage to your Azure VM later, you can run the configuration script again to automatically add the new disk as an extent (storage location) to your existing DVM repository. **NOTE:** You can also add a new disk manually, by adding a storage location to a DVM repository from within the Core Console. For more information, see the *Rapid Recovery User Guide* topic Adding a storage location to an existing repository.
Location	Confirm the default location.
Host caching	Select the appropriate host caching option.

Option	Description
	NOTE: You can select the default (None).

7. Review the information you specified for the new disk, and then click **OK**.

   After a brief wait, the new disk appears in the **Disks** pane.
8. Optionally, if you want to add any additional disks, repeat steps 5 through 7 of this procedure
9. Optionally, verify whether each storage volume you attached is recognized by the VM by using utilities such as Disk Management or Device Manager. If any volume is not recognized, Microsoft recommends rebooting the VM to ensure all storage drives are accessible.
10. Optionally, you can close the browser with your Azure account information.

Next steps

Proceed to the next step in the setup process, Running the Core configuration script from the VM desktop.

Running the Core configuration script from the VM desktop

This task describes the process of running a configuration script from the shortcut on the desktop of your Azure replication target VM. Quest recommends performing this process after first attaching storage to the Azure VM, and repeating it each time you add additional storage to your VM. Running this script typically takes about five minutes, after which the command window closes.

- You must license a Rapid Recovery replication target virtual machine from the Azure Marketplace. This process is performed on the resulting VM.
- After initial configuration of your VM, if you attach additional storage from the Azure Marketplace, running this script configures the virtual disk as the storage location for your repository.

Perform this step from the desktop of the Azure VM to configure the Rapid Recovery Core software.

CAUTION: During the execution of this script, if you are prompted with a dialog box to format the drive, *you must select* Cancel. The script then formats the storage drive using appropriate settings.

1. From the Azure VM desktop, right-click on the **Configure Rapid Recovery Replication Target for Azure** shortcut, and from the context-sensitive menu, select **Run as administrator**.

   A command window entitled **Administrator: Windows PowerShell** appears, and the script begins to run. Several operations occur sequentially, and the progress of the script is logged in the command window.
2. If a **Microsoft Windows** dialog box appears prompting you to format the disk before you can use it, click **Cancel**.

   The script continues to run; the script formats the storage drive in the most efficient manner for using the Rapid Recovery Core. When the script is complete, the command window closes. The **Core Console** shortcut appears on the desktop, to let users easily launch the Rapid Recovery Core Console.

Next steps

Before replicating, you must disable the Compatibility View feature in the Internet Explorer web browser. For more information, see Disabling Compatibility View in Internet Explorer.

Disabling Compatibility View in Internet Explorer

This task describes the process to disable the Compatibility View option of Internet Explorer. This step is required for using the Rapid Recovery Core Console on the Azure VM.

Internet Explorer includes a Compatibility View feature. The purpose of this feature is to correct the display of websites optimized for old versions of Internet Explorer (version 7 or earlier). By default, this option is typically enabled for all intranet sites, but can present problems when viewing modern web interfaces.

Disable the Compatibility View option as described in this topic to use the Rapid Recovery Core Console with Internet Explorer.

1. Open an Internet Explorer web browser window on the Azure VM.

   For example, double-click the Core Console shortcut on the VM desktop.

   An Internet Explorer web browser window opens. If the content does not display, check for and disable the Compatibility View feature as follows.

2. From Internet Explorer, click the  **Tools** icon, and then select **Compatibility View Settings**.

   The **Compatibility View Settings** dialog box appears.

3. In the **Compatibility View Settings** dialog box, clear the following settings:

Option	Description
Display intranet sites in Compatibility View	You must clear this option. This appears in all versions of Internet Explorer.
Display all websites in Compatibility View	Clear this option if it appears in your version of Internet Explorer.

4. Click **Close**.

   The dialog box closes, and Compatibility View is now disabled.

Understanding licensing

Each Core must have a software license that registers with the license portal.

Topics include:

- About Rapid Recovery licenses
- Activating your Rapid Recovery license

About Rapid Recovery licenses

To use and manage any version of Rapid Recovery, AppAssure, or DL series backup and recovery appliance software, you need two items:

1. **An account on the Rapid Recovery License Portal**.

   License portal accounts are free. If you are a new user, register at https://licenseportal.com. When you register, use the email address that is on file with your Quest Sales representative. If upgrading from a trial version, use the email address associated with the trial version. If you need to use a different email address, contact your Quest sales representative for assistance.

   NOTE: This license portal was previously known as the AppAssure License Portal. If you already have a license portal account that you have used for AppAssure, use that account information. Previous license portal users do not need to register a new account for Rapid Recovery.

   For more details about the license portal, please see the *Rapid Recovery License Portal User Guide*.

2. **A software license.**

   The Rapid Recovery Core software requires a valid software license to perform uninterrupted backups, replication, or data restoration.
   For the time period that it is valid, you can use a trial license. However, after a trial license expires, the Rapid Recovery Core stops taking snapshots, replicating, and restoring until you obtain and register a valid long-term license. For simple steps to register a temporary or long-term license, follow the procedure in the topic Activating your Rapid Recovery license.

   - **Rapid Recovery Core.** If you registered for a trial version of Rapid Recovery Core, the installer is configured with a trial license which you can use immediately. This temporary license is valid for 14 days, and can be extended one time by the group administrator to a 28-day license.
   - **Replication to a target Core.** If replicating to a target Core, you must have a valid replication-only license on the target Core.

     If using Replication Target for Microsoft Azure, your VM comes with a **Rapid Recovery 30-day trial key.lic** file (stored on the VM desktop). To continue replicating after the trial license expires, you must obtain and register a permanent replication-only license. This type of license is included for free to any licensed user of Rapid Recovery Core or AppAssure Core. To obtain a long-term replication-only license, contact your Quest Sales representative.
   - **Quest DL backup and recovery appliances.**

     If you purchased a Quest DL backup and recovery appliance, your appliance is configured with a 30-day temporary license that is activated automatically the first time you start the Core on the appliance. After you purchase software or a Quest DL appliance, you receive by email a long-term (non-trial) license file or license number. If specified on the sales order, the license is sent to the end user email address. Otherwise, the long-term license is sent to the contact email address on the sales order.

   The process for registering a temporary or long-term license are identical.

Contacting a Quest Sales representative

You can contact your Quest sales representative for assistance using the Contact Quest Software website at http://quest.com/company/contact-us.aspx.

For more information about licenses

For more information about Rapid Recovery licenses, see the following resources:

- For simple steps to register a temporary or long-term license, follow the procedure in the topic Activating your Rapid Recovery license.
- You can extensively manage Rapid Recovery licenses using the Rapid Recovery License Portal at https://licenseportal.com/. You must create an account to use this portal.
- For information on using the license portal, see the appropriate License Portal User Guide.
- For more information on managing Rapid Recovery licenses from the Rapid Recovery Core Console, see the *Rapid Recovery User Guide* topic Managing licenses.

  After upgrading your license, it is best practice to refresh the connection between the Core and the license portal. For more information, see the User Guide topic Contacting the Rapid Recovery License Portal server.

Activating your Rapid Recovery license

The Rapid Recovery Core software requires a software license. Follow this procedure to activate your Rapid Recovery Core license the first time you log in to the Rapid Recovery Core Console.

Before using the Rapid Recovery Core on an Azure VM as an incoming replication target, you must first disable Compatibility Mode. For more information, see Disabling Compatibility View in Internet Explorer.

Use this process to activate your temporary 30-day license, or to activate a perpetual license you received from a Quest Sales representative.

NOTE: If you select the temporary license, then to continue using Rapid Recovery Core after the introductory period, you must obtain a valid software license. For more information, see About Rapid Recovery licenses.

1. On your Azure VM desktop, double-click the **Core Console** shortcut icon.

   If Compatibility View is disabled, then the first time you open the Core Console, you see a prompt to upload a license file or enter a license key.
2. To upload a license file, do the following:
   a. From the **Choose license file or enter license key** field, click **Choose File**.

   The Choose File to Upload dialog box appears.

   b. Navigate to the license file and select the filename.

   For example, navigate to the desktop and select the Rapid Recovery 30-day trial key.lic file.

   c. From the **Choose File to Upload** dialog box, click **Open** to confirm the license file selection.

   The dialog box closes, and the filename of the license appears in the Choose license file or enter license key field.
3. To enter a license key you received from a Quest Support representative, do the following:
   a. In the **Choose license file or enter license key** field, type the license key precisely.

   You must enter the exact key. If you copy the key and paste it into the Choose license file or enter license key field, ensure that you do not include any spaces before or after the key.

b. Confirm the license key you entered key is correct.

4. To confirm the license file or key, click **Continue**.

   The license dialog box closes, and the license is applied to the Core. The Rapid Recovery Core Console user interface appears. In the Rapid Recovery Core Console, the **Welcome to the Core Quick Start Guide!** dialog box appears. Your software license is now registered for the appropriate period.

Next steps

- If you attached storage to your Azure VM before running the configuration script, the script automatically formats the virtual disk and uses it as the storage location for your repository. Your Core is then fully configured, and your repository is ready to use as a target for incoming replication from other Cores.
- If you ran the configuration script before you attached storage, or if you later attach additional storage, the easiest way to format the virtual disk and add it to your repository is to run the configuration script again. For more information, see Running the Core configuration script from the VM desktop
- You can also add storage locations from the Rapid Recovery Core Console. For more information, see the *Rapid Recovery User Guide* topic Managing a DVM repository, including the topic Adding a storage location to an existing DVM repository.
- If you want to include full recovery point chains in your replicated target Core, you must seed the data on the target Core. See Considerations for seeding data to your target Core.
- For information about using the Quick Start Guide, see the *Rapid Recovery User Guide* topic Understanding the Quick Start Guide.
- For general information about replication, see the *Rapid Recovery User Guide* topic Replication.

  For information about configuring replication, see the *Rapid Recovery User Guide* topics Configuring replication and Replicating to a self-managed target core.

Considerations for seeding data to your target Core

Once you start replicating to your target Core VM, any new recovery points saved to your source Core are replicated on your VM in the Azure cloud.

For more information on replication in Rapid Recovery, see the *Rapid Recovery User Guide,* including the parent topic Replication and the topic Replication with Rapid Recovery.

If your source Core captured one or more base image backups before you started replicating to the Azure VM, you may have incomplete recovery point chains in your target Core. Until all backup data from the source Core is transmitted to the target Core, creating full recovery point chains from the orphans, you can only perform file-level restore.

For more information on recovery point chains and orphans, see the *Rapid Recovery User Guide* topics Recovery point chains and orphans and When replication begins.

If you want your replicated target Core to have access to data saved previously on the original source Core, seed your target Core. The process of seeding unites each incremental backup with its base image, repairs the orphaned data with full recovery point chains. There are two approaches to seeding:

1. You can seed to the target Core over a network connection.

   For large data or slow connections, seeding by this method can take a substantial amount of time.
2. You can also create a seed drive from the source Core, saving backup data to external media and then transferring the initial data to the target Core.

If you do not need to seed data (for example, if you capture a base image after starting replication, and don't need access to earlier data), then replication can be completed entirely from the source Core.

To help decide which seeding approach is more appropriate, see the *Rapid Recovery User Guide* topics Determining your seeding needs and strategy and Performance considerations for replicated data transfer.

If using a seed drive to seed data for your replication target, you must send the storage media containing the seed drive file to a Microsoft Azure data center. An Azure data center representative attaches the media, and notifies you when it is ready (typically within hours). You can then consume (or import) the seed data in your target Core.

For information and links specific to seeding for Azure, see Seeding data to Azure using the Microsoft Azure Import/Export service.

For a detailed procedure to consume the data, see the *Rapid Recovery User Guide* topic Consuming the seed drive on a target Core.

Seeding data to Azure using the Microsoft Azure Import/Export service

If seeding your data to an Azure replication target, use the Microsoft Azure Import/Export service. This service has certain prerequisite and requirements. These are documented on the Azure website, and links to some relevant articles are included below.

Following are some guidelines for seeding to Azure.

- Transfer your repository archives to one or more 3.5-inch Serial Advanced Technology Attachment (SATA) II or SATA III internal hard drives, 8TB or smaller.
- You can transfer a maximum of 80TB of data, based on Microsoft's guidelines. Microsoft charges a nominal fee per drive to seed your data. For current pricing, see the Azure website or contact an Azure representative.
- You must have an existing Azure subscription and one or more Classic storage accounts to use the Azure Import/Export service.

Since Microsoft can change prerequisites, requirements, costs, and so on, always verify this information.

For more information, including specific articles regarding pricing and procedure for using the Microsoft Azure Import/Export service, see Microsoft Azure documentation.

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit https://www.quest.com/company/contact-us.aspx or call + 1-949-754-8000.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year.

The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with our product