vSphere Recovery Agent 9.20.1008
Release Notes, March 2, 2023

---

1 OVERVIEW

The vSphere Recovery Agent (VRA) provides data protection for VMware vSphere environments. The Agent can back up and restore VMs and templates across all ESXi hosts managed by a vCenter Server, or on a single ESXi host that is not managed by vCenter Server.

1.1 Compatibility

Portal	This VRA version is supported with Portal version 9.20 or later. To specify whether to quiesce the guest file system of each VM before backing it up, you must use Portal 9.30 or later. For more information, see New Features. *Note:* This VRA version checks the public key of the Portal AMP Proxy certificate when it tries to connect to Portal. If users are hosting their own Portal, we recommend updating the Portal AMP Proxy certificate before new VRAs are registered to Portal or existing VRAs are upgraded from version 8.80 or earlier. *Note:* You cannot manage the VRA with the legacy Windows CentralControl interface.
Vault	This VRA version is supported with Vault version 8.62, 8.61 and 8.56.
Granular Restore for Microsoft Exchange and SQL	To restore items from SQL Server and Exchange database backups created using the VRA, use Granular Restore for Microsoft Exchange and SQL version 9.00 or later.

Important: Do not run another backup solution in the same vSphere environment as the VRA. Conflicts can occur between the VRA and other backup software.

1.2 Release History

Version 9.20.1008, March 2, 2023

1.3 Supported Platforms

This vSphere Recovery Agent version is supported on the following platforms:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows 10 Professional 64-bit. Rapid VM Restores and the Backup Verification Report are not supported when the VRA is installed on Windows 10, since the iSCSI Target Server feature is required but cannot be installed on Windows 10.

1.4 Supported VMware vSphere Infrastructure

1.4.1 VMware vSphere

The following product versions are supported when the VRA protects all ESXi hosts managed by a vCenter Server:

vCenter Server:

- vCenter Server Appliance 8.0b (Build number: 21216066)
- vCenter Server Appliance 7.0 - up to Update 3k (Build number: 21290409)
- vCenter Server 6.7 - up to Update 3s (Build number: 20540798)
- vCenter Server Appliance 6.7 - up to Update 3s (Build number: 20540798)
- vCenter Server 6.5 - up to Update 3u (Build number: 20510539)
- vCenter Server Appliance 6.5 - up to Update 3u (Build number: 20510539)

ESXi Hosts:

- ESXi 8.0b (Build number: 21203435)
- ESXi 7.0 - up to Update 3k (Build number: 21313628)
- ESXi 6.7 - up to Update 3b (Build number: 15160138) with P08 ESXi670-202210001 (Build number: 20497097)
- ESXi 6.5 - up to Update 3a (Build number: 14320405) with P09 ESXi650-202210001 (Build number: 20502893)

vSAN:

- vSAN 8.0 (Build number: 20513097)
- vSAN 7.0 - up to Update 3i. Provided with ESXi 7.0 Update 3i (Build number: 20842708).
- vSAN 6.7 - up to EP23. Provided with ESXi 6.7 EP23 (Build number: 19195723).
- vSAN 6.6.1 - up to P06 (6.5 U3n). Provided with ESXi 6.5 Patch 06 (Build number: 17557206).

1.4.2 ESXi hosts not managed by vCenter Server

The following ESXi versions are supported when the VRA protects a single ESXi host that is not managed by vCenter Server:

- ESXi 8.0b (Build number: 21203435)
- ESXi 7.0 - up to Update 3k (Build number: 21313628)
- ESXi 6.7 - up to Update 3b (Build number: 15160138) with P08 ESXi670-202210001 (Build number: 20497097)
- ESXi 6.5 - up to Update 3a (Build number: 14320405) with P09 ESXi650-202210001 (Build number: 20502893)

Note: The VRA is not supported with the free vSphere Hypervisor.

1.4.3 Raw Device Mappings

The VRA backs up virtual disks which use virtual Raw Device Mapping (vRDM). Data backed up from a vRDM is restored as a VMDK. See VMware documentation for instructions on how to migrate a restored VMDK back to a vRDM.

When backing up VMs, the VRA skips physical Raw Device Mapping (pRDM), shared disks and independent disks. VMware does not allow these disks to be included in snapshots for VM-level backups. To back up these disks, you can install an Agent on the VM.

If a VM contains at least one disk that can be protected, the VM will be backed up.

1.5 Supported Windows File Systems for File and Folder Recovery

For file and folder recovery, the vSphere Recovery Agent currently supports the following Windows file systems:

- ReFS
- NTFS
- FAT
- FAT32

- Dynamic disks

Note: GPT partitions are supported for file and folder recovery, if they contain a supported file system.

1.6 Supported Applications for Application-consistent Backups

The vSphere Recovery Agent can perform application-consistent backups of the following Microsoft applications on Windows virtual machines:

- SQL Server 2022, 2019, 2017, 2016, 2014, 2012
- SharePoint Server 2019, 2016, 2013, 2010
- Exchange Server 2019, 2016, 2013, 2010
- Active Directory 2019, 2016, 2012 R2, 2012

As part of an application-consistent backup, the vSphere Recovery Agent can truncate SQL Server, Exchange and SharePoint transaction logs on VMs.

Note: The Agent can truncate logs for default SQL Server instances, but not for named SQL Server instances.

Note: Granular restore might not be supported with some SQL Server and Exchange versions. For supported application versions, please see the Granular Restore for Microsoft Exchange and SQL Release Notes.

---

2 NEW FEATURES

Specify whether to quiesce guest file systems when backing up VMs

When creating or editing a vSphere backup job using Portal 9.30 and VRA 9.20, you can specify whether to quiesce the file system of each VM before backing it up. Quiescing the file system on a VM brings the data into a consistent state that is suitable for backups.

Trying to quiesce a guest file system that cannot be quiesced can take significant time and resources and cause the VM to become unresponsive. When backing up VMs that cannot be quiesced, turning off guest file system quiescing can save backup time and system resources.

Note: Beginning with Portal 9.30 and VRA 9.20, the application-consistent option can only be enabled in a backup job if the guest file system quiescing option is enabled.

Backup verification log improvements

You can now view backup verification logs in Portal 9.30. Verification logs show the backup verification status of each VM in a job and the reason for any verification failure. Previously, you could only see backup verification results in Portal in the Backup Verification Report.

After a backup where VMs are verified, backup verification information for each VM in the job is incorporated into one VERIFYSAFESET log. When backups were verified using VRA 9.1*x* or 9.00, a MNT log for each VM remained in the job folder.

Note: If MNT logs from a previous VRA version remain in a job folder, you must delete the MNT logs manually. To preserve log information, you can save copies of the logs in another location before deleting the logs.

Security enhancements

Security enhancements have been added in this VRA version.

---

3 INSTALLATION REQUIREMENTS

Install VRA on a Windows physical or virtual machine that has:

- At least two CPUs.
- At least 4 GB of RAM.
- A minimum of 200 GB of free disk space. This ensures that there is sufficient space for the Agent and for files that the Agent generates during backups.
- Windows updates installed.
- Power management disabled.
- Access to the vCenter or ESXi host that you want to protect. For best performance, install VRA on a machine in the same subnet as the vCenter or ESXi host.

An account with full Administrator rights to the Windows machine is required for installing the VRA.

An account that is mapped to the Administrator role is required to connect to the vCenter and configure the VRA.

We recommend using firewalls or other mechanisms to isolate VRA and the vCenter from the Internet.

3.1 Feature-specific Requirements

3.1.1 Requirement for guest file system quiescing

To quiesce the guest file system of a VM before backing it up, VMware Tools version 11 or later must be installed on the VM.

3.1.2 Application-consistent Backup Requirements

To create application-consistent backups on a VM, VMware Tools version 11 or later must be installed on the VM.

Application-consistent backups are supported on VMs with hardware version 8 or later.

As part of an application-consistent backup, the VRA can truncate SQL Server, Exchange and SharePoint transaction logs on VMs on ESXi 8.0, 7.0, 6.7 and 6.5 hosts.

3.1.3 Rapid VM Restore and Backup Verification Requirements

The following table lists and describes requirements for Rapid VM Restores and backup verification. If VRA and Vault requirements are not met, backup verification settings do not appear for a VRA and Rapid VM Restore does not appear as a restore option in Portal. If vSphere environment requirements are not met, you can start a Rapid VM Restore but it will not finish successfully.

Note: Because the VRA uses automated Rapid VM Restore processes to verify VM backups, these features share some requirements.

Component	Rapid VM Restore requirement	Backup verification requirement

Component	Rapid VM Restore requirement	Backup verification requirement
VRA	vSphere Recovery Agent installed on a supported Windows Server platform. Windows File and Storage Services with the iSCSI Target Server feature must be installed on the server. If you install the iSCSI Target Server feature after installing VRA, you must stop and restart the VRA services (BUAgent and VVAgent) before you can perform backup verifications.	
Vault	A version 8.50 or later vault that is installed locally (i.e., not on a cloud server or in a remote datacenter). The Rapid VM Restore feature must be enabled on the vault. This feature is enabled by default on Satellite vaults. If you have a local Base vault, you can enable the Rapid VM Restore feature by running a script. See the Server Backup help or *vSphere Recovery Agent User Guide*.	
vSphere environment		
ESXi hosts	Each ESXi host must have the Software iSCSI Adapter installed and bound to a network port group that the VRA can reach. To migrate VMs restored using Rapid VM Restore to permanent storage, each ESXi host must have access to two datastores: one for writing changes while the VM runs using Rapid VM Restore, and one for permanent storage. Each datastore must have enough space for the restored VM. *Note:* On an ESXi host that is not managed by vCenter Server, Rapid VM Restore can be used to verify that VMs were backed up correctly, but cannot be used to restore VMs permanently. An ESXi server that is not part of a vCenter does not have the capabilities required to migrate VMs to permanent storage.	The ESXi host for running backup verifications must have the Software iSCSI Adapter installed and bound to a network port group that the VRA can reach. The ESXi host must be able to accommodate the expected load. During backup verification, the VRA starts each VM using an automated Rapid VM Restore process. One VM in each backup job is verified at a time and the original memory settings are used for each VM. If, for example, backup verification runs for five backup jobs at the same time and each VM uses 256 GB of RAM, backup verification could use up to 1268 GB of RAM on the host. *Note:* The ESXi host for running backup verifications is selected on the vSphere Settings tab for a VRA.
License	To migrate VMs restored using Rapid VM Restore to permanent storage, your VMware license must support storage migration.	
Datastores	We recommend using supported storage from the VMware Hardware Compatibility Guide: https://www.vmware.com/resources/compatibility/search.php	
	When you restore a VM using Rapid VM Restore, you must choose a datastore for writing changes while the VM runs using Rapid VM Restore. This datastore can be local, iSCSI or vSAN storage, but cannot be NFS storage. When you migrate a VM to permanent storage, the destination datastore can be local, iSCSI, vSAN or NFS storage.	When you enter backup verification settings, you must choose a datastore for verifying VMs. This datastore can be local, iSCSI or vSAN storage, but cannot be NFS storage.
VM		Backup verification is supported with Windows VMs. Backup verification is not supported with non-Windows operating systems (e.g., Linux). VMware Tools version 11 or later must be installed on the VM.

3.1.4 Ransomware Detection Requirements

The VRA can check for potential ransomware threats on Windows VMs when running a backup job. VMware Tools must be installed on the VMs. We recommend using the latest version of VMware Tools available.

The VRA can only check for ransomware threats on VMs that are running. The VRA cannot check for ransomware threats on VM templates.

3.2 Licensing Requirements

Each VRA claims two licenses from the Vault: a Server Agent license and a VMware plug-in license.

To migrate VMs restored using Rapid VM Restore to permanent storage, your VMware license must support storage migration.

3.3 Install/Upgrade

3.3.1 Install

The filename of the vSphere Recovery Agent installation kit is: vSphereRecoveryAgent-9-20-1008.exe

To obtain the executable file, contact your licensed service provider. For installation and configuration information, see the *vSphere Recovery Agent User Guide*.

The following files are installed for the agent:

buagent.exe – version 9.20.1008

FileScanner.exe – version 1.0.0.1

LogViewer.exe – version 9.20.1008

VV.exe – version 9.20.1008

VVAgent.exe – version 9.20.1008

XLogTranslator.exe – version 9.20.1008

dbghelp.dll – version 6.11.0001.404

evVss.dll – version 9.20.1008

InstallationCA.dll – version 9.20.1008

InstallHelper.dll – version 9.20.1008

IscsiTargetExtension.dll – version 9.20.1008

libcrypto-1_1-x64.dll – version 1.1.1q

libssl-1_1-x64.dll – version 1.1.1q

MsIscsiTargetLibrary.dll – version 9.20.1008

PluginCatBrowser.dll – version 9.20.1008

SystemStatePlugin.dll – version 9.20.1008

SystemVolumePlugin.dll – version 9.20.1008

VraRvmrExtension.dll – version 9.20.1008

vsphere-soap-generated.dll – version 9.20.1008

vsphere_utils.dll – version 9.20.1008

vSphereMount.dll – version 9.20.1008

vSphereWinPlugin.dll – version 9.20.1008

VVClMsg.dll – version 9.20.1008

You cannot install VRA on a machine where the Windows Agent is installed.

Do not install VRA on an Active Directory domain controller.

3.3.2 Upgrade

You can upgrade a VRA to version 9.20 from version 9.1*x*, 9.00, 8.8*x*, 8.60 or 8.40 by running the installation kit.

Note: If you upgrade a VRA to version 9.20 from a version earlier than 8.82, the first backup could take longer than a normal delta backup because the VRA reads all of the VM data.

---

4 FIXES, LIMITATIONS AND KNOWN ISSUES

4.1 Fixes

- Email notifications can now be sent from Portal when a vSphere backup job fails because the VRA cannot communicate with the vCenter or ESXi host. (EV-56159)

4.2 Limitations

Backup Limitations

- When backing up VMs, the VRA skips any physical Raw Device Mapping (pRDM), shared and independent disks. To back up data on these disks, you must install an Agent on the VM and use it to back up data on pRDMs and independent disks. VMware does not allow pRDM and independent disks to be included in snapshots used for VM-level backups.
- When performing an application-consistent backup, the VRA cannot truncate logs for named SQL Server instances. The VRA can truncate transaction logs for the default SQL Server instance and for all Exchange Server databases.

Restore Limitations

- If vCenter Server is running on a VM in a protected vSphere environment, the VRA cannot restore the vCenter Server VM directly to the vSphere environment. When the VRA is protecting a vCenter, VRA requires vCenter Server to run a restore.
- You can restore VMs with the VRA, but you cannot restore individual VMDKs.
- You cannot restore specific files and folders from disks that are encrypted using Bitlocker.
- You cannot restore specific files and folders from Linux VMs.
- During a granular (file and folder) restore, disks from the selected VM are mounted on the machine where the VRA is running. Files and folders on the disks are accessible to anyone on the system, including non-Admin users. If you are concerned about security, you must secure the Agent machine and prevent users from logging in to the machine locally.
- The VRA does not support file and folder restores of volumes from Windows Storage Spaces.
- The VRA does not restore disks that are attached to NVMe controllers.

- Distributed vSwitches are not restored for templates. If you back up a template connected to a distributed vSwitch and then restore the template, vCenter will report a warning for the template indicating that it is not connected to a network. In our restore log, the user will see the following message: VSPH-W-09851 dvPortgroup information not found in backup. dvSwitch will not be restored.

Rapid VM Restore Limitations

- You cannot use Rapid VM Restore to restore a VM from a backup created with vSphere Agent 7.3x. Before restoring a VM using Rapid VM Restore, you must run the backup job using vSphere Recovery Agent 8.x or later.
- Due to a vSphere limitation (https://kb.vmware.com/s/article/2149585), you cannot migrate a VM to a VMFS6 datastore in a vSphere 6.5 environment.

Installation Kit Limitations

- Repairs are not supported using the VRA installation kit. To change the Portal instance to which VRA is registered, you must uninstall the VRA and install it again.
- The VRA installation kit is only available in English. However, the VRA can be installed and is supported on non-English operating systems.

4.3 Known Issues

- If a VM is missing during a backup, the VM backup will reseed the next time the VM is present during a backup. If the VM had a potential ransomware threat before it was missing, the VM backup will be flagged as a potential threat after the backup reseeds. (EV-80399)
- If the VRA checks for potential ransomware threats during a VM backup, and the VM is busy with file copy operations or has a high I/O load, the backup can take longer than expected. However, the logs do not indicate why the backup took extra time. (EV-79865)
- The VRA does not restore disks that are attached to NVMe controllers. (EV-74308)
- When creating or editing a backup job, you might not be able to expand the list of VMs in the Include in Backup box if the VRA was upgraded from version 8.80, 8.82 or 8.83 to version 8.87 or 8.88 and then to version 9.00, 9.1*x* or 9.20.
  WORKAROUND: In Portal, go to the vSphere Settings tab of the VRA. Do not change the vSphere settings but click Verify and Save. You can then expand the list of VMs when you create or edit a job. (EV-84702)
- After you re-register a VRA to a vault, the vault network name appears as both the vault name and the network address in the VRA's vault settings in Portal.
  WORKAROUND: After you re-register a VRA to a vault, go to the VRA's vault settings in Portal and edit the vault name. (EV-85564)
- In some log messages (e.g., when a datastore does not have sufficient space for a restore), the datastore is identified by its Managed Object Browser (MOB) name (e.g., datastore-59) instead of by its friendly name or UUID. (EV-84080)
- In backup verification settings for a VRA, NFS datastores appear in the Temporary Datastore list. However, backup verifications fail if an NFS datastore is selected in this list.
  WORKAROUND: When entering backup verification settings for a VRA, select local, iSCSI or vSAN storage. (EV-74023)
- If you try to uninstall a VRA while backup verification is running, a "backup or restore is in progress" message appears and you cannot uninstall the VRA. Portal does not indicate that backup

verification is running.
WORKAROUND: Restart the VRA, or wait for the backup verification to finish. You can then uninstall the VRA. (EV-73901)

- If a backup verification process is canceled (e.g., because the backup job starts running again), the Backup Verification Report does not indicate which VMs were not verified. The report only shows the most recent backup verification that was completed for each VM. (EV-73889)
- In rare cases, if you start a VM backup while the previous backup is being verified, verification might be canceled for the new backup instead of the previous one. (EV-73792)
- If an ESXi host is part of a vCenter but lockdown mode is disabled for the host, a VRA can be registered directly to the ESXi host. However, if you use Rapid VM Restore to restore a VM and then cancel the Rapid VM Restore, the VM is marked as orphaned in the vCenter. The vCenter reports warnings because it is not aware of operations on the ESXi host.
  WORKAROUND: When an ESXi host is part of a vCenter, specify the vCenter host and credentials on the VRA's vSphere Settings tab instead of the ESXi host and credentials. (EV-70947)
  *Note:*If an ESXi host is part of a vCenter and lockdown mode is enabled for the host, you cannot register a VRA directly to the ESXi host.
- If you try to restore files and folders from a safeset that was created using the version 7.3*x* vSphere Agent, the VRA stops working and a core dump is created. This problem occurs with vSphere Recovery Agent version 8.87 or later.
  WORKAROUND: To restore files and folders from a safeset created using a version 7.3*x* vSphere Agent, please contact Support for assistance. (EV-68793, EV-68496)
- If you change the password for the account that is used to authenticate the VRA with an ESXi host, but do not specify the new password for the VRA within a short period of time (e.g., 90 minutes), the account could be locked out from the ESXi host.
  WORKAROUND: If you change the password for the account used to authenticate the VRA with an ESXi host, specify the new password for the VRA as soon as possible. If the account is locked out from the ESXi host, contact Support for assistance. (EV-52092)
- When you are restoring a VM in a vSphere 7.0 environment and the destination datastore runs out of space, a warning message appears in the restore log repeatedly but the restore does not fail for up to two hours. (EV-50800)
- You cannot restore a VM using Rapid VM Restore if the VM has a disk that is less than 8 MB in size. (EV-53265)
- If you restore a VM to a version 8.0 or 7.0 vCenter using Rapid VM Restore and start to migrate the VM to permanent storage, you cannot cancel the migration. (EV-53346)
- If you restore a VM using Rapid VM Restore, use vCenter to manually migrate the VM to another datastore and convert its disks, and then cancel the Rapid VM Restore, DRS automation is disabled for the VM.
  WORKAROUND: Use Portal to migrate a VM restored using Rapid VM Restore to permanent storage. If you have migrated a restored VM using vCenter, remove the VM manually from the VM Overrides list in the DRS configuration settings for the cluster. (EV-51053)
- An application-consistent backup cannot be created for a Windows 2019 VM that is EFI-boot, has a recovery volume and has a GPT-formatted system disk. Backups will be crash-consistent for these VMs. VMware is currently working with Microsoft support to resolve this issue.
  WORKAROUND: To allow application-consistent backups, do one of the following on each Windows 2019 VM:
    - Delete the recovery volume from the VM using the Microsoft diskpart command.

- Install Windows 2019 on an MBR-formatted disk.

  (EV-36585)

- In rare cases, particularly in vSphere 6.0 environments, application-consistent backups cannot be created for some VMs. Backups will be crash-consistent for these VMs. (EV-38818)
- NFS datastores appear in the Datastore list in Portal when you start a Rapid VM Restore. Rapid VM Restores are not supported with NFS datastores.
  WORKAROUND: When restoring a VM using Rapid VM Restore, select local, iSCSI or vSAN storage. (EV-39915)
- If you add a disk to a VM that is running using Rapid VM Restore, you cannot migrate the VM to permanent storage.
  WORKAROUND: Add the disk to the restored VM after the VM is migrated to permanent storage. (EV-38480, EV-38753)
- When performing an application-consistent backup with log truncation of a non-English SQL Server, the VRA might not be able to determine whether the logs were truncated. A warning message appears in the backup log, even though the logs may have been truncated.
- When you restore a VM that had CPU, memory and disk shares or reservations applied, these settings are not restored. (EV-39600)
- When you restore a VM that had a VM storage policy, the storage policy is not restored. (EV-39599)
- If you migrate a VM running using Rapid VM Restore to permanent storage without using Portal, VM overrides against storage and regular DRS are not removed when you stop the Rapid VM Restore process.
  WORKAROUND: Delete the VM overrides manually from vCenter. (EV-39127)
  RECOMMENDATION: To migrate a VM to permanent storage, use Portal rather than the vSphere Client or vSphere Web Client.
- When a VM's operating system is on a SCSI disk and the VM has a secondary IDE disk, the VM cannot boot after it is restored.
  WORKAROUND: Go into the BIOS of the restored VM and manually set the SCSI disk as the boot disk. (EV-39520)
- If the VRA stops working while a VM is running using Rapid VM Restore, the VM is not responsive and you cannot power off and delete the VM.
  WORKAROUND: From the command line of the ESXi host, kill the process that is running the VM. You can then delete the VM from disk. (EV-39059)
  RECOMMENDATION: Back up VMs while they are running using Rapid VM Restore.
- If Storage DRS moves a VM shortly after a backup begins, the backup can fail with the following message: *Failed to open vmdk "vmdkName" for reading. Information from VDDK: error code 4, message "A file was not found".* (EV-39631)
- If the VRA's VVAgent service stops running, a VM that is running using Rapid VM Restore might not be removed from the vCenter immediately.
  WORKAROUND: Either restart the BUAgent service, or wait approximately five minutes for the VM to be cleaned up. (EV-38054)
- If high availability settings are out of synch on ESXi hosts, a restore may fail if the original VM exists in the vCenter inventory.
  WORKAROUND: Disable and re-enable vSphere high availability, and then try the restore again. (EV-7350)

- If a long network disconnection (e.g., longer than several minutes) interrupts a restore, the restore may not continue when the network is reconnected. A shell of a partially-restored VM may remain in the vSphere UI.
  WORKAROUND: Manually delete the VM shell in the vSphere UI, and then restart the restore without interruption. (EV-7340, EV-23429)
- If a long network disconnection (e.g., longer than several minutes) interrupts a backup, the backup may not continue when the network is reconnected. (EV-23426)
- In some cases where network shares are mapped to drive letters on the machine where the Agent is installed, file and folder restores appear to be successful but you cannot access volumes from the VM backup. (EV-7344)
- After a granular restore, the RestoreMount folder remains on the machine where the VRA is running, but subfolders created during the granular restore may be removed. Subfolders created for a subsequent granular restore may have a new timestamp and entries. (EV-8782)
- Because VRA preserves Windows ACLs and permissions, you cannot restore files and folders where only one owner has permission to the files or folders, and that owner account does not exist on the machine where you are restoring the files and folders (EV-7343).

---

5 PRODUCT SUPPORT

5.1 Technical Support

Contact information for your provider is available through the Need Help button in Portal.

5.2 Product Updates

Product updates are available through your provider.

5.3 Documentation

The following documentation is available for vSphere Recovery Agent:

- Server Backup online help (https://onlinehelp.evault.com)
- Release notes (this document)
- User Guide