VERITAS

Increasing Ransomware Resilience with the Veritas Backup Exec Product Family

Protection, detection and recovery best practices..

White Paper | September 2021

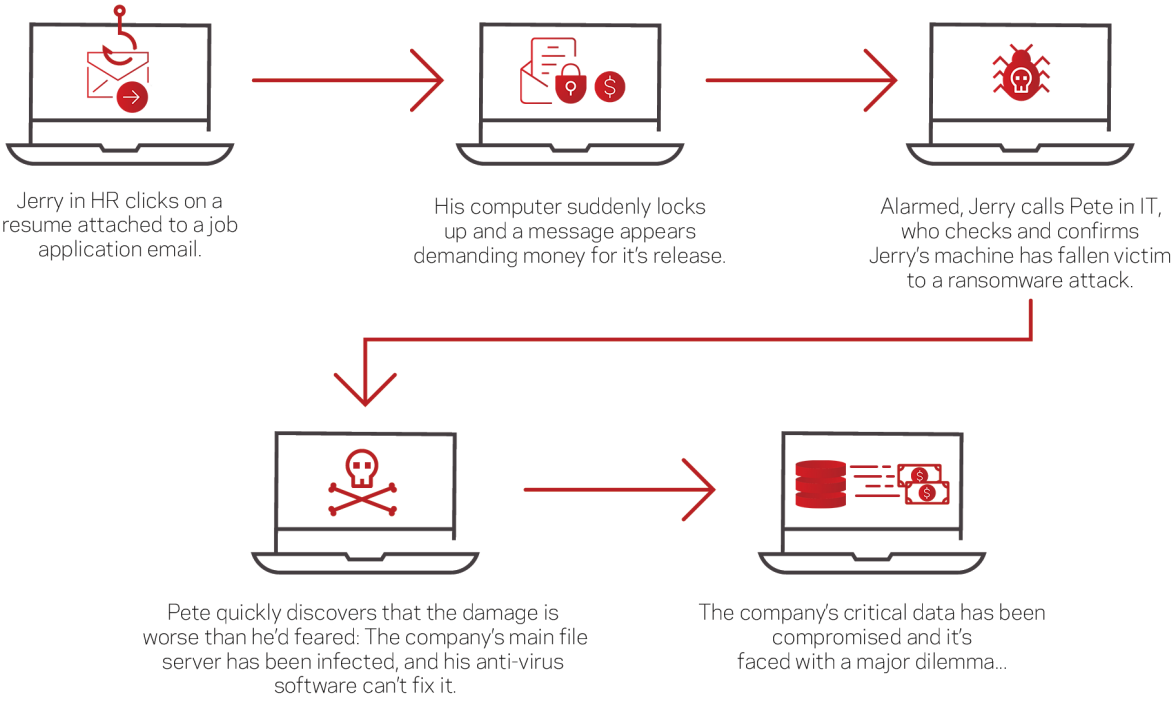
Contents

Ransomware Basics

What is ransomware?

Ransomware is a form of malware that uses a technique called cryptoviral extortion to encrypt or delete the unsuspecting user's data. Once it has encrypted the data, the malware then demands a ransom to decrypt it. Typically, those attacked pay the ransom using cryptocurrency; however, paying the ransom doesn't guarantee the cybercriminal will or even can provide a way to retrieve the data.

How does ransomware infect your environment?



Protecting Against Threats with the Backup Exec Product Family

There are proactive measures IT professionals can implement to help protect their organization's infrastructure from a ransomware attack:

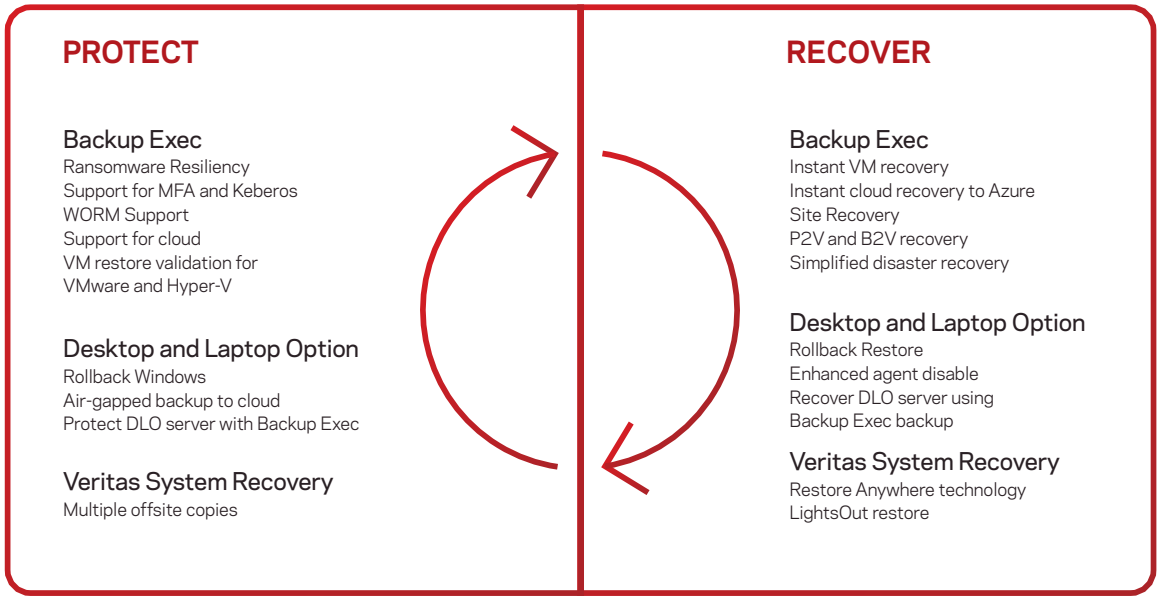
- ▪ Educate end users on the dangers of ransomware and the methods cybercriminal are using to gain access to their systems
- ▪ Install security software and keep it up-to-date
- ▪ Update operating systems to the latest patch level from the OS vendor
- ▪ Configure access controls and permissions appropriately
- ▪ Protect mission-critical systems—Industry standards follow the 3-2-1 rule: three (3) copies of data on two (2) different types of media plus at least one (1) off-site copy
- ▪ Test restore capabilities regularly
- ▪ Keep air-gapped long-term archival copies of data

Although these proactive approaches will help reduce the chances of a ransomware attack, the Veritas Backup ExecTM family of products can provide the flexibility of the 3-2-1 rule, the agility of orchestrated disaster recovery (DR) and an additional layer of protection In the event your system is impacted by ransomware, the Backup Exec family of products provides intuitive recovery options to help keep your business running with minimal downtime

	Backup Exec: ▪ Protects Windows, Linux, and Unix operating systems. ▪ Protects various application and database workloads, such as Microsoft SQL, including the ability to granularly recover items within these workloads. ▪ ▪ Protects and Instantly Recovers VMware and Hyper-V virtual machines (VMs).
	Desktop and Laptop Option: ▪ A user-centric backup solution that provides flexible implementation and centralized administration for endpoint data protection of an organization's Windows and Mac desktops and laptops.
	Veritas System Recovery ▪ Reduces complexity with a single solution that protects servers, laptops and VMs. ▪ Protects data and systems quickly, efficiently and frequently with image-based backup. ▪ Minimizes the disruption of system failure with fast, flexible and reliable recovery

Summary of Ransomware Features Available with the Backup Exec Product Family

PROTECT AND RECOVER EASILY



Backup Exec

Protect

- Ransomware Resilience—Blocks any non-Veritas process from writing to a backup disk or deduplication torage location.
- Ransomware Resilience—Added protection to the Backup Exec services, preventing malicious code injection by ransomware.
- Two-factor authentication (2FA) provides an extra layer of security when using the Remote Admin Console (RAC). Includes support for pure Kerberos environments.
- Ability to use Write Once Read Many (WORM) media.
- Validate VM for Recovery provides automated DR testing of VMware and Hyper-V VM backups.

Recover

- Instant Cloud Recovery integrates with Azure Site Recovery to provide a DRaaS with near-zero recovery point objective (RPO) and ecovery time objective (RTO).
- Instant VM Recovery provides near-zero RTO by standing-up Hyper-V and VMware VMs in a matter of minutes. Users can continue to use the system while it is migrated to the data store.
- Backup to Virtual (B2V) and Convert to Virtual (C2V) provide an additional layer of protection by having a powered-off copy available in an organization's virtual environment. In the event a physical machine is impacted by ransomware, you can power on and use this VM in a matter of minutes. You can perform this process simultaneously during the backup or after the backup complete.
- Simplified Disaster Recovery is a bare-metal recovery solution included with every install of Backup Exec so you can perform a DR of your Windows systems.

Desktop and Laptop Option

Protect

- Organizations can configure rollback windows to allow for multiple revisions across multiple days for extra protection for their endpoint machines. Doing so gives administrators the confidence that in the event of a ransomware attack, there will be a backup they can use to recover an endpoint to its previous state before the attack.
- Provides air-gapped backup to cloud storage.
- Protects a DLO management server using Backup Exec by backing up the DLO database and backup storage location.

Recover

- Rollback Restore allows recovery of an endpoint to a point in time prior to the ransomware attack as determined by the Rollback Window configuration.
- Enhanced Agent Disable lets administrators disable an endpoint once it's been determined the machine has been infected by ransomware. Once the endpoint has been disabled, the administrator can initiate a Rollback Restore to recover the infected endpoint.
- Enables recovery of a DLO management server using backups created by Backup Exec.

Veritas System Recovery

Protect

- Provides the ability for multiple off-site copies of user backups. The copies can be targeted to the cloud, network storage or removable media for an offline copy.

Recover

- Patented Restore Anywhere technology quickly restores entire physical and virtual systems from local or off-site destinations in minutes, even to bare metal, dissimilar hardware, remote locations or virtual environments.
- Patented LightsOut recovery technology allows administrators to easily recover a system from a remote location without physically visiting the system

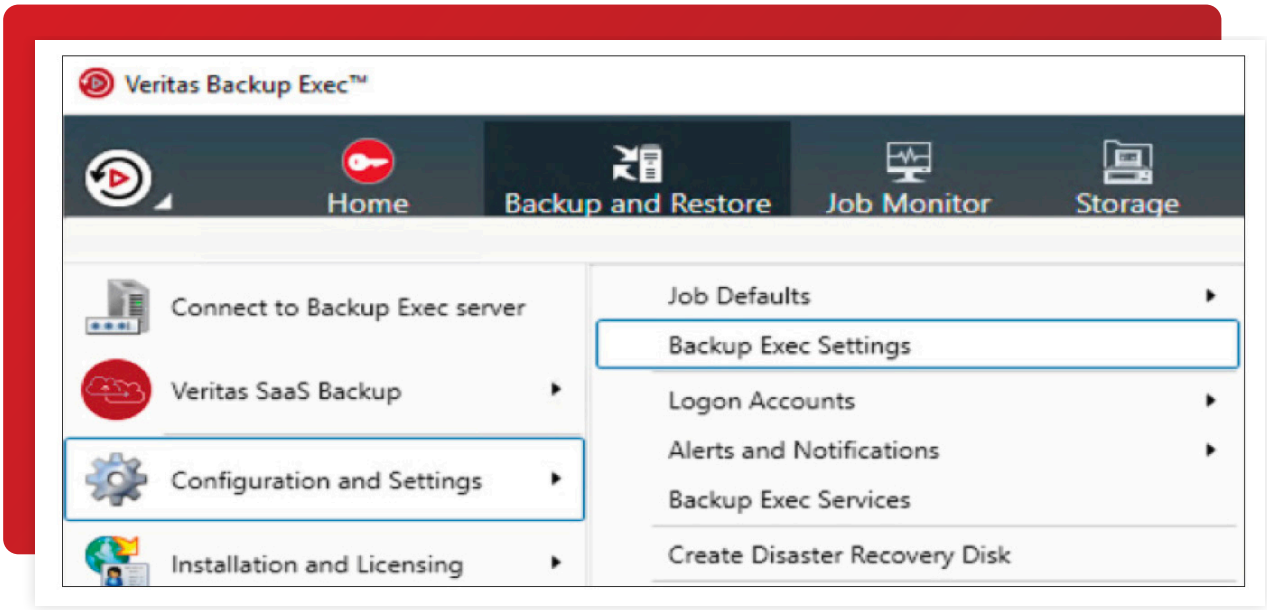
Configuring Veritas Solutions

Backup Exec: Protect

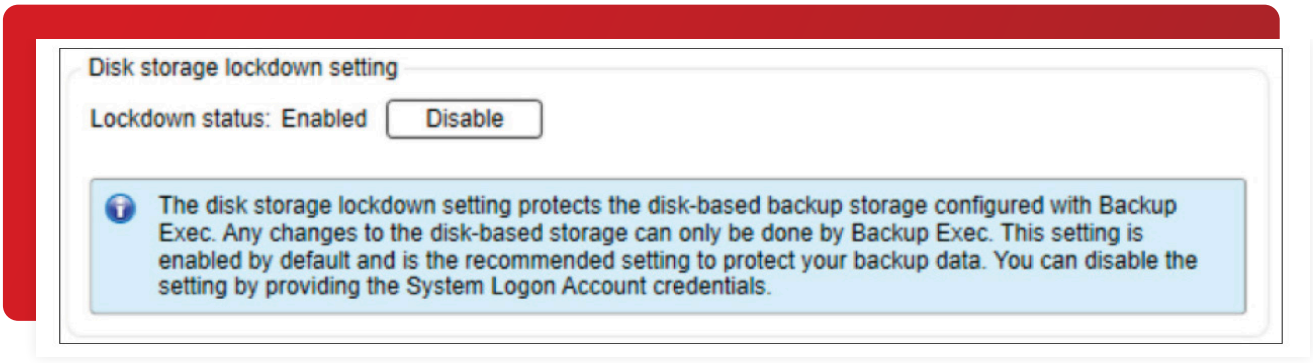
Ransomware Resilience

Ransomware resilience is enabled by default when you install Backup Exec (20.4 or later). You can configure this feature in the Backup Exec UI as follows:

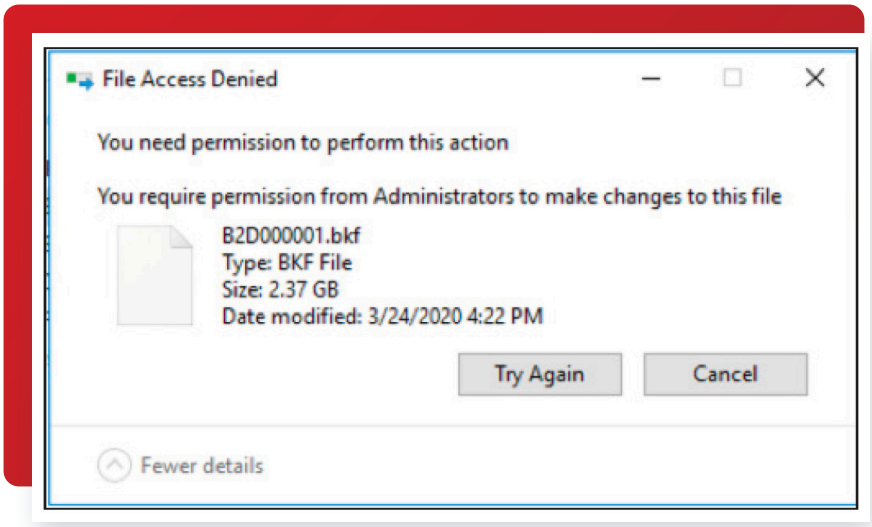
1. Click the Backup Exec button > choose Configuration and Settings > and select Backup Exec Settings



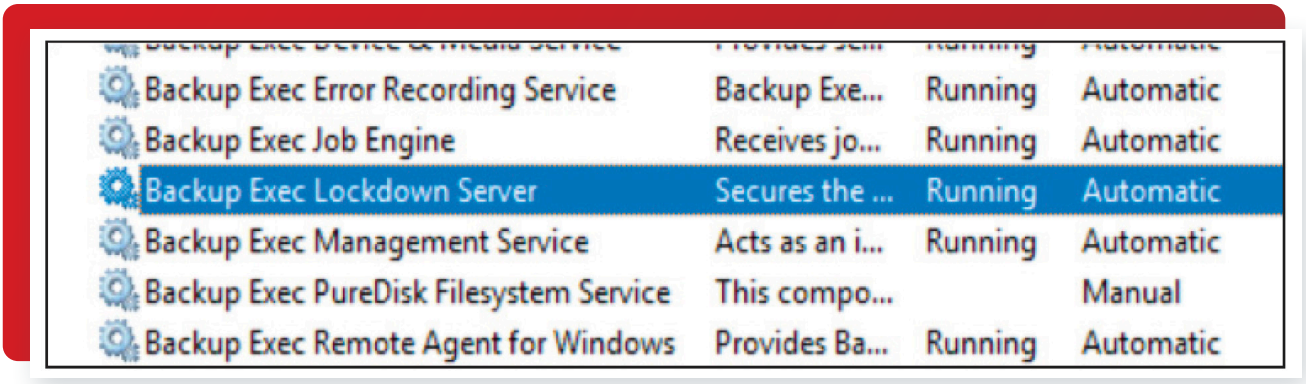
2. On the left menu, select Network and Security. Scroll down if needed and you'll see Disk storage lockdown setting, which you can enable or disable. To disable the setting, you'll be prompted for the system logon account password and the reason for disabling.



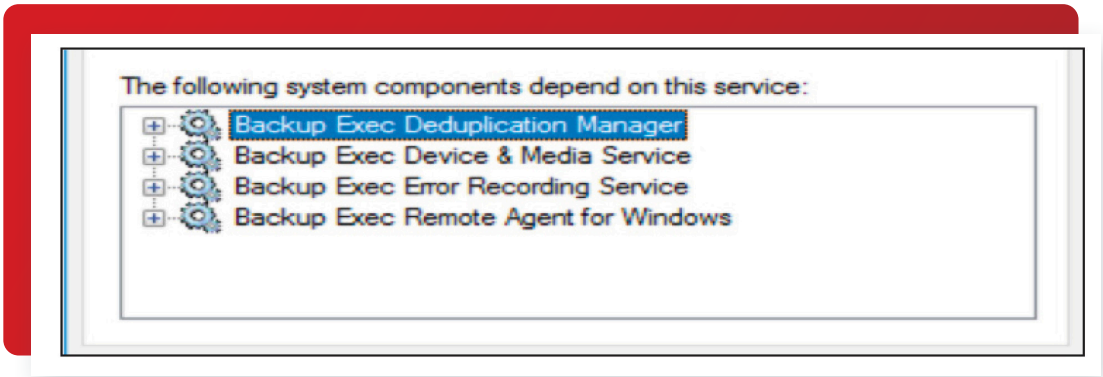
3. Any attempt to delete or modify your Backup to Disk folder will result in an error with a File Access Denied message. 1. Click the Backup Exec button > choose Configuration and Settings > and select Backup Exec Settings



4. In addition to protecting your Backup to Disk locations, the Backup Exec Lockdown Server service protects your Backup Exec services from any malicious code injection.



5. All critical Backup Exec services are dependent on this service

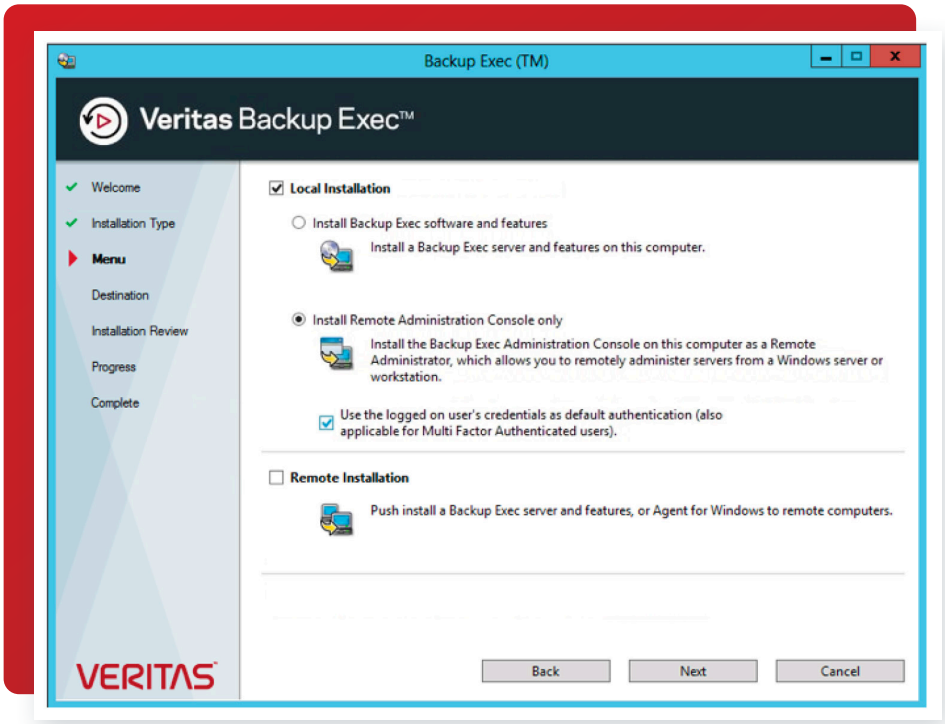


Two-Factor Authentication

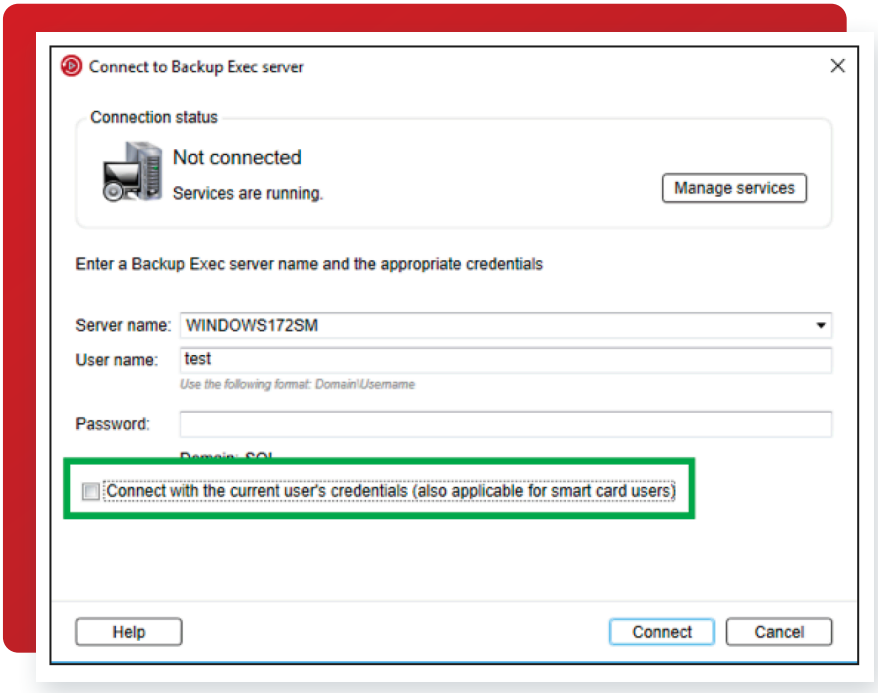
Backup Exec 21 offers the ability to configure 2FA for use with the RAC The RAC lets you manage your Backup Exec server from your workstation Backup Exec 21 supports SSO, PKI proxy-based authentication (for smart card users) and pure Kerberos environments Administrator rights are required on the Backup Exec server for the authenticating user

1. Configuring Backup Exec to use SSO and PKI proxy-based authentication:

   a. When installing the RAC on your workstation, check the box for "Use the logged-on user's credentials as default authentication (also applicable for Multi-Factor Authenticated users) "

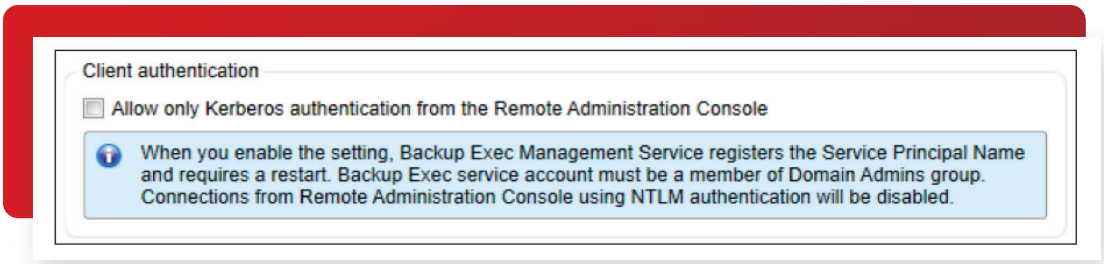


   b. You can also configure this feature after RAC install by selecting "Connect with the current user's credentials (also applicable for smart card users)" on the RAC login screen



2. Configuring Backup Exec to use Kerberos:

   a. On the Backup Exec server, click the **Backup Exec** button > **Configuration and Settings** > **Backup Exec Settings**. Select **Network and Security** on the left menu Under **Client authentication** select "Allow only Kerberos authentication from the Remote Administration Console "



   b. In Microsoft Active Directory, you'll need to create a Service Principal Name (SPN) to enable Kerberos for Backup Exec Kerberos will use the SPN for authenticating the RAC to the Backup Exec server For more information on configuring an SPN, see the Microsoft article https://docs microsoft com/en-us/windows/win32/ad/service-principal-names.

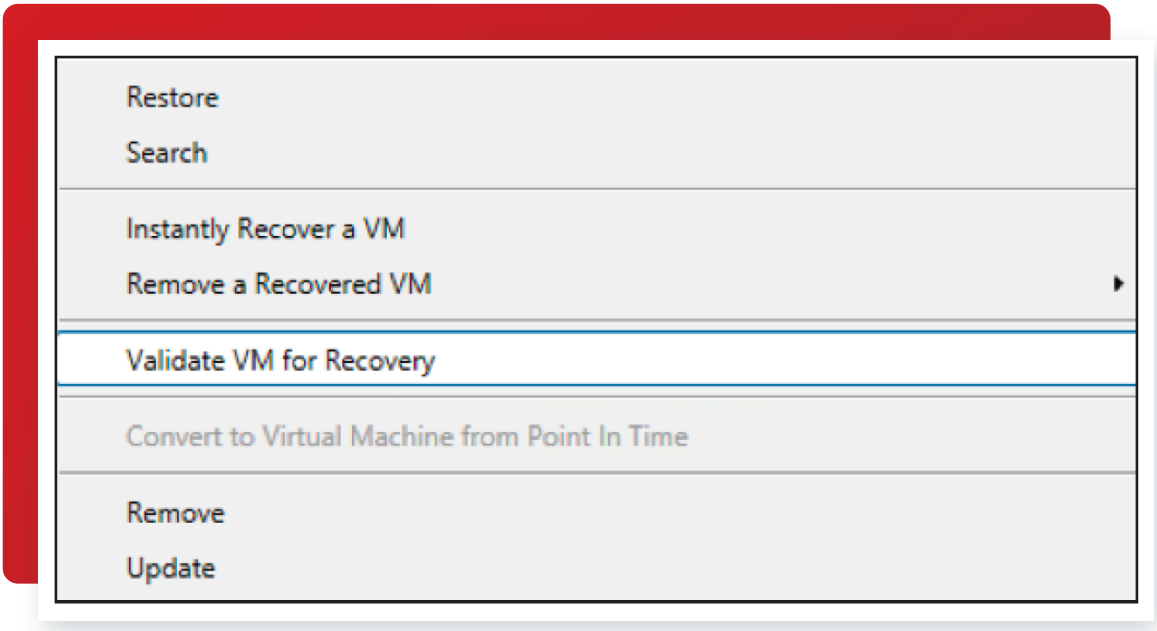
Using WORM Media in Backup Exec

Back Exec supports the ability to use WORM tape media WORM media provides an additional layer of protection for your backups that are targeted to tape by only allowing the backup application to write to the media once You don't need to configure anything in the Backup Exec UI to enable this feature For a full list of supported WORM devices, please see the Backup Exec Hardware Compatibility list

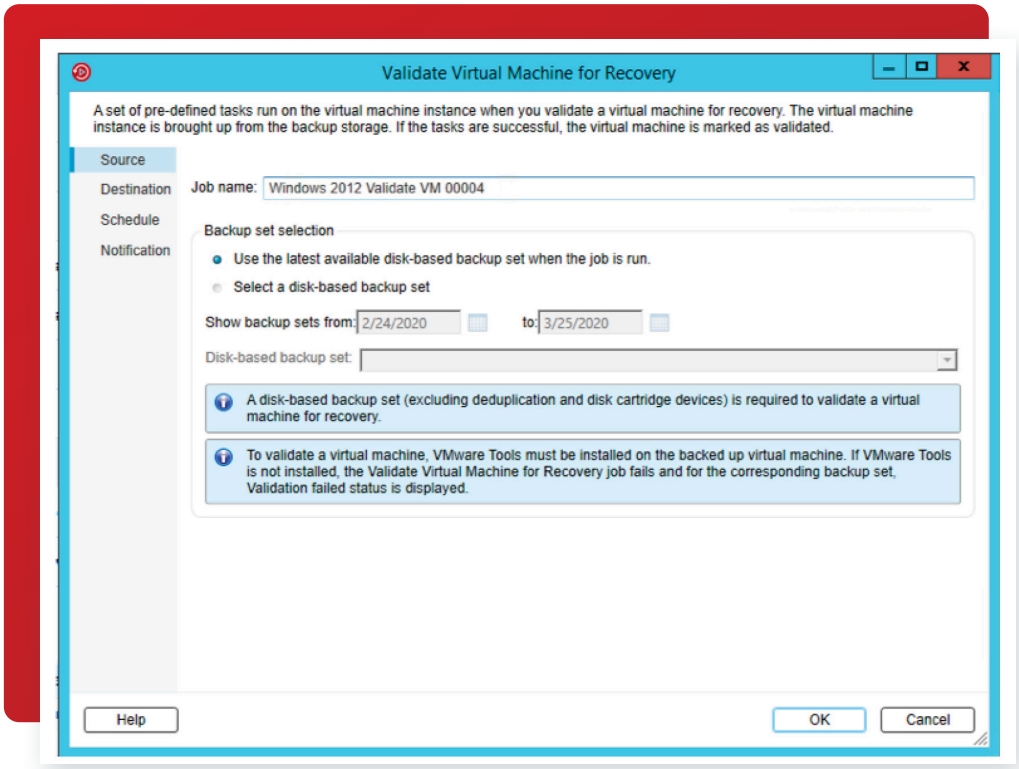
Validate VM for Recovery

Backup Exec can automatically verify that your VMware and Hyper-V VM backup can be instantly recovered to your ESX host, if needed When the configured job runs, the specified backup set is mounted on either the ESX or Hyper-V host The mounted VM is then powered on and a heartbeat check is performed to verify the VMware tools or the Hyper-V heartbeat services are running on the machine Once these checks are complete, the VM will be marked as ready for recovery This job requires the completion of a successful backup of the virtual resources

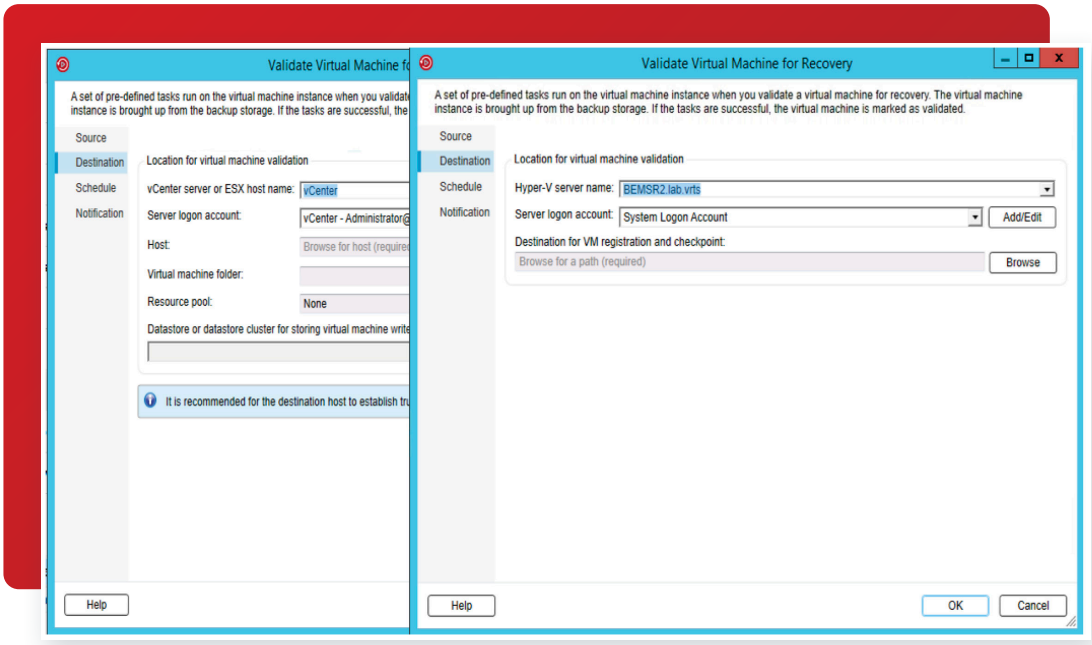
1. To configure the Validate VM for Recovery job, on the Backup and Restore tab, right-click the VM resource and select "Validate VM for Recovery"



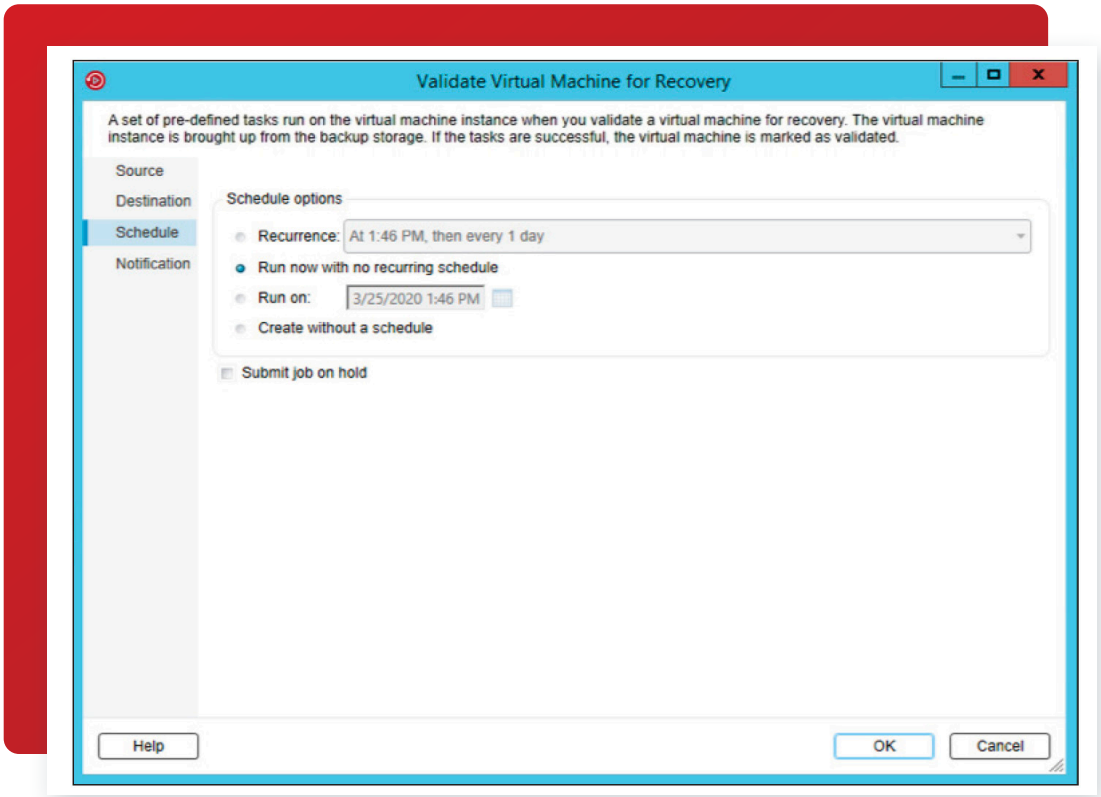
2. In the Validate VM for Recovery wizard on the **Source** tab, specify the "Job name" and the backup set to use for the validation You can select the most recent job or a set from a specific date



3. On the **Destination** tab, select the ESX or Hyper-V server from the dropdown menu you want to use for the validation.



4. On the **Schedule** tab, select the frequency with which you'd like the job to run.

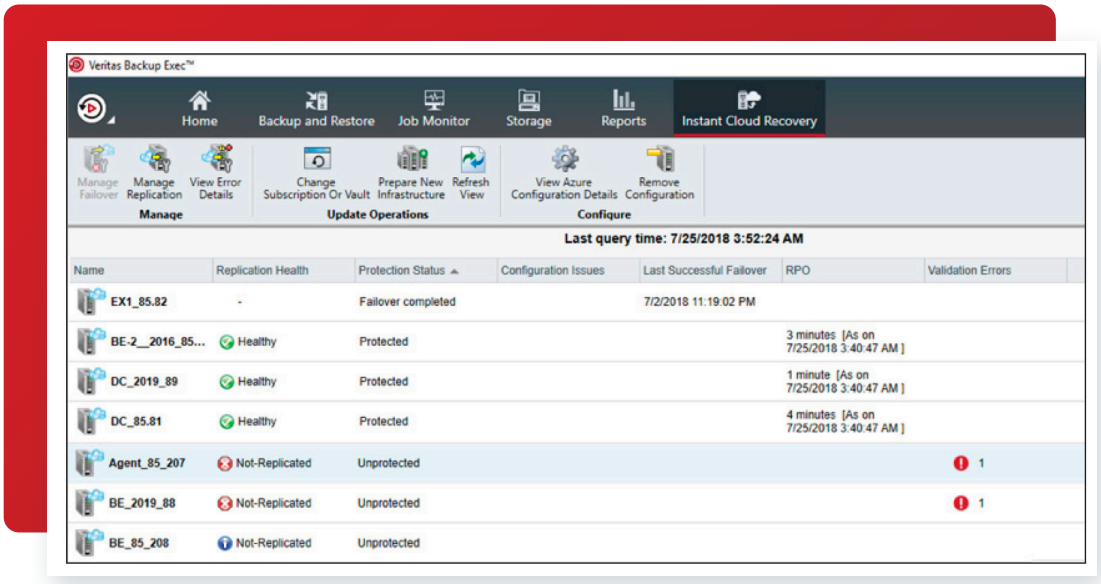


Backup Exec: Recover

Instant Cloud Recovery powered by Azure Site Recovery

With Instant Cloud Recovery, Backup Exec users can create automatically updated off-site replicas of VMs in the Azure cloud for quick failover in the event of a disaster This feature enables Backup Exec users to minimize the RPO and RTO for business-critical VM workloads Instant Cloud Recovery requires an Azure subscription and supports VMware and Hyper-V VMs

1. Backup Exec Instant Cloud Recovery provides a summary view, monitoring, replication health details and key actions directly from the Backup Exec console



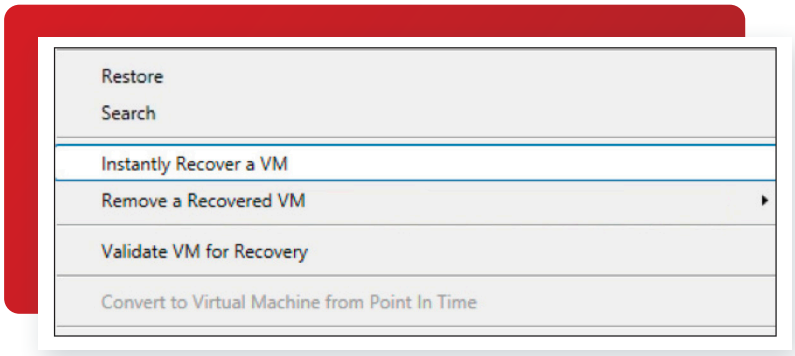
For more information on Backup Exec Instant Cloud Recovery and Azure Site Recovery, please see the following resources:

- To learn more about Backup Exec integration in the Azure Blog: https://azure.microsoft.com/en-gb/blog/azure-site-recoverypowers-veritas-backup-exec-instant-cloud-recovery-for-disaster-recovery/
- Introduction to Azure Site Recovery: https://channel9.msdn.com/Blogs/MVP-Azure/Intro-of-Azure-Site-Recovery-ASR
- See the tutorial for VMware with Azure Site Recovery: https://docs.microsoft.com/en-us/azure/site-recovery/vmware-azure-tutorial
- See the tutorial for Hyper-V with Azure Site Recovery: https://docs.microsoft.com/en-us/azure/site-recovery/hyper-v-azure-tutorial

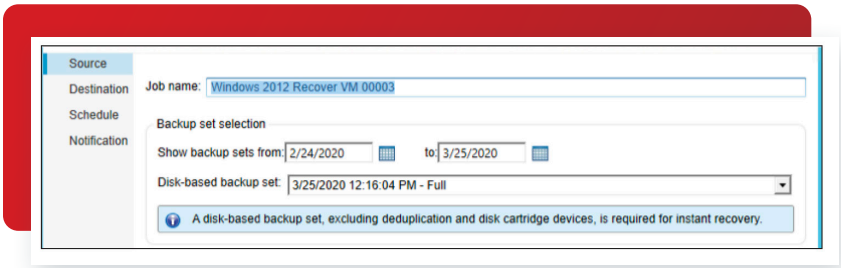
Instant Recovery of Virtual Machines

Backup Exec lets you recover a VM instantly without waiting to transfer the VM's data from a backup set Backup Exec starts the instantly recovered VM directly from the backup set, and users can access it on the VMware or Hyper-V host To fully restore the VM, use VMware Storage vMotion or Hyper-V Live Migration The VM remains available for use during the migration

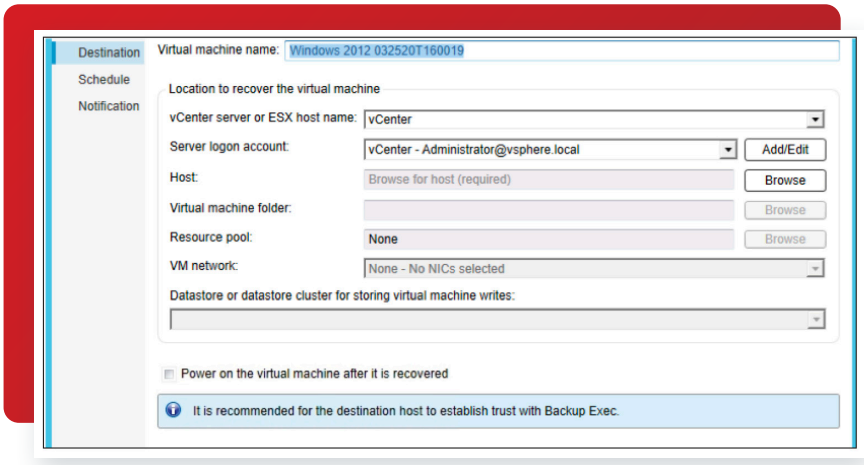
1. To use the Instantly Recovery a VM feature, select the **Backup and Restore** tab in the Backup Exec console. Right-click the VM you want to recover and select it.



2. Provide a name for the job and select the Backup to Disk source for the restore.



3. Select the Hyper-V or vCenter/ESX host for the recovered machine



4. **Schedule** the recovery

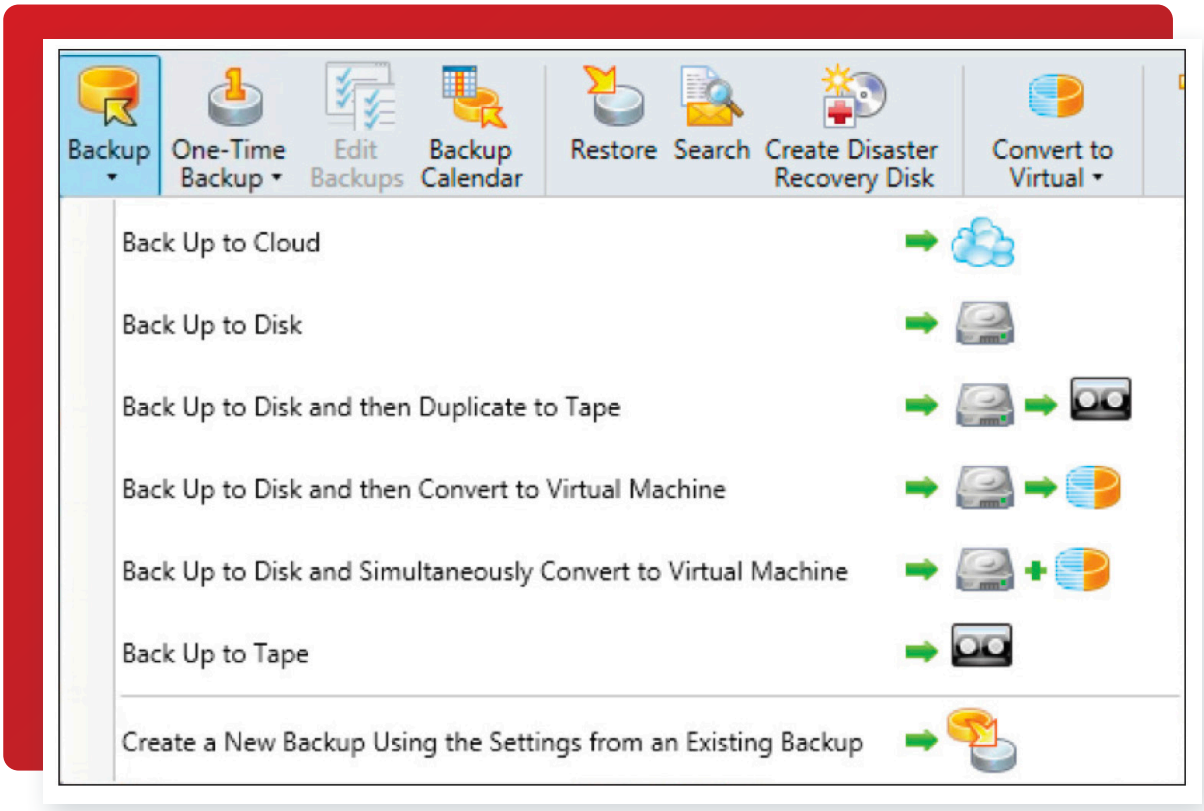
5. Once you've recovered your machine, you can now use VMware Storage vMotion or Hyper-V Live Migration to move your recovered machine to the desire datastore. For more information, please see the appropriate documentation:

- VMware Storage vMotion guide: https://docs vmware com/en/VMware-vSphere/6 5/com vmware vsphere vcenterhost doc/GUID-A15EE2F6-AAF5-40DC-98B7-0DF72E166888 html
- Hyper-V Live Migration guide: https://docs microsoft com/en-us/windows-server/virtualization/hyper-v/manage/use-live-migration-without-failover-clustering-to-move-a-virtual-machine

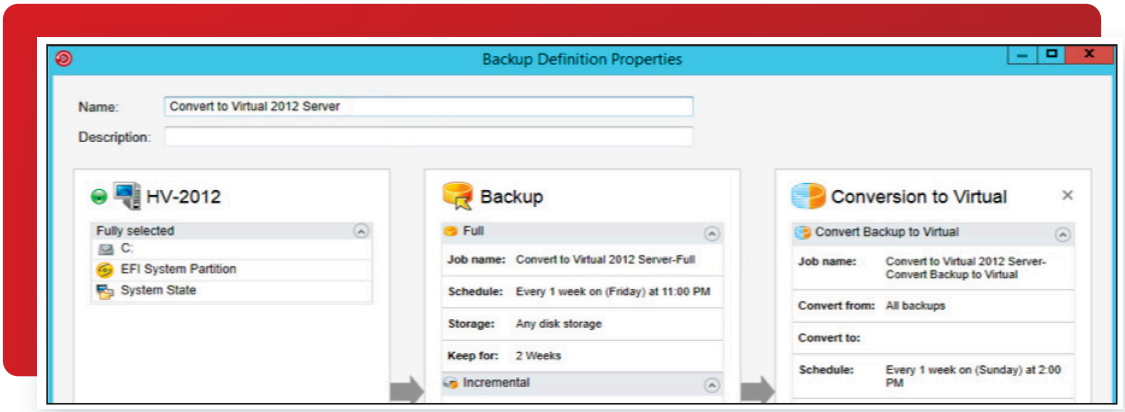
Backup to Virtual and Convert to Virtual

Backup Exec provides the ability to back up to a VM or convert an existing backup set to a VM In the event of a ransomware attack on your physical server, you can have your converted VM available with little downtime Backup to Virtual (B2V) will back up the physical server and simultaneously convert the server to a VM You can use Convert to Virtual (C2V) after you've completed a backup of your physical server You can schedule Convert to Virtual to run after the job completes or manually schedule it in a separate job

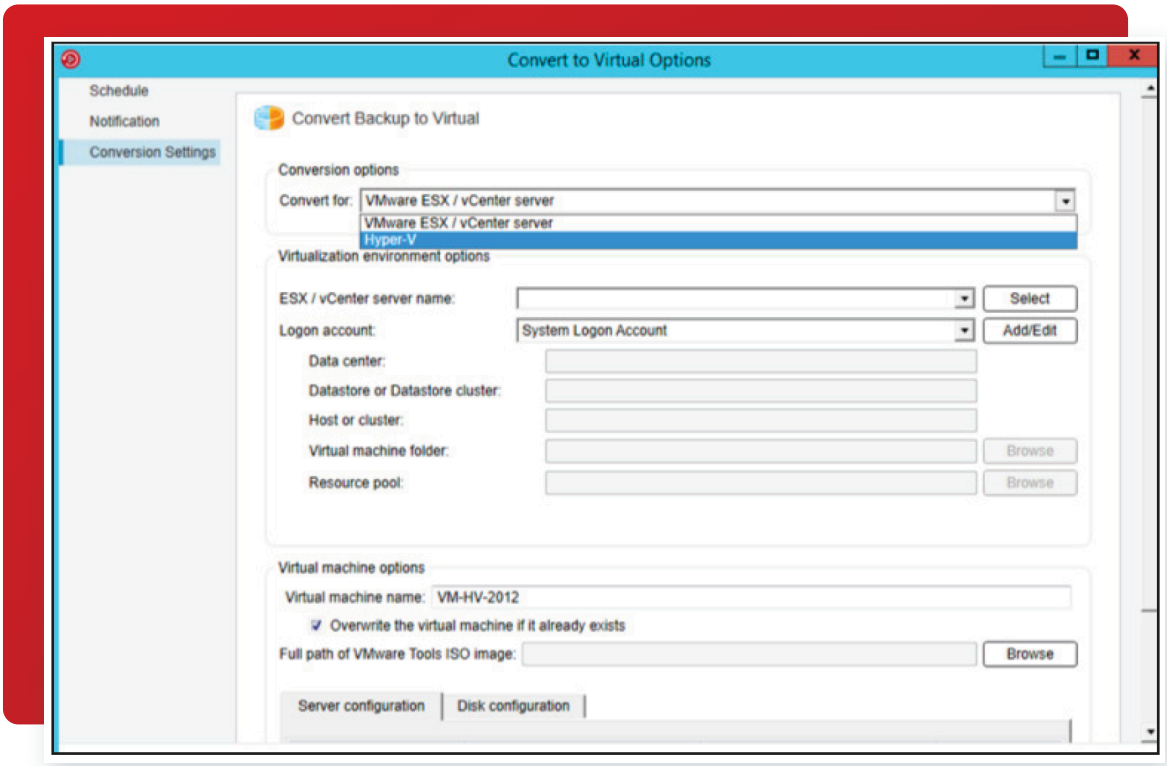
1. To configure the conversion of the physical server to a VM, click the **Backup and Restore** tab in the Backup Exec console Select the physical server you'd like to convert Click on **Backup** in the menu bar and then choose "Back Up to Disk and then Convert to Virtual Machine" or "Back Up to Disk and Simultaneously Convert to Virtual Machine "



2. In the backup wizard, verify you've selected the critical components for the conversion. The server you chose is indicated by the green icon next to the server name. Next, edit the settings of the **Conversion to Virtual** stage.



3. On the left menu, select **Conversion Settings.** Select the virtual technology you wish to use, Hyper-V or VMWare. Add the host information for the Hyper-V or VMware host. Next, complete the "Virtual machine options" section where you can change the server name, memory and disk configuration, if desired. To perform the conversion, you'll need the Hyper-V Integration Components ISO image or the VMware Tool ISO image, depending on the virtual host you're using.



Simplified Disaster Recovery

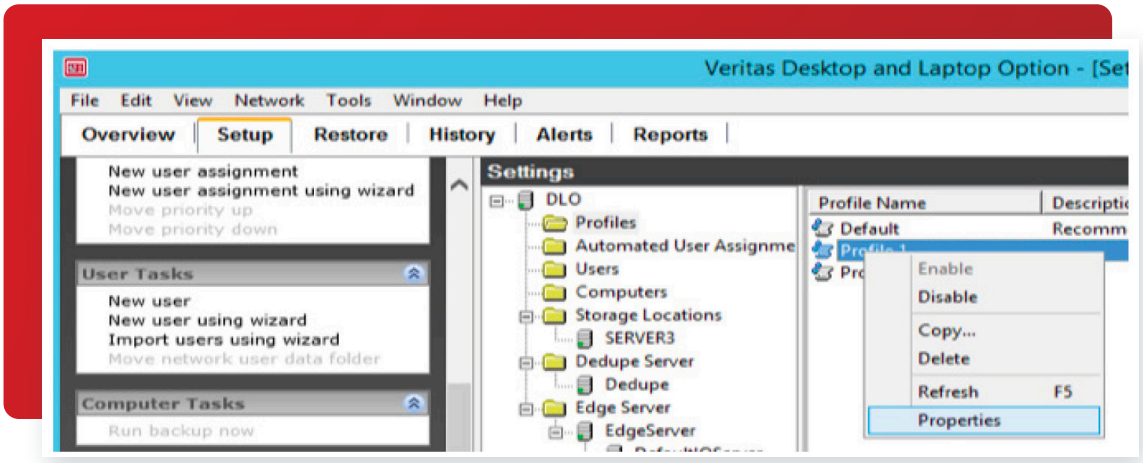
Simplified Disaster Recovery (SDR) is included with every install of Backup Exec so you can perform a DR of your Windows systems This feature requires you to protect the machine's critical resources in a single backup job After the backup is complete, use the Create Simplified Disaster Recovery Disk Wizard to create an SDR disk image for use during recovery Recovery includes a bare- metal or dissimilar hardware restore operation For more information on using SDR, please review the SDR section of the Backup Exec Administrator Guide

Desktop and Laptop Option: Protect

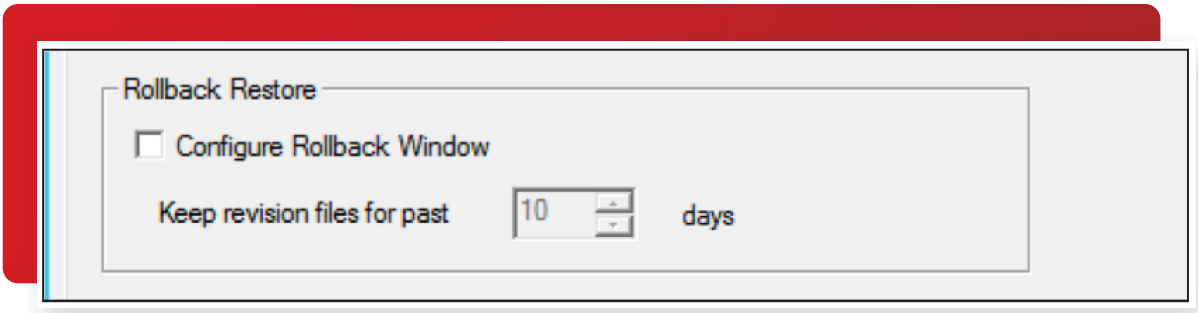
Rollback Windows

Desktop and Laptop Option 9.1 (DLO)—Introduced Rollback Windows functionality to allow administrators to manage the retention window for endpoint data. Administrators can configure the rollback window for each configured profile in the DLO.

1. To configure a rollback window, select the **Setup** tab in the DLO console. Select "Profiles" and then right-click on the name of the profile you want to modify.



2. On the **General** tab, select "Configure Rollback Window." Set the value to the desired recovery window.



Desktop and Laptop Option: Recover

Rollback Restore

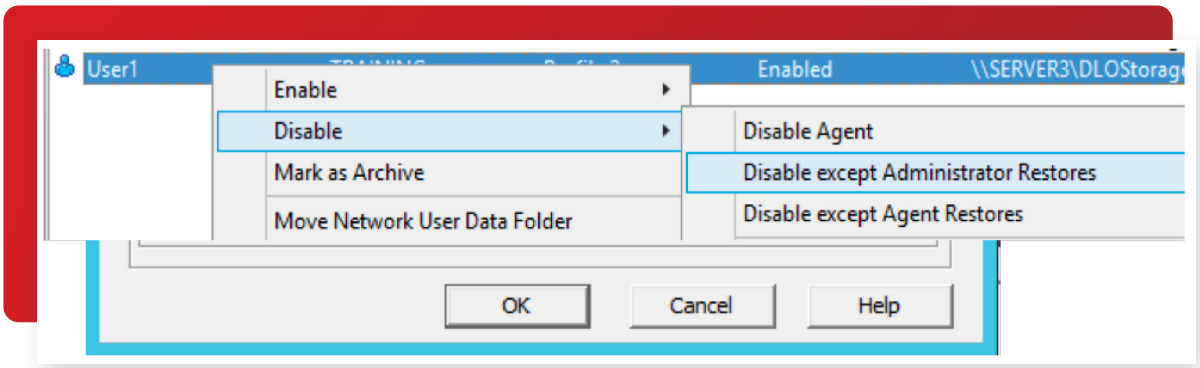
Rollback Restore lets administrators restore an endpoint to a point in time in the configured Rollback Window. The admin can configure the restore to recover to the original computer, to an alternate computer or staged to an alternate computer.

1. Select the **Restore** tab in the DLO console. Highlight the user to restore. You can select the restore option from the left menu or by right-clicking the user>select Restore>select restore method.
2. Select the option for **Rollback** restore and specify the window to recover.

Enhanced Agent Disable

In the event of a ransomware attack on an endpoint, the Desktop and Laptop Option provides an enhanced agent feature. This feature lets the administrator disable the endpoint from being included in further backup jobs until the endpoint can be recovered via a restore.

1. Select the **Setup** tab in the DLO console. Select "Users" under settings. Right-click on the desired user>select **Disable**>select "Disable except Administrator Restore."



Veritas System Recovery: Protect

Offsite Copy

Veritas System Recovery gives administrators the ability to have multiple offsite copies of a server backup Admins can configure this feature when defining a new backup job or can edit an existing job to enable an offsite copy.

This feature can copy your organization's latest complete recovery point to the following:

- A portable storage device
- ▪ A remote server in your network
- ▪ A remote FTP server
- ▪ Amazon S3 storage
- ▪ Microsoft Azure storage

Regardless of the method you use, storing copies of your recovery points at a remote location provides a crucial level of redundancy if your server is impacted by ransomware The Offsite Copy feature can double your data protection by ensuring you have a remote copy.

When you enable Offsite Copy, you specify up to two offsite copy destinations After the backup job finishes creating recovery points, Offsite Copy verifies that at least one of the offsite copy destinations is available Offsite Copy then begins copying the new recovery points to the offsite copy destinations.

Veritas System Recovery: Recover

Restore Anywhere Technology

Veritas System Recovery features the patented Restore Anywhere Technology, which enables you to quickly restore entire physical and virtual systems from local or off-site destinations in minutes, even to dissimilar hardware, remote locations or virtual environments Once you've created a recovery point for your server or endpoint, you'll need to use the System Recovery Disk Creation Utility to create a System Recovery Disk for use during the restore process in the event of a ransomware attack For more information on recovering a server or endpoint, please review the "Recovering a Computer" section of the Veritas System Recovery Administration Guide

LightsOut Restore

Veritas System Recovery includes the patented LightsOut Restore feature that allows you to recover a server remotely using your existing remote management utility It works regardless of the state of the computer, provided its file system is still intact LightsOut Restore installs a custom version of the Veritas System Recovery Disk directly to the file system on the system partition It then places a Veritas System Recovery Disk boot option in the Windows boot menu When you select the boot menu option, the computer will boot directly into the Veritas System Recovery Disk For more information on configuring LightsOut Restore, please review the "Configuring LightsOut Restore" section of the Veritas System Recovery Administration Guide

About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact information visit:
veritas.com/company/contact

V1008 09/21