Veeam Backup and Replication Operational Guide

Volume 3

Based on Version 12

Focused on Microsoft Hyper-V

By:

Dave Kawula   Cristal Kawula

Cary Sun   Emile Cabot

PUBLISHED BY

MVPDays Publishing
http://www.mvpdays.com

ISBN: TBD

Warning and Disclaimer

Every effort has been made to make this manual as complete and accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity concerning any loss or damages arising from the information contained in this book.

Feedback Information

We'd like to hear from you! If you have any comments about how we could improve the quality of this book, please don't hesitate to contact us by visiting www.checkyourlogs.net or emailing feedback@mvpdays.com.

Foreward

Here is another book by Dave, Cristal, Cary and Emile; what a significant milestone!

Ask yourself one question: Why? There are so many technologies, but why do we use what we use? Why do we do what we do? The answer is how. It's how we use something. I like to explain sometimes compliance in this way. No product or technology is inherently compliant. It's how it is implemented and how it is audited. The same goes for technology implementations; it's about how we use them. The how is the why.

Operations are still cool. There are so many razzle-dazzle job titles and buzzwords in the market today, but in the end, Operations are Operations. DevOps, PlatformOps, SRE (Sire Reliability Engineer), Platform Engineering... I do not need to go on, but no technology will take care of itself across all disciplines. How it is used, implemented, monitored, etc., matters today. Technology still needs humans and their knowledge.

Expert advice is the difference. We all learn from each other. When taking on the next new challenge, where does one go first? We look for resources to consume. Blogs, books like this, and social profiles; the established experts are the trusted advisors in the technology space. Call it community, social sharing, or what you want; we all find ourselves going to the go-to experts of a particular space.

Above and Beyond. What Dave, Cristal, Cary and Emile put forth in this book is outstanding in their practicing advice for technology. They could easily focus on their professional responsibilities and keep them narrow. But writing a book is hard work! Editing a book is hard work! I've not discussed this with them, but I'm sure they aren't doing it for the money of writing a book. They write this book because they go above and beyond, share, and care.

I'm sure you will enjoy this book, and a big congratulations on this book, Dave, Cristal, Cary and Emile.

Best Regards,

Rick W. Vanover Microsoft MVP, VMware vExpert, Cisco Champion
Senior Director, Product Strategy - Veeam Software
Twitter: @RickVanover

About the Authors

Dave Kawula – Microsoft MVP

Dave is a Microsoft Most Valuable Professional (MVP) with over 20 years of experience in the IT industry. His background includes data communications networks within multi-server environments, and he has led architecture teams for virtualization, System Centers, Exchange, Active Directory, and Internet gateways. Very active within the Microsoft technical and consulting teams, Dave has provided deep-dive technical knowledge and subject matter expertise on various System centers and operating system topics.

Dave is well-known as an evangelist for Microsoft, 1E, and Veeam technologies. Locating Dave is easy as he speaks at conferences and sessions each year, including TechEd, Ignite, MVP Days Community Roadshow, and VeeamOn.

Recently Dave has been honoured to take on the role of Conference Co-Chair of TechMentor and Cyber Security & Ransomware Live with fellow MVP Sami Laiho. The lineup of speakers and attendees attending this conference over the past 20 years is fantastic. Come down to Redmond or Orlando in 2018 and meet him in person. Check out his speaking site at https://sessionize.com/dave-kawula/

He recently tied for 1st place out of 1800 speakers at the Microsoft Ignite Conference in Orlando.

As the founder and Managing Principal Consultant at TriCon Elite Consulting, Dave is a leading technology expert for local customers and large international enterprises, providing optimal guidance and methodologies to achieve and maintain an efficient infrastructure.

BLOG: www.checkyourlogs.net

Twitter: @DaveKawula

Cristal Kawula – Microsoft MVP

Cristal Kawula co-founded MVPDays Community Roadshow and #MVPHour live Twitter Chat. She was also a Technical Advisory board member and the President of TriCon Elite Consulting. Cristal is the only 2nd Woman worldwide to receive the prestigious Veeam Vanguard award.

Cristal speaks at Microsoft Ignite, MVPDays, and other local user groups. In addition, she has been instrumental in founding MVPDays Publishing and has helped author over 25 + books.

At conferences like Microsoft Ignite, she has led community meetups on Women in IT, Parenting in IT, Diversity in Tech, and becoming a Community Rockstar.

BLOG: http://www.checkyourlogs.net

Twitter: @supercristal1

Cary Sun – Microsoft MVP

Cary Sun is a CISCO CERTIFIED INTERNETWORK EXPERT (CCIE No.4531) and MCSE, MCIPT, Citrix CCA with over twenty years in the planning, design, and implementation of network technologies and Management and system integration. Background includes hands-on experience with multi-platform, all LAN/WAN topologies, network administration, E-mail and Internet systems, security products, PCs and Servers environment. Expertise is analyzing users' needs and coordinating system designs from concept through implementation. Exceptional analysis, organization, communication, and interpersonal skills. Demonstrated ability to work independently or as an integral part of a team to achieve objectives and goals. Specialties: CCIE /CCNA / MCSE / MCITP / MCTS / MCSA / Solution Expert / CCA

Cary is a very active blogger at checkyourlogs.net and is permanently available online for questions from the community. His passion for technology is contagious, improving everyone around him at what they do.

Blog: https://www.checkyourlogs.net

Twitter:@SifuSun

Emile Cabot – Microsoft MVP

Emile started in the industry during the mid-90s working at an ISP and designing celebrity websites. He has a solid operational background specializing in Systems Management and collaboration solutions. In addition, he has spent many years performing infrastructure analyses and solution implementations for organizations ranging from 20 to over 200,000 employees. Coupling his wealth of experience with a small partner network, Emile works very closely with TriCon Elite, 1E, and Veeam to deliver low-cost solutions with minimal infrastructure requirements.

He actively volunteers as a member of the Canadian Ski Patrol, providing over 250 hours each year for first aid services and public education at Castle Mountain Resort and in the community.

BLOG: http://www.checkyourlogs.net

Twitter: @ecabot

Contents

Introduction

This book aims to showcase the fantastic expertise of our guest speakers of MVPDays Online. They have so much passion, expertise, and expert knowledge that it only seemed fitting to write it down in a book.

This book aims to show how to be operationally proficient using Veeam Backup and Replication, Veeam One and various other Veeam products and tools. We hope you find immense value in reviewing this guide and encourage you to share your operational knowledge and skills with others in the community.

Sample Files

All sample files for this book can be downloaded from http://www.checkyourlogs.net and www.github.com/mvpdays

Additional Resources

In addition to all the tips and tricks provided in this book, you can find extra resources like articles and video recordings on our blog http://www.checkyourlogs.net

Chapter 1

Prerequisites

This chapter will go over the system and port requirements. Before installing the Veeam Backup and Replication, all conditions must be met.

System Requirements

Before installing Veeam Backup and Replication, please ensure the virtual environment and servers meet system requirements.

Veeam Back and Replication Manager Server

Please ensure the server meets the following system requirements for the Veeam backup and replication manager server.

Components	Description
OS Platform	Windows Server 2022, 2019, 2016, 2012 R2, 2012, 11 (version21H2, 22H2), 10 (from version 1909 to version 22H2), 10 LTS (versions LTSB 1607, LTSC 1809, LTSC 2021)
OS Features	.NET Framework 4.7.2 or later, Windows Installer 4.5, PowerShell 5.1, SQL Server Management Objects, SQL Server System CLR Types, Report Viewer Redistributable 2015, Universal C Runtime, Firefox, Google Chrome, Microsoft Edge, RDP client version 7.0 or later. Option- Microsoft System Center Virtual Machine Manager 2019, 1807, 1801, Microsoft System Center 2016 Virtual Machine Manager Admin UI, Microsoft System Center 2012 R2 Virtual Machine Manager Admin UI, Microsoft

	System Center 2012 SP1 Virtual Machine Manager Admin UI.
Database	Microsoft SQL Server 2022, 2019, 2017, 2016, 2014, 2012

Veeam Backup and Replication Console Server

Before installing the Veeam backup and replication console server, please ensure the server meets the system requirements.

Components	Description
OS Platform	Windows Server 2022, 2019, 2016, 2012 R2, 2012, 11 (version21H2, 22H2), 10 (from version 1909 to version 22H2), 10 LTS (versions LTSB 1607, LTSC 1809, LTSC 2021)
OS Features	.NET Framework 4.7.2 or later, Windows Installer 4.5, PowerShell 5.1, SQL Server Management Objects, SQL Server System CLR Types, Report Viewer Redistributable 2015, Universal C Runtime, Firefox, Google Chrome, Microsoft Edge, and RDP client version 7.0 or later.

Veeam Backup and Replication Off-Host Backup Proxy Server

Please ensure the server meets the following system requirements for Veeam backup and replication off-host backup proxy server.

Components	Description
OS Platform	Windows Server 2022, 2019, 2016, 2012 R2, 2012

Veeam Backup and Replication Proxy Server for NAS Backup

Please ensure the server meets the system requirements of the Veeam backup and replication proxy server.

Components	Description
OS Platform	Windows Server 2022, 2019, 2016, 2012 R2, 2012, 11 (version21H2, 22H2), 10 (from version 1909 to version 22H2), 10 LTS (versions LTSB 1607, LTSC 1809, LTSC 2021)

Veeam Backup Repository Server

Please ensure the server meets the following Veeam backup repository server system requirements.

Components	Description
Windows OS Platform	Windows Server 2022, 2019, 2016, 2012 R2, 2012, 11 (version21H2, 22H2), 10 (from version 1909 to version 22H2), 10 LTS (versions LTSB 1607, LTSC 1809, LTSC 2021)
Linux distributions (64-bit versions)	CentOS 7.x, Debian 10.0 to 11.0, RHEL 7.0 to 9.1, Oracle Linux 7 (UEK3) to 9 (UEK R7), Oracle Linux 7 to 9 (RHCK), RHEL 7.0 to 9.1, SLES 12 SP4 or later, 15 SP1 or later, Ubuntu: 18.04 LTS, 20.04 LTS, and 22.04 LTS
Linux distributions (advanced XFS integration (fast clone))	Debian 10.x, and 11, RHEL 8.2 to 9.1, SLES 15 SP2, SP3, SP4, Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS

Veeam Tape Server

Please ensure the server meets the following system requirements for the Veeam Tape Server.

Components	Description

Windows OS Platform	Windows Server 2022, 2019, 2016, 2012 R2, 2012, 11 (version21H2, 22H2), 10 (from version 1909 to version 22H2), 10 LTS (versions LTSB 1607, LTSC 1809, LTSC 2021)
Linux distributions (64-bit versions)	CentOS 7.x, Debian 10.0 to 11.0, Oracle Linux 7 (UEK3) to 9 (UEK R7), Oracle Linux 7 to 9 (RHCK), RHEL 7.0 to 9.1, SLES 12 SP4 or later, 15 SP1 or later, Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS

Veeam WAN Accelerator

Please ensure the server meets the following Veeam WAN accelerator server system requirements.

Components	Description
Windows OS Platform	Windows Server 2022, 2019, 2016, 2012 R2, 2012, 11 (version21H2, 22H2), 10 (from version 1909 to version 22H2), 0 LTS (versions LTSB 1607, LTSC 1809, LTSC 2021)

Veeam Backup & Replication Gateway Server

Please ensure the server meets the following system requirements for the Veeam backup and replication gateway server.

Components	Description
Windows OS Platform	Windows Server 2022, 2019, 2016, 2012 R2, 2012, 11 (version21H2, 22H2), 10 (from version 1909 to version 22H2), 0 LTS (versions LTSB 1607, LTSC 1809, LTSC 2021)
Linux distributions	CentOS 7.x, Debian 10.0 to 11.0, Oracle Linux 7 (UEK3) to 9 (UEK R7), Oracle Linux 7 to 9 (RHCK), RHEL 7.0 to 9.1, SLES

	12 SP4 or later, 15 SP1 or later, Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS

Supported Applications

Veeam supports the following list of application-aware backups.

Components	Description
Active Directory	Windows Server 2022, 2019, 2016, 2012 R2, 2012, 2008 R2, 2008
Exchange	Exchange 2019, 2016, 2013 SP1, 2013
SharePoint	SharePoint 2022, 2019, 2016, 2013
SQL Server	SQL Server 2022 (only for Windows), 2019 (only for Windows), 2017 (only for Windows), 2016 SP2, 2014 SP3, 2012 SP4, 2008 R2 SP3, 2008 SP4
Oracle (Windows OS)	Oracle Database 11g Release 2, 12c Release 1, 12C Release 2, 18c, 19c, 21c
Oracle (Linux OS)	Oracle Database 11g Release 2, 12c Release 1, 12C Release 2, 18c, 19c, 21c
PostgreSQL	PostgreSQL 15, 14, 13, 12

Firewall Open Ports Requirements

You should only open the ports required for an application to run in a production environment. Locking an environment is required for most Cyber Security audits and best practices. The list below is the Port requirements for Veeam Backup and Replication. This list will help you securely build your environment, and these firewall rules for the required ports are automatically created when you install the Veeam Backup & Replication servers. However, some Linux distributions need to have manual firewall rules created.

Windows Servers

Windows servers require the following inbound and outbound ports opened. The inbound/outbound ports must be opened for Windows servers as Veeam backup infrastructure components or enable application-aware processing.

Sources	Target	Network Protocol	Port Number
Veeam backup & replication manager server	Windows server	TCP	445 135
Microsoft Hyper-V server or Off-host backup proxy		TCP	6160
Veeam backup repository		TCP	2500 to 3300
Veeam gateway server		TCP	6162
Veeam mount server		TCP	49152 to 65535
Veeam WAN accelerator server			
Veeam tape server			

Linux Servers

Linux servers require the following inbound and outbound ports opened. The inbound/outbound ports must be opened for Windows servers as Veeam backup infrastructure components or enable application-aware processing.

Sources	Target	Network Protocol	Port Number

Veeam backup & replication manager server	Linux servers	TCP	22
		TCP	6162
		TCP	2500 to 3300
Linux Servers	Veeam backup & replication manager server	TCP	2500 to 3300

Veeam Backup Manager Server

The Veeam Backup and Replication Servers require the following inbound and outbound ports opened.

Sources	Target	Network Protocol	Port Number
Veeam backup & replication manager server	SCVMM server	TCP	8100
	Hyper-V Host server	TCP	445 135
		TCP	6160
		TCP	6162
		TCP	6163
		TCP	2500 to 3300
		TCP	49152 to 65535
	Veeam Backup & Replication	TCP	1433

	configuration database server		
	DNS server	UDP	53
	Veeam update notification server (dev.veeam.com)	HTTPS TCP	443
	Veeam update license server (vbr.butler.veeam.com, autolk.veeam.com)	TCP	443
	SMB3 server	TCP	6160
		TCP	6162
	Veeam backup & replication manager server	TCP	9501
		TCP	6172
Management client PC		TCP	3389
REST client		TCP	9419
SCVMM		TCP	8732

Veeam Backup & Replication Console

The Veeam Backup & Replication Console application requires opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Veeam backup & replication console server	Veeam backup & replication manager server	TCP	9392
		TCP	10003
		TCP	9396
Veeam backup & replication console server	Veeam Mount server	TCP	2500 to 3300

Veeam Backup Proxy server

The Veeam Backup Proxy server requires opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Windows Hyper-V server/ Off-host backup proxy	Windows server	TCP	49152 to 65535
	SMB (CIFS) share	TCP	445 135
	NFS share	TCP, UDP	111 2049
	Veeam Gateway server	TCP UDP	49152 to 65535
Windows Hyper-V server		TCP	2500 to 3300

SMB3 server	Veeam backup proxy server (onhost or offhost)	TCP	2500 to 3300
Veeam backup & replication manager server	Offhost backup proxy	TCP	6163
	SMB3 server	TCP	6163
	Offhost file proxy	TCP	6210

Windows and Linux-based Backup Repository

The Windows and Linux-based Backup Repositories require opening the inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Veeam backup proxy server	Veeam backup repository	TCP	2500 to 3300
Veeam source backup repository	Veeam target backup repository	TCP	2500 to 3300
Veeam source backup repository	Azure Object storage repository gateway server	TCP	2500 to 3300
Veeam Backup repository/ secondary backup repository	Cache repository in NAS backup	TCP	2500 to 3300
Windows server running vPower NFS Service	Veeam backup repository gateway server as a backup repository	TCP	2500 to 3300

NFS Share Backup Repository

The NFS Share Backup Repository requires opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Veeam gateway server / Veeam backup proxy	NFS share is as a backup repository	TCP UDP	2049
		TCP UDP	111
	NFS share as a backup repository (version 3)	TCP UDP	mountd_port
		TCP UDP	statd_port
		TCP	lockd_port
		UDP	lockd_port

Windows SMB Backup Repository

The SMB Backup Repository requires opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Veeam gateway server / Veeam backup proxy	Windows SMB (CIFS) backup repository	TCP	445 135

Azure Object Storage Repository

The Azure Object Storage repository requires opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Veeam gateway server	Azure Object Storage	TCP	443
		HTTPS	xxx.blob.core.windows.net for the region of Global xxx.blob.core.chinacloudapi.cn for the region of China xxx.blob.core.cloudapi.de for the region of Germany xxx.blob.core.usgovcloudapi.net for the region of Government
		TCP	80
		HTTP	ocsp.digicert.com ocsp.msocsp.com *.d-trust.net

External Repository

The External Repository requires opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
		TCP	443

Veeam gateway server	Azure Object Storage		
		HTTPS	xxx.blob.core.windows.net for the region of Global xxx.blob.core.chinacloudapi.cn for the region of China xxx.blob.core.cloudapi.de for the region of Germany xxx.blob.core.usgovcloudapi.net for the region of Government
		TCP	80
		HTTP	ocsp.digicert.com ocsp.msocsp.com *.d-trust.net

Azure Archive Object Storage Repository

The Azure Archive Object Storage Repository requires opening the inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Veeam gateway server	Azure proxy appliance	TCP	443
		SSH	22

		HTTPS	Public/private IPv4 addresses of Azure appliance
Azure proxy appliance	Azure object storage	TCP	443
		HTTPS	xxx.blob.core.windows.net for the region of Global xxx.blob.core.chinacloudapi.cn for the region of China xxx.blob.core.cloudapi.de for the region of Germany xxx.blob.core.usgovcloudapi.net for the region of Government
		TCP	80
		HTTP	ocsp.digicert.com ocsp.msocsp.com *.d-trust.net

Veeam Gateway Server

The Veeam Gateway Server requires opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Veeam gateway server	Windows SMB (CIFS) backup repository	TCP	445 135

	NFS shares the backup repository	TCP, UDP	111, 2409

Veeam Tape Server

The Veeam Tape Server requires opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Veeam backup and replication manager server	Veeam tape server	TCP	6166
		TCP	2500 to 3300
Veeam tape server	Veeam backup and replication manager server	TCP	2500 to 3300

Veeam WAN Accelerator Server

The Veeam WAN Accelerator Server requires opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Veeam backup and replication manager server	Veeam WAN accelerator server	TCP	6160
		TCP	6162

		TCP	6164
Veeam WAN accelerator server	Veeam backup and replication manager server	TCP	2500 to 3300
	Veeam WAN accelerator server	TCP	6164
		TCP	6165

Veeam Guest Interaction Proxy with Non-Persistent Runtime Components

The Veeam Guest Interaction Proxy with non-persistent Runtime Components requires opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Veeam backup and replication manager server	VM guest Linux OS	TCP	22
	Veeam Guest interaction proxy	TCP	6190
		TCP	6290
		TCP	445
Veeam Guest interaction proxy	VM guest Windows OS	TCP	445 135
		TCP	49152 to 65535

		TCP	6167
	VM guest Linux OS	TCP	22
VM guest OS	Veeam Guest interaction proxy	TCP	2500 to 3300

Veeam Guest Interaction Proxy with Persistent Agent Components

The Veeam Guest Interaction Proxy with Persistent Agent Components requires opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Veeam Guest interaction proxy	VM guest OS	TCP	6160 11731
		TCP	6167
		TCP	6173 2500

Log Shipping Server Connections

The Log Shipping Server connections require opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
	Log shipping server	TCP	445

Veeam backup and replication manager server			135
		TCP	6160
		TCP	6162
		TCP	49152 to 65535
Log shipping server	Veeam backup repository	TCP	2500 to 3300

SQL Guest OS Connections

The SQL Server connections require opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Veeam Guest interaction proxy	SQL VM guest OS	TCP	445 135
		TCP	2500 to 3300
		TCP	6160 11731
		TCP	49152 to 65535
		TCP	6167

SQL VM guest OS	Veeam Guest interaction proxy	TCP	2500 to 3300
	Veeam backup repository	TCP	2500 to 3300
	Log shipping server	TCP	2500 to 3300

Oracle Guest OS Connections

The Oracle Server connections require opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Veeam Guest interaction proxy	Oracle VM guest OS (Microsoft Windows)	TCP	445 135
		TCP	2500 to 3300
		TCP	6160 11731
		TCP	49152 to 65535
		TCP	6167
	Oracle VM guest OS (Linux)	TCP	22
		TCP	2500 to 3300

Oracle VM guest OS	Veeam Guest interaction proxy	TCP	2500 to 3300
	Veeam backup repository	TCP	2500 to 3300
	Log shipping server	TCP	2500 to 3300

Veeam Mount Server

The Veeam Mount Server requires opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Veeam Mount server	Veeam backup and replication manager server	TCP	9401
	Veeam Backup repository	TCP	2500 to 3300
Veeam backup and replication manager server	Veeam Mount server	TCP	445
		TCP	2500 to 3300
		TCP	6160
		TCP	6162
		TCP	6170

		TCP	49152 to 65535

Veeam Helper Appliance

The Veeam Helper Appliance requires opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Veeam helper appliance	Veeam Backup repository	TCP	2500 to 3300
Veeam backup and replication manager server	Veeam helper appliance	TCP	22
		TCP	2500 to 3300
Veeam mount server	Veeam helper appliance	TCP	22
		TCP	2500 to 3300

Veeam Helper Host

The Veeam Helper Host requires opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Veeam helper host	Veeam Backup repository	TCP	2500 to 3300
	Veeam helper host	TCP	22

Veeam backup and replication manager server		TCP	2500 to 3300
		TCP	6162
Veeam mount server	Veeam helper host	TCP	22
		TCP	2500 to 3300

VM Guest OS

The VM Guest OS requires opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
VM guest OS	Veeam helper appliance	TCP	21
Veeam helper appliance	VM guest Linux or Unix OS	TCP	20
		TCP	2500 to 3300
Veeam helper host	VM guest Linux or Unix OS	TCP	2500 to 3300
Veeam backup and replication manager server	VM guest Linux or Unix OS	TCP	22
Veeam mount server	VM guest Windows OS	TCP	445 135

		TCP	6160 11731
		TCP	6173 2500
		TCP	49152 to 65535
Veeam backup and replication manager server	VM guest OS	TCP	2500 to 3300

Veeam U-AIR

The Veeam U-AIR requires opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Veeam U-AIR	Veeam Backup Enterprise manager server	TCP	9394

Application Item of Active Directory Domain Controller Restore

The Application Item of Active Directory Domain Controller Restore requires opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
		TCP	135

Veeam backup and replication manager server	Active directory VM guest OS	TCP UDP	389
		TCP	636 3268 3269
		TCP	49152 to 65535 (for Microsoft Windows server 2008 and later)

Application Item of Exchange Server Restore

The Exchange Server Restore Application Item requires opening the inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Veeam backup and replication manager server	Exchange 2003/2007 CAS Server	TCP	80 443
	Exchange 2010/2013/2016/2019 CAS Server	TCP	443

Application Item of SQL Server Restore

The SQL Server Restore Application Item requires opening the inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Veeam backup and replication manager server	SQL VM guest OS	TCP	1433 1434 and other

Azure Proxy Server

The Azure Proxy Server requires opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Veeam backup and replication manager server / Backup Repository server	Azure Proxy server	TCP	443

Azure Helper Appliance

The Azure Helper Appliance requires opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Veeam backup and replication manager server	Azure helper appliance	TCP	22

Azure Stack

Azure Stack requires opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Veeam backup and replication manager server	Azure stack	TCP	443 30024

SMTP Server

The SMTP Server requires opening the following inbound and outbound ports.

Sources	Target	Network Protocol	Port Number
Veeam backup and replication manager server	SMTP server	TCP	25

Chapter 2

Deployment

This chapter will walk you through installing and upgrading the Veeam Backup and Replication components. You must ensure that the devices meet the system requirements before installing or upgrading Veeam Backup and Replication components on the machine.

Veeam Backup and Replication v12 includes several new features and improvements, including:

- Direct-to-Object
- Direct-to-Cloud
- Immutable backups
- Hardened repository improvements
- Microsoft Azure Blob Storage immutability support
- HPE Storage immutability support
- Multi-factor authentication
- Kerberos-only authentication
- IPv6 support
- gMSA accounts for Windows
- Single-use credentials for Linux
- Automatic console lockouts
- Best practices analyzer
- Network-less discovery and deployment
- Dynamic protection scope
- in-cloud data flow

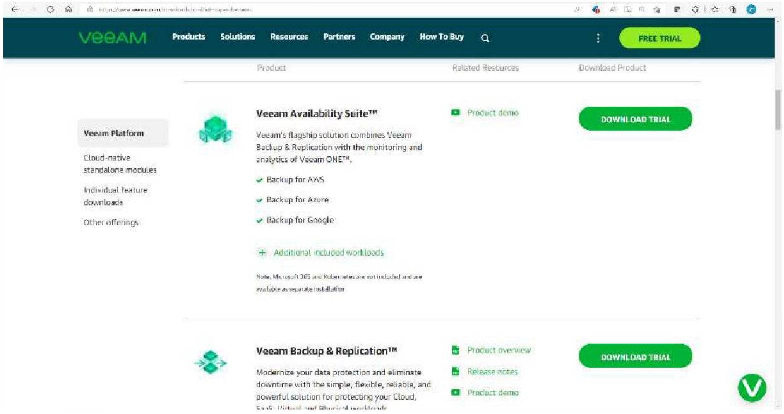
- Full portability
- PostgreSQL support for a configuration database
- VeeaMover
- Move backups between jobs
- Copy backups between repositories
- Multiple gateway server support
- Direct to archive
- Object storage as performance extent

These are only a few new features and improvements in Veeam Backup and Replication v12. Overall, the new release focuses on providing faster and more efficient backup and recovery, enhanced security, and greater flexibility and ease of management.

Install Veeam Backup and Replication v12 with PostgreSQL

When you install Veeam Backup & Replication, the Veeam Backup & Replication console is automatically installed on the backup server.

You can choose PostgreSQL as a Veeam Backup & Replication database. It has no size limit or computes restrictions and has improved performance over SQL Express.

Instructions	Screenshot (if applicable)
1. Log in to the Veeam Backup and Replication manager server. 2. Download the Veeam Backup and Replication v12 ISO image file from the Veeam website sign-in required).	

Veeam Availability Suite™

Veeam's flagship solution combines Veeam Backup & Replication with the monitoring and analytics of Veeam ONE™.

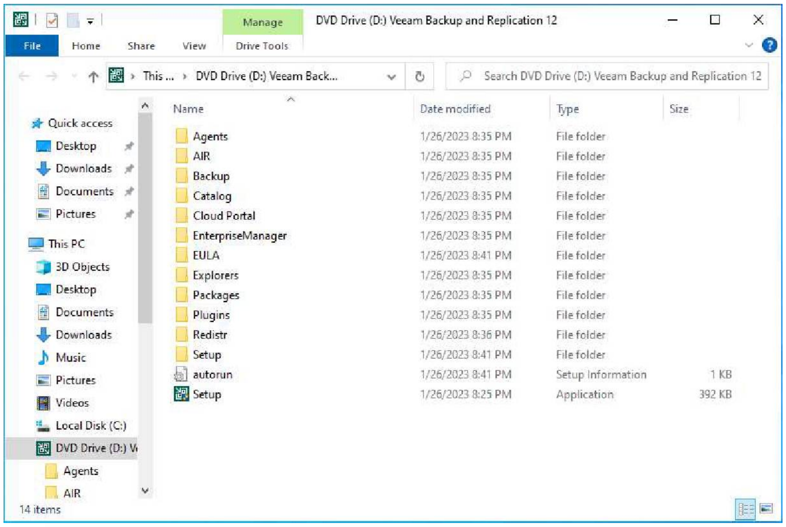
- ✓ Backup for AWS
- ✓ Backup for Azure
- ✓ Backup for Google

Note: Microsoft 365 and Kubernetes are not included and are available as separate installation

Veeam Backup & Replication™

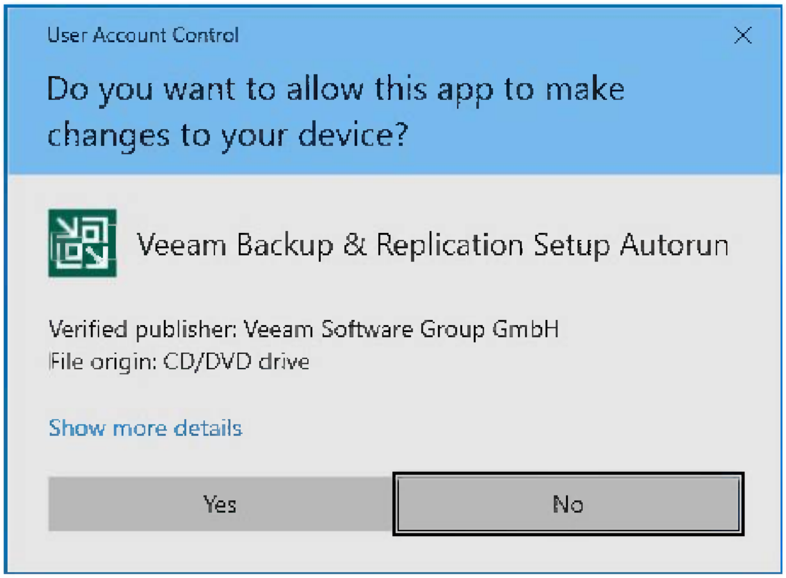
Modernize your data protection and eliminate downtime with the simple, flexible, reliable, and powerful solution for protecting your Cloud, SaaS, Virtual and Physical workloads

3. Mount the Veeam Backup and Replication v12 iso image file.
4. Run Setup.exe.



Name	Date modified	Type	Size
Agents	1/26/2023 8:35 PM	File folder	
AIR	1/26/2023 8:35 PM	File folder	
Backup	1/26/2023 8:35 PM	File folder	
Catalog	1/26/2023 8:35 PM	File folder	
Cloud Portal	1/26/2023 8:35 PM	File folder	
EnterpriseManager	1/26/2023 8:35 PM	File folder	
EULA	1/26/2023 8:41 PM	File folder	
Explorers	1/26/2023 8:35 PM	File folder	
Packages	1/26/2023 8:35 PM	File folder	
Plugins	1/26/2023 8:35 PM	File folder	
Redistr	1/26/2023 8:36 PM	File folder	
Setup	1/26/2023 8:41 PM	File folder	
autorun	1/26/2023 8:41 PM	Setup Information	1 KB
Setup	1/26/2023 8:25 PM	Application	392 KB

5. On the User Access Control page, click Yes.



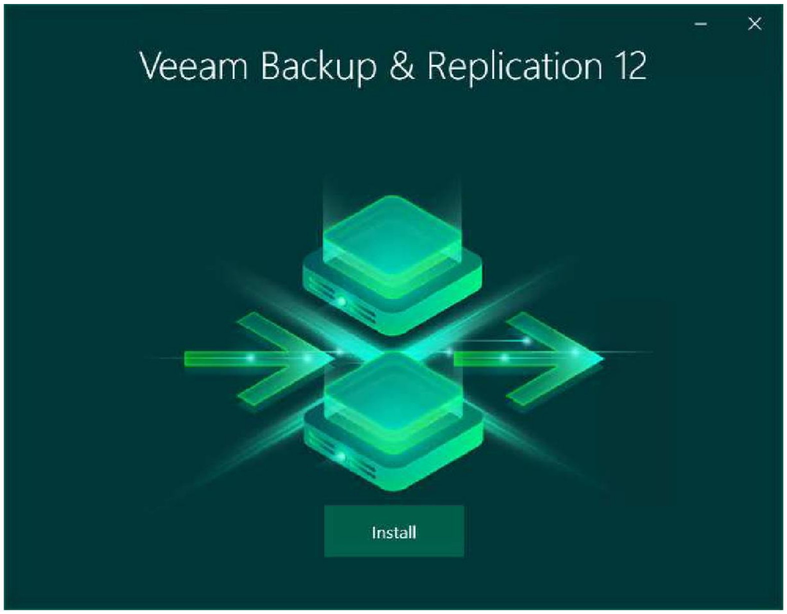
User Account Control

Do you want to allow this app to make changes to your device?

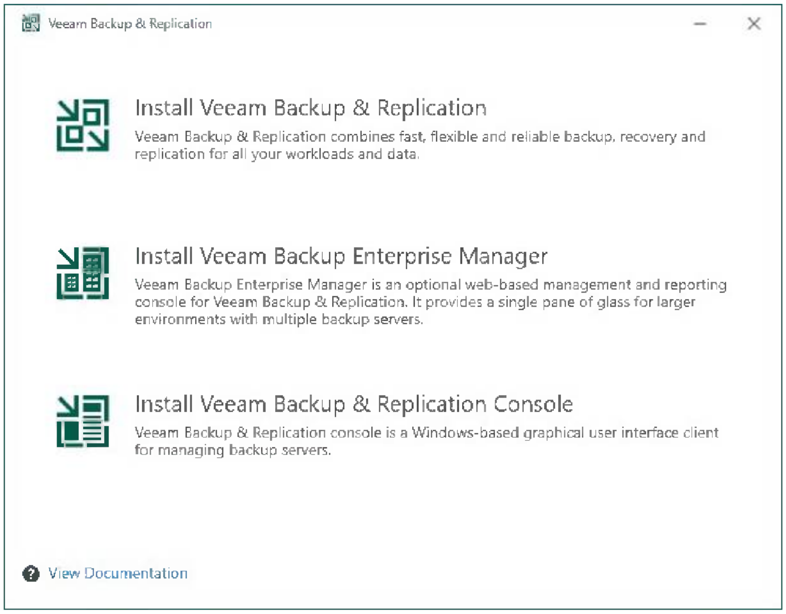
Veeam Backup & Replication Setup Autorun

Verified publisher: Veeam Software Group GmbH
File origin: CD/DVD drive

6. On the Veeam Backup & Replication 12 page, click Install.



7. Select Install Veeam Backup & Replication on the Veeam Backup & Replication page.


Veeam Backup & Replication

Install Veeam Backup & Replication

Veeam Backup & Replication combines fast, flexible and reliable backup, recovery and replication for all your workloads and data.

Install Veeam Backup Enterprise Manager

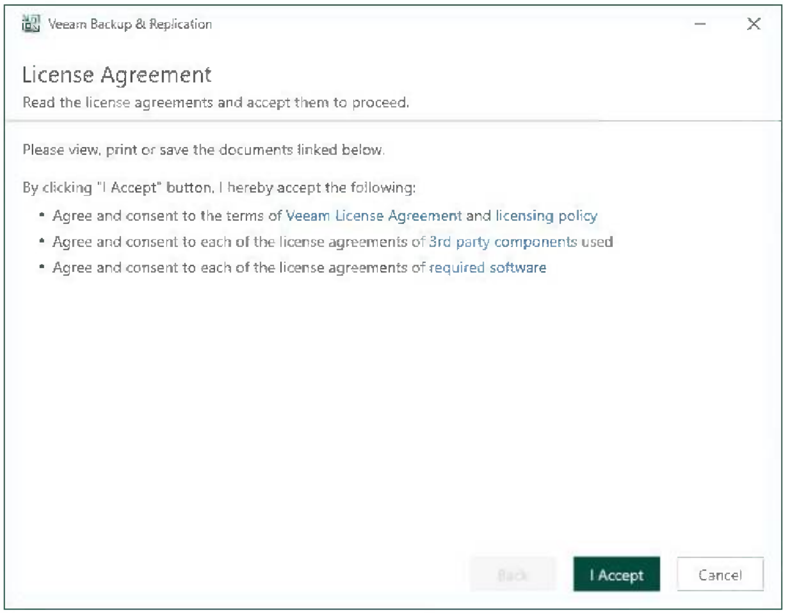
Veeam Backup Enterprise Manager is an optional web-based management and reporting console for Veeam Backup & Replication. It provides a single pane of glass for larger environments with multiple backup servers.

Install Veeam Backup & Replication Console

Veeam Backup & Replication console is a Windows-based graphical user interface client for managing backup servers.

View Documentation

8. Click I Accept on the License Agreement page.



License Agreement

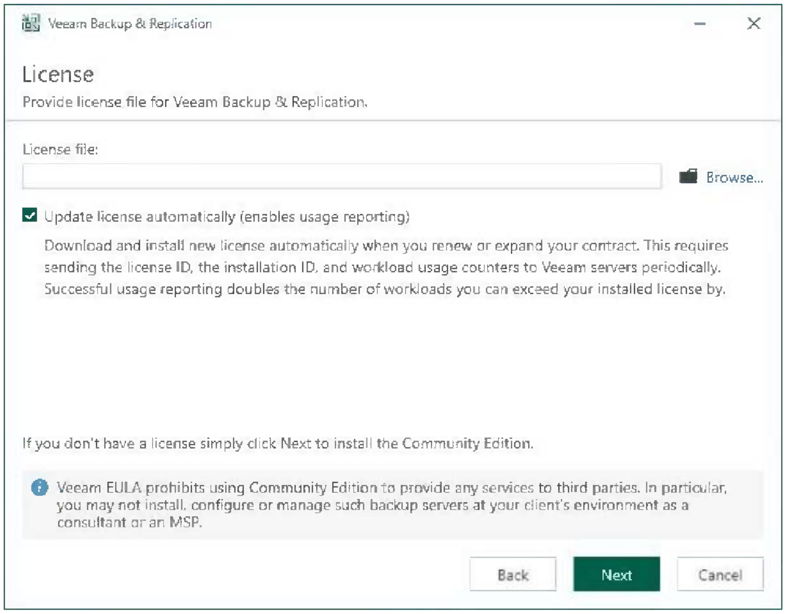
Read the license agreements and accept them to proceed.

Please view, print or save the documents linked below.

By clicking "I Accept" button, I hereby accept the following:

- Agree and consent to the terms of Veeam License Agreement and licensing policy
- Agree and consent to each of the license agreements of 3rd party components used
- Agree and consent to each of the license agreements of required software

9. Click Browse on the License page.



License

Provide license file for Veeam Backup & Replication.

License file:

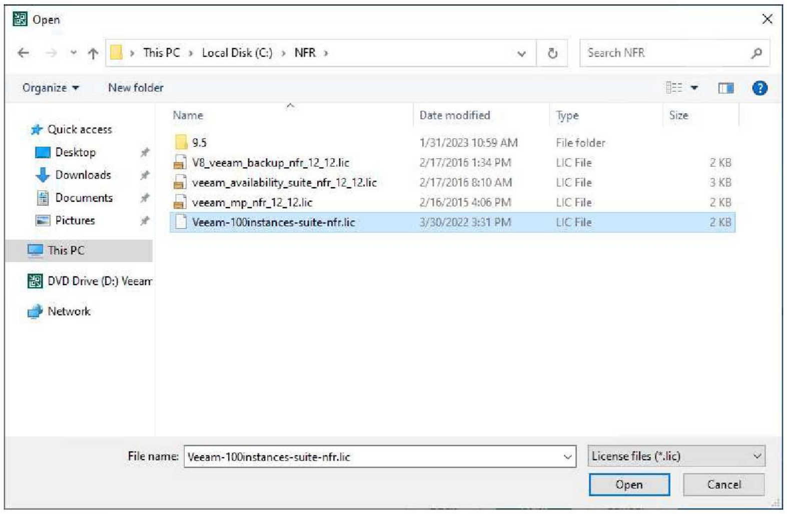
☑ Update license automatically (enables usage reporting)

Download and install new license automatically when you renew or expand your contract. This requires sending the license ID, the installation ID, and workload usage counters to Veeam servers periodically. Successful usage reporting doubles the number of workloads you can exceed your installed license by.

If you don't have a license simply click Next to install the Community Edition.

Veeam EULA prohibits using Community Edition to provide any services to third parties. In particular, you may not install, configure or manage such backup servers at your client's environment as a consultant or an MSP.

10. Select a license file for Veeam Backup & Replication and click Open.

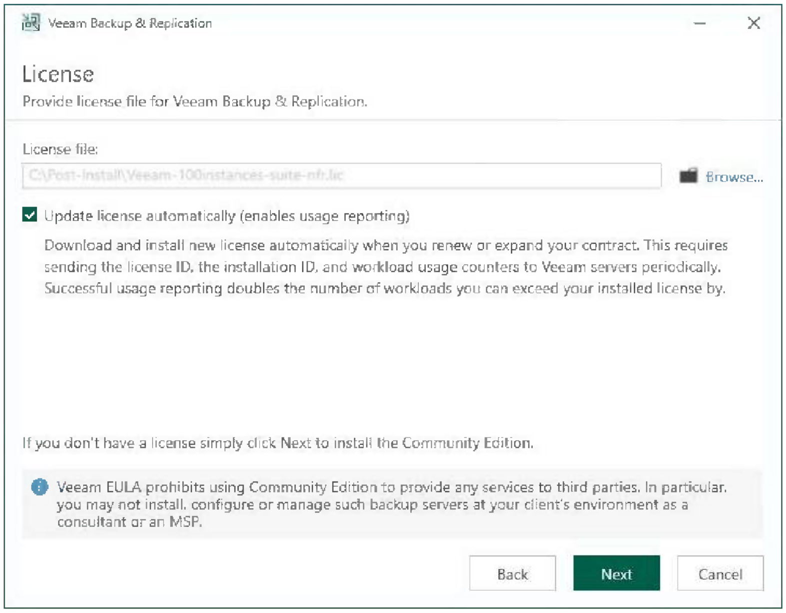


Name	Date modified	Type	Size
9.5	1/31/2023 10:59 AM	File folder	
V8_veeam_backup_nfr_12_12.lic	2/17/2016 1:34 PM	LIC File	2 KB
veeam_availability_suite_nfr_12_12.lic	2/17/2016 8:10 AM	LIC File	3 KB
veeam_mp_nfr_12_12.lic	2/16/2015 4:06 PM	LIC File	2 KB
Veeam-100instances-suite-nfr.lic	3/30/2022 3:31 PM	LIC File	2 KB

File name: Veeam-100instances-suite-nfr.lic

License files (*.lic)

11. On the License page, select Update license automatically (enable usage reporting). It will automatically download and install a new license when you renew or expand your contract.
12. Click Next.



License

Provide license file for Veeam Backup & Replication.

License file:

C:\Post-Install\Veeam-100instances-suite-nfr.lic

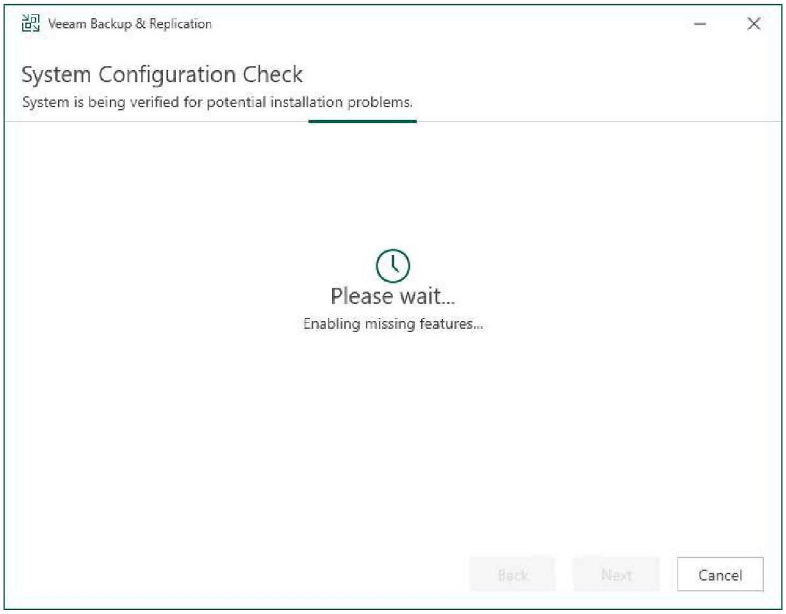
☑ Update license automatically (enables usage reporting)

Download and install new license automatically when you renew or expand your contract. This requires sending the license ID, the installation ID, and workload usage counters to Veeam servers periodically. Successful usage reporting doubles the number of workloads you can exceed your installed license by.

If you don't have a license simply click Next to install the Community Edition.

Veeam EULA prohibits using Community Edition to provide any services to third parties. In particular, you may not install, configure or manage such backup servers at your client's environment as a consultant or an MSP.

13. The setup wizard checks if the required software is installed on the machine during the System Configuration Check step. If required components are missing, the setup will attempt to install them independently. Rebooting is required after the components have been successfully installed. Click Reboot to restart the machine.



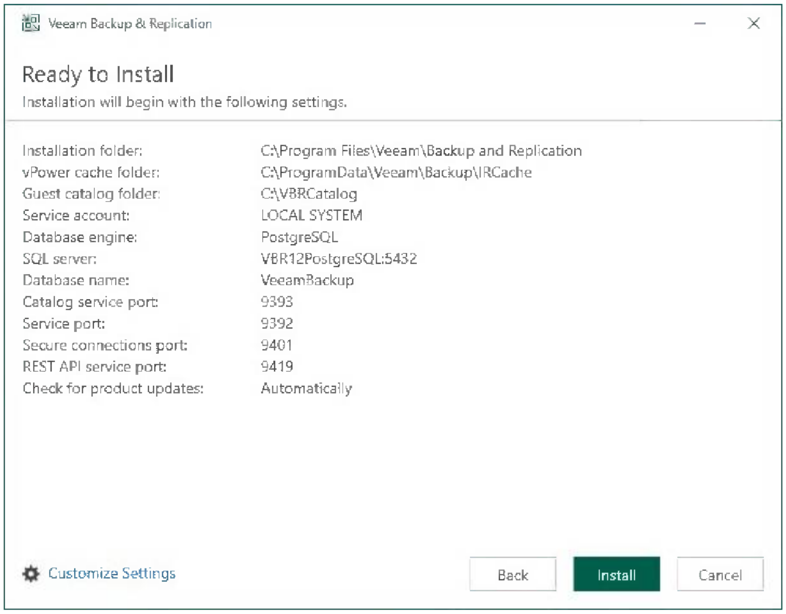
System Configuration Check

System is being verified for potential installation problems.

Please wait...

Enabling missing features...

14. Click Customize Settings on the Ready to Install page.

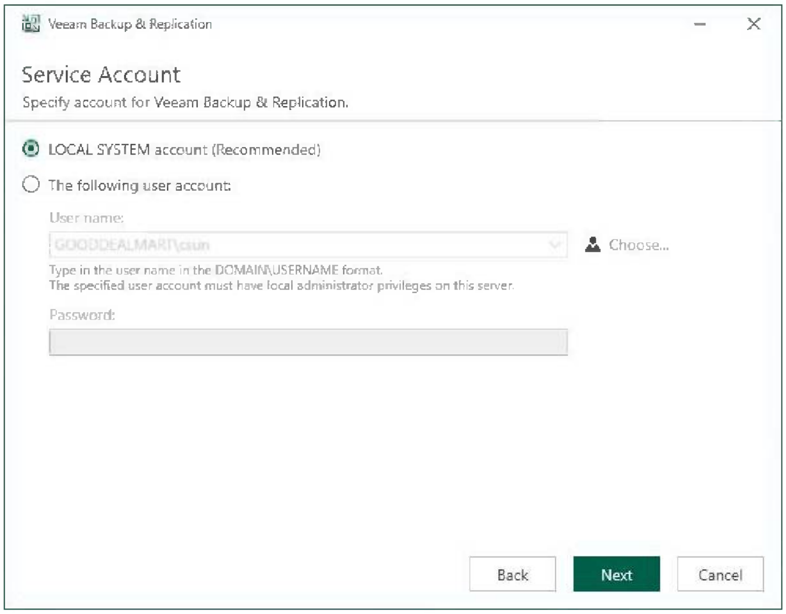


Ready to Install

Installation will begin with the following settings.

Installation folder:	C:\Program Files\Veeam\Backup and Replication
vPower cache folder:	C:\ProgramData\Veeam\Backup\IRCache
Guest catalog folder:	C:\VBRCatalog
Service account:	LOCAL SYSTEM
Database engine:	PostgreSQL
SQL server:	VBR12PostgreSQL:5432
Database name:	VeeamBackup
Catalog service port:	9393
Service port:	9392
Secure connections port:	9401
REST API service port:	9419
Check for product updates:	Automatically

15. On the Service Account page, select LOCAL SYSTEM account and click Next.



Veeam Backup & Replication

Service Account

Specify account for Veeam Backup & Replication.

● LOCAL SYSTEM account (Recommended)

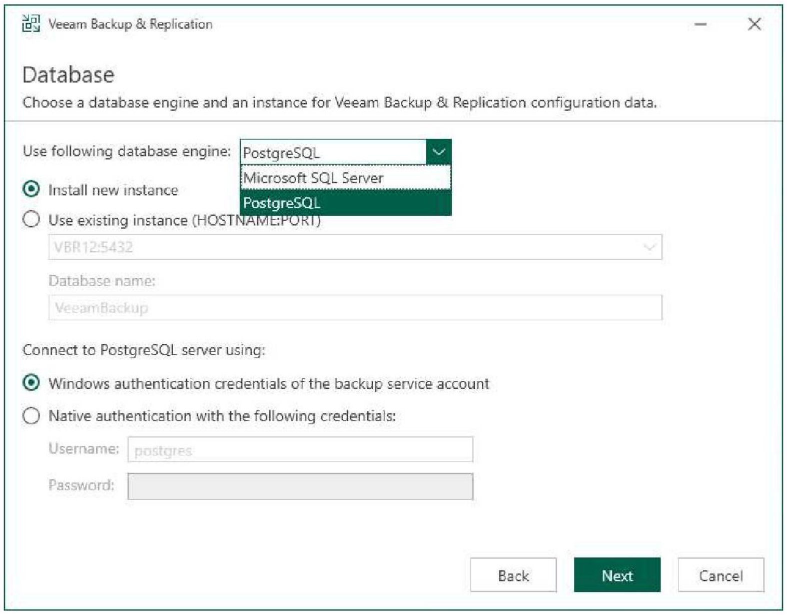
○ The following user account:

User name: GOODDEALMART\csun

Type in the user name in the DOMAIN\USERNAME format.
The specified user account must have local administrator privileges on this server.

Password:

16. On the Database page, select PostgreSQL from the database engine drop-down list.
17. Select the Install a new instance option to install a new PostgreSQL instance. PostgreSQL 15.1 will be installed on the Veeam Backup & Replication server, and a database named VeeamBackup will be created.



Veeam Backup & Replication

Database

Choose a database engine and an instance for Veeam Backup & Replication configuration data.

Use following database engine: PostgreSQL

● Install new instance

○ Use existing instance (HOSTNAME:PORT)

VBR12:5432

Database name:

VeeamBackup

Connect to PostgreSQL server using:

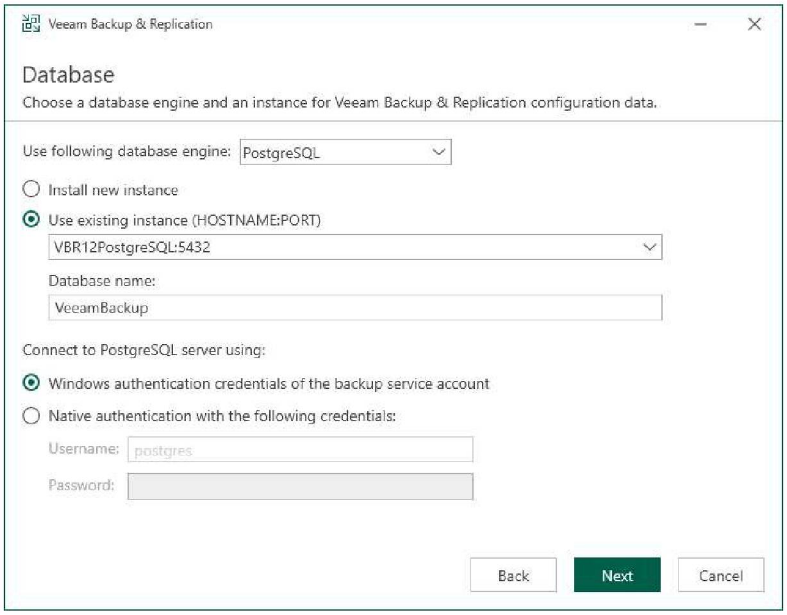
● Windows authentication credentials of the backup service account

○ Native authentication with the following credentials:

Username: postgres

Password:

18. Select the Use the existing instance option to use an already installed PostgreSQL instance. Then, in the HOSTNAME: PORT format, enter the instance name.
19. Enter a name for the Veeam Backup & Replication configuration database in the Database name field.
20. Select Windows authentication credentials of the backup service account to connect to PostgreSQL Server.
21. Click Next.



Veeam Backup & Replication

Database

Choose a database engine and an instance for Veeam Backup & Replication configuration data.

Use following database engine: PostgreSQL

○ Install new instance

● Use existing instance (HOSTNAME:PORT)

VBR12PostgreSQL:5432

Database name:

VeeamBackup

Connect to PostgreSQL server using:

● Windows authentication credentials of the backup service account

○ Native authentication with the following credentials:

Username: postgres

Password:

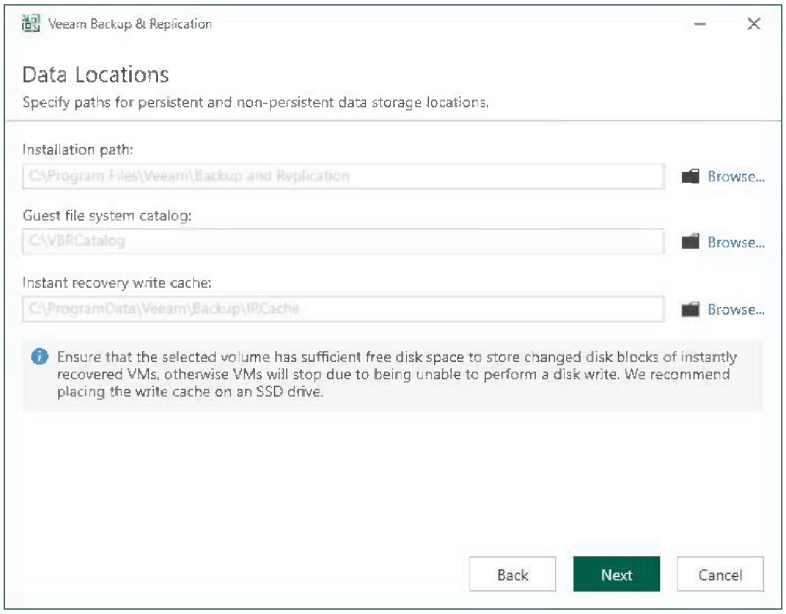
Note:

If you use an already installed PostgreSQL instance or make any changes to the machine hardware, you must perform additional PostgreSQL instance configuration. To accomplish this:

1. In the automatic mode, run the Set-VBRPSQLDatabaseServerLimits cmdlet.

2. Start the PostgreSQL service again.

22. On the Data locations page, click Browse and select the path in the Installation path field.
23. Browse and select the path in the Guest file system catalog: field.
24. Click Browse and select the path in the Instant recovery write cache field.
25. Click Next.



Data Locations

Specify paths for persistent and non-persistent data storage locations.

Installation path:

C:\Program Files\Veeam\Backup and Replication

Guest file system catalog:

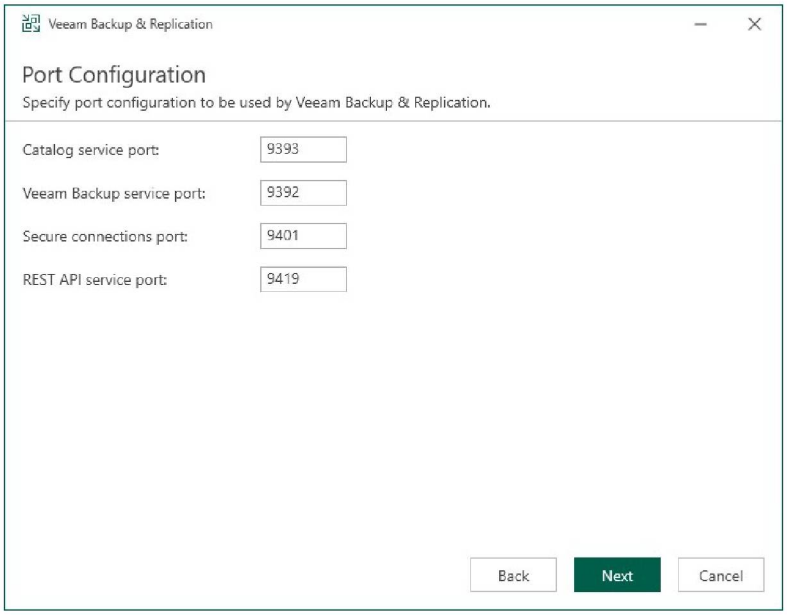
C:\VBRCatalog

Instant recovery write cache:

C:\ProgramData\Veeam\Backup\IRCache

Ensure that the selected volume has sufficient free disk space to store changed disk blocks of instantly recovered VMs, otherwise VMs will stop due to being unable to perform a disk write. We recommend placing the write cache on an SSD drive.

26. On the Port Configuration page, specify the port configuration to be used by Veeam Backup and Replication and click Next.



Port Configuration

Specify port configuration to be used by Veeam Backup & Replication.

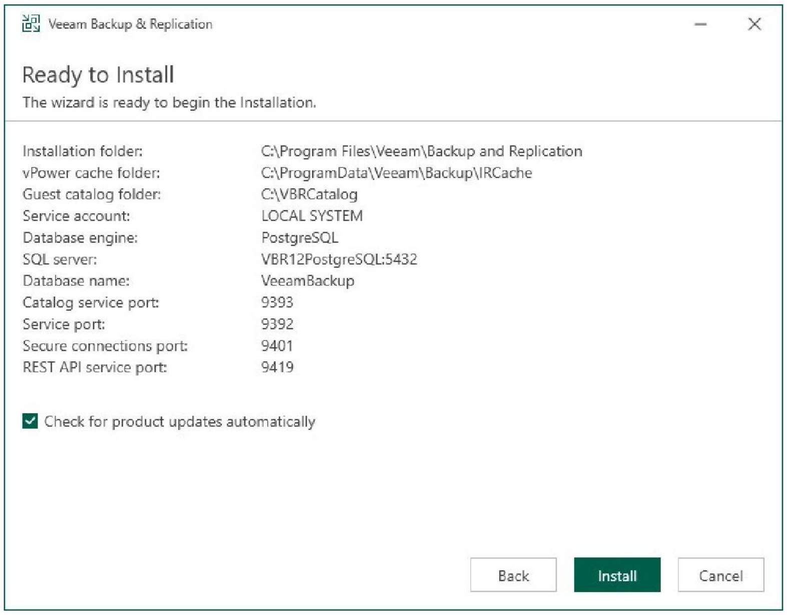
Catalog service port: 9393

Veeam Backup service port: 9392

Secure connections port: 9401

REST API service port: 9419

27. Click Install on the Ready to Install page.



Veeam Backup & Replication

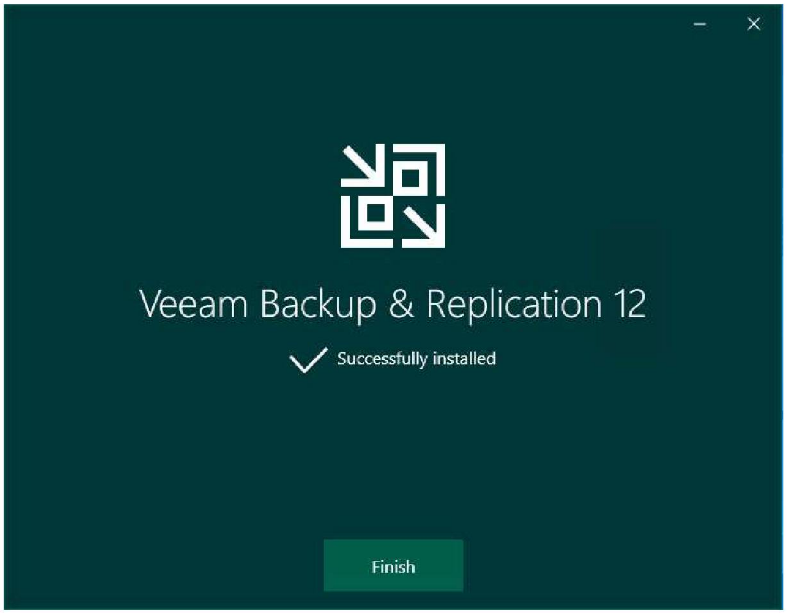
Ready to Install

The wizard is ready to begin the Installation.

Installation folder:	C:\Program Files\Veeam\Backup and Replication
vPower cache folder:	C:\ProgramData\Veeam\Backup\IRCache
Guest catalog folder:	C:\VBRCatalog
Service account:	LOCAL SYSTEM
Database engine:	PostgreSQL
SQL server:	VBR12PostgreSQL:5432
Database name:	VeeamBackup
Catalog service port:	9393
Service port:	9392
Secure connections port:	9401
REST API service port:	9419

☑ Check for product updates automatically

28. Click Finish on the Veeam Backup & Replication 12 Successfully installed page.



Veeam Backup & Replication 12

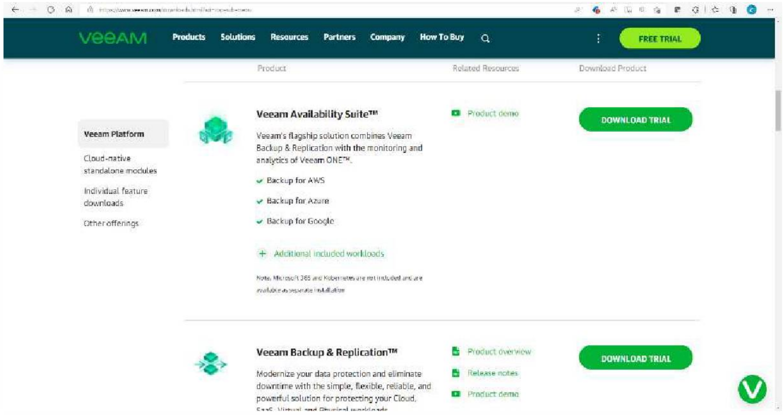
✓ Successfully installed

Install Veeam Backup and Replication v12 with Microsoft SQL (or SQL Express)

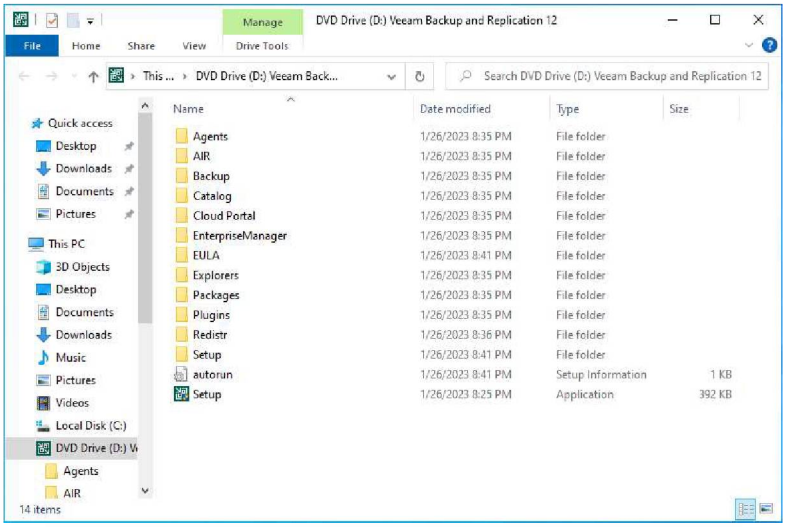
When you install Veeam Backup & Replication, the Veeam Backup & Replication console is automatically installed on the backup server.

You can choose Microsoft SQL as a Veeam Backup & Replication database. However, you installed a Microsoft SQL Server (or Express), either locally on the backup manager server or remotely. If Microsoft SQL Server is not already installed. In that case, the Veeam Backup & Replication won't install the Microsoft SQL Server Express Edition on the backup server automatically. You must install it before installing Veeam Backup and Replication v12 RTM version.

Microsoft SQL Server Express has a configuration data storage limit of 10 GB. The Express Edition is sufficient for the evaluation and small environments (500 VMs).

Instructions	Screenshot (if applicable)
1. Ensure the Microsoft SQL Server or Microsoft SQL Server Express is installed locally or remotely. 2. Log in to the Veeam Backup and Replication manager server. 3. Download the Veeam Backup and Replication v12 ISO image file from the Veeam website sign-in required).	 Veeam Availability Suite™ Veeam's flagship solution combines Veeam Backup & Replication with the monitoring and analytics of Veeam ONE™. Note, Microsoft 365 and Kubernetes are not included and are available as separate installation Veeam Backup & Replication™ Modernize your data protection and eliminate downtime with the simple, flexible, reliable, and powerful solution for protecting your Cloud, SaaS, Virtual and Physical workloads

4. Mount the Veeam Backup and Replication v12 iso image file.
5. Run Setup.exe.

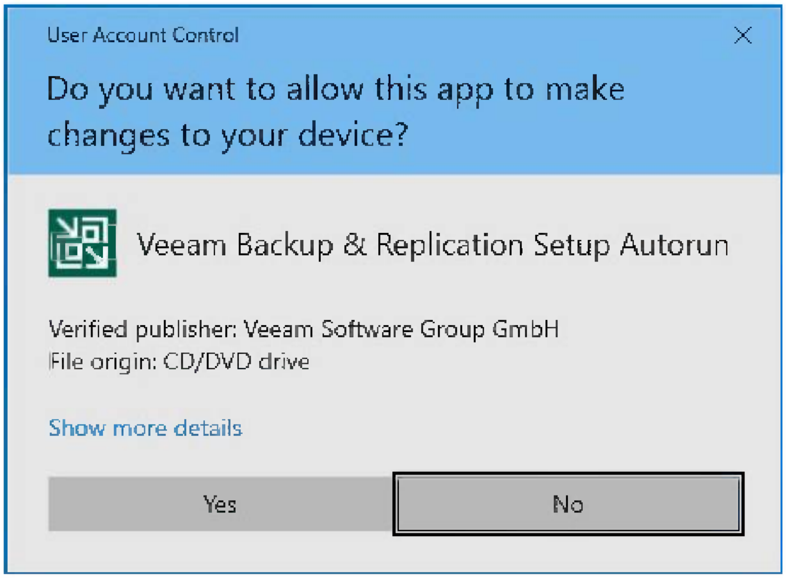


DVD Drive (D:) Veeam Backup and Replication 12

Name	Date modified	Type	Size
Agents	1/26/2023 8:35 PM	File folder	
AIR	1/26/2023 8:35 PM	File folder	
Backup	1/26/2023 8:35 PM	File folder	
Catalog	1/26/2023 8:35 PM	File folder	
Cloud Portal	1/26/2023 8:35 PM	File folder	
EnterpriseManager	1/26/2023 8:35 PM	File folder	
EULA	1/26/2023 8:41 PM	File folder	
Explorers	1/26/2023 8:35 PM	File folder	
Packages	1/26/2023 8:35 PM	File folder	
Plugins	1/26/2023 8:35 PM	File folder	
Redistr	1/26/2023 8:36 PM	File folder	
Setup	1/26/2023 8:41 PM	File folder	
autorun	1/26/2023 8:41 PM	Setup Information	1 KB
Setup	1/26/2023 8:25 PM	Application	392 KB

14 items

6. On the User Access Control page, click Yes.



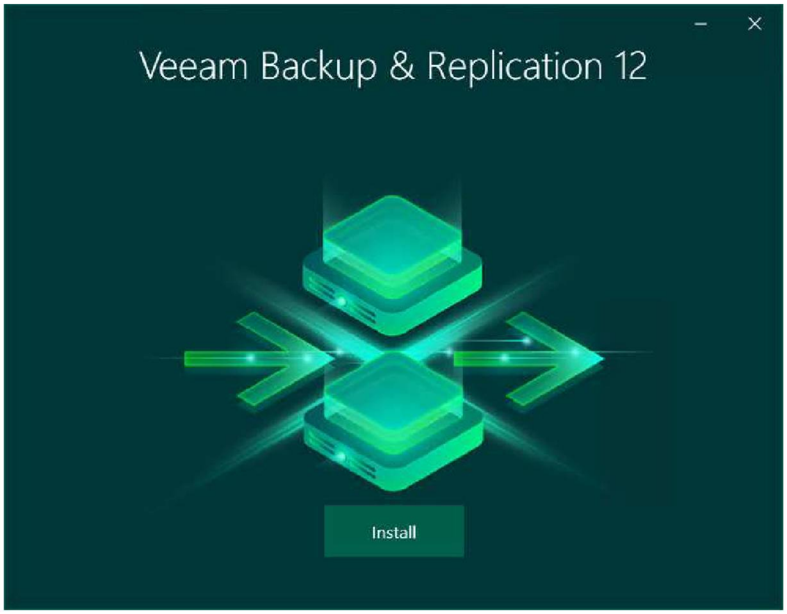
User Account Control

Do you want to allow this app to make changes to your device?

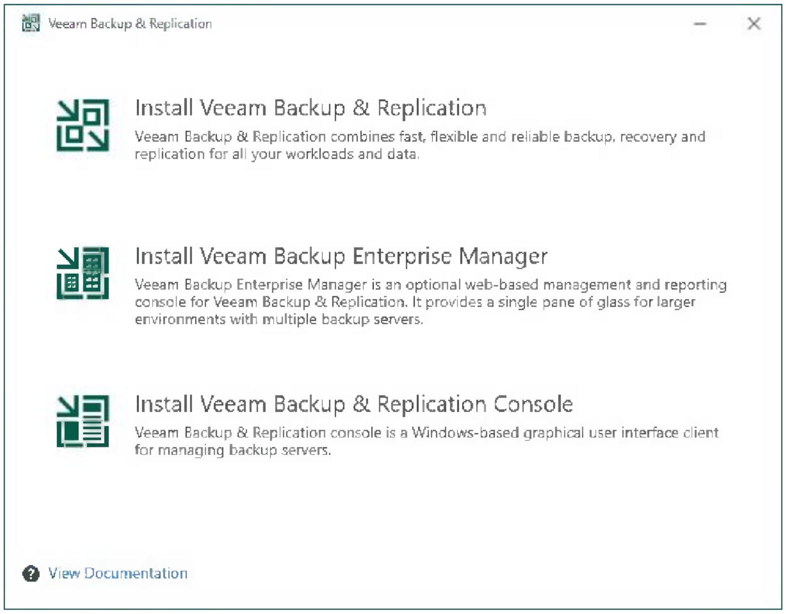
Veeam Backup & Replication Setup Autorun

Verified publisher: Veeam Software Group GmbH
File origin: CD/DVD drive

7. On the Veeam Backup & Replication 12 page, click Install.



8. Select Install Veeam Backup & Replication on the Veeam Backup & Replication page.



Install Veeam Backup & Replication

Veeam Backup & Replication combines fast, flexible and reliable backup, recovery and replication for all your workloads and data.

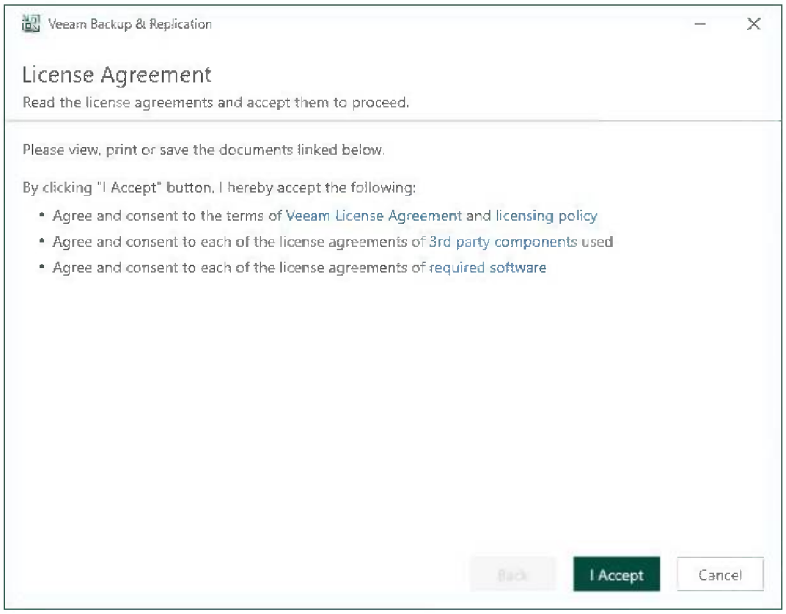
Install Veeam Backup Enterprise Manager

Veeam Backup Enterprise Manager is an optional web-based management and reporting console for Veeam Backup & Replication. It provides a single pane of glass for larger environments with multiple backup servers.

Install Veeam Backup & Replication Console

Veeam Backup & Replication console is a Windows-based graphical user interface client for managing backup servers.

9. Click I Accept on the License Agreement page.



License Agreement

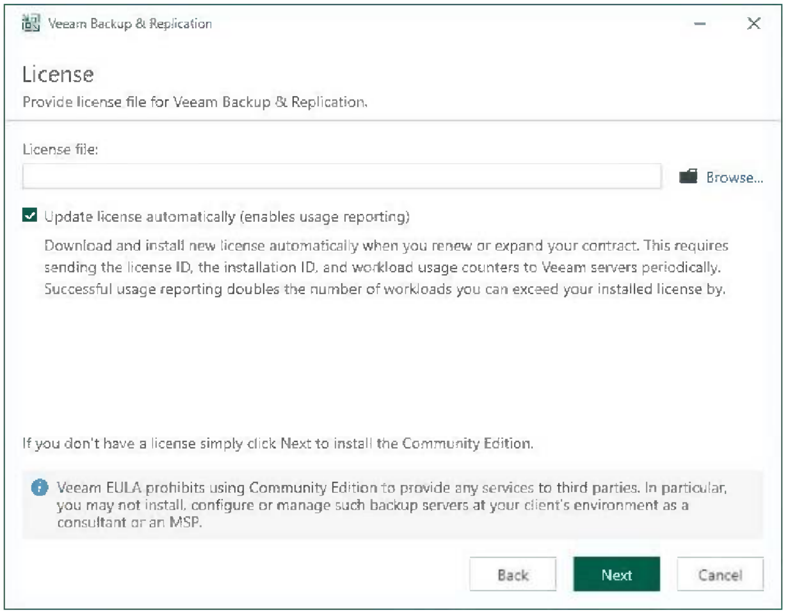
Read the license agreements and accept them to proceed.

Please view, print or save the documents linked below.

By clicking "I Accept" button, I hereby accept the following:

- Agree and consent to the terms of Veeam License Agreement and licensing policy
- Agree and consent to each of the license agreements of 3rd party components used
- Agree and consent to each of the license agreements of required software

10. Click Browse on the License page.



License

Provide license file for Veeam Backup & Replication.

License file:

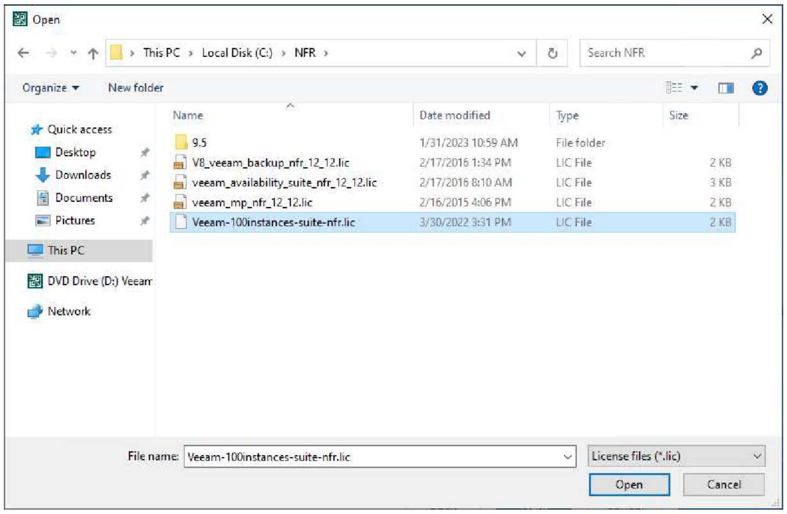
☑ Update license automatically (enables usage reporting)

Download and install new license automatically when you renew or expand your contract. This requires sending the license ID, the installation ID, and workload usage counters to Veeam servers periodically. Successful usage reporting doubles the number of workloads you can exceed your installed license by.

If you don't have a license simply click Next to install the Community Edition.

Veeam EULA prohibits using Community Edition to provide any services to third parties. In particular, you may not install, configure or manage such backup servers at your client's environment as a consultant or an MSP.

11. Select a license file for Veeam Backup & Replication and click Open.

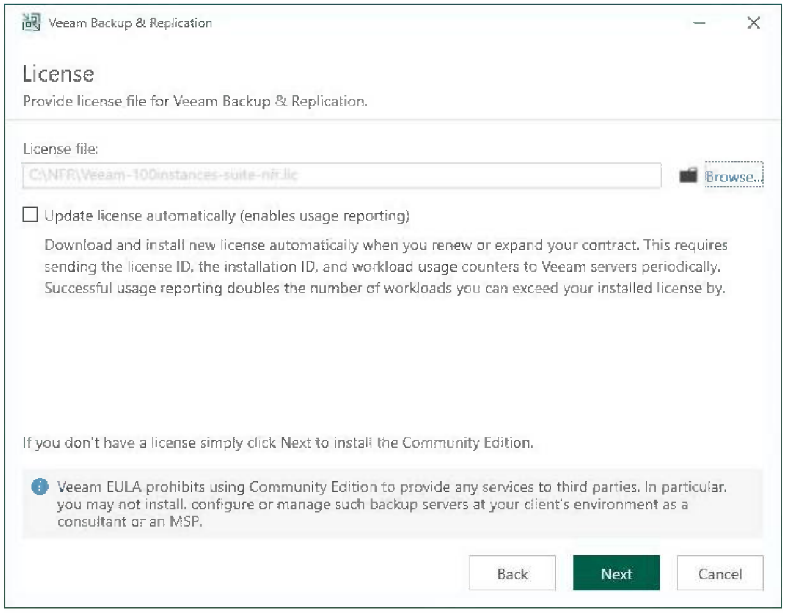


Name	Date modified	Type	Size
9.5	1/31/2023 10:59 AM	File folder	
V8_veeam_backup_nfr_12_12.lic	2/17/2016 1:34 PM	LIC File	2 KB
veeam_availability_suite_nfr_12_12.lic	2/17/2016 8:10 AM	LIC File	3 KB
veeam_mp_nfr_12_12.lic	2/16/2015 4:06 PM	LIC File	2 KB
Veeam-100instances-suite-nfr.lic	3/30/2022 3:31 PM	LIC File	2 KB

File name: Veeam-100instances-suite-nfr.lic

License files (*.lic)

12. On the License page, select Update license automatically (enable usage reporting). It will automatically download and install a new license when you renew or expand your contract.
13. Click Next.



License

Provide license file for Veeam Backup & Replication.

License file:

C:\NFR\Veeam-100instances-suite-nfr.lic

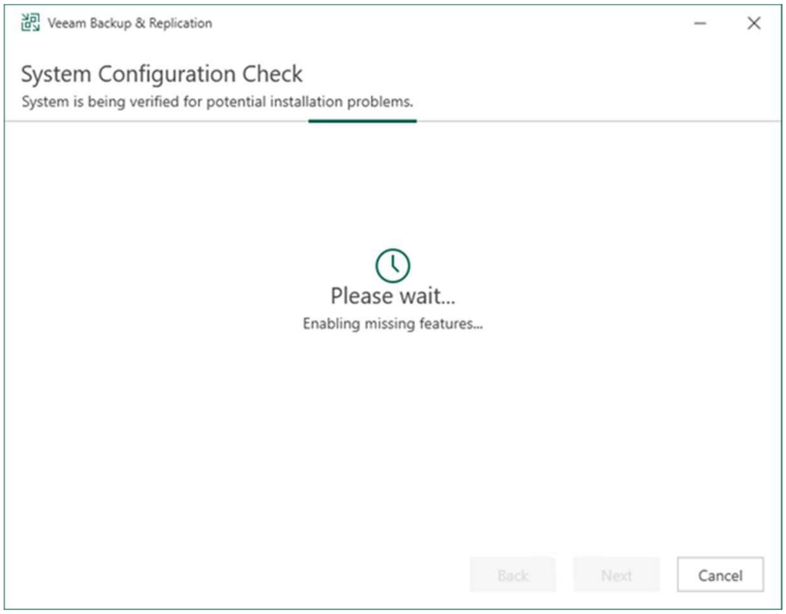
□ Update license automatically (enables usage reporting)

Download and install new license automatically when you renew or expand your contract. This requires sending the license ID, the installation ID, and workload usage counters to Veeam servers periodically. Successful usage reporting doubles the number of workloads you can exceed your installed license by.

If you don't have a license simply click Next to install the Community Edition.

Veeam EULA prohibits using Community Edition to provide any services to third parties. In particular, you may not install, configure or manage such backup servers at your client's environment as a consultant or an MSP.

14. The setup wizard checks if the required software is installed on the machine during the System Configuration Check step. If required components are missing, the setup will attempt to install them independently. Rebooting is required after the components have been successfully installed. Click Reboot to restart the machine.



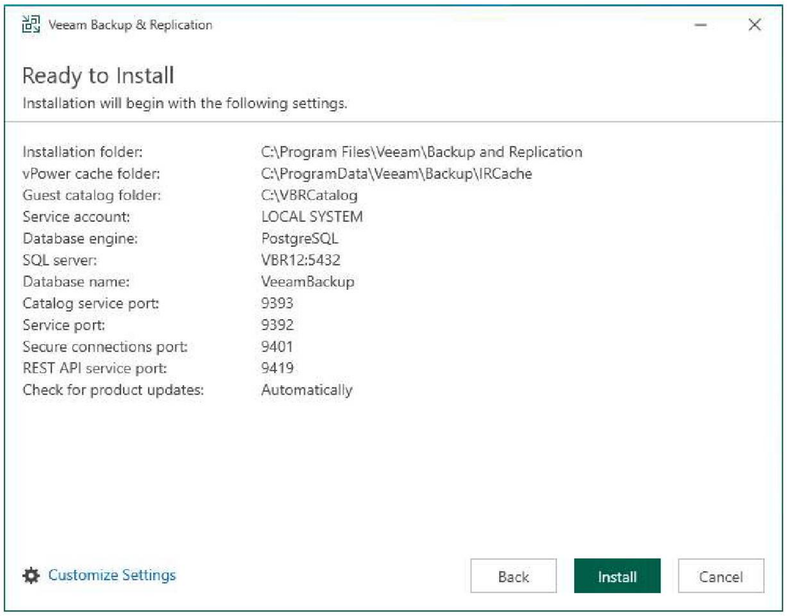
System Configuration Check

System is being verified for potential installation problems.

Please wait...

Enabling missing features...

15. Click Customize Settings on the Ready to Install page.

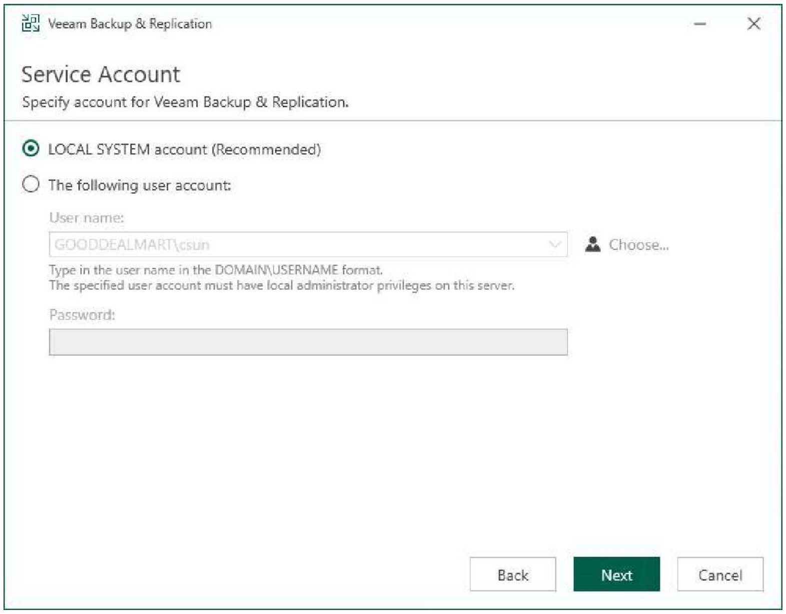


Ready to Install

Installation will begin with the following settings.

Installation folder:	C:\Program Files\Veeam\Backup and Replication
vPower cache folder:	C:\ProgramData\Veeam\Backup\IRCache
Guest catalog folder:	C:\VBRCatalog
Service account:	LOCAL SYSTEM
Database engine:	PostgreSQL
SQL server:	VBR12:5432
Database name:	VeeamBackup
Catalog service port:	9393
Service port:	9392
Secure connections port:	9401
REST API service port:	9419
Check for product updates:	Automatically

16. On the Service Account page, select LOCAL SYSTEM account and click Next.



Veeam Backup & Replication

Service Account

Specify account for Veeam Backup & Replication.

● LOCAL SYSTEM account (Recommended)

○ The following user account:

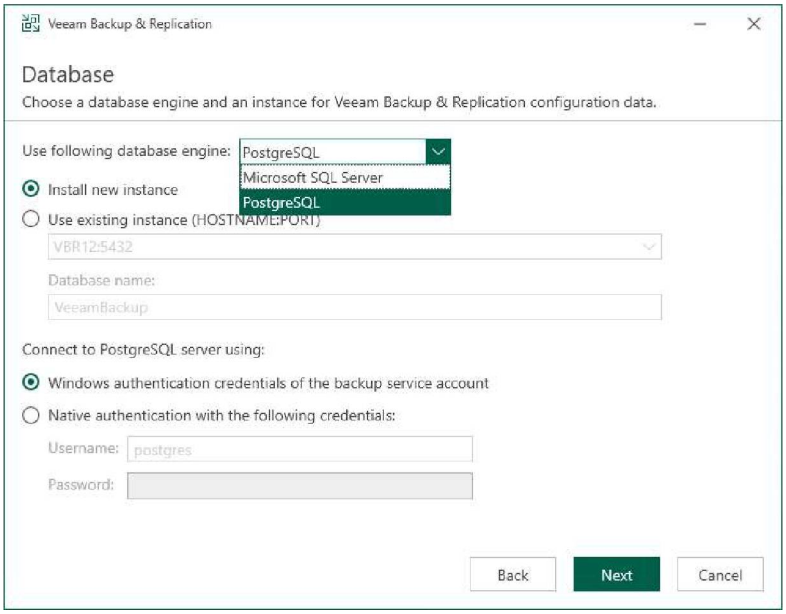
User name:

GOODDEALMART\csun

Type in the user name in the DOMAIN\USERNAME format.
The specified user account must have local administrator privileges on this server.

Password:

17. On the Database page, select the Microsoft SQL Server from the database engine drop-down list.



Veeam Backup & Replication

Database

Choose a database engine and an instance for Veeam Backup & Replication configuration data.

Use following database engine: PostgreSQL

● Install new instance

○ Use existing instance (HOSTNAME:PORT)

VBR12:5432

Database name:

VeeamBackup

Connect to PostgreSQL server using:

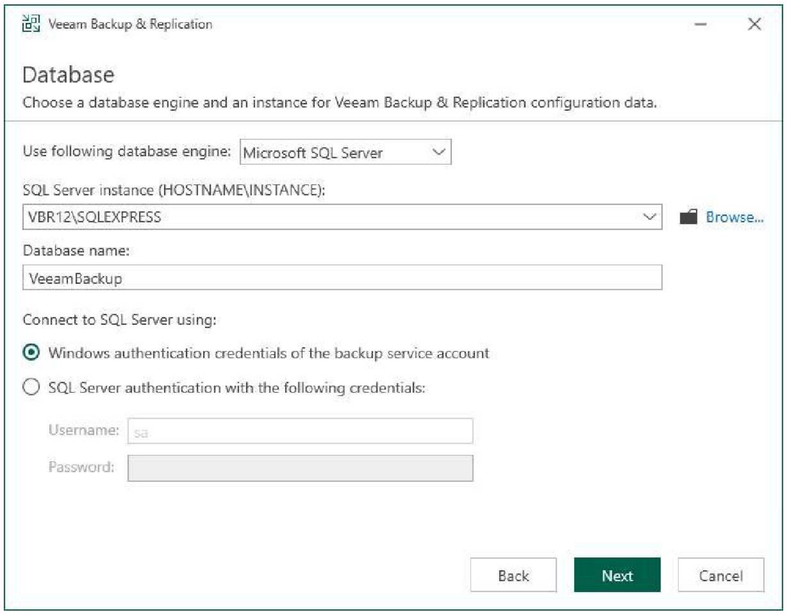
● Windows authentication credentials of the backup service account

○ Native authentication with the following credentials:

Username: postgres

Password:

18. Click Browse to select the SQL server and instance on the SQL Server instance session.
19. Select Windows authentication credentials of the backup service account to connect to SQL Server.
20. Click Next.



Database

Choose a database engine and an instance for Veeam Backup & Replication configuration data.

Use following database engine: Microsoft SQL Server

SQL Server instance (HOSTNAME\INSTANCE): VBR12\SQLEXPRESS

Database name: VeeamBackup

Connect to SQL Server using:

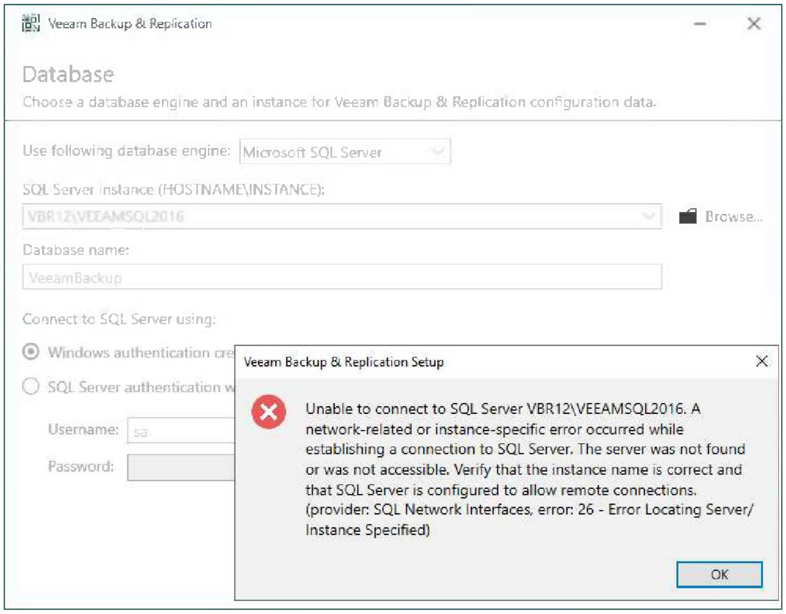
● Windows authentication credentials of the backup service account

○ SQL Server authentication with the following credentials:

Username: sa

Password:

21. The error message will pop up if the Microsoft SQL Server or Microsoft SQL Server Express does not install locally or remotely.



Database

Choose a database engine and an instance for Veeam Backup & Replication configuration data.

Use following database engine: Microsoft SQL Server

SQL Server instance (HOSTNAME\INSTANCE): VBR12\VEEAMSQL2016

Database name: VeeamBackup

Connect to SQL Server using:

● Windows authentication cre

○ SQL Server authentication w

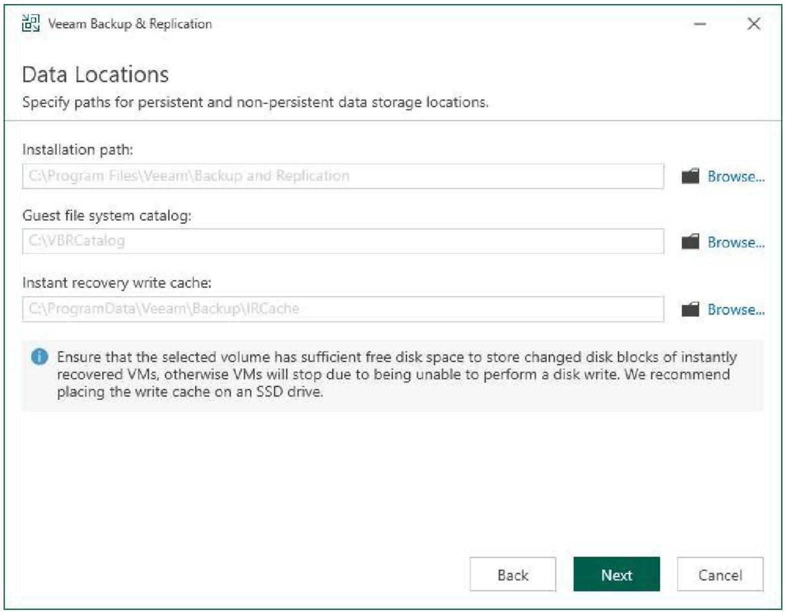
Username: sa

Password:

Veeam Backup & Replication Setup

Unable to connect to SQL Server VBR12\VEEAMSQL2016. A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: SQL Network Interfaces, error: 26 - Error Locating Server/Instance Specified)

22. On the Data locations page, click Browse and select the path in the Installation path field.
23. Browse and select the path in the Guest file system catalog: field.
24. Click Browse and select the path in the Instant recovery write cache field.
25. Click Next.



Data Locations

Specify paths for persistent and non-persistent data storage locations.

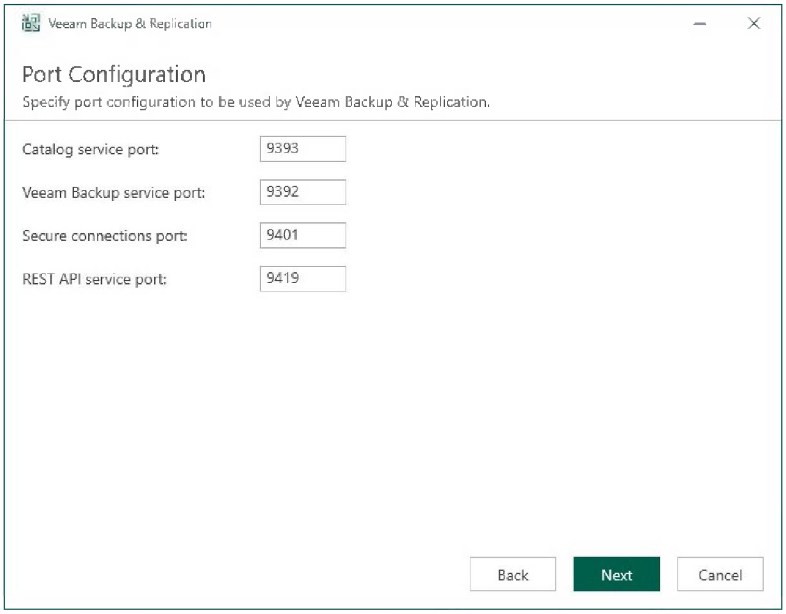
Installation path: C:\Program Files\Veeam\Backup and Replication

Guest file system catalog: C:\VBRCatalog

Instant recovery write cache: C:\ProgramData\Veeam\Backup\IRCache

Ensure that the selected volume has sufficient free disk space to store changed disk blocks of instantly recovered VMs, otherwise VMs will stop due to being unable to perform a disk write. We recommend placing the write cache on an SSD drive.

26. On the Port Configuration page, specify the port configuration to be used by Veeam Backup and Replication and click Next.



Port Configuration

Specify port configuration to be used by Veeam Backup & Replication.

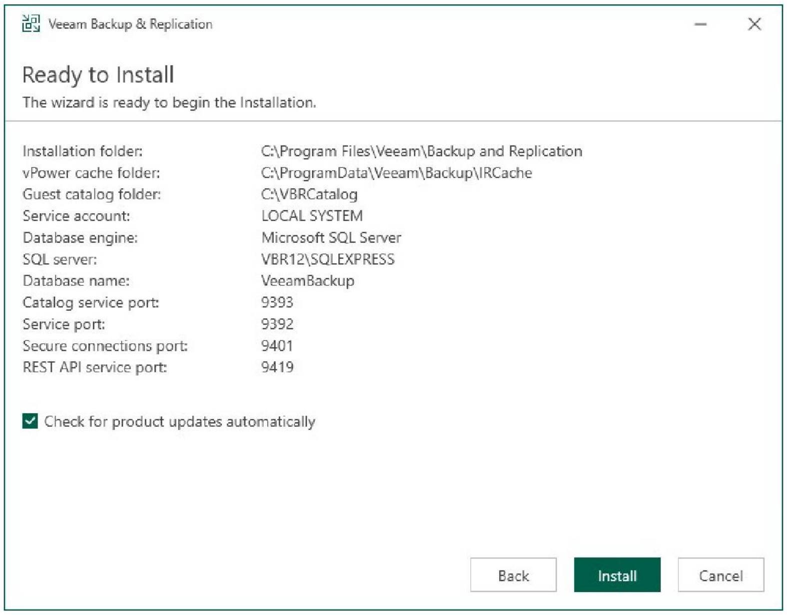
Catalog service port: 9393

Veeam Backup service port: 9392

Secure connections port: 9401

REST API service port: 9419

27. Click Install on the Ready to Install page.



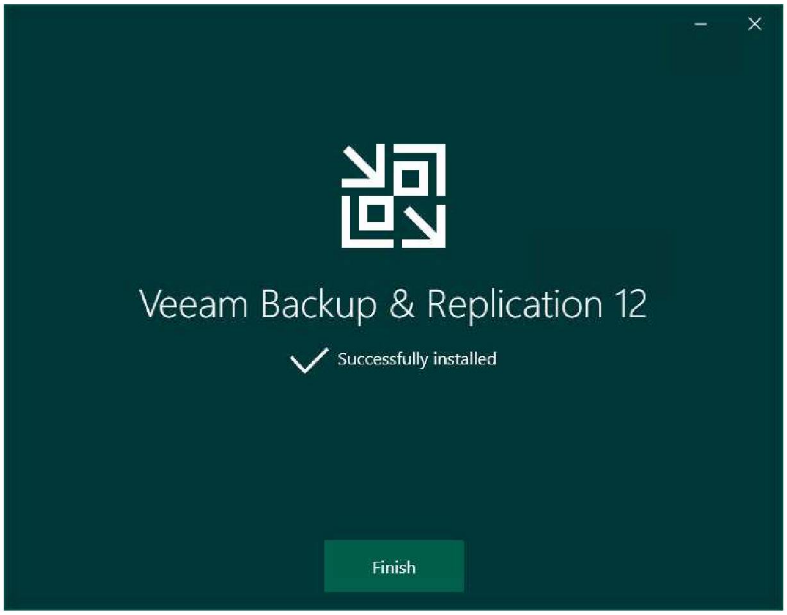
Ready to Install

The wizard is ready to begin the Installation.

```
Installation folder:          C:\Program Files\Veeam\Backup and Replication
vPower cache folder:          C:\ProgramData\Veeam\Backup\IRCache
Guest catalog folder:         C:\VBRCatalog
Service account:              LOCAL SYSTEM
Database engine:              Microsoft SQL Server
SQL server:                   VBR12\SQLEXPRESS
Database name:                VeeamBackup
Catalog service port:         9393
Service port:                 9392
Secure connections port:      9401
REST API service port:        9419
```

☑ Check for product updates automatically

28. Click Finish on the Veeam Backup & Replication 12 Successfully installed page.

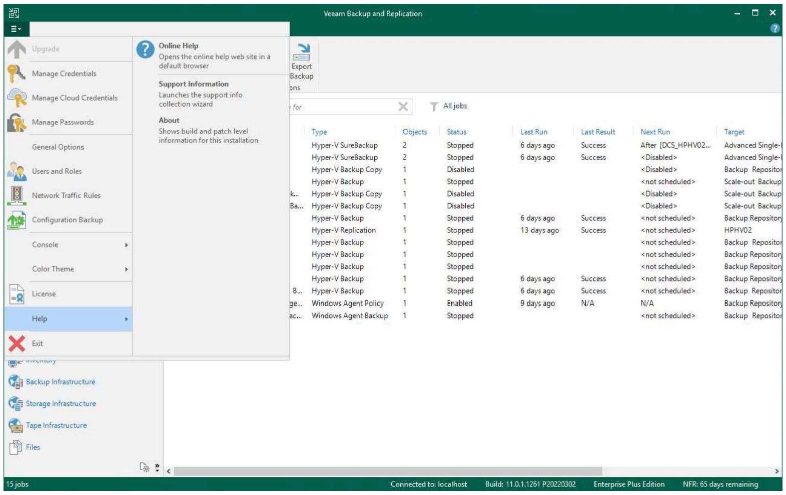


Veeam Backup & Replication 12

✓ Successfully installed

Upgrade the Existing Veeam Backup and Replication to v12

Veeam Backup and Replication v12 launched on Feb 14, 2023. If you are still using an older version, it is time to upgrade it to v12. To upgrade Veeam Backup & Replication to version 12, you must have version 10a (build 10.0.1.4854) or later installed on the supported operating system.

Instructions	Screenshot (if applicable)
1. Log in to the existing Veeam Backup and replication manager server. 2. Open the Veeam Backup & Replication Console. 3. Drop down the main menu, select Help, and click About to check Veeam Backup & Replication version.	

Online Help
Opens the online help web site in a default browser

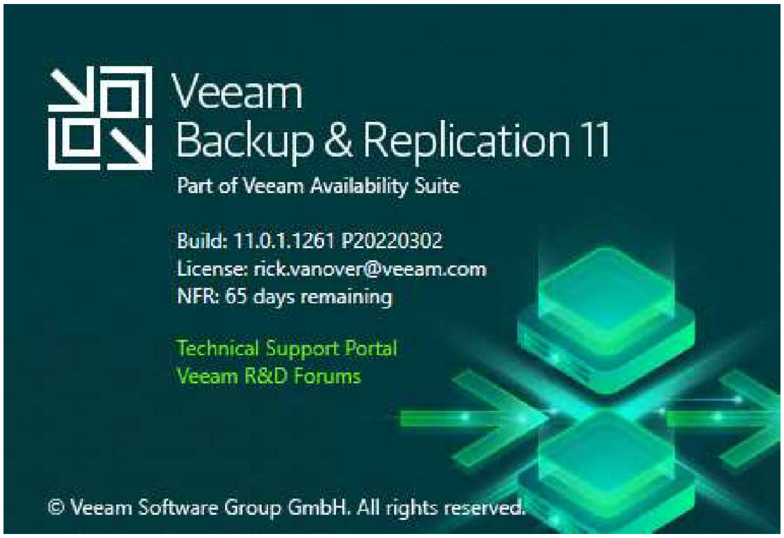
Support Information
Launches the support info collection wizard

About
Shows build and patch level information for this installation

	Type	Objects	Status	Last Run	Last Result	Next Run	Target
	Hyper-V SureBackup	2	Stopped	6 days ago	Success	After [DCS_HPHV02...	Advanced Single-
	Hyper-V SureBackup	2	Stopped	6 days ago	Success	<Disabled>	Advanced Single-
	Hyper-V Backup Copy	1	Disabled			<Disabled>	Backup Reposito
	Hyper-V Backup	1	Stopped			<not scheduled>	Scale-out Backup
k...	Hyper-V Backup Copy	1	Disabled			<Disabled>	Scale-out Backup
Ba...	Hyper-V Backup Copy	1	Disabled			<Disabled>	Scale-out Backup
	Hyper-V Backup	1	Stopped	6 days ago	Success	<not scheduled>	Backup Repository
	Hyper-V Replication	1	Stopped	13 days ago	Success	<not scheduled>	HPHV02
	Hyper-V Backup	1	Stopped			<not scheduled>	Backup Reposito
	Hyper-V Backup	1	Stopped			<not scheduled>	Backup Repository
	Hyper-V Backup	1	Stopped			<not scheduled>	Backup Repository
	Hyper-V Backup	1	Stopped	6 days ago	Success	<not scheduled>	Backup Repository
B...	Hyper-V Backup	1	Stopped	6 days ago	Success	<not scheduled>	Backup Reposito
ge...	Windows Agent Policy	1	Enabled	9 days ago	N/A	N/A	Backup Repository
ac...	Windows Agent Backup	1	Stopped			<not scheduled>	Backup Reposito

15 jobs   Connected to: localhost   Build: 11.0.1.1261 P20220302   Enterprise Plus Edition   NFR: 65 days remaining

4. Make sure the existing Veeam Backup and Replication version meets the requirements.

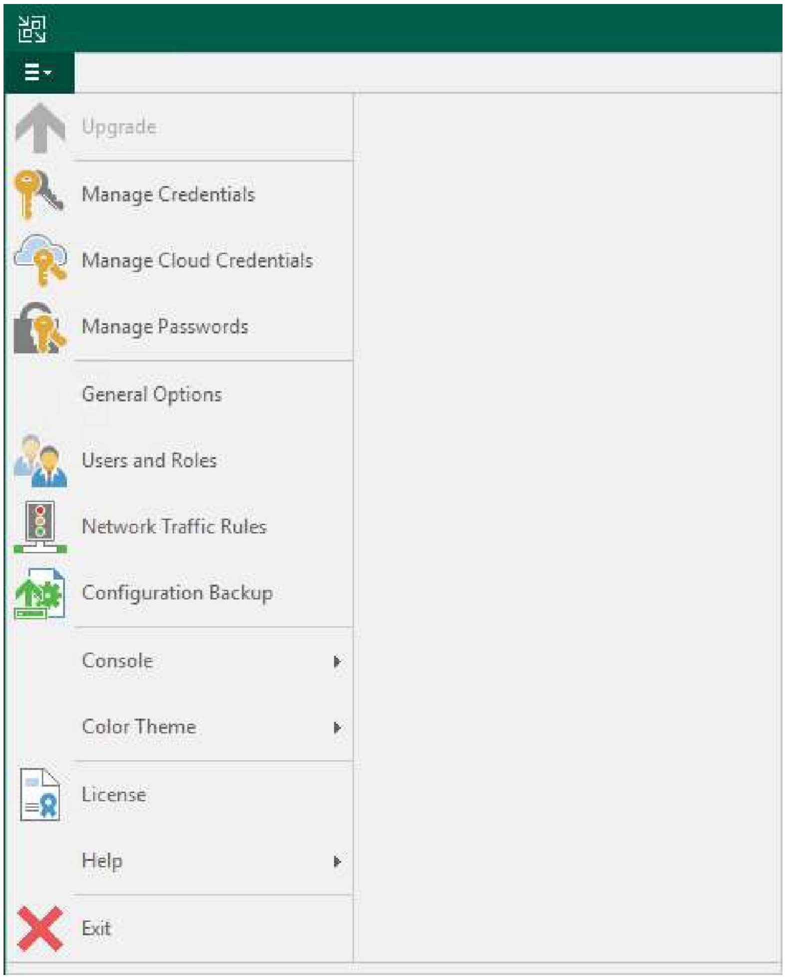


Veeam
Backup & Replication 11
Part of Veeam Availability Suite

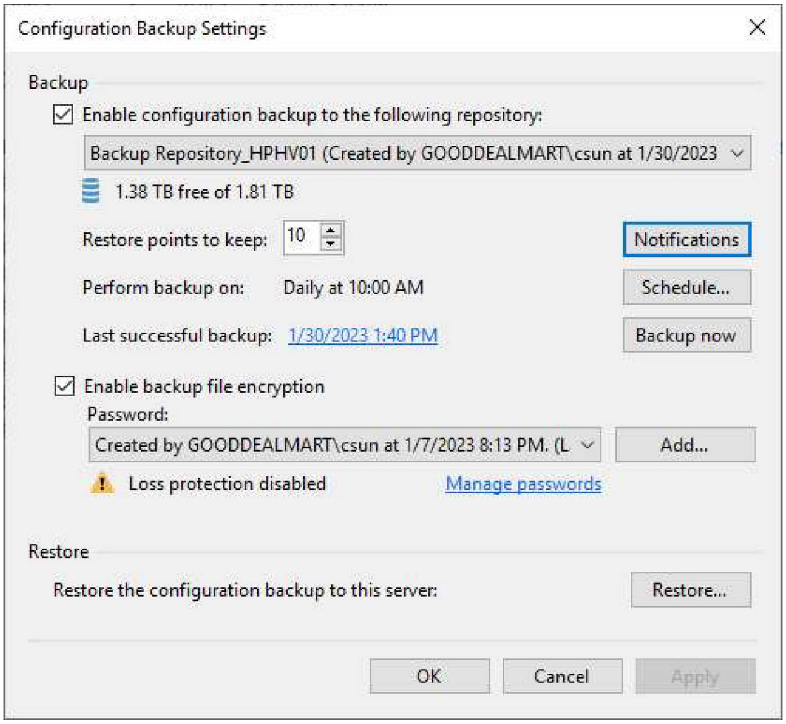
Build: 11.0.1.1261 P20220302
License: rick.vanover@veeam.com
NFR: 65 days remaining

© Veeam Software Group GmbH. All rights reserved.

5. Drop down the main menu and select Configuration Backup.



6. On the Configuration Backup Settings page, select Backup now to back up the current configuration.
7. Click OK to close the Configuration Backup Settings after the backup is completed.



Configuration Backup Settings

Backup

☑ Enable configuration backup to the following repository:

Backup Repository_HPHV01 (Created by GOODDEALMART\csun at 1/30/2023

1.38 TB free of 1.81 TB

Restore points to keep: 10

Perform backup on: Daily at 10:00 AM

Last successful backup: 1/30/2023 1:40 PM

☑ Enable backup file encryption

Password:

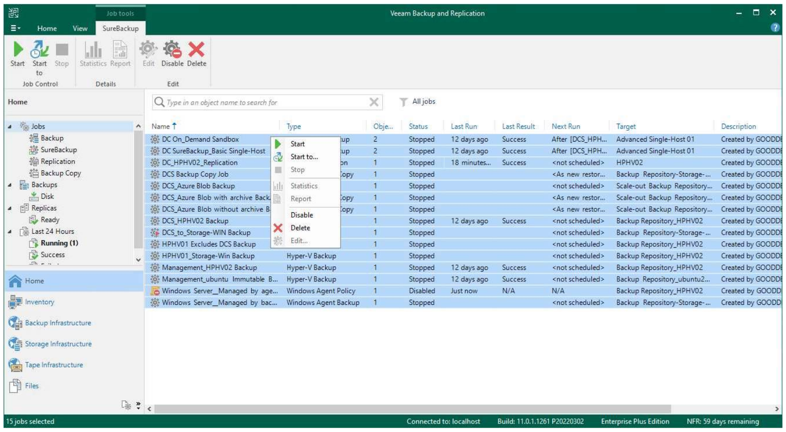
Created by GOODDEALMART\csun at 1/7/2023 8:13 PM. (L

Loss protection disabled

Restore

Restore the configuration backup to this server:

8. On the Home page, select Jobs.
9. Right-click jobs and select Disable to disable all jobs.



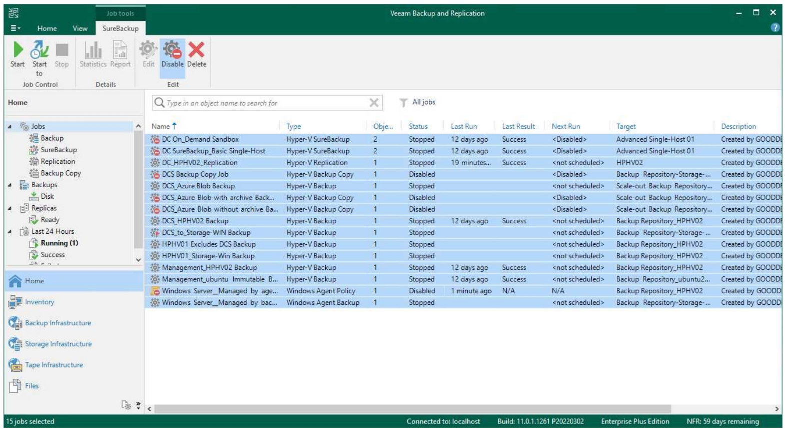
Veeam Backup and Replication

Name	Type	Obje...	Status	Last Run	Last Result	Next Run	Target	Description
DC On_Demand Sandbox	up	2	Stopped	12 days ago	Success	After [DCS_HPH...	Advanced Single-Host 01	Created by GOODDE
DC SureBackup_Basic Single-Host	up	2	Stopped	12 days ago	Success	After [DCS_HPH...	Advanced Single-Host 01	Created by GOODDE
DC_HPHV02_Replication	on	1	Stopped	18 minutes...	Success	<not scheduled>	HPHV02	Created by GOODDE
DCS Backup Copy Job	opy	1	Stopped			<As new restor...	Backup Repository-Storage-...	Created by GOODDE
DCS_Azure Blob Backup		1	Stopped			<not scheduled>	Scale-out Backup Repository...	Created by GOODDE
DCS_Azure Blob with archive Back	opy	1	Stopped			<As new restor...	Scale-out Backup Repository...	Created by GOODDE
DCS_Azure Blob without archive B	opy	1	Stopped			<As new restor...	Scale-out Backup Repository...	Created by GOODDE
DCS_HPHV02 Backup		1	Stopped	12 days ago	Success	<not scheduled>	Backup Repository_HPHV02	Created by GOODDE
DCS_to_Storage-WIN Backup		1	Stopped			<not scheduled>	Backup Repository-Storage-...	Created by GOODDE
HPHV01 Excludes DCS Backup		1	Stopped			<not scheduled>	Backup Repository_HPHV02	Created by GOODDE
HPHV01_Storage-Win Backup	Hyper-V Backup	1	Stopped			<not scheduled>	Backup Repository_HPHV02	Created by GOODDE
Management_HPHV02 Backup	Hyper-V Backup	1	Stopped	12 days ago	Success	<not scheduled>	Backup Repository_HPHV02	Created by GOODDE
Management_ubuntu Immutable B...	Hyper-V Backup	1	Stopped	12 days ago	Success	<not scheduled>	Backup Repository_ubuntu2...	Created by GOODDE
Windows Server__Managed by age...	Windows Agent Policy	1	Disabled	Just now	N/A	N/A	Backup Repository_HPHV02	Created by GOODD
Windows Server__Managed by bac...	Windows Agent Backup	1	Stopped			<not scheduled>	Backup Repository-Storage-...	Created by GOODD

15 jobs selected

Connected to: localhost Build: 11.0.1.1261 P20220302 Enterprise Plus Edition NFR: 59 days remaining

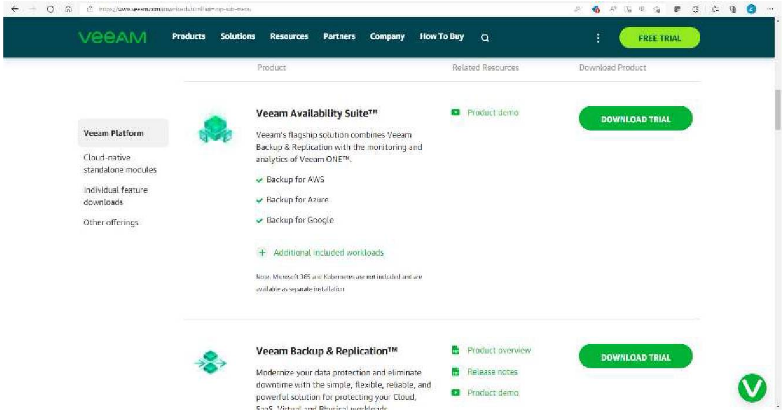
10. Make sure all jobs are disabled and close Veeam Backup & Replication Console.



Name	Type	Obje...	Status	Last Run	Last Result	Next Run	Target	Description
DC On_Demand Sandbox	Hyper-V SureBackup	2	Stopped	12 days ago	Success	<Disabled>	Advanced Single-Host 01	Created by GOODD
DC SureBackup_Basic Single-Host	Hyper-V SureBackup	2	Stopped	12 days ago	Success	<Disabled>	Advanced Single-Host 01	Created by GOODD
DC_HPHV02_Replication	Hyper-V Replication	1	Stopped	19 minutes...	Success	<not scheduled>	HPHV02	Created by GOODD
DCS Backup Copy Job	Hyper-V Backup Copy	1	Disabled			<Disabled>	Backup Repository-Storage-...	Created by GOODD
DCS_Azure Blob Backup	Hyper-V Backup	1	Stopped			<not scheduled>	Scale-out Backup Repository...	Created by GOODD
DCS_Azure Blob with archive Back...	Hyper-V Backup Copy	1	Disabled			<Disabled>	Scale-out Backup Repository...	Created by GOODD
DCS_Azure Blob without archive Ba...	Hyper-V Backup Copy	1	Disabled			<Disabled>	Scale-out Backup Repository...	Created by GOODD
DCS_HPHV02 Backup	Hyper-V Backup	1	Stopped	12 days ago	Success	<not scheduled>	Backup Repository_HPHV02	Created by GOODD
DCS_to_Storage-WIN Backup	Hyper-V Backup	1	Stopped			<not scheduled>	Backup Repository-Storage-...	Created by GOODD
HPHV01 Excludes DCS Backup	Hyper-V Backup	1	Stopped			<not scheduled>	Backup Repository_HPHV02	Created by GOODD
HPHV01_Storage-Win Backup	Hyper-V Backup	1	Stopped			<not scheduled>	Backup Repository_HPHV02	Created by GOODD
Management_HPHV02 Backup	Hyper-V Backup	1	Stopped	12 days ago	Success	<not scheduled>	Backup Repository_HPHV02	Created by GOODD
Management_ubuntu Immutable B...	Hyper-V Backup	1	Stopped	12 days ago	Success	<not scheduled>	Backup Repository_ubuntu2...	Created by GOODD
Windows Server__Managed by age...	Windows Agent Policy	1	Disabled	1 minute ago	N/A	N/A	Backup Repository_HPHV02	Created by GOODD
Windows Server__Managed by bac...	Windows Agent Backup	1	Stopped			<not scheduled>	Backup Repository-Storage-...	Created by GOODD

15 jobs selected   Connected to: localhost   Build: 11.0.1.1261 P20220302   Enterprise Plus Edition   NFR: 59 days remaining

11. Download the Veeam Backup and Replication v12 iso image file from the Veeam website. (Sign-in required).



Veeam Availability Suite™

Veeam's flagship solution combines Veeam Backup & Replication with the monitoring and analytics of Veeam ONE™.

- ✓ Backup for AWS
- ✓ Backup for Azure
- ✓ Backup for Google

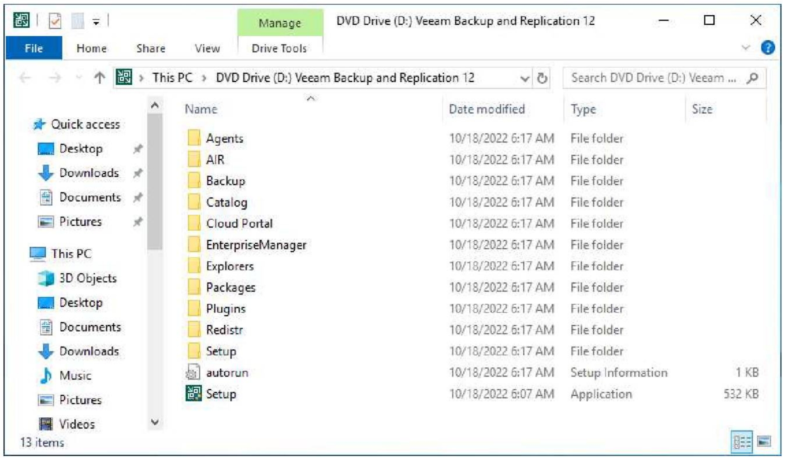
+ Additional included workloads

Note: Microsoft 365 and Kubernetes are not included and are available as separate installation

Veeam Backup & Replication™

Modernize your data protection and eliminate downtime with the simple, flexible, reliable, and powerful solution for protecting your Cloud, SaaS, Virtual and Physical workloads

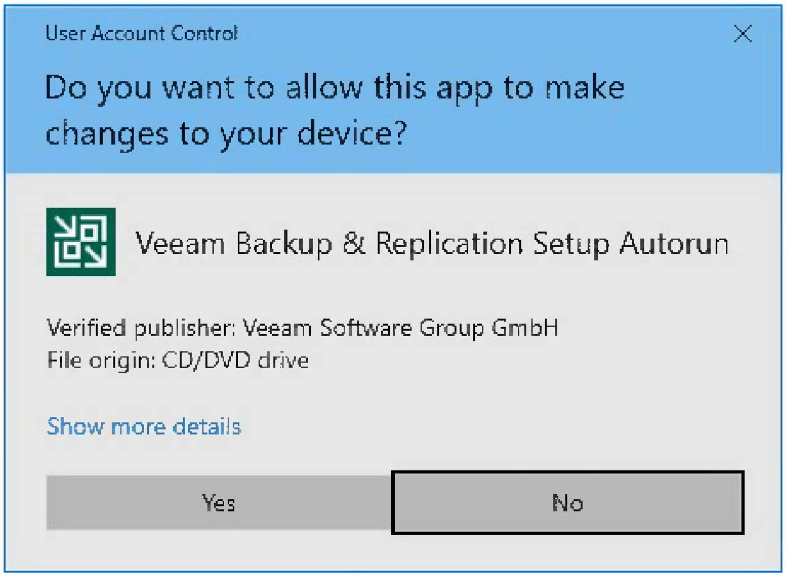
12. Mount the Veeam Backup & Replication v12 ISO image file.
13. Run Setup.exe.



Name	Date modified	Type	Size
Agents	10/18/2022 6:17 AM	File folder	
AIR	10/18/2022 6:17 AM	File folder	
Backup	10/18/2022 6:17 AM	File folder	
Catalog	10/18/2022 6:17 AM	File folder	
Cloud Portal	10/18/2022 6:17 AM	File folder	
EnterpriseManager	10/18/2022 6:17 AM	File folder	
Explorers	10/18/2022 6:17 AM	File folder	
Packages	10/18/2022 6:17 AM	File folder	
Plugins	10/18/2022 6:17 AM	File folder	
Redistr	10/18/2022 6:17 AM	File folder	
Setup	10/18/2022 6:17 AM	File folder	
autorun	10/18/2022 6:17 AM	Setup Information	1 KB
Setup	10/18/2022 6:07 AM	Application	532 KB

13 items

14. On the User Account Control page, click Yes.



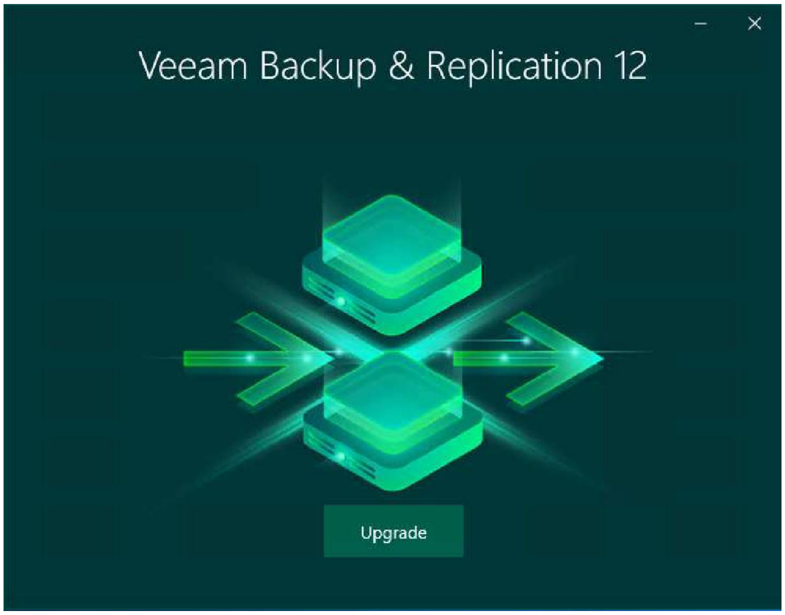
User Account Control

Do you want to allow this app to make changes to your device?

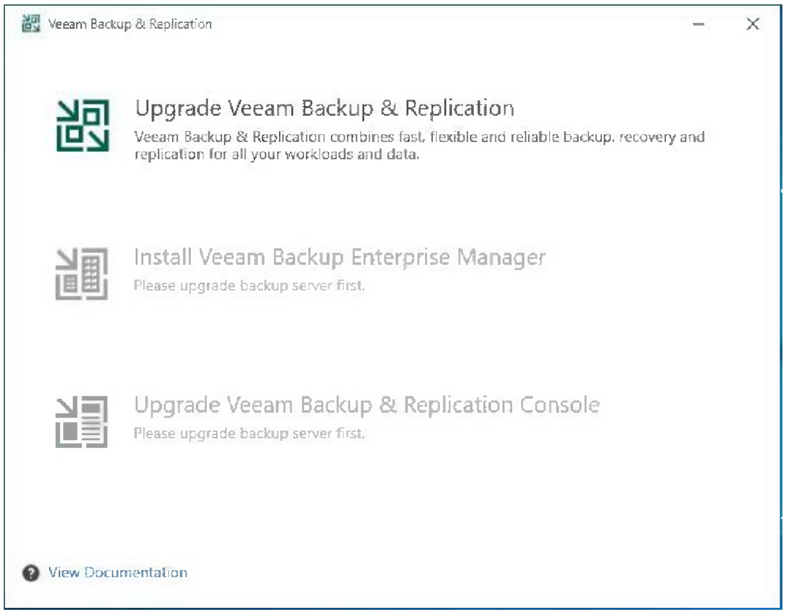
Veeam Backup & Replication Setup Autorun

Verified publisher: Veeam Software Group GmbH
File origin: CD/DVD drive

15. On the Veeam Backup & Replication 12 page, click Upgrade.



16. On the Veeam Backup & Replication page, select Upgrade Veeam Backup & Replication.



Upgrade Veeam Backup & Replication

Veeam Backup & Replication combines fast, flexible and reliable backup, recovery and replication for all your workloads and data.

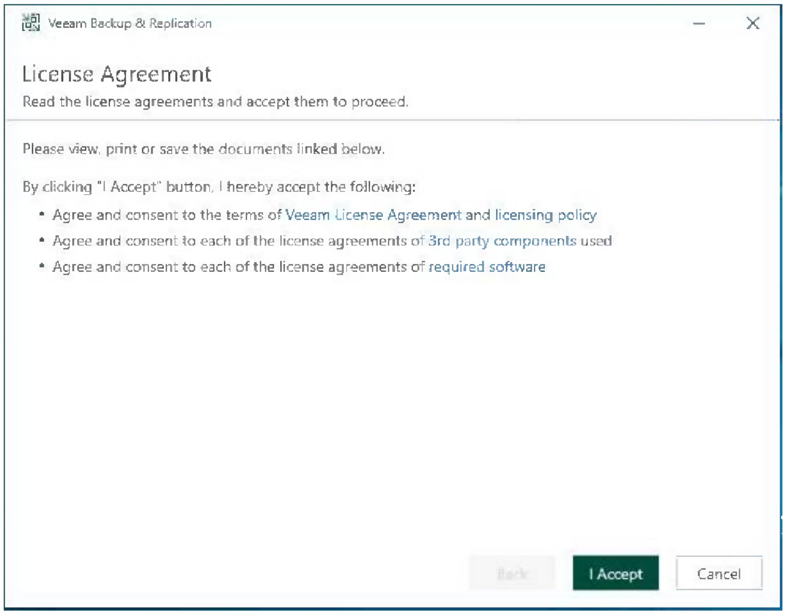
Install Veeam Backup Enterprise Manager

Please upgrade backup server first.

Upgrade Veeam Backup & Replication Console

Please upgrade backup server first.

17. On the License Agreement page, click I Accept.



License Agreement

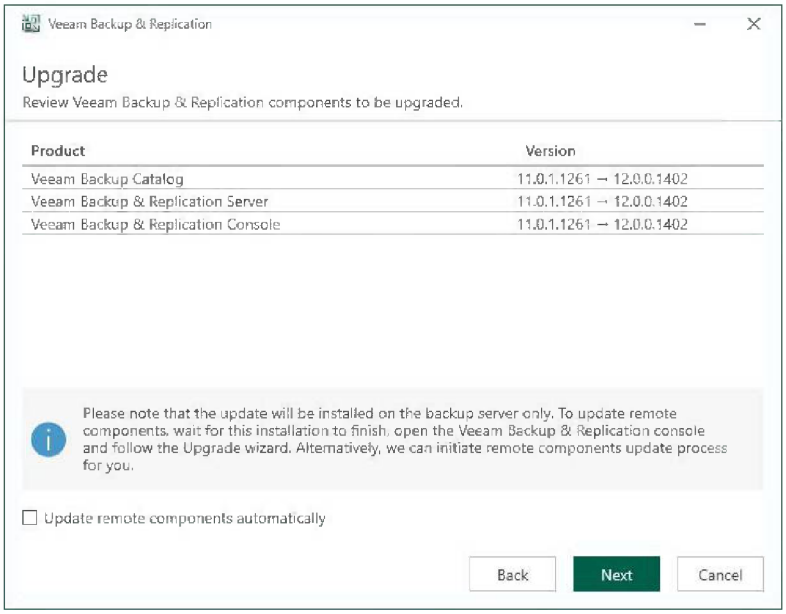
Read the license agreements and accept them to proceed.

Please view, print or save the documents linked below.

By clicking "I Accept" button, I hereby accept the following:

- Agree and consent to the terms of Veeam License Agreement and licensing policy
- Agree and consent to each of the license agreements of 3rd party components used
- Agree and consent to each of the license agreements of required software

18. On the Upgrade page, click Next.



Upgrade

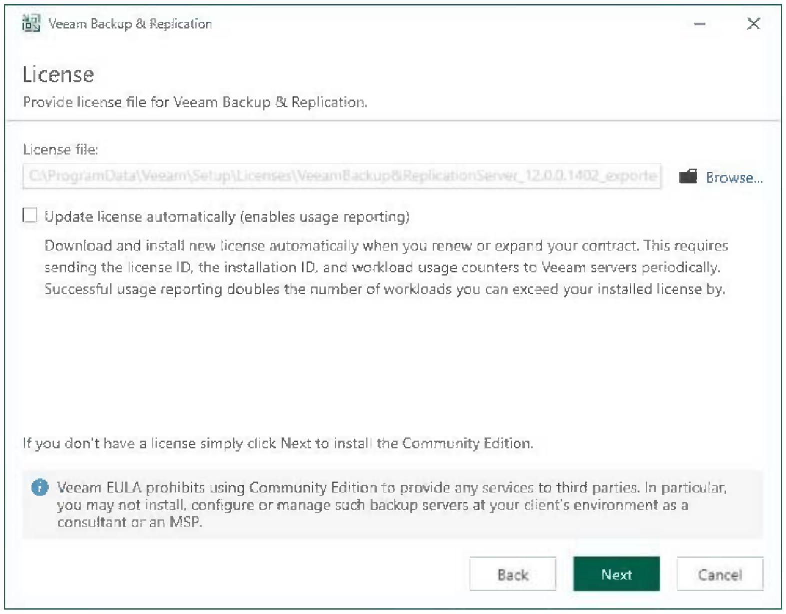
Review Veeam Backup & Replication components to be upgraded.

Product	Version
Veeam Backup Catalog	11.0.1.1261 → 12.0.0.1402
Veeam Backup & Replication Server	11.0.1.1261 → 12.0.0.1402
Veeam Backup & Replication Console	11.0.1.1261 → 12.0.0.1402

Please note that the update will be installed on the backup server only. To update remote components, wait for this installation to finish, open the Veeam Backup & Replication console and follow the Upgrade wizard. Alternatively, we can initiate remote components update process for you.

☐ Update remote components automatically

19. On the License page, click Browse.



License

Provide license file for Veeam Backup & Replication.

License file:

C:\ProgramData\Veeam\Setup\Licenses\VeeamBackup&ReplicationServer_12.0.0.1402_exporte

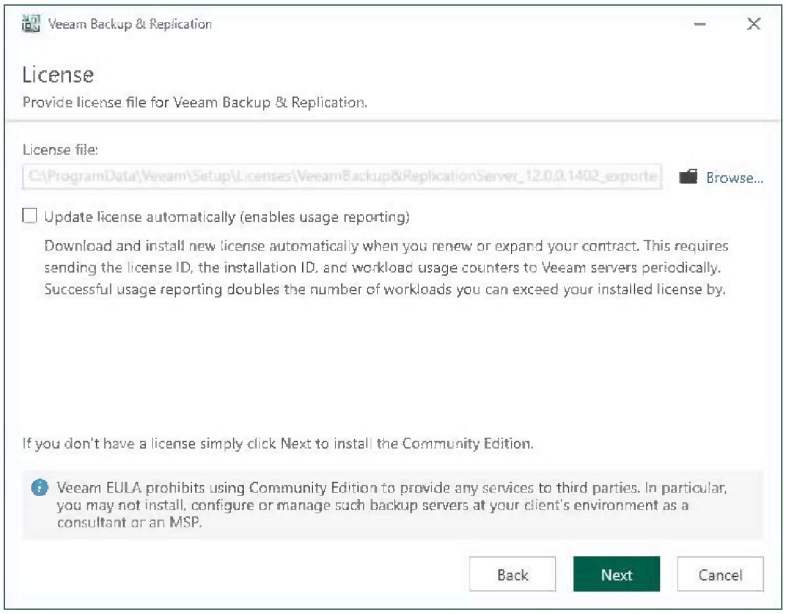
☐ Update license automatically (enables usage reporting)

Download and install new license automatically when you renew or expand your contract. This requires sending the license ID, the installation ID, and workload usage counters to Veeam servers periodically. Successful usage reporting doubles the number of workloads you can exceed your installed license by.

If you don't have a license simply click Next to install the Community Edition.

Veeam EULA prohibits using Community Edition to provide any services to third parties. In particular, you may not install, configure or manage such backup servers at your client's environment as a consultant or an MSP.

20. Select the Veeam Backup and Replication license file, and click Open.



Veeam Backup & Replication

License

Provide license file for Veeam Backup & Replication.

License file:

C:\ProgramData\Veeam\Setup\Licenses\VeeamBackup&ReplicationServer_12.0.0.1402_exporte

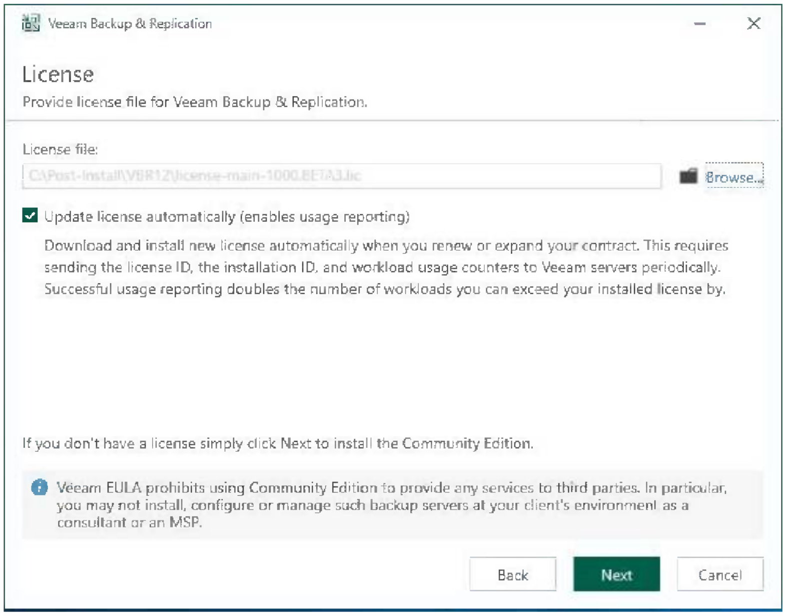
□ Update license automatically (enables usage reporting)

Download and install new license automatically when you renew or expand your contract. This requires sending the license ID, the installation ID, and workload usage counters to Veeam servers periodically. Successful usage reporting doubles the number of workloads you can exceed your installed license by.

If you don't have a license simply click Next to install the Community Edition.

Veeam EULA prohibits using Community Edition to provide any services to third parties. In particular, you may not install, configure or manage such backup servers at your client's environment as a consultant or an MSP.

21. Select Update license automatically (enable usage reporting) on the License page and click Next.



Veeam Backup & Replication

License

Provide license file for Veeam Backup & Replication.

License file:

C:\Post-Install\VBR12\license-main-1000.BETA3.lic

☑ Update license automatically (enables usage reporting)

Download and install new license automatically when you renew or expand your contract. This requires sending the license ID, the installation ID, and workload usage counters to Veeam servers periodically. Successful usage reporting doubles the number of workloads you can exceed your installed license by.

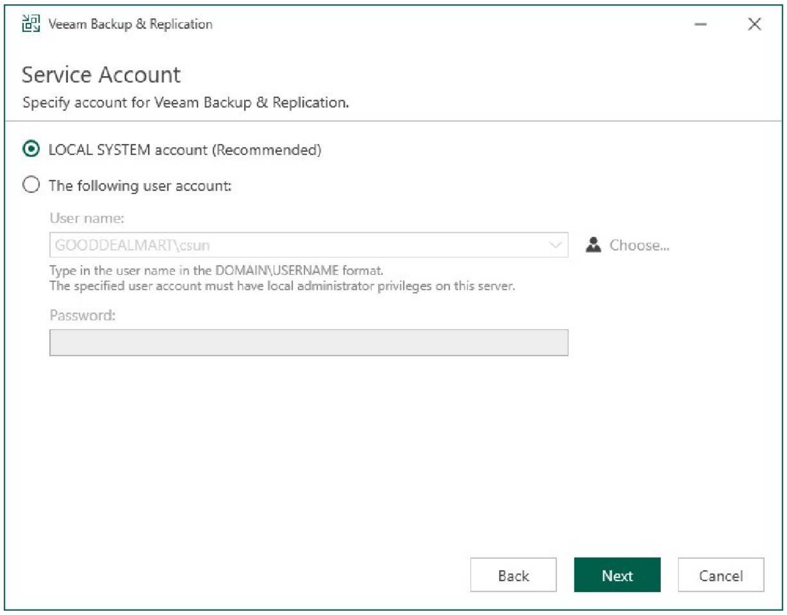
If you don't have a license simply click Next to install the Community Edition.

Veeam EULA prohibits using Community Edition to provide any services to third parties. In particular, you may not install, configure or manage such backup servers at your client's environment as a consultant or an MSP.

22. Select LOCAL SYSTEM account or specify another user account on the Service Account page and click Next.

Note:

If you would like to use the specified user account, the user account must be a member of the Administrators group on the Veeam Backup & Replication machine. Also, it must have db_owner rights for the configuration database.



Veeam Backup & Replication

Service Account

Specify account for Veeam Backup & Replication.

● LOCAL SYSTEM account (Recommended)

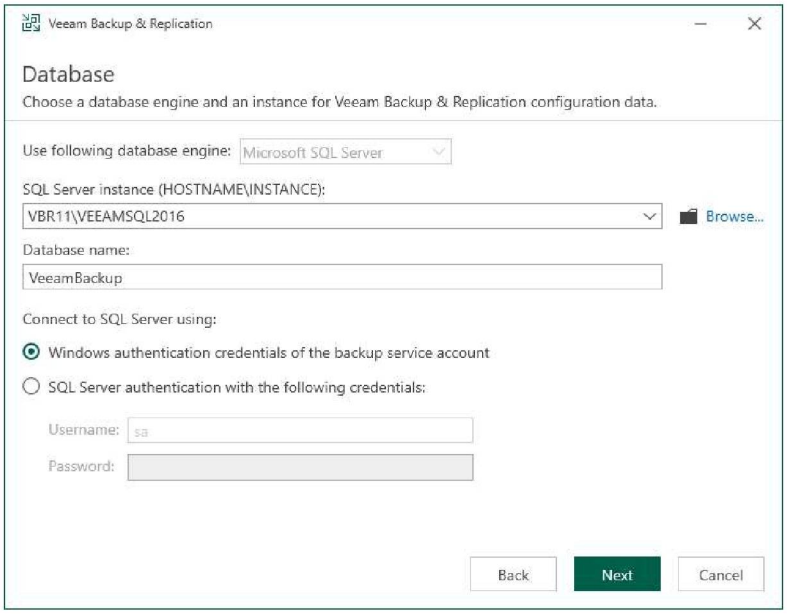
○ The following user account:

User name: GOODDEALMART\csun

Type in the user name in the DOMAIN\USERNAME format.
The specified user account must have local administrator privileges on this server.

Password:

23. On the Database page, click Next.



Veeam Backup & Replication

Database

Choose a database engine and an instance for Veeam Backup & Replication configuration data.

Use following database engine: Microsoft SQL Server

SQL Server instance (HOSTNAME\INSTANCE): VBR11\VEEAMSQL2016

Database name: VeeamBackup

Connect to SQL Server using:

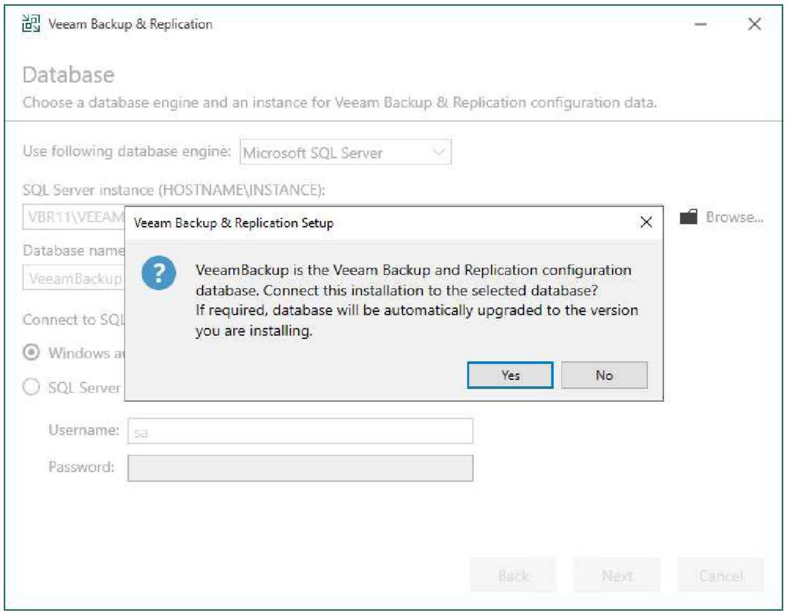
● Windows authentication credentials of the backup service account

○ SQL Server authentication with the following credentials:

Username: sa

Password:

24. Click Yes on the question pop-up message. Veeam will automatically upgrade the database to the version you are installing.



Veeam Backup & Replication

Database

Choose a database engine and an instance for Veeam Backup & Replication configuration data.

Use following database engine: Microsoft SQL Server

SQL Server instance (HOSTNAME\INSTANCE): VBR11\VEEAM

Database name: VeeamBackup

Connect to SQL

● Windows a

○ SQL Server

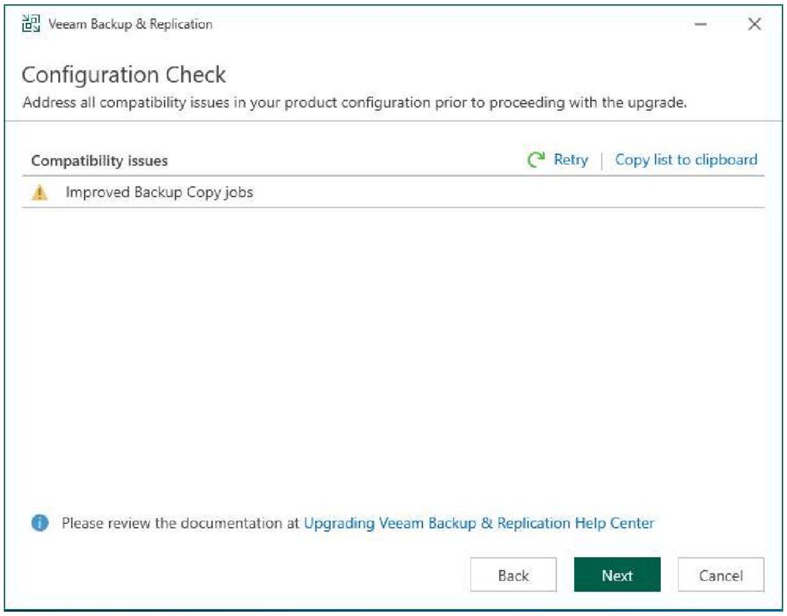
Username: sa

Password:

Veeam Backup & Replication Setup

VeeamBackup is the Veeam Backup and Replication configuration database. Connect this installation to the selected database?
If required, database will be automatically upgraded to the version you are installing.

25. If the Configuration Check page returns errors, resolve them before upgrading. If the check produces warning or information messages, you can proceed with the upgrade and deal with them later.
26. Click Next.



Veeam Backup & Replication

Configuration Check

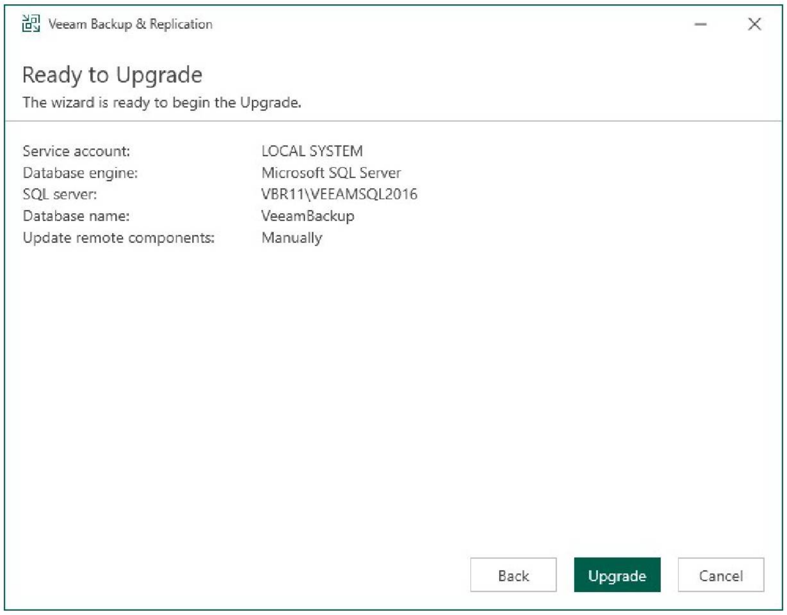
Address all compatibility issues in your product configuration prior to proceeding with the upgrade.

Compatibility issues

⚠ Improved Backup Copy jobs

Please review the documentation at Upgrading Veeam Backup & Replication Help Center

27. On the Ready to Upgrade page, click Upgrade.

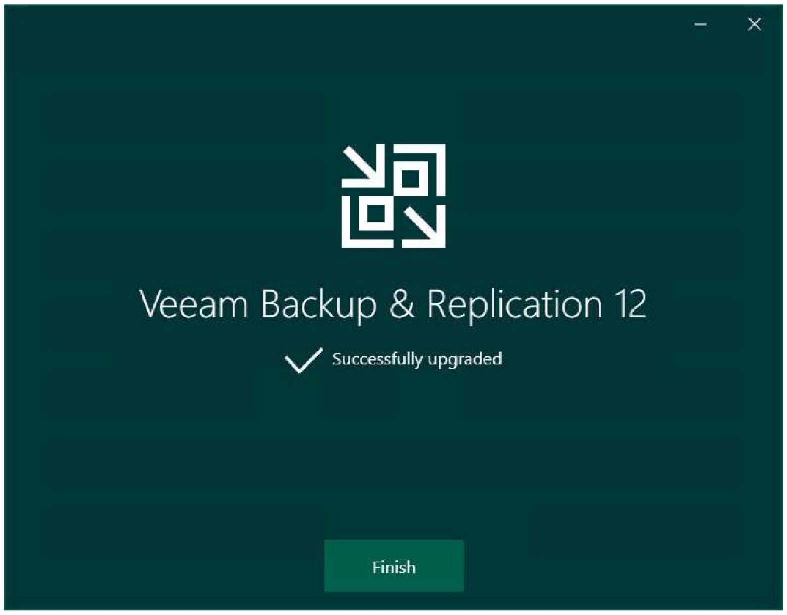


Ready to Upgrade

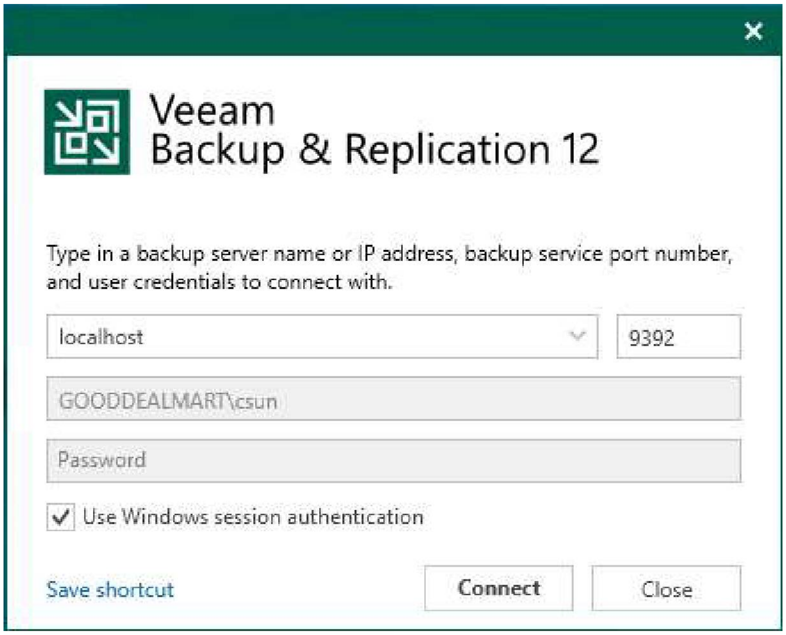
The wizard is ready to begin the Upgrade.

Service account: LOCAL SYSTEM
Database engine: Microsoft SQL Server
SQL server: VBR11\VEEAMSQL2016
Database name: VeeamBackup
Update remote components: Manually

28. On the Veeam Backup & Replication 12 successfully upgraded page, click Finish.



29. Open Veeam Backup & Replication management console and click Connect.



Veeam
Backup & Replication 12

Type in a backup server name or IP address, backup service port number, and user credentials to connect with.

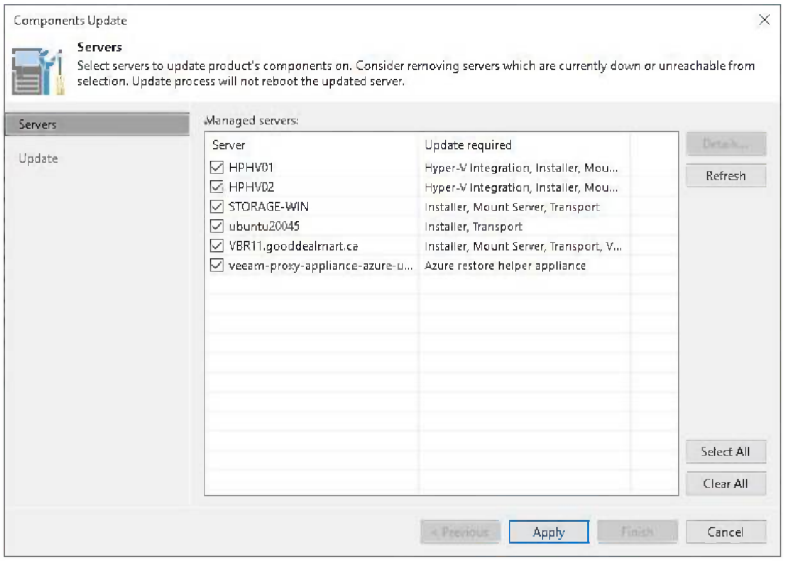
localhost | 9392

GOODDEALMART\csun

Password

☑ Use Windows session authentication

30. Select the all servers checkbox on the Components Update page and click Apply.



Components Update

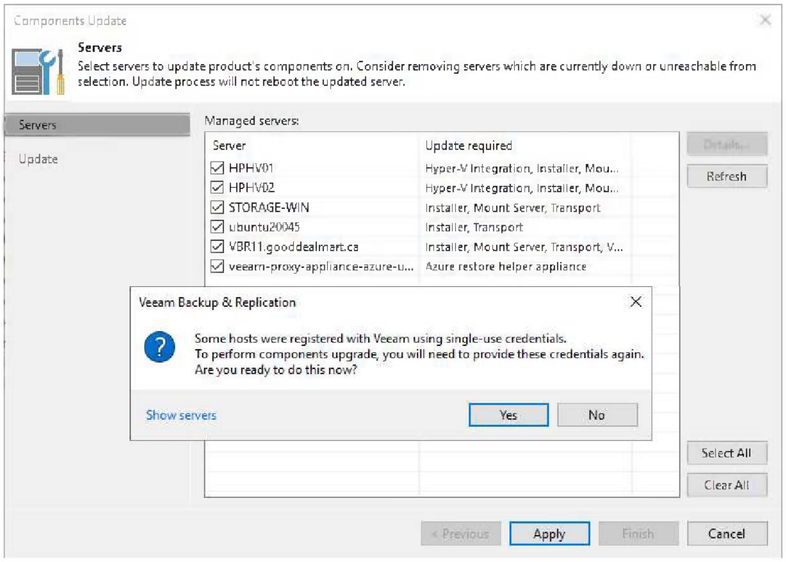
Servers

Select servers to update product's components on. Consider removing servers which are currently down or unreachable from selection. Update process will not reboot the updated server.

Managed servers:

Server	Update required
☑ HPHV01	Hyper-V Integration, Installer, Mou...
☑ HPHV02	Hyper-V Integration, Installer, Mou...
☑ STORAGE-WIN	Installer, Mount Server, Transport
☑ ubuntu20045	Installer, Transport
☑ VBR11.gooddealmart.ca	Installer, Mount Server, Transport, V...
☑ veeam-proxy-appliance-azure-u...	Azure restore helper appliance

31. Click Show servers on the provide signal-use credentials question page.



Servers

Select servers to update product's components on. Consider removing servers which are currently down or unreachable from selection. Update process will not reboot the updated server.

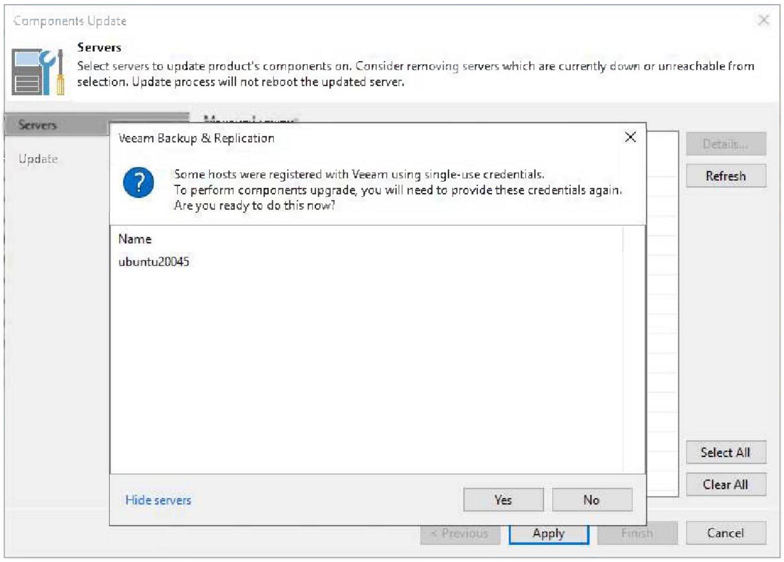
Managed servers:

Server	Update required
☑ HPHV01	Hyper-V Integration, Installer, Mou...
☑ HPHV02	Hyper-V Integration, Installer, Mou...
☑ STORAGE-WIN	Installer, Mount Server, Transport
☑ ubuntu20045	Installer, Transport
☑ VBR11.gooddealmart.ca	Installer, Mount Server, Transport, V...
☑ veeam-proxy-appliance-azure-u...	Azure restore helper appliance

Veeam Backup & Replication

Some hosts were registered with Veeam using single-use credentials.
To perform components upgrade, you will need to provide these credentials again.
Are you ready to do this now?

32. Review the Server listing and click Yes.



Servers

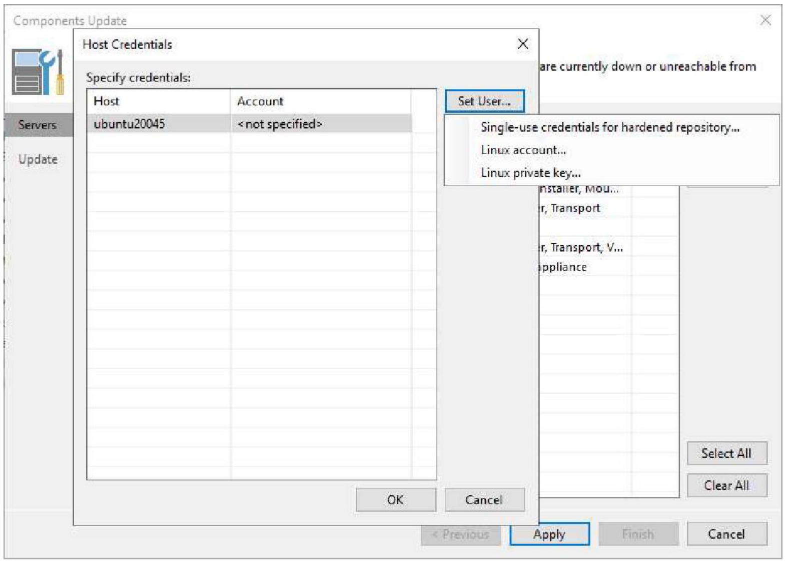
Select servers to update product's components on. Consider removing servers which are currently down or unreachable from selection. Update process will not reboot the updated server.

Veeam Backup & Replication

Some hosts were registered with Veeam using single-use credentials.
To perform components upgrade, you will need to provide these credentials again.
Are you ready to do this now?

Name
ubuntu20045

33. On the Host Credentials page, select the host, click Set User and select Singal-use credentials for the hardened repository.



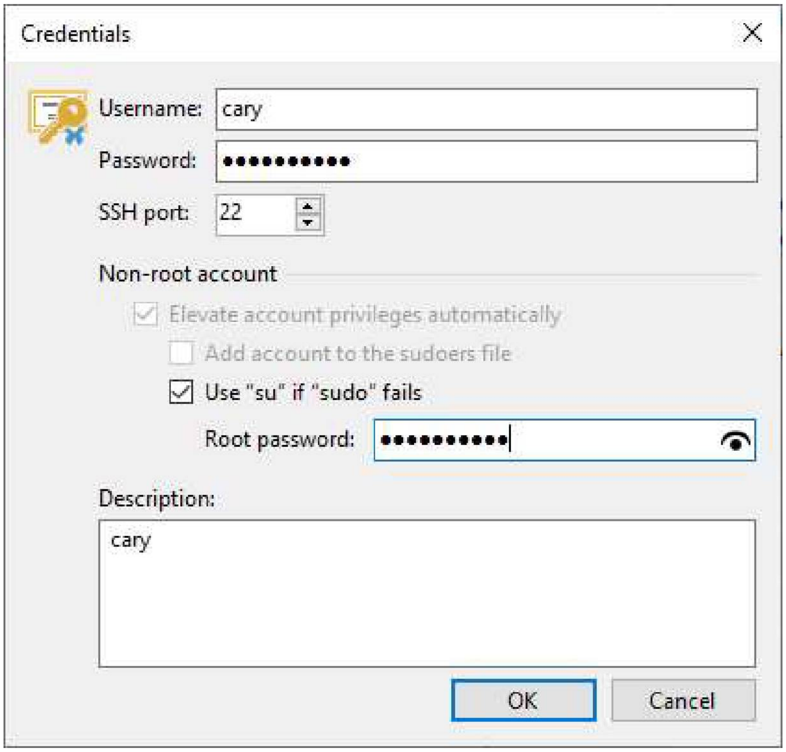
Components Update

Host Credentials

Specify credentials:

Host	Account
ubuntu20045	<not specified>

34. Enter your credential information and click OK.



Credentials

Username: cary

Password: ●●●●●●●●●●

SSH port: 22

Non-root account

☑ Elevate account privileges automatically

□ Add account to the sudoers file

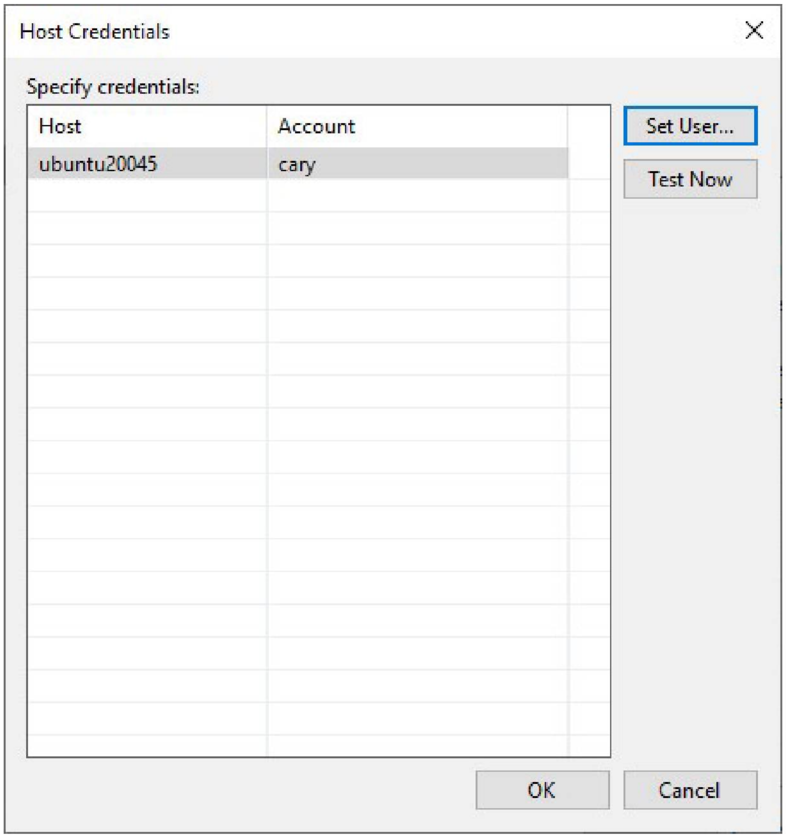
☑ Use "su" if "sudo" fails

Root password: ●●●●●●●●●●

Description:

cary

35. Click Test Now on the Host Credentials page.

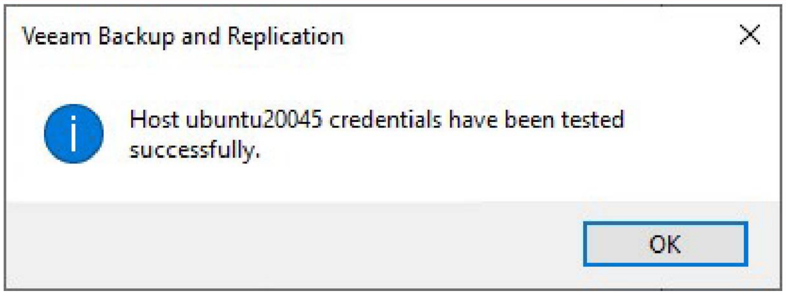


Host Credentials

Specify credentials:

Host	Account
ubuntu20045	cary

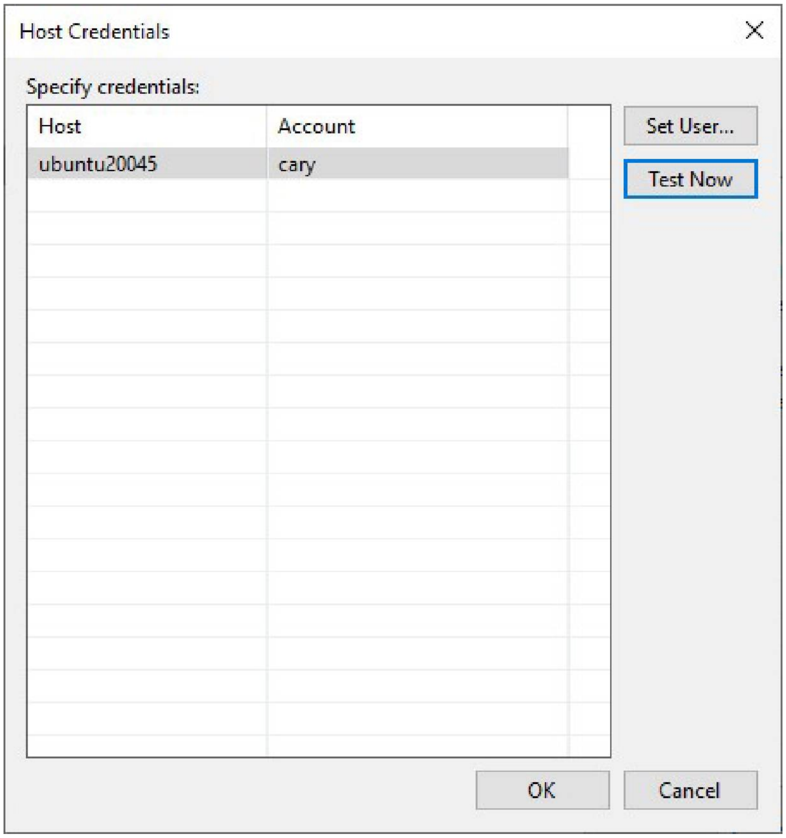
36. Ensure the credential has been tested successfully and click OK.



Veeam Backup and Replication

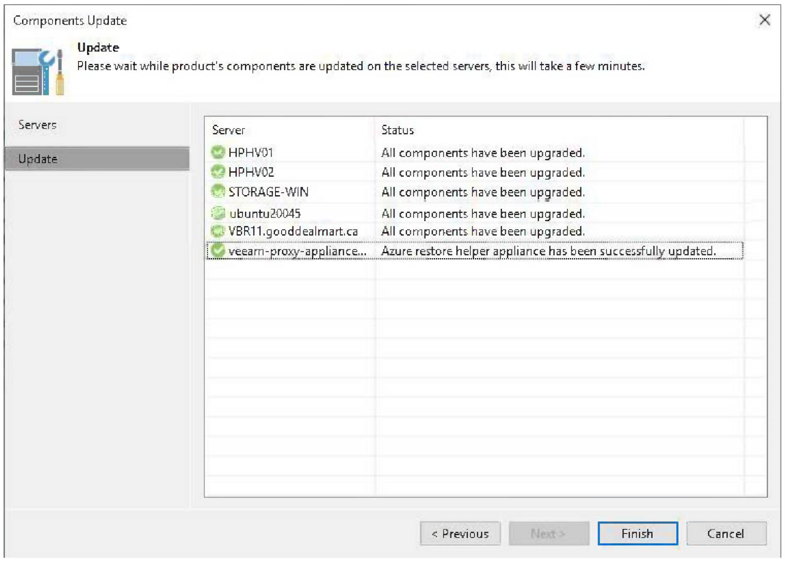
Host ubuntu20045 credentials have been tested successfully.

37. Click OK on the Host Credentials page.



Host	Account
ubuntu20045	cary

38. Ensure the components update successfully for selected servers and click Finish.



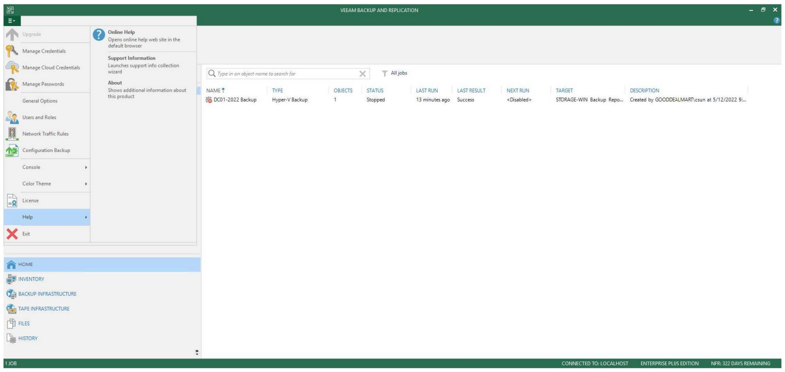
Components Update

Update

Please wait while product's components are updated on the selected servers, this will take a few minutes.

Server	Status
HPHV01	All components have been upgraded.
HPHV02	All components have been upgraded.
STORAGE-WIN	All components have been upgraded.
ubuntu20045	All components have been upgraded.
VBR11.gooddealmart.ca	All components have been upgraded.
veeam-proxy-appliance...	Azure restore helper appliance has been successfully updated.

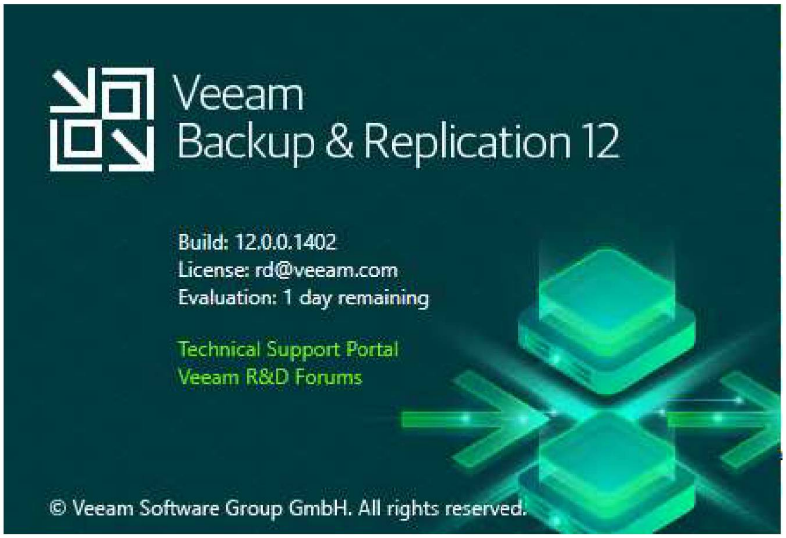
39. Drop down the main menu, select Help, and click About to check Veeam Backup & Replication version.



NAME	TYPE	OBJECTS	STATUS	LAST RUN	LAST RESULT	NEXT RUN	TARGET	DESCRIPTION
DC01-2022 Backup	Hyper-V Backup	1	Stopped	13 minutes ago	Success	<Disabled>	STORAGE-WIN Backup Repo...	Created by GOODDEALMART\csun at 5/12/2022 9:...

1 JOB   CONNECTED TO: LOCALHOST   ENTERPRISE PLUS EDITION   NFR: 322 DAYS REMAINING

40. Ensure the existing Veeam Backup and Replication version is upgraded.



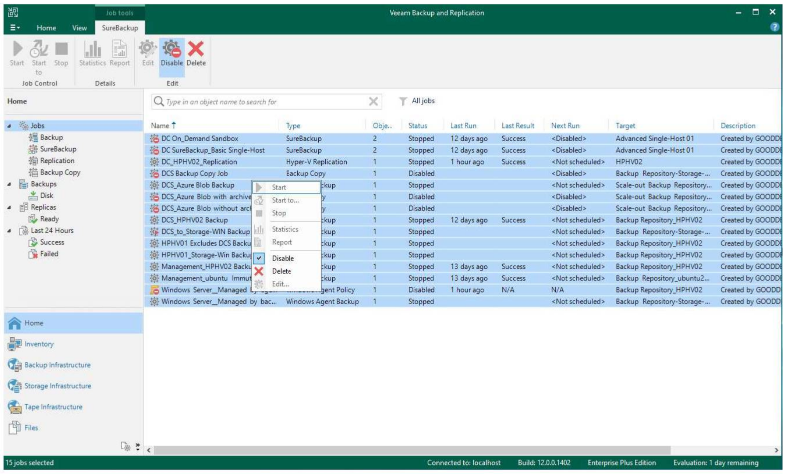
Veeam
Backup & Replication 12

Build: 12.0.0.1402
License: rd@veeam.com
Evaluation: 1 day remaining

Technical Support Portal
Veeam R&D Forums

© Veeam Software Group GmbH. All rights reserved.

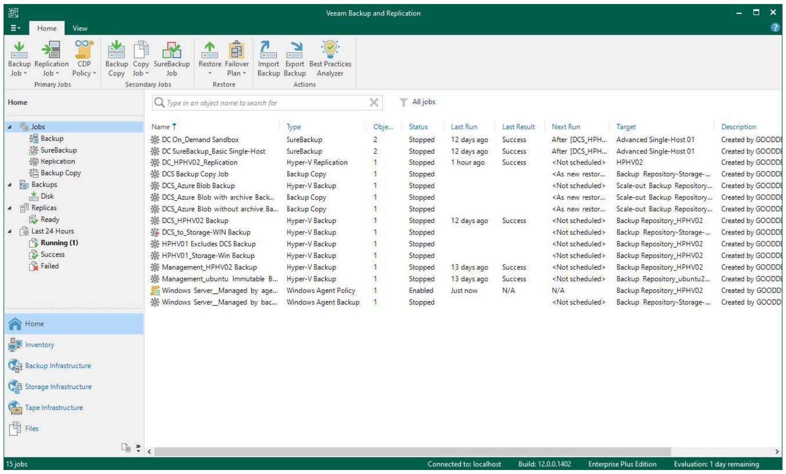
41. On the Home page, select Jobs.
42. Right-click jobs and unselect Disable to enable all jobs.



Name	Type	Obje...	Status	Last Run	Last Result	Next Run	Target	Description
DC On_Demand Sandbox	SureBackup	2	Stopped	12 days ago	Success	<Disabled>	Advanced Single-Host 01	Created by GOODD
DC SureBackup_Basic Single-Host	SureBackup	2	Stopped	12 days ago	Success	<Disabled>	Advanced Single-Host 01	Created by GOODD
DC_HPHV02_Replication	Hyper-V Replication	1	Stopped	1 hour ago	Success	<Not scheduled>	HPHV02	Created by GOODD
DCS Backup Copy Job	Backup Copy	1	Disabled			<Disabled>	Backup Repository-Storage-...	Created by GOODD
DCS_Azure Blob Backup	ckup	1	Stopped			<Not scheduled>	Scale-out Backup Repository...	Created by GOODD
DCS_Azure Blob with archive	y	1	Disabled			<Disabled>	Scale-out Backup Repository...	Created by GOODD
DCS_Azure Blob without arc	y	1	Disabled			<Disabled>	Scale-out Backup Repository...	Created by GOODD
DCS_HPHV02 Backup	ckup	1	Stopped	12 days ago	Success	<Not scheduled>	Backup Repository_HPHV02	Created by GOODD
DCS_to_Storage-WIN Backup	ckup	1	Stopped			<Not scheduled>	Backup Repository-Storage-...	Created by GOODD
HPHV01 Excludes DCS Backu	ckup	1	Stopped			<Not scheduled>	Backup Repository_HPHV02	Created by GOODD
HPHV01_Storage-Win Backu	ckup	1	Stopped			<Not scheduled>	Backup Repository_HPHV02	Created by GOODD
Management_HPHV02 Backu	ckup	1	Stopped	13 days ago	Success	<Not scheduled>	Backup Repository_HPHV02	Created by GOODD
Management_ubuntu Immut	ckup	1	Stopped	13 days ago	Success	<Not scheduled>	Backup Repository_ubuntu2...	Created by GOODD
Windows Server__Managed	gent Policy	1	Disabled	1 hour ago	N/A	N/A	Backup Repository_HPHV02	Created by GOODD
Windows Server__Managed by bac...	Windows Agent Backup	1	Stopped			<Not scheduled>	Backup Repository-Storage-...	Created by GOODD

15 jobs selected   Connected to: localhost   Build: 12.0.0.1402   Enterprise Plus Edition   Evaluation: 1 day remaining

43. Ensure all jobs are enabled.



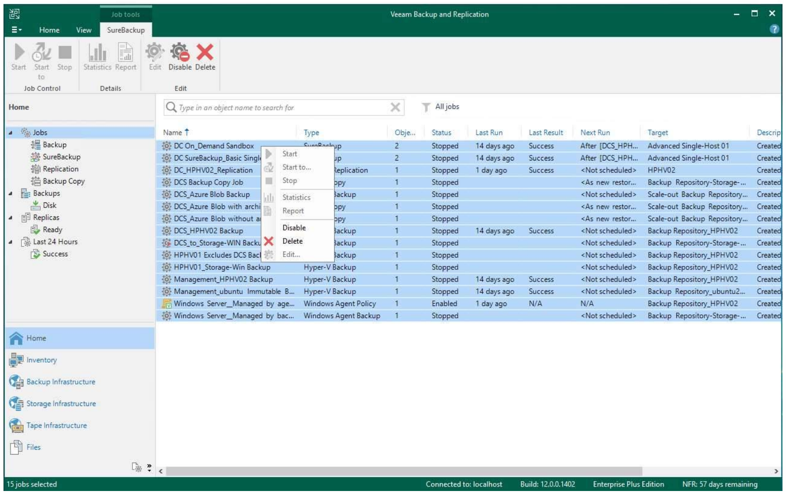
Name	Type	Obje...	Status	Last Run	Last Result	Next Run	Target	Description
DC On_Demand Sandbox	SureBackup	2	Stopped	12 days ago	Success	After [DCS_HPH...	Advanced Single-Host 01	Created by GOODD
DC SureBackup_Basic Single-Host	SureBackup	2	Stopped	12 days ago	Success	After [DCS_HPH...	Advanced Single-Host 01	Created by GOODD
DC_HPHV02_Replication	Hyper-V Replication	1	Stopped	1 hour ago	Success	<Not scheduled>	HPHV02	Created by GOODD
DCS Backup Copy Job	Backup Copy	1	Stopped			<As new restor...	Backup Repository-Storage-...	Created by GOODD
DCS_Azure Blob Backup	Hyper-V Backup	1	Stopped			<Not scheduled>	Scale-out Backup Repository...	Created by GOODD
DCS_Azure Blob with archive Back...	Backup Copy	1	Stopped			<As new restor...	Scale-out Backup Repository...	Created by GOODD
DCS_Azure Blob without archive Ba...	Backup Copy	1	Stopped			<As new restor...	Scale-out Backup Repository...	Created by GOODD
DCS_HPHV02 Backup	Hyper-V Backup	1	Stopped	12 days ago	Success	<Not scheduled>	Backup Repository_HPHV02	Created by GOODD
DCS_to_Storage-WIN Backup	Hyper-V Backup	1	Stopped			<Not scheduled>	Backup Repository-Storage-...	Created by GOODD
HPHV01 Excludes DCS Backup	Hyper-V Backup	1	Stopped			<Not scheduled>	Backup Repository_HPHV02	Created by GOODD
HPHV01_Storage-Win Backup	Hyper-V Backup	1	Stopped			<Not scheduled>	Backup Repository_HPHV02	Created by GOODD
Management_HPHV02 Backup	Hyper-V Backup	1	Stopped	13 days ago	Success	<Not scheduled>	Backup Repository_HPHV02	Created by GOODD
Management_ubuntu Immutable B...	Hyper-V Backup	1	Stopped	13 days ago	Success	<Not scheduled>	Backup Repository_ubuntu2...	Created by GOODD
Windows Server__Managed by age...	Windows Agent Policy	1	Enabled	Just now	N/A	N/A	Backup Repository_HPHV02	Created by GOODD
Windows Server__Managed by bac...	Windows Agent Backup	1	Stopped			<Not scheduled>	Backup Repository-Storage-...	Created by GOODD

15 jobs

Connected to: localhost   Build: 12.0.0.1402   Enterprise Plus Edition   Evaluation: 1 day remaining

Migrate the Existing Veeam Backup and Replication to the new server with PostgreSQL

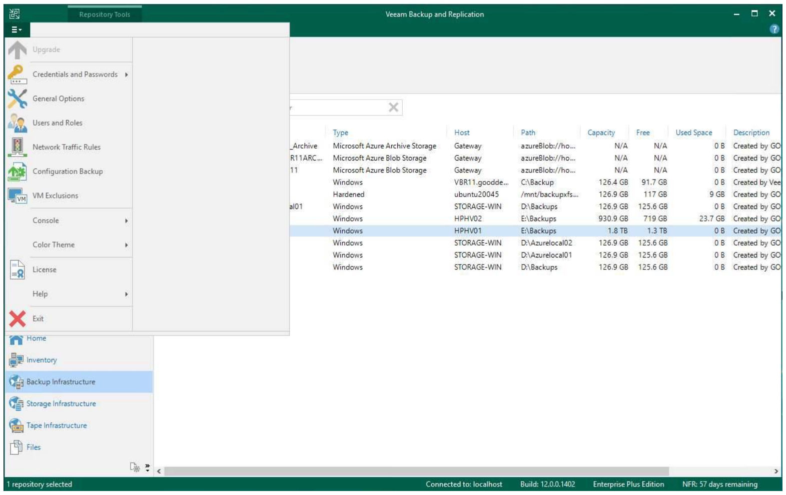
PostgreSQL is free and has no size limit or compute restrictions has improved performance over SQL Express.

Instructions	Screenshot (if applicable)
1. Log in to the existing Veeam Backup and replication manager server. 2. Open the Veeam Backup & Replication Console. 3. Select and right-click all jobs. 4. Select Disable.	

Name	Type	Obje...	Status	Last Run	Last Result	Next Run	Target	Descrip
DC On_Demand Sandbox	SureBackup	2	Stopped	14 days ago	Success	After [DCS_HPH...	Advanced Single-Host 01	Created
DC SureBackup_Basic Singl	up	2	Stopped	14 days ago	Success	After [DCS_HPH...	Advanced Single-Host 01	Created
DC_HPHV02_Replication	eplication	1	Stopped	1 day ago	Success	<Not scheduled>	HPHV02	Created
DCS Backup Copy Job	opy	1	Stopped			<As new restor...	Backup Repository-Storage-...	Created
DCS_Azure Blob Backup	ackup	1	Stopped			<Not scheduled>	Scale-out Backup Repository...	Created
DCS_Azure Blob with archi	opy	1	Stopped			<As new restor...	Scale-out Backup Repository...	Created
DCS_Azure Blob without a	opy	1	Stopped			<As new restor...	Scale-out Backup Repository...	Created
DCS_HPHV02 Backup	ackup	1	Stopped	14 days ago	Success	<Not scheduled>	Backup Repository_HPHV02	Created
DCS_to_Storage-WIN Backu	ackup	1	Stopped			<Not scheduled>	Backup Repository-Storage-...	Created
HPHV01 Excludes DCS Bacl	ackup	1	Stopped			<Not scheduled>	Backup Repository_HPHV02	Created
HPHV01_Storage-Win Backup	Hyper-V Backup	1	Stopped			<Not scheduled>	Backup Repository_HPHV02	Created
Management_HPHV02 Backup	Hyper-V Backup	1	Stopped	14 days ago	Success	<Not scheduled>	Backup Repository_HPHV02	Created
Management_ubuntu Immutable B...	Hyper-V Backup	1	Stopped	14 days ago	Success	<Not scheduled>	Backup Repository_ubuntu2...	Created
Windows Server_Managed by age...	Windows Agent Policy	1	Enabled	1 day ago	N/A	N/A	Backup Repository_HPHV02	Created
Windows Server_Managed by bac...	Windows Agent Backup	1	Stopped			<Not scheduled>	Backup Repository-Storage-...	Created

15 jobs selected   Connected to: localhost   Build: 12.0.0.1402   Enterprise Plus Edition   NFR: 57 days remaining

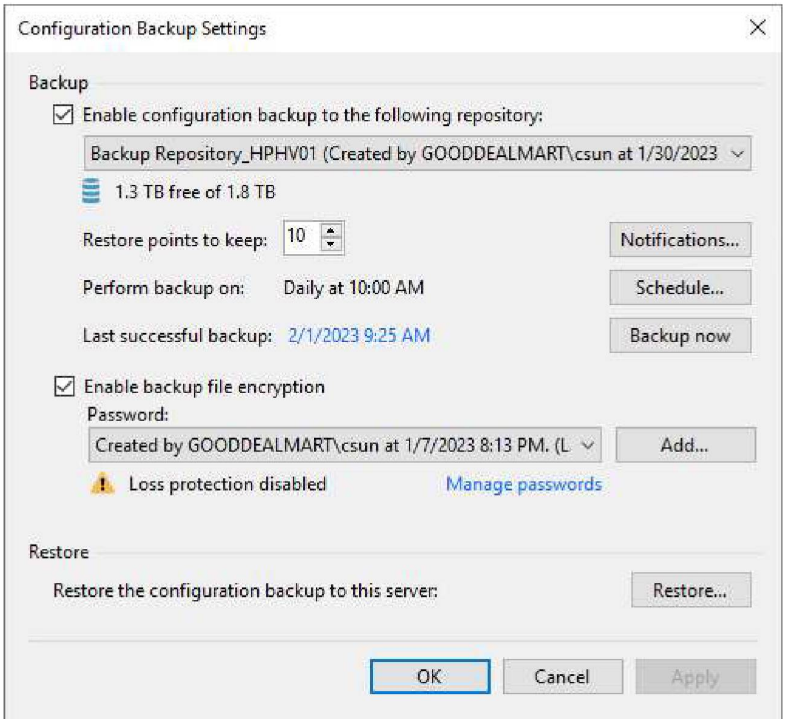
5. Drop down the main menu and select Configuration Backup.



	Type	Host	Path	Capacity	Free	Used Space	Description
_Archive	Microsoft Azure Archive Storage	Gateway	azureBlob://ho...	N/A	N/A	0 B	Created by GO
R11ARC...	Microsoft Azure Blob Storage	Gateway	azureBlob://ho...	N/A	N/A	0 B	Created by GO
11	Microsoft Azure Blob Storage	Gateway	azureBlob://ho...	N/A	N/A	0 B	Created by GO
	Windows	VBR11.goodde...	C:\Backup	126.4 GB	91.7 GB	0 B	Created by Vee
	Hardened	ubuntu20045	/mnt/backupxfs...	126.9 GB	117 GB	9 GB	Created by GO
al01	Windows	STORAGE-WIN	D:\Backups	126.9 GB	125.6 GB	0 B	Created by GO
	Windows	HPHV02	E:\Backups	930.9 GB	719 GB	23.7 GB	Created by GO
	Windows	HPHV01	E:\Backups	1.8 TB	1.3 TB	0 B	Created by GO
	Windows	STORAGE-WIN	D:\Azurelocal02	126.9 GB	125.6 GB	0 B	Created by GO
	Windows	STORAGE-WIN	D:\Azurelocal01	126.9 GB	125.6 GB	0 B	Created by GO
	Windows	STORAGE-WIN	D:\Backups	126.9 GB	125.6 GB	0 B	Created by GO

1 repository selected   Connected to: localhost   Build: 12.0.0.1402   Enterprise Plus Edition   NFR: 57 days remaining

6. Click Backup now on the Configuration Backup Settings page.



Configuration Backup Settings

Backup

☑ Enable configuration backup to the following repository:

Backup Repository_HPHV01 (Created by GOODDEALMART\csun at 1/30/2023

1.3 TB free of 1.8 TB

Restore points to keep: 10

Perform backup on: Daily at 10:00 AM

Last successful backup: 2/1/2023 9:25 AM

☑ Enable backup file encryption

Password:

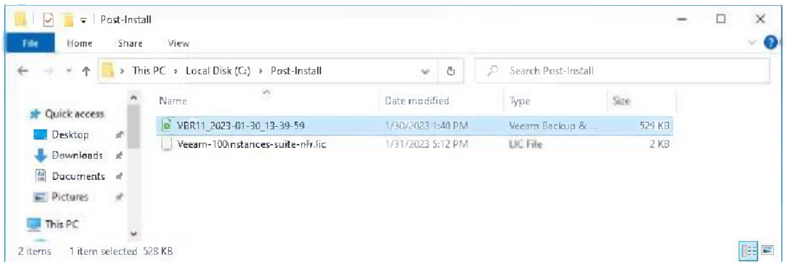
Created by GOODDEALMART\csun at 1/7/2023 8:13 PM. (L

Loss protection disabled

Restore

Restore the configuration backup to this server:

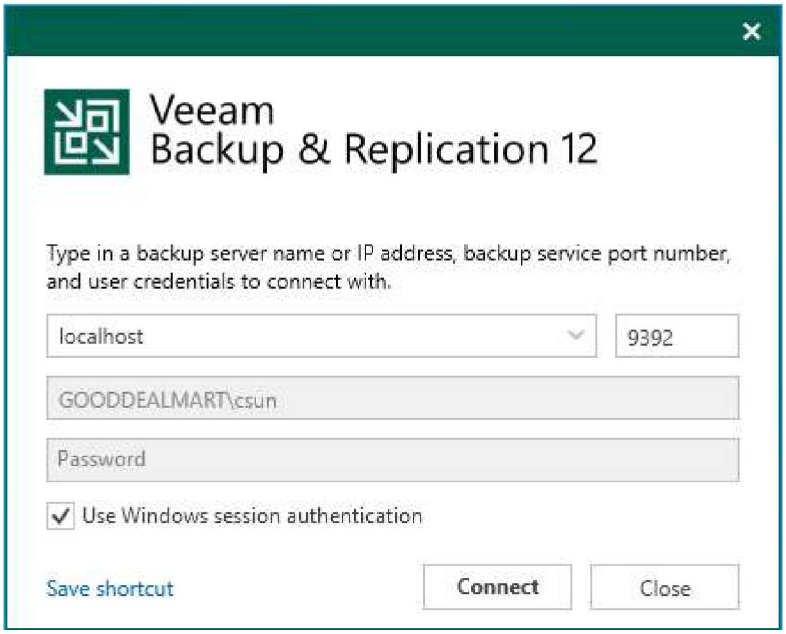
7. Copy the configuration file from the backup repository to the new Backup and Replication manager server.



Name	Date modified	Type	Size
VBR11_2023-01-30_13-39-59	1/30/2023 1:40 PM	Veeam Backup & ...	529 KB
Veeam-100instances-suite-nfr.lic	1/31/2023 5:12 PM	LIC File	2 KB

2 items 1 item selected 528 KB

8. Log in to the new Veeam Backup and Replication manager server.
9. Open the Veeam Backup & Replication Console, and click Connect.



Type in a backup server name or IP address, backup service port number, and user credentials to connect with.

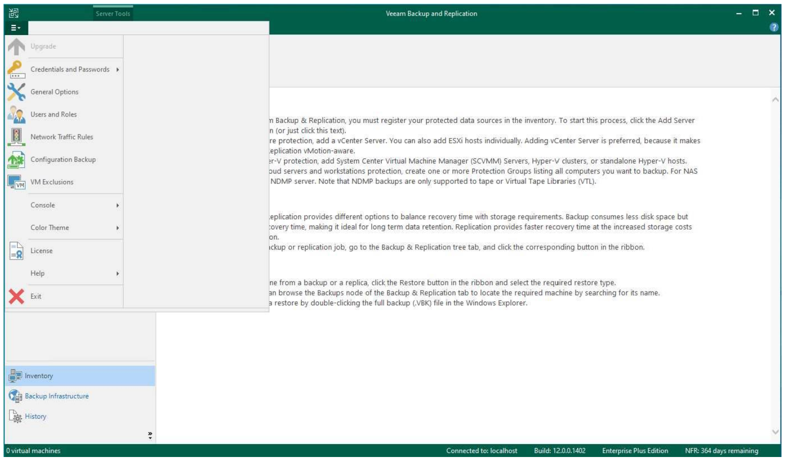
localhost 9392

GOODDEALMART\csun

Password

☑ Use Windows session authentication

10. Drop down the main menu and select Configuration Backup.



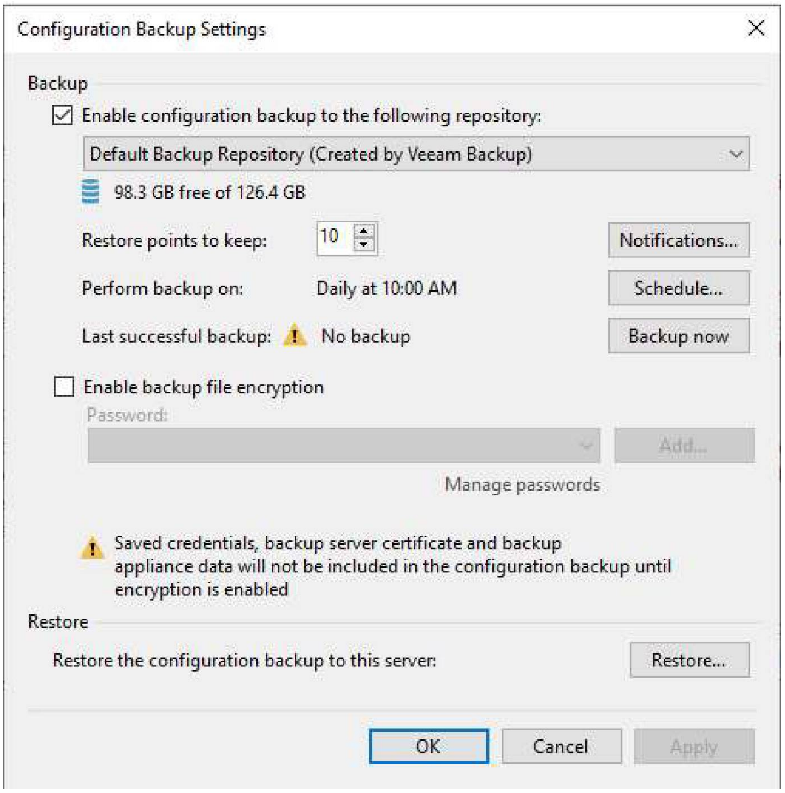
n Backup & Replication, you must register your protected data sources in the inventory. To start this process, click the Add Server
n (or just click this text).
re protection, add a vCenter Server. You can also add ESXi hosts individually. Adding vCenter Server is preferred, because it makes
eplication vMotion-aware.
er-V protection, add System Center Virtual Machine Manager (SCVMM) Servers, Hyper-V clusters, or standalone Hyper-V hosts.
oud servers and workstations protection, create one or more Protection Groups listing all computers you want to backup. For NAS
NDMP server. Note that NDMP backups are only supported to tape or Virtual Tape Libraries (VTL).

eplication provides different options to balance recovery time with storage requirements. Backup consumes less disk space but
covery time, making it ideal for long term data retention. Replication provides faster recovery time at the increased storage costs
on.
ckup or replication job, go to the Backup & Replication tree tab, and click the corresponding button in the ribbon.

ne from a backup or a replica, click the Restore button in the ribbon and select the required restore type.
an browse the Backups node of the Backup & Replication tab to locate the required machine by searching for its name.
a restore by double-clicking the full backup (.VBK) file in the Windows Explorer.

0 virtual machines | Connected to: localhost | Build: 12.0.0.1402 | Enterprise Plus Edition | NFR: 364 days remaining

11. Click Restore on the Configuration Backup Settings page.



Backup

☑ Enable configuration backup to the following repository:

Default Backup Repository (Created by Veeam Backup)

98.3 GB free of 126.4 GB

Restore points to keep: 10

Perform backup on: Daily at 10:00 AM

Last successful backup: ⚠ No backup

☐ Enable backup file encryption

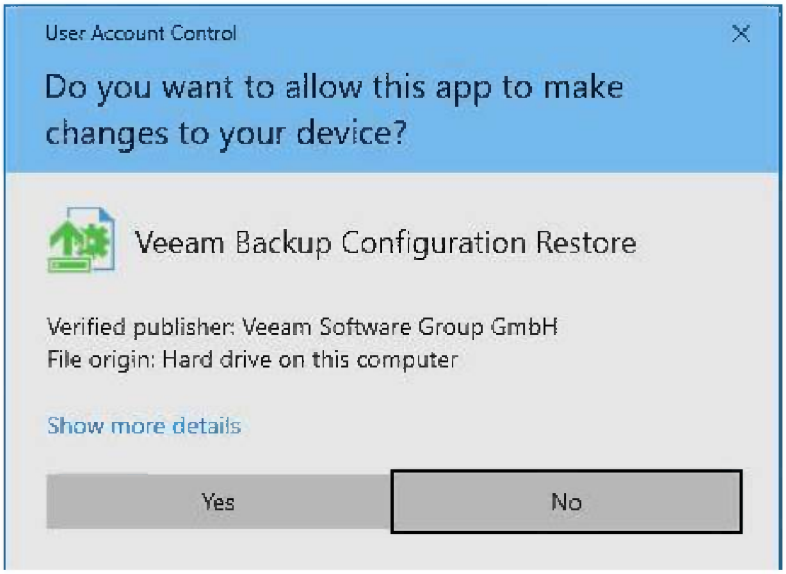
Password:

⚠ Saved credentials, backup server certificate and backup appliance data will not be included in the configuration backup until encryption is enabled

Restore

Restore the configuration backup to this server:

12. Click Yes on the User Account Control page.



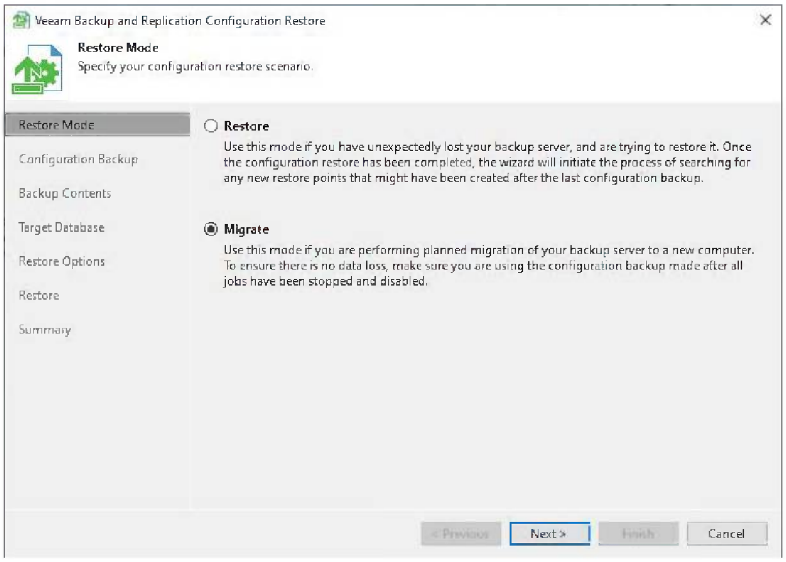
User Account Control

Do you want to allow this app to make changes to your device?

Veeam Backup Configuration Restore

Verified publisher: Veeam Software Group GmbH
File origin: Hard drive on this computer

13. Select Migrate on the Restore Mode page.



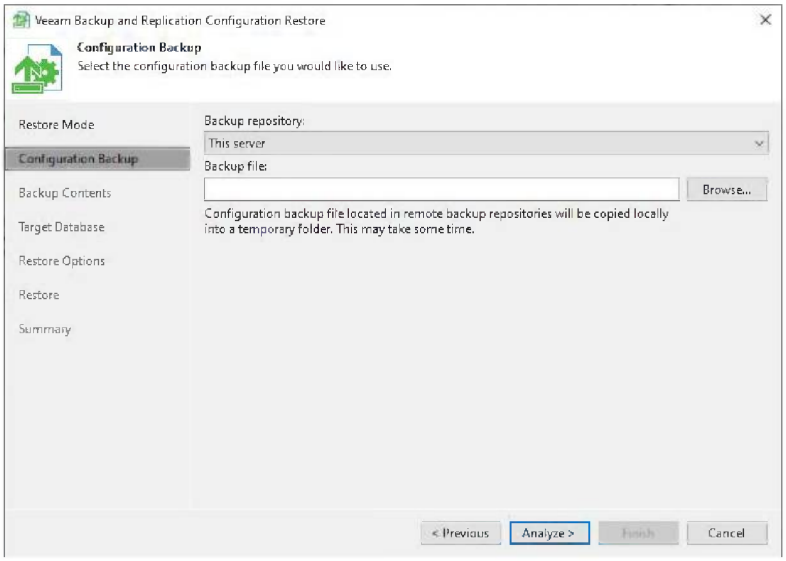
Veeam Backup and Replication Configuration Restore

Restore Mode
Specify your configuration restore scenario.

○ **Restore**
Use this mode if you have unexpectedly lost your backup server, and are trying to restore it. Once the configuration restore has been completed, the wizard will initiate the process of searching for any new restore points that might have been created after the last configuration backup.

● **Migrate**
Use this mode if you are performing planned migration of your backup server to a new computer. To ensure there is no data loss, make sure you are using the configuration backup made after all jobs have been stopped and disabled.

14. Select this server in the Backup repository field on the Configuration Backup page.
15. Click Browse in the Backup file field.



Veeam Backup and Replication Configuration Restore

Configuration Backup

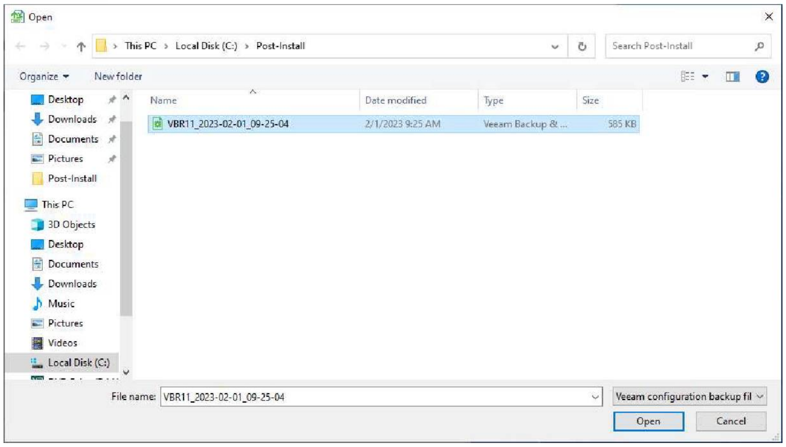
Select the configuration backup file you would like to use.

Backup repository: This server

Backup file:

Configuration backup file located in remote backup repositories will be copied locally into a temporary folder. This may take some time.

16. Select the backup configuration file and click Open.



Open

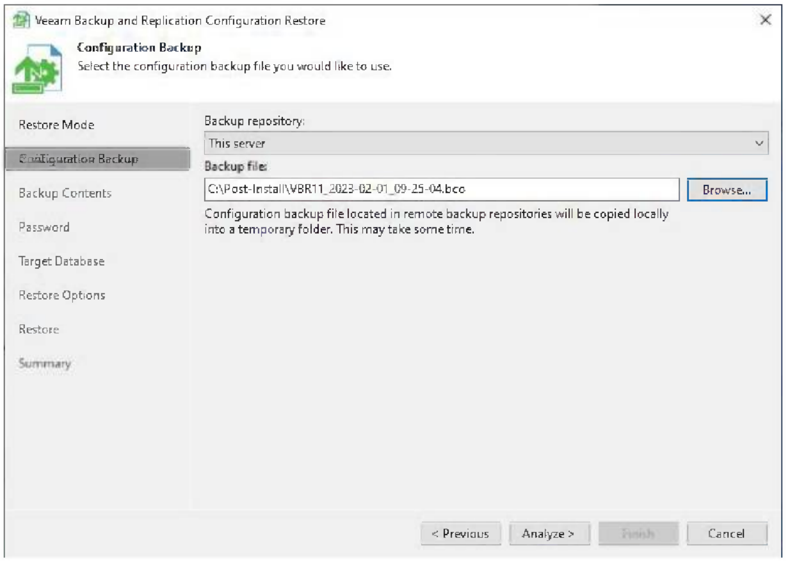
This PC > Local Disk (C:) > Post-Install

Name	Date modified	Type	Size
VBR11_2023-02-01_09-25-04	2/1/2023 9:25 AM	Veeam Backup & ...	585 KB

File name: VBR11_2023-02-01_09-25-04

Veeam configuration backup fil

17. Click Analyze on the Configuration Backup page.



Veeam Backup and Replication Configuration Restore

Configuration Backup

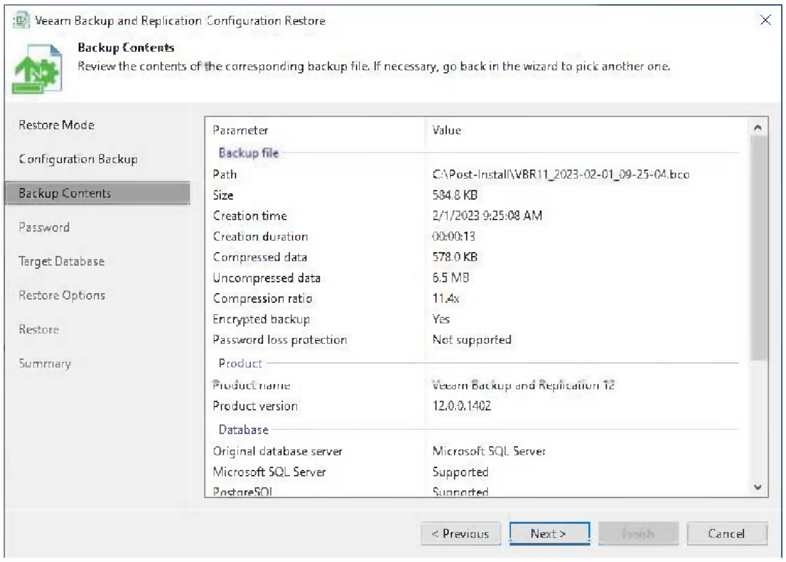
Select the configuration backup file you would like to use.

Backup repository: This server

Backup file: C:\Post-Install\VBR11_2023-02-01_09-25-04.bco

Configuration backup file located in remote backup repositories will be copied locally into a temporary folder. This may take some time.

18. Click Next on the Backup Contents page.



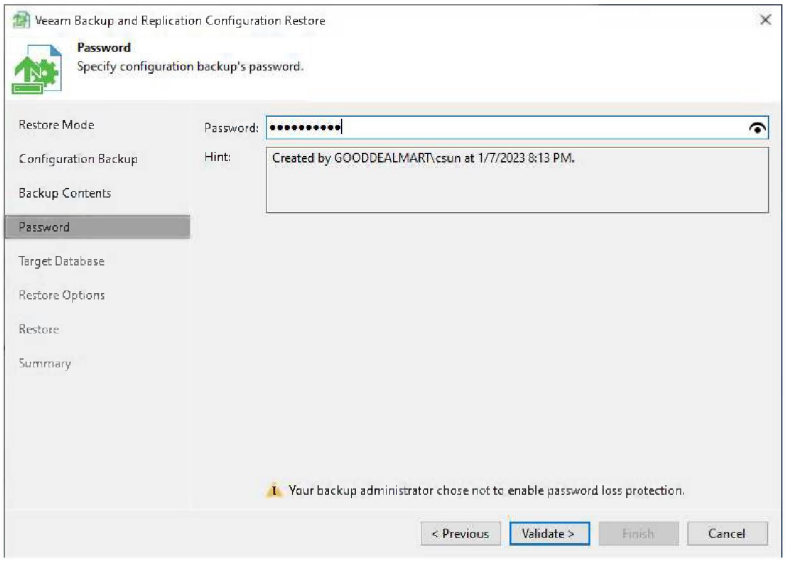
Veeam Backup and Replication Configuration Restore

Backup Contents

Review the contents of the corresponding backup file. If necessary, go back in the wizard to pick another one.

Parameter	Value
Backup file	
Path	C:\Post-Install\VBR11_2023-02-01_09-25-04.bco
Size	584.8 KB
Creation time	2/1/2023 9:25:08 AM
Creation duration	00:00:13
Compressed data	578.0 KB
Uncompressed data	6.5 MB
Compression ratio	11.4x
Encrypted backup	Yes
Password loss protection	Not supported
Product	
Product name	Veeam Backup and Replication 12
Product version	12.0.0.1402
Database	
Original database server	Microsoft SQL Server
Microsoft SQL Server	Supported
PostgreSQL	Supported

19. On the Password page, enter the password of the configuration file in the Password field.
20. Enter the description in the Hint field.
21. Click Validate.



Veeam Backup and Replication Configuration Restore

Password

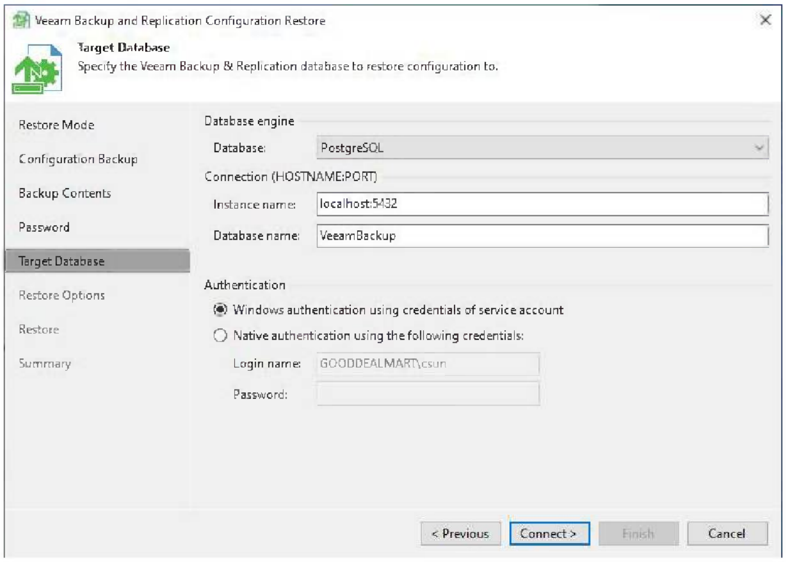
Specify configuration backup's password.

Password: ••••••••••

Hint: Created by GOODDEALMART\csun at 1/7/2023 8:13 PM.

Your backup administrator chose not to enable password loss protection.

22. Select PostgreSQL from the Database drop-down list on the Target Database page.
23. Enter the instance name and Database name in the Connection session.
24. Select Windows authentication using the service account credentials in the Authentication session.



Veeam Backup and Replication Configuration Restore

Target Database

Specify the Veeam Backup & Replication database to restore configuration to.

Database engine

Database: PostgreSQL

Connection (HOSTNAME:PORT)

Instance name: localhost:5432

Database name: VeeamBackup

Authentication

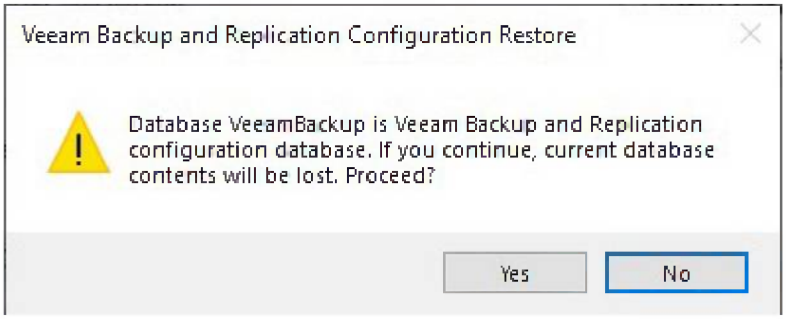
● Windows authentication using credentials of service account

○ Native authentication using the following credentials:

Login name: GOODDEALMART\csun

Password:

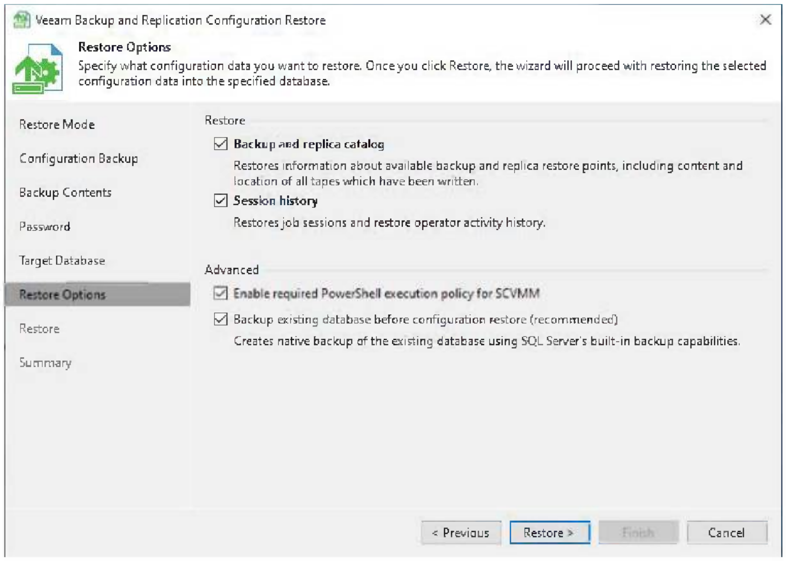
25. Click Yes on the warning message.



Veeam Backup and Replication Configuration Restore

Database VeeamBackup is Veeam Backup and Replication configuration database. If you continue, current database contents will be lost. Proceed?

26. Select the Backup and replica catalog checkbox on the Restore Options page.
27. Select the Session history checkbox.
28. Select Enable required PowerShell execution policy for SCVMM checkbox.
29. Select Backup existing database before configuration restore (recommended).
30. Click Restore.



Veeam Backup and Replication Configuration Restore

Restore Options

Specify what configuration data you want to restore. Once you click Restore, the wizard will proceed with restoring the selected configuration data into the specified database.

Restore

☑ **Backup and replica catalog**

Restores information about available backup and replica restore points, including content and location of all tapes which have been written.

☑ **Session history**

Restores job sessions and restore operator activity history.

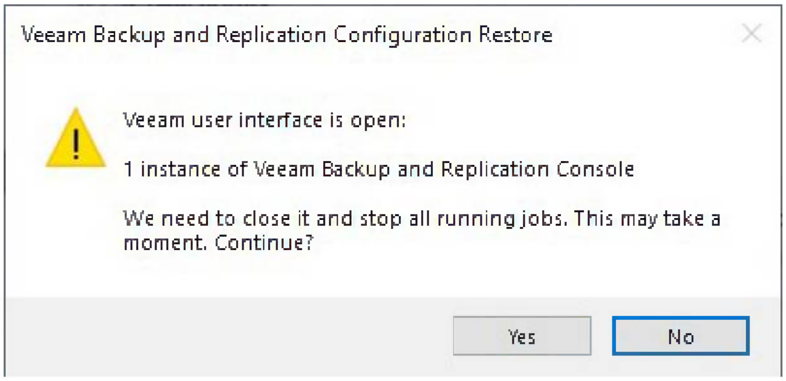
Advanced

☑ Enable required PowerShell execution policy for SCVMM

☑ Backup existing database before configuration restore (recommended)

Creates native backup of the existing database using SQL Server's built-in backup capabilities.

31. Click Yes on the close console and stop all running jobs warning messages.



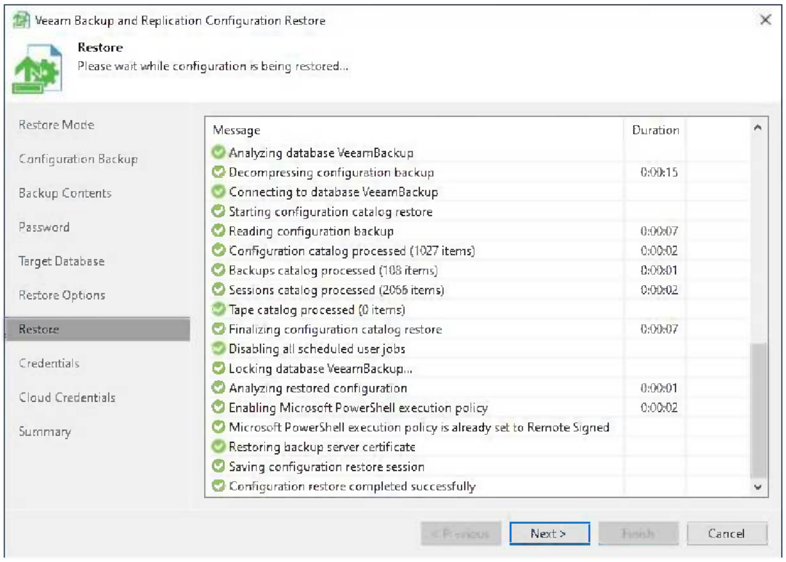
Veeam Backup and Replication Configuration Restore

Veeam user interface is open:

1 instance of Veeam Backup and Replication Console

We need to close it and stop all running jobs. This may take a moment. Continue?

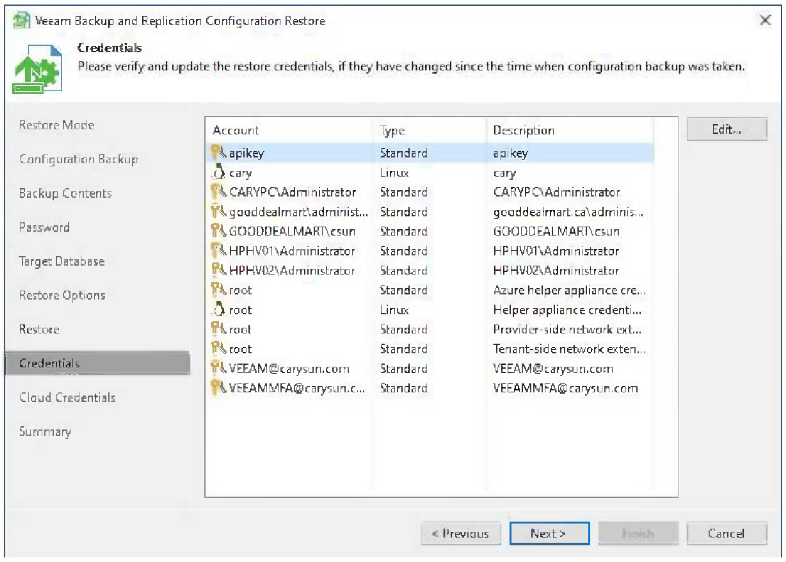
32. On the Restore page, ensure the Configuration restore is completed successfully and click Next.



Please wait while configuration is being restored...

Message	Duration
Analyzing database VeeamBackup	
Decompressing configuration backup	0:00:15
Connecting to database VeeamBackup	
Starting configuration catalog restore	
Reading configuration backup	0:00:07
Configuration catalog processed (1027 items)	0:00:02
Backups catalog processed (108 items)	0:00:01
Sessions catalog processed (2066 items)	0:00:02
Tape catalog processed (0 items)	
Finalizing configuration catalog restore	0:00:07
Disabling all scheduled user jobs	
Locking database VeeamBackup...	
Analyzing restored configuration	0:00:01
Enabling Microsoft PowerShell execution policy	0:00:02
Microsoft PowerShell execution policy is already set to Remote Signed	
Restoring backup server certificate	
Saving configuration restore session	
Configuration restore completed successfully	

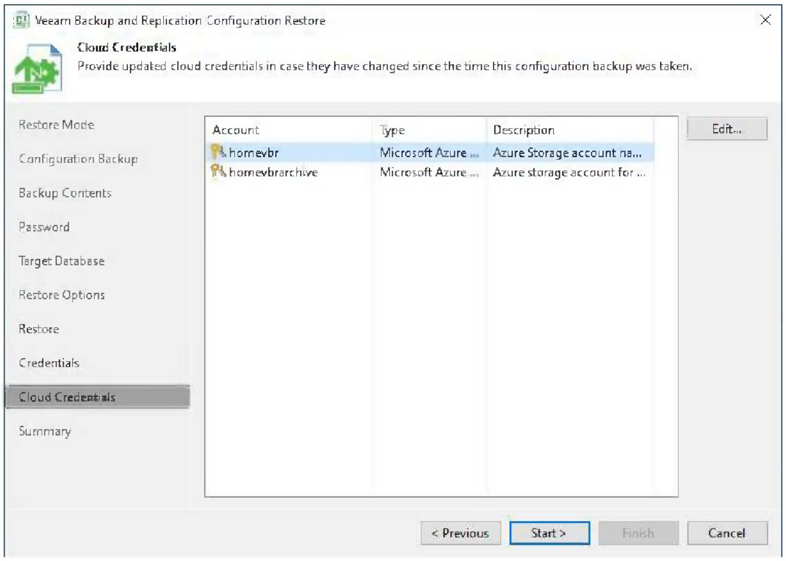
33. On the Credentials page, ensure all credentials are up-to-date and click Next.



Please verify and update the restore credentials, if they have changed since the time when configuration backup was taken.

Account	Type	Description
apikey	Standard	apikey
cary	Linux	cary
CARYPC\Administrator	Standard	CARYPC\Administrator
gooddealmart\administ...	Standard	gooddealmart.ca\adminis...
GOODDEALMART\csun	Standard	GOODDEALMART\csun
HPHV01\Administrator	Standard	HPHV01\Administrator
HPHV02\Administrator	Standard	HPHV02\Administrator
root	Standard	Azure helper appliance cre...
root	Linux	Helper appliance credenti...
root	Standard	Provider-side network ext...
root	Standard	Tenant-side network exten...
VEEAM@carysun.com	Standard	VEEAM@carysun.com
VEEAMMFA@carysun.c...	Standard	VEEAMMFA@carysun.com

34. Ensure all credentials are up-to-date on the Cloud Credentials page and click Start.

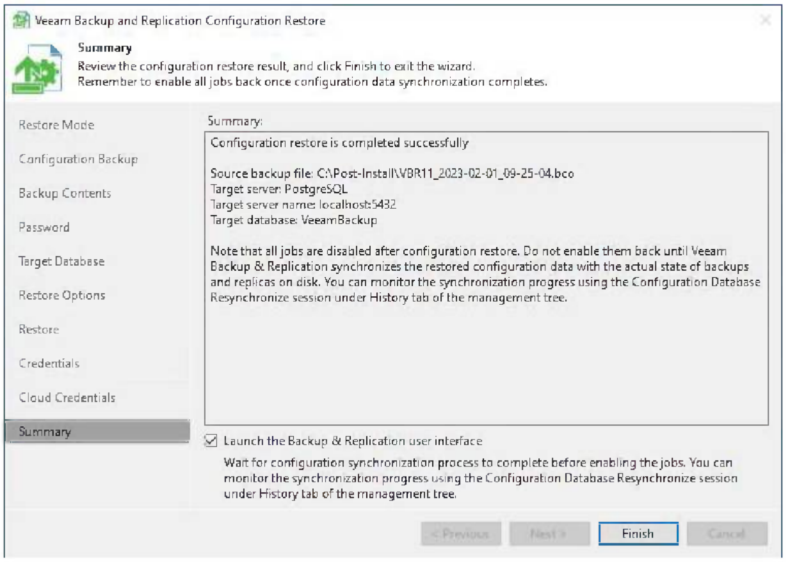


Cloud Credentials

Provide updated cloud credentials in case they have changed since the time this configuration backup was taken.

Account	Type	Description
homevbr	Microsoft Azure ...	Azure Storage account na...
homevbrarchive	Microsoft Azure ...	Azure storage account for ...

35. Click Finish on the Summary page.



Summary

Review the configuration restore result, and click Finish to exit the wizard.
Remember to enable all jobs back once configuration data synchronization completes.

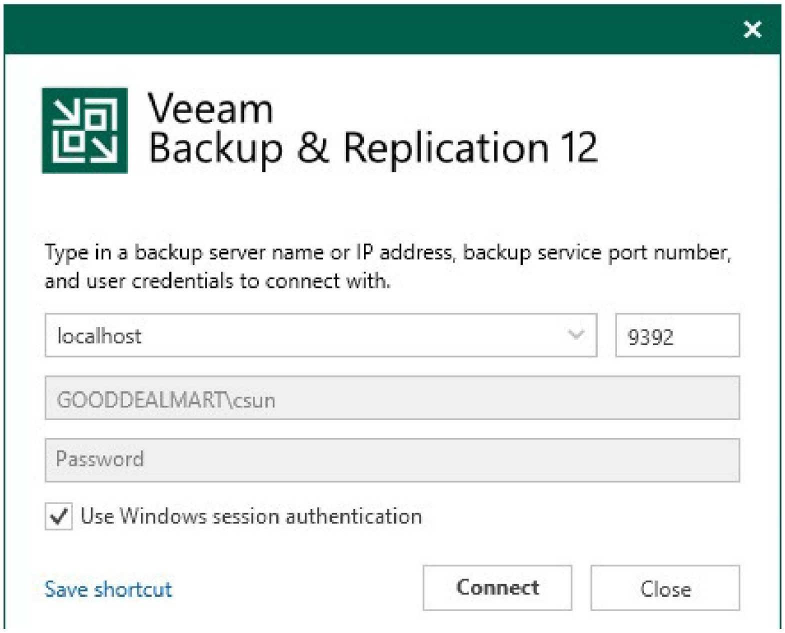
Summary:

```
Configuration restore is completed successfully

Source backup file: C:\Post-Install\VBR11_2023-02-01_09-25-04.bco
Target server: PostgreSQL
Target server name: localhost:5432
Target database: VeeamBackup

Note that all jobs are disabled after configuration restore. Do not enable them back until Veeam
Backup & Replication synchronizes the restored configuration data with the actual state of backups
and replicas on disk. You can monitor the synchronization progress using the Configuration Database
Resynchronize session under History tab of the management tree.
```

☑ Launch the Backup & Replication user interface

Wait for configuration synchronization process to complete before enabling the jobs. You can monitor the synchronization progress using the Configuration Database Resynchronize session under History tab of the management tree.

36. Open Veeam Backup & Replication console and click Connect.



Veeam Backup & Replication 12

Type in a backup server name or IP address, backup service port number, and user credentials to connect with.

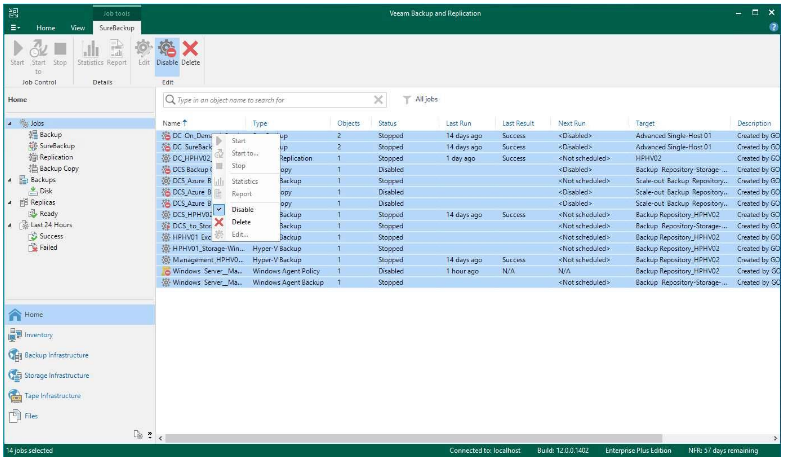
localhost 9392

GOODDEALMART\csun

Password

☑ Use Windows session authentication

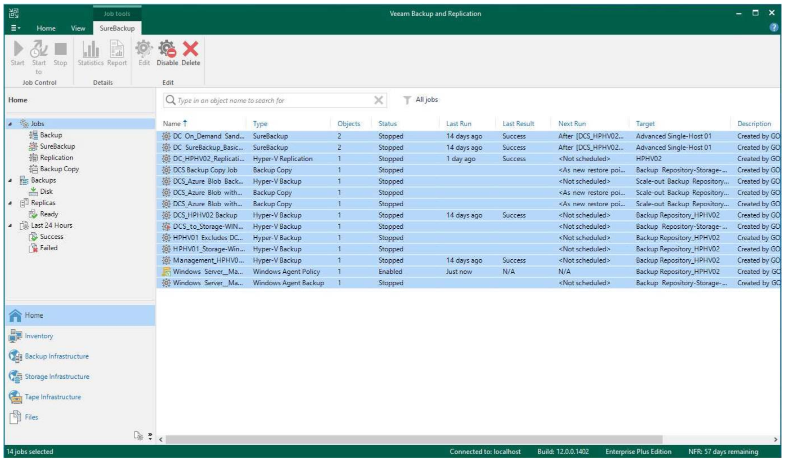
37. Select and right-click all jobs, and unselect Disable to enable all jobs.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
DC On_Dema	up	2	Stopped	14 days ago	Success	<Disabled>	Advanced Single-Host 01	Created by GO
DC SureBack	up	2	Stopped	14 days ago	Success	<Disabled>	Advanced Single-Host 01	Created by GO
DC_HPHV02_	Replication	1	Stopped	1 day ago	Success	<Not scheduled>	HPHV02	Created by GO
DCS Backup (	opy	1	Disabled			<Disabled>	Backup Repository-Storage-...	Created by GO
DCS_Azure B	Backup	1	Stopped			<Not scheduled>	Scale-out Backup Repository...	Created by GO
DCS_Azure B	opy	1	Disabled			<Disabled>	Scale-out Backup Repository...	Created by GO
DCS_Azure B	opy	1	Disabled			<Disabled>	Scale-out Backup Repository...	Created by GO
DCS_HPHV02	Backup	1	Stopped	14 days ago	Success	<Not scheduled>	Backup Repository_HPHV02	Created by GO
DCS_to_Stor	Backup	1	Stopped			<Not scheduled>	Backup Repository-Storage-...	Created by GO
HPHV01 Exc	Backup	1	Stopped			<Not scheduled>	Backup Repository_HPHV02	Created by GO
HPHV01_Storage-Win...	Hyper-V Backup	1	Stopped			<Not scheduled>	Backup Repository_HPHV02	Created by GO
Management_HPHV0...	Hyper-V Backup	1	Stopped	14 days ago	Success	<Not scheduled>	Backup Repository_HPHV02	Created by GO
Windows Server__Ma...	Windows Agent Policy	1	Disabled	1 hour ago	N/A	N/A	Backup Repository_HPHV02	Created by GO
Windows Server__Ma...	Windows Agent Backup	1	Stopped			<Not scheduled>	Backup Repository-Storage-...	Created by GO

14 jobs selected   Connected to: localhost   Build: 12.0.0.1402   Enterprise Plus Edition   NFR: 57 days remaining

38. Ensure all jobs are re-enabled.

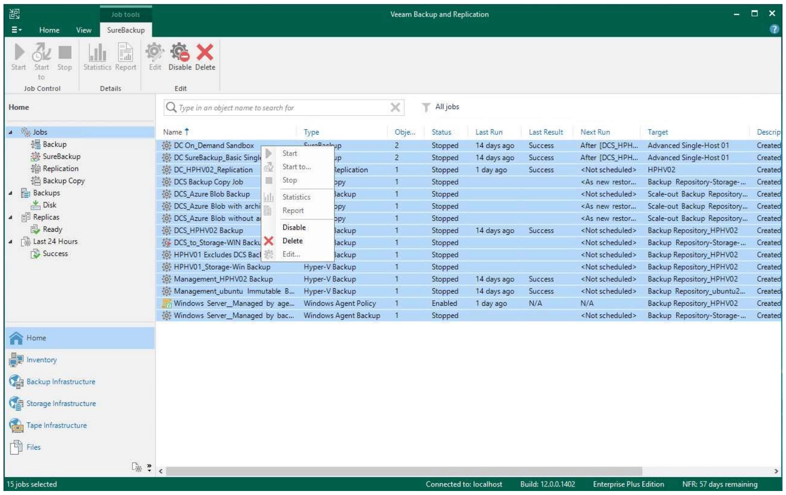


Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
DC On_Demand Sand...	SureBackup	2	Stopped	14 days ago	Success	After [DCS_HPHV02...	Advanced Single-Host 01	Created by GO
DC SureBackup_Basic...	SureBackup	2	Stopped	14 days ago	Success	After [DCS_HPHV02...	Advanced Single-Host 01	Created by GO
DC_HPHV02_Replicati...	Hyper-V Replication	1	Stopped	1 day ago	Success	<Not scheduled>	HPHV02	Created by GO
DCS Backup Copy Job	Backup Copy	1	Stopped			<As new restore poi...	Backup Repository-Storage-...	Created by GO
DCS_Azure Blob Back...	Hyper-V Backup	1	Stopped			<Not scheduled>	Scale-out Backup Repository...	Created by GO
DCS_Azure Blob with...	Backup Copy	1	Stopped			<As new restore poi...	Scale-out Backup Repository...	Created by GO
DCS_Azure Blob with...	Backup Copy	1	Stopped			<As new restore poi...	Scale-out Backup Repository...	Created by GO
DCS_HPHV02 Backup	Hyper-V Backup	1	Stopped	14 days ago	Success	<Not scheduled>	Backup Repository_HPHV02	Created by GO
DCS_to_Storage-WIN...	Hyper-V Backup	1	Stopped			<Not scheduled>	Backup Repository-Storage-...	Created by GO
HPHV01 Excludes DC...	Hyper-V Backup	1	Stopped			<Not scheduled>	Backup Repository_HPHV02	Created by GO
HPHV01_Storage-Win...	Hyper-V Backup	1	Stopped			<Not scheduled>	Backup Repository_HPHV02	Created by GO
Management_HPHV0...	Hyper-V Backup	1	Stopped	14 days ago	Success	<Not scheduled>	Backup Repository_HPHV02	Created by GO
Windows Server__Ma...	Windows Agent Policy	1	Enabled	Just now	N/A	N/A	Backup Repository_HPHV02	Created by GO
Windows Server__Ma...	Windows Agent Backup	1	Stopped			<Not scheduled>	Backup Repository-Storage-...	Created by GO

14 jobs selected   Connected to: localhost   Build: 12.0.0.1402   Enterprise Plus Edition   NFR: 57 days remaining

Migrate the Existing Veeam Backup and Replication to the new server with Microsoft SQL

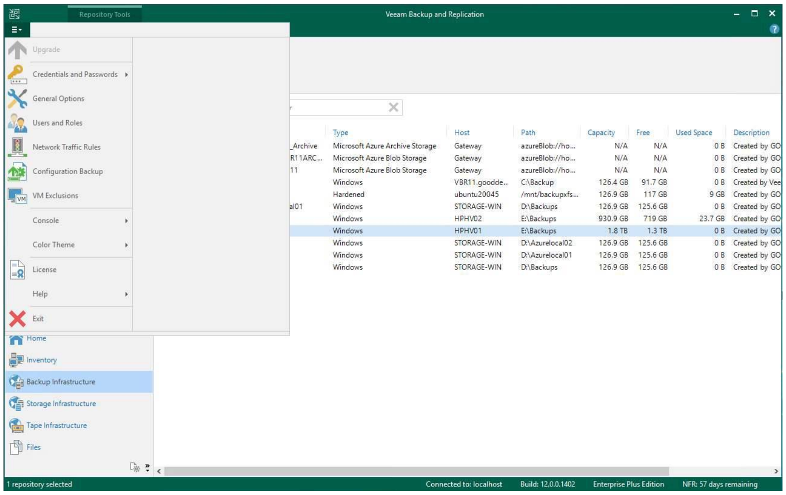
Microsoft SQL Server (or Express), either locally on the backup manager server or remotely. Microsoft SQL Server Express has a configuration data storage limit of 10 GB. The Express Edition is sufficient for the evaluation and small environments (500 VMs).

Instructions	Screenshot (if applicable)
1. Log in to the existing Veeam Backup and replication manager server. 2. Open the Veeam Backup & Replication Console. 3. Select and right-click all jobs. 4. Select Disable.	

Name	Type	Obje...	Status	Last Run	Last Result	Next Run	Target	Descrip
DC On_Demand Sandbox	SureBackup	2	Stopped	14 days ago	Success	After [DCS_HPH...	Advanced Single-Host 01	Created
DC SureBackup_Basic Singl	up	2	Stopped	14 days ago	Success	After [DCS_HPH...	Advanced Single-Host 01	Created
DC_HPHV02_Replication	eplication	1	Stopped	1 day ago	Success	<Not scheduled>	HPHV02	Created
DCS Backup Copy Job	py	1	Stopped			<As new restor...	Backup Repository-Storage-...	Created
DCS_Azure Blob Backup	ackup	1	Stopped			<Not scheduled>	Scale-out Backup Repository...	Created
DCS_Azure Blob with archi	py	1	Stopped			<As new restor...	Scale-out Backup Repository...	Created
DCS_Azure Blob without a	py	1	Stopped			<As new restor...	Scale-out Backup Repository...	Created
DCS_HPHV02 Backup	ackup	1	Stopped	14 days ago	Success	<Not scheduled>	Backup Repository_HPHV02	Created
DCS_to_Storage-WIN Backu	ackup	1	Stopped			<Not scheduled>	Backup Repository-Storage-...	Created
HPHV01 Excludes DCS Bac	ackup	1	Stopped			<Not scheduled>	Backup Repository_HPHV02	Created
HPHV01_Storage-Win Backup	Hyper-V Backup	1	Stopped			<Not scheduled>	Backup Repository_HPHV02	Created
Management_HPHV02 Backup	Hyper-V Backup	1	Stopped	14 days ago	Success	<Not scheduled>	Backup Repository_HPHV02	Created
Management_ubuntu Immutable B...	Hyper-V Backup	1	Stopped	14 days ago	Success	<Not scheduled>	Backup Repository_ubuntu2...	Created
Windows Server__Managed by age...	Windows Agent Policy	1	Enabled	1 day ago	N/A	N/A	Backup Repository_HPHV02	Created
Windows Server__Managed by bac...	Windows Agent Backup	1	Stopped			<Not scheduled>	Backup Repository-Storage-...	Created

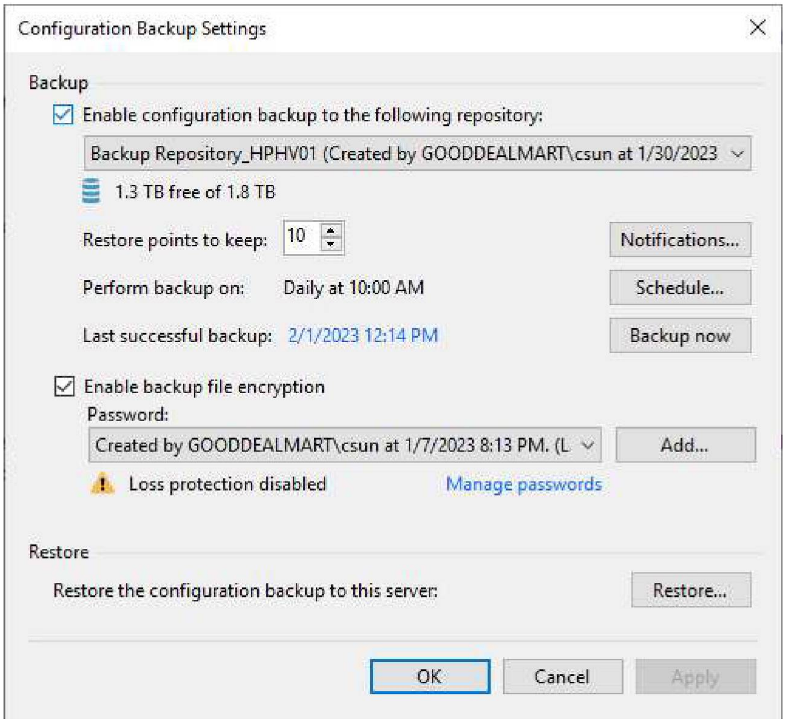
15 jobs selected Connected to: localhost Build: 12.0.0.1402 Enterprise Plus Edition NFR: 57 days remaining

5. Drop down the main menu and select Configuration Backup.



	Type	Host	Path	Capacity	Free	Used Space	Description
_Archive	Microsoft Azure Archive Storage	Gateway	azureBlob://ho...	N/A	N/A	0 B	Created by GO
R11ARC...	Microsoft Azure Blob Storage	Gateway	azureBlob://ho...	N/A	N/A	0 B	Created by GO
11	Microsoft Azure Blob Storage	Gateway	azureBlob://ho...	N/A	N/A	0 B	Created by GO
	Windows	VBR11.goodde...	C:\Backup	126.4 GB	91.7 GB	0 B	Created by Vee
	Hardened	ubuntu20045	/mnt/backupxfs...	126.9 GB	117 GB	9 GB	Created by GO
al01	Windows	STORAGE-WIN	D:\Backups	126.9 GB	125.6 GB	0 B	Created by GO
	Windows	HPHV02	E:\Backups	930.9 GB	719 GB	23.7 GB	Created by GO
	Windows	HPHV01	E:\Backups	1.8 TB	1.3 TB	0 B	Created by GO
	Windows	STORAGE-WIN	D:\Azurelocal02	126.9 GB	125.6 GB	0 B	Created by GO
	Windows	STORAGE-WIN	D:\Azurelocal01	126.9 GB	125.6 GB	0 B	Created by GO
	Windows	STORAGE-WIN	D:\Backups	126.9 GB	125.6 GB	0 B	Created by GO

6. Click Backup now on the Configuration Backup Settings page.



Configuration Backup Settings

Backup

☑ Enable configuration backup to the following repository:

Backup Repository_HPHV01 (Created by GOODDEALMART\csun at 1/30/2023

1.3 TB free of 1.8 TB

Restore points to keep: 10

Perform backup on: Daily at 10:00 AM

Last successful backup: 2/1/2023 12:14 PM

☑ Enable backup file encryption

Password:

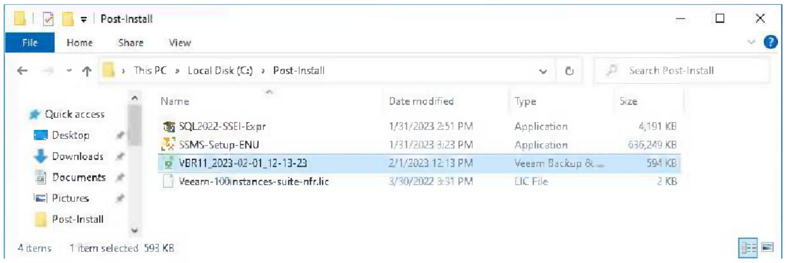
Created by GOODDEALMART\csun at 1/7/2023 8:13 PM. (L

Loss protection disabled

Restore

Restore the configuration backup to this server:

7. Copy the configuration file from the backup repository to the new Backup and Replication manager server.



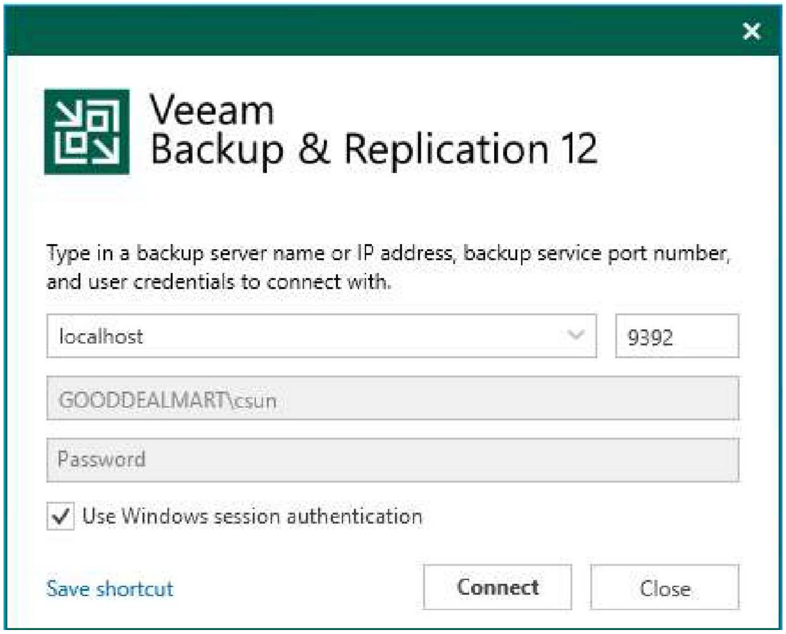
Post-Install

This PC › Local Disk (C:) › Post-Install

Name	Date modified	Type	Size
SQL2022-SSEI-Expr	1/31/2023 2:51 PM	Application	4,191 KB
SSMS-Setup-ENU	1/31/2023 3:23 PM	Application	636,249 KB
VBR11_2023-02-01_12-13-23	2/1/2023 12:13 PM	Veeam Backup &...	594 KB
Veeam-100instances-suite-nfr.lic	3/30/2022 3:31 PM	LIC File	2 KB

4 items 1 item selected 593 KB

8. Log in to the new Veeam Backup and Replication manager server.
9. Open the Veeam Backup & Replication Console, and click Connect.



Veeam
Backup & Replication 12

Type in a backup server name or IP address, backup service port number, and user credentials to connect with.

localhost

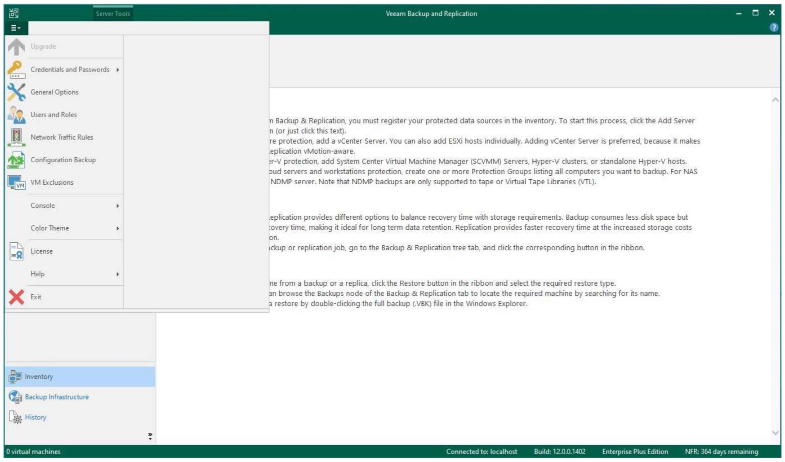
9392

GOODDEALMART\csun

Password

☑ Use Windows session authentication

10. Drop down the main menu and select Configuration Backup.



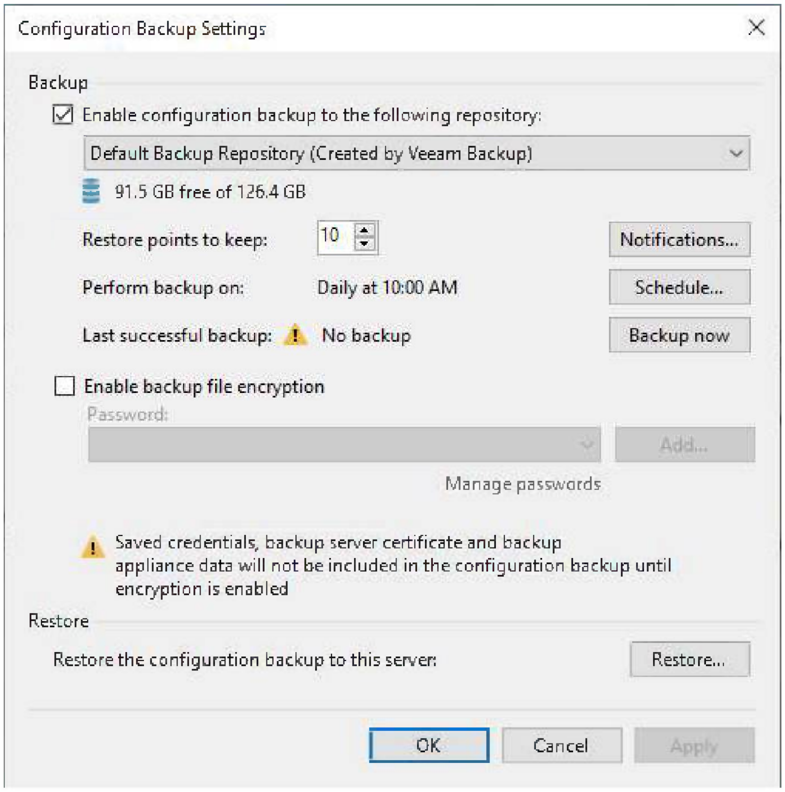
n Backup & Replication, you must register your protected data sources in the inventory. To start this process, click the Add Server
n (or just click this text).
re protection, add a vCenter Server. You can also add ESXi hosts individually. Adding vCenter Server is preferred, because it makes
eplication vMotion-aware.
er-V protection, add System Center Virtual Machine Manager (SCVMM) Servers, Hyper-V clusters, or standalone Hyper-V hosts.
oud servers and workstations protection, create one or more Protection Groups listing all computers you want to backup. For NAS
NDMP server. Note that NDMP backups are only supported to tape or Virtual Tape Libraries (VTL).

eplication provides different options to balance recovery time with storage requirements. Backup consumes less disk space but
covery time, making it ideal for long term data retention. Replication provides faster recovery time at the increased storage costs
on.
ckup or replication job, go to the Backup & Replication tree tab, and click the corresponding button in the ribbon.

ne from a backup or a replica, click the Restore button in the ribbon and select the required restore type.
an browse the Backups node of the Backup & Replication tab to locate the required machine by searching for its name.
a restore by double-clicking the full backup (.VBK) file in the Windows Explorer.

0 virtual machines   Connected to: localhost   Build: 12.0.0.1402   Enterprise Plus Edition   NFR: 364 days remaining

11. Click Restore on the Configuration Backup Settings page.



Configuration Backup Settings

Backup

☑ Enable configuration backup to the following repository:

Default Backup Repository (Created by Veeam Backup)

91.5 GB free of 126.4 GB

Restore points to keep: 10

Perform backup on: Daily at 10:00 AM

Last successful backup: ⚠ No backup

☐ Enable backup file encryption

Password:

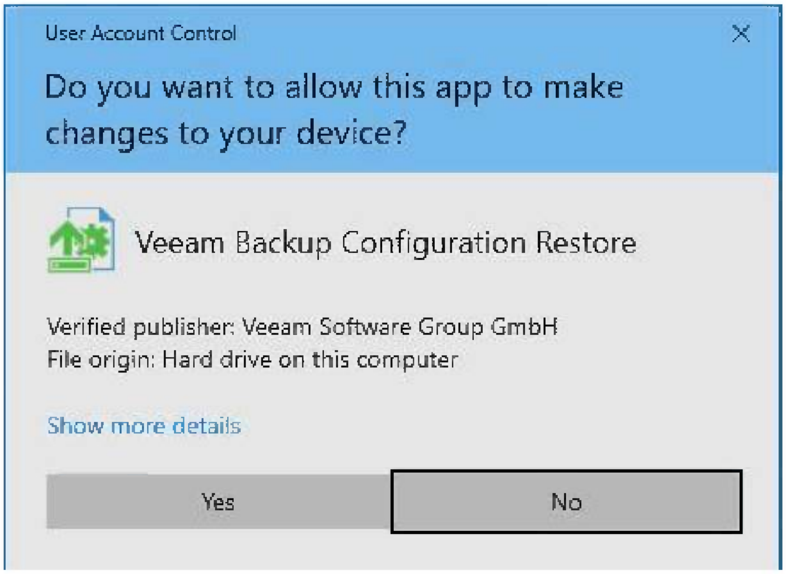
Manage passwords

⚠ Saved credentials, backup server certificate and backup appliance data will not be included in the configuration backup until encryption is enabled

Restore

Restore the configuration backup to this server:

12. Click Yes on the User Account Control page.

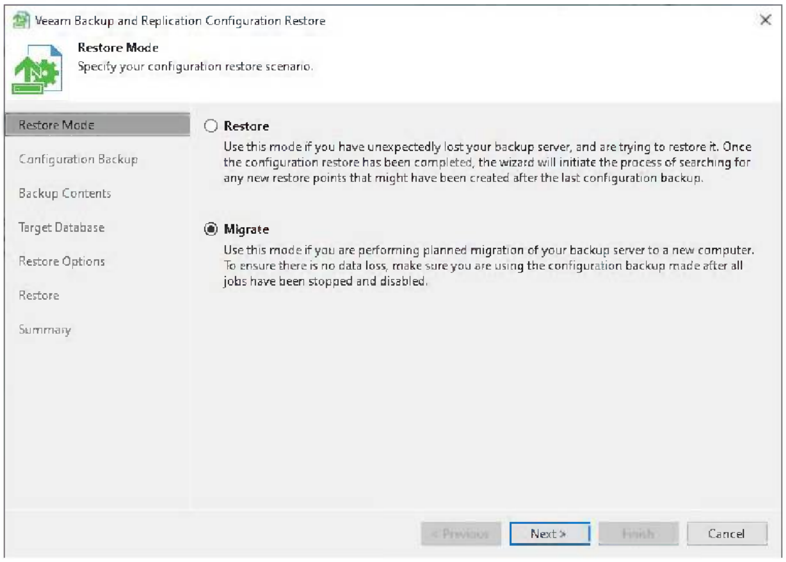


Do you want to allow this app to make changes to your device?

Veeam Backup Configuration Restore

Verified publisher: Veeam Software Group GmbH
File origin: Hard drive on this computer

13. Select Migrate on the Restore Mode page.



Restore Mode

Specify your configuration restore scenario.

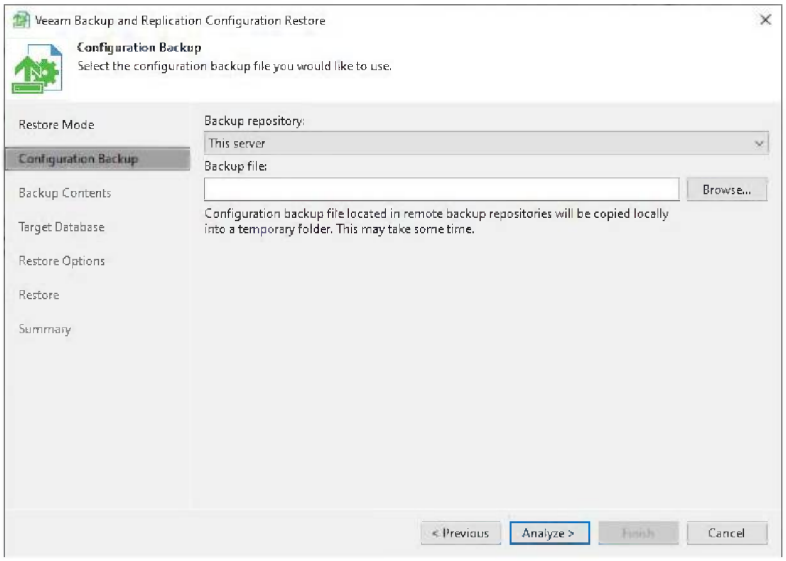
○ **Restore**

Use this mode if you have unexpectedly lost your backup server, and are trying to restore it. Once the configuration restore has been completed, the wizard will initiate the process of searching for any new restore points that might have been created after the last configuration backup.

● **Migrate**

Use this mode if you are performing planned migration of your backup server to a new computer. To ensure there is no data loss, make sure you are using the configuration backup made after all jobs have been stopped and disabled.

14. Select this server in the Backup repository field on the Configuration Backup page.
15. Click Browse in the Backup file field.



Veeam Backup and Replication Configuration Restore

Configuration Backup

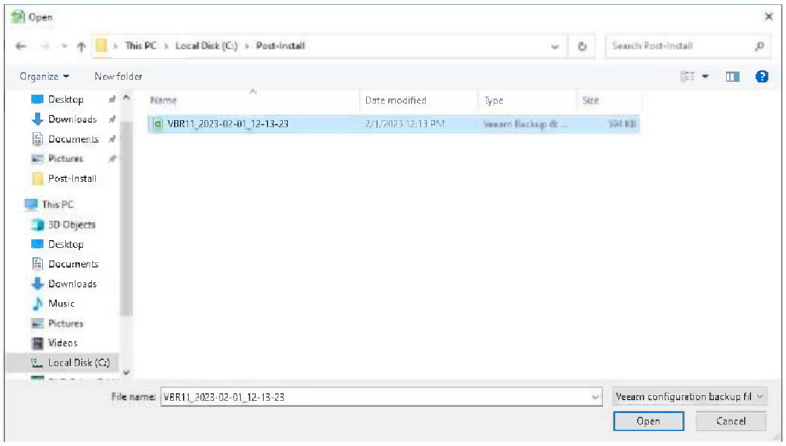
Select the configuration backup file you would like to use.

Backup repository: This server

Backup file:

Configuration backup file located in remote backup repositories will be copied locally into a temporary folder. This may take some time.

16. Select the backup configuration file and click Open.



Open

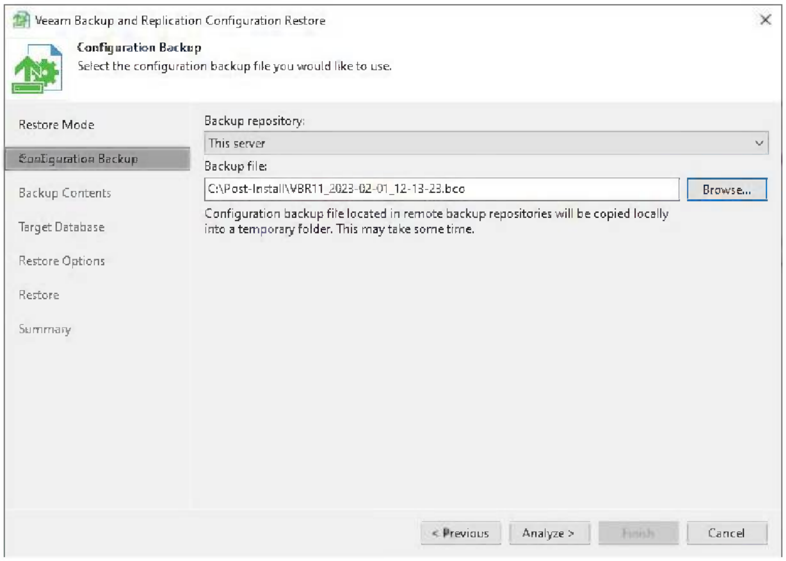
This PC › Local Disk (C:) › Post-Install

Name	Date modified	Type	Size
VBR11_2023-02-01_12-13-23	2/1/2023 12:13 PM	Veeam Backup & ...	594 KB

File name: VBR11_2023-02-01_12-13-23

Veeam configuration backup fil

17. Click Analyze on the Configuration Backup page.



Veeam Backup and Replication Configuration Restore

Configuration Backup

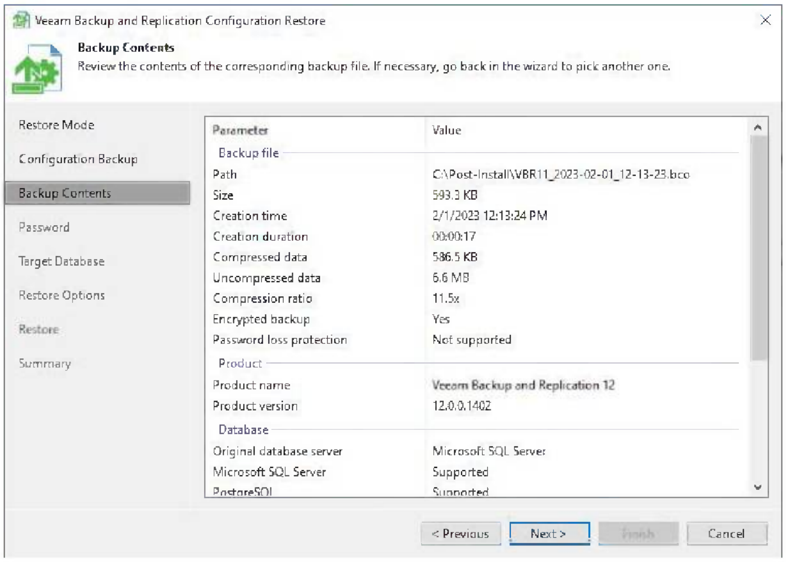
Select the configuration backup file you would like to use.

Backup repository: This server

Backup file: C:\Post-Install\VBR11_2023-02-01_12-13-23.bco

Configuration backup file located in remote backup repositories will be copied locally into a temporary folder. This may take some time.

18. Click Next on the Backup Contents page.



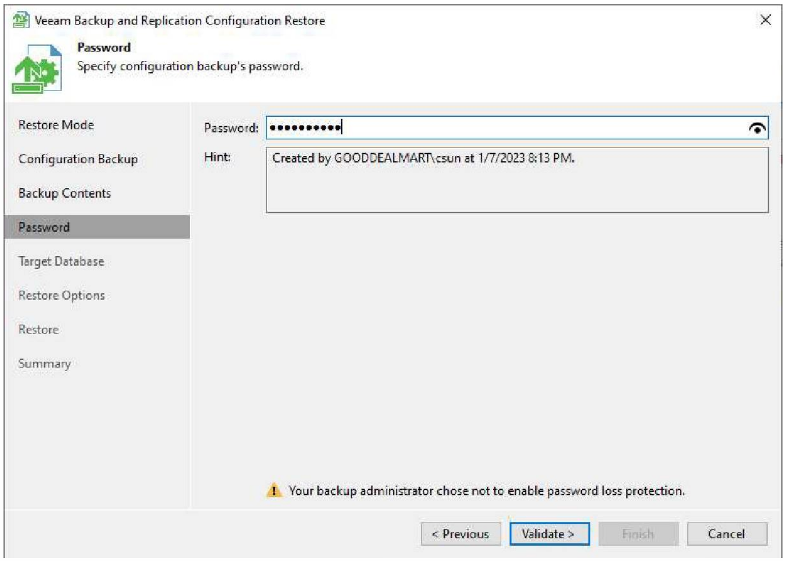
Veeam Backup and Replication Configuration Restore

Backup Contents

Review the contents of the corresponding backup file. If necessary, go back in the wizard to pick another one.

Parameter	Value
Backup file	
Path	C:\Post-Install\VBR11_2023-02-01_12-13-23.bco
Size	593.3 KB
Creation time	2/1/2023 12:13:24 PM
Creation duration	00:00:17
Compressed data	586.5 KB
Uncompressed data	6.6 MB
Compression ratio	11.5x
Encrypted backup	Yes
Password loss protection	Not supported
Product	
Product name	Veeam Backup and Replication 12
Product version	12.0.0.1402
Database	
Original database server	Microsoft SQL Server
Microsoft SQL Server	Supported
PostgreSQL	Supported

19. On the Password page, enter the password of the configuration file in the Password field.
20. Enter the description in the Hint field.
21. Click Validate.



Veeam Backup and Replication Configuration Restore

Password

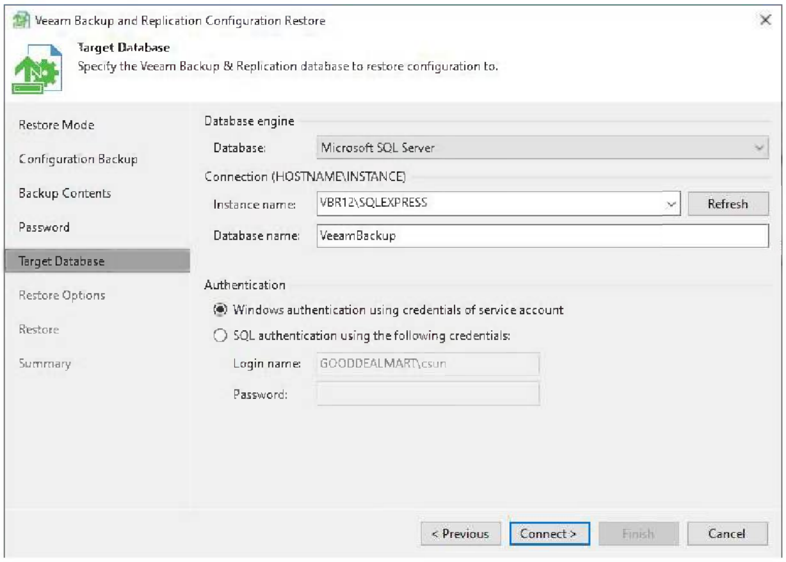
Specify configuration backup's password.

Password: ••••••••••

Hint: Created by GOODDEALMART\csun at 1/7/2023 8:13 PM.

Your backup administrator chose not to enable password loss protection.

22. Select Microsoft SQL Server from the Database drop-down list on the Target Database page.
23. Enter the instance name and Database name in the Connection session.
24. Select Windows authentication using the service account credentials in the Authentication session.



Veeam Backup and Replication Configuration Restore

Target Database

Specify the Veeam Backup & Replication database to restore configuration to.

Database engine

Database: Microsoft SQL Server

Connection (HOSTNAME\INSTANCE)

Instance name: VBR12\SQLEXPRESS

Database name: VeeamBackup

Authentication

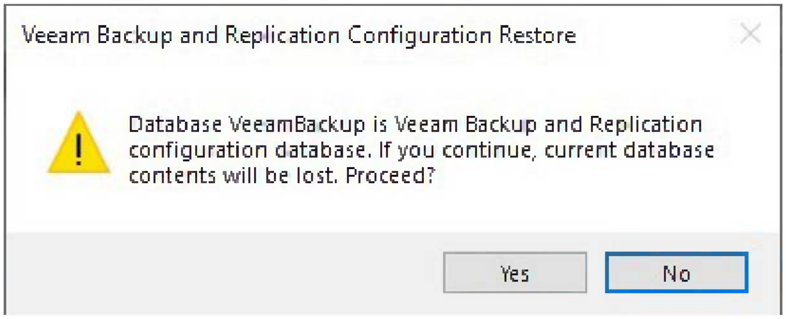
● Windows authentication using credentials of service account

○ SQL authentication using the following credentials:

Login name: GOODDEALMART\csun

Password:

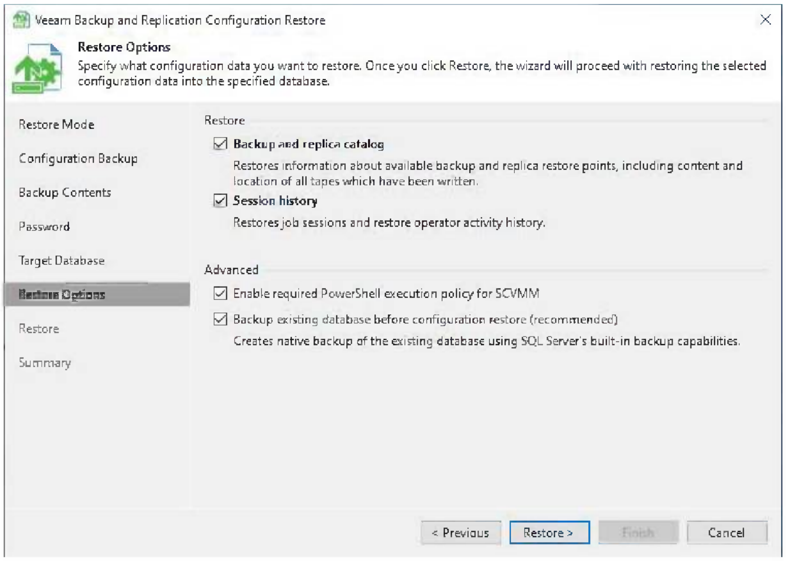
25. Click Yes on the warning message.



Veeam Backup and Replication Configuration Restore

Database VeeamBackup is Veeam Backup and Replication configuration database. If you continue, current database contents will be lost. Proceed?

26. Select the Backup and replica catalog checkbox on the Restore Options page.
27. Select the Session history checkbox.
28. Select Enable required PowerShell execution policy for SCVMM checkbox.
29. Select Backup existing database before configuration restore (recommended).
30. Click Restore.



Veeam Backup and Replication Configuration Restore

Restore Options

Specify what configuration data you want to restore. Once you click Restore, the wizard will proceed with restoring the selected configuration data into the specified database.

Restore

☑ **Backup and replica catalog**

Restores information about available backup and replica restore points, including content and location of all tapes which have been written.

☑ **Session history**

Restores job sessions and restore operator activity history.

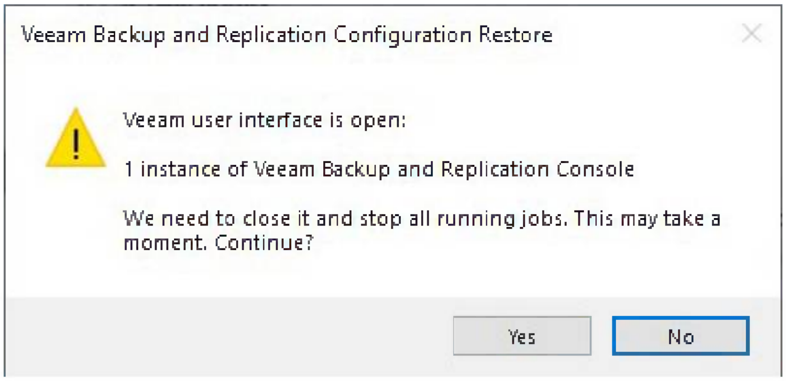
Advanced

☑ Enable required PowerShell execution policy for SCVMM

☑ Backup existing database before configuration restore (recommended)

Creates native backup of the existing database using SQL Server's built-in backup capabilities.

31. Click Yes on the warning message.



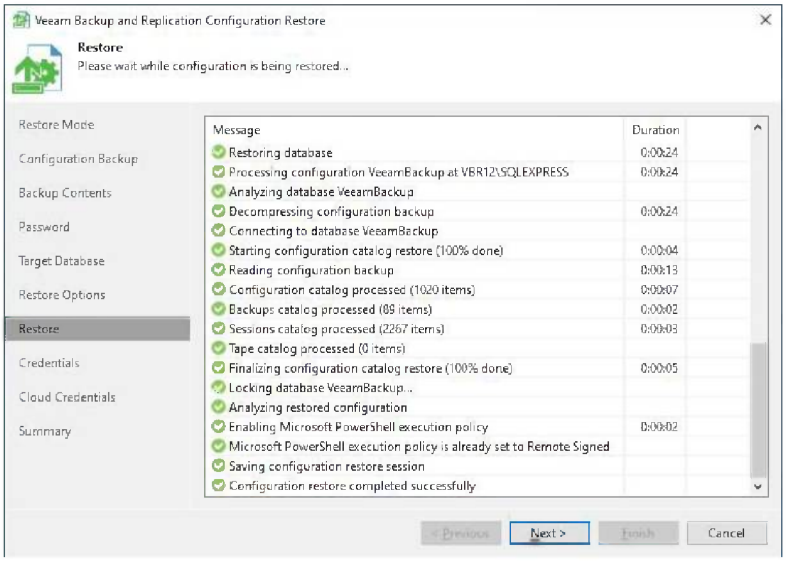
Veeam Backup and Replication Configuration Restore

Veeam user interface is open:

1 instance of Veeam Backup and Replication Console

We need to close it and stop all running jobs. This may take a moment. Continue?

32. On the Restore page, ensure the Configuration restore is completed successfully and click Next.



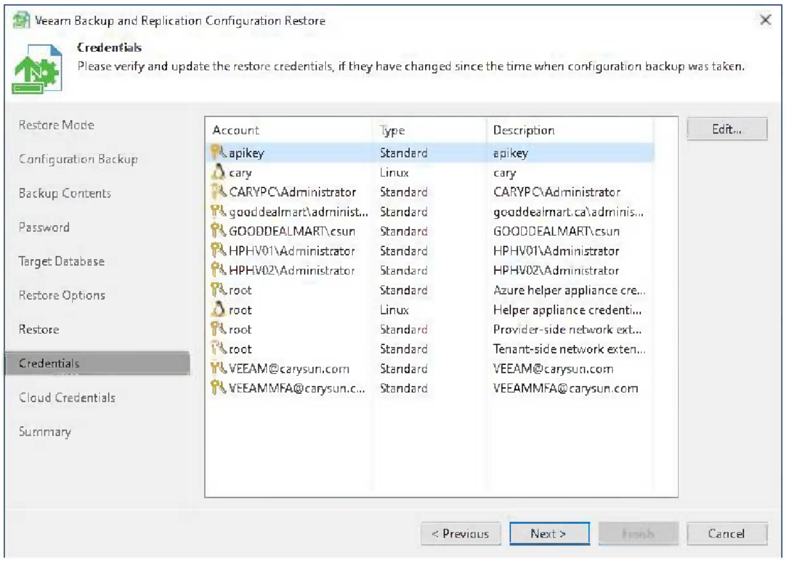
Veeam Backup and Replication Configuration Restore

Restore

Please wait while configuration is being restored...

Message	Duration
Restoring database	0:00:24
Processing configuration VeeamBackup at VBR12\SQLEXPRESS	0:00:24
Analyzing database VeeamBackup	
Decompressing configuration backup	0:00:24
Connecting to database VeeamBackup	
Starting configuration catalog restore (100% done)	0:00:04
Reading configuration backup	0:00:13
Configuration catalog processed (1020 items)	0:00:07
Backups catalog processed (89 items)	0:00:02
Sessions catalog processed (2267 items)	0:00:03
Tape catalog processed (0 items)	
Finalizing configuration catalog restore (100% done)	0:00:05
Locking database VeeamBackup...	
Analyzing restored configuration	
Enabling Microsoft PowerShell execution policy	0:00:02
Microsoft PowerShell execution policy is already set to Remote Signed	
Saving configuration restore session	
Configuration restore completed successfully	

33. On the Credentials page, ensure all credentials are up-to-date and click Next.



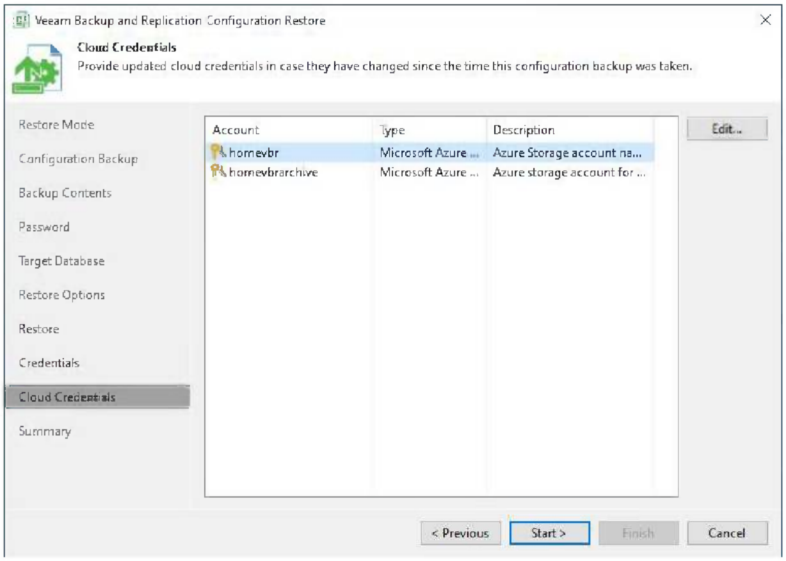
Veeam Backup and Replication Configuration Restore

Credentials

Please verify and update the restore credentials, if they have changed since the time when configuration backup was taken.

Account	Type	Description
apikey	Standard	apikey
cary	Linux	cary
CARYPC\Administrator	Standard	CARYPC\Administrator
gooddealmart\administ...	Standard	gooddealmart.ca\adminis...
GOODDEALMART\csun	Standard	GOODDEALMART\csun
HPHV01\Administrator	Standard	HPHV01\Administrator
HPHV02\Administrator	Standard	HPHV02\Administrator
root	Standard	Azure helper appliance cre...
root	Linux	Helper appliance credenti...
root	Standard	Provider-side network ext...
root	Standard	Tenant-side network exten...
VEEAM@carysun.com	Standard	VEEAM@carysun.com
VEEAMMFA@carysun.c...	Standard	VEEAMMFA@carysun.com

34. Ensure all credentials are up-to-date on the Cloud Credentials page and click Start.

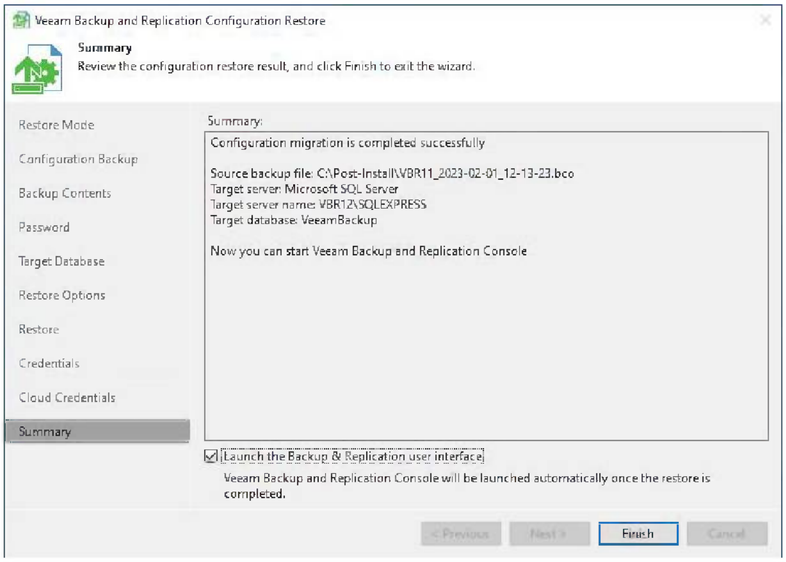


Cloud Credentials

Provide updated cloud credentials in case they have changed since the time this configuration backup was taken.

Account	Type	Description
homevbr	Microsoft Azure ...	Azure Storage account na...
homevbrarchive	Microsoft Azure ...	Azure storage account for ...

35. Click Finish on the Summary page.



Summary

Review the configuration restore result, and click Finish to exit the wizard.

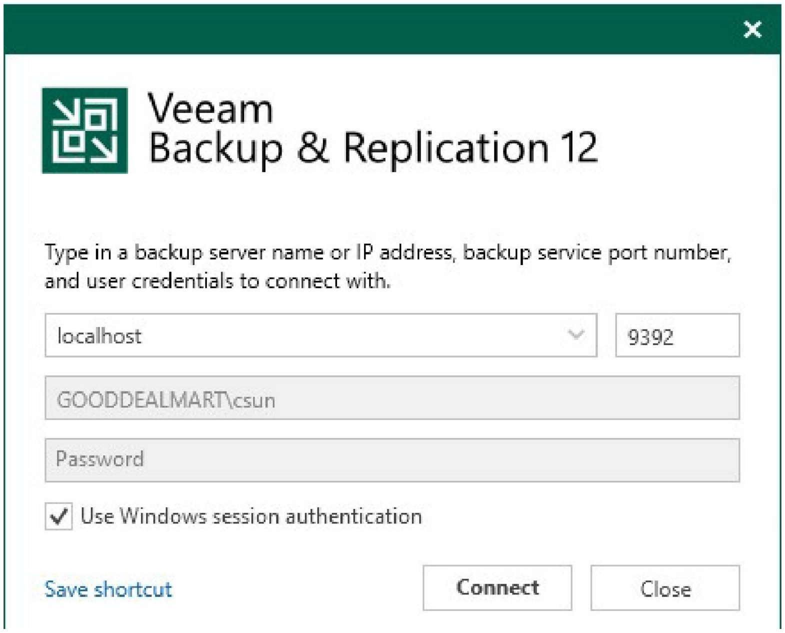
Summary:

```
Configuration migration is completed successfully

Source backup file: C:\Post-Install\VBR11_2023-02-01_12-13-23.bco
Target server: Microsoft SQL Server
Target server name: VBR12\SQLEXPRESS
Target database: VeeamBackup

Now you can start Veeam Backup and Replication Console
```

☑ Launch the Backup & Replication user interface

Veeam Backup and Replication Console will be launched automatically once the restore is completed.

36. Open Veeam Backup & Replication console and click Connect.



Veeam Backup & Replication 12

Type in a backup server name or IP address, backup service port number, and user credentials to connect with.

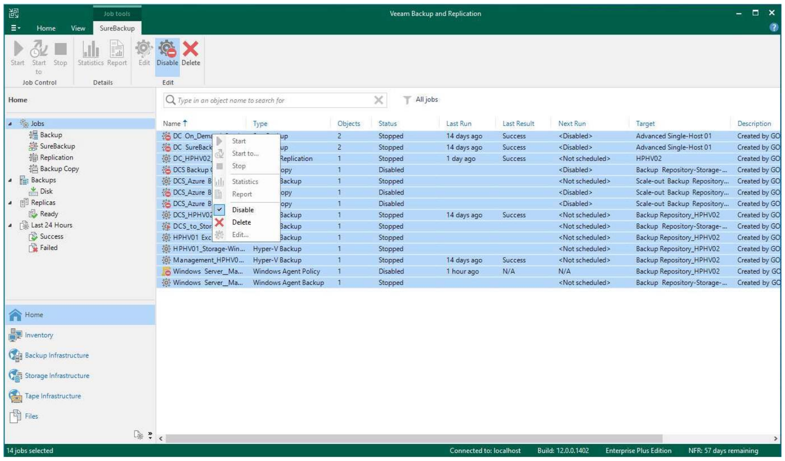
localhost | 9392

GOODDEALMART\csun

Password

☑ Use Windows session authentication

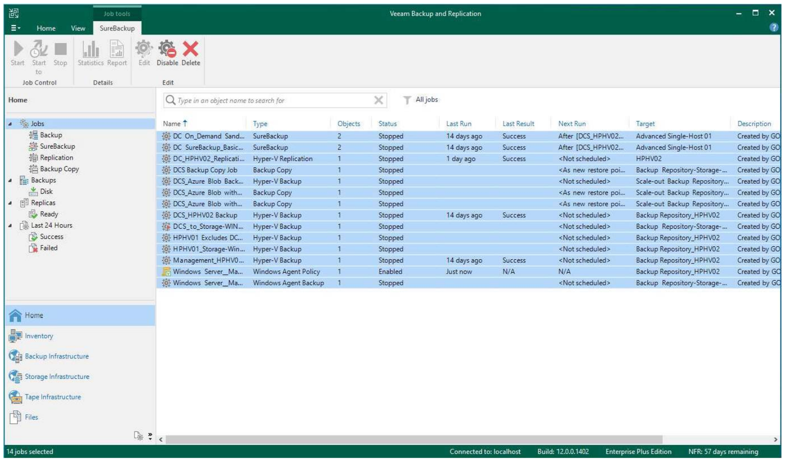
37. Select and right-click all jobs, and unselect Disable to enable all jobs.



Name	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
DC On_Dema	up	2	Stopped	14 days ago	Success	<Disabled>	Advanced Single-Host 01	Created by GO
DC SureBack	up	2	Stopped	14 days ago	Success	<Disabled>	Advanced Single-Host 01	Created by GO
DC_HPHV02_	Replication	1	Stopped	1 day ago	Success	<Not scheduled>	HPHV02	Created by GO
DCS Backup C	opy	1	Disabled			<Disabled>	Backup Repository-Storage-...	Created by GO
DCS_Azure B	Backup	1	Stopped			<Not scheduled>	Scale-out Backup Repository...	Created by GO
DCS_Azure B	opy	1	Disabled			<Disabled>	Scale-out Backup Repository...	Created by GO
DCS_Azure B	opy	1	Disabled			<Disabled>	Scale-out Backup Repository...	Created by GO
DCS_HPHV02	Backup	1	Stopped	14 days ago	Success	<Not scheduled>	Backup Repository_HPHV02	Created by GO
DCS_to_Stor	Backup	1	Stopped			<Not scheduled>	Backup Repository-Storage-...	Created by GO
HPHV01 Exc	Backup	1	Stopped			<Not scheduled>	Backup Repository_HPHV02	Created by GO
HPHV01_Storage-Win...	Hyper-V Backup	1	Stopped			<Not scheduled>	Backup Repository_HPHV02	Created by GO
Management_HPHV0...	Hyper-V Backup	1	Stopped	14 days ago	Success	<Not scheduled>	Backup Repository_HPHV02	Created by GO
Windows Server__Ma...	Windows Agent Policy	1	Disabled	1 hour ago	N/A	N/A	Backup Repository_HPHV02	Created by GO
Windows Server__Ma...	Windows Agent Backup	1	Stopped			<Not scheduled>	Backup Repository-Storage-...	Created by GO

14 jobs selected | Connected to: localhost | Build: 12.0.0.1402 | Enterprise Plus Edition | NFR: 57 days remaining

38. Ensure all jobs are re-enabled.

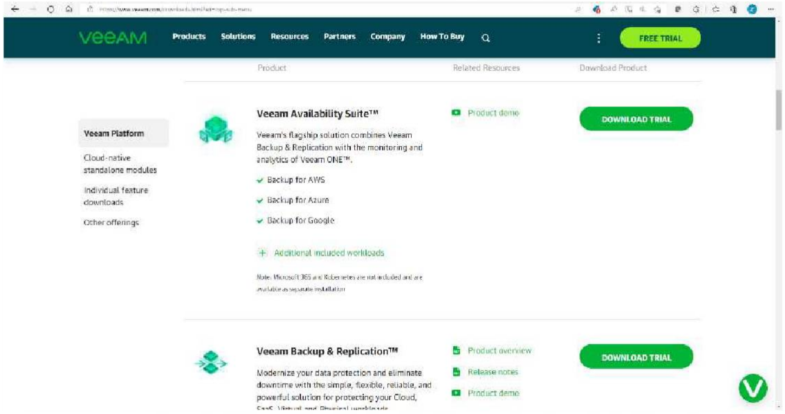
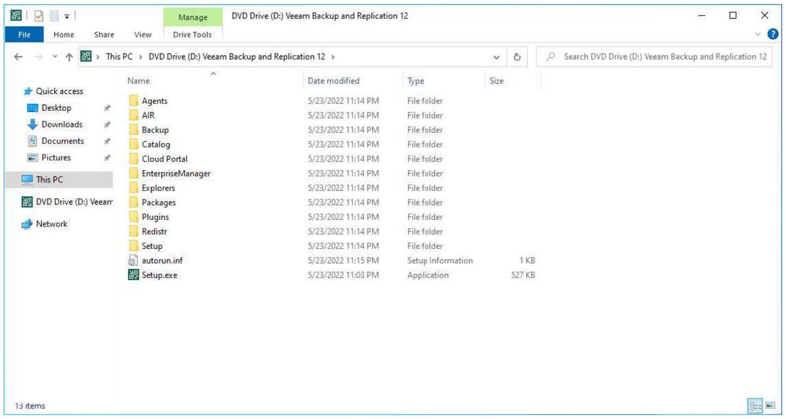


Name ↑	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Description
DC On_Demand Sand...	SureBackup	2	Stopped	14 days ago	Success	After [DCS_HPHV02...	Advanced Single-Host 01	Created by GO
DC SureBackup_Basic...	SureBackup	2	Stopped	14 days ago	Success	After [DCS_HPHV02...	Advanced Single-Host 01	Created by GO
DC_HPHV02_Replicati...	Hyper-V Replication	1	Stopped	1 day ago	Success	<Not scheduled>	HPHV02	Created by GO
DCS Backup Copy Job	Backup Copy	1	Stopped			<As new restore poi...	Backup Repository-Storage-...	Created by GO
DCS_Azure Blob Back...	Hyper-V Backup	1	Stopped			<Not scheduled>	Scale-out Backup Repository...	Created by GO
DCS_Azure Blob with...	Backup Copy	1	Stopped			<As new restore poi...	Scale-out Backup Repository...	Created by GO
DCS_Azure Blob with...	Backup Copy	1	Stopped			<As new restore poi...	Scale-out Backup Repository...	Created by GO
DCS_HPHV02 Backup	Hyper-V Backup	1	Stopped	14 days ago	Success	<Not scheduled>	Backup Repository_HPHV02	Created by GO
DCS_to_Storage-WIN...	Hyper-V Backup	1	Stopped			<Not scheduled>	Backup Repository-Storage-...	Created by GO
HPHV01 Excludes DC...	Hyper-V Backup	1	Stopped			<Not scheduled>	Backup Repository_HPHV02	Created by GO
HPHV01_Storage-Win...	Hyper-V Backup	1	Stopped			<Not scheduled>	Backup Repository_HPHV02	Created by GO
Management_HPHV0...	Hyper-V Backup	1	Stopped	14 days ago	Success	<Not scheduled>	Backup Repository_HPHV02	Created by GO
Windows Server_Ma...	Windows Agent Policy	1	Enabled	Just now	N/A	N/A	Backup Repository_HPHV02	Created by GO
Windows Server_Ma...	Windows Agent Backup	1	Stopped			<Not scheduled>	Backup Repository-Storage-...	Created by GO

14 jobs selected   Connected to: localhost   Build: 12.0.0.1402   Enterprise Plus Edition   NFR: 57 days remaining

Install Veeam Backup and Replication Console 12

When you install Veeam Backup & Replication, the Veeam Backup & Replication console is automatically installed on the backup server. If you want to access Veeam Backup & Replication remotely, you can install the Veeam Backup & Replication console on a dedicated machine.

Instructions	Screenshot (if applicable)
1. Log in to the Veeam Backup and Replication manager console machine. 2. Download the Veeam Backup and Replication v12 ISO image file from the Veeam website sign-in required).	
3. Mount Veeam Backup & Replication v12 iso image file. 4. Run Setup.exe.	

Veeam Availability Suite™

Veeam's flagship solution combines Veeam Backup & Replication with the monitoring and analytics of Veeam ONE™.

- ✓ Backup for AWS
- ✓ Backup for Azure
- ✓ Backup for Google

+ Additional included workloads

Note: Microsoft 365 and Kubernetes are not included and are available as separate installation

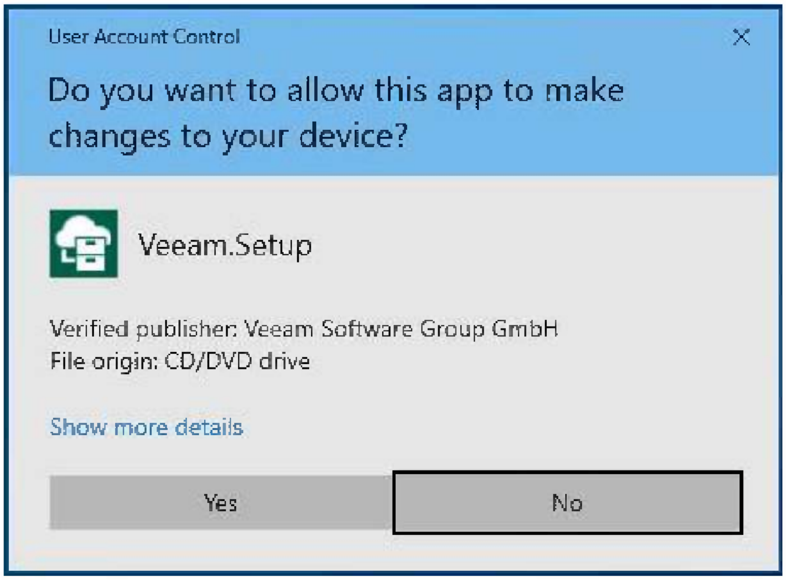
Veeam Backup & Replication™

Modernize your data protection and eliminate downtime with the simple, flexible, reliable, and powerful solution for protecting your Cloud, SaaS, Virtual and Physical workloads

Manage
DVD Drive (D:) Veeam Backup and Replication 12
File
Home
Share
View
Drive Tools
This PC › DVD Drive (D:) Veeam Backup and Replication 12 ›
Search DVD Drive (D:) Veeam Backup and Replication 12
Quick access
Desktop
Downloads
Documents
Pictures
This PC
DVD Drive (D:) Veeam
Network
13 items

Name	Date modified	Type	Size
Agents	5/23/2022 11:14 PM	File folder	
AIR	5/23/2022 11:14 PM	File folder	
Backup	5/23/2022 11:14 PM	File folder	
Catalog	5/23/2022 11:14 PM	File folder	
Cloud Portal	5/23/2022 11:14 PM	File folder	
EnterpriseManager	5/23/2022 11:14 PM	File folder	
Explorers	5/23/2022 11:14 PM	File folder	
Packages	5/23/2022 11:14 PM	File folder	
Plugins	5/23/2022 11:14 PM	File folder	
Redistr	5/23/2022 11:14 PM	File folder	
Setup	5/23/2022 11:14 PM	File folder	
autorun.inf	5/23/2022 11:15 PM	Setup Information	1 KB
Setup.exe	5/23/2022 11:03 PM	Application	527 KB

5. On the User Access Control page, click Yes.



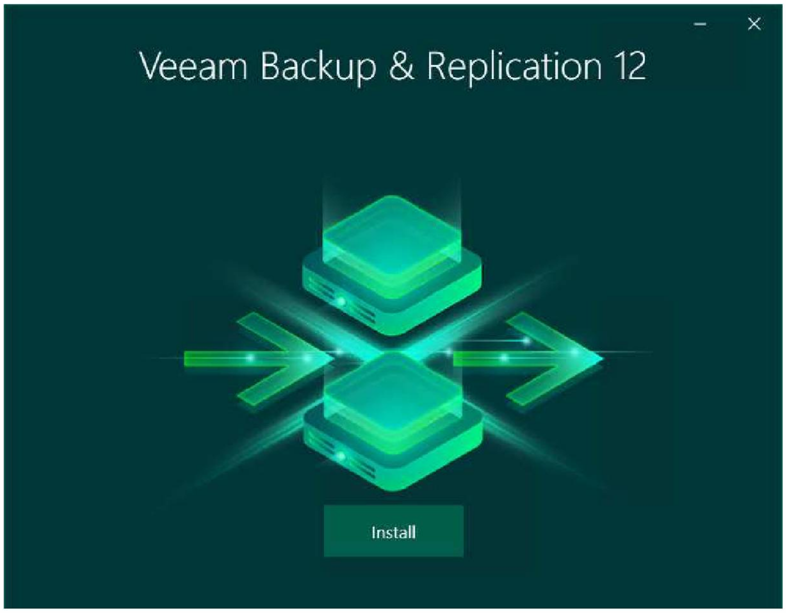
User Account Control

Do you want to allow this app to make changes to your device?

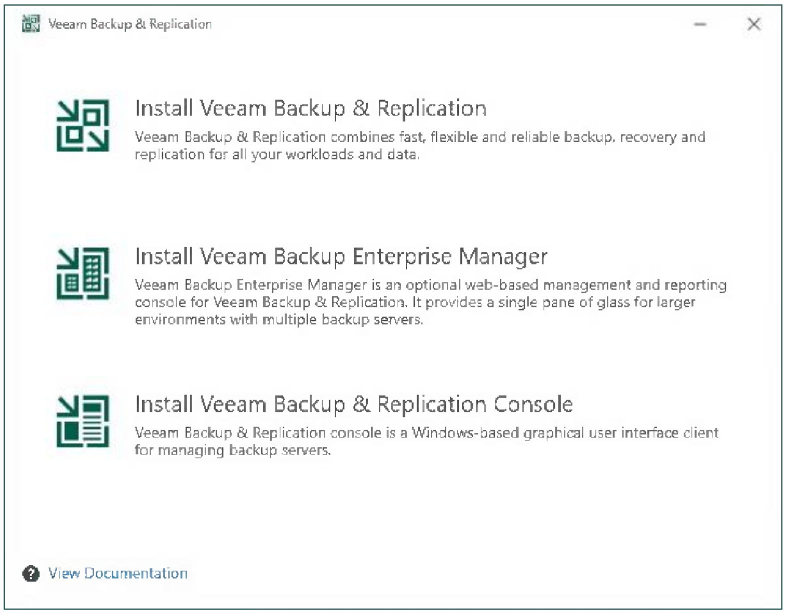
Veeam.Setup

Verified publisher: Veeam Software Group GmbH
File origin: CD/DVD drive

6. On the Veeam Backup & Replication 12 page, click Install.



7. Select Install Veeam Backup & Replication Console on the Veeam Backup & Replication page



Veeam Backup & Replication

Install Veeam Backup & Replication

Veeam Backup & Replication combines fast, flexible and reliable backup, recovery and replication for all your workloads and data.

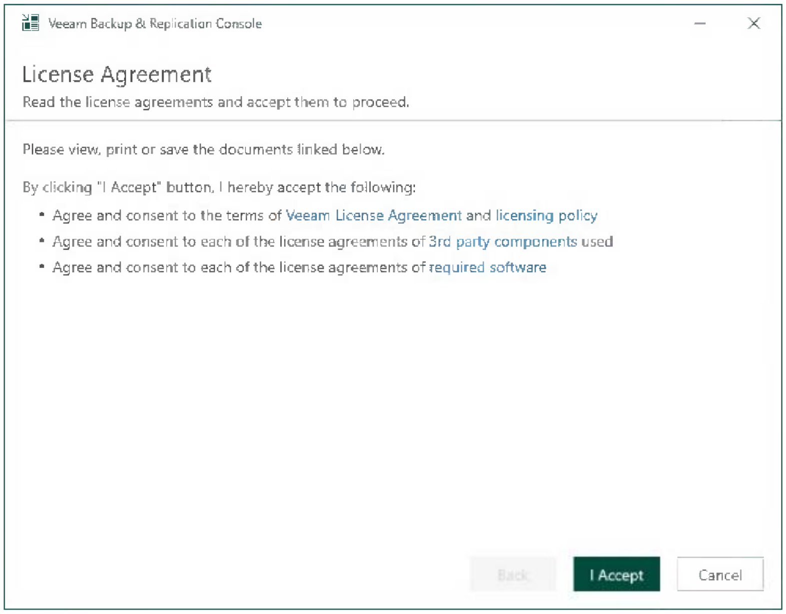
Install Veeam Backup Enterprise Manager

Veeam Backup Enterprise Manager is an optional web-based management and reporting console for Veeam Backup & Replication. It provides a single pane of glass for larger environments with multiple backup servers.

Install Veeam Backup & Replication Console

Veeam Backup & Replication console is a Windows-based graphical user interface client for managing backup servers.

8. Click I Accept on the License Agreement page.



Veeam Backup & Replication Console

License Agreement

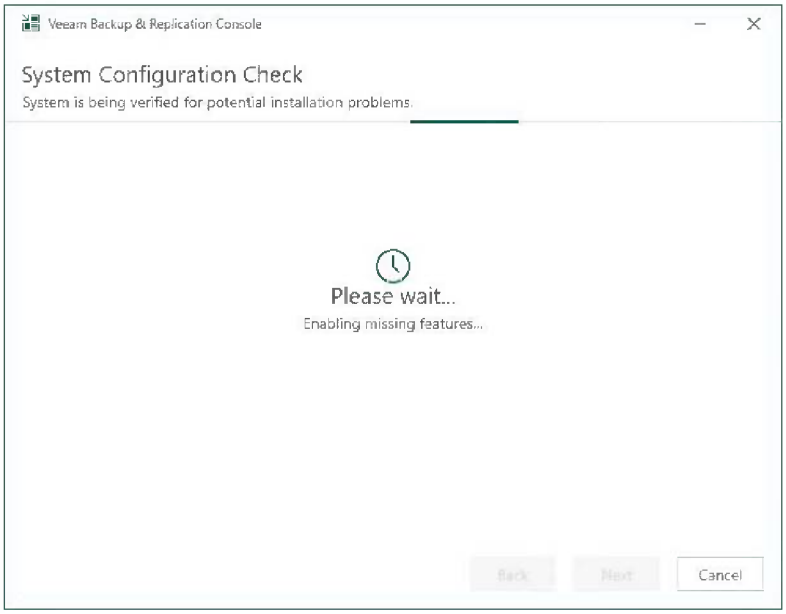
Read the license agreements and accept them to proceed.

Please view, print or save the documents linked below.

By clicking "I Accept" button, I hereby accept the following:

- Agree and consent to the terms of Veeam License Agreement and licensing policy
- Agree and consent to each of the license agreements of 3rd party components used
- Agree and consent to each of the license agreements of required software

9. The setup wizard checks if the required software is installed on the machine during the System Configuration Check step. If required components are missing, the setup will attempt to install them independently. Rebooting is required after the components have been successfully installed. Click Reboot to restart the machine.



Veeam Backup & Replication Console

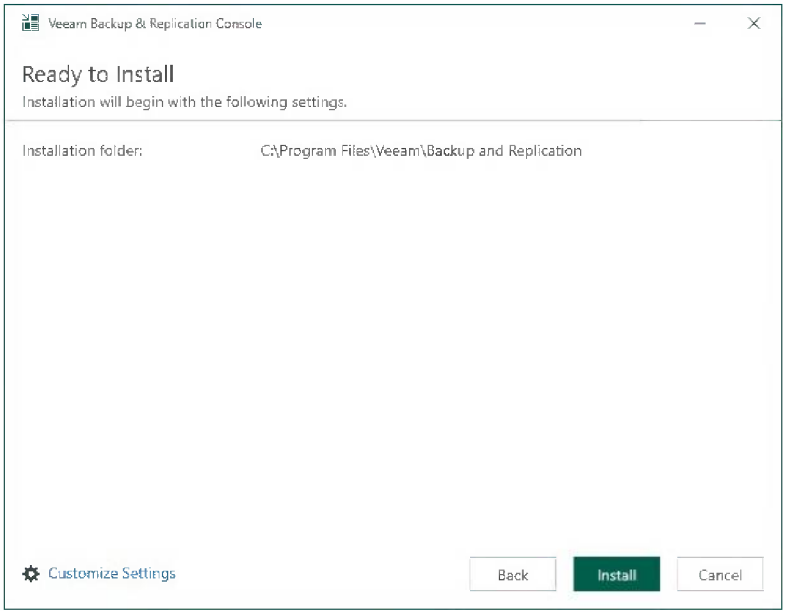
System Configuration Check

System is being verified for potential installation problems.

Please wait...

Enabling missing features...

10. Click Customize Settings on the Ready to Install page.



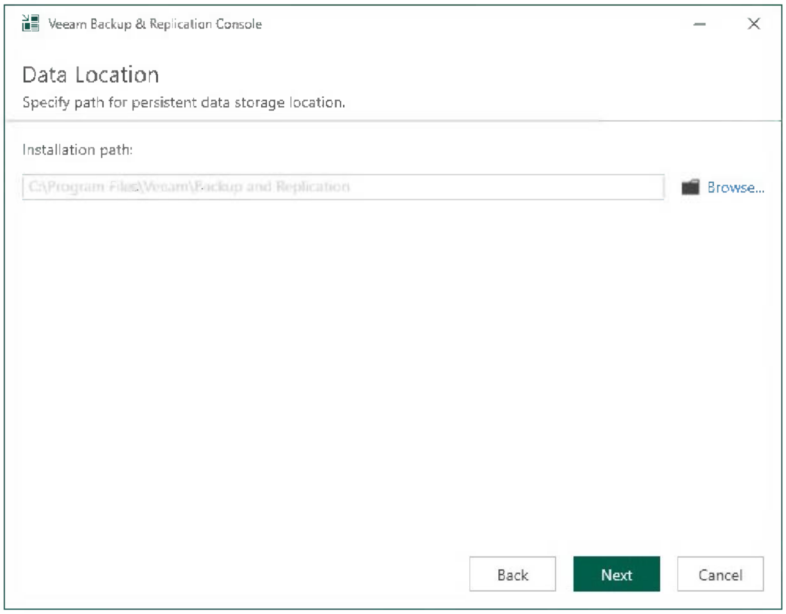
Veeam Backup & Replication Console

Ready to Install

Installation will begin with the following settings.

Installation folder: C:\Program Files\Veeam\Backup and Replication

11. On the Data locations page, click Browse and select the path in the Installation path field.
12. Click Next.



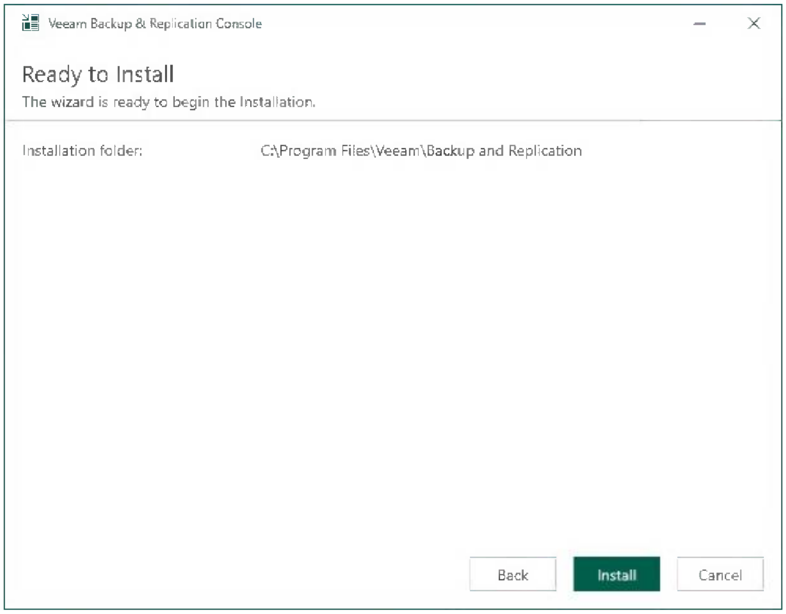
Data Location

Specify path for persistent data storage location.

Installation path:

C:\Program Files\Veeam\Backup and Replication

13. Click Install on the Ready to Install page.

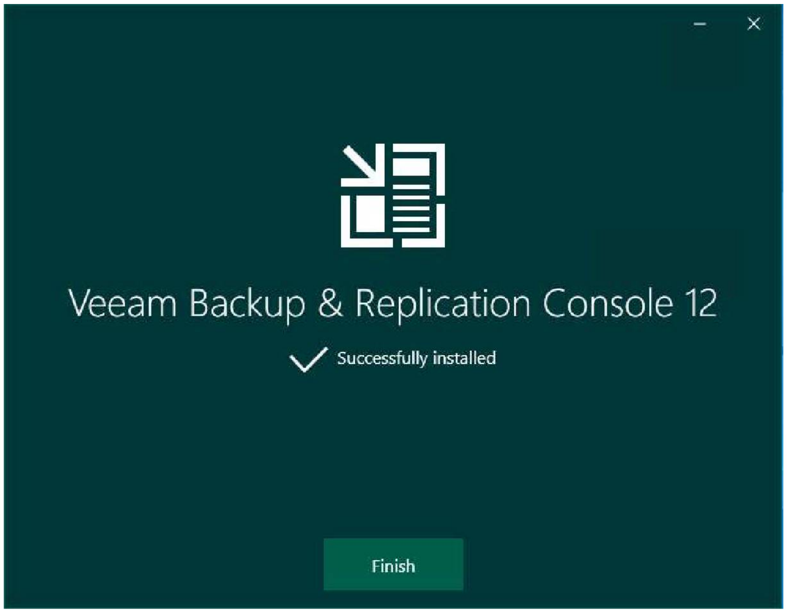


Ready to Install

The wizard is ready to begin the Installation.

Installation folder: C:\Program Files\Veeam\Backup and Replication

14. Click Finish on the Veeam Backup & Replication 12 Successfully installed page.

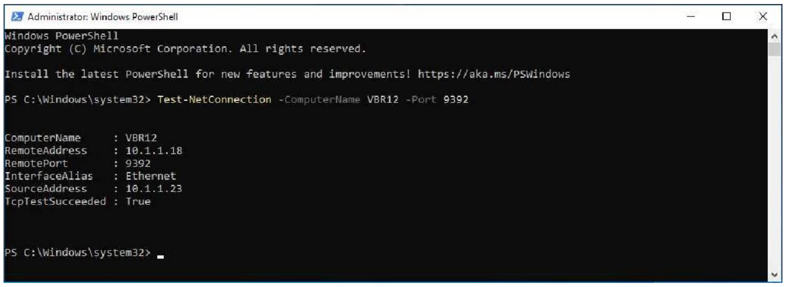


Veeam Backup & Replication Console 12

✓ Successfully installed

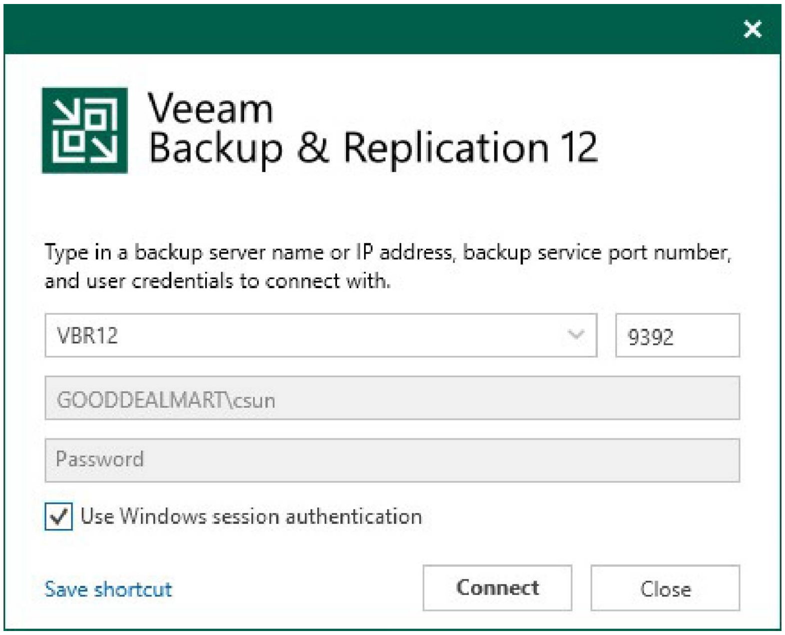
15. Verify that the Veeam Backup Service is running on the Veeam Backup Server, and then test connectivity to that service from the remote machine using the following PowerShell cmdlet.

Test-NetConnection -ComputerName <hostname/ip> -Port 9392



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> Test-NetConnection -ComputerName VBR12 -Port 9392


ComputerName     : VBR12
RemoteAddress    : 10.1.1.18
RemotePort       : 9392
InterfaceAlias   : Ethernet
SourceAddress    : 10.1.1.23
TcpTestSucceeded : True



PS C:\Windows\system32> _
```

16. Open the Veeam Backup & Replication Console, click Connect, enter the Backup & Replication manager server name or IP address, and click Connect.



Type in a backup server name or IP address, backup service port number, and user credentials to connect with.

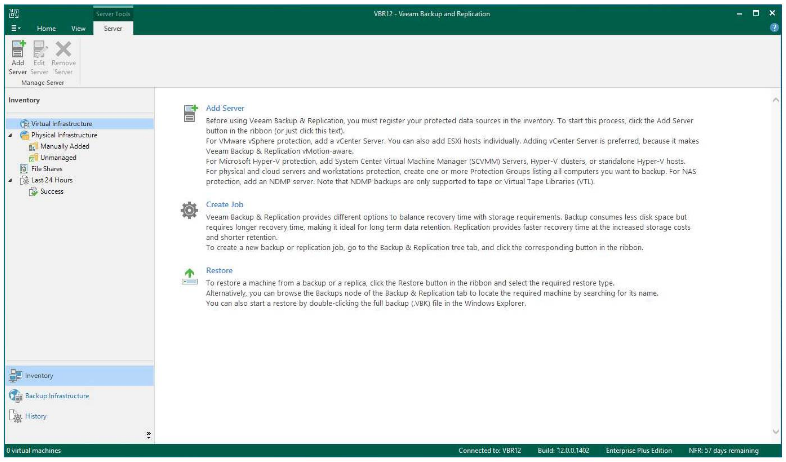
VBR12 | 9392

GOODDEALMART\csun

Password

☑ Use Windows session authentication

17. Ensure you can connect to the Veeam Backup & Replication manager server without issue.



Add Server

Before using Veeam Backup & Replication, you must register your protected data sources in the inventory. To start this process, click the Add Server button in the ribbon (or just click this text).
For VMware vSphere protection, add a vCenter Server. You can also add ESXi hosts individually. Adding vCenter Server is preferred, because it makes Veeam Backup & Replication vMotion-aware.
For Microsoft Hyper-V protection, add System Center Virtual Machine Manager (SCVMM) Servers, Hyper-V clusters, or standalone Hyper-V hosts.
For physical and cloud servers and workstations protection, create one or more Protection Groups listing all computers you want to backup. For NAS protection, add an NDMP server. Note that NDMP backups are only supported to tape or Virtual Tape Libraries (VTL).

Create Job

Veeam Backup & Replication provides different options to balance recovery time with storage requirements. Backup consumes less disk space but requires longer recovery time, making it ideal for long term data retention. Replication provides faster recovery time at the increased storage costs and shorter retention.
To create a new backup or replication job, go to the Backup & Replication tree tab, and click the corresponding button in the ribbon.

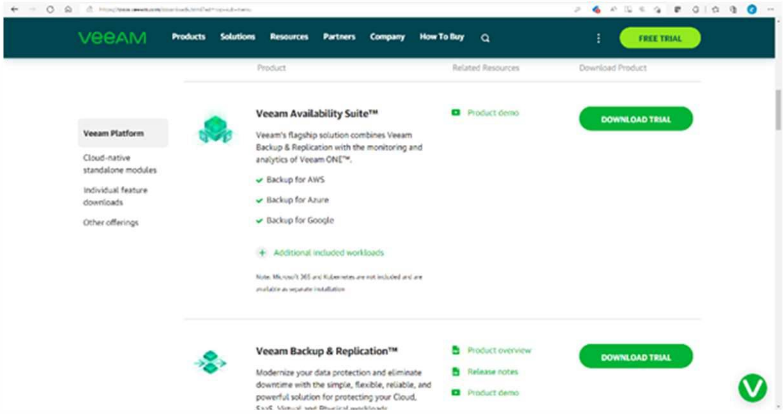
Restore

To restore a machine from a backup or a replica, click the Restore button in the ribbon and select the required restore type.
Alternatively, you can browse the Backups node of the Backup & Replication tab to locate the required machine by searching for its name.
You can also start a restore by double-clicking the full backup (.VBK) file in the Windows Explorer.

0 virtual machines | Connected to: VBR12 | Build: 12.0.0.1402 | Enterprise Plus Edition | NFR: 57 days remaining

Upgrade to Veeam Backup and Replication Console 12

To gain remote access to Veeam Backup & Replication v12, you must first upgrade the Veeam Backup & Replication console to v12 on a dedicated machine.

Instructions	Screenshot (if applicable)
1. Log in to the existing Veeam Backup and replication manager console machine. 2. Download the Veeam Backup and Replication v12 iso image file from the Veeam website. (Sign-in required).	

Veeam Availability Suite™

Veeam's flagship solution combines Veeam Backup & Replication with the monitoring and analytics of Veeam ONE™.

- ✓ Backup for AWS
- ✓ Backup for Azure
- ✓ Backup for Google

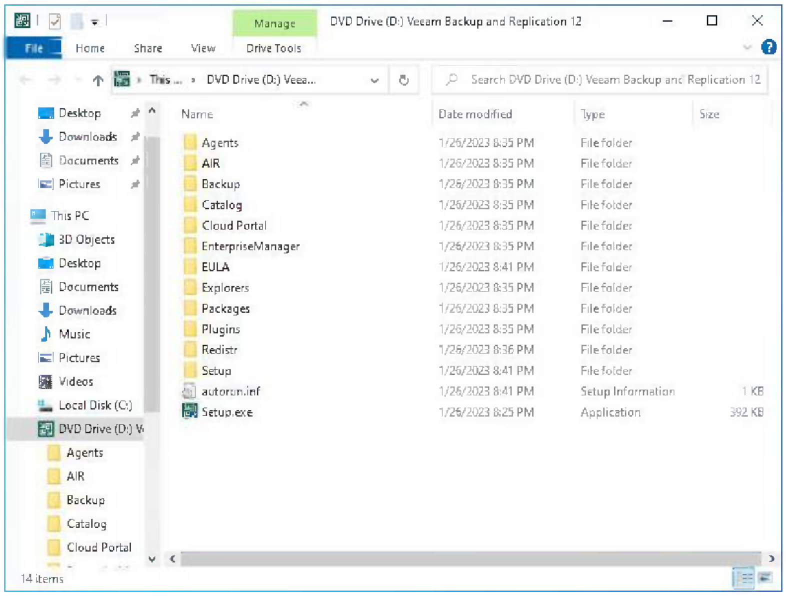
+ Additional included workloads

Note: Microsoft 365 and Kubernetes are not included and are available as separate installation

Veeam Backup & Replication™

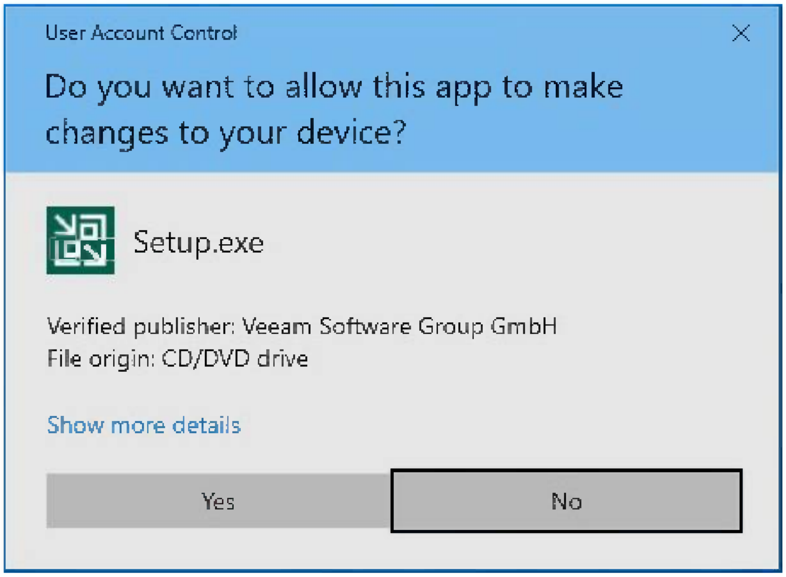
Modernize your data protection and eliminate downtime with the simple, flexible, reliable, and powerful solution for protecting your Cloud, SaaS, Virtual and Physical workloads

3. Mount the Veeam Backup & Replication v12 ISO image file.
4. Run Setup.exe.



Name	Date modified	Type	Size
Agents	1/26/2023 8:35 PM	File folder	
AIR	1/26/2023 8:35 PM	File folder	
Backup	1/26/2023 8:35 PM	File folder	
Catalog	1/26/2023 8:35 PM	File folder	
Cloud Portal	1/26/2023 8:35 PM	File folder	
EnterpriseManager	1/26/2023 8:35 PM	File folder	
EULA	1/26/2023 8:41 PM	File folder	
Explorers	1/26/2023 8:35 PM	File folder	
Packages	1/26/2023 8:35 PM	File folder	
Plugins	1/26/2023 8:35 PM	File folder	
Redistr	1/26/2023 8:36 PM	File folder	
Setup	1/26/2023 8:41 PM	File folder	
autorun.inf	1/26/2023 8:41 PM	Setup Information	1 KB
Setup.exe	1/26/2023 8:25 PM	Application	392 KB

5. Click Yes on the User Account Control page.

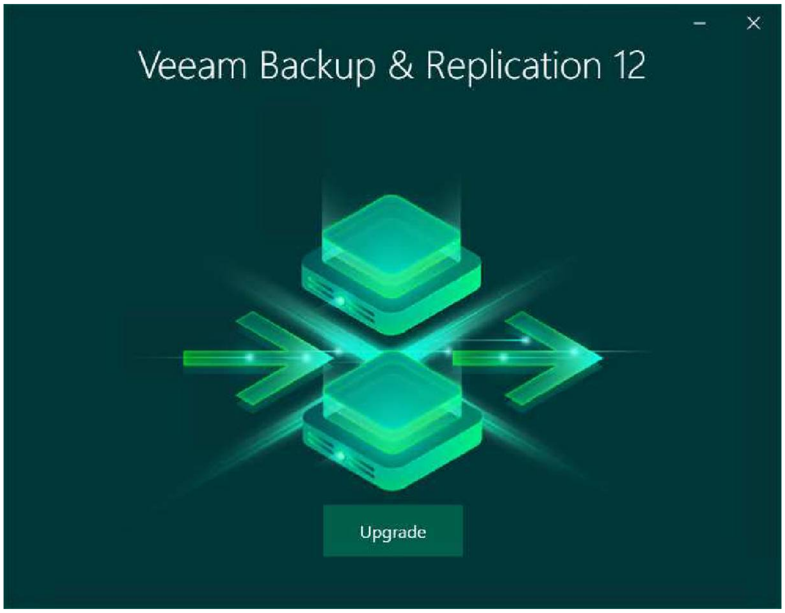

User Account Control

Do you want to allow this app to make changes to your device?

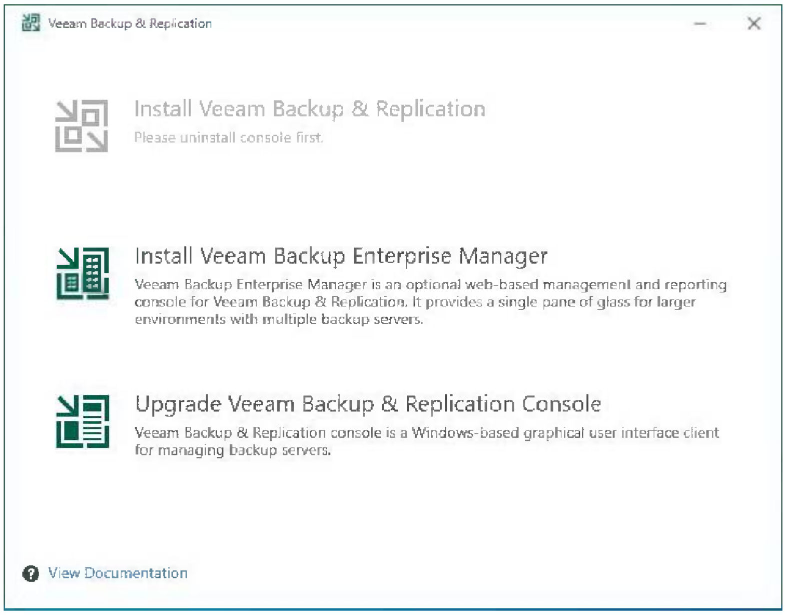
Setup.exe

Verified publisher: Veeam Software Group GmbH
File origin: CD/DVD drive

6. Click Upgrade on the Veeam Backup & Replication 12 page.



7. Select Upgrade Veeam Backup & Replication Console on the Veeam Backup & Replication page.



Veeam Backup & Replication

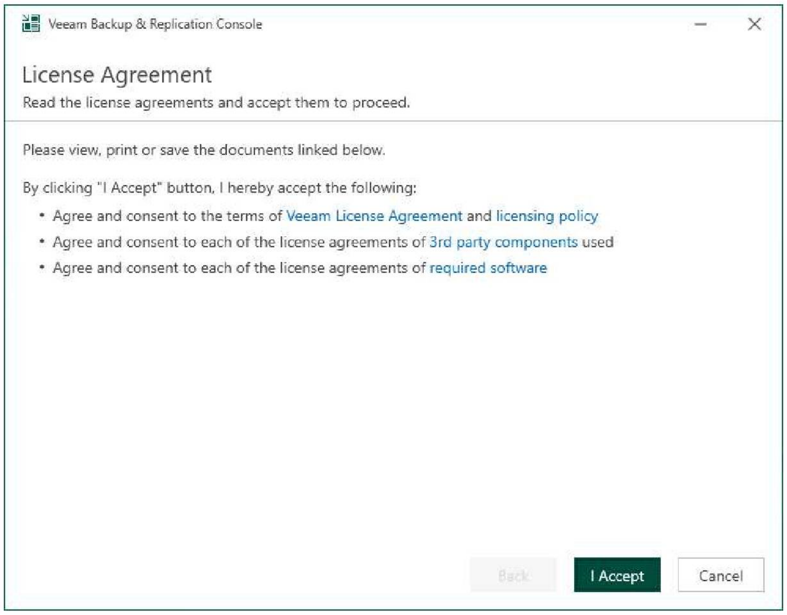
Install Veeam Backup & Replication
Please uninstall console first.

Install Veeam Backup Enterprise Manager
Veeam Backup Enterprise Manager is an optional web-based management and reporting console for Veeam Backup & Replication. It provides a single pane of glass for larger environments with multiple backup servers.

Upgrade Veeam Backup & Replication Console
Veeam Backup & Replication console is a Windows-based graphical user interface client for managing backup servers.

View Documentation

8. On the License Agreement page, click I Accept.



License Agreement

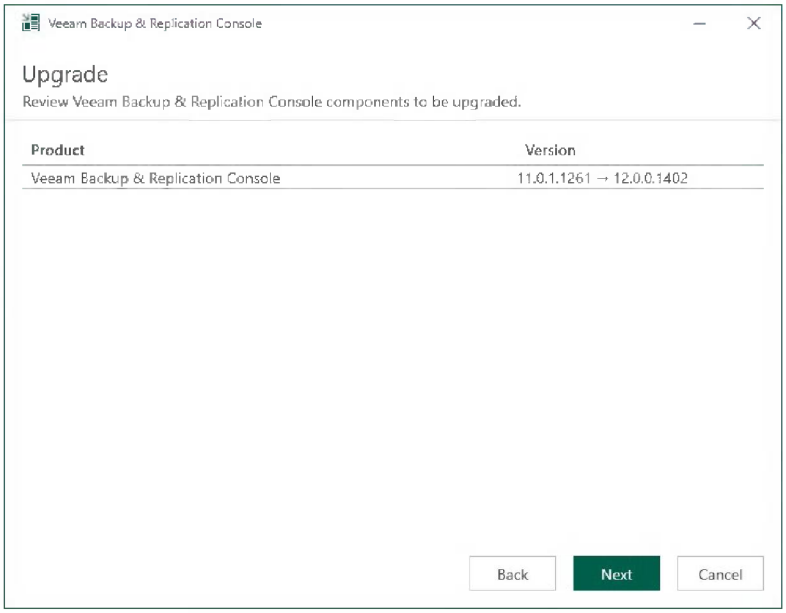
Read the license agreements and accept them to proceed.

Please view, print or save the documents linked below.

By clicking "I Accept" button, I hereby accept the following:

- Agree and consent to the terms of Veeam License Agreement and licensing policy
- Agree and consent to each of the license agreements of 3rd party components used
- Agree and consent to each of the license agreements of required software

9. On the Upgrade page, click Next.

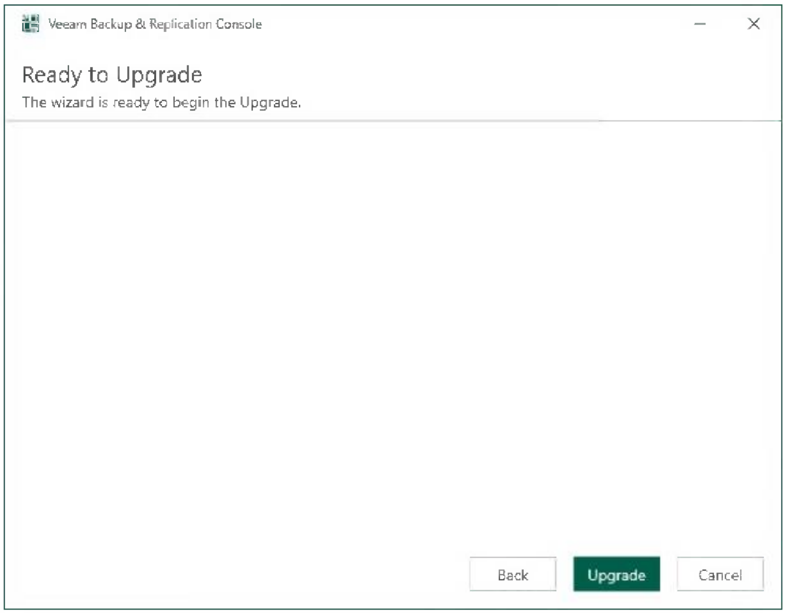


Upgrade

Review Veeam Backup & Replication Console components to be upgraded.

Product	Version
Veeam Backup & Replication Console	11.0.1.1261 → 12.0.0.1402

10. Click Upgrade on the Ready to Upgrade page.

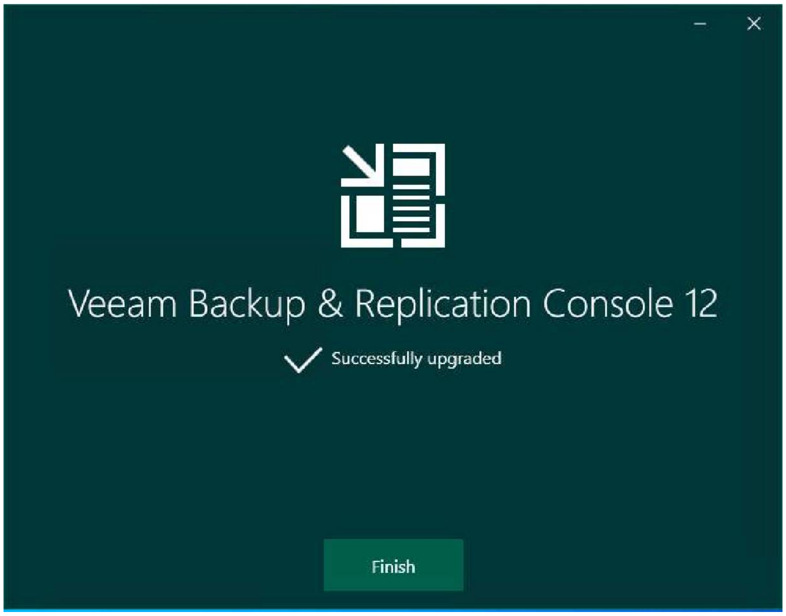


Veeam Backup & Replication Console

Ready to Upgrade

The wizard is ready to begin the Upgrade.

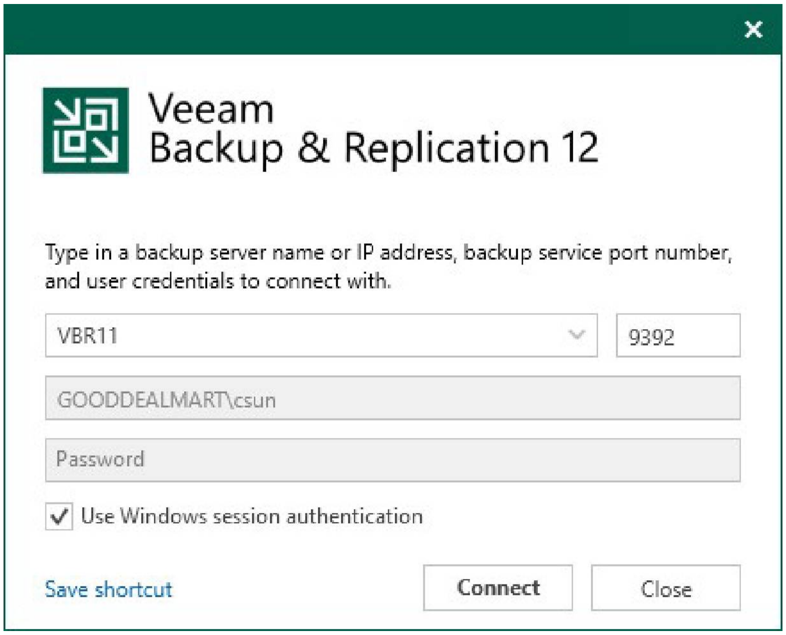
11. Click Finish on the Veeam Backup & Replication Console 12 successfully upgraded page.



Veeam Backup & Replication Console 12

Successfully upgraded

12. Open Veeam and Replication Console 12 and click Connect.



Veeam
Backup & Replication 12

Type in a backup server name or IP address, backup service port number, and user credentials to connect with.

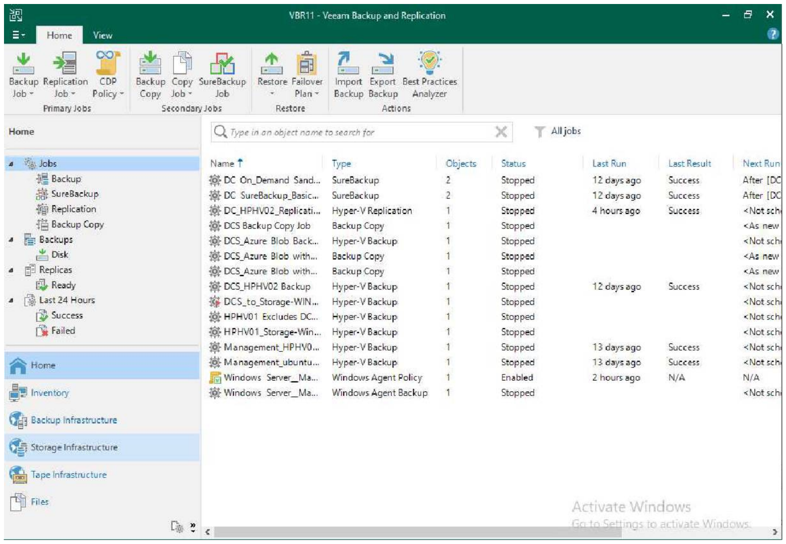
VBR11 | 9392

GOODDEALMART\csun

Password

☑ Use Windows session authentication

13. Ensure connection to Veeam Backup and Replication manager server is successful.



Name	Type	Objects	Status	Last Run	Last Result	Next Run
DC On_Demand Sand...	SureBackup	2	Stopped	12 days ago	Success	After [DC
DC SureBackup_Basic...	SureBackup	2	Stopped	12 days ago	Success	After [DC
DC_HPHV02_Replicati...	Hyper-V Replication	1	Stopped	4 hours ago	Success	<Not sch
DCS Backup Copy Job	Backup Copy	1	Stopped			<As new
DCS_Azure Blob Back...	Hyper-V Backup	1	Stopped			<Not sch
DCS_Azure Blob with...	Backup Copy	1	Stopped			<As new
DCS_Azure Blob with...	Backup Copy	1	Stopped			<As new
DCS_HPHV02 Backup	Hyper-V Backup	1	Stopped	12 days ago	Success	<Not sch
DCS_to_Storage-WIN...	Hyper-V Backup	1	Stopped			<Not sch
HPHV01 Excludes DC...	Hyper-V Backup	1	Stopped			<Not sch
HPHV01_Storage-Win...	Hyper-V Backup	1	Stopped			<Not sch
Management_HPHV0...	Hyper-V Backup	1	Stopped	13 days ago	Success	<Not sch
Management_ubuntu...	Hyper-V Backup	1	Stopped	13 days ago	Success	<Not sch
Windows Server_Ma...	Windows Agent Policy	1	Enabled	2 hours ago	N/A	N/A
Windows Server_Ma...	Windows Agent Backup	1	Stopped			<Not sch

Chapter 3 Configuration

This chapter will review the initial configurations of Veeam Backup and Replication. These include:

- Add Virtualization Servers and Hosts
- Add Physical Machines
- Add Backup Repositories
- Generation Settings

These steps must be configured before setting up Backup Jobs, covered in the next chapter.

Virtualization Servers and Hosts

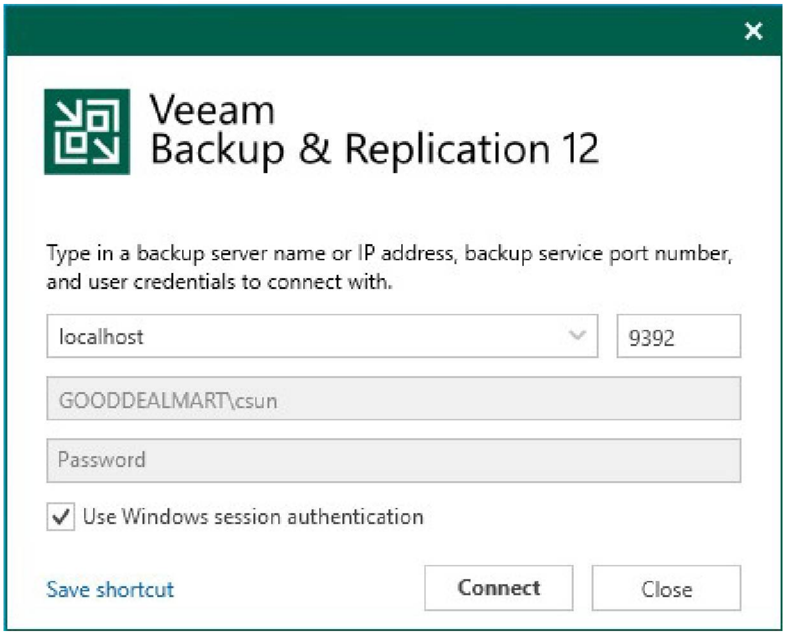
Veeam Backup & Replication allows you to build a scalable backup infrastructure for many environments. Physical and virtual machines can be added to the backup infrastructure and assigned different roles. In addition, Veeam Backup and Replication components can coexist on the same machine.

The Backup Infrastructure can be expanded with the following types of servers and hosts:

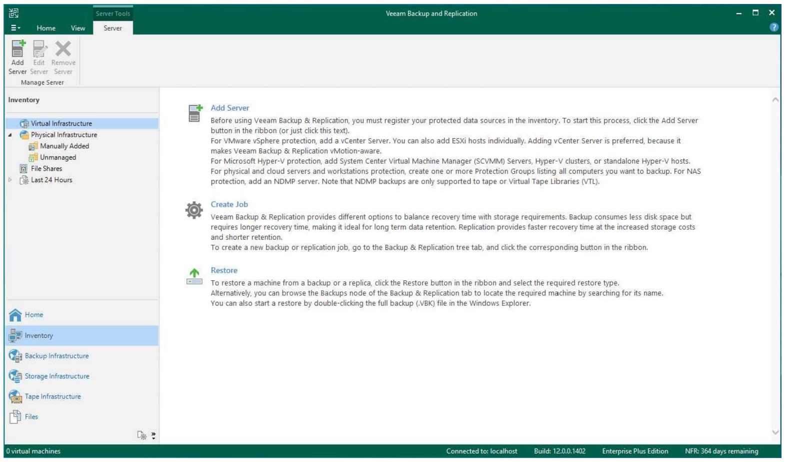
- Microsoft Hyper-V Standalone Servers
- Microsoft Hyper-V Cluster Servers
- Microsoft SMB3 Servers
- Microsoft Windows Servers
- Linux Server

Add Microsoft Hyper-V Standalone Servers

You must add the Microsoft Hyper-V standalone hosts you plan to use as source and target for backup, replication and other activities.

Instructions	Screenshot (if applicable)
1. Log in to the Veeam Backup and replication manager server. 2. Open the Veeam Backup & Replication Console, and click Connect.	 Veeam Backup & Replication 12 Type in a backup server name or IP address, backup service port number, and user credentials to connect with. localhost 9392 GOODDEALMART\csun Password ☑ Use Windows session authentication

3. On the Home page, select Inventory.
4. On the Inventory page, select Virtual Infrastructure and click Add Server.



Add Server

Before using Veeam Backup & Replication, you must register your protected data sources in the inventory. To start this process, click the Add Server button in the ribbon (or just click this text).
For VMware vSphere protection, add a vCenter Server. You can also add ESXi hosts individually. Adding vCenter Server is preferred, because it makes Veeam Backup & Replication vMotion-aware.
For Microsoft Hyper-V protection, add System Center Virtual Machine Manager (SCVMM) Servers, Hyper-V clusters, or standalone Hyper-V hosts.
For physical and cloud servers and workstations protection, create one or more Protection Groups listing all computers you want to backup. For NAS protection, add an NDMP server. Note that NDMP backups are only supported to tape or Virtual Tape Libraries (VTL).

Create Job

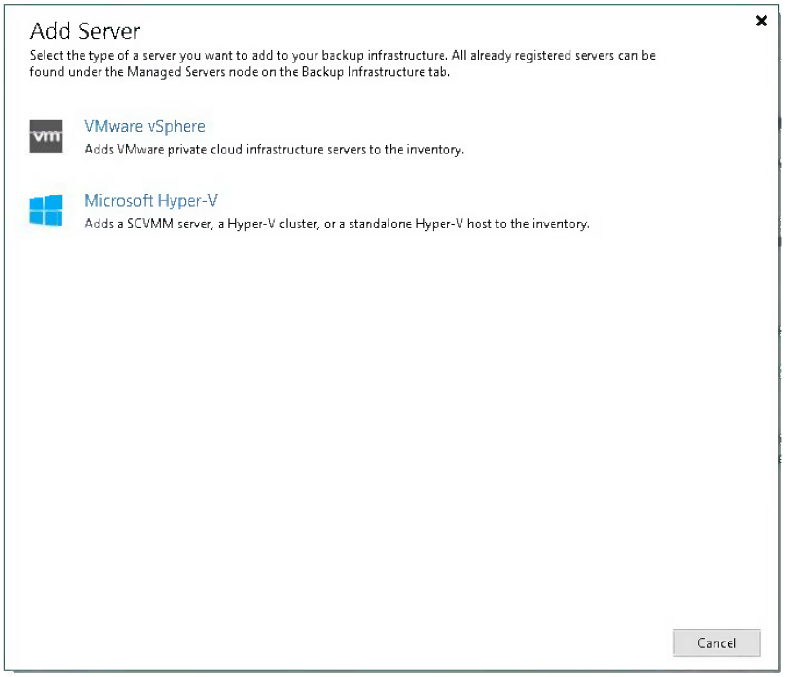
Veeam Backup & Replication provides different options to balance recovery time with storage requirements. Backup consumes less disk space but requires longer recovery time, making it ideal for long term data retention. Replication provides faster recovery time at the increased storage costs and shorter retention.
To create a new backup or replication job, go to the Backup & Replication tree tab, and click the corresponding button in the ribbon.

Restore

To restore a machine from a backup or a replica, click the Restore button in the ribbon and select the required restore type.
Alternatively, you can browse the Backups node of the Backup & Replication tab to locate the required machine by searching for its name.
You can also start a restore by double-clicking the full backup (.VBK) file in the Windows Explorer.

0 virtual machines | Connected to: localhost | Build: 12.0.0.1402 | Enterprise Plus Edition | NFR: 364 days remaining

5. On the Add Server page, select Microsoft Hyper-V.



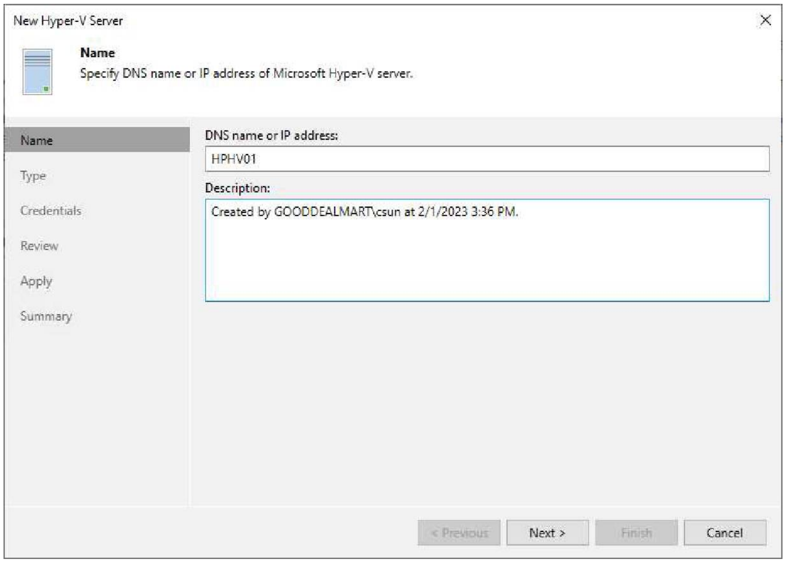
Add Server

Select the type of a server you want to add to your backup infrastructure. All already registered servers can be found under the Managed Servers node on the Backup Infrastructure tab.

VMware vSphere
Adds VMware private cloud infrastructure servers to the inventory.

Microsoft Hyper-V
Adds a SCVMM server, a Hyper-V cluster, or a standalone Hyper-V host to the inventory.

6. Enter the Microsoft Hyper-V server's full DNS name or IP address on the Name page.
7. Give a brief description in the Description field for future reference and click Next.



New Hyper-V Server

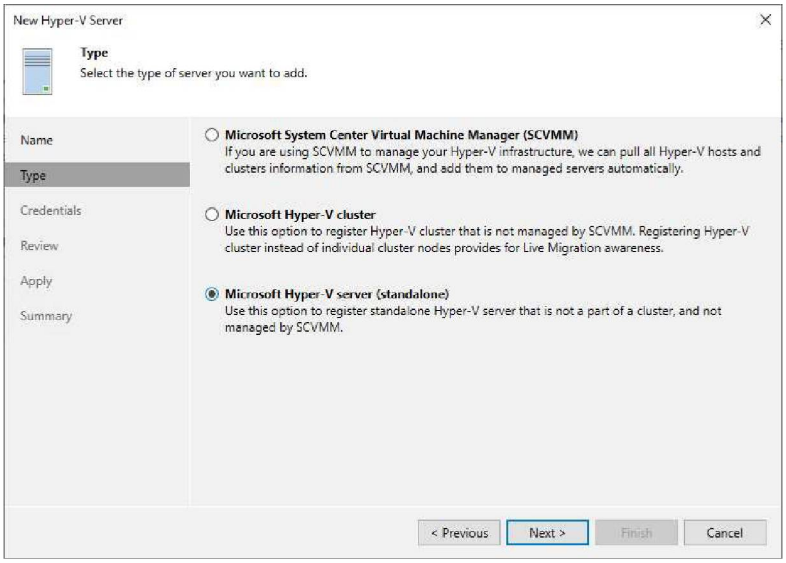
Name

Specify DNS name or IP address of Microsoft Hyper-V server.

DNS name or IP address: HPHV01

Description: Created by GOODDEALMART\csun at 2/1/2023 3:36 PM.

8. Select Microsoft Hyper-V server (standalone) on the Type page and click Next.



New Hyper-V Server

Type

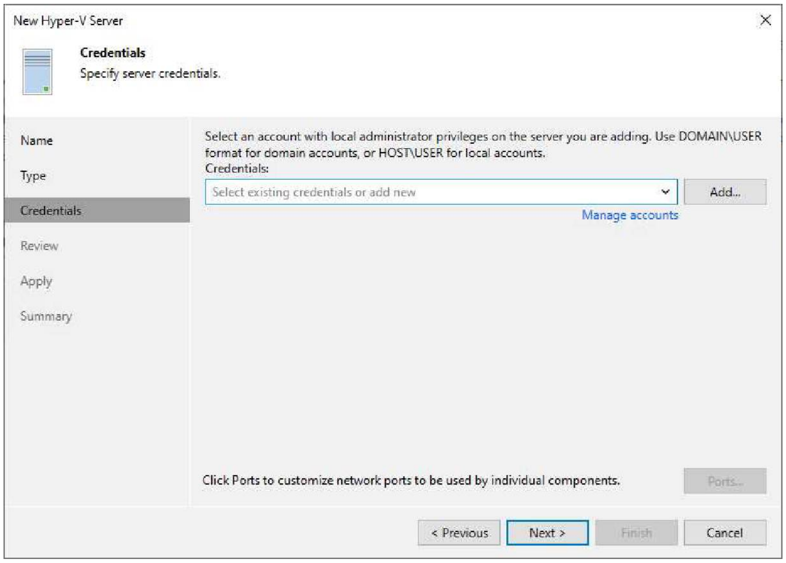
Select the type of server you want to add.

○ **Microsoft System Center Virtual Machine Manager (SCVMM)**
If you are using SCVMM to manage your Hyper-V infrastructure, we can pull all Hyper-V hosts and clusters information from SCVMM, and add them to managed servers automatically.

○ **Microsoft Hyper-V cluster**
Use this option to register Hyper-V cluster that is not managed by SCVMM. Registering Hyper-V cluster instead of individual cluster nodes provides for Live Migration awareness.

● **Microsoft Hyper-V server (standalone)**
Use this option to register standalone Hyper-V server that is not a part of a cluster, and not managed by SCVMM.

9. Select an account from the Credentials drop-down list on the Credentials page or click Add on the right to add the credentials.



New Hyper-V Server

Credentials

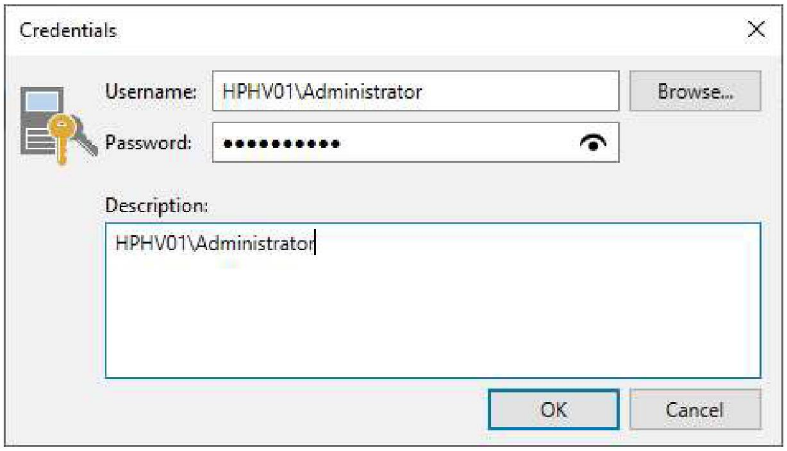
Specify server credentials.

Select an account with local administrator privileges on the server you are adding. Use DOMAIN\USER format for domain accounts, or HOST\USER for local accounts.

Credentials: Select existing credentials or add new

Click Ports to customize network ports to be used by individual components.

10. On the Credentials page, enter a user name in the Username field. You can also click Browse to select an existing user account.
11. Enter the password In the Password field.
12. Give a brief description in the Description field for future reference and click OK.



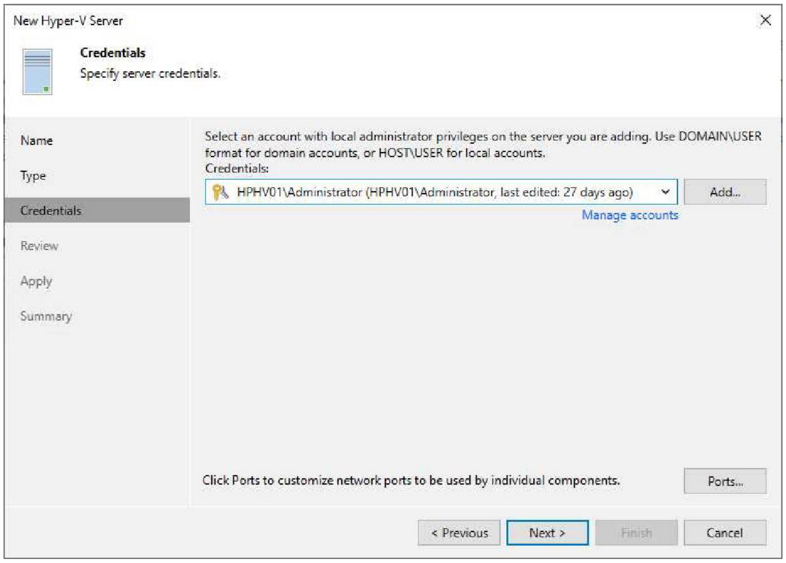
Credentials

Username: HPHV01\Administrator

Password: ●●●●●●●●●●●

Description: HPHV01\Administrator

13. On the Credentials page, click Ports.



New Hyper-V Server

Credentials

Specify server credentials.

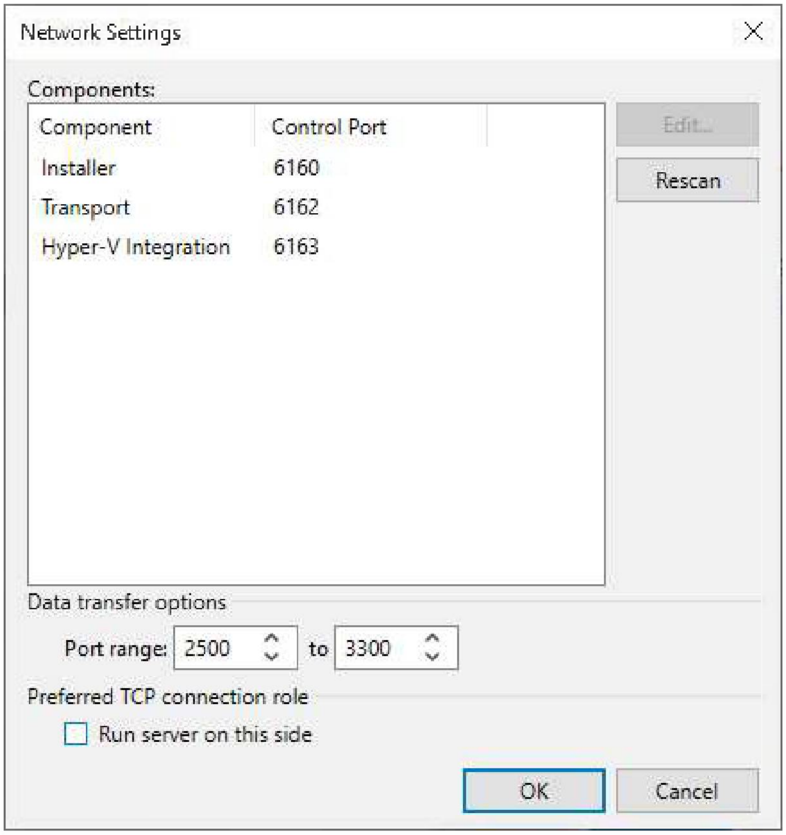
Select an account with local administrator privileges on the server you are adding. Use DOMAIN\USER format for domain accounts, or HOST\USER for local accounts.

Credentials:

HPHV01\Administrator (HPHV01\Administrator, last edited: 27 days ago)

Click Ports to customize network ports to be used by individual components.

14. If necessary, change the network ports used by Veeam Backup & Replication components on the Network Settings page.
15. Configure connection settings for file copy operations in the Network Settings window's Data transfer options section. Provide a set of ports for transmission channels between the source and target hosts (one port per task).
16. Select the Run server on this side checkbox in the Preferred TCP connection role section. The outside client cannot connect to the server on the NAT network in the NAT scenario. As a result, services that require external connection initiation may be disrupted.
17. Click OK.



Components:

Component	Control Port
Installer	6160
Transport	6162
Hyper-V Integration	6163

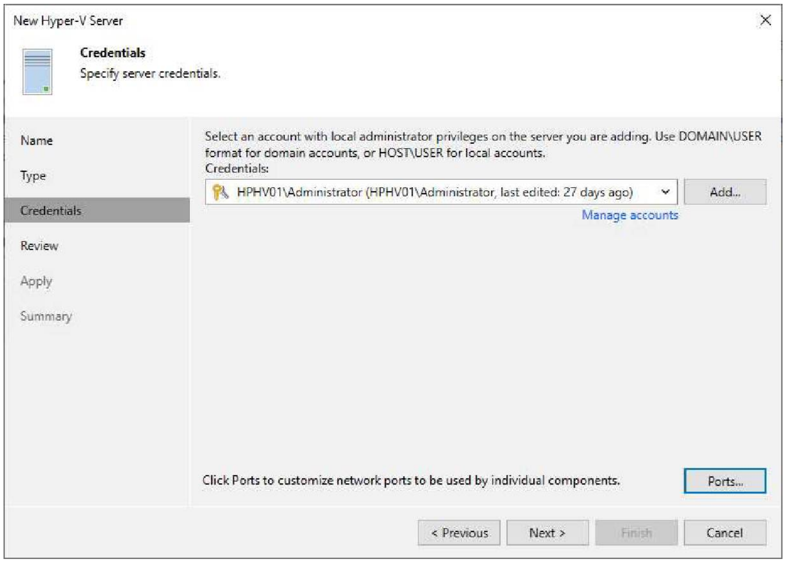
Data transfer options

Port range: 2500 to 3300

Preferred TCP connection role

□ Run server on this side

18. Click Next on the Credentials page.



Credentials

Specify server credentials.

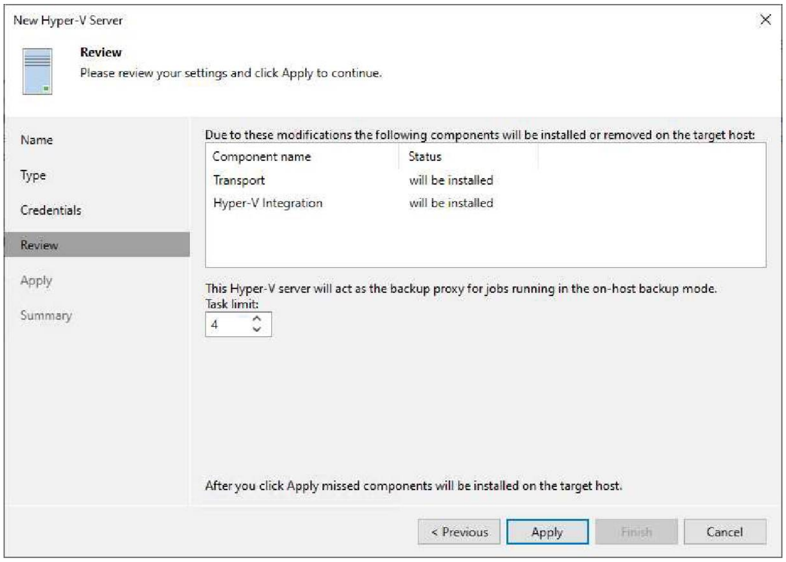
Select an account with local administrator privileges on the server you are adding. Use DOMAIN\USER format for domain accounts, or HOST\USER for local accounts.

Credentials:

HPHV01\Administrator (HPHV01\Administrator, last edited: 27 days ago)

Click Ports to customize network ports to be used by individual components.

19. If you add a standalone Microsoft Hyper-V host on the Review page, specify the number of tasks the Microsoft Hyper-V host must handle concurrently in the Max concurrent tasks field.
20. Click Apply.



Review

Please review your settings and click Apply to continue.

Due to these modifications the following components will be installed or removed on the target host:

Component name	Status
Transport	will be installed
Hyper-V Integration	will be installed

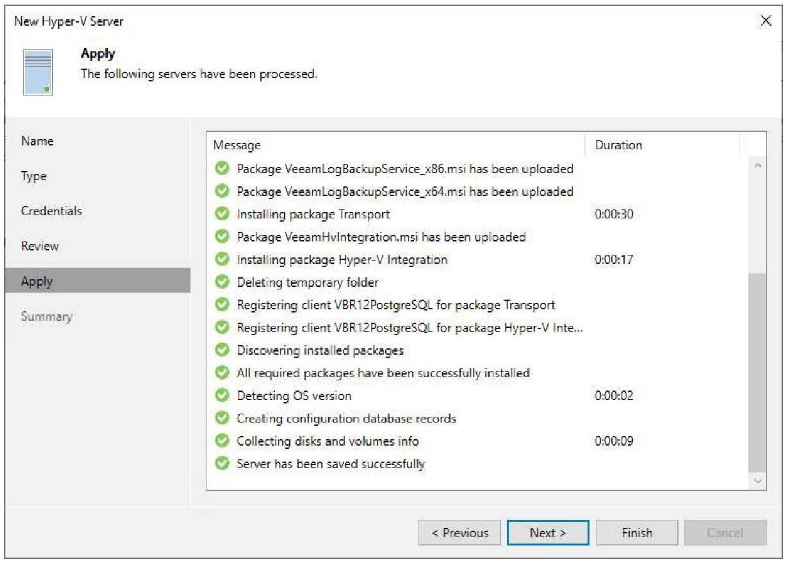
This Hyper-V server will act as the backup proxy for jobs running in the on-host backup mode.

Task limit:

4

After you click Apply missed components will be installed on the target host.

21. Click Next on the Apply page.

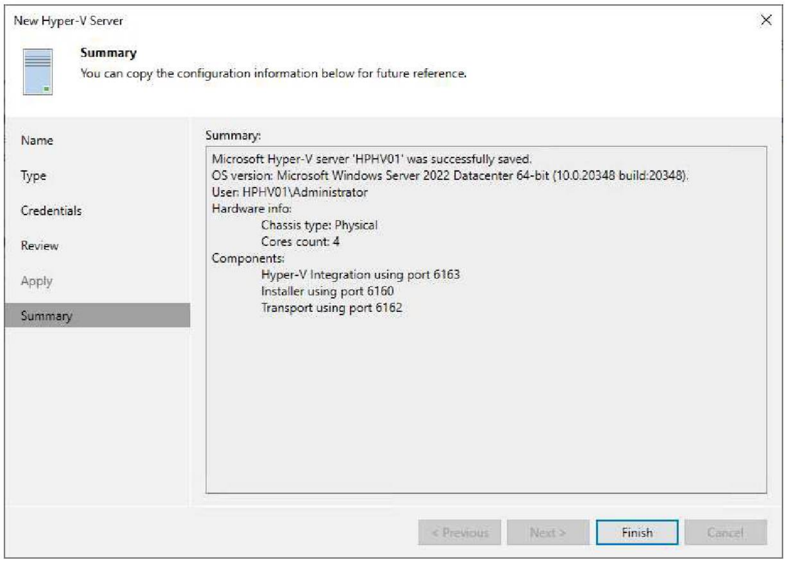


Apply

The following servers have been processed.

Message	Duration
Package VeeamLogBackupService_x86.msi has been uploaded	
Package VeeamLogBackupService_x64.msi has been uploaded	
Installing package Transport	0:00:30
Package VeeamHvIntegration.msi has been uploaded	
Installing package Hyper-V Integration	0:00:17
Deleting temporary folder	
Registering client VBR12PostgreSQL for package Transport	
Registering client VBR12PostgreSQL for package Hyper-V Inte...	
Discovering installed packages	
All required packages have been successfully installed	
Detecting OS version	0:00:02
Creating configuration database records	
Collecting disks and volumes info	0:00:09
Server has been saved successfully	

22. Click Finish on the Summary page.



Summary

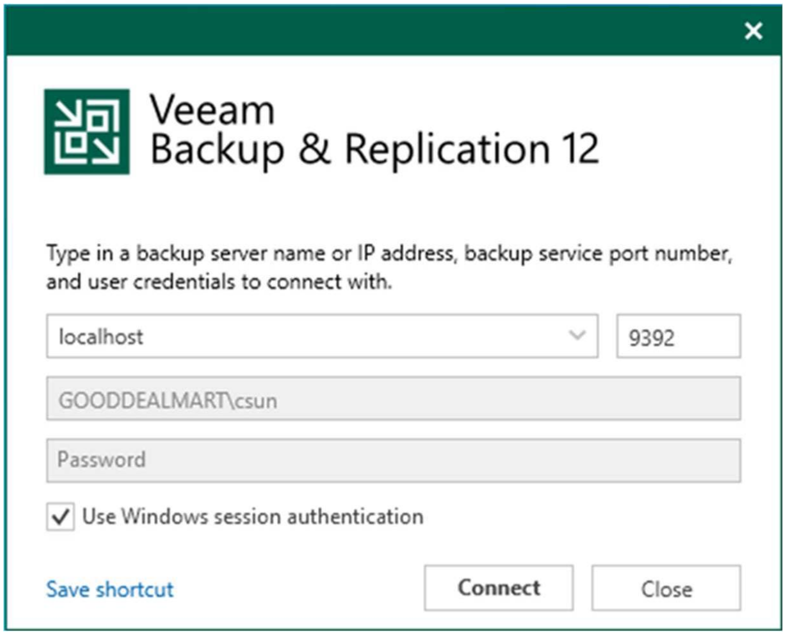
You can copy the configuration information below for future reference.

Summary:

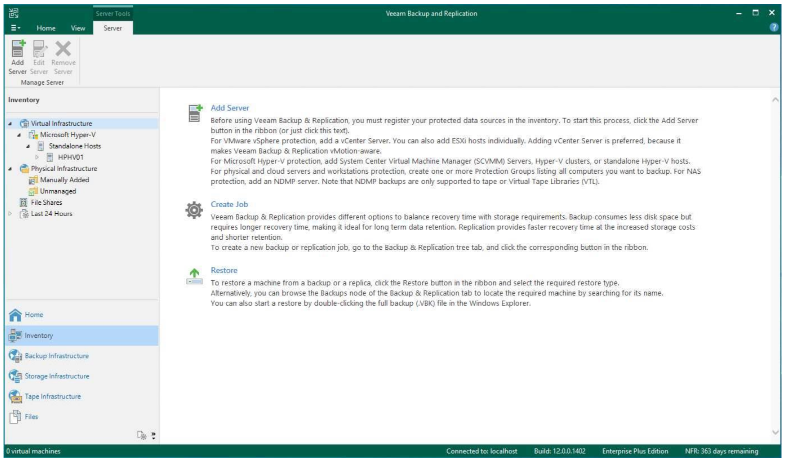
```
Microsoft Hyper-V server 'HPHV01' was successfully saved.
OS version: Microsoft Windows Server 2022 Datacenter 64-bit (10.0.20348 build:20348).
User: HPHV01\Administrator
Hardware info:
          Chassis type: Physical
          Cores count: 4
Components:
          Hyper-V Integration using port 6163
          Installer using port 6160
          Transport using port 6162
```

Add Microsoft Hyper-V Clusters

You must add the Microsoft Hyper-V clusters you plan to use as source and target for backup, replication and other activities.

Instructions	Screenshot (if applicable)
1. Log in to the Veeam Backup and replication manager server. 2. Open the Veeam Backup & Replication Console, and click Connect.	 Veeam Backup & Replication 12 Type in a backup server name or IP address, backup service port number, and user credentials to connect with. localhost 9392 GOODDEALMART\csun Password ☑ Use Windows session authentication

3. On the Home page, select Inventory.
4. On the Inventory page, select Virtual Infrastructure and click Add Server.



Add Server

Before using Veeam Backup & Replication, you must register your protected data sources in the inventory. To start this process, click the Add Server button in the ribbon (or just click this text).
For VMware vSphere protection, add a vCenter Server. You can also add ESXi hosts individually. Adding vCenter Server is preferred, because it makes Veeam Backup & Replication vMotion-aware.
For Microsoft Hyper-V protection, add System Center Virtual Machine Manager (SCVMM) Servers, Hyper-V clusters, or standalone Hyper-V hosts.
For physical and cloud servers and workstations protection, create one or more Protection Groups listing all computers you want to backup. For NAS protection, add an NDMP server. Note that NDMP backups are only supported to tape or Virtual Tape Libraries (VTL).

Create Job

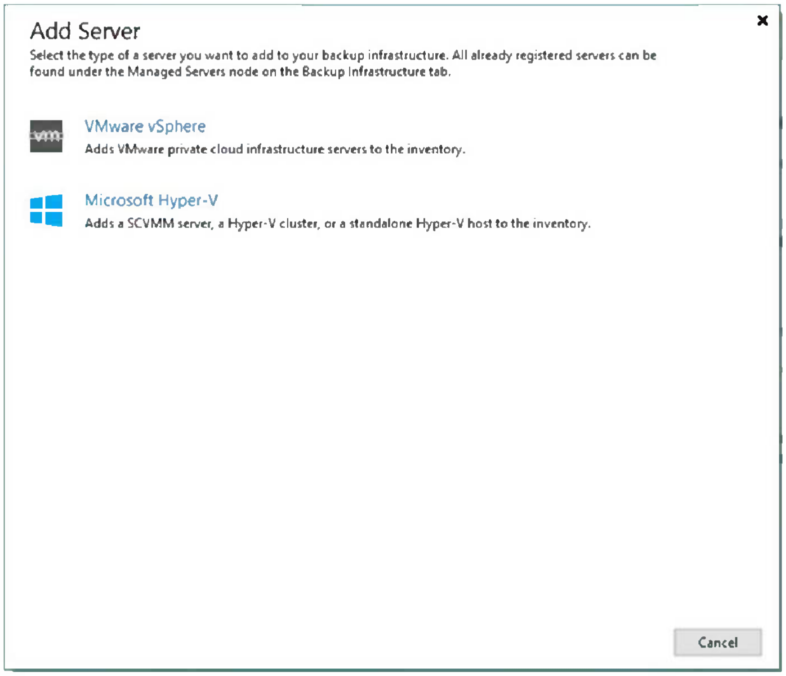
Veeam Backup & Replication provides different options to balance recovery time with storage requirements. Backup consumes less disk space but requires longer recovery time, making it ideal for long term data retention. Replication provides faster recovery time at the increased storage costs and shorter retention.
To create a new backup or replication job, go to the Backup & Replication tree tab, and click the corresponding button in the ribbon.

Restore

To restore a machine from a backup or a replica, click the Restore button in the ribbon and select the required restore type.
Alternatively, you can browse the Backups node of the Backup & Replication tab to locate the required machine by searching for its name.
You can also start a restore by double-clicking the full backup (.VBK) file in the Windows Explorer.

0 virtual machines   Connected to: localhost   Build: 12.0.0.1402   Enterprise Plus Edition   NFR: 363 days remaining

5. On the Add Server page, select Microsoft Hyper-V.



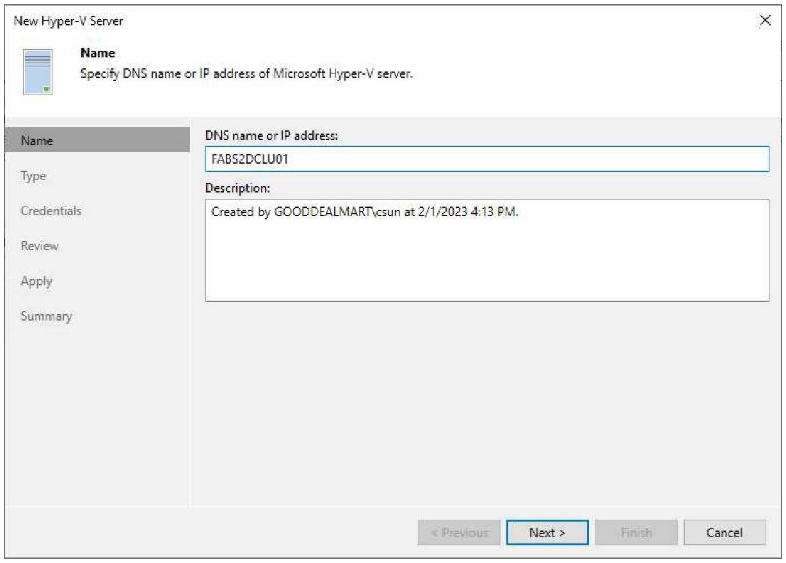
Add Server

Select the type of a server you want to add to your backup infrastructure. All already registered servers can be found under the Managed Servers node on the Backup Infrastructure tab.

VMware vSphere
Adds VMware private cloud infrastructure servers to the inventory.

Microsoft Hyper-V
Adds a SCVMM server, a Hyper-V cluster, or a standalone Hyper-V host to the inventory.

6. Enter the Microsoft Hyper-V Cluster's full DNS name or IP address on the Name page.
7. Give a brief description in the Description field for future reference and click Next.



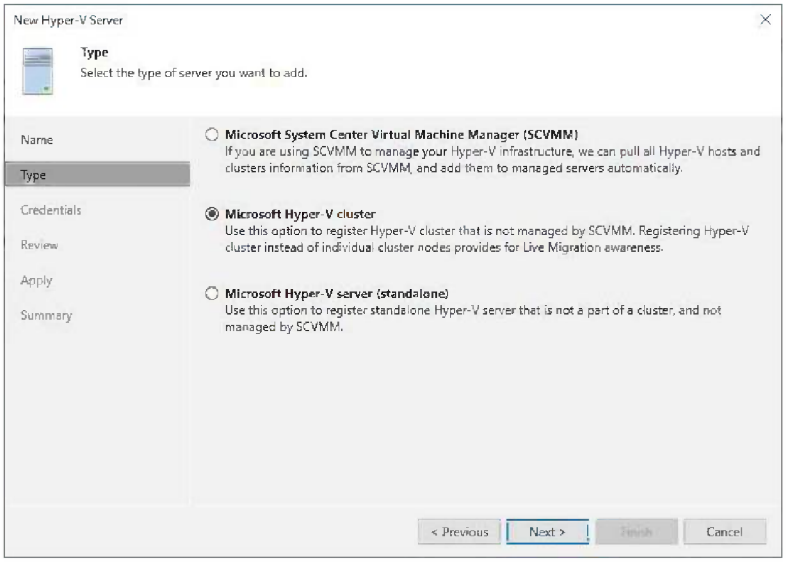
Name

Specify DNS name or IP address of Microsoft Hyper-V server.

DNS name or IP address: FABS2DCLU01

Description: Created by GOODDEALMART\csun at 2/1/2023 4:13 PM.

8. On the Type page, select Microsoft Hyper-V cluster and click Next.



Type

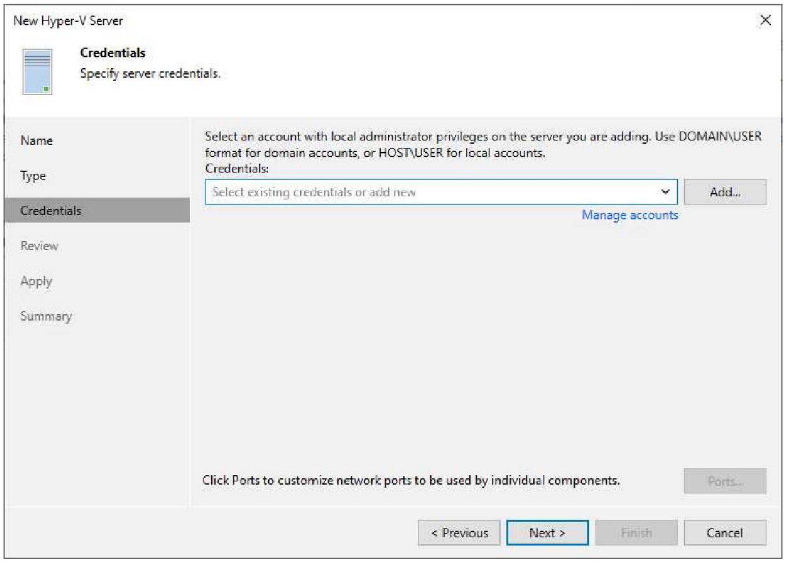
Select the type of server you want to add.

○ **Microsoft System Center Virtual Machine Manager (SCVMM)**
If you are using SCVMM to manage your Hyper-V infrastructure, we can pull all Hyper-V hosts and clusters information from SCVMM, and add them to managed servers automatically.

● **Microsoft Hyper-V cluster**
Use this option to register Hyper-V cluster that is not managed by SCVMM. Registering Hyper-V cluster instead of individual cluster nodes provides for Live Migration awareness.

○ **Microsoft Hyper-V server (standalone)**
Use this option to register standalone Hyper-V server that is not a part of a cluster, and not managed by SCVMM.

9. Select an account from the Credentials drop-down list on the Credentials page or click Add on the right to add the credentials.

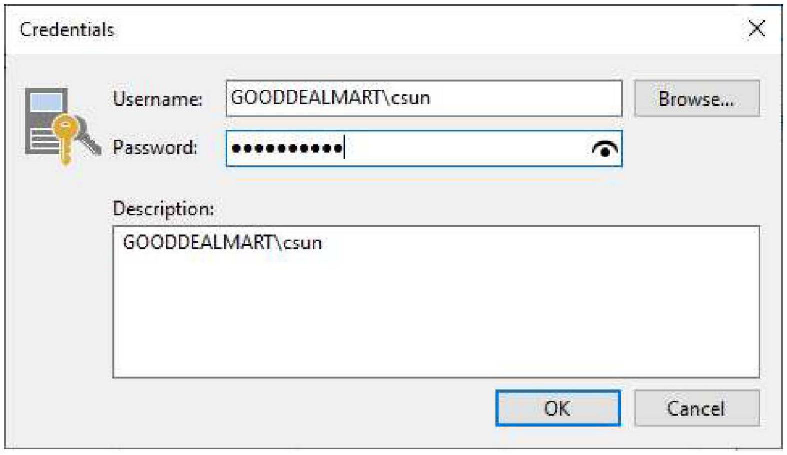


Select an account with local administrator privileges on the server you are adding. Use DOMAIN\USER format for domain accounts, or HOST\USER for local accounts.

Credentials: Select existing credentials or add new

Click Ports to customize network ports to be used by individual components.

10. On the Credentials page, enter a user name in the Username field. You can also click Browse to select an existing user account.
11. Enter the password In the Password field.
12. Give a brief description in the Description field for future reference and click OK.

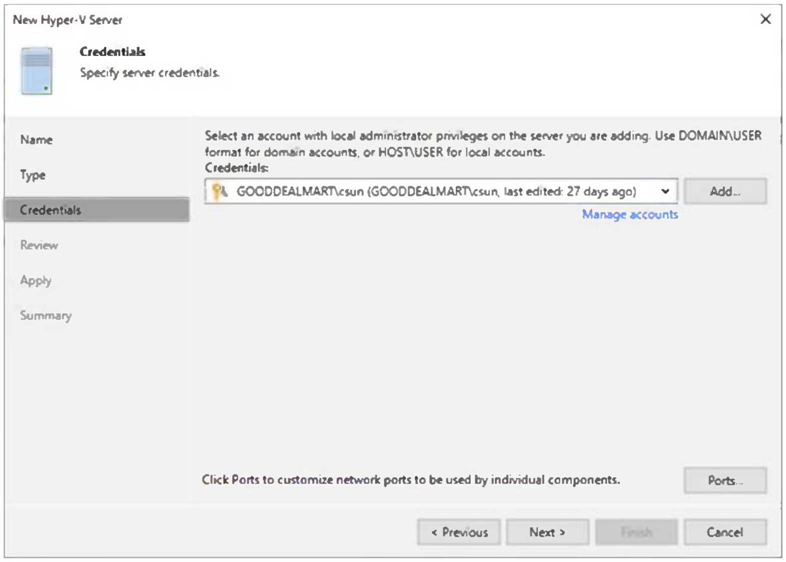


Username: GOODDEALMART\csun

Password: ••••••••••

Description: GOODDEALMART\csun

13. On the Credentials page, click Ports.

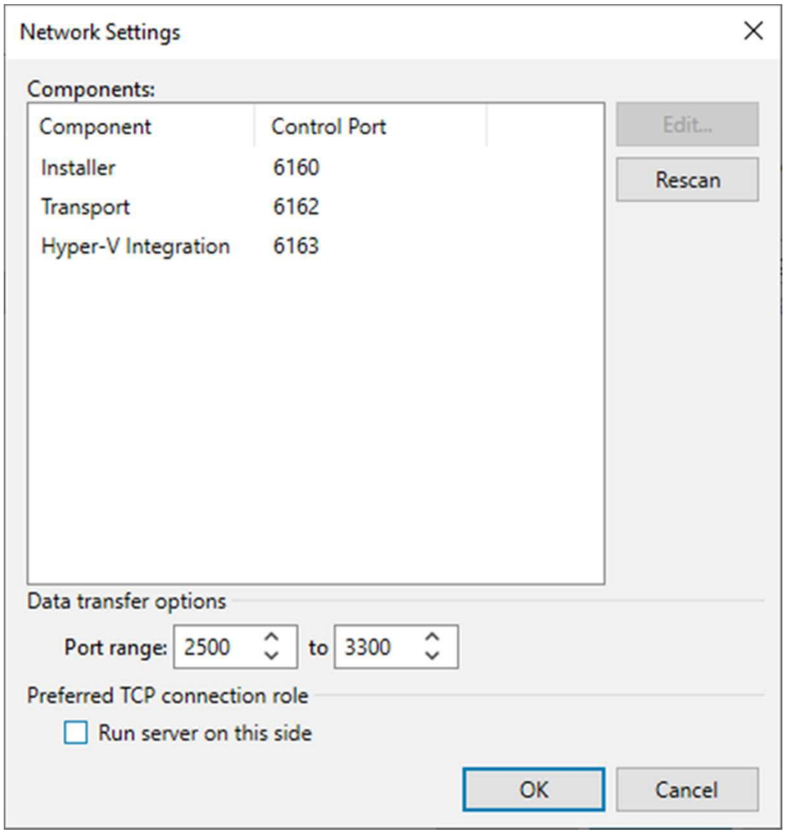


Select an account with local administrator privileges on the server you are adding. Use DOMAIN\USER format for domain accounts, or HOST\USER for local accounts.

Credentials: GOODDEALMART\csun (GOODDEALMART\csun, last edited: 27 days ago)

Click Ports to customize network ports to be used by individual components.

14. If necessary, change the network ports used by Veeam Backup & Replication components on the Network Settings page.
15. Configure connection settings for file copy operations in the Network Settings window's Data transfer options section. Provide a set of ports for transmission channels between the source and target hosts (one port per task).
16. Select the Run server on this side checkbox in the Preferred TCP connection role section. The outside client cannot connect to the server on the NAT network in the NAT scenario. As a result, services that require external connection initiation may be disrupted.
17. Click OK.



Components:

Component	Control Port
Installer	6160
Transport	6162
Hyper-V Integration	6163

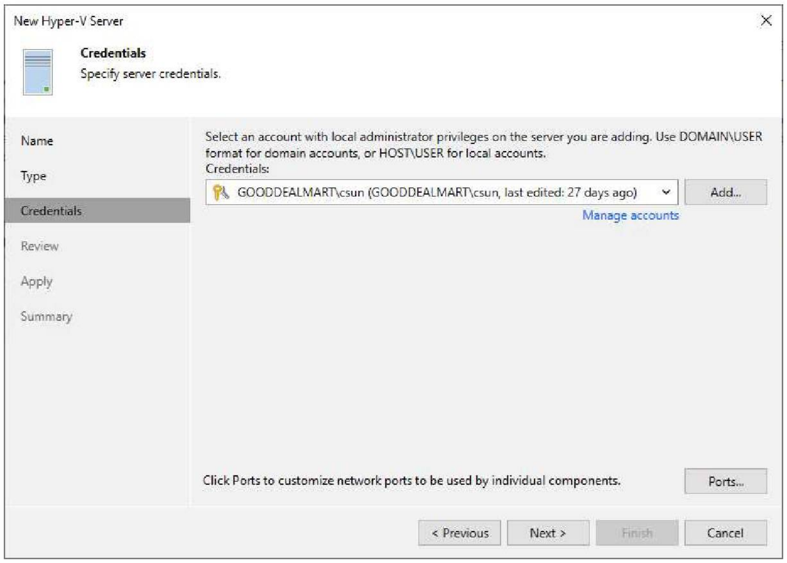
Data transfer options

Port range: 2500 to 3300

Preferred TCP connection role

□ Run server on this side

18. On the Credentials page, click Next.



Credentials

Specify server credentials.

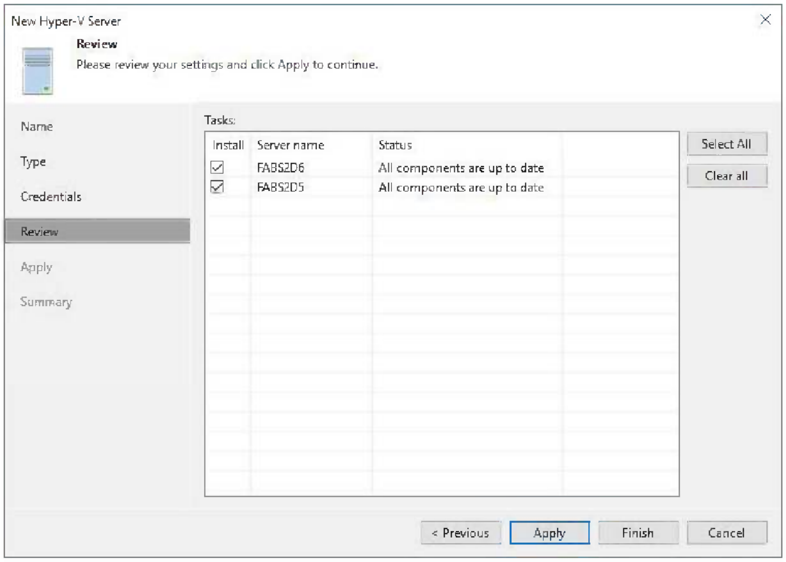
Select an account with local administrator privileges on the server you are adding. Use DOMAIN\USER format for domain accounts, or HOST\USER for local accounts.

Credentials:

GOODDEALMART\csun (GOODDEALMART\csun, last edited: 27 days ago)

Click Ports to customize network ports to be used by individual components.

19. Select all servers' checkboxes on the Review page and click Apply.



Review

Please review your settings and click Apply to continue.

Tasks:

Install	Server name	Status
☑	FABS2D6	All components are up to date
☑	FABS2D5	All components are up to date

20. Click Next on the Apply page.

21. Click Finish on the Summary page.

Add Microsoft SMB3 Servers

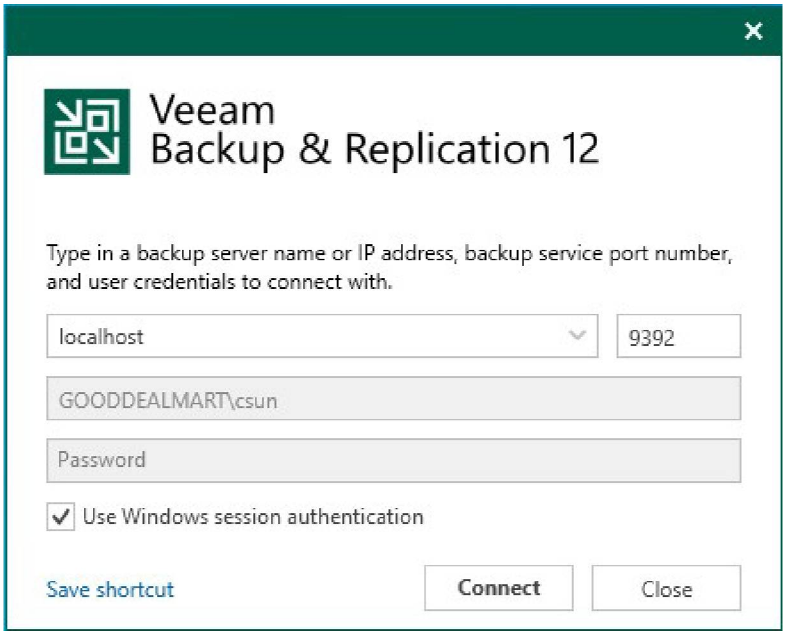
Veeam Backup & Replication can perform backup, replication, and file copy operations on Microsoft Hyper-V VMs whose discs are located on Microsoft SMB3 file shares.

If a Microsoft SMB3 server or cluster is not added to the backup infrastructure, Veeam Backup & Replication cannot process such VMs using the changed block tracking mechanism.

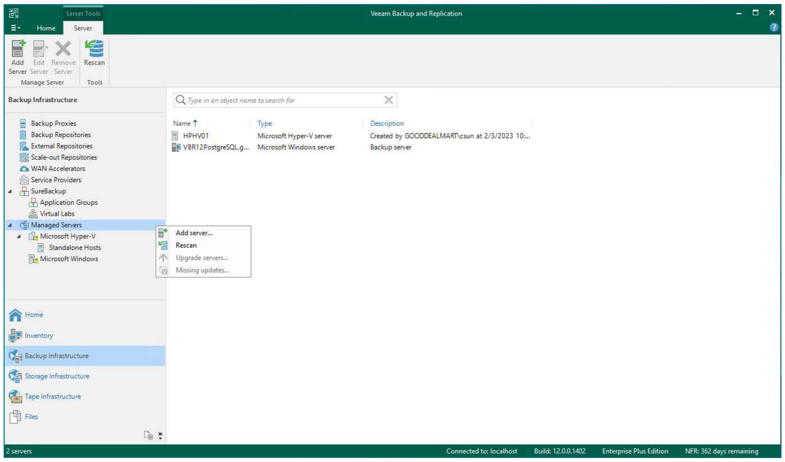
If VMs with discs on SMB3 shared folders are registered on Microsoft Hyper-V Server 2016 or later, a Microsoft SMB3 server is not required. However, if the Microsoft SMB3 server is not added, you cannot specify the Max snapshots, and latency control settings for SMB3 shared folders.

Note:

You cannot use Microsoft SMB3 shared folder as storage for VM replicas.

Instructions	Screenshot (if applicable)
1. Log in to the Veeam Backup and replication manager server. 2. Open the Veeam Backup & Replication Console, and click Connect.	 Veeam Backup & Replication 12 Type in a backup server name or IP address, backup service port number, and user credentials to connect with. localhost 9392 GOODDEALMART\csun Password ☑ Use Windows session authentication Save shortcut Connect Close

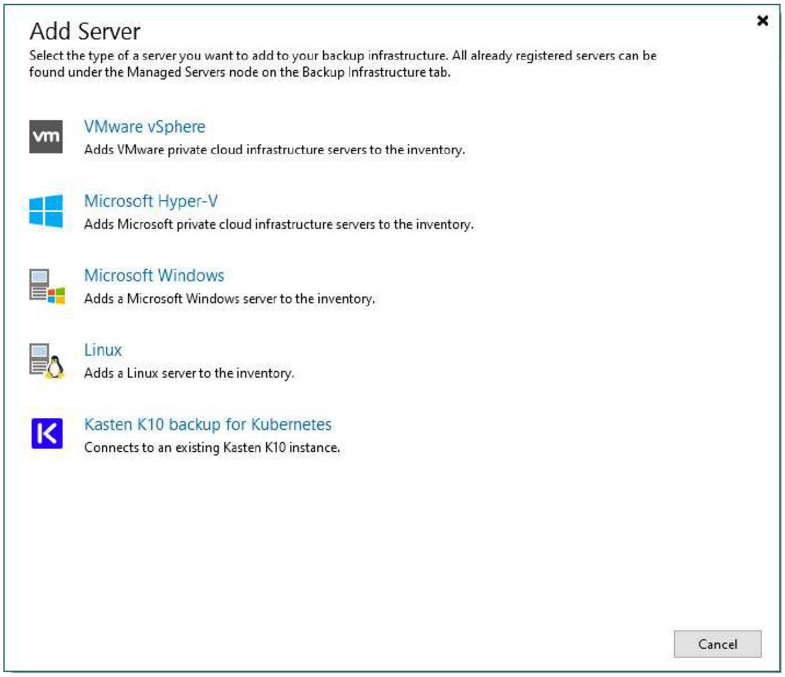
3. On the Home page, select Backup Infrastructure.
4. On the Backup Infrastructure page, select Managed Servers.
5. Right-click Managed Servers and select Add Server.



Name ↑	Type	Description
HPHV01	Microsoft Hyper-V server	Created by GOODDEALMART\csun at 2/3/2023 10:...
VBR12PostgreSQL.g...	Microsoft Windows server	Backup server

2 servers Connected to: localhost Build: 12.0.0.1402 Enterprise Plus Edition NFR: 362 days remaining

6. Select Microsoft Hyper-V on the Add Server Page.



Add Server

Select the type of a server you want to add to your backup infrastructure. All already registered servers can be found under the Managed Servers node on the Backup Infrastructure tab.

VMware vSphere
Adds VMware private cloud infrastructure servers to the inventory.

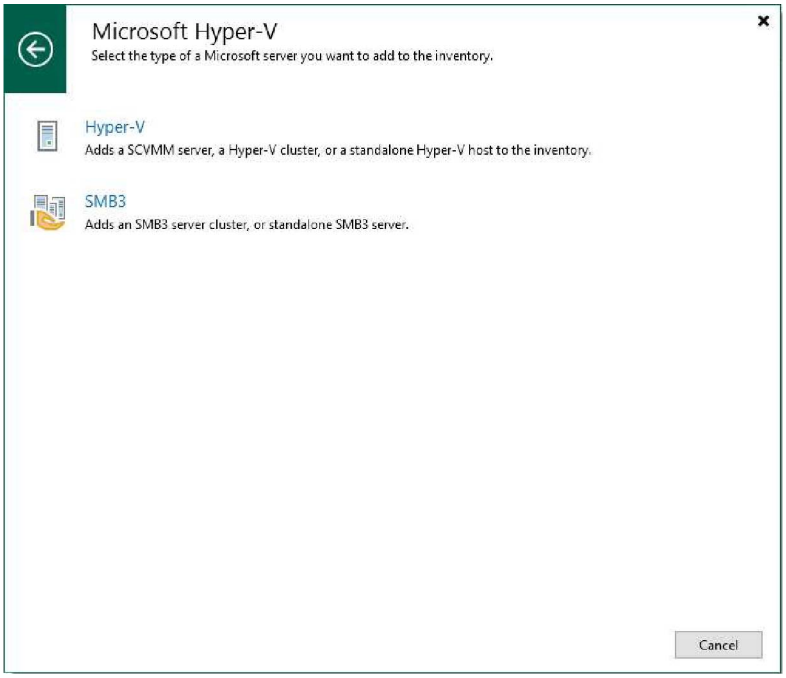
Microsoft Hyper-V
Adds Microsoft private cloud infrastructure servers to the inventory.

Microsoft Windows
Adds a Microsoft Windows server to the inventory.

Linux
Adds a Linux server to the inventory.

Kasten K10 backup for Kubernetes
Connects to an existing Kasten K10 instance.

7. Select SMB3 on the Microsoft Hyper-V page.



Microsoft Hyper-V

Select the type of a Microsoft server you want to add to the inventory.

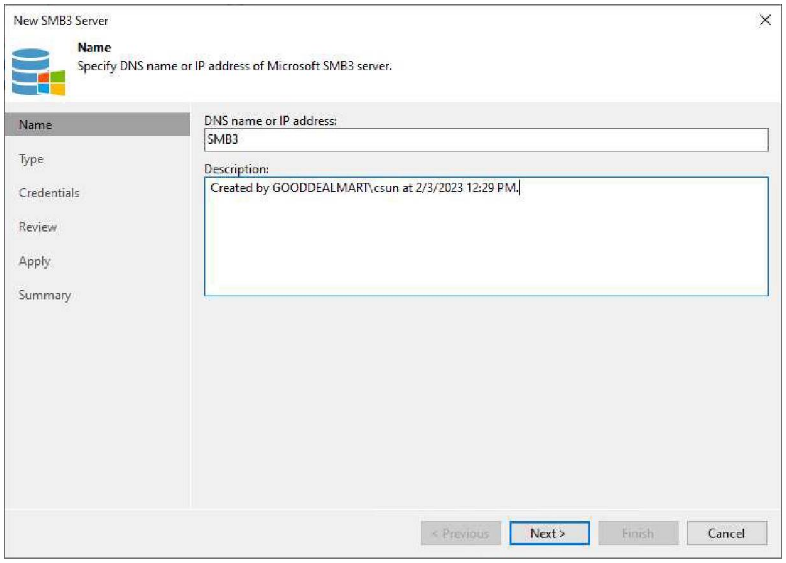
Hyper-V

Adds a SCVMM server, a Hyper-V cluster, or a standalone Hyper-V host to the inventory.

SMB3

Adds an SMB3 server cluster, or standalone SMB3 server.

8. Enter the Microsoft SMB3 server's full DNS name or IP address on the Name page.
9. Give a brief description in the Description field for future reference and click Next.



New SMB3 Server

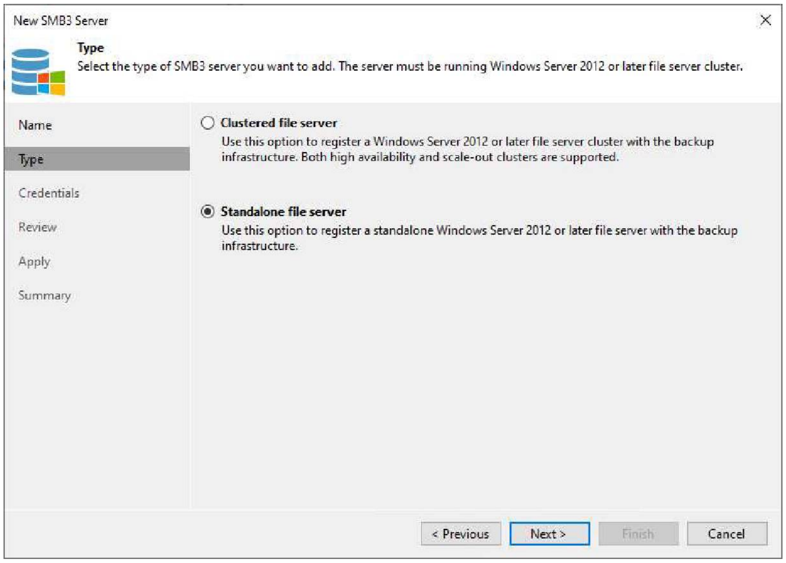
Name

Specify DNS name or IP address of Microsoft SMB3 server.

DNS name or IP address: SMB3

Description: Created by GOODDEALMART\csun at 2/3/2023 12:29 PM.

10. On the Type page, Choose the type of Microsoft SMB3 server you want to add and click Next.



Type

Select the type of SMB3 server you want to add. The server must be running Windows Server 2012 or later file server cluster.

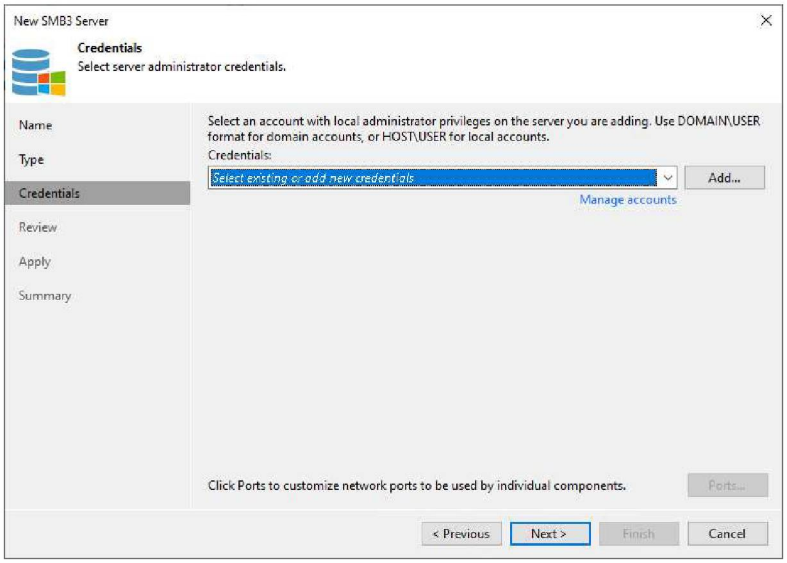
○ **Clustered file server**

Use this option to register a Windows Server 2012 or later file server cluster with the backup infrastructure. Both high availability and scale-out clusters are supported.

● **Standalone file server**

Use this option to register a standalone Windows Server 2012 or later file server with the backup infrastructure.

11. Select an account from the Credentials drop-down list on the Credentials page or click Add on the right to add the credentials.



Credentials

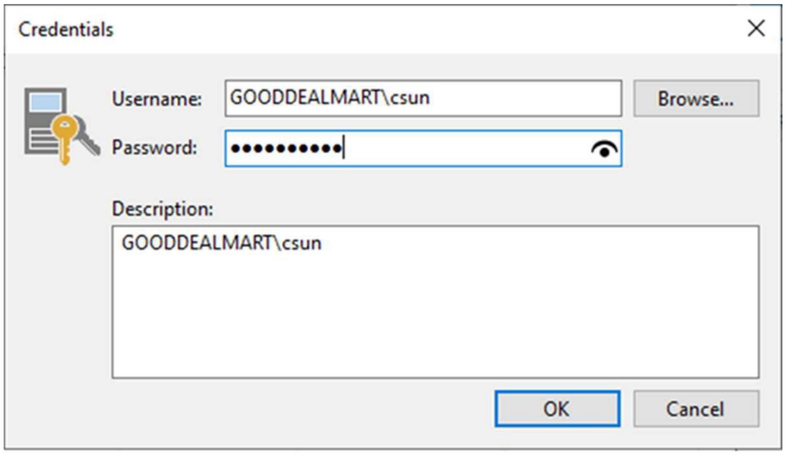
Select server administrator credentials.

Select an account with local administrator privileges on the server you are adding. Use DOMAIN\USER format for domain accounts, or HOST\USER for local accounts.

Credentials: Select existing or add new credentials

Click Ports to customize network ports to be used by individual components.

12. On the Credentials page, enter a user name in the Username field. You can also click Browse to select an existing user account.
13. Enter the password In the Password field.
14. Give a brief description in the Description field for future reference and click OK.



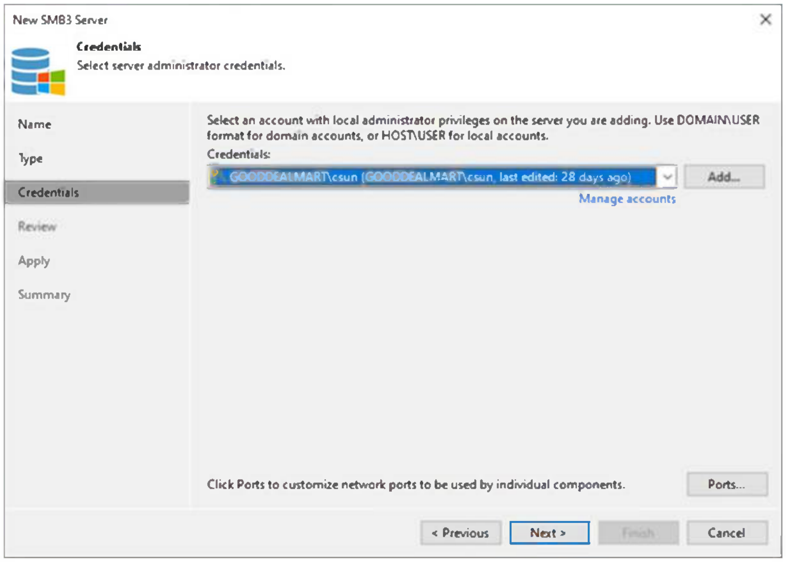
Credentials

Username: GOODDEALMART\csun

Password: ●●●●●●●●●●

Description: GOODDEALMART\csun

15. On the Credentials page, click Ports.



New SMB3 Server

Credentials

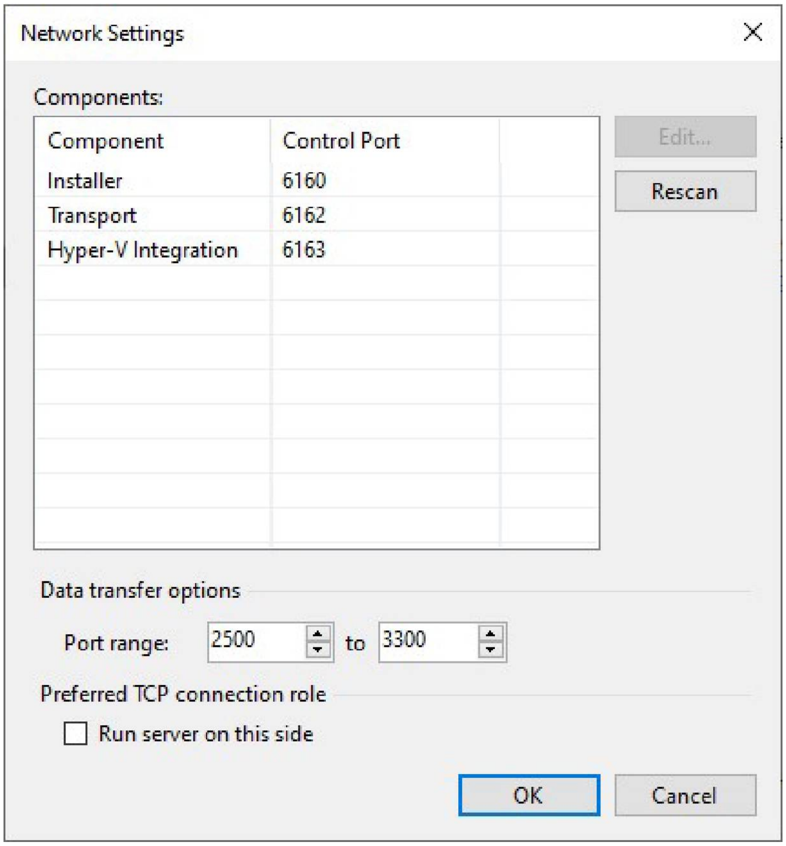
Select server administrator credentials.

Select an account with local administrator privileges on the server you are adding. Use DOMAIN\USER format for domain accounts, or HOST\USER for local accounts.

Credentials: GOODDEALMART\csun (GOODDEALMART\csun, last edited: 28 days ago)

Click Ports to customize network ports to be used by individual components.

16. If necessary, change the network ports used by Veeam Backup & Replication components on the Network Settings page.
17. Configure connection settings for file copy operations in the Network Settings window's Data transfer options section. Provide a set of ports for transmission channels between the source and target hosts (one port per task).
18. Select the Run server on this side checkbox in the Preferred TCP connection role section. The outside client cannot connect to the server on the NAT network in the NAT scenario. As a result, services that require external connection initiation may be disrupted.
19. Click OK.



Component	Control Port
Installer	6160
Transport	6162
Hyper-V Integration	6163

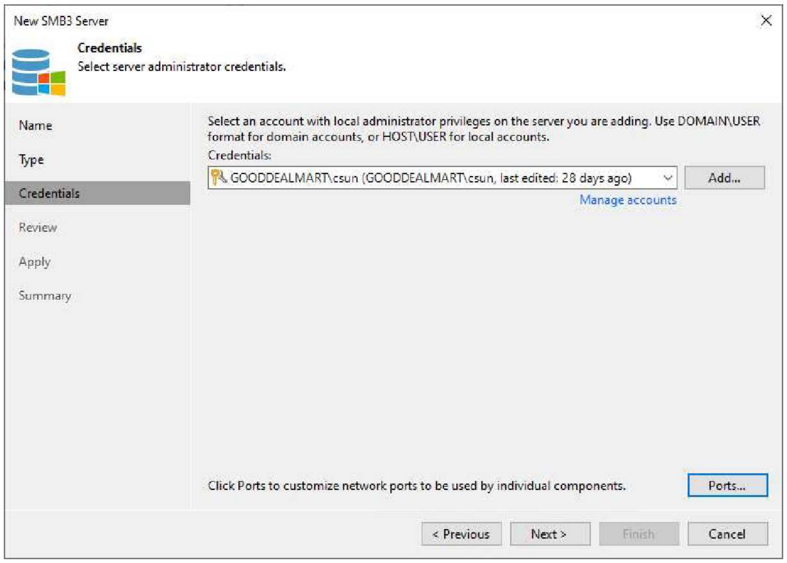
Data transfer options

Port range: 2500 to 3300

Preferred TCP connection role

□ Run server on this side

20. Click Next on the Credentials page.



Credentials

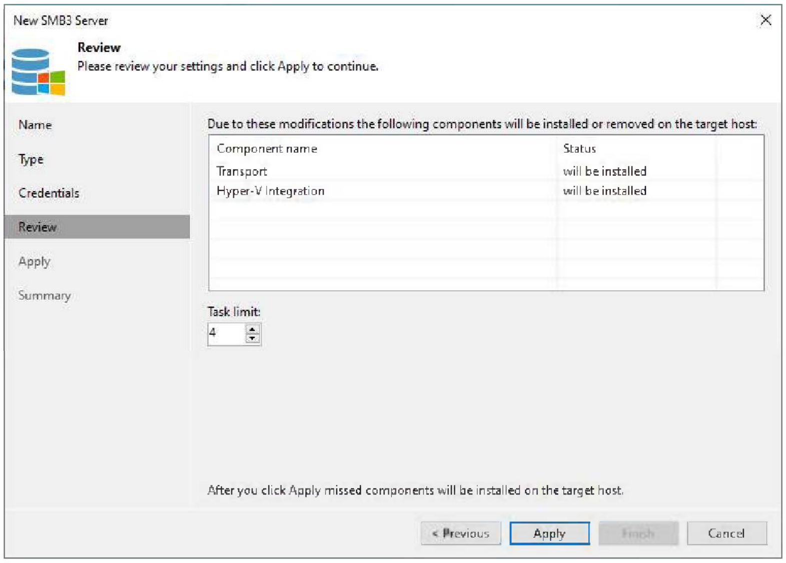
Select server administrator credentials.

Select an account with local administrator privileges on the server you are adding. Use DOMAIN\USER format for domain accounts, or HOST\USER for local accounts.

Credentials: GOODDEALMART\csun (GOODDEALMART\csun, last edited: 28 days ago)

Click Ports to customize network ports to be used by individual components.

21. If you add a standalone Microsoft Hyper-V host on the Review page, specify the number of tasks the Microsoft Hyper-V host must handle concurrently in the Task limit field.
22. Click Apply.



Review

Please review your settings and click Apply to continue.

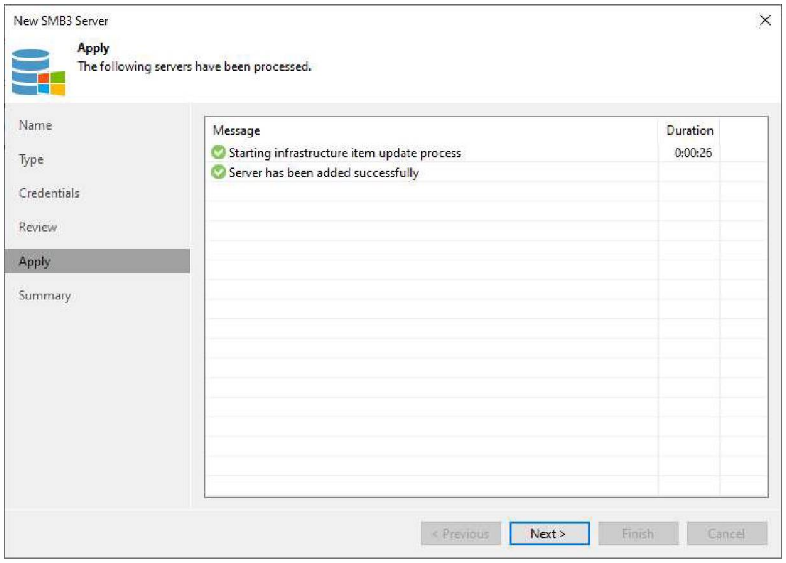
Due to these modifications the following components will be installed or removed on the target host:

Component name	Status
Transport	will be installed
Hyper-V Integration	will be installed

Task limit: 4

After you click Apply missed components will be installed on the target host.

23. Click Next on the Apply page.

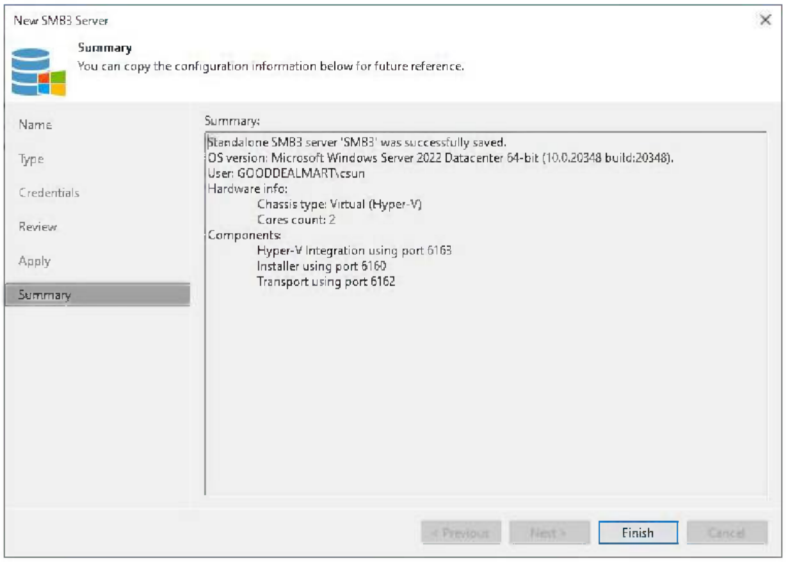


Apply

The following servers have been processed.

Message	Duration
✓ Starting infrastructure item update process	0:00:26
✓ Server has been added successfully	

Click Finish on the Summary page.



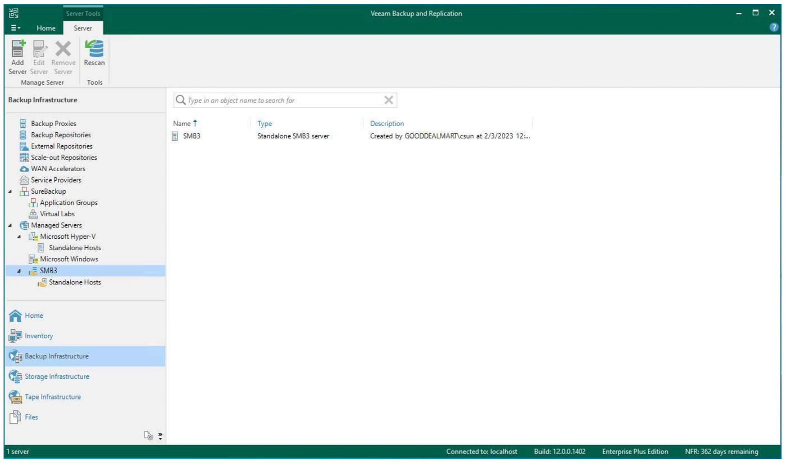
Summary

You can copy the configuration information below for future reference.

Summary:

```
Standalone SMB3 server 'SMB3' was successfully saved.
OS version: Microsoft Windows Server 2022 Datacenter 64-bit (10.0.20348 build:20348).
User: GOODDEALMART\csun
Hardware info:
        Chassis type: Virtual (Hyper-V)
        Cores count: 2
Components:
        Hyper-V Integration using port 6163
        Installer using port 6160
        Transport using port 6162
```

24. Ensure the new Microsoft SMB3 server is added.

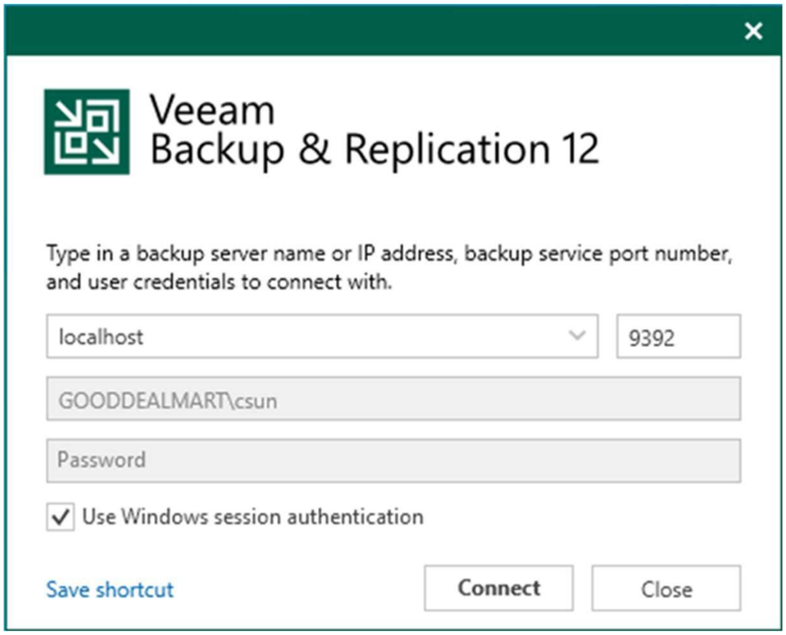


Name	Type	Description
SMB3	Standalone SMB3 server	Created by GOODDEALMART\csun at 2/3/2023 12:...

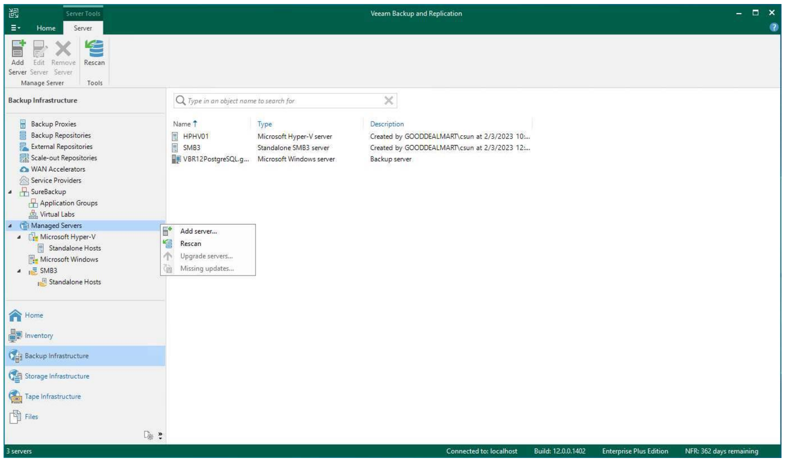
1 server Connected to: localhost Build: 12.0.0.1402 Enterprise Plus Edition NFR: 362 days remaining

Add Microsoft Windows Servers

Suppose you plan to use as backup infrastructure components and servers that you plan to use for various types of restore operations. In that case, you must add the Microsoft Windows servers to the backup infrastructure.

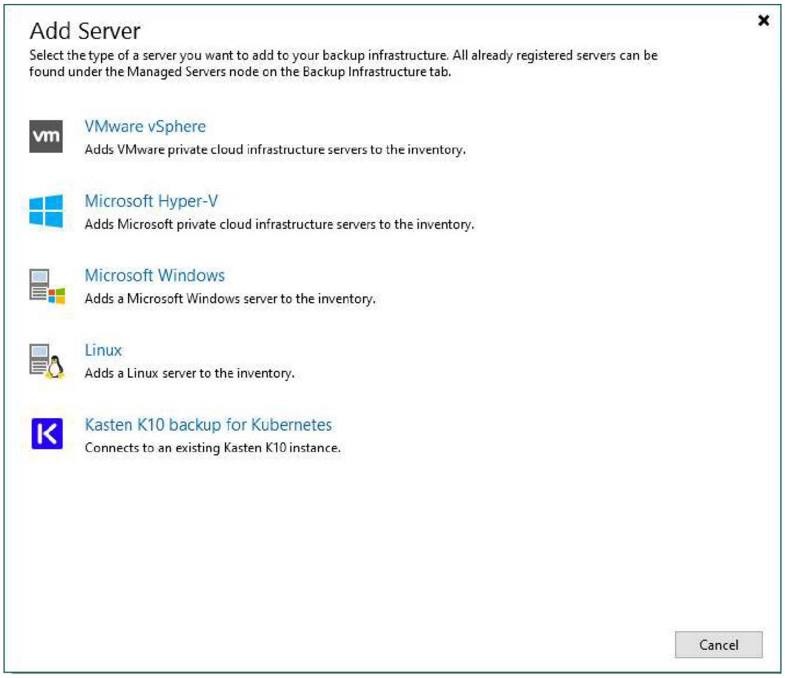
Instructions	Screenshot (if applicable)
1. Log in to the Veeam Backup and replication manager server. 2. Open the Veeam Backup & Replication Console, and click Connect.	 Veeam Backup & Replication 12 Type in a backup server name or IP address, backup service port number, and user credentials to connect with. localhost 9392 GOODDEALMART\csun Password ☑ Use Windows session authentication Save shortcut Connect Close

3. On the Home page, select Backup Infrastructure.
4. On the Backup Infrastructure page, select Managed Servers.
5. Right-click Managed Servers and select Add Server.



Name ↑	Type	Description
HPHV01	Microsoft Hyper-V server	Created by GOODDEALMART\csun at 2/3/2023 10:...
SMB3	Standalone SMB3 server	Created by GOODDEALMART\csun at 2/3/2023 12:...
VBR12PostgreSQL.g...	Microsoft Windows server	Backup server

6. On the Add Server page, select Microsoft Windows.



Add Server

Select the type of a server you want to add to your backup infrastructure. All already registered servers can be found under the Managed Servers node on the Backup Infrastructure tab.

VMware vSphere
Adds VMware private cloud infrastructure servers to the inventory.

Microsoft Hyper-V
Adds Microsoft private cloud infrastructure servers to the inventory.

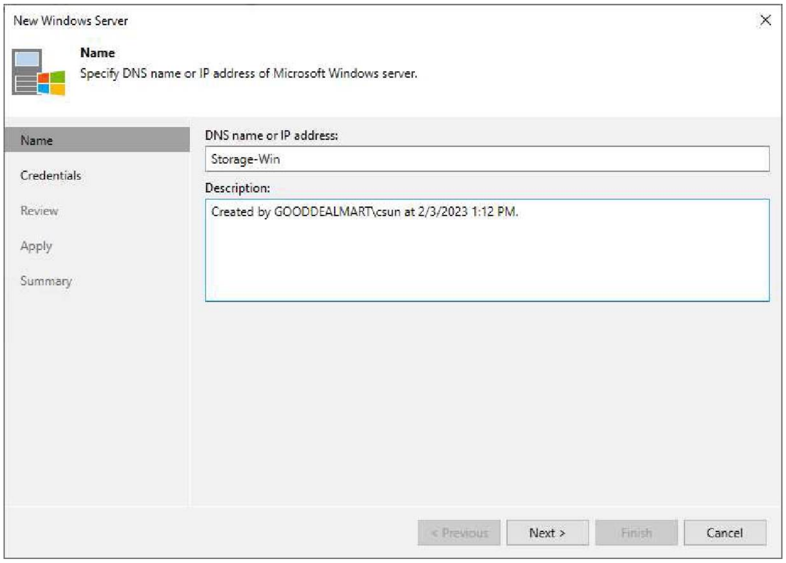
Microsoft Windows
Adds a Microsoft Windows server to the inventory.

Linux
Adds a Linux server to the inventory.

Kasten K10 backup for Kubernetes
Connects to an existing Kasten K10 instance.

7. Enter the Microsoft Windows server's full DNS name or IP address on the Name page.

8. Give a brief description in the Description field for future reference and click Next.



New Windows Server

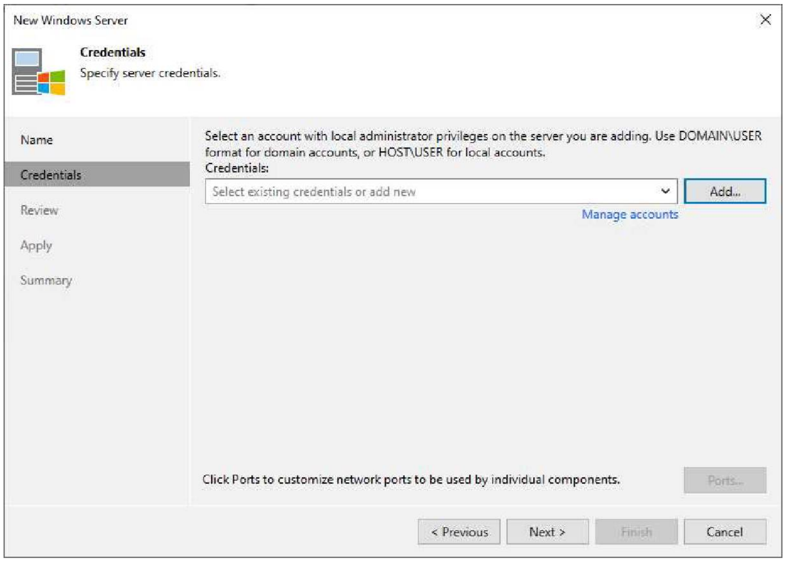
Name

Specify DNS name or IP address of Microsoft Windows server.

DNS name or IP address: Storage-Win

Description: Created by GOODDEALMART\csun at 2/3/2023 1:12 PM.

9. Select an account from the Credentials drop-down list on the Credentials page or click Add on the right to add the credentials.



New Windows Server

Credentials

Specify server credentials.

Select an account with local administrator privileges on the server you are adding. Use DOMAIN\USER format for domain accounts, or HOST\USER for local accounts.

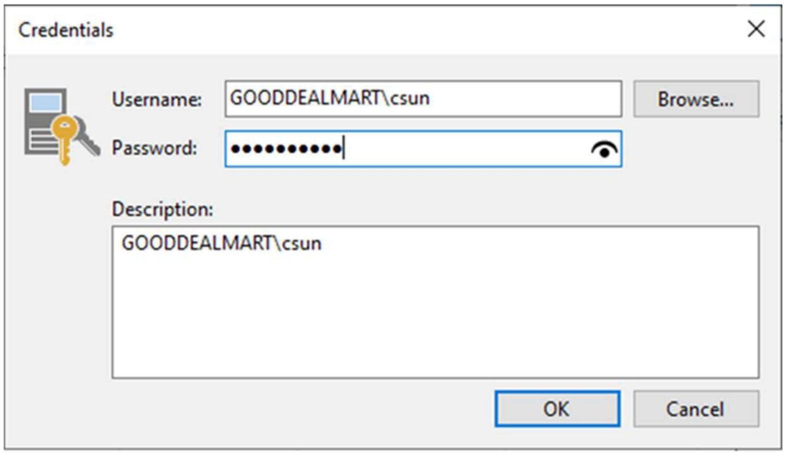
Credentials: Select existing credentials or add new

Click Ports to customize network ports to be used by individual components.

10. On the Credentials page, enter a user name in the Username field. You also can click Browse to select an existing user account.

11. Enter the password In the Password field.

12. Give a brief description in the Description field for future reference and click OK.



Credentials

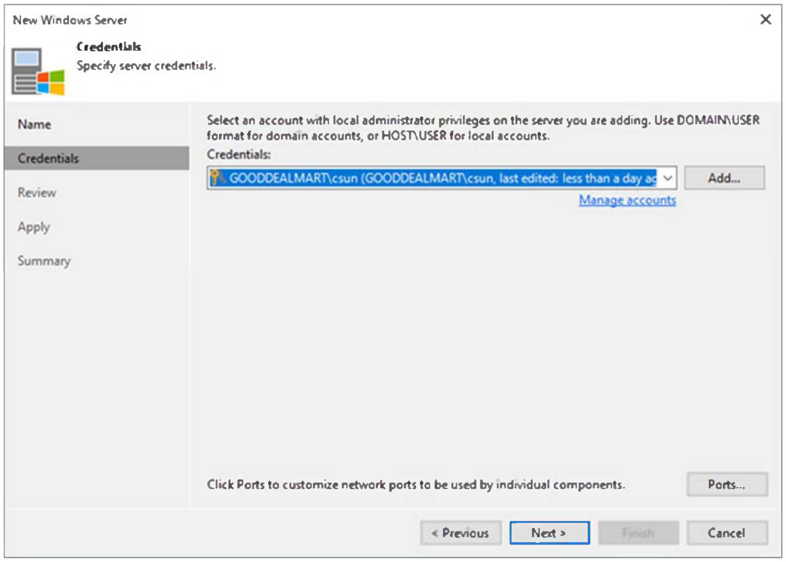
Username: GOODDEALMART\csun

Password: ●●●●●●●●●●

Description:

GOODDEALMART\csun

13. On the Credentials page, click Ports.



New Windows Server

Credentials

Specify server credentials.

Select an account with local administrator privileges on the server you are adding. Use DOMAIN\USER format for domain accounts, or HOST\USER for local accounts.

Credentials: GOODDEALMART\csun (GOODDEALMART\csun, last edited: less than a day ac

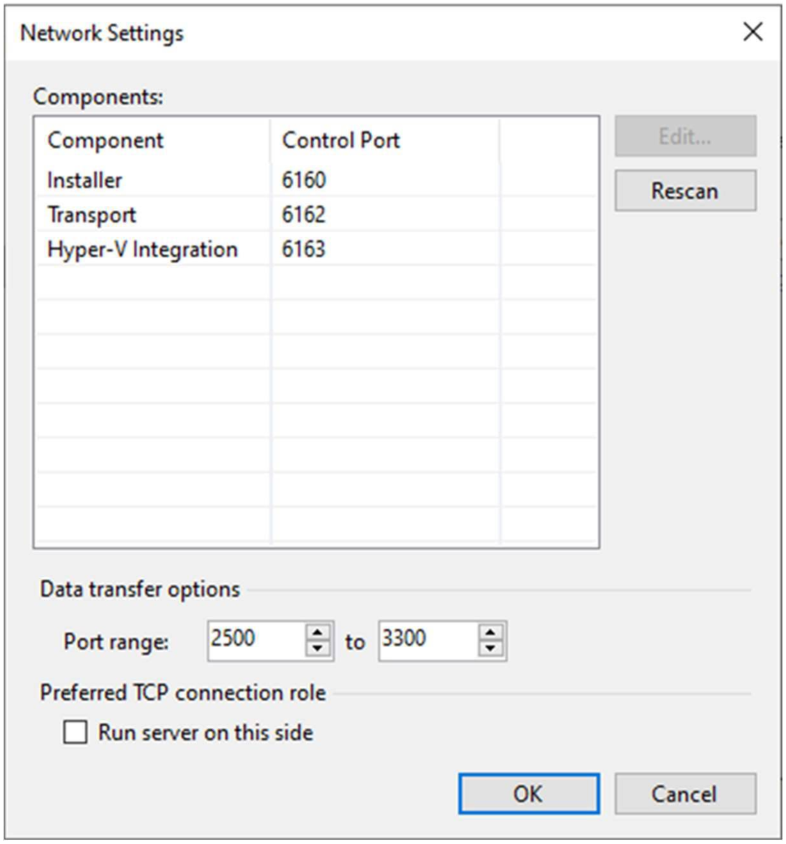
Click Ports to customize network ports to be used by individual components.

14. If necessary, change the network ports used by Veeam Backup & Replication components on the Network Settings page.

15. Configure connection settings for file copy operations in the Network Settings window's Data transfer options section. Provide a set of ports for transmission channels between the source and target hosts (one port per task).

16. Select the Run server on this side checkbox in the Preferred TCP connection role section. The outside client cannot connect to the server on the NAT network in the NAT scenario. As a result, services that require external connection initiation may be disrupted.

17. Click OK.



Components:

Component	Control Port
Installer	6160
Transport	6162
Hyper-V Integration	6163

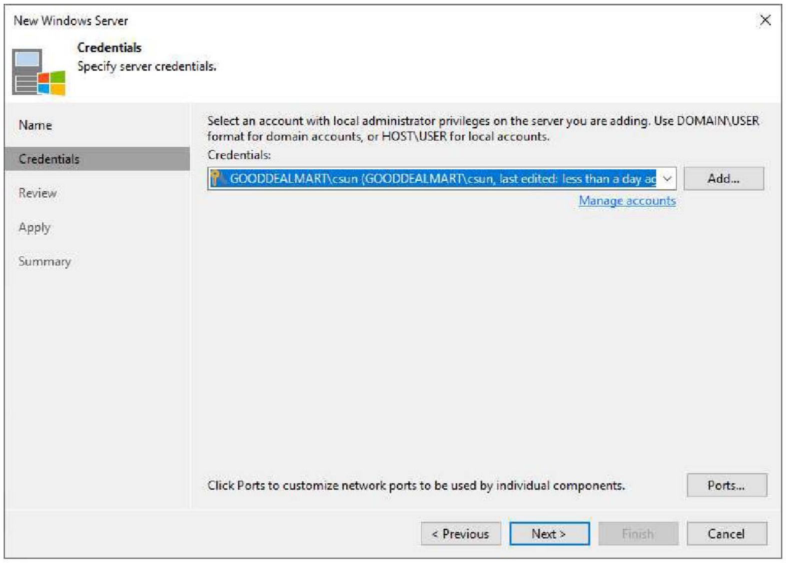
Data transfer options

Port range: 2500 to 3300

Preferred TCP connection role

☐ Run server on this side

18. On the Credentials page, click Next.



New Windows Server

Credentials

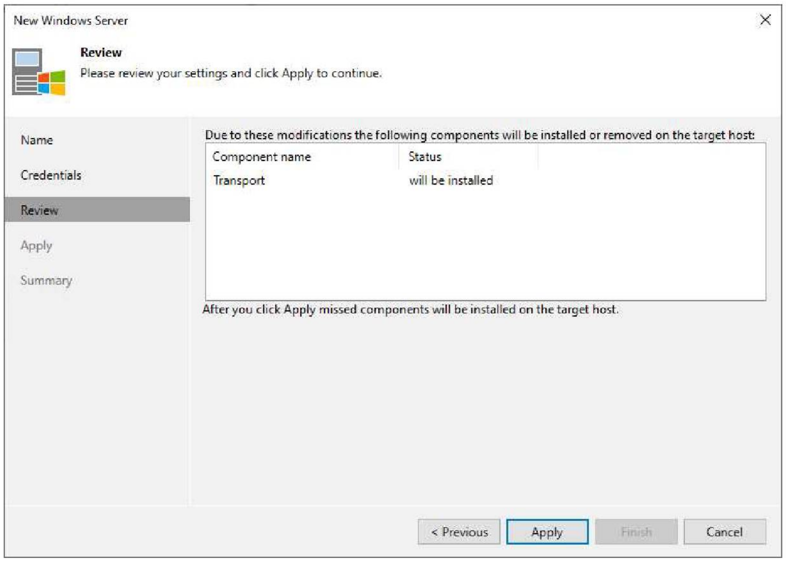
Specify server credentials.

Select an account with local administrator privileges on the server you are adding. Use DOMAIN\USER format for domain accounts, or HOST\USER for local accounts.

Credentials: GOODDEALMART\csun (GOODDEALMART\csun, last edited: less than a day ac

Click Ports to customize network ports to be used by individual components.

19. On the Review page, click Apply.



New Windows Server

Review

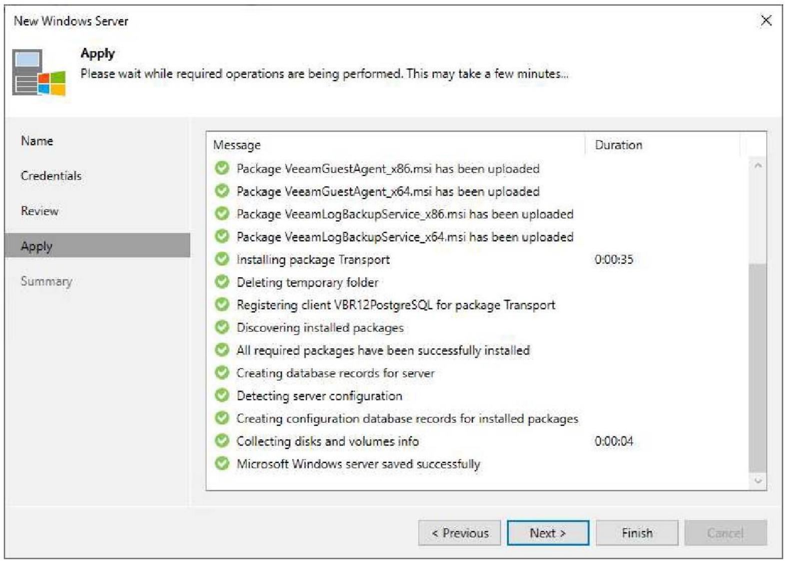
Please review your settings and click Apply to continue.

Due to these modifications the following components will be installed or removed on the target host:

Component name	Status
Transport	will be installed

After you click Apply missed components will be installed on the target host.

20. Click Next on the Apply page.

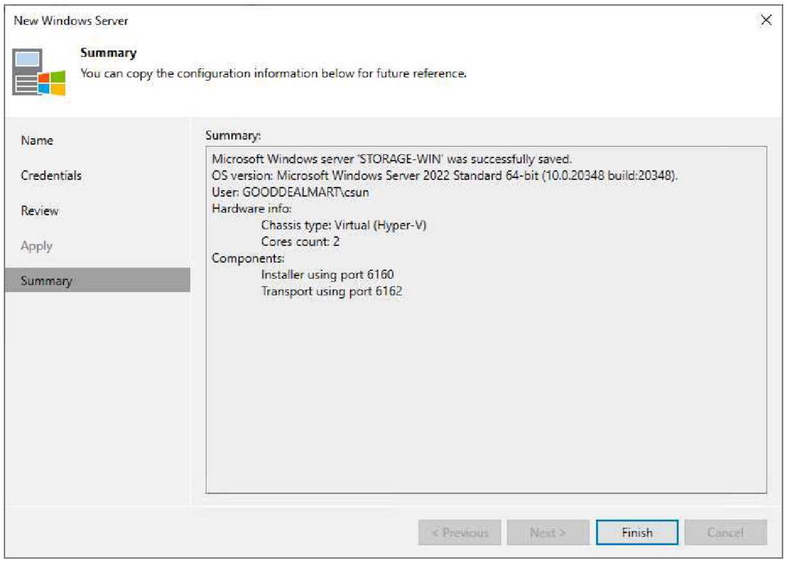


Apply

Please wait while required operations are being performed. This may take a few minutes...

Message	Duration
✓ Package VeeamGuestAgent_x86.msi has been uploaded	
✓ Package VeeamGuestAgent_x64.msi has been uploaded	
✓ Package VeeamLogBackupService_x86.msi has been uploaded	
✓ Package VeeamLogBackupService_x64.msi has been uploaded	
✓ Installing package Transport	0:00:35
✓ Deleting temporary folder	
✓ Registering client VBR12PostgreSQL for package Transport	
✓ Discovering installed packages	
✓ All required packages have been successfully installed	
✓ Creating database records for server	
✓ Detecting server configuration	
✓ Creating configuration database records for installed packages	
✓ Collecting disks and volumes info	0:00:04
✓ Microsoft Windows server saved successfully	

21. Click Finish on the Summary page.



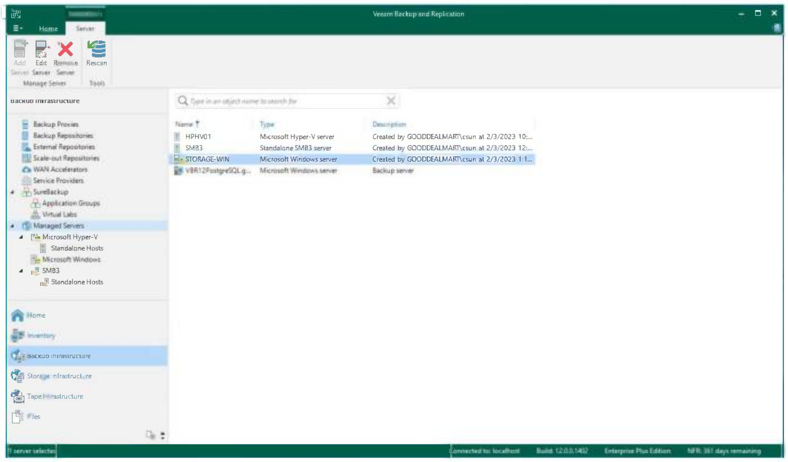
Summary

You can copy the configuration information below for future reference.

Summary:

```
Microsoft Windows server 'STORAGE-WIN' was successfully saved.
OS version: Microsoft Windows Server 2022 Standard 64-bit (10.0.20348 build:20348).
User: GOODDEALMART\csun
Hardware info:
        Chassis type: Virtual (Hyper-V)
        Cores count: 2
Components:
        Installer using port 6160
        Transport using port 6162
```

22. Ensure the new Microsoft Windows server is added.

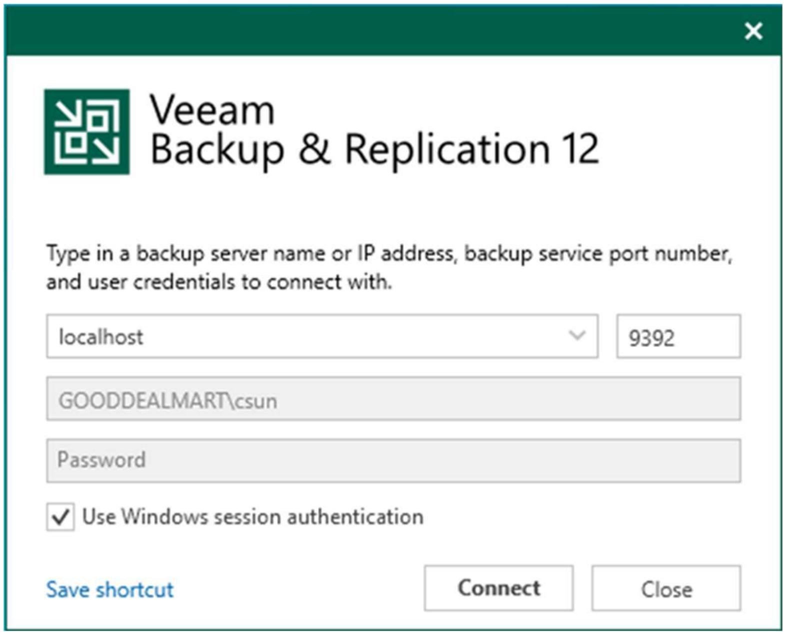


Name	Type	Description
HPHV01	Microsoft Hyper-V server	Created by GOODDEALMART\csun at 2/3/2023 10:...
SMB3	Standalone SMB3 server	Created by GOODDEALMART\csun at 2/3/2023 12:...
STORAGE-WIN	Microsoft Windows server	Created by GOODDEALMART\csun at 2/3/2023 1:1...
VBR12PostgreSQL.g...	Microsoft Windows server	Backup server

1 server selected Connected to: localhost Build: 12.0.0.1402 Enterprise Plus Edition NFR: 361 days remaining

Add Linux Server for a hardened repository

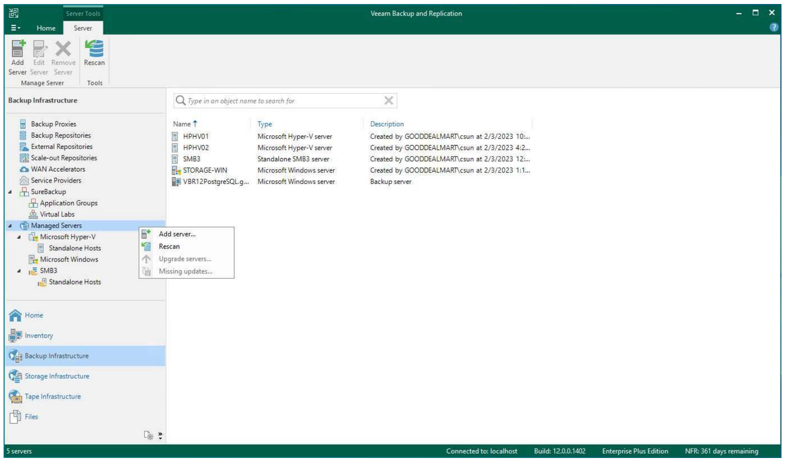
Suppose you plan to use backup infrastructure components and servers that you plan to use for various types of restore operations. In that case, you must add the Linux servers to the backup infrastructure.

Instructions	Screenshot (if applicable)
1. Log in to the Veeam Backup and replication manager server. 2. Open the Veeam Backup & Replication Console, and click Connect.	 Veeam Backup & Replication 12 Type in a backup server name or IP address, backup service port number, and user credentials to connect with. localhost 9392 GOODDEALMART\csun Password ☑ Use Windows session authentication

3. On the Home page, select Backup Infrastructure.

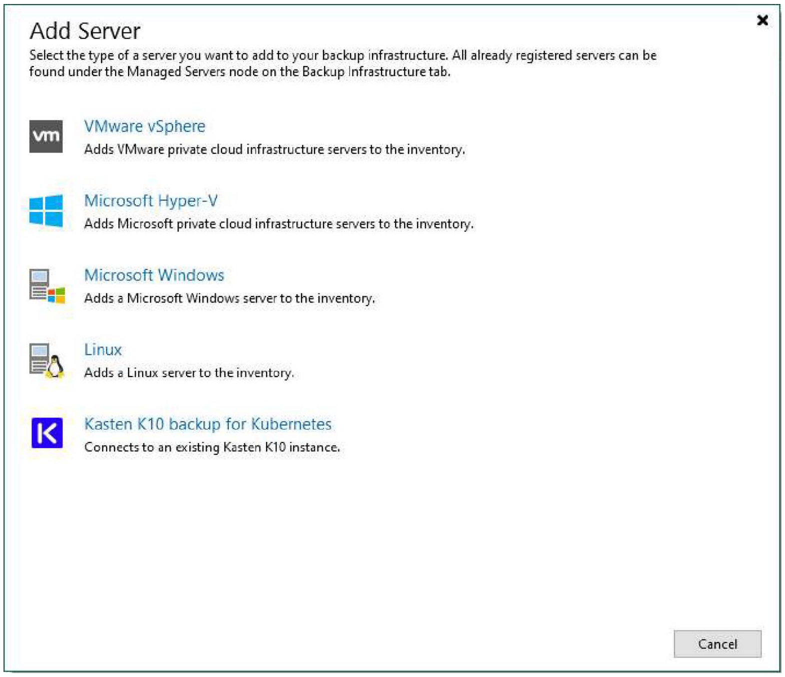
4. On the Backup Infrastructure page, select Managed Servers.

5. Right-click Managed Servers and select Add Server.



Name ↑	Type	Description
HPHV01	Microsoft Hyper-V server	Created by GOODDEALMART\csun at 2/3/2023 10:...
HPHV02	Microsoft Hyper-V server	Created by GOODDEALMART\csun at 2/3/2023 4:2...
SMB3	Standalone SMB3 server	Created by GOODDEALMART\csun at 2/3/2023 12:...
STORAGE-WIN	Microsoft Windows server	Created by GOODDEALMART\csun at 2/3/2023 1:1...
VBR12PostgreSQL.g...	Microsoft Windows server	Backup server

6. Select Linux on the Add Server page.



Add Server

Select the type of a server you want to add to your backup infrastructure. All already registered servers can be found under the Managed Servers node on the Backup Infrastructure tab.

VMware vSphere
Adds VMware private cloud infrastructure servers to the inventory.

Microsoft Hyper-V
Adds Microsoft private cloud infrastructure servers to the inventory.

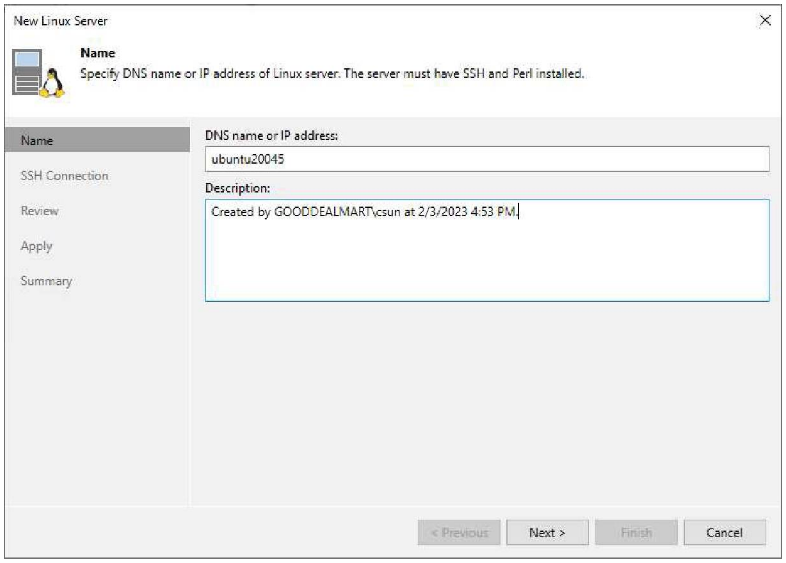
Microsoft Windows
Adds a Microsoft Windows server to the inventory.

Linux
Adds a Linux server to the inventory.

Kasten K10 backup for Kubernetes
Connects to an existing Kasten K10 instance.

7. Enter the Linux server's full DNS name or IP address on the Name page.

8. Give a brief description in the Description field for future reference and click Next.



New Linux Server

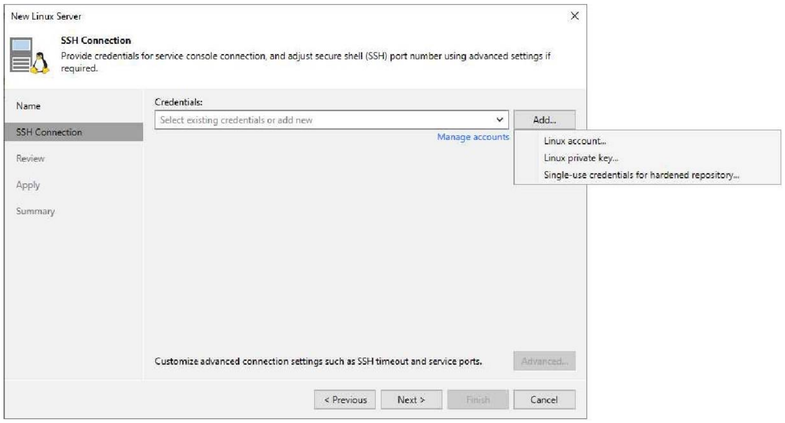
Name

Specify DNS name or IP address of Linux server. The server must have SSH and Perl installed.

DNS name or IP address: ubuntu20045

Description: Created by GOODDEALMART\csun at 2/3/2023 4:53 PM.

9. Click Add on the SSH Connection page and select Single-use credential for the hardened repository.



New Linux Server

SSH Connection

Provide credentials for service console connection, and adjust secure shell (SSH) port number using advanced settings if required.

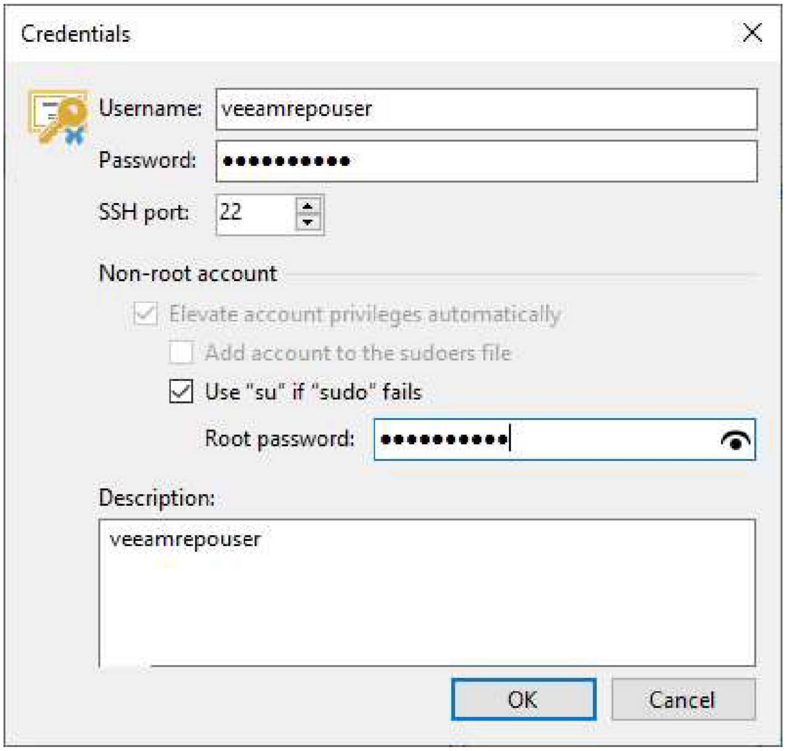
Credentials: Select existing credentials or add new

Customize advanced connection settings such as SSH timeout and service ports.

Note:

These credentials are not saved by Veeam Backup & Replication. They are only used to install Veeam Data Mover on the server. These credentials reduce the rights of the Veeam Data Mover. Single-use or temporary credentials are recommended options for a hardened repository.

10. On the Credentials page, Enter a username
11. Enter a user name in the Username field.
12. Enter a password in the Password field.
13. Enter 22 in the SSH port field.
14. Give a brief description in the Description field for future reference and click OK.



Credentials

Username: veeamrepouser

Password: ●●●●●●●●●●

SSH port: 22

Non-root account

☑ Elevate account privileges automatically

□ Add account to the sudoers file

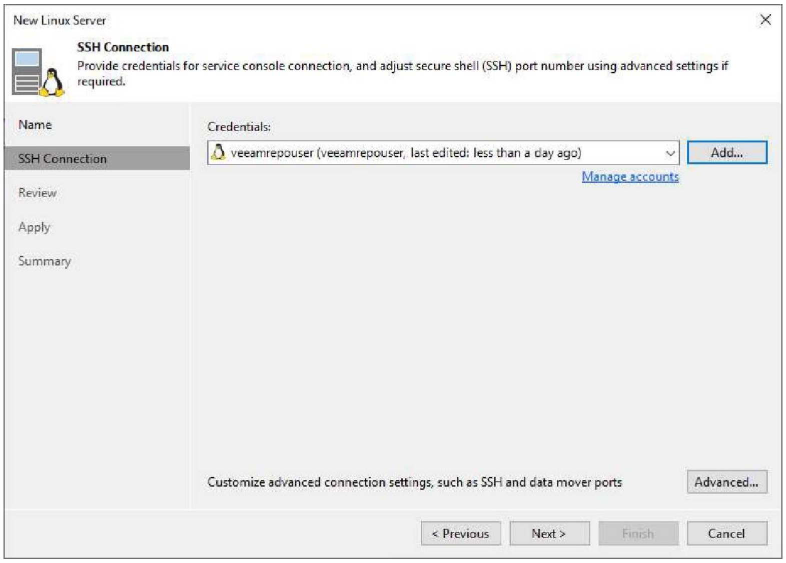
☑ Use "su" if "sudo" fails

Root password: ●●●●●●●●●●

Description:

veeamrepouser

15. On the SSH Connection page, click Advanced.



New Linux Server

SSH Connection

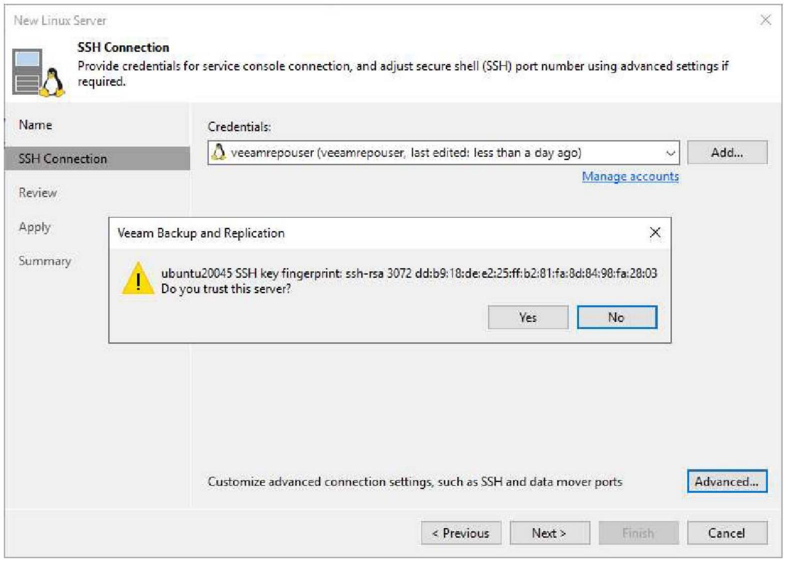
Provide credentials for service console connection, and adjust secure shell (SSH) port number using advanced settings if required.

Credentials:

veeamrepouser (veeamrepouser, last edited: less than a day ago)

Customize advanced connection settings, such as SSH and data mover ports

16. Select Yes on the trust warning message page.



SSH Connection

Provide credentials for service console connection, and adjust secure shell (SSH) port number using advanced settings if required.

Credentials: veeamrepouser (veeamrepouser, last edited: less than a day ago)

Veeam Backup and Replication

ubuntu20045 SSH key fingerprint: ssh-rsa 3072 dd:b9:18:de:e2:25:ff:b2:81:fa:8d:84:98:fa:28:03
Do you trust this server?

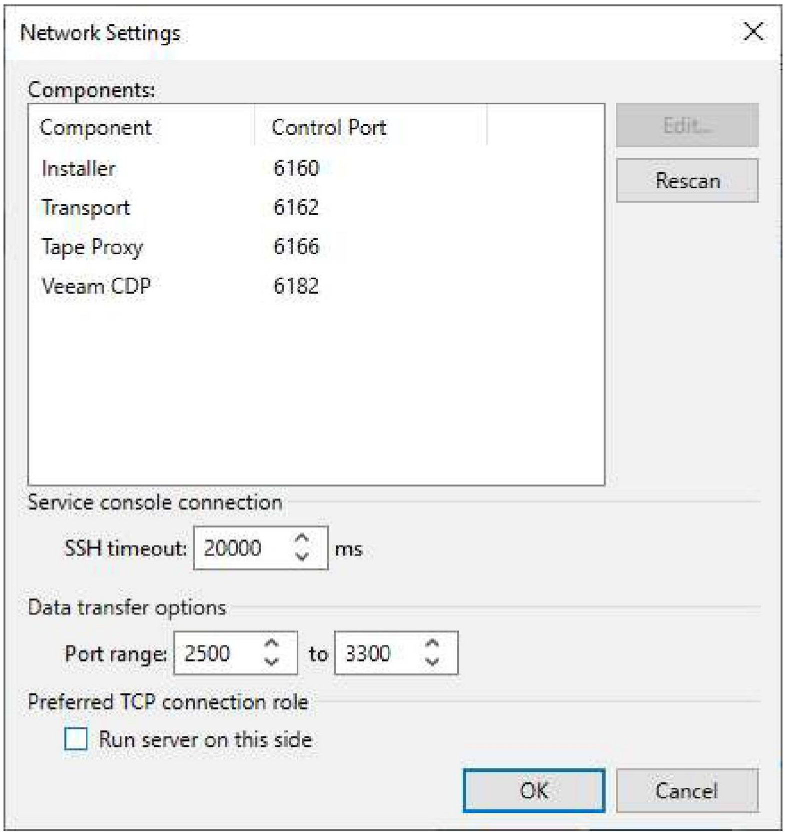
Customize advanced connection settings, such as SSH and data mover ports

17. If necessary, change the network ports used by Veeam Backup & Replication components on the Network Settings page.

18. In the Service console connection section, enter an SSH timeout. The default timeout is set to 20000 ms.

19. Configure connection settings for file copy operations in the Network Settings window's Data transfer options section. Provide a set of ports for transmission channels between the source and target hosts (one port per task).

20. Select the Run server on this side checkbox in the Preferred TCP connection role section. The outside client cannot connect to the server on the NAT network in the NAT scenario. As a result, services that require external connection initiation may be disrupted.



Components:

Component	Control Port
Installer	6160
Transport	6162
Tape Proxy	6166
Veeam CDP	6182

Service console connection

SSH timeout: 20000 ms

Data transfer options

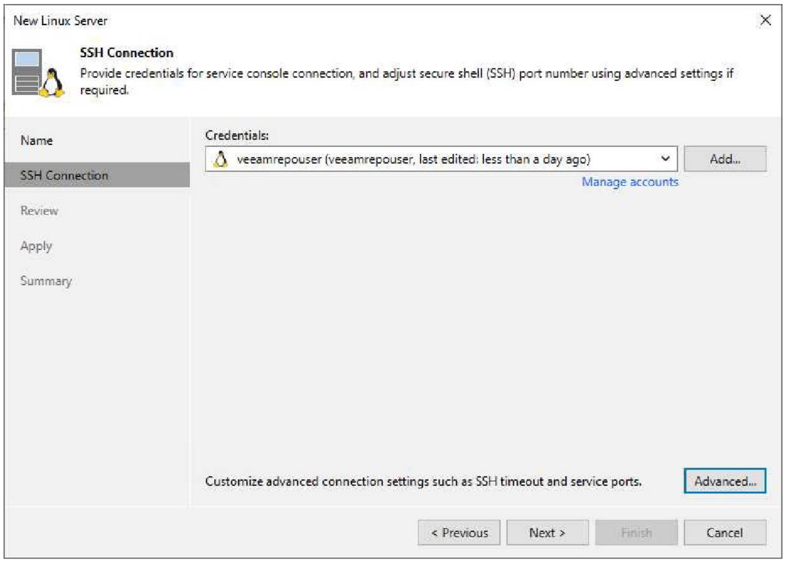
Port range: 2500 to 3300

Preferred TCP connection role

□ Run server on this side

21. Click OK.

22. Click Next on the SSH Connection page.



New Linux Server

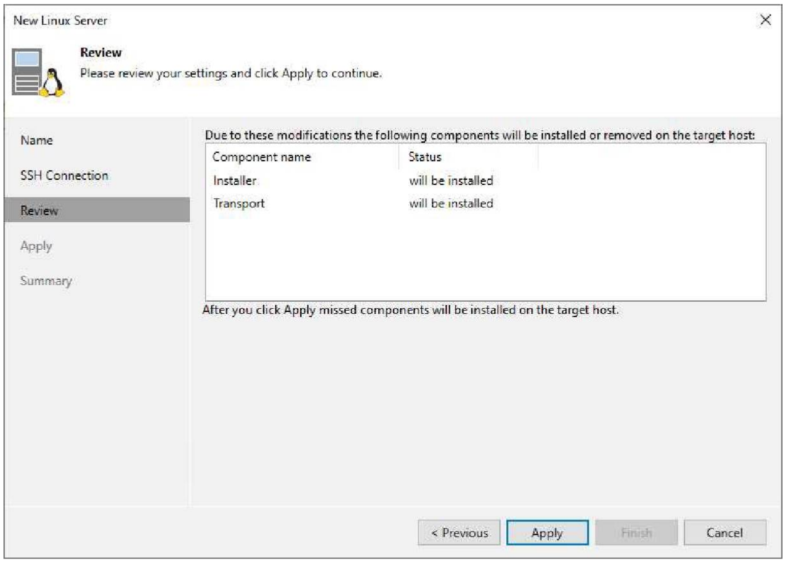
SSH Connection

Provide credentials for service console connection, and adjust secure shell (SSH) port number using advanced settings if required.

Credentials: veeamrepouser (veeamrepouser, last edited: less than a day ago)

Customize advanced connection settings such as SSH timeout and service ports.

23. Click Apply on the Review page.



New Linux Server

Review

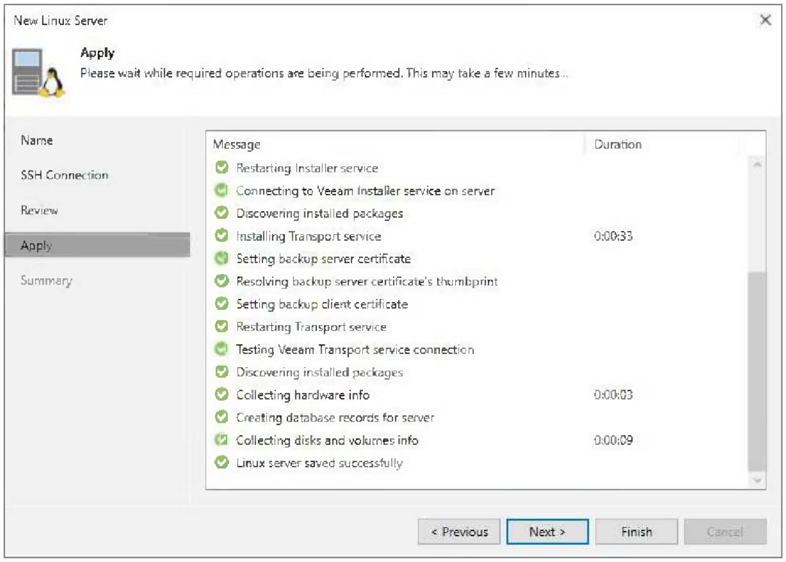
Please review your settings and click Apply to continue.

Due to these modifications the following components will be installed or removed on the target host:

Component name	Status
Installer	will be installed
Transport	will be installed

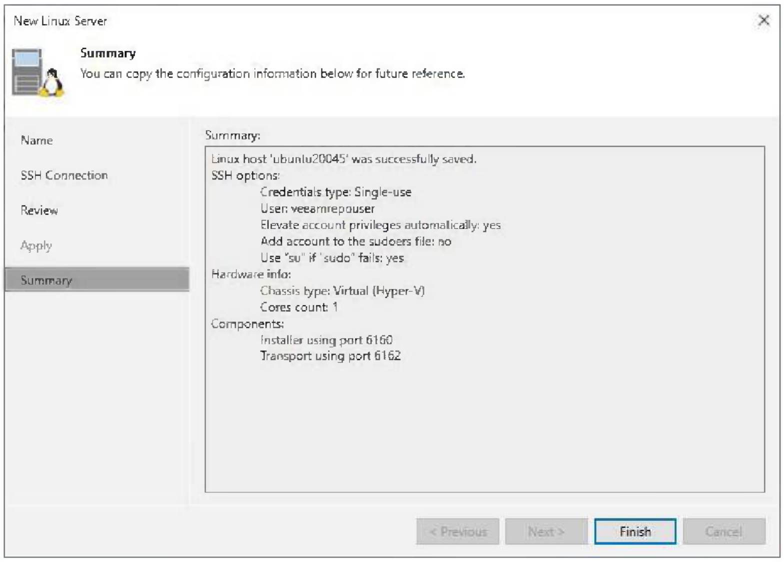
After you click Apply missed components will be installed on the target host.

24. Click Next on the Apply page.


New Linux Server
Apply
Please wait while required operations are being performed. This may take a few minutes...
Name
SSH Connection
Review
Apply
Summary
< Previous
Next >
Finish
Cancel

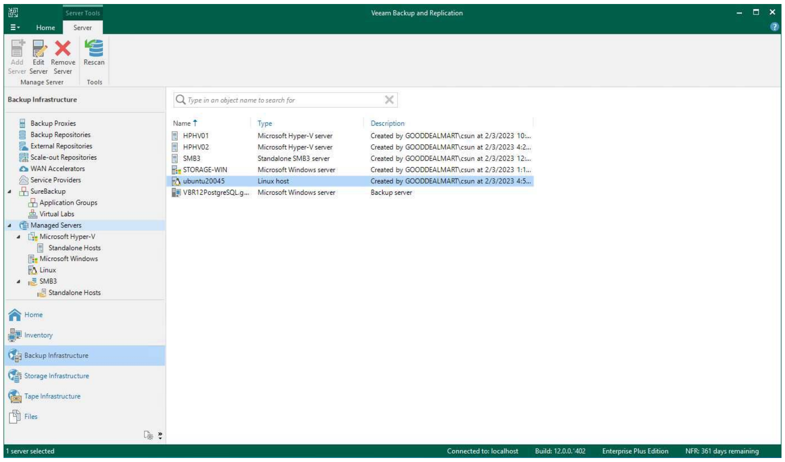
```
Message                                                   Duration
Restarting Installer service
Connecting to Veeam Installer service on server
Discovering installed packages
Installing Transport service                              0:00:33
Setting backup server certificate
Resolving backup server certificate's thumbprint
Setting backup client certificate
Restarting Transport service
Testing Veeam Transport service connection
Discovering installed packages
Collecting hardware info                                  0:00:03
Creating database records for server
Collecting disks and volumes info                         0:00:09
Linux server saved successfully
```

25. Click Finish on the Summary page.



```
Summary:
Linux host 'ubuntu20045' was successfully saved.
SSH options:
        Credentials type: Single-use
        User: veeamrepouser
        Elevate account privileges automatically: yes
        Add account to the sudoers file: no
        Use "su" if "sudo" fails: yes
Hardware info:
        Chassis type: Virtual (Hyper-V)
        Cores count: 1
Components:
        Installer using port 6160
        Transport using port 6162
```

26. Ensure the new Linux server is added.

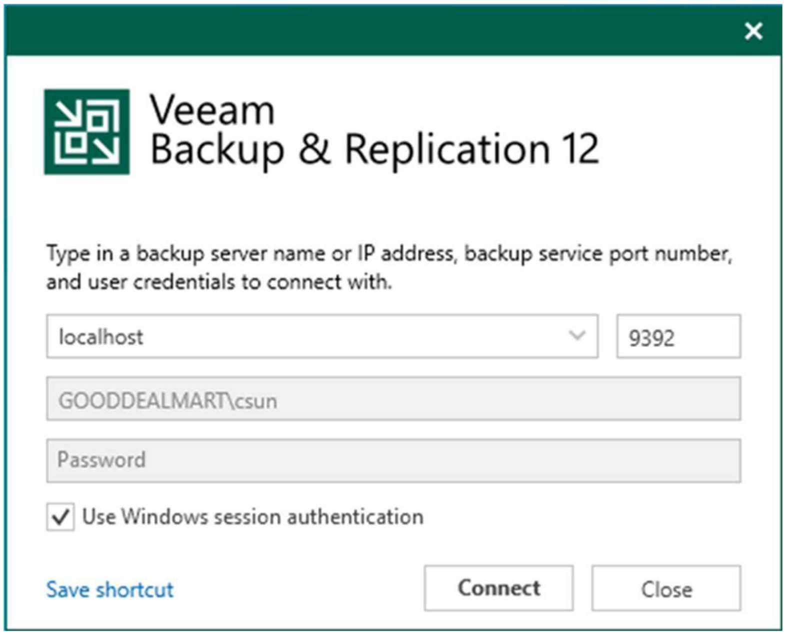


Name	Type	Description
HPHV01	Microsoft Hyper-V server	Created by GOODDEALMART\csun at 2/3/2023 10:...
HPHV02	Microsoft Hyper-V server	Created by GOODDEALMART\csun at 2/3/2023 4:2...
SMB3	Standalone SMB3 server	Created by GOODDEALMART\csun at 2/3/2023 12:...
STORAGE-WIN	Microsoft Windows server	Created by GOODDEALMART\csun at 2/3/2023 1:1...
ubuntu20045	Linux host	Created by GOODDEALMART\csun at 2/3/2023 4:5...
VBR12PostgreSQL.g...	Microsoft Windows server	Backup server

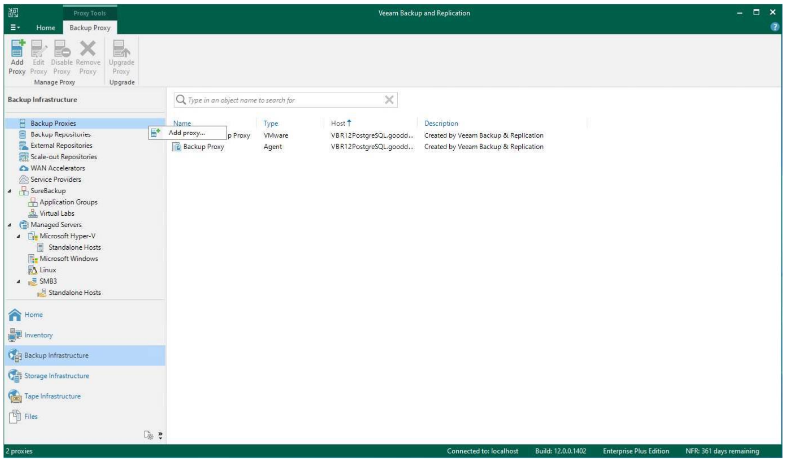
1 server selected Connected to: localhost Build: 12.0.0.1402 Enterprise Plus Edition NFR: 361 days remaining

Add Off-Host Backup proxy servers

Off-Host Backup proxy servers will retrieve VM data from the source datastore, process it and transfer it to the destination. The off-host backup proxy removes unwanted overhead on the production Hyper-V host.

Instructions	Screenshot (if applicable)
1. Log in to the Veeam Backup and replication manager server. 2. Open the Veeam Backup & Replication Console, and click Connect.	 Veeam Backup & Replication 12 Type in a backup server name or IP address, backup service port number, and user credentials to connect with. localhost 9392 GOODDEALMART\csun Password ☑ Use Windows session authentication Save shortcut Connect Close

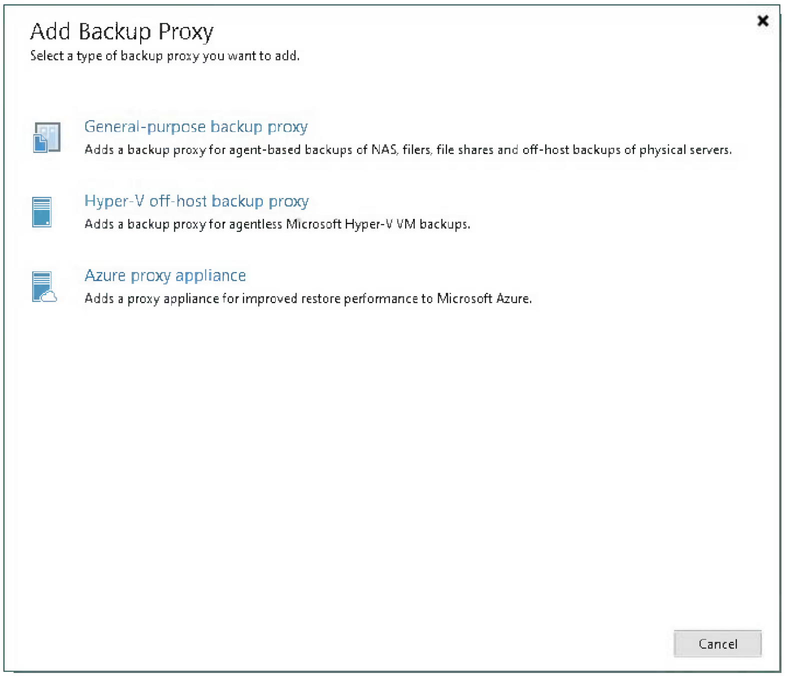
3. On the Home page, select Backup Infrastructure.
4. On the Backup Infrastructure page, select Backup Proxies.
5. Right-click Backup Proxies and select Add Proxies.



Name	Type	Host	Description
p Proxy	VMware	VBR12PostgreSQL.goodd...	Created by Veeam Backup & Replication
Backup Proxy	Agent	VBR12PostgreSQL.goodd...	Created by Veeam Backup & Replication

2 proxies | Connected to: localhost | Build: 12.0.0.1402 | Enterprise Plus Edition | NFR: 361 days remaining

6. Select Hyper-V off-host backup proxy on the Add Backup Proxy page.



Add Backup Proxy

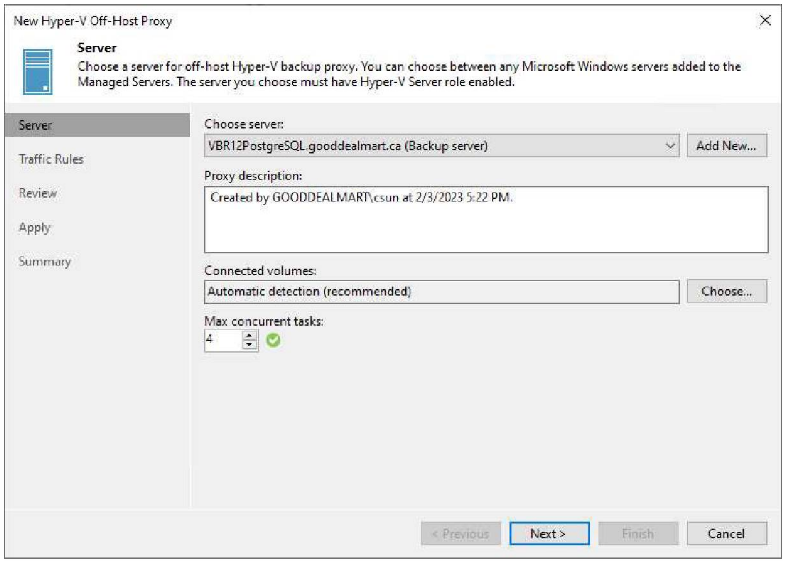
Select a type of backup proxy you want to add.

General-purpose backup proxy
Adds a backup proxy for agent-based backups of NAS, filers, file shares and off-host backups of physical servers.

Hyper-V off-host backup proxy
Adds a backup proxy for agentless Microsoft Hyper-V VM backups.

Azure proxy appliance
Adds a proxy appliance for improved restore performance to Microsoft Azure.

7. Click Add New in the Choose server field on the Server page.



New Hyper-V Off-Host Proxy

Server

Choose a server for off-host Hyper-V backup proxy. You can choose between any Microsoft Windows servers added to the Managed Servers. The server you choose must have Hyper-V Server role enabled.

Choose server: VBR12PostgreSQL.gooddealmart.ca (Backup server)

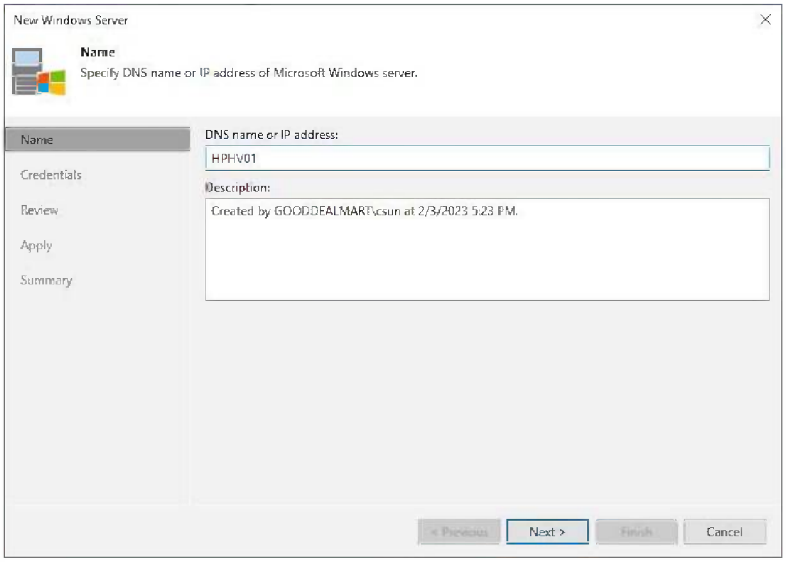
Proxy description: Created by GOODDEALMART\csun at 2/3/2023 5:22 PM.

Connected volumes: Automatic detection (recommended)

Max concurrent tasks: 4

8. Enter the Microsoft Windows server's full DNS name or IP address on the Name page.

9. Give a brief description in the Description field for future reference and click Next.



New Windows Server

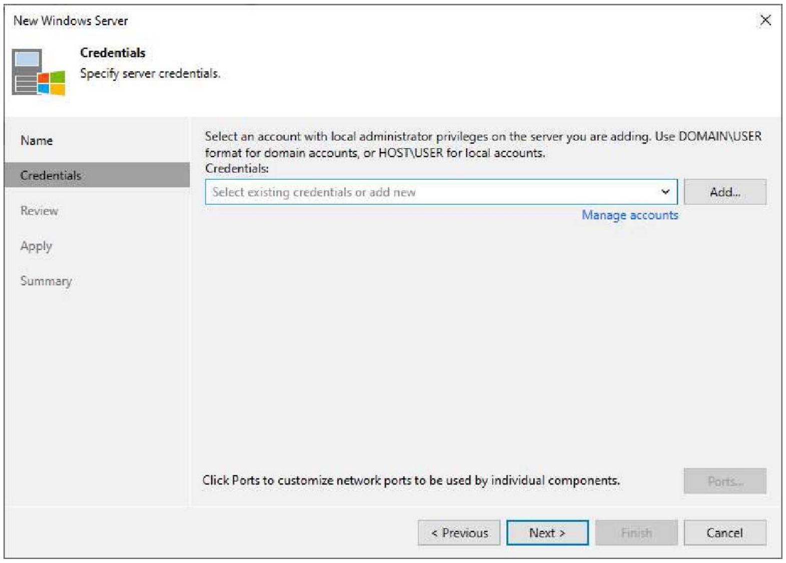
Name

Specify DNS name or IP address of Microsoft Windows server.

DNS name or IP address: HPHV01

Description: Created by GOODDEALMART\csun at 2/3/2023 5:23 PM.

10. Select an account from the Credentials drop-down list on the Credentials page or click Add on the right to add the credentials.



Credentials

Specify server credentials.

Select an account with local administrator privileges on the server you are adding. Use DOMAIN\USER format for domain accounts, or HOST\USER for local accounts.

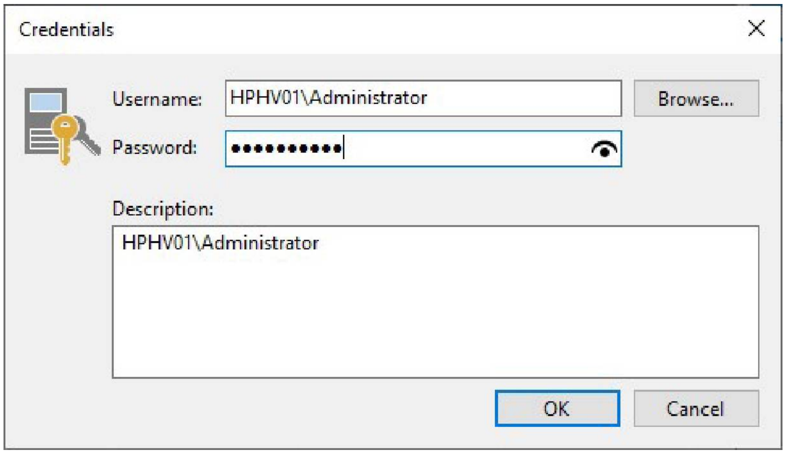
Credentials: Select existing credentials or add new

Click Ports to customize network ports to be used by individual components.

11. On the Credentials page, enter a user name in the Username field. You also can click Browse to select an existing user account.

12. Enter the password In the Password field.

13. Give a brief description in the Description field for future reference and click OK.

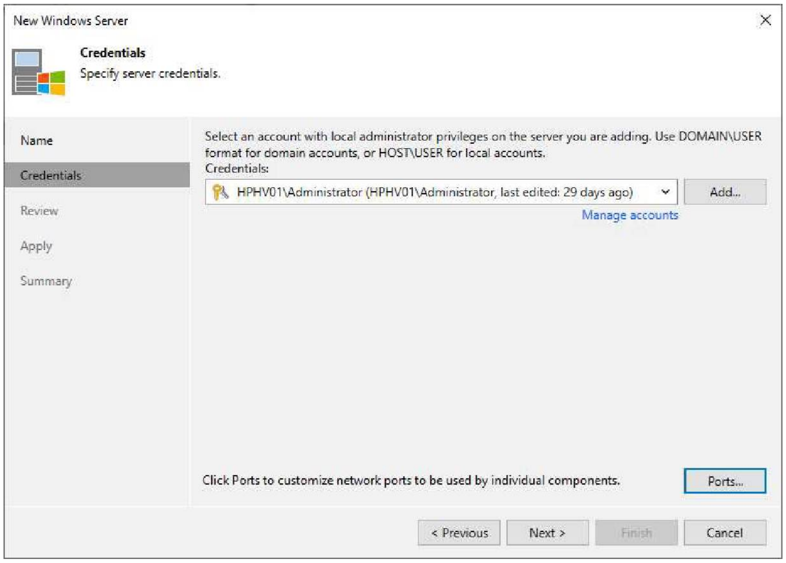


Username: HPHV01\Administrator

Password: ●●●●●●●●●●

Description: HPHV01\Administrator

14. On the Credentials page, click Ports.



New Windows Server

Credentials

Specify server credentials.

Select an account with local administrator privileges on the server you are adding. Use DOMAIN\USER format for domain accounts, or HOST\USER for local accounts.

Credentials:

HPHV01\Administrator (HPHV01\Administrator, last edited: 29 days ago)

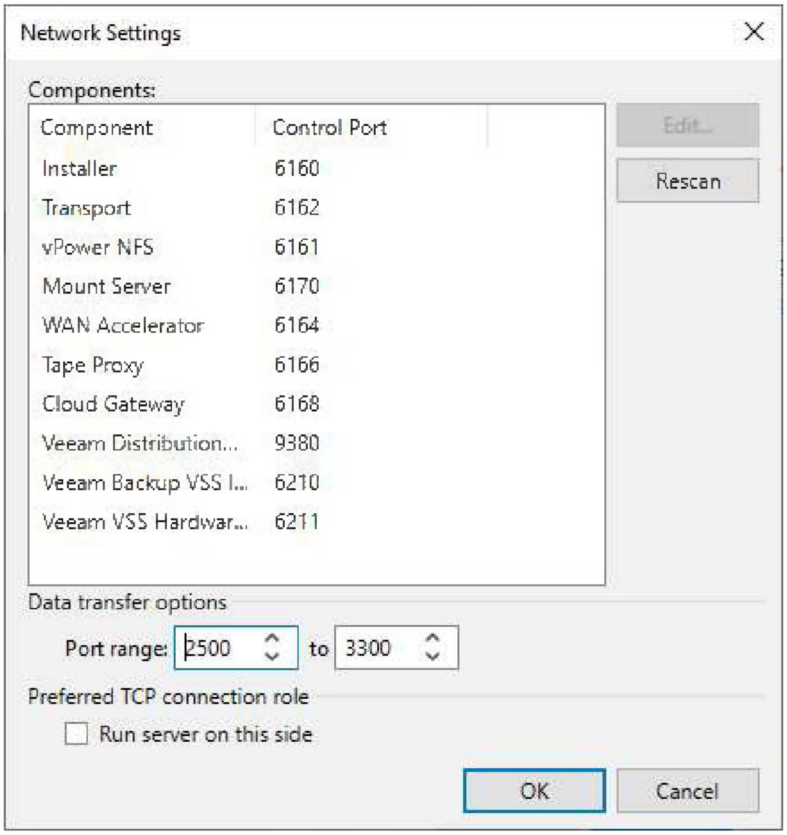
Click Ports to customize network ports to be used by individual components.

15. If necessary, change the network ports used by Veeam Backup & Replication components on the Network Settings page.

16. Configure connection settings for file copy operations in the Network Settings window's Data transfer options section. Provide a set of ports for transmission channels between the source and target hosts (one port per task).

17. Select the Run server on this side checkbox in the Preferred TCP connection role section. The outside client cannot connect to the server on the NAT network in the NAT scenario. As a result, services that require external connection initiation may be disrupted.

18. Click OK.



Components:

Component	Control Port
Installer	6160
Transport	6162
vPower NFS	6161
Mount Server	6170
WAN Accelerator	6164
Tape Proxy	6166
Cloud Gateway	6168
Veeam Distribution...	9380
Veeam Backup VSS I...	6210
Veeam VSS Hardwar...	6211

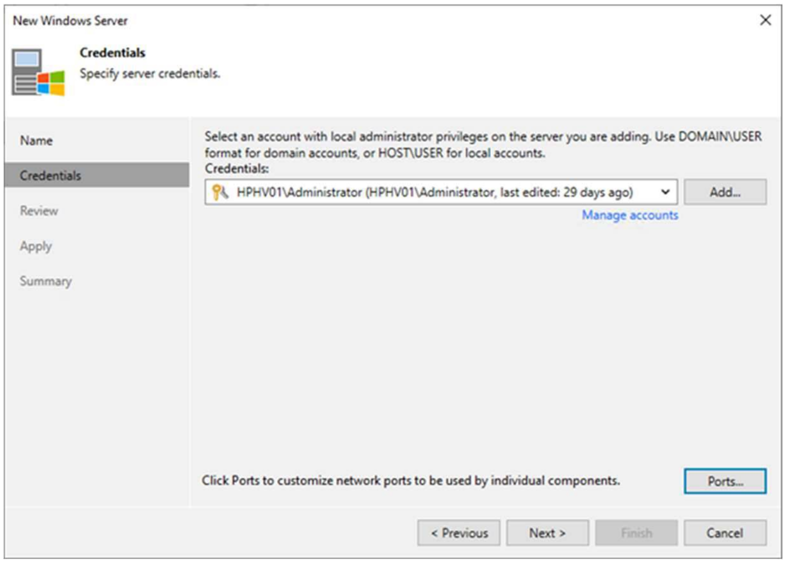
Data transfer options

Port range: 2500 to 3300

Preferred TCP connection role

□ Run server on this side

19. Click Next on the Credentials page.



New Windows Server

Credentials

Specify server credentials.

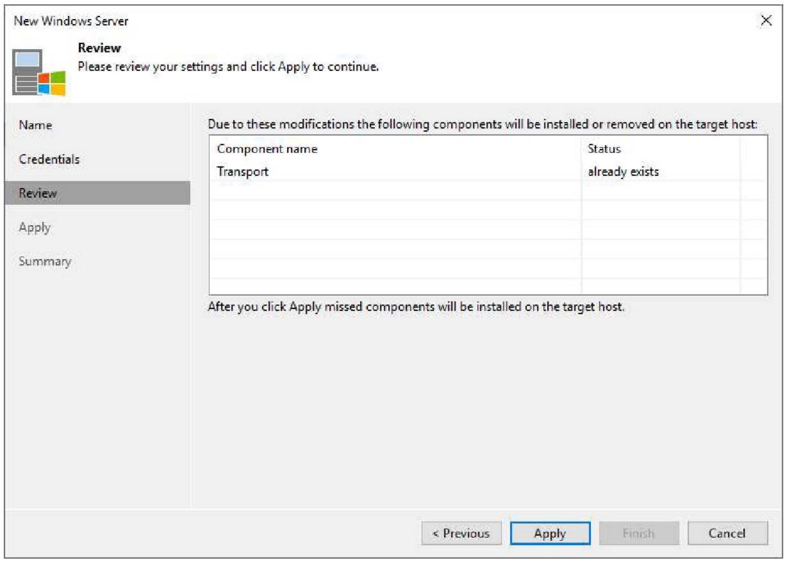
Select an account with local administrator privileges on the server you are adding. Use DOMAIN\USER format for domain accounts, or HOST\USER for local accounts.

Credentials:

HPHV01\Administrator (HPHV01\Administrator, last edited: 29 days ago)

Click Ports to customize network ports to be used by individual components.

20. Click Apply on the Review page.



New Windows Server

Review

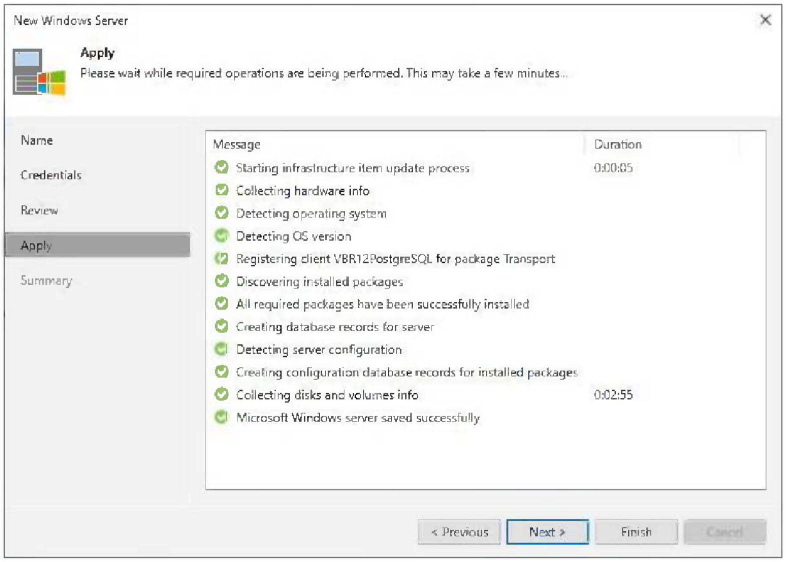
Please review your settings and click Apply to continue.

Due to these modifications the following components will be installed or removed on the target host:

Component name	Status
Transport	already exists

After you click Apply missed components will be installed on the target host.

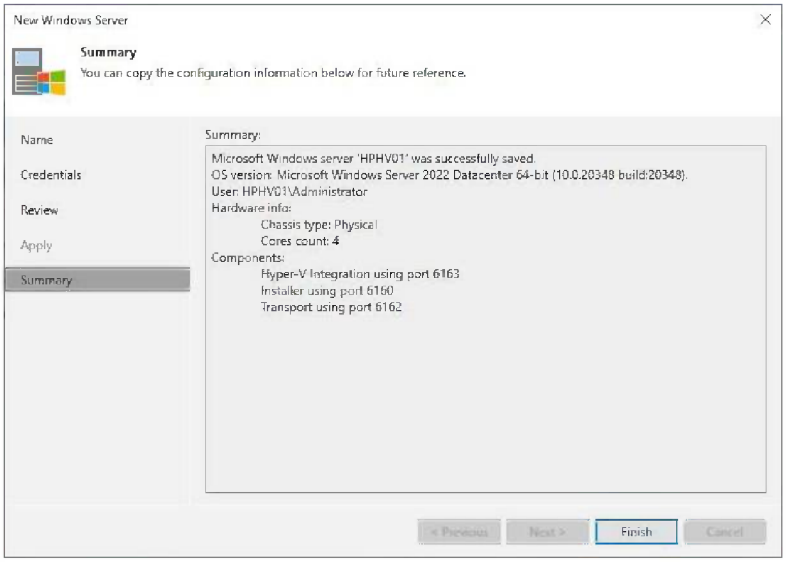
21. On the Apply page, click Next.



New Windows Server
Apply
Please wait while required operations are being performed. This may take a few minutes...
Name
Credentials
Review
Apply
Summary
< Previous
Next >
Finish
Cancel

```
Message                                                          Duration
Starting infrastructure item update process                      0:00:05
Collecting hardware info
Detecting operating system
Detecting OS version
Registering client VBR12PostgreSQL for package Transport
Discovering installed packages
All required packages have been successfully installed
Creating database records for server
Detecting server configuration
Creating configuration database records for installed packages
Collecting disks and volumes info                                0:02:55
Microsoft Windows server saved successfully
```

22. Click Finish on the Summary page.



Summary:

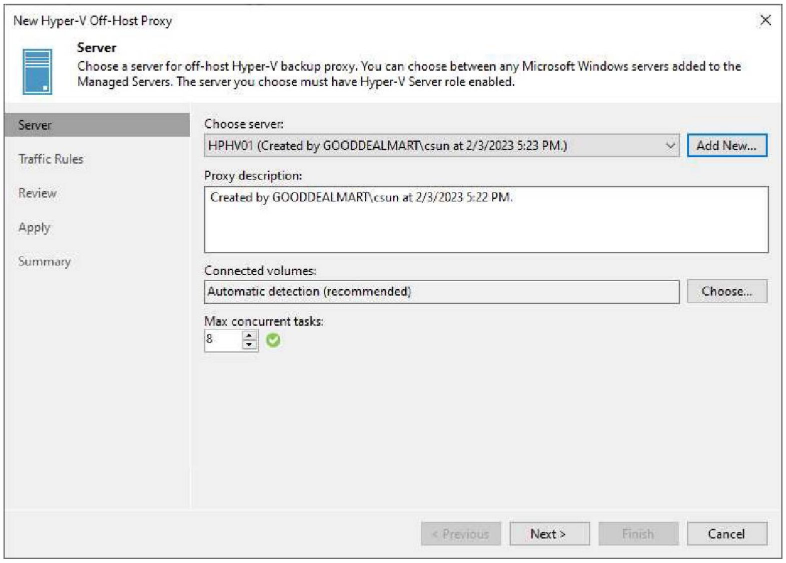
```
Microsoft Windows server 'HPHV01' was successfully saved.
OS version: Microsoft Windows Server 2022 Datacenter 64-bit (10.0.20348 build:20348).
User: HPHV01\Administrator
Hardware info:
        Chassis type: Physical
        Cores count: 4
Components:
        Hyper-V Integration using port 6163
        Installer using port 6160
        Transport using port 6162
```

23. Give a brief description in the Proxy description field for future reference.

24. In the Connected volumes field, leave the default settings.

25. Enter the number of tasks the off-host backup proxy must handle concurrently in the Max concurrent tasks field.

26. Click Next.



Server

Choose a server for off-host Hyper-V backup proxy. You can choose between any Microsoft Windows servers added to the Managed Servers. The server you choose must have Hyper-V Server role enabled.

Choose server: HPHV01 (Created by GOODDEALMART\csun at 2/3/2023 5:23 PM.)

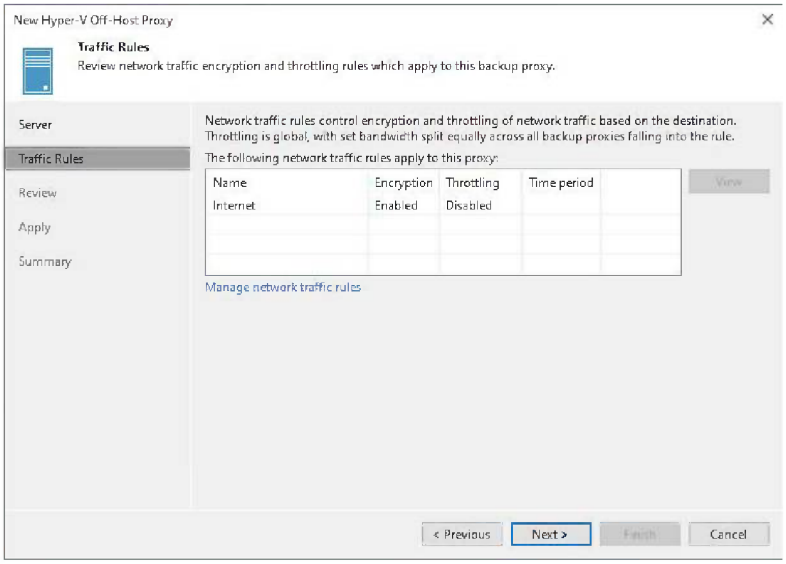
Proxy description: Created by GOODDEALMART\csun at 2/3/2023 5:22 PM.

Connected volumes: Automatic detection (recommended)

Max concurrent tasks: 8

27. On the Traffic Rules page, click Next.

28. You can open global network traffic settings and modify them directly from the New Hyper-V Off-Host Proxy wizard. To do this, click the Manage network traffic rules link at the bottom of the wizard.



Traffic Rules

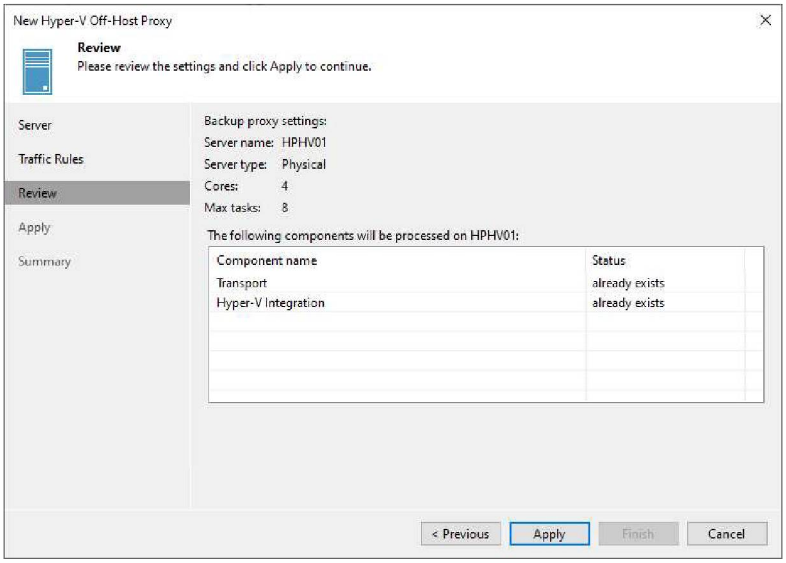
Review network traffic encryption and throttling rules which apply to this backup proxy.

Network traffic rules control encryption and throttling of network traffic based on the destination. Throttling is global, with set bandwidth split equally across all backup proxies falling into the rule.

The following network traffic rules apply to this proxy:

Name	Encryption	Throttling	Time period
Internet	Enabled	Disabled	

29. Click Apply on the Review page.



Review

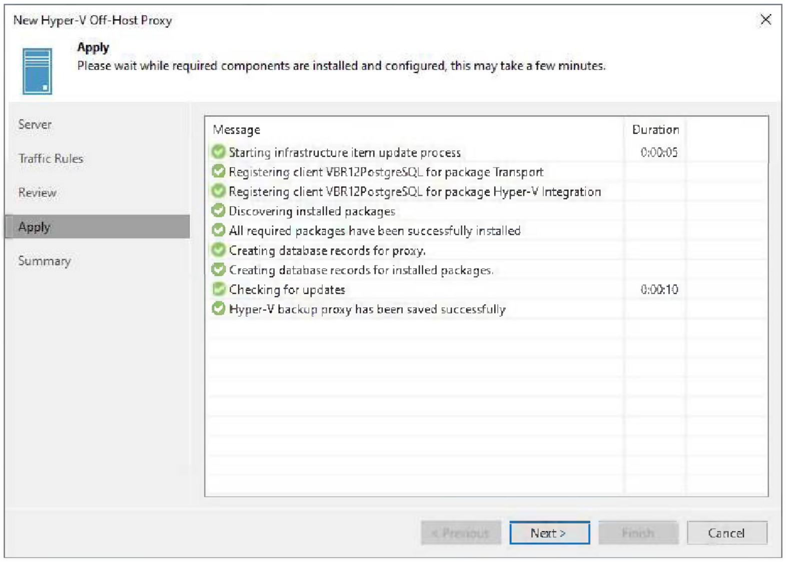
Please review the settings and click Apply to continue.

Backup proxy settings:
Server name: HPHV01
Server type: Physical
Cores: 4
Max tasks: 8

The following components will be processed on HPHV01:

Component name	Status
Transport	already exists
Hyper-V Integration	already exists

30. Click Next on the Apply page.

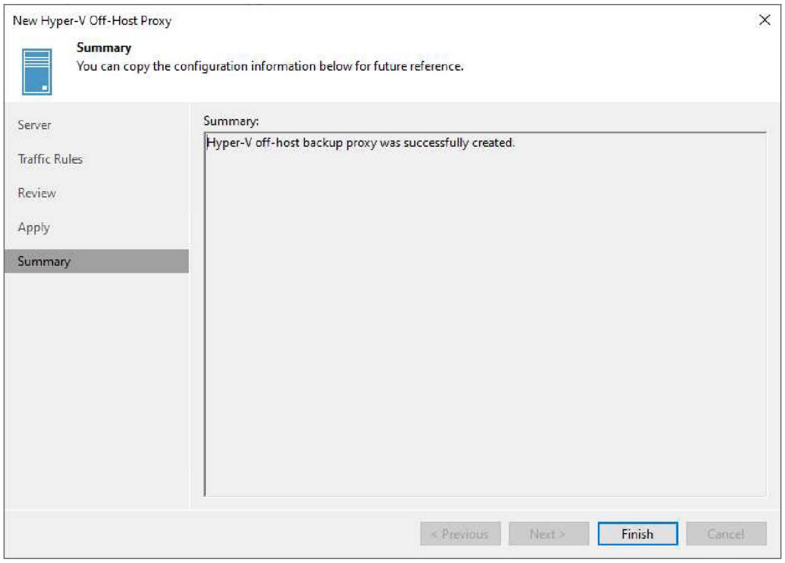


Apply

Please wait while required components are installed and configured, this may take a few minutes.

Message	Duration
✓ Starting infrastructure item update process	0:00:05
✓ Registering client VBR12PostgreSQL for package Transport	
✓ Registering client VBR12PostgreSQL for package Hyper-V Integration	
✓ Discovering installed packages	
✓ All required packages have been successfully installed	
✓ Creating database records for proxy.	
✓ Creating database records for installed packages.	
✓ Checking for updates	0:00:10
✓ Hyper-V backup proxy has been saved successfully	

31. Click Finish on the Summary page.



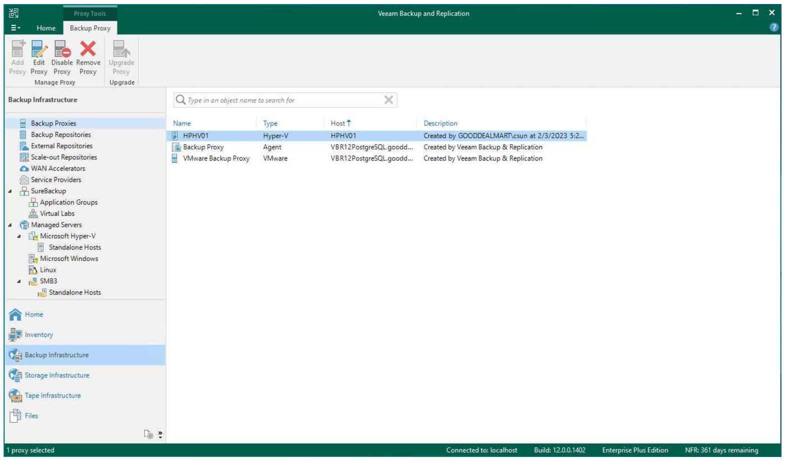
Summary

You can copy the configuration information below for future reference.

Summary:

Hyper-V off-host backup proxy was successfully created.

32. Ensure the new Off-Host Backup proxy server is added.



Name	Type	Host	Description
HPHV01	Hyper-V	HPHV01	Created by GOODDEALMART\csun at 2/3/2023 5:2...
Backup Proxy	Agent	VBR12PostgreSQL.goodd...	Created by Veeam Backup & Replication
VMware Backup Proxy	VMware	VBR12PostgreSQL.goodd...	Created by Veeam Backup & Replication

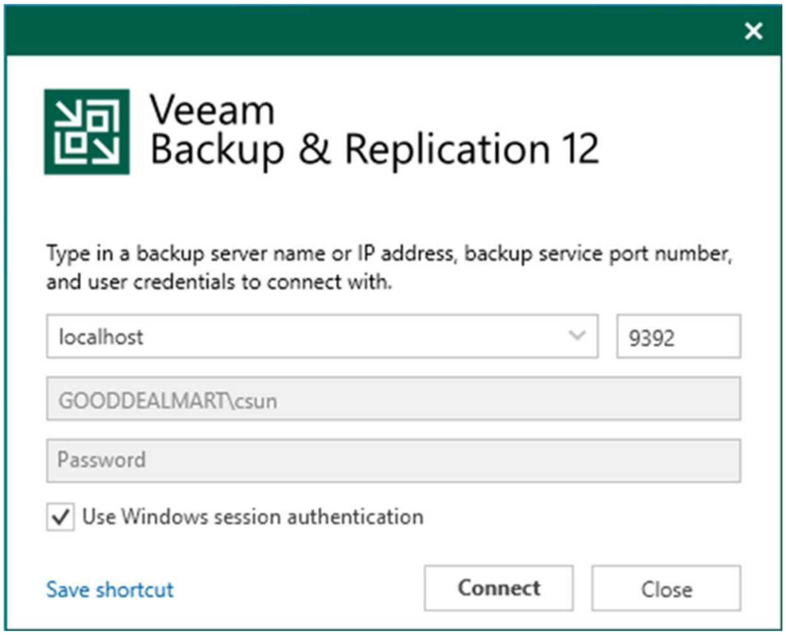
1 proxy selected   Connected to: localhost   Build: 12.0.0.1402   Enterprise Plus Edition   NFR: 361 days remaining

Add WAN Acceleration

Veeam's WAN acceleration technology optimizes data transfer to remote locations. It is explicitly designed for off-site backup copy and replication jobs. You must deploy a pair of WAN accelerators in your backup infrastructure to enable WAN acceleration and data deduplication technologies.

Note:

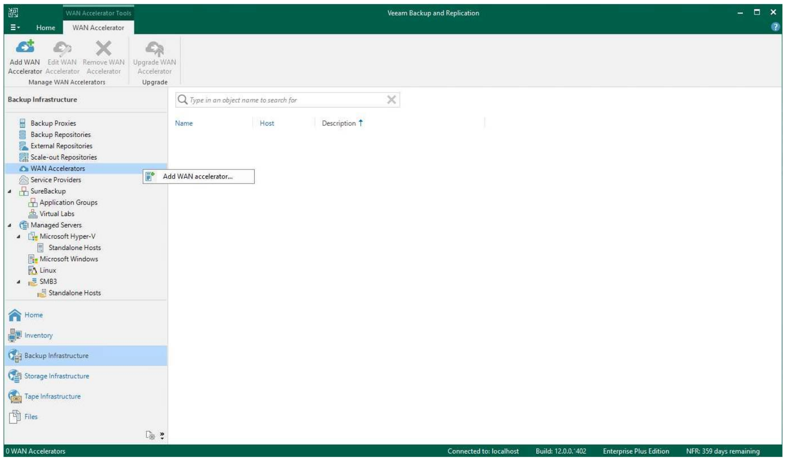
The Veeam Universal License includes WAN acceleration. Veeam Backup & Replication Enterprise or Enterprise Plus editions are required when using a legacy socket-based licence.

Instructions	Screenshot (if applicable)
1. Log in to the Veeam Backup and replication manager server. 2. Open the Veeam Backup & Replication Console and click Connect.	 Veeam Backup & Replication 12 Type in a backup server name or IP address, backup service port number, and user credentials to connect with. localhost 9392 GOODDEALMART\csun Password ☑ Use Windows session authentication

3. On the Home page, select Backup Infrastructure.

4. On the Backup Infrastructure page, select WAN Accelerators.

5. Right-click WAN Accelerators and select Add WAN Accelerator.



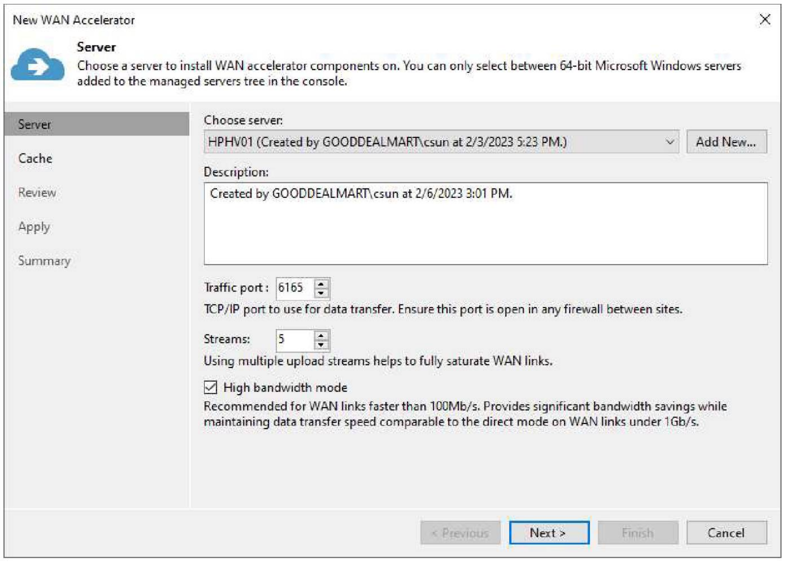
0 WAN Accelerators   Connected to: localhost   Build: 12.0.0.1402   Enterprise Plus Edition   NFR: 359 days remaining

6. Select a Microsoft Windows server from the Choose server drop-down list on the Server page.

7. Give a brief description in the Description field for future reference.

8. Specify the port number in the Traffic port field.

9. Specify the number of connections in the Streams field. If the link has low latency and high bandwidth, the default setting (5 streams) may sufficiently saturate it thoroughly. However, the link still needs to be fully utilized the number of streams may be increased. According to



Server

Choose a server to install WAN accelerator components on. You can only select between 64-bit Microsoft Windows servers added to the managed servers tree in the console.

Choose server: HPHV01 (Created by GOODDEALMART\csun at 2/3/2023 5:23 PM.)

Description: Created by GOODDEALMART\csun at 2/6/2023 3:01 PM.

Traffic port: 6165

TCP/IP port to use for data transfer. Ensure this port is open in any firewall between sites.

Streams: 5

Using multiple upload streams helps to fully saturate WAN links.

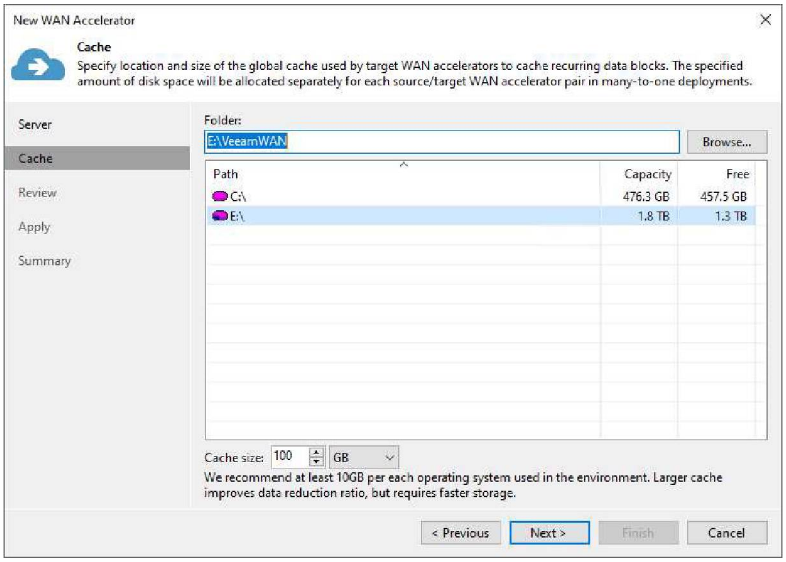
☑ High bandwidth mode

Recommended for WAN links faster than 100Mb/s. Provides significant bandwidth savings while maintaining data transfer speed comparable to the direct mode on WAN links under 1Gb/s.

tests, multiplying the link speed by 1.5 is a good best practice for estimating the number of streams required for high latency.

10. Veeam recommends using the High bandwidth mode option if your network bandwidth exceeds 100 Mbps. This mode offers significant bandwidth savings on WAN links less than 1 Gbps than the direct method.
11. Click Next.

12. Specify a path to the folder in the Folder field on the Cache page.
13. Specify the size for the global cache in the Cache size field.
14. Click Next.



New WAN Accelerator

Cache

Specify location and size of the global cache used by target WAN accelerators to cache recurring data blocks. The specified amount of disk space will be allocated separately for each source/target WAN accelerator pair in many-to-one deployments.

Folder: E:\VeeamWAN

Path	Capacity	Free
C:\	476.3 GB	457.5 GB
E:\	1.8 TB	1.3 TB

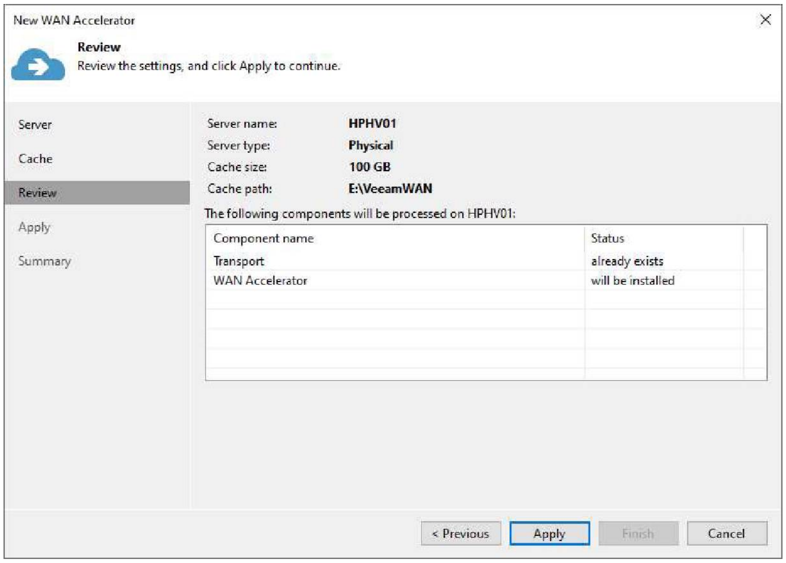
Cache size: 100 GB

We recommend at least 10GB per each operating system used in the environment. Larger cache improves data reduction ratio, but requires faster storage.

Note:

If both WAN accelerators (source and target) are set to High bandwidth, WAN acceleration does not use the global cache. However, remember that you can deactivate the High bandwidth mode and return to the Low bandwidth mode anytime.

15. On the Review page, click Apply.

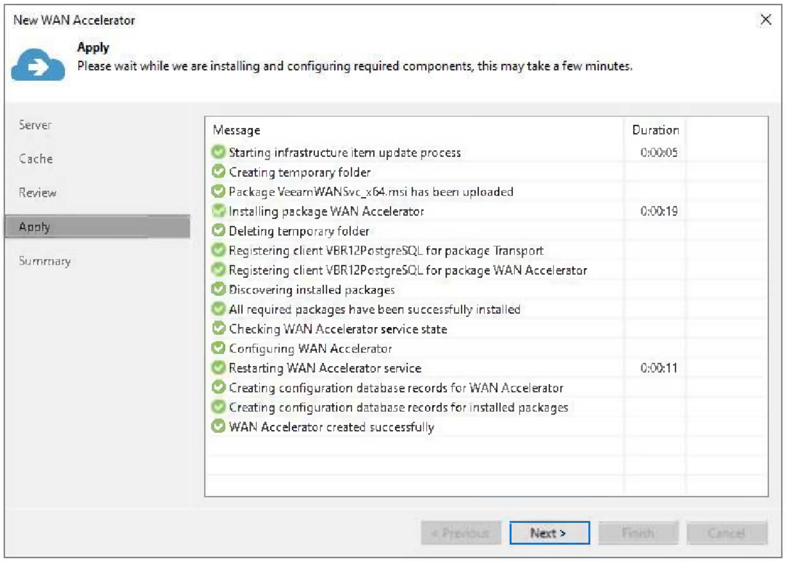


Server name: HPHV01
Server type: Physical
Cache size: 100 GB
Cache path: E:\VeeamWAN

The following components will be processed on HPHV01:

Component name	Status
Transport	already exists
WAN Accelerator	will be installed

16. Click Next on the Apply page.

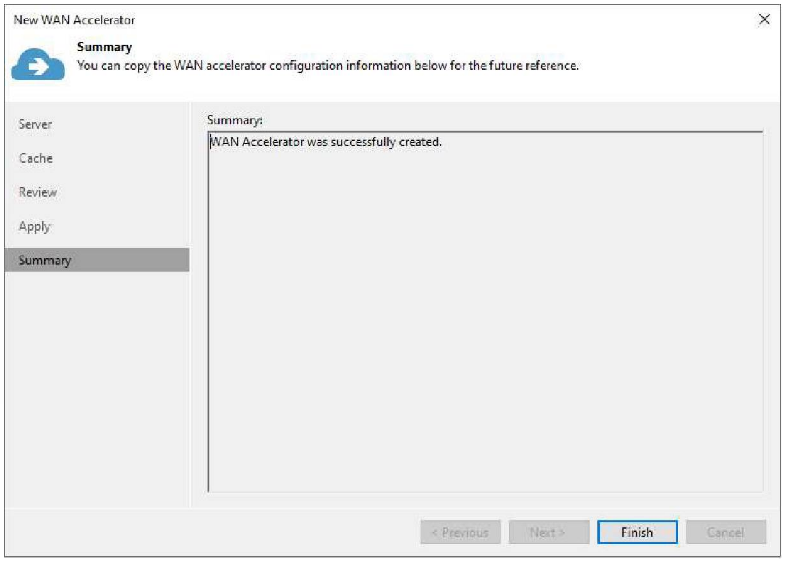


Apply

Please wait while we are installing and configuring required components, this may take a few minutes.

Message	Duration
✓ Starting infrastructure item update process	0:00:05
✓ Creating temporary folder	
✓ Package VeeamWANSvc_x64.msi has been uploaded	
✓ Installing package WAN Accelerator	0:00:19
✓ Deleting temporary folder	
✓ Registering client VBR12PostgreSQL for package Transport	
✓ Registering client VBR12PostgreSQL for package WAN Accelerator	
✓ Discovering installed packages	
✓ All required packages have been successfully installed	
✓ Checking WAN Accelerator service state	
✓ Configuring WAN Accelerator	
✓ Restarting WAN Accelerator service	0:00:11
✓ Creating configuration database records for WAN Accelerator	
✓ Creating configuration database records for installed packages	
✓ WAN Accelerator created successfully	

17. Click Finish on the Summary page.



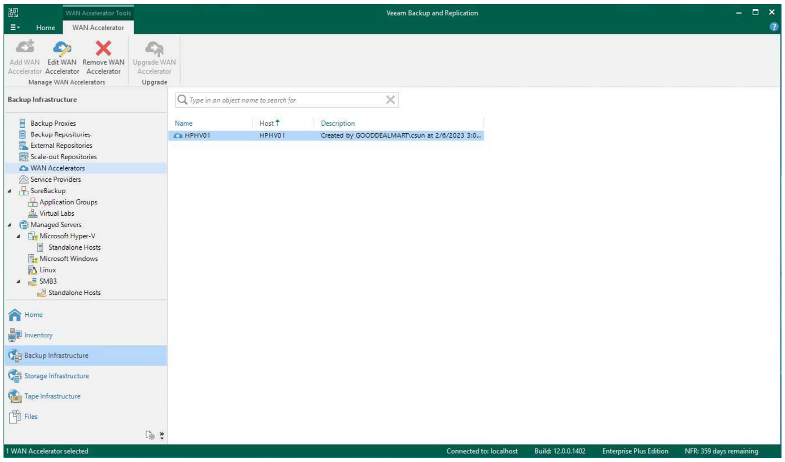
Summary

You can copy the WAN accelerator configuration information below for the future reference.

Summary:

WAN Accelerator was successfully created.

18. Verify that the WAN Accelerator has been added.



Name	Host	Description
HPHV01	HPHV01	Created by GOODDEALMART\csun at 2/6/2023 3:0...

1 WAN Accelerator selected Connected to: localhost Build: 12.0.0.1402 Enterprise Plus Edition NFR: 359 days remaining

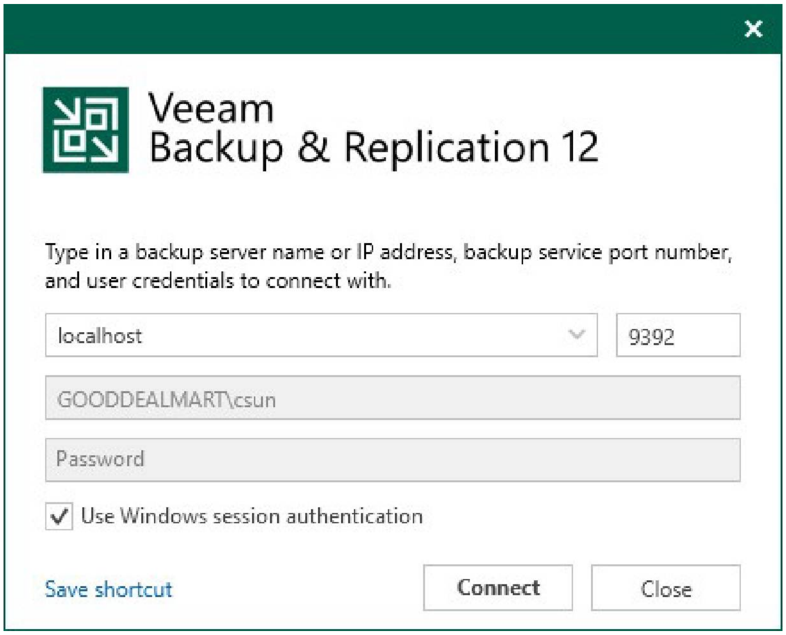
Physical Machines

Veeam Backup & Replication is a centralized control center for deploying and managing Veeam Agent, including Veeam Agent for Microsoft Windows, Linux, IBM AIX, Oracle Solaris, and Mac. Physical machines you want to protect with Veeam Agents are organized into protection groups in Veeam Backup & Replication. A protection group groups together protected computers of the same type. To simplify the management of such computers, Whether you create a protection group for laptops, workstations, servers or any other type of computer, Veeam Backup & Replication allows you to group them for dedicated and targeted protection easily. A separate protection group can also be used for Veeam Agent computers that you manage differently than other machines in your infrastructure.

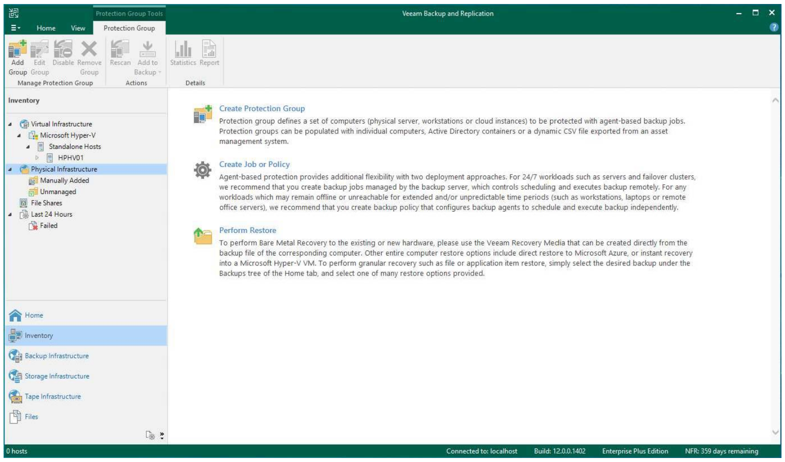
You can use protection groups to automate the Veeam Agent deployment and management on computers in the infrastructure. When you configure a protection group, you can specify scheduling options for protected computer discovery and Veeam Agent deployment. As a result, you do not need to install, configure, and run Veeam Agent on each computer whose data you wish to protect. Instead, you can use the Veeam Backup & Replication console to remotely perform all Veeam Agent deployment, administration, data protection, and disaster recovery tasks.

Add Veeam Agent to On-Premises Microsoft Windows Physical machines

You can back up and restore the On-Premises physical machines running Windows operating systems. Backup agents are installed on each computer by Veeam Backup & Replication.

Instructions	Screenshot (if applicable)
1. Log in to the Veeam Backup and replication manager server. 2. Open the Veeam Backup & Replication Console, and click Connect.	 Veeam Backup & Replication 12 Type in a backup server name or IP address, backup service port number, and user credentials to connect with. localhost 9392 GOODDEALMART\csun Password ☑ Use Windows session authentication Save shortcut Connect Close

3. Select Inventory on the Home page.
4. On the Inventory page, select Physical Infrastructure and click Create Protection Group.



Create Protection Group

Protection group defines a set of computers (physical server, workstations or cloud instances) to be protected with agent-based backup jobs. Protection groups can be populated with individual computers, Active Directory containers or a dynamic CSV file exported from an asset management system.

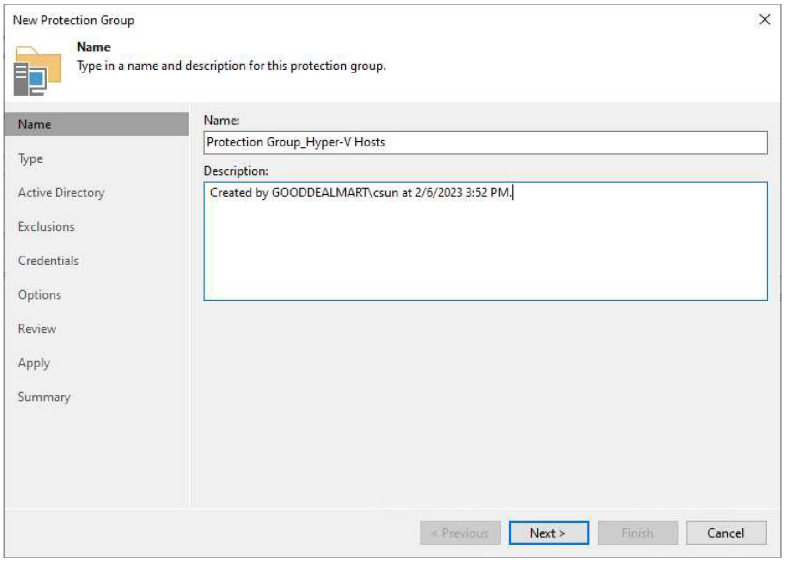
Create Job or Policy

Agent-based protection provides additional flexibility with two deployment approaches. For 24/7 workloads such as servers and failover clusters, we recommend that you create backup jobs managed by the backup server, which controls scheduling and executes backup remotely. For any workloads which may remain offline or unreachable for extended and/or unpredictable time periods (such as workstations, laptops or remote office servers), we recommend that you create backup policy that configures backup agents to schedule and execute backup independently.

Perform Restore

To perform Bare Metal Recovery to the existing or new hardware, please use the Veeam Recovery Media that can be created directly from the backup file of the corresponding computer. Other entire computer restore options include direct restore to Microsoft Azure, or instant recovery into a Microsoft Hyper-V VM. To perform granular recovery such as file or application item restore, simply select the desired backup under the Backups tree of the Home tab, and select one of many restore options provided.

5. On the Name page, specify a protection group name.
6. Give a brief description in the Description field for future reference and click Next.



Name

Type in a name and description for this protection group.

Name: Protection Group_Hyper-V Hosts

Description: Created by GOODDEALMART\csun at 2/6/2023 3:52 PM.

7. Select Specify protection scope for the created protection group on the Type page and click Next.

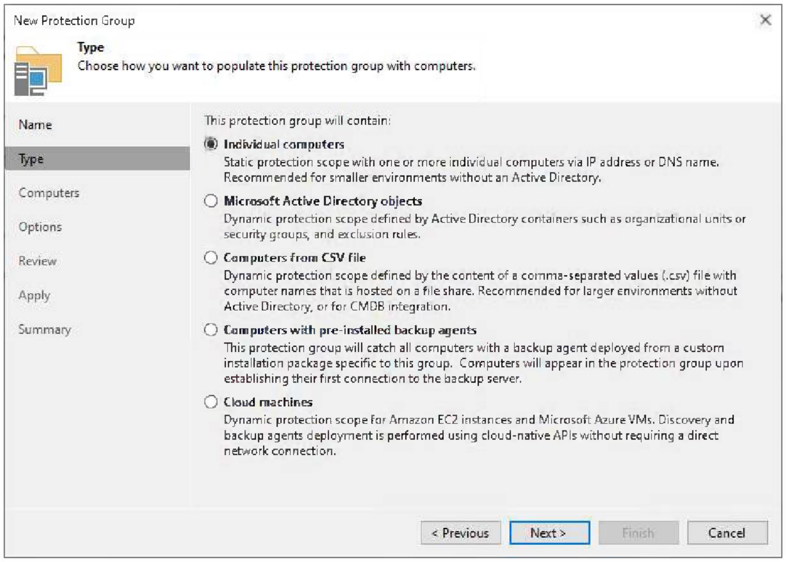
    - Individual computers: add specific computers to the protection group.

    - Microsoft Active Directory objects: select this option to add one or several Active Directory objects to the protection group.

    - Computers from CSV file: add to the protection scope computers listed in a CSV file.

    - Computers with pre-installed agents: create a protection group for pre-installed Veeam Agents.

    - Cloud machines: select this option to add Amazon EC2 instances or



Type

Choose how you want to populate this protection group with computers.

This protection group will contain:

● **Individual computers**
Static protection scope with one or more individual computers via IP address or DNS name. Recommended for smaller environments without an Active Directory.

○ **Microsoft Active Directory objects**
Dynamic protection scope defined by Active Directory containers such as organizational units or security groups, and exclusion rules.

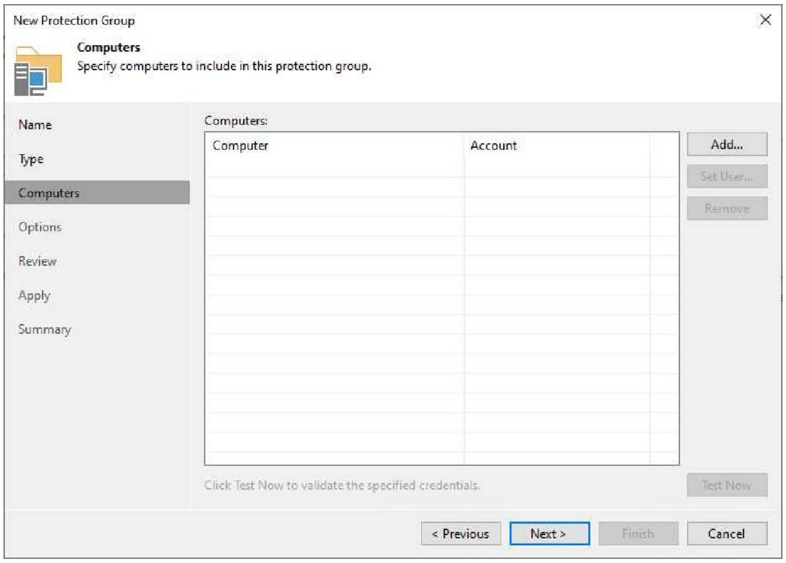
○ **Computers from CSV file**
Dynamic protection scope defined by the content of a comma-separated values (.csv) file with computer names that is hosted on a file share. Recommended for larger environments without Active Directory, or for CMDB integration.

○ **Computers with pre-installed backup agents**
This protection group will catch all computers with a backup agent deployed from a custom installation package specific to this group. Computers will appear in the protection group upon establishing their first connection to the backup server.

○ **Cloud machines**
Dynamic protection scope for Amazon EC2 instances and Microsoft Azure VMs. Discovery and backup agents deployment is performed using cloud-native APIs without requiring a direct network connection.

Microsoft Azure virtual machines.

8. Click Add on the Computers page.



Specify computers to include in this protection group.

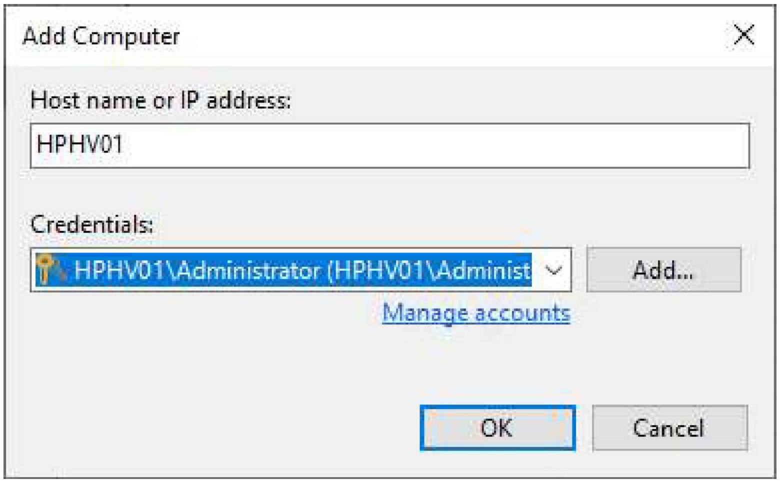
Computers:

Click Test Now to validate the specified credentials.

9. Specify a DNS name or IP address on the Add Computer page.

10. From the Credentials list, select a user account with administrative permissions on the computer and click OK.

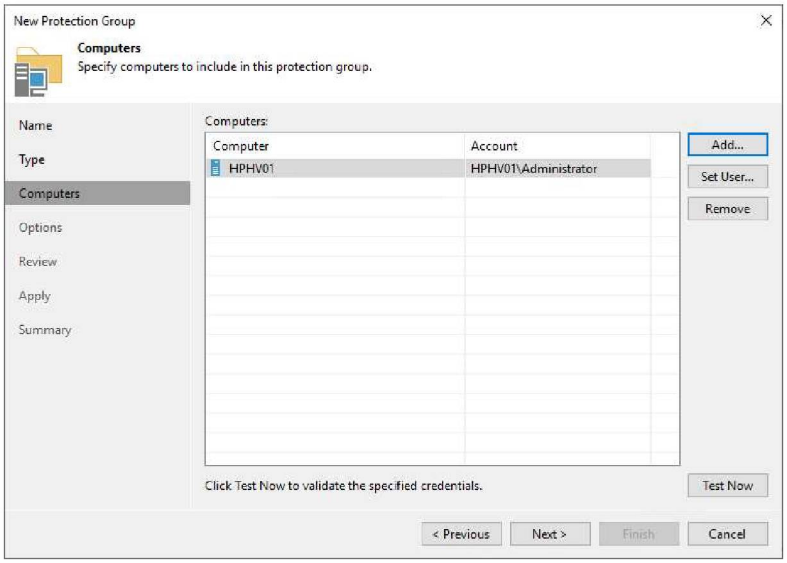
11. If you need to set up credentials beforehand, click the Manage accounts link or Add on the right.



Host name or IP address: HPHV01

Credentials: HPHV01\Administrator (HPHV01\Administ

12. Click Test Now on the Computers page.

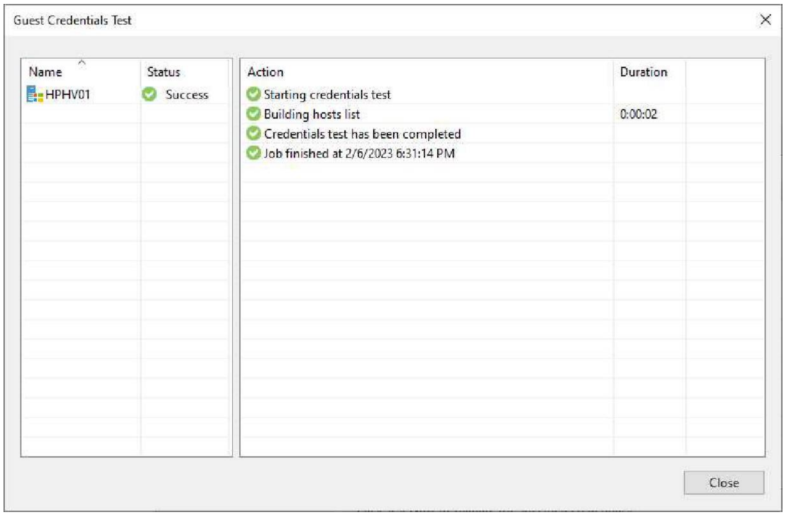


Computers
Specify computers to include in this protection group.

Computer	Account
HPHV01	HPHV01\Administrator

Click Test Now to validate the specified credentials.

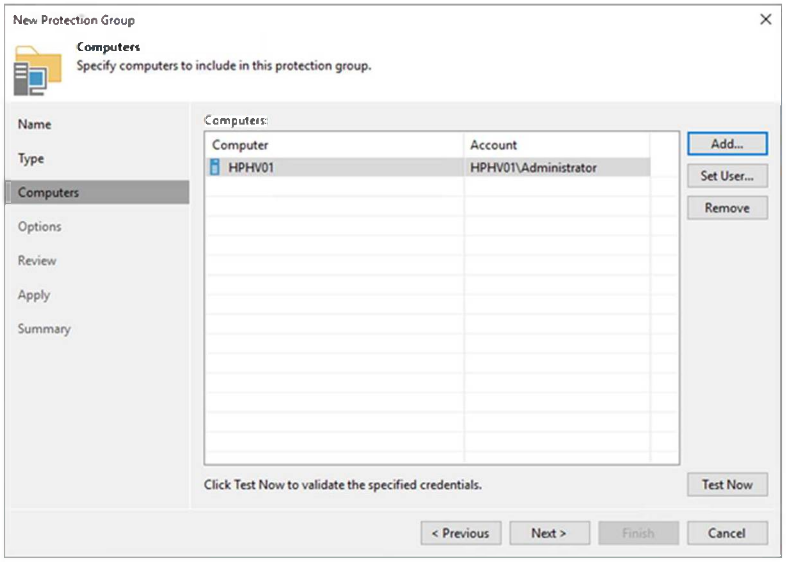
13. On the Guest Credentials Test page and click Close.



Name	Status
HPHV01	Success

Action	Duration
Starting credentials test	
Building hosts list	0:00:02
Credentials test has been completed	
Job finished at 2/6/2023 6:31:14 PM	

14. Click Next on the Computers page.



New Protection Group

Computers
Specify computers to include in this protection group.

Computers:

Computer	Account
HPHV01	HPHV01\Administrator

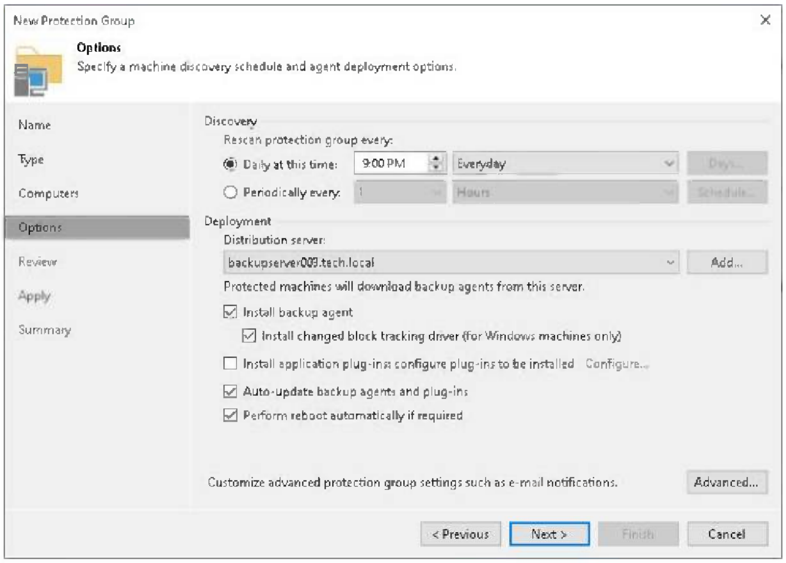
Click Test Now to validate the specified credentials.

15. On the Options page, in the Discovery section, define the schedule for automatic computer discovery within the scope of the protection group.

16. In the Deployment section, select a Microsoft Windows server from the Distribution server list to serve as a distribution server.

17. Select the Install Backup agent checkbox.

18. Select the Install changed block tracking driver (for



New Protection Group

Options
Specify a machine discovery schedule and agent deployment options.

Discovery
Rescan protection group every:
● Daily at this time: 9:00 PM Everyday
○ Periodically every: 1 Hours

Deployment
Distribution server:
backupserver009.tech.local
Protected machines will download backup agents from this server.
☑ Install backup agent
☑ Install changed block tracking driver (for Windows machines only)
☐ Install application plug-ins: configure plug-ins to be installed Configure...
☑ Auto-update backup agents and plug-ins
☑ Perform reboot automatically if required

Customize advanced protection group settings such as e-mail notifications.

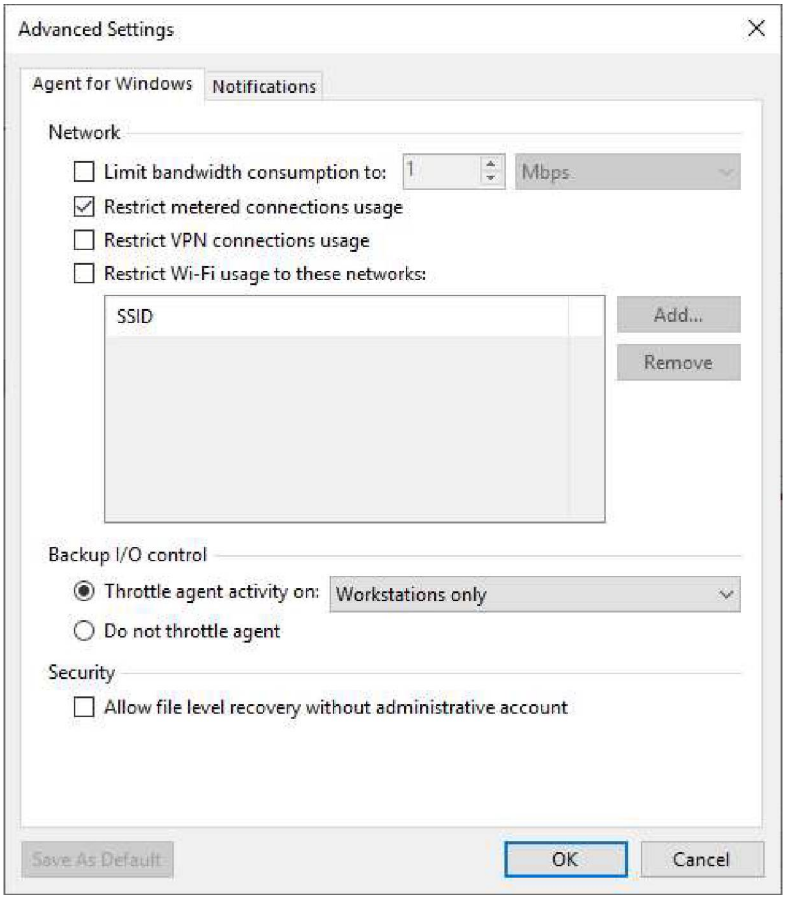
Windows machines only) checkbox.

19. Click Advanced to customize advanced protection group settings.

20. On the Advanced Settings page, specify the below settings that will be deployed on computers included in the protection group and click OK.

    - Limiting bandwidth consumption: specify the maximum speed for transferring backed-up data from the Veeam Agent computer to the target location.

    - Restrict metered connections usage: Veeam Agent automatically detects metered connections and does not perform backup when



Network

☐ Limit bandwidth consumption to: 1 Mbps

☑ Restrict metered connections usage

☐ Restrict VPN connections usage

☐ Restrict Wi-Fi usage to these networks:

Backup I/O control

● Throttle agent activity on: Workstations only

○ Do not throttle agent

Security

☐ Allow file level recovery without administrative account your computer is on such connection.

- Restrict VPN connection usage: Veeam Agent for Microsoft Windows will automatically detect a VPN connection and not perform a backup when the Veeam Agent computer is on such a connection.
- Restrict Wi-Fi usage to these networks: restrict usage of wireless networks for Veeam Agent running on Microsoft Windows workstations.

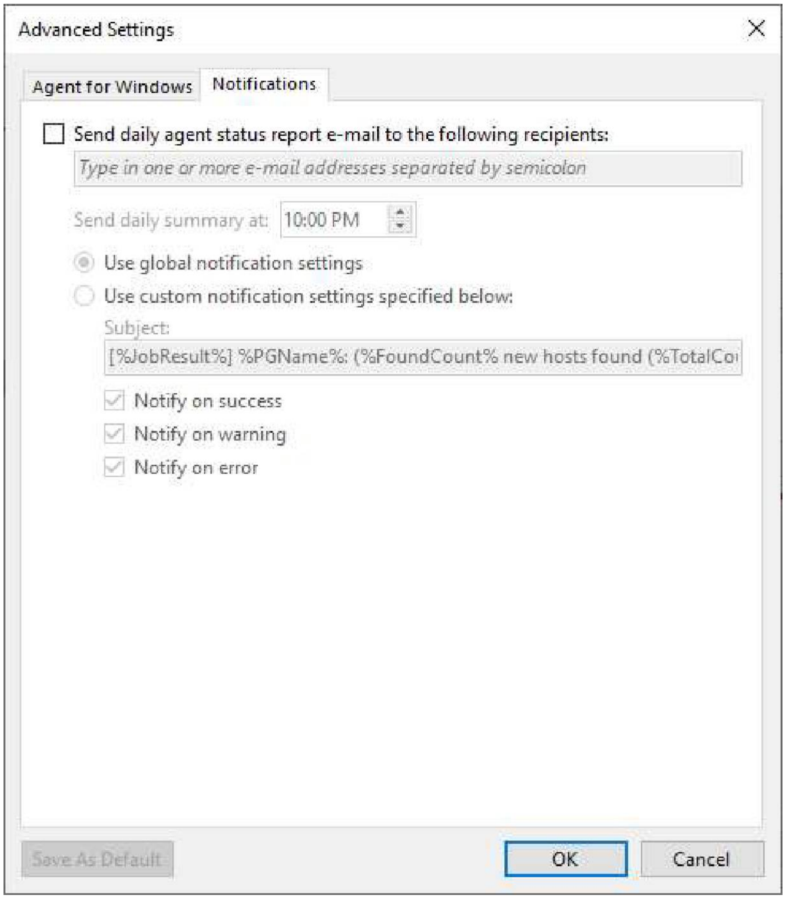
21. Backup I/O settings: You can instruct Veeam Agent for Microsoft Windows to throttle its activities during backup.

    - Throttle agent activity on the

type of computers to throttle Veeam Agent backup activities: Workstations, Servers, or All hosts.

22. Security settings: You can allow user accounts that do not have administrative privileges on a Veeam Agent computer to perform a file-level restore on this computer.

23. On the Advanced page, select Notifications.



Advanced Settings

□ Send daily agent status report e-mail to the following recipients:

Type in one or more e-mail addresses separated by semicolon

Send daily summary at: 10:00 PM

● Use global notification settings

○ Use custom notification settings specified below:

Subject:

[%JobResult%] %PGName%: (%FoundCount% new hosts found (%TotalCo

☑ Notify on success

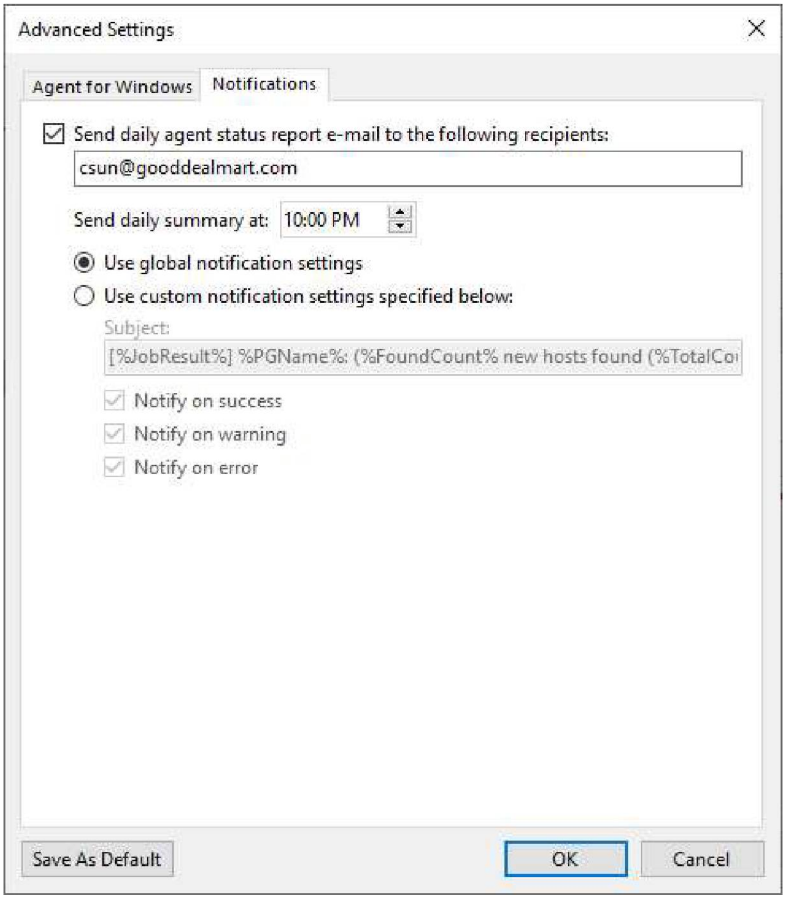
☑ Notify on warning

☑ Notify on error

24. On the Notification page, select Send daily agent status report e-mail to the following recipients: checkbox and enter an email address.

25. Enter several addresses separated by a semicolon.

26. You can use global notification settings or specify custom notification settings and click OK.



☑ Send daily agent status report e-mail to the following recipients:

csun@gooddealmart.com

Send daily summary at: 10:00 PM

● Use global notification settings

○ Use custom notification settings specified below:

Subject:

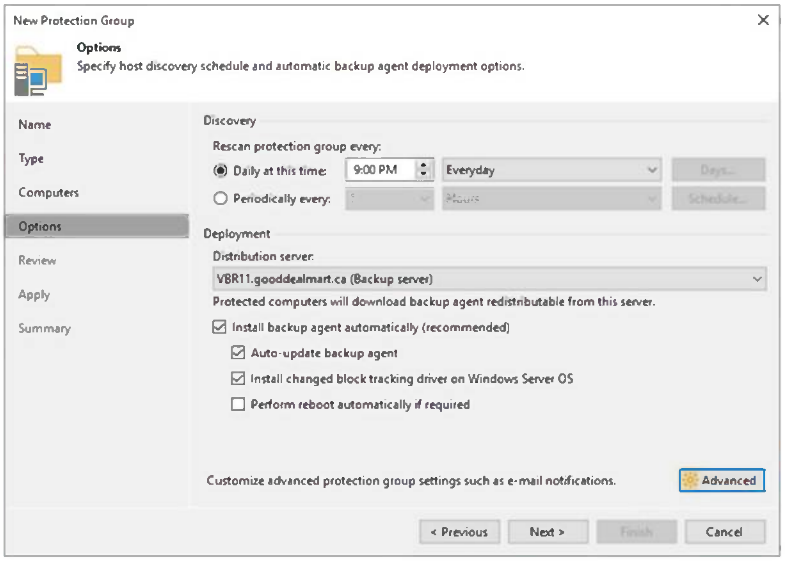
[%JobResult%] %PGName%: (%FoundCount% new hosts found (%TotalCo

☑ Notify on success

☑ Notify on warning

☑ Notify on error

27. On the Options page, click Next.



New Protection Group

Options

Specify host discovery schedule and automatic backup agent deployment options.

Discovery

Rescan protection group every:

● Daily at this time: 9:00 PM Everyday

○ Periodically every:

Deployment

Distribution server:

VBR11.gooddealmart.ca (Backup server)

Protected computers will download backup agent redistributable from this server.

☑ Install backup agent automatically (recommended)

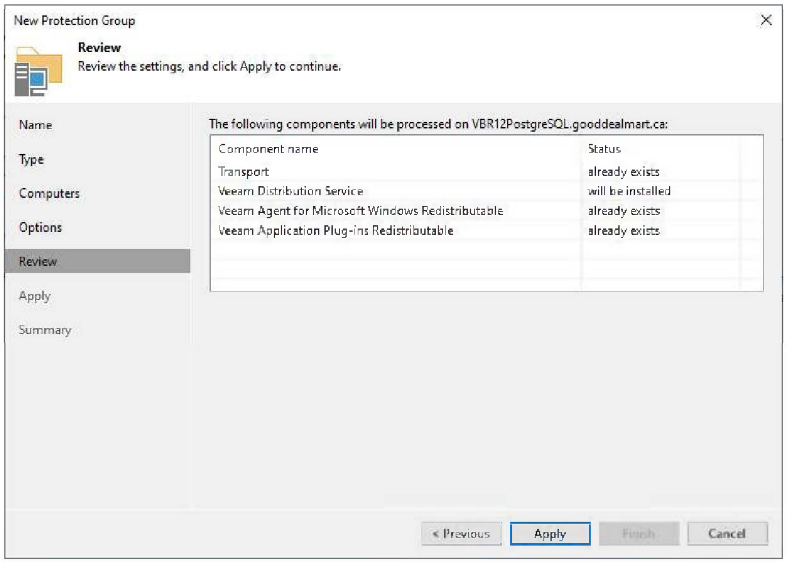
☑ Auto-update backup agent

☑ Install changed block tracking driver on Windows Server OS

☐ Perform reboot automatically if required

Customize advanced protection group settings such as e-mail notifications.

28. On the Review page, click Apply.



New Protection Group

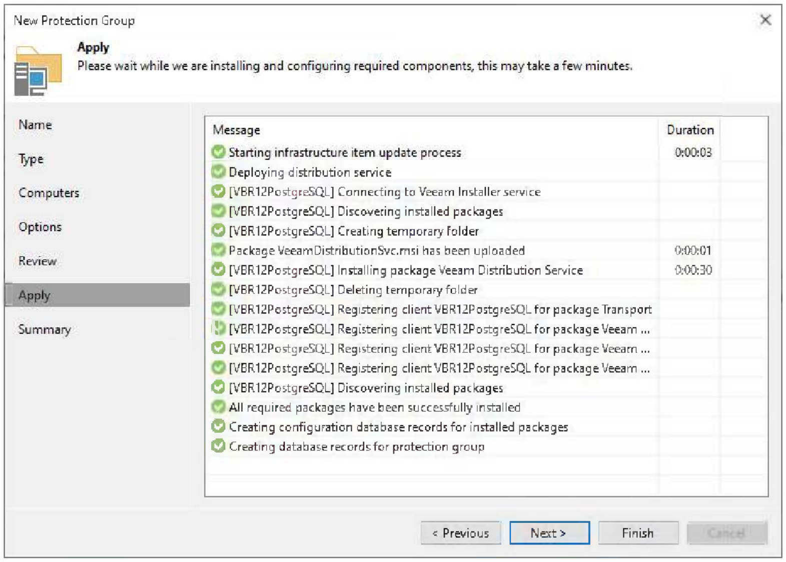
Review

Review the settings, and click Apply to continue.

The following components will be processed on VBR12PostgreSQL.gooddealmart.ca:

Component name	Status
Transport	already exists
Veeam Distribution Service	will be installed
Veeam Agent for Microsoft Windows Redistributable	already exists
Veeam Application Plug-ins Redistributable	already exists

29. Click Next on the Apply page.

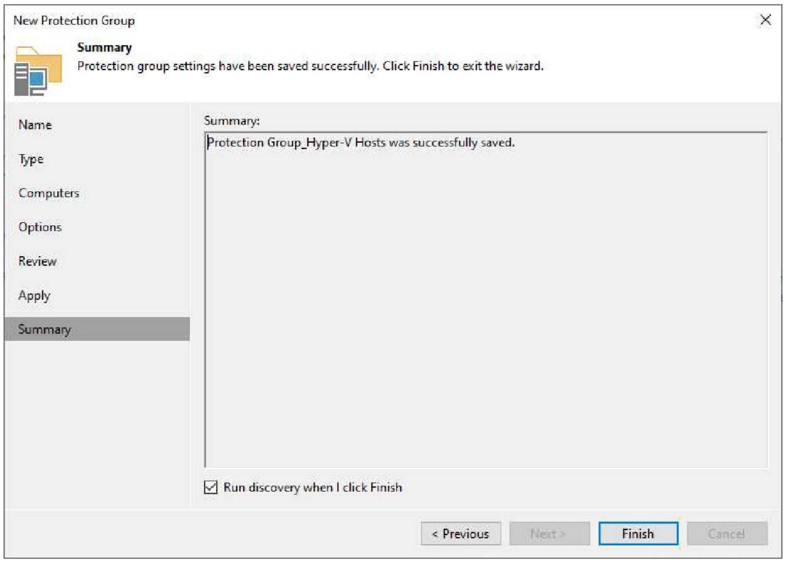


Apply

Please wait while we are installing and configuring required components, this may take a few minutes.

```
Message                                                                          Duration
Starting infrastructure item update process                                      0:00:03
Deploying distribution service
[VBR12PostgreSQL] Connecting to Veeam Installer service
[VBR12PostgreSQL] Discovering installed packages
[VBR12PostgreSQL] Creating temporary folder
Package VeeamDistributionSvc.msi has been uploaded                               0:00:01
[VBR12PostgreSQL] Installing package Veeam Distribution Service                  0:00:30
[VBR12PostgreSQL] Deleting temporary folder
[VBR12PostgreSQL] Registering client VBR12PostgreSQL for package Transport
[VBR12PostgreSQL] Registering client VBR12PostgreSQL for package Veeam ...
[VBR12PostgreSQL] Registering client VBR12PostgreSQL for package Veeam ...
[VBR12PostgreSQL] Registering client VBR12PostgreSQL for package Veeam ...
[VBR12PostgreSQL] Discovering installed packages
All required packages have been successfully installed
Creating configuration database records for installed packages
Creating database records for protection group
```

30. On the Summary page, select Run discovery when I click the Finish checkbox and click Finish.



Summary

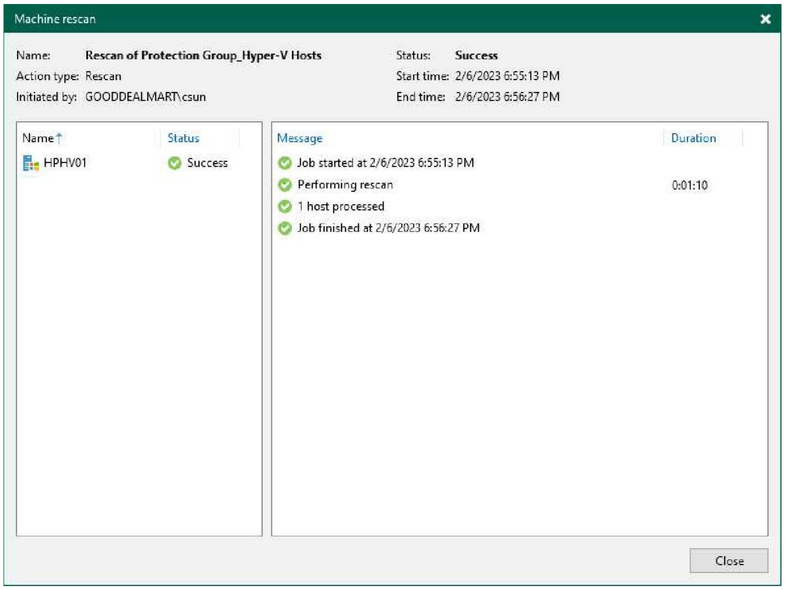
Protection group settings have been saved successfully. Click Finish to exit the wizard.

Summary:

Protection Group_Hyper-V Hosts was successfully saved.

☑ Run discovery when I click Finish

31. Ensure the operation is complete without error on the Agents discovery session page.



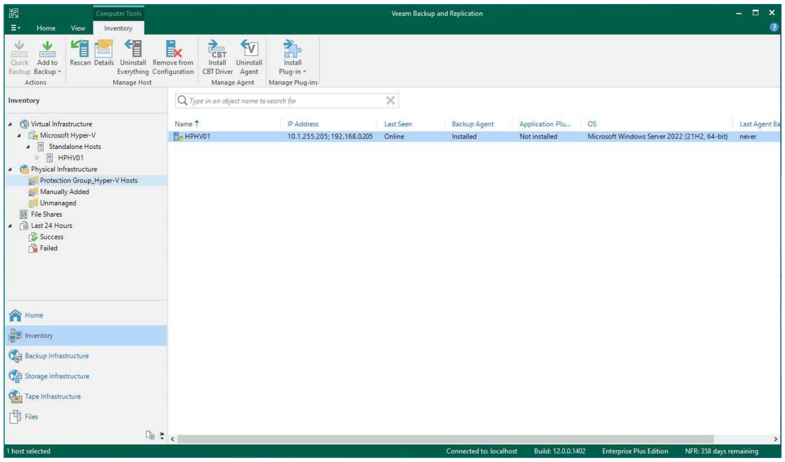
Name: Rescan of Protection Group_Hyper-V Hosts
Action type: Rescan
Initiated by: GOODDEALMART\csun

Status: Success
Start time: 2/6/2023 6:55:13 PM
End time: 2/6/2023 6:56:27 PM

Name	Status
HPHV01	Success

Message	Duration
Job started at 2/6/2023 6:55:13 PM	
Performing rescan	0:01:10
1 host processed	
Job finished at 2/6/2023 6:56:27 PM	

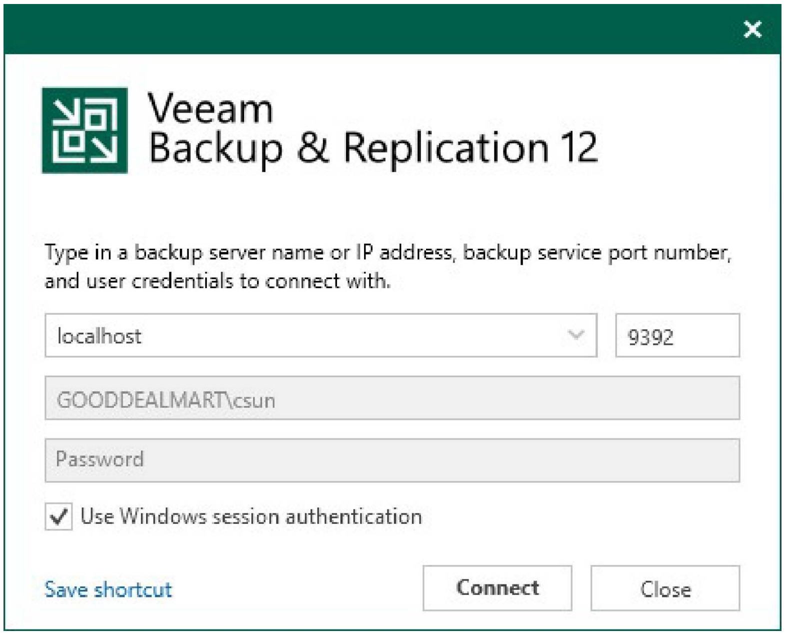
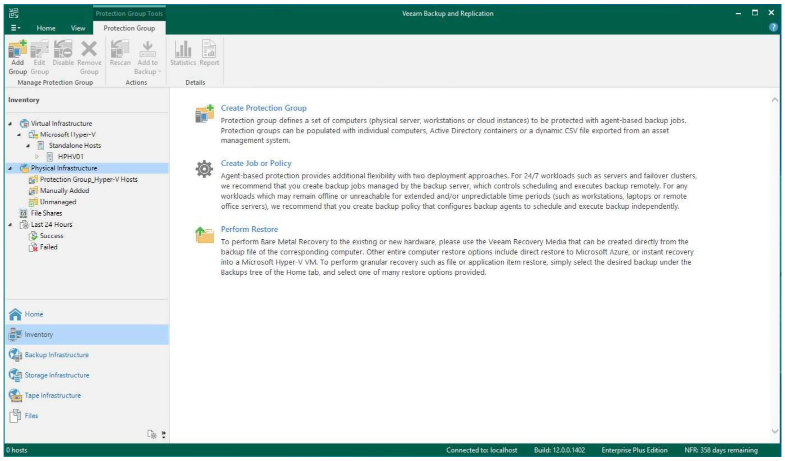
32. Verify that the protection group has been added.



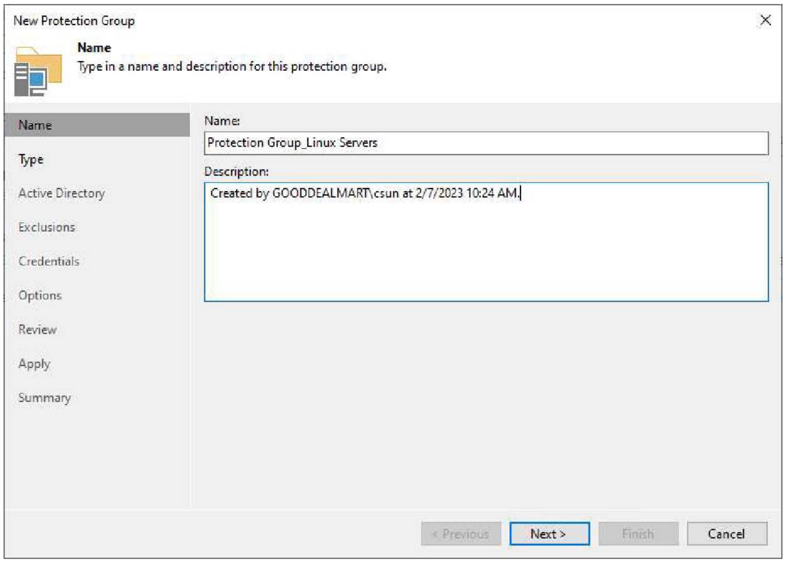
Name	IP Address	Last Seen	Backup Agent	Application Plu...	OS	Last Agent Ba
HPHV01	10.1.255.205; 192.168.0.205	Online	Installed	Not installed	Microsoft Windows Server 2022 (21H2, 64-bit)	never

Add Veeam Agent to On-Premises Linux Physical machines

You can back up and restore the On-Premises physical machines running Linux operating systems. Backup agents are installed on each computer by Veeam Backup & Replication.

Instructions	Screenshot (if applicable)
1. Log in to the Veeam Backup and replication manager server. 2. Open the Veeam Backup & Replication Console, and click Connect.	 Veeam Backup & Replication 12 Save shortcut Connect Close Type in a backup server name or IP address, backup service port number, and user credentials to connect with. localhost 9392 GOODDEALMART\csun Password ☑ Use Windows session authentication
3. Select Inventory on the Home page. 4. On the Inventory page, select Physical Infrastructure and click Create Protection Group.	 Protection Group Tools Veeam Backup and Replication Home View Protection Group Add Group Edit Group Disable Remove Group Manage Protection Group Rescan Add to Backup Actions Statistics Report Details Inventory Virtual Infrastructure Microsoft Hyper-V Standalone Hosts HPHV01 Physical Infrastructure Protection Group_Hyper-V Hosts Manually Added Unmanaged File Shares Last 24 Hours Success Failed Home Inventory Backup Infrastructure Storage Infrastructure Tape Infrastructure Files Create Protection Group Protection group defines a set of computers (physical server, workstations or cloud instances) to be protected with agent-based backup jobs. Protection groups can be populated with individual computers, Active Directory containers or a dynamic CSV file exported from an asset management system. Create Job or Policy Agent-based protection provides additional flexibility with two deployment approaches. For 24/7 workloads such as servers and failover clusters, we recommend that you create backup jobs managed by the backup server, which controls scheduling and executes backup remotely. For any workloads which may remain offline or unreachable for extended and/or unpredictable time periods (such as workstations, laptops or remote office servers), we recommend that you create backup policy that configures backup agents to schedule and execute backup independently. Perform Restore To perform Bare Metal Recovery to the existing or new hardware, please use the Veeam Recovery Media that can be created directly from the backup file of the corresponding computer. Other entire computer restore options include direct restore to Microsoft Azure, or instant recovery into a Microsoft Hyper-V VM. To perform granular recovery such as file or application item restore, simply select the desired backup under the Backups tree of the Home tab, and select one of many restore options provided. 0 hosts Connected to: localhost Build: 12.0.0.1402 Enterprise Plus Edition NFR: 358 days remaining

5. On the Name page, specify a protection group name.
6. Give a brief description in the Description field for future reference and click Next.
7. Select Specify protection scope for the created protection group on the Type page and click Next.
   - Individual computers: add specific computers to the protection group.
   - Microsoft Active Directory objects: select this option to add one or several Active Directory objects to the protection group.
   - Computers from CSV file: add to the protection scope computers listed in a CSV file.
   - Computers with pre-installed agents: create a protection group for pre-installed Veeam Agents.
   - Cloud machines: select this option to add Amazon



New Protection Group

Name

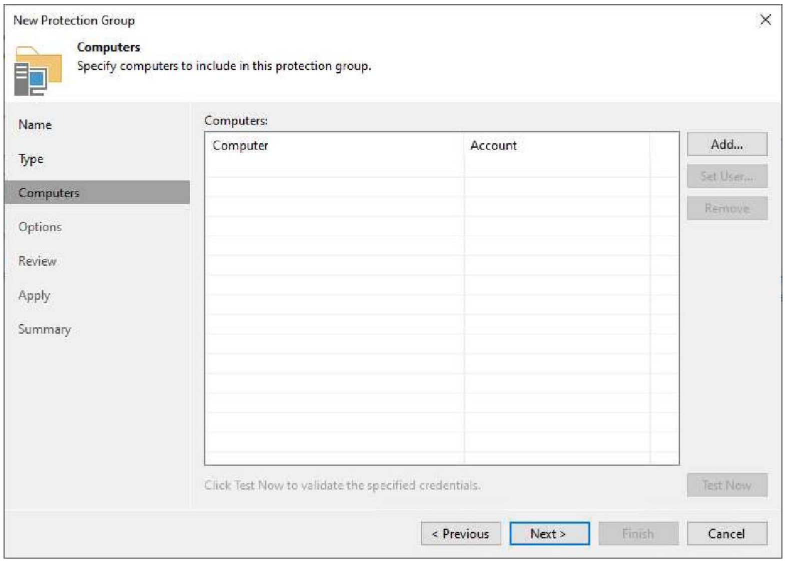
Type in a name and description for this protection group.

Name: Protection Group_Linux Servers

Description: Created by GOODDEALMART\csun at 2/7/2023 10:24 AM.

EC2 instances or
Microsoft Azure
virtual machines.

8. Click Add on the Computers page.



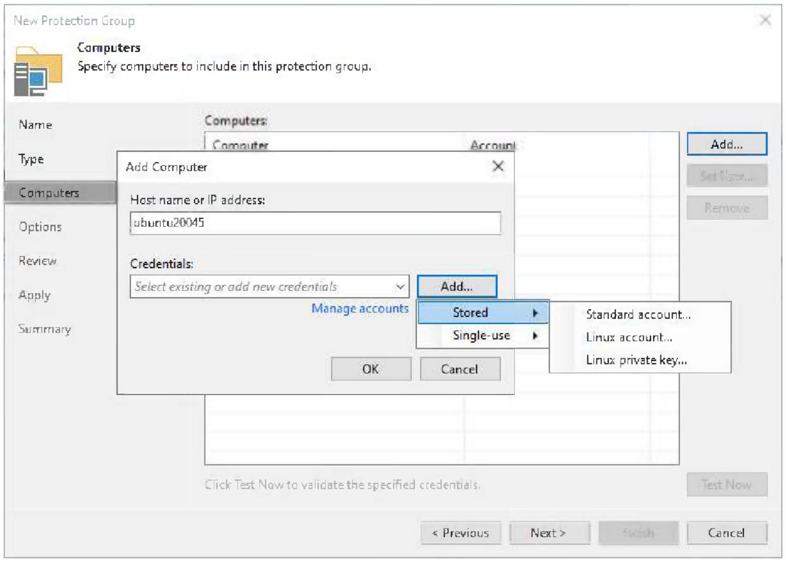
New Protection Group

Computers

Specify computers to include in this protection group.

Click Test Now to validate the specified credentials.

9. Specify a DNS name or IP address on the Add Computer page.
10. From the Credentials list, select a user account with administrative permissions on the computer and click OK.
11. If you need to set up credentials beforehand, click the Manage accounts link or Add on the right.
12. Click Add in the Credentials field, select Stored and click Linux account.



New Protection Group

Computers

Specify computers to include in this protection group.

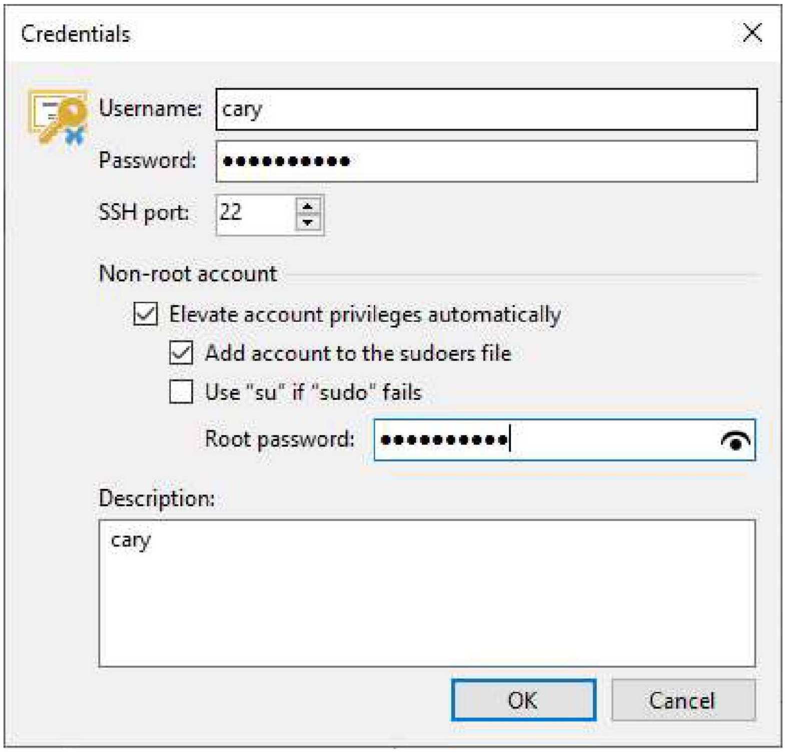
Add Computer

Host name or IP address: ubuntu20045

Credentials: Select existing or add new credentials

Click Test Now to validate the specified credentials.

13. On the Credentials page, Enter a user name in the Username field.
14. Enter a password in the Password field.
15. Enter 22 in the SSH port field.
16. Select the Elvate account privileges automatically checkbox for a non-root user with root account privileges.
17. Select Add account to the sudoers file checkbox.
18. Enter the password in the Root password field.
19. Give a brief description in the Description field for future reference and click OK.



Credentials

Username: cary

Password: ●●●●●●●●●●

SSH port: 22

Non-root account

☑ Elevate account privileges automatically

☑ Add account to the sudoers file

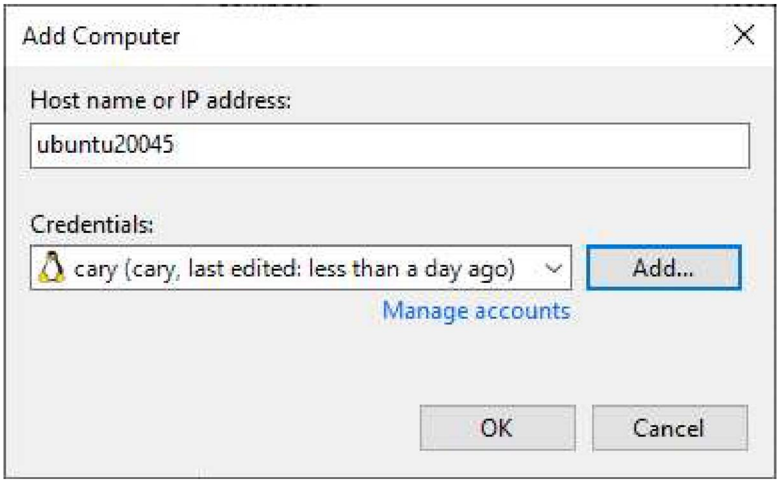
☐ Use "su" if "sudo" fails

Root password: ●●●●●●●●●●

Description:

cary

20. Click OK on the add Computer page.



Add Computer

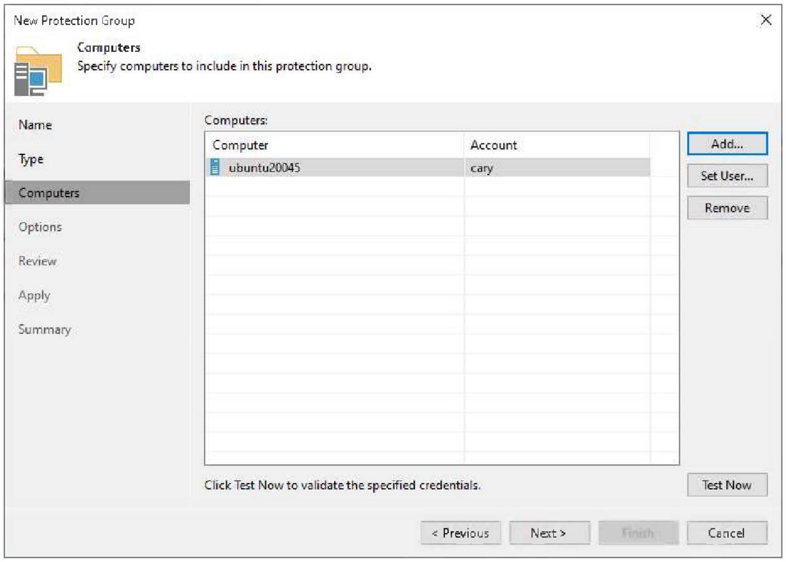
Host name or IP address:

ubuntu20045

Credentials:

cary (cary, last edited: less than a day ago)

21. Click Test Now on the Computers page.



New Protection Group

Computers

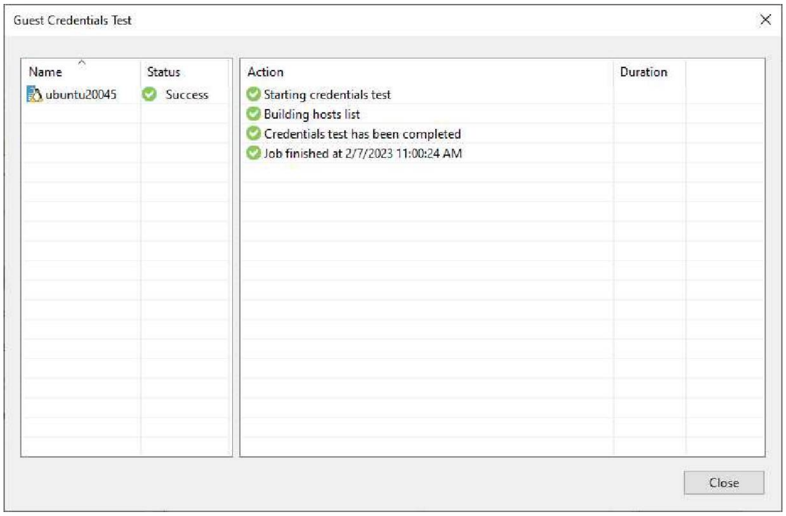
Specify computers to include in this protection group.

Computers:

Computer	Account
ubuntu20045	cary

Click Test Now to validate the specified credentials.

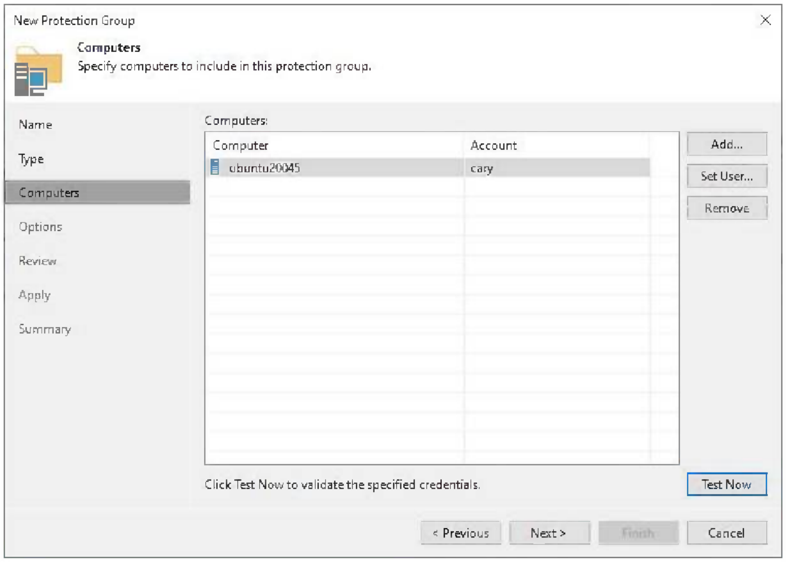
22. On the Guest Credentials Test page and click Close.



Guest Credentials Test

Name	Status	Action	Duration
ubuntu20045	✓ Success	✓ Starting credentials test	
		✓ Building hosts list	
		✓ Credentials test has been completed	
		✓ Job finished at 2/7/2023 11:00:24 AM	

23. Click Next on the Computers page.



New Protection Group

Computers
Specify computers to include in this protection group.

Name
Type
Computers
Options
Review
Apply
Summary

Computers:

Computer	Account
ubuntu20045	cary

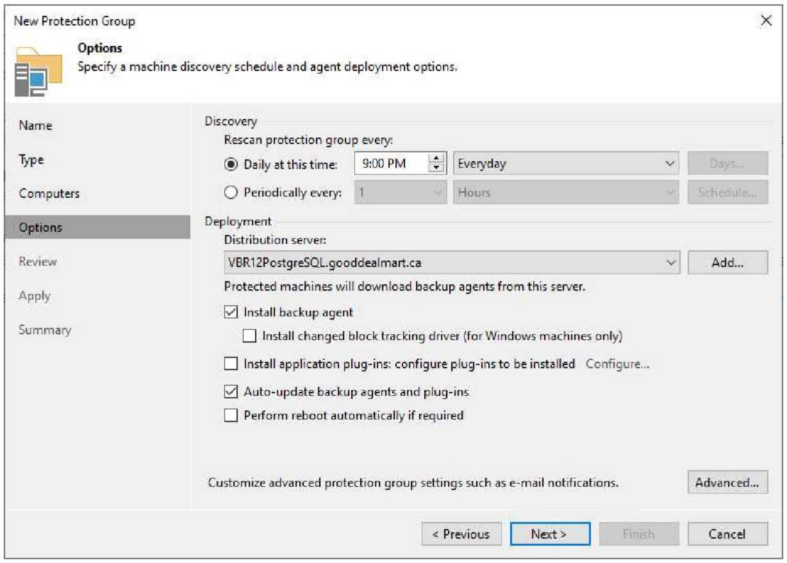
Add...
Set User...
Remove

Click Test Now to validate the specified credentials.

Test Now

< Previous   Next >   Finish   Cancel

24. On the Options page, in the Discovery section, define the schedule for automatic computer discovery within the scope of the protection group.
25. In the Deployment section, select a Microsoft Windows server from the Distribution server list to serve as a distribution server.
26. Select the Install Backup agent checkbox.
27. Click Advanced to customize advanced protection group settings.



New Protection Group

Options
Specify a machine discovery schedule and agent deployment options.

Name
Type
Computers
Options
Review
Apply
Summary

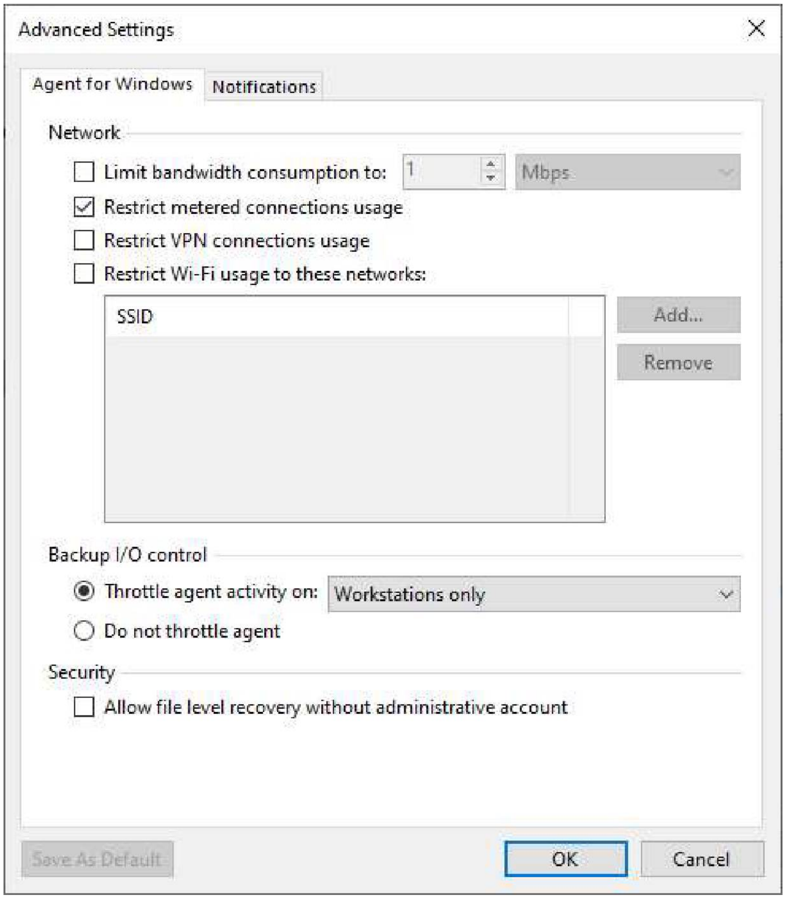
Discovery
Rescan protection group every:
● Daily at this time: 9:00 PM   Everyday   Days...
○ Periodically every: 1   Hours   Schedule...

Deployment
Distribution server:
VBR12PostgreSQL.gooddealmart.ca   Add...
Protected machines will download backup agents from this server.
☑ Install backup agent
□ Install changed block tracking driver (for Windows machines only)
□ Install application plug-ins: configure plug-ins to be installed Configure...
☑ Auto-update backup agents and plug-ins
□ Perform reboot automatically if required

Customize advanced protection group settings such as e-mail notifications.   Advanced...

< Previous   Next >   Finish   Cancel

28. On the Advanced Settings page, specify the below settings that will be deployed on computers included in the protection group and click OK.



Advanced Settings

Agent for Windows | Notifications

Network

□ Limit bandwidth consumption to: 1 Mbps

☑ Restrict metered connections usage

□ Restrict VPN connections usage

□ Restrict Wi-Fi usage to these networks:

SSID

Backup I/O control

● Throttle agent activity on: Workstations only

○ Do not throttle agent

Security

□ Allow file level recovery without administrative account

- Limiting bandwidth consumption: specify the maximum speed for transferring backed-up data from the Veeam Agent computer to the target location.

- Restrict metered connections usage: Veeam Agent automatically detects metered connections and does not perform backup when your computer is on such connection.

- Restrict VPN connection usage: Veeam Agent for Microsoft Windows will automatically detect a VPN connection and not perform a backup when the Veeam Agent computer is on such a connection.

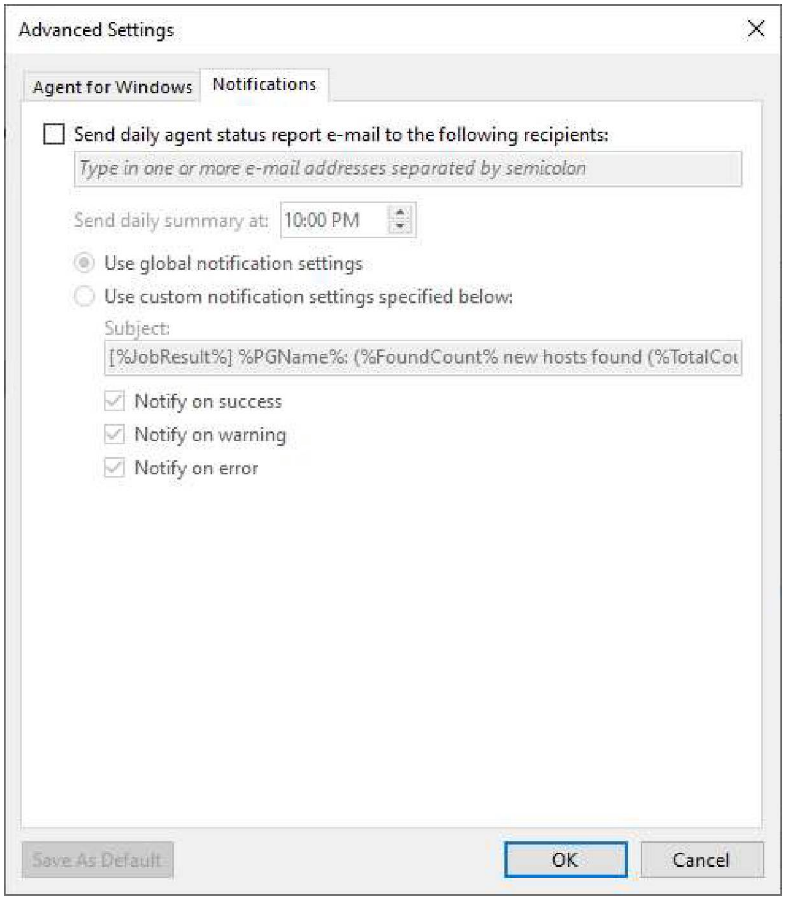
- Restrict Wi-Fi usage to these networks: restrict usage of wireless networks for Veeam Agent running on Microsoft Windows workstations.

29. Backup I/O settings: You can instruct Veeam Agent for Microsoft Windows to throttle its activities during backup.

    - Throttle agent activity on the type of computers to throttle Veeam Agent backup activities: Workstations, Servers, or All hosts.

30. Security settings: You can allow user accounts that do not have administrative privileges on a Veeam Agent computer to perform a file-level restore on this computer.

31. On the Advanced page, select Notifications.



□ Send daily agent status report e-mail to the following recipients:

Type in one or more e-mail addresses separated by semicolon

Send daily summary at: 10:00 PM

● Use global notification settings

○ Use custom notification settings specified below:

Subject:

[%JobResult%] %PGName%: (%FoundCount% new hosts found (%TotalCo

☑ Notify on success

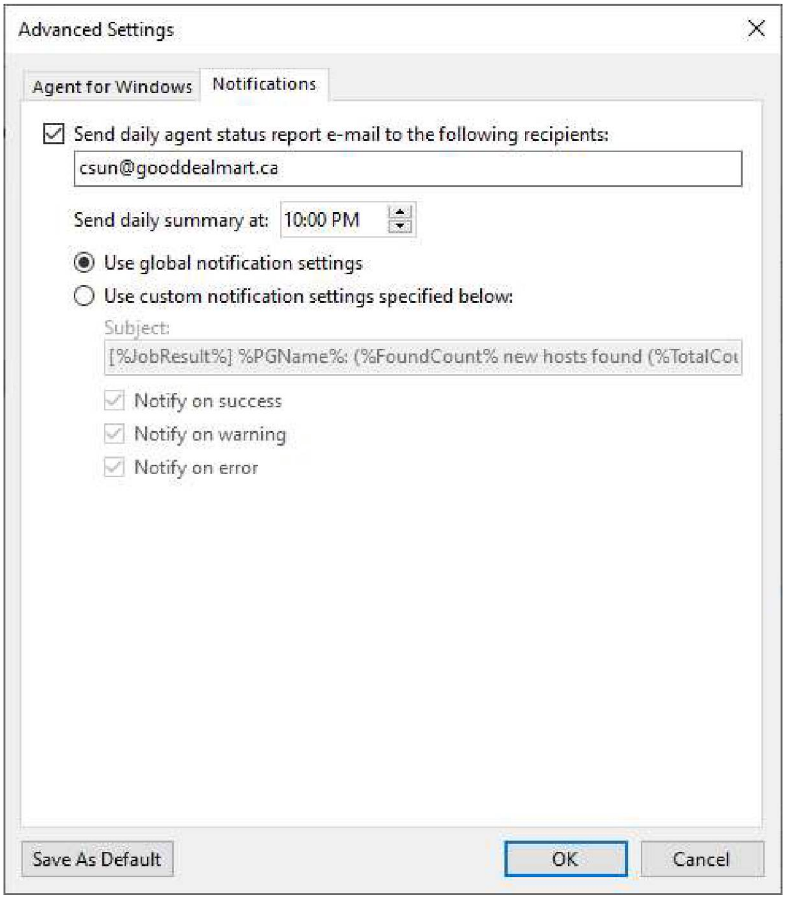
☑ Notify on warning

☑ Notify on error

32. On the Notification page, select Send daily agent status report e-mail to the following recipients: checkbox and enter an email address.

33. Enter several addresses separated by a semicolon.

34. You can use global notification settings or specify custom notification settings and click OK.



☑ Send daily agent status report e-mail to the following recipients:

csun@gooddealmart.ca

Send daily summary at: 10:00 PM

● Use global notification settings

○ Use custom notification settings specified below:

Subject:

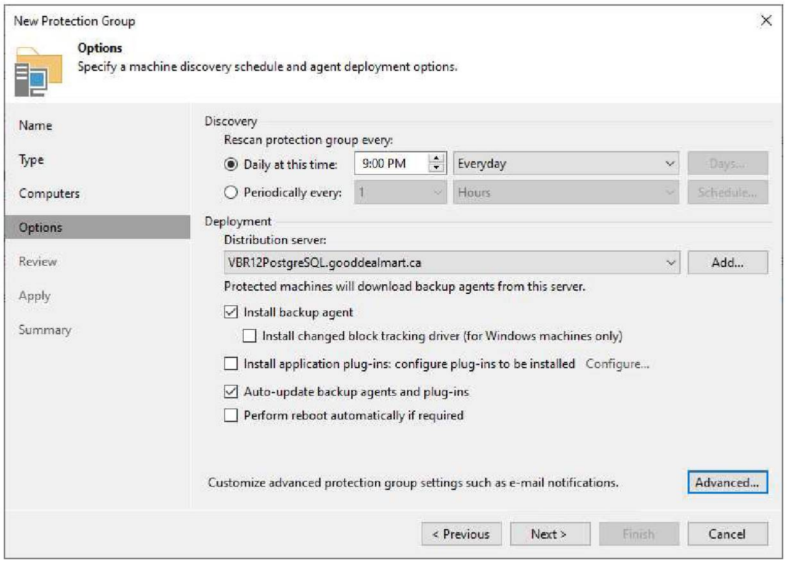
[%JobResult%] %PGName%: (%FoundCount% new hosts found (%TotalCo

☑ Notify on success

☑ Notify on warning

☑ Notify on error

35. On the Options page, click Next.



New Protection Group

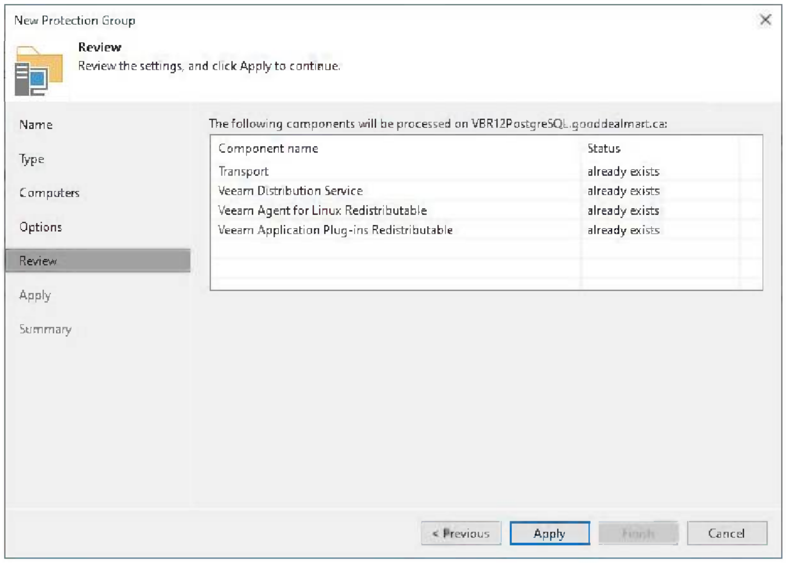
Options
Specify a machine discovery schedule and agent deployment options.

Discovery
Rescan protection group every:
● Daily at this time: 9:00 PM Everyday
○ Periodically every: 1 Hours

Deployment
Distribution server:
VBR12PostgreSQL.gooddealmart.ca
Protected machines will download backup agents from this server.
☑ Install backup agent
□ Install changed block tracking driver (for Windows machines only)
□ Install application plug-ins: configure plug-ins to be installed Configure...
☑ Auto-update backup agents and plug-ins
□ Perform reboot automatically if required

Customize advanced protection group settings such as e-mail notifications.

36. Click Apply on the Review page.



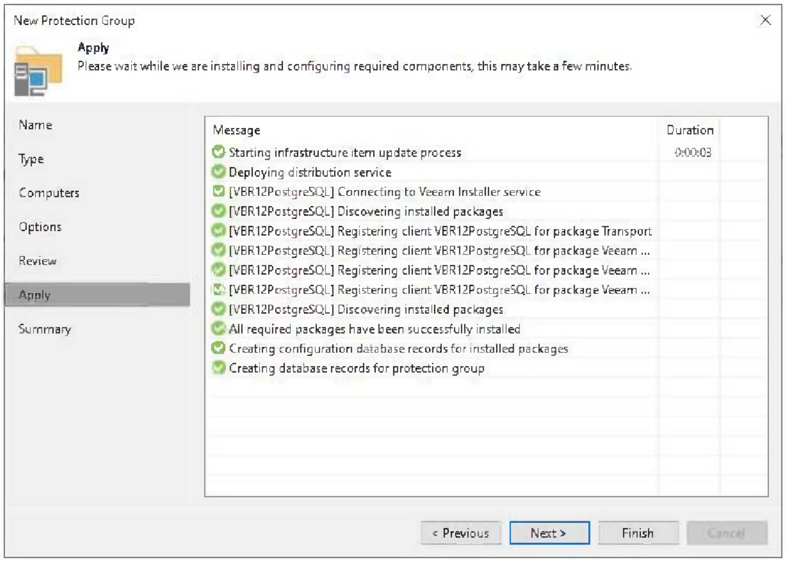
New Protection Group

Review
Review the settings, and click Apply to continue.

The following components will be processed on VBR12PostgreSQL.gooddealmart.ca:

Component name	Status
Transport	already exists
Veeam Distribution Service	already exists
Veeam Agent for Linux Redistributable	already exists
Veeam Application Plug-ins Redistributable	already exists

37. Click Next on the Apply page.



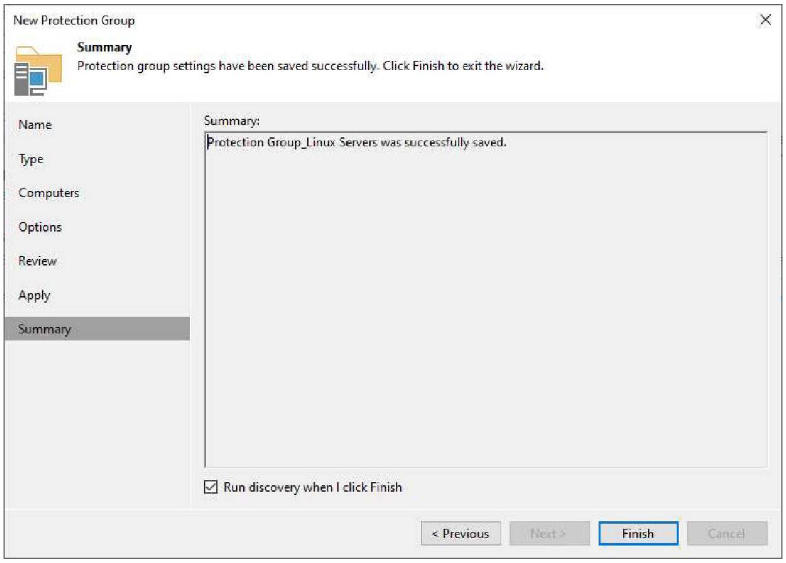
New Protection Group

Apply

Please wait while we are installing and configuring required components, this may take a few minutes.

Message	Duration
✓ Starting infrastructure item update process	0:00:03
✓ Deploying distribution service	
✓ [VBR12PostgreSQL] Connecting to Veeam Installer service	
✓ [VBR12PostgreSQL] Discovering installed packages	
✓ [VBR12PostgreSQL] Registering client VBR12PostgreSQL for package Transport	
✓ [VBR12PostgreSQL] Registering client VBR12PostgreSQL for package Veeam ...	
✓ [VBR12PostgreSQL] Registering client VBR12PostgreSQL for package Veeam ...	
✓ [VBR12PostgreSQL] Registering client VBR12PostgreSQL for package Veeam ...	
✓ [VBR12PostgreSQL] Discovering installed packages	
✓ All required packages have been successfully installed	
✓ Creating configuration database records for installed packages	
✓ Creating database records for protection group	

38. On the Summary page, select the Run discovery when I click the Finish checkbox and click Finish.



New Protection Group

Summary

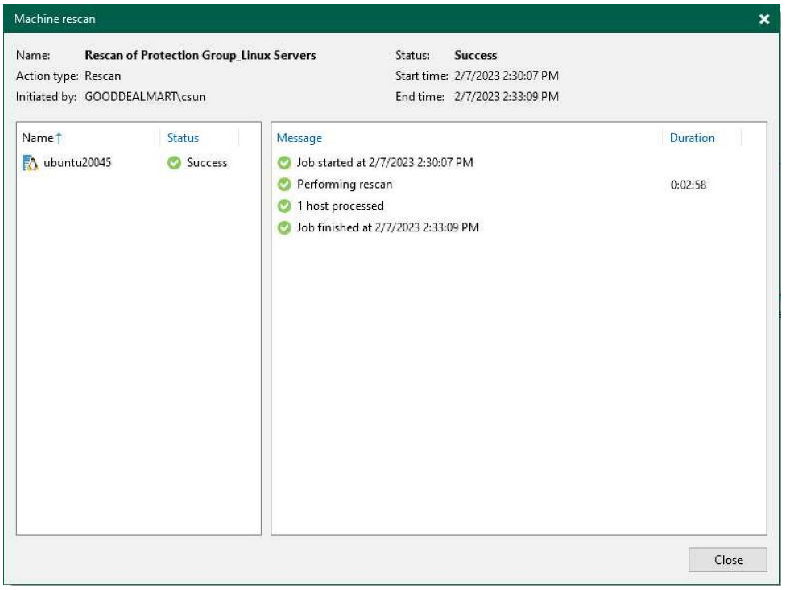
Protection group settings have been saved successfully. Click Finish to exit the wizard.

Summary:

Protection Group_Linux Servers was successfully saved.

☑ Run discovery when I click Finish

39. Verify the Machine rescan result and click Close.

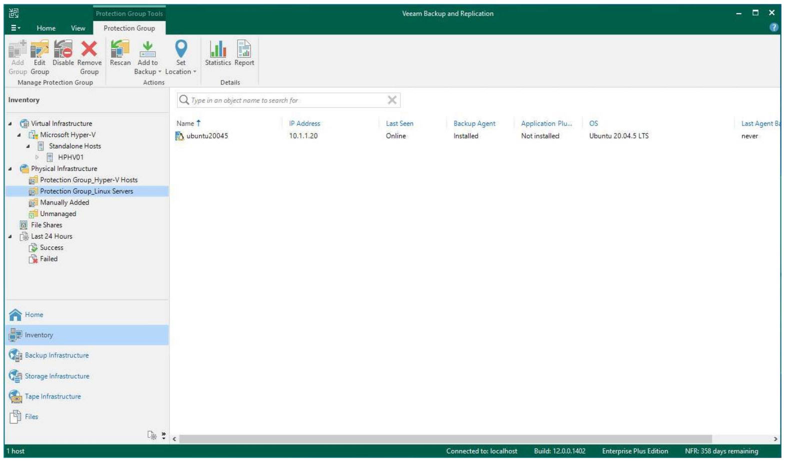


Name: Rescan of Protection Group_Linux Servers
Action type: Rescan
Initiated by: GOODDEALMART\csun
Status: Success
Start time: 2/7/2023 2:30:07 PM
End time: 2/7/2023 2:33:09 PM

Name ↑	Status
ubuntu20045	Success

Message	Duration
Job started at 2/7/2023 2:30:07 PM	
Performing rescan	0:02:58
1 host processed	
Job finished at 2/7/2023 2:33:09 PM	

40. Verify that the protection group has been added.



Name ↑	IP Address	Last Seen	Backup Agent	Application Plu...	OS	Last Agent Ba
ubuntu20045	10.1.1.20	Online	Installed	Not installed	Ubuntu 20.04.5 LTS	never

Backup Repository

Veeam stores backup files and metadata for replicated virtual machines in a backup repository. You can use the following storage types to set up a backup repository:

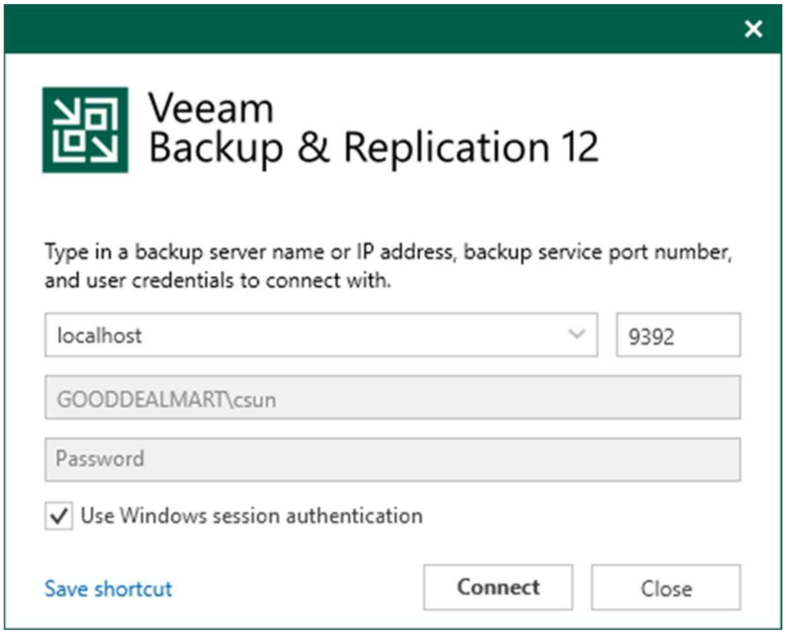
- Microsoft Windows server with local or network storage.
- Linux server with local or network storage.
- Linux server with a hardened repository.
- SMB (CIF) share network attached storage.
- NFS Share network attached storage.
- Deduplicatings storage appliances.
- Object storage.

Do not configure multiple backup repositories pointing to the exact location or using the same path.

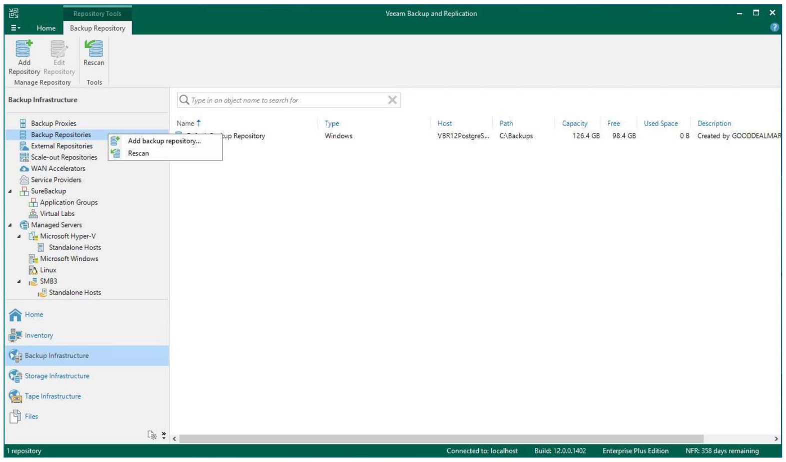
Add the Microsoft Windows server's local directory as a Backup Repository

You can add the following types of storage to the Microsoft Windows server as a backup repository:

- A local disk.
- A directly attached disk-based storage (such as a USB hard drive).
- SCSI/FC SAN LUN in case the server is connected to the SAN fabric.

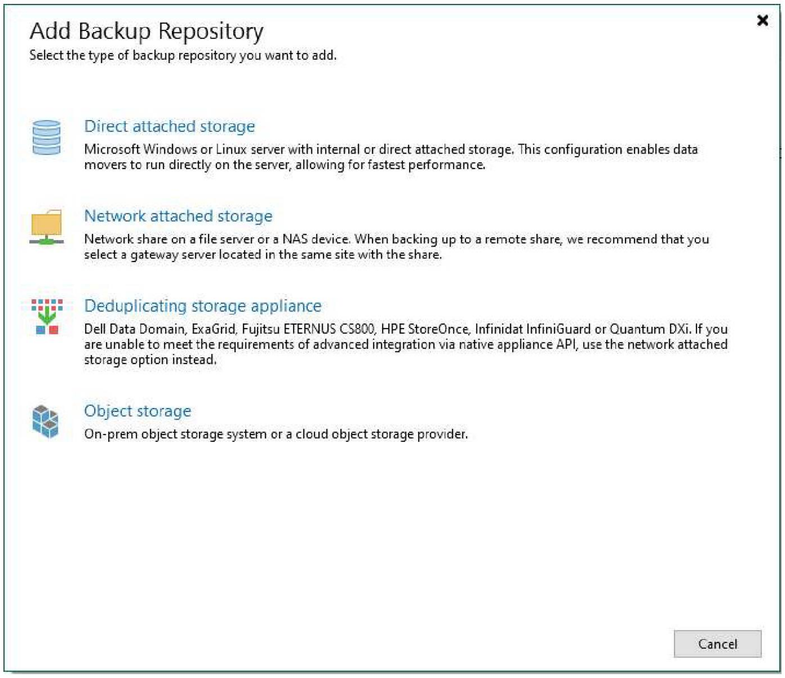
Instructions	Screenshot (if applicable)
1. Log in to the Veeam Backup and replication manager server. 2. Open the Veeam Backup & Replication Console and click Connect.	 Veeam Backup & Replication 12 Type in a backup server name or IP address, backup service port number, and user credentials to connect with. localhost 9392 GOODDEALMART\csun Password ☑ Use Windows session authentication Save shortcut Connect Close

3. Select Backup Infrastructure on the Home page.
4. Select Backup Repositories on the Backup Infrastructure page.
5. Right-click Backup Repositories and select Add backup repository.



Name	Type	Host	Path	Capacity	Free	Used Space	Description
up Repository	Windows	VBR12PostgreS...	C:\Backups	126.4 GB	98.4 GB	0 B	Created by GOODDEALMAR

6. Select Direct attached storage on the Add Backup Repository page.



Add Backup Repository

Select the type of backup repository you want to add.

Direct attached storage

Microsoft Windows or Linux server with internal or direct attached storage. This configuration enables data movers to run directly on the server, allowing for fastest performance.

Network attached storage

Network share on a file server or a NAS device. When backing up to a remote share, we recommend that you select a gateway server located in the same site with the share.

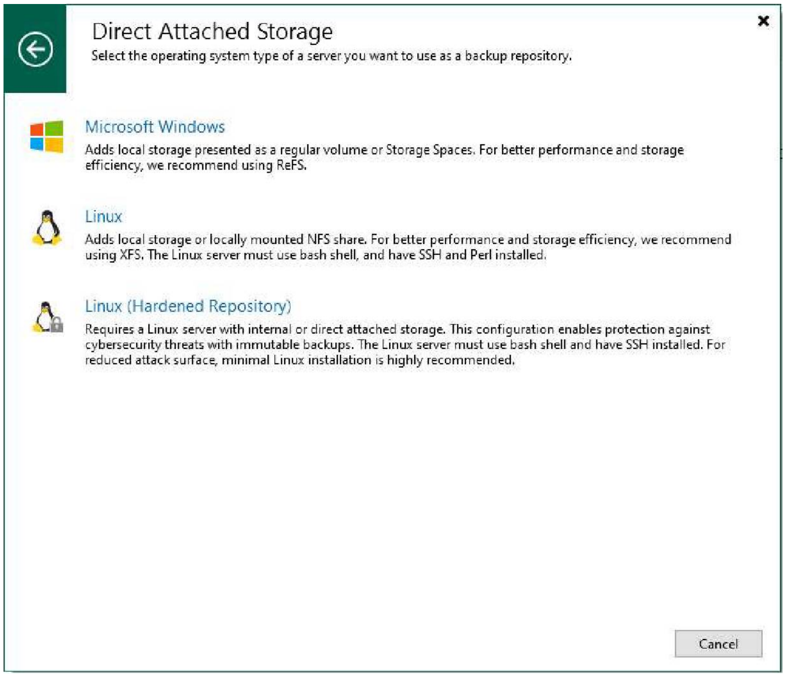
Deduplicating storage appliance

Dell Data Domain, ExaGrid, Fujitsu ETERNUS CS800, HPE StoreOnce, Infinidat InfiniGuard or Quantum DXi. If you are unable to meet the requirements of advanced integration via native appliance API, use the network attached storage option instead.

Object storage

On-prem object storage system or a cloud object storage provider.

7. Select Microsoft Windows on the Direct Attached Storage page.



Direct Attached Storage

Select the operating system type of a server you want to use as a backup repository.

Microsoft Windows

Adds local storage presented as a regular volume or Storage Spaces. For better performance and storage efficiency, we recommend using ReFS.

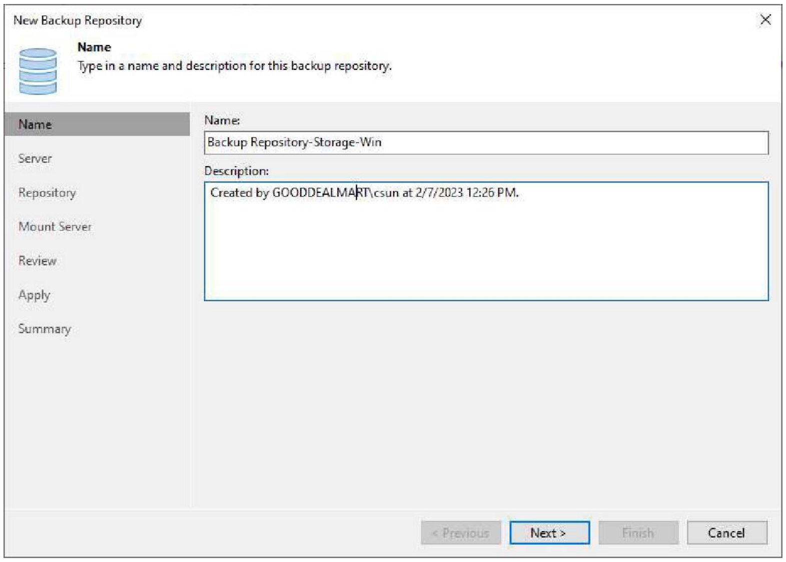
Linux

Adds local storage or locally mounted NFS share. For better performance and storage efficiency, we recommend using XFS. The Linux server must use bash shell, and have SSH and Perl installed.

Linux (Hardened Repository)

Requires a Linux server with internal or direct attached storage. This configuration enables protection against cybersecurity threats with immutable backups. The Linux server must use bash shell and have SSH installed. For reduced attack surface, minimal Linux installation is highly recommended.

8. On the Name page, specify a Backup Repository name.
9. Give a brief description in the Description field for future reference and click Next.



New Backup Repository

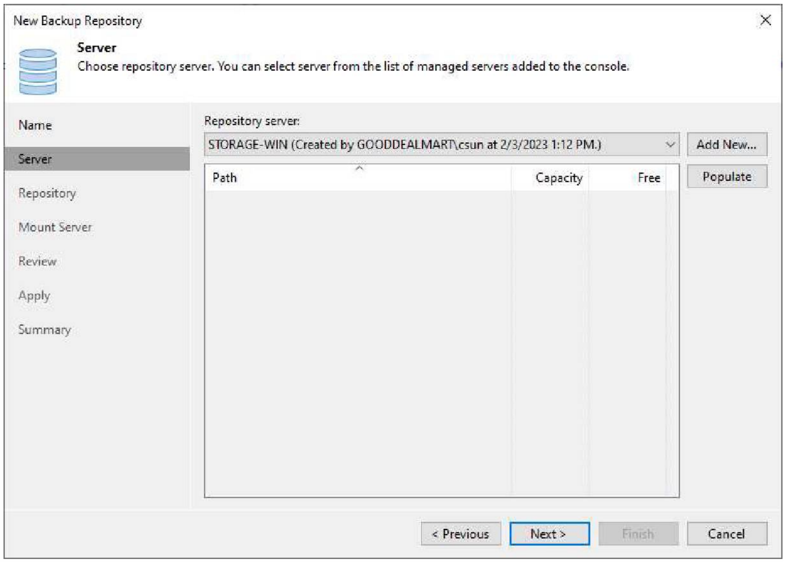
Name

Type in a name and description for this backup repository.

Name: Backup Repository-Storage-Win

Description: Created by GOODDEALMART\csun at 2/7/2023 12:26 PM.

10. On the Server page, select the Microsoft Windows server from the Repository server drop-down list and click Populate.



New Backup Repository

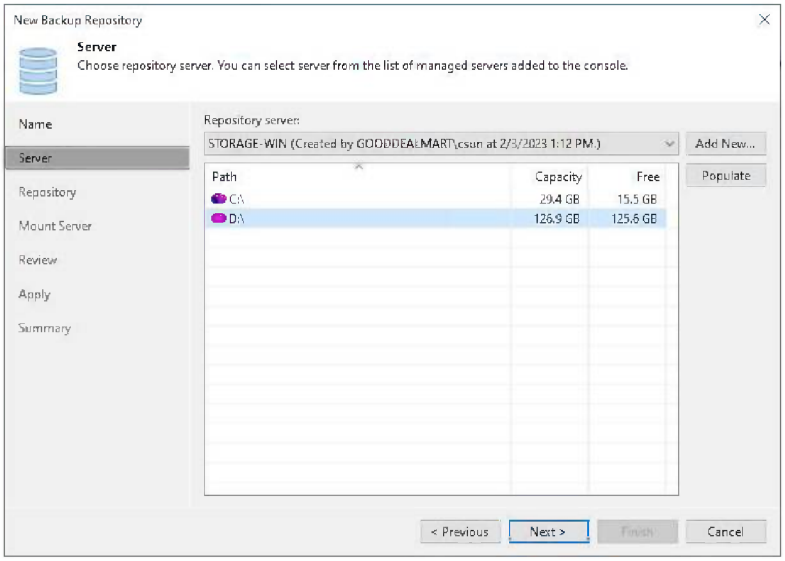
Server

Choose repository server. You can select server from the list of managed servers added to the console.

Repository server: STORAGE-WIN (Created by GOODDEALMART\csun at 2/3/2023 1:12 PM.)

Path	Capacity	Free

11. Select the disk and click Next.



New Backup Repository

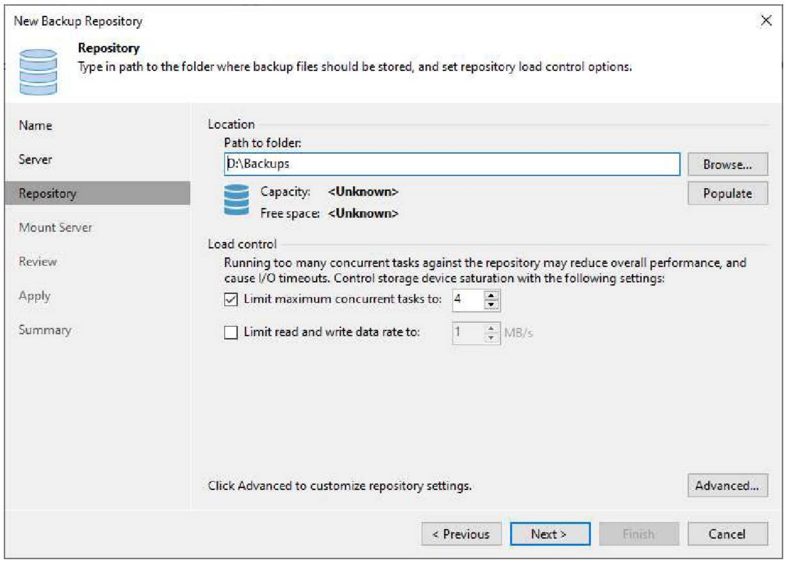
Server

Choose repository server. You can select server from the list of managed servers added to the console.

Repository server: STORAGE-WIN (Created by GOODDEALMART\csun at 2/3/2023 1:12 PM.)

Path	Capacity	Free
C:\	29.4 GB	15.5 GB
D:\	126.9 GB	125.6 GB

12. On the Repository page, click Populate to review the disk capacity and free space.



New Backup Repository

Repository

Type in path to the folder where backup files should be stored, and set repository load control options.

Location

Path to folder: D:\Backups

Capacity: **<Unknown>**

Free space: **<Unknown>**

Load control

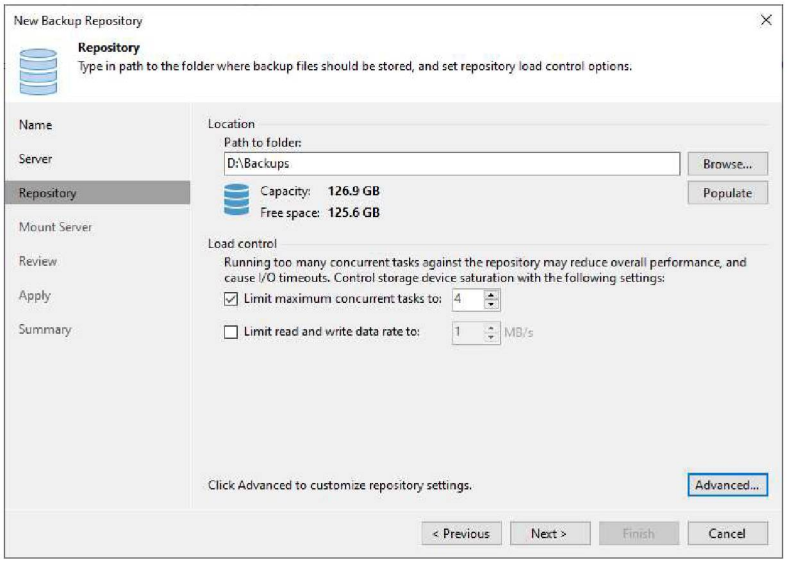
Running too many concurrent tasks against the repository may reduce overall performance, and cause I/O timeouts. Control storage device saturation with the following settings:

☑ Limit maximum concurrent tasks to: 4

☐ Limit read and write data rate to: 1 MB/s

Click Advanced to customize repository settings.

13. Use the Load control settings to manage the load on the backup repository and avoid storage I/O.
14. Click Advanced.



New Backup Repository

Repository

Type in path to the folder where backup files should be stored, and set repository load control options.

Location

Path to folder: D:\Backups

Capacity: **126.9 GB**

Free space: **125.6 GB**

Load control

Running too many concurrent tasks against the repository may reduce overall performance, and cause I/O timeouts. Control storage device saturation with the following settings:

☑ Limit maximum concurrent tasks to: 4

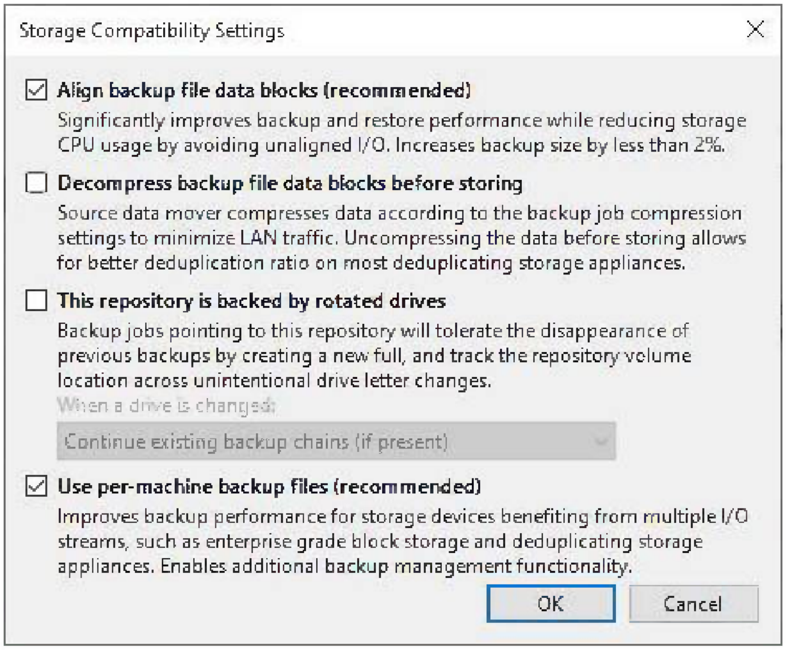
☐ Limit read and write data rate to: 1 MB/s

Click Advanced to customize repository settings.

15. On the Storage Compatibility Settings, select Align backup file data blocks (recommended) checkbox
16. Select Use per-machine backup files and click OK.

Note:

Select Decompress backup file data blocks before storing if you use a deduplicating storage feature or appliance.



Storage Compatibility Settings

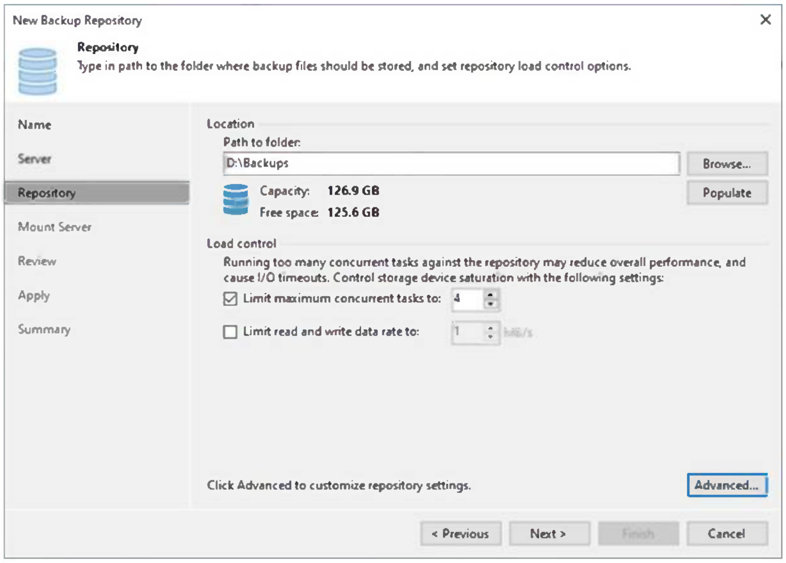
☑ **Align backup file data blocks (recommended)**
Significantly improves backup and restore performance while reducing storage CPU usage by avoiding unaligned I/O. Increases backup size by less than 2%.

□ **Decompress backup file data blocks before storing**
Source data mover compresses data according to the backup job compression settings to minimize LAN traffic. Uncompressing the data before storing allows for better deduplication ratio on most deduplicating storage appliances.

□ **This repository is backed by rotated drives**
Backup jobs pointing to this repository will tolerate the disappearance of previous backups by creating a new full, and track the repository volume location across unintentional drive letter changes.
When a drive is changed:
Continue existing backup chains (if present)

☑ **Use per-machine backup files (recommended)**
Improves backup performance for storage devices benefiting from multiple I/O streams, such as enterprise grade block storage and deduplicating storage appliances. Enables additional backup management functionality.

17. Click Next on the Repository page.



New Backup Repository

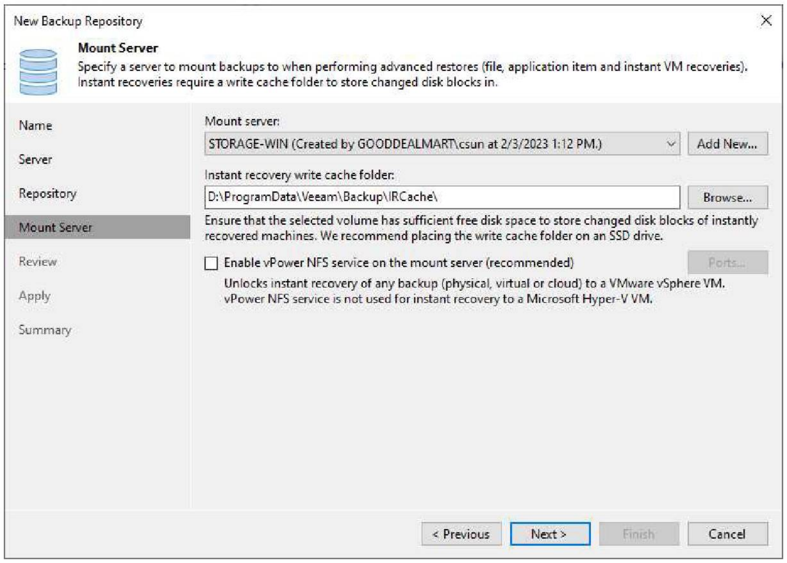
Repository
Type in path to the folder where backup files should be stored, and set repository load control options.

Location
Path to folder: D:\Backups
Capacity: 126.9 GB
Free space: 125.6 GB

Load control
Running too many concurrent tasks against the repository may reduce overall performance, and cause I/O timeouts. Control storage device saturation with the following settings:
☑ Limit maximum concurrent tasks to: 4
□ Limit read and write data rate to: 1 MB/s

Click Advanced to customize repository settings.

18. Select a mount server from the Mount server drop-down list on the Mount Server page.
19. Select a folder in the Instant recovery write cache folder field for writing cache during mount operations.
20. Unselect Enable vPower NFS service on the mount server because the vPower NFS service is not used for instant recovery to a Microsoft Hyper-V VM.
21. Click Next.



New Backup Repository

Mount Server

Specify a server to mount backups to when performing advanced restores (file, application item and instant VM recoveries). Instant recoveries require a write cache folder to store changed disk blocks in.

Mount server: STORAGE-WIN (Created by GOODDEALMART\csun at 2/3/2023 1:12 PM.)

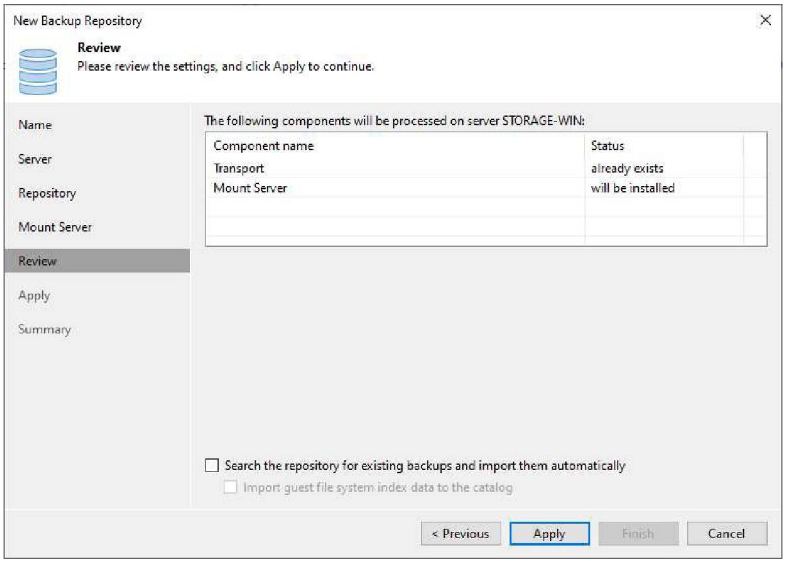
Instant recovery write cache folder: D:\ProgramData\Veeam\Backup\IRCache\

Ensure that the selected volume has sufficient free disk space to store changed disk blocks of instantly recovered machines. We recommend placing the write cache folder on an SSD drive.

☐ Enable vPower NFS service on the mount server (recommended)

Unlocks instant recovery of any backup (physical, virtual or cloud) to a VMware vSphere VM. vPower NFS service is not used for instant recovery to a Microsoft Hyper-V VM.

22. On the Review page, click Apply.
23. Select the Search the repository for existing backups and import them automatically checkbox if the backup repository contains backups previously created with Veeam Backup & Replication.
24. Select the Import guest file system index data to the catalog checkbox if the backup repository contains guest file system



New Backup Repository

Review

Please review the settings, and click Apply to continue.

The following components will be processed on server STORAGE-WIN:

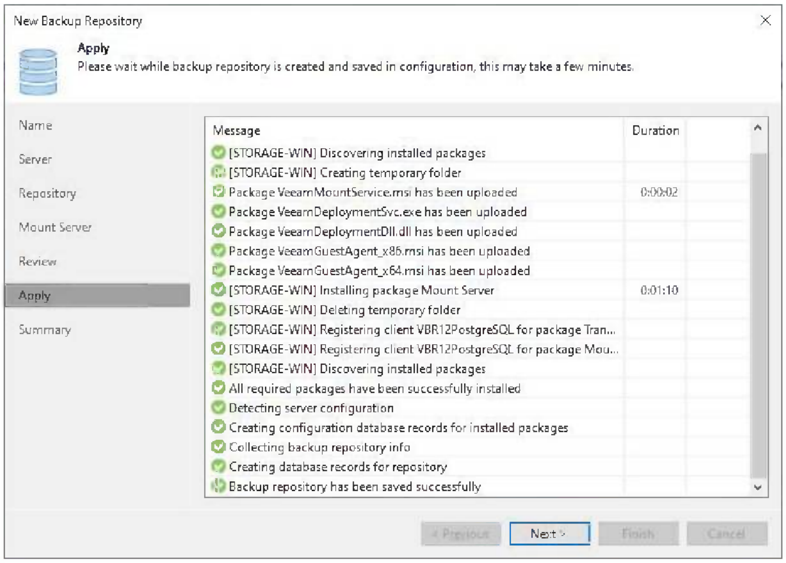
Component name	Status
Transport	already exists
Mount Server	will be installed

☐ Search the repository for existing backups and import them automatically

☐ Import guest file system index data to the catalog

index files previously created by Veeam Backup & Replication.

25. Click Next on the Apply page.

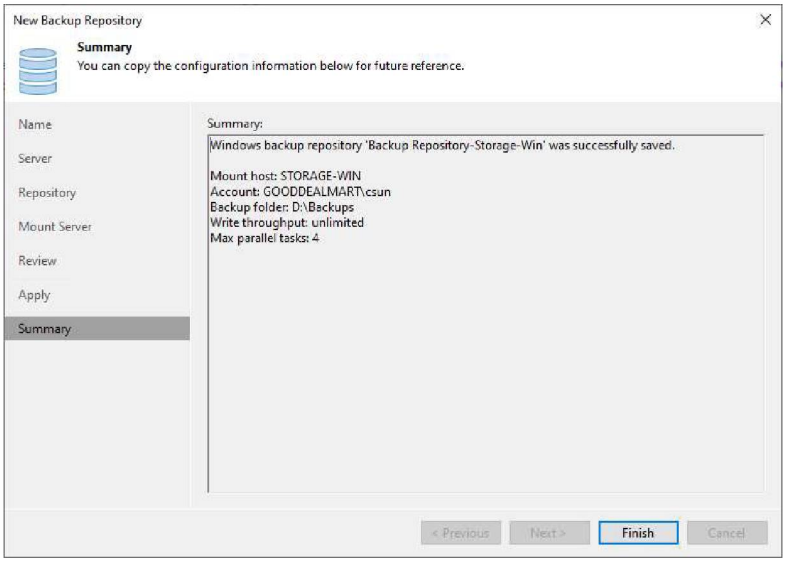


Apply

Please wait while backup repository is created and saved in configuration, this may take a few minutes.

Message	Duration
[STORAGE-WIN] Discovering installed packages	
[STORAGE-WIN] Creating temporary folder	
Package VeeamMountService.msi has been uploaded	0:00:02
Package VeeamDeploymentSvc.exe has been uploaded	
Package VeeamDeploymentDll.dll has been uploaded	
Package VeeamGuestAgent_x86.msi has been uploaded	
Package VeeamGuestAgent_x64.msi has been uploaded	
[STORAGE-WIN] Installing package Mount Server	0:01:10
[STORAGE-WIN] Deleting temporary folder	
[STORAGE-WIN] Registering client VBR12PostgreSQL for package Tran...	
[STORAGE-WIN] Registering client VBR12PostgreSQL for package Mou...	
[STORAGE-WIN] Discovering installed packages	
All required packages have been successfully installed	
Detecting server configuration	
Creating configuration database records for installed packages	
Collecting backup repository info	
Creating database records for repository	
Backup repository has been saved successfully	

26. Click Finish on the Summary page.



Summary

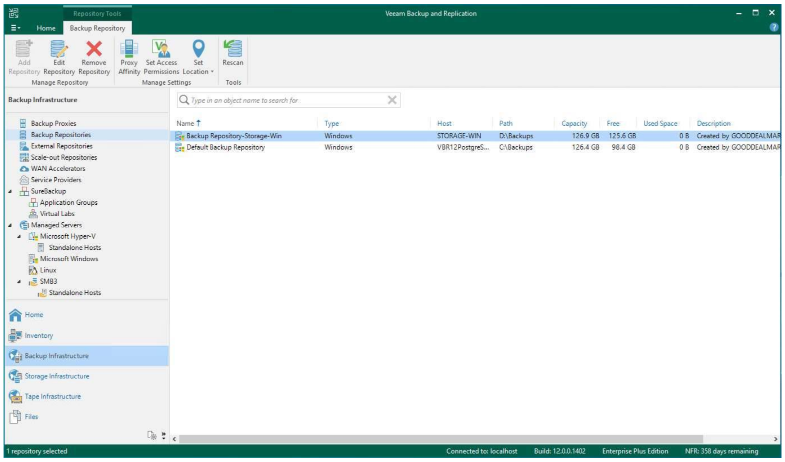
You can copy the configuration information below for future reference.

Summary:

Windows backup repository 'Backup Repository-Storage-Win' was successfully saved.

Mount host: STORAGE-WIN
Account: GOODDEALMART\csun
Backup folder: D:\Backups
Write throughput: unlimited
Max parallel tasks: 4

27. Verify that the new Backup Repository has been added.



Name ↑	Type	Host	Path	Capacity	Free	Used Space	Description
Backup Repository-Storage-Win	Windows	STORAGE-WIN	D:\Backups	126.9 GB	125.6 GB	0 B	Created by GOODDEALMAR
Default Backup Repository	Windows	VBR12PostgreS...	C:\Backups	126.4 GB	98.4 GB	0 B	Created by GOODDEALMAR

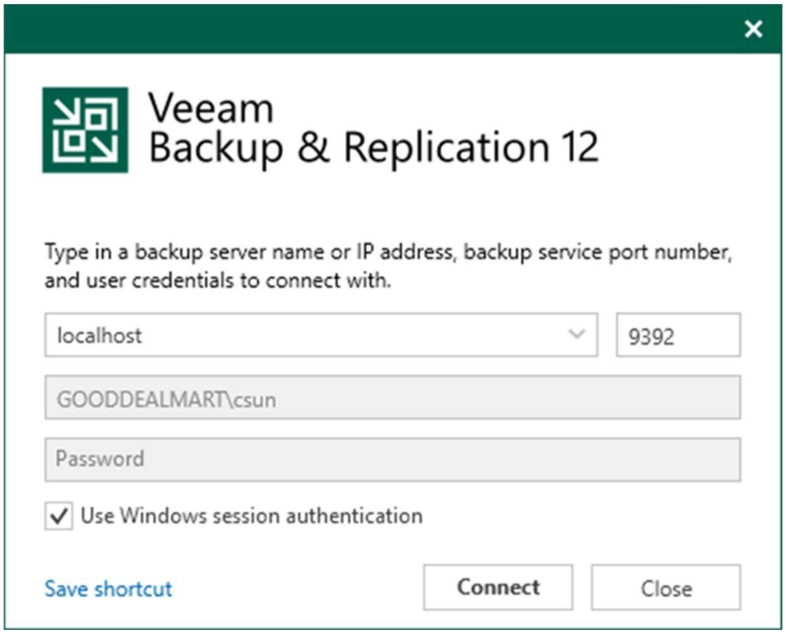
1 repository selected

Connected to: localhost Build: 12.0.0.1402 Enterprise Plus Edition NFR: 358 days remaining

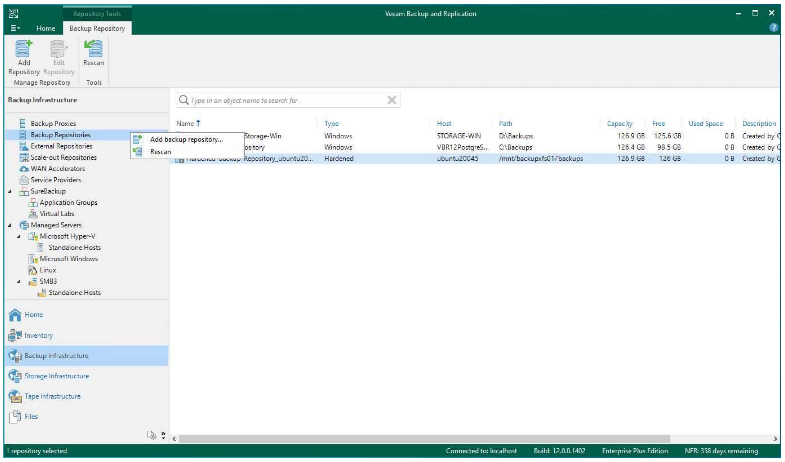
Add the Linux server’s local directory as a Backup Repository

You can add the following types of storage to the Linux server as a backup repository:

- A local disk.
- A directly attached disk-based storage (such as a USB hard drive).
- NFS share.
- SCSI/FC SAN LUN in case the server is connected to the SAN fabric.

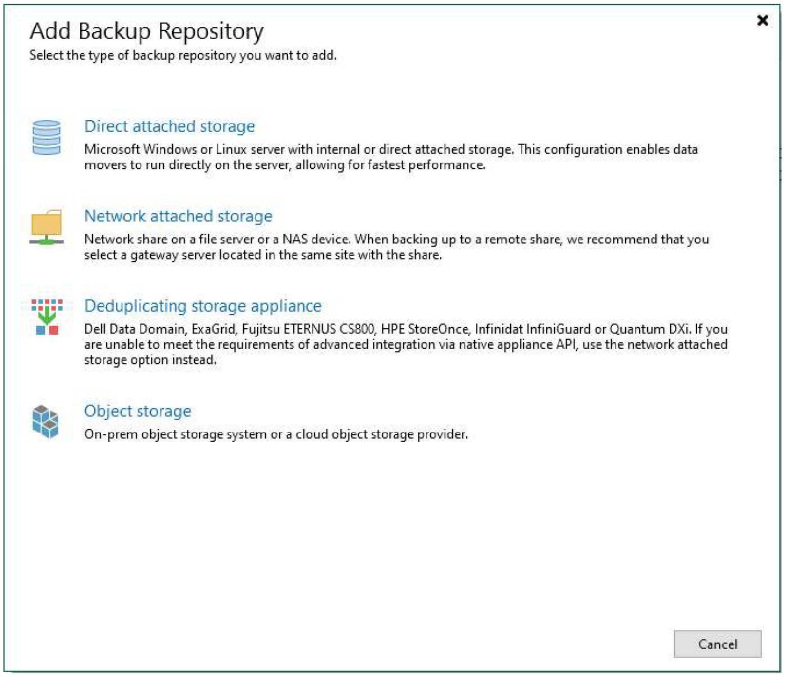
Instructions	Screenshot (if applicable)
1. Log in to the Veeam Backup and replication manager server. 2. Open the Veeam Backup & Replication Console, and click Connect.	 Veeam Backup & Replication 12 Type in a backup server name or IP address, backup service port number, and user credentials to connect with. localhost 9392 GOODDEALMART\csun Password ☑ Use Windows session authentication Save shortcut Connect Close

3. On the Home page, select Backup Infrastructure.
4. On the Backup Infrastructure page, select Backup Repositories.
5. Right-click Backup Repositories and select Add backup repository.



Name ↑	Type	Host	Path	Capacity	Free	Used Space	Description
Storage-Win	Windows	STORAGE-WIN	D:\Backups	126.9 GB	125.6 GB	0 B	Created by
ository	Windows	VBR12PostgreS...	C:\Backups	126.4 GB	98.5 GB	0 B	Created by
Repository_ubuntu20...	Hardened	ubuntu20045	/mnt/backupxfs01/backups	126.9 GB	126 GB	0 B	Created by

6. Select Direct attached storage on the Add Backup Repository page.



Add Backup Repository

Select the type of backup repository you want to add.

Direct attached storage

Microsoft Windows or Linux server with internal or direct attached storage. This configuration enables data movers to run directly on the server, allowing for fastest performance.

Network attached storage

Network share on a file server or a NAS device. When backing up to a remote share, we recommend that you select a gateway server located in the same site with the share.

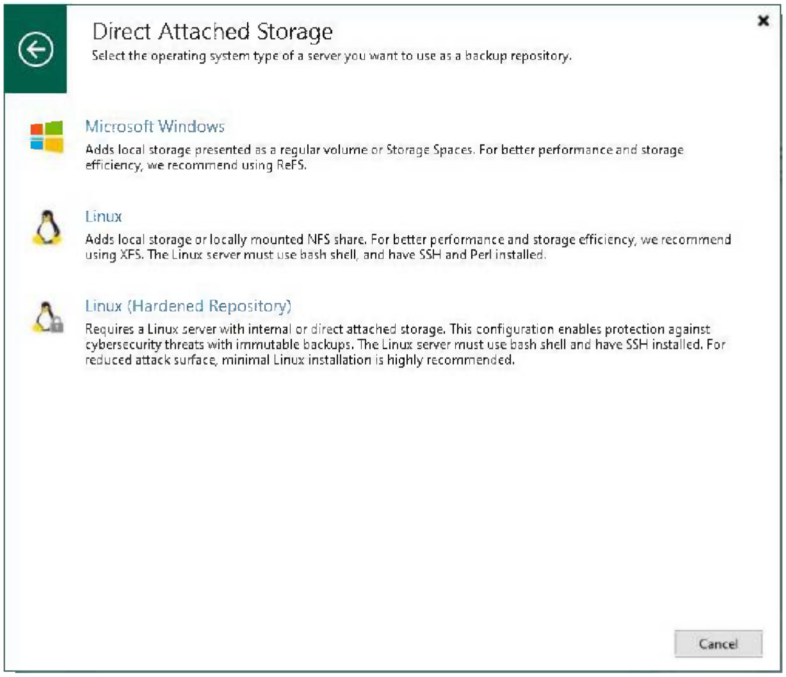
Deduplicating storage appliance

Dell Data Domain, ExaGrid, Fujitsu ETERNUS CS800, HPE StoreOnce, Infinidat InfiniGuard or Quantum DXi. If you are unable to meet the requirements of advanced integration via native appliance API, use the network attached storage option instead.

Object storage

On-prem object storage system or a cloud object storage provider.

7. Select Linux on the Direct Attached Storage page.



Direct Attached Storage

Select the operating system type of a server you want to use as a backup repository.

Microsoft Windows

Adds local storage presented as a regular volume or Storage Spaces. For better performance and storage efficiency, we recommend using ReFS.

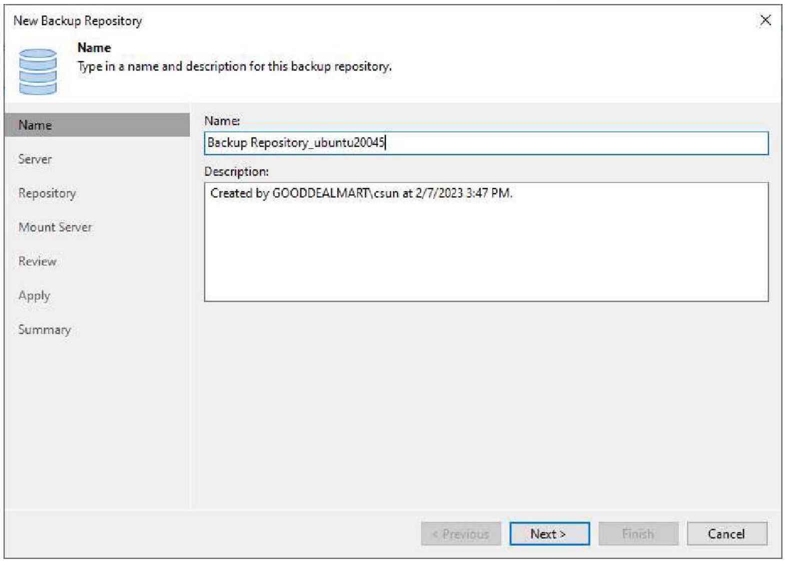
Linux

Adds local storage or locally mounted NFS share. For better performance and storage efficiency, we recommend using XFS. The Linux server must use bash shell, and have SSH and Perl installed.

Linux (Hardened Repository)

Requires a Linux server with internal or direct attached storage. This configuration enables protection against cybersecurity threats with immutable backups. The Linux server must use bash shell and have SSH installed. For reduced attack surface, minimal Linux installation is highly recommended.

8. On the Name page, specify a Backup Repository name.
9. Give a brief description in the Description field for future reference and click Next.



New Backup Repository

Name

Type in a name and description for this backup repository.

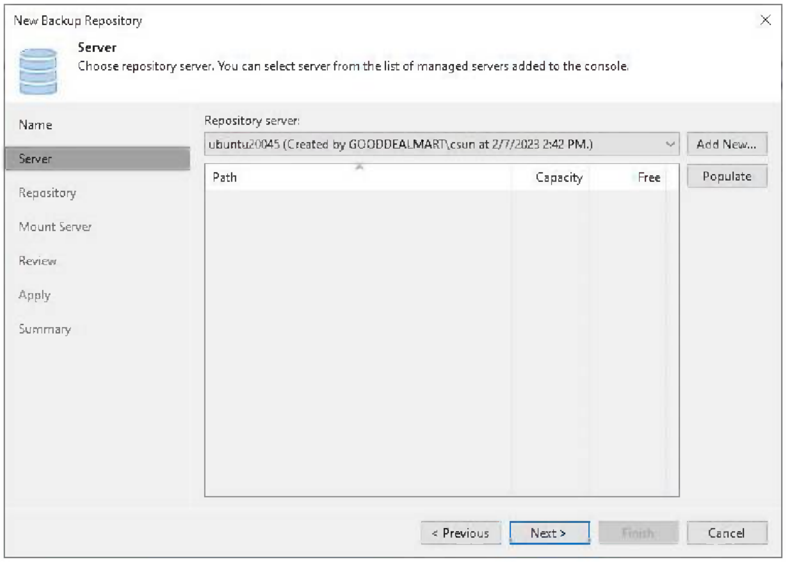
Name:

Backup Repository_ubuntu20045

Description:

Created by GOODDEALMART\csun at 2/7/2023 3:47 PM.

10. On the Server page, select the Linux server from the Repository server drop-down list and click Populate.



New Backup Repository

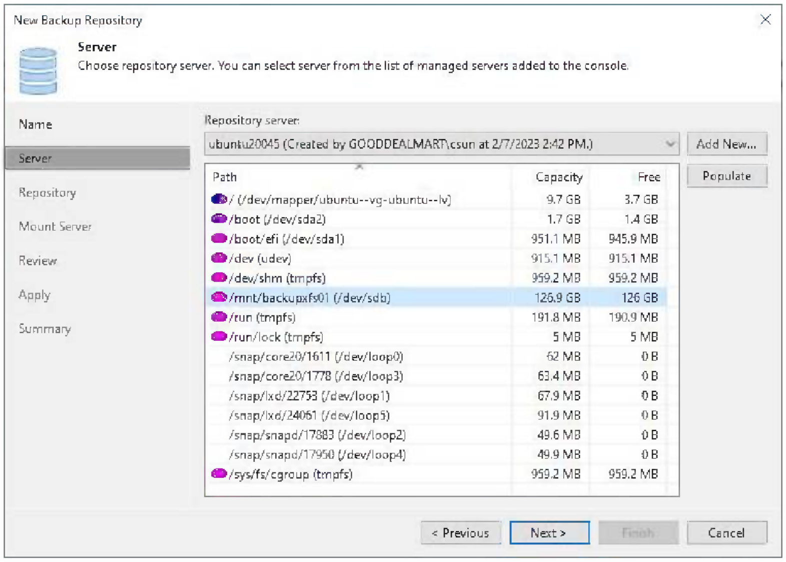
Server

Choose repository server. You can select server from the list of managed servers added to the console.

Repository server: ubuntu20045 (Created by GOODDEALMART\csun at 2/7/2023 2:42 PM.)

Path	Capacity	Free

11. Select the disk and click Next.



New Backup Repository

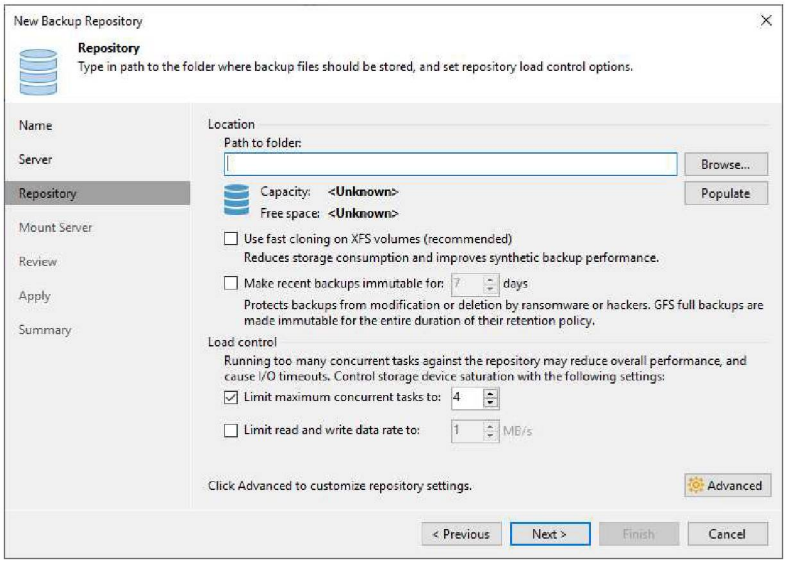
Server

Choose repository server. You can select server from the list of managed servers added to the console.

Repository server: ubuntu20045 (Created by GOODDEALMART\csun at 2/7/2023 2:42 PM.)

Path	Capacity	Free
/ (/dev/mapper/ubuntu--vg-ubuntu--lv)	9.7 GB	3.7 GB
/boot (/dev/sda2)	1.7 GB	1.4 GB
/boot/efi (/dev/sda1)	951.1 MB	945.9 MB
/dev (udev)	915.1 MB	915.1 MB
/dev/shm (tmpfs)	959.2 MB	959.2 MB
/mnt/backupxfs01 (/dev/sdb)	126.9 GB	126 GB
/run (tmpfs)	191.8 MB	190.9 MB
/run/lock (tmpfs)	5 MB	5 MB
/snap/core20/1611 (/dev/loop0)	62 MB	0 B
/snap/core20/1778 (/dev/loop3)	63.4 MB	0 B
/snap/lxd/22753 (/dev/loop1)	67.9 MB	0 B
/snap/lxd/24061 (/dev/loop5)	91.9 MB	0 B
/snap/snapd/17883 (/dev/loop2)	49.6 MB	0 B
/snap/snapd/17950 (/dev/loop4)	49.9 MB	0 B
/sys/fs/cgroup (tmpfs)	959.2 MB	959.2 MB

12. On the Repository page, click Browser for Path to folder.



New Backup Repository

Repository
Type in path to the folder where backup files should be stored, and set repository load control options.

Location

Path to folder:

Capacity: **<Unknown>**

Free space: **<Unknown>**

□ Use fast cloning on XFS volumes (recommended)
Reduces storage consumption and improves synthetic backup performance.

□ Make recent backups immutable for: 7 days
Protects backups from modification or deletion by ransomware or hackers. GFS full backups are made immutable for the entire duration of their retention policy.

Load control

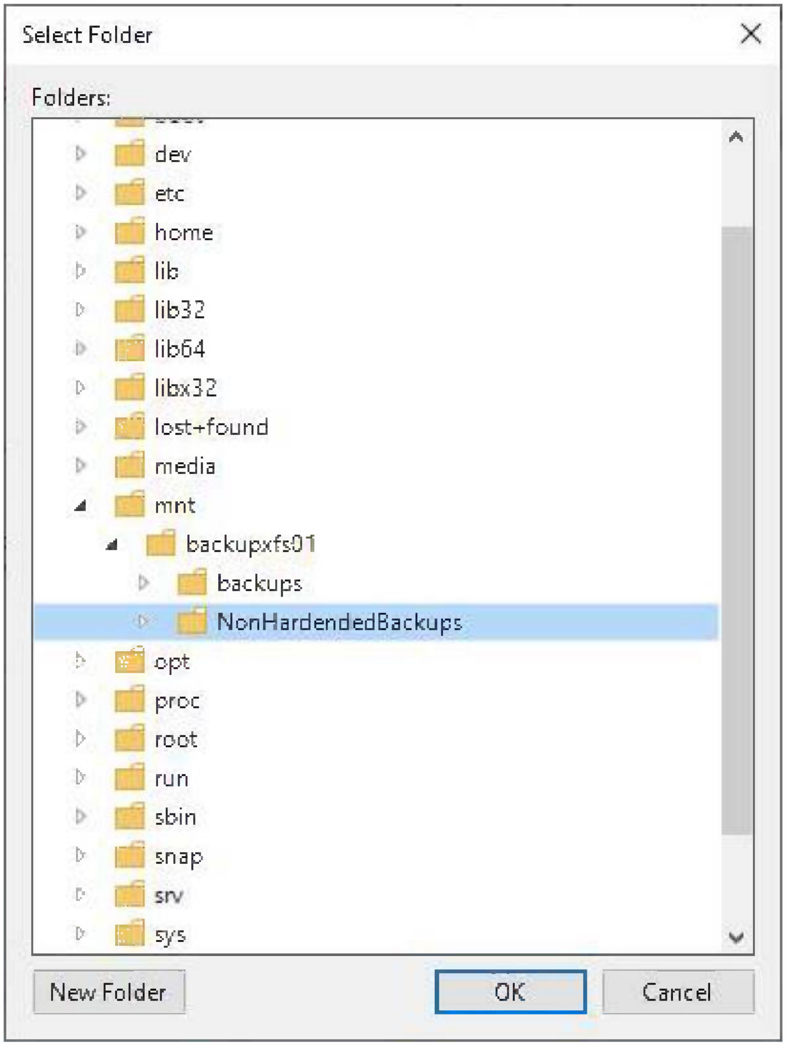
Running too many concurrent tasks against the repository may reduce overall performance, and cause I/O timeouts. Control storage device saturation with the following settings:

☑ Limit maximum concurrent tasks to: 4

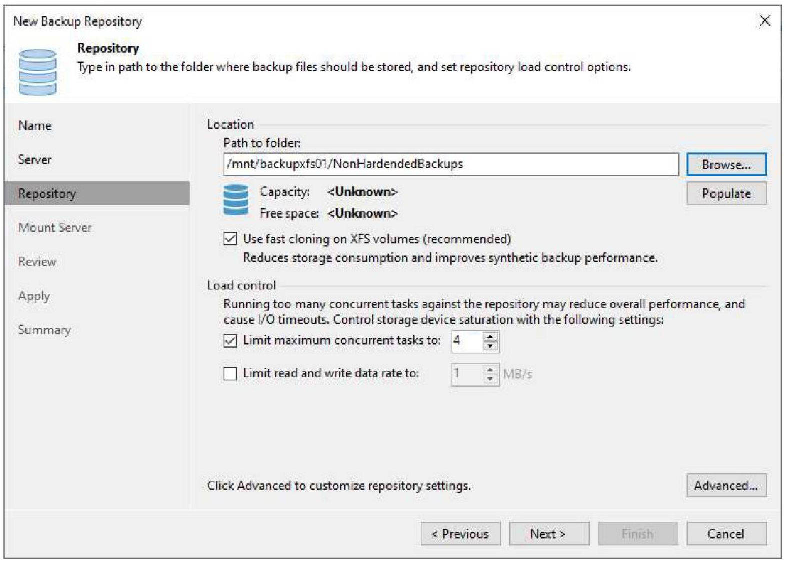
□ Limit read and write data rate to: 1 MB/s

Click Advanced to customize repository settings.

13. On the Select Folder page, expand the server.
14. Select the NonHardenedBackups folder and click OK.



15. On the Repository page, click Populate.



Repository

Type in path to the folder where backup files should be stored, and set repository load control options.

Location

Path to folder: /mnt/backupxfs01/NonHardendedBackups

Capacity: <Unknown>

Free space: <Unknown>

☑ Use fast cloning on XFS volumes (recommended)
Reduces storage consumption and improves synthetic backup performance.

Load control

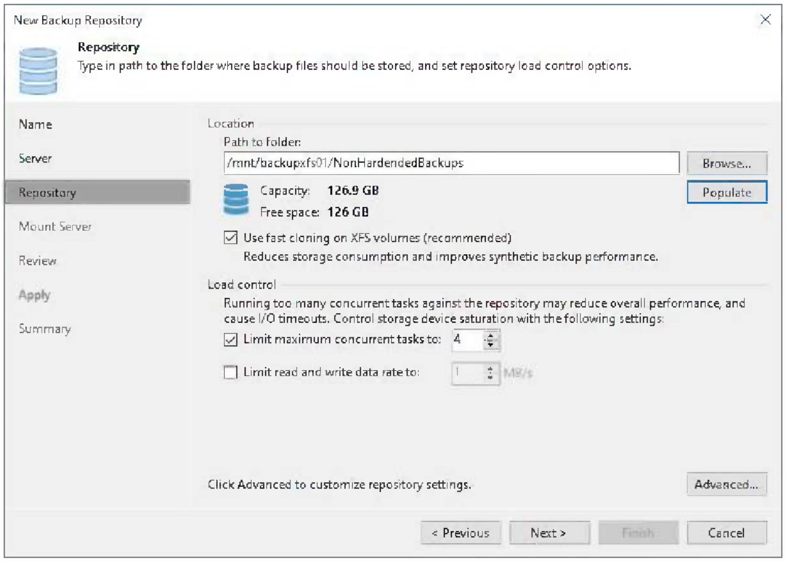
Running too many concurrent tasks against the repository may reduce overall performance, and cause I/O timeouts. Control storage device saturation with the following settings:

☑ Limit maximum concurrent tasks to: 4

□ Limit read and write data rate to: 1 MB/s

Click Advanced to customize repository settings.

16. On the Repository page, select Use fast closing on XFS volumes.
17. Use the Load control settings to manage the load on the backup repository and avoid storage I/O timeouts.
18. Click Advanced.



Repository

Type in path to the folder where backup files should be stored, and set repository load control options.

Location

Path to folder: /mnt/backupxfs01/NonHardendedBackups

Capacity: 126.9 GB

Free space: 126 GB

☑ Use fast cloning on XFS volumes (recommended)
Reduces storage consumption and improves synthetic backup performance.

Load control

Running too many concurrent tasks against the repository may reduce overall performance, and cause I/O timeouts. Control storage device saturation with the following settings:

☑ Limit maximum concurrent tasks to: 4

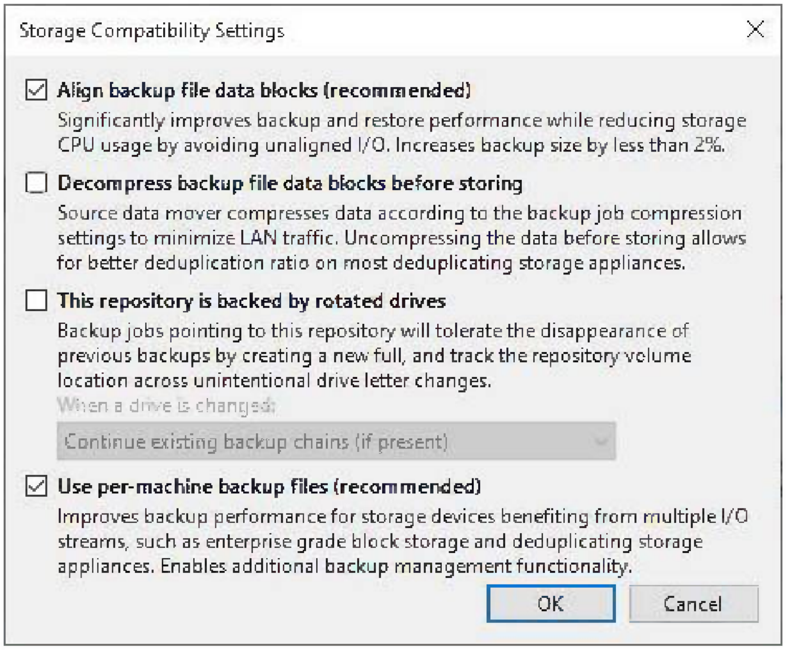
□ Limit read and write data rate to: 1 MB/s

Click Advanced to customize repository settings.

19. On the Storage Compatibility Settings, select Align backup file data blocks (recommended) checkbox
20. Select Use per-machine backup files and click OK.

Note:

Select Decompress backup file data blocks before storing if you use a deduplicating storage feature or appliance.



Storage Compatibility Settings

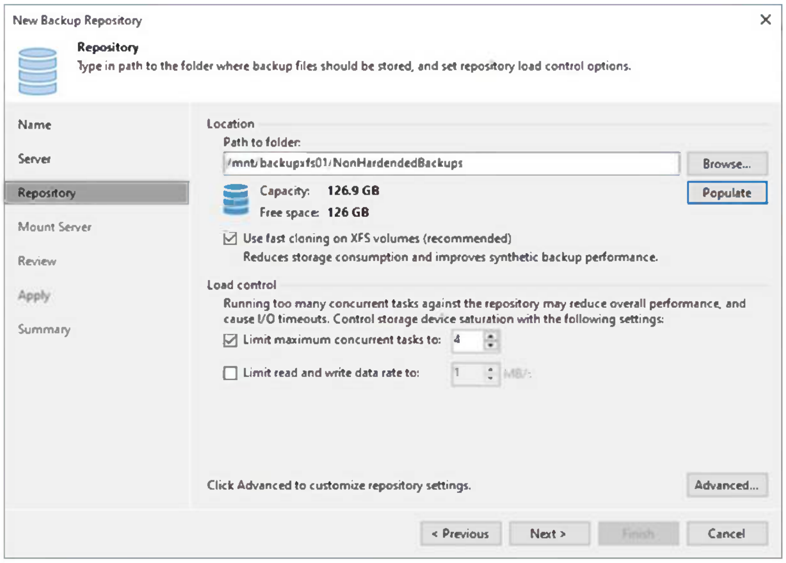
☑ **Align backup file data blocks (recommended)**
Significantly improves backup and restore performance while reducing storage CPU usage by avoiding unaligned I/O. Increases backup size by less than 2%.

☐ **Decompress backup file data blocks before storing**
Source data mover compresses data according to the backup job compression settings to minimize LAN traffic. Uncompressing the data before storing allows for better deduplication ratio on most deduplicating storage appliances.

☐ **This repository is backed by rotated drives**
Backup jobs pointing to this repository will tolerate the disappearance of previous backups by creating a new full, and track the repository volume location across unintentional drive letter changes.
When a drive is changed:
Continue existing backup chains (if present)

☑ **Use per-machine backup files (recommended)**
Improves backup performance for storage devices benefiting from multiple I/O streams, such as enterprise grade block storage and deduplicating storage appliances. Enables additional backup management functionality.

21. On the Repository page, click Next.



New Backup Repository

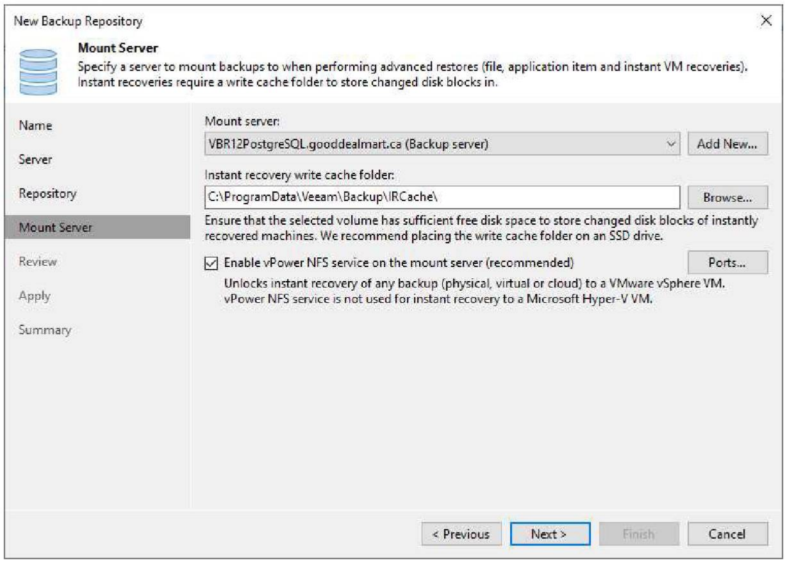
Repository
Type in path to the folder where backup files should be stored, and set repository load control options.

Location
Path to folder: /mnt/backupxfs01/NonHardendedBackups
Capacity: 126.9 GB
Free space: 126 GB
☑ Use fast cloning on XFS volumes (recommended)
Reduces storage consumption and improves synthetic backup performance.

Load control
Running too many concurrent tasks against the repository may reduce overall performance, and cause I/O timeouts. Control storage device saturation with the following settings:
☑ Limit maximum concurrent tasks to: 4
☐ Limit read and write data rate to: 1 MB/s

Click Advanced to customize repository settings.

22. Select a mount server from the Mount server drop-down list on the Mount Server page.
23. Select a folder in the Instant recovery write cache folder field for writing cache during mount operations.
24. Select Enable vPower NFS service on the mount server (recommend) and click Ports.



New Backup Repository

Mount Server

Specify a server to mount backups to when performing advanced restores (file, application item and instant VM recoveries). Instant recoveries require a write cache folder to store changed disk blocks in.

Mount server: VBR12PostgreSQL.gooddealmart.ca (Backup server)

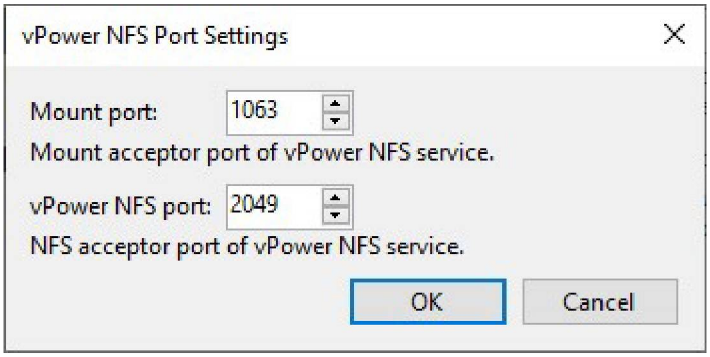
Instant recovery write cache folder: C:\ProgramData\Veeam\Backup\IRCache\

Ensure that the selected volume has sufficient free disk space to store changed disk blocks of instantly recovered machines. We recommend placing the write cache folder on an SSD drive.

☑ Enable vPower NFS service on the mount server (recommended)

Unlocks instant recovery of any backup (physical, virtual or cloud) to a VMware vSphere VM. vPower NFS service is not used for instant recovery to a Microsoft Hyper-V VM.

25. Review the ports settings on the vPower NFS Port Settings and click OK.



vPower NFS Port Settings

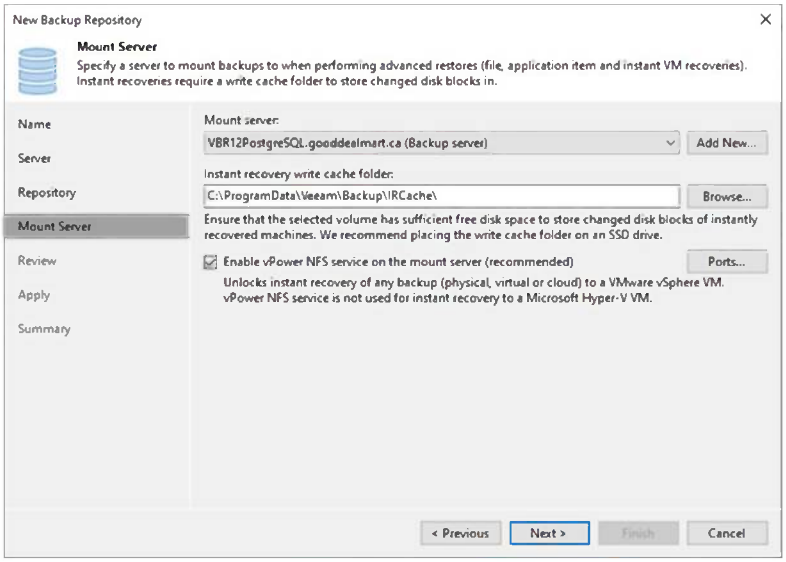
Mount port: 1063

Mount acceptor port of vPower NFS service.

vPower NFS port: 2049

NFS acceptor port of vPower NFS service.

26. Click Next on the Mount Server page.



New Backup Repository

Mount Server

Specify a server to mount backups to when performing advanced restores (file, application item and instant VM recoveries). Instant recoveries require a write cache folder to store changed disk blocks in.

Mount server:

VBR12PostgreSQL.gooddealmart.ca (Backup server)

Instant recovery write cache folder:

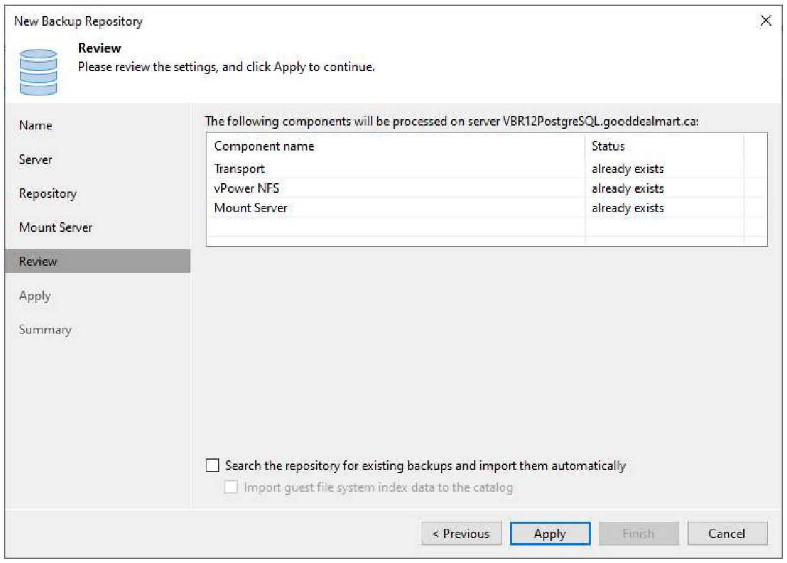
C:\ProgramData\Veeam\Backup\IRCache\

Ensure that the selected volume has sufficient free disk space to store changed disk blocks of instantly recovered machines. We recommend placing the write cache folder on an SSD drive.

☑ Enable vPower NFS service on the mount server (recommended)

Unlocks instant recovery of any backup (physical, virtual or cloud) to a VMware vSphere VM. vPower NFS service is not used for instant recovery to a Microsoft Hyper-V VM.

27. Click Apply on the Review page.
28. Select the Search the repository for existing backups and import them automatically checkbox if the backup repository contains backups previously created with Veeam Backup & Replication.
29. Select the Import guest file system index data to the catalog checkbox if the backup repository contains guest file system index files previously created by Veeam Backup & Replication.



New Backup Repository

Review

Please review the settings, and click Apply to continue.

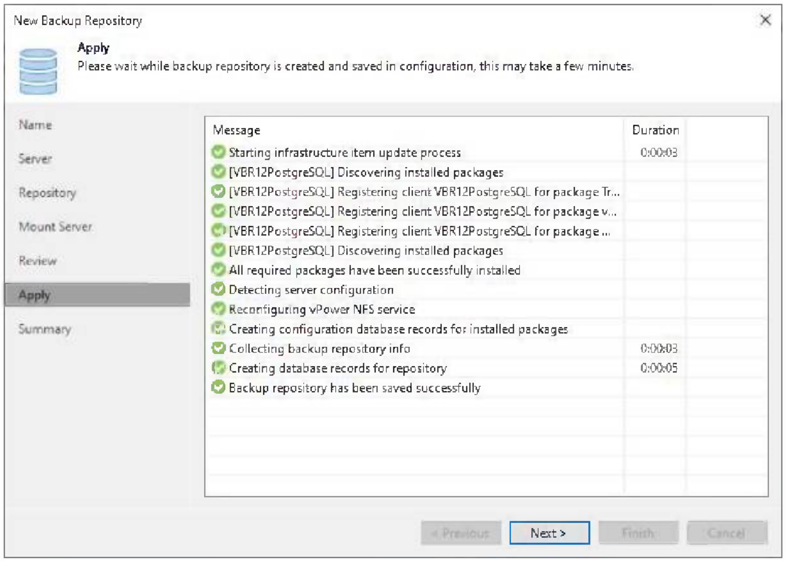
The following components will be processed on server VBR12PostgreSQL.gooddealmart.ca:

Component name	Status
Transport	already exists
vPower NFS	already exists
Mount Server	already exists

□ Search the repository for existing backups and import them automatically

□ Import guest file system index data to the catalog

30. Click Next on the Apply page.

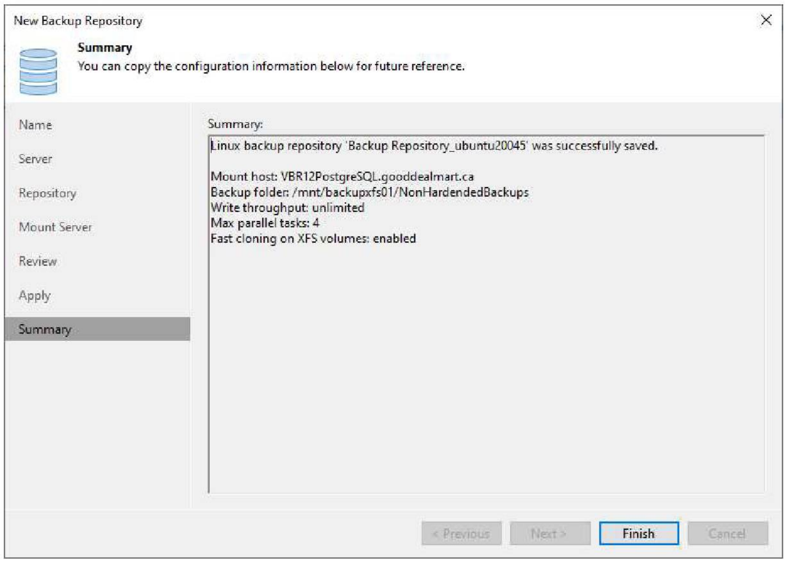


Apply

Please wait while backup repository is created and saved in configuration, this may take a few minutes.

Message	Duration
✓ Starting infrastructure item update process	0:00:03
✓ [VBR12PostgreSQL] Discovering installed packages	
✓ [VBR12PostgreSQL] Registering client VBR12PostgreSQL for package Tr...	
✓ [VBR12PostgreSQL] Registering client VBR12PostgreSQL for package v...	
✓ [VBR12PostgreSQL] Registering client VBR12PostgreSQL for package ...	
✓ [VBR12PostgreSQL] Discovering installed packages	
✓ All required packages have been successfully installed	
✓ Detecting server configuration	
✓ Reconfiguring vPower NFS service	
✓ Creating configuration database records for installed packages	
✓ Collecting backup repository info	0:00:03
✓ Creating database records for repository	0:00:05
✓ Backup repository has been saved successfully	

31. Click Finish on the Summary page.



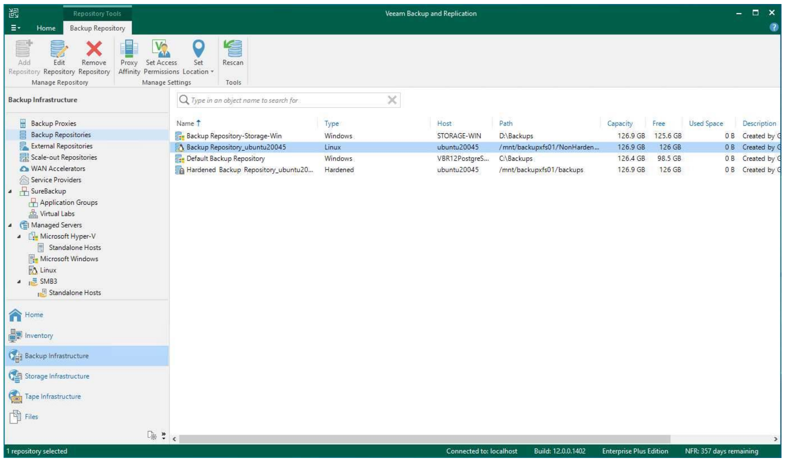
Summary

You can copy the configuration information below for future reference.

Summary:

```
Linux backup repository 'Backup Repository_ubuntu20045' was successfully saved.

Mount host: VBR12PostgreSQL.gooddealmart.ca
Backup folder: /mnt/backupxfs01/NonHardendedBackups
Write throughput: unlimited
Max parallel tasks: 4
Fast cloning on XFS volumes: enabled
```

32. Verify that the Linux Backup Repository has been added.



Name	Type	Host	Path	Capacity	Free	Used Space	Description
Backup Repository-Storage-Win	Windows	STORAGE-WIN	D:\Backups	126.9 GB	125.6 GB	0 B	Created by G
Backup Repository_ubuntu20045	Linux	ubuntu20045	/mnt/backupxfs01/NonHarden...	126.9 GB	126 GB	0 B	Created by G
Default Backup Repository	Windows	VBR12PostgreS...	C:\Backups	126.4 GB	98.5 GB	0 B	Created by G
Hardened Backup Repository_ubuntu20...	Hardened	ubuntu20045	/mnt/backupxfs01/backups	126.9 GB	126 GB	0 B	Created by G

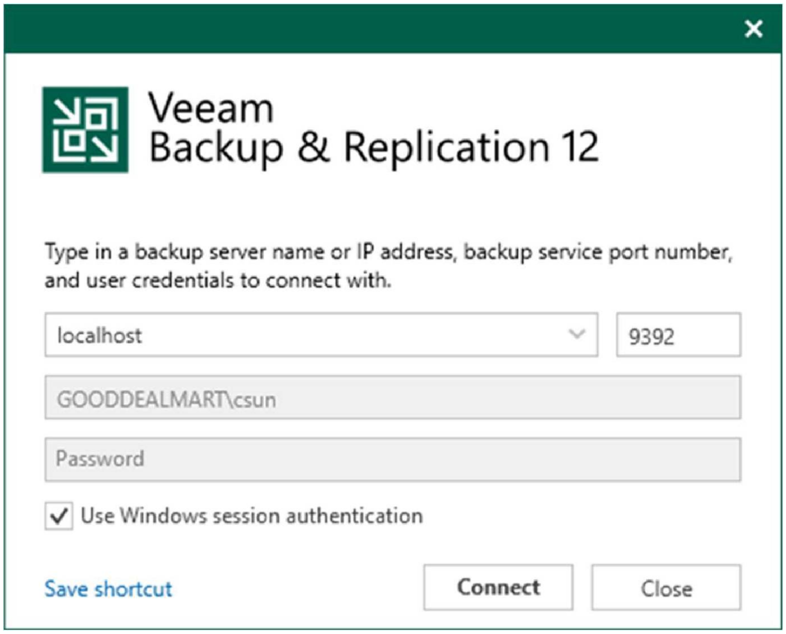
Add the Linux server’s local directory as a Hardened Backup Repository

You can add a hardened repository based on a Linux server to your backup infrastructure to protect your backup files from loss due to malware activity or unplanned actions. The hardened repository supports the following features:

- Immutability: You specify the period when you add a hardened repository, and backup files must be immutable.
- Single-use credentials: Credentials will only be used once to add the Linux server to the backup infrastructure. The backup infrastructure does not store these credentials. Therefore, the attacker cannot access the hardened repository even if the Veeam Backup & Replication server is compromised.

Instructions	Screenshot (if applicable)

1. Log in to the Veeam Backup and replication manager server.
2. Open the Veeam Backup & Replication Console, and click Connect.



Type in a backup server name or IP address, backup service port number, and user credentials to connect with.

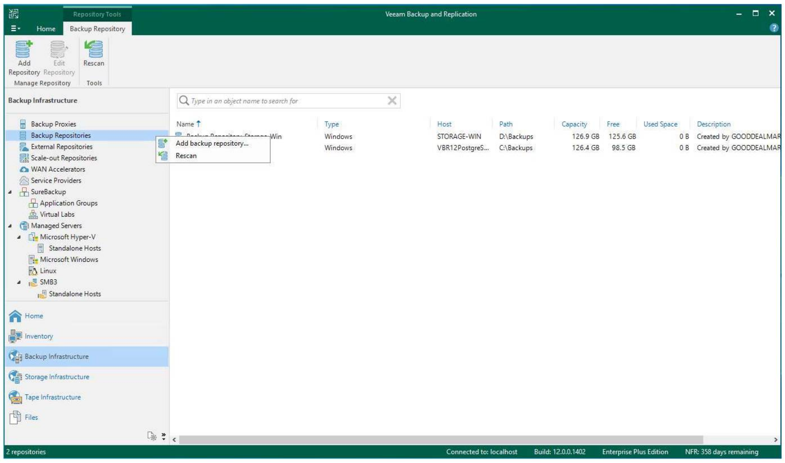
localhost 9392

GOODDEALMART\csun

Password

☑ Use Windows session authentication

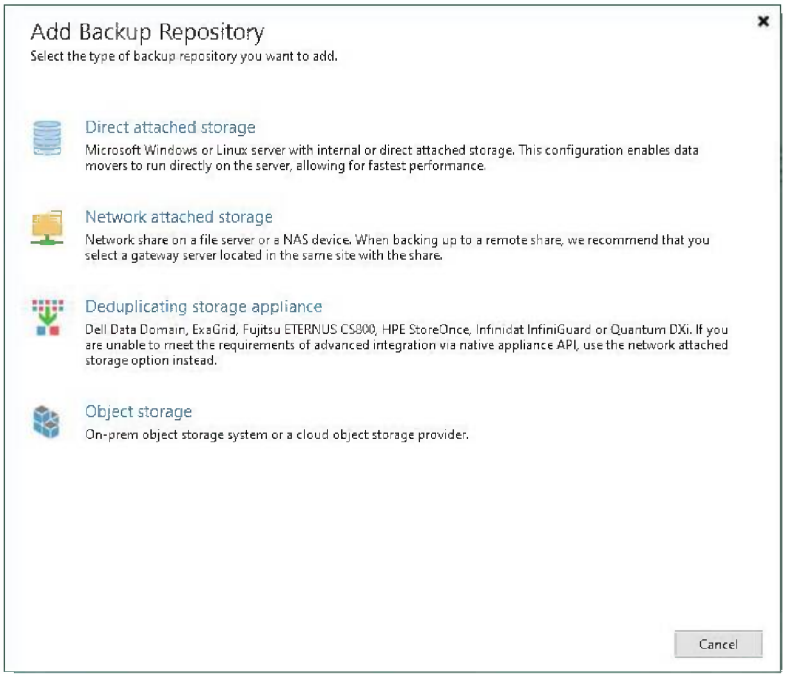
3. On the Home page, select Backup Infrastructure.
4. On the Backup Infrastructure page, select Backup Repositories.
5. Right-click Backup Repositories and select Add backup repository.



Name ↑	Type	Host	Path	Capacity	Free	Used Space	Description
Backup Repository: Storage-Win	Windows	STORAGE-WIN	D:\Backups	126.9 GB	125.6 GB	0 B	Created by GOODDEALMAR
	Windows	VBR12PostgreS...	C:\Backups	126.4 GB	98.5 GB	0 B	Created by GOODDEALMAR

2 repositories Connected to: localhost Build: 12.0.0.1402 Enterprise Plus Edition NFR: 358 days remaining

6. Select Direct attached storage on the Add Backup Repository page.



Add Backup Repository

Select the type of backup repository you want to add.

Direct attached storage

Microsoft Windows or Linux server with internal or direct attached storage. This configuration enables data movers to run directly on the server, allowing for fastest performance.

Network attached storage

Network share on a file server or a NAS device. When backing up to a remote share, we recommend that you select a gateway server located in the same site with the share.

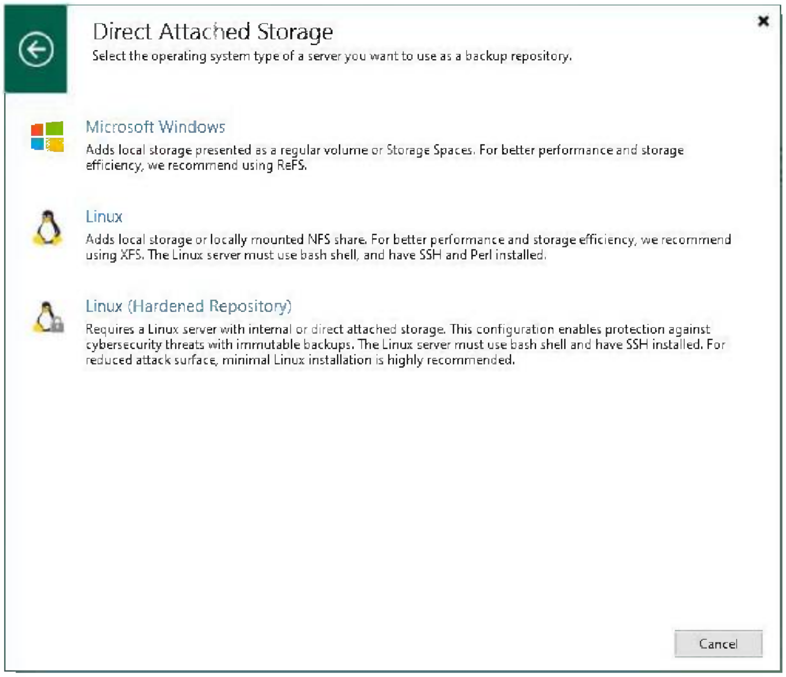
Deduplicating storage appliance

Dell Data Domain, ExaGrid, Fujitsu ETERNUS CS800, HPE StoreOnce, Infinidat InfiniGuard or Quantum DXi. If you are unable to meet the requirements of advanced integration via native appliance API, use the network attached storage option instead.

Object storage

On-prem object storage system or a cloud object storage provider.

7. Select Linux (Hardened Repository) on the Direct Attached Storage page.



Direct Attached Storage

Select the operating system type of a server you want to use as a backup repository.

Microsoft Windows

Adds local storage presented as a regular volume or Storage Spaces. For better performance and storage efficiency, we recommend using ReFS.

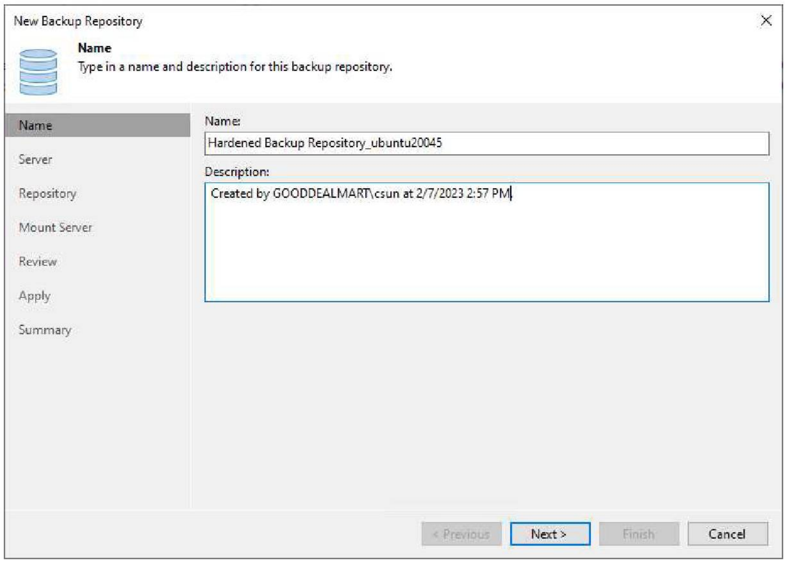
Linux

Adds local storage or locally mounted NFS share. For better performance and storage efficiency, we recommend using XFS. The Linux server must use bash shell, and have SSH and Perl installed.

Linux (Hardened Repository)

Requires a Linux server with internal or direct attached storage. This configuration enables protection against cybersecurity threats with immutable backups. The Linux server must use bash shell and have SSH installed. For reduced attack surface, minimal Linux installation is highly recommended.

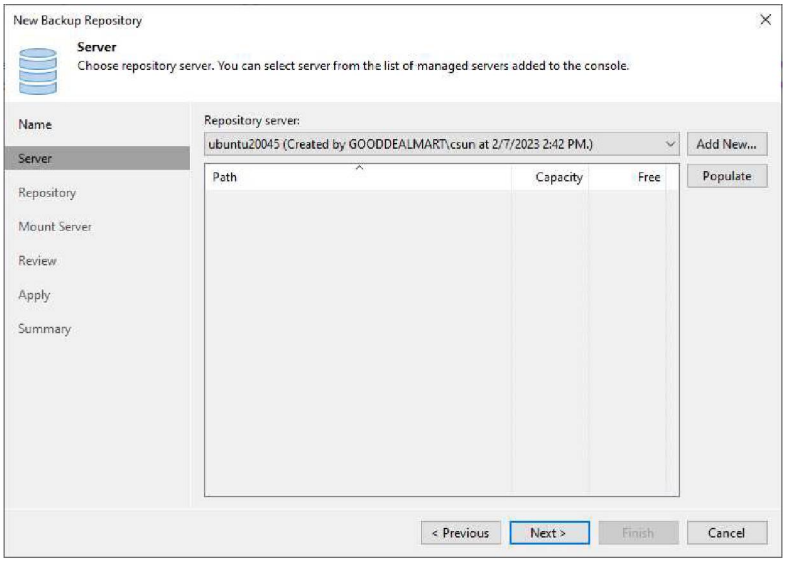
8. On the Name page, specify a Backup Repository name.
9. Give a brief description in the Description field for future reference and click Next.



Name:
Hardened Backup Repository_ubuntu20045

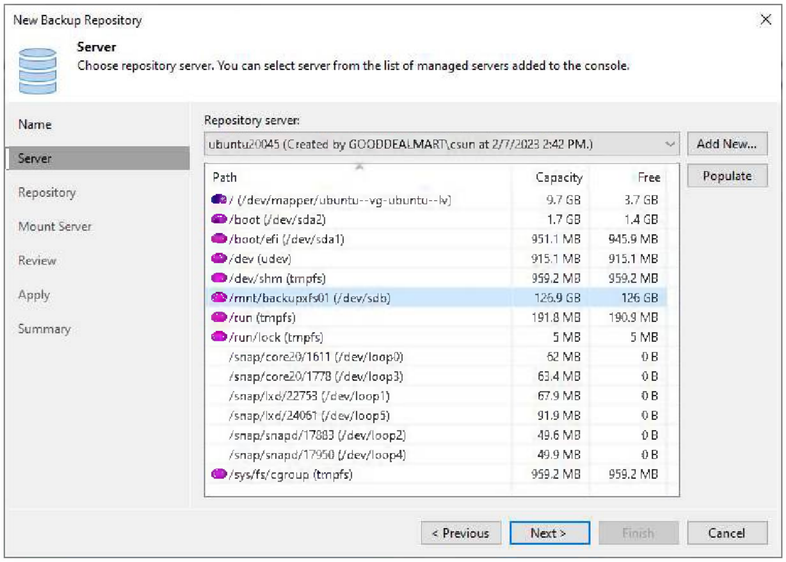
Description:
Created by GOODDEALMART\csun at 2/7/2023 2:57 PM

10. On the Server page, select the Linux server from the Repository server drop-down list and click Populate.



Repository server:
ubuntu20045 (Created by GOODDEALMART\csun at 2/7/2023 2:42 PM.)

11. Select the disk and click Next.



New Backup Repository

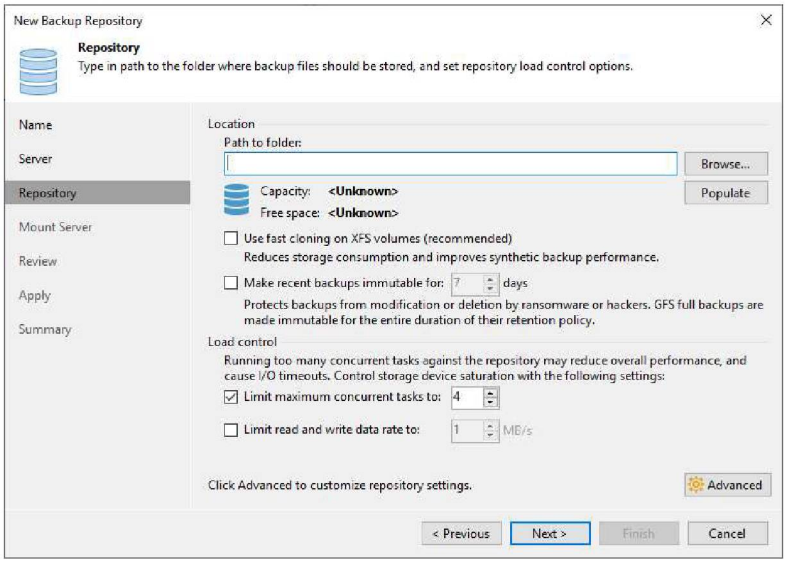
Server

Choose repository server. You can select server from the list of managed servers added to the console.

Repository server: ubuntu20045 (Created by GOODDEALMART\csun at 2/7/2023 2:42 PM.)

Path	Capacity	Free
/ (/dev/mapper/ubuntu--vg-ubuntu--lv)	9.7 GB	3.7 GB
/boot (/dev/sda2)	1.7 GB	1.4 GB
/boot/efi (/dev/sda1)	951.1 MB	945.9 MB
/dev (udev)	915.1 MB	915.1 MB
/dev/shm (tmpfs)	959.2 MB	959.2 MB
/mnt/backupxfs01 (/dev/sdb)	126.9 GB	126 GB
/run (tmpfs)	191.8 MB	190.9 MB
/run/lock (tmpfs)	5 MB	5 MB
/snap/core20/1611 (/dev/loop0)	62 MB	0 B
/snap/core20/1778 (/dev/loop3)	63.4 MB	0 B
/snap/lxd/22753 (/dev/loop1)	67.9 MB	0 B
/snap/lxd/24061 (/dev/loop5)	91.9 MB	0 B
/snap/snapd/17883 (/dev/loop2)	49.6 MB	0 B
/snap/snapd/17950 (/dev/loop4)	49.9 MB	0 B
/sys/fs/cgroup (tmpfs)	959.2 MB	959.2 MB

12. On the Repository page, click Browser for Path to folder.



New Backup Repository

Repository

Type in path to the folder where backup files should be stored, and set repository load control options.

Location

Path to folder:

Capacity: **<Unknown>**

Free space: **<Unknown>**

☐ Use fast cloning on XFS volumes (recommended)

Reduces storage consumption and improves synthetic backup performance.

☐ Make recent backups immutable for: 7 days

Protects backups from modification or deletion by ransomware or hackers. GFS full backups are made immutable for the entire duration of their retention policy.

Load control

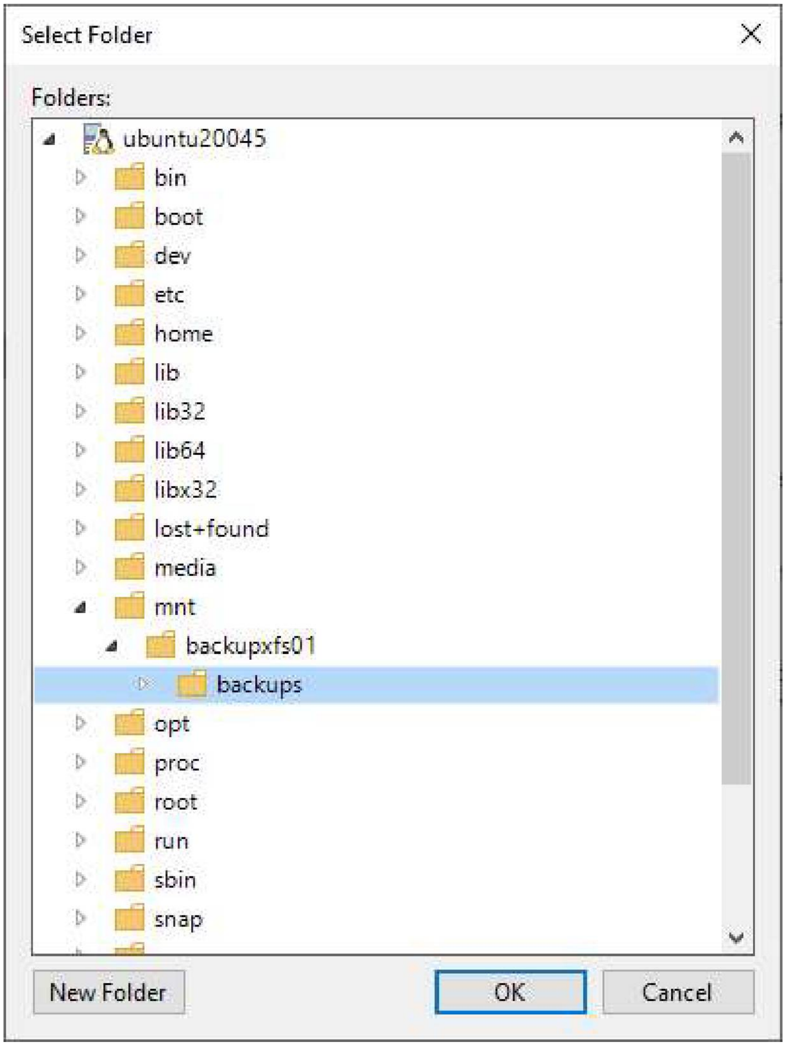
Running too many concurrent tasks against the repository may reduce overall performance, and cause I/O timeouts. Control storage device saturation with the following settings:

☑ Limit maximum concurrent tasks to: 4

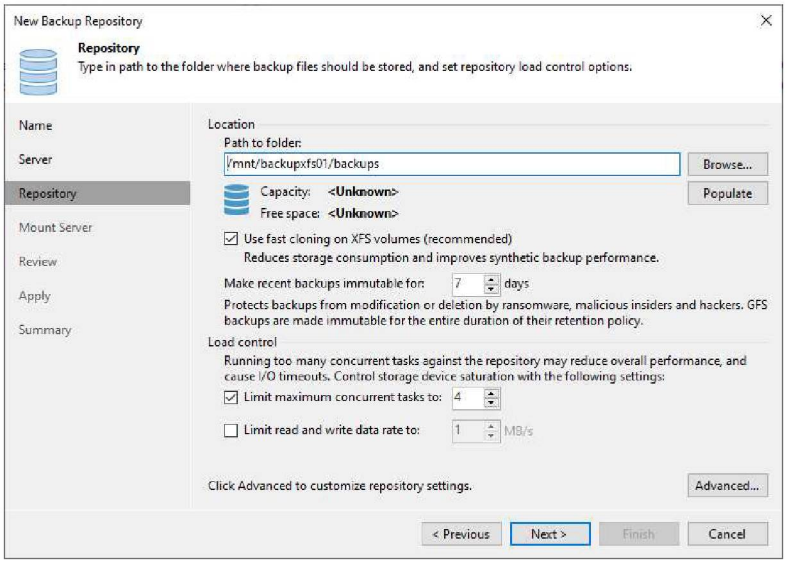
☐ Limit read and write data rate to: 1 MB/s

Click Advanced to customize repository settings.

13. On the Select Folder page, expand the server.
14. Select the backup folder and click OK.



15. On the Repository page, click Populate.



New Backup Repository

Repository

Type in path to the folder where backup files should be stored, and set repository load control options.

Location

Path to folder: /mnt/backupxfs01/backups

Capacity: **<Unknown>**

Free space: **<Unknown>**

☑ Use fast cloning on XFS volumes (recommended)

Reduces storage consumption and improves synthetic backup performance.

Make recent backups immutable for: 7 days

Protects backups from modification or deletion by ransomware, malicious insiders and hackers. GFS backups are made immutable for the entire duration of their retention policy.

Load control

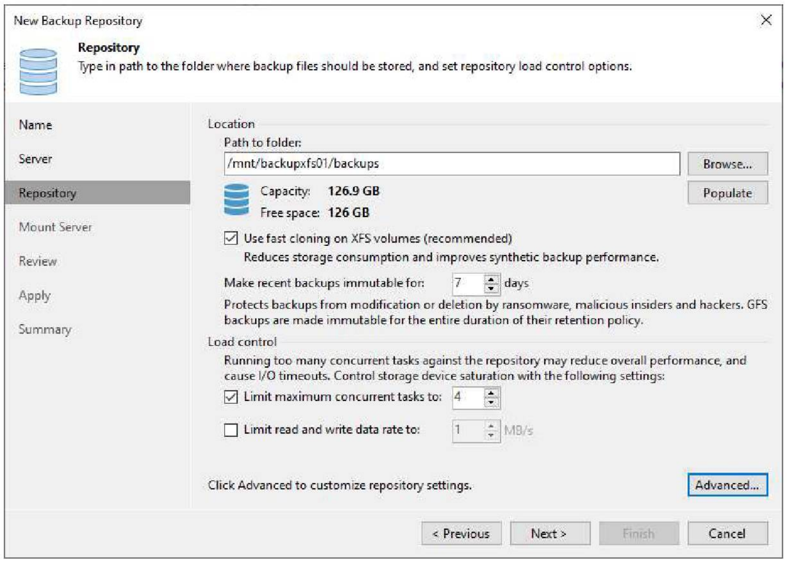
Running too many concurrent tasks against the repository may reduce overall performance, and cause I/O timeouts. Control storage device saturation with the following settings:

☑ Limit maximum concurrent tasks to: 4

☐ Limit read and write data rate to: 1 MB/s

Click Advanced to customize repository settings.

16. On the Repository page, select Use fast closing on XFS volumes.
17. Select Make recent backup immutable for 7 days. After that, it depends on your requirement.
18. Use the Load control settings to manage the load on the backup repository and avoid storage I/O timeouts.
19. Click Advanced.



New Backup Repository

Repository

Type in path to the folder where backup files should be stored, and set repository load control options.

Location

Path to folder: /mnt/backupxfs01/backups

Capacity: **126.9 GB**

Free space: **126 GB**

☑ Use fast cloning on XFS volumes (recommended)

Reduces storage consumption and improves synthetic backup performance.

Make recent backups immutable for: 7 days

Protects backups from modification or deletion by ransomware, malicious insiders and hackers. GFS backups are made immutable for the entire duration of their retention policy.

Load control

Running too many concurrent tasks against the repository may reduce overall performance, and cause I/O timeouts. Control storage device saturation with the following settings:

☑ Limit maximum concurrent tasks to: 4

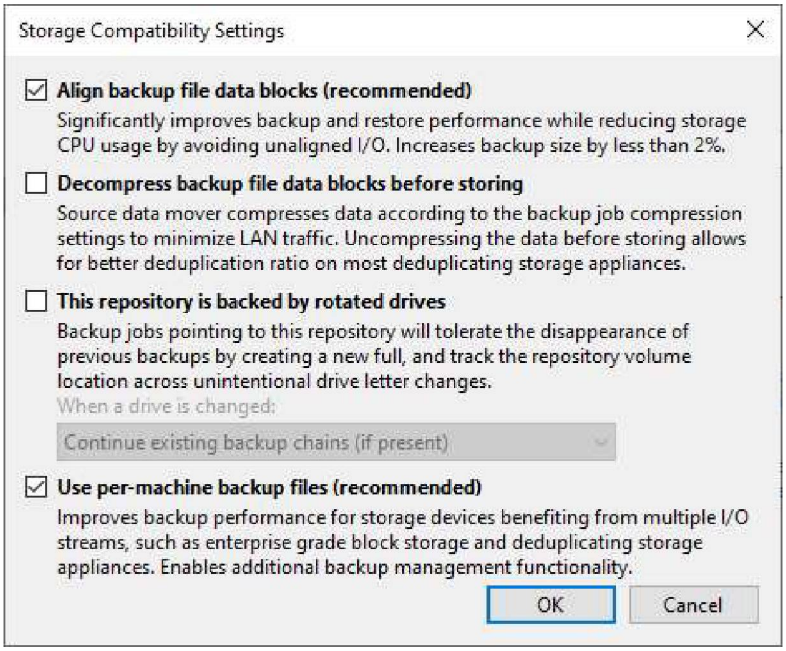
☐ Limit read and write data rate to: 1 MB/s

Click Advanced to customize repository settings.

20. On the Storage Compatibility Settings, select Align backup file data blocks (recommended) checkbox
21. Select Use per-machine backup files and click OK.

Note:

Select Decompress backup file data blocks before storing if you use a deduplicating storage feature or appliance.



Storage Compatibility Settings

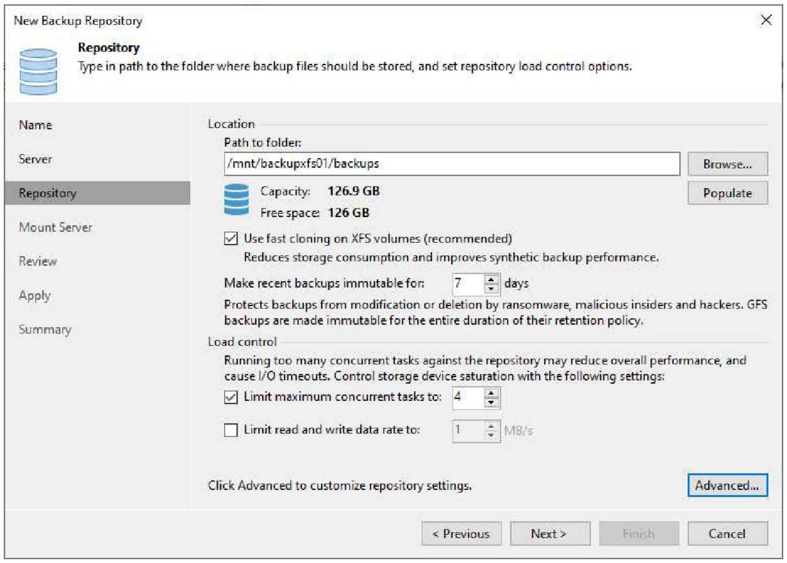
☑ **Align backup file data blocks (recommended)**
Significantly improves backup and restore performance while reducing storage CPU usage by avoiding unaligned I/O. Increases backup size by less than 2%.

□ **Decompress backup file data blocks before storing**
Source data mover compresses data according to the backup job compression settings to minimize LAN traffic. Uncompressing the data before storing allows for better deduplication ratio on most deduplicating storage appliances.

□ **This repository is backed by rotated drives**
Backup jobs pointing to this repository will tolerate the disappearance of previous backups by creating a new full, and track the repository volume location across unintentional drive letter changes.
When a drive is changed:
Continue existing backup chains (if present)

☑ **Use per-machine backup files (recommended)**
Improves backup performance for storage devices benefiting from multiple I/O streams, such as enterprise grade block storage and deduplicating storage appliances. Enables additional backup management functionality.

22. On the Repository page, click Next.



New Backup Repository

Repository
Type in path to the folder where backup files should be stored, and set repository load control options.

Location
Path to folder: /mnt/backupxfs01/backups
Capacity: **126.9 GB**
Free space: **126 GB**

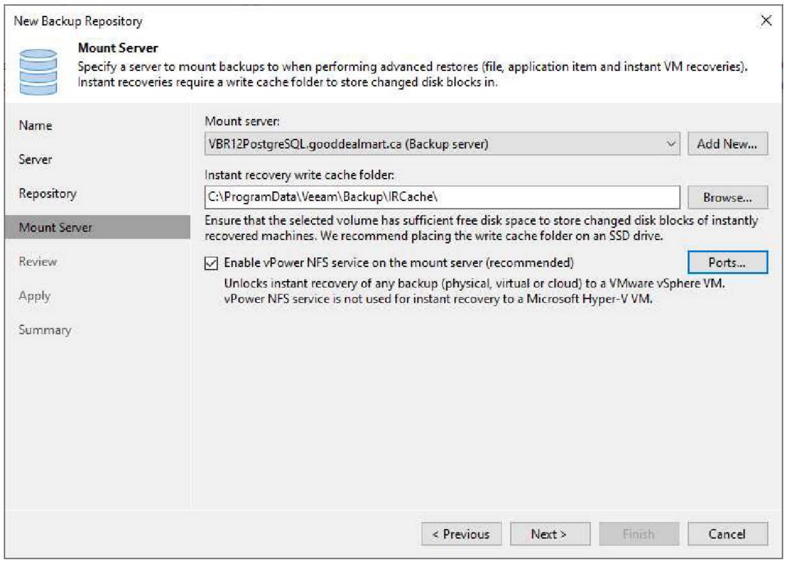
☑ Use fast cloning on XFS volumes (recommended)
Reduces storage consumption and improves synthetic backup performance.

Make recent backups immutable for: 7 days
Protects backups from modification or deletion by ransomware, malicious insiders and hackers. GFS backups are made immutable for the entire duration of their retention policy.

Load control
Running too many concurrent tasks against the repository may reduce overall performance, and cause I/O timeouts. Control storage device saturation with the following settings:
☑ Limit maximum concurrent tasks to: 4
□ Limit read and write data rate to: 1 MB/s

Click Advanced to customize repository settings.

23. Select a mount server from the Mount server drop-down list on the Mount Server page.
24. Select a folder in the Instant recovery write cache folder field for writing cache during mount operations.
25. Select Enable vPower NFS service on the mount server (recommend) and click Ports.


New Backup Repository

Mount Server

Specify a server to mount backups to when performing advanced restores (file, application item and instant VM recoveries). Instant recoveries require a write cache folder to store changed disk blocks in.

Mount server: VBR12PostgreSQL.gooddealmart.ca (Backup server)

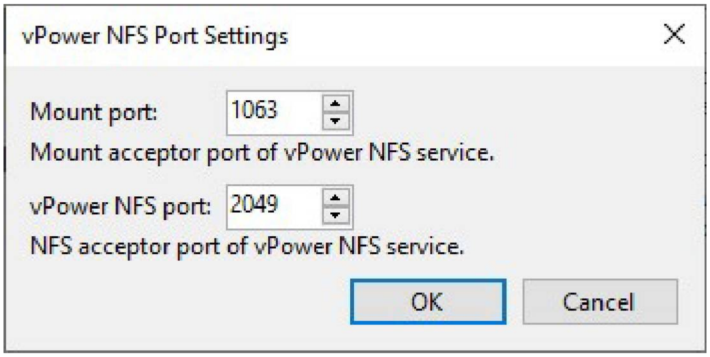
Instant recovery write cache folder: C:\ProgramData\Veeam\Backup\IRCache\

Ensure that the selected volume has sufficient free disk space to store changed disk blocks of instantly recovered machines. We recommend placing the write cache folder on an SSD drive.

☑ Enable vPower NFS service on the mount server (recommended)

Unlocks instant recovery of any backup (physical, virtual or cloud) to a VMware vSphere VM. vPower NFS service is not used for instant recovery to a Microsoft Hyper-V VM.

26. Review the ports settings on the vPower NFS Port Settings page and click OK.


vPower NFS Port Settings

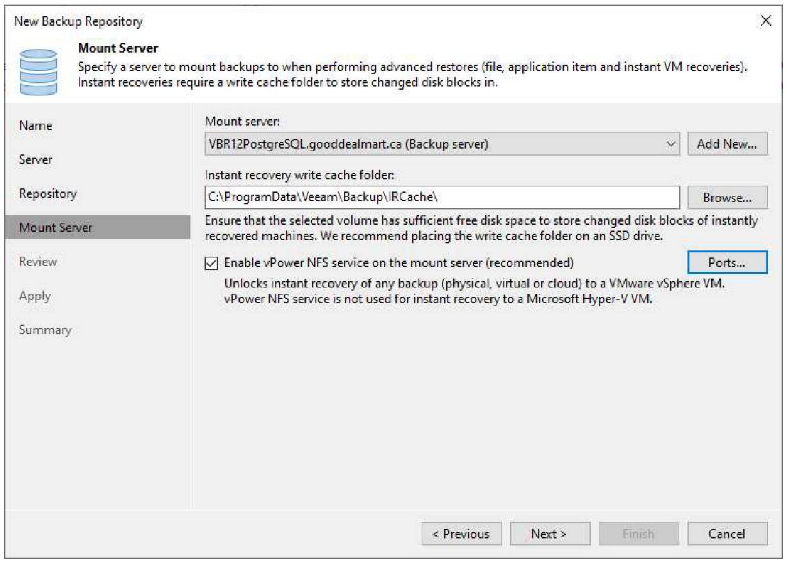
Mount port: 1063

Mount acceptor port of vPower NFS service.

vPower NFS port: 2049

NFS acceptor port of vPower NFS service.

27. Click Next on the Mount Server page.



New Backup Repository

Mount Server

Specify a server to mount backups to when performing advanced restores (file, application item and instant VM recoveries). Instant recoveries require a write cache folder to store changed disk blocks in.

Mount server: VBR12PostgreSQL.gooddealmart.ca (Backup server)

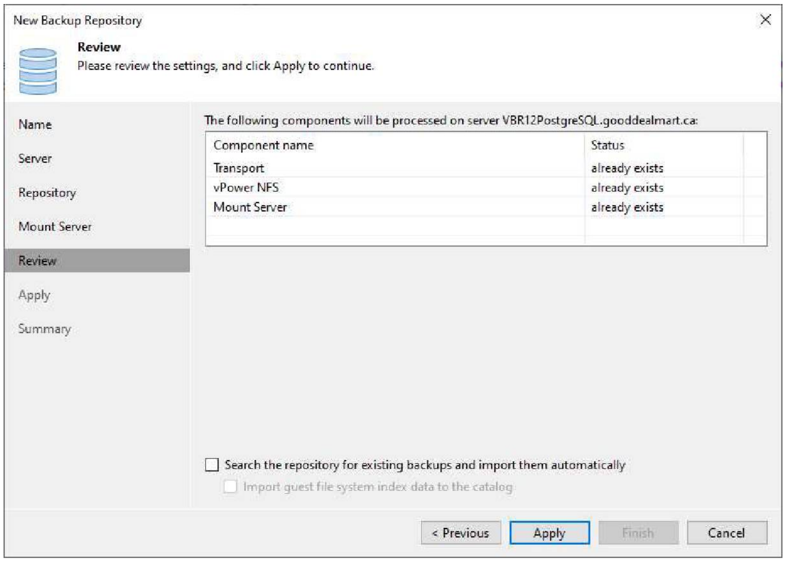
Instant recovery write cache folder: C:\ProgramData\Veeam\Backup\IRCache\

Ensure that the selected volume has sufficient free disk space to store changed disk blocks of instantly recovered machines. We recommend placing the write cache folder on an SSD drive.

☑ Enable vPower NFS service on the mount server (recommended)

Unlocks instant recovery of any backup (physical, virtual or cloud) to a VMware vSphere VM. vPower NFS service is not used for instant recovery to a Microsoft Hyper-V VM.

28. On the Review page, click Apply.
29. Select the Search the repository for existing backups and import them automatically checkbox if the backup repository contains backups previously created with Veeam Backup & Replication.
30. Select the Import guest file system index data to the catalog checkbox if the backup repository contains guest file system index files previously created by Veeam Backup & Replication.



New Backup Repository

Review

Please review the settings, and click Apply to continue.

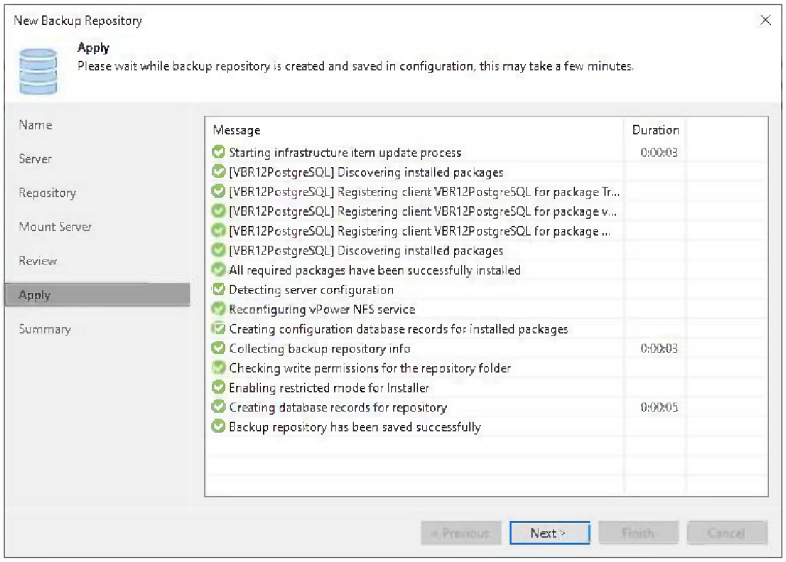
The following components will be processed on server VBR12PostgreSQL.gooddealmart.ca:

Component name	Status
Transport	already exists
vPower NFS	already exists
Mount Server	already exists

☐ Search the repository for existing backups and import them automatically

☐ Import guest file system index data to the catalog

31. Click Next on the Apply page.



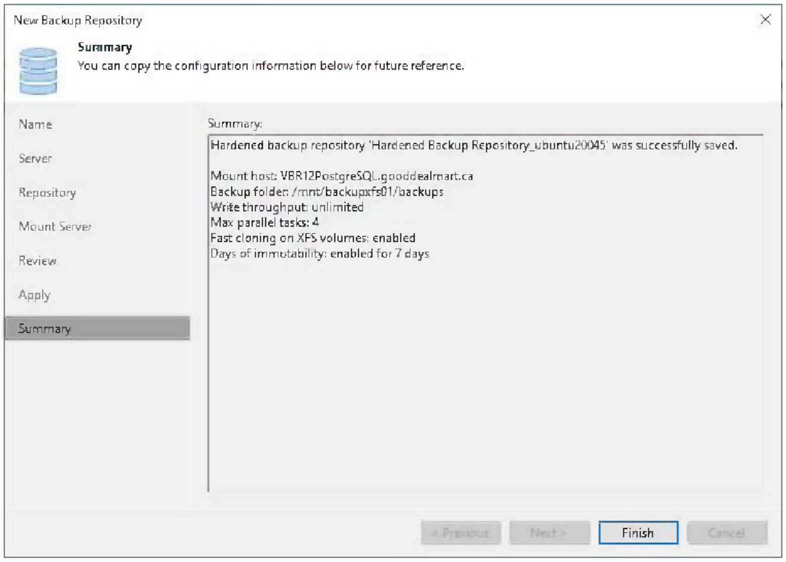
New Backup Repository

Apply

Please wait while backup repository is created and saved in configuration, this may take a few minutes.

Message	Duration
✓ Starting infrastructure item update process	0:00:03
✓ [VBR12PostgreSQL] Discovering installed packages	
✓ [VBR12PostgreSQL] Registering client VBR12PostgreSQL for package Tr...	
✓ [VBR12PostgreSQL] Registering client VBR12PostgreSQL for package v...	
✓ [VBR12PostgreSQL] Registering client VBR12PostgreSQL for package ...	
✓ [VBR12PostgreSQL] Discovering installed packages	
✓ All required packages have been successfully installed	
✓ Detecting server configuration	
✓ Reconfiguring vPower NFS service	
✓ Creating configuration database records for installed packages	
✓ Collecting backup repository info	0:00:03
✓ Checking write permissions for the repository folder	
✓ Enabling restricted mode for Installer	
✓ Creating database records for repository	0:00:05
✓ Backup repository has been saved successfully	

32. Click Finish on the Summary page.



New Backup Repository

Summary

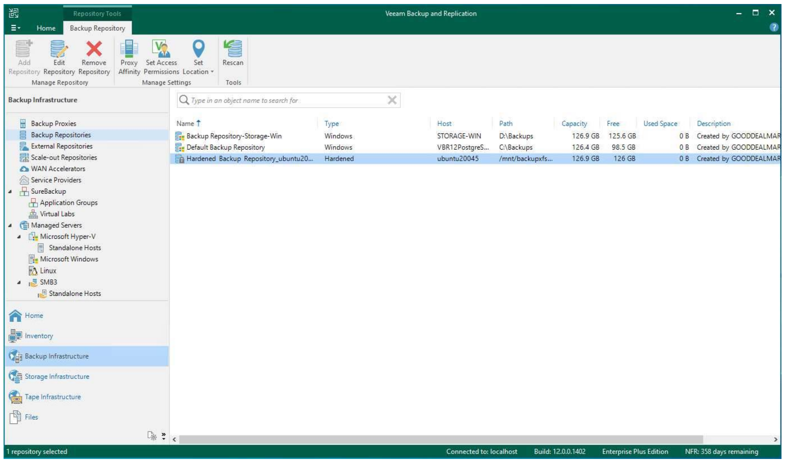
You can copy the configuration information below for future reference.

Summary:

Hardened backup repository 'Hardened Backup Repository_ubuntu20045' was successfully saved.

Mount host: VBR12PostgreSQL.gooddealmart.ca
Backup folder: /mnt/backupxfs01/backups
Write throughput: unlimited
Max parallel tasks: 4
Fast cloning on XFS volumes: enabled
Days of immutability: enabled for 7 days

33. Verify that the Hardened Backup Repository has been added.



Name	Type	Host	Path	Capacity	Free	Used Space	Description
Backup Repository-Storage-Win	Windows	STORAGE-WIN	D:\Backups	126.9 GB	125.6 GB	0 B	Created by GOODDEALMAR
Default Backup Repository	Windows	VBR12PostgreS...	C:\Backups	126.4 GB	98.5 GB	0 B	Created by GOODDEALMAR
Hardened Backup Repository_ubuntu20...	Hardened	ubuntu20045	/mnt/backupxfs...	126.9 GB	126 GB	0 B	Created by GOODDEALMAR

Add Network Attached Storage (SMB or CIFS Shares) as Backup Repository

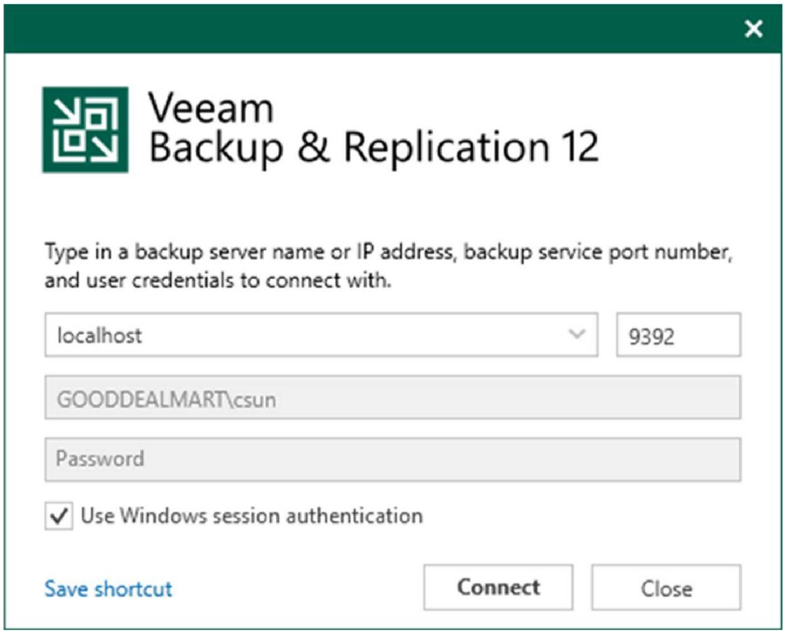
You can use network-attached storage (SMB or CIFS Shares) as backup repositories with Veeam Backup and Replication. A network-attached storage (NAS) device can be a shared folder on your computer or any other physical device accessed via the Server Message Block (SMB) protocol.

Note:

- You must deploy a gateway server because an SMB share cannot host Veeam Data Movers. However, Veeam Backup & Replication will automatically deploy a Veeam Data Mover on this gateway server.
- It is recommended that you deploy an additional gateway server in the remote site, closer to the SMB repository, if you plan to move VM data to an off-site SMB repository over a WAN link,

Instructions	Screenshot (if applicable)

1. Log in to the Veeam Backup and replication manager server.
2. Open the Veeam Backup & Replication Console and click Connect.



Type in a backup server name or IP address, backup service port number, and user credentials to connect with.

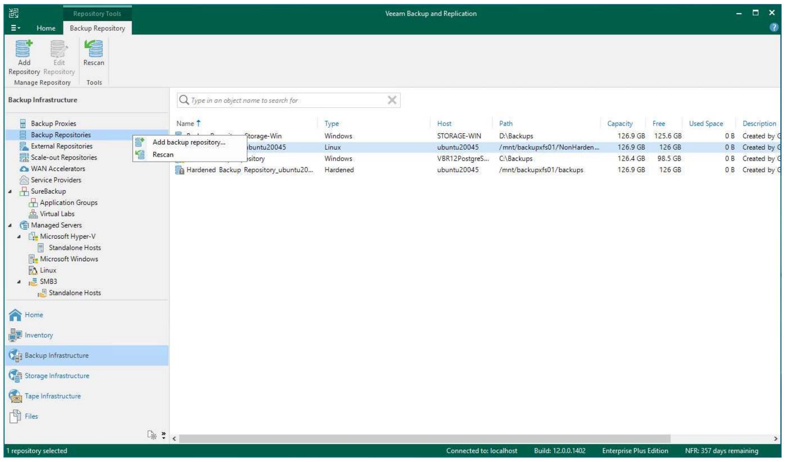
localhost | 9392

GOODDEALMART\csun

Password

☑ Use Windows session authentication

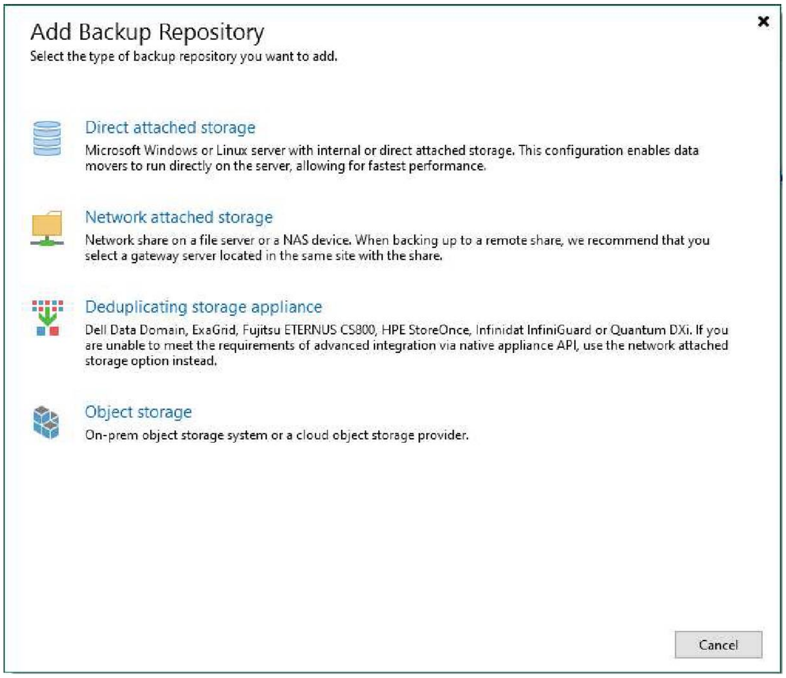
3. Select Backup Infrastructure on the Home page.
4. Select Backup Repositories on the Backup Infrastructure page.
5. Right-click Backup Repositories and select Add backup repository.



Name	Type	Host	Path	Capacity	Free	Used Space	Description
Storage-Win	Windows	STORAGE-WIN	D:\Backups	126.9 GB	125.6 GB	0 B	Created by G
buntu20045	Linux	ubuntu20045	/mnt/backupxfs01/NonHarden...	126.9 GB	126 GB	0 B	Created by G
sitory	Windows	VBR12PostgreS...	C:\Backups	126.4 GB	98.5 GB	0 B	Created by G
Hardened Backup Repository_ubuntu20...	Hardened	ubuntu20045	/mnt/backupxfs01/backups	126.9 GB	126 GB	0 B	Created by G

1 repository selected Connected to: localhost Build: 12.0.0.1402 Enterprise Plus Edition NFR: 357 days remaining

6. On the Add Backup Repository page, select Network attached storage.



Add Backup Repository

Select the type of backup repository you want to add.

Direct attached storage

Microsoft Windows or Linux server with internal or direct attached storage. This configuration enables data movers to run directly on the server, allowing for fastest performance.

Network attached storage

Network share on a file server or a NAS device. When backing up to a remote share, we recommend that you select a gateway server located in the same site with the share.

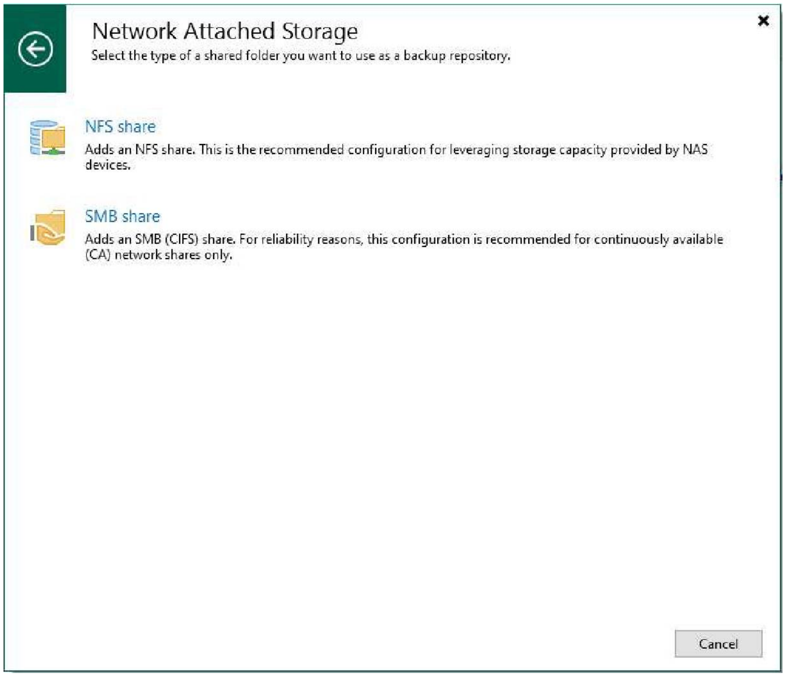
Deduplicating storage appliance

Dell Data Domain, ExaGrid, Fujitsu ETERNUS CS800, HPE StoreOnce, Infinidat InfiniGuard or Quantum DXi. If you are unable to meet the requirements of advanced integration via native appliance API, use the network attached storage option instead.

Object storage

On-prem object storage system or a cloud object storage provider.

7. Select SMB share on the Network Attached Storage.



Network Attached Storage

Select the type of a shared folder you want to use as a backup repository.

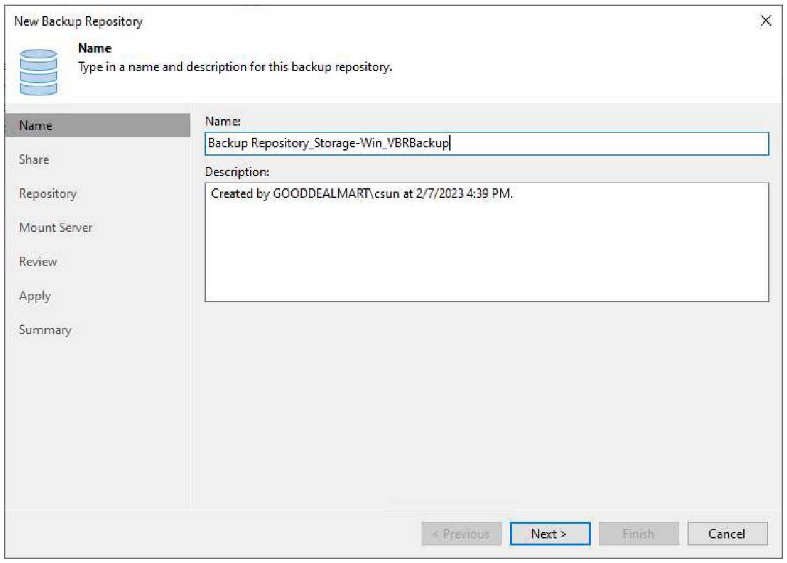
NFS share

Adds an NFS share. This is the recommended configuration for leveraging storage capacity provided by NAS devices.

SMB share

Adds an SMB (CIFS) share. For reliability reasons, this configuration is recommended for continuously available (CA) network shares only.

8. On the Name page, specify a Backup Repository name.
9. Give a brief description in the Description field for future reference and click Next.



New Backup Repository

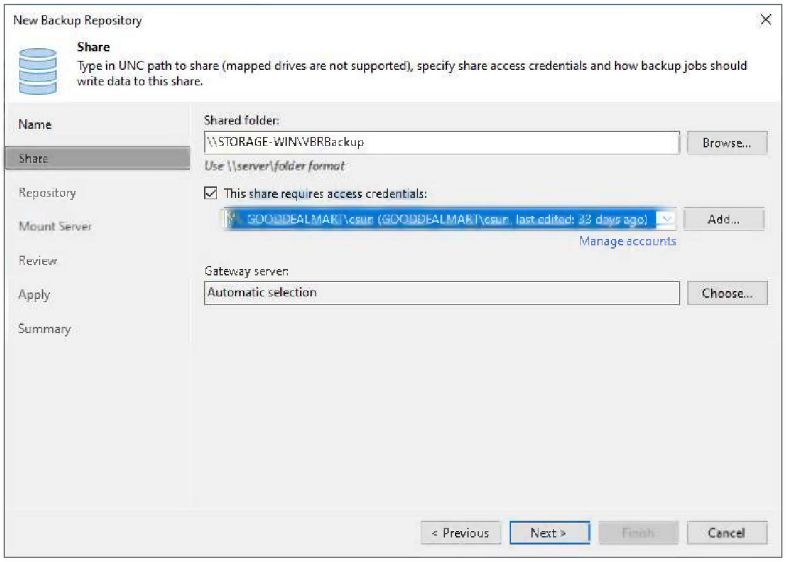
Name

Type in a name and description for this backup repository.

Name: Backup Repository_Storage-Win_VBRBackup

Description: Created by GOODDEALMART\csun at 2/7/2023 4:39 PM.

10. On the Share page, enter the share folder name in the Share folder field.
11. Select This share requires access credentials checkbox and select a credential from the drop-down list.
12. Select Automatic selection or click Choose to select the Gateway server.
13. Click Next.



New Backup Repository

Share

Type in UNC path to share (mapped drives are not supported), specify share access credentials and how backup jobs should write data to this share.

Shared folder: \\STORAGE-WIN\VBRBackup

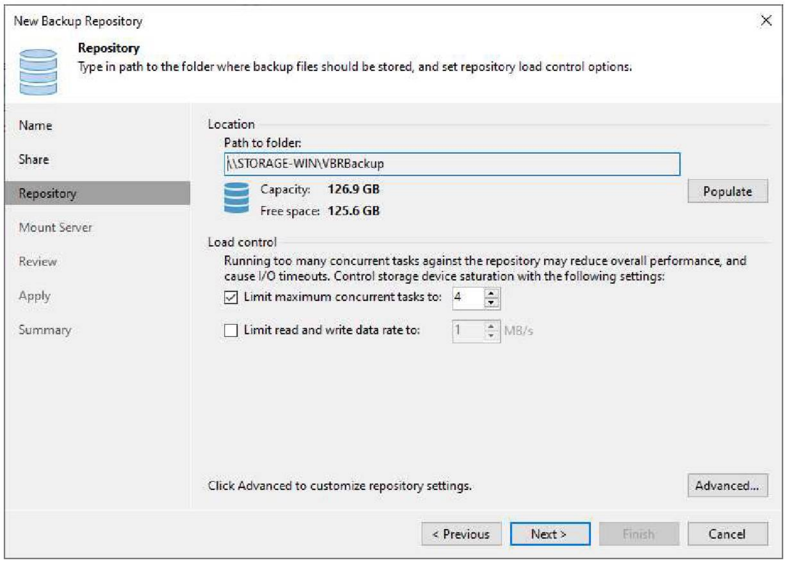
Use \\server\folder format

☑ This share requires access credentials:

GOODDEALMART\csun (GOODDEALMART\csun, last edited: 33 days ago)

Gateway server: Automatic selection

14. Use the Load control settings to manage the load on the backup repository and avoid storage I/O timeouts.
15. Click Advanced.



New Backup Repository

Repository

Type in path to the folder where backup files should be stored, and set repository load control options.

Location

Path to folder: \\STORAGE-WIN\VBRBackup

Capacity: **126.9 GB**

Free space: **125.6 GB**

Load control

Running too many concurrent tasks against the repository may reduce overall performance, and cause I/O timeouts. Control storage device saturation with the following settings:

☑ Limit maximum concurrent tasks to: 4

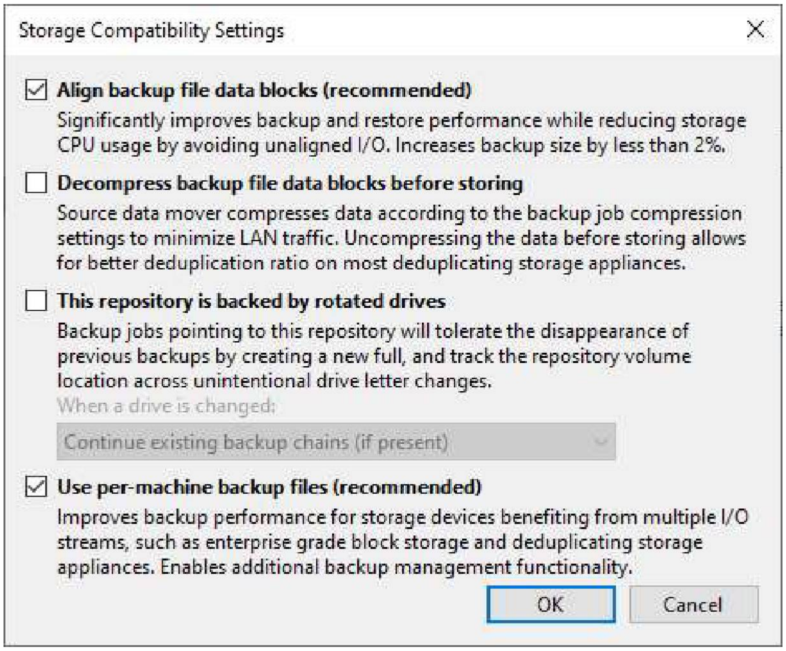
□ Limit read and write data rate to: 1 MB/s

Click Advanced to customize repository settings.

16. On the Storage Compatibility Settings, select Align backup file data blocks (recommended) checkbox
17. Select Use per-machine backup files and click OK.

Note:

Select Decompress backup file data blocks before storing if you use a deduplicating storage feature or appliance.



Storage Compatibility Settings

☑ **Align backup file data blocks (recommended)**

Significantly improves backup and restore performance while reducing storage CPU usage by avoiding unaligned I/O. Increases backup size by less than 2%.

□ **Decompress backup file data blocks before storing**

Source data mover compresses data according to the backup job compression settings to minimize LAN traffic. Uncompressing the data before storing allows for better deduplication ratio on most deduplicating storage appliances.

□ **This repository is backed by rotated drives**

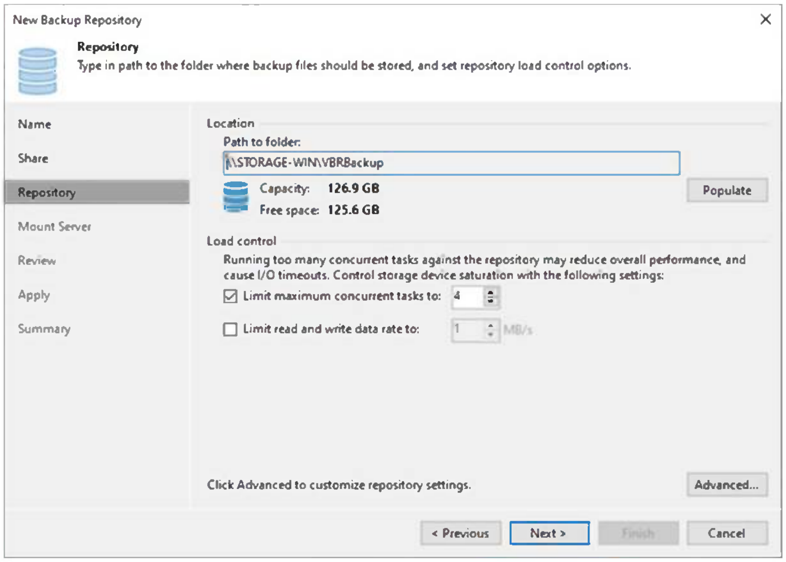
Backup jobs pointing to this repository will tolerate the disappearance of previous backups by creating a new full, and track the repository volume location across unintentional drive letter changes.

When a drive is changed: Continue existing backup chains (if present)

☑ **Use per-machine backup files (recommended)**

Improves backup performance for storage devices benefiting from multiple I/O streams, such as enterprise grade block storage and deduplicating storage appliances. Enables additional backup management functionality.

18. Click Next on the Repository page.



New Backup Repository

Repository

Type in path to the folder where backup files should be stored, and set repository load control options.

Location

Path to folder: \\STORAGE-WIN\VBRBackup

Capacity: 126.9 GB

Free space: 125.6 GB

Load control

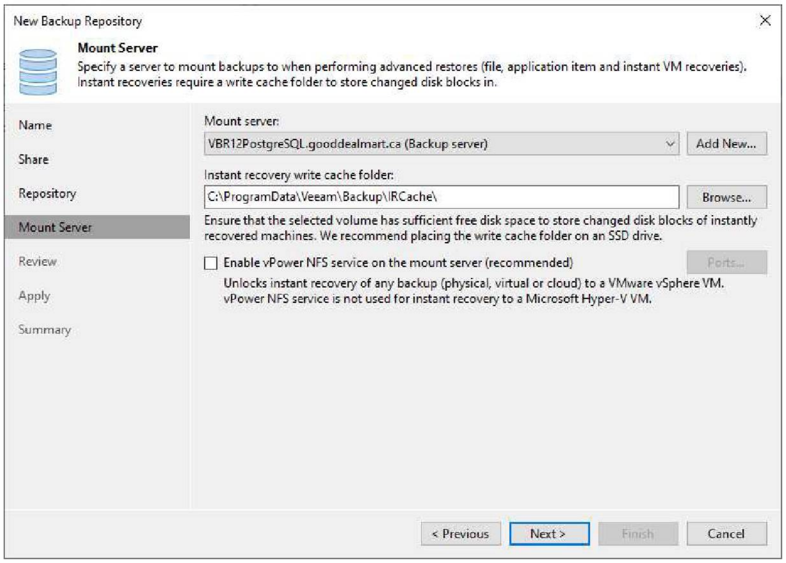
Running too many concurrent tasks against the repository may reduce overall performance, and cause I/O timeouts. Control storage device saturation with the following settings:

☑ Limit maximum concurrent tasks to: 4

☐ Limit read and write data rate to: 1 MB/s

Click Advanced to customize repository settings.

19. Select a mount server from the Mount server drop-down list on the Mount Server page.
20. Select a folder in the Instant recovery write cache folder field for writing cache during mount operations.
21. Unselect Enable vPower NFS service on the mount server because the vPower NFS service is not used for instant recovery to a Microsoft Hyper-V VM.
22. Click Next.



New Backup Repository

Mount Server

Specify a server to mount backups to when performing advanced restores (file, application item and instant VM recoveries). Instant recoveries require a write cache folder to store changed disk blocks in.

Mount server: VBR12PostgreSQL.gooddealmart.ca (Backup server)

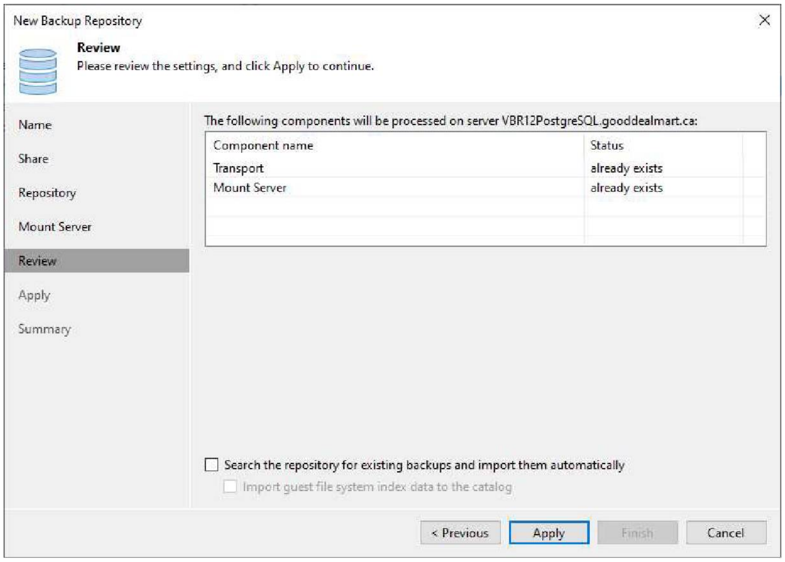
Instant recovery write cache folder: C:\ProgramData\Veeam\Backup\IRCache\

Ensure that the selected volume has sufficient free disk space to store changed disk blocks of instantly recovered machines. We recommend placing the write cache folder on an SSD drive.

☐ Enable vPower NFS service on the mount server (recommended)

Unlocks instant recovery of any backup (physical, virtual or cloud) to a VMware vSphere VM. vPower NFS service is not used for instant recovery to a Microsoft Hyper-V VM.

23. Click Apply on the Review page.
24. Select the Search the repository for existing backups and import them automatically checkbox if the backup repository contains backups previously created with Veeam Backup & Replication.
25. Select the Import guest file system index data to the catalog checkbox if the backup repository contains guest file system index files previously created by Veeam Backup & Replication.



Review

Please review the settings, and click Apply to continue.

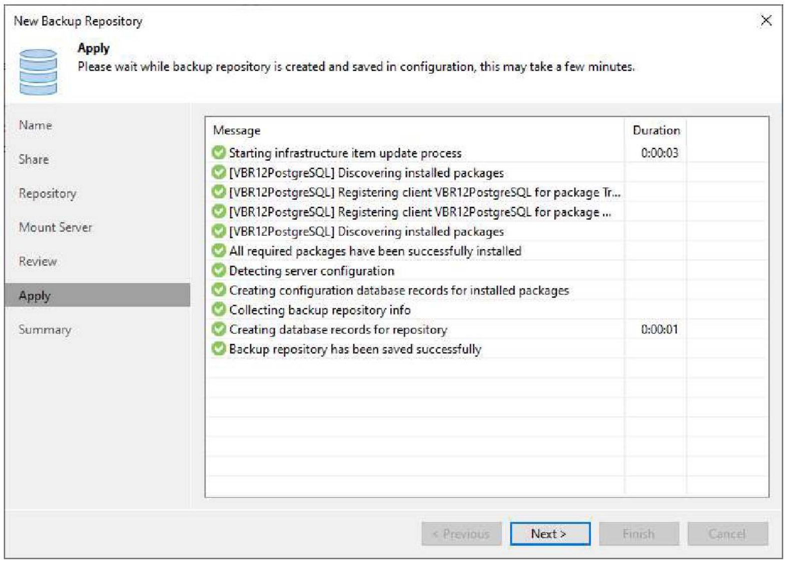
The following components will be processed on server VBR12PostgreSQL.gooddealmart.ca:

Component name	Status
Transport	already exists
Mount Server	already exists

□ Search the repository for existing backups and import them automatically

□ Import guest file system index data to the catalog

26. Click Next on the Apply page.

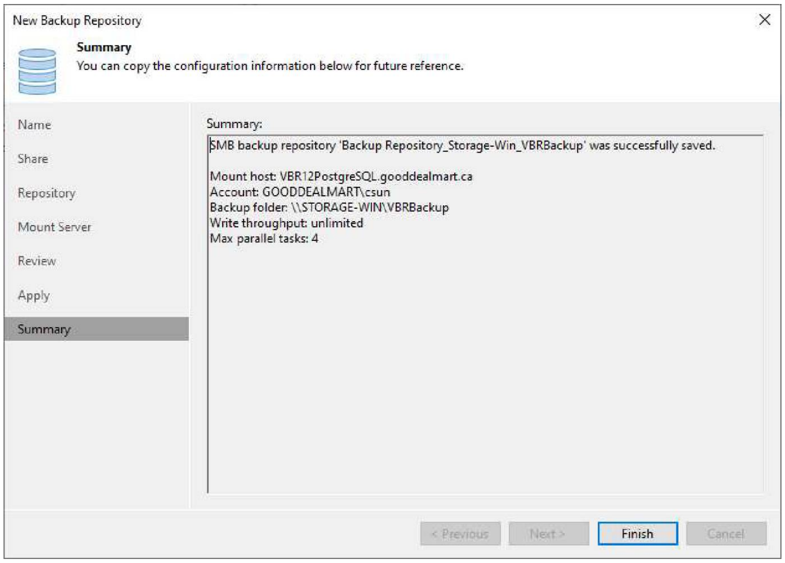


Apply

Please wait while backup repository is created and saved in configuration, this may take a few minutes.

Message	Duration
✓ Starting infrastructure item update process	0:00:03
✓ [VBR12PostgreSQL] Discovering installed packages	
✓ [VBR12PostgreSQL] Registering client VBR12PostgreSQL for package Tr...	
✓ [VBR12PostgreSQL] Registering client VBR12PostgreSQL for package ...	
✓ [VBR12PostgreSQL] Discovering installed packages	
✓ All required packages have been successfully installed	
✓ Detecting server configuration	
✓ Creating configuration database records for installed packages	
✓ Collecting backup repository info	
✓ Creating database records for repository	0:00:01
✓ Backup repository has been saved successfully	

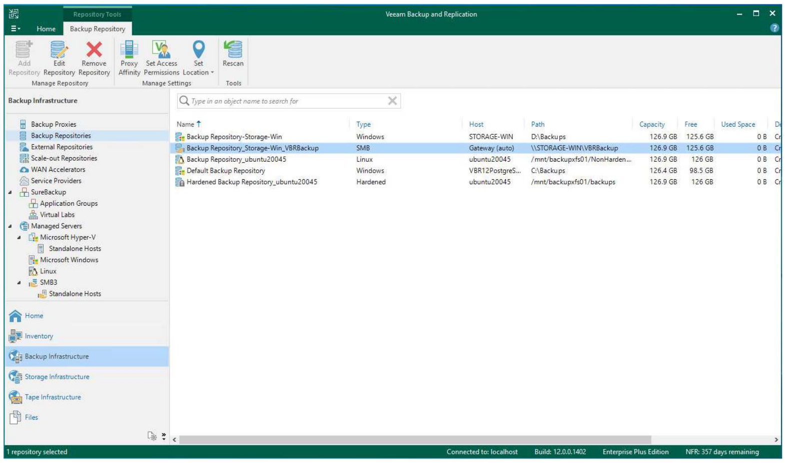
27. Click Finish on the Summary page.



Summary:

```
SMB backup repository 'Backup Repository_Storage-Win_VBRBackup' was successfully saved.

Mount host: VBR12PostgreSQL.gooddealmart.ca
Account: GOODDEALMART\csun
Backup folder: \\STORAGE-WIN\VBRBackup
Write throughput: unlimited
Max parallel tasks: 4
```

28. Verify that the Backup Repository has been added.



Name	Type	Host	Path	Capacity	Free	Used Space
Backup Repository-Storage-Win	Windows	STORAGE-WIN	D:\Backups	126.9 GB	125.6 GB	0 B
Backup Repository_Storage-Win_VBRBackup	SMB	Gateway (auto)	\\STORAGE-WIN\VBRBackup	126.9 GB	125.6 GB	0 B
Backup Repository_ubuntu20045	Linux	ubuntu20045	/mnt/backupxfs01/NonHarden...	126.9 GB	126 GB	0 B
Default Backup Repository	Windows	VBR12PostgreS...	C:\Backups	126.4 GB	98.5 GB	0 B
Hardened Backup Repository_ubuntu20045	Hardened	ubuntu20045	/mnt/backupxfs01/backups	126.9 GB	126 GB	0 B

1 repository selected
Connected to: localhost
Build: 12.0.0.1402
Enterprise Plus Edition
NFR: 357 days remaining

Add the Microsoft Windows server’s Rotated Drives as a Backup Repository

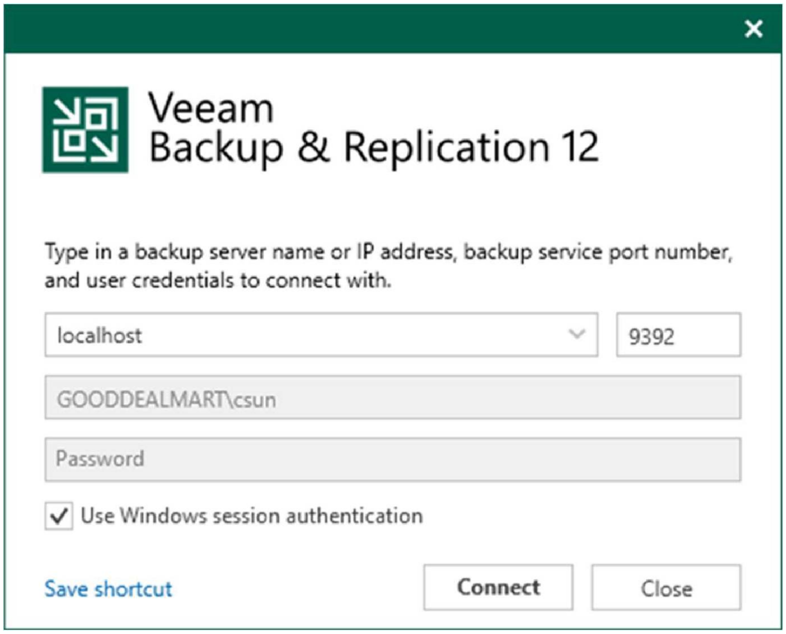
This scenario is helpful if you want to store backups on multiple external hard drives that you intend to move between locations. The drives that are rotated can be detachable USB or eSATA hard drives.

There are some limitations as below:

- Only one repository with rotated drives can be created on a single managed server.
- You cannot store archive full backups (GFS backups) created with backup jobs or backup copy jobs in backup repositories with a rotated drive.
- You cannot store per-machine backup files in backup repositories with rotated drives.
- You cannot rescan backup repositories with rotated drives.
- Scale-out backup repositories do not support rotated drives.
- Repositories with rotated drives are not supported as primary backup repositories, archive repositories, and secondary target repositories for NAS backup.

Instructions	Screenshot (if applicable)

1. Log in to the Veeam Backup and replication manager server.
2. Open the Veeam Backup & Replication Console and click Connect.



Veeam
Backup & Replication 12

Type in a backup server name or IP address, backup service port number, and user credentials to connect with.

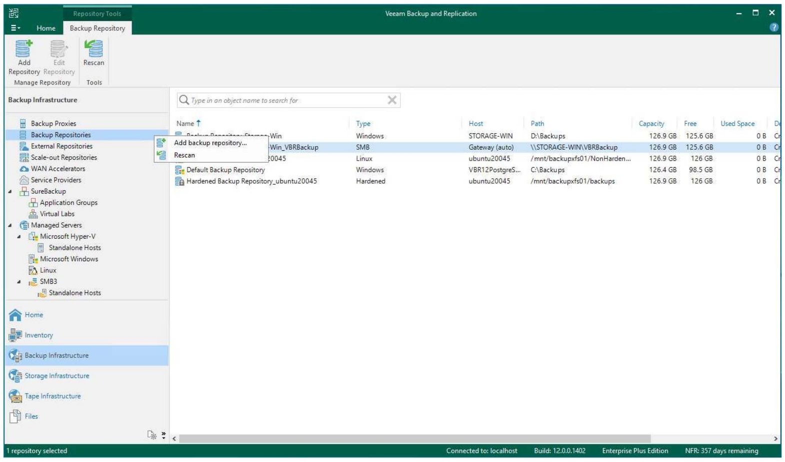
localhost 9392

GOODDEALMART\csun

Password

☑ Use Windows session authentication

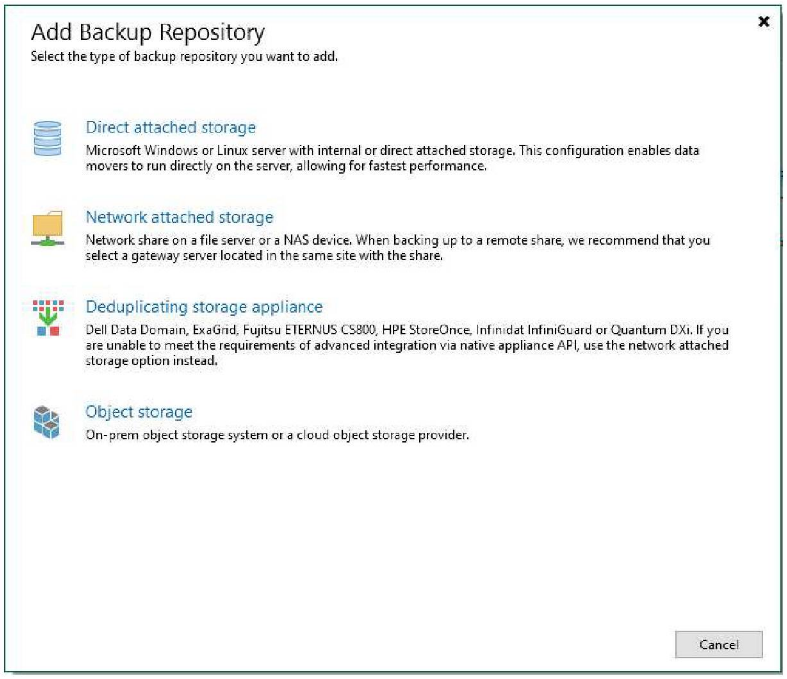
3. Select Backup Infrastructure on the Home page.
4. Select Backup Repositories on the Backup Infrastructure page.
5. Right-click Backup Repositories and select Add backup repository.



Name	Type	Host	Path	Capacity	Free	Used Space	De
Backup Repository Storage-Win	Windows	STORAGE-WIN	D:\Backups	126.9 GB	125.6 GB	0 B	Cr
-Win_VBRBackup	SMB	Gateway (auto)	\\STORAGE-WIN\VBRBackup	126.9 GB	125.6 GB	0 B	Cr
20045	Linux	ubuntu20045	/mnt/backupxfs01/NonHarden...	126.9 GB	126 GB	0 B	Cr
Default Backup Repository	Windows	VBR12PostgreS...	C:\Backups	126.4 GB	98.5 GB	0 B	Cr
Hardened Backup Repository_ubuntu20045	Hardened	ubuntu20045	/mnt/backupxfs01/backups	126.9 GB	126 GB	0 B	Cr

1 repository selected Connected to: localhost Build: 12.0.0.1402 Enterprise Plus Edition NFR: 357 days remaining

6. Select Direct attached storage on the Add Backup Repository page.



Add Backup Repository

Select the type of backup repository you want to add.

Direct attached storage

Microsoft Windows or Linux server with internal or direct attached storage. This configuration enables data movers to run directly on the server, allowing for fastest performance.

Network attached storage

Network share on a file server or a NAS device. When backing up to a remote share, we recommend that you select a gateway server located in the same site with the share.

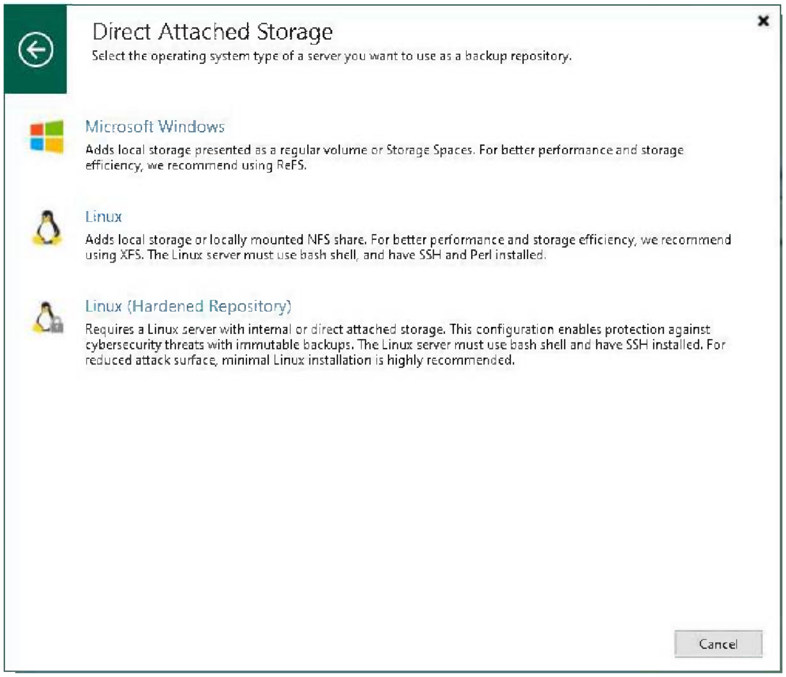
Deduplicating storage appliance

Dell Data Domain, ExaGrid, Fujitsu ETERNUS CS800, HPE StoreOnce, Infinidat InfiniGuard or Quantum DXi. If you are unable to meet the requirements of advanced integration via native appliance API, use the network attached storage option instead.

Object storage

On-prem object storage system or a cloud object storage provider.

7. Select Microsoft Windows on the Direct Attached Storage page.



Direct Attached Storage

Select the operating system type of a server you want to use as a backup repository.

Microsoft Windows

Adds local storage presented as a regular volume or Storage Spaces. For better performance and storage efficiency, we recommend using ReFS.

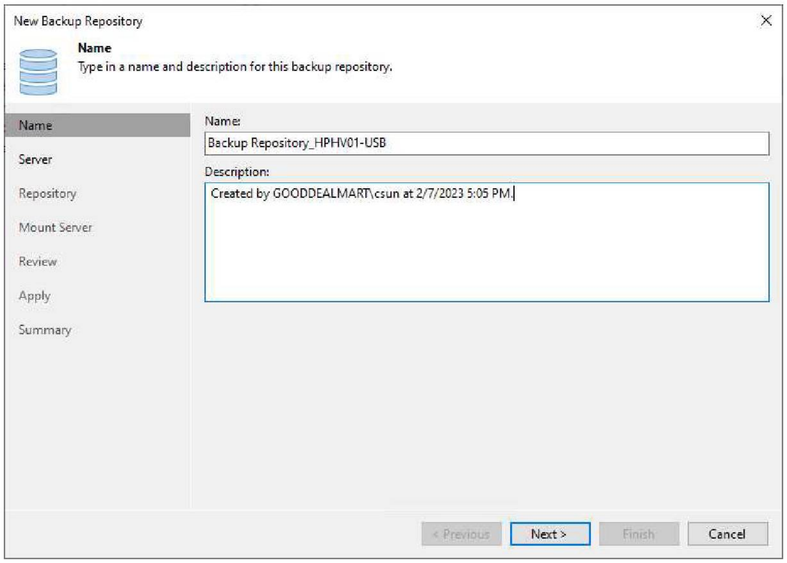
Linux

Adds local storage or locally mounted NFS share. For better performance and storage efficiency, we recommend using XFS. The Linux server must use bash shell, and have SSH and Perl installed.

Linux (Hardened Repository)

Requires a Linux server with internal or direct attached storage. This configuration enables protection against cybersecurity threats with immutable backups. The Linux server must use bash shell and have SSH installed. For reduced attack surface, minimal Linux installation is highly recommended.

8. On the Name page, specify a Backup Repository name.
9. Give a brief description in the Description field for future reference and click Next.

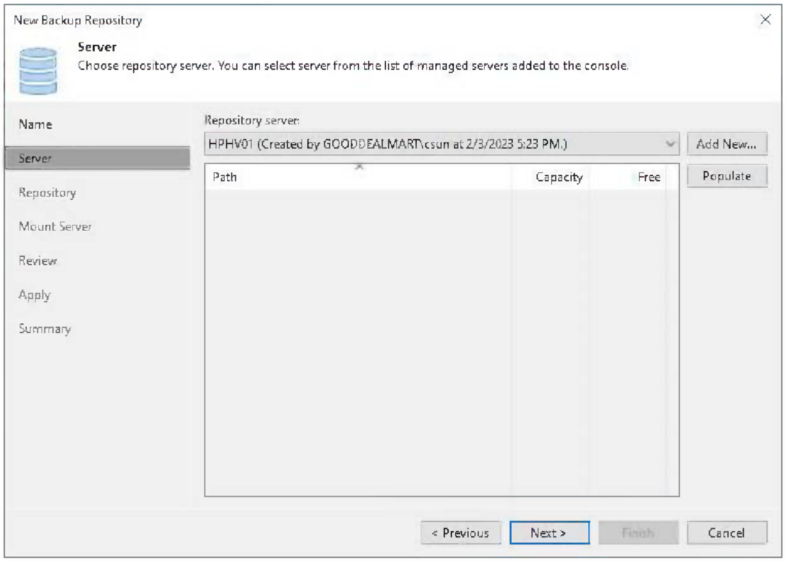


Type in a name and description for this backup repository.

Name: Backup Repository_HPHV01-USB

Description: Created by GOODDEALMART\csun at 2/7/2023 5:05 PM.

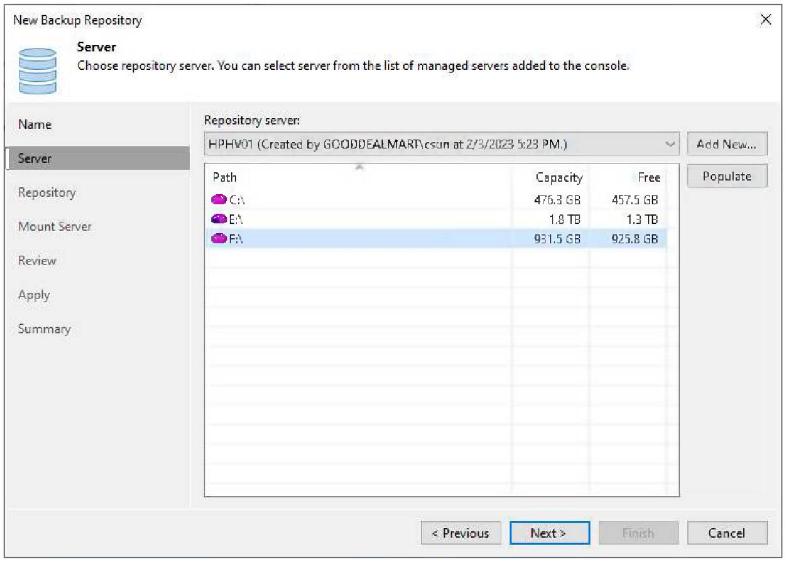
10. On the Server page, select the Microsoft Windows server from the Repository server drop-down list and click Populate.



Choose repository server. You can select server from the list of managed servers added to the console.

Repository server: HPHV01 (Created by GOODDEALMART\csun at 2/3/2023 5:23 PM.)

11. Select the disk and click Next.



New Backup Repository

Server

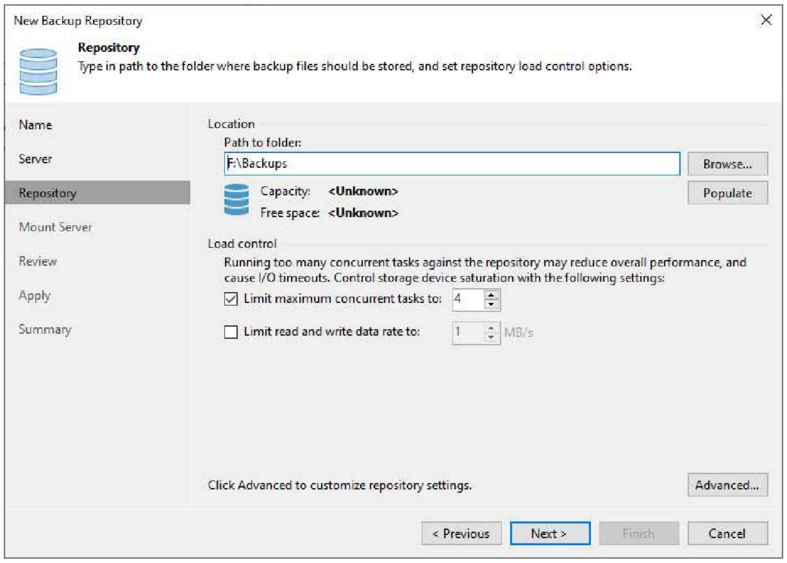
Choose repository server. You can select server from the list of managed servers added to the console.

Repository server:

HPHV01 (Created by GOODDEALMART\csun at 2/3/2023 5:23 PM.)

Path	Capacity	Free
C:\	476.3 GB	457.5 GB
E:\	1.8 TB	1.3 TB
F:\	931.5 GB	925.8 GB

12. On the Repository page, click Populate to review the disk capacity and free space.



New Backup Repository

Repository

Type in path to the folder where backup files should be stored, and set repository load control options.

Location

Path to folder:

F:\Backups

Capacity: **<Unknown>**

Free space: **<Unknown>**

Load control

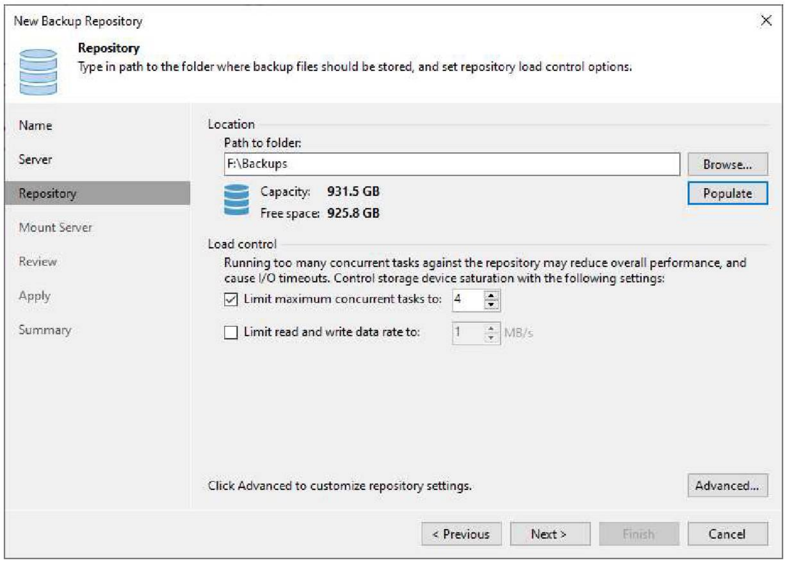
Running too many concurrent tasks against the repository may reduce overall performance, and cause I/O timeouts. Control storage device saturation with the following settings:

☑ Limit maximum concurrent tasks to: 4

☐ Limit read and write data rate to: 1 MB/s

Click Advanced to customize repository settings.

13. Use the Load control settings to manage the load on the backup repository and avoid storage I/O timeouts.
14. Click Advanced.



New Backup Repository

Repository
Type in path to the folder where backup files should be stored, and set repository load control options.

Location

Path to folder: F:\Backups

Capacity: 931.5 GB
Free space: 925.8 GB

Load control

Running too many concurrent tasks against the repository may reduce overall performance, and cause I/O timeouts. Control storage device saturation with the following settings:

☑ Limit maximum concurrent tasks to: 4

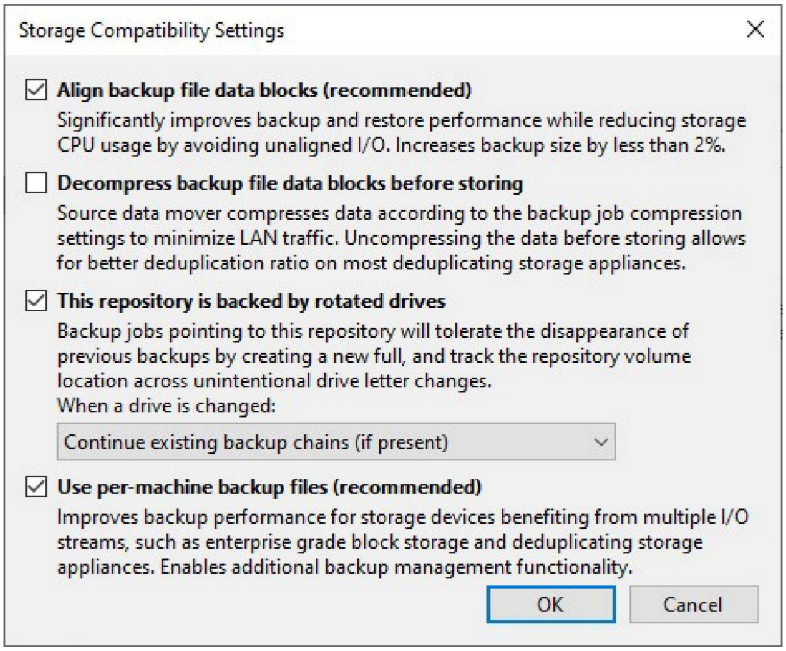
□ Limit read and write data rate to: 1 MB/s

Click Advanced to customize repository settings.

15. On the Storage Compatibility Settings, select Align backup file data blocks (recommended) checkbox
16. Select This repository is backed by rotated drives checkbox and Specify how Veeam Backup & Replication should react when a drive is swapped.
17. Select Use per-machine backup files and click OK.

Note:

Select Decompress backup file data blocks before storing if



Storage Compatibility Settings

☑ **Align backup file data blocks (recommended)**
Significantly improves backup and restore performance while reducing storage CPU usage by avoiding unaligned I/O. Increases backup size by less than 2%.

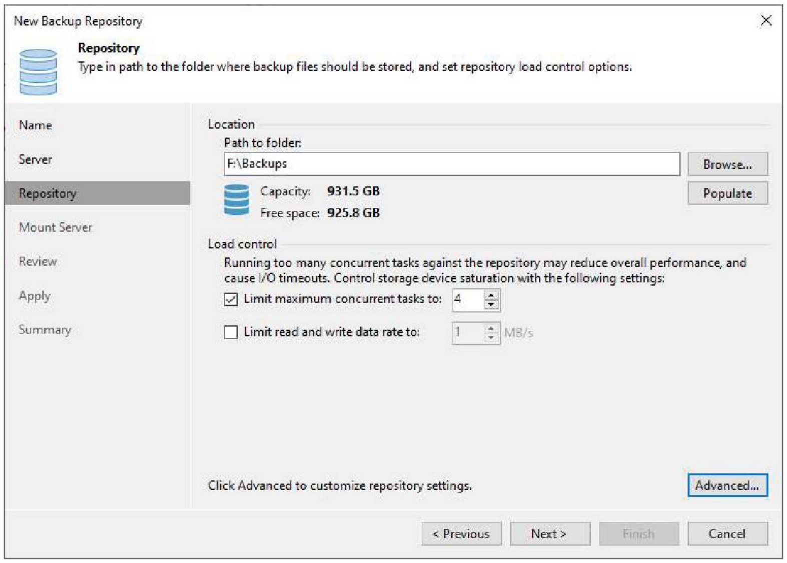
□ **Decompress backup file data blocks before storing**
Source data mover compresses data according to the backup job compression settings to minimize LAN traffic. Uncompressing the data before storing allows for better deduplication ratio on most deduplicating storage appliances.

☑ **This repository is backed by rotated drives**
Backup jobs pointing to this repository will tolerate the disappearance of previous backups by creating a new full, and track the repository volume location across unintentional drive letter changes.
When a drive is changed: Continue existing backup chains (if present)

☑ **Use per-machine backup files (recommended)**
Improves backup performance for storage devices benefiting from multiple I/O streams, such as enterprise grade block storage and deduplicating storage appliances. Enables additional backup management functionality.

you use a deduplicating storage feature or appliance.

18. Click Next on the Repository page.



Repository

Type in path to the folder where backup files should be stored, and set repository load control options.

Location

Path to folder: F:\Backups

Capacity: **931.5 GB**

Free space: **925.8 GB**

Load control

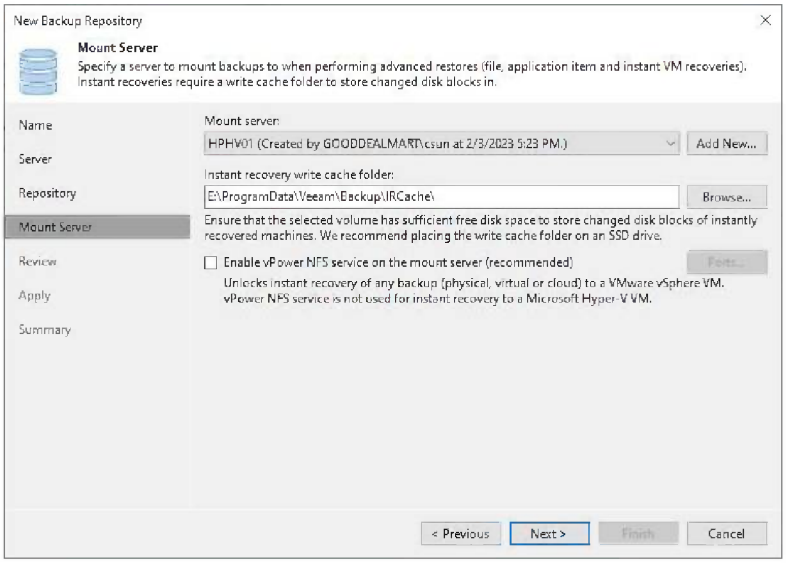
Running too many concurrent tasks against the repository may reduce overall performance, and cause I/O timeouts. Control storage device saturation with the following settings:

☑ Limit maximum concurrent tasks to: 4

□ Limit read and write data rate to: 1 MB/s

Click Advanced to customize repository settings.

19. Select a mount server from the Mount server drop-down list on the Mount Server page. The mount server is required for file-level and application items restoration.
20. Select a folder in the Instant recovery write cache folder field for writing cache during mount operations.
21. Unselect Enable vPower NFS service on the mount server because the



Mount Server

Specify a server to mount backups to when performing advanced restores (file, application item and instant VM recoveries). Instant recoveries require a write cache folder to store changed disk blocks in.

Mount server: HPHV01 (Created by GOODDEALMART\csun at 2/3/2023 5:23 PM.)

Instant recovery write cache folder: E:\ProgramData\Veeam\Backup\IRCache\

Ensure that the selected volume has sufficient free disk space to store changed disk blocks of instantly recovered machines. We recommend placing the write cache folder on an SSD drive.

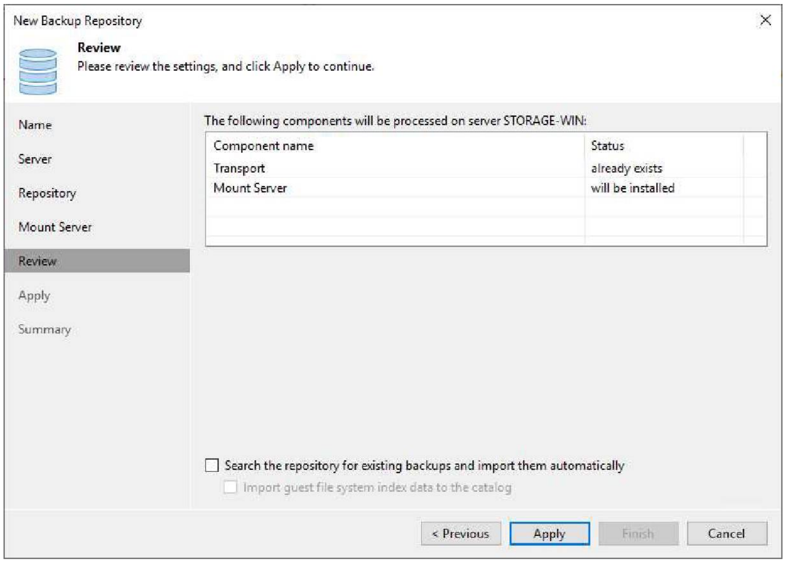
□ Enable vPower NFS service on the mount server (recommended)

Unlocks instant recovery of any backup (physical, virtual or cloud) to a VMware vSphere VM. vPower NFS service is not used for instant recovery to a Microsoft Hyper-V VM.

vPower NFS service is not used for instant recovery to a Microsoft Hyper-V VM.

22. Click Next.

23. Click Apply on the Review page.
24. Select the Search the repository for existing backups and import them automatically checkbox if the backup repository contains backups previously created with Veeam Backup & Replication.
25. Select the Import guest file system index data to the catalog checkbox if the backup repository contains guest file system index files previously created by Veeam Backup & Replication.



New Backup Repository

Review

Please review the settings, and click Apply to continue.

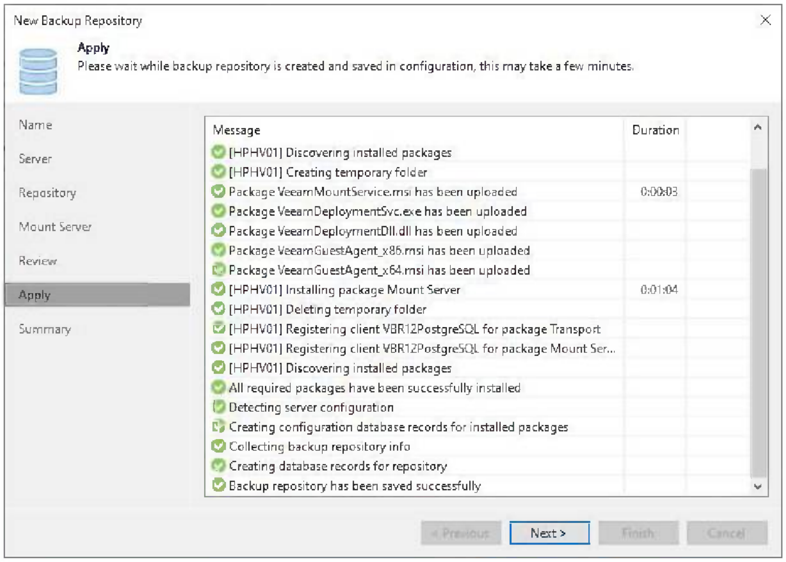
The following components will be processed on server STORAGE-WIN:

Component name	Status
Transport	already exists
Mount Server	will be installed

☐ Search the repository for existing backups and import them automatically

☐ Import guest file system index data to the catalog

26. Click Next on the Apply page.

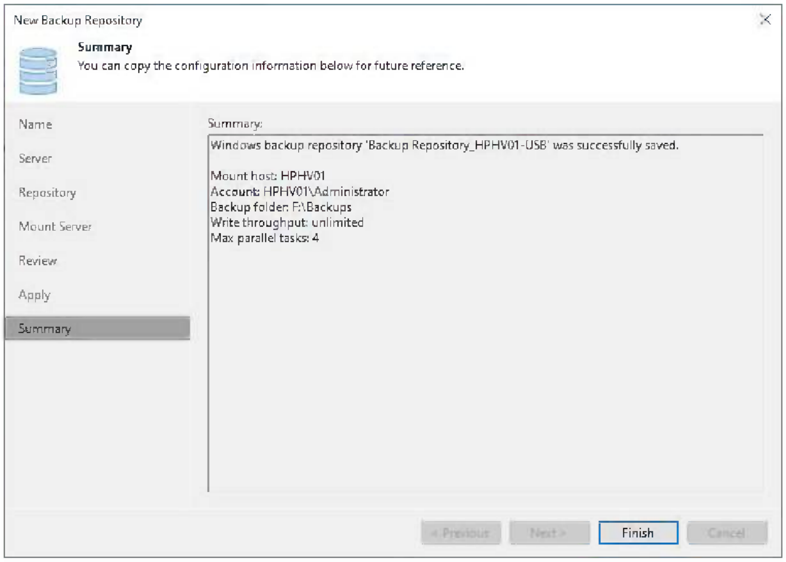


Apply

Please wait while backup repository is created and saved in configuration, this may take a few minutes.

Message	Duration
✓ [HPHV01] Discovering installed packages	
✓ [HPHV01] Creating temporary folder	
✓ Package VeeamMountService.msi has been uploaded	0:00:03
✓ Package VeeamDeploymentSvc.exe has been uploaded	
✓ Package VeeamDeploymentDll.dll has been uploaded	
✓ Package VeeamGuestAgent_x86.msi has been uploaded	
✓ Package VeeamGuestAgent_x64.msi has been uploaded	
✓ [HPHV01] Installing package Mount Server	0:01:04
✓ [HPHV01] Deleting temporary folder	
✓ [HPHV01] Registering client VBR12PostgreSQL for package Transport	
✓ [HPHV01] Registering client VBR12PostgreSQL for package Mount Ser...	
✓ [HPHV01] Discovering installed packages	
✓ All required packages have been successfully installed	
✓ Detecting server configuration	
✓ Creating configuration database records for installed packages	
✓ Collecting backup repository info	
✓ Creating database records for repository	
✓ Backup repository has been saved successfully	

27. Click Finish on the Summary page.



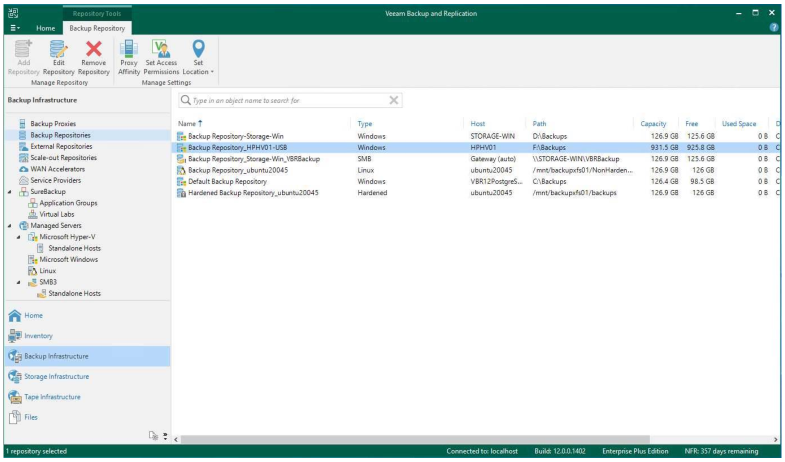
Summary

You can copy the configuration information below for future reference.

Summary:

```
Windows backup repository 'Backup Repository_HPHV01-USB' was successfully saved.

Mount host: HPHV01
Account: HPHV01\Administrator
Backup folder: F:\Backups
Write throughput: unlimited
Max parallel tasks: 4
```

28. Verify that the Rotated Drives Backup Repository has been added.

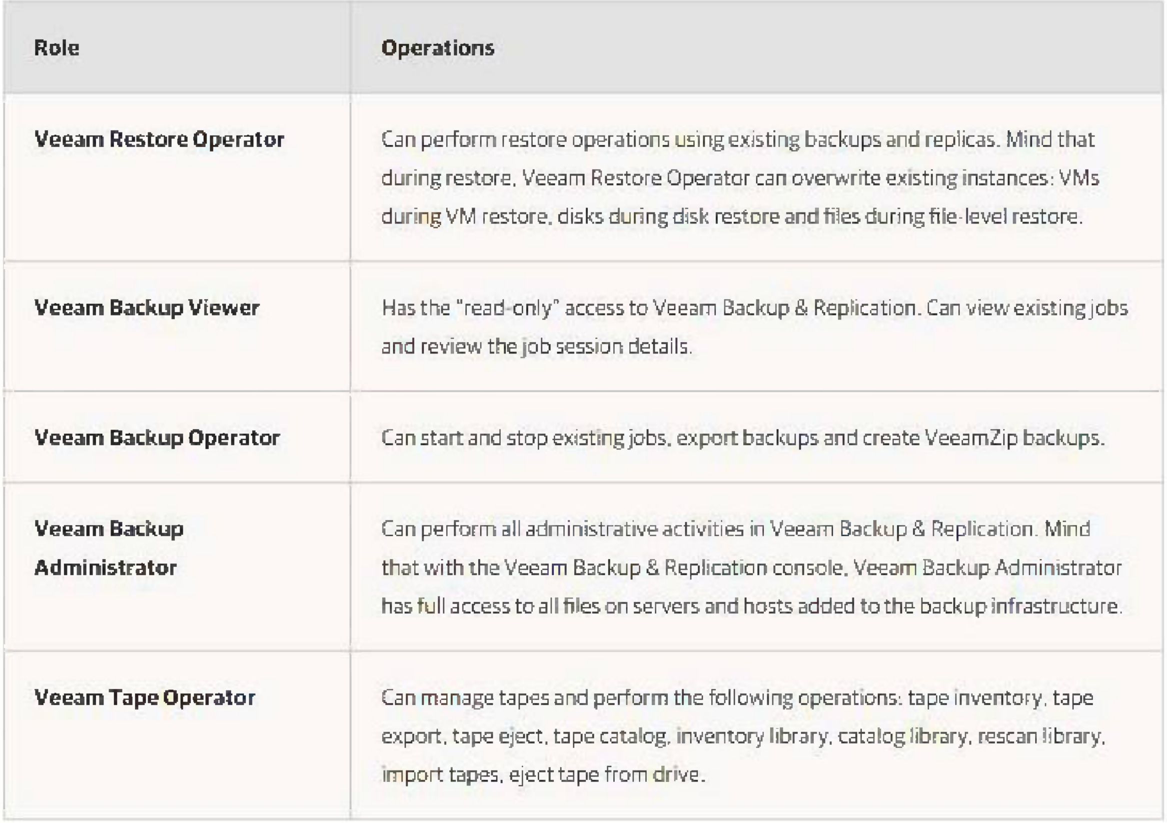


Name	Type	Host	Path	Capacity	Free	Used Space	D
Backup Repository-Storage-Win	Windows	STORAGE-WIN	D:\Backups	126.9 GB	125.6 GB	0 B	C
Backup Repository_HPHV01-USB	Windows	HPHV01	F:\Backups	931.5 GB	925.8 GB	0 B	C
Backup Repository_Storage-Win_VBRBackup	SMB	Gateway (auto)	\\STORAGE-WIN\VBRBackup	126.9 GB	125.6 GB	0 B	C
Backup Repository_ubuntu20045	Linux	ubuntu20045	/mnt/backupxfs01/NonHarden...	126.9 GB	126 GB	0 B	C
Default Backup Repository	Windows	VBR12PostgreS...	C:\Backups	126.4 GB	98.5 GB	0 B	C
Hardened Backup Repository_ubuntu20045	Hardened	ubuntu20045	/mnt/backupxfs01/backups	126.9 GB	126 GB	0 B	C

General and User Roles Settings

All jobs, backup infrastructure components, and other backup server-managed objects have general settings applied to them.

Users or groups who intend to work with Veeam Backup & Replication can be assigned one of the following roles.



Role	Operations
Veeam Restore Operator	Can perform restore operations using existing backups and replicas. Mind that during restore, Veeam Restore Operator can overwrite existing instances: VMs during VM restore, disks during disk restore and files during file-level restore.
Veeam Backup Viewer	Has the "read-only" access to Veeam Backup & Replication. Can view existing jobs and review the job session details.
Veeam Backup Operator	Can start and stop existing jobs, export backups and create VeeamZip backups.
Veeam Backup Administrator	Can perform all administrative activities in Veeam Backup & Replication. Mind that with the Veeam Backup & Replication console, Veeam Backup Administrator has full access to all files on servers and hosts added to the backup infrastructure.
Veeam Tape Operator	Can manage tapes and perform the following operations: tape inventory, tape export, tape eject, tape catalog, inventory library, catalog library, rescan library, import tapes, eject tape from drive.

Even if you exclude built-in administrator accounts (Domain\Administrator and Machine\Administrator) from all Veeam Backup & Replication roles, they have full access to Veeam Backup & Replication. So, for example, users added to the Administrators group will still have access to Veeam Backup & Replication if the Administrators group is removed from the Veeam Backup & Replication roles.

The Veeam Backup Administrator role must be assigned to the user account that runs the Veeam Backup Service. Users in the Administrators group are automatically assigned the Veeam Backup Administrator role during installation. If you change the default settings, ensure that you assign the appropriate user account as the Veeam Backup Administrator role. It is recommended that the Veeam Backup Administrator role be explicitly assigned to the user account rather than the group.

It is strongly advised to enable multi-factor authentication to protect administrator accounts from compromise (MFA).

If you enable MFA, remember that Veeam Backup & Replication must be run from the service account with MFA disabled.

Configure Multi-Factor Authentication for Users

Multi-factor authentication (MFA) is supported by Veeam Backup & Replication for additional user verification. A one-time password (OTP) generated in the mobile authenticator application is a secondary verification method. With login and password credentials, it creates a more secure environment and keeps user accounts safe.

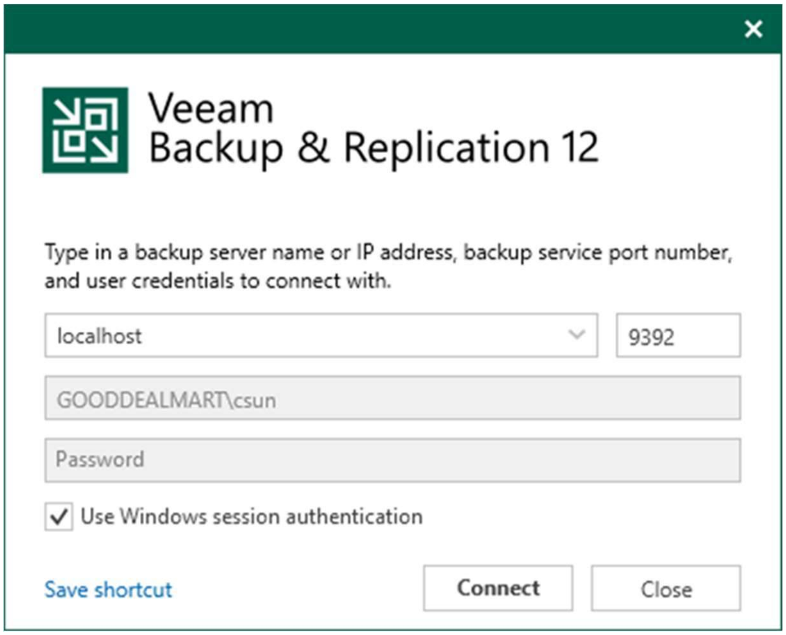
MFA has the following requirements and limitations:

- Users can only manage MFA with the Veeam Backup Administrator role.
- Veeam Backup & Replication Community Edition does not support MFA.
- Veeam Backup Enterprise Manager does not natively support MFA.
- User groups are not supported. You can enable MFA only for user accounts.
- MFA works only for interactive login.
- Push notifications for mobile devices are not supported. Only the mobile authenticator application provides an OTP code.

Instructions	Screenshot (if applicable)

1. Log in to the Veeam Backup and replication manager server.

2. Open the Veeam Backup & Replication Console and click Connect.



Veeam Backup & Replication 12

Type in a backup server name or IP address, backup service port number, and user credentials to connect with.

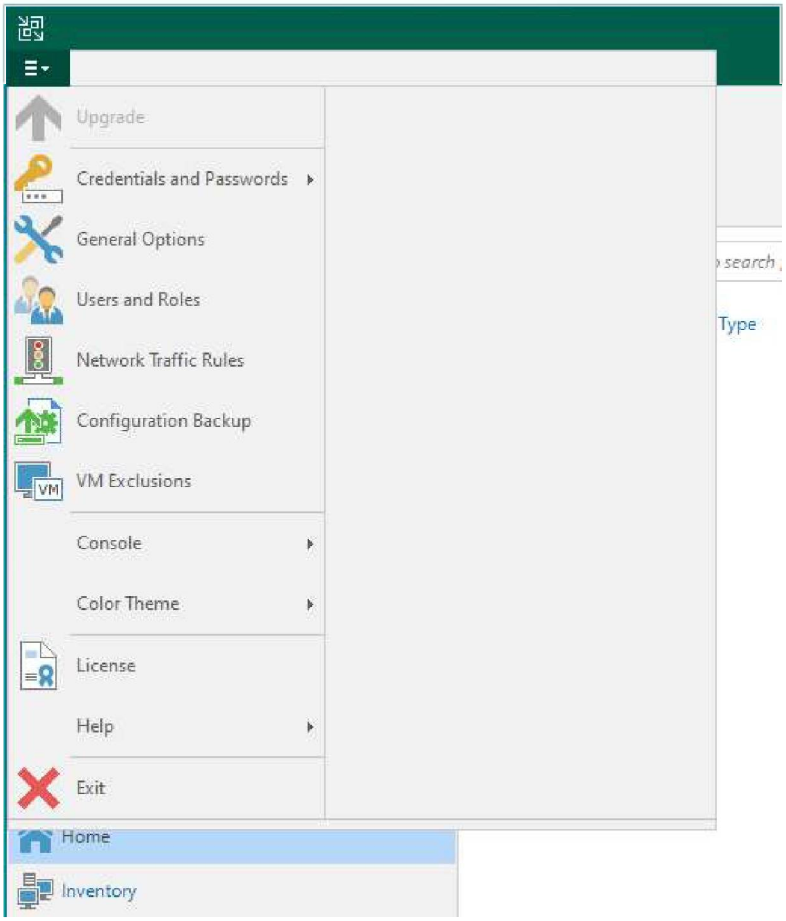
localhost 9392

GOODDEALMART\csun

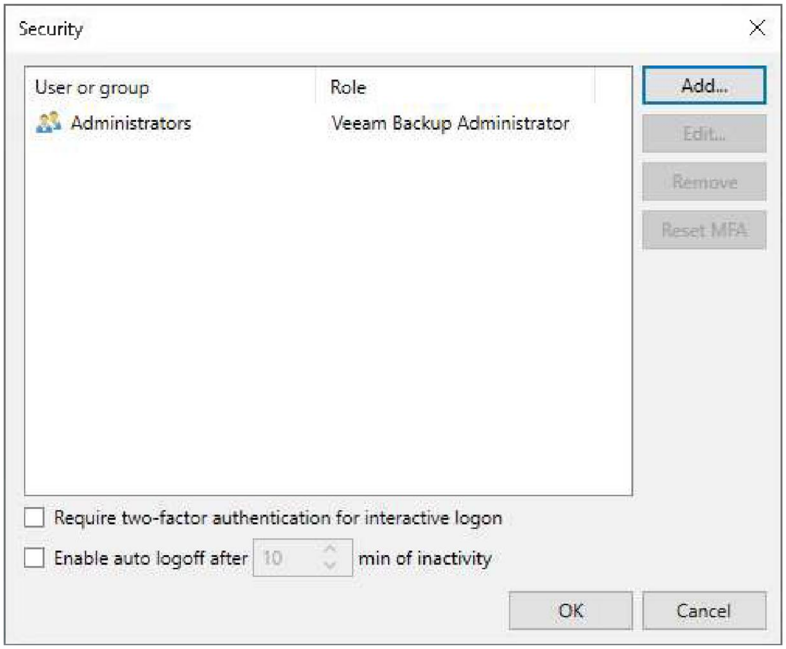
Password

☑ Use Windows session authentication

3. Select Users and Roles from the main menu.



4. Click Add on the Security page.



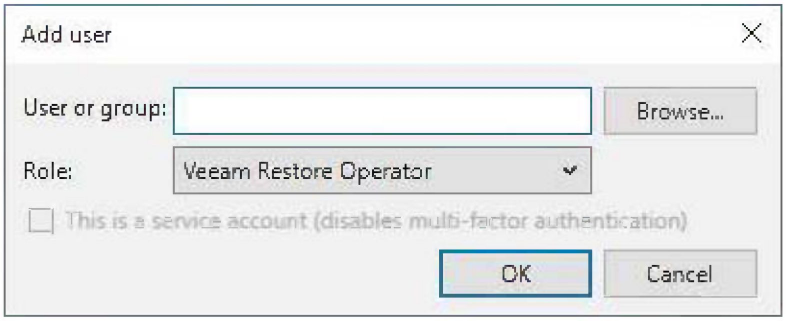
Security

User or group	Role
Administrators	Veeam Backup Administrator

□ Require two-factor authentication for interactive logon

□ Enable auto logoff after 10 min of inactivity

5. On the Add user page, click Browse in the User or group field.



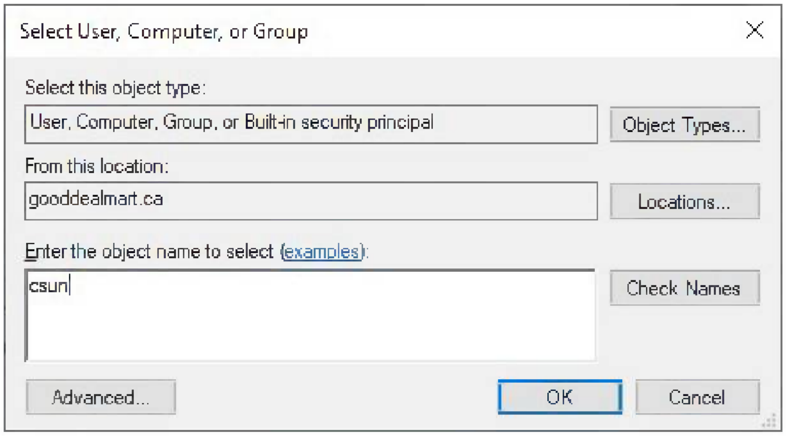
Add user

User or group:

Role: Veeam Restore Operator

□ This is a service account (disables multi-factor authentication)

6. Enter a user name on the Select User, Computer, or Group page and click Check Names.



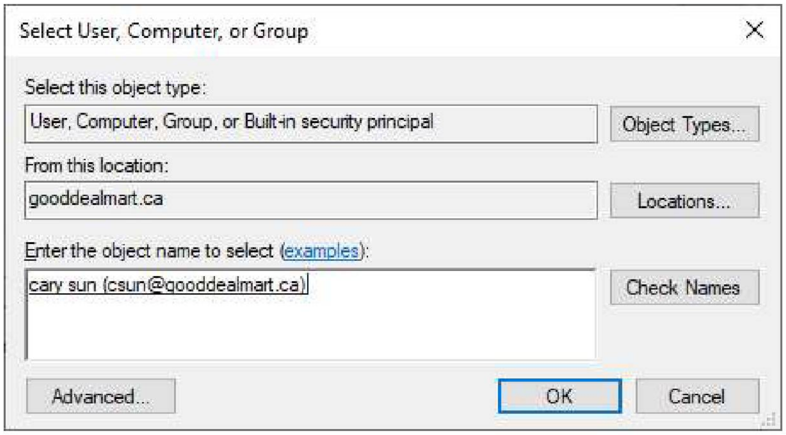
Select User, Computer, or Group

Select this object type: User, Computer, Group, or Built-in security principal

From this location: gooddealmart.ca

Enter the object name to select (examples): csun

7. Click OK on the Select User, Computer, or Group page.



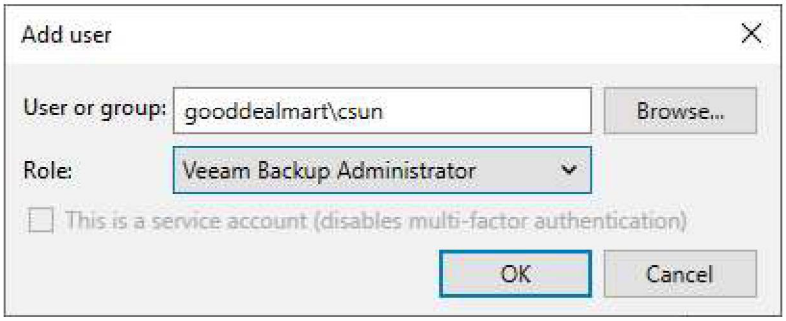
Select User, Computer, or Group

Select this object type: User, Computer, Group, or Built-in security principal

From this location: gooddealmart.ca

Enter the object name to select (examples): cary sun (csun@gooddealmart.ca)

8. Select a role from the Role drop-down list on the Add user page and click OK.



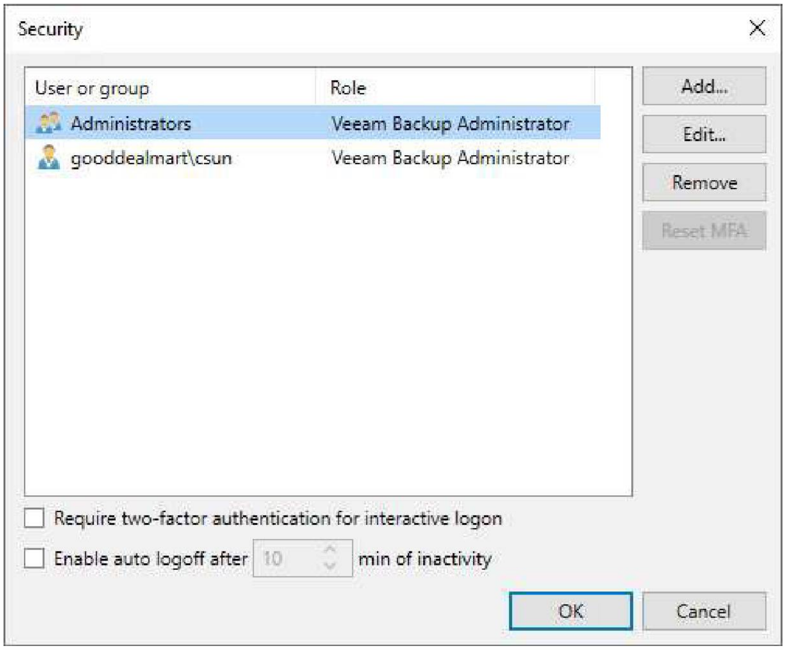
Add user

User or group: gooddealmart\csun

Role: Veeam Backup Administrator

□ This is a service account (disables multi-factor authentication)

9. On the Security page, select the Administrators group and click Remove.



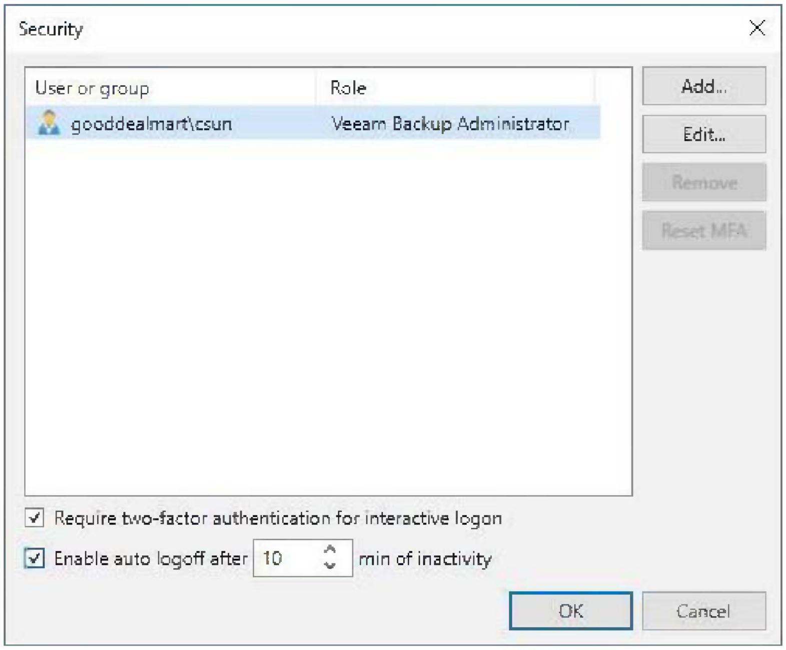
Security

User or group	Role
Administrators	Veeam Backup Administrator
gooddealmart\csun	Veeam Backup Administrator

□ Require two-factor authentication for interactive logon

□ Enable auto logoff after 10 min of inactivity

10. Select the new user.
11. Select the Require two-factor authentication for interactive Log in checkbox.
12. Select Enable auto logoff after a period min of inactivity.
13. Click OK.



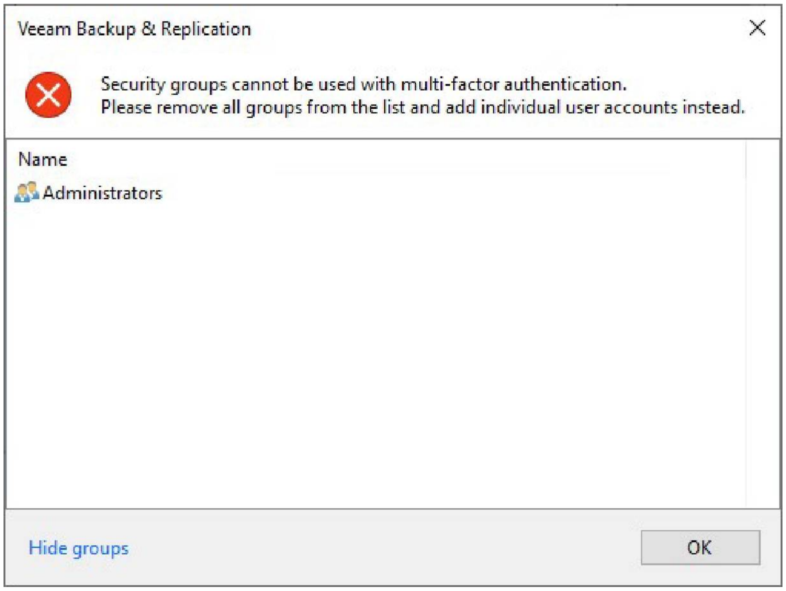
Security

User or group	Role
gooddealmart\csun	Veeam Backup Administrator

☑ Require two-factor authentication for interactive logon

☑ Enable auto logoff after 10 min of inactivity

14. Please remove all unsupported security groups from the list if the error message pops up.

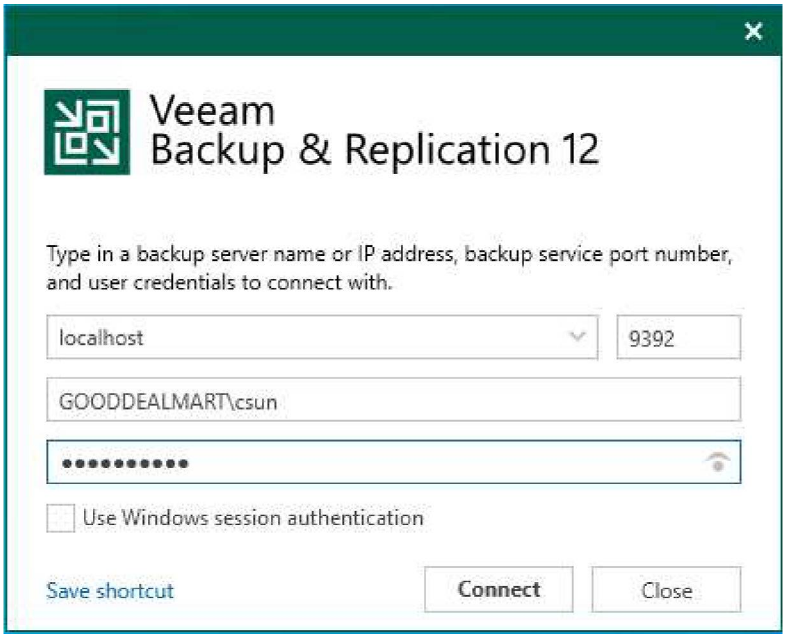


Veeam Backup & Replication

Security groups cannot be used with multi-factor authentication.
Please remove all groups from the list and add individual user accounts instead.

Name
Administrators

15. Close Veeam Backup and Replication console and reopen it.
16. Enter the user name and password on the Veeam Backup & Replication 12 page.



Veeam
Backup & Replication 12

Type in a backup server name or IP address, backup service port number, and user credentials to connect with.

localhost | 9392

GOODDEALMART\csun

●●●●●●●●●●●

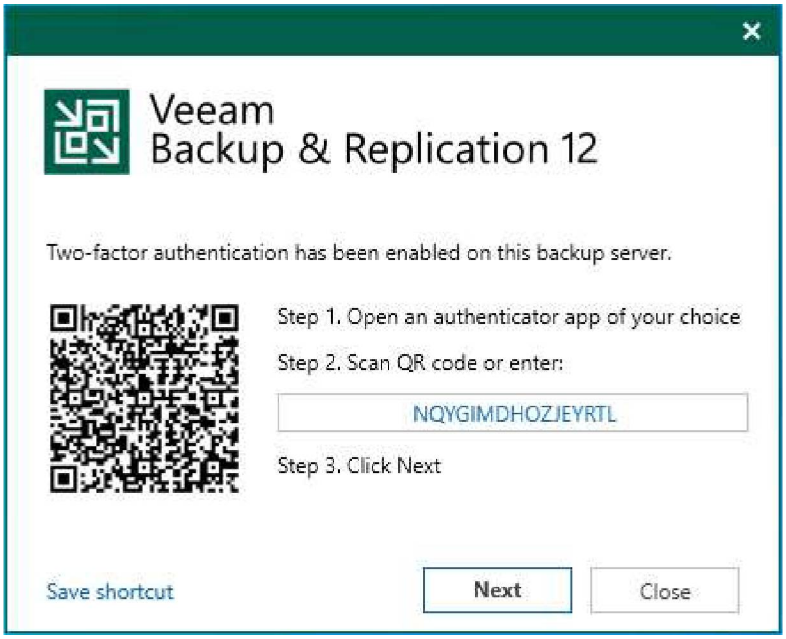
□ Use Windows session authentication

17. Open an Authentication APP from your device and select Add (+).

Note:

I have tried Microsoft and google authentication apps.

18. Scan the QR code or enter the code.



Two-factor authentication has been enabled on this backup server.

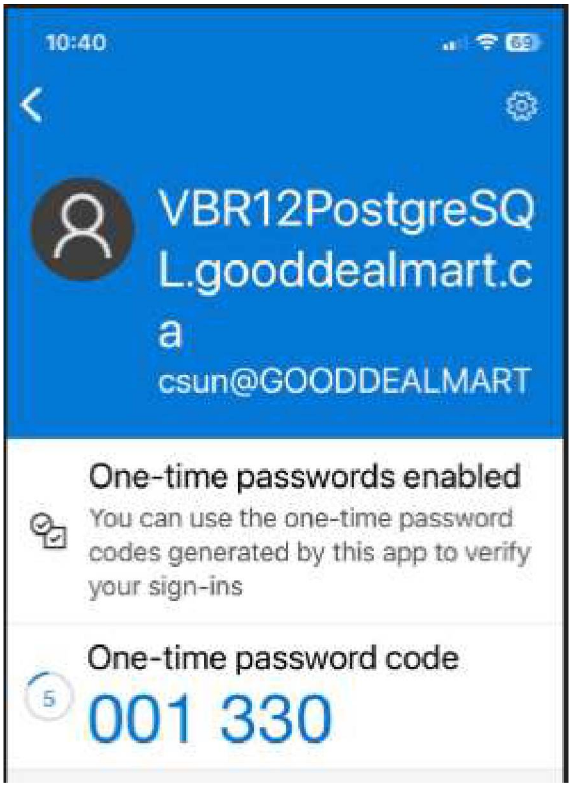
Step 1. Open an authenticator app of your choice

Step 2. Scan QR code or enter:

NQYGIMDHOZJEYRTL

Step 3. Click Next

19. Ensure the account add to your device successfully.



VBR12PostgreSQL.gooddealmart.ca

csun@GOODDEALMART

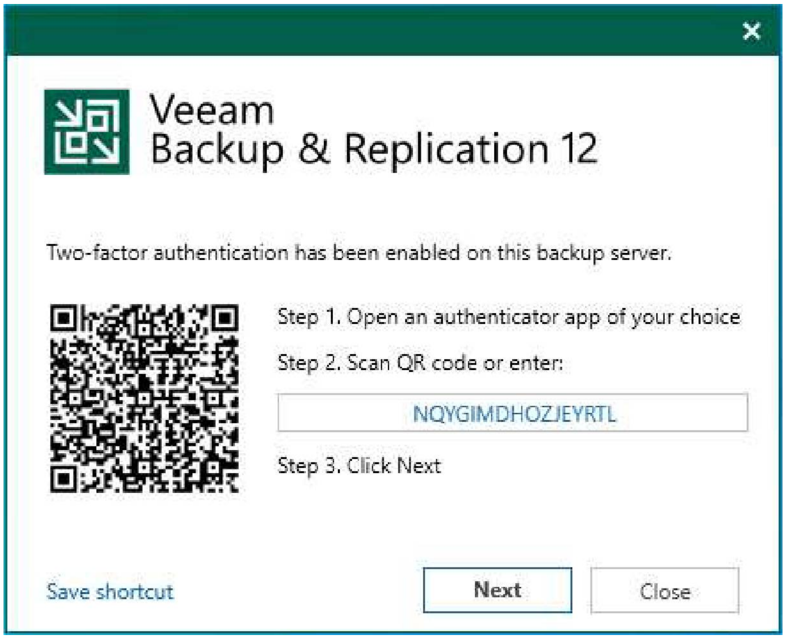
One-time passwords enabled

You can use the one-time password codes generated by this app to verify your sign-ins

One-time password code

001 330

20. Click Next on the Two-factor authentication enabled on this backup server page.



Veeam Backup & Replication 12

Two-factor authentication has been enabled on this backup server.

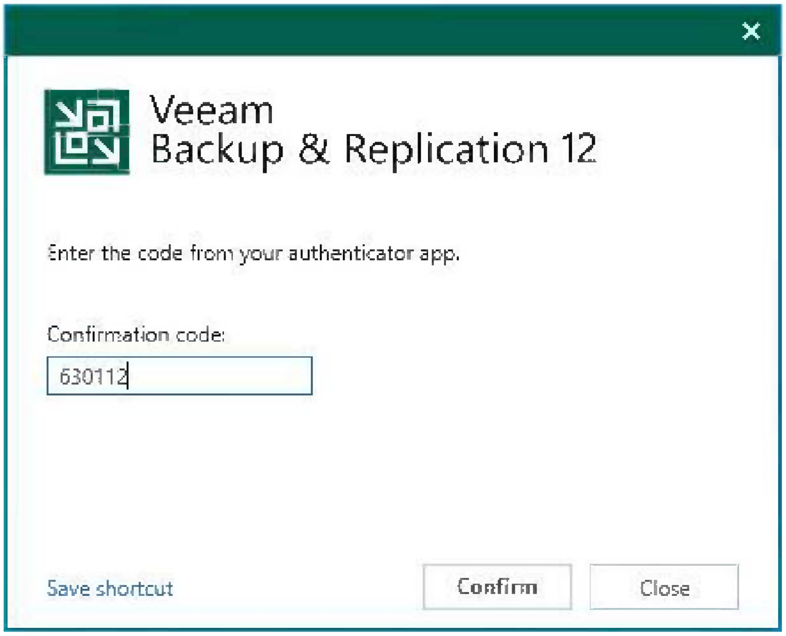
Step 1. Open an authenticator app of your choice

Step 2. Scan QR code or enter:

NQYGIMDHOZJEYRTL

Step 3. Click Next

21. Enter the one-time password code in the Confirmation code field and click Confirm.

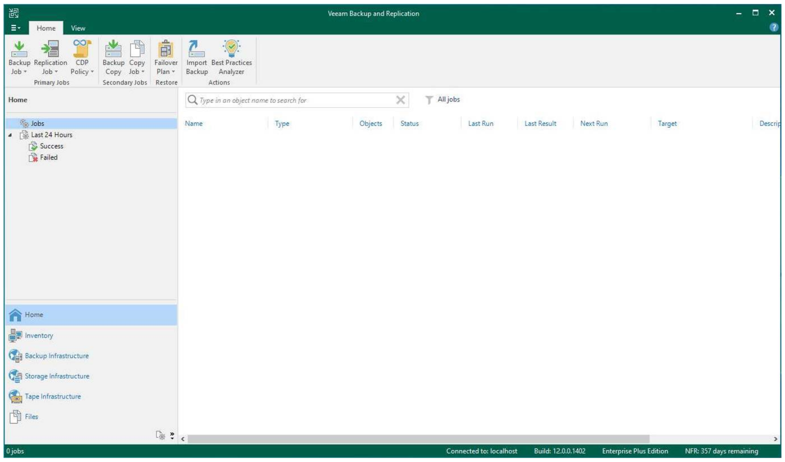


Veeam Backup & Replication 12

Enter the code from your authenticator app.

Confirmation code: 630112

22. Ensure that the open Veeam Backup and Replication console is successful.



Configure Group Managed Service Accounts (gMSA)

A Group Managed Service Account (gMSA) is a domain account that can be configured on the server. The Microsoft Windows operating system manages the password, so the administrator does not need to manage the password. Complex passwords are generated randomly and changed every 30 days, reducing the risk of brute force and dictionary attacks.

gMSA has the following requirements and limitations:

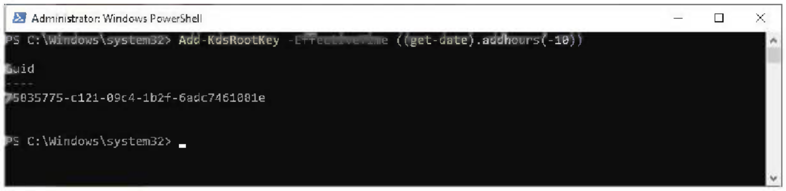
- Microsoft Windows Server 2012 and later support gMSAs.
- Backups of Linux target machines that are members of an Active Directory domain are not supported by gMSAs.
- Because gMSAs require a connection to the domain controller, these accounts can only be accessed via the network.
- If you use a gMSA to back up a machine, both the backup proxy and the target machine must have access to the domain controller to obtain the gMSA password. In addition, the gMSA must be added to a member of the Administrators group on the target machine (local or domain). Add to the member if Domain Administrator is only required for Microsoft Active Directory backups and local Administrator permissions are sufficient for all other supported applications.

Note:

gMSA is supported for application-aware processing for backups or replicas of VMs running Microsoft Active Directory (domain controllers), Microsoft Exchange, Microsoft SQL Server, and Oracle 12c Release 2 and later. However, the gMSA cannot back up or replicate VMs that run Microsoft SharePoint.

Instructions	Screenshot (if applicable)

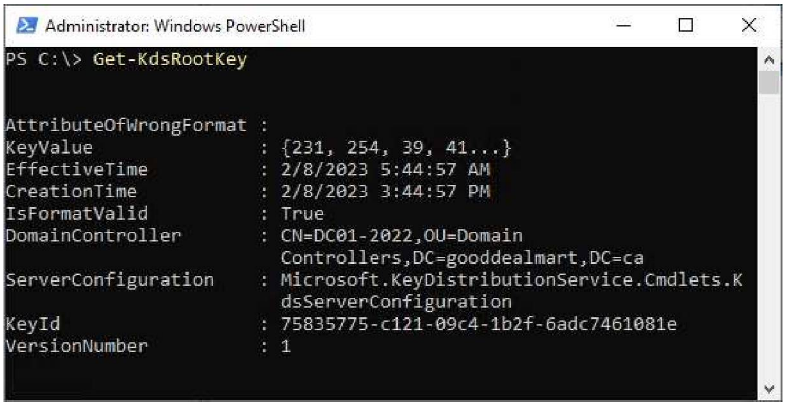
1. Log in to the domain controller server.
2. Open Windows PowerShell and run as administrator.
3. Run the cmdlet below to generate a root key. Add-KdsRootKey –EffectiveTime ((get-date).addhours(-10))



```
PS C:\Windows\system32> Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))

Guid
----
75835775-c121-09c4-1b2f-6adc7461081e


PS C:\Windows\system32> _
```

4. Run the cmdlet below to ensure the KDS root key has been created successfully.

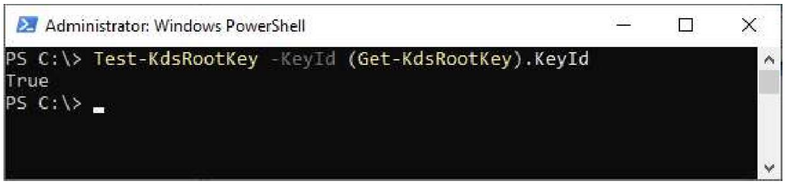
   Get-KdsRootKey



```
PS C:\> Get-KdsRootKey


AttributeOfWrongFormat :
KeyValue               : {231, 254, 39, 41...}
EffectiveTime          : 2/8/2023 5:44:57 AM
CreationTime           : 2/8/2023 3:44:57 PM
IsFormatValid          : True
DomainController       : CN=DC01-2022,OU=Domain
                         Controllers,DC=gooddealmart,DC=ca
ServerConfiguration    : Microsoft.KeyDistributionService.Cmdlets.K
                         dsServerConfiguration
KeyId                  : 75835775-c121-09c4-1b2f-6adc7461081e
VersionNumber          : 1
```

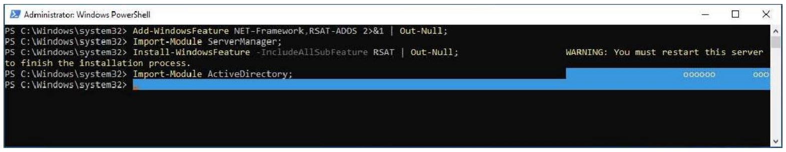
5. Run the cmdlet below to check the KDS key.

   Test-KdsRootKey -KeyId (Get-KdsRootKey).KeyId



```
PS C:\> Test-KdsRootKey -KeyId (Get-KdsRootKey).KeyId
True
PS C:\> _
```

6. Run the below cmdlet to enable gMSA. Add-WindowsFeature NET-Framework, RSAT-ADDS 2>&1 | Out-Null; Import-Module ServerManager;



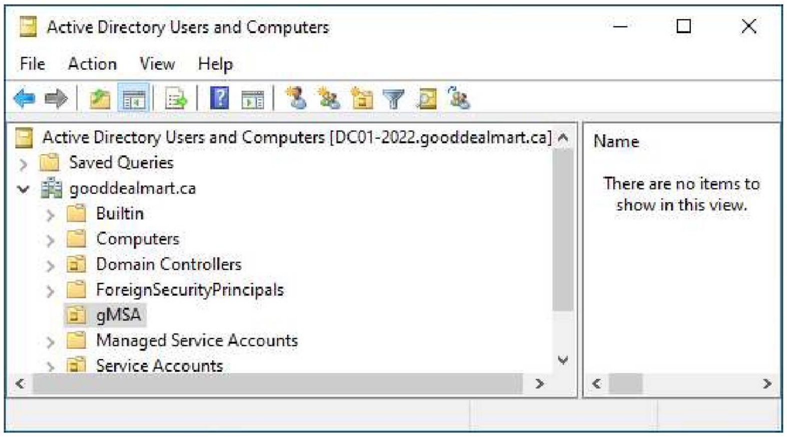
```
PS C:\Windows\system32> Add-WindowsFeature NET-Framework,RSAT-ADDS 2>&1 | Out-Null;
PS C:\Windows\system32> Import-Module ServerManager;
PS C:\Windows\system32> Install-WindowsFeature -IncludeAllSubFeature RSAT | Out-Null;          WARNING: You must restart this server
to finish the installation process.
PS C:\Windows\system32> Import-Module ActiveDirectory;                                                              oooooo      ooo
PS C:\Windows\system32>
```

Install-WindowsFeature -IncludeAllSubFeature RSAT | Out-Null; Import-Module ActiveDirectory;

7. Restart the domain controller server.

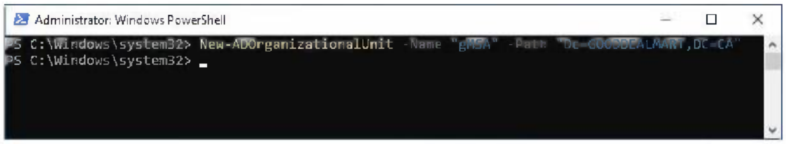
8. Log in to the domain controller server.
9. Select the Active Directory Users and Computers item from the Tools drop-down list on the Server Manager page.
10. Create a new Active Directory OU.

Note:
New-ADOrganizationalUnit -Name "gMSA" -Path "DC=GOODDEALMART, DC=CA."



Active Directory Users and Computers [DC01-2022.gooddealmart.ca]
Saved Queries
gooddealmart.ca
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
gMSA
Managed Service Accounts
Service Accounts

There are no items to show in this view.

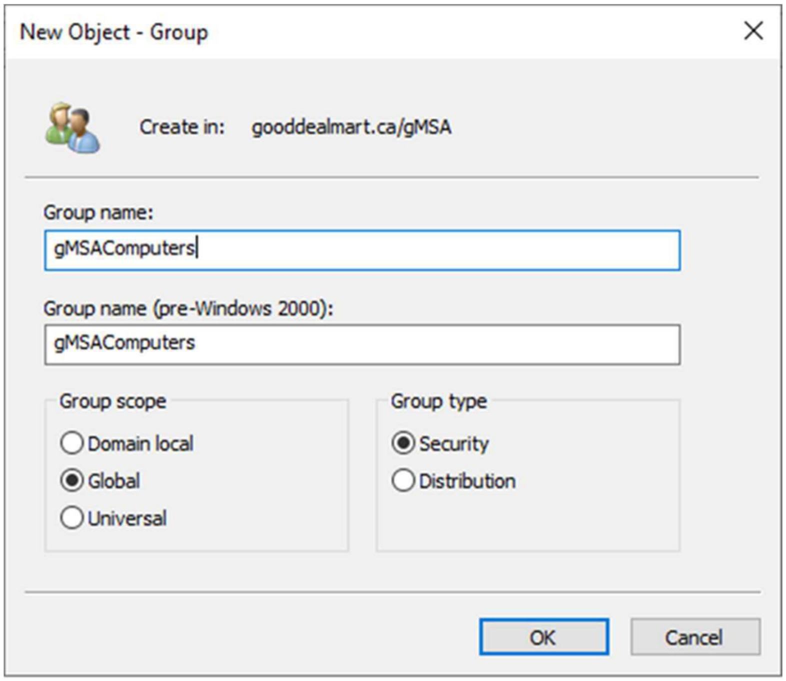


```
PS C:\Windows\system32> New-ADOrganizationalUnit -Name "gMSA" -Path "DC=GOODDEALMART,DC=CA"
PS C:\Windows\system32> _
```

11. Create a new security group for gMSA computers.

Note:

New-ADGroup -Name gMSAComputers -GroupCategory Security -GroupScope Global -Path "OU=gMSA, DC=GOODDEALMART, DC=CA."



New Object - Group

Create in: gooddealmart.ca/gMSA

Group name: gMSAComputers

Group name (pre-Windows 2000): gMSAComputers

Group scope

○ Domain local

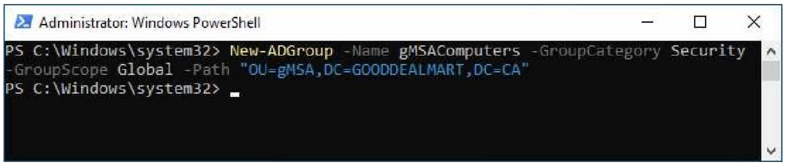
● Global

○ Universal

Group type

● Security

○ Distribution



Administrator: Windows PowerShell

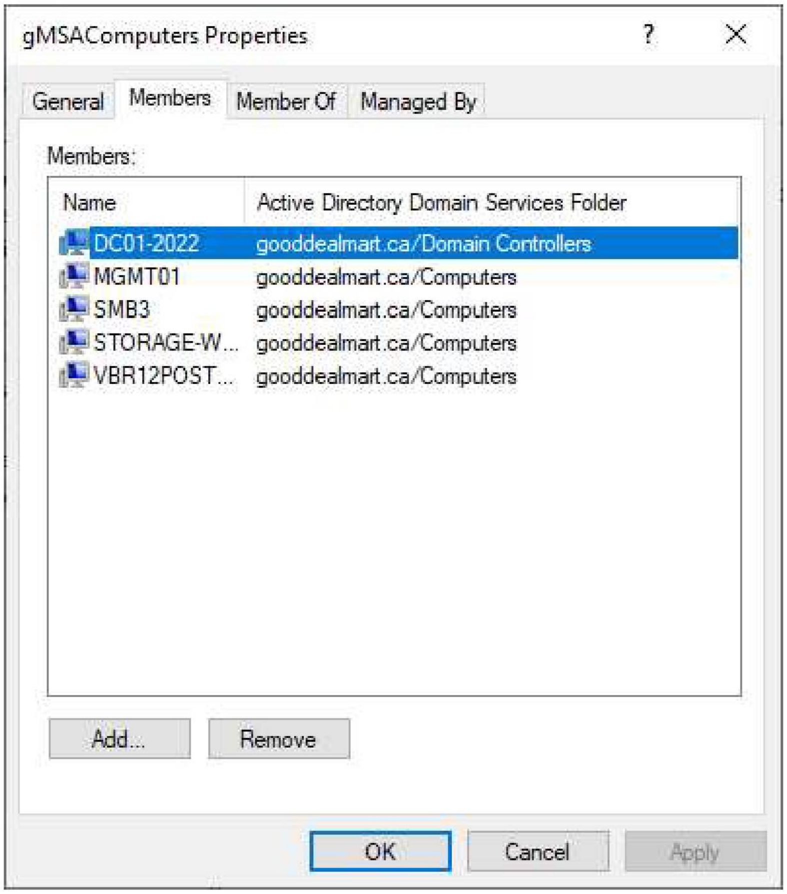
```
PS C:\Windows\system32> New-ADGroup -Name gMSAComputers -GroupCategory Security
-GroupScope Global -Path "OU=gMSA,DC=GOODDEALMART,DC=CA"
PS C:\Windows\system32> _
```

12. Add computer objects to the new security group. These computer objects will be allowed to use gMSA.

Note:

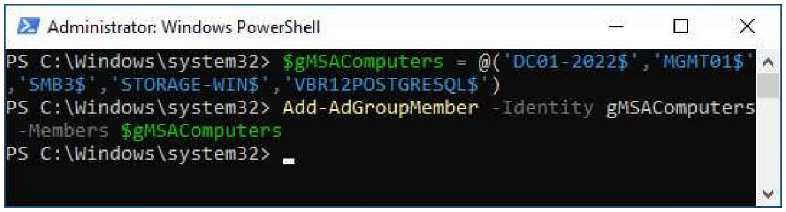
$gMSAComputers = @('DC01-2022$','MGMT01$','SMB3$','STORAGE-WIN$','VBR12POSTGRESQL$')

Add-AdGroupMember -Identity gMSAComputers -Members $gMSAComputers



Members:

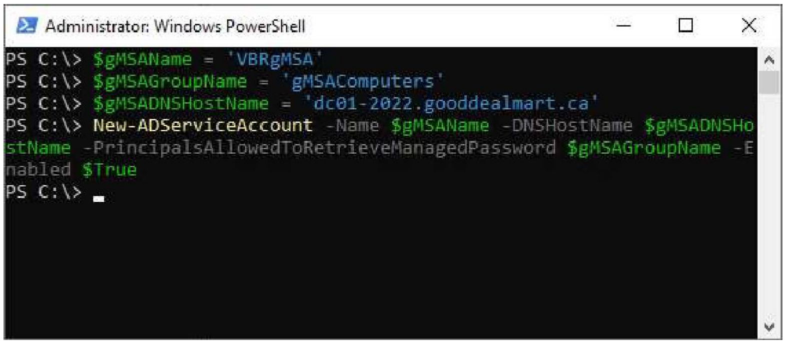
Name	Active Directory Domain Services Folder
DC01-2022	gooddealmart.ca/Domain Controllers
MGMT01	gooddealmart.ca/Computers
SMB3	gooddealmart.ca/Computers
STORAGE-W...	gooddealmart.ca/Computers
VBR12POST...	gooddealmart.ca/Computers



```
PS C:\Windows\system32> $gMSAComputers = @('DC01-2022$','MGMT01$'
,'SMB3$','STORAGE-WIN$','VBR12POSTGRESQL$')
PS C:\Windows\system32> Add-AdGroupMember -Identity gMSAComputers
 -Members $gMSAComputers
PS C:\Windows\system32> _
```

13. Open Windows PowerShell and run as administrator.
14. Run the below cmdlet to create a gMSA account.

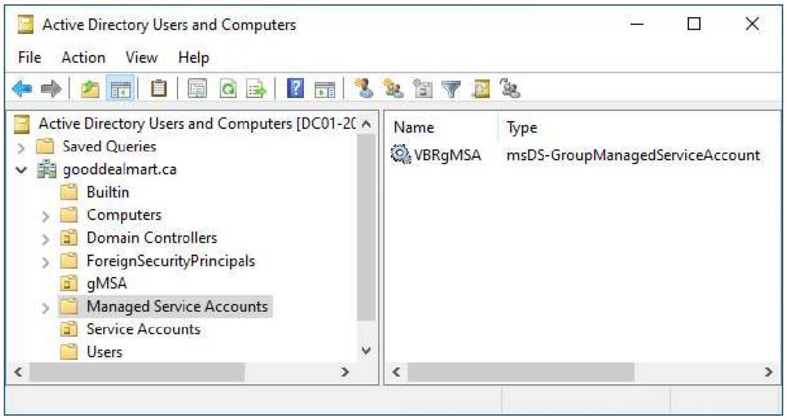
```
$gMSAName = 'VBRgMSA'
$gMSAGroupName = 'gMSAComputers'
$gMSADNSHostName = 'dc01-2022.gooddealmart.ca'

New-ADServiceAccount -Name $gMSAName -DNSHostName $gMSADNSHostName -PrincipalsAllowedToRetrieveManagedPassword $gMSAGroupName -Enabled $True
```



```
PS C:\> $gMSAName = 'VBRgMSA'
PS C:\> $gMSAGroupName = 'gMSAComputers'
PS C:\> $gMSADNSHostName = 'dc01-2022.gooddealmart.ca'
PS C:\> New-ADServiceAccount -Name $gMSAName -DNSHostName $gMSADNSHo
stName -PrincipalsAllowedToRetrieveManagedPassword $gMSAGroupName -E
nabled $True
PS C:\> _
```

15. Select the Active Directory Users and Computers from the Tools drop-down list on the Server Manager page.
16. Ensure the newly created VBRgMSA service account is shown in the Managed Service Accounts OU.

Note:
Use separate gMSAs accounts for critical

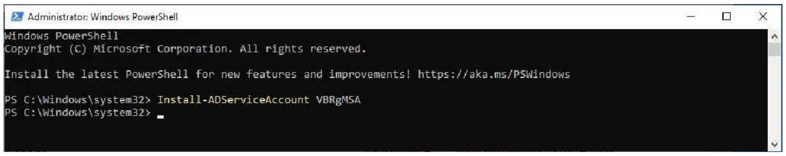


Name	Type
VBRgMSA	msDS-GroupManagedServiceAccount

backup infrastructure components to provide a more secure environment.

17. Run the below cmdlet to install gMSA on the domain controller as the target machine.

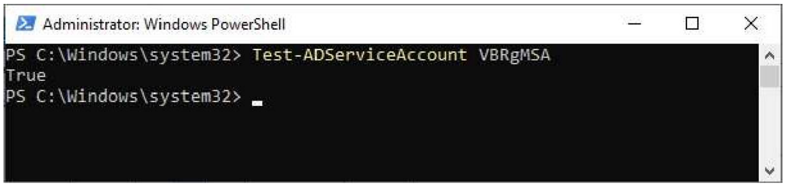
    Install-ADServiceAccount VBRgMSA



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> Install-ADServiceAccount VBRgMSA
PS C:\Windows\system32> _
```

18. Run the below cmdlet to ensure that the gMSA was successfully installed.

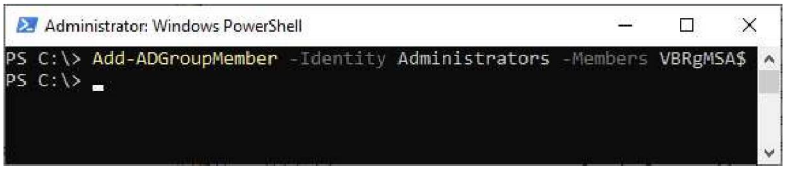
    Test-ADServiceAccount VBRgMSA



```
PS C:\Windows\system32> Test-ADServiceAccount VBRgMSA
True
PS C:\Windows\system32> _
```

19. Run the below cmdlet to Add the VBRgMSA service account to the domain Admins group.

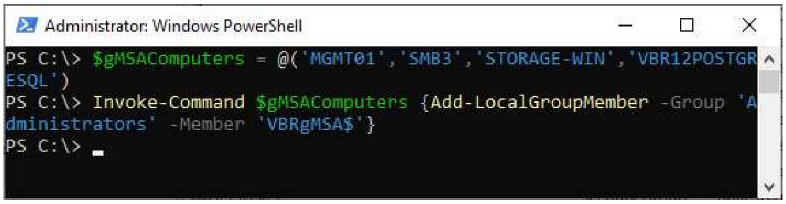
    Add-ADGroupMember -Identity Administrators -Members VBRgMSA$



```
PS C:\> Add-ADGroupMember -Identity Administrators -Members VBRgMSA$
PS C:\> _
```

20. Run the below cmdlet to Add the VBRgMSA service account to the Local Administrators group.

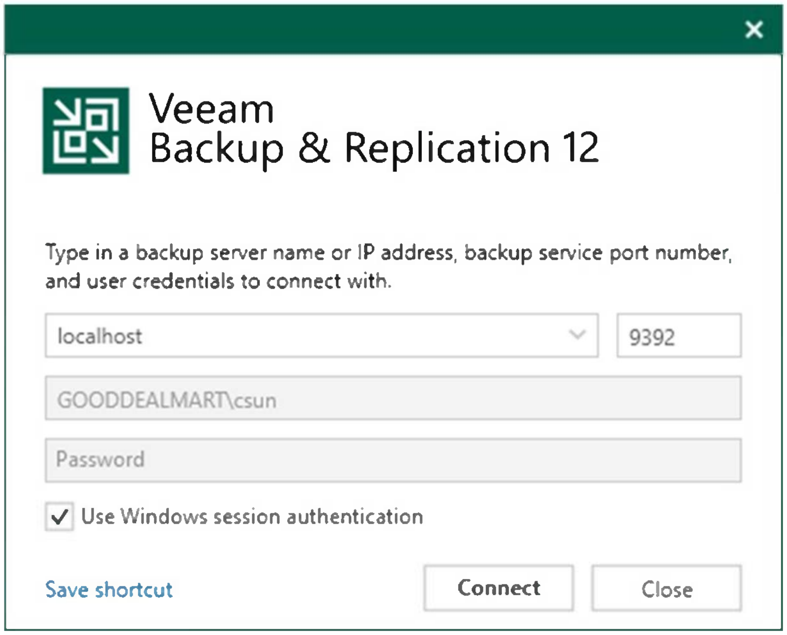
    $gMSAComputers = @('MGMT01','SMB3','STO



```
PS C:\> $gMSAComputers = @('MGMT01','SMB3','STORAGE-WIN','VBR12POSTGR
ESQL')
PS C:\> Invoke-Command $gMSAComputers {Add-LocalGroupMember -Group 'A
dministrators' -Member 'VBRgMSA$'}
PS C:\> _
```

```
RAGE-WIN','VBR12POSTGRESQL')

Invoke-Command $gMSAComputers {Add-LocalGroupMember -Group ‘Administrators’ -Member ‘VBRgMSA$’}
```

21. Log in to the Veeam Backup and replication manager server.
22. Open the Veeam Backup & Replication Console and click Connect.



Veeam
Backup & Replication 12

Type in a backup server name or IP address, backup service port number, and user credentials to connect with.

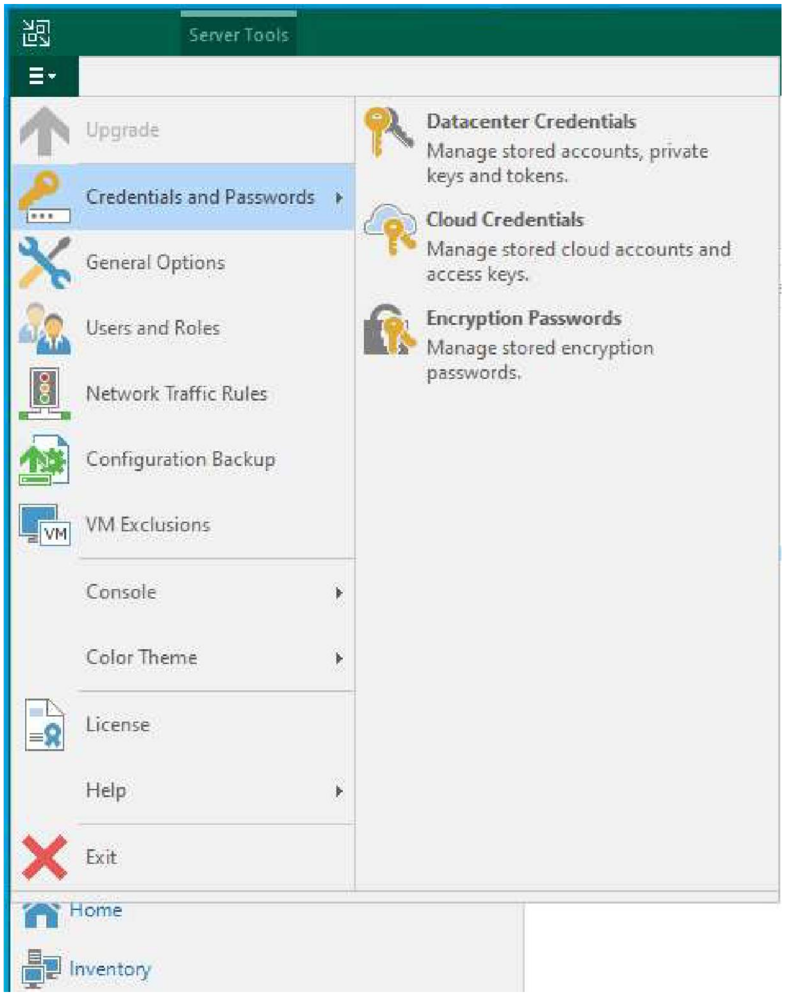
localhost 9392

GOODDEALMART\csun

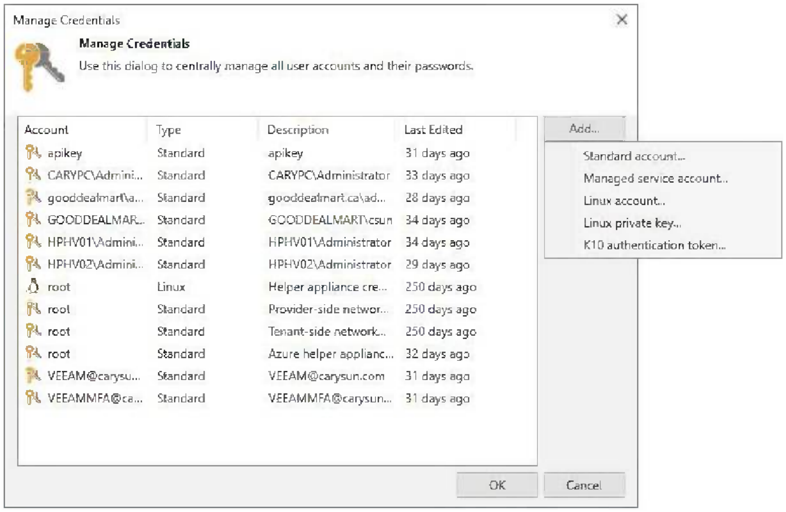
Password

☑ Use Windows session authentication

23. Select Credentials and Passwords from the main menu.
24. Select Datacenter Credentials.



25. Click Add on the Manage Credentials page and select Managed service account.



Manage Credentials

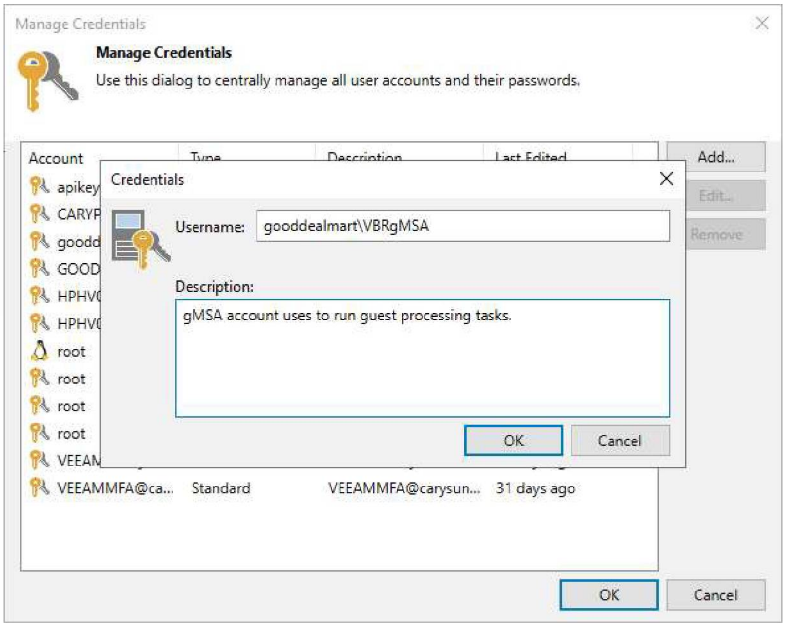
Manage Credentials

Use this dialog to centrally manage all user accounts and their passwords.

Account	Type	Description	Last Edited
apikey	Standard	apikey	31 days ago
CARYPC\Admini...	Standard	CARYPC\Administrator	33 days ago
gooddealmart\a...	Standard	gooddealmart.ca\ad...	28 days ago
GOODDEALMAR...	Standard	GOODDEALMART\csun	34 days ago
HPHV01\Admini...	Standard	HPHV01\Administrator	34 days ago
HPHV02\Admini...	Standard	HPHV02\Administrator	29 days ago
root	Linux	Helper appliance cre...	250 days ago
root	Standard	Provider-side networ...	250 days ago
root	Standard	Tenant-side network...	250 days ago
root	Standard	Azure helper applianc...	32 days ago
VEEAM@carysu...	Standard	VEEAM@carysun.com	31 days ago
VEEAMMFA@ca...	Standard	VEEAMMFA@carysun...	31 days ago

26. Enter the new gMSA account in the Username field on the Credentials page.

27. Give a brief description in the Description field for future reference and click OK.



Manage Credentials

Manage Credentials

Use this dialog to centrally manage all user accounts and their passwords.

Credentials

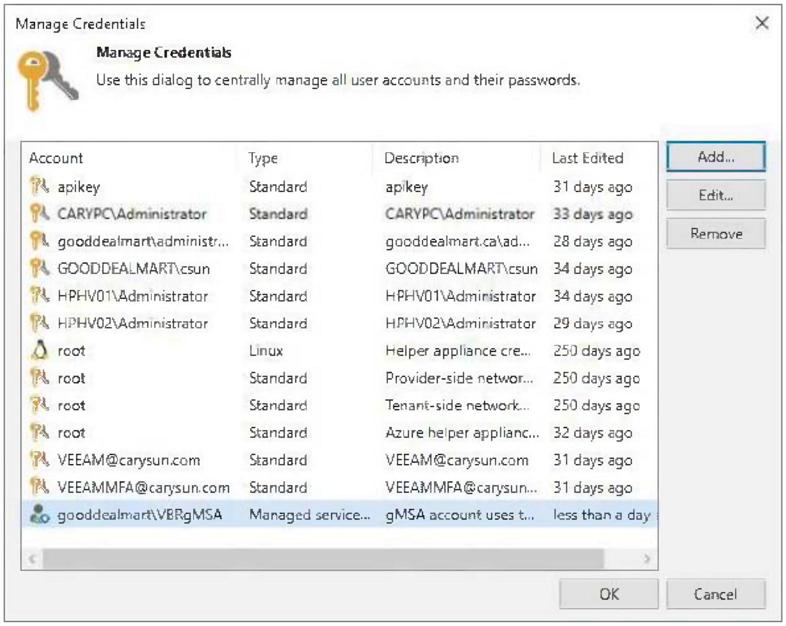
Username: gooddealmart\VBRgMSA

Description:

gMSA account uses to run guest processing tasks.

Account	Type	Description	Last Edited
VEEAMMFA@ca...	Standard	VEEAMMFA@carysun...	31 days ago

28. Ensure the gMSA account is added to the Manage Credentials page and click OK.



Manage Credentials

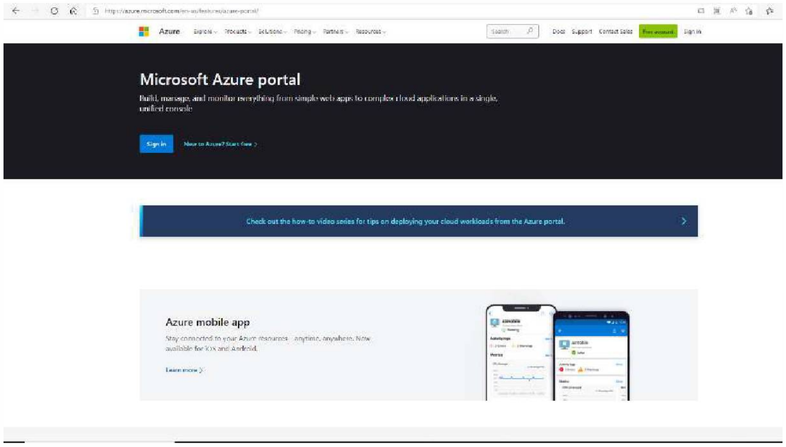
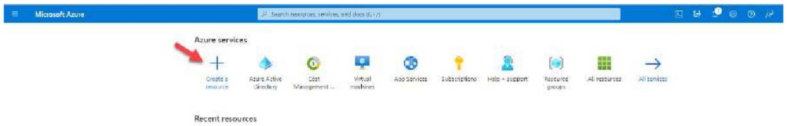
Manage Credentials

Use this dialog to centrally manage all user accounts and their passwords.

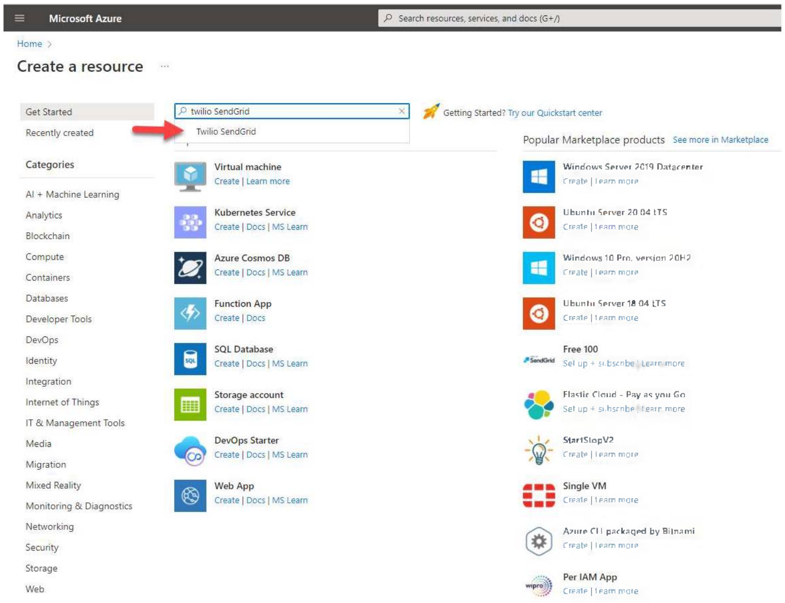
Account	Type	Description	Last Edited
apikey	Standard	apikey	31 days ago
CARYPC\Administrator	Standard	CARYPC\Administrator	33 days ago
gooddealmart\administr...	Standard	gooddealmart.ca\ad...	28 days ago
GOODDEALMART\csun	Standard	GOODDEALMART\csun	34 days ago
HPHV01\Administrator	Standard	HPHV01\Administrator	34 days ago
HPHV02\Administrator	Standard	HPHV02\Administrator	29 days ago
root	Linux	Helper appliance cre...	250 days ago
root	Standard	Provider-side networ...	250 days ago
root	Standard	Tenant-side network...	250 days ago
root	Standard	Azure helper applianc...	32 days ago
VEEAM@carysun.com	Standard	VEEAM@carysun.com	31 days ago
VEEAMMFA@carysun.com	Standard	VEEAMMFA@carysun...	31 days ago
gooddealmart\VBRgMSA	Managed service...	gMSA account uses t...	less than a day

Configure Notification with Free SendGrid Account of Azure

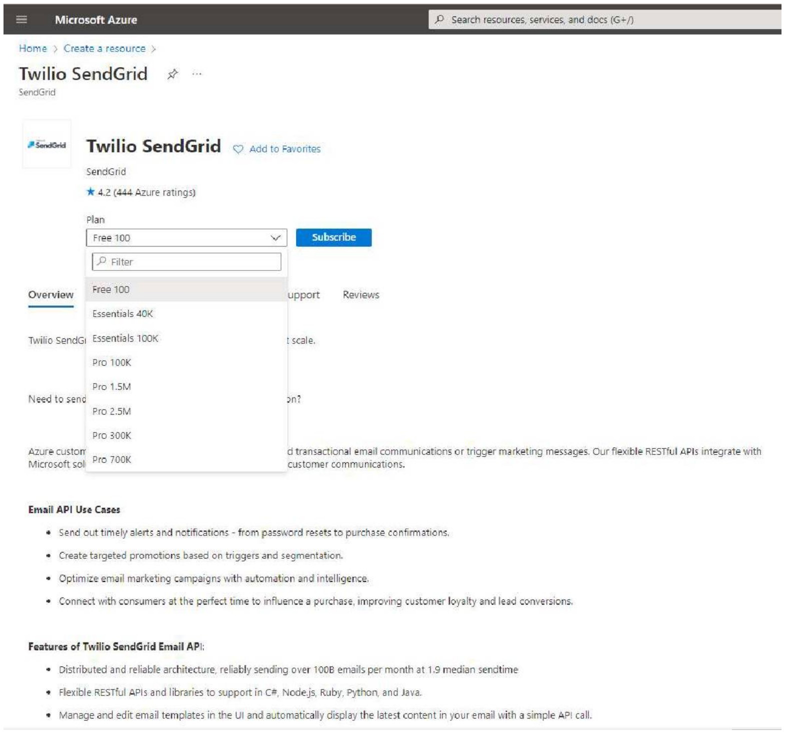
You can configure the SendGrid account as an SMTP relay for notification settings if you want Veeam Backup & Replication to send email notifications about backup job results.

Instructions	Screenshot (if applicable)
1. Sign in Azure portal with a global admin account. https://portal.azure.com	 http://azure.microsoft.com/en-us/features/azure-portal/ Microsoft Azure portal Build, manage, and monitor everything from simple web apps to complex cloud applications in a single, unified console. Sign in · New to Azure? Start free > Check out the how-to video series for tips on deploying your cloud workloads from the Azure portal. Azure mobile app Stay connected to your Azure resources—anytime, anywhere. Now available for iOS and Android. Learn more >
2. On the Azure services page, select +Create resource.	 Microsoft Azure Search resources, services, and docs (G+/) Azure services Create a resource · Azure Active Directory · Cost Management ... · Virtual machines · App Services · Subscriptions · Help + support · Resource groups · All resources · All services Recent resources

3. On the Create a resource page, search and select Twilio SendGrid.



4. On the Create Twilio SendGrid page, select subscribe Plan and click Subscribe.



Plan: Free 100

Twilio SendGı t scale.

Need to send on?

Azure custom d transactional email communications or trigger marketing messages. Our flexible RESTful APIs integrate with Microsoft sol customer communications.

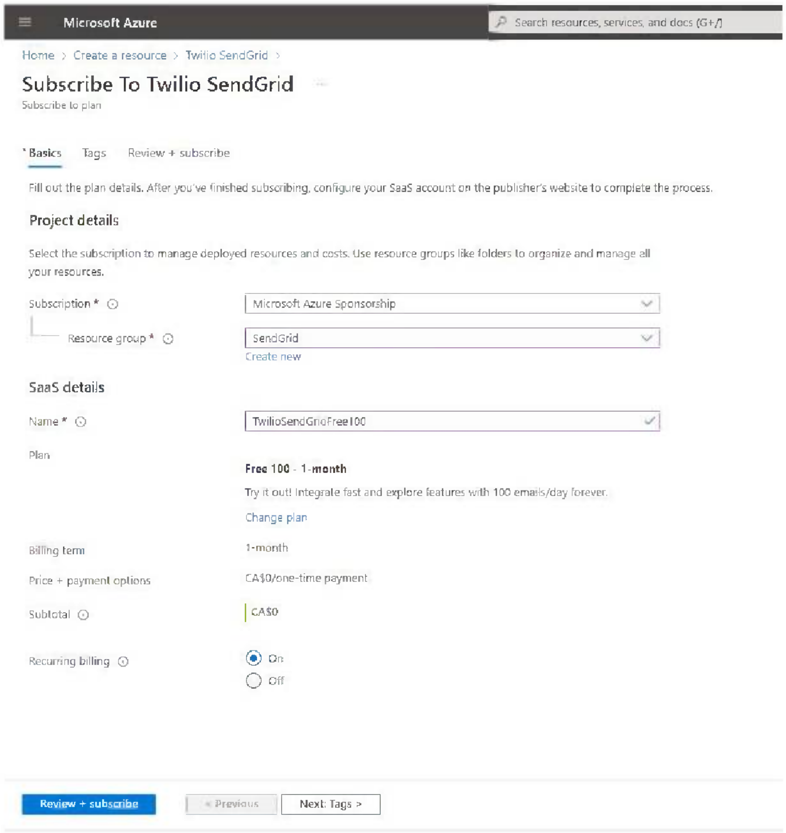
Email API Use Cases

- Send out timely alerts and notifications - from password resets to purchase confirmations.
- Create targeted promotions based on triggers and segmentation.
- Optimize email marketing campaigns with automation and intelligence.
- Connect with consumers at the perfect time to influence a purchase, improving customer loyalty and lead conversions.

Features of Twilio SendGrid Email API:

- Distributed and reliable architecture, reliably sending over 100B emails per month at 1.9 median sendtime
- Flexible RESTful APIs and libraries to support in C#, Node.js, Ruby, Python, and Java.
- Manage and edit email templates in the UI and automatically display the latest content in your email with a simple API call.

5. On the Create SendGrid Account page, select Basics, file in all the information and then click Next: Tags.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Create a resource > Twilio SendGrid >
* Basics
Tags
Review + subscribe
Review + subscribe
< Previous
Next: Tags >

Subscribe To Twilio SendGrid

Subscribe to plan

Fill out the plan details. After you've finished subscribing, configure your SaaS account on the publisher's website to complete the process.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Microsoft Azure Sponsorship

Resource group * : SendGrid

Create new

SaaS details

Name * : TwilioSendGridFree100

Plan: Free 100 - 1-month

Try it out! Integrate fast and explore features with 100 emails/day forever.

Change plan

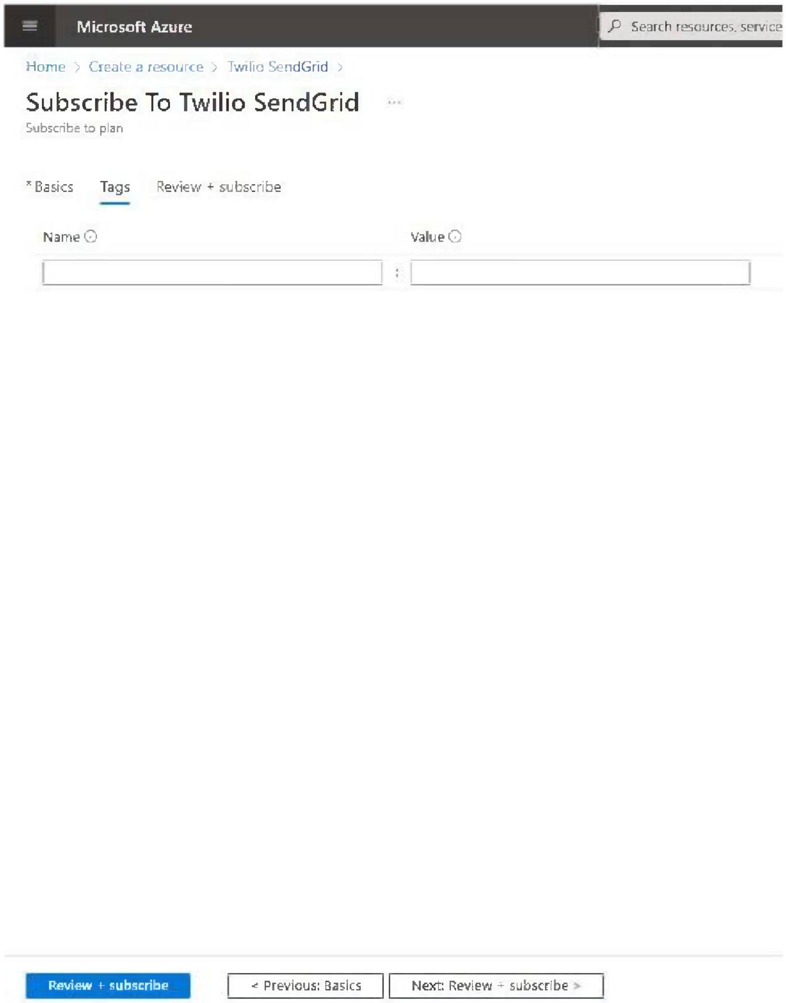
Billing term: 1-month

Price + payment options: CA$0/one-time payment

Subtotal: CA$0

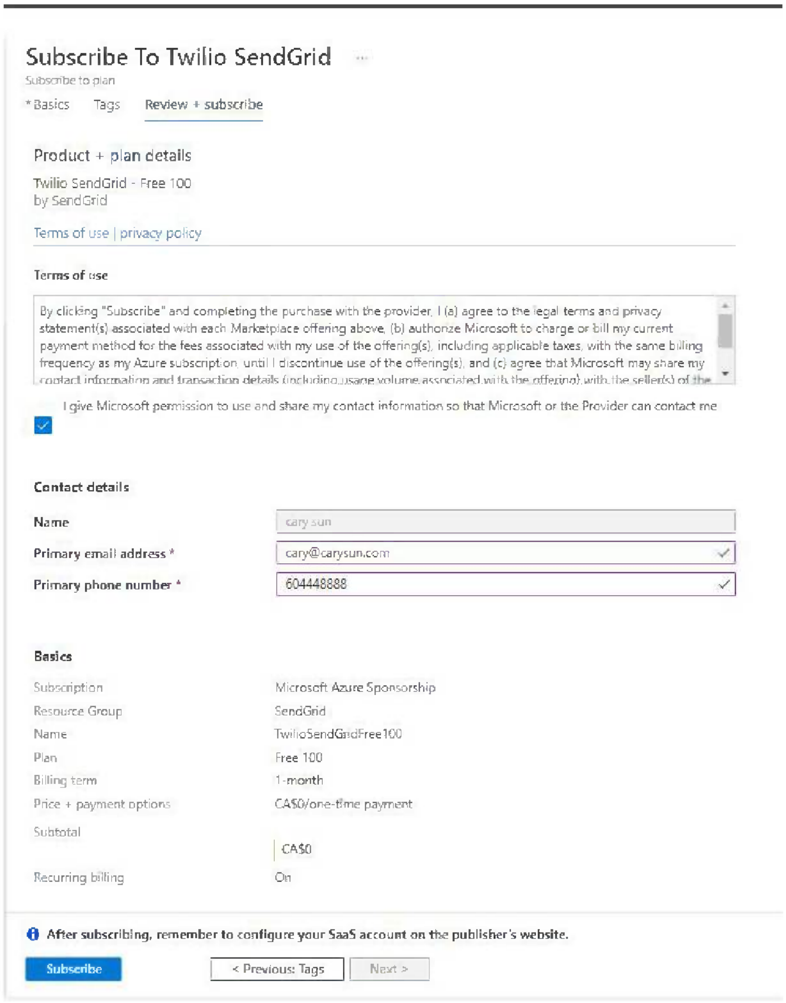
Recurring billing: ● On ○ Off

6. On the Tags page, click Next: Review + subscribe.



Microsoft Azure
Search resources, service
Home > Create a resource > Twilio SendGrid >
Subscribe To Twilio SendGrid ...
Subscribe to plan
* Basics
Tags
Review + subscribe
Name
Value
Review + subscribe
< Previous: Basics
Next: Review + subscribe >

7. On the Review + subscribe page, select I give Microsoft permission to use and share my contact information so that Microsoft or the provider can contact me.



Subscribe To Twilio SendGrid ...

Subscribe to plan

Product + plan details

Twilio SendGrid - Free 100
by SendGrid

Terms of use | privacy policy

Terms of use

By clicking "Subscribe" and completing the purchase with the provider, I (a) agree to the legal terms and privacy statement(s) associated with each Marketplace offering above, (b) authorize Microsoft to charge or bill my current payment method for the fees associated with my use of the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s), and (c) agree that Microsoft may share my contact information and transaction details (including usage volume associated with the offering) with the seller(s) of the

☑ I give Microsoft permission to use and share my contact information so that Microsoft or the Provider can contact me

Contact details

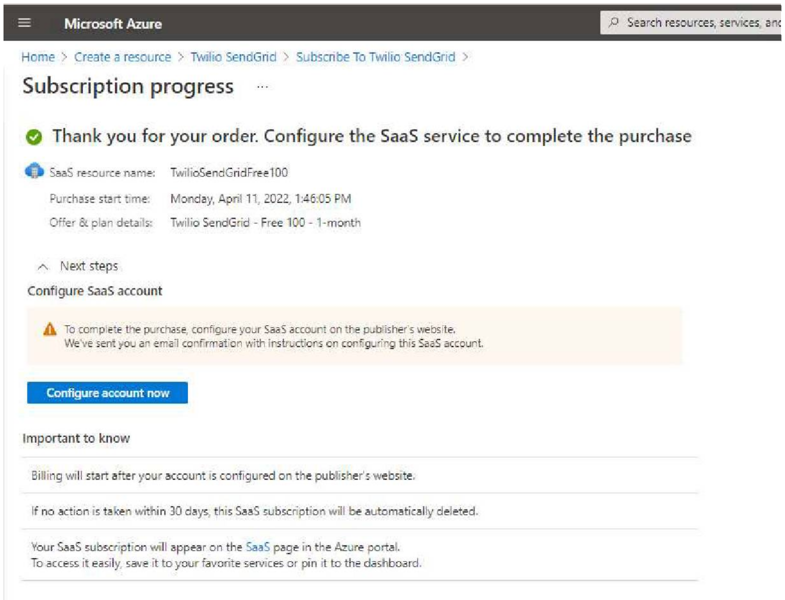
Name	cary sun
Primary email address *	cary@carysun.com ✓
Primary phone number *	604448888 ✓

Basics

Subscription	Microsoft Azure Sponsorship
Resource Group	SendGrid
Name	TwilioSendGridFree100
Plan	Free 100
Billing term	1-month
Price + payment options	CA$0/one-time payment
Subtotal	CA$0
Recurring billing	On

After subscribing, remember to configure your SaaS account on the publisher's website.

8. On the Configure SaaS account page, click Configure account now.


Microsoft Azure
Search resources, services, and
Home > Create a resource > Twilio SendGrid > Subscribe To Twilio SendGrid >

Subscription progress ...

Thank you for your order. Configure the SaaS service to complete the purchase

SaaS resource name: TwilioSendGridFree100

Purchase start time: Monday, April 11, 2022, 1:46:05 PM

Offer & plan details: Twilio SendGrid - Free 100 - 1-month

Next steps

Configure SaaS account

To complete the purchase, configure your SaaS account on the publisher's website.
We've sent you an email confirmation with instructions on configuring this SaaS account.

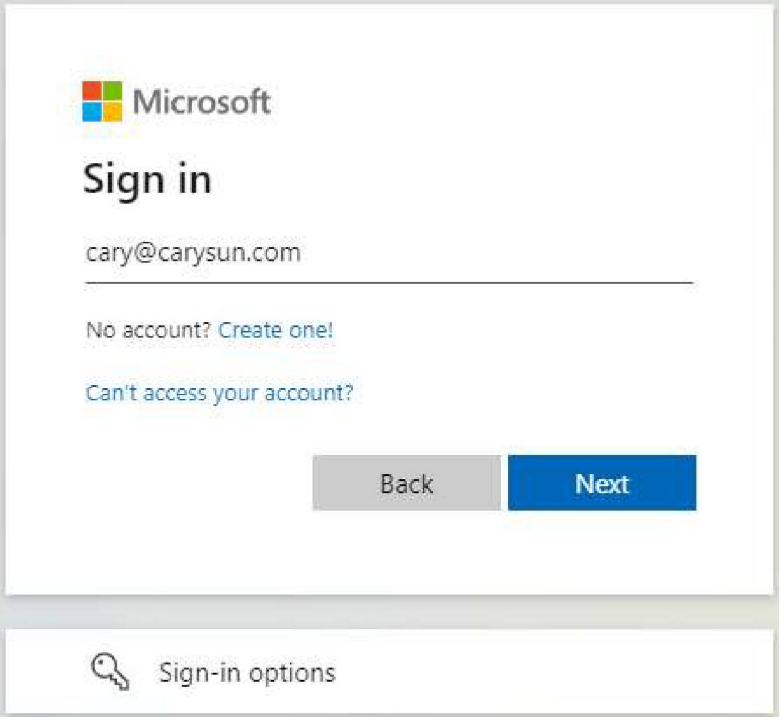
Important to know

Billing will start after your account is configured on the publisher's website.

If no action is taken within 30 days, this SaaS subscription will be automatically deleted.

Your SaaS subscription will appear on the SaaS page in the Azure portal.
To access it easily, save it to your favorite services or pin it to the dashboard.

9. On the Microsoft Sign-in page, enter your account name and click Next.

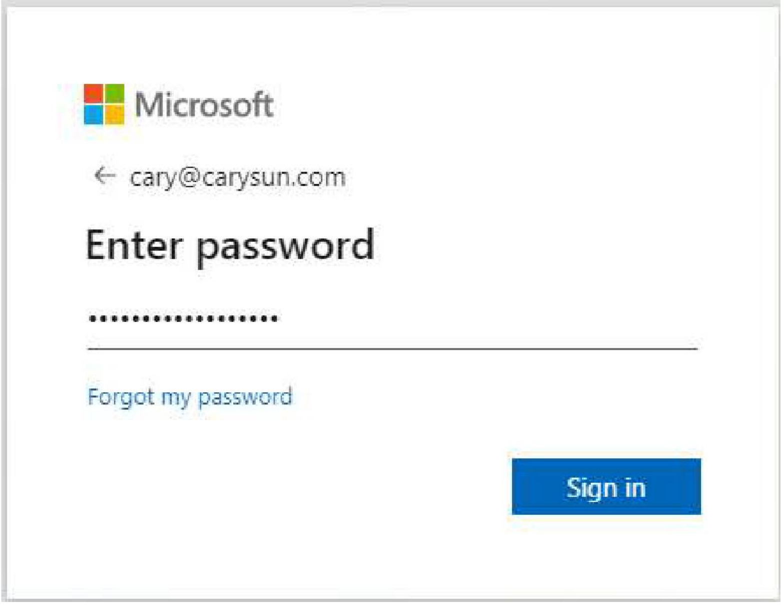


cary@carysun.com

No account? Create one!

Can't access your account?

10. Enter a password, and click Sign in.



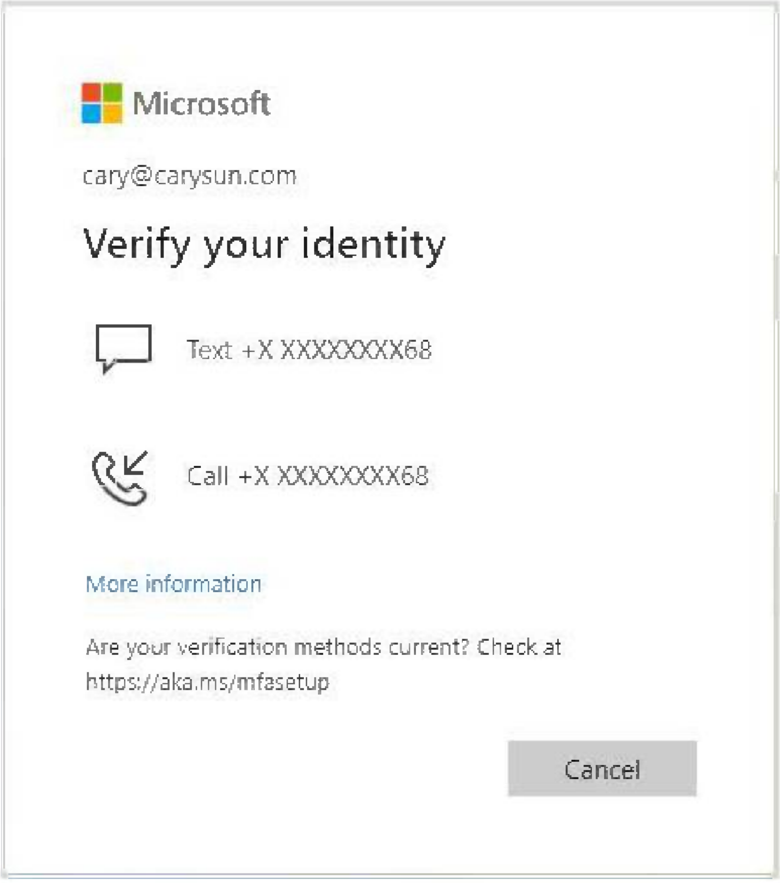
Microsoft

cary@carysun.com

Enter password

••••••••••••••••••

11. On the Verify your identity page, select the identity method.



Microsoft

cary@carysun.com

Verify your identity

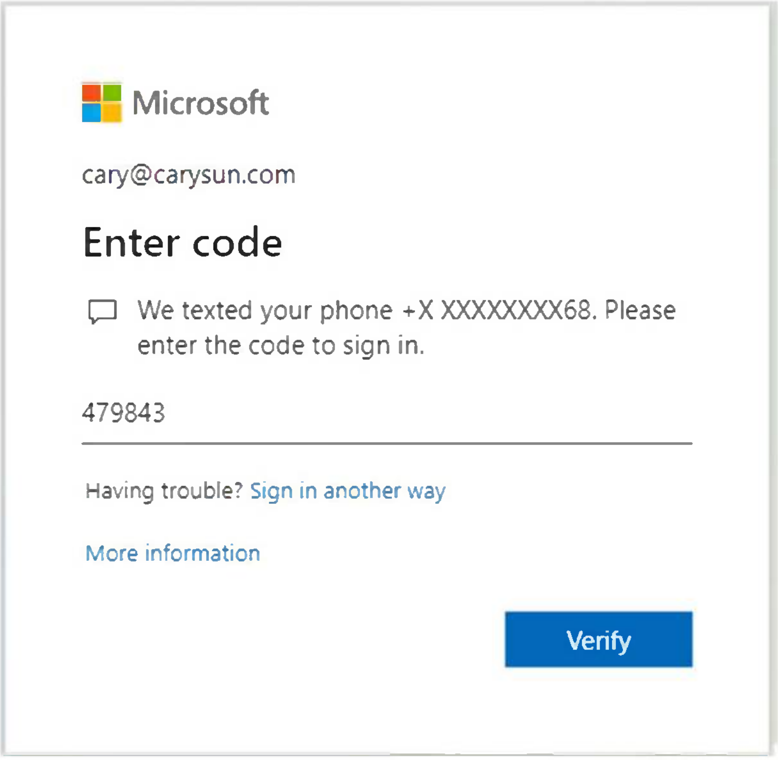
Text +X XXXXXXXX68

Call +X XXXXXXXX68

More information

Are your verification methods current? Check at https://aka.ms/mfasetup

12. Enter the code, and click Verify.



Microsoft

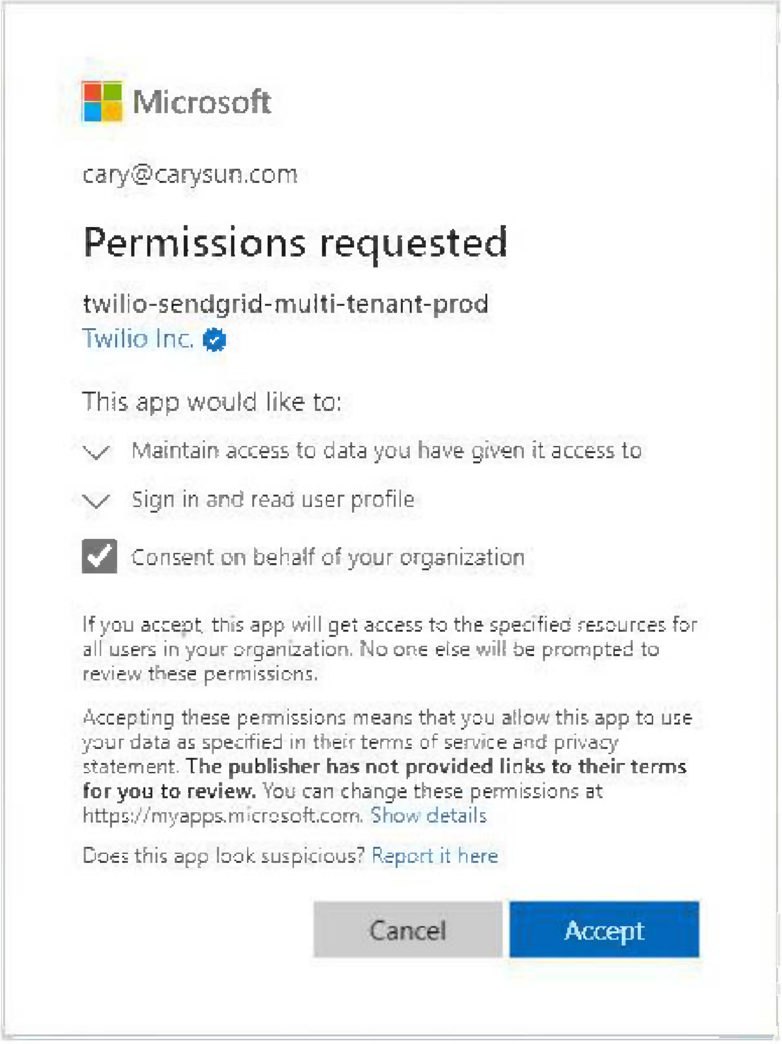
cary@carysun.com

Enter code

We texted your phone +X XXXXXXXX68. Please enter the code to sign in.

479843

13. On the Permissions requested page, select Consent on behalf of your organization and click Accept.



cary@carysun.com

Permissions requested

twilio-sendgrid-multi-tenant-prod
Twilio Inc.

This app would like to:

- Maintain access to data you have given it access to
- Sign in and read user profile

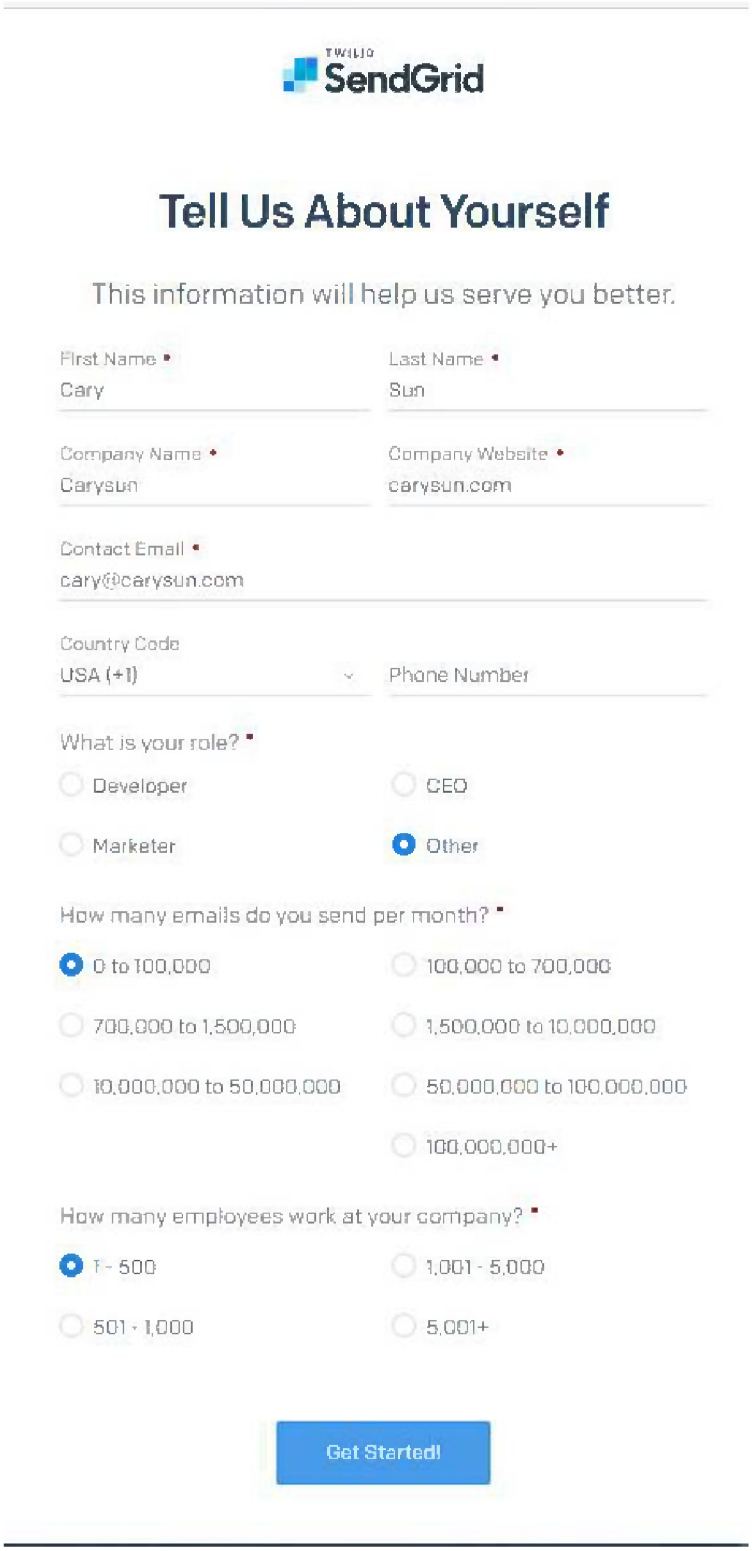
☑ Consent on behalf of your organization

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

14. Fill in the information, and click Get Started!



TWILIO SendGrid

Tell Us About Yourself

This information will help us serve you better.

First Name * Cary

Last Name * Sun

Company Name * Carysun

Company Website * carysun.com

Contact Email * cary@carysun.com

Country Code USA (+1)

Phone Number

What is your role? *

○ Developer ○ CEO

○ Marketer ● Other

How many emails do you send per month? *

● 0 to 100,000 ○ 100,000 to 700,000

○ 700,000 to 1,500,000 ○ 1,500,000 to 10,000,000

○ 10,000,000 to 50,000,000 ○ 50,000,000 to 100,000,000

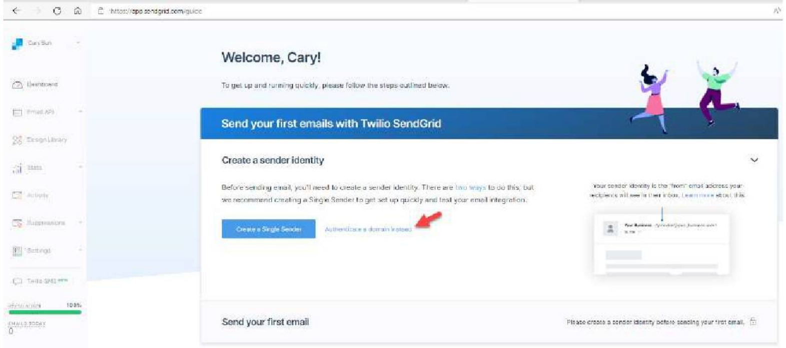
○ 100,000,000+

How many employees work at your company? *

● 1 - 500 ○ 1,001 - 5,000

○ 501 - 1,000 ○ 5,001+

15. On the SendGrid Welcome page, select Authentication a domain instead.



https://app.sendgrid.com/guide

Welcome, Cary!

To get up and running quickly, please follow the steps outlined below.

Send your first emails with Twilio SendGrid

Create a sender identity

Before sending email, you'll need to create a sender identity. There are two ways to do this, but we recommend creating a Single Sender to get set up quickly and test your email integration.

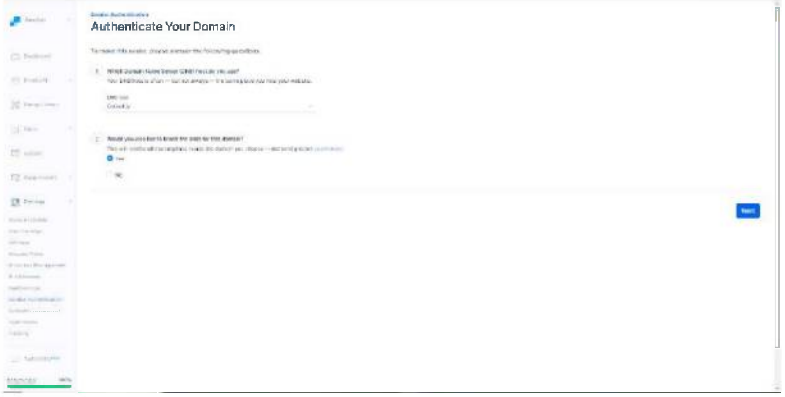
Create a Single Sender Authenticate a domain instead

Your sender identity is the "from" email address your recipients will see in their inbox. Learn more about this

Send your first email

Please create a sender identity before sending your first email.

16. On the Authenticate Your Domain page, select your DNS host, select Yes to rewrite all tracking links to use your chosen domain – not sendgrid.net, and click Next.

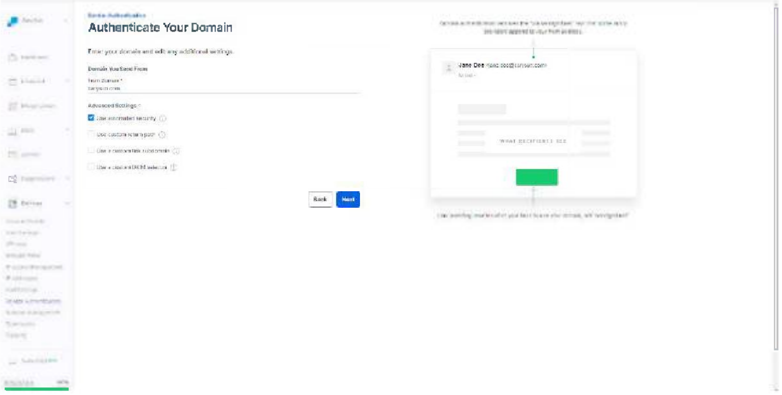


Authenticate Your Domain

● Yes

○ No

17. Enter your domain name on the Domain You Send From a page, and click Next.



Authenticate Your Domain

Enter your domain and edit any additional settings.

Domain You Send From

From Domain *

Advanced Settings

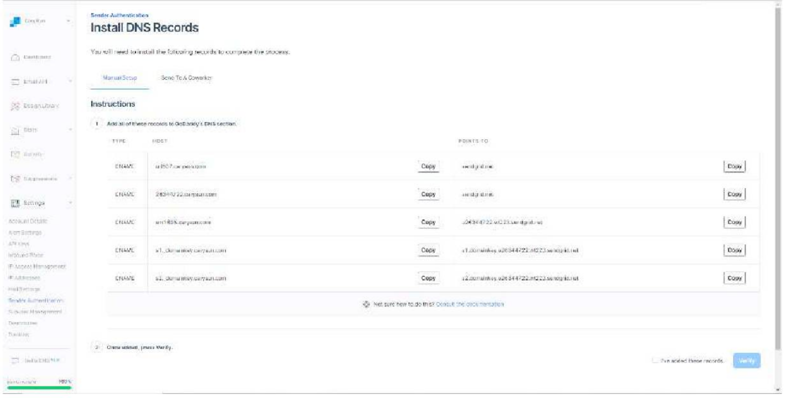
☑ Use automated security

□ Use custom return path

□ Use a custom link subdomain

□ Use a custom DKIM selector

18. On the Install DNS Records page, copy and add all these records to your External DNS records.



Sender Authentication

Install DNS Records

You will need to install the following records to complete the process.

Manual Setup | Send To A Coworker

Instructions

1 Add all of these records to GoDaddy's DNS section.

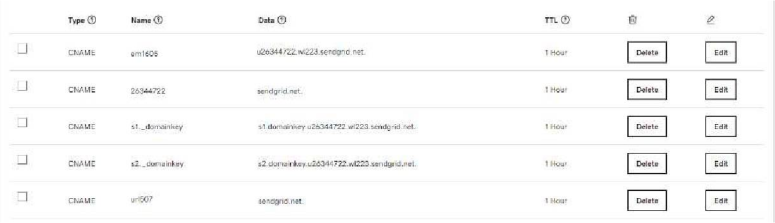
TYPE	HOST		POINTS TO	
CNAME	url507.caryaun.com	Copy	sendgrid.net	Copy
CNAME	26344722.caryaun.com	Copy	sendgrid.net	Copy
CNAME	em1606.caryaun.com	Copy	u26344722.wl223.sendgrid.net	Copy
CNAME	s1._domainkey.caryaun.com	Copy	s1.domainkey.u26344722.wl223.sendgrid.net	Copy
CNAME	s2._domainkey.caryaun.com	Copy	s2.domainkey.u26344722.wl223.sendgrid.net	Copy

Not sure how to do this? Consult the documentation

2 Once added, press Verify.

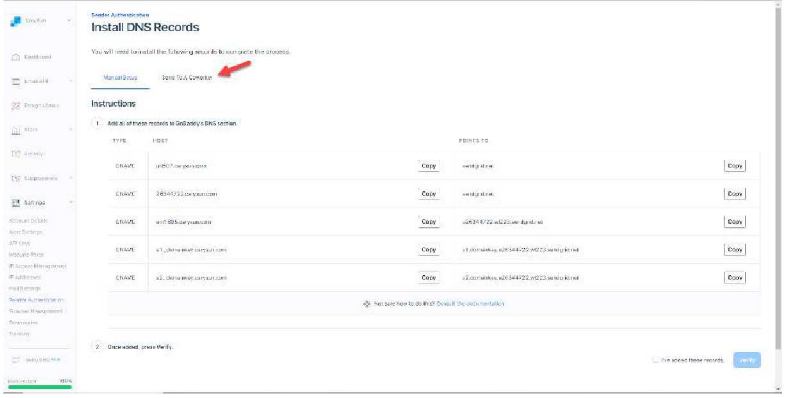
□ I've added these records. Verify

19. In my case, add them to GoDaddy.



	Type ⓘ	Name ⓘ	Data ⓘ	TTL ⓘ	🗑	✎
□	CNAME	em1606	u26344722.wl223.sendgrid.net.	1 Hour	Delete	Edit
□	CNAME	26344722	sendgrid.net.	1 Hour	Delete	Edit
□	CNAME	s1._domainkey	s1.domainkey.u26344722.wl223.sendgrid.net.	1 Hour	Delete	Edit
□	CNAME	s2._domainkey	s2.domainkey.u26344722.wl223.sendgrid.net.	1 Hour	Delete	Edit
□	CNAME	url507	sendgrid.net.	1 Hour	Delete	Edit

20. If you cannot add DNS records, select Send To A Coworker.



Sender Authentication

Install DNS Records

You will need to install the following records to complete the process.

Manual Setup | Send To A Coworker

Instructions

1 Add all of these records to GoDaddy's DNS section.

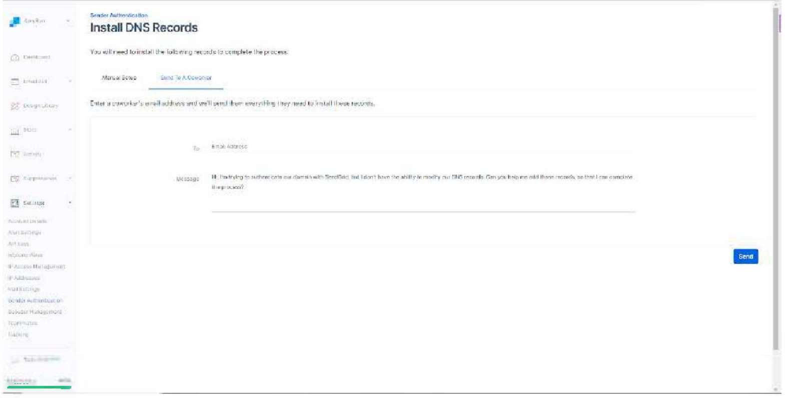
TYPE	HOST		POINTS TO	
CNAME	url507.caryaun.com	Copy	sendgrid.net	Copy
CNAME	26344722.caryaun.com	Copy	sendgrid.net	Copy
CNAME	em1606.caryaun.com	Copy	u26344722.wl223.sendgrid.net	Copy
CNAME	s1._domainkey.caryaun.com	Copy	s1.domainkey.u26344722.wl223.sendgrid.net	Copy
CNAME	s2._domainkey.caryaun.com	Copy	s2.domainkey.u26344722.wl223.sendgrid.net	Copy

Not sure how to do this? Consult the documentation

2 Once added, press Verify.

□ I've added these records. Verify

21. Type your coworker’s email address, and click Send. Then, ask your coworker to add these DNS records.



Sender Authentication

Install DNS Records

You will need to install the following records to complete the process.

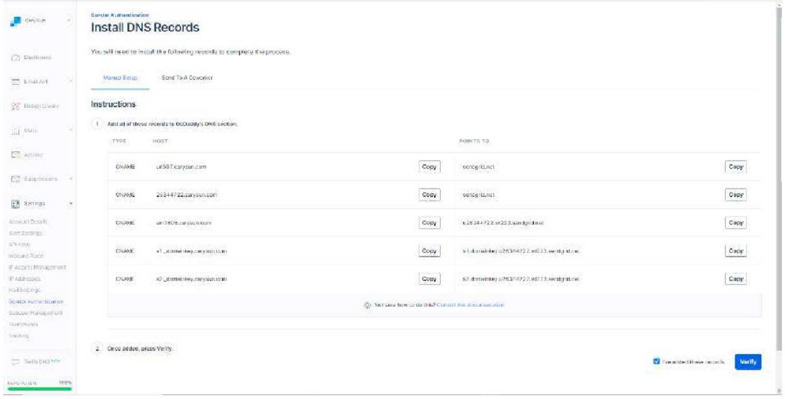
Manual Setup | Send To A Coworker

Enter a coworker's email address and we'll send them everything they need to install these records.

To: Email Address

Message: Hi, I'm trying to authenticate our domain with SendGrid, but I don't have the ability to modify our DNS records. Can you help me add these records, so that I can complete the process?

22. On the Install DNS Records page, select I've added these records, click Verify.



Sender Authentication

Install DNS Records

You will need to install the following records to complete the process.

Manual Setup | Send To A Coworker

Instructions

1 Add all of these records to GoDaddy's DNS section.

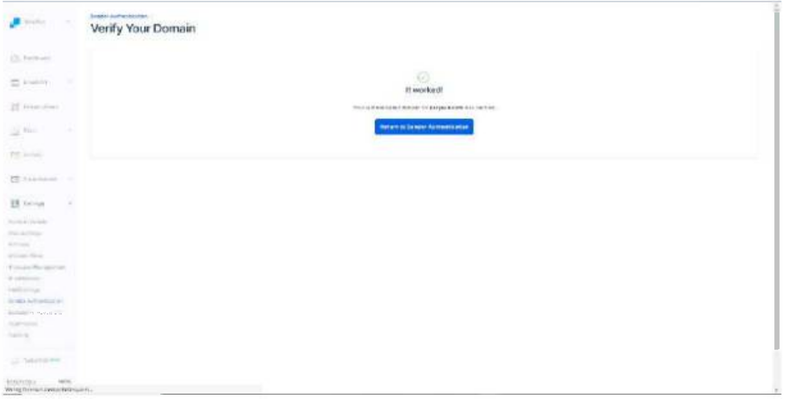
TYPE	HOST		POINTS TO	
CNAME	url507.carysun.com	Copy	sendgrid.net	Copy
CNAME	25344722.carysun.com	Copy	sendgrid.net	Copy
CNAME	em1808.carysun.com	Copy	u25344722.wl223.sendgrid.net	Copy
CNAME	s1._domainkey.carysun.com	Copy	s1.domainkey.u25344722.wl223.sendgrid.net	Copy
CNAME	s2._domainkey.carysun.com	Copy	s2.domainkey.u25344722.wl223.sendgrid.net	Copy

Not sure how to do this? Consult the documentation

2 Once added, press Verify.

☑ I've added these records. Verify

23. On the Verify Your Domain page, make sure your authenticated domain for the domain name was verified without issues and click Return to Sender Authentication.

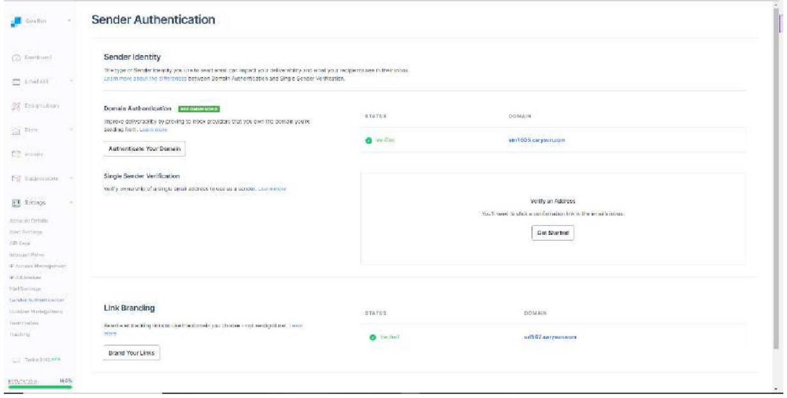


Sender Authentication

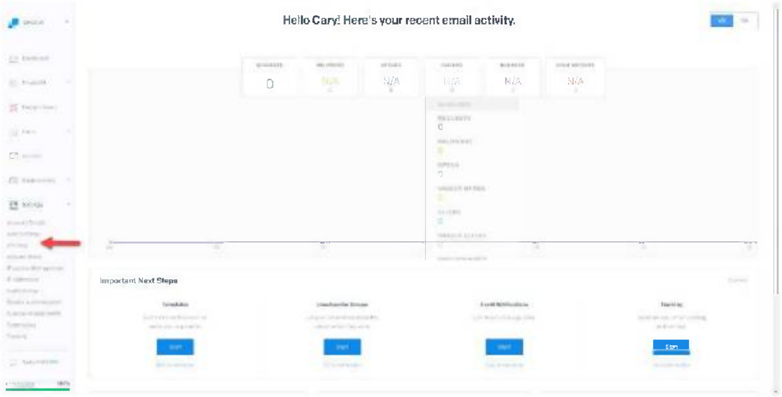
Verify Your Domain

It worked!

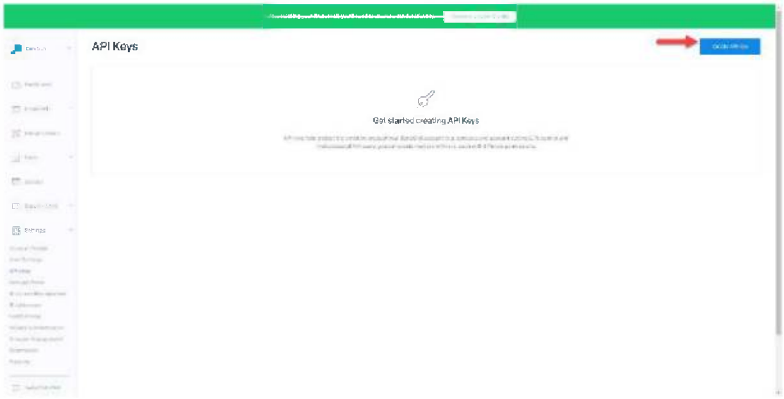
24. On the Sender Authentication page, ensure Domain Authentication and link Branding status is Verified.



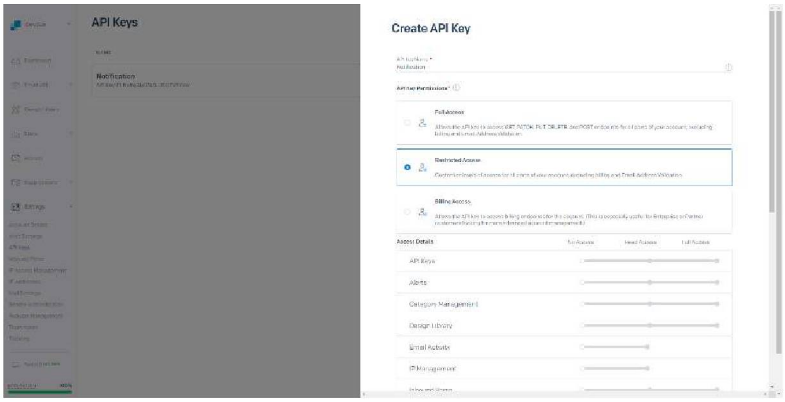
25. Under the Settings page, select API Keys.



26. On the API Keys page, select Create API Key.



27. On the Create API Key page, type the API Key Name and select Restricted Access as API Key Permissions.



Create API Key

API Key Name *
Notification

API Key Permissions *

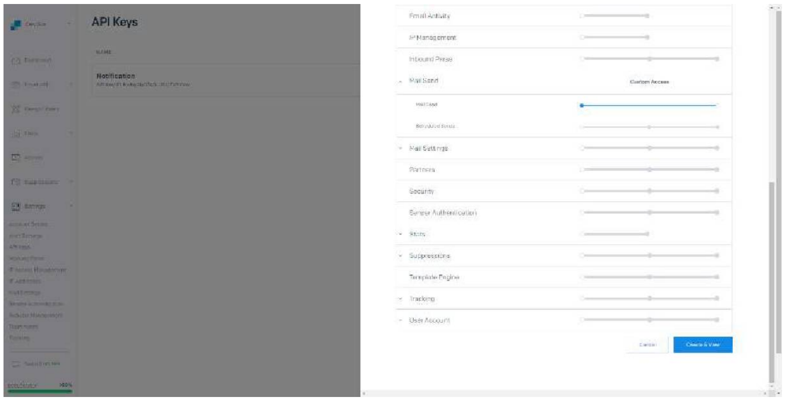
○ Full Access
Allows the API key to access GET, PATCH, PUT, DELETE and POST endpoints for all parts of your account, excluding billing and Email Address Validation.

● Restricted Access
Customize levels of access for all parts of your account, excluding billing and Email Address Validation.

○ Billing Access
Allows the API key to access billing endpoints for the account. (This is especially useful for Enterprise or Partner customers looking for more advanced account management.)

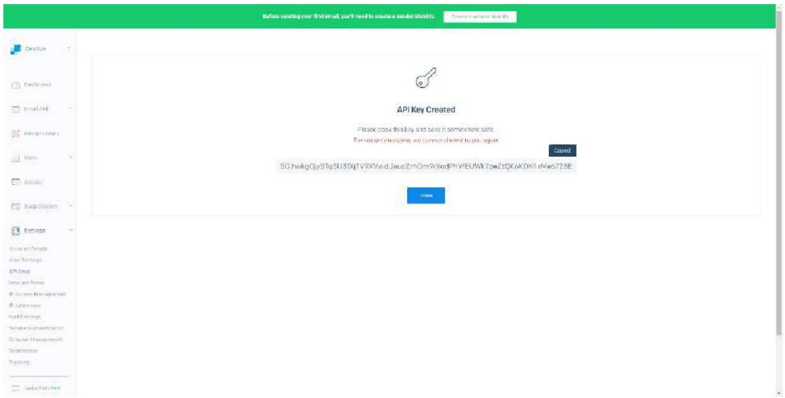
Access Details	No Access	Read Access	Full Access
API Keys			
Alerts			
Category Management			
Design Library			
Email Activity			
IP Management			
Inbound Parse			

28. Enable Mail Activity as Access Details, click Create & View.



Email Activity	
IP Management	
Inbound Parse	
Mail Send	Custom Access
Mail Send	
Scheduled Sends	
Mail Settings	
Partners	
Security	
Sender Authentication	
Stats	
Suppressions	
Template Engine	
Tracking	
User Account	

29. Copy the key on the API Key Created page, save it, and click Done.



Before sending your first email, you'll need to create a sender identity.

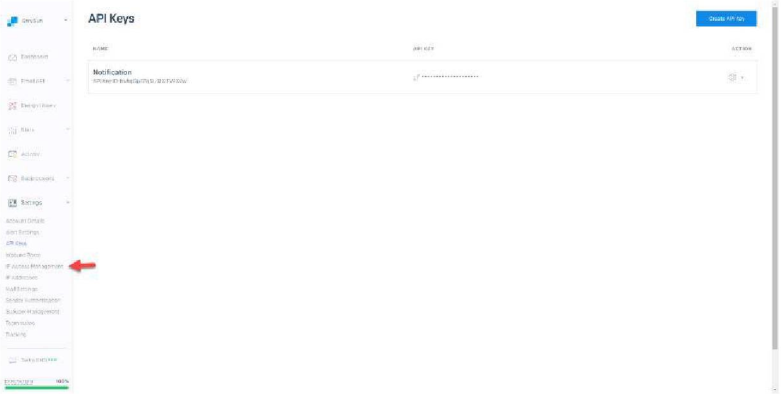
API Key Created

Please copy this key and save it somewhere safe.

For security reasons, we cannot show it to you again

SG.hwkgGjySTqSU3XqTV9XVw.dJaucZrhOm9rXedPhYfEUWk7peZtQK6KDXAxMe6728E

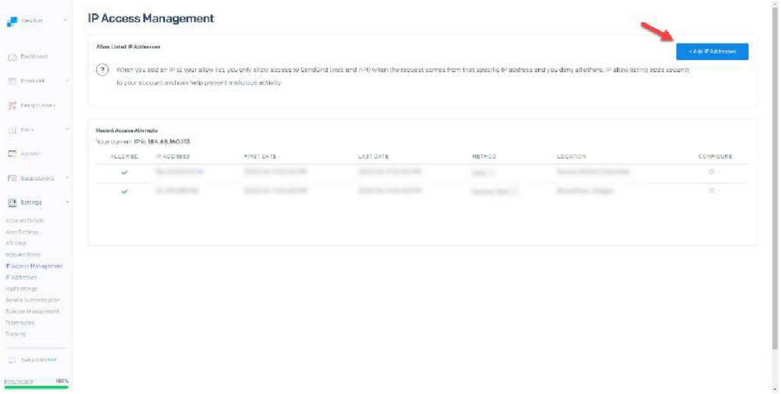
30. Under settings, select IP Access Management.



API Keys

NAME	API KEY	ACTION
Notification	••••••••••••••••••••	

31. On the IP Access Management page, click +Add UP Address.



IP Access Management

Allow Listed IP Addresses

+ Add IP Addresses

When you add an IP to your allow list, you only allow access to SendGrid (web and API) when the request comes from that specific IP address and you deny all others. IP allow listing adds security to your account and can help prevent malicious activity.

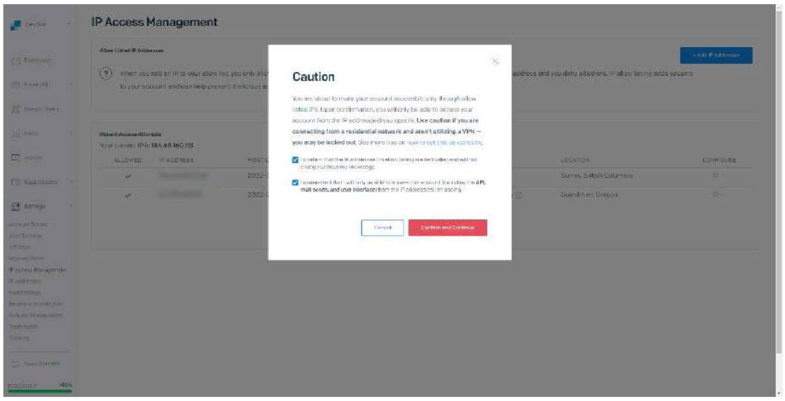
Recent Access Attempts

Your current IP is 184.65.160.113

ALLOWED	IP ADDRESS	FIRST DATE	LAST DATE	METHOD	LOCATION	CONFIGURE
✓						
✓						

32. On the Caution page, select I confirm that the IP addresses I'm allow listing are dedicated and will not change without my knowledge.

33. Select I understand that I will only be able to access this account (including the API, mail sends, and user interface) from the IP address(es) I'm adding,



Caution

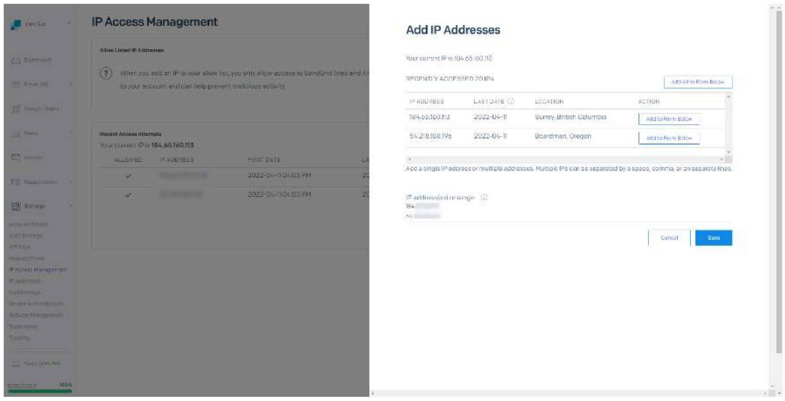
You are about to make your account accessible only through allow listed IPs. Upon confirmation, you will only be able to access your account from the IP address(es) you specify. **Use caution if you are connecting from a residential network and aren't utilizing a VPN — you may be locked out.** See more tips on how to set this up correctly.

☑ I confirm that the IP addresses I'm allow listing are dedicated and will not change without my knowledge.

☑ I understand that I will only be able to access this account (including the **API, mail sends, and user interface**) from the IP address(es) I'm adding.

34. Click Confirm and Continue.

35. On the Add IP Addresses page, add IP addresses or ranges you would like to allow access to SendGrid. Make sure to include the public IP address of the Veeam management server and click Save.



IP Access Management

Allow Listed IP Addresses

When you add an IP to your allow list, you only allow access to SendGrid (web and A to your account and can help prevent malicious activity

Recent Access Attempts

Your current IP is 184.65.160.113

ALLOWED	IP ADDRESS	FIRST DATE
✓	[redacted]	2022-04-11 04:03 PM
✓	[redacted]	2022-04-11 04:03 PM

Add IP Addresses

Your current IP is 184.65.160.113

RECENTLY ACCESSED 20 IPs

IP ADDRESS	LAST DATE	LOCATION	ACTION
184.65.160.113	2022-04-11	Surrey, British Columbia	Add to Form Below
54.218.168.195	2022-04-11	Boardman, Oregon	Add to Form Below

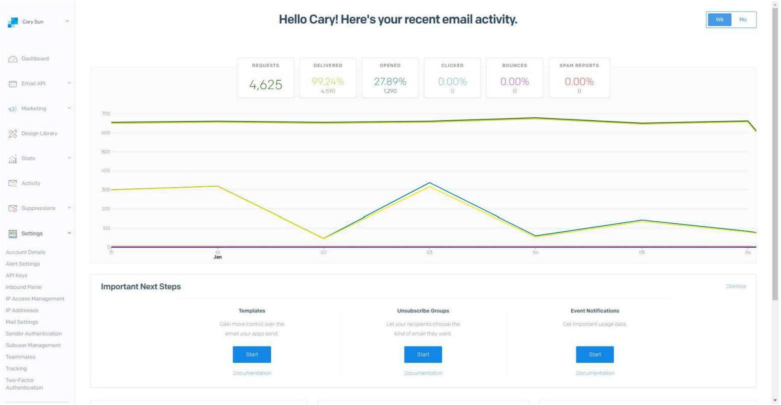
Add a single IP address or multiple addresses. Multiple IPs can be separated by a space, comma, or on separate lines.

IP address(es) or range

184.[redacted]

54.[redacted]

36. On the Home page, expand Settings and click Sender Authentication.



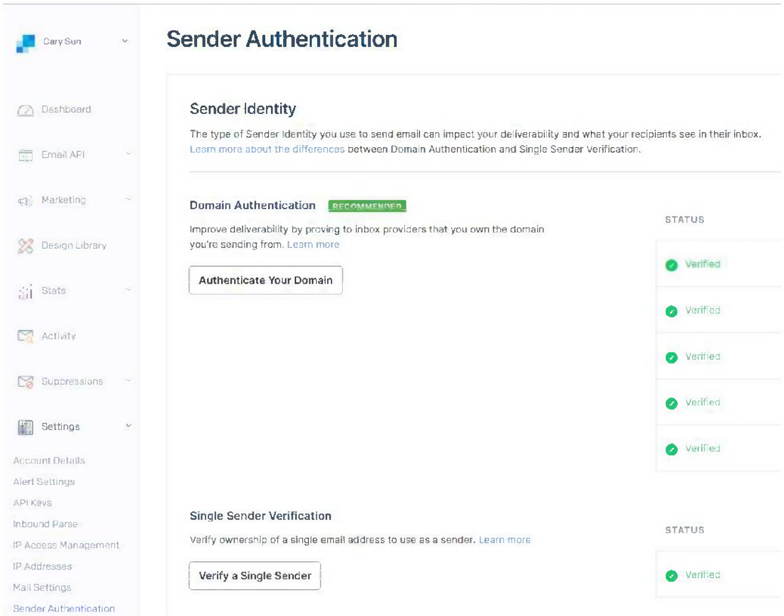
Hello Cary! Here's your recent email activity.

REQUESTS	DELIVERED	OPENED	CLICKED	BOUNCES	SPAM REPORTS
4,625	99.24% 4,590	27.89% 1,290	0.00% 0	0.00% 0	0.00% 0

Important Next Steps

Templates	Unsubscribe Groups	Event Notifications
Gain more control over the email your apps send.	Let your recipients choose the kind of email they want.	Get important usage data.

37. On the Sender Authentication page, click Authenticate Your Domain.



Sender Authentication

Sender Identity

The type of Sender Identity you use to send email can impact your deliverability and what your recipients see in their inbox. Learn more about the differences between Domain Authentication and Single Sender Verification.

Domain Authentication RECOMMENDED

Improve deliverability by proving to inbox providers that you own the domain you're sending from. Learn more

Authenticate Your Domain

STATUS

✓ Verified

✓ Verified

✓ Verified

✓ Verified

✓ Verified

Single Sender Verification

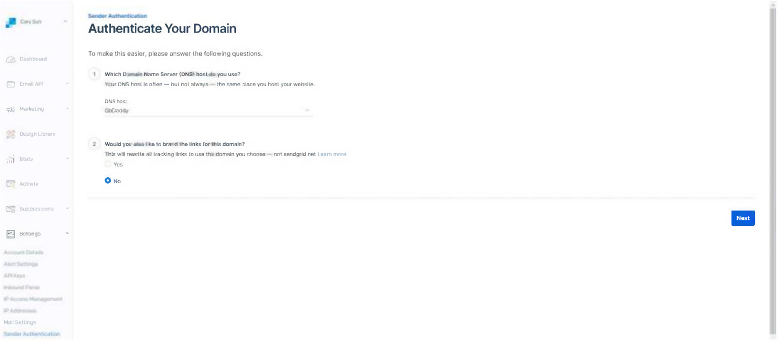
Verify ownership of a single email address to use as a sender. Learn more

Verify a Single Sender

STATUS

✓ Verified

38. Specify your DNS host from the drop-down list on the Authentication Your Domain page.
39. Select No Would you also like to brand the links for this domain?
40. Click Next.



Sender Authentication

Authenticate Your Domain

To make this easier, please answer the following questions.

1 Which Domain Name Server (DNS) host do you use?

Your DNS host is often — but not always — the same place you host your website.

DNS host
GoDaddy

2 Would you also like to brand the links for this domain?

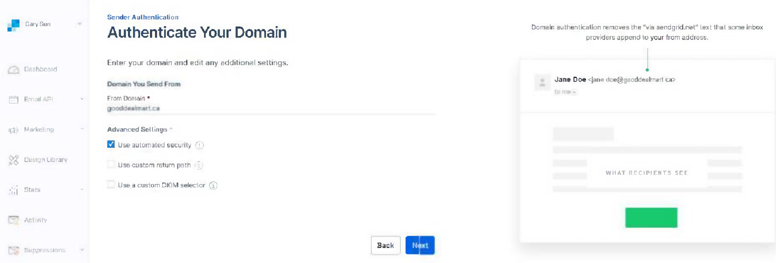
This will rewrite all tracking links to use this domain you choose — not sendgrid.net Learn more

○ Yes

● No

Next

41. On the Domain, You send From page, specify your FQDN name, and click Next.



Sender Authentication

Authenticate Your Domain

Enter your domain and edit any additional settings.

Domain You Send From

From Domain *
gooddealmart.ca

Advanced Settings ^

☑ Use automated security ⓘ

☐ Use custom return path ⓘ

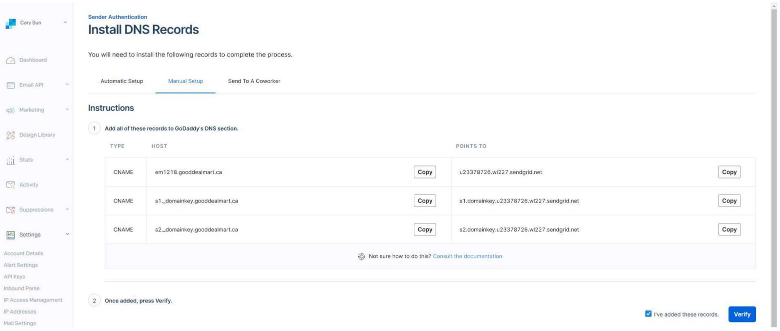
☐ Use a custom DKIM selector ⓘ

Back Next

Domain authentication removes the "via sendgrid.net" text that some inbox providers append to your from address.

Jane Doe <jane doe@gooddealmart ca>
to me

42. Add those CNAME records to your domain on the Install DNS Records page, select I've added these records, and click Verify.



Sender Authentication

Install DNS Records

You will need to install the following records to complete the process.

Instructions

1 Add all of these records to GoDaddy's DNS section.

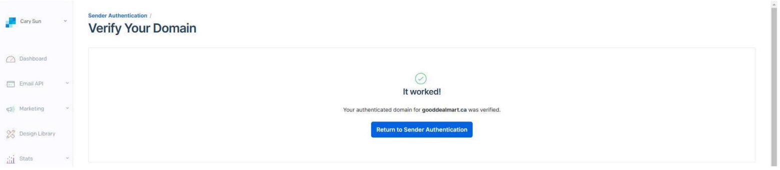
TYPE	HOST		POINTS TO	
CNAME	em1218.gooddealmart.ca	Copy	u23378726.wl227.sendgrid.net	Copy
CNAME	s1._domainkey.gooddealmart.ca	Copy	s1.domainkey.u23378726.wl227.sendgrid.net	Copy
CNAME	s2._domainkey.gooddealmart.ca	Copy	s2.domainkey.u23378726.wl227.sendgrid.net	Copy

Not sure how to do this? Consult the documentation

2 Once added, press Verify.

☑ I've added these records. Verify

43. On the Verify Your Domain page, ensure verification is successful and click Return to Send Authentication.



Sender Authentication /

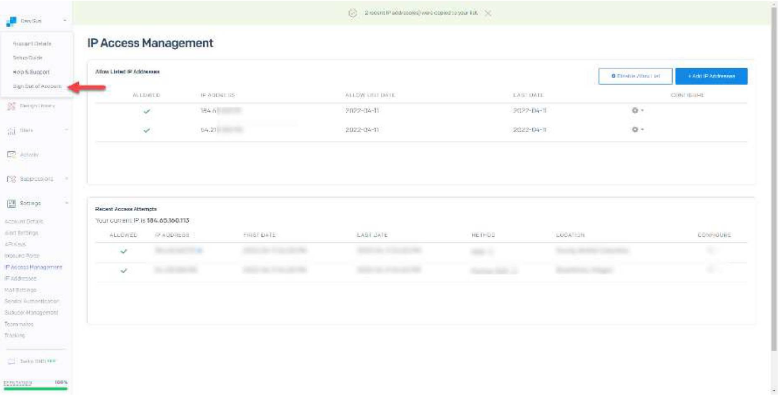
Verify Your Domain

It worked!

Your authenticated domain for **gooddealmart.ca** was verified.

Return to Sender Authentication

44. Sign Out of Account.



2 recent IP address(es) were copied to your list.

IP Access Management

Allow Listed IP Addresses

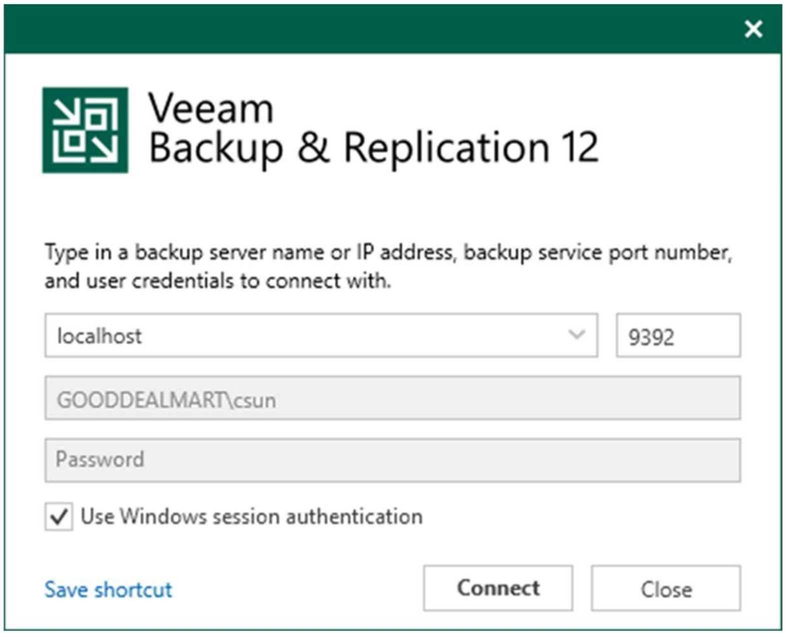
ALLOWED	IP ADDRESS	ALLOW LIST DATE	LAST DATE	CONFIGURE
✓	184.6[redacted]	2022-04-11	2022-04-11	⚙
✓	54.21[redacted]	2022-04-11	2022-04-11	⚙

Recent Access Attempts

Your current IP is 184.65.160.113

ALLOWED	IP ADDRESS	FIRST DATE	LAST DATE	METHOD	LOCATION	CONFIGURE
✓	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
✓	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	

45. Log in to the Veeam Backup and replication manager server.
46. Open the Veeam Backup & Replication Console and click Connect.



Veeam Backup & Replication 12

Type in a backup server name or IP address, backup service port number, and user credentials to connect with.

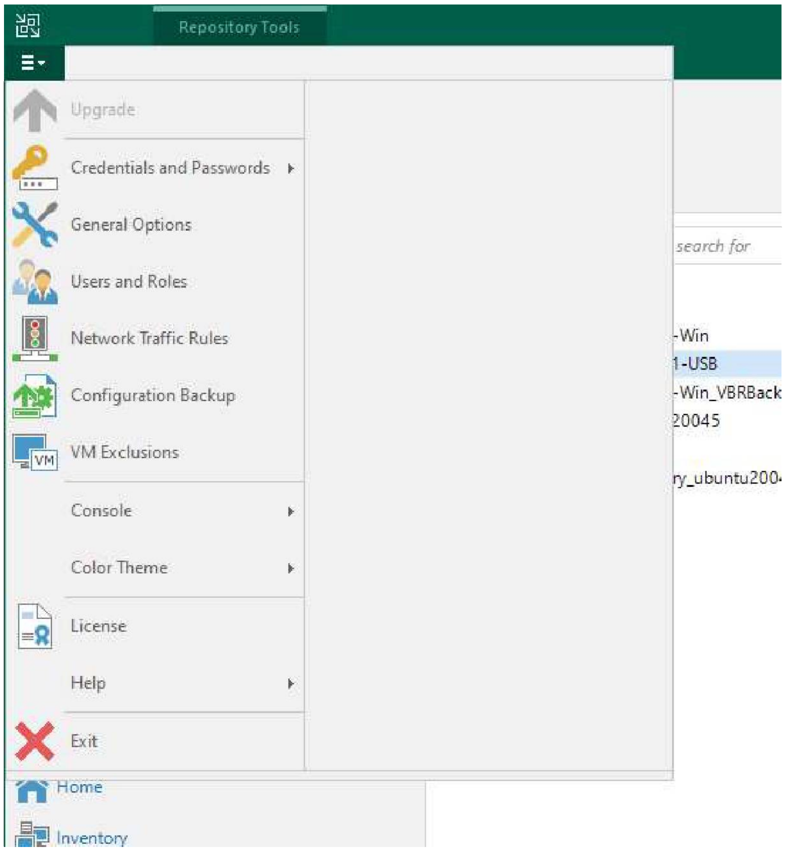
localhost 9392

GOODDEALMART\csun

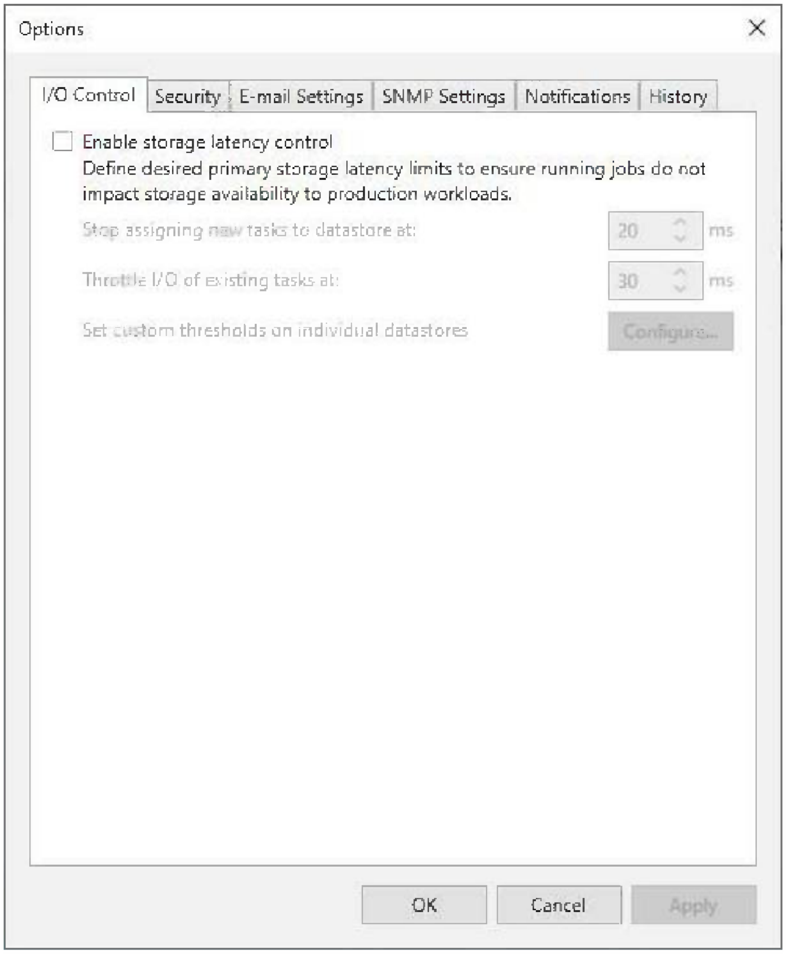
Password

☑ Use Windows session authentication

47. Select General Options from the main menu.



48. On the Options page, select Email Settings.



Options

I/O Control | Security | E-mail Settings | SNMP Settings | Notifications | History

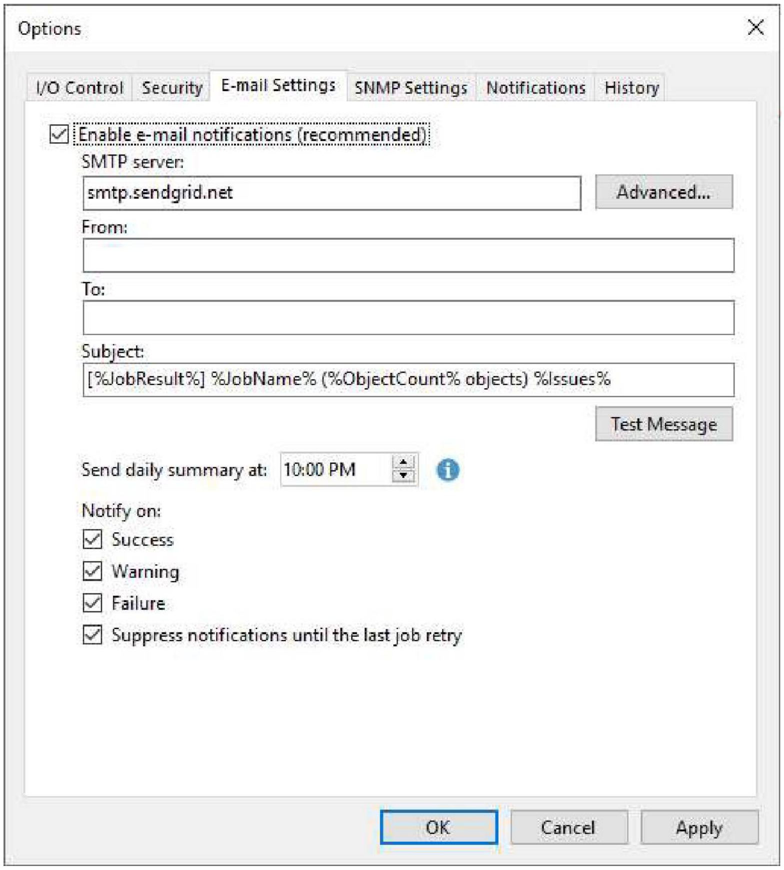
☐ Enable storage latency control
Define desired primary storage latency limits to ensure running jobs do not impact storage availability to production workloads.

Stop assigning new tasks to datastore at: 20 ms

Throttle I/O of existing tasks at: 30 ms

Set custom thresholds on individual datastores [Configure...]

49. Select Enable e-mail notification (recommend) on the Email Settings page.
50. In the SMTP server field, enter smtp.sendgrid.net, and click Advanced.



☑ Enable e-mail notifications (recommended)

SMTP server: smtp.sendgrid.net

From:

To:

Subject: [%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

Send daily summary at: 10:00 PM

Notify on:

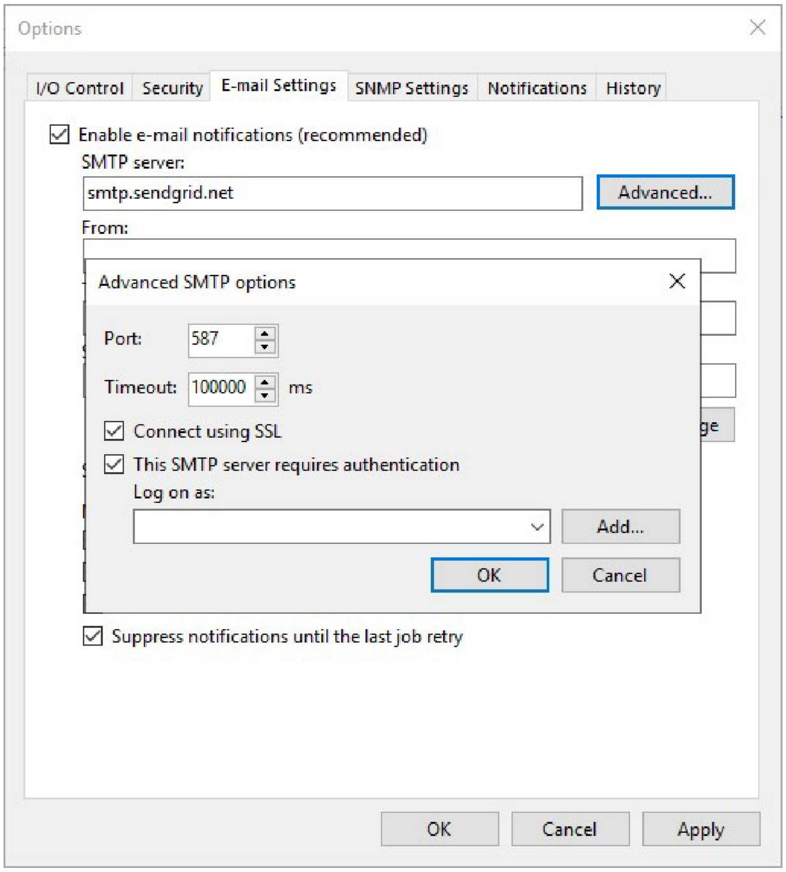
☑ Success

☑ Warning

☑ Failure

☑ Suppress notifications until the last job retry

51. On the Advanced SMTP options page, type 587 in the Port field.
52. Use 100000 milliseconds as the Timeout.
53. Select Connect using SSL.
54. Select This SMTP server requires authentication.
55. Click Add to add a credential as Log on as account.



☑ Enable e-mail notifications (recommended)

SMTP server: smtp.sendgrid.net

From:

Port: 587

Timeout: 100000 ms

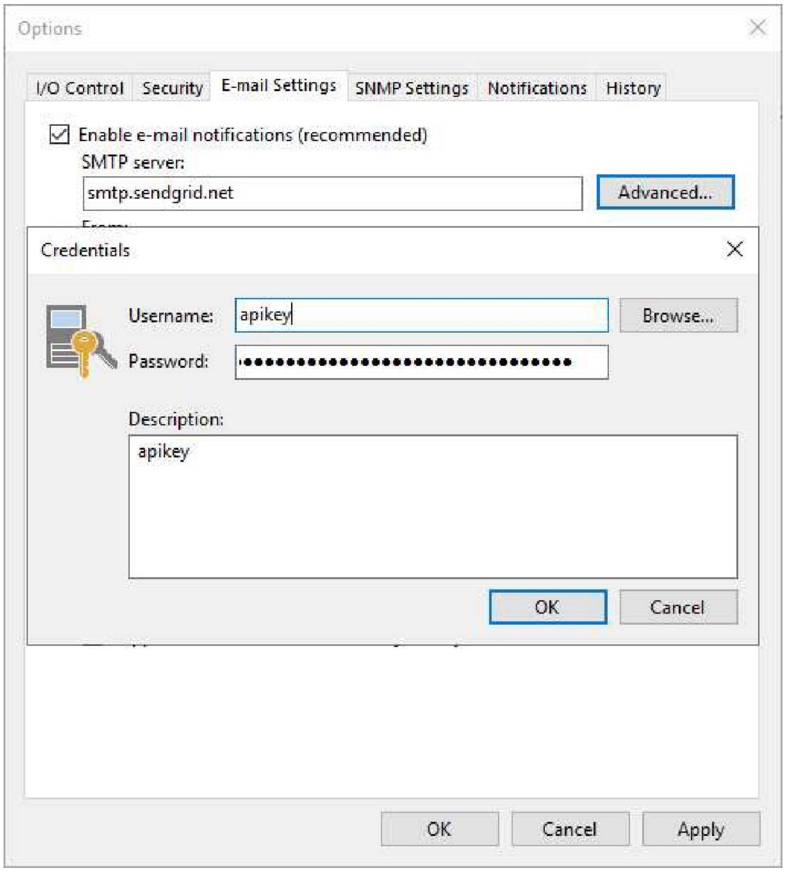
☑ Connect using SSL

☑ This SMTP server requires authentication

Log on as:

☑ Suppress notifications until the last job retry

56. Type apikey as Username.
57. Paste the apikey number as a password.
58. Click OK.



Options

☑ Enable e-mail notifications (recommended)

SMTP server: smtp.sendgrid.net

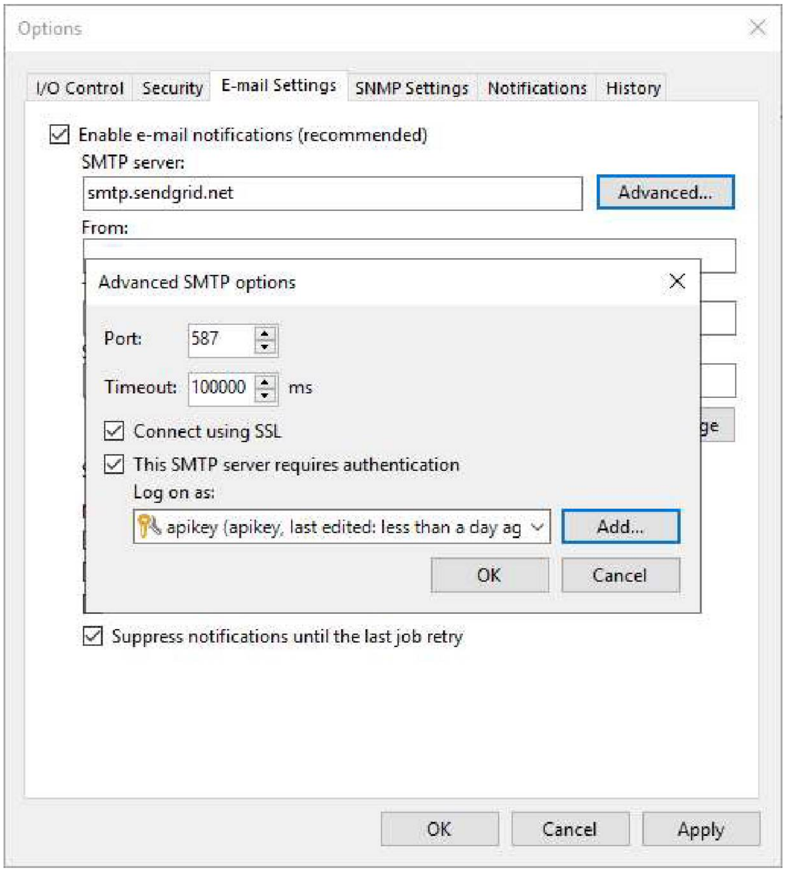
Credentials

Username: apikey

Password: ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●

Description: apikey

59. On the Advanced SMTP options page, click OK.



☑ Enable e-mail notifications (recommended)

SMTP server: smtp.sendgrid.net

From:

Advanced SMTP options

Port: 587

Timeout: 100000 ms

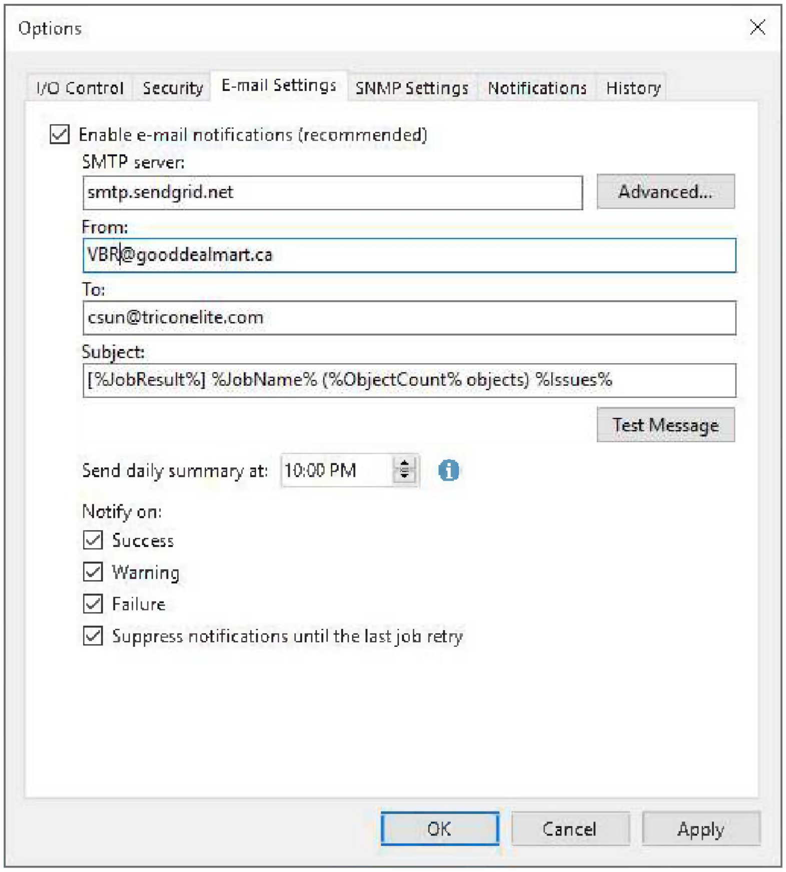
☑ Connect using SSL

☑ This SMTP server requires authentication

Log on as: apikey (apikey, last edited: less than a day ag

☑ Suppress notifications until the last job retry

60. In the From field, enter an email address you want to use as a sender.
61. In the To field, enter an email address of a notification recipient. To specify multiple email addresses, use a semicolon.
62. Click Test Message.



☑ Enable e-mail notifications (recommended)

SMTP server: smtp.sendgrid.net

From: VBR@gooddealmart.ca

To: csun@triconelite.com

Subject: [%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

Send daily summary at: 10:00 PM

Notify on:

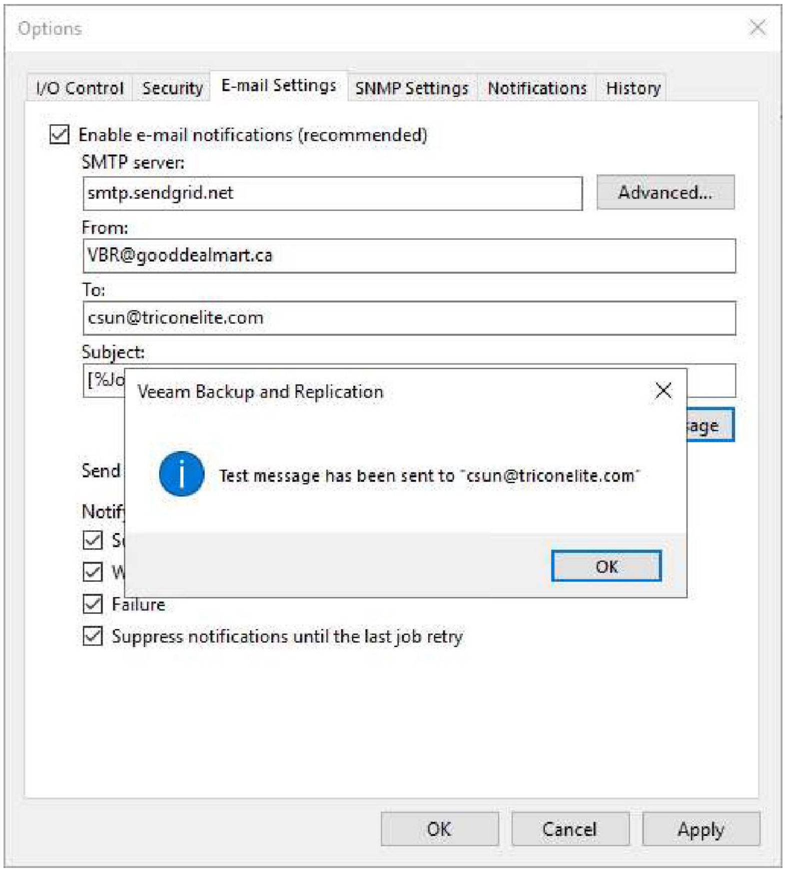
☑ Success

☑ Warning

☑ Failure

☑ Suppress notifications until the last job retry

63. Verify the test message sent successfully, and click OK.



☑ Enable e-mail notifications (recommended)

SMTP server: smtp.sendgrid.net

From: VBR@gooddealmart.ca

To: csun@triconelite.com

Subject: [%Jo

Send

Notif

☑ S

☑ W

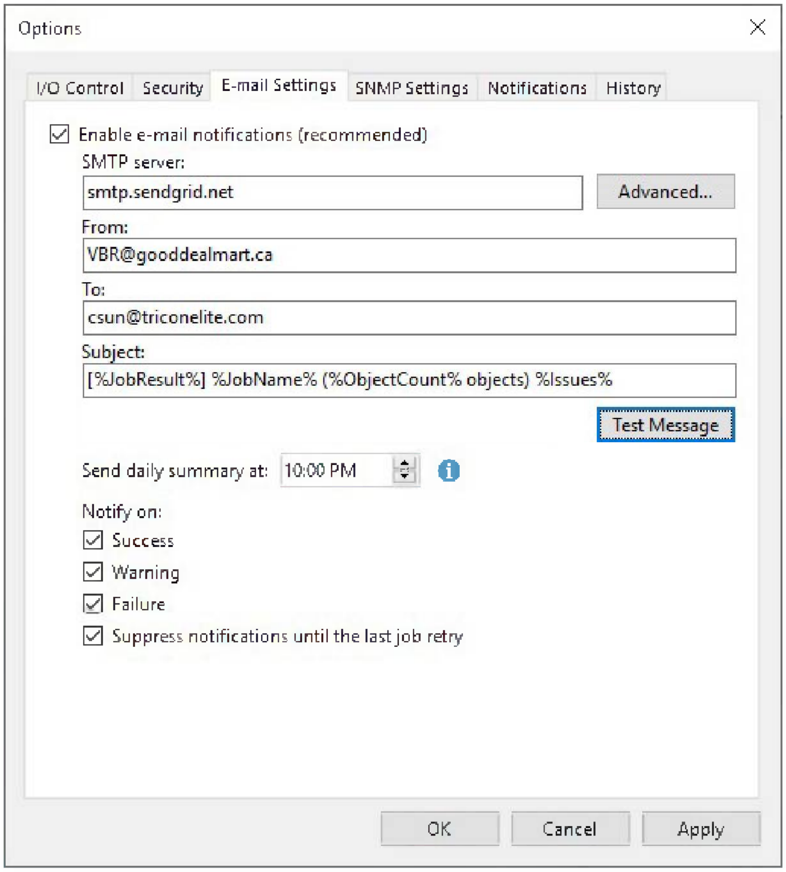
☑ Failure

☑ Suppress notifications until the last job retry

Veeam Backup and Replication

Test message has been sent to "csun@triconelite.com"

64. On the Options page, click OK.



☑ Enable e-mail notifications (recommended)

SMTP server: smtp.sendgrid.net

From: VBR@gooddealmart.ca

To: csun@triconelite.com

Subject: [%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

Send daily summary at: 10:00 PM

Notify on:

☑ Success

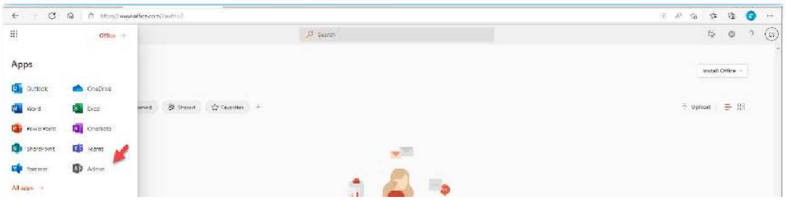
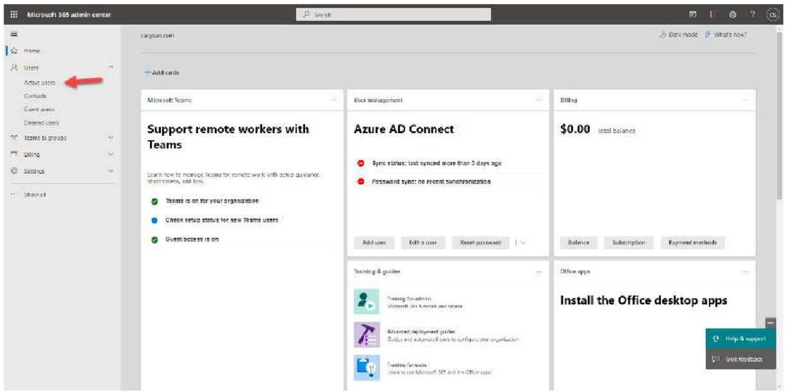
☑ Warning

☑ Failure

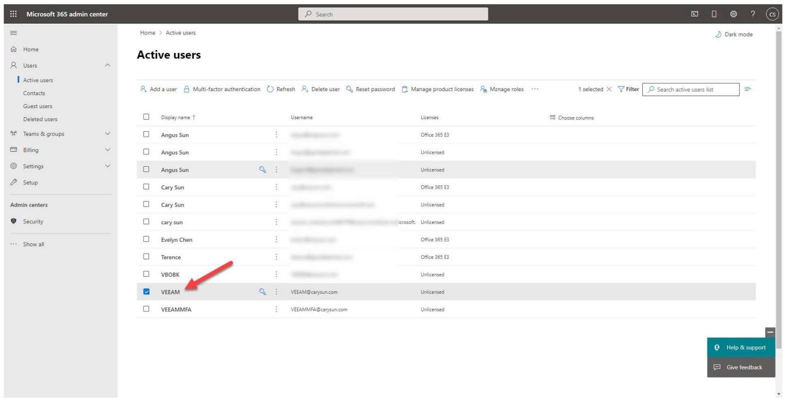
☑ Suppress notifications until the last job retry

Configure Notification with Microsoft Office 365 NON-MFA Account

You can configure Microsoft Office 365 non-MFA account for notification settings if you want Veeam Backup & Replication to send email notifications about backup job results.

Instructions	Screenshot (if applicable)
1. Sign in Office 365 portal with a Global Admin account and select Admin.	 Office Search Apps Outlook OneDrive Word Excel PowerPoint OneNote SharePoint Teams Yammer Admin All apps Shared Favorites Install Office Upload
2. On the Microsoft 365 admin center, expand Users and select Active users.	 Microsoft 365 admin center Search Dark mode What's new? Home Users Active users Contacts Guest users Deleted users Teams & groups Billing Settings Show all Add cards Microsoft Teams Support remote workers with Teams Teams is on for your organization Check setup status for new Teams users Guest access is on User management Azure AD Connect Sync status: last synced more than 3 days ago Password sync: no recent synchronization Add user Edit a user Reset password Billing $0.00 total balance Balance Subscription Payment methods Training & guides Training for admins Advanced deployment guides Training for users Office apps Install the Office desktop apps Help & support Give feedback

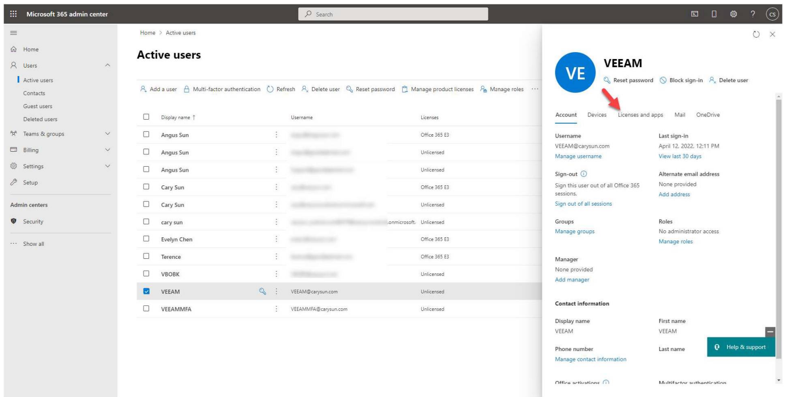
3. On the Active users' page, click Veeam service account (in my case, VEEAM).



Active users

	Display name ↑	Username	Licenses
□	Angus Sun	[redacted]	Office 365 E3
□	Angus Sun	[redacted]	Unlicensed
□	Angus Sun	[redacted]	Unlicensed
□	Cary Sun	[redacted]	Office 365 E3
□	Cary Sun	[redacted]	Unlicensed
□	cary sun	[redacted] icrosoft.	Unlicensed
□	Evelyn Chen	[redacted]	Office 365 E3
□	Terence	[redacted]	Office 365 E3
□	VBOBK	[redacted]	Unlicensed
☑	VEEAM	VEEAM@carysun.com	Unlicensed
□	VEEAMMFA	VEEAMMFA@carysun.com	Unlicensed

4. On the account page, select License and apps.



VEEAM

Username
VEEAM@carysun.com
Manage username

Last sign-in
April 12, 2022, 12:11 PM
View last 30 days

Sign-out
Sign this user out of all Office 365 sessions.
Sign out of all sessions

Alternate email address
None provided
Add address

Groups
Manage groups

Roles
No administrator access
Manage roles

Manager
None provided
Add manager

Contact information

Display name
VEEAM

First name
VEEAM

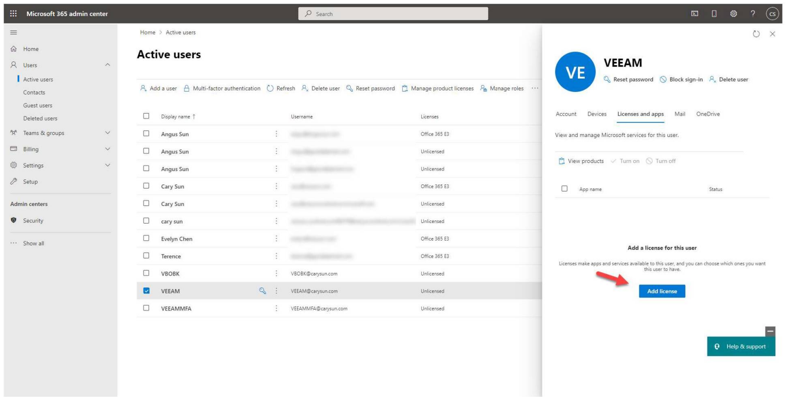
Phone number
Manage contact information

Last name

Office activations

Multifactor authentication

5. On the License and apps page, click Add license.



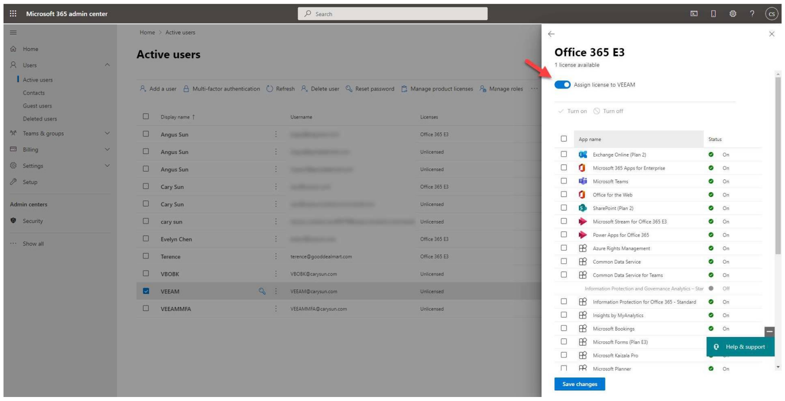
VEEAM

View and manage Microsoft services for this user.

Add a license for this user

Licenses make apps and services available to this user, and you can choose which ones you want this user to have.

6. On the Office 365 license page, enable Assign license to the account and click Save changes.



Active users

☐	Display name ↑	Username	Licenses
☐	Angus Sun	[redacted]	Office 365 E3
☐	Angus Sun	[redacted]	Unlicensed
☐	Angus Sun	[redacted]	Unlicensed
☐	Cary Sun	[redacted]	Office 365 E3
☐	Cary Sun	[redacted]	Unlicensed
☐	cary sun	[redacted]	Unlicensed
☐	Evelyn Chen	[redacted]	Office 365 E3
☐	Terence	terence@gooddealmart.com	Office 365 E3
☐	VBOBK	VBOBK@carysun.com	Unlicensed
☑	VEEAM	VEEAM@carysun.com	Unlicensed
☐	VEEAMMFA	VEEAMMFA@carysun.com	Unlicensed

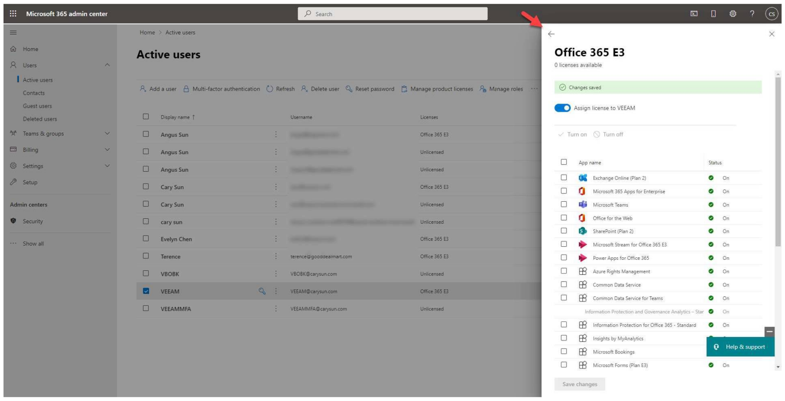
Office 365 E3

1 license available

Assign license to VEEAM

☐	App name	Status
☐	Exchange Online (Plan 2)	On
☐	Microsoft 365 Apps for Enterprise	On
☐	Microsoft Teams	On
☐	Office for the Web	On
☐	SharePoint (Plan 2)	On
☐	Microsoft Stream for Office 365 E3	On
☐	Power Apps for Office 365	On
☐	Azure Rights Management	On
☐	Common Data Service	On
☐	Common Data Service for Teams	On
	Information Protection and Governance Analytics – Star	Off
☐	Information Protection for Office 365 - Standard	On
☐	Insights by MyAnalytics	On
☐	Microsoft Bookings	On
☐	Microsoft Forms (Plan E3)	
☐	Microsoft Kaizala Pro	
☐	Microsoft Planner	On

7. Click Back <--.



Active users

☐	Display name ↑	Username	Licenses
☐	Angus Sun	[redacted]	Office 365 E3
☐	Angus Sun	[redacted]	Unlicensed
☐	Angus Sun	[redacted]	Unlicensed
☐	Cary Sun	[redacted]	Office 365 E3
☐	Cary Sun	[redacted]	Unlicensed
☐	cary sun	[redacted]	Unlicensed
☐	Evelyn Chen	[redacted]	Office 365 E3
☐	Terence	terence@gooddealmart.com	Office 365 E3
☐	VBOBK	VBOBK@carysun.com	Unlicensed
☑	VEEAM	VEEAM@carysun.com	Office 365 E3
☐	VEEAMMFA	VEEAMMFA@carysun.com	Unlicensed

Office 365 E3

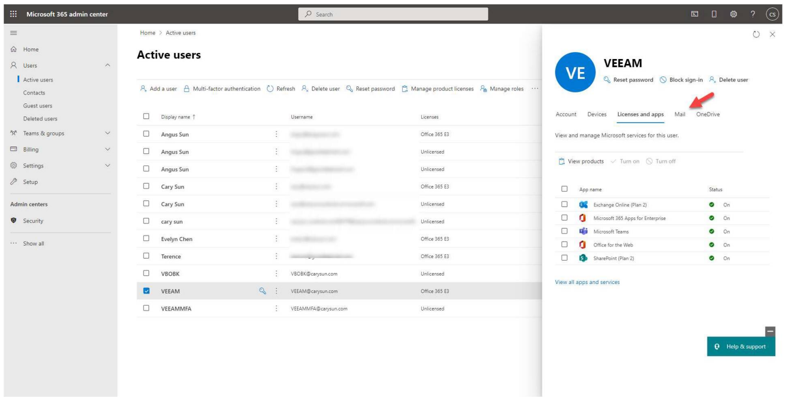
0 licenses available

Changes saved

Assign license to VEEAM

☐	App name	Status
☐	Exchange Online (Plan 2)	On
☐	Microsoft 365 Apps for Enterprise	On
☐	Microsoft Teams	On
☐	Office for the Web	On
☐	SharePoint (Plan 2)	On
☐	Microsoft Stream for Office 365 E3	On
☐	Power Apps for Office 365	On
☐	Azure Rights Management	On
☐	Common Data Service	On
☐	Common Data Service for Teams	On
	Information Protection and Governance Analytics – Star	On
☐	Information Protection for Office 365 - Standard	On
☐	Insights by MyAnalytics	On
☐	Microsoft Bookings	On
☐	Microsoft Forms (Plan E3)	On

8. On the account page, select Mail. It would be preferable to wait a few minutes before preparing a mailbox for the user.



Active users

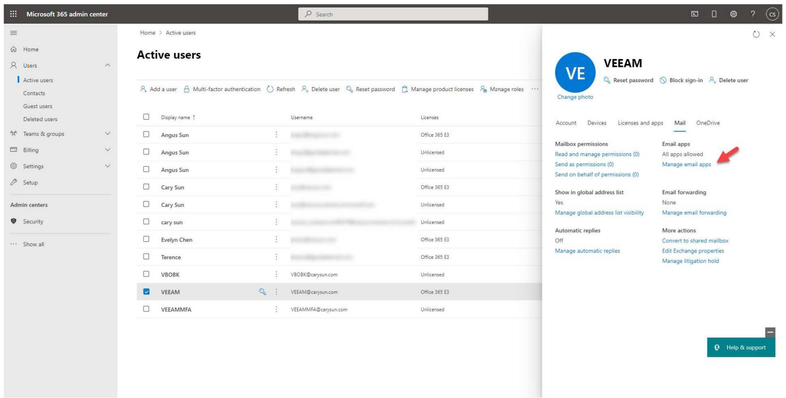
☐	Display name ↑	Username	Licenses
☐	Angus Sun	[redacted]	Office 365 E3
☐	Angus Sun	[redacted]	Unlicensed
☐	Angus Sun	[redacted]	Unlicensed
☐	Cary Sun	[redacted]	Office 365 E3
☐	Cary Sun	[redacted]	Unlicensed
☐	cary sun	[redacted]	Unlicensed
☐	Evelyn Chen	[redacted]	Office 365 E3
☐	Terence	[redacted]	Office 365 E3
☐	VBOBK	VBOBK@carysun.com	Unlicensed
☑	VEEAM	VEEAM@carysun.com	Office 365 E3
☐	VEEAMMFA	VEEAMMFA@carysun.com	Unlicensed

VEEAM

View and manage Microsoft services for this user.

☐	App name	Status
☐	Exchange Online (Plan 2)	On
☐	Microsoft 365 Apps for Enterprise	On
☐	Microsoft Teams	On
☐	Office for the Web	On
☐	SharePoint (Plan 2)	On

9. On the Mail page, select Manage email apps.



Active users

	Display name ↑	Username	Licenses
□	Angus Sun	[redacted]	Office 365 E3
□	Angus Sun	[redacted]	Unlicensed
□	Angus Sun	[redacted]	Unlicensed
□	Cary Sun	[redacted]	Office 365 E3
□	Cary Sun	[redacted]	Unlicensed
□	cary sun	[redacted]	Unlicensed
□	Evelyn Chen	[redacted]	Office 365 E3
□	Terence	[redacted]	Office 365 E3
□	VBOBK	VBOBK@carysun.com	Unlicensed
☑	VEEAM	VEEAM@carysun.com	Office 365 E3
□	VEEAMMFA	VEEAMMFA@carysun.com	Unlicensed

VEEAM

Mailbox permissions
Read and manage permissions (0)
Send as permissions (0)
Send on behalf of permissions (0)

Email apps
All apps allowed
Manage email apps

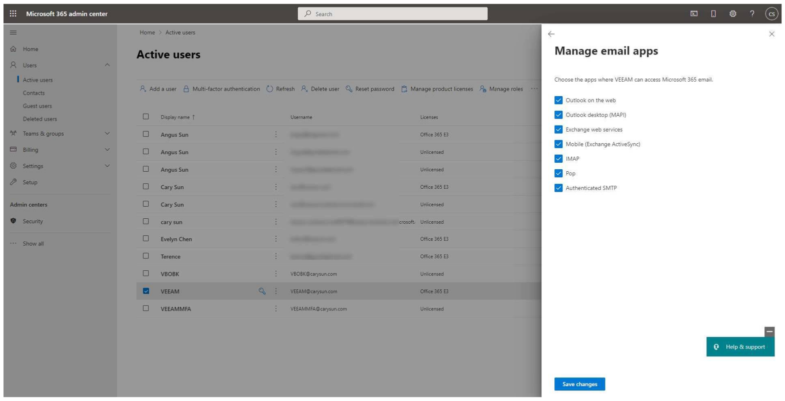
Show in global address list
Yes
Manage global address list visibility

Email forwarding
None
Manage email forwarding

Automatic replies
Off
Manage automatic replies

More actions
Convert to shared mailbox
Edit Exchange properties
Manage litigation hold

10. On the Manage email apps, select Authenticated SMTP and click Save changes.



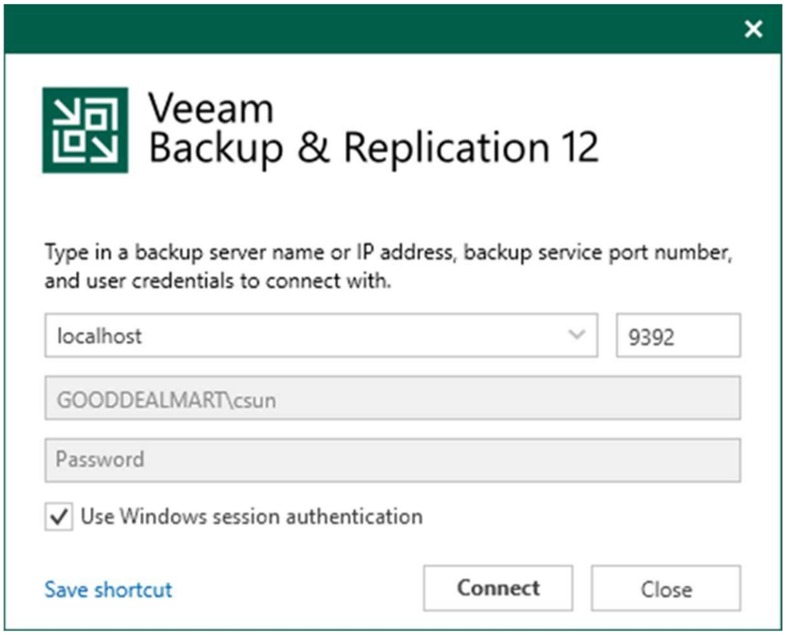
	Display name ↑	Username	Licenses
□	Angus Sun	[redacted]	Office 365 E3
□	Angus Sun	[redacted]	Unlicensed
□	Angus Sun	[redacted]	Unlicensed
□	Cary Sun	[redacted]	Office 365 E3
□	Cary Sun	[redacted]	Unlicensed
□	cary sun	[redacted]	Unlicensed
□	Evelyn Chen	[redacted]	Office 365 E3
□	Terence	[redacted]	Office 365 E3
□	VBOBK	VBOBK@carysun.com	Unlicensed
☑	VEEAM	VEEAM@carysun.com	Office 365 E3
□	VEEAMMFA	VEEAMMFA@carysun.com	Unlicensed

Manage email apps

Choose the apps where VEEAM can access Microsoft 365 email.

☑ Outlook on the web
☑ Outlook desktop (MAPI)
☑ Exchange web services
☑ Mobile (Exchange ActiveSync)
☑ IMAP
☑ Pop
☑ Authenticated SMTP

11. Log in to the Veeam Backup and replication manager server.
12. Open the Veeam Backup & Replication Console and click Connect.



Veeam
Backup & Replication 12

Type in a backup server name or IP address, backup service port number, and user credentials to connect with.

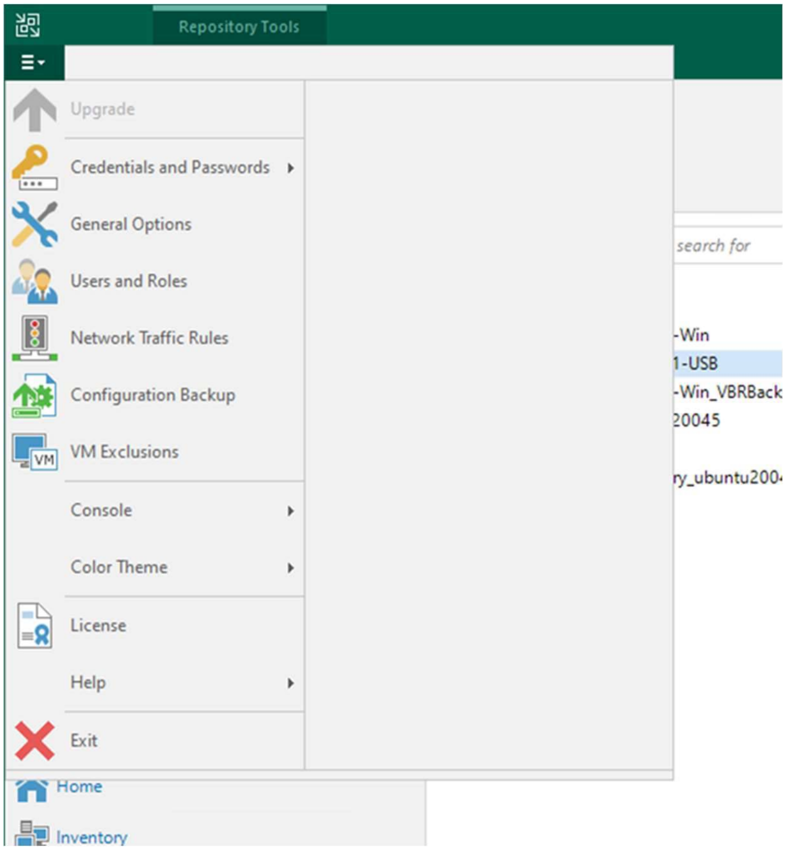
localhost 9392

GOODDEALMART\csun

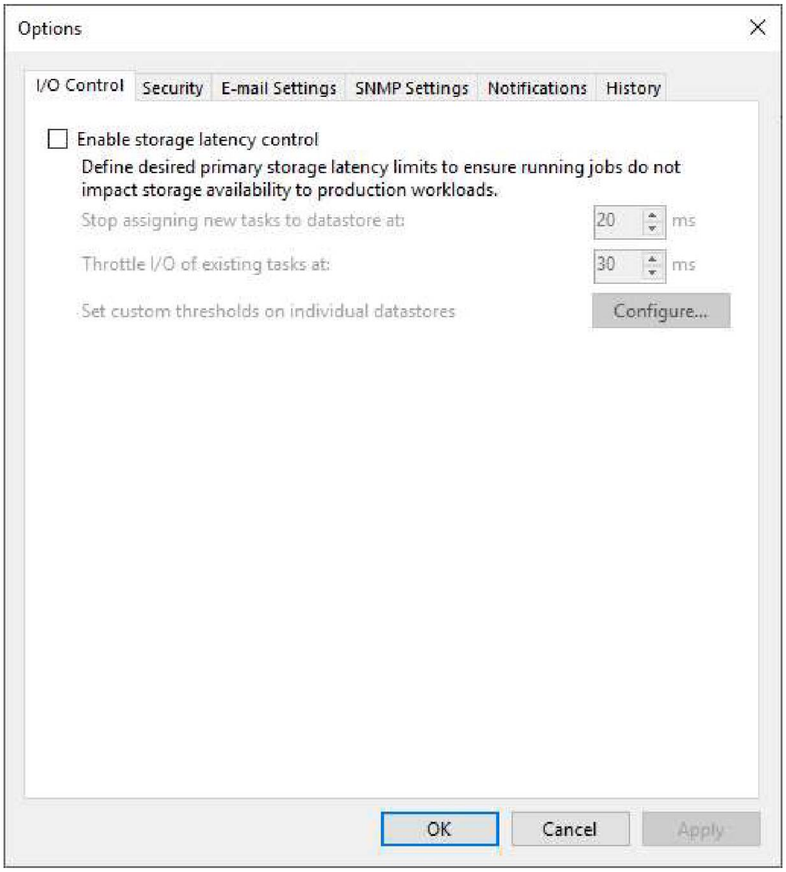
Password

☑ Use Windows session authentication

13. Select General Options from the main menu.



14. On the Options page, select Email Settings.



☐ Enable storage latency control

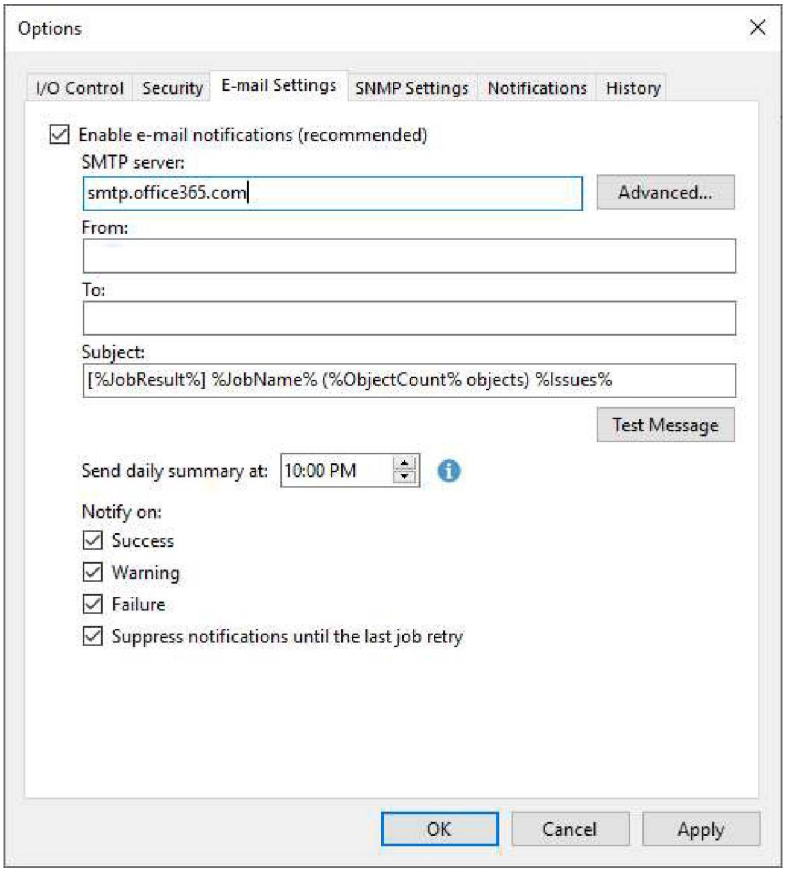
Define desired primary storage latency limits to ensure running jobs do not impact storage availability to production workloads.

Stop assigning new tasks to datastore at: 20 ms

Throttle I/O of existing tasks at: 30 ms

Set custom thresholds on individual datastores

15. Select Enable e-mail notification (recommend) on the Email Settings page.
16. In the SMTP server field, enter smtp.sendgrid.net, and click Advanced.



☑ Enable e-mail notifications (recommended)

SMTP server: smtp.office365.com

From:

To:

Subject: [%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

Send daily summary at: 10:00 PM

Notify on:

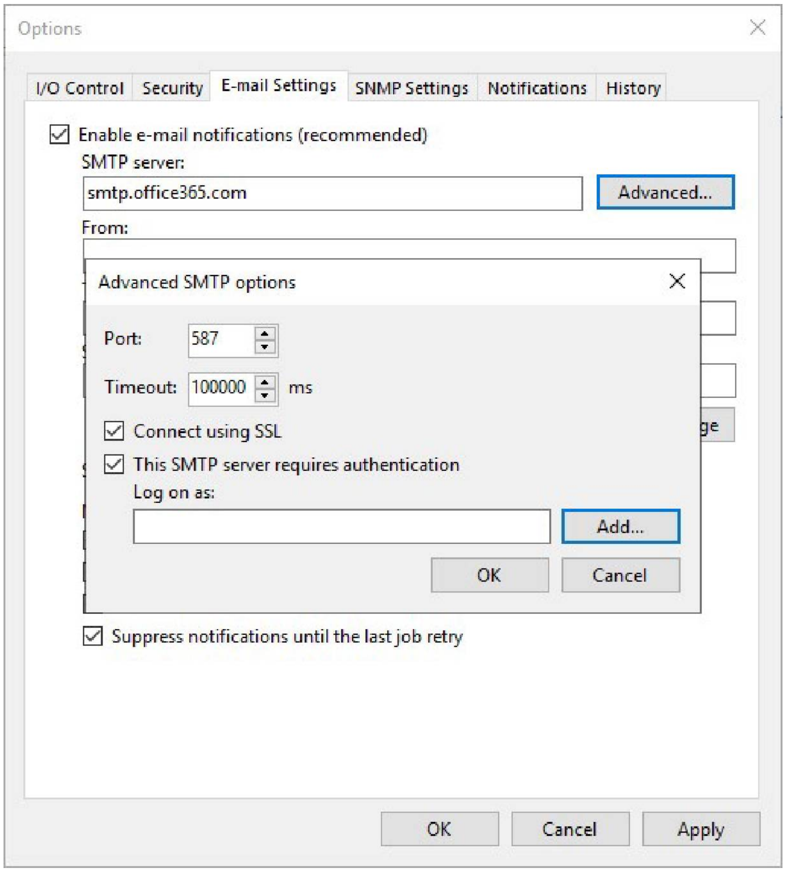
☑ Success

☑ Warning

☑ Failure

☑ Suppress notifications until the last job retry

17. On the Advanced SMTP options page, enter 587 in the Port field.
18. Use 100000 milliseconds as the Timeout.
19. Select Connect using SSL.
20. Select This SMTP server requires authentication.
21. Click Add to add a credential as Log on as account.



☑ Enable e-mail notifications (recommended)

SMTP server: smtp.office365.com

From:

Port: 587

Timeout: 100000 ms

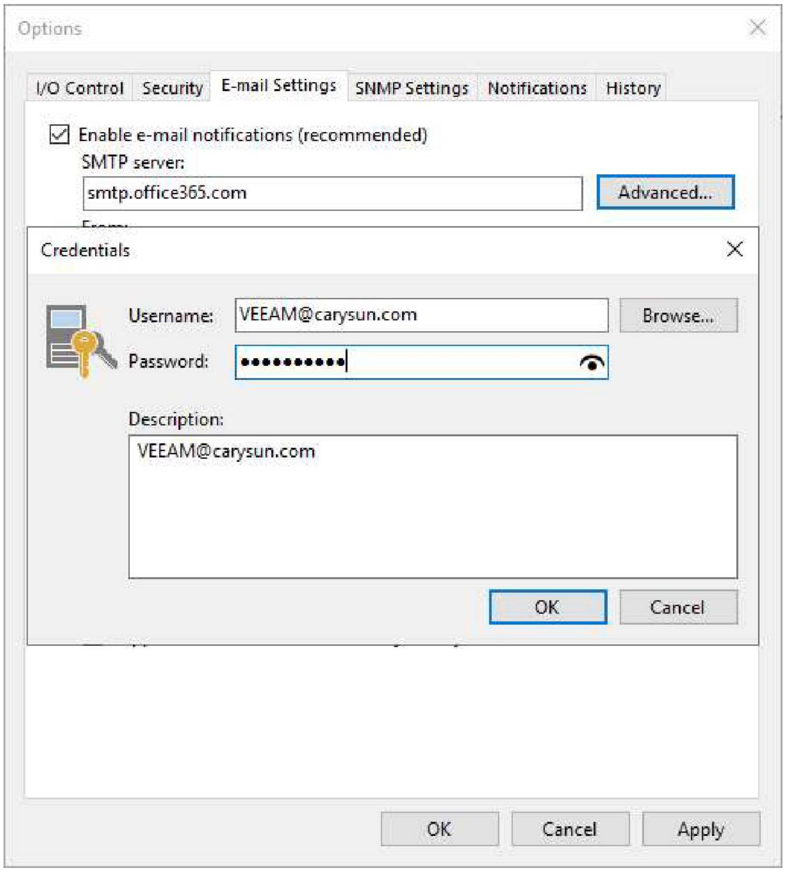
☑ Connect using SSL

☑ This SMTP server requires authentication

Log on as:

☑ Suppress notifications until the last job retry

22. The SMTP server requires authentication. Type the office 365 service account (VEEAM@carysun.com in my case) as Username, enter the account password, and click OK.



☑ Enable e-mail notifications (recommended)

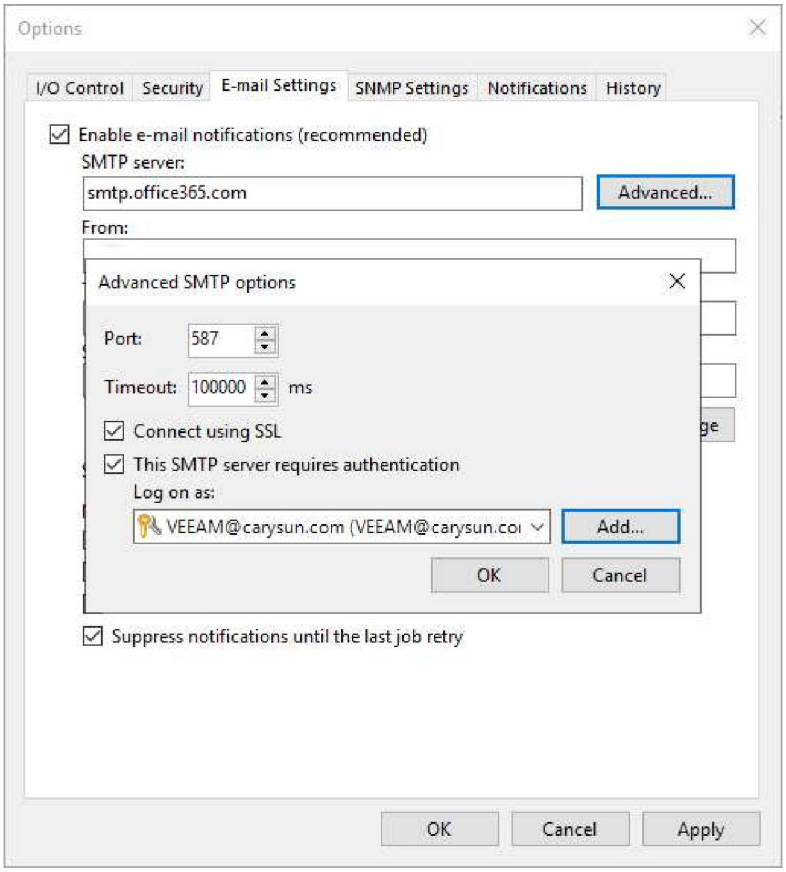
SMTP server: smtp.office365.com

Username: VEEAM@carysun.com

Password: ••••••••••

Description: VEEAM@carysun.com

23. On the Advanced SMTP options page, click OK.



Options

I/O Control | Security | E-mail Settings | SNMP Settings | Notifications | History

☑ Enable e-mail notifications (recommended)

SMTP server: smtp.office365.com

From:

Advanced SMTP options

Port: 587

Timeout: 100000 ms

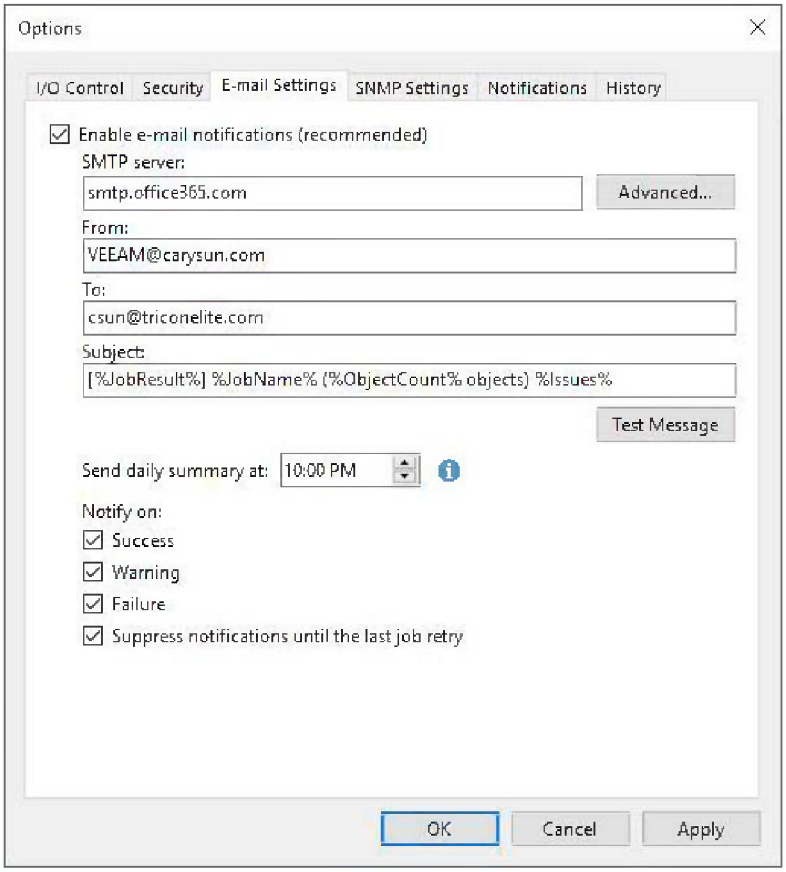
☑ Connect using SSL

☑ This SMTP server requires authentication

Log on as: VEEAM@carysun.com (VEEAM@carysun.coı

☑ Suppress notifications until the last job retry

24. In the From field, enter an email address you want to use as a sender.
25. In the To field, enter an email address of a notification recipient. To specify multiple email addresses, use a semicolon.
26. Click Test Message.



Options

☑ Enable e-mail notifications (recommended)

SMTP server: smtp.office365.com

From: VEEAM@carysun.com

To: csun@triconelite.com

Subject: [%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

Send daily summary at: 10:00 PM

Notify on:

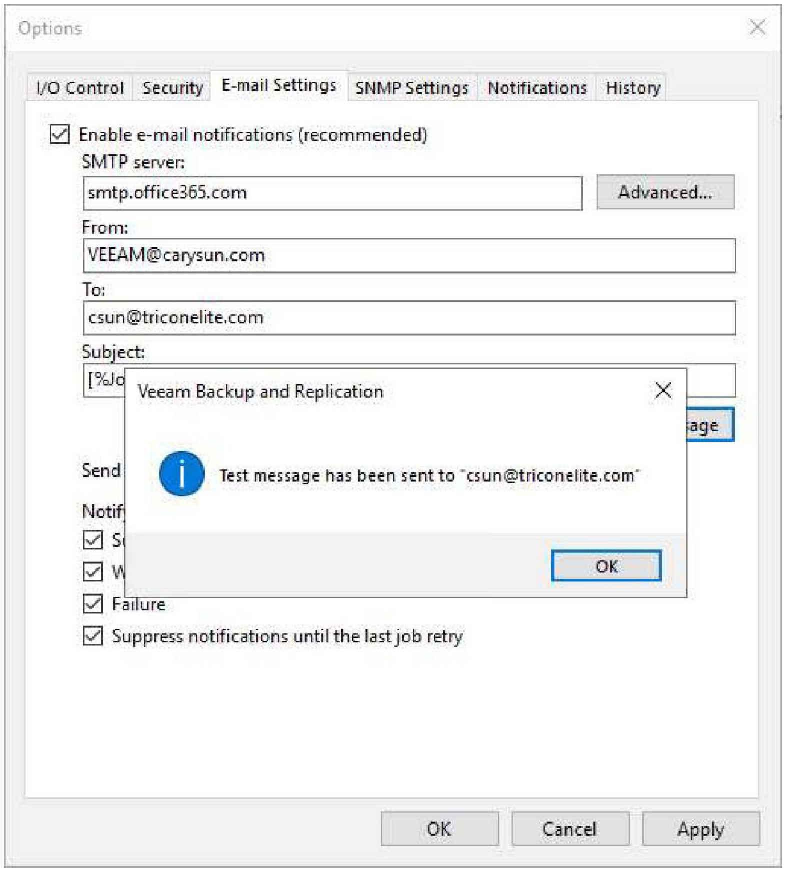
☑ Success

☑ Warning

☑ Failure

☑ Suppress notifications until the last job retry

27. Ensure the test email was successfully sent to recipients, and click OK.



☑ Enable e-mail notifications (recommended)

SMTP server: smtp.office365.com

From: VEEAM@carysun.com

To: csun@triconelite.com

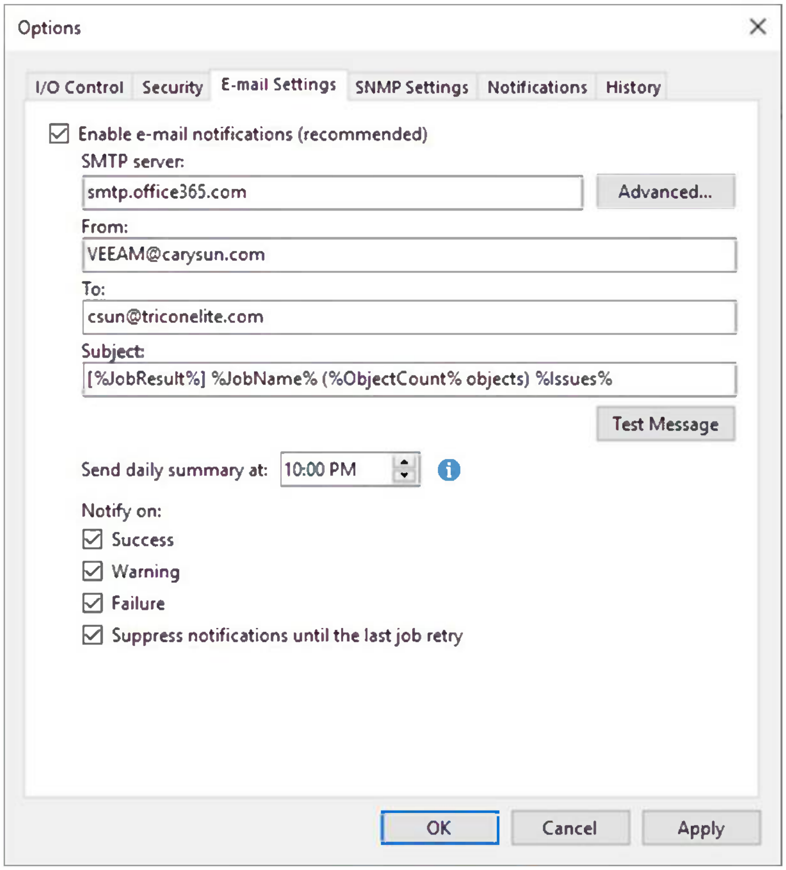
Subject: [%Jo

☑ Failure

☑ Suppress notifications until the last job retry

Test message has been sent to "csun@triconelite.com"

28. On the Email Settings page, System notifications are sent by default whenever a backup job session ends with the following states: Success, Warning, or Failure. Keep the default settings, and click OK.



☑ Enable e-mail notifications (recommended)

SMTP server: smtp.office365.com

From: VEEAM@carysun.com

To: csun@triconelite.com

Subject: [%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

Send daily summary at: 10:00 PM

Notify on:

☑ Success

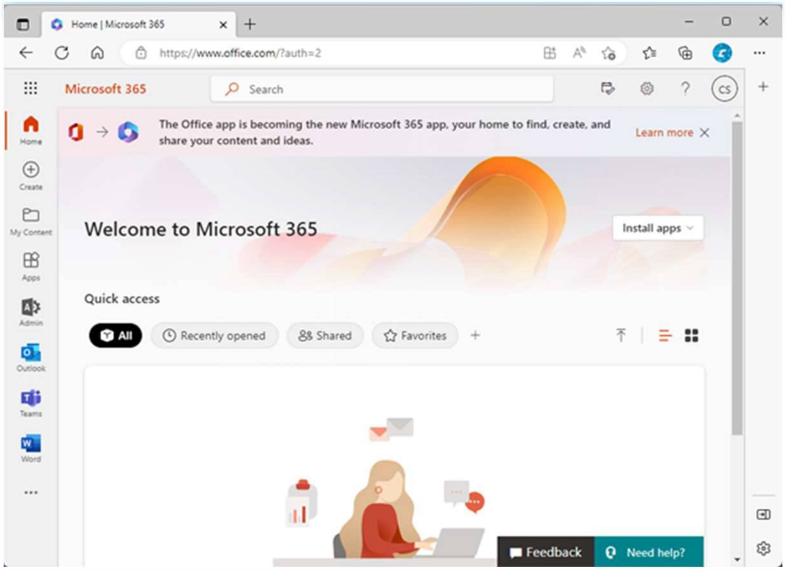
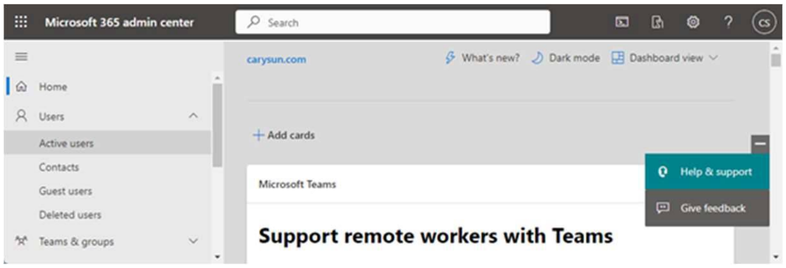
☑ Warning

☑ Failure

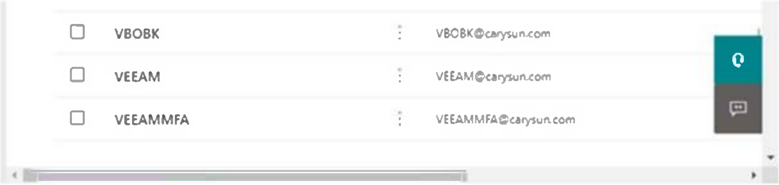
☑ Suppress notifications until the last job retry

Configure Notification with Microsoft Office 365 MFA Account

You can configure Microsoft Office 365 MFA account for notification settings if you want Veeam Backup & Replication to send email notifications about backup job results.

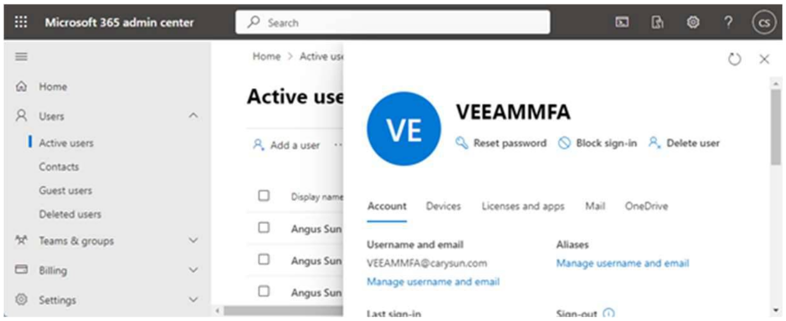
<table>
<tr><th>Instructions</th><th>Screenshot (if applicable)</th></tr>
<tr><td>1. Sign in Office 365 portal with a Global Admin account, and select Admin.</td><td>
The Office app is becoming the new Microsoft 365 app, your home to find, create, and share your content and ideas.
Welcome to Microsoft 365
</td></tr>
<tr><td>2. On the Microsoft 365 admin center, expand Users and select Active users.</td><td>
Support remote workers with Teams
</td></tr>
</table>

3. On the Active users' page, click Veeam service account (VEEAMMFA, in my case).



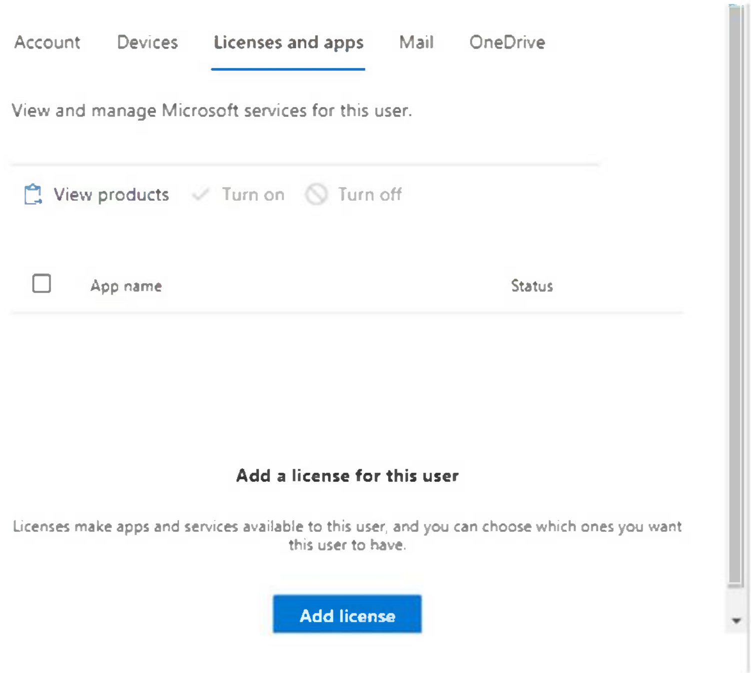
□	VBOBK	VBOBK@carysun.com
□	VEEAM	VEEAM@carysun.com
□	VEEAMMFA	VEEAMMFA@carysun.com

4. On the account page, select License and apps.



Username and email
VEEAMMFA@carysun.com

5. On the License and apps page, click Add license.

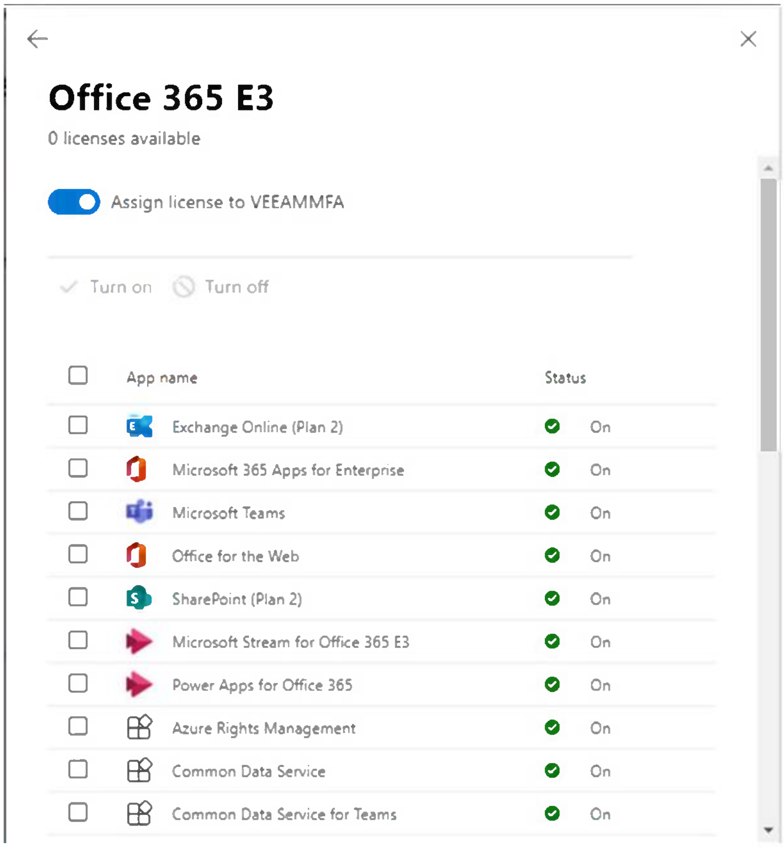


View and manage Microsoft services for this user.

Add a license for this user

Licenses make apps and services available to this user, and you can choose which ones you want this user to have.

6. On the Office 365 license page, enable Assign license to the account, and click Save changes.



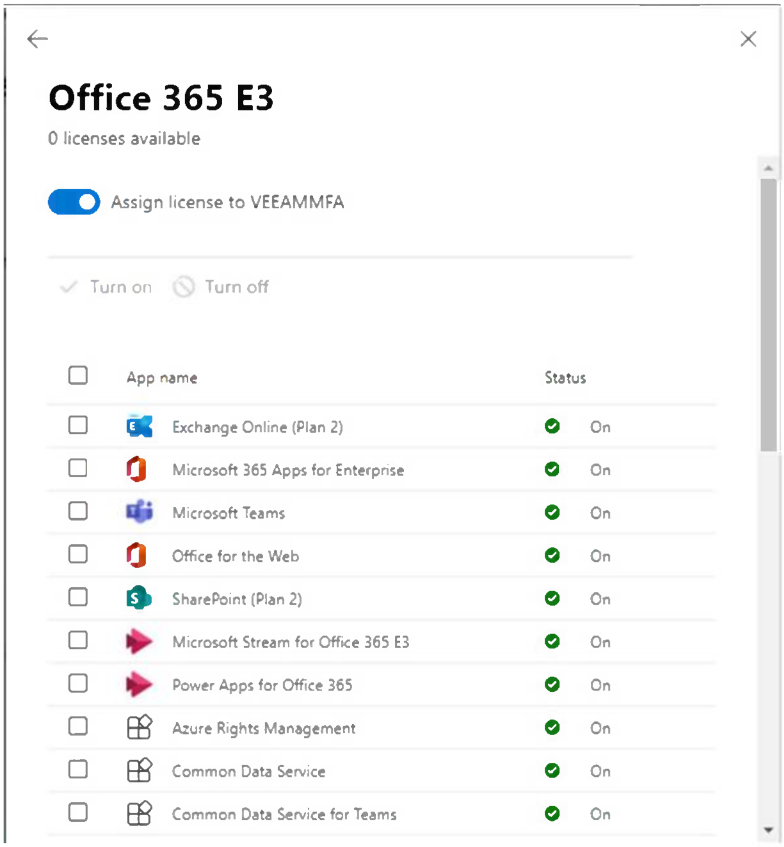
Office 365 E3

0 licenses available

● Assign license to VEEAMMFA

□	App name	Status
□	Exchange Online (Plan 2)	✓ On
□	Microsoft 365 Apps for Enterprise	✓ On
□	Microsoft Teams	✓ On
□	Office for the Web	✓ On
□	SharePoint (Plan 2)	✓ On
□	Microsoft Stream for Office 365 E3	✓ On
□	Power Apps for Office 365	✓ On
□	Azure Rights Management	✓ On
□	Common Data Service	✓ On
□	Common Data Service for Teams	✓ On

7. Click Back <--.



Office 365 E3

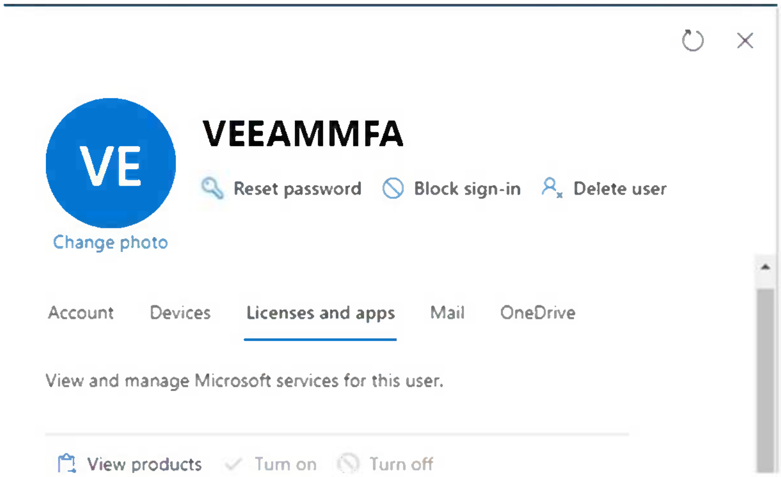
0 licenses available

Assign license to VEEAMMFA

✓ Turn on ⃠ Turn off

☐	App name	Status
☐	Exchange Online (Plan 2)	✓ On
☐	Microsoft 365 Apps for Enterprise	✓ On
☐	Microsoft Teams	✓ On
☐	Office for the Web	✓ On
☐	SharePoint (Plan 2)	✓ On
☐	Microsoft Stream for Office 365 E3	✓ On
☐	Power Apps for Office 365	✓ On
☐	Azure Rights Management	✓ On
☐	Common Data Service	✓ On
☐	Common Data Service for Teams	✓ On

8. On the account page, select Mail. It would be preferable to wait a few minutes before preparing a mailbox for the user.



VEEAMMFA

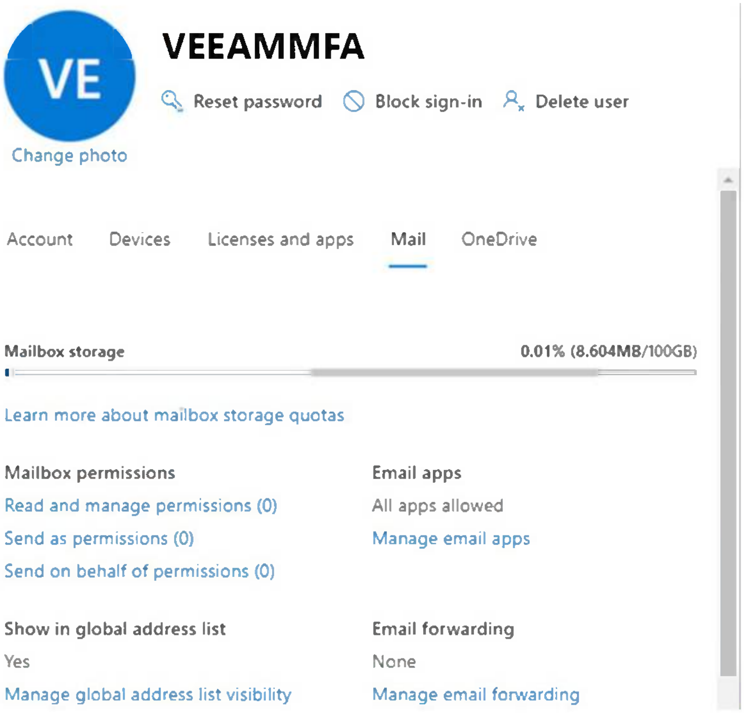
Reset password   Block sign-in   Delete user

Account   Devices   Licenses and apps   Mail   OneDrive

View and manage Microsoft services for this user.

View products   ✓ Turn on   ⃠ Turn off

9. On the Mail page, select Manage email apps.



VE

Change photo

VEEAMMFA

Reset password Block sign-in Delete user

Account Devices Licenses and apps Mail OneDrive

Mailbox storage 0.01% (8.604MB/100GB)

Learn more about mailbox storage quotas

Mailbox permissions

Read and manage permissions (0)

Send as permissions (0)

Send on behalf of permissions (0)

Email apps

All apps allowed

Manage email apps

Show in global address list

Yes

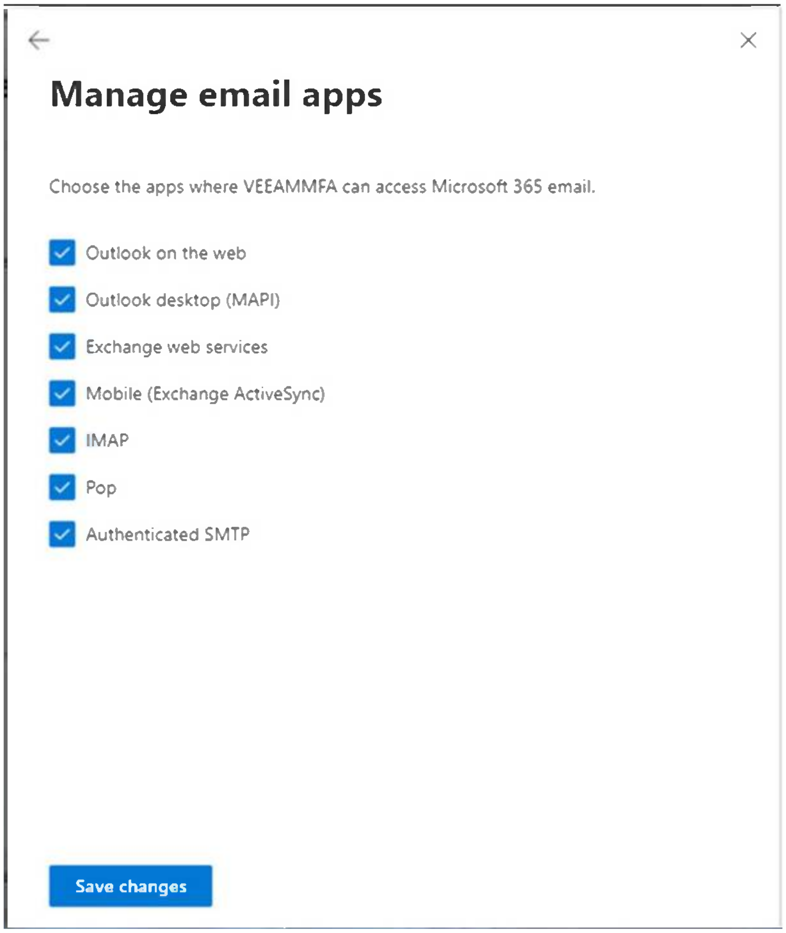
Manage global address list visibility

Email forwarding

None

Manage email forwarding

10. On the Manage email apps, select Authenticated SMTP and click Save changes.



Manage email apps

Choose the apps where VEEAMMFA can access Microsoft 365 email.

☑ Outlook on the web

☑ Outlook desktop (MAPI)

☑ Exchange web services

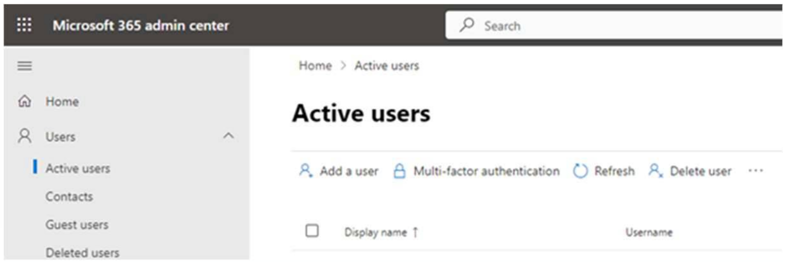
☑ Mobile (Exchange ActiveSync)

☑ IMAP

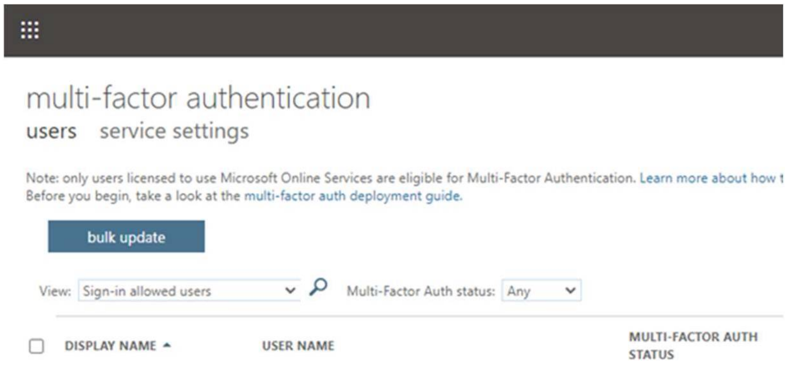
☑ Pop

☑ Authenticated SMTP

11. On the Active Users page, select Multi-factor authentication.



12. Sign in with a Global admin account.
13. On the multi-factor authentication page, select service settings.



multi-factor authentication

users service settings

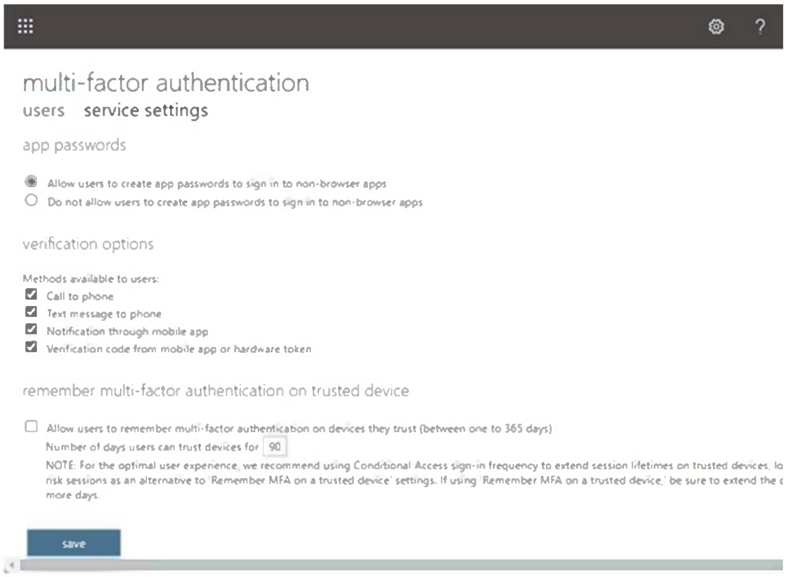
Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how t
Before you begin, take a look at the multi-factor auth deployment guide.

View: Sign-in allowed users

Multi-Factor Auth status: Any

□	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS

14. On the service settings page, select Allow users to create an app password to sign in to non-browser apps, click save and then sign out from the office 365 portal.



multi-factor authentication

users service settings

app passwords

● Allow users to create app passwords to sign in to non-browser apps
○ Do not allow users to create app passwords to sign in to non-browser apps

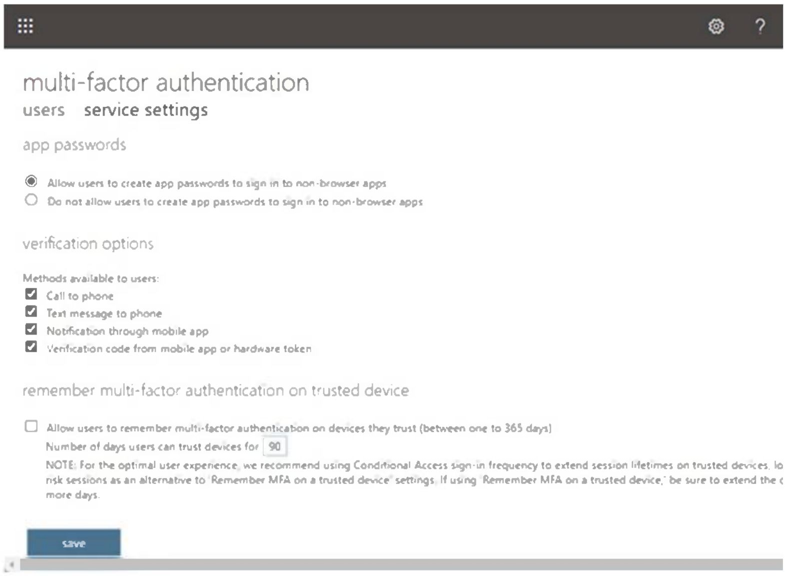
verification options

Methods available to users:
☑ Call to phone
☑ Text message to phone
☑ Notification through mobile app
☑ Verification code from mobile app or hardware token

remember multi-factor authentication on trusted device

□ Allow users to remember multi-factor authentication on devices they trust (between one to 365 days)
Number of days users can trust devices for 90
NOTE: For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend session lifetimes on trusted devices, lo
risk sessions as an alternative to 'Remember MFA on a trusted device' settings. If using 'Remember MFA on a trusted device,' be sure to extend the c
more days.

15. On the multi-factor authentication page, select users.



multi-factor authentication

users service settings

app passwords

● Allow users to create app passwords to sign in to non-browser apps
○ Do not allow users to create app passwords to sign in to non-browser apps

verification options

Methods available to users:

☑ Call to phone
☑ Text message to phone
☑ Notification through mobile app
☑ Verification code from mobile app or hardware token

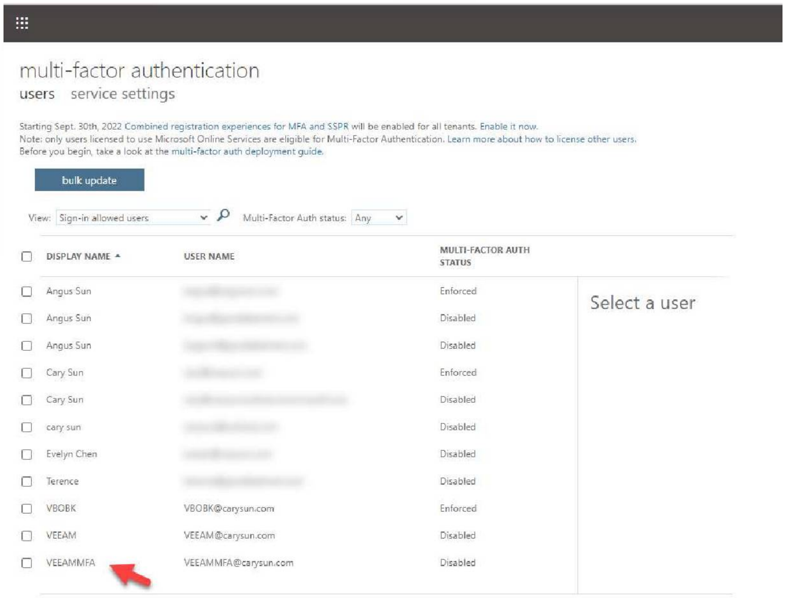
remember multi-factor authentication on trusted device

□ Allow users to remember multi-factor authentication on devices they trust (between one to 365 days)

Number of days users can trust devices for 90

NOTE: For the optimal user experience, we recommend using Conditional Access sign-in frequency to extend session lifetimes on trusted devices, lo risk sessions as an alternative to 'Remember MFA on a trusted device' settings. If using 'Remember MFA on a trusted device,' be sure to extend the c more days.

16. If the Veeam service account is non-MFA, follow the steps below to enable MFA.
17. On the users' page, click Veeam service account.



multi-factor authentication

users service settings

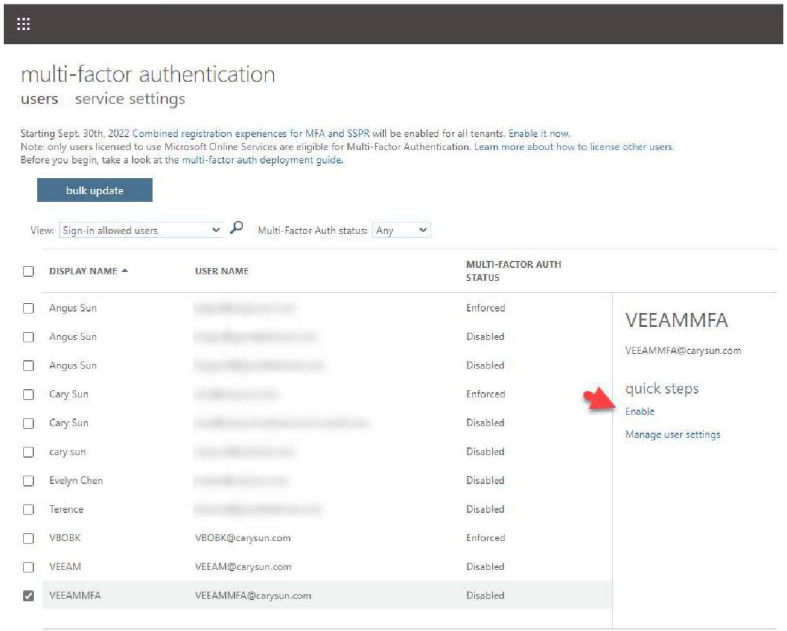
Starting Sept. 30th, 2022 Combined registration experiences for MFA and SSPR will be enabled for all tenants. Enable it now.
Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users.
Before you begin, take a look at the multi-factor auth deployment guide.

View: Sign-in allowed users Multi-Factor Auth status: Any

□	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
□	Angus Sun	[redacted]	Enforced
□	Angus Sun	[redacted]	Disabled
□	Angus Sun	[redacted]	Disabled
□	Cary Sun	[redacted]	Enforced
□	Cary Sun	[redacted]	Disabled
□	cary sun	[redacted]	Disabled
□	Evelyn Chen	[redacted]	Disabled
□	Terence	[redacted]	Disabled
□	VBOBK	VBOBK@carysun.com	Enforced
□	VEEAM	VEEAM@carysun.com	Disabled
□	VEEAMMFA	VEEAMMFA@carysun.com	Disabled

Select a user

18. On the quick steps page, select Enable.



multi-factor authentication

users service settings

Starting Sept. 30th, 2022 Combined registration experiences for MFA and SSPR will be enabled for all tenants. Enable it now.
Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users.
Before you begin, take a look at the multi-factor auth deployment guide.

View: Sign-in allowed users Multi-Factor Auth status: Any

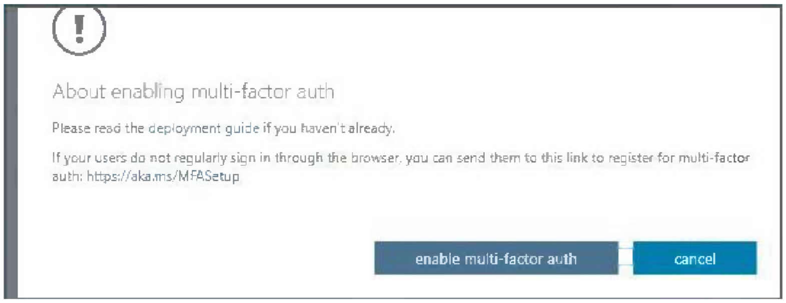
☐	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
☐	Angus Sun	[redacted]	Enforced
☐	Angus Sun	[redacted]	Disabled
☐	Angus Sun	[redacted]	Disabled
☐	Cary Sun	[redacted]	Enforced
☐	Cary Sun	[redacted]	Disabled
☐	cary sun	[redacted]	Disabled
☐	Evelyn Chen	[redacted]	Disabled
☐	Terence	[redacted]	Disabled
☐	VBOBK	VBOBK@carysun.com	Enforced
☐	VEEAM	VEEAM@carysun.com	Disabled
☑	VEEAMMFA	VEEAMMFA@carysun.com	Disabled

VEEAMMFA

VEEAMMFA@carysun.com

quick steps

19. Click enable multi-factor auth on the About helping multi-factor auth page.

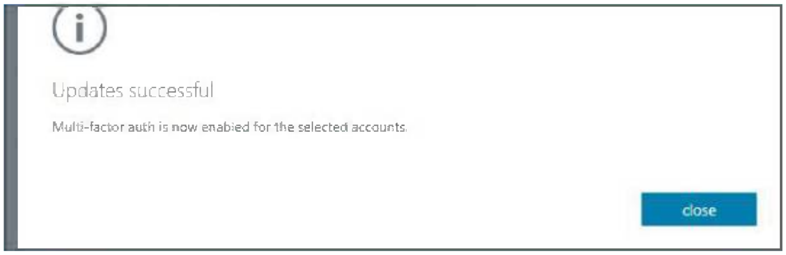


About enabling multi-factor auth

Please read the deployment guide if you haven't already.

If your users do not regularly sign in through the browser, you can send them to this link to register for multi-factor auth: https://aka.ms/MFASetup

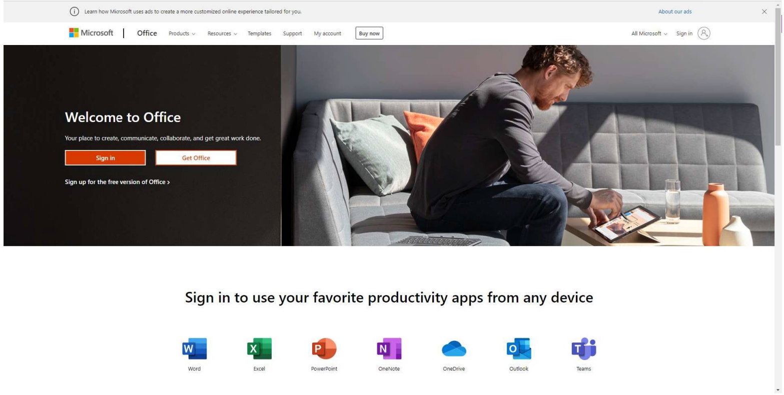
20. On the Updates, successful page, click Close.



Updates successful

Multi-factor auth is now enabled for the selected accounts.

21. Sign in Office 365 portal with a Veeam service account



Learn how Microsoft uses ads to create a more customized online experience tailored for you.

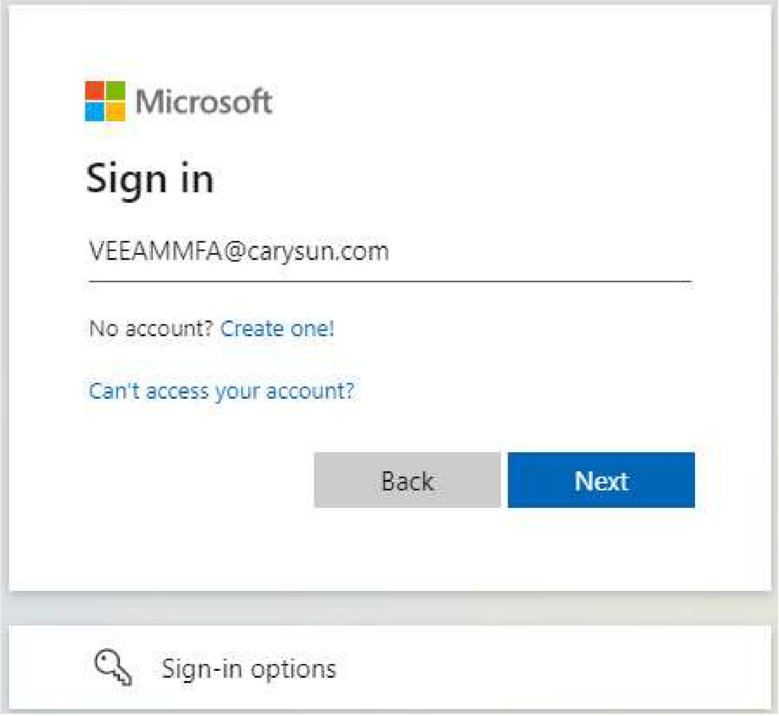
Welcome to Office

Your place to create, communicate, collaborate, and get great work done.

Sign up for the free version of Office ›

Sign in to use your favorite productivity apps from any device

22. On the Sign in page, enter the Veeam services account email address.



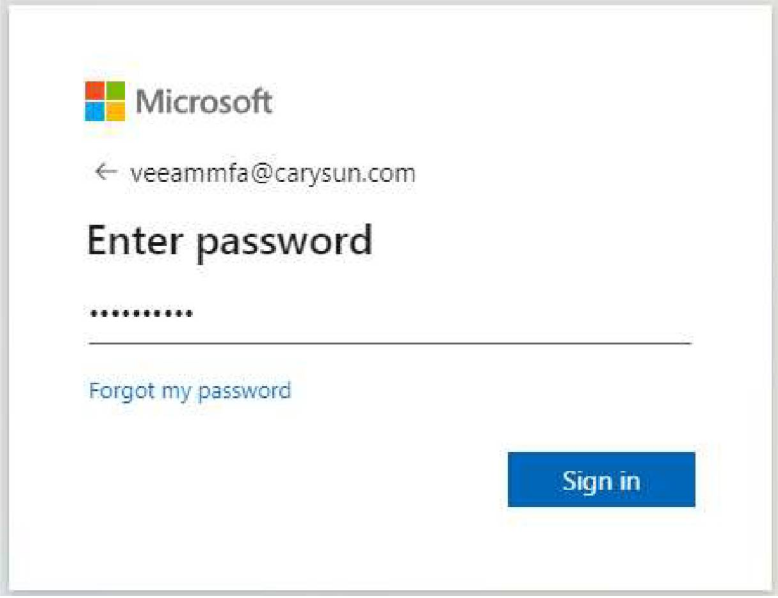
Sign in

VEEAMMFA@carysun.com

No account? Create one!

Can't access your account?

23. Enter the password.



Microsoft

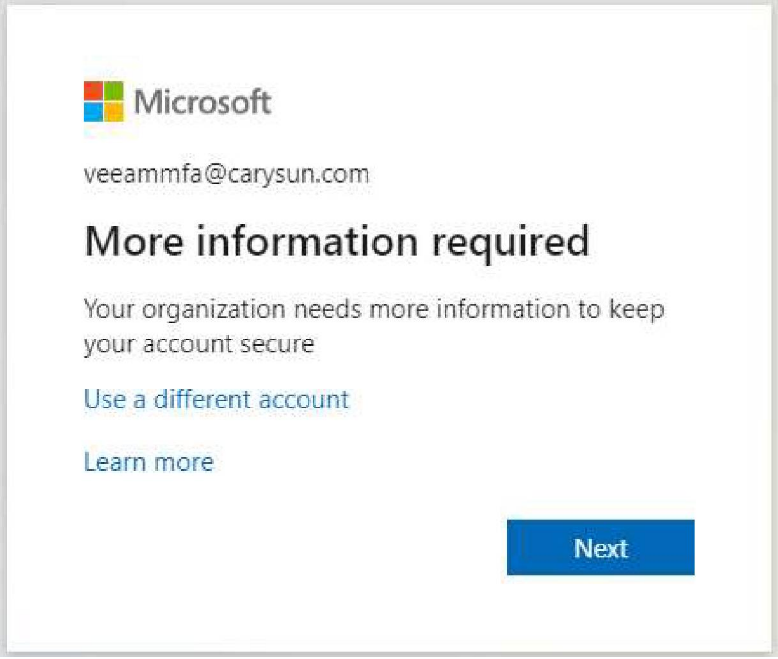
← veeammfa@carysun.com

Enter password

••••••••••

Forgot my password

24. On the More information required page, click Next.



Microsoft

veeammfa@carysun.com

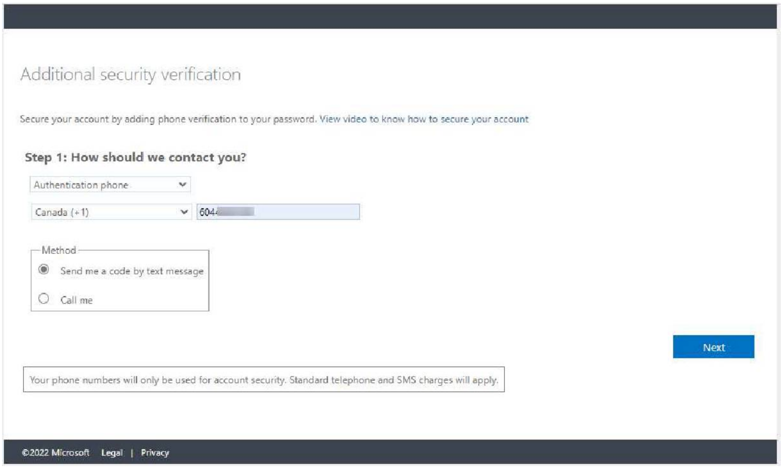
More information required

Your organization needs more information to keep your account secure

Use a different account

Learn more

25. Select Fill in the information on the Step 1 page and click Next.



Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 1: How should we contact you?

Authentication phone

Canada (+1) 604[redacted]

Method

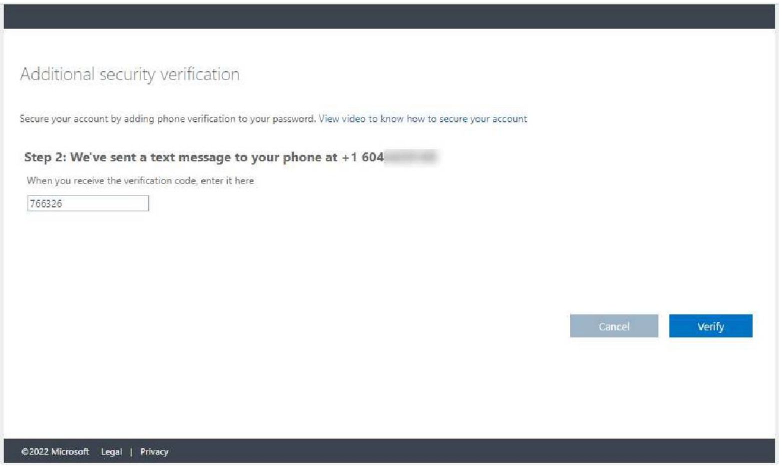
● Send me a code by text message

○ Call me

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

©2022 Microsoft Legal | Privacy

26. On the Step 2 page, enter the verification code and click Verify.



Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

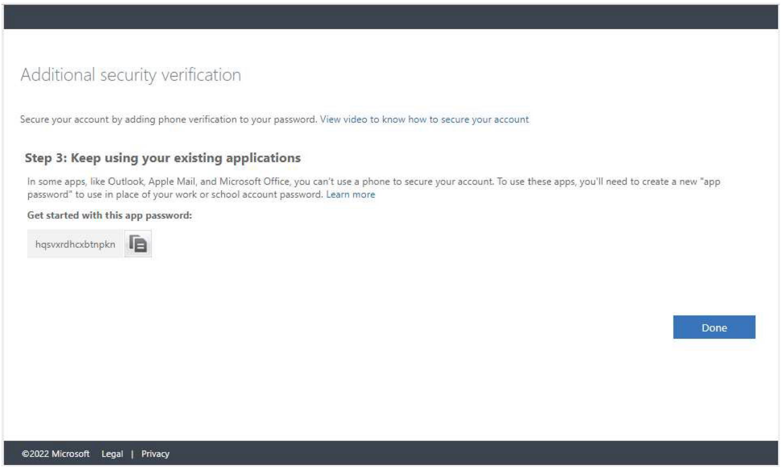
Step 2: We've sent a text message to your phone at +1 604[redacted]

When you receive the verification code, enter it here

766326

©2022 Microsoft Legal | Privacy

27. In Step 3, copy and save the app password, and click Done.



Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

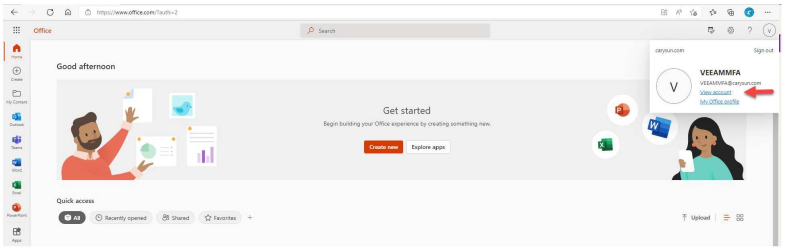
Step 3: Keep using your existing applications

In some apps, like Outlook, Apple Mail, and Microsoft Office, you can't use a phone to secure your account. To use these apps, you'll need to create a new "app password" to use in place of your work or school account password. Learn more

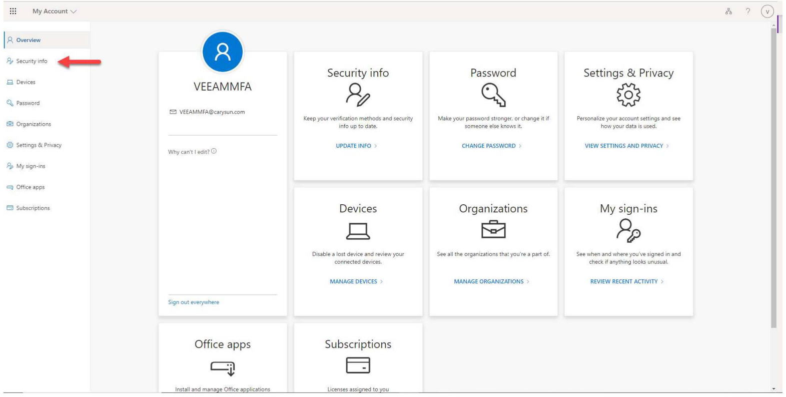
Get started with this app password:

hqsvxrdhcxbtnpkn

28. If the Veeam service account is an existing MFA account, follow the below steps to add App password authentication.
29. Sign in to the Office 365 portal with the Veeam service account and select View account.

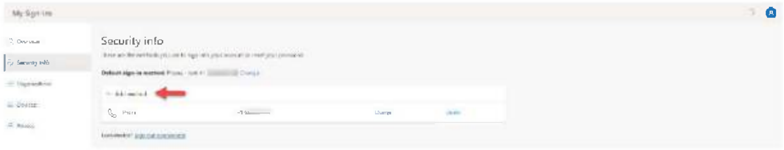


30. On the My account page, select Security info.

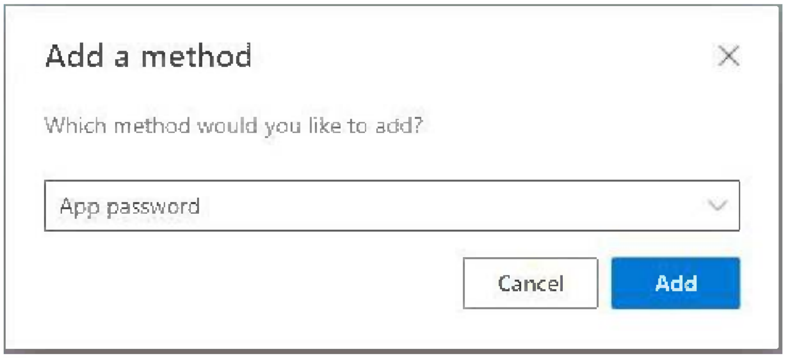


My Account
Overview
Security info
Devices
Password
Organizations
Settings & Privacy
My sign-ins
Office apps
Subscriptions
VEEAMMFA
VEEAMMFA@carysun.com
Why can't I edit?
Sign out everywhere
Security info
Keep your verification methods and security info up to date.
UPDATE INFO
Password
Make your password stronger, or change it if someone else knows it.
CHANGE PASSWORD
Settings & Privacy
Personalize your account settings and see how your data is used.
VIEW SETTINGS AND PRIVACY
Devices
Disable a lost device and review your connected devices.
MANAGE DEVICES
Organizations
See all the organizations that you're a part of.
MANAGE ORGANIZATIONS
My sign-ins
See when and where you've signed in and check if anything looks unusual.
REVIEW RECENT ACTIVITY
Office apps
Install and manage Office applications
Subscriptions
Licenses assigned to you

31. On the Security info page, select the +Add method.



32. On the Add Method, select App password and click Add.

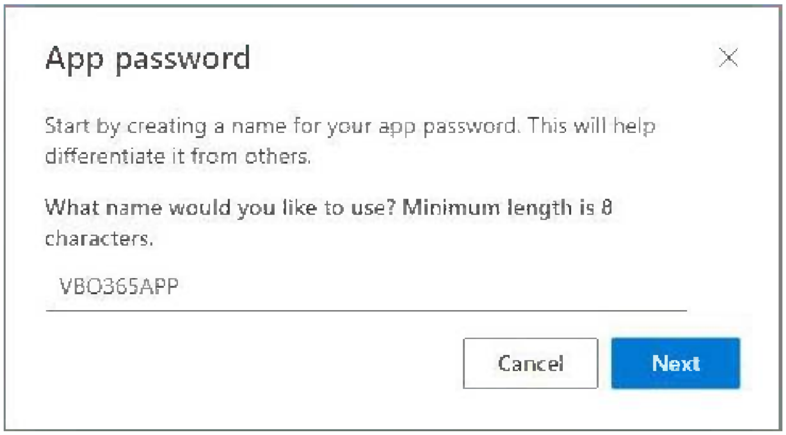


Add a method

Which method would you like to add?

App password

33. Type VBO365APP as the name of the App password, and click Next.



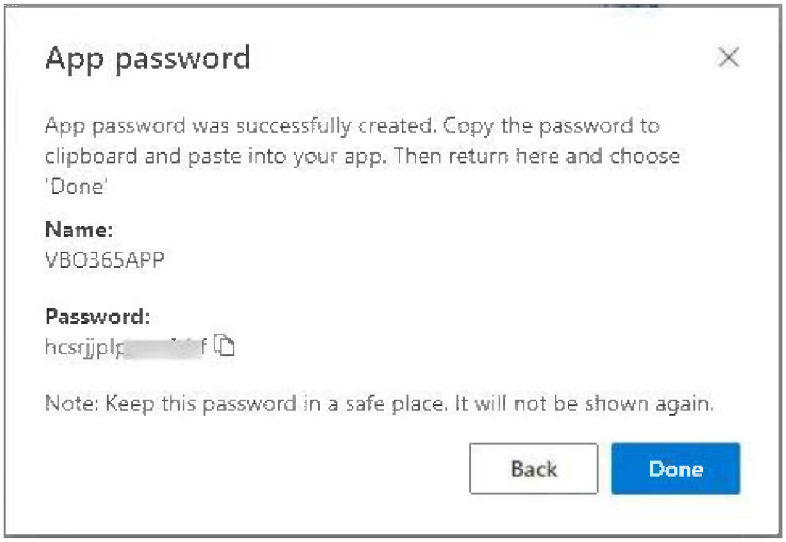
App password

Start by creating a name for your app password. This will help differentiate it from others.

What name would you like to use? Minimum length is 8 characters.

VBO365APP

34. Copy and keep the password in a safe place. Then, it will not be shown again.
35. Click Done.



App password

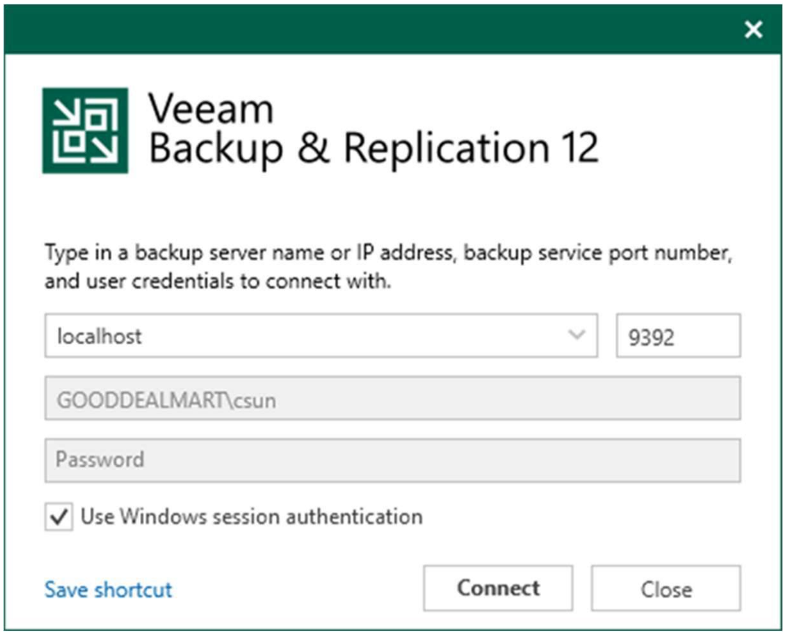
App password was successfully created. Copy the password to clipboard and paste into your app. Then return here and choose 'Done'

Name:
VBO365APP

Password:
hcsrjjplp[redacted]f

Note: Keep this password in a safe place. It will not be shown again.

36. Log in to the Veeam Backup and replication manager server.
37. Open the Veeam Backup & Replication Console and click Connect.



Veeam
Backup & Replication 12

Type in a backup server name or IP address, backup service port number, and user credentials to connect with.

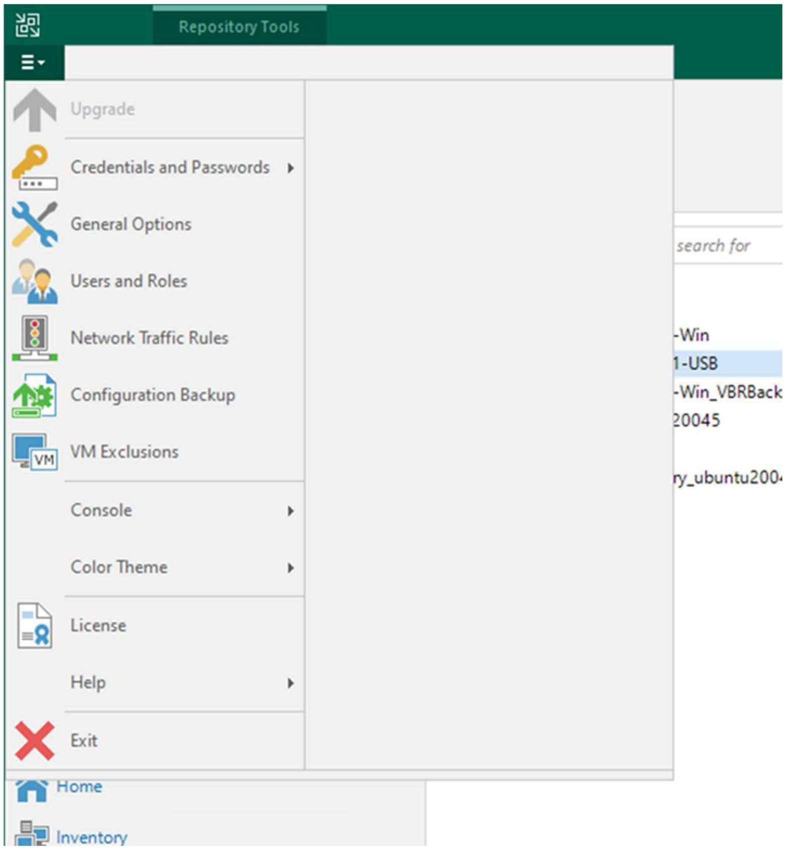
localhost | 9392

GOODDEALMART\csun

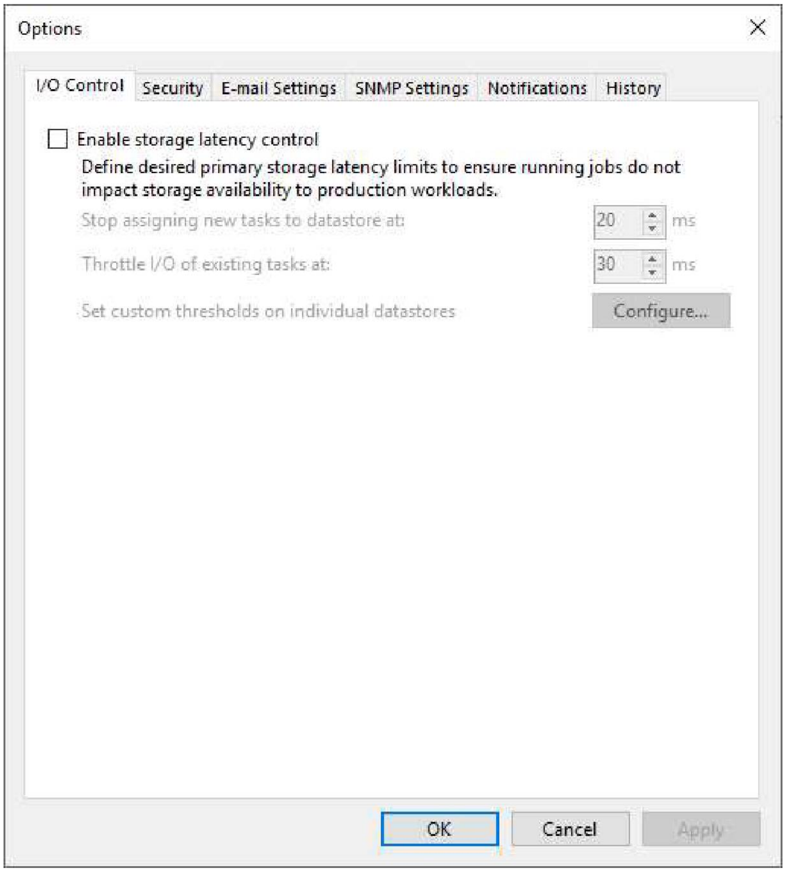
Password

☑ Use Windows session authentication

38. Select General Options from the main menu.



39. On the Options page, select Email Settings.



□ Enable storage latency control

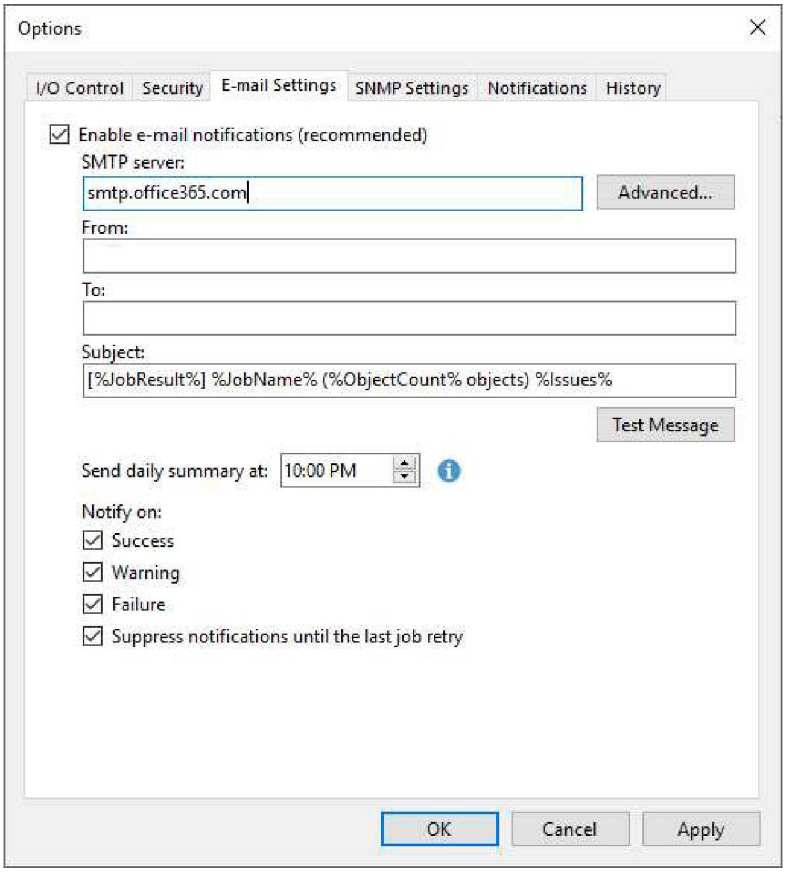
Define desired primary storage latency limits to ensure running jobs do not impact storage availability to production workloads.

Stop assigning new tasks to datastore at: 20 ms

Throttle I/O of existing tasks at: 30 ms

Set custom thresholds on individual datastores

40. Select Enable e-mail notification (recommend) on the Email Settings page.
41. In the SMTP server field, enter smtp.sendgrid.net and click Advanced.



☑ Enable e-mail notifications (recommended)

SMTP server: smtp.office365.com

From:

To:

Subject: [%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

Send daily summary at: 10:00 PM

Notify on:

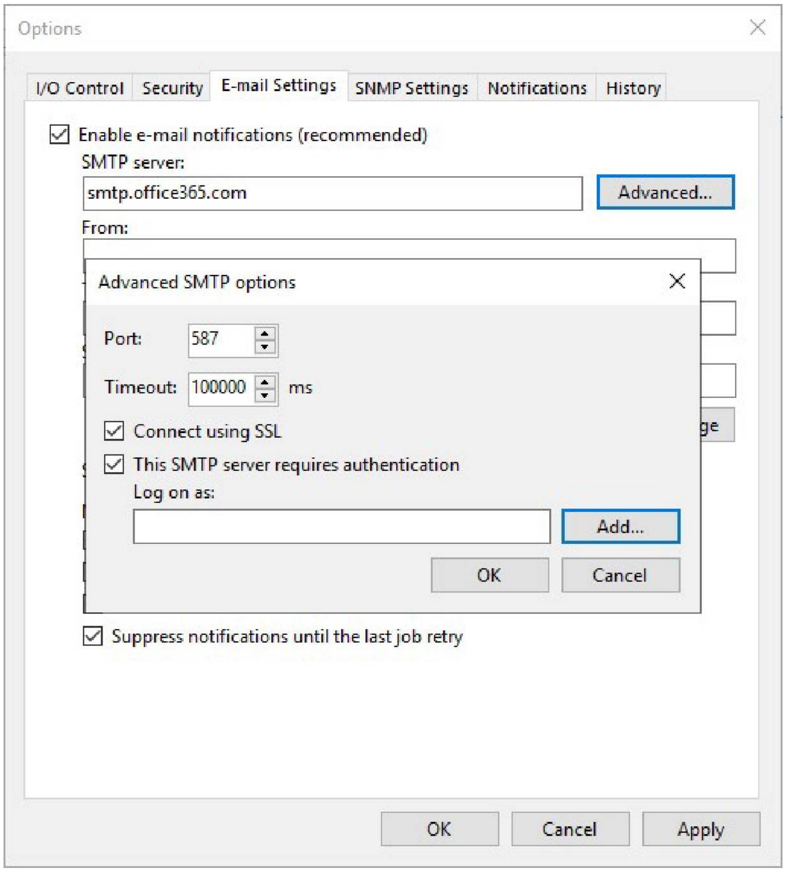
☑ Success

☑ Warning

☑ Failure

☑ Suppress notifications until the last job retry

42. On the Advanced SMTP options page, enter 587 in the Port field.
43. Use 100000 milliseconds as the Timeout.
44. Select Connect using SSL.
45. Select This SMTP server requires authentication.
46. Click Add to add a credential as Log on as account.



☑ Enable e-mail notifications (recommended)

SMTP server: smtp.office365.com

Advanced SMTP options

Port: 587

Timeout: 100000 ms

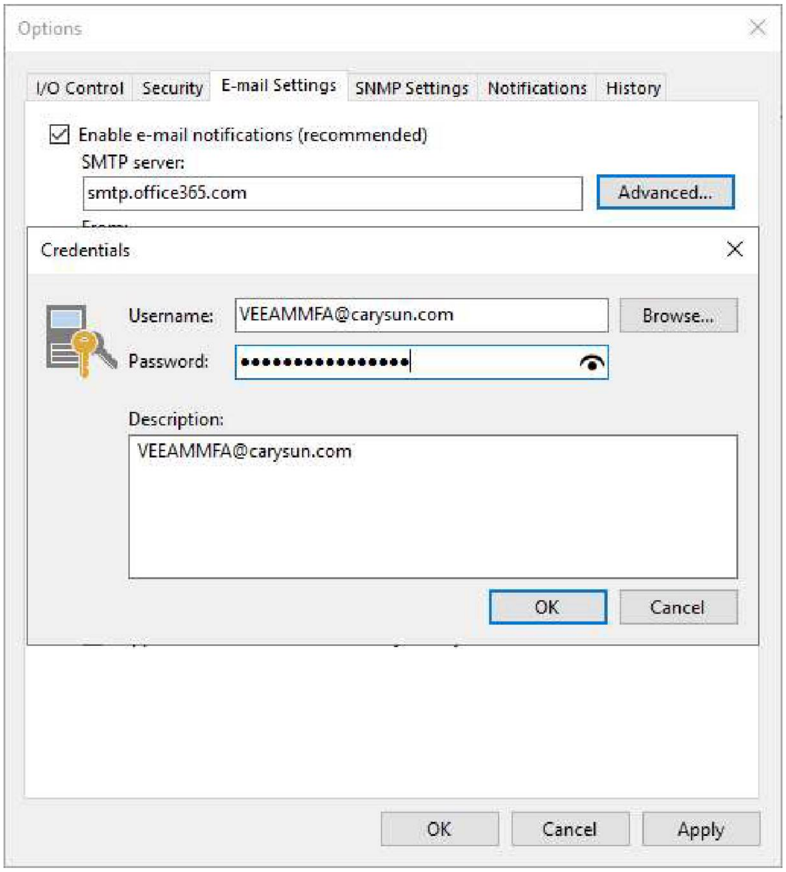
☑ Connect using SSL

☑ This SMTP server requires authentication

Log on as:

☑ Suppress notifications until the last job retry

47. The SMTP server requires authentication. Type the office 365 service account (VEEAMMFA@carysun.com in my case) as Username, enter the App password as the password, and click OK.



☑ Enable e-mail notifications (recommended)

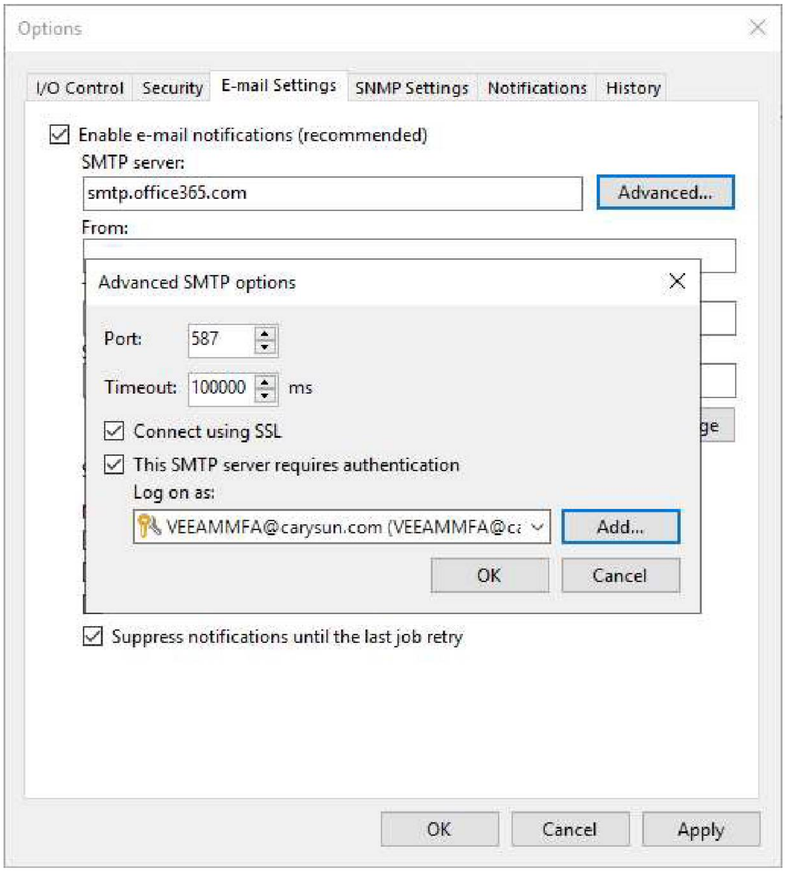
SMTP server: smtp.office365.com

Username: VEEAMMFA@carysun.com

Password: ••••••••••••••••

Description: VEEAMMFA@carysun.com

48. On the Advanced SMTP options page, click OK.



☑ Enable e-mail notifications (recommended)

SMTP server: smtp.office365.com

Advanced SMTP options

Port: 587

Timeout: 100000 ms

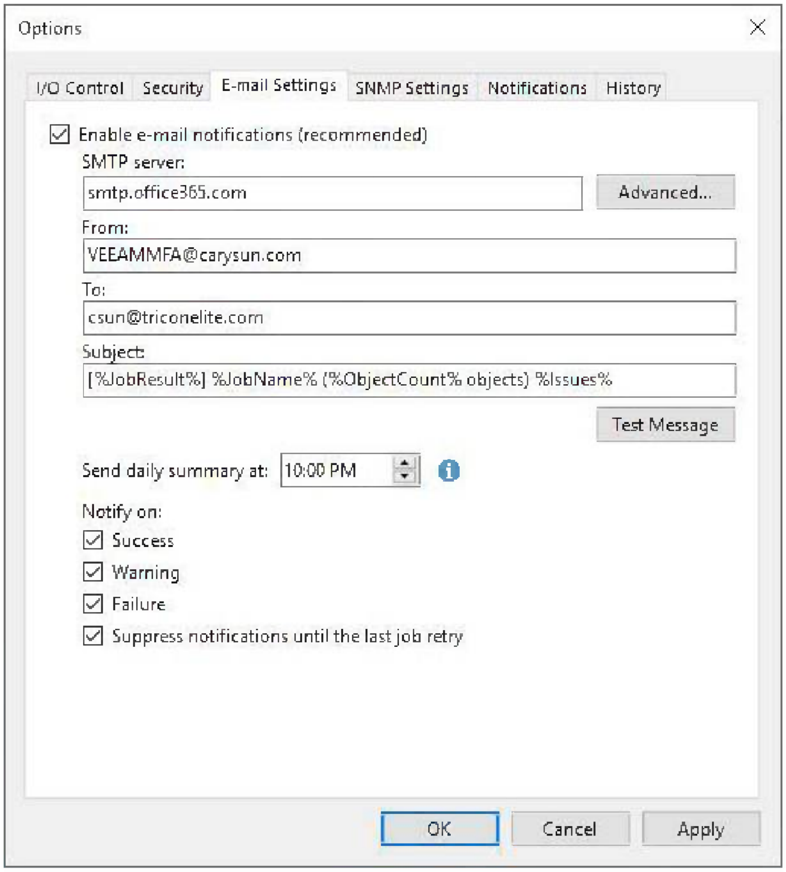
☑ Connect using SSL

☑ This SMTP server requires authentication

Log on as: VEEAMMFA@carysun.com (VEEAMMFA@ca

☑ Suppress notifications until the last job retry

49. In the From field, enter the Veeam service account's email address as a sender.
50. In the To field, enter an email address of a notification recipient. To specify multiple email addresses, use a semicolon.
51. Click Test Message.



☑ Enable e-mail notifications (recommended)

SMTP server: smtp.office365.com

From: VEEAMMFA@carysun.com

To: csun@triconelite.com

Subject: [%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

Send daily summary at: 10:00 PM

Notify on:

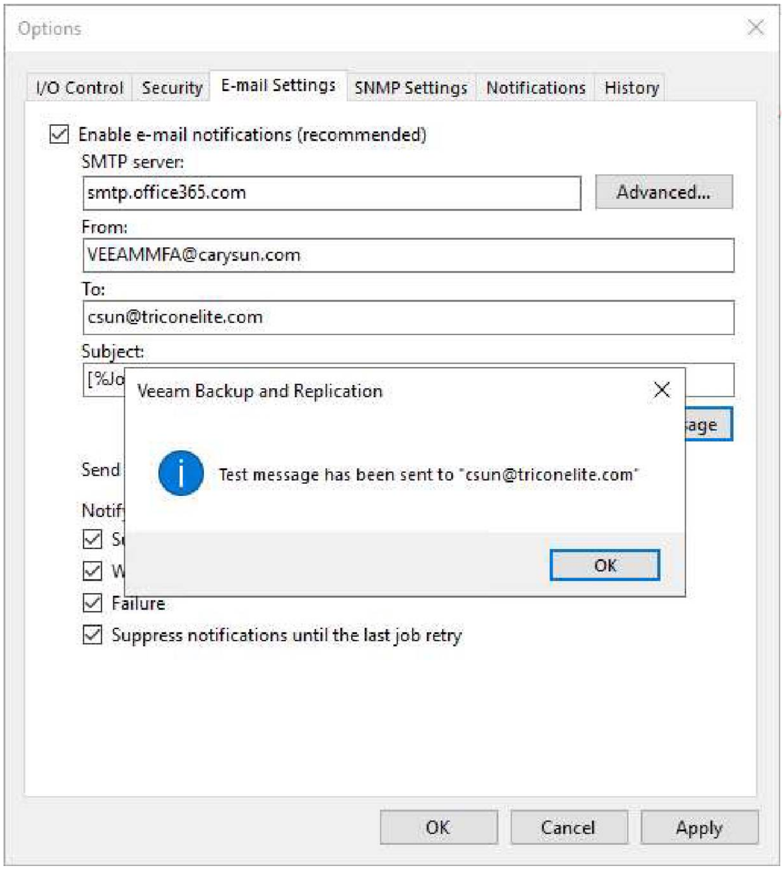
☑ Success

☑ Warning

☑ Failure

☑ Suppress notifications until the last job retry

52. Ensure the test email was successfully sent to recipients, and click OK.



☑ Enable e-mail notifications (recommended)

SMTP server: smtp.office365.com

From: VEEAMMFA@carysun.com

To: csun@triconelite.com

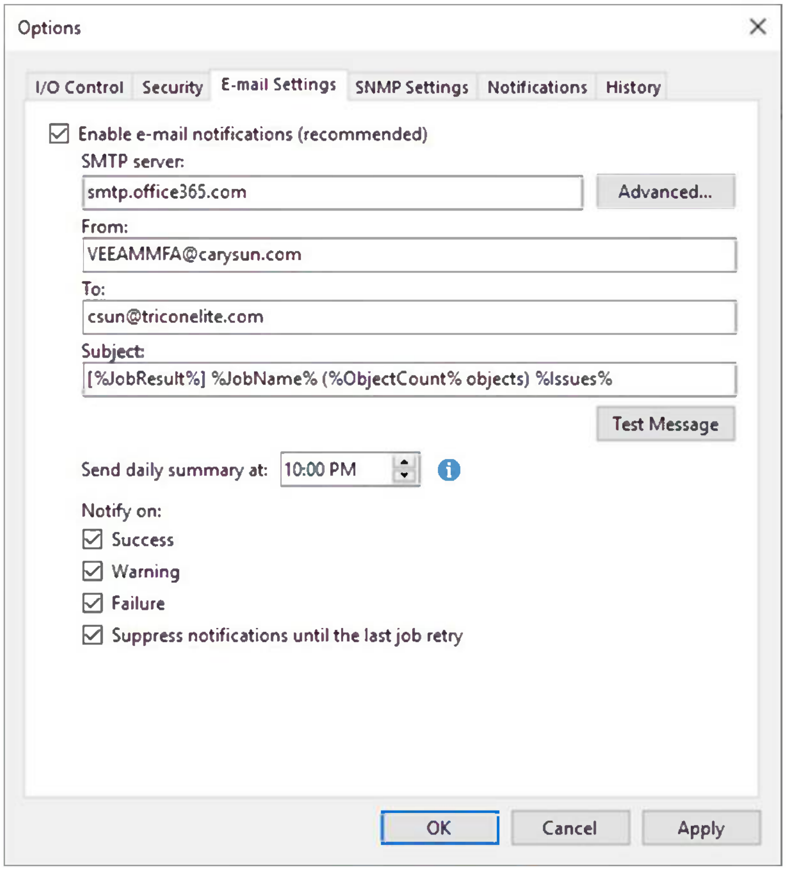
Subject: [%Jo

☑ Failure

☑ Suppress notifications until the last job retry

Test message has been sent to "csun@triconelite.com"

53. On the Notifications page, system notifications are sent by default whenever a backup job session ends with the following states: Success, Warning, or Failure. Keep the default settings, and click OK.



Options

I/O Control | Security | E-mail Settings | SNMP Settings | Notifications | History

☑ Enable e-mail notifications (recommended)

SMTP server: smtp.office365.com

From: VEEAMMFA@carysun.com

To: csun@triconelite.com

Subject: [%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

Send daily summary at: 10:00 PM

Notify on:

☑ Success

☑ Warning

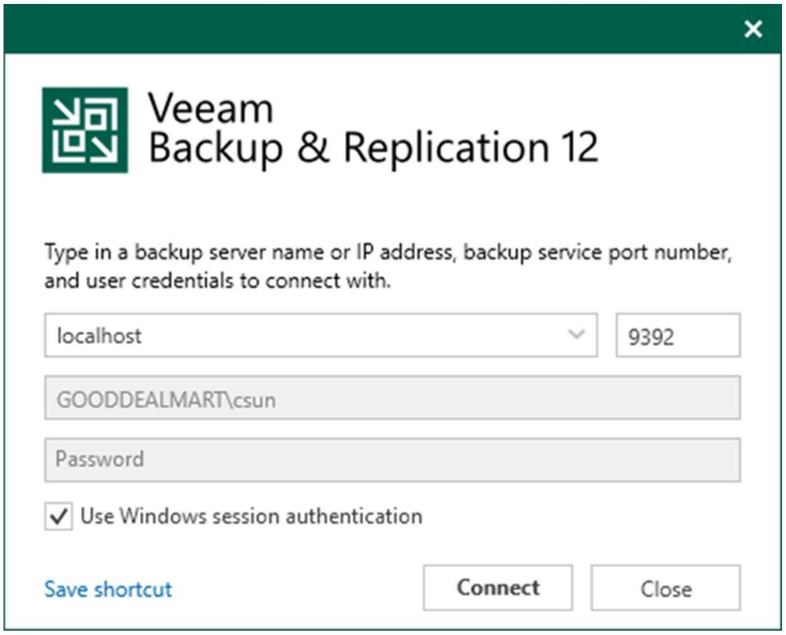
☑ Failure

☑ Suppress notifications until the last job retry

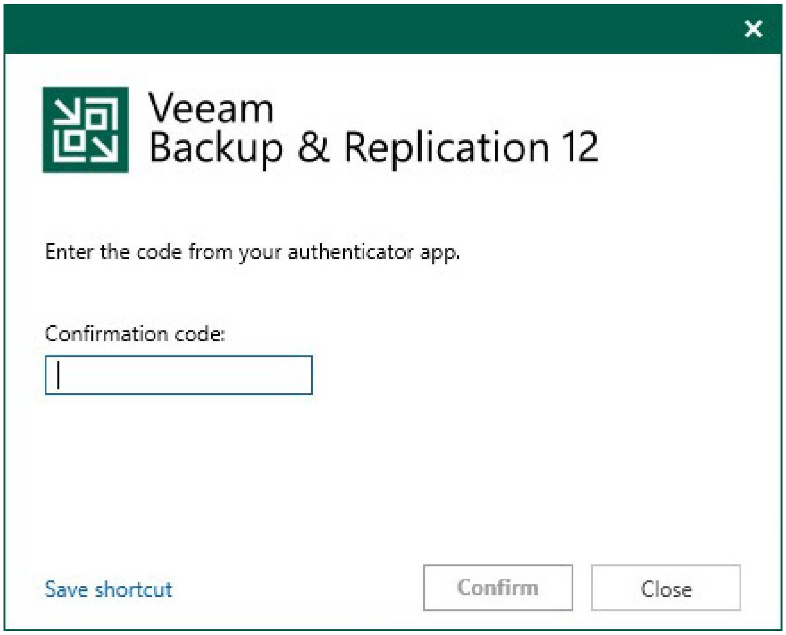
Enable Configuration Backup

The configuration database of Veeam Backup & Replication can be backed up and restored. If the backup server fails, you can quickly reinstall it and restore its configuration from a backup configuration.

You can also use configuration backups to restore the configuration from one backup server to another in the backup infrastructure. For example, Veeam Backup & Replication exports configuration data from the database and saves it to the backup repository during configuration backup.

Instructions	Screenshot (if applicable)
1. Log in to the Veeam Backup and replication manager server. 2. Open the Veeam Backup & Replication Console and click Connect.	 Veeam Backup & Replication 12 Type in a backup server name or IP address, backup service port number, and user credentials to connect with. localhost 9392 GOODDEALMART\csun Password ☑ Use Windows session authentication

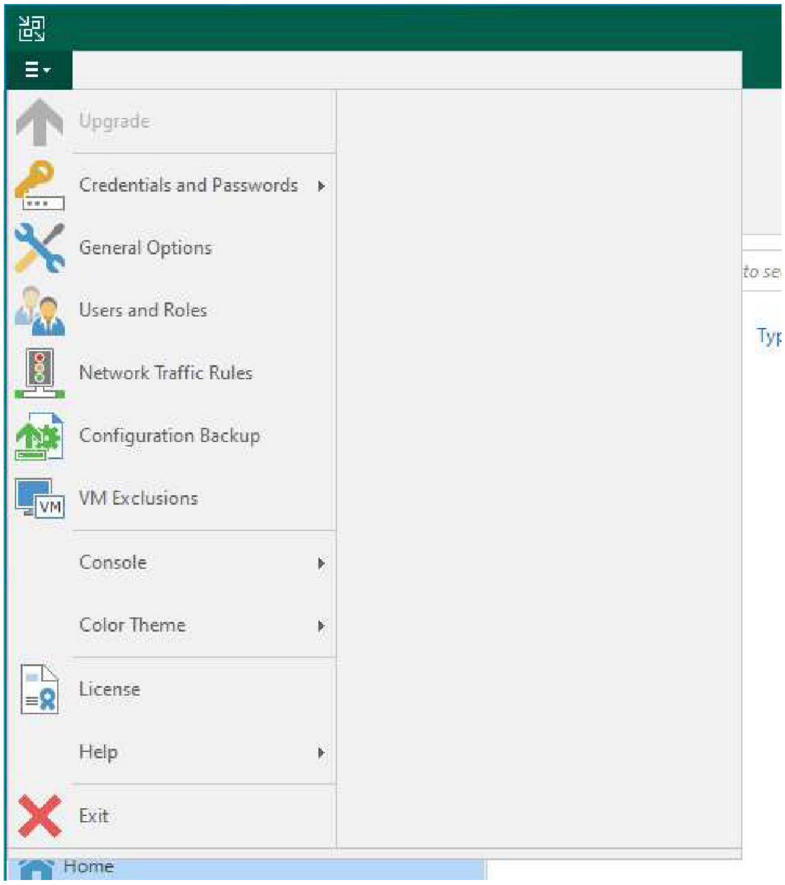
3. Enter the MFA Confirmation code and click Confirm.



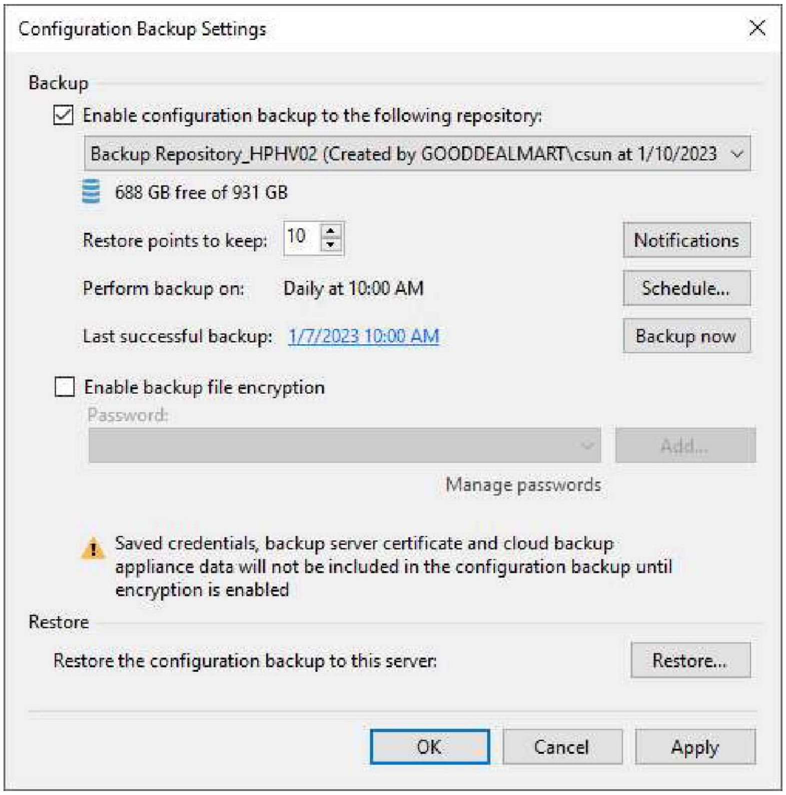
Enter the code from your authenticator app.

Confirmation code:

4. Select Configuration Backup from the Man menu.



5. Select Enable configuration backup to the following repository checkbox on the Configuration Backup Settings page.
6. Select the backup repository from the drop-down list.
7. Enter the restore points number in the Restore points to keep field.
8. Click Notifications.



Configuration Backup Settings

Backup

☑ Enable configuration backup to the following repository:

Backup Repository_HPHV02 (Created by GOODDEALMART\csun at 1/10/2023

688 GB free of 931 GB

Restore points to keep: 10

Perform backup on: Daily at 10:00 AM

Last successful backup: 1/7/2023 10:00 AM

☐ Enable backup file encryption

Password:

Saved credentials, backup server certificate and cloud backup appliance data will not be included in the configuration backup until encryption is enabled

Restore

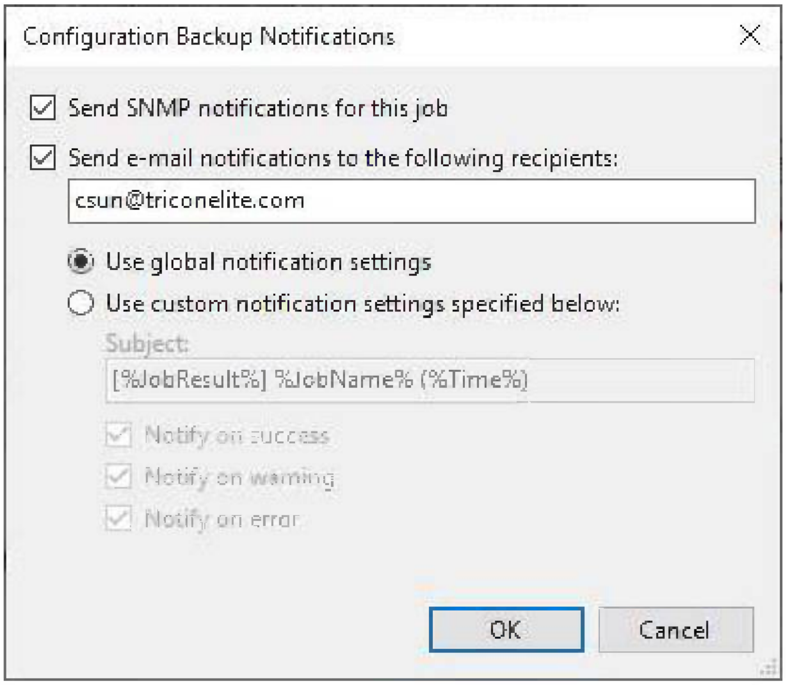
Restore the configuration backup to this server:

9. Select Send SNMP notification on this job checkbox's Configuration Backup Notification page. If necessary.

10. Select Send e-mail notifications to the following recipients check box and enter a recipient's email address. You can enter multiple addresses, each email address separated by a semicolon.

11. Select the Use global notification settings checkbox.

12. Click OK.



Configuration Backup Notifications

☑ Send SNMP notifications for this job

☑ Send e-mail notifications to the following recipients:

csun@triconelite.com

● Use global notification settings

○ Use custom notification settings specified below:

Subject:

[%JobResult%] %JobName% (%Time%)

☑ Notify on success

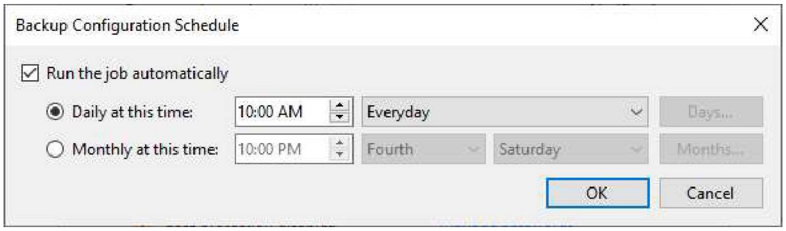
☑ Notify on warning

☑ Notify on error

13. Click Schedule on the Configuration Backup Settings page.

14. On the Backup Configuration Schedule page, select Run the job automatically checkbox.

15. Select Daily at this time, enter the backup time in the time field and select every day from the drop-down list.



Backup Configuration Schedule

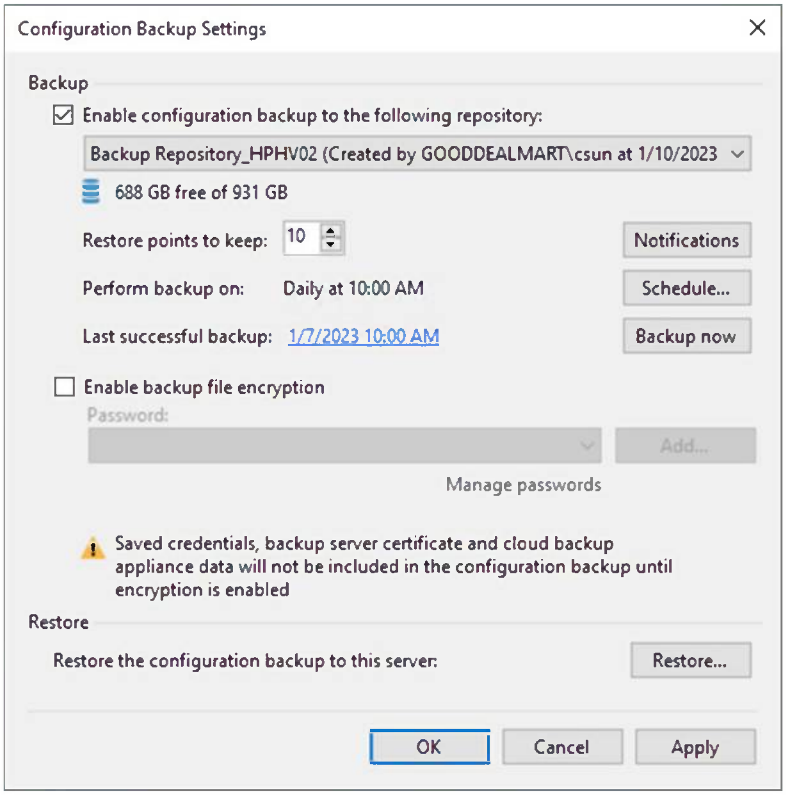
☑ Run the job automatically

● Daily at this time: 10:00 AM Everyday

○ Monthly at this time: 10:00 PM Fourth Saturday

16. Click OK.

17. On the Configuration Backup Settings page, click Backup now if you want to back up manually.



Configuration Backup Settings

Backup

☑ Enable configuration backup to the following repository:

Backup Repository_HPHV02 (Created by GOODDEALMART\csun at 1/10/2023

688 GB free of 931 GB

Restore points to keep: 10

Perform backup on: Daily at 10:00 AM

Last successful backup: 1/7/2023 10:00 AM

☐ Enable backup file encryption

Password:

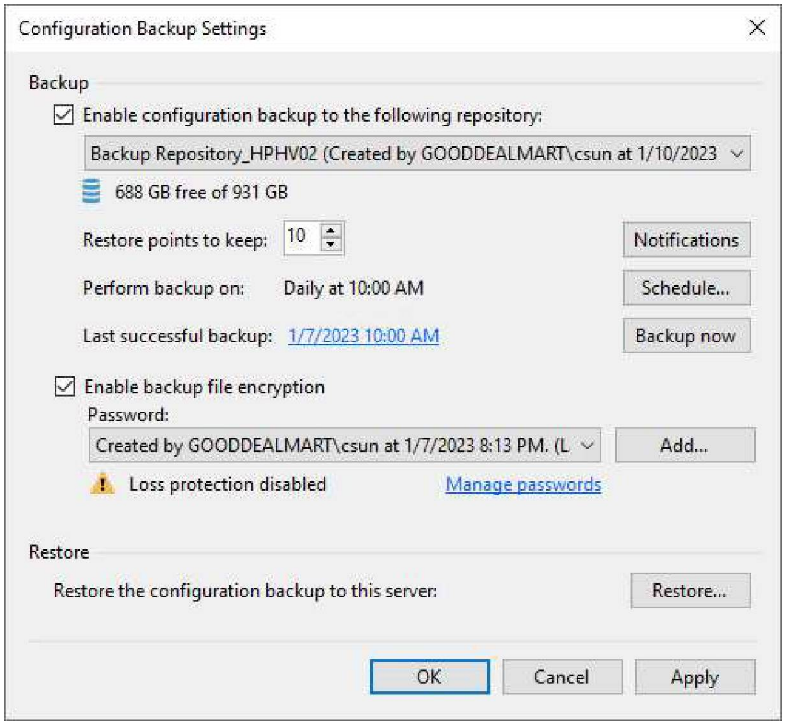
Manage passwords

⚠ Saved credentials, backup server certificate and cloud backup appliance data will not be included in the configuration backup until encryption is enabled

Restore

Restore the configuration backup to this server:

18. Select Enable backup file encryption on the Configuration Backup Settings page.
19. Select a password from the Password drop-down list or click Add to create a password.
20. Click OK.



Configuration Backup Settings

Backup

☑ Enable configuration backup to the following repository:

Backup Repository_HPHV02 (Created by GOODDEALMART\csun at 1/10/2023

688 GB free of 931 GB

Restore points to keep: 10

Perform backup on: Daily at 10:00 AM

Last successful backup: 1/7/2023 10:00 AM

☑ Enable backup file encryption

Password:

Created by GOODDEALMART\csun at 1/7/2023 8:13 PM. (L

Loss protection disabled

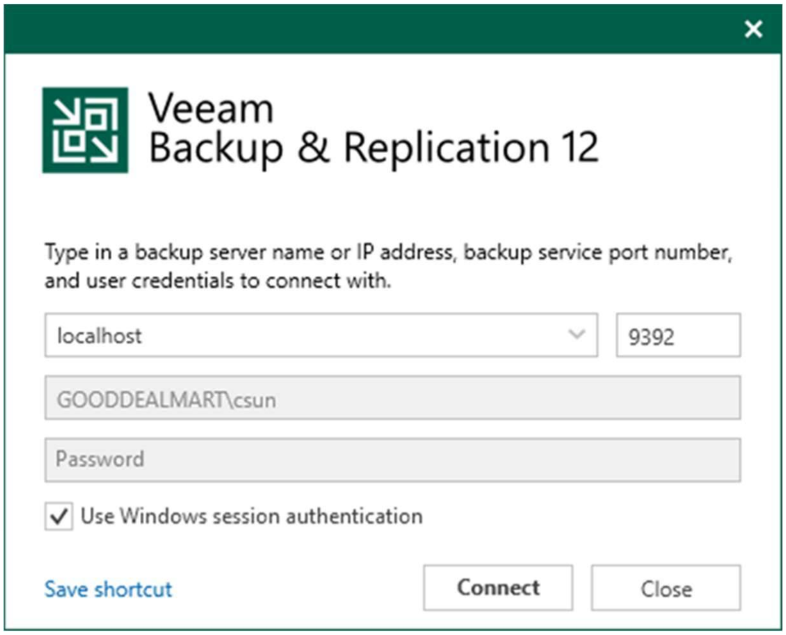
Restore

Restore the configuration backup to this server:

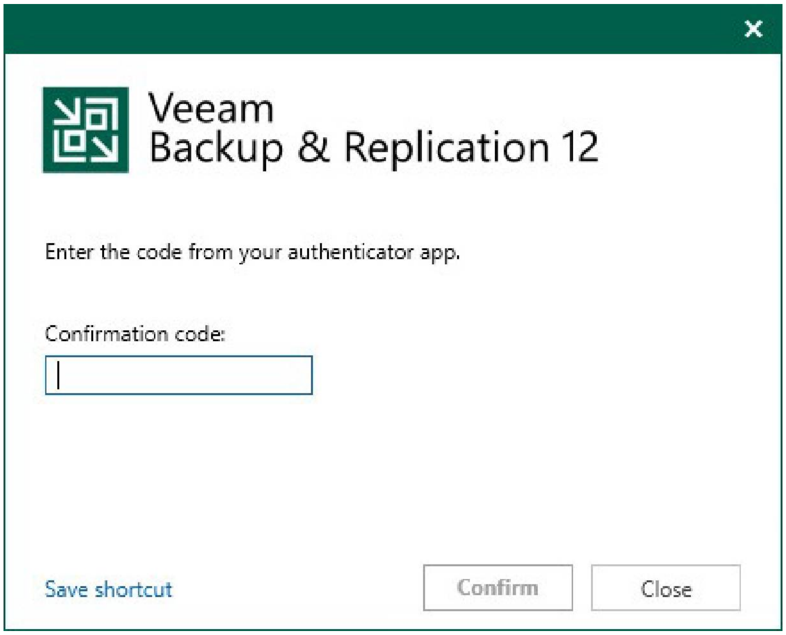
Configure Best Practices Analyzer

Veeam Backup & Replication includes a built-in tool that checks your backup server configuration to ensure it adheres to the Microsoft Windows Server operating system and Veeam backup infrastructure components security best practices.

The tool Best Practices Analyzer examines the following configuration parameters.

Instructions	Screenshot (if applicable)
1. Log in to the Veeam Backup and replication manager server. 2. Open the Veeam Backup & Replication Console and click Connect.	 Veeam Backup & Replication 12 Type in a backup server name or IP address, backup service port number, and user credentials to connect with. localhost 9392 GOODDEALMART\csun Password ☑ Use Windows session authentication

3. Enter the MFA Confirmation code and click Confirm.

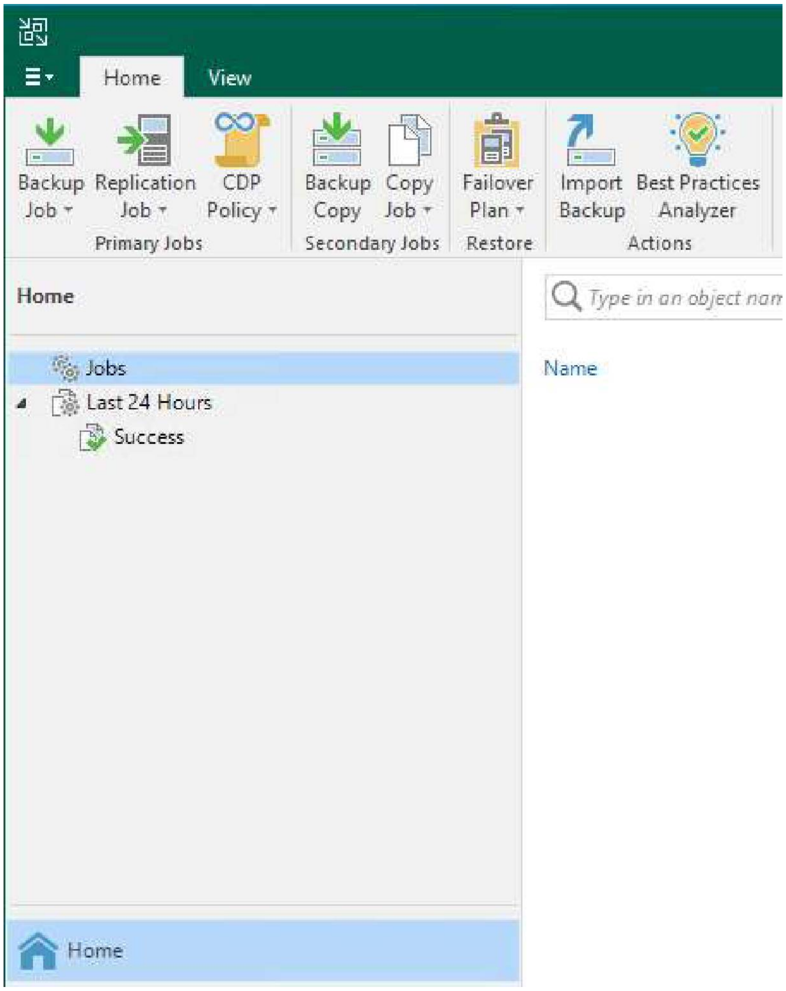


Veeam Backup & Replication 12

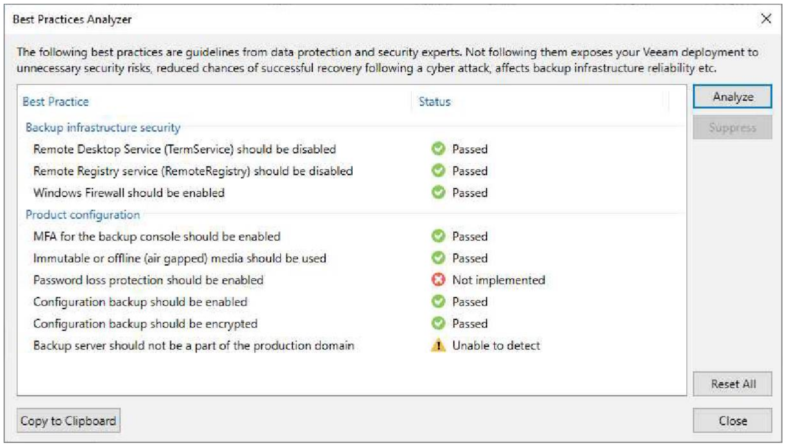
Enter the code from your authenticator app.

Confirmation code:

4. Select the Best Practices Analyzer on the Home page.



5. On the Best Practices Analyzer page, click Analyze after setting up the parameters as recommended and ensure that the status is changed to Passed.

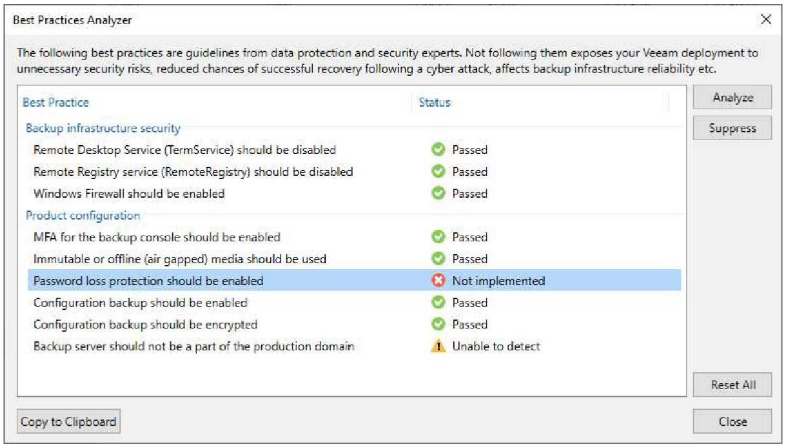


Best Practices Analyzer

The following best practices are guidelines from data protection and security experts. Not following them exposes your Veeam deployment to unnecessary security risks, reduced chances of successful recovery following a cyber attack, affects backup infrastructure reliability etc.

Best Practice	Status
Backup infrastructure security	
Remote Desktop Service (TermService) should be disabled	✓ Passed
Remote Registry service (RemoteRegistry) should be disabled	✓ Passed
Windows Firewall should be enabled	✓ Passed
Product configuration	
MFA for the backup console should be enabled	✓ Passed
Immutable or offline (air gapped) media should be used	✓ Passed
Password loss protection should be enabled	✗ Not implemented
Configuration backup should be enabled	✓ Passed
Configuration backup should be encrypted	✓ Passed
Backup server should not be a part of the production domain	⚠ Unable to detect

6. Select the parameter and click Suppress to skip the security check.

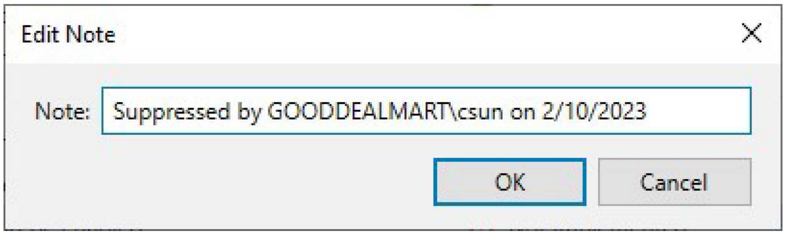


Best Practices Analyzer

The following best practices are guidelines from data protection and security experts. Not following them exposes your Veeam deployment to unnecessary security risks, reduced chances of successful recovery following a cyber attack, affects backup infrastructure reliability etc.

Best Practice	Status
Backup infrastructure security	
Remote Desktop Service (TermService) should be disabled	✓ Passed
Remote Registry service (RemoteRegistry) should be disabled	✓ Passed
Windows Firewall should be enabled	✓ Passed
Product configuration	
MFA for the backup console should be enabled	✓ Passed
Immutable or offline (air gapped) media should be used	✓ Passed
Password loss protection should be enabled	✗ Not implemented
Configuration backup should be enabled	✓ Passed
Configuration backup should be encrypted	✓ Passed
Backup server should not be a part of the production domain	⚠ Unable to detect

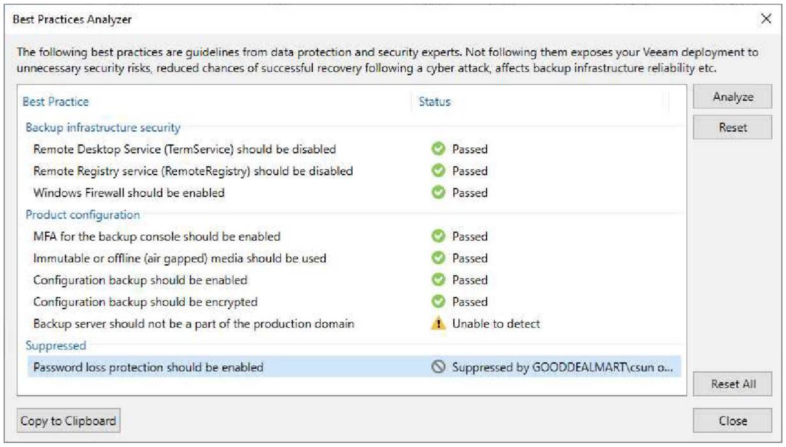
7. Comment briefly on the Note field on the Edit Note page for future reference, and click OK.



Edit Note

Note: Suppressed by GOODDEALMART\csun on 2/10/2023

8. Click Close on the Best Practices Analyzer page.



Best Practices Analyzer

The following best practices are guidelines from data protection and security experts. Not following them exposes your Veeam deployment to unnecessary security risks, reduced chances of successful recovery following a cyber attack, affects backup infrastructure reliability etc.

Best Practice	Status
Backup infrastructure security	
Remote Desktop Service (TermService) should be disabled	✓ Passed
Remote Registry service (RemoteRegistry) should be disabled	✓ Passed
Windows Firewall should be enabled	✓ Passed
Product configuration	
MFA for the backup console should be enabled	✓ Passed
Immutable or offline (air gapped) media should be used	✓ Passed
Configuration backup should be enabled	✓ Passed
Configuration backup should be encrypted	✓ Passed
Backup server should not be a part of the production domain	⚠ Unable to detect
Suppressed	
Password loss protection should be enabled	⊘ Suppressed by GOODDEALMART\csun o...

Chapter 4

Backup

Veeam Backup is a software application for data protection and disaster recovery in virtualized environments. It provides backup, recovery, replication, and continuous data protection for VMware vSphere and Microsoft Hyper-V virtual machines, physical servers, and cloud-based workloads.

Veeam Backup & Replication creates VM image-level backups. Image-level backups can be used for various restore scenarios, such as Instant Recovery, restoring full VM, recovery VM file, recovery file-level, etc.

Veeam Backup offers several features that help protect data, including:

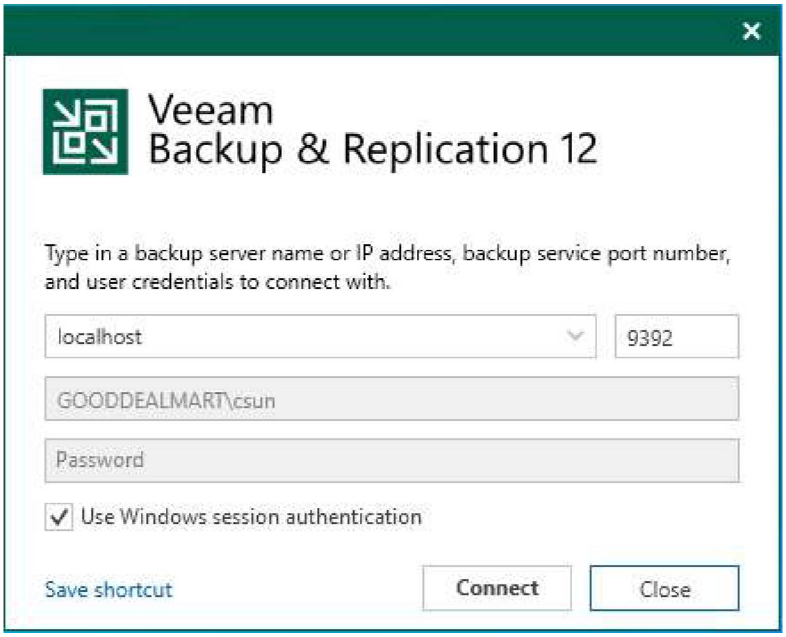
- Backup and replication: Veeam Backup provides backup and replication of virtual machines, physical servers, and cloud workloads. Backups can be scheduled, and Veeam Backup offers several backup methods, including incremental and full backups.
- Recovery: Veeam Backup allows quick and easy recovery of virtual machines, files, and application items, including granular-level recovery for emails and SharePoint items.
- Monitoring and reporting: Veeam Backup provides monitoring and reporting of backup and replication jobs, allowing administrators to identify issues and ensure backups are running as expected quickly.
- Cloud integration: Veeam Backup integrates with several cloud providers, including AWS, Microsoft Azure, and Google Cloud Platform, allowing backups to be stored in the cloud.

Veeam Backup is a powerful, flexible data protection and disaster recovery solution in virtualized environments.

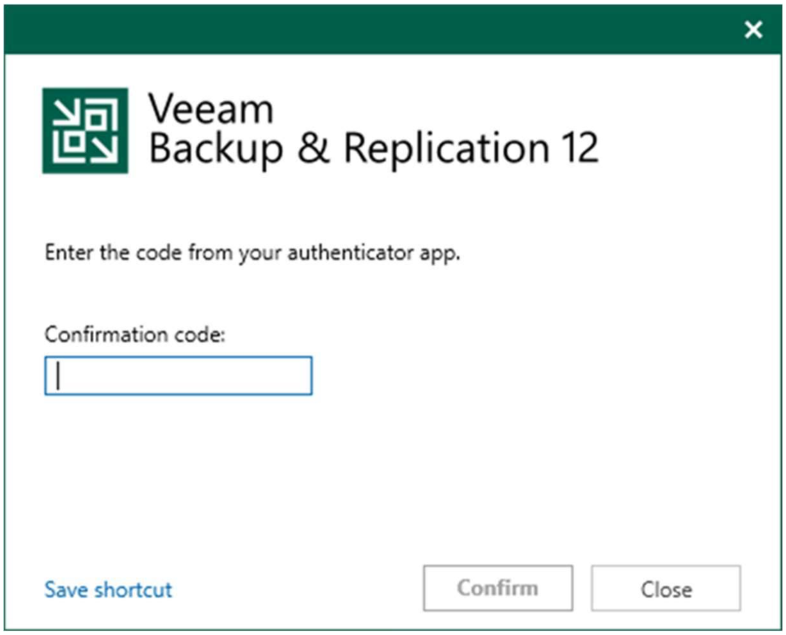
Create a Backup job to backup the specified VMs

To backup VMs, you must first create a backup job. The backup job specifies how, where, and when VM data should be backed up. A single job can process one or more virtual machines. Jobs can be started by hand or scheduled for a specific time.

This procedure creates a backup job to back up the production VMs specified.

Instructions	Screenshot (if applicable)
1. Log in to the Veeam Backup and replication manager server. 2. Open the Veeam Backup & Replication Console and click Connect.	 Veeam Backup & Replication 12 Type in a backup server name or IP address, backup service port number, and user credentials to connect with. localhost 9392 GOODDEALMART\csun Password ☑ Use Windows session authentication

3. Enter the MFA Confirmation code and click Confirm.

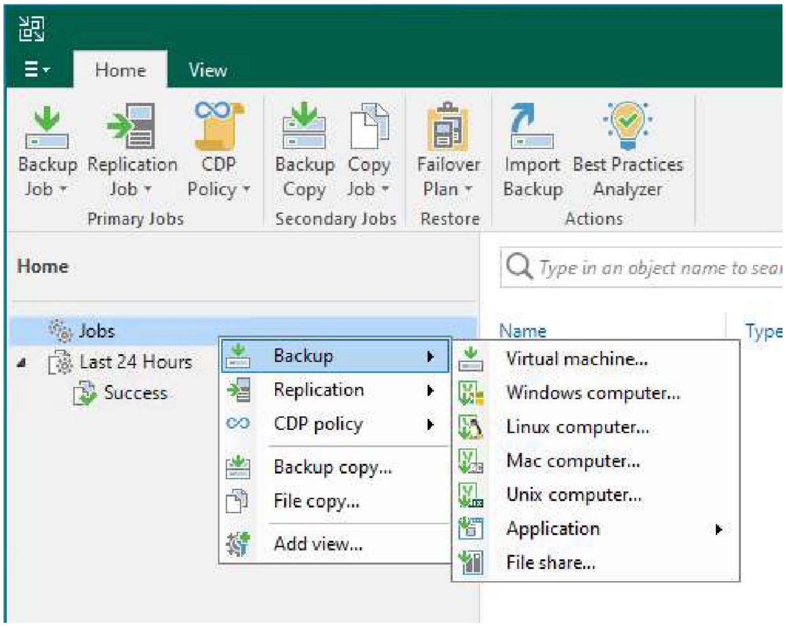


Veeam Backup & Replication 12

Enter the code from your authenticator app.

Confirmation code:

4. Select Jobs on the Home page and right-click Jobs.
5. Select Backup and click Virtual machine.

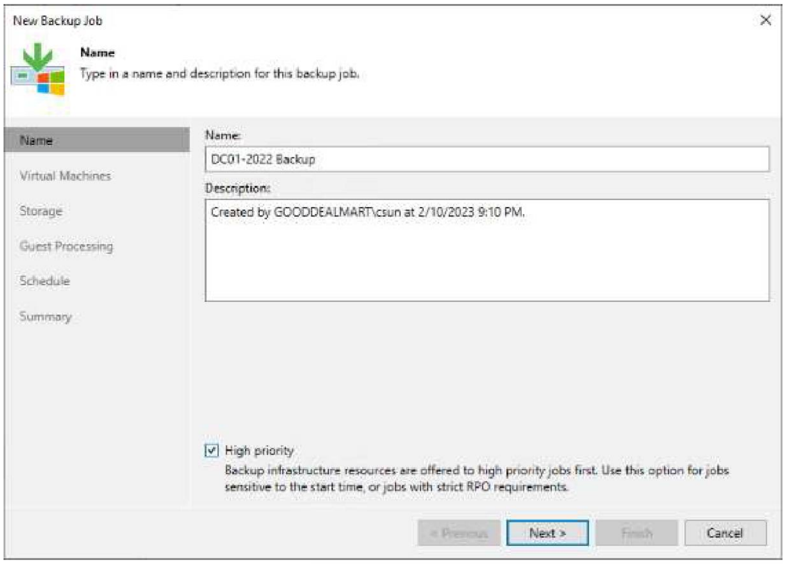


6. On the Name page, enter a name for the backup job in the Name field.

7. Give a brief description in the Description field for the future.

8. Select the High priority checkbox if you want this job to allocate resources in the first place.

9. Click Next.



New Backup Job

Name

Type in a name and description for this backup job.

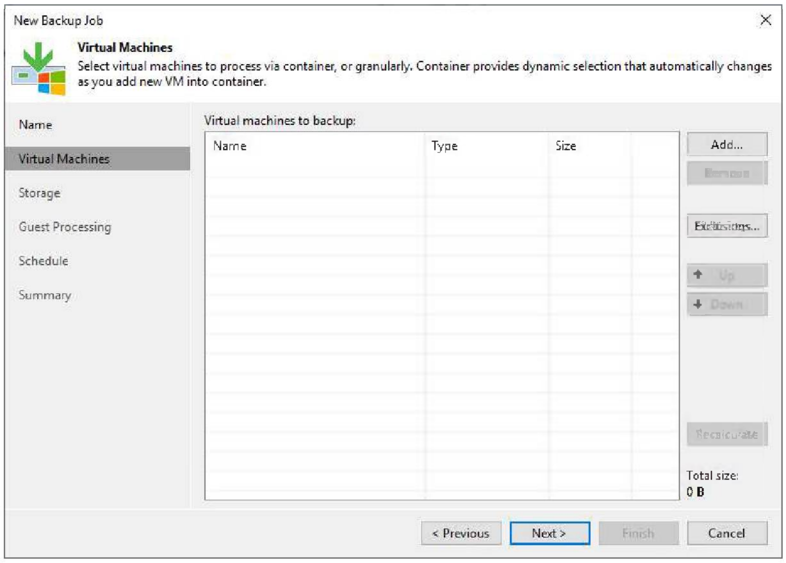
Name: DC01-2022 Backup

Description: Created by GOODDEALMART\csun at 2/10/2023 9:10 PM.

☑ High priority

Backup infrastructure resources are offered to high priority jobs first. Use this option for jobs sensitive to the start time, or jobs with strict RPO requirements.

10. Click Add on the Virtual Machines page.



New Backup Job

Virtual Machines

Select virtual machines to process via container, or granularly. Container provides dynamic selection that automatically changes as you add new VM into container.

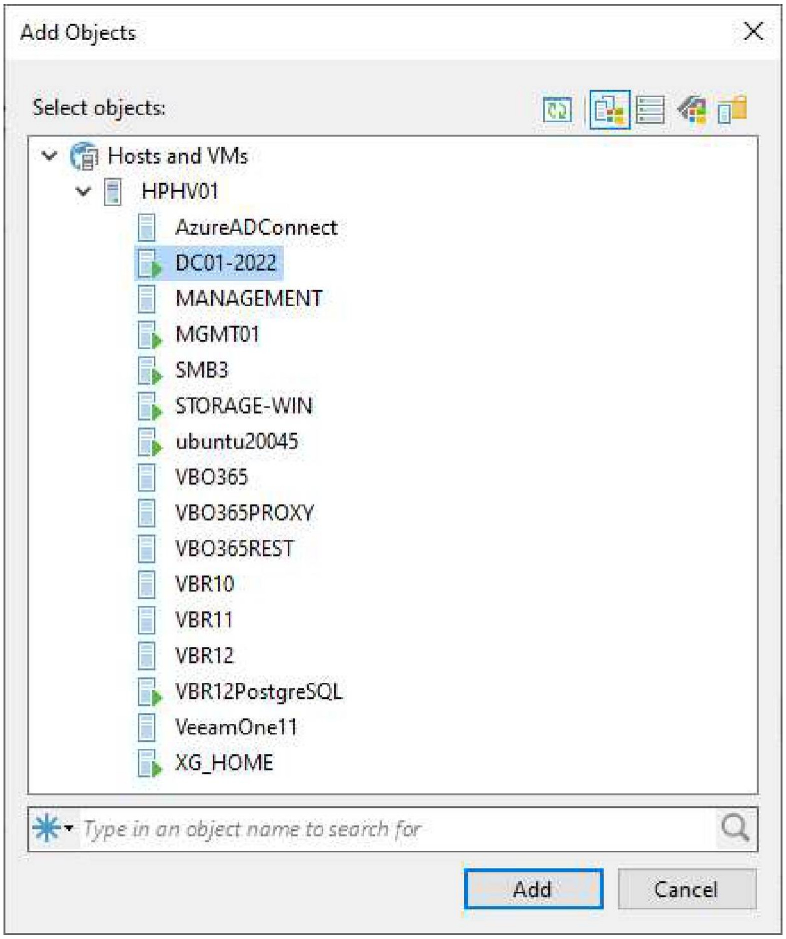
Virtual machines to backup:

Name	Type	Size

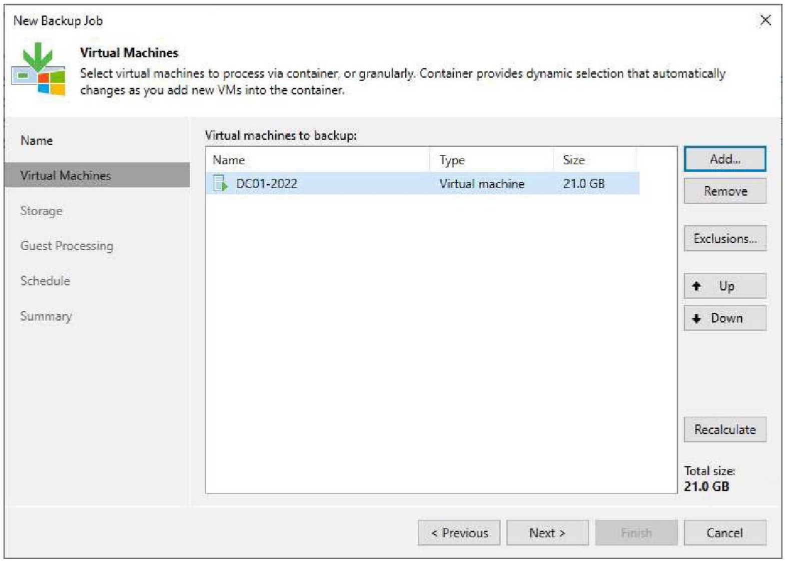
Total size: 0 B

11. Select the VM from the Select objects list on the Add Objects page and click Add.

12. If you have multiple VMS that needs to back up in the same backup job, you can repeat the step to add them.



13. Click Next on the Virtual Machines page.



New Backup Job

Virtual Machines

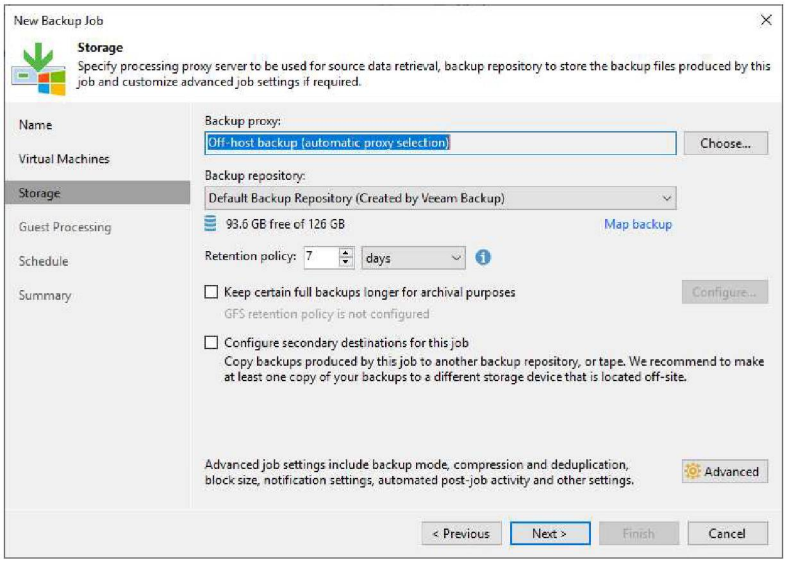
Select virtual machines to process via container, or granularly. Container provides dynamic selection that automatically changes as you add new VMs into the container.

Virtual machines to backup:

Name	Type	Size
DC01-2022	Virtual machine	21.0 GB

Total size: **21.0 GB**

14. On the Storage page, click Choose to select a backup proxy if you don't want to use the default Off-host backup (automatic proxy selection) setting.



New Backup Job

Storage

Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Backup proxy: Off-host backup (automatic proxy selection)

Backup repository: Default Backup Repository (Created by Veeam Backup)

93.6 GB free of 126 GB

Retention policy: 7 days

☐ Keep certain full backups longer for archival purposes

GFS retention policy is not configured

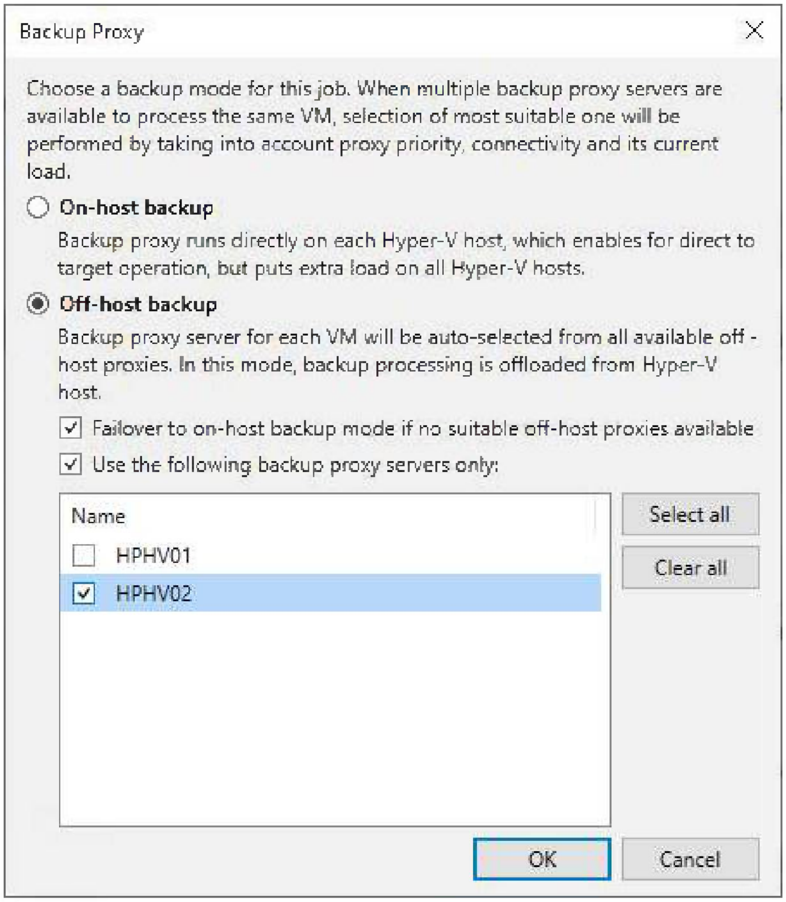
☐ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

15. On the Backup Proxy page, if you select On-host backup mode, the source Microsoft HyperV host will serve as both the source host and the backup proxy. In this mode, Veeam Data Mover runs directly on the source host, which speeds up data retrieval but places additional strain on the host.

16. If you select Off-host backup mode, Veeam Data Mover will run on a dedicated off-host backup proxy. All backup processing operations from the source host are routed to the off-host backup proxy in this model.



Backup Proxy

Choose a backup mode for this job. When multiple backup proxy servers are available to process the same VM, selection of most suitable one will be performed by taking into account proxy priority, connectivity and its current load.

○ **On-host backup**

Backup proxy runs directly on each Hyper-V host, which enables for direct to target operation, but puts extra load on all Hyper-V hosts.

● **Off-host backup**

Backup proxy server for each VM will be auto-selected from all available off - host proxies. In this mode, backup processing is offloaded from Hyper-V host.

☑ Failover to on-host backup mode if no suitable off-host proxies available

☑ Use the following backup proxy servers only:

Name
□ HPHV01
☑ HPHV02

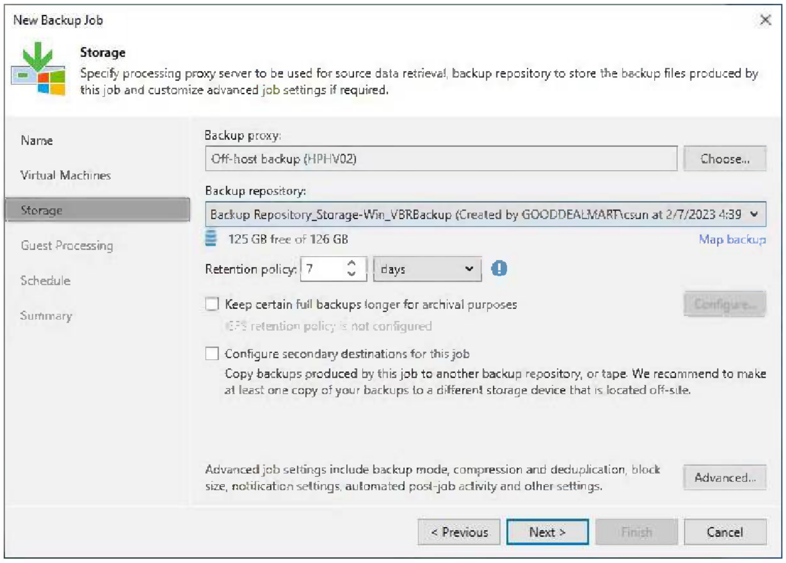
17. If the off-host backup mode is selected for the job, but no off-host backup proxies are available when the job begins, Veeam Backup & Replication will transition to on-host backup mode.

18. You unselect the Failover to on-host backup mode if no suitable off-host

proxies are available in the checkbox. Still, the job will fail to start if off-host backup proxies are unavailable or configured properly.

19. Click OK.

20. Select the backup repository from the Backup repository drop-down list where the created backup files must be saved.



New Backup Job

Storage

Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Backup proxy: Off-host backup (HPHV02)

Backup repository: Backup Repository_Storage-Win_VBRBackup (Created by GOODDEALMART\csun at 2/7/2023 4:39

125 GB free of 126 GB

Retention policy: 7 days

□ Keep certain full backups longer for archival purposes

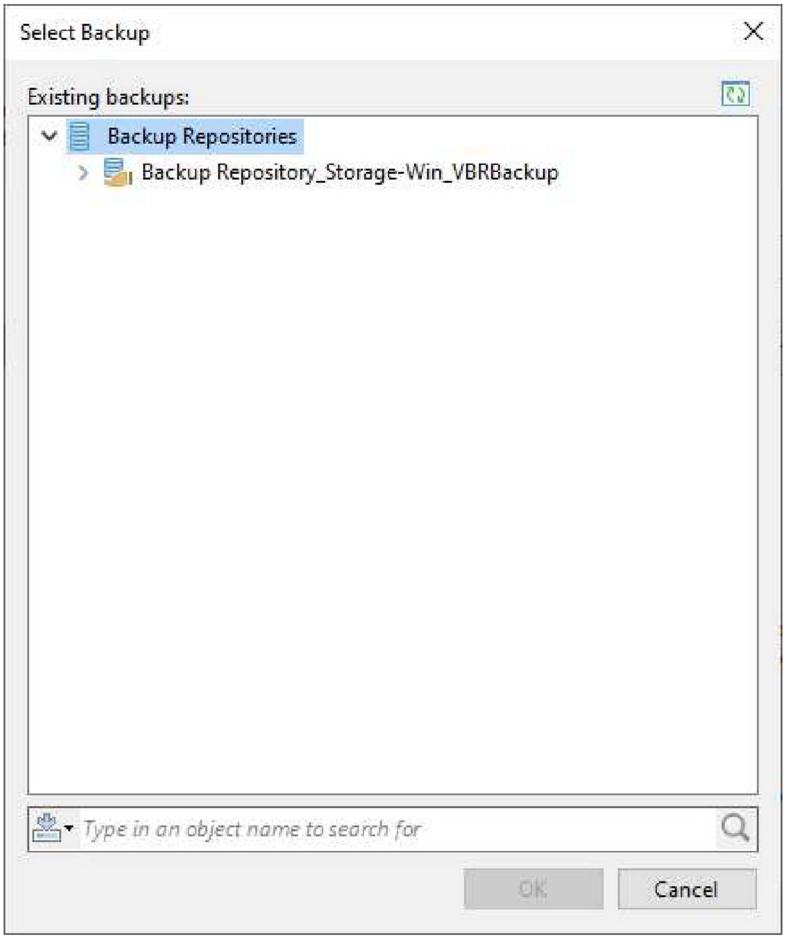
GFS retention policy is not configured

□ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

21. Click Map backup is helpful if you have relocated backup files to a new backup repository and want to point the job to existing backups in this new backup repository. Backup job mapping can also be used if the configuration database becomes corrupt and you need to reconfigure backup jobs.



Select Backup

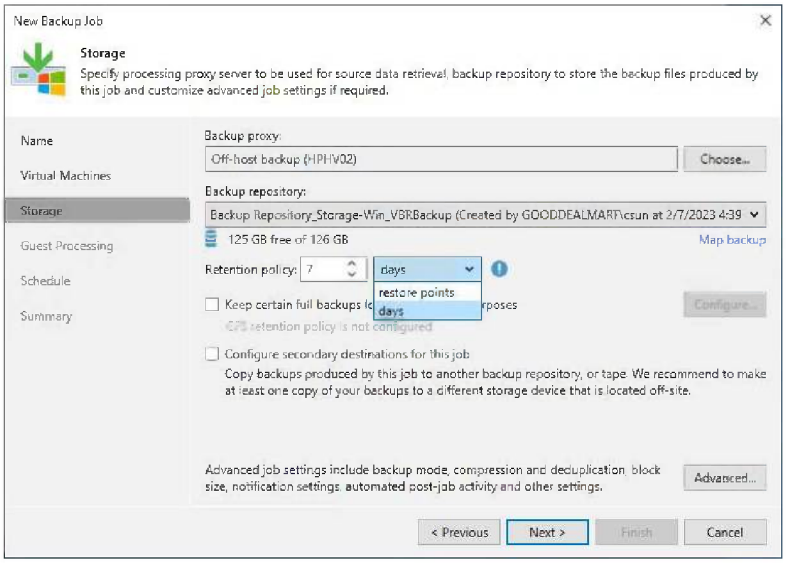
Existing backups:

Backup Repositories

Backup Repository_Storage-Win_VBRBackup

22. Set the retention policy settings for restore points in the Retention Policy field.

23. Select days or restore points from the drop-down list.



New Backup Job

Storage

Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Backup proxy: Off-host backup (HPHV02)

Backup repository: Backup Repository_Storage-Win_VBRBackup (Created by GOODDEALMART\csun at 2/7/2023 4:39

125 GB free of 126 GB

Retention policy: 7 days

□ Keep certain full backups lo rposes

GFS retention policy is not configured

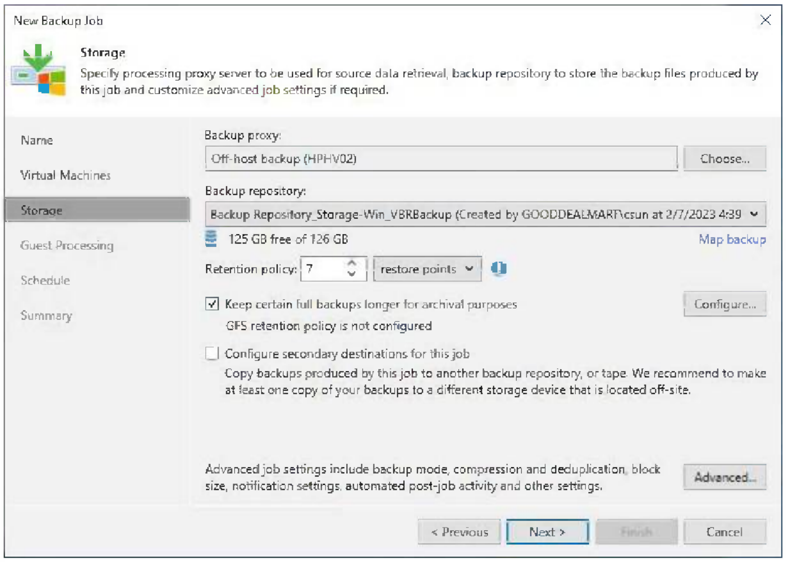
□ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

24. You can configure GFS retention policy settings for the backup job to ignore the short-term retention policy for some full backups and store them for long-term archiving.

25. Select the Keep certain full backups for longer for archival purposes. Then, if you need it, click Configure.



New Backup Job

Storage

Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Backup proxy: Off-host backup (HPHV02)

Backup repository: Backup Repository_Storage-Win_VBRBackup (Created by GOODDEALMART\csun at 2/7/2023 4:39

125 GB free of 126 GB

Retention policy: 7 restore points

☑ Keep certain full backups longer for archival purposes

GFS retention policy is not configured

□ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

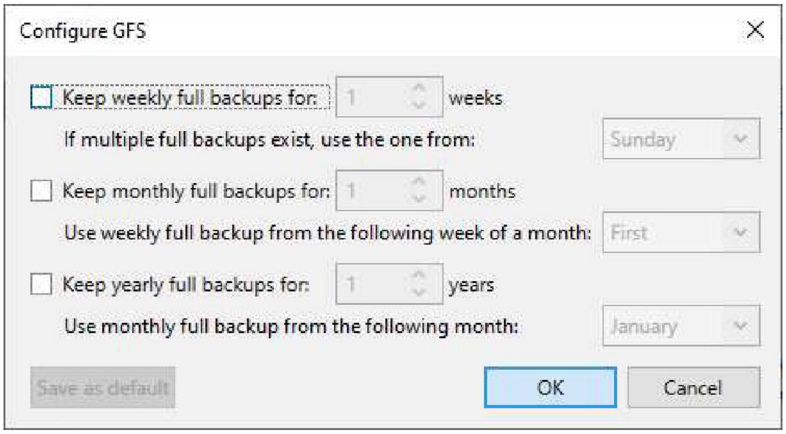
Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

26. Select the Keep weekly full backups for check box, and specify the number of weeks you want to prevent restore points from being modified and deleted.

27. Select the Keep monthly full backups for check box, and specify the months you want to prevent restore points from being modified and deleted.

28. Select the Keep yearly full backups for check box, and specify the years you want to prevent restore points from being modified and deleted.

29. Click OK.



Configure GFS

☐ Keep weekly full backups for: 1 weeks

If multiple full backups exist, use the one from: Sunday

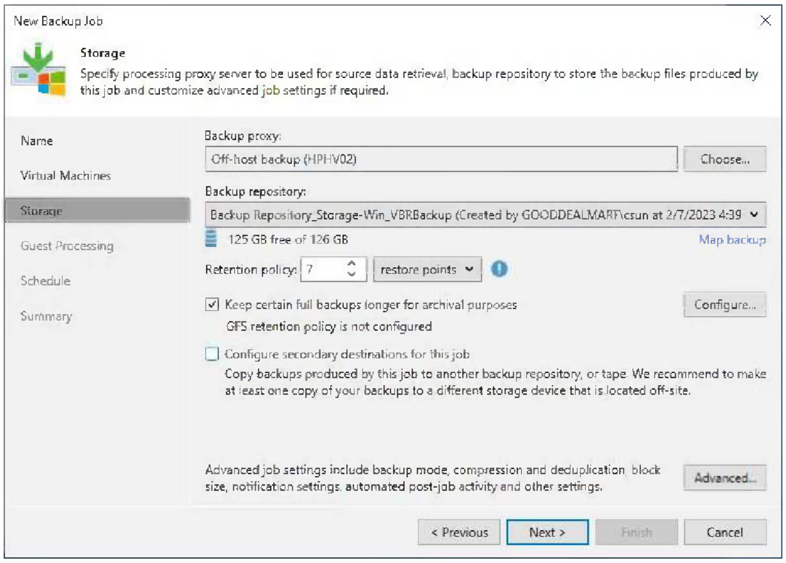
☐ Keep monthly full backups for: 1 months

Use weekly full backup from the following week of a month: First

☐ Keep yearly full backups for: 1 years

Use monthly full backup from the following month: January

30. On the Storage page, click Advanced.



New Backup Job

Storage

Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Backup proxy: Off-host backup (HPHV02)

Backup repository: Backup Repository_Storage-Win_VBRBackup (Created by GOODDEALMART\csun at 2/7/2023 4:39

125 GB free of 126 GB

Retention policy: 7 restore points

☑ Keep certain full backups longer for archival purposes

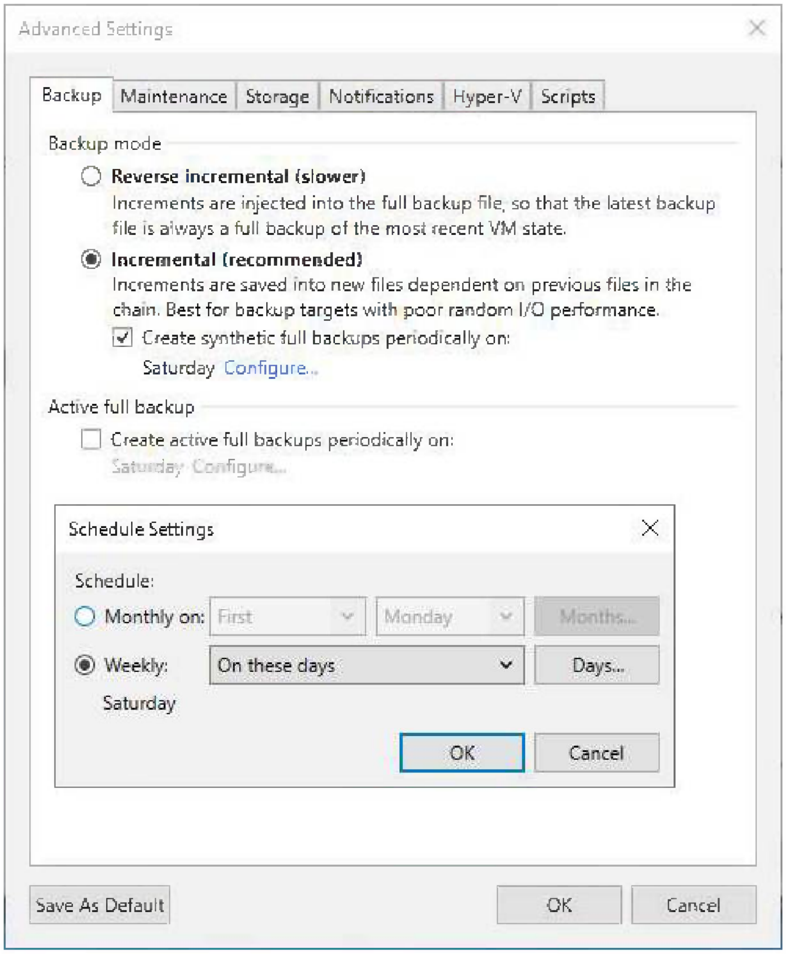
GFS retention policy is not configured

☐ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

31. On the Backup page, select Incremental (recommended).
32. Select create synthetic full backups periodically or active full backups periodically checkbox.
33. Click Configure to schedule full backups periodically and click OK.



Advanced Settings

Backup | Maintenance | Storage | Notifications | Hyper-V | Scripts

Backup mode

○ **Reverse incremental (slower)**
Increments are injected into the full backup file, so that the latest backup file is always a full backup of the most recent VM state.

● **Incremental (recommended)**
Increments are saved into new files dependent on previous files in the chain. Best for backup targets with poor random I/O performance.

☑ Create synthetic full backups periodically on:
Saturday Configure...

Active full backup

□ Create active full backups periodically on:
Saturday Configure...

Schedule Settings

Schedule:

○ Monthly on: First | Monday | Months...

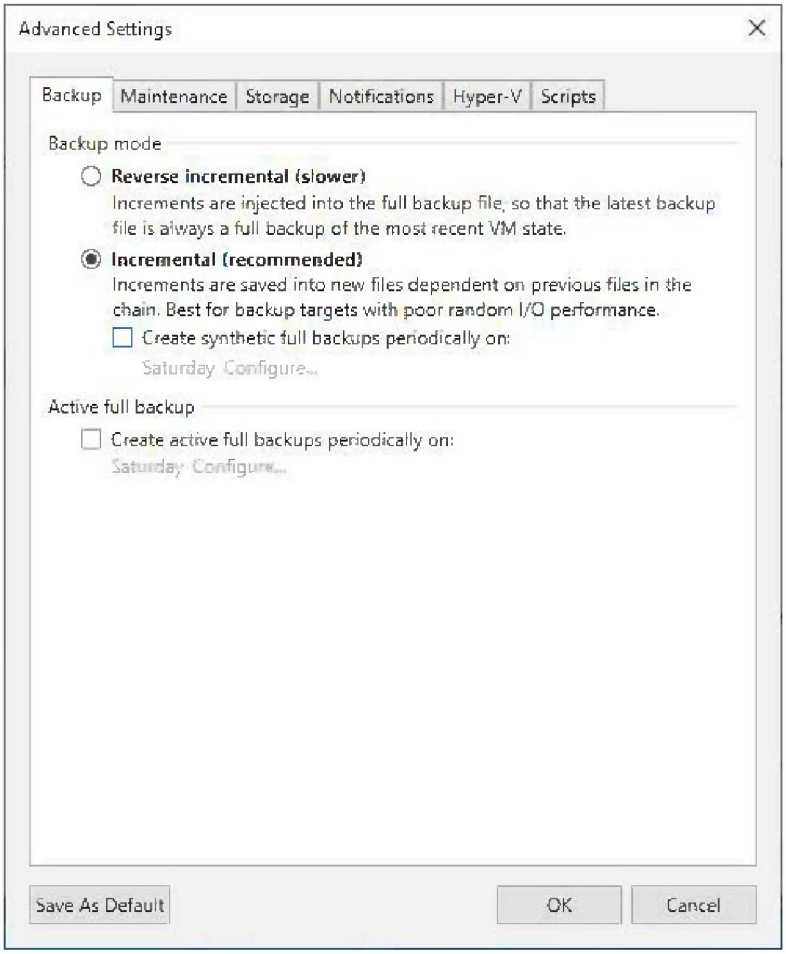
● Weekly: On these days | Days...

Saturday

OK Cancel

Save As Default OK Cancel

34. Select Incremental and disable synthetic full or active full backups to create a forever forward incremental backup chain if needed.



Advanced Settings

Backup mode

○ **Reverse incremental (slower)**
Increments are injected into the full backup file, so that the latest backup file is always a full backup of the most recent VM state.

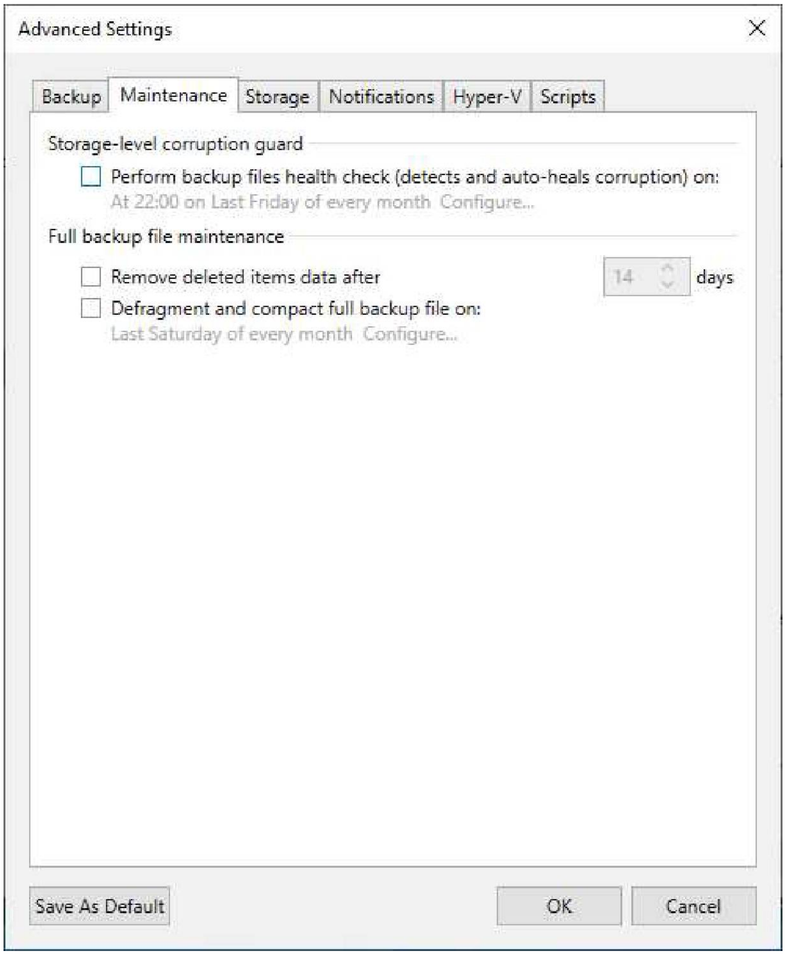
● **Incremental (recommended)**
Increments are saved into new files dependent on previous files in the chain. Best for backup targets with poor random I/O performance.

□ Create synthetic full backups periodically on:
Saturday Configure...

Active full backup

□ Create active full backups periodically on:
Saturday Configure...

35. On the Advanced Settings, select Maintenance.



Advanced Settings

Storage-level corruption guard

□ Perform backup files health check (detects and auto-heals corruption) on:
At 22:00 on Last Friday of every month Configure...

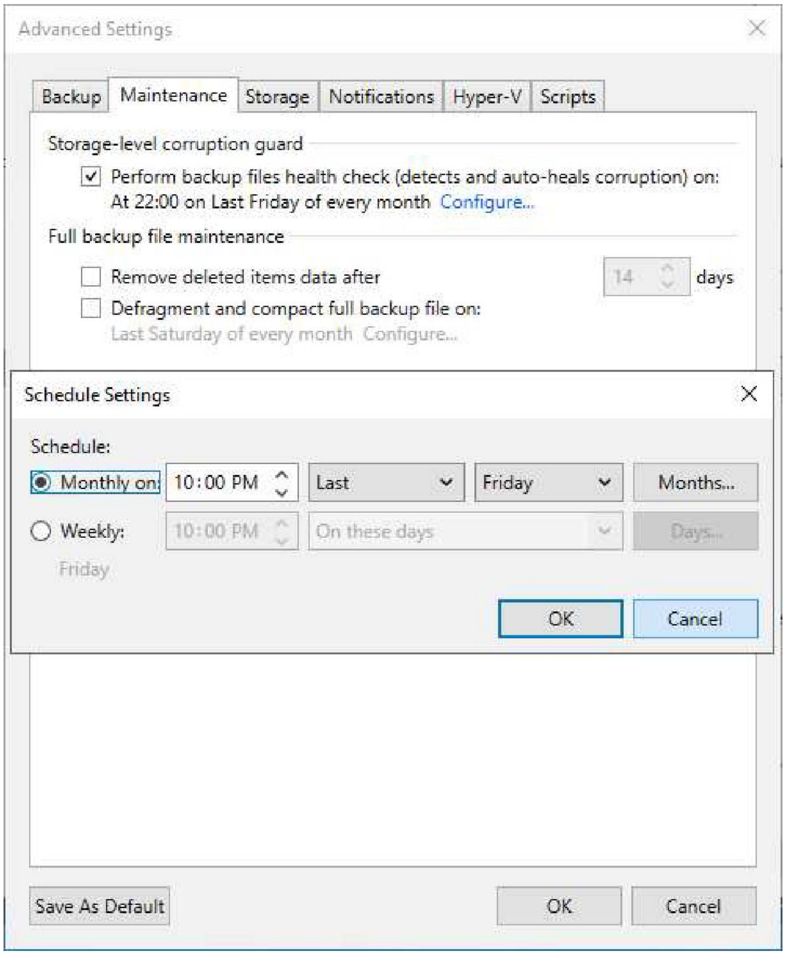
Full backup file maintenance

□ Remove deleted items data after 14 days

□ Defragment and compact full backup file on:
Last Saturday of every month Configure...

36. To regularly perform a health check on the backup chain's most recent restore point, select the Perform backup files health check (detects and auto-heals corruption) checkbox in the Storage-level corruption guard section.

37. Click Configure to set a timetable for the health check.



Advanced Settings

Storage-level corruption guard

☑ Perform backup files health check (detects and auto-heals corruption) on:
At 22:00 on Last Friday of every month Configure...

Full backup file maintenance

□ Remove deleted items data after 14 days

□ Defragment and compact full backup file on:
Last Saturday of every month Configure...

Schedule Settings

Schedule:

● Monthly on: 10:00 PM Last Friday Months...

○ Weekly: 10:00 PM On these days Days...
Friday

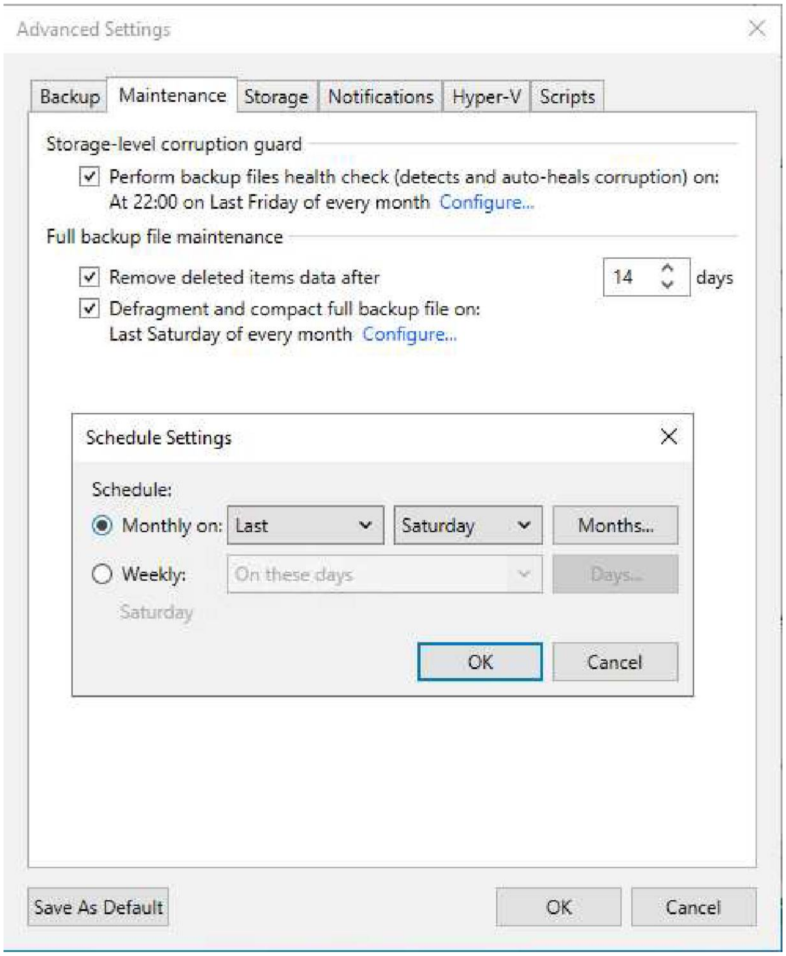
38. Select the Remove deleted items data after the checkbox and enter the few days you want backup data for deleted VMs to be kept.

39. Select the Defragment and compact full backup file checkbox and click Configure.

40. Set the schedule for the compact operation to compact a full backup periodically.

Note:

GFS retention is not compatible with defragment and compact functionality.



Storage-level corruption guard

☑ Perform backup files health check (detects and auto-heals corruption) on:
At 22:00 on Last Friday of every month Configure...

Full backup file maintenance

☑ Remove deleted items data after 14 days

☑ Defragment and compact full backup file on:
Last Saturday of every month Configure...

Schedule:

● Monthly on: Last Saturday

○ Weekly: On these days
Saturday

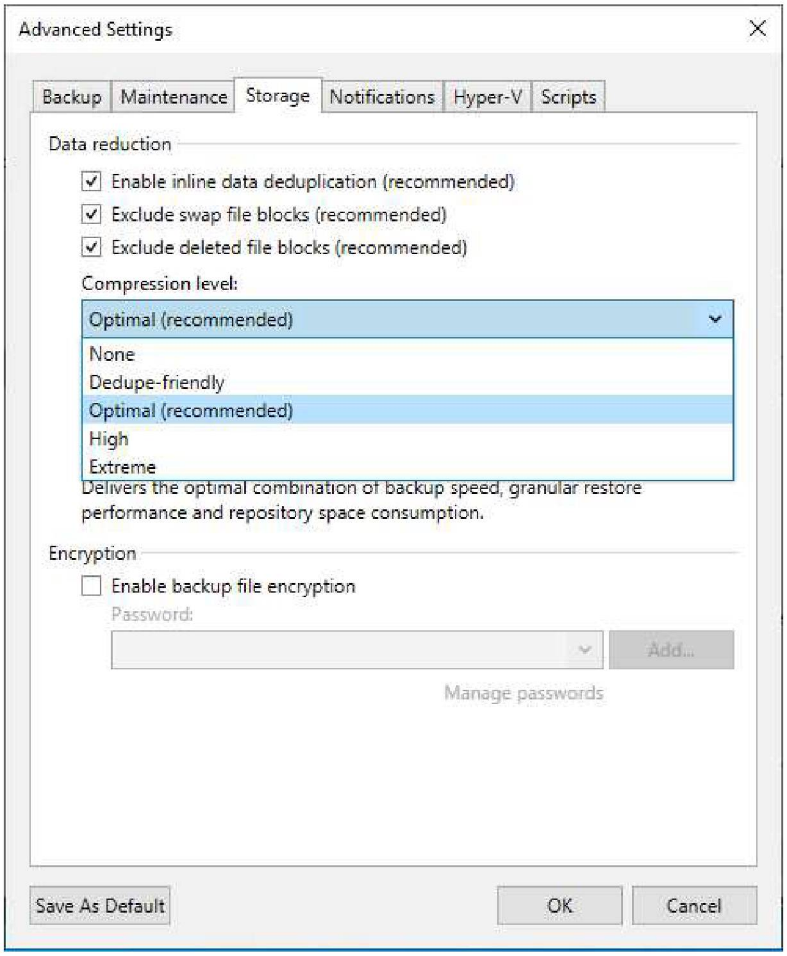
41. On Advanced Settings, select Storage.

42. Select the Enable inline data deduplication (recommended) checkbox.

43. Select the Exclude swap file blocks (recommended) checkbox.

44. Select the Exclude deleted file blocks (recommended) checkbox.

45. Select the compression level for the backup from the drop-down list.



Data reduction

☑ Enable inline data deduplication (recommended)

☑ Exclude swap file blocks (recommended)

☑ Exclude deleted file blocks (recommended)

Compression level:

Optimal (recommended)

- None
- Dedupe-friendly
- Optimal (recommended)
- High
- Extreme

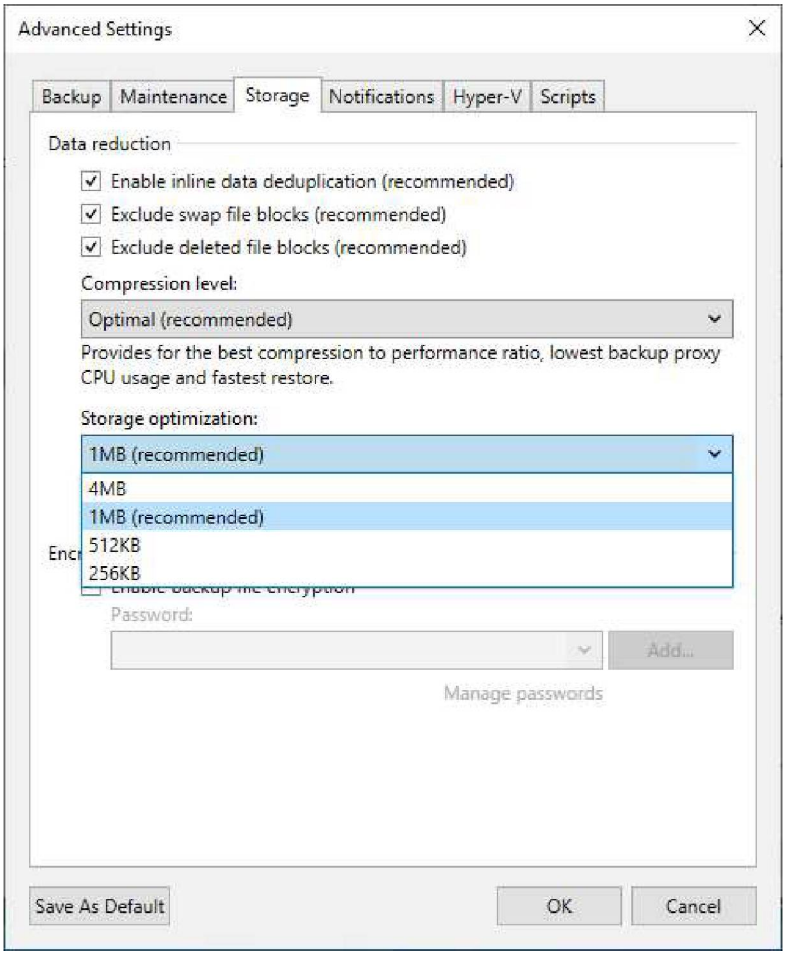
Delivers the optimal combination of backup speed, granular restore performance and repository space consumption.

Encryption

□ Enable backup file encryption

Password:

46. Select the Storage optimization for the backup from the drop-down list.



Advanced Settings

Data reduction

☑ Enable inline data deduplication (recommended)

☑ Exclude swap file blocks (recommended)

☑ Exclude deleted file blocks (recommended)

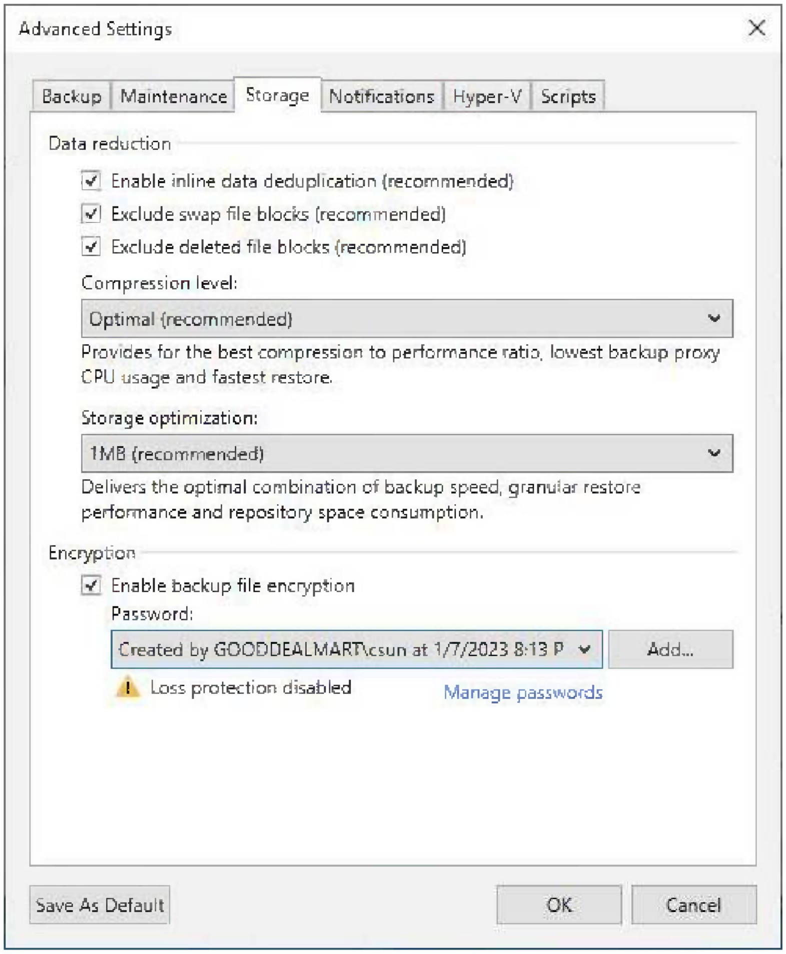
Compression level: Optimal (recommended)

Provides for the best compression to performance ratio, lowest backup proxy CPU usage and fastest restore.

Storage optimization: 1MB (recommended)

47. Select the Enable backup file encryption checkbox to encrypt the content of backup files.

48. Select a password from the drop-down list. Then, if you still need to do, click Add or use the Manage passwords link to create a new password.



Advanced Settings

Data reduction

☑ Enable inline data deduplication (recommended)

☑ Exclude swap file blocks (recommended)

☑ Exclude deleted file blocks (recommended)

Compression level: Optimal (recommended)

Provides for the best compression to performance ratio, lowest backup proxy CPU usage and fastest restore.

Storage optimization: 1MB (recommended)

Delivers the optimal combination of backup speed, granular restore performance and repository space consumption.

Encryption

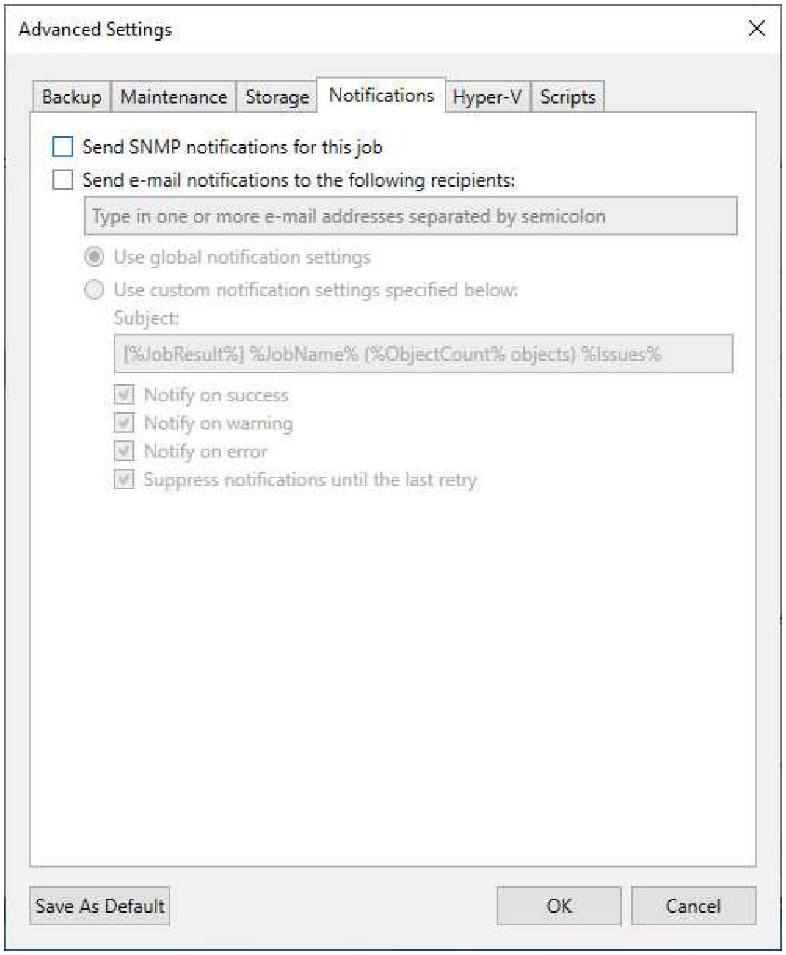
☑ Enable backup file encryption

Password: Created by GOODDEALMART\csun at 1/7/2023 8:13 P

Loss protection disabled

49. On the Advanced Settings, select Notifications.

50. Keep the default settings.



Advanced Settings

□ Send SNMP notifications for this job

□ Send e-mail notifications to the following recipients:

Type in one or more e-mail addresses separated by semicolon

● Use global notification settings

○ Use custom notification settings specified below:

Subject:

[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

☑ Notify on success

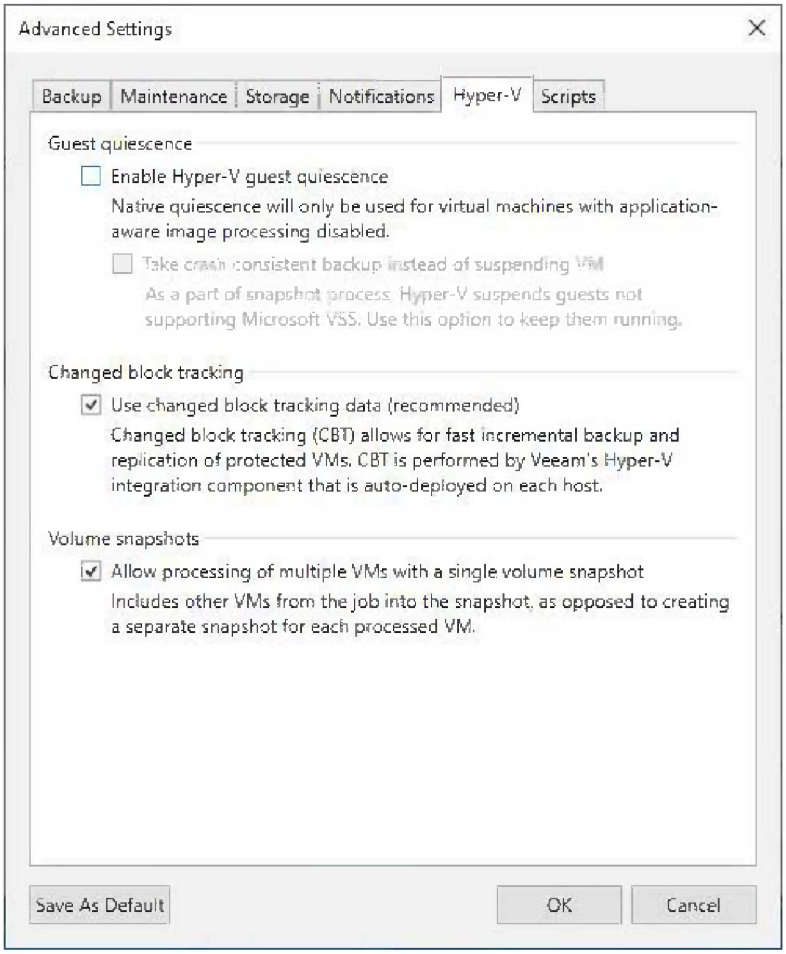
☑ Notify on warning

☑ Notify on error

☑ Suppress notifications until the last retry

51. On the Advanced Settings, select Hyper-V.

52. Keep the default settings.



Guest quiescence

□ Enable Hyper-V guest quiescence

Native quiescence will only be used for virtual machines with application-aware image processing disabled.

□ Take crash consistent backup instead of suspending VM

As a part of snapshot process, Hyper-V suspends guests not supporting Microsoft VSS. Use this option to keep them running.

Changed block tracking

☑ Use changed block tracking data (recommended)

Changed block tracking (CBT) allows for fast incremental backup and replication of protected VMs. CBT is performed by Veeam's Hyper-V integration component that is auto-deployed on each host.

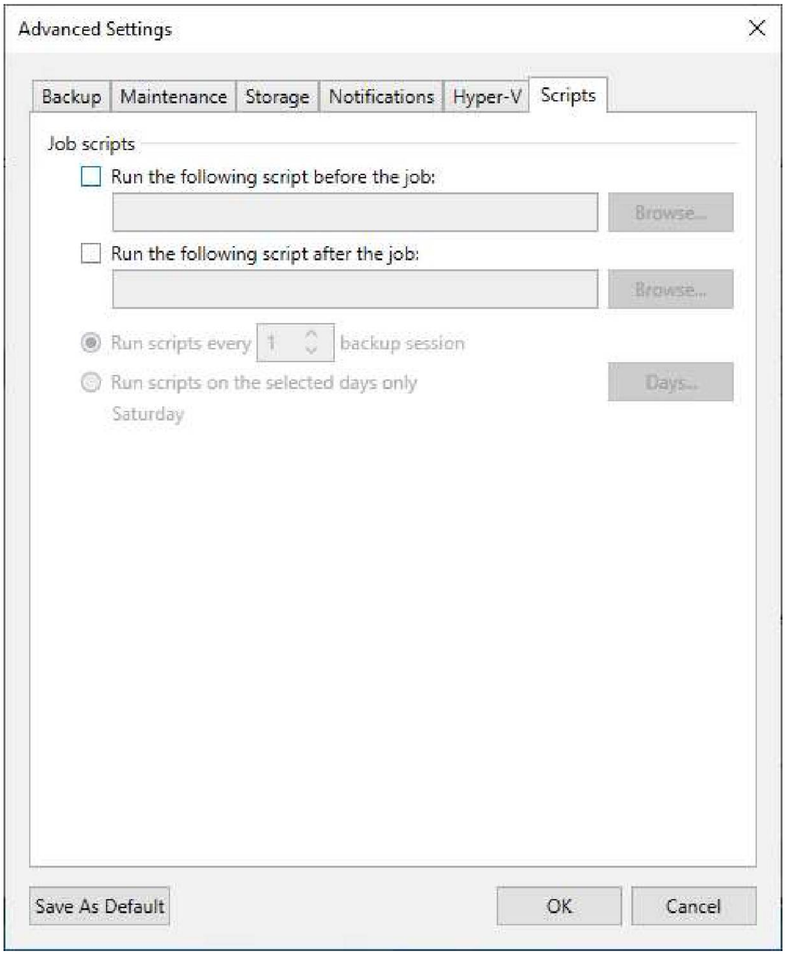
Volume snapshots

☑ Allow processing of multiple VMs with a single volume snapshot

Includes other VMs from the job into the snapshot, as opposed to creating a separate snapshot for each processed VM.

53. On the Advanced Settings page, click Scripts and keep the default settings.

54. Click OK.



Advanced Settings

Backup | Maintenance | Storage | Notifications | Hyper-V | Scripts

Job scripts

□ Run the following script before the job:

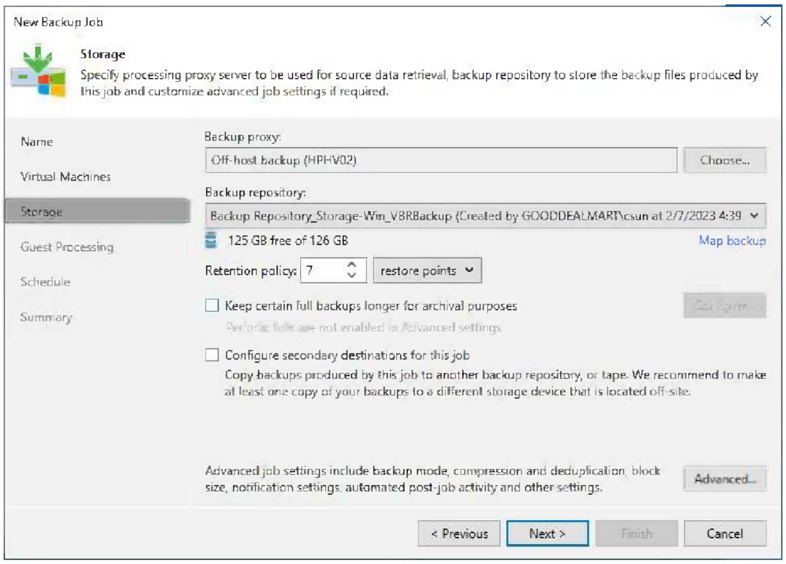
□ Run the following script after the job:

● Run scripts every 1 backup session

○ Run scripts on the selected days only

Saturday

55. On the Storage page, click Next.



Storage

Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Backup proxy: Off-host backup (HPHV02)

Backup repository: Backup Repository_Storage-Win_VBRBackup (Created by GOODDEALMART\csun at 2/7/2023 4:39

125 GB free of 126 GB

Retention policy: 7 restore points

□ Keep certain full backups longer for archival purposes

Periodic fulls are not enabled in Advanced settings

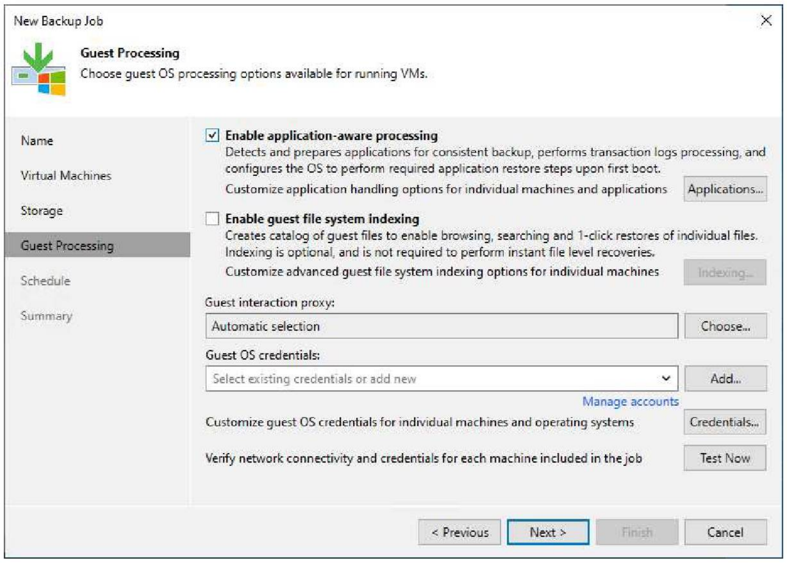
□ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

56. When you add VMs running VSS-aware applications to the backup job, you can enable application-aware processing to create a transactionally consistent backup. The transactionally consistent backup ensures that applications on VMs can be recovered without data loss.

57. Select the Enable application-aware processing checkbox on the Guest Processing page and click Applications.



Guest Processing

Choose guest OS processing options available for running VMs.

☑ **Enable application-aware processing**

Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

Customize application handling options for individual machines and applications

□ **Enable guest file system indexing**

Creates catalog of guest files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries.

Customize advanced guest file system indexing options for individual machines

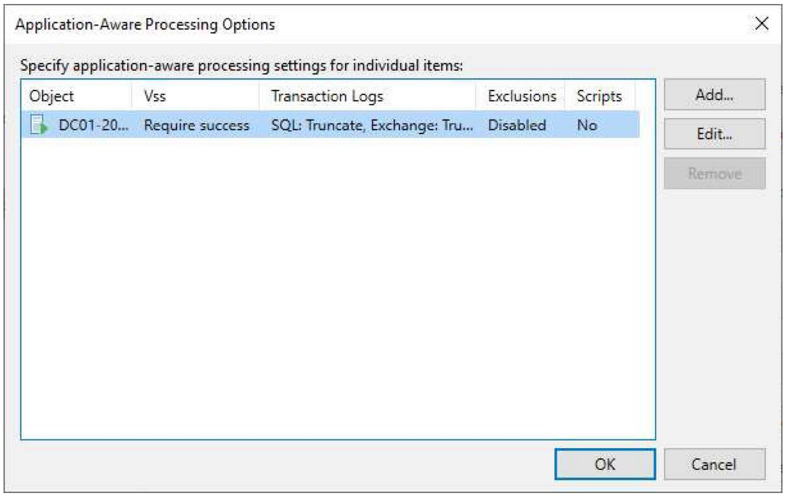
Guest interaction proxy: Automatic selection

Guest OS credentials: Select existing credentials or add new

Customize guest OS credentials for individual machines and operating systems

Verify network connectivity and credentials for each machine included in the job

58. On the Application-Aware Processing Options page, select the VM and click Edit.



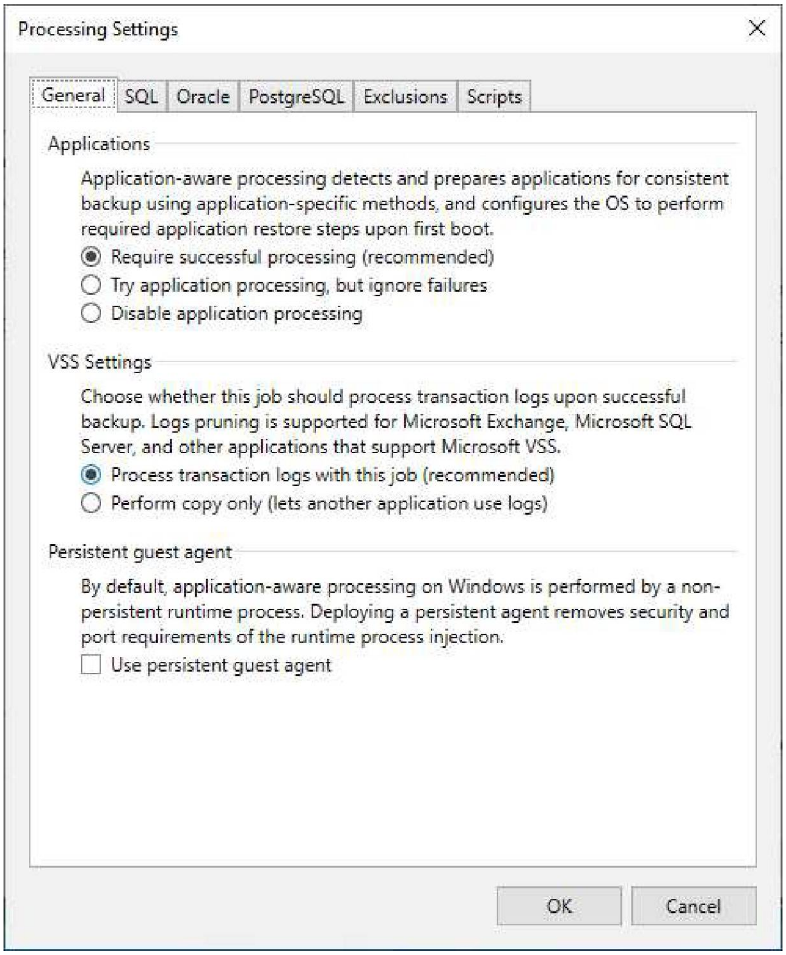
Application-Aware Processing Options

Specify application-aware processing settings for individual items:

Object	Vss	Transaction Logs	Exclusions	Scripts
DC01-20...	Require success	SQL: Truncate, Exchange: Tru...	Disabled	No

59. On the Processing Settings, click General.

60. Keep the default settings.



Processing Settings

Applications

Application-aware processing detects and prepares applications for consistent backup using application-specific methods, and configures the OS to perform required application restore steps upon first boot.

● Require successful processing (recommended)

○ Try application processing, but ignore failures

○ Disable application processing

VSS Settings

Choose whether this job should process transaction logs upon successful backup. Logs pruning is supported for Microsoft Exchange, Microsoft SQL Server, and other applications that support Microsoft VSS.

● Process transaction logs with this job (recommended)

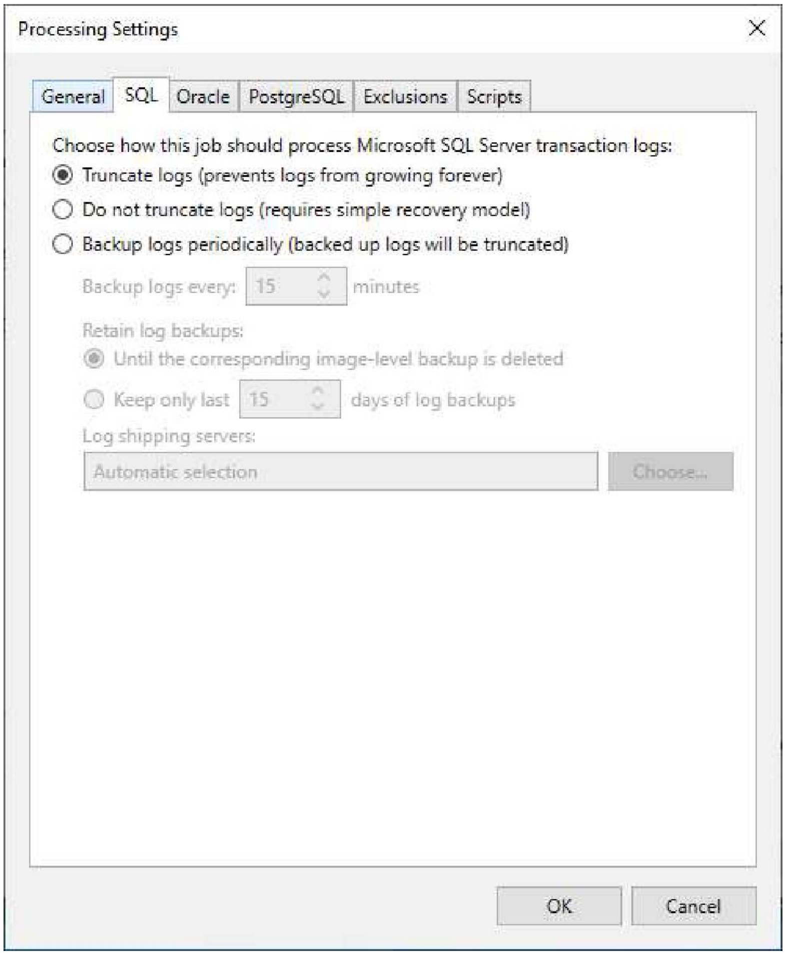
○ Perform copy only (lets another application use logs)

Persistent guest agent

By default, application-aware processing on Windows is performed by a non-persistent runtime process. Deploying a persistent agent removes security and port requirements of the runtime process injection.

□ Use persistent guest agent

61. On the Processing Settings page, click SQL if the VM is a Microsoft SQL Server VM.
62. Select Truncate logs (Prevents logs from growing forever) to truncate transaction logs after a successful backup.



Choose how this job should process Microsoft SQL Server transaction logs:

● Truncate logs (prevents logs from growing forever)

○ Do not truncate logs (requires simple recovery model)

○ Backup logs periodically (backed up logs will be truncated)

Backup logs every: 15 minutes

Retain log backups:

● Until the corresponding image-level backup is deleted

○ Keep only last 15 days of log backups

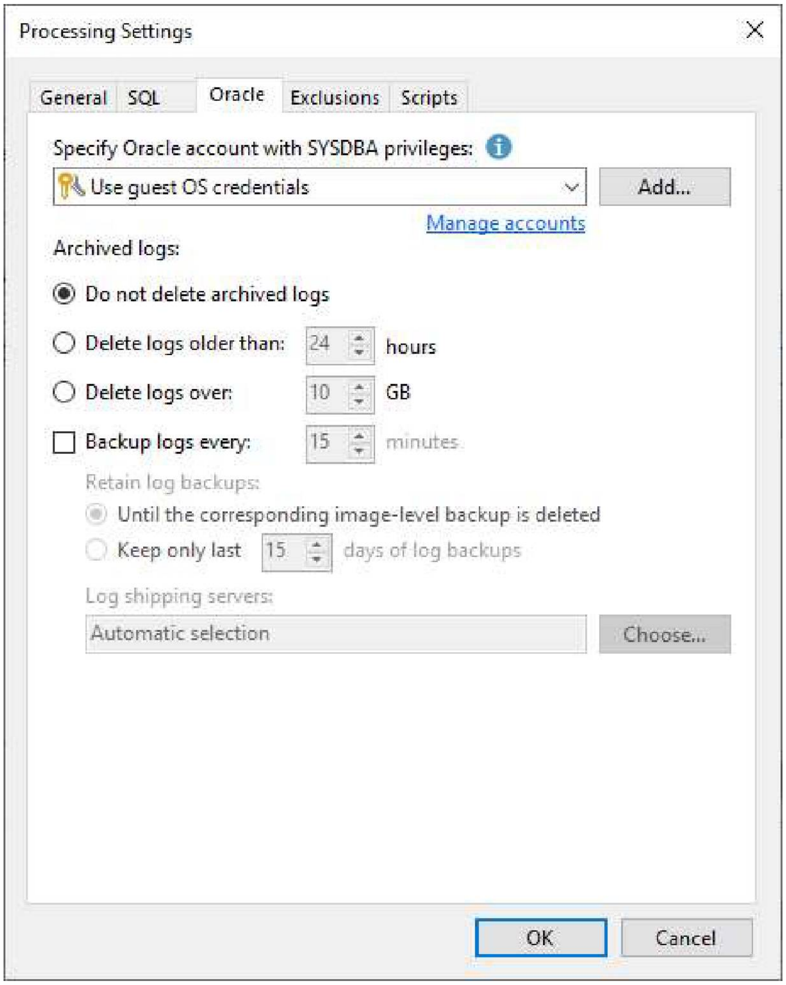
Log shipping servers:

Automatic selection

63. On the Processing Settings page, click Oracle if the VM is an Oracle Server.

64. Select a user account from the drop-down list.

65. Select Do not delete archived logs checkbox.



Processing Settings

General | SQL | Oracle | Exclusions | Scripts

Specify Oracle account with SYSDBA privileges:

Use guest OS credentials

Archived logs:

● Do not delete archived logs

○ Delete logs older than: 24 hours

○ Delete logs over: 10 GB

□ Backup logs every: 15 minutes

Retain log backups:

● Until the corresponding image-level backup is deleted

○ Keep only last 15 days of log backups

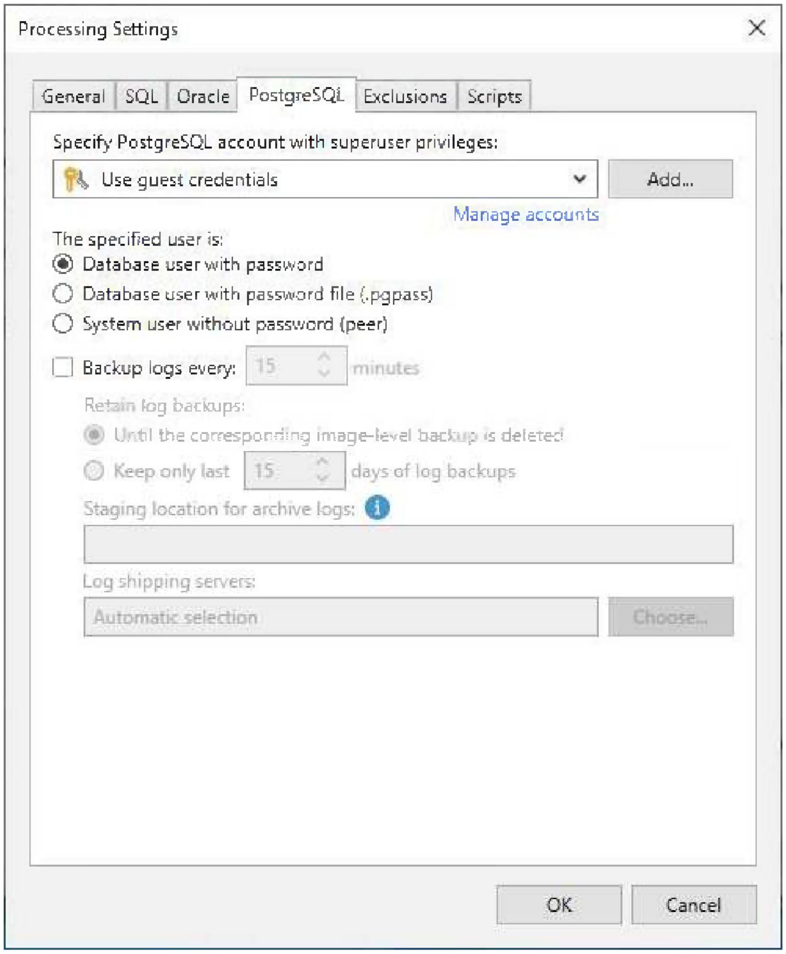
Log shipping servers:

Automatic selection

66. On the Processing Settings page, click PostgreSQL if the VM is a PostgreSQL Server VM.

67. Select a user account from the drop-down list.

68. Select Database user with password checkbox.



Specify PostgreSQL account with superuser privileges:

Use guest credentials

The specified user is:

● Database user with password

○ Database user with password file (.pgpass)

○ System user without password (peer)

□ Backup logs every: 15 minutes

Retain log backups:

● Until the corresponding image-level backup is deleted

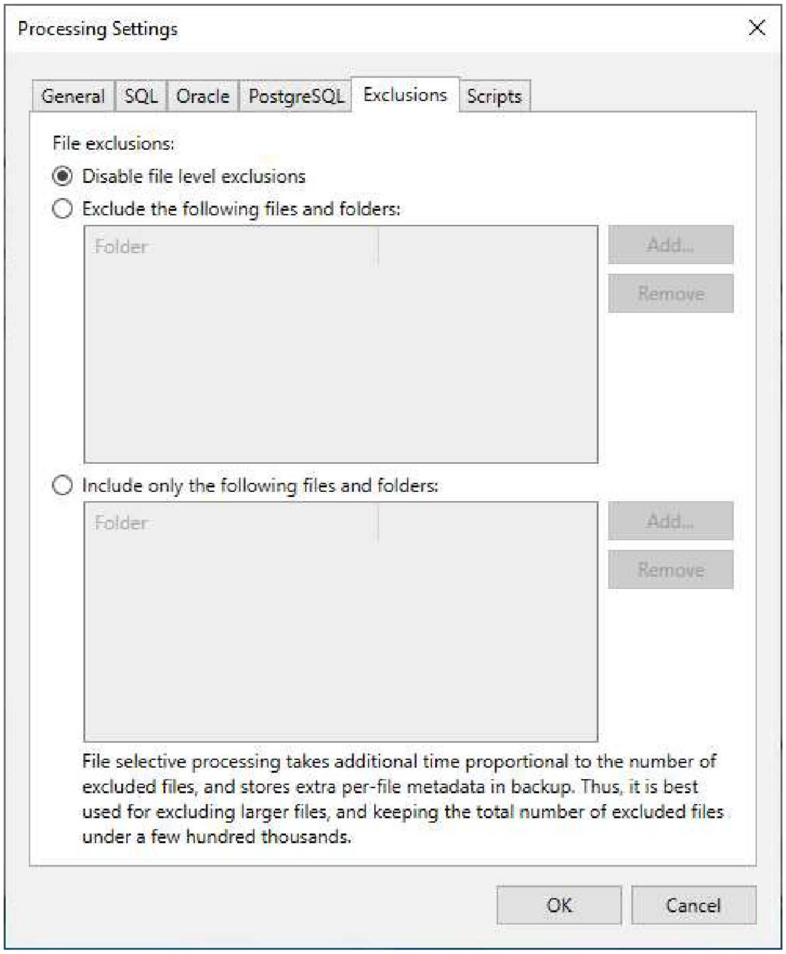
○ Keep only last 15 days of log backups

Staging location for archive logs:

Log shipping servers:

Automatic selection

69. On the Processing Settings page, click Exclusions and keep the default settings.



File exclusions:

● Disable file level exclusions

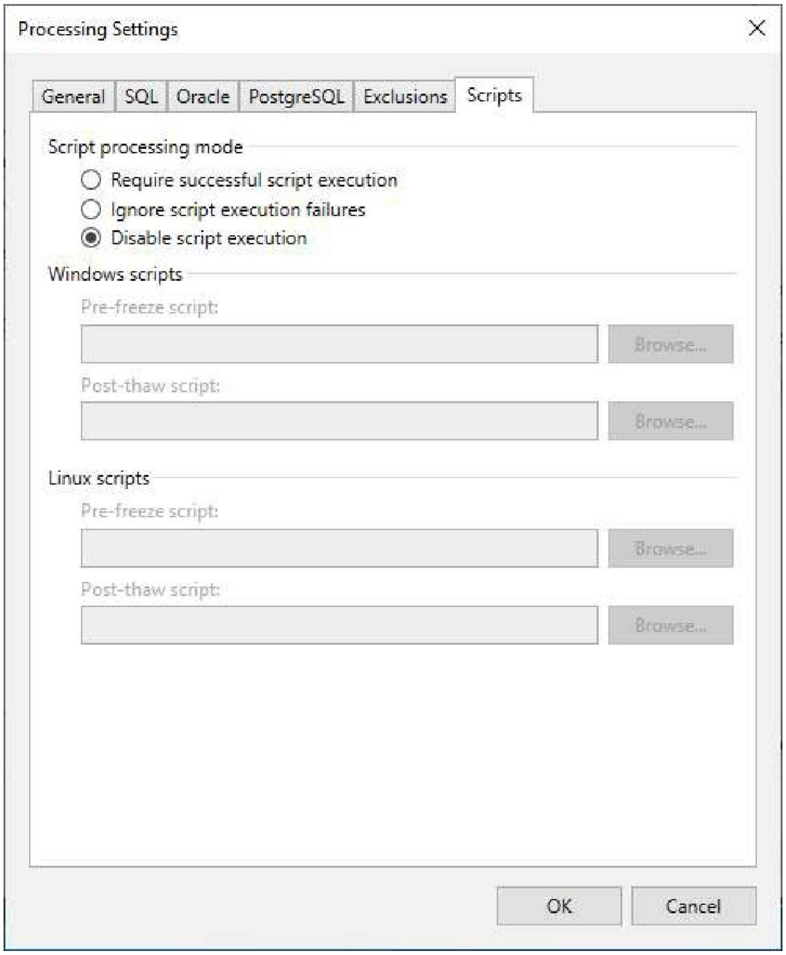
○ Exclude the following files and folders:

○ Include only the following files and folders:

File selective processing takes additional time proportional to the number of excluded files, and stores extra per-file metadata in backup. Thus, it is best used for excluding larger files, and keeping the total number of excluded files under a few hundred thousands.

70. On the Processing Settings page, click Scripts and keep the default settings.

71. Click OK.



Processing Settings

General | SQL | Oracle | PostgreSQL | Exclusions | Scripts

Script processing mode

○ Require successful script execution
○ Ignore script execution failures
● Disable script execution

Windows scripts

Pre-freeze script:

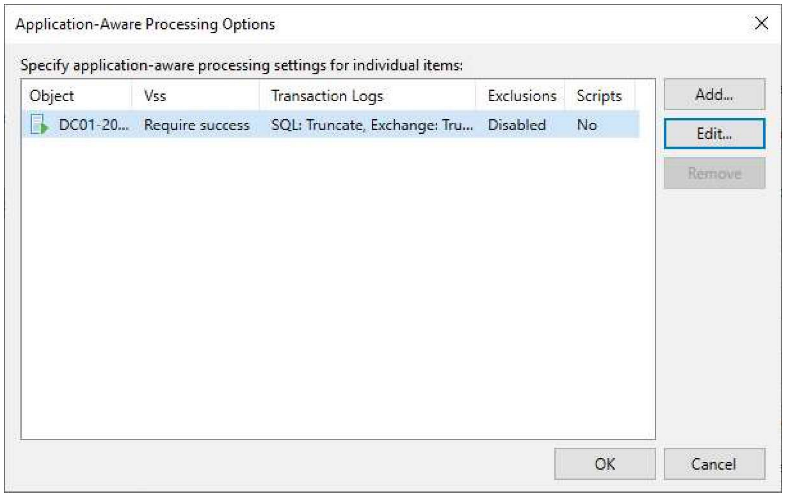
Post-thaw script:

Linux scripts

Pre-freeze script:

Post-thaw script:

72. On the Application-Aware Processing Options page, click OK.

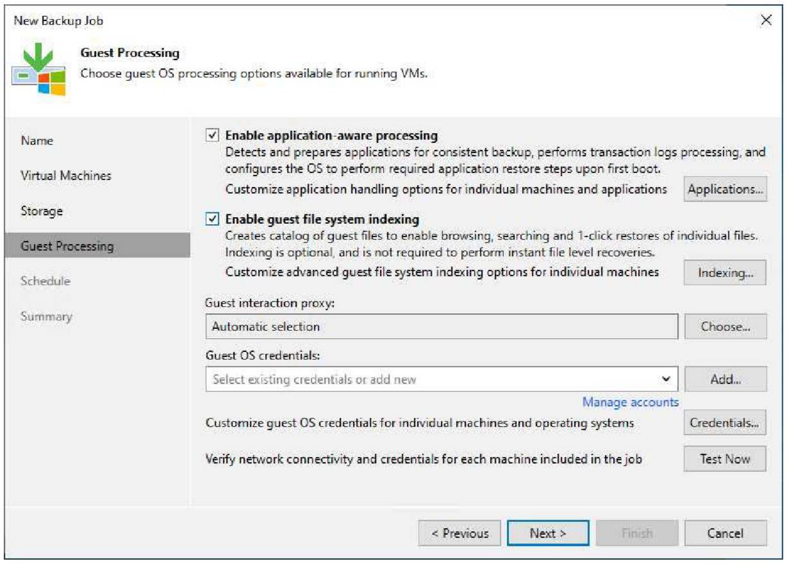


Application-Aware Processing Options

Specify application-aware processing settings for individual items:

Object	Vss	Transaction Logs	Exclusions	Scripts
DC01-20...	Require success	SQL: Truncate, Exchange: Tru...	Disabled	No

73. Select the Enable guest file system indexing checkbox and click Indexing.



New Backup Job

Guest Processing

Choose guest OS processing options available for running VMs.

☑ Enable application-aware processing

Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

Customize application handling options for individual machines and applications

☑ Enable guest file system indexing

Creates catalog of guest files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries.

Customize advanced guest file system indexing options for individual machines

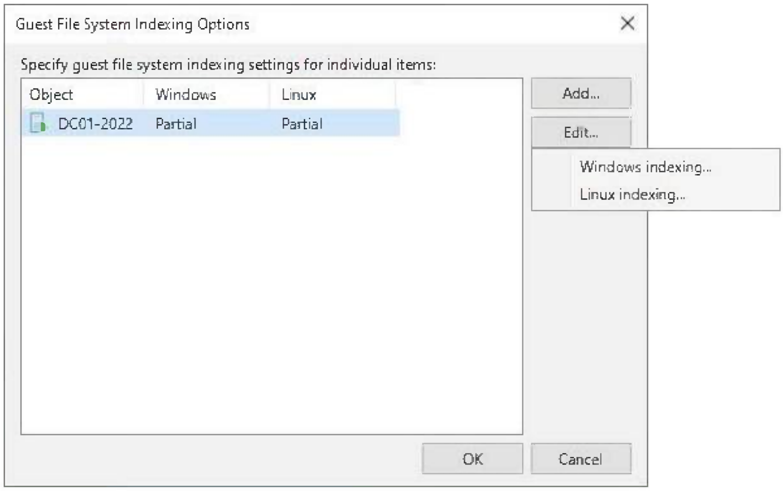
Guest interaction proxy: Automatic selection

Guest OS credentials: Select existing credentials or add new

Customize guest OS credentials for individual machines and operating systems

Verify network connectivity and credentials for each machine included in the job

74. On the Guest File System Indexing Options page, select the VM, click Edit and select Windows indexing.



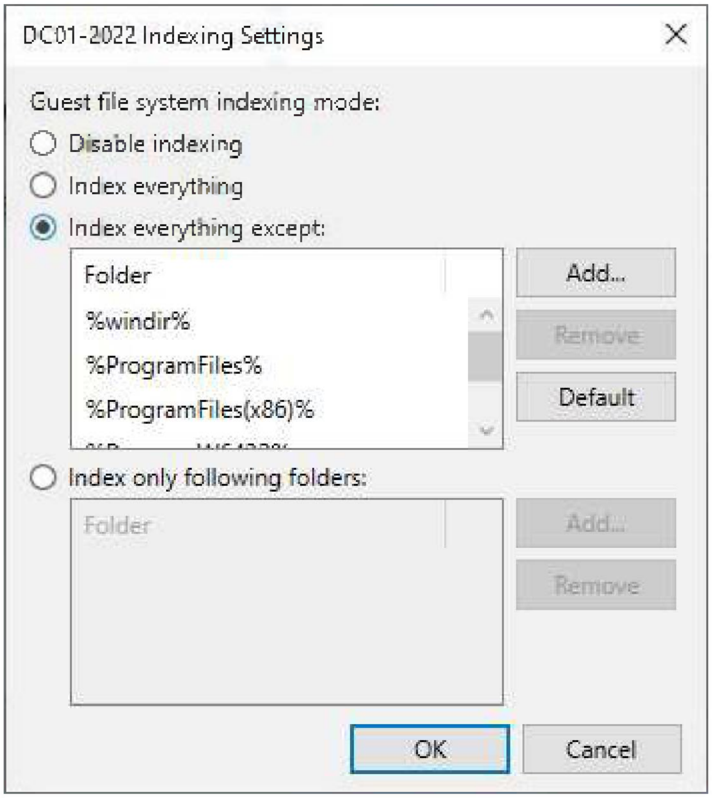
Guest File System Indexing Options

Specify guest file system indexing settings for individual items:

Object	Windows	Linux
DC01-2022	Partial	Partial

75. On the Guest file system indexing mode page, keep the default settings.

76. Click OK.



DC01-2022 Indexing Settings

Guest file system indexing mode:

○ Disable indexing

○ Index everything

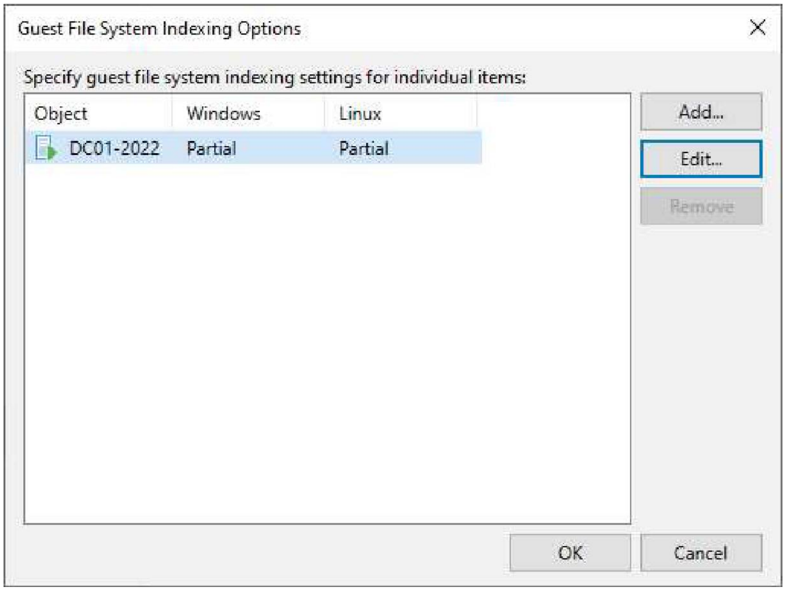
● Index everything except:

Folder
%windir%
%ProgramFiles%
%ProgramFiles(x86)%

○ Index only following folders:

Folder

77. Click OK on the Guest file system indexing mode page.

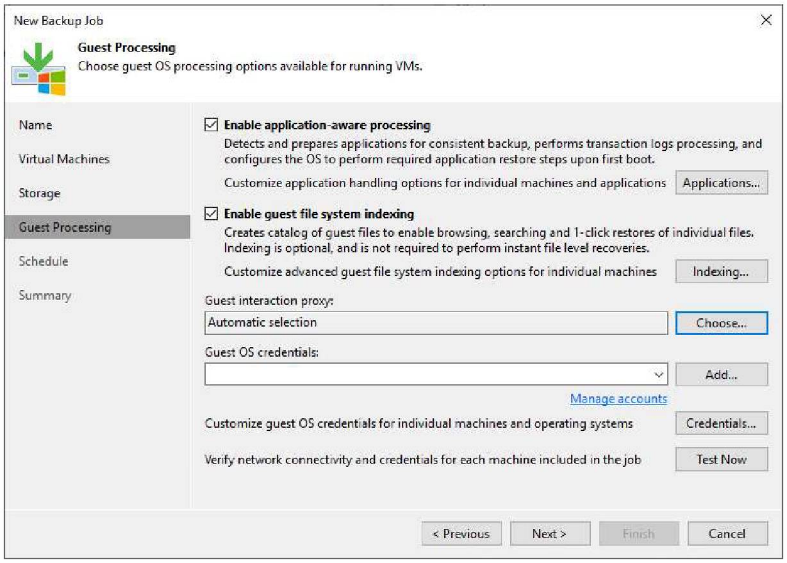


Guest File System Indexing Options

Specify guest file system indexing settings for individual items:

Object	Windows	Linux
DC01-2022	Partial	Partial

78. Click Choose on the Guest interaction proxy field on the Guest Processing page.



New Backup Job

Guest Processing

Choose guest OS processing options available for running VMs.

☑ **Enable application-aware processing**

Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

Customize application handling options for individual machines and applications

☑ **Enable guest file system indexing**

Creates catalog of guest files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries.

Customize advanced guest file system indexing options for individual machines

Guest interaction proxy: Automatic selection

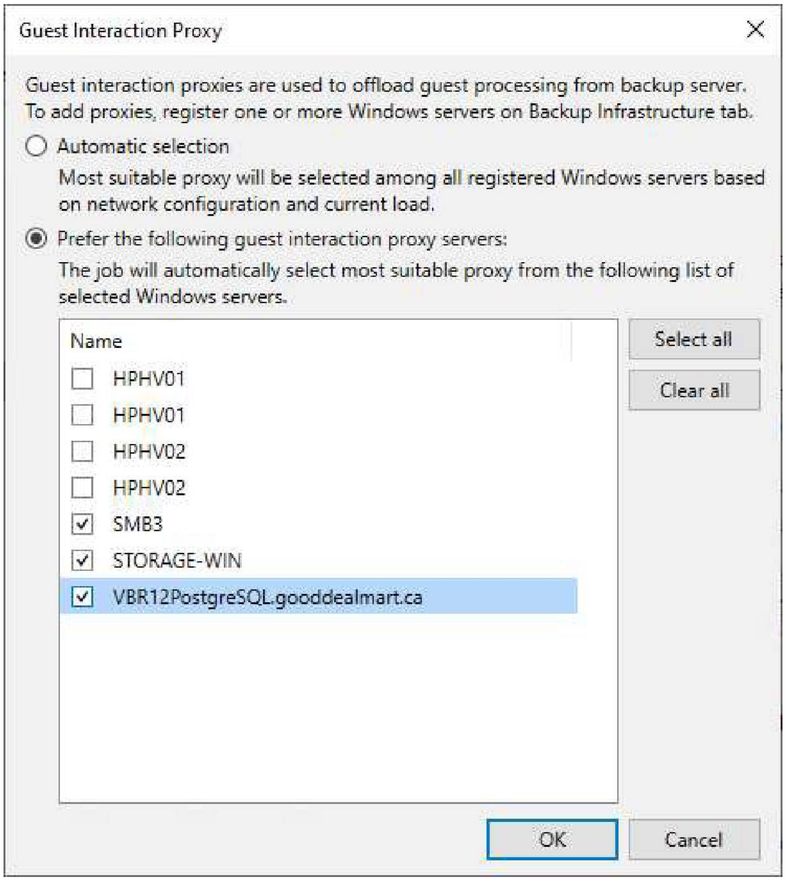
Guest OS credentials:

Customize guest OS credentials for individual machines and operating systems

Verify network connectivity and credentials for each machine included in the job

79. On the Guest Interaction Proxy page, select the domain member servers as the Guest Interaction proxy when you use gMSA as the guest OS credential.

80. Click OK.



Guest Interaction Proxy

Guest interaction proxies are used to offload guest processing from backup server. To add proxies, register one or more Windows servers on Backup Infrastructure tab.

○ Automatic selection

Most suitable proxy will be selected among all registered Windows servers based on network configuration and current load.

● Prefer the following guest interaction proxy servers:

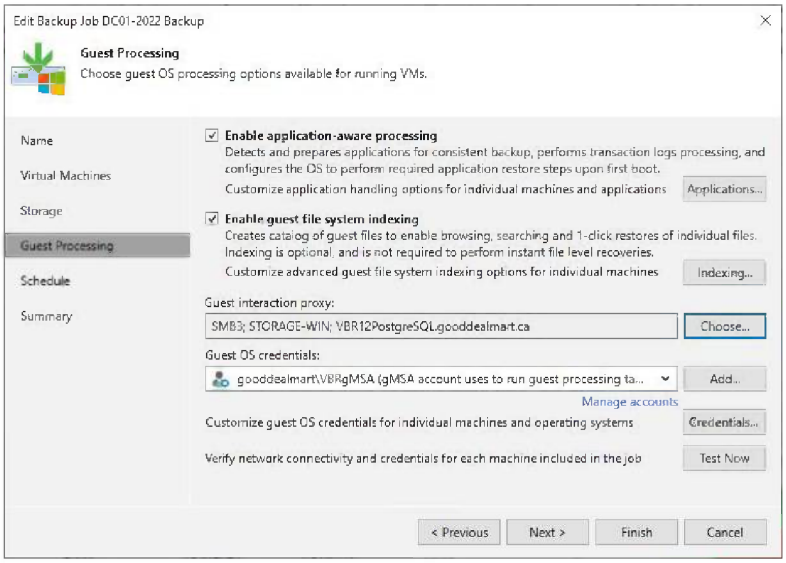
The job will automatically select most suitable proxy from the following list of selected Windows servers.

Name
□ HPHV01
□ HPHV01
□ HPHV02
□ HPHV02
☑ SMB3
☑ STORAGE-WIN
☑ VBR12PostgreSQL.gooddealmart.ca

81. Choose a user account on the Guest Processing page with sufficient permissions from the Guest OS credentials drop-down list.

82. If you have multiple VMs at the same job, click Credentials to Customize guest OS credentials for individual machines and operating systems.

83. On the Guest Processing page, click Test Now to verify network connectivity and credentials for each machine included in the job.



Edit Backup Job DC01-2022 Backup

Guest Processing

Choose guest OS processing options available for running VMs.

☑ **Enable application-aware processing**

Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

Customize application handling options for individual machines and applications

☑ **Enable guest file system indexing**

Creates catalog of guest files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries.

Customize advanced guest file system indexing options for individual machines

Guest interaction proxy:

SMB3; STORAGE-WIN; VBR12PostgreSQL.gooddealmart.ca

Guest OS credentials:

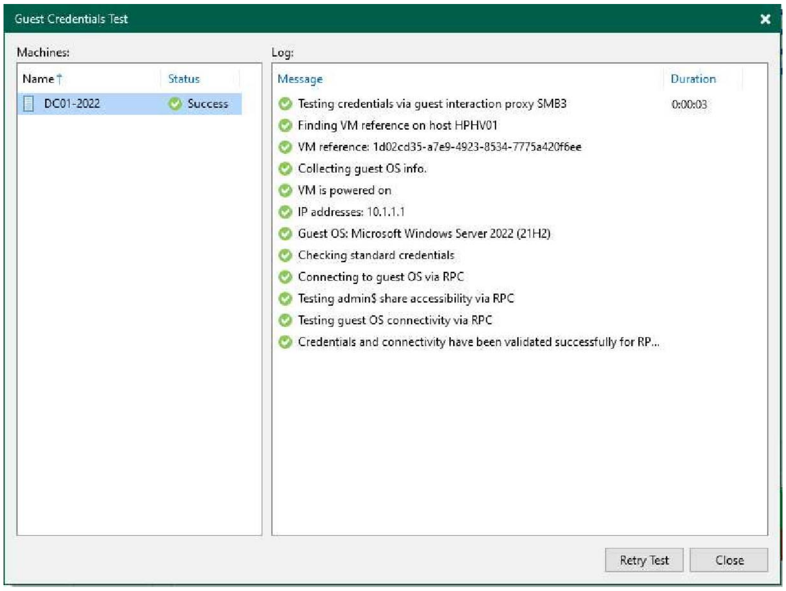
gooddealmart\VBRgMSA (gMSA account uses to run guest processing ta...

Customize guest OS credentials for individual machines and operating systems

Verify network connectivity and credentials for each machine included in the job

84. On the Guest Credentials Test page, ensure verification success for each machine.

85. Click Close.



Guest Credentials Test

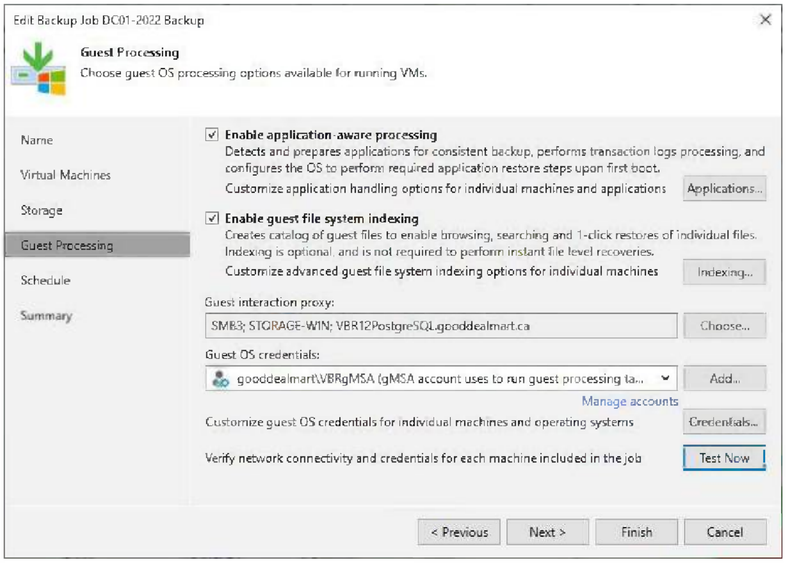
Machines:

Name	Status
DC01-2022	Success

Log:

```
Message                                                                  Duration
Testing credentials via guest interaction proxy SMB3                     0:00:03
Finding VM reference on host HPHV01
VM reference: 1d02cd35-a7e9-4923-8534-7775a420f6ee
Collecting guest OS info.
VM is powered on
IP addresses: 10.1.1.1
Guest OS: Microsoft Windows Server 2022 (21H2)
Checking standard credentials
Connecting to guest OS via RPC
Testing admin$ share accessibility via RPC
Testing guest OS connectivity via RPC
Credentials and connectivity have been validated successfully for RP...
```

86. Click Next on the Guest Processing page.



Edit Backup Job DC01-2022 Backup

Guest Processing

Choose guest OS processing options available for running VMs.

☑ Enable application-aware processing

Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

Customize application handling options for individual machines and applications

☑ Enable guest file system indexing

Creates catalog of guest files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries.

Customize advanced guest file system indexing options for individual machines

Guest interaction proxy: SMB3; STORAGE-WIN; VBR12PostgreSQL.gooddealmart.ca

Guest OS credentials: gooddealmart\VBRgMSA (gMSA account uses to run guest processing ta...

Customize guest OS credentials for individual machines and operating systems

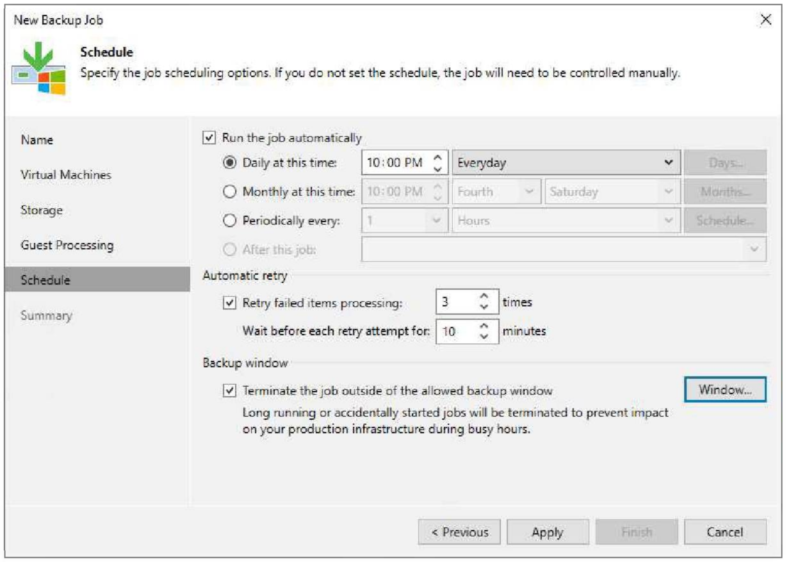
Verify network connectivity and credentials for each machine included in the job

87. Select Run the job automatically checkbox on the Schedule page and select your specified schedule.

88. Define whether Veeam Backup & Replication should retry the backup job if it fails in the Automatic retry section.

89. Define the time interval the backup job must complete in the Backup window section. The backup window ensures that the job does not overlap with production hours and that there is no unnecessary overhead on the production environment.

90. Click Apply.



New Backup Job

Schedule

Specify the job scheduling options. If you do not set the schedule, the job will need to be controlled manually.

☑ Run the job automatically

● Daily at this time: 10:00 PM Everyday

○ Monthly at this time: 10:00 PM Fourth Saturday

○ Periodically every: 1 Hours

○ After this job:

Automatic retry

☑ Retry failed items processing: 3 times

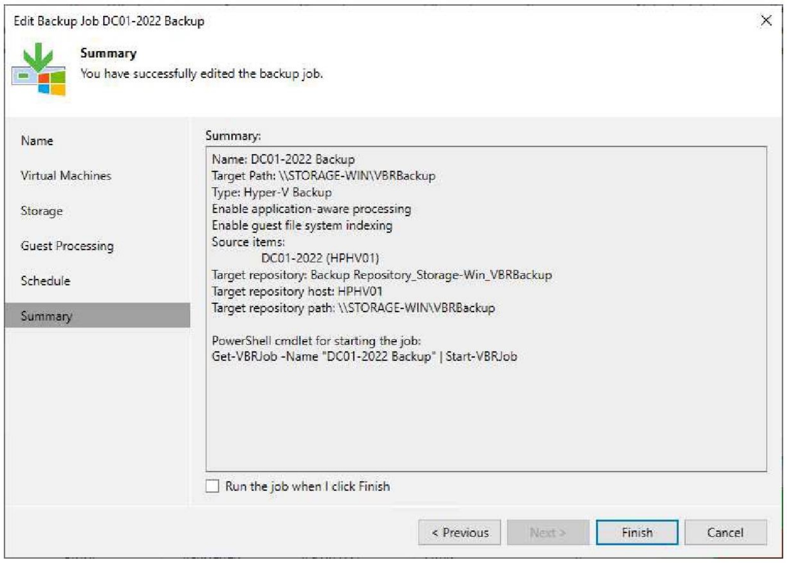
Wait before each retry attempt for: 10 minutes

Backup window

☑ Terminate the job outside of the allowed backup window

Long running or accidentally started jobs will be terminated to prevent impact on your production infrastructure during busy hours.

91. Click Finish on the Summary page.

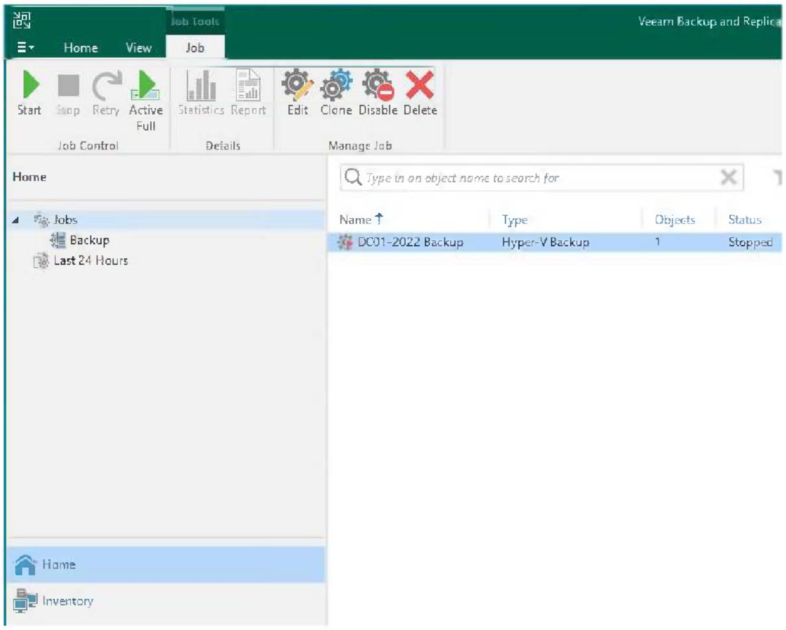


Summary:

```
Name: DC01-2022 Backup
Target Path: \\STORAGE-WIN\VBRBackup
Type: Hyper-V Backup
Enable application-aware processing
Enable guest file system indexing
Source items:
        DC01-2022 (HPHV01)
Target repository: Backup Repository_Storage-Win_VBRBackup
Target repository host: HPHV01
Target repository path: \\STORAGE-WIN\VBRBackup

PowerShell cmdlet for starting the job:
Get-VBRJob -Name "DC01-2022 Backup" | Start-VBRJob
```

□ Run the job when I click Finish

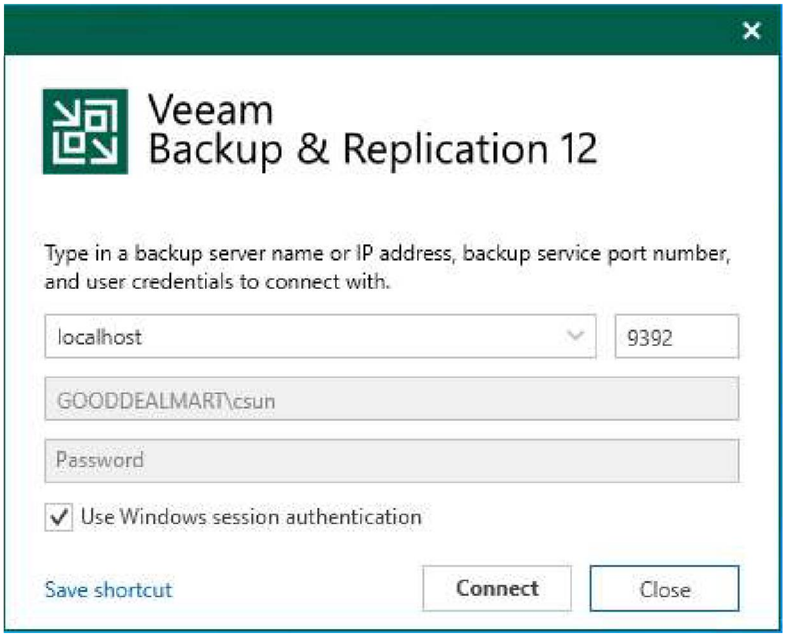
92. Verify that the backup job has been added.



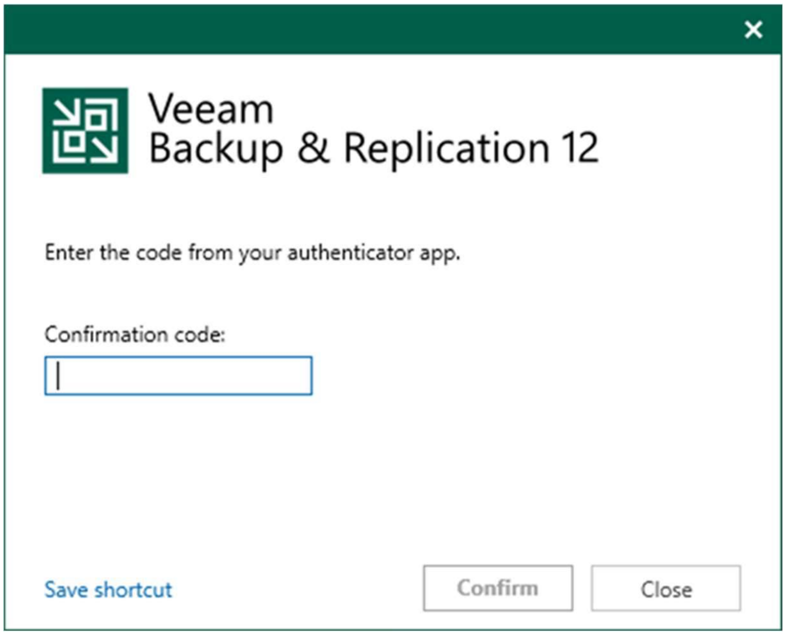
Name ↑	Type	Objects	Status
DC01-2022 Backup	Hyper-V Backup	1	Stopped

Create an Immutable Backup job to backup the specified VMs

Immutable Backup is a Veeam Backup & Replication feature that protects against ransomware attacks by preventing malicious software from modifying or deleting backup data.
Immutable backup means that once data is written to a backup repository, it cannot be modified, overwritten, or deleted until a specified retention period has passed. This can prevent ransomware from corrupting or encrypting backup data because the malware cannot modify or delete the backup files.

Instructions	Screenshot (if applicable)
1. Log in to the Veeam Backup and replication manager server. 2. Open the Veeam Backup & Replication Console and click Connect.	 Veeam Backup & Replication 12 Type in a backup server name or IP address, backup service port number, and user credentials to connect with. localhost 9392 GOODDEALMART\csun Password ☑ Use Windows session authentication Save shortcut Connect Close

3. Enter the MFA Confirmation code and click Confirm.



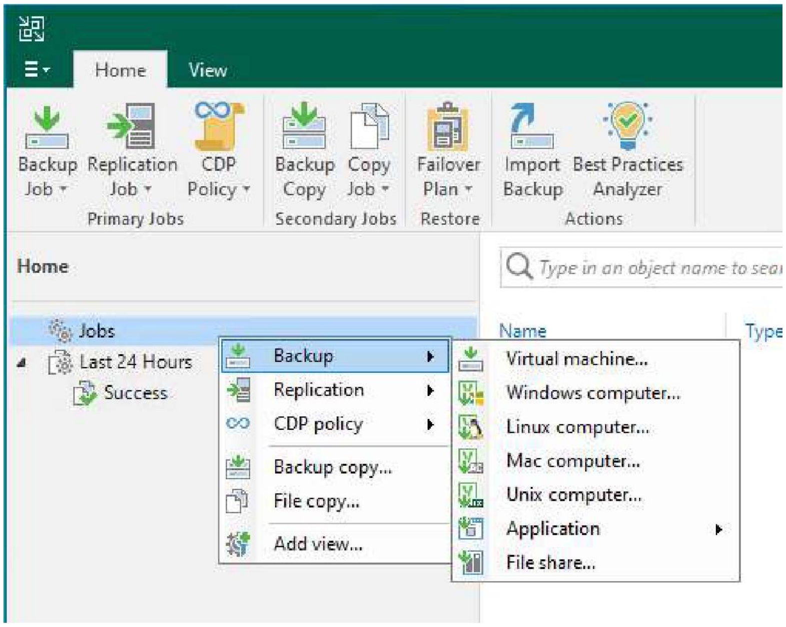
Veeam Backup & Replication 12

Enter the code from your authenticator app.

Confirmation code:

4. Select Jobs on the Home page and right-click Jobs.

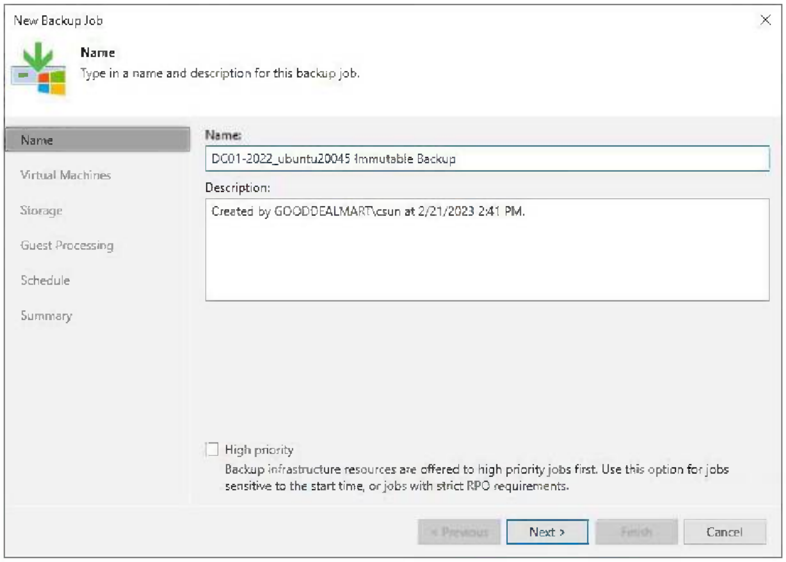
5. Select Backup and click Virtual machine.



6. On the Name page, enter a name for the backup job in the Name field.

7. Give a brief description in the Description field for the future.

8. Click Next.



Name

Type in a name and description for this backup job.

Name:

DC01-2022_ubuntu20045 Immutable Backup

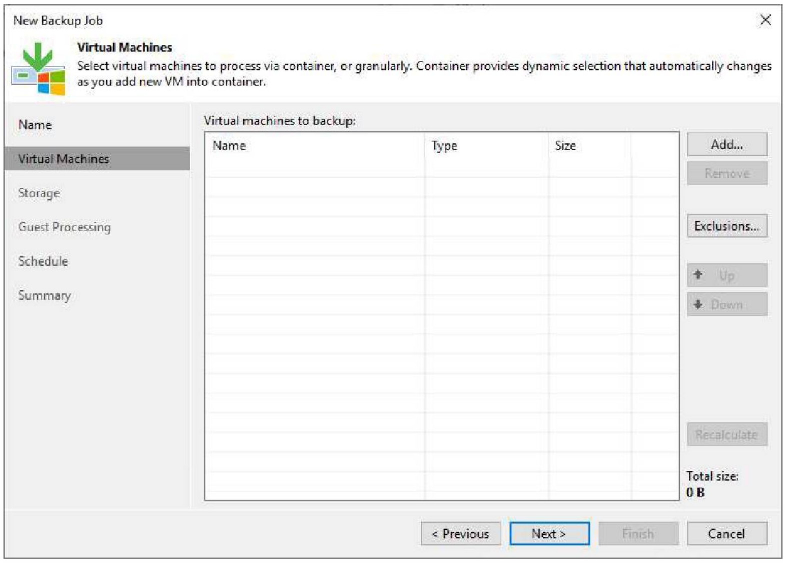
Description:

Created by GOODDEALMART\csun at 2/21/2023 2:41 PM.

□ High priority

Backup infrastructure resources are offered to high priority jobs first. Use this option for jobs sensitive to the start time, or jobs with strict RPO requirements.

9. Click Add on the Virtual Machines page.



Virtual Machines

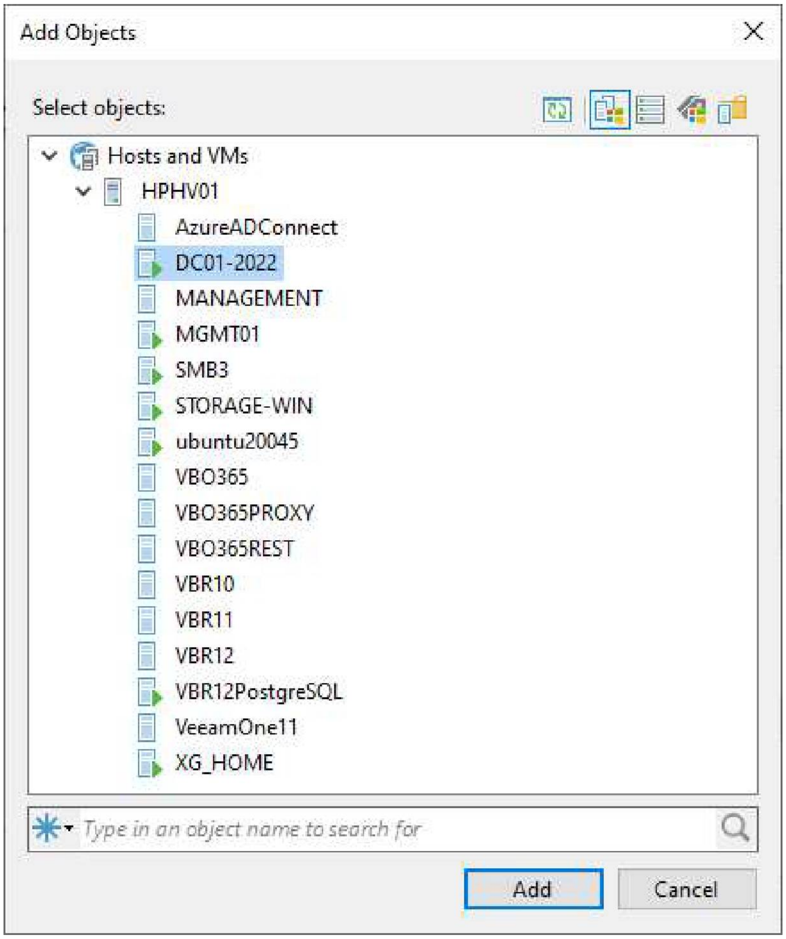
Select virtual machines to process via container, or granularly. Container provides dynamic selection that automatically changes as you add new VM into container.

Virtual machines to backup:

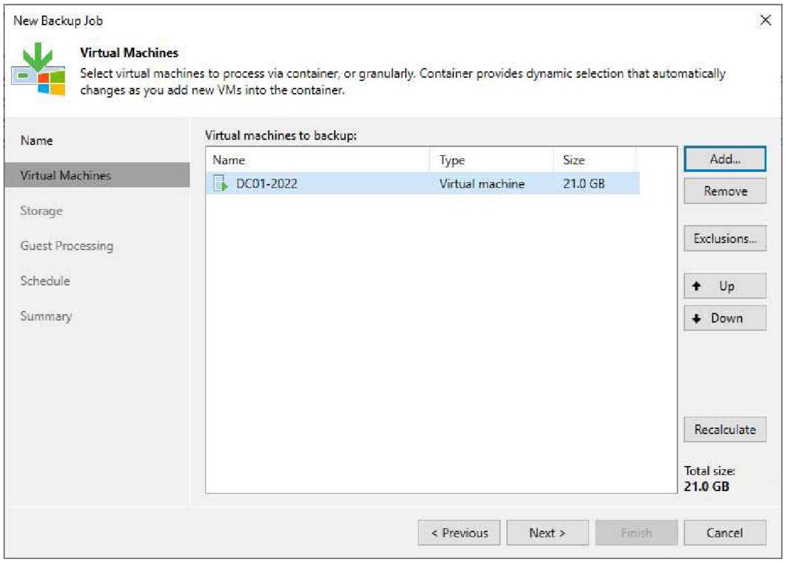
Total size:
0 B

10. Select the VM from the Select objects list on the Add Objects page and click Add.

11. If you have multiple VMS that needs to back up in the same backup job, you can repeat the step to add them.



12. Click Next on the Virtual Machines page.



New Backup Job

Virtual Machines

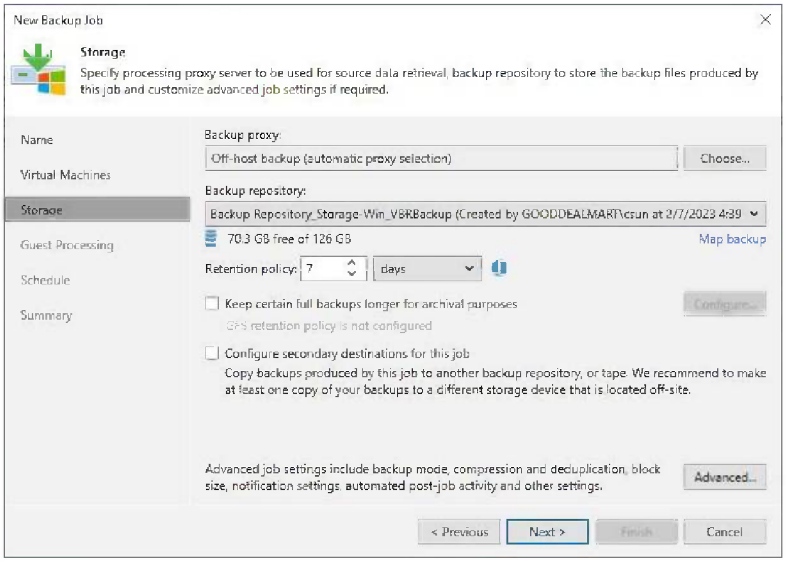
Select virtual machines to process via container, or granularly. Container provides dynamic selection that automatically changes as you add new VMs into the container.

Virtual machines to backup:

Name	Type	Size
DC01-2022	Virtual machine	21.0 GB

Total size: 21.0 GB

13. On the Storage page, click Choose to select a backup proxy if you don't want to use the default Off-host backup (automatic proxy selection) setting.



New Backup Job

Storage

Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Backup proxy: Off-host backup (automatic proxy selection)

Backup repository: Backup Repository_Storage-Win_VBRBackup (Created by GOODDEALMART\csun at 2/7/2023 4:39

70.3 GB free of 126 GB

Retention policy: 7 days

☐ Keep certain full backups longer for archival purposes

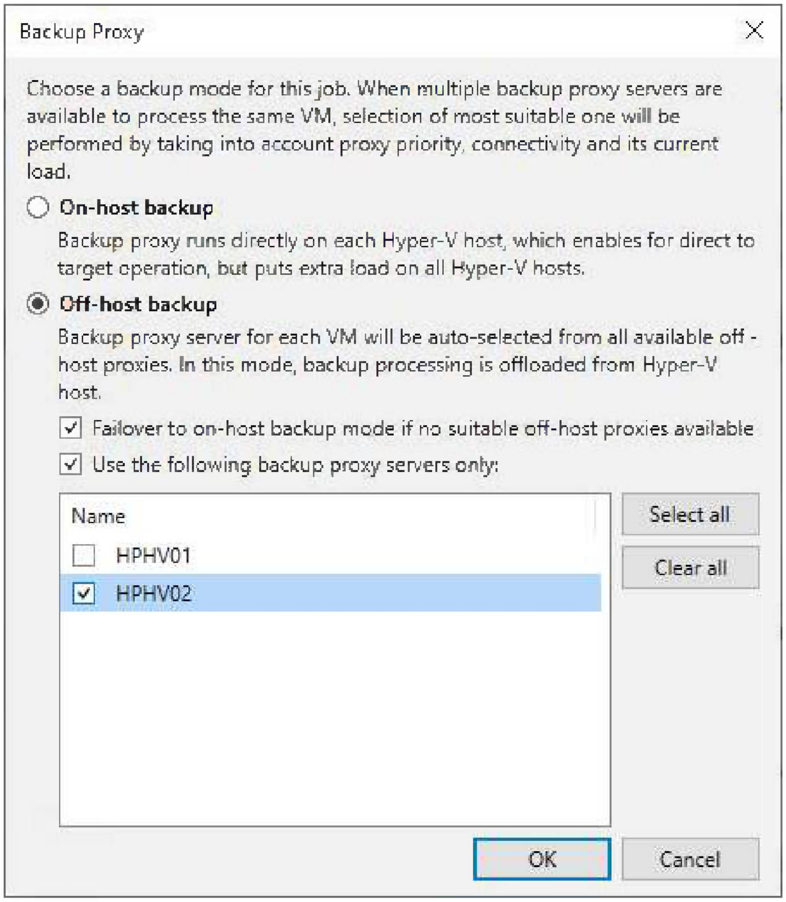
GFS retention policy is not configured

☐ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

14. On the Backup Proxy page, if you select On-host backup mode, the source Microsoft HyperV host will serve as both the source host and the backup proxy. In this mode, Veeam Data Mover runs directly on the source host, which speeds up data retrieval but places additional strain on the host.



Backup Proxy

Choose a backup mode for this job. When multiple backup proxy servers are available to process the same VM, selection of most suitable one will be performed by taking into account proxy priority, connectivity and its current load.

○ **On-host backup**

Backup proxy runs directly on each Hyper-V host, which enables for direct to target operation, but puts extra load on all Hyper-V hosts.

● **Off-host backup**

Backup proxy server for each VM will be auto-selected from all available off - host proxies. In this mode, backup processing is offloaded from Hyper-V host.

☑ Failover to on-host backup mode if no suitable off-host proxies available

☑ Use the following backup proxy servers only:

Name
□ HPHV01
☑ HPHV02

15. If you select Off-host backup mode, Veeam Data Mover will run on a dedicated off-host backup proxy. All backup processing operations from the source host are routed to the off-host backup proxy in this model.

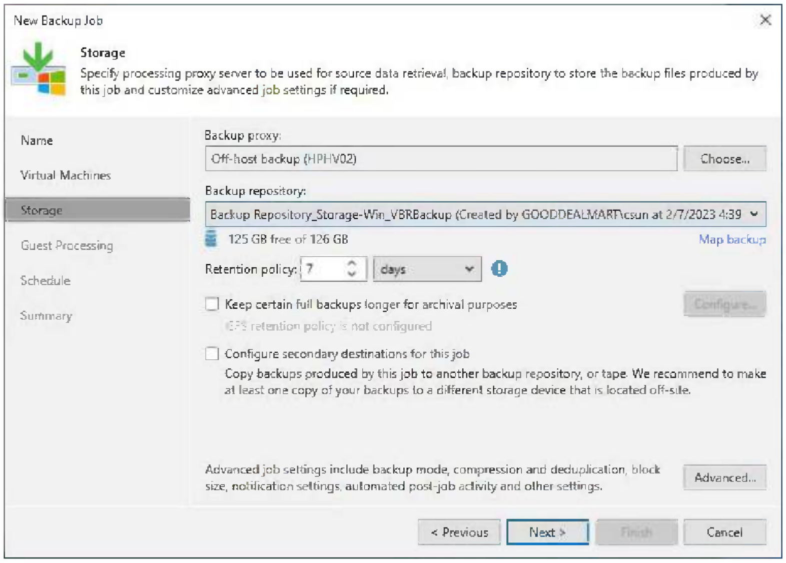
16. If the off-host backup mode is selected for the job, but no off-host backup proxies are available when the job begins, Veeam Backup & Replication will transition to on-host backup mode.

17. You unselect the Failover to on-host backup mode if no suitable off-host

proxies are available in the checkbox. Still, the job will fail to start if off-host backup proxies are unavailable or configured properly.

18. Click OK.

19. Select the Hardened backup repository from the Backup repository drop-down list.



New Backup Job

Storage

Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Backup proxy: Off-host backup (HPHV02)

Backup repository: Backup Repository_Storage-Win_VBRBackup (Created by GOODDEALMART\csun at 2/7/2023 4:39

125 GB free of 126 GB

Retention policy: 7 days

□ Keep certain full backups longer for archival purposes

GFS retention policy is not configured

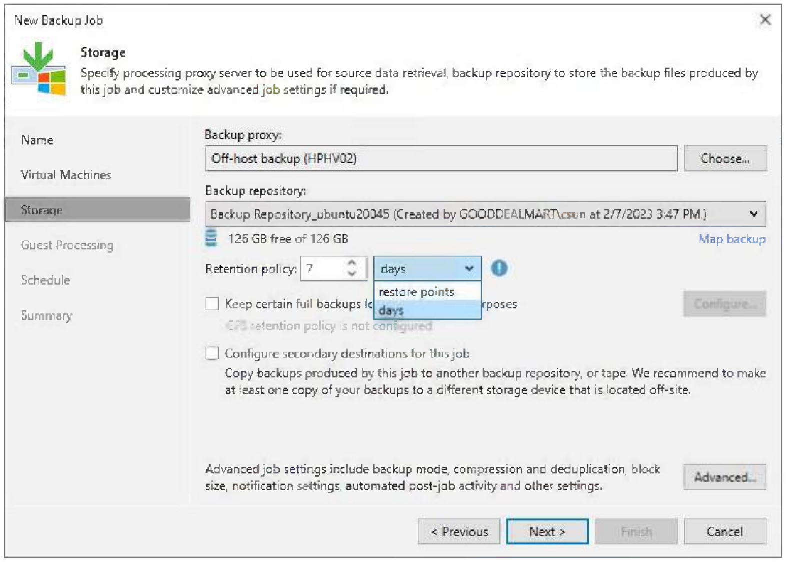
□ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

20. Set the retention policy settings for restore points in the Retention Policy field.

21. Select days or restore points from the drop-down list.



New Backup Job

Storage

Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Name
Virtual Machines
Storage
Guest Processing
Schedule
Summary

Backup proxy: Off-host backup (HPHV02)

Backup repository: Backup Repository_ubuntu20045 (Created by GOODDEALMART\csun at 2/7/2023 3:47 PM.)

126 GB free of 126 GB

Retention policy: 7 days

restore points
days

☐ Keep certain full backups lo… rposes

GFS retention policy is not configured

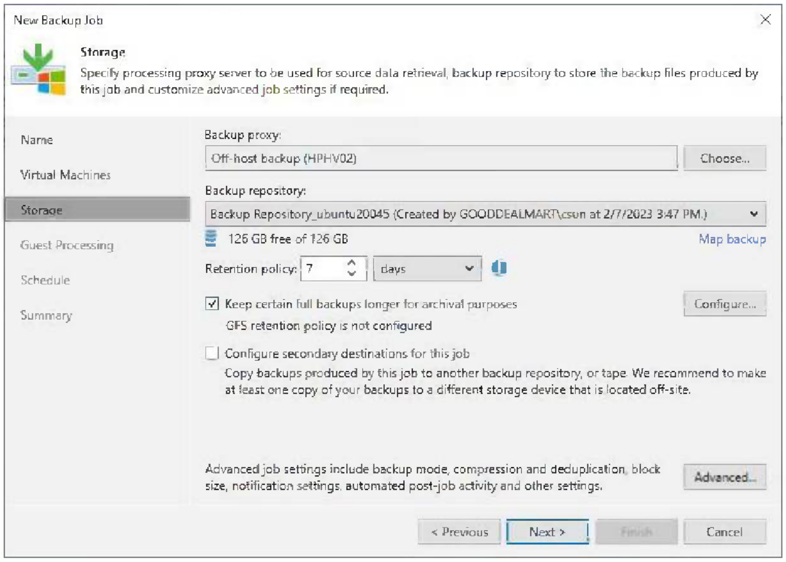
☐ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

22. You can configure GFS retention policy settings for the backup job to ignore the short-term retention policy for some full backups and store them for long-term archiving.

23. Select the Keep certain full backups for longer for archival purposes checkbox and click Configure.



New Backup Job

Storage

Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Name
Virtual Machines
Storage
Guest Processing
Schedule
Summary

Backup proxy: Off-host backup (HPHV02)

Backup repository: Backup Repository_ubuntu20045 (Created by GOODDEALMART\csun at 2/7/2023 3:47 PM.)

126 GB free of 126 GB

Retention policy: 7 days

☑ Keep certain full backups longer for archival purposes

GFS retention policy is not configured

☐ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

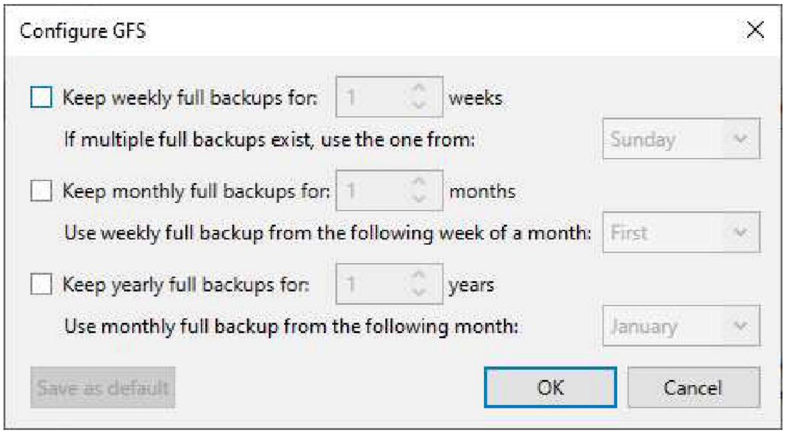
Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

24. Select the Keep weekly full backups for check box, and specify the number of weeks you want to prevent restore points from being modified and deleted.

25. Select the Keep monthly full backups for check box, and specify the months you want to prevent restore points from being modified and deleted.

26. Select the Keep yearly full backups for check box, and specify the years you want to prevent restore points from being modified and deleted.

27. Click OK.



Configure GFS

□ Keep weekly full backups for: 1 weeks

If multiple full backups exist, use the one from: Sunday

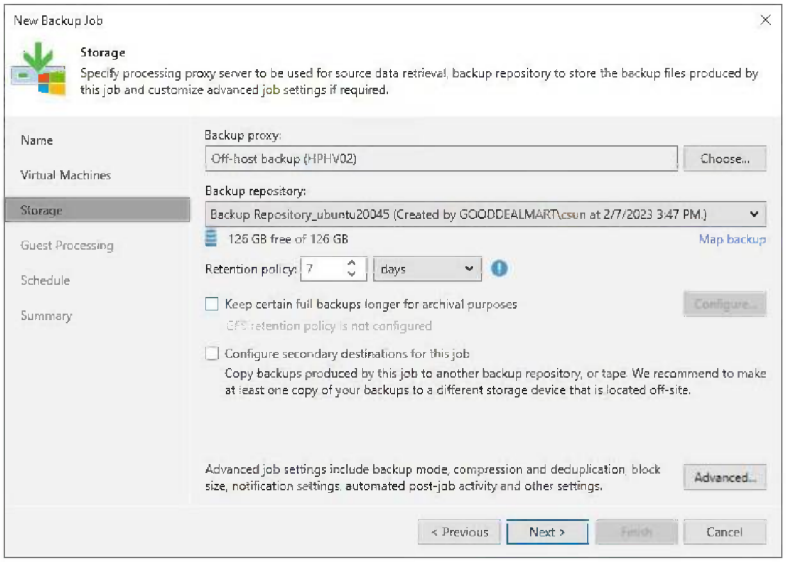
□ Keep monthly full backups for: 1 months

Use weekly full backup from the following week of a month: First

□ Keep yearly full backups for: 1 years

Use monthly full backup from the following month: January

28. On the Storage page, click Advanced.



New Backup Job

Storage

Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Backup proxy: Off-host backup (HPHV02)

Backup repository: Backup Repository_ubuntu20045 (Created by GOODDEALMART\csun at 2/7/2023 3:47 PM.)

126 GB free of 126 GB

Retention policy: 7 days

□ Keep certain full backups longer for archival purposes

GFS retention policy is not configured

□ Configure secondary destinations for this job

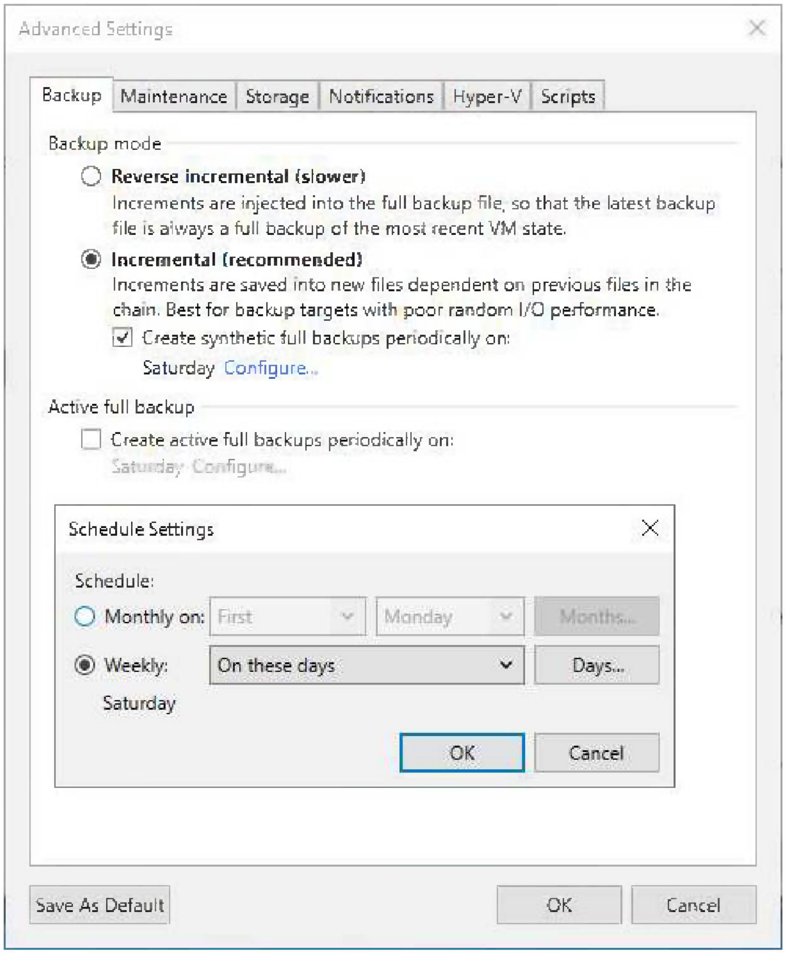
Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

29. On the Backup page, select Incremental (recommended).

30. Select create synthetic full backups periodically or active full backups periodically checkbox.

31. Click Configure to schedule full backups periodically and click OK.



Advanced Settings

Backup mode

○ **Reverse incremental (slower)**
Increments are injected into the full backup file, so that the latest backup file is always a full backup of the most recent VM state.

● **Incremental (recommended)**
Increments are saved into new files dependent on previous files in the chain. Best for backup targets with poor random I/O performance.

☑ Create synthetic full backups periodically on:
Saturday Configure...

Active full backup

□ Create active full backups periodically on:
Saturday Configure...

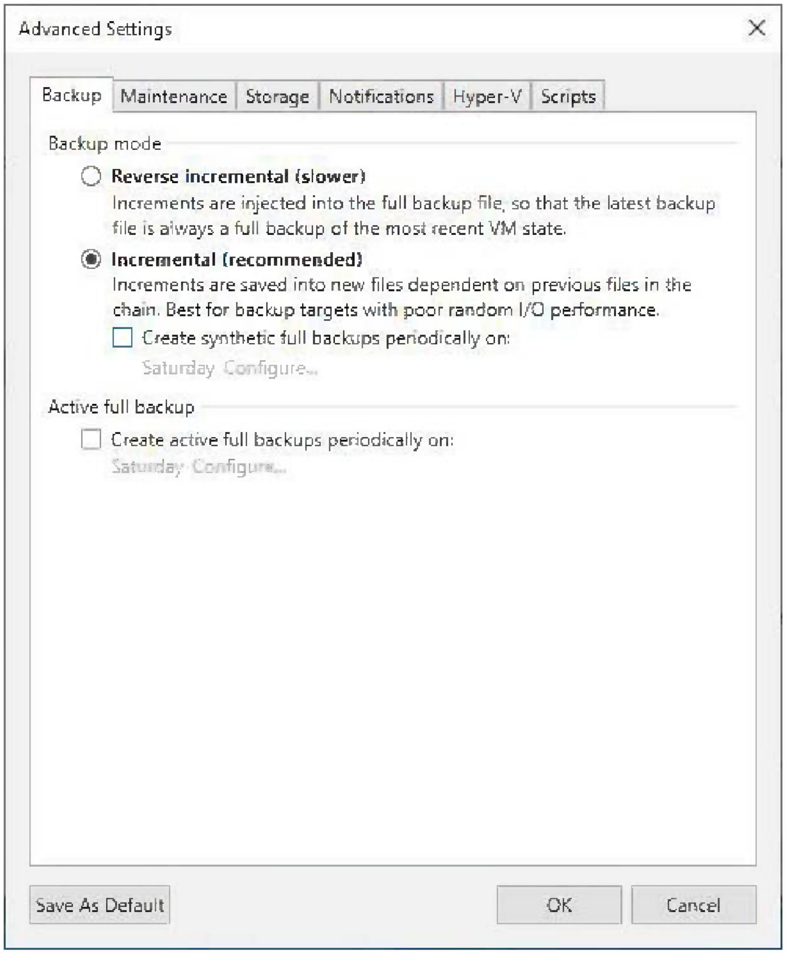
Schedule Settings

Schedule:

○ Monthly on: First Monday Months...

● Weekly: On these days Days...
Saturday

32. Select Incremental and disable synthetic full or active full backups to create a forever forward incremental backup chain if needed.



Advanced Settings

Backup | Maintenance | Storage | Notifications | Hyper-V | Scripts

Backup mode

○ **Reverse incremental (slower)**
Increments are injected into the full backup file, so that the latest backup file is always a full backup of the most recent VM state.

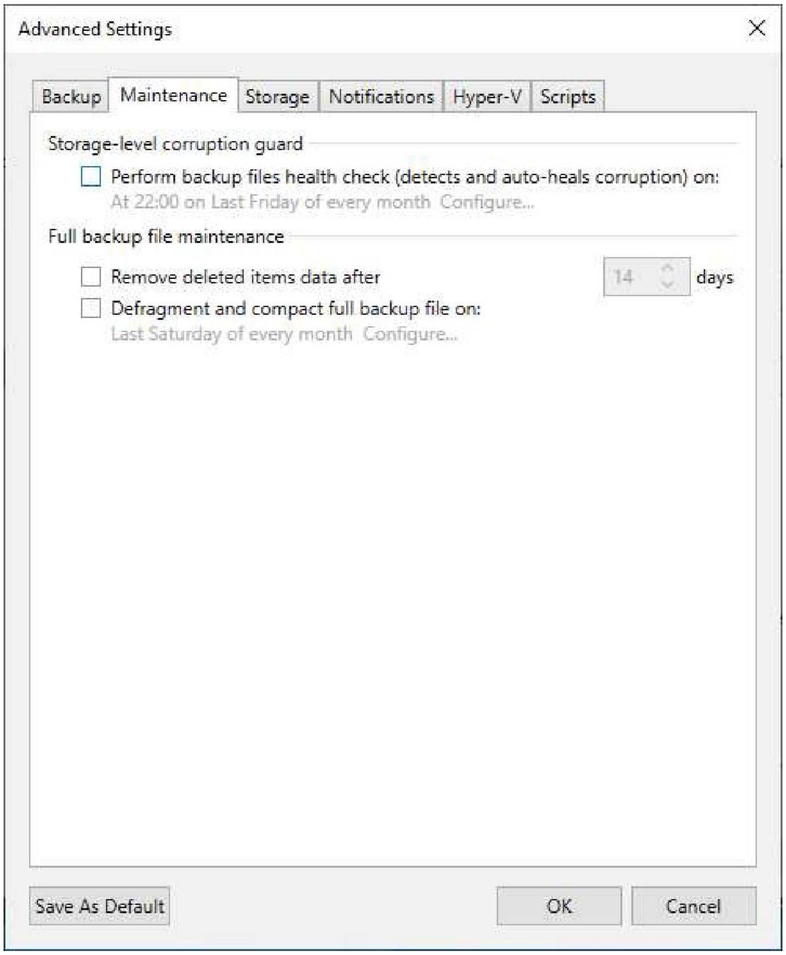
● **Incremental (recommended)**
Increments are saved into new files dependent on previous files in the chain. Best for backup targets with poor random I/O performance.

□ Create synthetic full backups periodically on:
Saturday Configure...

Active full backup

□ Create active full backups periodically on:
Saturday Configure...

33. On the Advanced Settings, select Maintenance.



Advanced Settings

Storage-level corruption guard

□ Perform backup files health check (detects and auto-heals corruption) on:
At 22:00 on Last Friday of every month Configure...

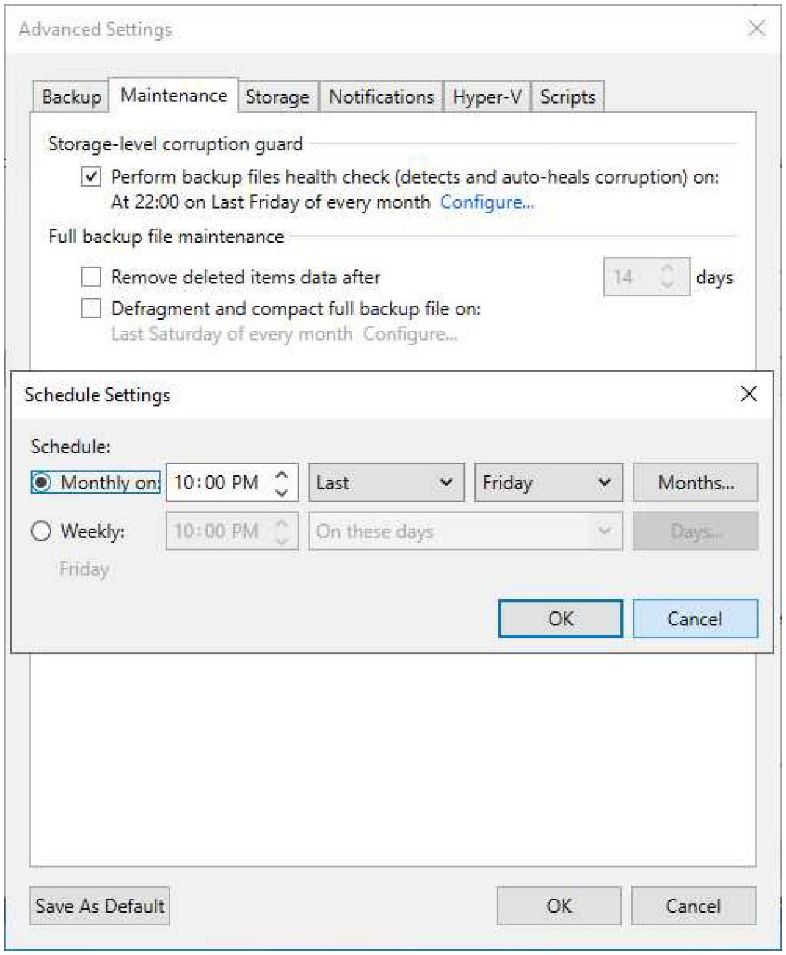
Full backup file maintenance

□ Remove deleted items data after 14 days

□ Defragment and compact full backup file on:
Last Saturday of every month Configure...

34. To regularly perform a health check on the backup chain's most recent restore point, select the Perform backup files health check (detects and auto-heals corruption) checkbox in the Storage-level corruption guard section.

35. Click Configure to set a timetable for the health check.



Storage-level corruption guard

☑ Perform backup files health check (detects and auto-heals corruption) on:
At 22:00 on Last Friday of every month Configure...

Full backup file maintenance

☐ Remove deleted items data after 14 days

☐ Defragment and compact full backup file on:
Last Saturday of every month Configure...

Schedule Settings

Schedule:

● Monthly on: 10:00 PM Last Friday Months...

○ Weekly: 10:00 PM On these days Days...
Friday

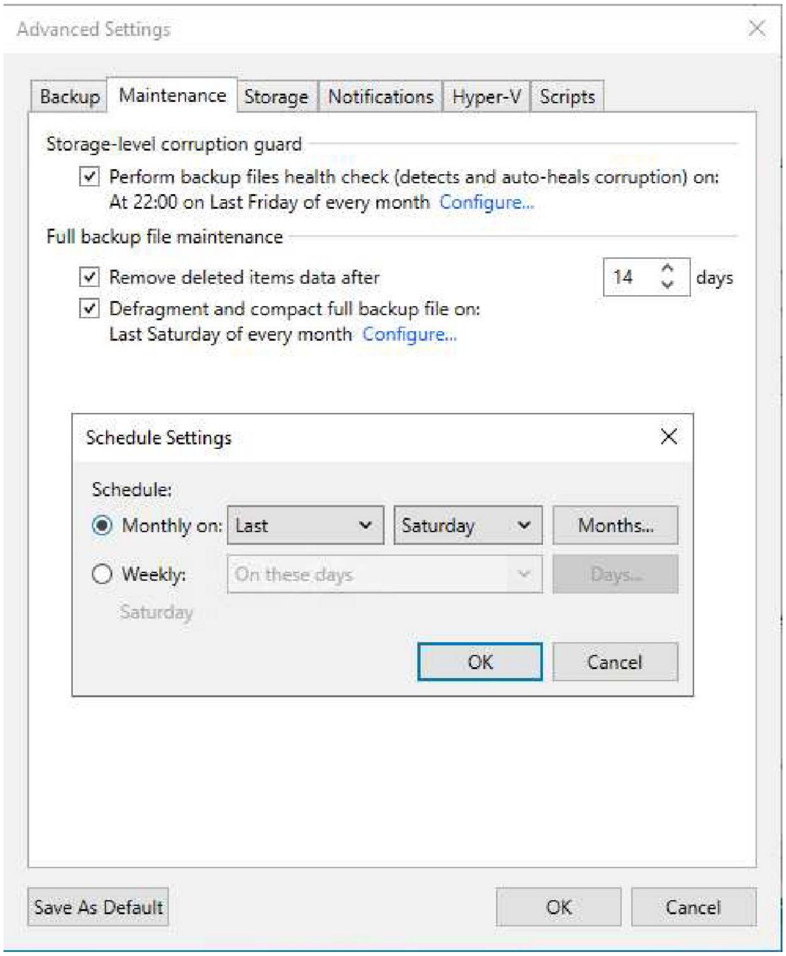
36. Select the Remove deleted items data after the checkbox and enter the few days you want backup data for deleted VMs to be kept.

37. Select the Defragment and compact full backup file checkbox and click Configure.

38. Set the schedule for the compact operation to compact a full backup periodically.

Note:

GFS retention is not compatible with defragment and compact functionality.



Advanced Settings

Backup | Maintenance | Storage | Notifications | Hyper-V | Scripts

Storage-level corruption guard

☑ Perform backup files health check (detects and auto-heals corruption) on:
At 22:00 on Last Friday of every month Configure...

Full backup file maintenance

☑ Remove deleted items data after 14 days

☑ Defragment and compact full backup file on:
Last Saturday of every month Configure...

Schedule Settings

Schedule:

● Monthly on: Last Saturday Months...

○ Weekly: On these days Days...
Saturday

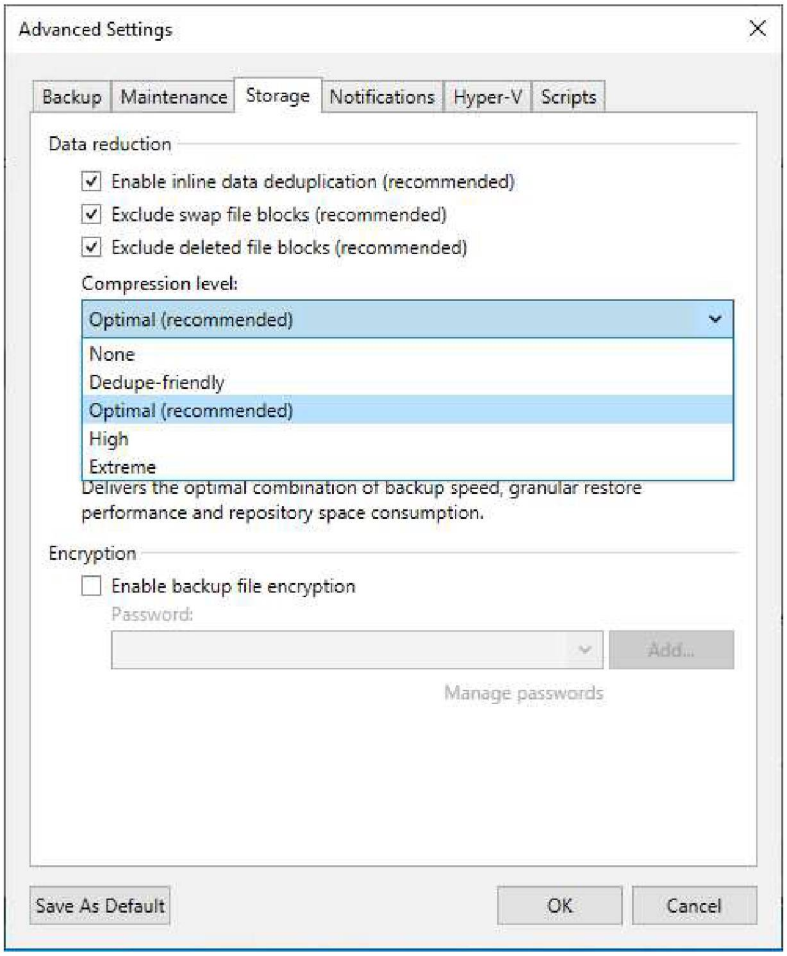
39. On Advanced Settings, select Storage.

40. Select the Enable inline data deduplication (recommended) checkbox.

41. Select the Exclude swap file blocks (recommended) checkbox.

42. Select the Exclude deleted file blocks (recommended) checkbox.

43. Select the compression level for the backup from the drop-down list.



Advanced Settings

Data reduction

☑ Enable inline data deduplication (recommended)

☑ Exclude swap file blocks (recommended)

☑ Exclude deleted file blocks (recommended)

Compression level:

Optimal (recommended)

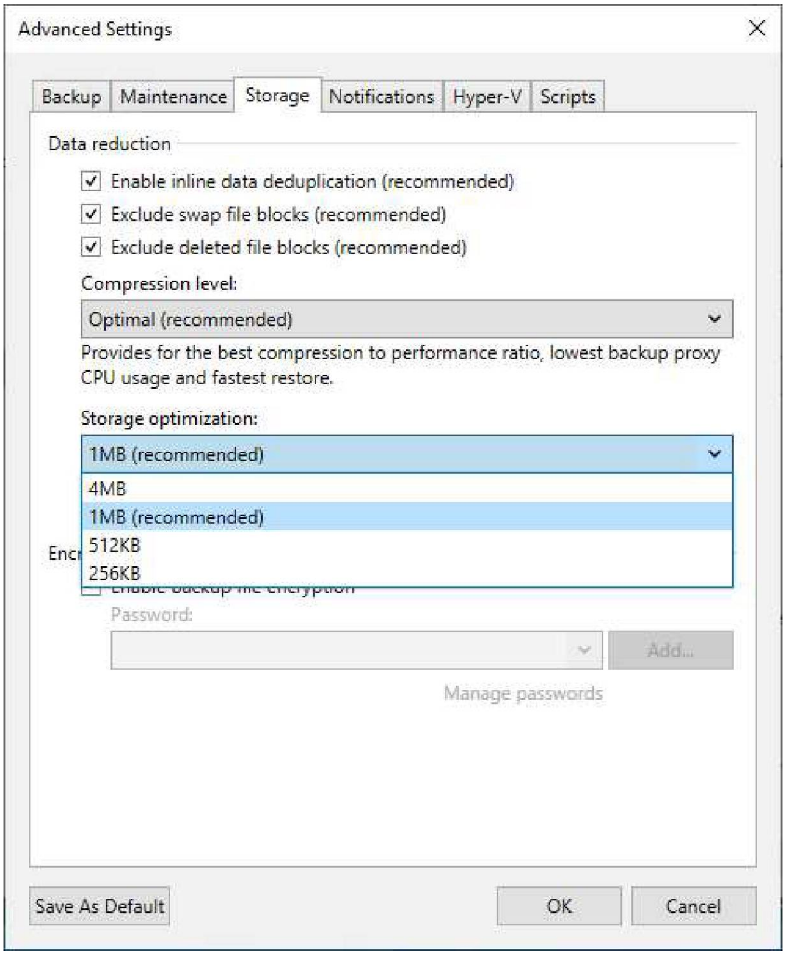
Delivers the optimal combination of backup speed, granular restore performance and repository space consumption.

Encryption

□ Enable backup file encryption

Password:

44. Select the Storage optimization for the backup from the drop-down list.



Advanced Settings

Data reduction

☑ Enable inline data deduplication (recommended)

☑ Exclude swap file blocks (recommended)

☑ Exclude deleted file blocks (recommended)

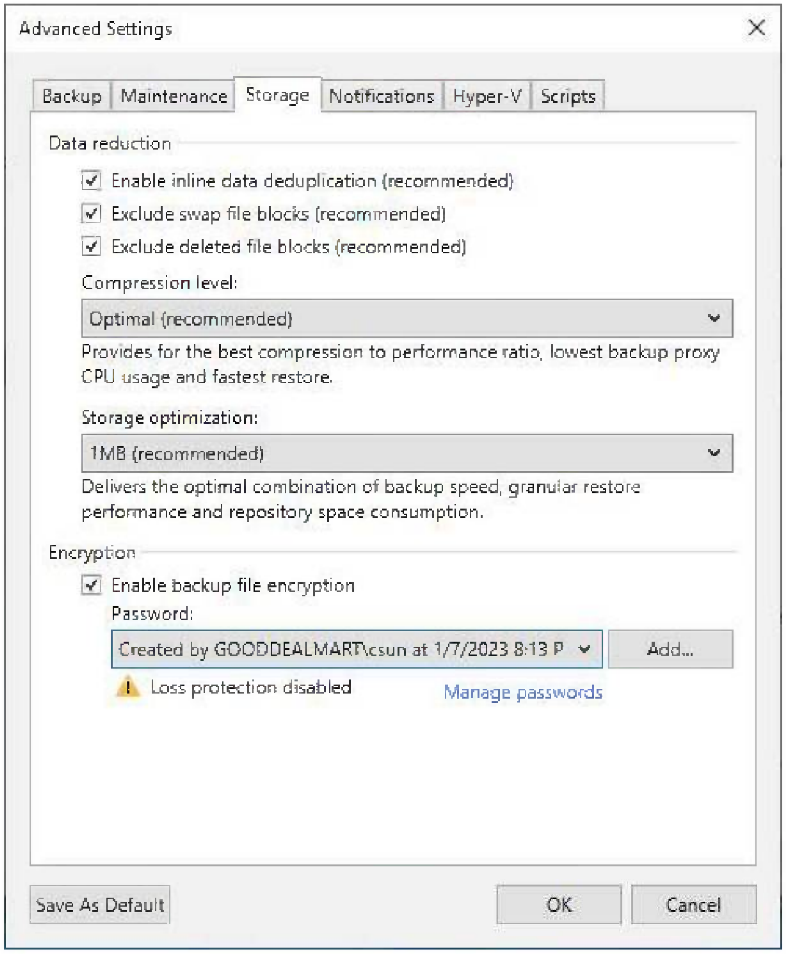
Compression level: Optimal (recommended)

Provides for the best compression to performance ratio, lowest backup proxy CPU usage and fastest restore.

Storage optimization: 1MB (recommended)

45. Select the Enable backup file encryption checkbox to encrypt the content of backup files.

46. Select a password from the drop-down list. Then, if you still need to do, click Add or use the Manage passwords link to create a new password.



Advanced Settings

Data reduction

☑ Enable inline data deduplication (recommended)

☑ Exclude swap file blocks (recommended)

☑ Exclude deleted file blocks (recommended)

Compression level: Optimal (recommended)

Provides for the best compression to performance ratio, lowest backup proxy CPU usage and fastest restore.

Storage optimization: 1MB (recommended)

Delivers the optimal combination of backup speed, granular restore performance and repository space consumption.

Encryption

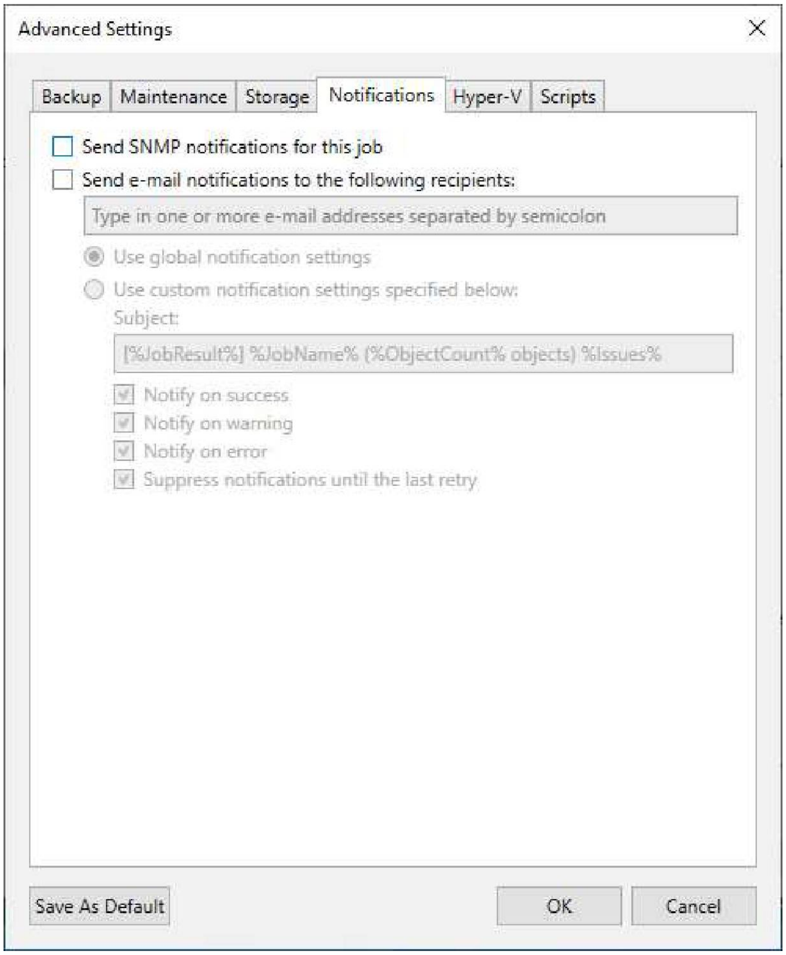
☑ Enable backup file encryption

Password: Created by GOODDEALMART\csun at 1/7/2023 8:13 P

Loss protection disabled

47. Select Notifications on the Advanced Settings.

48. Keep the default settings.



Advanced Settings

□ Send SNMP notifications for this job

□ Send e-mail notifications to the following recipients:

Type in one or more e-mail addresses separated by semicolon

● Use global notification settings

○ Use custom notification settings specified below:

Subject:

[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

☑ Notify on success

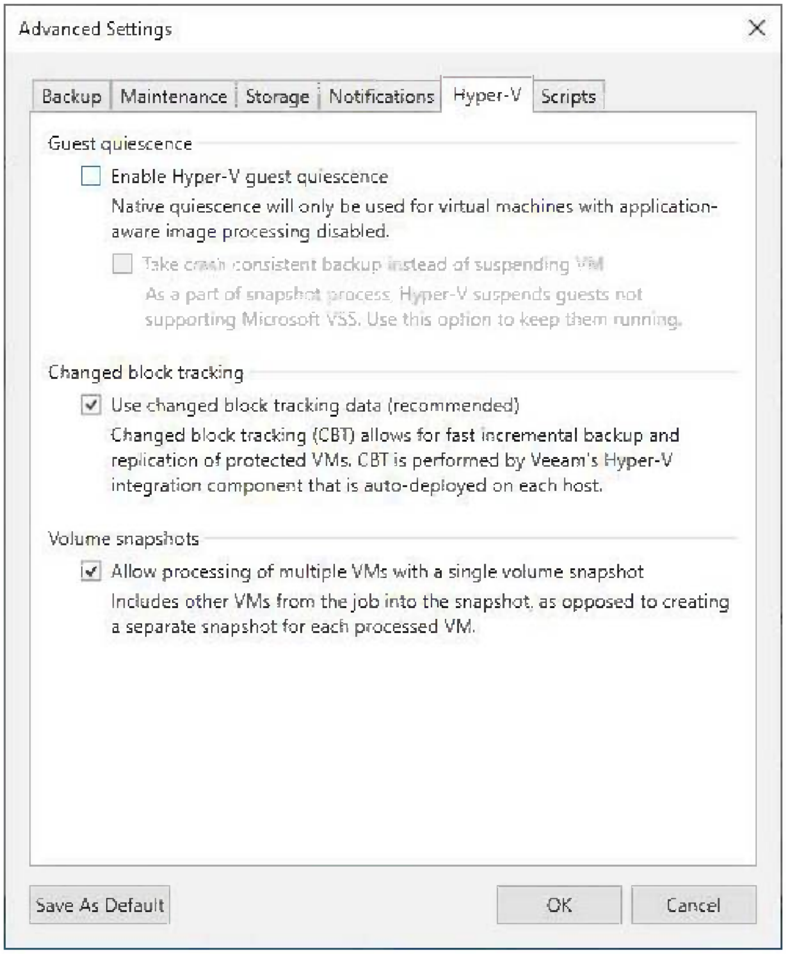
☑ Notify on warning

☑ Notify on error

☑ Suppress notifications until the last retry

49. Select Hyper-V on the Advanced Settings.

50. Keep the default settings.



Guest quiescence

□ Enable Hyper-V guest quiescence

Native quiescence will only be used for virtual machines with application-aware image processing disabled.

□ Take crash consistent backup instead of suspending VM

As a part of snapshot process, Hyper-V suspends guests not supporting Microsoft VSS. Use this option to keep them running.

Changed block tracking

☑ Use changed block tracking data (recommended)

Changed block tracking (CBT) allows for fast incremental backup and replication of protected VMs. CBT is performed by Veeam's Hyper-V integration component that is auto-deployed on each host.

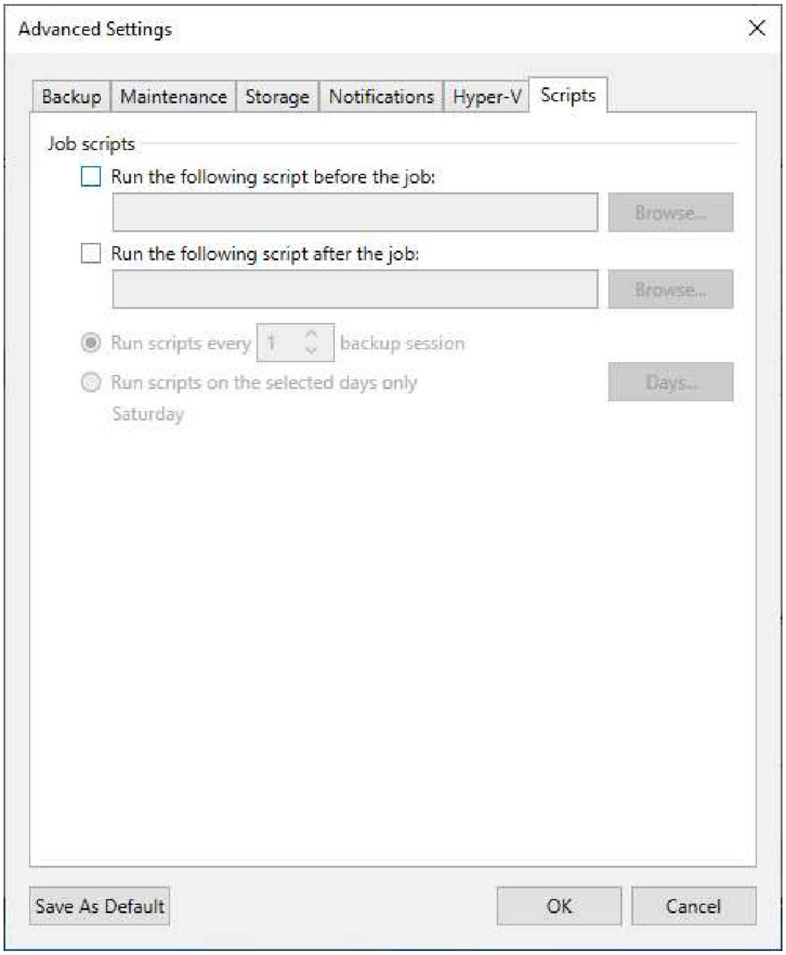
Volume snapshots

☑ Allow processing of multiple VMs with a single volume snapshot

Includes other VMs from the job into the snapshot, as opposed to creating a separate snapshot for each processed VM.

51. On the Advanced Settings page, select Scripts and keep the default settings.

52. Click OK.



Advanced Settings

Job scripts

□ Run the following script before the job:

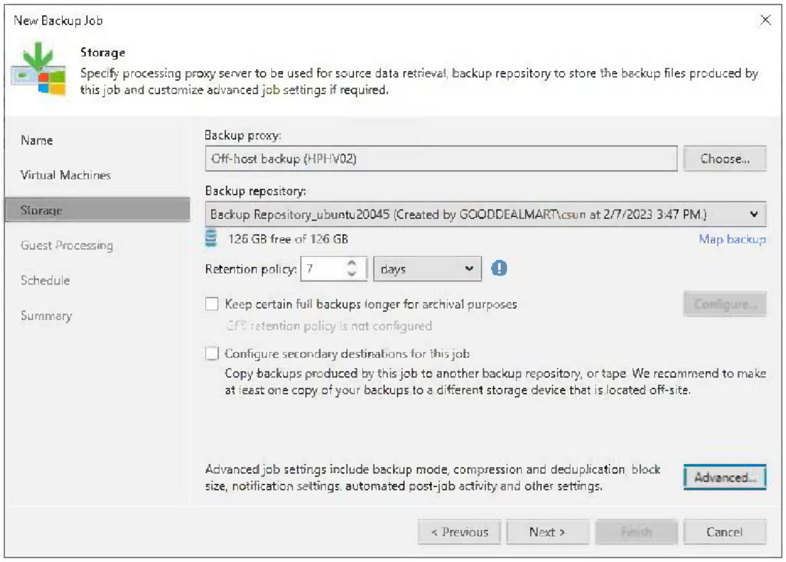
□ Run the following script after the job:

● Run scripts every 1 backup session

○ Run scripts on the selected days only

Saturday

53. Click Next on the Storage page.



New Backup Job

Storage

Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Backup proxy: Off-host backup (HPHV02)

Backup repository: Backup Repository_ubuntu20045 (Created by GOODDEALMART\csun at 2/7/2023 3:47 PM.)

126 GB free of 126 GB

Retention policy: 7 days

☐ Keep certain full backups longer for archival purposes

GFS retention policy is not configured

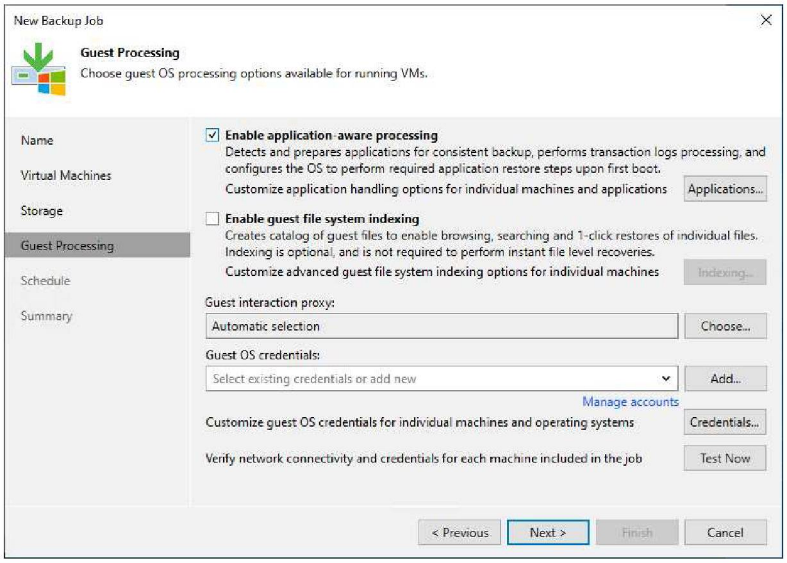
☐ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

54. When you add VMs running VSS-aware applications to the backup job, you can enable application-aware processing to create a transactionally consistent backup. The transactionally consistent backup ensures that applications on VMs can be recovered without data loss.

55. Select the Enable application-aware processing checkbox on the Guest Processing page and click Applications.



New Backup Job

Guest Processing

Choose guest OS processing options available for running VMs.

☑ **Enable application-aware processing**

Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

Customize application handling options for individual machines and applications

☐ **Enable guest file system indexing**

Creates catalog of guest files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries.

Customize advanced guest file system indexing options for individual machines

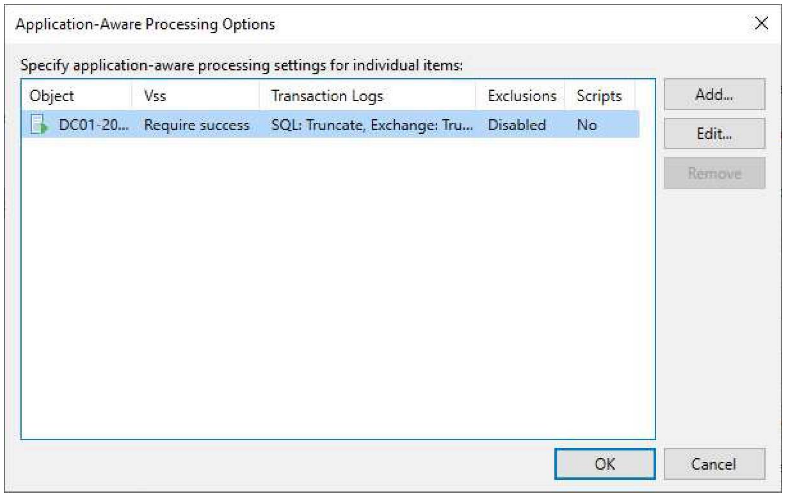
Guest interaction proxy: Automatic selection

Guest OS credentials: Select existing credentials or add new

Customize guest OS credentials for individual machines and operating systems

Verify network connectivity and credentials for each machine included in the job

56. On the Application-Aware Processing Options page, select the VM and click Edit.



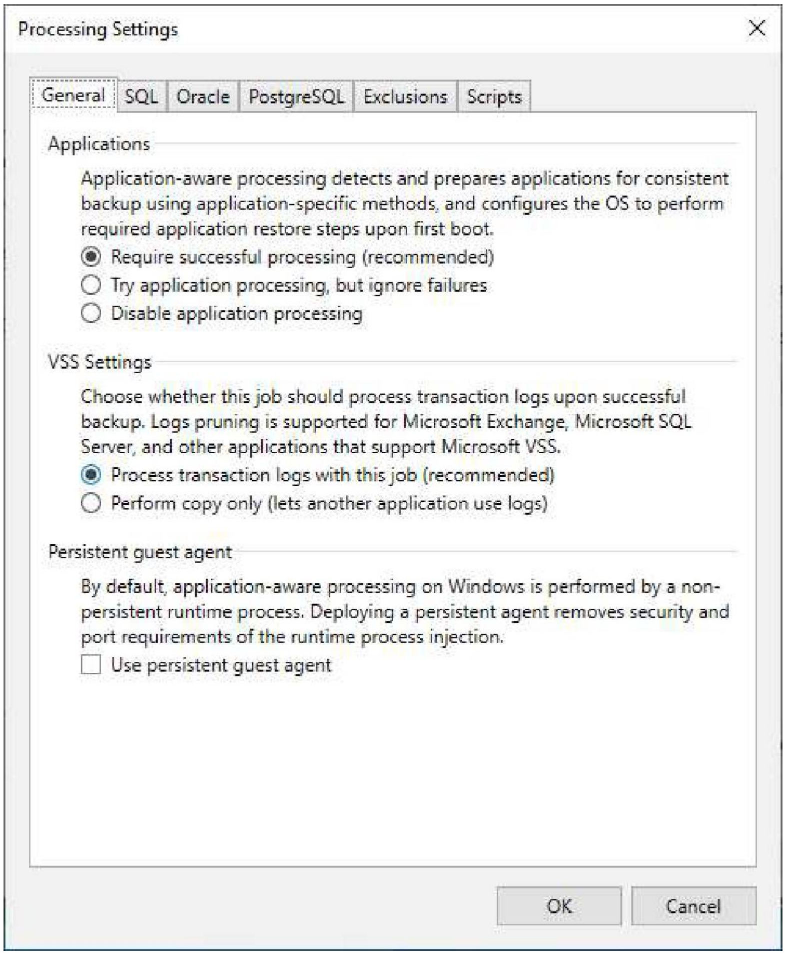
Application-Aware Processing Options

Specify application-aware processing settings for individual items:

Object	Vss	Transaction Logs	Exclusions	Scripts
DC01-20...	Require success	SQL: Truncate, Exchange: Tru...	Disabled	No

57. On the Processing Settings, click General.

58. Keep the default settings.



Processing Settings

Applications

Application-aware processing detects and prepares applications for consistent backup using application-specific methods, and configures the OS to perform required application restore steps upon first boot.

● Require successful processing (recommended)

○ Try application processing, but ignore failures

○ Disable application processing

VSS Settings

Choose whether this job should process transaction logs upon successful backup. Logs pruning is supported for Microsoft Exchange, Microsoft SQL Server, and other applications that support Microsoft VSS.

● Process transaction logs with this job (recommended)

○ Perform copy only (lets another application use logs)

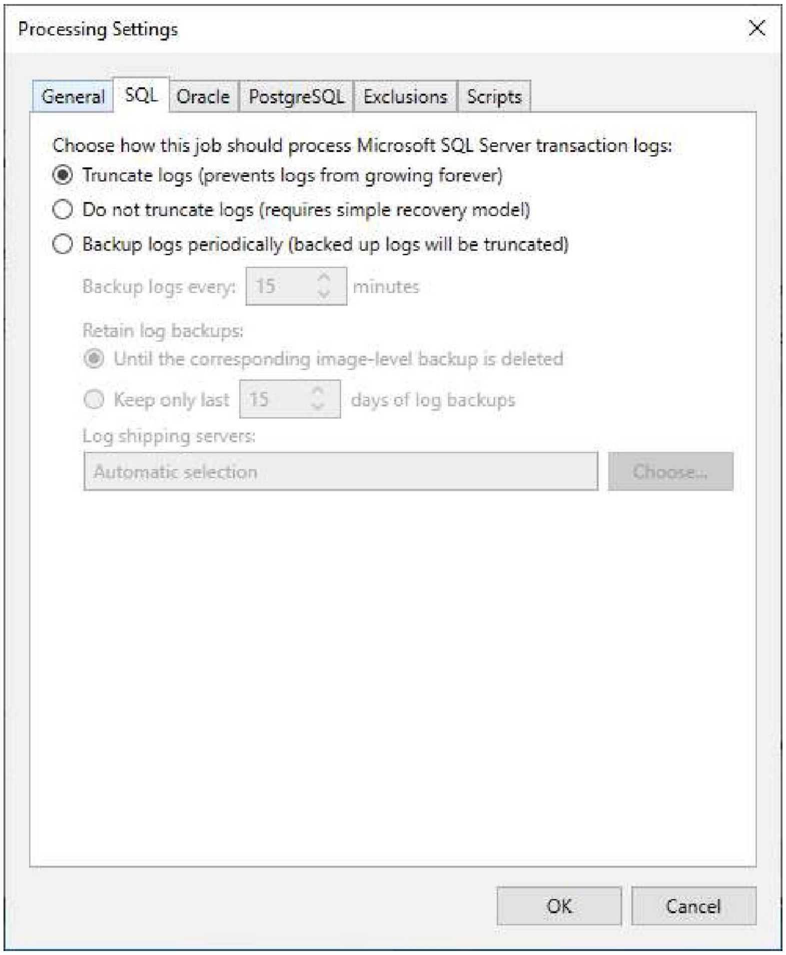
Persistent guest agent

By default, application-aware processing on Windows is performed by a non-persistent runtime process. Deploying a persistent agent removes security and port requirements of the runtime process injection.

□ Use persistent guest agent

59. On the Processing Settings page, click SQL if the VM is a Microsoft SQL Server VM.

60. Select Truncate logs (Prevents logs from growing forever) to truncate transaction logs after a successful backup.



Processing Settings

Choose how this job should process Microsoft SQL Server transaction logs:

● Truncate logs (prevents logs from growing forever)

○ Do not truncate logs (requires simple recovery model)

○ Backup logs periodically (backed up logs will be truncated)

Backup logs every: 15 minutes

Retain log backups:

● Until the corresponding image-level backup is deleted

○ Keep only last 15 days of log backups

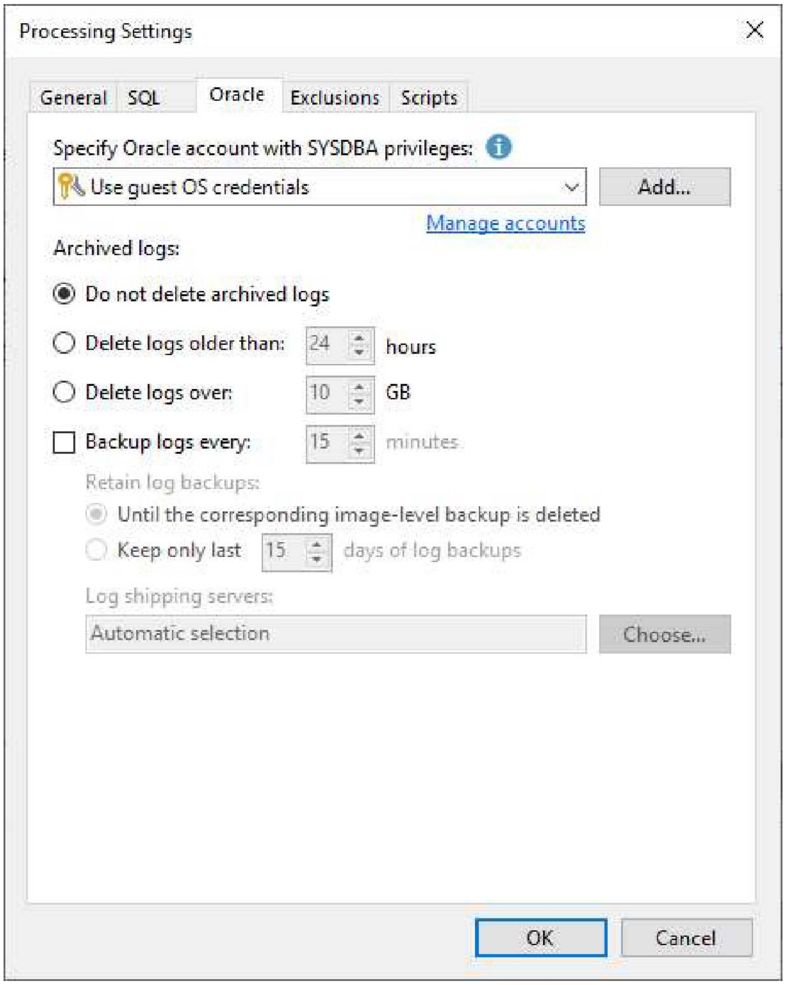
Log shipping servers:

Automatic selection

61. On the Processing Settings page, click Oracle if the VM is an Oracle Server.

62. Select a user account from the drop-down list.

63. Select Do not delete archived logs checkbox.



Processing Settings

Specify Oracle account with SYSDBA privileges:

Use guest OS credentials

Archived logs:

● Do not delete archived logs

○ Delete logs older than: 24 hours

○ Delete logs over: 10 GB

□ Backup logs every: 15 minutes

Retain log backups:

● Until the corresponding image-level backup is deleted

○ Keep only last 15 days of log backups

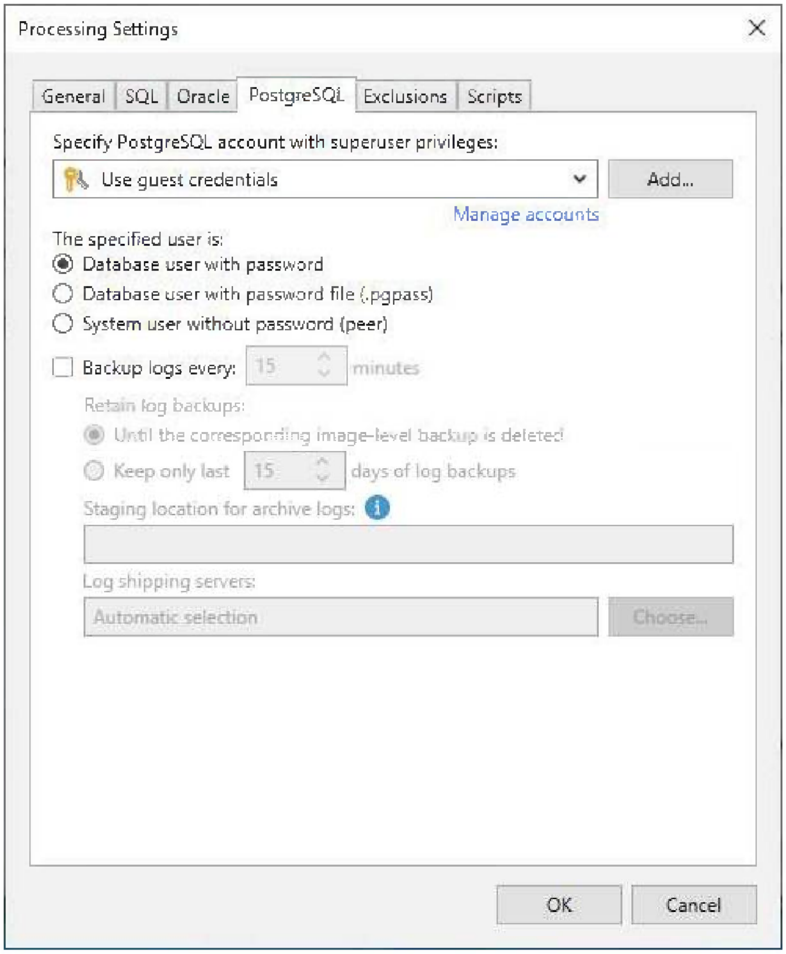
Log shipping servers:

Automatic selection

64. On the Processing Settings page, click PostgreSQL if the VM is a PostgreSQL Server VM.

65. Select a user account from the drop-down list.

66. Select Database user with password checkbox.



Specify PostgreSQL account with superuser privileges:

Use guest credentials

The specified user is:

● Database user with password

○ Database user with password file (.pgpass)

○ System user without password (peer)

□ Backup logs every: 15 minutes

Retain log backups:

● Until the corresponding image-level backup is deleted

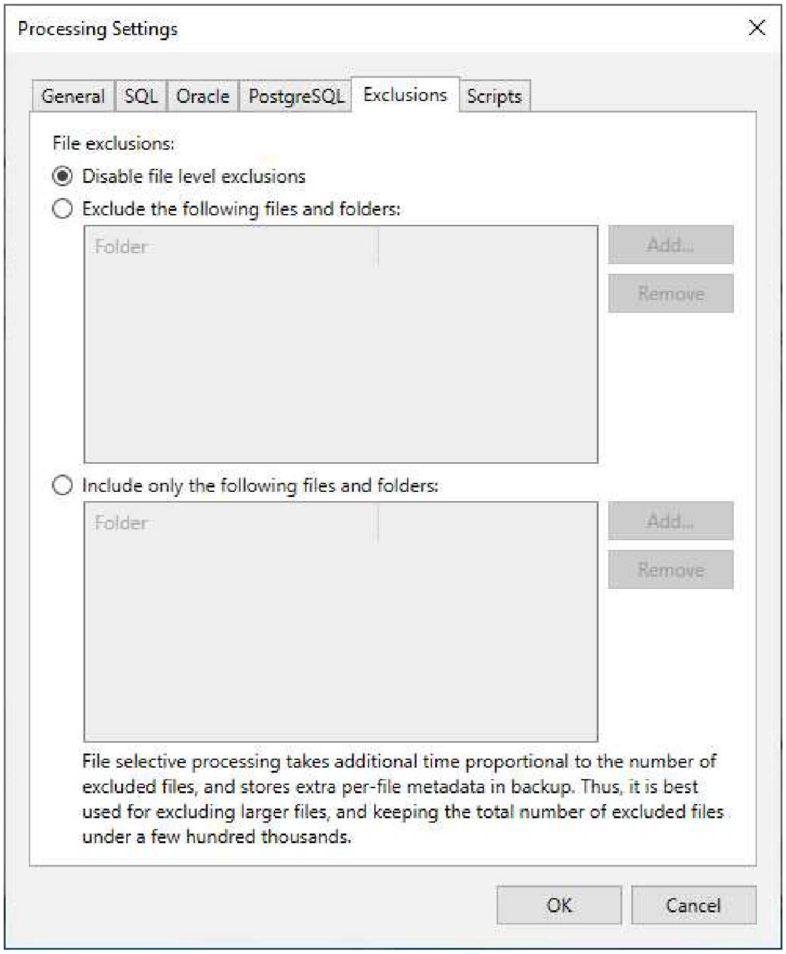
○ Keep only last 15 days of log backups

Staging location for archive logs:

Log shipping servers:

Automatic selection

67. On the Processing Settings page, click Exclusions and keep the default settings.



Processing Settings

File exclusions:

● Disable file level exclusions

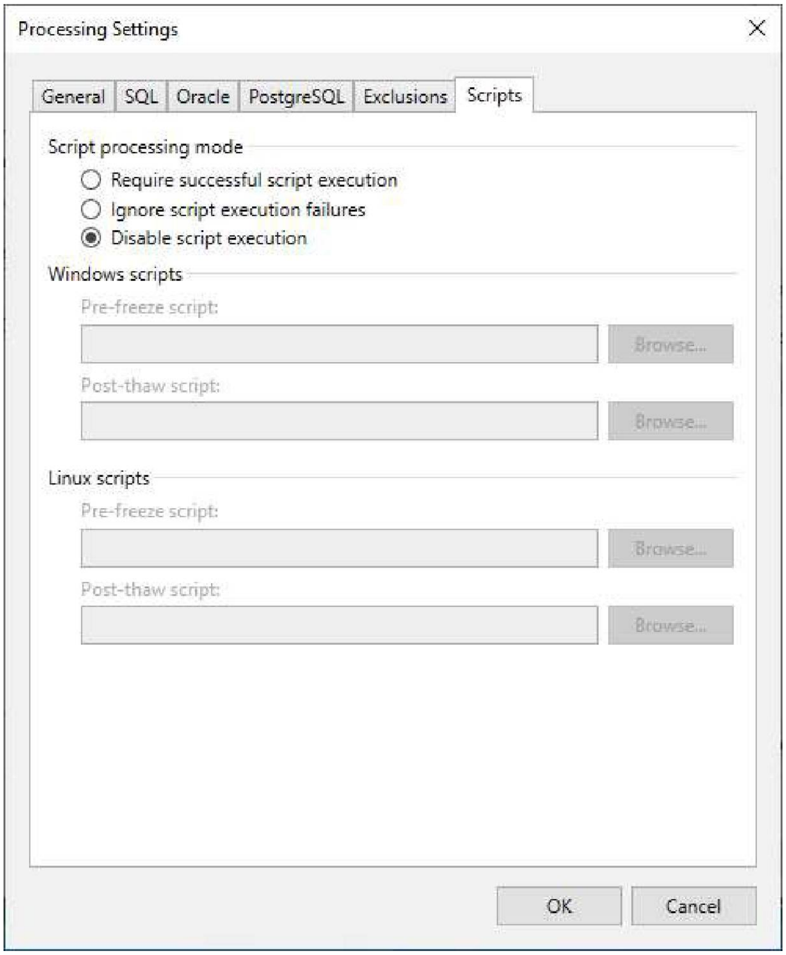
○ Exclude the following files and folders:

○ Include only the following files and folders:

File selective processing takes additional time proportional to the number of excluded files, and stores extra per-file metadata in backup. Thus, it is best used for excluding larger files, and keeping the total number of excluded files under a few hundred thousands.

68. On the Processing Settings page, click Scripts and keep the default settings.

69. Click OK.



Processing Settings

Script processing mode

○ Require successful script execution

○ Ignore script execution failures

● Disable script execution

Windows scripts

Pre-freeze script:

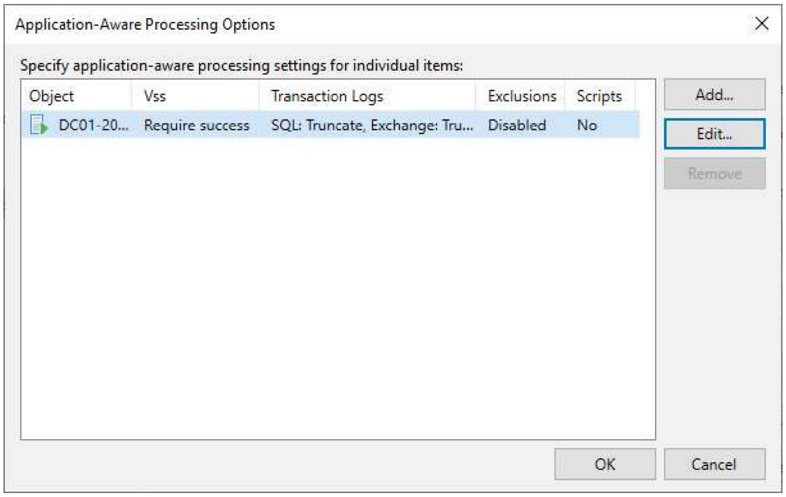
Post-thaw script:

Linux scripts

Pre-freeze script:

Post-thaw script:

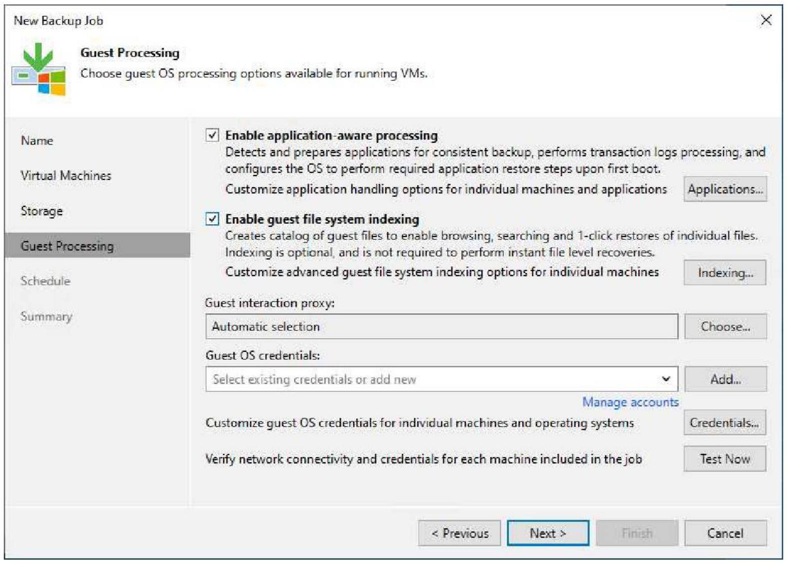
70. On the Application-Aware Processing Options page, click OK.


Application-Aware Processing Options

Specify application-aware processing settings for individual items:

Object	Vss	Transaction Logs	Exclusions	Scripts
DC01-20...	Require success	SQL: Truncate, Exchange: Tru...	Disabled	No

71. Select the Enable guest file system indexing checkbox and click Indexing.


New Backup Job

Guest Processing
Choose guest OS processing options available for running VMs.

☑ **Enable application-aware processing**
Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.
Customize application handling options for individual machines and applications

☑ **Enable guest file system indexing**
Creates catalog of guest files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries.
Customize advanced guest file system indexing options for individual machines

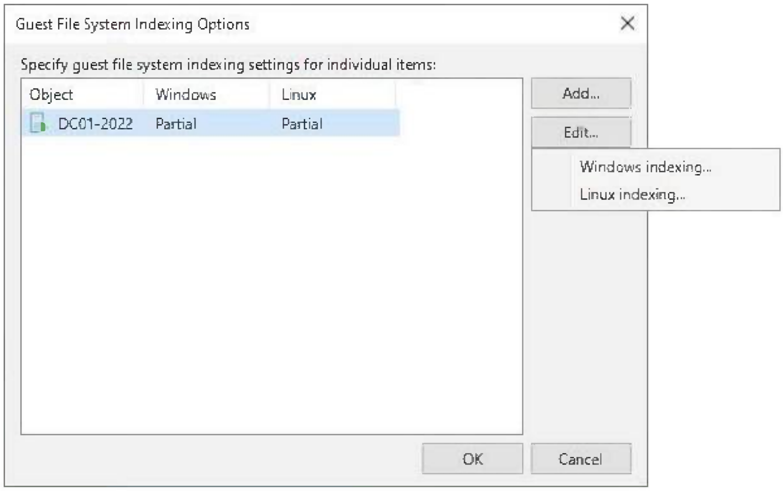
Guest interaction proxy: Automatic selection

Guest OS credentials: Select existing credentials or add new

Customize guest OS credentials for individual machines and operating systems

Verify network connectivity and credentials for each machine included in the job

72. On the Guest File System Indexing Options page, select the VM, click Edit and select Windows indexing.



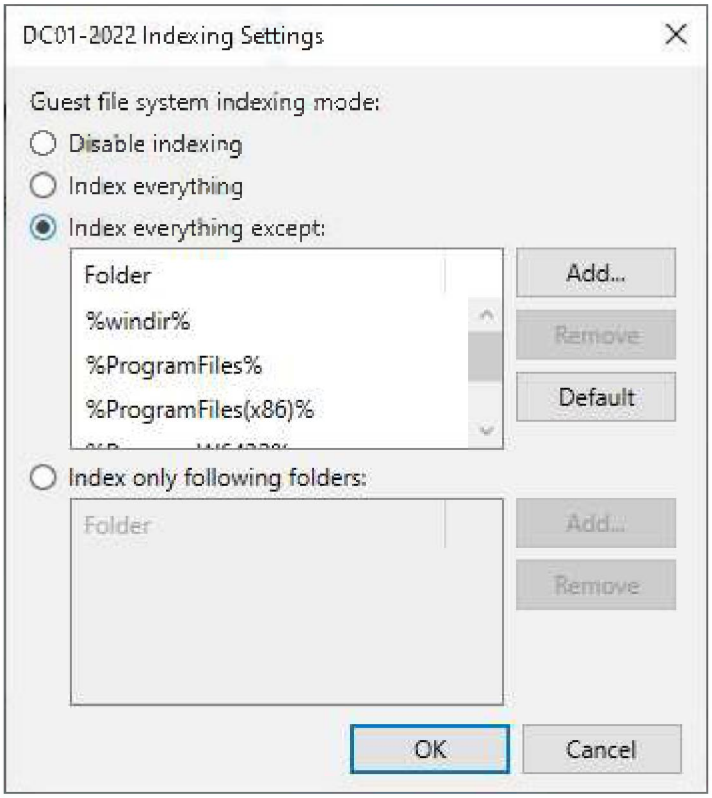
Guest File System Indexing Options

Specify guest file system indexing settings for individual items:

Object	Windows	Linux
DC01-2022	Partial	Partial

73. On the Guest file system indexing mode page, keep the default settings.

74. Click OK.



DC01-2022 Indexing Settings

Guest file system indexing mode:

○ Disable indexing

○ Index everything

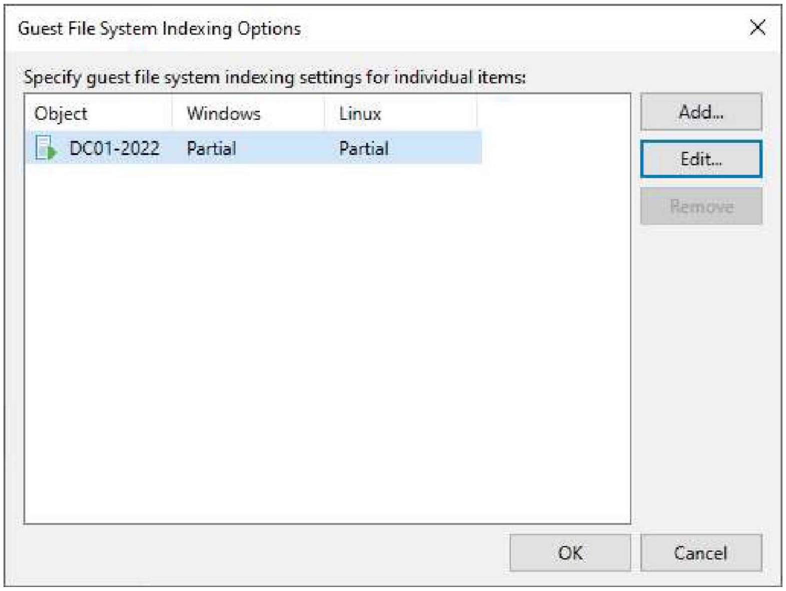
● Index everything except:

Folder
%windir%
%ProgramFiles%
%ProgramFiles(x86)%

○ Index only following folders:

Folder

75. Click OK on the Guest file system indexing mode page.

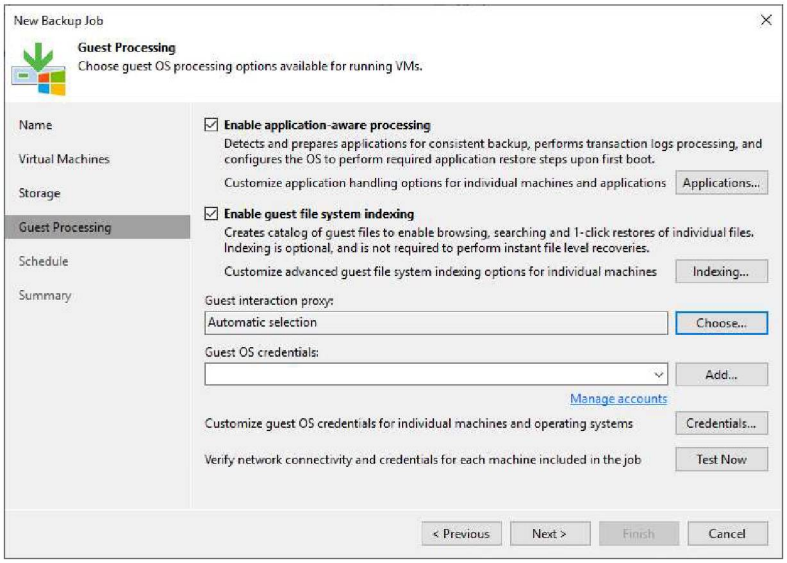


Guest File System Indexing Options

Specify guest file system indexing settings for individual items:

Object	Windows	Linux
DC01-2022	Partial	Partial

76. Keep the default Automatic selection setting in the Guest interaction proxy field.



New Backup Job

Guest Processing
Choose guest OS processing options available for running VMs.

☑ **Enable application-aware processing**
Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.
Customize application handling options for individual machines and applications

☑ **Enable guest file system indexing**
Creates catalog of guest files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries.
Customize advanced guest file system indexing options for individual machines

Guest interaction proxy:
Automatic selection

Guest OS credentials:

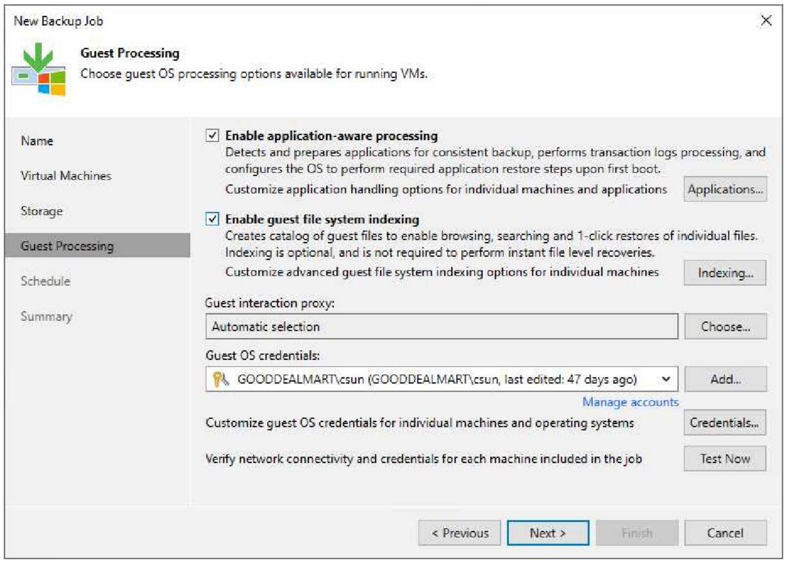
Customize guest OS credentials for individual machines and operating systems

Verify network connectivity and credentials for each machine included in the job

77. Choose a user account on the Guest Processing page with sufficient permissions from the Guest OS credentials drop-down list.

78. If you have multiple VMs at the same job, click Credentials to Customize guest OS credentials for individual machines and operating systems.

79. On the Guest Processing page, click Test Now to verify network connectivity and credentials for each machine included in the job.



Guest Processing
Choose guest OS processing options available for running VMs.

☑ **Enable application-aware processing**
Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.
Customize application handling options for individual machines and applications

☑ **Enable guest file system indexing**
Creates catalog of guest files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries.
Customize advanced guest file system indexing options for individual machines

Guest interaction proxy:
Automatic selection

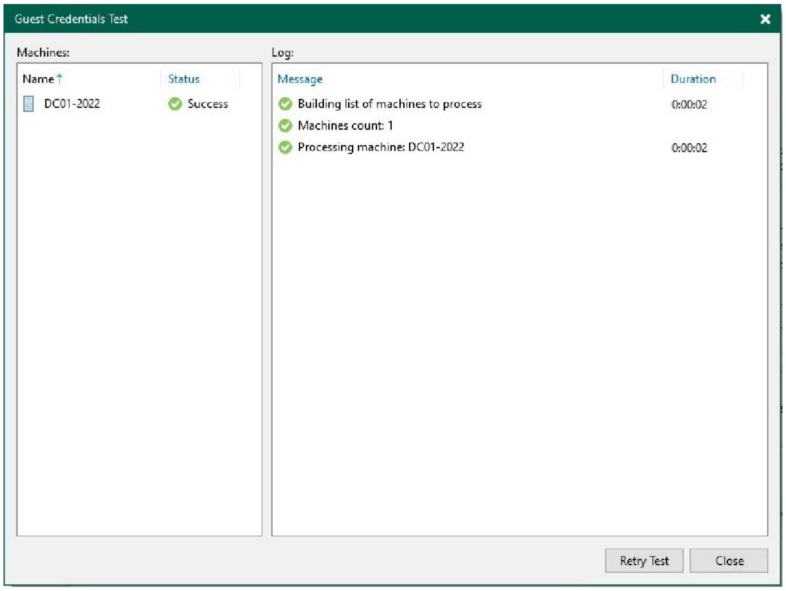
Guest OS credentials:
GOODDEALMART\csun (GOODDEALMART\csun, last edited: 47 days ago)

Customize guest OS credentials for individual machines and operating systems

Verify network connectivity and credentials for each machine included in the job

80. On the Guest Credentials Test page, ensure verification success for each machine.

81. Click Close.



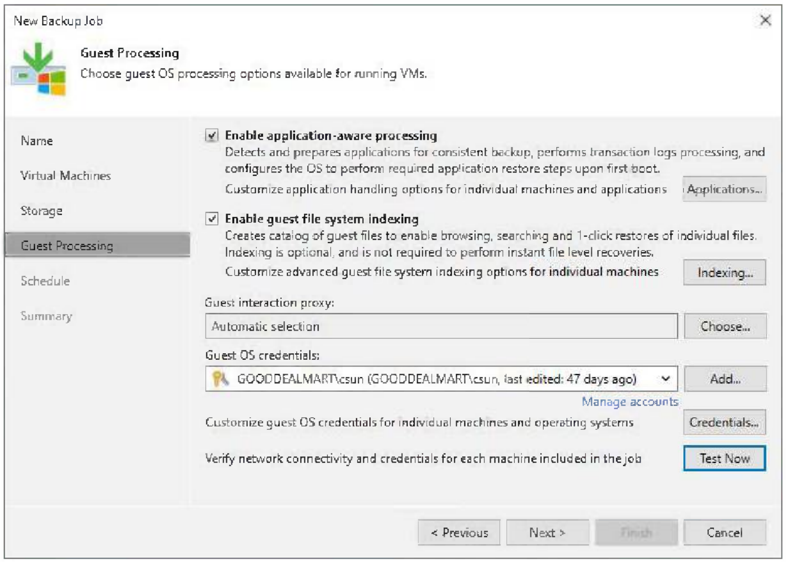
Machines:

Name ↑	Status
DC01-2022	✓ Success

Log:

Message	Duration
✓ Building list of machines to process	0:00:02
✓ Machines count: 1	
✓ Processing machine: DC01-2022	0:00:02

82. Click Next on the Guest Processing page.



Guest Processing

Choose guest OS processing options available for running VMs.

☑ Enable application-aware processing

Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

Customize application handling options for individual machines and applications

☑ Enable guest file system indexing

Creates catalog of guest files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries.

Customize advanced guest file system indexing options for individual machines

Guest interaction proxy:

Automatic selection

Guest OS credentials:

GOODDEALMART\csun (GOODDEALMART\csun, last edited: 47 days ago)

Customize guest OS credentials for individual machines and operating systems

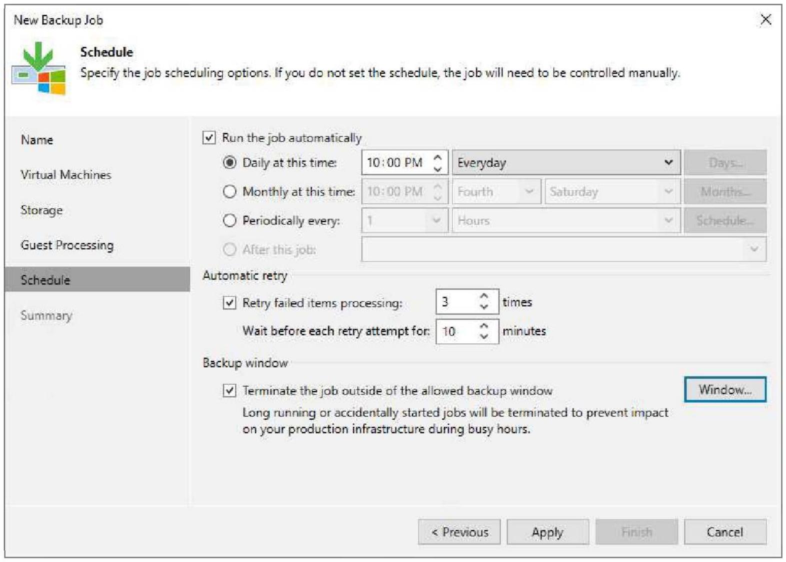
Verify network connectivity and credentials for each machine included in the job

83. Select Run the job automatically checkbox on the Schedule page and select your specified schedule.

84. Define whether Veeam Backup & Replication should retry the backup job if it fails in the Automatic retry section.

85. Define the time interval the backup job must complete in the Backup window section. The backup window ensures that the job does not overlap with production hours and that there is no unnecessary overhead on the production environment.

86. Click Apply.



New Backup Job

Schedule

Specify the job scheduling options. If you do not set the schedule, the job will need to be controlled manually.

☑ Run the job automatically

● Daily at this time: 10:00 PM Everyday Days...

○ Monthly at this time: 10:00 PM Fourth Saturday Months...

○ Periodically every: 1 Hours Schedule...

○ After this job:

Automatic retry

☑ Retry failed items processing: 3 times

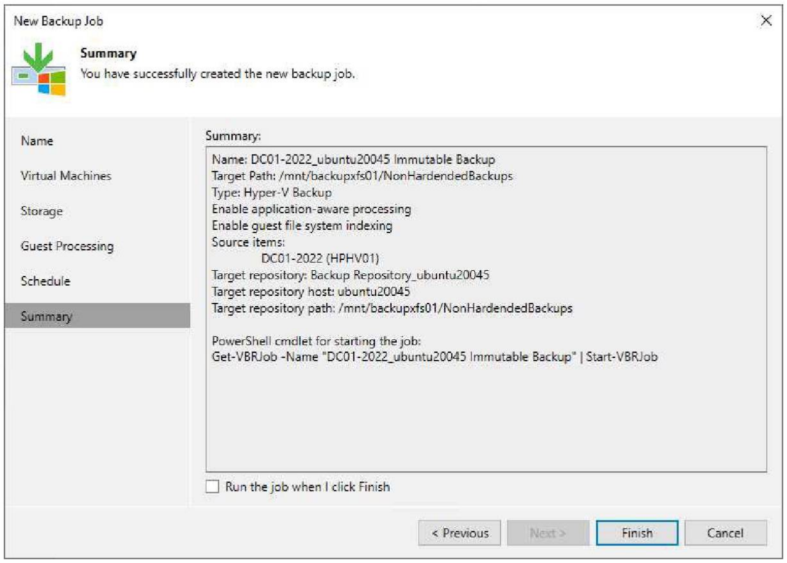
Wait before each retry attempt for: 10 minutes

Backup window

☑ Terminate the job outside of the allowed backup window Window...

Long running or accidentally started jobs will be terminated to prevent impact on your production infrastructure during busy hours.

87. Click Finish on the Summary page.



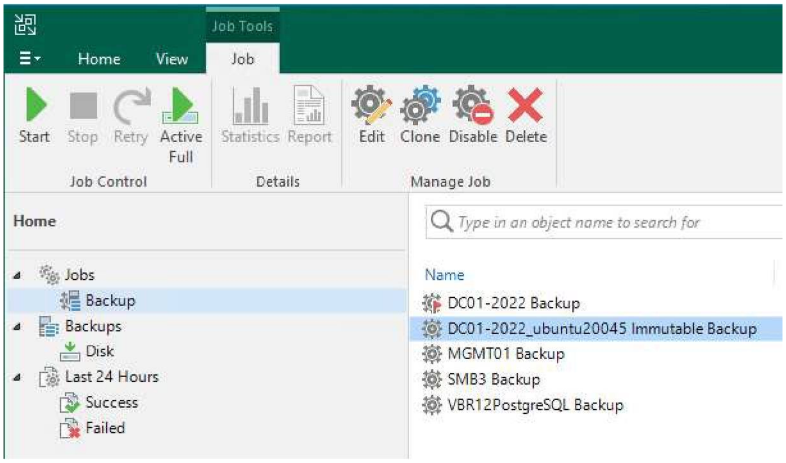
You have successfully created the new backup job.

Summary:

```
Name: DC01-2022_ubuntu20045 Immutable Backup
Target Path: /mnt/backupxfs01/NonHardendedBackups
Type: Hyper-V Backup
Enable application-aware processing
Enable guest file system indexing
Source items:
        DC01-2022 (HPHV01)
Target repository: Backup Repository_ubuntu20045
Target repository host: ubuntu20045
Target repository path: /mnt/backupxfs01/NonHardendedBackups

PowerShell cmdlet for starting the job:
Get-VBRJob -Name "DC01-2022_ubuntu20045 Immutable Backup" | Start-VBRJob
```

□ Run the job when I click Finish

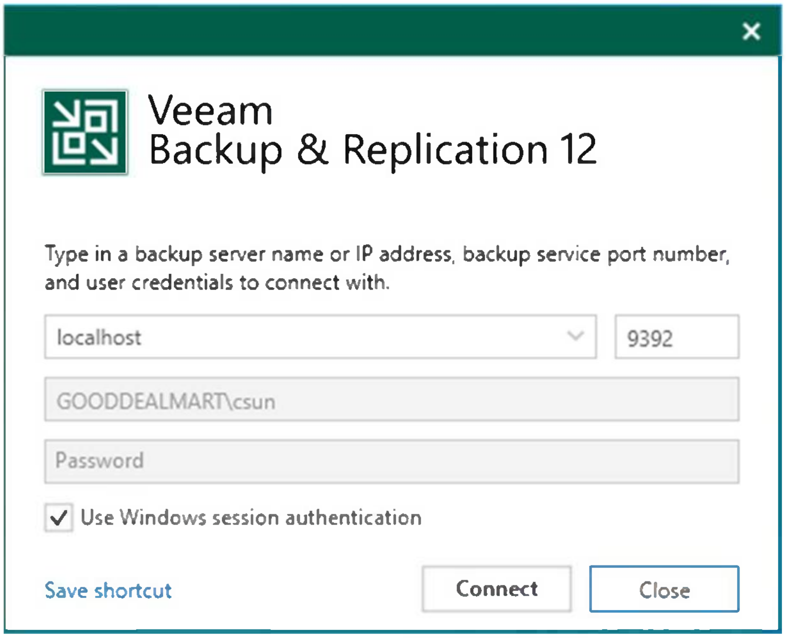
88. Verify that the backup job has been added.



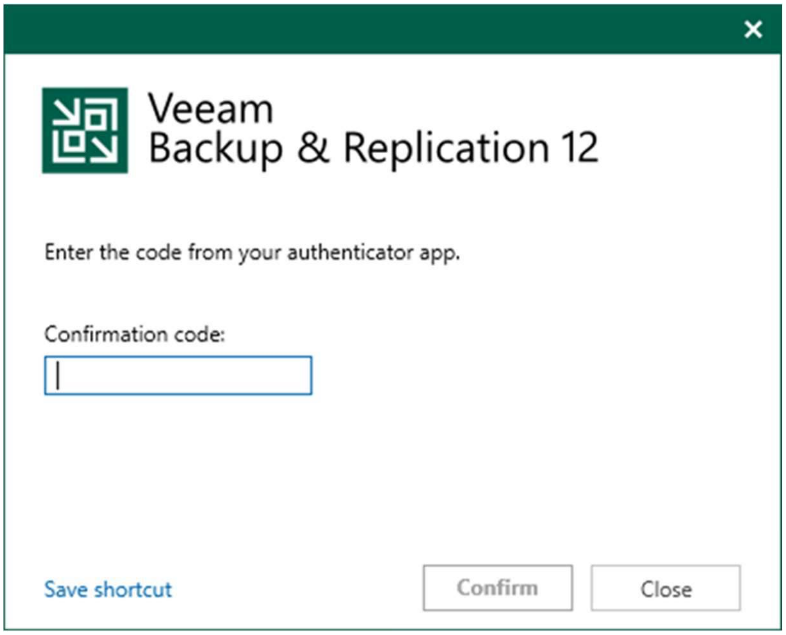
Name
DC01-2022 Backup
DC01-2022_ubuntu20045 Immutable Backup
MGMT01 Backup
SMB3 Backup
VBR12PostgreSQL Backup

Create a Backup job to backup the specified Physical Machines (Managed by Backup Server Mode)

This procedure uses the managed backup server mode to create a backup job to back up the specific physical production machines.

Instructions	Screenshot (if applicable)
1. Log in to the Veeam Backup and replication manager server. 2. Open the Veeam Backup & Replication Console and click Connect.	 Veeam Backup & Replication 12 Type in a backup server name or IP address, backup service port number, and user credentials to connect with. localhost 9392 GOODDEALMART\csun Password ☑ Use Windows session authentication

3. Enter the MFA Confirmation code and click Confirm.



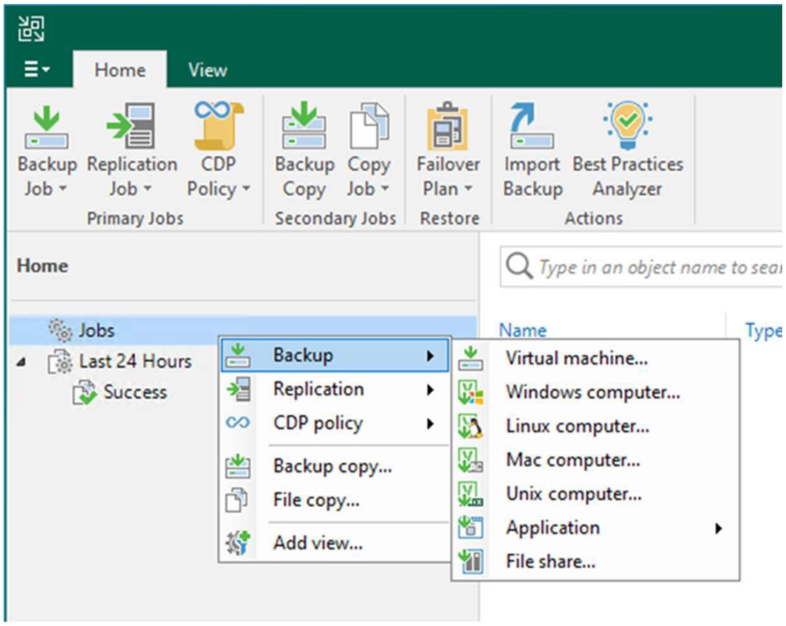
Veeam Backup & Replication 12

Enter the code from your authenticator app.

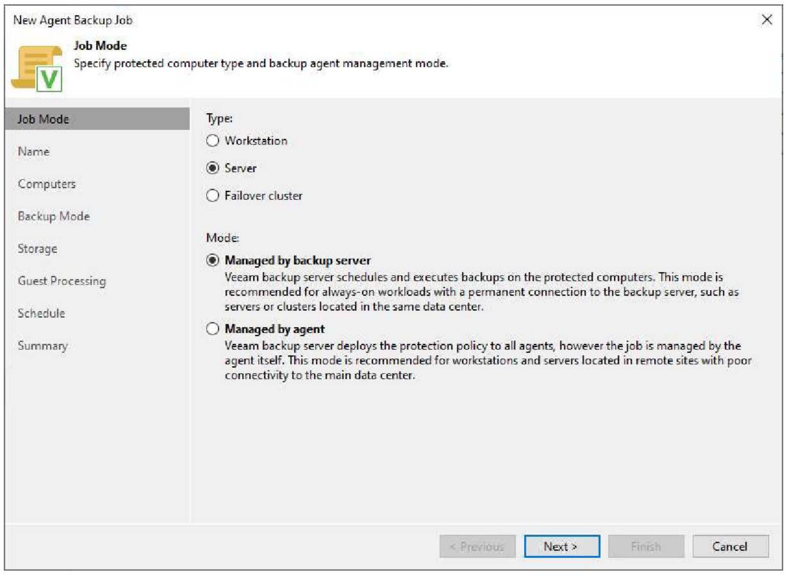
Confirmation code:

4. Select Jobs on the Home page and right-click Jobs.

5. Select Backup and click Windows computer.



6. Select Managed by backup server mode on the Job Mode page and click Next.



New Agent Backup Job

Job Mode

Specify protected computer type and backup agent management mode.

Type:

○ Workstation

● Server

○ Failover cluster

Mode:

● **Managed by backup server**

Veeam backup server schedules and executes backups on the protected computers. This mode is recommended for always-on workloads with a permanent connection to the backup server, such as servers or clusters located in the same data center.

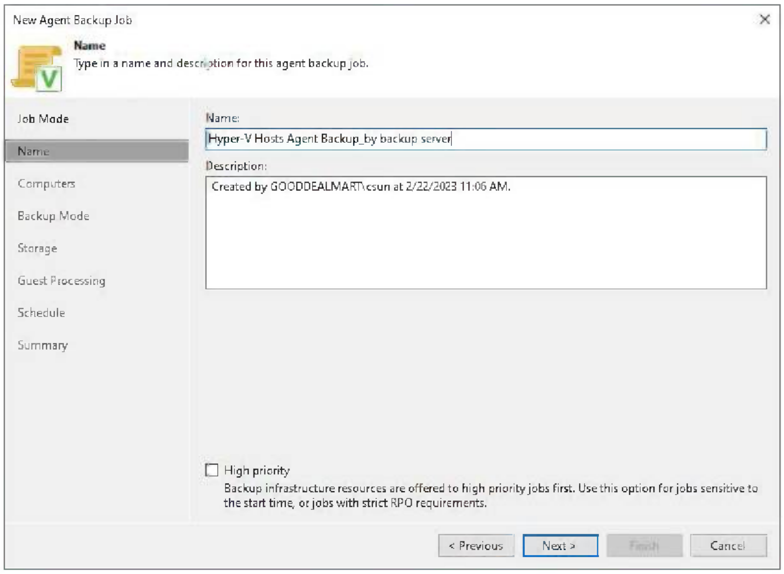
○ **Managed by agent**

Veeam backup server deploys the protection policy to all agents, however the job is managed by the agent itself. This mode is recommended for workstations and servers located in remote sites with poor connectivity to the main data center.

7. On the Name page, enter a name for the backup job in the Name field.

8. Give a brief description in the Description field for the future.

9. Click Next.



New Agent Backup Job

Name

Type in a name and description for this agent backup job.

Name:

Hyper-V Hosts Agent Backup_by backup server

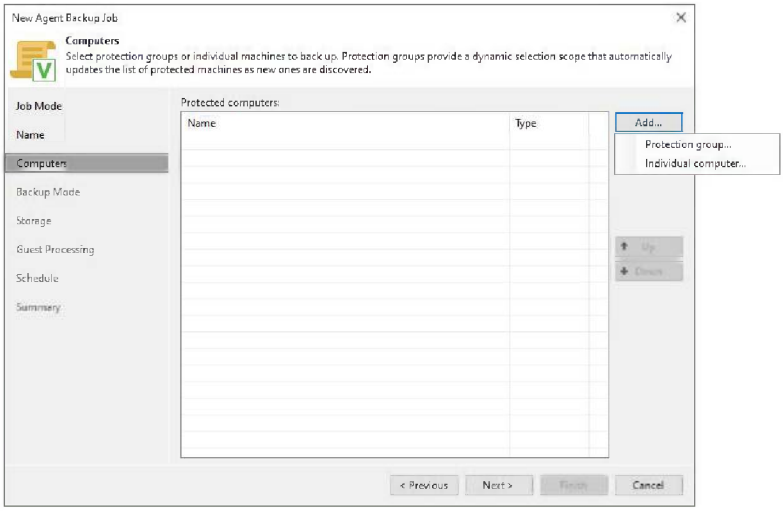
Description:

Created by GOODDEALMART\csun at 2/22/2023 11:06 AM.

□ High priority

Backup infrastructure resources are offered to high priority jobs first. Use this option for jobs sensitive to the start time, or jobs with strict RPO requirements.

10. On the Computers page, click Add and select Protection group.



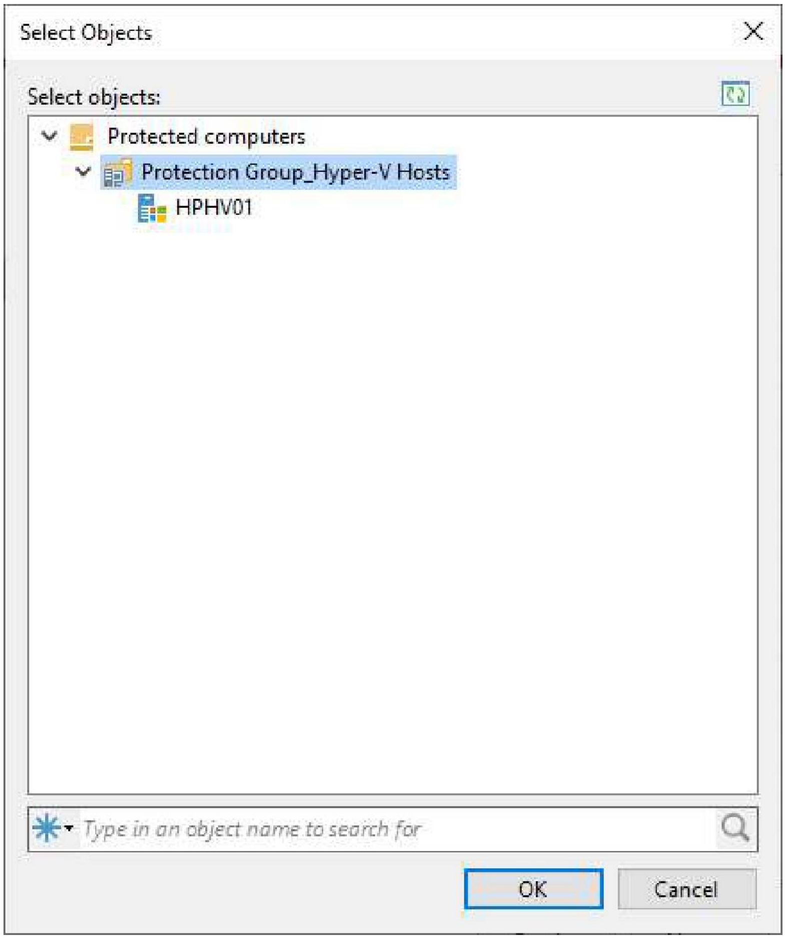
New Agent Backup Job

Computers

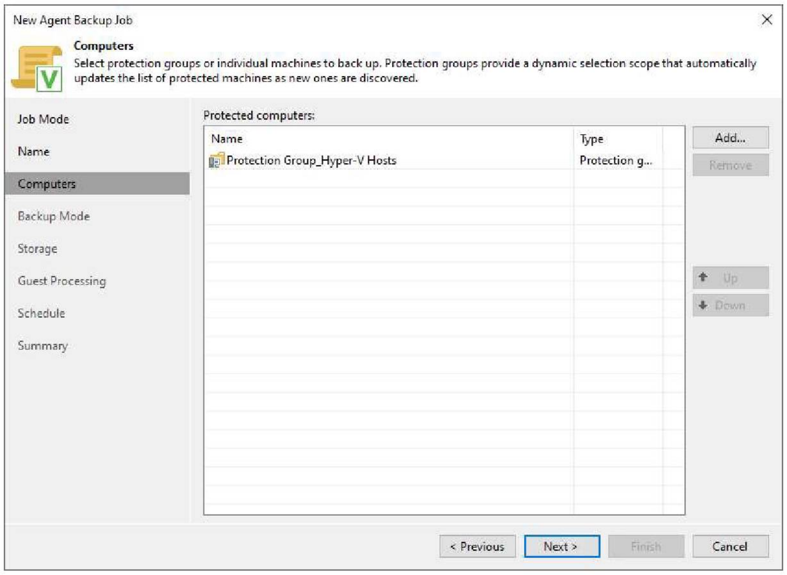
Select protection groups or individual machines to back up. Protection groups provide a dynamic selection scope that automatically updates the list of protected machines as new ones are discovered.

11. Select the protection group on the Select Objects page and click OK.

12. You can select multiple protection groups for the same backup job and repeat the step to add them.


Select Objects
Select objects:
Protected computers
Protection Group_Hyper-V Hosts
HPHV01
Type in an object name to search for
OK
Cancel

13. Click Next on the Computers page.



New Agent Backup Job

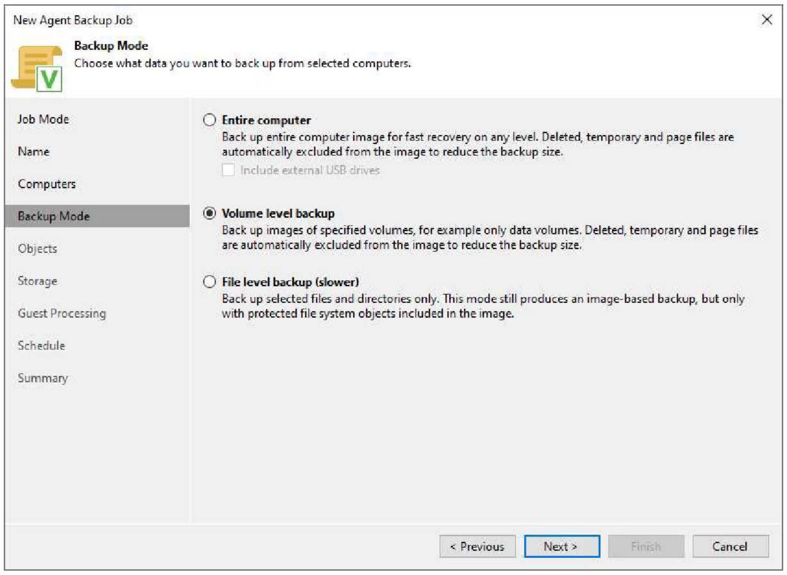
Computers

Select protection groups or individual machines to back up. Protection groups provide a dynamic selection scope that automatically updates the list of protected machines as new ones are discovered.

Protected computers:

Name	Type
Protection Group_Hyper-V Hosts	Protection g...

14. Select Volume level backup mode on the Backup Mode page to back up the specified computer volumes and click Next.



New Agent Backup Job

Backup Mode

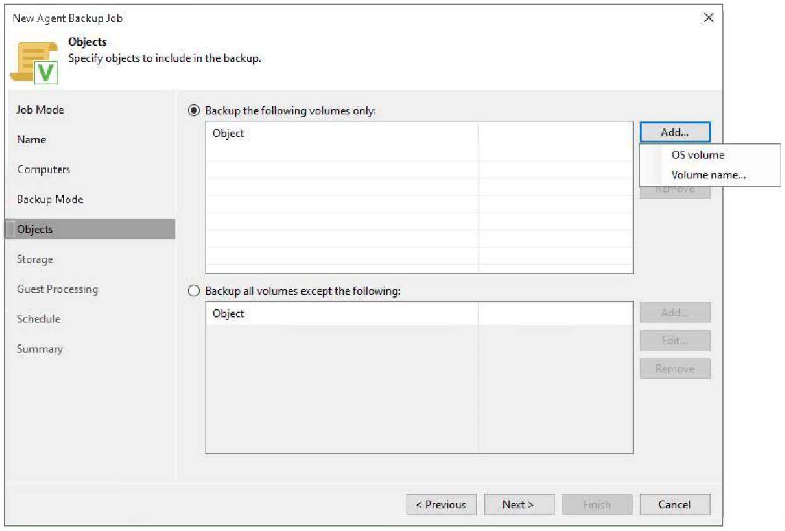
Choose what data you want to back up from selected computers.

○ **Entire computer**
Back up entire computer image for fast recovery on any level. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.
□ Include external USB drives

● **Volume level backup**
Back up images of specified volumes, for example only data volumes. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.

○ **File level backup (slower)**
Back up selected files and directories only. This mode still produces an image-based backup, but only with protected file system objects included in the image.

15. On the Objects page, select Backup the following volumes only.
16. Click Add and select OS volume.
17. Click Next



New Agent Backup Job

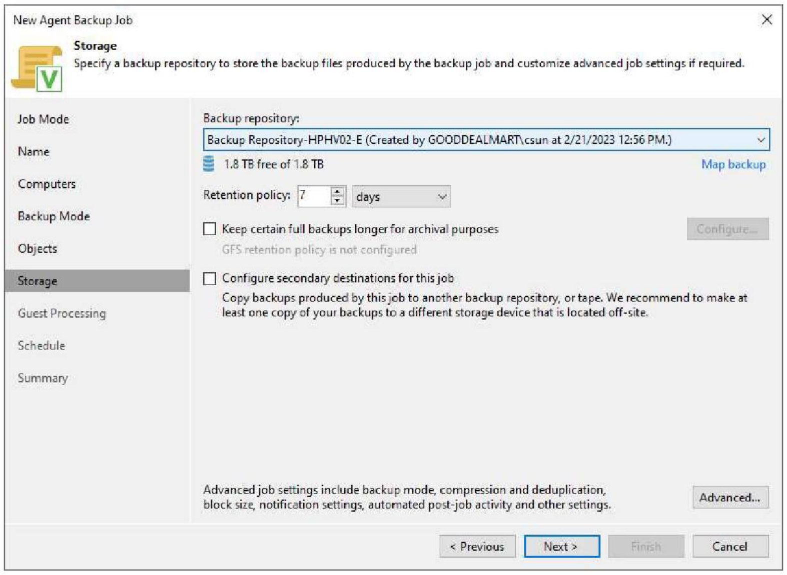
Objects

Specify objects to include in the backup.

● Backup the following volumes only:

○ Backup all volumes except the following:

18. Select the backup repository from the Backup repository drop-down list on the Storage page.



New Agent Backup Job

Storage

Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.

Backup repository:

Backup Repository-HPHV02-E (Created by GOODDEALMART\csun at 2/21/2023 12:56 PM.)

1.8 TB free of 1.8 TB

Retention policy: 7 days

□ Keep certain full backups longer for archival purposes

GFS retention policy is not configured

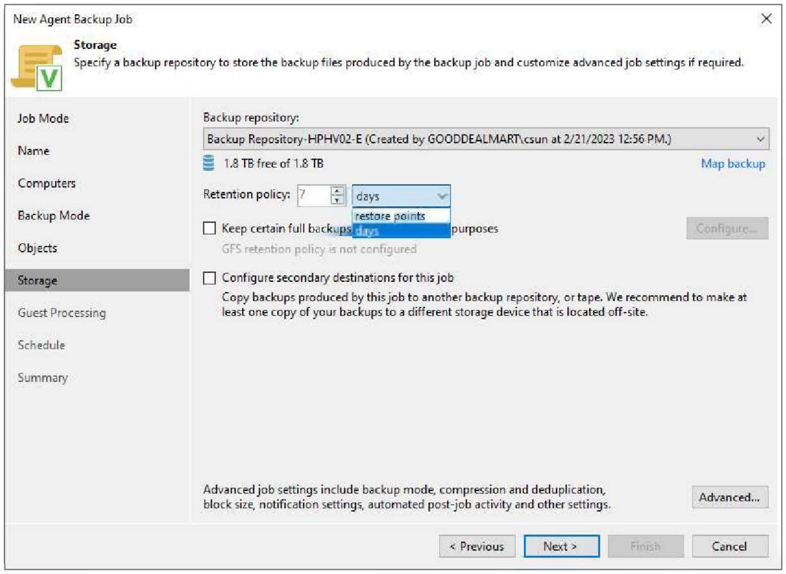
□ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

19. Set the retention policy settings for restore points in the Retention Policy field.

20. Select days or restore points from the drop-down list.


New Agent Backup Job

Storage

Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.

Backup repository: Backup Repository-HPHV02-E (Created by GOODDEALMART\csun at 2/21/2023 12:56 PM.)

1.8 TB free of 1.8 TB

Retention policy: 7 days

□ Keep certain full backups longer for archival purposes

GFS retention policy is not configured

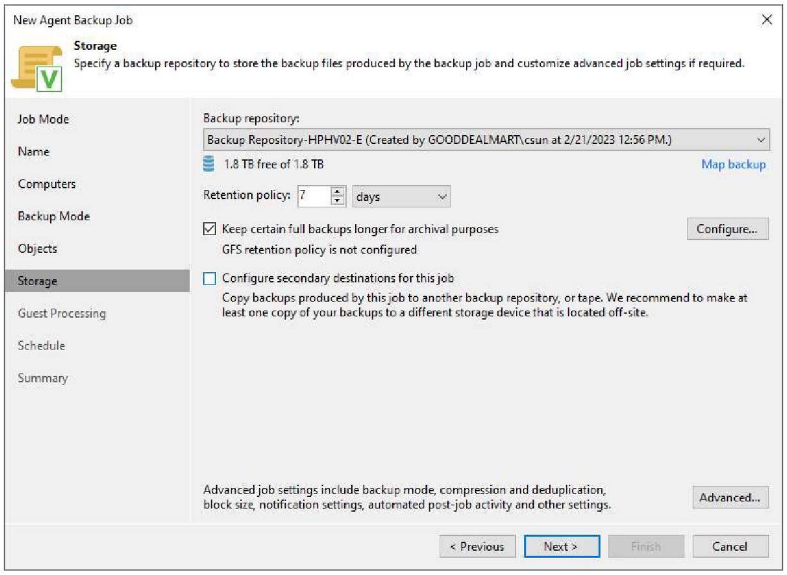
□ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

21. You can configure GFS retention policy settings for the backup job to ignore the short-term retention policy for some full backups and store them for long-term archiving.

22. Select the Keep certain full backups for longer for archival purposes. Then, if you need it, click Configure.


New Agent Backup Job

Storage

Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.

Backup repository: Backup Repository-HPHV02-E (Created by GOODDEALMART\csun at 2/21/2023 12:56 PM.)

1.8 TB free of 1.8 TB

Retention policy: 7 days

☑ Keep certain full backups longer for archival purposes

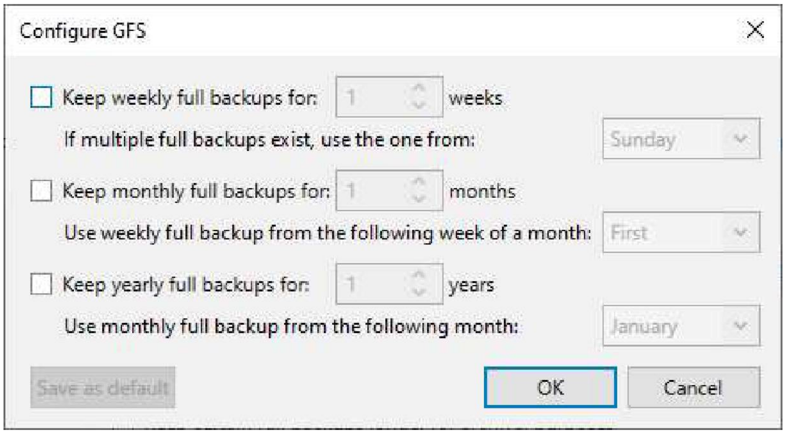
GFS retention policy is not configured

□ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

23. Select the Keep weekly full backups for check box, and specify the number of weeks you want to prevent restore points from being modified and deleted.



Configure GFS

□ Keep weekly full backups for: 1 weeks

If multiple full backups exist, use the one from: Sunday

□ Keep monthly full backups for: 1 months

Use weekly full backup from the following week of a month: First

□ Keep yearly full backups for: 1 years

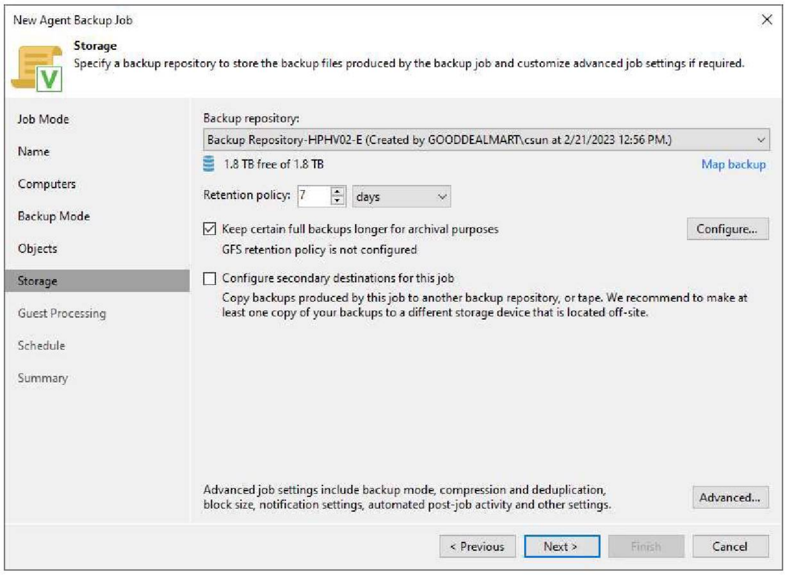
Use monthly full backup from the following month: January

24. Select the Keep monthly full backups for check box, and specify the months you want to prevent restore points from being modified and deleted.

25. Select the Keep yearly full backups for check box, and specify the years you want to prevent restore points from being modified and deleted.

26. Click OK.

27. On the Storage page, click Advanced.



New Agent Backup Job

Storage

Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.

Backup repository: Backup Repository-HPHV02-E (Created by GOODDEALMART\csun at 2/21/2023 12:56 PM.)

1.8 TB free of 1.8 TB

Retention policy: 7 days

☑ Keep certain full backups longer for archival purposes

GFS retention policy is not configured

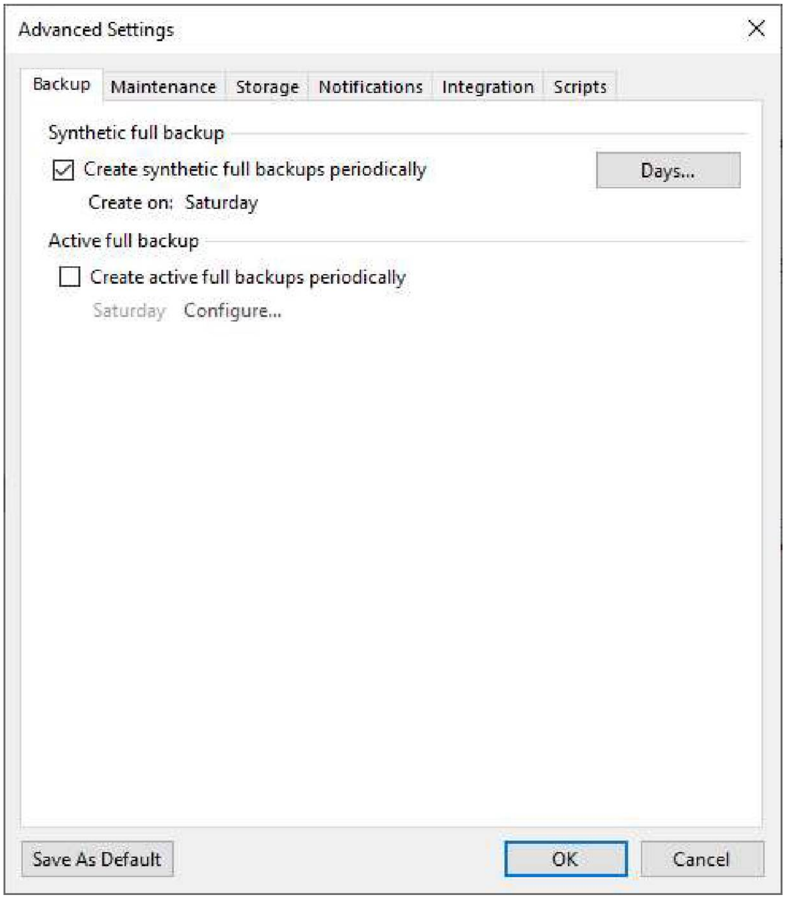
□ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

28. Select Create synthetic full backups or Active full backups periodically checkbox.

29. Schedule full backups periodically and click OK.



Synthetic full backup

☑ Create synthetic full backups periodically

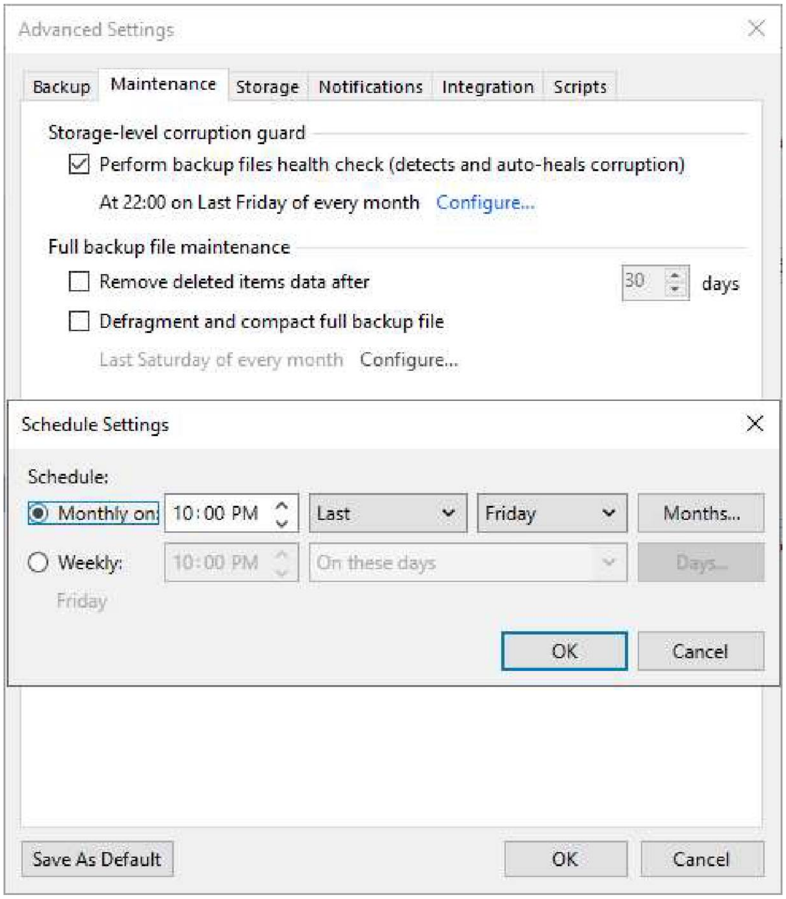
Create on: Saturday

Active full backup

□ Create active full backups periodically

Saturday

30. On the Advanced Settings, select Maintenance.
31. To regularly perform a health check on the backup chain's most recent restore point, select the Perform backup files health check (detects and auto-heals corruption) checkbox in the Storage-level corruption guard section.
32. Click Configure to set a timetable for the health check.



Advanced Settings

Storage-level corruption guard

☑ Perform backup files health check (detects and auto-heals corruption)

At 22:00 on Last Friday of every month Configure...

Full backup file maintenance

□ Remove deleted items data after 30 days

□ Defragment and compact full backup file

Last Saturday of every month Configure...

Schedule Settings

Schedule:

● Monthly on: 10:00 PM Last Friday Months...

○ Weekly: 10:00 PM On these days Days...

Friday

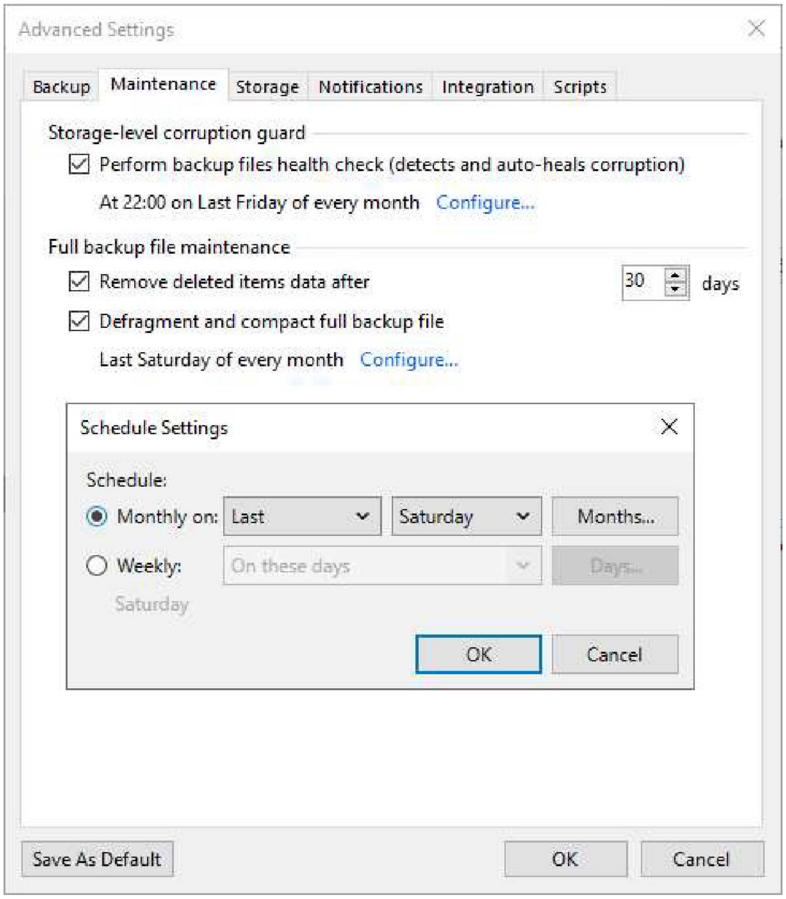
33. Select the Remove deleted items data after the checkbox and enter the few days you want backup data for deleted VMs to be kept.

34. Select the Defragment and compact full backup file checkbox and click Configure.

35. Set the schedule for the compact operation to compact a full backup periodically.

Note:

You don’t need to enable the defragment and compact functionality checkbox if GFS retention is enabled.



Advanced Settings

Storage-level corruption guard

☑ Perform backup files health check (detects and auto-heals corruption)

At 22:00 on Last Friday of every month Configure...

Full backup file maintenance

☑ Remove deleted items data after 30 days

☑ Defragment and compact full backup file

Last Saturday of every month Configure...

Schedule Settings

Schedule:

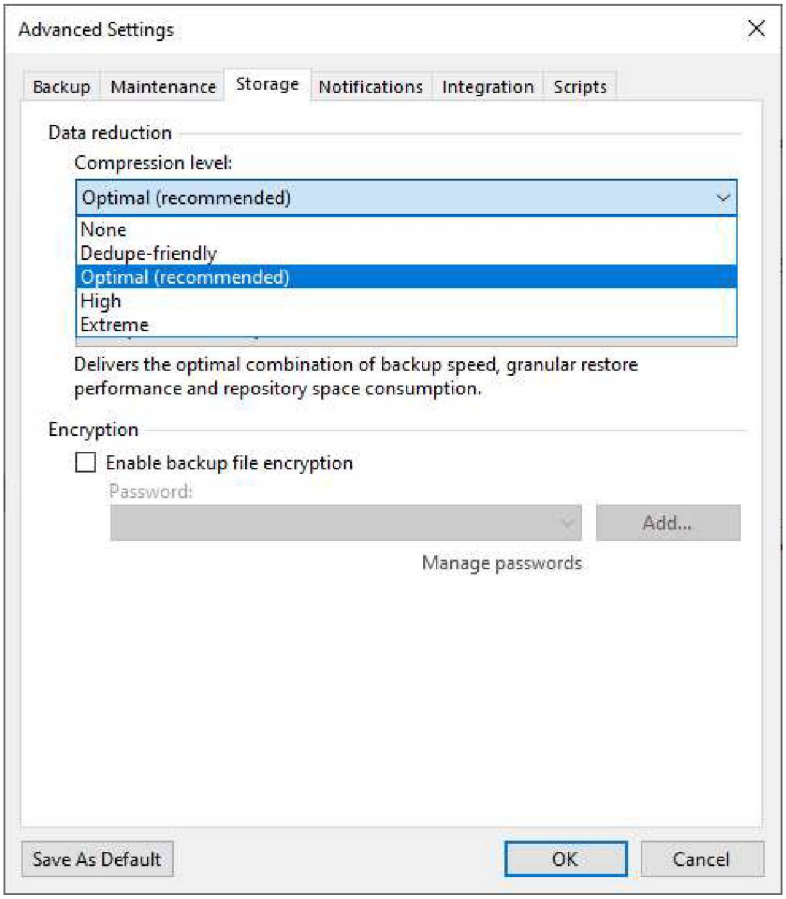
● Monthly on: Last Saturday Months...

○ Weekly: On these days Days...

Saturday

36. On Advanced Settings, select Storage.

37. Select the Compression level from the drop-down list.



Data reduction

Compression level: Optimal (recommended)

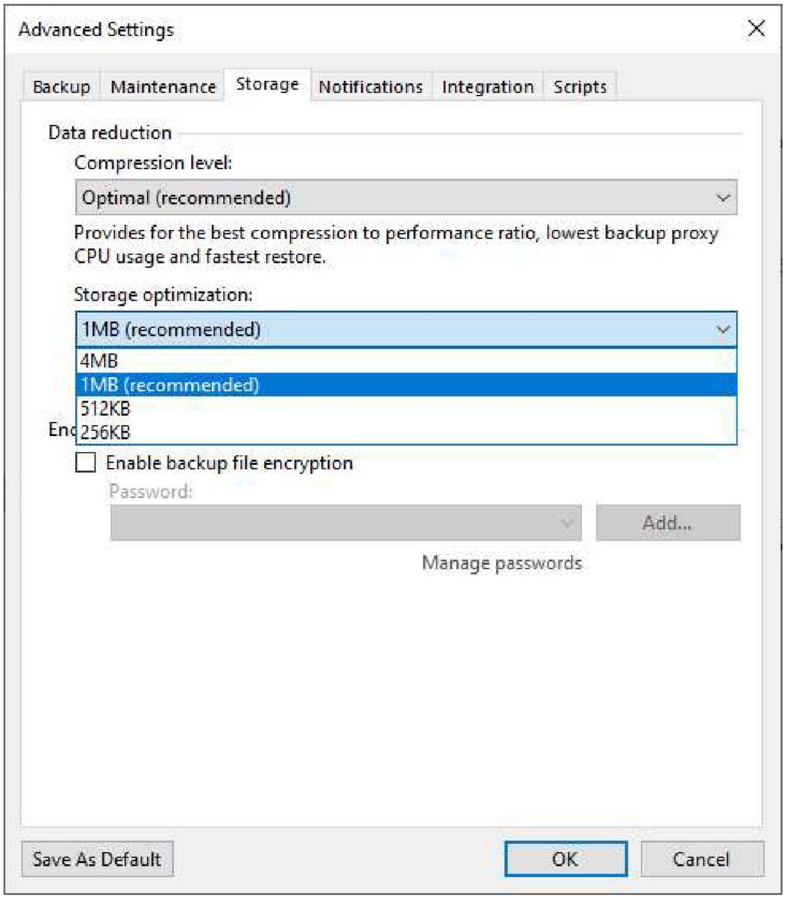
Delivers the optimal combination of backup speed, granular restore performance and repository space consumption.

Encryption

□ Enable backup file encryption

Password:

38. Select Storage optimization from the drop-down list.



Advanced Settings

Data reduction

Compression level: Optimal (recommended)

Provides for the best compression to performance ratio, lowest backup proxy CPU usage and fastest restore.

Storage optimization: 1MB (recommended)

- 4MB
- 1MB (recommended)
- 512KB
- 256KB

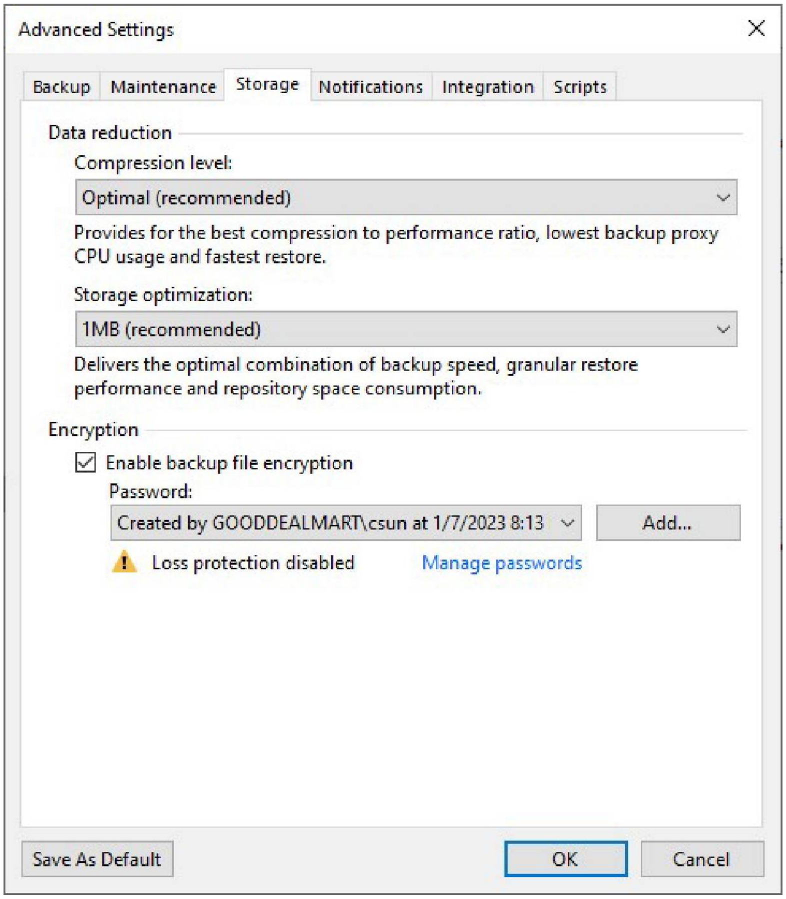
Enc

□ Enable backup file encryption

Password:

39. Select the Enable backup file encryption checkbox to encrypt the content of backup files.

40. Select a password from the drop-down list. Then, if you still need to do, click Add or use the Manage passwords link to create a new password.



Data reduction

Compression level: Optimal (recommended)

Provides for the best compression to performance ratio, lowest backup proxy CPU usage and fastest restore.

Storage optimization: 1MB (recommended)

Delivers the optimal combination of backup speed, granular restore performance and repository space consumption.

Encryption

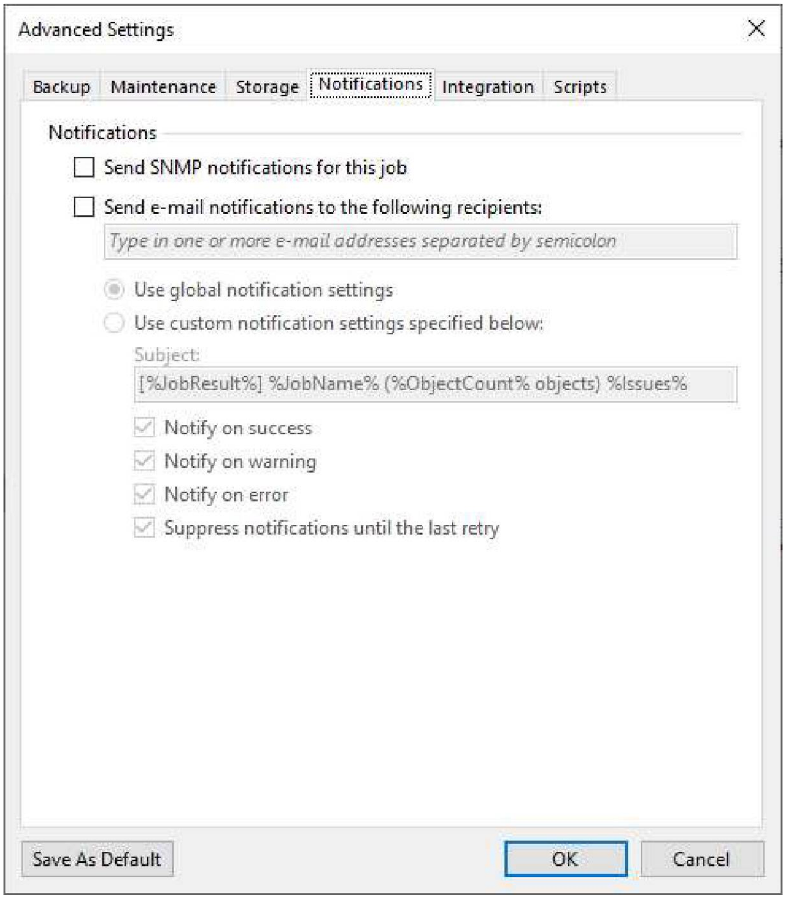
☑ Enable backup file encryption

Password: Created by GOODDEALMART\csun at 1/7/2023 8:13

Loss protection disabled

41. On the Advanced Settings, select Notifications.

42. Keep the default settings.



Advanced Settings

Notifications

□ Send SNMP notifications for this job

□ Send e-mail notifications to the following recipients:

Type in one or more e-mail addresses separated by semicolon

● Use global notification settings

○ Use custom notification settings specified below:

Subject:

[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

☑ Notify on success

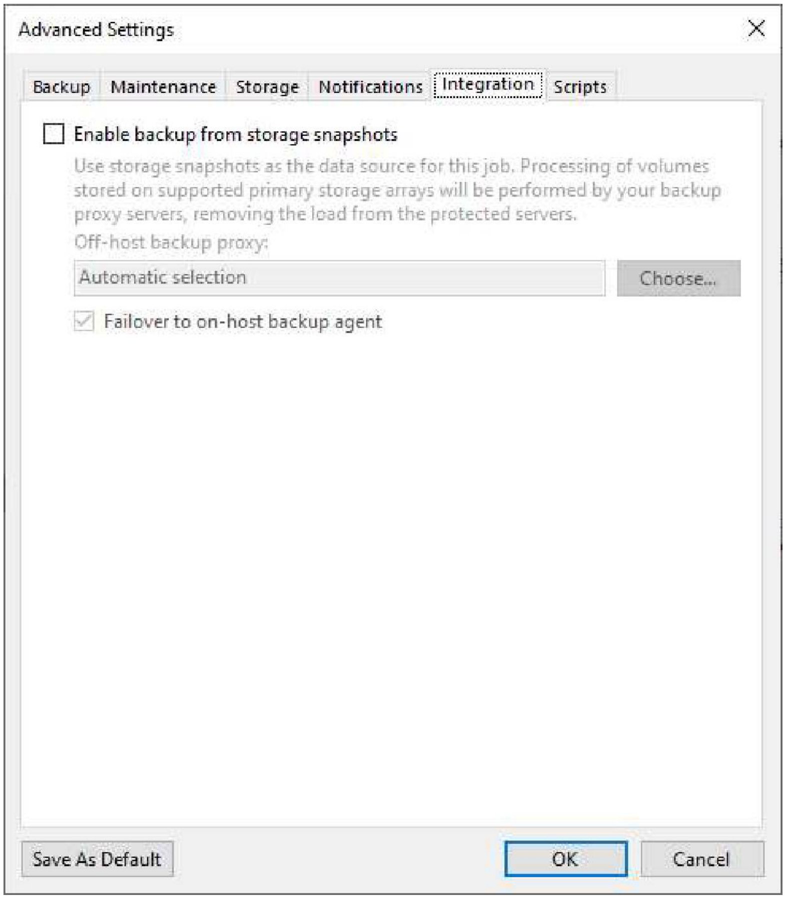
☑ Notify on warning

☑ Notify on error

☑ Suppress notifications until the last retry

43. On the Advanced Settings, select Integration.

44. Keep the default settings.



Advanced Settings

□ Enable backup from storage snapshots

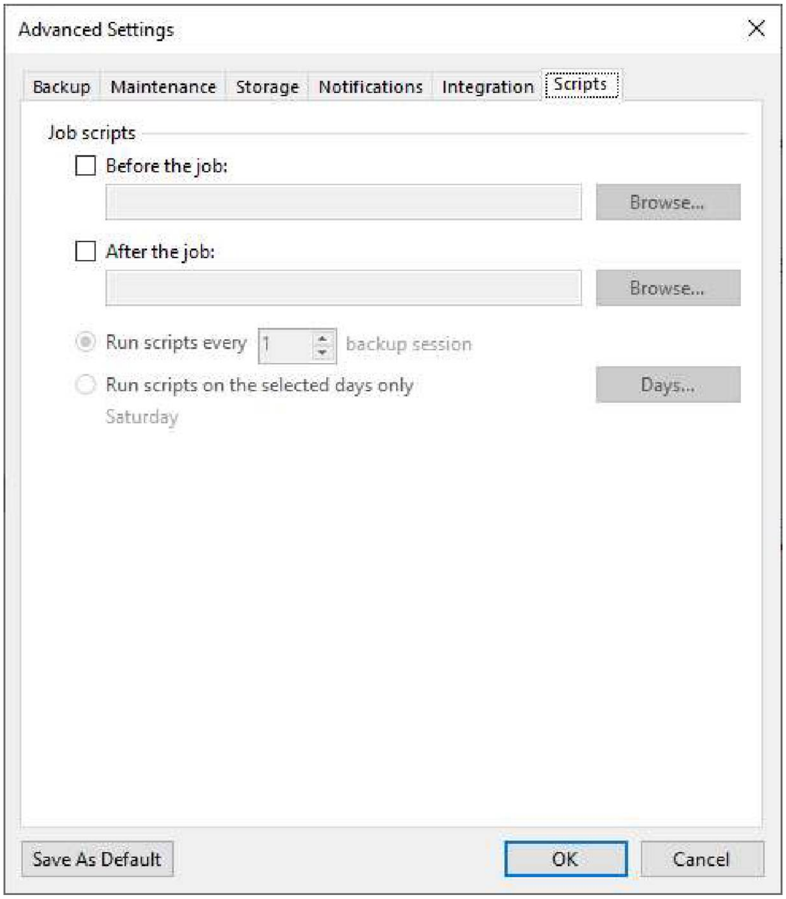
Use storage snapshots as the data source for this job. Processing of volumes stored on supported primary storage arrays will be performed by your backup proxy servers, removing the load from the protected servers.

Off-host backup proxy: Automatic selection

☑ Failover to on-host backup agent

45. On the Advanced Settings page, select Scripts.

46. Keep the default settings and click OK.



Advanced Settings

Job scripts

□ Before the job:

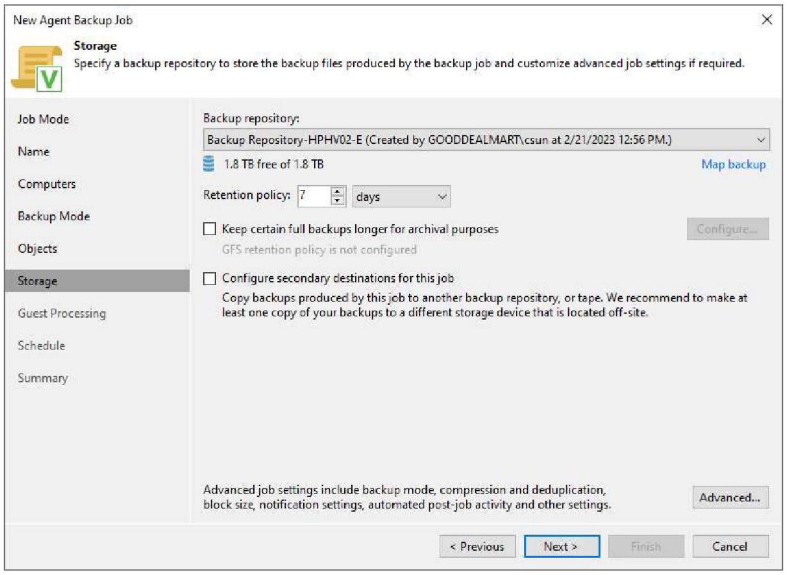
□ After the job:

● Run scripts every 1 backup session

○ Run scripts on the selected days only

Saturday

47. On the Storage page, click Next.



New Agent Backup Job

Storage

Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.

Backup repository:

Backup Repository-HPHV02-E (Created by GOODDEALMART\csun at 2/21/2023 12:56 PM.)

1.8 TB free of 1.8 TB

Retention policy: 7 days

☐ Keep certain full backups longer for archival purposes

GFS retention policy is not configured

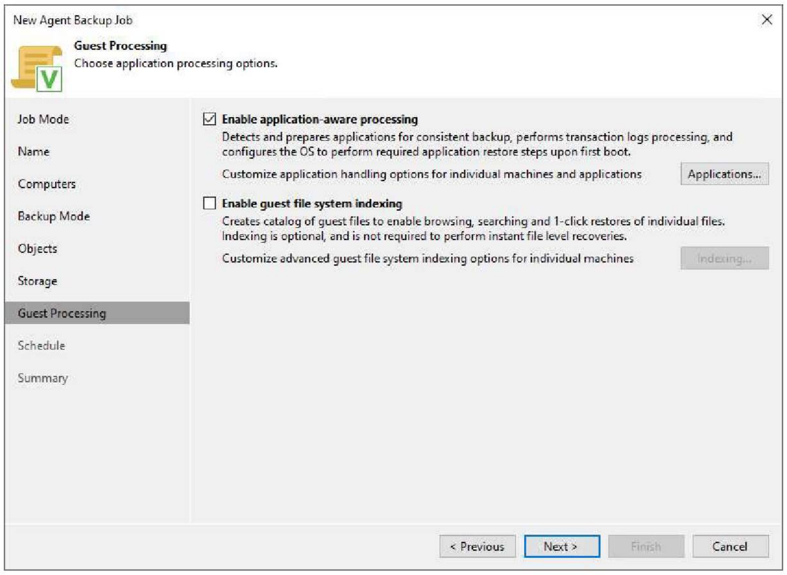
☐ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

48. When you add Physical machines running VSS-aware applications to the backup job, you can enable application-aware processing to create a transactionally consistent backup. The transactionally consistent backup ensures that applications on VMs can be recovered without data loss.

49. Select the Enable application-aware processing checkbox on the Guest Processing



New Agent Backup Job

Guest Processing

Choose application processing options.

☑ **Enable application-aware processing**

Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

Customize application handling options for individual machines and applications

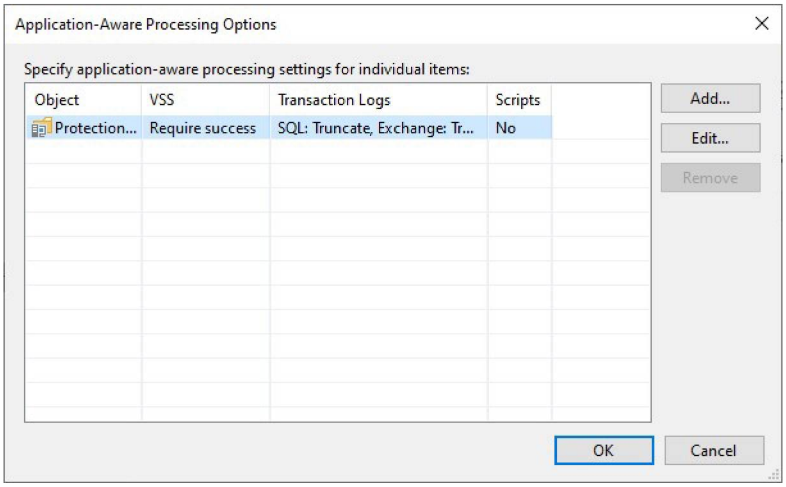
☐ **Enable guest file system indexing**

Creates catalog of guest files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries.

Customize advanced guest file system indexing options for individual machines

page, and click Applications.

50. On the Application-Aware Processing Options page, select the Object and click Edit.



Application-Aware Processing Options

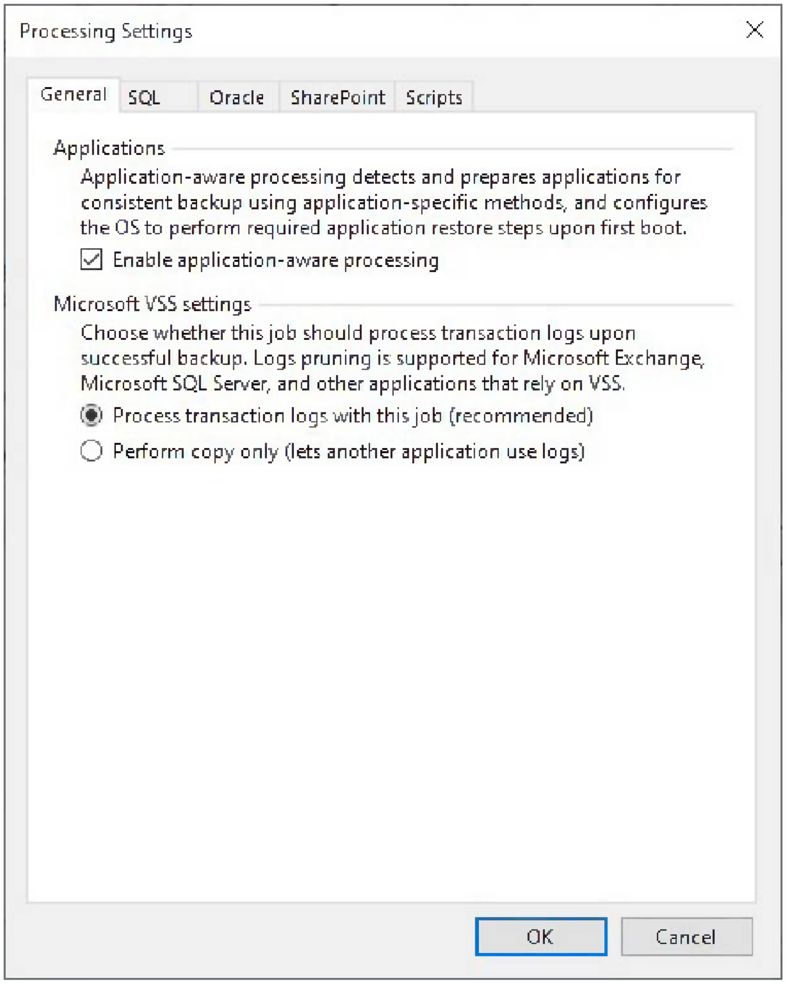
Specify application-aware processing settings for individual items:

Object	VSS	Transaction Logs	Scripts
Protection...	Require success	SQL: Truncate, Exchange: Tr...	No

51. On the Processing Settings page, select General.

52. Select Enable application-aware processing checkbox.

53. Select Process transaction logs with this job (recommended).



Applications

Application-aware processing detects and prepares applications for consistent backup using application-specific methods, and configures the OS to perform required application restore steps upon first boot.

☑ Enable application-aware processing

Microsoft VSS settings

Choose whether this job should process transaction logs upon successful backup. Logs pruning is supported for Microsoft Exchange, Microsoft SQL Server, and other applications that rely on VSS.

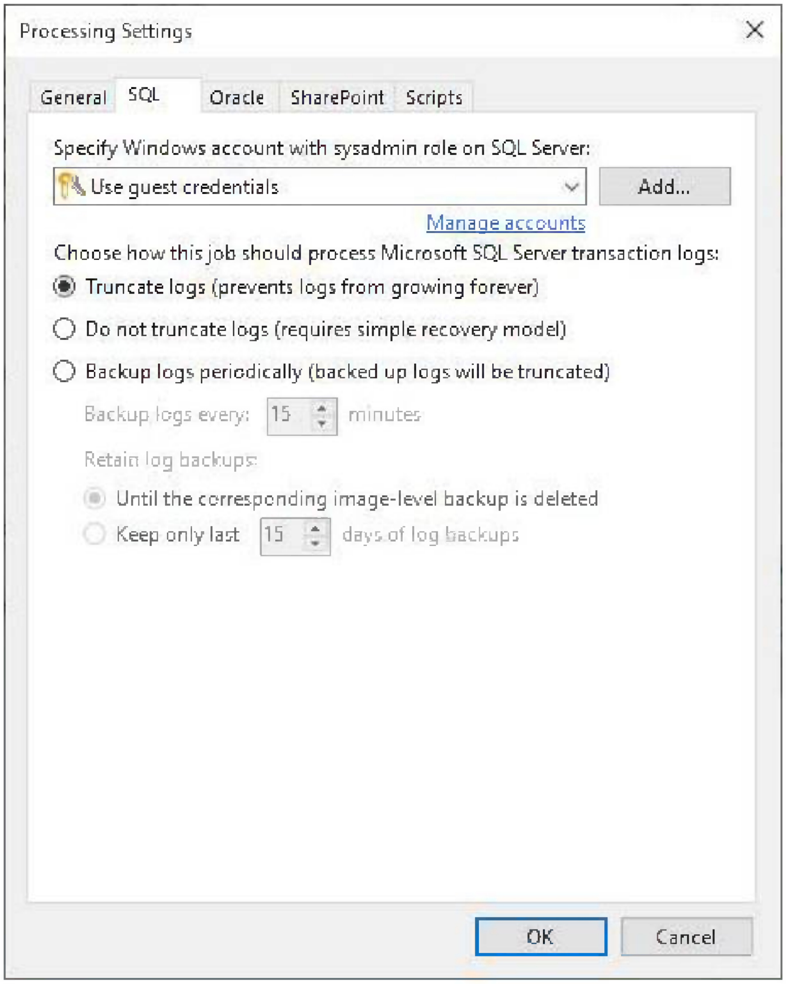
● Process transaction logs with this job (recommended)

○ Perform copy only (lets another application use logs)

54. On the Processing Settings page, click SQL if the Physical Machine is a Microsoft SQL Server.

55. Select a user account from the drop-down list.

56. Select Truncate logs (Prevents logs from growing forever).



Specify Windows account with sysadmin role on SQL Server:

Use guest credentials

Choose how this job should process Microsoft SQL Server transaction logs:

● Truncate logs (prevents logs from growing forever)

○ Do not truncate logs (requires simple recovery model)

○ Backup logs periodically (backed up logs will be truncated)

Backup logs every: 15 minutes

Retain log backups:

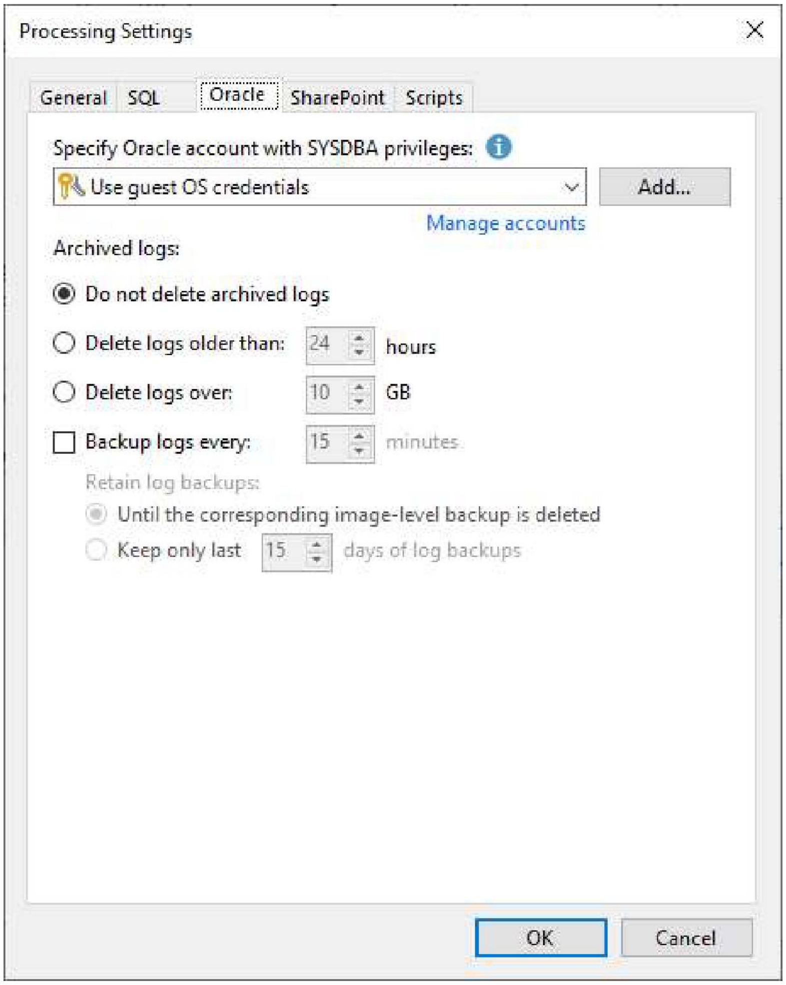
● Until the corresponding image-level backup is deleted

○ Keep only last 15 days of log backups

57. Select Oracle on the Processing Settings page if the Physical Machine is an Oracle Server.

58. Select a user account from the drop-down list.

59. Select Do not delete archived logs.



Processing Settings

Specify Oracle account with SYSDBA privileges:

Use guest OS credentials

Archived logs:

● Do not delete archived logs

○ Delete logs older than: 24 hours

○ Delete logs over: 10 GB

□ Backup logs every: 15 minutes

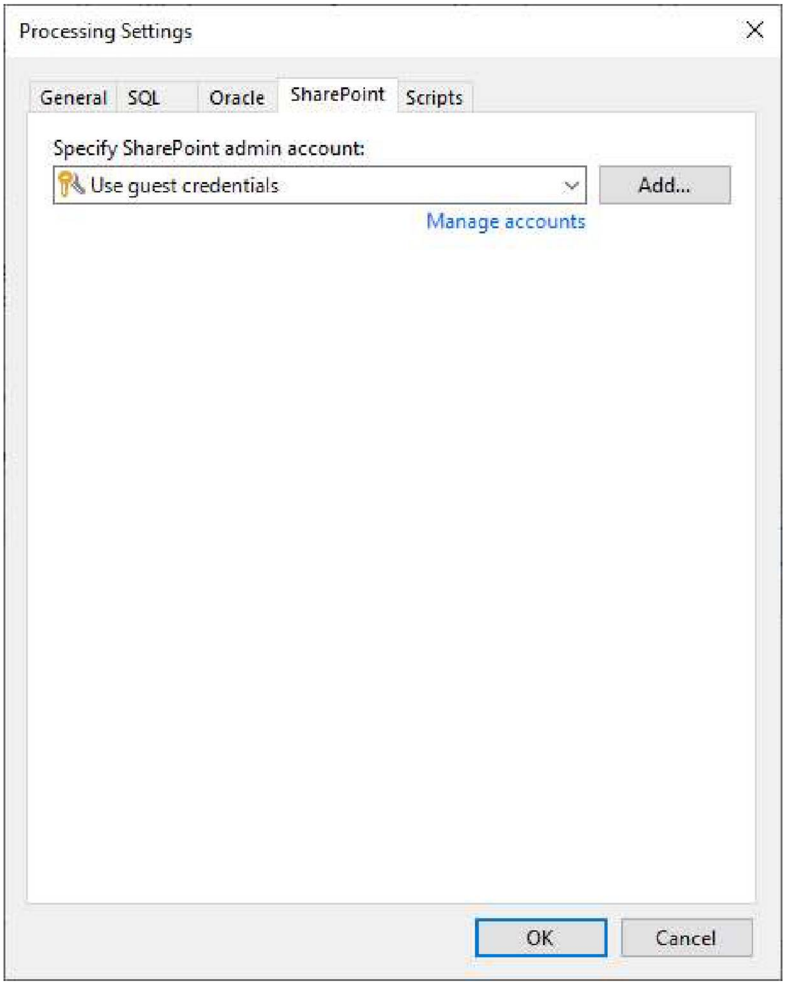
Retain log backups:

● Until the corresponding image-level backup is deleted

○ Keep only last 15 days of log backups

60. On the Processing Settings page, select SharePoint if the Physical Machine is a SharePoint Server.

61. Select a user account from the drop-down list.



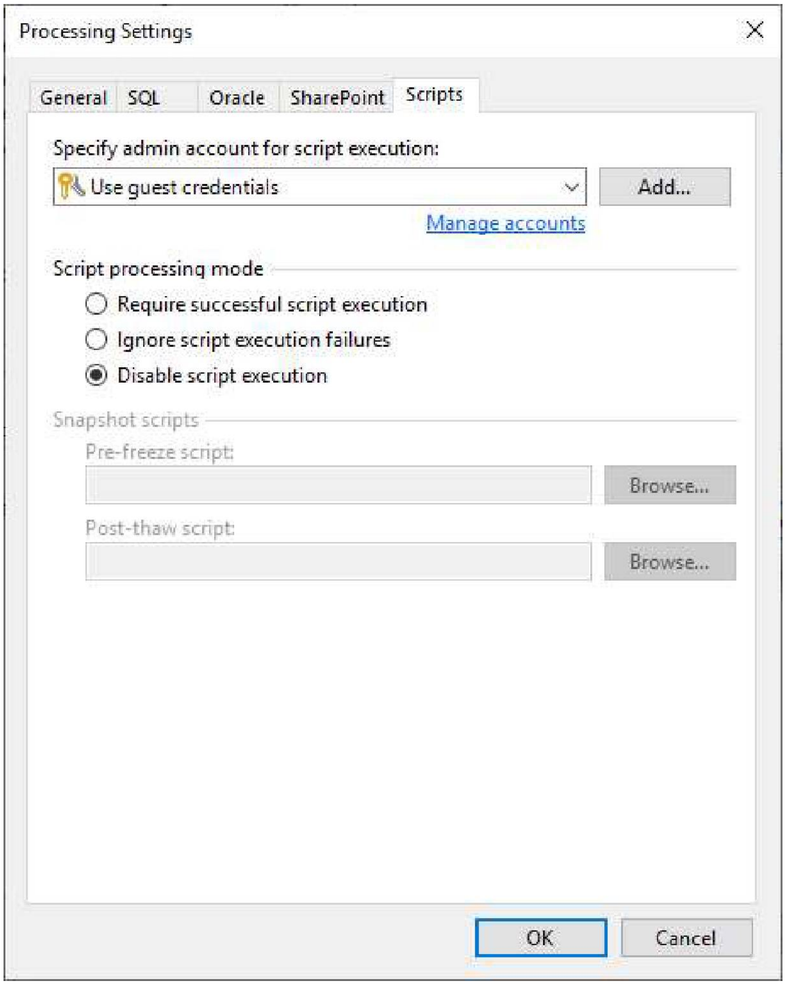
Processing Settings

Specify SharePoint admin account:

Use guest credentials

62. On the Processing Settings page, select Scripts.

63. Keep the default settings and click OK.



Processing Settings

Specify admin account for script execution: Use guest credentials

Script processing mode

○ Require successful script execution

○ Ignore script execution failures

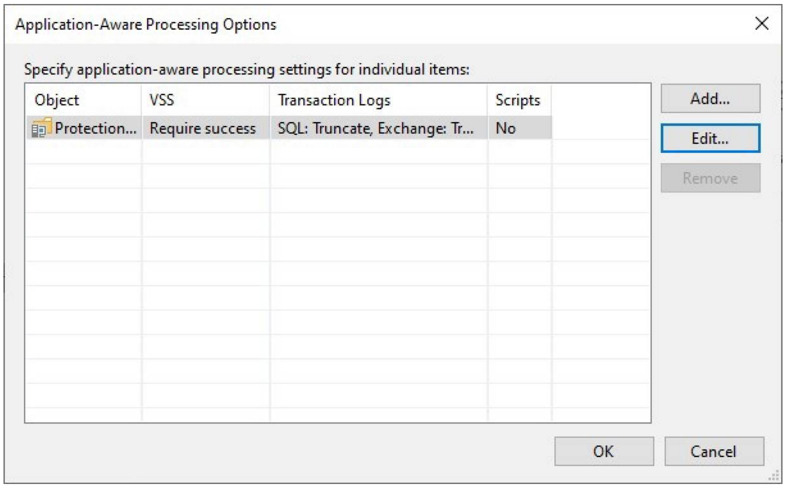
● Disable script execution

Snapshot scripts

Pre-freeze script:

Post-thaw script:

64. On the Application-Aware Processing Options page, click OK.

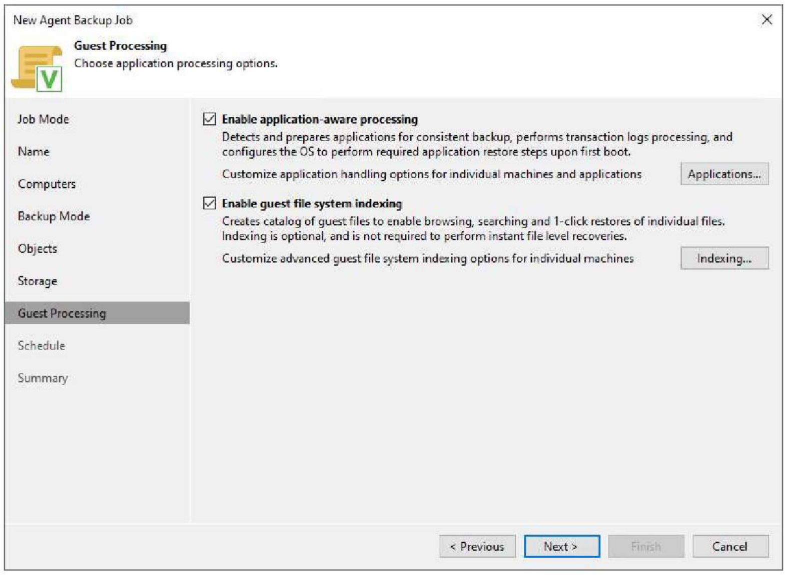


Application-Aware Processing Options

Specify application-aware processing settings for individual items:

Object	VSS	Transaction Logs	Scripts
Protection...	Require success	SQL: Truncate, Exchange: Tr...	No

65. Select the Enable guest file system indexing checkbox and click Indexing.



New Agent Backup Job

Guest Processing

Choose application processing options.

☑ **Enable application-aware processing**

Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

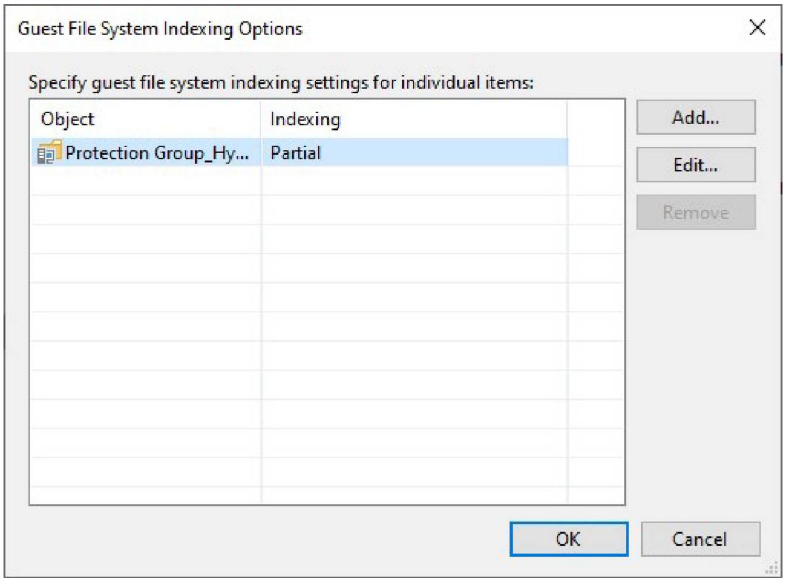
Customize application handling options for individual machines and applications

☑ **Enable guest file system indexing**

Creates catalog of guest files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries.

Customize advanced guest file system indexing options for individual machines

66. On the Guest File System Indexing Options page, select the Object, click Edit and.



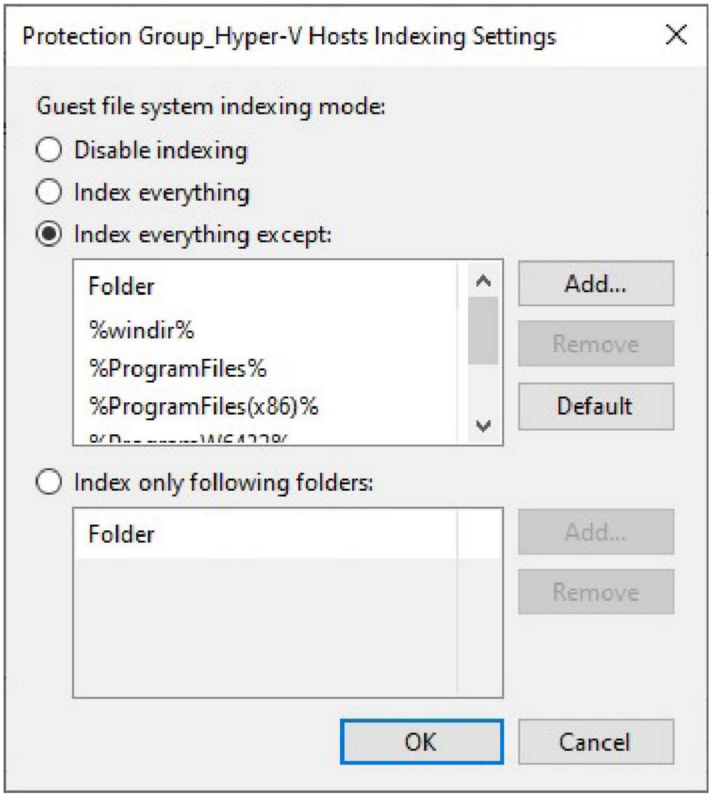
Guest File System Indexing Options

Specify guest file system indexing settings for individual items:

Object	Indexing
Protection Group_Hy...	Partial

67. On the Guest file system indexing mode page, keep the default settings.

68. Click OK.



Protection Group_Hyper-V Hosts Indexing Settings

Guest file system indexing mode:

○ Disable indexing

○ Index everything

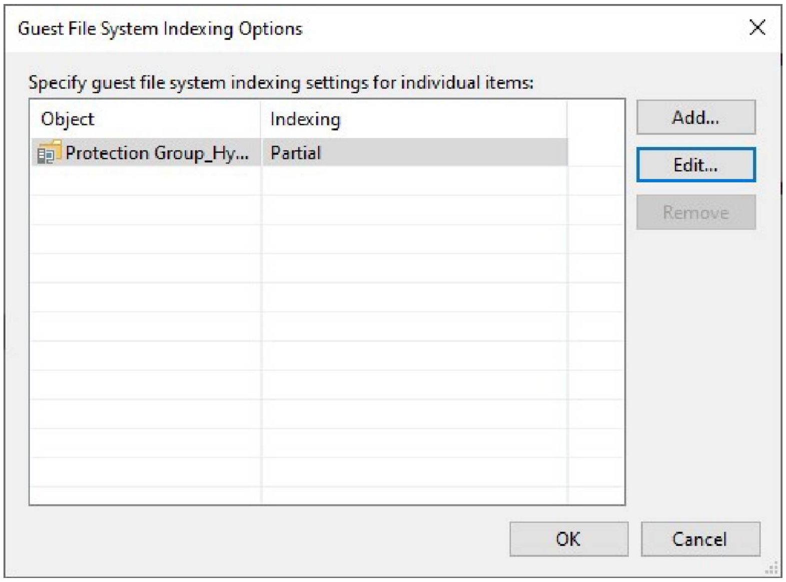
● Index everything except:

Folder
%windir%
%ProgramFiles%
%ProgramFiles(x86)%

○ Index only following folders:

Folder

69. On the Guest File System Indexing Options page, click OK.

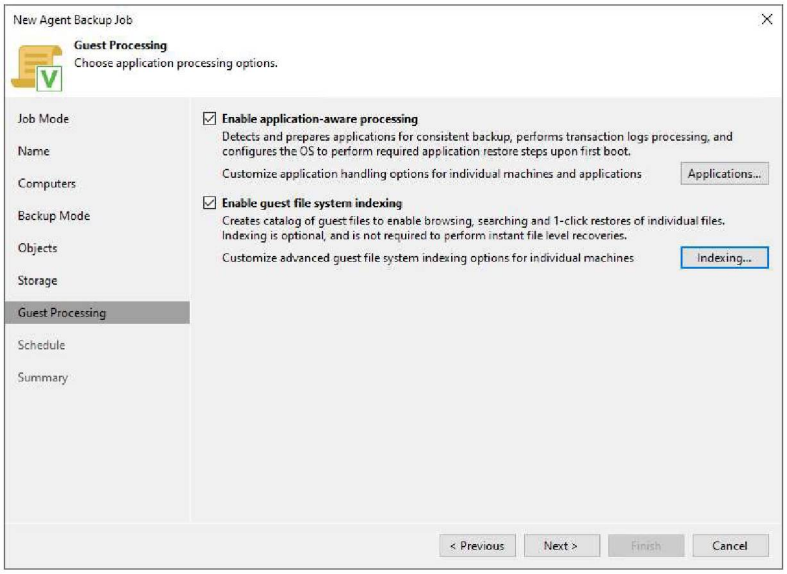


Guest File System Indexing Options

Specify guest file system indexing settings for individual items:

Object	Indexing
Protection Group_Hy...	Partial

70. On the Guest Processing page, click Next.



New Agent Backup Job

Guest Processing

Choose application processing options.

☑ **Enable application-aware processing**

Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

Customize application handling options for individual machines and applications

☑ **Enable guest file system indexing**

Creates catalog of guest files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries.

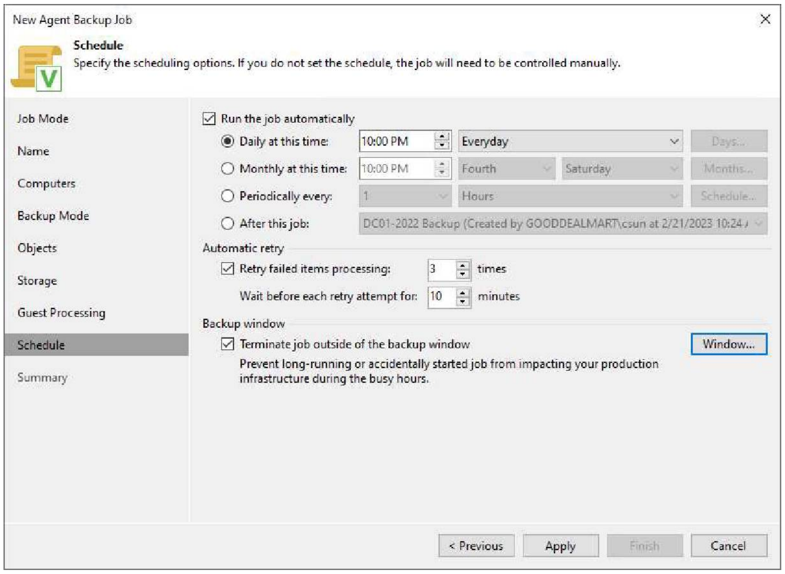
Customize advanced guest file system indexing options for individual machines

71. Select Run the job automatically checkbox on the Schedule page and select your specified schedule.

72. Define whether Veeam Backup & Replication should retry the backup job if it fails in the Automatic retry section.

73. Define the time interval the backup job must complete in the Backup window section. The backup window ensures that the job does not overlap with production hours and that there is no unnecessary overhead on the production environment.

74. Click Apply.



New Agent Backup Job

Schedule

Specify the scheduling options. If you do not set the schedule, the job will need to be controlled manually.

☑ Run the job automatically

● Daily at this time: 10:00 PM Everyday

○ Monthly at this time: 10:00 PM Fourth Saturday

○ Periodically every: 1 Hours

○ After this job: DC01-2022 Backup (Created by GOODDEALMART\csun at 2/21/2023 10:24 /

Automatic retry

☑ Retry failed items processing: 3 times

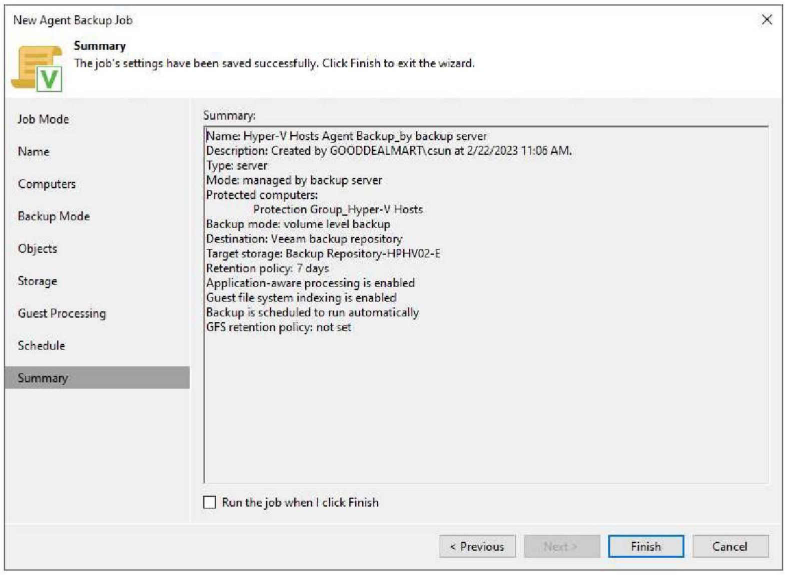
Wait before each retry attempt for: 10 minutes

Backup window

☑ Terminate job outside of the backup window

Prevent long-running or accidentally started job from impacting your production infrastructure during the busy hours.

75. On the Summary page, click Finish.



Summary

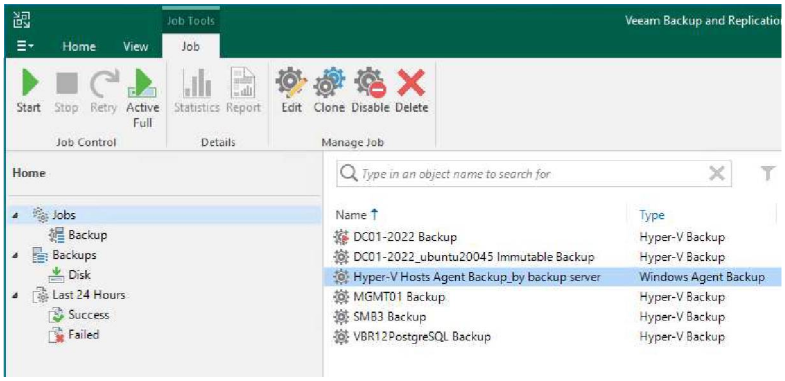
The job's settings have been saved successfully. Click Finish to exit the wizard.

Summary:

```
Name: Hyper-V Hosts Agent Backup_by backup server
Description: Created by GOODDEALMART\csun at 2/22/2023 11:06 AM.
Type: server
Mode: managed by backup server
Protected computers:
          Protection Group_Hyper-V Hosts
Backup mode: volume level backup
Destination: Veeam backup repository
Target storage: Backup Repository-HPHV02-E
Retention policy: 7 days
Application-aware processing is enabled
Guest file system indexing is enabled
Backup is scheduled to run automatically
GFS retention policy: not set
```

☐ Run the job when I click Finish

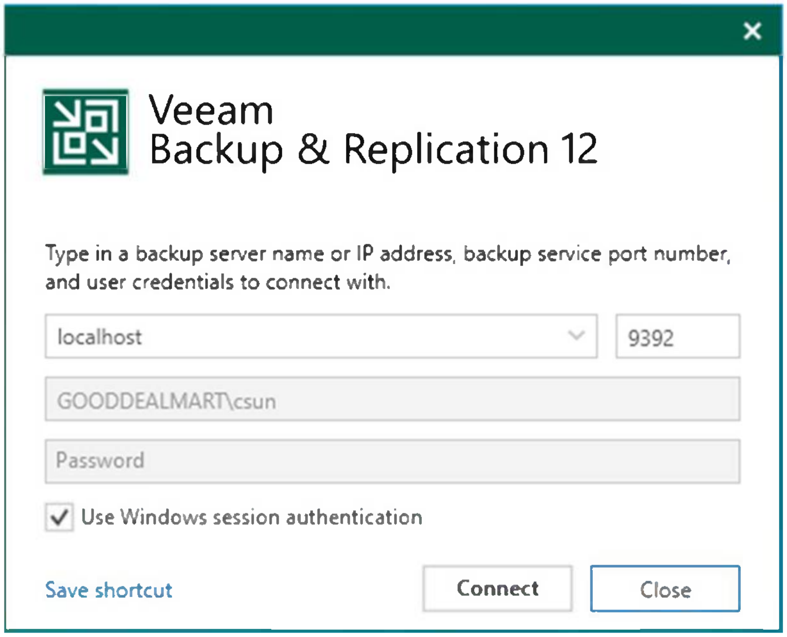
76. Verify that the backup job has been added



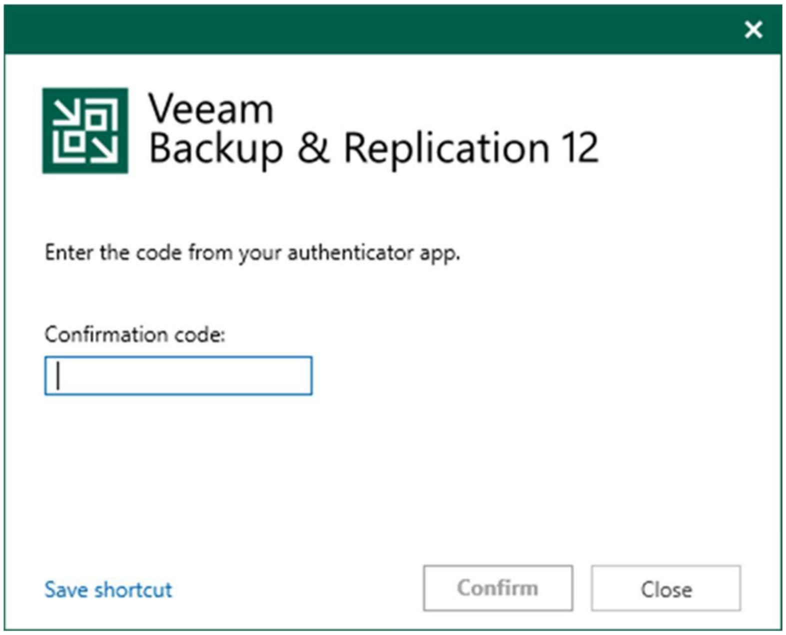
Name ↑	Type
DC01-2022 Backup	Hyper-V Backup
DC01-2022_ubuntu20045 Immutable Backup	Hyper-V Backup
Hyper-V Hosts Agent Backup_by backup server	Windows Agent Backup
MGMT01 Backup	Hyper-V Backup
SMB3 Backup	Hyper-V Backup
VBR12PostgreSQL Backup	Hyper-V Backup

Create a Backup job to backup the specified Physical Machines (Managed by Agent Mode)

This procedure uses the managed backup server mode to create a backup job to back up the specific physical production machines.

Instructions	Screenshot (if applicable)
1. Log in to the Veeam Backup and replication manager server. 2. Open the Veeam Backup & Replication Console and click Connect.	 Veeam Backup & Replication 12 Type in a backup server name or IP address, backup service port number, and user credentials to connect with. localhost 9392 GOODDEALMART\csun Password ☑ Use Windows session authentication Save shortcut Connect Close

3. Enter the MFA Confirmation code and click Confirm.



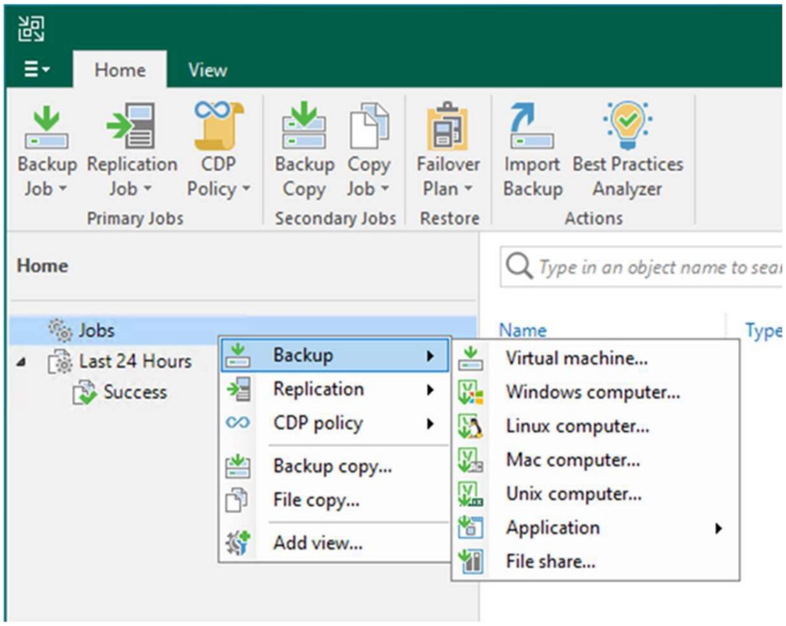
Veeam Backup & Replication 12

Enter the code from your authenticator app.

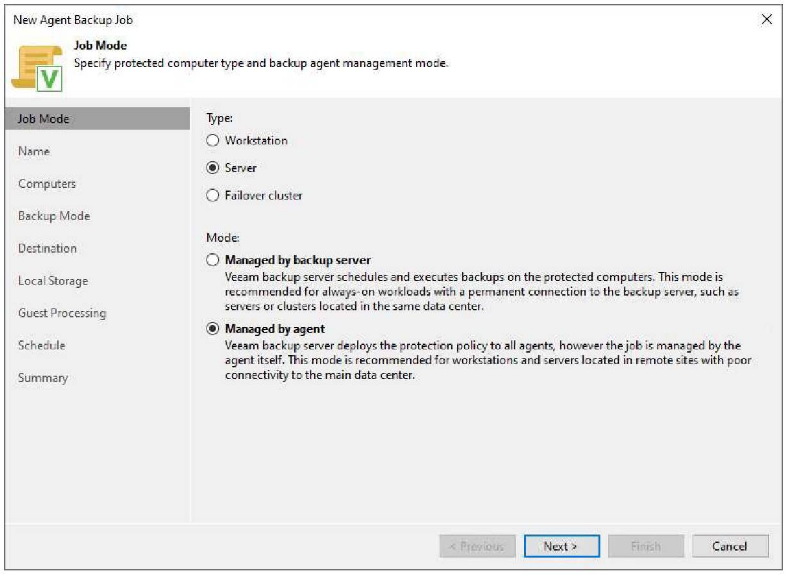
Confirmation code:

4. Select Jobs on the Home page and right-click Jobs.

5. Select Backup and click Windows computer.



6. On the Job Mode page, select Managed by agent mode and click Next.



Job Mode

Specify protected computer type and backup agent management mode.

Type:

○ Workstation

● Server

○ Failover cluster

Mode:

○ **Managed by backup server**

Veeam backup server schedules and executes backups on the protected computers. This mode is recommended for always-on workloads with a permanent connection to the backup server, such as servers or clusters located in the same data center.

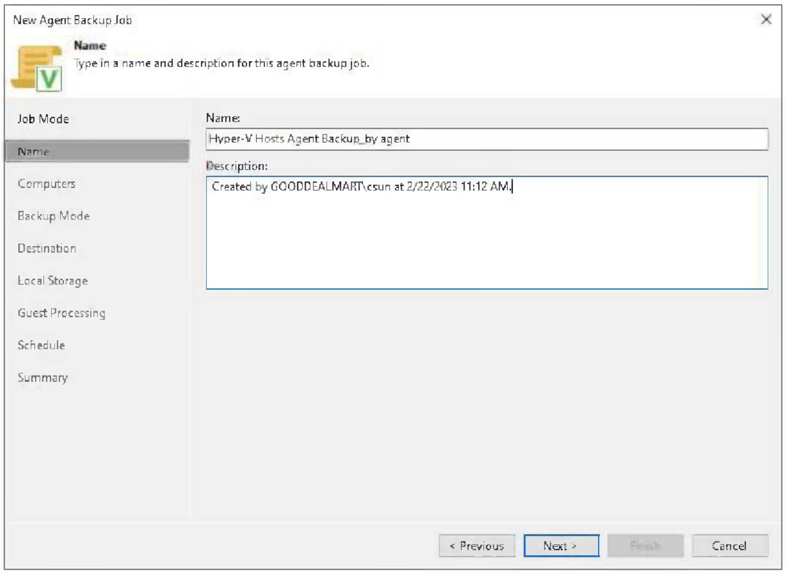
● **Managed by agent**

Veeam backup server deploys the protection policy to all agents, however the job is managed by the agent itself. This mode is recommended for workstations and servers located in remote sites with poor connectivity to the main data center.

7. On the Name page, enter a name for the backup job in the Name field.

8. Give a brief description in the Description field for the future.

9. Click Next.



Name

Type in a name and description for this agent backup job.

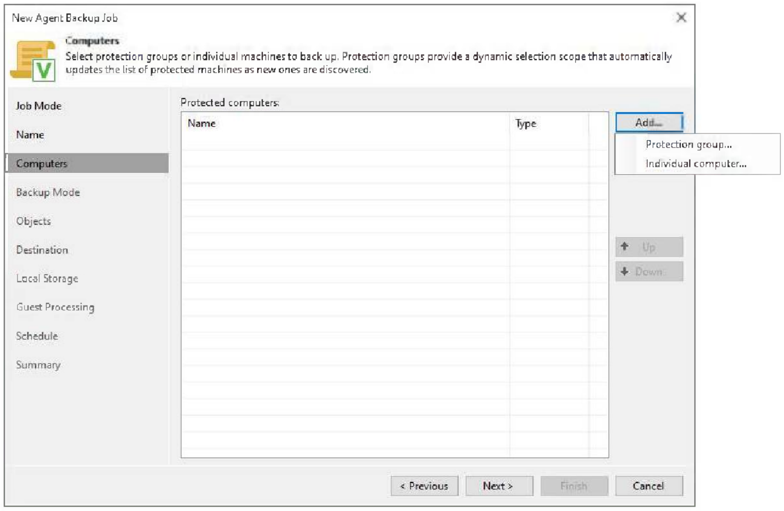
Name:

Hyper-V Hosts Agent Backup_by agent

Description:

Created by GOODDEALMART\csun at 2/22/2023 11:12 AM.

10. On the Computers page, click Add and select Protection group.



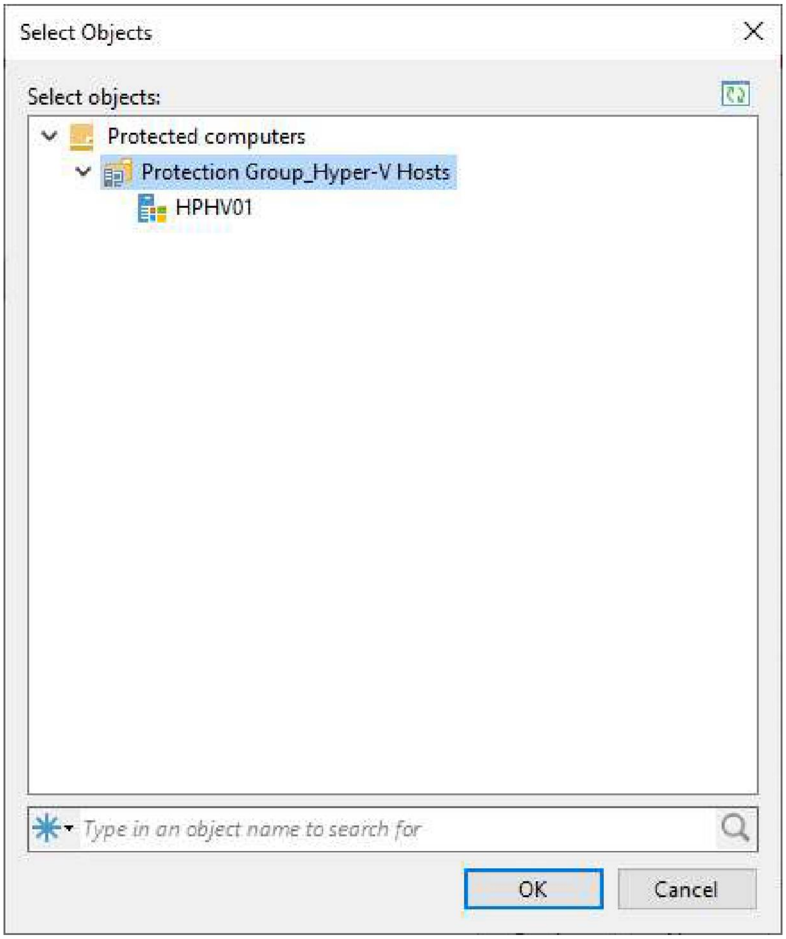
New Agent Backup Job

Computers

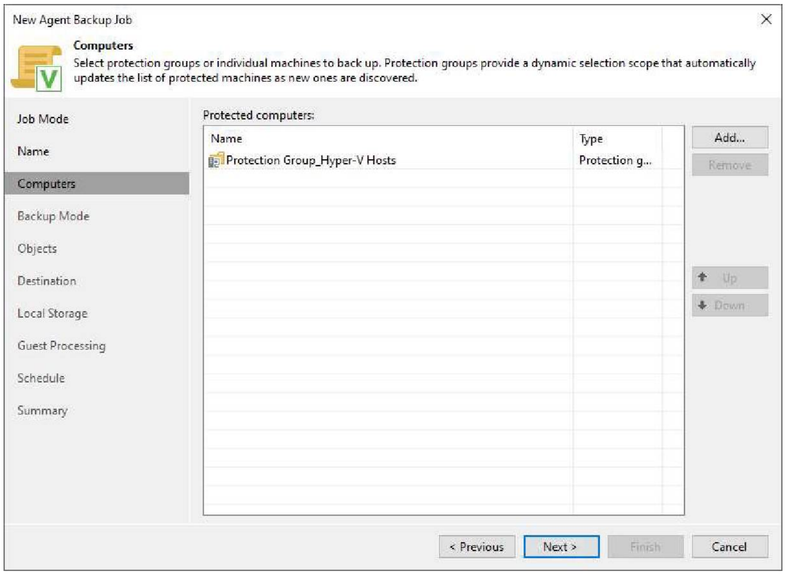
Select protection groups or individual machines to back up. Protection groups provide a dynamic selection scope that automatically updates the list of protected machines as new ones are discovered.

11. Select the protection group on the Select Objects page and click OK.

12. You can select multiple protection groups for the same backup job and repeat the step to add them.


Select Objects
Select objects:
Protected computers
Protection Group_Hyper-V Hosts
HPHV01
Type in an object name to search for
OK
Cancel

13. Click Next on the Computers page.



New Agent Backup Job

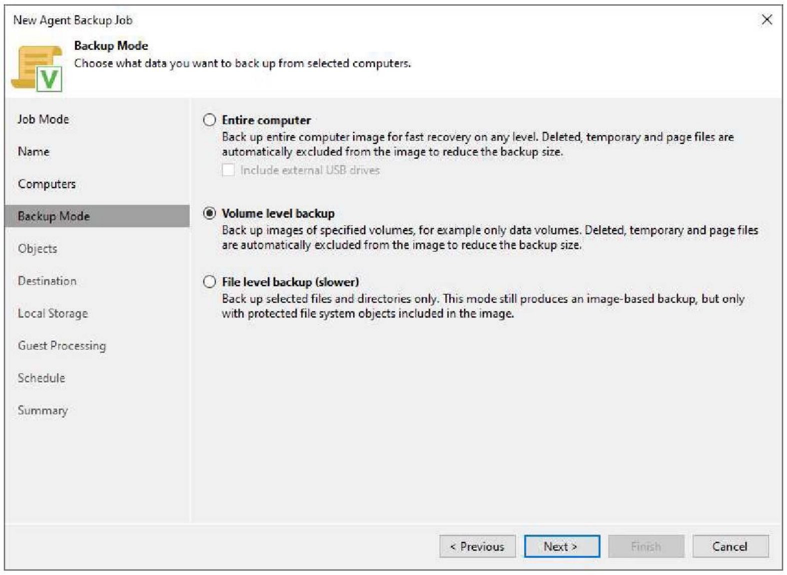
Computers

Select protection groups or individual machines to back up. Protection groups provide a dynamic selection scope that automatically updates the list of protected machines as new ones are discovered.

Protected computers:

Name	Type
Protection Group_Hyper-V Hosts	Protection g...

14. Select Volume level backup mode on the Backup Mode page to back up the specified computer volumes and click Next.



New Agent Backup Job

Backup Mode

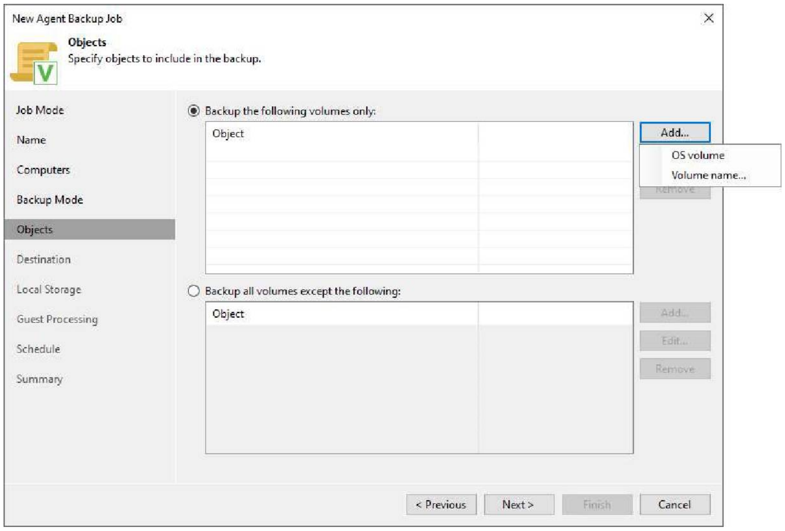
Choose what data you want to back up from selected computers.

○ **Entire computer**
Back up entire computer image for fast recovery on any level. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.
□ Include external USB drives

● **Volume level backup**
Back up images of specified volumes, for example only data volumes. Deleted, temporary and page files are automatically excluded from the image to reduce the backup size.

○ **File level backup (slower)**
Back up selected files and directories only. This mode still produces an image-based backup, but only with protected file system objects included in the image.

15. On the Objects page, select Backup the following volumes only.
16. Click Add and select OS volume.
17. Click Next



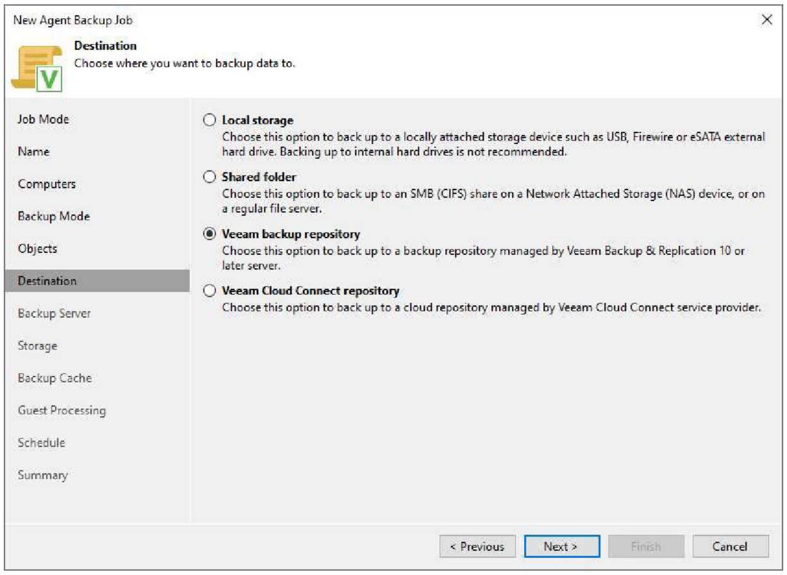
New Agent Backup Job

Objects
Specify objects to include in the backup.

● Backup the following volumes only:

○ Backup all volumes except the following:

18. Select the Veeam backup repository and click Next.



New Agent Backup Job

Destination
Choose where you want to backup data to.

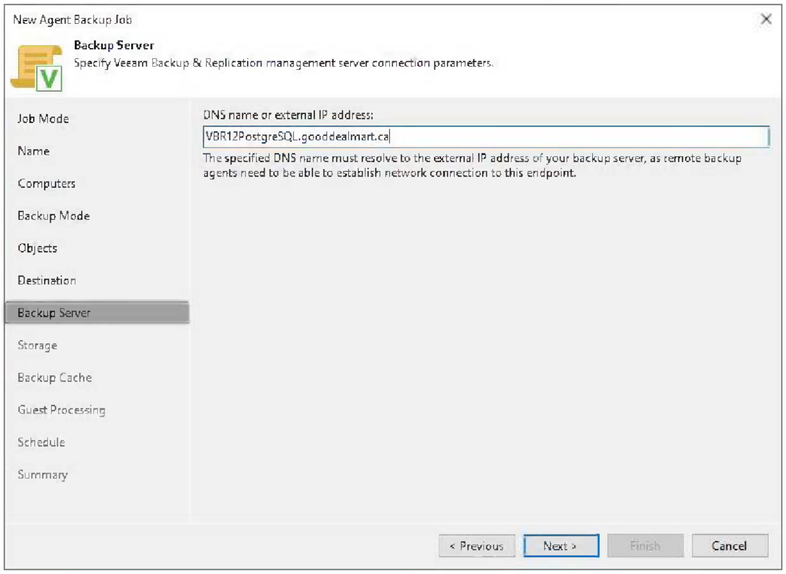
○ **Local storage**
Choose this option to back up to a locally attached storage device such as USB, Firewire or eSATA external hard drive. Backing up to internal hard drives is not recommended.

○ **Shared folder**
Choose this option to back up to an SMB (CIFS) share on a Network Attached Storage (NAS) device, or on a regular file server.

● **Veeam backup repository**
Choose this option to back up to a backup repository managed by Veeam Backup & Replication 10 or later server.

○ **Veeam Cloud Connect repository**
Choose this option to back up to a cloud repository managed by Veeam Cloud Connect service provider.

19. Enter the Veeam Backup and Replication manager server name or IP address in the DNS name or external IP address field on the Backup Server page.



New Agent Backup Job

Backup Server

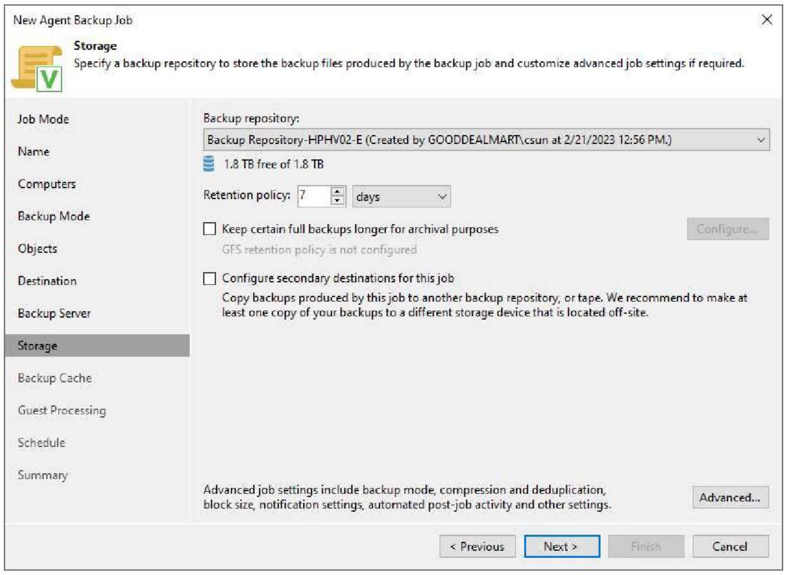
Specify Veeam Backup & Replication management server connection parameters.

DNS name or external IP address:

VBR12PostgreSQL.gooddealmart.ca

The specified DNS name must resolve to the external IP address of your backup server, as remote backup agents need to be able to establish network connection to this endpoint.

20. Select the backup repository from the Backup repository drop-down list on the Storage page.



New Agent Backup Job

Storage

Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.

Backup repository:

Backup Repository-HPHV02-E (Created by GOODDEALMART\csun at 2/21/2023 12:56 PM.)

1.8 TB free of 1.8 TB

Retention policy: 7 days

□ Keep certain full backups longer for archival purposes

GFS retention policy is not configured

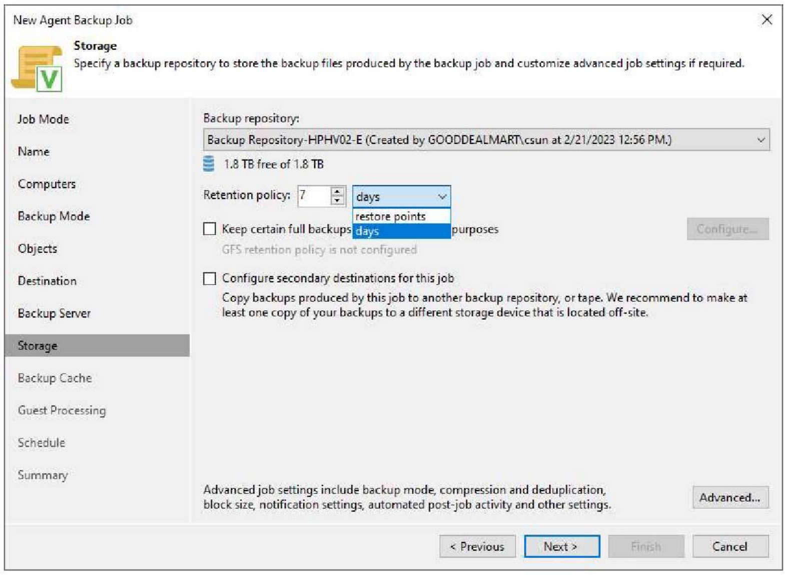
□ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

21. Set the retention policy settings for restore points in the Retention Policy field.

22. Select days or restore points from the drop-down list.



New Agent Backup Job

Storage

Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.

Backup repository:

Backup Repository-HPHV02-E (Created by GOODDEALMART\csun at 2/21/2023 12:56 PM.)

1.8 TB free of 1.8 TB

Retention policy: 7 days

restore points
days

□ Keep certain full backups ... purposes

GFS retention policy is not configured

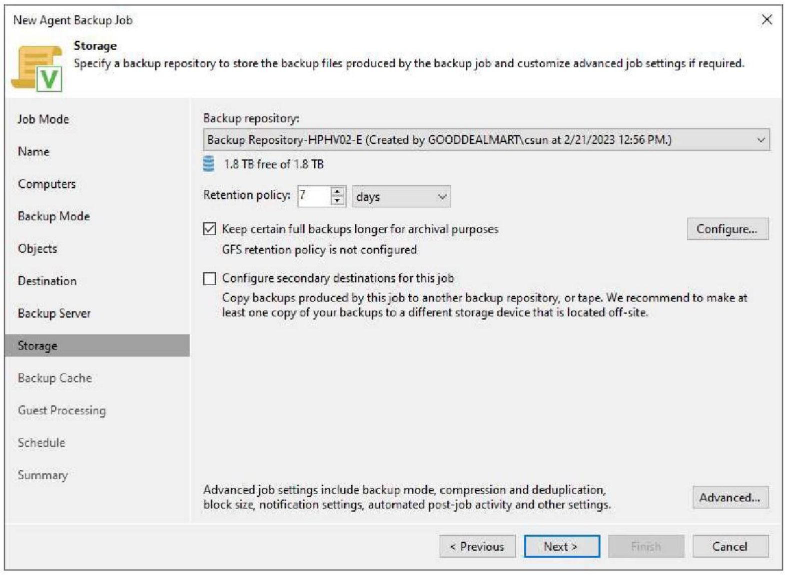
□ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

23. You can configure GFS retention policy settings for the backup job to ignore the short-term retention policy for some full backups and store them for long-term archiving.

24. Select the Keep certain full backups for longer for archival purposes. Then, if you need it, click Configure.



New Agent Backup Job

Storage

Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.

Backup repository:

Backup Repository-HPHV02-E (Created by GOODDEALMART\csun at 2/21/2023 12:56 PM.)

1.8 TB free of 1.8 TB

Retention policy: 7 days

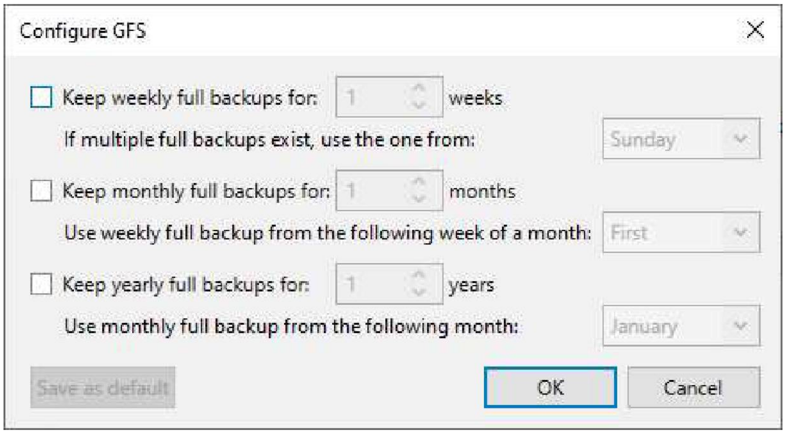
☑ Keep certain full backups longer for archival purposes

GFS retention policy is not configured

□ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.



Configure GFS

□ Keep weekly full backups for: 1 weeks

If multiple full backups exist, use the one from: Sunday

□ Keep monthly full backups for: 1 months

Use weekly full backup from the following week of a month: First

□ Keep yearly full backups for: 1 years

Use monthly full backup from the following month: January

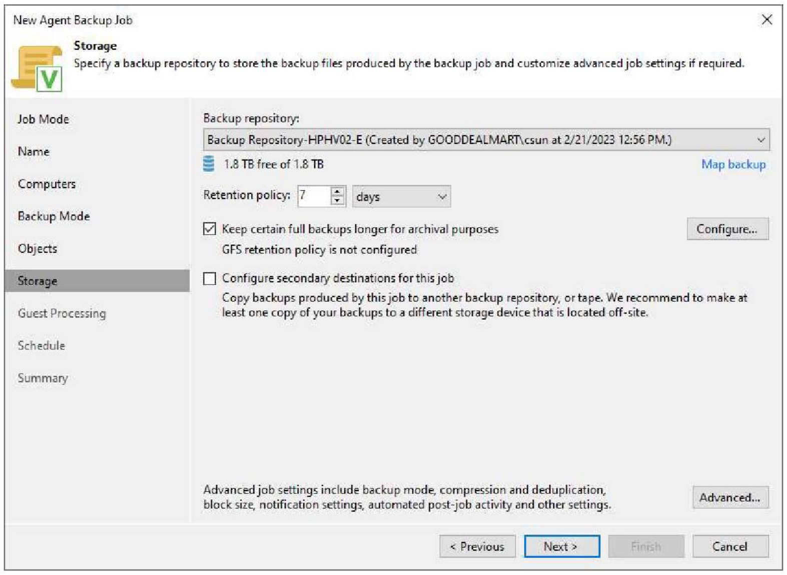
25. Select the Keep weekly full backups for checkbox, and specify the number of weeks you want to prevent restore points from being modified and deleted.

26. Select the Keep monthly full backups for checkbox, and specify the months you want to prevent restore points from being modified and deleted.

27. Select the Keep yearly full backups for checkbox, and specify the years you want to prevent restore points from being modified and deleted.

28. Click OK.

29. On the Storage page, click Advanced.



New Agent Backup Job

Storage

Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.

Backup repository: Backup Repository-HPHV02-E (Created by GOODDEALMART\csun at 2/21/2023 12:56 PM.)

1.8 TB free of 1.8 TB

Retention policy: 7 days

☑ Keep certain full backups longer for archival purposes

GFS retention policy is not configured

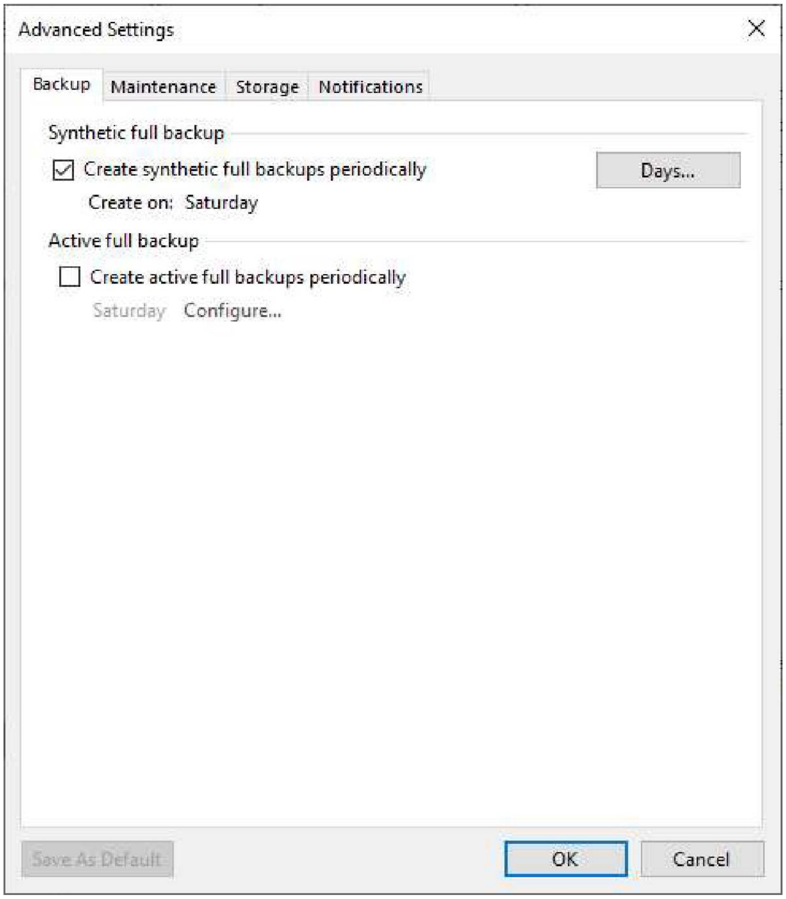
□ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

30. Select Create synthetic full backups or Active full backups periodically checkbox.

31. Schedule full backups periodically and click OK.



Advanced Settings

Synthetic full backup

☑ Create synthetic full backups periodically

Create on: Saturday

Active full backup

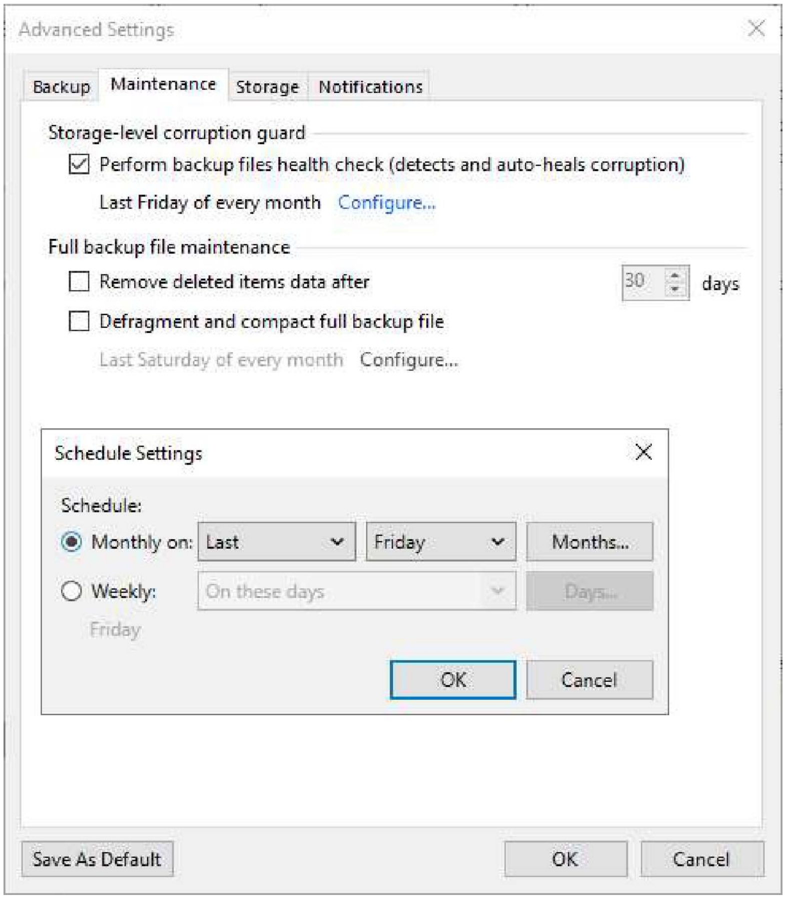
□ Create active full backups periodically

Saturday Configure...

32. On the Advanced Settings, select Maintenance.

33. To regularly perform a health check on the backup chain's most recent restore point, select the Perform backup files health check (detects and auto-heals corruption) checkbox in the Storage-level corruption guard section.

34. Click Configure to set a timetable for the health check.



Storage-level corruption guard

☑ Perform backup files health check (detects and auto-heals corruption)

Last Friday of every month Configure...

Full backup file maintenance

□ Remove deleted items data after 30 days

□ Defragment and compact full backup file

Last Saturday of every month Configure...

Schedule:

● Monthly on: Last Friday

○ Weekly: On these days

Friday

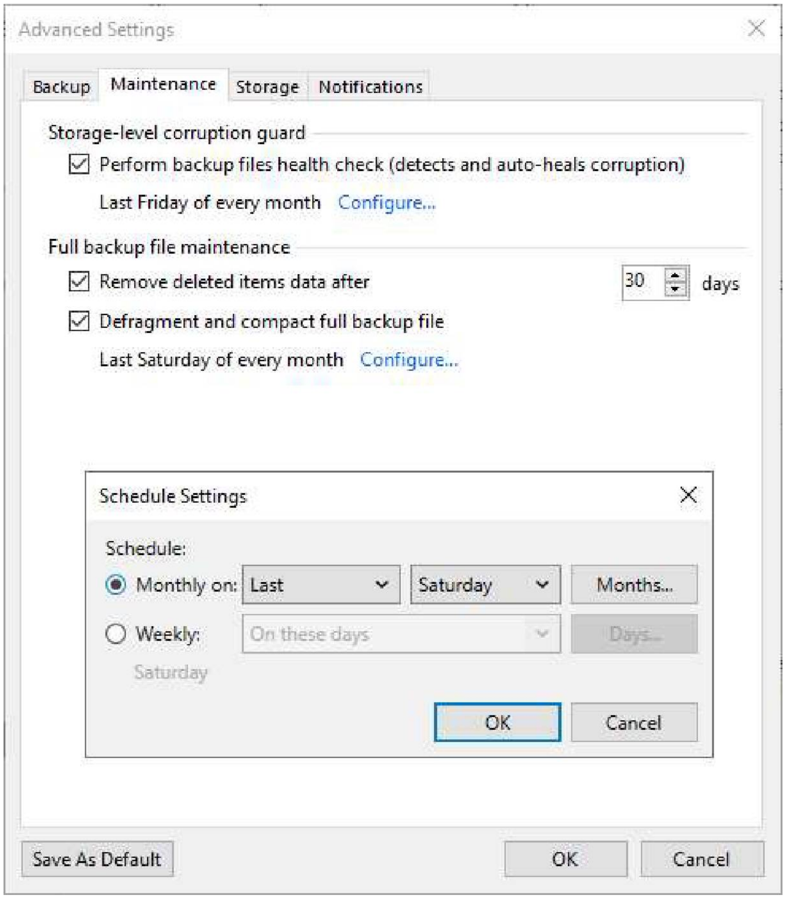
35. Select the Remove deleted items data after the checkbox and enter the few days you want backup data for deleted VMs to be kept.

36. Select the Defragment and compact full backup file checkbox and click Configure.

37. Set the schedule for the compact operation to compact a full backup periodically.

Note:

You don’t need to enable the defragment and compact functionality checkbox if GFS retention is enabled.



Advanced Settings

Backup | Maintenance | Storage | Notifications

Storage-level corruption guard

☑ Perform backup files health check (detects and auto-heals corruption)

Last Friday of every month Configure...

Full backup file maintenance

☑ Remove deleted items data after 30 days

☑ Defragment and compact full backup file

Last Saturday of every month Configure...

Schedule Settings

Schedule:

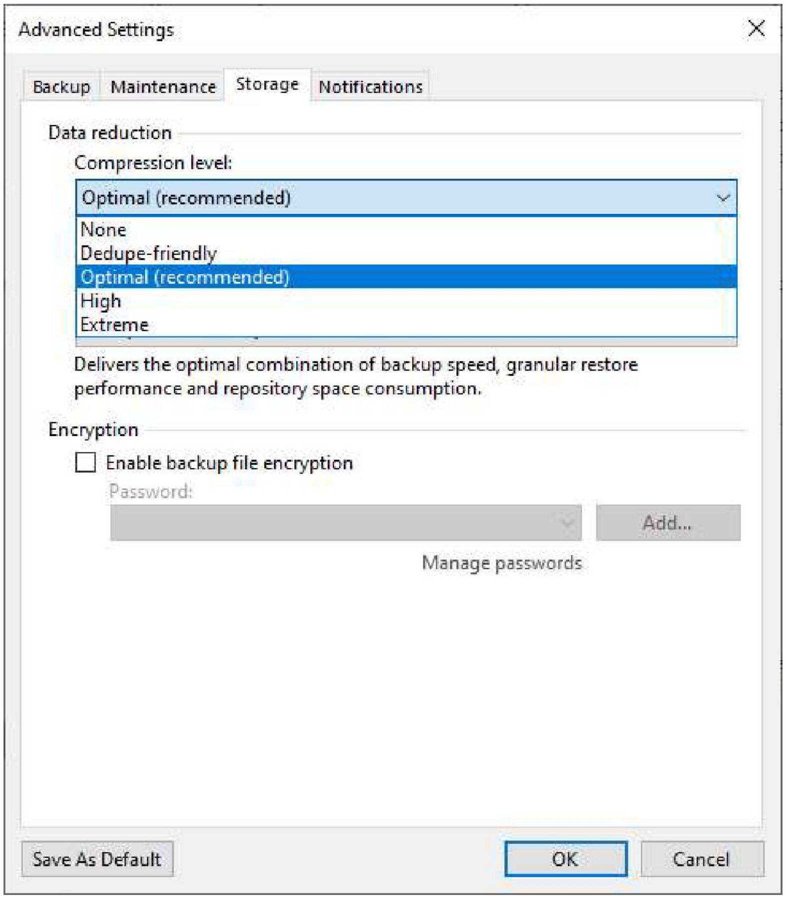
● Monthly on: Last Saturday Months...

○ Weekly: On these days Days...

Saturday

38. On Advanced Settings, select Storage.

39. Select the Compression level from the drop-down list.



Advanced Settings

Data reduction

Compression level: Optimal (recommended)

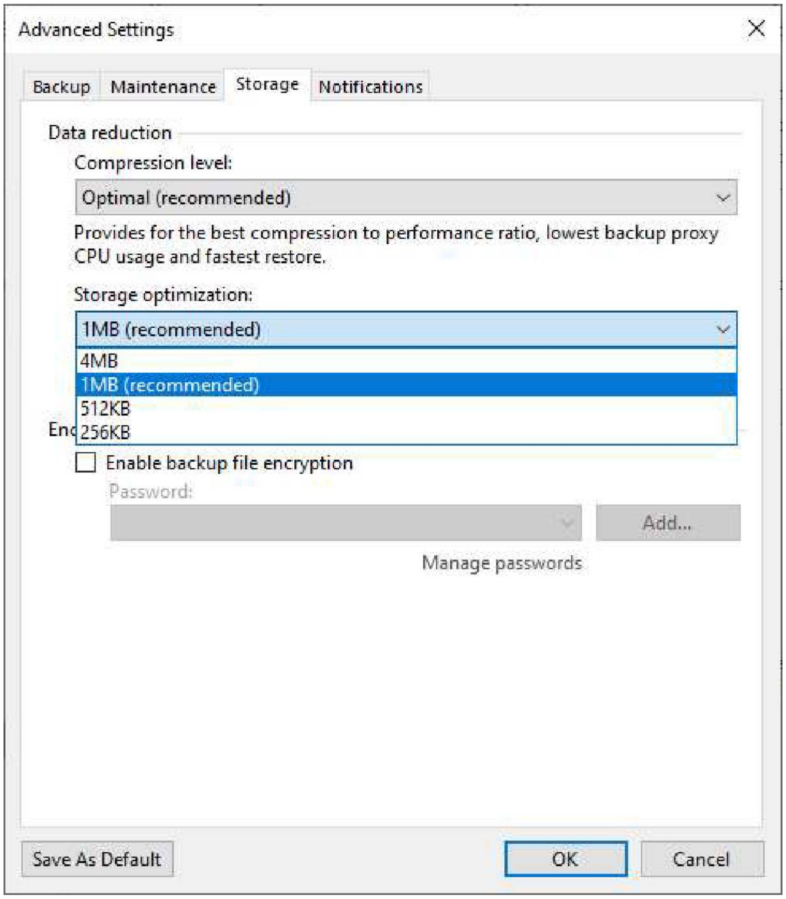
Delivers the optimal combination of backup speed, granular restore performance and repository space consumption.

Encryption

□ Enable backup file encryption

Password:

40. Select Storage optimization from the drop-down list.



Data reduction

Compression level: Optimal (recommended)

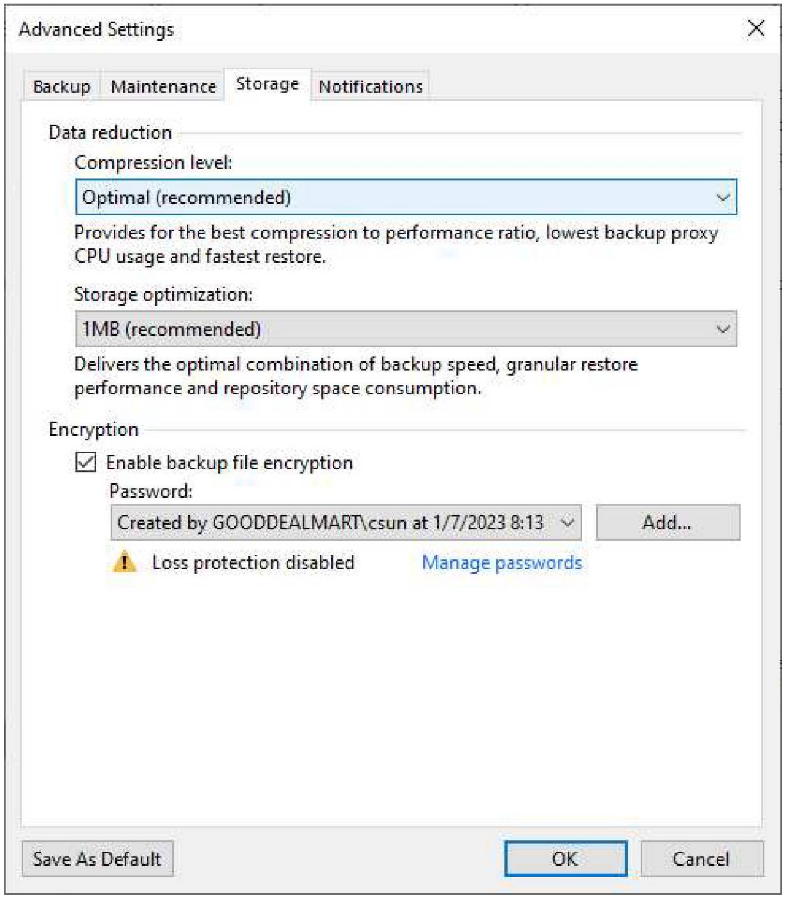
Provides for the best compression to performance ratio, lowest backup proxy CPU usage and fastest restore.

Storage optimization: 1MB (recommended)

☐ Enable backup file encryption

41. Select the Enable backup file encryption checkbox to encrypt the content of backup files.

42. Select a password from the drop-down list. Then, if you still need to do, click Add or use the Manage passwords link to create a new password.



Advanced Settings

Data reduction

Compression level: Optimal (recommended)

Provides for the best compression to performance ratio, lowest backup proxy CPU usage and fastest restore.

Storage optimization: 1MB (recommended)

Delivers the optimal combination of backup speed, granular restore performance and repository space consumption.

Encryption

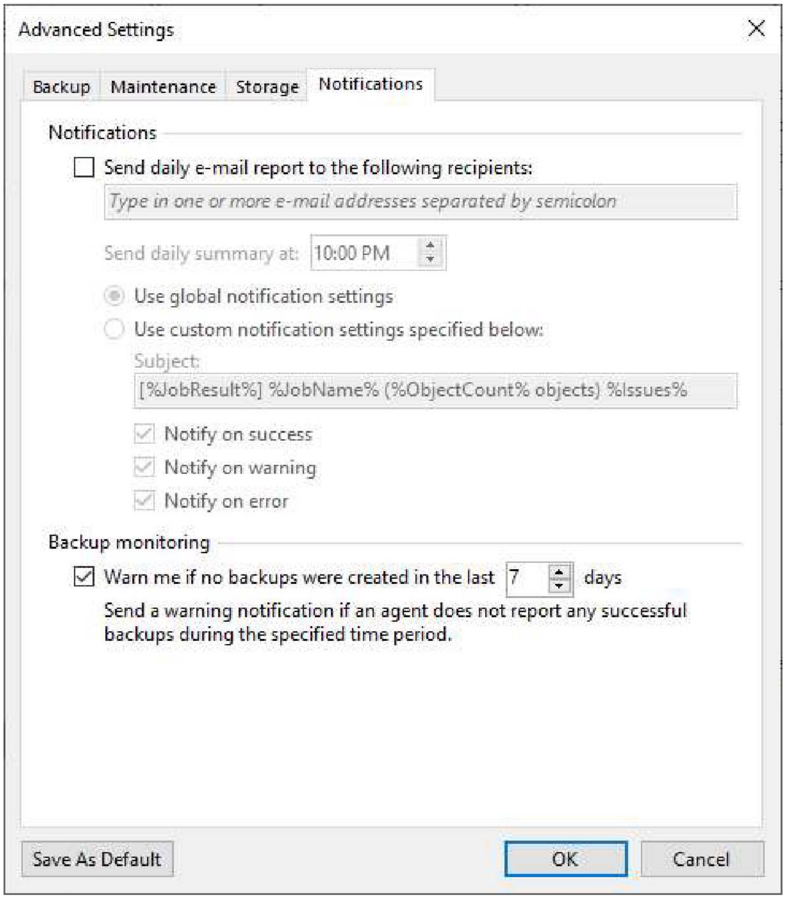
☑ Enable backup file encryption

Password: Created by GOODDEALMART\csun at 1/7/2023 8:13

Loss protection disabled

43. On the Advanced Settings, select Notifications.

44. Keep the default settings and click OK.



Advanced Settings

Notifications

☐ Send daily e-mail report to the following recipients:

Type in one or more e-mail addresses separated by semicolon

Send daily summary at: 10:00 PM

● Use global notification settings

○ Use custom notification settings specified below:

Subject:

[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

☑ Notify on success

☑ Notify on warning

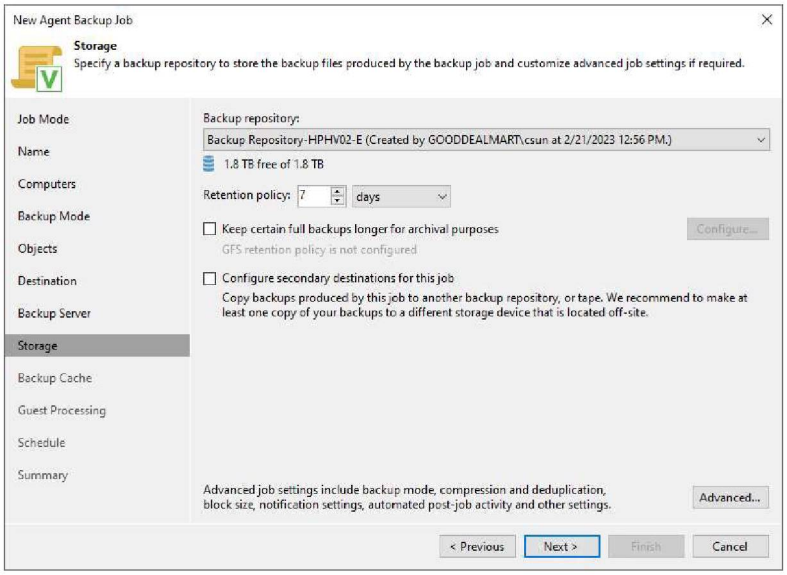
☑ Notify on error

Backup monitoring

☑ Warn me if no backups were created in the last 7 days

Send a warning notification if an agent does not report any successful backups during the specified time period.

45. On the Storage page, click Next.



New Agent Backup Job

Storage

Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.

Backup repository:

Backup Repository-HPHV02-E (Created by GOODDEALMART\csun at 2/21/2023 12:56 PM.)

1.8 TB free of 1.8 TB

Retention policy: 7 days

□ Keep certain full backups longer for archival purposes

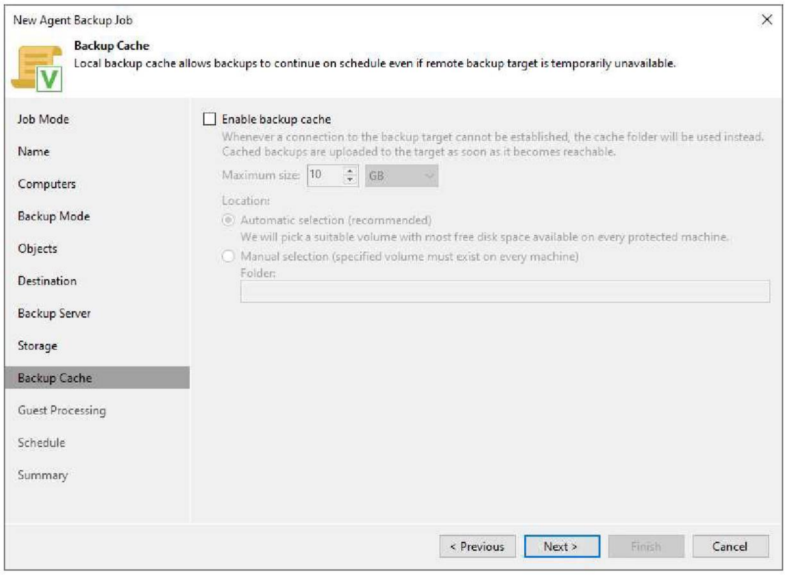
GFS retention policy is not configured

□ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

46. On the Backup Cache page, keep the default settings and click Next.



New Agent Backup Job

Backup Cache

Local backup cache allows backups to continue on schedule even if remote backup target is temporarily unavailable.

□ Enable backup cache

Whenever a connection to the backup target cannot be established, the cache folder will be used instead. Cached backups are uploaded to the target as soon as it becomes reachable.

Maximum size: 10 GB

Location:

● Automatic selection (recommended)

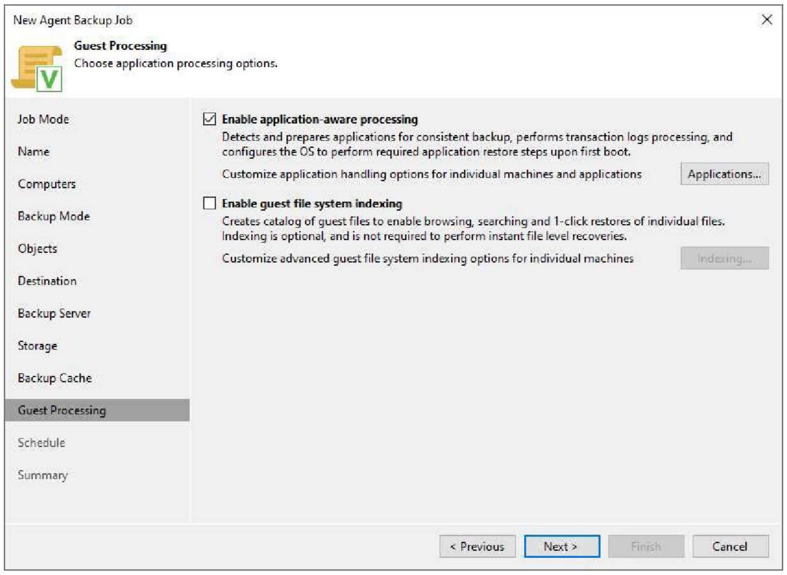
We will pick a suitable volume with most free disk space available on every protected machine.

○ Manual selection (specified volume must exist on every machine)

Folder:

47. When you add Physical machines running VSS-aware applications to the backup job, you can enable application-aware processing to create a transactionally consistent backup. The transactionally consistent backup ensures that applications on VMs can be recovered without data loss.

48. Select the Enable application-aware processing checkbox on the Guest Processing page, and click Applications.



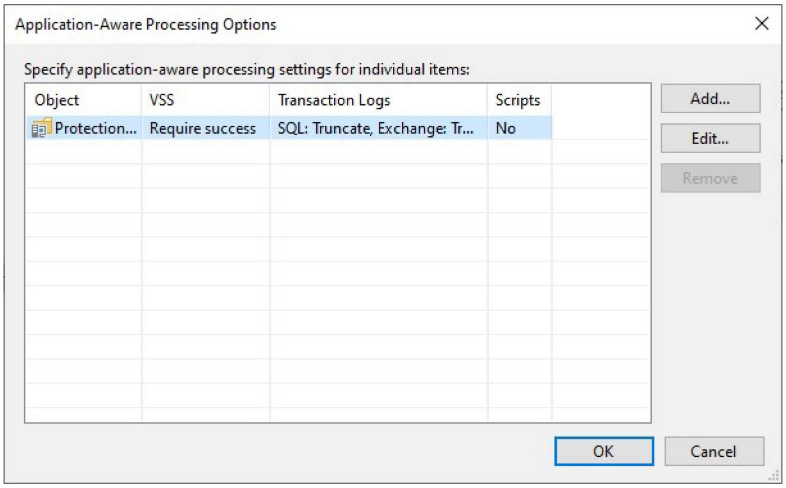
New Agent Backup Job

Guest Processing
Choose application processing options.

☑ **Enable application-aware processing**
Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.
Customize application handling options for individual machines and applications

☐ **Enable guest file system indexing**
Creates catalog of guest files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries.
Customize advanced guest file system indexing options for individual machines

49. On the Application-Aware Processing Options page, select the Object and click Edit.



Application-Aware Processing Options

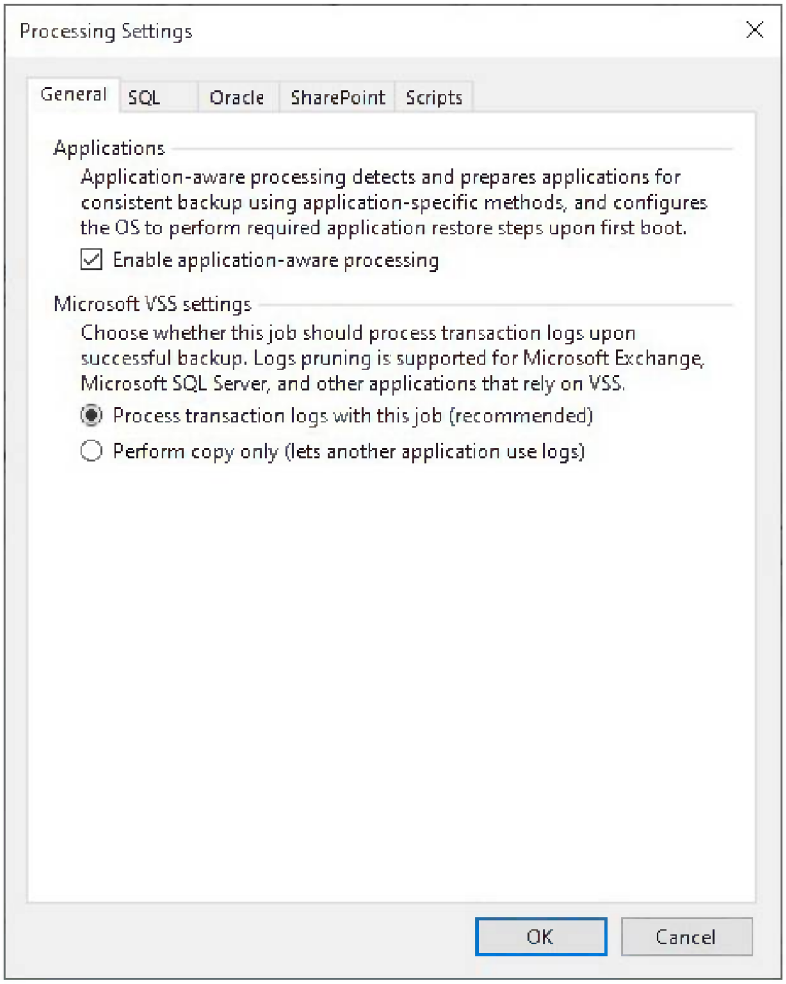
Specify application-aware processing settings for individual items:

Object	VSS	Transaction Logs	Scripts
Protection...	Require success	SQL: Truncate, Exchange: Tr...	No

50. On the Processing Settings page, select General.

51. Select Enable application-aware processing checkbox.

52. Select Process transaction logs with this job (recommended).



Applications

Application-aware processing detects and prepares applications for consistent backup using application-specific methods, and configures the OS to perform required application restore steps upon first boot.

☑ Enable application-aware processing

Microsoft VSS settings

Choose whether this job should process transaction logs upon successful backup. Logs pruning is supported for Microsoft Exchange, Microsoft SQL Server, and other applications that rely on VSS.

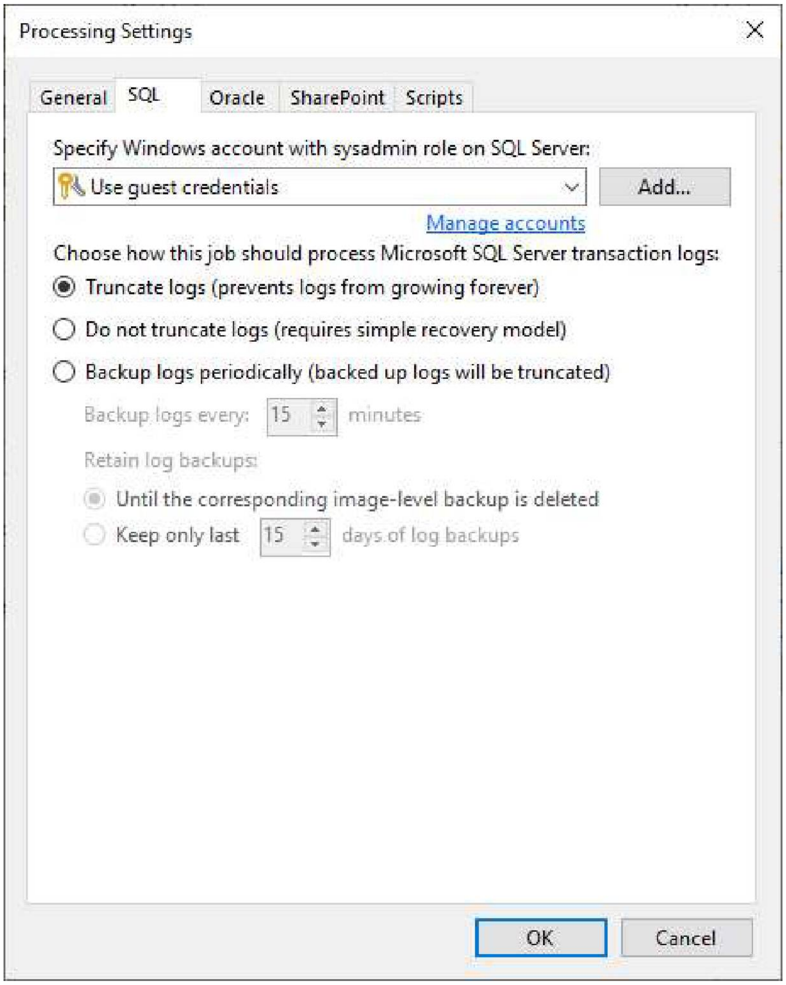
● Process transaction logs with this job (recommended)

○ Perform copy only (lets another application use logs)

53. On the Processing Settings page, click SQL if the Physical Machine is a Microsoft SQL Server.

54. Select a user account from the drop-down list.

55. Select Truncate logs (Prevents logs from growing forever).



Processing Settings

Specify Windows account with sysadmin role on SQL Server:

Use guest credentials

Choose how this job should process Microsoft SQL Server transaction logs:

● Truncate logs (prevents logs from growing forever)

○ Do not truncate logs (requires simple recovery model)

○ Backup logs periodically (backed up logs will be truncated)

Backup logs every: 15 minutes

Retain log backups:

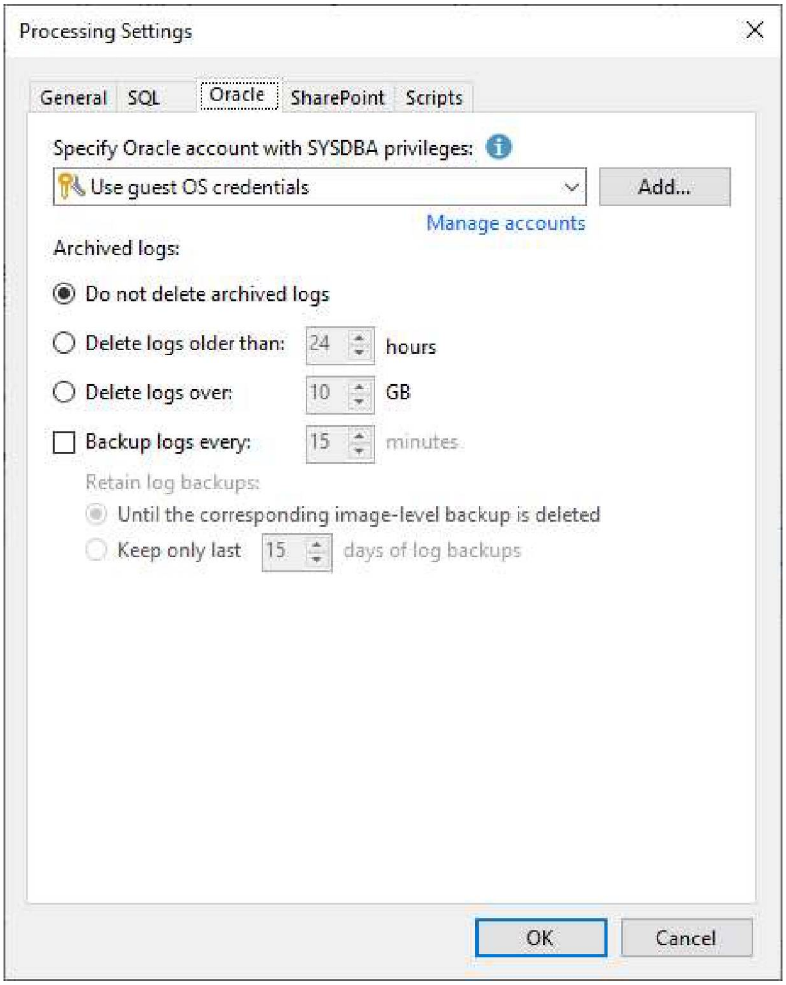
● Until the corresponding image-level backup is deleted

○ Keep only last 15 days of log backups

56. Select Oracle on the Processing Settings page if the Physical Machine is an Oracle Server.

57. Select a user account from the drop-down list.

58. Select Do not delete archived logs.



Specify Oracle account with SYSDBA privileges: Use guest OS credentials

Archived logs:

● Do not delete archived logs

○ Delete logs older than: 24 hours

○ Delete logs over: 10 GB

□ Backup logs every: 15 minutes

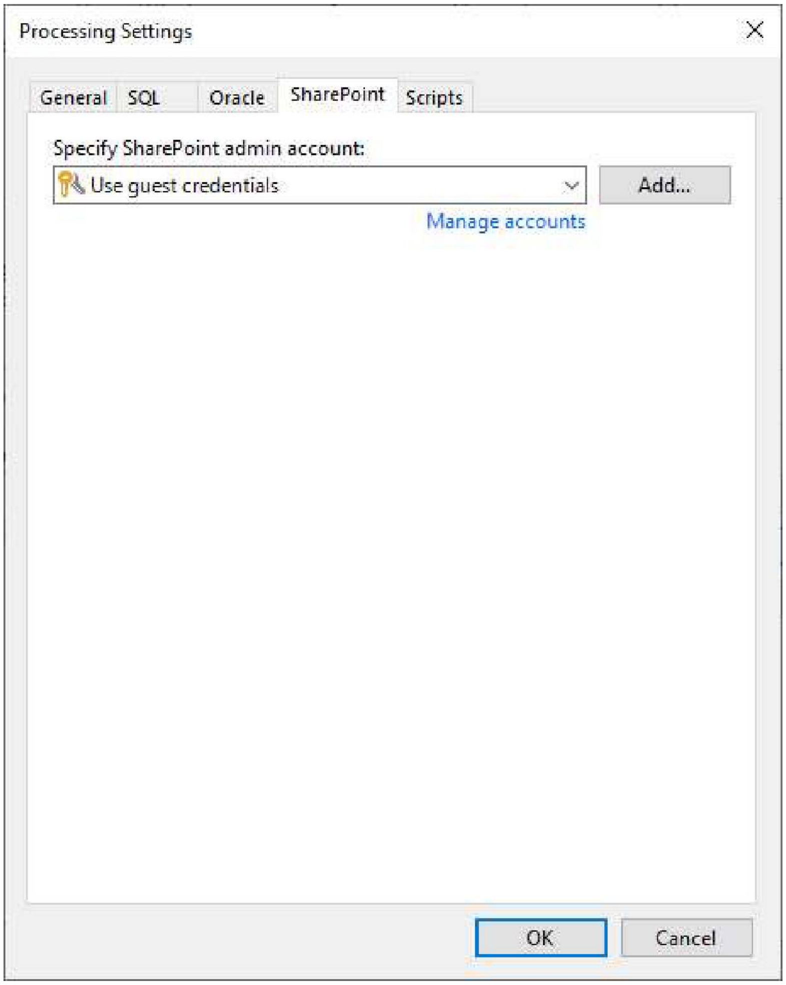
Retain log backups:

● Until the corresponding image-level backup is deleted

○ Keep only last 15 days of log backups

59. On the Processing Settings page, select SharePoint if the Physical Machine is a SharePoint Server.

60. Select a user account from the drop-down list.

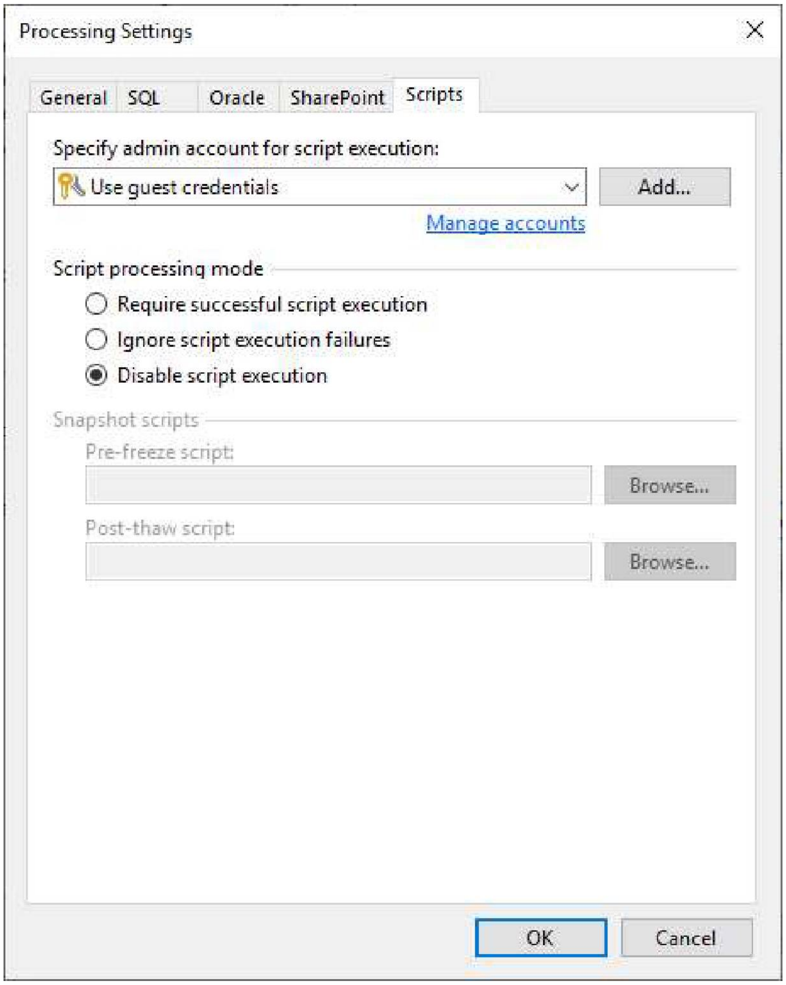

Processing Settings

Specify SharePoint admin account:

Use guest credentials

61. On the Processing Settings page, select Scripts.

62. Keep the default settings and click OK.



Processing Settings

Specify admin account for script execution: Use guest credentials

Script processing mode

○ Require successful script execution

○ Ignore script execution failures

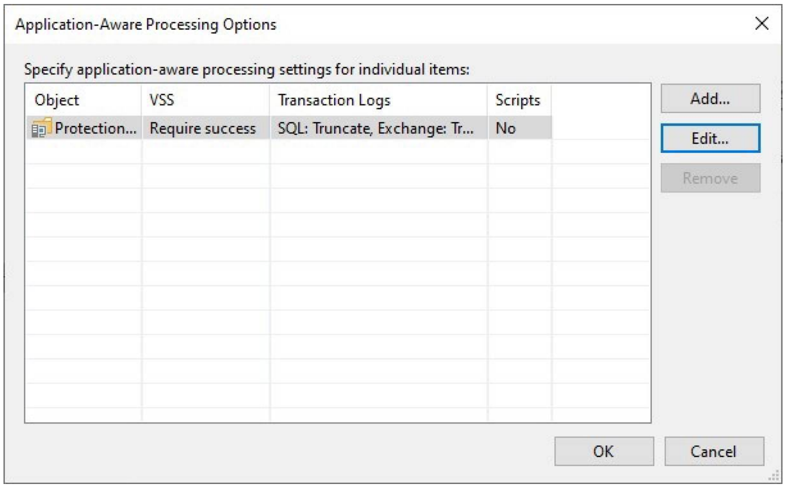
● Disable script execution

Snapshot scripts

Pre-freeze script:

Post-thaw script:

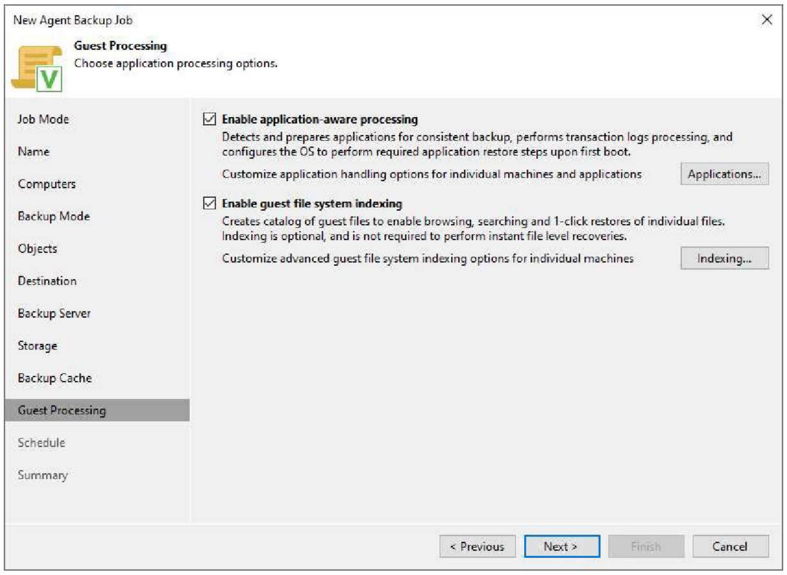
63. On the Application-Aware Processing Options page, click OK.



Specify application-aware processing settings for individual items:

Object	VSS	Transaction Logs	Scripts
Protection...	Require success	SQL: Truncate, Exchange: Tr...	No

64. Select the Enable guest file system indexing checkbox and click Indexing.



Guest Processing

Choose application processing options.

☑ **Enable application-aware processing**

Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

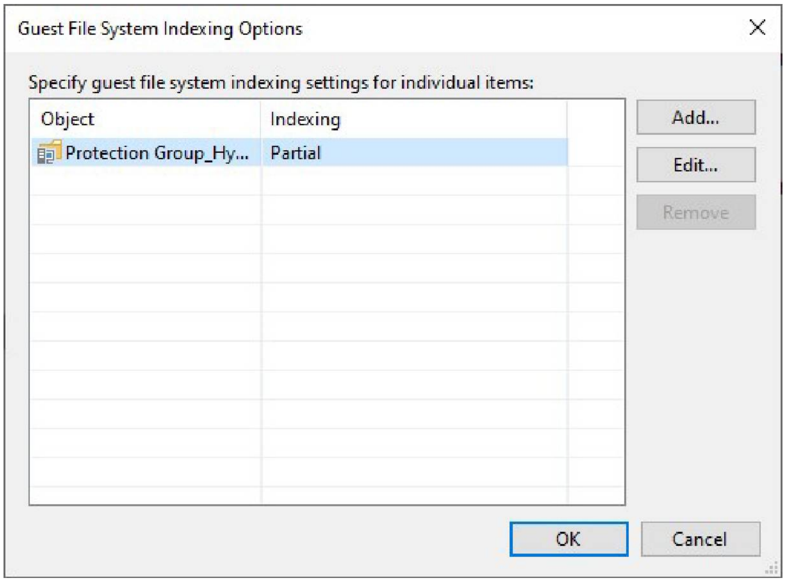
Customize application handling options for individual machines and applications

☑ **Enable guest file system indexing**

Creates catalog of guest files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries.

Customize advanced guest file system indexing options for individual machines

65. On the Guest File System Indexing Options page, select the Object, click Edit and.



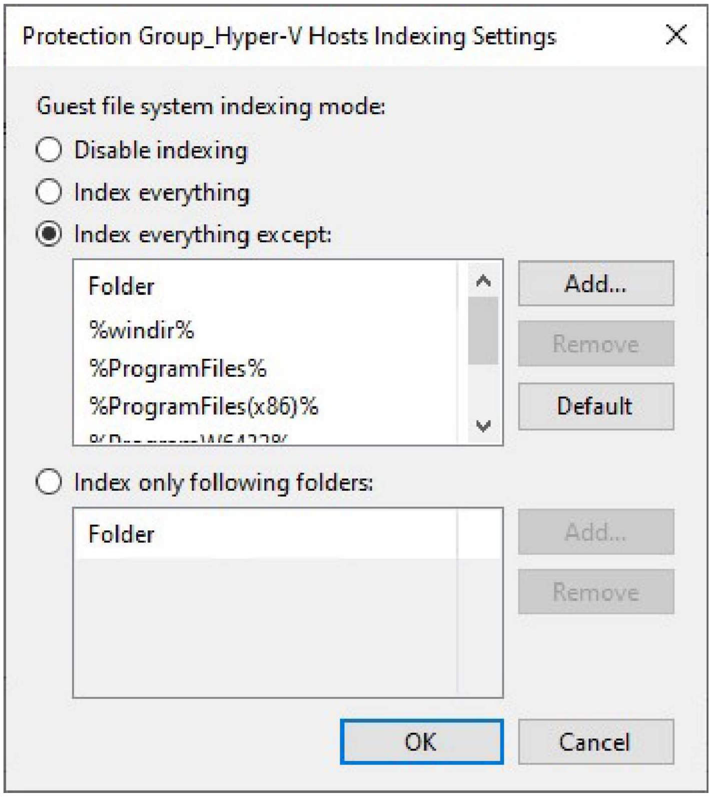
Guest File System Indexing Options

Specify guest file system indexing settings for individual items:

Object	Indexing
Protection Group_Hy...	Partial

66. On the Guest file system indexing mode page, keep the default settings.

67. Click OK.



Protection Group_Hyper-V Hosts Indexing Settings

Guest file system indexing mode:

○ Disable indexing

○ Index everything

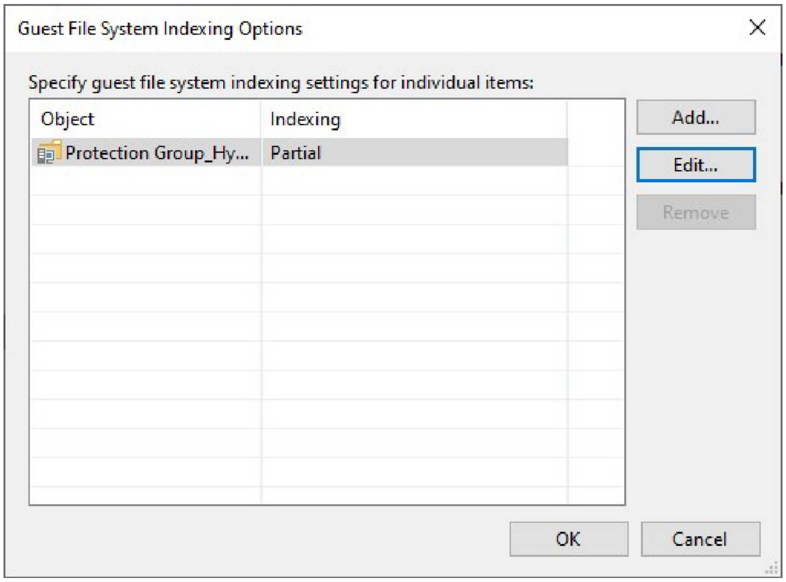
● Index everything except:

Folder
%windir%
%ProgramFiles%
%ProgramFiles(x86)%

○ Index only following folders:

Folder

68. On the Guest File System Indexing Options page, click OK.

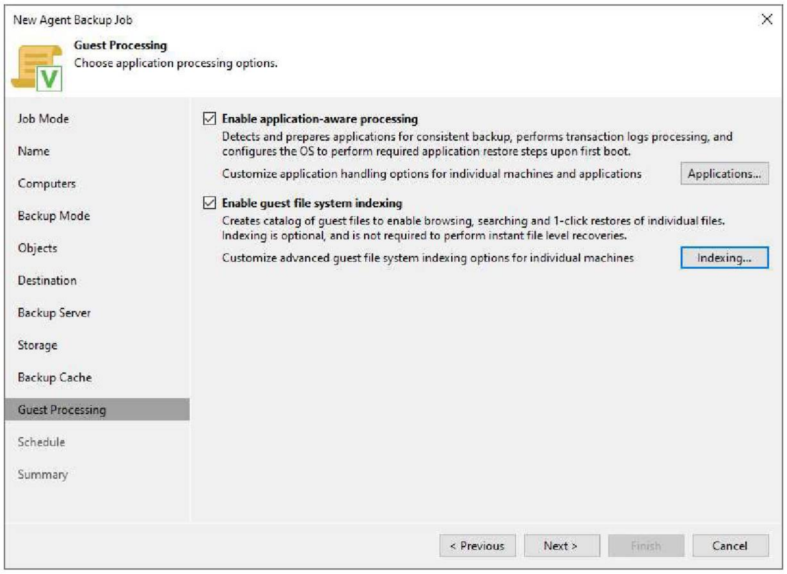


Guest File System Indexing Options

Specify guest file system indexing settings for individual items:

Object	Indexing
Protection Group_Hy...	Partial

69. On the Guest Processing page, click Next.



New Agent Backup Job

Guest Processing

Choose application processing options.

☑ **Enable application-aware processing**

Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

Customize application handling options for individual machines and applications

☑ **Enable guest file system indexing**

Creates catalog of guest files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries.

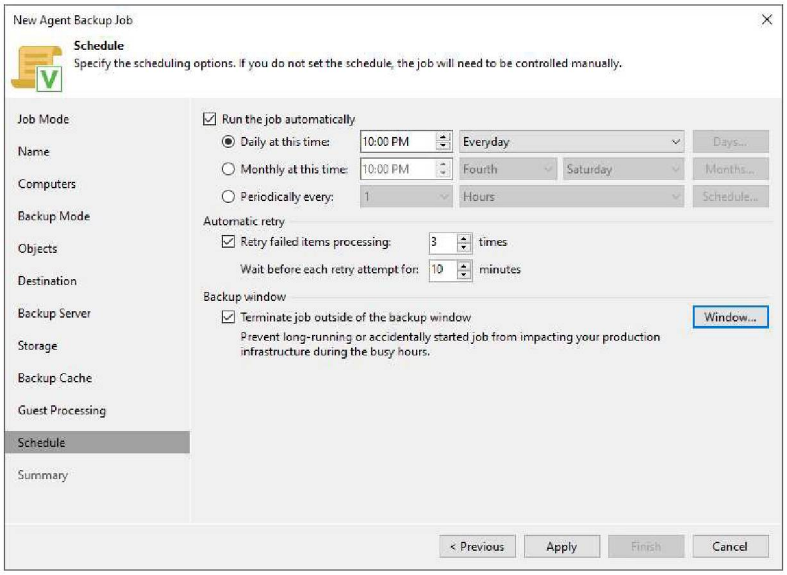
Customize advanced guest file system indexing options for individual machines

70. Select Run the job automatically checkbox on the Schedule page and select your specified schedule.

71. Define whether Veeam Backup & Replication should retry the backup job if it fails in the Automatic retry section.

72. Define the time interval the backup job must complete in the Backup window section. The backup window ensures that the job does not overlap with production hours and that there is no unnecessary overhead on the production environment.

73. Click Apply.



New Agent Backup Job

Schedule

Specify the scheduling options. If you do not set the schedule, the job will need to be controlled manually.

☑ Run the job automatically

● Daily at this time: 10:00 PM Everyday

○ Monthly at this time: 10:00 PM Fourth Saturday

○ Periodically every: 1 Hours

Automatic retry

☑ Retry failed items processing: 3 times

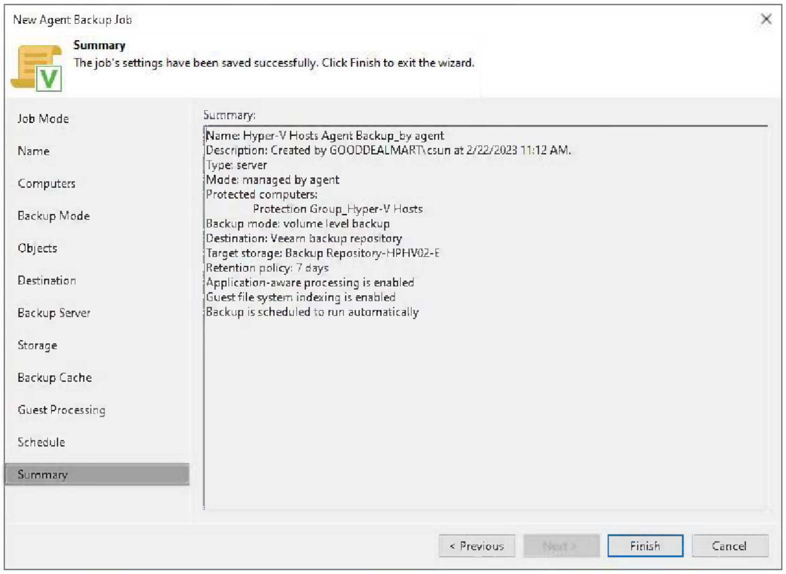
Wait before each retry attempt for: 10 minutes

Backup window

☑ Terminate job outside of the backup window

Prevent long-running or accidentally started job from impacting your production infrastructure during the busy hours.

74. On the Summary page, click Finish.



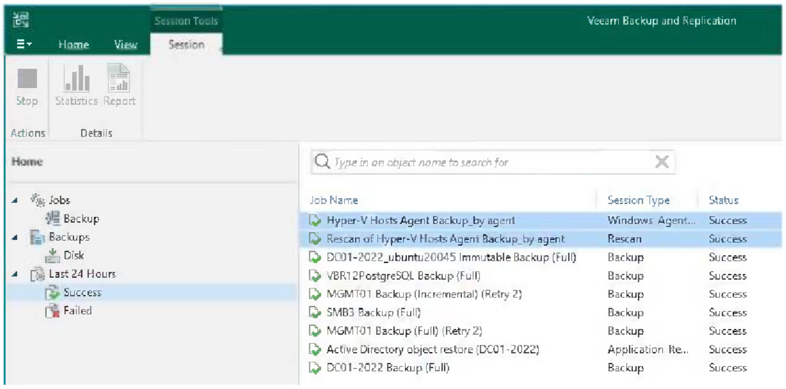
Summary

The job's settings have been saved successfully. Click Finish to exit the wizard.

Summary:

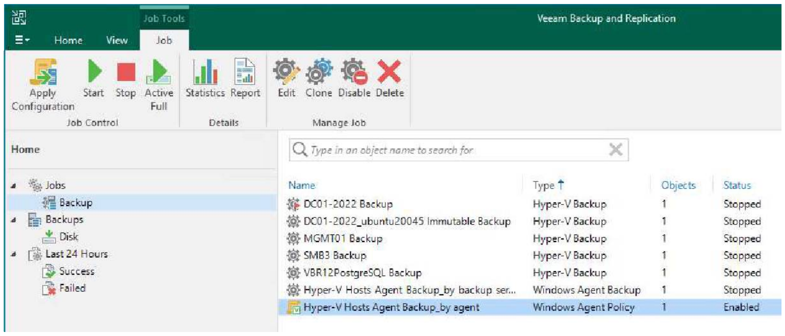
```
Name: Hyper-V Hosts Agent Backup_by agent
Description: Created by GOODDEALMART\csun at 2/22/2023 11:12 AM.
Type: server
Mode: managed by agent
Protected computers:
        Protection Group_Hyper-V Hosts
Backup mode: volume level backup
Destination: Veeam backup repository
Target storage: Backup Repository-HPHV02-E
Retention policy: 7 days
Application-aware processing is enabled
Guest file system indexing is enabled
Backup is scheduled to run automatically
```

75. Verify that the Machine rescan and Job configured are completed without issues.



Job Name	Session Type	Status
Hyper-V Hosts Agent Backup_by agent	Windows Agent...	Success
Rescan of Hyper-V Hosts Agent Backup_by agent	Rescan	Success
DC01-2022_ubuntu20045 Immutable Backup (Full)	Backup	Success
VBR12PostgreSQL Backup (Full)	Backup	Success
MGMT01 Backup (Incremental) (Retry 2)	Backup	Success
SMB3 Backup (Full)	Backup	Success
MGMT01 Backup (Full) (Retry 2)	Backup	Success
Active Directory object restore (DC01-2022)	Application Ite...	Success
DC01-2022 Backup (Full)	Backup	Success

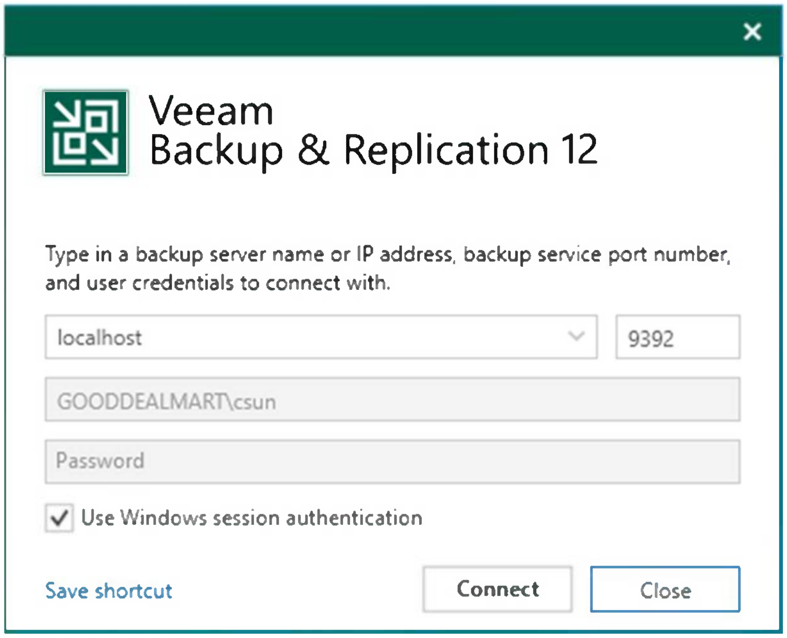
76. Verify that the backup job has been added



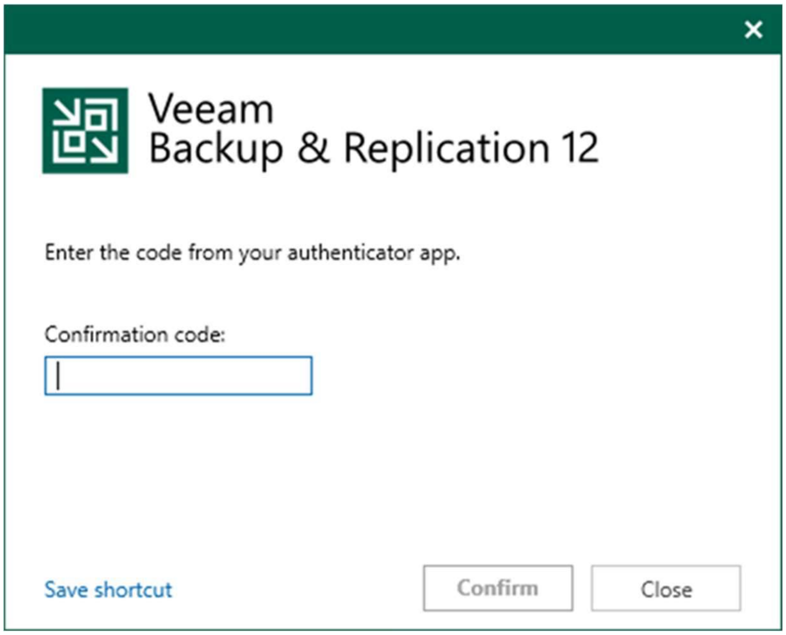
Name	Type	Objects	Status
DC01-2022 Backup	Hyper-V Backup	1	Stopped
DC01-2022_ubuntu20045 Immutable Backup	Hyper-V Backup	1	Stopped
MGMT01 Backup	Hyper-V Backup	1	Stopped
SMB3 Backup	Hyper-V Backup	1	Stopped
VBR12PostgreSQL Backup	Hyper-V Backup	1	Stopped
Hyper-V Hosts Agent Backup_by backup ser...	Windows Agent Backup	1	Stopped
Hyper-V Hosts Agent Backup_by agent	Windows Agent Policy	1	Enabled

Create a Backup job to backup all VMS of the Hyper-V Host

This procedure creates a backup job to back up all VMS of the production Hyper-V host. The new VMS will be backed up automatically after the backup job is created. You don't need to modify the backup job settings.

Instructions	Screenshot (if applicable)
1. Log in to the Veeam Backup and replication manager server. 2. Open the Veeam Backup & Replication Console and click Connect.	 Veeam Backup & Replication 12 Type in a backup server name or IP address, backup service port number, and user credentials to connect with. localhost 9392 GOODDEALMART\csun Password ☑ Use Windows session authentication

3. Enter the MFA Confirmation code and click Confirm.

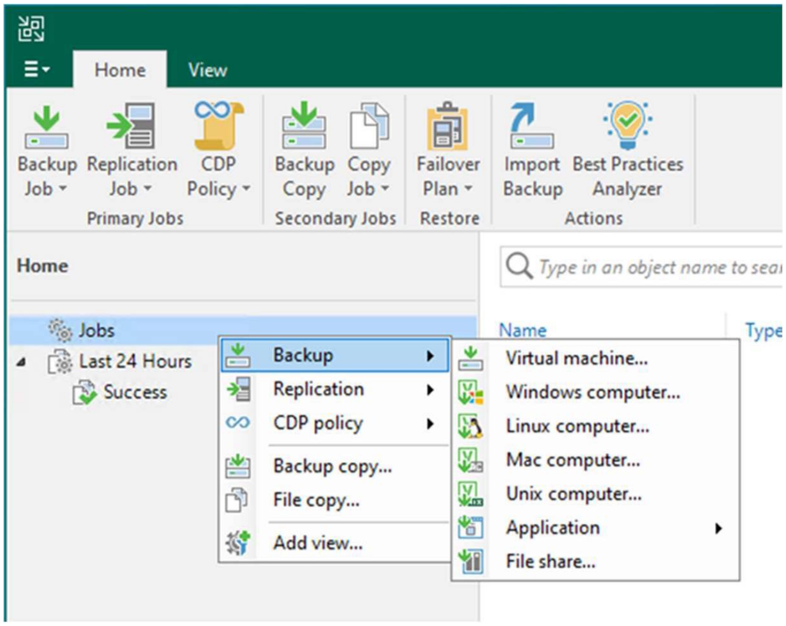


Veeam Backup & Replication 12

Enter the code from your authenticator app.

Confirmation code:

4. Select Jobs on the Home page and right-click Jobs.
5. Select Backup and click Virtual machine.

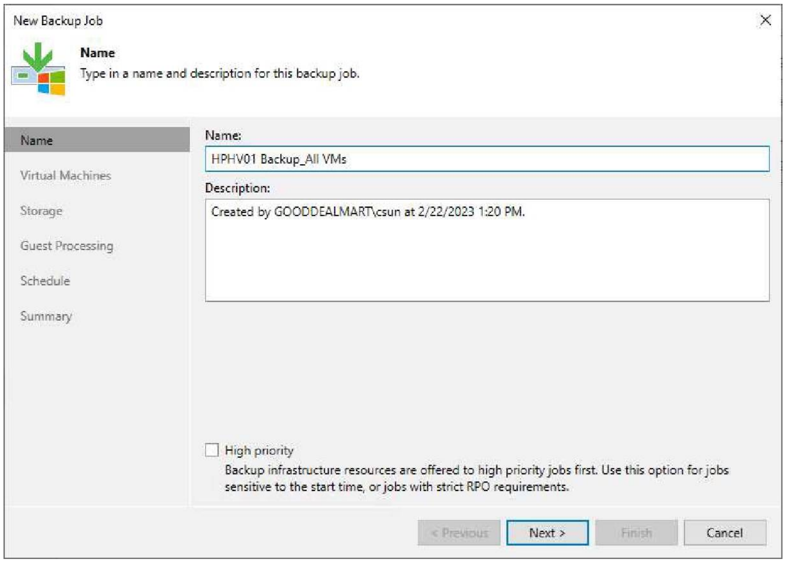


6. On the Name page, enter a name for the backup job in the Name field.

7. Give a brief description in the Description field for the future.

8. Select the High priority checkbox if you want this job to allocate resources in the first place.

9. Click Next.



New Backup Job

Name

Type in a name and description for this backup job.

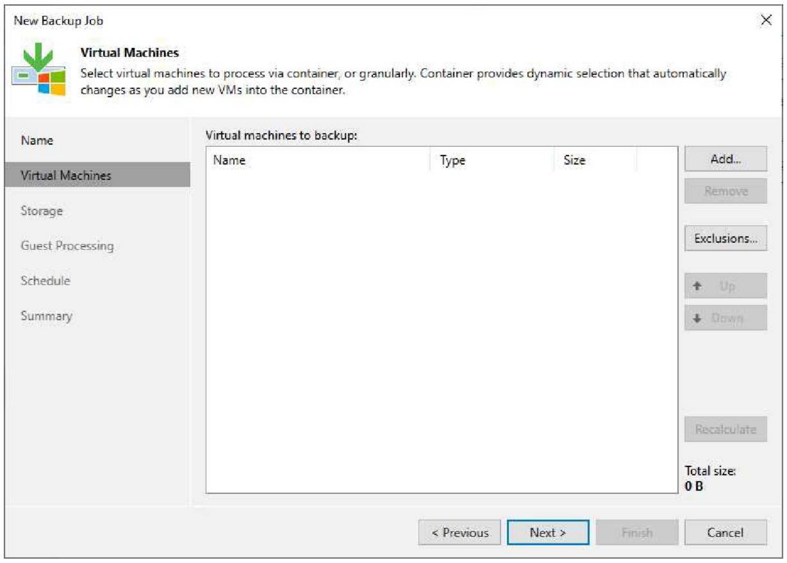
Name: HPHV01 Backup_All VMs

Description: Created by GOODDEALMART\csun at 2/22/2023 1:20 PM.

□ High priority

Backup infrastructure resources are offered to high priority jobs first. Use this option for jobs sensitive to the start time, or jobs with strict RPO requirements.

10. Click Add on the Virtual Machines page.



New Backup Job

Virtual Machines

Select virtual machines to process via container, or granularly. Container provides dynamic selection that automatically changes as you add new VMs into the container.

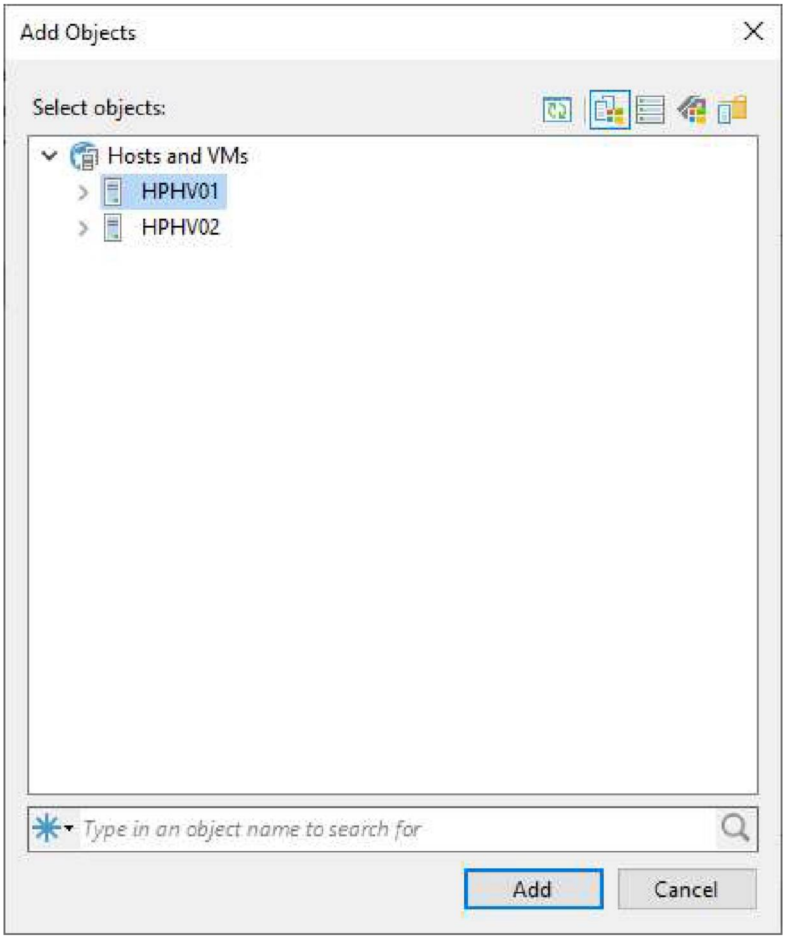
Virtual machines to backup:

Name	Type	Size

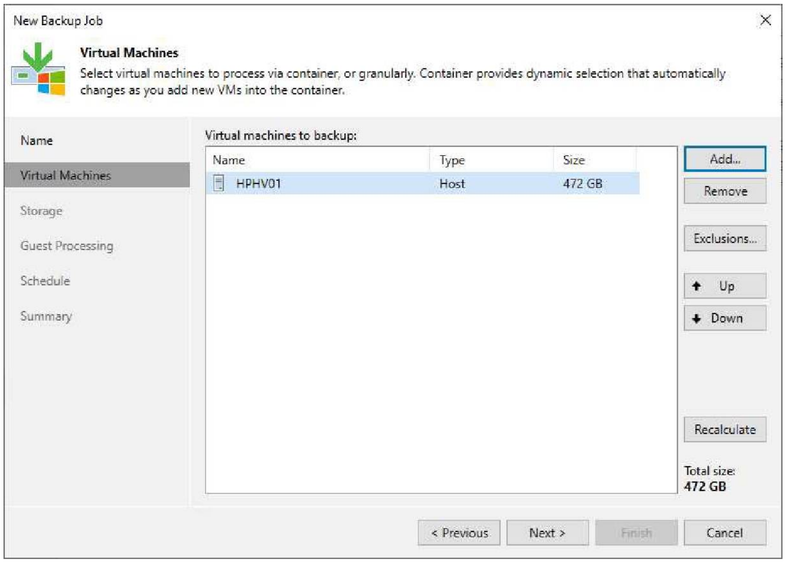
Total size: 0 B

11. Select the Host from the Select objects list on the Add Objects page and click Add.

12. If you have multiple Hosts that need to back up in the same backup job, you can repeat the step to add them.



13. Click Next on the Virtual Machines page.



New Backup Job

Virtual Machines

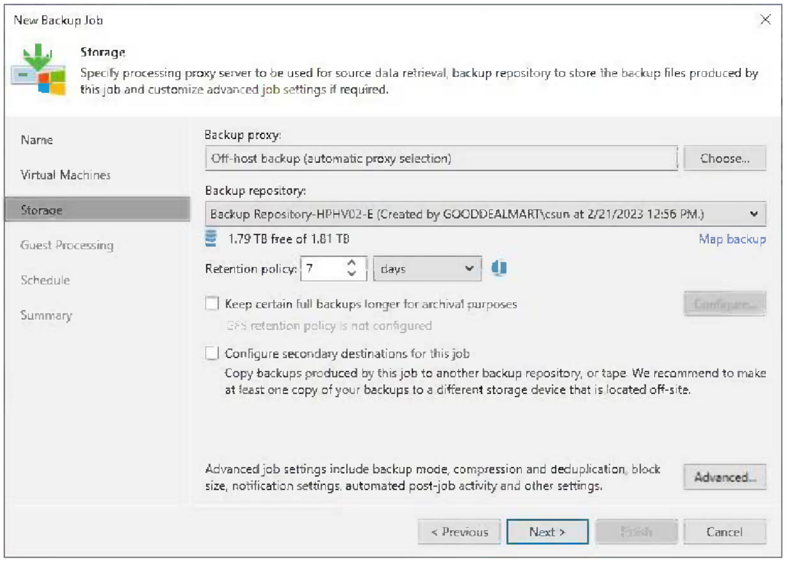
Select virtual machines to process via container, or granularly. Container provides dynamic selection that automatically changes as you add new VMs into the container.

Virtual machines to backup:

Name	Type	Size
HPHV01	Host	472 GB

Total size: **472 GB**

14. On the Storage page, click Choose to select a backup proxy if you don't want to use the default Off-host backup (automatic proxy selection) setting.



New Backup Job

Storage

Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Backup proxy: Off-host backup (automatic proxy selection)

Backup repository: Backup Repository-HPHV02-E (Created by GOODDEALMART\csun at 2/21/2023 12:56 PM.)

1.79 TB free of 1.81 TB

Retention policy: 7 days

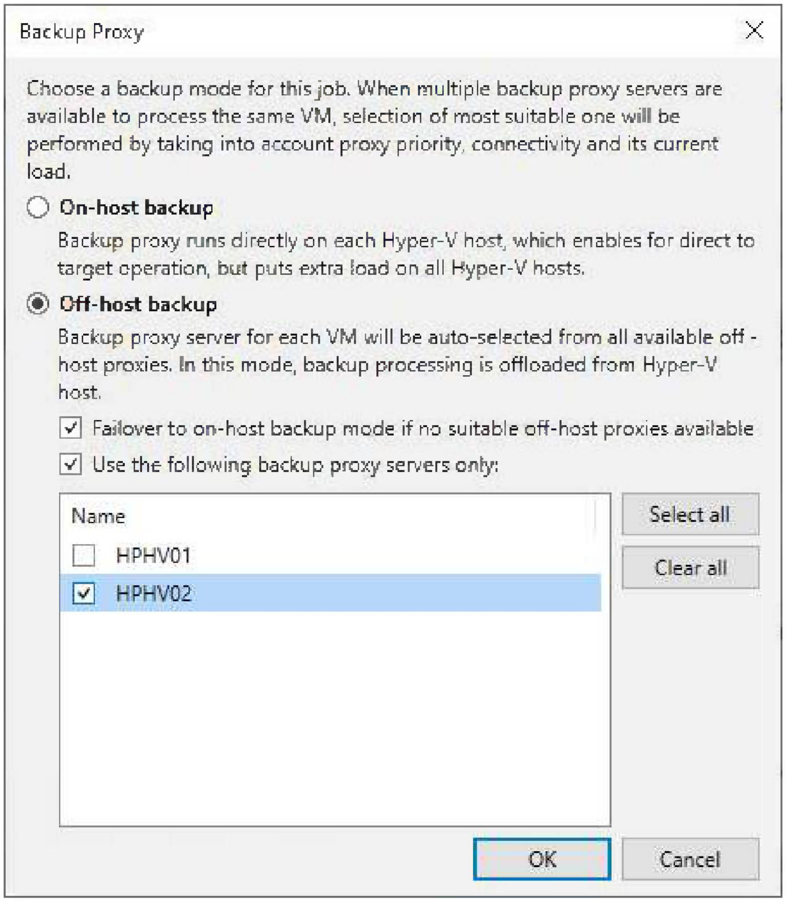
□ Keep certain full backups longer for archival purposes

GFS retention policy is not configured

□ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.



Backup Proxy

Choose a backup mode for this job. When multiple backup proxy servers are available to process the same VM, selection of most suitable one will be performed by taking into account proxy priority, connectivity and its current load.

○ **On-host backup**

Backup proxy runs directly on each Hyper-V host, which enables for direct to target operation, but puts extra load on all Hyper-V hosts.

● **Off-host backup**

Backup proxy server for each VM will be auto-selected from all available off - host proxies. In this mode, backup processing is offloaded from Hyper-V host.

☑ Failover to on-host backup mode if no suitable off-host proxies available

☑ Use the following backup proxy servers only:

Name
☐ HPHV01
☑ HPHV02

15. On the Backup Proxy page, if you select On-host backup mode, the source Microsoft HyperV host will serve as both the source host and the backup proxy. In this mode, Veeam Data Mover runs directly on the source host, which speeds up data retrieval but places additional strain on the host.

16. If you select Off-host backup mode, Veeam Data Mover will run on a dedicated off-host backup proxy. All backup processing operations from the source host are routed to the off-host backup proxy in this model.

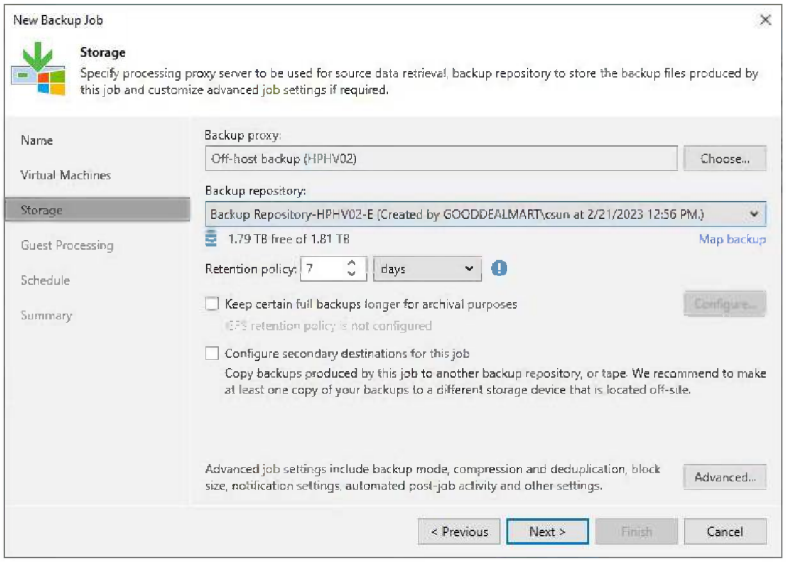
17. If the off-host backup mode is selected for the job, but no off-host backup proxies are available when the job begins, Veeam Backup & Replication will transition to on-host backup mode.

18. You unselect the Failover to on-host backup mode if no suitable off-host

proxies are available in the checkbox. Still, the job will fail to start if off-host backup proxies are unavailable or configured properly.

19. Click OK.

20. Select the backup repository from the Backup repository drop-down list where the created backup files must be saved.



New Backup Job

Storage

Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Backup proxy: Off-host backup (HPHV02)

Backup repository: Backup Repository-HPHV02-E (Created by GOODDEALMART\csun at 2/21/2023 12:56 PM.)

1.79 TB free of 1.81 TB

Retention policy: 7 days

□ Keep certain full backups longer for archival purposes

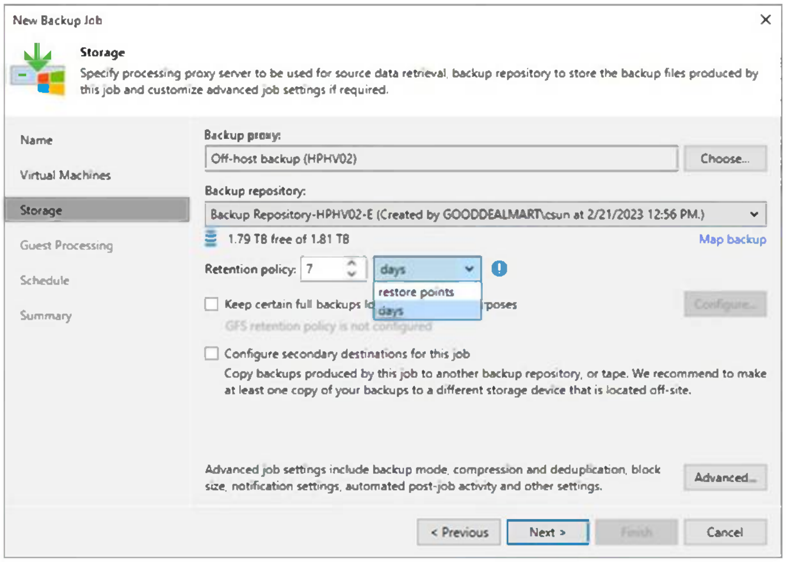
GFS retention policy is not configured

□ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

21. Set the retention policy settings for restore points in the Retention Policy field.
22. Select days or restore points from the drop-down list.



New Backup Job

Storage

Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Backup proxy: Off-host backup (HPHV02)

Backup repository: Backup Repository-HPHV02-E (Created by GOODDEALMART\csun at 2/21/2023 12:56 PM.)

1.79 TB free of 1.81 TB

Retention policy: 7 days

□ Keep certain full backups lo… poses

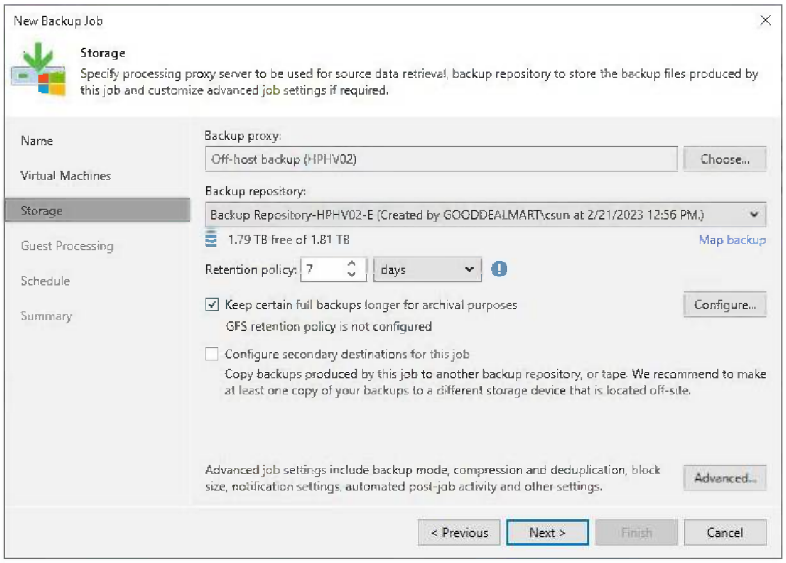
GFS retention policy is not configured

□ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

23. You can configure the backup job's GFS retention policy settings to ignore the short-term retention policy for some full backups and store them for long-term archiving.
24. Select Keep certain full backups for longer for archival purposes and click Configure.



New Backup Job

Storage

Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Backup proxy: Off-host backup (HPHV02)

Backup repository: Backup Repository-HPHV02-E (Created by GOODDEALMART\csun at 2/21/2023 12:56 PM.)

1.79 TB free of 1.81 TB

Retention policy: 7 days

☑ Keep certain full backups longer for archival purposes

GFS retention policy is not configured

□ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

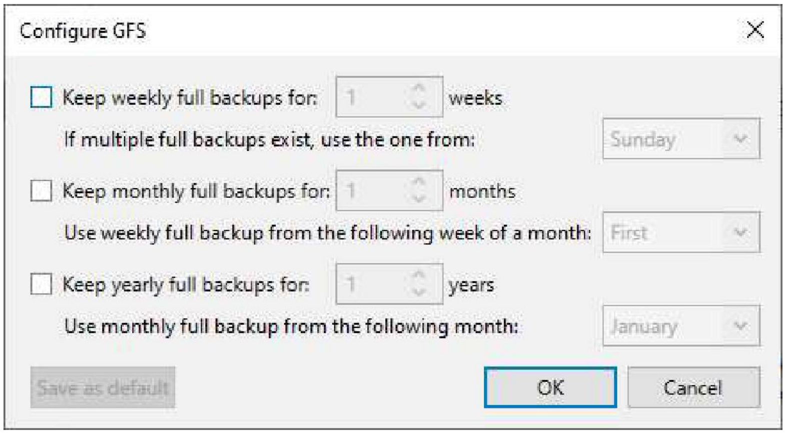
Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

25. Select the Keep weekly full backups for checkbox, and specify the number of weeks you want to prevent restore points from being modified and deleted.

26. Select the Keep monthly full backups for checkbox, and specify the months you want to prevent restore points from being modified and deleted.

27. Select the Keep yearly full backups for checkbox, and specify the years you want to prevent restore points from being modified and deleted.

28. Click OK.



Configure GFS

□ Keep weekly full backups for: 1 weeks

If multiple full backups exist, use the one from: Sunday

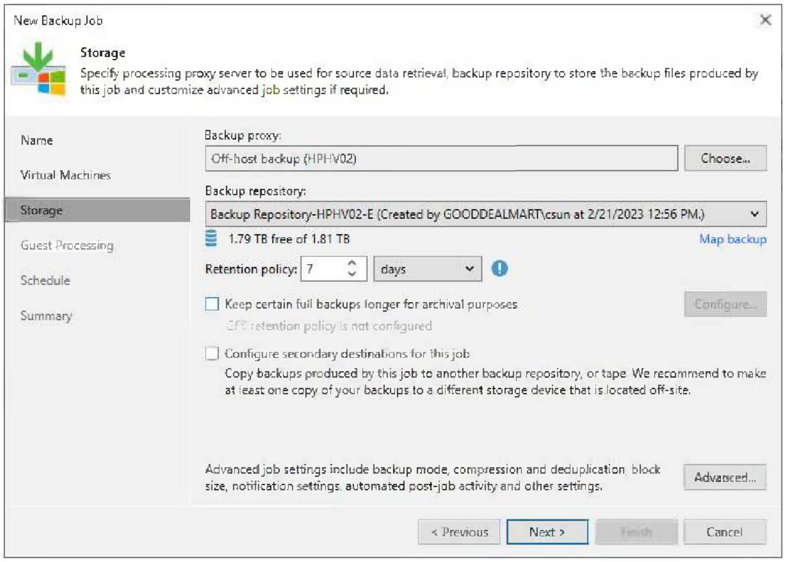
□ Keep monthly full backups for: 1 months

Use weekly full backup from the following week of a month: First

□ Keep yearly full backups for: 1 years

Use monthly full backup from the following month: January

29. On the Storage page, click Advanced.



New Backup Job

Storage

Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Backup proxy: Off-host backup (HPHV02)

Backup repository: Backup Repository-HPHV02-E (Created by GOODDEALMART\csun at 2/21/2023 12:56 PM.)

1.79 TB free of 1.81 TB

Retention policy: 7 days

□ Keep certain full backups longer for archival purposes

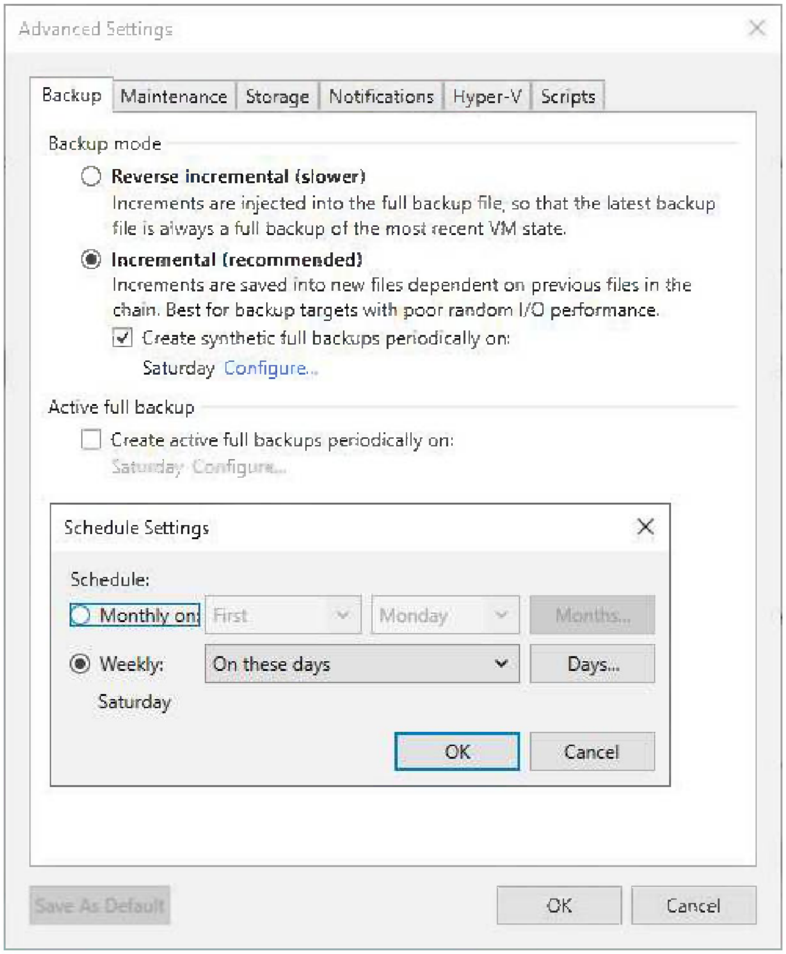
GFS retention policy is not configured

□ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

30. On the Backup page, select Incremental (recommended).
31. Select create synthetic full backups periodically or active full backups periodically checkbox.
32. Click Configure to schedule full backups periodically and click OK.



Advanced Settings

Backup | Maintenance | Storage | Notifications | Hyper-V | Scripts

Backup mode

○ **Reverse incremental (slower)**
Increments are injected into the full backup file, so that the latest backup file is always a full backup of the most recent VM state.

● **Incremental (recommended)**
Increments are saved into new files dependent on previous files in the chain. Best for backup targets with poor random I/O performance.

☑ Create synthetic full backups periodically on:
Saturday Configure...

Active full backup

□ Create active full backups periodically on:
Saturday Configure...

Schedule Settings

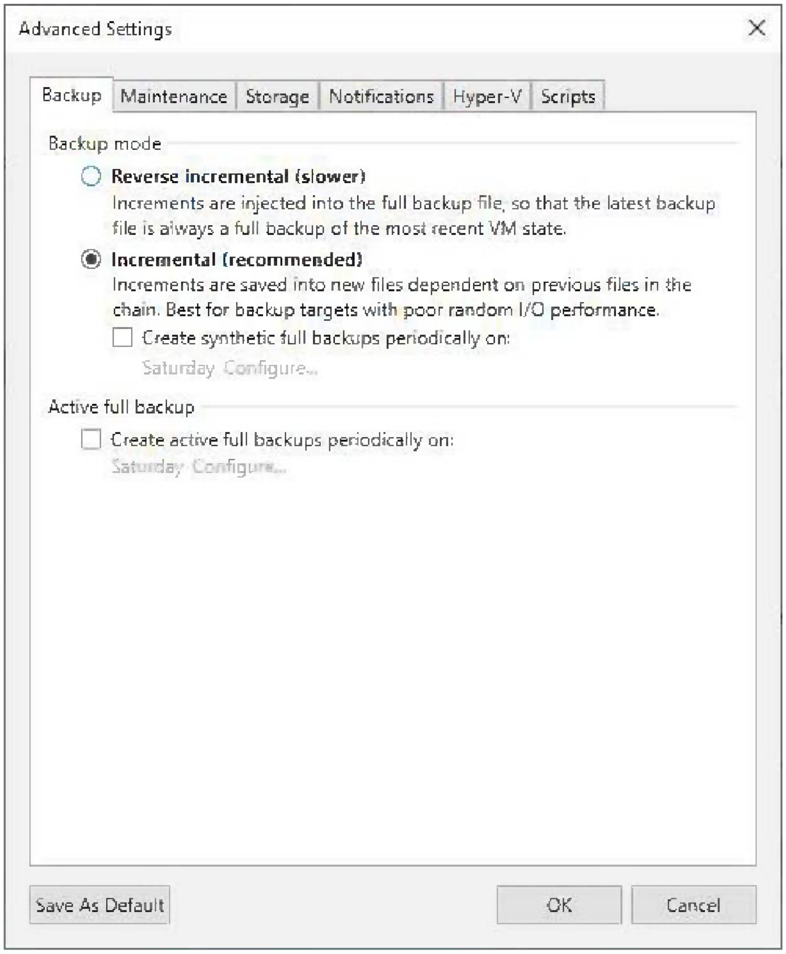
Schedule:

○ Monthly on: First | Monday | Months...

● Weekly: On these days | Days...

Saturday

33. Select Incremental and disable synthetic full and active full backups to create a forever forward incremental backup chain.



Advanced Settings

Backup mode

○ **Reverse incremental (slower)**
Increments are injected into the full backup file, so that the latest backup file is always a full backup of the most recent VM state.

● **Incremental (recommended)**
Increments are saved into new files dependent on previous files in the chain. Best for backup targets with poor random I/O performance.

□ Create synthetic full backups periodically on:
Saturday Configure...

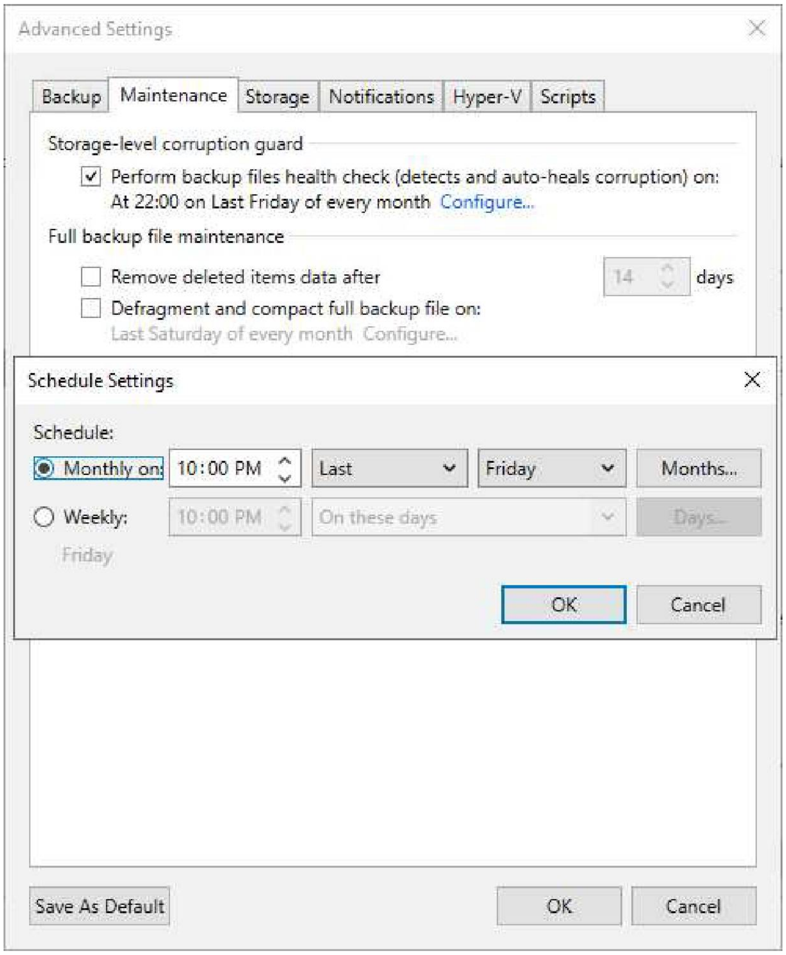
Active full backup

□ Create active full backups periodically on:
Saturday Configure...

34. On the Advanced Settings, Maintenance.

35. To regularly perform a health check on the backup chain's most recent restore point, select the Perform backup files health check (detects and auto-heals corruption) checkbox in the Storage-level corruption guard section.

36. Click Configure to set a timetable for the health check.



Storage-level corruption guard

☑ Perform backup files health check (detects and auto-heals corruption) on:
At 22:00 on Last Friday of every month Configure...

Full backup file maintenance

□ Remove deleted items data after 14 days

□ Defragment and compact full backup file on:
Last Saturday of every month Configure...

Schedule Settings

Schedule:

● Monthly on: 10:00 PM | Last | Friday | Months...

○ Weekly: 10:00 PM | On these days | Days...
Friday

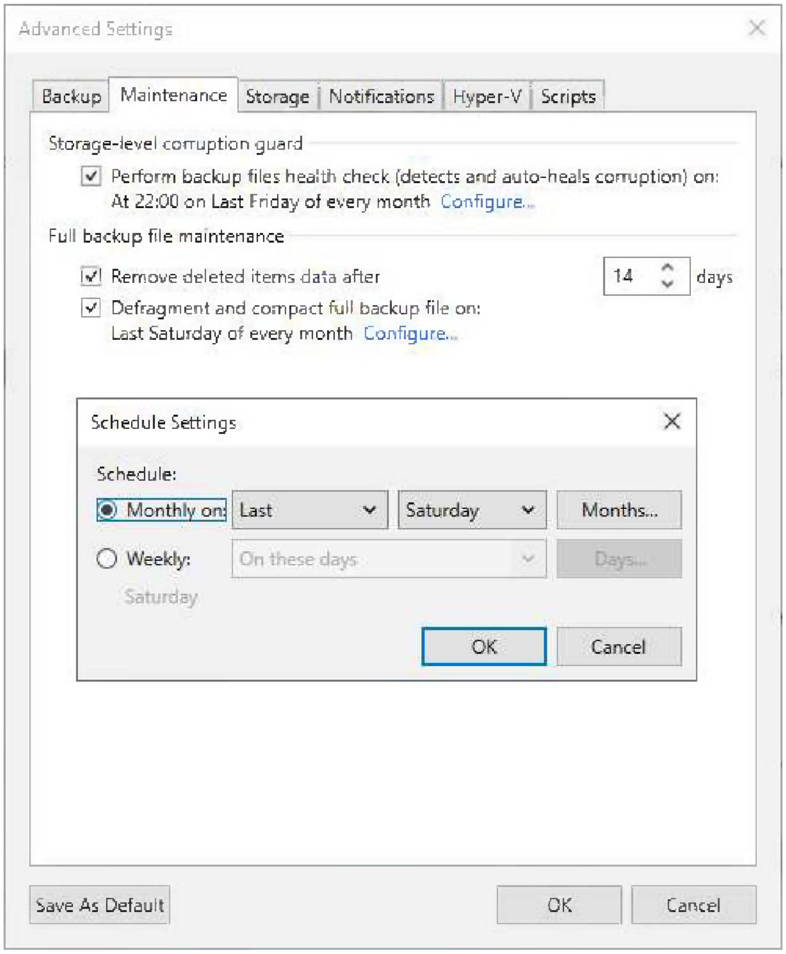
37. Select the Remove deleted items data after the checkbox and enter the few days you want backup data for deleted VMs to be kept.

38. Select the Defragment and compact full backup file checkbox and click Configure.

39. Set the schedule for the compact operation to compact a full backup periodically.

Note:

GFS retention is not compatible with defragment and compact functionality.



Advanced Settings

Storage-level corruption guard

☑ Perform backup files health check (detects and auto-heals corruption) on:
At 22:00 on Last Friday of every month Configure...

Full backup file maintenance

☑ Remove deleted items data after 14 days

☑ Defragment and compact full backup file on:
Last Saturday of every month Configure...

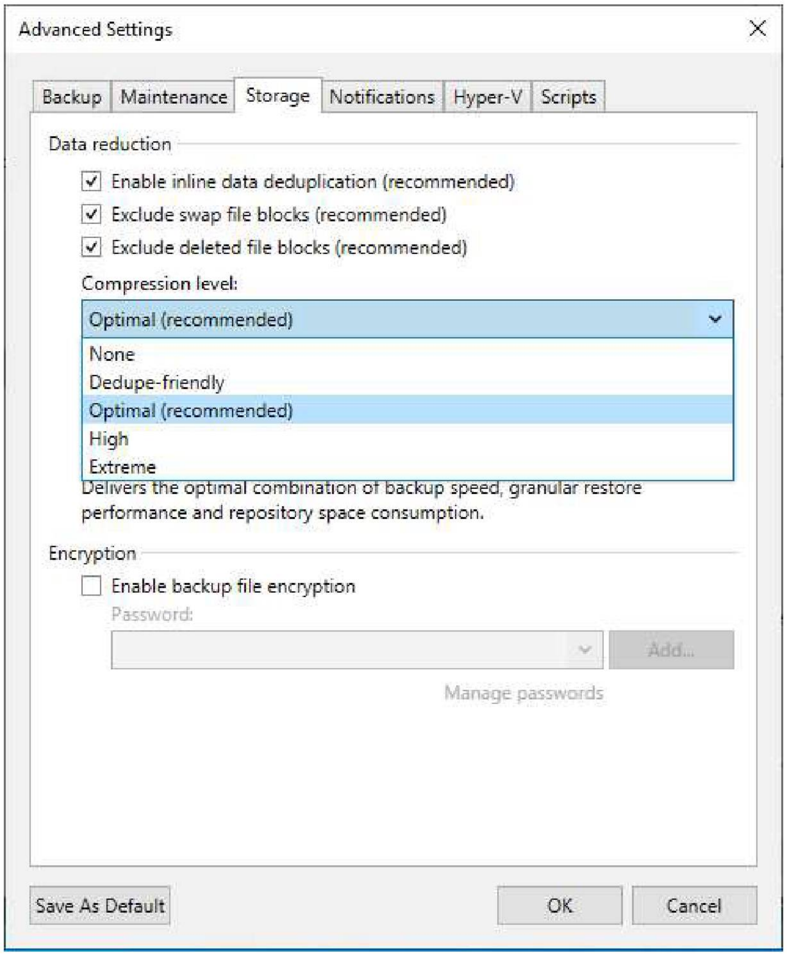
Schedule Settings

Schedule:

● Monthly on: Last Saturday

○ Weekly: On these days
Saturday

40. On Advanced Settings, select Storage.
41. Select the Enable inline data deduplication (recommended) checkbox.
42. Select the Exclude swap file blocks (recommended) checkbox.
43. Select the Exclude deleted file blocks (recommended) checkbox.
44. Select the compression level for the backup from the drop-down list.



Advanced Settings

Data reduction

☑ Enable inline data deduplication (recommended)

☑ Exclude swap file blocks (recommended)

☑ Exclude deleted file blocks (recommended)

Compression level: Optimal (recommended)

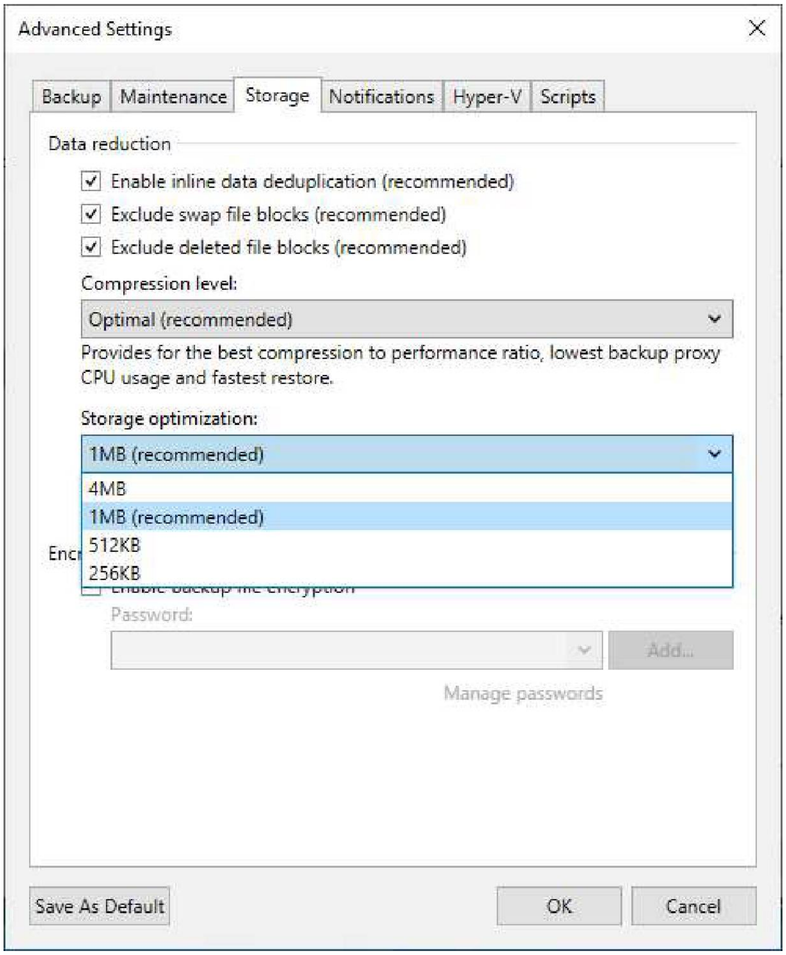
Delivers the optimal combination of backup speed, granular restore performance and repository space consumption.

Encryption

☐ Enable backup file encryption

Password:

45. Select the Storage optimization for the backup from the drop-down list.



Advanced Settings

Data reduction

☑ Enable inline data deduplication (recommended)

☑ Exclude swap file blocks (recommended)

☑ Exclude deleted file blocks (recommended)

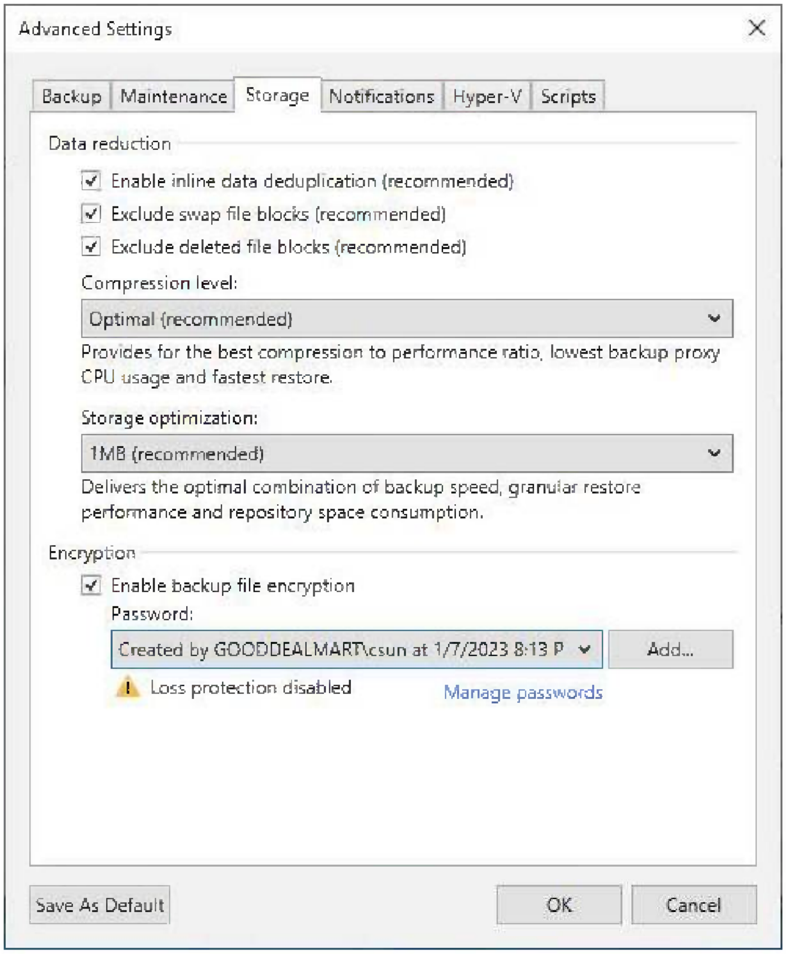
Compression level: Optimal (recommended)

Provides for the best compression to performance ratio, lowest backup proxy CPU usage and fastest restore.

Storage optimization: 1MB (recommended)

46. Select the Enable backup file encryption checkbox to encrypt the content of backup files.

47. Select a password from the drop-down list. Then, if you still need to do, click Add or use the Manage passwords link to create a new password.



Advanced Settings

Data reduction

☑ Enable inline data deduplication (recommended)

☑ Exclude swap file blocks (recommended)

☑ Exclude deleted file blocks (recommended)

Compression level: Optimal (recommended)

Provides for the best compression to performance ratio, lowest backup proxy CPU usage and fastest restore.

Storage optimization: 1MB (recommended)

Delivers the optimal combination of backup speed, granular restore performance and repository space consumption.

Encryption

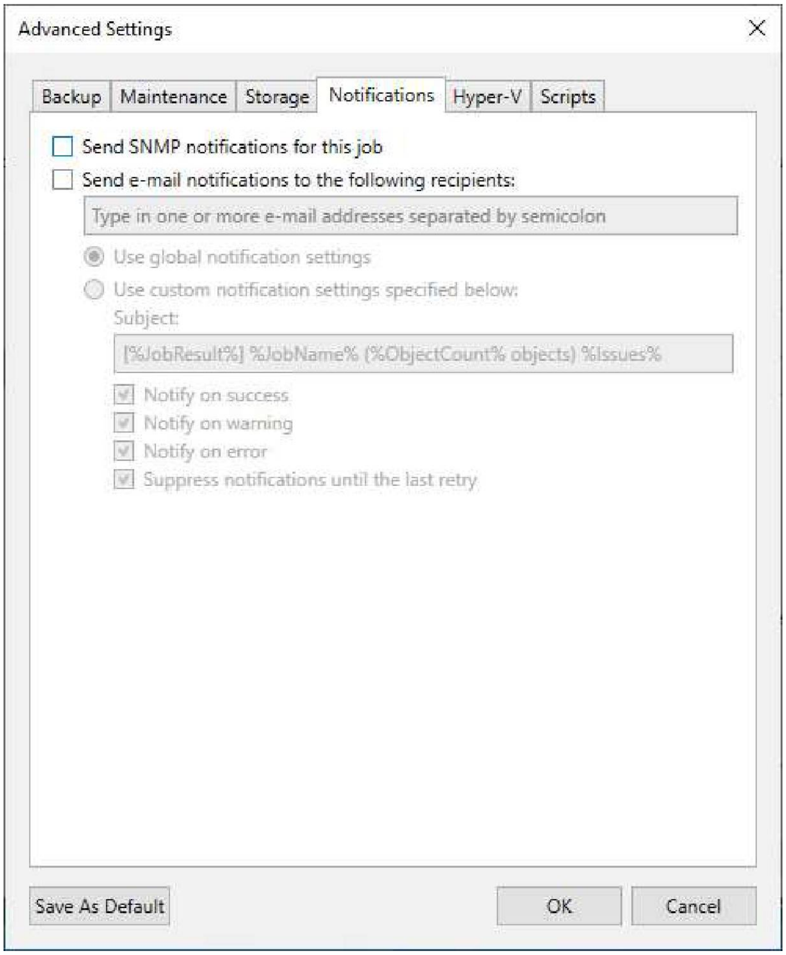
☑ Enable backup file encryption

Password: Created by GOODDEALMART\csun at 1/7/2023 8:13 P

Loss protection disabled

48. On the Advanced Settings, select Notifications.

49. Keep the default settings.



Advanced Settings

Backup | Maintenance | Storage | Notifications | Hyper-V | Scripts

□ Send SNMP notifications for this job

□ Send e-mail notifications to the following recipients:

Type in one or more e-mail addresses separated by semicolon

● Use global notification settings

○ Use custom notification settings specified below:

Subject:

[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

☑ Notify on success

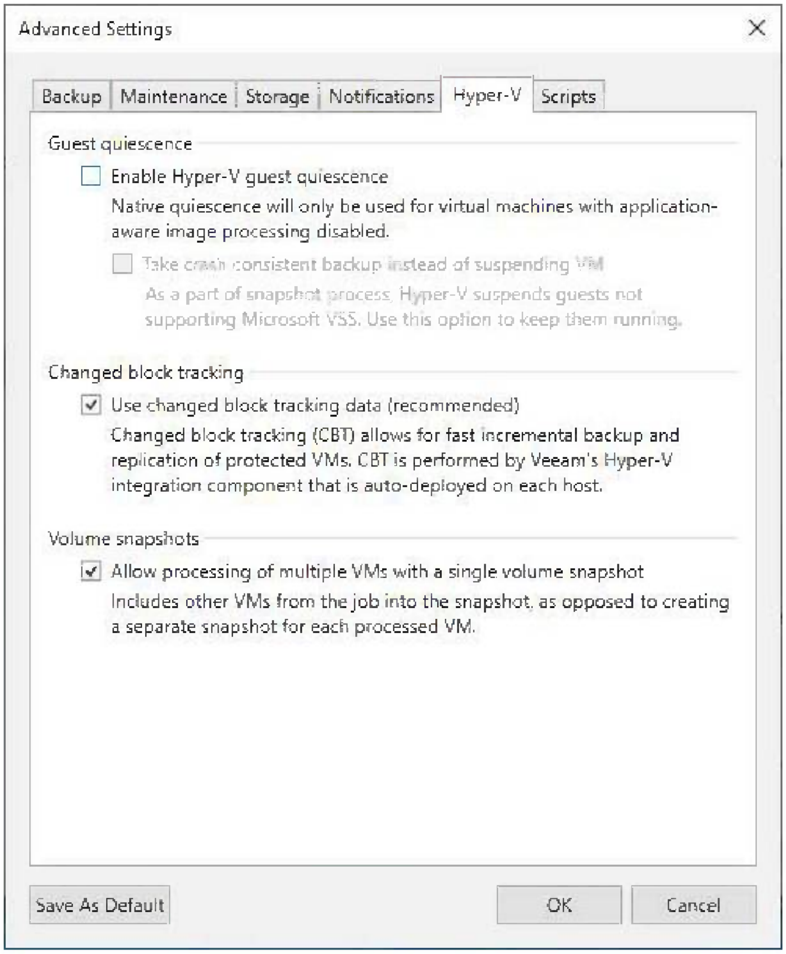
☑ Notify on warning

☑ Notify on error

☑ Suppress notifications until the last retry

50. On the Advanced Settings, select Hyper-V.

51. Keep the default settings.



Guest quiescence

□ Enable Hyper-V guest quiescence

Native quiescence will only be used for virtual machines with application-aware image processing disabled.

□ Take crash consistent backup instead of suspending VM

As a part of snapshot process, Hyper-V suspends guests not supporting Microsoft VSS. Use this option to keep them running.

Changed block tracking

☑ Use changed block tracking data (recommended)

Changed block tracking (CBT) allows for fast incremental backup and replication of protected VMs. CBT is performed by Veeam's Hyper-V integration component that is auto-deployed on each host.

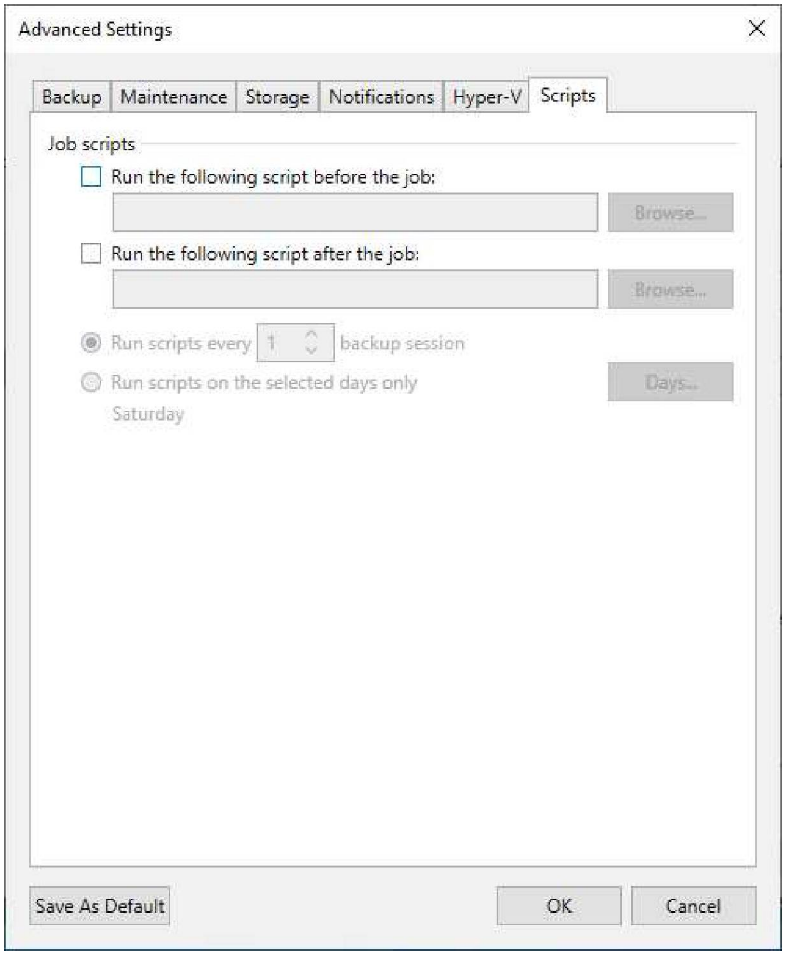
Volume snapshots

☑ Allow processing of multiple VMs with a single volume snapshot

Includes other VMs from the job into the snapshot, as opposed to creating a separate snapshot for each processed VM.

52. On the Advanced Settings page, click Scripts and keep the default settings.

53. Click OK.



Advanced Settings

Job scripts

□ Run the following script before the job:

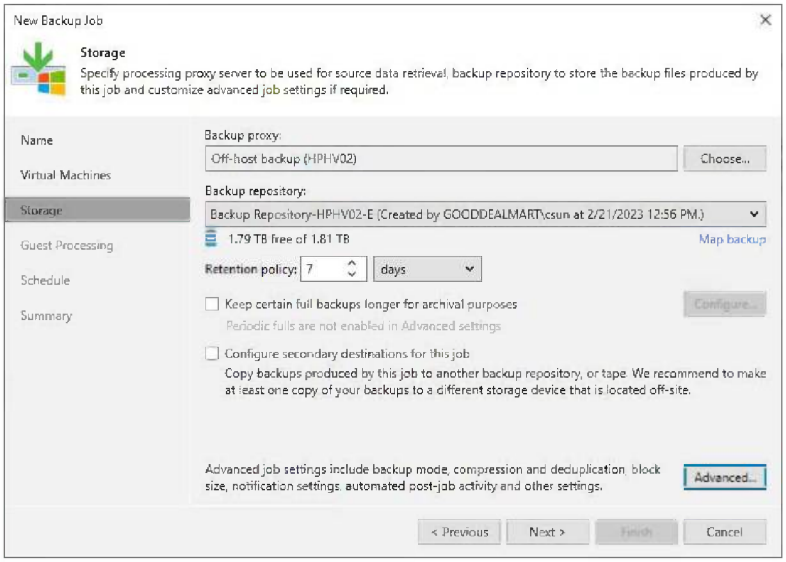
□ Run the following script after the job:

● Run scripts every 1 backup session

○ Run scripts on the selected days only

Saturday

54. Click Next on the Storage page.



New Backup Job

Storage

Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.

Backup proxy: Off-host backup (HPHV02)

Backup repository: Backup Repository-HPHV02-E (Created by GOODDEALMART\csun at 2/21/2023 12:56 PM.)

1.79 TB free of 1.81 TB

Retention policy: 7 days

□ Keep certain full backups longer for archival purposes

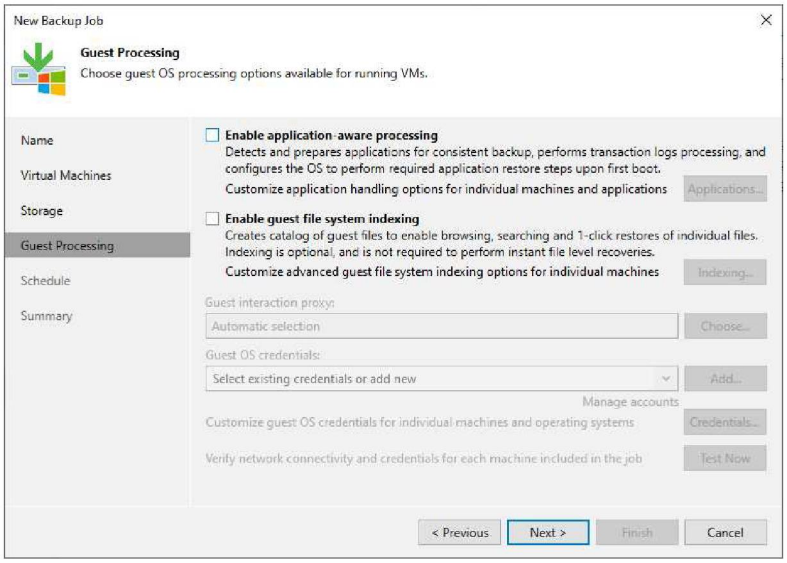
Periodic fulls are not enabled in Advanced settings

□ Configure secondary destinations for this job

Copy backups produced by this job to another backup repository, or tape. We recommend to make at least one copy of your backups to a different storage device that is located off-site.

Advanced job settings include backup mode, compression and deduplication, block size, notification settings, automated post-job activity and other settings.

55. Click Next on the Guess Processing page.



New Backup Job

Guest Processing

Choose guest OS processing options available for running VMs.

□ **Enable application-aware processing**

Detects and prepares applications for consistent backup, performs transaction logs processing, and configures the OS to perform required application restore steps upon first boot.

Customize application handling options for individual machines and applications

□ **Enable guest file system indexing**

Creates catalog of guest files to enable browsing, searching and 1-click restores of individual files. Indexing is optional, and is not required to perform instant file level recoveries.

Customize advanced guest file system indexing options for individual machines

Guest interaction proxy: Automatic selection

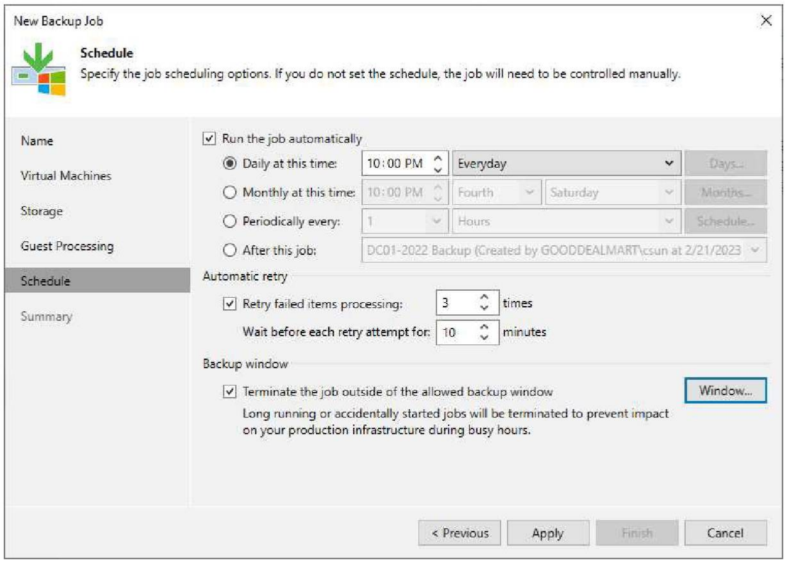
Guest OS credentials: Select existing credentials or add new

Manage accounts

Customize guest OS credentials for individual machines and operating systems

Verify network connectivity and credentials for each machine included in the job

56. Select Run the job automatically checkbox on the Schedule page and select your specified schedule.
57. Define whether Veeam Backup & Replication should retry the backup job if it fails in the Automatic retry section.
58. Define the time interval the backup job must complete in the Backup window section. The backup window ensures that the job does not overlap with production hours and that there is no unnecessary overhead on the production environment.
59. Click Apply.



New Backup Job

Schedule

Specify the job scheduling options. If you do not set the schedule, the job will need to be controlled manually.

☑ Run the job automatically

● Daily at this time: 10:00 PM Everyday

○ Monthly at this time: 10:00 PM Fourth Saturday

○ Periodically every: 1 Hours

○ After this job: DC01-2022 Backup (Created by GOODDEALMART\csun at 2/21/2023

Automatic retry

☑ Retry failed items processing: 3 times

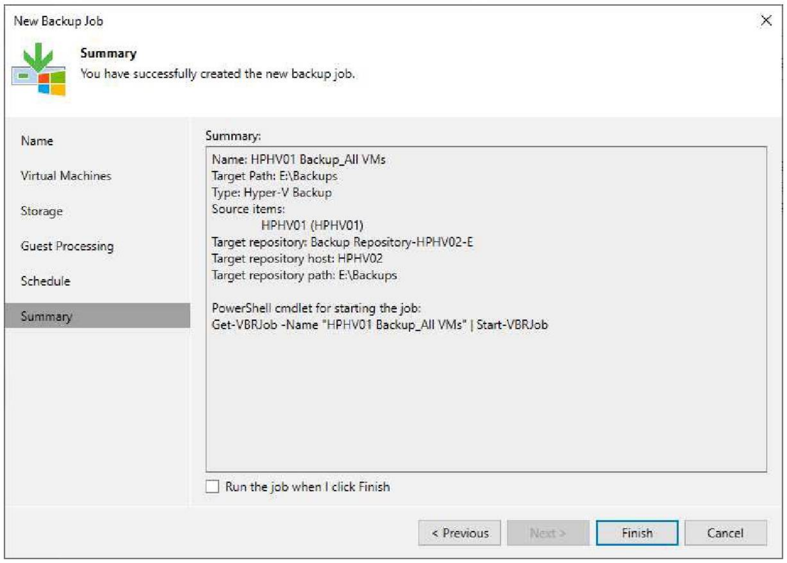
Wait before each retry attempt for: 10 minutes

Backup window

☑ Terminate the job outside of the allowed backup window

Long running or accidentally started jobs will be terminated to prevent impact on your production infrastructure during busy hours.

60. Click Finish on the Summary page.



New Backup Job

Summary

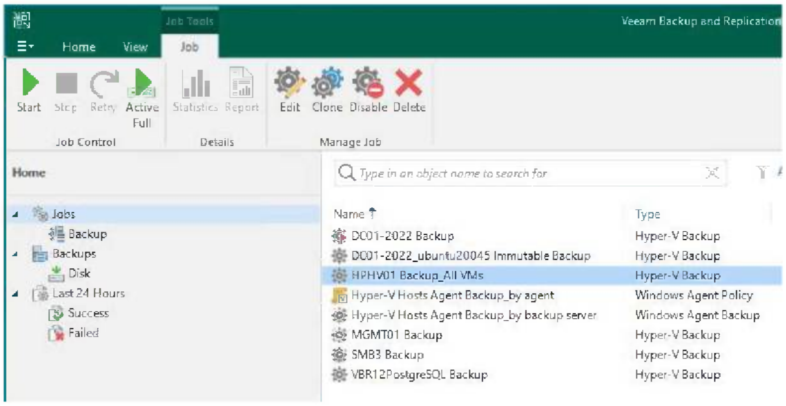
You have successfully created the new backup job.

Summary:

```
Name: HPHV01 Backup_All VMs
Target Path: E:\Backups
Type: Hyper-V Backup
Source items:
        HPHV01 (HPHV01)
Target repository: Backup Repository-HPHV02-E
Target repository host: HPHV02
Target repository path: E:\Backups

PowerShell cmdlet for starting the job:
Get-VBRJob -Name "HPHV01 Backup_All VMs" | Start-VBRJob
```

□ Run the job when I click Finish

61. Verify that the backup job has been added.



Name ↑	Type
DC01-2022 Backup	Hyper-V Backup
DC01-2022_ubuntu20045 Immutable Backup	Hyper-V Backup
HPHV01 Backup_All VMs	Hyper-V Backup
Hyper-V Hosts Agent Backup_by agent	Windows Agent Policy
Hyper-V Hosts Agent Backup_by backup server	Windows Agent Backup
MGMT01 Backup	Hyper-V Backup
SMB3 Backup	Hyper-V Backup
VBR12PostgreSQL Backup	Hyper-V Backup