

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

h [p://www.mvpdays.com](http://www.mvpdays.com)

Copyright © 2023 by MVPDays Publishing

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means without the publisher's prior written permission.

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 some times 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 (Site 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 ranked 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: <http://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

Foreward	iii
About the Authors	v
Dave Kawula – Microsoft MVP	v
Cristal Kawula – Microsoft MVP	vi
Cary Sun – Microsoft MVP	vii
Emile Cabot – Microsoft MVP	viii
Contents	ix
Introduction	14
Sample Files	14
Additional Resources	14
Chapter 1	15
Prerequisites	15
System Requirements	15
Veeam Back and Replication Manager Server	15
Veeam Backup and Replication Console Server	16
Veeam Backup and Replication Off-Host Backup Proxy Server	16
Veeam Backup and Replication Proxy Server for NAS Backup	17
Veeam Backup Repository Server	17
Veeam Tape Server	17

Veeam WAN Accelerator	18
Veeam Backup & Replication Gateway Server	18
Supported Applications.....	19
Firewall Open Ports Requirements	19
Windows Servers	20
Linux Servers	20
Veeam Backup Manager Server.....	21
Veeam Backup & Replication Console	23
Veeam Backup Proxy server	23
Windows and Linux-based Backup Repository	24
NFS Share Backup Repository.....	25
Windows SMB Backup Repository	25
Azure Object Storage Repository	26
External Repository	26
Azure Archive Object Storage Repository.....	27
Veeam Gateway Server	28
Veeam Tape Server.....	29
Veeam WAN Accelerator Server.....	29
Veeam Guest Interaction Proxy with Non-Persistent Runtime Components	30
Veeam Guest Interaction Proxy with Persistent Agent Components	31
Log Shipping Server Connections	31
SQL Guest OS Connections.....	32
Oracle Guest OS Connections	33
Veeam Mount Server.....	34
Veeam Helper Appliance	35

Veeam Helper Host	35
VM Guest OS	36
Veeam U-AIR	37
Application Item of Active Directory Domain Controller Restore	37
Application Item of Exchange Server Restore	38
Application Item of SQL Server Restore	38
Azure Proxy Server	39
Azure Helper Appliance	39
Azure Stack.....	39
SMTP Server.....	40
Chapter 2.....	41
Deployment.....	41
Install Veeam Backup and Replication v12 with PostgreSQL	43
Install Veeam Backup and Replication v12 with Microsoft SQL (or SQL Express)	53
Upgrade the Existing Veeam Backup and Replication to v12	63
Migrate the Existing Veeam Backup and Replication to the new server with PostgreSQL	83
Migrate the Existing Veeam Backup and Replication to the new server with Microsoft SQL	96
Install Veeam Backup and Replication Console 12.....	109
Upgrade to Veeam Backup and Replication Console 12	116
Chapter 3.....	122
Configuration.....	122
Virtualization Servers and Hosts	123
Add Microsoft Hyper-V Standalone Servers	124

Add Microsoft Hyper-V Clusters	132
Add Microsoft SMB3 Servers	140
Add Microsoft Windows Servers.....	149
Add Linux Server for a hardened repository	157
Add Off-Host Backup proxy servers	166
Add WAN Acceleration	177
Physical Machines	183
Add Veeam Agent to On-Premises Microsoft Windows Physical machines	184
Add Veeam Agent to On-Premises Linux Physical machines	198
Backup Repository.....	211
Add the Microsoft Windows server's local directory as a Backup Repository.....	212
Add the Linux server's local directory as a Backup Repository.....	221
Add the Linux server's local directory as a Hardened Backup Repository	233
Add Network Attached Storage (SMB or CIFS Shares) as Backup Repository ...	245
Add the Microsoft Windows server's Rotated Drives as a Backup Repository	253
General and User Roles Settings.....	263
Configure Multi-Factor Authentication for Users	265
Configure Group Managed Service Accounts (gMSA).....	276
Configure Notification with Free SendGrid Account of Azure	287
Configure Notification with Microsoft Office 365 NON-MFA Account.....	317
Configure Notification with Microsoft Office 365 MFA Account.....	331
Enable Configuration Backup	355
Configure Best Practices Analyzer	362
Chapter 4.....	367

Backup 367

 Create a Backup job to backup the specified VMs..... 368

 Create an Immutable Backup job to backup the specified VMs 406

 Create a Backup job to backup the specified Physical Machines (Managed by Backup Server Mode)..... 442

 Create a Backup job to backup the specified Physical Machines (Managed by Agent Mode) 474

 Create a Backup job to backup all VMS of the Hyper-V Host 506

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 Replica on, all conditions must be met.

System Requirements

Before installing Veeam Backup and Replica on, 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 replica on manager server.

Components	Description
OS Platform	Windows Server 2022, 2019, 2016, 2012 R2, 2012, 11 (version 21H2, 22H2), 10 (from version 1909 to version 22H2), 10 LTS (versions LTSC 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 (version 21H2, 22H2), 10 (from version 1909 to version 22H2), 10 LTS (versions LTSC 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 (version 21H2, 22H2), 10 (from version 1909 to version 22H2), 10 LTS (versions LTSC 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 (version 21H2, 22H2), 10 (from version 1909 to version 22H2), 10 LTS (versions LTSC 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 Pla orm	Windows Server 2022, 2019, 2016, 2012 R2, 2012, 11 (version21H2, 22H2), 10 (from version 1909 to version 22H2), 10 LTS (versions LTSC 1607, LTSC 1809, LTSC 2021)
Linux distribu ons (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	Descrip on
Windows OS Pla orm	Windows Server 2022, 2019, 2016, 2012 R2, 2012, 11 (version21H2, 22H2), 10 (from version 1909 to version 22H2), 0 LTS (versions LTSC 1607, LTSC 1809, LTSC 2021)

Veeam Backup & Replication Gateway Server

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

Components	Descrip on
Windows OS Pla orm	Windows Server 2022, 2019, 2016, 2012 R2, 2012, 11 (version21H2, 22H2), 10 (from version 1909 to version 22H2), 0 LTS (versions LTSC 1607, LTSC 1809, LTSC 2021)
Linux distribu ons	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 applications for on-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 & Replica on 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 & replica on 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 & replica on manager server	Linux servers	TCP	22
		TCP	6162
		TCP	2500 to 3300
Linux Servers	Veeam backup & replica on manager server	TCP	2500 to 3300

Veeam Backup Manager Server

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

Sources	Target	Network Protocol	Port Number
Veeam backup & replica on 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 & Replica on	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	2049
		UDP	
	NFS share as a backup repository (version 3)	TCP	111
		UDP	
		TCP	mountd_port
		UDP	
		TCP	statd_port
		UDP	
		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 replica on manager server	Veeam tape server	TCP	6166
		TCP	2500 to 3300
Veeam tape server	Veeam backup and replica on 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 replica on manager server	Veeam WAN accelerator server	TCP	6160
		TCP	6162

		TCP	6164
Veeam WAN accelerator server	Veeam backup and replica on 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 replica on 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 interac on proxy	TCP	2500 to 3300

Veeam Guest Interaction Proxy with Persistent Agent Components

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

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

Log Shipping Server Connections

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

Sources	Target	Network Protocol	Port Number
	Log shipping server	TCP	445

Veeam backup and replica on 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 interac on 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 interac on 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 replica on 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 replica on 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 replica on 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 replica on 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 replica on 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 replica on 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 replica on 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 replica on 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 replica on 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 replica on 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 replica on manager server	SMTP server	TCP	25

Chapter 2

Deployment

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

Veeam Backup and Replica on 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
- VeeamMover
- 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

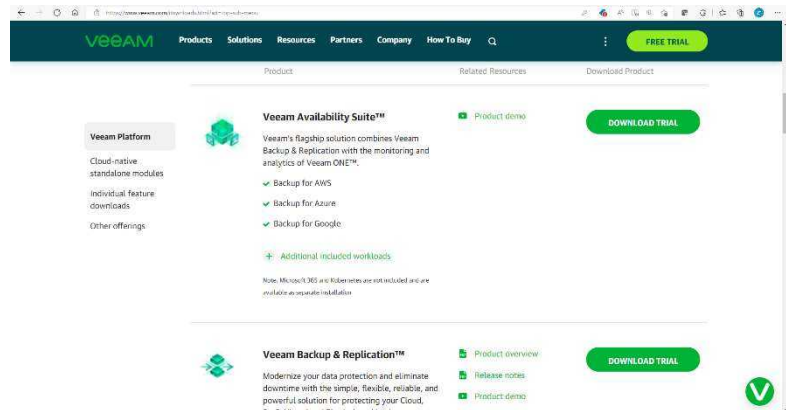
When you install Veeam Backup & Replication on the Veeam Backup & Replication console is automatically installed on the backup server.

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.

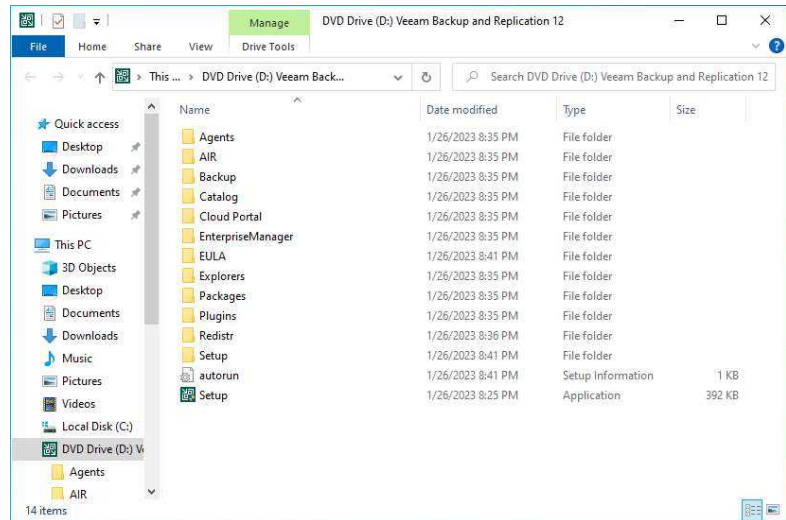
Instructions

Screenshot (if applicable)

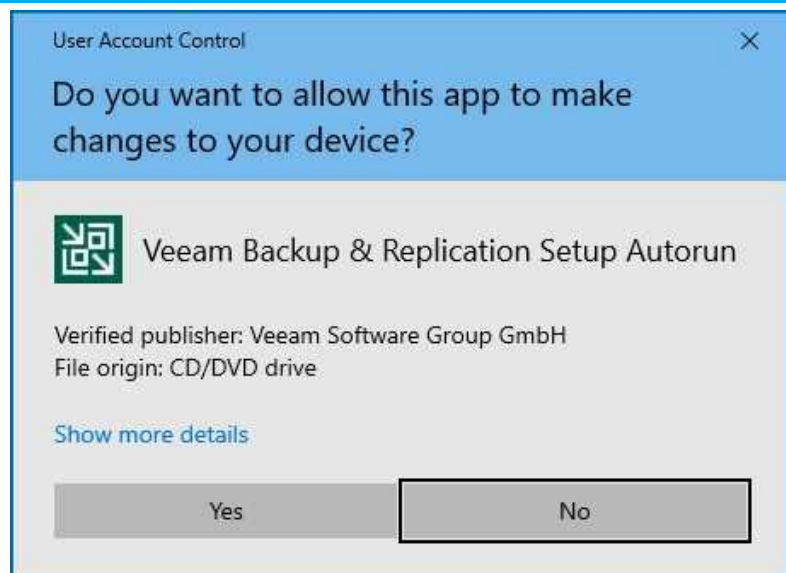
1. Log in to the Veeam Backup and Replication manager server.
2. Download the Veeam Backup and Replication v12 ISO image file from the Veeam website sign-in (required).



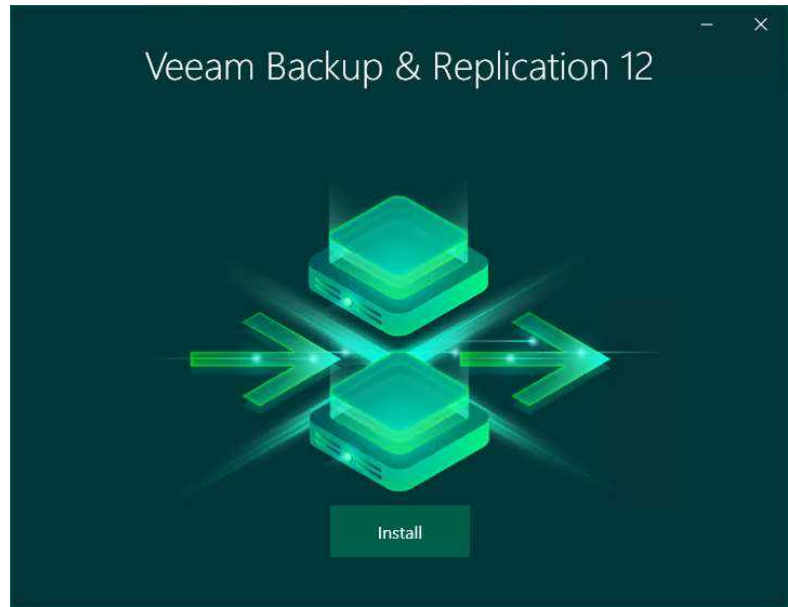
3. Mount the Veeam Backup and Replica on v12 iso image file.
4. Run Setup.exe.



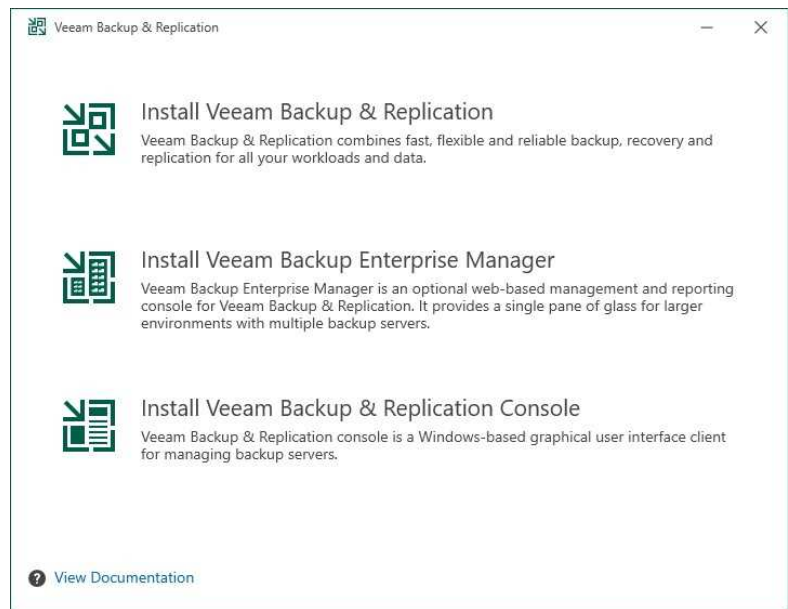
5. On the User Access Control page, click Yes.



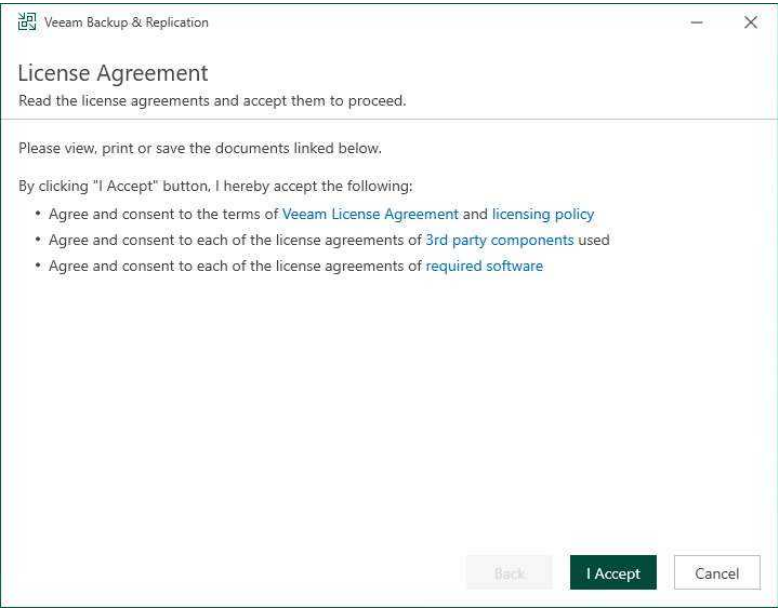
6. On the Veeam Backup & Replication 12 page, click Install.



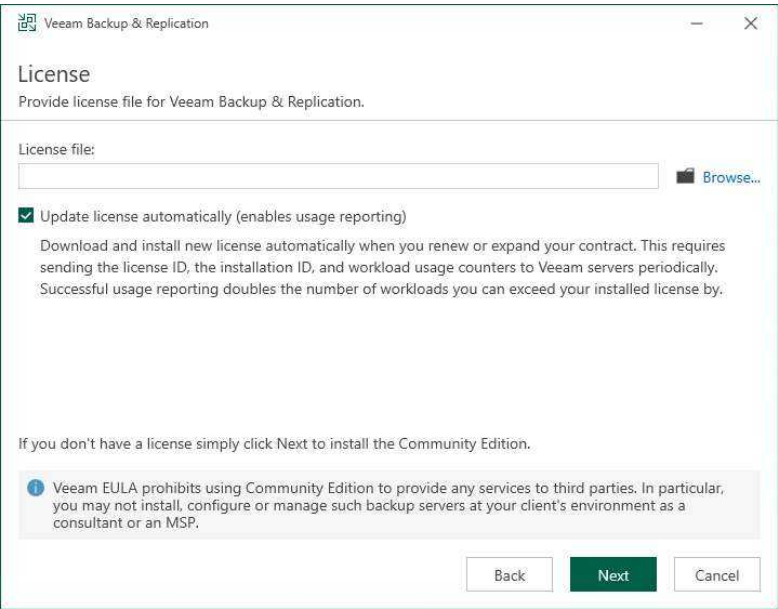
7. Select Install Veeam Backup & Replication on the Veeam Backup & Replication page.



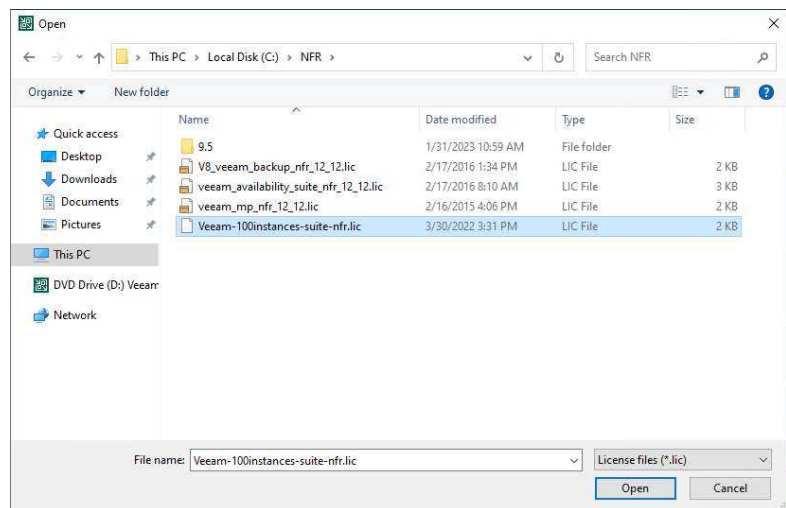
8. Click I Accept on the License Agreement page.



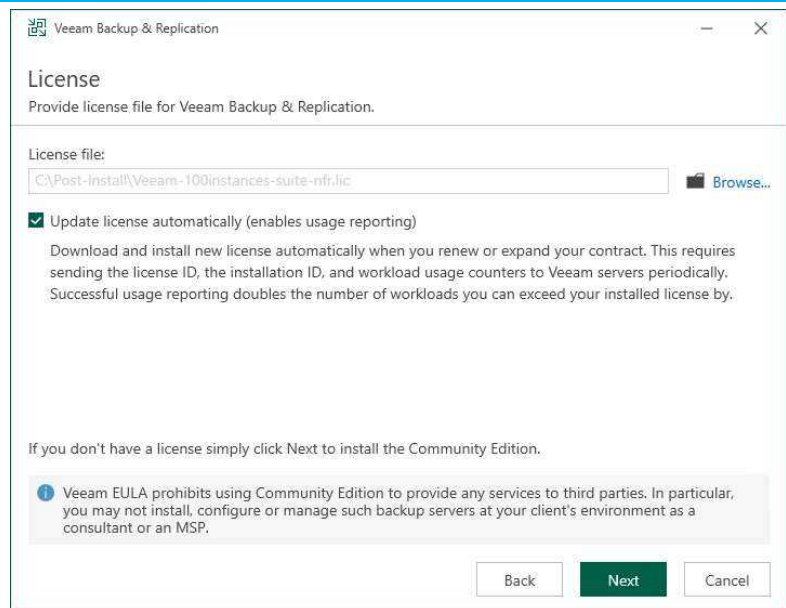
9. Click Browse on the License page.



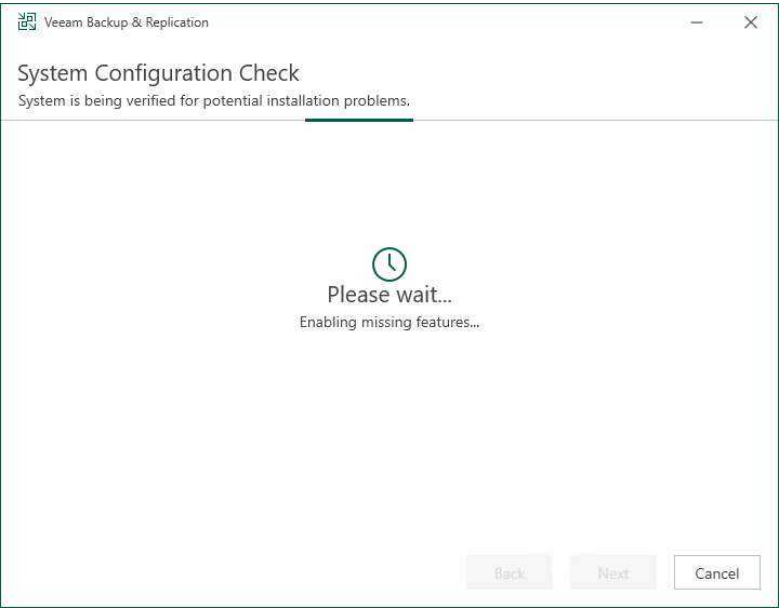
10. Select a license file for Veeam Backup & Replication and click Open.



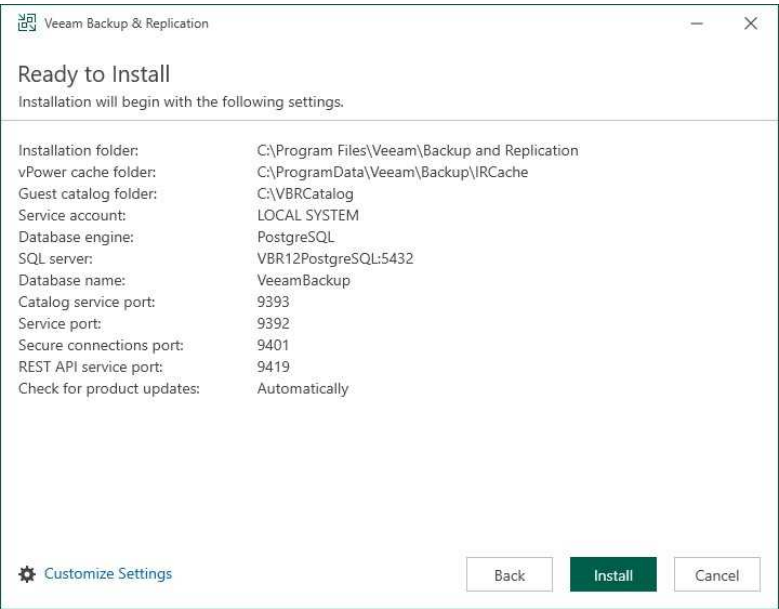
11. On the License page, select Update license automatically (enable usage reporting). It will automatically download and install a new license when you renew or expand your contract.
12. Click Next.



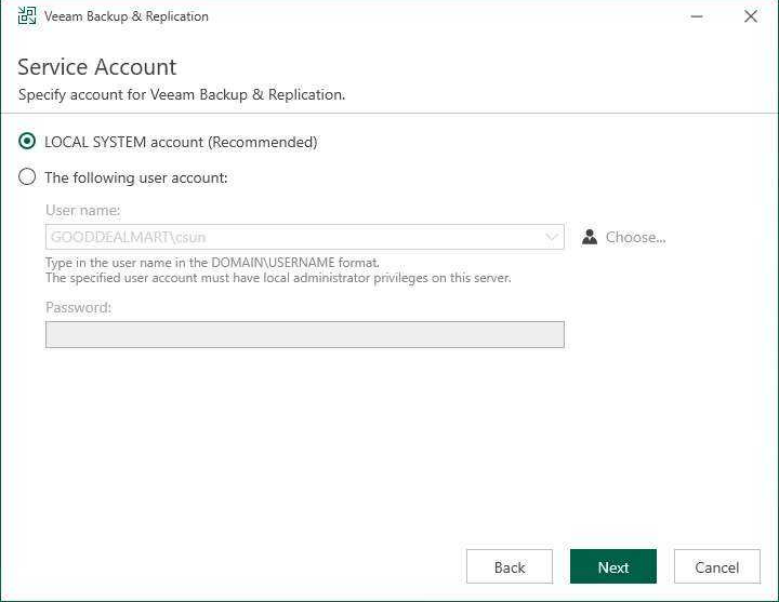
13. The setup wizard checks if the required software is installed on the machine during the System Configuration Check step. If required components are missing, the setup will attempt to install them independently. Rebooting is required after the components have been successfully installed. Click Reboot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



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

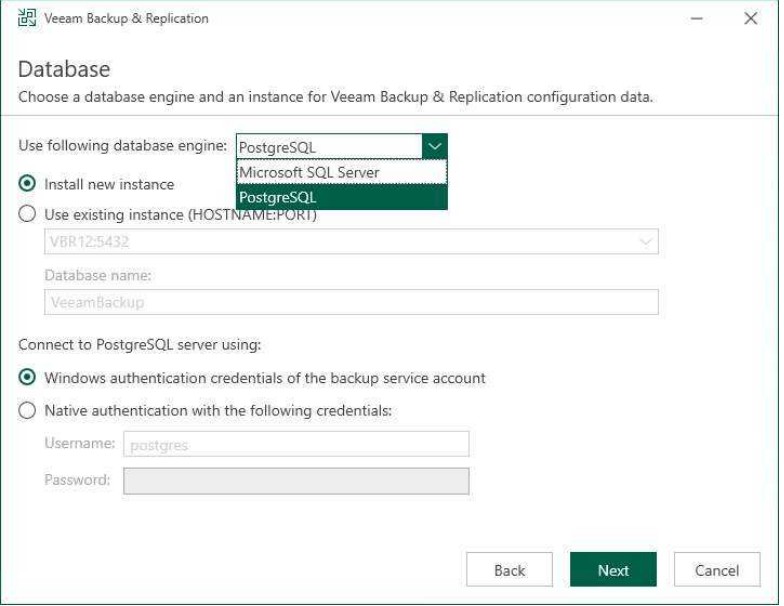


15. On the Service Account page, select LOCAL SYSTEM account and click Next.



The screenshot shows the 'Service Account' configuration window in Veeam Backup & Replication. The window title is 'Veeam Backup & Replication' and the subtitle is 'Service Account'. The main instruction is 'Specify account for Veeam Backup & Replication.' There are two radio button options: 'LOCAL SYSTEM account (Recommended)' which is selected, and 'The following user account:'. Below the second option, there are fields for 'User name:' (containing 'GOODDEALMART\csun') and 'Password:'. A 'Choose...' button is next to the user name field. A note states: 'Type in the user name in the DOMAIN\USERNAME format. The specified user account must have local administrator privileges on this server.' At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

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.



The screenshot shows the 'Database' configuration window in Veeam Backup & Replication. The window title is 'Veeam Backup & Replication' and the subtitle is 'Database'. The main instruction is 'Choose a database engine and an instance for Veeam Backup & Replication configuration data.' There are two radio button options: 'Install new instance' which is selected, and 'Use existing instance (HOSTNAME:PORT)'. Below the second option, there is a dropdown menu for 'Use following database engine:' showing 'PostgreSQL', 'Microsoft SQL Server', and 'PostgreSQL'. Below this, there is a dropdown for 'VBR12:5432'. There is a 'Database name:' field containing 'VeeamBackup'. Below this, there is a section 'Connect to PostgreSQL server using:' with two radio button options: 'Windows authentication credentials of the backup service account' which is selected, and 'Native authentication with the following credentials:'. Below the second option, there are fields for 'Username:' (containing 'postgres') and 'Password:'. At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

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.

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.

The screenshot shows the 'Database' configuration window in Veeam Backup & Replication. The window title is 'Veeam Backup & Replication'. The subtitle is 'Database'. The main instruction is 'Choose a database engine and an instance for Veeam Backup & Replication configuration data.'.

The 'Use following database engine:' dropdown is set to 'PostgreSQL'.

There are two radio buttons for instance selection:

- ☐ Install new instance
- ☒ Use existing instance (HOSTNAME:PORT)

The 'Use existing instance' option is selected, and the dropdown below it shows 'VBR12PostgreSQL:5432'.

The 'Database name:' text box contains 'VeeamBackup'.

Under 'Connect to PostgreSQL server using:', there are two radio buttons:

- ☒ Windows authentication credentials of the backup service account
- ☐ Native authentication with the following credentials:

The 'Native authentication' option is not selected, so the 'Username:' and 'Password:' text boxes are empty.

At the bottom right, there are three buttons: 'Back', 'Next' (highlighted in green), and 'Cancel'.

- 2. Start the PostgreSQL service again.

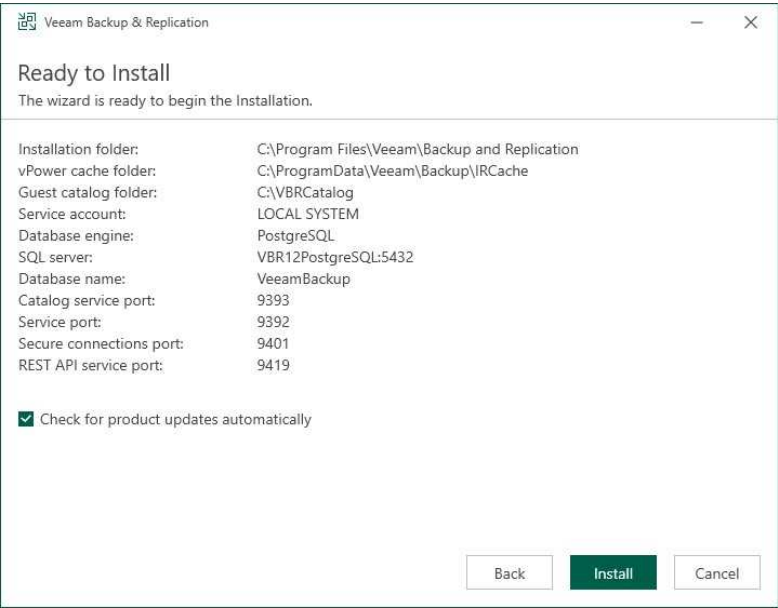
- 22. On the Data locations page, click Browse and select the path in the Installation path field.
- 23. Browse and select the path in the Guest file system catalog: field.
- 24. Click Browse and select the path in the Instant recovery write cache field.
- 25. Click Next.

The screenshot shows the 'Data Locations' configuration window in Veeam Backup & Replication. The window title is 'Veeam Backup & Replication'. The subtitle is 'Data Locations'. Below the subtitle is the instruction 'Specify paths for persistent and non-persistent data storage locations.' There are three text input fields, each with a 'Browse...' button to its right. The first field is labeled 'Installation path:' and contains the text 'C:\Program Files\Veeam\Backup and Replication'. The second field is labeled 'Guest file system catalog:' and contains the text 'C:\VBRCatalog'. The third field is labeled 'Instant recovery write cache:' and contains the text 'C:\ProgramData\Veeam\Backup\IRCache'. Below these fields is a blue information icon followed by a warning message: '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.' At the bottom right of the window are three buttons: 'Back', 'Next' (highlighted in green), and 'Cancel'.

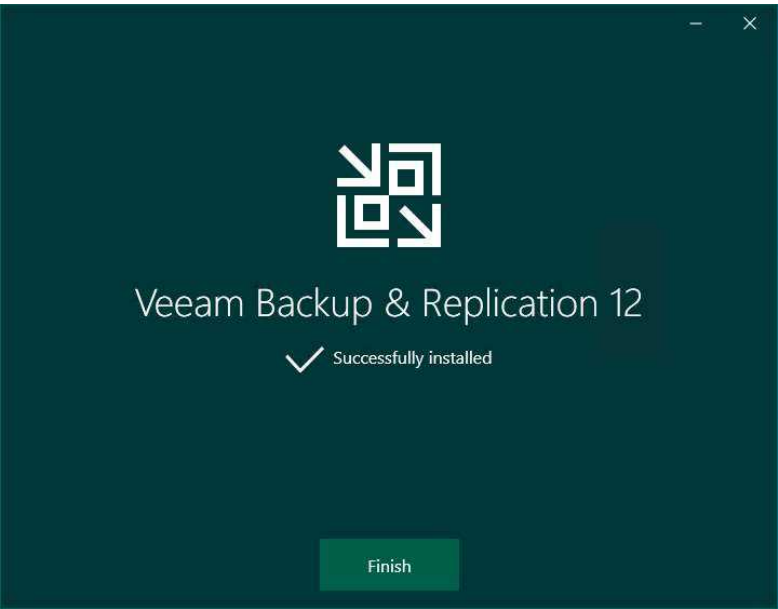
- 26. On the Port Configuration page, specify the port configuration to be used by Veeam Backup and Replication and click Next.

The screenshot shows the 'Port Configuration' window in Veeam Backup & Replication. The window title is 'Veeam Backup & Replication'. The subtitle is 'Port Configuration'. Below the subtitle is the instruction 'Specify port configuration to be used by Veeam Backup & Replication.' There are four text input fields. The first is labeled 'Catalog service port:' and contains the value '9393'. The second is labeled 'Veeam Backup service port:' and contains the value '9392'. The third is labeled 'Secure connections port:' and contains the value '9401'. The fourth is labeled 'REST API service port:' and contains the value '9419'. At the bottom right of the window are three buttons: 'Back', 'Next' (highlighted in green), and 'Cancel'.

27. Click Install on the Ready to Install page.



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



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.

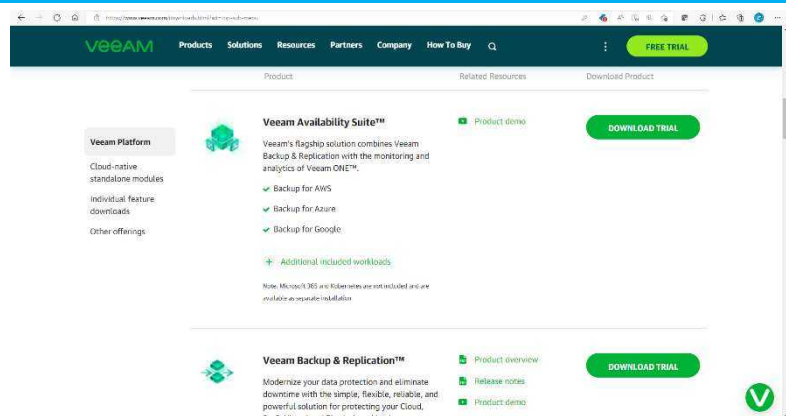
You can choose Microsoft SQL as a Veeam Backup & Replication database. However, you installed a Microsoft SQL Server (or Express), either locally on the backup manager server or remotely. If Microsoft SQL Server is not already installed. In that case, the Veeam Backup & Replication won't install the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

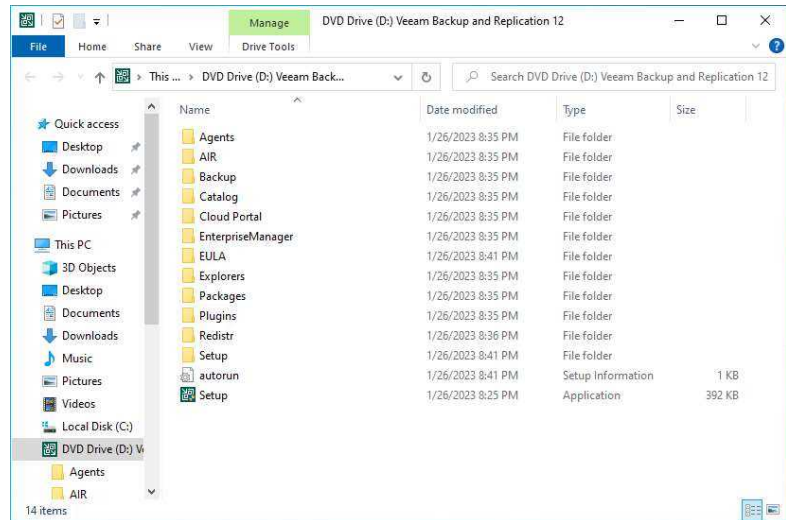
Instructions

Screenshot (if applicable)

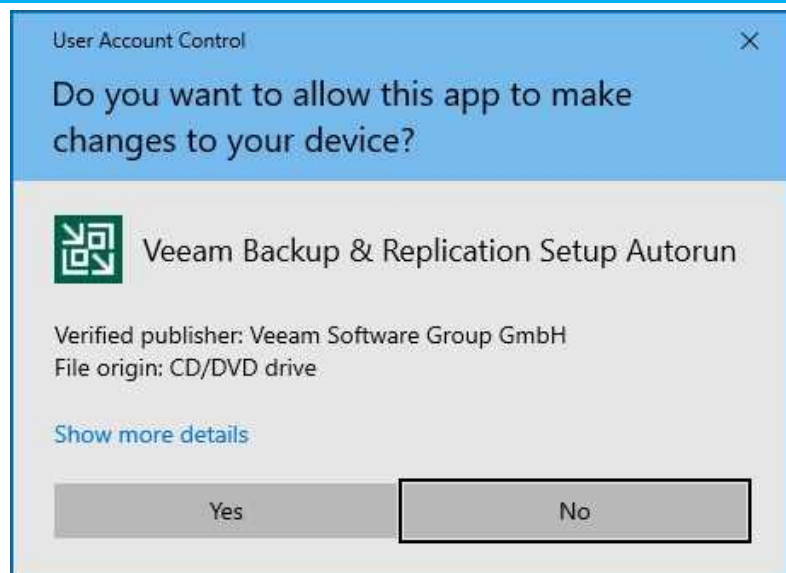
1. Ensure the Microsoft SQL Server or Microsoft SQL Server Express is installed locally or remotely.
2. Log in to the Veeam Backup and Replication manager server.
3. Download the Veeam Backup and Replication v12 ISO image file from the Veeam website sign-in (required).



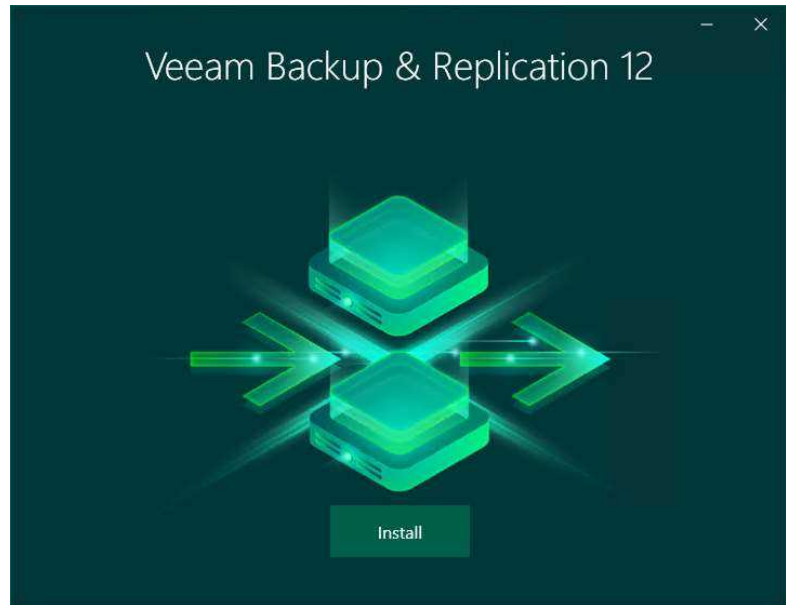
4. Mount the Veeam Backup and Replica on v12 iso image file.
5. Run Setup.exe.



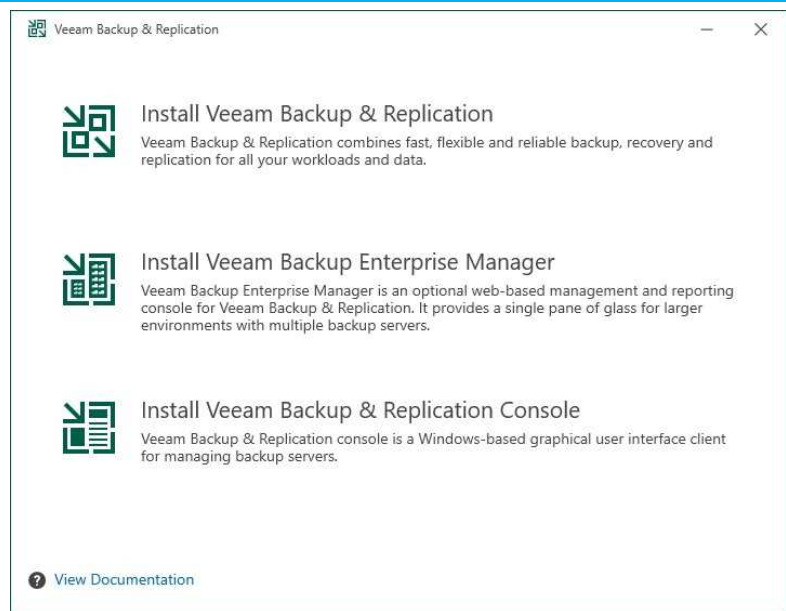
6. On the User Access Control page, click Yes.



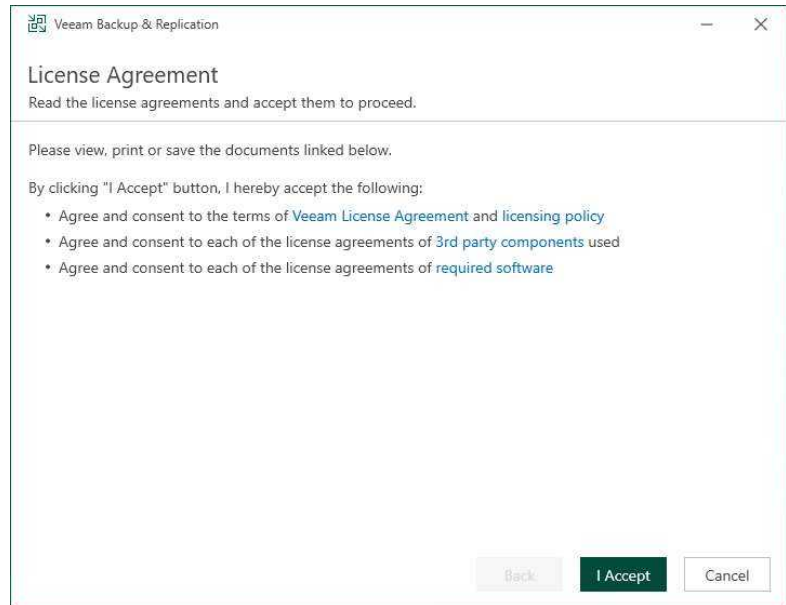
7. On the Veeam Backup & Replication 12 page, click Install.



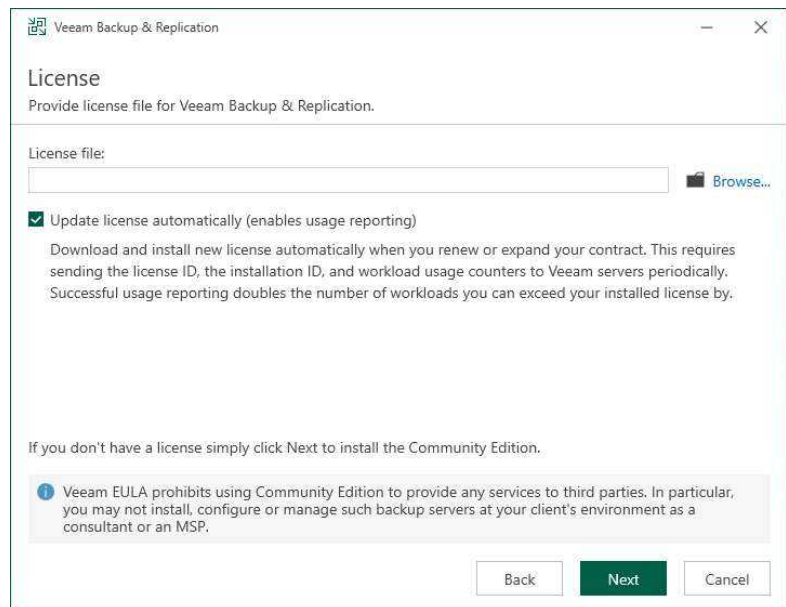
8. Select Install Veeam Backup & Replication on the Veeam Backup & Replication page.



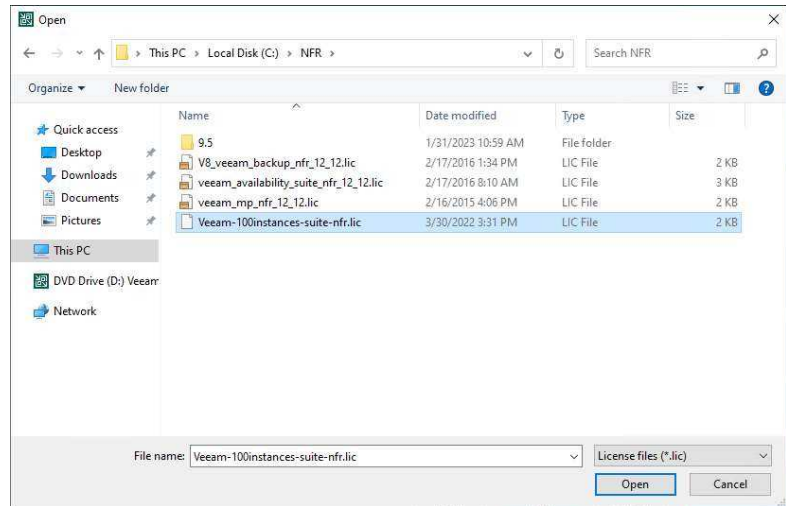
9. Click I Accept on the License Agreement page.



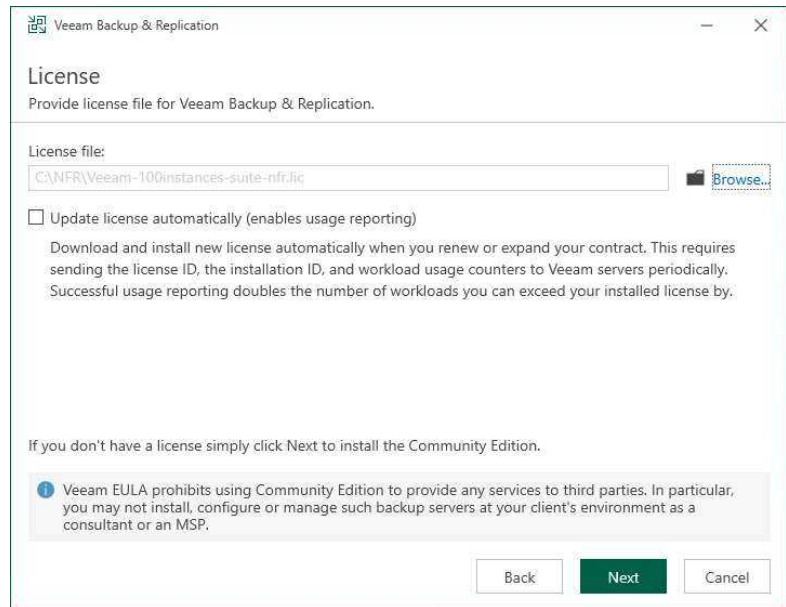
10. Click Browse on the License page.



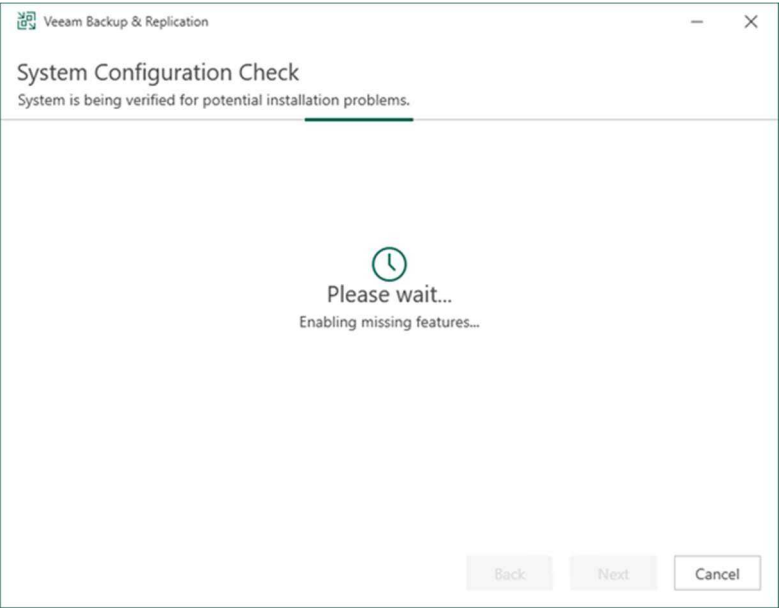
11. Select a license file for Veeam Backup & Replication and click Open.



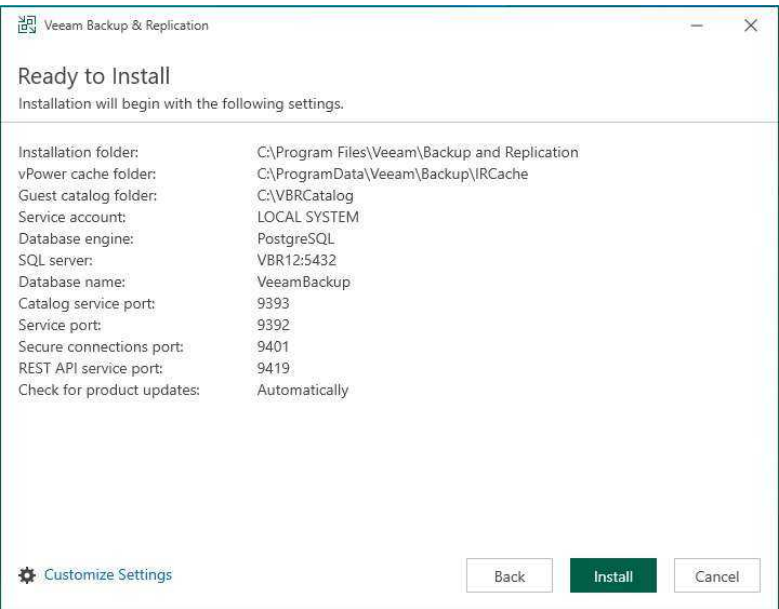
12. On the License page, select Update license automatically (enable usage reporting). It will automatically download and install a new license when you renew or expand your contract.
13. Click Next.



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.



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



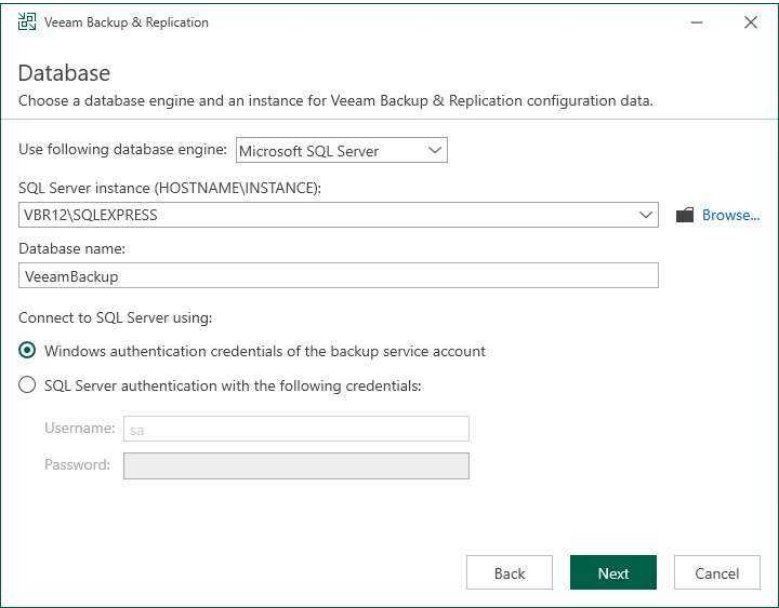
16. On the Service Account page, select LOCAL SYSTEM account and click Next.

The screenshot shows the 'Service Account' configuration window in Veeam Backup & Replication. The window title is 'Veeam Backup & Replication'. The main heading is 'Service Account' with the subtitle 'Specify account for Veeam Backup & Replication.' There are two radio button options: 'LOCAL SYSTEM account (Recommended)' which is selected, and 'The following user account:'. Below the second option, there are fields for 'User name:' (containing 'GOODDEALMART\csun') and 'Password:'. A 'Choose...' button is next to the user name field. A note states: 'Type in the user name in the DOMAIN\USERNAME format. The specified user account must have local administrator privileges on this server.' At the bottom right, there are three buttons: 'Back', 'Next' (highlighted in green), and 'Cancel'.

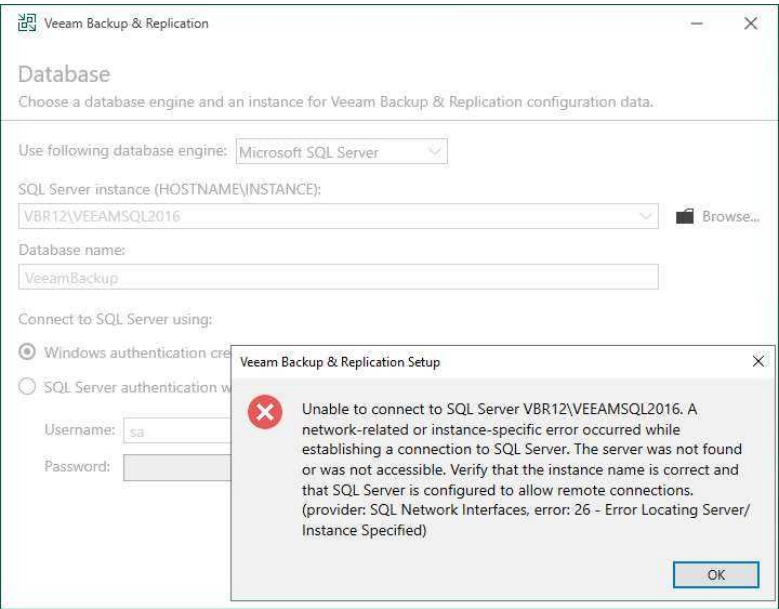
17. On the Database page, select the Microsoft SQL Server from the database engine drop-down list.

The screenshot shows the 'Database' configuration window in Veeam Backup & Replication. The window title is 'Veeam Backup & Replication'. The main heading is 'Database' with the subtitle 'Choose a database engine and an instance for Veeam Backup & Replication configuration data.' There are two radio button options: 'Install new instance' which is selected, and 'Use existing instance (HOSTNAME:PORT)'. Below the second option, there is a text field containing 'VBR12:5432'. There is a 'Database name:' field containing 'VeeamBackup'. A dropdown menu for 'Use following database engine:' is open, showing 'PostgreSQL' (selected), 'Microsoft SQL Server', and 'PostgreSQL'. Below this, there is a section 'Connect to PostgreSQL server using:' with two radio button options: 'Windows authentication credentials of the backup service account' which is selected, and 'Native authentication with the following credentials:'. Below the second option, there are fields for 'Username:' (containing 'postgres') and 'Password:'. At the bottom right, there are three buttons: 'Back', 'Next' (highlighted in green), and 'Cancel'.

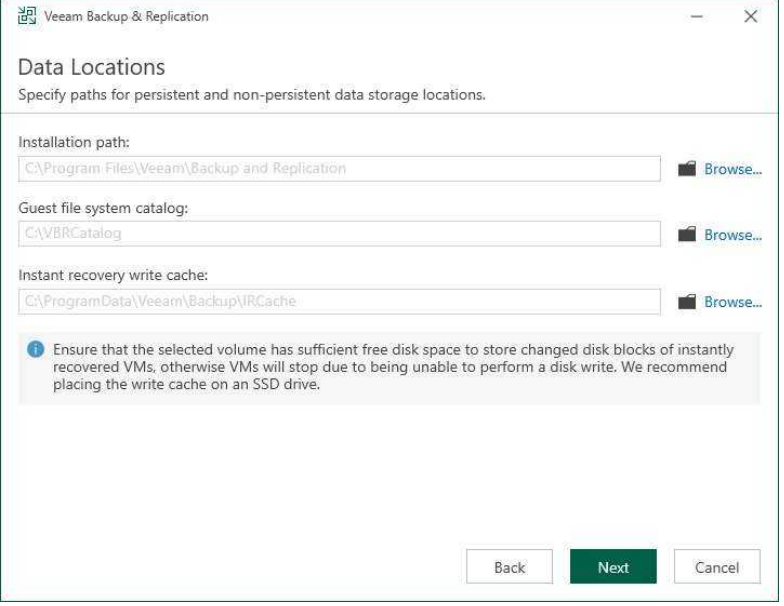
- 18. Click Browse to select the SQL server and instance on the SQL Server instance session.
- 19. Select Windows authentication credentials of the backup service account to connect to SQL Server.
- 20. Click Next.



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

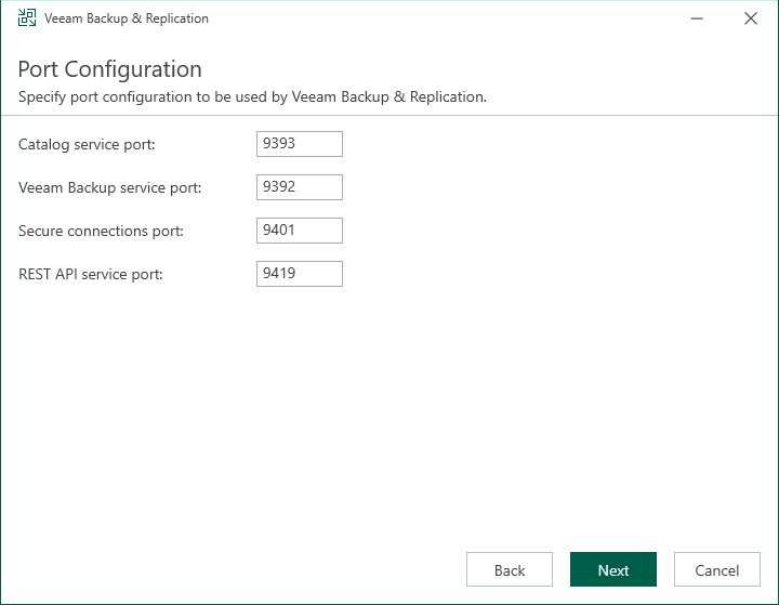


22. On the Data locations page, click Browse and select the path in the Installation path field.
23. Browse and select the path in the Guest file system catalog: field.
24. Click Browse and select the path in the Instant recovery write cache field.
25. Click Next.



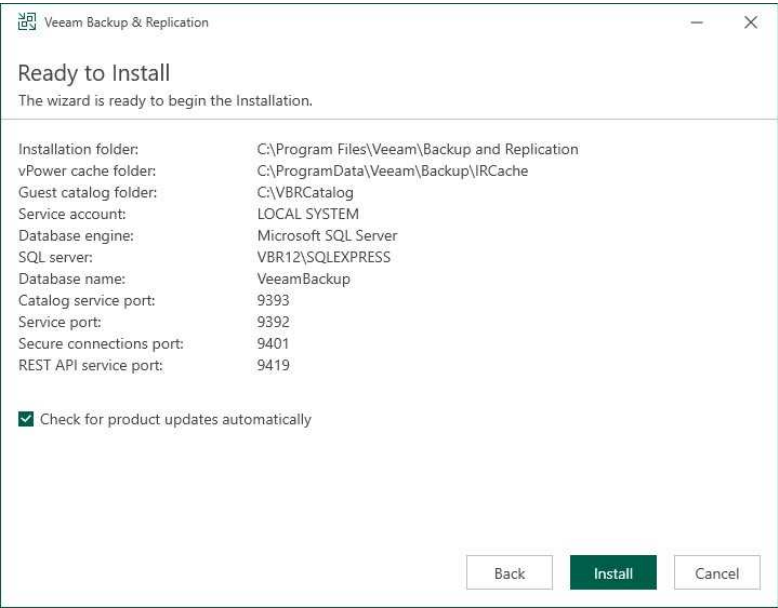
The screenshot shows the 'Data Locations' configuration window in Veeam Backup & Replication. The window title is 'Veeam Backup & Replication'. The subtitle is 'Data Locations'. Below the subtitle is the instruction 'Specify paths for persistent and non-persistent data storage locations.' There are three text input fields, each with a 'Browse...' button to its right. The first field is 'Installation path:' with the value 'C:\Program Files\Veeam\Backup and Replication'. The second field is 'Guest file system catalog:' with the value 'C:\VBRCatalog'. The third field is 'Instant recovery write cache:' with the value 'C:\ProgramData\Veeam\Backup\IRCache'. Below these fields is a blue information icon followed by a note: '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.' At the bottom right are three buttons: 'Back', 'Next' (highlighted in green), and 'Cancel'.

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

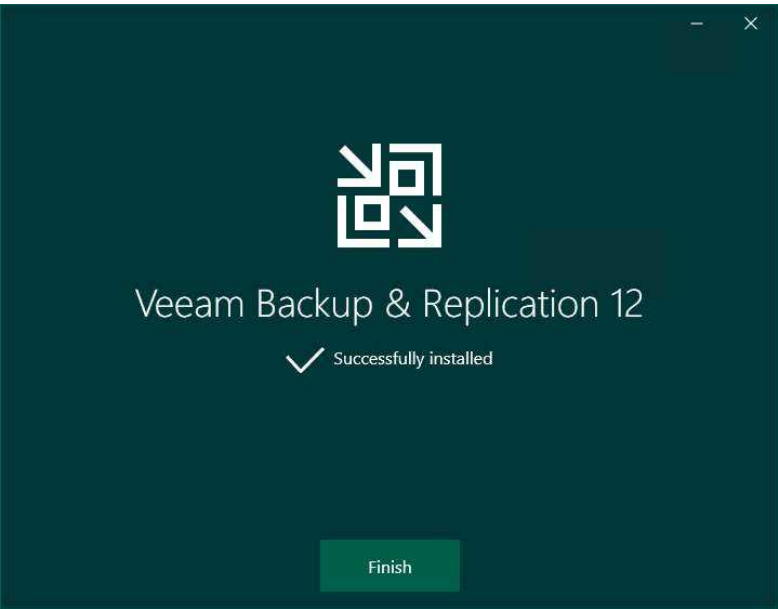


The screenshot shows the 'Port Configuration' window in Veeam Backup & Replication. The window title is 'Veeam Backup & Replication'. The subtitle is 'Port Configuration'. Below the subtitle is the instruction 'Specify port configuration to be used by Veeam Backup & Replication.' There are four text input fields. The first is 'Catalog service port:' with the value '9393'. The second is 'Veeam Backup service port:' with the value '9392'. The third is 'Secure connections port:' with the value '9401'. The fourth is 'REST API service port:' with the value '9419'. At the bottom right are three buttons: 'Back', 'Next' (highlighted in green), and 'Cancel'.

27. Click Install on the Ready to Install page.

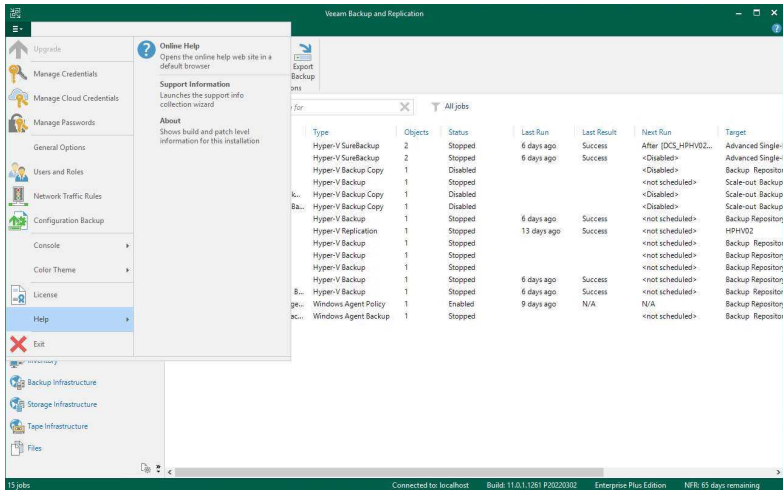


28. Click Finish on the Veeam Backup & Replication 12 Successfully installed page.



Upgrade the Existing Veeam Backup and Replication to v12

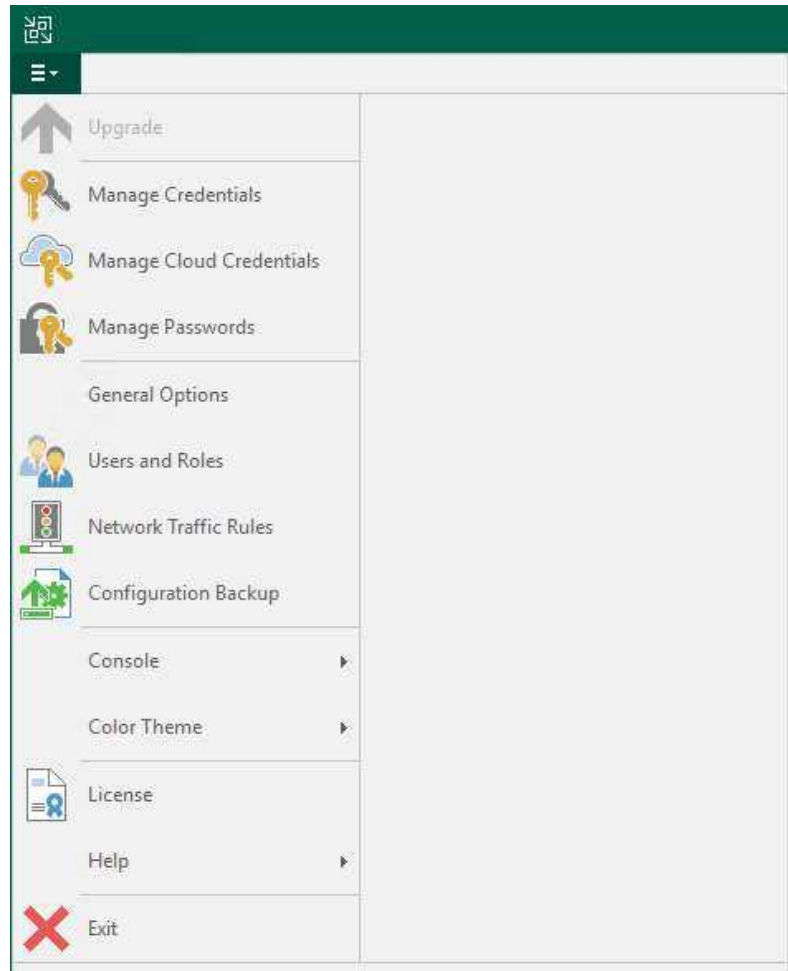
Veeam Backup and Replication v12 launched on Feb 14, 2023. If you are still using an older version, it is time to upgrade it to v12. To upgrade Veeam Backup & Replication to version 12, you must have version 10a (build 10.0.1.4854) or later installed on the supported operating system.

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.	 The screenshot shows the Veeam Backup and Replication console interface. The 'Help' menu is open, displaying options like 'Online Help', 'Support Information', and 'About'. The 'About' dialog box is visible, showing the current version (11.0.1.1261) and build (P20220302). The main console window displays a list of backup jobs with columns for Type, Objects, Status, Last Run, Last Result, Next Run, and Target. <table><tr><th>Type</th><th>Objects</th><th>Status</th><th>Last Run</th><th>Last Result</th><th>Next Run</th><th>Target</th></tr><tr><td>Hyper-V SureBackup</td><td>2</td><td>Stopped</td><td>6 days ago</td><td>Success</td><td>After (DCS_HPV02...</td><td>Advanced Single-Backup Replicator</td></tr><tr><td>Hyper-V SureBackup</td><td>2</td><td>Stopped</td><td>6 days ago</td><td>Success</td><td><Disabled></td><td>Advanced Single-Backup Replicator</td></tr><tr><td>Hyper-V Backup Copy</td><td>1</td><td>Disabled</td><td></td><td></td><td><Disabled></td><td>Scale-out Backup Replicator</td></tr><tr><td>Hyper-V Backup</td><td>1</td><td>Stopped</td><td></td><td></td><td><not scheduled></td><td>Scale-out Backup Replicator</td></tr><tr><td>Hyper-V Backup Copy</td><td>1</td><td>Disabled</td><td></td><td></td><td><Disabled></td><td>Scale-out Backup Replicator</td></tr><tr><td>Hyper-V Backup Copy</td><td>1</td><td>Disabled</td><td></td><td></td><td><Disabled></td><td>Scale-out Backup Replicator</td></tr><tr><td>Hyper-V Backup</td><td>1</td><td>Stopped</td><td>6 days ago</td><td>Success</td><td><not scheduled></td><td>Backup Replicator</td></tr><tr><td>Hyper-V Replication</td><td>1</td><td>Stopped</td><td>13 days ago</td><td>Success</td><td><not scheduled></td><td>HPHV02</td></tr><tr><td>Hyper-V Backup</td><td>1</td><td>Stopped</td><td></td><td></td><td><not scheduled></td><td>Backup Replicator</td></tr><tr><td>Hyper-V Backup</td><td>1</td><td>Stopped</td><td></td><td></td><td><not scheduled></td><td>Backup Replicator</td></tr><tr><td>Hyper-V Backup</td><td>1</td><td>Stopped</td><td></td><td></td><td><not scheduled></td><td>Backup Replicator</td></tr><tr><td>Hyper-V Backup</td><td>1</td><td>Stopped</td><td>6 days ago</td><td>Success</td><td><not scheduled></td><td>Backup Replicator</td></tr><tr><td>Hyper-V Backup</td><td>1</td><td>Stopped</td><td>6 days ago</td><td>Success</td><td><not scheduled></td><td>Backup Replicator</td></tr><tr><td>Windows Agent Policy</td><td>1</td><td>Enabled</td><td>9 days ago</td><td>N/A</td><td>N/A</td><td>Backup Replicator</td></tr><tr><td>Windows Agent Backup</td><td>1</td><td>Stopped</td><td></td><td></td><td><not scheduled></td><td>Backup Replicator</td></tr></table>	Type	Objects	Status	Last Run	Last Result	Next Run	Target	Hyper-V SureBackup	2	Stopped	6 days ago	Success	After (DCS_HPV02...	Advanced Single-Backup Replicator	Hyper-V SureBackup	2	Stopped	6 days ago	Success	<Disabled>	Advanced Single-Backup Replicator	Hyper-V Backup Copy	1	Disabled			<Disabled>	Scale-out Backup Replicator	Hyper-V Backup	1	Stopped			<not scheduled>	Scale-out Backup Replicator	Hyper-V Backup Copy	1	Disabled			<Disabled>	Scale-out Backup Replicator	Hyper-V Backup Copy	1	Disabled			<Disabled>	Scale-out Backup Replicator	Hyper-V Backup	1	Stopped	6 days ago	Success	<not scheduled>	Backup Replicator	Hyper-V Replication	1	Stopped	13 days ago	Success	<not scheduled>	HPHV02	Hyper-V Backup	1	Stopped			<not scheduled>	Backup Replicator	Hyper-V Backup	1	Stopped			<not scheduled>	Backup Replicator	Hyper-V Backup	1	Stopped			<not scheduled>	Backup Replicator	Hyper-V Backup	1	Stopped	6 days ago	Success	<not scheduled>	Backup Replicator	Hyper-V Backup	1	Stopped	6 days ago	Success	<not scheduled>	Backup Replicator	Windows Agent Policy	1	Enabled	9 days ago	N/A	N/A	Backup Replicator	Windows Agent Backup	1	Stopped			<not scheduled>	Backup Replicator
Type	Objects	Status	Last Run	Last Result	Next Run	Target																																																																																																											
Hyper-V SureBackup	2	Stopped	6 days ago	Success	After (DCS_HPV02...	Advanced Single-Backup Replicator																																																																																																											
Hyper-V SureBackup	2	Stopped	6 days ago	Success	<Disabled>	Advanced Single-Backup Replicator																																																																																																											
Hyper-V Backup Copy	1	Disabled			<Disabled>	Scale-out Backup Replicator																																																																																																											
Hyper-V Backup	1	Stopped			<not scheduled>	Scale-out Backup Replicator																																																																																																											
Hyper-V Backup Copy	1	Disabled			<Disabled>	Scale-out Backup Replicator																																																																																																											
Hyper-V Backup Copy	1	Disabled			<Disabled>	Scale-out Backup Replicator																																																																																																											
Hyper-V Backup	1	Stopped	6 days ago	Success	<not scheduled>	Backup Replicator																																																																																																											
Hyper-V Replication	1	Stopped	13 days ago	Success	<not scheduled>	HPHV02																																																																																																											
Hyper-V Backup	1	Stopped			<not scheduled>	Backup Replicator																																																																																																											
Hyper-V Backup	1	Stopped			<not scheduled>	Backup Replicator																																																																																																											
Hyper-V Backup	1	Stopped			<not scheduled>	Backup Replicator																																																																																																											
Hyper-V Backup	1	Stopped	6 days ago	Success	<not scheduled>	Backup Replicator																																																																																																											
Hyper-V Backup	1	Stopped	6 days ago	Success	<not scheduled>	Backup Replicator																																																																																																											
Windows Agent Policy	1	Enabled	9 days ago	N/A	N/A	Backup Replicator																																																																																																											
Windows Agent Backup	1	Stopped			<not scheduled>	Backup Replicator																																																																																																											

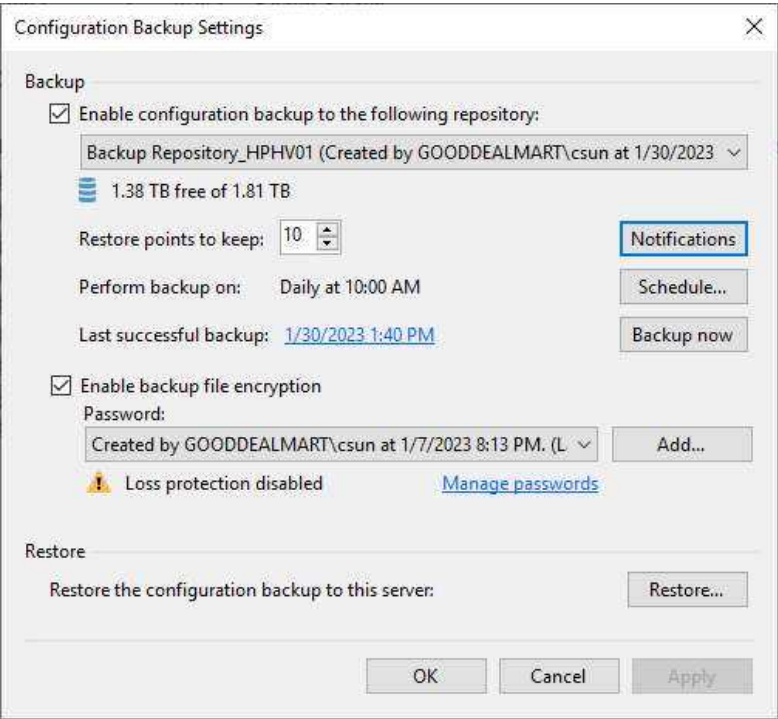
4. Make sure the existing Veeam Backup and Replication version meets the requirements.



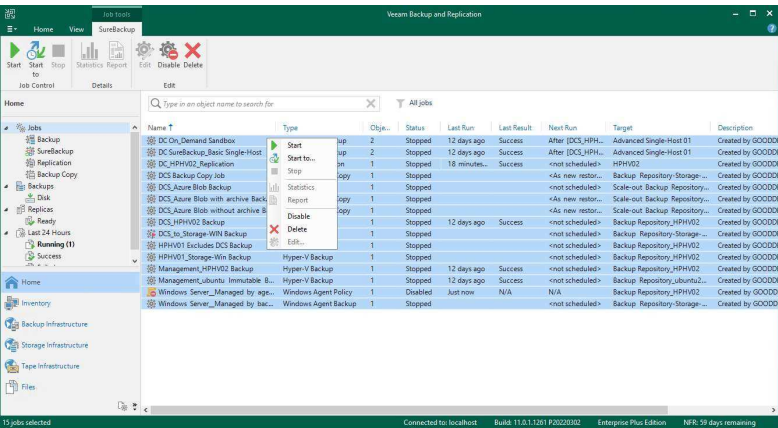
5. Drop down the main menu and select Configuration Backup.



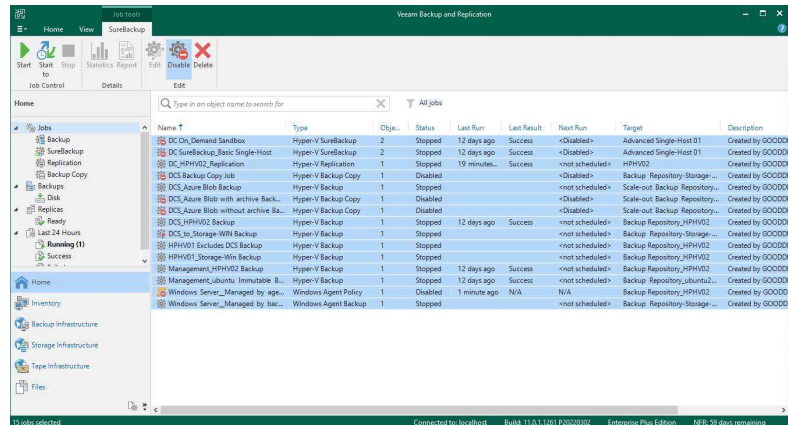
- 6. On the Configuration Backup Settings page, select Backup now to back up the current configuration.
- 7. Click OK to close the Configuration Backup Settings page after the backup is completed.



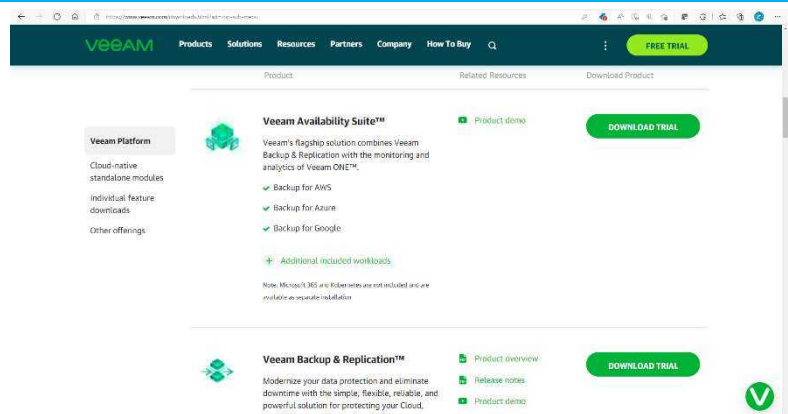
- 8. On the Home page, select Jobs.
- 9. Right-click jobs and select Disable to disable all jobs.



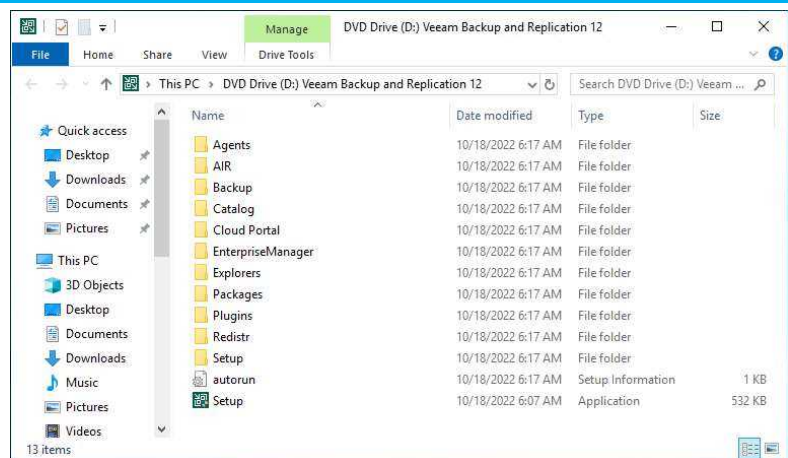
10. Make sure all jobs are disabled and close Veeam Backup & Replica on Console.



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



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



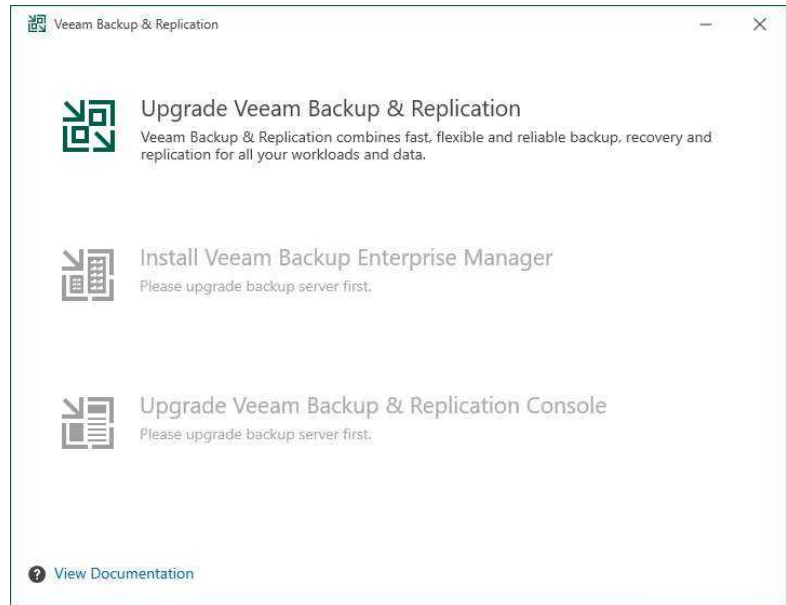
14. On the User Account Control page, click Yes.



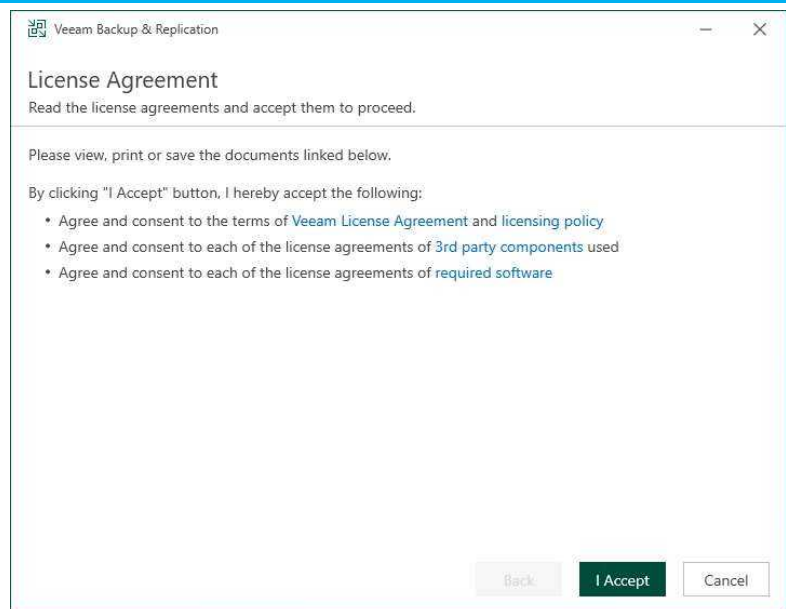
15. On the Veeam Backup & Replication 12 page, click Upgrade.



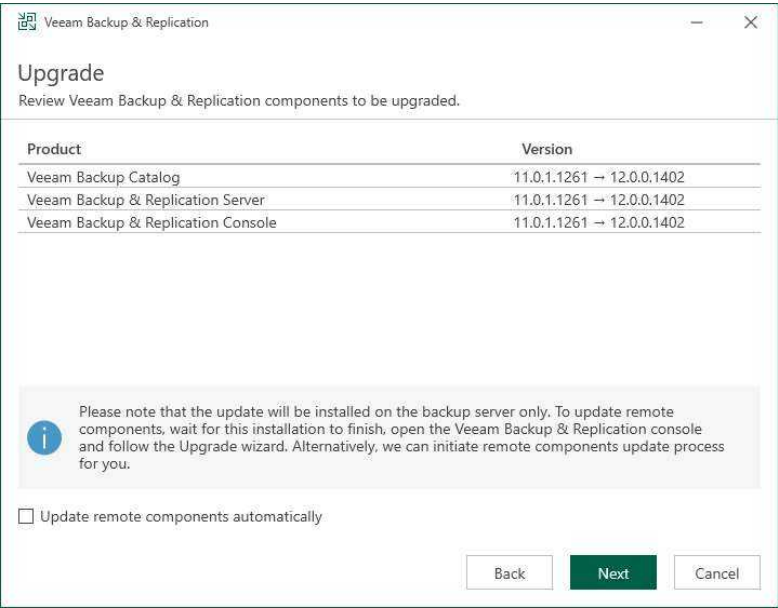
16. On the Veeam Backup & Replica on page, select Upgrade Veeam Backup & Replica on.



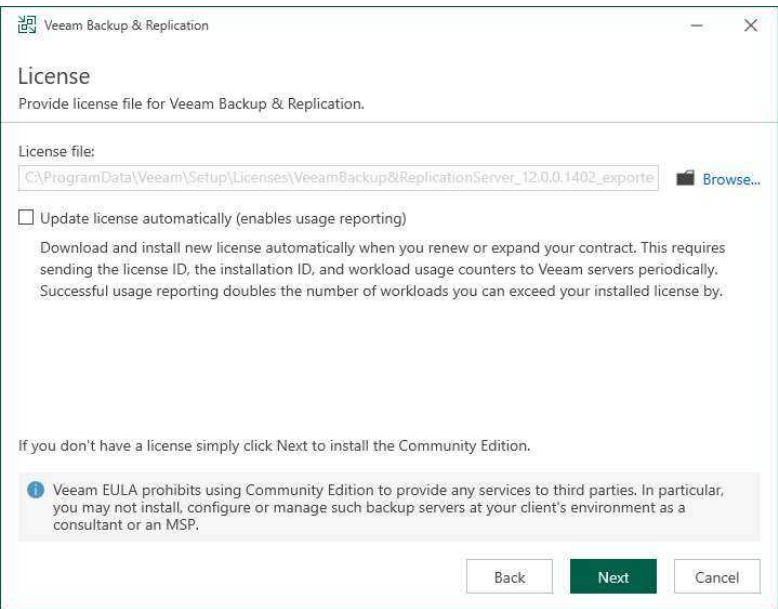
17. On the License Agreement page, click I Accept.



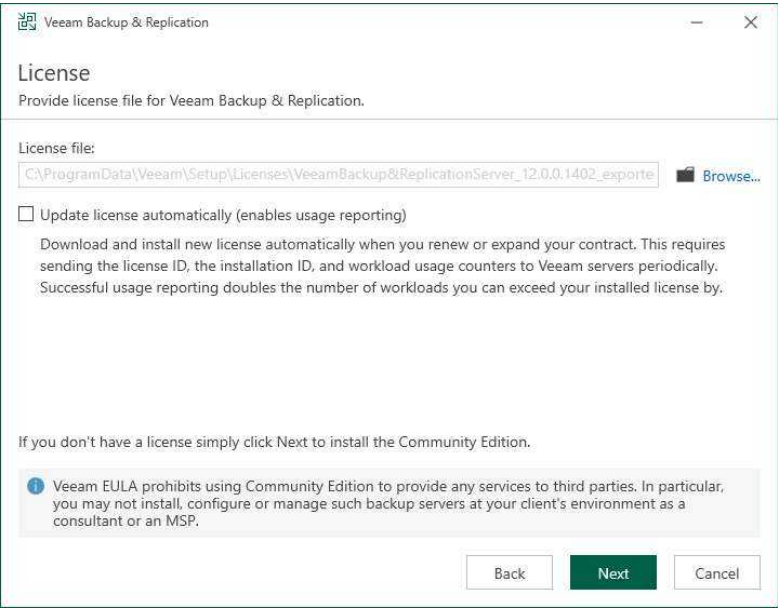
18. On the Upgrade page, click Next.



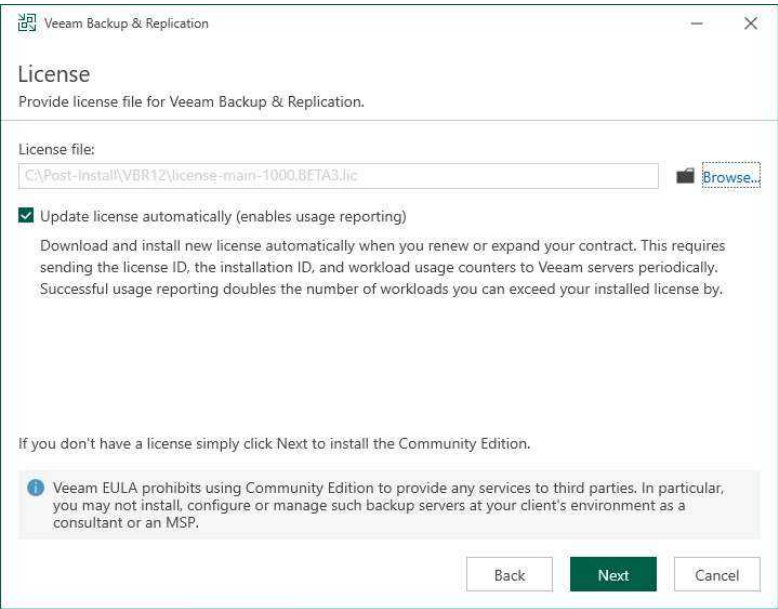
19. On the License page, click Browse.



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



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



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

Note:

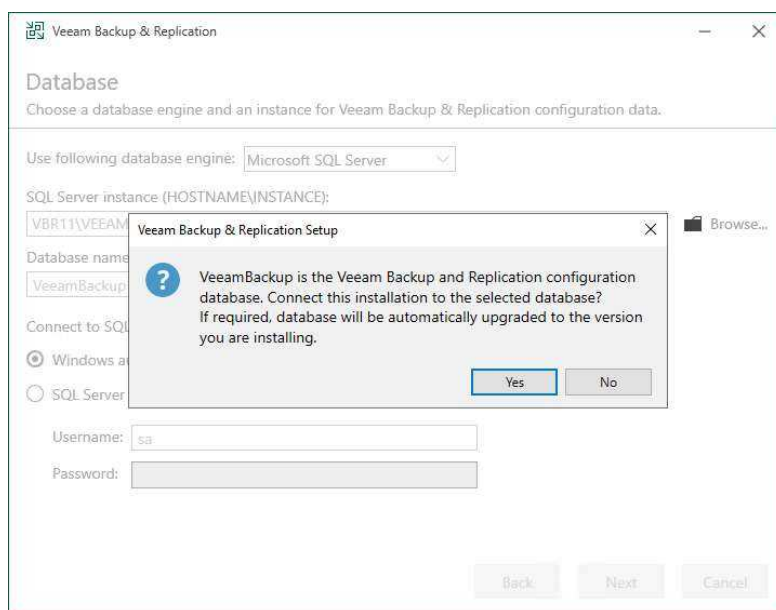
If you would like to use the specified user account, the user account must be a member of the Administrators group on the Veeam Backup & Replica on machine. Also, it must have db_owner rights for the configuration database.

The screenshot shows the 'Service Account' configuration window in Veeam Backup & Replication. The window title is 'Veeam Backup & Replication'. The subtitle is 'Service Account'. The main instruction is 'Specify account for Veeam Backup & Replication.' There are two radio button options: 'LOCAL SYSTEM account (Recommended)' which is selected, and 'The following user account:'. Below the second option, there are fields for 'User name:' (containing 'GOODDEALMART\csun') and 'Password:'. A 'Choose...' button is next to the user name field. A note below the password field states: 'Type in the user name in the DOMAIN\USERNAME format. The specified user account must have local administrator privileges on this server.' At the bottom right, there are three buttons: 'Back', 'Next' (highlighted in green), and 'Cancel'.

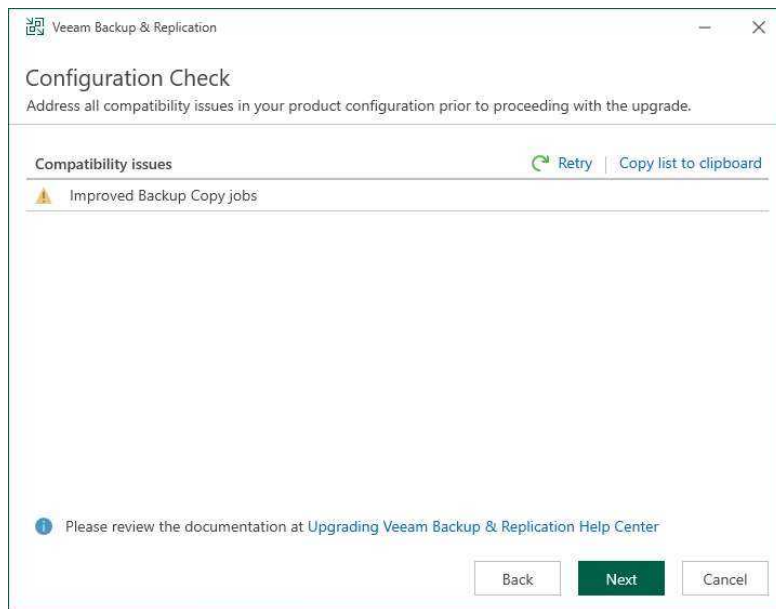
23. On the Database page, click Next.

The screenshot shows the 'Database' configuration window in Veeam Backup & Replication. The window title is 'Veeam Backup & Replication'. The subtitle is 'Database'. The main instruction is 'Choose a database engine and an instance for Veeam Backup & Replication configuration data.' There are two sections. The first section, 'Use following database engine:', has a dropdown menu set to 'Microsoft SQL Server'. Below it, 'SQL Server instance (HOSTNAME\INSTANCE):' has a dropdown menu set to 'VBR11\VEEAMSQL2016' and a 'Browse...' button. The 'Database name:' field contains 'VeeamBackup'. The second section, 'Connect to SQL Server using:', has two radio button options: 'Windows authentication credentials of the backup service account' which is selected, and 'SQL Server authentication with the following credentials:'. Below the second option, there are fields for 'Username:' (containing 'sa') and 'Password:'. At the bottom right, there are three buttons: 'Back', 'Next' (highlighted in green), and 'Cancel'.

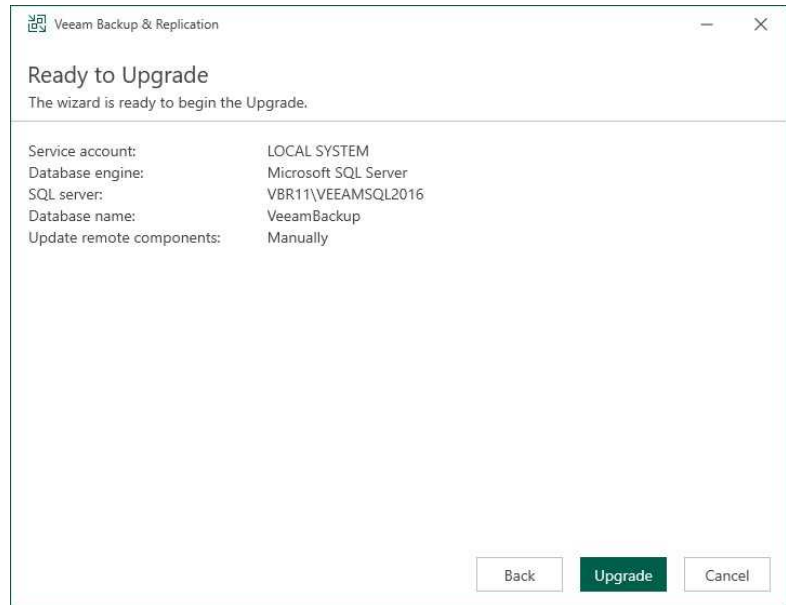
24. Click Yes on the question pop-up message. Veeam will automatically upgrade the database to the version you are installing.



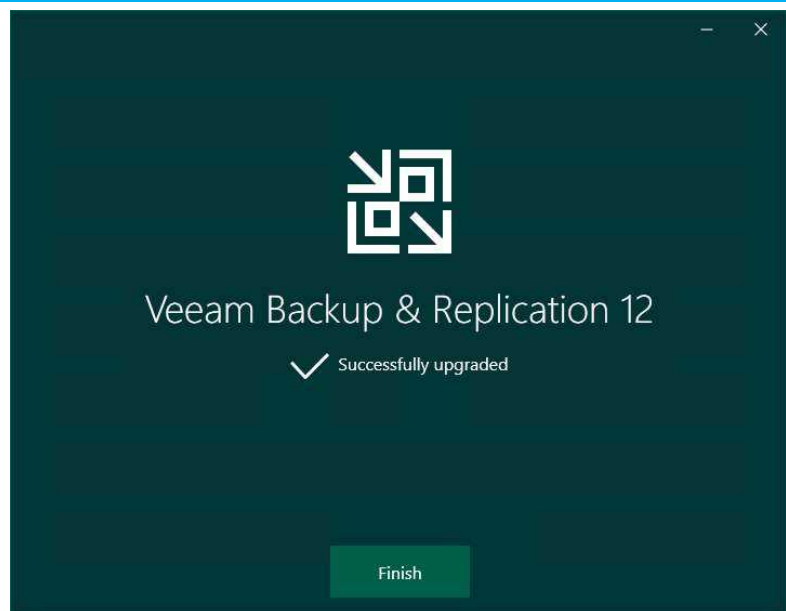
25. If the Configuration Check page returns errors, resolve them before upgrading. If the check produces warning or information messages, you can proceed with the upgrade and deal with them later.
26. Click Next.



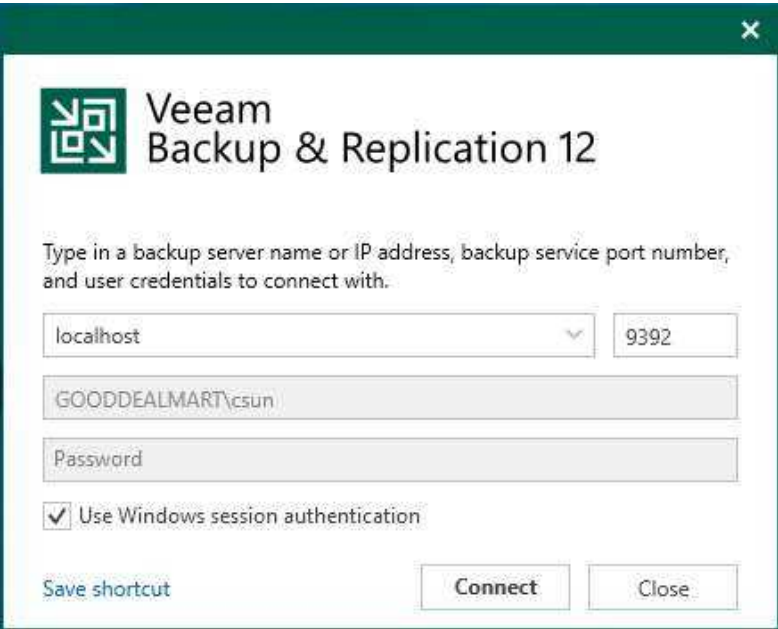
27. On the Ready to Upgrade page, click Upgrade.



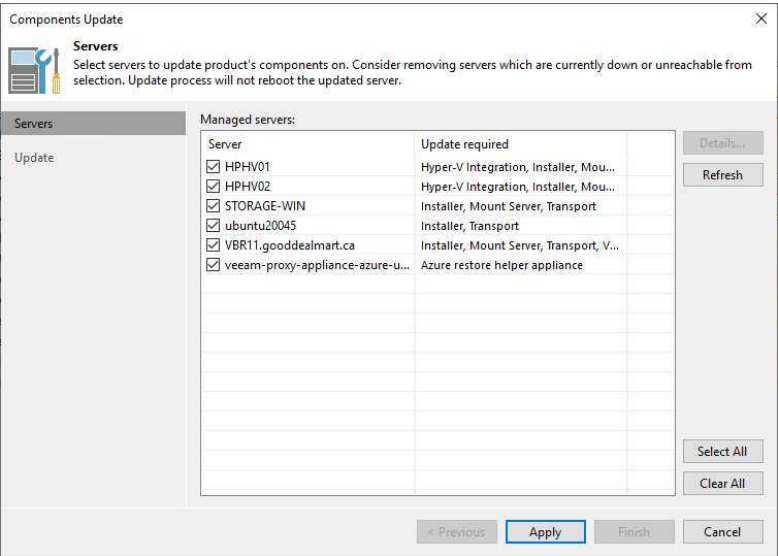
28. On the Veeam Backup & Replica on 12 successfully upgraded page, click Finish.



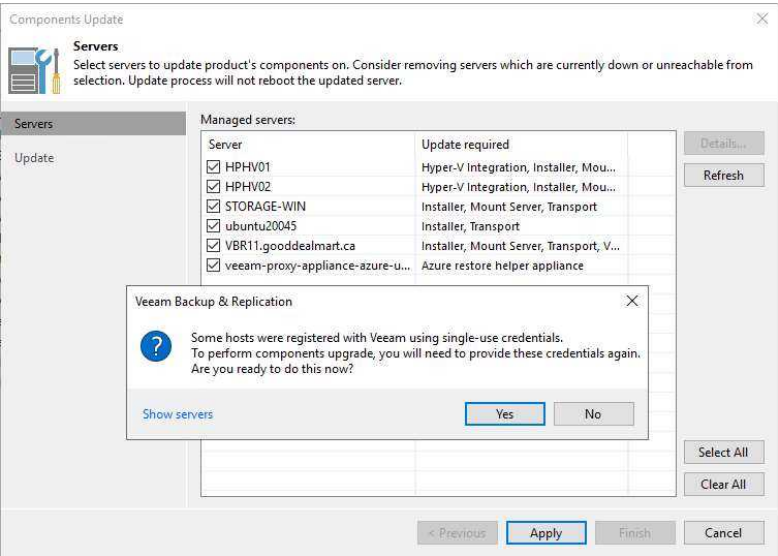
29. Open Veeam Backup & Replica on management console and click Connect.



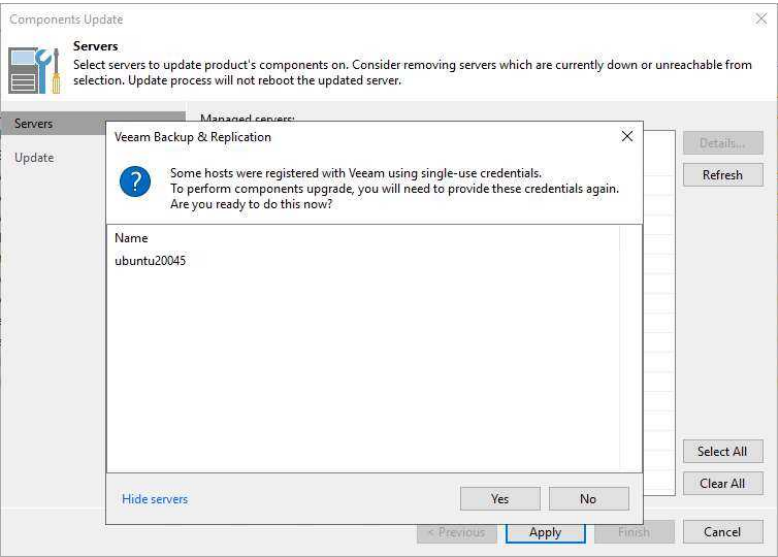
30. Select the all servers checkbox on the Components Update page and click Apply.



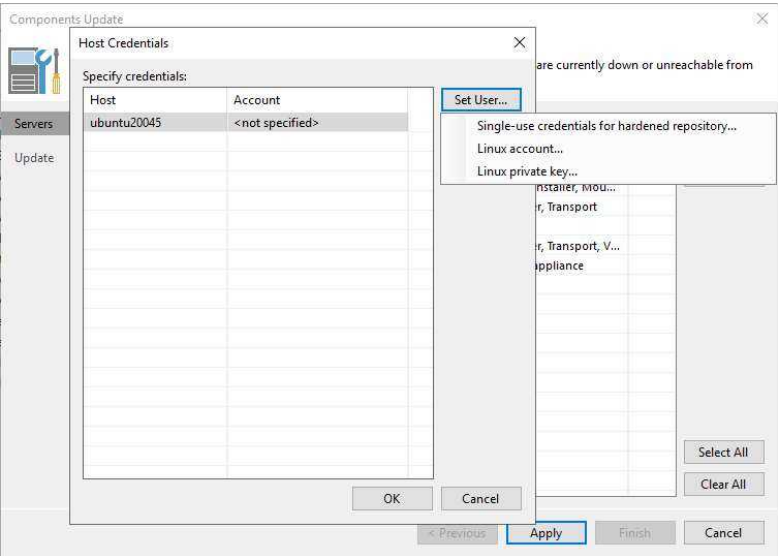
31. Click Show servers on the provide signal-use creden als ques on page.



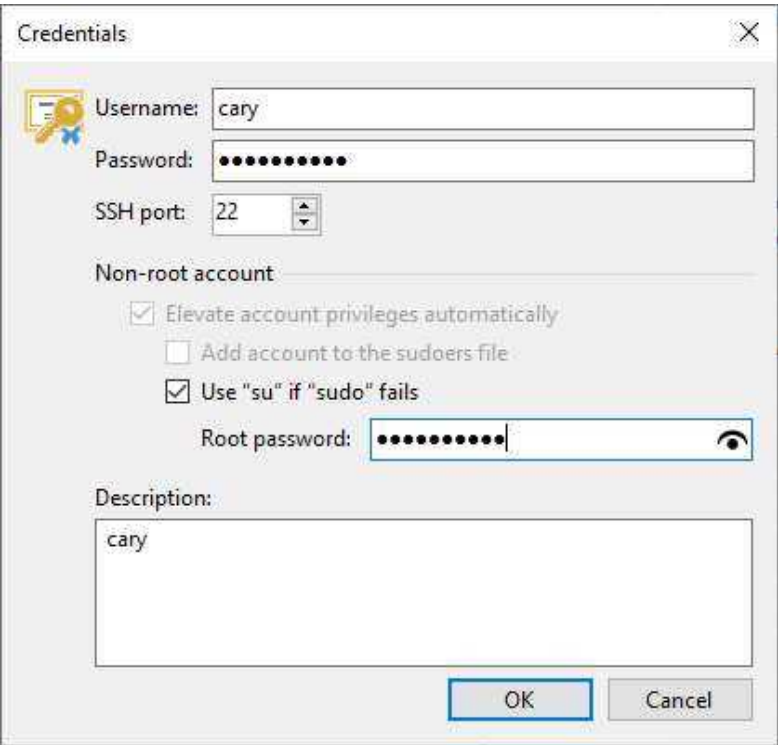
32. Review the Server list and click Yes.



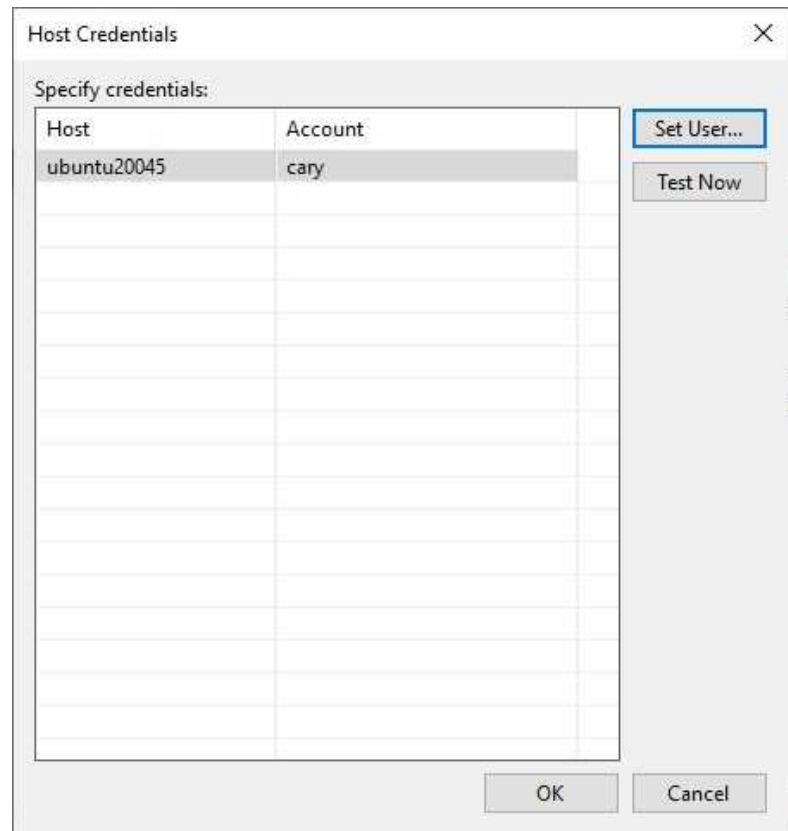
33. On the Host Credentials page, select the host, click Set User and select Single-use credentials for the hardened repository.



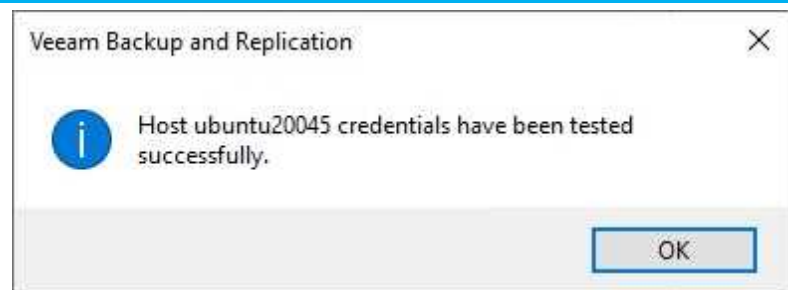
34. Enter your credential information and click OK.



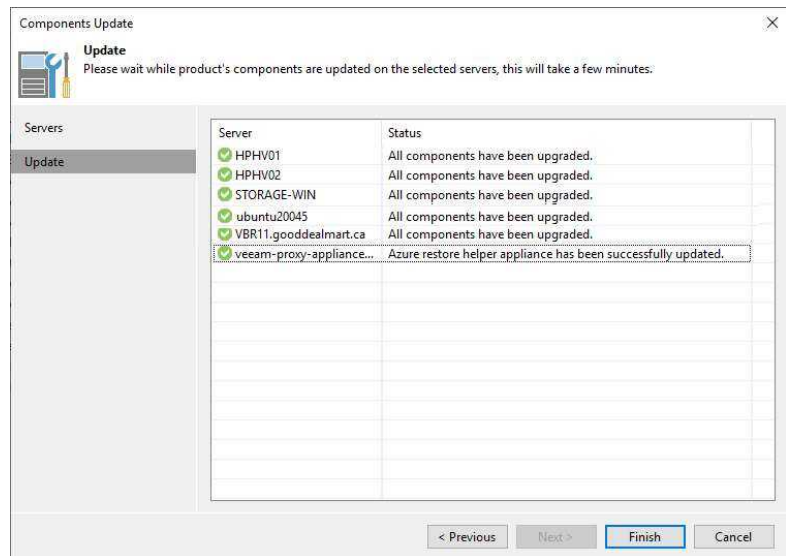
35. Click Test Now on the Host Credentials page.



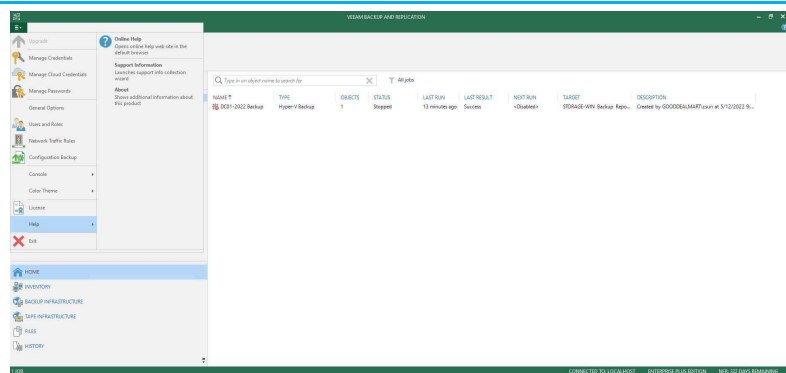
36. Ensure the credential has been tested successfully and click OK.



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



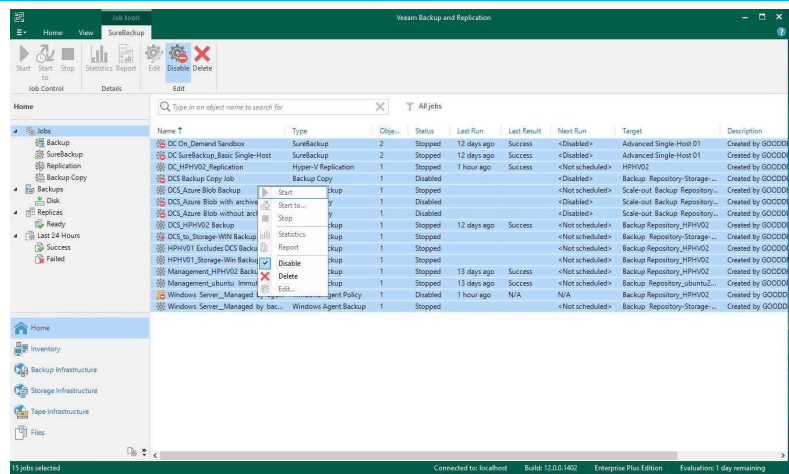
39. Drop down the main menu, select Help, and click About to check Veeam Backup & Replica on version.



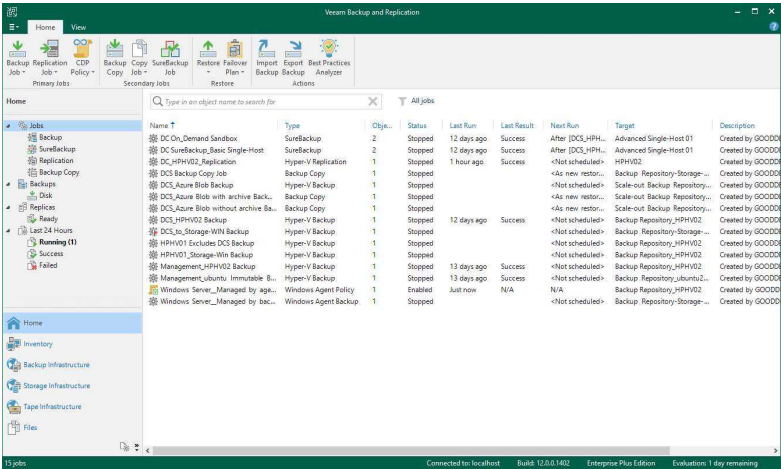
40. Ensure the existing Veeam Backup and Replication version is upgraded.



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



43. Ensure all jobs are enabled.



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.

Instruc ons

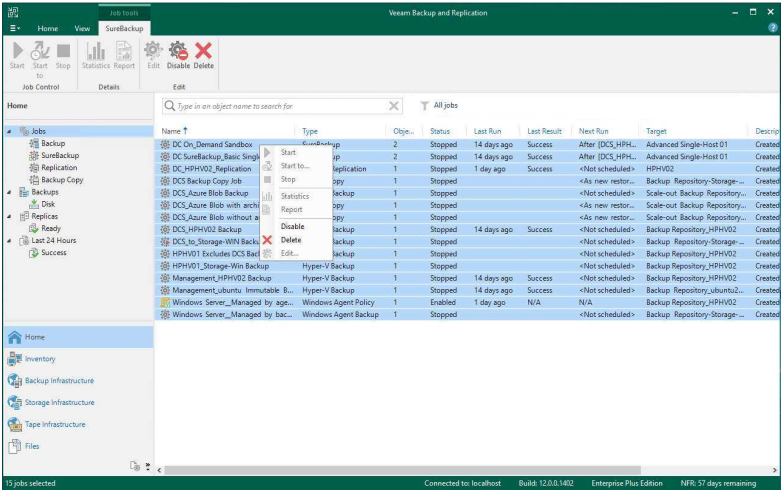
Screenshot (if applicable)

1. Log in to the existing Veeam Backup and replication manager server.

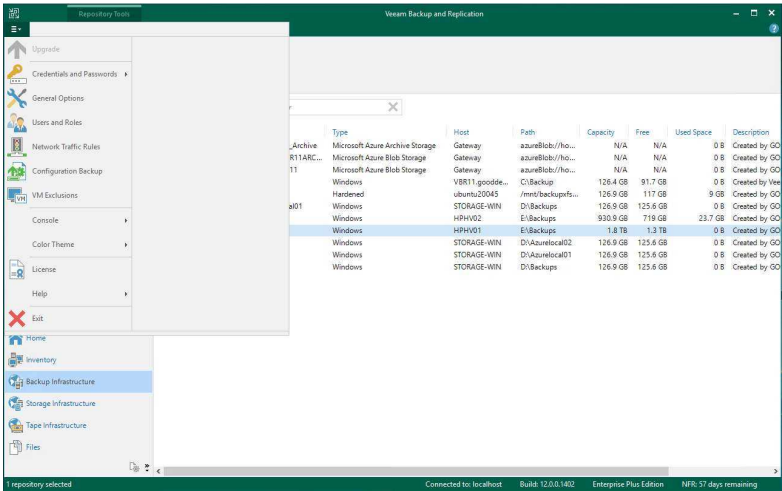
2. Open the Veeam Backup & Replication Console.

3. Select and right-click all jobs.

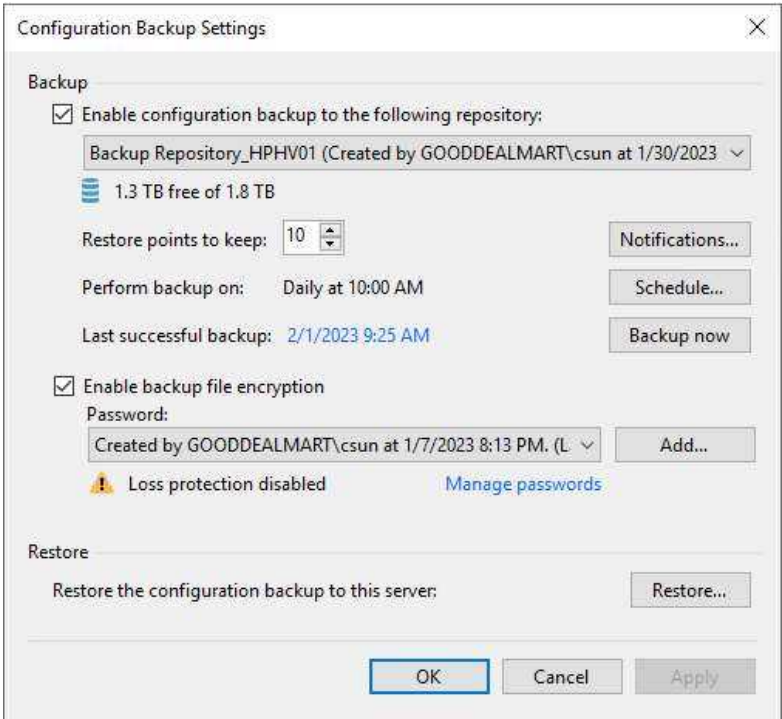
4. Select Disable.



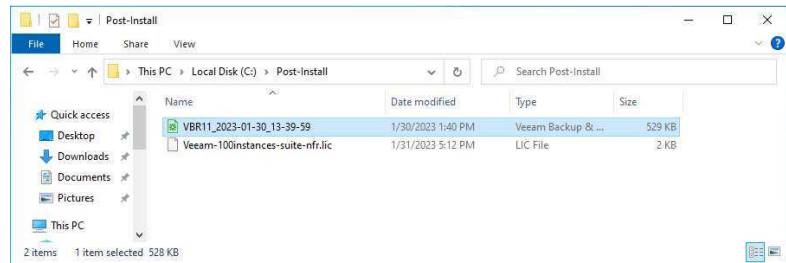
- 5. Drop down the main menu and select Configuration on Backup.



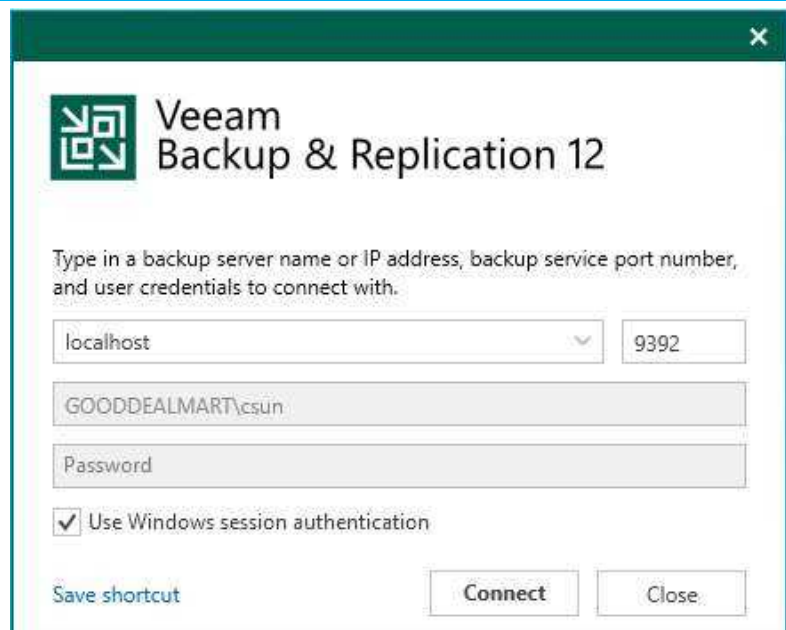
- 6. Click Backup now on the Configuration Backup Settings page.



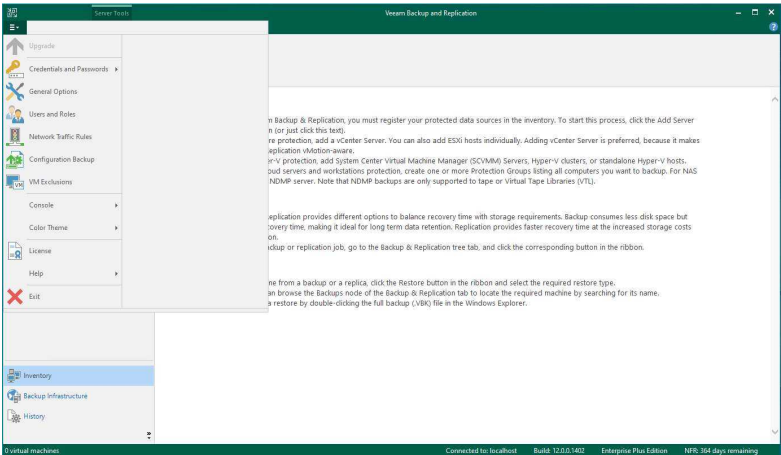
- Copy the configuration file from the backup repository to the new Backup and Replication manager server.



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



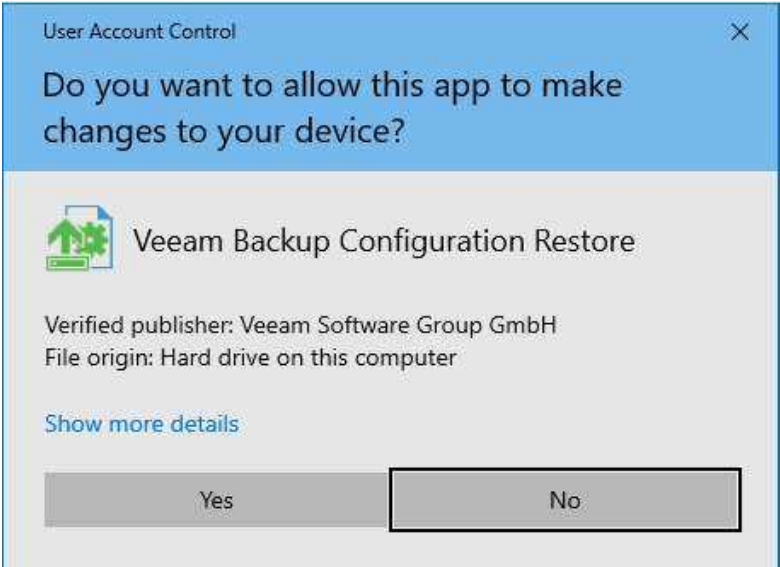
10. Drop down the main menu and select Configuration on Backup.



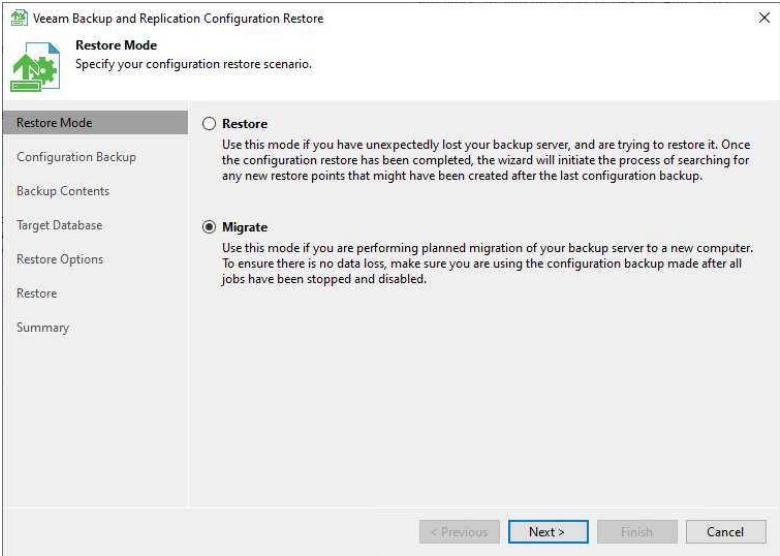
11. Click Restore on the Configuration Backup Settings page.



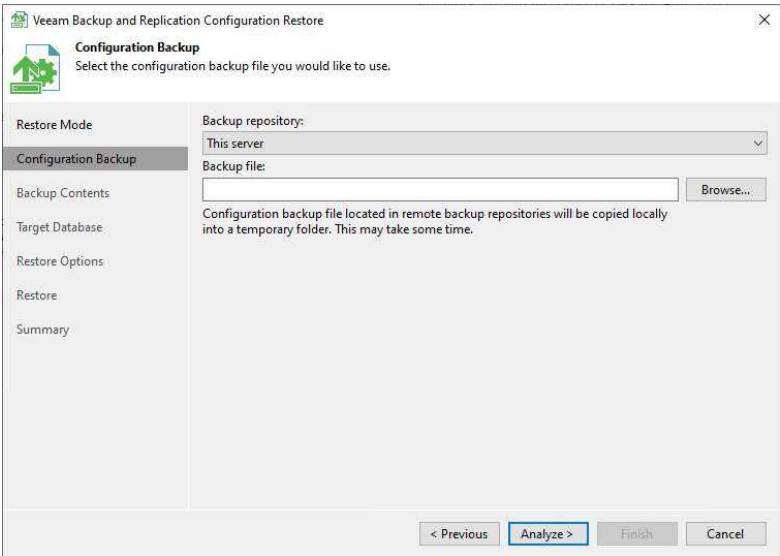
12. Click Yes on the User Account Control page.



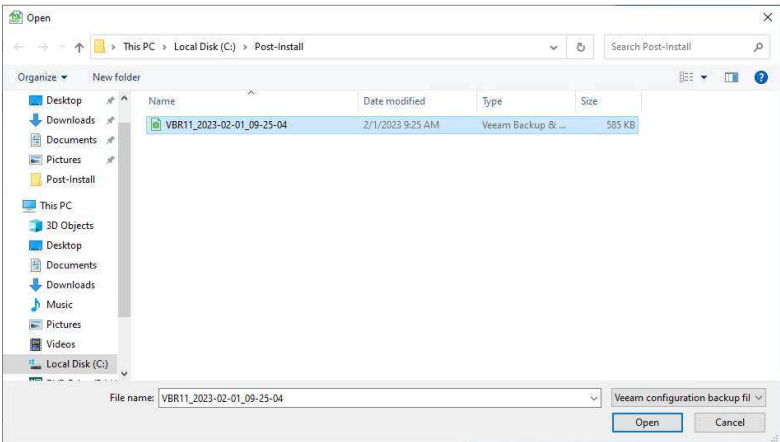
13. Select Migrate on the Restore Mode page.



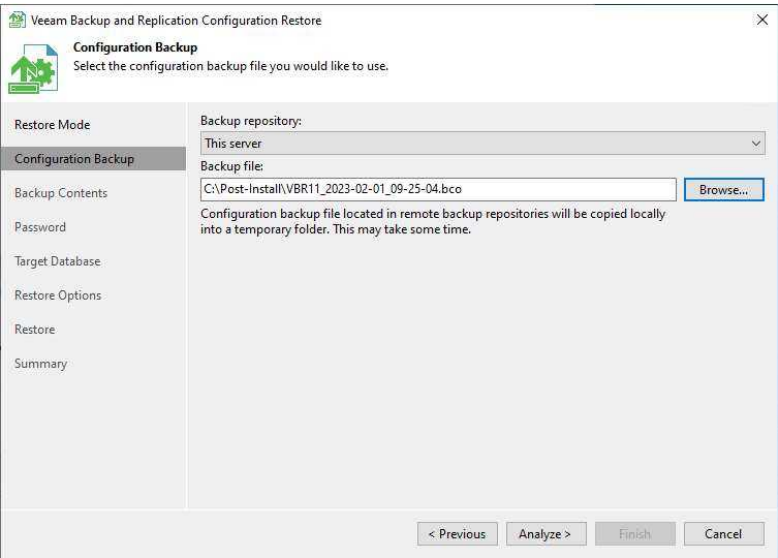
- 14. Select this server in the Backup repository field on the Configura on Backup page.
- 15. Click Browse in the Backup file field.



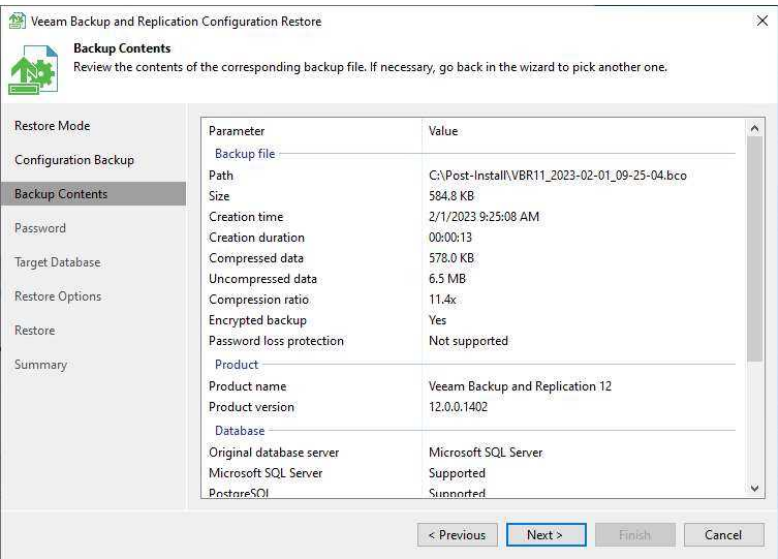
- 16. Select the backup configura on file and click Open.



17. Click Analyze on the Configuration Backup page.



18. Click Next on the Backup Contents page.



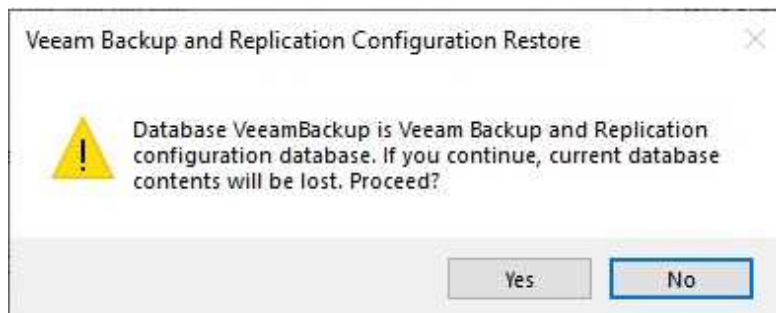
19. On the Password page, enter the password of the configuration file in the Password field.
20. Enter the description in the Hint field.
21. Click Validate.

The screenshot shows the 'Veeam Backup and Replication Configuration Restore' window, specifically the 'Password' tab. The left sidebar contains a list of tabs: 'Restore Mode', 'Configuration Backup', 'Backup Contents', 'Password' (selected), 'Target Database', 'Restore Options', 'Restore', and 'Summary'. The main area has a 'Password' field with a masked password '*****' and a 'Hint' field containing the text 'Created by GOODDEALMART\csun at 1/7/2023 8:13 PM.'. At the bottom, there is a warning icon and text: 'Your backup administrator chose not to enable password loss protection.' The bottom right corner has buttons: '< Previous', 'Validate >', 'Finish', and 'Cancel'.

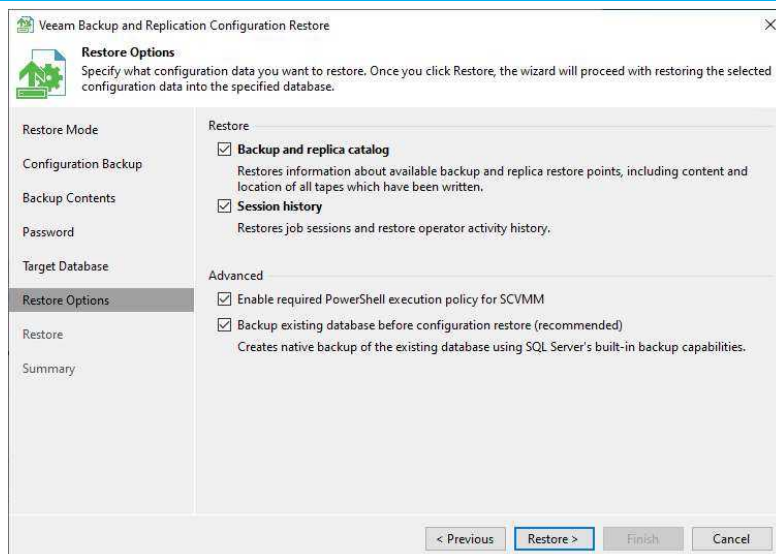
22. Select PostgreSQL from the Database drop-down list on the Target Database page.
23. Enter the instance name and Database name in the Connection session.
24. Select Windows authentication using the service account credentials in the Authentication session.

The screenshot shows the 'Veeam Backup and Replication Configuration Restore' window, specifically the 'Target Database' tab. The left sidebar contains a list of tabs: 'Restore Mode', 'Configuration Backup', 'Backup Contents', 'Password', 'Target Database' (selected), 'Restore Options', 'Restore', and 'Summary'. The main area has a 'Database engine' section with a 'Database' dropdown set to 'PostgreSQL'. Below it is a 'Connection (HOSTNAME:PORT)' section with 'Instance name' set to 'localhost:5432' and 'Database name' set to 'VeeamBackup'. The 'Authentication' section has two radio buttons: 'Windows authentication using credentials of service account' (selected) and 'Native authentication using the following credentials:'. The 'Native authentication' section has 'Login name' set to 'GOODDEALMART\csun' and an empty 'Password' field. The bottom right corner has buttons: '< Previous', 'Connect >', 'Finish', and 'Cancel'.

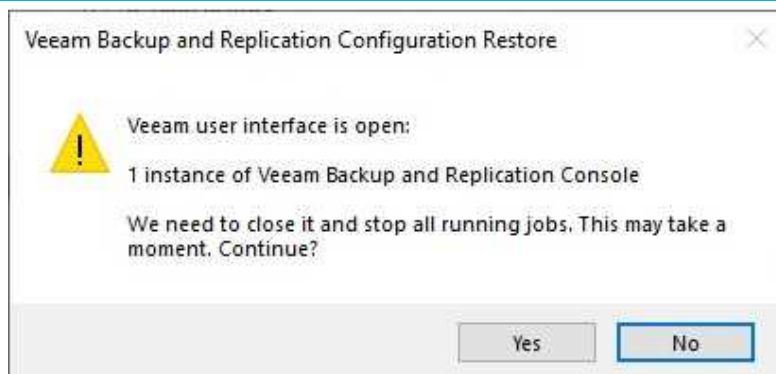
25. Click Yes on the warning message.



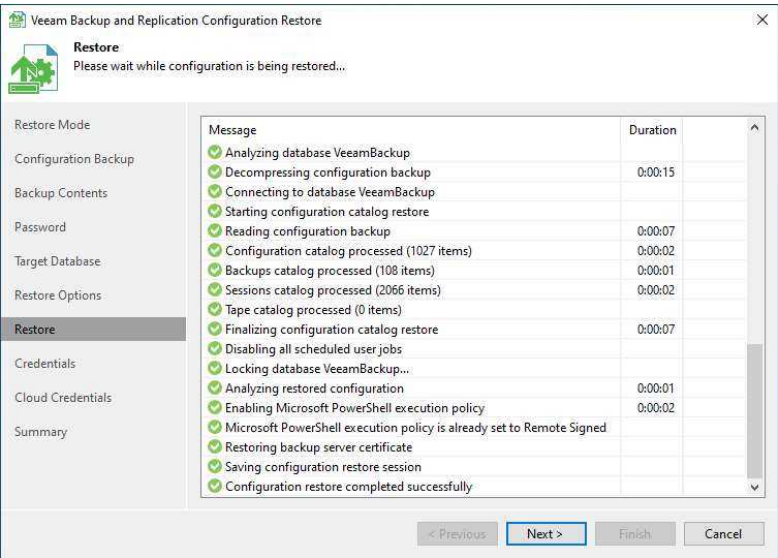
26. Select the Backup and replica catalog checkbox on the Restore Options page.
27. Select the Session history checkbox.
28. Select Enable required PowerShell execution policy for SCVMM checkbox.
29. Select Backup existing database before configuration restore (recommended).
30. Click Restore.



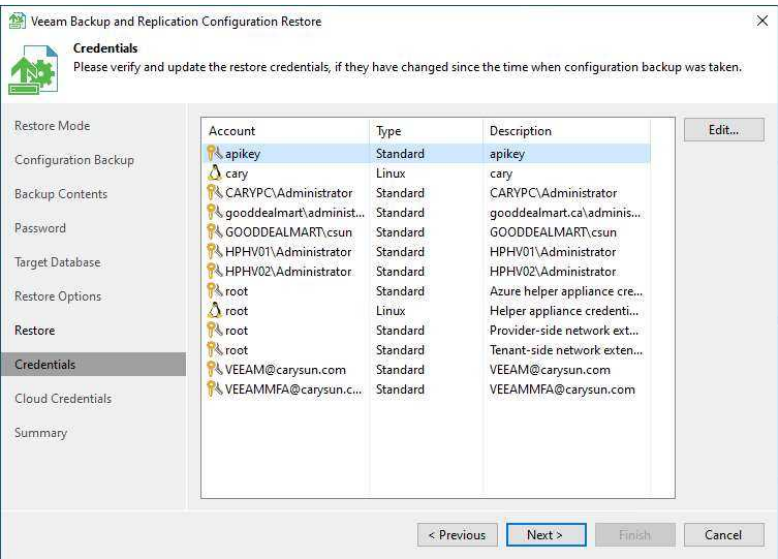
31. Click Yes on the close console and stop all running jobs warning messages.



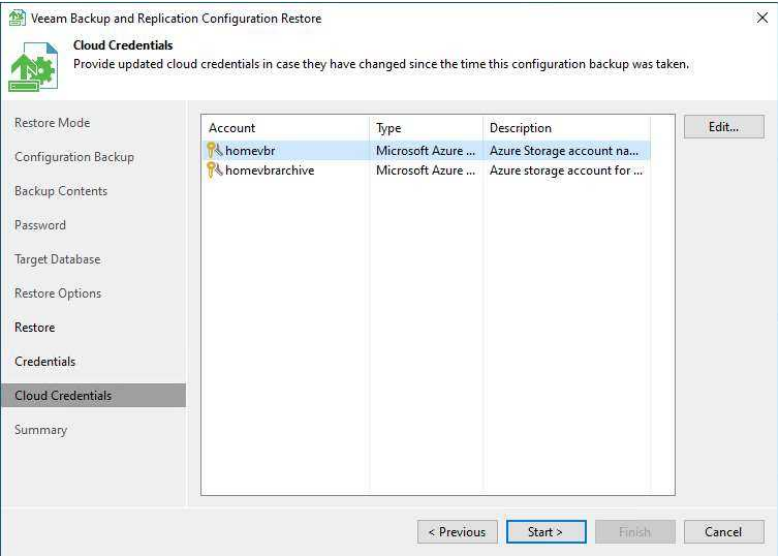
32. On the Restore page, ensure the Configuration restore is completed successfully and click Next.



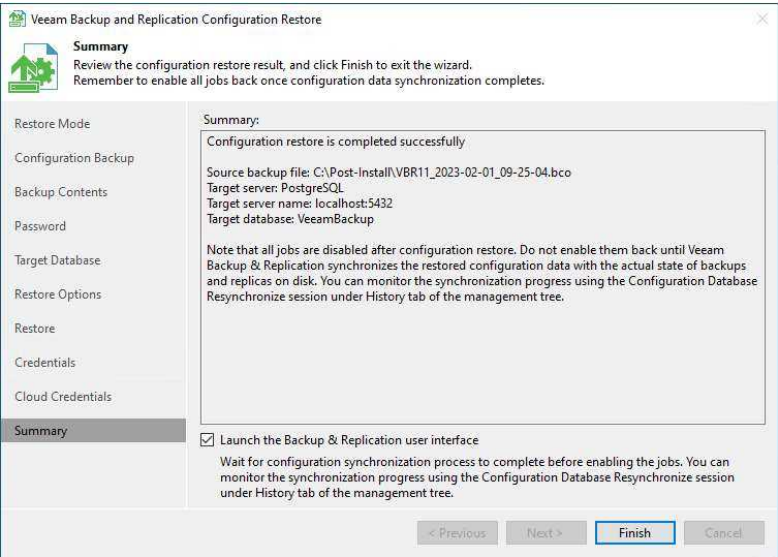
33. On the Credentials page, ensure all credentials are up-to-date and click Next.



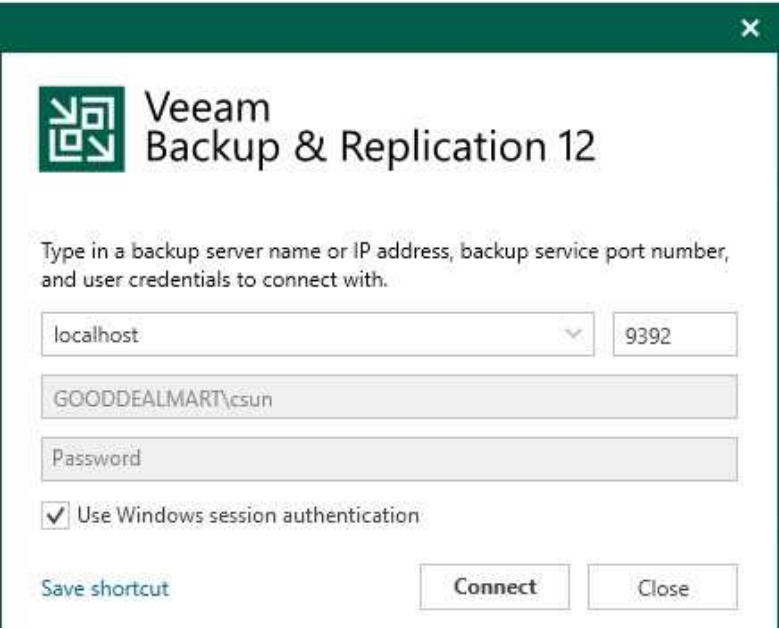
34. Ensure all credentials are up-to-date on the Cloud Credentials page and click Start.



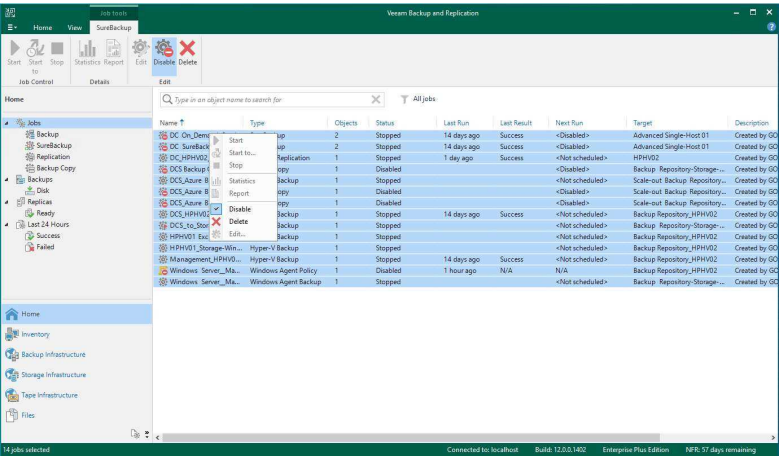
35. Click Finish on the Summary page.



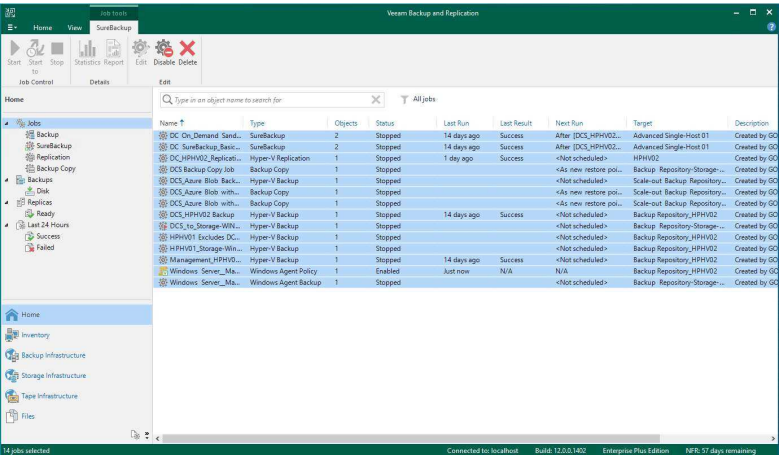
36. Open Veeam Backup & Replica on console and click Connect.



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



38. Ensure all jobs are re-enabled.



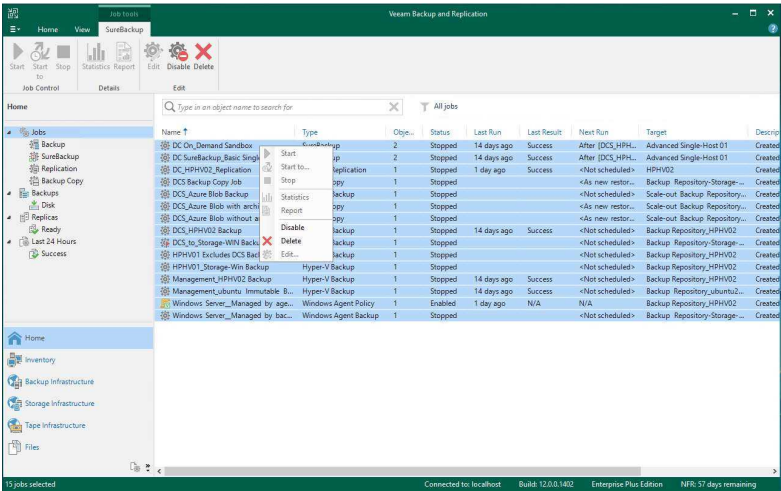
Migrate the Existing Veeam Backup and Replication to the new server with Microsoft SQL

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

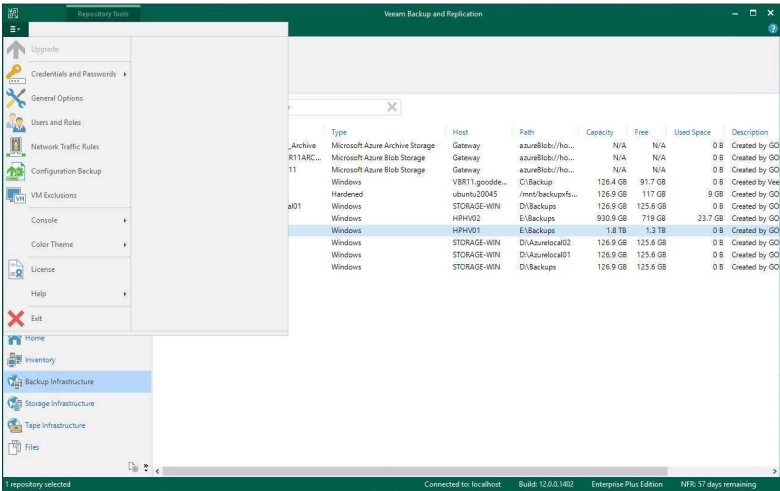
Instructions

Screenshot (if applicable)

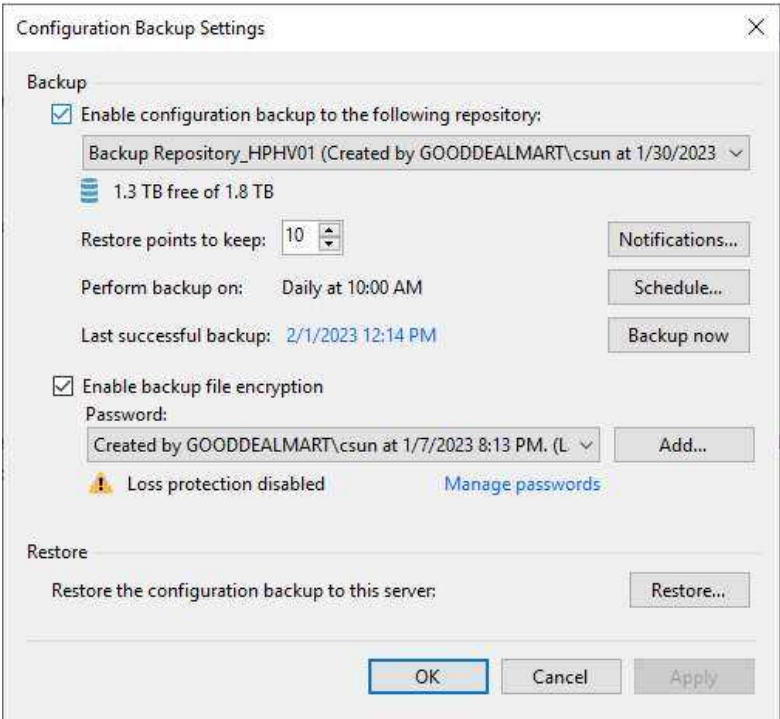
1. Log in to the existing Veeam Backup and Replication manager server.
2. Open the Veeam Backup & Replication Console.
3. Select and right-click all jobs.
4. Select Disable.



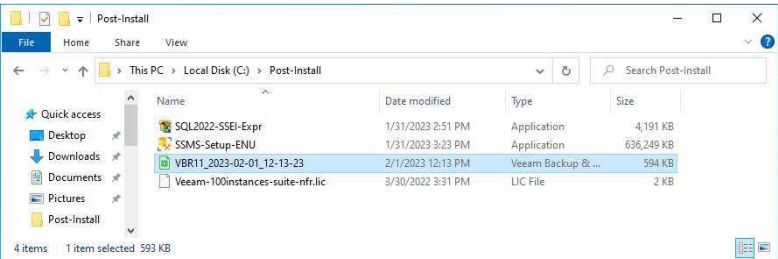
5. Drop down the main menu and select Configuration on Backup.



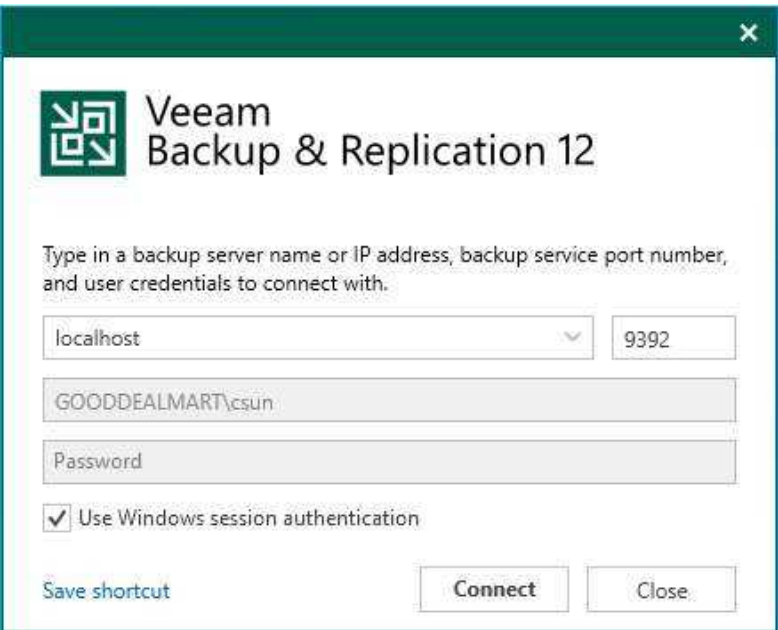
6. Click Backup now on the Configuration Backup Settings page.



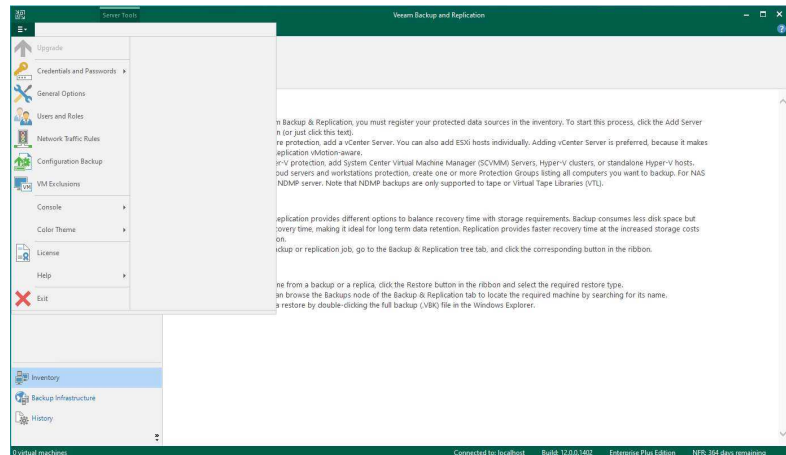
- 7. Copy the configuration file from the backup repository to the new Backup and Replication manager server.



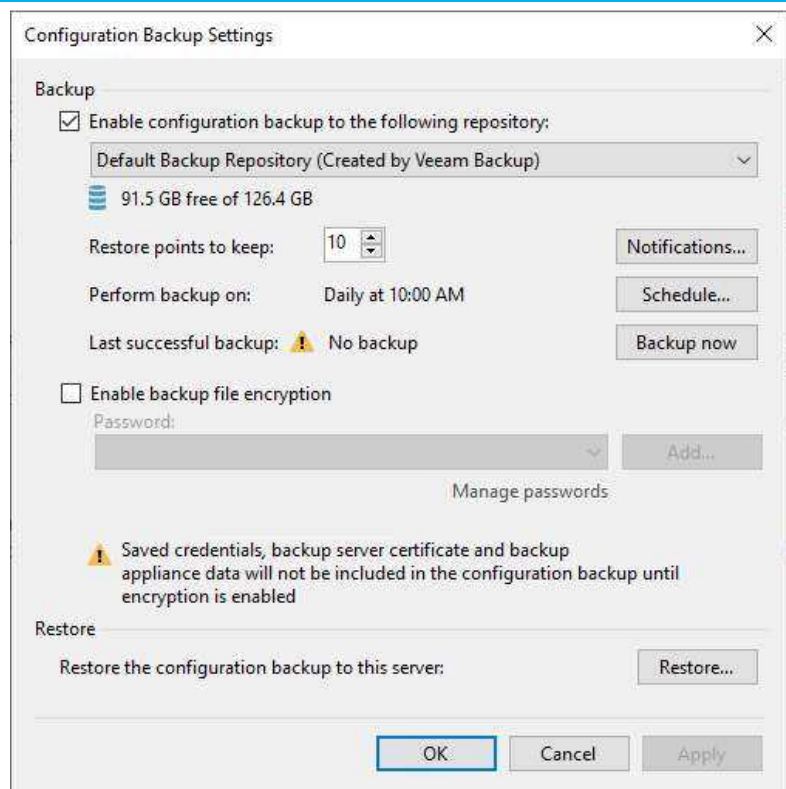
- 8. Log in to the new Veeam Backup and Replication manager server.
- 9. Open the Veeam Backup & Replication Console, and click Connect.



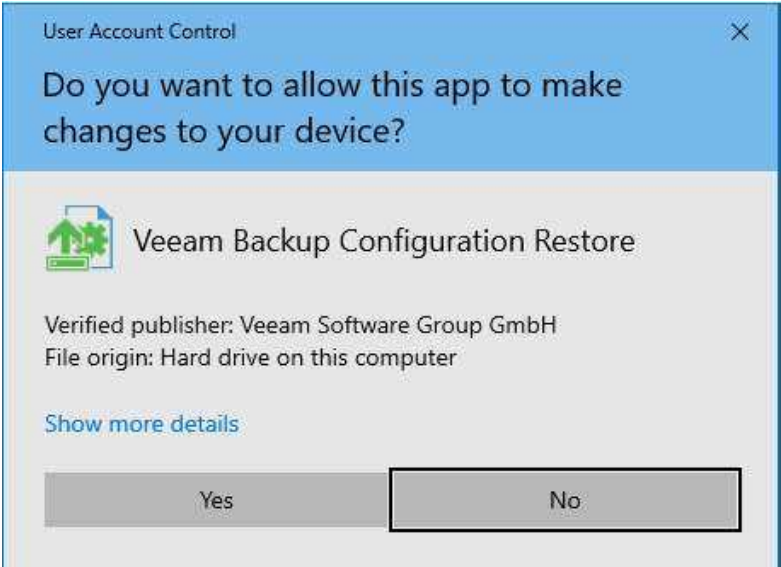
- Drop down the main menu and select Configuration on Backup.



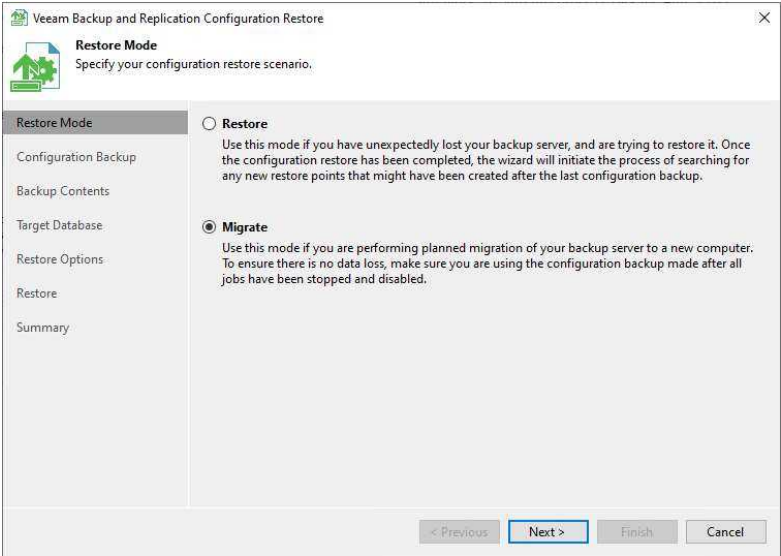
- Click Restore on the Configuration Backup Settings page.



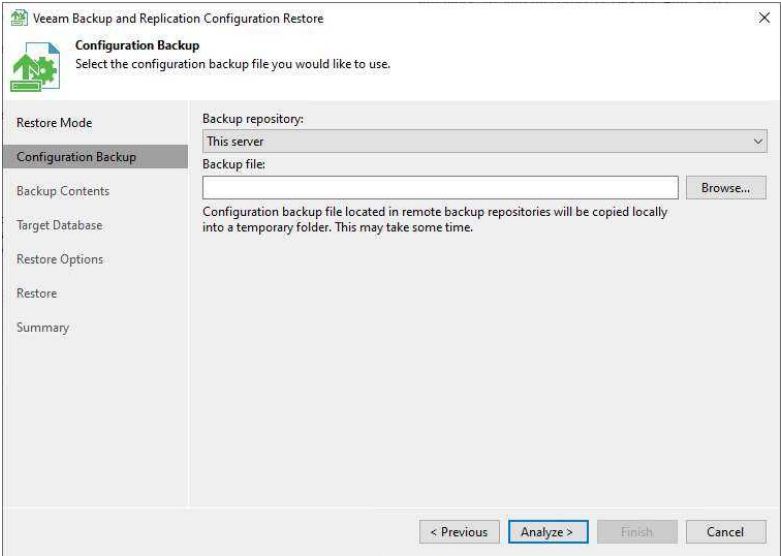
12. Click Yes on the User Account Control page.



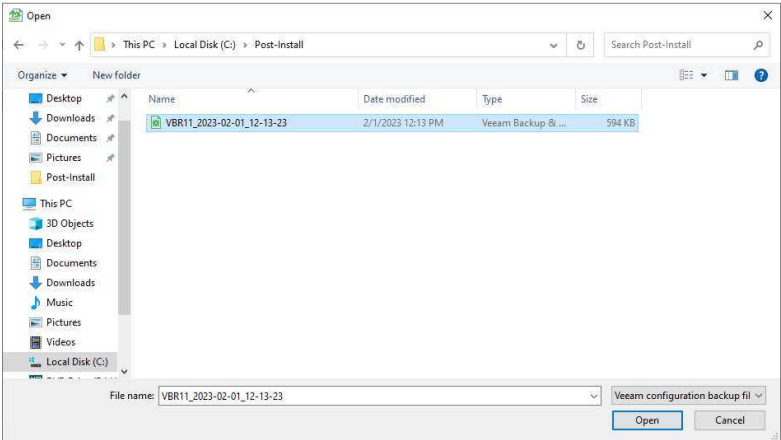
13. Select Migrate on the Restore Mode page.



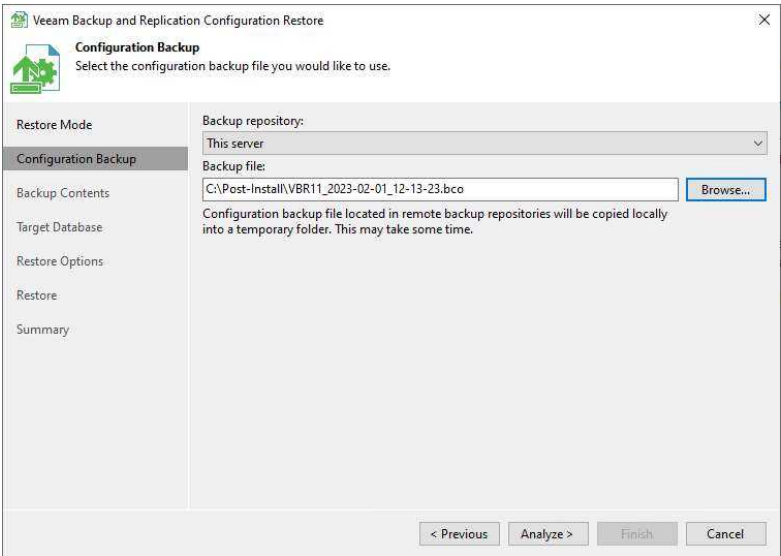
- 14. Select this server in the Backup repository field on the Configuration Backup page.
- 15. Click Browse in the Backup file field.



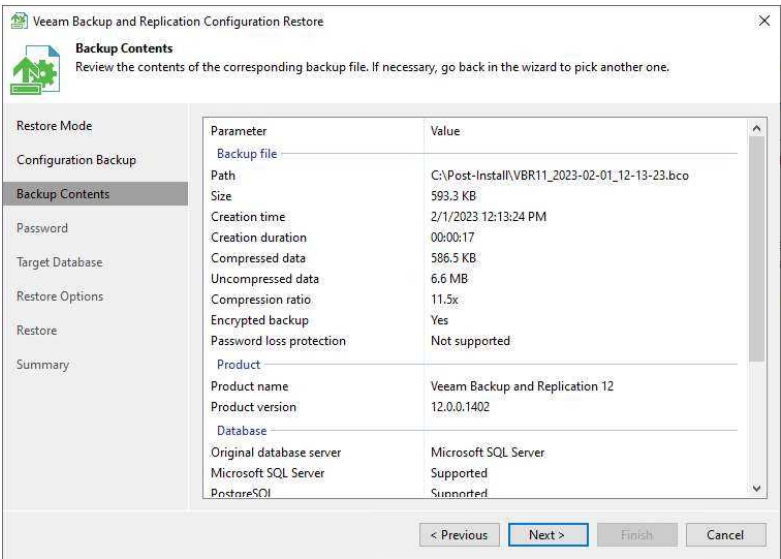
- 16. Select the backup configura on file and click Open.



17. Click Analyze on the Configuration Backup page.



18. Click Next on the Backup Contents page.



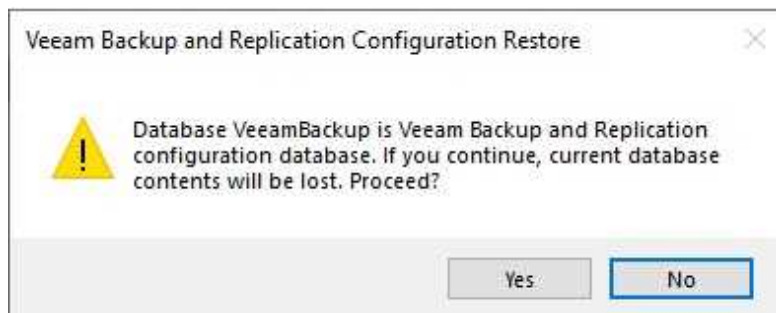
19. On the Password page, enter the password of the configuration file in the Password field.
20. Enter the description in the Hint field.
21. Click Validate.

The screenshot shows the 'Veeam Backup and Replication Configuration Restore' dialog box, specifically the 'Password' page. The left sidebar contains a list of steps: 'Restore Mode', 'Configuration Backup', 'Backup Contents', 'Password' (which is highlighted), 'Target Database', 'Restore Options', 'Restore', and 'Summary'. The main area is titled 'Specify configuration backup's password.' and contains a 'Password' field with masked characters (dots), a 'Hint' field with the text 'Created by GOODDEALMART\csun at 1/7/2023 8:13 PM.', and a warning icon with the message 'Your backup administrator chose not to enable password loss protection.' At the bottom, there are four buttons: '< Previous', 'Validate >' (highlighted with a blue border), 'Finish', and 'Cancel'.

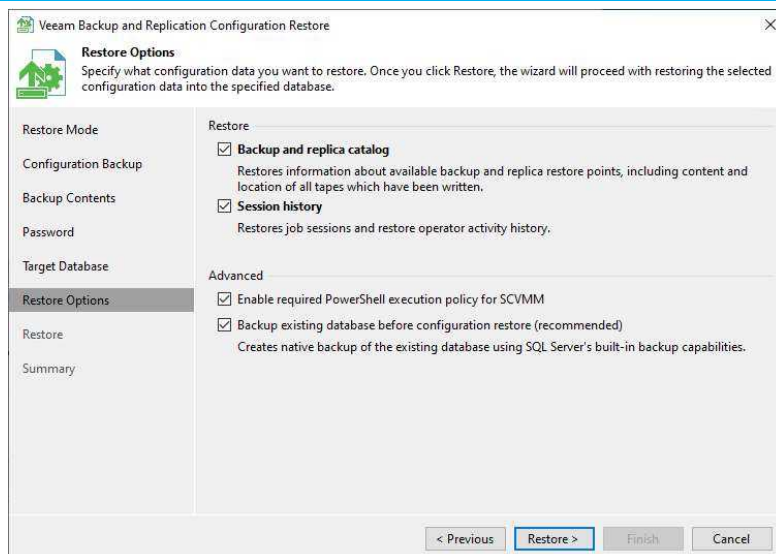
22. Select Microsoft SQL Server from the Database drop-down list on the Target Database page.
23. Enter the instance name and Database name in the Connection session.
24. Select Windows authentication using the service account credentials in the Authentication session.

The screenshot shows the 'Veeam Backup and Replication Configuration Restore' dialog box, specifically the 'Target Database' page. The left sidebar contains a list of steps: 'Restore Mode', 'Configuration Backup', 'Backup Contents', 'Password', 'Target Database' (which is highlighted), 'Restore Options', 'Restore', and 'Summary'. The main area is titled 'Specify the Veeam Backup & Replication database to restore configuration to.' and contains several fields: 'Database engine' (set to 'Microsoft SQL Server'), 'Database' (set to 'Microsoft SQL Server'), 'Connection (HOSTNAME\INSTANCE)' (set to 'VBR12\SQLEXPRESS'), 'Instance name' (set to 'VBR12\SQLEXPRESS'), 'Database name' (set to 'VeeamBackup'), and 'Authentication' (set to 'Windows authentication using credentials of service account'). At the bottom, there are four buttons: '< Previous', 'Connect >' (highlighted with a blue border), 'Finish', and 'Cancel'.

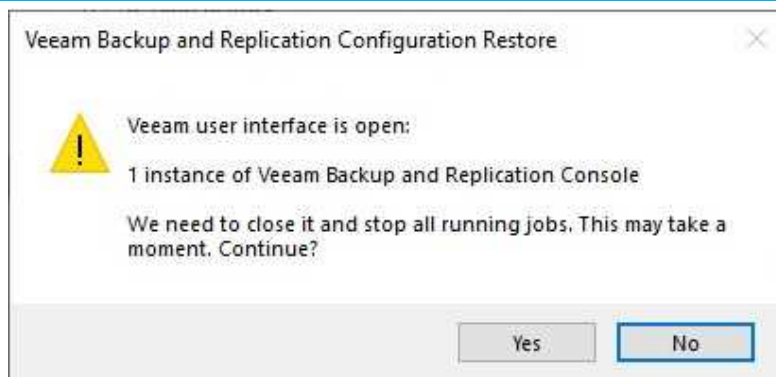
25. Click Yes on the warning message.



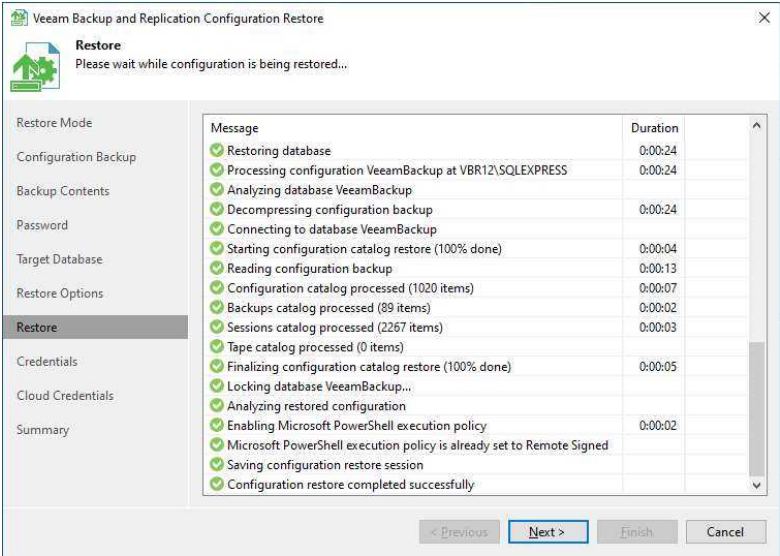
26. Select the Backup and replica catalog checkbox on the Restore Options page.
27. Select the Session history checkbox.
28. Select Enable required PowerShell execution policy for SCVMM checkbox.
29. Select Backup existing database before configuration restore (recommended).
30. Click Restore.



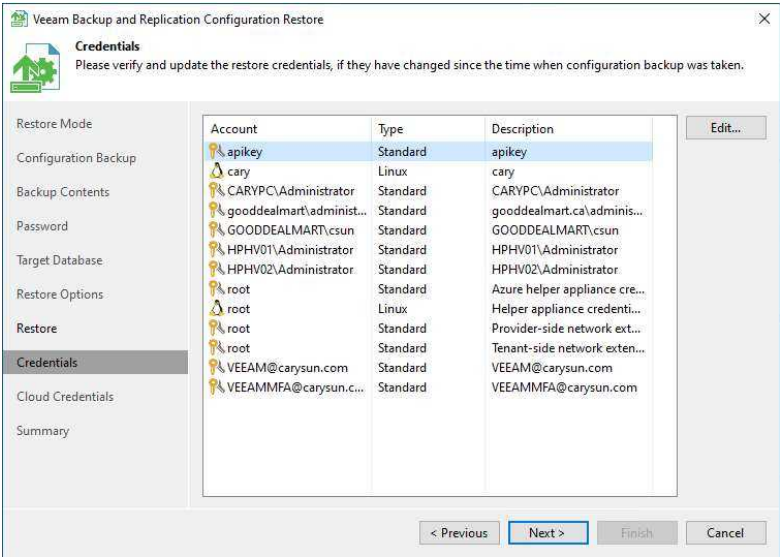
31. Click Yes on the warning message.



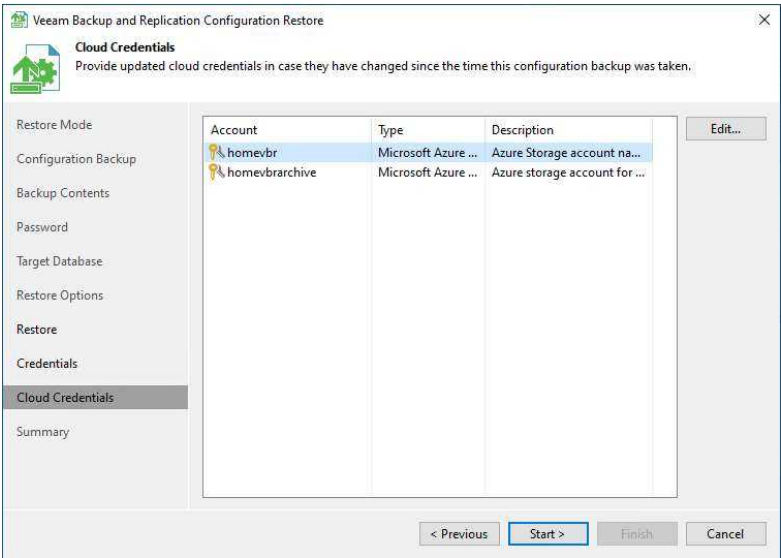
32. On the Restore page, ensure the Configuration restore is completed successfully and click Next.



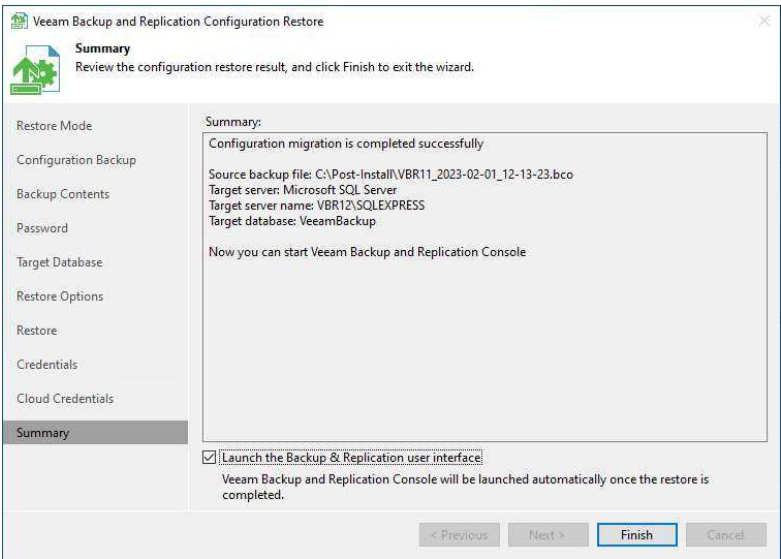
33. On the Credentials page, ensure all credentials are up-to-date and click Next.



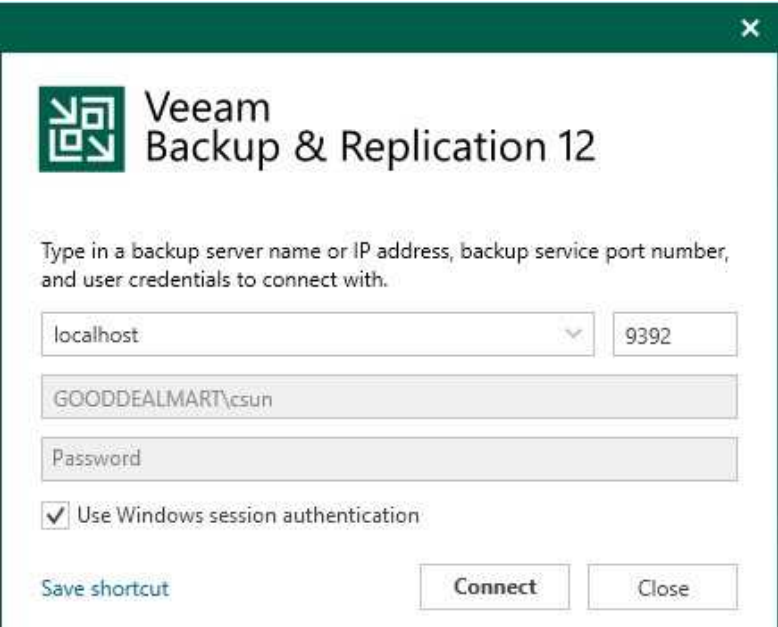
34. Ensure all credentials are up-to-date on the Cloud Credentials page and click Start.



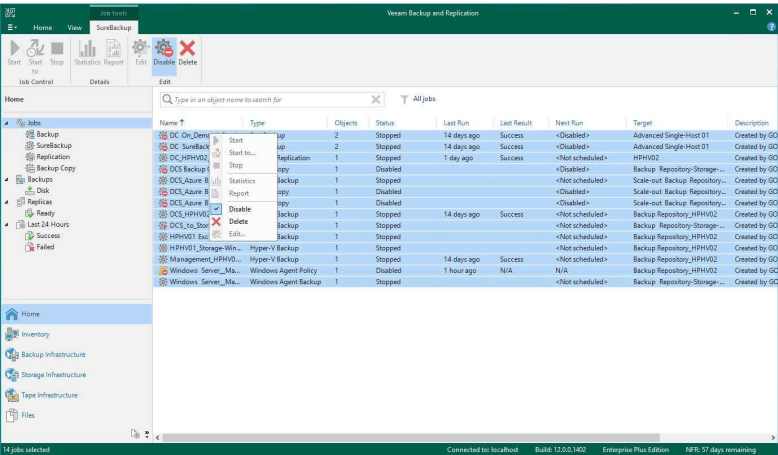
35. Click Finish on the Summary page.



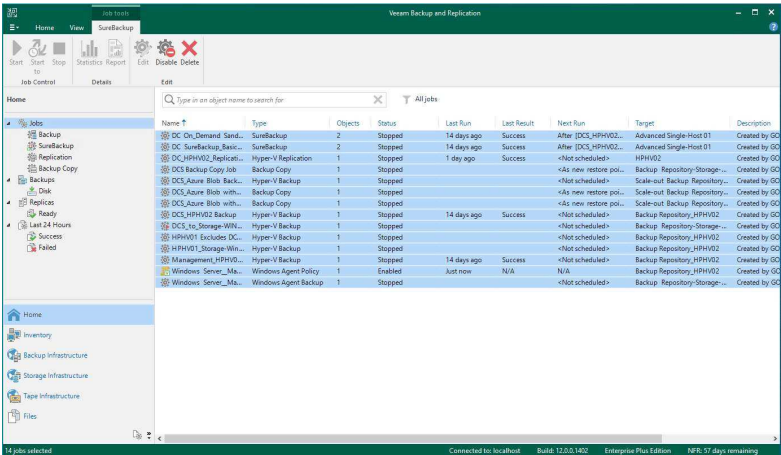
36. Open Veeam Backup & Replica on console and click Connect.



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



38. Ensure all jobs are re-enabled.



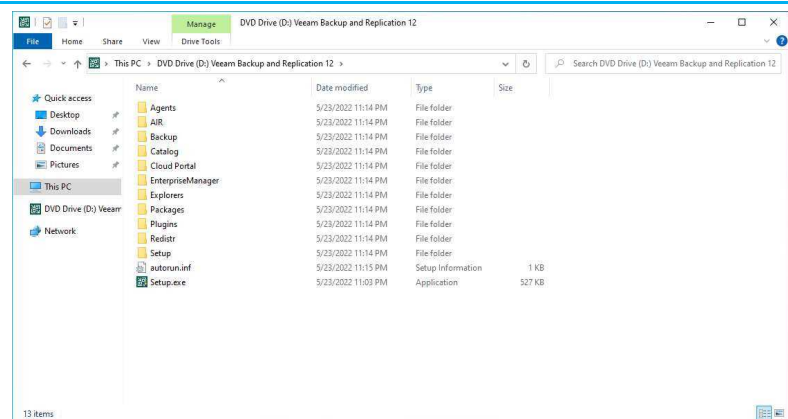
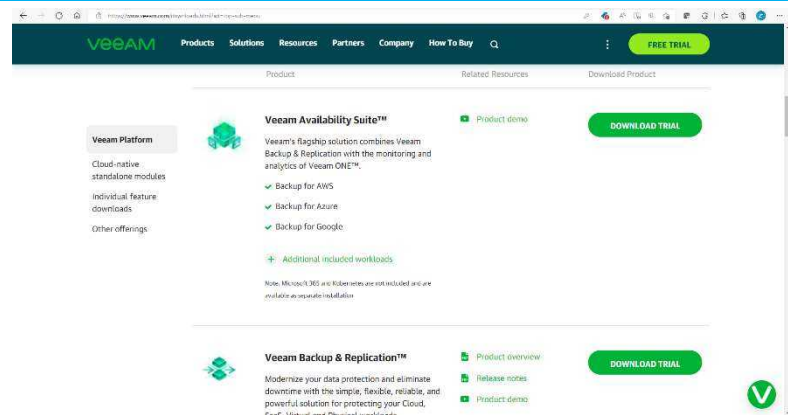
Install Veeam Backup and Replication Console 12

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

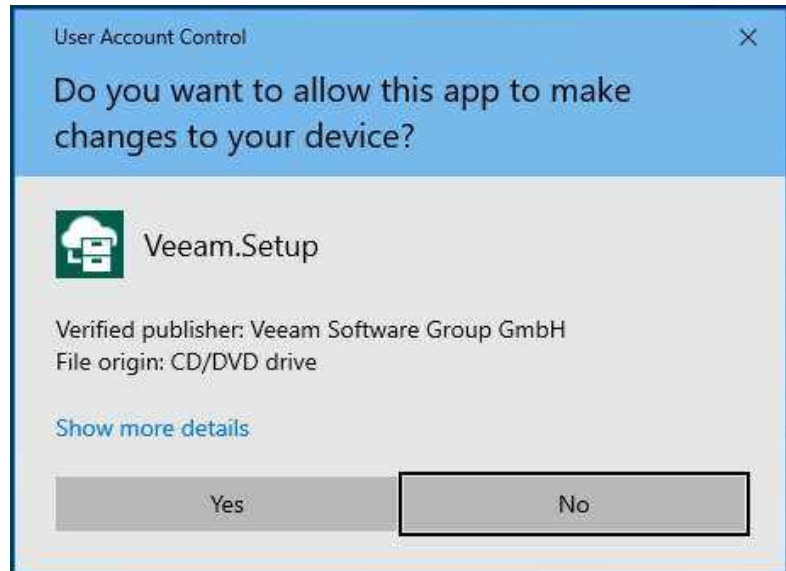
Instructions

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.



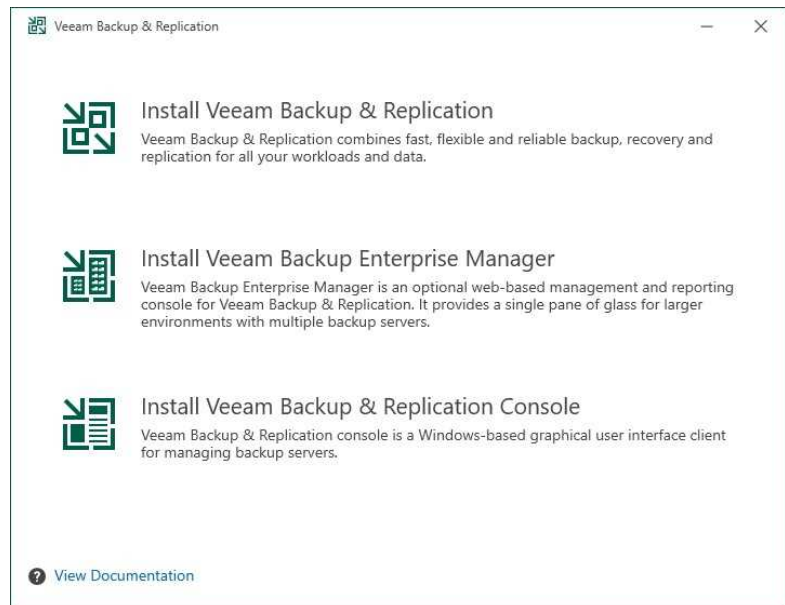
5. On the User Access Control page, click Yes.



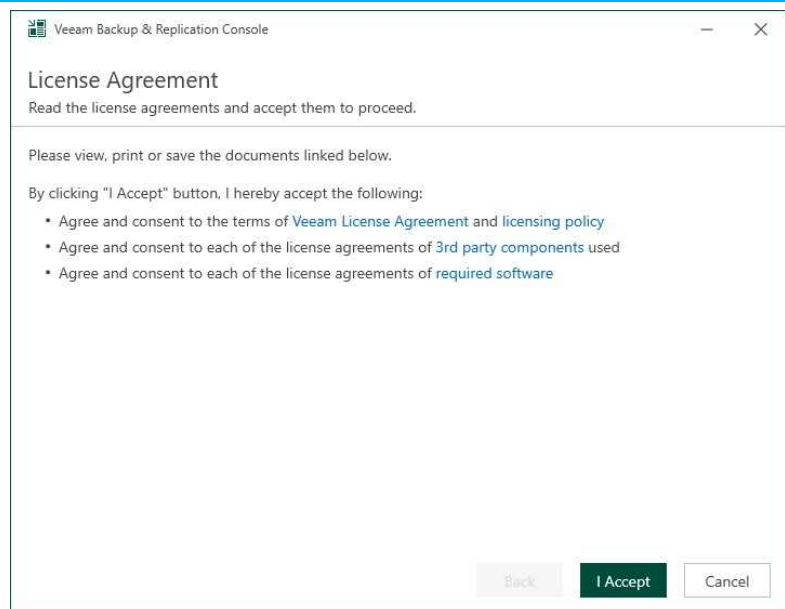
6. On the Veeam Backup & Replica on 12 page, click Install.



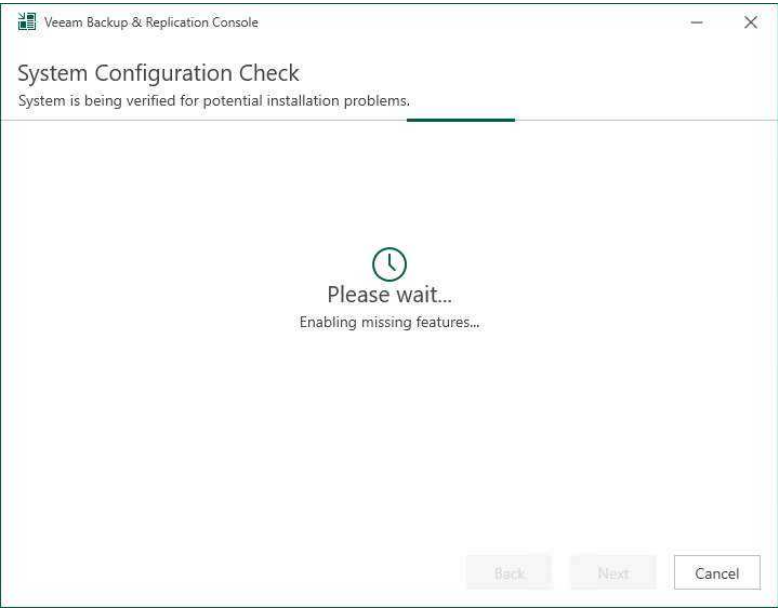
7. Select Install Veeam Backup & Replication on the Veeam Backup & Replication on page



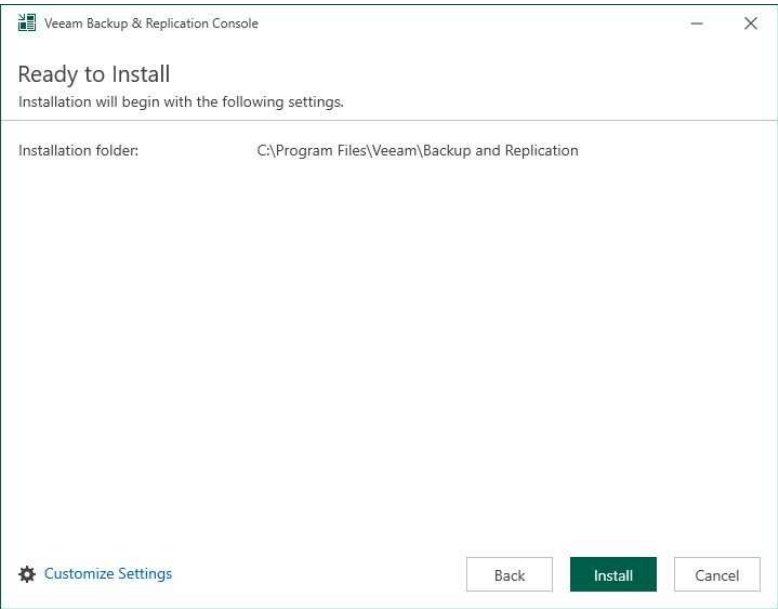
8. Click I Accept on the License Agreement page.



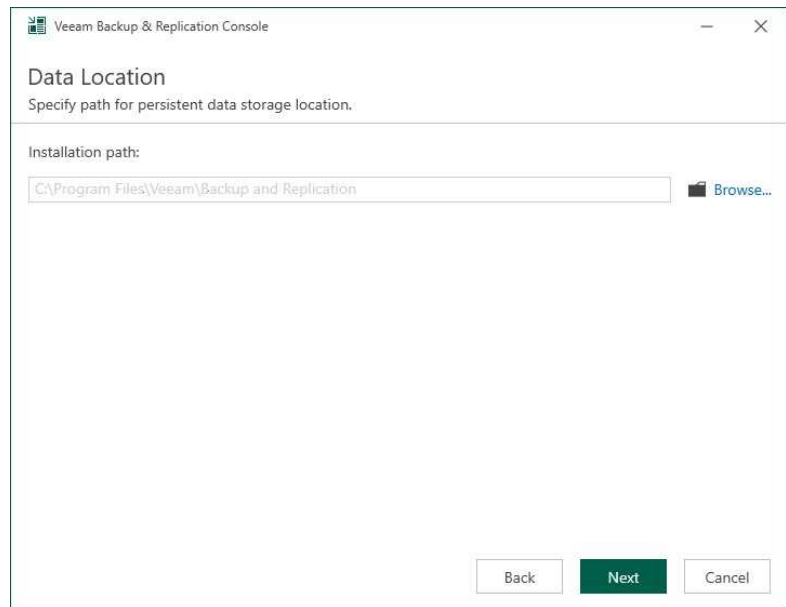
9. The setup wizard checks if the required software is installed on the machine during the System Configuration Check step. If required components are missing, the setup will attempt to install them independently. Rebooting is required after the components have been successfully installed. Click Reboot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



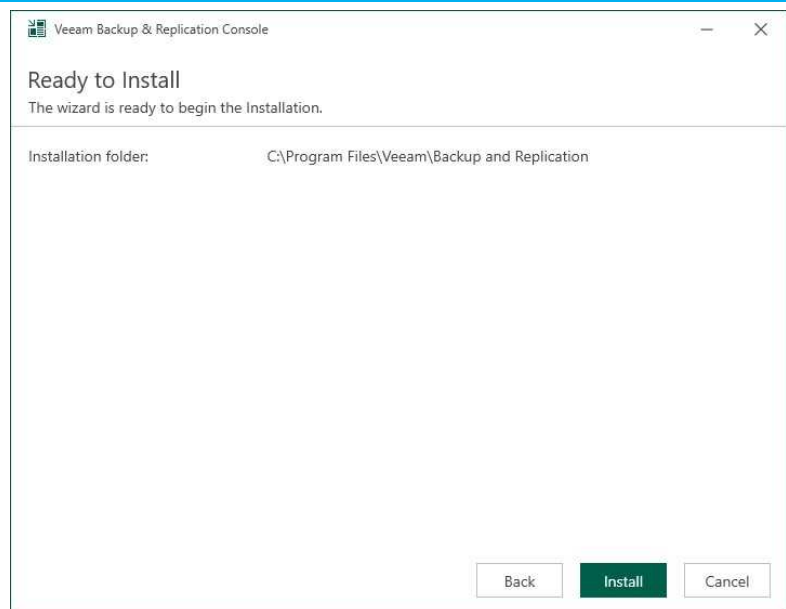
10. Click Customize Settings on the Ready to Install page.



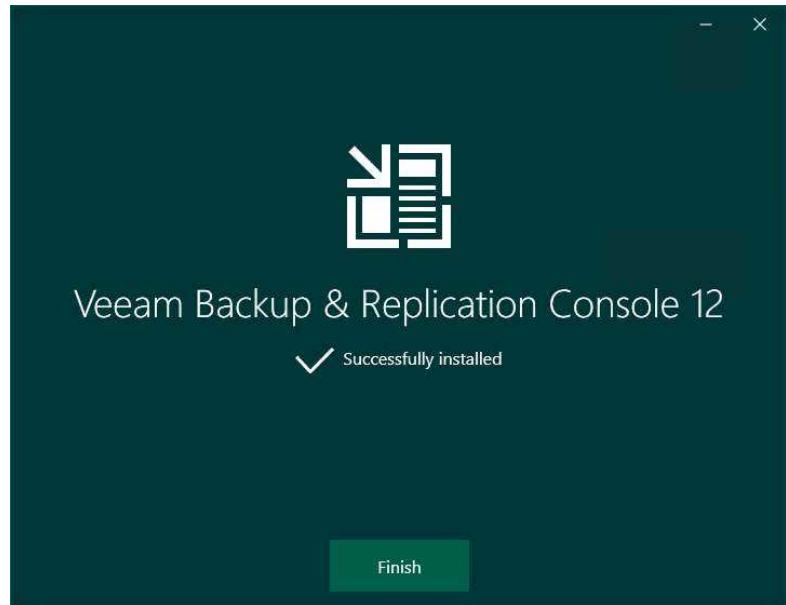
11. On the Data locations page, click Browse and select the path in the Installation path field.
12. Click Next.



13. Click Install on the Ready to Install page.

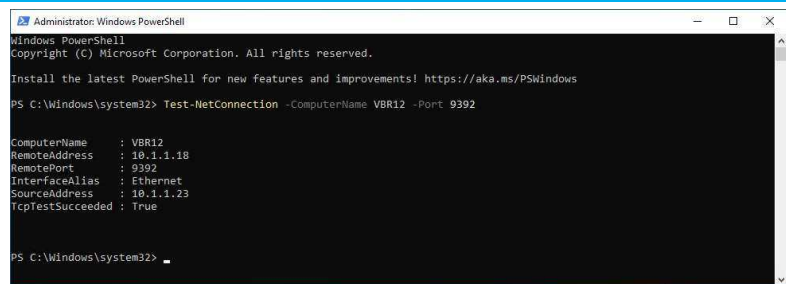


14. Click Finish on the Veeam Backup & Replication 12 Successfully installed page.

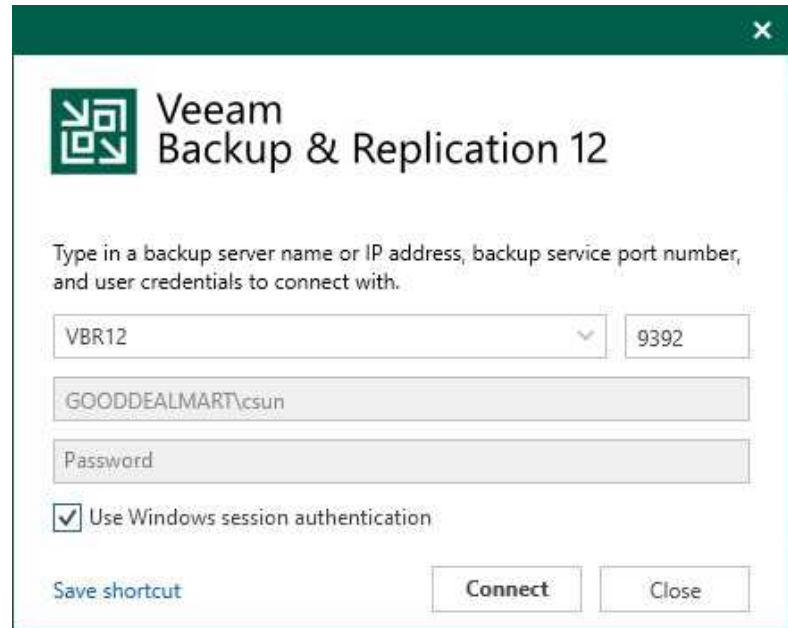


15. Verify that the Veeam Backup Service is running on the Veeam Backup Server, and then test connectivity to that service from the remote machine using the following PowerShell cmdlet.

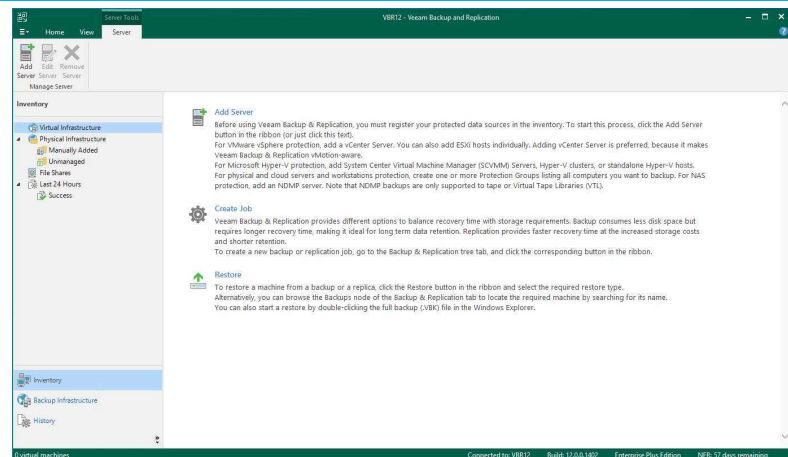
Test-NetConnection -
ComputerName
<hostname/ip> -Port 9392



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



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



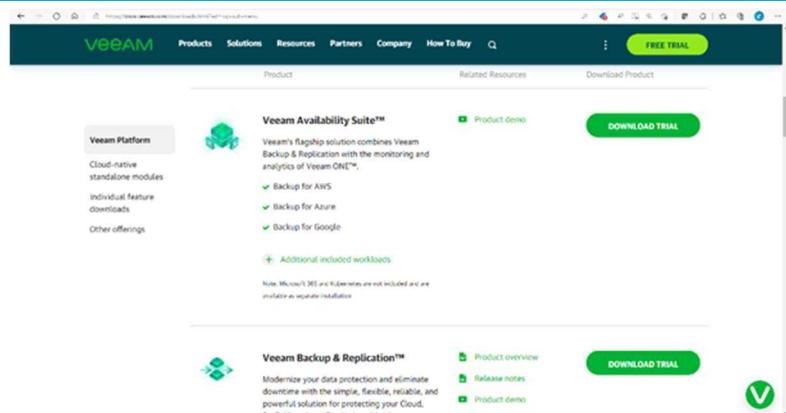
Upgrade to Veeam Backup and Replication Console 12

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

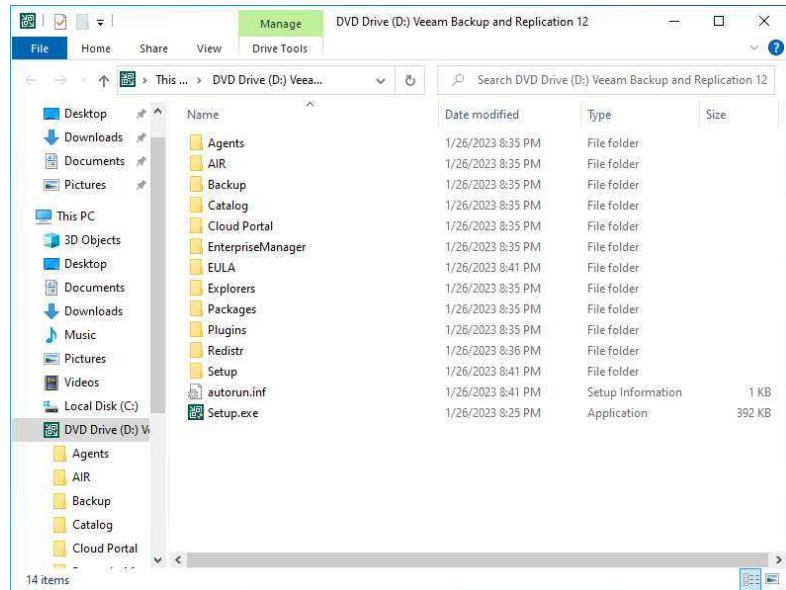
Instructions

Screenshot (if applicable)

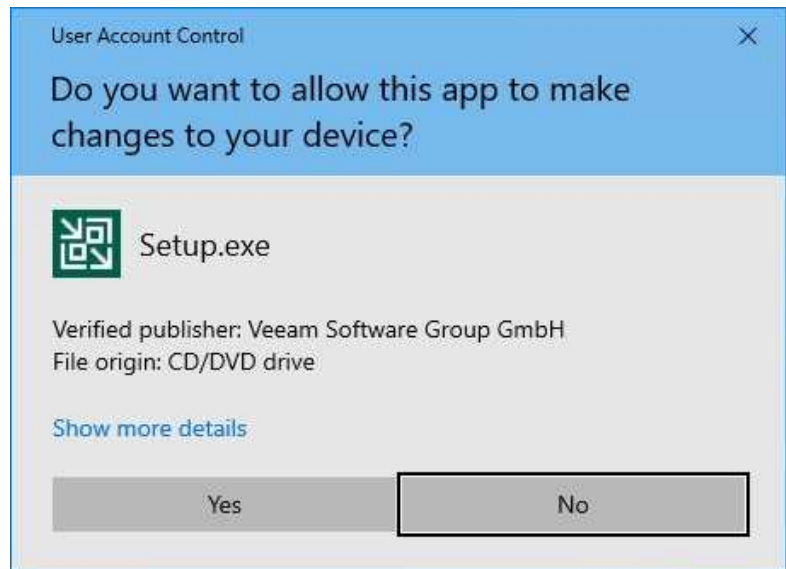
1. Log in to the existing Veeam Backup and replica on manager console machine.
2. Download the Veeam Backup and Replica on v12 iso image file from the Veeam website. (Sign-in required).



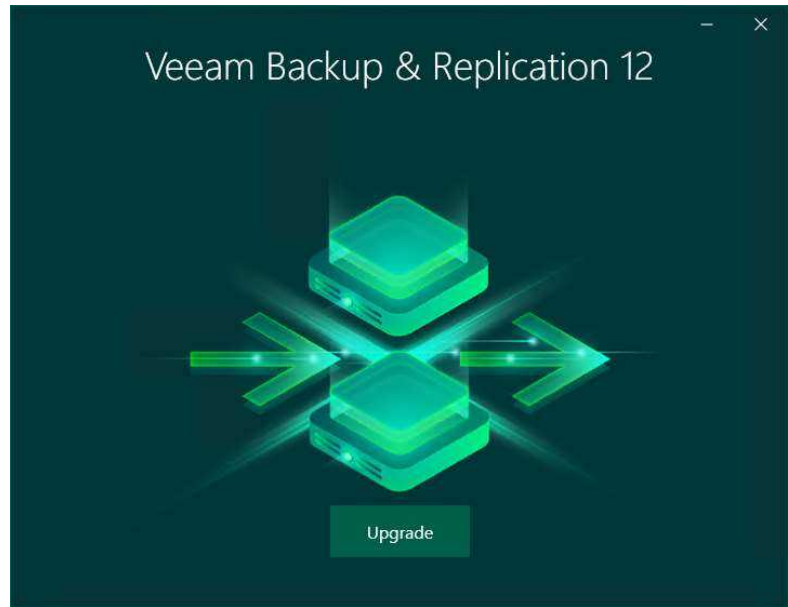
3. Mount the Veeam Backup & Replica on v12 ISO image file.
4. Run Setup.exe.



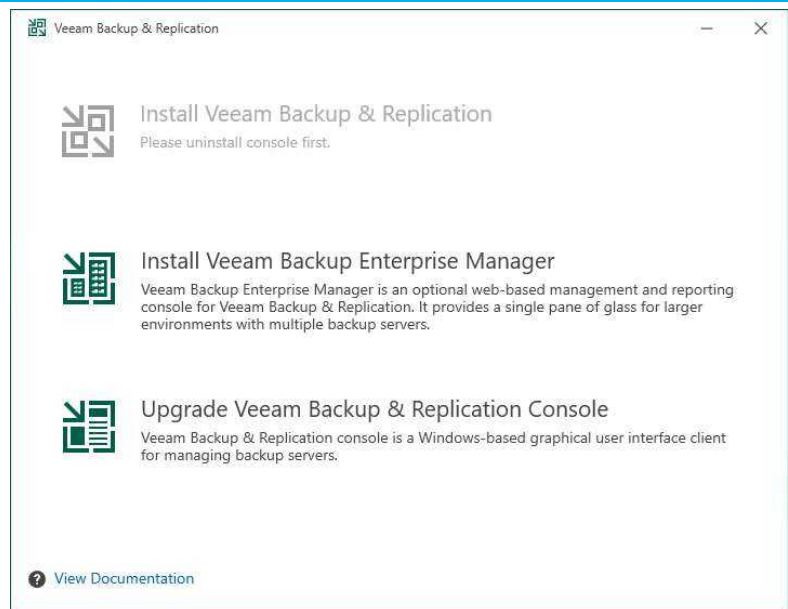
5. Click Yes on the User Account Control page.



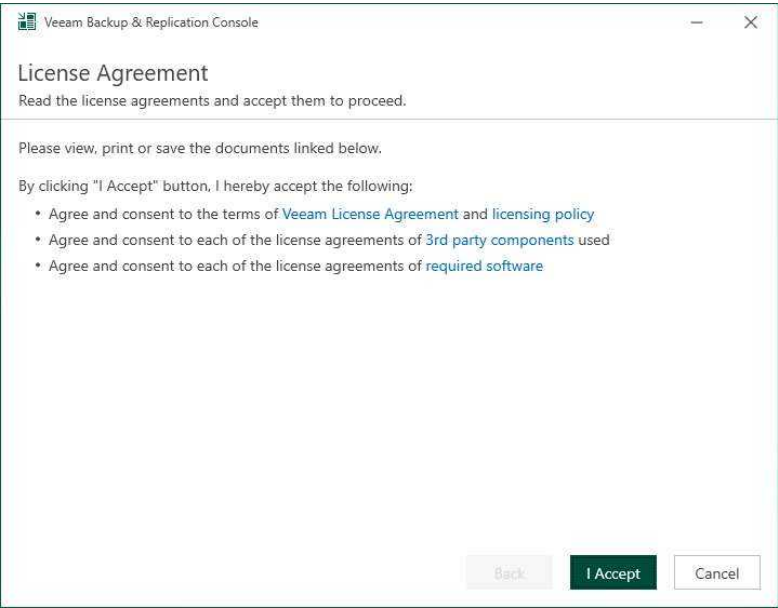
- Click Upgrade on the Veeam Backup & Replication 12 page.



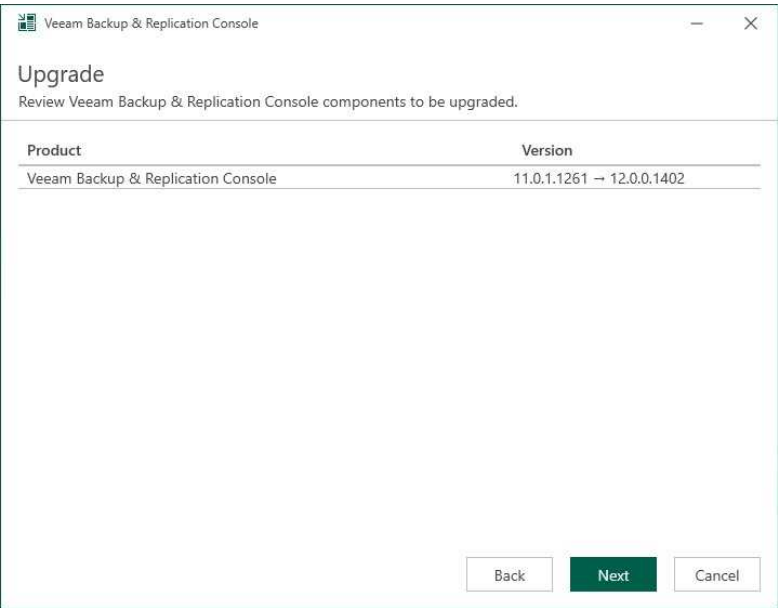
- Select Upgrade Veeam Backup & Replication Console on the Veeam Backup & Replication page.



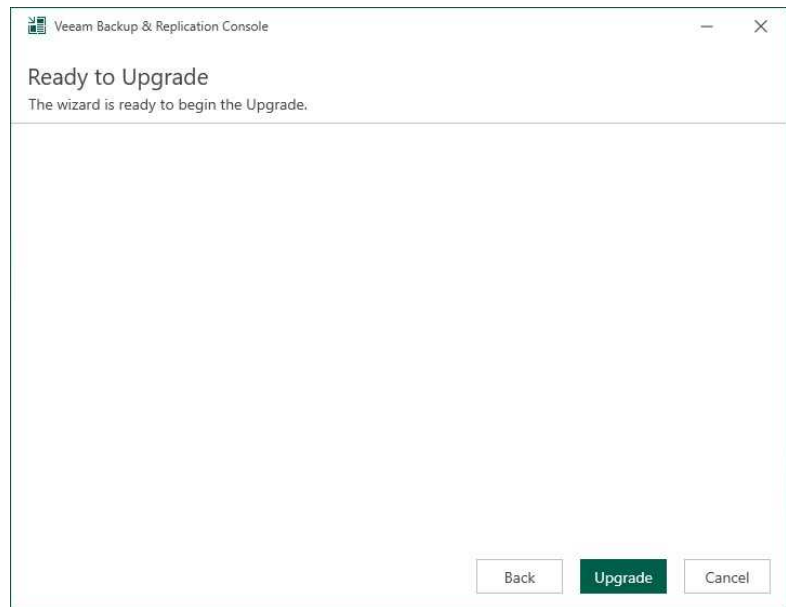
8. On the License Agreement page, click I Accept.



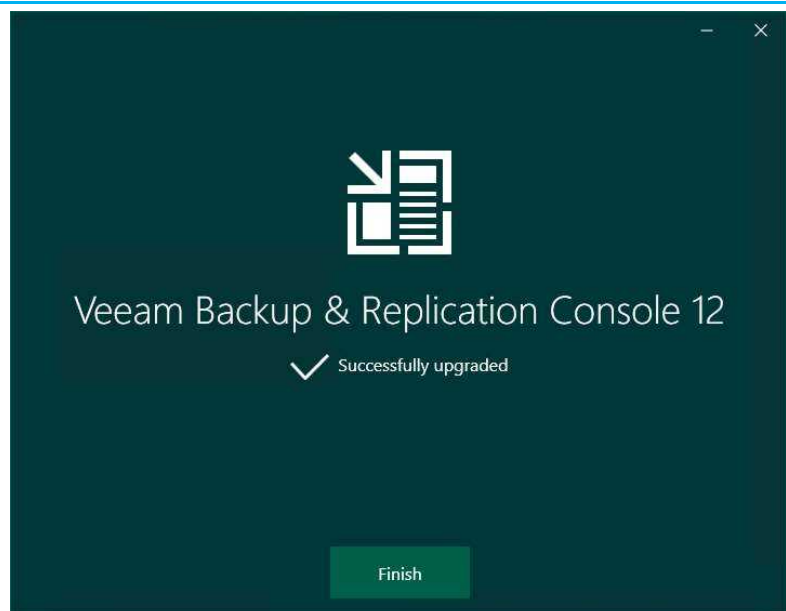
9. On the Upgrade page, click Next.



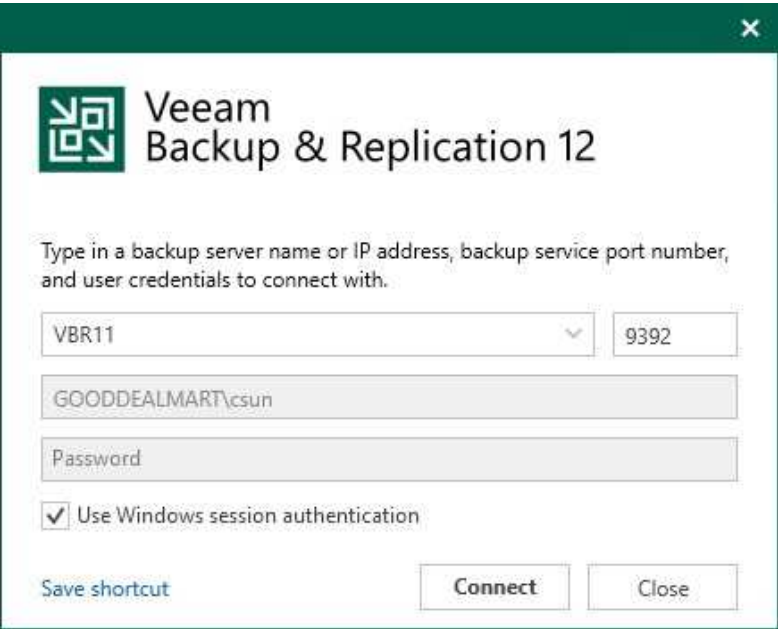
10. Click Upgrade on the Ready to Upgrade page.



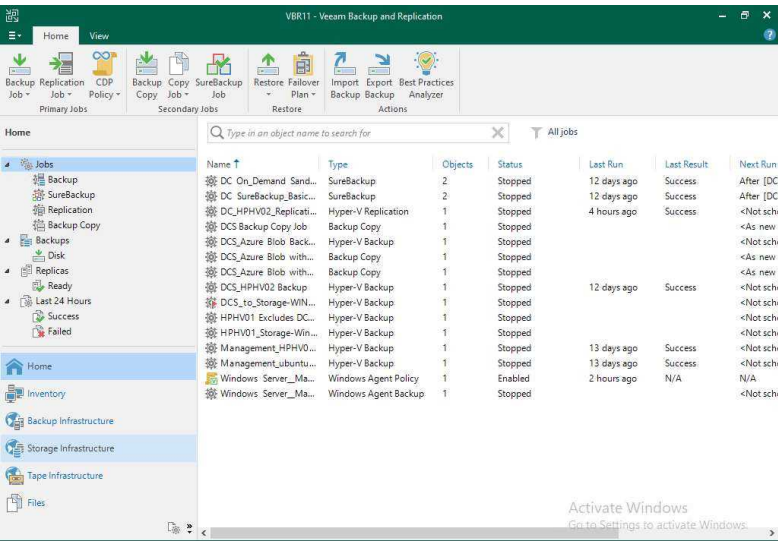
11. Click Finish on the Veeam Backup & Replication Console 12 successfully upgraded page.



12. Open Veeam and
Replica on Console 12
and click Connect.



13. Ensure connec on to
Veeam Backup and
Replica on manager
server is successful.



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
- General Settings

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

Virtualization Servers and Hosts

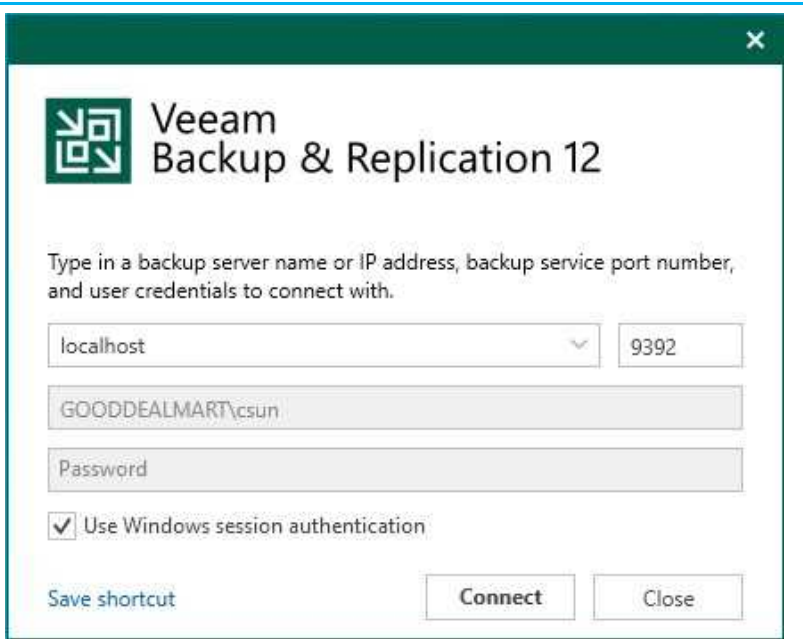
Veeam Backup & Replica on allows you to build a scalable backup infrastructure for many environments. Physical and virtual machines can be added to the backup infrastructure and assigned different roles. In addition, Veeam Backup and Replica on components can coexist on the same machine.

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

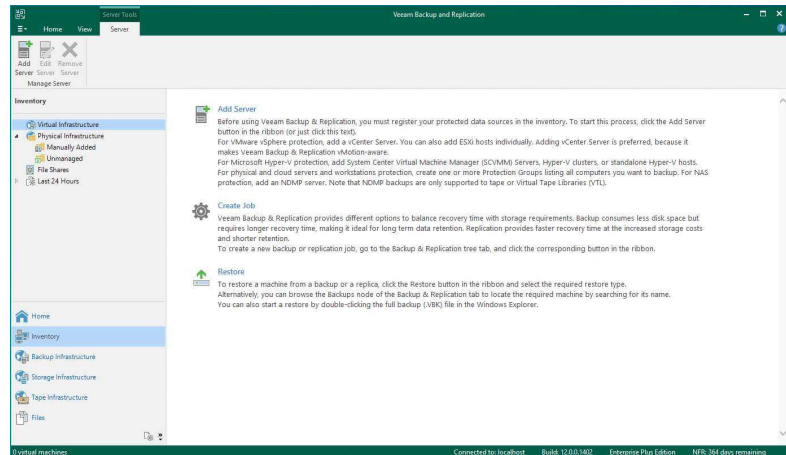
- Microsoft Hyper-V Standalone Servers
- Microsoft Hyper-V Cluster Servers
- Microsoft SMB3 Servers
- Microsoft Windows Servers
- Linux Server

Add Microsoft Hyper-V Standalone Servers

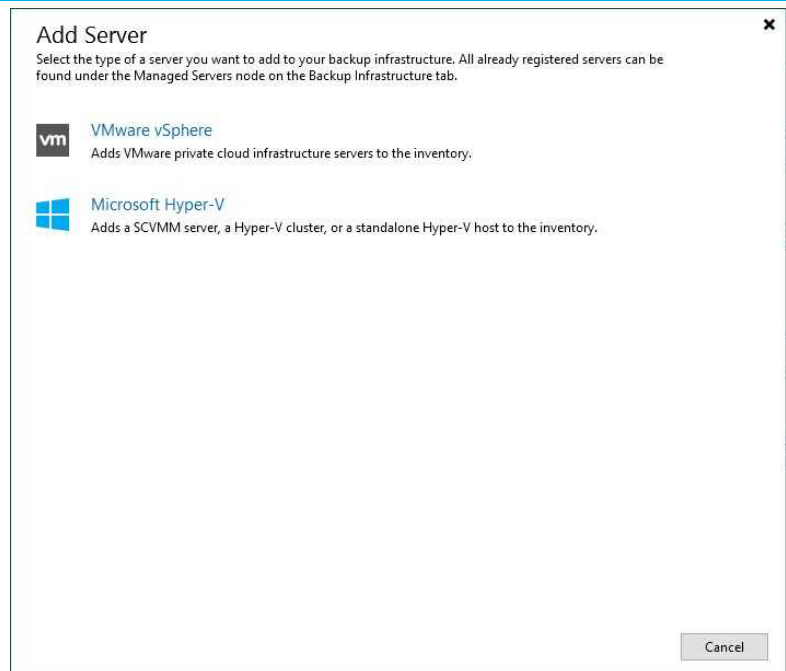
You must add the Microsoft Hyper-V standalone hosts you plan to use as source and target for backup, replication and other activities.

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.	 The screenshot shows the Veeam Backup & Replication 12 console window. The title bar is green with the Veeam logo and the text 'Veeam Backup & Replication 12'. The main area is white and contains the following elements: a text prompt 'Type in a backup server name or IP address, backup service port number, and user credentials to connect with.', a dropdown menu with 'localhost' selected, a text box with '9392', a text box with 'GOODDEALMART\csun', a text box with 'Password', a checked checkbox labeled 'Use Windows session authentication', a 'Save shortcut' button, a 'Connect' button, and a 'Close' button.

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



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



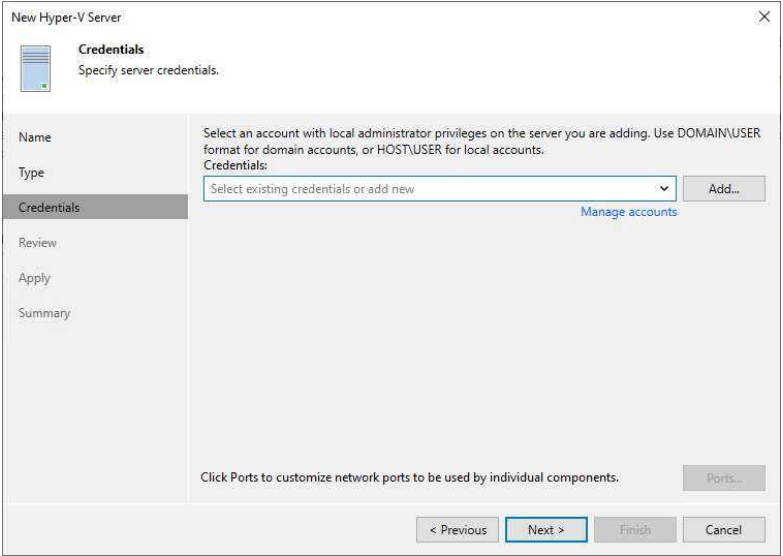
- 6. Enter the Microsoft Hyper-V server's full DNS name or IP address on the Name page.
- 7. Give a brief description in the Description field for future reference and click Next.

The screenshot shows the 'New Hyper-V Server' wizard at the 'Name' step. The left sidebar contains links for Name, Type, Credentials, Review, Apply, and Summary. The main area has a 'Name' section with the instruction 'Specify DNS name or IP address of Microsoft Hyper-V server.' and a text box containing 'HPHV01'. Below it is a 'Description' section with a text box containing 'Created by GOODDEALMART\csun at 2/1/2023 3:36 PM.'. At the bottom are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

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

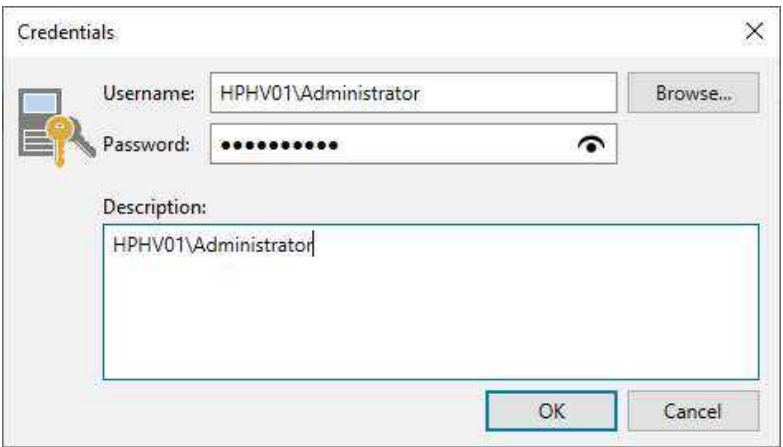
The screenshot shows the 'New Hyper-V Server' wizard at the 'Type' step. The left sidebar contains links for Name, Type, Credentials, Review, Apply, and Summary. The main area has a 'Type' section with the instruction 'Select the type of server you want to add.' and three radio button options: 'Microsoft System Center Virtual Machine Manager (SCVMM)', 'Microsoft Hyper-V cluster', and 'Microsoft Hyper-V server (standalone)'. The 'standalone' option is selected. At the bottom are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

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



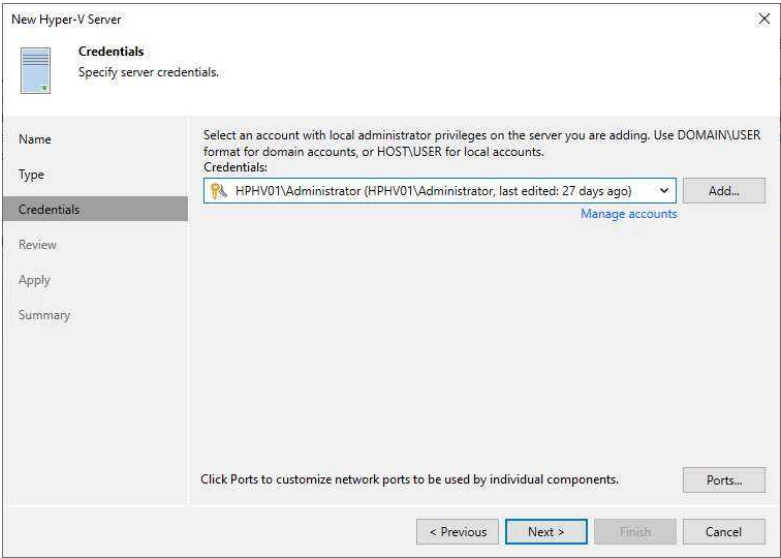
The screenshot shows the 'New Hyper-V Server' wizard with the 'Credentials' page selected. The page title is 'Credentials' with the subtitle 'Specify server credentials.' On the left, a navigation pane shows 'Name', 'Type', 'Credentials' (selected), 'Review', 'Apply', and 'Summary'. The main area contains instructions: '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.' Below this is a 'Credentials:' label and a drop-down menu with the text 'Select existing credentials or add new'. To the right of the drop-down is an 'Add...' button. Below the drop-down is a link that says 'Manage accounts'. At the bottom of the main area, there is a link that says 'Click Ports to customize network ports to be used by individual components.' and a 'Ports...' button. At the very bottom of the wizard are four buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

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.

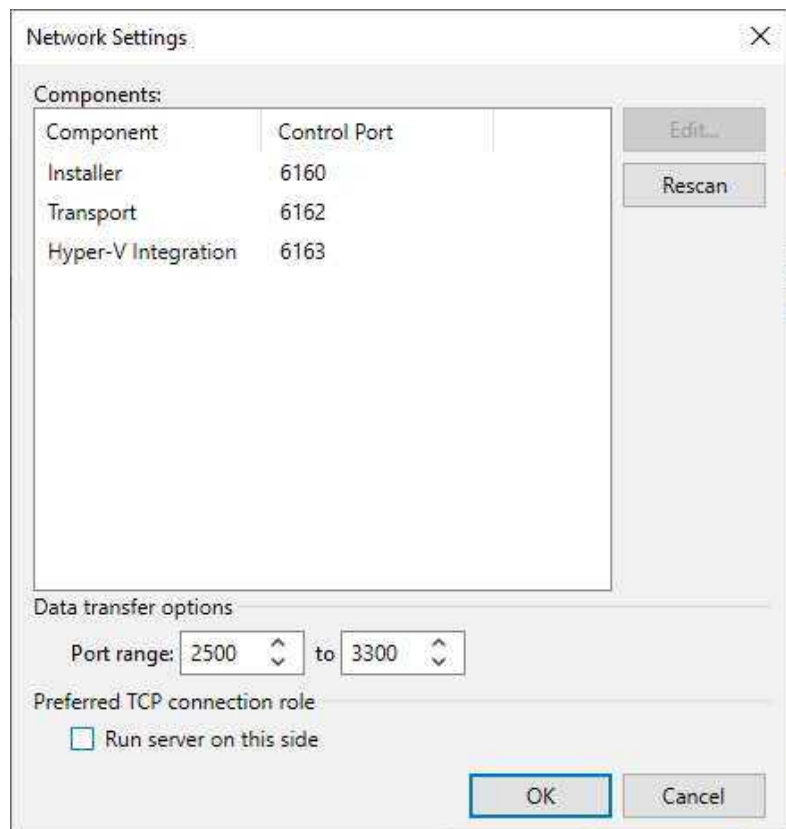


The screenshot shows the 'Credentials' dialog box. It has a title bar with 'Credentials' and a close button. On the left is a key icon. The 'Username:' field contains 'HPHV01\Administrator' and has a 'Browse...' button to its right. The 'Password:' field is masked with dots and has an eye icon to its right. The 'Description:' field contains 'HPHV01\Administrator'. At the bottom right are 'OK' and 'Cancel' buttons.

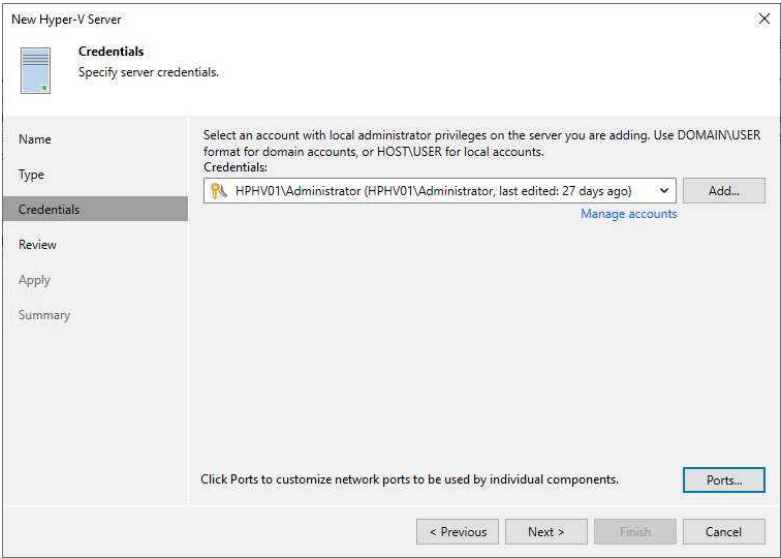
13. On the Credentials page, click Ports.



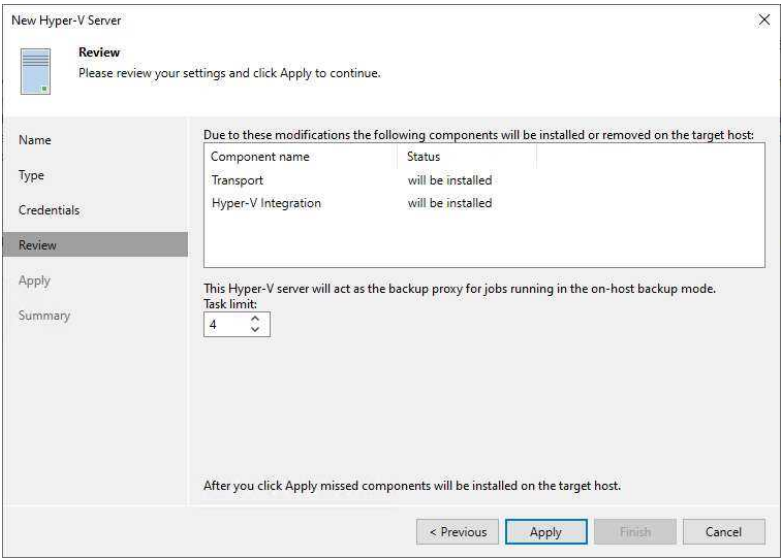
14. If necessary, change the network ports used by Veeam Backup & Replica on components on the Network Settings page.
15. Configure connection settings for file copy operations in the Network Settings window's Data transfer options section. Provide a set of ports for transmission channels between the 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 initialization may be disrupted.
17. Click OK.



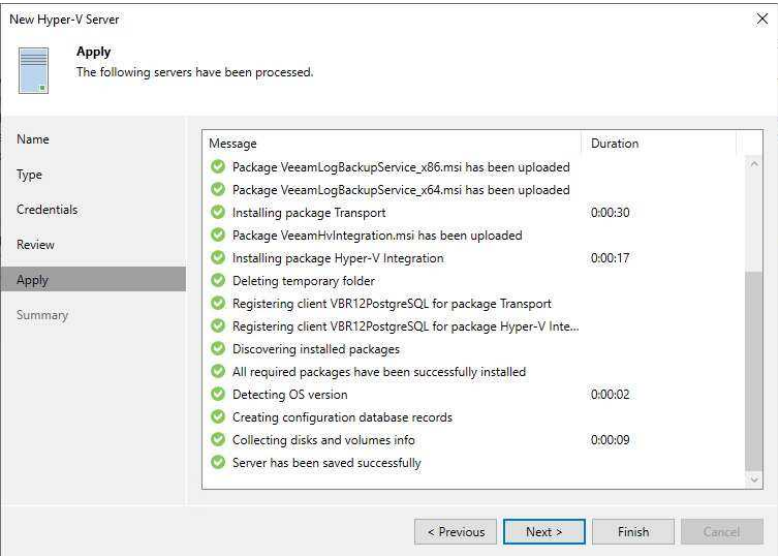
18. Click Next on the Credentials page.



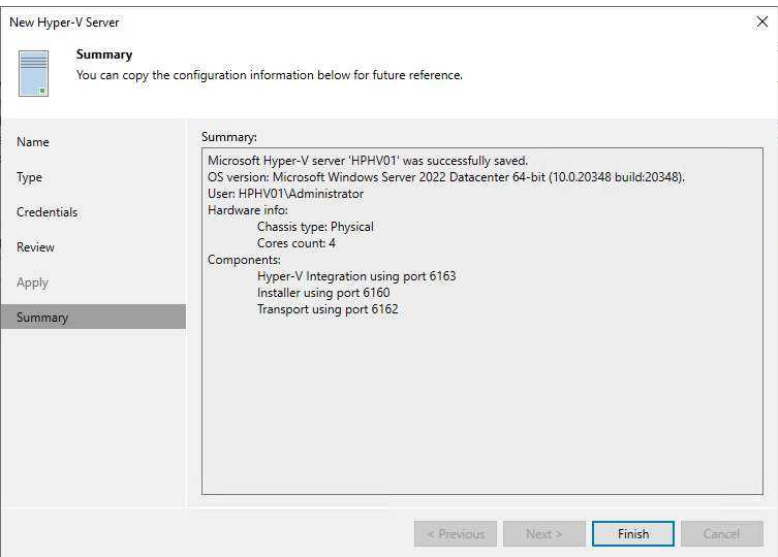
19. If you add a standalone Microsoft Hyper-V host on the Review page, specify the number of tasks the Microsoft Hyper-V host must handle concurrently in the Max concurrent tasks field.
20. Click Apply.



21. Click Next on the Apply page.

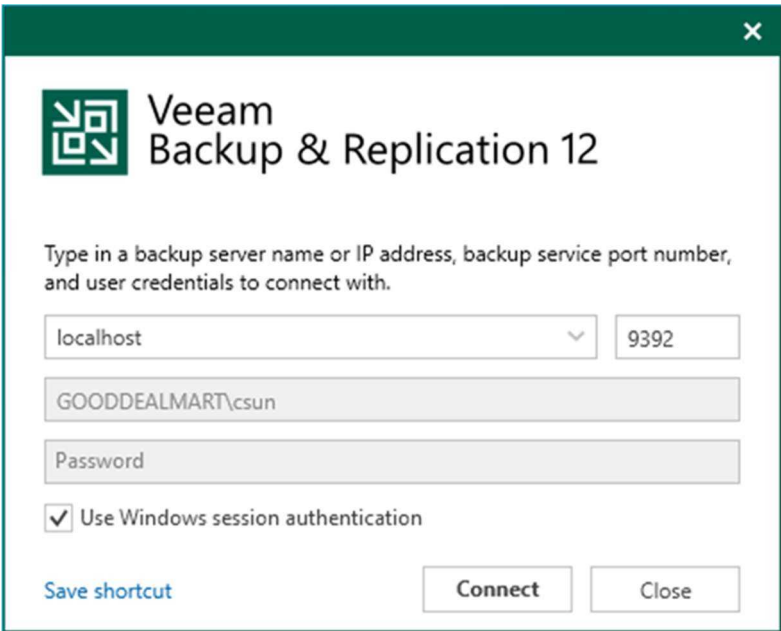


22. Click Finish on the Summary page.

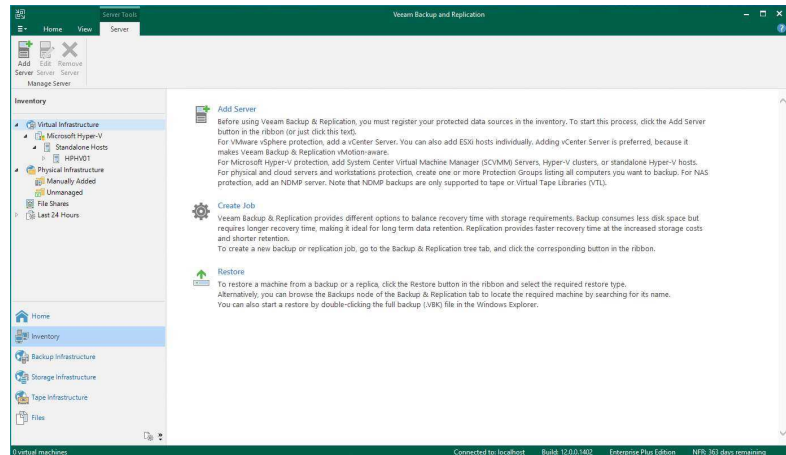


Add Microsoft Hyper-V Clusters

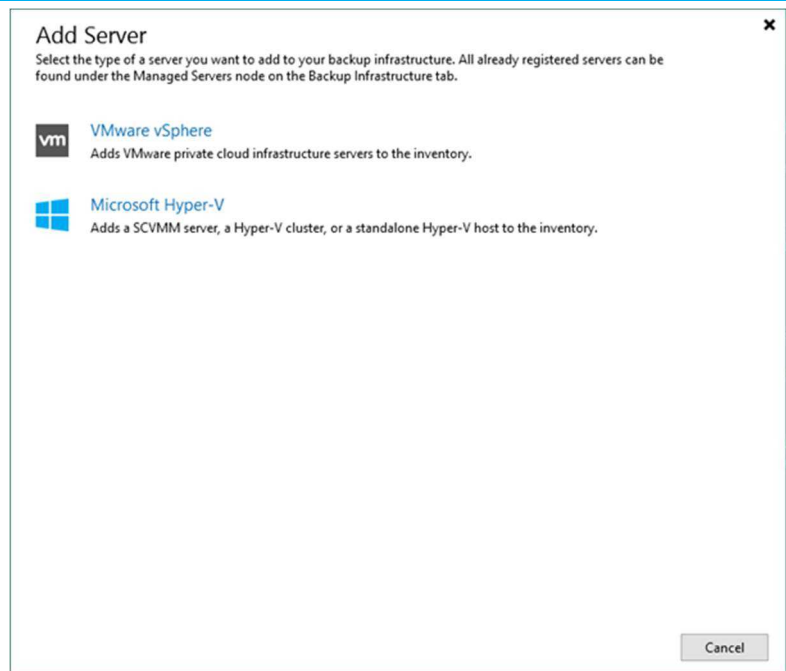
You must add the Microsoft Hyper-V clusters you plan to use as source and target for backup, replication and other activities.

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.	 The screenshot shows a window titled "Veeam Backup & Replication 12" with a close button in the top right corner. The window contains the Veeam logo and the text "Type in a backup server name or IP address, backup service port number, and user credentials to connect with." Below this text are four input fields: a dropdown menu showing "localhost" with a downward arrow, a text box containing "9392", a text box containing "GOODDEALMART\csun", and a text box containing "Password". Below these fields is a checkbox labeled "Use Windows session authentication" which is checked. At the bottom left is a link "Save shortcut" in blue. At the bottom right are two buttons: "Connect" and "Close".

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



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



- 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.

New Hyper-V Server

Name

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

Name

Type

Credentials

Review

Apply

Summary

DNS name or IP address:

FABS2DCU01

Description:

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

< Previous

Next >

Finish

Cancel

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

New Hyper-V Server

Type

Select the type of server you want to add.

Name

Type

Credentials

Review

Apply

Summary

☐ 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.

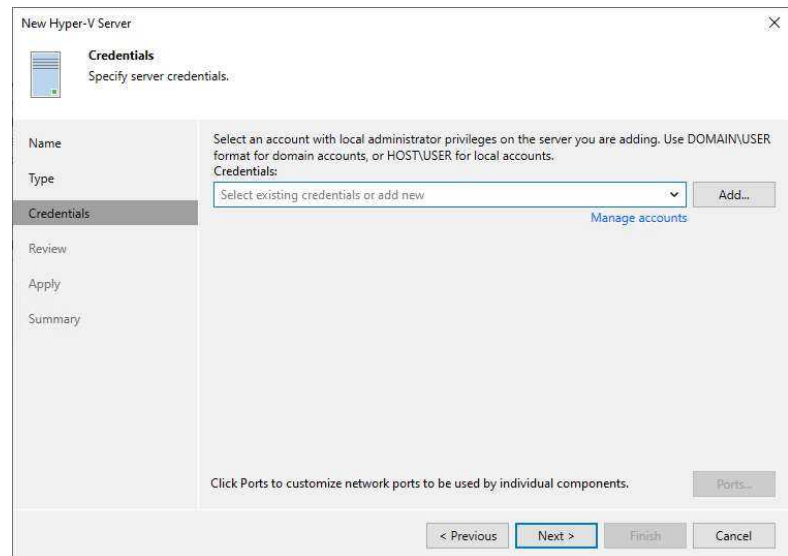
< Previous

Next >

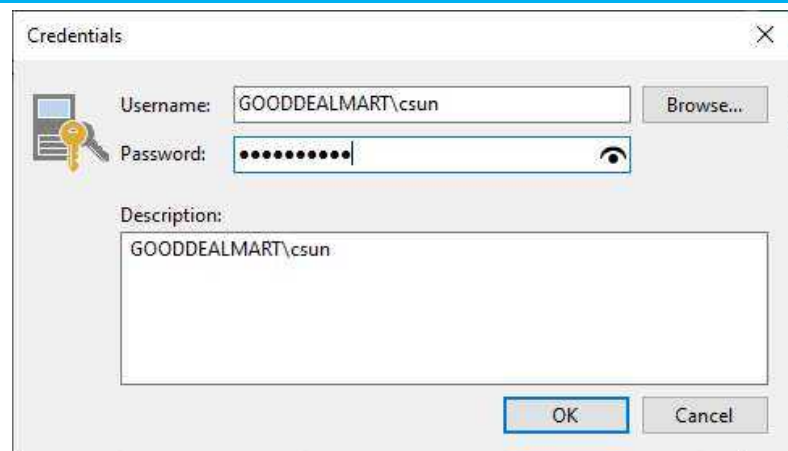
Finish

Cancel

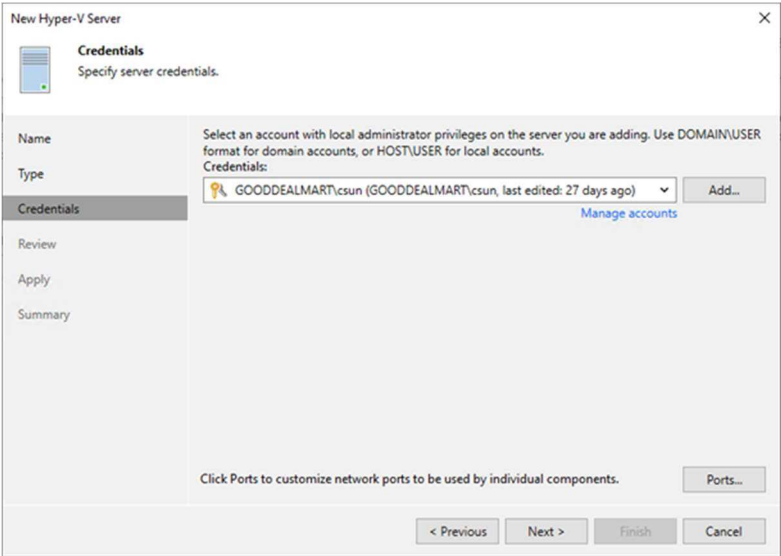
9. Select an account from the Credentials drop-down list on the Credentials page or click Add on the right to add the credentials.



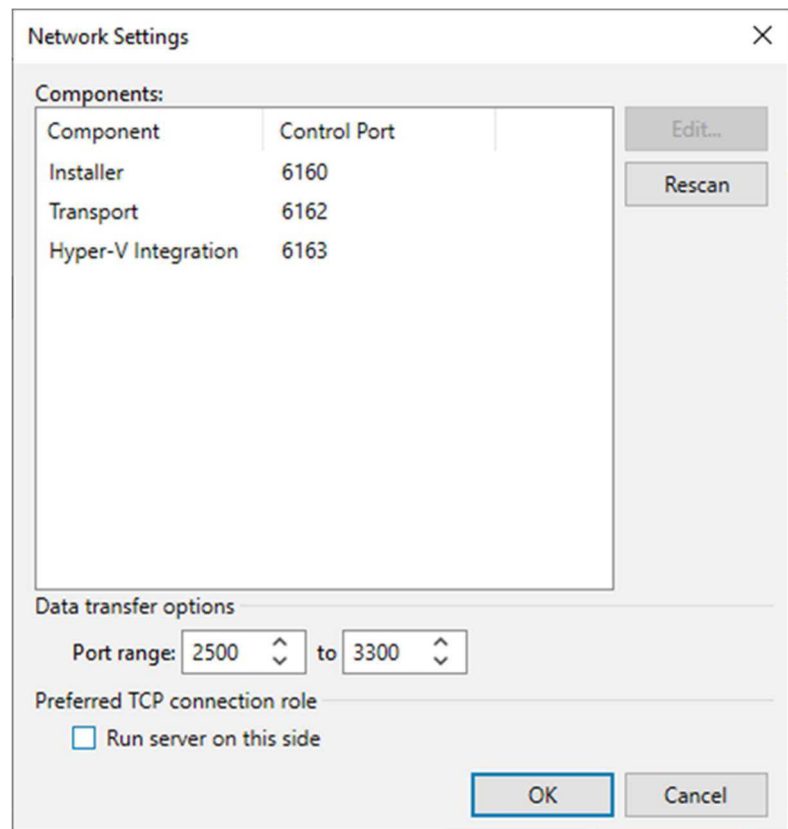
10. On the Credentials page, enter a user name in the Username field. You can also click Browse to select an existing user account.
11. Enter the password in the Password field.
12. Give a brief description in the Description field for future reference and click OK.



13. On the Credentials page, click Ports.



14. If necessary, change the network ports used by Veeam Backup & Replica on 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 initialization may be disrupted.
17. Click OK.



18. On the Credentials page, click Next.

New Hyper-V Server

**Credentials**
Specify server credentials.

Name

Type

Credentials

Review

Apply

Summary

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)

Add...

[Manage accounts](#)

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

Ports...

< Previous

Next >

Finish

Cancel

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

New Hyper-V Server

Review

Please review your settings and click Apply to continue.

Name
Type
Credentials
Review
Apply
Summary

Tasks:

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

Select All
Clear all

< Previous **Apply** Finish Cancel

20. Click Next on the Apply page.

21. Click Finish on the Summary page.
-

Add Microsoft SMB3 Servers

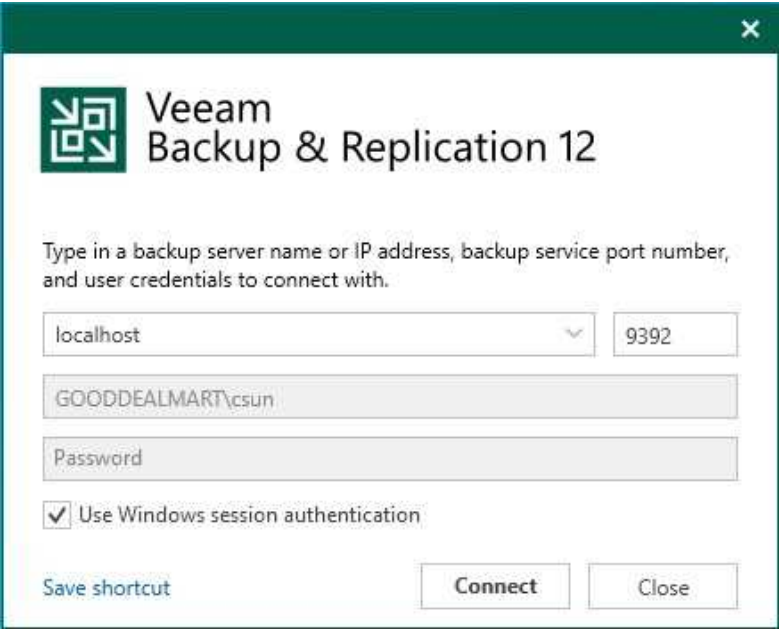
Veeam Backup & Replication can perform backup, replication, and file copy operations on Microsoft Hyper-V VMs whose discs are located on Microsoft SMB3 file shares.

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.

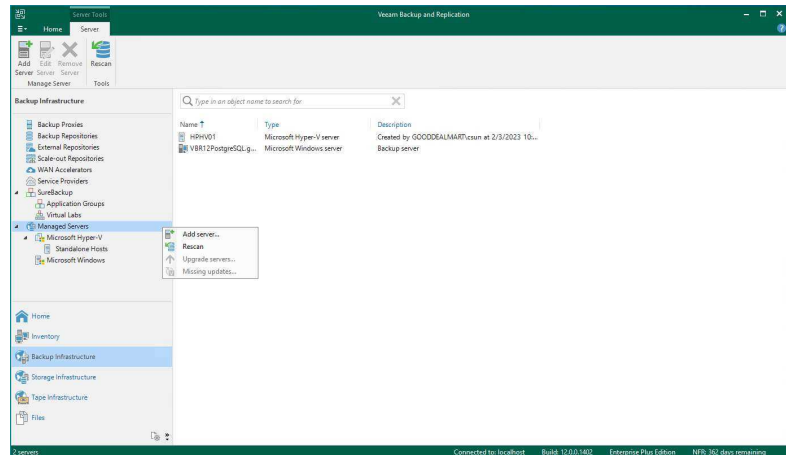
If VMs with discs on SMB3 shared folders are registered on Microsoft Hyper-V Server 2016 or later, a Microsoft SMB3 server is not required. However, if the Microsoft SMB3 server is not added, you cannot specify the Max snapshots, and latency control settings for SMB3 shared folders.

Note:

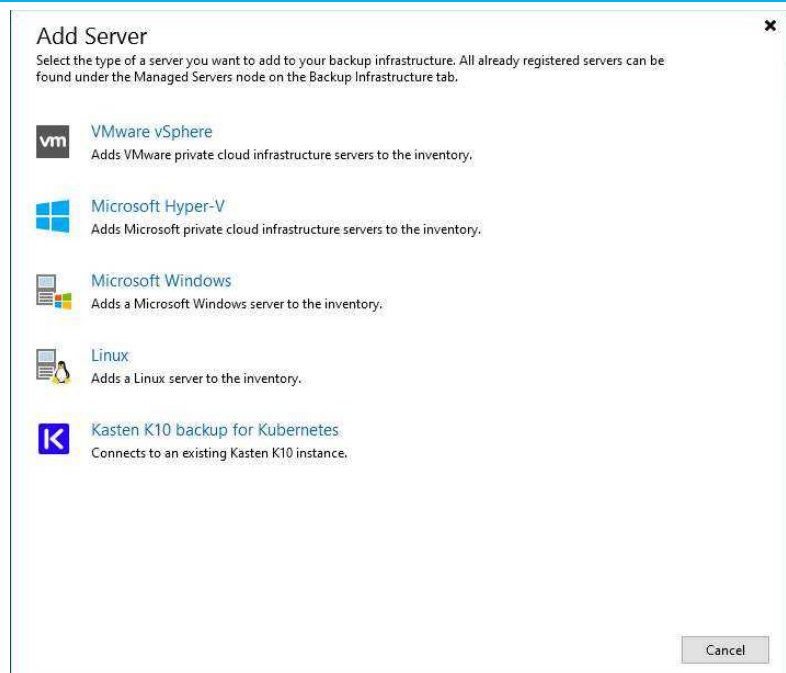
You cannot use Microsoft SMB3 shared folder as storage for VM replicas.

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.	 The screenshot shows the 'Veeam Backup & Replication 12' console window. It features a dark green header with the Veeam logo and title. Below the header, there is a text prompt: 'Type in a backup server name or IP address, backup service port number, and user credentials to connect with.' This is followed by four input fields: a dropdown menu showing 'localhost', a text box with '9392', a text box with 'GOODDEALMART\csun', and a password field labeled 'Password'. Below these fields is a checkbox labeled 'Use Windows session authentication' which is checked. At the bottom of the window are three buttons: 'Save shortcut', 'Connect', and 'Close'.

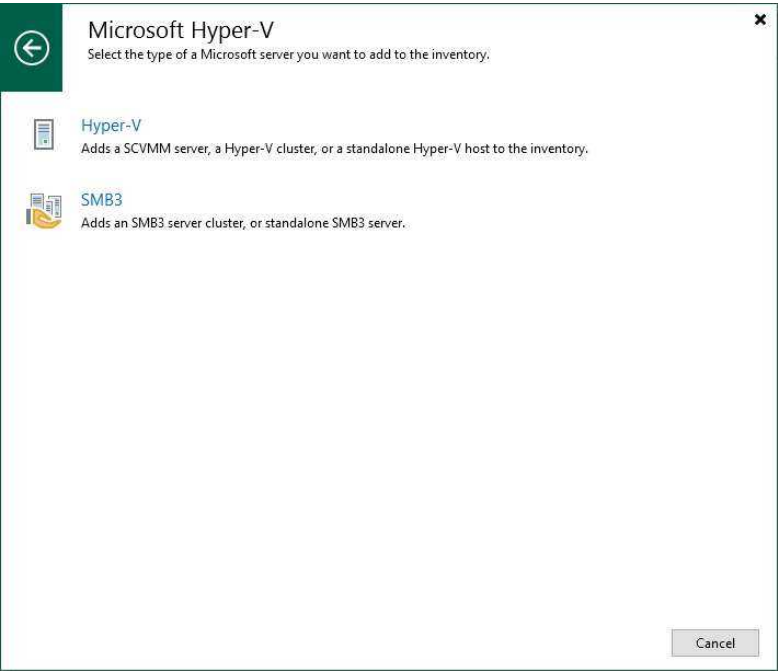
3. On the Home page, select Backup Infrastructure.
4. On the Backup Infrastructure page, select Managed Servers.
5. Right-click Managed Servers and select Add Server.



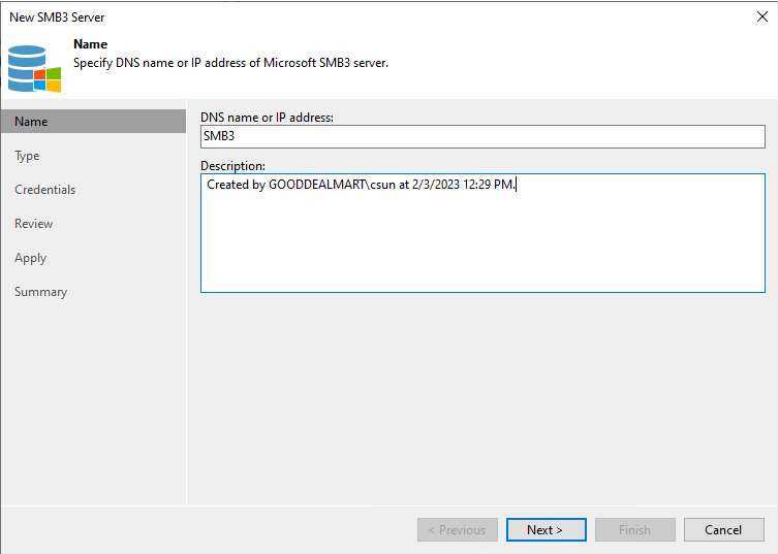
6. Select Microsoft Hyper-V on the Add Server Page.



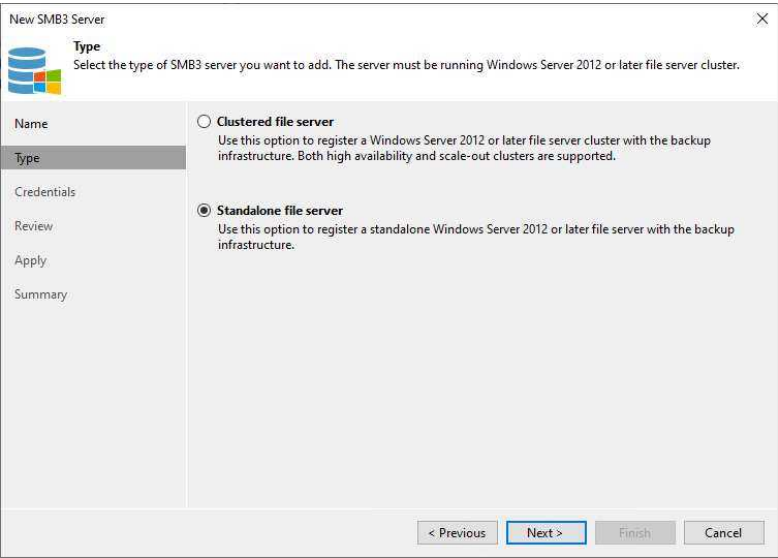
- 7. Select SMB3 on the Microsoft Hyper-V page.



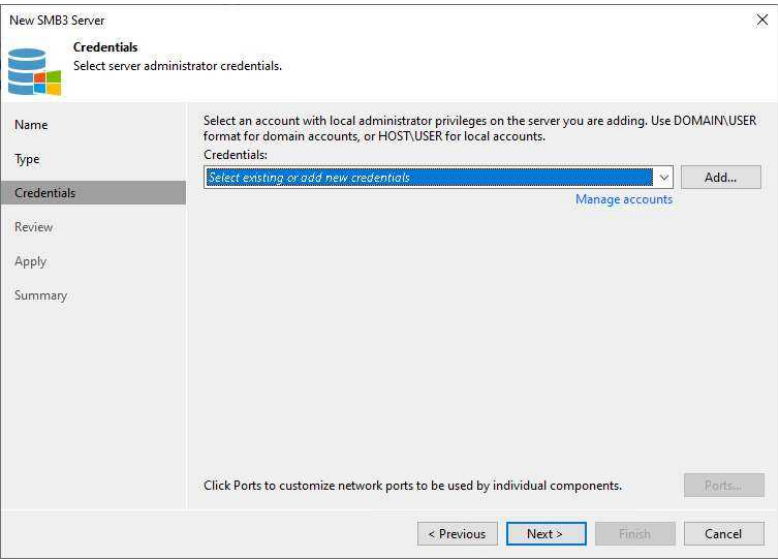
- 8. Enter the Microsoft SMB3 server's full DNS name or IP address on the Name page.
- 9. Give a brief description in the Description field for future reference and click Next.



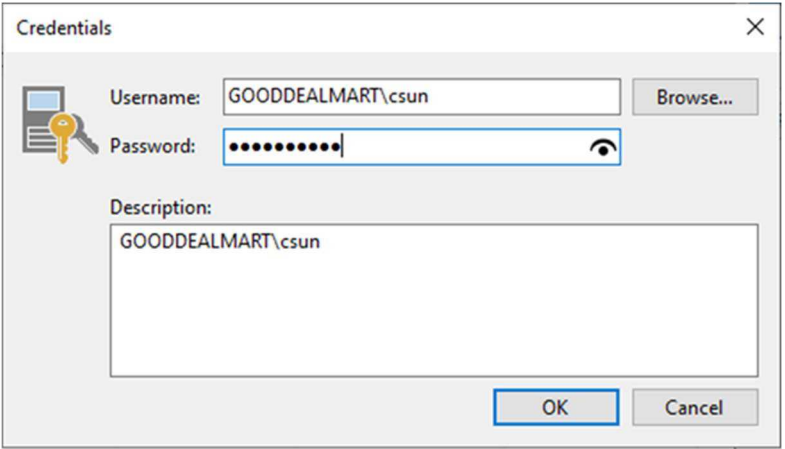
10. On the Type page, Choose the type of Microsoft SMB3 server you want to add and click Next.



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

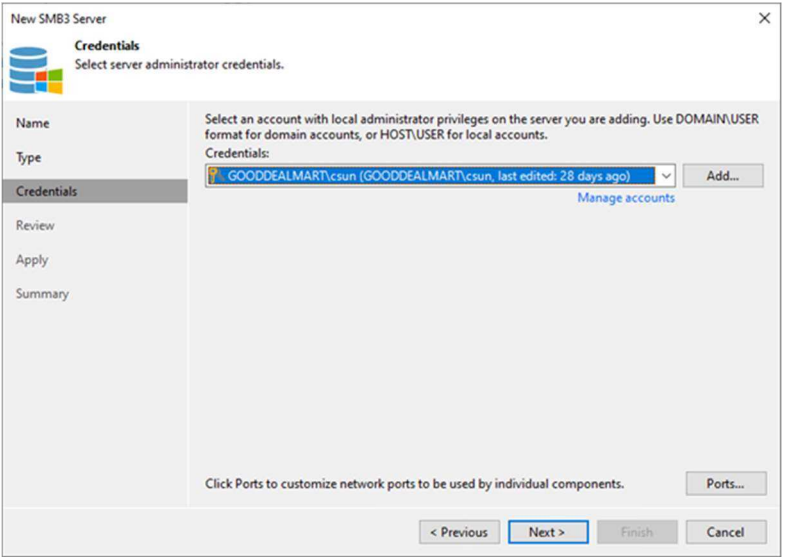


12. On the Credentials page, enter a user name in the Username field. You can also click Browse to select an existing user account.
13. Enter the password in the Password field.
14. Give a brief description in the Description field for future reference and click OK.



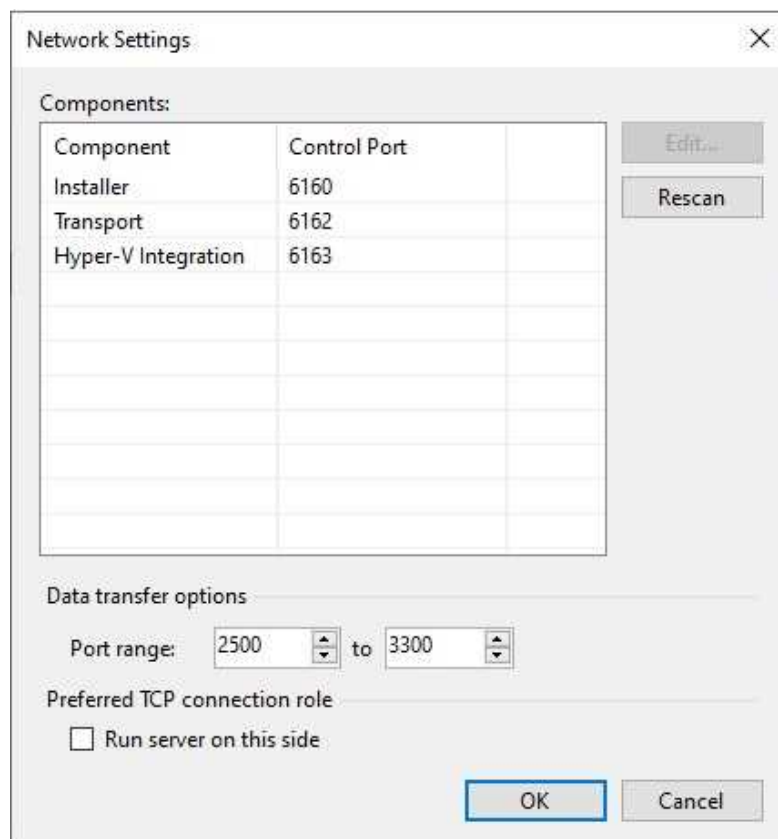
The 'Credentials' dialog box is shown. It has a title bar with a close button (X). Inside, there is a key icon next to the 'Username' field, which contains 'GOODDEALMART\csun'. To the right of the 'Username' field is a 'Browse...' button. Below the 'Username' field is the 'Password' field, which is masked with dots. To the right of the 'Password' field is an eye icon. Below the 'Password' field is the 'Description' field, which contains 'GOODDEALMART\csun'. At the bottom right are 'OK' and 'Cancel' buttons.

15. On the Credentials page, click Ports.

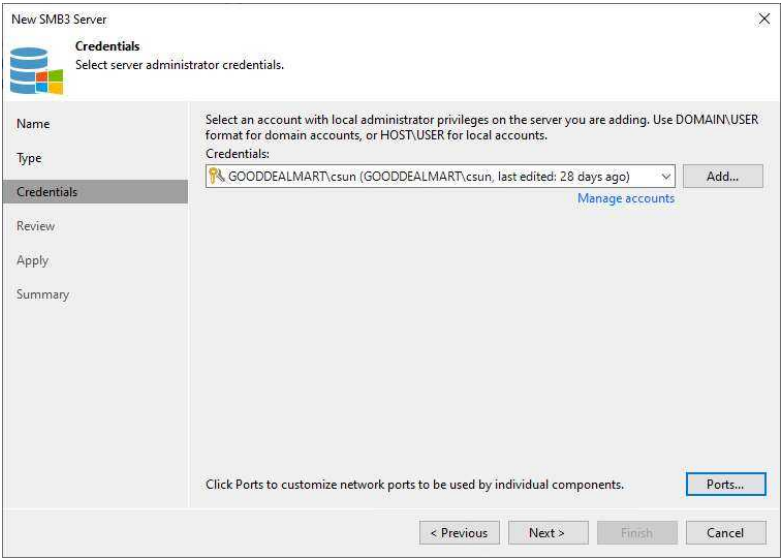


The 'New SMB3 Server' wizard is shown, specifically the 'Credentials' page. The title bar says 'New SMB3 Server' and 'Credentials'. Below the title bar is a sub-header 'Select server administrator credentials.' and a paragraph: 'Select an account with local administrator privileges on the server you are adding. Use DOMAIN\USER format for domain accounts, or HOST\USER for local accounts.' Below this is a 'Credentials:' label and a dropdown menu showing 'GOODDEALMART\csun (GOODDEALMART\csun, last edited: 28 days ago)'. To the right of the dropdown is an 'Add...' button. Below the dropdown is a link 'Manage accounts'. On the left side, there is a list of steps: 'Name', 'Type', 'Credentials' (which is selected), 'Review', 'Apply', and 'Summary'. At the bottom, there is a paragraph: 'Click Ports to customize network ports to be used by individual components.' and a 'Ports...' button. At the very bottom are navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

16. If necessary, change the network ports used by Veeam Backup & Replica on 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 initialization may be disrupted.
19. Click OK.

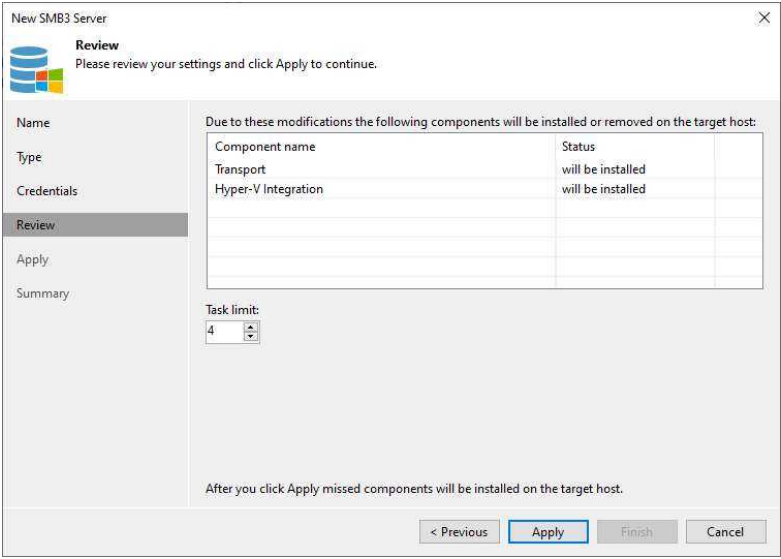


20. Click Next on the Credentials page.

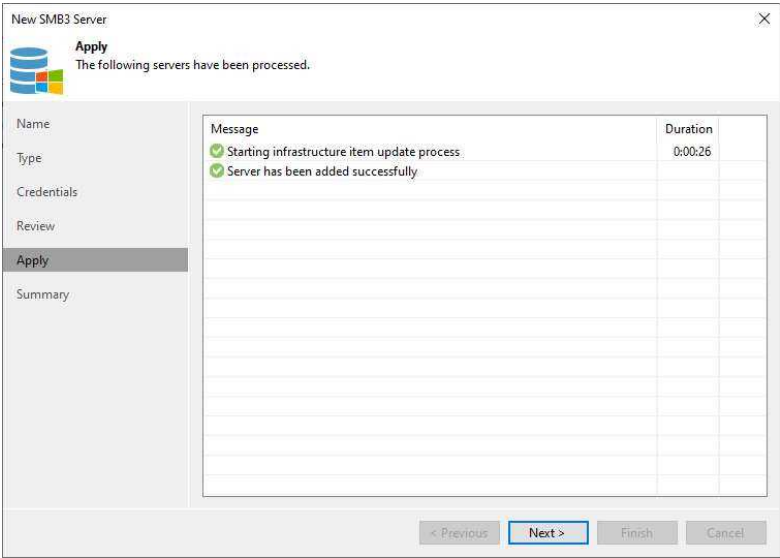


21. If you add a standalone Microsoft Hyper-V host on the Review page, specify the number of tasks the Microsoft Hyper-V host must handle concurrently in the Task limit field.

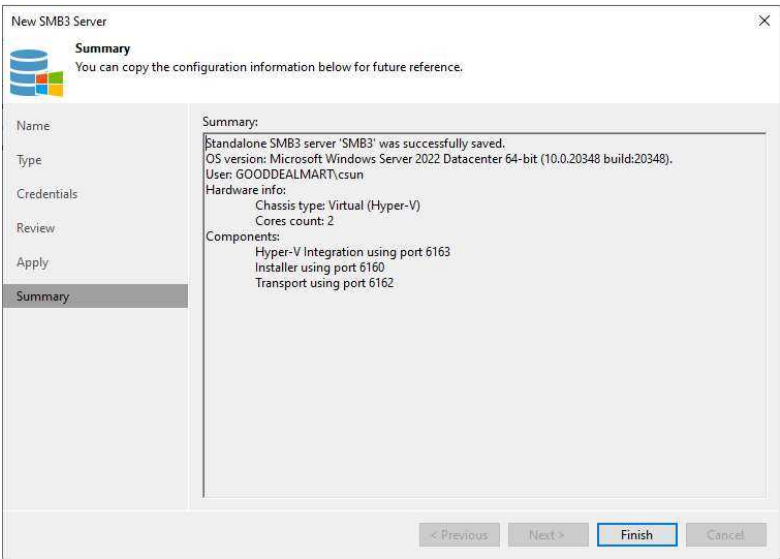
22. Click Apply.



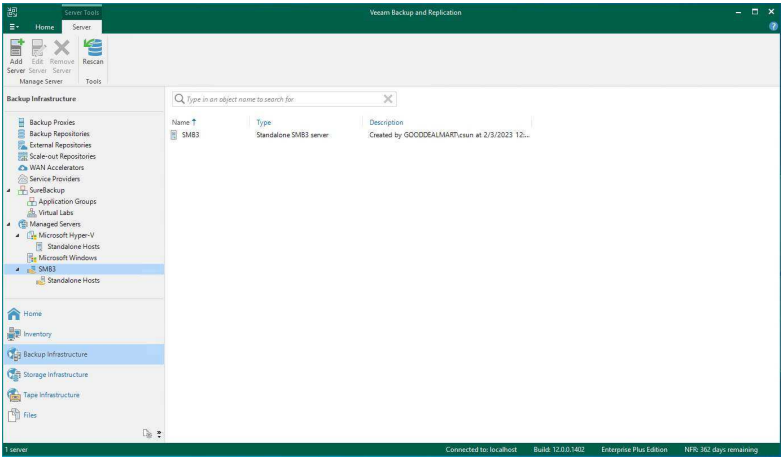
23. Click Next on the Apply page.



Click Finish on the Summary page.

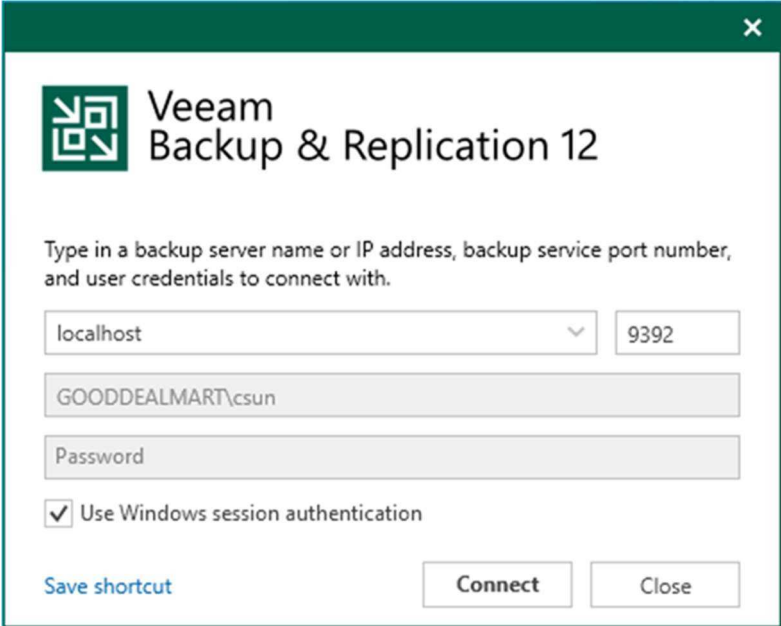


24. Ensure the new Microsoft SMB3 server is added.

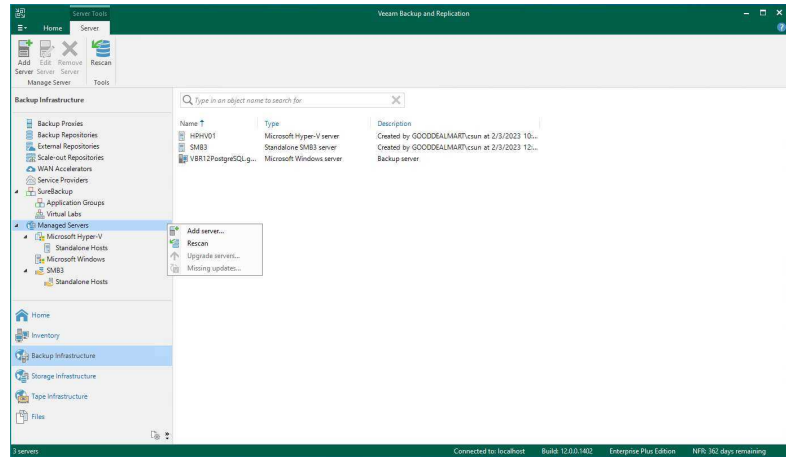


Add Microsoft Windows Servers

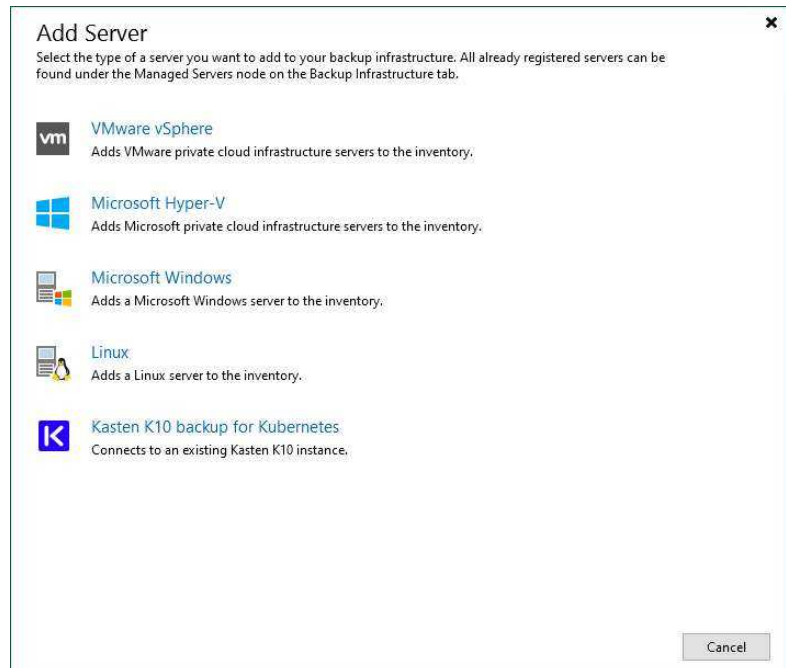
Suppose you plan to use as backup infrastructure components and servers that you plan to use for various types of restore operations. In that case, you must add the Microsoft Windows servers to the backup infrastructure.

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.	 The screenshot shows a window titled "Veeam Backup & Replication 12" with a green header bar. Inside the window, there is a Veeam logo and the text "Type in a backup server name or IP address, backup service port number, and user credentials to connect with." Below this, there are four input fields: a dropdown menu showing "localhost", a text box with "9392", a text box with "GOODDEALMART\csun", and a text box with "Password". There is a checkbox labeled "Use Windows session authentication" which is checked. At the bottom, there are three buttons: "Save shortcut" (in blue text), "Connect", and "Close".

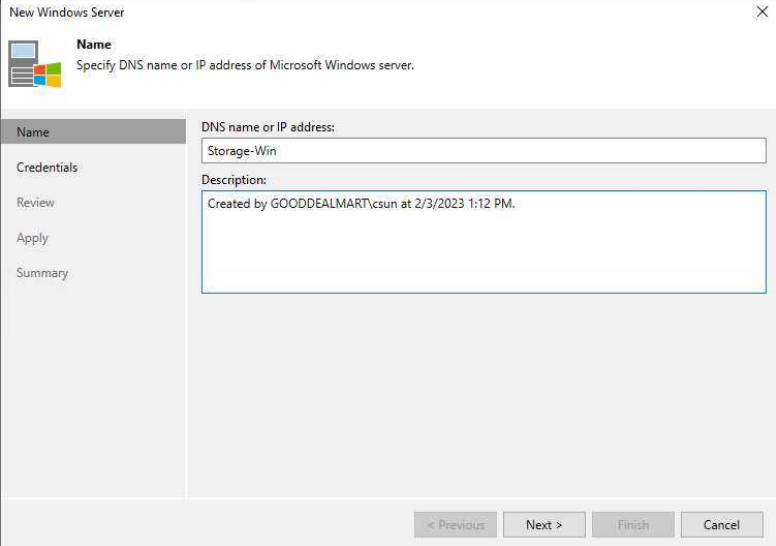
3. On the Home page, select Backup Infrastructure.
4. On the Backup Infrastructure page, select Managed Servers.
5. Right-click Managed Servers and select Add Server.



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

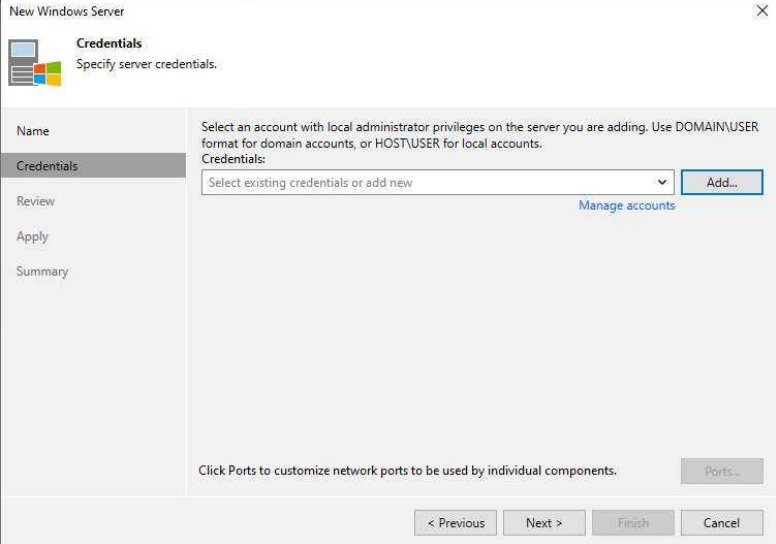


7. Enter the Microsoft Windows server's full DNS name or IP address on the Name page.
8. Give a brief description in the Description field for future reference and click Next.



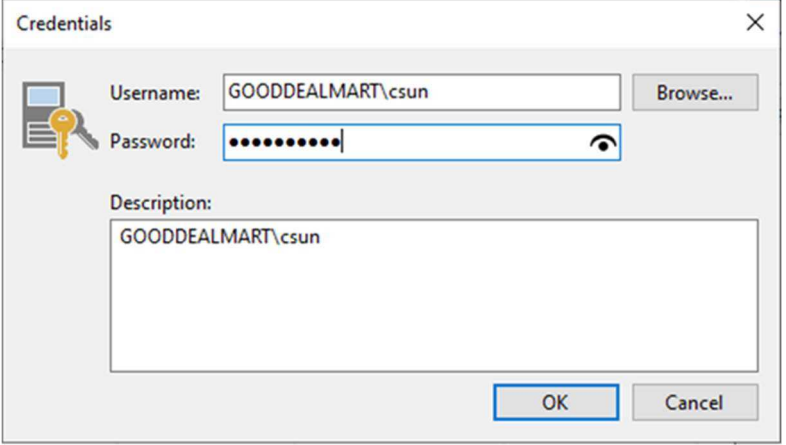
The screenshot shows the 'New Windows Server' wizard at the 'Name' step. The left sidebar has 'Name' selected, with 'Credentials', 'Review', 'Apply', and 'Summary' below it. The main area has a title 'Name' and a subtitle 'Specify DNS name or IP address of Microsoft Windows server.' Below this is a text box labeled 'DNS name or IP address:' containing 'Storage-Win'. A 'Description:' text box below it contains 'Created by GOODDEALMART\csun at 2/3/2023 1:12 PM.'. At the bottom are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

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



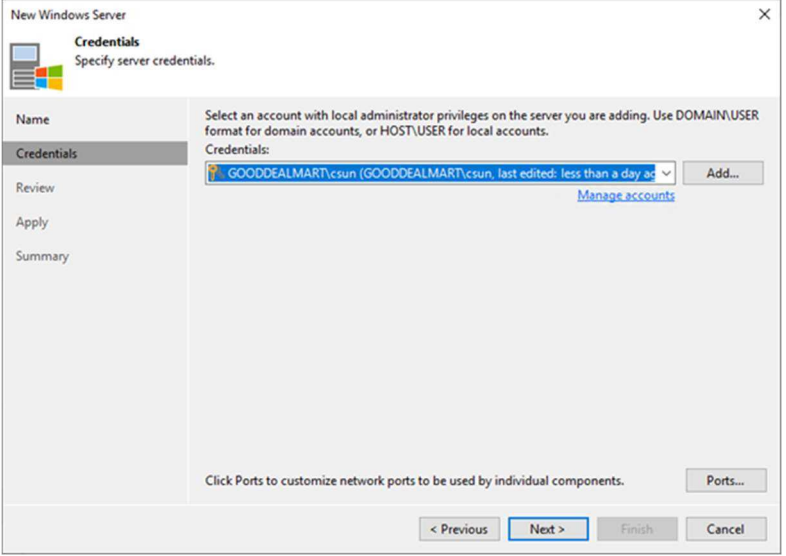
The screenshot shows the 'New Windows Server' wizard at the 'Credentials' step. The left sidebar has 'Credentials' selected, with 'Name', 'Review', 'Apply', and 'Summary' below it. The main area has a title 'Credentials' and a subtitle 'Specify server credentials.' Below this is a text box labeled 'Credentials:' with a dropdown menu showing 'Select existing credentials or add new' and an 'Add...' button to its right. A link 'Manage accounts' is below the dropdown. At the bottom, there is a section 'Click Ports to customize network ports to be used by individual components.' with a 'Ports...' button. At the very bottom are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

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.



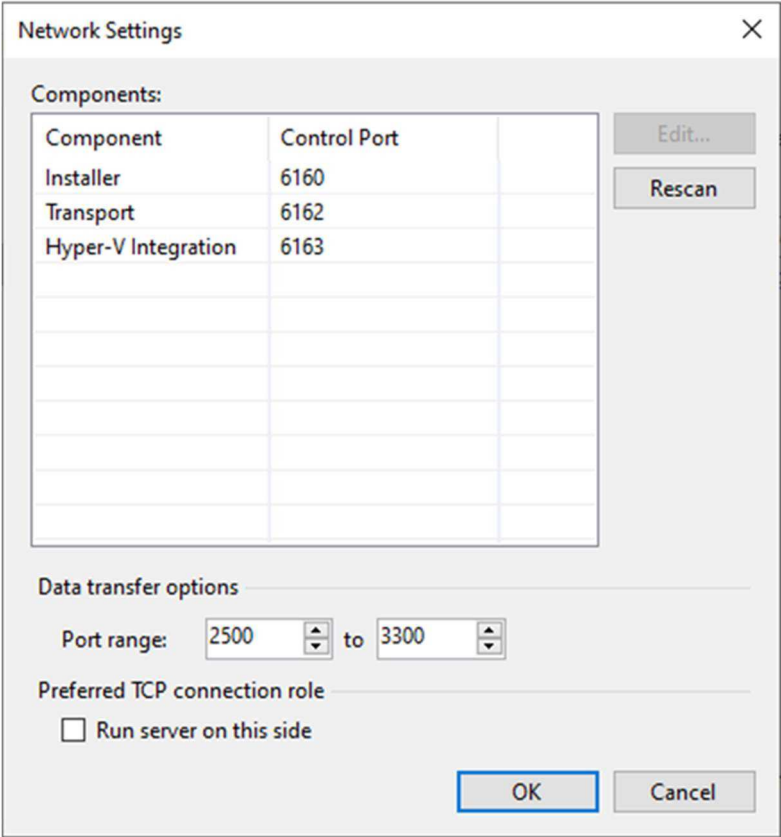
The 'Credentials' dialog box is shown. It has a title bar with 'Credentials' and a close button. Inside, there is a 'Username' field with the text 'GOODDEALMART\csun' and a 'Browse...' button to its right. Below it is a 'Password' field with masked characters and a toggle icon. A 'Description' text area contains the text 'GOODDEALMART\csun'. At the bottom are 'OK' and 'Cancel' buttons.

13. On the Credentials page, click Ports.

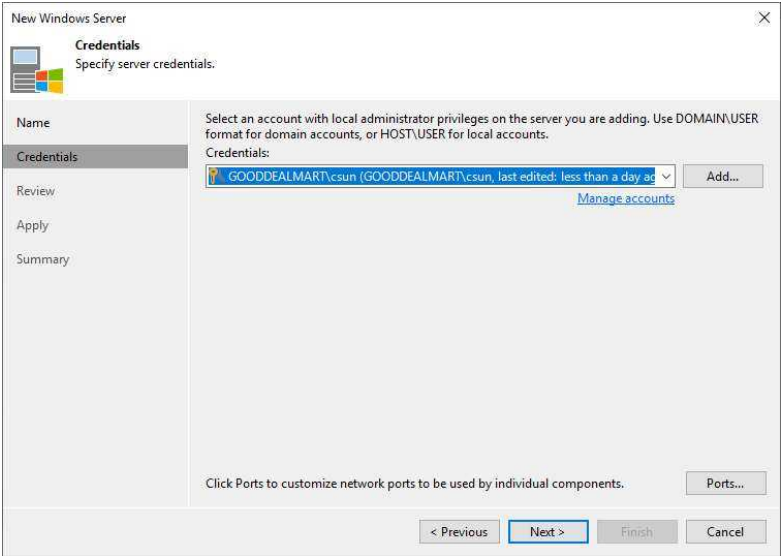


The 'New Windows Server' wizard is shown, specifically the 'Credentials' page. The title bar says 'New Windows Server' and 'Credentials'. The subtitle is 'Specify server credentials.' On the left is a navigation pane with 'Name', 'Credentials', 'Review', 'Apply', and 'Summary'. The main area has instructions: '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.' Below this, it says 'Credentials:' followed by a dropdown menu showing 'GOODDEALMART\csun (GOODDEALMART\csun, last edited: less than a day ago)' and an 'Add...' button. A link 'Manage accounts' is also present. At the bottom, there is a 'Ports...' button and a note: 'Click Ports to customize network ports to be used by individual components.' Navigation buttons at the very bottom are '< Previous', 'Next >', 'Finish', and 'Cancel'.

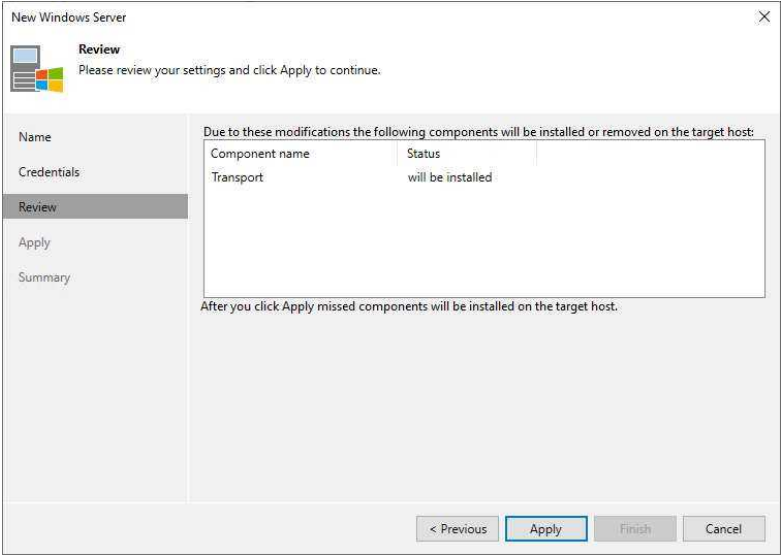
- 14. If necessary, change the network ports used by Veeam Backup & Replica on components on the Network Settings page.
- 15. Configure connection settings for file copy operations in the Network Settings window's Data transfer options section. Provide a set of ports for transmission channels between 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 initialization may be disrupted.
- 17. Click OK.



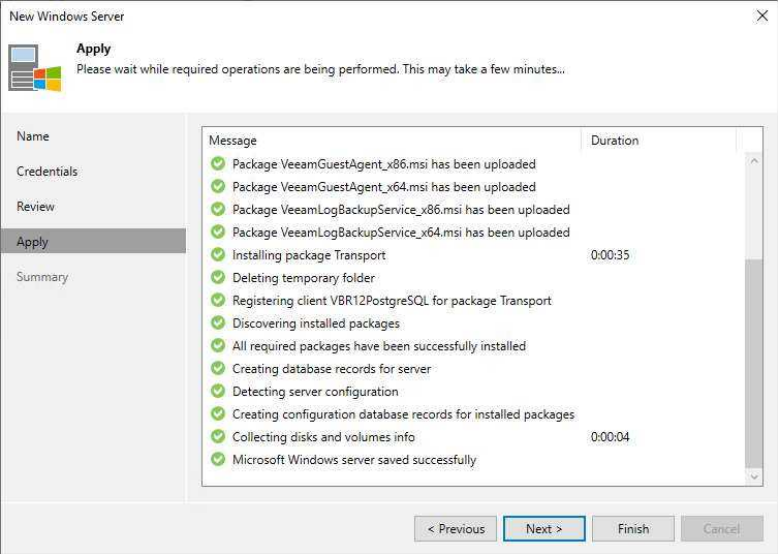
18. On the Credentials page, click Next.



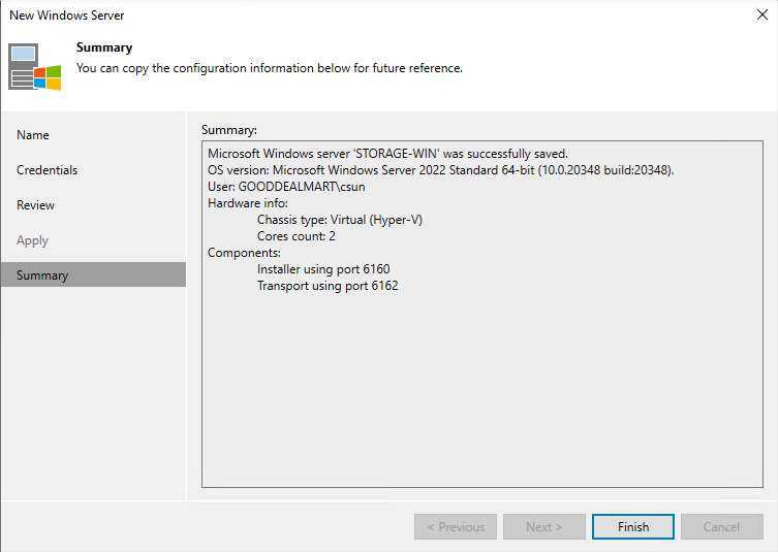
19. On the Review page, click Apply.



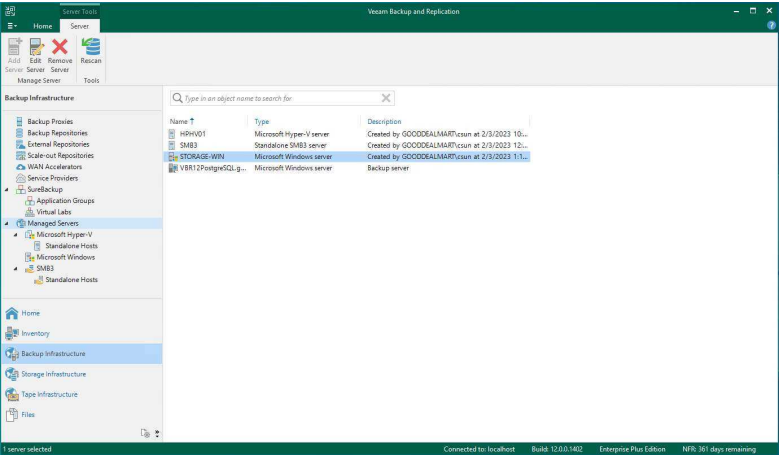
20. Click Next on the Apply page.



21. Click Finish on the Summary page.

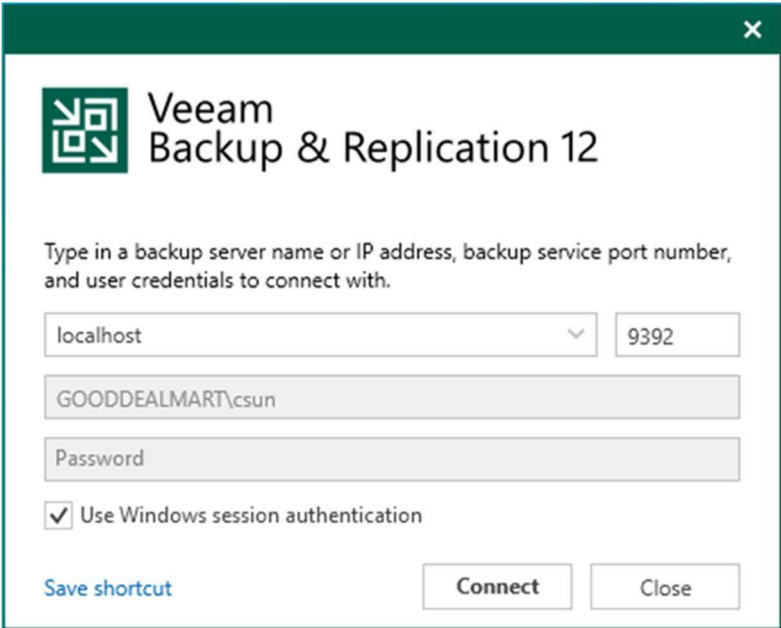


22. Ensure the new Microsoft Windows server is added.

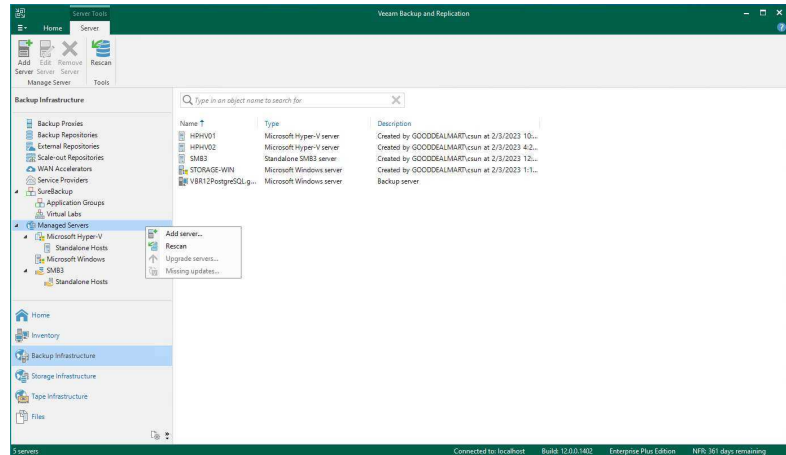


Add Linux Server for a hardened repository

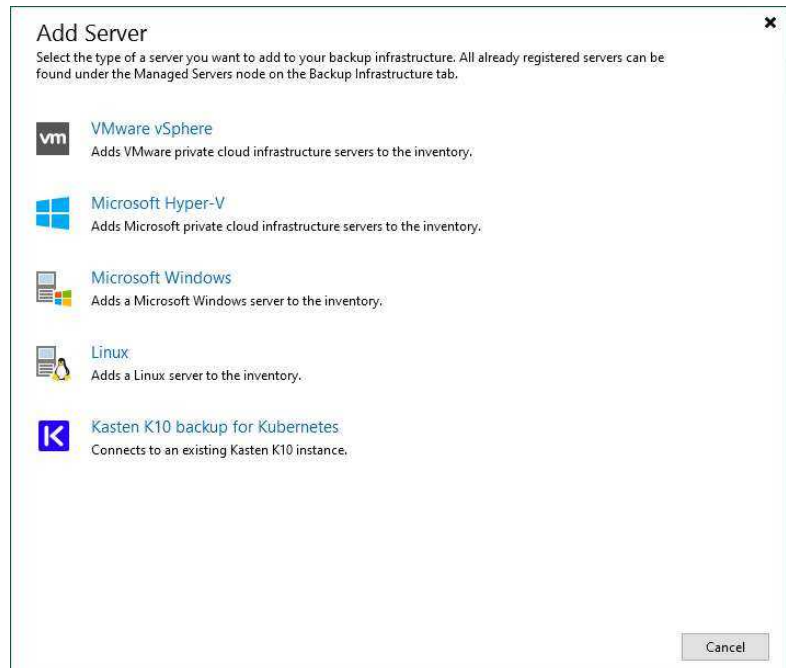
Suppose you plan to use backup infrastructure components and servers that you plan to use for various types of restore operations. In that case, you must add the Linux servers to the backup infrastructure.

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.	 A screenshot of the Veeam Backup & Replication 12 console window. The window has a dark green title bar with a close button (X) in the top right corner. The main content area has a white background. At the top left is the Veeam logo, followed by the text "Veeam Backup & Replication 12". Below this is a prompt: "Type in a backup server name or IP address, backup service port number, and user credentials to connect with." There are four input fields: a dropdown menu showing "localhost", a text box containing "9392", a text box containing "GOODDEALMART\csun", and a text box containing "Password". Below these fields is a checkbox labeled "Use Windows session authentication" which is checked. At the bottom left is a blue link "Save shortcut". At the bottom right are two buttons: "Connect" and "Close".

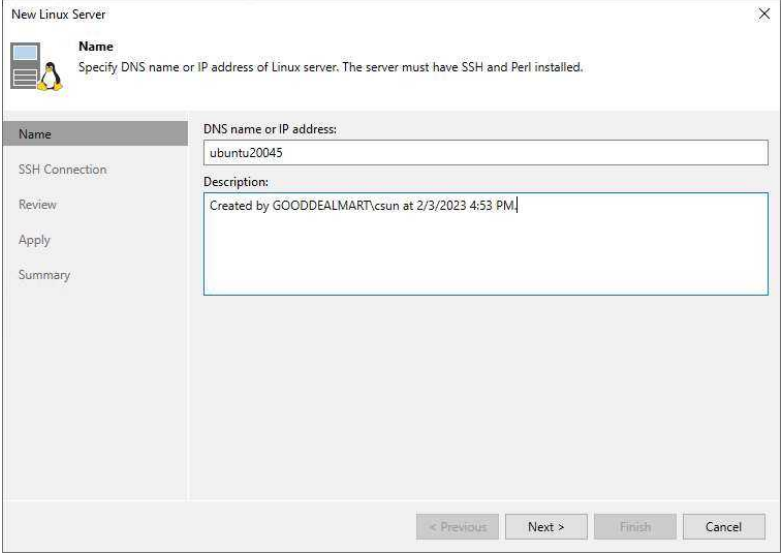
3. On the Home page, select Backup Infrastructure.
4. On the Backup Infrastructure page, select Managed Servers.
5. Right-click Managed Servers and select Add Server.



6. Select Linux on the Add Server page.



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.

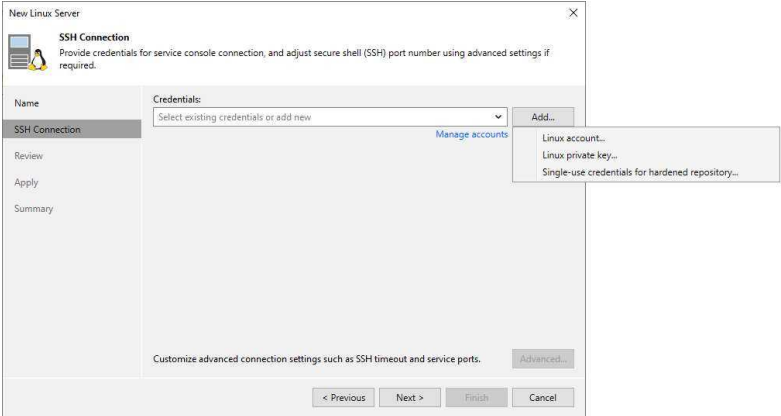


The screenshot shows the 'New Linux Server' dialog box with the 'Name' tab selected. The 'DNS name or IP address' field contains 'ubuntu20045'. The 'Description' field contains 'Created by GOODDEALMART\csun at 2/3/2023 4:53 PM'. The left sidebar shows 'Name', 'SSH Connection', 'Review', 'Apply', and 'Summary'. The bottom has buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

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

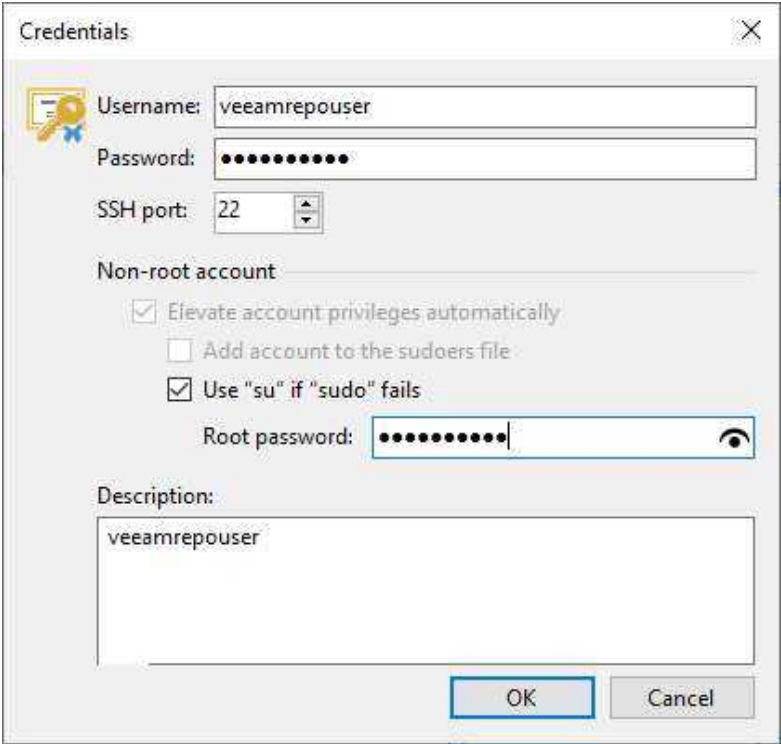
Note:

These credentials are not saved by Veeam Backup & Replica. 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.

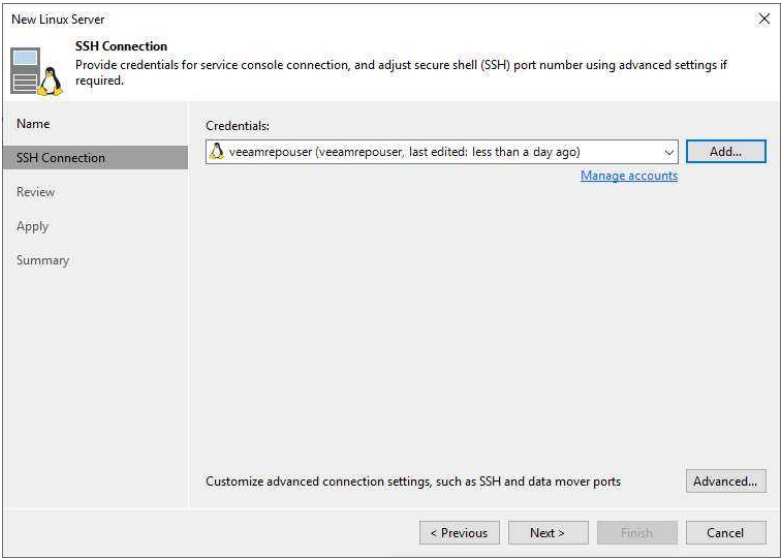


The screenshot shows the 'New Linux Server' dialog box with the 'SSH Connection' tab selected. The 'Credentials' dropdown menu is open, showing options: 'Linux account...', 'Linux private key...', and 'Single-use credentials for hardened repository...'. The 'Add...' button is visible. The left sidebar shows 'Name', 'SSH Connection', 'Review', 'Apply', and 'Summary'. The bottom has buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

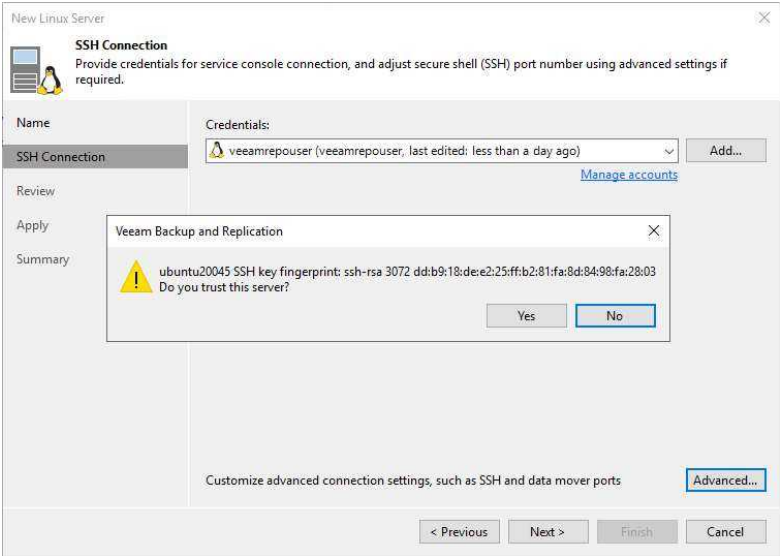
- 10. On the Credentials page, Enter a username
- 11. Enter a user name in the Username field.
- 12. Enter a password in the Password field.
- 13. Enter 22 in the SSH port field.
- 14. Give a brief description in the Description field for future reference and click OK.



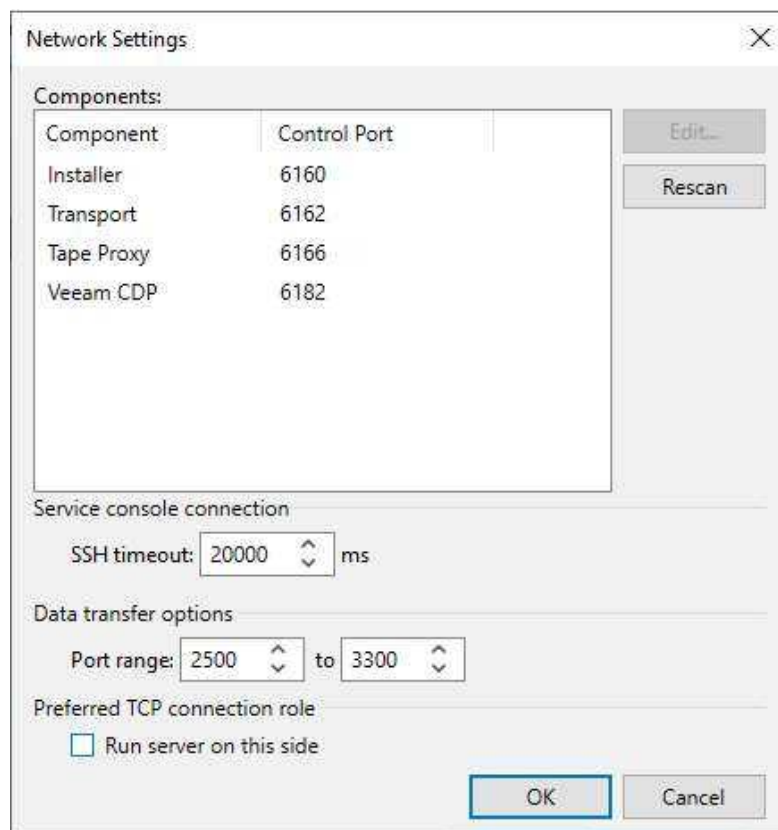
- 15. On the SSH Connection page, click Advanced.



16. Select Yes on the trust warning message page.



17. If necessary, change the network ports used by Veeam Backup & Replica on 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 initialization may be disrupted.



21. Click OK.

22. Click Next on the SSH Connection page.

The screenshot shows the 'New Linux Server' window with the 'SSH Connection' tab selected. The window title is 'New Linux Server'. Below the title bar, there's a section for 'SSH Connection' with a penguin icon and the text 'Provide credentials for service console connection, and adjust secure shell (SSH) port number using advanced settings if required...'. On the left, there's a sidebar with 'Name', 'SSH Connection', 'Review', 'Apply', and 'Summary'. The 'SSH Connection' tab is active. The main area shows 'Credentials:' with a dropdown menu showing 'veeamrepouser (veeamrepouser, last edited: less than a day ago)' and an 'Add...' button. Below this is a link 'Manage accounts'. At the bottom, there's a text 'Customize advanced connection settings such as SSH timeout and service ports.' and an 'Advanced...' button. The bottom navigation bar has '< Previous', 'Next >', 'Finish', and 'Cancel' buttons.

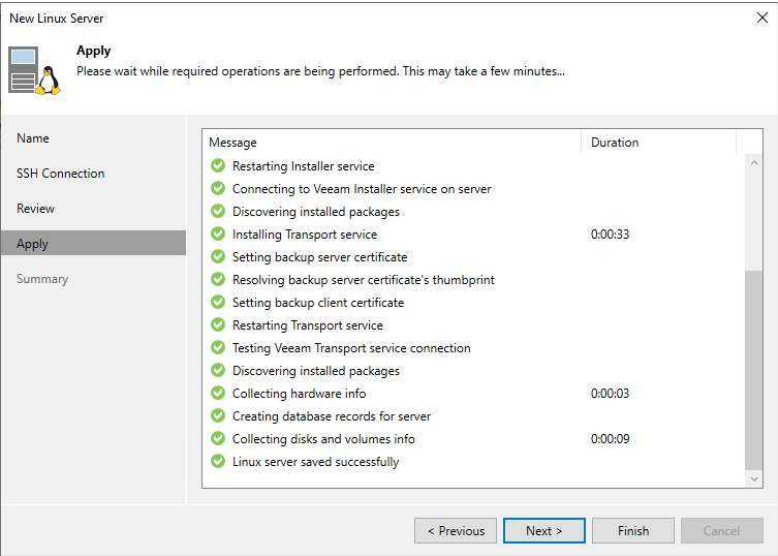
23. Click Apply on the Review page.

The screenshot shows the 'New Linux Server' window with the 'Review' tab selected. The window title is 'New Linux Server'. Below the title bar, there's a section for 'Review' with a penguin icon and the text 'Please review your settings and click Apply to continue.'. On the left, there's a sidebar with 'Name', 'SSH Connection', 'Review', 'Apply', and 'Summary'. The 'Review' tab is active. The main area shows a table with the following content:

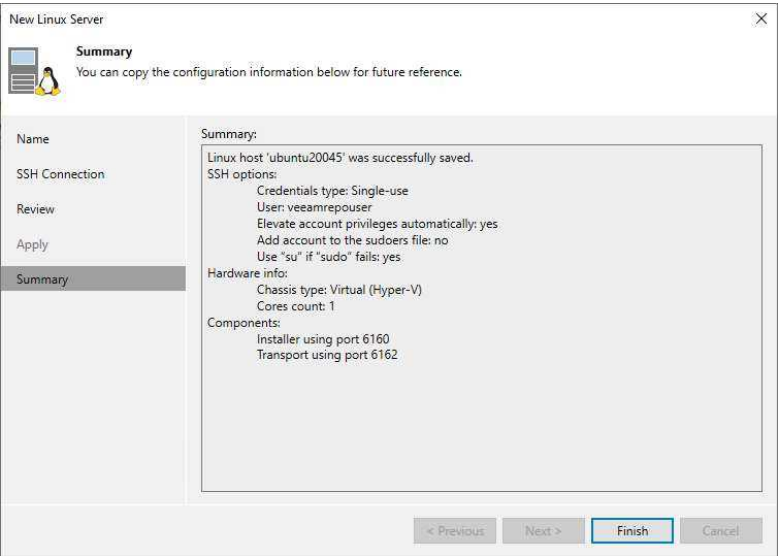
Due to these modifications the following components will be installed or removed on the target host:	
Component name	Status
Installer	will be installed
Transport	will be installed

Below the table, there's a text 'After you click Apply missed components will be installed on the target host.'. The bottom navigation bar has '< Previous', 'Apply', 'Finish', and 'Cancel' buttons.

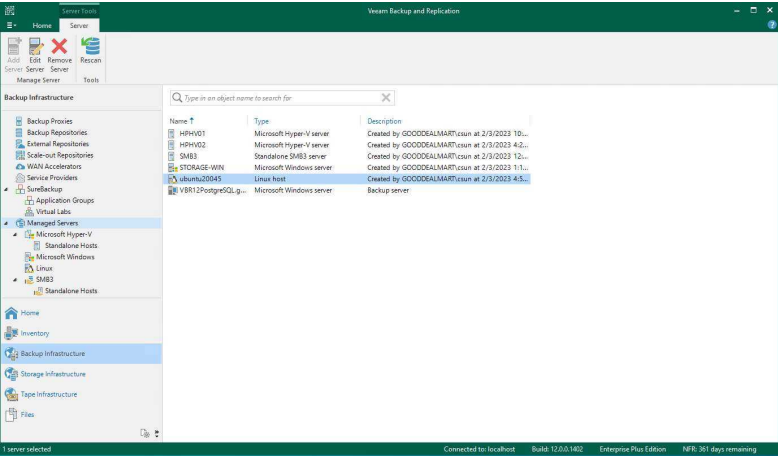
24. Click Next on the Apply page.



25. Click Finish on the Summary page.

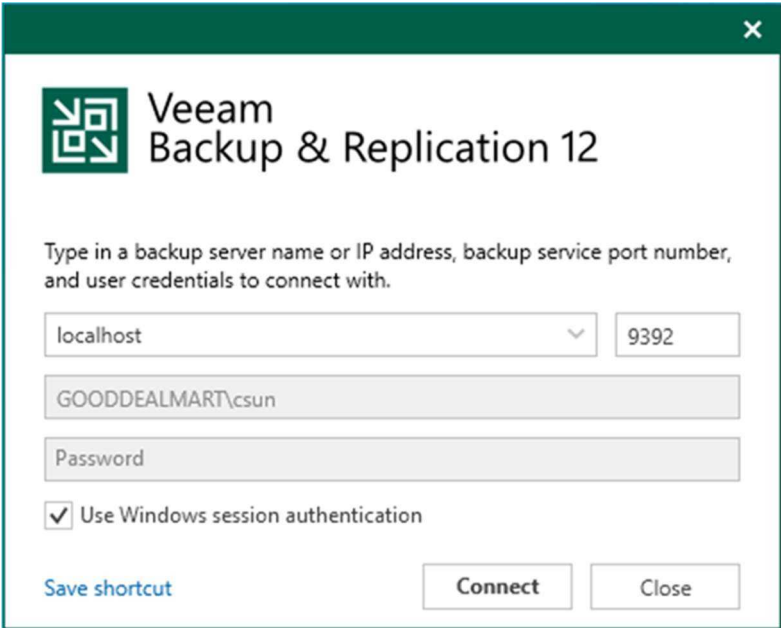


26. Ensure the new Linux server is added.

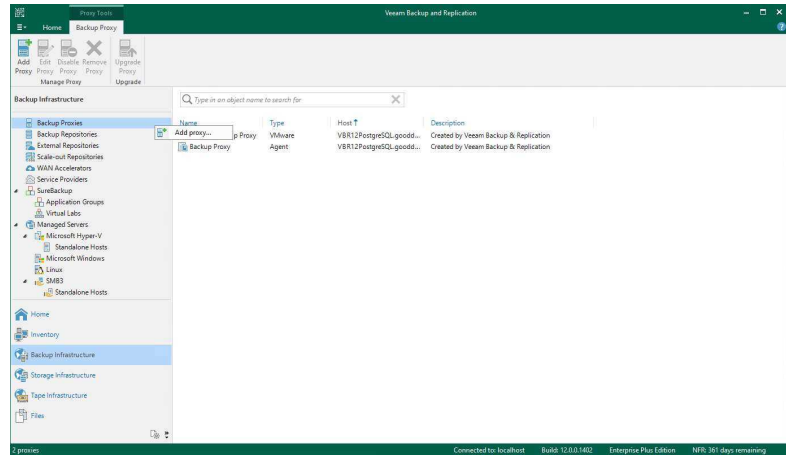


Add Off-Host Backup proxy servers

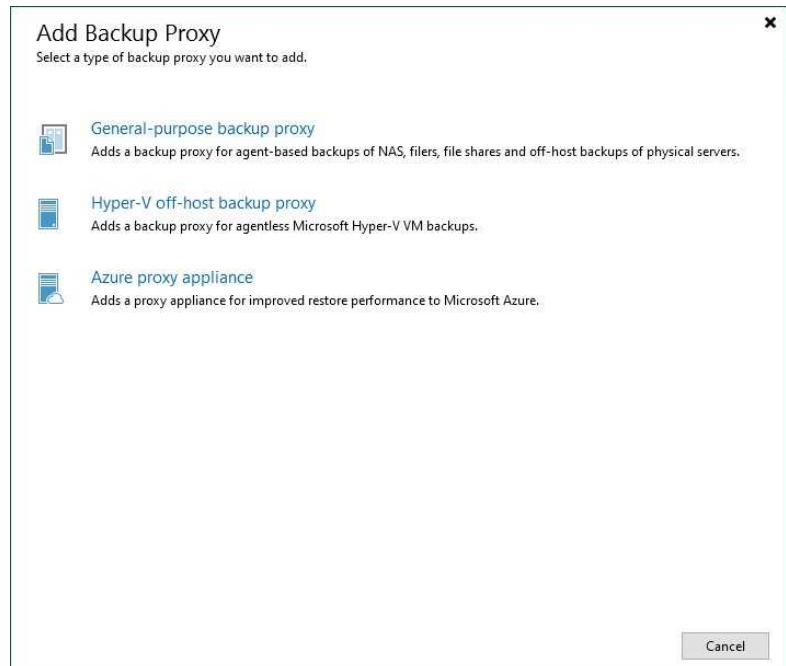
Off-Host Backup proxy servers will retrieve VM data from the source datastore, process it and transfer it to the destination. The off-host backup proxy removes unwanted overhead on the production Hyper-V host.

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.	 A screenshot of the Veeam Backup & Replication 12 console window. The window has a dark green title bar with a close button (X) in the top right corner. The main area is white and contains the Veeam logo (a green square with a white geometric pattern) and the text "Veeam Backup & Replication 12". Below this, there is a prompt: "Type in a backup server name or IP address, backup service port number, and user credentials to connect with." There are four input fields: a dropdown menu with "localhost" selected, a text box with "9392", a text box with "GOODDEALMART\csun", and a text box with "Password". Below these fields is a checkbox labeled "Use Windows session authentication" which is checked. At the bottom left is a blue link "Save shortcut". At the bottom right are two buttons: "Connect" and "Close".

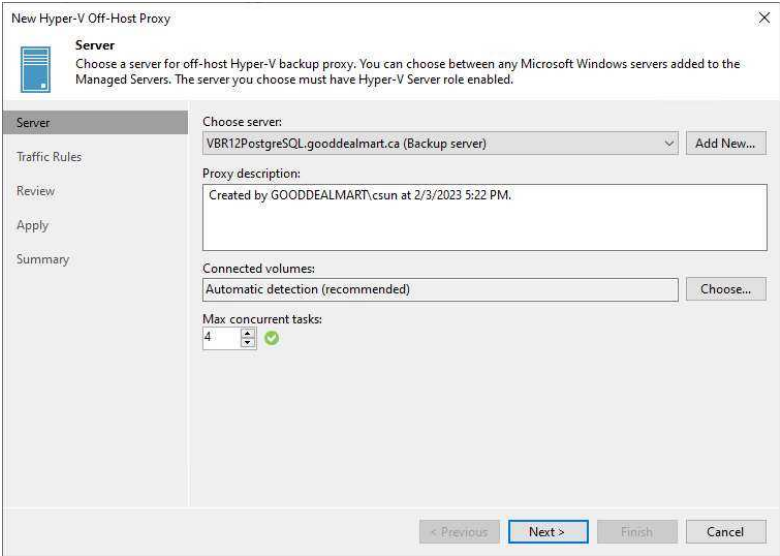
3. On the Home page, select Backup Infrastructure.
4. On the Backup Infrastructure page, select Backup Proxies.
5. Right-click Backup Proxies and select Add Proxies.



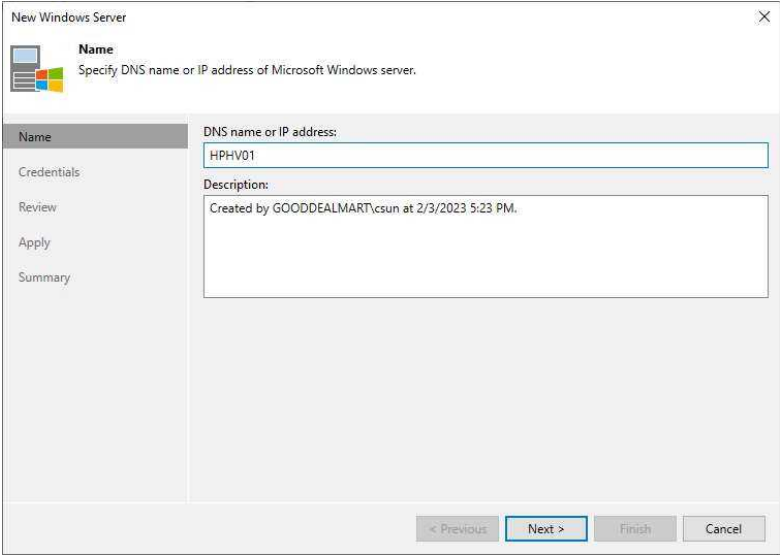
6. Select Hyper-V off-host backup proxy on the Add Backup Proxy page.



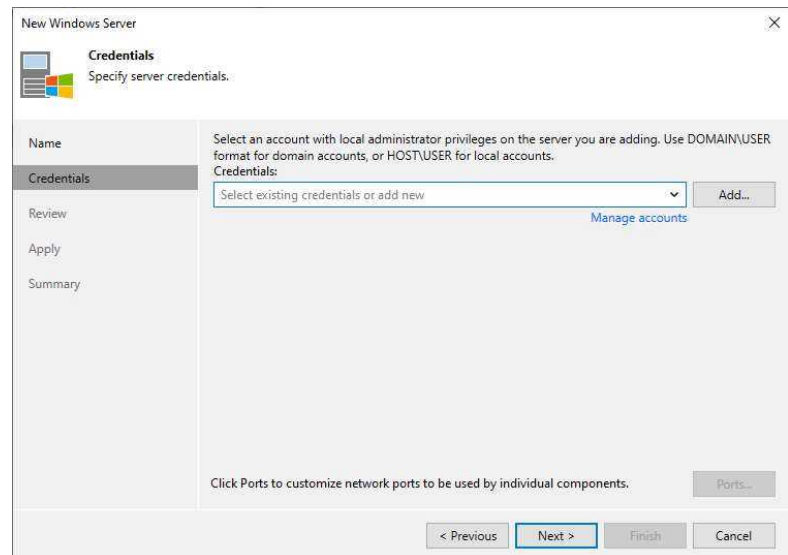
- 7. Click Add New in the Choose server field on the Server page.



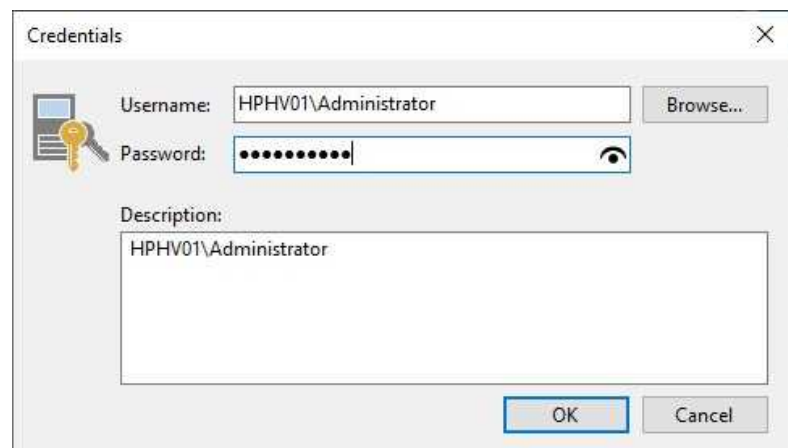
- 8. Enter the Microsoft Windows server's full DNS name or IP address on the Name page.
- 9. Give a brief description in the Description field for future reference and click Next.



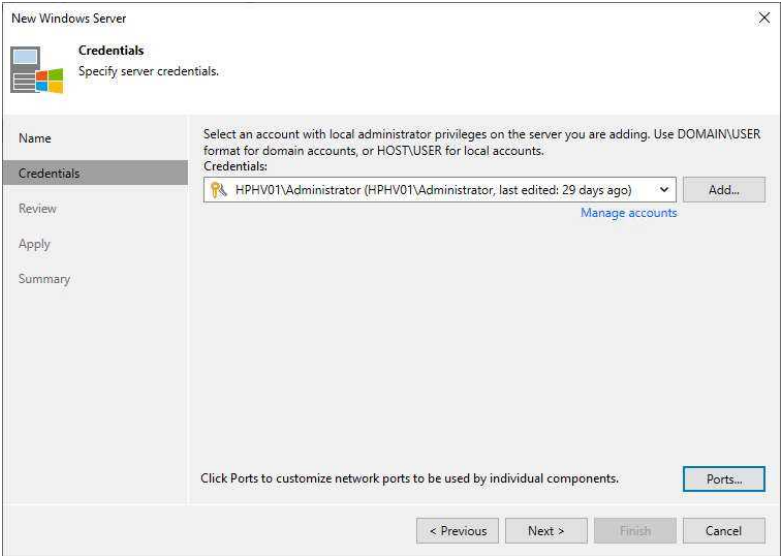
10. Select an account from the Credentials drop-down list on the Credentials page or click Add on the right to add the credentials.



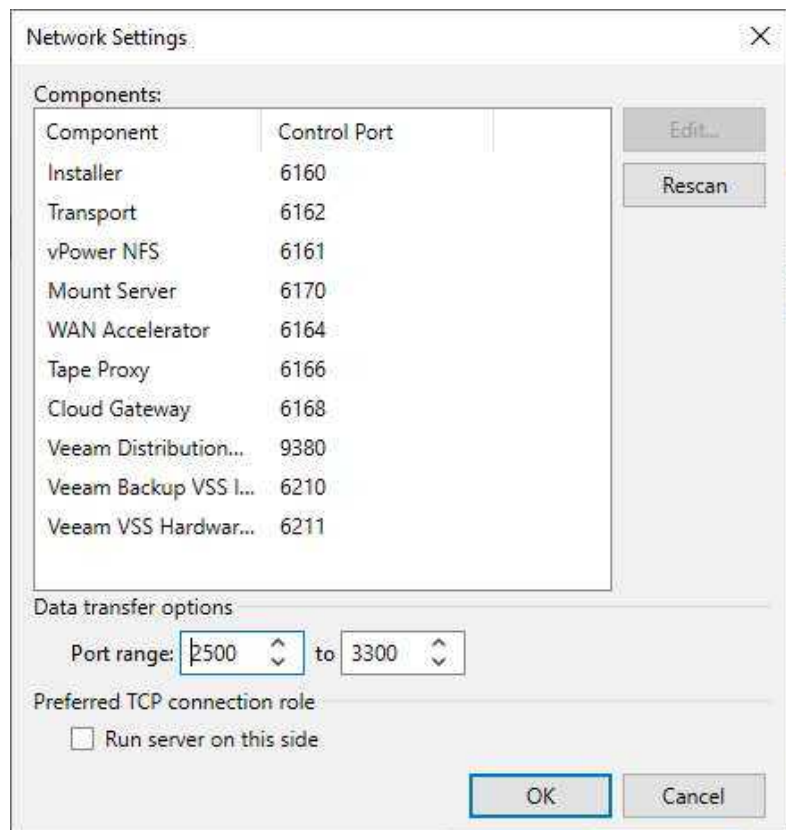
11. On the Credentials page, enter a user name in the Username field. You also can click Browse to select an existing user account.
12. Enter the password in the Password field.
13. Give a brief description in the Description field for future reference and click OK.



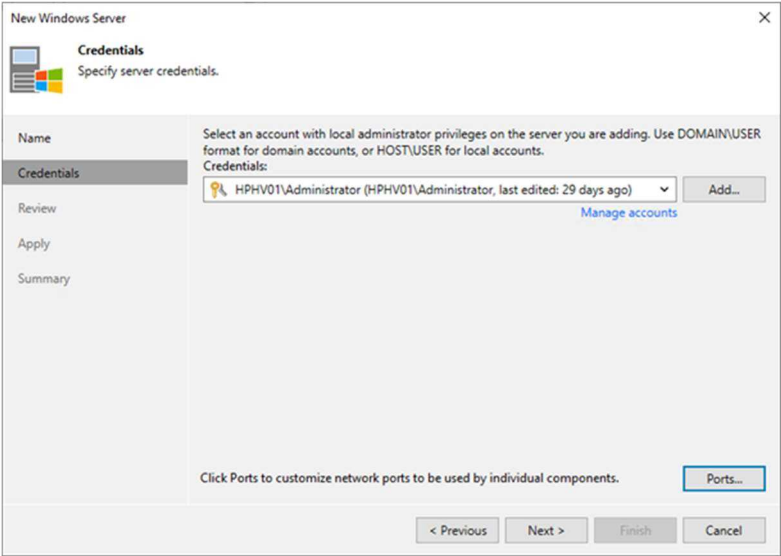
14. On the Credentials page, click Ports.



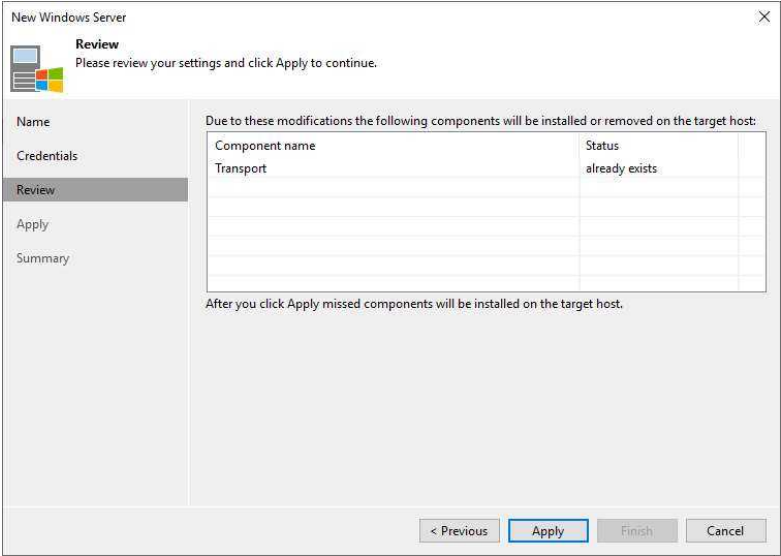
15. If necessary, change the network ports used by Veeam Backup & Replica on components on the Network Settings page.
16. Configure connection settings for file copy operations in the Network Settings window's Data transfer options section. Provide a set of ports for transmission channels between the 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 initialization may be disrupted.
18. Click OK.



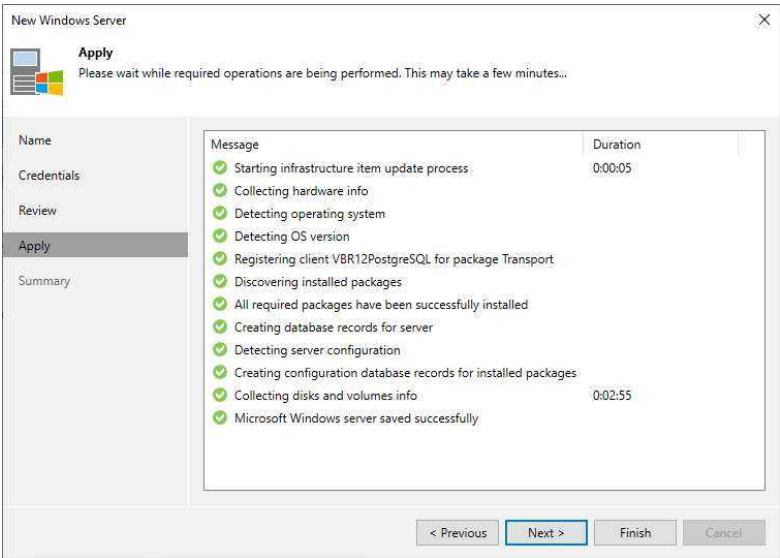
19. Click Next on the Credentials page.



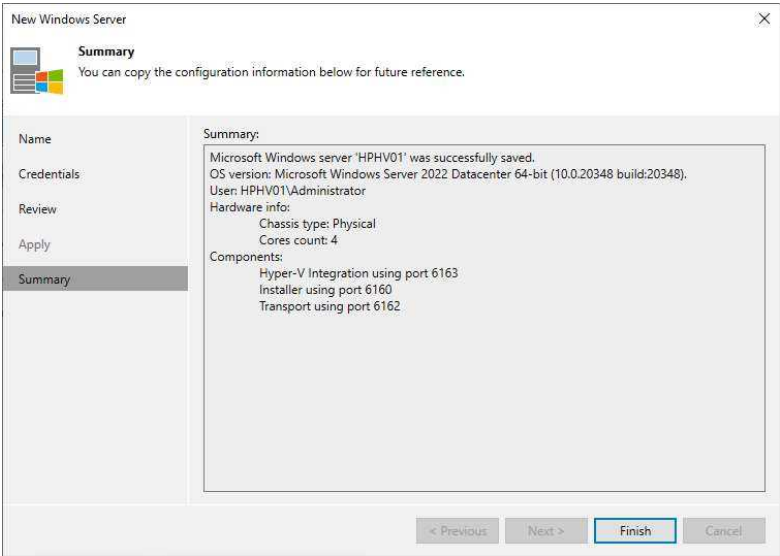
20. Click Apply on the Review page.



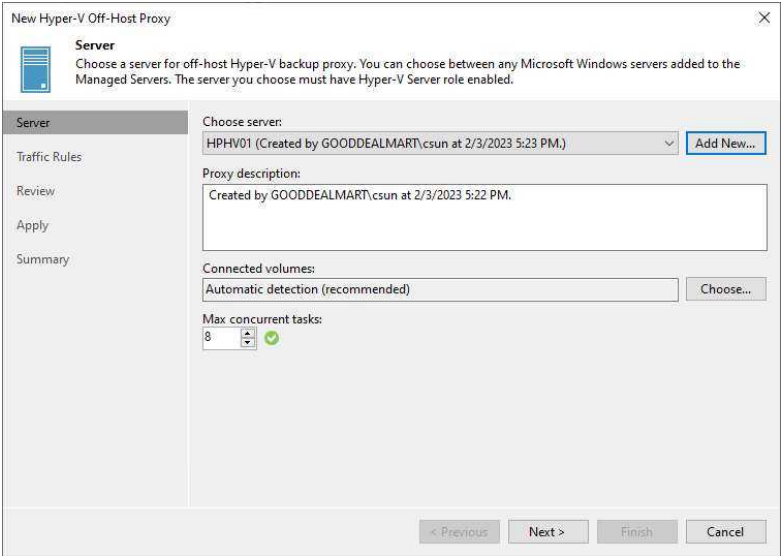
21. On the Apply page, click Next.



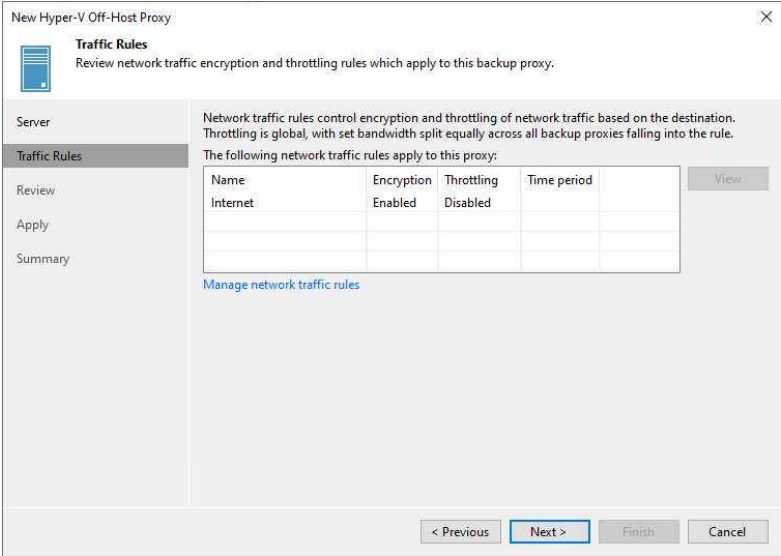
22. Click Finish on the Summary page.



- 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.



- 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.



29. Click Apply on the Review page.

New Hyper-V Off-Host Proxy

Review
Please review the settings and click Apply to continue.

Server

Traffic Rules

Review

Apply

Summary

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

< Previous Apply Finish Cancel

30. Click Next on the Apply page.

New Hyper-V Off-Host Proxy

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

Server

Traffic Rules

Review

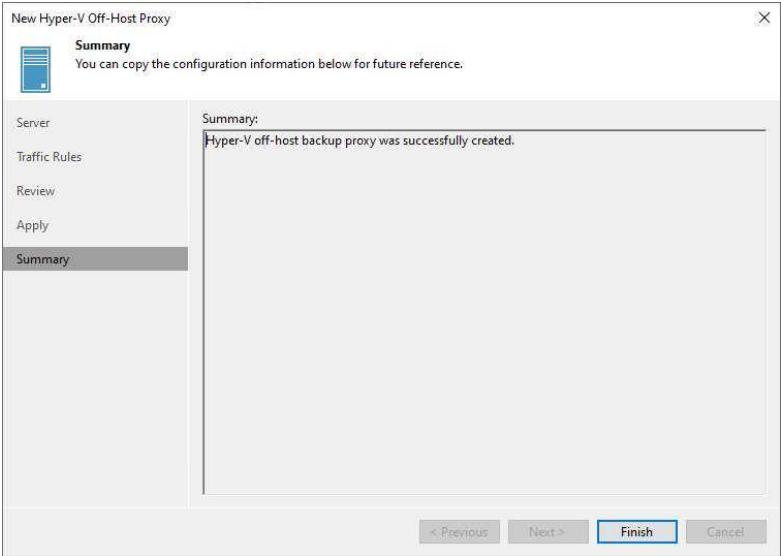
Apply

Summary

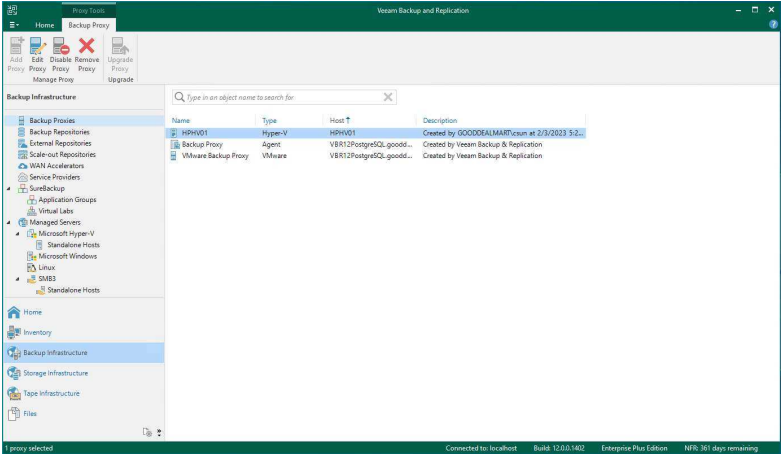
Message	Duration
✓ Starting infrastructure item update process	0:00:05
✓ Registering client VBR12PostgreSQL for package Transport	
✓ Registering client VBR12PostgreSQL for package Hyper-V Integration	
✓ Discovering installed packages	
✓ All required packages have been successfully installed	
✓ Creating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

< Previous Next > Finish Cancel

31. Click Finish on the Summary page.



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

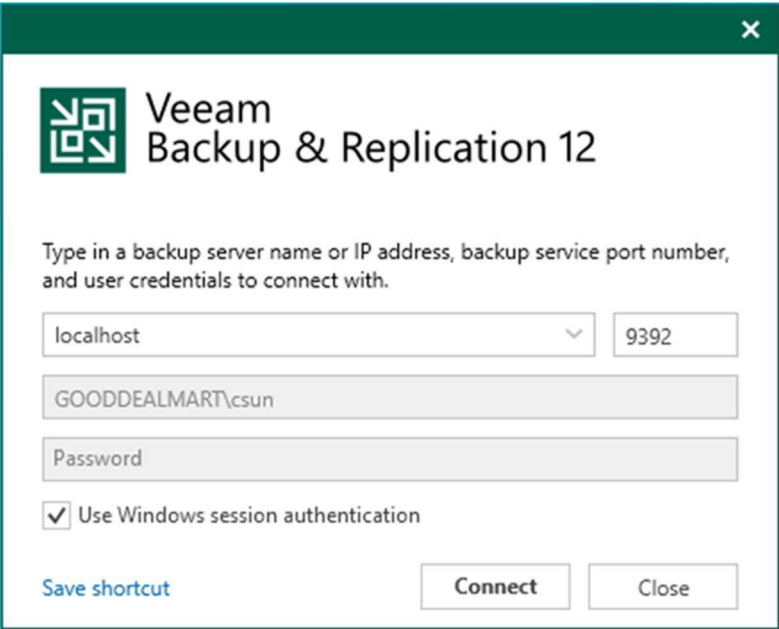


Add WAN Acceleration

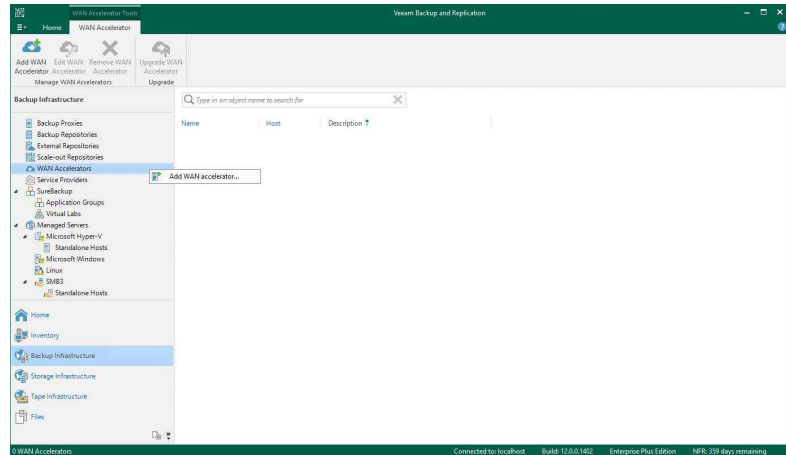
Veeam's WAN acceleration technology optimizes data transfer to remote locations. It is explicitly designed for off-site backup copy and replication jobs. You must deploy a pair of WAN accelerators in your backup infrastructure to enable WAN acceleration and data deduplication technologies.

Note:

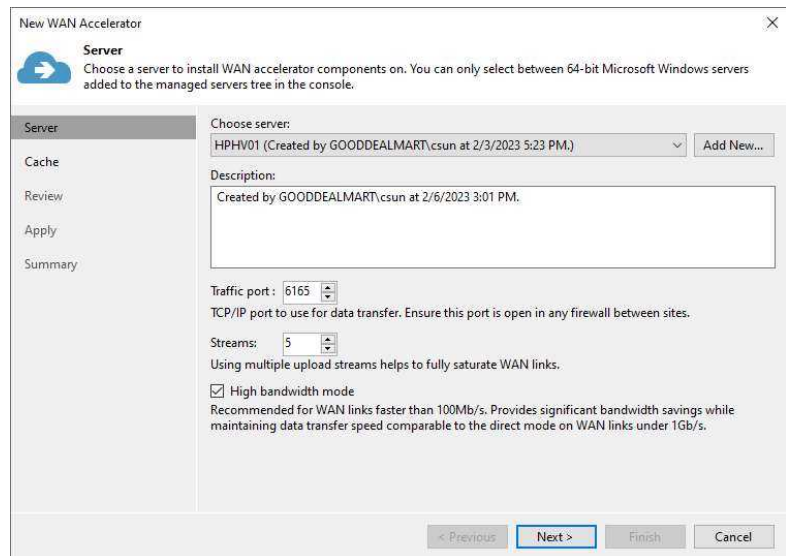
The Veeam Universal License includes WAN acceleration. Veeam Backup & Replication Enterprise or Enterprise Plus editions are required when using a legacy socket-based licence.

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.	

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.



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



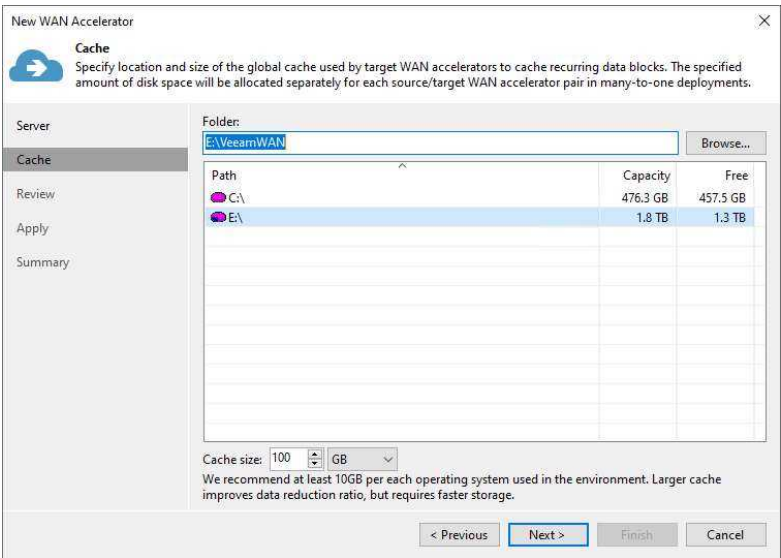
tests, multiplying the link speed by 1.5 is a good best practice for estimating the number of streams required for high latency.

- 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.

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 any me.

15. On the Review page, click Apply.

New WAN Accelerator

Review

Review the settings, and click Apply to continue.

Server

Cache

Review

Apply

Summary

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

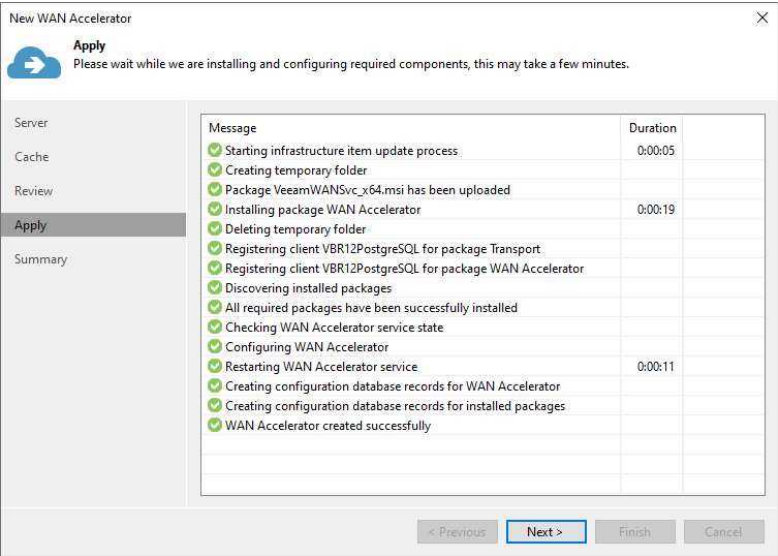
< Previous

Apply

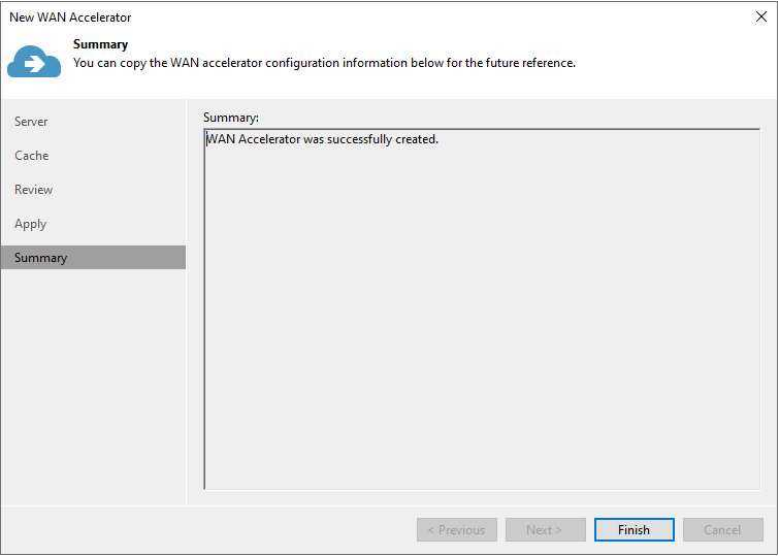
Finish

Cancel

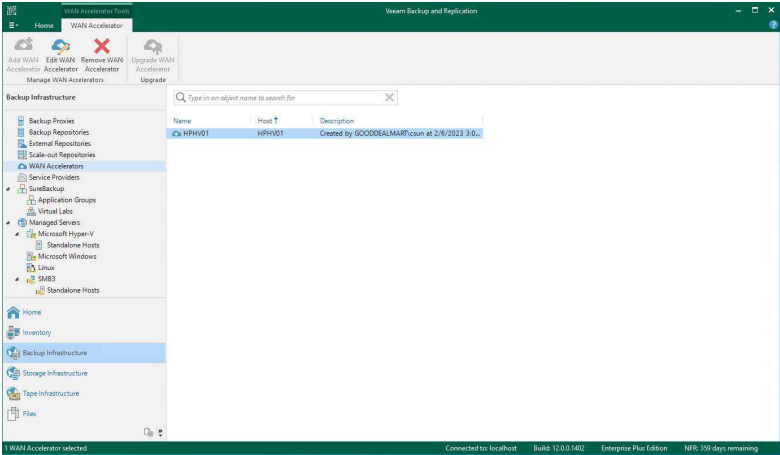
16. Click Next on the Apply page.



17. Click Finish on the Summary page.



18. Verify that the WAN Accelerator has been added.



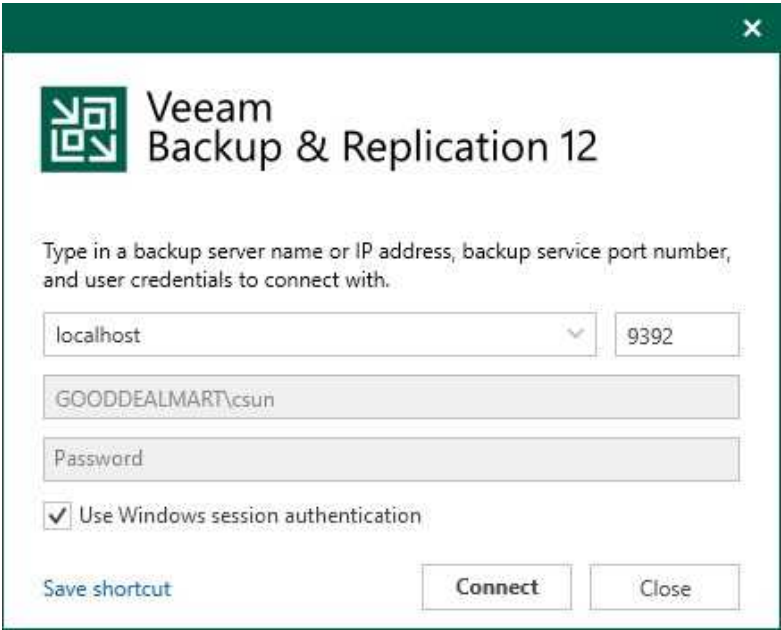
Physical Machines

Veeam Backup & Replica console 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 & Replica console. 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 & Replica console 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.

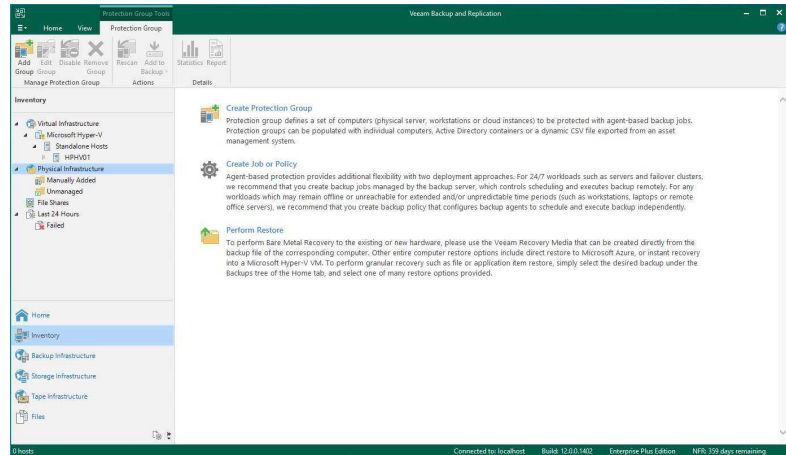
You can use protection groups to automate the Veeam Agent deployment and management on computers in the infrastructure. When you configure a protection group, you can specify scheduling options for protected computer discovery and Veeam Agent deployment. As a result, you do not need to install, configure,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

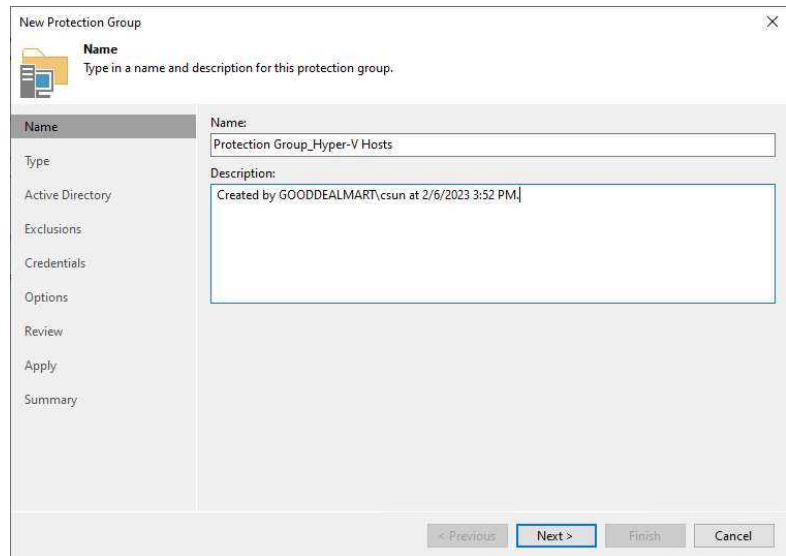
You can back up and restore the On-Premises physical machines running Windows operating systems. Backup agents are installed on each computer by Veeam Backup & Replication.

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.	 The screenshot shows the 'Veeam Backup & Replication 12' console window. It has a dark green title bar with a close button. The main area is white with the Veeam logo and title. Below the title, it says 'Type in a backup server name or IP address, backup service port number, and user credentials to connect with.' There are three input fields: a dropdown menu showing 'localhost', a text box with '9392', and a text box with 'GOODDEALMART\csun'. Below these is a 'Password' field. A checkbox labeled 'Use Windows session authentication' is checked. At the bottom, there are three buttons: 'Save shortcut', 'Connect', and 'Close'.

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

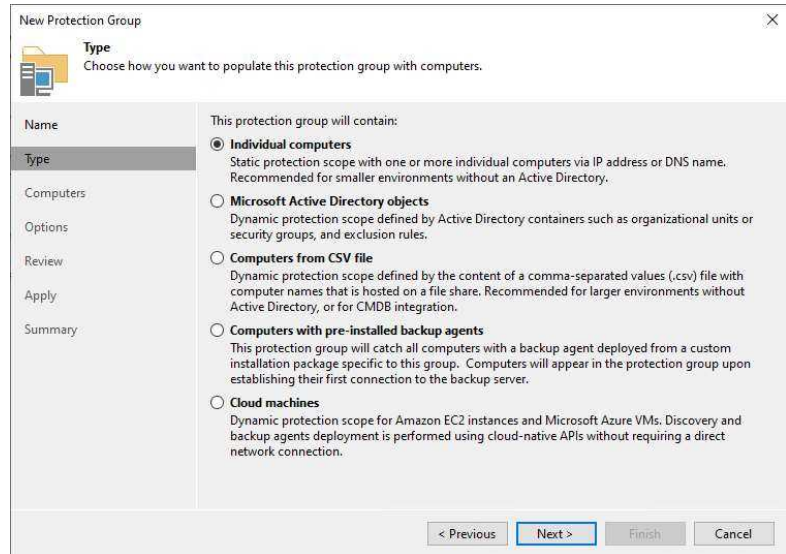


5. On the Name page, specify a protection group name.
6. Give a brief description in the Description field for future reference and click Next.



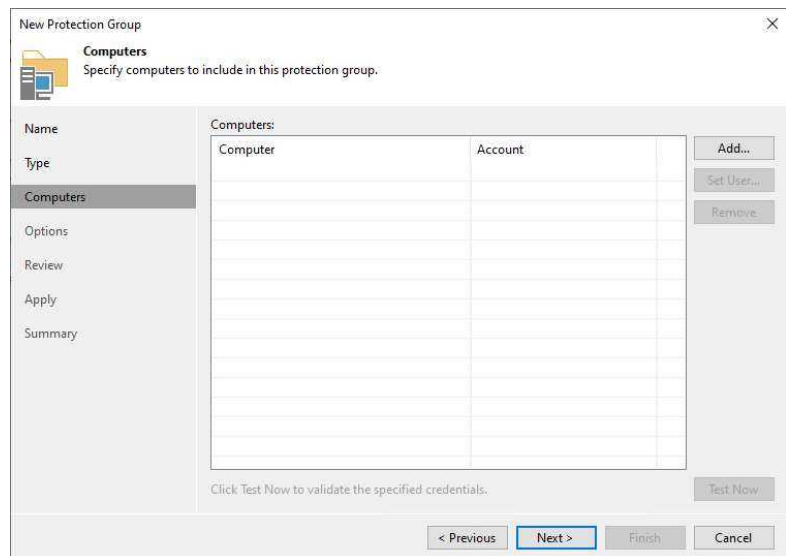
7. Select Specify protection scope for the created protection group on the Type page and click Next.

- 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 EC2 instances or

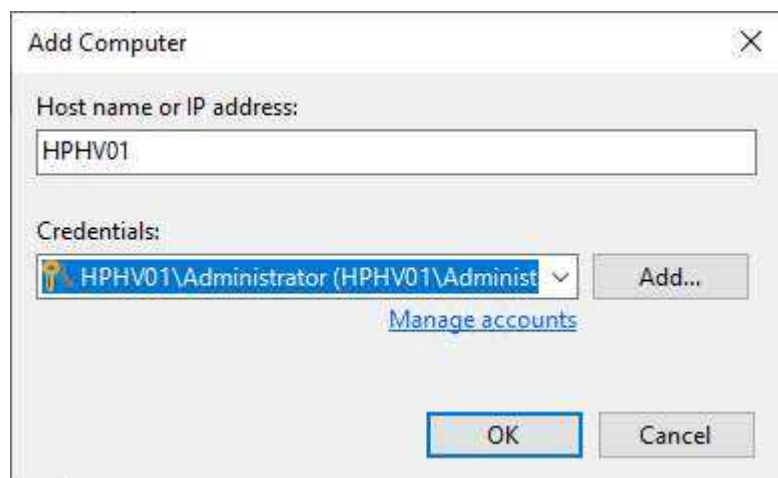


Microsoft Azure
virtual machines.

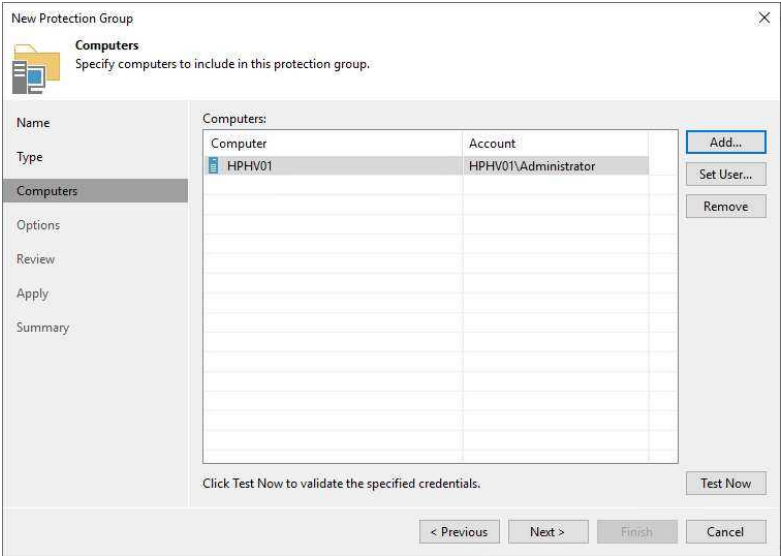
8. Click Add on the Computers page.



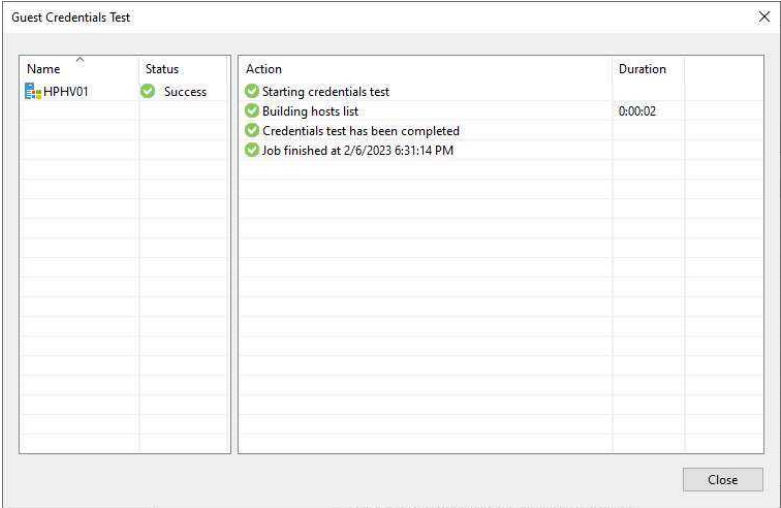
9. Specify a DNS name or IP address on the Add Computer page.
10. From the Credentials list, select a user account with administrative permissions on the computer and click OK.
11. If you need to set up credentials beforehand, click the Manage accounts link or Add on the right.



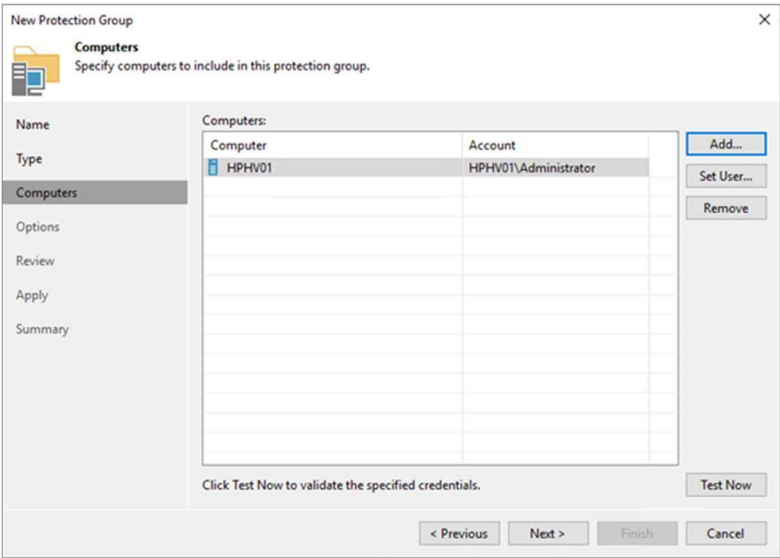
12. Click Test Now on the Computers page.



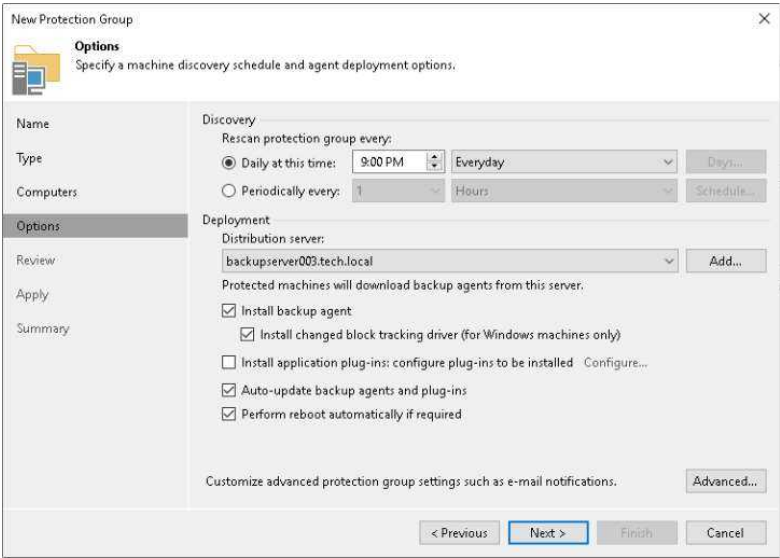
13. On the Guest Credentials Test page and click Close.



14. Click Next on the Computers page.



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

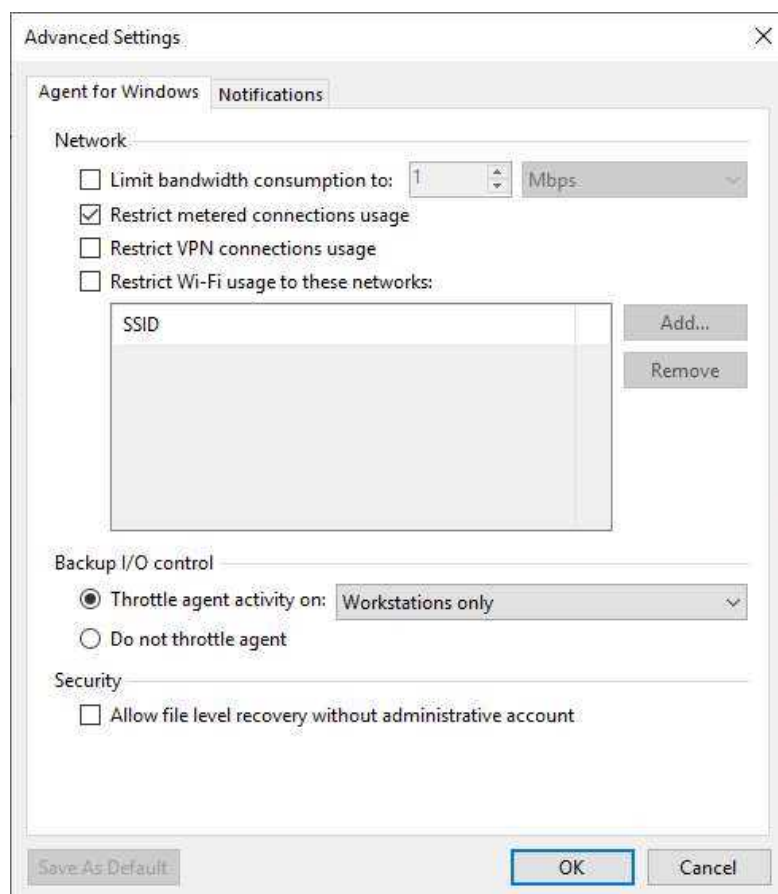


Windows machines only) checkbox.

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



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

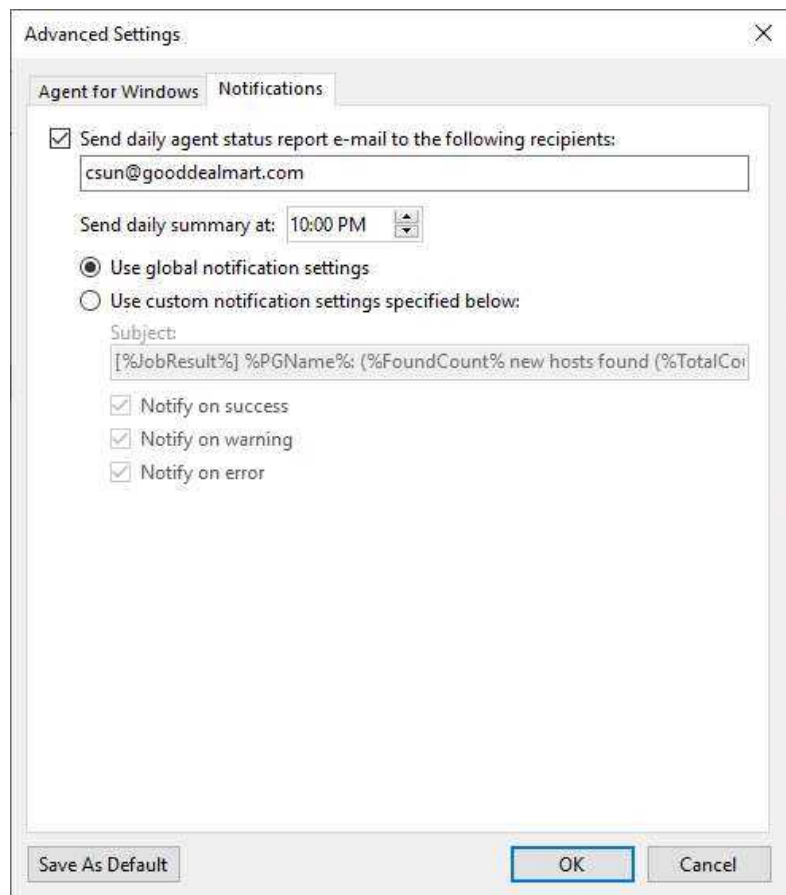
type of computers
to throttle Veeam
Agent backup
activities:
Workstations,
Servers, or All
hosts.

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 No notifications.



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.



27. On the Options page, click Next.

New Protection Group

Options
Specify host discovery schedule and automatic backup 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: 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. [Advanced](#)

< Previous Next > Finish Cancel

28. On the Review page, click Apply.

New Protection Group

Review
Review the settings, and click Apply to continue.

Name

Type

Computers

Options

Review

Apply

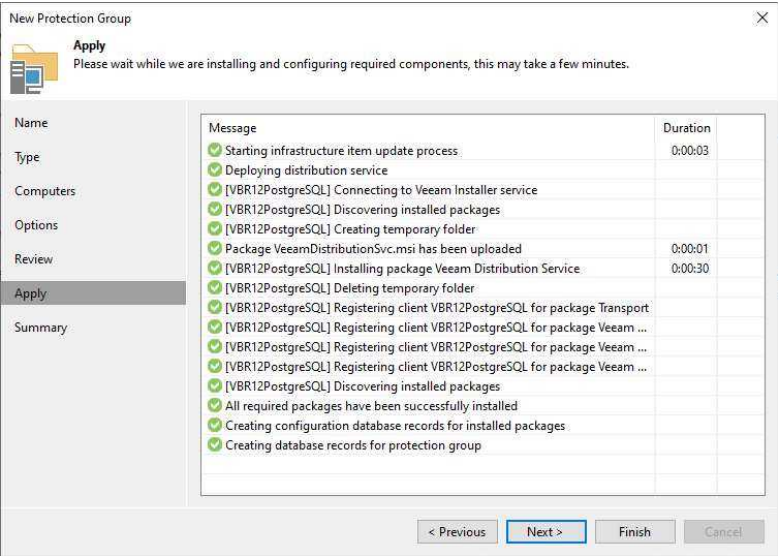
Summary

The following components will be processed on VBR12PostgreSQL.gooddealmart.ca:

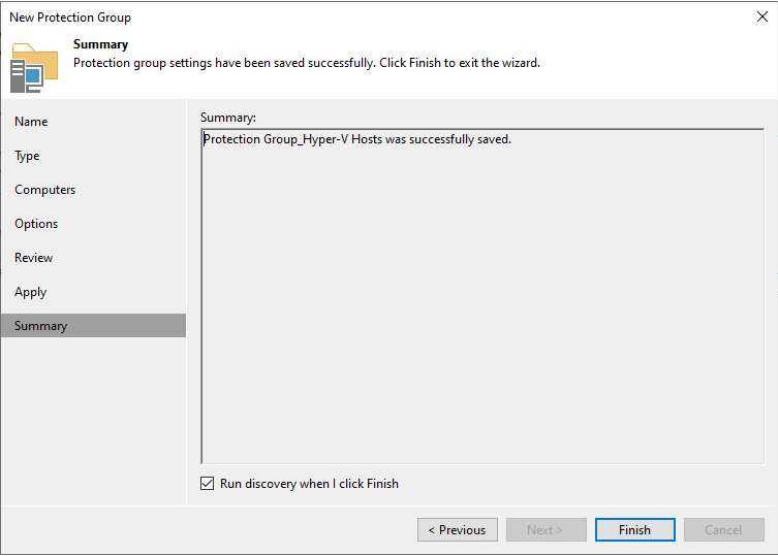
Component name	Status
Transport	already exists
Veeam Distribution Service	will be installed
Veeam Agent for Microsoft Windows Redistributable	already exists
Veeam Application Plug-ins Redistributable	already exists

< Previous **Apply** Finish Cancel

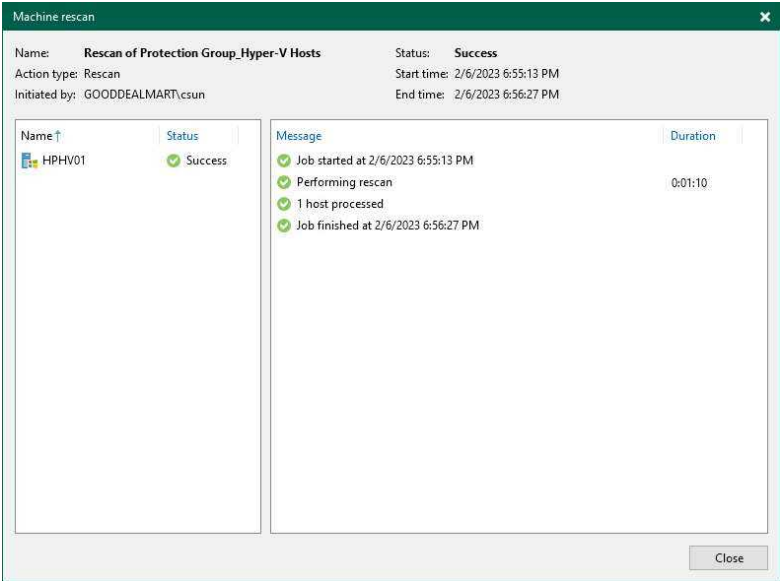
29. Click Next on the Apply page.



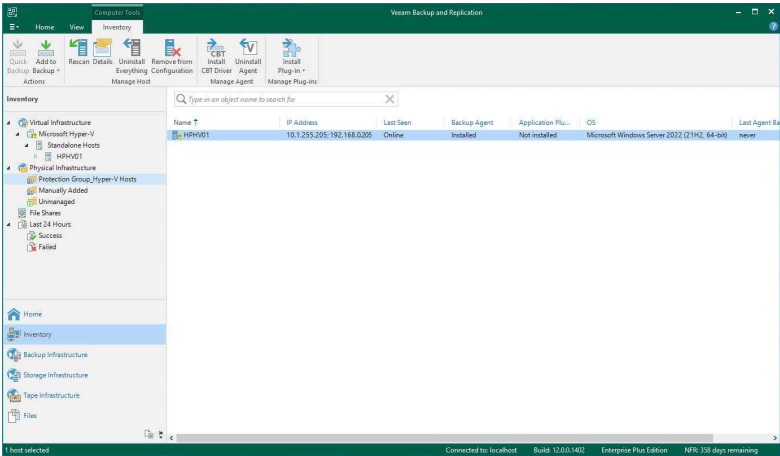
30. On the Summary page, select Run discovery when I click the Finish checkbox and click Finish.



31. Ensure the operation is complete without error on the Agents discovery session page.

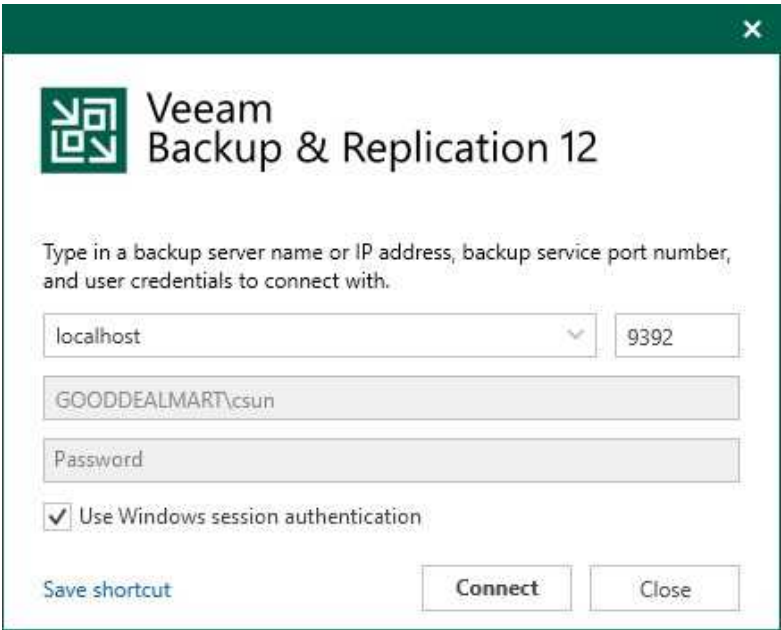
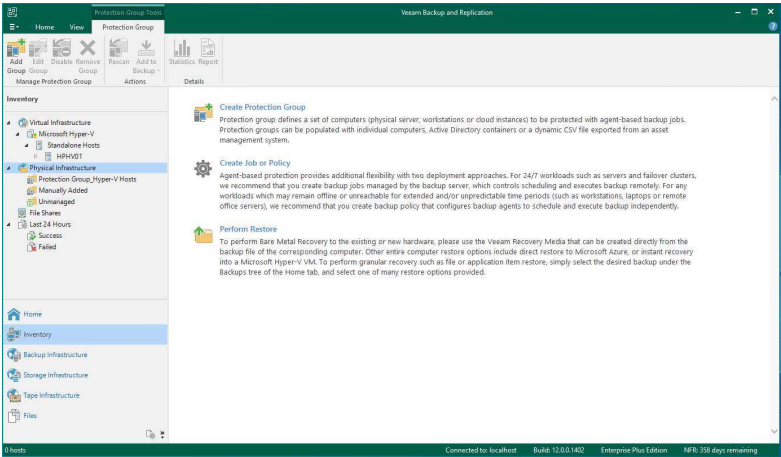


32. Verify that the protection group has been added.



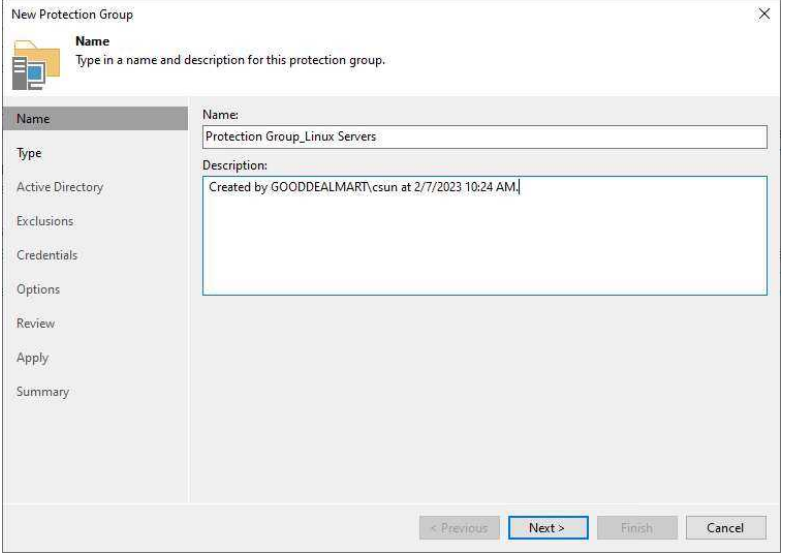
Add Veeam Agent to On-Premises Linux Physical machines

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

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



The screenshot shows the 'New Protection Group' dialog box with the 'Name' tab selected. The 'Name' field contains 'Protection Group_Linux Servers' and the 'Description' field contains 'Created by GOODDEALMART\csun at 2/7/2023 10:24 AM'. The 'Type' tab is also visible in the left sidebar. At the bottom, there are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

New Protection Group

Name
Type in a name and description for this protection group.

Name:
Protection Group_Linux Servers

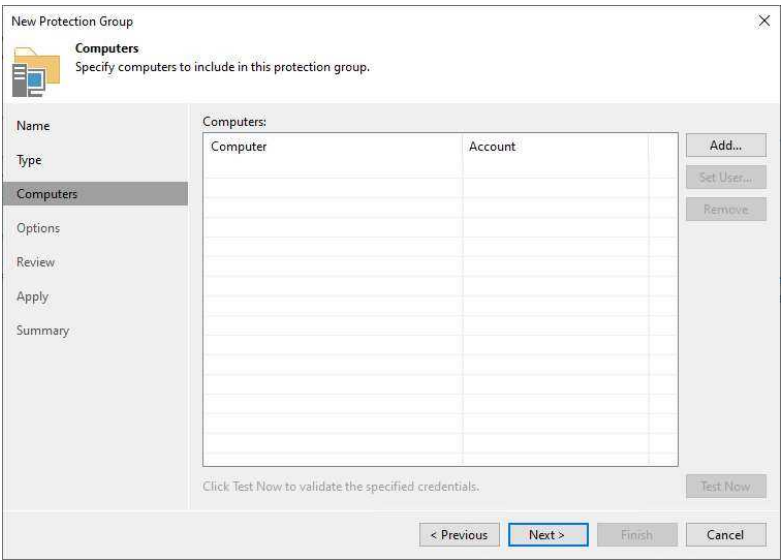
Description:
Created by GOODDEALMART\csun at 2/7/2023 10:24 AM

Type
Active Directory
Exclusions
Credentials
Options
Review
Apply
Summary

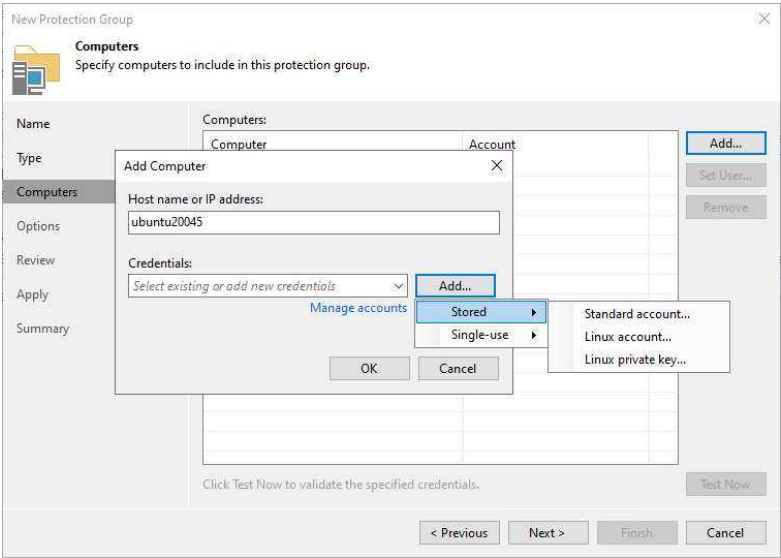
< Previous **Next >** Finish Cancel

EC2 instances or
Microsoft Azure
virtual machines.

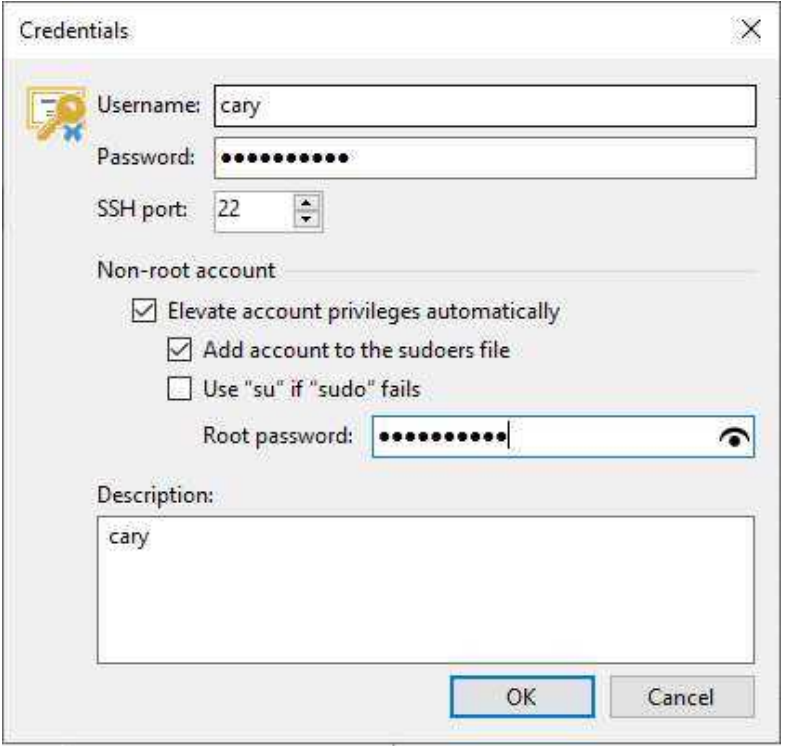
- 8. Click Add on the Computers page.



- 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.



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 Elevate 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

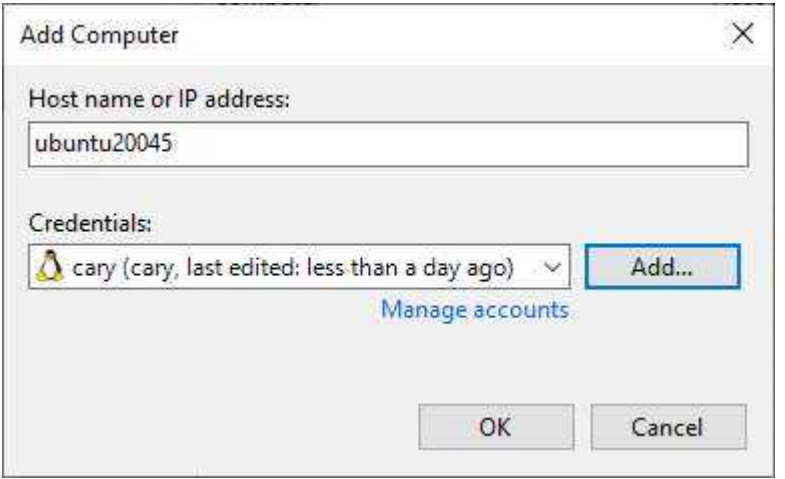
☐ Use "su" if "sudo" fails

Root password:

Description: cary

OK Cancel

20. Click OK on the add Computer page.



Add Computer

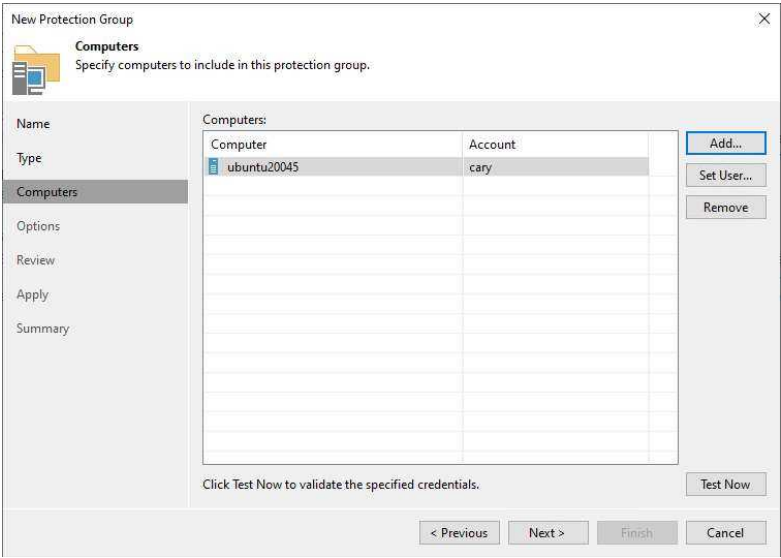
Host name or IP address: ubuntu20045

Credentials: cary (cary, last edited: less than a day ago) Add...

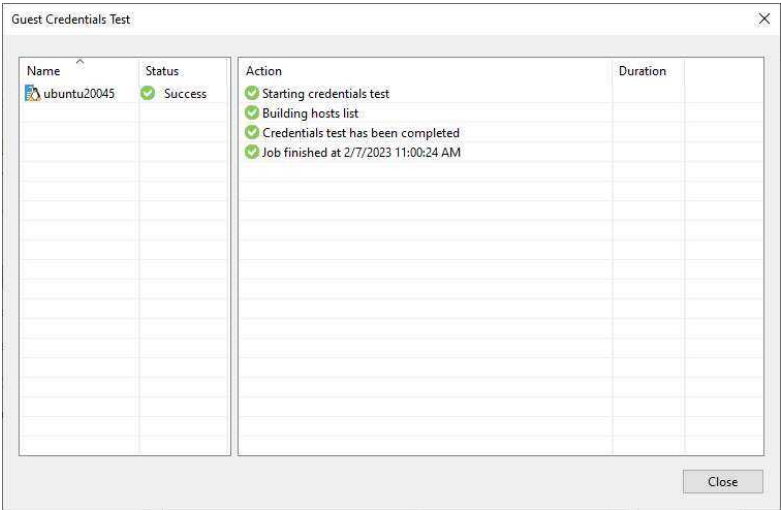
[Manage accounts](#)

OK Cancel

21. Click Test Now on the Computers page.



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



23. Click Next on the Computers page.

The screenshot shows the 'New Protection Group' dialog box with the 'Computers' tab selected. The left sidebar contains links for Name, Type, Computers, Options, Review, Apply, and Summary. The main area is titled 'Computers' with the instruction 'Specify computers to include in this protection group.' Below this is a table with columns 'Computer' and 'Account'. One entry is visible: 'ubuntu20045' with account 'cary'. To the right of the table are buttons for 'Add...', 'Set User...', and 'Remove'. At the bottom right is a 'Test Now' button. At the bottom are navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

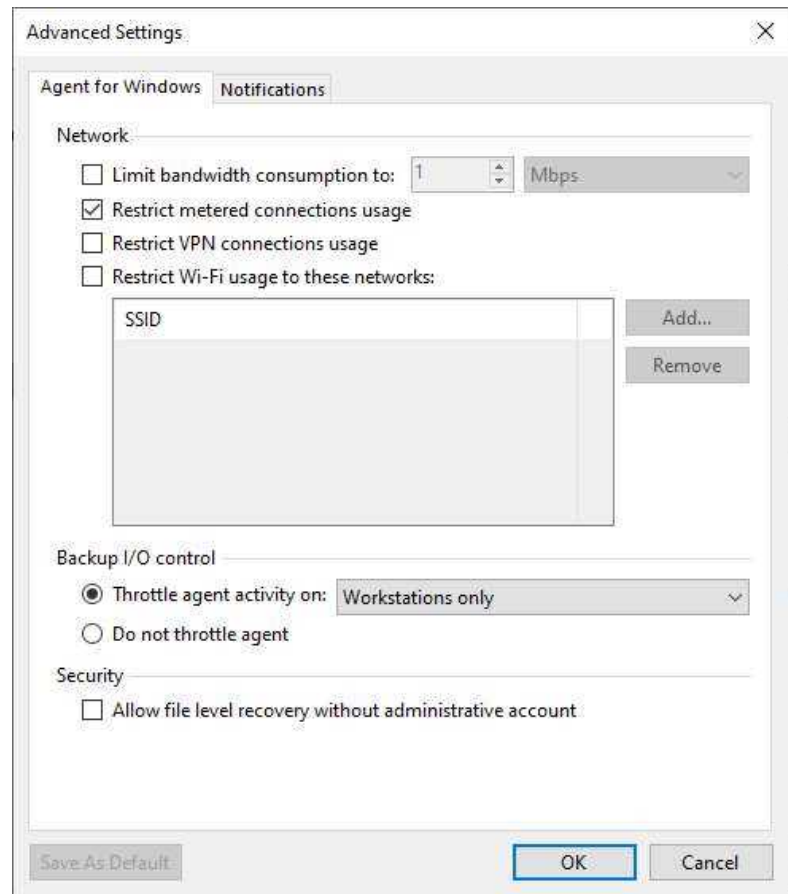
Computer	Account
ubuntu20045	cary

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.

The screenshot shows the 'New Protection Group' dialog box with the 'Options' tab selected. The left sidebar is the same as the previous screenshot. The main area is titled 'Options' with the instruction 'Specify a machine discovery schedule and agent deployment options.' It is divided into two sections: 'Discovery' and 'Deployment'.
In the 'Discovery' section, 'Rescan protection group every:' is set to 'Daily at this time: 9:00 PM' with a dropdown for 'Everyday' and a 'Days...' button. There is also an option for 'Periodically every: 1' with a dropdown for 'Hours' and a 'Schedule...' button.
In the 'Deployment' section, the 'Distribution server:' is set to 'VBR12PostgreSQL.gooddealmart.ca' with an 'Add...' button. Below this, it says 'Protected machines will download backup agents from this server.' There are several checkboxes: 'Install backup agent' (checked), 'Install changed block tracking driver (for Windows machines only)' (unchecked), 'Install application plug-ins: configure plug-ins to be installed' (unchecked, with a 'Configure...' button), 'Auto-update backup agents and plug-ins' (checked), and 'Perform reboot automatically if required' (unchecked).
At the bottom right is an 'Advanced...' button. At the bottom are navigation buttons: '< Previous', 'Next >', 'Finish', and '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.

- 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.



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.



35. On the Options page, click Next.

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

36. Click Apply on the Review page.

New Protection Group

Review

Review the settings, and click Apply to continue.

Name

Type

Computers

Options

Review

Apply

Summary

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

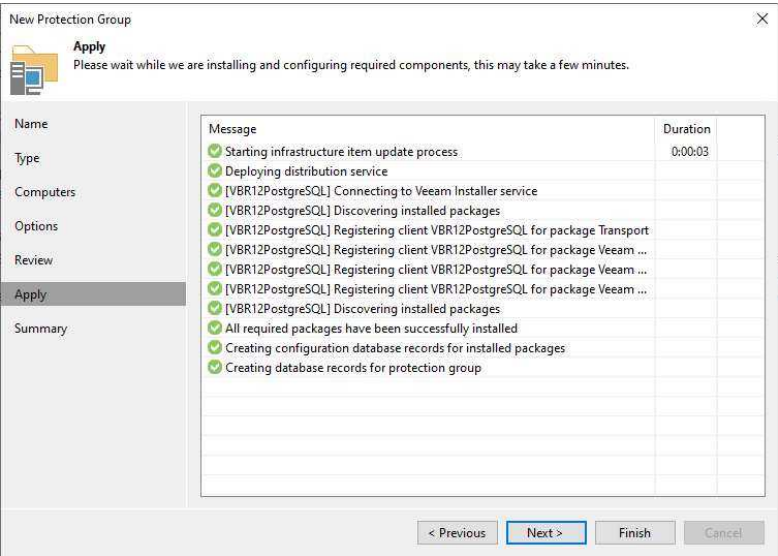
< Previous

Apply

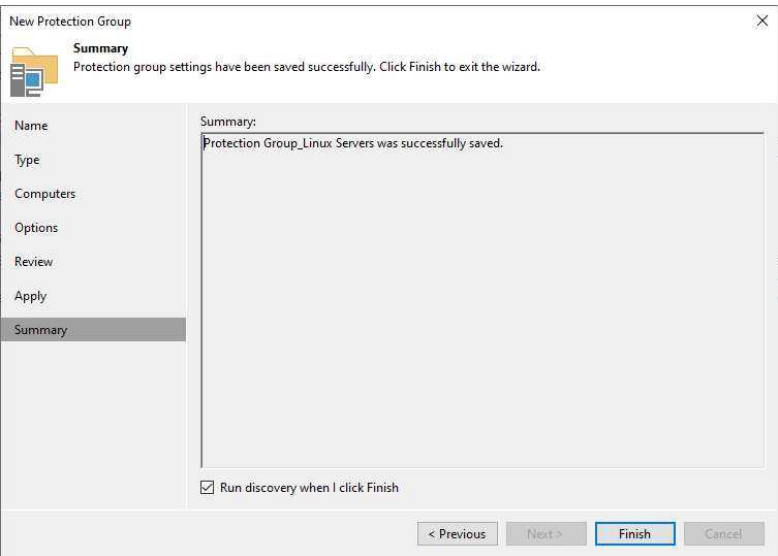
Finish

Cancel

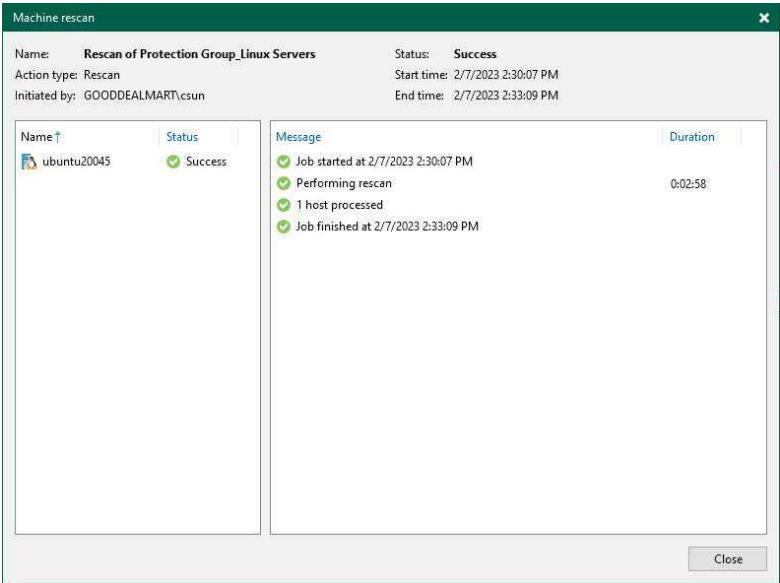
37. Click Next on the Apply page.



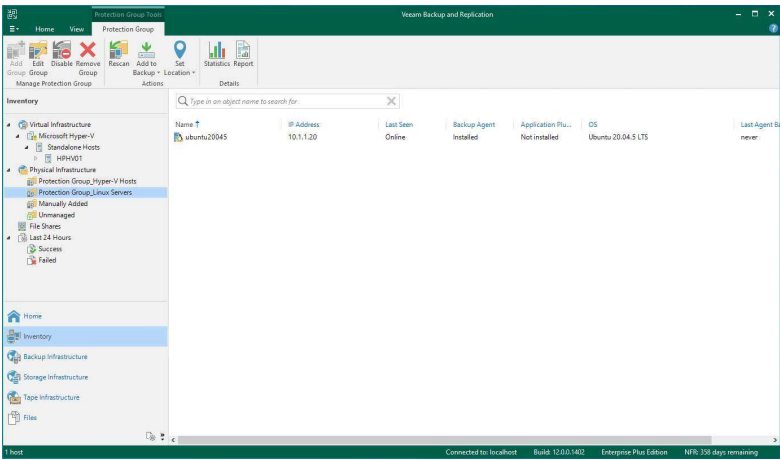
38. On the Summary page, select the Run discovery when I click the Finish checkbox and click Finish.



39. Verify the Machine rescan result and click Close.



40. Verify that the protection group has been added.



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:

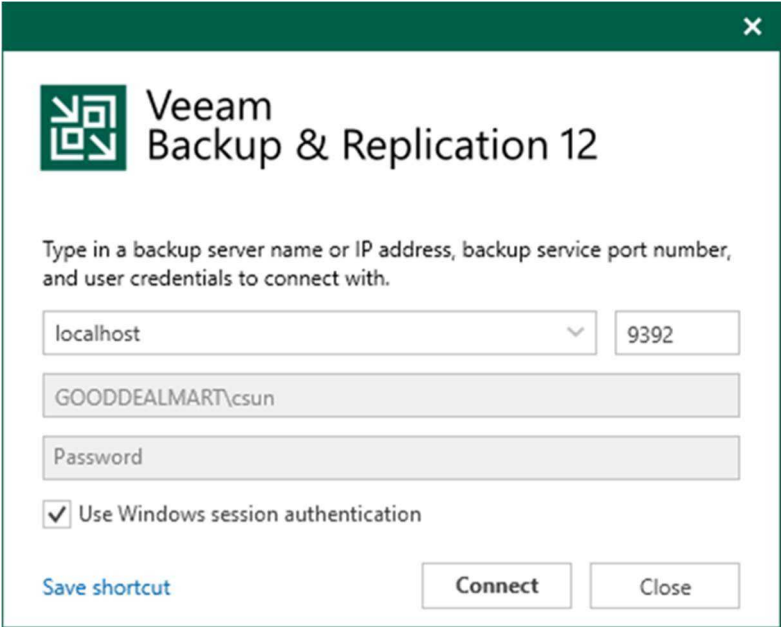
- Microsoft Windows server with local or network storage.
- Linux server with local or network storage.
- Linux server with a hardened repository.
- SMB (CIF) share network attached storage.
- NFS Share network attached storage.
- Deduplicating storage appliances.
- Object storage.

Do not configure multiple backup repositories pointing to the exact location or using the same path.

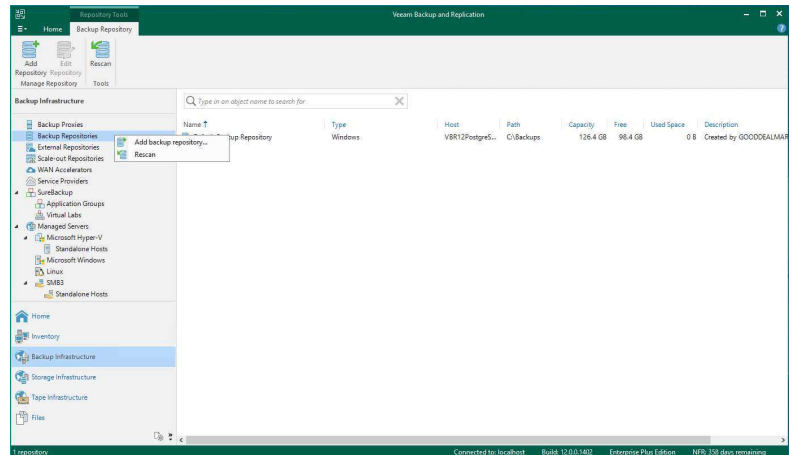
Add the Microsoft Windows server’s local directory as a Backup Repository

You can add the following types of storage to the Microsoft Windows server as a backup repository:

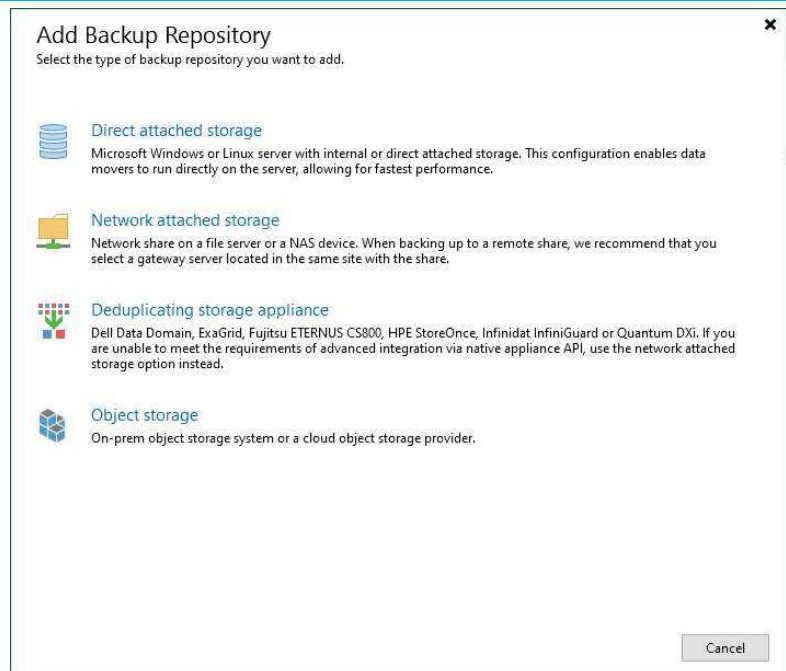
- A local disk.
- A directly attached disk-based storage (such as a USB hard drive).
- SCSI/FC SAN LUN in case the server is connected to the SAN fabric.

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.	 The screenshot shows the Veeam Backup & Replication 12 console window. The title bar is green with the Veeam logo and the text 'Veeam Backup & Replication 12'. The main area is white and contains the following elements: a dropdown menu with 'localhost' selected, a text box with '9392', a text box with 'GOODDEALMART\csun', a text box with 'Password', a checkbox labeled 'Use Windows session authentication' which is checked, a 'Save shortcut' link, and two buttons labeled 'Connect' and 'Close'.

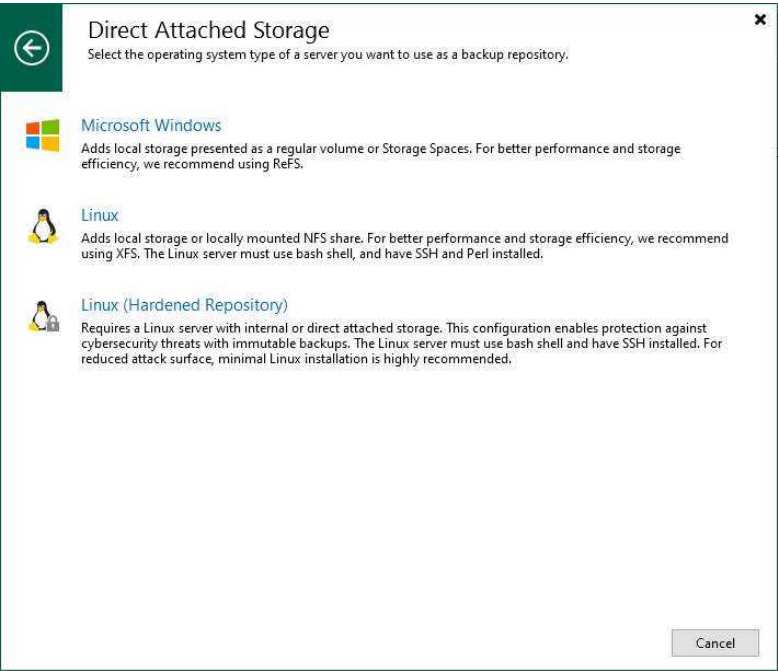
3. Select Backup Infrastructure on the Home page.
4. Select Backup Repositories on the Backup Infrastructure page.
5. Right-click Backup Repositories and select Add backup repository.



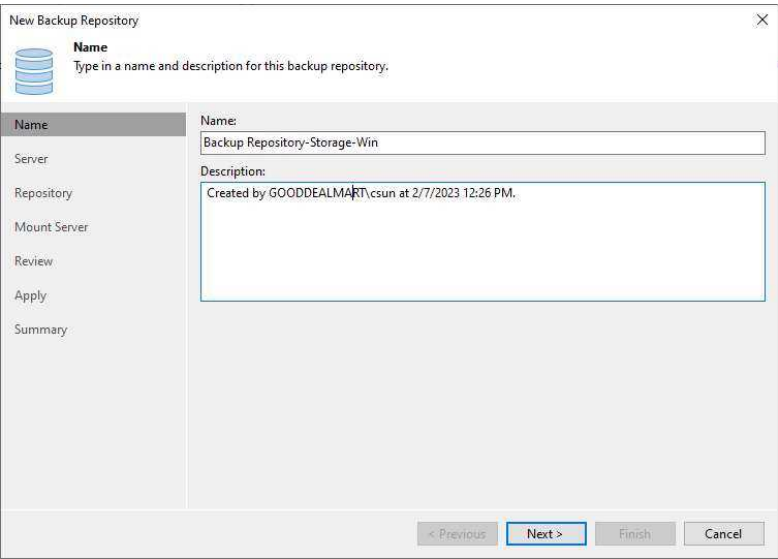
6. Select Direct attached storage on the Add Backup Repository page.



- 7. Select Microsoft Windows on the Direct Attached Storage page.



- 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.



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.

Name

Repository server: STORAGE-WIN (Created by GOODDEALMART,csun at 2/3/2023 1:12 PM.) Add New...

Path Capacity Free

Populate

< Previous Next > Finish Cancel

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.

Name

Repository server: STORAGE-WIN (Created by GOODDEALMART,csun at 2/3/2023 1:12 PM.) Add New...

Path Capacity Free

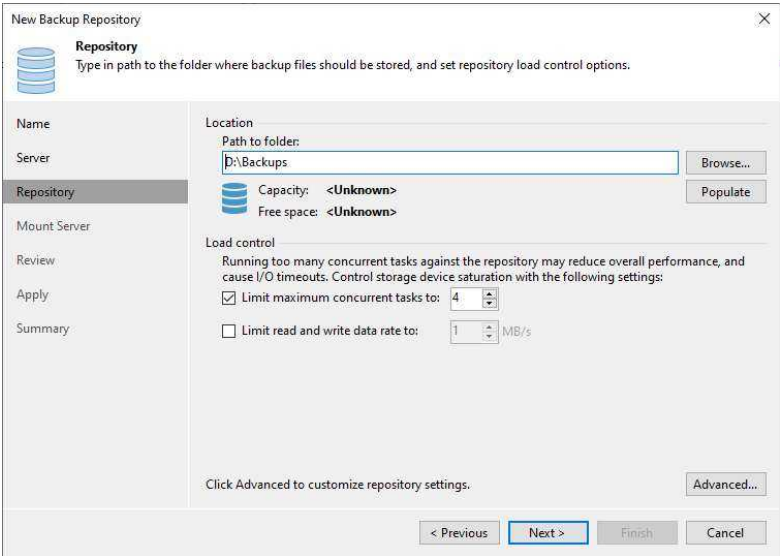
C:\ 29.4 GB 15.5 GB

D:\ 126.9 GB 125.6 GB

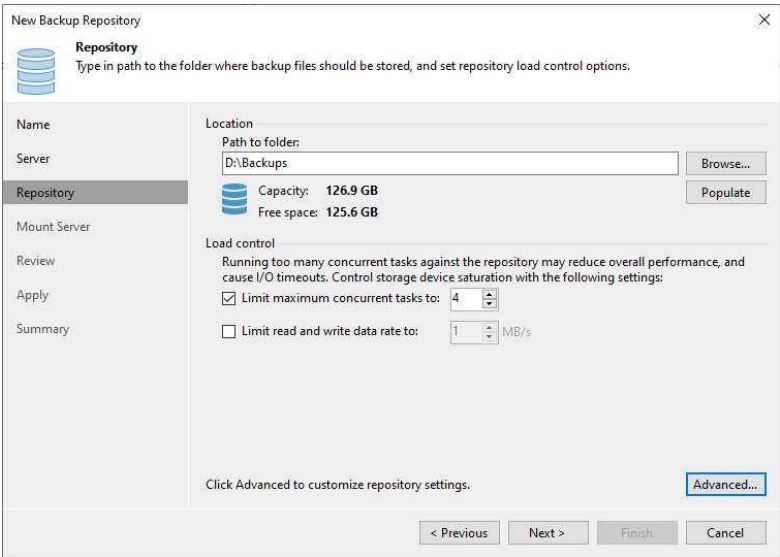
Populate

< Previous Next > Finish Cancel

12. On the Repository page, click Populate to review the disk capacity and free space.

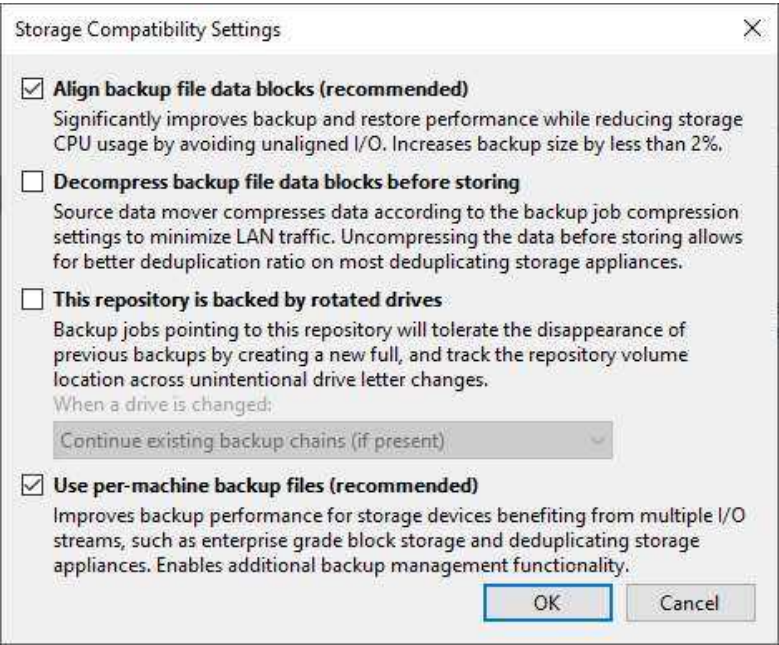


13. Use the Load control settings to manage the load on the backup repository and avoid storage I/O.
14. Click Advanced.

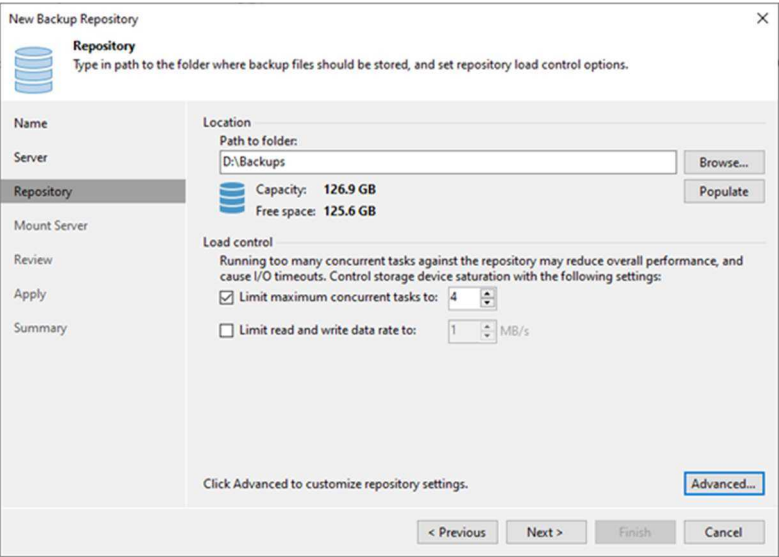


- 15. On the Storage Compatibility Settings, select Align backup file data blocks (recommended) checkbox
- 16. Select Use per-machine backup files and click OK.

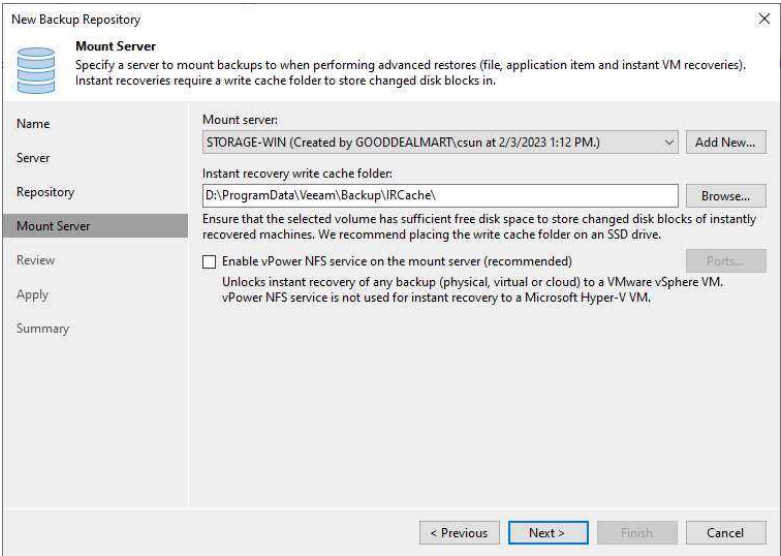
Note:
Select Decompress backup file data blocks before storing if you use a deduplicating storage feature or appliance.



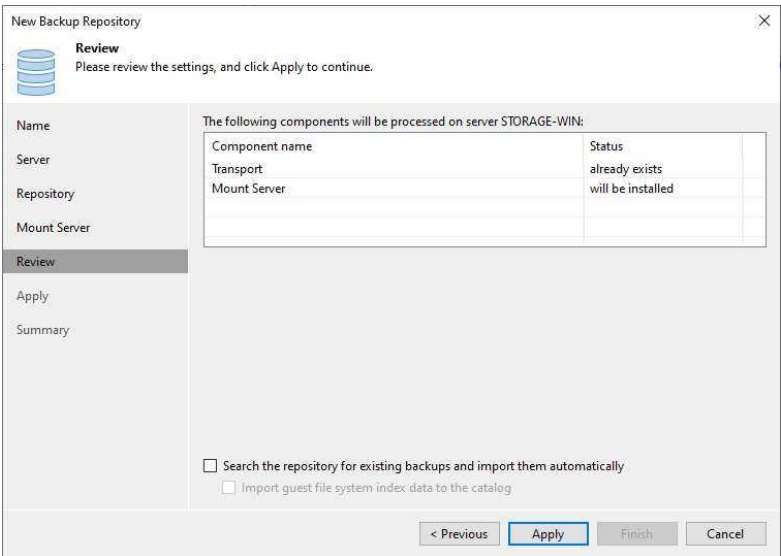
- 17. Click Next on the Repository page.



- 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.

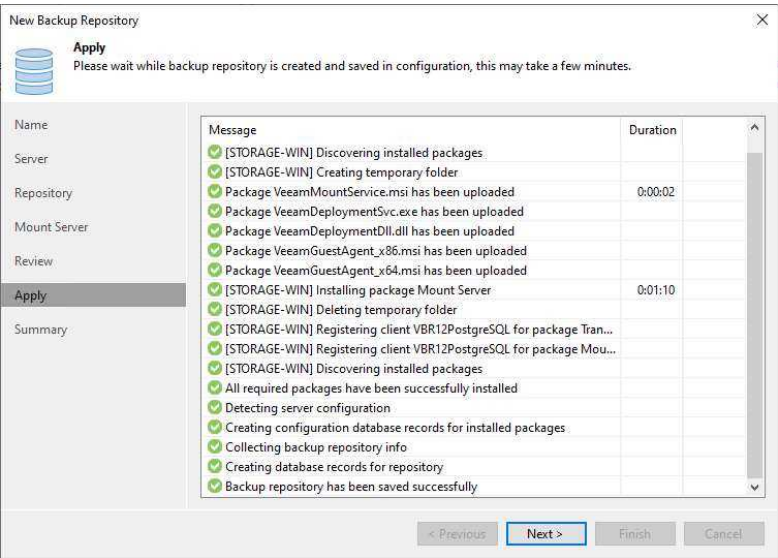


- 22. On the Review page, click Apply.
- 23. Select the Search the repository for existing backups and import them automatically checkbox if the backup repository contains backups previously created with Veeam Backup & Replica on.
- 24. Select the Import guest file system index data to the catalog checkbox if the backup repository contains guest file system

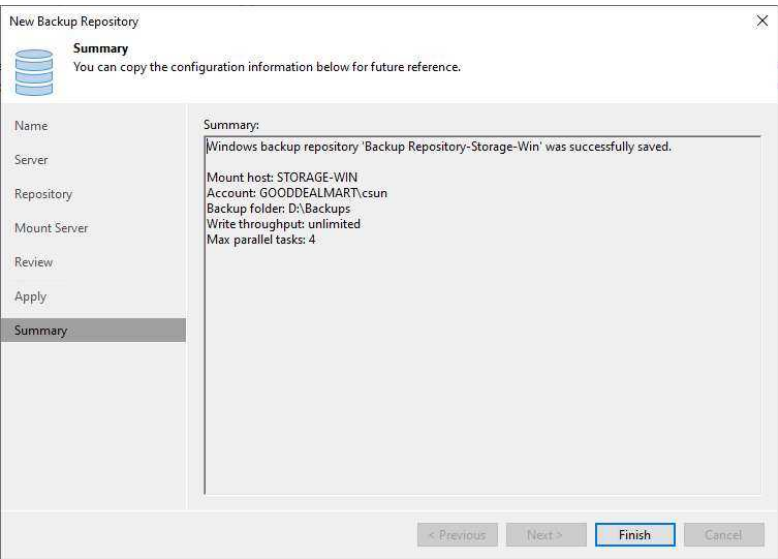


index files previously
created by Veeam Backup
& Replica on.

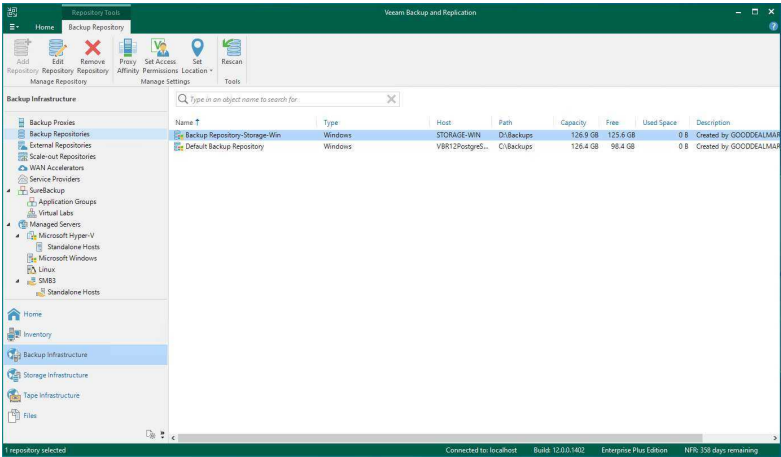
25. Click Next on the Apply
page.



26. Click Finish on the
Summary page.



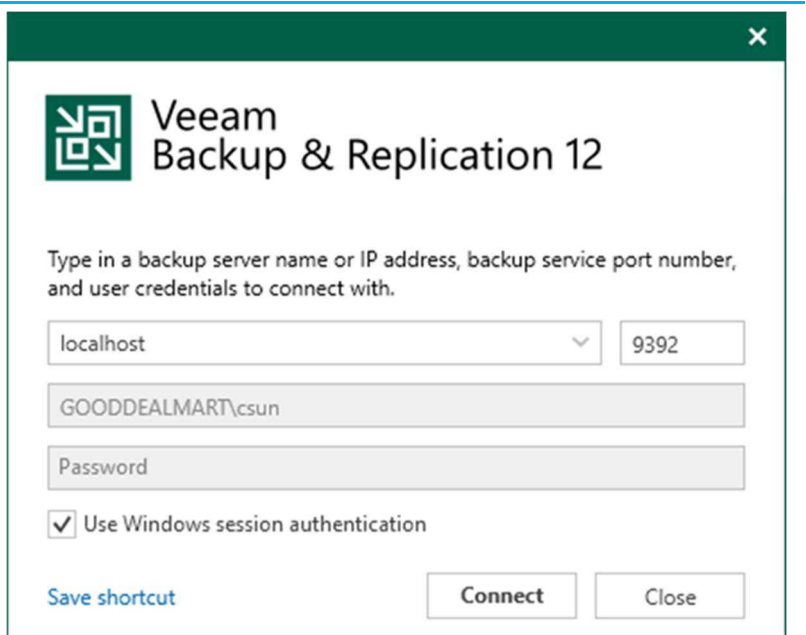
27. Verify that the new Backup Repository has been added.



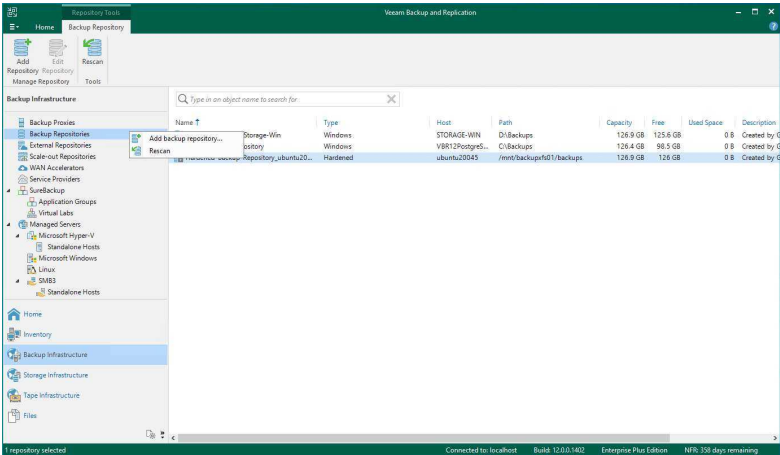
Add the Linux server's local directory as a Backup Repository

You can add the following types of storage to the Linux server as a backup repository:

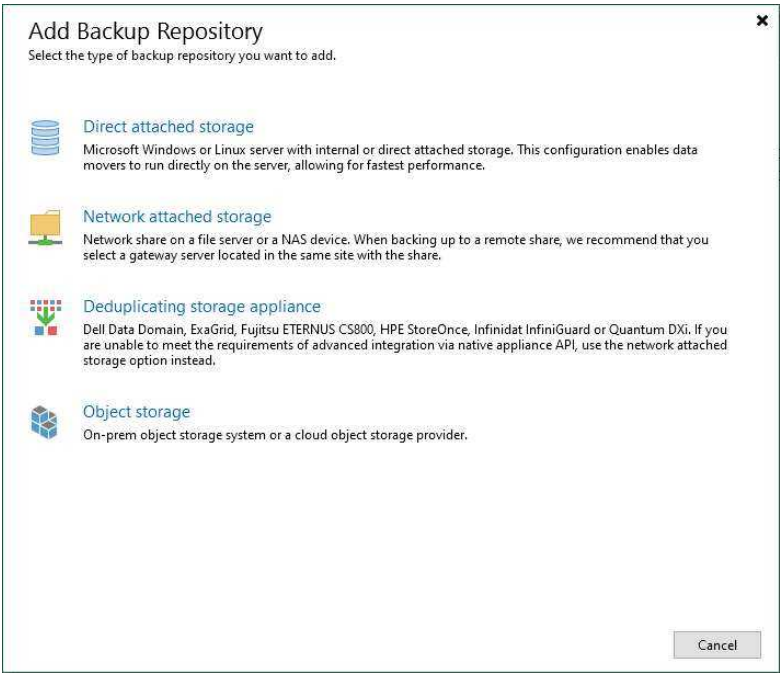
- A local disk.
- A directly attached disk-based storage (such as a USB hard drive).
- NFS share.
- SCSI/FC SAN LUN in case the server is connected to the SAN fabric.

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.	 The screenshot shows the 'Veeam Backup & Replication 12' console window. It has a dark green title bar with a close button. The main area is white with the Veeam logo and title. Below the title, it says 'Type in a backup server name or IP address, backup service port number, and user credentials to connect with.' There are four input fields: a dropdown menu with 'localhost' selected, a text box with '9392', a text box with 'GOODDEALMART\csun', and a password field labeled 'Password'. Below these fields is a checkbox labeled 'Use Windows session authentication' which is checked. At the bottom, there are three buttons: 'Save shortcut' (blue text), 'Connect' (white button), and 'Close' (white button).

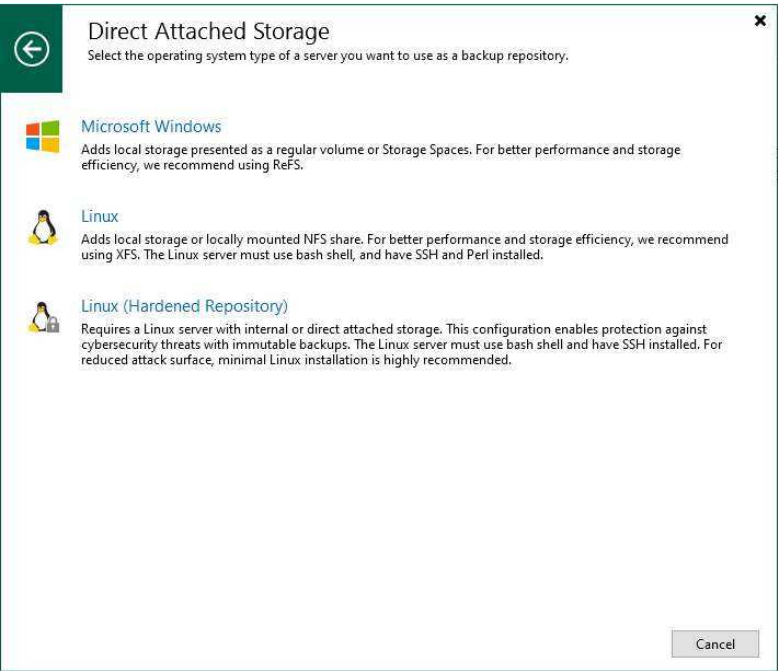
- 3. On the Home page, select Backup Infrastructure.
- 4. On the Backup Infrastructure page, select Backup Repositories.
- 5. Right-click Backup Repositories and select Add backup repository.



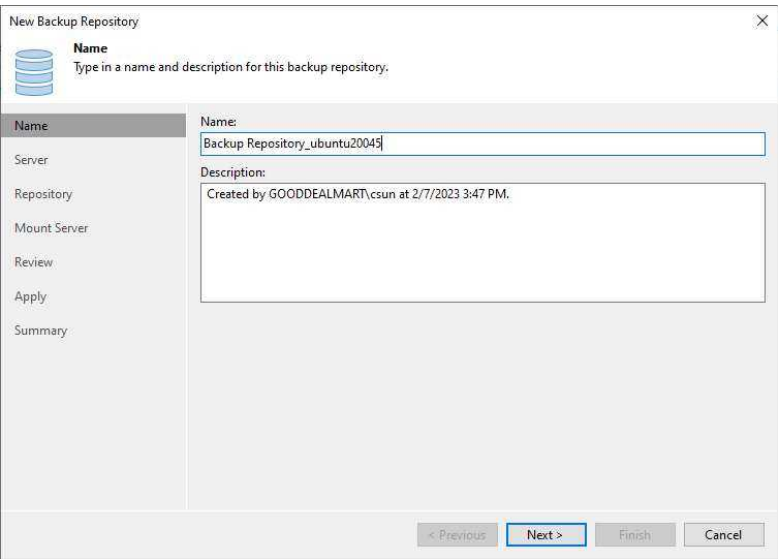
- 6. Select Direct attached storage on the Add Backup Repository page.



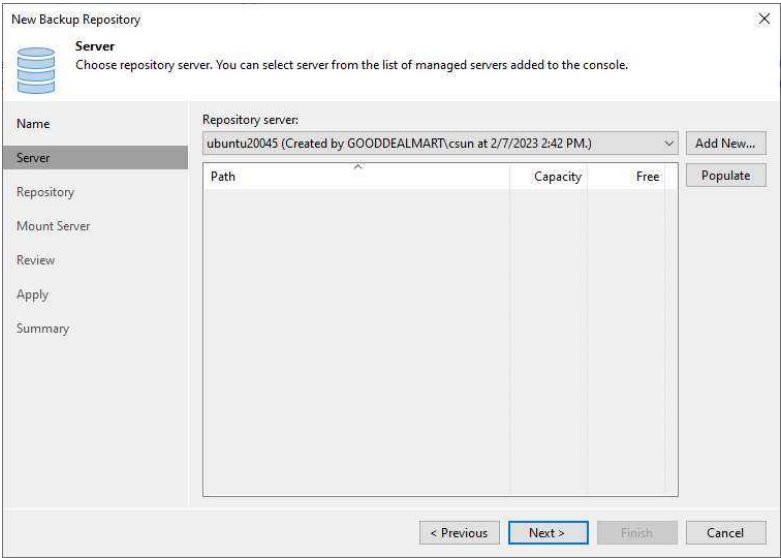
7. Select Linux on the Direct Attached Storage page.



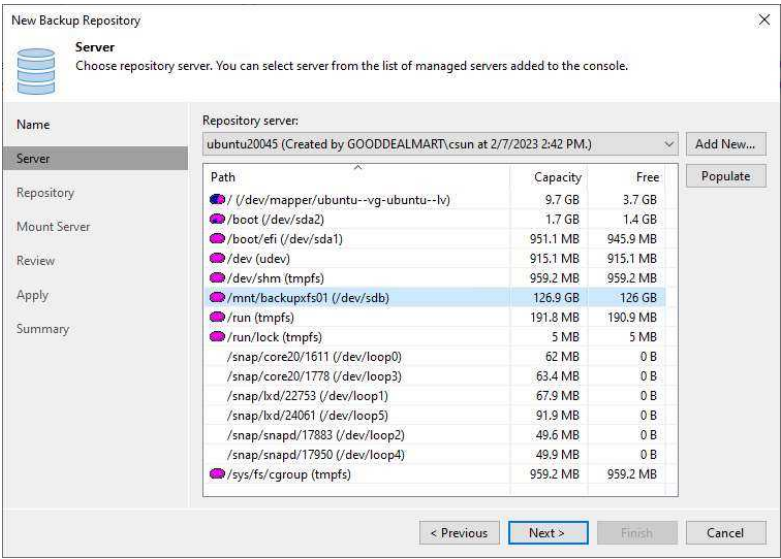
8. On the Name page, specify a Backup Repository name.
9. Give a brief description in the Description field for future reference and click Next.



10. On the Server page, select the Linux server from the Repository server drop-down list and click Populate.



11. Select the disk and click Next.



12. On the Repository page, click **Browse** 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.

Name

Server

Repository

Mount Server

Review

Apply

Summary

Location

Path to folder:

Browse...

Capacity: <Unknown>

Free space: <Unknown>

Populate

☐ 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.

Advanced

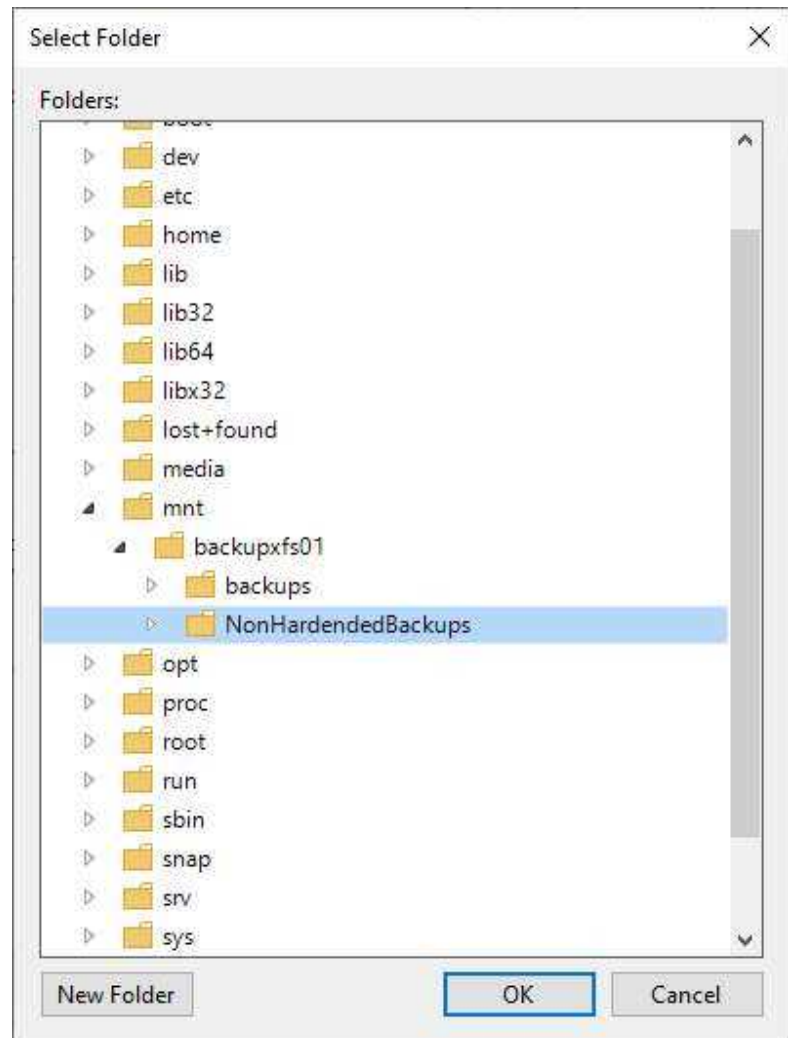
< Previous

Next >

Finish

Cancel

13. On the Select Folder page, expand the server.
14. Select the NonHardenedBackups 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.

Name

Server

Repository

Mount Server

Review

Apply

Summary

Location

Path to folder:
/mnt/backupxfs01/NonHardendedBackups **Browse...**

Capacity: <Unknown>
Free space: <Unknown> **Populate**

☒ 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. **Advanced...**

< Previous Next > Finish Cancel

16. On the Repository page, select Use fast cloning 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.

New Backup Repository

Repository
Type in path to the folder where backup files should be stored, and set repository load control options.

Name

Server

Repository

Mount Server

Review

Apply

Summary

Location

Path to folder:
/mnt/backupxfs01/NonHardendedBackups **Browse...**

Capacity: 126.9 GB
Free space: 126 GB **Populate**

☒ 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

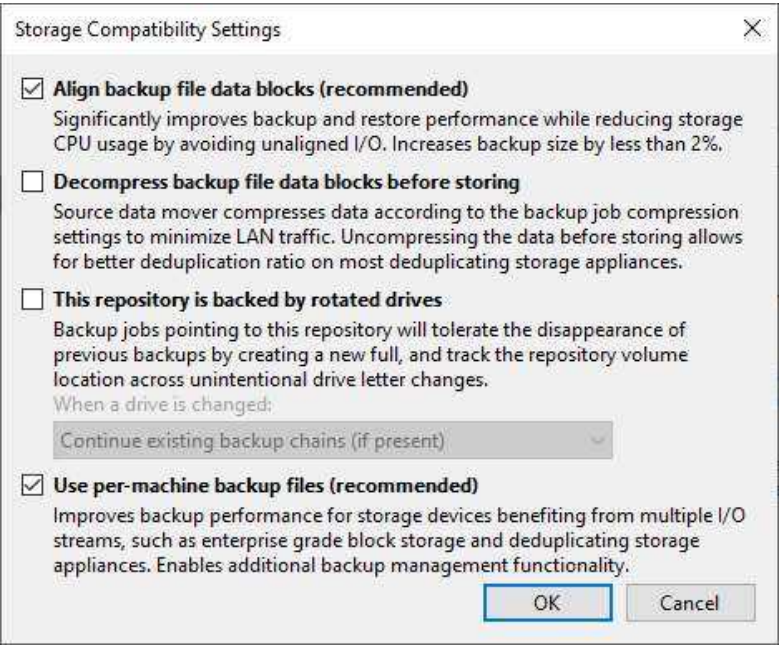
Click Advanced to customize repository settings. **Advanced...**

< Previous Next > Finish Cancel

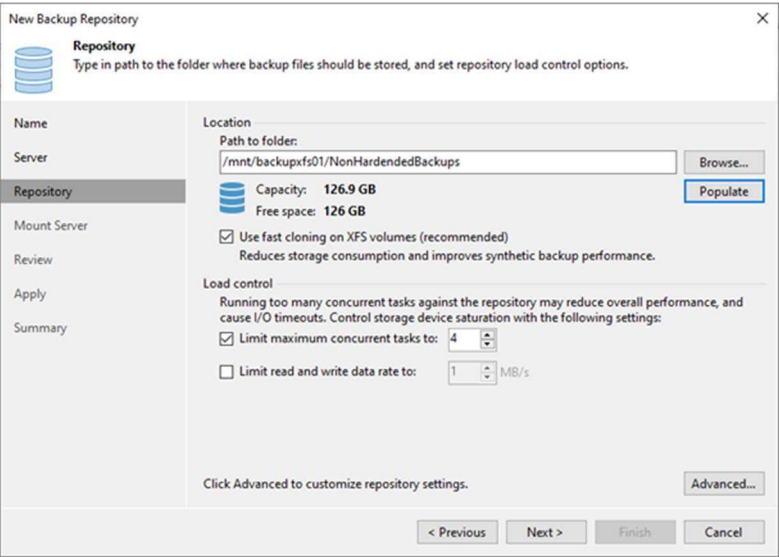
- 19. On the Storage Compatibility Settings, select Align backup file data blocks (recommended) checkbox
- 20. Select Use per-machine backup files and click OK.

Note:

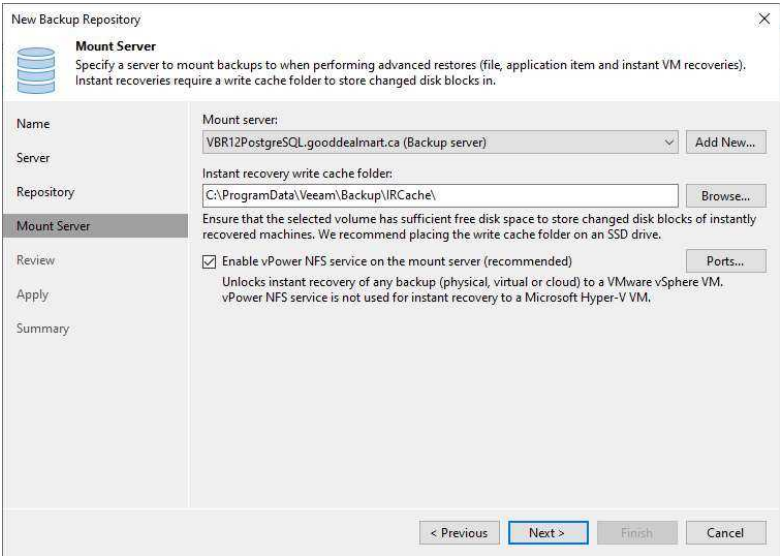
Select Decompress backup file data blocks before storing if you use a deduplicating storage feature or appliance.



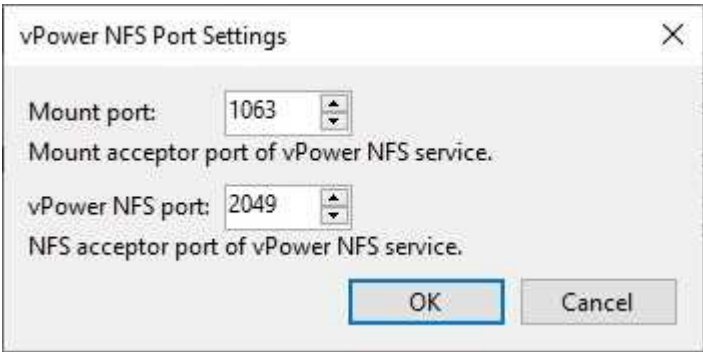
- 21. On the Repository page, click Next.



- 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 (recommended) and click Ports.



- 25. Review the ports settings on the vPower NFS Port Settings dialog box and click OK.



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.

Name
Server
Repository
Mount Server
Review
Apply
Summary

Mount server:
VBR12PostgreSQL.gooddealmart.ca (Backup server) Add New...

Instant recovery write cache folder:
C:\ProgramData\Veeam\Backup\IRCache\ Browse...

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) Ports...
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.

< Previous **Next >** Finish Cancel

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 & Replica on.
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 & Replica on.

New Backup Repository

Review
Please review the settings, and click Apply to continue.

Name
Server
Repository
Mount Server
Review
Apply
Summary

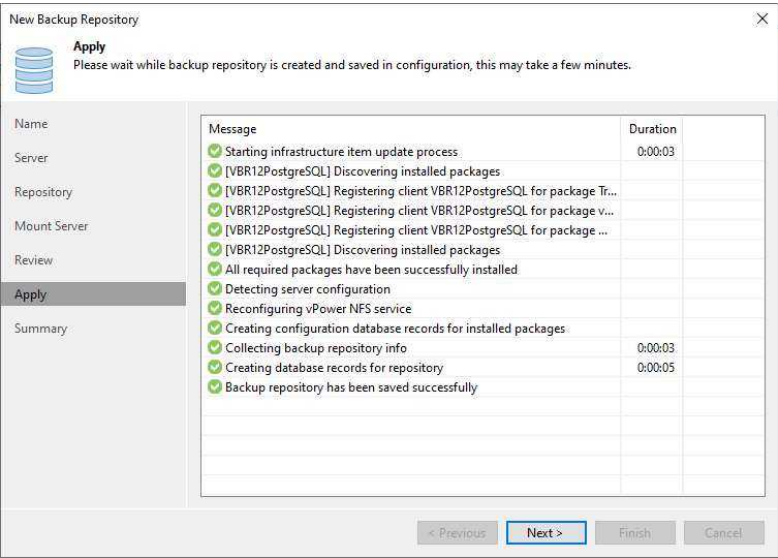
The following components will be processed on server VBR12PostgreSQL.gooddealmart.ca:

Component name	Status
Transport	already exists
vPower NFS	already exists
Mount Server	already exists

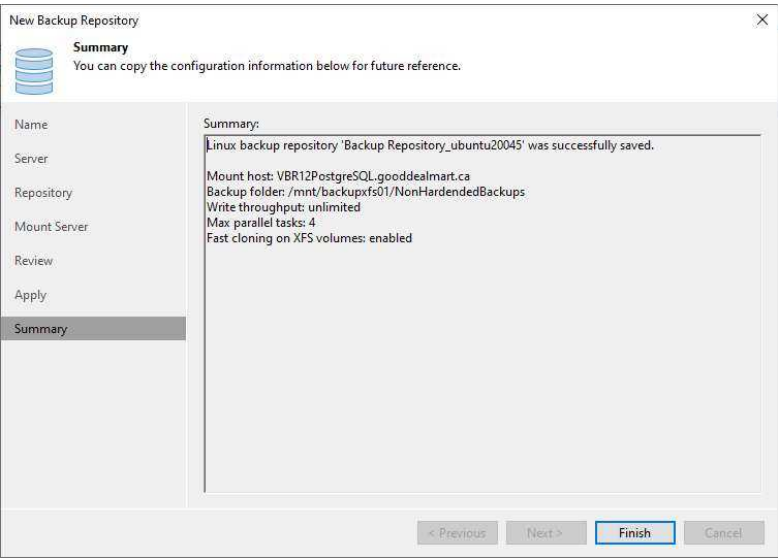
☐ Search the repository for existing backups and import them automatically
☐ Import guest file system index data to the catalog

< Previous **Apply** Finish Cancel

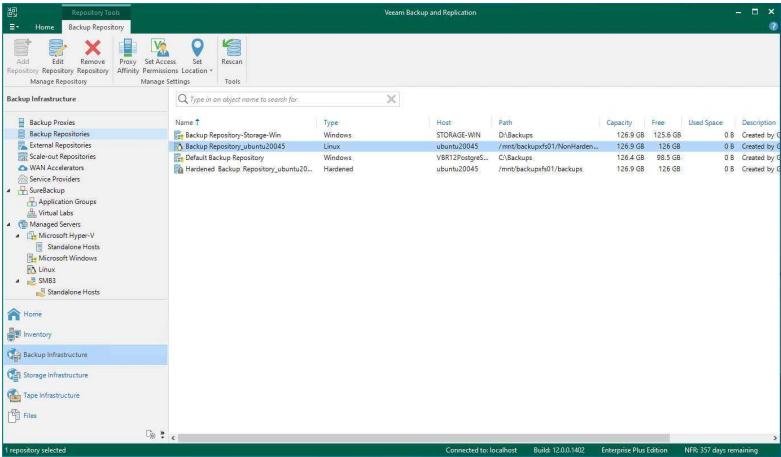
30. Click Next on the Apply page.



31. Click Finish on the Summary page.



32. Verify that the Linux Backup Repository has been added.



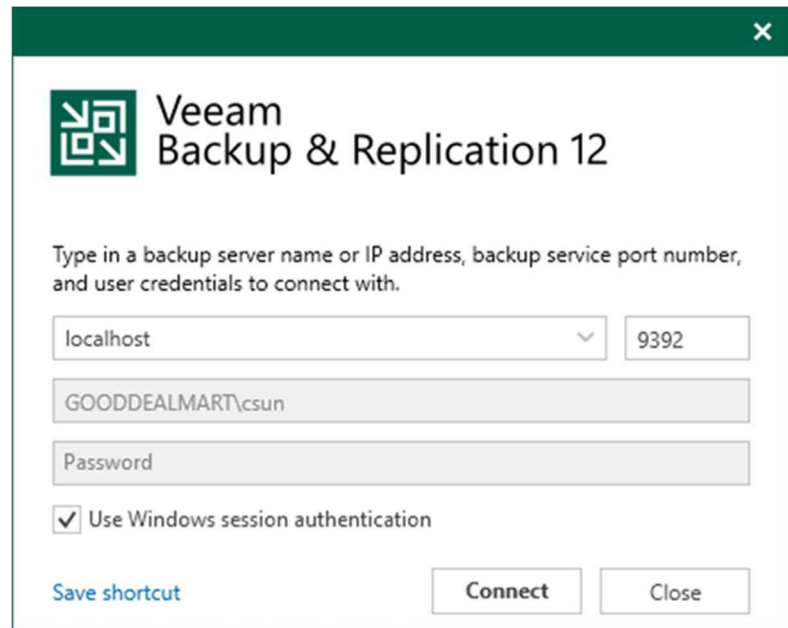
Add the Linux server’s local directory as a Hardened Backup Repository

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:

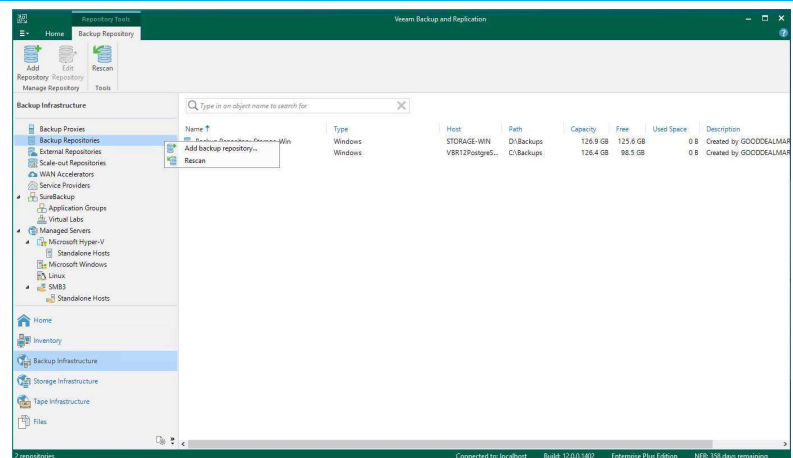
- **Immutability:** You specify the period when you add a hardened repository, and backup files must be immutable.
- **Single-use credentials:** Credentials will only be used once to add the Linux server to the backup infrastructure. The backup infrastructure does not store these credentials. Therefore, the attacker cannot access the hardened repository even if the Veeam Backup & Replication server is compromised.

Instructions	Screenshot (if applicable)
--------------	----------------------------

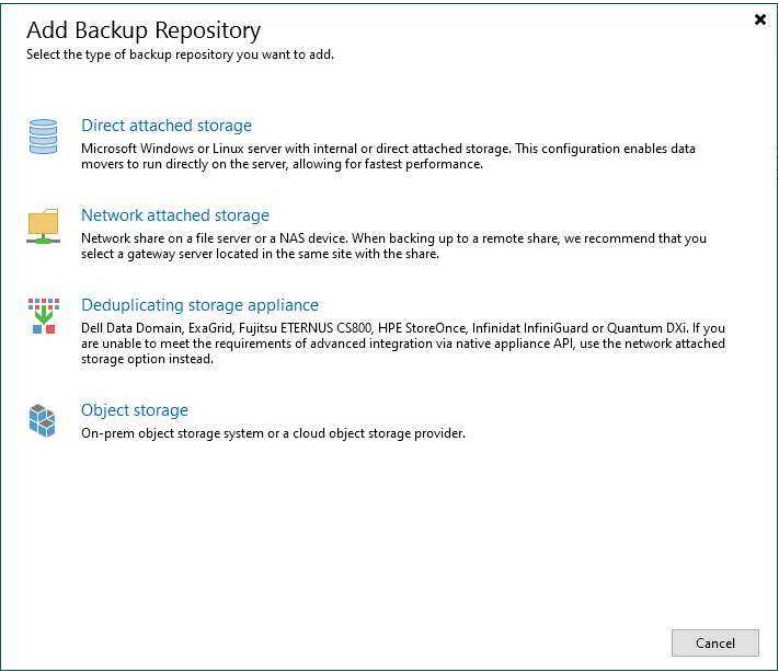
1. Log in to the Veeam Backup and replication manager server.
2. Open the Veeam Backup & Replication Console, and click Connect.



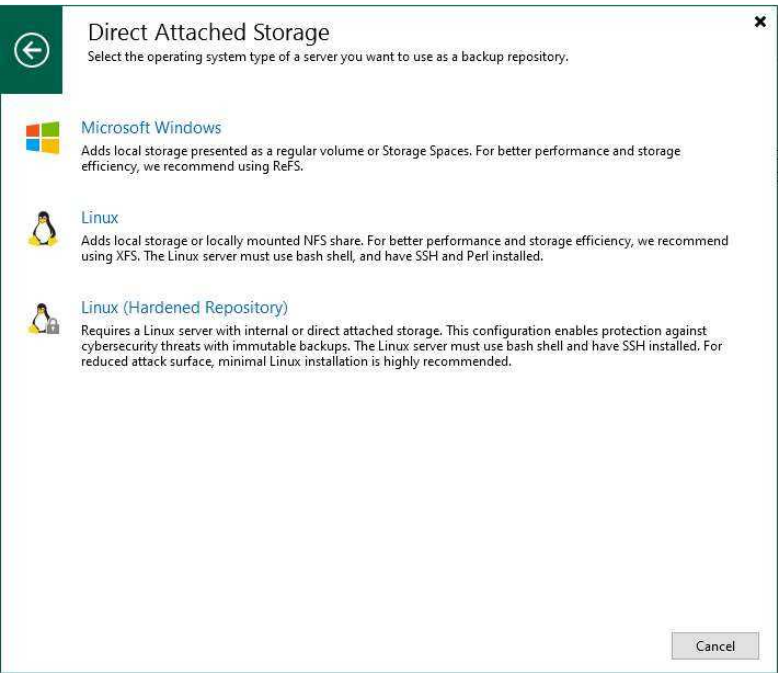
3. On the Home page, select Backup Infrastructure.
4. On the Backup Infrastructure page, select Backup Repositories.
5. Right-click Backup Repositories and select Add backup repository.



6. Select Direct attached storage on the Add Backup Repository page.



7. Select Linux (Hardened Repository) on the Direct Attached Storage page.



- 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

Server

Repository

Mount Server

Review

Apply

Summary

Name:

Hardened Backup Repository_ubuntu20045

Description:

Created by GOODDEALMART\csun at 2/7/2023 2:57 PM

< Previous

Next >

Finish

Cancel

- 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.

Name

Server

Repository

Mount Server

Review

Apply

Summary

Repository server:

ubuntu20045 (Created by GOODDEALMART\csun at 2/7/2023 2:42 PM.)

Add New...

Path	Capacity	Free
------	----------	------

Populate

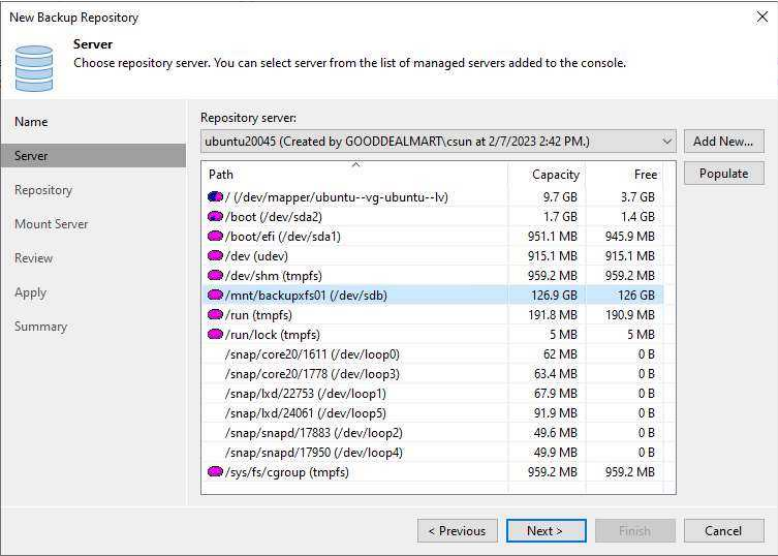
< Previous

Next >

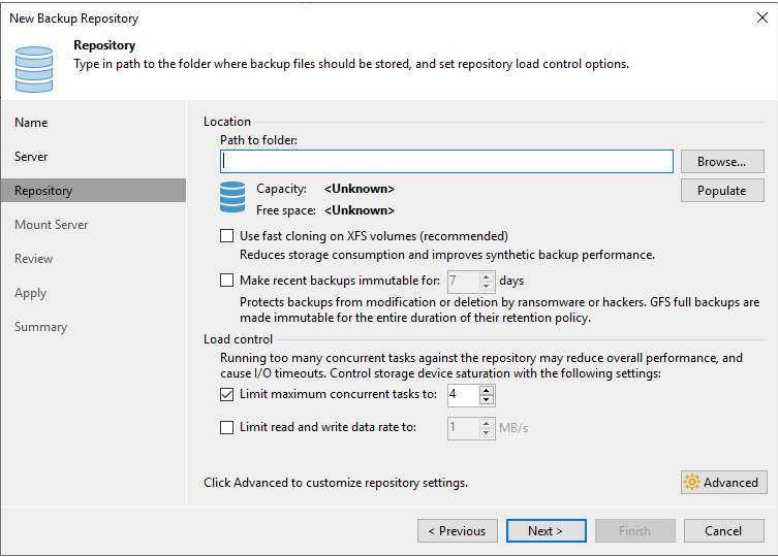
Finish

Cancel

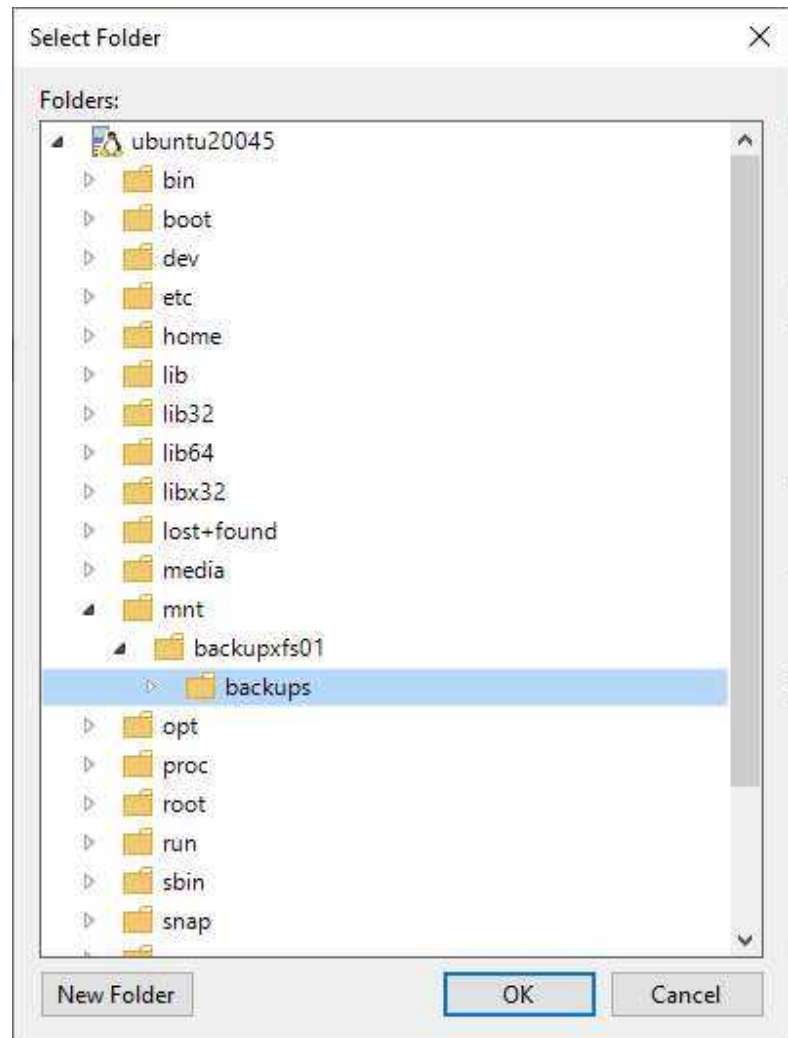
11. Select the disk and click Next.



12. On the Repository page, click Browser for Path to folder.



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.

Name

Server

Repository

Mount Server

Review

Apply

Summary

Location

Path to folder: /mnt/backups01/backups Browse...

Capacity: <Unknown> Populate

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. Advanced...

< Previous Next > Finish Cancel

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.

Name

Server

Repository

Mount Server

Review

Apply

Summary

Location

Path to folder: /mnt/backups01/backups Browse...

Capacity: 126.9 GB Populate

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

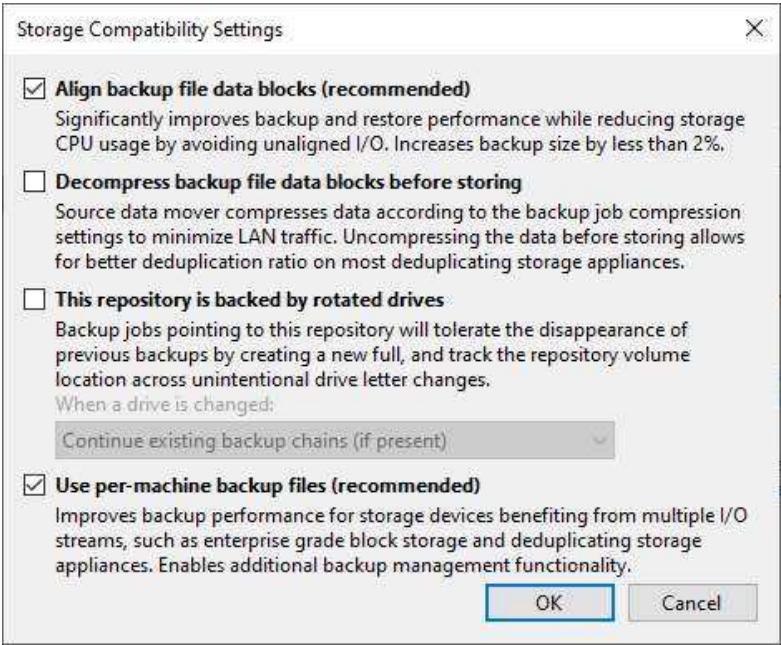
Click Advanced to customize repository settings. Advanced...

< Previous Next > Finish Cancel

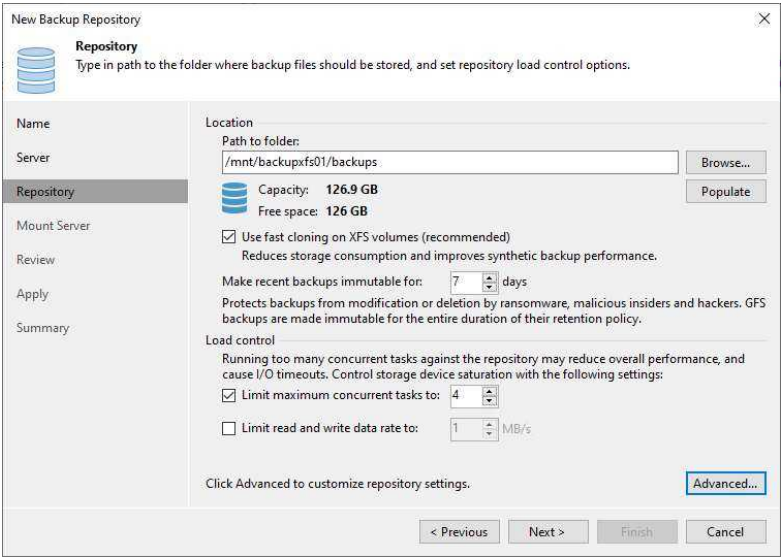
- 20. On the Storage Compatibility Settings, select Align backup file data blocks (recommended) checkbox
- 21. Select Use per-machine backup files and click OK.

Note:

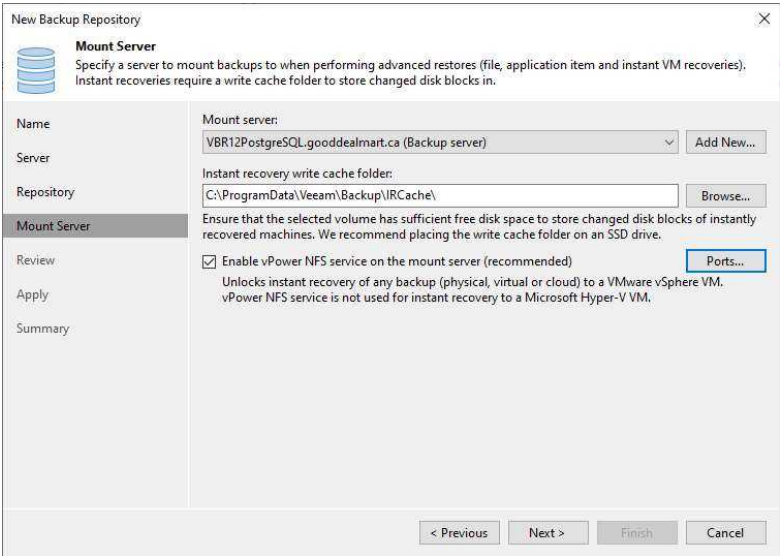
Select Decompress backup file data blocks before storing if you use a deduplicating storage feature or appliance.



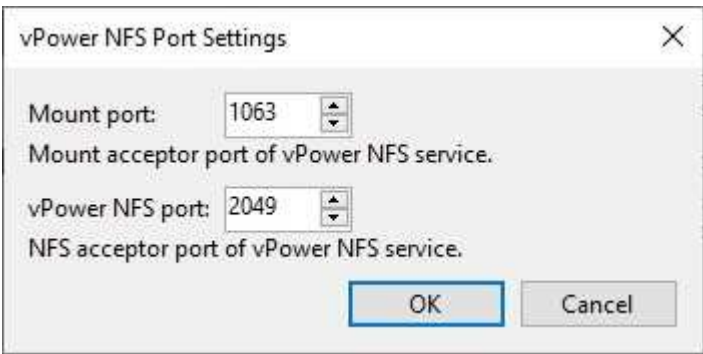
- 22. On the Repository page, click Next.



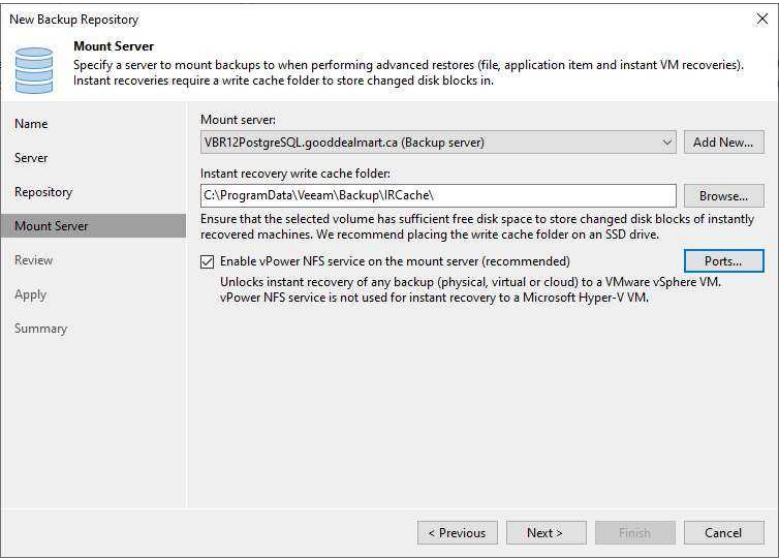
- 23. Select a mount server from the Mount server drop-down list on the Mount Server page.
- 24. Select a folder in the Instant recovery write cache folder field for writing cache during mount operations.
- 25. Select Enable vPower NFS service on the mount server (recommended) and click Ports.



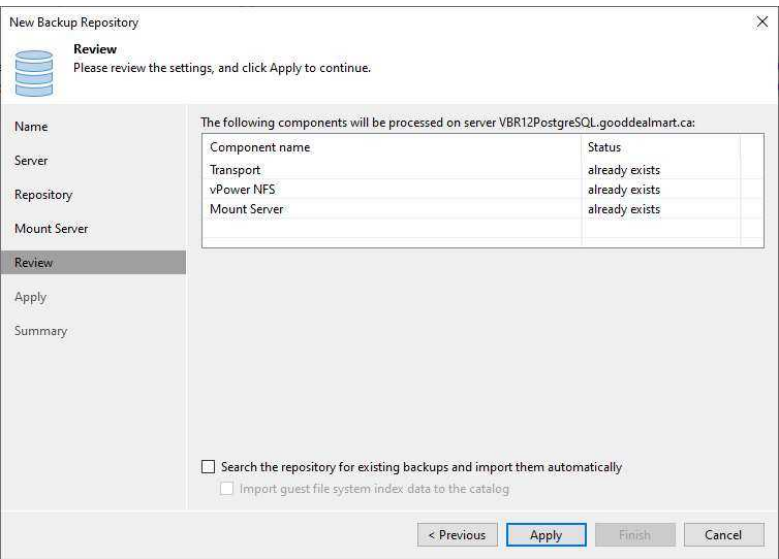
- 26. Review the ports settings on the vPower NFS Port Settings page and click OK.



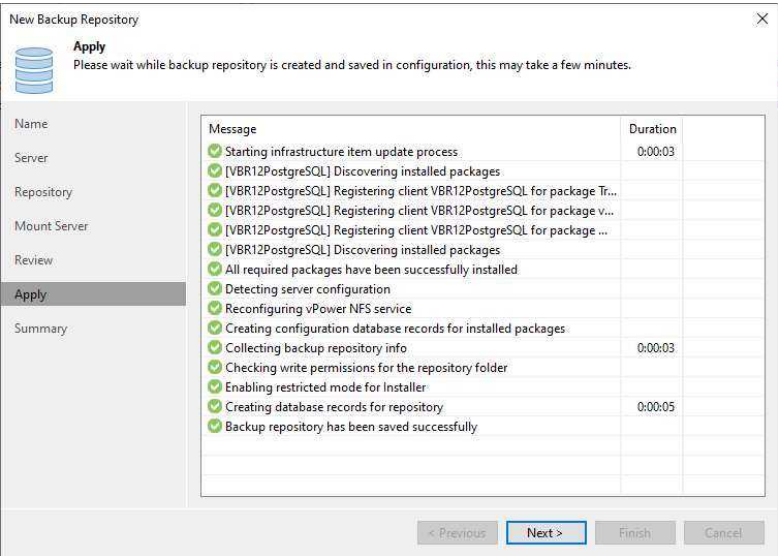
27. Click Next on the Mount Server page.



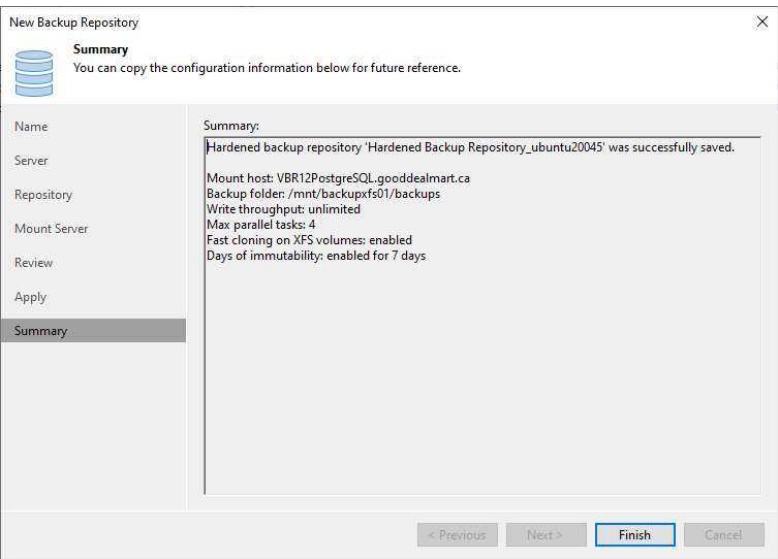
- 28. On the Review page, click Apply.
- 29. Select the Search the repository for existing backups and import them automatically checkbox if the backup repository contains backups previously created with Veeam Backup & Replica on.
- 30. Select the Import guest file system index data to the catalog checkbox if the backup repository contains guest file system index files previously created by Veeam Backup & Replica on.



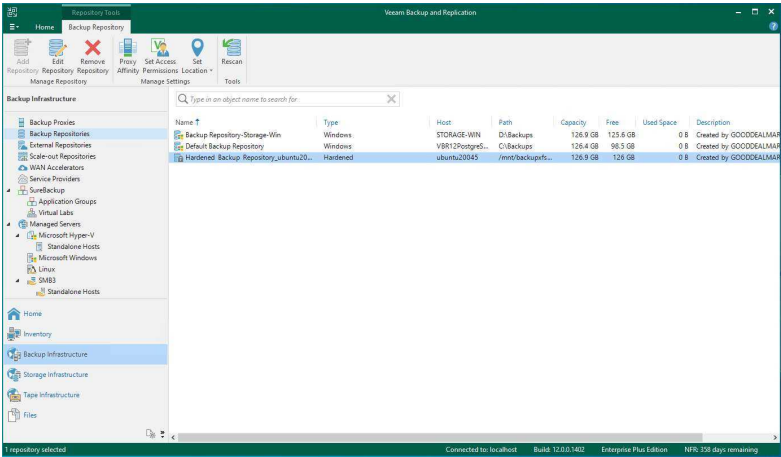
31. Click Next on the Apply page.



32. Click Finish on the Summary page.



33. Verify that the Hardened Backup Repository has been added.



Add Network Attached Storage (SMB or CIFS Shares) as Backup Repository

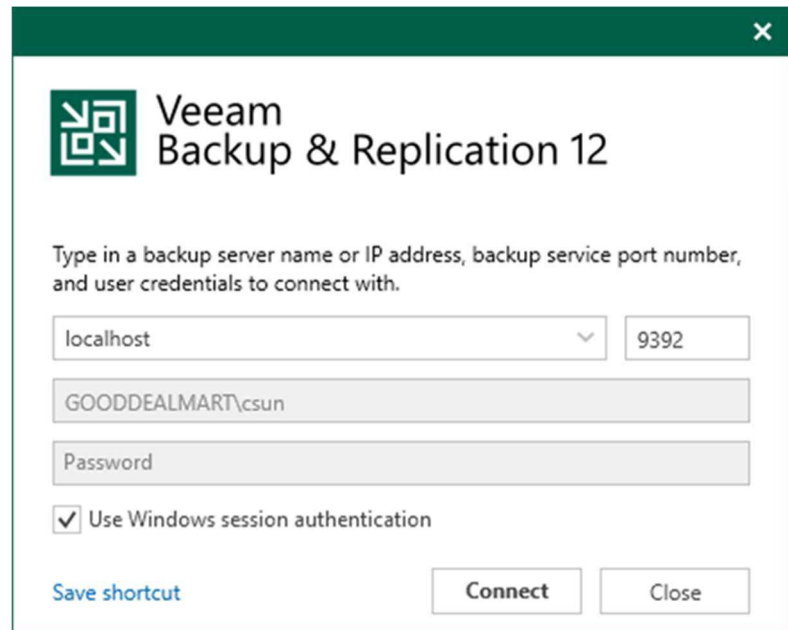
You can use network-attached storage (SMB or CIFS Shares) as backup repositories with Veeam Backup and Replica. A network-attached storage (NAS) device can be a shared folder on your computer or any other physical device accessed via the Server Message Block (SMB) protocol.

Note:

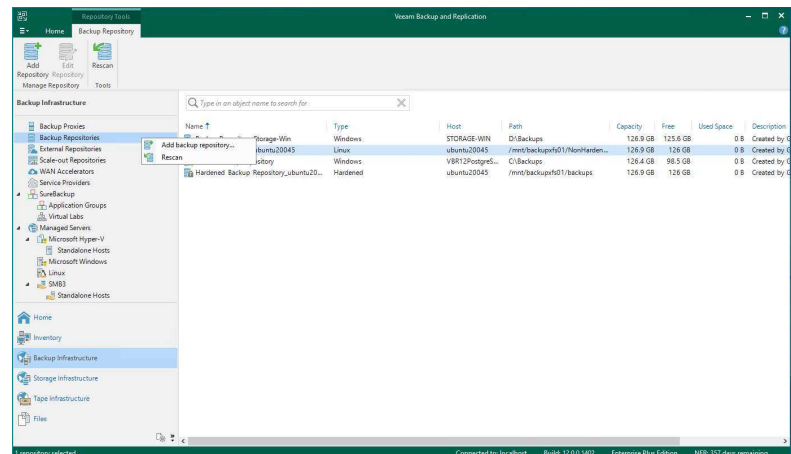
- You must deploy a gateway server because an SMB share cannot host Veeam Data Movers. However, Veeam Backup & Replica will automatically deploy a Veeam Data Mover on this gateway server.
- It is recommended that you deploy an additional gateway server in the remote site, closer to the SMB repository, if you plan to move VM data to an off-site SMB repository over a WAN link,

Instructions	Screenshot (if applicable)
--------------	----------------------------

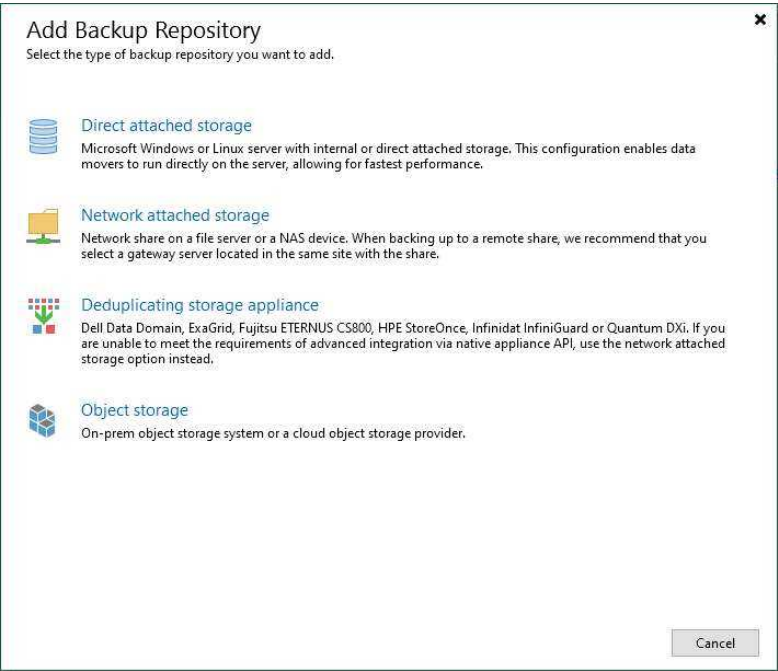
1. Log in to the Veeam Backup and replication manager server.
2. Open the Veeam Backup & Replication Console and click Connect.



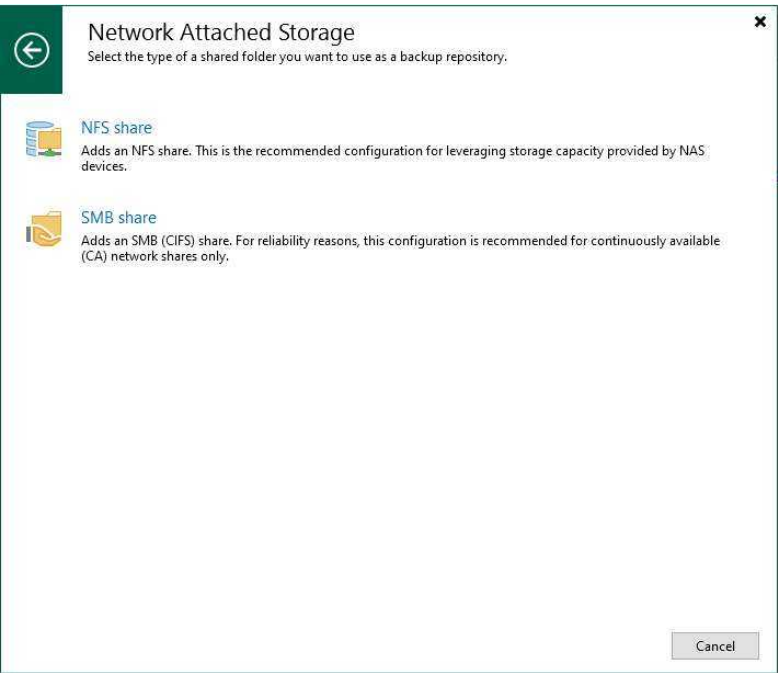
3. Select Backup Infrastructure on the Home page.
4. Select Backup Repositories on the Backup Infrastructure page.
5. Right-click Backup Repositories and select Add backup repository.



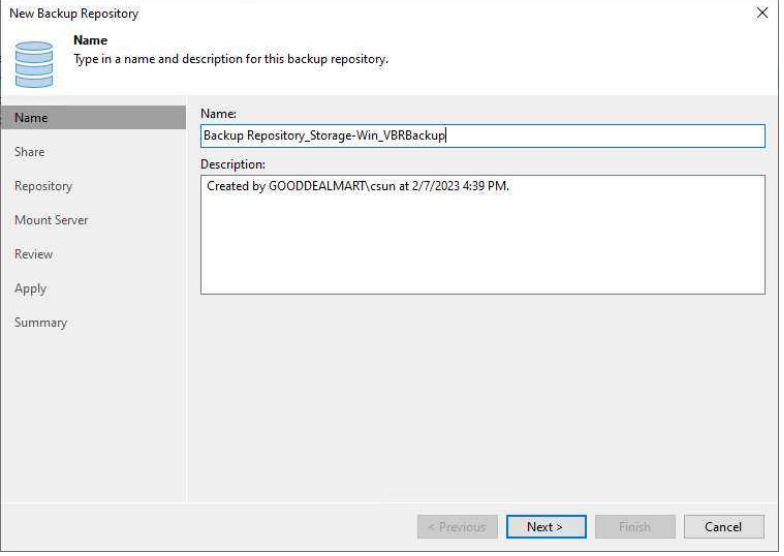
6. On the Add Backup Repository page, select Network attached storage.



7. Select SMB share on the Network Attached Storage.

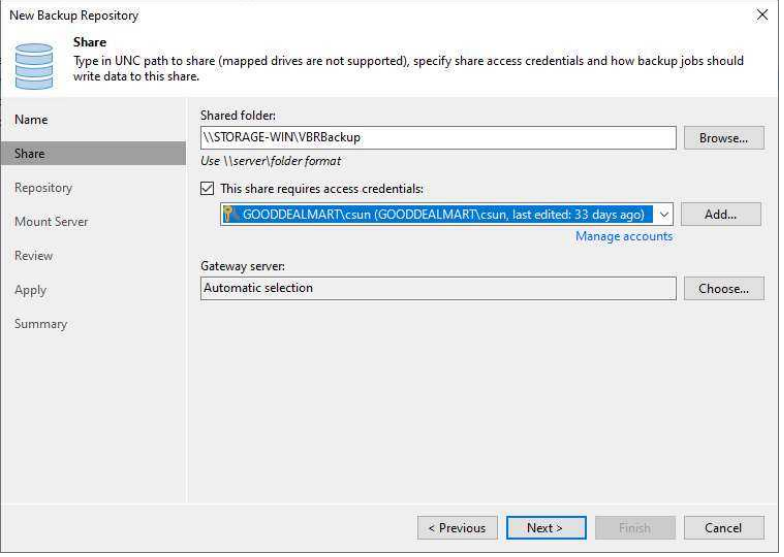


8. On the Name page, specify a Backup Repository name.
9. Give a brief description in the Description field for future reference and click Next.



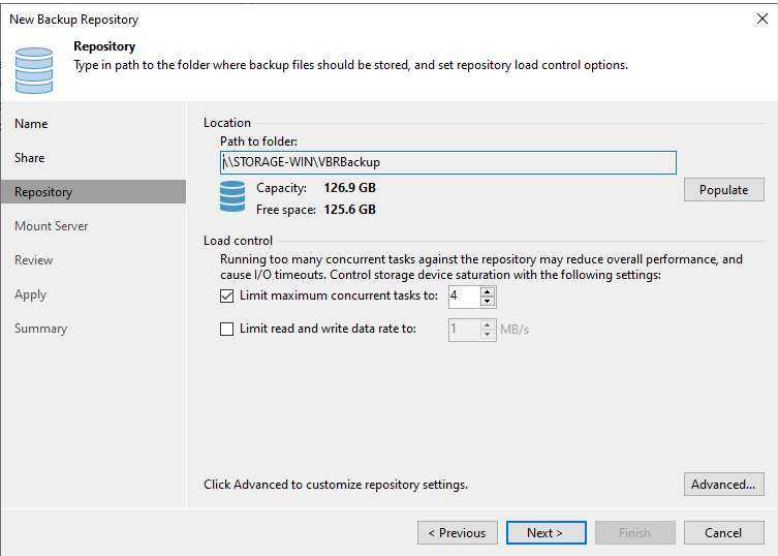
The screenshot shows the 'New Backup Repository' wizard at the 'Name' step. The left sidebar has 'Name' selected. The main area has a 'Name' field with the text 'Backup Repository_Storage-Win_VBRBackup' and a 'Description' field with the text 'Created by GOODDEALMART\csun at 2/7/2023 4:39 PM.'. At the bottom are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

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.



The screenshot shows the 'New Backup Repository' wizard at the 'Share' step. The left sidebar has 'Share' selected. The main area has a 'Shared folder' field with the text '\\STORAGE-WIN\VBRBackup' and a 'Browse...' button. Below it is a checkbox 'This share requires access credentials:' which is checked, and a dropdown menu showing 'GOODDEALMART\csun (GOODDEALMART\csun, last edited: 33 days ago)' with an 'Add...' button. At the bottom are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

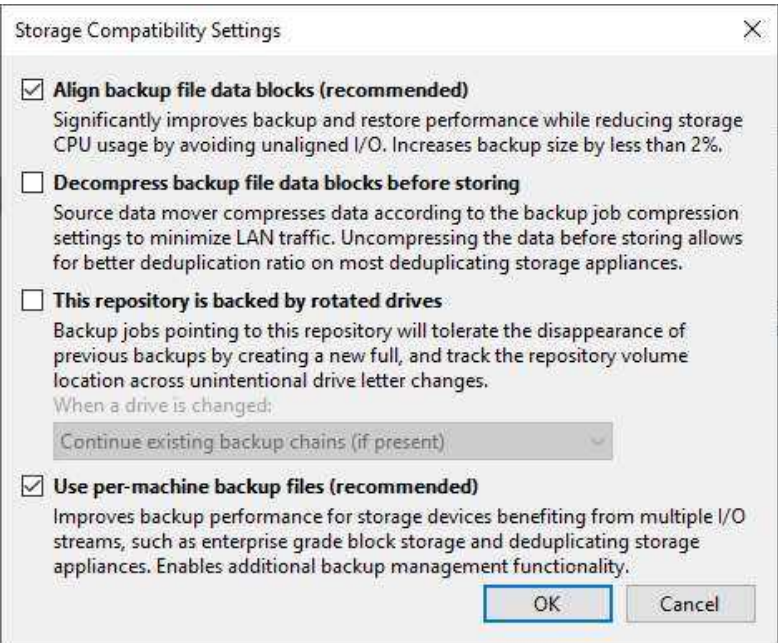
- 14. Use the Load control settings to manage the load on the backup repository and avoid storage I/O timeouts.
- 15. Click Advanced.



- 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.



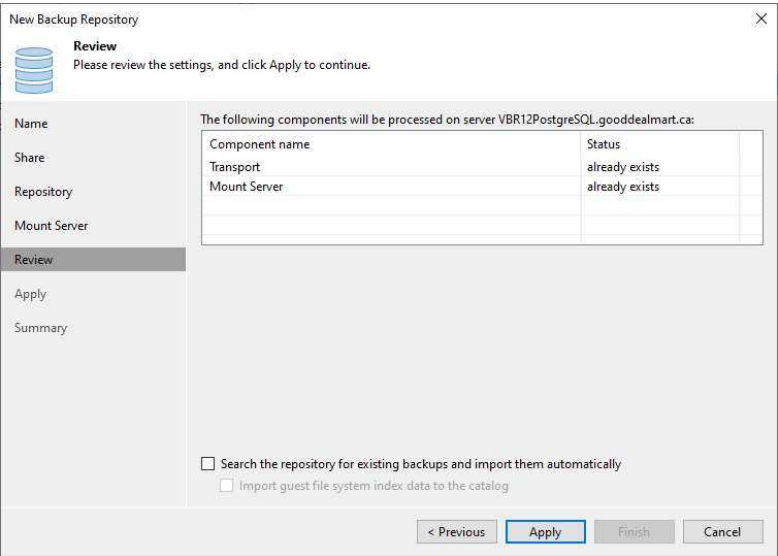
18. Click Next on the Repository page.

The screenshot shows the 'New Backup Repository' wizard, specifically the 'Repository' page. The left sidebar contains a list of steps: Name, Share, Repository (highlighted), Mount Server, Review, Apply, and Summary. The main area is titled 'Repository' and includes the instruction: 'Type in path to the folder where backup files should be stored, and set repository load control options.' Under the 'Location' section, the 'Path to folder:' is set to '\\STORAGE-WIN\VBRBackup'. Below this, the 'Capacity' is 126.9 GB and 'Free space' is 125.6 GB, with a 'Populate' button. The 'Load control' section contains a warning about concurrent tasks and two checkboxes: 'Limit maximum concurrent tasks to:' (set to 4) and 'Limit read and write data rate to:' (set to 1 MB/s). At the bottom, there is an 'Advanced...' button and navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

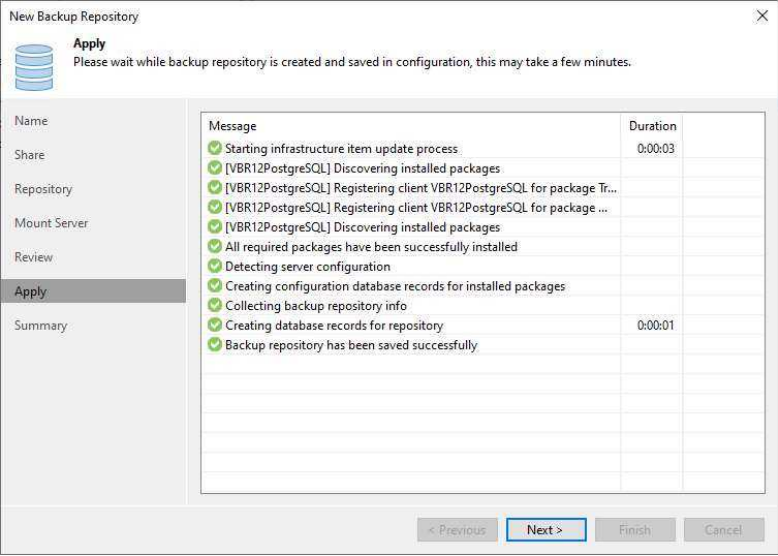
19. Select a mount server from the Mount server drop-down list on the Mount Server page.
20. Select a folder in the Instant recovery write cache folder field for writing cache during mount operations.
21. Unselect Enable vPower NFS service on the mount server because the vPower NFS service is not used for instant recovery to a Microsoft Hyper-V VM.
22. Click Next.

The screenshot shows the 'New Backup Repository' wizard, specifically the 'Mount Server' page. The left sidebar contains a list of steps: Name, Share, Repository, Mount Server (highlighted), Review, Apply, and Summary. The main area is titled 'Mount Server' and includes the instruction: '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.' Under the 'Mount server:' section, a dropdown menu shows 'VBR12PostgreSQL.gooddealmart.ca (Backup server)' with an 'Add New...' button. Below this, the 'Instant recovery write cache folder:' is set to 'C:\ProgramData\Veeam\Backup\IRCaché\'. A 'Browse...' button is next to it. A note states: '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.' There is an unchecked checkbox for 'Enable vPower NFS service on the mount server (recommended)' and a 'Ports...' button. A description below reads: '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.' At the bottom, there are navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

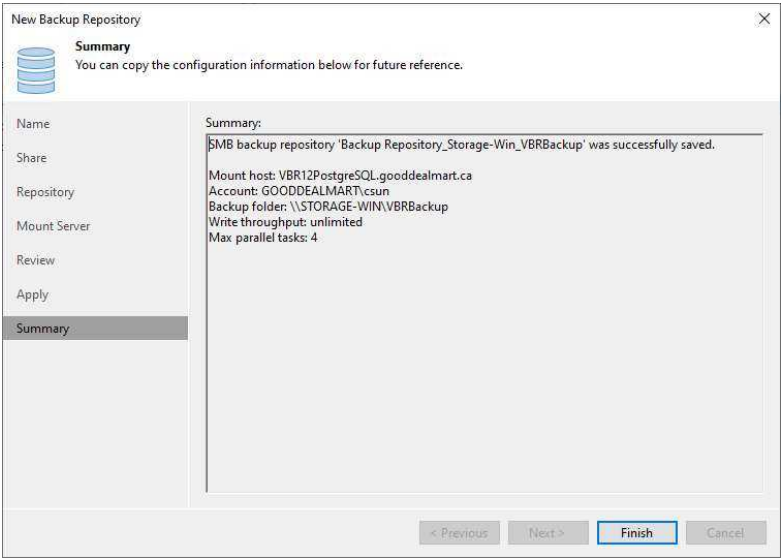
- 23. Click Apply on the Review page.
- 24. Select the Search the repository for existing backups and import them automatically checkbox if the backup repository contains backups previously created with Veeam Backup & Replica on.
- 25. Select the Import guest file system index data to the catalog checkbox if the backup repository contains guest file system index files previously created by Veeam Backup & Replica on.



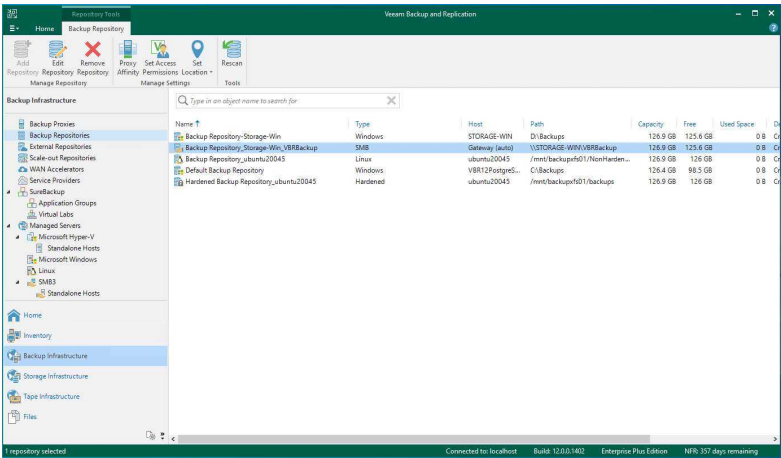
- 26. Click Next on the Apply page.



27. Click Finish on the Summary page.



28. Verify that the Backup Repository has been added.



Add the Microsoft Windows server’s Rotated Drives as a Backup Repository

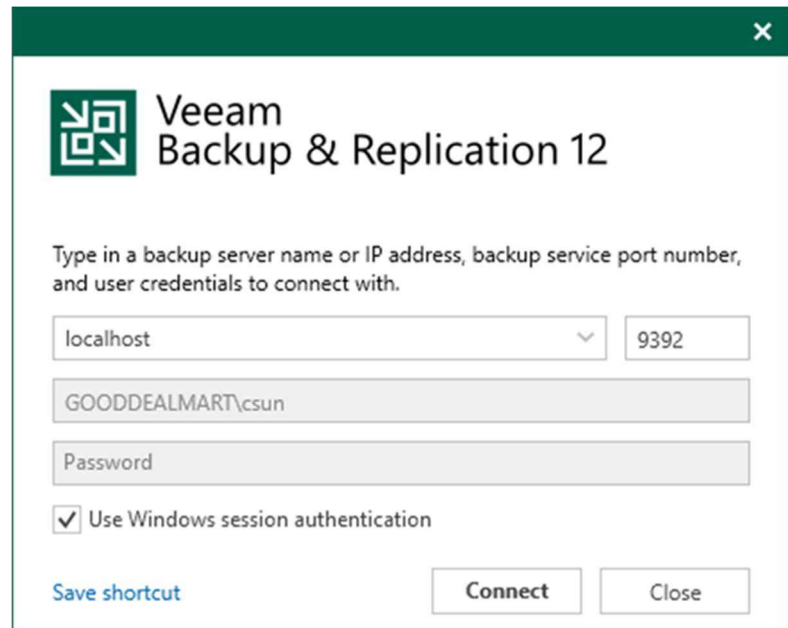
This scenario is helpful if you want to store backups on multiple external hard drives that you intend to move between locations. The drives that are rotated can be detachable USB or eSATA hard drives.

There are some limitations as below:

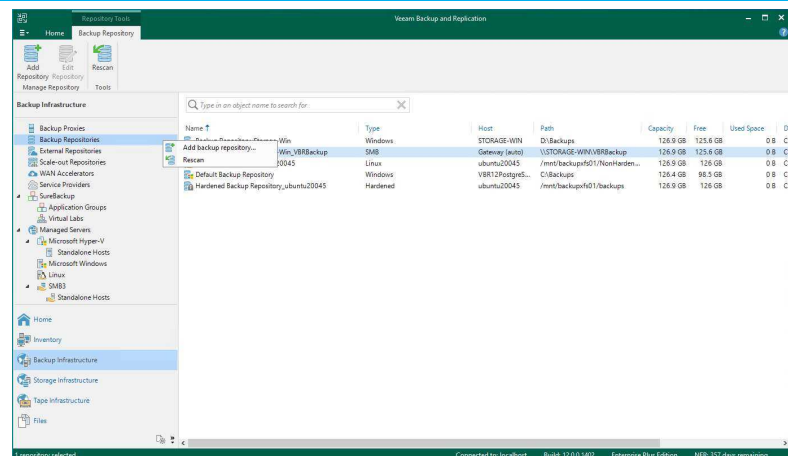
- Only one repository with rotated drives can be created on a single managed server.
- You cannot store archive full backups (GFS backups) created with backup jobs or backup copy jobs in backup repositories with a rotated drive.
- You cannot store per-machine backup files in backup repositories with 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)
--------------	----------------------------

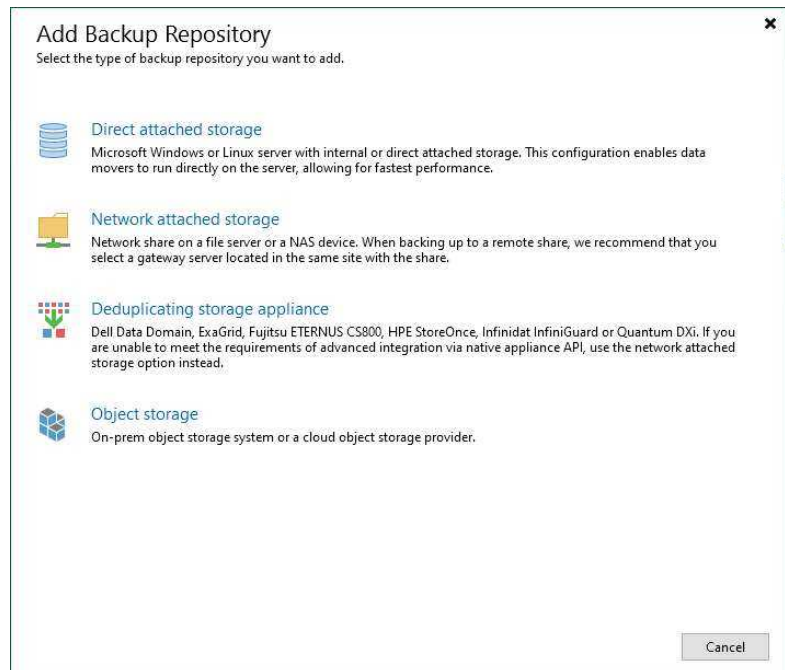
1. Log in to the Veeam Backup and replication manager server.
2. Open the Veeam Backup & Replication Console and click Connect.



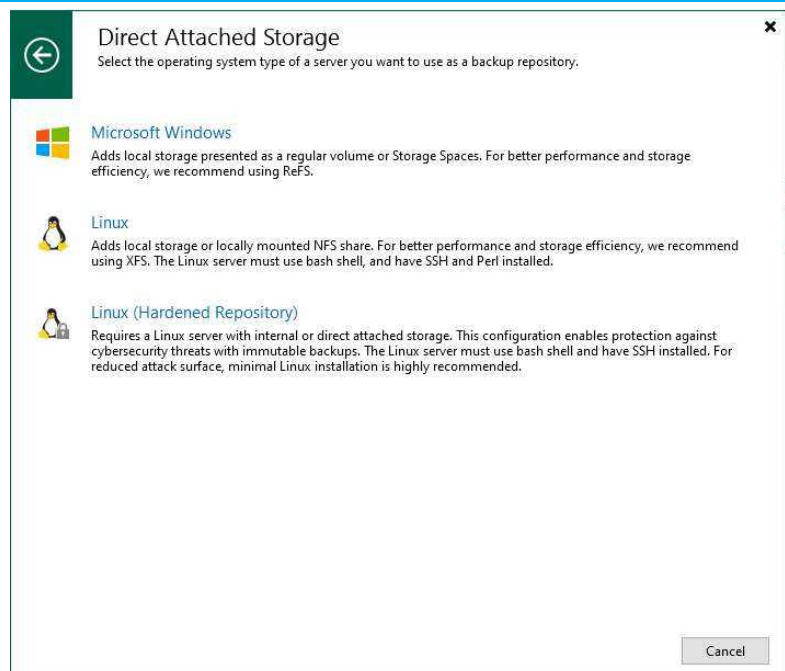
3. Select Backup Infrastructure on the Home page.
4. Select Backup Repositories on the Backup Infrastructure page.
5. Right-click Backup Repositories and select Add backup repository.



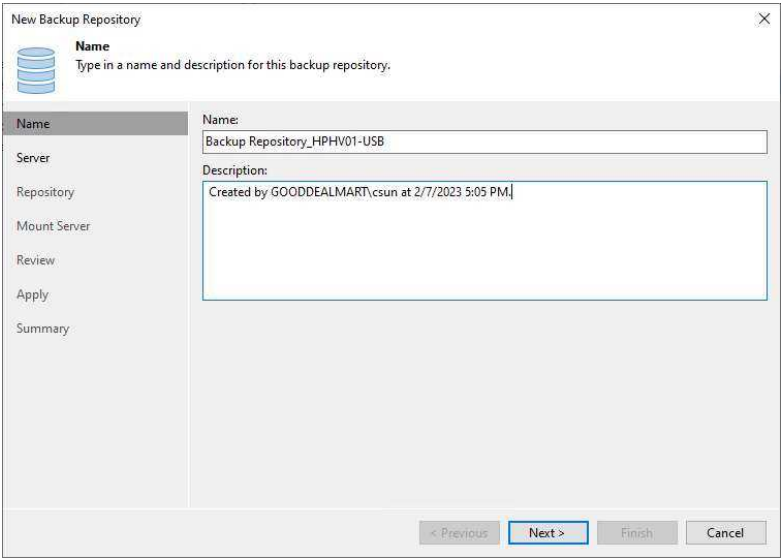
6. Select Direct attached storage on the Add Backup Repository page.



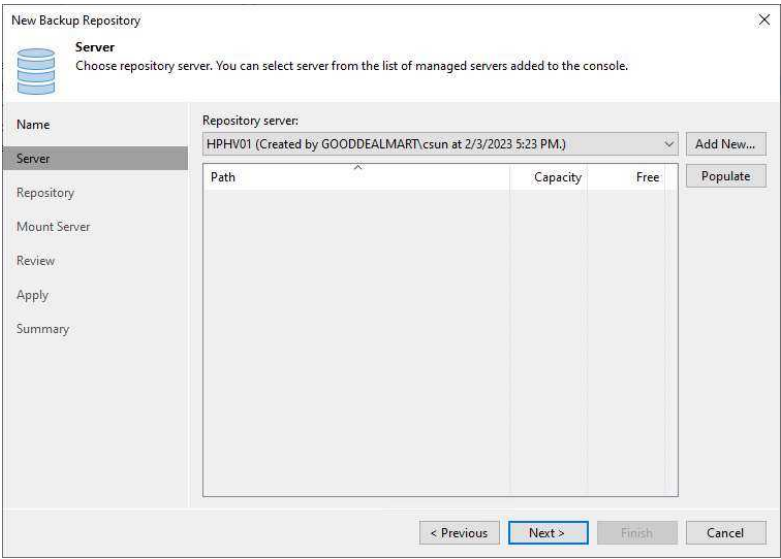
7. Select Microsoft Windows on the Direct Attached Storage page.



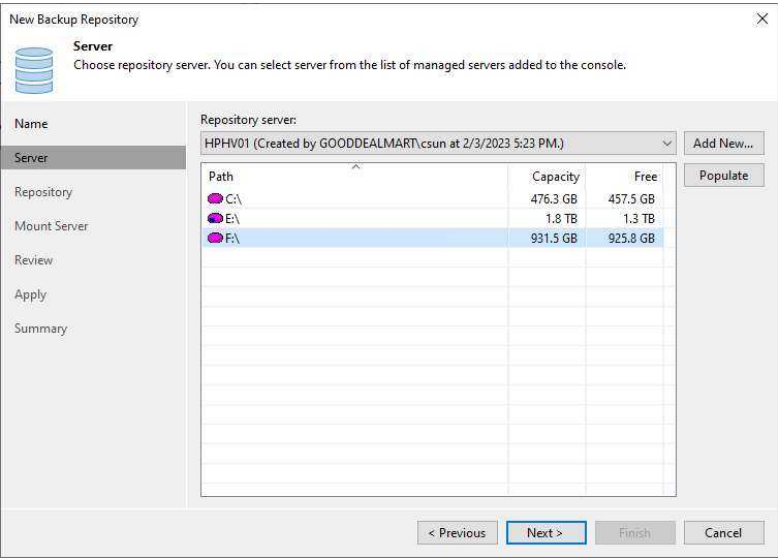
- 8. On the Name page, specify a Backup Repository name.
- 9. Give a brief description in the Description field for future reference and click Next.



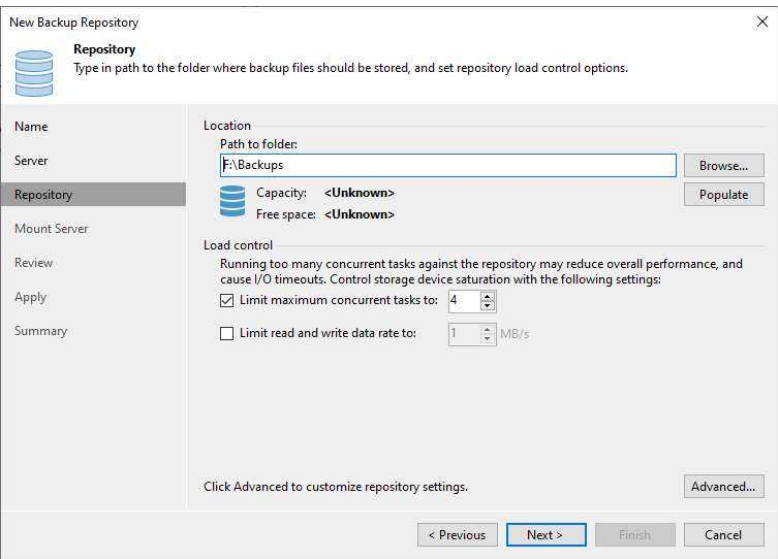
- 10. On the Server page, select the Microsoft Windows server from the Repository server drop-down list and click Populate.



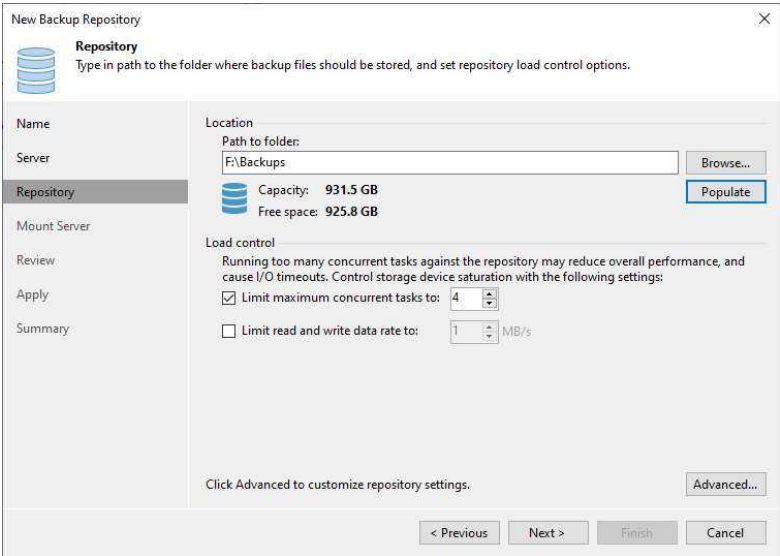
11. Select the disk and click Next.



12. On the Repository page, click Populate to review the disk capacity and free space.



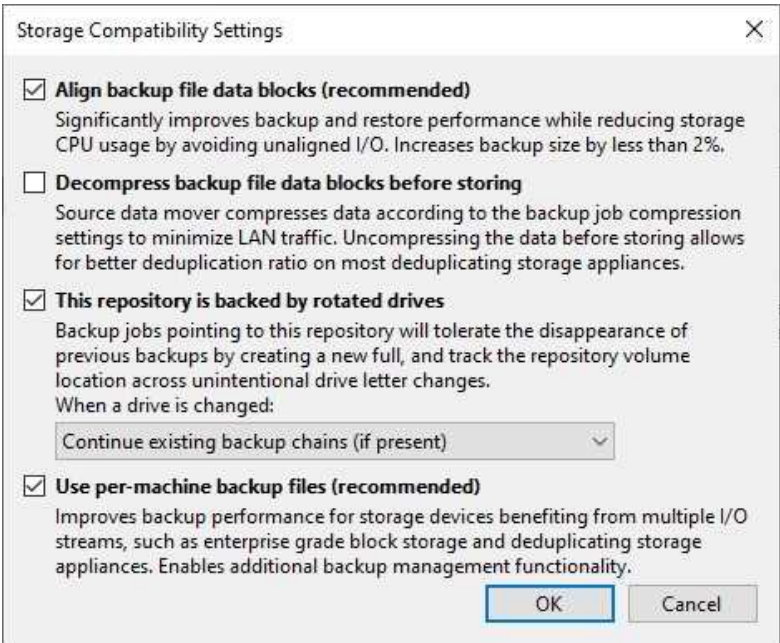
- 13. Use the Load control settings to manage the load on the backup repository and avoid storage I/O timeouts.
- 14. Click Advanced.



- 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 & Replica 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



you use a deduplicating storage feature or appliance.

18. Click Next on the Repository page.

The screenshot shows the 'New Backup Repository' dialog box with the 'Repository' tab selected. The left sidebar contains links for Name, Server, Repository, Mount Server, Review, Apply, and Summary. The main area is titled 'Repository' and includes instructions: 'Type in path to the folder where backup files should be stored, and set repository load control options.' Under 'Location', the 'Path to folder' is set to 'F:\Backups' with a 'Browse...' button. Below this, the capacity is '931.5 GB' and free space is '925.8 GB', with a 'Populate' button. The 'Load control' section has a warning about concurrent tasks and two options: 'Limit maximum concurrent tasks to:' (set to 4) and 'Limit read and write data rate to:' (set to 1 MB/s). An 'Advanced...' button is at the bottom right. Navigation buttons at the bottom are '< Previous', 'Next >', 'Finish', and 'Cancel'.

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

The screenshot shows the 'New Backup Repository' dialog box with the 'Mount Server' tab selected. The left sidebar is the same as the previous screenshot. The main area is titled 'Mount Server' and includes instructions: '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.' Under 'Mount server', a dropdown menu shows 'HPHV01 (Created by GOODDEALMART\csun at 2/3/2023 5:23 PM.)' with an 'Add New...' button. Below this, the 'Instant recovery write cache folder' is set to 'E:\ProgramData\Veeam\Backup\IRCache\' with a 'Browse...' button. A note states: '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.' There is an unchecked checkbox for 'Enable vPower NFS service on the mount server (recommended)' with a 'Ports...' button. A description below reads: '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.' Navigation buttons at the bottom are '< Previous', 'Next >', 'Finish', and 'Cancel'.

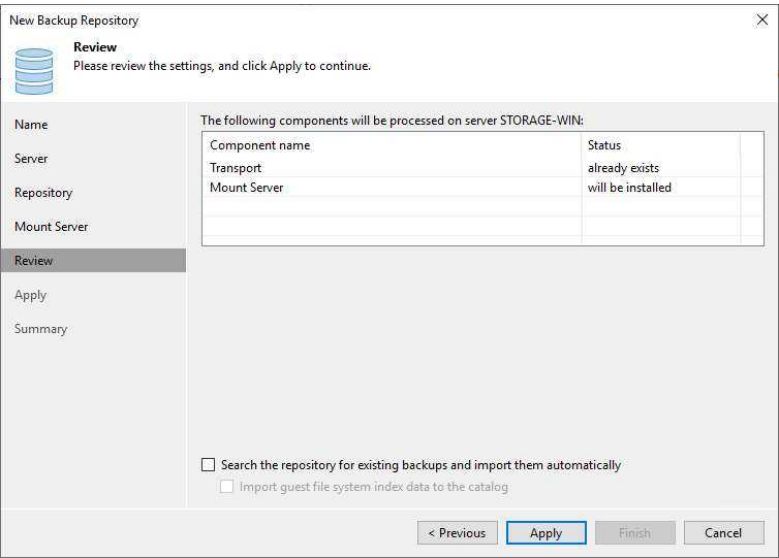
vPower NFS service is not used for instant recovery to a Microsoft Hyper-V VM.

22. Click Next.

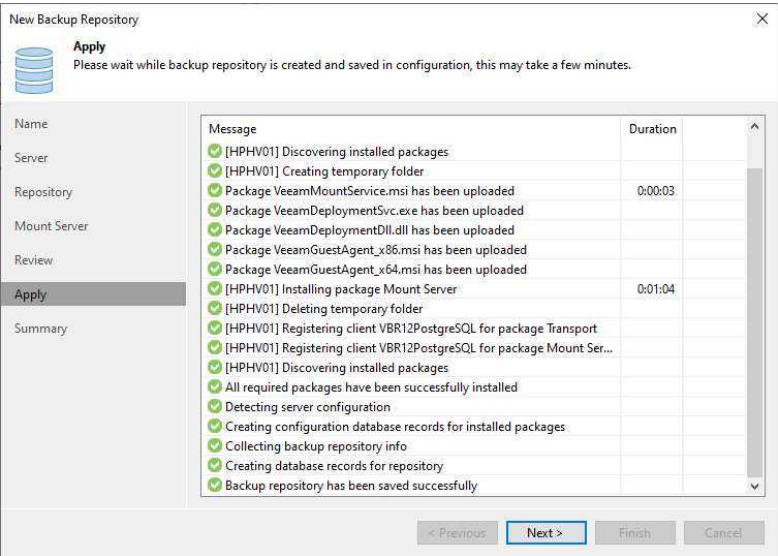
23. Click Apply on the Review page.

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 & Replica on.

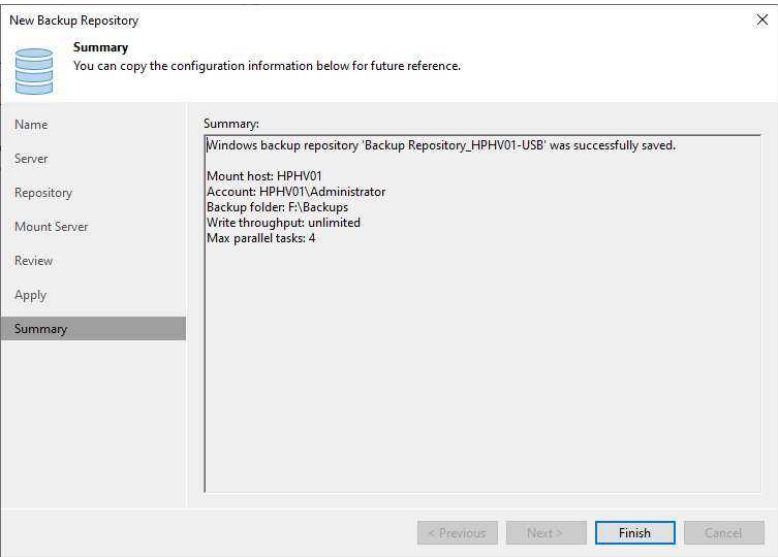
25. Select the Import guest file system index data to the catalog checkbox if the backup repository contains guest file system index files previously created by Veeam Backup & Replica on.



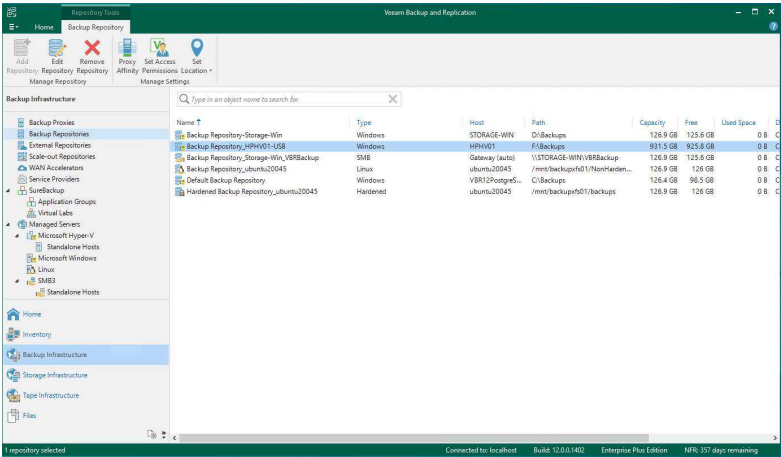
26. Click Next on the Apply page.



27. Click Finish on the Summary page.



28. Verify that the Rotated Drives Backup Repository has been added.



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

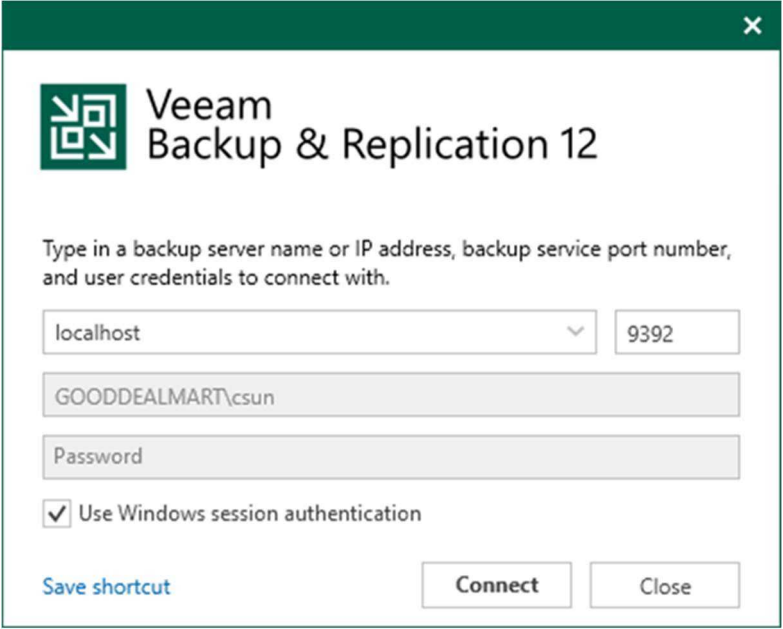
Multi-factor authentication (MFA) is supported by Veeam Backup & Replication for additional user verification. A one-time password (OTP) generated in the mobile authenticator application is a secondary verification method. With login and password credentials, it creates a more secure environment and 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.



The image shows a screenshot of the Veeam Backup & Replication 12 connection dialog box. The dialog has a dark green header bar with the Veeam logo and the text 'Veeam Backup & Replication 12'. Below the header, there is a text prompt: 'Type in a backup server name or IP address, backup service port number, and user credentials to connect with.' The form contains several input fields: a dropdown menu for the server name (currently showing 'localhost'), a text box for the port number (currently showing '9392'), a text box for the username (currently showing 'GOODDEALMART\csun'), and a text box for the password (currently showing 'Password'). There is a checkbox labeled 'Use Windows session authentication' which is checked. At the bottom of the dialog, there are three buttons: 'Save shortcut' (in blue text), 'Connect', and 'Close'.

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

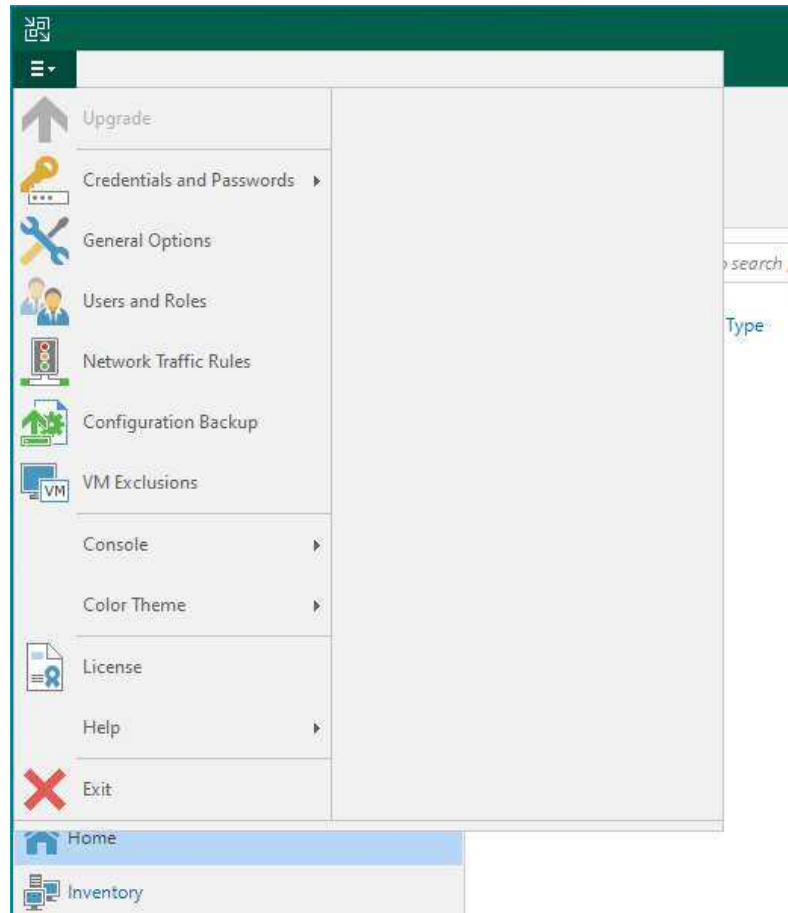
GOODDEALMART\csun

Password

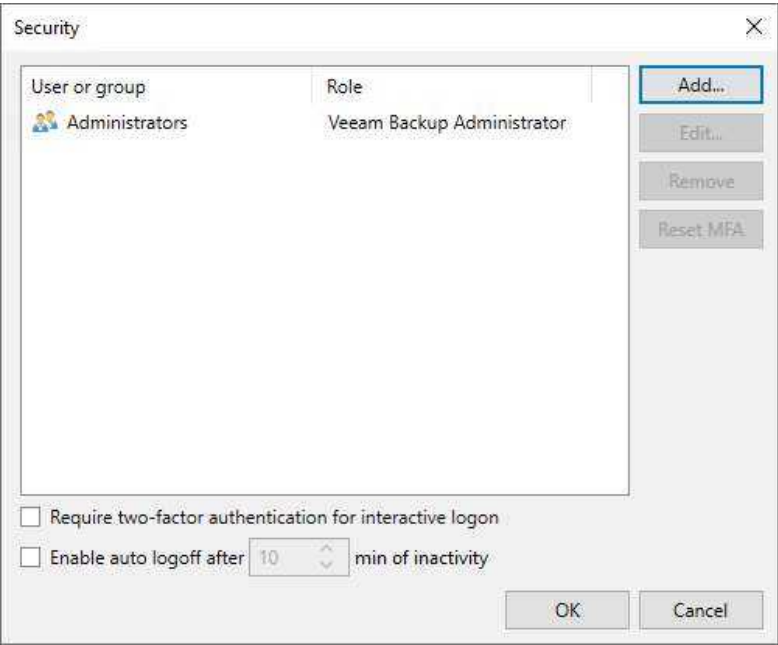
☒ Use Windows session authentication

Save shortcut Connect Close

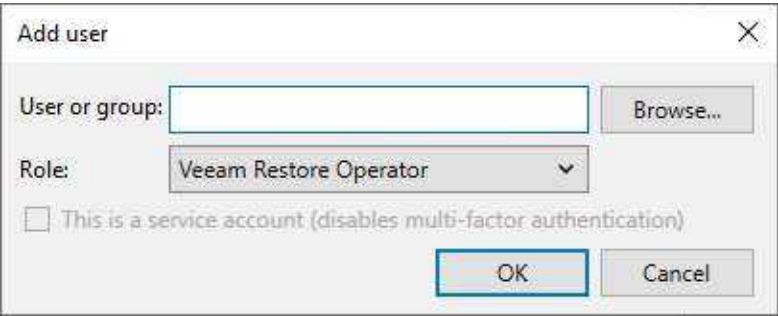
3. Select Users and Roles from the main menu.



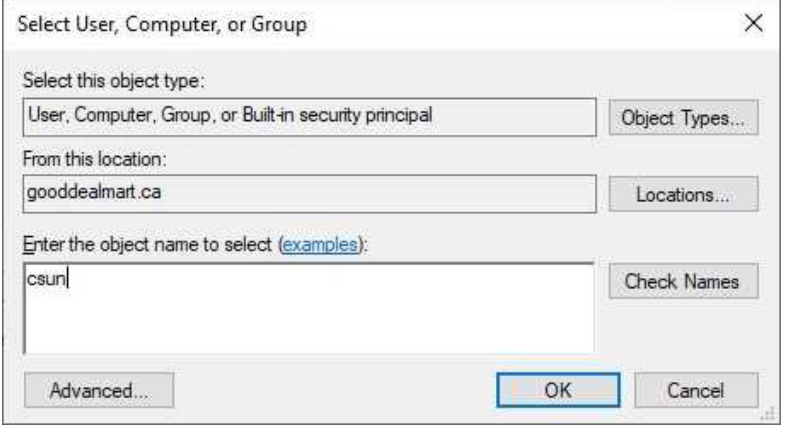
4. Click Add on the Security page.



5. On the Add user page, click Browse in the User or group field.



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

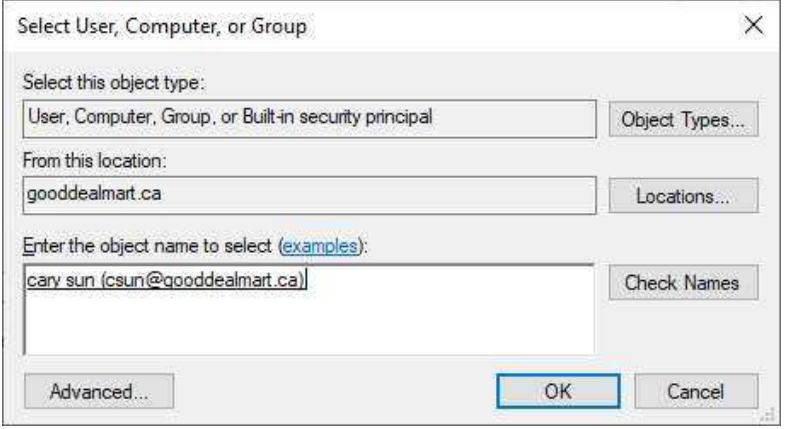
From this location:
gooddealmart.ca

Enter the object name to select (examples):
csun

Check Names

Advanced... OK Cancel

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

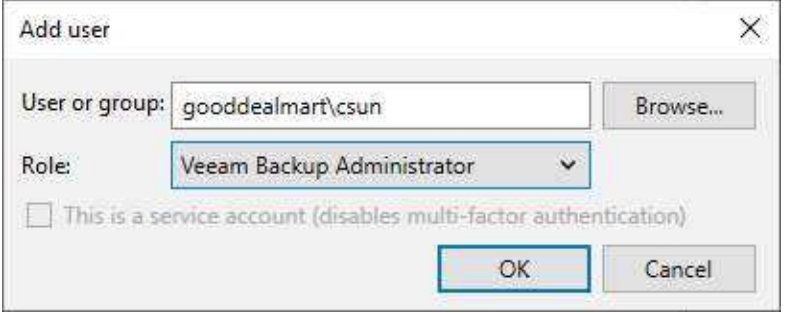
From this location:
gooddealmart.ca

Enter the object name to select (examples):
cary sun (csun@gooddealmart.ca)

Check Names

Advanced... OK Cancel

8. Select a role from the Role drop-down list on the Add user page and click OK.



Add user

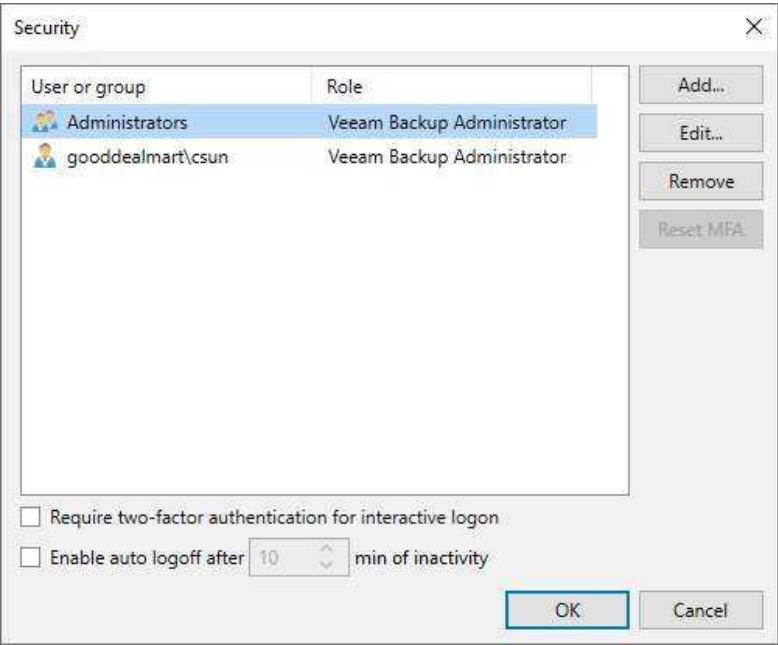
User or group: gooddealmart\csun

Role: Veeam Backup Administrator

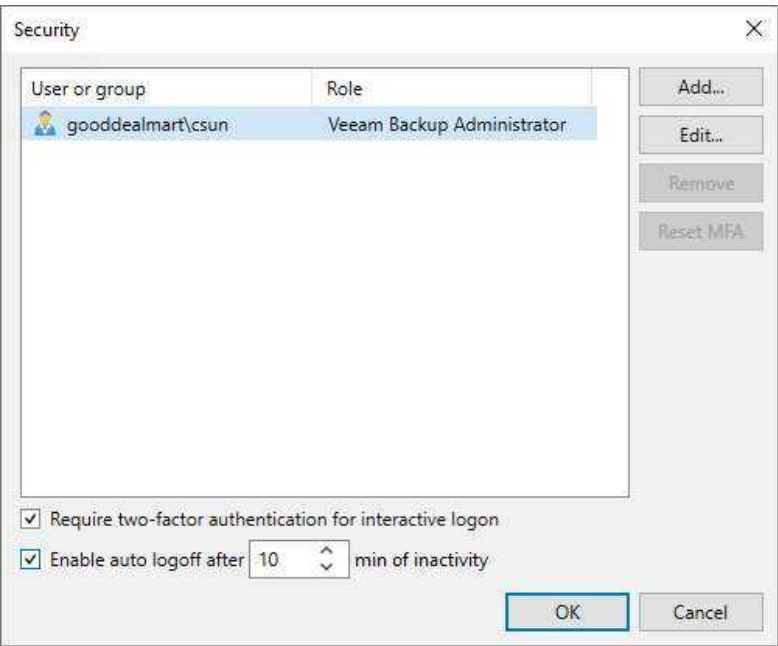
☐ This is a service account (disables multi-factor authentication)

OK Cancel

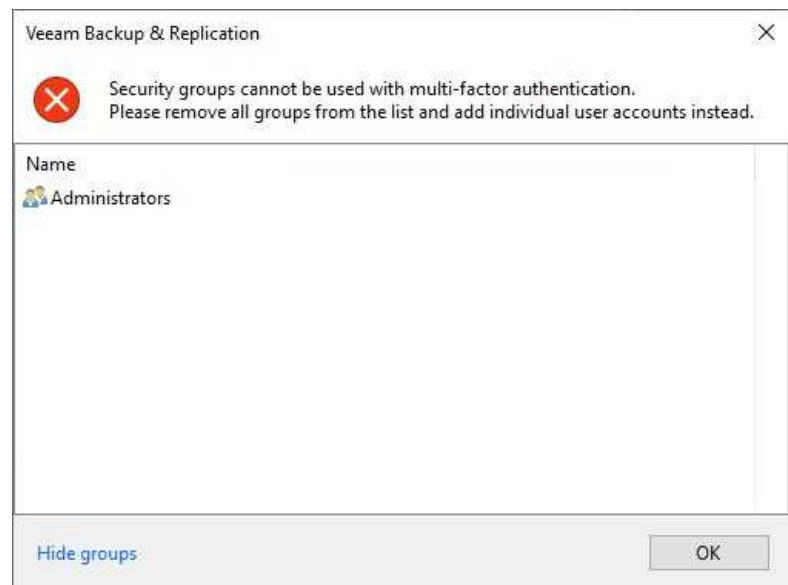
9. On the Security page, select the Administrators group and click Remove.



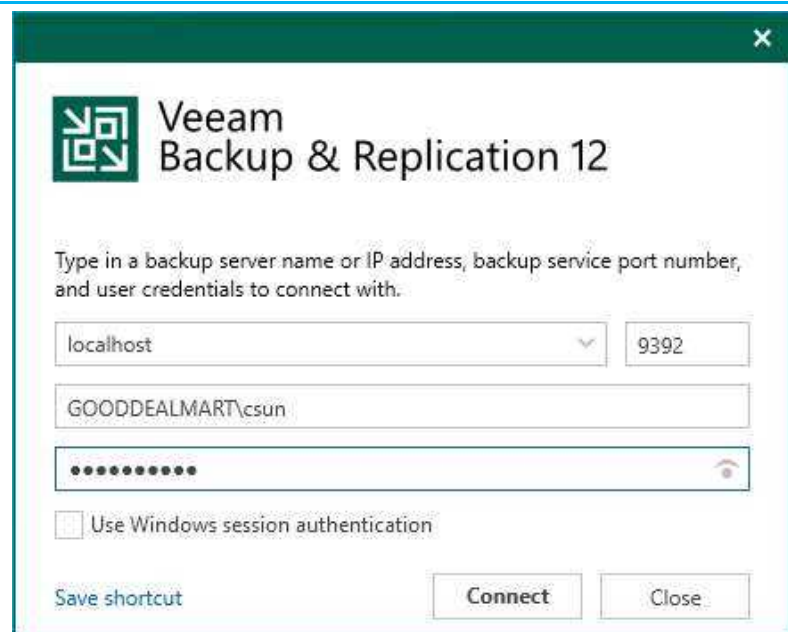
10. Select the new user.
11. Select the Require two-factor authentication for interactive Log in checkbox.
12. Select Enable auto logoff after a period min of inactivity.
13. Click OK.



14. Please remove all unsupported security groups from the list if the error message pops up.



15. Close Veeam Backup and Replica on console and reopen it.
16. Enter the user name and password on the Veeam Backup & Replica on 12 page.

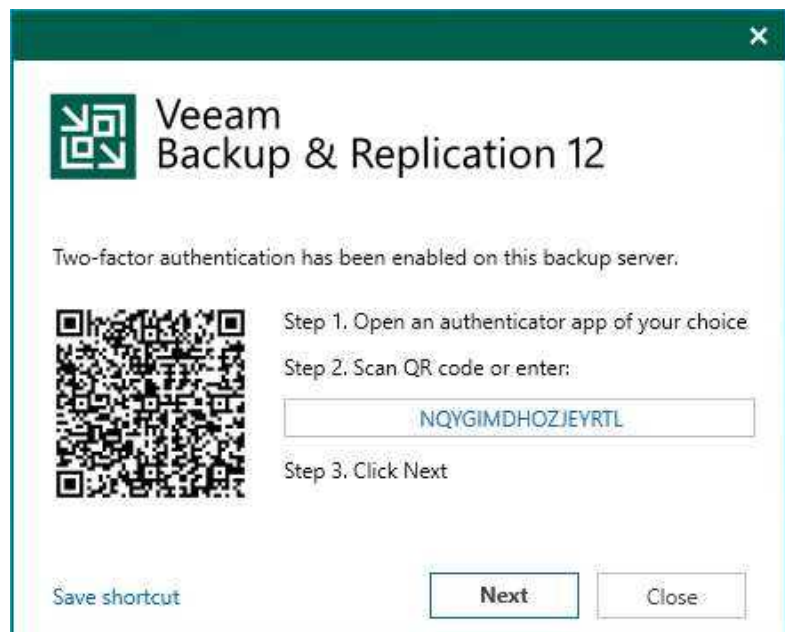


17. Open an Authentication APP from your device and select Add (+).

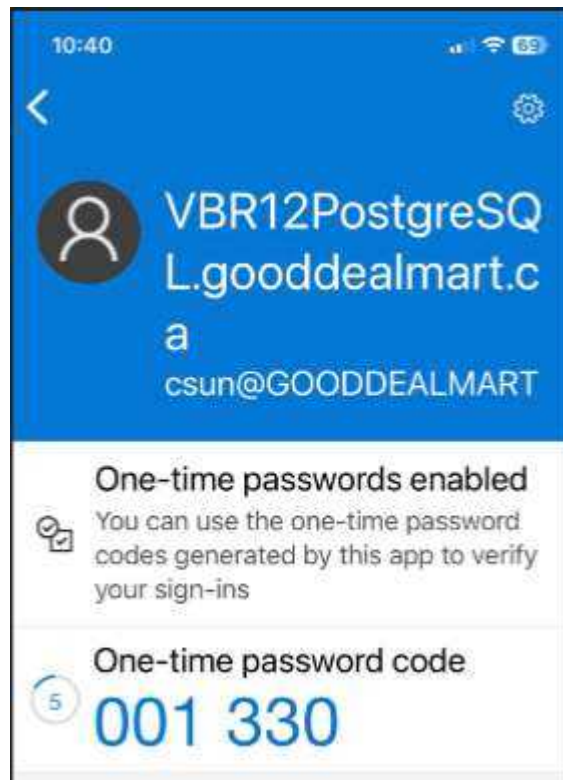
Note:

I have tried Microsoft and Google authentication apps.

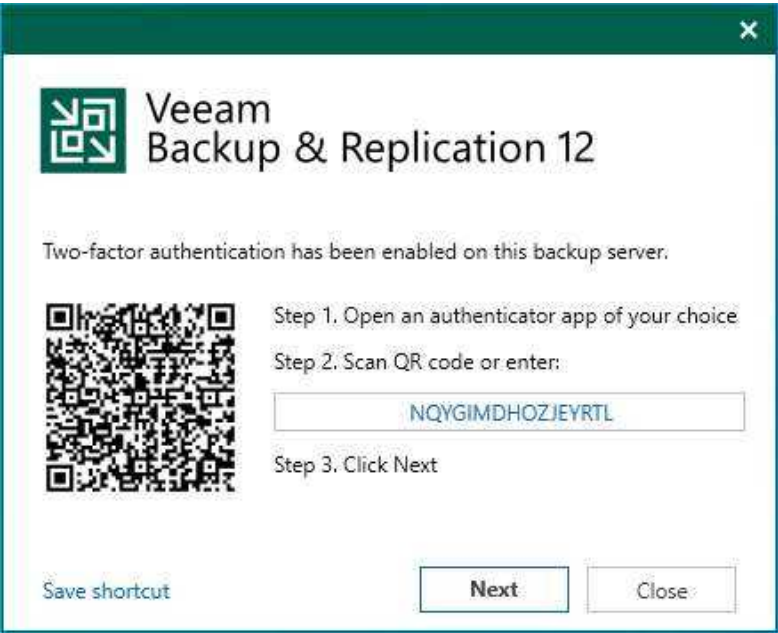
18. Scan the QR code or enter the code.



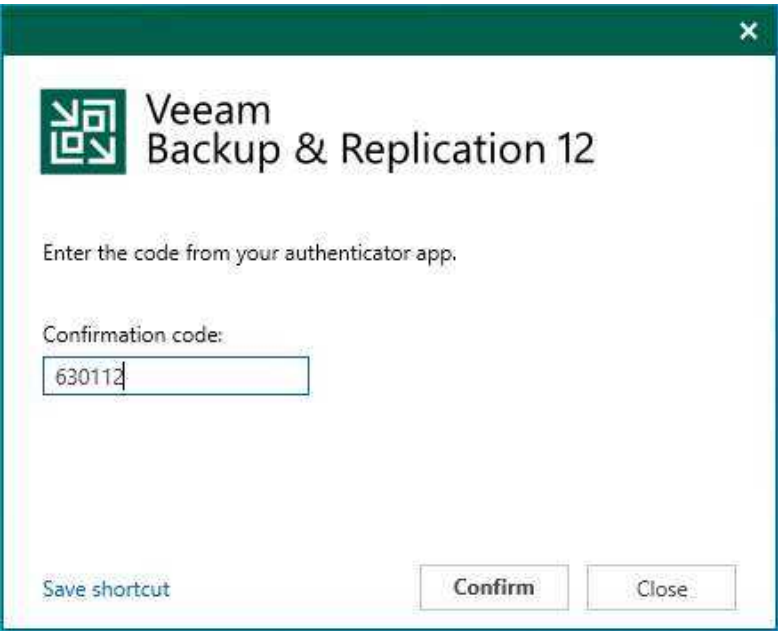
19. Ensure the account add to your device successfully.



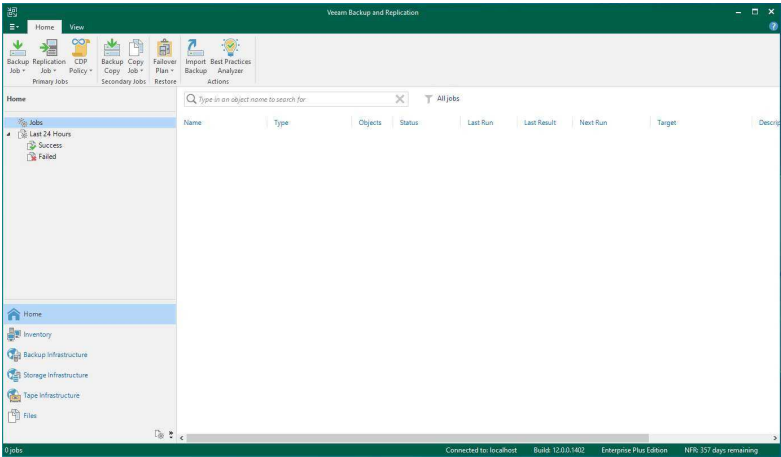
20. Click Next on the Two-factor authentication enabled on this backup server page.



21. Enter the one-time password code in the Confirmation code field and click Confirm.



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:

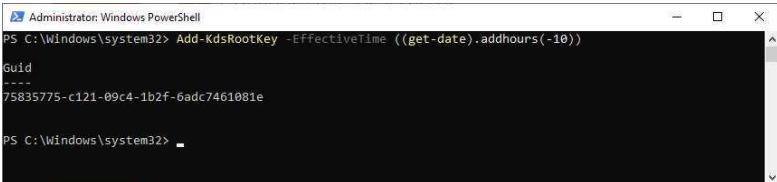
- Microsoft Windows Server 2012 and later support gMSAs.
- Backups of Linux target machines that are members of an Active Directory domain are not supported by gMSAs.
- Because gMSAs require a connection to the domain controller, these accounts can only be accessed via the network.
- If you use a gMSA 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))`



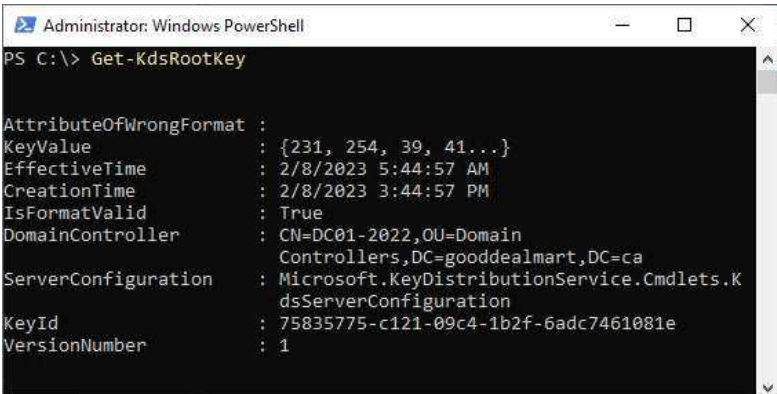
```
Administrator: Windows PowerShell
PS C:\Windows\system32> Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))

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`



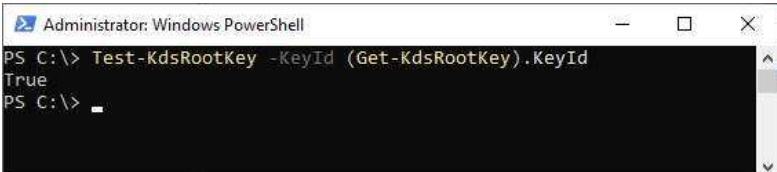
```
Administrator: Windows PowerShell
PS C:\> Get-KdsRootKey

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

PS C:\>
```

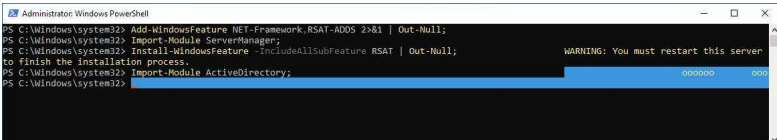
5. Run the cmdlet below to check the KDS key.

`Test-KdsRootKey -KeyId (Get-KdsRootKey).KeyId`



```
Administrator: Windows PowerShell
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;`



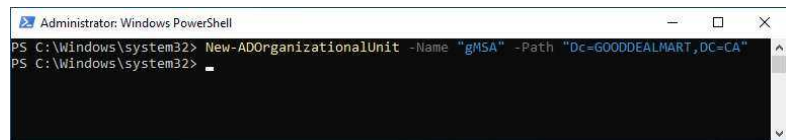
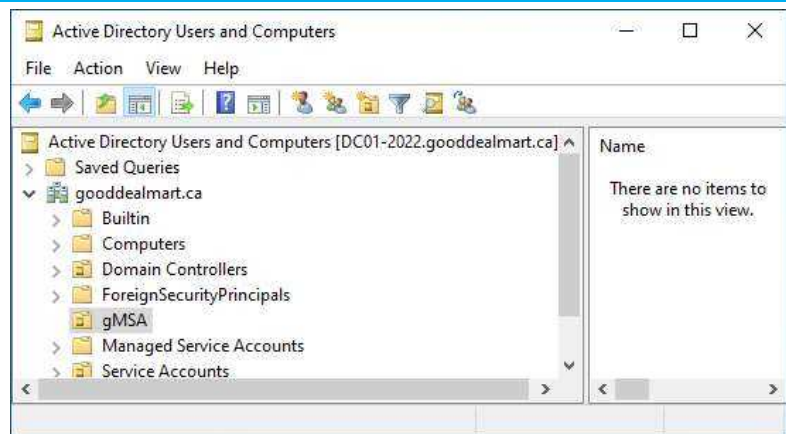
```
Administrator: Windows PowerShell
PS C:\Windows\system32> Add-WindowsFeature NET-Framework,RSAT-ADDS 2>&1 | Out-Null;
PS C:\Windows\system32> Import-Module ServerManager;
PS C:\Windows\system32> Install-WindowsFeature -IncludeAllSubFeature RSAT | Out-Null;
WARNING: You must restart this server to finish the installation process.
PS C:\Windows\system32> Import-Module ActiveDirectory;
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:

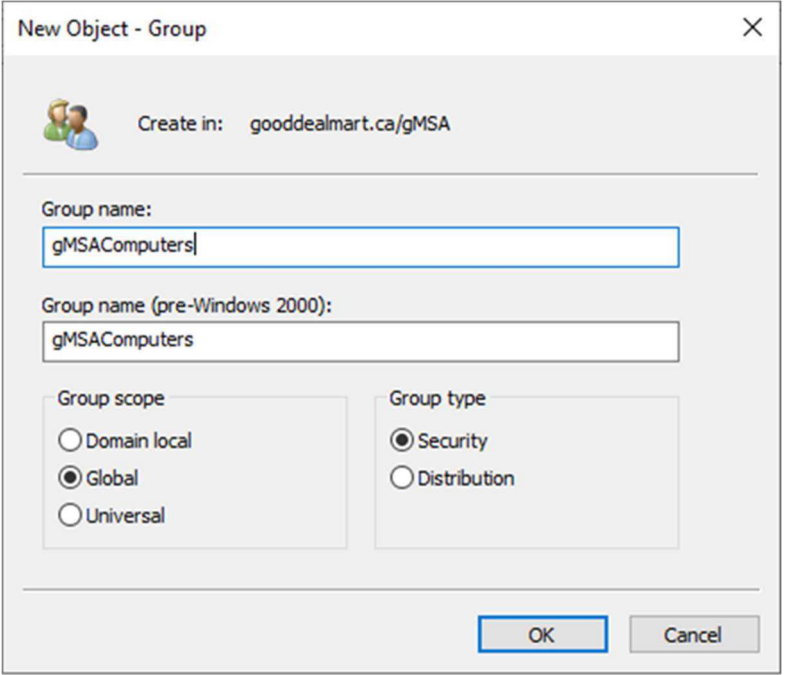
New-ADOrganizationalUnit -
Name "gMSA" -Path
"DC=GOODDEALMART,
DC=CA."



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

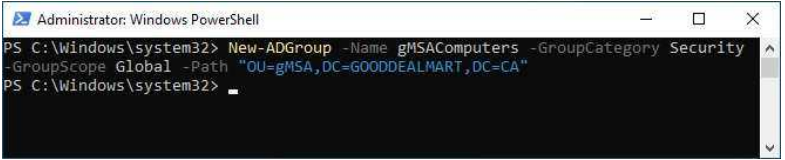
Group scope

☐ Domain local
☒ Global
☐ Universal

Group type

☒ Security
☐ Distribution

OK Cancel

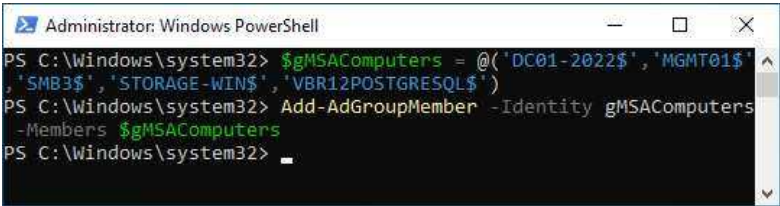
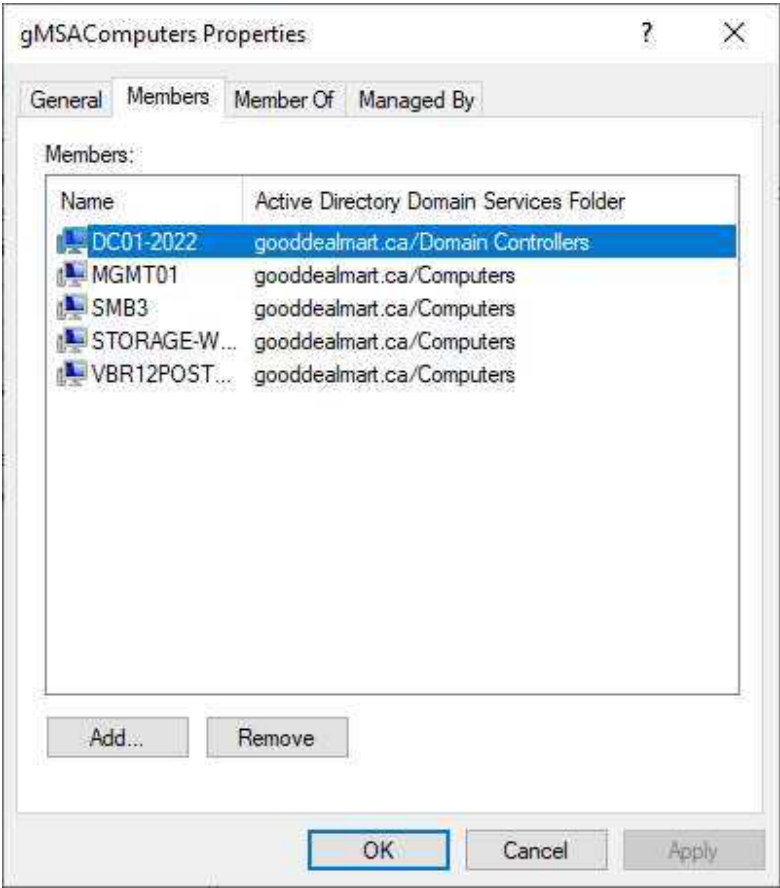


```
Administrator: Windows PowerShell  
PS C:\Windows\system32> New-ADGroup -Name gMSAComputers -GroupCategory Security  
-GroupScope Global -Path "OU=gMSA,DC=GOODDEALMART,DC=CA"  
PS C:\Windows\system32>
```

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



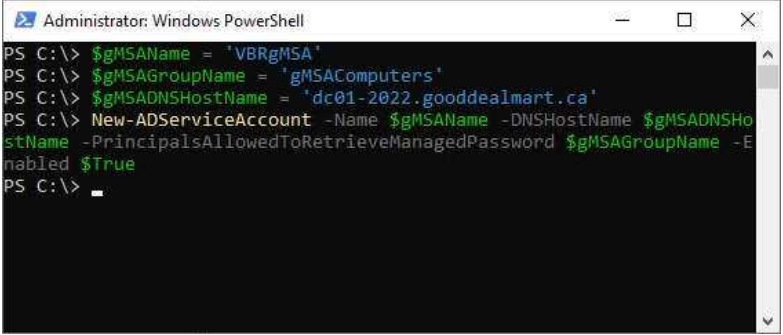
13. Open Windows

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
veManagedPassword
$gMSAGroupName -
Enabled $True
```



```
Administrator: Windows PowerShell
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:\>
```

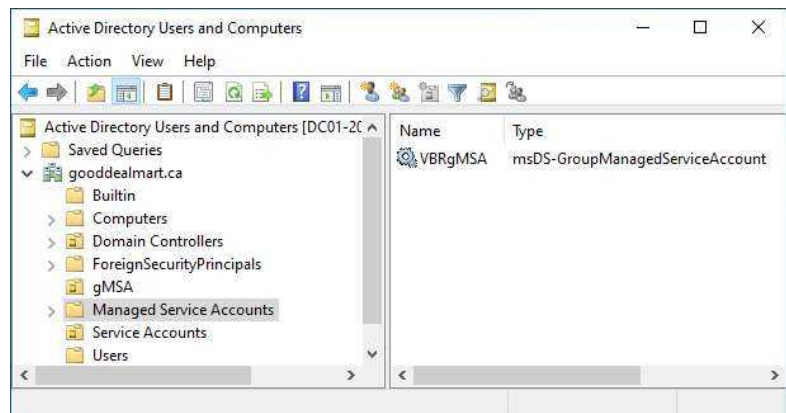
15. Select the Active

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:

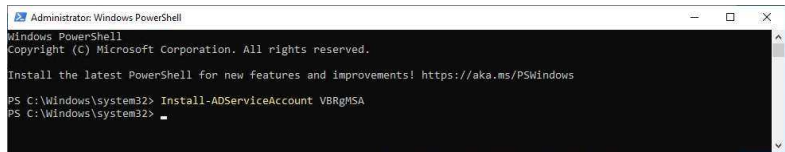
Use separate gMSAs accounts for cri cal



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



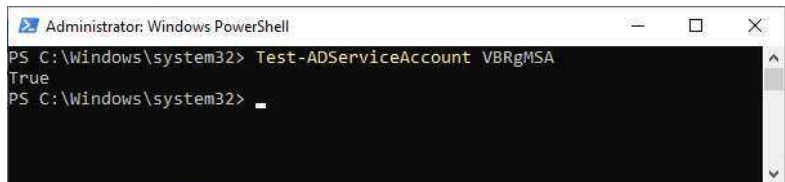
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (c) Microsoft Corporation. All rights reserved.

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.

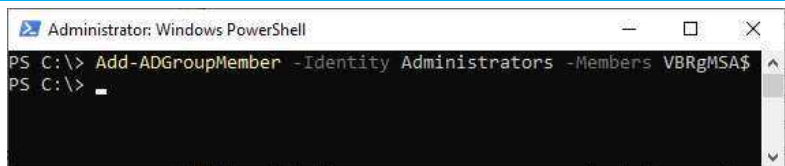
Test-ADServiceAccount
VBRgMSA



```
Administrator: Windows PowerShell
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.

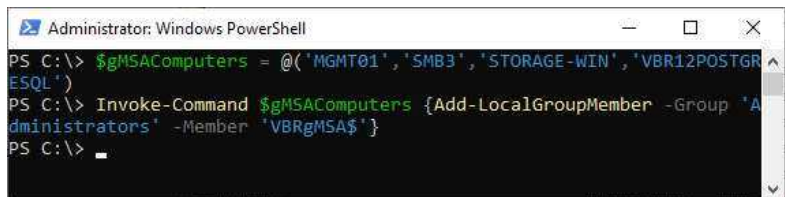
Add-ADGroupMember -
Identity Administrators -
Members VBRgMSA\$



```
Administrator: Windows PowerShell
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



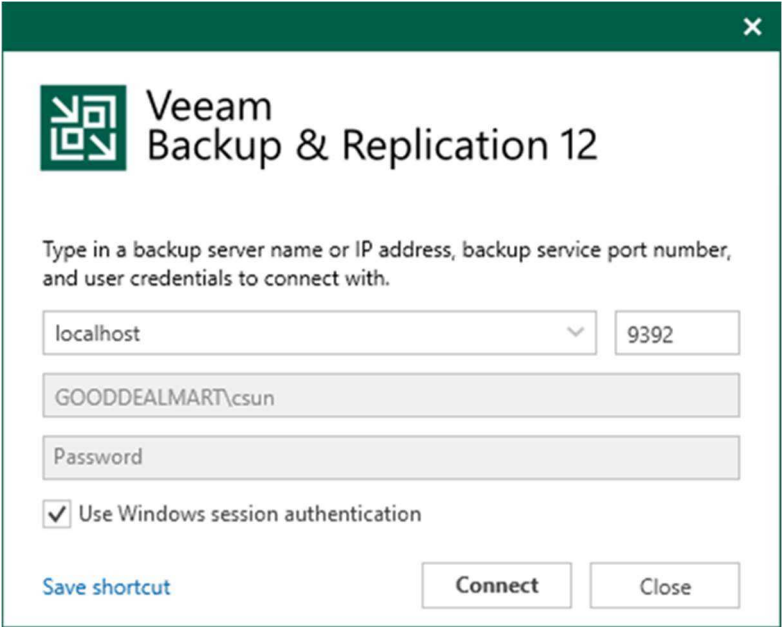
```
Administrator: Windows PowerShell
PS C:\> $gMSAComputers = @('MGMT01','SMB3','STORAGE-WIN','VBR12POSTGR
ESQL')
PS C:\> Invoke-Command $gMSAComputers {Add-LocalGroupMember -Group 'A
dministrators' -Member 'VBRgMSA$'}
PS C:\>
```



```
RAGE-  
WIN','VBR12POSTGRESQL'  
)
```

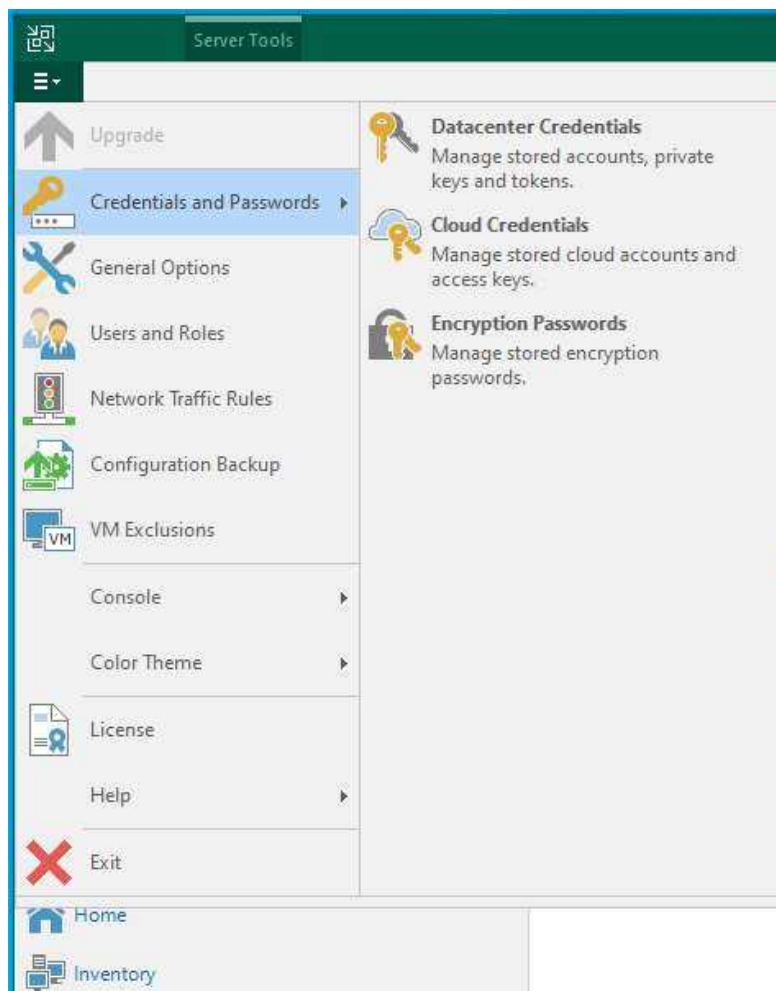
```
Invoke-Command  
$gMSAComputers {Add-  
LocalGroupMember -  
Group 'Administrators' -  
Member 'VBRgMSA$'}
```

21. Log in to the Veeam Backup and replication manager server.
22. Open the Veeam Backup & Replication Console and click Connect.

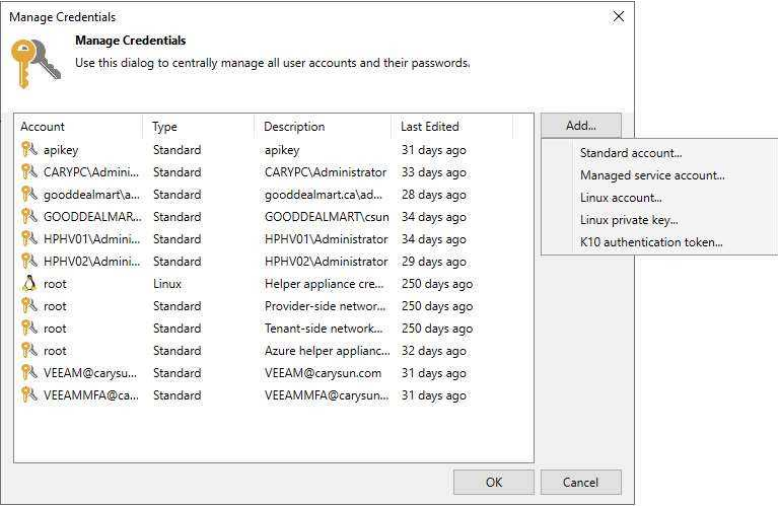


The screenshot shows a window titled "Veeam Backup & Replication 12" with a dark green header bar containing a close button (X). The window has a white background with the Veeam logo (a green square with white geometric patterns) on the left. Below the logo, the text "Veeam Backup & Replication 12" is displayed. A instruction text reads: "Type in a backup server name or IP address, backup service port number, and user credentials to connect with." Below this, there are three input fields: a dropdown menu showing "localhost" with a downward arrow, a text box containing "9392", and a text box containing "GOODDEALMART\csun". Below these fields is a text box labeled "Password". At the bottom left, there is a checked checkbox labeled "Use Windows session authentication". At the bottom right, there are three buttons: "Save shortcut" (in blue text), "Connect" (in a white box with a green border), and "Close" (in a white box with a green border).

23. Select Credentials and Passwords from the main menu.
24. Select Datacenter Credentials.

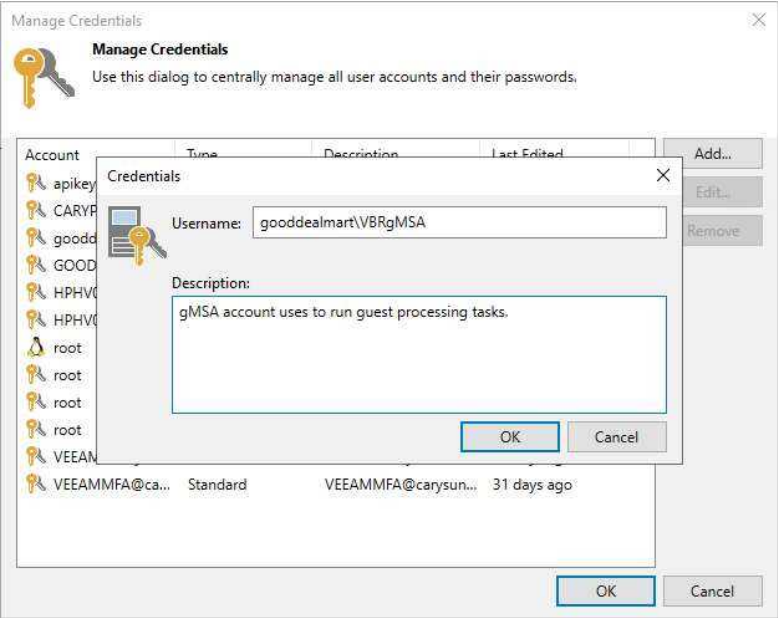


25. Click Add on the Manage Credentials page and select Managed service account.

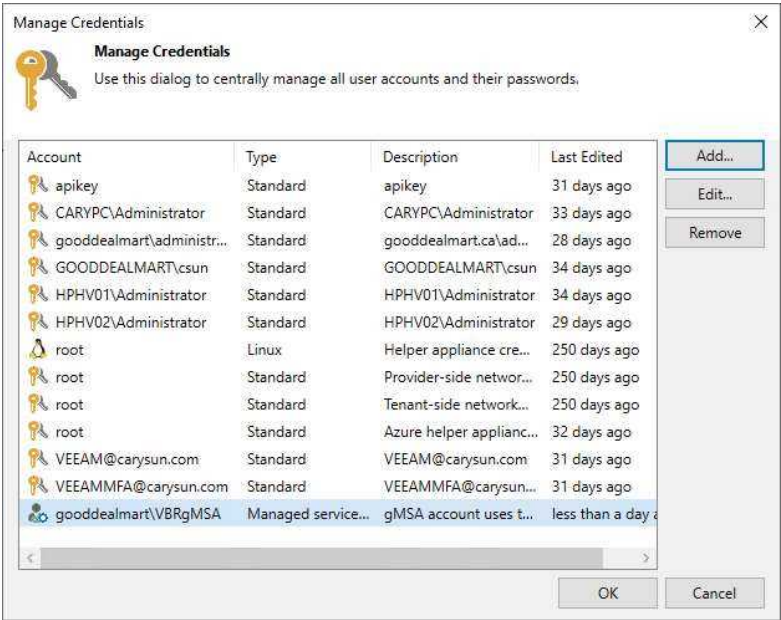


26. Enter the new gMSA account in the Username field on the Credentials page.

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

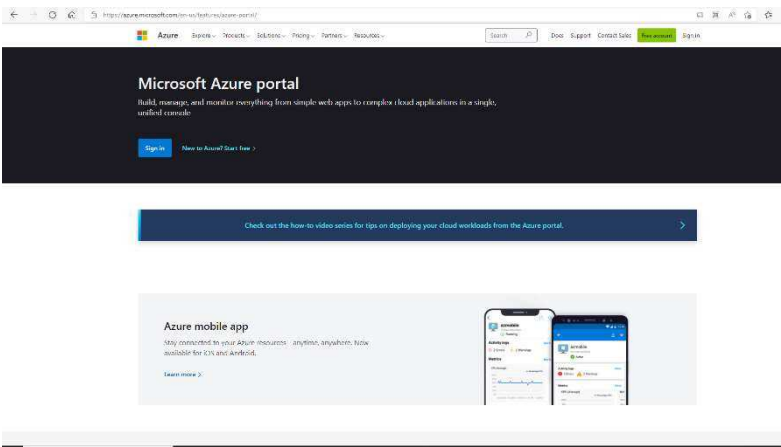
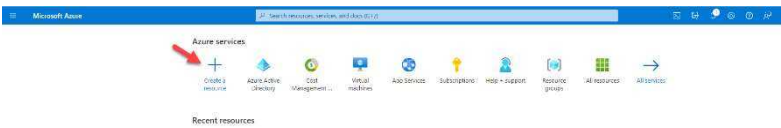


28. Ensure the gMSA account is added to the Manage Credentials page and click OK.

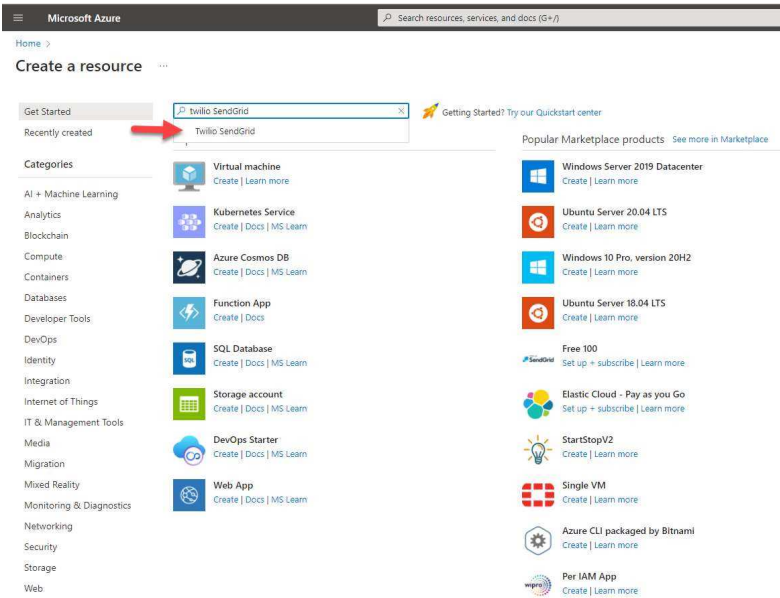


Configure Notification with Free SendGrid Account of Azure

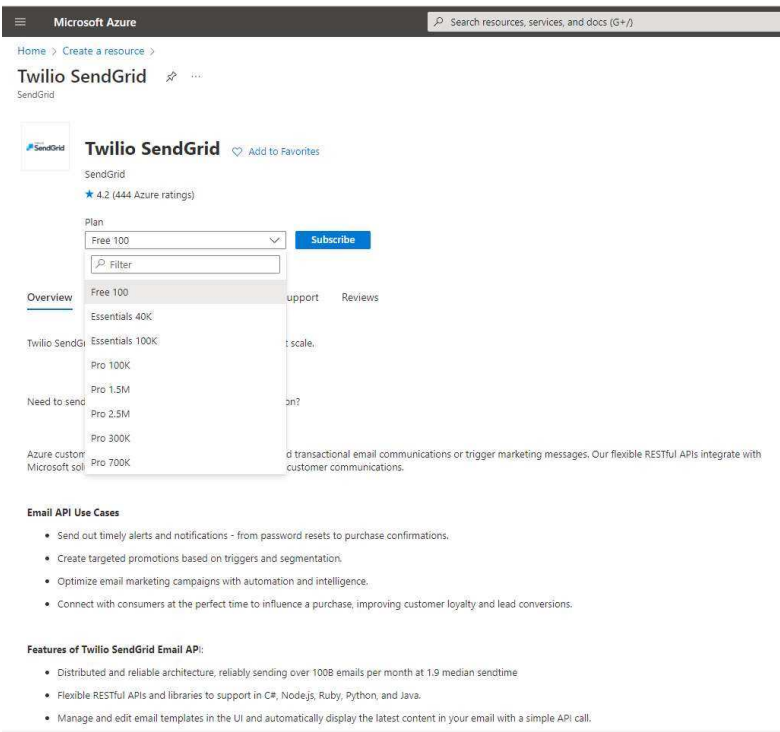
You can configure the SendGrid account as an SMTP relay for notification settings if you want Veeam Backup & Replica to send email notifications about backup job results.

Instructions	Screenshot (if applicable)
1. Sign in Azure portal with a global admin account. https://portal.azure.com	
2. On the Azure services page, select +Create resource.	

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.



5. On the Create SendGrid Account page, select Basics, fill in all the information and then click Next: Tags.

Microsoft Azure

Search resources, services, and docs (G+)

[Home](#) > [Create a resource](#) > [Twilio SendGrid](#) >

Subscribe To Twilio SendGrid

Subscribe to plan

* Basics Tags Review + subscribe

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 *

Resource group *

Microsoft Azure Sponsorship

SendGrid

[Create new](#)

SaaS details

Name *

Plan

TwilioSendGridFree100

Free 100 - 1-month
Try it out! Integrate fast and explore features with 100 emails/day forever.
[Change plan](#)

Billing term

Price + payment options

Subtotal

Recurring billing

1-month

CA\$0/one-time payment

CA\$0

☒ On
☐ Off

Review + subscribe

< Previous

Next: Tags >

- 6. On the Tags page, click
Next: Review + subscribe.

Microsoft Azure

Search resources, services, or documentation

[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 >

- 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

Basics Tags **Review + subscribe**

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 ✓

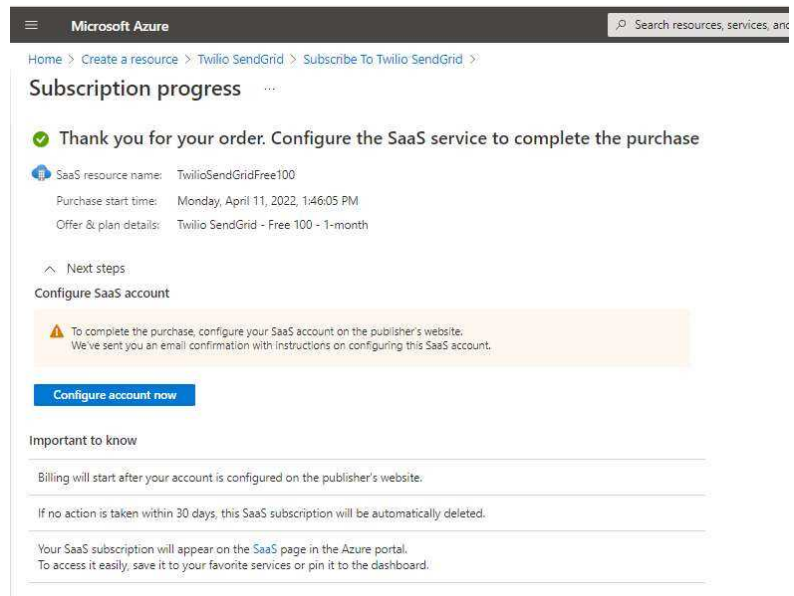
Basics

Subscription	Microsoft Azure Sponsorship
Resource Group	SendGrid
Name	TwilioSendGridFree100
Plan	Free 100
Billing term	1-month
Price + payment options	CAD\$0/one-time payment
Subtotal	CAD\$0
Recurring billing	On

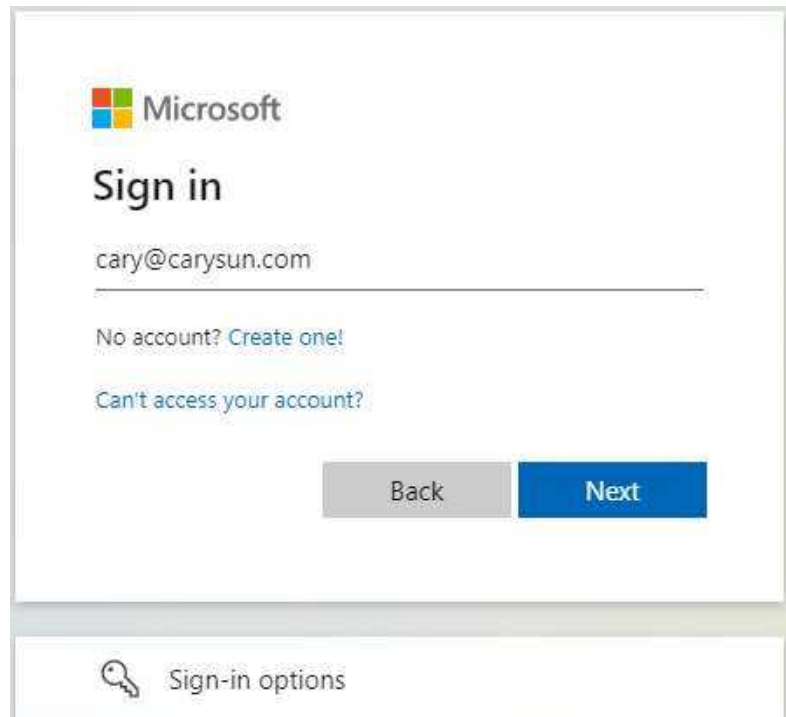
After subscribing, remember to configure your SaaS account on the publisher's website.

[Subscribe](#) [< Previous: Tags](#) [Next >](#)

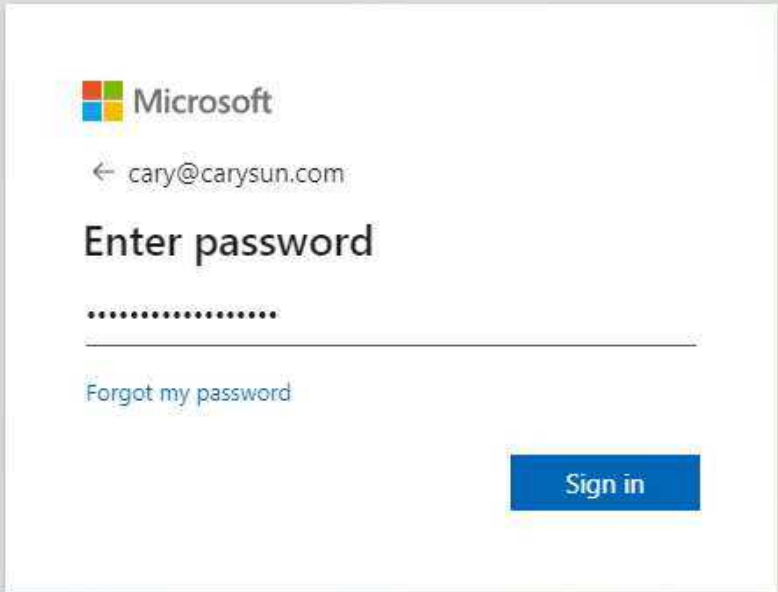
- On the Configure SaaS account page, click **Configure account now**.



- On the Microsoft Sign-in page, enter your account name and click **Next**.



10. Enter a password, and click Sign in.

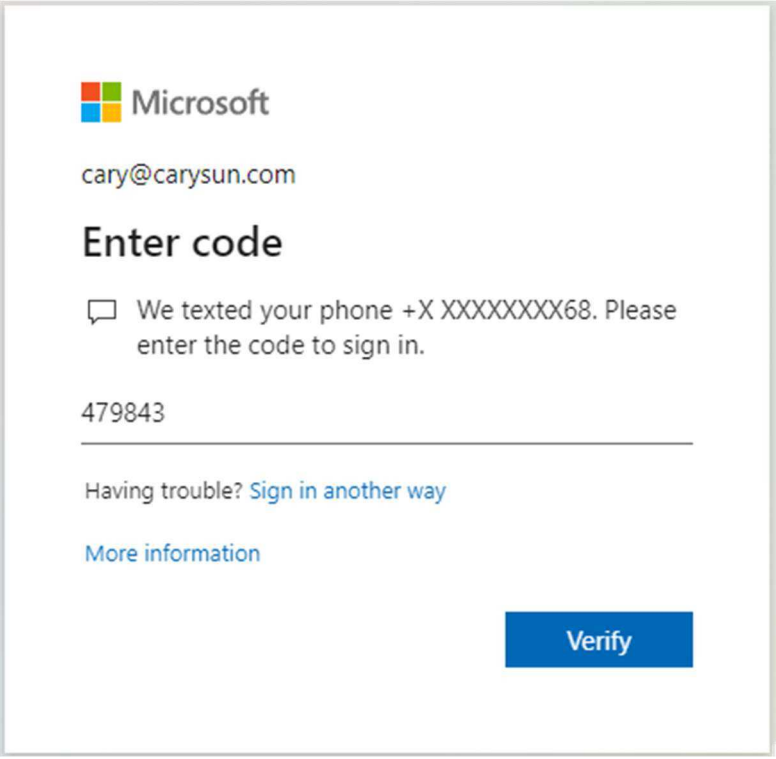


The image shows a Microsoft sign-in page. At the top left is the Microsoft logo. Below it, the email address 'cary@carysun.com' is displayed with a back arrow to its left. The main heading is 'Enter password'. Below this is a password input field represented by a series of dots. Under the password field is a link that says 'Forgot my password'. In the bottom right corner, there is a blue rectangular button with the text 'Sign in' in white.

11. On the Verify your identity page, select the identity method.



12. Enter the code, and click Verify.



A screenshot of a Microsoft sign-in verification screen. At the top is the Microsoft logo. Below it is the email address 'cary@carysun.com'. The main heading is 'Enter code'. A message with a speech bubble icon says 'We texted your phone +X XXXXXXXX68. Please enter the code to sign in.' Below this is a text input field containing the code '479843'. At the bottom left are two links: 'Having trouble? Sign in another way' and 'More information'. At the bottom right is a blue 'Verify' button.

Microsoft

cary@carysun.com

Enter code

💬 We texted your phone +X XXXXXXXX68. Please enter the code to sign in.

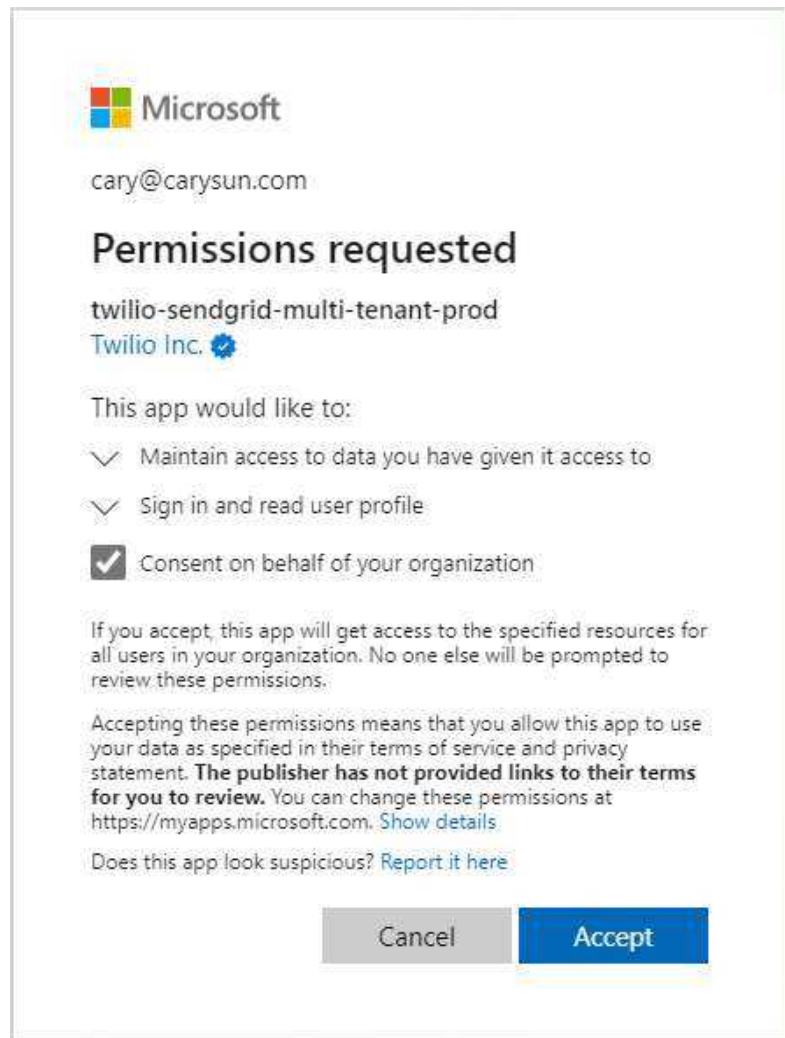
479843

Having trouble? [Sign in another way](#)

[More information](#)

Verify

13. On the Permissions requested page, select Consent on behalf of your organization and click Accept.



14. Fill in the information, and click Get Started!



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+

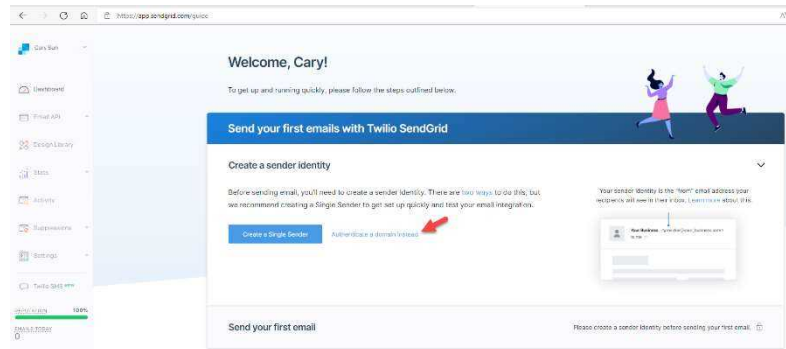
How many employees work at your company? •

☒ 1- 500 ☐ 1,001 - 5,000

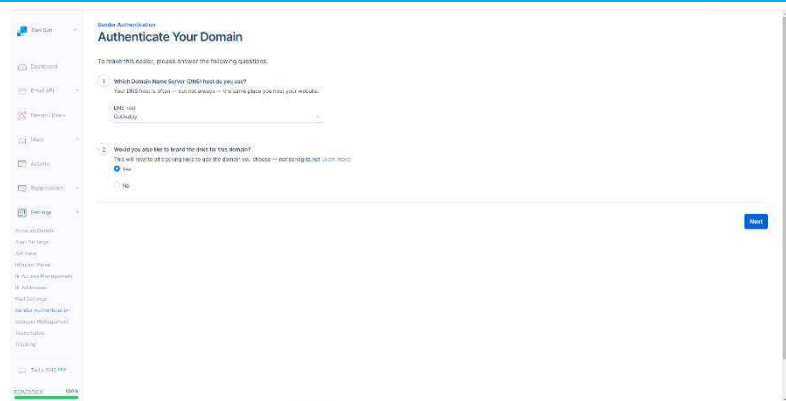
☐ 501 - 1,000 ☐ 5,001+

Get Started!

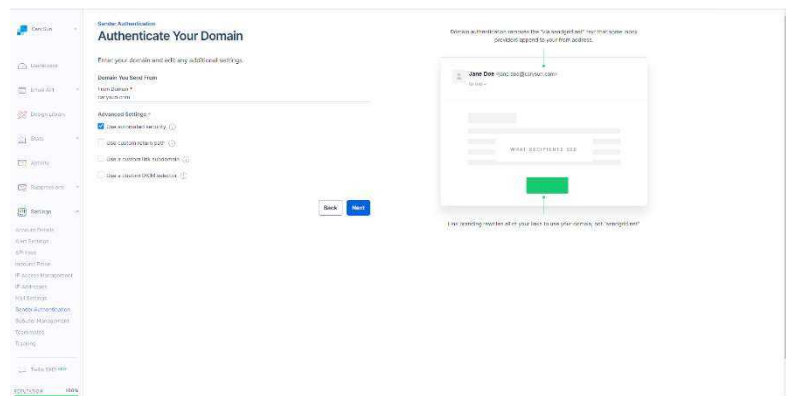
15. On the SendGrid Welcome page, select Authenticate on a domain instead.



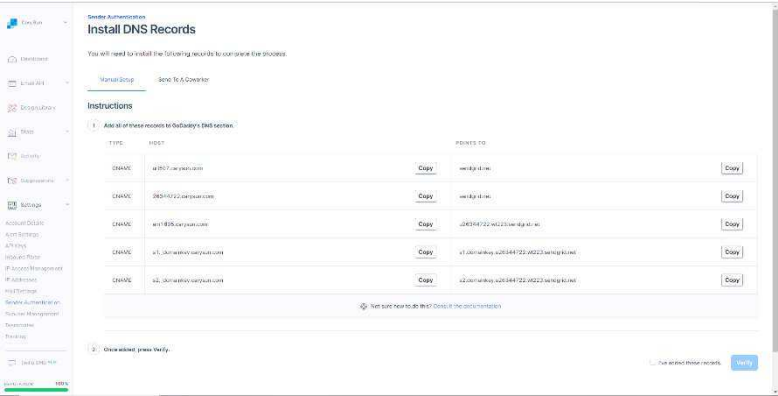
16. On the Authenticate Your Domain page, select your DNS host, select Yes to rewrite all tracking links to use your chosen domain – not sendgrid.net, and click Next.



17. Enter your domain name on the Domain You Send From page, and click Next.



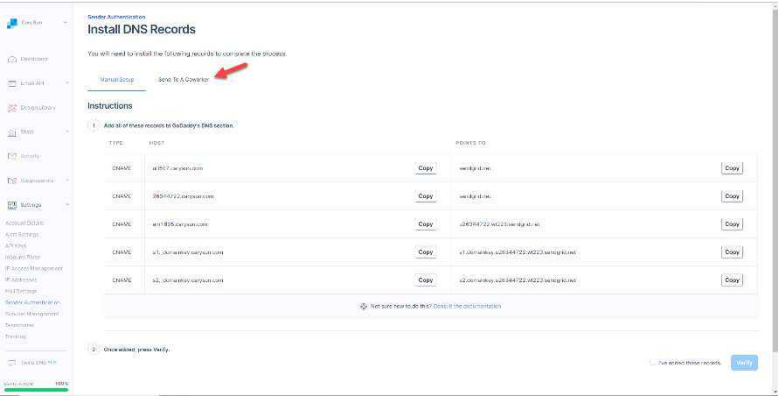
18. On the Install DNS Records page, copy and add all these records to your External DNS records.



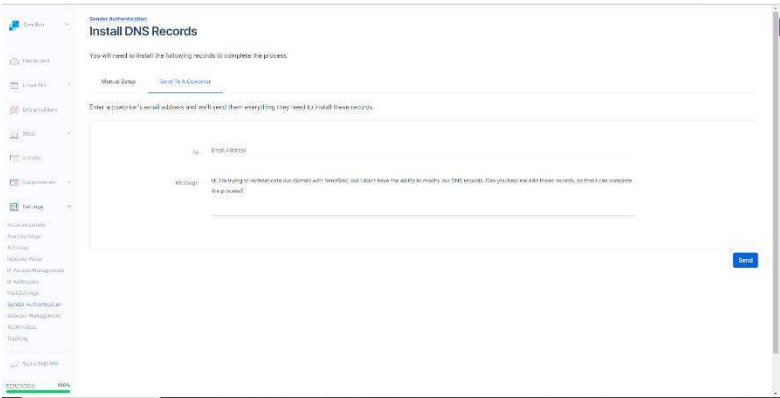
19. In my case, add them to GoDaddy.

Type	Name	Data	TTL	Delete	Edit
CNAME	en1605	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	u1507	sendgrid.net.	1 Hour	Delete	Edit

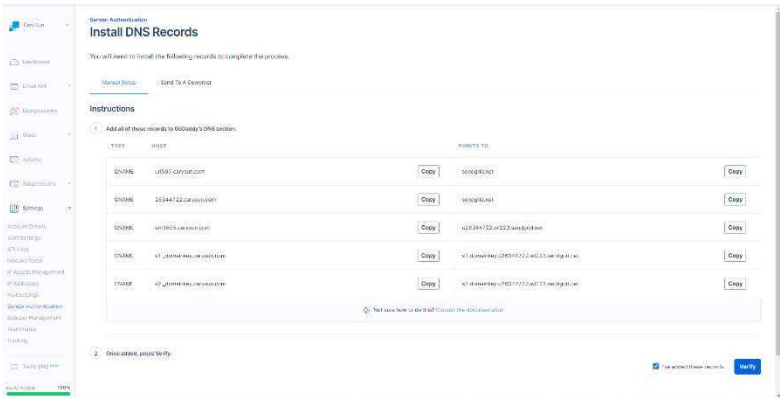
20. If you cannot add DNS records, select Send To A Coworker.



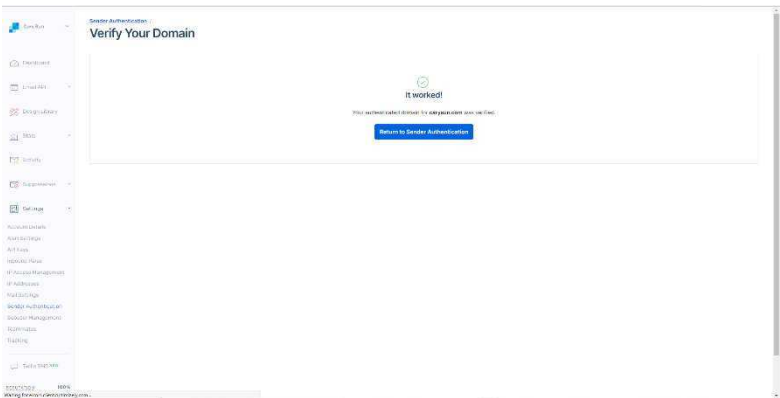
21. Type your coworker's email address, and click Send. Then, ask your coworker to add these DNS records.



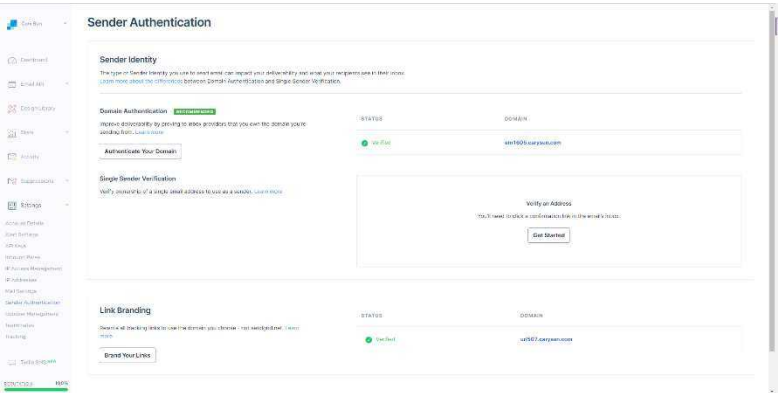
22. On the Install DNS Records page, select I've added these records, click Verify.



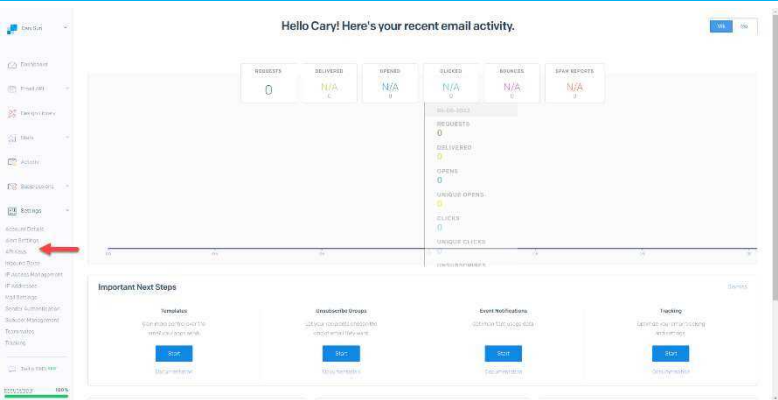
23. On the Verify Your Domain page, make sure your authenticated domain for the domain name was verified without issues and click Return to Sender Authentication.



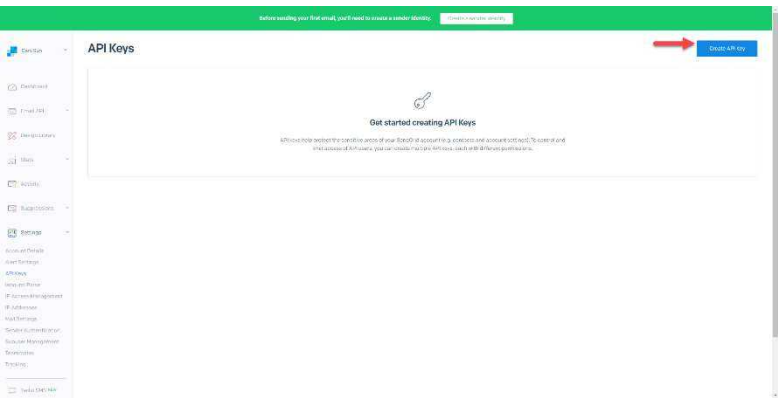
24. On the Sender Authentication page, ensure Domain Authentication and link Branding status is Verified.



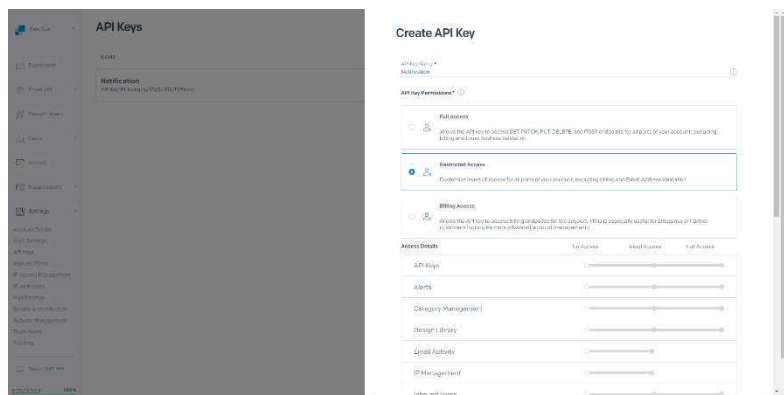
25. Under the Settings page, select API Keys.



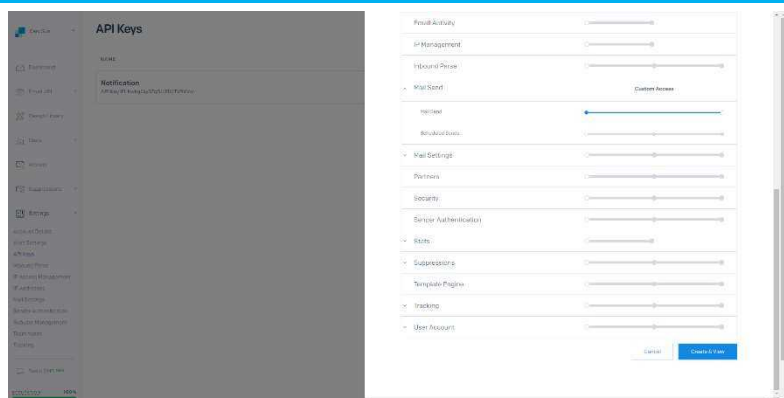
26. On the API Keys page, select Create API Key.



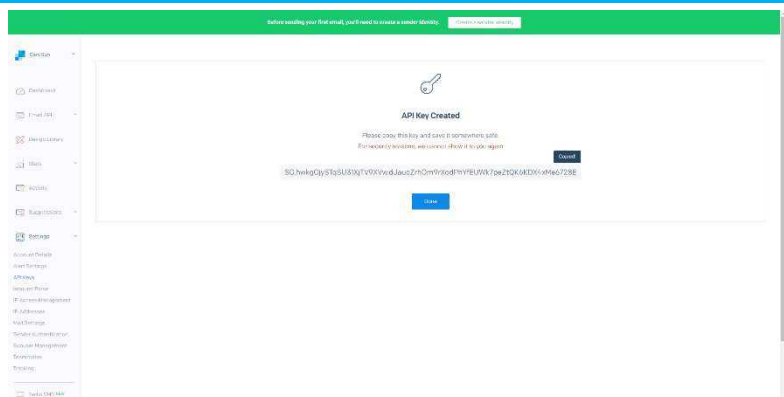
27. On the Create API Key page, type the API Key Name and select Restricted Access as API Key Permissions.



28. Enable Mail Activity as Access Details, click Create & View.

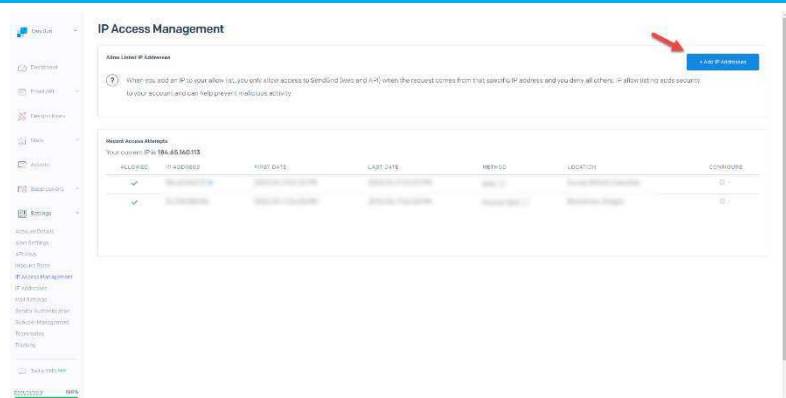


29. Copy the key on the API Key Created page, save it, and click Done.



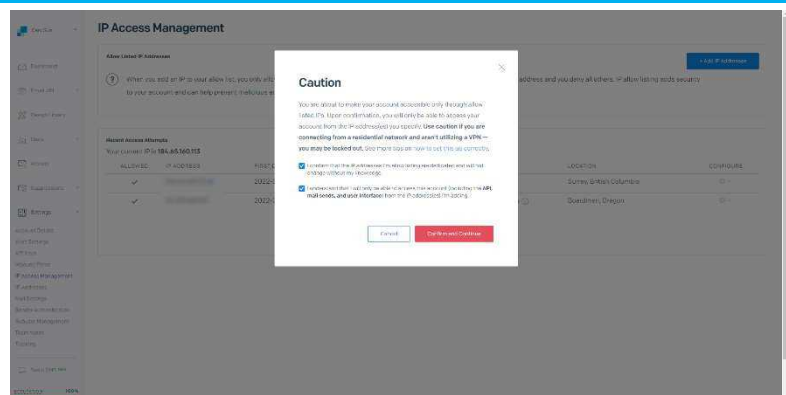
30. Under settings, select IP Access Management.

31. On the IP Access Management page, click +Add UP Address.



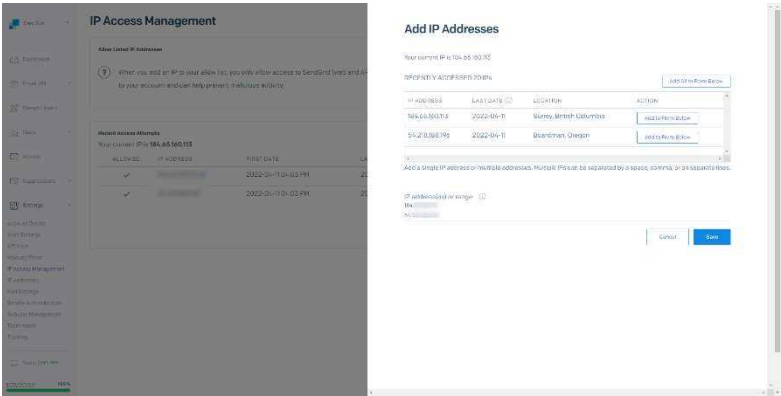
32. On the Confirmation page, select I confirm that the IP addresses I'm allowing are dedicated and will not change without my knowledge.

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,

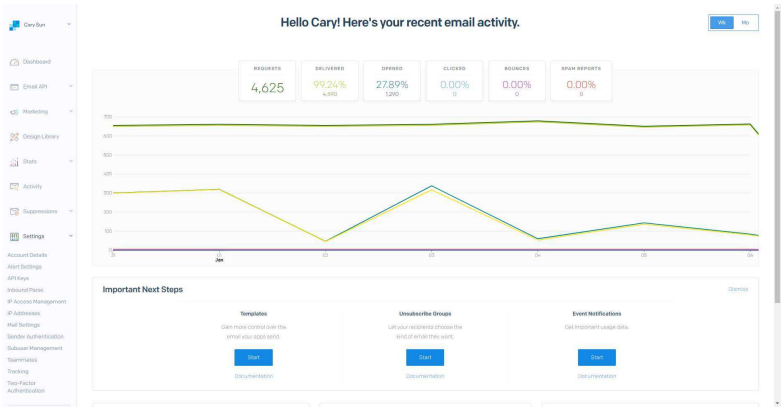


34. Click Confirm and Continue.

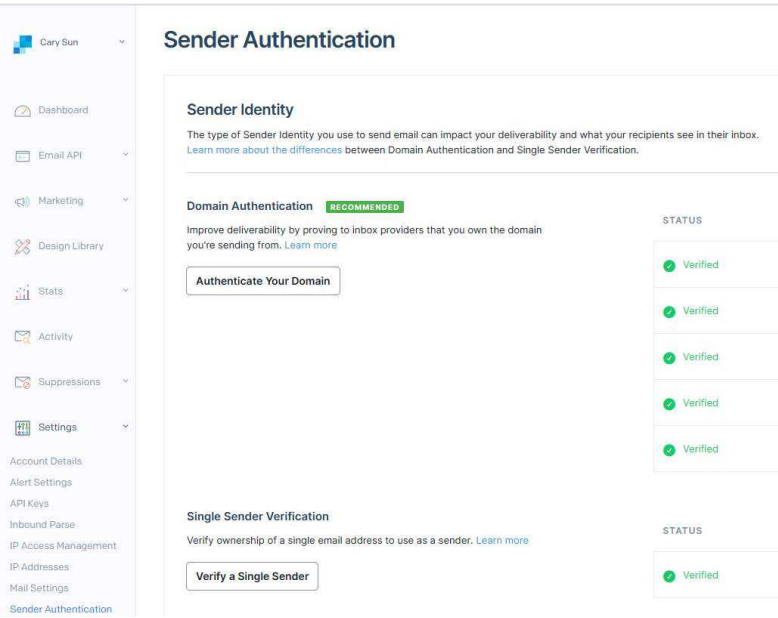
35. On the Add IP Addresses page, add IP addresses or ranges you would like to allow access to SendGrid. Make sure to include the public IP address of the Veeam management server and click Save.



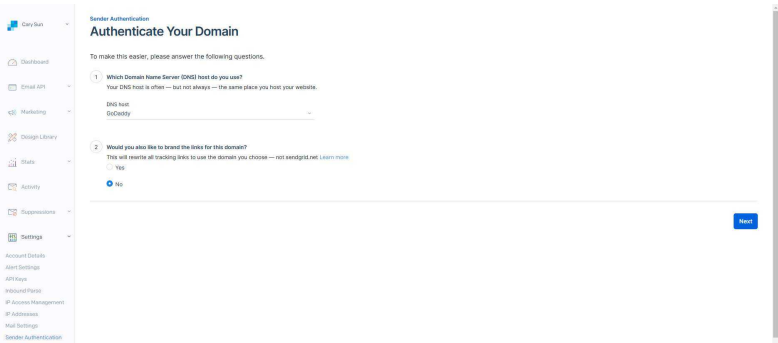
36. On the Home page, expand Settings and click Sender Authentication.



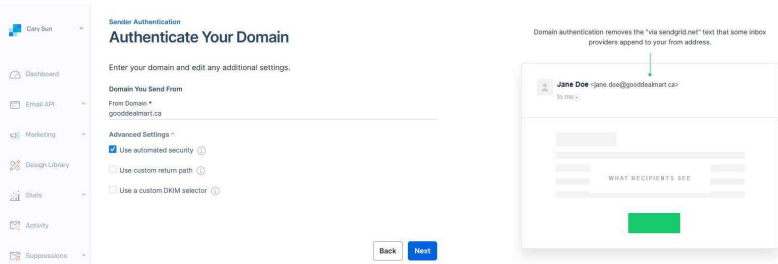
37. On the Sender Authentication page, click Authenticate Your Domain.



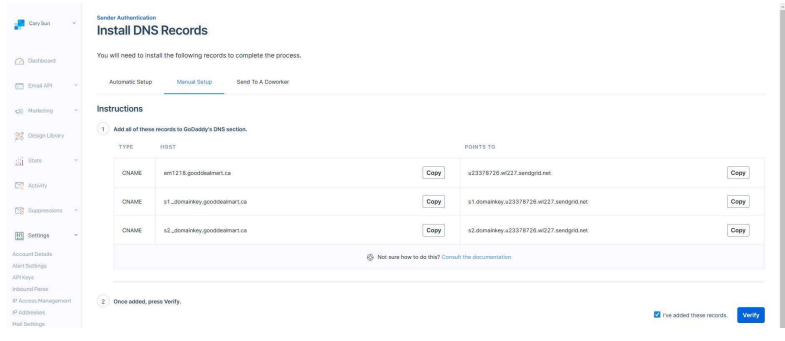
38. Specify your DNS host from the drop-down list on the Authenticate Your Domain page.
39. Select No Would you also like to brand the links for this domain?
40. Click Next.



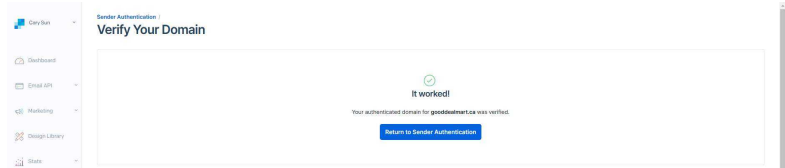
41. On the Domain, You send From page, specify your FQDN name, and click Next.



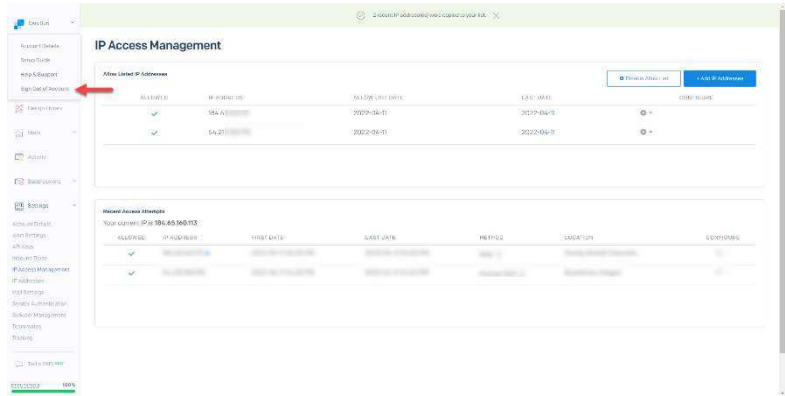
42. Add those CNAME records to your domain on the Install DNS Records page, select I've added these records, and click Verify.



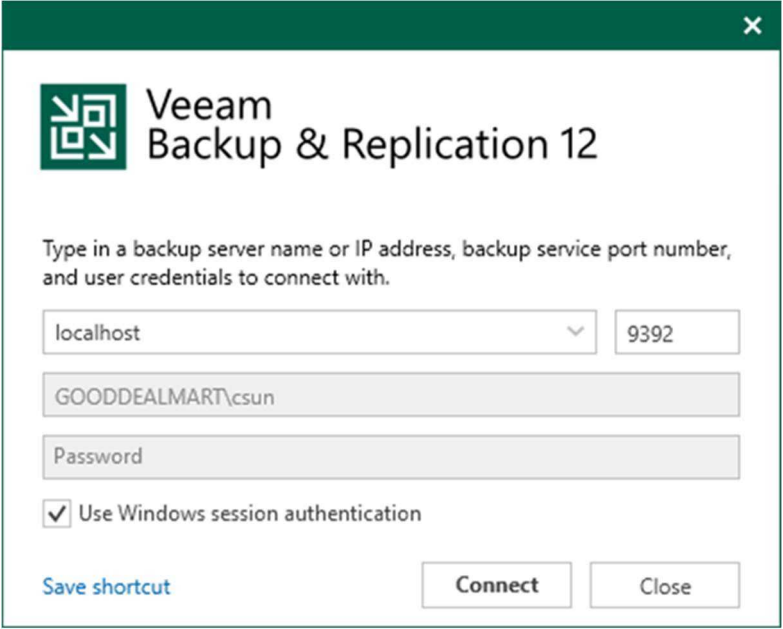
43. On the Verify Your Domain page, ensure verification is successful and click Return to Send Authentication.



44. Sign Out of Account.



45. Log in to the Veeam Backup and replication manager server.
46. Open the Veeam Backup & Replication Console and click Connect.



The image shows a Windows-style dialog box titled "Veeam Backup & Replication 12". It has a dark green header bar with a close button (X) in the top right corner. The main area is white and contains the Veeam logo (a green square with white geometric patterns) followed by the text "Veeam Backup & Replication 12". Below the title, there is a instruction: "Type in a backup server name or IP address, backup service port number, and user credentials to connect with." There are four input fields: a dropdown menu with "localhost" selected, a text box with "9392", a text box with "GOODDEALMART\csun", and a password field labeled "Password". Below these fields is a checkbox labeled "Use Windows session authentication" which is checked. At the bottom, there are three buttons: "Save shortcut" (in blue text), "Connect", and "Close".

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

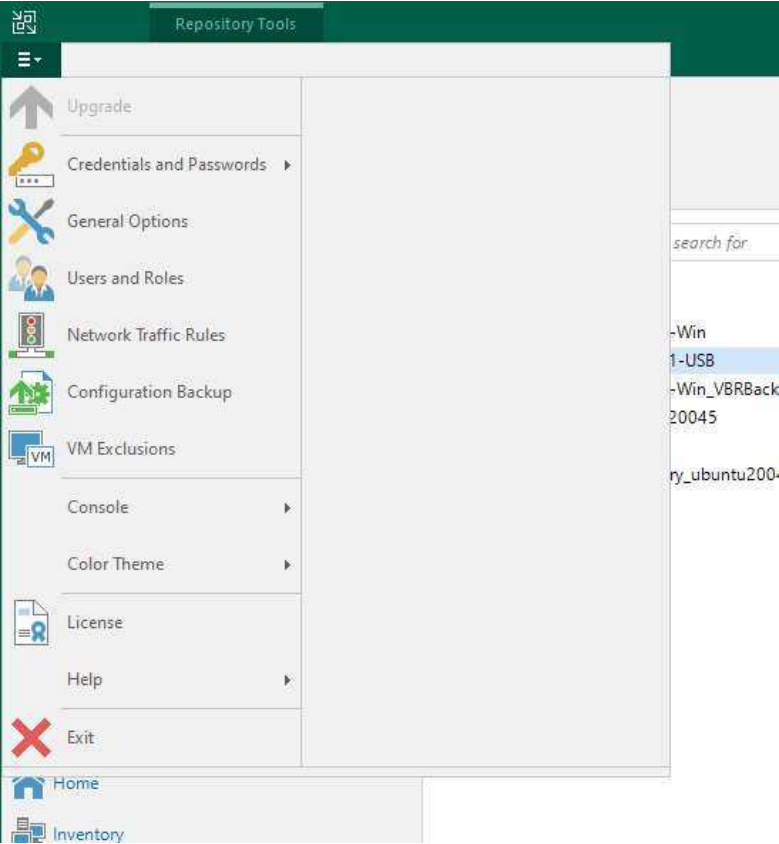
GOODDEALMART\csun

Password

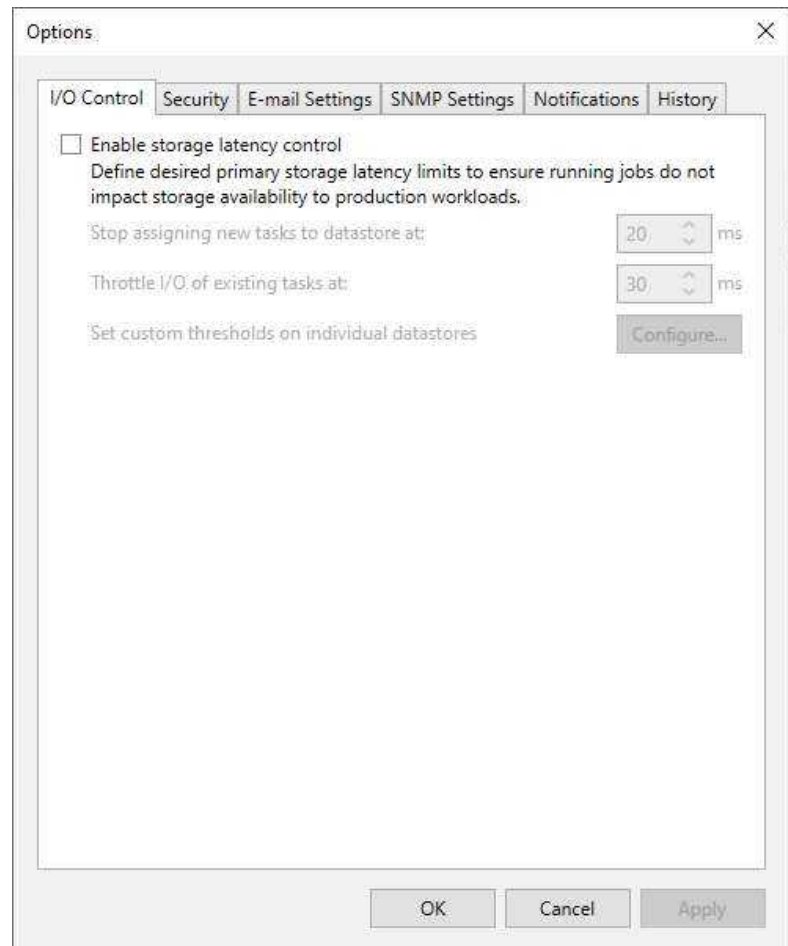
☒ Use Windows session authentication

Save shortcut Connect Close

47. Select General Options from the main menu.



48. On the Options page,
select Email Settings.



49. Select Enable e-mail notification (recommended) on the Email Settings page.
50. In the SMTP server field, enter smtp.sendgrid.net, and click Advanced.

Options

I/O Control Security **E-mail Settings** SNMP Settings Notifications History

☒ Enable e-mail notifications (recommended)

SMTP server:
smtp.sendgrid.net Advanced...

From:

To:

Subject:
[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

Test Message

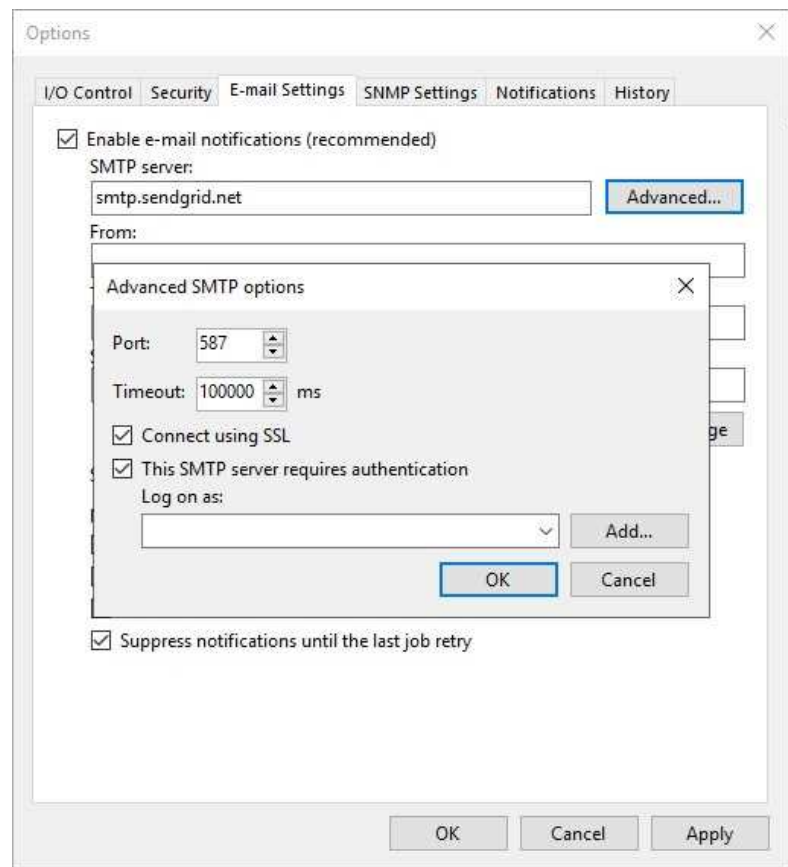
Send daily summary at: 10:00 PM ⓘ

Notify on:

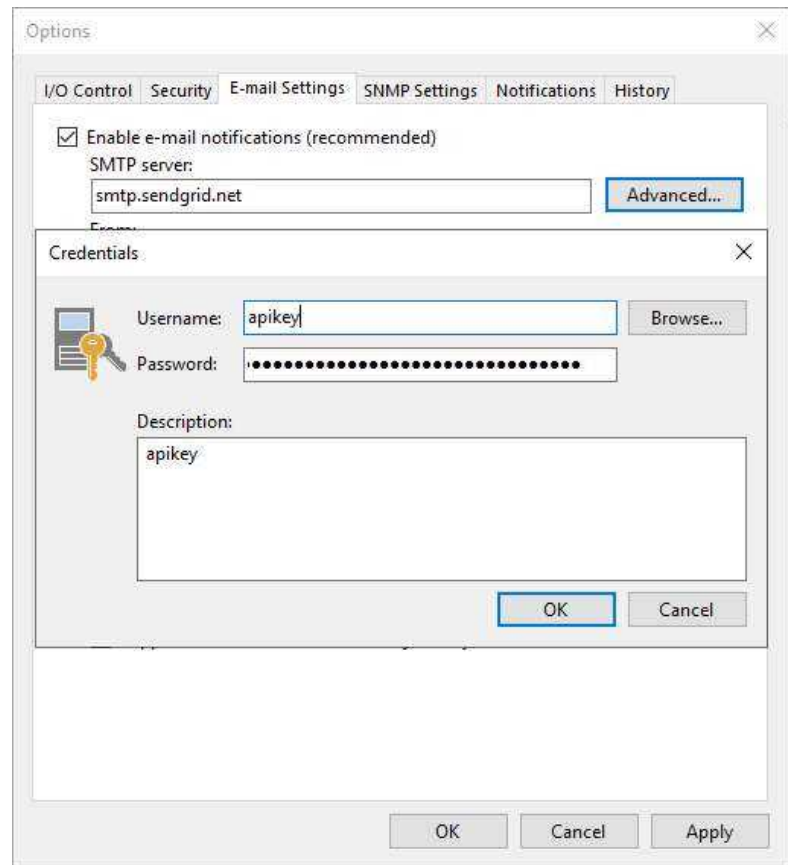
- ☒ Success
- ☒ Warning
- ☒ Failure
- ☒ Suppress notifications until the last job retry

OK Cancel Apply

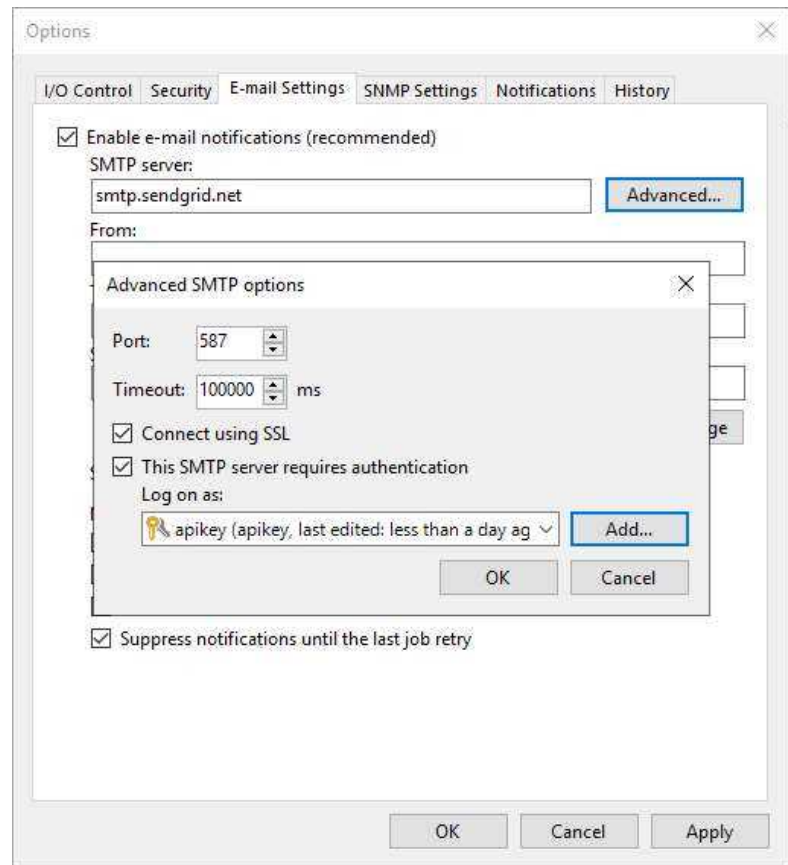
51. On the Advanced SMTP options page, type 587 in the Port field.
52. Use 100000 milliseconds as the Timeout.
53. Select Connect using SSL.
54. Select This SMTP server requires authentication.
55. Click Add to add a credential as Log on as account.



56. Type apikey as Username.
57. Paste the apikey number as a password.
58. Click OK.



59. On the Advanced SMTP options page, click OK.



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.

The screenshot shows the 'Options' dialog box with the 'E-mail Settings' tab selected. The 'Enable e-mail notifications (recommended)' checkbox is checked. The 'SMTP server' field contains 'smtp.sendgrid.net'. The 'From:' field contains 'VBR@gooddealmart.ca'. The 'To:' field contains 'csun@triconelite.com'. The 'Subject:' field contains '[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%'. There is a 'Test Message' button. The 'Send daily summary at:' field is set to '10:00 PM'. Under 'Notify on:', the checkboxes for 'Success', 'Warning', 'Failure', and 'Suppress notifications until the last job retry' are all checked. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Options

I/O Control Security E-mail Settings SNMP Settings Notifications History

☒ Enable e-mail notifications (recommended)

SMTP server:
smtp.sendgrid.net Advanced...

From:
VBR@gooddealmart.ca

To:
csun@triconelite.com

Subject:
[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

Test Message

Send daily summary at: 10:00 PM ⓘ

Notify on:

☒ Success

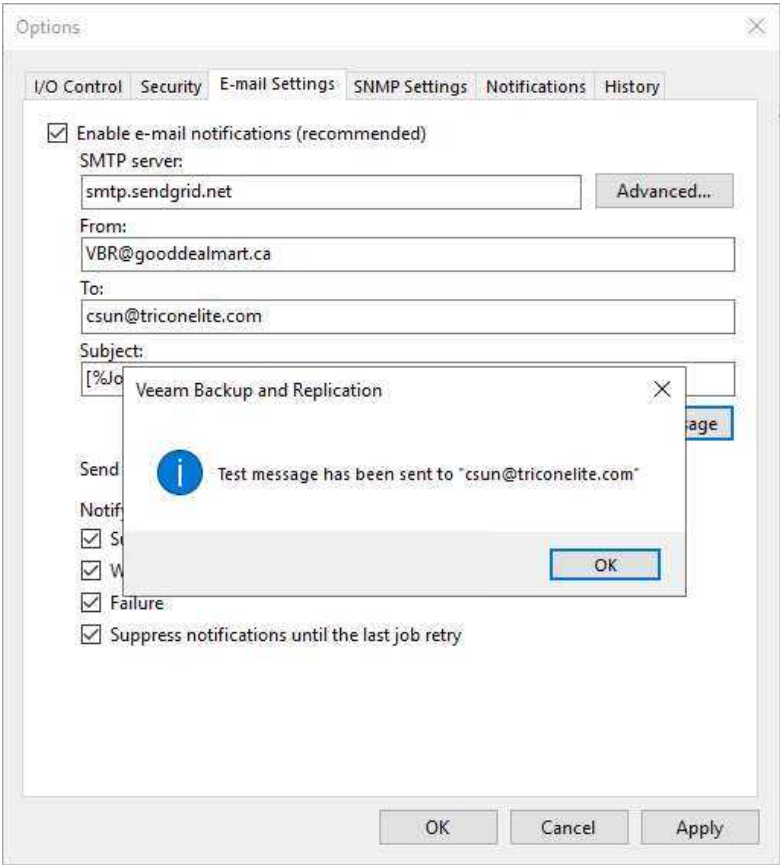
☒ Warning

☒ Failure

☒ Suppress notifications until the last job retry

OK Cancel Apply

63. Verify the test message sent successfully, and click OK.



64. On the Options page, click OK.

The screenshot shows the 'Options' dialog box with the 'E-mail Settings' tab selected. The 'Enable e-mail notifications (recommended)' checkbox is checked. The 'SMTP server' is set to 'smtp.sendgrid.net'. The 'From' field is 'VBR@gooddealmart.ca' and the 'To' field is 'csun@triconelite.com'. The 'Subject' field contains a template: '[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%'. A 'Test Message' button is located to the right of the subject field. Below these fields, the 'Send daily summary at' is set to '10:00 PM'. Under the 'Notify on:' section, four checkboxes are checked: 'Success', 'Warning', 'Failure', and 'Suppress notifications until the last job retry'. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

Options

I/O Control Security E-mail Settings SNMP Settings Notifications History

☒ Enable e-mail notifications (recommended)

SMTP server:
smtp.sendgrid.net Advanced...

From:
VBR@gooddealmart.ca

To:
csun@triconelite.com

Subject:
[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

Test Message

Send daily summary at: 10:00 PM ⓘ

Notify on:

- ☒ Success
- ☒ Warning
- ☒ Failure
- ☒ Suppress notifications until the last job retry

OK Cancel Apply

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 & Replica to send email notifications about backup job results.

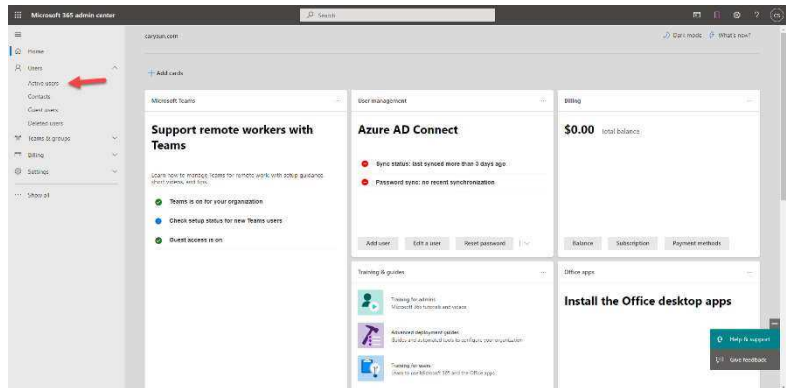
Instructions

Screenshot (if applicable)

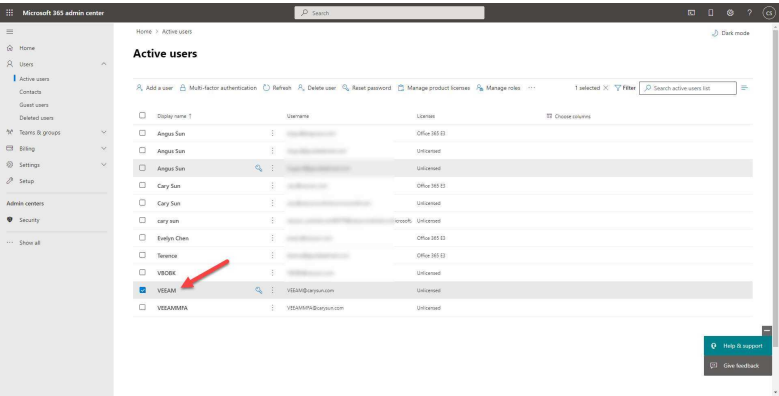
1. Sign in Office 365 portal with a Global Admin account and select Admin.



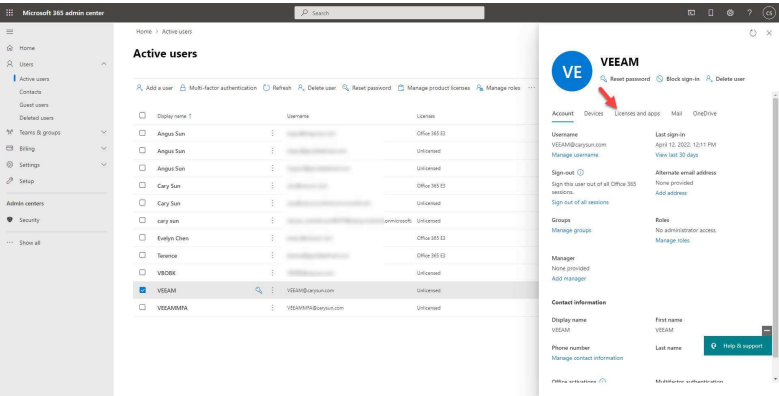
2. On the Microsoft 365 admin center, expand Users and select Active users.



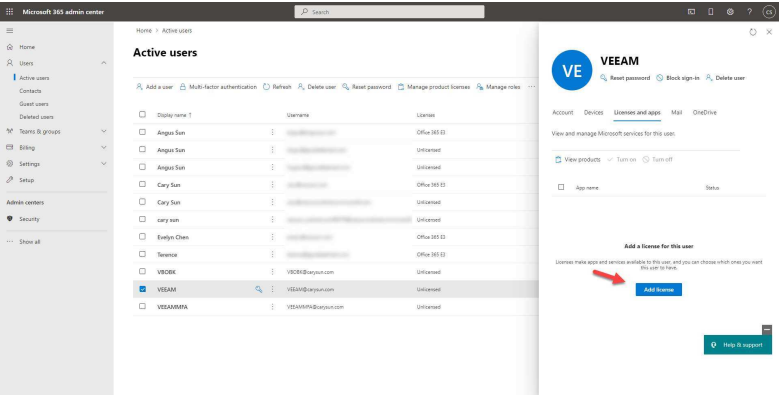
3. On the Active users' page, click Veeam service account (in my case, VEEAM).



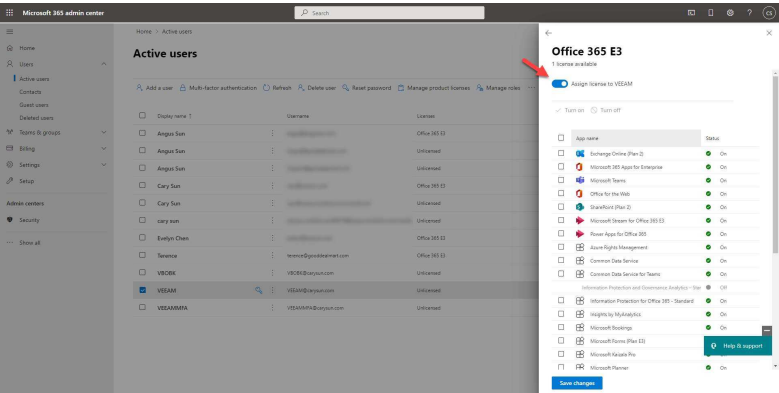
4. On the account page, select License and apps.



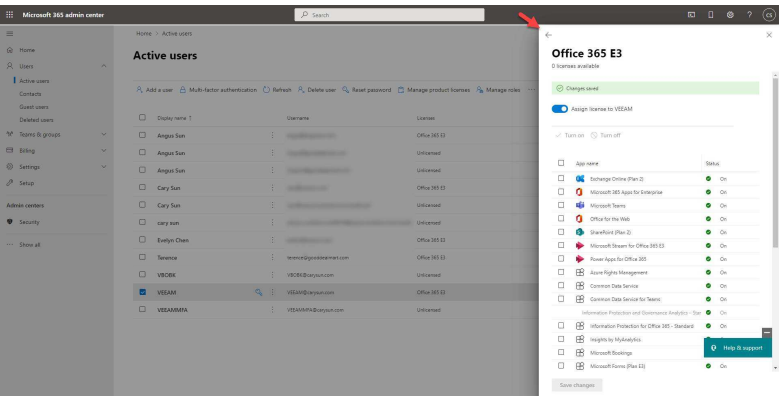
5. On the License and apps page, click Add license.



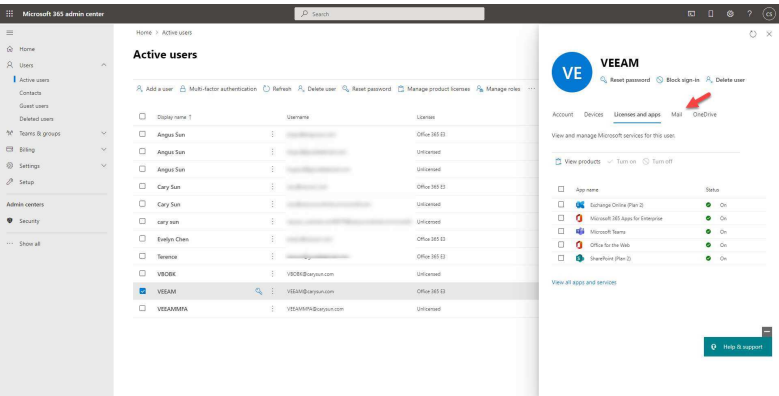
6. On the Office 365 license page, enable Assign license to the account and click Save changes.



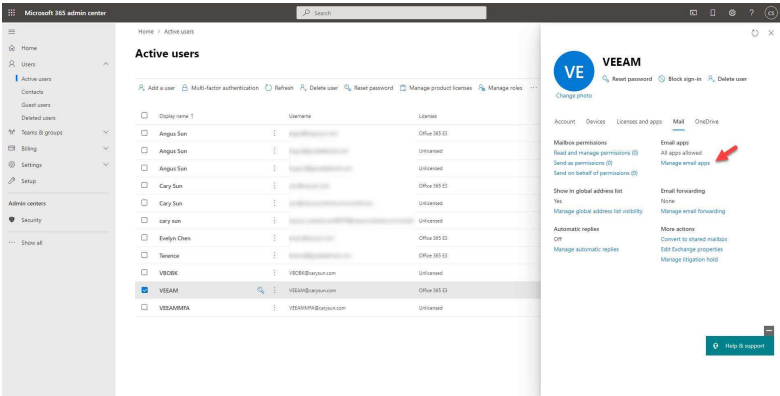
7. Click Back <--.



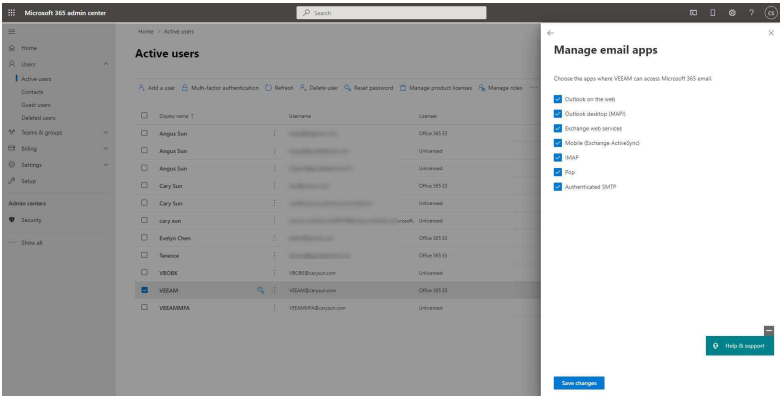
8. On the account page, select Mail. It would be preferable to wait a few minutes before preparing a mailbox for the user.



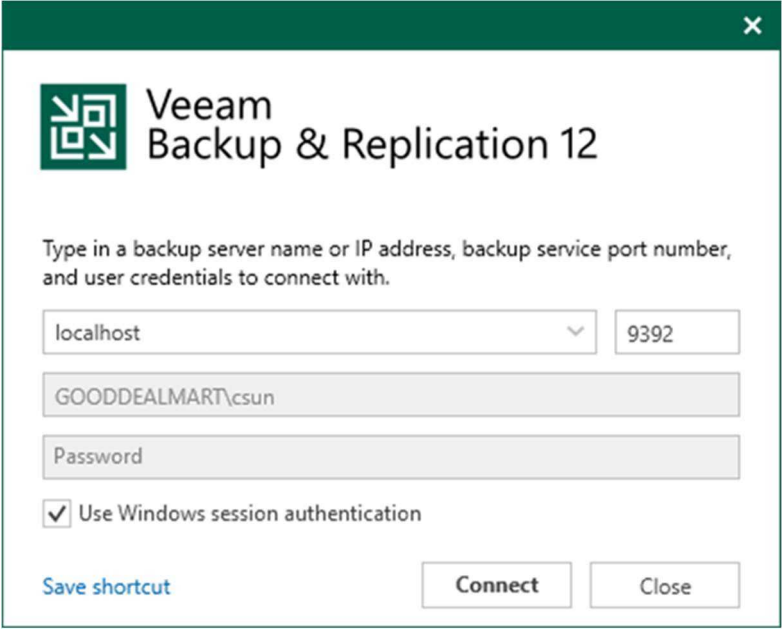
9. On the Mail page, select Manage email apps.



10. On the Manage email apps, select Authenticated SMTP and click Save changes.



11. Log in to the Veeam Backup and replication manager server.
12. Open the Veeam Backup & Replication Console and click Connect.



The image shows a Windows-style dialog box titled "Veeam Backup & Replication 12". It has a dark green header bar with a close button (X) in the top right corner. The main area is white and contains the Veeam logo (a green square with white geometric patterns) followed by the text "Veeam Backup & Replication 12". Below this, there is a prompt: "Type in a backup server name or IP address, backup service port number, and user credentials to connect with." There are three input fields: a dropdown menu with "localhost" selected, a text box with "9392", and a text box with "GOODDEALMART\csun". Below these is a "Password" text box. A checkbox labeled "Use Windows session authentication" is checked. At the bottom, there is a "Save shortcut" link on the left and two buttons, "Connect" and "Close", on the right.

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

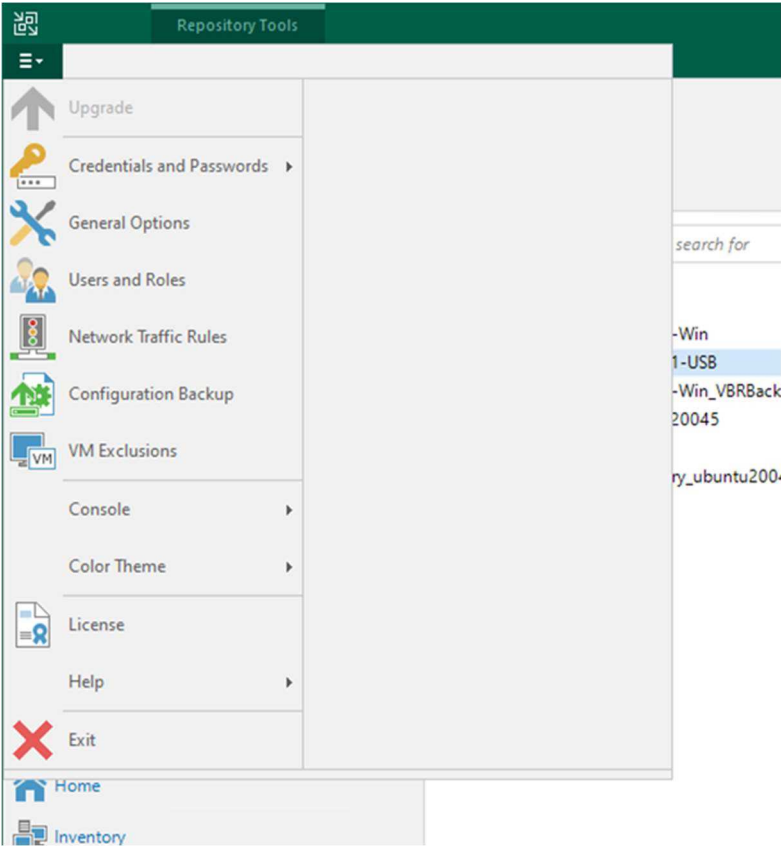
GOODDEALMART\csun

Password

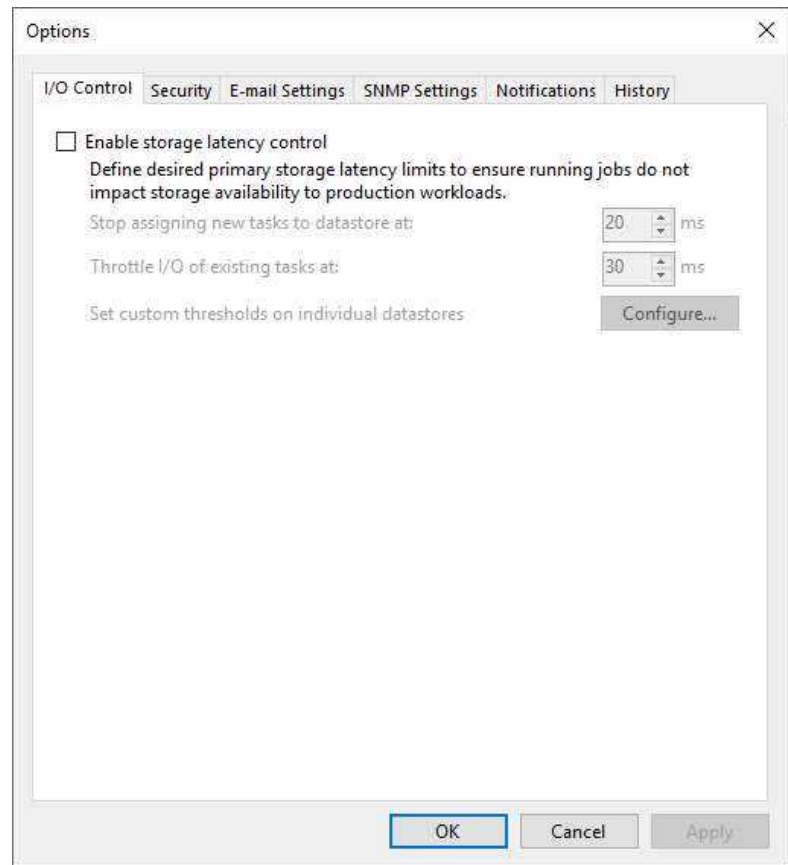
☒ Use Windows session authentication

[Save shortcut](#) **Connect** **Close**

13. Select General Options from the main menu.



14. On the Options page,
select Email Settings.



- 15. Select Enable e-mail notification (recommended) on the Email Settings page.
- 16. In the SMTP server field, enter smtp.sendgrid.net, and click Advanced.

Options

I/O ControlSecurityE-mail SettingsSNMP SettingsNotificationsHistory

☒ Enable e-mail notifications (recommended)

SMTP server:

smtp.office365.comAdvanced...

From:

To:

Subject:

[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

Test Message

Send daily summary at: 10:00 PM ⓘ

Notify on:

☒ Success

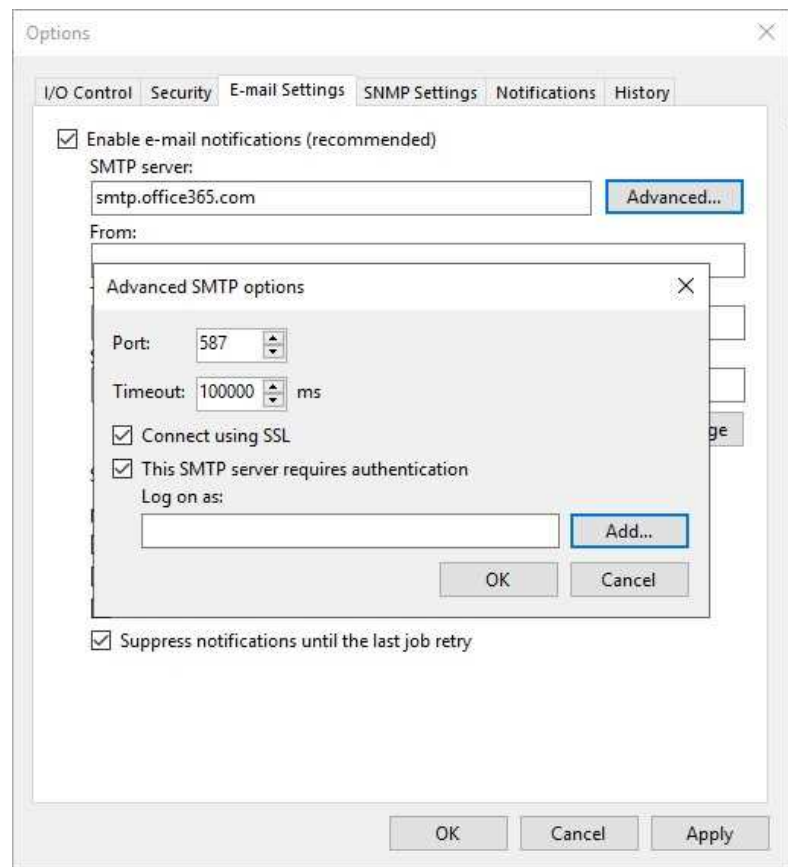
☒ Warning

☒ Failure

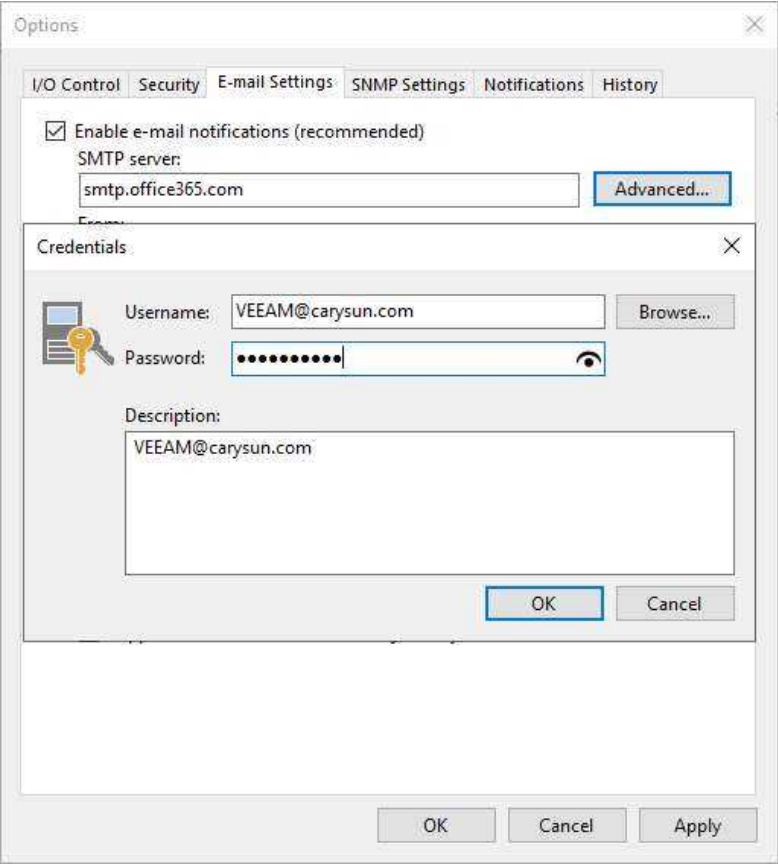
☒ Suppress notifications until the last job retry

OKCancelApply

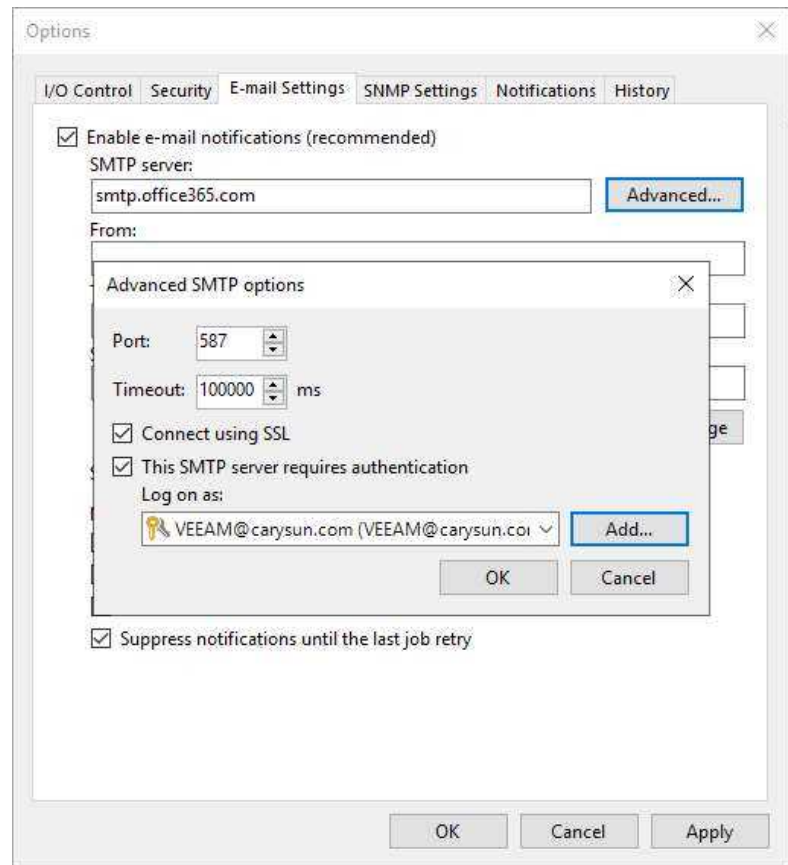
17. On the Advanced SMTP options page, enter 587 in the Port field.
18. Use 100000 milliseconds as the Timeout.
19. Select Connect using SSL.
20. Select This SMTP server requires authentication.
21. Click Add to add a credential as Log on as account.



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.



23. On the Advanced SMTP options page, click OK.



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.

The screenshot shows the 'Options' dialog box with the 'E-mail Settings' tab selected. The 'Enable e-mail notifications (recommended)' checkbox is checked. The 'SMTP server' field contains 'smtp.office365.com'. The 'From' field contains 'VEEAM@carysun.com'. The 'To' field contains 'csun@triconelite.com'. The 'Subject' field contains '[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%'. There is a 'Test Message' button. The 'Send daily summary at' field is set to '10:00 PM'. Under 'Notify on:', the checkboxes for 'Success', 'Warning', 'Failure', and 'Suppress notifications until the last job retry' are all checked. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Options

I/O Control Security E-mail Settings SNMP Settings Notifications History

☒ Enable e-mail notifications (recommended)

SMTP server:
smtp.office365.com Advanced...

From:
VEEAM@carysun.com

To:
csun@triconelite.com

Subject:
[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

Test Message

Send daily summary at: 10:00 PM ⓘ

Notify on:

☒ Success

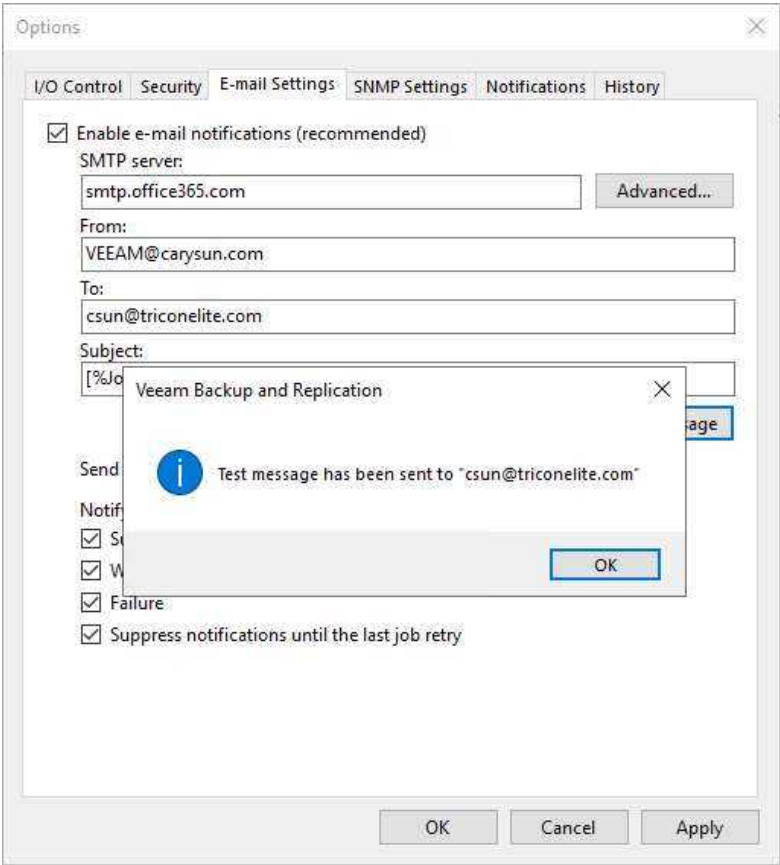
☒ Warning

☒ Failure

☒ Suppress notifications until the last job retry

OK Cancel Apply

27. Ensure the test email was successfully sent to recipients, and click OK.



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.

The screenshot shows the 'Options' dialog box with the 'E-mail Settings' tab selected. The 'Enable e-mail notifications (recommended)' checkbox is checked. The SMTP server is set to 'smtp.office365.com'. The 'From' field is 'VEEAM@carysun.com' and the 'To' field is 'csun@triconelite.com'. The 'Subject' field contains a template: '[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%'. There is a 'Test Message' button. The 'Send daily summary at' is set to '10:00 PM'. Under 'Notify on:', all three checkboxes (Success, Warning, Failure) are checked, and 'Suppress notifications until the last job retry' is also checked. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Options

I/O Control Security E-mail Settings SNMP Settings Notifications History

☒ Enable e-mail notifications (recommended)

SMTP server: smtp.office365.com Advanced...

From: VEEAM@carysun.com

To: csun@triconelite.com

Subject: [%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

Test Message

Send daily summary at: 10:00 PM ⓘ

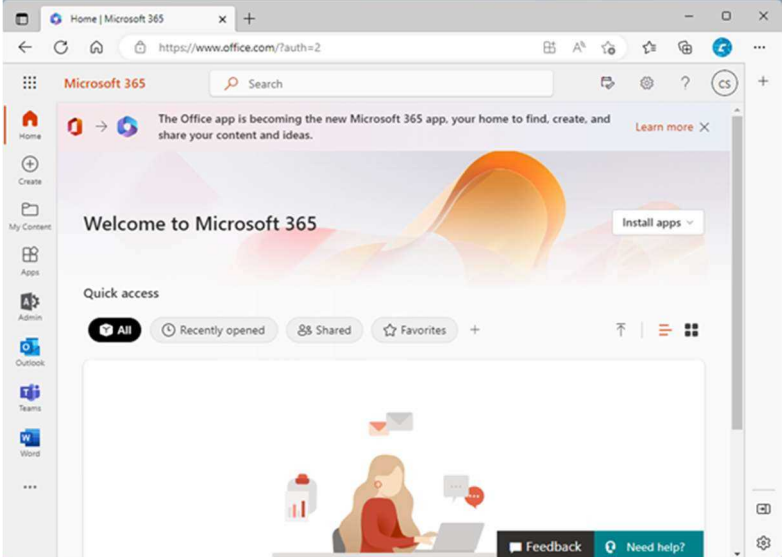
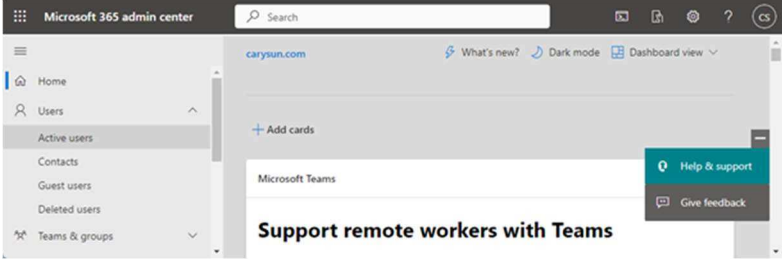
Notify on:

- ☒ Success
- ☒ Warning
- ☒ Failure
- ☒ Suppress notifications until the last job retry

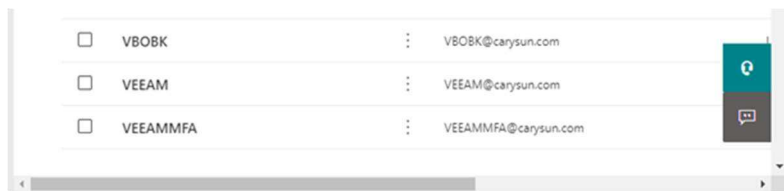
OK Cancel Apply

Configure Notification with Microsoft Office 365 MFA Account

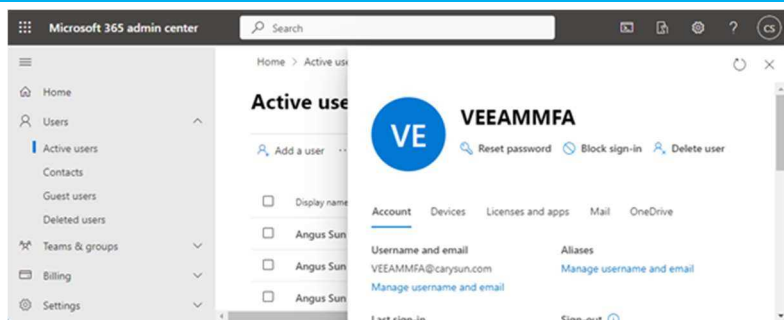
You can configure Microsoft Office 365 MFA account for notification settings if you want Veeam Backup & Replication to send email notifications about backup job results.

Instructions	Screenshot (if applicable)
1. Sign in Office 365 portal with a Global Admin account, and select Admin.	
2. On the Microsoft 365 admin center, expand Users and select Active users.	

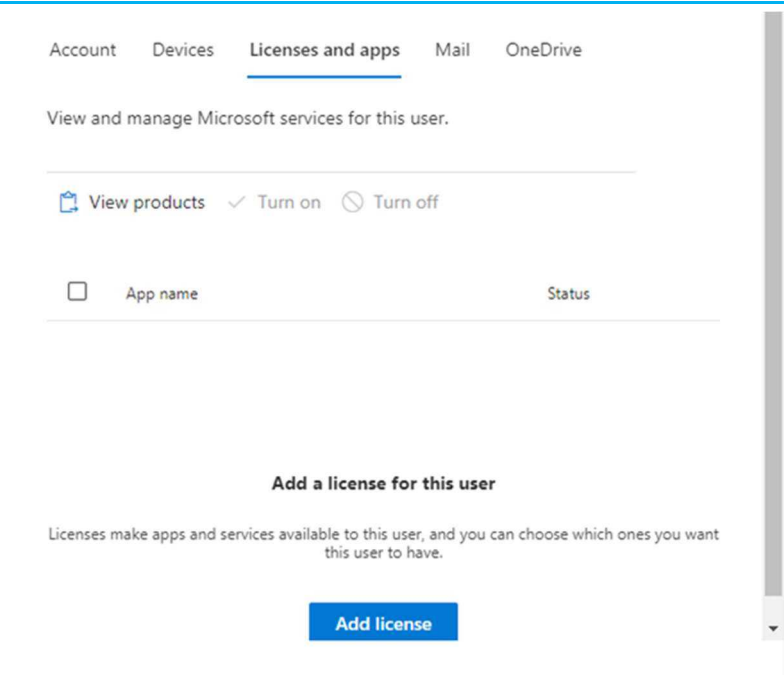
3. On the Active users' page, click Veeam service account (VEEAMMFA, in my case).



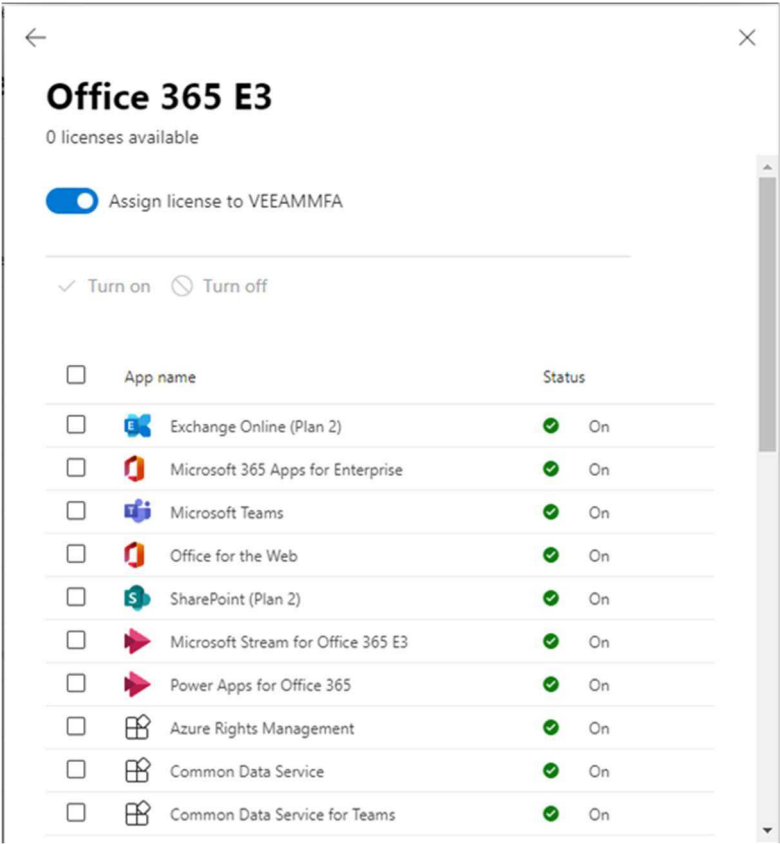
4. On the account page, select License and apps.



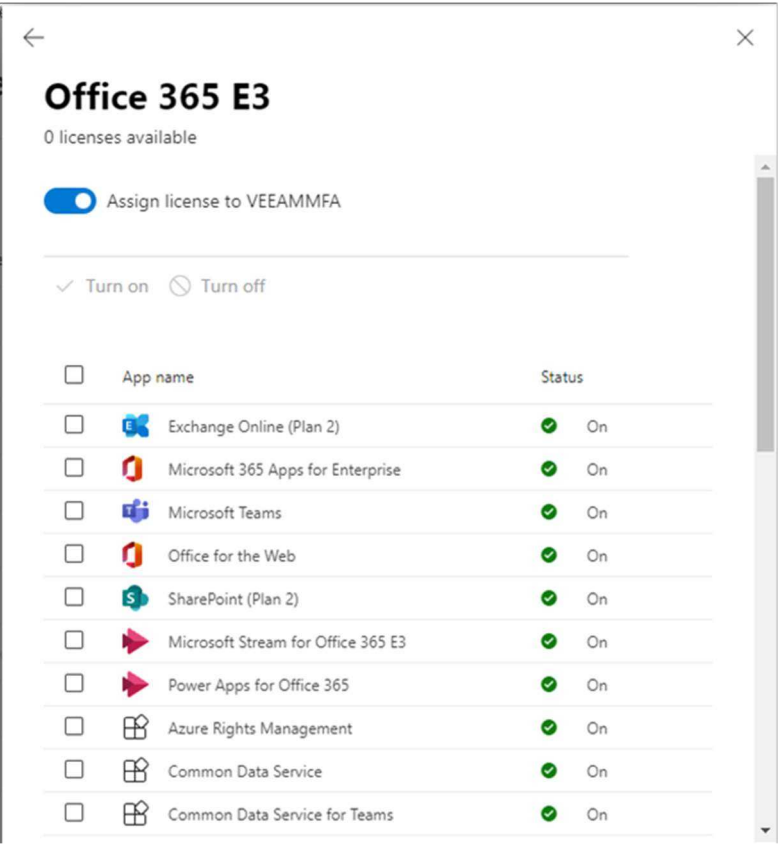
5. On the License and apps page, click Add license.



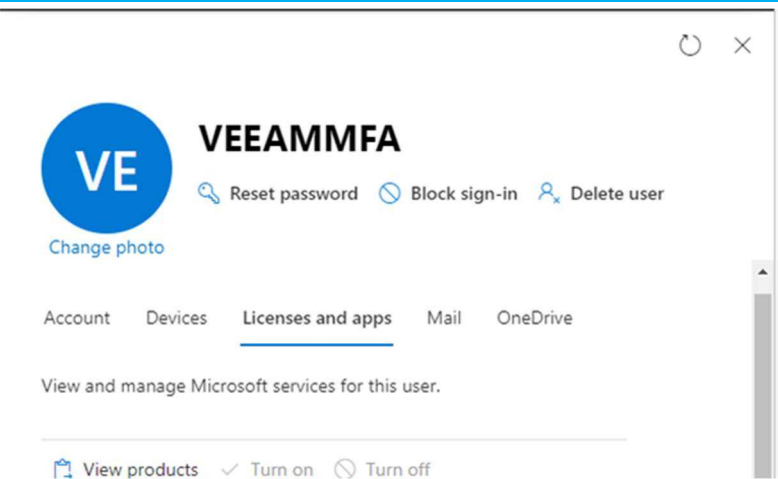
- 6. On the Office 365 license page, enable Assign license to the account, and click Save changes.



7. Click Back <--.



8. On the account page, select Mail. It would be preferable to wait a few minutes before preparing a mailbox for the user.



9. On the Mail page, select Manage email apps.



VEEAMMFA

 Reset password  Block sign-in  Delete user

[Change photo](#)

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 \(0\)](#)

Show in global address list

Yes

[Manage global address list visibility](#)

Email apps

All apps allowed

[Manage email apps](#)

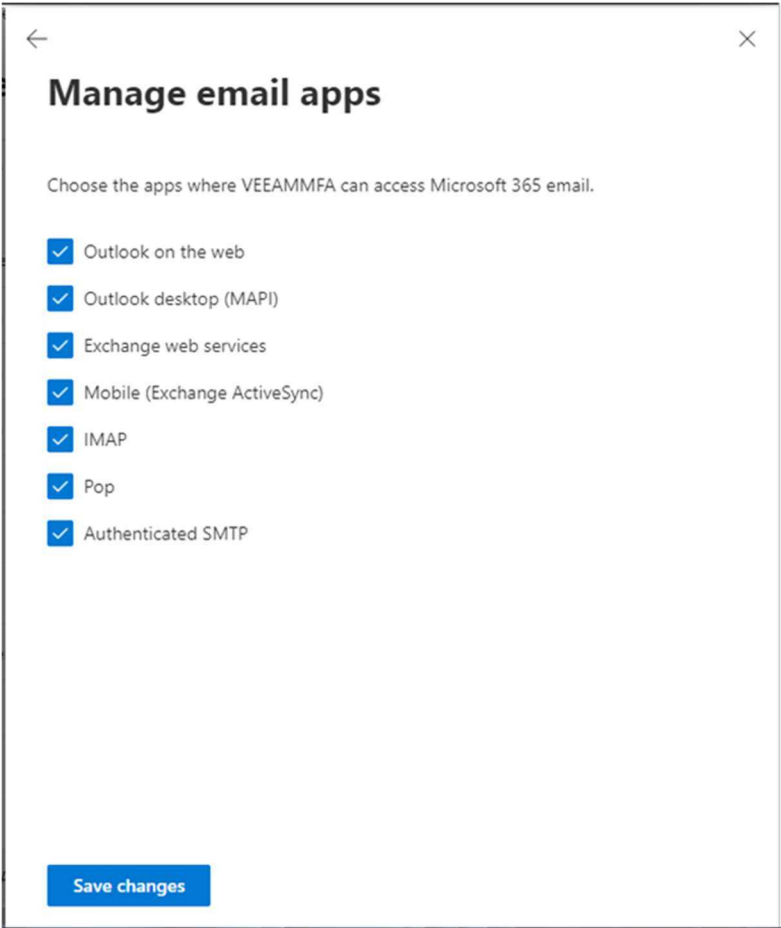
Email forwarding

None

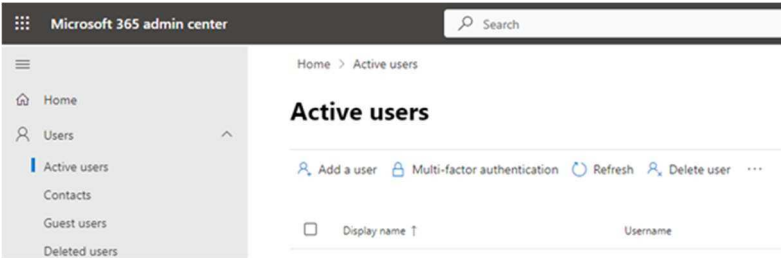
[Manage email forwarding](#)

335

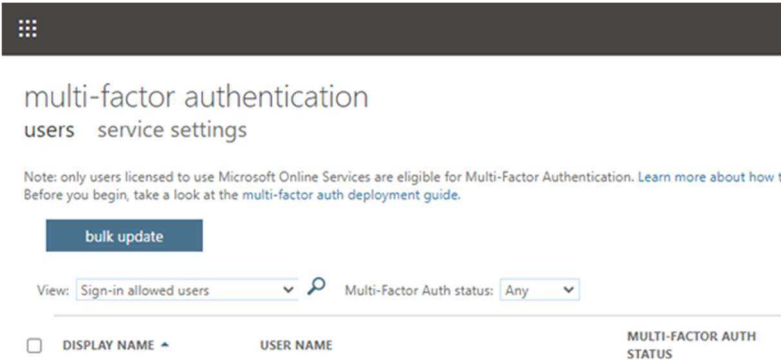
10. On the Manage email apps, select Authenticated SMTP and click Save changes.



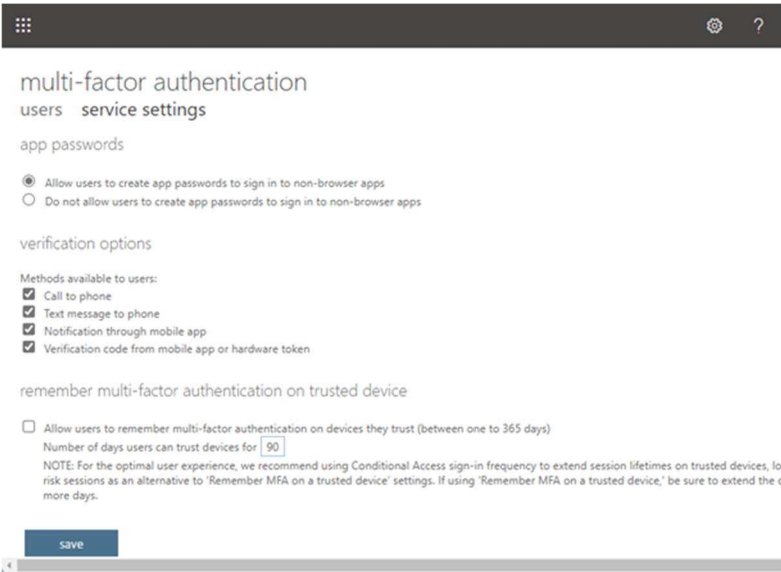
11. On the Active Users page, select Multi-factor authentication.



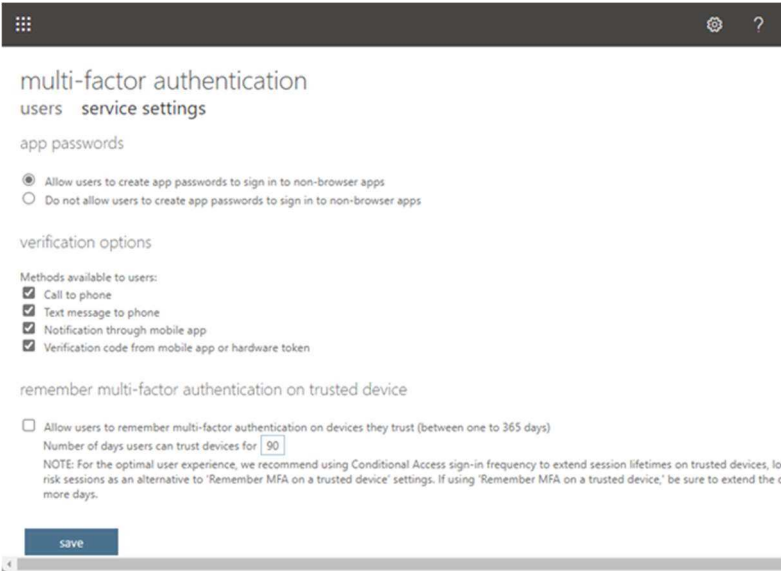
- 12. Sign in with a Global admin account.
- 13. On the multi-factor authentication page, select service settings.



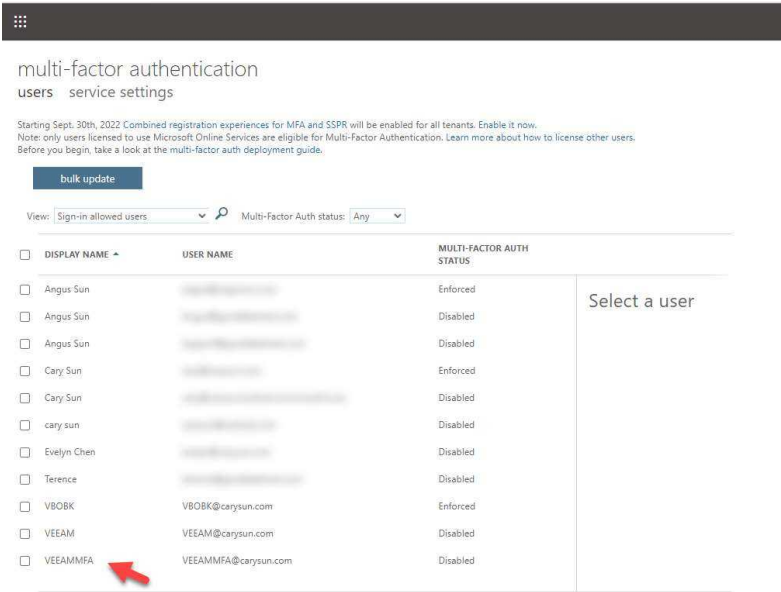
- 14. On the service settings page, select Allow users to create an app password to sign in to non-browser apps, click save and then sign out from the office 365 portal.



15. On the multi-factor authentication page, select users.



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.



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.

bulk update

View: Sign-in allowed users

Multi-Factor Auth status: Any

☐	DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
☐	Angus Sun	angus.sun@carlson.com	Enforced
☐	Angus Sun	angus.sun@carlson.com	Disabled
☐	Angus Sun	angus.sun@carlson.com	Disabled
☐	Cary Sun	cary.sun@carlson.com	Enforced
☐	Cary Sun	cary.sun@carlson.com	Disabled
☐	cary sun	cary.sun@carlson.com	Disabled
☐	Terence	terence@carlson.com	Disabled
☐	Terence	terence@carlson.com	Disabled
☐	VEEAM	VEEAM@carlson.com	Enforced
☐	VEEAM	VEEAM@carlson.com	Disabled
☒	VEEAMMFA	VEEAMMFA@carlson.com	Disabled

VEEAMMFA

VEEAMMFA@carlson.com

quick steps

Enable

Manage user settings

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>

enable multi-factor auth

cancel

20. On the Updates, successful page, click Close.

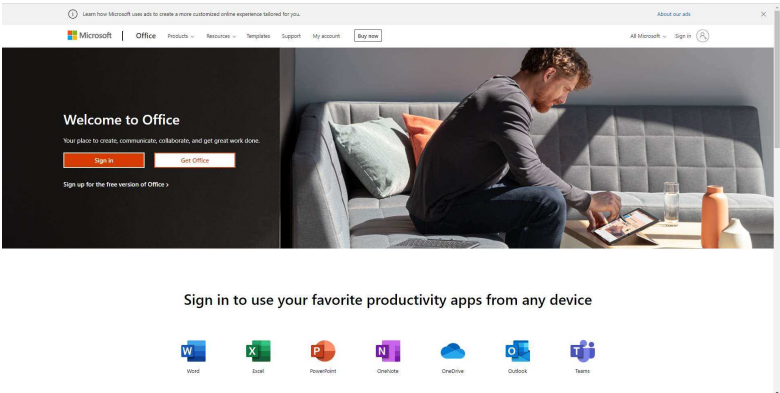
i

Updates successful

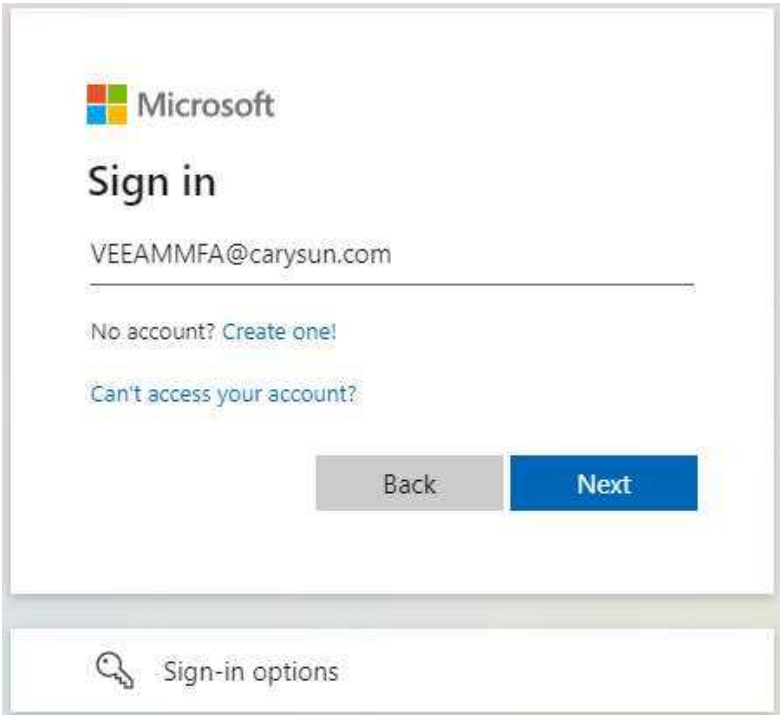
Multi-factor auth is now enabled for the selected accounts.

close

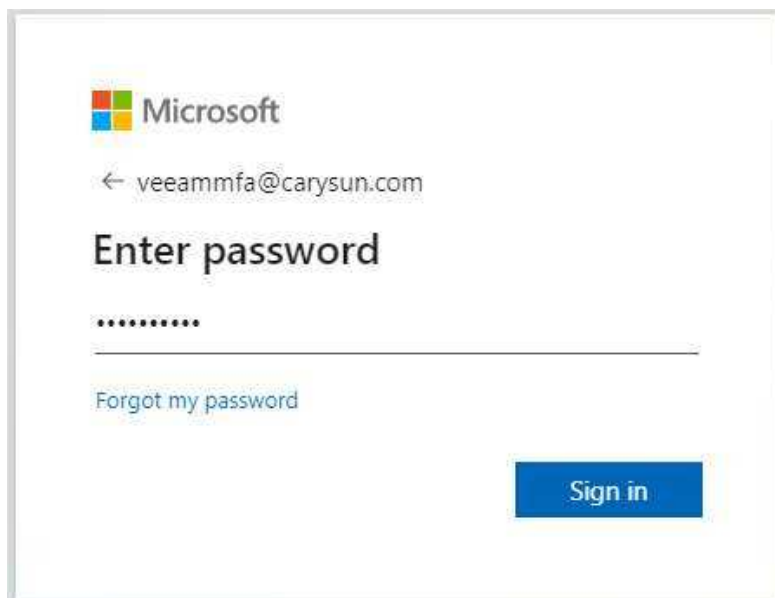
21. Sign in Office 365 portal with a Veeam service account



22. On the Sign in page, enter the Veeam services account email address.

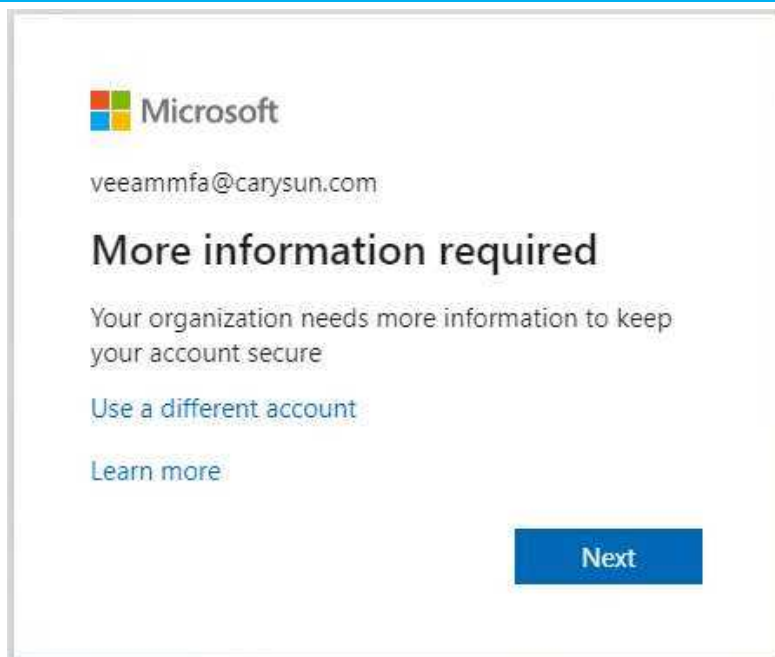


23. Enter the password.



The image shows a Microsoft sign-in page. At the top is the Microsoft logo. Below it is the email address veeammfa@carysun.com with a back arrow to its left. The main heading is "Enter password". Below the heading is a password input field with a masked password of eight dots. Underneath the input field is a link that says "Forgot my password". In the bottom right corner is a blue button labeled "Sign in".

24. On the More information required page, click Next.



The image shows a Microsoft "More information required" page. At the top is the Microsoft logo. Below it is the email address veeammfa@carysun.com. The main heading is "More information required". Below the heading is a message: "Your organization needs more information to keep your account secure". Underneath this message are two links: "Use a different account" and "Learn more". In the bottom right corner is a blue button labeled "Next".

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

Method

☒ Send me a code by text message

☐ Call me

Next

Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

©2022 MicrosoftLegalPrivacy

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

When you receive the verification code, enter it here

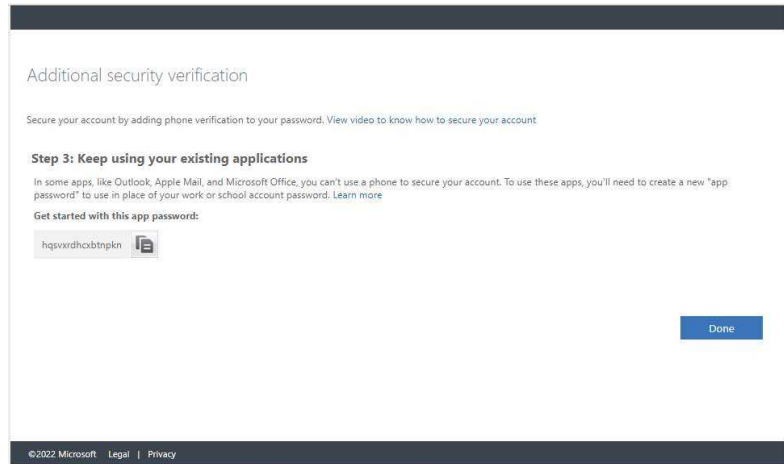
766326

Cancel

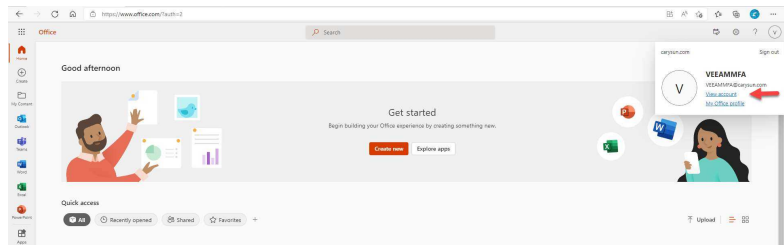
Verify

©2022 MicrosoftLegalPrivacy

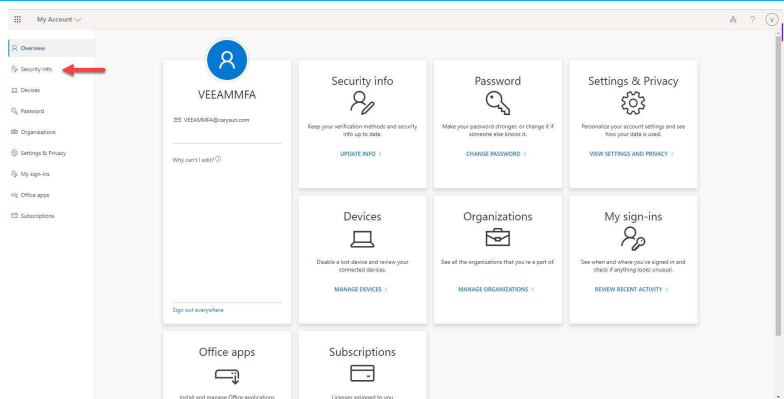
27. In Step 3, copy and save the app password, and click Done.



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.



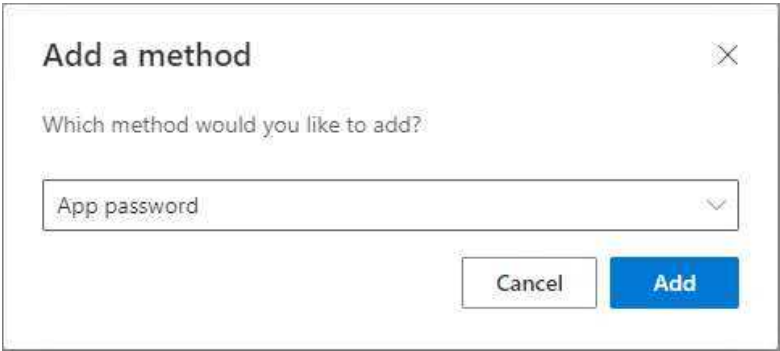
30. On the My account page, select Security info.



31. On the Security info page, select the +Add method.



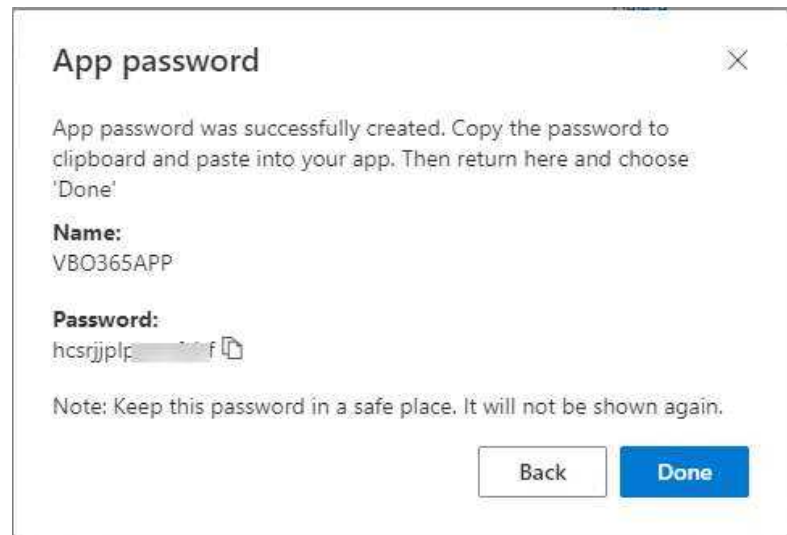
32. On the Add Method, select App password and click Add.



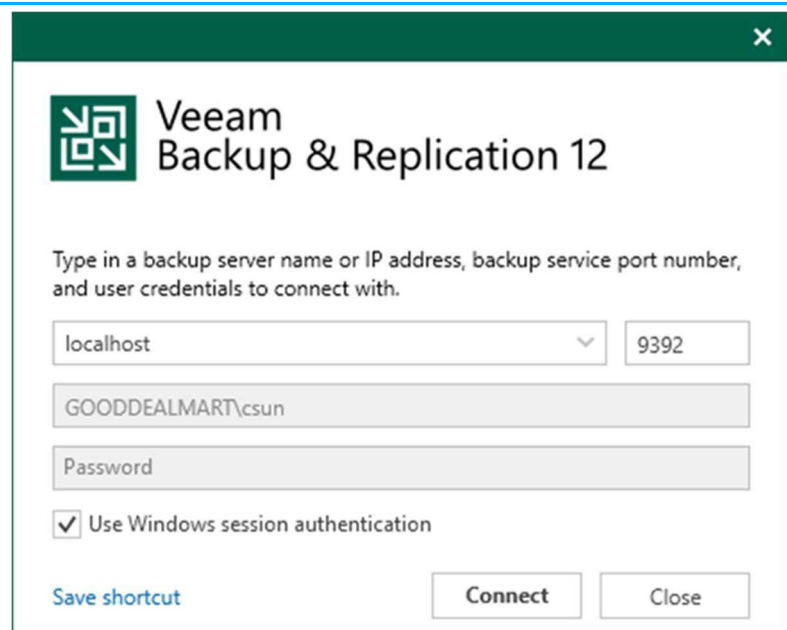
33. Type VBO365APP as the name of the App password, and click Next.



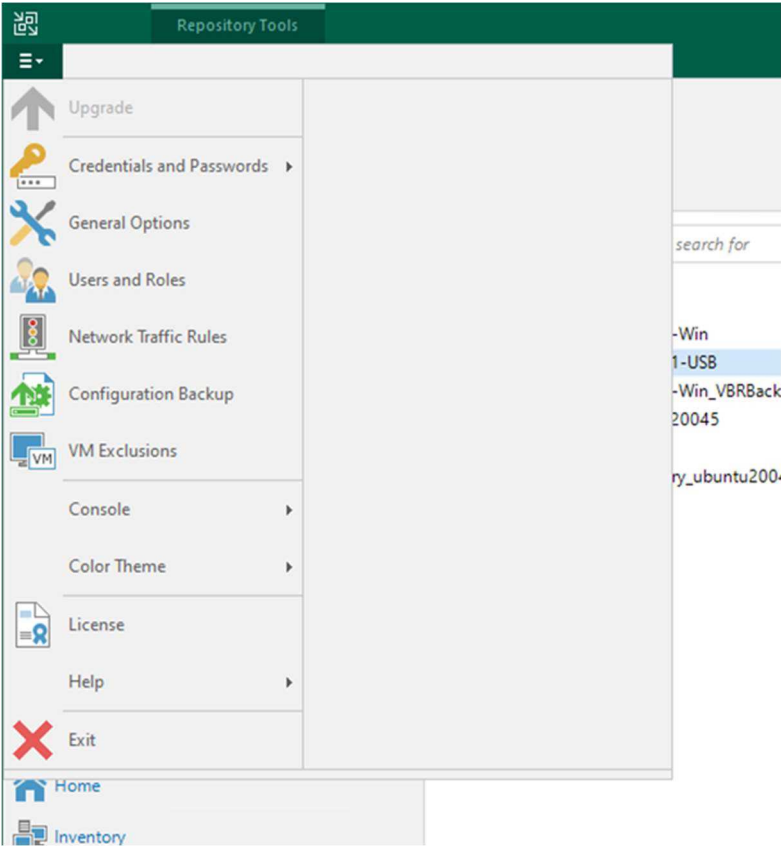
34. Copy and keep the password in a safe place. Then, it will not be shown again.
35. Click Done.



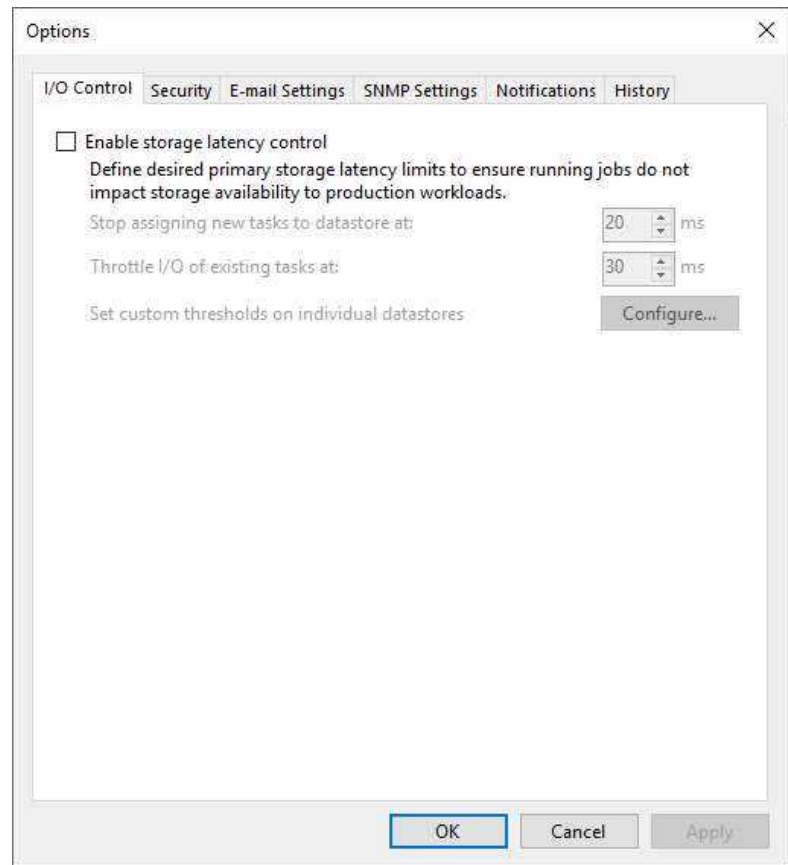
36. Log in to the Veeam Backup and replication manager server.
37. Open the Veeam Backup & Replication Console and click Connect.



38. Select General Options from the main menu.



39. On the Options page,
select Email Settings.



- 40. Select Enable e-mail notification (recommended) on the Email Settings page.
- 41. In the SMTP server field, enter smtp.sendgrid.net and click Advanced.

Options

I/O ControlSecurityE-mail SettingsSNMP SettingsNotificationsHistory

☒ Enable e-mail notifications (recommended)

SMTP server:

smtp.office365.com

Advanced...

From:

To:

Subject:

[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

Test Message

Send daily summary at: 10:00 PM ⓘ

Notify on:

☒ Success

☒ Warning

☒ Failure

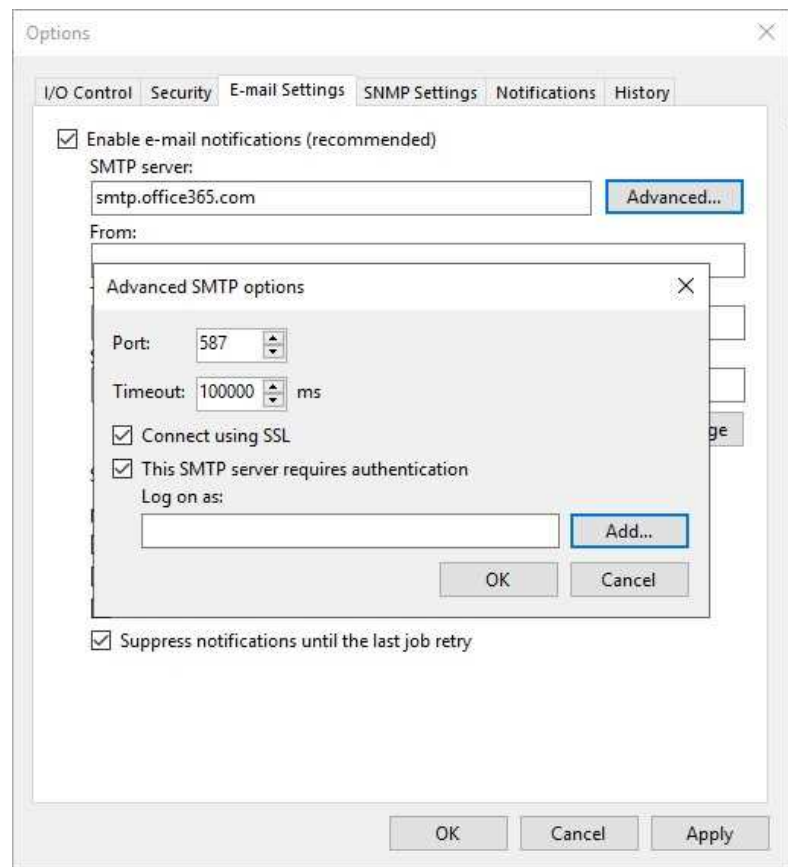
☒ Suppress notifications until the last job retry

OK

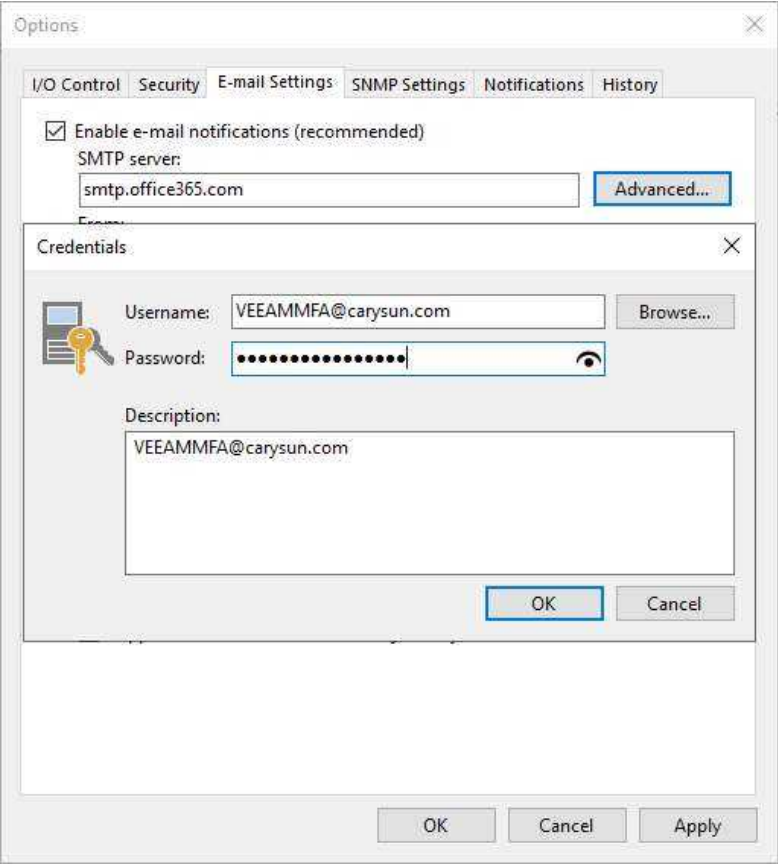
Cancel

Apply

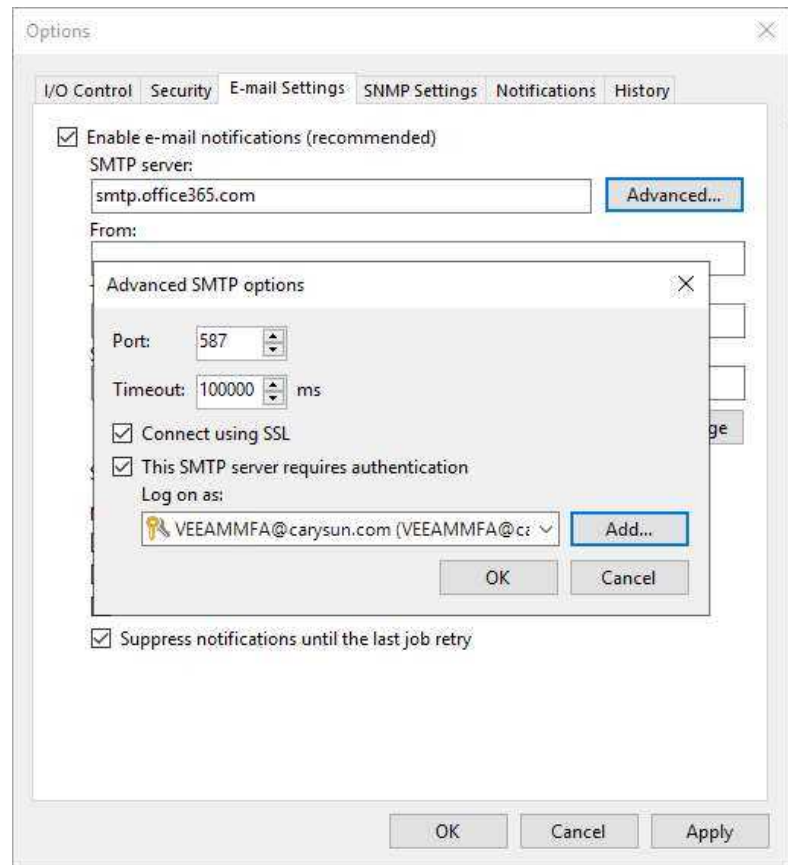
42. On the Advanced SMTP options page, enter 587 in the Port field.
43. Use 100000 milliseconds as the Timeout.
44. Select Connect using SSL.
45. Select This SMTP server requires authentication.
46. Click Add to add a credential as Log on as account.



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.



48. On the Advanced SMTP options page, click OK.



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.

The screenshot shows the 'Options' dialog box with the 'E-mail Settings' tab selected. The 'Enable e-mail notifications (recommended)' checkbox is checked. The 'SMTP server' field contains 'smtp.office365.com'. The 'From' field contains 'VEEAMMFA@carysun.com'. The 'To' field contains 'csun@triconelite.com'. The 'Subject' field contains a template string: '[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%'. There is a 'Test Message' button. The 'Send daily summary at' dropdown is set to '10:00 PM'. Under 'Notify on:', the checkboxes for 'Success', 'Warning', 'Failure', and 'Suppress notifications until the last job retry' are all checked. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Options

I/O Control Security E-mail Settings SNMP Settings Notifications History

☒ Enable e-mail notifications (recommended)

SMTP server:
smtp.office365.com Advanced...

From:
VEEAMMFA@carysun.com

To:
csun@triconelite.com

Subject:
[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

Test Message

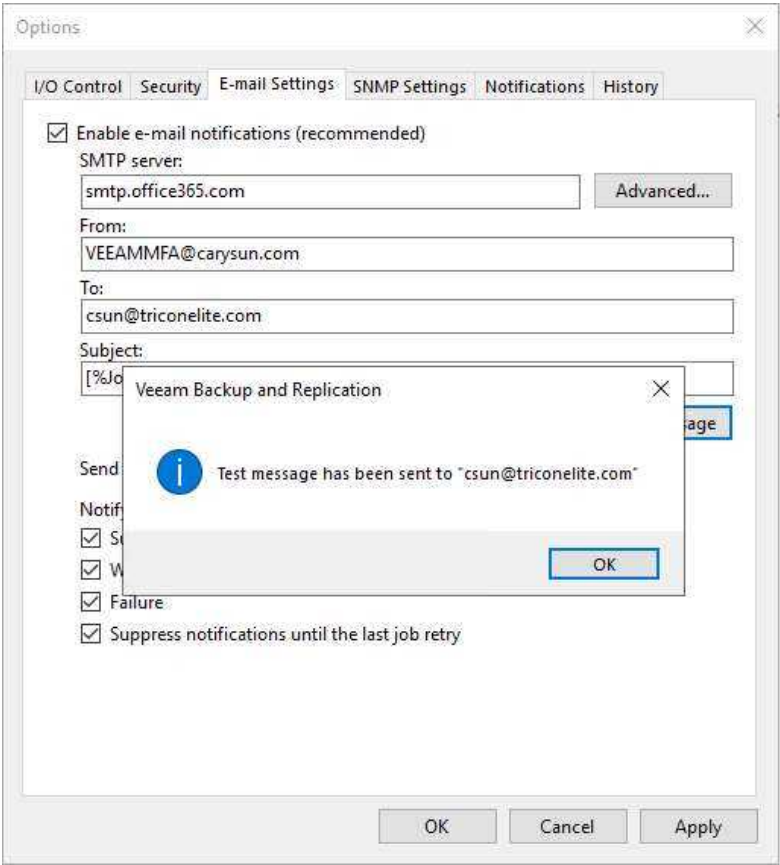
Send daily summary at: 10:00 PM ⓘ

Notify on:

- ☒ Success
- ☒ Warning
- ☒ Failure
- ☒ Suppress notifications until the last job retry

OK Cancel Apply

52. Ensure the test email was successfully sent to recipients, and click OK.



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.

The screenshot shows the 'Options' dialog box with the 'E-mail Settings' tab selected. The 'Enable e-mail notifications (recommended)' checkbox is checked. The SMTP server is set to 'smtp.office365.com'. The 'From' field is 'VEEAMMFA@carysun.com' and the 'To' field is 'csun@triconelite.com'. The 'Subject' field contains a template: '[%JobResult%] %JobName% (%ObjectCount% objects) %Issues%'. There is a 'Test Message' button. The 'Send daily summary at' is set to '10:00 PM'. Under 'Notify on:', all three checkboxes (Success, Warning, Failure) are checked, and 'Suppress notifications until the last job retry' is also checked. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Options

I/O Control Security E-mail Settings SNMP Settings Notifications History

☒ Enable e-mail notifications (recommended)

SMTP server: smtp.office365.com Advanced...

From: VEEAMMFA@carysun.com

To: csun@triconelite.com

Subject: [%JobResult%] %JobName% (%ObjectCount% objects) %Issues%

Test Message

Send daily summary at: 10:00 PM ⓘ

Notify on:

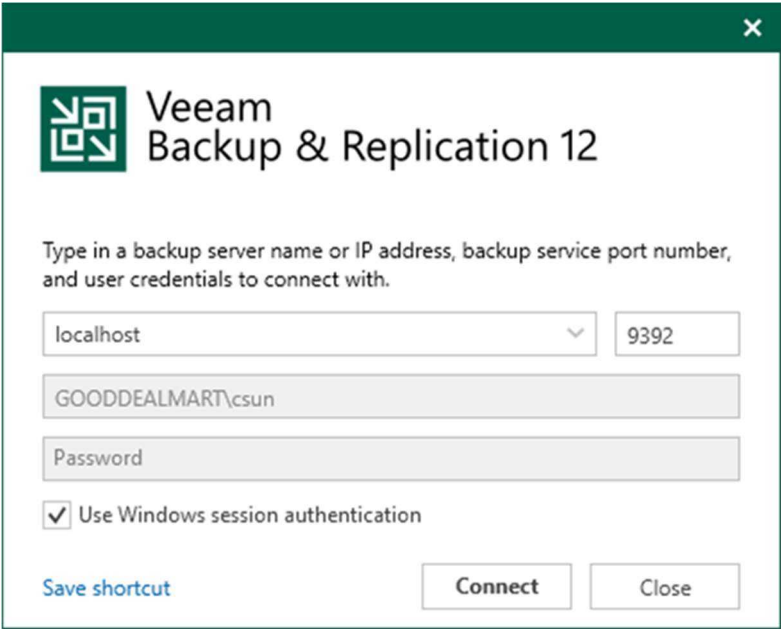
- ☒ Success
- ☒ Warning
- ☒ Failure
- ☒ Suppress notifications until the last job retry

OK Cancel Apply

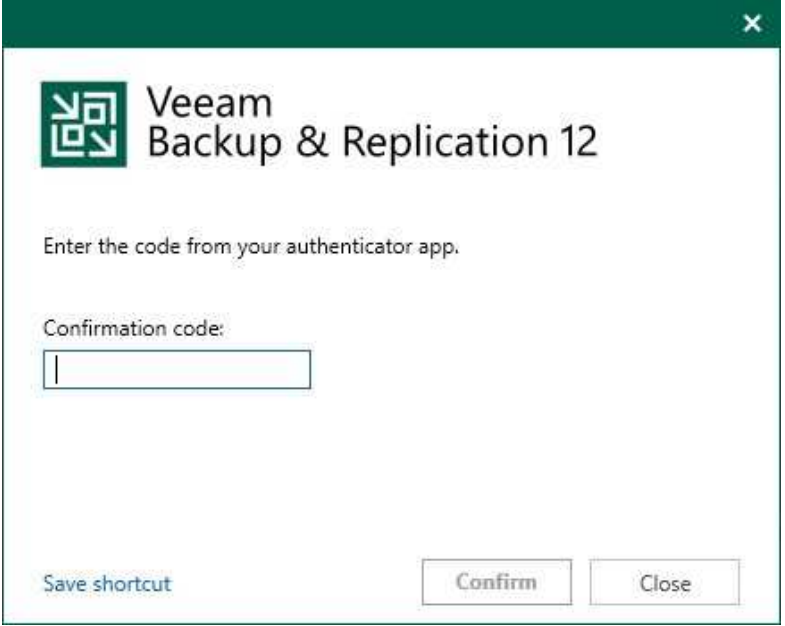
Enable Configuration Backup

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.

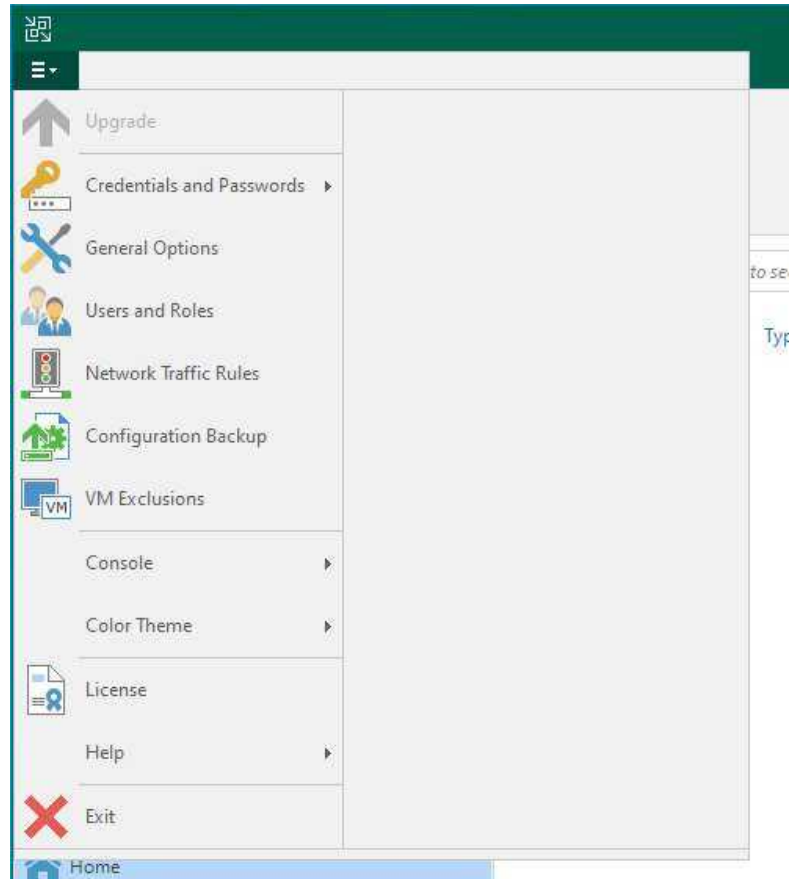
Instructions	Screenshot (if applicable)
1. Log in to the Veeam Backup and replication manager server. 2. Open the Veeam Backup & Replication Console and click Connect.	 The screenshot shows the 'Veeam Backup & Replication 12' console window. It has a dark green title bar with a close button. The main area is white with the Veeam logo and title. Below the title, it says 'Type in a backup server name or IP address, backup service port number, and user credentials to connect with.' There are three input fields: a dropdown menu showing 'localhost', a text box with '9392', and a text box with 'GOODDEALMART\csun'. Below these is a 'Password' field. A checkbox labeled 'Use Windows session authentication' is checked. At the bottom, there are three buttons: 'Save shortcut' (blue text), 'Connect' (white button), and 'Close' (white button).

3. Enter the MFA Confirmation code and click Confirm.



A screenshot of a Veeam Backup & Replication 12 MFA confirmation dialog box. The dialog has a dark green header bar with a close button (X) in the top right corner. Below the header, the Veeam logo is on the left, followed by the text "Veeam Backup & Replication 12". The main content area contains the instruction "Enter the code from your authenticator app." followed by the label "Confirmation code:" and a text input field with a cursor. At the bottom, there are three buttons: "Save shortcut" on the left, and "Confirm" and "Close" on the right.

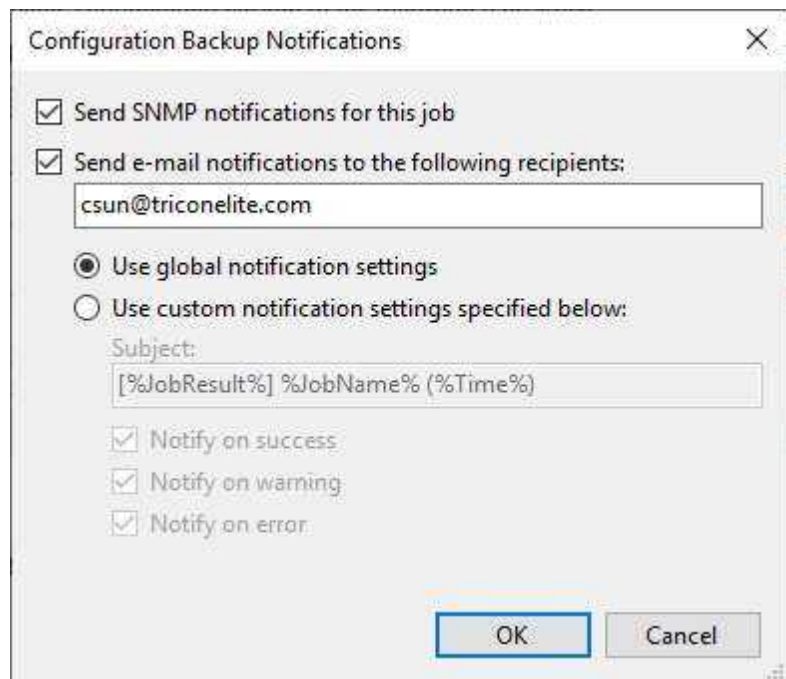
4. Select Configuration Backup from the Main menu.



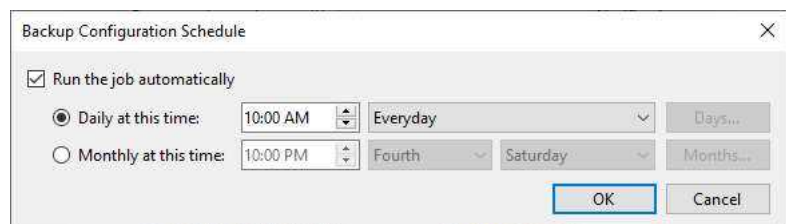
5. Select Enable configuration backup to the following repository checkbox on the Configuration Backup Settings page.
6. Select the backup repository from the drop-down list.
7. Enter the restore points number in the Restore points to keep field.
8. Click Notifications.

The screenshot shows the 'Configuration Backup Settings' dialog box. It has a title bar with a close button. The 'Backup' section is active, showing a checked checkbox for 'Enable configuration backup to the following repository:'. Below this is a dropdown menu showing 'Backup Repository_HPHV02 (Created by GOODDEALMART\csun at 1/10/2023)' and a status bar indicating '688 GB free of 931 GB'. There are three input fields: 'Restore points to keep' with a value of 10, 'Perform backup on:' set to 'Daily at 10:00 AM', and 'Last successful backup:' showing '1/7/2023 10:00 AM'. To the right of these fields are three buttons: 'Notifications', 'Schedule...', and 'Backup now'. Below the 'Backup' section is an unchecked checkbox for 'Enable backup file encryption'. Underneath it is a 'Password:' label, a text input field, and an 'Add...' button. A 'Manage passwords' link is also present. A warning message with an exclamation mark icon states: 'Saved credentials, backup server certificate and cloud backup appliance data will not be included in the configuration backup until encryption is enabled'. The 'Restore' section at the bottom has a label 'Restore the configuration backup to this server:' and a 'Restore...' button. At the very bottom are 'OK', 'Cancel', and 'Apply' buttons.

9. Select Send SNMP notification checkbox's Configuration Backup Notification page. If necessary.
10. Select Send e-mail notifications to the following recipients checkbox 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.

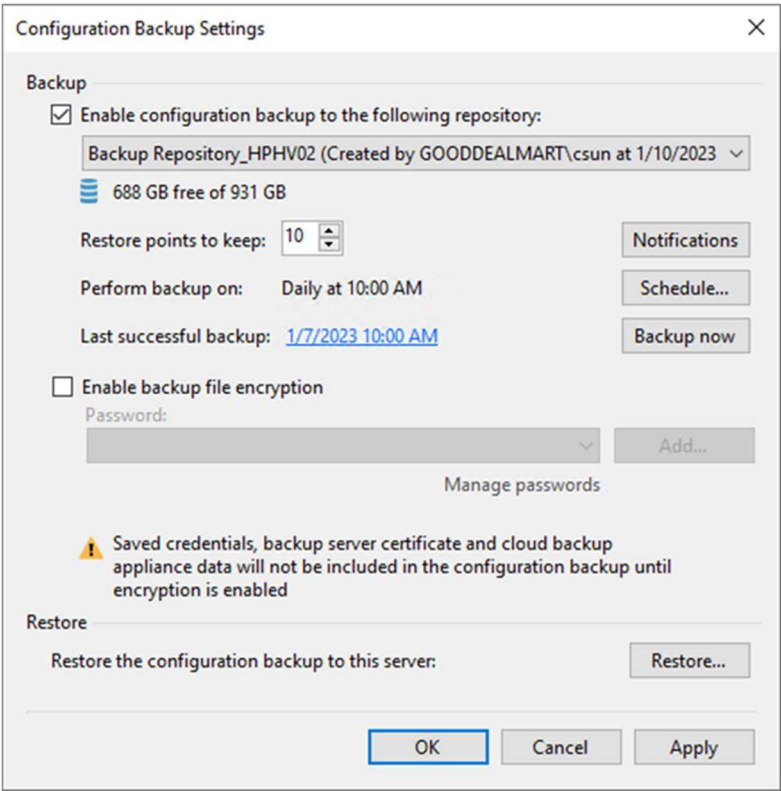


13. Click Schedule on the Configuration Backup Settings page.
14. On the Backup Configuration Schedule page, select Run the job automatically checkbox.
15. Select Daily at this time, enter the backup time in the time field and select every day from the drop-down list.

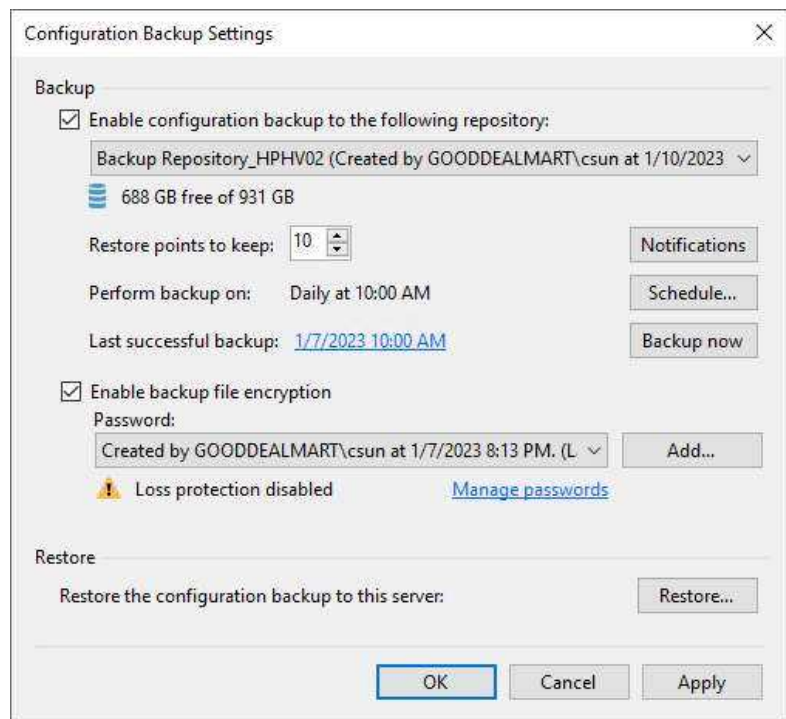


16. Click OK.

17. On the Configuration Backup Settings page, click Backup now if you want to back up manually.



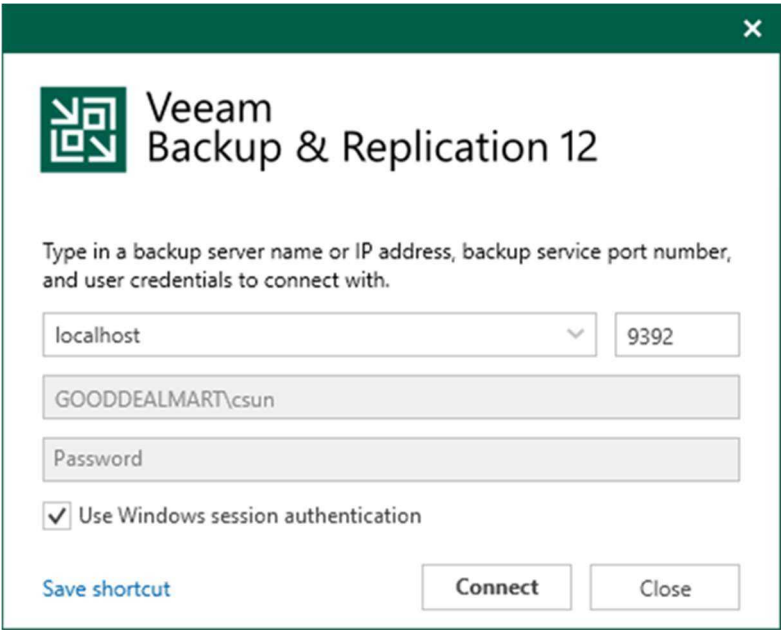
18. Select Enable backup file encryption on the Configuration Backup Settings page.
19. Select a password from the Password drop-down list or click Add to create a password.
20. Click OK.



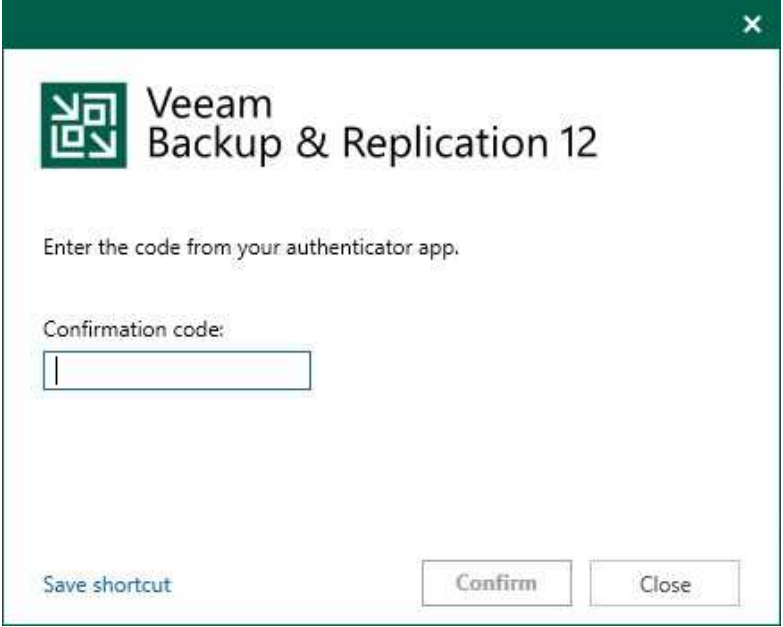
Configure Best Practices Analyzer

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.	 The screenshot shows a window titled "Veeam Backup & Replication 12" with a close button (X) in the top right corner. The window contains the Veeam logo and the text "Type in a backup server name or IP address, backup service port number, and user credentials to connect with." Below this text are four input fields: a dropdown menu showing "localhost", a text box containing "9392", a text box containing "GOODDEALMART\csun", and a password field labeled "Password". There is a checkbox labeled "Use Windows session authentication" which is checked. At the bottom left is a link "Save shortcut", and at the bottom right are two buttons: "Connect" and "Close".

3. Enter the MFA Confirmation code and click Confirm.



A screenshot of a Veeam Backup & Replication 12 MFA confirmation dialog box. The dialog has a dark green header bar with a close button (X) in the top right corner. Below the header, the Veeam logo is on the left, and the text "Veeam Backup & Replication 12" is on the right. The main area contains the instruction "Enter the code from your authenticator app." followed by the label "Confirmation code:" and a text input field with a cursor. At the bottom, there are three buttons: "Save shortcut" on the left, and "Confirm" and "Close" on the right.

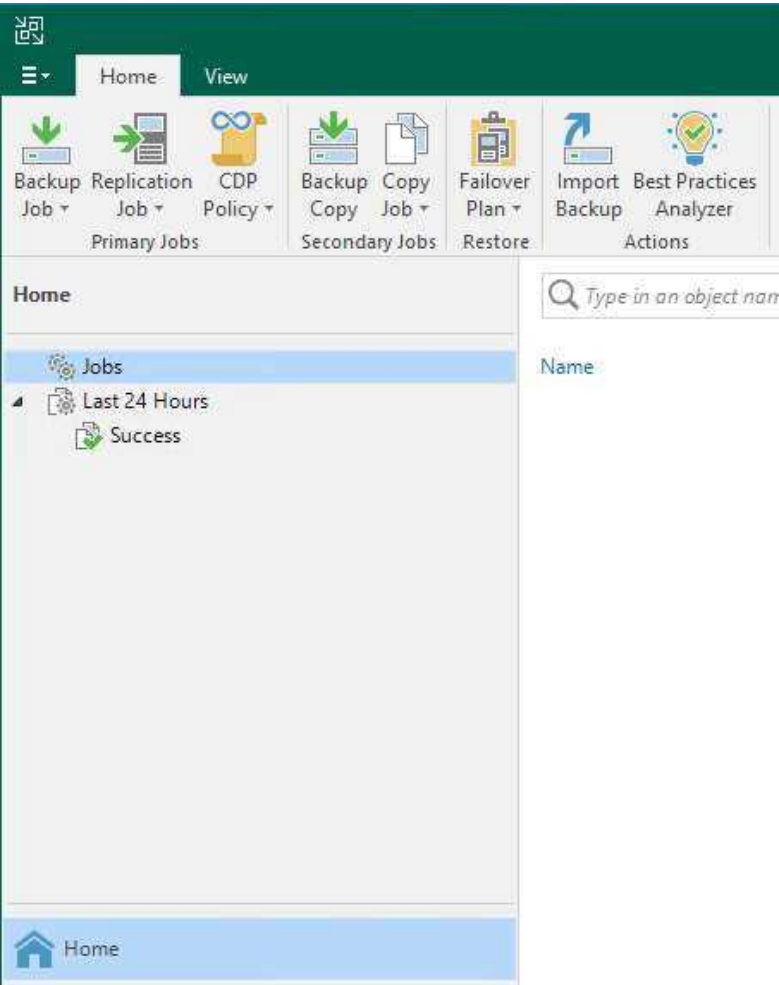
Veeam Backup & Replication 12

Enter the code from your authenticator app.

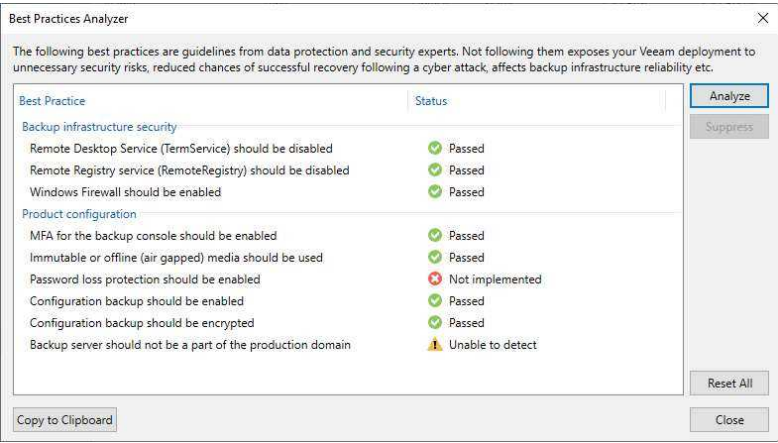
Confirmation code:

Save shortcut Confirm Close

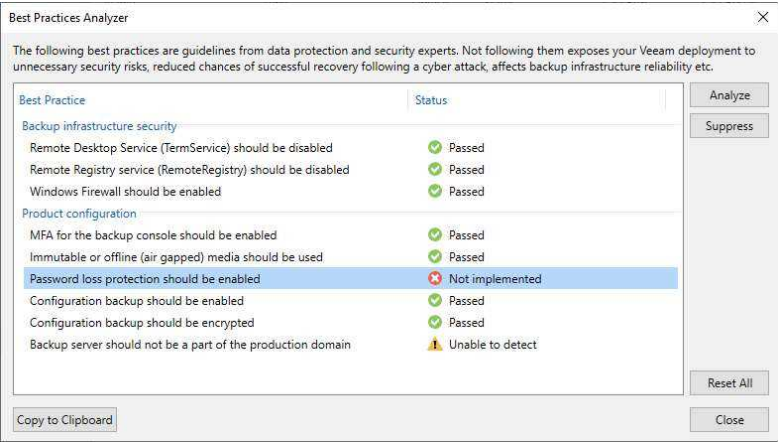
4. Select the Best Practices Analyzer on the Home page.



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.



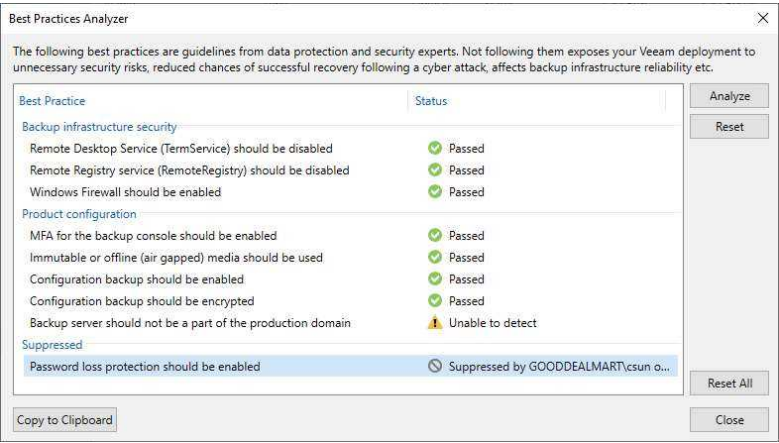
6. Select the parameter and click Suppress to skip the security check.



7. Comment briefly on the Note field on the Edit Note page for future reference, and click OK.



8. Click Close on the Best Practices Analyzer page.



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:

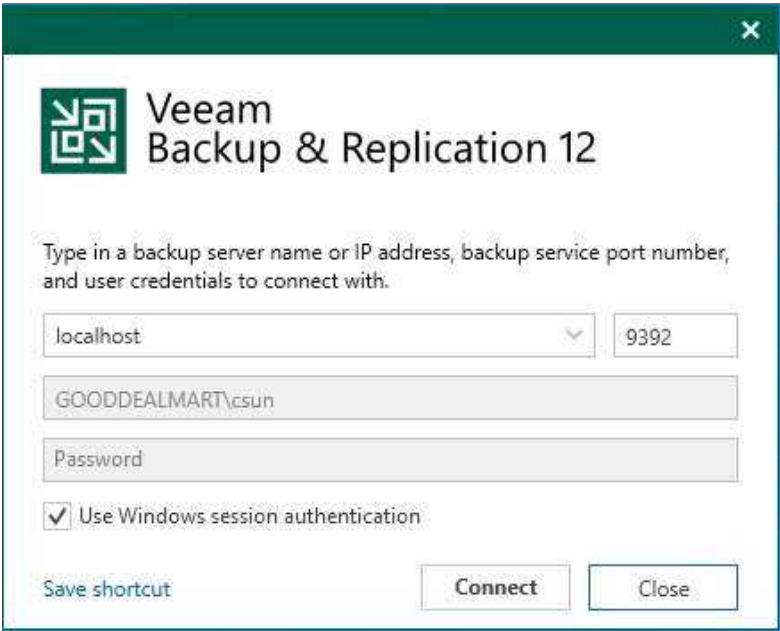
- **Backup and replication:** Veeam Backup provides backup and replication of virtual machines, physical servers, and cloud workloads. Backups can be scheduled, and Veeam Backup offers several backup methods, including incremental and full backups.
- **Recovery:** Veeam Backup allows quick and easy recovery 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.

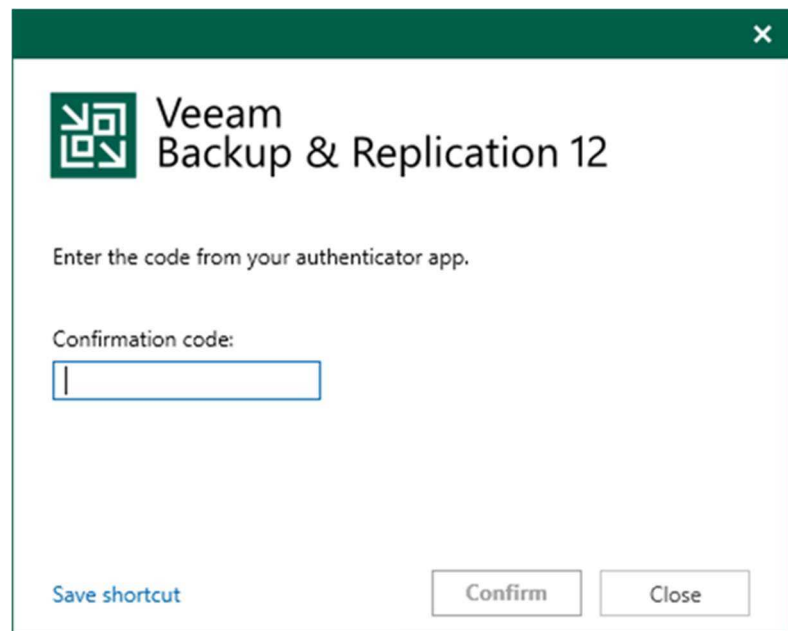
Create a Backup job to backup the specified VMs

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.

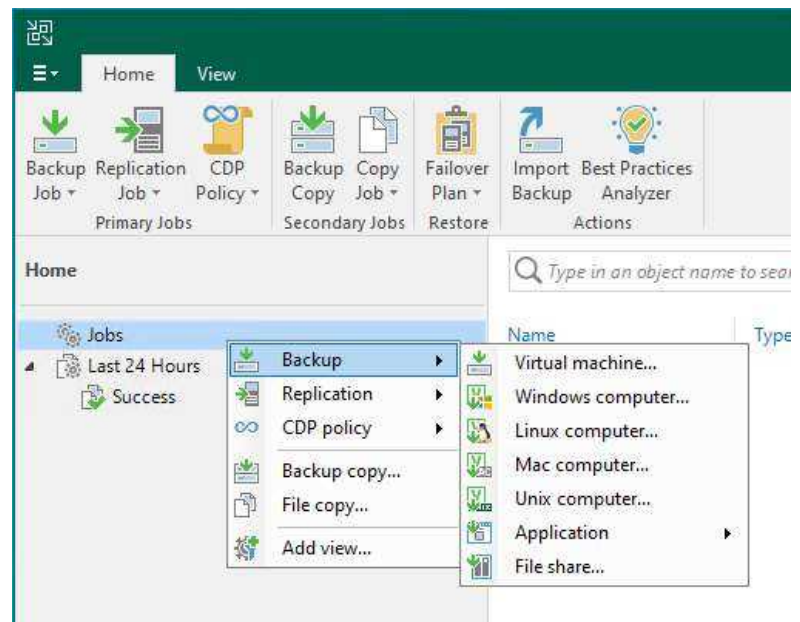
This procedure creates a backup job to back up the production VMs specified.

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.	

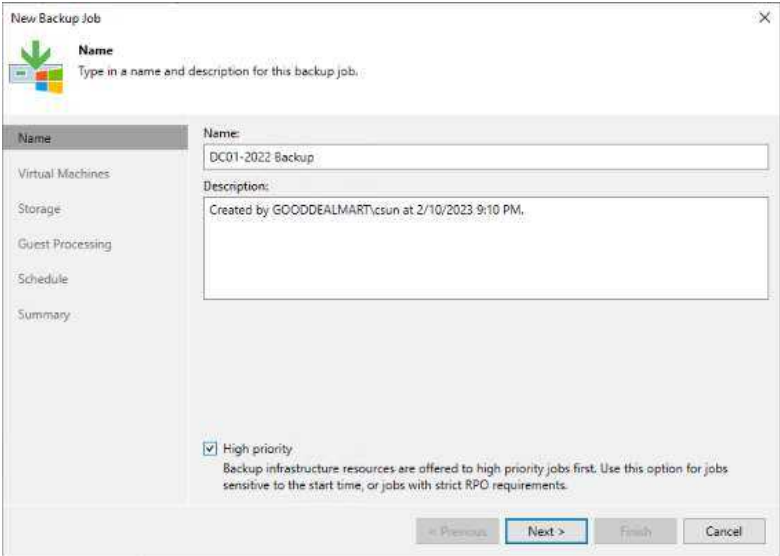
3. Enter the MFA Confirmation code and click Confirm.



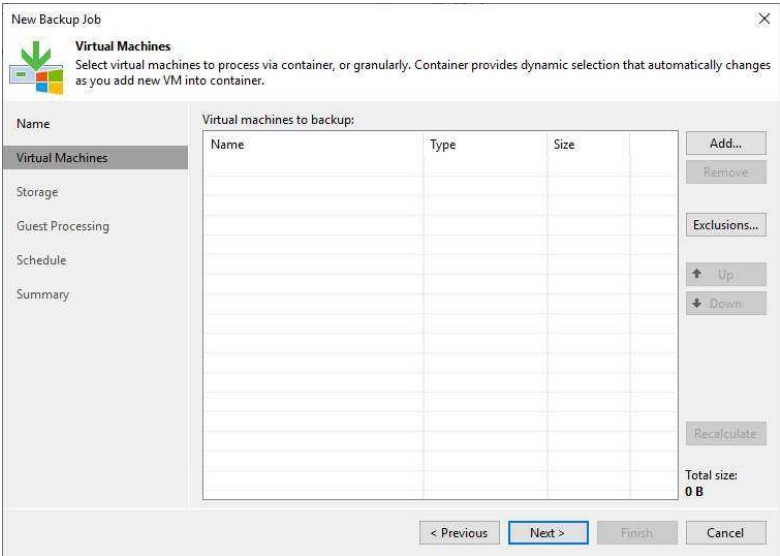
4. Select Jobs on the Home page and right-click Jobs.
5. Select Backup and click Virtual machine.



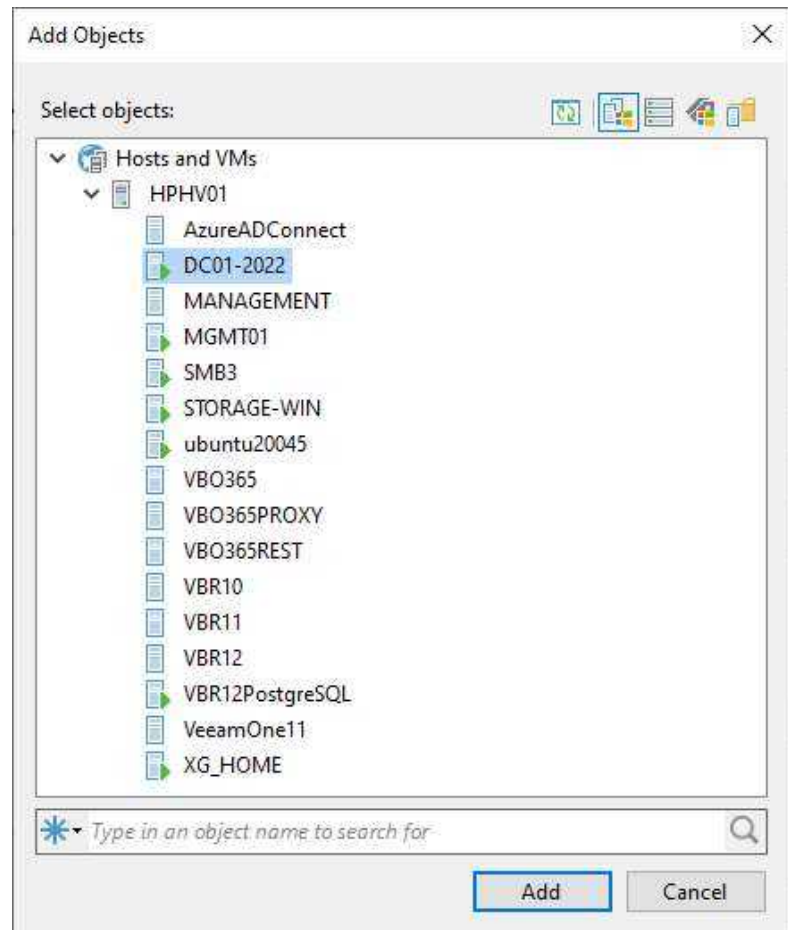
- 6. On the Name page, enter a name for the backup job in the Name field.
- 7. Give a brief description in the Description field for the future.
- 8. Select the High priority checkbox if you want this job to allocate resources in the first place.
- 9. Click Next.



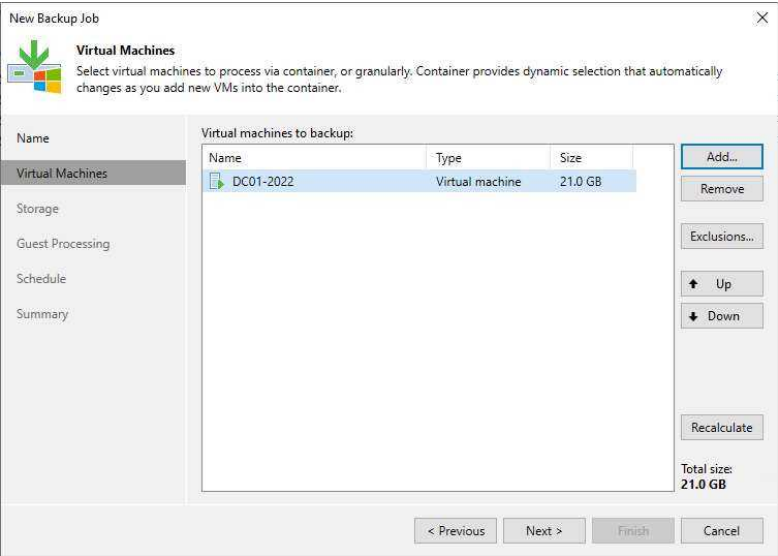
- 10. Click Add on the Virtual Machines page.



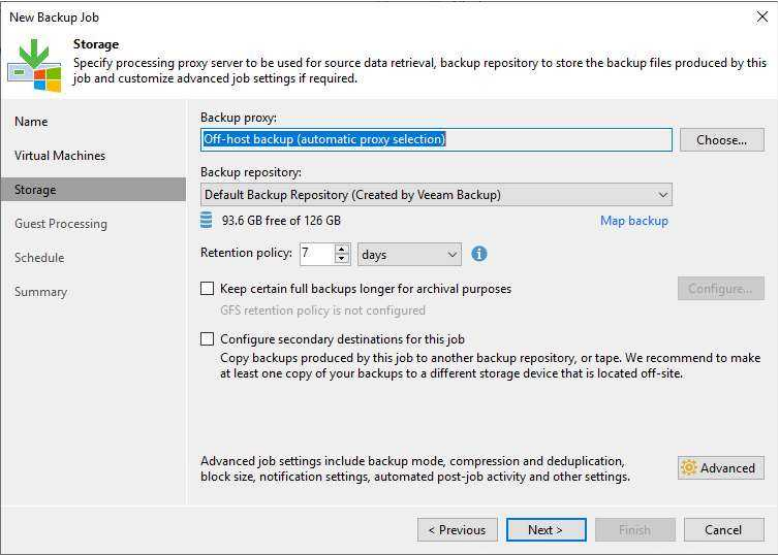
11. Select the VM from the Select objects list on the Add Objects page and click Add.
12. If you have multiple VMS that need to be backed up in the same backup job, you can repeat the step to add them.



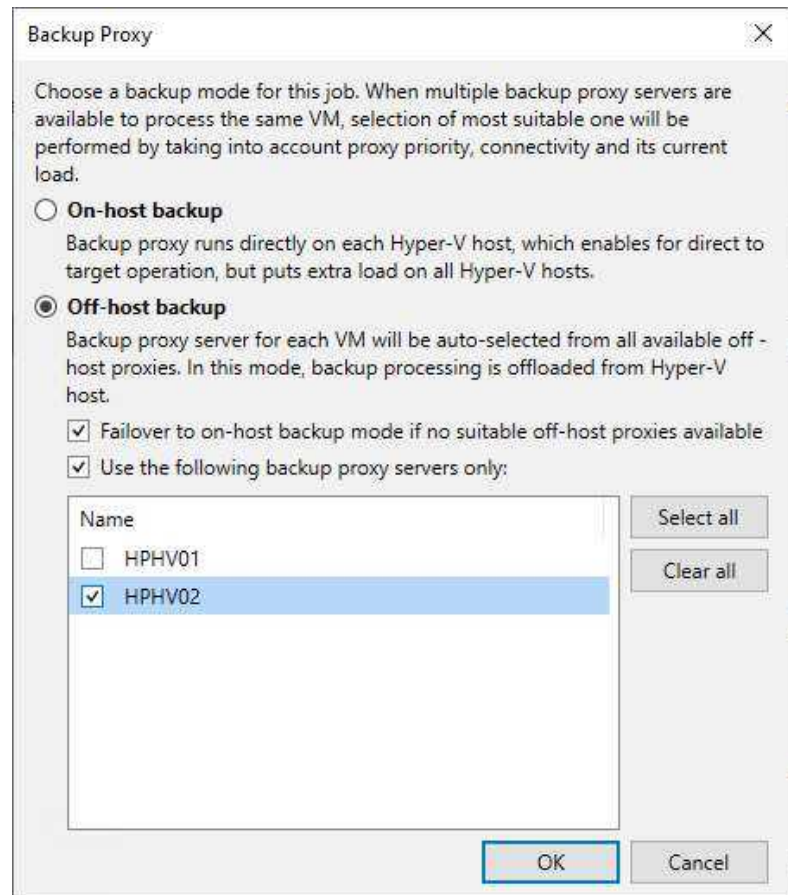
13. Click Next on the Virtual Machines page.



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) (automatic proxy selection) setting.



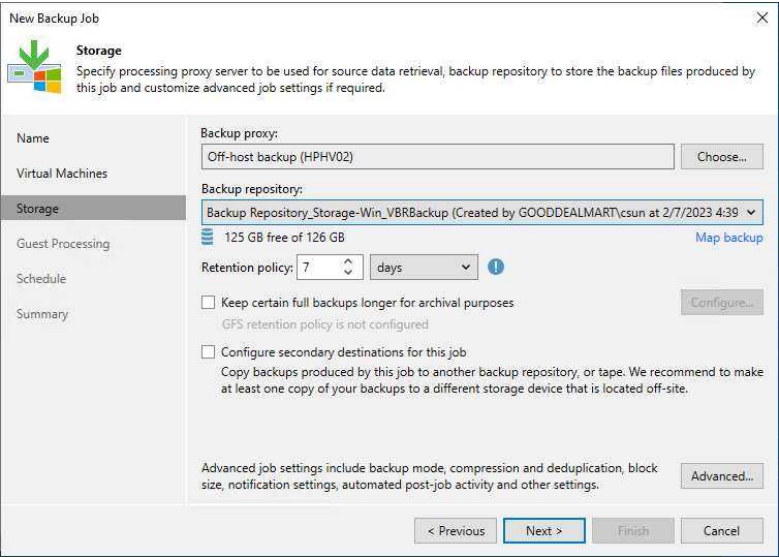
15. On the Backup Proxy page, if you select On-host backup mode, the source Microsoft HyperV host will serve as both the source host and the backup proxy. In this mode, Veeam Data Mover runs directly on the source host, which speeds up data retrieval but places additional strain on the host.
16. If you 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 & Replica will transition to on-host backup mode.
18. You unselect the Failover to on-host backup mode if no suitable off-host



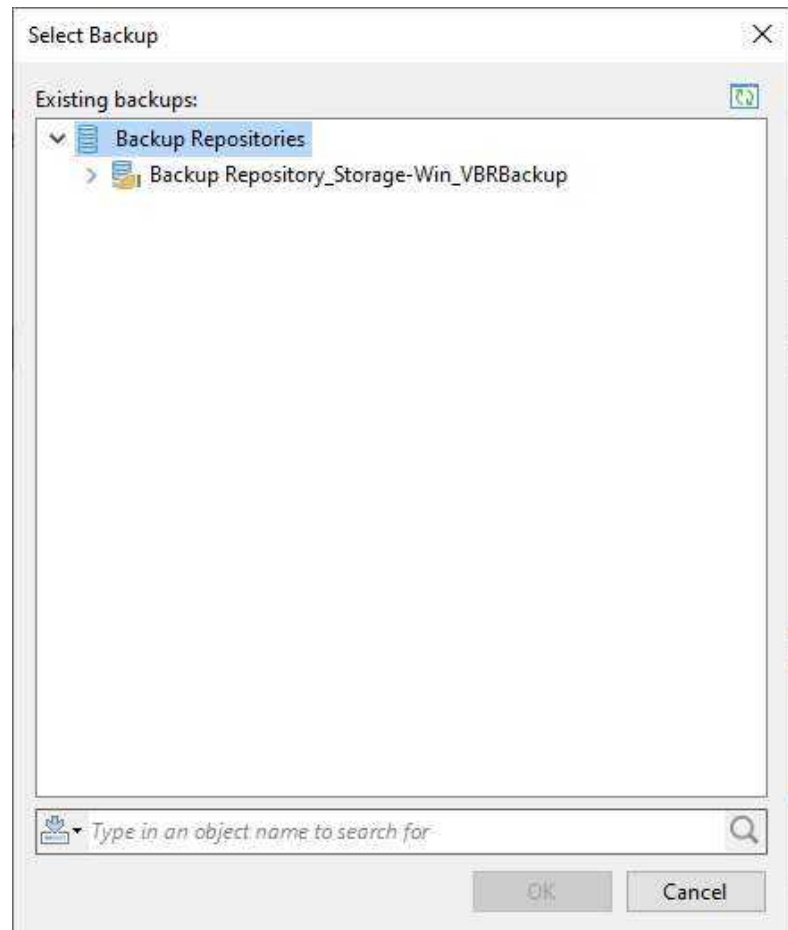
proxies are available in the checkbox. Still, the job will fail to start if off-host backup proxies are unavailable or configured properly.

19. Click OK.

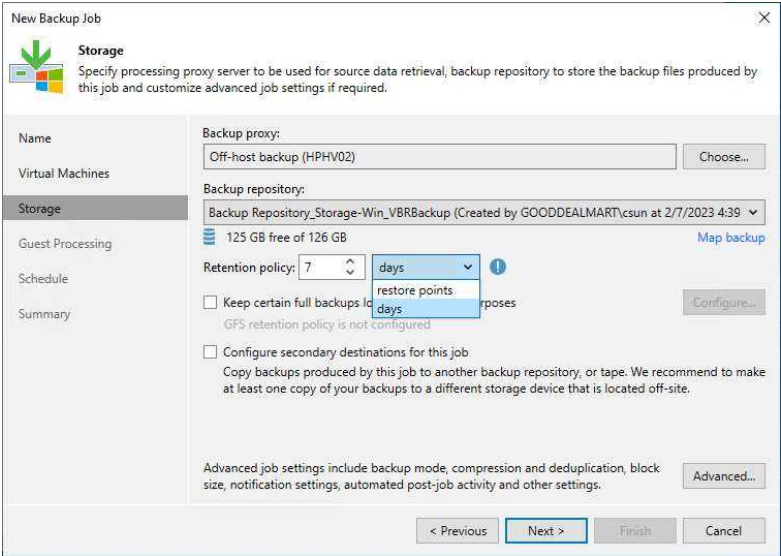
20. Select the backup repository from the Backup repository drop-down list where the created backup files must be saved.



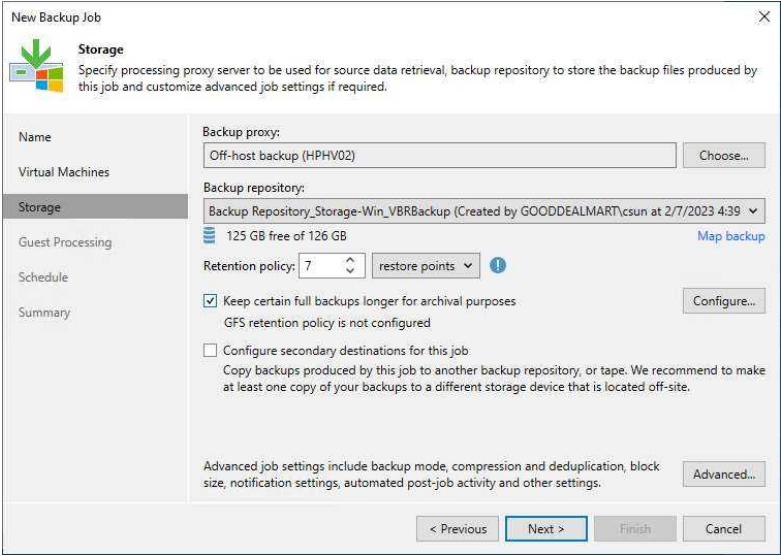
21. Click Map backup is helpful if you have relocated backup files to a new backup repository and want to point the job to existing backups in this new backup repository. Backup job mapping can also be used if the configuration database becomes corrupt and you need to reconfigure backup jobs.



- 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.



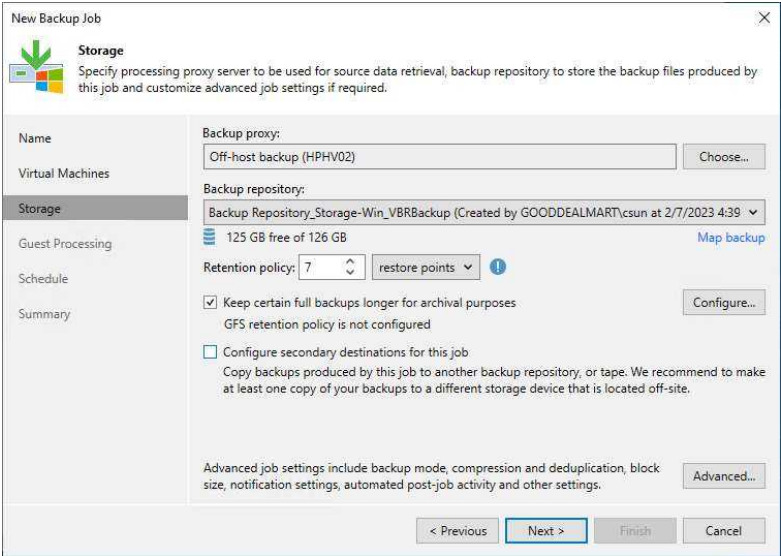
- 24. You can configure GFS retention policy settings for the backup job to ignore the short-term retention policy for some full backups and store them for long-term archiving.
- 25. Select the Keep certain full backups for longer for archival purposes. Then, if you need it, click Configure.



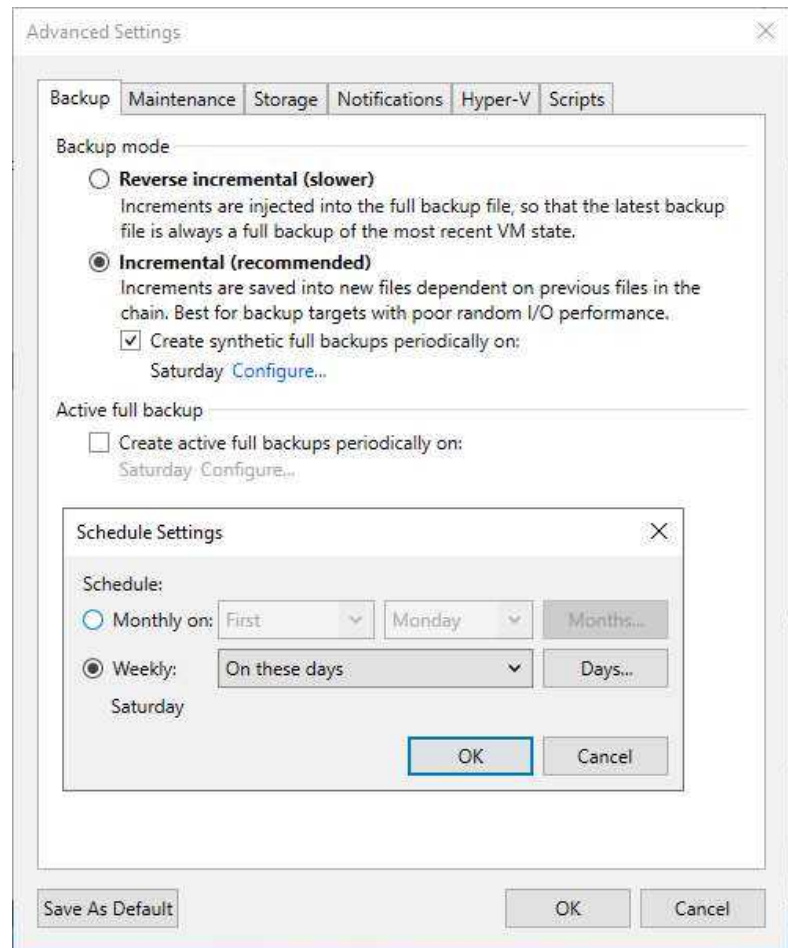
26. Select the Keep weekly full backups for check box, and specify the number of weeks you want to prevent restore points from being modified and deleted.
27. Select the Keep monthly full backups for check box, and specify the months you want to prevent restore points from being modified and deleted.
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.



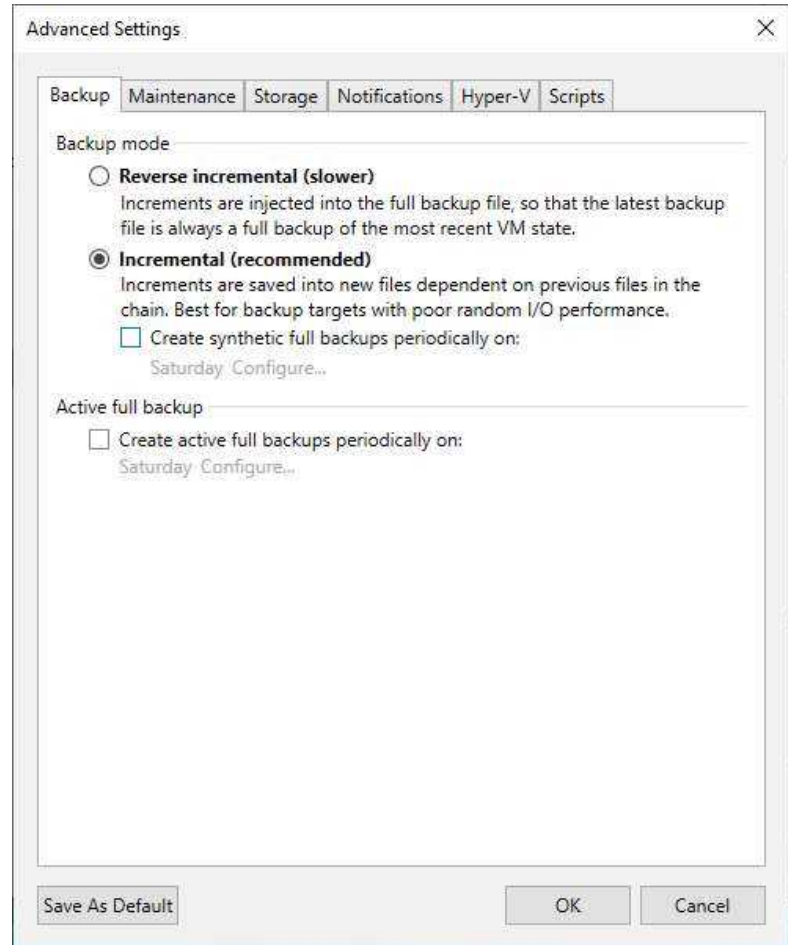
30. On the Storage page, click Advanced.



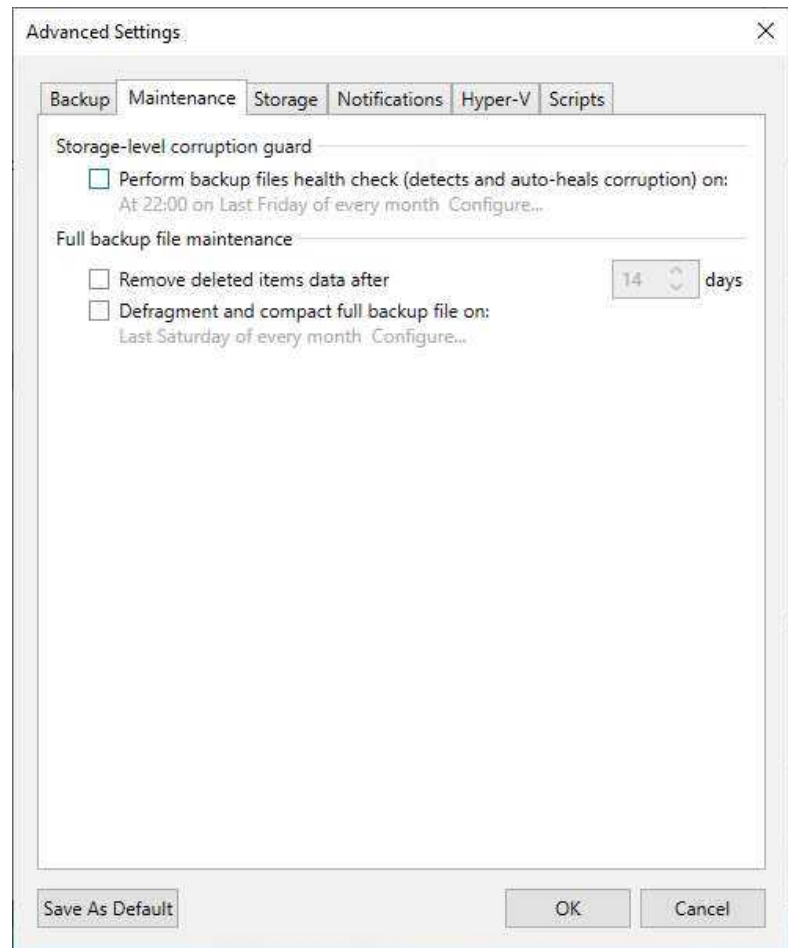
31. On the Backup page, select Incremental (recommended).
32. Select create synthetic full backups periodically or active full backups periodically checkbox.
33. Click Configure to schedule full backups periodically and click OK.



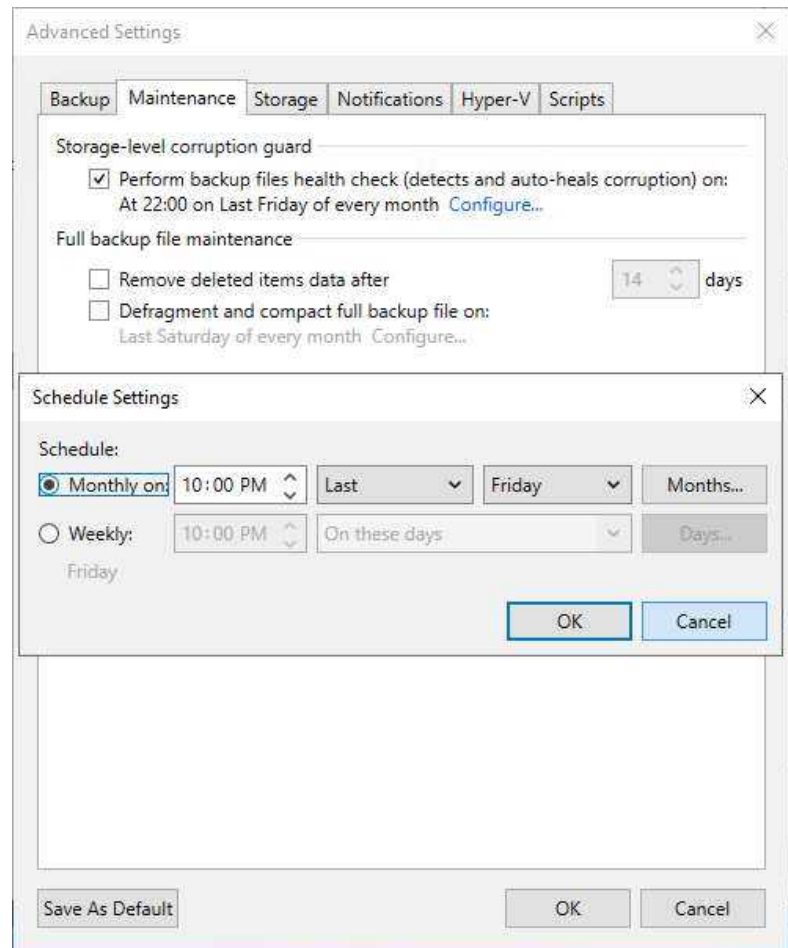
34. Select Incremental and disable synthetic full or active full backups to create a forever forward incremental backup chain if needed.



35. On the Advanced Settings, select Maintenance.



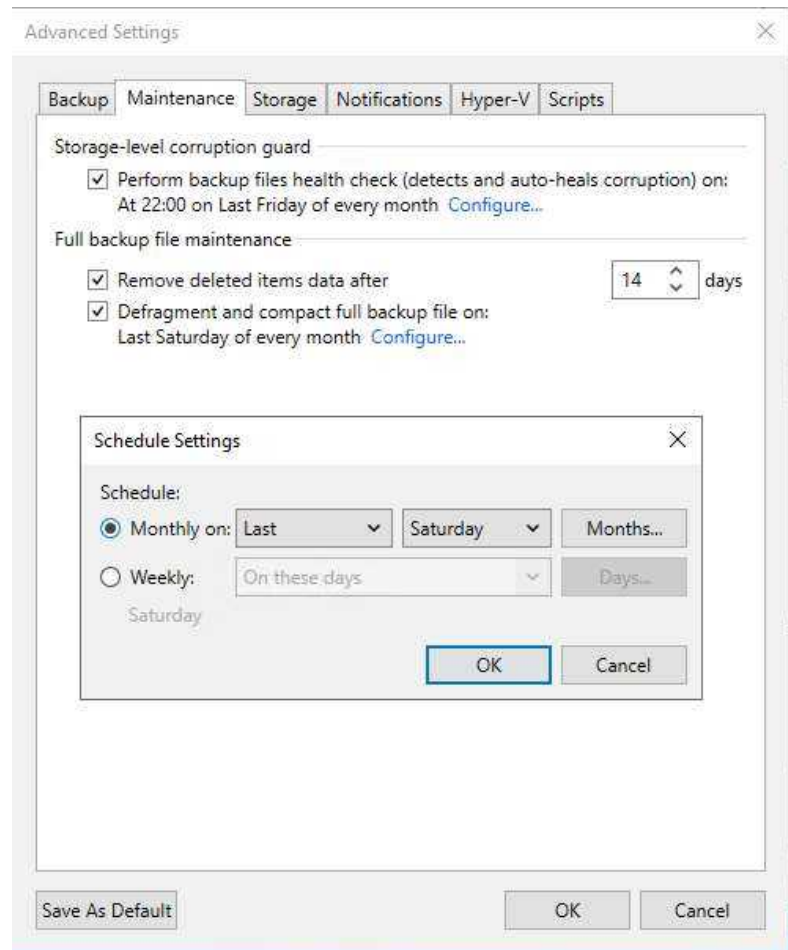
36. To regularly perform a health check on the backup chain's most recent restore point, select the Perform backup files health check (detects and auto-heals corrupt on) checkbox in the Storage-level corruption guard section.
37. Click Configure to set a timetable for the health check.



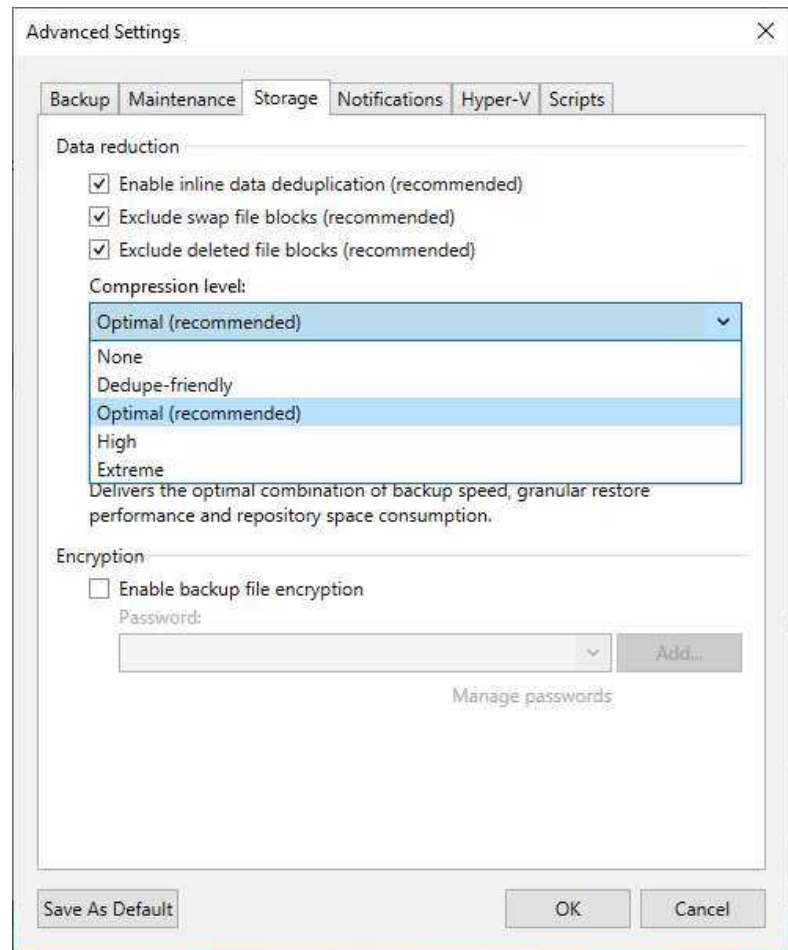
38. Select the Remove deleted items data after the checkbox and enter the few days you want backup data for deleted VMs to be kept.
39. Select the Defragment and compact full backup file checkbox and click Configure.
40. Set the schedule for the compact operation to compact a full backup periodically.

Note:

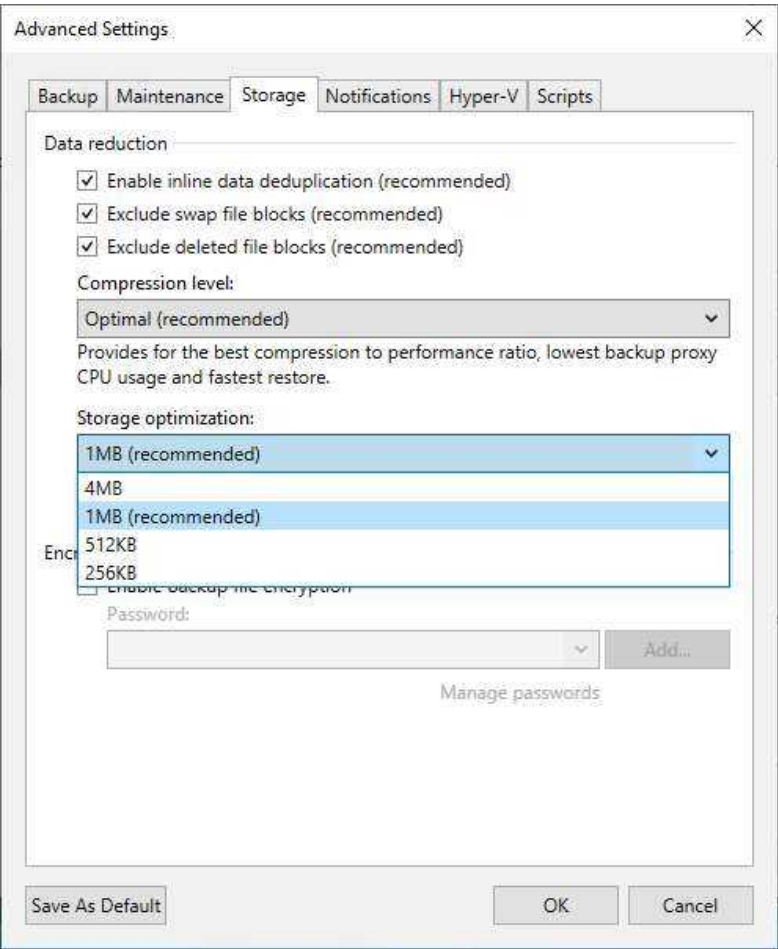
GFS retention is not compatible with defragment and compact functionality.



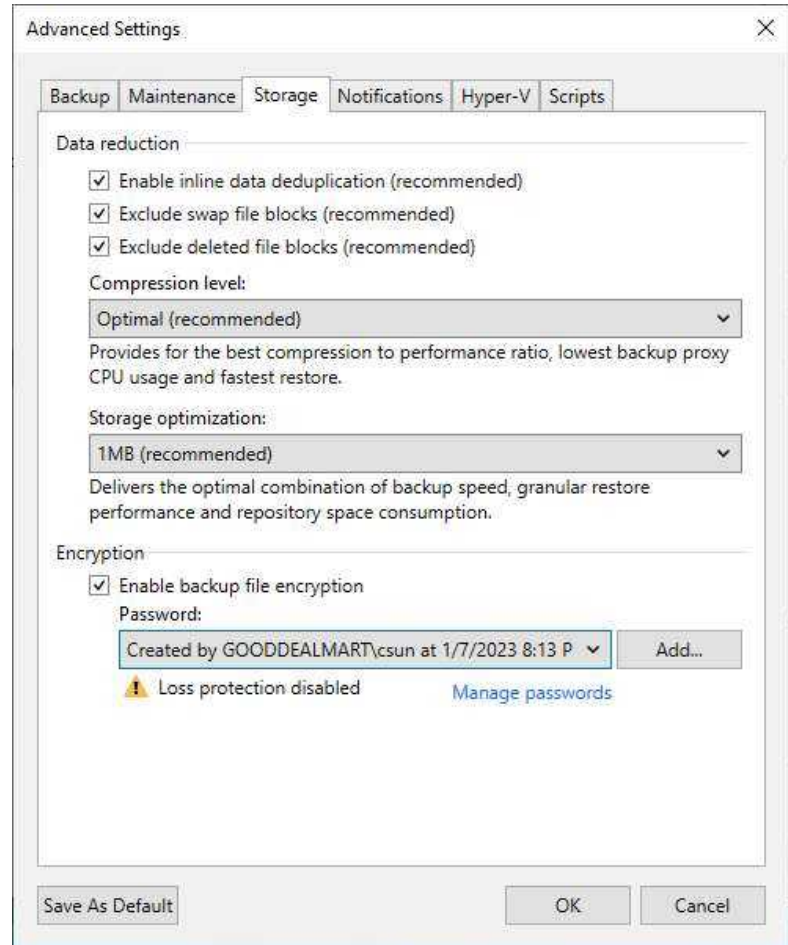
41. On Advanced Settings, select Storage.
42. Select the Enable inline data deduplication (recommended) checkbox.
43. Select the Exclude swap file blocks (recommended) checkbox.
44. Select the Exclude deleted file blocks (recommended) checkbox.
45. Select the compression level for the backup from the drop-down list.



46. Select the Storage optimization for the backup from the drop-down list.

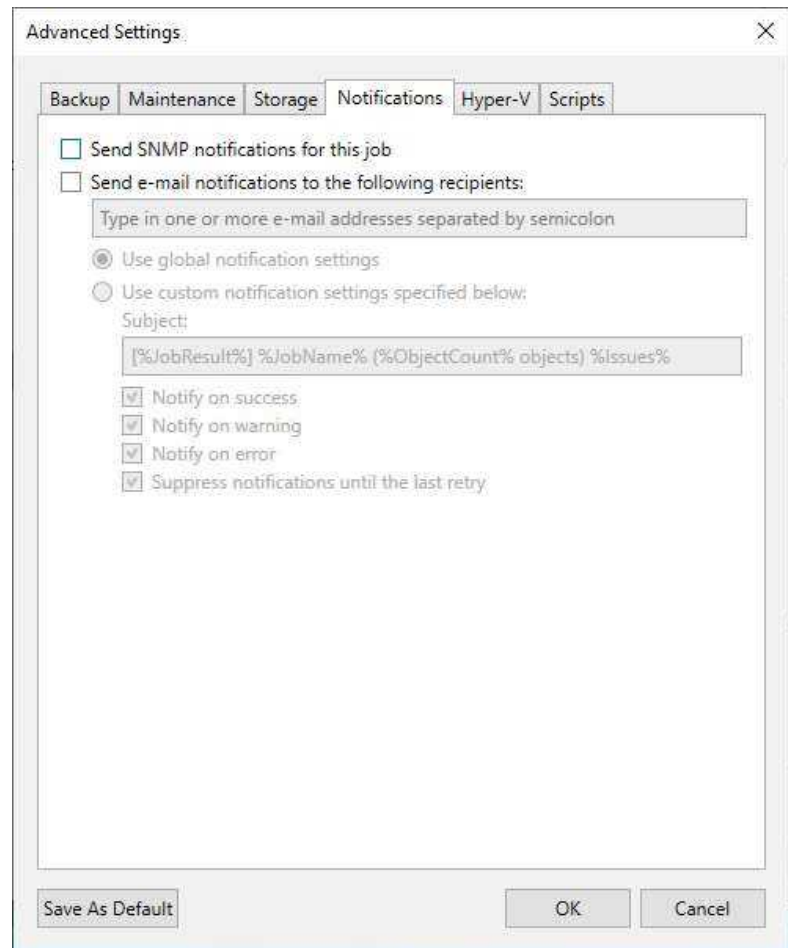


47. Select the Enable backup file encryption checkbox to encrypt the content of backup files.
48. Select a password from the drop-down list. Then, if you still need to do, click Add or use the Manage passwords link to create a new password.

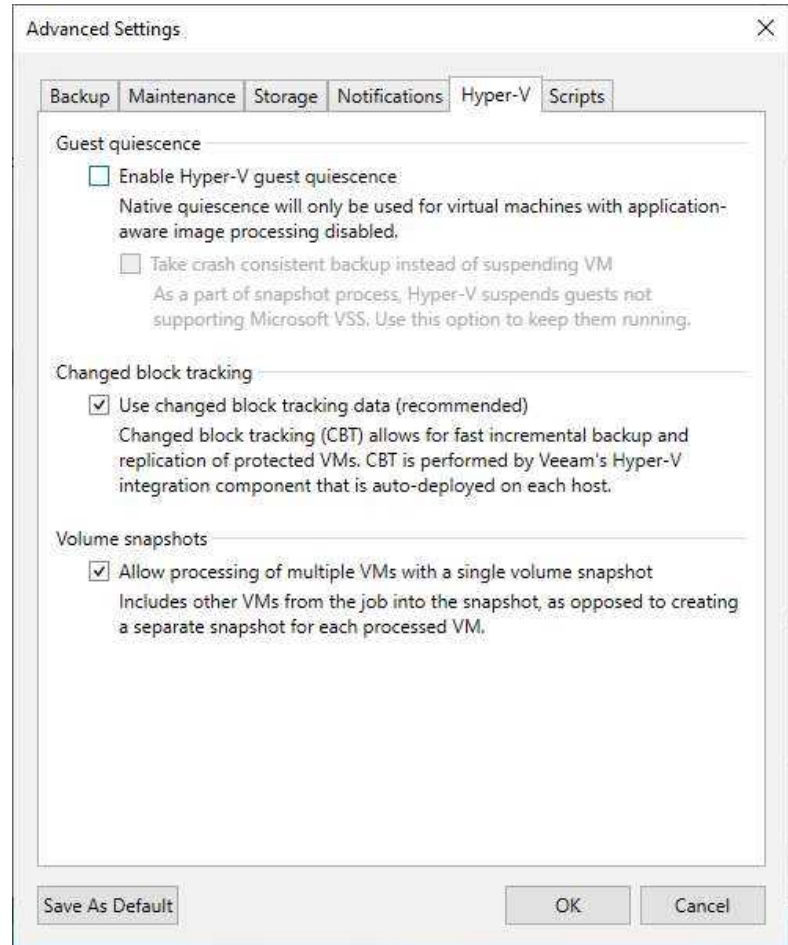


49. On the Advanced Settings, select No notifications.

50. Keep the default settings.

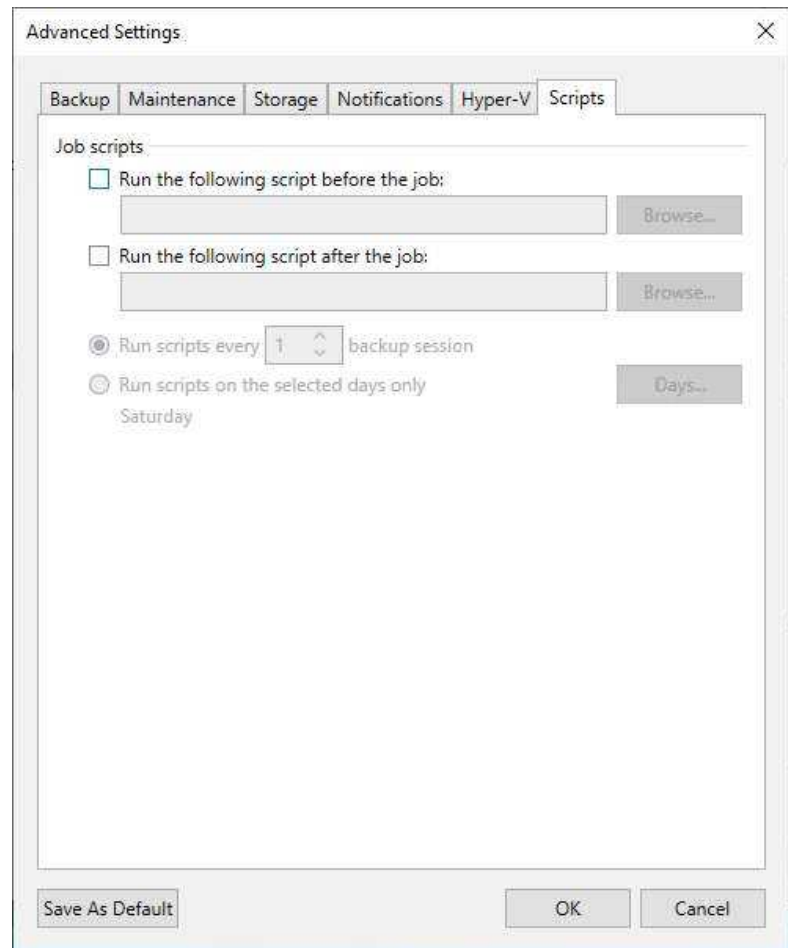


51. On the Advanced Settings, select Hyper-V.
52. Keep the default settings.

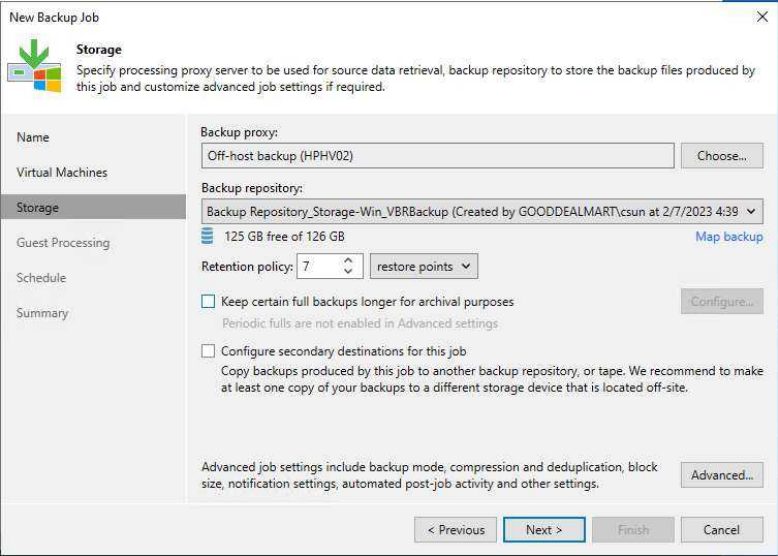


53. On the Advanced Settings page, click Scripts and keep the default settings.

54. Click OK.

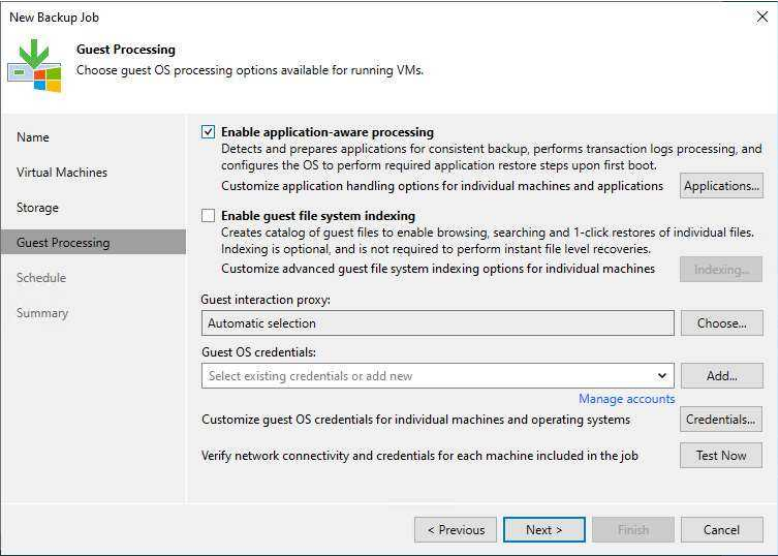


55. On the Storage page, click Next.

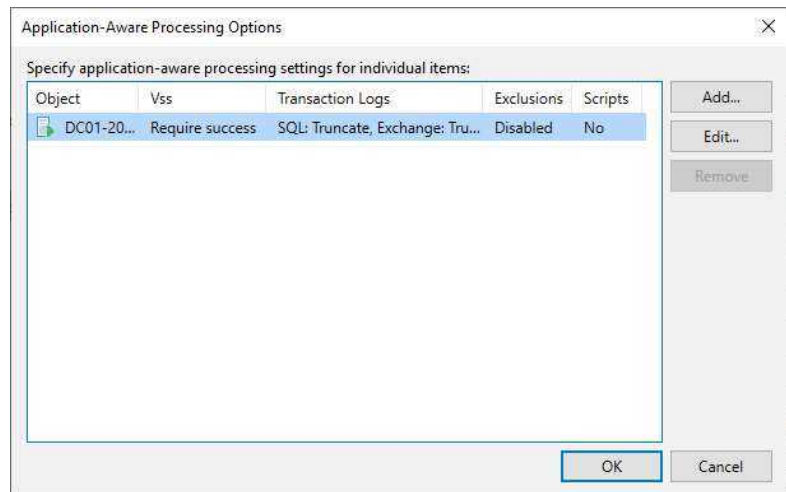


56. When you add VMs running VSS-aware applications to the backup job, you can enable application-aware processing to create a transactionally consistent backup. The transactionally consistent backup ensures that applications on VMs can be recovered without data loss.

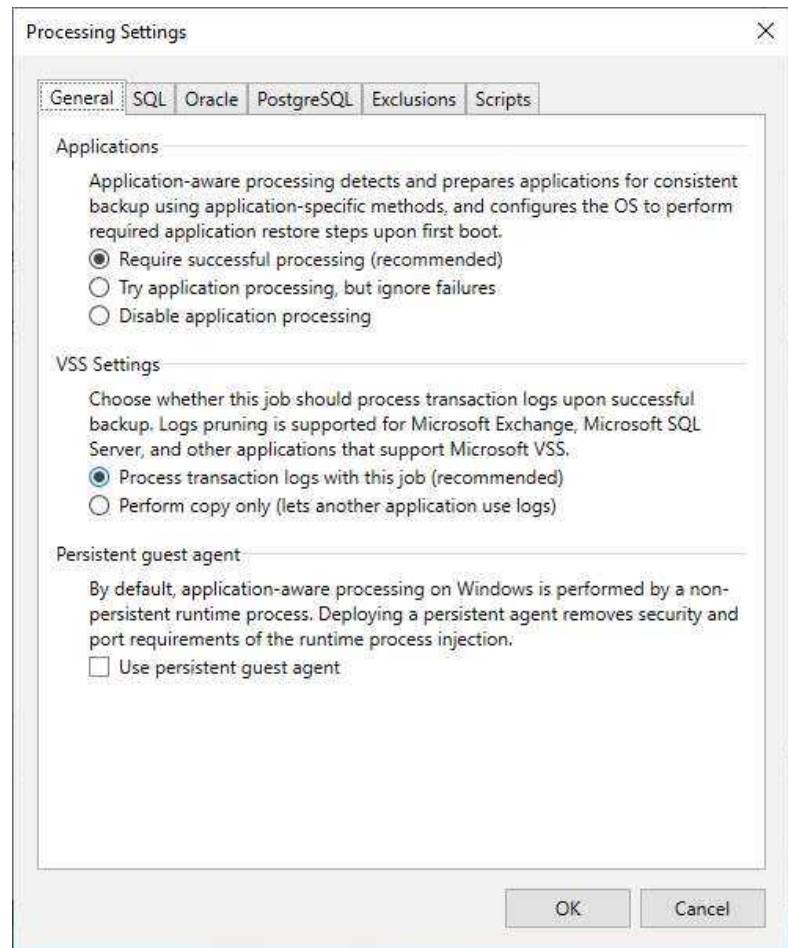
57. Select the Enable application-aware processing checkbox on the Guest Processing page and click Applications.



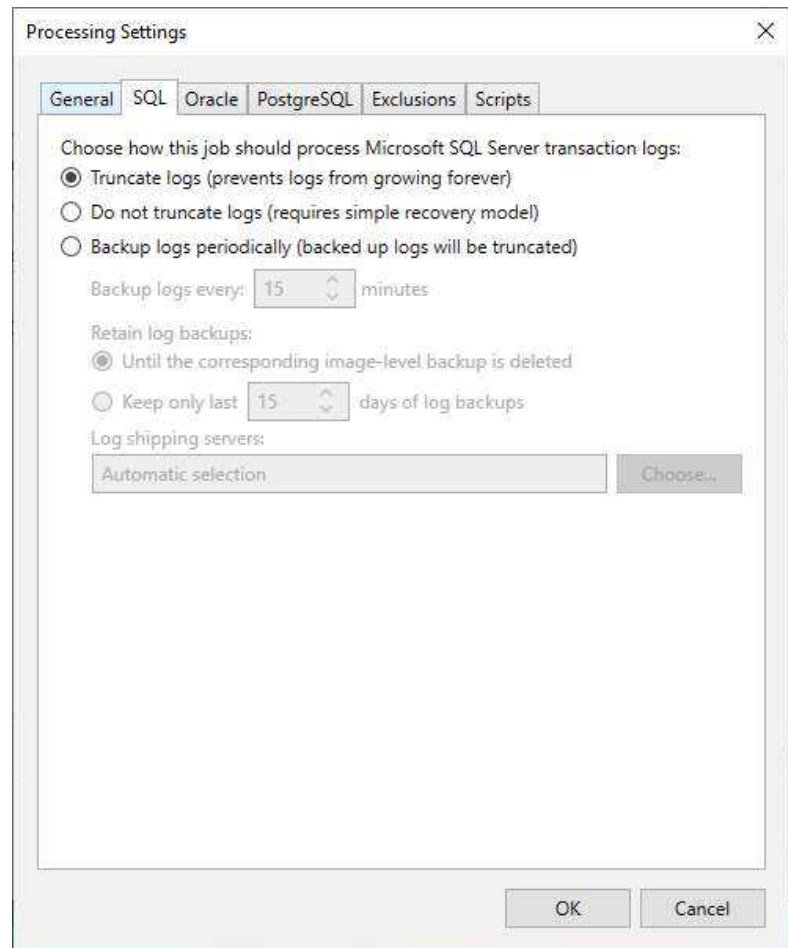
58. On the Application-Aware Processing Options page, select the VM and click Edit.



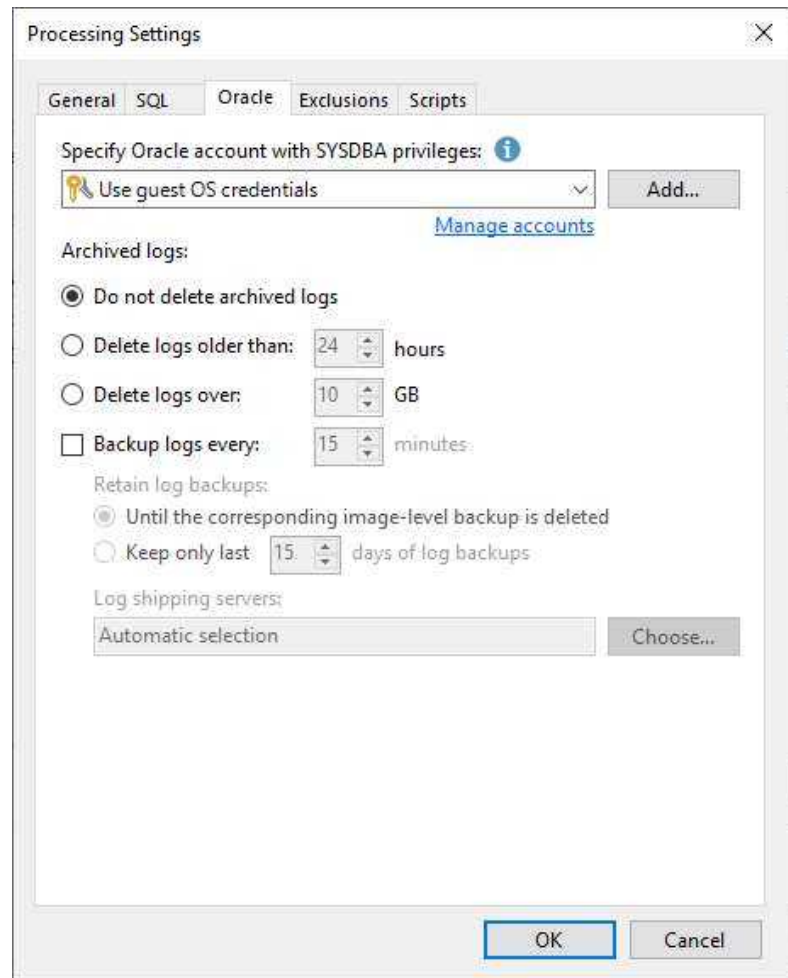
59. On the Processing Settings, click General.
60. Keep the default settings.



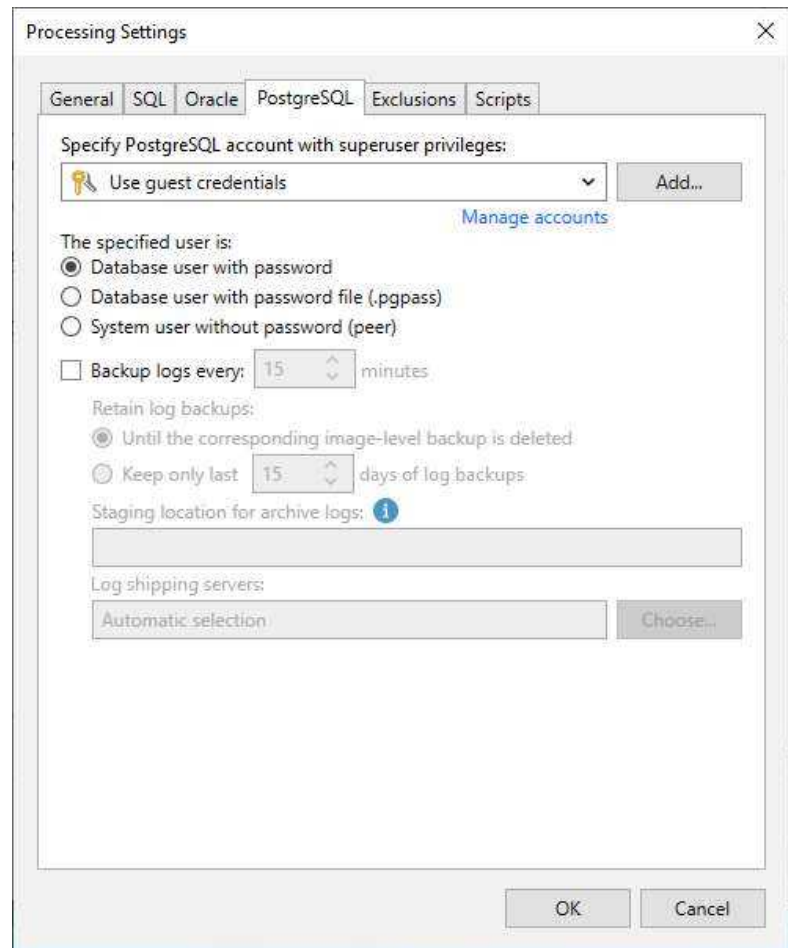
61. On the Processing Settings page, click SQL if the VM is a Microsoft SQL Server VM.
62. Select Truncate logs (Prevents logs from growing forever) to truncate transaction logs after a successful backup.



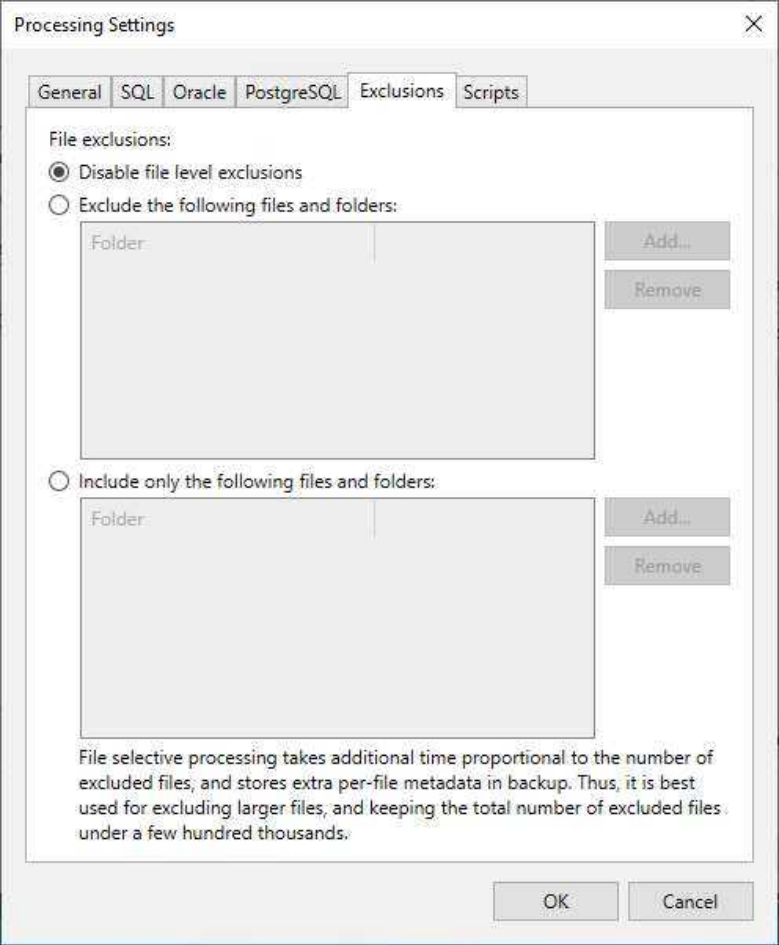
63. On the Processing Settings page, click Oracle if the VM is an Oracle Server.
64. Select a user account from the drop-down list.
65. Select Do not delete archived logs checkbox.



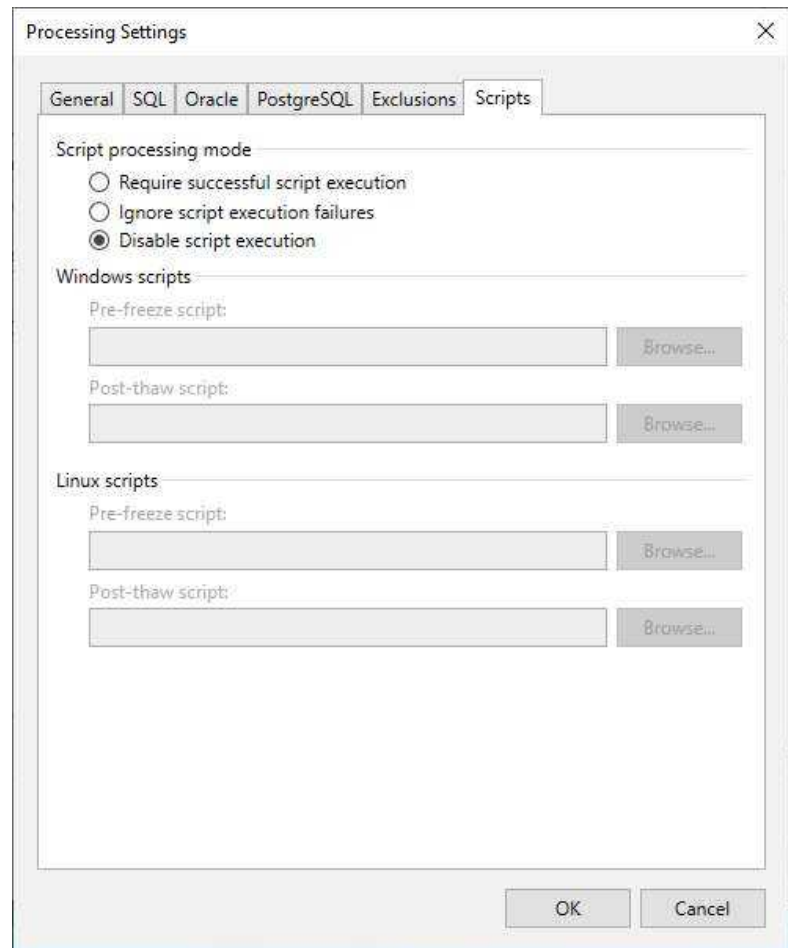
66. On the Processing Settings page, click PostgreSQL if the VM is a PostgreSQL Server VM.
67. Select a user account from the drop-down list.
68. Select Database user with password checkbox.



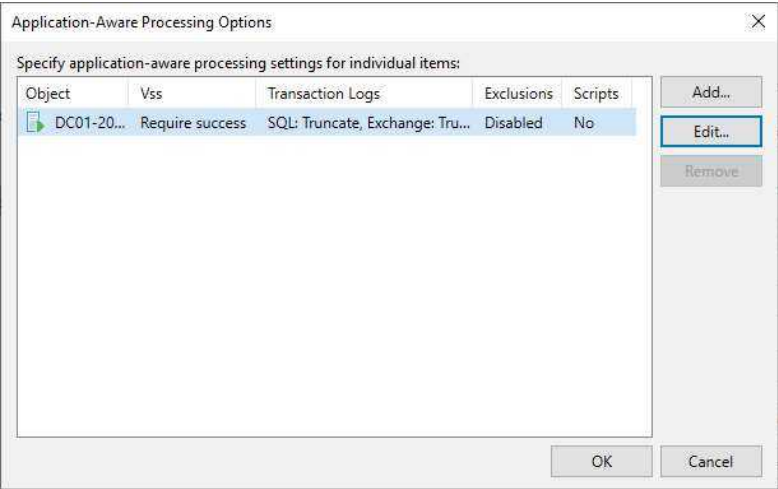
69. On the Processing Settings page, click Exclusions and keep the default settings.



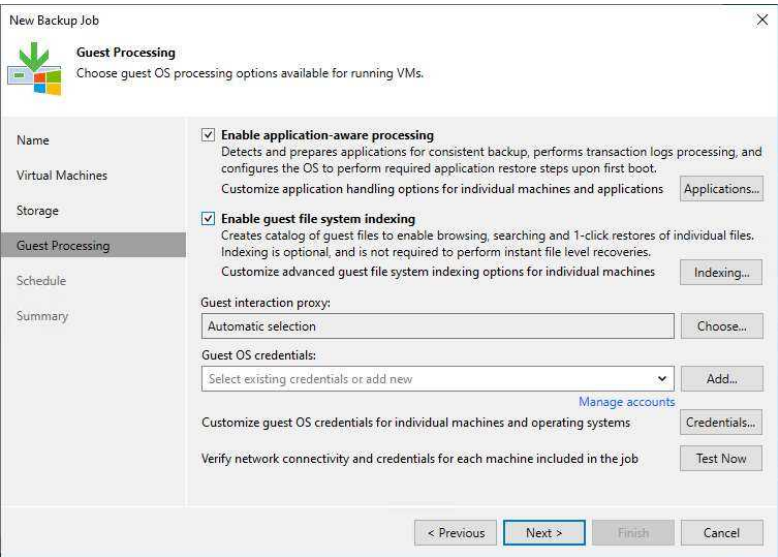
70. On the Processing Settings page, click Scripts and keep the default settings.
71. Click OK.



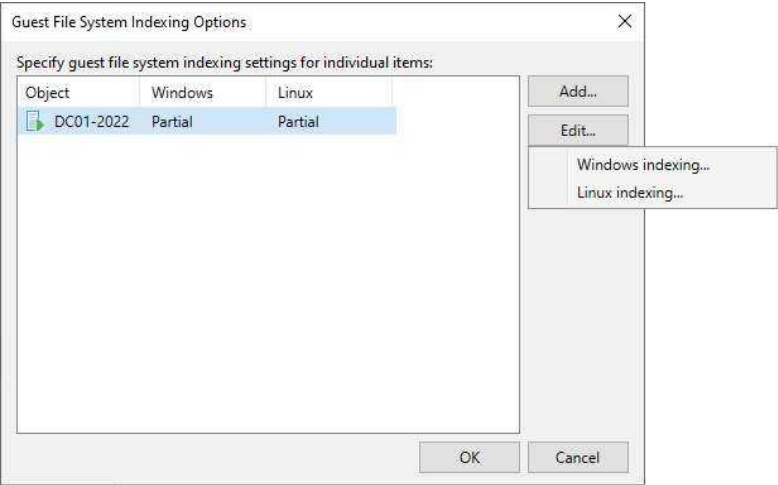
72. On the Application-Aware Processing Options page, click OK.



73. Select the Enable guest file system indexing checkbox and click Indexing.

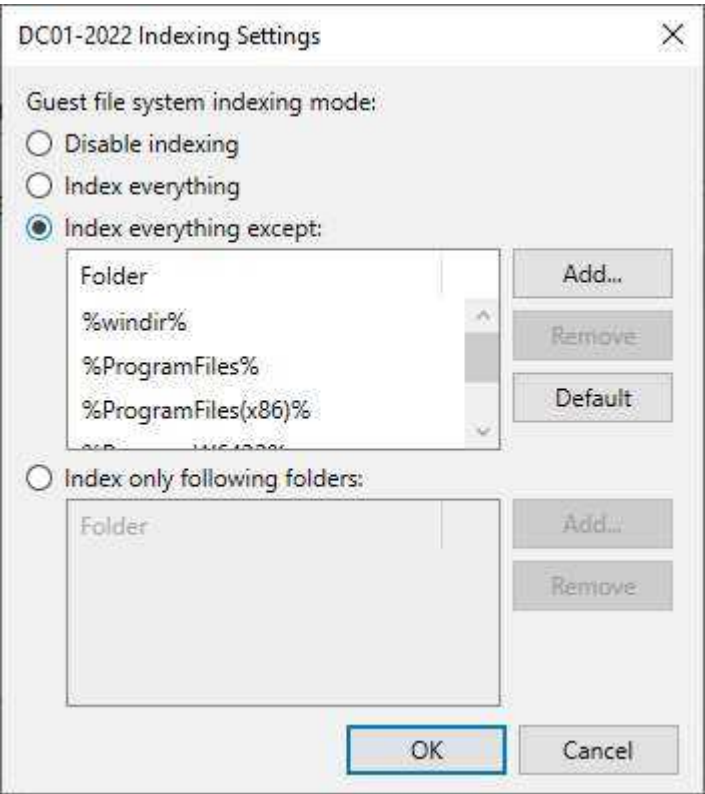


74. On the Guest File System Indexing Options page, select the VM, click Edit and select Windows indexing.

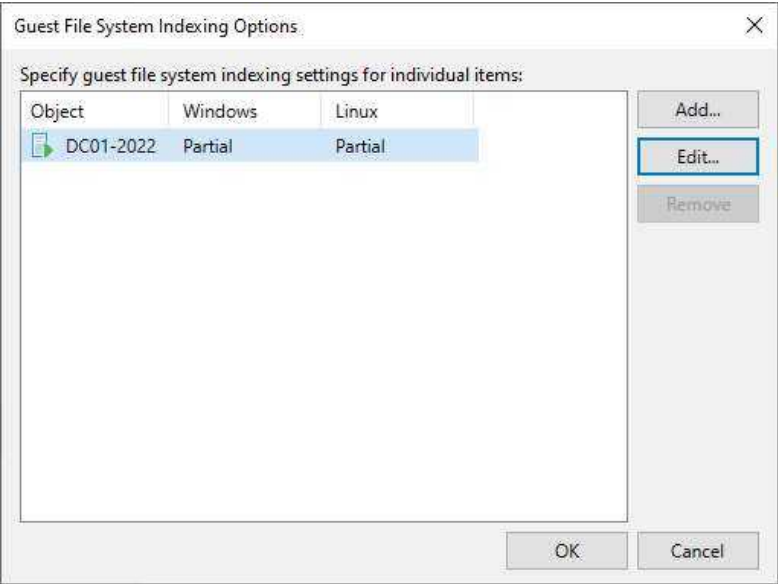


75. On the Guest file system indexing mode page, keep the default settings.

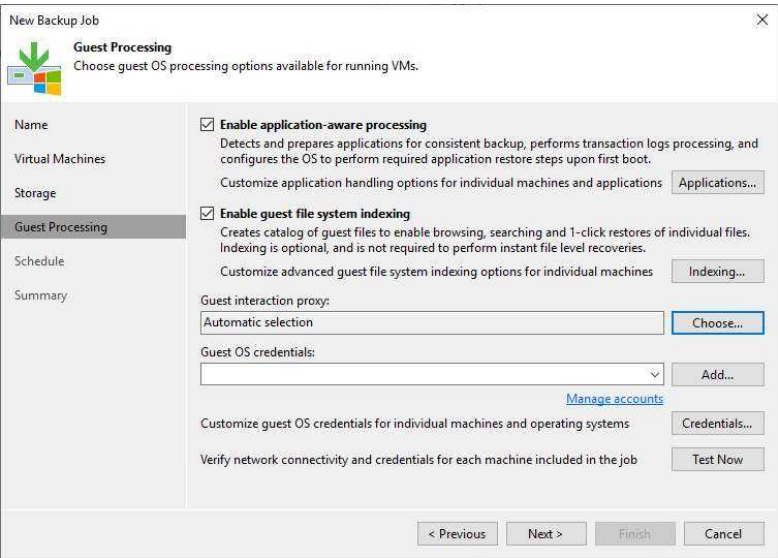
76. Click OK.



77. Click OK on the Guest file system indexing mode page.

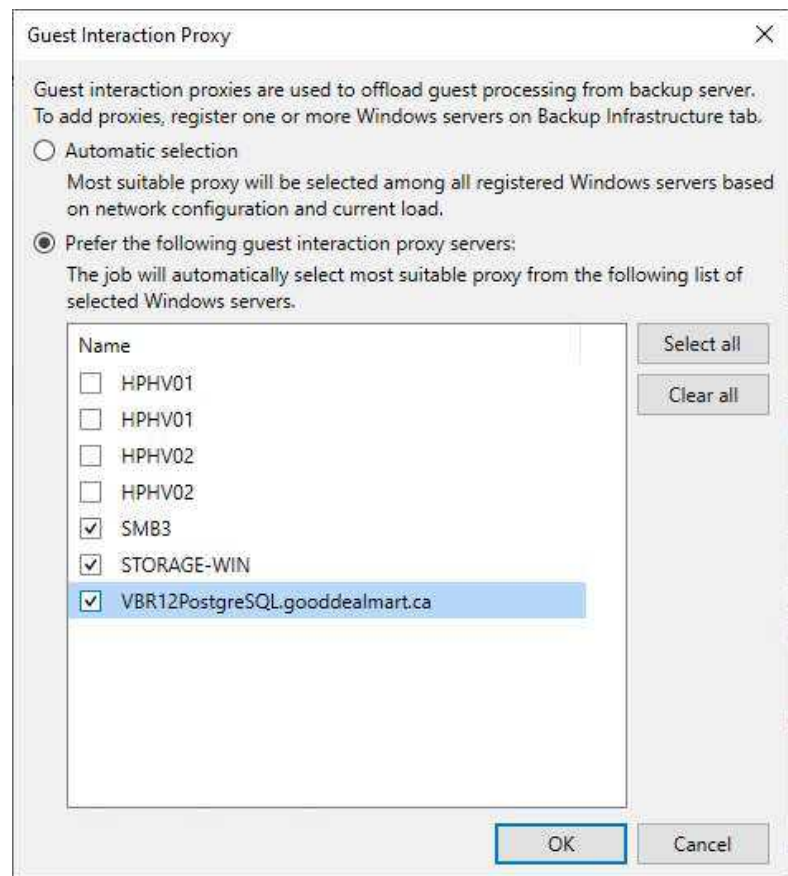


78. Click Choose on the Guest interaction proxy field on the Guest Processing page.

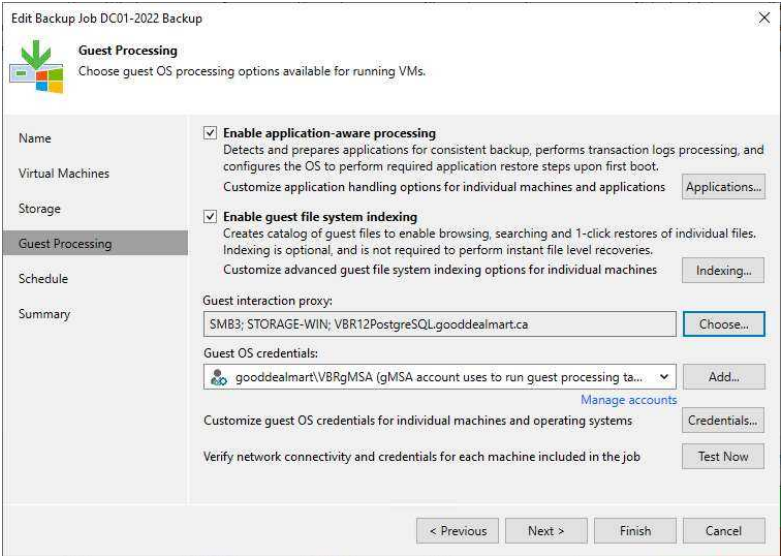


79. On the Guest Interaction Proxy page, select the domain member servers as the Guest Interaction proxy when you use gMSA as the guest OS credential.

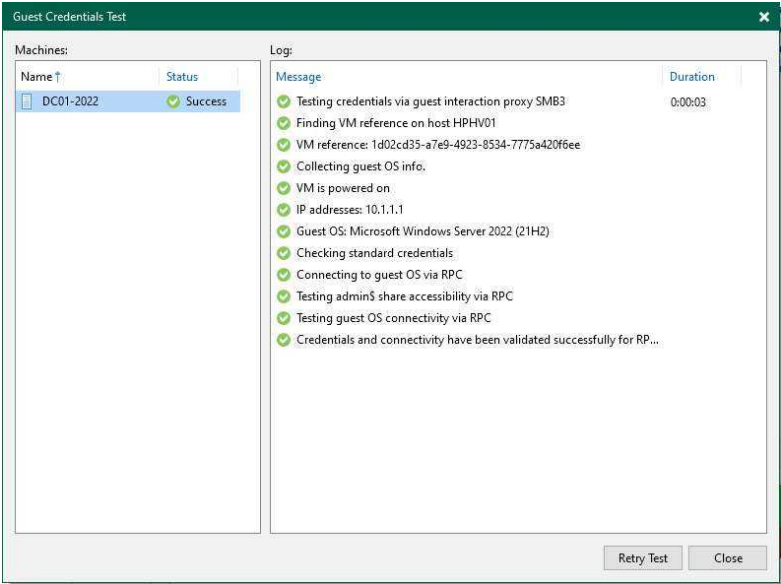
80. Click OK.



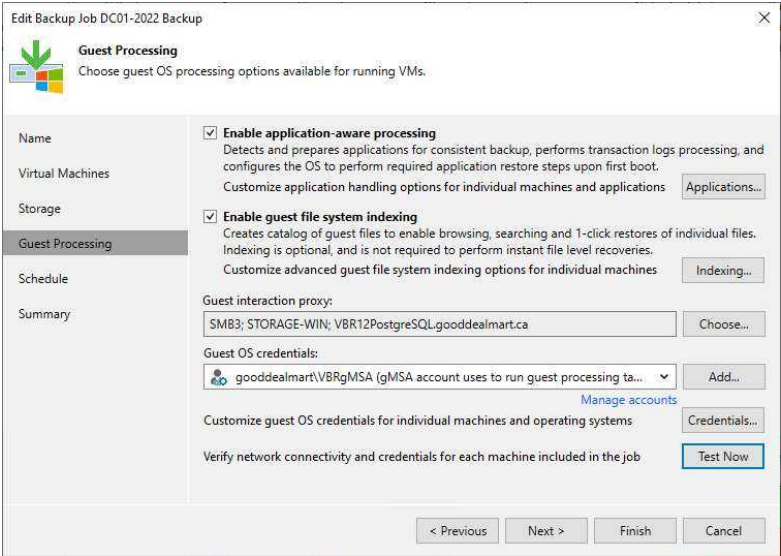
- 81. Choose a user account on the Guest Processing page with sufficient permissions from the Guest OS credentials drop-down list.
- 82. If you have multiple VMs at the same job, click Credentials to Customize guest OS credentials for individual machines and operating systems.
- 83. On the Guest Processing page, click Test Now to verify network connectivity and credentials for each machine included in the job.



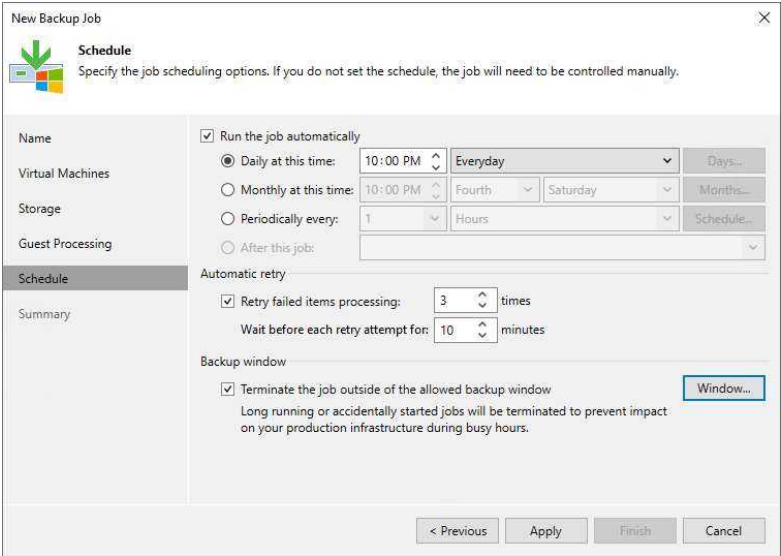
- 84. On the Guest Credentials Test page, ensure verification on success for each machine.
- 85. Click Close.



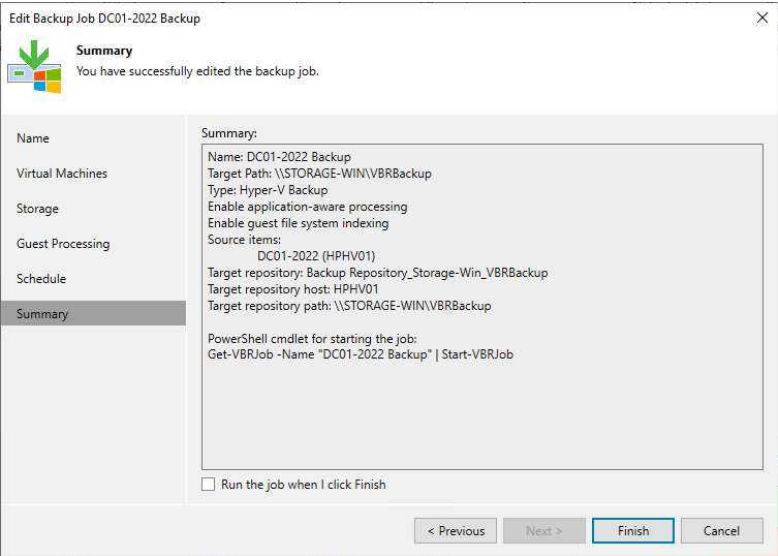
- 86. Click Next on the Guest Processing page.



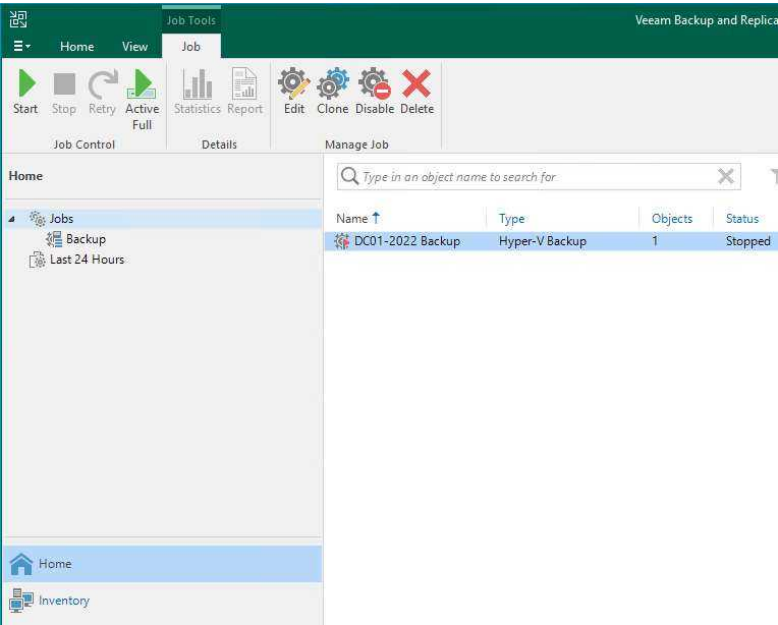
- 87. Select Run the job automatically checkbox on the Schedule page and select your specified schedule.
- 88. Define whether Veeam Backup & Replica should retry the backup job if it fails in the Automatic retry section.
- 89. Define the time interval the backup job must complete in the Backup window 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.



91. Click Finish on the Summary page.

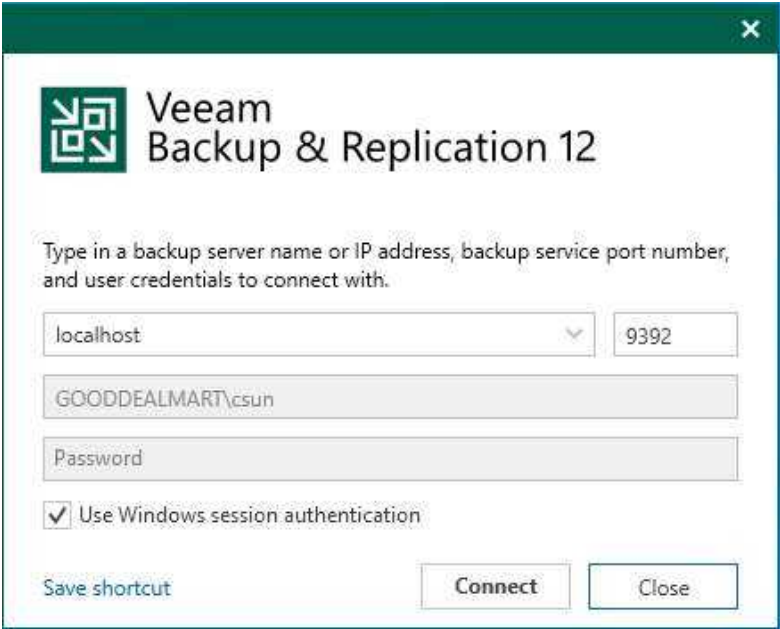


92. Verify that the backup job has been added.

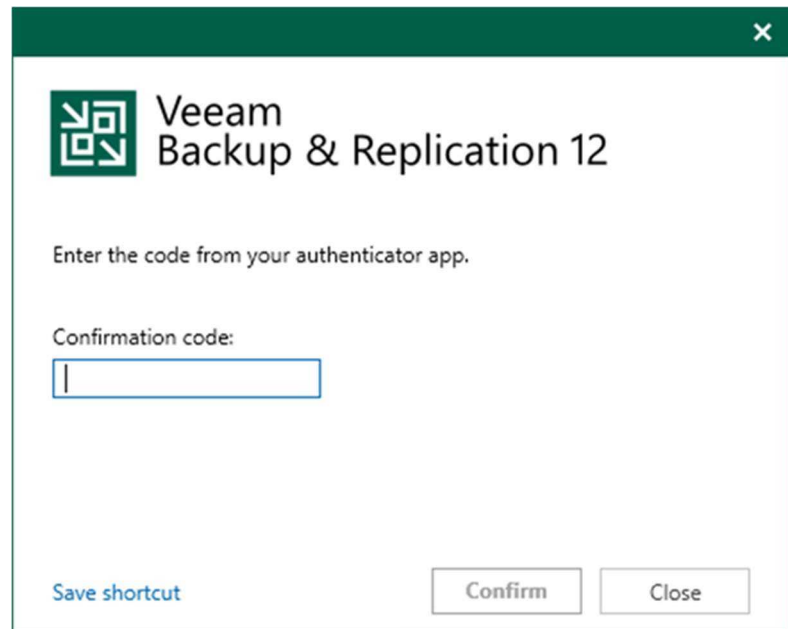


Create an Immutable Backup job to backup the specified VMs

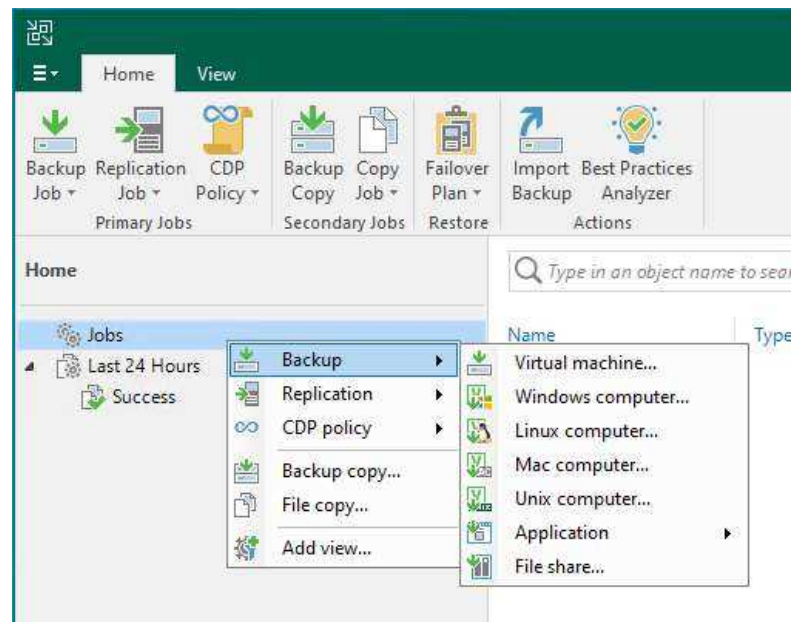
Immutable Backup is a Veeam Backup & Replication feature that protects against ransomware attacks by preventing malicious software from modifying or deleting backup data. Immutable backup means that once data is written to a backup repository, it cannot be modified, overwritten, or deleted until a specified 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.	 The screenshot shows the 'Veeam Backup & Replication 12' connection window. It has a green title bar with a close button. The window contains the Veeam logo and the title 'Veeam Backup & Replication 12'. Below this, it says 'Type in a backup server name or IP address, backup service port number, and user credentials to connect with.' There are three input fields: a dropdown menu showing 'localhost', a text box with '9392', and a text box with 'GOODDEALMART\csun'. Below these is a 'Password' field. A checkbox labeled 'Use Windows session authentication' is checked. At the bottom, there are three buttons: 'Save shortcut', 'Connect', and 'Close'.

3. Enter the MFA Confirmation code and click Confirm.



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.

New Backup Job



Name
Type in a name and description for this backup job.

Name

Virtual Machines

Storage

Guest Processing

Schedule

Summary

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.

< PREVIOUS

Next >

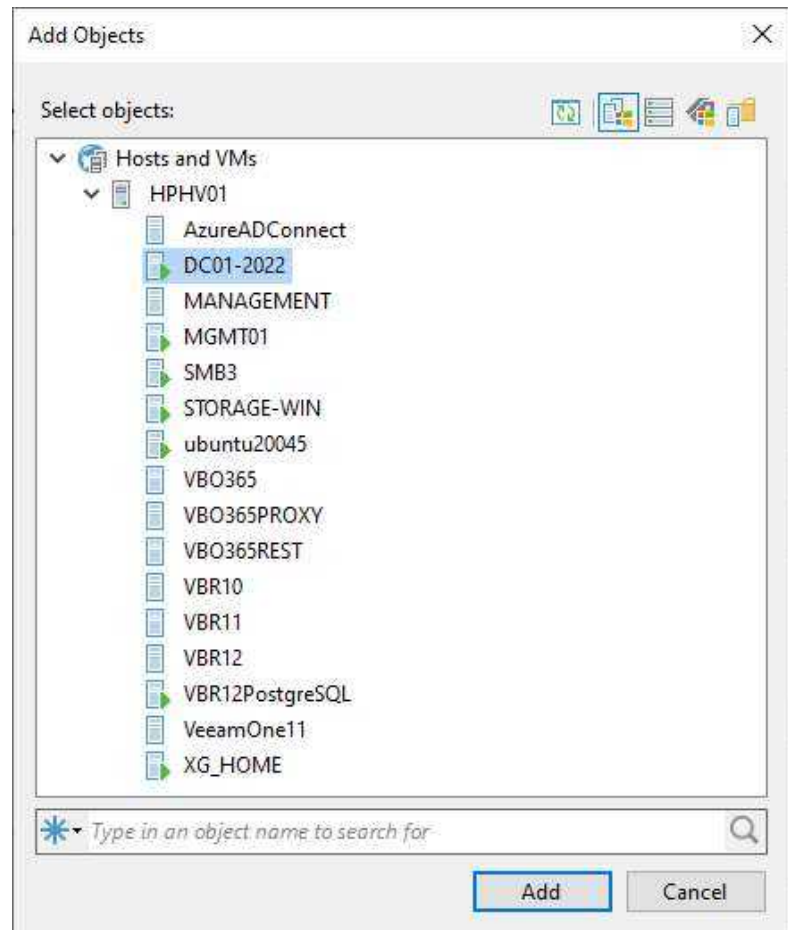
FINISH

CANCEL

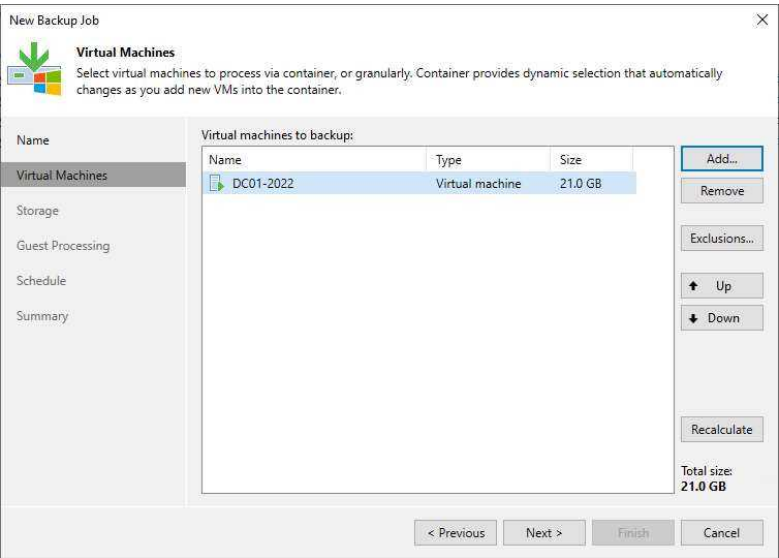
- Click Add on the Virtual Machines page.

[illegible]

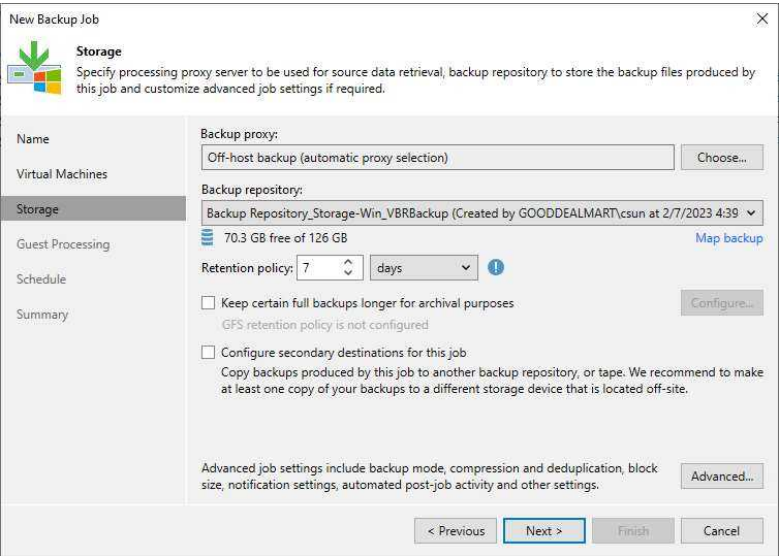
10. Select the VM from the Select objects list on the Add Objects page and click Add.
11. If you have multiple VMS that need to be backed up in the same backup job, you can repeat the step to add them.



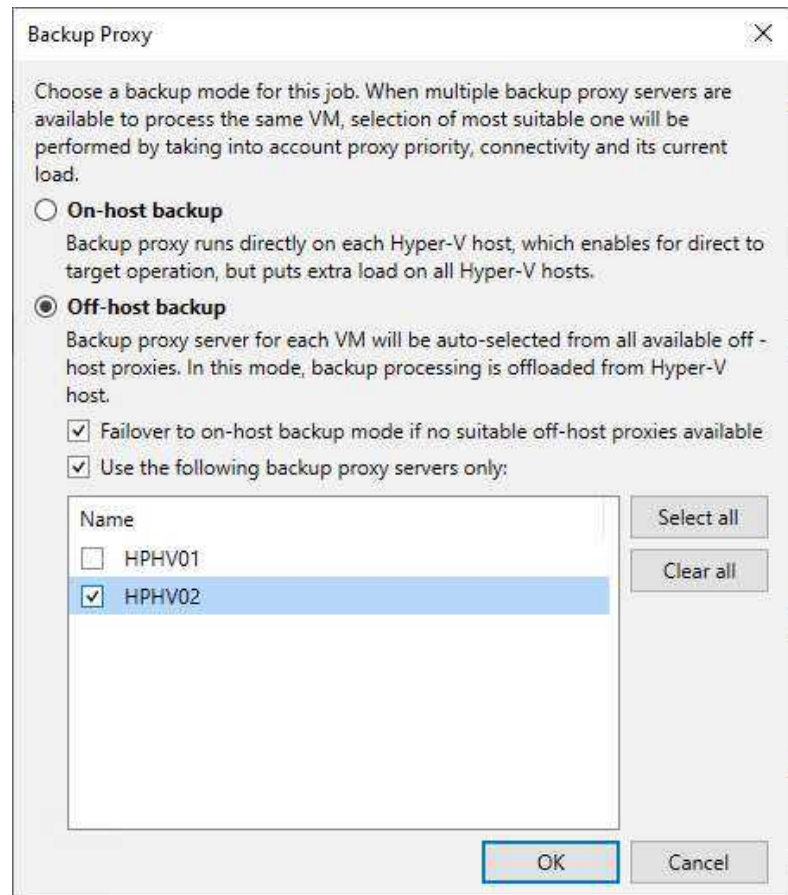
12. Click Next on the Virtual Machines page.



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) or use the default Off-host backup (automatic proxy selection) setting.



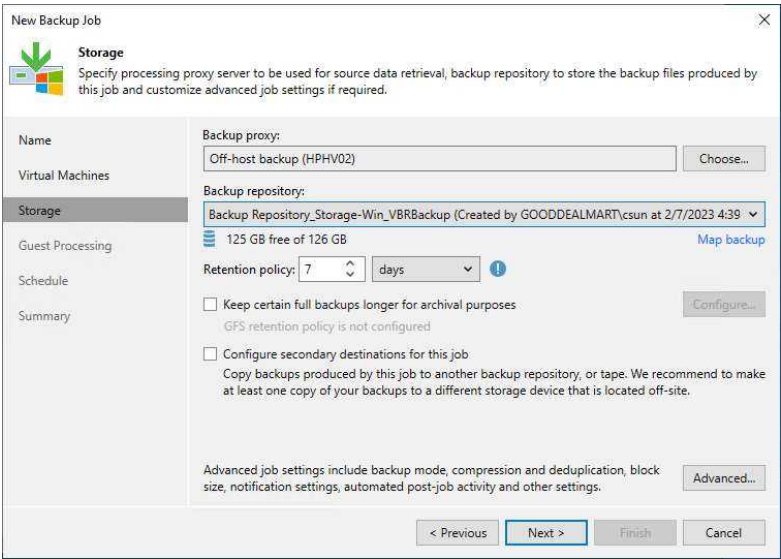
14. On the Backup Proxy page, if you select On-host backup mode, the source Microsoft HyperV host will serve as both the source host and the backup proxy. In this mode, Veeam Data Mover runs directly on the source host, which speeds up data retrieval but places additional strain on the host.
15. If you 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 & Replica 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.



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: [Field]
Virtual Machines: [Field]
Storage
Guest Processing: [Field]
Schedule: [Field]
Summary: [Field]

Backup proxy: [Off-host backup (HPHV02)] [Choose...]
Backup repository: [Backup Repository_ubuntu20045 (Created by GOODDEALMART\csun at 2/7/2023 3:47 PM.)] [Map backup]
126 GB free of 126 GB
Retention policy: 7 [days] [restore points] [days] [Configure...]
☐ 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. [Advanced...]
[< Previous] [Next >] [Finish] [Cancel]

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: [Field]
Virtual Machines: [Field]
Storage
Guest Processing: [Field]
Schedule: [Field]
Summary: [Field]

Backup proxy: [Off-host backup (HPHV02)] [Choose...]
Backup repository: [Backup Repository_ubuntu20045 (Created by GOODDEALMART\csun at 2/7/2023 3:47 PM.)] [Map backup]
126 GB free of 126 GB
Retention policy: 7 [days] [Configure...]
☒ 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. [Advanced...]
[< Previous] [Next >] [Finish] [Cancel]

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.



28. On the Storage page, click Advanced.

New Backup Job

Storage

Virtual Machines

Guest Processing

Schedule

Summary

Storage

Guest Processing

Schedule

Summary

Backup proxy:
Off-host backup (HPHV02)
Choose...

Backup repository:
Backup Repository_ubuntu20045 (Created by GOODDEALMART\csun at 2/7/2023 3:47 PM.)
126 GB free of 126 GB
Map backup

Retention policy: 7 days
Keep certain full backups longer for archival purposes
GFS retention policy is not configured
Configure...

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.
Advanced...

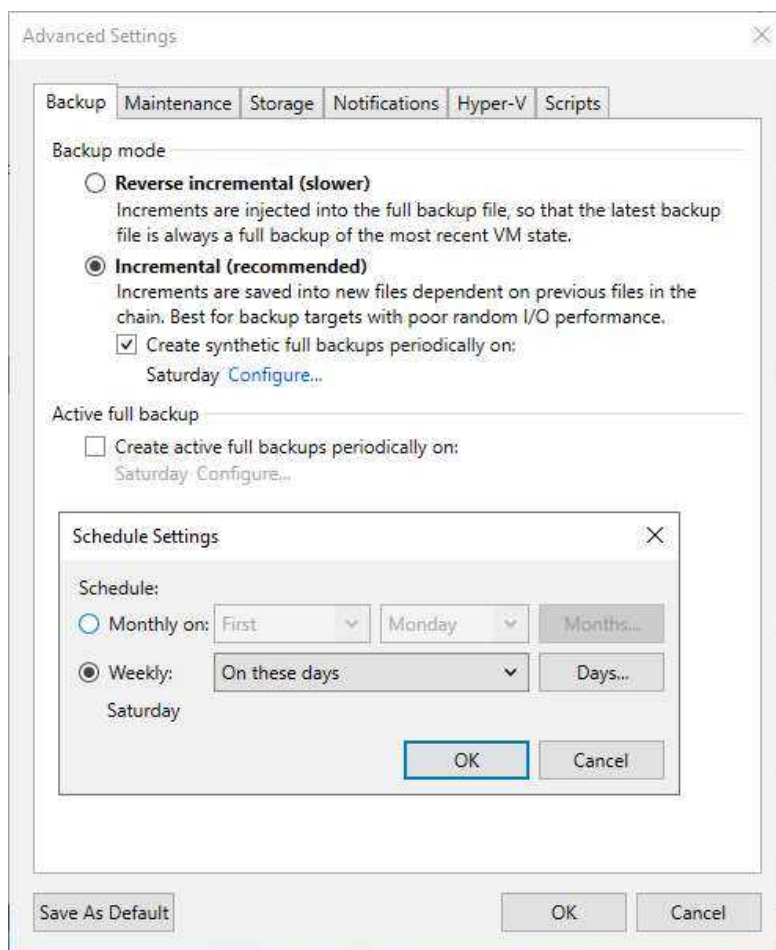
< Previous

Next >

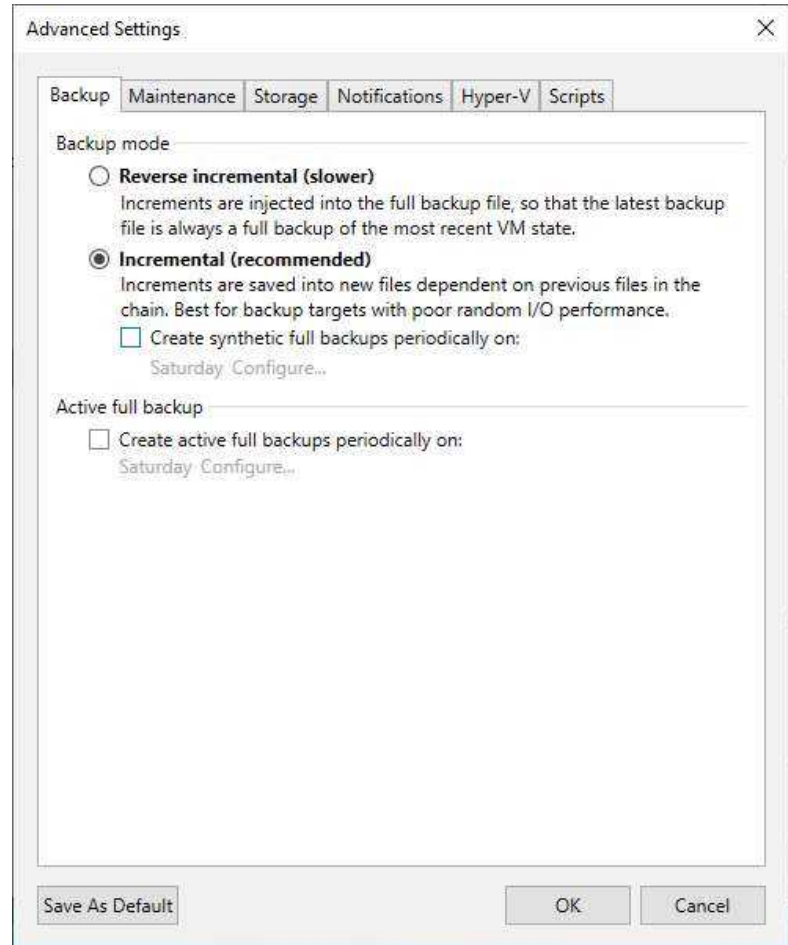
Finish

Cancel

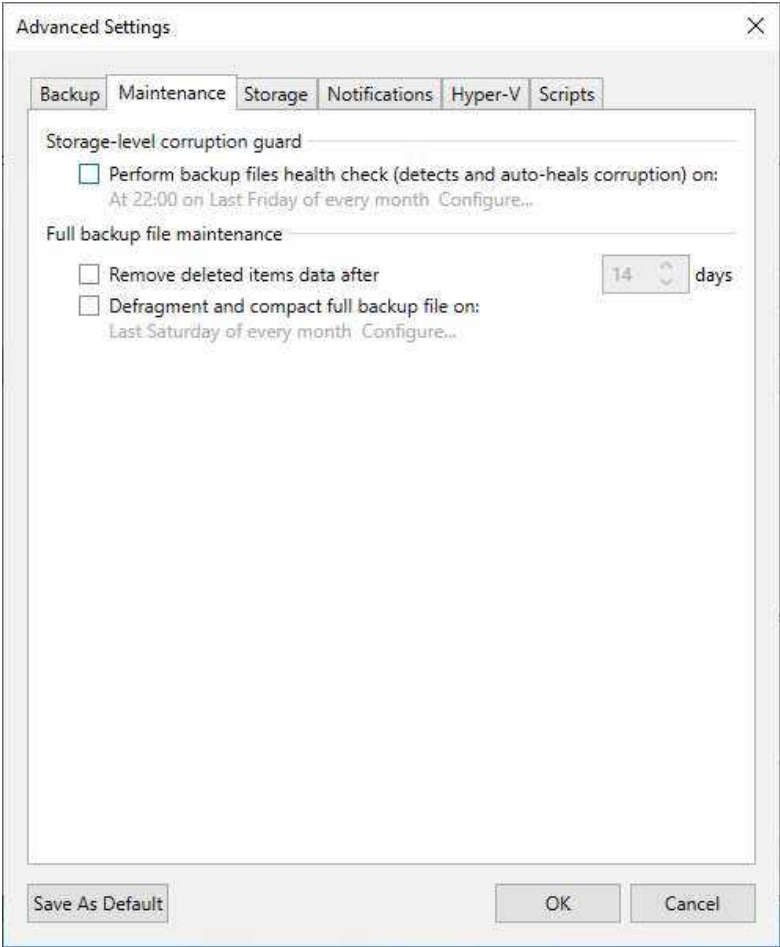
29. On the Backup page, select Incremental (recommended).
30. Select create synthetic full backups periodically or active full backups periodically checkbox.
31. Click Configure to schedule full backups periodically and click OK.



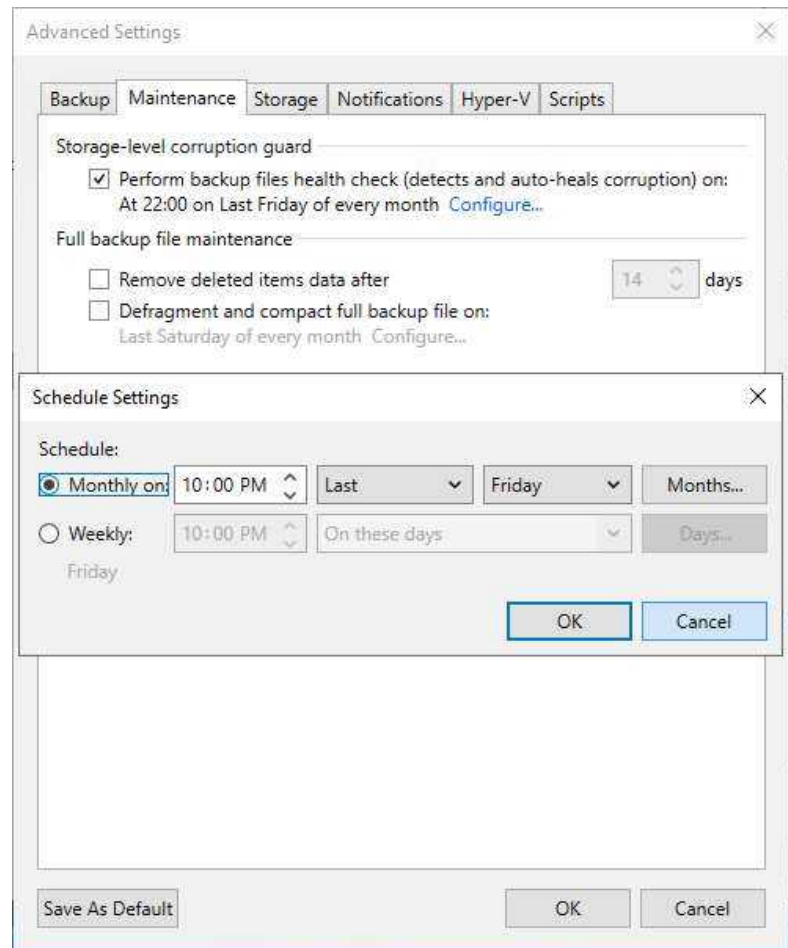
32. Select Incremental and disable synthetic full or active full backups to create a forever forward incremental backup chain if needed.



33. On the Advanced Settings, select Maintenance.



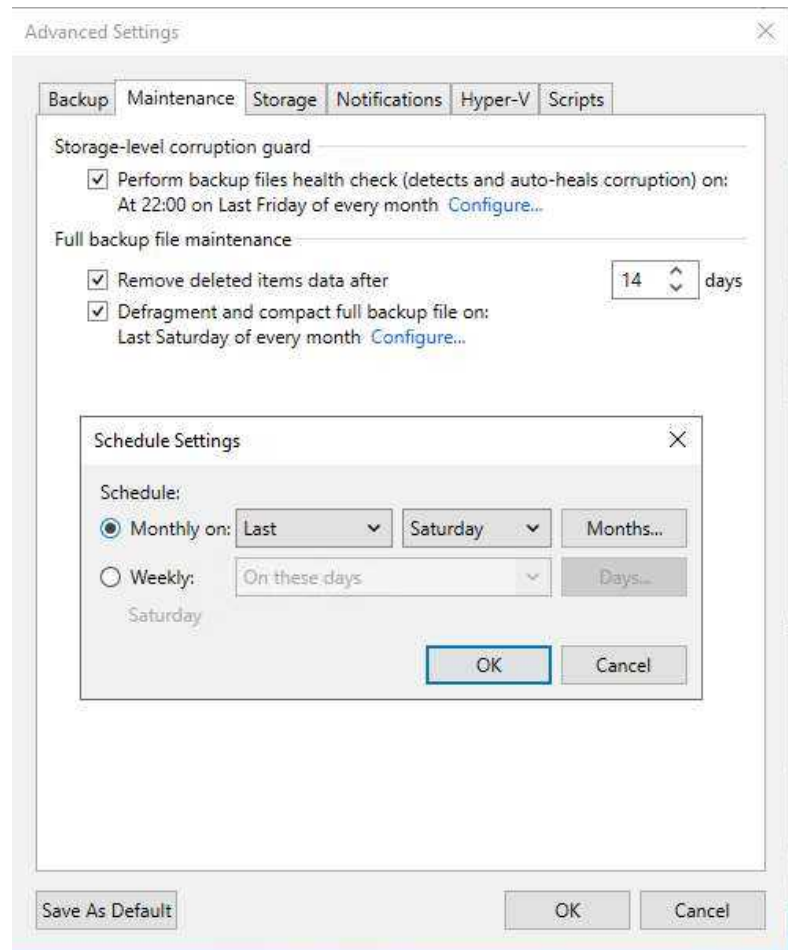
34. To regularly perform a health check on the backup chain's most recent restore point, select the Perform backup files health check (detects and auto-heals corrupt on) checkbox in the Storage-level corruption guard section.
35. Click Configure to set a timetable for the health check.



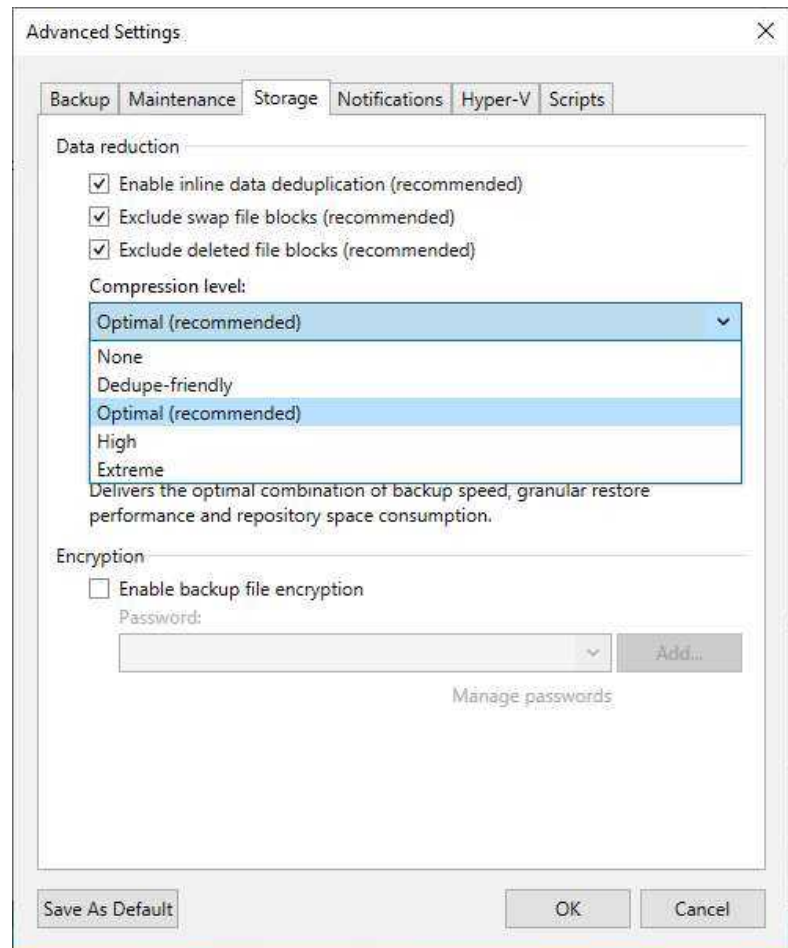
36. Select the Remove deleted items data after the checkbox and enter the few days you want backup data for deleted VMs to be kept.
37. Select the Defragment and compact full backup file checkbox and click Configure.
38. Set the schedule for the compact operation to compact a full backup periodically.

Note:

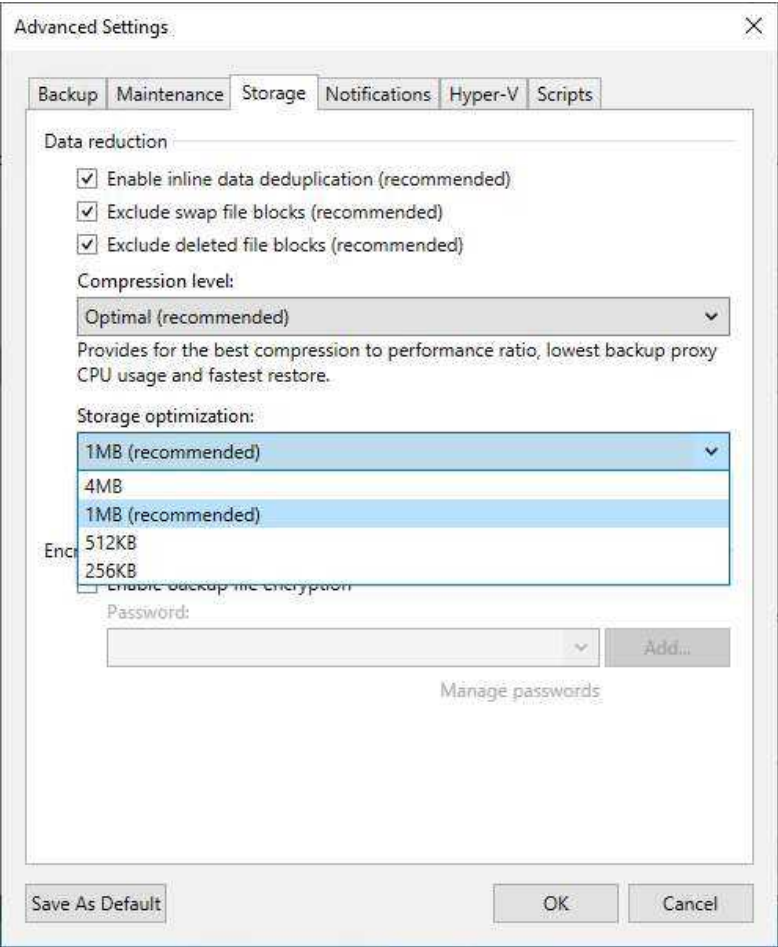
GFS retention is not compatible with defragment and compact functionality.



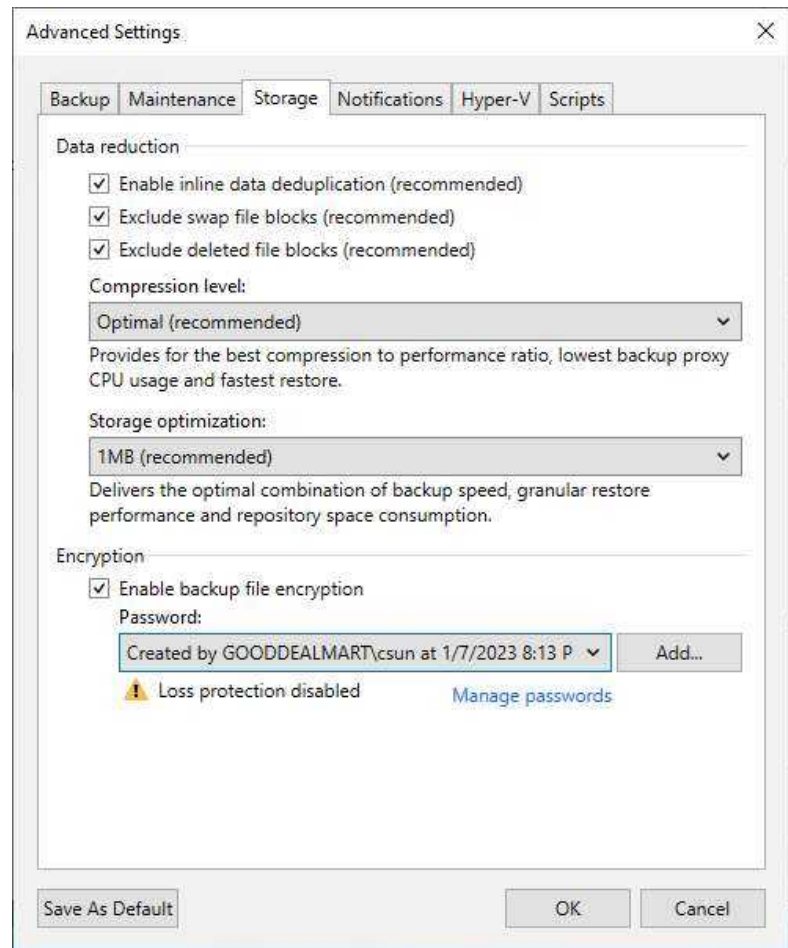
39. On Advanced Settings, select Storage.
40. Select the Enable inline data deduplication (recommended) checkbox.
41. Select the Exclude swap file blocks (recommended) checkbox.
42. Select the Exclude deleted file blocks (recommended) checkbox.
43. Select the compression level for the backup from the drop-down list.



44. Select the Storage optimization for the backup from the drop-down list.

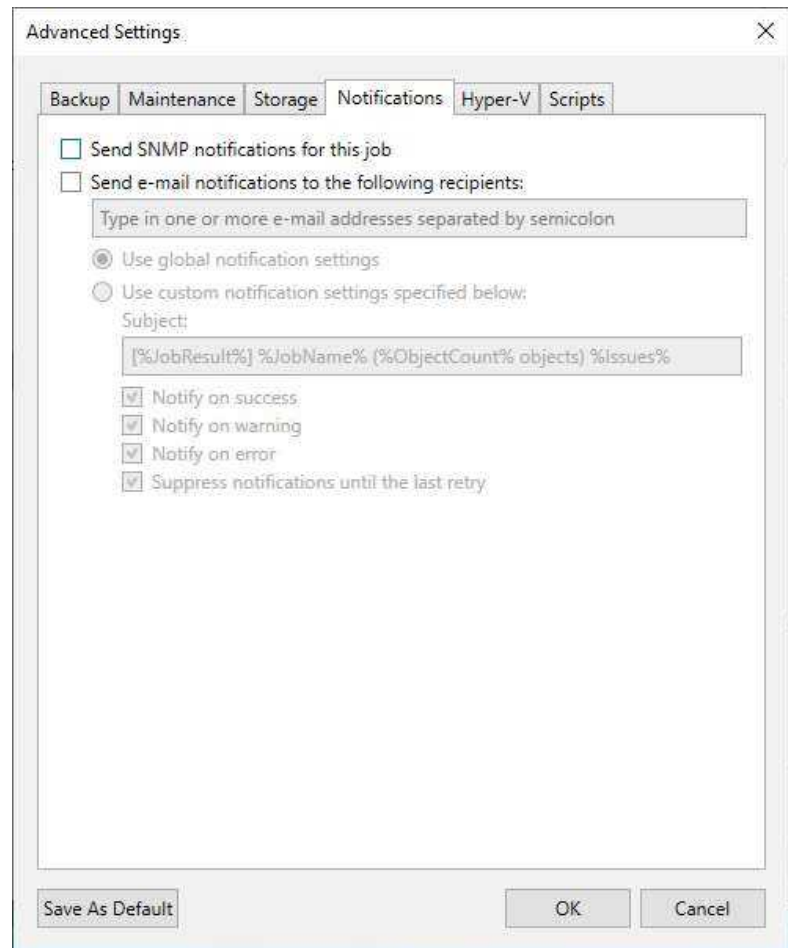


45. Select the Enable backup file encryption checkbox to encrypt the content of backup files.
46. Select a password from the drop-down list. Then, if you still need to do, click Add or use the Manage passwords link to create a new password.

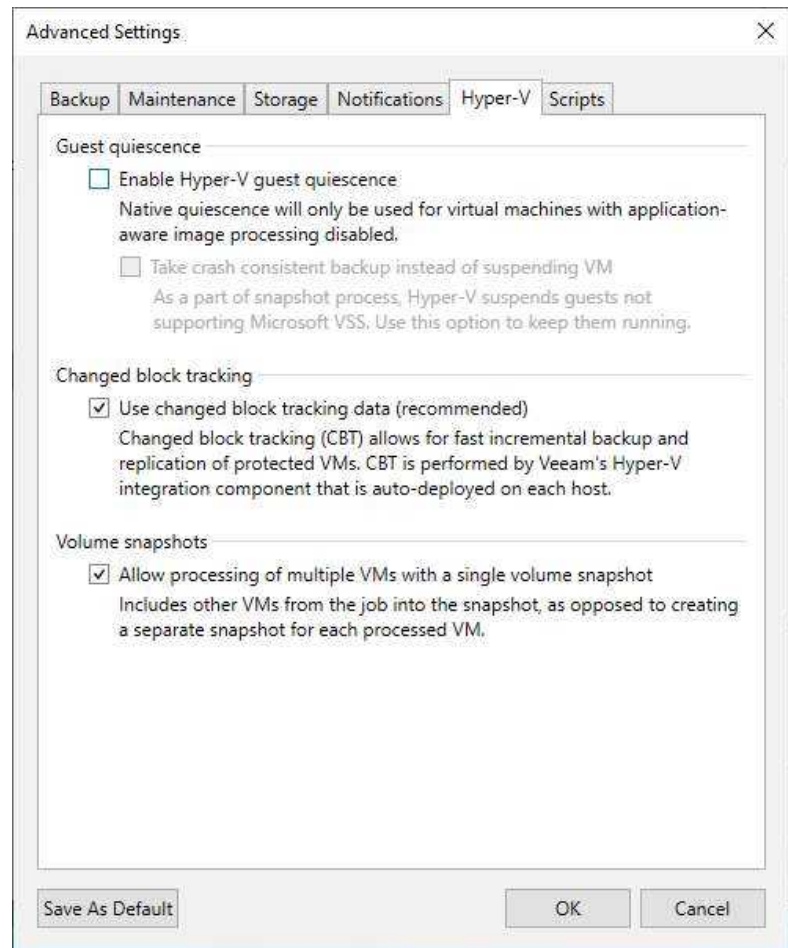


47. Select Noifica ons on the Advanced Se ings.

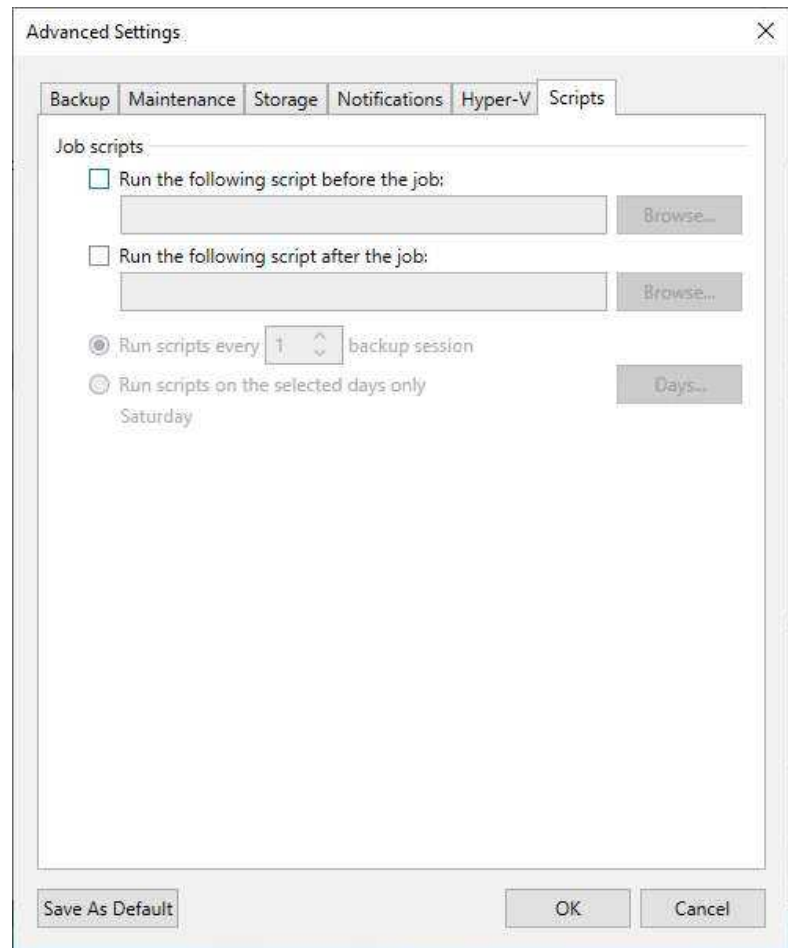
48. Keep the default se ings.



49. Select Hyper-V on the Advanced Settings.
50. Keep the default settings.



51. On the Advanced Settings page, select Scripts and keep the default settings.
52. Click OK.



53. Click Next on the Storage page.

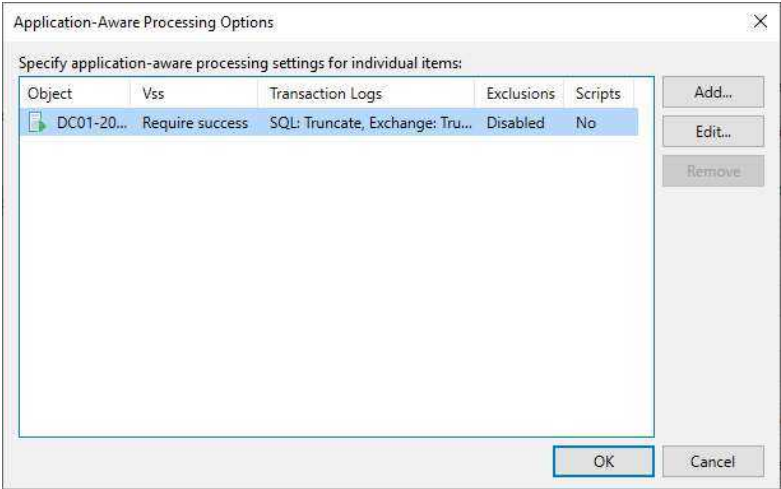
The screenshot shows the 'New Backup Job' dialog box with the 'Storage' tab selected. The left sidebar contains links for Name, Virtual Machines, Storage, Guest Processing, Schedule, and Summary. The main area is titled 'Storage' and includes instructions: 'Specify processing proxy server to be used for source data retrieval, backup repository to store the backup files produced by this job and customize advanced job settings if required.' The 'Backup proxy' is set to 'Off-host backup (HPHV02)'. The 'Backup repository' is 'Backup Repository_ubuntu20045 (Created by GOODDEALMART\csun at 2/7/2023 3:47 PM.)'. The 'Retention policy' is set to '7 days'. There are checkboxes for 'Keep certain full backups longer for archival purposes' and 'Configure secondary destinations for this job'. An 'Advanced...' button is at the bottom right. Navigation buttons at the bottom are '< Previous', 'Next >', 'Finish', and 'Cancel'.

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.

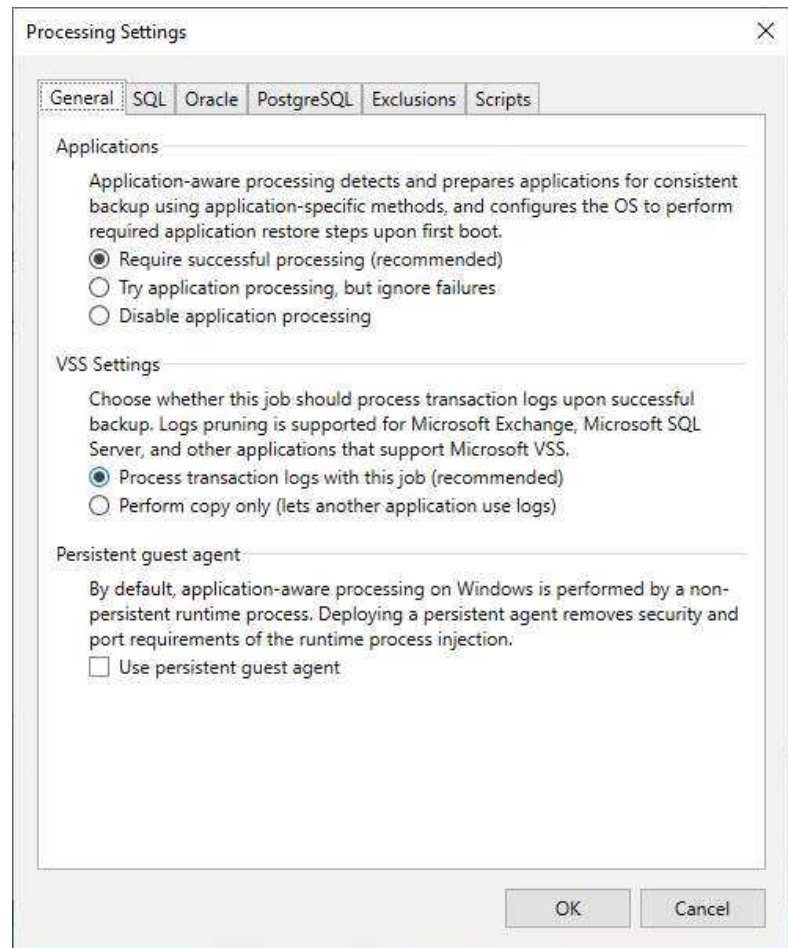
55. Select the Enable application-aware processing checkbox on the Guest Processing page and click Applications.

The screenshot shows the 'New Backup Job' dialog box with the 'Guest Processing' tab selected. The left sidebar is the same as in the previous screenshot. The main area is titled 'Guest Processing' and includes instructions: 'Choose guest OS processing options available for running VMs.' The 'Enable application-aware processing' checkbox is checked. Below it, there is a description and an 'Applications...' button. The 'Enable guest file system indexing' checkbox is unchecked. Below it, there is a description and an 'Indexing...' button. The 'Guest interaction proxy' is set to 'Automatic selection'. The 'Guest OS credentials' are set to 'Select existing credentials or add new'. There are buttons for 'Add...', 'Manage accounts', 'Credentials...', and 'Test Now'. Navigation buttons at the bottom are '< Previous', 'Next >', 'Finish', and 'Cancel'.

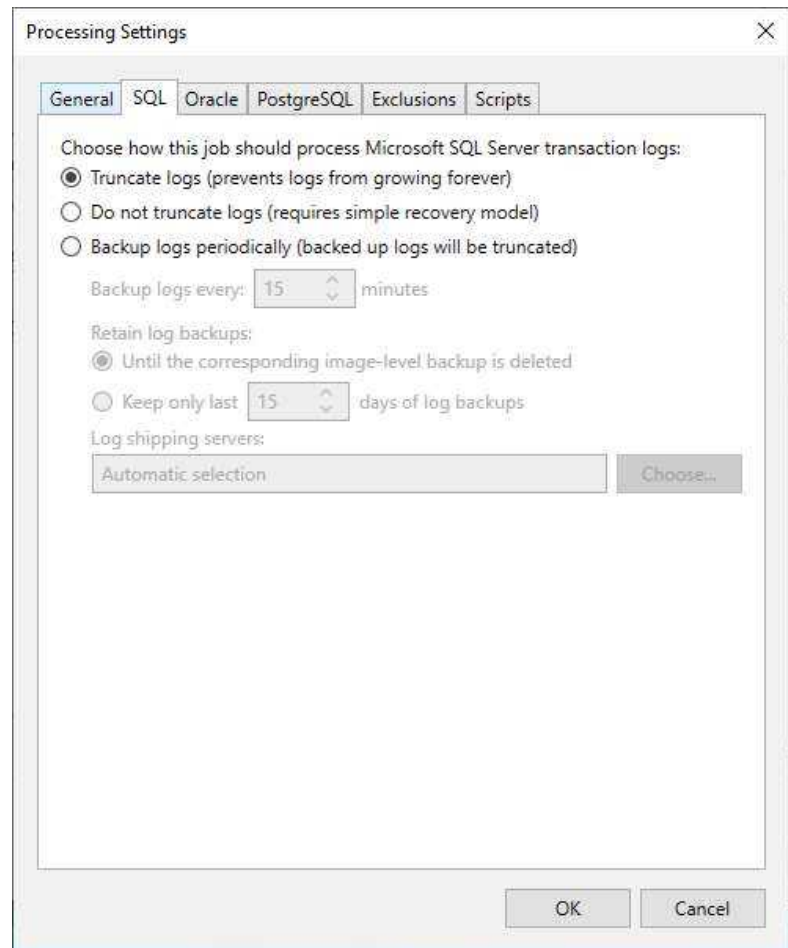
56. On the Application-Aware Processing Options page, select the VM and click Edit.



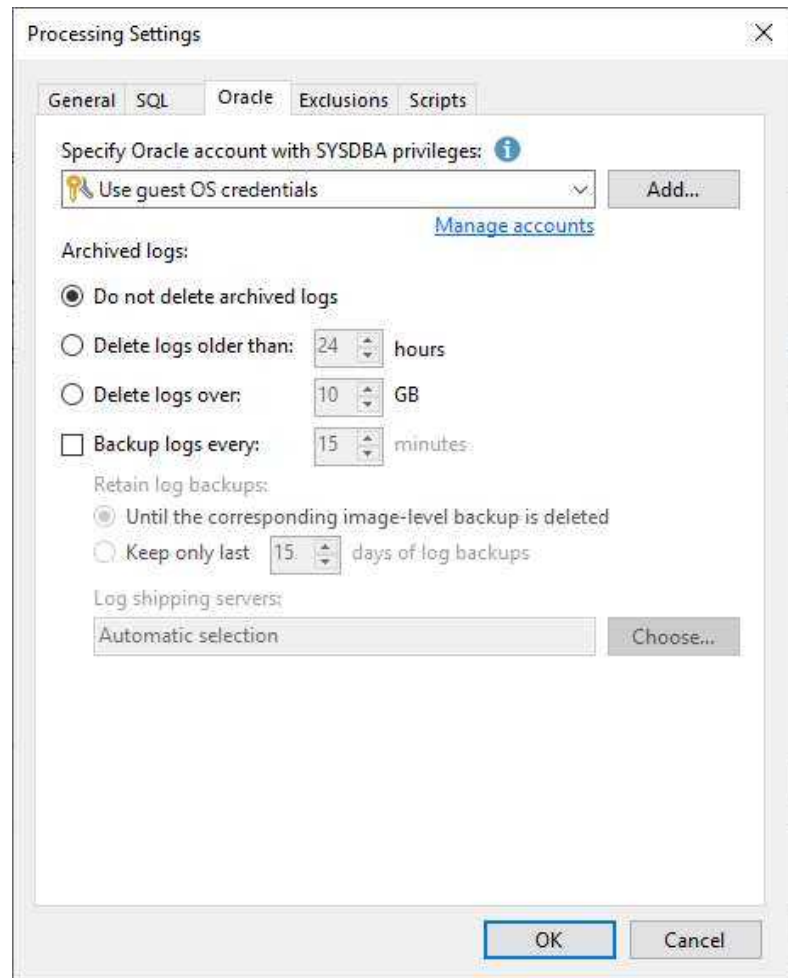
57. On the Processing Settings, click General.
58. Keep the default settings.



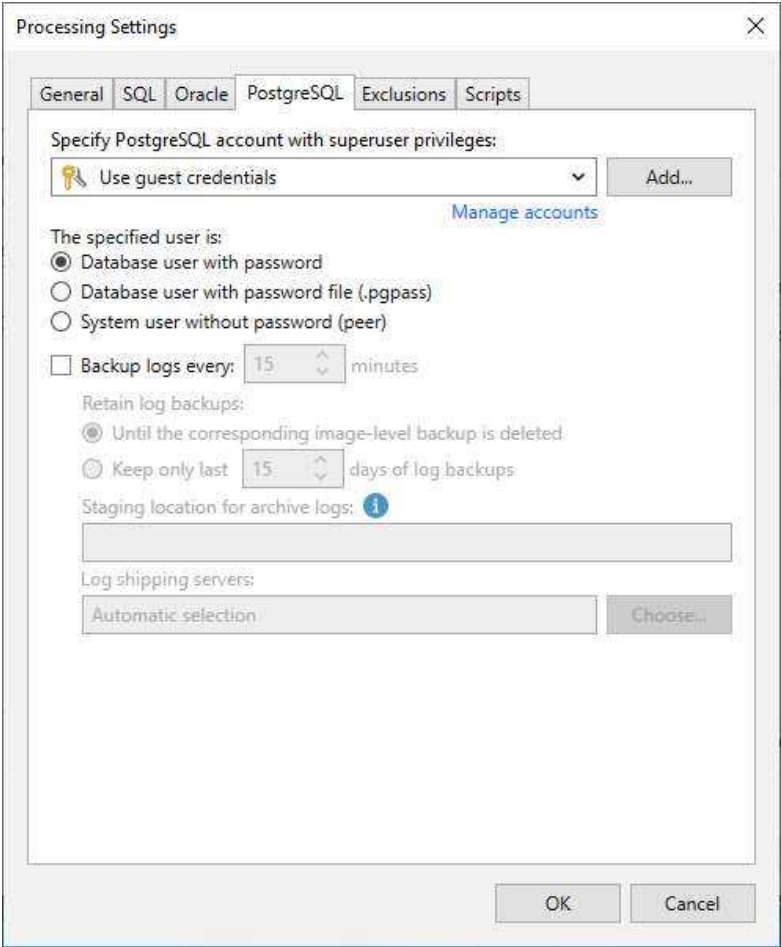
59. On the Processing Settings page, click SQL if the VM is a Microsoft SQL Server VM.
60. Select Truncate logs (Prevents logs from growing forever) to truncate transaction logs after a successful backup.



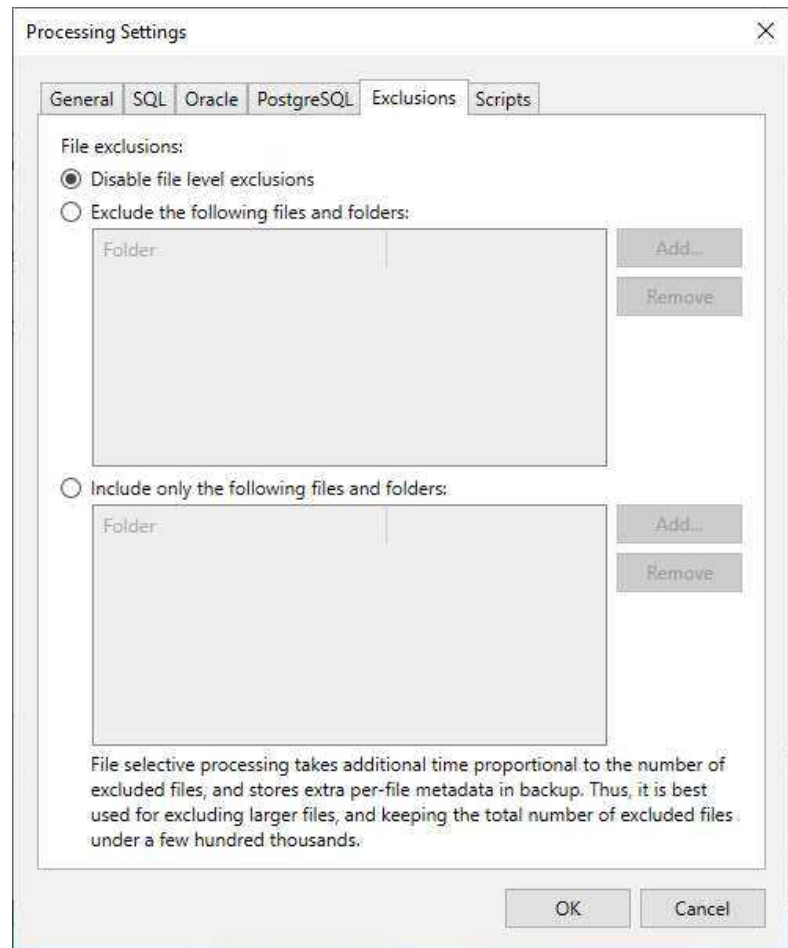
61. On the Processing Settings page, click Oracle if the VM is an Oracle Server.
62. Select a user account from the drop-down list.
63. Select Do not delete archived logs checkbox.



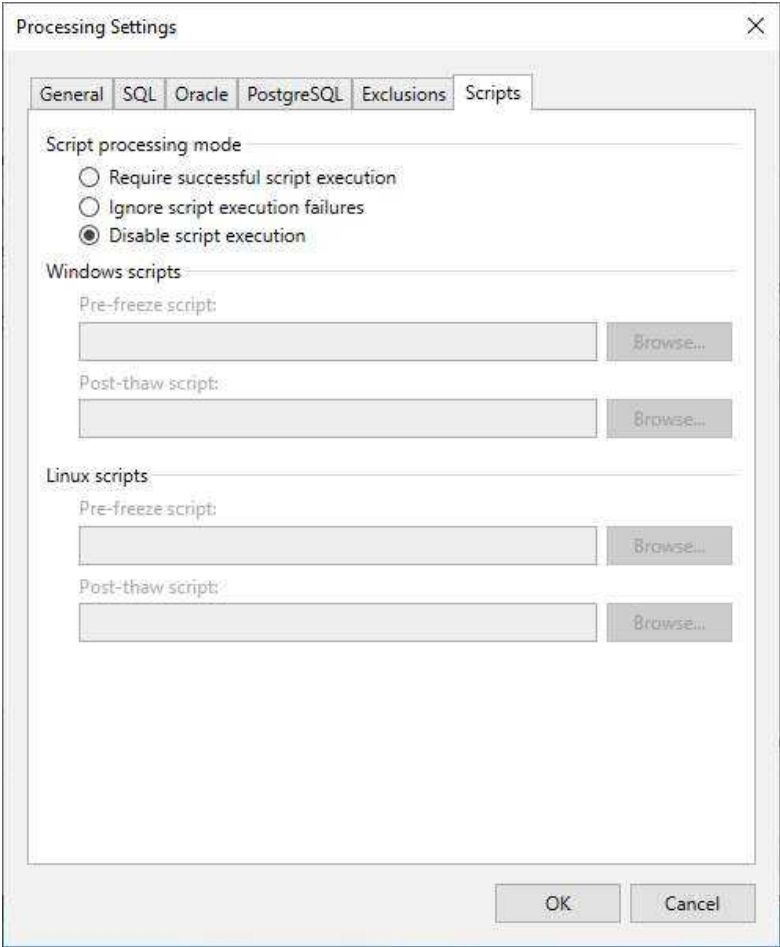
- 64. On the Processing Settings page, click PostgreSQL if the VM is a PostgreSQL Server VM.
- 65. Select a user account from the drop-down list.
- 66. Select Database user with password checkbox.



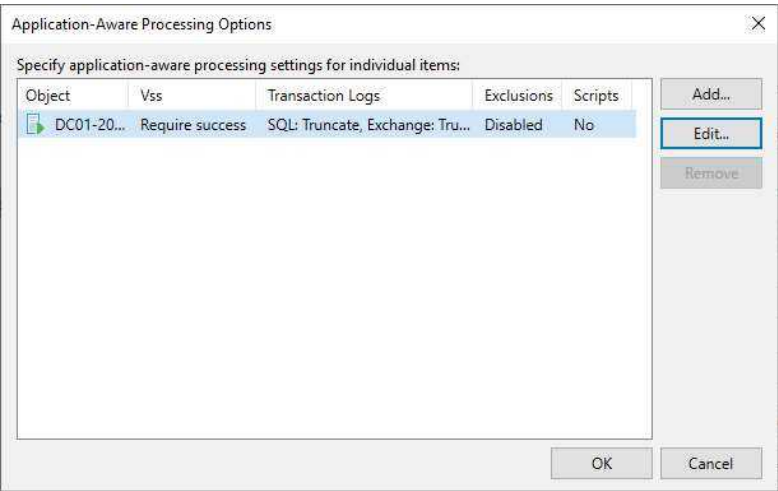
67. On the Processing Settings page, click Exclusions and keep the default settings.



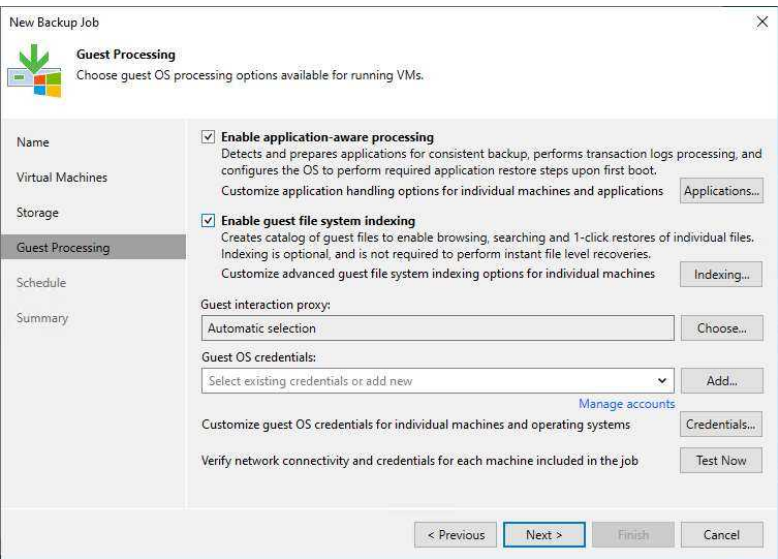
- 68. On the Processing Settings page, click Scripts and keep the default settings.
- 69. Click OK.



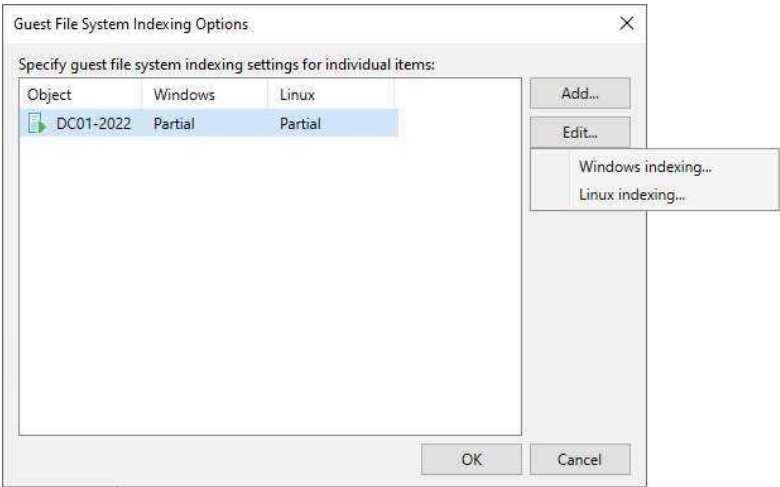
70. On the Application-Aware Processing Options page, click OK.



71. Select the Enable guest file system indexing checkbox and click Indexing.

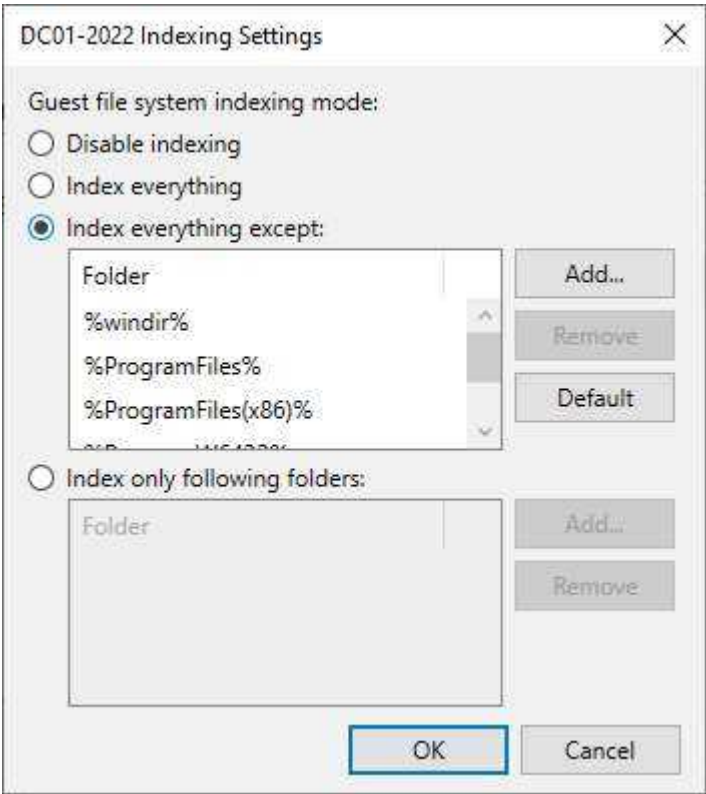


72. On the Guest File System Indexing Options page, select the VM, click Edit and select Windows indexing.

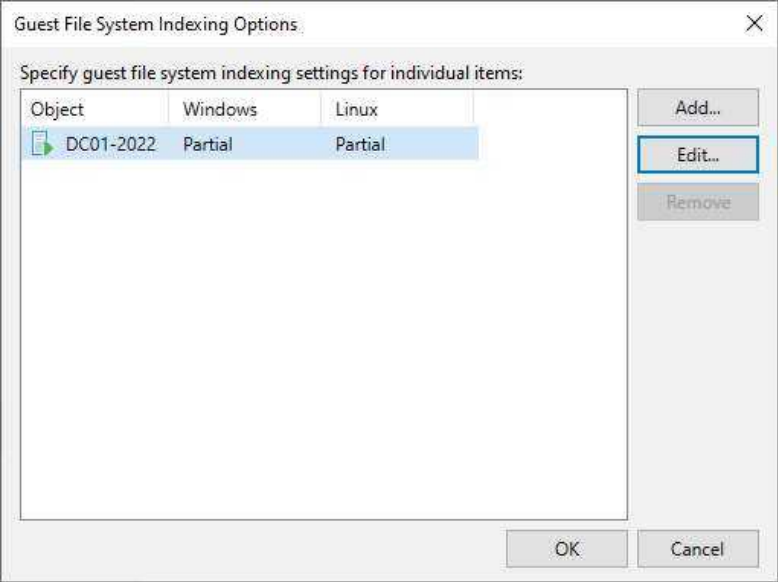


73. On the Guest file system indexing mode page, keep the default settings.

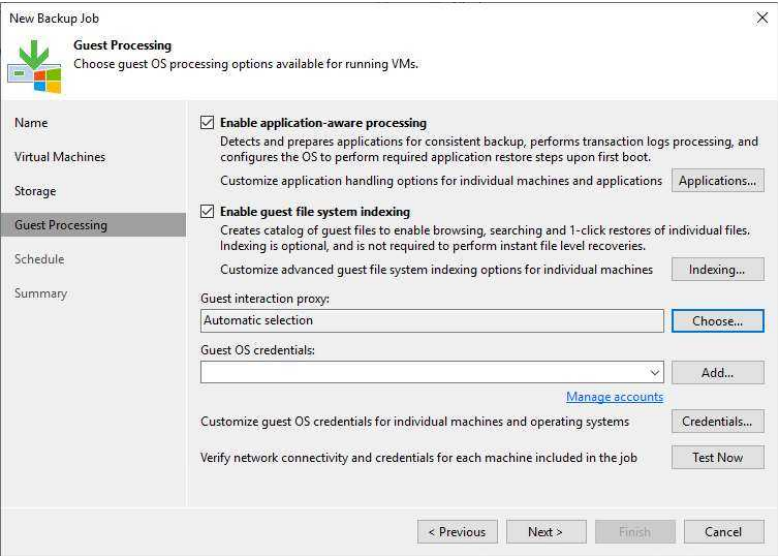
74. Click OK.



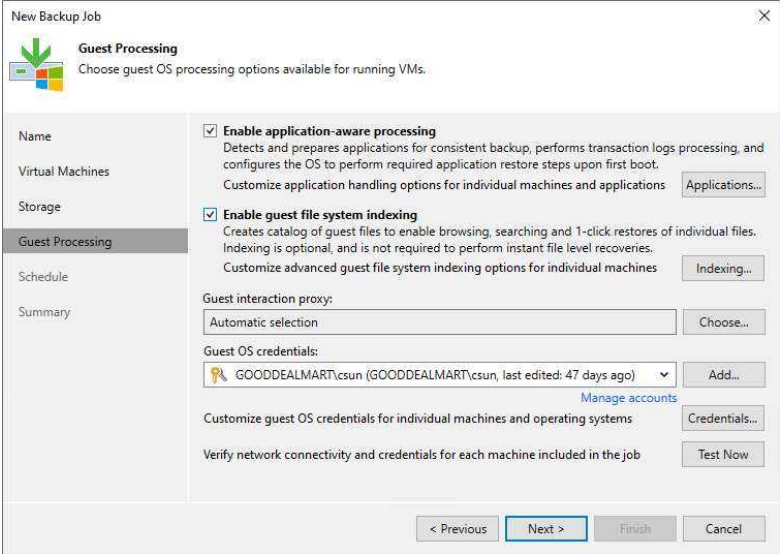
75. Click OK on the Guest file system indexing mode page.



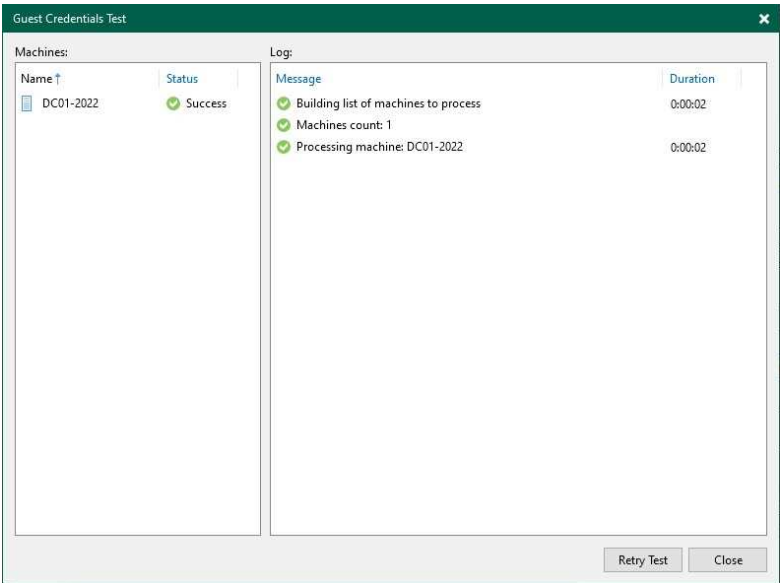
76. Keep the default Automatic selection in the Guest interaction proxy field.



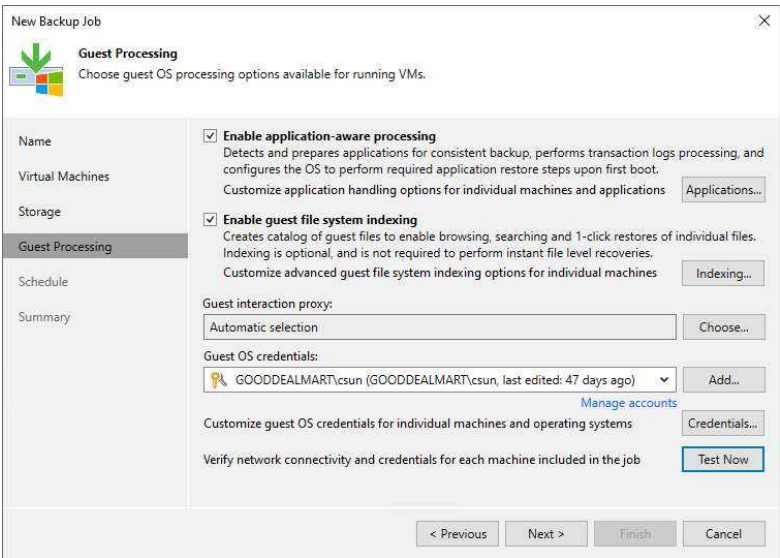
- 77. Choose a user account on the Guest Processing page with sufficient permissions from the Guest OS credentials drop-down list.
- 78. If you have multiple VMs at the same job, click Credentials to Customize guest OS credentials for individual machines and operating systems.
- 79. On the Guest Processing page, click Test Now to verify network connectivity and credentials for each machine included in the job.



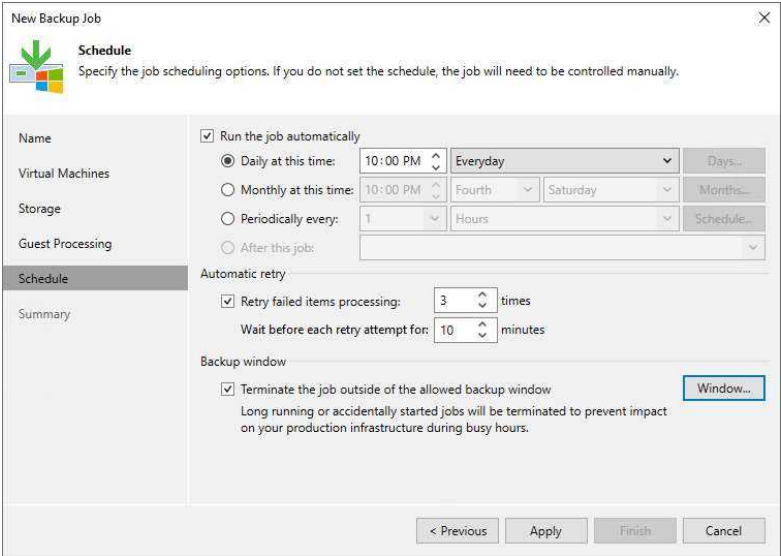
- 80. On the Guest Credentials Test page, ensure verification on success for each machine.
- 81. Click Close.



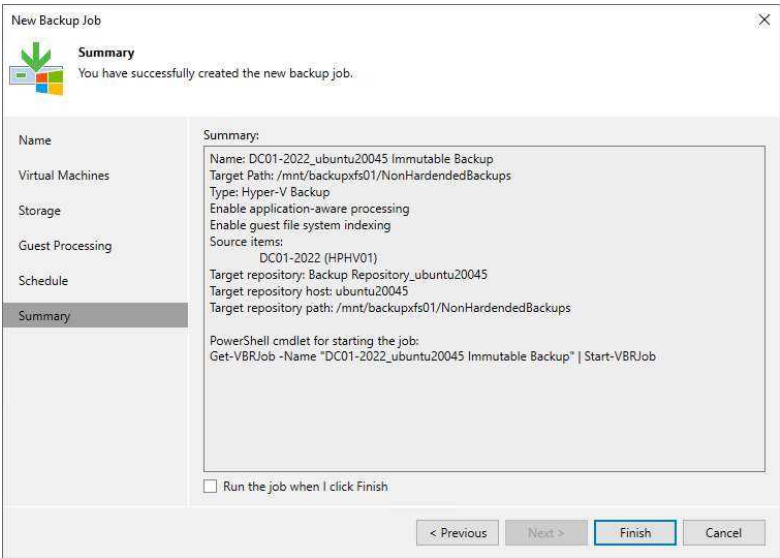
- 82. Click Next on the Guest Processing page.



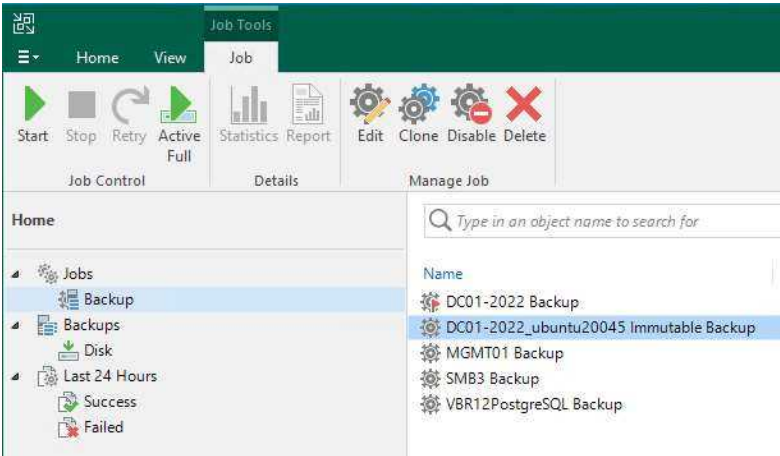
- 83. Select Run the job automatically checkbox on the Schedule page and select your specified schedule.
- 84. Define whether Veeam Backup & Replica should retry the backup job if it fails in the Automatic retry section.
- 85. Define the time interval the backup job must complete in the Backup window 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.



87. Click Finish on the Summary page.

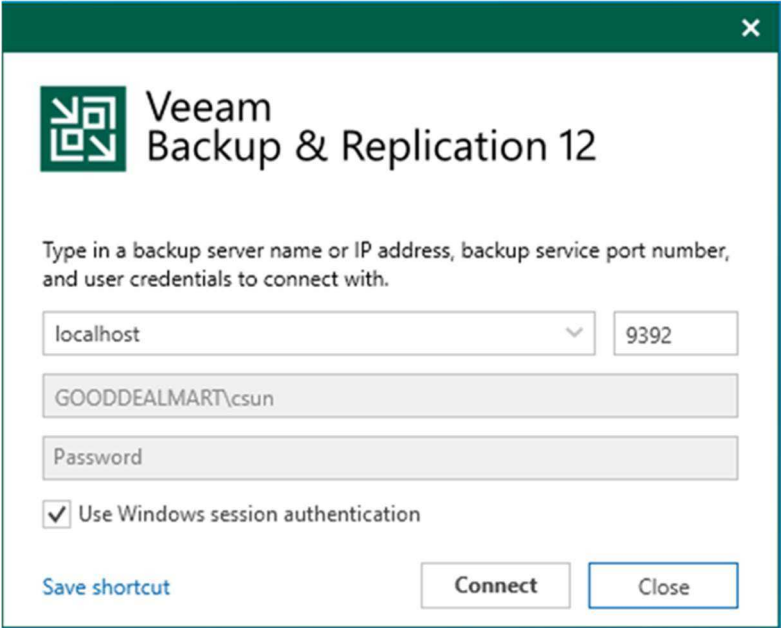


88. Verify that the backup job has been added.

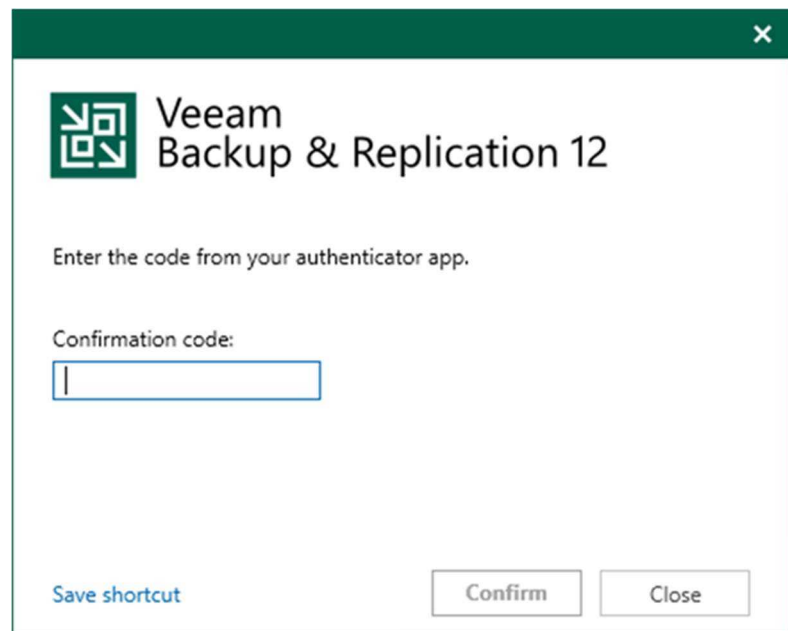


Create a Backup job to backup the specified Physical Machines (Managed by Backup Server Mode)

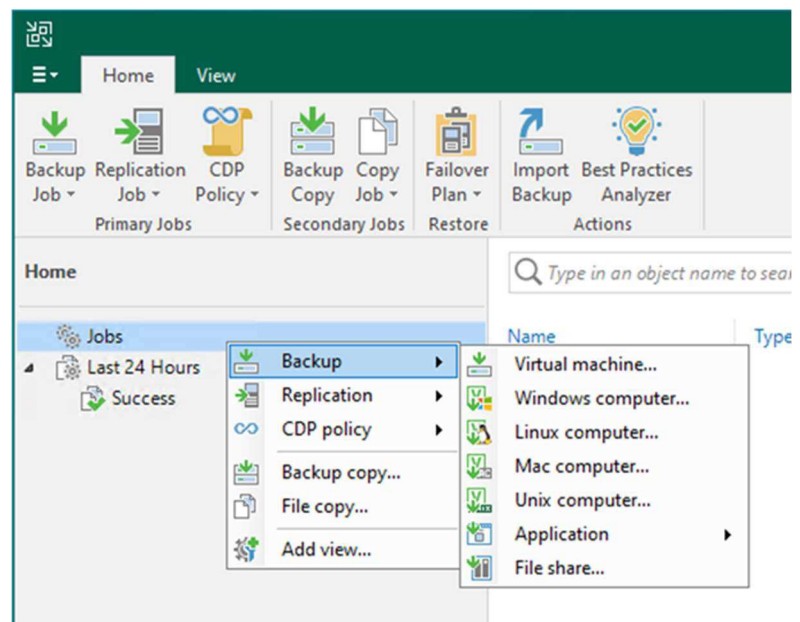
This procedure uses the managed backup server mode to create a backup job to back up the specific physical production machines.

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.	

3. Enter the MFA Confirmation code and click Confirm.



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.

Job Mode

Name

Computers

Backup Mode

Storage

Guest Processing

Schedule

Summary

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.

< Previous **Next >** Finish Cancel

- 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

Computers

Backup Mode

Storage

Guest Processing

Schedule

Summary

Name:

Hyper-V Hosts Agent Backup_by backup server

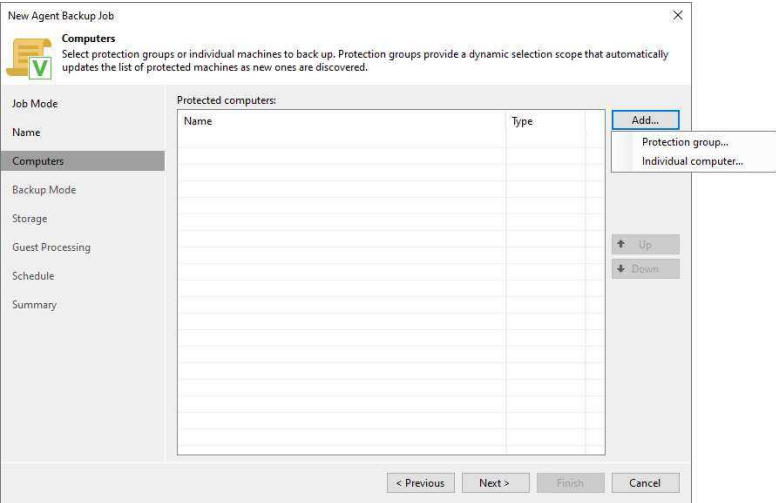
Description:

Created by GOODDEALMART\csun at 2/22/2023 11:06 AM.

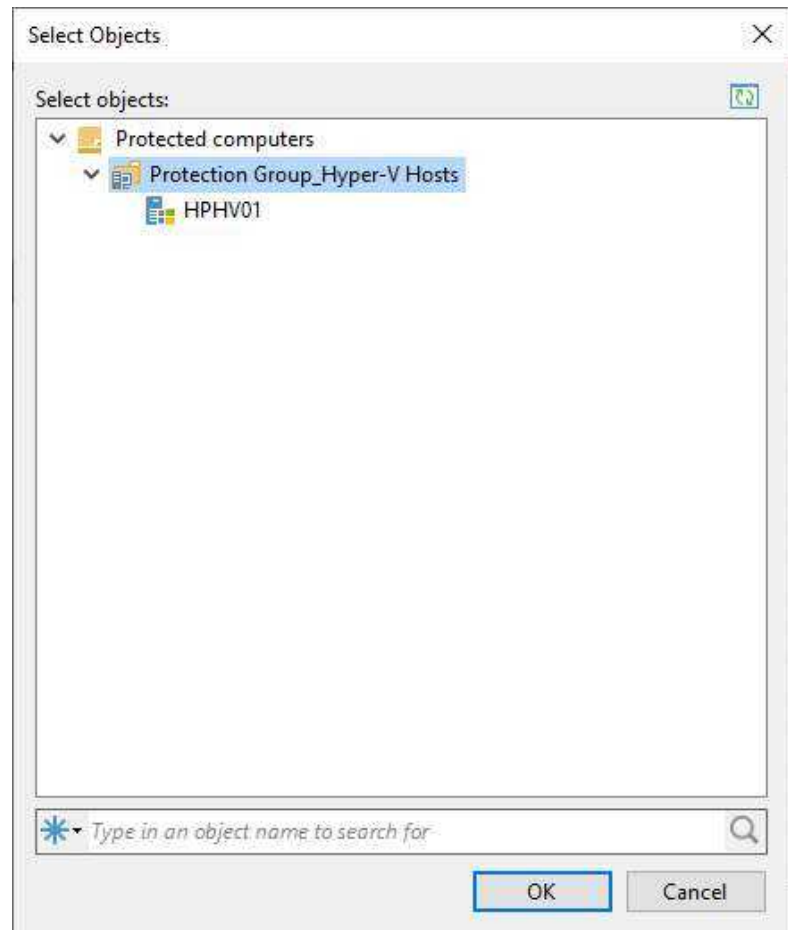
☐ High priority
Backup infrastructure resources are offered to high priority jobs first. Use this option for jobs sensitive to the start time, or jobs with strict RPO requirements.

< Previous **Next >** Finish Cancel

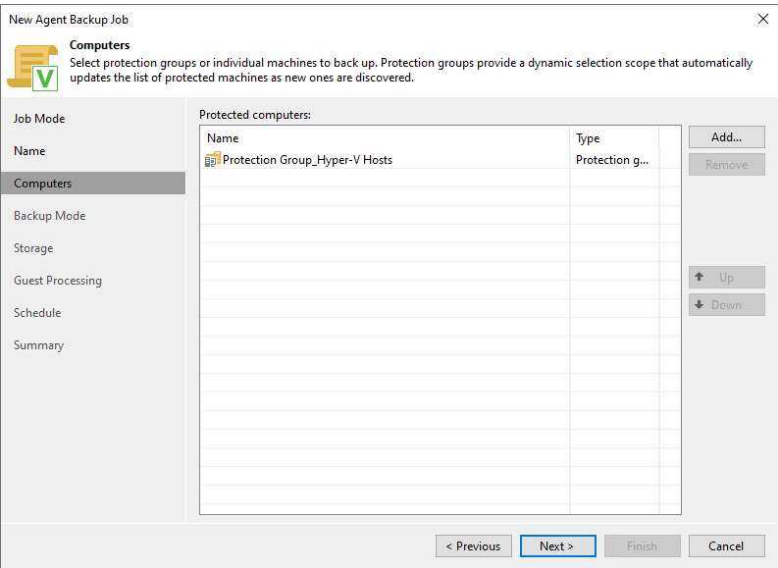
10. On the Computers page, click Add and select Protection group.



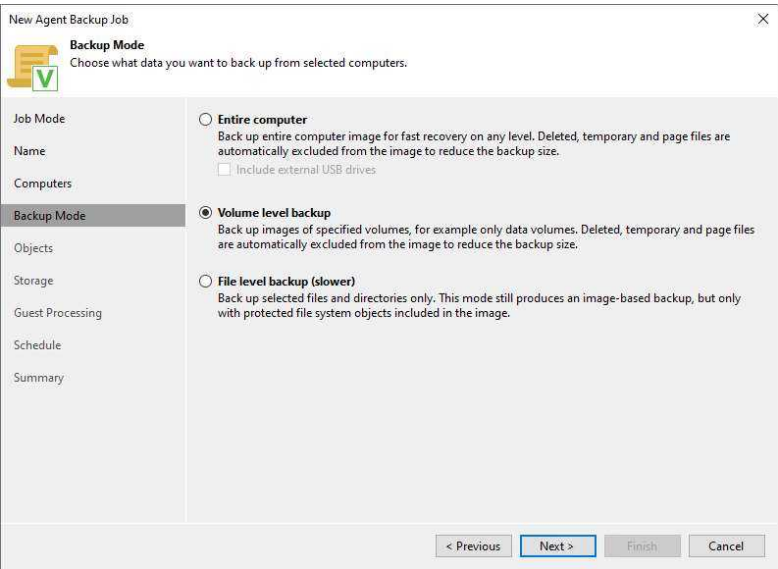
11. Select the protection group on the Select Objects page and click OK.
12. You can select multiple protection groups for the same backup job and repeat the step to add them.



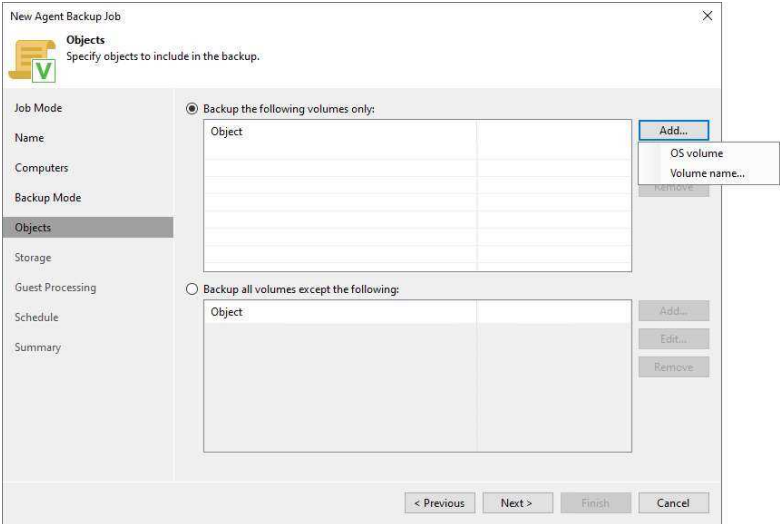
13. Click Next on the Computers page.



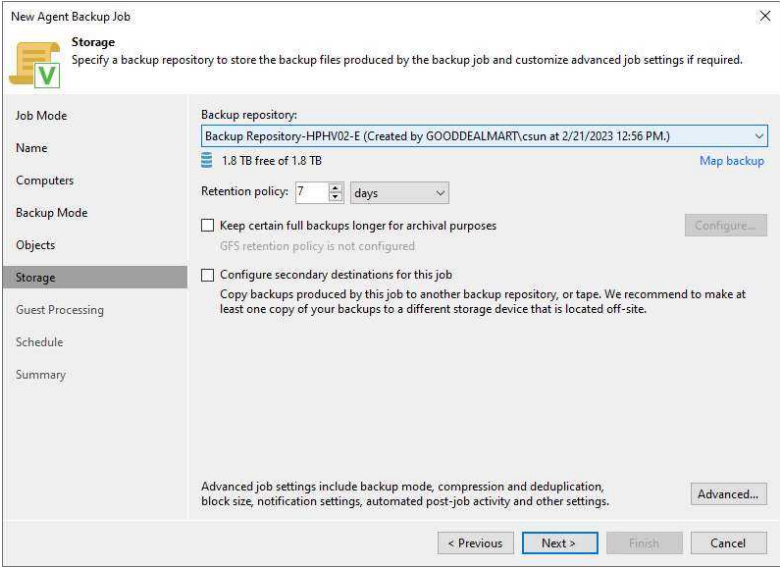
14. Select Volume level backup mode on the Backup Mode page to back up the specified computer volumes and click Next.



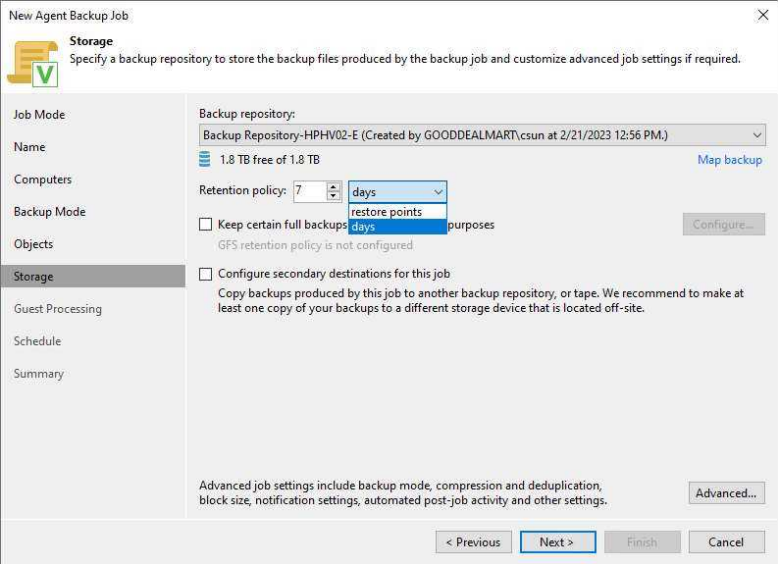
- 15. On the Objects page, select Backup the following volumes only.
- 16. Click Add and select OS volume.
- 17. Click Next



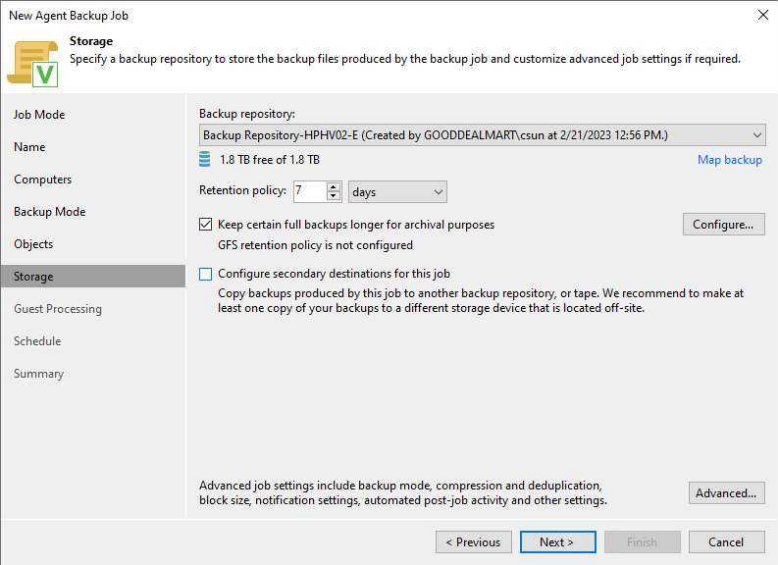
- 18. Select the backup repository from the Backup repository drop-down list on the Storage page.



- 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.



- 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.



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.
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.

Job Mode

Name

Computers

Backup Mode

Objects

Storage

Guest Processing

Schedule

Summary

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 5 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.

Map backup

Configure...

Advanced...

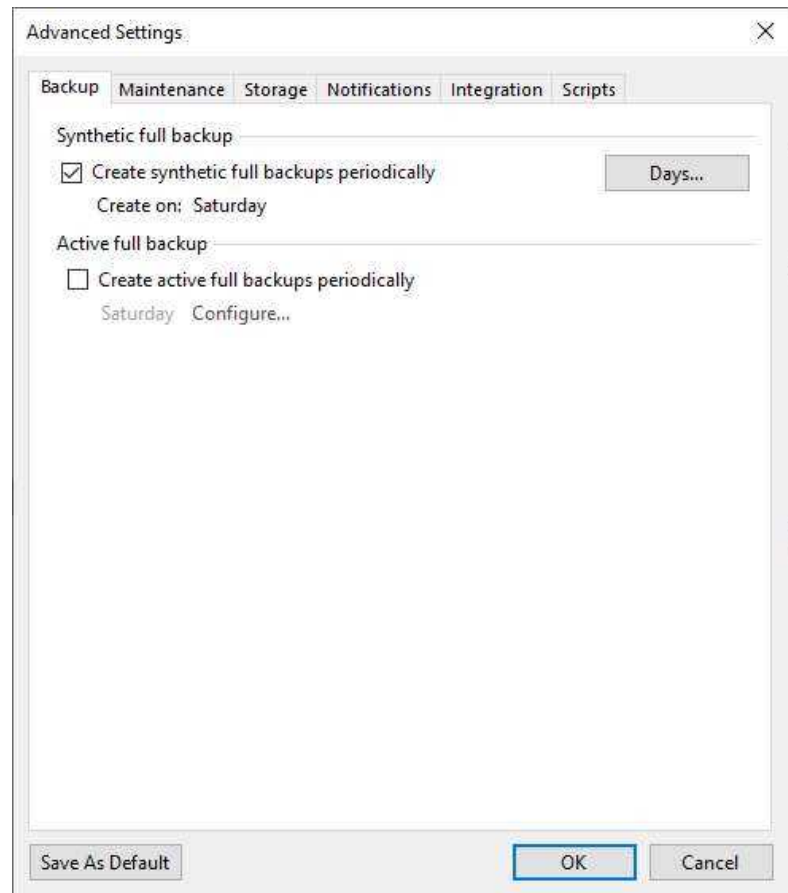
< Previous

Next >

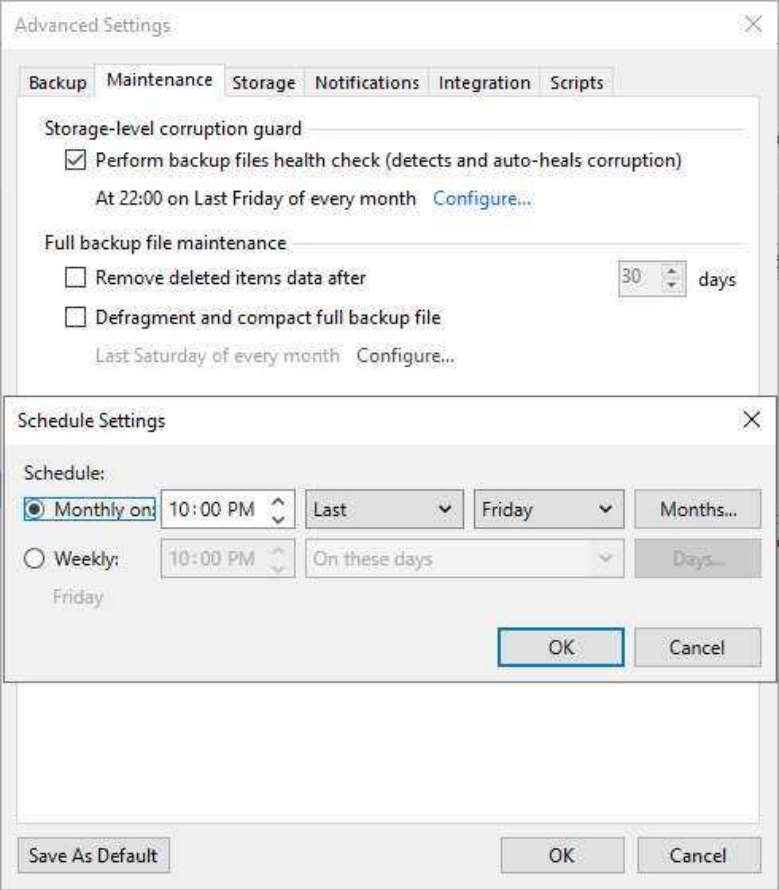
Finish

Cancel

28. Select Create synthetic full backups or Active full backups periodically checkbox.
29. Schedule full backups periodically and click OK.



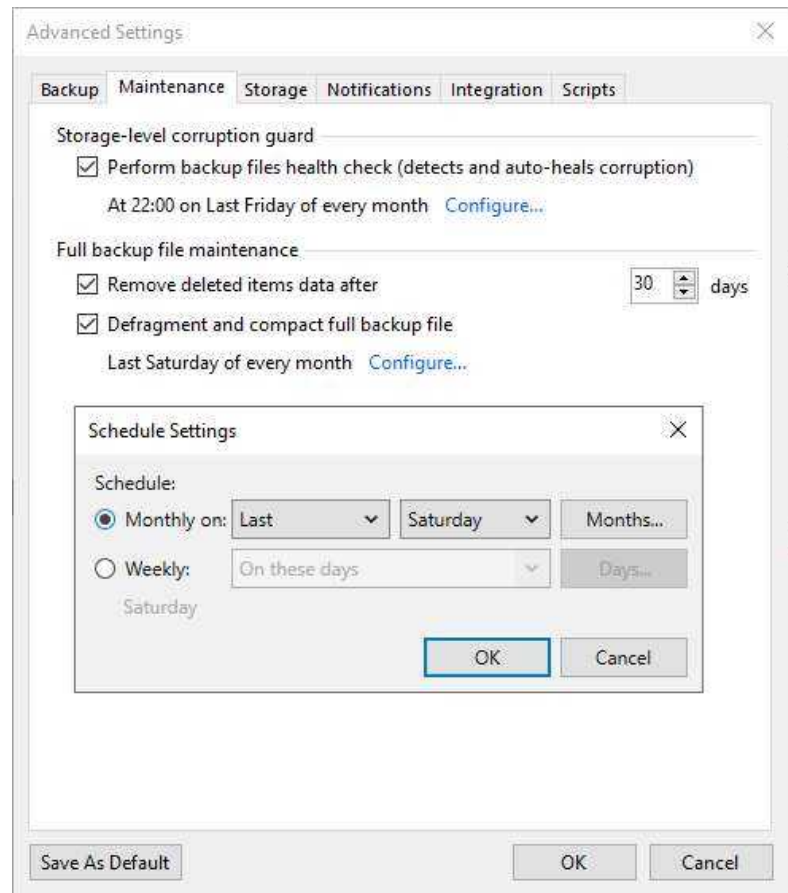
- 30. On the Advanced Settings, select Maintenance.
- 31. To regularly perform a health check on the backup chain's most recent restore point, select the Perform backup files health check (detects and auto-heals corruption) checkbox in the Storage-level corruption guard section.
- 32. Click Configure to set a timetable for the health check.



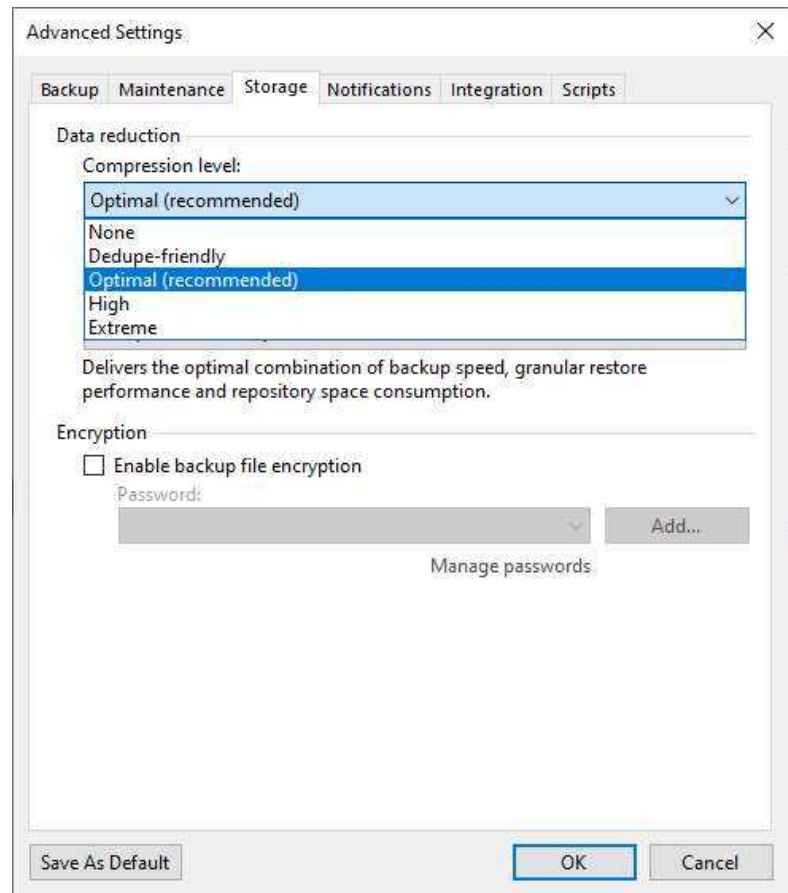
33. Select the Remove deleted items data after the checkbox and enter the few days you want backup data for deleted VMs to be kept.
34. Select the Defragment and compact full backup file checkbox and click Configure.
35. Set the schedule for the compact operation to compact a full backup periodically.

Note:

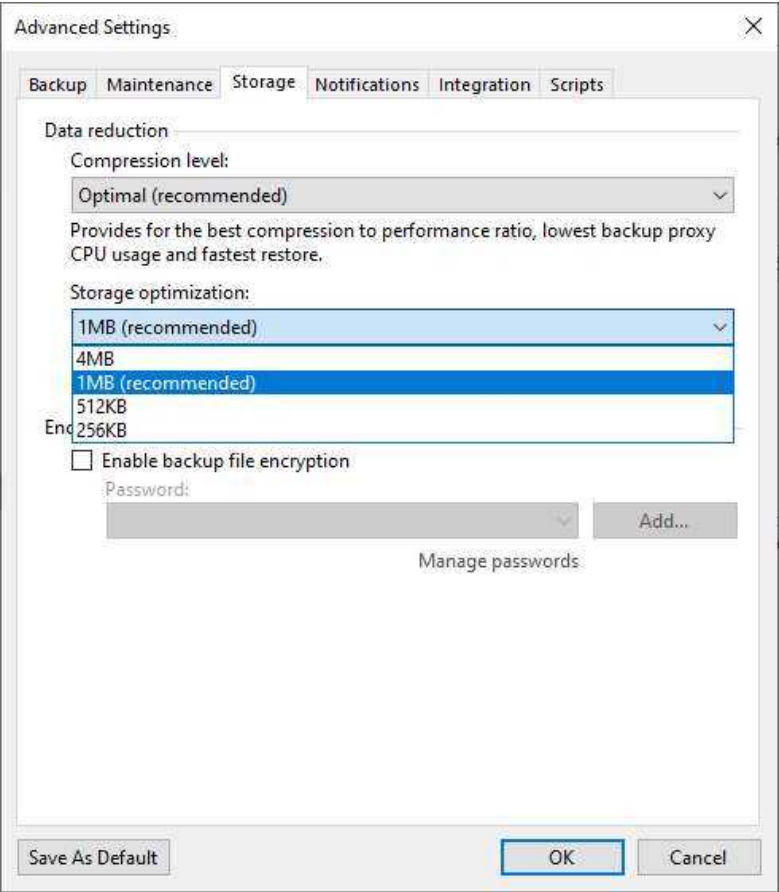
You don't need to enable the defragment and compact functionality checkbox if GFS retention is enabled.



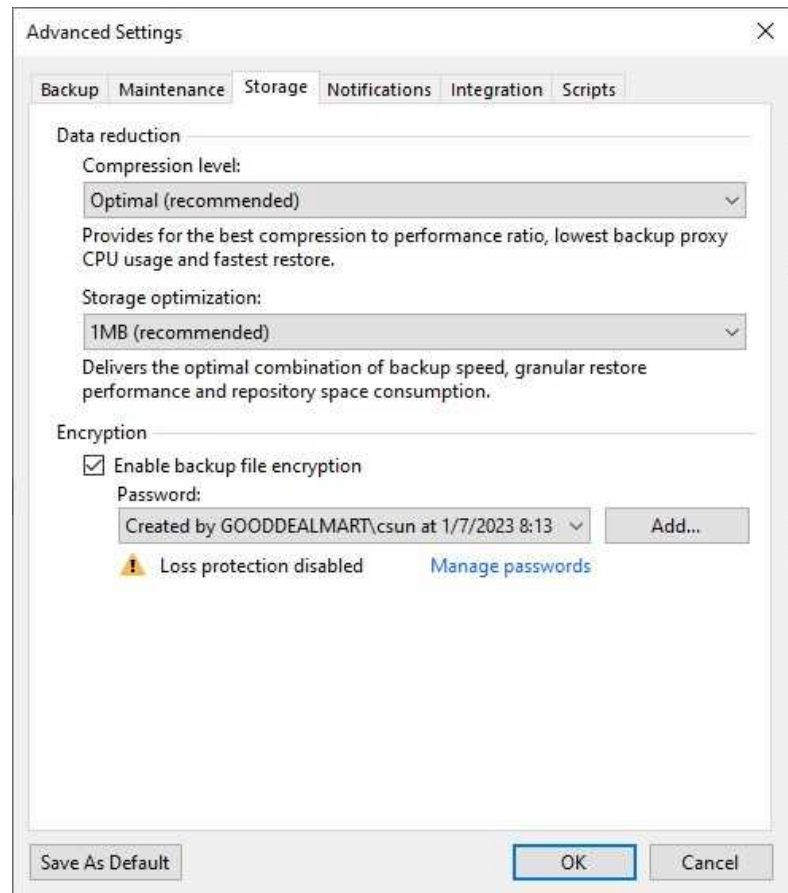
36. On Advanced Settings, select Storage.
37. Select the Compression level from the drop-down list.



38. Select Storage optimization from the drop-down list.



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.

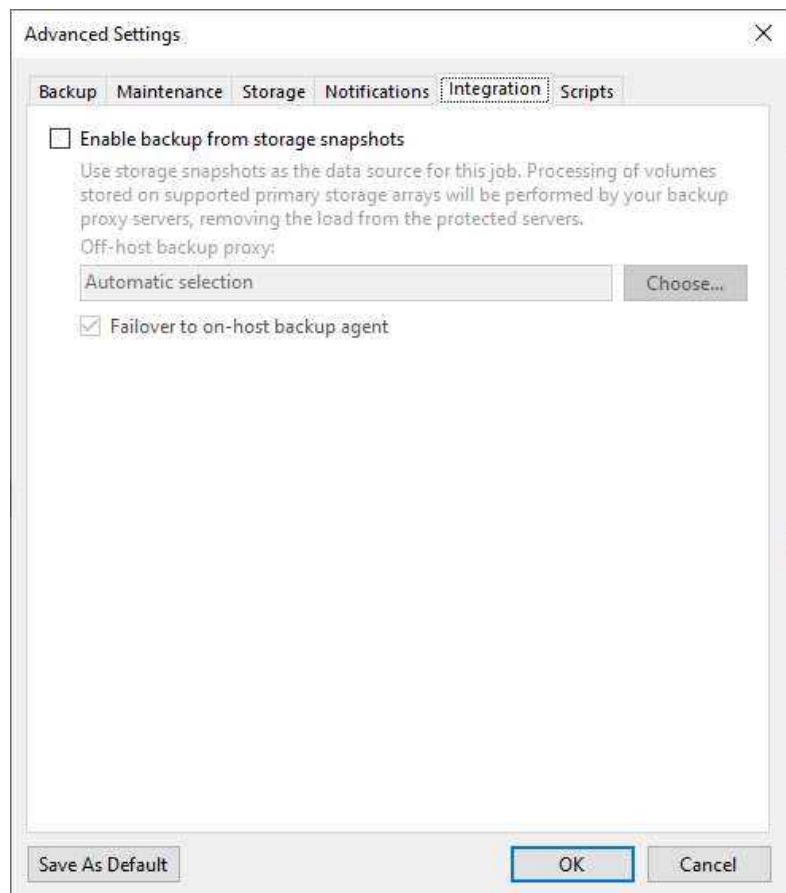


41. On the Advanced Settings, select No notifications.
42. Keep the default settings.

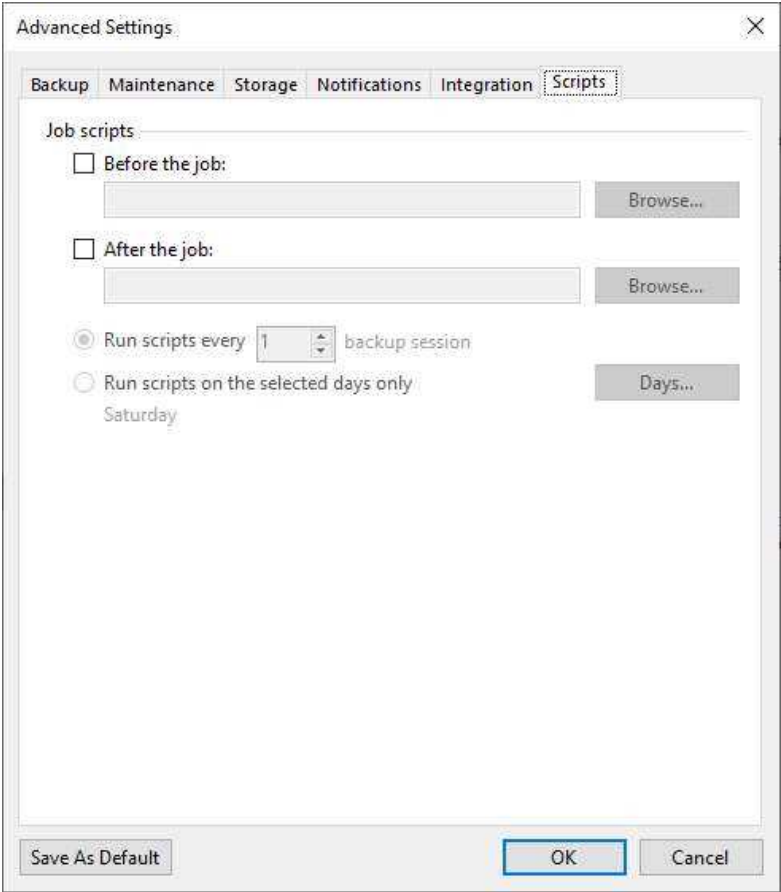


43. On the Advanced Settings, select Integration.

44. Keep the default settings.



- 45. On the Advanced Settings page, select Scripts.
- 46. Keep the default settings and click OK.



47. On the Storage page, click Next.

The screenshot shows the 'New Agent Backup Job' dialog box with the 'Storage' tab selected. The left sidebar contains a list of tabs: Job Mode, Name, Computers, Backup Mode, Objects, Storage (selected), Guest Processing, Schedule, and Summary. The main area is titled 'Storage' and contains the following options: 'Backup repository:' with a dropdown menu showing 'Backup Repository-HPHV02-E (Created by GOODDEALMART\csun at 2/21/2023 12:56 PM.)' and '1.8 TB free of 1.8 TB'; 'Retention policy:' with a dropdown menu showing '7 days'; a checkbox for 'Keep certain full backups longer for archival purposes' (unchecked); a checkbox for 'Configure secondary destinations for this job' (unchecked); and a button 'Advanced...'. At the bottom, there are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

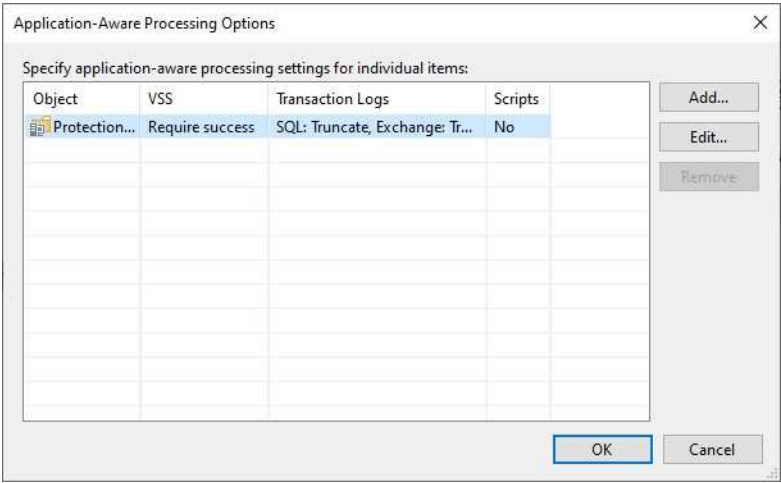
48. When you add Physical machines running VSS-aware applications to the backup job, you can enable application-aware processing to create a transactionally consistent backup. The transactionally consistent backup ensures that applications on VMs can be recovered without data loss.

The screenshot shows the 'New Agent Backup Job' dialog box with the 'Guest Processing' tab selected. The left sidebar contains a list of tabs: Job Mode, Name, Computers, Backup Mode, Objects, Storage, Guest Processing (selected), Schedule, and Summary. The main area is titled 'Guest Processing' and contains the following options: a checkbox for 'Enable application-aware processing' (checked), a checkbox for 'Enable guest file system indexing' (unchecked), and buttons for 'Applications...' and 'Indexing...'. At the bottom, there are buttons for '< Previous', 'Next >', 'Finish', and 'Cancel'.

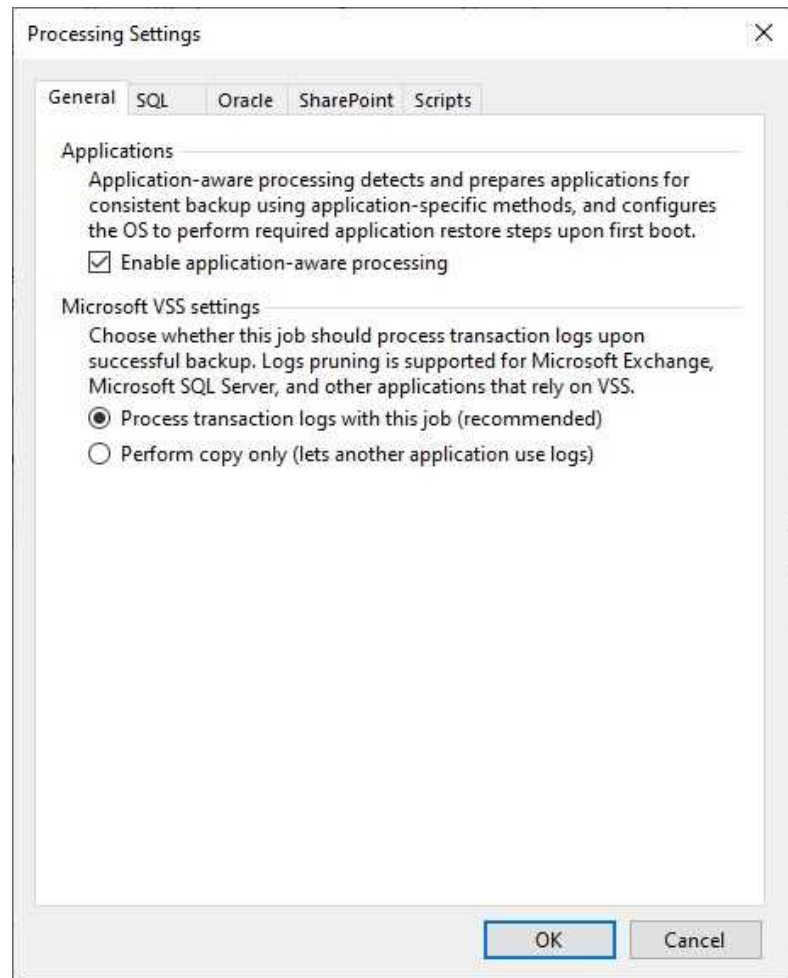
49. Select the Enable application-aware processing checkbox on the Guest Processing

page, and click
Applica ons.

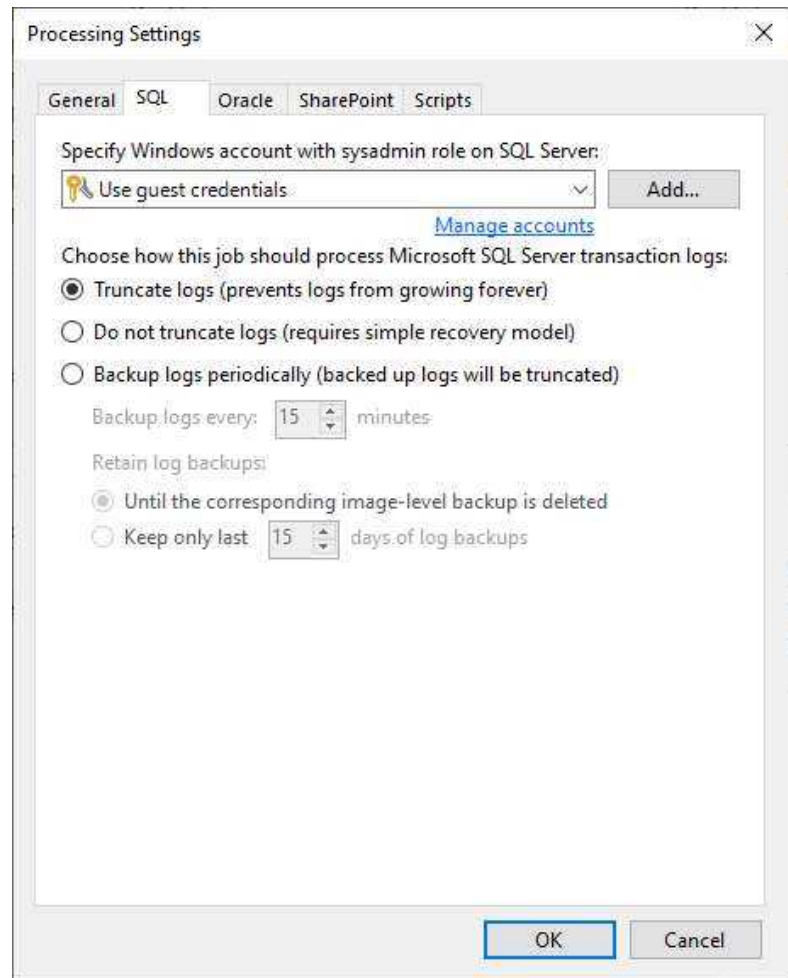
50. On the Applica on-Aware Processing Op ons page, select the Object and click Edit.



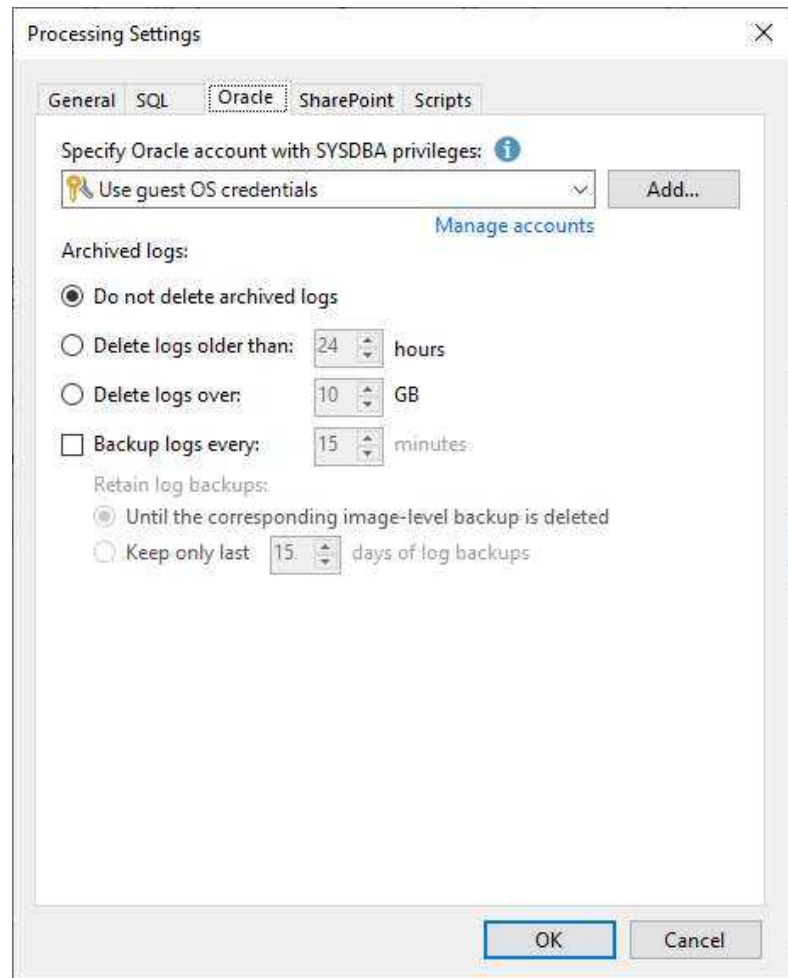
51. On the Processing Settings page, select General.
52. Select Enable application-aware processing checkbox.
53. Select Process transaction logs with this job (recommended).



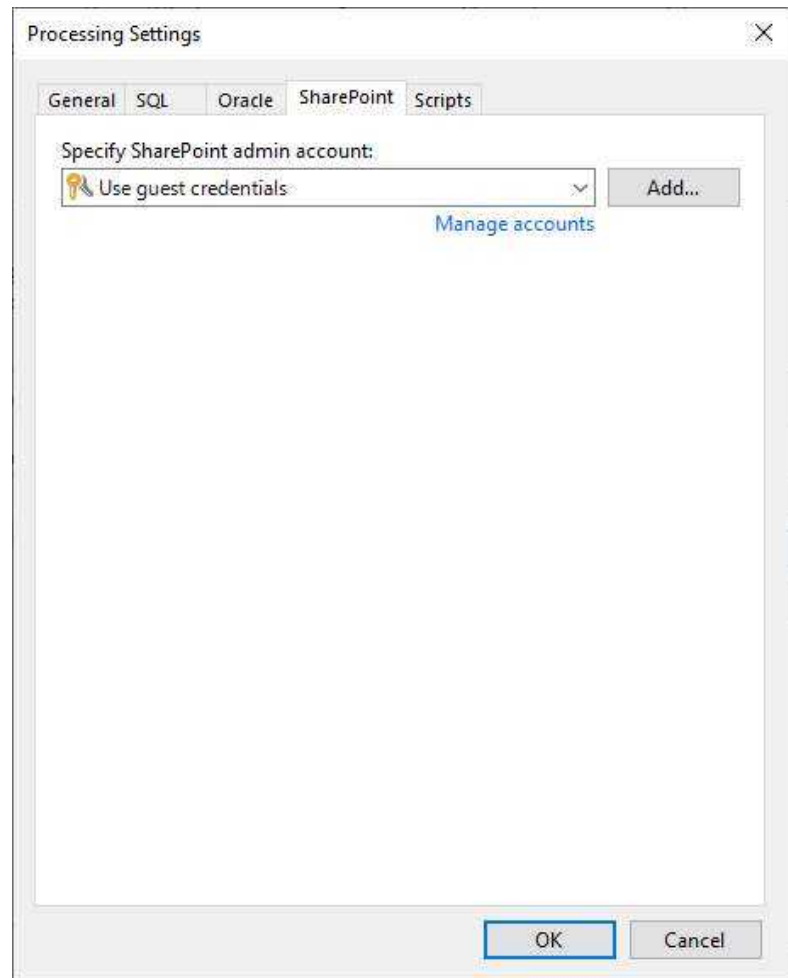
54. On the Processing Settings page, click SQL if the Physical Machine is a Microsoft SQL Server.
55. Select a user account from the drop-down list.
56. Select Truncate logs (Prevents logs from growing forever).



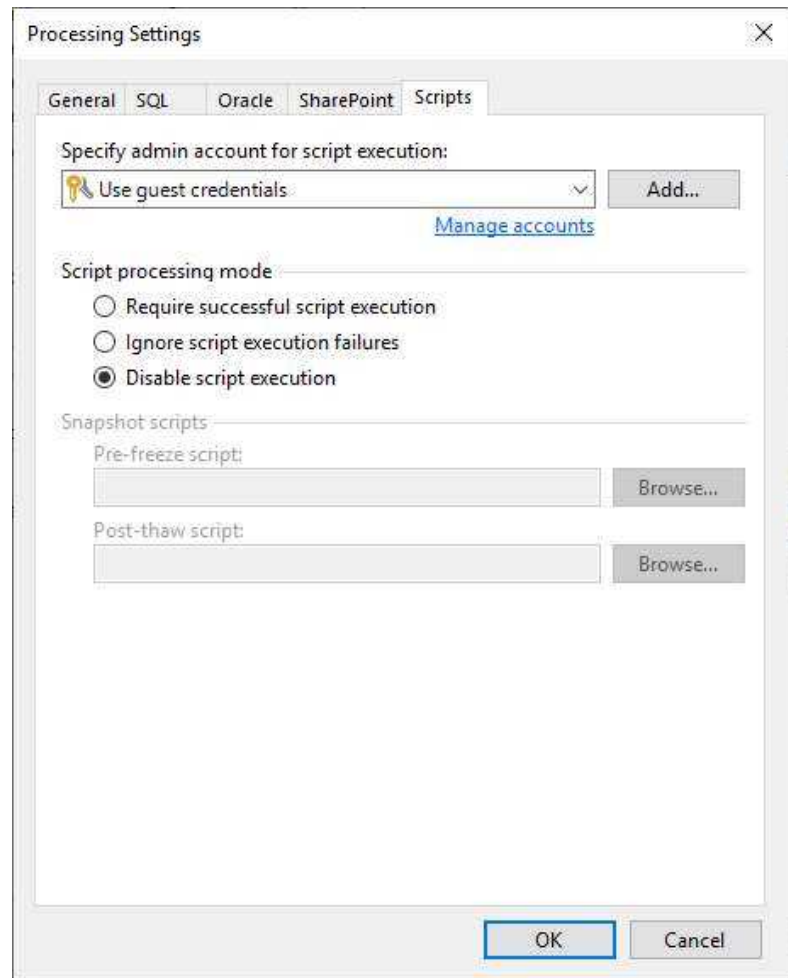
- 57. Select Oracle on the Processing Settings page if the Physical Machine is an Oracle Server.
- 58. Select a user account from the drop-down list.
- 59. Select Do not delete archived logs.



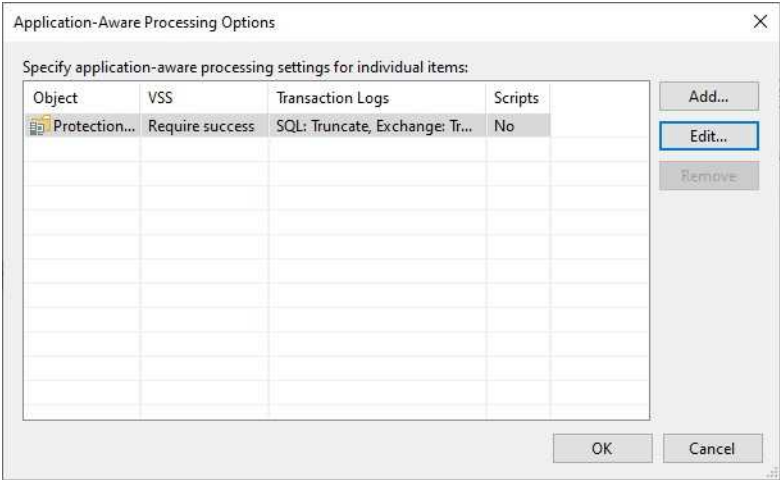
60. On the Processing Settings page, select SharePoint if the Physical Machine is a SharePoint Server.
61. Select a user account from the drop-down list.



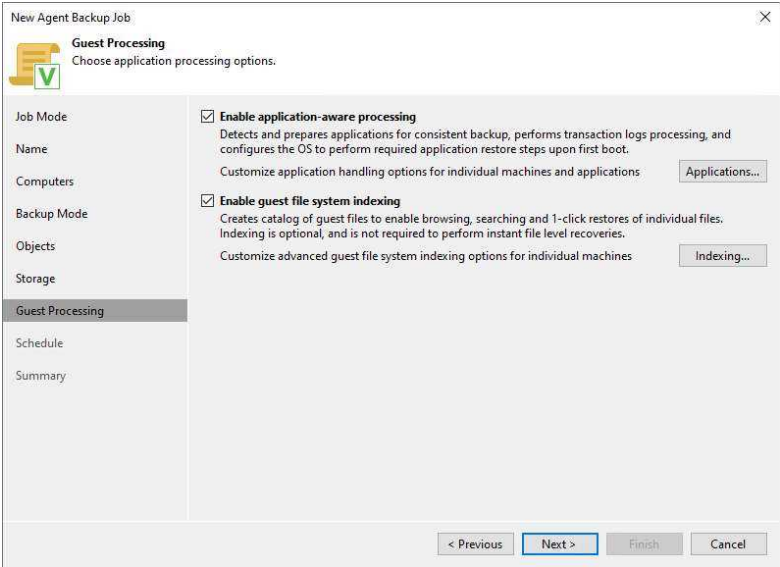
62. On the Processing Settings page, select Scripts.
63. Keep the default settings and click OK.



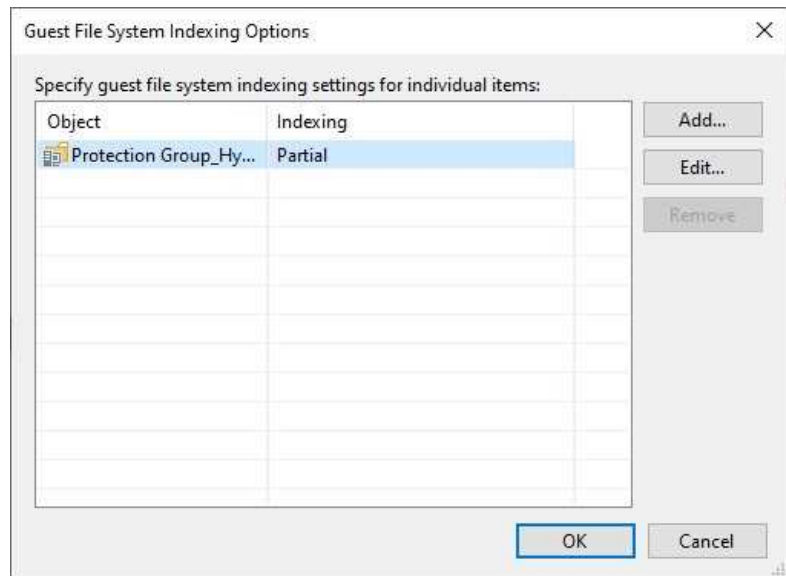
64. On the Application-Aware Processing Options page, click OK.



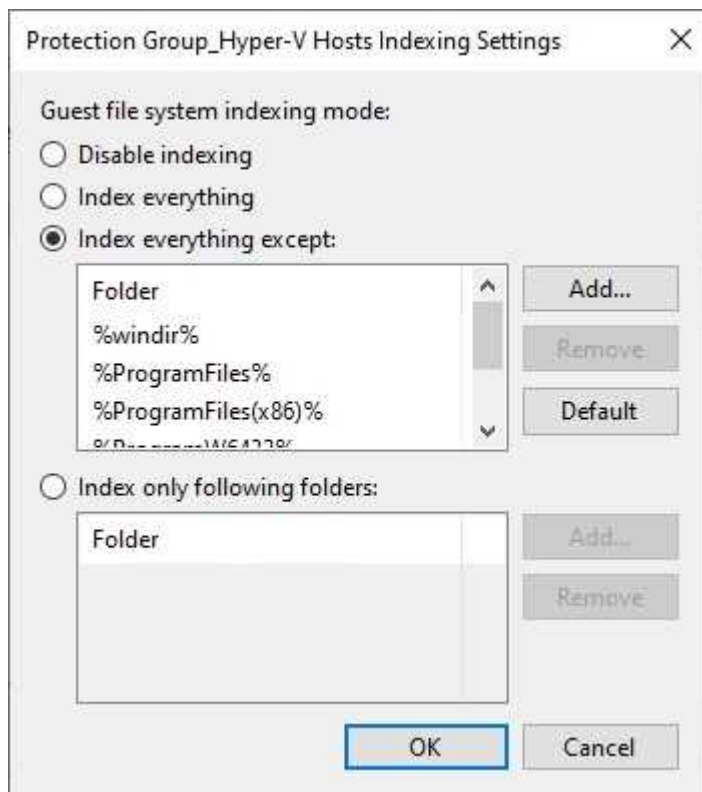
65. Select the Enable guest file system indexing checkbox and click Indexing.



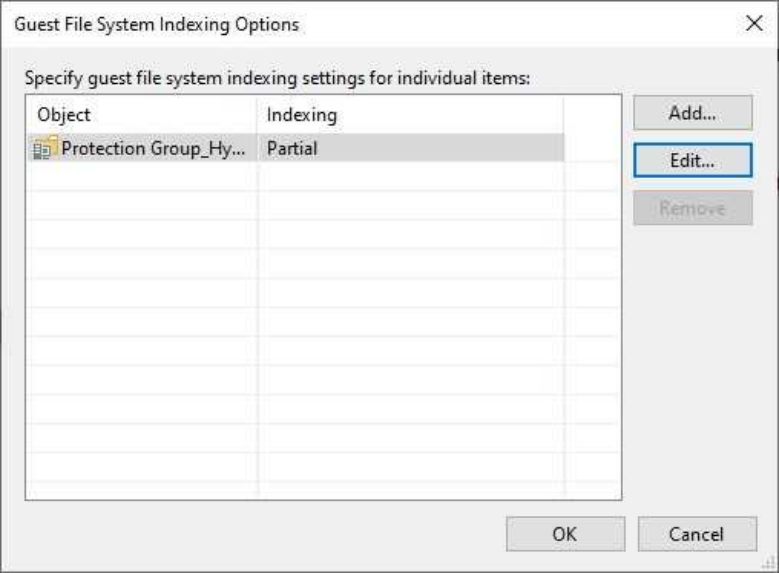
66. On the Guest File System Indexing Options page, select the Object, click Edit and.



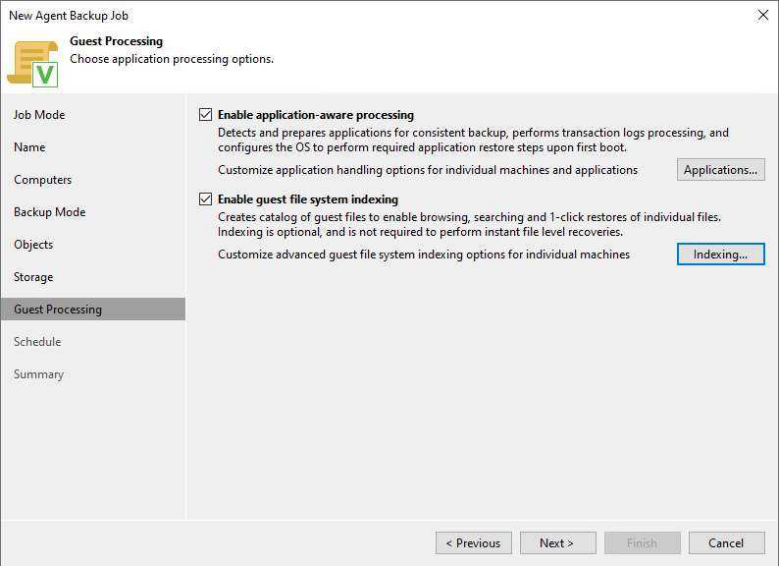
67. On the Guest file system indexing mode page, keep the default settings.
68. Click OK.



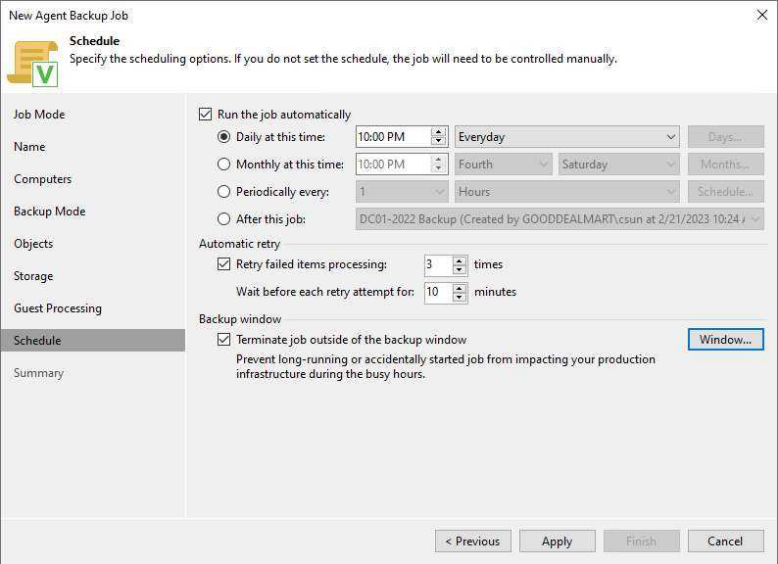
69. On the Guest File System Indexing Options page, click OK.



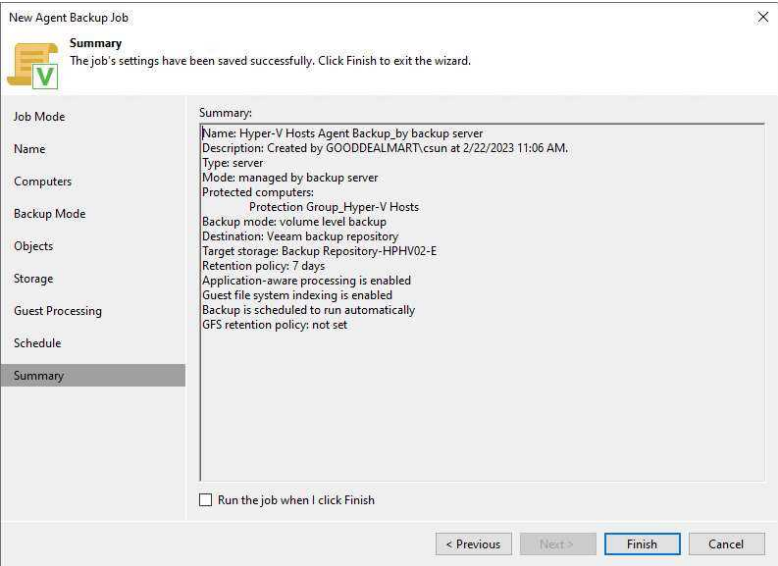
70. On the Guest Processing page, click Next.



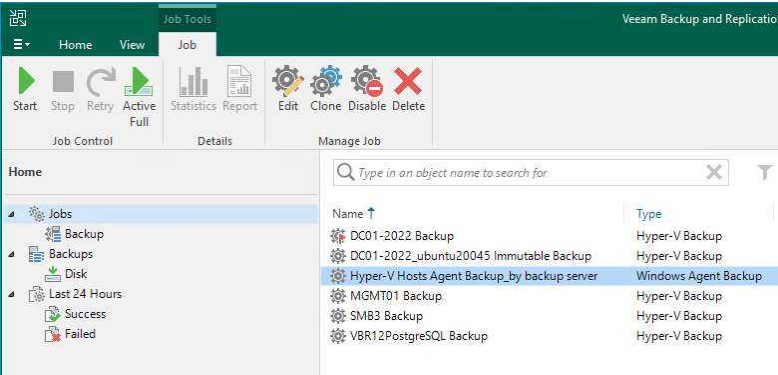
- 71. Select Run the job automatically checkbox on the Schedule page and select your specified schedule.
- 72. Define whether Veeam Backup & Replica should retry the backup job if it fails in the Automatic retry section.
- 73. Define the time interval the backup job must complete in the Backup window 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.



75. On the Summary page, click Finish.

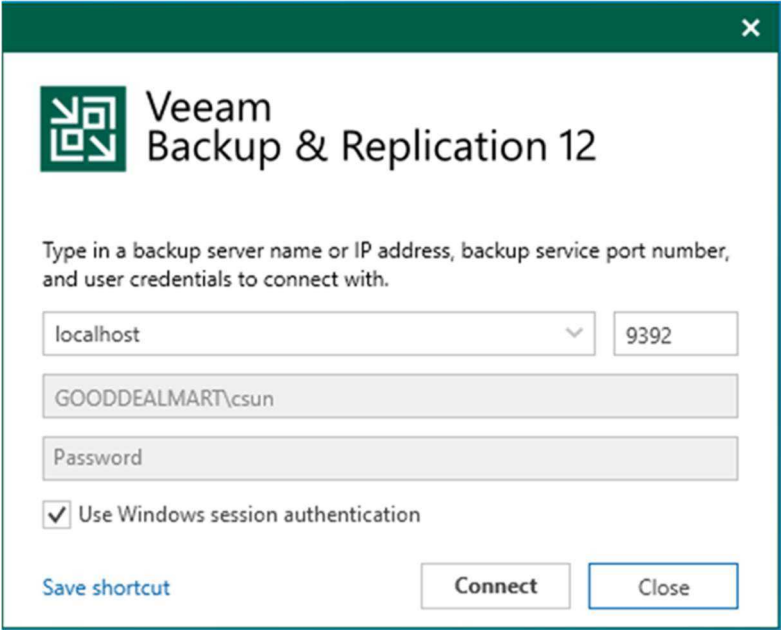


76. Verify that the backup job has been added

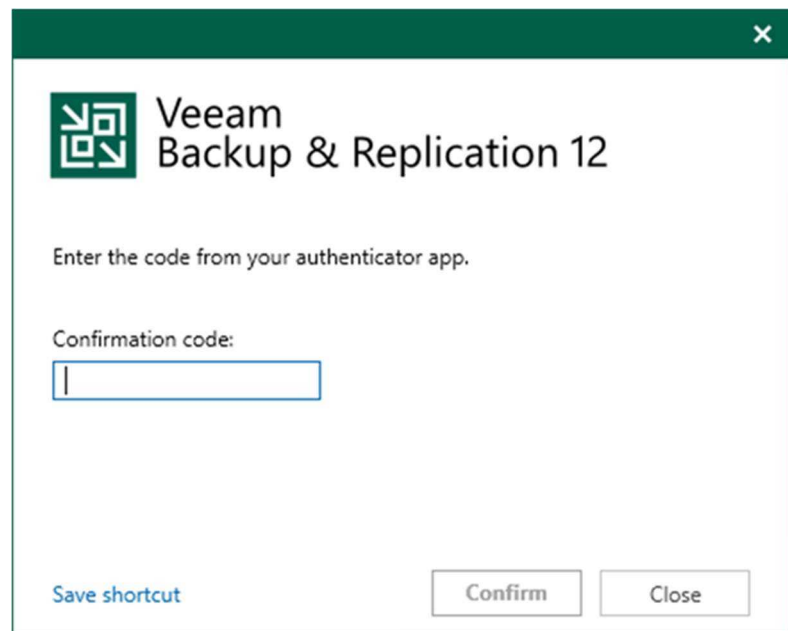


Create a Backup job to backup the specified Physical Machines (Managed by Agent Mode)

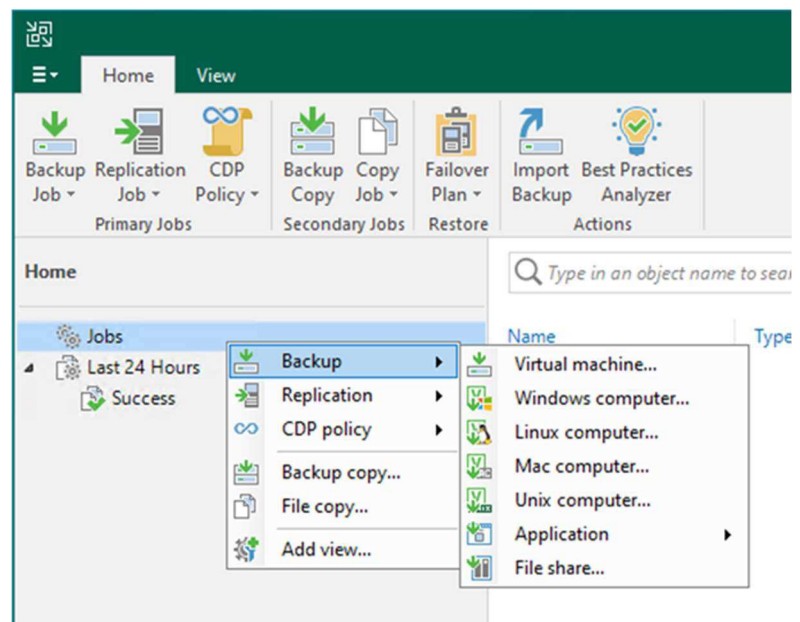
This procedure uses the managed backup server mode to create a backup job to back up the specific physical product on machines.

Instruc ons	Screenshot (if applicable)
1. Log in to the Veeam Backup and replica on manager server. 2. Open the Veeam Backup & Replica on Console and click Connect.	 The screenshot shows the Veeam Backup & Replication 12 console window. It has a dark green title bar with a close button. The main area is white with the Veeam logo and title. Below the title, there is a prompt: "Type in a backup server name or IP address, backup service port number, and user credentials to connect with." There are four input fields: a dropdown menu showing "localhost", a text box with "9392", a text box with "GOODDEALMART\csun", and a password field labeled "Password". Below these fields is a checkbox labeled "Use Windows session authentication" which is checked. At the bottom, there are three buttons: "Save shortcut" (blue text), "Connect" (white button), and "Close" (white button).

3. Enter the MFA Confirmation code and click Confirm.



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.

New Agent Backup Job

Job Mode

Specify protected computer type and backup agent management mode.

Job Mode

Name

Computers

Backup Mode

Destination

Local Storage

Guest Processing

Schedule

Summary

Type:

☐ Workstation

☒ Server

☐ Failover cluster

Mode:

☐ Managed by backup server

☒ Managed by agent

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.

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.

< Previous

Next >

Finish

Cancel

- 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.

Job Mode

Name

Computers

Backup Mode

Destination

Local Storage

Guest Processing

Schedule

Summary

Name:

Hyper-V Hosts Agent Backup_by agent

Description:

Created by GOODDEALMART\csun at 2/22/2023 11:12 AM

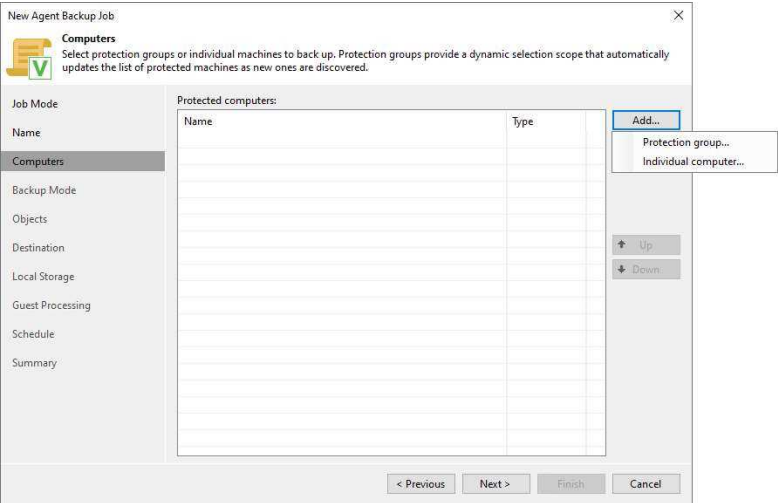
< Previous

Next >

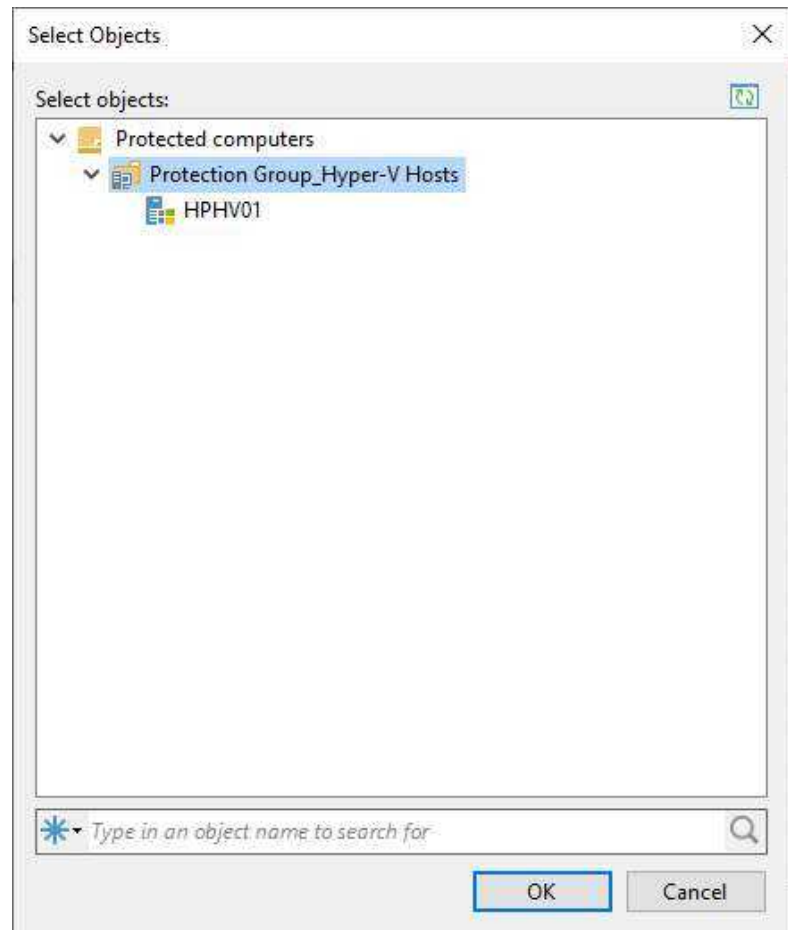
Finish

Cancel

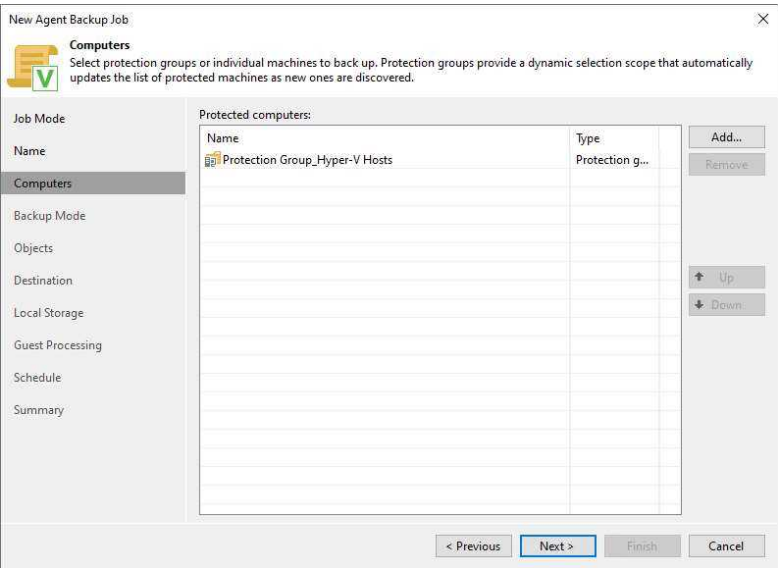
10. On the Computers page, click Add and select Protection group.



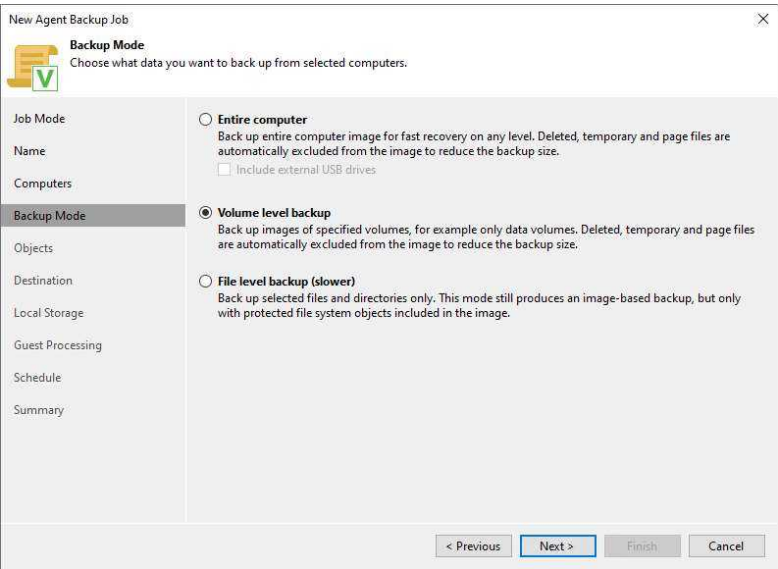
11. Select the protection group on the Select Objects page and click OK.
12. You can select multiple protection groups for the same backup job and repeat the step to add them.



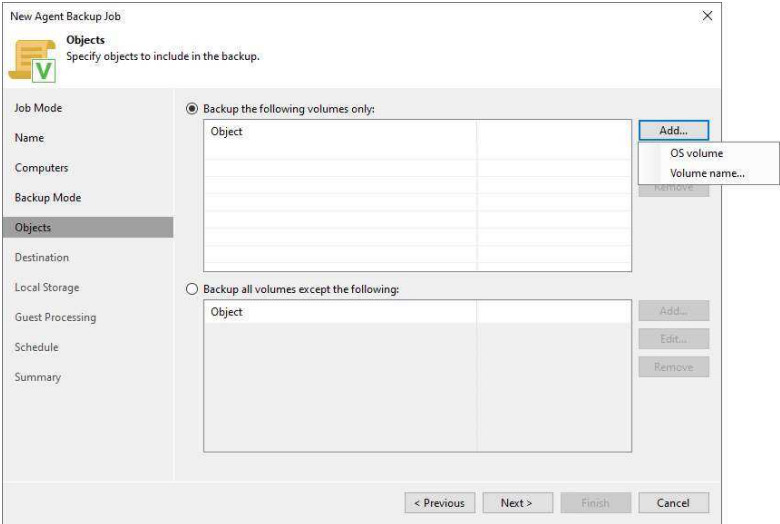
13. Click Next on the Computers page.



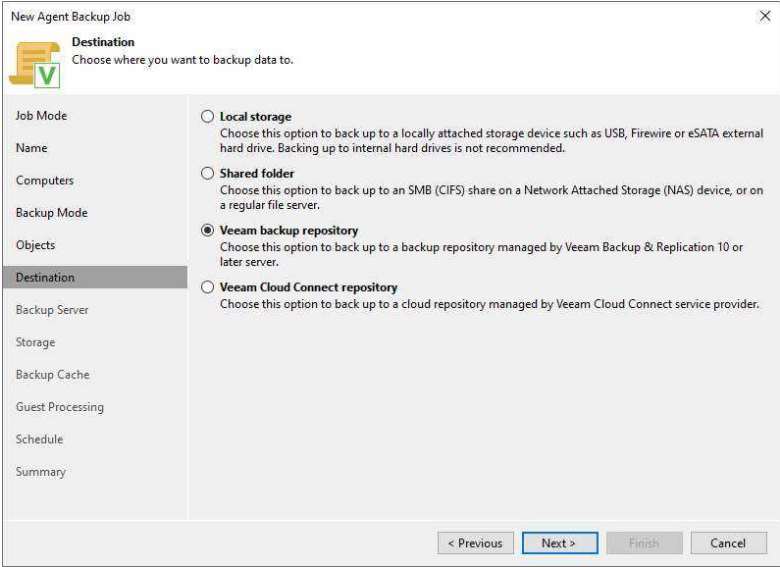
14. Select Volume level backup mode on the Backup Mode page to back up the specified computer volumes and click Next.



- 15. On the Objects page, select Backup the following volumes only.
- 16. Click Add and select OS volume.
- 17. Click Next



- 18. Select the Veeam backup repository and click Next.



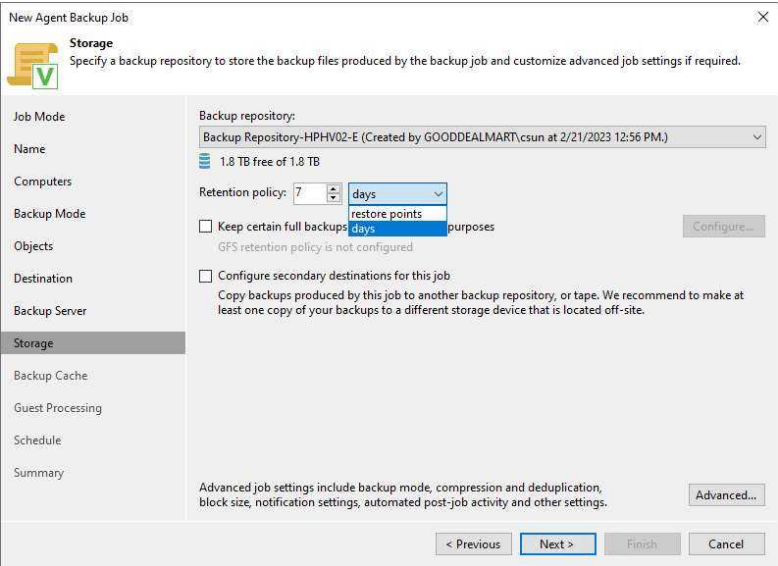
19. Enter the Veeam Backup and Replica on manager server name or IP address in the DNS name or external IP address field on the Backup Server page.

The screenshot shows the 'New Agent Backup Job' wizard, specifically the 'Backup Server' step. The left sidebar lists the steps: Job Mode, Name, Computers, Backup Mode, Objects, Destination, Backup Server (selected), Storage, Backup Cache, Guest Processing, Schedule, and Summary. The main area is titled 'Backup Server' and contains the instruction 'Specify Veeam Backup & Replication management server connection parameters.' Below this, there is a field for 'DNS name or external IP address:' with the value 'VBR12PostgreSQL.gooddealmart.ca' entered. A note states: '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.' At the bottom, there are navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.

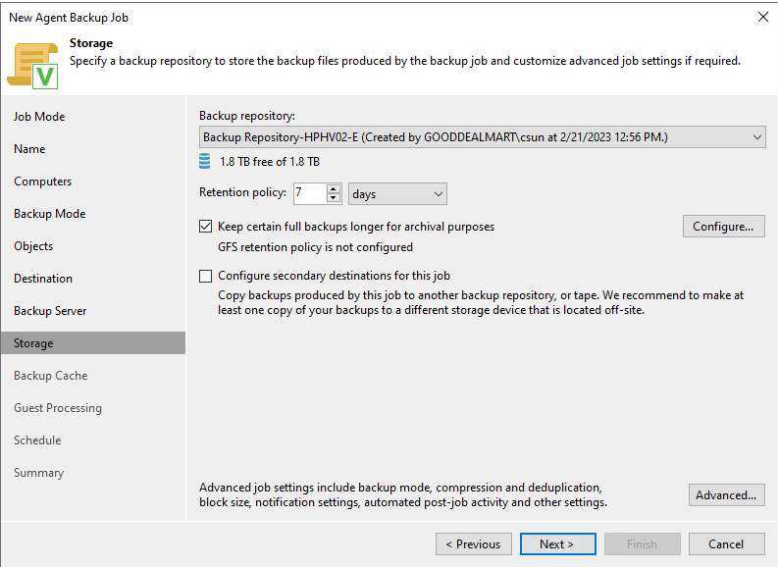
20. Select the backup repository from the Backup repository drop-down list on the Storage page.

The screenshot shows the 'New Agent Backup Job' wizard, specifically the 'Storage' step. The left sidebar lists the steps: Job Mode, Name, Computers, Backup Mode, Objects, Destination, Backup Server, Storage (selected), Backup Cache, Guest Processing, Schedule, and Summary. The main area is titled 'Storage' and contains the instruction 'Specify a backup repository to store the backup files produced by the backup job and customize advanced job settings if required.' Below this, there is a 'Backup repository:' dropdown menu showing 'Backup Repository-HPHV02-E (Created by GOODDEALMART\csun at 2/21/2023 12:56 PM.)'. Below the dropdown, it shows '1.8 TB free of 1.8 TB'. There is a 'Retention policy:' field set to '7' days. There are two checkboxes: 'Keep certain full backups longer for archival purposes' (unchecked) and 'Configure secondary destinations for this job' (unchecked). A note states: '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.' At the bottom, there are navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'. There is also an 'Advanced...' button.

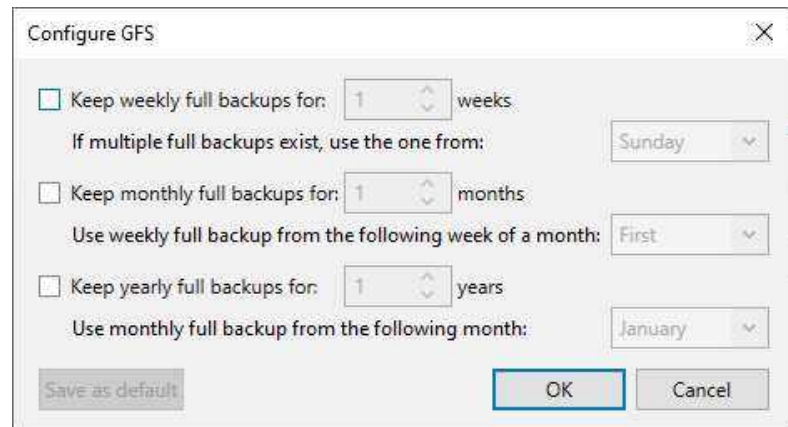
- 21. Set the retention policy settings for restore points in the Retention Policy field.
- 22. Select days or restore points from the drop-down list.



- 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.



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.

Job Mode

Name

Computers

Backup Mode

Objects

Storage

Guest Processing

Schedule

Summary

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 5 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.

Map backup

Configure...

Advanced...

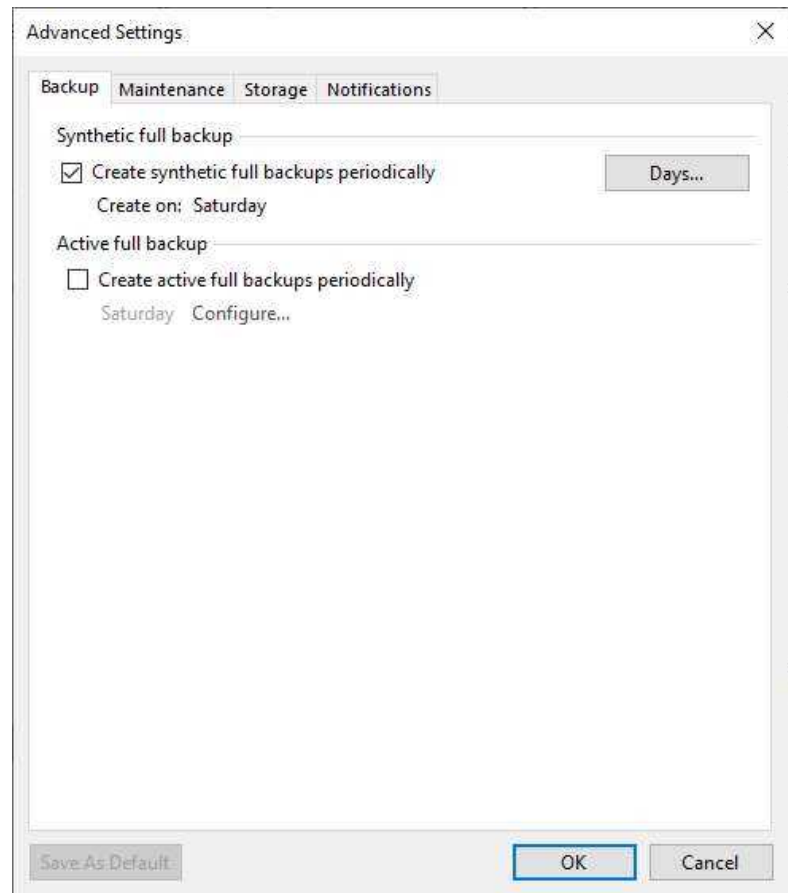
< Previous

Next >

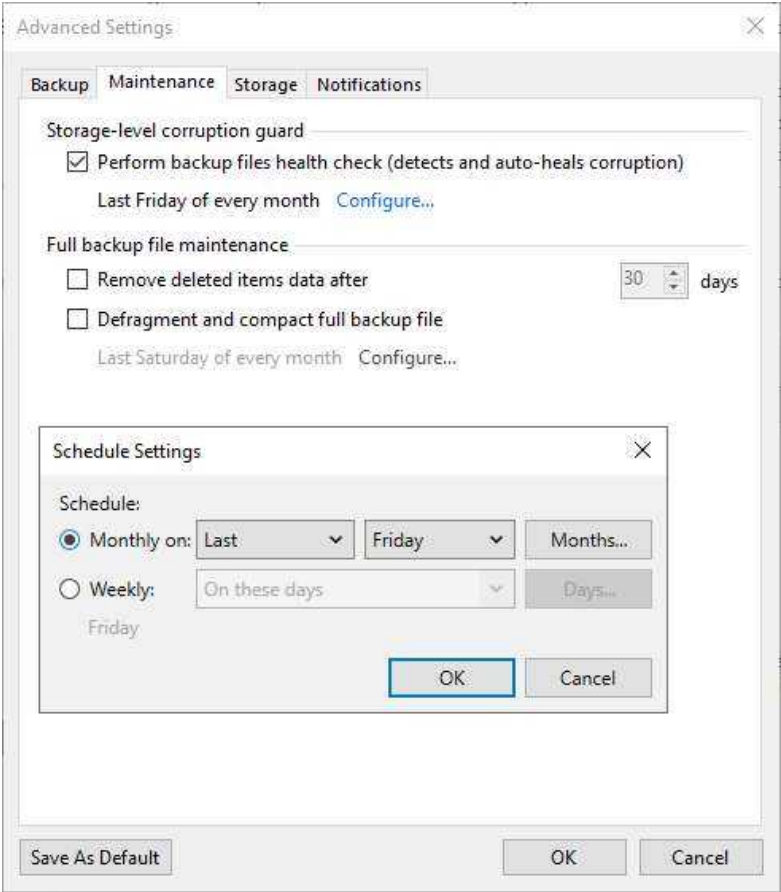
Finish

Cancel

30. Select Create synthetic full backups or Active full backups periodically checkbox.
31. Schedule full backups periodically and click OK.



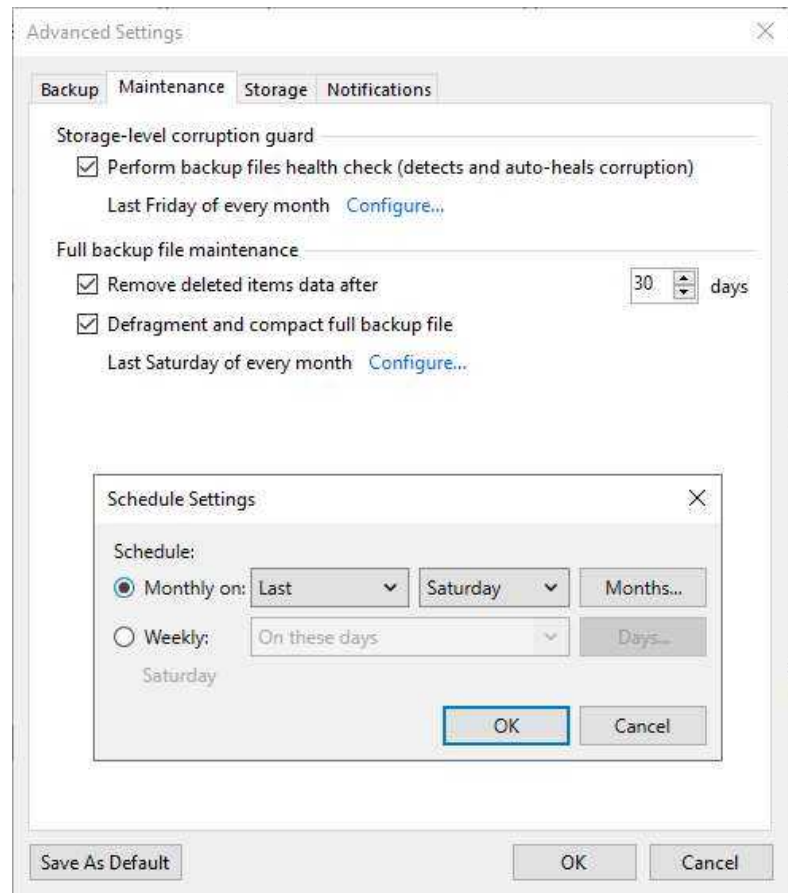
- 32. On the Advanced Settings, select Maintenance.
- 33. To regularly perform a health check on the backup chain's most recent restore point, select the Perform backup files health check (detects and auto-heals corruption) checkbox in the Storage-level corruption guard section.
- 34. Click Configure to set a schedule for the health check.



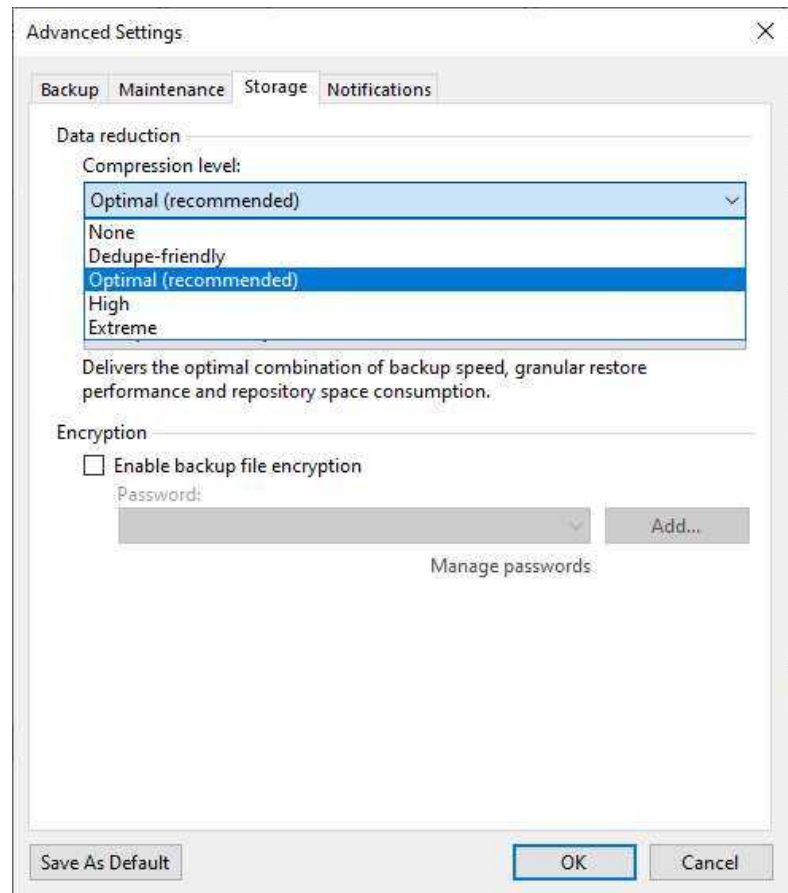
35. Select the Remove deleted items data after the checkbox and enter the few days you want backup data for deleted VMs to be kept.
36. Select the Defragment and compact full backup file checkbox and click Configure.
37. Set the schedule for the compact operation to compact a full backup periodically.

Note:

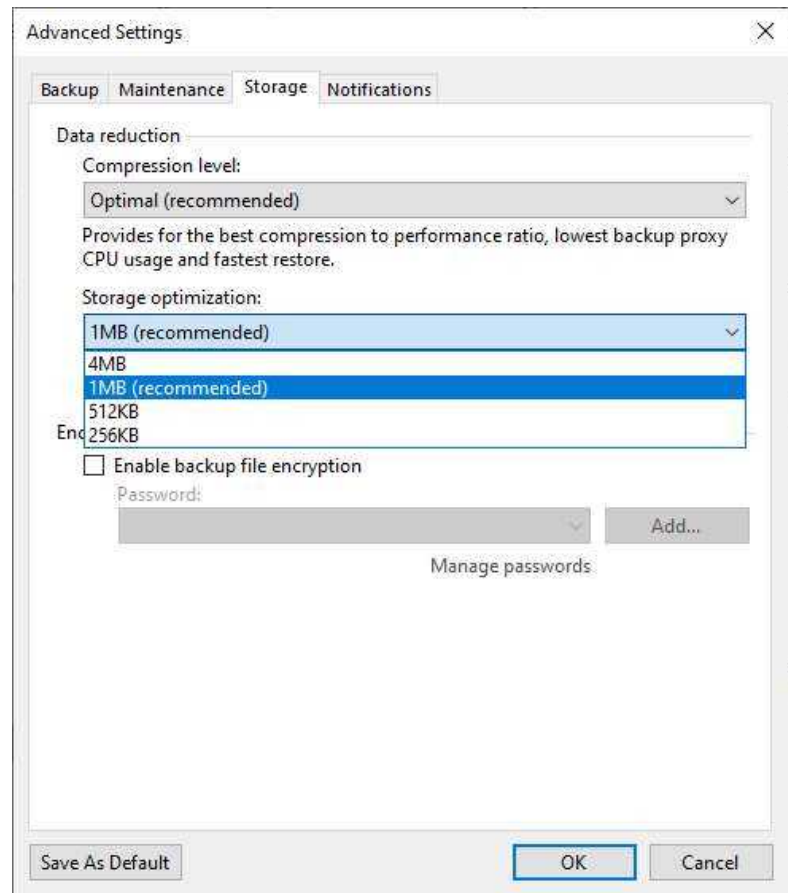
You don't need to enable the defragment and compact functionality checkbox if GFS retention is enabled.



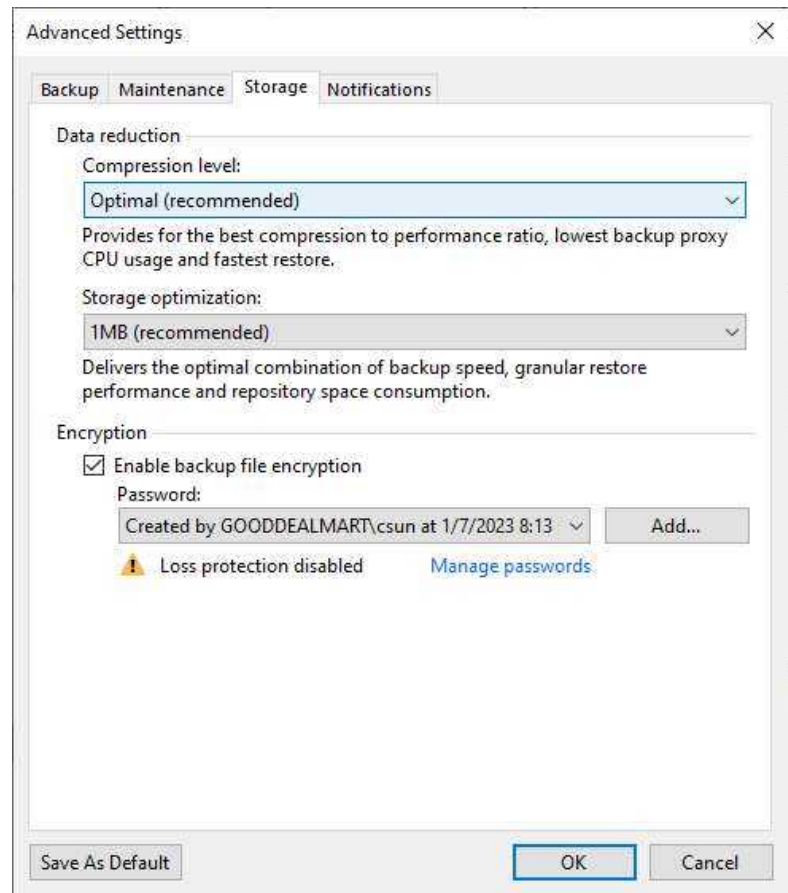
38. On Advanced Settings, select Storage.
39. Select the Compression level from the drop-down list.



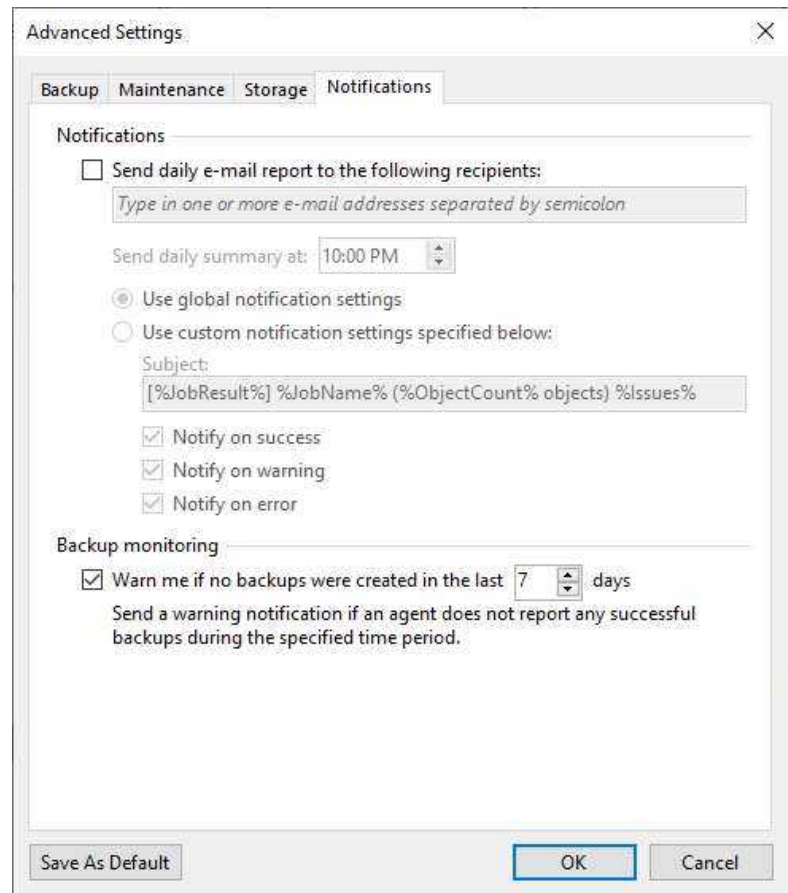
40. Select Storage optimization from the drop-down list.



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.



43. On the Advanced Settings, select No notifications.
44. Keep the default settings and click OK.



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.

Job Mode

Name

Computers

Backup Mode

Objects

Destination

Backup Server

Storage

Backup Cache

Guest Processing

Schedule

Summary

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.

< Previous Next > Finish Cancel

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.

Job Mode

Name

Computers

Backup Mode

Objects

Destination

Backup Server

Storage

Backup Cache

Guest Processing

Schedule

Summary

☐ 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.

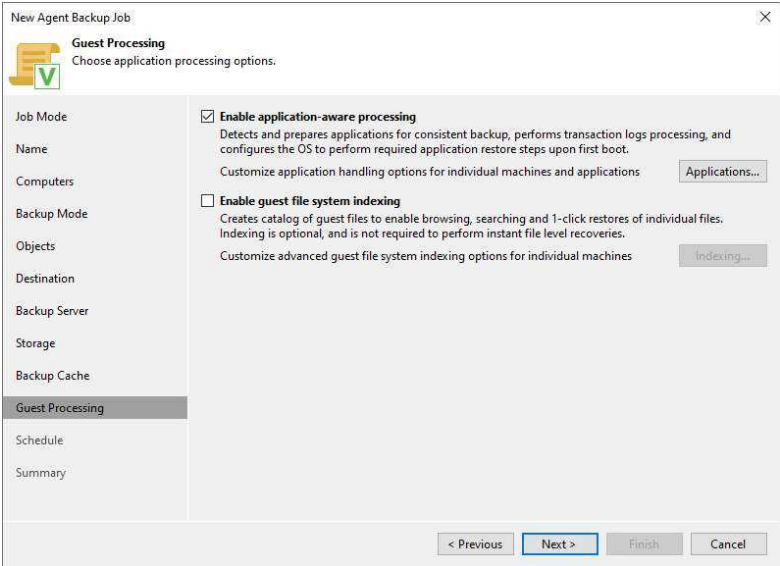
Maximum size: 10 GB

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:

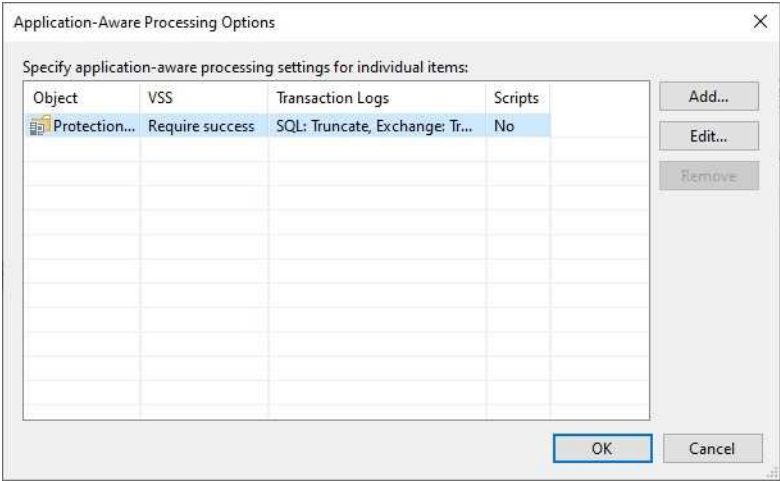
< Previous Next > Finish Cancel

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.

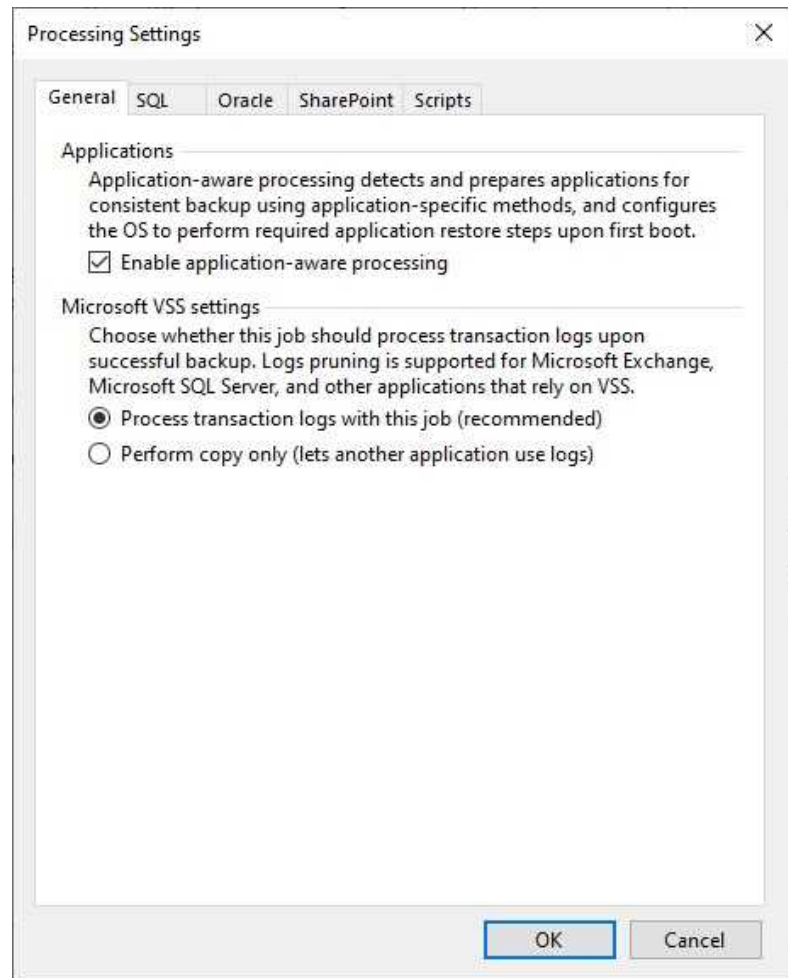
48. Select the Enable application-aware processing checkbox on the Guest Processing page, and click Applications.



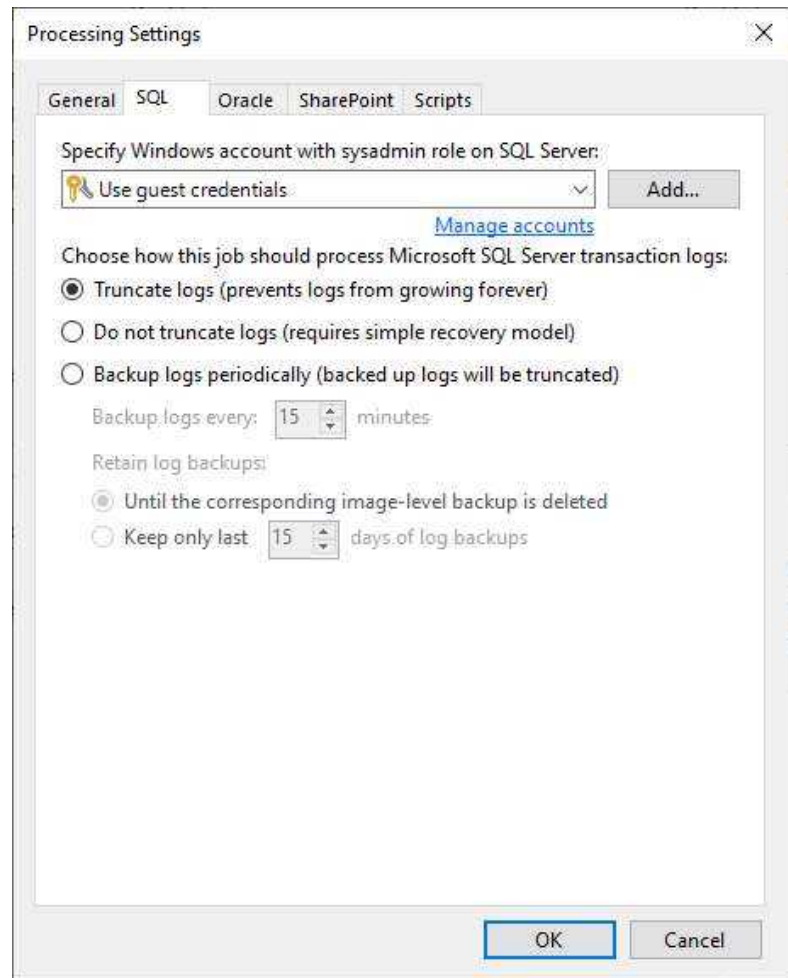
49. On the Application-Aware Processing Options page, select the Object and click Edit.



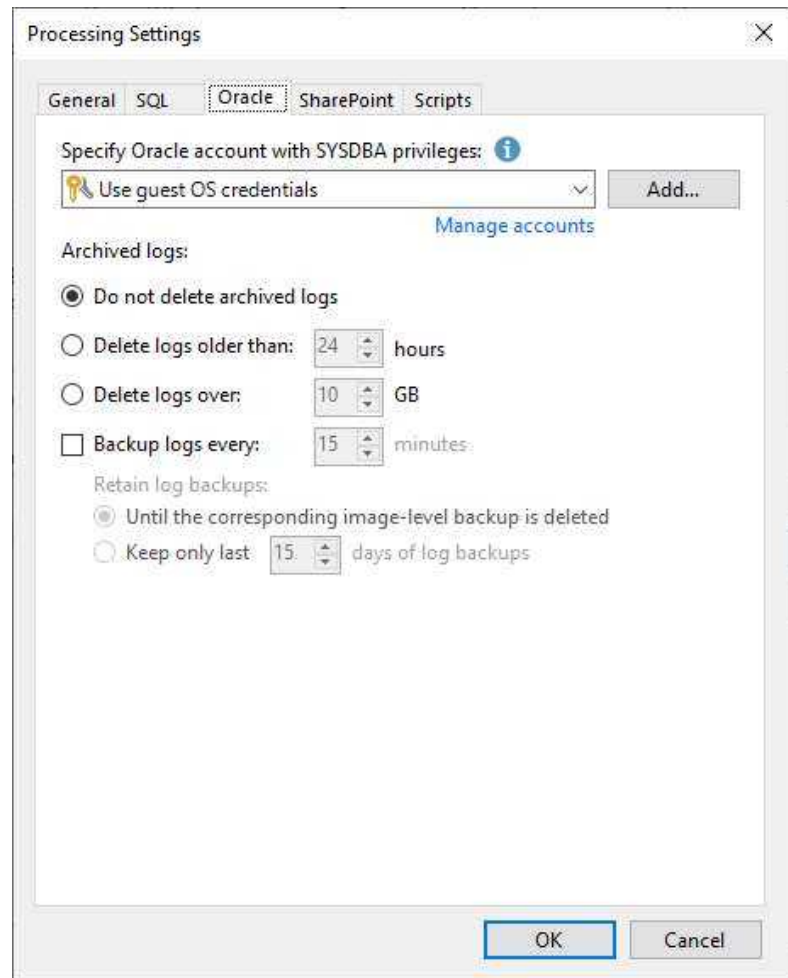
50. On the Processing Settings page, select General.
51. Select Enable application-aware processing checkbox.
52. Select Process transaction logs with this job (recommended).



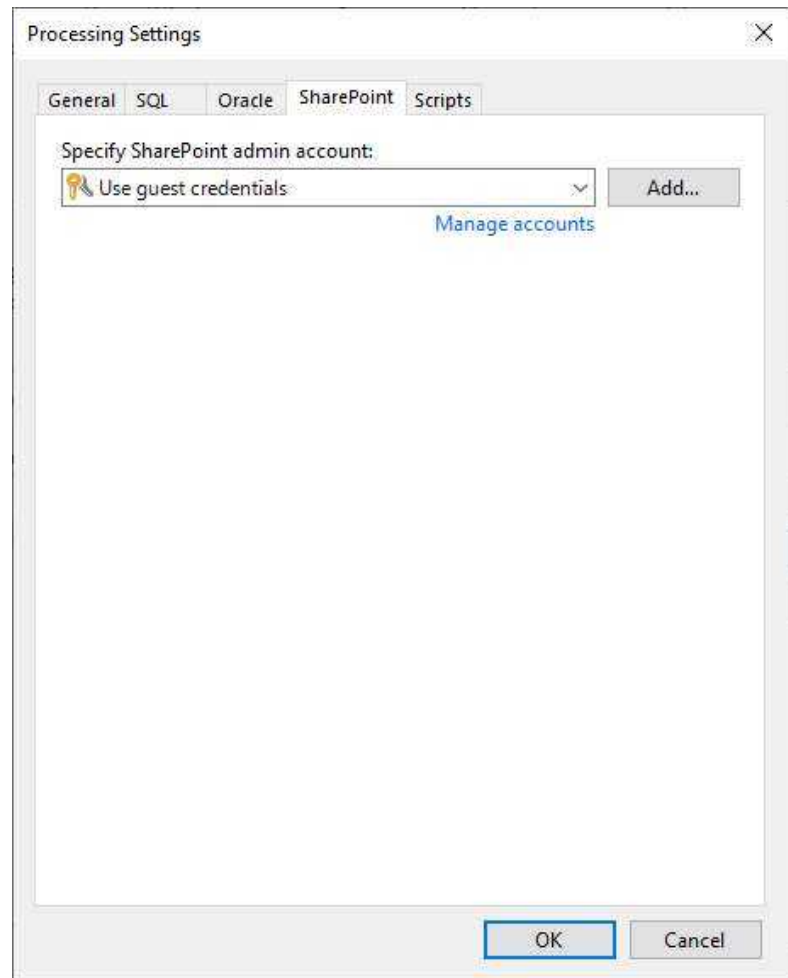
53. On the Processing Settings page, click SQL if the Physical Machine is a Microsoft SQL Server.
54. Select a user account from the drop-down list.
55. Select Truncate logs (Prevents logs from growing forever).



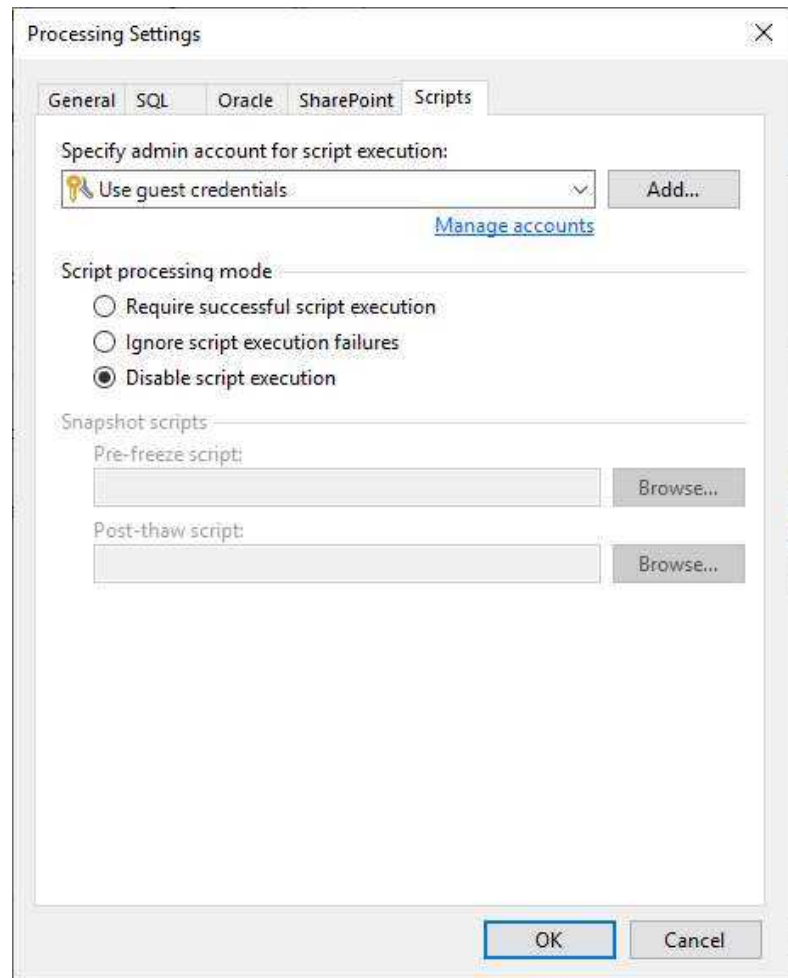
56. Select Oracle on the Processing Settings page if the Physical Machine is an Oracle Server.
57. Select a user account from the drop-down list.
58. Select Do not delete archived logs.



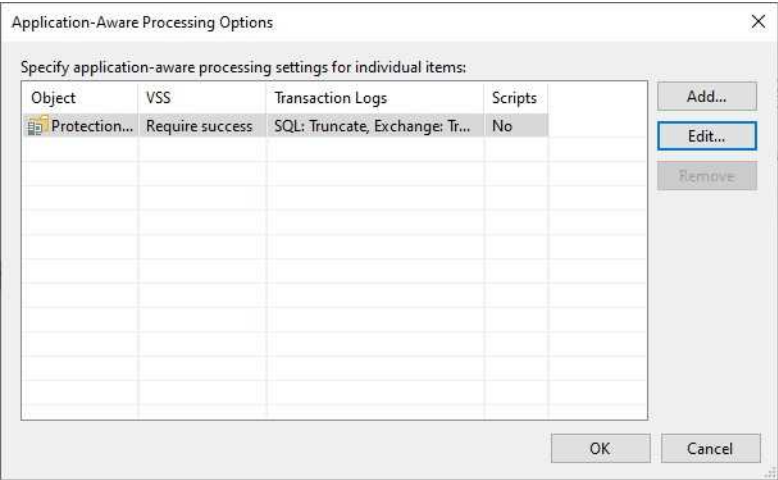
59. On the Processing Settings page, select SharePoint if the Physical Machine is a SharePoint Server.
60. Select a user account from the drop-down list.



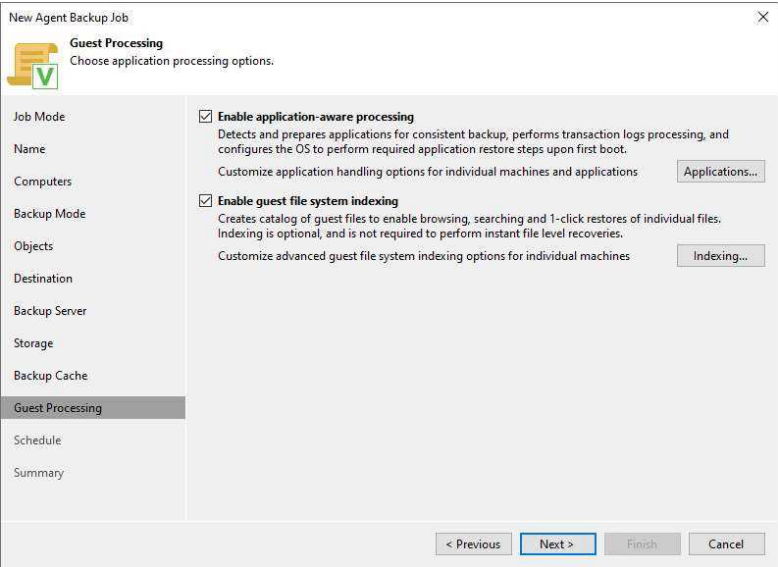
61. On the Processing Settings page, select Scripts.
62. Keep the default settings and click OK.



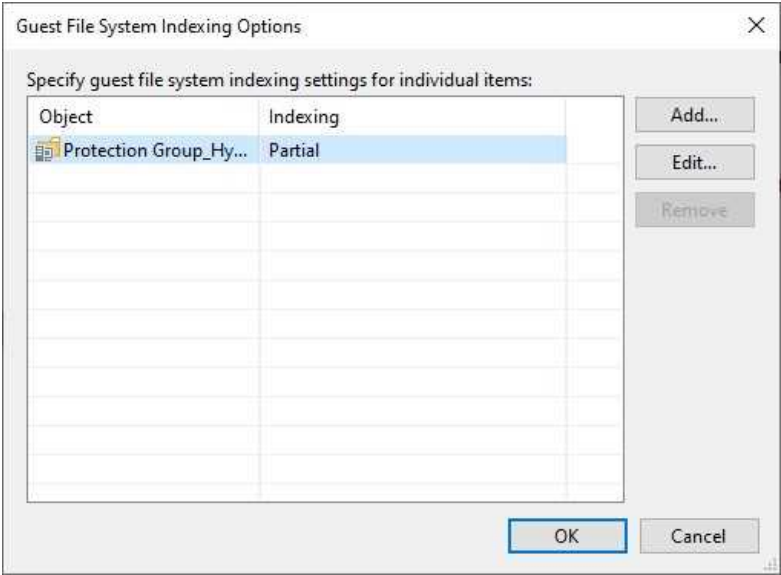
63. On the Application-Aware Processing Options page, click OK.



64. Select the Enable guest file system indexing checkbox and click Indexing.

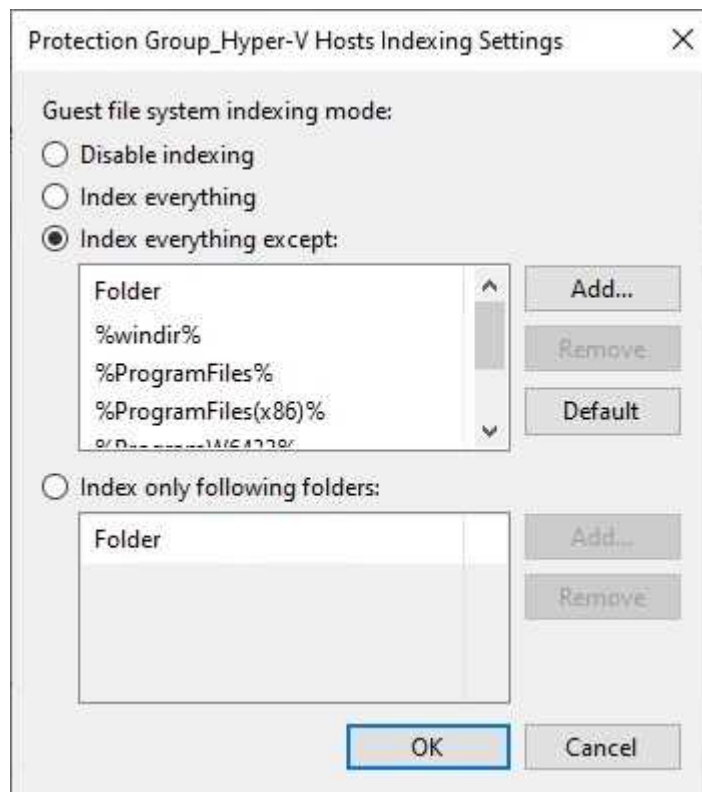


65. On the Guest File System Indexing Options page, select the Object, click Edit and.

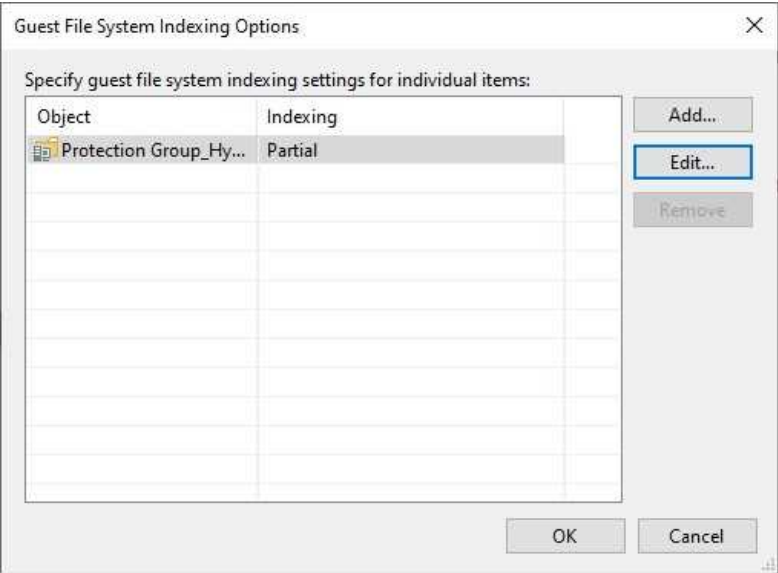


66. On the Guest file system indexing mode page, keep the default settings.

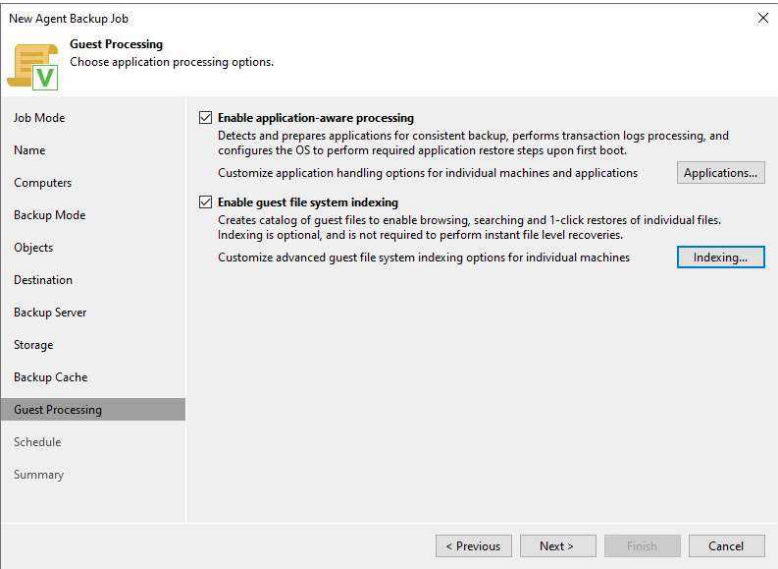
67. Click OK.



68. On the Guest File System Indexing Options page, click OK.



69. On the Guest Processing page, click Next.



70. Select Run the job automatically checkbox on the Schedule page and select your specified schedule.

71. Define whether Veeam Backup & Replica 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.

The screenshot shows the 'New Agent Backup Job' dialog box with the 'Schedule' tab selected. The 'Run the job automatically' checkbox is checked. The schedule is set to 'Daily at this time: 10:00 PM' on 'Everyday'. The 'Automatic retry' section has 'Retry failed items processing' set to 3 times and 'Wait before each retry attempt for' set to 10 minutes. The 'Backup window' section has 'Terminate job outside of the backup window' checked, with a note: 'Prevent long-running or accidentally started job from impacting your production infrastructure during the busy hours.' A 'Window...' button is visible next to the note. The 'Summary' tab is also visible at the bottom.

New Agent Backup Job

Schedule
Specify the scheduling options. If you do not set the schedule, the job will need to be controlled manually.

Job Mode

☒ 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...

Automatic retry

☒ Retry failed items processing: 3 times

Wait before each retry attempt for: 10 minutes

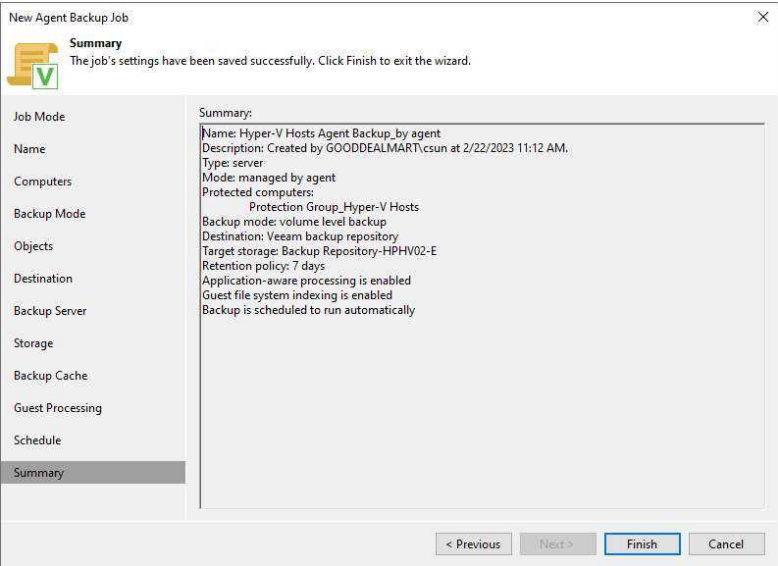
Backup window

☒ Terminate job outside of the backup window

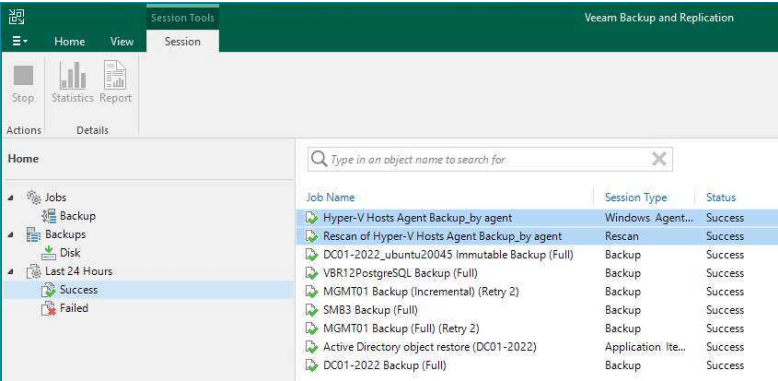
Prevent long-running or accidentally started job from impacting your production infrastructure during the busy hours. [Window...](#)

< Previous Apply Finish Cancel

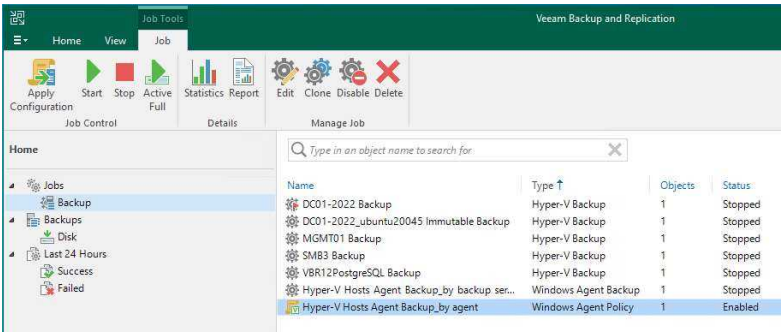
74. On the Summary page, click Finish.



75. Verify that the Machine rescan and Job configured are completed without issues.

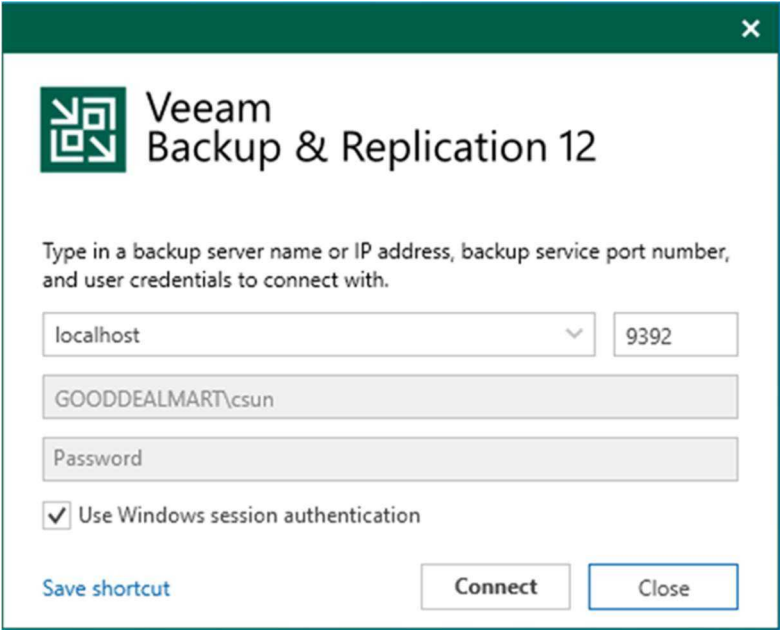


76. Verify that the backup job has been added

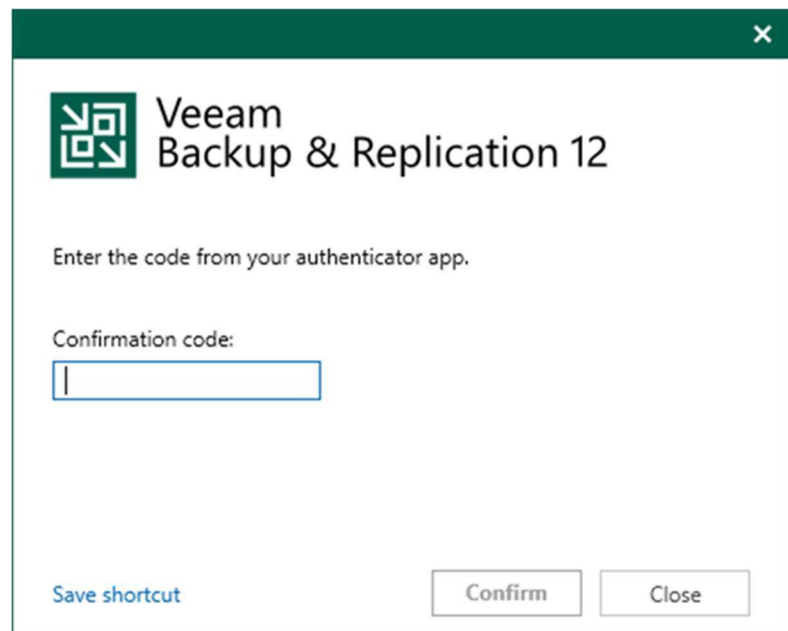


Create a Backup job to backup all VMS of the Hyper-V Host

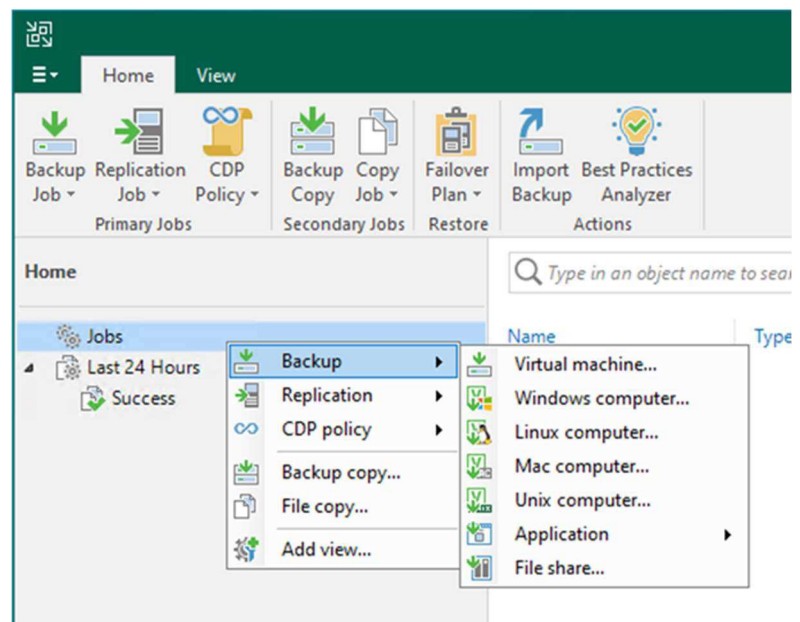
This procedure creates a backup job to back up all VMS of the product on Hyper-V host. The new VMS will be backed up automatically after the backup job is created. You don't need to modify the backup job settings.

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.	 The screenshot shows the Veeam Backup & Replication 12 console window. It has a dark green title bar with a close button. The main area is white with the Veeam logo and title. Below the title, there is a prompt: "Type in a backup server name or IP address, backup service port number, and user credentials to connect with." There are four input fields: a dropdown menu showing "localhost", a text box with "9392", a text box with "GOODDEALMART\csun", and a password field labeled "Password". Below these fields is a checkbox labeled "Use Windows session authentication" which is checked. At the bottom, there are three buttons: "Save shortcut" (blue text), "Connect" (white button), and "Close" (white button).

3. Enter the MFA Confirmation code and click Confirm.



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

Virtual Machines

Storage

Guest Processing

Schedule

Summary

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.

< Previous

Next >

Finish

Cancel

- 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.

Name

Virtual Machines

Storage

Guest Processing

Schedule

Summary

Virtual machines to backup:

Name	Type	Size
------	------	------

Add...

Remove

Exclusions...

Up

Down

Recalculate

Total size: 0 B

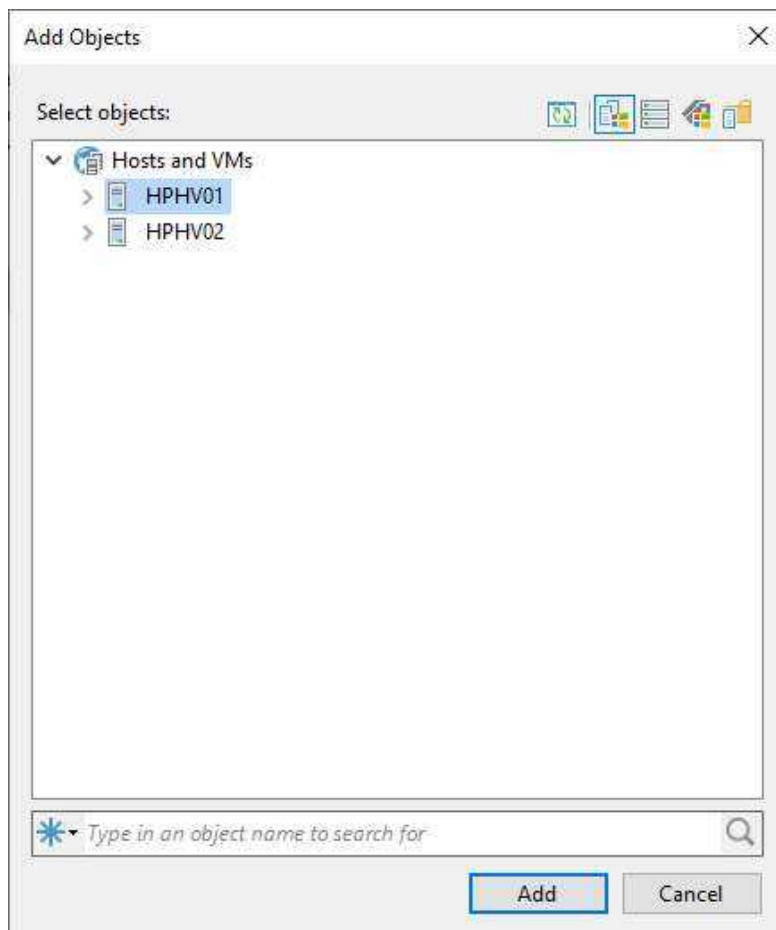
< Previous

Next >

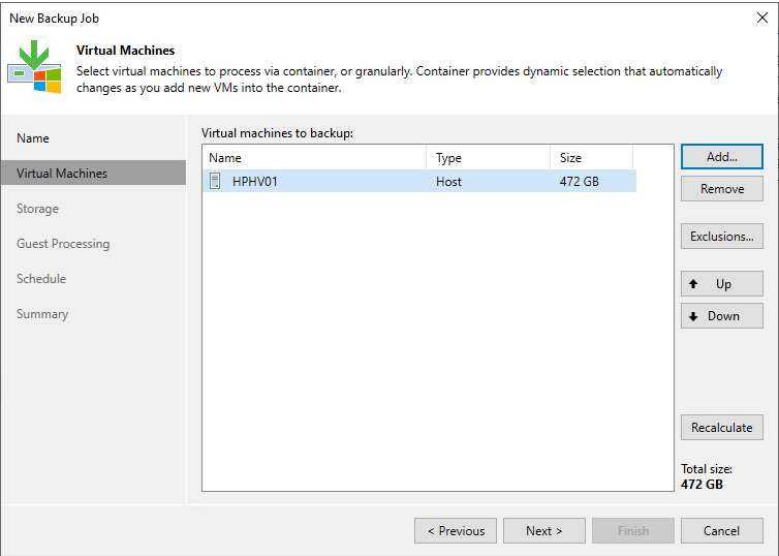
Finish

Cancel

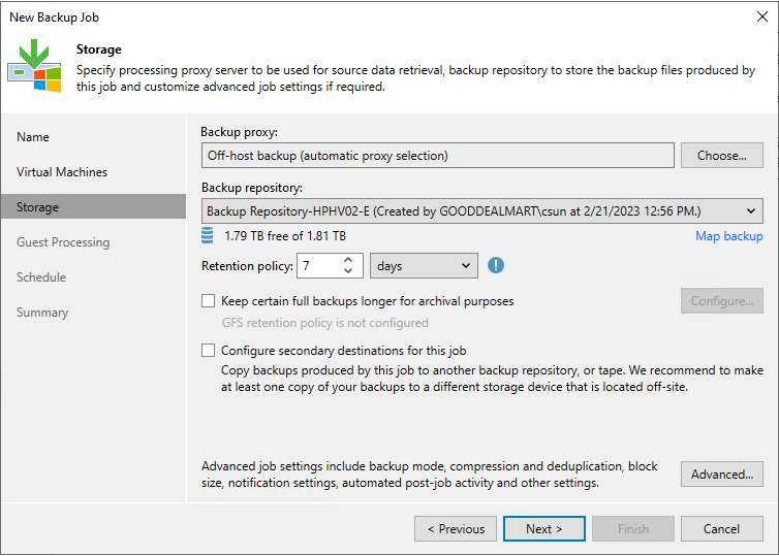
11. Select the Host from the Select objects list on the Add Objects page and click Add.
12. If you have multiple Hosts that need to back up in the same backup job, you can repeat the step to add them.



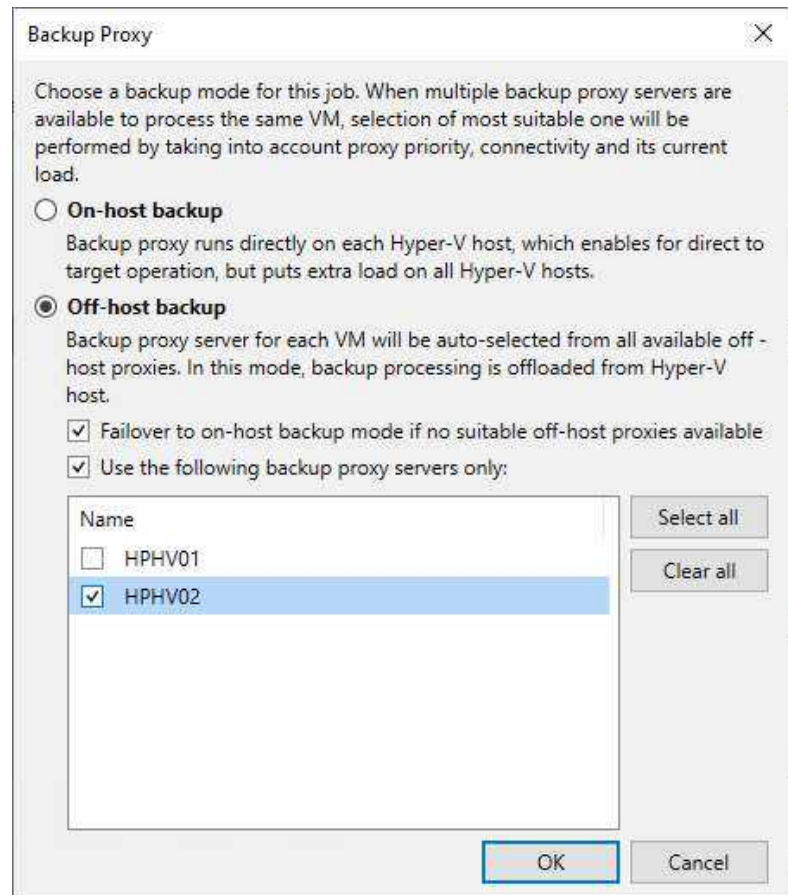
13. Click Next on the Virtual Machines page.



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) or use the default Off-host backup (automatic proxy selection) setting.



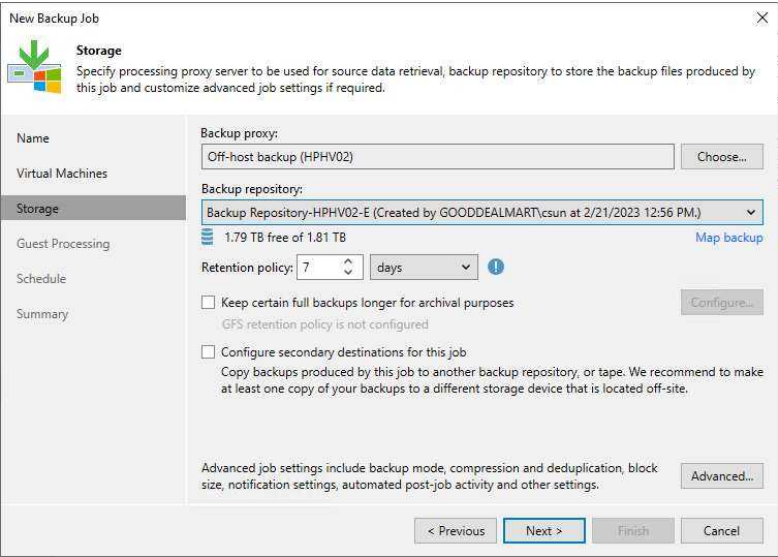
15. On the Backup Proxy page, if you select On-host backup mode, the source Microsoft HyperV host will serve as both the source host and the backup proxy. In this mode, Veeam Data Mover runs directly on the source host, which speeds up data retrieval but places additional strain on the host.
16. If you 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 & Replica will transition to on-host backup mode.
18. You unselect the Failover to on-host backup mode if no suitable off-host



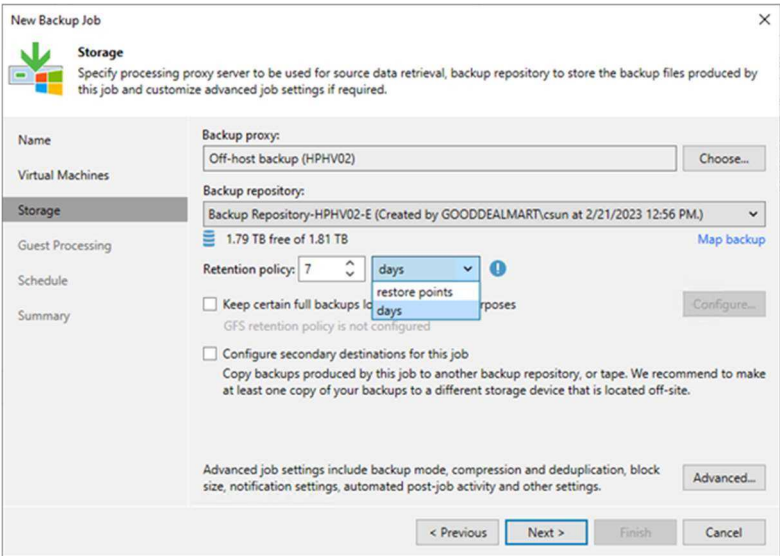
proxies are available in the checkbox. Still, the job will fail to start if off-host backup proxies are unavailable or configured properly.

19. Click OK.

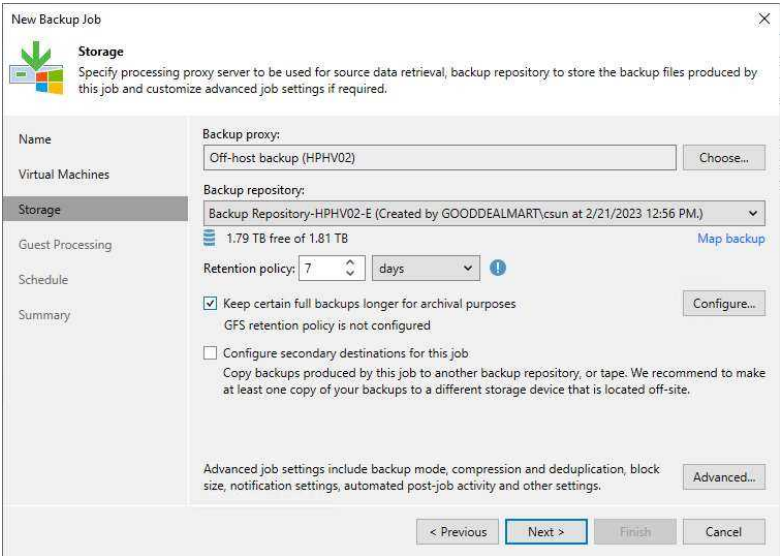
20. Select the backup repository from the Backup repository drop-down list where the created backup files must be saved.



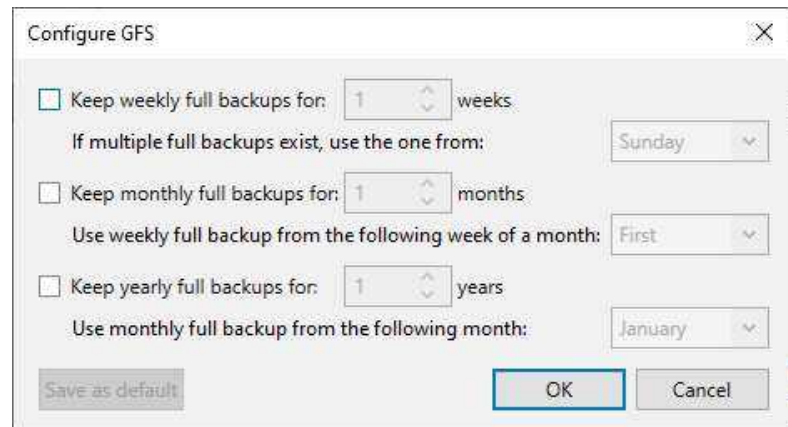
- 21. Set the retention policy settings for restore points in the Retention Policy field.
- 22. Select days or restore points from the drop-down list.



- 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'.



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 Backup Job

Storage

Virtual Machines

Guest Processing

Schedule

Summary

Backup proxy:

Off-host backup (HPHV02)

Choose...

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

Map backup

Retention policy:

7

days

Keep certain full backups longer for archival purposes

Configure...

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.

Advanced...

< Previous

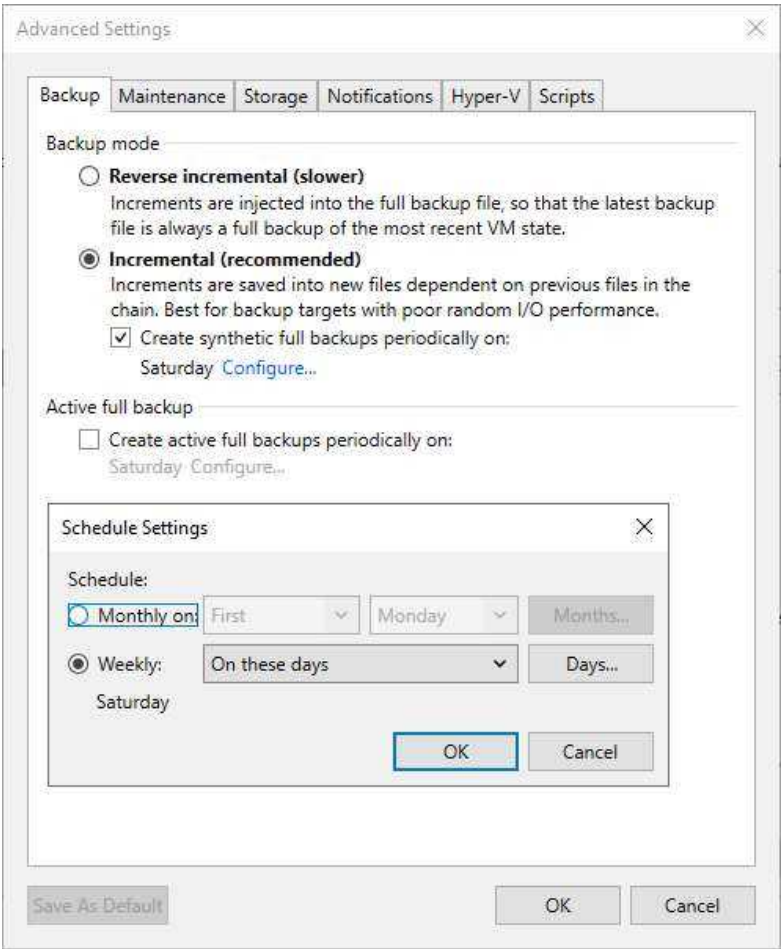
Next >

Finish

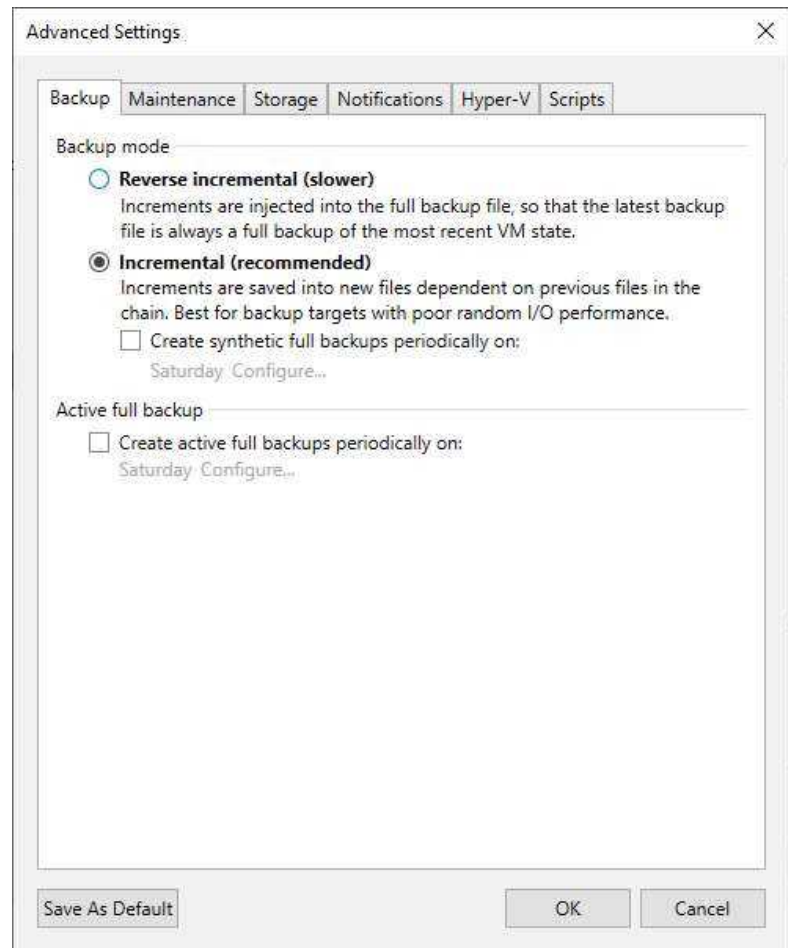
Cancel

515

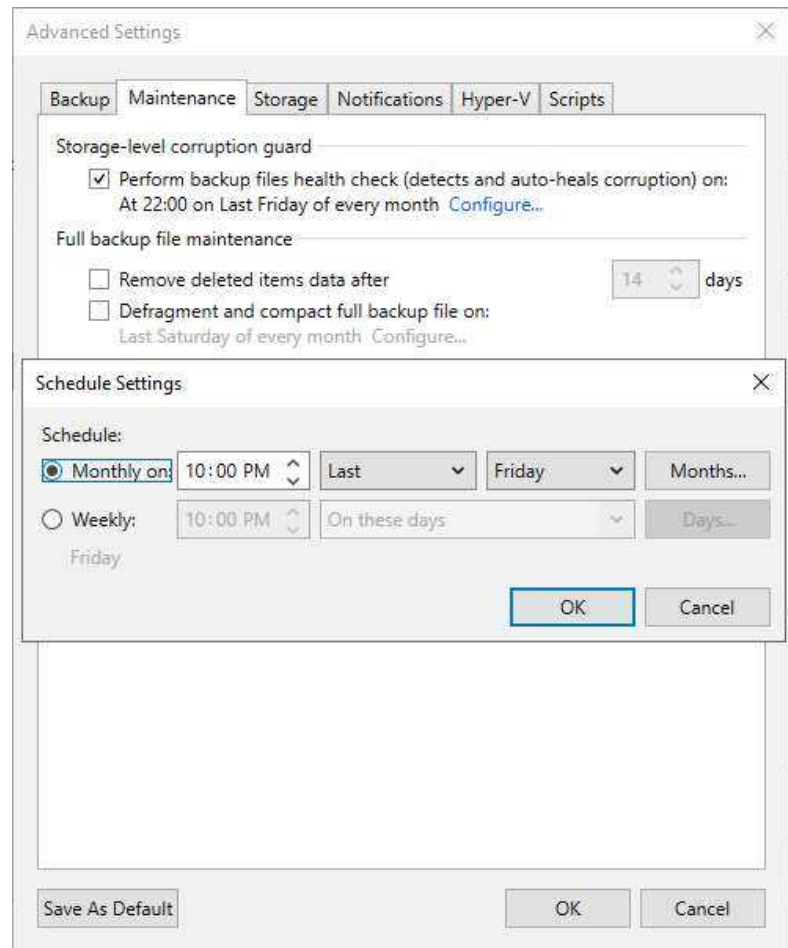
- 30. On the Backup page, select Incremental (recommended).
- 31. Select create synthetic full backups periodically or active full backups periodically checkbox.
- 32. Click Configure to schedule full backups periodically and click OK.



33. Select Incremental and disable synthetic full and active full backups to create a forever forward incremental backup chain.



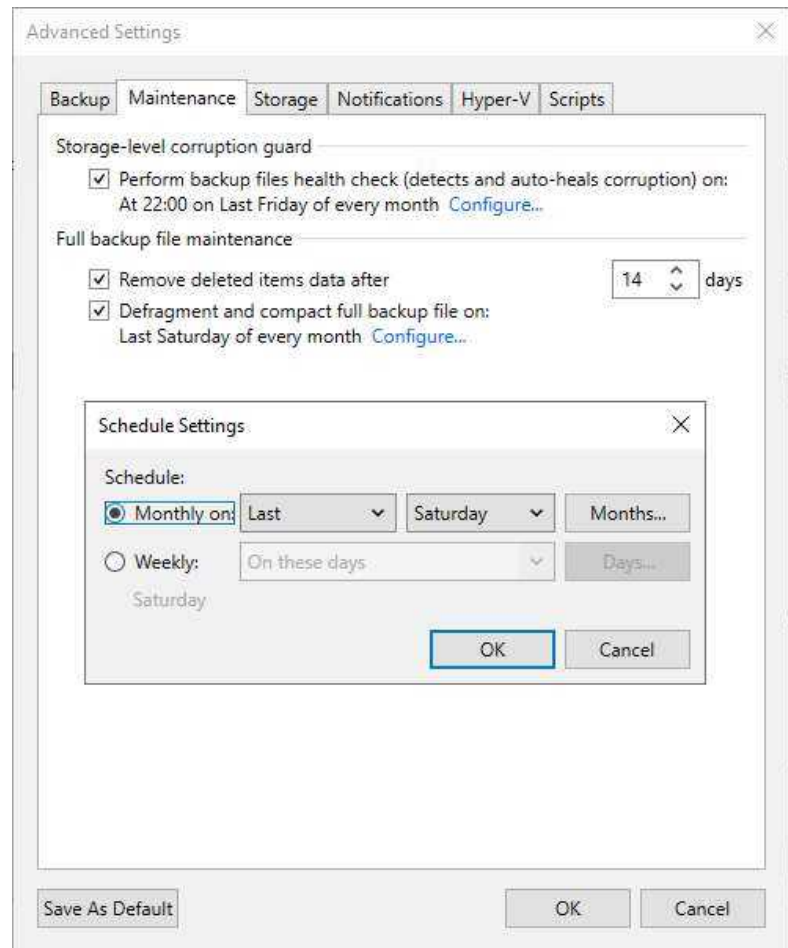
34. On the Advanced Settings, Maintenance.
35. To regularly perform a health check on the backup chain's most recent restore point, select the Perform backup files health check (detects and auto-heals corruption) checkbox in the Storage-level corruption guard section.
36. Click Configure to set a timetable for the health check.



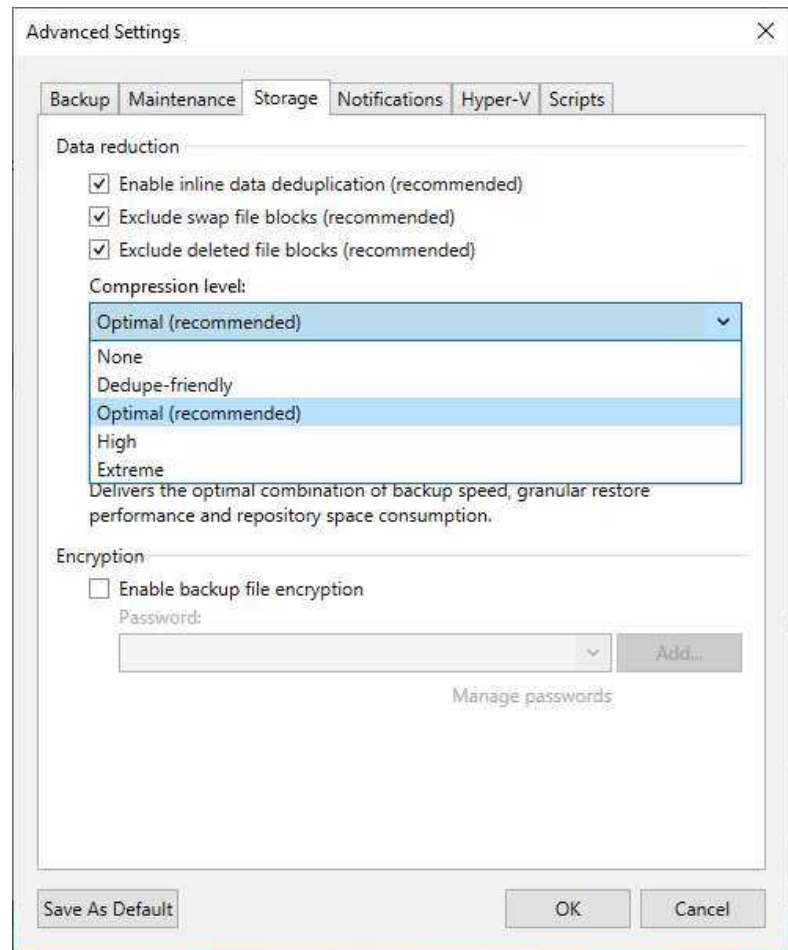
37. Select the Remove deleted items data after the checkbox and enter the few days you want backup data for deleted VMs to be kept.
38. Select the Defragment and compact full backup file checkbox and click Configure.
39. Set the schedule for the compact operation to compact a full backup periodically.

Note:

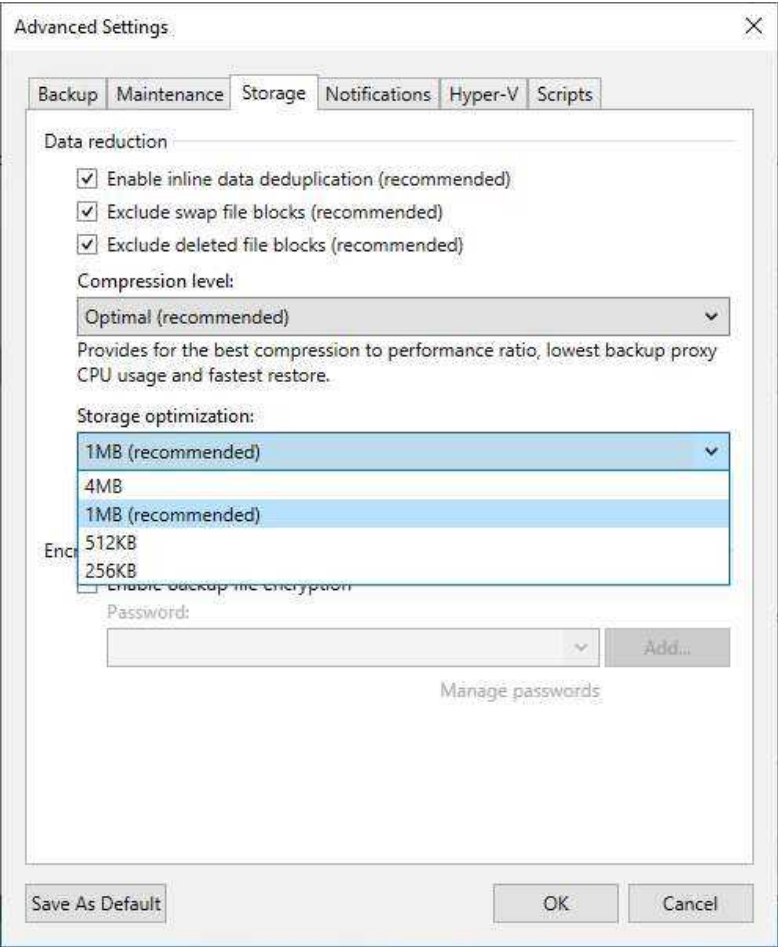
GFS retention is not compatible with defragment and compact functionality.



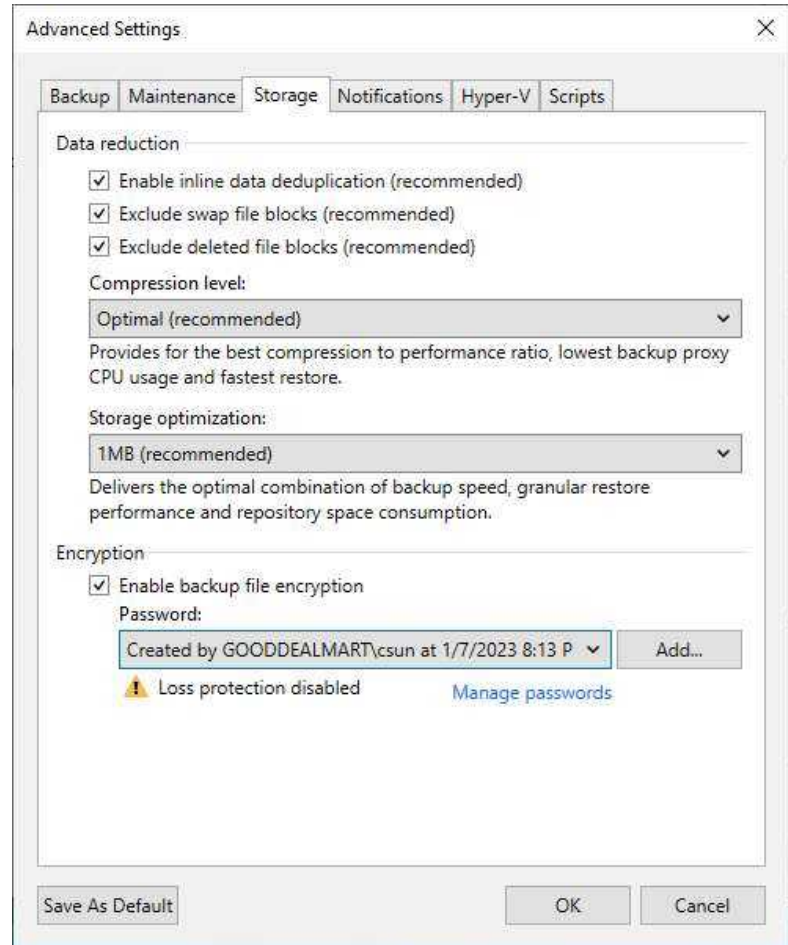
40. On Advanced Settings, select Storage.
41. Select the Enable inline data deduplication (recommended) checkbox.
42. Select the Exclude swap file blocks (recommended) checkbox.
43. Select the Exclude deleted file blocks (recommended) checkbox.
44. Select the compression level for the backup from the drop-down list.



45. Select the Storage optimization for the backup from the drop-down list.

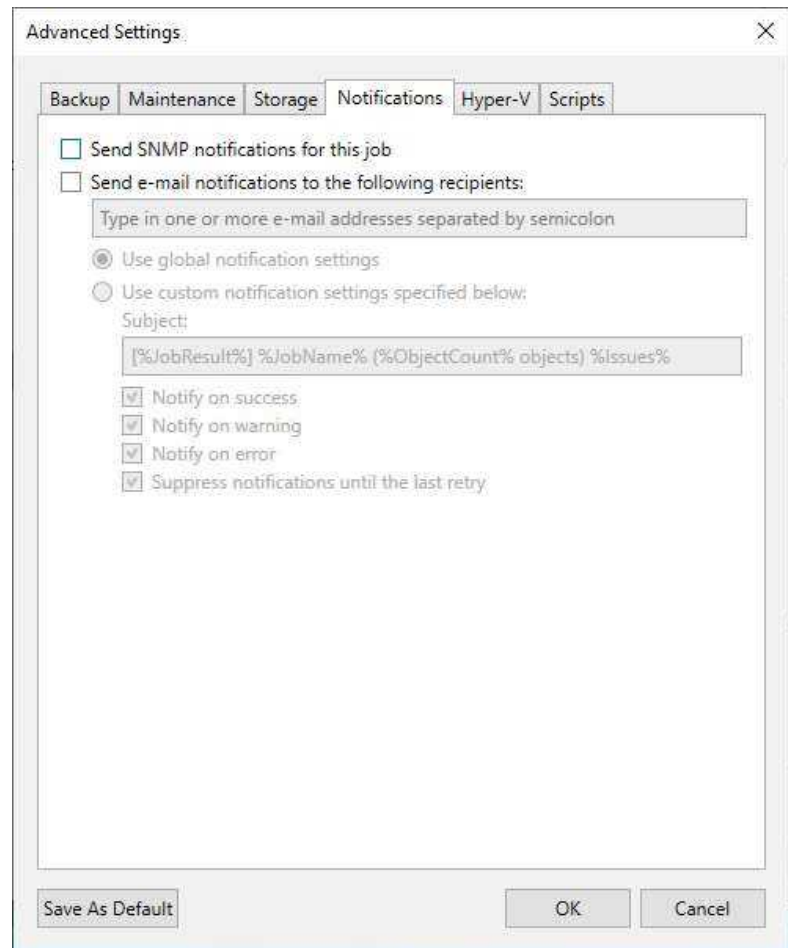


46. Select the Enable backup file encryption checkbox to encrypt the content of backup files.
47. Select a password from the drop-down list. Then, if you still need to do, click Add or use the Manage passwords link to create a new password.



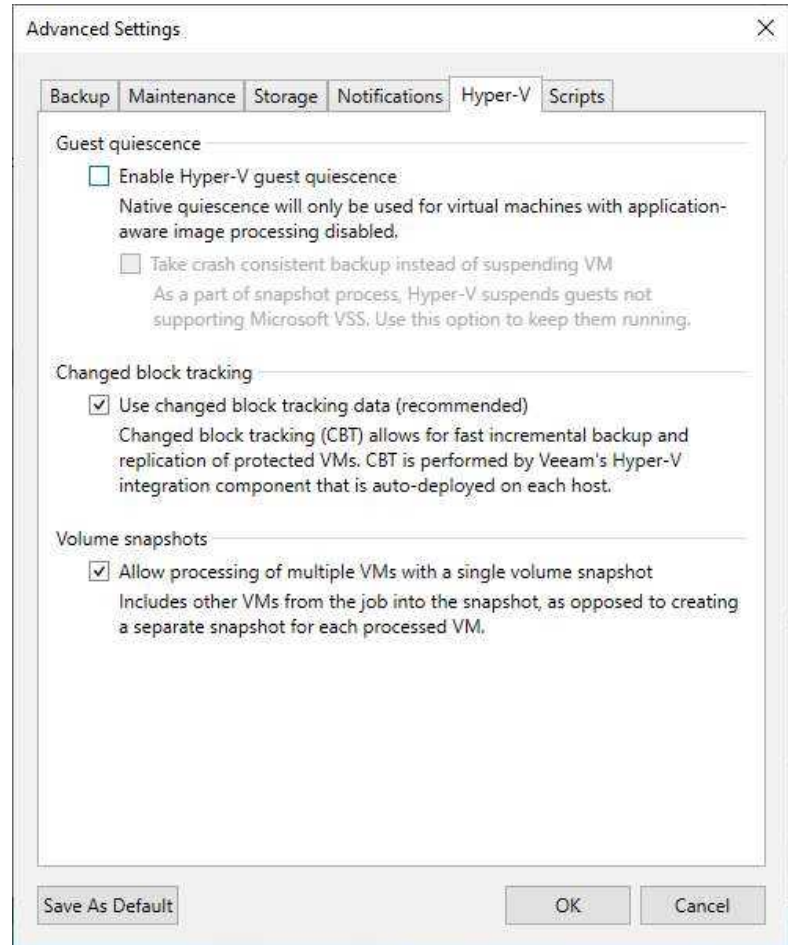
48. On the Advanced Settings, select No notifications.

49. Keep the default settings.



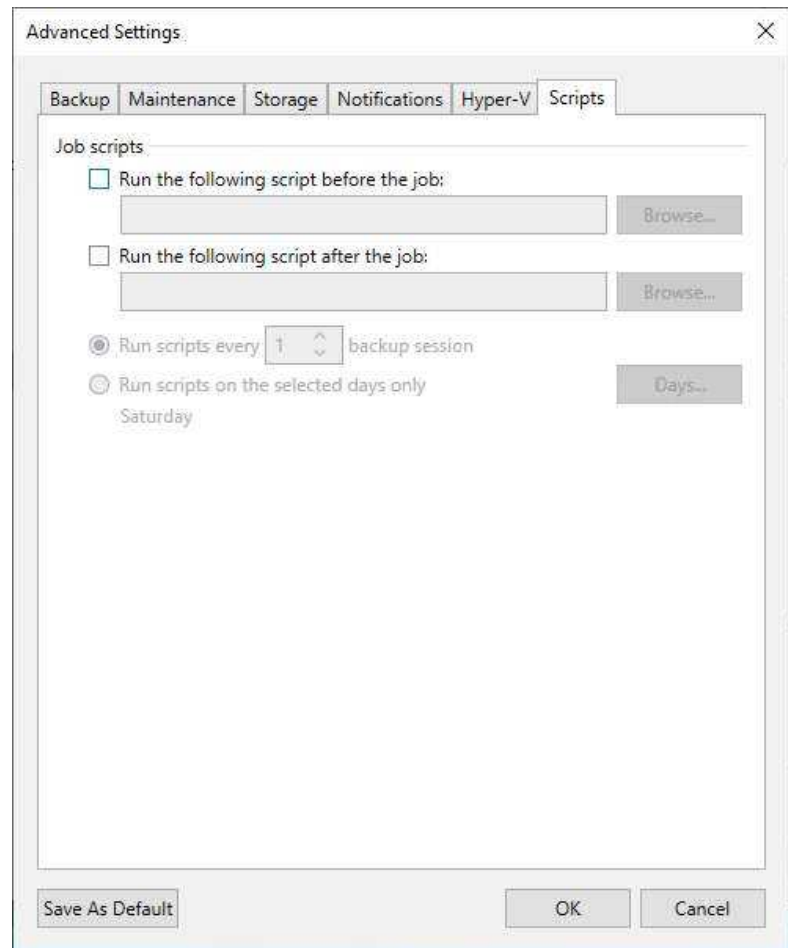
50. On the Advanced Settings, select Hyper-V.

51. Keep the default settings.



52. On the Advanced Settings page, click Scripts and keep the default settings.

53. Click OK.



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.

Name
Virtual Machines
Storage
Guest Processing
Schedule
Summary

Backup proxy:
Off-host backup (HPHV02) Choose...

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 Map backup

Retention policy: 7 days

☐ Keep certain full backups longer for archival purposes
Periodic fulls are not enabled in Advanced settings. Configure...

☐ 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. Advanced...

< Previous Next > Finish Cancel

55. Click Next on the Guest Processing page.

New Backup Job

Guest Processing
Choose guest OS processing options available for running VMs.

Name
Virtual Machines
Storage
Guest Processing
Schedule
Summary

☐ 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 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 Indexing...

Guest interaction proxy:
Automatic selection Choose...

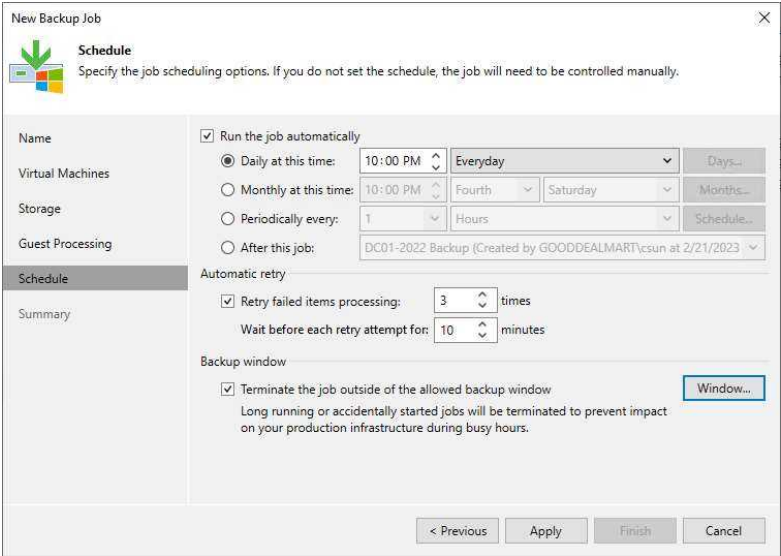
Guest OS credentials:
Select existing credentials or add new Add... Manage accounts

Customize guest OS credentials for individual machines and operating systems Credentials...

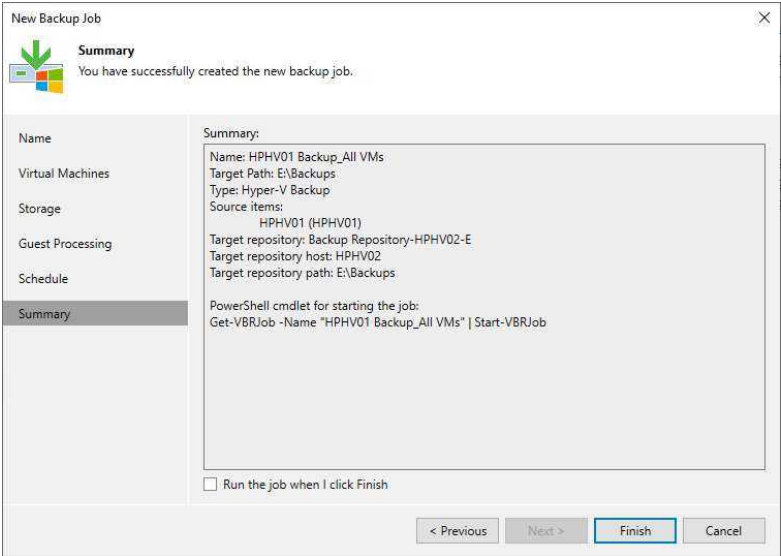
Verify network connectivity and credentials for each machine included in the job Test Now

< Previous Next > Finish Cancel

- 56. Select Run the job automatically checkbox on the Schedule page and select your specified schedule.
- 57. Define whether Veeam Backup & Replica 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.



60. Click Finish on the Summary page.



61. Verify that the backup job has been added.

