
Veeam Best Practise 9.5u4a

Release 1.0.0

Oct 18, 2019

1	Veeam Best Practice V9.5u4a	3
1.1	Introduction	3
1.1.1	About This Guide	3
1.1.2	Intended Audience	3
1.1.3	Authors	4
1.2	Contacting Veeam Software	4
1.2.1	Online Support	4
1.2.2	Customer Support	4
1.2.3	Company Contacts	5
1.3	DNS Resolution	5
1.3.1	Example <code>hosts</code> file	5
1.4	Backup Server	5
1.5	Deployment Method	6
1.5.1	Virtual deployment	6
1.5.2	Physical deployment	6
1.6	Backup Server Placement	6
1.6.1	Host and Storage Discovery	7
1.6.2	File-level Recovery Data Flow	8
1.6.3	Disaster Recovery Optimization	10
1.6.4	Examples	10
1.7	Sizing and System Requirements	12
1.7.1	Compute requirements	12
1.7.2	Operating system	12
1.7.3	Disk space	13
1.7.4	Other software	14
1.7.5	Installing Veeam Backup & Replication updates	14
1.8	Veeam Backup & Replication Database	15
1.8.1	SQL Server Edition	15
1.8.2	Database Placement	15
1.8.3	Sizing	16
1.8.4	SQL Server Configuration Tips	16
1.8.5	Modifying Database Connection Settings	16
1.8.6	Migrating Veeam Database	17
1.9	Protecting Veeam Backup & Replication Configuration	17
1.9.1	Protecting the Veeam Backup Server	17
1.9.2	Planning for Disaster Recovery of Veeam Backup Server	17

1.9.3	Antivirus on Veeam Servers	18
1.10	Veeam Backup Enterprise Manager	19
1.10.1	Whether to Deploy?	19
1.10.2	Using Enterprise Manager for Restore Operations	19
1.10.3	RESTful API Service	21
1.11	Veeam vCloud Director Self-Service Portal	21
1.11.1	Requirements and limits	21
1.11.2	File Level Restore for Windows VMs	22
1.11.3	File Level Restore for Linux VMs	23
1.11.4	Multiple concurrent restores	27
1.12	Indexing	29
1.12.1	Indexing and Search Overview	29
1.12.2	When to Use Indexing?	30
1.12.3	How Veeam Indexing Works	30
1.12.4	Temporary VM Disk Usage	30
1.12.5	Sizing Enterprise Manager Catalog	31
1.12.6	Recommended Settings	31
1.12.7	Using Veeam Backup Search (Optional Component)	32
1.13	Proxy Servers - Intro	32
1.13.1	Intelligent Load Balancing	33
1.13.2	Parallel Processing	34
1.13.3	Backup Proxy Services and Components	34
1.14	Proxy Server - VMware vSphere	34
1.14.1	Storage optimizations	34
1.14.2	Veeam Advanced Data Fetcher (ADF)	35
1.14.3	Intelligent Load Balancing	35
1.15	Transport Modes	35
1.15.1	Direct Storage Access	35
1.15.2	Virtual appliance mode	36
1.15.3	Network mode	36
1.16	Direct Storage Access	36
1.16.1	Pros	37
1.16.2	Cons	37
1.16.3	Example	37
1.16.4	Recommendations	37
1.16.5	Security Considerations for Direct SAN	38
1.16.6	Summary	39
1.17	Virtual Appliance Mode	39
1.17.1	Pros	39
1.17.2	Cons	40
1.17.3	Considerations and Limitations	40
1.17.4	vSphere 6.5 and Encryption	40
1.17.5	Recommendations	41
1.18	Network Mode	41
1.18.1	Pros	43
1.18.2	Cons	43
1.18.3	Recommendations	44
1.19	Backup from Storage Snapshots	44
1.19.1	How it works	45
1.19.2	Configuration	47
1.19.3	When to use	48
1.20	NetApp Data ONTAP	48
1.20.1	Backup from secondary snapshots	48
1.20.2	Snapshot Orchestration	49

1.21	Nimble Storage	51
1.21.1	Storage array configuration	51
1.21.2	Snapshot only jobs	52
1.21.3	Snapshot replication	52
1.21.4	Backup from secondary storage	53
1.22	Selecting a Transport Mode	54
1.22.1	Very small	54
1.22.2	Small and Medium	54
1.22.3	Large	55
1.22.4	Enterprise	55
1.23	Sizing a Backup Proxy	55
1.23.1	Processing Resources	56
1.23.2	Calculating required proxy tasks	56
1.23.3	How many VMs per job?	57
1.23.4	How Many Tasks per Proxy?	57
1.23.5	Considerations and Limitations	58
1.24	Proxy Server - Microsoft Hyper-V	58
1.24.1	On-host backup	59
1.24.2	Off-host backup	60
1.25	Proxy Server - Nutanix AHV	61
1.25.1	How It Works: Integration Details	62
1.26	Restoring VMs to an HPE 3PAR with thin disks	63
1.26.1	3PAR useful facts	63
1.26.2	Additional resources	64
1.27	Data DellEMC DataDomain Advanced Scalability Design	64
1.27.1	Gateway server role explained	64
1.27.2	DataDomain MTree	65
1.27.3	DataDomain replication overview	66
1.27.4	Veeam B&R Integration	67
1.27.5	Working with Veeam Agents	81
1.28	Backup Repository	83
1.28.1	The 3-2-1 rule	83
1.29	Repository Type	84
1.29.1	Server-Based Repository: DAS or SAN?	84
1.29.2	Windows or Linux?	85
1.29.3	Physical or Virtual?	85
1.29.4	NTFS or ReFS?	85
1.29.5	SMB Share	86
1.30	SMB Repository	87
1.30.1	Gateway Server	87
1.31	Deduplication Appliances	88
1.31.1	Overview	88
1.31.2	Using a Deduplication Appliance	88
1.31.3	Deduplication Appliance as a Primary Backup Repository	88
1.31.4	Using Deduplication Appliance as a Backup Copy Repository	89
1.31.5	Using Deduplication Appliance as a Virtual Tape Library	89
1.31.6	File-Level Recovery and Veeam Explorers	89
1.31.7	Best Practices	89
1.32	Deduplication integration specifics	90
1.32.1	EMC DataDomain	90
1.32.2	ExaGrid	93
1.32.3	HPE StoreOnce	94
1.33	Windows Server Deduplication	95
1.34	Object Storage Repository	95

1.34.1	Lifecycle Rules & Tiering	95
1.34.2	Manual Deletion	96
1.34.3	Security	96
1.34.4	Cost Considerations	96
1.35	Configuration Guidelines	96
1.35.1	Parallel Processing	96
1.35.2	General guidelines for virtual repositories	96
1.35.3	SOBR	97
1.35.4	Blocks sizes	97
1.35.5	File System Formats	98
1.35.6	Using “Large File” Switch for NTFS	98
1.35.7	Keeping File Size Under Control	98
1.35.8	Synthetic Backup and Caching	98
1.36	Repository Sizing	99
1.36.1	Estimating Repository Capacity	99
1.37	Per VM backup files	101
1.37.1	Maximum number of VMs per job	102
1.37.2	Performance	103
1.37.3	Deduplication	103
1.38	Scale Out Backup Repository	103
1.38.1	File placement policies	103
1.38.2	Scale-out Backup repository and network considerations	104
1.39	Capacity Tier	104
1.39.1	General	104
1.39.2	Block Size	105
1.40	WAN Acceleration	105
1.40.1	Determining Required Bandwidth	105
1.41	Analyzing Backup Job	105
1.42	Analyzing Backup Copy Job	106
1.43	Comparing Direct Mode with WAN Accelerated Mode	108
1.44	Backup Mode Effect	108
1.45	Configuration	108
1.45.1	Source WAN Accelerator	109
1.46	Sizing For Wan Acceleration	110
1.46.1	Hardware	110
1.46.2	Disk Size	111
1.46.3	VeeamWAN\GlobalCache\src	111
1.46.4	VeeamWAN\Digests	111
1.46.5	Target WAN Accelerator	112
1.47	Sizing Targets for One to One and One to Many relationships	114
1.47.1	Sizing for each scenario:	115
1.48	How Many WAN Accelerators to Deploy?	116
1.49	Is Wan Acceleration right for your environment?	116
1.49.1	Global Cache on Spinning Disk	116
1.50	Tape Support	117
1.50.1	Overview	117
1.50.2	Tape Device Connection	118
1.51	Tape Devices Deployment	120
1.51.1	Data Block Size	120
1.52	Media Management	121
1.52.1	Automated Drive Cleaning	122
1.52.2	Working with Tape Libraries	123
1.52.3	Media Information	123
1.52.4	Media Pool	124

1.52.5	Media Set	124
1.52.6	Media Vault	124
1.53	Backup Modes	125
1.54	Sizing	125
1.55	Using 3rd party tape software	126
1.56	Tape Encryption	126
1.57	Tips	126
1.58	Configuring Backup to tape	127
1.59	Tape Parallel Processing	127
1.59.1	Note: You cannot enable parallel processing for GFS media pools.	127
1.59.2	Processing Backup Chains Simultaneously	128
1.60	Virtual Full Backups	128
1.60.1	Prioritising Tape backups over Primary backups	128
1.61	File Backup to Tape	128
1.61.1	Note: If the file to tape job fails to complete in 3 weeks, it is terminated by timeout.	129
1.61.2	VM Backup to Tape	129
1.61.3	Backup Repositories as Source	130
1.61.4	Linking Primary Jobs	130
1.62	Restores	130
1.62.1	VM Restore from Tape to Infrastructure	130
1.63	Veeam Explorers	131
1.63.1	Explorer for Storage Snapshots	131
1.64	Interaction with vSphere	132
1.64.1	vCenter Server	132
1.64.2	Impact of Snapshot Operations	133
1.64.3	How to Mitigate?	135
1.64.4	Considerations for NFS Datastores	136
1.64.5	Snapshot Hunter	137
1.64.6	Storage Latency Control	137
1.64.7	vCenter Server Connection Count	139
1.64.8	Veeam Infrastructure cache	140
1.64.9	Security	142
1.65	Hyper-V backup modes	142
1.65.1	Limiting the impact of On-Host backup mode on the production infrastructure	143
1.66	Change block tracking on Hyper-V	143
1.66.1	Microsoft Resilient Change Tracking in Hyper-V 2016	143
1.66.2	Change block tracking on third party SMB implementation	144
1.66.3	Mixed clusters and Change Block Tracking	144
1.67	Backup of Microsoft S2D hyper converged cluster	144
1.68	Guest interaction	144
1.68.1	PowerShell Direct	144
1.68.2	Linux Integration Services and application awareness issue##	145
1.69	Guest restoration	145
1.69.1	Instant VM recovery storage requirement	145
1.70	Job Configuration	145
1.71	Backup Methods	145
1.71.1	Forward Incremental	146
1.71.2	Forever Forward Incremental	148
1.71.3	Reverse Incremental	149
1.72	Encryption	150
1.72.1	Overview	150
1.72.2	Backup and Backup Copy Job Encryption	150
1.72.3	Tape Job Encryption	151
1.72.4	Network Transport Encryption	152

1.73	Deduplication and Compression	154
1.73.1	Storage Optimization Overview	154
1.73.2	Deduplication	154
1.73.3	Compression	155
1.73.4	BitLooker	157
1.74	Backup Job	158
1.74.1	Job Layout and Object Selection	158
1.74.2	Storage maintenance	159
1.74.3	Job Chaining	160
1.74.4	Load Balancing	160
1.74.5	Binding Jobs to Specific Proxies	161
1.75	Backup Copy Job	162
1.75.1	Backup Copy Job Scheduling	162
1.75.2	Job Layout and Object Selection	163
1.75.3	Initial synchronization	164
1.75.4	Additional Options	164
1.76	Replication Job	166
1.76.1	Onsite Replication	168
1.76.2	Offsite Replication	168
1.76.3	Replication from Backups	171
1.76.4	Backup from Replica	172
1.77	Application-Aware Image Processing	172
1.77.1	How Veeam Guest OS Processing Works	172
1.77.2	Selecting Guest Processing Options	172
1.77.3	Guest Interaction Proxy	173
1.77.4	Guest Access Credentials	173
1.77.5	Required Ports	174
1.77.6	Sizing	174
1.77.7	File exclusions	174
1.78	Data Verification Using Virtual Labs	175
1.78.1	Virtual Lab Appliance Overview	175
1.78.2	How SureBackup Job Works	177
1.78.3	Virtual Lab in Complex Environments	181
1.78.4	Scaling out SureBackup jobs	184
1.79	Overview of Applications Support	184
1.80	Active Directory	185
1.80.1	Preparation	185
1.80.2	Job configuration	185
1.80.3	Restore and failover	185
1.80.4	Recovery verification	185
1.81	Microsoft Exchange	185
1.81.1	Preparation	185
1.81.2	Job configuration	186
1.81.3	Granular item restore	186
1.82	Microsoft SQL Server	186
1.82.1	Virtual Machine Image Level Application Aware Backup:	186
1.82.2	Veeam Agent Based Backup for SQL Servers:	186
1.82.3	Preparation	187
1.82.4	Job Configuration	187
1.82.5	Virtual Machine Image Level Backup:	187
1.82.6	Veeam Agent Based Backup:	188
1.82.7	Restore	188
1.82.8	SQL Failover Cluster Database Restore: (Applicable to agent based cluster backup only)	188
1.83	Microsoft SharePoint Server	189

1.83.1	Job configuration	189
1.83.2	Granular item restore	189
1.84	Oracle	189
1.84.1	Preparation	189
1.84.2	Job configuration	190
1.84.3	Job workflow	190
1.84.4	Restore and failover	191
1.84.5	Granular item restore	191
1.85	MySQL	192
1.85.1	Backup Options:	192
1.85.2	HotBackup Database Online Dump:	192
1.85.3	Cold Backup Database Shutdown:	196
1.86	Restore:	198
1.86.1	Database Online Dump During Backup Operations:	198
1.86.2	Online Dump to Staging server	198
1.86.3	HotBackup Database Freeze.	198
1.86.4	ColdBackup Database Shutdown.	199
1.87	IBM Lotus Domino	199
1.87.1	Background	199
1.87.2	Procedure:	199
1.87.3	Restores:	200
1.88	SAP HANA	200
1.89	SAP HANA Backup Options:	201
1.89.1	File Backup:	201
1.89.2	Backint API:	202
1.89.3	Storage Snapshot:	202
1.90	Virtual Machine running SAP HANA Database Backup:	203
1.90.1	Configure Backup:	203
1.90.2	SAP HANA Backup Process:	203
1.91	SAP HANA Backup with Veeam Agent for Linux:	204
1.91.1	Configure SAP HANA Physical Server Backup:	204
1.91.2	SAP HANA Backup Process:	204
1.92	Permissions:	205
1.93	SAP HANA Pre-Freeze Script Configuration Options:	205
1.93.1	User & Secure User Store Authenticaiton:	206
1.93.2	Additional configurable options:	206
1.94	SAP HANA Post-Thaw Script Configuration Options:	206
1.94.1	User & Secure User Store:	206
1.94.2	Verify Veeam HANA Backup via SAP HANA Studio:	207
1.95	Restore:	207
1.95.1	Virtual Machine running SAP HANA Database Restore:	207
1.95.2	Entire VM Restore (Quick RollBack to restore only disk blocks with changes)	208
1.95.3	Instant VM Recovery	210
1.95.4	Physical Server running SAP HANA DB Restore.	211
1.95.5	Restore Disk or Files:	211
1.95.6	Bare-Metal Restore:	212
1.96	POC Guide	212
1.97	Assessment	213
1.97.1	Veeam ONE Monitor	213
1.97.2	Veeam ONE Reporter	214
1.98	Accelerated Evaluation	221
1.99	Enhanced Evaluation	221
1.100	Enhanced Evaluation - Workshop Example	222
1.100.1	Infrastructure Discovery	222

1.100.2	Network and Firewall	223
1.100.3	Proxy/Repository Systems	224
1.100.4	Backup & Replication Server	224
1.100.5	Veeam ONE	225
1.100.6	Enterprise Manager	225
1.100.7	Restore Points	225
1.101	Enhanced Evaluation - Preparation	225
1.101.1	Preparation steps	225
1.102	Automation	226
1.102.1	Command line	226
1.102.2	PowerShell	226
1.102.3	RESTful API	227
1.102.4	A simple RESTful API example - adding a guest to a backup job	227
1.103	Infrastructure Hardening	232
1.103.1	Protect	233
1.103.2	Hardening	233
1.103.3	Secure by Design	233
1.103.4	Remove Unused Components	234
1.103.5	Console Access	234
1.103.6	Roles and Users	235
1.103.7	Required Permissions	235
1.103.8	Encryption	236
1.103.9	Backup & Replication Database	236
1.103.10	Segmentation	237
1.103.11	Visibility	237
1.103.12	Recovery Strategy	238
1.104	Segmentation using Zones	238
1.104.1	Untrusted Zone	240
1.104.2	DMZ	240
1.104.3	Management Zone	240
1.104.4	Trusted Zone	241
1.104.5	Restricted Zone	241
1.104.6	Audit Zone	241
1.105	Hardening Backup Repository - Linux	241
1.105.1	Create a Dedicated Repository Account	242
1.105.2	Set Permissions on the Repository Directory	242
1.105.3	Configure the Linux Repository in Veeam	243
1.105.4	Modify the Firewall	244
1.105.5	Use Veeam Encryption	245
1.106	Hardening Backup Repository - Windows	245
1.106.1	Standalone and Physical secured	246
1.106.2	Local Account with administrative access	246
1.106.3	Set permissions on the repository directory	248
1.106.4	Modify the Firewall	249
1.106.5	Disable remote RDP services	250
1.107	Backup & Replication Anatomy	250
1.108	Backup	251
1.108.1	1. Initialization Phase	251
1.108.2	2a. Guest Processing for Windows-Based VMs	252
1.108.3	2b. Guest Processing for Windows-Based VMs (VIX)	253
1.108.4	2c. Guest Processing for Linux/Unix-Based VMs	254
1.108.5	3. Creating a VM Snapshot	254
1.108.6	4. Releasing the Guest OS Activities	254
1.108.7	5. VM Data Transport	255

1.108.8	5a. Direct SAN Access Data Transport Mode	255
1.108.9	5b. Virtual Appliance Data Transport Mode	255
1.108.10	5c. Network Data Transport Mode	256
1.108.11	6. Committing VM Snapshot	257
1.109	VM Restore	258
1.109.1	1. Initialization Phase	258
1.109.2	2. Restoring VM Configuration	258
1.109.3	3. Creating VM Snapshot	259
1.109.4	4. VM Data Transport	260
1.109.5	4a. Direct SAN Access Data Transport Mode	260
1.109.6	4b. Virtual Appliance Data Transport Mode	261
1.109.7	4c. Network Data Transport Mode	262
1.109.8	5. Committing VM Snapshot	263
1.110	Instant VM Recovery	264
1.110.1	Step by step description of the IVMR process implemented in Veeam Backup and Replication	264
1.110.2	Performance concerns	265
1.111	Windows File-Level Restore	265
1.111.1	1. Initialization Phase	265
1.111.2	2a. Restoring Windows Guest OS Files (Network-Based)	266
1.111.3	2b. Restoring Windows Guest OS Files (Networkless)	266
1.111.4	3. Dismounting Backup Content	267
1.112	Replication	267
1.113	Networking Diagrams	268
1.114	Backup Server	268
1.115	Proxy Server	271
1.116	Repository Server	272
1.117	Storage Integrations	274
1.118	Data Validation	275
1.119	Application-aware Image Processing	276
1.120	Enterprise Manager	276
1.121	Sizing and System Requirements Appendix	277
1.121.1	Veeam Backup and Replication management server resources.	277
1.121.2	Proxy Server Resources	278
1.121.3	Repository Server Resources	278
1.121.4	SQL Server Database Sizing Guide	279
2	Indices and tables	281

Last Updated on 2019-10-18

This is the new home for Veeam V10 Best Practice
Please use branches and do not merge to the master

1.1 Introduction

Welcome to the Best Practices guide for Veeam Backup & Replication.

1.1.1 About This Guide

This guide is developed by Veeam architects, and its content is also validated by support, developers and QA departments to ensure highest possible quality. If you have any questions or comments, please reach out the authors directly, or via your local Veeam Software representative.

Keep in mind this book is optimized for digital consumption, and the most recent version is always available on [Veeambp.com](https://www.veeam.com/best-practices).

1.1.2 Intended Audience

This guide is intended for backup administrators or consultants managing Veeam Backup & Replication on a daily basis.

Most sections of this guide assume you already have hands on experience with Backup & Replication, and will serve as an “advanced user guide”, meaning that more basic usage information, system requirements and the like must be found in [User Guide in Veeam Helpcenter](#).

Service providers delivering BaaS and DRaaS with Veeam Cloud Connect should refer to the corresponding [Veeam Cloud Connect Book](#) or [Veeam Cloud Connect Reference Architecture](#).

1.1.3 Authors

Current maintainers:

- Ali Salman
- Andrea Borella (@AndreBore)
- Bram De Laat
- Edwin Weijdema (@viperian)
- Luca Dell'Oca (@dellock6)
- Matthias Mehrtens
- Pascal di Marco
- Paul Szelesi (@PSzelesi)
- Phillip Moore
- Stanislav Simakov
- Stefan Zimmermann

Old contributors:

- Preben Berg (@poulpreben)
- Andreas Neufert (@AndyandtheVMs)
- Tom Sightler

1.2 Contacting Veeam Software

At Veeam Software we value the feedback from our customers. It is important not only to help you quickly with technical issues, but it is our mission to listen to your input, and build products that incorporate your suggestions.

1.2.1 Online Support

If you have any questions about Veeam solutions, you may use the following resources:

- Veeam Helpcenter at helpcenter.veeam.com
- Veeam Community Forums at forums.veeam.com

1.2.2 Customer Support

Should you have any technical concerns, suggestions or questions, please visit the Veeam Customer Portal at cp.veeam.com to open a case, search our knowledge base, reference documentation, manage your licenses or obtain the latest product release.

1.2.3 Company Contacts

For the most up-to-date information about company contacts and office locations, please visit www.veeam.com/contacts.html.

1.3 DNS Resolution

Domain Name System (DNS) resolution is critical for Veeam Backup & Replication deployment (VBR) and configuration. All infrastructure components should be resolvable through a fully qualified domain name (FQDN). This is especially important for vSphere/Hyper-V hosts and clusters. Resolvable means that components are accessible through both forward (A) and reverse (PTR) lookups.

Ensure that the Veeam Backup & Replication server is installed on a machine that has a resolvable fully qualified domain name (FQDN). To check that the FQDN is resolvable, type `nslookup your-vbr-server-fqdn.domain.local` at a command line prompt. If the FQDN is resolvable, the `nslookup` command returns the IP and name of the Veeam Backup & Replication server.

Only if DNS resolution is **not** available you may add the infrastructure components like e.g. VMware vCenter, ESXi and managed Veeam servers to the local `hosts` file on *all* managed Veeam servers. When using this workaround it is recommended to add both short name and fully qualified domain name in the `hosts` file.

When ESXi hosts are added to vCenter it is recommended to use FQDN. When backing up through the network with the Network Block Device (NBD) transport mode, the FQDN is returned via VMware API for Data Protection (VADP) so the backup proxy server must be able to resolve the FQDN via DNS. Using the `hosts` file the data transport path can be altered for NBD transfers.

Please see the example below.

1.3.1 Example `hosts` file

```
10.0.4.10      vcenter      vcenter.example.com

# 10.0.4.21     esx1        esx1.example.com # commented out management interface
# 10.0.4.22     esx2        esx2.example.com # commented out management interface

10.255.4.21    esx1        esx1.example.com # dedicated 10 GbE backup network
10.255.4.22    esx2        esx2.example.com # dedicated 10 GbE backup network
```

To explicitly alter the data transport path, the `hosts` file must be deployed on all backup proxy servers. For easier management, please see the [Carbon module](#) and `Set-HostsEntry` by Aaron Jensen.

1.4 Backup Server

Veeam Backup & Replication is a modular solution that lets you build a scalable availability infrastructure for environments of different sizes and configurations. The Backup Server is the core component. Features & component requirements will affect your decision how you install the backup server e.g. one datacenter or multiple locations. It could mean that you choose to install additional backup servers or services in remote locations to optimize the data streams.

Before installing the Veeam Backup & Replication server it is important to understand the different data streams generated by the Veeam Backup Server (VBR) Services.

1.5 Deployment Method

You may deploy the Veeam Backup & Replication server as either a physical or virtual server. It will run on any server with Windows Server 2008 R2 or higher installed (64-bit only). Install Veeam Backup & Replication and its components on dedicated machines. Backup infrastructure component roles can be co-installed. The following guidelines may help in deciding which deployment type is the best fit for your environment.

1.5.1 Virtual deployment

For most cases, virtual is the recommended deployment. As it provides high availability for the backup server component via features like vSphere High Availability, vSphere Fault Tolerance or Hyper-V Failover Clustering. It also provides great flexibility in sizing and scaling as the environment grows.

The VM can also be replicated to a secondary location such as a DR site. If the virtual machine itself should fail or in the event of a datacenter/infrastructure failure, the replicated VM can be powered on. Best practice in a two-site environment is to install the Backup server in the DR site, in the event of a disaster it is already available to start the recovery.

1.5.2 Physical deployment

In small-medium environments (up to 500 VMs) it is common to see an all-in-one physical server running the Backup & Replication server, backup proxy and backup repository components. This is also referred to as an “Appliance Model” deployment.

In large environments (over 2,500 VMs) installing Backup & Replication services on separate servers either virtual or physical will provide better performance. When running many jobs simultaneously, *consuming large amounts of CPU and RAM*, scaling up the virtual Backup & Replication server to satisfy the system requirements may become impractical.

An advantage of running the Veeam Backup & Replication server on a physical server is that it runs independently from the virtual platform. This might be an ideal situation when recovering the virtual platform from a disaster. Should the physical server itself fail, there are additional steps to take before reestablishing operations:

1. Install and update the operating system on a new server
2. Install Veeam Backup & Replication
3. Restore the configuration backup

In an enterprise environment, you may choose to install an additional backup server to speed up the recovery process during a disaster. You may re-use existing availability components such as a proxy or repository server for the standby Backup & Replication server. During a disaster the configuration backup can easily be restored to this server.

Tip: It is recommended to store the configuration backup, *using a file copy job*, in a location that is always available to this standby Backup & Replication server.

1.6 Backup Server Placement

The Backup server runs a number of processes, e.g. the Backup Service, Backup Manager services and in some scenarios a Mount Server as well. In this chapter we will evaluate how each of those components are affected by placement of the Backup & Replication server.

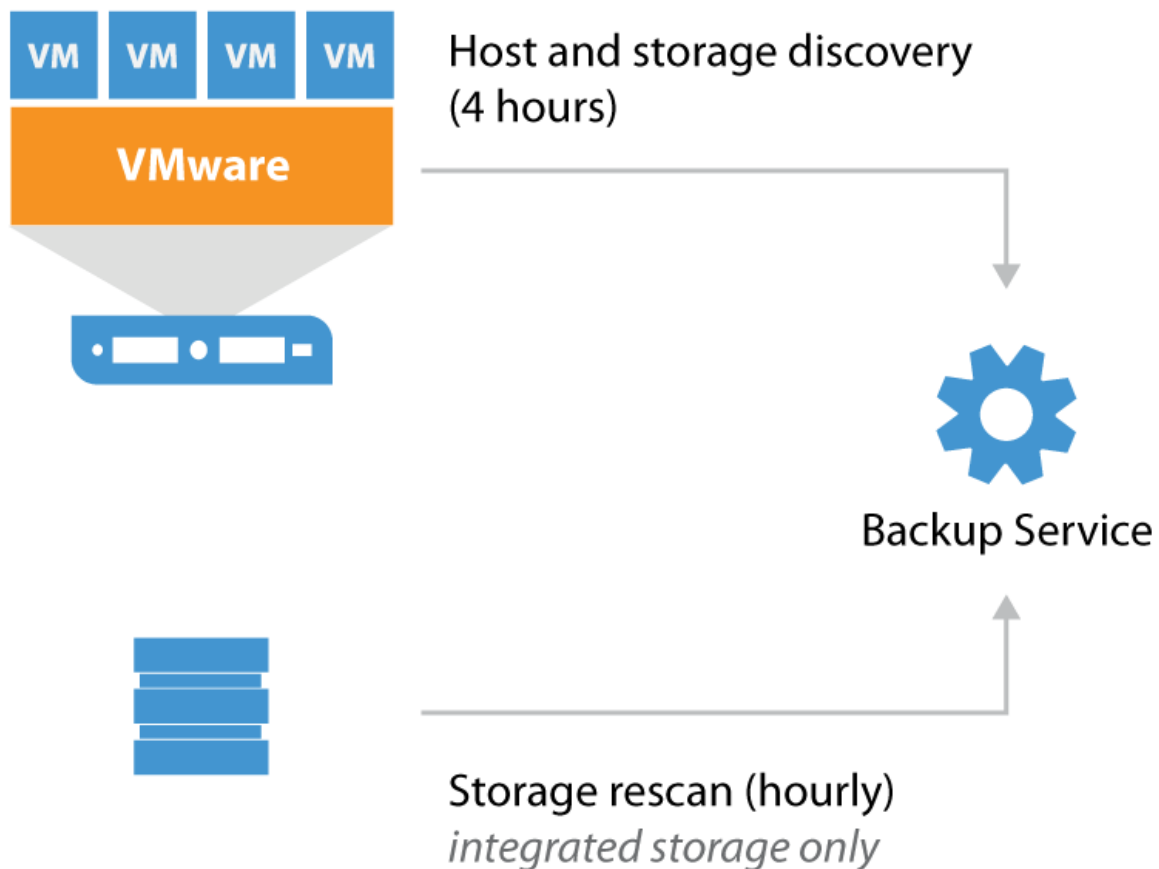
By evaluating the roles and understanding the data flow between the services it is possible to optimize overall backup performance and restore throughput significantly.

1.6.1 Host and Storage Discovery

To collect information about the virtual infrastructure all managed vCenters and their connected hosts and datastores are periodically rescanned. This rescan process is visible in the **History** tab > **System** section in the Veeam Backup & Replication console. As seen here, the Host discovery process runs every four hours. All the collected information is stored within the configuration database.

The amount of collected information is typically very small however the Host discovery process may take longer or even exceed the default schedule in highly distributed environments^[1]. If hosts or clusters are connected to vCenter over a high-latency link you may consider deploying a Backup server locally on the ROBO, then you can create a vCenter service account with a limited scope to that particular location in order to reduce the window of the Host discovery process. If the ROBO uses a stand-alone host it is possible to add the host as a managed server directly instead of through vCenter.

Note: Avoid adding individual hosts to the backup infrastructure if using shared storage in a vSphere cluster.



and storage discovery

Host

If storage with advanced integration (HPE, NetApp, EMC, Nimble) are added to the **Storage Integration** tab there will additionally be a Storage discovery process periodically rescanning storage hourly. This process checks all snapshots for virtual machine restore points for usage within Veeam Explorer for Storage Snapshots. The Veeam Backup & Replication server itself will not perform the actual scanning of volumes but it will use the management API's of

the storage controller to read information about present snapshots. Only proxy servers with required storage paths available will be used for the actual storage rescanning process[^2].

The following table shows the three different scanning workflows:

Adding new storage controller	Creating new snapshot	Automatic scanning
1. Storage Monitor runs in background 2. Detecting new volumes 3. Scanning volumes for snapshots every 10 minutes 4. Lists initiators 5. Searching storage exports in VMware 6. Export and scan the snapshots with proxies 7. Update configuration database	1. Collect specific storage information 2. List of volumes, snapshots, LUNs and NFS exports 3. Checking licenses, FC and iSCSI server 4. Lists initiators 5. Searching storage exports in VMware 6. Mapping discovered VMs from datastores to snapshots 7. Mapping discovered VMs from datastores to snapshots 8. Export and scan the discovered objects with proxies	1. Creating new Snapshot 2. Lists initiators 3. Testing iSCSI, NFS and FC from proxies 4. Searching storage exports in VMware 5. Mapping discovered VMs from datastores to snapshots 6. Searching storage exports in VMware 7. Mapping discovered VMs from datastores to snapshots 8. Export and scan the snapshots with proxies 9. Update configuration database

The scan of a storage controller performs, depending on the protocol, several tasks on the storage operating system. Therefore it is recommended to have some performance headroom on the controller. If your controller is already running on >90% CPU utilization, keep in mind that the scan might take significant time to complete.

The scanning interval of 10 minutes and 7 days can be changed with the following registry keys.

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication
- Key: SanMonitorTimeout
- Type: REG_DWORD
- Default value: 600
- Defines in seconds how frequent we should monitor SAN infrastructure and run incremental rescan in case of new new instances
- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication
- Key: SanRescan_Periodically_Days
- Type: REG_DWORD
- Default value: 7
- Defines in days how frequent we should initiate periodic full rescan after Veeam Backup service rescan

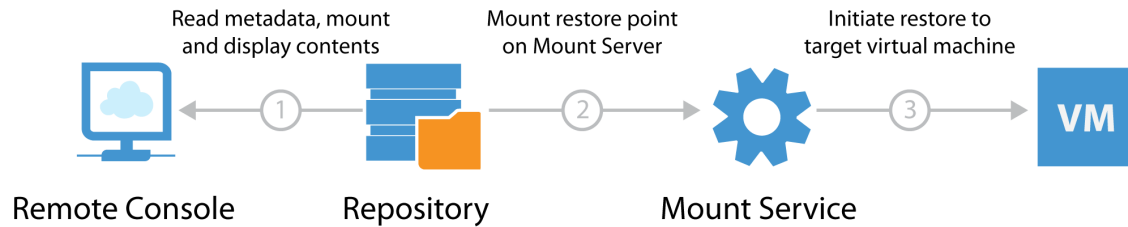
Per default Veeam will scan all volumes and LUNs on the storage subsystem. During rescan, each present snapshot produces a snapshot clone, mounts to a proxy server, scans the filesystem, lookup for discovered VMs and unmounts. This is repeated for every present snapshot.

Example: A storage system with 50 volumes or LUNs with 10 snapshots for each. Scanning the entire system means 500 (50x10) mounts and clones are performed. Depending on the performance of the storage system and the proxy server, this can take significant time.

To minimize the scan time it is recommended to select the volumes used by VMware within the setup wizard to avoid the overhead of scanning unused data volumes.

1.6.2 File-level Recovery Data Flow

To perform file-level restores for a Windows-based or other OS VM Veeam mounts all VM disk files from the backup files (stored on the repository server) to a Mount Service.



Data

flow at restore

When file-level recovery is performed from the Veeam backup console, two mounts are initiated:

1. The remote console - for displaying restore point contents
2. The mount server - for performing actual restore traffic to the target VM

Note: For VMs not running a Windows operating system, a Linux based FLR helper appliance mounts the backup file for reading the file system.

Between 50-400 MB of data is transferred between the console and backup repository. If the first file mount is performed over a slow connection it may take considerable time to load the file-level recovery wizard. If there is significant latency between the backup repository and console, it is recommended to deploy an instance of the console on or closer to the repository server.

Veeam Enterprise Manager

Veeam Enterprise Manager is a self-service portal where administrators or service desk representatives can initiate restores for VMs, files, e-mail items, Oracle and SQL databases.

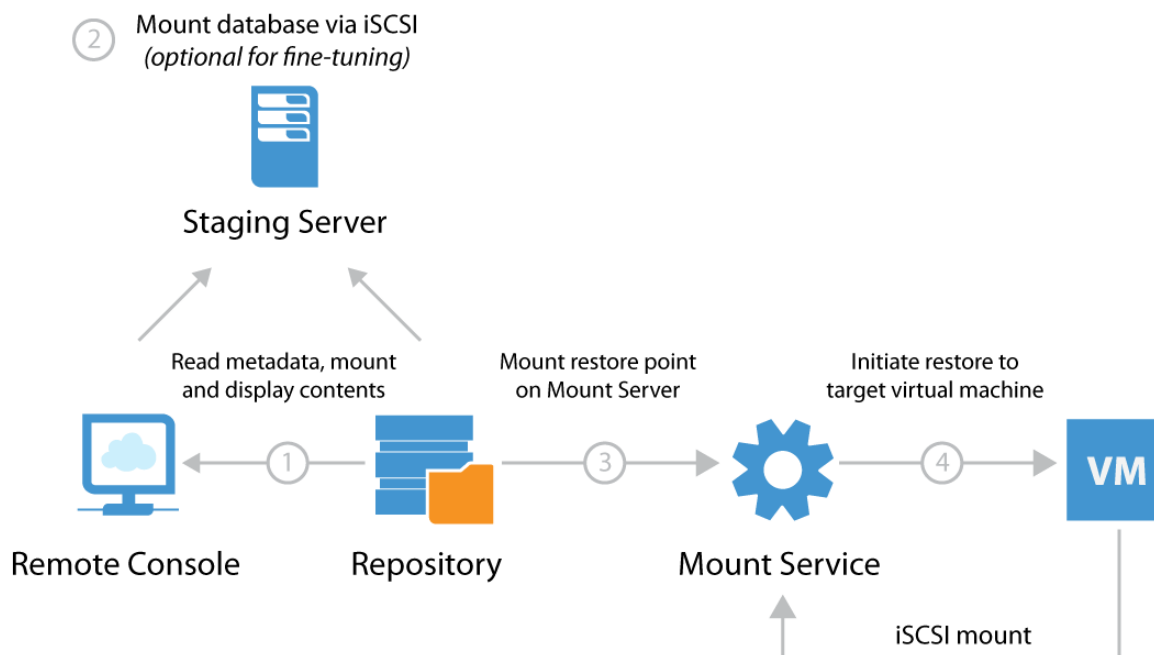
It is possible to avoid the first mount entirely by using “guest file system indexing”^[3]. When guest file system indexing is enabled, the content of the guest VM is stored in the Veeam Catalog and presented through Veeam Enterprise Manager. Veeam Enterprise Manager will initiate the file-level restore with the mount server without requiring the first mount.

Note: If guest file system indexing is disabled restores may still be initiated through Enterprise Manager however they will still require the first mount to be performed with similar performance implications as previously described.

Veeam Explorers

Veeam Explorers are installed as part of the backup server and backup console when installed remotely. When performing item-level recoveries the file-level recovery engine is leveraged. Please see the previous section for deployment considerations.

The Veeam Explorer for SQL Server, SharePoint and Oracle all use a staging server to allow selecting a specific point in time for point-in-time restore. This introduces an additional connection as illustrated below.



Server

Staging

1.6.3 Disaster Recovery Optimization

When using Veeam for replicating VMs to a disaster recovery (DR) site, it is recommended to keep the Backup & Replication server in the DR site alongside the replicas. When the backup server is located in the DR site it enables true "1-Click Failover" by being able to start Failover Plans immediately and thus eliminate manual reconfiguration before the failover process can be initiated.

Proper planning dictates that to get 1-Click Failover working it requires that the vSphere clusters in each location are connected to separate vCenter servers. In the event of an outage in the primary datacenter it is only possible for the Backup & Replication server in the DR site to initiate failover if the vCenter server itself is available.

In cases when it is impossible to have multiple vCenter instances across sites (e.g. Metro Cluster or similar active-active configurations), the recommended solution is to use vCenter Server and following these steps in event of a disaster:

1. Replicate vCenter from primary site to secondary site with low RPO
2. Configure VMware DRS affinity rules^[4] for pinning replica vCenter VM to a specific host
3. Connect to specified host and manually power on replicated vCenter VM
4. Verify vCenter availability through Veeam Backup & Replication
5. Initiate Failover Plans

1.6.4 Examples

In this section we will outline two examples based on two enterprises with 50 remote/branch offices (ROBO). They have the following common characteristics:

- One vCenter Server in HQ managing all ROBO sites
- Local backup jobs for fast backup and restore performance
- Offsite copies from the ROBO consolidated at HQ for D/R protection

Example 1: Centralized Job Configuration

IT requires *one* central management console for the entire backup infrastructure, administration and job scheduling. The backup administrator can follow these guidelines:

1. Install and configure Veeam Backup & Replication in HQ
2. Add the vCenter Server via the Veeam Backup & Replication console
3. Add the ROBO backup server as Managed Server in the **Backup Infrastructure** tab
4. Configure the HQ backup server with the roles Backup Repository and optionally WAN accelerator
5. Configure the ROBO backup server with the roles Backup Proxy, Backup Repository and optionally as WAN accelerator^[5]
6. Configure one or more Backup Jobs for each ROBO pointing to its local backup repository
7. At HQ configure one or more Backup Copy Jobs for each ROBO pointing to the backup repository
8. Install Veeam Backup Console on the ROBO backup server for faster restore via the local Mount Server

Note: The remote console installation files are on the same installation media as Veeam Backup & Replication (\Backup\Shell.x64.msi)

Constraints

Please consider the following constraint:

- If a WAN link between HQ and a ROBOs fails, no backup jobs will run, as the backup server will not be able to communicate with the remote ESXi hosts via the centralized vCenter Server
- When performing file-level restore for non-indexed virtual machines at the ROBO via Veeam Enterprise Manager the restore point will be mounted over the WAN link to HQ for displaying the contents of the restore point. Thus it is recommended to use indexing for such virtual machines

Example 2: Distributed Job Configuration

IT requires local backup jobs and backup copy jobs (with optional WAN acceleration) are created at the ROBO. For security considerations, each ROBO is provided with delegated access to VMware vCenter. Restore capabilities from backup copy jobs should be configured and managed at HQ as well as delegated restore and license management for all sites via Veeam Enterprise Manager. The backup administrator may follow these guidelines:

1. Install Enterprise Manager at HQ
2. Install and configure Veeam Backup & Replication on each ROBO
3. On vCenter Server, create separate service accounts per ROBO with a limited scope for displaying only relevant hosts or clusters
4. At the ROBO, add vCenter Server via the **Backup Infrastructure** tab using the scoped service account
5. *Optional:* At the ROBO, configure a local WAN accelerator and create or re-use an existing WAN accelerator at HQ (please note many-to-one configurations are supported)

6. At the ROBO, add and configure the Repository Server at HQ (please note many-to-one configurations are supported)
7. Configure one or more Backup Jobs at each ROBO pointing to its local backup repository
8. Configure one or more Backup Copy Jobs at each ROBO pointing to the centralized backup repository at HQ (use WAN acceleration as needed)
9. Install Veeam Backup & Replication Console at HQ. When using the remote console for connecting to remote instances, it is possible to leverage faster file-level or item-level restores at HQ via the console's built-in Mount Server

Note: As components are managed by multiple backup servers, always ensure that the same patch/update/version level is used for the entire Veeam backup infrastructure.

[^1]: In very large or extremely distributed environments, it is possible to extend the schedule frequency by altering registry key `VolumesDiscover_Periodically_Hours` (REG_DWORD, default: 4) [^2]: Storage rescan procedure > [Re-Scanning Storage Systems](#) [^3]: More information about guest file system indexing in Veeam Help-center > [Guest file system indexing](#) [^4]: VMware Distributed Resource Scheduler > [VM-Host Affinity Rules](#) [^5]: Remember to add sufficient resources if all three roles can run on the remote backup server.

1.7 Sizing and System Requirements

In this section, we will describe how to configure and size the Veeam backup server.

Sizing with Veeam is cumulative in respect to configurations, if you want to create an all-in-one appliance (Appliance Model) add all the resource requirements together (CPU + Memory) to understand what in total you will need, combining roles such as the proxy and repository merits the same considerations

1.7.1 Compute requirements

Recommended Veeam backup server configuration is **1 CPU core (physical or virtual) and 4 GB RAM per 10 concurrently running jobs**. Concurrent jobs include any running backup or replication jobs as well as any job with a continuous schedule such as backup copy jobs and tape jobs.

The minimum recommendation is 2 CPU cores and 8 GB RAM.

It is recommended to group multiple virtual machines into a single job for better efficiency and resource usage. With default configuration it is recommended to configure around 30 VMs per job. The recommendation can be increased by over 10x (300+ VMs) by leveraging additional features such as [per VM backup files](#). Please refer to the [Job Configuration](#) section of this guide to learn more about job design.

All configuration and session information is stored in the configuration database. In larger environments the load on the SQL Server hosting the configuration database may be significant and is highly dependent on the amount of concurrently running jobs. For more information please see the [Backup Server Database](#) section of this guide.

1.7.2 Operating system

The Veeam backup server requires Microsoft Windows 2008 R2 or later (64-bit only). The latest supported version of Windows OS is always recommended (currently Microsoft Windows 2016) as it will also support restoring from virtual machines with ReFS file systems or workloads with Windows Server Deduplication enabled.

For the full list of supported operating systems, please refer to the corresponding [System Requirements](#) section of the Veeam User Guide.

1.7.3 Disk space

This section explains what folders you should plan for when preparing for installation of the Veeam backup server.

The folders are detailed here as follows:

Installation folder

Default location is `C:\Program Files\Veeam\Backup and Replication`

Plan for 40 GB. If installing in a virtual machine, thin disks may be used. By default the installer will choose the drive with most available free space for the built in backup repository.

Log files

Default location is `C:\ProgramData\Veeam\Backup`

Log file growth will depend on the number and frequency of jobs and the number of instances being protected. Consider that the logging level may also affect the log size, if you need to change the logging level or log file location refer to this Veeam Knowledge Base article: <https://www.veeam.com/kb1825>.

It is recommended to not configure the logging level below 4, as it may complicate troubleshooting. Logging level 6 is very intrusive, and should only be configured for short periods of time when requested by Veeam Support.

Plan for 3 GB log files generated per 100 protected instances, with a 24 hour RPO. For environments with more than 500 protected instances it is recommended to change the default location to a different fast access disk. Many concurrently running jobs may produce a lot of write streams to log files, than can slow down operations for the Veeam Backup Service and Backup Manager processes.

Veeam Backup Catalog folder

Default location is `C:\VBRCatalog`

This folder is used if guest indexing in backup jobs is enabled. For more information, refer to the *Guest Indexing* section of this guide. To change the default location, refer to this Veeam Knowledge Base article: <https://www.veeam.com/kb1453>

vPower NFS folder

Default location is `C:\ProgramData\Veeam\Backup\NfsDatastore`

When booting VMs with Instant VM Recovery or SureBackup, this folder is used by default to store all configuration files and redo logs of the running VM. To offload the changes to a specific production datastore refer to the corresponding page of the Instant VM Recovery wizard.

We recommend installing vPower NFS Services on each Windows-based backup repository. For SMB/CIFS based repositories or deduplication appliances it is recommended to configure vPower NFS on the gateway server. For Linux-based repositories it is recommended to configure vPower NFS on a managed Windows machine as close as possible to the Linux repository (similar to selecting a Gateway Server for SMB/CIFS or storages that use enhanced deduplication technologies).

The vPower NFS server is bound to backup repositories and the folder location is defined per server. To achieve best performance for VMs running off of vPower NFS please configure the fastest possible storage on the backup server or backup repository. To change the folder location please see the following steps.

1. In the **Backup Infrastructure**, select the **repository** you wish to change.

2. Right click the **repository** and go to **properties**
3. When the wizard opens navigate to the **Mount server** settings
4. Using the browser buttons locate the new location for your vPower NFS storage
5. Finish the wizard

It is recommended to reserve at least 10 GB space for this folder. If you plan to start a significant number of VMs or run VMs over a longer period increase the space accordingly to fit the produced/estimated amount of changes generated by the running VMs (conservative average change rate can be defined as 100 GB per 1 TB VM per 24 hours - or 10%). Additional disk space is consumed when using Quick Migration. See more information here > [Veeam Help Center > Performing Instant VM Recovery > Before You Begin](#).

Important! Make sure vPower NFS is configured correctly on the Veeam backup server itself as it will be used when deploying Virtual Lab for SureBackup or when performing file-level recovery for Linux-based VMs.

For information on folders required for Enterprise Manager, backup proxy and repository servers (backup targets) and WAN accelerators, as well as for recommendations on their sizing please refer to the corresponding sections of this guide.

1.7.4 Other software

It is strongly recommended that no highly-transactional and business-critical software is deployed on the same machine as the Veeam backup server. This could be (but not limited to) software such as Active Directory, Exchange Server or other intensive production databases on the SQL server instance. If possible it would be preferable to have no other software at all running on the Veeam Backup Server.

It is recommended to follow antivirus exclusion guidelines as explained in [Veeam KB 1999](#).

If it is not possible to connect to a remote SQL staging server for Veeam Explorers you can install Standard or Enterprise versions of SQL (depending on your licensing) locally for staging databases for item-level restores on the backup server. This installation can also be used to store the Veeam backup database if required as long as sufficient resources are assigned to the host machine, however do not run any instances in production from this installation that may affect the operation of the backups or restore processes. SQL express is included in the distribution but is limited to a 10GB database.

Note: Remote SQL Server for staging is supported from v9.0

Other software such as Microsoft Outlook (64-bit) for mail export to PST files via Veeam Explorer for Exchange, or a PDF viewer for reading Veeam documentation are considered non-disruptive.

1.7.5 Installing Veeam Backup & Replication updates

New Veeam releases and updates are installed on the Veeam Enterprise Manager and Veeam backup servers by the setup wizard or by using the unattended installation method (also referred to as “silent installation”). For detailed instructions check the latest release notes.

Note: Veeam Backup Enterprise Manager must be updated before updating Veeam backup servers.

After installing updates open the Veeam Backup & Replication management console. The **Update** screen will be displayed and will guide you through updating distributed components on other Veeam managed servers (like proxy and repository servers, vPower NFS servers, WAN accelerators and tape servers).

Note: As Veeam deploys no agents on the virtual machines, you do not need to update any software (agents) on the VMs.

1.8 Veeam Backup & Replication Database

Veeam Availability Suite, which includes Veeam Backup & Replication, Veeam ONE and Enterprise Manager, stores all information about backup infrastructure, jobs settings, job history, sessions and other configuration data in an SQL server instance.

When planning the Veeam Backup & Replication deployment you must choose the placement of the configuration database. It may be either a local or remote SQL Server with several licensing options available. Please see the following recommendations to ensure your Backup & Replication setup will scale to the size of your infrastructure.

1.8.1 SQL Server Edition

Microsoft SQL Server 2012 SP3 Express Edition is included in the Veeam Backup & Replication setup which is a convenient option for most smaller deployments. It does however have several limitations^[1] which may affect performance:

- Each instance uses only up to 1 GB of RAM
- Each instance uses only up to 4 cores of the first CPU
- Database size cannot exceed 10 GB

It is recommended to install Standard or Enterprise Edition if any of the following apply:

- **When protecting more than 500 VMs.** It is recommended to use Standard or Enterprise versions of Microsoft SQL Server. The max database size allowed by Express Edition is usually sufficient, so do not consider this a constraint. Veeam Backup & Replication console and job processing may however slow down as a result of CPU and RAM constraints on the SQL Server Express instance.
- **When using Files to Tape jobs extensively,** the database may grow significantly, and the 10 GB limitation may be exceeded quickly.
- **When unable to configure an external staging server.** For Veeam Explorer for Microsoft SQL Server or Veeam Explorer for Microsoft SharePoint. When working with databases larger than 10 GB, SQL Server Express cannot mount the databases.
- **When databases are using advanced features of Microsoft SQL Server.** Such as encryption or table partitioning, the licensing level of the staging server (local or remote) must match the level of the original instance.

If none of the above apply it is recommended to use Microsoft SQL Server Express Edition for the sake of simplicity.

Tip: Veeam Backup & Replication supports Microsoft SQL Server 2008 or higher. To leverage Microsoft SQL Server 2014 enhancements (cardinality estimator has proved to show significant improvements for large queries), it is highly recommended to update the database server to Microsoft SQL Server (Express) 2014 or higher.

1.8.2 Database Placement

It is possible to leverage a remote SQL Server as staging server during restores in Veeam Explorer products. There are no specific edition requirements for neither SQL Express, Standard or Enterprise instance of SQL Server installed locally on the backup server. It is still recommended to run the SQL Server locally (when resource and planning allow) on the backup server for lowest latency and highest performance.

There may still be scenarios where a remote SQL Server is the better choice:

- **High Availability** - SQL Clustering and AlwaysOn Availability Group on external SQL Servers can be used for configuration database high availability
- **Fast Recovery** - Failover to a standby backup server can be simplified by connecting to the configuration database directly without the need for restoring from a configuration backup

- **Licensing** - Some enterprises have dedicated virtual clusters for SQL Server due to licensing constraints. In such cases, you may place the Veeam configuration database on existing instances to lower the overall TCO

1.8.3 Sizing

Veeam Backup & Replication may consume high amounts of CPU and RAM while processing backup or replication jobs. To achieve better performance and load balancing it is necessary to provide sufficient RAM and CPU resources to Veeam components. Remember to add additional resources, if the backup server is responsible for multiple roles, such as repository server or backup proxy.

Please follow these guidelines:

Number of concurrently running jobs CPU RAM			Up to 25 2 4 GB
Up to 50 4 8 GB	Up to 100 8 16 GB		

Note: Concurrently running jobs include any job type with a continuous schedule such as Backup Copy Jobs.

When running more than 100 jobs concurrently increase the amount of resources by 2 CPU cores and 4GB of RAM for every 25 concurrently running Jobs.

It is recommended to place the configuration database on fast, resilient storage subsystem. Performant storage for backing the configuration database will result in overall increased processing performance. Jobs with a lot of metadata such as very large SharePoint farms with thousands of sites, SQL Server instances with many databases or Files to Tape jobs may increase the I/O requirements for the configuration database.

1.8.4 SQL Server Configuration Tips

Veeam Backup & Replication does not require any specific settings^[^2] on the SQL Server in order to utilize the capabilities of Veeam Explorer for SharePoint or SQL. Both local and remote SQL Servers can be used for staging purposes, the corresponding requirements are detailed on [Veeam Helpcenter](#) and can be found through the following links:

- [Veeam Explorer for Microsoft SharePoint](#)
- [Veeam Explorer for Microsoft SQL Server](#)

Tip:

- Enable and configure all features used by production databases.
- When possible use the highest license level and latest version and cumulative update level installed in any VM.
- Using an older version of SQL Server for the configuration database than running in a protected VM may result in warnings in job session logs when such VMs are processed.

If you plan to restore encrypted databases with Veeam Explorer for Microsoft SQL Server or SharePoint you will need a valid encryption certificate on the staging Microsoft SQL Server^[^3].

Follow Microsoft general recommendations for optimal SQL performance, for example, place the SQL tempdb on the fastest disks for best performance.

1.8.5 Modifying Database Connection Settings

To modify database connection settings or connect to another Veeam configuration database use the DBConfig utility as described in the product documentation at https://www.veeam.com/documentation-guides-datasheets.html/docs/backup/vsphere/dbconfig_utility.html?ver=95.

If using SQL authentication consider that all Veeam UI and Veeam PowerShell changes are communicated using this authentication.

1.8.6 Migrating Veeam Database

To migrate Veeam configuration database to another SQL Server follow the recommendations provided in these Veeam Knowledge Base articles:

- <https://www.veeam.com/kb1250>
- <https://www.veeam.com/kb1889>

[^1]: Features Supported by the Editions of SQL Server 2012 [https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2012/cc645993\(v=sql.110\)](https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2012/cc645993(v=sql.110))

[^2]: Generic requirements for SQL Server can be found here: https://www.veeam.com/documentation-guides-datasheets.html/docs/backup/vsphere/system_requirements.html?ver=95

[^3]: For restoring encrypted databases, please see: <https://www.veeam.com/kb2006>

1.9 Protecting Veeam Backup & Replication Configuration

1.9.1 Protecting the Veeam Backup Server

As recommended by best practice for disaster recovery you can place Veeam Backup & Replication installation on a virtual machine and protect it with backups or replicas. Out-of-the box Veeam automatically creates configuration backups on the default backup repository.

These configuration backups contain all the information about Veeam Backup & Replication, like Backup Infrastructure components and objects, Backup jobs (passwords are not stored by default), Sessions and Tape setup. The configuration backup can be used to automatically rebuild the Veeam Backup & Replication server with all objects, sessions and jobs.

To restore all jobs and their metadata (you will be asked for all required passwords during the restore process). Please refer to the Veeam Backup & Replication User Guide for further details: https://helpcenter.veeam.com/docs/backup/vsphere/vbr_config.html?ver=95

If restoring the backup configuration to a newly provisioned server, it is highly recommended that the replacement server has the same DNS name, VBR version and patch level as the original backup server, this is especially true if using Veeam Agents for Windows or Linux.

Tip: If encryption is enabled for configuration backup the passwords are also stored in the configuration backup files.

1.9.2 Planning for Disaster Recovery of Veeam Backup Server

Having a solid disaster recovery strategy for your availability components, like the backup server, is key to a successful recovery. For all situations follow these basic guide lines:

1. Make sure the daily configuration backup is **not** placed in the default location on the backup server itself
2. Modify the backup configuration backup settings to point to a secure backup repository on a different location/site
3. Schedule the configuration backup to run when the backup server is least occupied;
4. Make sure the configuration backup is encrypted to protect the configuration details. Also all passwords are than stored in the configuration backup files

5. Check that you receive notifications about the status of the configuration backup job results
6. Think about placement of the backup server, configuration backup and database. This is highly depended on the overall infrastructure design and DR strategy of your organization

By default, Veeam Backup & Replication is configured to create a daily configuration backup. The resulting configuration backup file is stored in the `\VeeamConfigBackup\%BackupServer%` folder on the default backup repository. However, for security's sake, it is recommended that you do **not** store configuration backups on the **default backup repository** or in any other folder on the backup server. In this case, if the backup server fails, its configuration data will remain, and you will be able to recover the failed backup server.

When the backup server is in the primary site it is recommended to replicate the Veeam backup server VM to the secondary site (verify network and IP mapping settings before you begin; refer to https://helpcenter.veeam.com/docs/backup/vsphere/replica_job.html?ver=95 for details).

Note you cannot IP map a replica Veeam backup server if the control of the replica is by the same server being replicated, it can only be done using another VBR server to control that replica)

Also check the location of the configuration database, when the database is external ensure this server is also replicated to the secondary site. If the server is replicated successfully, in the event of a disaster, you may start its replica in the secondary location without having to reinstall Veeam Backup & Replication. This will help to lower overall Recovery Time Objective (RTO).

Tip Use Veeam's File Copy Job to place a copy of the configuration backup at the DR site. You can configure another repository for that purpose.

Note All data required for a restore is directly placed within the backup file (which VMs are in the backup file as well as deduplication and encryption information), even in the event that configuration database is lost or damaged you can set up a new Veeam backup server and import the backup files there, or even use the stand-alone "Extract" utility (both a command line and a graphical version are provided). Then you will be able to restore VMs, files and application data without restoring the configuration database.

Note: Backup copy jobs do not process configuration backups. Remember that configuration backups are not processed with backup to tape jobs; if you want to store configuration backups on tape use file to tape jobs instead.

Note: Although it is supported, writing configuration backups on block repositories like DD Boost or Catalyst store is not recommended. This kind of repositories can not be accessed without a backup server installed. Using a regular SMB share, to save configuration backups, can really make things easier when it comes to rebuild completely a failed backup server: .BCO files can be accessed directly as soon as the new server is up and running and they can be copied locally to be imported without configuring anything first on the backup server.

1.9.3 Antivirus on Veeam Servers

Antivirus software monitors all 'write' operations on the operating system and this also extends to Veeam backup files. Data that is processed by a backup proxy and repository can overload the antivirus system so that it blocks the backup files, this can slow down the backup process or even lead to backup file corruption. To avoid this it is recommended the following exclusions specified in KB1999 <https://www.veeam.com/kb1999>, are added on all Veeam servers including Veeam backup server, proxy server, repository server, WAN accelerator server, tape server, and others.

Tip: Due to the complex nature of antivirus software some additional exclusions may be needed. If the antivirus has a logging or history system you can review its logs to detect whether it has taken any actions that might affected Veeam Backup & Replication operations.

Consider that other services or process may be using ports configured for the Veeam vPower NFS Service. To avoid possible issues it is recommended to stop the Veeam vPower NFS Service if you do not plan to use it. Make sure that none of the NFS ports are used by other software (including antivirus systems). For more information please refer to this Veeam Knowledge Base article: <https://www.veeam.com/kb1055>.

1.10 Veeam Backup Enterprise Manager

1.10.1 Whether to Deploy?

Enterprise Manager is intended for centralized reporting and management of multiple backup servers. It provides delegated restore and self-service capabilities as well as the ability for users to request Virtual Labs from backup administrators. It provides a central management point for multiple backup servers from a single interface. Enterprise Manager is also a part of the data encryption and decryption processes implemented in the Veeam solution and best practice recommend deploying Enterprise Manager in the following scenarios:

- It is recommended to deploy Enterprise Manager if you are using encryption for backup or backup copy jobs. If you have enabled password loss protection (https://helpcenter.veeam.com/docs/backup/em/em_manage_keys.html?ver=95) for the connected backup servers backup files will be encrypted with an additional private key which is unique for each instance of Enterprise Manager. This will allow Enterprise Manager administrators to unlock backup files using a challenge/response mechanism effectively acting as a Public Key Infrastructure (PKI).
- If an organization has a Remote Office/Branch Office (ROBO) deployment then leverage Enterprise Manager to provide site administrators with granular restore access via web UI (rather than providing access to Backup & Replication console).
- In enterprise deployments delegation capabilities can be used to elevate the 1st line support to perform in-place restores without administrative access.
- For deployments spanning multiple locations with stand-alone instances of Enterprise Manager will be helpful in managing licenses across these instances to ensure compliance.
- Searching the Indexes can also be used to find files that have been backed up and the indexes stored in the Enterprise Manager database.
- Enterprise Manager is required when automation is essential to delivering IT services — to provide access to the Veeam RESTful API.

If the environment includes a single instance of Backup & Replication you may not need to deploy Enterprise Manager, especially if you want to avoid additional SQL Server database activity and server resource consumption (which can be especially important if using SQL Server Express Edition).

Note: If Enterprise Manager is not deployed, password loss protection will be unavailable.

1.10.2 Using Enterprise Manager for Restore Operations

1-Click File-level Restore

With Enterprise Manager, you can restore VM guest files with a single click. To support this capability the VM restore point must be created with application-aware image processing enabled. Additionally, if guest file system indexing is enabled, it is possible to search for files across VM backups.

Note: It is possible to restore VM guest files even when application-aware image processing or file indexing is disabled. If both are disabled, the restore operator must type in guest OS credentials during a file-level restore.

The backup catalog on the Enterprise Manager server will be used to store indexing data replicated from the backup catalog on Veeam backup server(s). For more information about the process, refer to the [Enterprise Manager User Guide](#). To learn more about Veeam Backup Catalog sizing refer to the “[Indexing](#)” section of this document.

1-Click Application Item-level Restore

You can restore items from Microsoft Exchange, Microsoft SQL Server and Oracle Databases with a single click using Veeam Backup Enterprise Manager. These capabilities were developed to elevate the 1st line support engineers, enabling them to recover mail items and other Microsoft Exchange objects without any direct visibility of the mailbox or database content. Database administrators are now able to restore Microsoft SQL Server and/or Oracle databases without addressing the backup team.

Microsoft Exchange Mailbox Items Restore

The process of restoring an Exchange mailbox is described in the [Backup and Restore of Microsoft Exchange Items](#) section of the Veeam Backup Enterprise Manager User Guide.

To create an application-aware image backup of Microsoft Exchange database VM ensure you back up at least one server holding the Client Access Server (CAS) role (This can be Exchange Server with the Mailbox Database role or a dedicated server. Contact the Exchange administrator if necessary). A server holding the CAS role is used to discover the mailbox location for the corresponding user. You should supply credentials for authentication with the CAS server on the **Configuration > Settings** page as described [here](#).

Microsoft SQL Server Database Restore

To perform database level restores of SQL Server databases using Enterprise Manager ensure you enable application-aware image processing for the corresponding backup job. To use point-in-time recovery enable log file backups of the Microsoft SQL Server VM. For more details refer to the [Backup and Restore of Microsoft SQL Server Databases](#) section of the Veeam Backup Enterprise Manager User Guide.

Oracle Database Restore

To perform database level, restore of Oracle databases using Enterprise Manager ensure you enable application-aware image processing for the corresponding backup job. To use point-in-time recovery, enable log file backups of the Oracle VM. For more details refer to the [Backup and Restore of Oracle Database](#) section of the Veeam Backup Enterprise Manager User Guide.

You have two options to restore through Enterprise Manager: 1-Click Restore to Original Location or Restore with Custom Settings. When restoring with custom settings make sure that the restore operator is enabled to also restore Oracle Databases. For more information see [providing access rights](#)

Note: Database restore from storage snapshots via Enterprise Manager is **not** supported.

Self-Service File Restore

In addition to 1-Click File-Level Restore Backup & Replication allows VM administrators to restore files or folders from a VM guest OS using a browser from within the VM guest OS, without creating specific users or assigning them specific roles at the Veeam Enterprise Manager level. To do this an administrator of the VM can access the self-service web portal using the default URL: “https://ENTERPRISE_MANAGER:9443/selfrestore”.

Tip: This feature is available only for the Windows-based VMs and requires Veeam Backup & Replication Enterprise *Plus* license. The VM needs to be in the same domain with the Enterprise Manager or in a trusted one (for SID resolution)

The process goes as follows:

1. During the backup of a VM with guest processing enabled, Veeam detects users who have local administrator access rights to that machine and stores this information in the Enterprise Manager database.
2. User enters the self-service web portal URL in the web browser and enters the account name and password to access the necessary VM guest OS.
3. After logging in the user is presented with the most recent restore point for that VM (the one this user authenticated to) on the **Files** tab of the web portal.

Note: This feature also works for backups from Veeam Agents for Windows stored on a Veeam Backup & Replication repository.

For more information on using this feature refer to the [Self-Restore of VM Guest Files](#) section of the Veeam Backup Enterprise Manager User Guide.

Self-Service Backup Portal for vCloud Director

Enterprise Manager in version 9.5 also supports a Veeam Self-Service Backup Portal that provides vCloud Director organization administrators with a UI for self-service operations on VMs protection. For that, a vCloud Director organization administrator can access the self-service portal using the default URL: “https://enterprise_manager_host_name:9443/vCloud/OrgName”.

1.10.3 RESTful API Service

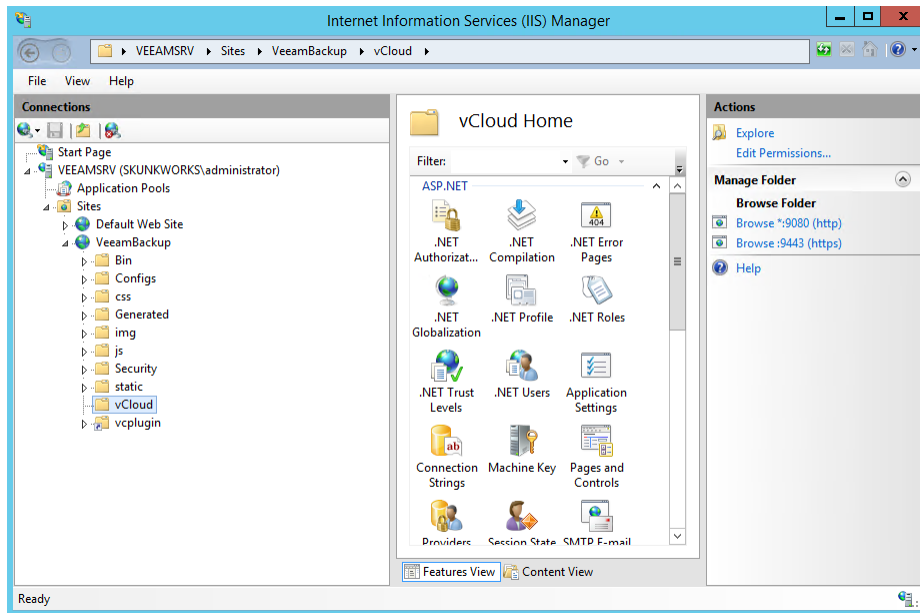
The RESTful API service is installed as part of Veeam Backup Enterprise Manager. To provide access to the API consider that authentication will take place through Enterprise Manager. Enterprise Manager user role assignments (**Portal User**, **Restore Operator**, **Portal Administrator**) and their access scopes access will be inherited by the RESTful API service. For more information on role assignment see the [Configuring Security Settings](#) section of the Veeam Backup Enterprise Manager User Guide.

1.11 Veeam vCloud Director Self-Service Portal

vCloud Director Self-Service Portal is designed for service providers running VMware vCloud Director and willing to offer self-service capabilities to their tenants. With the portal, users can configure their own backup jobs, and restore virtual machines and single files without any intervention from the service provider. From a technical point of view, the portal is an additional component of Veeam Enterprise Manager, and as such it is installed during the Enterprise Manager installation.

1.11.1 Requirements and limits

- Supported versions of vCloud Director are: 8.10, 8.0, 5.6, 5.5.
- only one vCloud Director installation (single cell or cell cluster) can be managed by a single Enterprise Manager. If a service provider has multiple vCloud Director installations, they will require the same amount of Enterprise Managers to protect all of them.
- vCloud Director Self-Service Portal cannot be installed on a different machine than Enterprise Manager. For this reason, plan the placement and the security of the Portal accordingly.

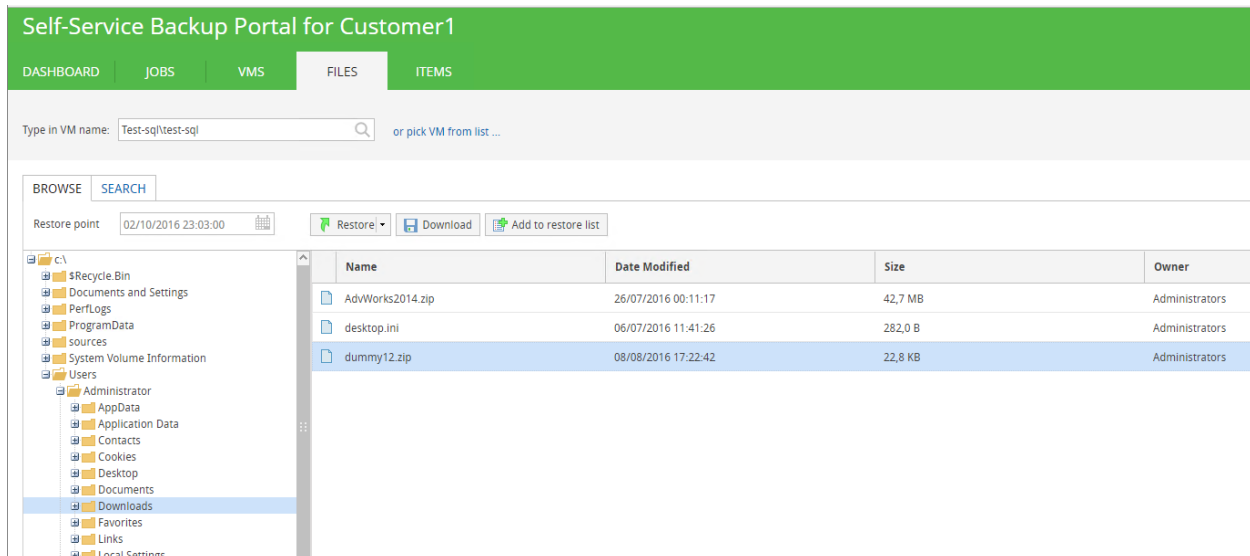


In order to harden the installation of the vCloud Portal, administrators can work on the IIS (Internet Information Server) website created by Veeam installer, and leverage all the security features available in IIS itself.

NOTE: Because the vCloud Portal is a subfolder of the Enterprise Manager installation, in order to modify its settings, the same settings need to be edited for the entire installation.

1.11.2 File Level Restore for Windows VMs

When a file needs to be restored for a Windows VM, a tenant uses the Self-Service Backup Portal to mount and browse a backup set (or he can use the search function to look for the same file):



The mount operation of the index is instantaneous, and a tenant can browse the content of the backup set to look for the file(s) he needs. Once the file has been identified, there are three different options:

Name	Date Modified
AdvWorks2014.zip	26/07/2016 00:11:17
desktop.ini	06/07/2016 11:41:26
dummy12.zip	08/08/2016 17:22:42

- tenant can download the file locally into his own workstation from the Self-Service Backup Portal
- tenant can restore the file in its original location inside the guest VM, overwriting the previous version
- tenant can restore the file in its original location inside the guest VM with a new name, so that both the new and the previous versions are kept

Option 2 and 3 use the same restore mechanism: Veeam first tries to connect to the Guest VM via the network, but since this is usually an isolated network inside vCloud Director and there is no direct connectivity between the vCloud Organization Network and the management network where Veeam (actually, the mount server) is deployed, VMware VIX API (up to vSphere 6.0) or VMware vSphere Guest Interaction API (starting from vSphere 6.5) are used to complete a networkless restore.

Initiated by	Started at	Status	Ended at	Total objects	Progress	Target
Customer1\customer1	03/10/2016 11:03:23	Success	03/10/2016 11:05:03	1	100%	Original

DETAILS	LOG
---------	-----


```

Starting FLR job for VM test-sql
FLR job started successfully on server 'vbr.skunkworks.local'
test-sql: File level restore started
test-sql: Mounting restore point
test-sql: Batch mode
test-sql: Using vbr as mount server
test-sql: Restoring file "c:\Users\Administrator\Downloads\dummy12.zip"
test-sql: Total size on disk: 22.8 KB
test-sql: Folders to restore: 0
test-sql: Files to restore: 1
test-sql: Restored "c:\Users\Administrator\Downloads\dummy12.zip"
test-sql: Dismounting restore point from VBR
test-sql: Restored data size: 22.8 KB
test-sql: Restored files: 1
test-sql: Restored folders: 0
test-sql: Restore job is completed
test-sql: Transmission agent has been stopped
FLR job completed successfully
Updating FLR session history
  
```

The file is restored in the original location, with the “RESTORED-“ prefix:

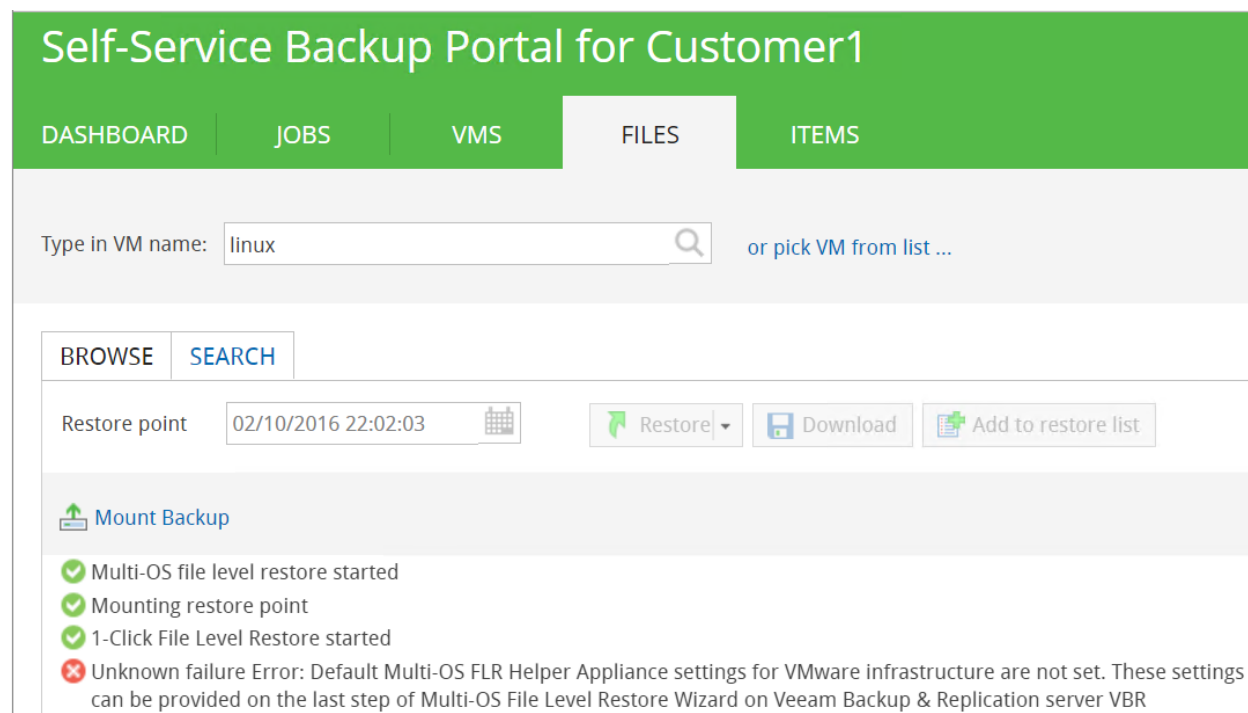
Name	Date modified	Type	Size
AdvWorks2014	7/26/2016 12:11 AM	File folder	
dummy12	8/8/2016 5:22 PM	File folder	
AdvWorks2014	7/26/2016 12:11 AM	Compressed (zipped) Folder	43,774 KB
dummy12	8/8/2016 5:22 PM	Compressed (zipped) Folder	23 KB
RESTORED-dummy12	8/8/2016 5:22 PM	Compressed (zipped) Folder	23 KB

**** NOTE:**** vSphere API used for these operations are mainly designed for executing commands inside the Guest OS, not for file transfers. For this reason, performance of large file restore operations may not be optimal. Please consider the “Download” option for such activities.

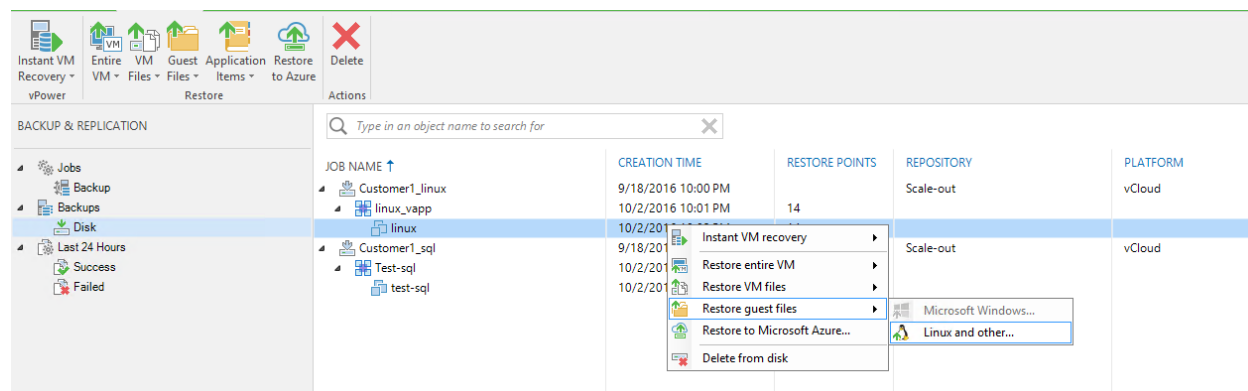
1.11.3 File Level Restore for Linux VMs

When a file needs to be restored for a Linux VM, some additional configuration needs to be completed by the service provider, otherwise the tenant will not be able to execute any restore.

Veeam Backup & Replication uses a Multi-OS FLR Helper Appliance virtual appliance to run file level restores for non-Microsoft file systems. This appliance is configured by a Veeam administrator before it can be used for any file restore. Otherwise, the first time a tenant tries to restore a file for one of his Linux VMs, he will receive this error in the Self-Service Backup Portal:



A Veeam administrator needs to configure the appliance from the Veeam Console. This can be achieved by initiating a file lever restore for any Linux VM:



The restore wizards asks to configure the Helper Appliance. The wizard suggests that the appliance should be connected to the same network where the guest VM is located, but it misses the other important information, that the FLR appliance needs to connect first of all to the Veeam mount server via port TCP/6170.

FLR Appliance Configuration

Specify ESX(i) server, resource pool and network settings for FLR helper appliance. Be sure to choose the same network where the VM you are restoring files to is located.

Host:

Statistics

VMs: 18 total

18 running

Resource pool:

Network:

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address:

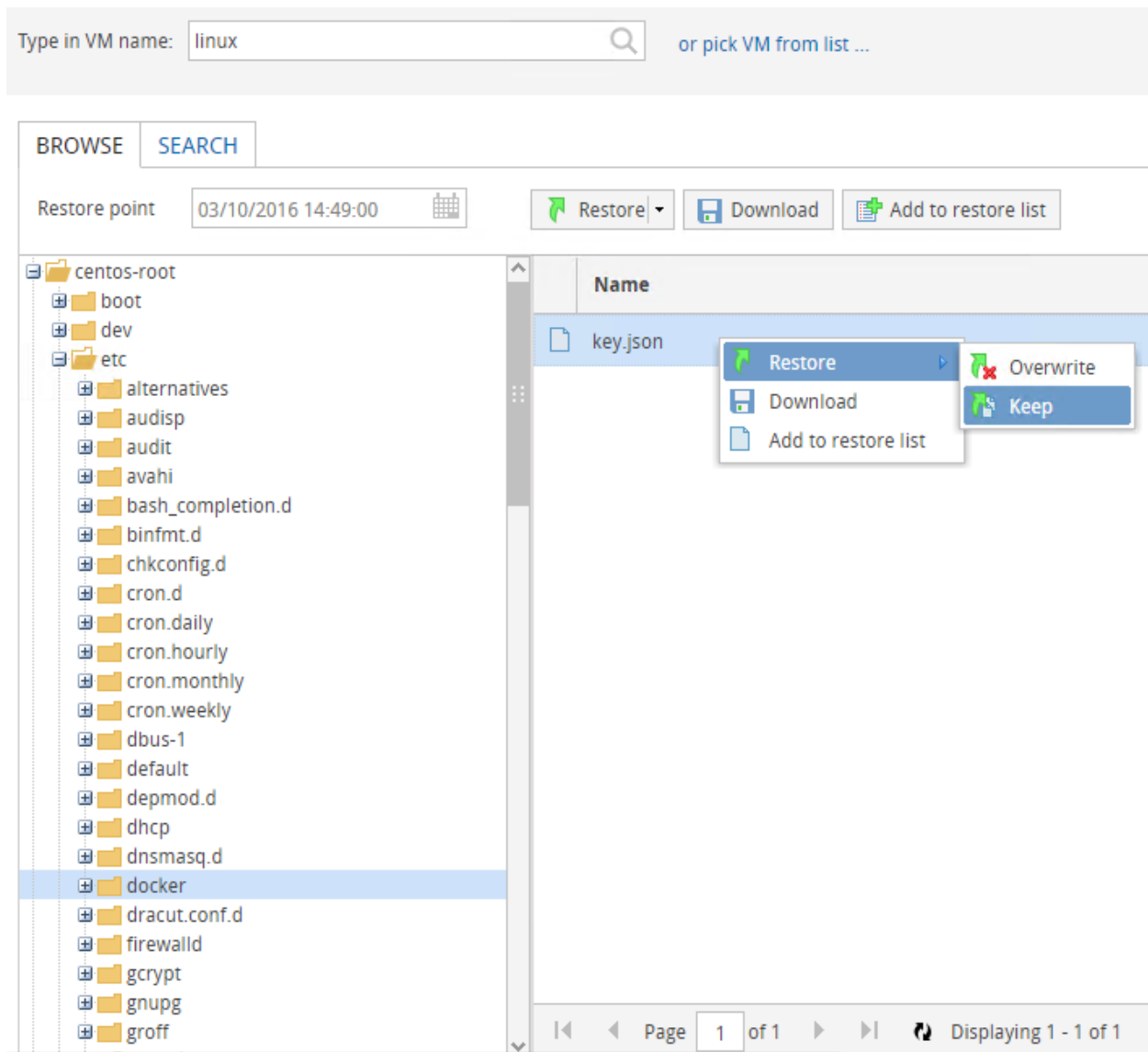
Subnet mask:

Default gateway:

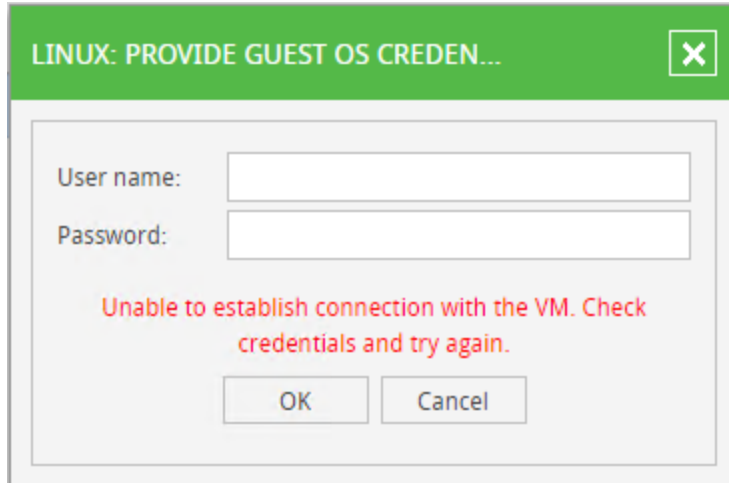
☐ Enable FTP server on appliance (advanced)

☐ Restore from Novell Storage Services (NSS) file system

In this example, **dvp-prodVM** is a management network where the different Veeam components are running. Once the FLR appliance is configured from the Veeam Backup Server, its configuration can be used also from the Self-Service Backup Portal by a tenant to mount the backup in the web interface:



The tenant has the three different options to restore one or more files from the backup set. While the Download option is immediately consumable by the tenant, the two Restore options require even more networking configurations, as the Veeam Backup Server would try to connect to the Guest VM to start the restore process from within the guest, but since there's no network connectivity between the two, it will fail:



For this reason, when Veeam Backup & Replication is used in completely fenced environments, we suggest to leverage the download options of the vCloud Self-service portal, and let tenant consume this portal to retrieve the files they need. To avoid a double operation of downloading the file to their workstations and then uploading them again to the linux machine, we suggest as a best practice to access the portal from a virtual machine already running inside the vCloud virtual datacenter. If the machine used to retrieve the files is not the final destination of the restored files, a tenant will just need a tool like WinSCP to transfer the file to the linux machine, but both the download and the scp copy will happen in a local network, with the files not even leaving the service provider datacenter.

1.11.4 Multiple concurrent restores

If the service provider is offering the self-service capabilities of the Veeam vCloud Portal, it could not be so uncommon that multiple tenants will start a restore operation at the same time.

Customer1 owns a single linux virtual machine called **linux**, inside the **linux_vapp** vcloud app. He wants to restore a file from the latest backup, so he starts the procedure from the self-service portal as described before; the customer selects the restore point and asks the software to initiate the mount operation.

The customer can browse the content of the backup, do searches, and download any file he may need. In the backend, Veeam Backup & Replication is using the FLR Appliance to mount the backup and read the linux filesystem used by the linux virtual machine.

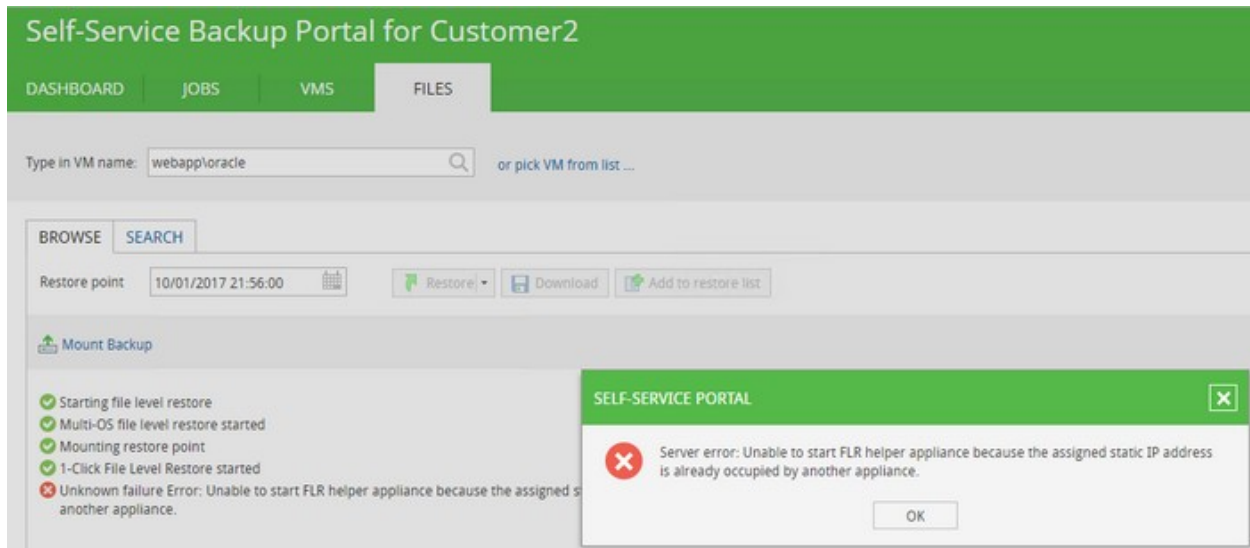
The machine is automatically disposed (powered off and deleted from the vSphere environment):

- After 15 minutes of inactivity from the vCloud Portal
- If the restore operator logs out from the vCloud Portal

For the entire duration of the restore process, the FLR will be powered on and used by the tenant.

The configuration of the FLR appliance can be done in two ways, by **assigning a fixed IP address** or by **leveraging a DHCP server**. As the appliance is often managed as a regular server, and to be sure it always have an IP address to start and execute the restores, many administrators configure it with a static IP address. The IP 10.2.50.126 in our example is a static IP address as you can see from the previous screenshot.

During a file restore from the portal, Veeam Backup & Replication uses the existing configuration of the FLR appliance, since there is no possibility to change the configuration from the portal itself. This works perfectly for one single restore operation, but if another tenant tries to do a file restore for one of his linux machines after the first customer is already performing a restore, an error will be returned:



Customer2 has to wait until **Customer1** has no restore operation running anymore, before he can start his own restore. This is done on purpose to avoid multiple FLR appliances to be spin up using multiple times the same IP address, thus leading to unexpected results.

To allow multiple concurrent restores, the solution is to configure the FLR appliance with a dynamic IP address, once a service provider has verified that a DHCP server is available in the port group where the appliance will be connected:

FLR Appliance Configuration

Specify ESX(i) server, resource pool and network settings for FLR helper appliance. Be sure to choose the same network where the VM you are restoring files to is located.

Host: Choose...

Statistics
VMs: 19 total
19 running

Resource pool: Choose...

Network: Choose...

☒ Obtain an IP address automatically

☐ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

☐ Enable FTP server on appliance (advanced)

☐ Restore from Novell Storage Services (NSS) file system

OK Cancel

With this configuration, multiple restore operations can be supported:

Name	Provisioned Space	Used Space	Memory Size	IP Address
VeeamFLR_linux_d4893489-ce52-4e01-ad39-f95_54cbfe61-1725-4566-9328-59b2e1f88701	17.16 GB	17.16 GB	1024 MB	10.2.50.85
VeeamFLR_oracle_2ac432cb-9265-4a24-81f9-1c_611a8622-49cc-48df-bf8f-1c778d003148	31.16 GB	31.16 GB	1024 MB	10.2.50.87

1.12 Indexing

1.12.1 Indexing and Search Overview

Veeam Backup & Replication performs backups at the image-level using APIs available from the underlying hypervisor. It has no direct visibility of the file structure after backup is finished. It is possible to Use File Level Recovery (FLR) wizard or Enterprise Manager to mount VMs from within a backup file and access/restore VM guest files. If a user wants to perform file restore from the central Enterprise Manager it is not possible within an acceptable timeframe to mount all backup files and VMs in it to find a file that the Enterprise Manager user wants to restore. To support advanced file-level restore scenarios Veeam offers the capability to index files on VMs being backed up. Indexing is available for both Windows & Linux VMs allowing users of Enterprise Manager to browse and search for the necessary files and to perform one-click file restores.

The sections below will outline some specific use cases for indexing and describe best practices and guidelines for sizing.

1.12.2 When to Use Indexing?

File-level indexing should be enabled only if you plan to utilize advanced file search and one-click file level restore capabilities of Enterprise Manager (including delegated restore). While indexing is a job-level setting you can use filters to index only a subset of files. It is possible to exclude specific VMs from indexing as described for example in [This section](#) of the Veeam Backup Enterprise Manager User Guide

1.12.3 How Veeam Indexing Works

Veeam indexing creates a separate index file in the catalog for each restore point. These index files are used by Veeam Enterprise Manager to support file browsing or searching without a need to mount the restore point to the mount server. Users can quickly search for files across multiple restore points viewing the required file history when looking for a specific version of a document. They can also select a specific VM and browse the file system to restore guest files.

Enterprise Manager allows for file-level restore functions to be delegated to a subset of users by leveraging the role-based access control.

During the VM backup job run the following operations are performed If configured:

1. Veeam accesses the guest OS (using credentials specified in the job settings) and injects a small run-time process to collect the list of files.
 - For Microsoft Windows-based VMs the process gathers file metadata by reading the MFT data of the supported file system (NTFS and ReFS).
 - For Linux-based VMs the process leverages the existing “locate” database that is commonly installed on most Linux distributions. Veeam uses the following software packages for it: mlocate, gzip and tar

These operations take place in parallel with the backup and do not increase the duration of the process. For more details on the indexing process refer to the [Veeam Backup Enterprise Manager User Guide](#).

1. Veeam Backup & Replication creates a catalog (index) of the VM guest OS files and stores index files on the Veeam backup server in the `C:\VBRCatalog\Index\Machines\{vm_name}` folder. Creation of the index is extremely fast and has minimal impact on network and VMware environment.
2. Once the index is created and stored on Veeam backup servers, the indexing service on Veeam Backup Enterprise Manager performs index copy — it aggregates index data for all VM image backups from multiple backup servers to the Enterprise Manager database while the original index files in the backup servers are deleted to conserve space. The consolidated indexes are stored on the Enterprise Manager server in the `C:\VBRCatalog\Index\Catalog` and are used for search queries .

Important To Note!

- To search within the index catalog it is necessary to deploy Veeam Backup Enterprise Manager, this component is in charge of catalog data replication and retention (see [this section](#) of the User Guide for more details).
- If you enable indexing without configuring Enterprise Manager the indexes in the `VBRCatalog` folder of the backup server will never be collected or deleted and will eventually fill up the disk drive.

1.12.4 Temporary VM Disk Usage

During the indexing process indexing information is temporarily stored on the local VM guest requiring additional free space on the system drive.

Windows VM

Temporary space required on the first drive in the VM (: \ drive):

100 MB per one million files

This was tested with one million files with 20 characters long filenames in one directory. Depending on the saved metadata and folder structure of the files, the value can be lower or higher.

Linux VM

Temporary space required in /tmp:

50 MB per one million files

Linux indexes require around 50% less space because `mlocate` does not index metadata such as timestamps and ownership.

1.12.5 Sizing Enterprise Manager Catalog

The Veeam Catalog Service is responsible for maintaining index data. When running on the backup server this catalog service will maintain index data for all jobs that run on that specific server as long as the backup data remains on disk. When running on the Enterprise Manager server the service will move index data from all managed backup servers into the Enterprise Manager local catalog deleting the files from the originating backup server catalog. So it should be sized appropriately to hold all data from the remote Veeam servers.

- When using a *Standard* license, Enterprise Manager will only keep index data for restore points still in repositories.
- For *Enterprise* and *Enterprise Plus* licenses, you can configure Enterprise Manager to keep indexes even longer, with the default being 3 months. This can significantly increase the amount of space required for the catalog.

Estimated used space of the final index file after compression is approximately 2 MB per 1,000,000 files for a single VM restore point on the Enterprise Manager server. The indexes are also stored in the backup files and temporary folders on the backup server.

Example

Below is an example that summarizes the information above. The example is given *per* indexed VM containing 10,000,000 files.

```
2 MB * 10 million files * 60 restore points per month * 3 months index
retention = 3.5 GB
```

1.12.6 Recommended Settings

Follow these recommendations when setting up Veeam indexing:

- Place the catalog on a dedicated volume of high performance disk. To change the default Veeam Catalog folder location refer to this Veeam Knowledge Base article: <https://www.veeam.com/kb1453>.
- You can enable NTFS compression on the catalog folder. This can reduce the space requirements by well over 50%. For very large catalogs (with 100s of VMs and 10's of millions of files) it can be more beneficial to use a Windows 2012 R2 volume with Data Deduplication enabled. This volume should be dedicated to index files and configured to run deduplication functions outside of the normal backup window.

- It is recommended to enable indexing only on VMs where the advanced search capabilities are necessary. Use filters to exclude unnecessary files from indexing (Windows system folder, Program Files and other system directories are excluded by default). For the Linux systems to be indexed, make sure they have **mlocate** or another compatible **locate** package installed.
- Configure index retention in Veeam Backup Enterprise Manager to the minimum necessary to meet the IT policy requirements. Index retention setting is available in the Enterprise Manager web console under **Configuration > Settings > Guest File System Catalog**.
- To enhance search performance, SSDs can be used. If you plan to index a very large number of VMs it is recommended to limit the search scope at restore to a single VM before you click the search button, this will bring faster results.

Notes:

To take advantage of indexing on SUSE Linux Enterprise Server (SLES) you must be running version 12 or above. In lower versions that do not contain by default the mlocate package you may try this OpenSUSE package <https://software.opensuse.org/package/mlocate>

Veeam Backup Enterprise Manager SQL database (*VeeamBackupReporting*) will not grow much while using indexing functions, as this database will only store the corresponding metadata.

1.12.7 Using Veeam Backup Search (Optional Component)

In its early versions Veeam did not have its own indexing engine, instead it used the Veeam Backup Search component to connect to the Microsoft Search Server 2010 that provided search capabilities. Now Veeam has its own built in indexing engine developed specifically for this purpose.

It is no longer a requirement to have a Veeam Backup Search configured as Veeam Integrated indexing engine can be more performant.

If you need to use that Veeam Backup Search component (and Microsoft Search Server) for indexing consider the following notes:

- Microsoft Search Server Express Edition can be used as it has no limitations for the number of indexed files.
- Other editions of Microsoft Search Server deliver higher scalability because Search Server components can be separately installed on multiple servers. If you are using Enterprise Manager consider that it can spread the load between multiple Microsoft Search Servers Express automatically.
- Microsoft Search Server functionality is used to scan content in the shared *VBRCatalog* folder on the Veeam Backup Enterprise Manager server and to create a content index on the Search Server; this content index is used to process search queries. For more details, refer to the [Veeam Backup Search](#) section of the User Guide.

Note: Though using content index streamlines the search process the index itself can require significant space on disk in `C:\VBRCatalog\Journal\[YYYY_MM]\[search-server]`.

- Search Server requires an SQL database for its operation. Consider that Microsoft SQL Server Express Edition leverages only one CPU which limits the Search Server performance. The database size supported by this edition is also limited (in particular, 10 GB for Microsoft SQL Server 2008 R2 Express Edition or later).

1.13 Proxy Servers - Intro

With backup proxies you can easily scale Veeam backup infrastructure based on the organization demands:

- In a **simple deployment** scenario for smaller environments or POC, the backup proxy is automatically installed on the Veeam backup server as part of the Veeam Backup & Replication installation.

- In **advanced deployments**, the backup proxy role is manually assigned to one or more Windows servers. This approach allows for offloading the Veeam backup server, achieving better performance and reducing the backup window.

Backup proxies can be deployed both in the primary site, where the backup server is located, or in a remote site where additional infrastructure needs being backed up. A proxy server can be installed on any managed Microsoft Windows server added to the backup infrastructure. Depending on whether the proxy server is installed on a physical or virtual machine, different transport modes are available.

A backup proxy handles data traffic between the vSphere or Hyper-V infrastructure and Backup & Replication during backup, replication (at source and target), VM copy, VM migration jobs or VM restore. They are also used to detect and scan snapshots to enable Veeam Explorer for Storage Snapshots features when any supported primary storage is added to the backup server.

Backup proxy operations include the following:

- Retrieving VM data from production storage
- In-line source side data deduplication to skip whitespace and redundant blocks reported by vSphere Change Block Tracking (CBT), Veeam File Change Tracking (FCT) for Hyper-V versions from 2008 R2 to 2012 R2 or Resilient Change Tracking (RCT) for Hyper-V 2016.
- Performing in-line compression and deduplication before sending it to the backup repository (for backup) or another backup proxy (for replication)
- BitLocker: Applies to VMs running Windows OS and using NTFS. For more information, see the corresponding section of this guide > [Deduplication and Compression - BitLocker](#)
- AES256 encryption, if enabled.

Technically a backup proxy runs a light-weight transport service that takes a few seconds to deploy. When you add a Windows-based server to Veeam backup management console assigning the proxy role to it, Backup & Replication installs the necessary components, and starts the required services on that server. Any host in a Hyper-V cluster is automatically enabled as proxy server, when it is added to the infrastructure. When a job is started, the backup server manages the dispatching of tasks to proxy servers using its built-in *Intelligent Load Balancer* (ILB).

1.13.1 Intelligent Load Balancing

To specify the threshold for proxy load an administrator uses the **Max concurrent tasks** proxy setting (one task will be consumed for processing a single VM disk), Backup & Replication uses a unique load balancing algorithm to automatically spread the load across multiple proxies. This feature allows you to increase backup performance, minimize backup time window and optimize data flow.

The default proxy server is configured for 2 simultaneous tasks at installation, whereas subsequently added proxy servers analyze the CPU configuration. The proxy server automatically proposes configuring 1 task per CPU core. During deployment, it is determined which datastores or CSV the proxy can access. This information is stored in the configuration database, and is used at backup time to automatically select the best transport mode depending on the type of connection between the backup proxy and datastore.

After the algorithm identifies all existing backup proxies it distributes tasks via the built-in Real-time Scheduler (RTS):

1. It discovers the number of tasks being processed at the moment by each proxy and looks for the server with the lowest load and the best connection.
2. All tasks are added to a “VMs to process” queue. When a proxy task slot becomes available, RTS will automatically assign the next VM disk backup task to it.
3. Priority goes to the disk that belongs to an already processed VM, after that VMs of already running jobs have next higher priority.

Tip: At the repository, which writes the backup data, only one thread is writing to the backup storage *per running job*. If few jobs with a high number of VMs are processed simultaneously, you may experience that these threads cannot fully utilize the available backup storage performance. If throughput per I/O stream is a bottleneck, consider enabling [per VM backup files](#).

Tip: Default recommended value is **1** task per core/vCPU, with at least 2 CPUs. To optimize the backup window, you can cautiously oversubscribe the **Max concurrent tasks** count, but monitor CPU and RAM usage carefully.

1.13.2 Parallel Processing

Veeam Backup & Replication supports parallel processing of VMs/VM disks:

- It can process multiple VMs within a job simultaneously, increasing data processing rates.
- If a VM was created with multiple disks, Veeam will process these disks simultaneously to reduce backup time and minimize VMware snapshot lifetime.
- RTS gives priority to currently running parallel processes for VM disk backups.

To achieve the best backup window it is recommended to slightly oversubscribe the tasks slots, and start more jobs simultaneously. This allow Veeam to leverage the maximum of the task slots and lead into an optimal backup window.

Note: Parallel processing is a global setting that is turned on by default. If you had upgraded from older versions please check and enable this setting.

1.13.3 Backup Proxy Services and Components

Veeam backup proxy uses the following services and components:

- **Veeam Installer Service** - A service that is installed and started on the Windows server once it is added to the list of managed servers in the Veeam Backup & Replication console. This service analyses the system, installs and upgrades necessary components and services.
- **Veeam Transport Service** – A service responsible for deploying and coordinating executable modules that act as “data movers”. It performs main job activities on behalf of Veeam Backup & Replication (communicating with VMware Tools, copying VM files, performing data deduplication and compression, and so on).
- **VeeamAgent.exe process** - a data mover which can be started multiple times (on demand) for each data stream on the proxy. These processes can operate in either read or write mode. When used on a proxy server for backup, they are only performing read operations, while “write” mode is used for writing data on a target backup proxy (replication). Veeam agents in write mode are also used on all repository types, but will not be discussed in this chapter.

1.14 Proxy Server - VMware vSphere

Like any backup vendor using VMware vStorage API for Data Protection (VADP), Backup & Replication is using the VMware Virtual Disk Development Kit (VDDK) within the Veeam Transport Service. This is necessary for management interaction with vCenter and ESXi hosts, while in some scenarios, VDDK is bypassed in favor of Veeam *Advanced Data Fetcher* for performance reasons.

1.14.1 Storage optimizations

Stock VDDK transport modes have some limitations, such as being unable to process multiple disks in parallel when using [virtual appliance transport mode](#) (hot-add), introducing excessive VMFS metadata updates when performing

replication, or being unable to backup from NFS based datastores. To overcome these limitations, Veeam introduced logic to bypass VDDK, when it is more optimal to do so.

1.14.2 Veeam Advanced Data Fetcher (ADF)

Veeam Advanced Data Fetcher (ADF) adds increased queue depth for >2x read performance on enterprise storage arrays. ADF is supported for Backup from Storage Snapshots, Direct NFS and virtual appliance mode.

Other enhancements include:

- a proprietary NFS client for backing up VMs on NFS datastores
- parallel processing of multiple VM disks when backing up via hot-add
- parallel processing of multiple VM disks during restore
- bypass VDDK when performing replication or VM restores via hot-add, to avoid excessive VMFS metadata updates
- allow restore via Direct SAN

1.14.3 Intelligent Load Balancing

When it comes to distribute the workload in VMware vSphere environments, first Backup & Replication checks if data processing can be assigned to a backup proxy with the following priority:

1. Direct Storage Access (which includes VDDK based Direct SAN or Veeam proprietary Direct NFS).
2. Virtual appliance mode (hot-add)
3. Network Block Device (NBD)

For more details, see the [Transport Modes](#) section of this guide.

1.15 Transport Modes

Job efficiency and time required for its completion are highly dependent on the data transport mode. Transport mode is a method used by the Veeam proxy to retrieve VM data from the source host and write VM data to the target destination.

1.15.1 Direct Storage Access

In this mode, the backup proxy server has direct access to the storage volumes on which VMs reside. When configured, the backup proxy will retrieve data directly from the storage, bypassing the ESXi infrastructure.

Depending on storage protocols utilized, the proxy can be deployed as follows:

- On a physical server for FibreChannel, FCoE, iSCSI or NFS
- On a virtual machine for iSCSI and NFS

Both options can be used for [Backup from Storage Snapshots](#). When used with NFS datastores or Backup from Storage Snapshots, Direct Storage Access mode will also utilize the [Advanced Data Fetcher](#).

1.15.2 Virtual appliance mode

As the disks are hot-added, you may find the virtual appliance mode referred to as `hotadd` in documentation and logs.

To work in this mode the backup proxy must be deployed as a VM. For smaller deployments (e.g., several branch offices with a single ESXi host per each office) you can deploy a virtual backup proxy on a ESXi host that has access to all required datastores. When backup or replication takes place and a VM snapshot is processed the snapshotted disks are mapped to the proxy to read data (at backup) and write data (at restore/replication); later they are unmapped.

1.15.3 Network mode

You may find network mode referred to as `nbd` in documentation and logs.

The most widespread backup method is network mode, which transports VM data through the VMkernel interfaces of the VMware ESXi host on which the VM resides.

The benefit of using NBD is the fact that it requires no additional configuration, and is supported regardless of physical or virtual proxy deployments, or storage protocols used (including local storage, VMware Virtual Volumes or VMware vSAN). This is also the reason NBD is used as the fallback method, in case Backup from Storage Snapshots, Direct Storage Access or Virtual Appliance backup modes fail.

The only requirement is the proxy being able to access ESXi hosts on port 902/tcp. NBD backup throughput is typically limited to using up to 40% of the bandwidth available on the corresponding VMkernel interfaces. If NBD-SSL is enabled, the throughput is typically 10% slower than regular NBD. NBD-SSL is *enforced* for ESXi 6.5 hosts. Read more about this in [Virtual Appliance Mode section - vSphere 6.5 and encryption](#).

Starting from vSphere 6.5b (ESXi build 5146846 and VDDK libraries version shipped with Veeam B&R update 3) unencrypted is available again and encrypted VMs can be backed up using regular NBD mode. [More info regarding the content of the VMware vSphere update can be found here](#).

The following sections explain transport modes in detail.

1.16 Direct Storage Access

Direct Storage Access covers two transport modes: VDDK based “Direct SAN”, and “Direct NFS” which utilizes a proprietary Veeam NFS client. Direct NFS also utilizes [Advanced Data Fetcher \(ADF\)](#).

The Direct SAN mode uses a direct data path (Fibre Channel or iSCSI) between the VMFS datastore and the backup proxy for data transfer. The proxy requires read access to the datastores so Fibre Channel zoning or iSCSI initiator configuration and LUN masking on the storage array must reflect this. In most cases, the Veeam backup proxies are added to the same “host group” on the storage as the existing ESXi hosts, in order to ensure all LUNs are masked correctly.

To use Direct NFS backup mode, the proxies need access to the NFS network and must be configured in the NFS server’s “exports” for read and/or write access. As NFS based storage uses IP, the real-time scheduler (RTS) will ensure to always use the nearest backup proxy (by means of the fewest network “hops”). This is especially useful if the NFS network traffic has to cross IP routing devices.

If write access is provided, Veeam will automatically perform full VM restore via Direct Storage Access for thick provisioned VMs.

1.16.1 Pros

- Direct Storage Access mode provides very fast and the most reliable predictable backup performance (typically using 8 Gb Fibre Channel or 10 GbE for iSCSI and NFS).
- Produces zero impact on vSphere hosts and VM production networks for backup data transport.
- It is possible to perform full VM restore using Direct Storage Access. This mode will be used automatically if eligible backup proxies are available in the backup infrastructure and if the VM disks are thick provisioned.
- Direct Storage Access is the fastest backup and restore mode for NFS datastores. It uses multiple concurrent read and write streams with an increased queue depth via ADF.
- Direct Storage Access for NFS datastores will mitigate the “VM stun” issues that may be caused by Virtual Appliance Mode (hot-add).
- Direct Storage Access for FC and iSCSI can be used for replication at the target for the initial replication (with thick provisioned disks) only. For NFS datastores, Direct Storage Access can be used for initial and incremental replication passes. There are no differences on the source replication proxy.

1.16.2 Cons

- Typically, Direct Storage Access requires a physical server for Fibre Channel, iSCSI or NFS connection. For virtual only deployments, Direct Storage Access for iSCSI and NFS is possible, but would transport the data through networks of the ESXi hosts, typically making hot-add the more efficient choice.
- Restore via Direct Storage Access using Fibre Channel or iSCSI is possible only for thick-provisioned VM disks. At restore the data stream needs to be coordinated in the background with vCenter or an ESXi host which can slow down the restore speed. Consider adding additional hot-add proxy servers for restore (FC/iSCSI only).
- Direct SAN mode (FC/iSCSI only) is the most difficult backup mode to configure as it involves reconfiguring not only the storage but also the SAN, (Fibre Channel zoning, LUN masking, or reconfiguration of iSCSI targets) to provide the physical proxy server(s) with direct access to the production VMFS datastores. When such configuration has been implemented it is extremely important to ensure that HBAs, NIC drivers and firmwares are up-to-date and that multi path driver software (e.g. MPIO) is properly configured.

For more information about configuring Direct Storage Access refer to FAQ at [Veeam Community Forums: Direct Storage Access Mode](#)

1.16.3 Example

If datastores or virtual raw device mapping (vRDM) LUNs are connected via shared storage using Fibre Channel, FCoE or iSCSI, you may add a backup proxy as a member to that shared storage using LUN masking. This will allow for accessing the storage system for backup and restore.

Ensure that a connection between the storage and backup proxy can be established. Verify FC HBAs, zoning, multi-path, driver software and iSCSI configurations including any network changes. To test the connection, you may review volumes visible in Windows Disk Management (as offline), adding one disk per storage system at a time. Once the initial connection has been verified, add the remaining volumes for that storage array.

1.16.4 Recommendations

- Use the multipath driver software of the storage vendors choice (preferred integration into Microsoft MPIO) to avoid disk or cluster failovers at storage level. This will also prevent the whole storage system from being affected by possible failovers if wrong data paths are used. It is highly recommended to contact the storage vendor for optimal settings.

- If you attach a large number of volumes to the backup proxy, consider that logging for the process of searching for the correct volume during the job run can require extra processing time per VM disk (as well as for overall volume count). To avoid Veeam logging becoming a bottleneck you can disable logging for this particular task this with the following registry setting:
- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication
- Key: VDDKLogLevel
- Type: REG_DWORD
- Value: 0 (to disable)
- Default: 1

Note: As this reduces the amount of information in debug logs, remember to enable it again when working with Veeam support (to facilitate debugging of Direct Storage Access related challenges).

- To achieve performance/cost optimum, consider using fewer proxies with more CPU cores available. This will help to fully utilize the HBA or NIC capacity of each proxy server. A 2 CPU System with 2x 12 cores is considered a good configuration balanced between throughput and costs.

1.16.5 Security Considerations for Direct SAN

During deployment of the proxy role to a Windows VM, Backup & Replication uses the following security mechanisms to protect them:

- Windows SAN Policy is changed to “Offline (shared)”. This prevents Windows from automatically bringing the attached volumes online and also prevents Windows write operations to the volumes. During Direct SAN restore, if the disks are offline, the proxy will attempt bringing the volume online, and verify that it is writeable. In case the operation fails, restore will failover to using NBD mode through the same proxy.
- Veeam deploys VMware VDDK to the backup proxy. In most cases, VDDK coordinates read and write operations (Direct SAN restore) with VMware vSphere allowing VMware’s Software to control the read and write streams in a reliable manner.

If necessary, you can take additional measures as follows:

- Disable automount. Open an elevated command prompt and disable automount using the following commands:

```
diskpart
automount disable
```

- Disable Disk Management snap-in with:
Group Policy\User Configuration > Administrative Templates > Windows Components > Microsoft Management Console > Restricted/Permitted snap-ins > Disk Management.
- Restrict the amount of users with administrative access to proxy servers.
- Present LUNs as read-only to the backup proxy server. This capability is supported by most modern storage. When possible, implement read-only LUN masking on the storage system or read-only zoning on the Fibre Channel switches (possible on most Brocade variants).

If a VMFS datastore is manually brought online in Windows Disk Management by mistake, and disk resignaturing is initiated, the datastore will become unavailable, and VMs will stop. Please contact VMware Support for assistance with recreating the VMFS disk signature. For more information on Windows re-signaturing process and VMware datastores please refer to [VMware KB1002168: Unable to access the VMware virtual machine file system datastore when the partition is missing or is not set to type fb](#)

1.16.6 Summary

Use Direct Storage Access whenever possible for fast backups and reduced load on the ESXi hosts. Consider using hot-add proxies, as these typically restore faster than Direct SAN restores. Direct SAN uses VDDK, which can cause excessive metadata updates while hot-add restores bypass VDDK.

For NFS datastores, Direct NFS is the best choice for both backup and restore. It delivers the highest possible throughput, without any negative side effects. You can use it for virtual and physical proxy deployments.

1.17 Virtual Appliance Mode

As the default setting, virtual appliance mode (`hot-add`) has become quite popular for all-in-one deployments of Veeam Backup & Replication within virtual machines (for details, see the [Deployment Scenarios](#) section of the User Guide). It is also often used, when Veeam is deployed in branch office configurations (ROBO).

This mode supports a 100% virtual deployment, and uses the VMware ESXi storage I/O stack, providing very efficient backups and having very little overhead in terms of throughput. During backup or replication, while the original VM is running off of a VM snapshot, the original virtual machine disks (VMDK) are mounted via SCSI hot-add to the backup proxy server. Once the backup or replication job finishes, the disks are unmounted from the proxy server, and the VM snapshot is committed.

Note: For more information on how it works, refer to the section “[Data Backup and Restore in Virtual Appliance Mode](#)” in Veeam Help Center.

As an example, virtual appliance mode is a good choice for highly dynamic environments, where it can be difficult for backup administrators to maintain access to newly created datastores for Direct Storage Access. Prerequisites for using virtual appliance mode are described in the following knowledge base article: [Appliance Mode \(Hotadd\) Requirements and Troubleshooting](#)

When planning for the Virtual Appliance mode for a backup proxy consider the time required for actual hot-add operations (such as adding and removing VM disks from the source virtual machine) it can add up to 1-2 minutes per VM. For a backup job containing 100 virtual machines this could result in more than two hours of adding and removing disks with no actual data processing. To mitigate the issue enable parallel processing and process multiple disks from the same virtual machine simultaneously (using this transport mode).

Tip: It is recommended to benchmark how such operations affect the backup window by monitoring a test job in the vSphere console.

Veeam developed Direct Storage Access for NFS based datastores to overcome the problems with disk hot-add and release which causes significant stuns for NFS based VMs). Direct Storage Access should be used for all virtual and physical proxy deployment to backup and restore NFS datastore based VMs.

1.17.1 Pros

- Using the Virtual Appliance mode for proxy servers enables a fully virtual deployment.
- As the proxy will perform source side data deduplication and compression, this mode will provide satisfactory performance in environments running 1 GbE configurations.
- Virtual appliance mode utilizes Veeam Advanced Data Fetcher (ADF), providing significant increase in throughput for enterprise class storage.

1.17.2 Cons

- If working in this mode the backup proxy will occupy the virtual infrastructure resources impacting consolidation ratio. This could ultimately require additional physical ESXi hosts and licensing.
- This mode requires additional planning and configuration in the enterprise environments because of the additional large disk Hot-Add processes in VMware vSphere.
- In situations with a high number of VMware clusters with individual datastores a minimum of one proxy per cluster is needed, this can increase management overhead.

1.17.3 Considerations and Limitations

Additional load is put on the vCenter Server and ESXi hosts as each disk is mapped and unmapped (disk hot-add) at the backup proxies.

Note: For more information see vCenter Server connection overview in the “Veeam Backup & Replication Server” section of this guide.

It may occur that VMware API reports that unmap and snapshot commit were done correctly but a snapshot file still remains on disk. These “orphaned snapshots” will grow over time and can fill up the datastore leading to downtime. To mitigate the issue, Veeam implemented the following functionality:

- Veeam Snapshot Hunter. This feature automatically initiates disk consolidation for VMs in the “Virtual machine disks consolidation is needed” state. For more information please see [Snapshot Hunter](#) section
- Bypassing Virtual Disk Development Kit (VDDK) processing to overcome some limitations and performance challenges, in particular:
 - Veeam can back up multiple disks of VM in parallel on same proxy (default number is 4).
 - Typical “hot-add I/O bursts” during hot-add operations are mitigated by bypassing VMware VDDK during restores and replication.
 - When performing writes via hot-add and VDDK, excessive metadata updates on the VMFS datastore will occur. This significantly impacts performance for other workloads on the datastore, and slows down restore throughput. Bypassing VDDK helps overcoming this limitation
- To avoid some VMware issues related to NFS datastore and hot-add processing (described at <https://kb.vmware.com/s/article/2010953>), enable a specific setting that will process VM backups only on backup proxies that run on the same host. For details see <https://www.veeam.com/kb1681>. To avoid this completely, it is recommended to use the Direct NFS backup mode for backup and restore of NFS datastore based VMs.

Note: For additional tips refer to the [Impact of Snapshot Operations](#) section of this guide.

1.17.4 vSphere 6.5 and Encryption

Virtual appliance mode is typically the best choice to ensure data availability for vSphere 6.5 clusters with encrypted virtual machines. In order to support backup of encrypted virtual machines, the virtual backup proxy must be encrypted within the same encryption domain (using the same KMIP server).

Backup modes Direct Storage Access and Backup from Storage Snapshots are unavailable for encrypted virtual machines. NBD will be slower as virtual appliance mode as vSphere 6.5 also enforces SSL/TLS encryption for network mode (NBD). Thus, virtual appliance mode will be the best performing choice, and it reduces host CPU load.

1.17.5 Recommendations

- Virtual appliance mode should be used when it is not possible to leverage Direct Storage Access, for example in the case of local datastores, Virtual Volumes (VVOL) or vSAN.
- You will need at least one type of (virtual) SCSI controller added to Proxy Server VM that is used somewhere at the VMs in your infrastructure to allow VMware to HotAdd the VM disks at backup.
- Add an extra SCSI controller to allow for more VM disks processing in parallel (check the corresponding Veeam proxy settings, default value is 4). The limit for a single controller is the maximum number of devices per SCSI controller (15). Max SCSI controllers per VM is 4 = 60 disks max. Adding one additional SCSI controller is usually sufficient.
- When deploying hot-add backup proxies avoid cloning existing VMs as this may lead to identical UUIDs and cause hot-add operations to fail.
- You may re-use any existing Windows server VM (to save on licensing). The Veeam data mover process runs with 'below normal' priority by default.

Note: Changed block tracking (CBT) will be disabled for these hot-add proxies. Consider that it may impact the backup window in case the said virtual machines should be included in backup or replication jobs.

Useful links

- Specific client OS limitations for Hot-Add processing are documented in [Veeam Backup & Replication Release Notes](#),
-

Appliance Mode (Hotadd) Requirements and Troubleshooting

- [How to test hotadd manually](#)

1.18 Network Mode

Network mode is by far the easiest backup mode to implement as it requires no additional configuration. With this mode, Veeam uses the same interface to inspect, backup and restore VMware configuration files as well as to read Change Block Tracking (CBT) information.

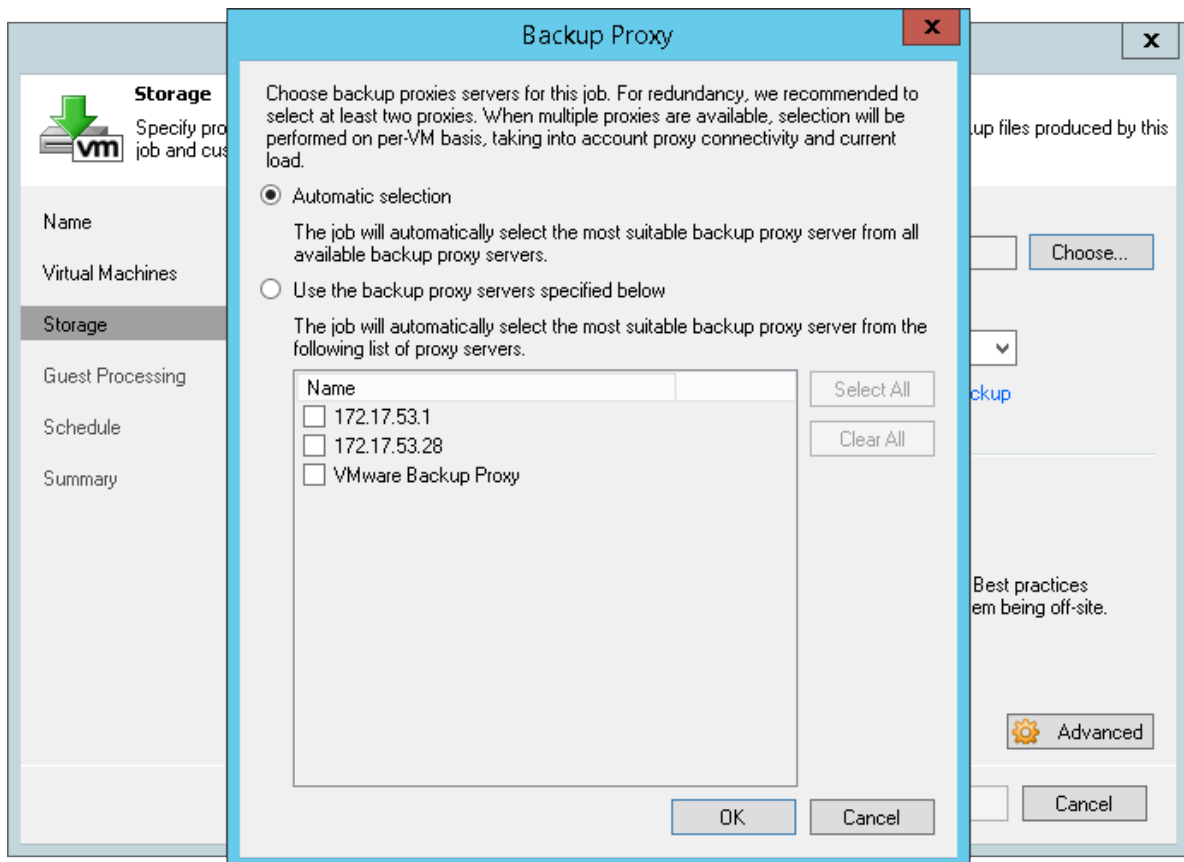
In this mode, the backup proxy will query vCenter for the name of the ESXi host on which the VM scheduled for backup resides. Typically, hosts are added to vCenter using FQDN, which means NBD relies heavily on properly working DNS resolution. Regardless if the ESXi hosts are connected to vCenter using a VMkernel interface on an isolated management network, VADP backup solutions will attempt to connect to this same interface. Please see the section on [DNS Resolution](#) for more information on how to override the default interface used for NBD backups.

As the only prerequisite, the backup server and proxy server requires ports 443/tcp and 902/tcp being open to the ESXi hosts.

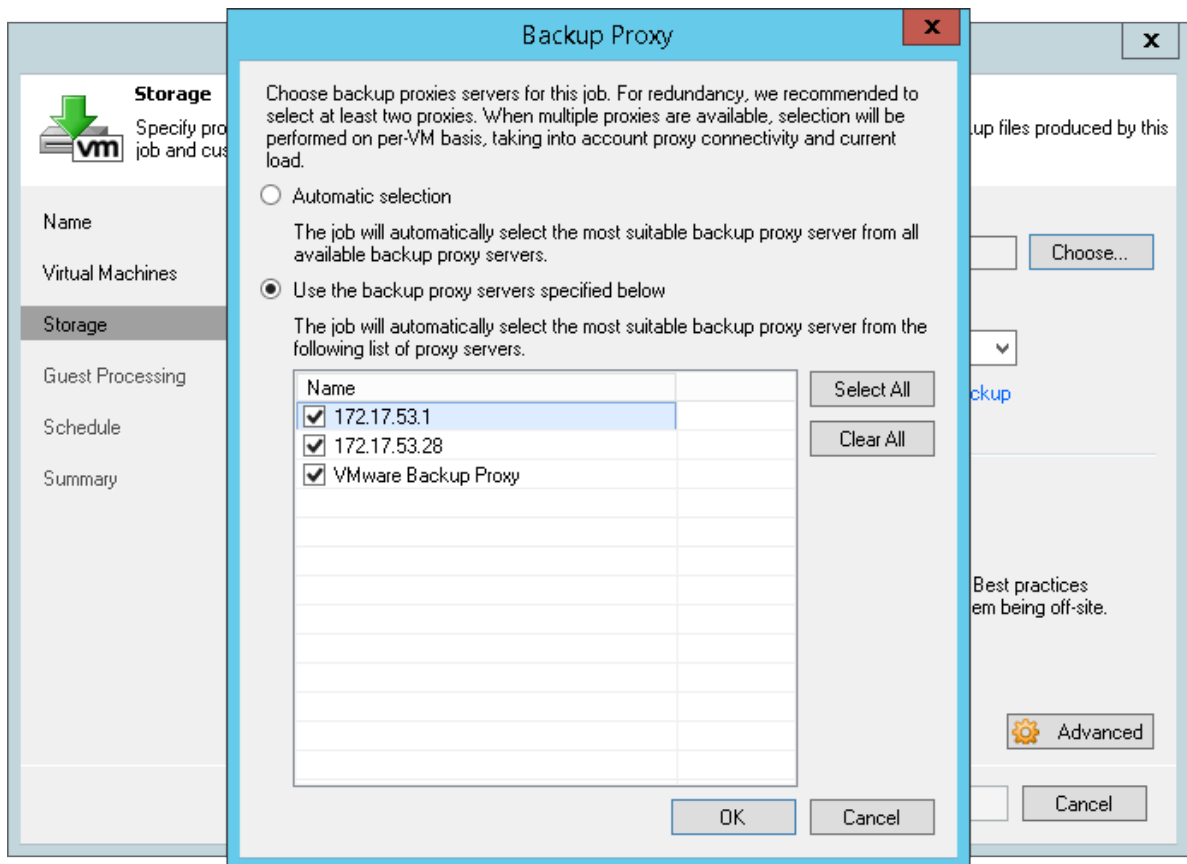
Note: It is highly recommended to maintain a good network connection between the VMware ESXi VMKernel port and Veeam Backup & Replication as it will be used by many other features like Instant VM Recovery, Virtual Lab and SureBackup, Linux FLR appliance, config files backups etc.

For load balancing, Veeam uses a selection of proxy servers based on the network subnet:

- Backup proxies in the same subnets as the VMKernel interfaces are selected if you have the **Automatic Selection** proxy setting configured in the backup jobs.



- If no proxy servers are available within same subnet as the VMKernel interface of the ESXi host, you may have to manually select the proxies that are most suitable to process the backup job. It is recommended not to use **Automatic selection** in such scenarios, as proxies might be selected which would transfer data across too many network hops (or even across WAN links). You can manually select all eligible proxies to enable load balancing.



- In case you work with several branches or datacenter environments it is also recommended that you manually choose the proxies (per site) in the job settings to reduce the time spent by the Real Time Scheduler to determine eligible backup proxies.

1.18.1 Pros

- Network mode can be used for both backup and restore with same speed.
- Works with both physical and virtual backup proxies.
- Being the most mature of all transport modes, it supports all types of storage.
- Is recommended for NFS based storage in cases where Direct NFS is unavailable. Using NBD will minimize VM stuning. See also the “[Considerations for NFS Datastores](#)” section of this guide.
- Performance on 10 GbE VMkernel interfaces typically provide around 400-500 MB/s of throughput per host.
- As data transfers initiate very quickly, network mode is preferable for processing incremental backups on relatively static virtual machines (VMs generating a small amount of change).
- It can be helpful when dealing with many clusters with individual storage configurations (e.g. hosting providers). In such deployments, using network mode for data transfer can help reducing Veeam footprint and costs as well as to increase security (if compared to other modes and storage configuration).

1.18.2 Cons

- Typically, network mode uses only up to 40% of the available bandwidth of the external VMKernel interface due to throttling mechanisms implemented on the management interfaces.

- It can be even slower on 1 Gb Ethernet (about 10-20 MB/s) due to throttling mechanisms, so especially restores via network mode can take very long.

Tip: Please see the section on [DNS Resolution](#) for information on how to override the network interface used for NBD backups e.g. when both 1 GbE and 10 GbE VMkernel interfaces are available. It is preferred to force usage of 10 GbE for highest possible throughput in such cases.

1.18.3 Recommendations

When you choose network mode (NBD), you entirely avoid dealing with hot-add vCenter and ESXi overhead or physical SAN configuration. NBD is a very fast and reliable way to perform backups. In emergency situations when you need fast restore the following tips can be helpful:

- Consider setting up at least one virtual backup proxy for hot-add based restores. This will result in higher throughput and thus lower RTO.
- Consider restoring to a thin disk format and later use standard VMware methods to change the disk format to thick disk if needed, as thin disk restores have to transport less data.
- Another way to speed up restores is using Instant VM Recovery with Storage vMotion (if license is available) as it is not affected by the same throughput limitations as the VMkernel interfaces.

When using NBD for backup, please consider the following:

- As there is no overhead on backup proxies (like SCSI hot-add or
- searching for the right volumes in Direct Storage Access),
- network mode can be recommended for scenarios with high-frequency backups or replication jobs, as well as for environments with very low overall data and change rate (VDI).
- To protect VMware, Veeam reduces the number of permitted NBD connections to 28. Please see the corresponding section in [Interaction with vSphere](#) for more information on how to alter the configuration using registry keys.

1.19 Backup from Storage Snapshots

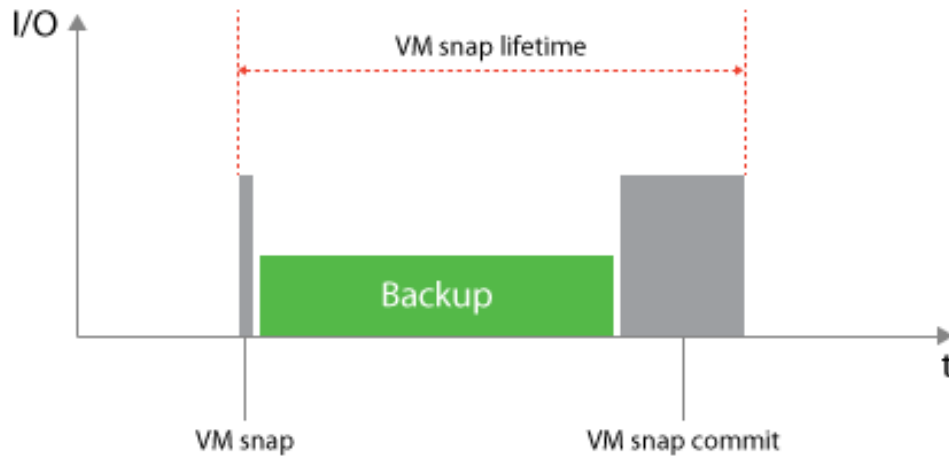
Veeam Backup & Replication offers integration with certain storage arrays for VM snapshot offloading. The number of supported storage vendors and arrays is constantly growing, a current list can be reviewed here:

[Backup from Storage Snapshots for the world's leading storage providers](#)

Licensing and system requirements are described in the Veeam User Guide: [Backup from Storage Snapshots](#).

The storage integration covered in this section is VMware only and does not apply for Hyper-V. Any protocol supported by Backup from Storage Snapshots will utilize the Advanced Data Fetcher to optimize for retrieving data on enterprise grade storage.

Backup from Storage Snapshots (BfSS) is a feature included in the storage array integrations and a way to optimize and enhance VM backups in a very easy way. The main objective for implementing BfSS is to minimize the lifetime of a VM snapshot, which reduces the time for VM snapshot commit and I/O in the vSphere environment.



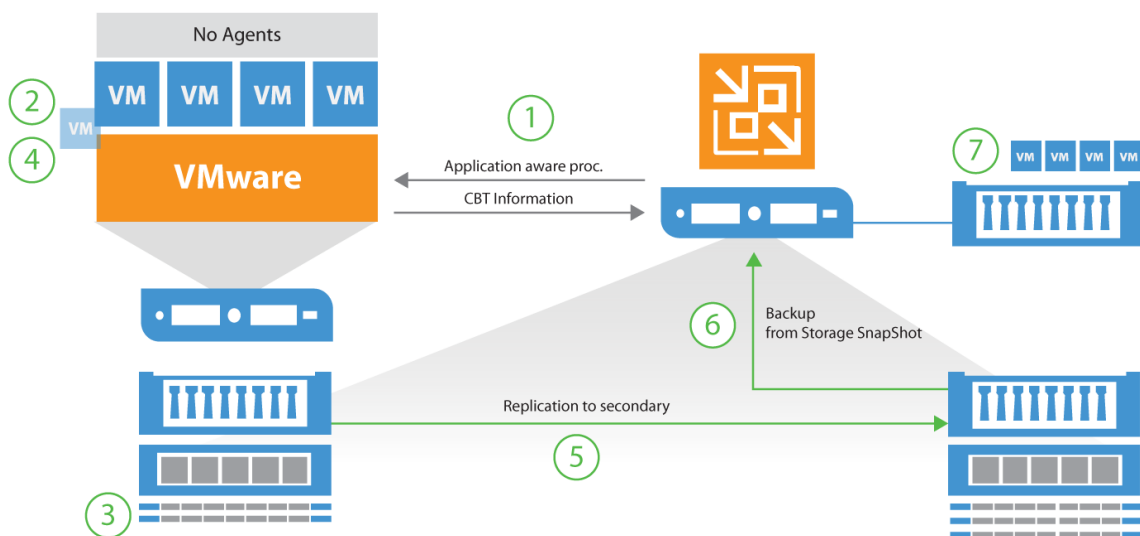
Backup

from Storage Snapshots - VM snapshot lifetime

For regular VADP based backups, the VM snapshot is created and remains open (VM snap lifetime) until the VM backup is completed. Especially with large or highly transactional VMs, that can lead to large snapshot delta files being created during the backup followed by hours of snapshot commit tasks within vSphere producing high I/O on the production storage. Ultimately, these long snapshot commits may lead to unresponsive VMs. For more information about the impact of VM snapshots please see the “[Interaction with vSphere](#)” section of this book.

1.19.1 How it works

By using BfSS, the VM snapshot lifetime will be significantly reduced. In this section, we will go through the steps performed.



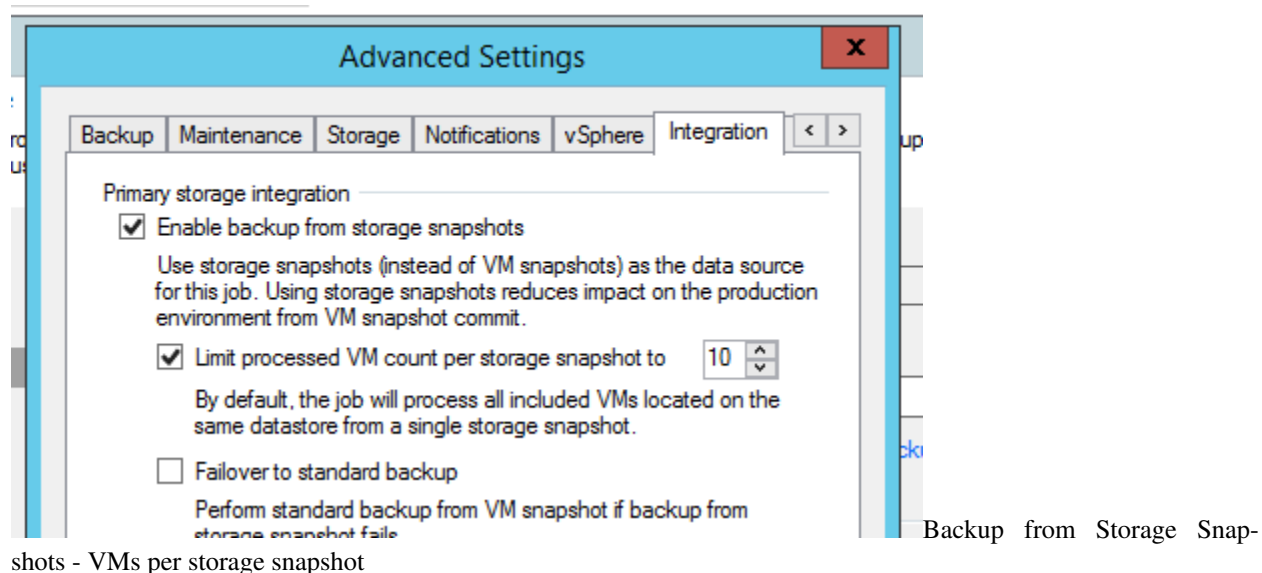
Backup

from Storage Snapshots - data flow overview

1. Application-aware processing ensures transactional consistency within the VM

2. Veeam requests a VM snapshot via VMware APIs
3. Immediately after creating the VM snapshot, a storage snapshot request is issued for saving the VM *including* the application consistent VM snapshot within the storage snapshot.
4. When the storage snapshot has been created, the VM snapshot is deleted
5. (*NetApp only - optional*) Trigger a replication update to secondary storage via SnapMirror or SnapVault
6. Mount storage snapshot to the Veeam backup proxy server
7. Read data from the storage snapshot and write to a Veeam backup repository

VM processing limit

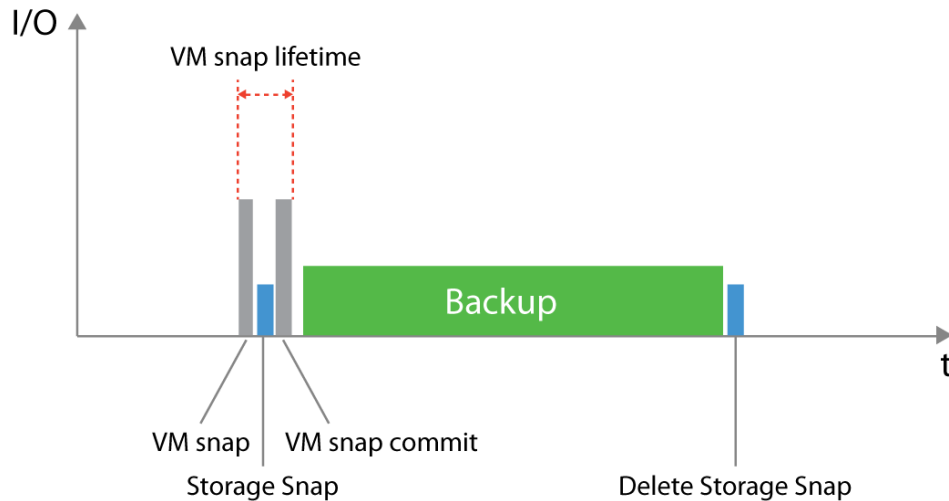


When adding a large number of virtual machines to a job, by default steps 1 and 2 (above) are repeated until all virtual machines within the job have successfully completed. Only then will BfSS proceed to step 3 and issue the storage snapshot. If adding 100s of VMs to a backup or replication job, this could cause a very high VM snapshot lifetime for the first VMs in the job list.

When configuring such large jobs, it is advised to configure the maximum number of VMs within one storage snapshot. The setting is available in the advanced job settings under the **Integration** tab.

Example: When creating a job with 100 VMs, and setting the limit to 10, BfSS will instruct the job manager to process the first 10 VMs (step 1 and 2), issue the storage snapshot and proceed with the backup (step 3-7). When step 7 has successfully completed for the first 10 VMs, the job will repeat the above for the following 10 VMs in the job.

As seen below, when ensuring proper configuration of BfSS, minimal VM snapshot lifetime is achieved, and reduces overall I/O penalty on the production storage for highly transactional VMs.

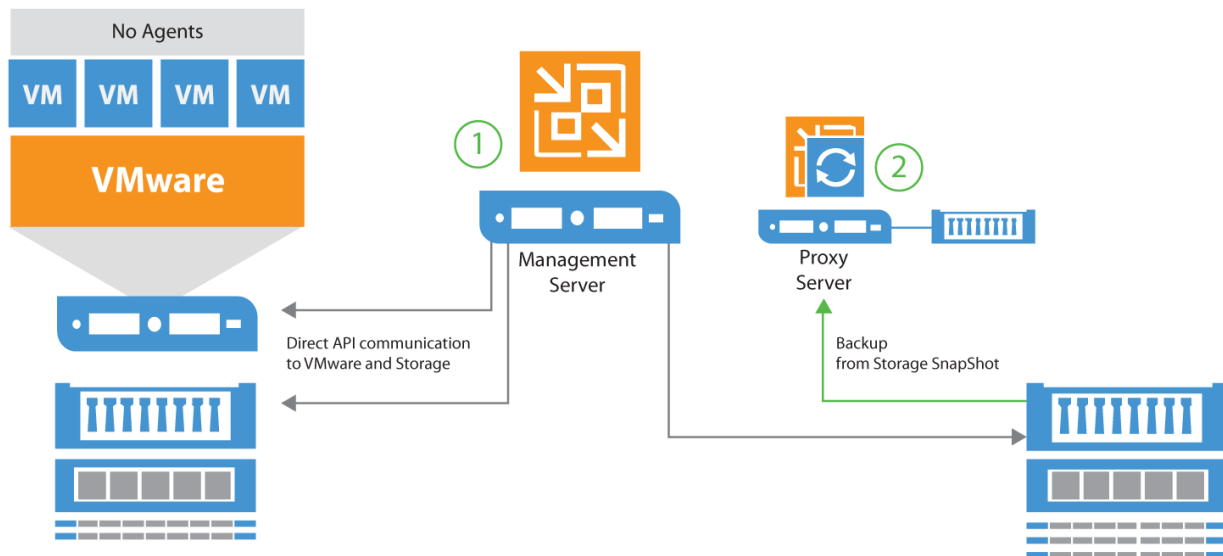


Backup

from Storage Snapshots - reduced VM snapshot lifetime

1.19.2 Configuration

Enabling BfSS requires minimal configuration, but understanding the tasks and responsibilities of involved components are key when troubleshooting and optimizing for high performance and low RTO/RPO.



The backup server is responsible for all API requests towards vSphere and storage arrays for determining present volumes, snapshots and all necessary details such as initiator groups, LUN mappings and which protocols are available.

The proxy server(s) are used for reading data from the storage snapshot and sending it to the backup repository. To leverage Backup from Storage Snapshots, the following configuration requirements must be met:

Backup server must have access to the management interfaces of the storage array. All additional prerequisites such as LUN mappings, creation of initiator groups for iSCSI, altering NFS exports and snapshot management are

subsequently handled via this connection.

Backup proxy servers must be able to directly access the storage array via the same protocol used for connecting the production datastore (FibreChannel, iSCSI or NFS). As opposed to using [Direct Storage Access](#), it is not a requirement for the proxy server to have access to the production datastore itself, as it reads data blocks directly from the cloned storage snapshot.

As described in previous sections, the backup server and proxy server can be deployed on one single server or scaled out on different servers. In most environments, where BfSS is applicable, the components are usually separated for scalability reasons.

1.19.3 When to use

When using Backup from Storage Snapshots, overall job processing may take longer, as additional steps are performed such as mapping vSphere Changed Block Tracking (CBT) to offsets of the storage snapshot, and the snapshot must be cloned and mounted on the backup proxy server. The mount overhead can take several seconds on block protocols as HBAs or initiators must be rescanned. It mostly affects FC deployments.

With this in mind, using BfSS on small VMs or VMs with a very low change rate is not advised. As the VM snapshot lifetime on such VMs is very short, the benefits of using BfSS are minimal.

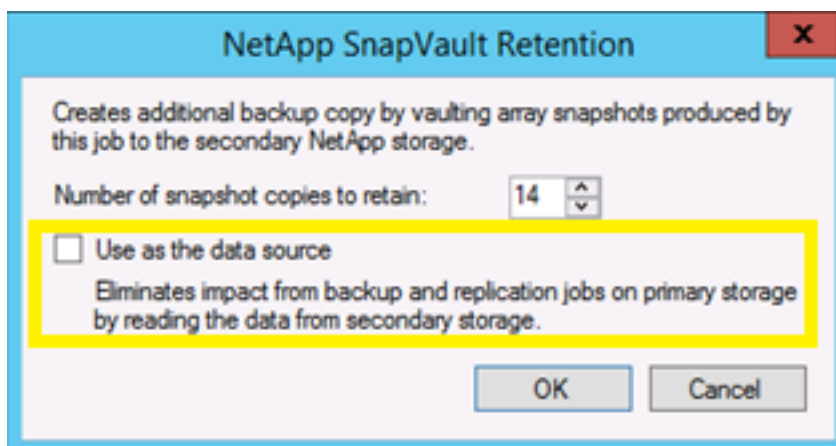
In most environments, large VMs or highly transactional VMs producing large amounts of changed data benefit most from using BfSS. Using the [VM Change Rate Estimation](#) report in Veeam Availability Suite, you may quickly identify such VMs.

VMs with either virtual or physical Raw Device Mapping (RDM) are not supported with BfSS. Such VMs will failover to backing up via standard methods if allowed in the job settings.

1.20 NetApp Data ONTAP

Specifically for NetApp Data ONTAP, Veeam offers some specific additional capabilities.

1.20.1 Backup from secondary snapshots



Backup from Storage Snapshots -

backup from secondary

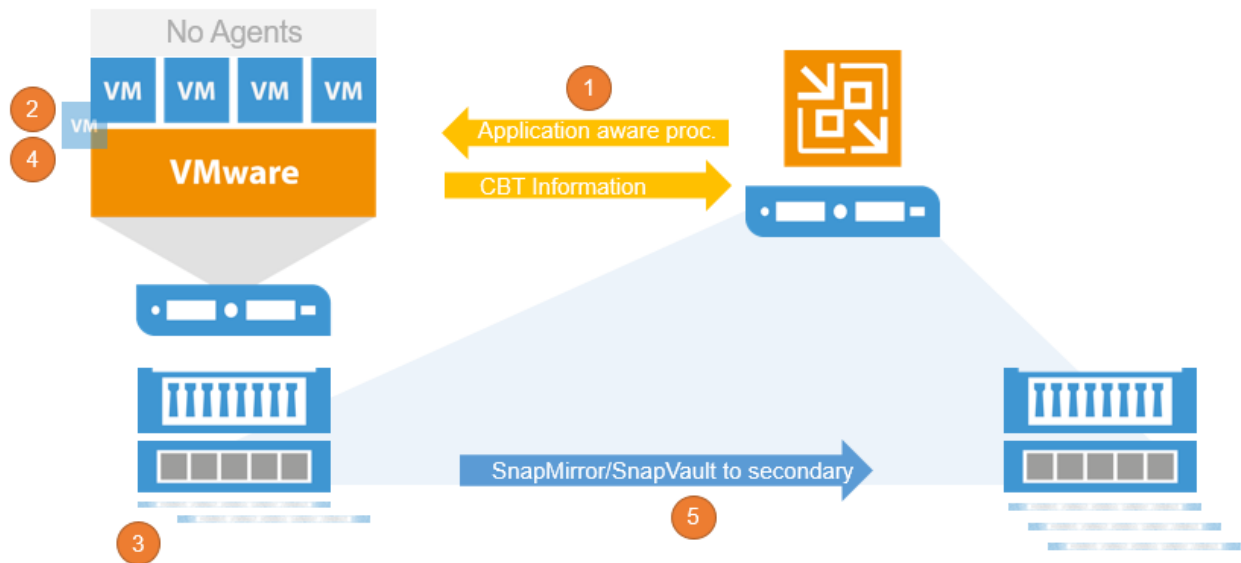
In case you use NetApp SnapVault or SnapMirror, Veeam can create a primary snapshot, update the secondary (SV/SM) Snapshot and backup the CBT changes to the backup file. It is configured with a job setting in the “Ad-

vanced” section if Veeam should allow fallback to the primary snapshot for backup. You can find the setting within the secondary destination window of your backup job and enable “Use as the data source”.

1.20.2 Snapshot Orchestration

For NetApp ONTAP storage systems Veeam offers a SnapShot Orchestration only feature. SnapShot orchestration means to use storage SnapShots as backup target. The feature can be used without any need to run a real backup to an external repository. Veeam is taking care of all required storage related tasks like data retention, SnapShot management and SnapMirror/SnapVault updates to secondary sides.

The workflow for Storage Orchestration is:



1. (Optional) Application-aware processing ensures transactional consistency within the VM
 2. Veeam requests a VM snapshot via VADP
 3. Immediately after creating the VM snapshot, a storage snapshot request is issued for saving the VM *including* the application consistent VM snapshot within the storage snapshot.
 4. When the storage snapshot has been created, the VM snapshot is deleted
 5. Trigger a replication update to secondary storage via SnapMirror or SnapVault
- To configure a “SnapShot only” job set the Repository to “NetApp SnapShot only”

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.

Left Panel:

- Name
- Virtual Machines
- Storage**
- Secondary Target
- Guest Processing
- Schedule
- Summary

Main Content Area:

Backup proxy: Automatic selection Choose...

Backup repository: NetApp SnapShot (Primary storage snapshot only) ▼

Retention policy
Restore points to keep on disk: 14 ⬆ ⬇ ⬆ i

☒ Configure secondary destinations for this job
Copy backups produced by this job to another backup repository, or to tape. Best practices recommend maintaining at least 2 backups of production data, with one of them being 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

The retention policy defines the number of storage snapshots to keep. To store 2 snapshots a day for 1 week, configure the retention to 14 restore points with a schedule set to “*periodically every 12 hours*”. If the job is configured with a high or lower schedule frequency, adjust the number of restore points accordingly.

If you use a secondary NetApp ONTAP system with SnapMirror and/or SnapVault you can set the box for a secondary destination and set the retention.

When using Snapshot Orchestration please take care of the retry scheduler setting.

Edit Backup Job [BfSS-NFS-sec]

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

☒ Run the job automatically

☒ Daily at this time: 22:00 Everyday Days...

☐ Monthly at this time: 22:00 Fourth Saturday Months...

☐ Periodically every: 1 Hours Schedule...

☐ After this job: BfSS-iSCSI-sec (Created by RLP\Administrator at 15.12.2015 19:1)

Automatic retry

☒ Retry failed VMs processing: 3 times

Wait before each retry attempt for: 15 minutes

Backup window

☐ Terminate job if it exceeds allowed backup window Window...

If the job does not complete within allocated backup window, it will be terminated to prevent snapshot commit during production hours.

< Previous Next > Finish Cancel

If you have for example 100 VMs in one job and 10 of these VMs are failing in the first run Veeam will rerun the job based on the retry settings. If the setting is set to 3 (default) Veeam will try 3 more time to process the failed VMs. For every successful retry Veeam will create a new Snapshot. If all retries are needed to proceed the failed VMs that ends in 3 Snapshots for one run. It is recommended to not set the value higher than 3 or disable the automatic retry to avoid a high number of Snapshots being created during every run.

All Veeam restore capabilities are also available from storage snapshots. For more please refer to the [Veeam Explorer for Storage Snapshots](#) section.

1.21 Nimble Storage

This section contains integration specific information for configuring orchestration of snapshot creation and replication between Nimble Storage arrays.

1.21.1 Storage array configuration

1. Browse the NimbleOS web GUI: **Manage – Protection – Volume Collections**
2. Add a new volume by clicking on **New Volume Collection**
3. Add the **Volume Collection Name** on the **Introduction**.

Be careful with the naming to stay within the limits of 80 characters. 4. Select **None** on the **Synchronization** tab.

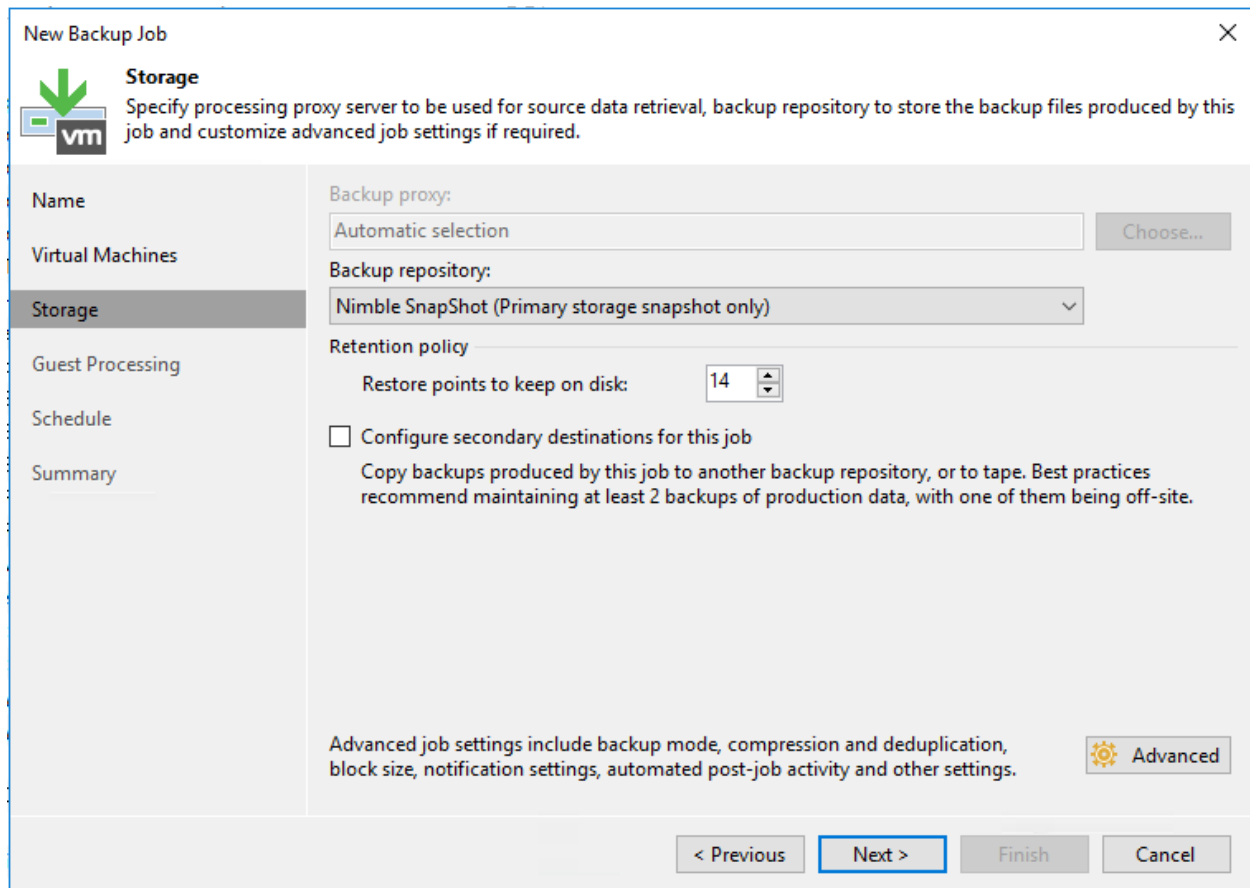
Veeam will orchestrate the creation of a volume snapshot, and initiate replication to the secondary Nimble array before the backup job starts. 5. Set the scheduling for Nimble Storage snapshots.

Note that Veeam Backup & Replication uses its own engine to initiate the creation and replication of snapshots.

Nimble configuration will not allow empty scheduling. Therefore you can choose **Weeks** or **Repeat Every Week** and **Replicate to** set to “2” as the minimum - or any desired configuration, as these configurations will not be used by Veeam. 6. Associate the desired volume for replication on the Volumes Tab

1.21.2 Snapshot only jobs

When a job is configured for using “Nimble snapshot” as the backup repository, Veeam will not copy any data from the source storage to a target repository. Instead Veeam will orchestrate the creation of a storage snapshot, and can entirely skip VMware snapshot creation, in case application-aware image processing is left disabled.



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:
Automatic selection Choose...

Backup repository:
Nimble SnapShot (Primary storage snapshot only) ▼

Retention policy
Restore points to keep on disk: 14 ▲▼

☐ Configure secondary destinations for this job
Copy backups produced by this job to another backup repository, or to tape. Best practices recommend maintaining at least 2 backups of production data, with one of them being 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

Snapshot

It is not recommended to rely on storage snapshots as backups, as it violates the **3-2-1 rule**. It is however a great complement to traditional backups to achieve lower RPO, in case the primary storage array is still available, when a restore is needed.

Note: It is recommended by the vendor that volumes should be in individual Volume Collections. Please verify Nimble Volume Collections configuration before running the snapshot-only job, otherwise it may not operate properly - for example, replicate more data than expected.

1.21.3 Snapshot replication

When configuring backups using the “snapshot only” repository, or regular repositories, it is possible to configure orchestration of replication to a secondary Nimble Storage array by checking the **Configure secondary destinations**

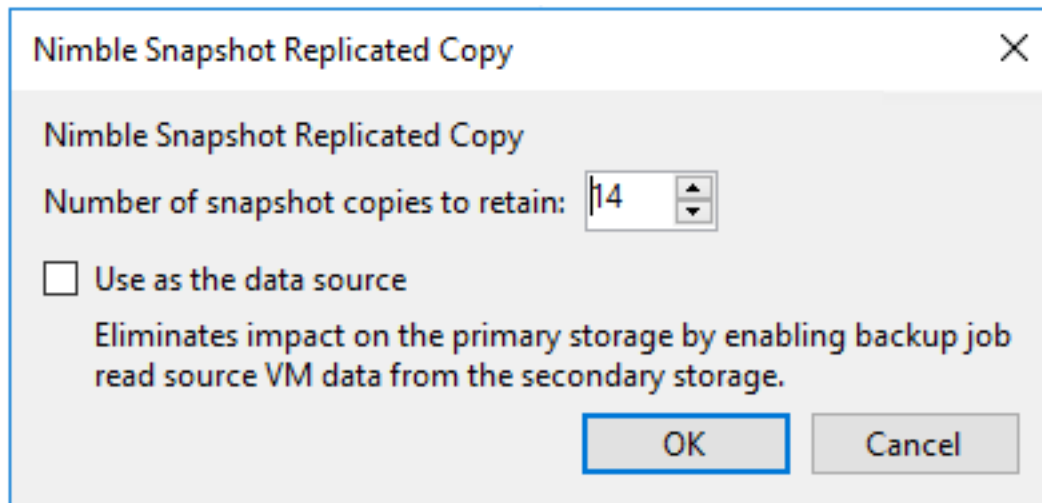
for this job.

Storage secondary destination

By clicking **Add / Nimble Snapshot Replicated Copy**, it is possible to configure how many snapshots should be retained at the target Nimble Storage array. During the job run, Veeam will search for replication settings configured on the Volume Collection for the source volume being snapshot. Please see the initial paragraph of this chapter for details on configuring Volume Collections.

1.21.4 Backup from secondary storage

When performing backups to a backup repository, it is possible to configure using the replicated copy at the target Nimble Storage array as the source for the repository based backup.



Nimble Storage

secondary source

1.22 Selecting a Transport Mode

Depending on the size of the environment, there are different recommendations for selecting a transport mode. For simplicity, a couple of definitions will be used in this section:

Name	Definition
Very small	Single host with local disks as primary datastores. Typical ROBO configuration.
Small	2-4 hosts with shared storage. Typical ROBO configuration or small datacenter
Medium	4-20 hosts with shared storage
Large	20-100 hosts with shared storage
Enterprise	More than 100 hosts

Keep in mind that within larger datacenters, multiple definitions may apply. As an example, it is possible that a separate management or DMZ cluster without shared storage could benefit from using the “Very small” or “Small” recommendations, while the main production environment is leveraging recommendations based on “Medium” to “Enterprise” datacenter sizes.

1.22.1 Very small

- Virtual Appliance (Hot-Add) mode is the recommended option, as it gives you the best performance.
- NBD over 10GbE VMKernel interfaces link will provide a very stable and good performing solution without any special configuration needed.
- NBD over 1GbE VMKernel interfaces can be used for failover.
- Direct Storage Access mode or Backup from Storage Snapshots modes are typically unavailable, as the disks of the host are local and thus cannot be mounted to an external proxy server.

1.22.2 Small and Medium

- If storage integration is available, use Backup from Storage Snapshots (BfSS)^[1]
- For NFS based Storage, use Direct Storage Access
- For shared storage connected via FC or iSCSI, you can choose one of the following two modes:
 - **Physical proxy:** Direct Storage Access will provide the best backup performance. For example, you can configure a physical server with access to FC datastores on the local site and perform backups to a

local repository. If you use thin-provisioned disks for the VMs, configuring a dedicated backup proxy for restoring via Virtual Appliance (hot-add) mode can help to increasing restore performance.

- **Virtual proxy:** The Virtual Appliance (hot-add) mode is a good and fast backup mode. Avoid to backing up VMs on NFS datastores using hot-add. Use Direct Storage Access or NBD backup modes instead.
- NBD over 10 GbE VMKernel Interfaces link will provide a very stable and good performing solution.
- NBD over 1 GbE VMKernel Interfaces can be used for failover and for situations where you do not have to transport much data.
- When using NBD, check the [Network Mode](#) chapter for tuning tips.

1.22.3 Large

In addition to the above considerations for Small and Medium, please see the following guidelines:

- When Direct Storage Access or Backup from Storage Snapshots are unavailable, and when virtual proxy servers are disallowed, Network Mode (NBD) is the only choice. In such cases, 10GbE interfaces are a must.
- For virtual only deployments (virtual proxies only) in environments with many isolated clusters, using network mode (NBD) may be ideal. As hot-add requires at least one proxy within each cluster, it may require many more proxy servers compared to using network mode.
- A combination of hot-add mode for large clusters and NBD mode for smaller clusters may be ideal.

1.22.4 Enterprise

In addition to the above considerations for Large, please see the following guidelines:

- In large enterprise scale environments, the deployment of Veeam components, configuration and job creation is typically automated using the Veeam PowerShell SDK.
- To balance the management load, it is recommended to use multiple Veeam backup servers for at least every 5,000 VMs and federate them for central reporting and administration by using either Veeam Enterprise Manager, Veeam Managed Backup Portal, Veeam Management Pack for Microsoft System Center Operations Manager or Veeam ONE.
- When running a central backup server and with multiple branches connected to it, a dedicated backup server is recommended for at least every 200 branches. Consider using Veeam Enterprise Manager for federation.

[^1]: In case storage integration is used with Backup from Storage Snapshots (BfSS), the overhead of mapping blocks from VMware CBT and the storage snapshot can increase processing time and lead to longer backup windows. To mitigate, consider the majority if the VMs can be backed up with one of the other transport modes and use BfSS only for the largest VMs or high change rates (typically 10% of VMs). Veeam ONE Change Rate Estimation report can help to identify such VMs.

1.23 Sizing a Backup Proxy

Getting the right amount of processing power is essential to achieving the RTO/RPO defined by the business. In this section, we will outline the recommendations to follow for appropriate sizing.

1.23.1 Processing Resources

As described above, you may define the max concurrent tasks value in the backup proxy settings. It is best practices to plan for 1 physical core or 1 vCPU and 2 GB of RAM for each of the tasks. A task processes 1 VM disk at a time and CPU/RAM resources are used for inline data deduplication, compression, encryption and other features that are running on the proxy itself.

In the User Guide it is stated that proxy servers require 2 GB RAM + 500 MB per task. Please consider these values as minimum requirements. Using the above mentioned recommendations allow for growth and additional inline processing features or other special job settings that increase RAM consumption.

If the proxy is used for other roles like Gateway Server for SMB shares, EMC DataDomain DDBoost, HPE StoreOnce Catalyst or if you run the backup repository on the server, remember stacking system requirements for all the different components. Please see related chapters for each components for further details.

Tip: Doubling the proxy server task count will - in general - reduce the backup window by 2x.

1.23.2 Calculating required proxy tasks

Depending on the infrastructure and source storage performance, these numbers may turn out being too conservative. We recommend to performing a POC to examine the specific numbers for the environment.

$D = \text{Source data in MB}$

$W = \text{Backup window in seconds}$

$T = \text{Throughput in MB/s} = \frac{D}{W}$

$CR = \text{Change rate}$

$CF = \text{Cores required for full backup} = \frac{T}{100}$

$CI = \text{Cores required for incremental backup} = \frac{T \cdot CR}{25}$

Example

Our sample infrastructure has the following characteristics:

- 1,000 VMs
- 100 TB of consumed storage
- 8 hours backup window
- 10% change rate

By inserting these numbers into the equations above, we get the following results.

$D = 100 \text{ TB} \cdot 1024 \cdot 1024 = 104,857,600 \text{ MB}$

$W = 8 \text{ hours} \cdot 3600 \text{ seconds} = 28,800 \text{ seconds}$

$T = \frac{104857600}{28800} = 3,641 \text{ MB/s}$

We use the average throughput to predict how many cores are required to meet the defined SLA.

$CF = \frac{T}{100} \approx 36 \text{ cores}$

The equation is modified to account for decreased performance for incremental backups in the following result:

$CI = \frac{T \cdot CR}{25} \approx 14 \text{ cores}$

As seen above, incremental backups typically have lower compute requirements, on the proxy servers.

Considering each task consumes up to 2 GB RAM, we get the following result:

36 cores and 72 GB RAM

- For a physical server, it is recommended to install dual CPUs with 10 cores each. 2 physical servers are required.
- For virtual proxy servers, it is recommended to configure multiple proxies with maximum 8 vCPUs to avoid co-stop scheduling issues. 5 virtual proxy servers are required.

If we instead size only for incremental backups rather than full backups, we can predict alternative full backup window with less compute:

$$WS = \frac{104857600}{14 \cdot 100}$$

$$W = \frac{WS}{3600} \approx 21 \text{ hours}$$

If the business can accept this increased backup window for periodical full backups, it is possible to lower the compute requirement by more than 2x and get the following result:

14 cores and 28 GB RAM

- For a physical server, it is recommended to install dual CPUs with 10 cores each. 1 physical server is required.
- For virtual proxy servers, it is recommended to configure multiple proxies with maximum 8 vCPUs to avoid co-stop scheduling issues. 2 virtual proxy servers are required.

If you need to achieve a 2x smaller backup window (4 hours), then you may double the resources - 2x the amount of compute power (split across multiple servers).

The same rule applies if the change rate is 2x higher (20% change rate). To process a 2x increase in amount of changed data, it is also required to double the proxy resources.

Note: Performance largely depends on the underlying storage and network infrastructure.

Required processing resources may seem too high if compared with traditional agent-based solutions. However, consider that instead of using all VMs as processing power for all backup operations (including data transport, source deduplication and compression), Veeam Backup & Replication uses its proxy and repository resources to offload the virtual infrastructure. Overall, required CPU and RAM resources utilized by backup and replication jobs are typically below 5% (and in many cases below 3%) of all virtualization resources.

1.23.3 How many VMs per job?

- For per job backup files: 30 VMs per job
- For per VM backup files: 300 VMs per job

Consider that some tasks within a job are still sequential processes. For example, a merge process writing the oldest incremental file into the full backup file is started after the last VM finishes backup processing. If you split the VMs into multiple jobs these background processes are parallelized and overall backup window can be lower. Be as well careful with big jobs when you use Storage Snapshots at Backup from Storage Snapshots. Guest processing and Scheduling of jobs that contain multiple snapshots can lead into difficult scheduling situation and jobs spending time waiting for (free) resources. A good size for jobs that write to per VM chain enabled repositories is 50-200 VMs per Job.

Also, remember that the number of concurrently running backup jobs should not exceed 100. Veeam can handle more, but a “sweet spot” for database load, load balancing and overall processing is about 80-100 concurrently running jobs.

1.23.4 How Many Tasks per Proxy?

Typically, in a virtual environment, proxy servers use 4, 6 or 8 vCPUs, while in physical environments you can use a server with a single quad core CPU for small sites, while more powerful systems (dual 10-16 core CPU) are typically

deployed at the main datacenter with the Direct SAN Access processing mode.

Note: Parallel processing may also be limited by max concurrent tasks at the repository level.

So, in a virtual-only environment you will have slightly more proxies with a smaller proxy task slot count, while in a physical infrastructure with good storage connection you will have a very high parallel proxy task count per proxy.

The “sweet spot” in a physical environment is about 20 processing tasks on a 2x10 Core CPU proxy with 48GB RAM and two 16 Gbps FC cards for read, plus one or two 10GbE network cards.

Depending on the primary storage system and backup target storage system, any of the following methods can be recommended to reach the best backup performance:

- Running fewer proxy tasks with a higher throughput per current proxy task
- Running higher proxy task count with less throughput per task

As performance depends on multiple factors like storage load, connection, firmware level, raid configuration, access methods and more, it is recommended to do a Proof of Concept to define optimal configuration and the best possible processing mode.

1.23.5 Considerations and Limitations

Remember that several factors can negatively affect backup resource consumption and speed:

- **Compression level** - It is not recommended to set it to “*High*” (as it needs 2 CPU Cores per proxy task) or to *Extreme* (which needs a lot of CPU power but provides only 2-10% additional space saving). However, if you have a lot of free CPU resources during the backup time window, you can consider to use “*High*” compression mode.
- **Block Size** - The smaller the block size, the more RAM is needed for deduplication. For example, you will see a increase in RAM consumption when using “*LAN*” mode compared to Local target, and even higher RAM load (2-4 times) when using “*WAN*”. Best practice for most environments is to use default job settings (“*Local*” for backup jobs and “*LAN*” for replication jobs) where another is not mentioned in the documentation or this guide for specific cases.
- **Antivirus** - see the corresponding [KB](#) for the complete list of paths that need to be excluded from antivirus scanning
- **3rd party applications** – it is not recommended to use an application server as a backup proxy.

1.24 Proxy Server - Microsoft Hyper-V

In Microsoft Hyper-V environments VMs usually reside on local storage and CSV (Cluster Shared Volume). Veeam Backup & Replication leverages the VSS (Volume Shadow Copy) framework and proprietary Microsoft Hyper-V components to retrieve data and it acts as the VSS requestor. Interacting with the VSS framework, it obtains information about the infrastructure and identifies volumes where VM files are located and triggers the VSS coordinator to create the volume snapshots.

The backup process, in Microsoft Hyper-V environments, expects the VM to be quiesced before taking the snapshot of the volume to make sure that there are no incomplete transactions in a database or no open files. Veeam Backup & Replication uses three methods to prepare Hyper-V VMs for backup:

- **Online backup** - the native Microsoft Hyper-V method for creating application-consistent backup without any downtime.
- **Offline backup** - an alternative native method to obtain consistent backup. It requires a little downtime: Hyper-V uses the OS hibernation to freeze the VM’s I/O.

- **Crash-consistent backup** - Veeam's proprietary method that allows the creation of crash-consistent backup without hibernating nor suspending the VM (no downtime required).

Whenever possible, Veeam Backup & Replication uses online backup to quiesce VMs. If online backup cannot be performed, Veeam Backup & Replication uses one of the other two methods to prepare a VM for backup.

Note: If online backup cannot be performed, Veeam Backup & Replication fails over to the crash-consistent backup. If you do not want to produce a crash-consistent backup, you can instruct Veeam Backup & Replication to use the offline backup method.

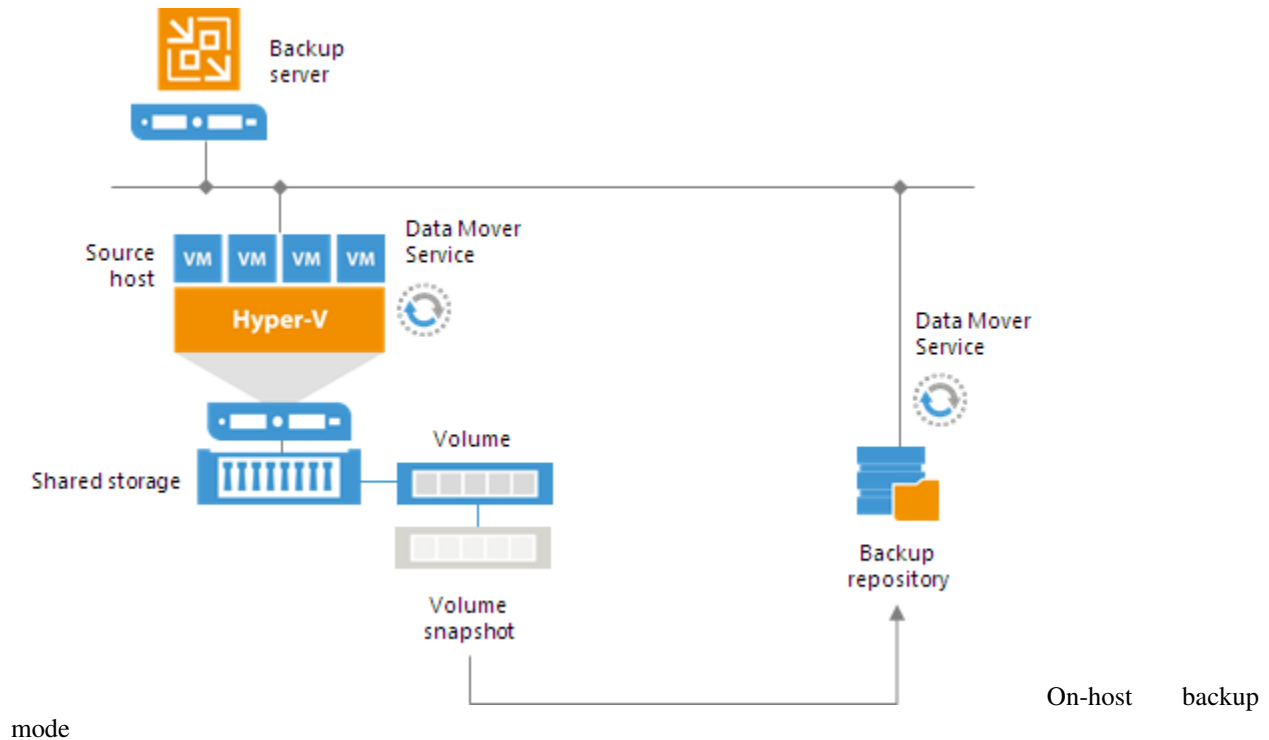
1.24.1 On-host backup

This is the default and **recommended** backup method as it works out of the box. On-host backup mode uses the native Microsoft Hyper-V VSS provider which is proven to be stable and reliable. During on-host backup processing, VM data is processed by the source Microsoft Hyper-V host the VM is running on, and the role of the backup proxy is assigned to the Hyper-V host which owns the CSV (Cluster Shared Volume) according to the following rules:

- If you back up or replicate VMs whose disks are located on a CSV in Microsoft Hyper-V Server 2012R2 or 2016, and Microsoft CSV Software Shadow Copy Provider is used for snapshot creation, Veeam Backup & Replication assigns the role of an "*on-host backup proxy*" to the host owning the CSV. If VM disks are located on different CSVs, Veeam Backup & Replication may use several on-host backup proxies, which are the corresponding hosts owning the CSVs.
- In case you perform backup or replication of VMs whose disks are located on a CSV in Microsoft Hyper-V 2008 R2, and a VSS software or hardware provider is used for snapshot creation, Veeam Backup & Replication assigns the role of an "*on-host backup proxy*" to the host on which the processed VM is registered.

The on-host backup process works in the following way:

1. Veeam Backup & Replication requests the native Hyper-V VSS provider to create snapshots of the corresponding volumes.
2. The Veeam Data Mover service that runs on the Hyper-V host mounts the snapshots, starts processing VMs' data and transfers it to the destination (either a backup repository or a secondary Hyper-V infrastructure).
3. Once the operation is complete, the volume snapshot is deleted.



1.24.2 Off-host backup

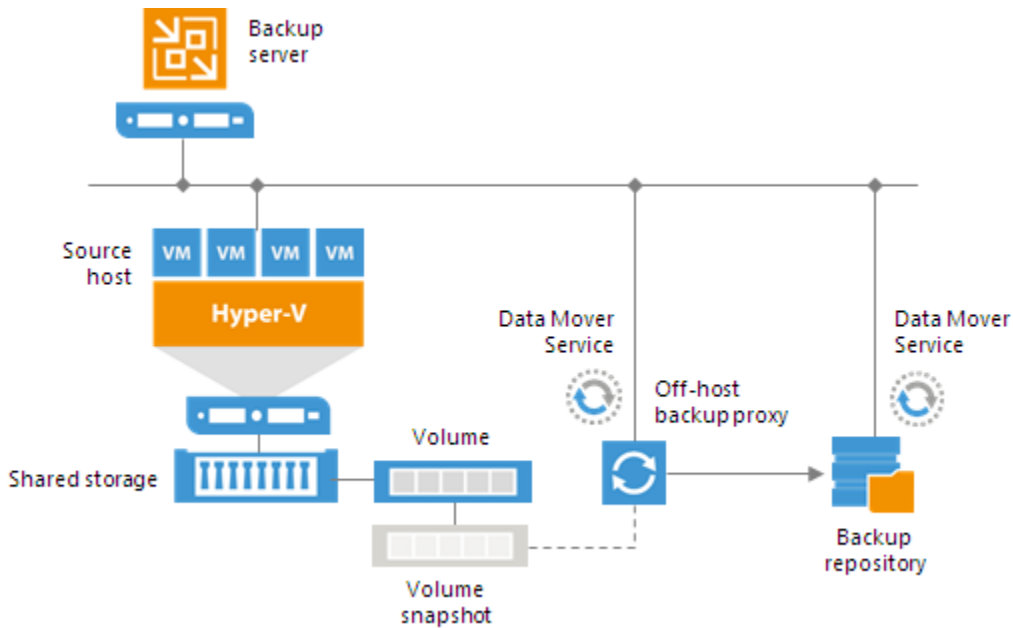
In this backup mode, backup operations are moved from the Hyper-V hosts to one or more dedicated physical server(s). The Veeam Data Mover service running on a dedicated machine, called “*off-host proxy*”, retrieves VM data from the source volume using “*transportable shadow copies*”. This technology allows Veeam Backup & Replication to create a snapshot of the CSV (Cluster Shared Volume) on which VM disks are saved and then import and mount this snapshot onto a different server which is part of the same SAN (Storage Area Network).

Off-host backup mode requires third-party components that are not shipped with Veeam Backup & Replication: the so called **VSS Hardware Provider**, which are usually distributed as part of client components supplied by the storage vendor. These VSS providers must be tested in your dedicated environment (e.g. a MS Cluster and multi Off-Host Proxy environment). Please also check the storage snapshot logs after backup.

For more information regarding the off-proxy requirements, refer to the [official documentation page](#).

The off-host backup process works in the following way:

1. Veeam Backup & Replication triggers a snapshot of the required volume on the Microsoft Hyper-V host.
2. This snapshot is mounted to the “*off-host backup proxy*”.
3. The Veeam Data Mover service running on the off-host backup proxy processes VM data on the mounted snapshot and transfers it to the destination (either a backup repository or a secondary Hyper-V infrastructure).
4. Once the operation is complete, the snapshot is detached from the off-host proxy and deleted from the storage system.



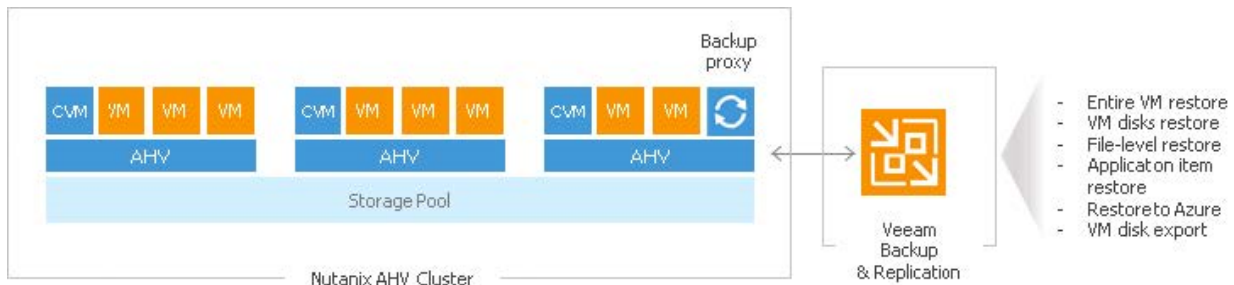
Off-host backup

mode

1.25 Proxy Server - Nutanix AHV

To back up Nutanix AHV VMs, Veeam Backup & Replication uses an agentless approach. The solution works at the hypervisor level. It creates image-based backups of VMs, capturing the whole VM data at a specific point in time, including OS, system state data, application data and so on. Backups of Nutanix AHV VMs are stored on Veeam backup repositories in the native Veeam format. You can use the resulting backup files for different restore scenarios:

- Entire VM restore
- VM disks restore
- File-level restore
- Application item restore
- Restore to Microsoft Azure
- VM disk export



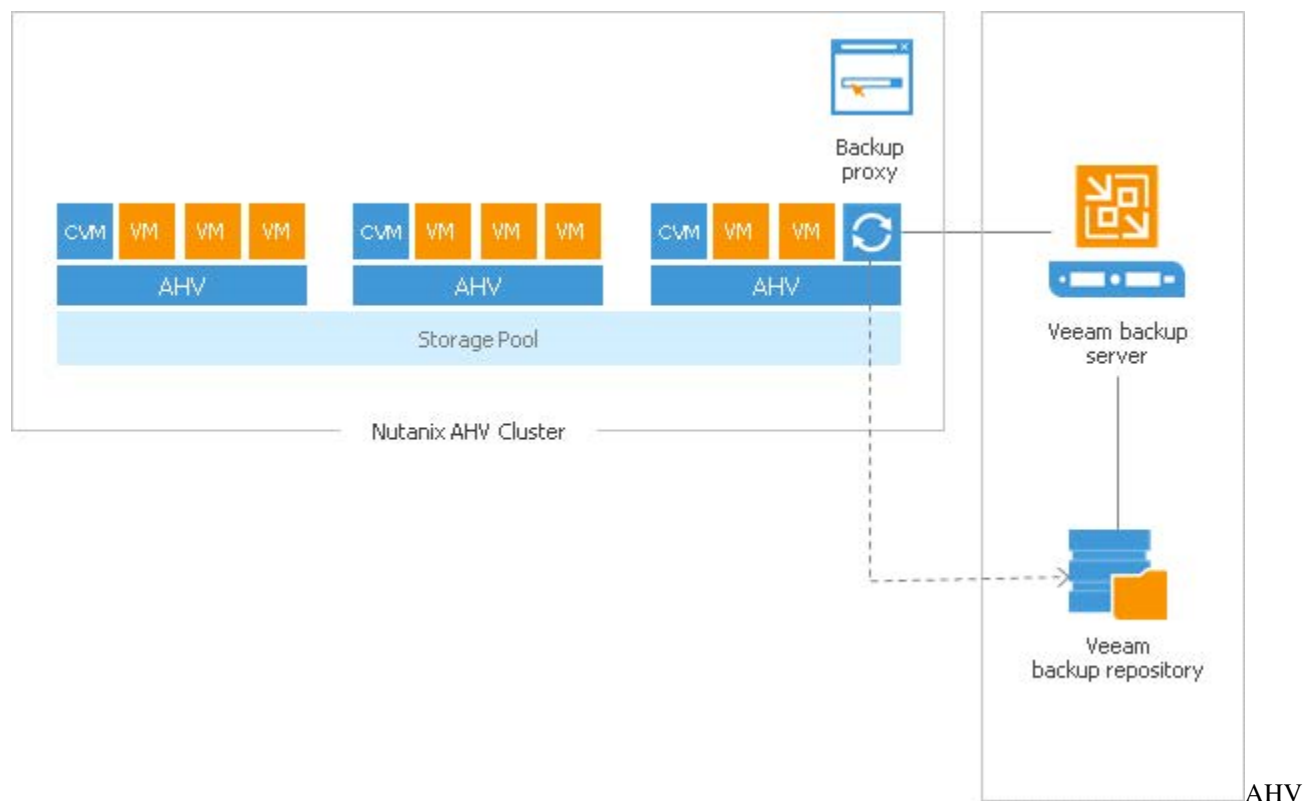
AHV

Proxy

1.25.1 How It Works: Integration Details

The core component enabling Veeam integration with the Nutanix AHV platform is a backup proxy. The backup proxy is a Linux-based virtual module that acts as a broker, or coordinator between the Nutanix AHV platform on one side and the Veeam backup server on the other side. The backup proxy in the Nutanix integration scheme is an all-in-one box that is responsible for backup, entire VM restore and VM disk restore operations. The backup proxy communicates with the AHV platform via Nutanix RESTful API, assigns necessary resources for backup and restore operations, reads/writes data from/to AHV datastores and transports VM data to/from target Veeam backup repositories. The backup proxy is also responsible for job management and scheduling, data compression and deduplication, applying retention policy settings to backup chains, as well as performing other backup and restore related activities.

A proxy deployed in one cluster can only serve that cluster. That is, if to backup and restore VMs from another cluster you will need to deploy another proxy running on that specific cluster.



Proxy

Backup proxy comes with a web-based portal that allows users to perform the following tasks:

- Configure connections to components in the Veeam backup infrastructure.
- Configure and run backup jobs for Nutanix AHV VMs.
- Restore VMs back to Nutanix AHV clusters.
- Restore VM disks and attach them to VMs hosted on Nutanix AHV clusters.

In addition to restore options available in the backup proxy web portal, administrators working with the Veeam Backup & Replication console can also perform the following data recovery operations with backups of Nutanix AHV VMs stored on Veeam backup repositories:

- Restore VM guest OS files
- Restore application items

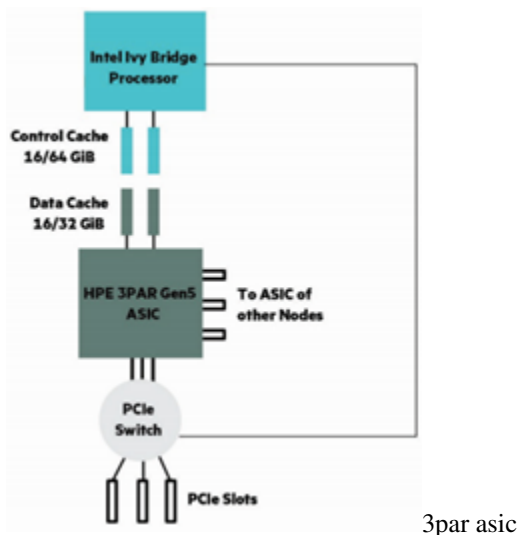
- Export VM disks to VMDK, VHD and VHDX formats
- Export VMs to Microsoft Azure

1.26 Restoring VMs to an HPE 3PAR with thin disks

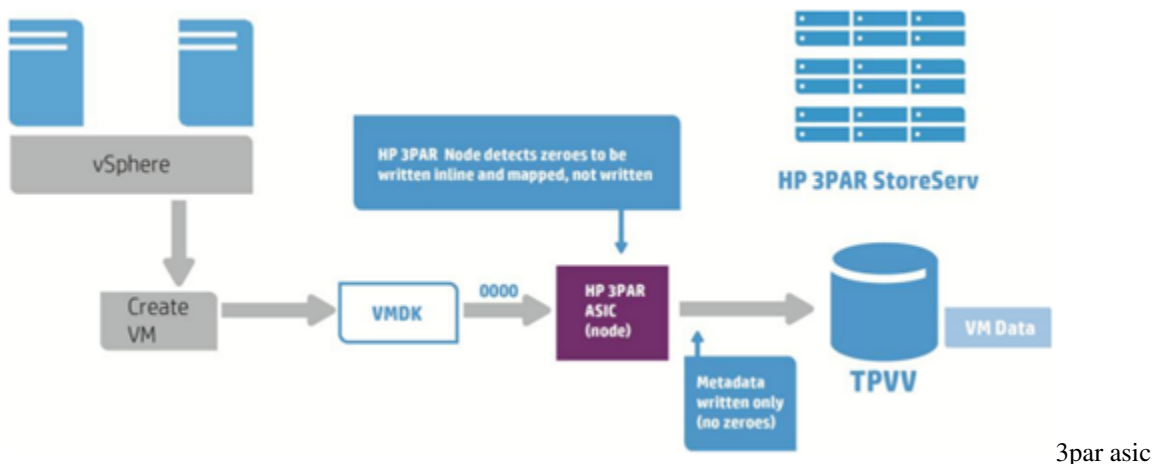
Restoring a VM with thin disks leads to a painful slow restore on HPE 3PAR arrays. Usually this condition happens only when restoring backups taken from another infrastructure to a new one, based on HPE 3PAR. Leaving restore options with all the default value, the original format of the virtual disks is kept and if the restored VMs had originally thin provisioned disks, it will be restored with the same format. HPE best practices' regarding 3PAR is to provision VMs using think disks.

1.26.1 3PAR useful facts

3PAR has a built-in chip, ASIC, used for features like zero-detection, RAID calculation and dedupe/compression:



ASIC can eliminate zeros inline, avoiding useless writes on a virtual volume (LUN):



When a thin-provisioned VM is deleted, the underlying array is not informed that the data is no longer in use (this is an expected behavior in vSphere – that's how it works) and, when writes occur, the previously allocated blocks must be first purged. There is a manual procedure, described here, to manually trigger the unmap of these blocks. What is

not working as expected with 3PAR arrays is that when a write in thin provision mode occurs on previously written blocks, ASIC cannot intercept zeroes and an unexpected data format leads to poor write performances. The same condition would not happen if you restore thin provisioned disks on newly created 3PAR virtual volume.

When restoring VMs on a 3PAR based infrastructure, force the restore in thick (lazy zeroed works as well – and will also save some time) if source VM were created with thin disks. All the zeroes will be automatically detected, skipped and never written. There will much less writes and less I/O flowing to the array.

1.26.2 Additional resources

[Why the right architecture matters with vSphere](#)

[HPE 3PAR StoreServ Storage and VMware vSphere 6.5 best practices](#)

[HPE 3PAR VMware ESX/ESXi Implementation Guide](#)

[HPE 3PAR StoreServ Architecture](#)

1.27 Data DellEMC DataDomain Advanced Scalability Design

The following document explains how to configure VBR when using multiple proxies that write backups on the same Dell EMC Data Domain.

When it comes to big environments, using the default configuration and let all proxies that process VMs backups passing through a single gateway server, to write data on the Data Domain, could not be the best option. Gateway server is a component that must be properly sized to avoid bottlenecks along the way to the repository and, if it is not explicitly fixed in the repository configuration, one will be picked based on the software logic (see *selection algorithm*).

Rather than using the default configuration, this document provides guidelines to achieve the maximum parallelism by having all the proxies writing on a different repository (proxy and gateway roles are on the same server). To reduce management overhead, all the Dell EMC Data Domain repositories will be grouped in a single Scale-out Backup Repository.

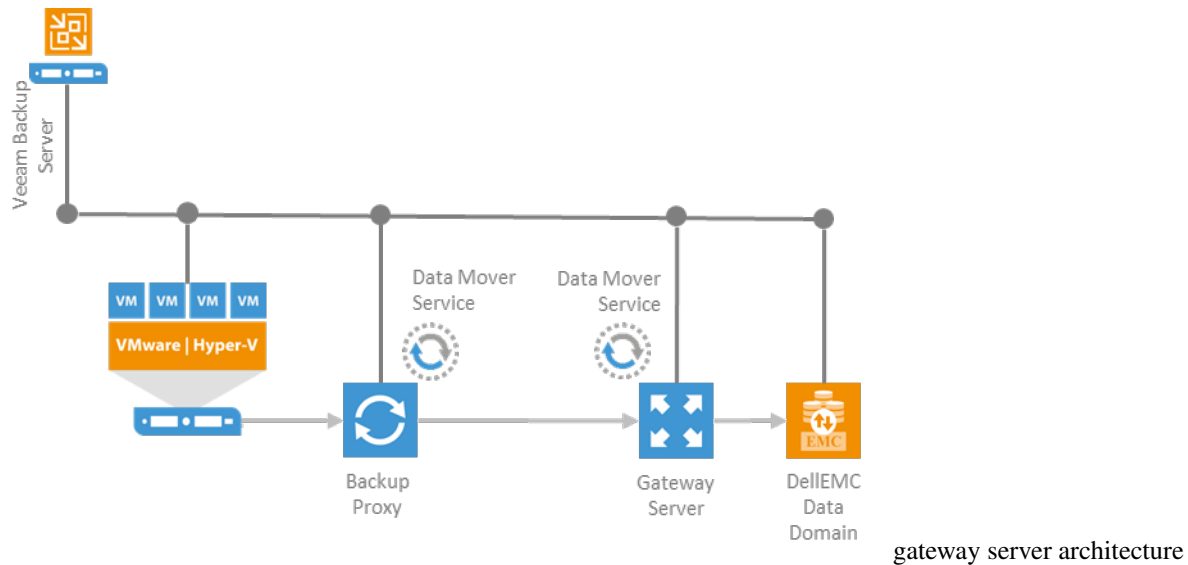
1.27.1 Gateway server role explained

From the user guide:

A gateway server is an auxiliary backup infrastructure component that “bridges” the backup server and backup repository. The gateway server is required if you deploy the following types of backup repositories in the backup infrastructure:

- Shared folder backup repositories
- Dell EMC Data Domain deduplicating storage appliance
- HPE StoreOnce deduplicating storage appliance

Shared folder repositories, EMC Data Domain and HPE StoreOnce cannot host Data Mover Services — Veeam components that establish a connection between a backup proxy and backup repository (in case of backup jobs) or between backup repositories (in case of backup copy jobs). To overcome this limitation, Veeam Backup & Replication uses gateway servers. In the backup infrastructure, a gateway server hosts the target Veeam Data Mover. Veeam Backup & Replication establishes a connection between the source Veeam Data Mover and target Veeam Data Mover, and transports data from/to backup repositories via gateway servers.



Selection Algorithm

| Type of job | Gateway server | Synthetic operations | | - | - | - | | Backup job | Backup proxy that was assigned the first to process VM data for a backup job. | Synthetic operations are performed on the mount server associated with the backup repository. If the mount server is not accessible, Veeam Backup & Replication fails over to the backup server. | | Backup copy job | Direct data path: mount server associated with the backup repository. If the mount server is not accessible, Veeam Backup & Replication fails over to the backup server. Over WAN accelerators: source and/or target WAN accelerator (depending on the shared folder backup repository location). | Synthetic operations are performed on the mount server associated with the backup repository. If the mount server is not accessible, Veeam Backup & Replication fails over to the backup server. These rules are applied to the direct data path and processing over WAN accelerators. | | Tape job | If there is a direct connection between a backup repository and tape device, the role of a gateway server is assigned to the tape server. Otherwise the role of a gateway server is assigned to the backup server. | Synthetic operations are performed on the mount server associated with the backup repository. If the mount server is not accessible, Veeam Backup & Replication fails over to the backup server. | | Restore operations | Backup proxy used for a restore operation | - | | Replication from backup | Target backup proxy assigned for a replication operation | - |

1.27.2 DataDomain MTree

MTree overview and limits

Dell EMC defines an MTree as logical partitions of the file system and they are identified by a unique name. MTrees are used to create (protocols can be mixed, except VTL):

- DD Boost storage units
- VTL pools
- NFS/SMB shares

MTrees allow granular management of snapshots and quotas. Quotas apply only to logical data written to an MTree.

There is a fixed amount of MTrees that can be create on a Data Domain system and it depends by the model and DD OS version.

| DataDomain system | DD OS version | Configurable MTree's | Concurrently Active MTree's | | - | - | - | - | | DD9800 | 6.0+ | 256 | 256 | | DD9500 | 5.7+ | 256 | 256 | | DD6800, DD9300 | 6.0+ | 128 | 128 | | DD6300 | 6.0+ | 100 | 32 | | DD990, DD4200, DD4500, DD7200 | 5.7+ | 128 | 128 | | All other DD systems | 5.7+ | 100 | up to 32 |

MTree attributes and statistics

| Item | Description | | | | MTree Name | The pathname of the MTree (/data/coll/mtree-name). | | Quota Hard Limit | Percentage of hard limit quota used. | | Quota Soft Limit | Percentage of soft limit quota used. | | Last 24 Hr Pre-Comp | Amount of raw data from the backup application that has been written in the last 24 hours. | | Last 24 Hr Post-Comp | Amount of storage used after compression in the last 24 hours. | | Last 24 Hr Comp Ratio | The compression ratio for the last 24 hours. | | Weekly Avg Post-Comp | Average amount of compressed storage used in the last five weeks. | | Last Week Post-Comp | Average amount of compressed storage used in the last seven days. | | Weekly Avg Comp Ratio | The average compression ratio for the last five weeks. | | Last Week Comp Ratio | The average compression ratio for the last seven days. |

1.27.3 DataDomain replication overview

Data Domain Replicator is a technology that allows replication between two (or more) Data Domain systems. The replication process is network-efficient as no data re-hydrate happens when transferring data between two systems.

To reduce bandwidth usage, Data Domain Replicator performs two levels of deduplication:

- local – determines the unique segments that must be replicated over WAN
- cross-site – it further reduces bandwidth requirement when multiple systems are replicating to the same target (many to one architecture)

Data Domain Replicator is a **licensed feature**.

Replication types

Replication always involves at least two Data Domain systems, identified as source and destination and each system can be either source and destination (cross-replication). The process is always asynchronous.

A Data Domain can be set up for different kind of replication, such as:

- Directory – replication based on single directory (the smallest entity within an MTree)
- Collection – entire Data Domain content
- MTree – entire MTree replication, including all subfolders

Replication requirements

For any replication type, requirements are:

- A destination Data Domain system must have available storage capacity that is at least the size of the expected maximum size of the source directory.
- The file system must be enabled or, based on the replication type, will be enabled as part of the replication initialization.
- The source must exist.
- The destination must not exist.
- The destination will be created when a context is built and initialized.
- After replication is initialized, ownership and permissions of the destination are always identical to those of the source.
- In the replication command options, a specific replication pair is always identified by the destination.

- Both systems must have an active, visible route through the IP network so that each system can resolve its partner's host name.

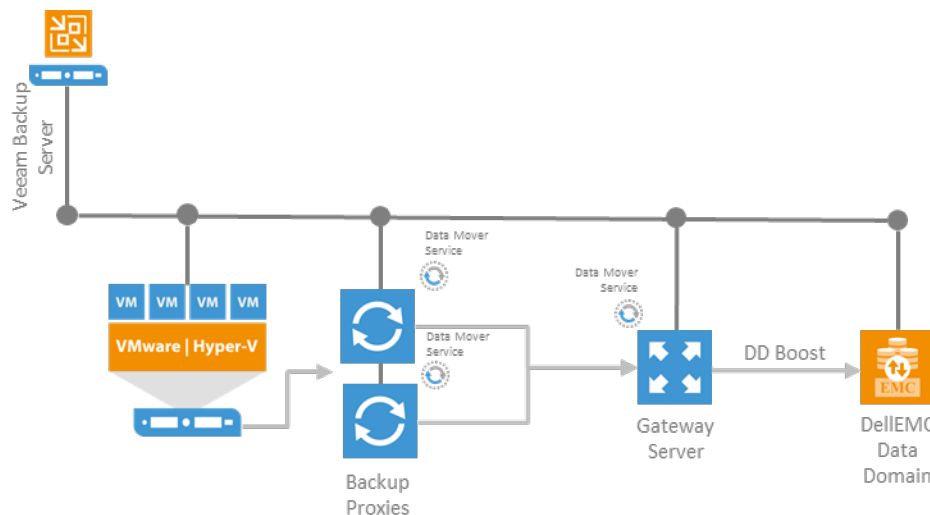
1.27.4 Veeam B&R Integration

Advanced Scalability Design

Avoiding Bottlenecks

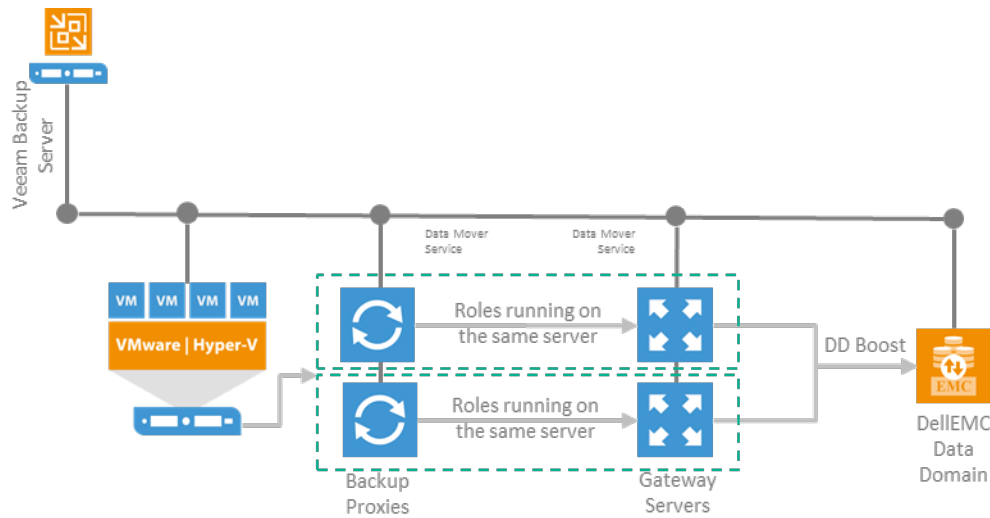
When dealing with enterprise environments and there are multiple proxies that process VMs data, the gateway server role that spawns on one of them can be very resources consuming and it can potentially lead to an unbalanced load between all the proxies in the pool.

By design, a backup repository can have only one gateway server therefore all the proxies will send all the data to the assigned gateway server as follow:



Moreover, **DDBOOST dedupe happens only between gateway and repository**. Data transfer, either proxy to proxy and proxy to gateway benefits of Veeam's software compression only.

To avoid bottlenecks the best option is to make sure **every proxy is also its gateway server and writes backup on its own backup repository**. The architecture will look as follow:



Setting up MTree

To maintain configuration as simple as possible, all VBR backups will be written on a single MTree. Doing that, monitoring the MTree will be an easy task: all the statistics related to the MTree will apply to the entire backup set, such as dedupe ratio, compression, daily written, etc.

Log into Data Domain management interface and create the MTree and its associated user:

Dell EMC Data Domain System Manager

Protocols DD Boost

DD Boost Status: **Enabled** [Disable] [More Tasks] [?]

Kerberos Mode: Disabled [Configure]

Settings Active Connections IP Network **Storage Units**

[View DD Boost Replications](#)

Storage Unit	User	Quota Hard Limit	Last 24hr Pre-Comp	Last 24hr Post-Comp	Last 24hr Comp Ratio	Weekly Avg Post-Comp	Last Week Post-Comp	Weekly Avg Comp Ratio	Last Week Comp Ratio
No record found.									

Items Selected: 0

Storage Unit Space Usage Daily Written

No storage unit is selected.

mtree configuration 1

Create Storage Unit

Name: su-itlabvbr01-ddboost

User: Create a new Local User...

User: vbrddboost

Password:

Verify Password:

Management Role: none

i The user will be added to the DD Boost access list.

Quota Settings *

Pre-Comp Soft Limit ☒ None ☐ Set to specific value: GiB ▼

Pre-Comp Hard Limit ☒ None ☐ Set to specific value: GiB ▼

! Global quota enforcement is disabled

? Create Cancel

dd mtree configu-

ration 2

Tip: Name the MTree including backups server's hostname to better identify the environment you are working on.

As soon as the MTree is created, note the path that it has on the Data Domain file system:

DELL EMC

Data Domain System Manager

HOME

HEALTH

DATA MANAGEMENT

REPLICATION

PROTOCOLS

DD Boost

CIFS

NFS

HARDWARE

ADMINISTRATION

MAINTENANCE

Protocols DD Boost

DD Boost

DD Boost Status: Enabled

Disable

Kerberos Mode: Disabled

Configure

Settings

Active Connections

IP Network

Storage Units

View DD Boost Replications

Storage Units

	Storage Unit	User	Quota Hard Limit	Last 24hr Pre-Comp	Last 24hr Post-Comp	Last 24hr Comp Ratio	Weekly Avg Post Comp	Last Week Post-Comp	Weekly Avg Comp Ratio	Last Week Comp Ratio
<input checked="" type="checkbox"/>	su-itlabvbr01-ddboost	vbrddboost	Disabled	0.0 GiB	0.0 GiB	0.0x	0.0 GiB	0.0 GiB	0.0x	0.0x

Items Selected: 1

Storage Unit

Space Usage

Daily Written

Summary

Download Compression Details

Quota

Physical Capacity Measurements

Snapshots

Assign Schedules

Total Files: 0

Full Path: /data/col1/su-itlabvbr01-ddboost

Status: RW (Read Write)

Pre-Comp Used: 0 MiB

Used (Post-Comp): N/A

Compression: N/A

Last Measurement Time: N/A

Schedules: 0

Submitted Measurements: 0

Quota Enforcement: Disabled

Pre-Comp Soft Limit: None

Pre-Comp Hard Limit: None

Quota Summary: None

Total Snapshots: 0

Expired: 0

Unexpired: 0

Oldest Snapshot: -

Newest Snapshot: -

Next Scheduled: -

Assigned Snapshot Schedules: -

mtree configuration 3

Every proxy will have its own sub-folder within the MTree (the folder will be created during the repository creation wizard in VBR):

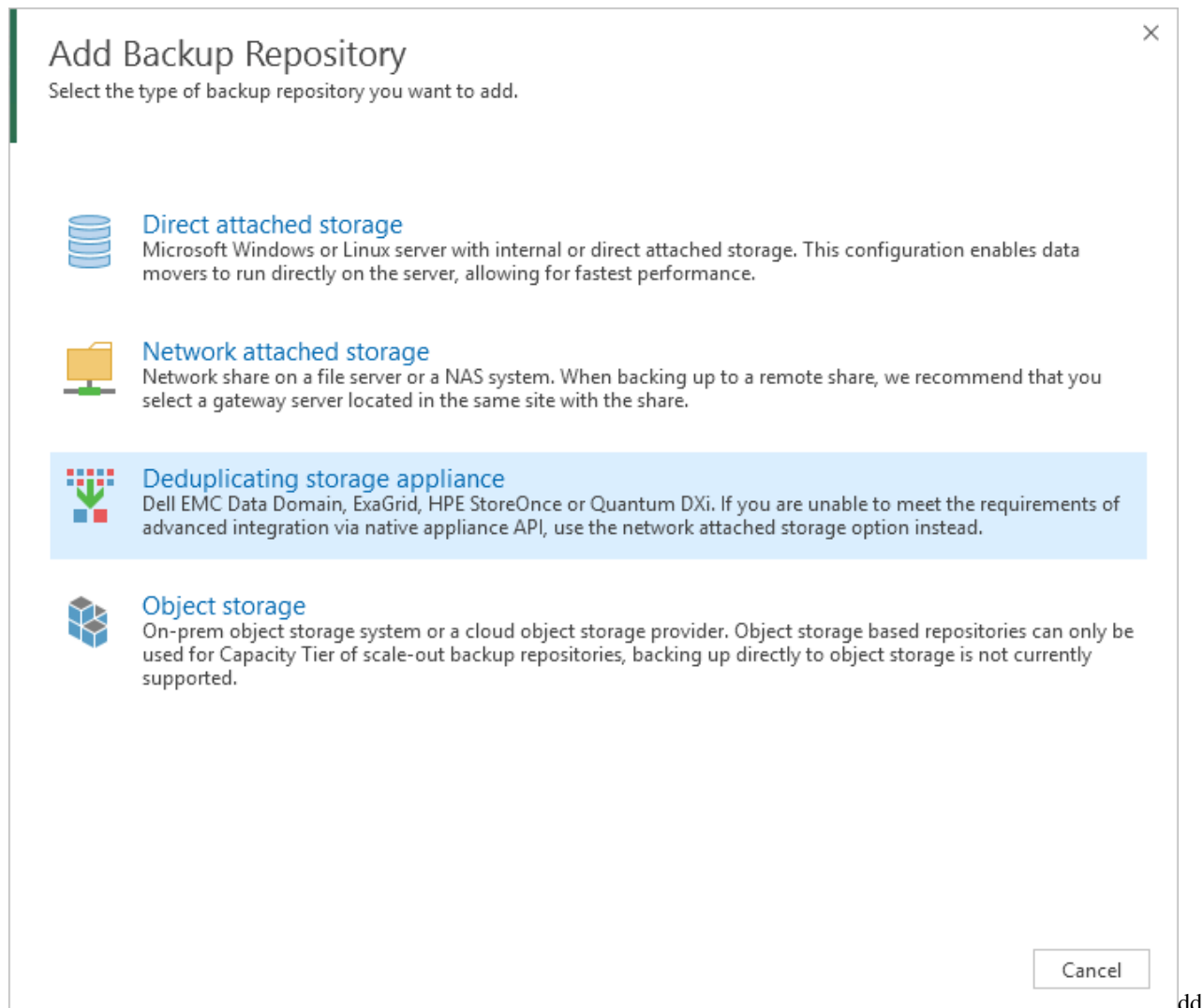
```
/data/col1/su-itlabvbr01-ddboost/proxy_01
/data/col1/su-itlabvbr01-ddboost/proxy_02
/data/col1/su-itlabvbr01-ddboost/proxy_n
```

This is key to maintain backup file separated and to not create any kind of inconsistencies in VBR database.

Configuring VBR repositories

As said above, there will be one repository for each proxy processing VMs data so the following step has to be repeated for each proxy in the infrastructure.

- 1. Start the repository configuration wizard, select ‘Deduplicating storage appliance’ and then ‘Dell EMC Data Domain’:



repo conf 1

1. Name each repository including the name of the proxy that will access it (it will be easy to identify the extent once it will be part of the Scale-out Backup Repository):

New Backup Repository

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

Name

Dell EMC Data Domain

Repository

Mount Server

Review

Apply

Name:
itlabddve01_ext-prx01

Description:
Created by VEEAMITA\andrea at 2/19/2019 11:07 AM.

< Previous Next > Finish Cancel

repo conf 2

1. Type in Data Domain hostname and select the proxy that will access the repository:

New Backup Repository

Dell EMC Data Domain
Specify Dell EMC Data Domain storage name and credentials.

Name

Dell EMC Data Domain

Repository

Mount Server

Review

Apply

Type in Data Domain server name:
itlabddve01.veeamita.local

☐ Use Fibre Channel (FC) connectivity
DDBoost-over-FC server name can be found on Data Management > DDBoost > Fibre Channel tab

Credentials:
vbrddboost (Data Domain - ddboost user for VBR, last edited: less than a day ago) Add...

[Manage accounts](#)

Gateway server:
☐ Automatic selection
☒ The following server:
itlabprx01.veeamita.local (Created by VEEAMITA\andrea at 7/13/2018 9:00 AM.)

☐ Enable DDBoost encryption: Medium

< Previous Next > Finish Cancel

repo conf 3

1. Browse the storage units and create the folder where the proxy (and its gateway server) will write backup files:

New Backup Repository

Repository

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

Name

Dell EMC Data Domain

Repository

Mount Server

Review

Apply

Location

Storage unit

Browse...

Capacity:

Free space:

Populate

Load control

Running too many concurrent tasks against the same repository may reduce overall performance, and cause I/O operations to timeout. Control storage device saturation with the following settings:

☒ Limit maximum concurrent tasks to:

8

☐ Limit read and write data rates to:

MB/s

Click Advanced to customize repository settings

Advanced...

< Previous

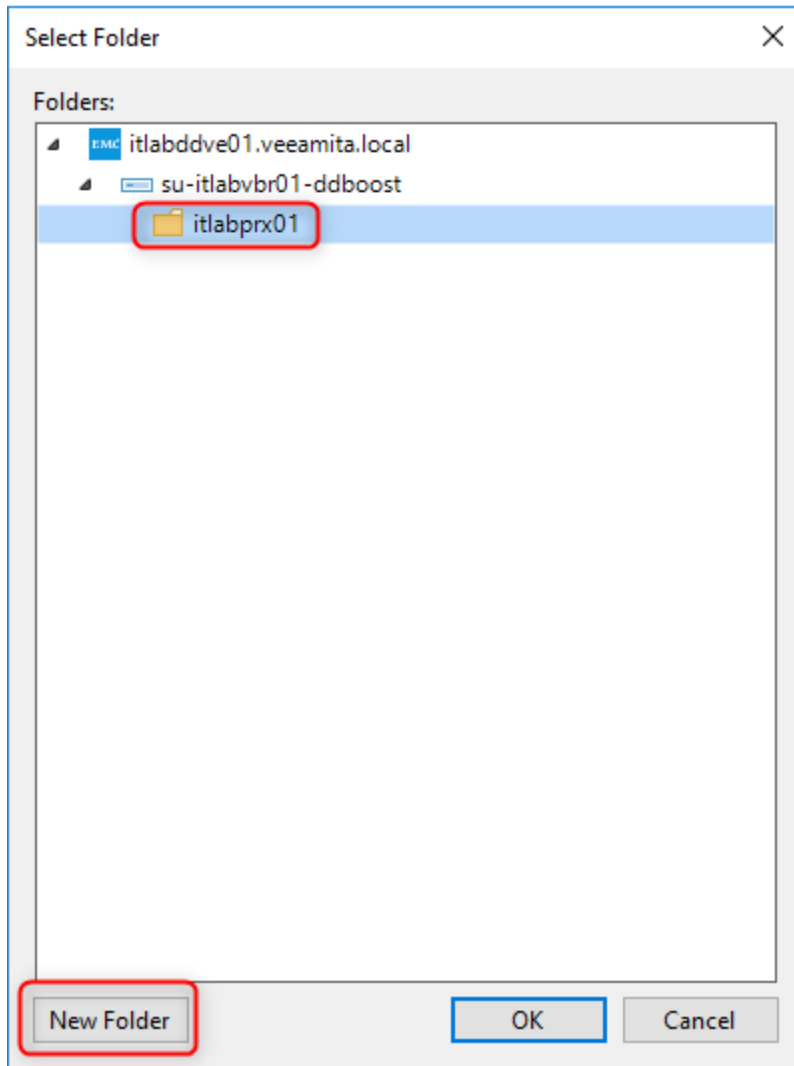
Next >

Finish

Cancel

repo conf 41

dd



dd repo conf 42

1. Select the same server for the mount server role as well, in this way all the traffic related to this extent will be isolated and will pass through the same server for both read and write:

New Backup Repository

Mount Server
Specify a server to mount backups to for file-level restores. vPower NFS service allows for running virtual machines directly from backup files, enabling advanced functionality such as Instant VM Recovery, SureBackup and On-Demand Sandbox.

Name
Dell EMC Data Domain

Repository
Mount Server

Mount server:
itlabprx01.veeamita.local (Created by VEEAMITA\andrea at 7/13/2018 9:00 AM.) Add New...

☒ **Enable vPower NFS service on the mount server (recommended)**
Specify vPower NFS write cache location on the mount server. Make sure the selected volume has enough free disk space available to store changed disk blocks of instantly recovered VMs.

Folder: C:\ProgramData\Veeam\Backup\NfsDatastore Browse...

Click Ports to change NFS server and backup mount listener ports Ports...

< Previous Next > Finish Cancel

repo conf 5

1. All the repositories needed to create the Scale-out Backup Repository are now configured. Review the configuration and make sure the MTree path is correct and every repository contains the directory where the gateway server will write the backup files:

VEEAM BACKUP AND REPLICATION

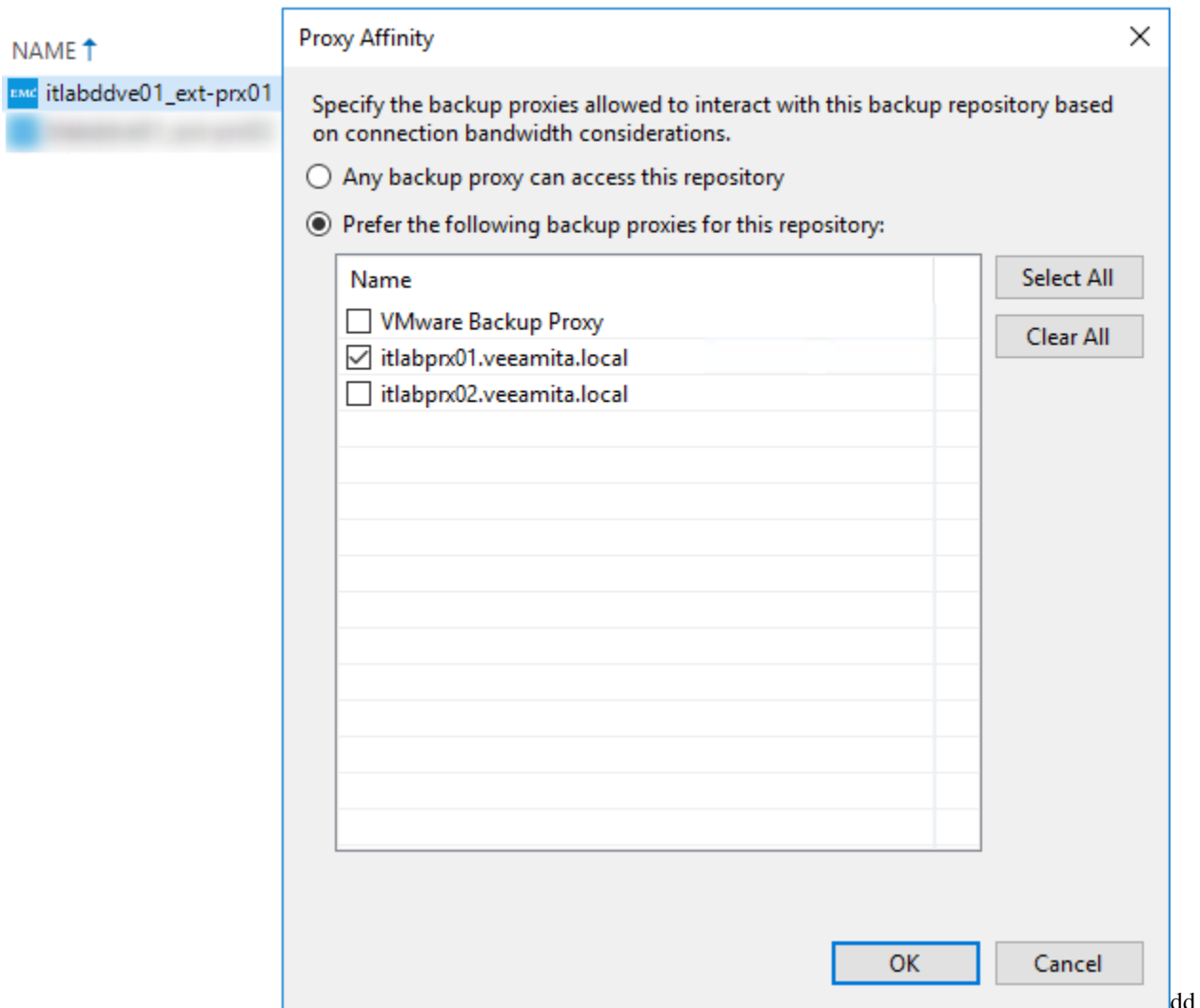
REPOSITORY TOOLS: Add Repository, Edit Repository, Rescan, Upgrade, Manage Repository, Tools

BACKUP INFRASTRUCTURE

NAME	TYPE	HOST	PATH
itlabddve01_ext-prx01	Dell EMC Data Domain	itlabprx01.veeamita.local	ddboost://itlabddve01.veeamita.local:su-itlabvbr01-ddboost@/itlabprx01
itlabddve01_ext-prx02	Dell EMC Data Domain	itlabprx02.veeamita.local	ddboost://itlabddve01.veeamita.local:su-itlabvbr01-ddboost@/itlabprx02

repo conf 6

1. For each repository configure the proxy affinity to avoid unnecessary traffic between the proxies (all the proxies must reach directly their backup repository without using a different gateway server):

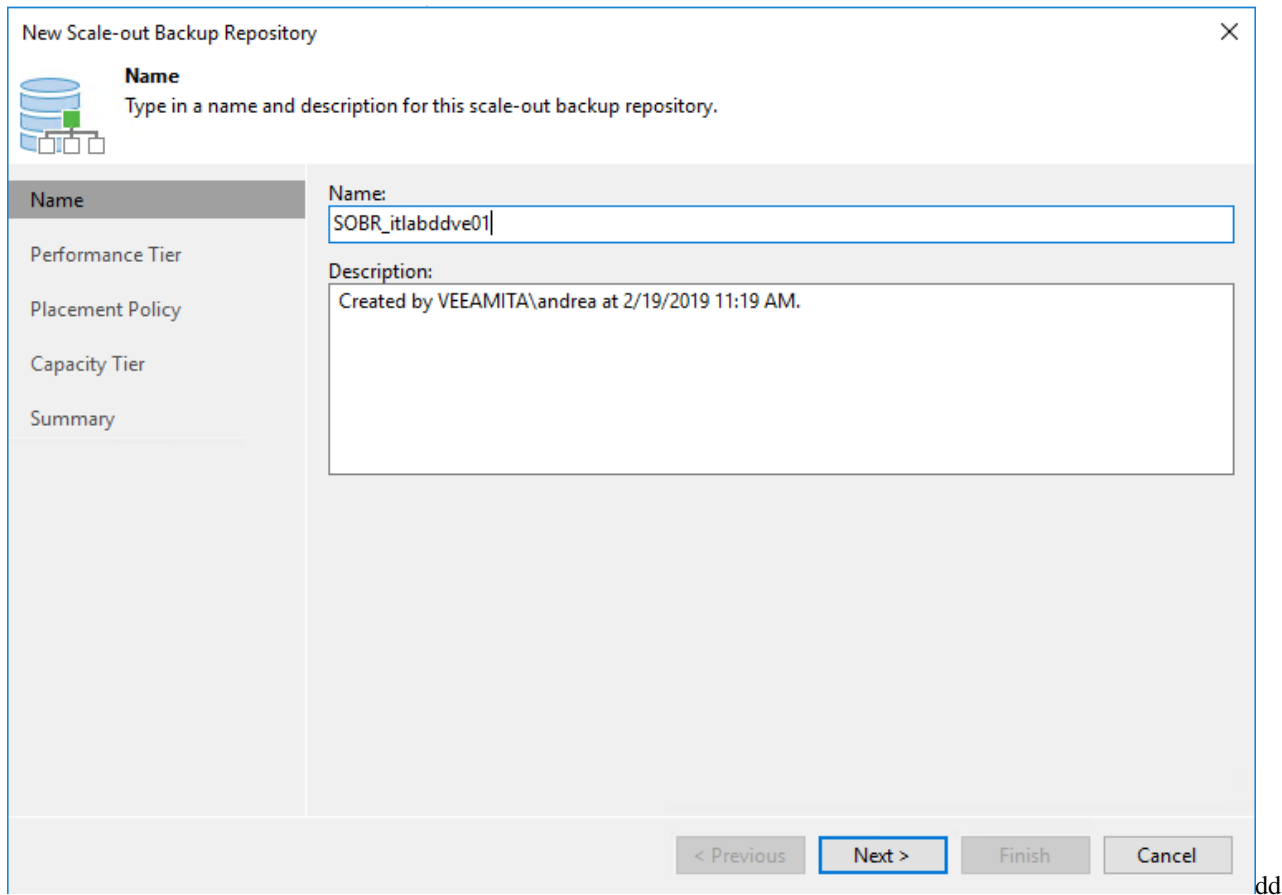


repo conf 7

Setting up Scale-out Backup Repository

The Scale-out Backup Repository is needed to keep the management as simple as possible and to not manually assign backup jobs to a single backup repository (and therefore to a single proxy – losing all the benefits of the parallel processing).

1. Name the Scale-out Backup Repository:



New Scale-out Backup Repository

Name
Type in a name and description for this scale-out backup repository.

Name

Performance Tier

Placement Policy

Capacity Tier

Summary

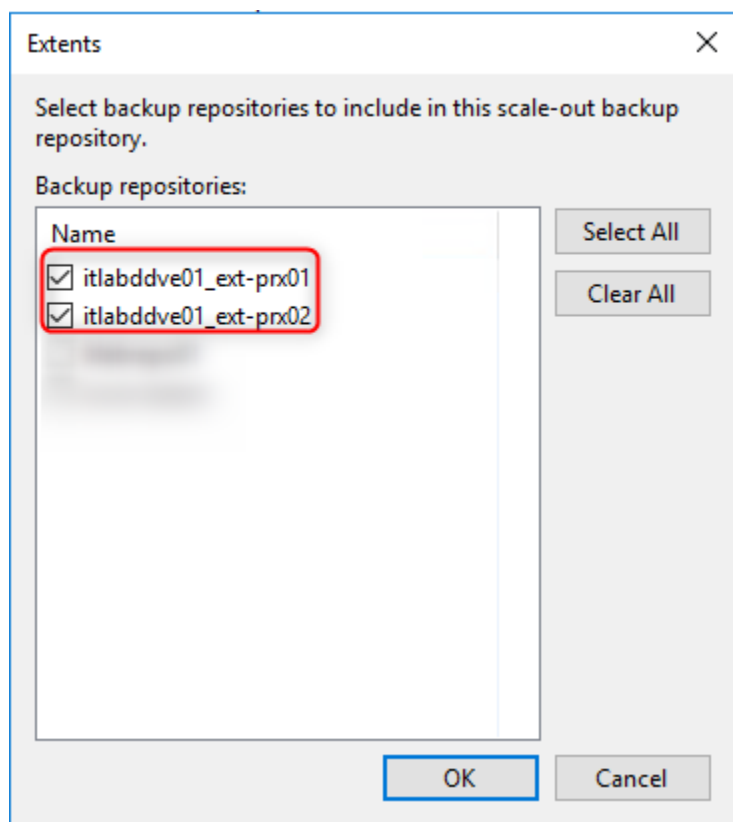
Name: SOBR_itlabddve01

Description: Created by VEEAMITA\andrea at 2/19/2019 11:19 AM.

< Previous Next > Finish Cancel

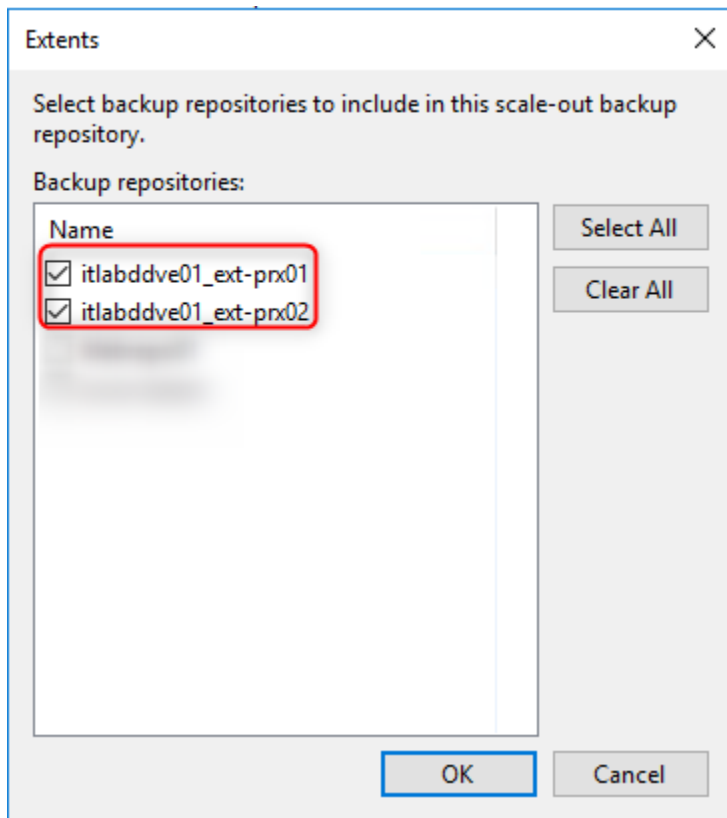
sobr 1

1. Add the extents:



dd sobr 2

1. Set the Scale-out Backup Repository in 'Data Locality' mode for a better distribution of the backup file with the extents:



dd sobr 3

Creating backup jobs

Backup jobs can be configured point the Scale-out Backup Repository and they will benefit of the parallel processing at maximum scale: VMs can be processed using all the proxies available and each proxy will write backup data directly on its extent.

1. Create the backup job and use the Scale-out Backup Repository as repository leaving proxy selection algorithm to automatic (Data Domain suggested tweaks will be set automatically):

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:
Automatic selection Choose...

Backup repository:
SOBR_itlabddve01 (Created by VEEAMITA\andrea at 2/19/2019 11:19 AM.) Map backup

142 GB free of 142 GB

Restore points to keep on disk: 14 i

☐ Configure secondary destinations for this job
Copy backups produced by this job to another backup repository, or to tape. Best practices recommend maintaining at least 2 backups of production data, with one of them being 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

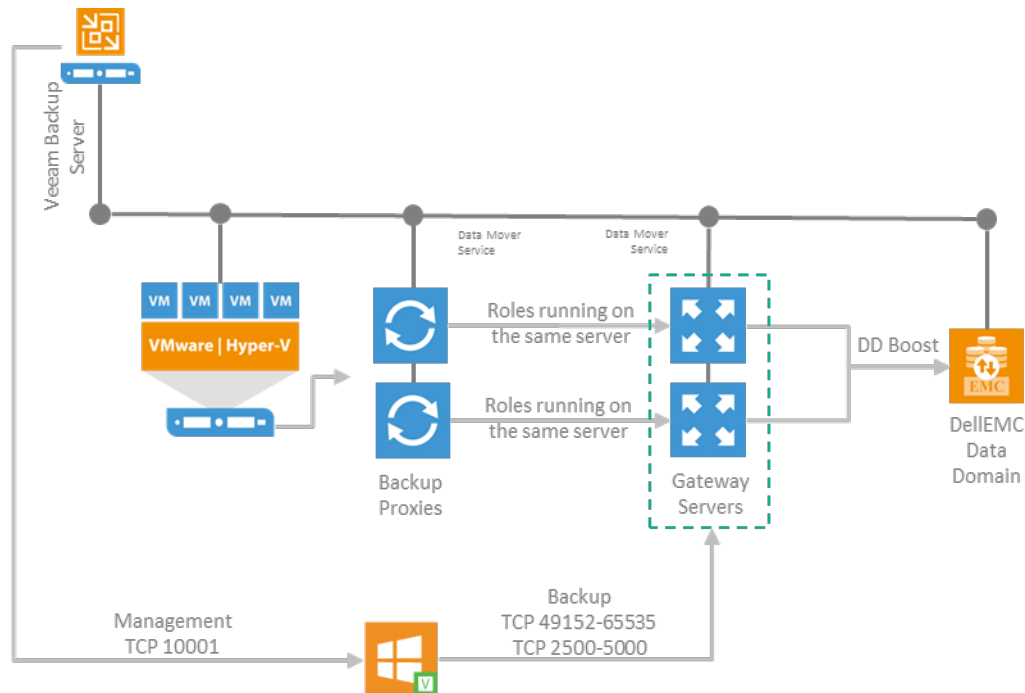
backup job configuration 1

1.27.5 Working with Veeam Agents

VAW

Veeam Agent for Windows supports Dell EMC Data Domain Boost and it can write backup passing through the gateway servers.

The same architecture mentioned above can be used:



dd VAW 1

VAW jobs will use the same Scale-out backup Repository used for VMs backup.

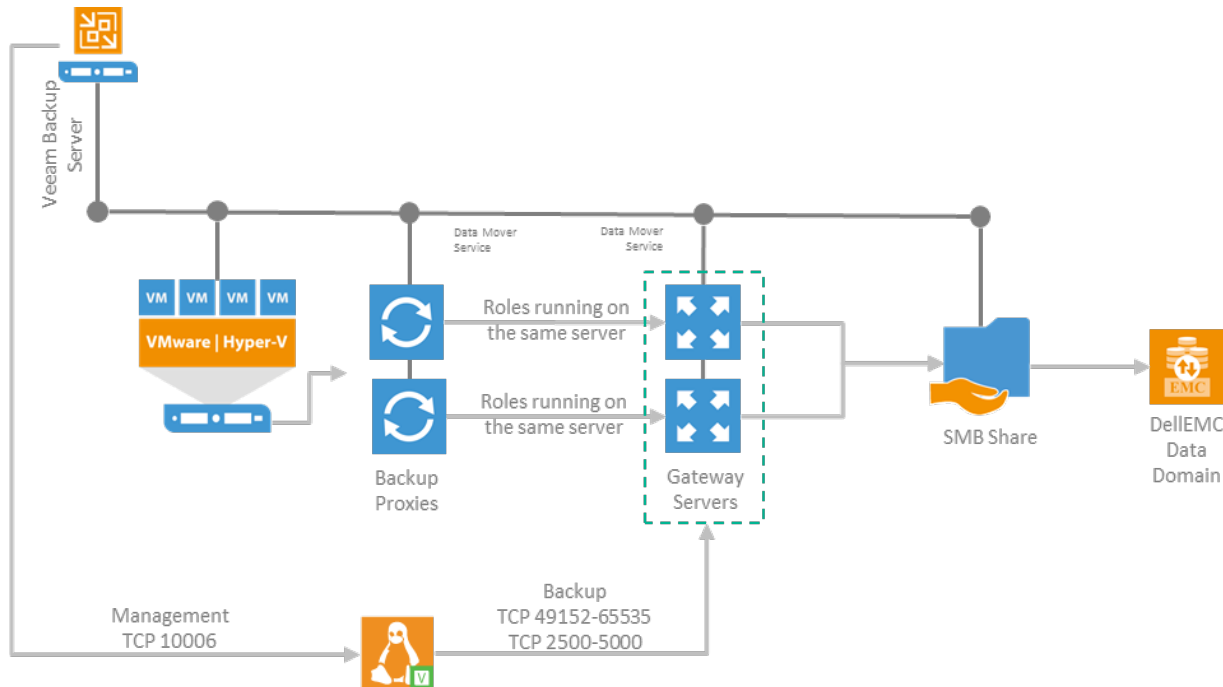
The suggested backup mode, like any other VM job targeting a Data Domain, is incremental with synthetic full as it will be performed moving existing blocks.

VAL

Things for Linux agents are slightly different as VAL does not support yet DDBOOST.

To overcome this limitation, it is recommended to create a dedicated MTree that will be used as NAS repositories. Even though Data Domain supports multiple protocols on the same MTree, it is not recommended: at the first repository rescan, having the same data accessible from different repositories the entire backup catalog would be imported twice (or even more times).

Depending on the number of agents deployed it is possible to leverage the same scalable architecture using either multiple gateways, each one with its own backup repositories (a sub-folder within the same MTree) or simplifying a little bit the architecture using just one repository and leaving the gateway selection to automatic.



dd

VAL 1

Regarding the data transfer, it will benefit of Veeam's compression only. The deduplication will happen asynchronously, as soon as the backup files will be written on the Data Domain.

The backup repository, that will be created as NAS repository, must be properly set. Veeam provides auto-configuration for all the different kind of supported repositories. However, in this case a general SMB share will be used and all the advanced attributes must be manually set according to the Best Practice guide [recommendations](#).

As there is no DDBOOST integration, the suggested backup mode is incremental with Active weekly full. To tune properly backup jobs, follow Veeam's Best Practice dedicated [section](#).

Data Domain uses a single dedupe domain so no matter how many MTree will be used, all the data written into it will be deduplicated globally.

1.28 Backup Repository

Before you start planning for the repository, go through Veeam Backup & Replication online documentation at <https://helpcenter.veeam.com> to get basic understanding of repositories.

You can balance the load across the backup infrastructure by setting up several repositories in the environment and limiting the number of concurrent jobs for each repository, or if you have a proper license you can leverage Scale-out Backup Repository as explained later on in this section.

1.28.1 The 3-2-1 rule

The 3-2-1 rule states that an environment, in order to be properly protected, has to have **3 copies of data, stored on 2 different media, with at least 1 copy in a different location**. Each of the parts of the rule involves the use of a storage device, that's why a Backup Repository is such a key component in each Veeam deployment.

The 3-2-1 rule however is a data protection strategy, whereas **availability** requires the different storage implemented in this strategy to support additional capabilities like:

- Instant VM recovery
- File transforms
- Distant copies
- Item restoration
- Sure Backup

This is the reason why v9.0 introduced two major new features for Veeam backup repositories : **Scale-out Backup Repository** and **Per-VM Backup chains**.

1.29 Repository Type

Being storage-agnostic, Veeam Backup & Replication supports a wide range of repository types, each offering its own set of specific capabilities. So when deciding on repository storage, you might consider the following:

- Capacity
- Write performance
- Read performance
- Data density
- Security
- Backup file utilization

As a basic guideline, a repository should be highly resilient, since it is hosting customer data. It also needs to be scalable, allowing the backup to grow as needed.

Organization policies may require different storage types for backups with different retention. In such scenarios, you may configure two backup repositories:

- A high-performance repository hosting several recent retention points for instant restores and other quick operations
- A repository with more capacity, but using a cheaper and slower storage, storing long-term retention points

You can consume both layers by setting up a backup copy job from the first to the second repository, or leverage Scale-out Backup Repository, if licensed.

1.29.1 Server-Based Repository: DAS or SAN?

Direct-Attached Storage (DAS)

This is an easy, fast and lowcost way to use storage. It is a new approach to use microsegmentation instead of monolithic solutions. The DAS approach is in terms of performance a very fast solution. It can be used as a dedicated system to one Cluster or in a Scale-out Backup Repository. DAS is a normal industry standard x64 server with a bunch of disks attached to it.

- It is recommended to use a performant RAID controller with local battery cache. Be aware of any RAID overhead when designing a DAS solution. Typically RAID 6/60 (depends on the amount of disks) is recommended (IO overhead of factor 6). The Stripe Size should be 256KB or greater.
- Since a DAS storage can be fully dedicated to backup operations, this type of repository is considered to offer a good balance between “performance” and “cost” factors.

- A strong benefit of a DAS repository is that it supports the features offered by Veeam Backup & Replication in a very flexible way. In particular, it provides good read and write performance, sufficient for Veeam vPower-based features (such as Instant VM Recovery, SureBackup, and others). As it typically provides good random I/O performance, it will be the optimal solution when using I/O intensive backup modes such as reverse incremental or forever forward incremental (also used in backup copy job).
- For scalability you can scale vertical (more disks in an enclosure or additional) and horizontal (more servers, if e.g. the network throughput is reached, the SAS channels are saturated, more IOPS are needed for restore reasons)

Tip: When using Microsoft based repositories, use the RAID controller, to build the RAID set and set the Stripe Size there. Don't use any kind of Software or HBA based RAID Level.

| Pros | Cons | |-----|-----| | Cost | single Point of Failure is the RAID Controller | Performance | | Simplicity | | Microsegmentation |

SAN Storage

This is an advanced and manageable solution that offers the same advantages as DAS, and adds more advantages like higher availability and resiliency.

The volume size and quantity are easily adjustable over time, thus offering a scalable capacity.

Tip: You can configure multiple backup repositories on the SAN storage to increase repository throughput to the storage system.

| Pros | Cons | |-----|-----| | Reliability | Complexity | | Performance | Cost | | Technical capabilities | Monolithic approach |

1.29.2 Windows or Linux?

The main difference between Windows and Linux in regards to Veeam repositories is the way they handle NAS shares – this can be summarized as a choice between NFS and SMB. It depends on your IT infrastructure and security what is better to manage and to maintain.

1.29.3 Physical or Virtual?

You can use a virtual machine as a repository server, however, keep in mind that the storage and associated transport media will be heavily occupied.

If you are using a SAN storage, it can be accessed through software iSCSI initiators, or directly (as a VMDK or RDM mounted to the Repository VM).

Best practice is to avoid using the same storage technology that is used for the virtualized infrastructure, as the loss of this single system would lead to the loss of both copies of the data, the production ones and their backups.

In general we recommend whenever possible to use physical machines as repositories, in order to maximize performance and have a clear separation between the production environment that needs to be protected and the backup storage.

1.29.4 NTFS or ReFS?

You can use both filesystems from Microsoft as filesystem for a Veeam Repository. Both filesystems have different behaviour during different backup situations.

NTFS:

When using NTFS please make sure that

- the volume is formatted with 64KB block size

Be aware of the following points during synthetic operations

- NTFS will read and write all blocks during a merge or synthetic full operation, which will result in a very high IO load and a high resulting queue length of the storage system
- The highest impact to disk queue length will be in a per VM mode merging an incremental in FFI or Reverse Mode

ReFS:

ReFS is using linked clone technology. This is perfect for synthetic operations and will save dramatic IOs and throughput during operations like merges or creating synthetic fulls.

When using ReFS please make sure that

- the volume is formatted with 64KB block size
- check <https://docs.microsoft.com/en-us/windows-server/storage/refs/refs-overview>
- Configure 256 KB block size on LUNs (Storage or RAID Controller)
- never bring linked clone space savings into your calculation for required storage space
- make sure your server has 1 GB RAM per 1 TB used on repository, add additional 8 GB for the Windows Server operating system.
- „All ReFS supported configurations must use Windows Server Catalog certified hardware” - please contact your hardware vendor
- Never use any shared LUN concept with ReFS and a Veeam Repository
- Check the existing driver version of ReFS. The minimum should start from ReFS.sys 10.0.14393.2097
- ReFS will flush metadata during synthetic processes to the disk very pushy. These meta data flushes are based on 4KB blocks. Your controller and disk system should be able to handle these OS related system behaviours.

1.29.5 SMB Share

When using a SMB share as target please check the following points

- SMB 3.x.x must be fully supported by the storage vendor or Windows Server (recommended Windows Server 2016+)
- To improve performance and reduce the latency impact, use one of the RDMA features Windows Server provides with SMB direct. RoCE or iWarp.
- a 10 Gbit/s network interface can be saturated with modern CPUs. If the repository is able to write faster than consider 40 Gbit/s connections between source and repository
- Try to avoid too many routing hops between source and Veeam Repository this will add latency and reduce your performance
- When an application writes data to an SMB share using WinAPI, it receives success for this I/O operation prematurely - right after the corresponding data gets put into the Microsoft SMB client's sending queue. If subsequently the connection to a share gets lost – then the queue will remain in the memory, and SMB client

will wait for the share to become available to try and finish writing that cached data. However, if a connection to the share does not restore in a timely manner, the content of the queue will be lost forever.

1.30 SMB Repository

While an SMB repository is often considered to provide less performance than direct attached storage, it still can provide very good results as a repository due to leveraging Veeam's load-balancing technology for write operations, as explained in the next sections.

1.30.1 Gateway Server

When you set up an SMB share as a repository, the following options are available:

- Automatic selection of the server as the SMB gateway proxy (that is, the server that will host the target-side transport component and thus perform the role of “data writer” towards the SMB share itself).
- Specify a specific server (among the available managed Windows servers in Veeam Backup & Replication) as an SMB gateway proxy.

The second option is very helpful in situations where the SMB share is located on a remote location, since it avoids that the automatic selection uses a server that is not local to the SMB share, thus having all synthetic operations or backup copy jobs occurring over the WAN link (which is usually slower than the local link). It is always recommended to use an SMB gateway server as close as possible to the SMB storage. By specifying the SMB gateway you have a better chance of keeping the data flow under control and avoid data crossing the WAN links unnecessarily.

As single stream performance for SMB repositories may be suboptimal, you can potentially increase performance of your SMB storage by configuring several repositories pointing to the same folder using different gateway servers. With multiple proxies, the automatic SMB gateway may be a good option and can be configured by selecting **Automatic** from the drop-down list.

Tip: Gateway servers must be properly sized as regular Windows repositories. If you are using Automatic mode, remember that the same machine could be elected backup proxy and gateway server simultaneously. Apply sizing accordingly.

Another option for increasing the number of streams is using per VM backup files. Please see the corresponding section of this guide for more information > [Per VM backup files](#)

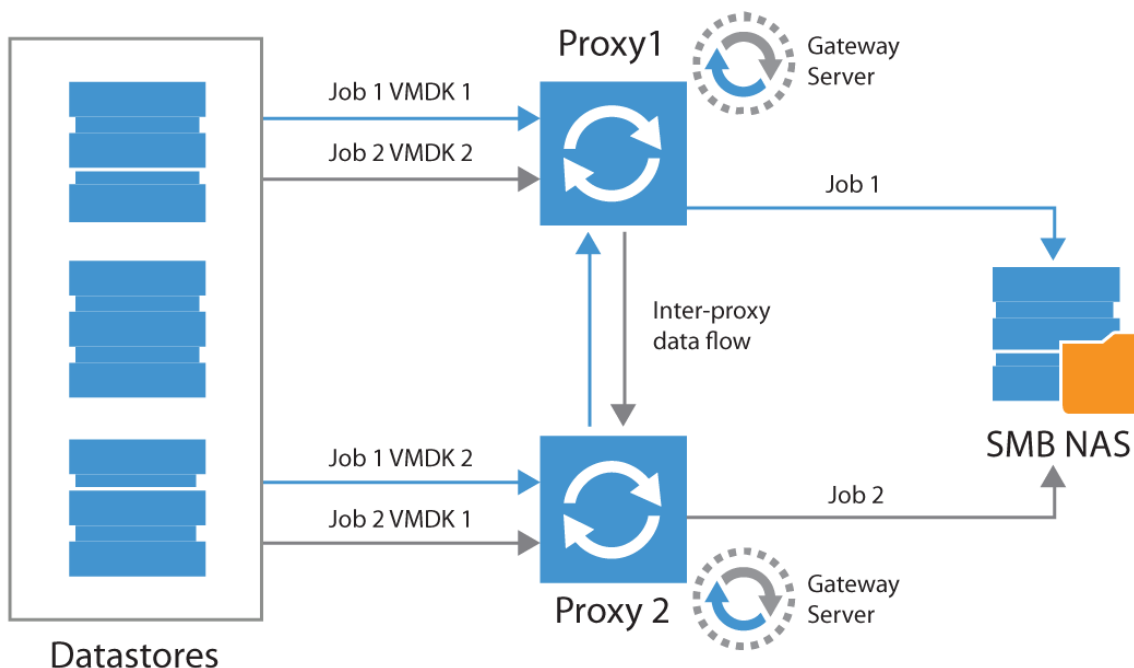
Load Balancing (with Automatic Selection)

Even when multiple proxies are used to process a given backup job, only **one*** Windows server (called “gateway server”) per backup chain will be used to write data to the SMB share. In **Automatic** mode the first selected proxy in the running job will become the gateway server. If per-vm backup files are enabled, this applies to each per-vm chain, thus multiple gateway servers may be started concurrently.

Here are some recommendations for managing backup proxies used as gateway servers:

- The networking between the multiple proxies should be sized correctly to allow data to flow from each proxy to the gateway server.
- As the first backup proxy of a job is used as the gateway server, it may happen that all the gateway server instances of different jobs (or per-vm backup file chains) are started on the same proxy. This requires proper sizing of CPU and RAM; ensure resource monitoring is in place.

Note: Consider that increasing the number of jobs also increases the number of threads to the NAS storage.



Scaling out using this approach will allow for processing larger amounts of data and optimize the throughput of the SMB shares. Best practice for large scale environments is to use at least a mid range or enterprise NAS storage system that provides good I/O performance. Low end NAS devices often have non official implementations of the SMB protocol that may improve performance test results, but may also corrupt backup files. For these devices it is discouraged to use SMB.

1.31 Deduplication Appliances

1.31.1 Overview

Deduplication applied to storage is a technique aimed at reducing the storage space consumption.

Deduplicated storage systems are often optimized for write operations and can offer rather high ingest rates. However, any random read I/O may suffer from re-hydration processes required during restores. For this reason we recommend to use these devices mainly as secondary targets, where parameters like price per GB are more important than restore performance.

1.31.2 Using a Deduplication Appliance

As a storage-agnostic product, Veeam Backup & Replication can use any deduplication appliance as a repository in different use cases: primary backup repository, backup copy repository, and Virtual Tape Library (VTL) container.

1.31.3 Deduplication Appliance as a Primary Backup Repository

Unless you are using DDBoost protocol on EMC DataDomain storage or Catalyst on HPE StoreOnce, you should configure primary jobs for forward incremental with active full backups - since jobs with transformation will require

block “de-hydration” and then “re-hydration” on the storage. Such operations require significant time and I/O.

Note: “Re-hydration” is the act of restoring the original blocks in a non-deduplicated form. During backup files transformation the same blocks are read and then written back to the appliance where they are de-hydrated (deduplicated) again. This two-step process can generate significant load on the appliance, slowing down operations.

Also, consider that Instant VM Recovery might not be as fast as expected – unless the deduplication appliance offers a fast non deduplicated area for the most recent restore points (such as ExaGrid).

The downside of active fulls is the need to transport the entire amount of virtual machines on a weekly/monthly basis. This can lead to long snapshot commit, so this mode needs to be planned carefully. It is recommended to limit the use for primary backup jobs to the integrated deduplication appliances, where synthetic operations can be used.

1.31.4 Using Deduplication Appliance as a Backup Copy Repository

By default a backup copy job applies transformations to the backup chain. This could lead to the “de-hydration”/“re-hydration” overhead at the end of the backup copy job cycle, due to synthetic full or transformation. When using non-integrated appliances, use the option of Active Fulls for Backup Copy jobs.

If one of the integrated appliances is used, synthetic operations will be performed on the appliance itself, so they will require minimal additional time and lower I/O.

1.31.5 Using Deduplication Appliance as a Virtual Tape Library

If a deduplication appliance is used in Virtual Tape Library (VTL) mode, it is required to store the backup files in a staging area, which is uncompressed. Sending compressed and/or deduplicated backup files to a VTL will compromise the efficiency of the deduplication appliance.

The repository used for staging should be configured with “Decompress before storing” advanced option enabled, which ensures previously applied compression at the job level is ignored.

Also, ensure that the appliance meets Veeam tape requirements described in the [User Guide](#).

1.31.6 File-Level Recovery and Veeam Explorers

By design, Veeam Explorers perform a large amount of random read operations on the backup repository. To optimize for such operations on deduplication devices, following the job and repository configuration best practices (see below) is paramount. If the recommendations are not fully implemented, this may lead to significant waiting time when launching file-level recovery or Veeam Explorers.

To further reduce restore time, it is recommended to enable file-level indexing for backup jobs located on deduplication repositories. Indexing VMs will remove the waiting time for mounting a restore point when browsing contents via Enterprise Manager.

1.31.7 Best Practices

In this section, we will distinguish between integrated and non-integrated deduplication appliances.

Integrated appliances are:

- HPE StoreOnce - via Catalyst API
- EMC DataDomain - via DDBoost API
- ExaGrid - via integrated Veeam datamover

If the mentioned integration API is unavailable due to licensing restrictions, or if any other deduplication appliance is used, the appliance should be considered *non-integrated*.

One special case of deduplication appliance is Quantum DXi. Quantum features integrated data mover service that is able to assist Veeam Backup and Replication without need to add an appliance as a special type of repository (see [Quantum and Veeam new integration](#) for more details and [KB2155](#) for specifics of job configuration).

In order to optimize throughput for deduplication appliances, please use the following configuration guidelines:

Job configuration

The following settings are configured in the backup job “Edit” wizard under Storage > Advanced. Options not defined in this table are optional and not related to backup repositories using deduplication storage.

Configuration tab	Setting	Value
Backup	Backup mode	Incremental
Backup	Create synthetic full backups periodically	Enabled - if integrated
Backup	Transform previous backup chains into rollbacks	Disabled
Backup	Create active full backups periodically	Enabled - if non-integrated
Maintenance	Perform backup file health check	Disabled
Maintenance	Defragment and compact full backup file	Disabled
Storage	Enable inline data deduplication	Disabled
Storage	Exclude swap file blocks	Enabled
Storage	Exclude deleted file blocks	Enabled
Storage	Compression level	Optimal
Storage	Storage optimization	Local target (16TB+ backup files)
Storage	Enable backup file encryption	Disabled

Hardware assisted encryption is available for EMC DataDomain via DDBoost, but must be configured in the integration specific repository configuration. If enabled on the job level data reduction efficiency will be significantly degraded.

Repository configuration

The following settings are configured in the “Edit Repository” wizard under Repository > Advanced.

Setting	Value
Align backup file data blocks	Enabled - only if repository uses fixed block size deduplication (almost never true)
Decompress backup data blocks before storing	Enabled
This repository is backed by rotated hard drives	Disabled
Use per-VM backup files	Enabled

1.32 Deduplication integration specifics

1.32.1 EMC DataDomain

Selecting DataDomain as a repository will automatically recommend job and repository settings according to best practices. For more information, refer to vendor guidelines.

DDBoost allows for the following capabilities:

- Source side deduplication between the Veeam gateway server and DataDomain appliance. This will reduce the amount of data sent over the network to the appliance
- Better LAN parallelization, since DDBoost manages its own network load balancing algorithms which are considered more efficient than standard network links aggregation
- Seamless Veeam files transformations like synthetic full or forever forward incremental
- DDBoost can be used through Fibre Channel SAN, providing a totally LAN-free backup solution

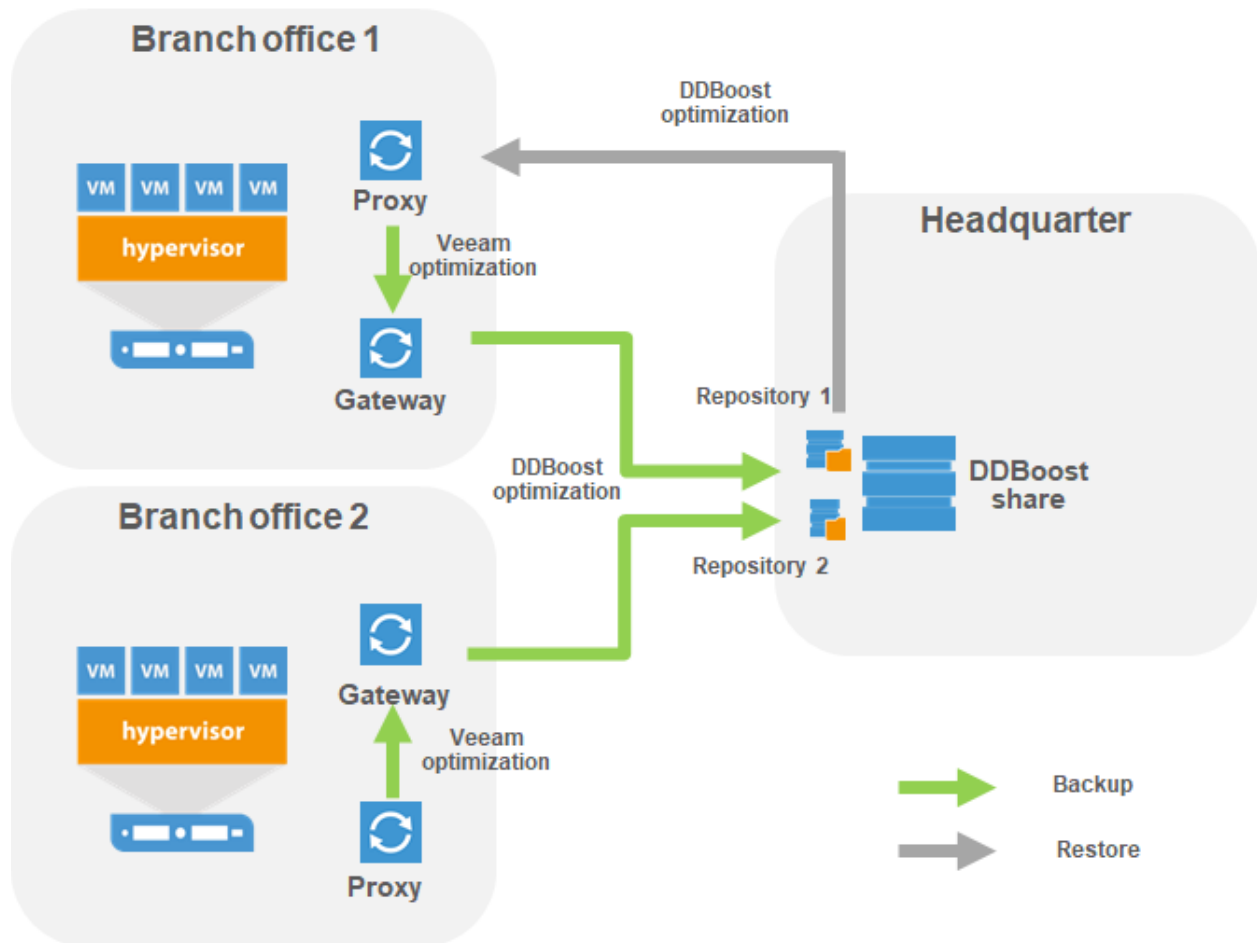
For more details, refer to the DDBoost configuration guide by Rick Vanover: [Best Practices for EMC VNX/VNXe and Data Domain with Veeam Availability Suite](#).

DDBoost over WAN backup copy jobs and Remote Office/Branch Office configuration

When leveraging Backup copy jobs and DDBoost over a WAN network, specific attention should be paid to the mount server location to optimize the network traffic.

As specified in the user's guide, DDBoost API is leveraged on the gateway server when it is explicitly defined in the repository properties.

- Since it is sending deduplicated data to the DDBoost share the gateway server must reside as close as possible to the source data.
- The gateway server being part of the repository properties, one DDBoost repository shall be created per remote site.
- To limit the number of objects created on the DataDomain, it is possible to create many Veeam DDBoost repositories pointing to a single DDBoost share, changing only the name and gateway server. For such configuration the number of parallel tasks allowed on each repository must be considered globally. It is recommended to set it to a small amount at first sight to avoid overflowing the common DDBoost share.
- During restore process, the rehydration is performed on the proxy used by the restore job. It is advised to manually select a proxy residing as close as possible to the restored guest host during the restore task configuration.



API role distribution

DDBoost

Chain Length Limitation

Consider that DataDomain can support only up to 60 incremental restore points for a single full backup. For details, refer to the Veeam Backup & Replication User Guide: [Limitations for EMC Data Domain](#)

Configuring DDBoost over FC device set

When configuring datadomain over FC, it must be decided how many DFC devices should be advertised to the repository gateway.

Andrea Borella posted an interesting article on [why and how to configure DDBoost for FC connection](#) based on an EMC publication [EMC® Data Domain Boost for Partner Integration](#) which is summarized below.

Qdepth limitation

The Data Domain system imposes a limit of 64 simultaneous requests to a single DFC SCSI device (qdepth). Because of this limit, the number of devices advertised needs to be tuned depending on the maximum number of simultaneous jobs to the system at any given time. Knowing Microsoft Windows is qdepth constrained to one SCSI request at a time through each of its generic SCSI device, the number of devices to advertise on the DataDomain side can be calculated using the following rules:

- **D=max(X,Y)** where
 - D is the number of devices to advertise on the DataDomain
 - X is the Number of DFC needed on the DataDomain to stand the parallelisation
 - Y is the requested number of SCSI targets on the Gateway server to respect the parallel tasks number as configured.

On the DataDomain side: X calculation

- Let J be the maximum number of simultaneous jobs running using DFC to the DataDomain system at any given time.
- Let C be the maximum number of connections per job:
 - 3 for Data Domain Extended Retention Systems
 - 1 for other types Data Domain systems
- Maximum simultaneous connections to the DD system:
 - **S = JxC**
 - DFC Device Count **X=roundup(min(64, 2x(S/128)))**
 - All DFC access groups must be configured with “X” devices.
- Let's assume the gateway/repository is configured for
 - 60 parallel tasks
 - Only one gateway will access the DataDomain MTree
 - **S=60x1=60**
 - **X=roundup(min(64,2x(60/128)))=1**

A single DFC can support 60 active connections.

On the server side: Y calculation

Assuming that:

- the repository is configured for 60 parallel tasks: **J=60**.

- the Gateway server is configured with 2 FC initiators
- the DataDomain has 2 FC targets
- Zoning is such that both targets are presented to both initiators
- gateway will then access each DFC through 4 physical path and will use 4 generic SCSI devices to access a single DFC, allowing up to 4 parallel tasks for a single DFC: **P=4**.
- **Y=J/P=60/4=15**

The windows server needs 15 DFC to keep 60 tasks in parallel.

Final result

- **D=max(X,Y)=max(1,15)=15**

We need to configure 15 DFCs on the DataDomain.

1.32.2 ExaGrid

ExaGrid appliances run an integrated Veeam data mover similar to a Linux based backup repository. With ExaGrid, there is no requirement for a Windows based gateway server.

See [ExaGrid Storage Best Practices](#) for more information.

As a rule of thumb, the “landing zone” (which is the zone that will hold most recent set of data) should have sufficient capacity to keep at least an uncompressed full backup and one incremental as computed on the online repository sizer, so that each backup can fully be written there and processed. This ensures Backup copy, SureBackup, Instant VM Recovery and item-level restores will be usable for the latest restore point without rehydration overhead.

Exagrid Best Practice guide

You can refer to [Veeam KB 2056](#) for a precise configuration guide. The official Exagrid configuration guide is directly available in the Exagrid appliance help section (Help/Named VM backup applications/Using Veeam Backup and Replication software with an Exagrid system).

Exagrid and Scale Out Backup repository

Starting with Exagrid software 5, an Exagrid appliance can be configured as part of a grid and as a Scale Out Backup Repository extent. The difference between the landing zone and the global deduplication area should then be considered.

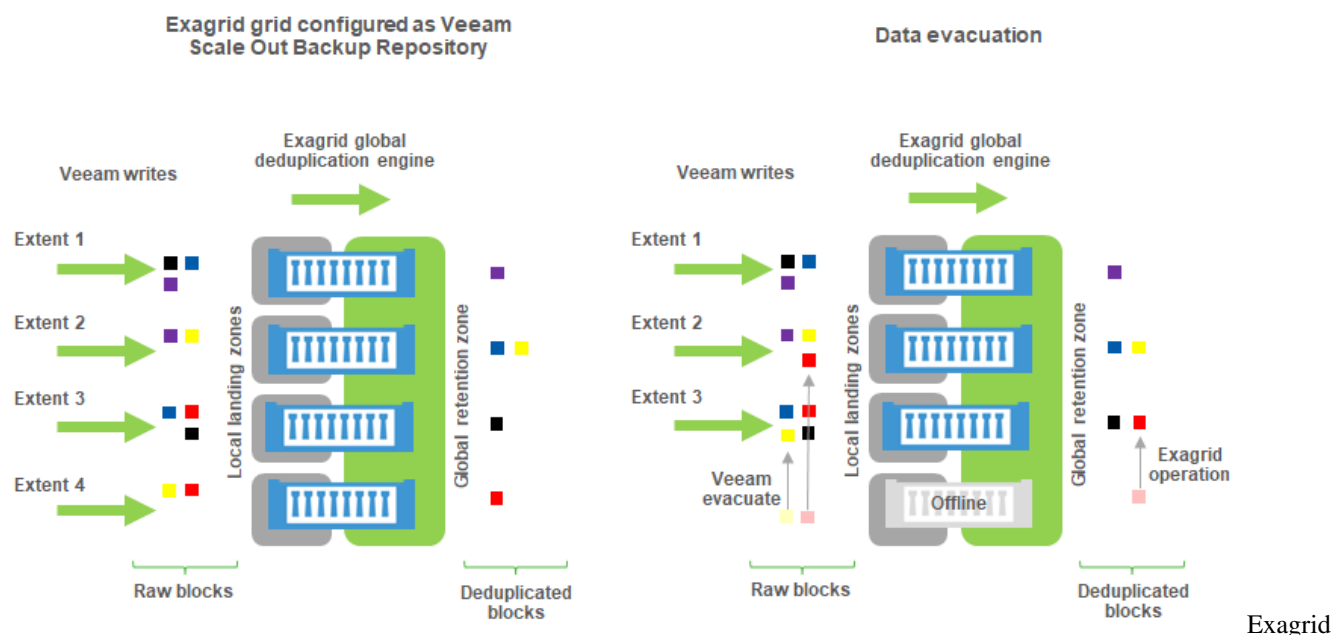
As a matter of fact, the deduplication engine will run asynchronously and deduplicate the landing zone into a global retention zone for each grid member. Whenever a deduplicated block is already hosted on a member of the grid, it will not be treated by the local grid member.

As a consequence, each member of the grid will be considered as a unique extent holding its own data by the Veeam Scale Out Backup Repository engine, while the deduplicated data effectively used by the extent could reside on a different member of the grid.

In case of extent maintenance the landing zone will be brought offline by the Scale Out Backup Repository manager. All the backup chains kept in the landing zone will be unavailable while the deduplicated part of the data held by appliance where the offline extent resides will still be available to the other members of the grid. All chains but the ones hosted on the offline member will be available for Veeam operations.

If an evacuate operation is triggered on the Veeam Backup and Replication side to remove an appliance from the grid only the landing zone will be evacuated by the Veeam transport agent. The deduplicated data should thereafter be evacuated through a specific process handled by the Exagrid support.

If the grid member becomes offline before being evacuated by Exagrid support some unique deduplicated blocks might be lost potentially corrupting all the backup chains of the grid.



Scale Out Backup Repository

1.32.3 HPE StoreOnce

Selecting StoreOnce appliance as a repository will automatically recommend job and repository settings according to best practices. For more information, refer to vendor guidelines.

When using HPE Catalyst, consider the following recommendations:

If the Catalyst Store is configured as **High Bandwidth** on the appliance, Low Bandwidth mode can be forced using the specific option "Gateway server and StoreOnce are connected over WAN" in the repository properties.

If the Catalyst Store is configured as **Low Bandwidth**, additional payload verification is introduced. Over high latency connections, disabling the verification may improve performance. However, the defaults should be left for local connections.

Catalyst low bandwidth, backup copy jobs and Remote Office/Branch Office configuration

Same considerations as per DataDomain should be taken into account.

Chain Length Limitation

HPE StoreOnce has a limit on the number of concurrently opened files, this limit is important when restoring VM's. The maximum length of a backup chain (Full backup file plus all incremental backup files) depends on which HPE StoreOnce model is used. Lookup your HPE StoreOnce model in: [Limitations for HPE StoreOnce](#) to find the maximum limit.

Backup copy job and Catalyst feature

A backup copy job is by definition a forever forward incremental job.

If it is required to keep more restore points than allowed by the chain length limitation, then the GFS retention on a weekly basis must be enabled alongside with the “Read the entire restore point from source backup...” option selected.

This will disable the Catalyst synthetic full feature on the backup copy job and force an active full backup copy process (eg. full read of the primary backup chain on the GFS schedule basis). The backup copy job will then be processed as an **Active full and Incremental** job.

1.33 Windows Server Deduplication

Follow the recommendations provided in the configuration guidelines above; here is the summary:

1. Use **Windows 2012 R2** or **Windows 2016** and apply all patches (some roll-ups contain improvements to deduplication). Having most up to date system is critical for ensuring data safety.
2. Format the disk using the command line “/L” option (for “large size file records”) and **64KB** cluster size (use parameters /Q /L /A:64K)
3. Follow [compression and deduplication guidelines](#) for non-integrated deduplication storage in previous chapter.
4. (For Windows Server 2016 and later) the “Virtualized Backup Server” deduplication profile is to be preferred ([check the following link](#))
5. Modify garbage collection schedule to run daily rather than weekly.
6. Use backup jobs configured to perform Active full with Incrementals.
7. If possible, spread active full backups over the entire week.
8. Try to keep the .VBK files below 1TB in size (there is no official support from Microsoft for files bigger than this; see [https://msdn.microsoft.com/en-us/library/hh769303\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/hh769303(v=vs.85).aspx)). Large files take a long time to deduplicate and will have to be fully reprocessed if the process is interrupted.
9. Where possible, use multiple volumes. Windows deduplication can process multiple volumes using multi-core CPU – one CPU core per volume; see <http://blogs.technet.com/b/filecab/archive/2014/12/04/sizing-volumes-for-data-deduplication-in-windows-server.aspx> for details.)
10. Configure deduplication process to run once a day, and for as long as possible.

More information on Windows Server 2016 Data Deduplication can be found [here](#).

1.34 Object Storage Repository

The Object Storage Repository cannot be used on its own but has to be configured as [Capacity Tier](#) in the [Scale-out Backup Repository](#).

1.34.1 Lifecycle Rules & Tiering

Do **not** configure any tiering or lifecycle rules on object storage buckets used for Veeam Object Storage Repositories. This is currently **not supported**.

The cause for this is:

1. Tiering and lifecycle rules in object storages are based on object age. However, with Veeam’s implementation even a very old block could still be relevant for the latest offloaded backup file when the block was not changed between the restore points. An object storage vendor can not know which blocks are still relevant and which not and thus can not make proper tiering decisions.

2. The vendor APIs for the different storage products are not transparent. E.g. accessing Amazon S3 or Amazon Glacier requires the use of different APIs. When tiering/lifecycle management is done on cloud provider side Veeam is not aware of what happened and cannot know how to access which blocks.

1.34.2 Manual Deletion

Do **not delete manually** from an object storage bucket used for a Veeam Object Repository. Veeam will take care of deleting old objects based on your configured retention period in the backup or backup copy job.

You can safely delete everything manually when the Object Storage Repository is decommissioned completely (unconfigured in VBR).

1.34.3 Security

Create an own bucket and own user where possible for the Object Storage Repository and limit the user account to have only the required access on the object storage bucket.

1.34.4 Cost Considerations

When using public cloud object storage always consider all costs.

Putting data to the object storage requires API PUT calls. These calls normally cost by the thousand.

When data is at rest the used resources are normally priced by GB/month.

Do never forget prices for restores. These prices do include API requests (GET) but also the egress traffic cost from the cloud datacenter which can be immense depending on how much data is required to be pulled from the cloud. Veeam tries to leverage the locally available data blocks to reduce cost, but blocks which are not present on premise have to be pulled from the cloud.

1.35 Configuration Guidelines

1.35.1 Parallel Processing

A repository can be configured to limit the amount of parallel tasks it can process at a time; with parallel processing enabled (by default) a *task* is one VMDK handled by the proxy during a backup job, or by a repository during a backup copy job. If there are many parallel tasks on the proxy side for only few tasks on the backup repository, this will lead the Veeam scheduler service to wait for available resources on the repository. To prevent such situation, you can figure out on which side the bottleneck will be (proxy or repository) and then set the overall amount of parallel tasks on the proxies equal to the total amount of parallel tasks on the repositories.

Note: Consider tasks for read operations on backup repositories (like backup copy jobs).

1.35.2 General guidelines for virtual repositories

To right sizing a backup repository, consider the following:

- Each vCPU core should have no more than 2 concurrent tasks loaded into it
- For each vCPU, you need to count 4 GB of memory
- With bigger machines, also network limits come into play , and that's another reason to build many smaller repositories

Suppose you have a VM with 8 vCPU. You need 32Gb of memory, and this repository could be able to handle up to 16 concurrent tasks (we can go higher, but that's a good starting point). Now, in general we say that one task doing incremental backups runs at about 25 MB/s, that is 200 Mbit/s. If the VM has the usual vmxnet3 link, that's 10Gb and divided by 200 Mbit/s it gives you a bottleneck at around 50 tasks, that would be 25 vCPU. So, it is not recommended to go above this size or you may end up to overload the network.

Also take into account that multiple virtual repos may be running over the same physical ESXi and its links, so you also need to consider using anti-affinity rules to keep those repos away from each other.

1.35.3 SOBR

For any type of extent, and also for ReFS, we tend to suggest 200TB as the biggest size. Even though some customer go even bigger where a physical server is involved, we recommend to not go too big to avoid potential failures (read also downtime, not just damages). Smaller server equal to smaller failure domains. This goes into combination with what written above, so if you need for example 600TB of usable space, then you know you need 3 extents. Sometime this number is bigger, since for example people using SAN as the source for their volumes can only create up to 64TB volumes, so this becomes the biggest size of a single extent. This is also true for virtual repositories when a VMDK is used, unless you want to use RDM (which we are fine with).

When using SOBR along with ReFS extents make sure you select data locality policy to enable block cloning. With performance policy the backup chain gets split, incrementals and fulls are placed on different extents. ReFS requires all the restore points to be on the same extent.

1.35.4 Blocks sizes

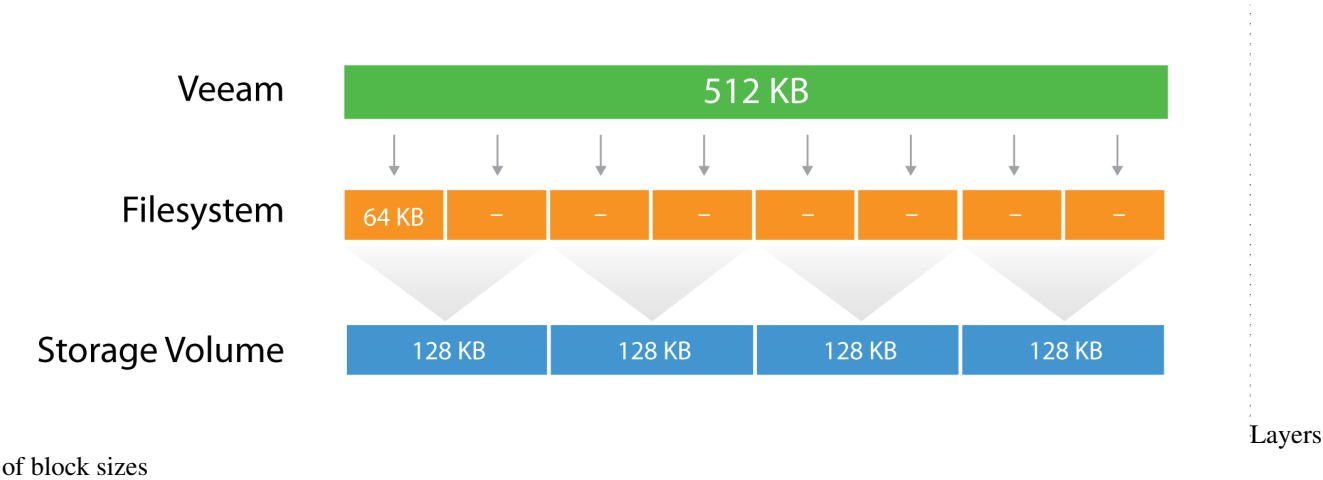
During the backup process data blocks are processed in chunks and stored inside backup files in the backup repository. You can customize the block size during the Job Configuration using the Storage Optimization setting of the backup job.

By default block size is set to **Local target**, which is 1 MB before compression. Since compression ratio is very often around 2x, with this block size Veeam will write around 512 KB or less to the repository per block.

This value can be used to better configure storage arrays; especially low-end storage systems can greatly benefit from an optimized stripe size.

There are three layers where the block size can be configured: Veeam block size for the backup files, the Filesystem, and the Storage volumes.

Let's use a quick example:



The Veeam block size of 512KB is going to be written in the underlying filesystem, which has a block size of 64k. It means that one block will consume 8 blocks at the filesystem level, but no block will be wasted, as the two are aligned. If possible, set the block size at the filesystem layer as close as possible to the expected Veeam block size.

Then, below the filesystem there is the storage array. Even on some low-end storage systems, the block size (also called stripe size) can be configured. If possible, again, set the stripe size as close as possible to the expected Veeam block size. It's important that each layer is aligned with the others, either by using the same value (if possible) or a value that is a division of the bigger one. This limits to a minimum the so called **write overhead**: with a 128KB block size at the storage layer, a Veeam block requires 4 I/O operations to be written. This is a 2x improvement compared for example with a 64KB stripe size.

Tip: As can be seen from the field, optimal value for the stripe size is often between 128 KB and 256 KB; however. It is highly recommended to test this prior to deployment whenever possible.

For more information, refer to this blog post: <https://www.virtualtothecore.com/veeam-backups-slow-check-stripe-size/>

1.35.5 File System Formats

In addition to the storage stripe size alignment, as explained in the previous paragraph, the file system may also benefit from using a larger cluster size (or Allocation Unit Size). For example, during formatting of NTFS volumes, Allocation Unit Size is set to 4KB by default. To mitigate fragmentation issues, configure to 64 KB whenever possible.

It is also recommended to use a journaling file systems (this makes exFAT a less reliable option than NTFS).

1.35.6 Using “Large File” Switch for NTFS

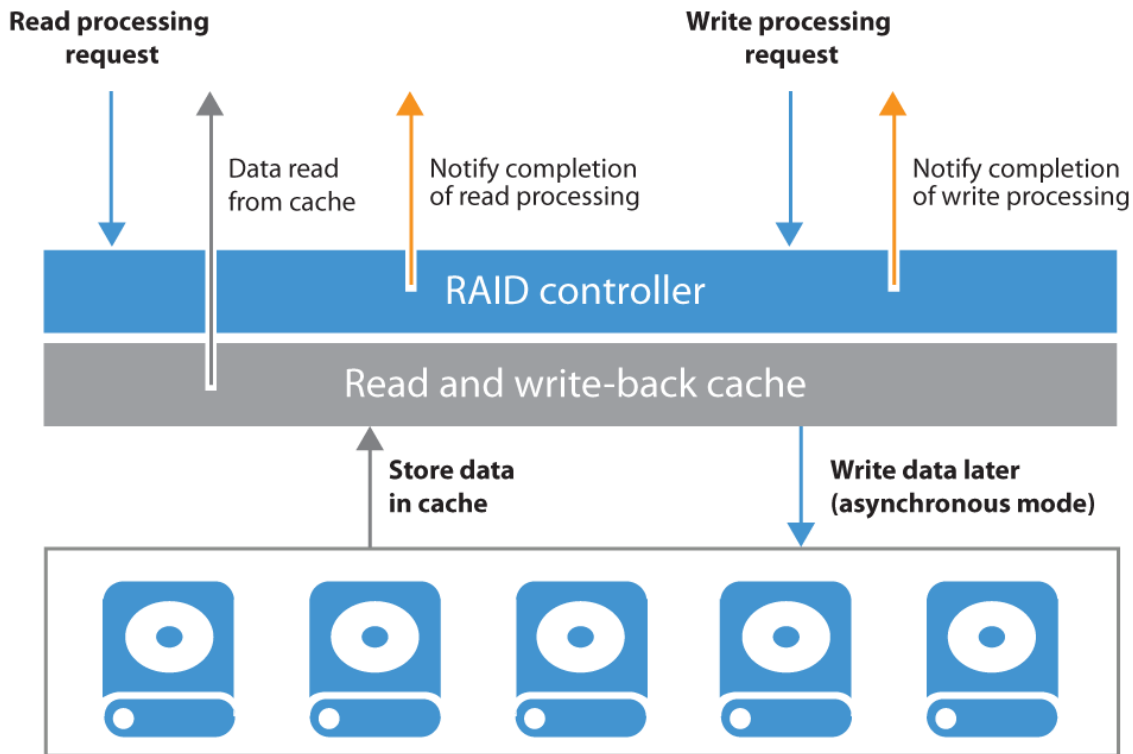
A file size limitation can be occasionally reached on NTFS, especially on Windows Server with deduplication enabled. This happens due to a hard limit reached on the file records size because of the high level of file fragmentation. To mitigate the issue, we recommend to format Windows NTFS repositories with the “/L” (large files) option.

1.35.7 Keeping File Size Under Control

Try to avoid backup chains growing too much. Remember that very big objects can become hardly manageable. Since Veeam allows a backup chain to be moved from one repository to another with nothing more than a copy/paste operation of the files themselves, it is recommended to keep backup chain size (the sum of a single full and linked Incrementals) under 10 TB per job (~16TB of source data). This will allow for a smooth, simple and effortless repository storage migration.

1.35.8 Synthetic Backup and Caching

To get the best out of a synthetic backup and enhance the performance, it is recommended to use a write-back cache. Read and write request processing with write-back cache utilization is shown in the figure below.



1.36 Repository Sizing

In mid-sized or enterprise environments, the recommended amount of CPU for a repository is 1 core per concurrent job that processes data on a repository server. At least 2 cores allow for the Operating System to be more responsive.

Note: When using ReFS add additional 1GB RAM for each 1TB backup stored on the repository.

It is recommended to configure 4 GB RAM per core plus 8 GB for basic OS operations. The same amount of resources are needed for SMB gateway servers. Also, consider that VM recovery processes (Instant Recovery, FLR and others) require sufficient resources (as described in [System Requirements](#)).

1.36.1 Estimating Repository Capacity

When estimating the amount of required disk space, you should know the following:

- Total size of VMs being backed up
- Frequency of backups
- Retention period for backups
- Will jobs use forward or reverse incremental

Also, when testing is not possible beforehand, you should make assumptions on compression and deduplication ratios, change rates, and other factors. The following figures are typical for most deployments; however, it is important to understand the specific environment to figure out possible exceptions:

- Data reduction thanks to Compression and Deduplication is usually 2:1 or more; it's common to see 3:1 or better, but you should always be conservative when estimating required space.
- Typical daily change rate is between 2 and 5% in a mid-size or enterprise environment; this can greatly vary among servers; some servers show much higher values. If possible, run monitoring tools like Veeam ONE to have a better understanding of the real change rate values.
- Include additional space for one-off full backups.
- Include additional space for backup chain transformation (forward forever incremental, reverse incremental) – at least the size of a full backup multiplied by 1.25x.

Note: When using deduplication appliances, please contact the vendor for sizing guidelines.

Using the numbers above, you can estimate required disk space for any job. Besides, always leave plenty of extra headroom for future growth, additional full backups, moving VMs, restoring VMs from tape.

A repository sizing tool that can be used for estimation is available at <http://vee.am/rps>. Note that this tool is not officially supported by Veeam, and it should be used “as is”, but it's nonetheless heavily used by Veeam Architects and regularly updated.

Tip: With Veeam Availability Suite, you can use Veeam ONE together with Veeam Backup & Replication. Among the many reports, Veeam ONE has the **VM Change Rate Estimation** report from the “Infrastructure Assessment” report pack; this can be used as an indicative pre-deployment assessment of the potential amount of space that should be available on the backup repositories. This report is built measuring the number of VM virtual disk write operations supplied by VMware vSphere while additional compression and deduplication (usually 2 to 3 times) ratio should be assumed.

It is also recommended to periodically run the “Capacity Planning for Backup Repositories” report from the “Veeam Backup & Replication Reports” pack to analyze the amount of free space on backup repositories and estimate the projected growth and consequent space consumption. The report provides recommendations for adjusting the allocated storage resources in order to meet the future demand for backup storage. Furthermore, it calculates the amount of additional space that needs to be provisioned to accommodate the necessary restore points.

For more information on Veeam Availability Suite, please refer to its Reviewer's Guide at <https://helpcenter.veeam.com/>

Examples

The examples below explain the impact of backup method and retention policy on the estimated repository size, assuming the environment is the same in all three cases.

Environment: 10 VMs, 100GB each, 80GB avg/used

2:1 Estimated Compression/Deduplication, 5% daily change

Example 1

Backup: Reverse Incremental, Daily Backup, 30 Day Retention

- Estimated Full Backup Size: $10 * 80\text{GB (Used space)} * 50\% \text{ (2:1 Compression)} = 400\text{GB}$
- Estimated Reverse Incremental Size: $10 * 80\text{GB} * 50\% \text{ (2:1 Comp)} * 5\% \text{ (Change Rate)} * 29 \text{ (reverse incremental restore points)} = 580\text{GB}$
- Spare : 500 GB
- Estimated total Backup Size: $400\text{GB} + 580\text{GB} + 500 = 1480 \text{ GB}$

Example 2

Backup: Forward Incremental, Daily Backup, 30 Day Retention, Weekly Full

- Estimated Full Backup Size: $10 * 80\text{GB (Used space)} * 50\% \text{ (2:1 Compression)} = 400\text{GB}$
- Estimated space for 6 Weekly Fulls (Max required for 30 Day Retention): $400\text{GB} * 6 = 2400\text{GB}$
- Estimated Forward Incremental Size Max: $10 * 80\text{GB} * 50\% * 5\% * 32 = 640\text{GB}$
- Estimated total Backup Size: $2400\text{GB} + 640\text{GB} = 3,040\text{GB} (\sim 3\text{TB})$

Example 3

Backup: Forward Incremental, Daily Backup, 30 Day Retention, Monthly Full

- Estimated Full Backup Size: $10 * 80\text{GB (Used space)} * 50\% \text{ (2:1 Compression)} = 400\text{GB}$
- Estimated space for 3 Monthly Fulls (Max req for 30 Day Retention): $400\text{GB} * 3 = 1200\text{GB}$
- Estimated Forward Incremental Size Max: $10 * 80\text{GB} * 50\% * 5\% * 60 = 1200\text{GB}$
- Estimated total Backup Size: $1200\text{GB} + 1200\text{GB} = 2,400\text{GB} (\sim 2.4\text{TB})$

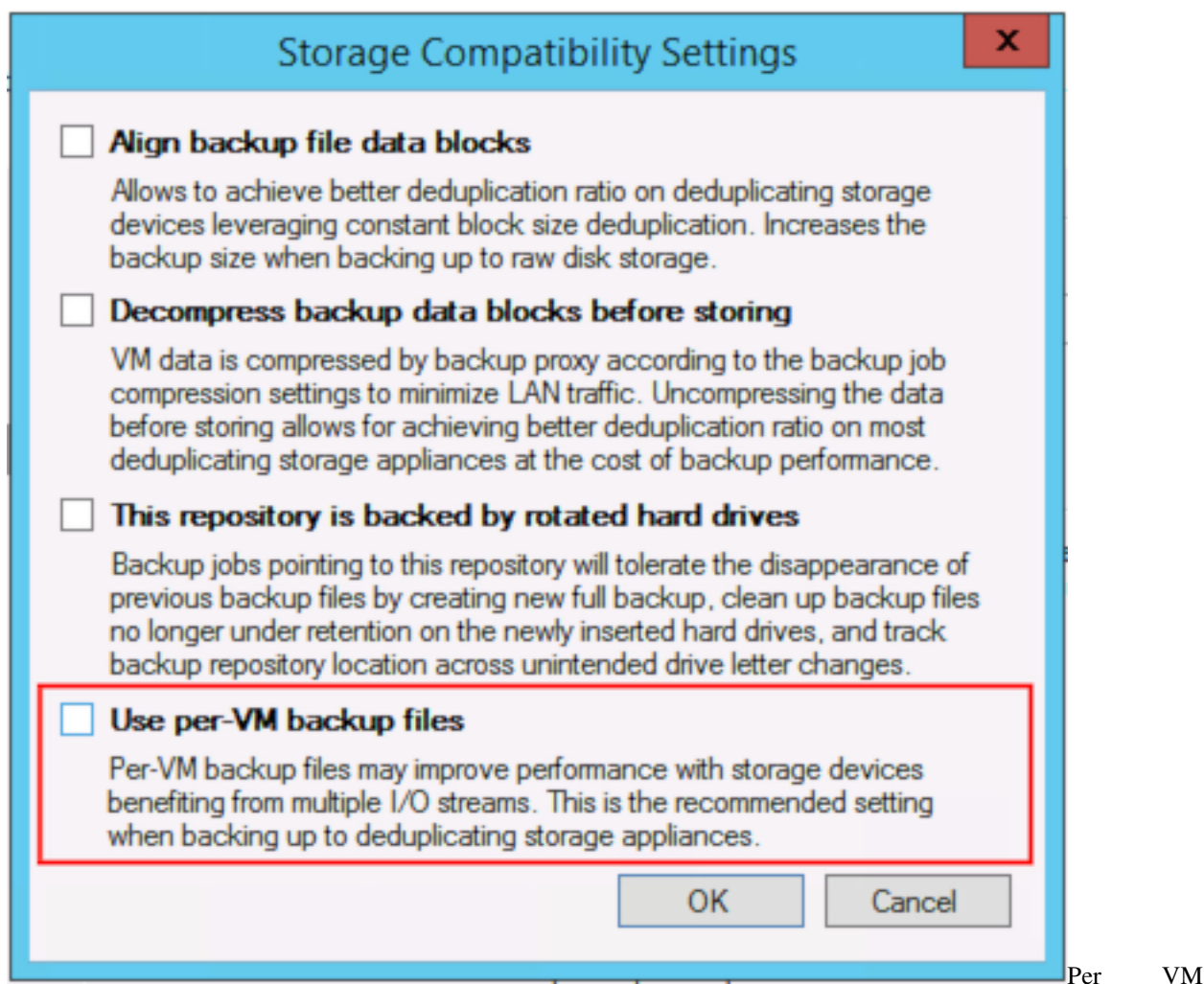
To summarize, when estimating the size of the repositories, use the following best practices:

- Be conservative when estimating compression and deduplication ratios if actual ratios and disk content are unknown.
- Use higher estimates for change rate if a significant number of servers are transactional such as Microsoft SQL and Microsoft Exchange.
- Include enough free space to take at least one and a quarter extra full backup for each transformation job.

1.37 Per VM backup files

It is possible to write one backup file chain per each VM on a repository, compared to the regular chain holding data for all the VMs of a given job. This option greatly eases job management, allowing to create jobs containing much more VMs than jobs with single chains, and also enhances performance thanks to more simultaneous write streams towards a repository, even when running a single job.

In addition to optimizing write performance with additional streams to multiple files, there are other positive side effects as well. When using the forward incremental forever backup mode, you may experience improved merge performance. When backup file compacting is enabled, per VM backup files require less free space: instead of requiring sufficient space to temporarily accommodate an additional entire full backup file, only free space equivalent to the largest backup file in the job is required. Parallel processing to tape will also have increased performance, as multiple files can be written to separate tape devices simultaneously.



backup files

Per VM backup files is an advanced option available for backup repositories, and it is disabled by default for new backup repositories. If enabled on an existing repository, an active full backup is required after the option has been enabled.

**** NOTE: In Scale-Out Backup Repositories, Per-VM backup files option is ENABLED by default ****

1.37.1 Maximum number of VMs per job

With per VM backup files the recommendation for number of VMs per job can be increased significantly. Even if technically jobs containing five thousands VMs have been successfully tested in a lab, feedback from the field shows a sweet spot at around 300 VMs per backup job, more for management reasons and unexpected side effects than pure performance matters.

When designing your jobs, keep in mind that several operations such as synthetic operations, health checks and Backup Copy Jobs will be pending until all VMs in the job have completed successfully. For those reasons, extremely large jobs may be impractical.

1.37.2 Performance

To avoid counter productive effects, attention should be paid on not having too many write threads towards a storage used as a repository. For example, a low range NAS storage will probably not react very well to a high amount of parallel processes created by per VM backup files. To limit this effects, refer to Repository configuration options, especially the **Concurrent tasks** limit.

1.37.3 Deduplication

Using Per VM backup file will negatively impact repository space usage since Veeam deduplication is file based. If backup jobs have been created while grouping similar guests to optimize deduplication and if Active Full is used, per VM Backup chain might require additional repository space.

1.38 Scale Out Backup Repository

Veeam Scale-out Backup Repository is a logical entity made of multiple “simple” repositories, grouped together into a single abstracted object, that can be used as a target for any backup and backup copy job operation.

Scale-out Backup Repository is an extremely easy way for both medium and large customers to extend repositories when they run out of space. Instead of facing the long and cumbersome relocation of backup chains, users will be able to add a new extent (that is any of the “simple” backup repositories supported by Veeam Backup & Replication) to the existing Scale-out Repository — or group multiple repositories to create a new one.

As of version 9.5 U4 one Capacity Tier extent can be added per SOBR. The Capacity Tier extent can only be backed by an object storage repository and is meant to extend the SOBR with a cheap long-term storage tier for older backup files. Backup files are moved to the Capacity Tier based on age when all other requirements are fulfilled.

The only requirement is the ownership of a proper license, and that at least two simple repositories have been added to Veeam Backup & Replication already. As per default settings, it is recommended to enable “per VM backup files” on the Scale-out Backup Repository for optimal balancing of disk usage.

NOTE: the default backup repository created during the installation cannot be used in a Scale-out Backup Repository as long as it's the target of Configuration Backup, as this type of job is not supported by Scale-out Backup Repository. If the default repository needs to be added to a Scale-out Backup Repository, consider first to change the target of Configuration Backup.

For additional technical information, the online documentation is available here : [Helpcenter SoBR](#).

1.38.1 File placement policies

Scale-out Backup Repository has two different options for file placement.

Data Locality

This is the default policy, and it works by placing all the dependent files of a backup chain into the same extent. Every extent grouped with this policy has the same chances of receiving a backup chain as the algorithm treats them equally, and the major parameter for the initial placement is the free space value.

The failure domain is a single extent, as the loss of a given extent impacts only the backup chains stored into that extent. Policy can be violated by Veeam itself if, for example, one of the extents has no free space left, and the additional incremental is stored in a different extent. This because the priority is always to complete a backup or backup copy.

Performance Performance policy places dependent incremental backup files on a different extent from the corresponding fulls. In order to choose which extent will hold the different files when using the performance policy, for each extent users are able to assign it a “role”.

Important: When using integrated deduplication devices, virtual synthetic operations may not work, if the full and incremental backup files are placed on separate extents. Please use Data Locality mode instead.

Users can configure each repository of the group to accept full backups, incremental backups or both. As soon as a new backup chain is stored into a performance Scale-out Backup Repository, the different files are placed in accordance to the policy itself.

Note: in order to leverage the performance policy correctly users need to use at least two different repositories. Even if it's possible to assign both roles to the same repository, this configuration makes little sense and the best results can be obtained by splitting full backup files and incremental backup files over different physical extents.

Performance policy increases the failure domain — a backup chain is split over at least two repositories, thus the loss of one of the two corrupts the entire backup chain. This is a consideration that Veeam architects need to evaluate carefully. There is a trade-off between the increased performance guaranteed by the performance placement policy, and the increased failure domain.

1.38.2 Scale-out Backup repository and network considerations

Scale-out Backup Repository is, as the name implies, a scale out architecture, based on multiple datamovers, with a notion of master and slave repository datamovers.

During backups, the master datamover is always started where the write is happening. During restore, the master is always started where the VBK is located, as most blocks are likely retrieved from this location.

A master datamover is the only repository datamover receiving data from a source datamover (a proxy in a backup job or a source repository in a backup copy job). A master datamover is able to communicate if needed with other slave datamovers to retrieve their data.

As in any scale-out solution, careful design should be applied to the network, as communications between the different data movers may increase network consumption, regardless the policy in use or the specific design of the scale-out architecture. When using Scale-out Backup Repository, 10 Gb networks are always recommended.

1.39 Capacity Tier

The Capacity Tier extends the SOBR virtually unlimited depending on the type of object storage which backs the Capacity Tier.

Only one Capacity Tier can be configured per SOBR. The Capacity Tier must be an [Object Storage Repository](#).

To understand more about the Capacity Tier and how offloading works, please refer to the Veeam Helpcenter article about [Capacity Tier](#).

1.39.1 General

The VBR 9.5 U4 implementation of Capacity Tier is a **move only** functionality. This means within a SOBR the backup files do only exist once, either on a Performance or on the Capacity Tier extent. Therefore the Cloud Tier offload functionality is not a replacement for a backup copy and is no proper way of fulfilling the 3-2-1 rule.

The retention of the objects in the Capacity Tier is controlled by the backup or backup copy job's retention policy in restore points and not on repository level. The operational restore window in the SOBR configuration does only define which retention files can be offloaded.

Offloading to object storage will only happen if the retention period and the operational restore window do overlap. E.g. if you configure 14 retention points with one backup per day and you want to offload to the Capacity Tier after 14 days, you will never offload anything. If you configure 21 retention points with the same operational restore window there should be roughly 7 retention points offloaded to object storage (based on other requirements, like sealed backup chains).

1.39.2 Block Size

The created data-block-objects in the object storage are based on the backup's configured block size (Storage optimizations). The default is `Local Target` and refers to an uncompressed block size of 1024 KB. Every block is offloaded as a single object in the object storage and thus requires one API call per read or write operation (GET/PUT).

For the same amount of data a larger block size would mean less objects and less API calls, on the other hand larger block sizes mean a higher probability of changes in the block which reduces the efficiency of intelligent block cloning.

Experience shows that the default `Local Target` setting with the uncompressed 1024 KB block size is the best general purpose setting and should be configured in most cases. In corner cases other block sizes might show lower cost, e.g. by reducing API calls.

1.40 WAN Acceleration

By combining multiple technologies such as network compression, multi-threading, dynamic TCP window size, variable block size deduplication and global caching, WAN acceleration provides sufficient capability when the network bandwidth is low or dramatically reduced when performing Backup Copy and Replication jobs. This technology is specifically designed to accelerate Veeam job. Any other WAN acceleration technology should be disabled for Veeam traffic.

To determine whether WAN acceleration is necessary in an environment, it is important to understand what particular savings can be achieved.

1.40.1 Determining Required Bandwidth

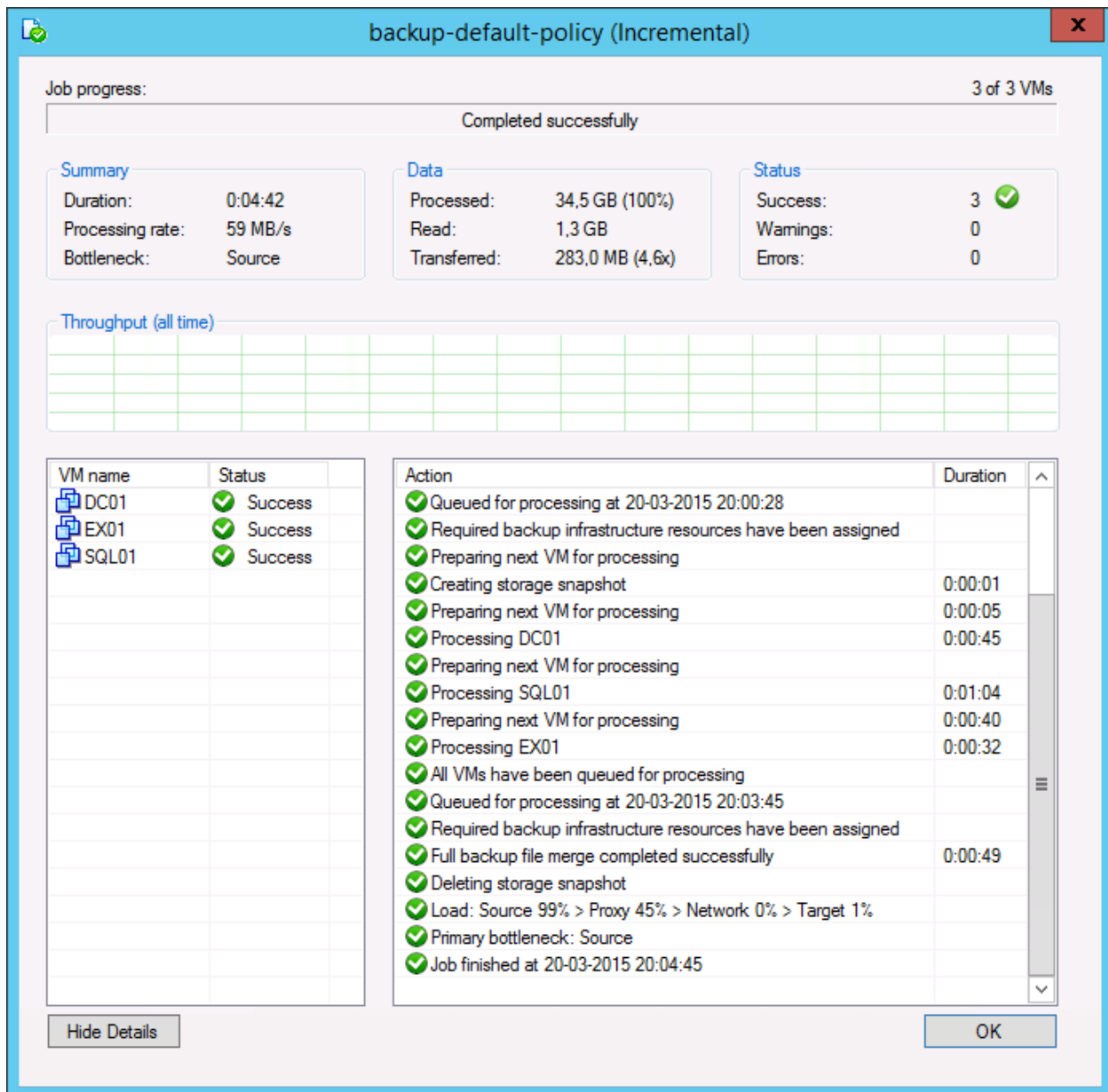
When using WAN acceleration on links with low bandwidth, you may have to manually seed the initial copy to the target. For more information, refer to the [WAN Acceleration](#) section of the Veeam Backup & Replication User Guide.

The WAN accelerator uses its own digests based on the hashes of the blocks inside a VM disk, which means that it reads data from the backup files and re-hydrating them on the fly, or it reads directly from the source VM in case of replication. The WAN accelerator component will then process those data blocks with much more efficient data deduplication and compression algorithms. This is the reason why the WAN accelerator consumes significant amounts of CPU and RAM resources.

To determine how much data has to be transferred over the WAN link with and without WAN acceleration enabled in a backup copy job, you can compare the daily changes of the primary backup job statistics (as the same data is transported in a standard backup copy job without WAN acceleration) with the WAN accelerated backup copy job log and statistics.

1.41 Analyzing Backup Job

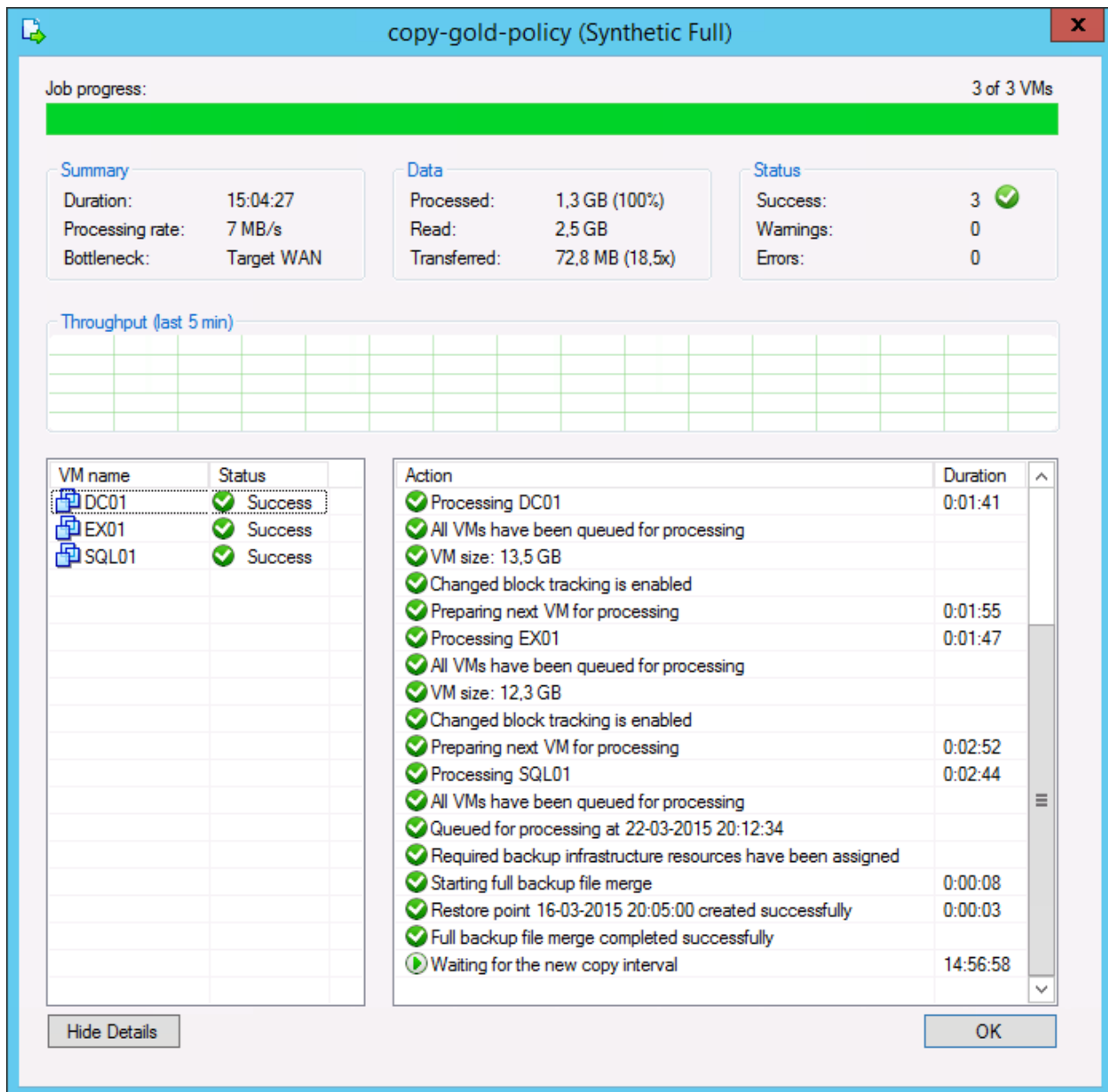
During both full and incremental job sessions, three metrics are displayed in the session data: **Processed**, **Read** and **Transferred**. To better understand the difference between direct data transfer and WAN accelerated mode, examine the **Read** and **Transferred** values:



- **Read** — amount of data read from the production storage prior to applying any compression and deduplication. This is the amount of data that will be optimized by the WAN accelerator.
- **Transferred** — amount of data written to the backup repository after applying compression and deduplication. This is the amount of data that will be processed by the backup copy job running in Direct Transfer mode (without WAN acceleration), assuming all VMs from the backup job are included in the backup copy job.

1.42 Analyzing Backup Copy Job

When analyzing a backup copy job you can see the same metrics in the job session Data: **Processed**, **Read** and **Transferred**. Comparing the backup copy job with WAN acceleration enabled and the backup job, it is possible to correlate the information in both outputs.



- The amount of **Processed** blocks in the backup copy job session is equal to the amount of **Read** blocks in the backup job session. This is the most important metric, as it is the amount of data that has to be processed by the WAN accelerator.
- The number of **Read** blocks for the **backup copy job** is typically higher than the amount of **Processed** - this is due to the backup copy job using a differing fingerprinting algorithm that works with a different block size compared to the fingerprinting algorithm and block size used by **backup jobs** that created the original backup file. For this reason, this metric can be ignored.
- The amount of **Transferred** data is the amount of data actually transferred over the WAN link.

1.43 Comparing Direct Mode with WAN Accelerated Mode

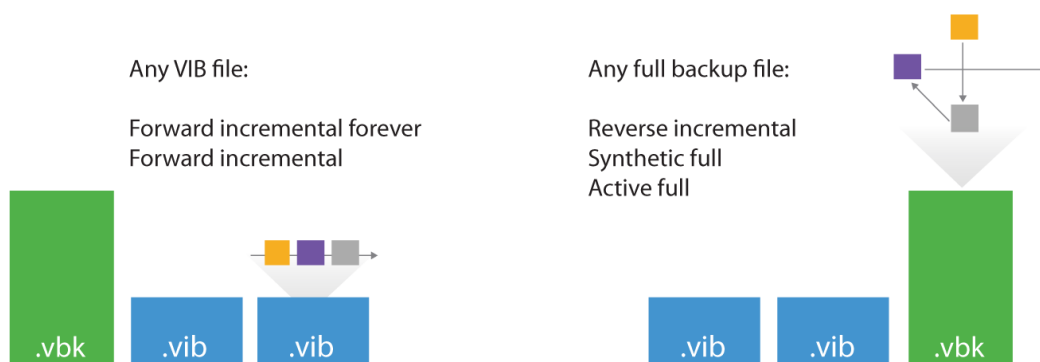
Consider that the savings rate (18.5x) displayed in the GUI is based on **Processed** data (“re-hydrated” data blocks). In the example above, 283 MB would have been transferred over the WAN link in Direct Transfer mode, while only 72.8 MB were transferred after enabling WAN acceleration. The actual savings rate equals 3.9x in this relatively static demo infrastructure, whilst it would typically be significantly higher in real-life scenarios.

Note: Approximate savings ratio can be assumed as of 10x.

To calculate possible savings and needed bandwidth you may use the following calculator [Bandwidth Calculator](#).

1.44 Backup Mode Effect

When planning for WAN acceleration, review the backup mode used on the primary backup job. Some backup methods produce a random I/O workload on the source repository (as opposed to sequential I/O patterns in other backup modes). The methods of reading from source is illustrated by the figure below:



For example, forward incremental and forever forward incremental methods will make backup copy jobs work much faster, as read operations will be sequential rather than random. To avoid similar fragmentation and random I/O on forward incremental modes, keep [backup storage maintenance](#) enabled when possible.

Though a workload penalty may not be significant, it can be a good idea to monitor the storage latency on the backup repository, especially if the reported bottleneck is *Source*. If the storage latency on the backup repository is high, it is recommended that you change the backup mode in order to increase the throughput of one pair of WAN accelerators.

1.45 Configuration

Thanks to our friends at PernixData for helping with I/O analysis using [PernixData Architect](#).

When configuring the WAN accelerator, not all configuration parameters affect both source and target WAN accelerators. In this section we will highlight what settings should be considered on each side.

1.45.1 Source WAN Accelerator

At the first step of the WAN accelerator configuration wizard, you can change the default setting of five TCP threads. This setting applies to the source WAN accelerator only and is automatically configured to mirror the number on the target WAN accelerator at the beginning of each job. This ensures different source WAN accelerators can have different settings when using the same target WAN accelerator at different times. The maximum setting is 100 simultaneous threads for throughput optimization and compensation for high latency or packet loss.

Edit WAN Accelerator

Server

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

Server

Choose server: veeam-hv01.democenter.int Add New...

Description:

WAN accelerator backed by SSD cache

Traffic port : 6165
TCP/IP port to use for data transfer. Ensure this port is open in any firewall between sites.

Streams: 5
Using multiple upload streams helps to fully saturate WAN links.

< Previous Next > Finish Cancel

If the link has low latency and high bandwidth, the default setting (5 streams) may be enough to fully saturate it. If the link is still not saturated, the number of streams may be increased accordingly.

Testing shows that with high latency links, **link speed x 1.5** is a good best practice for estimating the number of streams required. Below is an example benchmark on a 10 Mbit/s WAN link with 100 milliseconds of latency.

Link (Mbit/s)	Latency (ms)	Packet loss (%)	Streams	Throughput (Mbps)
10	100	0	3	3.5
10	100	0	10	7.5
10	100	0	15	10
10	100	0	20	10

Increasing the number of streams to more than required for fully saturating the link will cause initialization of data transfers to slow down, as the data transfer will wait for all streams to initialize and stabilize before beginning transferring any data.

Tip: To test different scenarios in the lab before deploying WAN acceleration, you can use a WAN emulator (such as WANem).

Edit WAN Accelerator

Cache

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

Server

Cache

Review

Apply

Summary

Folder:

W:\VeeamWAN Browse...

Path	Capacity	Free
C:\	59.7 GB	13.8 GB
S:\	5.0 TB	4.5 TB
T:\	5.0 TB	4.5 TB
U:\	5.0 TB	4.4 TB
V:\	5.0 TB	4.4 TB
W:\	100.0 GB	88.9 GB

Cache size: 5 GB

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

< Previous Next > Finish Cancel

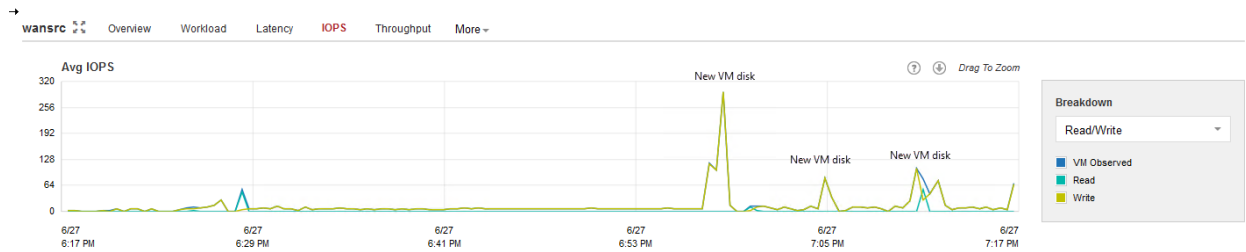
When configuring the cache location for the source WAN accelerator, consider that the actual cache size on the source is irrelevant, as it is used only for digest files (where block hashes are stored). However, if a WAN accelerator will be used for bi-directional acceleration (act as both source and target), follow the guidelines provided in the “*Target WAN Accelerator*” section below.

1.46 Sizing For Wan Acceleration

When configuring the WAN accelerator on the source side, consider that all VM disk data blocks are already in the source backup repository and they can simply be re-read from the source repository when needed. This is the reason why configuring the cache size on a source WAN accelerator is not as important but still must exist as a number. It is never used for caching any data. However, there are other files residing in the source WAN accelerator folder, and the file structure will be described in the following sections.

1.46.1 Hardware

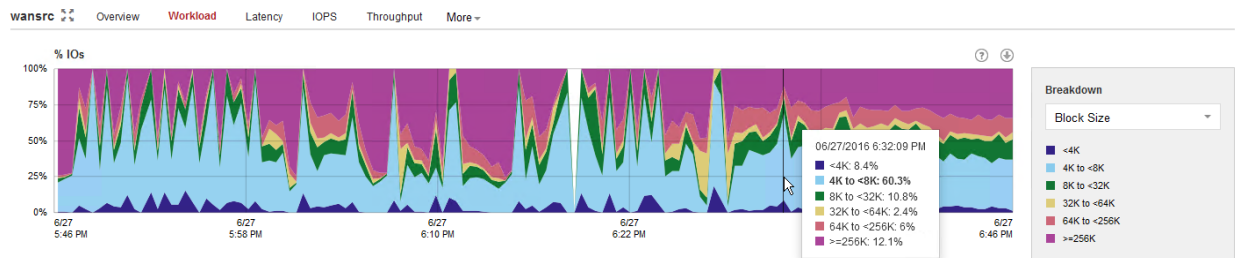
The source WAN accelerator will consume a high amount of CPU and memory whilst re-applying the WAN optimized compression algorithm. Recommended system configuration is 4 CPU cores and 8 GB RAM. When using an existing Veeam Managed Server for Wan Acceleration which already has a role such as Veeam Backup & Replication Server, Proxy or windows Repository ensure you have not overcommitted the CPUs on that host and there is resource for each source and Target Wan Accelerator. If there is not enough CPU cores free the job will wait for a free cpu to continue.



Source

WAN accelerator IOPS

The I/O requirements for the source WAN accelerator spikes every time a new VM disk starts processing. Thus, it is recommended to deploy WAN accelerators on disk configurations with decent I/O performance.



Source

WAN accelerator IO size

The typical I/O pattern is made of many small blocks, so using high latency spinning disks is not recommended.

1.46.2 Disk Size

Each digest file consumes up to 2% of its source VM disk size. This means, for example, that a 2 TB VM disk file can produce a digests file up to 40 GB in size.

Additionally, plan for 10 GB of working space for payloads and other temporary files.

- Formula: $(\text{Source data size in GB} * 2\%) + 10 \text{ GB}$
- Example with 2 TB source data: $(2,000 \text{ GB} * 2\%) + 10 \text{ GB} = 50 \text{ GB}$

For understanding how disk space is consumed, please see the following sections.

Note: As the cache size on the source WAN accelerator will always be ignored, the digests file will be produced regardless of cache setting been configured. They may consume considerable disk space.

1.46.3 VeeamWAN\GlobalCache\src

Only a `data.veeamdrf` file is located in the `\VeeamWAN\GlobalCache\src` folder. This file will be synchronized from the target WAN accelerator during the very first job run (or if the cache was manually cleared) to understand what data blocks are already cached in the target WAN accelerator. The size of this file is typically up to 2% of the configured target cache size; thus, it may take some time for the initial data transfer to begin.

1.46.4 VeeamWAN\Digests

On the source WAN accelerator there are the VM disk digests that take up disk space. For each processed VM disk, a disk digest file is created and placed in `\VeeamWAN\Digests\<JobId>_<VMId>_<DiskId>_<RestorePointID>`.

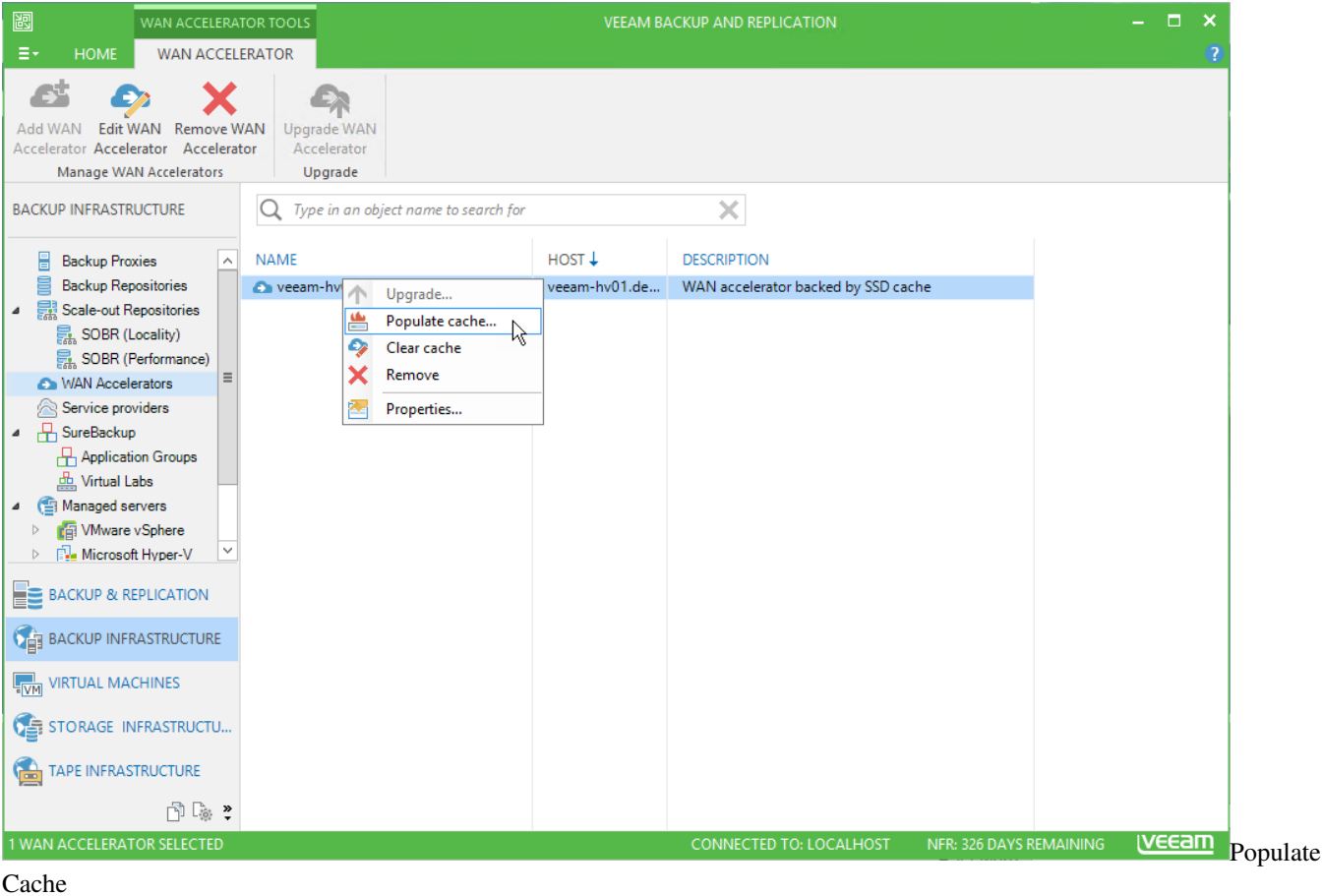
Note: Although the Digest folder is created on the target accelerator no data is stored on the target normally, however it must be sized into the target in case the digest on the source becomes corrupt or is missing. In this case the target will calculate its own digests in this location until the source WAN Accelerator comes back online.

Traffic throttling rules should be created in both directions. See [Network Traffic Throttling and Multithreaded Data Transfer](#) for more information.

1.46.5 Target WAN Accelerator

The following recommendations apply to configuring a target WAN accelerator:

- The cache size setting configured on the target WAN accelerator will be applied to the pair of WAN accelerators. This should be taken into account when sizing for many-to-one scenarios, as configuring 100 GB cache size will result in 100 GB multiplied by the number of pairs^[^1] configured for each target WAN accelerator.
- It is recommended to configure the cache size at 10 GB for each operating system^[^2] processed by the WAN accelerator.
- Once the target WAN accelerator is deployed, it is recommended to use the cache population feature (see [this section](#) of the User Guide for details). When using this feature, the WAN accelerator service will scan through selected repositories for protected operating system types.
- It is also possible to seed the initial copy of data to the target repository to further reduce the amount of data that needs to be transferred during the first run.



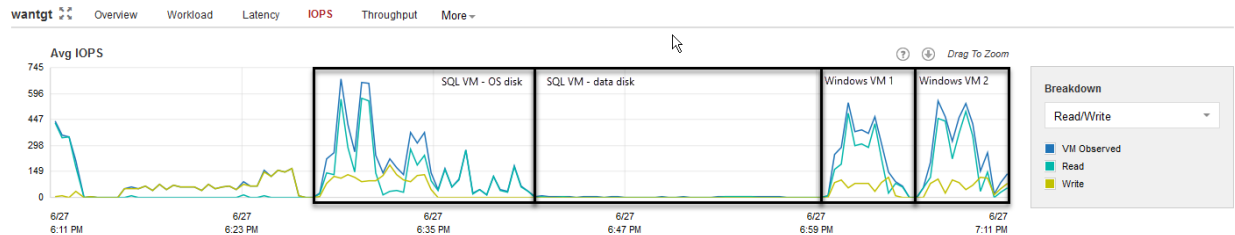
Cache

Sizing

Hardware

Although a target WAN accelerator will consume less CPU resources than the source, the I/O requirements for the target side are higher.

For each processed data block, the WAN accelerator will update the cache file (if required), or it may retrieve the data block from the target repository (if possible). As described in the user guide, the cache is active on operating system data blocks, while other data blocks are being processed only with the WAN optimized data reduction algorithm (in-line compression).



Target

WAN accelerator IOPS

Tests show that there are no significant performance differences in using spinning disk drives as storage for the target WAN accelerator cache rather than flash storage. However, when multiple source WAN accelerators are connected to a single target WAN accelerator (many-to-one deployment), it is recommended to use SSD or equivalent storage for the target cache, as the I/O is now the sum of all the difference sources.

Disk Size

Ensure that sufficient space has been allocated for global cache on the target WAN accelerator.

At least 10 GB per each different OS that is backed up. That is, if you plan to backup VMs running Windows 8, Windows 2008 R2, Windows 2012 and RHEL 6 (four different operating systems), you will need at least $10 \text{ GB} \times 4 = 40 \text{ GB}$

Plan for additional **20 GB** of working space for cache population, payload and other temporary files.

If the cache is pre-populated, an additional temporary cache is created. The temporary cache will be converted into being the cache used for the first connected source. Subsequently connected sources will duplicate the cache of the first pair. As caches are duplicated the configured cache size is considered **per pair** of WAN accelerators.

Formulas:

- Formula for configured cache size (insert this number in configuration wizard):
 - $(\text{Number of operating systems} \times 10 \text{ GB}) + 20 \text{ GB}$
- Formula for used disk space:
 - $(\text{Number of sources} \times \text{<formula for configured cache size>})$

Examples:

- Example with one source and two operating systems:
 - Configured cache size: $(2 \text{ operating systems} \times 10 \text{ GB}) + 20 \text{ GB} = 40 \text{ GB}$
 - Used disk space: $(1 \text{ source} \times 40 \text{ GB}) = 40 \text{ GB}$
- Example with five sources and four operating systems:

- Configured cache size: $(4 \text{ operating systems} * 10 \text{ GB}) + 20 \text{ GB} = 60 \text{ GB}$
- Used disk space: $(5 \text{ sources} * 60 \text{ GB}) = 300 \text{ GB}$

Digest space must be built into the equation using the same size for each source target:

- Example with one source two operating systems
 - one source digest space 20GB equates to target digest requiring 20GB
 - so 20GB + Cache disk space '(2 operating systems * 10 GB) 20GB' is 40GB
- Example with 5 source
 - Five source with digest space 20GB each equates to target digest requiring $20\text{GB} * 5$, 100GB
 - so 100GB + Cache disk space '(2 operating systems * 10 GB * five sources) 100GB' is 200GB

For understanding how the disk space is consumed, please see the following sections.

VeeamWAN\GlobalCache\trg

For each pair there will be a subfolder in the `trg` directory, with a UUID describing which source WAN accelerator the cache is attached to. In each of those subfolders, the `blob.bin` file containing the cache will be located. That file size corresponds to the setting configured in the management console.

Note: The `blob.bin` file will exist for all connected source WAN accelerators.

VeeamWAN\GlobalCache\temp

When connecting a new source WAN accelerator, the `temp` folder will temporarily contain the `data.veeamdrf` file that is later transferred to the source containing the cache manifest.

1.47 Sizing Targets for One to One and One to Many relationships

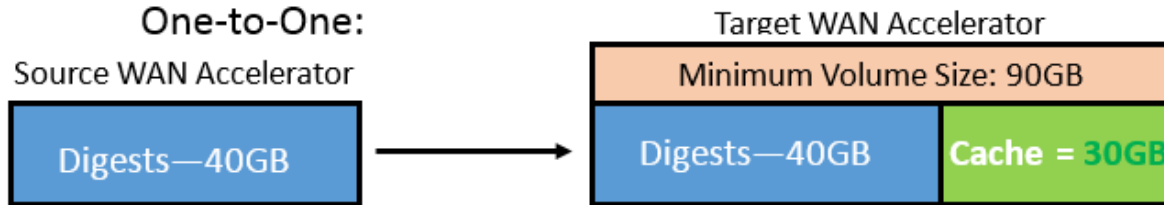
WAN Accelerator Cache/Digest Provisioning

we can have two types of relationship with our Source and Target accelerators, One to One and many to One.

One to one is the most simplest form, this is where one Source Accelerator is mapped to a single Target Accelerator at the other location.

The other type is **Many to One** where many source accelerators will map to a single target accelerator in a **fan in** type design. this is a common configuration and best practice is to have no more than 4 source accelerators to a single target for resource reasons.

1.47.1 Sizing for each scenario:

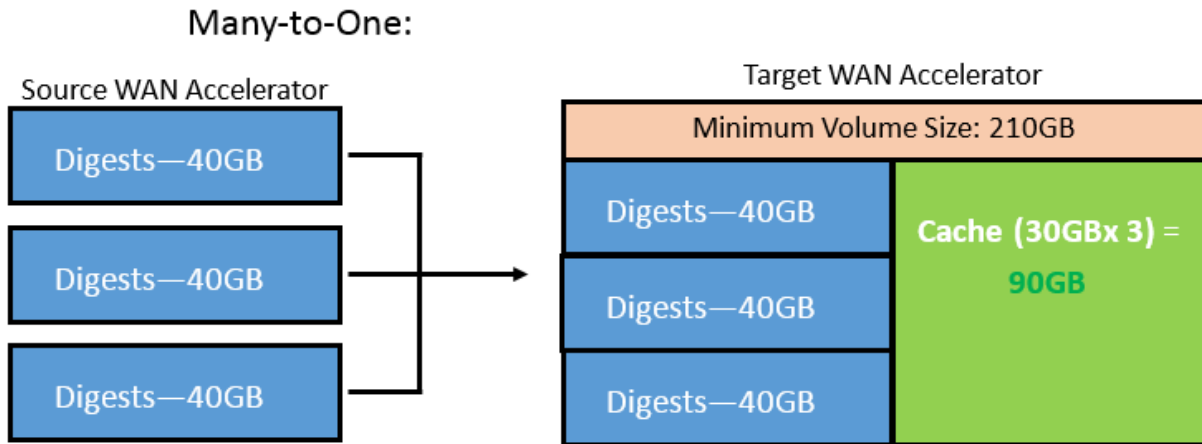


with One to One relationship

If we assume that we have 3 VMs, each with unique OSes (for instance, Win 2008R2, Win 2012R2, Solaris 10) each OS requires 10GB to be allocated for it.

The Cache itself is wholly independent from the digests required. That is, the Veeam GUI does not make any determination of how much you can allocate for a digest and so on.

The digest is essentially an index of what cached blocks go where. For digest size, 1TB of VM disk capacity we are backing up should correspond with 20GB of disk space. That is, for 10VMs we are backing up whose capacity is 2TB, you must account/allocate 40GB for digest data on the Source WAN Accelerator. This limitation is not applied to the Target WAN Accelerator.



with One to One relationship

For a Many-to-1 setup, the global cache is calculated per 1 Source WAN Accelerator working with the Target WAN Accelerator.

In this case the global cache needs to be increased proportionally.

If we use the same VMs in the previous example, the cache is only required to be 30GB. However, since we're using 3 Source WAN Accelerators, the cache size must be 90GB in response.

On the Target WAN Accelerator, cache size is dictated by the amount of Source WAN Accelerators plus number of operating systems in use, the digests space on the target end in this example cannot be excluded from the calculation even though it may never be used. We may require 120GB of Digest space at source so this needs to be added to the cache size (90GB) at target resulting in a requirement of 210GB of capacity at a minimum on the target.

When creating a WAN Accelerator in the user interface it relates to cache sizing only, digest sizing should be part of the overall design and included as part of the specification of the WAN Acceleration host.

Note: The target accelerator will use the digest capacity in the event the source digest becomes unavailable, is rebuilt or becomes corrupt. The target will use the spare capacity to calculate the digests on the target.

1.48 How Many WAN Accelerators to Deploy?

As the source WAN accelerator can only process one task at a time (one VM disk in a backup copy job or replication job), you may need to deploy multiple WAN accelerator pairs to meet the performance demands.

As the target WAN accelerator can handle multiple incoming streams (as described in the [Many-to-One WAN Acceleration](#) section of the User Guide), it is recommended to maintain a 4:1 ratio between the number of source WAN accelerators per target WAN accelerator.

This guideline is very much dependent on the WAN link speed. Many source sites with low bandwidth will create little pressure on the target WAN accelerator. So, for instance, in multiple ROBO configurations a 10:1 ratio can be considered.

If there are sites with very high bandwidth (such as datacenter-to-datacenter replication), they will produce a much more significant load on both the target WAN accelerator and the target repository due to the second data block lookup (for more information, refer to the [User Guide](#)).

Note: The secondary data block lookup is used, when a data block is not available in the WAN accelerator cache. When there is a WAN cache “miss”, the secondary lookup for the same data block is performed on the target repository. If it is found here, it is read back to the WAN accelerator instead of re-transmitting over WAN.

Assuming the source and target repositories can deliver the throughput required for the optimal processing rate, use the guidelines that follow.

Note: The numbers below are processing rates. The WAN link usage is dependent on the achieved data reduction ratio.

- Average throughput per target WAN accelerator: 500 Mbit/s (62.5 MB/s)
- Depending on the achieved data reduction rate (typically 10x), the transfer rate over the WAN link will vary.
 - If the processing rate is 62.5 MB/s, and the data reduction rate is 10x, then it is possible to sustain 6.25 MB/s (50 Mbit/s) over the WAN link.
 - If the WAN link has high bandwidth (above 100Mbps) consider using backup copy jobs without WAN Acceleration. However, if you use WAN accelerators in that scenario, it may require deployment of multiple WAN accelerator to fully saturate the WAN link.

[^1]: A pair of WAN accelerators means any source WAN accelerator paired with the target WAN accelerator. [^2]: All Linux operating systems are considered as one in terms of WAN accelerator sizing.

1.49 Is Wan Acceleration right for your environment?

Wan Acceleration is designed to optimize high latency or low bandwidth links between locations. there is a natural overhead and resource requirement when this is in operation and there will come a break point in regard to does Wan Acceleration work for me.

There are a number of ways to determine this based around speed and your available resources.

Wan Acceleration can be one to one or one to many connections, the first thing you should consider is the bandwidth available between the locations to see if the cost of optimizing your traffic is outweighed by the speed of your link.

The following is a general rule to look at when designing your transport:

1.49.1 Global Cache on Spinning Disk

- **Link less than 3Mb/s** - WAN likely saturated; processing rate dependent on data reduction ratio (estimated 10x)

- **Link more than 3Mb/s and less than 50Mb/s** - WAN will not be fully utilized, expect ~5MB/s processing rate but less bandwidth.
- **Link more than 50Mb/s** - WAN will not be fully utilized, using direct mode copy will use more bandwidth but likely be faster**

These numbers are to be considered as a base line , “Your mileage may vary”. The performance of the underlying storage where the Global Dedupe Cache is located can greatly impact the performance of the WAN Accelerator function. Tests show that there are no significant performance differences in using spinning disk drives as storage for the target WAN accelerator cache rather than flash storage. However, when multiple source WAN accelerators are connected to a single target WAN accelerator (many-to-one deployment), it is recommended to use SSD or equivalent storage for the target cache, as the I/O is now the sum of all the difference sources.

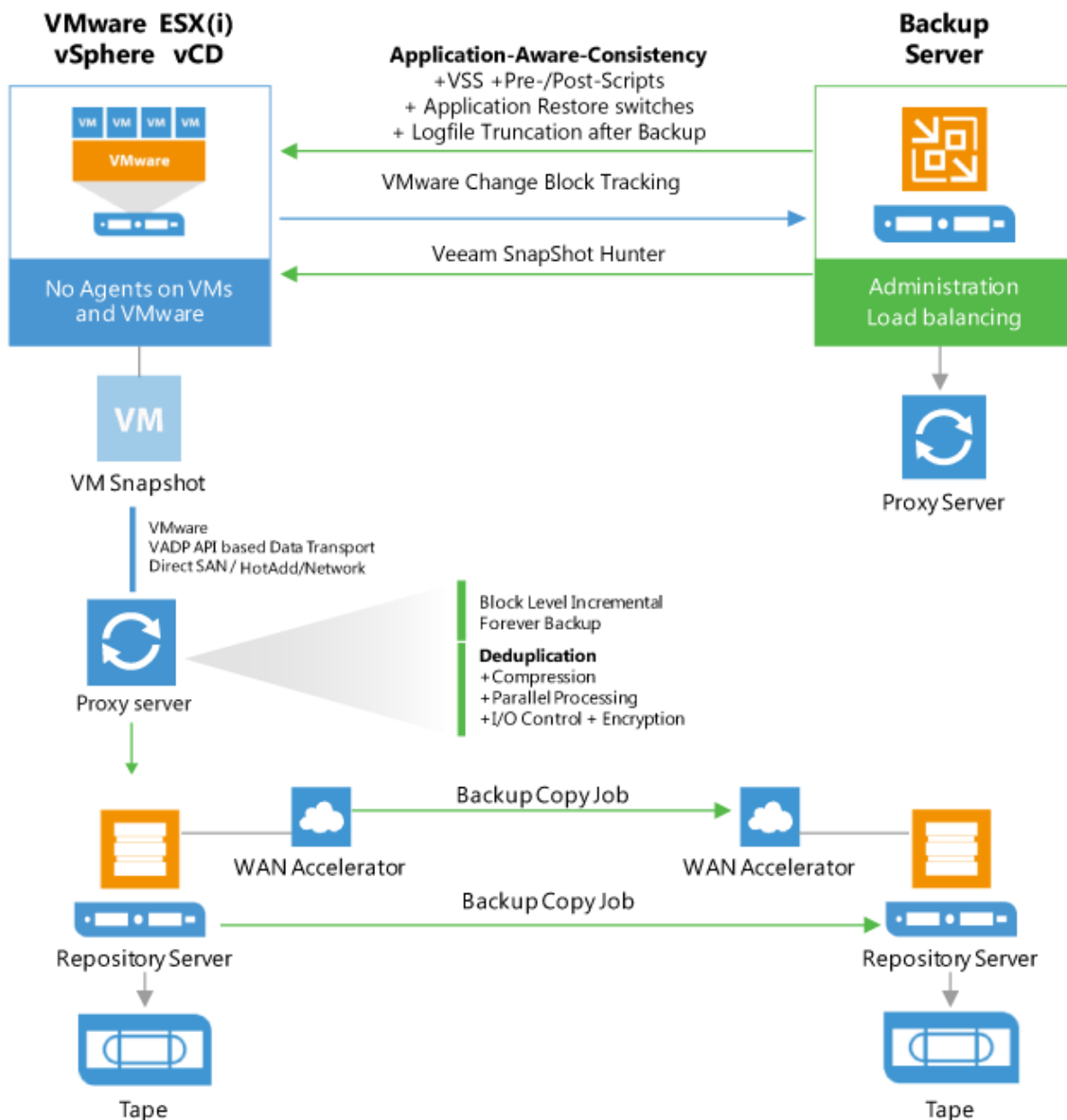
One more point to focus on is the repository used at the target-wan-accelerator, data may be taken from the repository at the target WAN accelerator if the data is not found in the global cache but is known to exist in a previous transfer. If slow disks are used it can have an impact on the speed of the completion of the job and overall processing rate.

Other factors are also present such as is this link going to have bi-directional data flow when using the Wan Accelerators, how many jobs will be using the link at the same time. Measure your overall saturation of the link prior to using Wan Acceleration to ensure that it meets your needs.

1.50 Tape Support

1.50.1 Overview

The diagram below illustrates the main components and processes within the backup infrastructure when tape support is implemented in Veeam Backup & Replication:



1.50.2 Tape Device Connection

The following configuration prerequisites must be met:

- All connection types require driver installation
- You can use generic drivers from Microsoft Windows, but they may not provide as high performance as the vendor's
- Separate drivers for tape drives and for tape media libraries should be installed

- StorageTek ACSLS is not supported while a direct connection to the library is needed
- Dynamic Drive Sharing is not supported
- Library Partitioning is supported
- Multiple control paths are supported only when control path failover and MPIO is configured correctly. Please contact the vendor for more information.

Connection Type Compatibility

- FC/SAS/SCSI/FCoE/Infiniband/iSCSI or other block technology to physical Tape Proxy are supported with Windows driver as long as the tape vendor supports the connection. (“Unknown media changer” support for FC/SAS and VTLs)
- FC/SAS redirect to VMware VM is unsupported
- FC/SAS redirect to Hyper-V VM is unsupported
- FC/SAS to iSCSI Converter/Bridge is supported
- Starwind Tape Redirector is supported

Tape device support

The Veeam Ready database provides a list of all partner solutions that have successfully passed Veeam’s testing criteria. Solutions are grouped by company name, Veeam Ready classification, and more. [Veeam Ready Database](#)

Supported

- LTO-3 or higher
- For VTLs, see the corresponding section under Deduplication Storage

Not supported

- IBM “Jaguar” TS11x0 Enterprise tape drives
- StorageTek T10000 tape drives
- Older Tape drives like DLT or AIT

Drivers

- IBM drivers: use “non-exclusive” driver setup and start installation with administrative rights.
- HP drivers: these are not installable with the downloaded install .exe file on a VM (for example, to use with VTL). As a solution, run the install .exe and choose Extract. Use Device Manager → Update driver and select the drivers for tape drives and (if you use HP/HP emulation tape library) for media changer.

Unknown Medium Changers

Veeam supports medium changers that have no Microsoft Windows drivers available. Make sure that such device is recognized as an unknown medium changer in the Microsoft Device Manager list.

It is recommended that you use tape devices with original equipment manufacturer (OEM) drivers. Limitations VMware does not support tape drives connected directly to ESX(i) 4.x and later. For more information, see VMware vSphere Release Notes.

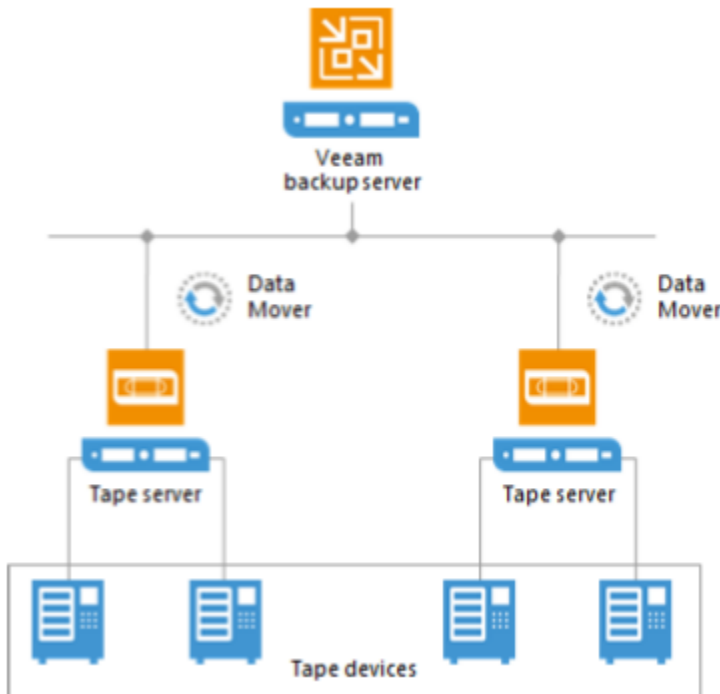
For more details and recommendations on configuring vendor-supported tape drives and media changers on ESX/ESXi, refer to VMware documentation at <https://kb.vmware.com/s/article/1016407>.

Note: Veeam Backup & Replication uses the MTF (Microsoft Tape Format) industry format to write data to tape. Veeam Backup & Replication does not support using WORM (Write Once Read Many) tapes.

1.51 Tape Devices Deployment

To connect tape devices to Veeam Backup & Replication, you need to deploy a tape server. The Tape Server is a Veeam Role that directly connects to tape libraries and to the Veeam backup server and manages traffic between tape devices and the Veeam backup server. The connected tape devices are recognized by the Veeam Backup & Replication automatically.

The Data Movers run on tape servers and other components of backup infrastructure. They receive tasks from the Veeam backup server and communicate to each other to transfer the data. The Data Movers are light-weight services that take a few seconds to deploy. Deployment is fully automated: when you assign a tape server role to a server, Veeam Backup & Replication installs the necessary components on this server and starts the required services.



1.51.1 Data Block Size

Tape Drives use hardware dependent block sizes to read/write tape data. Generally, the drives support a range of block sizes and report this range to Veeam Backup & Replication. If you use a tape library with multiple drives or a number

of standalone drives, Veeam Backup & Replication uses a unified block size to write data to tapes. Veeam Backup & Replication collects the block size ranges reported by each drive, compares them and detects a range of block sizes that can be supported by all drives. This range is additionally limited by storage controllers settings used in your infrastructure. From this range, Veeam Backup & Replication supports only values divisible by 1024. You can check the resulting range of block sizes supported by Veeam Backup & Replication for a particular drive in the Drives properties. For details, see Working with Drives.

Note: If you connect the tape devices via HBA, Veeam Backup & Replication uses the block size configured for the HBA.

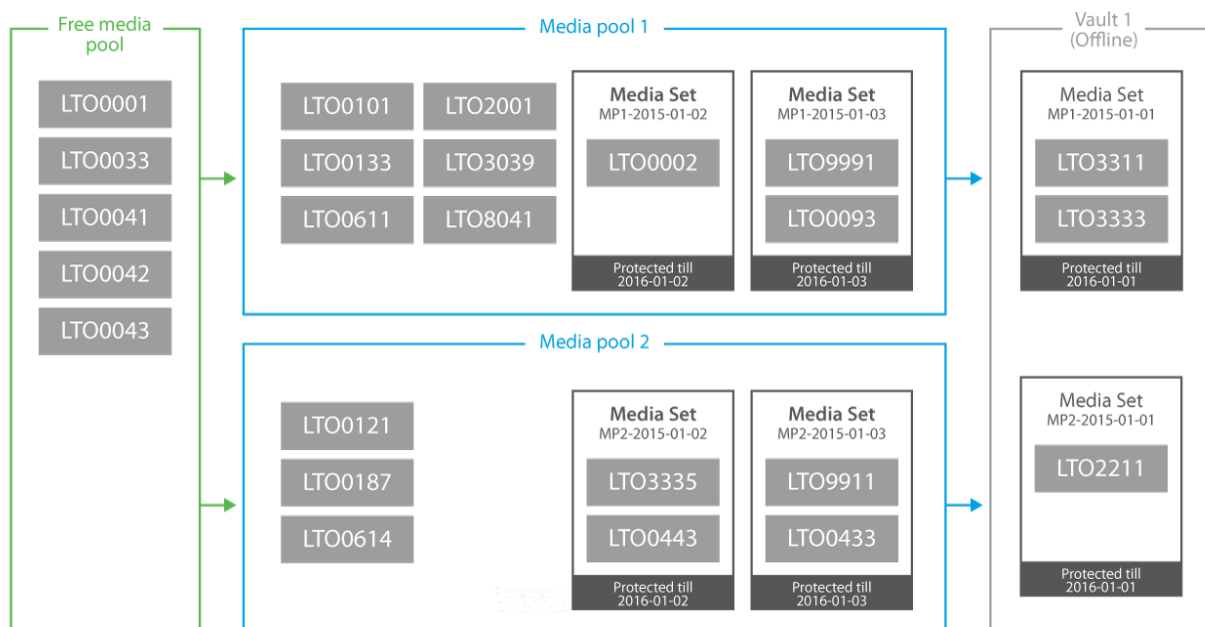
The block size is unified for: All drives in one library (if the drives support different block sizes)

- All standalone drives connected to one tape server.
- Mind the block size range when working with the following tapes:
 - Tapes with Veeam backups written by another tape library,
 - Tapes with Veeam backups written on another tape server,
 - Tapes written with other data transfer configuration settings,
 - Tapes written on a 3rd party device.

The tapes must be written with block size that match the value, currently used for the tape device you are using for restore.

If you have a number of Veeam backup servers, you can easily reconnect a tape server to another Veeam backup server without reconfiguring the tape device: Veeam backup server will recognize the library settings automatically. Note that when you reconnect the tape server, the tape jobs will not run with another Veeam backup server unless you copy the configuration.

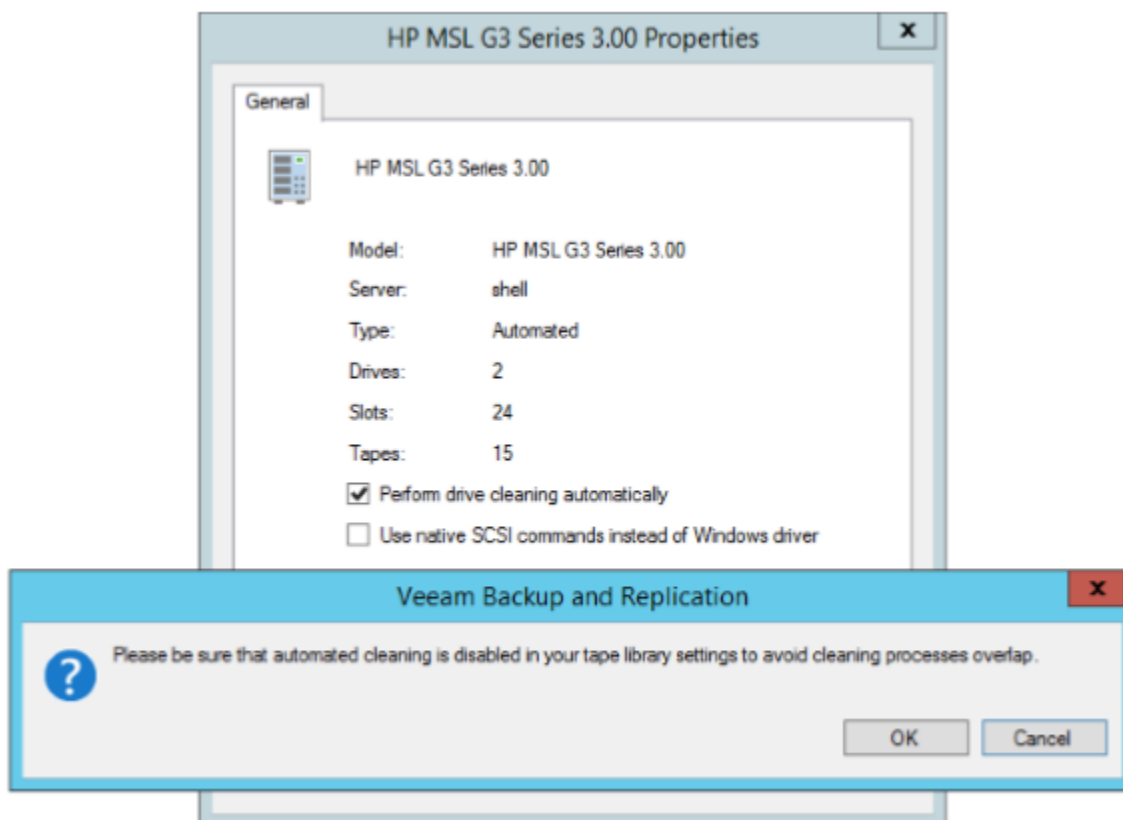
1.52 Media Management



1.52.1 Automated Drive Cleaning

You can instruct Veeam Backup & Replication to automatically clean the tape library drives. Assigning the automated cleaning to Veeam Backup & Replication prevents possible overlapping of cleaning tasks and tape jobs. Such overlapping may cause tape jobs failures. To instruct Veeam Backup & Replication to automatically clean the drives:

1. Open the Tape Infrastructure view.
2. Expand the Libraries node and select the needed library. Click Properties on the ribbon. You can also right-click the necessary library in the working area and select Properties.
3. In the Properties window, select the Perform drive cleaning automatically option.



If you enable the automated drive cleaning option in Veeam Backup & Replication, make sure that you disabled the drive cleaning tasks on your tape library device.

Veeam Backup & Replication cleans the drives at the beginning of backup to tape jobs or file to tape job run. The cleaning is not performed during other tape operations such as, for example, cataloging or export. To clean the drives automatically, Veeam Backup & Replication performs the following actions:

1. The tape library alerts Veeam Backup & Replication on a drive that requires cleaning.
2. Veeam Backup & Replication waits for a tape job to start.
3. When the tape job locks necessary drives for writing data, Veeam Backup & Replication checks which of them requires cleaning.
4. Veeam Backup & Replication ejects the tape from the drive, inserts a cleaning tape and performs the cleaning.
5. Veeam Backup & Replication ejects the cleaning tape and inserts the tape that was reserved for the tape job.
6. The tape job writes the data on tape.

The cleaning process usually takes several minutes.

The cleaning tapes are located in the Unrecognized media pool. The worn-out cleaning tapes are moved to the Retired media pool automatically.

If a tape job locks multiple drives simultaneously for parallel processing, and one or more drives require cleaning, all drives wait until the cleaning is finished. After cleaning, all drives start writing simultaneously.

The automated drive cleaning does not affect creation of media sets.

Limitations for Automated Drive Cleaning: You cannot enable the automated drive cleaning on standalone tape drives. You cannot start the drive cleaning manually with Veeam Backup & Replication. The drive cleaning is fully automated.

1.52.2 Working with Tape Libraries

All tape libraries managed by Veeam Backup & Replication are shown as a list of devices under the Libraries node in the Tape Infrastructure view. All connected devices are discovered automatically during the rescan procedure. When you add a new tape device to the tape server, it appears in your console after rescan. To view properties of a tape library:

1. Open the Tape Infrastructure view
2. Expand the Libraries node and select the needed library.
3. Click Properties on the ribbon. (You can also right-click the necessary library in the working area and select Properties).
4. Select the Perform drive cleaning automatically check box if you want Veeam Backup & Replication to manage the tape drives cleaning.

For more information about automated drives cleaning, see Automated Drive Cleaning. Select the Use native SCSI commands instead of Windows driver check box if your library is an unknown media changer.

1.52.3 Media Information

Veeam Backup Database Veeam Backup & Replication catalogues information of all archived data and stores this information in the Veeam backup database. The registered tapes stay in the database until you remove the information about them. You can always view details for each tape, for example, information about backups written to it, even if the tape is not inserted in the library. The catalogue lets quickly detect location of the required items on tape. The catalogue correlates the archived files and the restore points to the names of the corresponding tapes. Both online or offline, and the names of the media sets within were the data was written.

When you start restore, Veeam Backup & Replication prompts for the tapes you need to bring online. As a result, you can restore data from tape much quicker. Veeam Backup & Replication uses the following catalogues for storing the tape-related data:

- Tape Catalogue stores information about files/folders archived to tape media with file to tape jobs, as well as backup files produced by backup to tape jobs. The content of the Tape catalogue can be examined in the Files view.
- Backup catalogue stores information about VMs whose backups are archived to tape media with backup to tape jobs. The content of the Backup catalogue can be examined under the Backups > Tape node in the Backup & Replication view

1.52.4 Media Pool

A media pool simply defines a group of tapes managed by Veeam Veeam Backup & Replication. There are three types of media pools:

- **Service media pools.** Created and managed automatically. It is not possible to modify their settings. They contains:
 - Empty media starts out in the **Free pool** indicating it's available for use in other pools.
 - Unknown media will be placed to the **Unrecognized pool** so that it is not overwritten.
 - After inventory or cataloging, media with existing data is placed into the **Imported pool**. Review the contents and place such media into the **Free pool** for overwrite or leave in **Imported pool** to keep the data.
 - Exhausted or broken tapes are placed into the **Retired pool** and are not used further.
- **Media pools** are groups of media to which backup data can be written.
 - You can create as many custom media pools as needed.
 - Media can be assigned to a pool manually, or configured to be automatically assigned from the free pool.
 - Configure each pool settings according to the purpose of the pool, such as the overwrite protection period that is applied to all media within the pool.
 - Since v9 a (Custom) Tape Pool can be spanned over multiple tape libraries. The idea is to use the capacity and drives of multiple tape systems together and to failover to another tape library in case one library goes offline.
- **GFS media pools** are used to store weekly, monthly, quarterly and yearly backups on tape.
 - You can create as many GFS tape pools as needed.
 - Media can be assigned to a pool manually, or configured to be automatically assigned from the free pool. As well optional can define specific tapes for specific media sets (for example yearly backups).
 - Configure each pool settings according to the purpose of the pool, such as the overwrite protection period that is applied to all media within the pool.

1.52.5 Media Set

A media set is a subset of a media pool that contains at least one backup. A new media set can be created for every backup, or on a time based schedule (i.e. weekly). It is also possible to reuse the same media set forever. When a media set contains at least one full backup, it is a self-sufficient restore point. It means that if you have all tapes from the media set at hand, you can be sure that restore will be successful.

1.52.6 Media Vault

A media vault is used to organize offline media. For example, you have a service organization that transports the tapes to a safe at a bunker. You can name the vault accordingly and add some useful information in the description (phone number, place, etc.). When you need to transport physical tapes to the safe, add these tapes to the vault manually or set automatic export of offline tapes to a vault in the tape jobs or media pools properties.

1.53 Backup Modes

Backup jobs can create different backup types of backup file chains on disk depending on the backup mode used. Depending on backup mode, “Backup to Tape” jobs either copies files to tape or synthesize a full backup. The following rules apply:

- When archiving reverse incremental backups, the behavior varies on the type of media pool used:
 - **Standard Media Pool:** The tape job will always copy the full backup and ignore any rollback files (VRB)
 - **GFS Media Pool:** The tape job will create a full backup from VRB files on specified day(s) as per schedule.
- When archiving forward incremental backups, *with* active or synthetic full scheduled, the backup chain on tape will be a copy of the backup chain on disk. The virtual full option in tape job configuration is ignored.
- If you archive forward incremental backups without synthetic or active full enabled, or archive Backup Copy Jobs, the full files are synthesized from existing restore points on disk. The virtual full backup schedule can be configured on the “Backup to Tape” job.

For more information about virtual full to tape, please see [Veeam Help Center](https://helpcenter.veeam.com/docs/backup/vsphere/virtual_full_backup.html?ver=95)

If the source backup job contains multiple chains, and the checkbox “Process latest full backup chain only” in advanced job settings is unchecked, you will be prompted for a decision, when creating a Backup to Tape job. You may choose to either only the last backup chain or all existing restore points.

1.54 Sizing

For the highest throughput, enabling [parallel processing for the Backup to Tape](#) is recommended. You need to size the servers and storage connection accordingly. It can be helpful to create multiple partitions with 2-4 tape drives and add these partitions to different tape servers. Adding these libraries to the [media pool](#) and enabling parallel processing will distribute the load across multiple drives and tape servers.

Note: Parallel processing for tape is unavailable for GFS media pools.

Install Windows 2012 R2 or above on the tape server for best performance. Use the latest Veeam version and patch level as they often contain tape throughput optimizations.

Perform a POC to test throughput of tape and disk. If you have no opportunity to test speed, assume that the lowest speed for backup to tape jobs with LTO5/6 is 50MB/s as a conservative estimate. We highly recommend to do a POC to evaluate real throughput to avoid additional hardware costs.

The GFS (Grandfather, Father, Son) tape job can help avoid a complex Backup to Tape job creation by handling weekly, monthly, quarterly and yearly backups in a single job.

For Backup to Tape jobs that use forward incremental (without synthetic or active fulls) jobs or Backup Copy Jobs as source of the data, it may be required to temporarily disable the job using pre- and post scripts, as the transform process of forever incremental forever will terminate the tape job. Another option is to increase the restore points of these jobs temporarily. By increasing the number of restore points for the source job, the Backups to Tape job will not be terminated by the merge process. However, please note this will increase the transform time significantly once the setting is reverted and is highly discouraged for large jobs. An example of this implementation can be found here: [v9 GFS job - No more continuous?](#)

1.55 Using 3rd party tape software

As Veeam Backup & Replication tracks and orchestrates all backups written to tape, Veeam recommends using the built-in Veeam tape features (Backups to Tape and Files to Tape jobs).

However, in some situations you may want to use an existing library with non-LTO tapes, or you need to integrate Veeam Backup & Replication into an existing backup-to-tape software. Veeam backup files contain all information needed for restore (e.g. deduplication information, VM metadata, etc.), and you can use the existing backup-to-tape solution to bring the Veeam backup files on tape. This approach can also support enterprise customer “Segregation of duty” demands as two complete different teams can handle backups and tape backups. No single person can delete by mistake or on purpose the primary and tape chain. Before having two backup solutions co-exist on the same server, please verify they do not conflict each other.

1.56 Tape Encryption

Veeam uses hardware encryption if it is provided by the tape device and enabled in Veeam Backup & Replication. Tape library should work in the application-managed encryption mode.

If the hardware based encryption is not supported by the tape device, software based AES-256 encryption is used. Please note software based encryption may cause significant performance degradation, if not natively accelerated by the CPU of the tape server.

Hardware based encryption is typically available for LTO-4 or newer libraries, and while a license is often required, this is usually supported for free by the tape library vendor.

When archiving data, Veeam generates a user key which is stored with data on tape. If you restore data using another Veeam backup server, provide the password or utilize the Password Loss Protection in Enterprise Manager. See the [User Guide](#) for more information.

If the hardware encryption option is used, and you archive to tape Veeam backups that are already encrypted on disk, they will be encrypted twice. If you restore such backups with double encryption on the same Veeam backup server they will be decrypted automatically. To decrypt on another Veeam backup server, you will need to enter the two passwords accordingly.

For additional details on tape encryption, see the corresponding section of this guide > [Encryption](#)

1.57 Tips

- “Short Erase” all tapes before use with Veeam to avoid any problems cause by data from other backup software
- Install latest Windows Updates
- Install latest firmware on library, drives, HBA (verify interoperability)
- Install separate HBAs for tape is recommended, but not required
- A staging area for backup files is required when restoring from tape. Keep this in mind when sizing backup repositories.
- Tape compression should be disabled **for** tape jobs, when backup files

are already compressed at the backup repository

- “File to Tape” engine is optimized for smaller amount of big files (e.g. backup files) only

1.58 Configuring Backup to tape

Before you configure a backup to tape job, complete the following prerequisites:

- You must have Veeam Backup & Replication Enterprise license or higher is installed on the Veeam backup server.
- You must pre-configure backup job(s) that produce the backup for archiving.
- The primary backup job must have at least 2 restore points on disk.
- The primary backup copy job must have at least 4 restore points on disk.
- You must configure one or more simple media pool with the necessary media set and retention settings.
- You must load tapes to the tape device and configure the target media pool so that it has access to them. If the media pool has no available tape, the tape job will wait for 72 hours and then terminate.

Mind the following limitations:

- The backup to tape job processes only VBK (full backups) and VIB files (forward incremental backups).
- If you back up to tape a reverse incremental chain, the tape job will always copy the full backup.
- Reverse incremental backups (VRB) are skipped from processing.
- Microsoft SQL Server log files (VLB) are skipped from processing.

1.59 Tape Parallel Processing

If your tape library has multiple drives, you can use drives simultaneously for writing data to tape. This option is useful if you have a lot of tape jobs running at the same time or you have a lot of data that must be written to tape in a limited backup window.

1.59.1 Note: You cannot enable parallel processing for GFS media pools.

To process the tape data in parallel, you can split the data across drives in 2 ways:

- Parallel processing for tape jobs
- Parallel processing for source chains of one (or more) tape jobs Processing Tape Jobs Simultaneously When you process tape jobs in parallel, the media pool assigns a drive to each running tape job.

The media pool can use the predefined maximum number of drives and process the equal number of tape jobs simultaneously.

For example, if you set 3 drives as the maximum, you can process up to 3 tape jobs at the same time. If you have more jobs running at the same time, they are queued. When one of the jobs finishes and releases its drive, the first queued job takes the drive.

This option is available for backup to tape and file to tape jobs. For example:

- You set the maximum number of drives to 3.
- 4 tape jobs start at the same time. The tape jobs start and jobs A, B and C occupy 3 drives to write data to tape. The Tape job D is queued and waits. When one of the jobs finishes and releases its drive, the Tape job D takes the drive and starts writing data.

1.59.2 Processing Backup Chains Simultaneously

When you select processing backup chains in parallel, the media pool processes several primary jobs simultaneously. If the primary jobs produce per-VM backups, the media pool processes several per-VM backup chains simultaneously. This option is available for backup to tape jobs only. For example:

- You set the maximum number of drives to 3.
- Tape job A has 4 primary jobs. Tape job A starts, and occupies 3 drives to process 3 primary jobs. The fourth primary job is queued and waits. When one of the drives is released, the fourth primary job takes the drive and starts writing data. If another tape job starts, it will be queued and wait until Tape job A finishes. Note: If the media pool is configured to fail over to another library in case all tape drives are busy, only tape jobs can use drives of the next library. You cannot split source backup chains within one job across libraries.

1.60 Virtual Full Backups

Virtual full allows you to backup up forever forward incremental backup chains to tape. The forever forward incremental chain always keeps on disk one full backup followed by a fixed number of increments. The full backup is constantly rebuilt: as new increments appear, the older ones are injected into the full.

Unlike disk backups, tape archives are static: tape jobs cannot rebuild backups once they are written to tape. Also, the standard backup to tape scheme (archiving new restore points during each tape session) cannot be used: the tape archive would have one full backup and an endless chain of increments all of which would be required for restore.

To adapt the forever forward incremental chains to tapes, Veeam Backup & Replication uses the virtual full. The virtual full mechanism creates a periodic synthesized full backup on tape. The periodic fulls split the forever incremental backup chain into shorter series of files that can be effectively stored to tapes. Each series contains one synthesized full backup and a set of increments. Such series are convenient for restore: you will need to load to the tape device only those tapes that are part of one series.

The virtual full does not require additional repository disk space: it is synthesized directly on tape on the fly, when the tape job runs. To build such full backup, Veeam Backup & Replication uses backup files that are already stored on the backup repository. If the primary job produces a forever incremental backup chain or is a backup copy job, Veeam Backup & Replication will periodically create a virtual full backup. You can configure the full backup with the scheduler.

The virtual full cannot be switched off; however, it is disabled automatically if the primary job periodically creates active full or synthetic full backups. The virtual full does not depend on the job settings for incremental backups. If you enable the virtual full for the job, it will be created in any case, no matter whether you enable or do not enable incremental backups.

1.60.1 Prioritising Tape backups over Primary backups

Sometimes, the primary job may start when the tape job is still running. By default, the primary job has priority. In this case, the tape job terminates with error and no data is written to tape. Select the Prevent this job from being interrupted by primary backup jobs option if you want to give the tape job a higher priority. If this option is selected, the primary job will wait until the tape job finishes. Note that the primary job may start with a significant delay.

1.61 File Backup to Tape

File to tape job allows you to back up to tape any Microsoft Windows or Linux files. To back up Veeam backup files, you can use backup to tape jobs that are specially intended for this and offer more possibilities. However, you can archive backups as files using file to tape job. The file to tape job compares the source files to the files stored in tape

archive and copies the changes to tape. You can create both full and incremental backups of files on tape. Veeam Backup & Replication supports file backup from any server which has been added as a managed server to the Veeam Backup console (that is, Windows or Linux server, including physical boxes). You can also archive files residing on NAS devices. When planning file to tape jobs, consider that the job performance depends more on the number of files to back up than on the amount of data. For example, writing a large number of small files with overall size of 10GB with one job will take more time than writing one 10GB file. If your job contains an extra-large number of files (like millions of files) with one job, the job performance will be affected significantly. To improve performance, consider creating several file to tape jobs.

1.61.1 Note: If the file to tape job fails to complete in 3 weeks, it is terminated by timeout.

1.61.2 VM Backup to Tape

To back up data to tape, you need to create and run tape jobs dedicated to archive Veeam backups that were produced by Veeam backup jobs to tapes. When a backup to tape job runs, it does not create new backups: it locates already existing backups and copies them from backup repository to tape. You need to set the source of the tape job: jobs and/or backup repositories. Jobs as Source The following jobs can be primary for tape jobs:

- VMware backup jobs
- Hyper-V backup jobs
- VMware backup copy jobs
- Hyper-V backup copy jobs
- Windows Agent backup jobs
- Linux Agent backup jobs
- Windows Agent backup copy jobs
- Linux Agent backup copy jobs.

When the tape job starts on it's schedule, it picks the restore points that were produced by the primary jobs in period since the last tape job run. If you change the configuration of the primary jobs, the tape job is updated automatically: it adds new VMs to the list of VMs to archive or stops archiving VMs that were removed from primary jobs. The primary jobs may use any backup method:

- Forever forward incremental backup method: To back up the forever forward incremental chains to tape, the tape job uses the virtual full. The virtual full creates a synthetic full backup on tape regularly (for example, once a week) and splits the chain into short series of tapes which is more convenient for restore. For more information, see Virtual Full Backup. The source backup chain must contain 4 or more restore points. If the primary job is backup copy job, keep in mind that the last restore point of the backup copy job stays active until the next restore point is created. The tape job does not copy such active points, because they may be updated. For this reason, the backup chain on tape will be always one restore point shorter than on disk.
- Forward incremental backup method: When the tape job backs up the forward incremental chain to tape, it creates a copy of the disk backup chain. The source backup chain must contain 2 or more restore points.
- Reverse incremental backup method: The last backup in the reverse incremental backup chain is always the full backup. If the source backup chain is reverse incremental, the tape job will copy the full backup each time the tape job runs. The increments are skipped. The source backup chain may contain any number of restore points.

1.61.3 Backup Repositories as Source

When you add a repository as source to tape job, the tape job constantly scans the selected repository (or repositories) and writes the newly created backups to tape. The tape job monitors the selected repository in a background mode. You can set explicit backup windows for the tape job. In this case, the tape job will start on the set time and archive all new restore points that were created in period since the last job run. If you create or remove backup jobs that use this repository, or if you change the configuration of such backup jobs, you do not need to reconfigure the tape job that archives the repository. Mixed Jobs To one tape job, you can link an unlimited number of sources. You can mix primary jobs of different type: backup and backup copy, and of different platform (VMware, Hyper-V, Windows Agent or Linux Agent). You can add jobs and repositories as source to the same tape job. Important! The tape job looks only for the Veeam backups that are produced by backup jobs running on your console. Other files will be skipped. Note that to back up files, you need to configure file to tape job.

1.61.4 Linking Primary Jobs

You can add primary jobs to tape jobs at any moment: when you create a tape job, or later. Adding primary jobs is not obligatory when you create a tape job: you can create an “empty” job and use it as a secondary destination target. When you link jobs, the tape job processes them in the same way as the jobs added with the Tape Job Wizard. For more information, see Linking Backup Jobs to Backup to Tape Jobs.

1.62 Restores

1.62.1 VM Restore from Tape to Infrastructure

Restoring a VM from tape with Veeam Backup & Replication is a lot like restoring a VM from disk. For example, you can choose a desired restore point, select the target location or change the configuration of the restored VM. To restore a VM from tape, you can choose between the following options:

- restore directly to infrastructure
- restore through a staging repository

To choose the needed option, select Restore directly to the infrastructure or Restore through the staging repository at the Backup Repository step of the Full VM Restore wizard.

Restore Directly to Infrastructure

When you restore VMs from tape directly to the infrastructure, the restore process publishes the VMs to the virtual infrastructure copying the VM data directly from tape. This option is recommended if you want to restore one VM or a small number of VMs from a large backup that contains a lot of VMs. In this case, you do not need to provide a staging repository for a large amount of data most of which is not needed to you at the moment. This option is slow if you restore many VMs. The VMs are restored one by one: this requires a lot of rewinding of tape as tapes do not provide random access to data.

Restore Through Staging Repository

When you restore VMs from tape through a staging repository, the restore process temporarily copies the whole restore point to a backup repository or a folder on disk. After that Veeam starts a regular VM restore. This option is recommended if you want to restore a lot of VMs from a backup as the disk provides a much faster access to random data blocks than tape.

Backup Restore from Tape to Repository

This option allows you to copy VM backups from tape to repository. This is helpful if you need some backups on disk for later use, or also for VM guest OS files restore. You can restore full backups or incremental backups to a repository or any location of your choice. The restored backup is registered in the Veeam Backup & Replication console as an imported disk backup so that you can use it for any restore from disk scenario later on. For one restore session at a time, you can choose one restore point available on tape.

File Restore from Tape

You can restore files and folders that were previously archived with file to tape jobs. Restoring capabilities allows you to restore files to their original location or another server, preserving ownership and access permissions. The file restore process allows you to restore files to any restore point available on tape.

1.63 Veeam Explorers

Veeam Explorers are tools included in all editions for item-level recovery from several application. As of v9.5, following Explorers are available:

- Veeam Explorer for Active Directory
- Veeam Explorer for SQL Server
- Veeam Explorer for Exchange
- Veeam Explorer for SharePoint
- Veeam Explorer for Oracle
- Veeam Explorer for Storage Snapshots

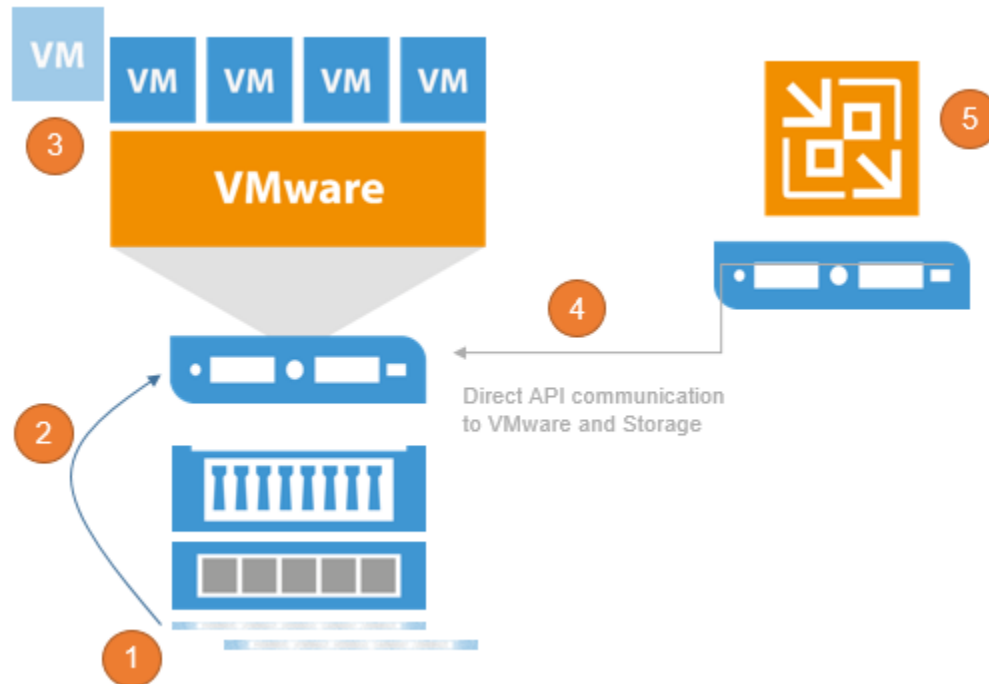
Each Explorer has a corresponding user guide available in Helpcenter: [Veeam Backup Explorers User Guide](#). For specifics of performing granular restore of certain applications refer to the Applications section of this guide.

1.63.1 Explorer for Storage Snapshots

Veeam Explorer for Storage Snapshots (VESS) is included, but it is related to storage integrations with primary storage. This is explained in the [Backup from Storage Snapshots](#) section of this guide.

VESS is a very easy way to perform item-level recovery directly from storage snapshots. Veeam is able to use discover and mount any storage snapshot for restores. By combining the Veeam application consistent with crash consistent snapshots, the RPO for certain applications can be significantly reduced.

When opening VESS, the following workflow kicks off:



1. Creating a Clone of the Snapshot to make it writeable
2. In case of Block access (iSCSI, FC, FCoE) mount the new LUN to a an ESXi and register a temporary datastore, in case of NFS access the existing NFS datastore and look for the cloned VM
3. Register the temporary VM within the VMware inventory
4. Access the VM using the VMware API
5. Show the content as a Veeam Explorer to restore

After restoring and exiting VESS, the temporary datastore, VM and LUN clones will be rolled back and cleaned up.

1.64 Interaction with vSphere

Veeam Backup & Replication relies heavily on the vSphere infrastructure it is protecting. Much of the implementation success depends on the performance and stability of this environment. In this section, we will discuss those interactions and note the items that should be considered for a successful implementation.

While it is possible to connect a Veeam Backup & Replication server directly to ESX(i) hosts, this section assumes a vSphere environment with at least one vCenter Server, and that the backup server is integrated at the vCenter Server level, as this is the best practice configuration in almost all use cases.

1.64.1 vCenter Server

One of the most critical components of any vSphere environment is the vCenter Server. This server provides a single view of the entire virtual environment, and a central point of management. Veeam Backup & Replication communicates with the vCenter Server in many operations. For this reason, fast and stable communication between Veeam Backup & Replication and the vCenter Server is critical to achieving a stable backup environment.

Consider some important factors:

- Problems with connectivity to the vCenter Server is one of the top reasons for failed Veeam jobs. Having a well-performing vCenter Server with reliable connectivity will mitigate this issue and provide a strong backbone for a reliable backup infrastructure.
- The vCenter Server must be reliable and always available when backup jobs are running. It must be able to answer queries and perform actions in a reasonable amount of time. If the vCenter Server performs poorly during normal operations, this should be corrected prior to implementing Veeam Backup & Replication.
- For larger environments, with many concurrent jobs, especially jobs that run at short intervals, the load on the vCenter Server can be significant. The vCenter Server must be able to handle increased transactional workload to prevent random job failures due to command timeouts.
- The backup server must have reliable network connectivity to the vCenter Server. It is generally suggested that the backup server is placed in close logical proximity to the vCenter Server, but this is not always the best deployment option. In cases where the backup server and vCenter Server must be deployed across a distance, the only real requirement is that this connection is consistent and reliable.
- When maintenance is being performed on the vCenter Server, best practice would dictate that all Veeam Backup & Replication jobs must be idle, and the Veeam Backup Service should be stopped. This includes applying Windows updates (if using the vCenter Server installable version), vCenter Server patches and upgrades, or any maintenance that would require the vCenter service to be restarted or the system rebooted.

1.64.2 Impact of Snapshot Operations

To create VM backups, Veeam Backup & Replication leverages the VMware vSphere snapshot functionality. When Veeam Backup & Replication begins the backup of a VM, it communicates with vSphere to request a snapshot of the VM, and after the backup of the VM is complete, Veeam requests that vSphere remove the snapshot (with the exception of backup jobs leveraging Backup from Storage Snapshots). The creation and removal of snapshots in vSphere creates a significant impact on the environment what must be taken into account. This section will describe various factors that should be considered regarding this process, and offer several techniques to minimize the impact of snapshot operations.

As a concept, VMware vSphere snapshots are a simple technology. A VM generally contains at least one virtual disk, which is represented by a VMDK file. When a snapshot is taken, VMware vSphere continues to read blocks from the file as normal. However, for any new blocks that are written to the disk, these writes are redirected to a new “thin” VMDK file called the delta file.

Since the original VMDK file is only being used for reads, it provides a consistent view of the blocks that made up the VM at the time the snapshot was taken. This allows Veeam Backup & Replication to read this base disk as a consistent image for backup and replication functions. When the snapshot is removed, the blocks that were written to the delta file are read and written back into the original VMDK, and finally the delta file is discarded.

As Veeam Backup & Replication leverages the snapshot technology for performing backups, you should ensure it is possible to snapshot the virtual machine disks, since there are certain configurations that do not support snapshots. To identify VMs that do not support snapshots, see [VMware KB article 1025279](#) ; you can also use [Veeam ONE assessment reports](#) to automatically detect them before starting Veeam Availability project.

As with many things in technology, although the concept is simple, the actual implementation is a little more complex. The following section is a quick look at the impact of various operations on the VM and underlying infrastructure.

Snapshot Creation

The actual operation of creating a snapshot generally has only a minor impact: the snapshot file has to be created, and there is a very short “stun” of the VM. This “stun” is generally short enough (typically, less than 1 sec), so it is rarely an issue except for the most time-sensitive applications.

Note: Veeam Backup & Replication leverages a standard VM snapshot for the backup process. These VMware snapshots have a single file size limitations. Keep in mind, that the maximum file size include all snapshot files and the data disk in total. For example if you have an old VMFS version 3 the maximum file size (including snapshots) is 2TB and so your data disk should not be sized over 1.98TB to still be able to create snapshots. For details, see [VMware KB article 1012384](#).

The default number of concurrently open snapshots per datastore in Veeam Backup & Replication is 4. This behavior can be changed by creating the following registry key:

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication
- Key: MaxSnapshotsPerDatastore
- Type: REG_DWORD
- Default value: 4

Snapshot Open

Simply having a snapshot open for a running VM involves some performance penalty on the VM, the ESX(i) host and the underlying storage. The host has to track the I/O, split writes to the snapshot file and update the snapshot file metadata. This overhead, in turn, impacts the guest (primarily, with slower I/O).

This is generally most notable for VMs with significant write load, and has less impact on read performance.

From the storage perspective, VMs running with an open snapshot require additional space to store the snapshot data, and additional I/O load on the datastore. This is generally more noted on systems with significant write I/O load.

Note: Refer to VMware Knowledge Base article at www.kb.vmware.com/kb/1035550 for information on vMotion and Storage vMotion processes performed with open snapshots.

Snapshot Removal

Snapshot removal is the step with the highest impact from the performance perspective. I/O load increases significantly, due to the extra R/W operations required to commit the snapshot blocks back into the original VMDK. This eventually leads to the VM “stun” required to commit the final bits of the snapshot. The “stun” is typically a short pause usually only a few seconds or less, when the VM is unresponsive (“lost ping”), while the very last bits of the snapshot file are committed.

VMware vSphere uses the “rolling snapshot” for older versions and the same method as storage vMotion uses starting from vSphere 6.0u1 to minimize the impact and duration of the stun, as described below:

For vSphere 6u1 and newer: The host leverages the Storage vMotion Mirror driver to copy all needed data to the original data disks. When completed, a “Fast Suspend” and “Fast Resume” is performed (comparable with vMotion) to bring the original data files online.

For older vSphere Versions (Rolling Snapshot):

1. The host takes a second, “helper”, snapshot to hold new writes.
2. The host reads the blocks from the original snapshot and commits them to the original VMDK file.
3. The host checks the size of the “helper” snapshot. If the size is over the threshold, step 1 is repeated.
4. Once all helper snapshots are determined to be under the threshold size, vSphere “stuns” the VM and commits the last bits of the snapshot.

This “stun” period can be less than one second for small VMs with light load, or several seconds for larger VMs with significant load. To external clients, this small stun looks like the server is busy and thus might delay a response for a few seconds. However, applications that are very sensitive to delays may experience issues with this short period of unresponsiveness.

For explanation of snapshot removal issues, see [VMware KB article 1002836](#).

1.64.3 How to Mitigate?

To mitigate the impact of snapshots, consider the following recommendations:

- Upgrade to vSphere 6u1 or newer to use the new Storage vMotion based Snapshot commit processing.
- **Minimize the number of open snapshots per datastore.** Multiple open snapshots on the same datastore are sometimes unavoidable, but the cumulative effect can be bad. Keep this in mind when designing datastores, deploying VMs and creating backup and replication schedules. Leveraging backup by datastore can be useful in this scenario.
- **Consider snapshot impact during job scheduling.** When possible, schedule backups and replication job during periods of low activity. Leveraging the Backup Window functionality can keep long-running jobs from running during production. See the corresponding setting on the **Schedule** tab of the job wizard
- **Use the vStorage APIs for Array Integration (VAAI) where available.** VAAI can offer significant benefits:
 - Hardware Lock Assist improves the granularity of locking required during snapshot growth operations, as well as other metadata operations, thus lowering the overall SAN overhead when snapshots are open.
 - VAAI in vSphere 5.x offers native snapshot offload support and should provide significant benefits once vendors release full support.
 - VAAI is sometimes also available as an ESXi plugin from the NFS storage vendor.
- **Design datastores with enough IOPS to support snapshots.** Snapshots create additional I/O load and thus require enough I/O headroom to support the added load. This is especially important for VMs with moderate to heavy transactional workloads. Creating snapshots in VMware vSphere will cause the snapshot files to be placed on the same VMFS volumes as the individual VM disks. This means that a large VM, with multiple VMDKs on multiple datastores, will spread the snapshot I/O load across those datastores. However, it actually limits the ability to design and size a dedicated datastore for snapshots, so this has to be factored in the overall design.

Note: This is the default behavior that can be changed, as explained in the VMware Knowledge Base: <https://kb.vmware.com/s/article/1002929>

- **Allocate enough space for snapshots.** VMware vSphere 5.x puts the snapshot VMDK on the same datastore with the parent VMDK. If a VM has virtual disks on multiple datastores, each datastore must have enough space to hold the snapshots for their volume. Take into consideration the possibility of running multiple snapshots on a single datastore. According to the best practices, it is strongly recommended to have 10% free space within a datastore for a general use VM, and at least 20% free space within a datastore for a VM with high change rate (SQL server, Exchange server, and others).

Note: This is the default behavior that can be changed, as explained in the VMware Knowledge Base: <https://kb.vmware.com/s/article/1002929>

- **Watch for low disk space warnings.** Veeam Backup & Replication warns you when there is not enough space for snapshots. The default threshold value for production datastores is 10% . Keep in mind that you must increase this value significantly if using very large datastores (up to 62 TB). You can increase the warning threshold in the backup server options, of the Veeam Backup & Replication UI. You can also create a registry key to prevent Veeam Backup & Replication from taking additional snapshots if the threshold is breached:
 - Path: HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication
 - Key: BlockSnapshotThreshold
 - Type: REG_DWORD
 - Default value (in GB): 10

Tip: Use the [Veeam ONE Configuration Assessment Report](#) to detect datastores with less than 10% of free disk space available for snapshot processing.

- **Enable parallel processing.** Parallel processing tries to backup multiple VM disks that belong to a single VM at the same time. This reduces snapshot lifetime to the minimum. This option is enabled by default. Please note if you upgraded from v6.5 or earlier versions, you have to enable this option explicitly in the backup server options.
- **Tune heartbeat thresholds in failover clusters.** Some application clustering software can detect snapshot commit processes as failure of the cluster member and failover to other cluster members. Coordinate with the application owner and increase the cluster heartbeat thresholds. A good example is Exchange DAG heartbeat. For details, see [Veeam KB Article 1744](#).

1.64.4 Considerations for NFS Datastores

Backup from NFS datastores involves some additional consideration, when the **virtual appliance (hot-add)** transport mode is used. Hot-add takes priority in the intelligent load balancer, when Backup from Storage Snapshots or Direct NFS are unavailable.

Datastores formatted with the VMFS file system have native capabilities to determine which cluster node is the owner of a particular VM, while VMs running on NFS datastores rely on the LCK file that resides within the VM folder.

During hot-add operations, the host on which the hot-add proxy resides will temporarily take ownership of the VM by changing the contents of the LCK file. This may cause significant additional “stuns” to the VM. Under certain circumstances, the VM may even end up being unresponsive. The issue is recognized by VMware and documented in <https://kb.vmware.com/s/article/2010953>.

Note: This issue does not affect Veeam Direct NFS as part of Veeam Direct Storage Access processing modes and Veeam Backup from Storage Snapshots on NetApp NFS datastores. We highly recommend you to use one of these 2 backup modes to avoid problems.

In hyperconverged infrastructures (HCI), it is preferred to keep the datamover close the backed up VM to avoid stressing the storage replication network with backup traffic. If the HCI is providing storage via the NFS protocol (such as Nutanix), it is possible to force a Direct NFS data mover on the same host using the following registry key:

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication
- Key: EnableSameHostDirectNFSMode
- Type: REG_DWORD
- Default value: 0 (*disabled*)

Value = 1 - when a proxy is available on the same host, Veeam Backup & Replication will leverage it. If the proxy is busy, Veeam Backup & Replication will wait for its availability; if it becomes unavailable, Veeam Backup & Replication will switch to NBD mode.

If for what ever reason Direct NFS processing can not be used and HotAdd is configured, ensure that proxies running in the Virtual Appliance mode (Hot-Add) are on the same host as the protected VMs.

To give preference to a backup proxy located on the same host as the VMs, you can create the following registry key:

- Path: HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication
- Key: EnableSameHostHotAddMode
- Type: REG_DWORD
- Default value: 0 (*disabled*)

Value = 1 – when proxy A is available on the same host, Veeam Backup & Replication will leverage it. If proxy A is busy, Veeam Backup & Replication will wait for its availability; if it becomes unavailable, another Hot-Add proxy (proxy B) will be used.

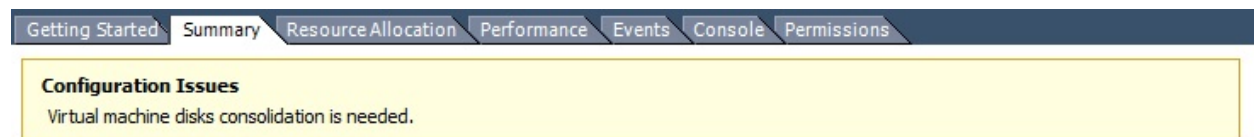
Value = 2 - when proxy A is available on the same host, Veeam Backup & Replication will leverage it. If proxy A is busy, Veeam Backup & Replication will wait for its availability; if it becomes unavailable, Veeam Backup & Replication will switch to NBD mode.

This solution will typically result in deploying a significant number of proxy servers, and may not be preferred in some environments. For such environments, it is recommended switching to Network mode (NBD) if Direct NFS backup mode can not be used.

1.64.5 Snapshot Hunter

At Veeam Support, one of the most commonly raised support cases was for orphaned snapshots. Orphaned snapshots were caused by VMware's own failed snapshot commit operations due to unreleased VMDK file locks during VDDK operations. Veeam uses the VMware standard VM snapshot processing for backup and replication processes, so although Veeam was not the origin of the orphaned snapshots, as Veeam uses VMware snapshots, Veeam is often seen as a root cause as this issue was only discovered when a backup failed.

If not monitored appropriately, VMware orphaned snapshots can cause many unexpected problems. The most common problems are overfilled VM datastores, or snapshots growing so large they are impossible to commit. This is a well-known VMware vSphere issue described in [VMware KB article 1007814](#). The only way to manually remediate this issue is cloning the VM and performing a new full VM backup.



Veeam Snapshot Hunter automatically detects any VM with the configuration issue “Virtual machine disks consolidation needed”. Prior to performing backup of such VMs, Veeam Backup & Replication will trigger disk consolidation (provided that the datastore performance threshold specified in the [Storage Latency Control](#) settings is not exceeded).

Snapshot Hunter will attempt consolidation eight (8) times. If consolidation fails after all retries, Veeam Backup & Replication will send an e-mail with a warning.

You can view information on the Snapshot Hunter sessions on the **History > System** view in Veeam Backup & Replication console.

Note: Currently, the default behavior of Snapshot Hunter cannot be changed. As Snapshot Hunter will automatically retry consolidation up to eight times, it may be inappropriate for some VMs that require planned downtime to consolidate the snapshot manually. Such VMs should be excluded from backup or replication jobs until the orphaned snapshots are manually removed.

If you are evaluating Veeam Backup & Replication, use the [Infrastructure Assessment Reports](#) included in Veeam Availability Suite to identify VMs with snapshots that can be affected by automatic snapshot consolidation.

1.64.6 Storage Latency Control

One question that often arises during the development of a solid availability design is how many proxy servers should be deployed. There must be a balance between the production infrastructure performance (as you must avoid overloading production storage), and completing backup jobs in time.

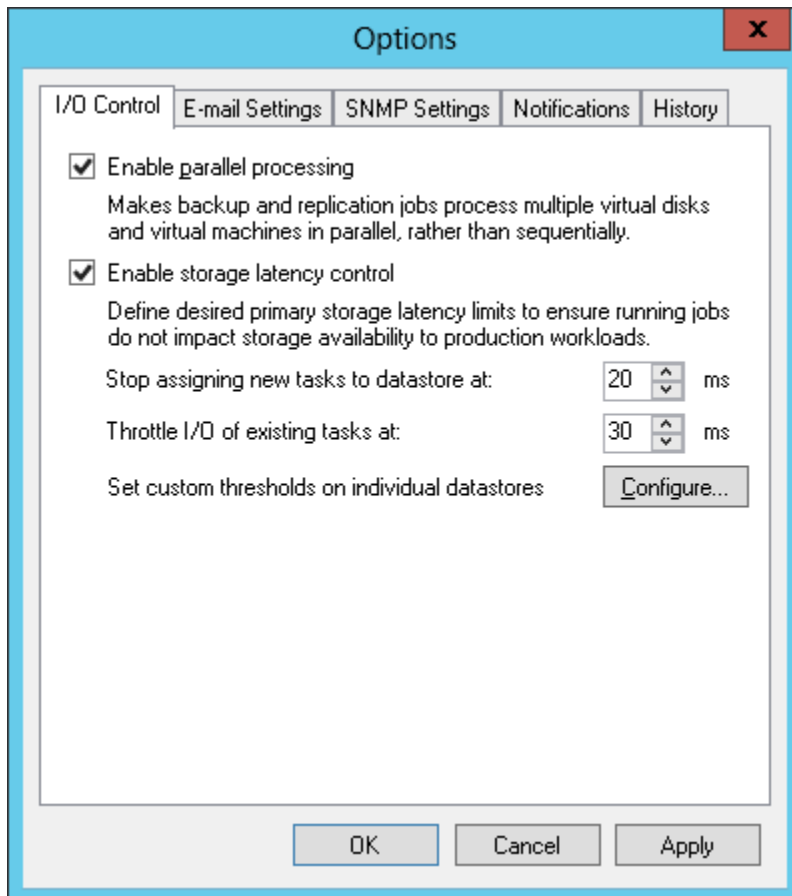
Modern CPUs have many physical cores and can run many tasks simultaneously. The impact of having many proxy servers reading data blocks from the production storage at a very high throughput may be negative. With this in mind,

many businesses avoided running backup or replication jobs during business hours to ensure good response time for their end users. Storage Latency Control was implemented to help avoid this issue.

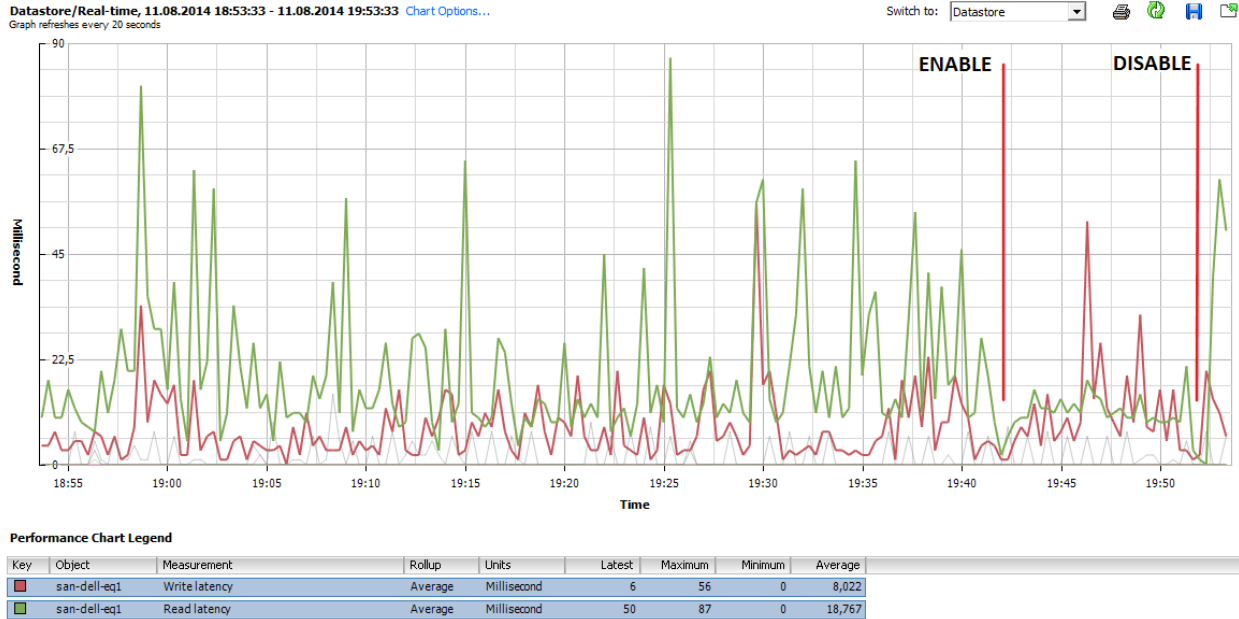
When Storage Latency Control is enabled, it monitors the storage read latency on the production datastores using real-time metrics from the hypervisor. By default, metrics from the hypervisor are collected every 20 seconds. These settings are inherited from vSphere.

The first Storage Latency Control threshold **Stop assigning new tasks to datastore at** puts a limitation on assigning new tasks (one task equals one VM disk). If the latency for a particular datastore is exceeded, no more proxy tasks will be assigned to it, until the latency drops below the threshold.

If limiting the number of tasks assigned to the datastore is not sufficient, Storage Latency Control will throttle the throughput for existing tasks according to the second threshold **Throttle I/O of existing tasks at**.



The results of enabling Storage Latency Control are very easy to review using the vSphere Client.



When to Use?

Storage Latency Control provides a smart way to extend backup windows or even eliminate backup windows, and run data protection operations during production hours.

When Storage Latency Control is enabled, Veeam Backup & Replication measures the storage latency before processing each VM disk (and also during processing, if **Throttle I/O of existing tasks at** setting is enabled). Furthermore, if the storage latency for a given datastore is already above the threshold, committing VM snapshots can be delayed. In some environments, enabling Storage Latency Control will reduce the overall throughput, as latency increases during the backup window.

However, in most environments having this feature enabled will provide better availability to production workloads during backup and replication. Thus, if you observe performance issues during backup and replication, it is recommended to enable Storage Latency Control.

Storage Latency Control is available in Enterprise and Enterprise Plus editions. The Enterprise Plus customers are offered better granularity, as they can adjust latency thresholds individually for each datastore. This can be really helpful in infrastructures where some datastores contain VMs with latency-sensitive applications, while latency thresholds for datastores containing non-critical systems can be increased to avoid throttling.

1.64.7 vCenter Server Connection Count

If you attempt to start a large number of parallel Veeam backup jobs (typically, more than 100, with some thousand VMs in them) leveraging the VMware VADP backup API or if you use Network Transport mode (NBD) you may face two kinds of limitations:

- Limitation on vCenter SOAP connections
- Limitation on NFC buffer size on the ESXi side

All backup vendors that use VMware VADP implement the VMware VDDK kit in their solutions. This kit provides standard API calls for the backup vendor, and helps to read and write data. During backup operations, all vendors have to deal with two types of connections: the VDDK connections to vCenter Server and ESXi, and vendor's own connections. The number of VDDK connections may vary for different VDDK versions.

If you try to back up thousands of VMs in a very short time frame, you can run into the SOAP session count limitation. For example, in vSphere 5.1 the default maximum number of sessions is 500. If you hit this limitation, you can increase the vCenter Server SOAP connection limit from 500 to 1000. For details, see <https://kb.vmware.com/s/article/2004663>.

Veeam's scheduling component does not keep track of the connection count. For this reason, it is recommended to periodically check the number of vCenter Server connections within the main backup window to see if you can possibly run into a bottleneck in future, and increase the limit values on demand only.

You can also optimize the ESXi network (NBD) performance by increasing the NFC buffer size from 16384 to 32768 MB (or conservatively higher) and reducing the cache flush interval from 30s to 20s. For details how to do this, see [VMware KB article 2052302](#). After increaing NFC buffer setting, you can increase the following Veeam Registry setting to add addition Veeam NBD connections:

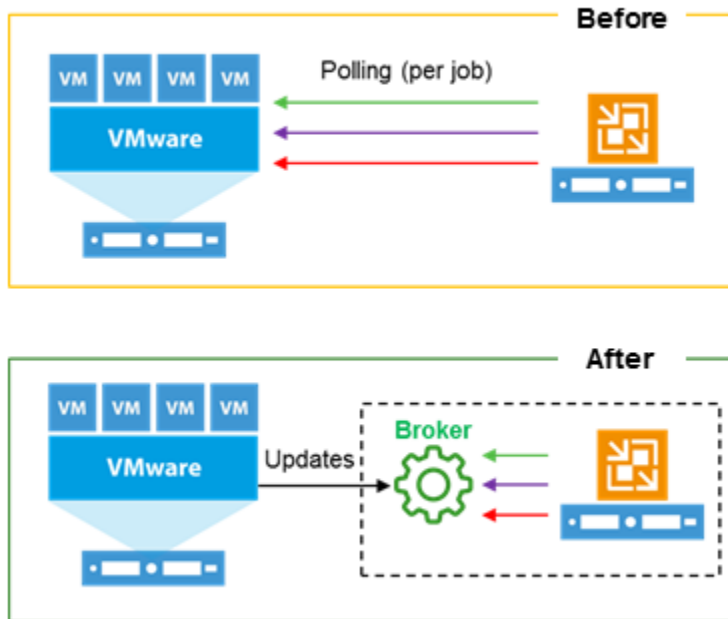
- Path: HKLM\SOFTWARE\Veeam\Veeam Backup and Replication
- Key: ViHostConcurrentNfcConnections
- Type: REG_DWORD
- Default value: 7 (*disabled*)

Be careful with this setting. If the buffer vs. NFC Connection ratio is too aggressive, jobs may fail.

1.64.8 Veeam Infrastructure cache

A new service in Veeam Backup & Replication v9.5 is **Infrastructure Cache** reflected as the “Veeam Broker Service” windows service. With it, Veeam can cache directly into memory an inventory of the objects in a vCenter hierarchy. The collection is very efficient as it uses memory and it is limited to just the data needed by Veeam Backup & Replication.

This cache is stored into memory, so at each restart of the Veeam services its content is lost; this is not a problem as the initial retrieval of data is done as soon as the Veeam server is restarted. From here on, Veeam “subscribed” to a specific API available in vSphere, so that it can receive in “push” mode any change to the environment, without the need anymore to do a full search on the vCenter hierarchy during every operation.



The most visible effects of this new service are:

- The load against vCenter SOAP connection is heavily reduced, as we have now one single connection per Veeam server instead of each job running a new query against vCenter;
- Every navigation operation of the vSphere hierarchy is instantaneous;
- The initialization of every job is almost immediate, as now the Infrastructure Cache service creates a copy in memory of its cache dedicated to each job, instead of the Veeam Manager service completing a full search against vCenter:

ACTION	DURATION
✓ Job started at 23/10/2016 16:51:19	
✓ Building VMs list	0:00:02
✓ VM size: 0,0 B	
✓ Changed block tracking is enabled	
✓ Processing NewVM-Test	0:01:09
✓ All VMs have been queued for processing	
✓ Job finished at 23/10/2016 16:53:01	

No special memory consideration needs to be done for the Infrastructure Cache, as its requirements are really low: as an example, the cache for an environment with 12 hosts and 250 VMs is only 120MB, and this number does not grow linearly since most of the size is fixed even for smaller environments.

1.64.9 Security

When connecting Veeam Backup & Replication to the vCenter Server infrastructure, you must supply credentials that the backup server will use to communicate with the vCenter Server.

The features that Veeam provides, such as backup, restore, replication, and SureBackup, interact with vSphere at the fundamental level. Certain permissions are required to take snapshots, create VMs, datastores, and resource groups. Because of this level of interaction, it is generally recommended that Veeam Backup & Replication uses a restricted account with the permissions that are required to complete the job.

However, in some environments full administrative permissions are not desirable or permitted. For those environments, Veeam has identified the minimum permissions required for the various software functions. Review the “[Required Permissions](#)” document (not changed since V9.0) and configure the account used by Veeam Backup & Replication to meet these requirements.

You can also leverage security to restrict the part of the environment that the backup server can “see”. This can have multiple benefits beyond security in that it lowers the time required to parse the vCenter Server hierarchy and reduces the memory footprint required to cache this information. However, care must be taken when attempting to use this level of restriction, as some permissions must be provided at the very top of the vCenter Server tree. Specifically if you access the vCenter over a WAN link such scoping can reduce the (management background) WAN traffic.

For a detailed description of accounts, rights and permissions required for Veeam Backup & Replication operations, see the “[Required Permissions](#)” document (not changed since V9.0).

1.65 Hyper-V backup modes

Veeam Backup and Replication provides two different backup modes to process Hyper-V backups, both relying on the Microsoft VSS framework.

- **On-Host** backup mode, for which backup data processing is on the Hyper-V node hosting the VM, leveraging non transportable shadow copies by using software VSS provider.
- **Off-Host** backup mode, for which backup data processing is offloaded to another non clustered participating Hyper-V node, leveraging transportable shadow copies using Hardware VSS provider provided by the SAN storage vendor.

Backup mode availability is heavily depending on the underlying virtualization infrastructure, leaving Off-Host backup mode available only to protect virtual machines hosted on SAN storage volumes. It is important that the VSS Framework provided by the storage vendor is tested and certified to work with Microsoft Hyper-V Clusters. Intensive checks of vendor VSS provider during POC is highly recommended (Cluster environment).

Performance wise, since both backup modes are using the exact same Veeam transport services, the only differentiating factors will be the additional time requested to manage transportable snapshots (in favor of On-Host mode) and the balance between compute and backup resources consumption during backup windows (in favor of Off-Host mode).

When using Windows Server 2016 On-Host proxy mode is very fast and will reduce the amount of included components. The Veeam Agent will then allocate the performance for deduplication and compression on the hosts systems. Consider that when planning the Veeam Job design. Please be aware that you will need up to 2GB of RAM on the Hyper-V Host per running task (one task = backup of one virtual disk). This memory must be free during Backup, otherwise the Hyper-V Host will start paging, what will end up in a slow system at all.

Backup modes selection matrix

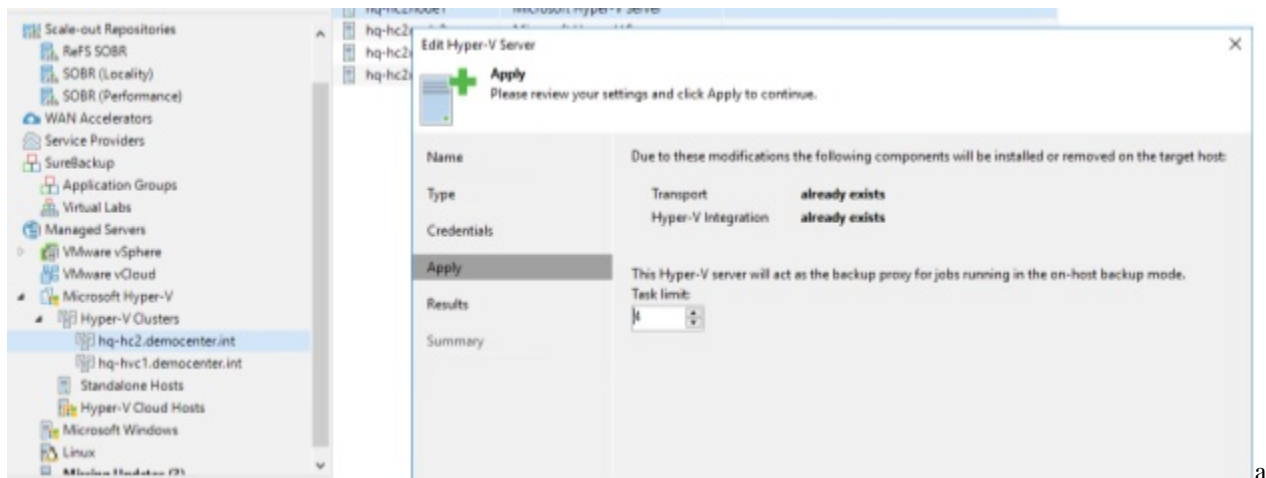
PRO	CON	On-Host	Simplifies management	Does not depend on third party VSS provider	Does not require additional hardware, load is spread over all Hyper-V hosts	Can be used on any Hyper-V infrastructures	Requires additional resources from the hypervisors (CPU, Network IO and RAM) during the backup window, for IO processing and optimization	Off-Host	No impact on the compute resources on the hosting Hyper-V Server	Adds additional
-----	-----	---------	-----------------------	---	---	--	---	----------	--	-----------------

delay for snapshots transportation Available only for virtualization infrastructures based on SAN storage Depends on third party VSS provider

1.65.1 Limiting the impact of On-Host backup mode on the production infrastructure

While consuming production resources for backup purpose the On-Host backup mode disadvantages can be mitigated by the following guidelines.

- **Spreading load across hypervisors.** It should be kept in mind that the backup load, instead of being carried by a limited number of dedicated proxies, will be spread through all the hypervisors. Default Veeam setting is to limit backup to 4 parallel tasks per hypervisor, which will use a maximum of four cores and 8 GB of RAM. This can be modified in the “Managed server” section of the Veeam Console, through the “Task limit” setting. For example the calculation results in a total amount of 24 cores and 48 GB of RAM needed for Veeam transport services, and the infrastructure comprises 12 Hyper-V servers, each server task limit can be set to 2.



text

- **Leveraging storage latency control.** This feature allows to protect the volumes (globally for enterprise edition, and individually for enterprise plus edition) from high latency, by monitoring and adjusting backup load accordingly. Please refer to [user guide](#) proper section for further information.

1.66 Change block tracking on Hyper-V

Depending on the combination of Hyper-V OS version and the primary storage type, the mechanism for tracking changes may differ.

1.66.1 Microsoft Resilient Change Tracking in Hyper-V 2016

Before version 2016, Microsoft did not offer native change block tracking leading Veeam to develop a private CBT engine to drastically optimize backups process. In version 2016 of Hyper-V, Microsoft has implemented its own changed block tracking mechanism, named “Resilient Change Tracking”. To benefit RCT, the following prerequisites must be met, otherwise incremental backups or replication will have to read entirely the source virtual disks to recalculate differences:

- Hyper-V server version 2016
- Cluster functional level is upgraded to 2016

- VM configuration version is upgraded to 8.0

1.66.2 Change block tracking on third party SMB implementation

Since Veeam own Change Block Tracking filter driver is not compatible with third party SMB implementations (as sometimes implemented on hyper converged infrastructures) it is advised to upgrade the cluster nodes to Hyper-V 2016 to leverage Microsoft native RCT in such situations.

1.66.3 Mixed clusters and Change Block Tracking

As migrating Hyper-V clusters from 2012 R2 to 2016 can be done using the “rolling procedure” a Hyper-V cluster might temporary run different versions, impacting the CBT mechanism usage. Be aware that the transition time should be limited to days, during updating the cluster to 2016.

Hosts OS\VM Level\Cluster Level\CBT\	1	2	3	4	5	6	7	8	9	10
All 2012 R2\lower than 8\lower than 9\Veeam filter driver\										
Mixed\Lower or equal to 8\Lower than 9\No CBT\										
All 2016\Lower than 8\Equal to 9\No CBT\										
All 2016\Equal to 8\Equal to 9\Microsoft RCT\										

1.67 Backup of Microsoft S2D hyper converged cluster

For Storage Spaces direct (S2D) Clusters only On-Host proxy mode is available because of the local storage used by S2D.

When configuring a hyper converged infrastructure based on Microsoft Storage Spaces Direct one limitation to know about is that a volume (CSV) hosting virtual machines is owned by a single node of the cluster at a given time. This implies that all IOs (including backup workload generated by all nodes) will be served by the single node owning the volume.

A good rule of thumb to avoid such potential bottleneck is to create a number of volumes (CSV) equal or 2 times greater than the number of nodes composing the cluster, spreading IOs servicing across all nodes.

1.68 Guest interaction

1.68.1 PowerShell Direct

Introduced by Microsoft in Hyper-V 2016, PowerShell Direct is a new method allowing to interact with the guest even if no direct network connection is available between the Veeam guest interaction proxy and the guest itself.

PowerShell Direct requires the following prerequisites:

- PowerShell 2.0 or later
- Host must be Windows Server 2016
- Guest must be Windows Server 2016 or Windows 10

PowerShell Direct can be easily tested on the host, using the following command.

```
Enter-PSSession -VMName VMName
```

1.68.2 Linux Integration Services and application awareness issue##

It has sometimes been observed that some Built-in Linux Integration Services versions failed to communicate the guest IP address to the Hypervisor, causing the Veeam application aware processing to fail.

Please refer to the following Technet [blogpost](#) for further explanations on where to find and how to install LIS.

1.69 Guest restoration

1.69.1 Instant VM recovery storage requirement

When performing [Instant VM recovery](#), Veeam will immediately pre-allocate the necessary amount of storage on the target infrastructure, even though the guest image used is residing on the backup repository.

Note : this pre-allocation is performed only for Instant VM Recovery Usage. Sure Backup processing will use a thin provisioning mechanism instead, preserving resources on the infrastructure.

Note : Instant VM recovery, will send Data over the production (DNS aware) network. During “recover to production” the preferred network are not used for data traffic. The recommendation based on fast Instant VM recovery and reover to production will be in a fast network for the Hyper-V parent partition.

1.70 Job Configuration

In the following section, you will learn more about configuration guidelines for different job types, and how to optimize both the user experience of using Backup & Replication, and the backend operations to get the most of the available infrastructure.

1.71 Backup Methods

Veeam Backup & Replication stores backups on disk using a simple, self-contained file based approach. However, there are several methods to create and store those files on the file system. This section will provide an overview of these methods, their pros and cons, as well as recommendations on use cases for each one.

Backup mode directly influences disk I/O on both production storage and backup repository, and backups size; for these reasons it is recommended to carefully review capabilities of the destination storage when selecting one. Take a look at [Deduplication Appliances](#) section of this guide for important details on using dedicated deduplicating hardware appliances for storing backups.

For a graphical representation of the mentioned backup modes in this section, please see [Veeam KB1799](#).

As a generic overview for I/O impact of the backup modes, please see this table:

Method	I/O impact on destination storage
Forward incremental	1\$times\$ write I/O for incremental backup size
Forward incremental, active full	1\$times\$ write I/O for total full backup size
Forward incremental, transform	2\$times\$ I/O (1x read, 1x write) for incremental backup size
Forward incremental, synthetic full	2\$times\$ I/O (1x read, 1x write) for entire backup chain
Reversed incremental	3\$times\$ I/O (1x read, 2x write) for incremental backup size
Synthetic full with transform to rollbacks	4\$times\$ I/O (2x read, 2x write) for entire backup chain

While changing backup mode is one way of reducing amount of I/O on backup repository it is also possible to leverage features of the filesystem to avoid extra I/O. Currently Veeam Backup and Replication supports advanced features of one filesystem, Microsoft ReFS 3.1 (available in Windows Server 2016), to completely eliminate unnecessary

read/write operations in certain configurations. For more details refer to the corresponding section of this guide.
[ReFS chapter is working in progress]

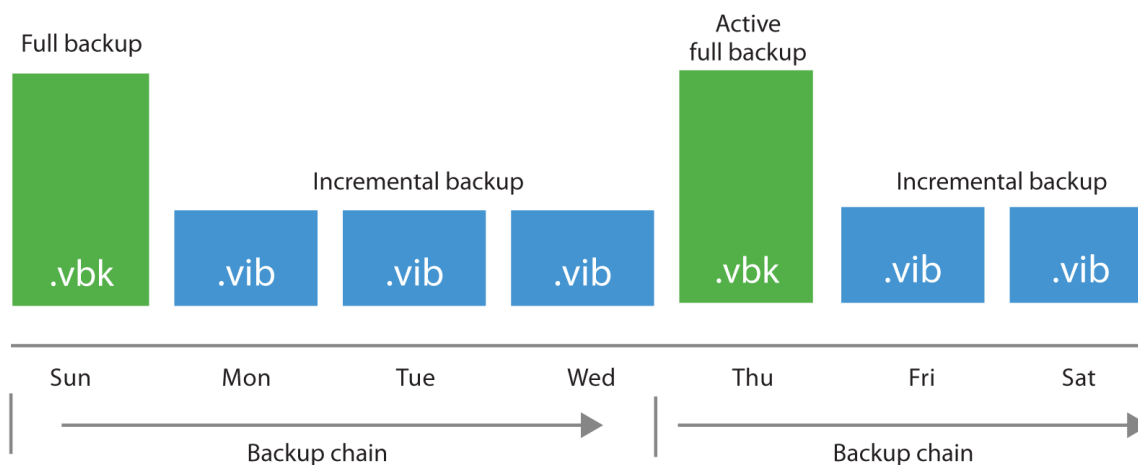
1.71.1 Forward Incremental

The forward incremental backup method is the simplest and easiest to understand; it generally works well with all storage devices although it requires more storage space than other backup methods due to the fact that it requires the creation of periodic full backups (either using active or synthetic backups), typically scheduled weekly. This is necessary because the incremental backups are dependent on the initial full backup; thus, older full backups cannot be removed from the retention chain until a newer backup chain is created. When a new full backup is created, a new chain is started, and the old backups can be removed once the new chain meets the retention requirements.

Active Full Backups

The first time a job is run it always performs an active full backup. During this process the VM is read in full (with the exception of blank blocks and swap areas), and VM data is stored (typically compressed and deduplicated) into a full backup file (.VBK).

Each time an active full is performed (either on schedule or by manually triggering the Active Full command), a new .VBK file is created by reading all data from the production storage. Following incremental backups are stored in incremental backup files (.VIB).



When performing active full backups, all blocks are re-read from the source storage.

I/O Impact of Active Full

When creating an active full, the I/O pattern on the backup storage is mainly sequential writes, which generally provides good performance for most storage solutions. However, all the data (not just the changes) has to be copied from the production storage, and this will increase the duration of the backup activity and the time a VM snapshot remains open (see also the “[Impact of Snapshot Operations](#)” section of this guide). The snapshot lifetime can be reduced by leveraging *Backup from Storage Snapshots*.

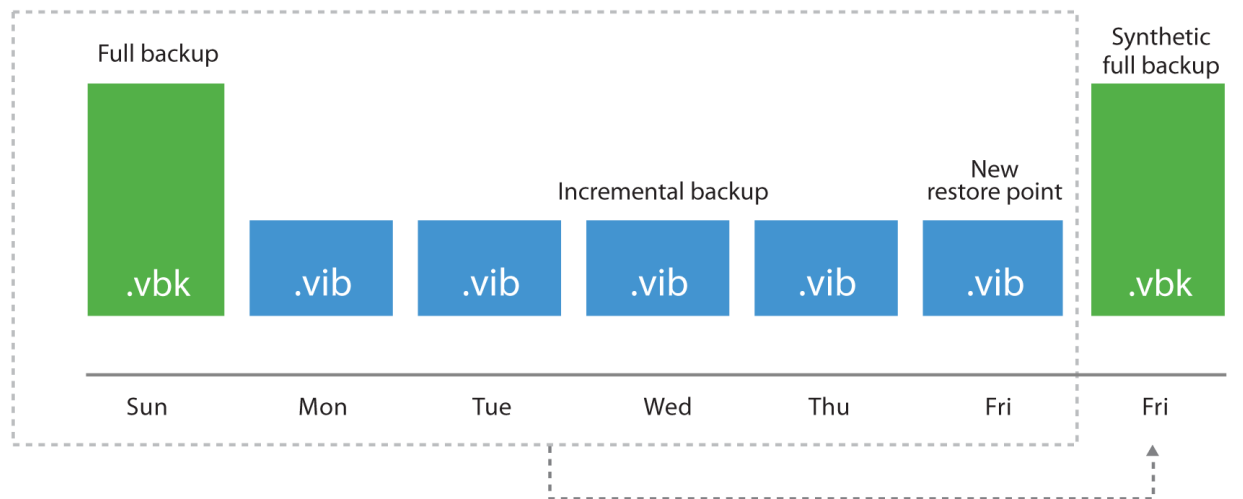
When to use

Forward incremental backup provides good performance with almost any storage and the highest level of backup chain consistency since each new chain is populated by re-reading VM source data. Incremental backups are still processed using Changed Block Tracking (CBT) thus data reduction is still possible. Active Full can be used in any case where plenty of repository space is available, the backup window allows enough time and network bandwidth is sufficient to support reading the source data in full.

| Use | Don't Use | | ————— | | Recommended for deduplication appliances that use SMB or NFS protocols. | When backup window does not allow enough time for re-reading all of the source VM data. | | On storage systems that use software or non-caching RAID hardware such as many low-end NAS devices. | For large or performance sensitive VMs where re-reading the data can have a negative impact on the VMs performance. |

Synthetic Full

Synthetic full reads the data already stored in the most recent backup chain (full and its dependent incrementals) to create a new full backup directly into the destination storage.



If a synthetic full is scheduled, when the job runs, it first creates a normal incremental backup to collect the most recent changes.

After the job completes the incremental backup, the synthetic full generation is started. It reads the most recent version of each block for every VM in the job from the backup chain, and writes those blocks into a new VBK file. This is how a new full backup is “synthetically” created.

I/O Impact of Synthetic Full

Synthetic full I/O patterns need to be split into two different operation: the creation of the additional incremental is exactly like any other incremental job. However, the synthetic creation of the full backup is an I/O intensive process, all in charge of the Veeam repository. Since the process reads individual blocks from the various files in the chain and writes those blocks to the full backup file, the I/O pattern is roughly 50%-50% read/write mix. The processing speed is limited by the IOPS and latency capabilities of the repository storage, so it may take a significant amount of time. However, there is no impact on the source storage or production networks during this time as I/O occurs only inside the repository.

NOTE: if an SMB share type of repository is used, the Veeam repository role is executed in the [Gateway Server](#) there is going to be network traffic between the gateway server itself and the SMB share.

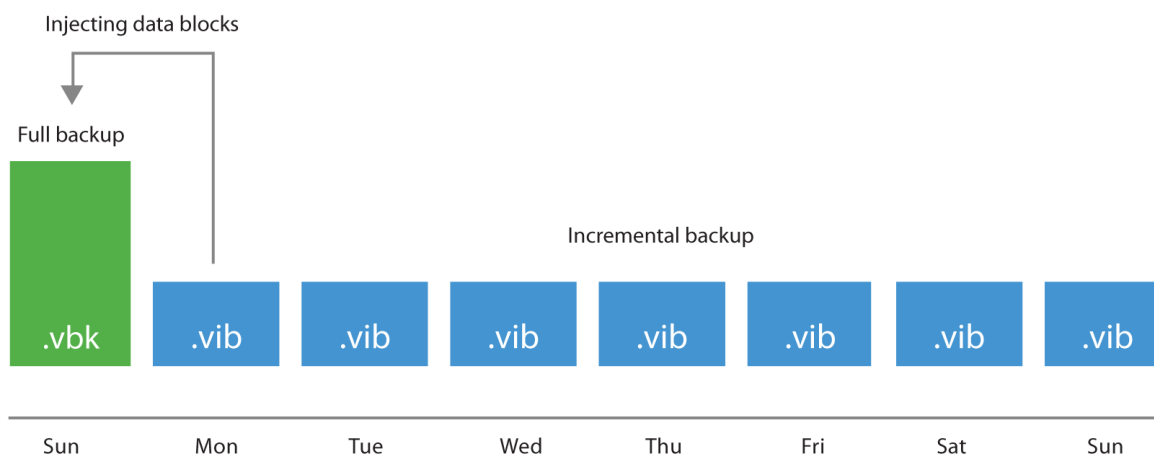
Recommendations on Usage

Due to the way synthetic full works, having many smaller backups jobs with fewer VMs will allow for faster synthetic full operations. Keep this in mind when setting up jobs that will use this method or choose to use *Per VM Backup Files*.

| Use | Don't Use | | _____ |
 _____ || When repository storage uses fast disks with caching RAID controllers and large stripes. | Small NAS boxes with limited spindles that depend on software RAID. || Deduplication appliances that support offloading synthetic operations (DataDomain, StoreOnce and ExaGrid) | Deduplication appliances that use SMB or NFS protocols. |

1.71.2 Forever Forward Incremental

Forever forward incremental method creates one full backup file (VBK) on the first execution, and then only incremental backups (VIBs) are created. This method allows backup space to be utilized efficiently, as there is only a single full backup on disk, and when the desired retention is reached a merge process is initiated. It reads the oldest incremental backup and writes its content inside the full file, virtually moving it forward in the timeline where the merged incremental was before.



I/O Impact of Merge Process

The merging process is performed at the end of the backup job once the retention for the job has been reached. This process will read the blocks from the oldest incremental backup (VIB file) and write those blocks into the VBK file; the I/O pattern is a 50%-50% read-write mix on the target storage. The time required to perform the merge depends on the size of the incremental data and the random I/O performance of the underlying storage.

Recommendations on Usage

The primary advantage of using forever forward incremental backup method is space savings. However, the tradeoff is the required resources for the merge process. The merge process may take a considerable amount of time, depending

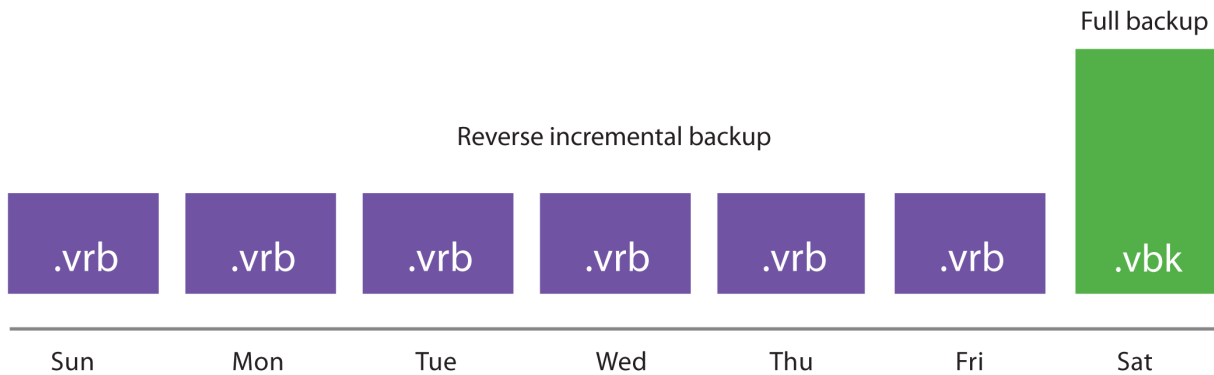
on the amount of incremental changes that the job has to process. The advantage is that the merge process impacts only the target storage.

Like with synthetic full, it is recommended to have many smaller jobs with a limited number of VMs, as this can significantly increase the performance of synthetic merge process. Very large jobs can experience significant increase in time due to extra metadata processing. This may be remediated by combining forever forward incremental mode with *per VM backup files*.

| Use | Don't Use | | _____ | _____ | |
 Repositories with good performance | Smaller backup repositories or NAS devices with limited spindles and cache | |
 Ideal for VMs with low change rate | Jobs with significant change rate may take a long time to merge |

1.71.3 Reverse Incremental

As every other backup method, during its first run reverse incremental backup creates a full backup file (VBK). All subsequent backups are incremental, that is, only changed data blocks are copied. During the incremental backup, updated blocks are written directly into the full backup file, while replaced blocks are taken out and written into a rollback file (.VRB).



This method provides space-efficient backup, as there is only one full backup to store. It also facilitates retention, since removing old restore points is simply a matter of deleting old VRB files.

The disadvantage is that creation of rollback files occurs during the backup process itself, which results in higher I/O load on the target storage and can slow down the backup process.

Also, over time the in-place injection of new blocks into the full file causes fragmentation of the VBK file. This can be partially fixed by using compact operations.

I/O Impact of Reverse Incremental

During the backup process new blocks are read from the source VM and are written directly to the VBK file. If this block replaces an existing older block, this old block is read from the VBK and then written to the VRB file, and replaced by the new one into the VBK file itself. This means that reverse incremental backups creates a 33%-66% read-write IO pattern on the target storage during the backup process itself. This I/O typically becomes the limiting factor for backup performance of the job. As the rollback is created during the backup process itself, backup throughput can be limited by target storage. This slower performance can lead to VM snapshots staying open for a longer time.

This can be especially noticeable for VMs with a high change rate, or when running multiple concurrent jobs.

Recommendations on Usage

Use	Don't Use		
RAID controllers and large stripe sizes	Small NAS boxes with limited I/O performance		When repository storage uses fast disk with caching
Deduplication appliances due to random I/O pattern			VMs with low change rate
			High change rate VMs, as VM snapshot may be open for a long time

1.72 Encryption

1.72.1 Overview

The encryption technology in Veeam Backup & Replication allows you to protect data both while it is in transfer between backup components and at rest, when it is stored at its final destination. This can be disk, tape or a cloud repository. Customers can use one of the encryption methods or a combination of both to protect against unauthorized access to important data through all the steps in the data protection process.

Veeam Backup Enterprise Manager additionally provides Password Loss Protection option that allows authorized Veeam users to recover data from the backup even if the encryption password is lost. If the password gets lost, the backup server will provide a challenge key for Enterprise Manager. Using asymmetric encryption with a public/private key pair, Enterprise Manager generates a response which the backup server can use for unlocking the backup file without having the password available. For more details on this feature refer to the [corresponding section](#) of the User Guide.

The encryption algorithms used are industry standard in all cases, leveraging AES-256 and public key encryption methods. [Data Encryption](#) section of the User Guide provides detailed information on the encryption algorithms and standards used by the product.

The following sections describe encryption options available in the product, what they protect, when they should be used and best practices for their use.

1.72.2 Backup and Backup Copy Job Encryption

What does it do?

Backup and backup copy job encryption is designed to protect data at rest. These settings protect data if unauthorized user gets access to backup files outside of the backup infrastructure. Authorized users of the Veeam console do not need to know the password to restore data from encrypted backups. Encryption does not prevent authorized Veeam users from being able to access data stored in backups.

An example is the use of rotated drives for an offsite repository. Because these drives are rotated offsite, they are at a higher risk of falling into the hands of unauthorized users. Without encryption enabled, these unauthorized users could install their own copy of Veeam Backup & Replication and gain access to the stored backups easily.

On the other hand, if the backup files are encrypted, unauthorized users cannot access any data in the backups or even learn any critical information about the backup infrastructure as even backup metadata is encrypted. Without the key used for encryption or access to the original Veeam Backup & Replication console itself, the backup files remain secure.

How does it work?

For encryption functionality to work backup encryption keys have to be generated. Those keys use mathematical symmetric cryptography and are not used to encrypt the data itself to avoid impacting backup performance. Instead,

for each backup session a unique session symmetric encryption key is generated automatically and then stored in the backup file encrypted with the backup encryption key. Then each data block (compressed or not depending on the job configuration) is encrypted using the session key previously generated for the current job session and stored in the backup file. In case Password Loss Protection functionality is enabled an additional copy of session keys is stored in the backup file encrypted with the Enterprise Manager encryption keys.

This approach provides a method for encrypting backups without compromising backup performance.

When to use it?

Backup and backup copy job encryption should be used if backups are transported offsite, or if unauthorized users may easily gain access to backup files in another way than by using the Veeam console. Common scenarios are:

- Offsite backups to a repository using rotated drives
- Offsite backups using unencrypted tapes
- Offsite backups to a Veeam Cloud Connect provider
- Regulatory or policy based requirements to store backups in encrypted form

Active full backup is required for enabling encryption to take effect if it was disabled for the job previously.

Best Practices

- Enable encryption if you plan to store backups in locations outside of your security domain.
- While CPU usage for encryption is minimal for most modern processors, some amount of resources will still be consumed. If Veeam backup proxies are already highly loaded, take it into account prior to enabling job-level encryption.
- Use strong passwords for job encryption and develop a policy for changing them regularly. Veeam Backup & Replication helps with this, as it tracks passwords' age.
- Store passwords in a secure location.
- Obtain Enterprise or a higher level license for Veeam Backup & Replication, configure Veeam Backup Enterprise Manager and connect backup servers to it to enable Password Loss Protection.
- Export a copy of the active keyset from Enterprise Manager (see [User Guide](#) for more information).
- Back up the Veeam Backup Enterprise Manager configuration database and create an image-level backup of the Veeam Backup Enterprise Manager server. If these backups are also encrypted, make sure that passwords are not lost as there will be no Password Loss Protection for these backups.

1.72.3 Tape Job Encryption

What does it do?

Similar to backup job encryption, tape job encryption is designed to protect data at rest. These settings protect data if an unauthorized user gains access to tape media outside of the backup infrastructure. Authorized users do not need to know the password to restore data from encrypted tape backups. Encryption does not prevent authorized Veeam users from being able to access data stored in tape backups.

Typical use case is to protect data on tapes when media is shipped to an offsite location or to a 3rd party. Without encryption enabled, a lost tape could easily be accessed, and data stored on tapes could be compromised.

How does it work?

Similar to encryption for backups on disk, a session encryption key is used to encrypt data blocks as they are written to tape. Tape encryption can leverage either hardware tape encryption (if present and enabled) or software-based encryption. If the tape drive supports hardware encryption, the session key is sent to the tape device via SCSI commands and the drive itself performs the encryption prior to writing data to tape. This allows encryption to occur with no impact on the CPU of the tape server. If the tape hardware does not support encryption, Veeam falls back automatically to using software-based AES-256 data encryption prior to sending data to the tape device.

When to use it?

Tape job encryption should be used any time you want to protect the data stored on tape from unauthorized access by a 3rd party. Tapes are commonly transported offsite and thus have a higher chance of being lost and turning up in unexpected places. Encrypting tapes can provide an additional layer of protection if tapes are lost.

If tape jobs are writing already encrypted data to tape (for example, Veeam data from backup jobs that already have encryption enabled), you may find it acceptable to not use tape-level encryption. However, be aware that a user who gets access to the tape will be able to restore the backup files. Although this user will not be able to access the backup data in those files, some valuable information, for example, job names used for backup files, may leak.

Best Practices

- Enable encryption if you plan to store tapes in locations outside of your security domain.
- Consider the risks/benefits of enabling tape job encryption even if the source data is already encrypted and evaluate appropriately the acceptable level of risk.
- Use strong passwords for tape job encryption and develop a policy for changing them regularly (you can use Veeam Backup & Replication password age tracking capability).
- Store passwords in a secure location.
- Obtain Enterprise or a higher level license for Veeam Backup & Replication, configure Veeam Backup Enterprise Manager and connect backup servers to it to enable Password Loss Protection.
- Back up the Veeam Backup Enterprise Manager configuration database and create an image-level backup of the Veeam Backup Enterprise Manager server. If these backups are also encrypted, make sure that passwords are not lost as there will be no Password Loss Protection for these backups.

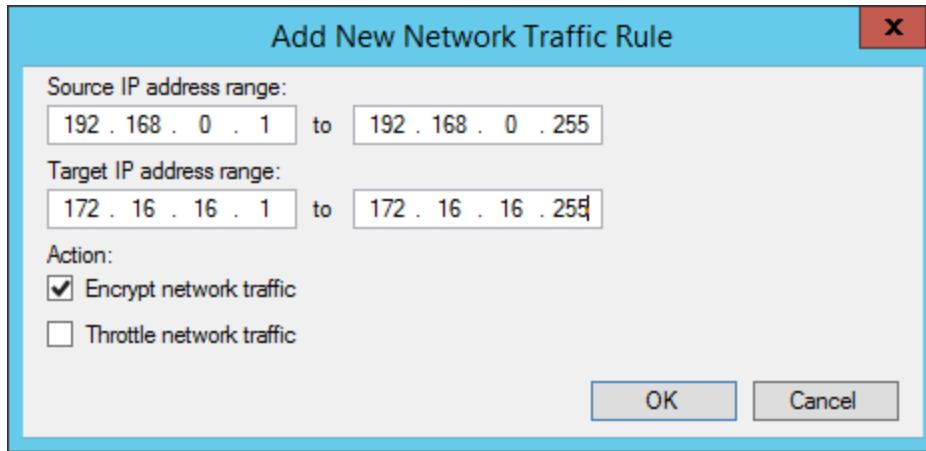
1.72.4 Network Transport Encryption

What does it do?

Unlike the backup and tape job encryption features, the network transport encryption feature is designed to protect data “in-flight”. For example, when the proxy is sending data across the network to the backup repository, data can be encrypted between these two points even if job-level encryption is not enabled. This is primarily useful when the network between the source and target is not trusted, for example, when sending data across the Internet.

How does it work?

Network encryption in Veeam Backup & Replication is controlled via the global Network Traffic options.



Network Traffic Encryption

Whenever two backup infrastructure components need to communicate with each other over the IP network, a dynamic key is generated by the backup server and communicated to each node over a secure channel. The two components then establish an encrypted connection between each other using this key, and all communications between these two components for that session are then encrypted with this key. The key has a one-time use and it's discarded once the session is completed.

When to use it?

Network transport encryption should be used if the network between two backup infrastructure components is untrusted or if the user desires to protect Veeam traffic across the network from potential network sniffing or “man in the middle” attacks.

By default, Veeam Backup & Replication automatically encrypts communication between two nodes if either one or both has an interface configured (if used or not) that is not within the RFC1918 private address space (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 169.254.0.0/16). Veeam also automatically uses network-level encryption for any connection with Veeam Cloud Connect service providers. However, Cloud Connect establishes a TLS 1.2 encrypted tunnel to the service provider in a different way. To learn more about specific Cloud Connect encryption mechanism, watch this YouTube video: [How Veeam Cloud Connect Encryption works](#).

Best Practices

- Enable encryption if network-level attacks are a security concern.
- Network-level encryption can use significant CPU resources, especially on the encrypting side (source) of the connection. Make sure that component nodes have enough resources. Modern CPU's can offload encryption and reduce the amount of CPU resources required. For Intel CPU's specifically, you may check your CPU model on [Intel ARK](#) and look for the [AES-NI](#) capability.
- Use network-level encryption only where required. If backup infrastructure components are running on a network that is using non-RFC1918 IP addresses but is still private and secure from attacks, consider using the following registry key to disable automatic network-layer encryption.
 - Path: HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication
 - Key: DisablePublicIPTrafficEncryption
 - Type: REG_DWORD
 - Value: 1 (default: 0)

1.73 Deduplication and Compression

1.73.1 Storage Optimization Overview

Veeam Backup & Replication takes advantage of multiple techniques for optimizing the size of stored backups, primarily compression and deduplication. The main goal of these techniques is to strike the correct balance between the amount of data read and transferred during backup as well as what is stored on the backup target while providing acceptable backup and restore performance. Veeam Backup & Replication attempts to use reasonable defaults based on various factors but there can be cases when leveraging settings other than default might be valuable.

1.73.2 Deduplication

What does it do?

The primary purpose of deduplication is to reduce the amount of data that has to be stored on disk by detecting redundant data within the backup and storing it only once. Veeam deduplication is based on identifying duplicate blocks inside a single VM disk or across multiple VMs inside the same job. This is primarily beneficial when VMs are deployed from the same template since the base image is identical, but it's less useful for incremental data.

How does it work?

Deduplication is performed both by the source proxy (only for virtual disk currently being processed) and the target repository. Target repository deduplication is applied only to blocks belonging to the same backup chain so its efficiency depends on whether *per-VM chains* are enabled or not. In the case of per-VM chains, only virtual disks belonging to the same VM will be deduplicated, while for regular chains virtual disks of all VMs in the same job will be deduplicated.

Veeam offers 4 different storage optimization settings that impact the size of read blocks and hash calculations for deduplication:

- **Local** – this is the default setting and is recommended when using a disk-based repository. When this setting is selected, Veeam reads data and calculates hashes in 1 MB chunks.
- **LAN** – this value is recommended when using a file-based repository such as SMB shares. When this setting is selected, Veeam reads data and calculates hashes in 512 KB chunks.
- **WAN** – this value is recommended when backing up directly over a slow link or for replication as it creates the smallest backups files at the cost of memory and backup performance. When this setting is selected, Veeam reads data and calculates hashes in 256 KB chunks.
- **Local (>16 TB)** – this setting is recommended for large backup jobs with more than 16 TB of source data in the job. When this setting is selected, Veeam reads data hashes and calculates data on 4 MB blocks.

The smaller the block size, the more CPU will be consumed for hash calculations and the more RAM will be used to store those hashes.

Note: Local (>16TB) underlying block size has changed in v9.0 from 8 MB to 4 MB. If you upgrade to Veeam Backup & Replication v9.0 from a previous version, this option will be displayed as “Local Target (legacy 8MB block size)” in the list and will still use the 8 MB blocks size. It is recommended that you switch to an option that uses a smaller block size and create an active full backup to apply the new setting.

When to use it?

Veeam deduplication should be enabled in almost all cases, *except* when backing up to deduplication devices. Disabling in-line deduplication in such cases significantly increases restore performance.

However, there are a few special cases where a user might consider disabling this option:

- **Large compressed or deduplicated source VMs** – when backing up VMs, especially large VMs (>1 TB) that contain already compressed data (images, video, Windows deduplicated file servers, etc), it may be beneficial to simply disable Veeam deduplication since it is unlikely to gain additional space savings for this type of source data. Note that Veeam deduplication is a job-level setting so VMs of the same type should be grouped and processed within the same job.

When do I change the defaults?

As a rule, the default settings provided by Veeam are designed to provide a good balance between backup size and backup and restore performance and resource usage during the backup process. However, given an abundance of processing resources or other specifics of the environment, it might be useful to change the defaults for a particular job.

For example, transactional servers like Microsoft Exchange and Microsoft SQL commonly make small changes across the disk. If you use the 1 MB blocks setting, this can lead to a great amount of incremental changes each day. The WAN optimization with its smaller block size of 256 KB may significantly decrease the size of incremental backups. However, this can have a very significant impact on the backup speed and the amount of memory needed during the backup process on the repository, especially for large backup jobs.

A 2 TB Microsoft Exchange server may need only 2 GB of RAM on the repository during backup when using default settings of Local (1 MB) blocks, but would potentially need 8 GB of RAM on the repository with WAN (256 KB) blocks. Also, transform operations such as synthetic full backups, forever forward merge and reverse incremental rollback will require four times the I/O operations compared to the 1 MB block, and this can significantly increase total backup time. All of this must be taken into consideration prior to changing the defaults.

Best practices

- Unless you have a really good understanding of the impact that can cause block size changing, stick to the defaults.
- If you want to change the default block size, be sure to test it well and make sure you have planned appropriately for the extra I/O and memory requirements on the repository.
- When using a block size smaller than the default one for a large server, it is recommended to use a backup mode that does not perform synthetic processing (like forward incremental with scheduled active full).

Setting	Block Size	Maximum recommended job size	LAN	Local	WAN
256 KB	4 TB of source data	1	512 KB	1,024 KB	1
1 MB	16 TB of source data	2	1,024 KB	16 TB of source data	2
4 MB	64 TB of source data	4	4,096 KB	64 TB of source data	4

Note: Block size changes will only become effective after an active full is created.

1.73.3 Compression

What does it do?

The purpose of compression is to reduce the amount of data that has to be transferred across the wire and stored on disk. Veeam Backup & Replication leverages several different compression algorithms that provide various balances

between compression ratios, throughput and the amount of CPU use on the backup proxy. Compression provides maximum effect on space savings in a backup job, so understanding the tradeoffs in these settings can be very important.

How does it work?

Veeam Backup & Replication performs compression on a per-block basis, using the block size selected by the storage optimization settings. The proxy reads each block from the source disk and applies the compression algorithm to the block before transferring it to the repository. This saves network bandwidth between the proxy and repository and allows the repository to store the already compressed block as soon as it receives it.

There are multiple compression options available:

- **None** – this option disables compression for the job. The proxy reads blocks and sends them uncompressed to the repository where they are written to disk as is.
- **Dedupe-friendly** – this option uses the very simple RLE compression algorithm that needs very little CPU. It creates somewhat predictable data patterns, which is useful if users want to leverage 3rd party WAN accelerators with Veeam and/or a deduplication appliance (without the “decompress before storing” setting). This allows the network stream to be moderately compressed while still being effectively cached.
- **Optimal** – this is the default compression used on Veeam jobs that leverages LZ4 compression. It provides typical compression ratios around 2:1 with fairly light CPU overhead. This light CPU overhead allows for excellent throughput with rates up to 150 MB/s per core and even faster decompression rates. This is a most commonly used practice that allows achieving excellent balance between performance and compression savings.
- **High** – this option uses `zlib` compression tuned for low to moderate CPU overhead. This setting provides for around 10% higher compression ratios compared to optimal, but uses over 50% more CPU horsepower with rates up to 100 MB/core. If proxies are not CPU bound, this extra saving may still be very much worth it, especially for larger repositories or if the bandwidth available is less than the 100 MB/s limit (i.e., 1 Gb links or less).
- **Extreme** – this option uses `zlib` compression tuned for high CPU overhead. This setting uses even more CPU and lowers throughput even further to around 50 MB/core, while only typically giving around 3-5% additional savings. It is quite rarely used, however, in cases where bandwidth between the proxy and repository is limited, for example, when you run primary backups directly through WAN links.

When to use it?

Veeam compression should almost always be enabled. However, when using a deduplicating storage system as a repository for storing Veeam backups, it might be desirable to disable Veeam compression at the repository level by using the **Decompress backup data blocks before storing** advanced option in repository configuration.

Enabling compression at the job level, and decompressing once sent to the repository will reduce the traffic between proxy server and backup repository by approximately 50% on average. If proxy and repository runs on the same server, the compression engine is automatically bypassed to prevent spending CPU for applying compression. The uncompressed traffic is sent between local data movers using shared memory instead.

When do I change the defaults?

As a rule, the default settings provided by Veeam are designed to provide a good balance between backup size and backup and restore performance and resource usage during the backup process. However, given an abundance of resources or other specifics of the environment, it might be useful to change the defaults in particular circumstances. For example, if you know that CPU resources are plentiful, and backups are unable to make full use of the CPU due to other bottlenecks (disk/network), it might be worth increasing the compression level.

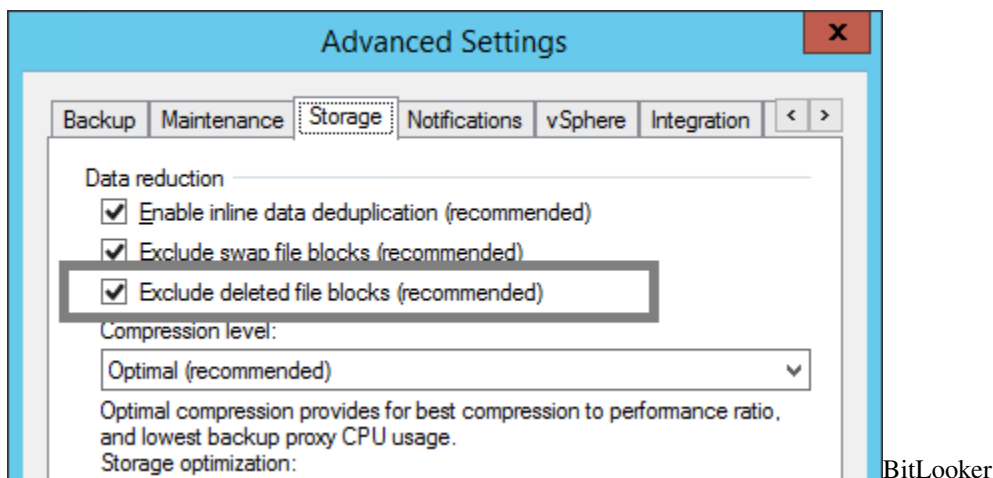
Compression settings can be changed on the job at any time and any new backup sessions will write new blocks with the new compression mode. Old blocks already stored in backups will remain in their existing compression level.

Best Practices

- Defaults are good, don't change values without understanding the impact.
- Use compression levels above optimal only if you have plenty of CPU and understand that maximum throughput, especially during full backups, will likely be significantly lower, especially if the backup proxy CPUs can't take more load.
- Test various compression levels and see how they impact the environment, but always remember the balance. A single backup job with a few concurrent streams may seem fine with **Extreme** compression, but may overload all available proxy CPUs during production run of all jobs.
- Remember that higher compression ratios may also negatively impact restore speeds.

1.73.4 BitLocker

The option "Exclude deleted file blocks" is the third configurable option in job settings. In several places you will see references to this feature under the name "BitLocker".



When enabled, the proxy server will perform inline analysis of the Master File Table (MFT) of NTFS file systems and automatically skip blocks that have been marked as deleted.

When upgrading from versions prior to v9.0, this setting is disabled for existing backup jobs. To enable it for existing jobs, use the following PowerShell commands.

```
Add-PSSnapIn VeeamPSSnapin;

Foreach ($job in Get-VBRJob) {
    $job.Options.ViSourceOptions.DirtyBlocksNullingEnabled = $true;
    $job.SetOptions($job.Options)
}
```

It is always recommended to leave BitLocker enabled, as it will reduce the amount of backup storage space required.

1.74 Backup Job

1.74.1 Job Layout and Object Selection

Veeam Backup and Replication allows you to flexibly select objects to add to the job. At the **Virtual Machines** step of the job wizard, the **Add Objects** screen offers various “views” into the vCenter architecture that match the views provided by the vSphere client. You can switch between the **Hosts and Clusters**, **VMs and Templates**, **Datastores and VMs** or **Tags** views by pressing the appropriate button on the backup object selection screen.

This screen also provides an advanced object exclusion tool that allows you to select a parent object and then exclude child objects, or even individual disks within a VM.

Note When selecting very high level containers with many virtual machines, such as datacenters, clusters or large folders, it is important to keep in mind that tape archive jobs, or SureBackup jobs with linked jobs cannot exclude certain objects from being processed

More guidelines on object selection are listed below.

Important: Veeam Backup and Replication supports encrypted VMs (in vSphere 6.5) but the resulting backups will contain unencrypted data. Thus it is strongly recommended to enable in transit and at rest job level encryption to ensure safety of the data. For more details on requirements and limitations of the backup of encrypted VMs refer to the [corresponding section](#) of the User Guide.

Increasing Deduplication Rate

If the target repository is not configured to use per VM backup files, deduplication across all VMs within a single job is available. When using per VM backup files, deduplication is only available within a single VM backup chain, which reduces its efficiency but still makes it relevant. The following recommendation applies to job level deduplication only.

Grouping VMs running the same operating system or deployed from similar templates into a single job will increase deduplication rate. Job sizing guidelines still apply, and it is recommended to monitor the backup window and the size of the job for manageability.

Container based jobs

Adding resource pools, folders, datastores, or vSphere Tags (vSphere 5.5 and higher) to backup jobs makes backup management easier. New machines that are member of such constructs or containers are automatically included in the backup job, and machines removed from the container are immediately removed from job processing.

When creating jobs based on groups or constructs, ensure that the configured constructs do not overlap. Overlapping constructs may cause undesired results. For instance, when creating jobs based on datastores, VMs with disks residing on multiple datastores included in more than one backup job will cause the VM to be backed up in each job.

Tags

Tags are very convenient for a policy driven approach to data protection. However, it is recommended to follow these guidelines:

- Monitor the number of VMs automatically added to the job to avoid too many VMs being backed up within a single job
- Only one tag can be used to include a VM in a job
- Using tags, you can classify VMs by service levels, using different backup jobs for different service levels

- Veeam ONE Business View (OBV) is a very convenient tool for managing vSphere Tags. OBV allows for creating classification rules and update corresponding tags in vCenter. Classifications can be defined from CPU, RAM, VM naming convention, folder, resource pool, datastore etc. OBV can also import VM/host/datastore descriptions from a CSV file. This feature can be useful when refreshing VMware tags, for example, to update a CMDB.

Exclusions

It is recommended to limit the number of exclusions in backup jobs. While exclusions can be very useful, the virtual infrastructure is dynamic and changes rapidly. It is quite possible that a VM gets moved to a folder or resource pool that is excluded which makes it unprotected. Monitoring [Protected VMs](#) with Veeam ONE is highly recommended.

Also remember that exclusions have higher priority over inclusions in Veeam Backup & Replication.

Compression and Storage Optimization

Detailed descriptions of compression and storage optimization settings and their influence on the backup infrastructure is provided in the [Deduplication and Compression](#) section of this guide. In almost all cases deduplication should be left enabled. Veeam Backup & Replication uses source side deduplication which decreases the amount of data that must be transferred to the target repository.

When using a deduplication appliance for storing backups, please see the [Deduplication Appliances](#) section of this guide for a detailed description of compression and storage optimization settings.

Encryption

A detailed description of encryption settings and its influence on the backup infrastructure is provided in the [Encryption](#) section above in this document.

For general guidelines about encryption, refer to the Veeam User Guide: [Encryption keys](#).

1.74.2 Storage maintenance

While data amount is growing and backup window is decreasing, forward incremental forever backups have become increasingly important in any backup solution. Backup jobs with no scheduled synthetic or active full backups are becoming more widely adopted. Forward incremental with weekly synthetic full backups is however still the default setting.

The two main objections towards using a forever forward incremental backup mode are the following:

The first one is **full backup file fragmentation**, leading to undesired VBK file growth over time, and degradation of performance due to fragmentation. Previously it was recommended to perform periodical active full backups in order to create a new VBK file and backup chain. This would mitigate issues of fragmentation and remove whitespace left by deleted data blocks.

The second objection is **silent storage corruption**. If ever a file or block in the chain got corrupted by a storage related issue, all subsequent consolidations or restores from this could be affected.

To address both objections, following features are available under the “Maintenance” tab, in the Advanced settings of a backup job.

Full backup file maintenance - “Defragment and compacting”

Full backup file maintenance will address two issues: VBK file fragmentation caused by transforms (forward incremental forever or reverse incremental) and left over whitespace from deleted data blocks. These issues are mitigated by synthesizing a new full backup file on the backup repository, i.e. copying blocks from the existing VBK file into a new VBK file, and subsequently deleting the original file. This process may also be referred to as “compacting”.

How does it work? During VBK compacting, a new VBK file is created. Existing blocks are copied from the previous VBK, requiring free space equivalent to the size of an additional full backup in the repository. In the [Restore Point Simulator](#), this space is part of the “Work space” parameter. When using Scale-out Backup Repository in Performance Mode, the compacting process may utilize multiple extents and significantly speed up the compacting process.

When to use? For every backup job with full transforms. Defragmentation will benefit most jobs that are configured to generate a single chain per job, keeping files smaller and restore optimal speed over time.

When to avoid? When using deduplication storage, it is recommended to disable the “Defragment and compact” option. As deduplication appliances are fragmented by their very nature and also have very poor support for random I/O workloads, the compacting feature will not enhance backup or restore performance.

Storage-level corruption guard

In addition to using SureBackup for restore validation, storage-level corruption guard was introduced to provide a greater level of confidence in integrity of the backups.

How does it work? When a job has finished, storage-level corruption guard will perform a CRC verification for the most recent restore point. It will validate whether the contents of the backup chain blocks match the content described within the backup file metadata. If a mismatch is discovered, it will attempt to repair the data block from production storage, assuming the block still exists and has not been overwritten. If it exists, the backup file will be repaired. If not, storage-level corruption guard will fail and make the user aware that a new full backup is required, and that the backup chain must be recovered from a secondary copy of the backup.

When to use? It is recommended to use storage-level corruption guard for any backup job with no active full backups scheduled. Synthetic full backups are still “incremental forever” and may suffer from corruption over time.

When to avoid? It is highly discouraged to use storage-level corruption guard on any storage that performs native “scrubbing” to detect silent data corruptions. Such storage will automatically heal silent data corruptions from parity disks or using erasure coding. This is the case for most deduplication appliances.

For more information, please see Veeam Helpcenter: [Health Check for Backup Files](#).

1.74.3 Job Chaining

Chaining backup jobs is convenient in certain circumstances, but should be used with caution. For example, if a job as part of a chain fails or stops responding, the entire job chain delivers poor backup success rate.

A common way to handle multiple jobs is to let the built-in Intelligent Load Balancing (ILB) handle the proxy/repository resources by starting multiple jobs in parallel and consequently using all available proxy/repository resources. This allows optimal task scheduling and provides the shortest backup window.

1.74.4 Load Balancing

When planning job schedules, you should consider balancing the load on source and target disks. Too many jobs accessing the same disk will load the storage significantly; this makes the job run slower or may have a negative impact on the VMs performance. To mitigate this problem, you can utilize [Storage Latency Control](#) (or Backup I/O Control) settings.

Veeam has a load balancing method that automatically allocates proxy resources making a choice between all proxies managed by Veeam Backup & Replication that are available at the moment.

For more details on load balancing, refer to the Veeam Backup & Replication User Guide at [Resource scheduling](#).

1.74.5 Binding Jobs to Specific Proxies

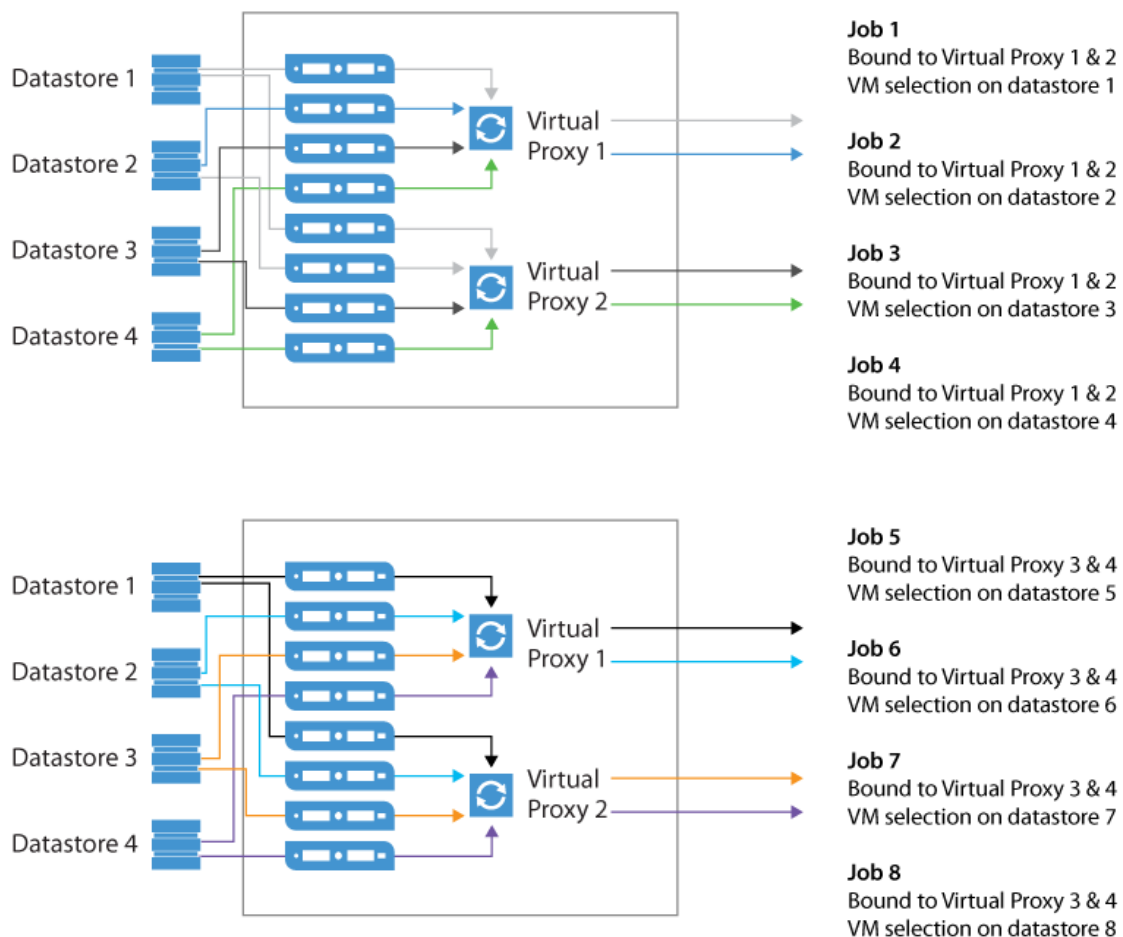
Refer to the User Guide in order to examine the advanced deployment scenario with multiple proxies: [Advanced deployments](#).

While configuring a backup job, you can disable the automatic proxy selection. Instead, you can select particular proxies from the list of proxies managed by Veeam backup server, and assign them to the job. This is a very good way to manage distributed infrastructures; also it helps you to keep performance under control.

For example, you can back up a cluster residing on a multiple blade chassis. In this case, if using virtual proxies, keep the proxies' load well-balanced and optimize the network traffic.

Dedicated proxies can be also very helpful if you use a stretched cluster and do not want proxy traffic to cross over inter-switch links.

See the illustration below as a good starting point to reach and keep control on high backup throughput. In this example, administrator wants to keep network traffic as much as possible inside the chassis; only the proxy-to-repository traffic goes via an external link.



You can use [Proxy Affinity](#) to allow only specific proxies to interact with a given repository.

Tip: To optimize load balancing in a distributed environment where backup proxies are located in multiple sites, it is recommended to select all proxies from the same site in the corresponding job.

1.75 Backup Copy Job

Instead of just copying backup files to a second destination, Veeam uses a more intelligent and secure way of bringing restore points to a second backup target. Backup copy jobs read specific VM restore points from backup files and store them as a new backup file chain on the destination. The second chain is independent from the first chain and adds therefore an additional level of protection. You can store VMs from multiple backup jobs in the same backup copy job, or you can select a subset of VMs from a bigger backup job as source if you do not want to backup all VMs to the backup copy job destination.

Every backup copy job creates its own folder on the target backup repository and stores its data in this location. The folder has the same name as the backup copy job.

Once created, a backup copy job will immediately start processing the latest existing restore point for all VMs included in the job, as long as it has been created less than one synchronization interval before the start of the backup copy job.

By default, Veeam Backup & Replication keeps 7 restore points on the target backup repository in case of simple retention policy (see the “[Simple Retention Policy](#)” section of the User Guide for details). If you plan to use Grandfather-Father-Son (GFS) retention, refer to the “[GFS Retention Policy](#)” section for details.

Backup copy jobs file chains layout will depend on the repository option: “Per VM backup files” will generate one file chain per each VM, otherwise a chain will be generated per each job.

If a backup copy job cannot process all requested VMs before the end of an incremental execution interval (by default 24 hours), the job will still create backup files on the target backup repository for per-vm chains however some VMs could be left inconsistent or in an unprotected state. In the case of non per-vm chains this will fail with an error. This might be caused by precedence of the backup task over the backup copy task. The backup copy process will resume from the last full data transaction during the next synchronization interval.

Limitations of backup copy jobs are described in Veeam Backup & Replication User Guide at https://helpcenter.veeam.com/backup/vsphere/backup_copy_select_point.html.

Important Note: Jobs with WAN acceleration enabled will process VMs sequentially, while jobs using direct mode will process included VMs in parallel according to free task slots availability on backup repositories.

1.75.1 Backup Copy Job Scheduling

By design, a backup copy job is a process that runs continuously. This process includes several stages.

A copy job restarts every time at the defined **Copy every** interval setting (default is 12:00 AM daily) and monitors for new restore points of the selected VMs to appear in the specified sources. On the **Schedule** tab it is possible to define time period when data transfers are allowed. This is especially helpful, when transferring multiple times per day (e.g. hourly synchronization interval), or again when the bandwidth used to transfer the backup copy jobs can only be used during the night.

The concept of the “interval” is used to define two parameters: how often the job should be looking for new points, and for daily intervals at what time it should start looking for points. If you set an interval of 1 day, that equals to instruct the backup copy job that once a day, starting at the selected time, it should begin looking for new restore points. When the restore point is found, the copy job will copy it. However, once a single point is copied, another point for that VM will not be copied until the next interval starts.

The synchronization interval is implemented to provide a policy driven approach to offsite copies. Since the copy job can contain multiple source backup jobs, and most source backup jobs neither start nor complete at the same time, the

synchronization interval is helpful in defining a policy for when it should look for restore points across the included source jobs.

Another reason for this design is that you may run local backups more often (for example, hourly), but you may only want to copy data offsite only daily or weekly, thus you can set the backup copy “interval” independently of the schedule of the backup jobs it is using as source.

The backup copy job has the following phases:

1. **Pre-job activity** — if enabled, the pre-job scripts are executed at the very beginning of a copy interval.
2. **Health check** — if scheduled, backup file integrity is verified before the next copy is initiated.
3. **Data transfer (synchronization) phase** — during this phase, the backup copy job checks for a new restore point in the source, creates a file for a new restore point at the target and starts copying the state of the latest restore point of each processed VM to the target repository. The data transfer (synchronization) phase starts at specific time configured in the job properties (see [Synchronization Intervals](#)). You can define any interval needed in minutes, hours or days. Moreover, you can specify the time slot during which data can and cannot be transferred over the network, thus regulating network usage (see [Backup Copy Window](#)).
4. **Transform phase** — copy jobs are by nature running in “forever forward incremental” mode, and perform transform operations on the target backup repository accordingly. Additionally, it is possible to schedule health checks or backup file compacting as described in the [Backup Job](#) section. The transform phase begins when all VMs are successfully copied to the target, or if the synchronization interval expires.

Note: the transform process itself puts additional pressure on the target repository. In large environments with deduplication storage appliances used as backup repositories or with backup copy jobs processing a large number of VMs or big VMs, the transform process can take a significant amount of time. For non-integrated deduplication appliances, it is recommended to use the “Read entire restore point...” option. This forces the Backup Copy Job to running forward incremental with periodical full backups copied entirely from the source backup repository rather than being synthesized from existing data.

5. **Compact full backups** — if enabled, the recent full backup file is re-created on the same repository, writing all the blocks close to each other as much as possible to reduce fragmentation.
6. **Post-job activity** — if enabled, several post-job activities are executed before the job enters the idle phase, such as post-job scripts and sending e-mail reports.
7. **Idle phase** — for the most time, the backup copy job remains in the *Idle* state, waiting for a new restore point to appear on the source backup repository. When the synchronization interval expires, a new interval starts at step 1.

For more information, refer to the corresponding section of the User Guide > [Backup Copy Job](#).

1.75.2 Job Layout and Object Selection

Source Object Container

- **Select from infrastructure:** this selects specific VMs or containers from the virtual infrastructure. The scheduler will look for the most recent restore point containing the VMs within the synchronization interval. The scheduler will look for restore points in all backups, regardless which job generated the restore point. If the restore point is locked (e.g. the backup job creating it is running), the backup copy job waits for the restore point to be unlocked and then start copying the state of the VM restore point according to its defined schedule.
- **Select from job:** this method of selection is very useful if you have multiple backup jobs protecting the same VMs. In this case, you can bind the backup copy job to a specific job you want to copy. The job container will protect all the VMs in the selected source job(s).

- **Select from backup:** this method is equivalent to the **Select from infrastructure** method, but allows for selecting specific VMs inside specific backups. This is helpful, when only certain critical VMs should be copied offsite.

Backup Copy and Tags

As you can select any VM to be copied from multiple backups, you can plan for policy-based configurations. For instance, you may not want to apply GFS retention over some VMs like web servers, DHCP, etc. In this situation, you can use VMware tags to simplify the management of backup copy process. Tags can be easily defined according to the desired backup copy configuration, using VMware vSphere or Veeam ONE Business View to apply tags.

1.75.3 Initial synchronization

When creating the initial copy to the secondary repository, it is recommended to use backup seeding (see [Creating Seed for Backup Copy Job](#)) whenever possible. Especially when transferring large amounts of data over less performant WAN links, the seeding approach can help mitigating initial synchronization issues.

While Backup Copy Jobs were designed for WAN resiliency, the initial copy is more error prone, as it is typically transferring data outside the datacenter over less reliable links (high latency, or packet loss). Another issue that can be solved by seeding is when the full backup is larger than the amount of data that can be transferred in an interval. Even if the interval can be extended to accomodate the initial transfer, this may lead to upload times of even multiple days. Seeding can speed up the initial sync by removing the need for the sync.

The most frequent synchronization issues are described in the User Guide > [Handling Backup Copy Job Issues](#).

1.75.4 Additional Options

Restore Point Lookup

By default, after a restart of the job interval (the **Copy every** setting), a backup copy job analyzes the VM list it has to protect, and searches *backwards in time* for newer restore point states. If the state of the restore point in the target repository is older than the state in the source repository, the new state is transferred.

For example, if the backup job is scheduled to run at 10:20 PM, and the backup copy job uses the default schedule of copying the latest restore point state every day at 10:00 PM, the state copied by the backup copy job is typically one day behind. In the image below, you can see some VMs affected by this behavior.

VMware - Backup Copy to DataDomain	7/17/2016 10:00 PM
demo-AD	8/1/2016 6:17 PM
demo-domino	8/1/2016 6:15 PM
demo-Exchange	8/1/2016 6:14 PM
demo-linux1	7/31/2016 11:51 PM
demo-linux2	8/1/2016 10:25 PM
demo-Oracle	8/1/2016 6:13 PM
demo-SQLandSP	8/1/2016 6:18 PM
demo-sql-ao-db1	8/1/2016 1:02 PM
demo-sql-ao-db2	8/1/2016 6:14 PM
demo-win1	7/31/2016 10:24 PM
demo-win2	7/31/2016 10:24 PM
exchange2013mbx1	8/1/2016 6:16 PM
exchange2013mbx2	8/1/2016 6:14 PM
exchange2013wit1	7/31/2016 10:24 PM

Backup Copy Job - example of

VMs behind schedule

To change this behavior, it is possible to use the `BackupCopyLookForward` registry key as described below. Reevaluating the example above, using this registry key, the backup copy job will still start searching at 10:00 PM, but will now wait for a new restore point state created after this point in time.

- Path: `HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication`
- Key: `BackupCopyLookForward`
- Type: `REG_DWORD`
- Value: `1`

The following forum thread provides a very good explanation of the backup copy scheduler and the `LookForward` registry key > [Veeam Community Forums - Backup Copy Intervals](#)

Backup Copy from Backup Copy

Since v8, it is possible to use a backup copy job as a source for data transfer and to generate another backup copy. For this, select the VMs from infrastructure and specify the backup repository holding the primary backup copy restore points as the source.

Job Seeding

Usually, a backup copy is used to send data remotely. If it is necessary to send data over a slow link, you can seed the backup copy job by taking the following steps:

1. Create a "local" backup copy job and target it at a removable device used as a backup repository, or copy the backup files afterwards. Run the created backup copy job to create a full backup set on this device. Note that also the `.vbm` file has to be moved.
2. Once the backup copy job is over, delete the local backup copy job from the Veeam console.
3. Transport the removable device with the created backup files to the destination site.
4. Copy backup file to the target backup repository.
5. Import the backup on the target. If already imported, perform a rescan.

6. Create the final backup copy job on the Veeam console. On the **Target** step of the **Backup copy job** wizard, use the **Map backup** link and select the transported backup — this backup will be used as a “seed”.

If you are using a WAN accelerated transfer, refer to the WAN Accelerator section for proper cache population procedure: https://helpcenter.veeam.com/backup/vsphere/wan_populate_cache.html.

Note: Only the initial first run of a reverse incremental chain can be used with seeding (but any forward incremental chain can be used). See [kb1856](#) for more information.

1.76 Replication Job

Note: This section focuses on replicating VMs to your own virtual infrastructure. When implementing Cloud Connect replication for DRaaS only source configuration details of this section are relevant to end user side of the deployment. For more information on implementing DRaaS on Cloud Connect provider side refer to the [Cloud Connect Reference Architecture](#) document.

Replication jobs are used to replicate VMs to another or the same virtual environment (instead of creating deduplicated and compressed backup files at a backup run). Veeam can store up to 28 restore points (on VMware platforms).

Like backup, replication is a job-driven process. In many ways, it works similarly to forward incremental backup:

- During the first run of a replication job, Veeam Backup & Replication copies a whole VM image and registers the replicated VM on the target ESXi host. In case of replicating to a cluster, a host with least amount of VMs registered at the moment will be used.
- During subsequent runs, the replication job copies only incremental changes, and creates restore points for the VM replica — so the VM can be recovered to the selected state. Every restore point is in fact a regular VMware snapshot.
- When you perform incremental replication, data blocks that have changed since the last replication cycle are written to the snapshot delta file next to the full VM replica. The number of restore points in the chain depends on the retention policy settings.

Replication infrastructure and process are very similar to those used for backup. They include a source host, a target host with associated data stores, one or two proxy servers and a repository for storing meta data on the source side. The source host and the target host are the two terminal points between which the replicated data is moved.

Replicated data is collected, elaborated and transferred with the help of Veeam data movers. The data movers involved in replication are the source proxy, the target proxy and the repository. The data mover hosted on the repository processes replica metadata files on the source side.

Important! Although the replica data is written to the target datastore, certain replica metadata must be located on a backup repository. This metadata is used by the source proxy and thus should be deployed closer to the source host and therefore no compression/uncompress processing is used.

The replication process involves the following steps:

1. When a new replication session is started, the source-side data mover (proxy task) performs the same operations as in backup process. In addition, in cases when VMware CBT mechanism cannot be used, the source-side data mover interacts with the repository data mover to obtain replica metadata — in order to detect which blocks have changed since the previous job run.
2. The source-side data mover compresses the copied blocks of data and transfers them to the target data mover.
Note: In on-site replication scenarios, the source-side transport service and the target-side transport service may run on the same backup proxy.
3. The target-side data mover uncompresses replica data and writes it to the destination datastore.

Veeam Backup & Replication supports a number of replication scenarios that depend on the location of the target host and will be discussed later in this section.

During replication cycles, Veeam Backup & Replication creates the following files for a VM replica:

- A full VM replica (a set of VM configuration files and virtual disks).

During the first replication cycle, Veeam Backup & Replication copies these files to the selected datastore to the <ReplicaName> folder, and registers a VM replica on the target host.

- Replica restore points (snapshot delta files). During incremental runs, the replication job creates a snapshot delta file in the same folder, next to a full VM replica.
- Replica metadata where replica checksums are stored. Veeam Backup & Replication uses this file to quickly detect changed blocks of data between two replica states. Metadata files are stored on the backup repository (source side).

During the first run of a replication job, Veeam Backup & Replication creates a replica with empty virtual disks on the target datastore. Disks are then populated with data copied from the source side.

To streamline the replication process, you can deploy the backup proxy on a virtual machine. The virtual backup proxy must be registered on an ESXi host with direct connection to the target datastore. In this case, the backup proxy will be able to use the Virtual Appliance (HotAdd) transport mode for writing replica data to target. In case of a NFS datastore at the target location, you can as well use Direct Storage access mode (Direct NFS) to write the data.

If the **Virtual Appliance** mode is applicable, replica virtual disks are mounted to the backup proxy and populated through the ESX I/O stack. This results in increased writing speed and fail-safe replication to ESXi targets. For information on Virtual Appliance mode, see https://helpcenter.veeam.com/docs/backup/vsphere/virtual_appliance.html?ver=95.

If the backup proxy is deployed on a physical server, or the Virtual Appliance or Direct NFS mode cannot be used for other reasons, Veeam Backup & Replication will use the **Network** transport mode to populate replica disk files. For information on the Network mode, see https://helpcenter.veeam.com/docs/backup/vsphere/network_mode.html?ver=95.

<<<<<<< HEAD The Direct SAN mode (as part of Direct Storage Access) can only be used together with replication targets in case of transferring thick-provisioned VM disks at the first replication run. As replication restore points are based on VMware snapshots, that are thin provisioned by definition, Veeam will fail-back to Virtual Appliance (HotAdd) mode or Network mode, if configured at proxy transport settings. Direct SAN mode or backup from storage snapshots can be used on the source side in any scenario.

Note: Veeam Backup and Replication supports replicating VMs residing on VVOLs but VVOLs are not supported as a replication target datastore

Replication of encrypted VMs is supported but comes with requirements and limitations outlined in the **corresponding section** of the User Guide. Replication of encrypted VMs is NOT supported when the target is Veeam Cloud Connect.

If the **Virtual Appliance** mode is applicable, replica virtual disks are mounted to the backup proxy and populated through the ESX I/O stack. This results in increased writing speed and fail-safe replication to ESXi targets. For information on Virtual Appliance mode, see https://helpcenter.veeam.com/backup/vsphere/virtual_appliance.html?ver=95.

If the backup proxy is deployed on a physical server, or the Virtual Appliance or Direct NFS mode cannot be used for other reasons, Veeam Backup & Replication will use the **Network** transport mode to populate replica disk files. For information on the Network mode, see https://helpcenter.veeam.com/backup/vsphere/network_mode.html?ver=95.

The Direct SAN mode (as part of Direct Storage Access) can only be used together with replication targets in case of transferring thick-provisioned VM disks at the first replication run. As replication restore points are based on VMware snapshots, that are thin provisioned by definition, Veeam will failback to Virtual Appliance (HotAdd) mode or Network mode, if configured at proxy transport settings. Direct SAN mode or backup from storage snapshots can be used on the source side in any scenario.

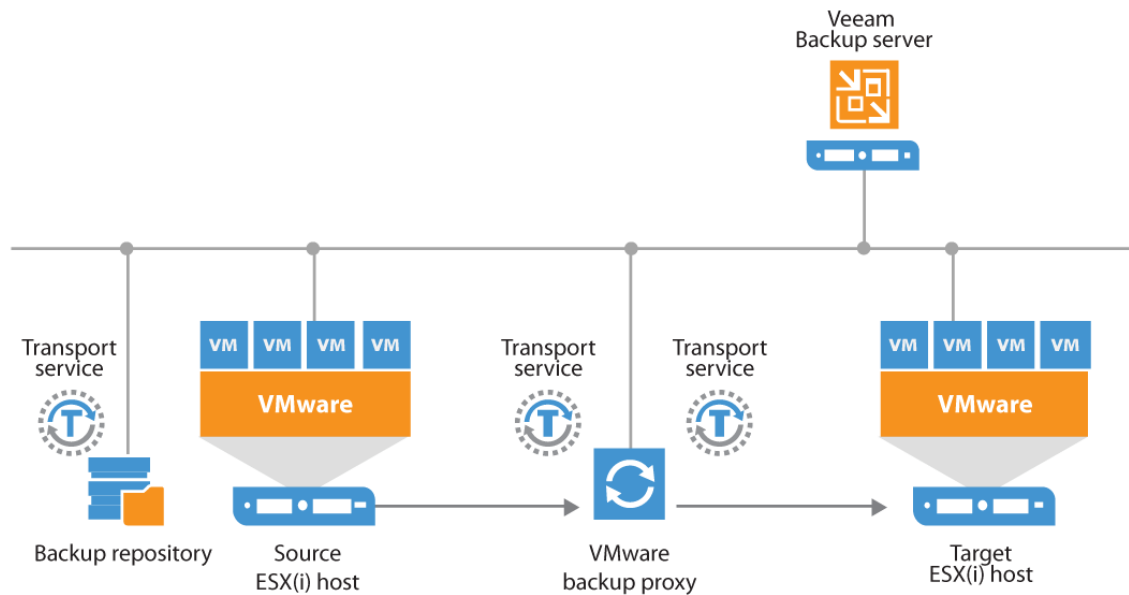
Note: Veeam Backup and Replication supports replicating VMs residing on VVOLs but VVOLs are not supported as replication target datastore.

Note: Replication of encrypted VMs is supported but comes with requirements and limitations outlined in the [corresponding section](#) of the User Guide. Replication of encrypted VMs is NOT supported when the target is Veeam Cloud Connect.

parent of 2492291... Merge branch 'master' into dev

1.76.1 Onsite Replication

If the source and target hosts are located in the same site, you can use one backup proxy for data processing and a backup repository for storing replica metadata. The backup proxy must have access to both hosts, source and target. In this scenario, the source-side data mover and the target-side data mover will be started on the same backup proxy. Replication data will be transferred between these two data movers and will not be compressed.



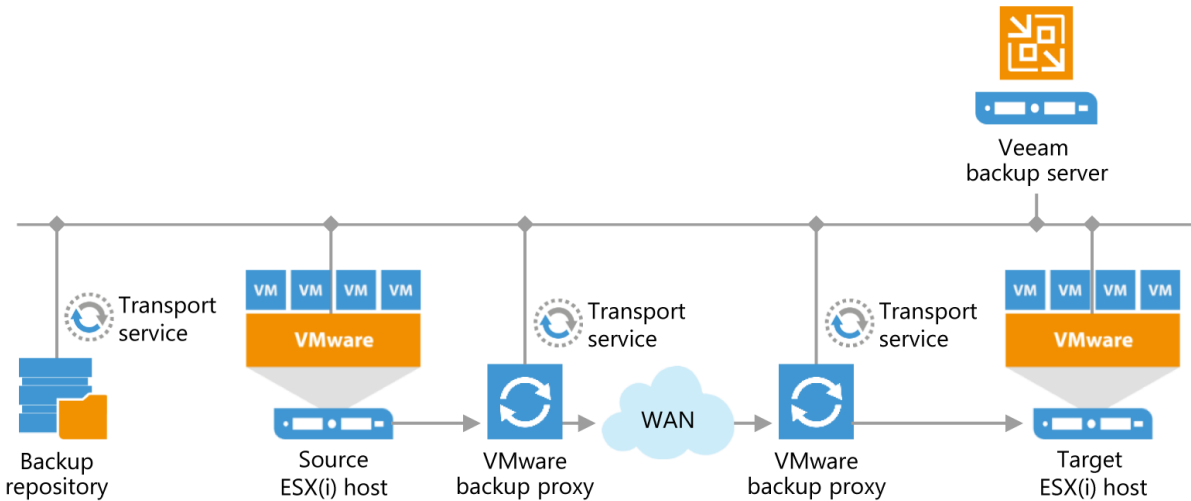
1.76.2 Offsite Replication

The common requirement for offsite replication is that one Veeam data mover runs in the production site (closer to the source host), and another data mover runs in a remote site (closer to the target host). During backup, the data movers maintain a stable connection, which allows for uninterrupted operation over WAN or slow links.

Thus, to replicate across remote sites, deploy at least one local backup proxy in each site:

1. A source backup proxy in the production site.
2. A target backup proxy in the remote site.

The backup repository for meta data must be deployed in the production site, closer to the source backup proxy.



Tip: It is recommended to place a Veeam backup server on the replica target side so that it can perform a failover when the source side is down. When planning off-site replication, consider advanced possibilities — replica seeding, replica mapping and WAN acceleration. These mechanisms reduce the amount of replication traffic while network mapping and re-IP streamline replica configuration.

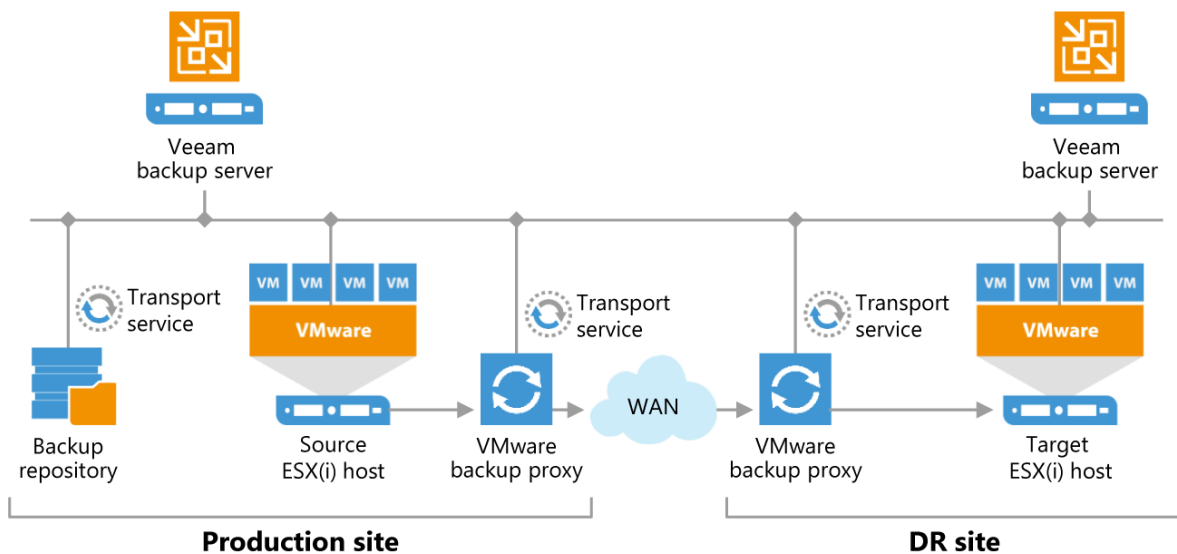
For offsite replication, open the connections between the Veeam backup components:

- The Veeam backup server must have access to the vCenter Server, the ESXi hosts, the source backup proxy and the target backup proxy.
- The source backup proxy must have access to the Veeam backup server, the source ESXi host, backup repository holding the replica metadata, the target proxy, and the source vCenter Server.
- The target backup proxy must have access to the Veeam backup server, the source proxy, the target ESXi host, and the target vCenter Server.

The source proxy compresses data and sends it via the WAN to the target proxy, where the data is uncompressed. Note that you also can seed the replica by sending the backup files offsite (using some external media, for example) and then only synchronise it with incremental job runs.

In this scenario:

- The Veeam backup server in the production site will be responsible for backup jobs (and/or local replication).
- The Veeam backup server in the DR site will control replication from the production site to the DR site.



Thus, in disaster situation, all recovery operations (failover, failback and other) will be performed by the Veeam backup server in the DR site. Additionally, it may be worth installing the Veeam Backup Enterprise Manager to have visibility across the two Veeam backup servers so that you only have to license the source virtual environment once (used from both backup servers)

Tip: Plan for possible failover carefully. DNS and possibly authentication services (Active Directory, for example, or DHCP server if some replicated VMs do not use static addresses) should be implemented redundant across both sides. vCenter Server (and vCD) infrastructure should be as well considered for the failover scenario. In most cases, Veeam does not need a vCenter Server for replica target processing. It can be best practice to add the ESXi hosts from the replica target side (only) directly to Veeam Backup & Replication as managed servers and to perform replication without vCenter Server on the target side. In this scenario a failover can be performed from the Veeam console without a working vCenter Server itself (for example to failover the vCenter Server virtual machine).

Replication bandwidth estimation has always been a challenge, because it depends on multiple factors such as the number and size of VMs, change rate (at least daily, per RPO cycle is ideal), RPO target, replication window. Full information about these factors, however, is rarely at hand. You may try to set up a backup job having the same settings as the replication job and test the bandwidth (as the backup job will transfer the same amount of data as the replication job). **Veeam ONE** (specifically Infrastructure Assessment report packs) may help with estimating change rates and collecting other information about the infrastructure.

Also, when replicating VMs to a remote DR site, you can manage network traffic by applying traffic throttling rules or limiting the number of data transfer connections. See Veeam Backup & Replication User Guide for more information: https://helpcenter.veeam.com/docs/backup/vsphere/setting_network_traffic_throttling.html?ver=95.

Tip: Replication can leverage WAN acceleration allowing a more effective use of the link between the source and remote sites. For more information, see the User Guide https://helpcenter.veeam.com/docs/backup/vsphere/wan_acceleration.html?ver=95 or the present document (the *WAN Acceleration* section above).

Also, when replicating VMs to a remote DR site, you can manage network traffic by applying traffic throttling rules or limiting the number of data transfer connections. See Veeam Backup & Replication User Guide for more information: https://helpcenter.veeam.com/backup/vsphere/setting_network_traffic_throttling.html?ver=95.

Tip: Replication can leverage WAN acceleration allowing a more effective use of the link between the source and remote sites. For more information, see the User Guide https://helpcenter.veeam.com/docs/backup/vsphere/wan_acceleration.html?ver=95 or the present document (the “WAN Acceleration” section above).

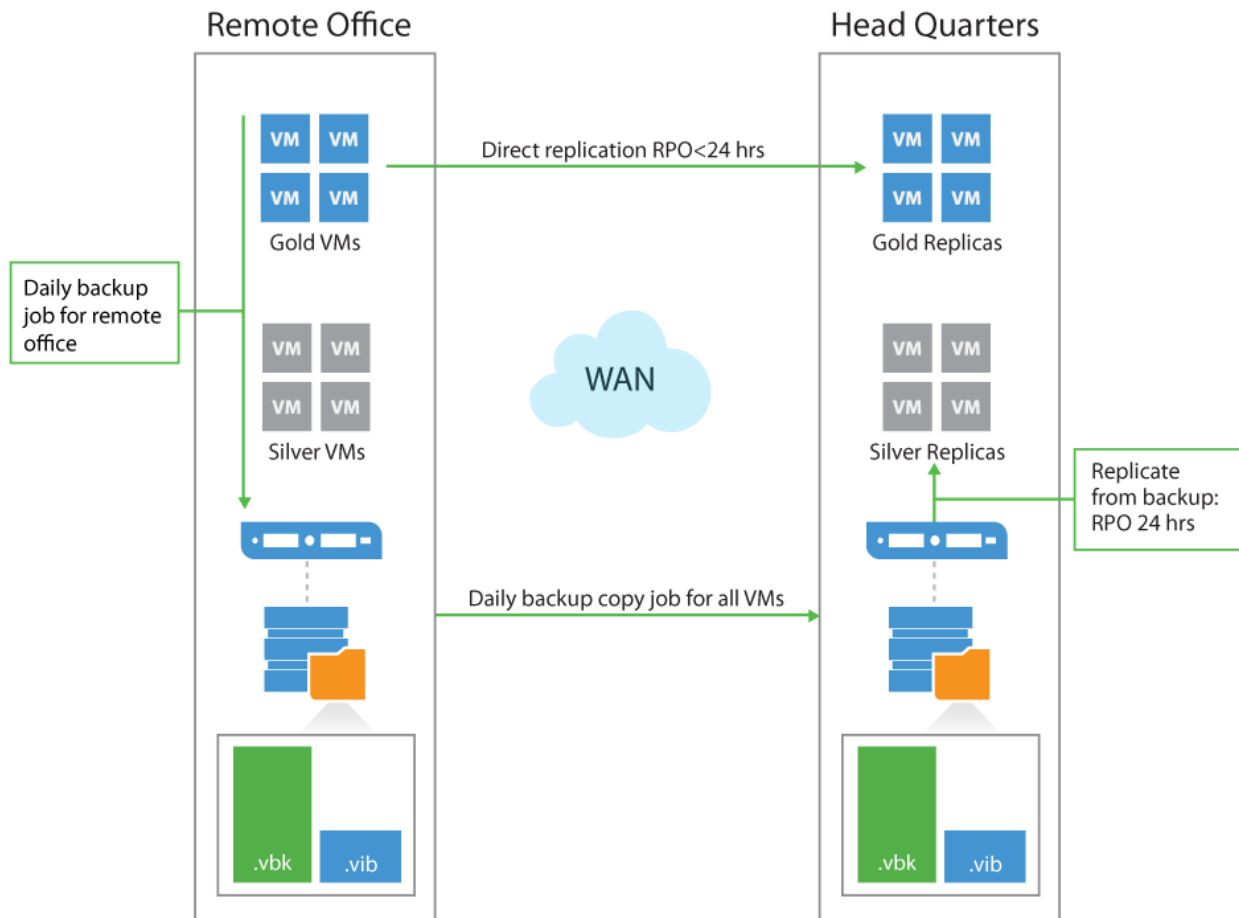
parent of 2492291... Merge branch 'master' into dev

1.76.3 Replication from Backups

When using replication from backup, the target VM is updated using data coming from the backup files created by a backup or backup copy job.

In some circumstances, you can get a better RTO with an RPO greater or equal to 24 hours, using replicas from backup. A common example beside the usage of proactive VM restores, is a remote office infrastructure, where the link between the remote site and the headquarters provides limited capacity.

In this case, the data communication link should be mostly used for the critical VM replicas synchronization with a challenging RPO. Now, assuming that a backup copy job runs for all VMs every night, some non-critical VMs can be replicated from the daily backup file. This requires only one VM snapshot and only one data transfer.



You can find additional information about replica from backup in the appropriate section of the Veeam Backup & Replication User Guide: https://helpcenter.veeam.com/docs/backup/vsphere/replica_from_backup.html?ver=95

You can find additional information about replica from backup in the appropriate section of the Veeam Backup & Replication User Guide: https://helpcenter.veeam.com/backup/vsphere/replica_from_backup.html?ver=95

dev

Tip: This feature is sometimes named and used as proactive restore. Together with SureReplica, it is a powerful feature for availability.

1.76.4 Backup from Replica

It may appear an effective solution to create a VM backup from its offsite replica (for example, as a way to offload a production infrastructure); however, this design is not at all valid because of VMware limitations concerning CBT (you cannot use CBT if the VM was never started). There is a very well documented forum thread about this subject: <https://forums.veeam.com/vmware-vsphere-f24/backup-the-replicated-vms-t3703-90.html>.

1.77 Application-Aware Image Processing

When configuring Veeam backup and replication jobs, you can specify how the transactionally-consistent backup images of VMware VMs should be created. Two methods are available for bringing VM file system and applications into consistent state: VMware Tools quiescence and Veeam's proprietary application-aware image processing (using Microsoft VSS or Linux scripts). Key features of both methods are illustrated by the following table:

Feature	VMware Tools Quiescence	Application-Aware Image Processing
Support for consistent backup on Windows guest	Yes	Yes
Sync driver for Linux guest	Yes	No
Support for application-aware backup	Limited	Yes
Pre-VSS preparation for specific applications (e.g. Oracle)	No	Yes
Support for application log truncation (Microsoft SQL Server and Exchange Server)	No	Yes
Support for scripts	Yes (need to be placed on VM guest)	Yes (can be centrally distributed)
Interaction with user via UI	Not needed	Not needed
Error reporting	Within VM guest OS	Centralized, on Veeam backup server

1.77.1 How Veeam Guest OS Processing Works

1. First, Veeam Backup & Replication performs guest OS inventory to find out if there is a VSS-aware application running inside a VM.
2. Veeam Backup & Replication runs pre-freeze script (if any) for the Microsoft Windows/Linux guest OS with applications that utilize other means of VM quiescence.
3. Then VSS quiescence of the VM is performed, including restore awareness settings.
4. VM snapshot is created.
5. VSS unfreeze ("thaw") is performed.
6. Veeam Backup & Replication runs post-thaw script (if any) for the Microsoft Windows/Linux guest OS.
7. Backup data transfer and snapshot commit is performed.
8. Finally, log file truncation is performed with VSS (for Microsoft SQL Server and Exchange Server) or using native Oracle commands (for Oracle databases on Linux).

1.77.2 Selecting Guest Processing Options

When on the **Guest Processing** step of the job wizard, you are presented with the variety of options (as described in detail in the User Guide (https://helpcenter.veeam.com/docs/backup/vsphere/backup_job_vss_vm.html?ver=95)).

Note that you can use pre- and post-job scripting to automate job global settings from the Veeam Backup & Replication server itself. It is recommended to use the VM guest processing options for interaction with VMs.

To select the necessary options, refer to the table below.

VM guest OS type	Linux (with applications and known user for Guest OS processing)	Windows and VMware VSS-supported applications (without known user for Guest OS processing)	Windows with VSS-aware applications	Windows (no VSS-aware applications)	Linux with applications	Linux server (no applications)
Guest OS processing is applicable	Y	Y	Y	Y	Y	N
Use VMware Tools quiescence	N	Y	N	N	N	N

VMware Tools quiescence with VMware Script processing | Y | N | N | N | N | N | N | Enable Veeam Application-Aware Image Processing | N | N | Y | N | N | N | Enable Veeam Application-Aware Image Processing and InGuest Scripts | N | N | N | Y | N | N | Disable Veeam Application-Aware Image Processing | N | N | N | N | N | Y | N |

To coordinate proper VSS and indexing activities, Veeam Backup & Replication deploys a small executable component inside a VM. It is installed only during VSS quiescence procedure and removed immediately after the processing is finished, producing very low impact on VM performance and stability. As for connection method for accessing VM guest OS, Veeam first tries to connect to the VM over network using RPC and then by VMware VIX channel through VMware Tools (for Windows guest only).

1.77.3 Guest Interaction Proxy

Depending on the guest VM operating system and/or Veeam Backup and Replication Edition different servers may be selected to perform guest processing step and initiate connection to a VM as per the table below.

Edition	Windows	Linux	Standard	Backup server	Backup server	Enterprise	Guest interaction proxy
			Backup server	Enterprise Plus	Guest interaction proxy	Backup server	

Any Windows server managed by Veeam Backup and Replication can be selected to act as guest interaction proxy but the preference would be given to the server that has IP address in the same subnet as subject VM. This functionality allows for having only small limited range of ports to allow through the firewalls in restricted environments and for that reason it is recommended to have guest interaction proxies in all VM subnets that are not supposed to be directly accessible from the network where Veeam backup server resides.

For details on network configuration refer to the section “Required ports” below.

Tip: If the backup server has no network connection to the VMs and deploying additional guest interaction proxies is not practical/possible (for example, service provider environments), order in which backup server or guest interaction proxy tries to communicate to a VM can be changed using the following registry key:

Path	HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication
Key	InverseVssProtocolOrder
Type	REG_DWORD (32-bit)
Value	0 = try connection through RPC, failover to VIX (default)
Value	1 = try connection through VIX, failover to RPC

RPC connection means injecting the file via the “ADMIN\$” share on the target VM. See Veeam Knowledge Base article at <https://www.veeam.com/kb1230> for more information. Consider that this is a global setting that will be applied on the Veeam backup server level and affects all jobs with application-aware image processing.

1.77.4 Guest Access Credentials

Depending on the VM guest OS processing options selected (enabled or disabled application-aware image processing) and on the guest access method, you may need to supply access credentials for the guest OS, as described in the tables below.

Tip: To verify the credentials you supplied on the Guest Processing step of the job wizard, click **Test Now** button.

Windows OS

Application-Aware Image Processing (AAIP)	VMware Tools Quiescence	Veeam via VIX	Veeam via RPC
Disabled (crash-consistent)			
Membership in the local Administrators group	User account not needed	No	Yes
Enter username as <servername>\Administrator [^3] or <domain>\Administrator	No	Yes	[^1]
UAC can be enabled	Yes	Yes	[^2]
VMware Tools must be installed and up to date	Yes	Yes	Yes
	No		

Linux OS

| Linux guest OS processing | VMware Tools Quiescence | Veeam via SSH | Disabled (crash-consistent) | | - | - | - |
- | | Root user account | No | Yes | No | | User requires `sudo` rights | No | Yes | No | | Certificate-based authentication
available | No | Yes | No | | VMware Tools must be installed and up to date | Yes | Yes | No |

1.77.5 Required Ports

The following ports should be open between the Veeam backup server and VM for guest OS processing:

- For Windows VMs - remote RPC ports, including Dynamic Port Range (TCP ports 1025 to 5000 - for Microsoft Windows 2003, 49152-65535 - for Microsoft Windows 2008 and newer); TCP/UDP ports 135, 137-139, 445.
- For Linux VMs – SSH port (default is TCP port 22)

For details, refer to the Veeam Backup & Replication User Guide (https://helpcenter.veeam.com/docs/backup/vsphere/used_ports.html?v)

1.77.6 Sizing

Since guest processing produces very low impact on VM performance, no special considerations on sizing are required. If you use VSS processing with VMware Tools quiescence or Veeam in-guest processing, you need free space on each drive of the VM for the software VSS snapshot. Please check Microsoft requirements for more information.

1.77.7 File exclusions

Another operation Veeam Backup can do on guest OS level (NTFS only) is excluding certain files or folders from the backup. Alternatively the job can be configured to include only specified files or folders in the backup.

This functionality operates very similarly and shares a lot of characteristics with excluding Windows page file and deleted file blocks. It may help reduce size of the backup files or implement additional data protection strategies for specific data. Backups for which this option was enabled remain image-level and hypervisor APIs are used to retrieve VM data. File exclusion feature uses a combination of NTFS MFT data and guest file system indexes collected by in-guest coordination process to determine which virtual disk blocks belong to the excluded files and thus should not be included in the backup.

Full file/folder paths, environment variables or file masks can be used to define exclusions. For more details on configuring exclusions and its limitations refer to the [corresponding User Guide section](#).

Note: Generic file exclusions (defined for high level folders) are most effective. File masks exclusions require guest file system indexes and generating indexes may put additional stress on guest VM and will increase backup time. For this reason it is recommended to avoid using file system masks especially on file servers with large number (thousands) of small files and use high level folder exclusions instead. When using include filters, file exclusions are created for everything else and can take significant time.

How file exclusion works

For each VM in a job that has exclusions enabled Veeam Backup and Replication performs the following operations:

1. Virtual machine NTFS MFT is read into the memory cache on the backup proxy, data blocks that store excluded files are marked as deleted.
2. When sending data blocks to target repository data is read both from the VM snapshot and memory cache on the backup proxy. Target repository reconstructs VM disks without excluded VM blocks.

3. Virtual machine NTFS is modified using the data in the cache on the proxy and information about excluded data blocks is saved in the backup file or replica metadata. This information is necessary as CBT is not aware of which blocks were excluded and is used to determine which blocks should be processed during the next backup session.
-

[^1]: Only this account is able to bypass the UAC prompt for launching processes with administrative privileges. If not applicable, see [^2].

[^2]: When performing application-aware image processing on Windows via VIX, UAC must be entirely disabled, unless the user account is the local administrator account (SID S-...-500).

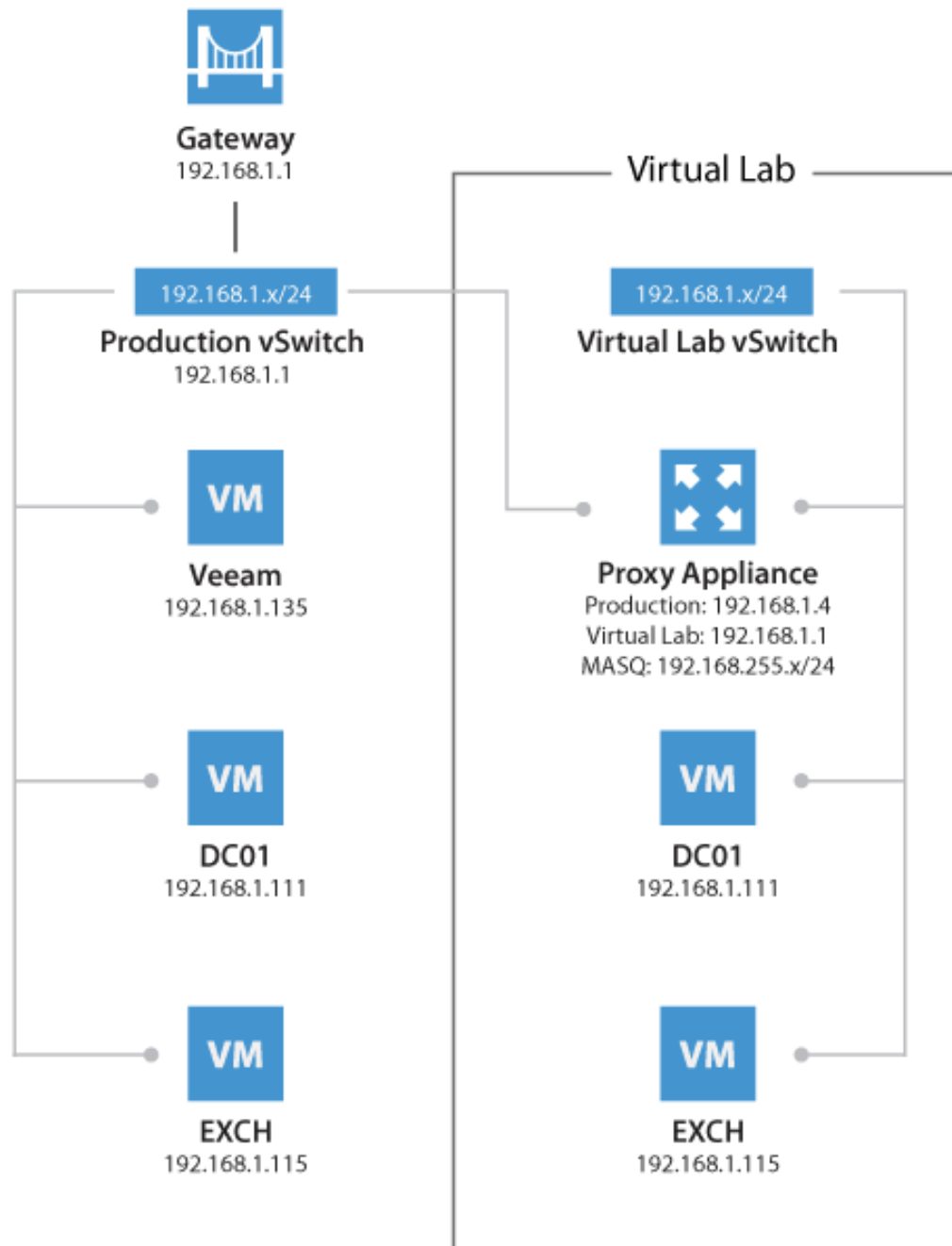
[^3]: Local administrator accounts other than the built-in Administrator account may not have rights to manage a server remotely, even if remote management is enabled. The remote User Account Control (UAC) LocalAccountTokenFilterPolicy registry setting must be configured on the VM guest to allow local accounts of the Administrators group other than the built-in administrator account to remotely manage the server:

```
|||—:|—||Path|HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System  
||Key|LocalAccountTokenFilterPolicy||Type|REG_DWORD (32-bit)||Value|1 = disable token filter  
and allow remote management by local administrative accounts || 0 (default) = enable token filter and do not allow  
remote management by local accounts| |||
```

1.78 Data Verification Using Virtual Labs

1.78.1 Virtual Lab Appliance Overview

The Virtual Lab appliance operates as a gateway to offer network connectivity between the Veeam backup server and the isolated virtual machines in the Virtual Lab. It can also be used to provide access to other clients coming from the production network using static mapping. If VMs running in the isolated network need Internet access, the Virtual Lab appliance can act as a proxy server.



When a SureBackup job is executed the static routes to reach the masqueraded networks are temporarily added to the routing table on the Veeam backup server. To review the routing table, you can open a command prompt on the Veeam backup server and execute:

```
route print -4
```

You may run this command before and after starting the SureBackup job to compare the differences.

The routes are added just after the Virtual Lab appliance has booted and has been correctly initialized by the Veeam backup server. As routes are added, this will ensure the Virtual Lab appliance is the gateway for all packets destined to the masquerade networks.

To avoid network reconfiguration of physical components, place the backup server and the Virtual Lab appliance in the same network subnet.

Check Veeam Backup & Replication documentation for configuration details:

- [vPower Users Guide](#)
- [Recovery Verification help](#)

1.78.2 How SureBackup Job Works

SureBackup leverages the capabilities of the Virtual Lab appliance to create an isolated environment where different tests can be executed against VMs. These VMs are powered on directly from the backup files using the vPower technology.

Booting the Virtual Lab Appliance

1. Virtual Lab appliance configuration file is built and mapped to the Virtual Lab appliance as an ISO.
2. Virtual Lab appliance network interfaces are reconfigured for appropriate isolated networks.
3. The Virtual Lab appliance is powered on.
4. The SureBackup job waits for IP configuration to be published and stabilized through VMware Tools.
5. A static route for the configured masqueraded networks is added dynamically to the routing table of the Veeam backup server. Those static routes define the IP address of the Virtual Lab appliance as the gateway towards the masqueraded networks.

Booting Virtual Machines

1. If the Application Group is based on backups, Veeam publishes and registers VMs using Veeam vPower NFS from the repository containing the backup file. This step is skipped if the VMs are replicas.
2. Veeam reconfigures the VMs and connects them to the isolated port groups of the Virtual Lab. If a network connection is configured to be connected to a port group that is not available in the Virtual Lab, those network are disconnected automatically.
3. Veeam creates a snapshot for the VMs in order to redirect write operations to the production datastore selected during the Virtual Lab configuration and on which the virtual appliance files will be deployed.
4. If the domain controller role is selected, registry settings are injected in the VM to ensure the NETLOGON service will not shutdown due to missing peer communication.^[1]
5. VMs are powered on.
6. During boot VMware Tools announce IP configuration of VMs. The SureBackup job waits for this information to stabilize.

Note: If VMware Tools are not installed on the virtual machine the job will wait for the duration of **Maximum allowed boot time** configured for the VMs. This will slow down SureBackup jobs significantly. Therefore, it is always recommended to install VMware Tools on a verified VM.

Testing Virtual Machines

1. **VMware Tools heartbeat** is used for verifying that the VM OS is successfully started. SureBackup will wait a predefined amount of time for the heartbeat to register however if a heartbeat is seen before the timeout period expires the tests continue automatically.
2. **PING** tests are initiated according to the masqueraded network configuration. The ping is sent from the Veeam backup server using the static routes added during the job execution. Since the masquerade network is not part of the Veeam backup server's own subnet, the packet is sent to the gateway matching the Virtual Lab network (usually the virtual lab appliance).
3. **Application-specific testing** uses scripts and is enabled based on the roles assigned to a VM in the application group configuration. The built-in roles will check corresponding TCP ports for a given service. The built-in role for SQL Server provides additional testing (see next section), and custom scripts may be used for third party applications. Requests are sent from the Veeam backup server, and the routing to the virtual machine is handled by the Virtual Lab proxy appliance.
4. **CRC verification** is optionally available and is disabled by default. If enabled, it will ensure all content of the backup file is consistent with the hash values at the time they were written. This consistency check is using the CRC algorithm for hashing.

Note: This feature reads the entire backup file, and requires significant time to complete.

5. **Custom scripts** are stored on the Veeam Backup Server and are launched by the account that controls the Veeam Backup Service. The authentication mechanism used to run remote commands on the tested guests will depend on the operating system.
 - **Windows script:** Veeam Backup & Replication starts a new shell (cmd.exe) as the user running the Veeam Backup & Replication Service (default being "Local System Account") using the switch "/NETONLY" to use the specified credentials (e.g. database user in the tested environment) only when through a remote connection. This is imposed by the fact that the credentials needed for testing (specified in the credentials configuration tab) might not be existent in the domain where Veeam Backup Services are running.
 - **Linux scripts** will use a utility software called "plink.exe" to run remote commands over the virtual lab gateway. "plink.exe" is executed by the account running Veeam services while all subsequent commands in the script will use the credentials specified in the SureBackup script configuration tab.
6. **Specific concerns about SQL server authentication mode:** if the tested Microsoft SQL server accepts a Windows type authentication, the isolated domain credentials specified in the configuration tab will be used (like testing a SQL DB using the "runas /netonly" shell environment). If an SQL type authentication is requested by the tested database (typically "sa" user), the script should then be manually invoked and SQL credentials passed as arguments. The script to invoke is "%ProgramFiles%\Veeam\Backup and Replication\Backup\Veeam.Backup.SqlChecker.vbs" and arguments should be in the exact order:
 - %log_path : default script log path "%programdata%\Veeam\Backup\Name_of_SureBackup_Job"
 - %vm_ip% : masqueraded IP of the SQL server
 - SQL user
 - SQL password

In this case the script will only use SQL type credentials making useless to specify Windows credentials as the script argument.

If **Linked Jobs** are configured for the SureBackup job, linked VMs will start booting once all virtual machines explicitly defined within the Application Group have been successfully booted and verified. Remember that by default 3 VMs are tested at the same time in a Linked Job. There may be more than 3 VMs linked, but the following ones will stay in the testing queue. The limit can be adjusted in the SureBackup job configuration wizard, and may be increased if the backup repository and hypervisor can both handle the load accordingly.

Guest predefined roles

When adding a guest image to the or the linked job, it is possible to assign a predefined role, for which Veeam Backup will automatically configure boot options and run a default set of application test accordingly, following rules described in below table.

Role	Default startup options	Default test script	Default application timeout
Domain Controller (authoritative or non authoritative)	600s maximum boot time	120s application timeout	Connection test on port 53
Global Catalog	1800s maximum boot time	120s application timeout	Connection test on port 389
Mail Server	1800s maximum boot time	120s application timeout	Connection test on port 25
SQL server	1800s maximum boot time	120s application timeout	Run "USE" SQL command against all defined databases on the server
Veeam Backup for Office 365	1800s maximum boot time	120s application timeout	Connection test on port 9191
Web Server	600s maximum boot time	120s application timeout	Connection test on port 80

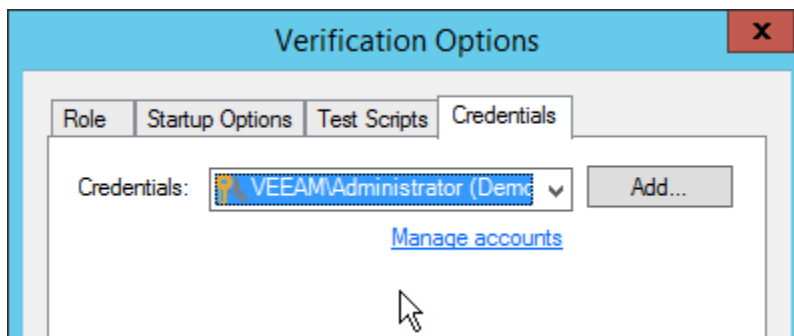
Note : You will notice that the Domain Controller startup mode (authoritative or not) can now be chosen. Veeam will mark the server accordingly so it boots in the selected mode. This is especially useful if many DC needs to be tested in a single SureBackup job. Please remind that if a single (or the first) Domain Controller is booted, it might use the authoritative mode. Subsequent Domain controllers must then use non-authoritative mode and will then synchronize from the authoritative one.

Checking SQL Server Database Availability

A dedicated Visual Basic script is included to allow for testing whether all databases on a given instance are available. This script is available in the Veeam installation folder as the `Veeam.Backup.SqlChecker.vbs` file.

By default, the script tries to retrieve and check *all* instances; you can optionally configure one or more specific instances to be tested. The script enumerates all databases and checks if these databases are available, using the `USE <db>` statement.

When running scripts that require authentication, when executed the script will impersonate the service account under which the Veeam Backup Service is running (default is SYSTEM). To specify different credentials configure them in the 'Credentials' tab in the Application Group settings.

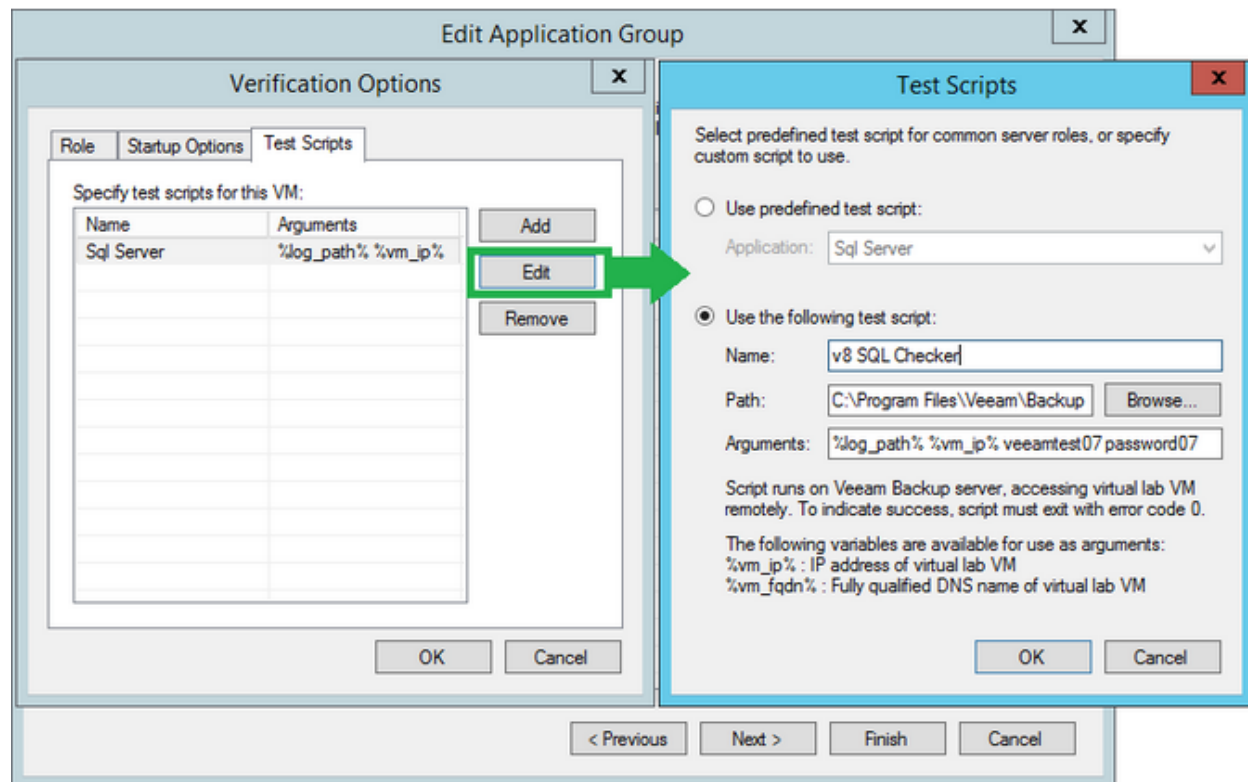


Credentials settings in Application Group

Important! To ensure successful authentication it is required for the specified user to have *public* access to all databases.

The `SqlChecker.vbs` script also accepts two additional parameters to use SQL authentication instead of Windows based authentication. In order to use SQL authentication you need to add a custom test script instead of the built-in SQL Server role, and specify the following path and arguments:

- Name: SQL checker
- Path: *Browse for the Veeam.Backup.SqlChecker.vbs file*
- Arguments: `%log_path% %vm_ip% sa sa_account_password`



Example

custom role

Creating Custom Roles

Though there are a number of built-in tests intended for application-level testing, you may need to develop additional scripts for testing proprietary applications. This is the procedure to do so:

1. Open the Veeam installation folder and look in the `SbRoles` folder. All roles are defined in the XML files available in this folder.
2. To create custom roles, duplicate one of the above mentioned files and modify the `<Id>` tag using a UUID generator (such as <https://www.uuidgenerator.net>). Use this configuration file to specify the GUI settings.

When creating custom roles for Linux-based applications you may need to execute the generated code locally within the VM. To do so, use `\Putty\plink.exe` shipped with the product and located in the Veeam Backup & Replication installation directory.

When executing bash scripts locally on a Linux virtual machine using `plink.exe`, the exit codes are passed to the SureBackup job, enabling correct error reporting. If using `plink.exe` in combination with a SSH private key, you should connect manually (one time) to the VM via SSH using `putty.exe` from the Veeam backup server in order to accept the target VM SSH fingerprint; otherwise, the SureBackup job will wait for this input and ultimately timeout.

Note: You can use `puttygen.exe` to create a private key.

Another option for testing service availability with `Veeam.Backup.ConnectionTester.exe` is described in <https://www.veeam.com/kb1312>.

Common Issues

When performing SureBackup, there are few common issues you may come across. Most of these issues are described in Veeam knowledge base articles:

- When restoring Windows 2008 R2 virtual machines with the VMXNET3 network adapter, the resulting virtual machine obtains a new NIC, and all network settings have to be adjusted manually. The solution is explained in [Veeam KB1570](#)
- When using DHCP with leases bound to MAC addresses, ensure that the vNIC MAC address is configured as `static`. Otherwise the VM will boot with a MAC in the Virtual Lab, and the VM may get a different IP address > [Setting a static MAC address for a virtual NIC](#)
- Some Linux distributions use `udev` for assigning names to NICs. If the MAC address changes during replication or Instant VM Recovery, the NIC's configuration file may not be applied. For more information, please see [RHEL6 SureBackup](#)

Troubleshooting Mode

If you need to troubleshoot Virtual Lab, it is recommended to start sessions in the Troubleshooting Mode. To do so:

1. Open up **Statistics** for a SureBackup job.
2. Right-click the VM you want to troubleshoot.
3. Select **Start**.

The SureBackup lab will now start in troubleshooting mode, which means that errors will not cause the Virtual Lab to shut down immediately.

If the selected VM is in an application group, this VM and previous ones are started. If the VM is part of a linked job, the entire Application Group and the selected VM is started.

This mode is especially helpful during an implementation phase while measuring application boot times via vPower NFS, or implementing custom verification scripts. When you have finished troubleshooting, you can stop the SureBackup session manually.

Tip: On the Virtual Lab appliance, ICMP traffic is blocked on all network interfaces connected to isolated networks, unless you check the “Allow proxy appliance to act as internet proxy for virtual machines in this lab”. This may lead to undesired behavior of some systems, as they will be unable to ping their gateway.

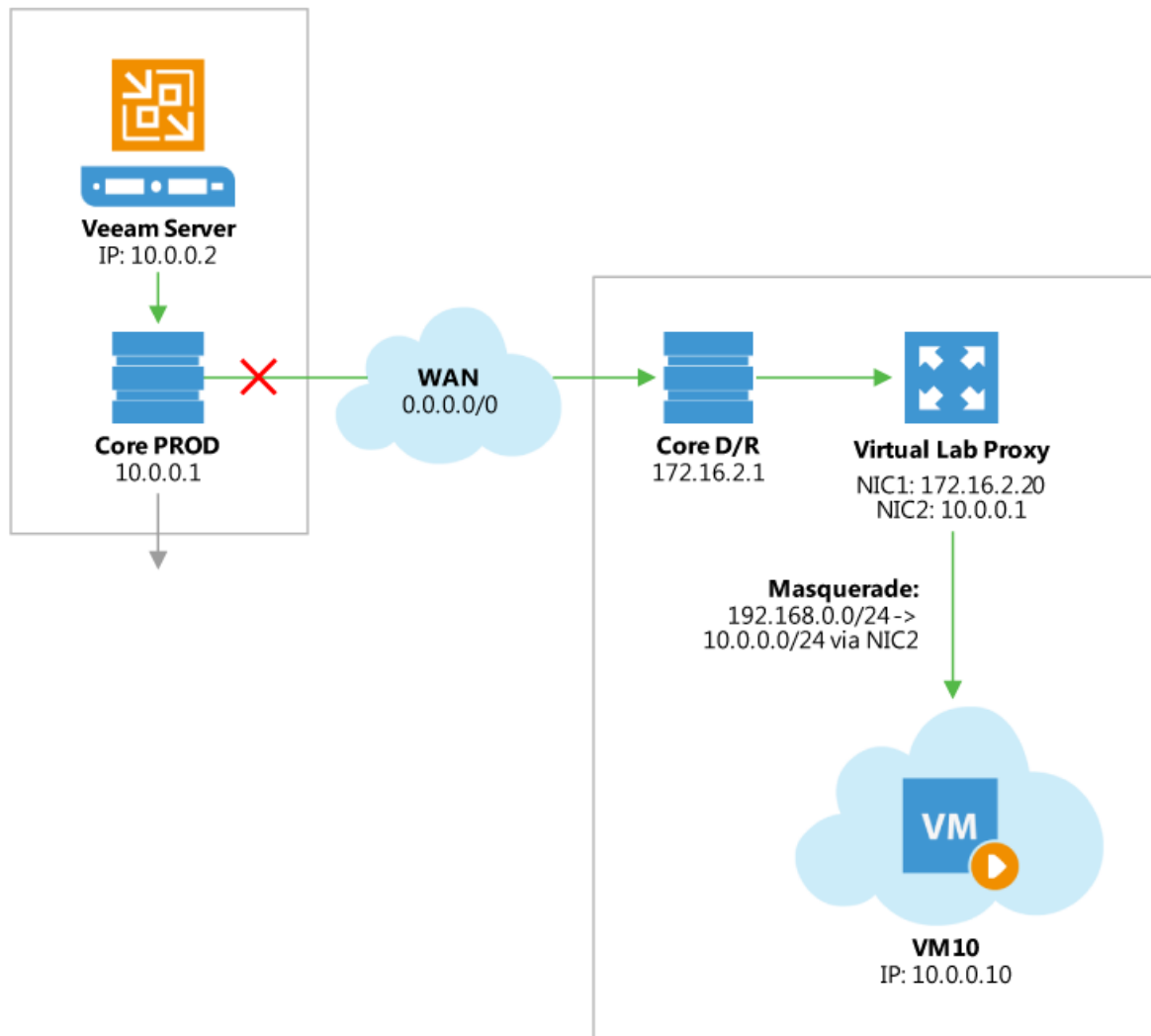
1.78.3 Virtual Lab in Complex Environments

When using standard vSwitches in a VMware vSphere infrastructure, the Virtual Lab proxy appliance and the isolated networks must run on the same ESXi host (“Basic Single-Host” and “Advanced Single-Host” configurations). The reason is that standard vSwitches and their port groups are bound to one single host. Since the Virtual Lab port groups are isolated by nature, these networks are not known at the core network in terms of VLAN tagging or routing.

When Distributed vSwitch (dvSwitch) is available, port groups can span multiple ESXi hosts (“Advanced Multi-Host” configuration). Distributed vSwitches are typically required when using Virtual Lab for replicas (SureReplica) as replicas will often span multiple hosts. vSphere Distributed Resource Scheduler (DRS) may also distribute VMs across multiple hosts within a cluster once they are started.

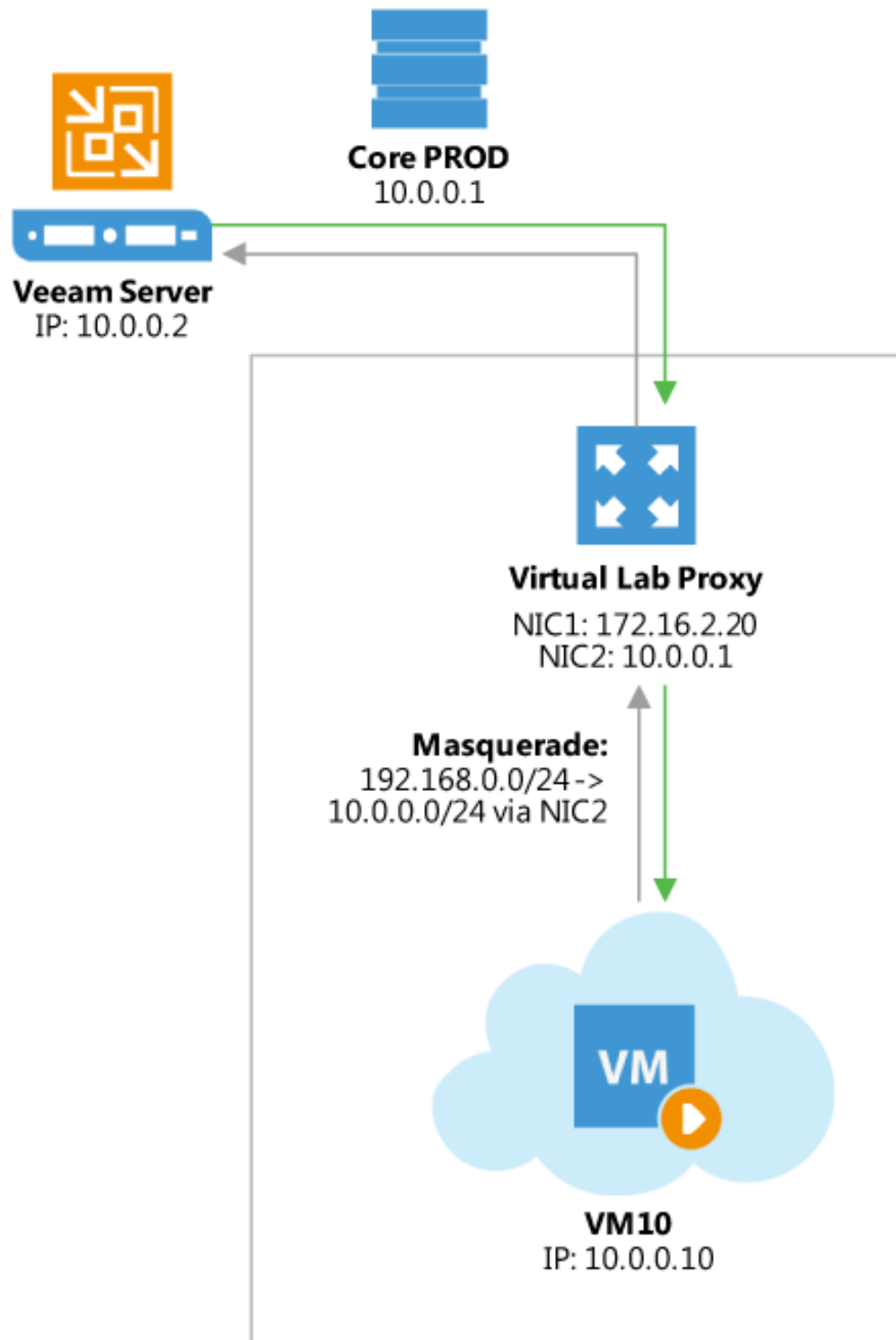
Important! Please check the following help article and the links at the bottom of the webpage before you configure Virtual Labs for Distributed vSwitch: [Advanced Multi-Host Virtual Labs](#).

Even in environments where Distributed vSwitch is available, make sure that the Veeam backup server and the Virtual Lab proxy appliance are placed in the same VLAN to prevent network packets (sent to the masquerading IP subnets) from being routed.



Most DR datacenters are configured with different IP networks from production to allow for “active-active” configurations. In such cases, layer 3 (L3) is used for networking configuration and routing is in place to establish communications between the production site and the DR site.

For more information, please see the [Backup Server Placement](#) section of this guide.



[^1]: For more information about Domain Controller restore, please see the corresponding thread in Veeam Community Forums > [Veeam B&R v5 recovery of a domain controller](#)

1.78.4 Scaling out SureBackup jobs

When it comes to managing thousands of virtual machines such as backup as a Service (BaaS) providers do, it might then become difficult to simply configure and run a SureBackup against a linked job containing thousands of images. Attention must then be paid to timing and resource consumption.

Linked jobs

Using linked jobs A first option to scale out SureBackup jobs consists of leveraging the infrastructure resources at their maximum to test all the guests contained in the “linked job” attached to the job.

Here are a few guidelines to run the biggest possible SureBackup jobs:

- **Leverage non-production infrastructure:** As a very flexible feature, SureBackup allows to test the images on any cluster, this could be a small infrastructure dedicated to SureBackup, preproduction or development clusters usually underused at night.
- **Run simple and quick tests:** Commonly, backup providers don’t have administrative credentials on the objects they manage limiting or removing application testing from possible verifications. This simplifies the tests and reduces the time required to test the VMs using only the heartbeat test.
- **Rely on fast read repository:** SureBackup performance will heavily depend on the boot time of the tested guests. Keep in mind that Instant VM Recovery performance is directly related to underlying repository performance , especially on random reads. Another good option to apply to the repository is per-vm backup file since it will accelerate restore operations

Using random guests in Virtual lab

Luca Dell’Oca raised the possibility in his blog post to daily randomly select a set of virtual machines while eliminating the ones already tested. These VMs are included in the Virtual Lab and then tested. Assuming you could test 10 to 20 VMs daily, this can lead to 1000 VMs in 50 days. You can also choose to make this even more simple and randomly select 10 VMs every day, giving a very good idea on possible backup corruption statistics while modifying the script.

Note: Per application group design the whole application group will fail when a guest test fails leaving further images untested. Also, all VMs of the application group will stay online until the application group is powered off, limiting by design the number of guests to simultaneously test.

1.79 Overview of Applications Support

Veeam Backup and Replication features native support for several applications, providing full support for backup and restore. Applications with no native support can be easily protected and subsequently restored as well, sometimes requiring additional configuration or manual operations depending on the application. This section is dedicated to covering specifics of implementing protection for some of them.

It is possible to ensure data safety and transactional consistency for applications not covered in this guide using pre-freeze and post-thaw scripts that will execute inside of the virtual machine. Subject application has to provide the way to prepare itself appropriately.

Generally speaking pre-freeze and post-thaw scripts have to (depending on the capabilities of the application):

- **Pre-freeze** - freeze transactions or create application-level consistent snapshot of its data. Alternatively application services can be shut down but this involved short user service downtime and thus is not desirable.
- **Post-thaw** - unfreeze transactions or delete snapshot created by pre-freeze (where applies). In case services were shutdown they should be started again.

Certain applications do not require these steps as they include self-healing mechanics or maintain transactional consistency by other means, application documentation has to be checked and/or application vendor has to be contacted for specifics on achieving this.

Note that in addition to configuring application consistency for such applications, restore process has to be properly planned as additional steps would have to be followed to restore them as well. Using [U-AIR \(Universal Application Item Recovery\) functionality](#) allows for performing restores of any applications including custom in-house built provided the native application management tools are used.

1.80 Active Directory

Veeam Backup and Replication natively supports backup of Microsoft Active Directory controllers and allows for image level and granular AD items restore.

1.80.1 Preparation

For Microsoft Active Directory, check the tombstone lifetime settings, as described in Veeam Explorers User Guide at Veeam Help Center (https://helpcenter.veeam.com/docs/backup/explorers/vead_recommendations.html?ver=95).

1.80.2 Job configuration

For backup and restore of domain controllers to work properly application aware image processing option has to be enabled in the job properties. For more details refer to the [corresponding section](#) of the User Guide.

1.80.3 Restore and failover

It is a good practice to implement redundant Active Directory configuration with several domain controllers which helps eliminate single point of failure. Depending on the Active Directory architecture it might make sense to rebuild domain controller that was lost instead of restoring it from the backup. One of such cases is if FSMO roles from the lost domain controller were seized on another one, then it is better to deploy a new VM instead of restoring a server which still thinks it is holding the role. Finally if you are redeploying, make sure all FSMO roles are being held by a controller and that you clean up the meta data of the controller that is not coming back.

1.80.4 Recovery verification

There are two Domain Controller roles available in application group configuration - for authoritative and non-authoritative restore. When testing recovery of one domain controller only choosing role with authoritative restore will speed up verification process.

1.81 Microsoft Exchange

Veeam Backup and Replication supports variety of Exchange configuration including DAG deployments. For more details refer to the corresponding section of the User Guide.

1.81.1 Preparation

DAG clustered configurations may require adjusting cluster timeouts to avoid failovers during backup as per [KB1744](#).

1.81.2 Job configuration

For backup and restore of Exchange servers to work properly application aware image processing option has to be enabled in the job properties. For more details refer to the [corresponding section](#) of the User Guide.

1.81.3 Granular item restore

When mounting Exchange database Veeam Explorer for Exchange replays relevant log files which may significantly increase time needed for mount operation in case there is a lot of logs to replay. As lagged DAG technology relies on keeping lots of Exchange logs expect Veeam Explorer taking significant amount of time to mount EDBs when performing item restore from lagged DAG mailbox servers.

1.82 Microsoft SQL Server

Veeam supports following options to backup SQL Server databases:

- Virtual Machine Image Level Application Aware Backup.
- Veeam Agent Based Backup for Physical and Cluster SQL servers.

1.82.1 Virtual Machine Image Level Application Aware Backup:

Veeam supports image level application aware backup of SQL databases.

Supported Configuration:

- SQL Server Standalone Deployment.
- SQL Always-on Availability Groups.

Unsupported Configuration:

- SQL Server Failover Cluster Instances

Note: Please read the whitepaper on benefits of using [SQL Always-on Availability Groups for Virtual Environment](#)

1.82.2 Veeam Agent Based Backup for SQL Servers:

Supported Configuration:

- SQL Server Standalone deployment.
- SQL Always-on Availability Groups.
- SQL server Failover Cluster Instances.

Unsupported Configuration:

- Backup of CSV (Cluster Shared Volumes) is not supported. Cluster disks used as CSV are automatically excluded from backup.
- AlwaysOn Availability Groups based on multiple Failover Cluster Instances are not supported.
- AlwaysOn Clusterless Availability Groups are not supported.

1.82.3 Preparation

The following section will provide the best practices to verify SQL Server for the smooth and fast backup:

Check the Status VSS Writers / Providers:

1. Open a command prompt as Administrator.
2. Type “vssadmin list providers” and press enter.
3. Verify all the writers are in health state.
4. Type “vssadmin list writers” and press enter
5. Check and confirm writers are “Stable with no errors”.

Check the performance of SQL Server:

As backup is I/O intensive operations check the SQL server performance status before start taking the backup: To verify the SQL Server Health:

1. Open Performance Monitor.
2. Add below objects verify the performance: a. Under the Memory object, add the counter: Available MB b. Under the Processor object, add the counter: %Processor Time (Instance: Total) c. Under the Physical Disk object, add the counters: Avg. Disk Sec/Read and Avg. Disk Sec/Write (All Instances) d. Under the Paging File object, add the counter: %Usage (Instance: Total)

Check [Microsoft KB](#) to validate the health status of SQL Server.

1.82.4 Job Configuration

1.82.5 Virtual Machine Image Level Backup:

Standalone SQL Server:

No additional configuration is required to backup the standalone SQL server, you can configure the backup with application aware processing to take the backup of SQL server with the databases.

Please check the Veeam User’s Guide sections to get the more information about [SQL backup configuration](#)

SQL Always-on Availability Group:

When backing up AlwaysOn availability group make sure all cluster nodes are processed by the same backup job for transaction logs processing and restores to work properly. Consider increasing cluster timeouts in case failover occurs during the backup, similar to Exchange DAG as per KB1744.

You can also use [KB2110](#) to excluded specify database from application aware processing.

Transactions Logs Backup:

Please be aware that transactions logs are processed periodically and stored in temporary folder inside of the VM before shipping to repository/shipping server. Default location of the temporary folder is %allusersprofile%\Veeam\Backup. The default location is in most cases the system partition to avoid the situation to run out of space in the system partition, it's the best practices to change the temporary folder location to the windows disk volume where enough space is available for staging the transactions logs.

To change temporary folder use SqlTempLogPath (STRING) registry value as described at How It Works: SQL Server and Transaction Log Backup: • Path: HKEY_LOCAL_MACHINE\SOFTWARE\Veeam\Veeam Backup and Replication • Key: SqlTempLogPath • Type: REG_SZ • Default value: undefined

As best practices it's highly recommended to periodically shrink the SQL log file, Please follow [Microsoft KB](#) for more information.

1.82.6 Veeam Agent Based Backup:

Veeam Agent is requiring to backup following configuration of SQL Servers:

1. SQL Virtual Machine with RDM (Raw Device Mapping)
2. SQL Failover Cluster Instances.
3. SQL Physical Server

To backup the SQL Failover cluster, the backup need to be configured and manage by Veeam Backup Server.

1.82.7 Restore

Restore is integrated part of SQL Server protection, Veeam provides following options to restore SQL Server:

1. VM or Physical Server Restore.
 - Instant VM or Server Restore.
 - BMR Restore for Physical.
 - Full VM Restore.
2. SQL Application Item Level Restore.

Veeam uses specially designed Veeam Explorer for SQL to perform application item level restore, to optimize the restore of SQL database install Veeam Management console on SQL server locally to perform the restores.

1.82.8 SQL Failover Cluster Database Restore: (Applicable to agent based cluster backup only)

SQL Database Restore:

Please follow the below steps to restore SQL database:

1. File Level Restore to local Veeam Server.
2. Copy the mdf and ldf file to target SQL Server.
3. Attach the Database to target SQL Server.

SQL Table Level Restore:

1. Restore SQL Database to Staging SQL Server(Stand alone SQL Node)
2. Open SQL Server Management Studio. Connect both staging and target SQL server(intend to do the restore)
3. Right-click on the database name, then select “Tasks” > “Export data...” from the object explorer.
4. The SQL Server Import/Export wizard opens; click on “Next”.
5. Provide authentication and select the staging server; click “Next”
6. Specify the target SQL Server; click on “Next”.
7. Select the tables to restore.
8. Complete the restore.

1.83 Microsoft SharePoint Server

1.83.1 Job configuration

For backup and restore of SharePoint servers to work properly application aware image processing option has to be enabled in the job properties. For more details refer to the [corresponding section](#) of the User Guide. As SharePoint deployments may spread across several servers make sure to familiarize yourself with the [Required Microsoft SharePoint Backup Job Settings](#) section of the User Guide.

1.83.2 Granular item restore

Explorer for SharePoint relies on the ability to restore data from SharePoint SQL database, refer to the corresponding section of this guide on best practices to SQL Server restore for details relevant to that process.

For information on restrictions and limitations of SharePoint restore refer to the [corresponding section](#) of the User Guide.

1.84 Oracle

Veeam Backup and Replication natively supports backup of Oracle database servers and allows for image level and granular Oracle databases restore.

Note: 32-bit Oracle instances on 64-bit Linux, and Oracle RAC are not supported.

1.84.1 Preparation

Only databases in ARCHIVELOG mode will be backed up online, databases in NOARCHIVELOG mode will be shut down which will cause **database availability disruption**.

Logs are stored temporarily on the guest filesystem before they are shipped for processing. This may cause undesired behavior if there is no enough space available in default location and changing temporary location from default is recommended as per [KB 2093](#).

When backing up Oracle on Linux, the backup server is used for initiating connections, whereas a Guest Interaction Proxy will be selected for Oracle on Windows.

As restore is integral part of Oracle protection, special attention should be paid to planning Veeam Explorer for Oracle configuration, specifically network connectivity between mount server and staging servers in restricted environments. Ports used for communication between them are listed in the corresponding section of the User Guide (https://helpcenter.veeam.com/docs/backup/vsphere/used_ports.html?ver=95#explorers).

Permissions

Certain level of access is expected from the user account configured for performing Oracle backup. Refer to the corresponding section of the User Guide for details (https://helpcenter.veeam.com/docs/backup/explorers/veo_connection_to_source_server.html?ver=95).

When processing Linux instances, the same user account specified for application awareness is used to process the Oracle backup. For Windows instances, you may specify two separate accounts.

Note: It is not possible to use different accounts to access different Oracle instances running on the same VM, make sure specified credentials can be used to access all instances on a VM in those cases.

Windows OS

User account used to connect to a VM should have local administrator privileges on guest VM and read/write access to database files on filesystem level.

In addition this account or separate Oracle account in case it is different should have SYSDBA rights, this can be achieved by adding it to **ora_dba** local group.

Linux OS

Root account or account elevated to root should be used to connect to a VM. Automatic adding to **sudoers** can be enabled for the account but note that **sudoers** file entry will not be removed automatically. Persistent **sudoers** file entry with *NOPASSWD: ALL* option can be added manually, for example:

```
oraclebackup ALL=(ALL) NOPASSWD: ALL
```

This account should be included in the **oinstall[^1]** group to access Oracle database files hierarchy, and to **asmadmin** group (where applies).

In addition this account or separate Oracle account in case it is different should have SYSDBA rights, this can be achieved by adding it to **dba** local group.

1.84.2 Job configuration

Refer to the corresponding section of the User Guide (https://helpcenter.veeam.com/docs/backup/vsphere/replica_vss_transaction_oracle) for details on configuring Oracle database backup and transaction logs processing.

Avoid using aggressive logs truncation settings for databases protected with Data Guard as it may affect logs synchronization to secondary server. Data Guard should have enough time to transport logs remotely before they are truncated thus generally having “Delete logs older than” option less than 24 hours is not recommended.

1.84.3 Job workflow

Oracle on Linux backup workflow

1. Coordination component which will perform all the necessary steps is injected into the guest VM. This component is the same as the one used for Linux application-aware image processing in general.
2. Perform application discovery. This is done using native OS methods, coordination component queries `/etc/oraInst.loc` and reads `inventory.xml` which is then compared to `/etc/oratab` information.
3. Status and version of instance(s) is fetched.
4. Disk group information is retrieved for ASM instances.
5. Log mode is identified, this information will later be used for decisions on how exactly the database has to be processed. Database files, CDB (Oracle 12 only) and current DBID information is retrieved.
6. At this step archive log necessary information was collected and Veeam will start doing actual backup, modifying database state - current archive log is archived and all archive log information is retrieved.
7. PFILE backup is created and archived into the backup metadata.
8. Additional information is collected and recorded (current DBID, SCN, Sequence IDs, database unique name, domain, recovery file destination, basic listener information and current archive log).
9. Coordination component is shut down and then restarted again to finalize the backup: database is put into backup mode and database snapshot is created.

Oracle on Windows backup workflow

Behavior on Windows depends on the state of VSS writer, Oracle version and database type.

|| VSS enabled | VSS disabled | Pluggable database || - | - | - | - || Oracle 11 | Oracle VSS writer is engaged, NOARCHIVELOG databases are shut down and excluded from VSS processing | Same workflow as for Linux | N/A
 || Oracle 12 | Oracle VSS writer is engaged, NOARCHIVELOG databases are shut down and excluded from VSS processing | Same workflow as for Linux | Same workflow as for Linux, VSS writer is skipped |

1.84.4 Restore and failover

Before the backup the database (in ARCHIVELOG mode only) is put into backup mode, this has to be taken into consideration when performing restore - restoring database server VM is not enough for restoring the service, database has to be put out of backup mode:

```
ALTER DATABASE END BACKUP
```

1.84.5 Granular item restore

Oracle restore using Veeam Explorer for Oracle uses a combination of executing commands via SSH or RPC depending on the platform, and using the RMAN client. VM disks are mounted to target server using iSCSI (Windows) or FUSE and loop device (Linux). Only database files will be restored, not instance files. Instance files may be recovered through file-level recovery if needed.

Ensure the account used to connect to target/staging server has enough permissions on operating system and database as described in the corresponding section of [User Guide](#) or earlier in this guide.

Note: When restoring to Linux ensure that account used to connect to restore target server has valid shell.

Restore workflow

When performing restore Veeam Explorer follows the following steps:

1. Oracle instance/database discovery is performed and information is collected, that includes path validation and disk space availability checks.
2. VM disks are mounted.
3. Target database is shut down and dropped, configuration is cleaned (configuration and temporary instance files).
4. Database is started from the temporary location, if that fails another restore attempt is performed with safe set of parameters.
5. After successful test start from temporary location database is restored to proper location using automatically generated RMAN script.
6. Restore control files are restored after that. Database is updated to specific transaction prior to that in case point in time was selected for restore.
7. Fast Recovery Area parameters are restored and database is upgraded accordingly if restoring 32-bit instance to 64-bit.
8. To finalize restore mounted backup is removed from RMAN repository, restored database is restarted and new DB ID is generated. Remaining bits of the configuration are restored as well - parameter file is restored to proper path along with password file, DBNAME is changed if needed, logs are reset and online logs are recreated.

1.85 MySQL

Veeam supports backup and restore of MySQL databases.

1.85.1 Backup Options:

The following options are supported to backup MySQL databases:

- HotBackup Database Online Dump. o Online Dump to the same server. o Online Dump to Staging server
- HotBackup Database Freeze.
- ColdBackup Database Shutdown.

1.85.2 HotBackup Database Online Dump:

There are multiple options available regarding Database Online Dump, one of the option is to use Veeam [Pre & Post Thaw Scripts](#) to dump the database during the backup operations and other option to dump the database to another staging server and protect the staging server from Veeam.

Let's go through each option one by one in the details:

Database Online Dump During Backup Operations:

In this option the pre-freeze script will dump all databases hosted on the guest to a single file under the /tmp directory. Before the VM snapshot creation, the mysql dump native command will dump a copy of the database while service will remain available.

The dump will be deleted by post-thaw script after the guest snapshot has been successful. Pre Freeze Script:

1. Use Editor
2. Copy the content in the editor.

```
#!/bin/bash
# config:
# when running on debian we can use existing debian-sys-maint account using defaults_
↪file
# otherwise, specify username and password below using use_credentials
#use_credentials="-uroot -p"
defaults_file="/etc/my.cnf"
dump_file="/tmp/mysql_dump.sql"
database="--all-databases"
if [ -f $defaults_file ]
then
opts="--defaults-file=$defaults_file"
elif [ -n $use_credentials ]
then
opts="$opts $use_credentials"
else
echo "$0 : error, no mysql authentication method set" | logger
exit 1
fi
opts="$opts $database"
echo "$0 executing mysqldump" | logger
mysqldump $opts >$dump_file 2>/dev/null
if [ $? -ne 0 ]
then
echo "$0 : mysqldump failed" | logger
exit 2
else
echo "$0 : mysqldump succeeded" | logger
sync;sync
fi
```

1. Save script as PreFreeze.sh
2. Use script as [pre-freeze script](#) in a backup job.

Post-Thaw Scripts

1. Use Editor
2. Copy the below in the editor:

```
#!/bin/bash
dump_file="/tmp/mysql_dump.sql"
if [ -f $dump_file ]
then
echo "$0 deleting mysql dump file $dump_file" | logger
rm -f $dump_file > /dev/null 2>&1
exit 0
else
echo "$0 could not locate mysql dump file $dump"
```

1. Save file as PostThaw.sh.
2. Use script as [Post-Thaw script](#) in the backupjob

****Online Dump to Staging server**

Another option is to dump the MySQL database to staging server and protect staging server from backup job.

1. Create new server or use any existing server as NFS Share.
2. Create Script to dump the MySQL database to Staging server
3. Use Editor
4. Copy below sample code in the editor:

```
#!/bin/bash
# Shell script to backup MySQL database

# Set these variables
MyUSER=""          # DB_USERNAME
MyPASS=""          # DB_PASSWORD
MyHOST=""          # DB_HOSTNAME

# Backup Dest directory
DEST="" # /home/username/backups/DB

# Email for notifications
EMAIL=""

# How many days old files must be to be removed
DAYS=3

# Linux bin paths
MYSQL="$(which mysql)"
MYSQLDUMP="$(which mysqldump)"
GZIP="$(which gzip)"

# Get date in dd-mm-yyyy format
NOW="$(date +%d-%m-%Y_%s)"

# Create Backup sub-directories
MBD="$DEST/$NOW/mysql"
install -d $MBD

# DB skip list
SKIP="information_schema
another_one_db"

# Get all databases
DBS="$($MYSQL -h $MyHOST -u $MyUSER -p$MyPASS -Bse 'show databases')"
```

```
# Archive database dumps
for db in $DBS
do
    skipdb=-1
    if [ "$SKIP" != "" ];
    then
        for i in $SKIP
        do
            [ "$db" == "$i" ] && skipdb=1 || :
        done
    fi

    if [ "$skipdb" == "-1" ] ; then
        FILE="$MBD/$db.sql"
        $MYSQLDUMP -h $MyHOST -u $MyUSER -p$MyPASS $db > $FILE
    fi
done
```

(continues on next page)

(continued from previous page)

```

    fi
done

# Archive the directory, send mail and cleanup
cd $DEST
tar -cf $NOW.tar $NOW
$GZIP -9 $NOW.tar

echo "MySQL backup is completed! Backup name is $NOW.tar.gz" | mail -s "MySQL backup"
↪$EMAIL
rm -rf $NOW

# Remove old files
find $DEST -mtime +$DAYS -exec rm -f {} \;

```

1. Save file as DB_Backup.sh.
2. Use Linux Scheduler to run the script on desired time for the backup.
3. Configure the backup of staging VM.

***HotBackup Database Freeze.

In this option, Veeam will freeze the database during pre-freeze script and release the database in post-thaw, MySQL table will be flashed to disk into read-only state and writable once the VM snapshot has been created.

1. Use editor
2. Copy the sample code

```

#!/bin/bash
# config:
# when running on debian we can use existing debian-sys-maint account using defaults_
↪file
# otherwise, specify username and password below using use_credentials
#use_credentials="-uroot -p"
defaults_file="/etc/my.cnf"
timeout=300
lock_file=/tmp/mysql_tables_read_lock
###
if [ -f $defaults_file ]; then
opts="--defaults-file=$defaults_file"
fi
if [ -n $use_credentials ]; then
opts="$opts $use_credentials"
fi
sleep_time=$((timeout+10))
rm -f $lock_file
echo "$0 executing FLUSH TABLES WITH READ LOCK" | logger
mysql $opts -e "FLUSH TABLES WITH READ LOCK; system touch $lock_file; system nohup_
↪sleep
$sleep_time; system echo\ lock released|logger; " > /dev/null &
mysql_pid=$!
echo "$0 child pid $mysql_pid" | logger
c=0
while [ ! -f $lock_file ]
do
# check if mysql is running
if ! ps -p $mysql_pid 1>/dev/null ; then

```

(continues on next page)

(continued from previous page)

```
echo "$0 mysql command has failed (bad credentials?)" | logger
exit 1
fi
sleep 1
c=$((c+1))
if [ $c -gt $timeout ]; then
echo "$0 timed out waiting for lock" | logger
touch $lock_file
kill $mysql_pid
fi
done
echo $mysql_pid > $lock_file
exit 0
```

1. Save as PreFreeze.sh.
2. Configure the script as prefreeze script in the backup job.

Post-Thaw Script:

1. Use Editor
2. Copy the sample code

```
#!/bin/bash
lock_file=/tmp/mysql_tables_read_lock
###
mysql_pid=$(cat $lock_file)
echo "$0 sending sigterm to $mysql_pid" | logger
pkill -9 -P $mysql_pid
rm -f $lock_file
exit 0
```

1. Save code as Post-Thaw.sh
2. Configure post-thaw script in the backup job.

Tip

Adjust the timeout according to database size, in the sample script we have set 300 seconds for timeout

1.85.3 Cold Backup Database Shutdown:

In this option, Veeam will use pre and post-thaw script to stop and start the MySQL service using init.d or systemctl commands, depending on the database packages during the snapshot operations.

Pre-Freeze Script

1. Use Editor
2. Copy the sample code below

```
#!/bin/bash
timeout=300
if [ -f /var/run/mysqld/mysqld.pid ]
then
mysql_pid=$(cat /var/run/mysqld/mysqld.pid) >/dev/null 2>&1
```

(continues on next page)

(continued from previous page)

```

else
echo "$0 : Mysql not started or bad mysql pid file location" | logger
exit 1
fi
echo "$0 : Processing pre-freeze backup script" | logger
/etc/init.d/mysqld stop mysql & > /dev/null 2>&1
c=0
while [ true ]
do
if [ $c -gt $timeout ]
then
echo "$0 : timed out, mysql shutdown failed" | logger
exit 2
fi

# check if mysql is running
if [ -f /var/run/mysqld/mysqld.pid ]
then
echo "$0 : Waiting 5 more seconds for mysql shutdown" | logger
sleep 5
c=$((c+5))
else
echo "$0 : Mysql stopped" | logger
sync;sync
break

fi
done

```

1. Save code as Pre-Freeze.sh
2. Configure the script to run with backup job as pre-freeze script.

Post-Thaw Script:

1. Use Editor
2. Copy the sample code below

```

#!/bin/bash
timeout=300
echo "$0 : processing post-thaw backup script" | logger
if [ -f /var/run/mysqld/mysqld.pid ]
then
mysql_pid=$(cat /var/run/mysqld/mysqld.pid) >/dev/null 2>&1
echo "$0 : Mysql already started with PID $mysql_pid" | logger
exit 1
fi
/etc/init.d/mysqld start mysql & > /dev/null 2>&1
c=0
while [ true ]
do
if [ $c -gt $timeout ]
then
echo "$0 : timed out, mysql startup failed" | logger
exit 2

```

(continues on next page)

(continued from previous page)

```

fi
# check if mysql is running
if [ -f /var/run/mysqld/mysqld.pid ]
then
mysql_pid=$(cat /var/run/mysqld/mysqld.pid) >/dev/null 2>&1
echo "$0 : MySQL started with pid $mysql_pid" | logger
break
else
echo "$0 : Waiting 5 more seconds for mysql startup"
sleep 5
c=$((c+5))
fi
done

```

1. Save code as Postthaw.sh
2. Configure the backup job to run the script as Post Thaw Script.

1.86 Restore:

The restore is the integrated part of MySQL protection strategy. Veeam provides multiple option of MySQL restores depends on the backup method. Let's go through the option for each backup method.

1.86.1 Database Online Dump During Backup Operations:

For this backup option, Veeam provides following restore options depends on the failure:

Failure	Restore Option	-----	-----	Server Failed	Instant Server Restore	Database or Application
Level Failure	Guest File Level Restore	Database Item Level Restore	Veeam Universal Application Item Restore			

1.86.2 Online Dump to Staging server

In this backup job, Veeam provides following restore options

Failure	Restore Option	-----	-----	Database Restore	Instant File Level Restore
---------	----------------	-------	-------	------------------	----------------------------

Tip

In addition to online dump to staging server, take crash-consistency backup of mysql server and in case of server failure restore the mysql server from crash-consistency backup and use database dump from staging server to restore the database.

1.86.3 HotBackup Database Freeze.

For this backup option, Veeam provides following restore options depends on the failure:

Failure	Restore Option	-----	-----	Server Failed	Instant Server Restore	Database or Application
Level Failure	Guest File Level Restore	Database Item Level Restore	Veeam Universal Application Item Restore			

1.86.4 ColdBackup Database Shutdown.

For this backup option, Veeam provides following restore options depends on the failure:

| Failure | Restore Option | | | | Server Failed | Instant Server Restore | | Database or Application Level Failure | Guest File Level Restore | | Database Item Level Restore | Veeam Universal Application Item Restore

For more details about protection and restore use [MySQL Protection Whitepaper](#)

1.87 IBM Lotus Domino

Veeam supports the backup and restores of IBM Lotus Domino.

1.87.1 Background

To protect the Lotus Domino following files and folder are required to be backup:

- Domino server data files
- All databases
- Template files
- notes.ini file
- ID files
- Mail.box As IBM Lotus Domino is a non VSS-aware application, to take the consistent backup of Lotus Domino, we will use the methods explained in the next section.

1.87.2 Procedure:

In this section, we will create the scripts to be run to take a consistent backup of Lotus Domino. There are two methods to take backup of IBM Lotus Domino:

- Domino Online Backup.
- Domino Service Shutdown & Start.

Domino Online Backup:

This will close all the connection and write the RAM to the disk, but beware that client can reopen a database at any point in time, snapshot on average take 3-5 seconds select a time which is off-production when very fewer clients are connected. To use this option, follow the steps below:

1. Open a notepad
2. Copy the content in the notepad. `"" c:\Domino\nserver.exe -c "drop all" timeout /t 10 /nobreak c:\domino\nserver.exe -c "dbcache flush" timeout /t 30 /nobreak ""`
3. Save the file as "OnlineBackup.bat"

Copy the script to Veeam Backup Server, and configure the job to run it as pre-freeze . Please click on the link for more information about [VSS Scripts](#)

Domino Service Shutdown & Start:

In this method we will use commands to stop domino service as pre-freeze script and post-thaw script will start the domino services, it will have around 5-15 seconds downtime depends on the server performance. This method will ensure 100% consistency backup.

To use this option, follow the step below: Pre-Backup Script:

1. Open a notepad.
2. Copy the contents: `" net stop "Lotus Domino Server (DominoData)" "`
3. Save the file as "PreFreezeScript.bat" Post-Thaw Script:
4. Open a notepad.
5. Copy the contents: `" net start "Lotus Domino Server (DominoData)" "`
6. Save the file as "post-thaw.bat"

Copy the scripts to Veeam Backup Server, and configure the job to run pre-freeze and post-thaw scripts. Please click on the link for more information about [VSS Scripts](#)

1.87.3 Restores:

Restores is the integrated part of IBM Lotus Domino protection, Veeam offers followings option to restore IBM Lotus Domino Server:

1. Instant Server Restore – Instant VM Recovery.
2. Instant Individual Emails Restore.

###Instant Server Restore – Instant VM Recovery: In case of complete server failure, you can use Veeam Instant VM Restore to bring back the Domino server in less than 15 mints*

Instant Individual Emails Restore:

In order to recover the individual emails, please follow the steps below:

1. Install a Note Client. (User should have full access to production database)
2. Start Instant File Level Restore.
3. Access NSF files under the c:\VeeamFLR path and subfolders (All Domino Server Disks are mounted on this path).
4. Select the emails and copy back to production mailbox.
5. If DAOS enabled on the Domino Server, You can search the missing file and restore with Veeam Instant File Level Restore. For more information please check [Lotus KB](#)

Note:

Currently, there is no option to work with Domino Log files, you may consider changing transaction logging to circular logging follow >the [Lotus KB](#) to change the transaction logging option

1.88 SAP HANA

Veeam provides following options to protect SAP HANA Environment:

- Virtual Machine running SAP HANA Database – Agentless Virtual Machine Image Level Backup.
- Physical Server running SAP HANA Database – Agent based backup.

1.89 SAP HANA Backup Options:

SAP HANA comes with native functionality for backup and recovery and provide different options to backup SAP HANA Environment.

There are three backups options in HANA:

- File System Backup
- Backint API
- Storage Snapshot.

Note

Veeam supports **Storage Snapshot** based backup of SAP HANA Database.

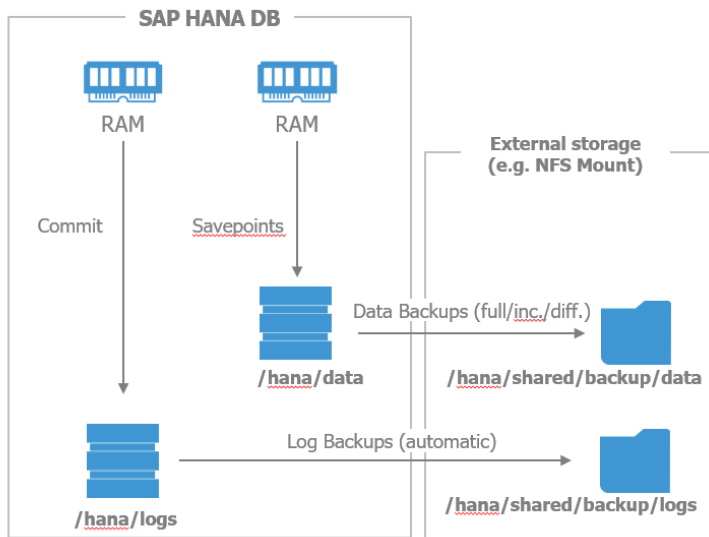
1.89.1 File Backup:

With the file backup option, customer can backup data and logs to file system.

Backup can be triggered using:

- SAP HANA Cockpit.
- SAP HANA Studio.
- SQL Commands.
- DBA cockpit.

File backup



Full/inc./diff. backup can be started:

- Manually at HANA Studio
- SQL script (manual/external scheduler)
- SAP DBA Cockpit (external scheduler)

Log backup will run automatically as defined in global.ini of SAP HANA

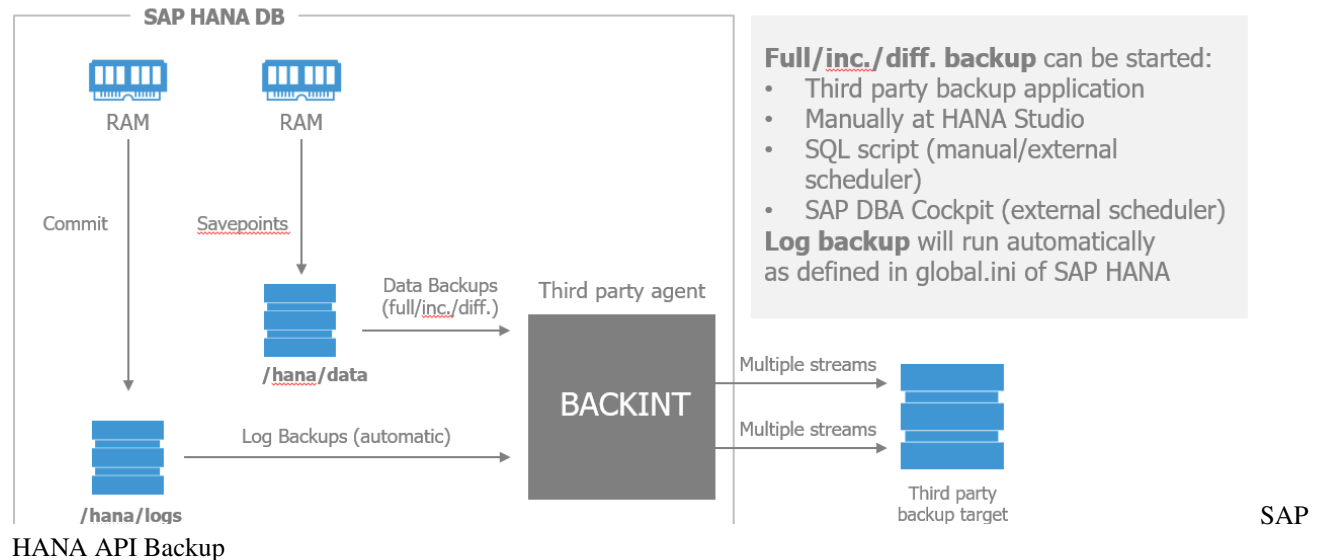
SAP

HANA FILE Backup

1.89.2 Backint API:

SAP HANA provides an option to use third-party backup tools to communication with SAP HANA database through Backint API for SAP HANA.

BACKINT



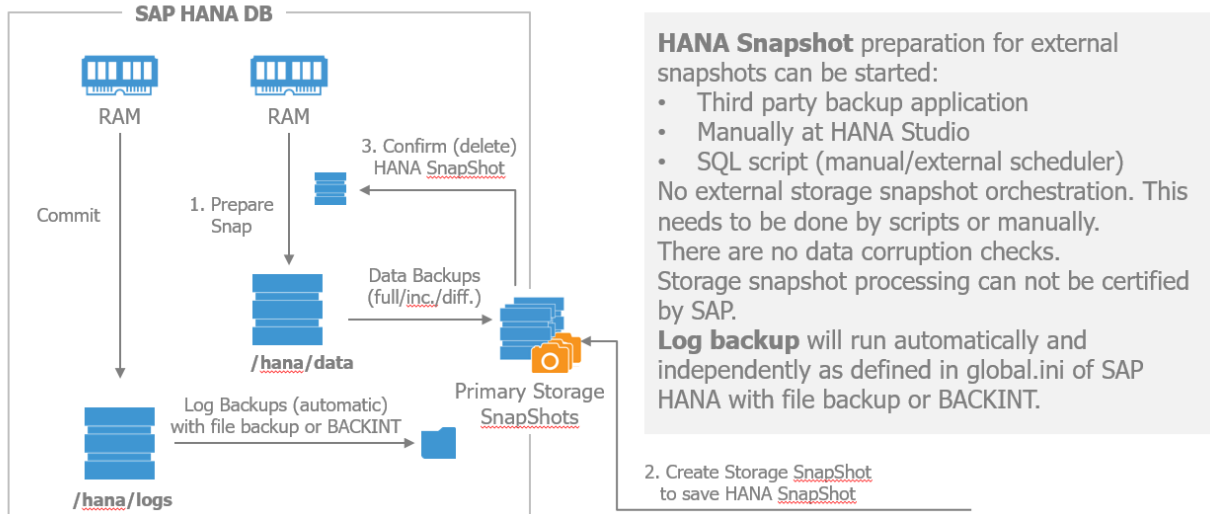
1.89.3 Storage Snapshot:

Storage snapshot allows to take backup of SAP HANA Database.

A storage snapshot created in three steps:

- PREPARE
- CONFIRM
- ABANDON (* Only if there was an error in the creation of the snapshot *)

Snapshot



SAP

HANA Snapshot Backup

Note

Snapshots are not part of the **Backint API specification**, and **currently no certification is required for 3rd party tools using HANA snapshots**

1.90 Virtual Machine running SAP HANA Database Backup:

Veeam uses HANA database snapshot backup method by using Veeam guest processing **Pre & Post Thaw Scripts** Virtual HANA Backup with Agentless Image Level Backup: Veeam Backup & Replication uses the scripts **Pre & Post Thaw Scripts** which allow the execution of the backups via HANA Snapshot and also provide option to purge the transactions logs.

The Pre & Post Thaw scripts can be download from [VeeamHub](#)

1.90.1 Configure Backup:

1. **Create Backup Job**
2. Select SAP HANA VM to Backup.
3. At the **Guest Processing step**, click **Applications**.
4. Click the **Scripts tab**.
5. In the **Linux Scripts** section, specify paths to **SAP HANA BACKUP [Pre-Freeze and Post-Thaw Scripts]** (https://helpcenter.veeam.com/docs/backup/vsphere/backup_job_vss_scripts_vm.html?ver=95).

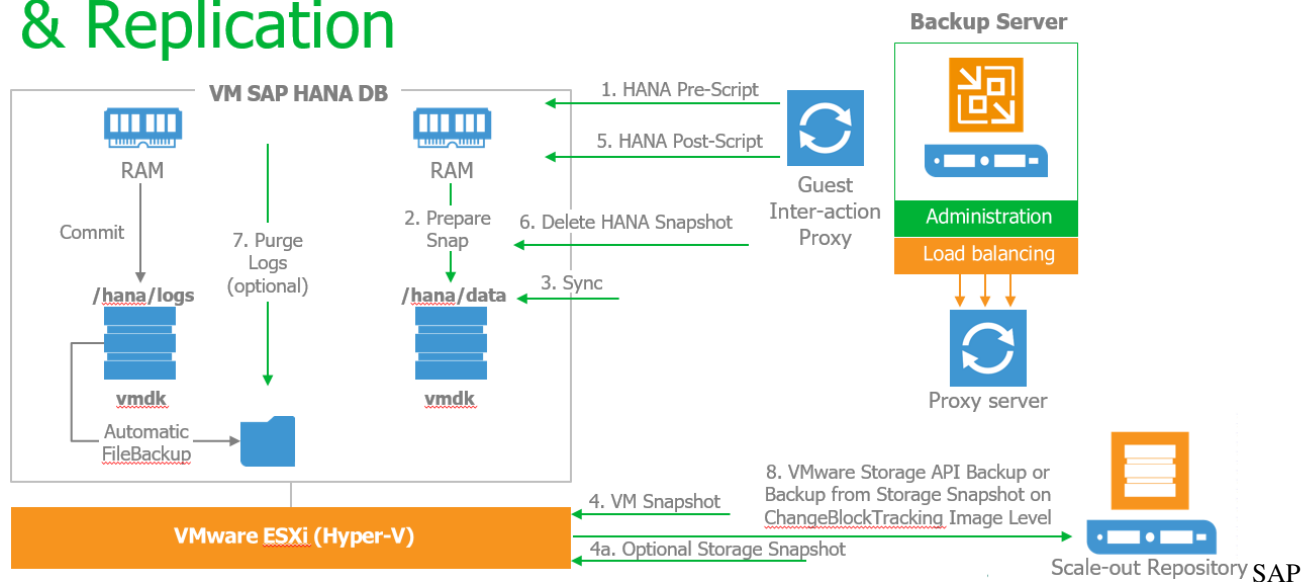
1.90.2 SAP HANA Backup Process:

Please find below the process to backup Virtual Machine with SAP HANA DB:

1. Veeam Backup Server execute the *HANA Pre-freeze Script* to prepare the internal snapshot of the SAP HANA database.

2. Prepare Snap.
3. The data will be synchronized and the pointers of the Transaction Logs and the internal SAP HANA backup catalog will be updated to confirm the snapshot
4. Veeam will create Virtual Machine Snapshot.
5. Veeam Backup Server execute the *HANA Post-Freeze Script*
6. Removal of the HANA Snapshot to save system space
7. Optionally Purge transaction logs through the script.
8. Data transfer to the Veeam repository.

HANA backup with Veeam Backup & Replication



HANA Virtual Machine Backup

1.91 SAP HANA Backup with Veeam Agent for Linux:

Similar to agentless virtual machine image based backup, Veeam Agent for Linux will use the same [Pre & Post-Thaw Scripts] (https://helpcenter.veeam.com/docs/backup/vsphere/backup_job_vss_scripts_vm.html?ver=95) scripts.

1.91.1 Configure SAP HANA Physical Server Backup:

Install Veeam Agent for Linux to SAP HANA Physical Server, configure the [backup job] https://helpcenter.veeam.com/docs/agentforlinux/userguide/backup_job_create.html?ver=20 and use **script settings** select Snapshot scripts to configure **Pre Freeze & Post-Thaw Script**

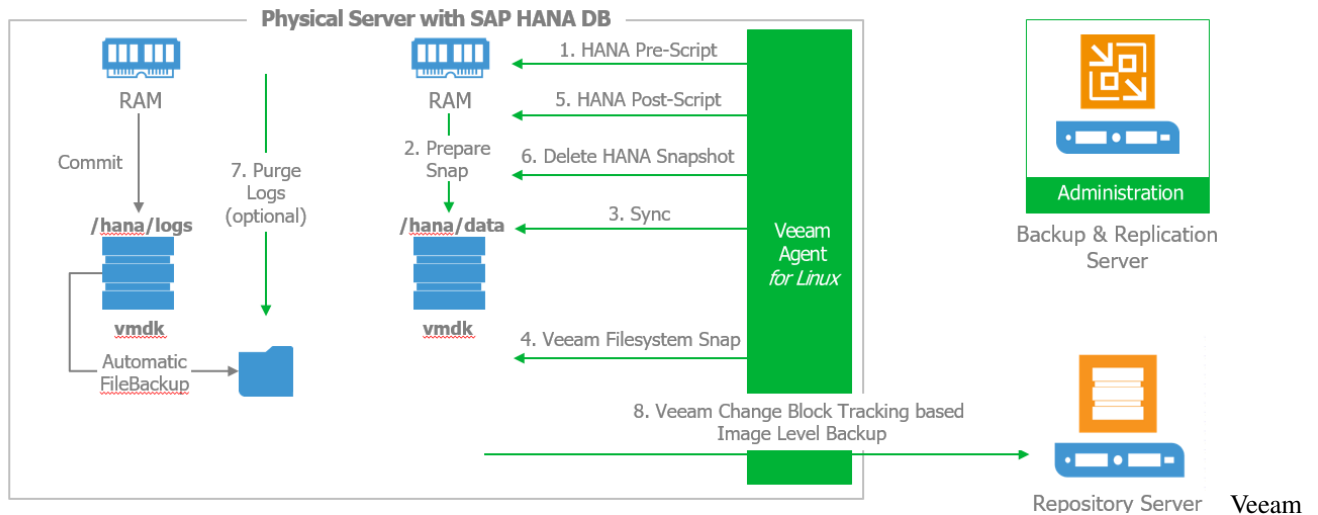
1.91.2 SAP HANA Backup Process:

Please find below process to backup Physical Server with SAP HANA DB:

1. Veeam Agent execute the *HANA Pre-freeze Script* to prepare the internal snapshot of the SAP HANA database.

2. Prepare Snap.
3. The data will be synchronized and the pointers of the Transaction Logs and the internal SAP HANA backup catalog will be updated to confirm the snapshot
4. Veeam agent create the file system snapshot.
5. Veeam Agent execute the *HANA Post-Freeze Script*
6. Delete HANA Snapshot.
7. Optionally Purge transaction logs through the script.
8. Veeam Change Block Tracking based Image Level Backup.

HANA backup with Veeam Agent for Linux



Agent for Linux SAP HANA Backup

1.92 Permissions:

For the standard username/password in the script user should have following privileges in SAP HANA environment:

- Backup Admin.
- Catalog Read.

More about [user, roles and privileges] (<https://help.sap.com/viewer/742945a940f240f4a2a0e39f93d3e2d4/2.0.01/en-US/45955420940c4e80a1379bc7270cead6.html>)

1.93 SAP HANA Pre-Freeze Script Configuration Options:

Starting with version 1.0 the script supports the use of an external config file. While it's still possible to manually set the username, password, keyprefix, purgelogs and purgedays options directly in the script, using a config file has the advantage that future updates to the script can be implemented without any changes to the file and the same exact script can be run on many different servers with the config options stored locally on each HANA server.

By default the script checks for the config file in the path /etc/veeam/hana.conf but this can be overridden with the -c parameter

1.93.1 User & Secure User Store Authenticaiton:

The script can use standard username/password or Secure User Store Authentication Secure User Store requires a key for each instance which must be configured outside of this script using hdbuserstore executable (part of hdbclient install).

To use standard Username and Password set these, otherwise leave them empty username="" password=""

To use Secure User Store for SAP HANA authentication select a key prefix. This prefix will be combined with the instance number to reference a specific key for authentication. For example, the default prefix is HDB, so for HANA instance 00 the script will attempt to use key HDB00 to authenticate.

create Secure User Store use the following command syntax: ./hdbuserstore set :3<instance#>15

For example, to create keys for instance 00 and 01 on host "hana01" using a username "VEEAM" and password "Backup123" run the following commands as the OS user that will be running the script to create their secure store: ./hdbuserstore set HDB00 hana01:30015 VEEAM Backup123 ./hdbuserstore set HDB01 hana01:30115 VEEAM Backup123

1.93.2 Additional configurable options:

ursrap=/usr/sap Path to sapservices file/HANA install path timeout=30 Maximum number of seconds to wait for snapshots to enter prepared state keyprefix="HDB"

1.94 SAP HANA Post-Thaw Script Configuration Options:

1.94.1 User & Secure User Store:

To use standard Username and Password set these, otherwise leave them empty

```
username=""  
password=""
```

To use Secure User Store for SAP HANA authentication select a key prefix.This prefix will be combined with the instance number to reference a specific key for authentication. For example, the default prefix is HDB, so for # instance 00 the script will attempt to use key HDB00 to authenticate.

To create Secure User Store use the following command syntax: ./hdbuserstore set <key> <host>:3<instance#>15 <user> <password>

For example, to create keys for instance 00 and 01 on host "hana01"

using a username "VEEAM" and password "Backup123" run the following commands as the OS user that will be running the script to create their secure store ./hdbuserstore set HDB00 hana01:30015 VEEAM Backup123 ./hdbuserstore set HDB01 hana01:30115 VEEAM Backup123

For HANA 2.0 SP1 and higher, which are always installed as multi-tenant databases even when a single tenant is in use, you must specify that the connection use the port of the SYSTEMDB as follows:

```
./hdbuserstore set HDB00 hana01:30113@SYSTEMDB VEEAM Backup123
```

For more information about keystore use please refer to the [SAP HANA documentation](#)

Additional configurable options

usrsap=/usr/sap> Set to HANA install path keyprefix="HDB"

Note

Other than the above-mentioned parameters only if applicable script should not be modified unless a special configuration is required.

1.94.2 Verify Veeam HANA Backup via SAP HANA Studio:

You can verify the Veeam HANA Database backup from SAP HANA Studio as shown in the figure below:

Backup Catalog

☐ Show Log Backups ☐ Show Delta Backups

Status	Started	Duration	Size	Backup Type	Destination...
✓	16-08-2017 1:25:49	00h 00m 12s	3,06 GB	Data Backup	Snapshot
✓	15-08-2017 14:25:49	00h 00m 06s	3,06 GB	Data Backup	Snapshot
✓	15-08-2017 1:48:34	00h 00m 05s	3,05 GB	Data Backup	Snapshot
✓	15-08-2017 1:13:36	00h 02m 56s	3,06 GB	Data Backup	Snapshot
✓	15-08-2017 0:23:06	00h 00m 10s	3,06 GB	Data Backup	Snapshot
✓	14-08-2017 20:55:49	00h 00m 13s	3,06 GB	Data Backup	Snapshot

Backup Details

ID: 1502857549607
 Status: Successful
 Backup Type: Data Backup
 Destination Type: Snapshot
 Started: 16-08-2017 1:25:49 (America/Santiago)
 Finished: 16-08-2017 1:26:02 (America/Santiago)
 Duration: 00h 00m 12s
 Size: 3,06 GB
 Throughput: n.a.
 System ID:
 Comment: Veeam Backup Pre-Freeze - Wed Aug 16 01:25:49 -03 2017
 Additional Information: <ok>
 Location: /hana/data/HDB/mnt00001/

Host	Service	Size	Name	Source Type	EBID
demop	xsengine	144,00 MB	hdb00002	volume	Veeam...
demop	nameserver	144,00 MB	hdb00001	volume	Veeam...
demop	indexserver	2,78 GB	hdb00003	volume	Veeam...

HANA Studio

1.95 Restore:

Restore is the integrated part of SAP HANA protection, Veeam provides various restore option to restore SAP HANA environment.

- Virtual SAP HANA Restore.
- Physical SAP HANA Restore.

1.95.1 Virtual Machine running SAP HANA Database Restore:

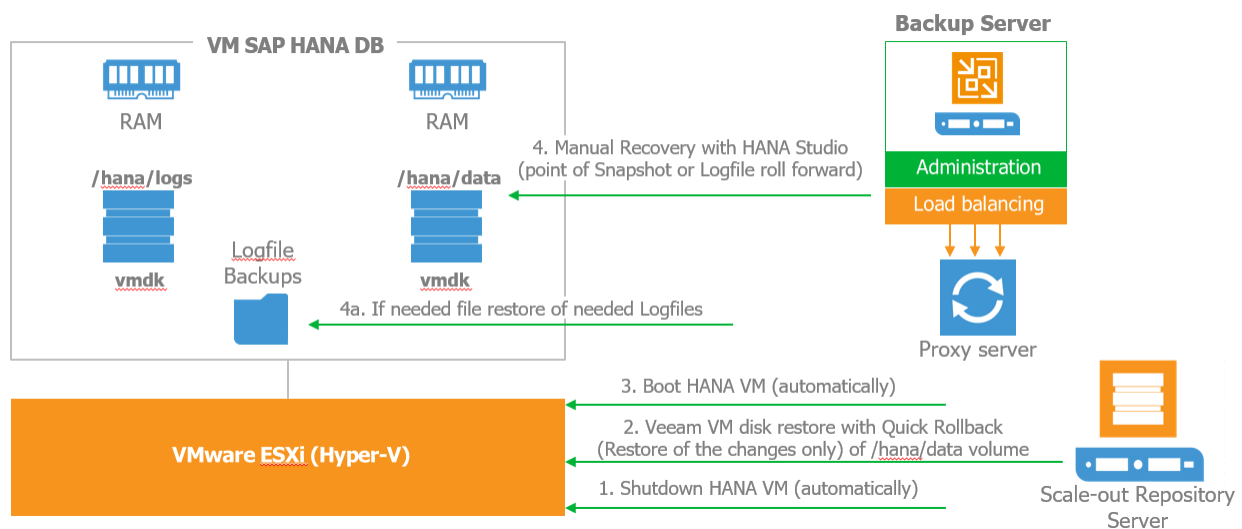
Veeam provides following options to restore Virtual SAP HANA Environment:

- Entire VM Restore (with Quick Rollback to restore only disk blocks with changes)
- Instant VM Recovery.

1.95.2 Entire VM Restore (Quick RollBack to restore only disk blocks with changes)

In event of database corruption or revert back the changes in the database, use the option to restore disk, below is the SAP HANA database restore process: Figure 1.0

1. The Virtual machine is turned off through the disk recovery of Veeam Backup & Replication.
2. Recovery of the disk by enabling “Quick Rollback” in the recovery task.
3. When you finish recovering only the blocks that have changed, the virtual machine is turned on.
4. Open HANA Studio and select Restore Method including point in time Figure 1.1
5. HANA Studio will show the restored database point with a green point and will recover the database to it. Figure 1.2
6. HANA Will apply all log files to the point selected in the HANA studio restore wizard



Figure

1.0

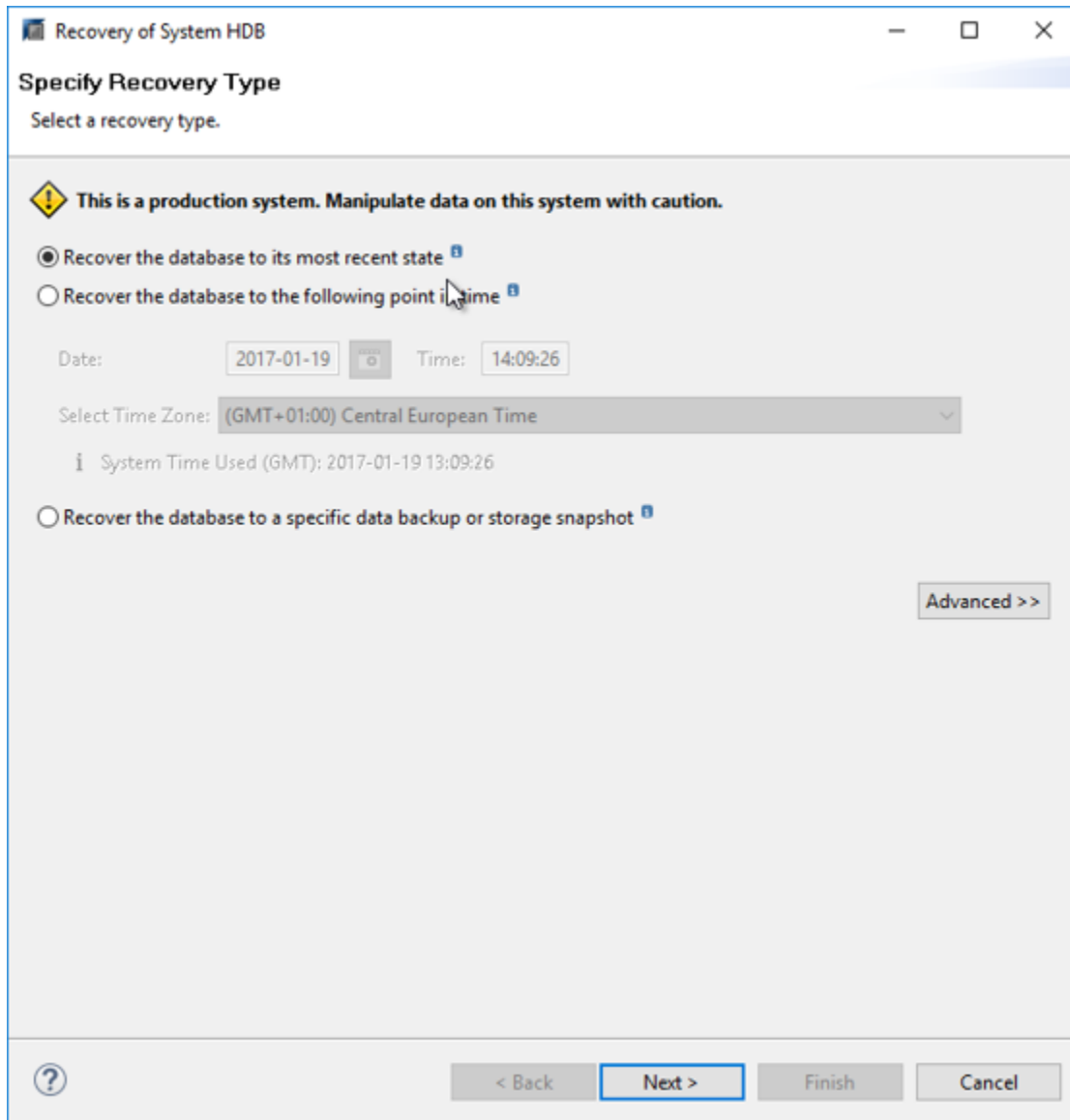


Figure 1.1

Recovery of System HDB

Select a Backup

Select a backup to recover the SAP HANA database

Backups

The overview shows backups that were recorded in the backup catalog as successful.

Start Time	Location	Backup Prefix	Available
2017-08-15 19:37:25	/hana/data/HDB	SNAPSHOT	●
2017-08-15 14:25:49	/hana/data/HDB	SNAPSHOT	✗
2017-08-15 01:48:34	/hana/data/HDB	SNAPSHOT	✗
2017-08-15 01:13:36	/hana/data/HDB	SNAPSHOT	✗
2017-08-15 00:23:06	/hana/data/HDB	SNAPSHOT	✗
2017-08-14 20:55:49	/hana/data/HDB	SNAPSHOT	✗

Refresh Show More

Details of Selected Item

Start Time: 2017-08-15 19:37:25 Destination Type: SNAPSHOT Source System: HDB

Size: 3,06 GB Backup ID: 15028366450 External Backup ID: Veeam Backup Post-Thaw

Backup Name: /hana/data/HDB

Alternative Location:

Check Availability

< Back Next > Finish Cancel

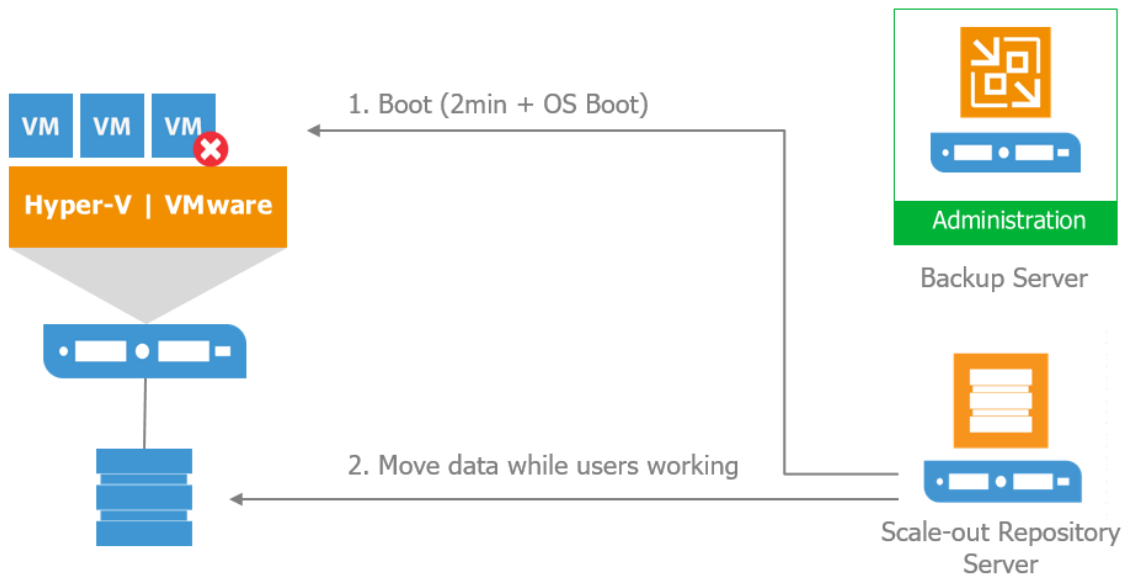
Figure

1.2

1.95.3 Instant VM Recovery

In the event of complete disaster, you can use [Instant VM Recovery](#) to restore SAP HANA Virtual Machine in less than 15 mins SAP HANA will be able to provide services again**, below is the process to restore SAP HANA with [Instant VM Recovery](#) See Figure 1.3

1. Veeam through vPower NFS is presented as a repository on the host containing the virtual machine backup point. And turn on the virtual machine in the infrastructure.
2. Data is then migrated online without affecting the SAP services directly to the production storage. Therefore, in less than 15 minutes SAP HANA will be able to provide services again in case of disaster.



Instant

VM Recovery SAP

1.95.4 Physical Server running SAP HANA DB Restore.

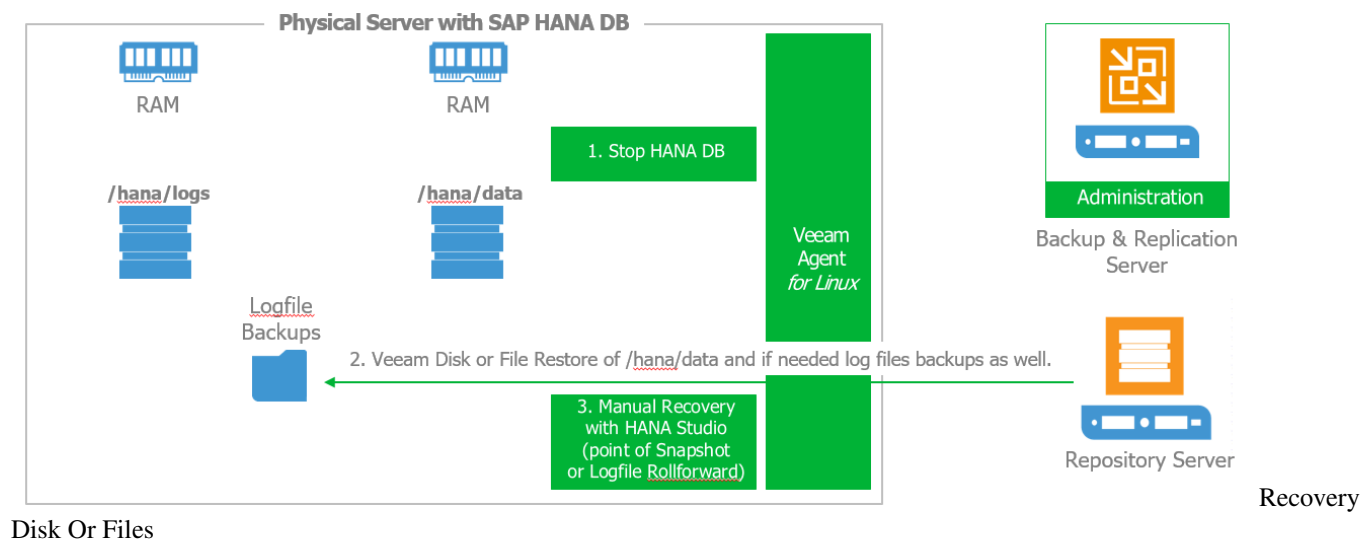
Veeam provides following option to recover Physical Server running SAP HANA database:

- Recover Disk or Files
- Bare-Metal Recovery

1.95.5 Restore Disk or Files:

Please follow the restore procedure explained in [Veeam Agent for Linux Guide](#)

1. Stop SAP HANA services
2. Recover disk volume, files or logs if necessary
3. Recovery process in SAP HANA Studio as explained in section Entire VM Restore.



1.95.6 Bare-Metal Restore:

Please follow the restore procedure explained in [Veeam Agent for Linux guide](#)

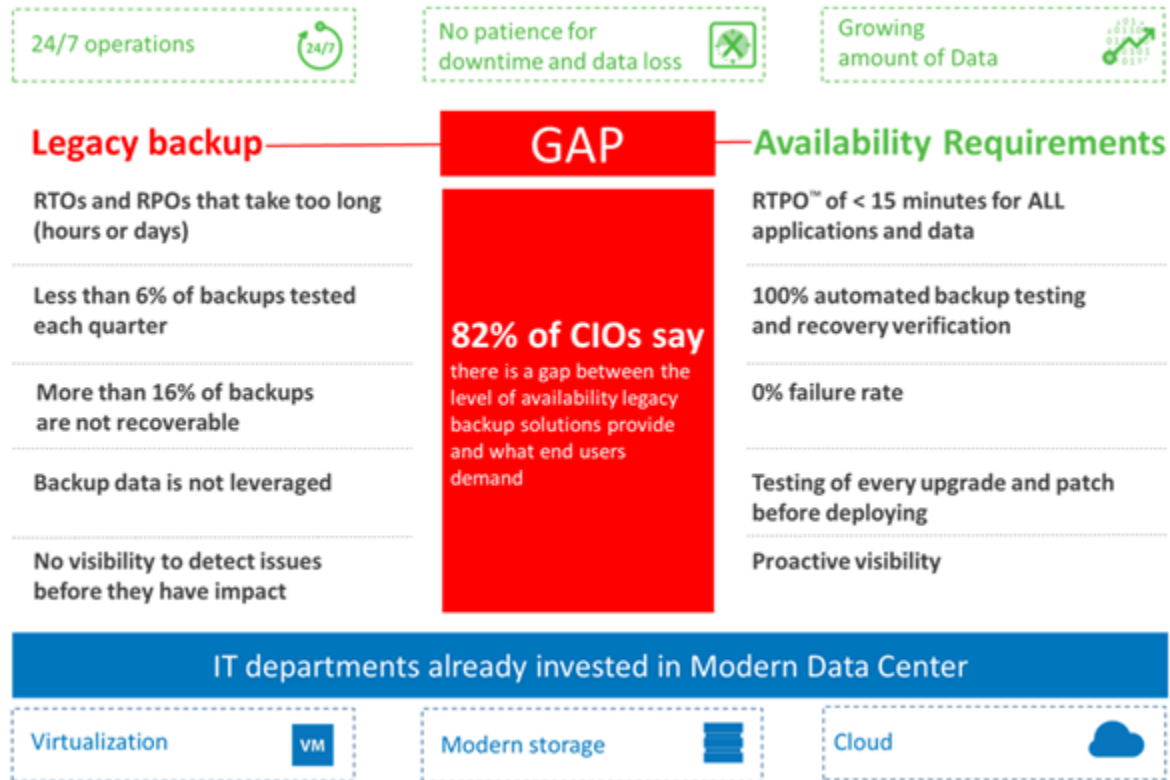
1.96 POC Guide

Organizations are modernizing their data centers in order to provision IT services faster, strengthen security and control, and lower operational costs. While building modern data centers, organizations invest in server virtualization, modern storage applications and cloud-based services. However, businesses are facing new demands from end users including access to data and applications 24/7, no patience for downtime or data loss, and exponential data growth at more than 50% per year.

This opens a gap—an availability gap—between the requirements of the Always-On Business™ and IT's ability to effectively deliver availability. In fact, 82% of CIOs say there is a gap between the level of availability they provide and what end users demand.

Veeam bridges this gap by providing customers a new kind of solution – Availability for the Modern Data Center, which delivers RTPO of < 15 minutes for all applications and data.

Organizations now can leverage their investments in the modern data center to meet new demands of the always-on business.



The

Availability Gap

This section of the document will demonstrate how Veeam solutions can be used throughout an entire datacenter availability project, beginning with the first assessment phase, to the project implementation from a technical perspective.

Note: While these guidelines focus on enterprise customers with more than 100 hosts or 1,000 virtual machines, Veeam Availability Suite is applicable to any infrastructure size.

1.97 Assessment

Before starting a project, it is very important to understand customers' needs, vision and the IT environment. While the first two can be the outcome of an initial project meeting, the IT environment can be analyzed with Veeam ONE, which is part of the Veeam Availability Suite.

The following information is very important and can help to streamline the project and proactively prevent situations that impact the environment:

1.97.1 Veeam ONE Monitor

Alerts tab

Check the Alerts tab of Veeam ONE Monitor if there are specific errors that need to be addressed **before** you bring extra load to the environment with backup processing that can cause business critical situations. Use "All Deployment Projects" area in the Reporter tool when planning to add extra resource into the environment, this will give a good indicator of the effect the new systems will make to the current setup.

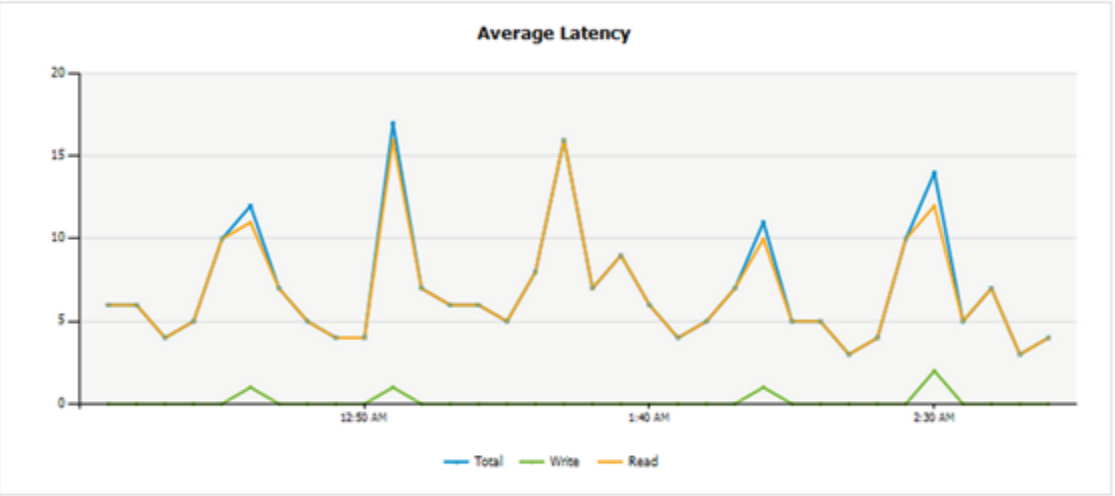
1.97.2 Veeam ONE Reporter

Storage Latency

Datastore Datacenter01\esx32-ds1 Details

Latency

Datastore Average Latency (milliseconds)				
Latency	Average	Minimum	Maximum	Trend
Total	6.97	3	17	Decreasing
Write	0.15	0	2	Increasing
Read	6.82	3	16	Decreasing



Total Latency by Host (milliseconds)					
Latency	Host	Average	Minimum	Maximum	Trend
Total	vcenter02\esx32.veeam.local	6.97	3	17	Decreasing
Write	vcenter02\esx32.veeam.local	0.15	0	2	Increasing
Read	vcenter02\esx32.veeam.local	6.82	3	16	Decreasing

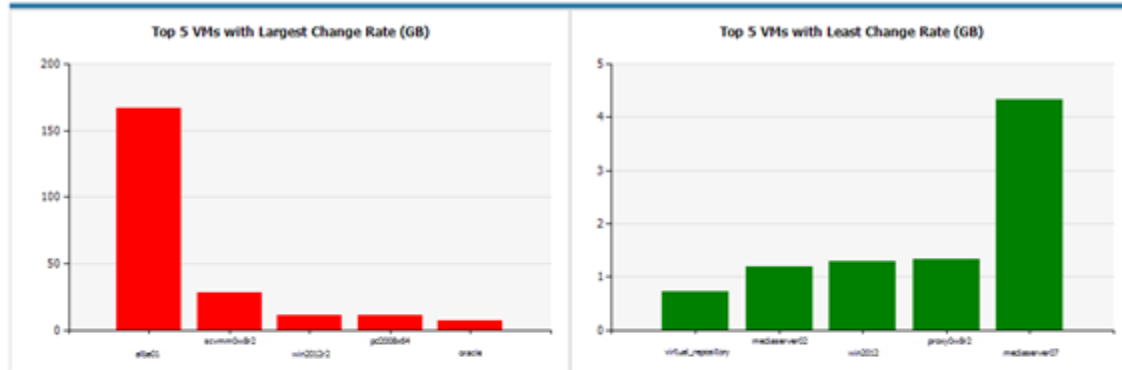
ONE Reporter - Storage Latency

This report will help you identify storage systems that are under heavy pressure or at its maximum load. Let Veeam ONE run at least 24 hours and check if there are high latency situations.

Veeam

Change Rate Estimation

Summary



Details

Scope	VM	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	Total
clb0wdr2	10	57.82 GB	12.81 GB	11.03 GB	123.50 GB	8.73 GB	9.07 GB	10.87 GB	233.82 GB
	alt02	47.70 GB	2.68 GB	< 1 GB	114.59 GB	< 1 GB	< 1 GB	1.85 GB	166.96 GB
	scmm0wdr2	3.86 GB	4.02 GB	4.11 GB	3.96 GB	4.17 GB	4.39 GB	3.96 GB	28.47 GB
	win2012r2	2.55 GB	2.29 GB	2.73 GB	1.06 GB	< 1 GB	< 1 GB	1.15 GB	11.37 GB
	pd2008r4	1.44 GB	1.59 GB	1.66 GB	1.44 GB	1.80 GB	1.43 GB	1.81 GB	11.17 GB
	oracle	0.99 GB	1.02 GB	1.03 GB	1.03 GB	< 1 GB	1.08 GB	1.04 GB	7.00 GB
	mediaserver07	< 1 GB	< 1 GB	< 1 GB	< 1 GB	< 1 GB	< 1 GB	< 1 GB	4.32 GB
	prsv0wdr2	< 1 GB	< 1 GB	< 1 GB	< 1 GB	< 1 GB	< 1 GB	< 1 GB	1.33 GB
	win2012	< 1 GB	< 1 GB	< 1 GB	< 1 GB	< 1 GB	< 1 GB	< 1 GB	1.29 GB
	mediaserver02	< 1 GB	< 1 GB	< 1 GB	< 1 GB	< 1 GB	< 1 GB	< 1 GB	1.19 GB
Total:		57.82 GB	12.81 GB	11.03 GB	123.50 GB	8.73 GB	9.07 GB	10.87 GB	233.82 GB

Veeam

ONE Reporter - Change Rate Estimation

This report will help you identify VMs with a high change rate at the block level (relevant for incremental backups). You can later configure the backup or replication job to process them at the beginning of the backup window, to address the longer job runtimes. In general, this report will give you numbers for backup target storage planning.

Infrastructure Overview



Infrastructure Overview

Description

This report provides general inventory configuration information, including all vCenter servers, clusters, hosts, VMs, datastores, and networks in your virtual environment.

Report Summary

Report Created: 12/19/2014 4:09 PM
 Hosts per Cluster: 3.4
 VMs per Host: 33.1
 Datastores per Host: 2.6
 VMs per Datastore: 12.5

vCenter Servers

vCenter Servers								
vCenter Servers	Datacenters	Clusters	Shared Datastores	Virtual Machines	Hosts	Physical CPU(GHz)	Physical Memory(GB)	Datastore Capacity(TB)
vcenter02	1	1	0	188	3	71.96	159.9	29.35
172.16.16.168	2	3	4	21	8	112.83	125.53	8.28
vcenter01	2	0	6	337	4	81.44	191.79	31.73
cloudvc.veeam.local	1	1	0	16	2	8.4	16	0.38
Total	6	5	10	562	17	274.64	493.22	69.73

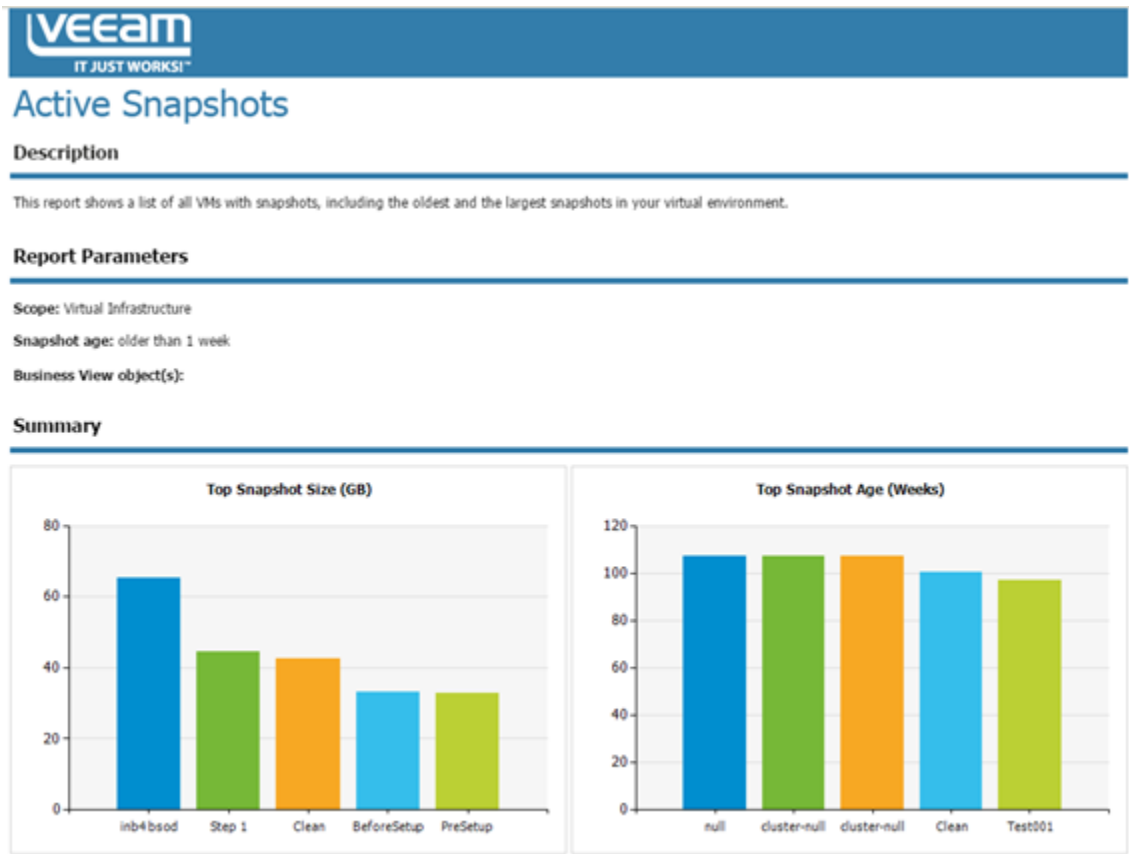
Clusters

Clusters								
Name	Hosts	vCenter Server	Total Memory(GB)	Total CPU(GHz)	Total Storage(TB)	DRS Status	DRS Automation Level	HA Status
DRS-HA Cluster	2	172.16.16.168	14	23.94	2.02	enabled	manual	enabled
PROD1 Cluster	3	172.16.16.168	47.99	66.55	2.97	disabled		disabled
PROD2 Cluster	2	172.16.16.168	31.6	12.76	2.57	disabled		disabled
Core	2	cloudvc.veeam.local	16	8.4	0.38	enabled	fullyAutomated	disabled
VSAN Cluster01	3	vcenter02	159.9	71.96	14.52	enabled	fullyAutomated	disabled

Veeam

ONE Reporter - Infrastructure Overview


Active Snapshots



ONE Reporter - Active Snapshots

VMware snapshots are often done to save a specific state of the VM for some time. While they are created very easily, administrators forget to delete them over time. Together with administrators, you can release all snapshots that are not needed anymore. This will help prevent datastore downtimes because of snapshots filling up the whole physical storage.

Orphaned Snapshots



IT JUST WORKS!™

Orphaned VM Snapshots

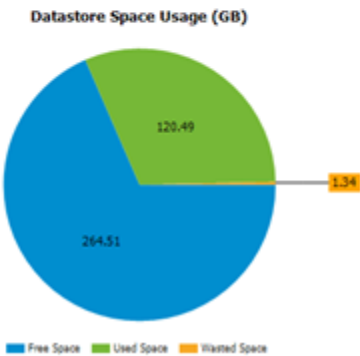
Description

This report provides information on VM snapshots that are located on the datastores and are not visible to the Snapshot Manager.

Report Parameters

Scope: cloudvrc.veeam.local
Datastores: All Datastores

Summary

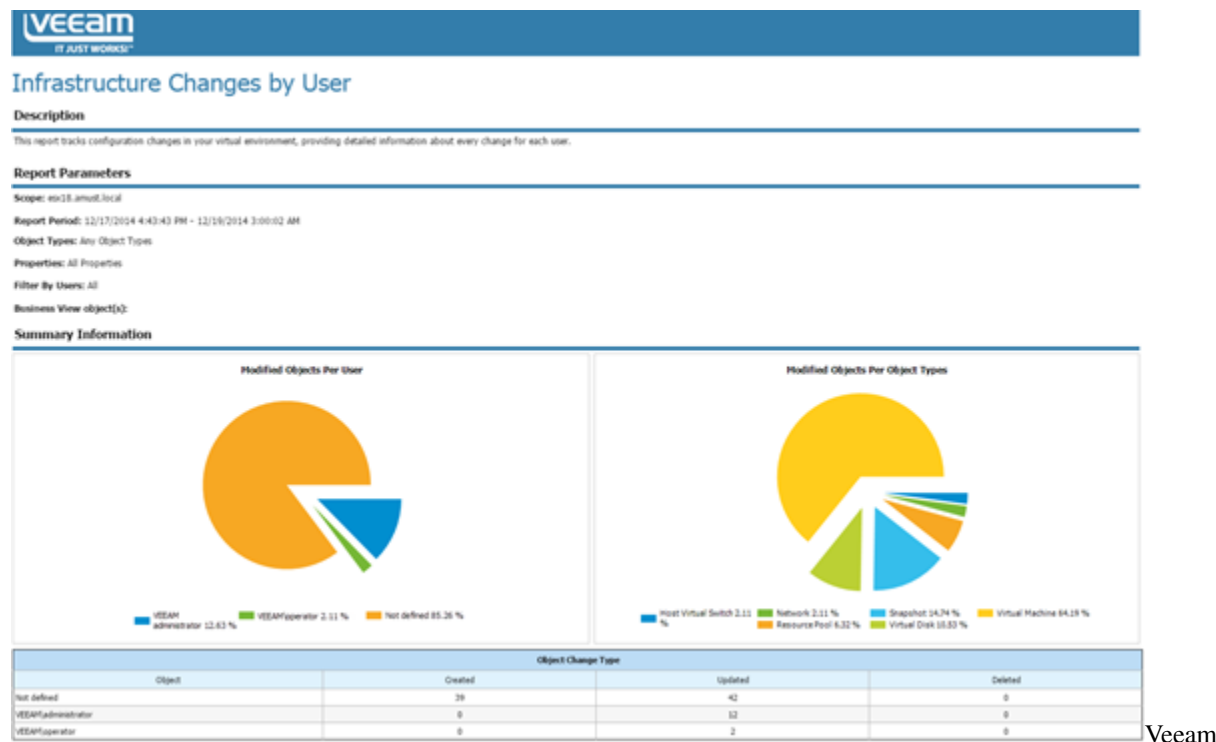


Veeam

ONE Reporter - Orphaned Snapshots

This report detects VM snapshots that are still active on data stores but do not show up in the VMware Snapshot Manager. Veeam Backup & Replication and its Snapshot Hunter will correct this situation by consolidating these snapshots, which can bring extra load at the first backup POC. We strongly recommend that you tune the VMware environment and consolidate all orphaned snapshots before you start a Backup & Replication project.

Infrastructure Changes by User



ONE Reporter - Infrastructure Changes by User

In the later POC phase, create a separate account for a VMware user and use this account for all authentication operations in Veeam Backup & Replication. With the Infrastructure Changes by User report, you can track and document all changes done by this user.

Inventory

Change Details

Who Changed	Change Type	Object Type	Object Location	Object Name	When Changed	Property	New Value	Old Value
[-] VEEAM\administrator								
	[-] Modified							
		Virtual Machine	>vcenter01>Columbus>esx18.veeam.local	srv07	12/18/2014 4:38:53 PM	Tools: Status	OK	not running
			>vcenter01>Columbus>esx18.veeam.local		12/18/2014 4:38:53 PM	Computer name	srv07.qahv1.veeam.local	Not set
			>vcenter01>Columbus>esx18.veeam.local	srv02	12/19/2014 2:52:00 AM	Power state	poweredOn	poweredOff
			>vcenter01>Columbus>esx18.veeam.local		12/19/2014 2:52:00 AM	CD/DVD: Is mounted	True	False
			>vcenter01>Columbus>esx18.veeam.local		12/19/2014 2:52:00 AM	Tools: Status	out of date	not running
			>vcenter01>Columbus>esx18.veeam.local		12/19/2014 2:52:00 AM	Computer name	srv02.dev.amust.local	Not set
			>vcenter01>Columbus>esx18.veeam.local	srv08	12/18/2014 3:55:42 PM	CD/DVD: Is mounted	True	False
			>vcenter01>Columbus>esx18.veeam.local		12/18/2014 3:55:42 PM	Power state	poweredOn	poweredOff
			>vcenter01>Columbus>esx18.veeam.local		12/18/2014 3:55:42 PM	Tools: Status	out of date	not running
			>vcenter01>Columbus>esx18.veeam.local	l-ds01	12/18/2014 11:26:35 PM	Network Adapter: IP	fe80::e132:1a5a:67fc:3a5c, 172.16.14.203	fe80::e132:1a5a:67fc:3a5c, 172.16.15.45
			>vcenter01>Columbus>esx18.veeam.local		12/18/2014 11:26:35 PM	Power state	poweredOn	poweredOff
			>vcenter01>Columbus>esx18.veeam.local		12/18/2014 11:26:35 PM	Tools: Status	OK	not running

ONE Reporter - Inventory

This report provides the most complete and up-to-date configuration information on all objects in the virtual environment. It can be used offline at the planning phase to address any virtual infrastructure-related questions.

There are many additional interesting reports in the Veeam Availability Suite.

Check out the [VMware Optimization](#) or [Hyper-V Optimization](#) sections of Veeam ONE Reporter. A good example is

the Garbage Files Report that can identify possible wasted space on data stores. In some cases, it helped to free up 10 TB+ of space on the tier 1 storage.

1.98 Accelerated Evaluation

Many customers decide to do a small scale Proof of Concept (POC) after seeing their first live demonstration and presentation in meetings with partners and/or Veeam System Engineers. The idea is to get started with the interface of Veeam Backup & Replication and to test if everything works as expected/presented within your environment.

As enterprise environments are sometimes very complicated from the firewall and storage perspective, in most cases customers decide to do a POC in small test environments. Typically, a test environment includes:

- ESXi hosts & vCenter Server *And/Or* Hyper-V hosts & Microsoft System Center Virtual Machine Manager
- All-in-one Veeam Backup & Replication, Veeam Proxy & Veeam Repository server
- 10-20 VMs running various business applications

It is possible to carry out a Veeam Backup & Replication POC in such environment with only a single Veeam backup server on a VM with 8 cores and 8-16GB of RAM. (Since this test is focused on the user interface experience, no special preparation is needed from the performance perspective.)

Customers often drive this POC themselves. To assist customers with this task, Veeam has published a good Evaluator's Guide that includes configuration screenshots with minimal required background information.

One thing to remember when running a POC with Veeam is that you want to test something with meaning, testing a backup because it backs up is important however having a goal is also important.

Even for a small POC, a plan is essential, a write up can be as simple as:

- How many machines, set a specific number and record their names.
- What applications are you testing and why, what is the criteria for success on each machine.
- What types of recovery are you going to test and why (Veeam currently has 57 ways to recover).
- What are your expectations from the testing process.
- What functionality do you want to see in action.

We all know Veeam will protect virtual machines, the aim of your POC should be to see how well it lives up to your expectation at doing specific types of protection and recovery.

See Veeam HelpCenter for Evaluator's Guides:

- [VMware vSphere environments](#)
- [Microsoft Hyper-V environments](#)

1.99 Enhanced Evaluation

Based on the information gathered during the assessment phase and customer requirements, you may design a solution on paper and possibly implement it. Most likely such designs are going to change over multiple revisions during the implementation phase after communicating with other departments e.g. security, networking and storage teams. It may also happen that the customer comes up with new demands based on new findings or insights. This may result in delay for the implementation and ultimately lead to increased cost.

This chapter about The Enhanced Evaluation should help you avoid such situations. We will explain how the approach used by Veeam architects can help you simplify and streamline the design phase and steer all project participants

towards the same goals. This will optimize the implementation phase and ultimately cut cost due to less time spent revising the design and realigning stakeholders.

1.100 Enhanced Evaluation - Workshop Example

This section describes how to conduct an infrastructure discovery and assessment session with a customer. Below is an example of how Veeam Architects hold such meetings with customers. The example below is just one example of many possible ways of the meeting content; please have a look at other chapters of this guide to prepare for such meeting.

1.100.1 Infrastructure Discovery

1. Start with the first main customer datacenter. Figure out the following:
2. Virtualization platform and version
3. Main storage system, type, connection
4. Is storage virtualization used (between the storage arrays and hypervisor)?
5. Next would be the second customer datacenter (if available)
6. Is this the same platform as the main datacenter, if not what is it?
7. Are there any storage replication/mirroring involved?
8. Is an Active/Active cluster used?

For proper backup proxy implementation **and** backup mode selection, it **is** important to know where the data that you want to back up **is** located, **and** whether you can access all data **from a** single site.

1. Obtain information about network connections:
2. Is there a 10 GbE LAN?
3. Is there a WAN connection between the 2 datacenters?
4. What is the VMKernel Interface physical link speed?
5. Is the VMware vCenter Server or Microsoft SCVMM server physical or virtual? Where is it located? Are both hypervisor platforms used?

This is necessary to know if you plan to use the Virtual Appliance (HotAdd) or Network backup mode. 10GbE gives you faster processing for the Network mode. To learn more, see the [Backup Proxy](#) chapter.

1. Define the amount of production data:
2. Number of VMs (needed to design jobs)
3. Used data (needed to define the backup target and configure jobs settings)
4. Number of ESXi hosts and number of used sockets (this regards Veeam licensing).
5. Number of clusters
6. Other information
7. Create the first Veeam implementation draft/sample scenario:

8. Start with the repository, discussing customer demands. In the example, customer wanted to have the backup data in both data centers. If so, you could decide to implement repositories on both sides (half of the data on each side) and use the backup copy job to move data to the second site.
9. Discuss proxy implementation. The customer agreed to implement physical proxy servers connected to their Fibre Channel network. As the customer used thick-provisioned VMware VM disks, this ensured a fast and reliable backup and restore. Check out the [Backup Proxy](#) section of this guide to determine the best proxy implementation and select a transport mode for the environment.
10. Plan for the backup server. In this example, it was placed on a VM and replicated to the second datacenter. (The underlying datastore of the VM was not replicated to the second site, only the VM.)
11. Add other required components. The customer was already using two IBM TS3500 libraries for long-term retention with the existing backup software (agents). They prepared a partition on each library with 4x LTO6 drives for use with Veeam. You would proceed and connect them to the 2 physical servers (having the proxy and repository roles assigned), and additionally assign the tape server role to these servers.
12. Define OS/applications:
13. Create a list of used operating systems.
14. Create a list of all applications starting with the most critical. Find out whether Microsoft SQL and Microsoft SharePoint are used, as it can influence the version and type of the Microsoft SQL Server on which the Veeam configuration database must be deployed (Express Edition may be not sufficient).
15. Define business-critical applications/VMs to plan for availability. Planning for backup is very important for them, as this mainly influence the RPO and stability of existing applications. It is even more important to plan for disaster recovery scenarios.
16. Define the number of VMs that are business critical.
17. Find out whether slower performance is OK at disaster recovery (consider using Instant VM Recovery).

In this example, the customer used a third small datacenter with a single storage system (Quorum) for the storage virtualization. During the discussion the customer identified 50 VMs that were business-critical and needed full performance even at disaster recovery. Thus, in the next step, you would add 2 ESXi hosts to that Quorum datacenter and replicate these 50 VMs every hour to that datacenter. The connection speed is to be 10 GbE. So, in case of disaster recovery the customer could just boot up all VMs with full speed.

Important! use all available Veeam possibilities to implement the best RTO and RPO times in a customers environment.

For the VM recovery scenario, you can mix classic VM restore (best for small VMs), Instant VM Recovery (best for huge data servers) and VM replica failover (best for database systems with extreme I/O requirements). Together with the customer, check the “possible failure domains” (single storage system / whole datacenter / 1 datastore) and decide if the designed Veeam implementation fits into these needs and is in line with the budget.

1.100.2 Network and Firewall

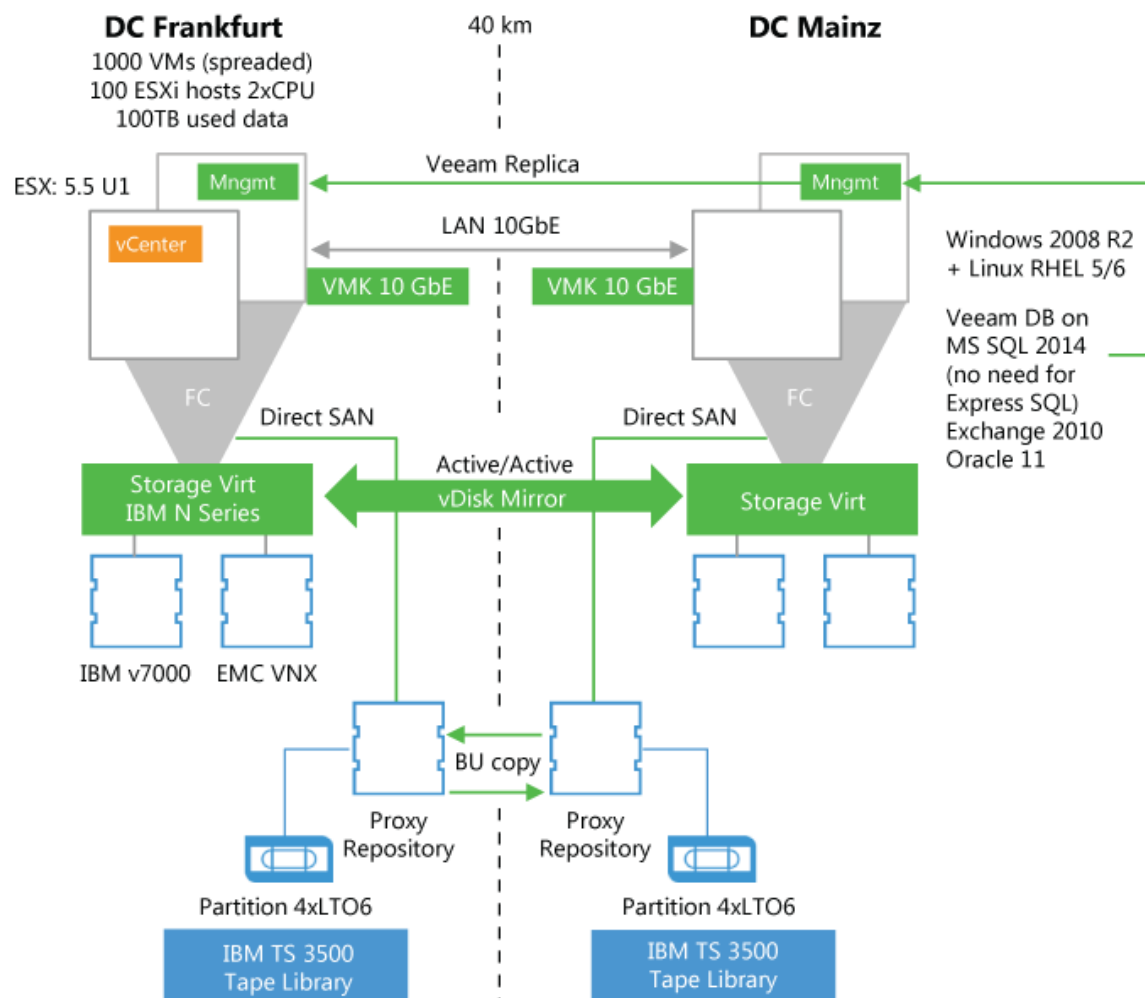
Veeam Availability Suite is elastic and lets you implement different backup infrastructure schemes. Firewalls can be used between all backup infrastructure components. The only exception is RPC inspection functionality: it can cause delays in connections, and Veeam Backup & Replication can run into timeouts. However, the best practice is to place backup infrastructure components in the same network segment as the corresponding VMware components to allow for efficient and fast usage of the network bandwidth.

1.100.3 Proxy/Repository Systems

Proxy and repository servers should be placed in the VMKernel networks. Veeam Backup & Replication uses the VMKernel interfaces to read out configuration data and disk data (in case of Network mode), and to map Veeam vPower NFS data stores for fast recovery (Instant VM Recovery).

1.100.4 Backup & Replication Server

As the backup server communicates mainly with the vCenter Server and other backup infrastructure components, it should be placed next to the vCenter Server in most cases. The backup infrastructure for this sample scenario would look as follows:



Enhanced

Evaluation - Example

1.100.5 Veeam ONE

Veeam ONE components should be placed next to the vCenter Server and should be able to read from the backup server and ESXi hosts (over the CIM protocol) as well. See Veeam ONE documentation for more information: [Veeam ONE Deployment Guide](#).

1.100.6 Enterprise Manager

When Veeam Backup Enterprise Manager is used with Self-Restore services, it should be placed in the internal DMZ in most cases.

1.100.7 Restore Points

In the sample case, the customer needed daily backup with 14 restore points; the points were to be held on 2 sites (multiplied with backup copy job). The customer also wanted to offload the weekly full backups on tape and hold them for a period slightly longer than one year in both tape libraries.

The customer also needed to replicate the most critical VMs to the Quorum datacenter hourly, between 7:00 and 19:00. The number of replication restore points to be maintained was the maximum possible (here 28 restore points).

In many architecture meetings, planning for the retention policies is the most time-consuming part as you are likely to engage different administrators and management team members from different departments in this process. These team members have to translate their file-based existing restore point policies into a new way (image-level backup). It is a matter of concern because a longer retention chain will result in expensive storage space costs.

Important! Remember to agree on backing up Microsoft SQL Server transaction logs with Veeam Backup & Replication.

If speaking about the storage sizing, the tool at [Veeam Restore Points Calculator](#) can help to illustrate the retention chains on disk and estimate the required capacity.

1.101 Enhanced Evaluation - Preparation

After having agreed and discussed the points in the Workshop Example section, proceed with the enhanced POC to demonstrate that Veeam Availability Suite can work in customer's environment with excellent speed.

Typically, the enhanced POC is carried out under the following conditions:

- The environment resembles the production environment, with all firewalls in place.
- Involved storage systems are similar to the production storage systems.
- Veeam storage integration is used whenever possible.
- 100-200 VMs will be back-upped/replicated to demonstrate the scalability and great load balancing power.
- All major applications are back-upped to test all restore scenarios.

1.101.1 Preparation steps

1. Prepare for the POC planning with the Veeam User Guide and this document.
2. Complete a POC document including all your designs and plans, including chosen servers for the tests and why they are important. Set criteria for success on each machine and what is tested and expected outcome.

3. Check out the necessary firewall ports and help the customer with the internal firewall change requests. Refer to the corresponding sections in the User Guide and this document.

Tip: Perform firewall planning thoroughly: if something is misconfigured, this may block the entire POC. In most cases, it is not easy to detect problems and introduce firewall changes, when the POC is underway. However, it is a good idea to ask the customer to have the firewall administrator at hand in case you need an urgent modification. 4. Create a separate vCenter Server account for Veeam ONE (read-only + datastore browsing + CIM) so that you are able to track what users do. 5. If you want to use the storage integration feature, check out the corresponding chapter in this guide, set up the storage and the SAN network together with the storage administrators. **Limit the scope** of storage system rescan **to the volumes used** in the POC. 6. If you want to use SureBackup, make sure that a virtualized Domain Controller is present if needed (e.g. for Microsoft Exchange). 7. Let the customer prepare all used antivirus systems upfront so that you do not run into trouble. Check the [Antivirus section](#) of this guide and Veeam KB1999. 8. Ask the customer to prepare a decent performing storage system for the POC. Avoid low-end NAS appliances for enhanced evaluations. 9. Let the customer prepare all operating systems and database installations. Set up Veeam Backup & Replication and backup infrastructure components together with the customer and place the folders correctly. 10. Ensure that the document relating to all the testing is accurate and up to date including all success criteria for each machine being tested. This will keep control for POC, each test and a schedule can be built around the testing avoiding random testing of features.

1.102 Automation

The bigger the environment, the more automation is needed to reduce the administration effort. For example, if you are operating 40 branch offices with independent Veeam installations, you may want to roll out and configure backup servers with scripts, and automatically create jobs in the same location. Another example is automatic job creation for 2,000-3,000 VMs with exactly the same configurations, which can limit user-caused misconfiguration.

1.102.1 Command line

Following operations are managed through the Windows command line:

- Installation - [Link to Help Center](#)
- Updates - [Link to Help Center](#)

1.102.2 PowerShell

Operations in Veeam Backup & Replication can be automated with Veeam PowerShell snap-in in the following areas:

- Configuration
- Job creation/job editing
- Working with external schedulers (UC4/TWS and other) to start Veeam jobs
- Restores
- Reporting
- Datacenter migration (quick migration or replication)

The PowerShell plugin is available with all commercial versions of the product.

Note: PowerShell plugin is also available with Veeam Backup FREE, although limited: <https://www.veeam.com/blog/veeam-backup-free-edition-now-with-powershell.html>

Our customers and partners use this functionality to scale out backup infrastructure environments to nearly 100,000 VMs under a single Veeam Backup Enterprise Manager instance with multiple backup servers located in different datacenters.

The best starting point to get in touch with the Veeam PowerShell plugin is to read the Veeam PowerShell User Guide > [Veeam Help Center - PowerShell Reference](#).

You can find help for the scripts in the [Veeam Community Forums - PowerShell](#) section. If you need some examples, refer to the following thread: [Getting Started and Code Examples](#)

1.102.3 RESTful API

In the Veeam Enterprise Manager, there is as well RESTful API that allows you to create workflows in orchestration tools or to integrate Veeam Backup Enterprise Manager (self-services) in your own “cloud” portal. Specifically, this is an option that comes with Enterprise Plus Editions and is focused on the hosting business.

Here is a list of external resources:

- [Veeam Help Center - RESTful API Reference](#)
- [Veeam Community Forums](#)
- [Veeam Help Center - Beginner Example](#)

1.102.4 A simple RESTful API example - adding a guest to a backup job

In the following section, the Veeam WEB client will be used for convenience as it is quite simple by nature and instantly available through enterprise manager URL. Also, the browser used is configured to accept cookies to simplify the authentication token management.

Authentication on the REST server

From the client browser, connect to the URL `http://EM:9399/web/#/api/` and enter credentials as requested. Then, follow the latest version URL to get the list of all accessible resources types. `http://EM:9399/web/#/api/sessionMngr/?v=latest`

Building a query to retrieve the vCenter UID

Once logged in, knowing the vCenter Name where the VM we want to add resides, we need to get the vCenter UID.

Referring to the REST API guide https://helpcenter.veeam.com/docs/backup/rest/get_managedservers_id.html?ver=95 we can gather necessary informations to build a query.

- Object type is “ManagedServer”
- Property to filter is “ManagedServerType” from which “VC” corresponds to vCenter
- Property to filter is “Name” equal to “vc.democenter.int” in this example

Note: the “ManagedServerType” has been added to the query for demonstration purpose.

`http://EM:9399/web/#/api/query?type=ManagedServer&filter=(ManagedServerType==VC;Name==”vcsa.democenter.int`

```
<?xml version="1.0" encoding="UTF-8"?>
<QueryResult xmlns="http://www.veeam.com/ent/v1.0" xmlns:xsd="http://www.w3.org/2001/
→XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <Refs>
    <Ref UID="urn:veeam:ManagedServer:93fe5565-0ae7-4574-abb5-0f4ea8c5e9bd" Name=
→"vcsa.democenter.int" Href="http://hq-vbrem1.democenter.int:9399/api/managedServers/
→93fe5565-0ae7-4574-abb5-0f4ea8c5e9bd" Type="ManagedServerReference">
      <Links>
        <Link Href="http://hq-vbrem1.democenter.int:9399/api/managedServers/93fe5565-
→0ae7-4574-abb5-0f4ea8c5e9bd?format=Entity" Name="vcsa.democenter.int" Type=
→"ManagedServer" Rel="Alternate"/>
        <Link Href="http://hq-vbrem1.democenter.int:9399/api/backupServers/d7b8bcdd-
→dbc5-40a3-9a50-dd8ba65cfa91" Name="hq-vbr1.democenter.int" Type=
→"BackupServerReference" Rel="Up"/>
      </Links>
    </Ref>
  </Refs>
  <PagingInfo PageNum="1" PageSize="100" PagesCount="1">
    <Links>
      <Link Href="http://hq-vbrem1.democenter.int:9399/api/query?type=ManagedServer&
→filter=(ManagedServerType%3d%3dVC%3bName%3d%3d%22vcsa.democenter.int%22)&
→pageSize=100&page=1" Rel="First"/>
      <Link Href="http://hq-vbrem1.democenter.int:9399/api/query?type=ManagedServer&
→filter=(ManagedServerType%3d%3dVC%3bName%3d%3d%22vcsa.democenter.int%22)&
→pageSize=100&page=1" Rel="Last"/>
    </Links>
  </PagingInfo>
</QueryResult>
```

The lookup service necessitates a “HierarchyRoot” resource type in the urn, which is an alternate representation of the “ManagedServer”. We then must send a GET to the managed server resource representation: <http://EM:9399/web/#/api/managedServers/25fb843d-92a3-45d4-836c-0531afe4df9b?format=Entity> and find the “Alternate” representation of type “HierarchyRoot” in the proposed links.

```
<Link Href="http://hq-vbrem1.democenter.int:9399/api/hierarchyRoots/93fe5565-0ae7-
→4574-abb5-0f4ea8c5e9bd" Name="vcsa.democenter.int" Type="HierarchyRootReference"
→Rel="Alternate"/>
```

From here, send a GET request to the HierarchyRoot resource representation to pick up its UID (simply clicking on the URL will send the GET request).

<http://hq-vbrem1.democenter.int:9399/api/hierarchyRoots/93fe5565-0ae7-4574-abb5-0f4ea8c5e9bd?format=Entity>

```
<?xml version="1.0" encoding="UTF-8"?>
<HierarchyRoot Href="http://hq-vbrem1.democenter.int:9399/api/hierarchyRoots/93fe5565-
→0ae7-4574-abb5-0f4ea8c5e9bd?format=Entity" Type="HierarchyRoot" Name="vcsa.
→democenter.int" UID="urn:veeam:HierarchyRoot:93fe5565-0ae7-4574-abb5-0f4ea8c5e9bd"
→xmlns="http://www.veeam.com/ent/v1.0" xmlns:xsd="http://www.w3.org/2001/XMLSchema"
→xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <Links>
    <Link Href="http://hq-vbrem1.democenter.int:9399/api/backupServers/d7b8bcdd-dbc5-
→40a3-9a50-dd8ba65cfa91" Name="hq-vbr1.democenter.int" Type="BackupServerReference"
→Rel="Up"/>
    <Link Href="http://hq-vbrem1.democenter.int:9399/api/hierarchyRoots/93fe5565-0ae7-
→4574-abb5-0f4ea8c5e9bd" Name="vcsa.democenter.int" Type="HierarchyRootReference"
→Rel="Alternate"/>
    <Link Href="http://hq-vbrem1.democenter.int:9399/api/managedServers/93fe5565-0ae7-
→4574-abb5-0f4ea8c5e9bd?format=Entity" Name="vcsa.democenter.int" Type="ManagedServer"
→Rel="Related"/>
```

(continues on next page)

(continued from previous page)

```

</Links>
<HierarchyRootId>93fe5565-0ae7-4574-abb5-0f4ea8c5e9bd</HierarchyRootId>
<UniqueId>FFB4D8B6-CEC0-4DF8-87D5-82D931ED6FBD</UniqueId>
<HostType>VC</HostType>
</HierarchyRoot>

```

The required reference for further use is the UID “urn:veeam:HierarchyRoot:93fe5565-0ae7-4574-abb5-0f4ea8c5e9bd” corresponding to the Veeam managed vCenter server where the VM should reside.

Note: It could have been more simple to directly work on the ManagedServer UID and directly change the resource type from “ManagedServer” to “HierarchyRoot”. The complex method was chosen for demonstration purpose.

Building a lookup to retrieve the virtual machine ID

Knowing the UID of the “Host” (vCenter), and the name of the guest we want to add to a job, we can build the lookup URL using the name of the VM as a selection criteria. The rules to build the lookup request are detailed in the REST API guide : https://helpcenter.veeam.com/docs/backup/rest/lookup_query.html?ver=95#params.

<http://hq-vbrem1.democenter.int:9399/web/#/api/lookup?host=urn:veeam:HierarchyRoot:93fe5565-0ae7-4574-abb5-0f4ea8c5e9bd&name=demo-win1&type=Vm>

```

<?xml version="1.0" encoding="UTF-8"?>
<HierarchyItems xmlns="http://www.veeam.com/ent/v1.0" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <HierarchyItem Type="HierarchyItem">
    <ObjectRef>urn:VMware:Vm:93fe5565-0ae7-4574-abb5-0f4ea8c5e9bd.vm-48911</ObjectRef>
    <ObjectType>Vm</ObjectType>
    <ObjectName>demo-win1</ObjectName>
  </HierarchyItem>
</HierarchyItems>

```

The UID here is given by the “ObjectRef” property: “urn:VMware:Vm:93fe5565-0ae7-4574-abb5-0f4ea8c5e9bd.vm-48911”. As you can see, the UID of the VM comprises the UID of the management server appended with the Mo-Ref of the VM. This is useful if you want to automatically build a Veeam VM reference, knowing its management server and Mo-Ref. This “manual” type construction of references can be used for automation purpose.

Building a query to retrieve the Job ID

Knowing the Name of the job where the VM should be added (“Test REST”) we can request the query service to get its ID:

[http://hq-vbrem1.democenter.int:9399/web/#/api/query?type=job&filter=\(Name==%22Test%20REST%22\)](http://hq-vbrem1.democenter.int:9399/web/#/api/query?type=job&filter=(Name==%22Test%20REST%22))

```

<?xml version="1.0" encoding="UTF-8"?>
<QueryResult xmlns="http://www.veeam.com/ent/v1.0" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <Refs>
    <Ref UID="urn:veeam:Job:455c0799-ede5-4ade-a7b2-02d2d0fac3de" Name="Test REST"
    <Href="http://hq-vbrem1.democenter.int:9399/api/jobs/455c0799-ede5-4ade-a7b2-02d2d0fac3de" Type="JobReference">
    <Links>
      <Link Href="http://hq-vbrem1.democenter.int:9399/api/backupServers/d7b8bcdd-dbc5-40a3-9a50-dd8ba65cfa91" Name="hq-vbr1.democenter.int" Type=
      <"BackupServerReference" Rel="Up"/>
      <Link Href="http://hq-vbrem1.democenter.int:9399/api/jobs/455c0799-ede5-4ade-a7b2-02d2d0fac3de?format=Entity" Name="Test REST" Type="Job" Rel="Alter

```

(continued from previous page)

```

    <Link Href="http://hq-vbrem1.democenter.int:9399/api/jobs/455c0799-ede5-4ade-
    ↪a7b2-02d2d0fac3de/backupSessions" Type="BackupJobSessionReferenceList" Rel="Down"/>
  </Links>
</Ref>
</Refs>
<PagingInfo PageNum="1" PageSize="100" PagesCount="1">
  <Links>
    <Link Href="http://hq-vbrem1.democenter.int:9399/api/query?type=job&filter=(Name
    ↪%3d%3d%22Test+REST%22)&pageSize=100&page=1" Rel="First"/>
    <Link Href="http://hq-vbrem1.democenter.int:9399/api/query?type=job&filter=(Name
    ↪%3d%3d%22Test+REST%22)&pageSize=100&page=1" Rel="Last"/>
  </Links>
</PagingInfo>
</QueryResult>

```

The ID is given by the last part of the Ref UID : “urn:veeam:Job:455c0799-ede5-4ade-a7b2-02d2d0fac3de”. The URL to access the job resource representation is directly given by the link pointing to the “JobReference” type: <http://hq-vbrem1.democenter.int:9399/api/jobs/455c0799-ede5-4ade-a7b2-02d2d0fac3de>

Note: To access the resource (not the resource representation) and get more details, you shall follow the “Alternate” related object, which type is “Job” and not “JobReference”.

Adding the VM to the job

Knowing the “Jobs” resource representation structure, the resource to be called to add the VM to the job is “/jobs/{ID}/includes” with a POST verb. In case of any doubt about the resource to call, the REST reference guide offers a precise representation of the resource tree: https://helpcenter.veeam.com/docs/backup/rest/post_jobs_id_includes.html?ver=95

As stated by the “Min/Max” column, the only mandatory parameters to add in the request body are the container reference (a VM in our example) and name “HierarchyObjRef” and “HierarchyObjName”.

All other guest related parameters are described in the documentation. Specific credentials for inguest processing are described by the resource “/backupServers/{ID}/credentials”.

- Order
- GuestProcessingOptions
 - VssSnapshotOptions
 - WindowsGuestFSIndexingOptions
 - LinuxGuestFSIndexingOptions
 - SQLBackupOptions
 - WindowsCredentialsId
 - LinuxCredentialsId
 - FSFileExcludeOptions
 - OracleBackupOptions

We will then form a HTTP phrase: Type: POST

URL: <http://hq-vbrem1.democenter.int:9399/web/#/api/jobs/455c0799-ede5-4ade-a7b2-02d2d0fac3de/includes>

Header: (automatically handled by the client since cookies are in use) :

Cookie: X-RestSvcSessionId=Session_ID

Body:

```
<?xml version="1.0" encoding="UTF-8"?>
<CreateObjectInJobSpec xmlns="http://www.veeam.com/ent/v1.0" xmlns:xsd="http://www.w3.
→org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <HierarchyObjRef>urn:VMware:Vm:93fe5565-0ae7-4574-abb5-0f4ea8c5e9bd.vm-48911</
→HierarchyObjRef>
  <HierarchyObjName>demo-win1</HierarchyObjName>
</CreateObjectInJobSpec>
```

To access the POST request from the Veeam WEB client, open the resource view of the job ID 455c0799-ede5-4ade-a7b2-02d2d0fac3de and follow the proposed link leading to add a VM in the job (Type="ObjectInJob", Rel="Create").

```
<Link Href="http://hq-vbrem1.democenter.int:9399/api/jobs/455c0799-ede5-4ade-a7b2-
→02d2d0fac3de/includes" Type="ObjectInJob" Rel="Create"/>
```

This will automatically form the HTTP request :

From there, the body can be modified to indicate proper VM reference:

```
<?xml version="1.0" encoding="utf-8"?>
<CreateObjectInJobSpec xmlns="http://www.veeam.com/ent/v1.0" xmlns:xsd="http://www.w3.
→org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <HierarchyObjRef>urn:VMware:Vm:93fe5565-0ae7-4574-abb5-0f4ea8c5e9bd.vm-48911</
→HierarchyObjRef>
  <HierarchyObjName>demo-win1</HierarchyObjName>
</CreateObjectInJobSpec>
```

Upon completion, a return code 200 should be sent by the server, pointing to the corresponding task.

To verify if the added VM is in the job, we can send a query using the "ObjectInJob" type as described in the available querying type (refer to user guide "Query Syntax" section for more informations). The possible filter parameters are described in the "(GET) /jobs/{ID}/includes/{ID}" section of the reference guide.

http://hq-vbrem1.democenter.int:9399/web/#/api/query?type=ObjectInJob&filter=(JobName=="Test REST";Name=="demo-win1")

```
<?xml version="1.0" encoding="UTF-8"?>
<QueryResult xmlns="http://www.veeam.com/ent/v1.0" xmlns:xsd="http://www.w3.org/2001/
→XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <Resources>
    <sInObjectJob>
      <ObjectInJob Href="http://hq-vbrem1.democenter.int:9399/api/jobs/455c0799-ede5-
→4ade-a7b2-02d2d0fac3de/includes/8242bd6d-1aaf-41d7-9a11-e51fad56318f" Type=
→"ObjectInJob">
        <Links>
          <Link Href="http://hq-vbrem1.democenter.int:9399/api/jobs/455c0799-ede5-
→4ade-a7b2-02d2d0fac3de/includes/8242bd6d-1aaf-41d7-9a11-e51fad56318f" Rel="Delete"/>
          <Link Href="http://hq-vbrem1.democenter.int:9399/api/jobs/455c0799-ede5-
→4ade-a7b2-02d2d0fac3de?format=Entity" Name="Test REST" Type="Job" Rel="Up"/>
        </Links>
        <ObjectInJobId>8242bd6d-1aaf-41d7-9a11-e51fad56318f</ObjectInJobId>
        <HierarchyObjRef>urn:VMware:Vm:93fe5565-0ae7-4574-abb5-0f4ea8c5e9bd.vm-48911</
→HierarchyObjRef>
        <Name>demo-win1</Name>
        <DisplayName>demo-win1</DisplayName>
        <Order>1</Order>
        <GuestProcessingOptions>
          <VssSnapshotOptions>
```

(continues on next page)

(continued from previous page)

```

        <VssSnapshotMode>Disabled</VssSnapshotMode>
        <IsCopyOnly>>false</IsCopyOnly>
    </VssSnapshotOptions>
    <WindowsGuestFSIndexingOptions>
        <FileSystemIndexingMode>Disabled</FileSystemIndexingMode>
        <IncludedIndexingFolders/>
        <ExcludedIndexingFolders/>
    </WindowsGuestFSIndexingOptions>
    <LinuxGuestFSIndexingOptions>
        <FileSystemIndexingMode>Disabled</FileSystemIndexingMode>
        <IncludedIndexingFolders/>
        <ExcludedIndexingFolders/>
    </LinuxGuestFSIndexingOptions>
    <SqlBackupOptions>
        <TransactionLogsProcessing>OnlyOnSuccessJob</TransactionLogsProcessing>
        <BackupLogsFrequencyMin>15</BackupLogsFrequencyMin>
        <UseDbBackupRetention>>true</UseDbBackupRetention>
        <RetainDays>15</RetainDays>
    </SqlBackupOptions>
    <WindowsCredentialsId>00000000-0000-0000-0000-000000000000</
→WindowsCredentialsId>
    <LinuxCredentialsId>00000000-0000-0000-0000-000000000000</
→LinuxCredentialsId>
    </GuestProcessingOptions>
    </ObjectInJob>
</sInObjectJob>
</Resources>
<PagingInfo PageNum="1" PageSize="100" PagesCount="1">
    <Links>
        <Link Href="http://hq-vbreml.democenter.int:9399/api/query?type=ObjectInJob&
→filter=(JobName%3d%3d%22Test+REST%22%3bName%3d%3d%22demo-win1%22) &pageSize=100&
→page=1" Rel="First"/>
        <Link Href="http://hq-vbreml.democenter.int:9399/api/query?type=ObjectInJob&
→filter=(JobName%3d%3d%22Test+REST%22%3bName%3d%3d%22demo-win1%22) &pageSize=100&
→page=1" Rel="Last"/>
    </Links>
    </PagingInfo>
</QueryResult>

```

Closing the connection

The final step is to close the connection. Using the VEEAM REST client, closing the client will close the connection. Using any other client, a DELETE should be sent to the session resource representation (leaving the body empty, as the session is referenced to in the URL as a resource).

1.103 Infrastructure Hardening

Running your Veeam Backup & Replication infrastructure in a secure configuration is a daunting task even for security professionals. This chapter provides practical advice to help administrators to harden their infrastructure following security best practices so that they can confidently deploy their Veeam services and lower their chances of being compromised.

Hardening is about securing the infrastructure against attacks, by reducing its attack surface and thus eliminating as many risks as possible. One of the main measures in hardening is removing all non-essential software programs and

utilities from the deployed Veeam components. While these components may offer useful features to the administrator, if they provide ‘back-door’ access to the system, they must be removed during the hardening process.

But also, creating visibility in what goes on in the infrastructure is part of hardening your infrastructure. Making sure you will notice when an attack is/ or has taken place and then making sure logs and traces are saved for law-enforcement and security specialists when needed.

1.103.1 Protect

Protecting your infrastructure successfully is all about understanding the current attack vectors; what and whom you are protecting, your Veeam infrastructure, against. If you know what and whom you are protecting against, makes it easier to take the correct countermeasures. One of those countermeasures is hardening.

Looking at the different Veeam Backup & Replication components you have to protect the following components:

- Veeam Backup server
- User Accounts
- Backup repositories
- Backup data flows

Consider the Veeam Backup & Replication server to be the **Number 1** target on your infrastructure and it should have very restricted access. As a general rule the backup server is the single greatest target a hacker can claim on your network. Also the backup repositories which holds the backup files are a primary target.

1.103.2 Hardening

Within the hardening process of your Veeam infrastructure there are a few steps everyone should always consider and act upon, namely:

1. *Secure by Design*
2. *Remove Unused Components*
3. *Console Access*
4. *Roles and Users*
5. *Required Permissions*
6. *Encryption*
7. *Backup & Replication Database*
8. *Segmentation*
9. *Visibility*
10. *Recovery Strategy*

1.103.3 Secure by Design

Overly complex designs become harder for the IT team to manage and overlook and it makes it easier for an attacker to exploit and stay in the shadows. Simpler designs that can be easily overviewed are in basis more secure. Use the K.I.S.S.[^1] (Keep It Simple and Straightforward) principle for your designs.

Adding security to an already existing infrastructure is much harder and costly than thinking about it while designing a new or refreshing an existing infrastructure. In a virtual infrastructure, it is good use to build up a Master image

which has been hardened from the start. Removing all known attack vectors and only open up access when Veeam components are added and needs specific (port) openings or extra software to function properly. This way all builds are consistent and kept up-to-date which makes it secure in the basis.

Consider the Veeam Backup & Replication server to be the **Number 1** target on your infrastructure and it should have very restricted access. As a general rule the backup server is the single greatest target a hacker can claim on your network.

1.103.4 Remove Unused Components

Remove all non-essential software programs and utilities from the deployed Veeam components. While these programs may offer useful features to the administrator, if they provide 'back-door' access to the system, they must be removed during the hardening process. Think about additional software like **web browsers, java, adobe reader** and such. All parts which do not belong to the operating system or to active Veeam components, remove it. It will make maintaining an up-to-date patch level much easier.

Veeam Backup & Replication Server

- Remove the Backup & Replication Console from the Veeam Backup & Replication server. The console is installed locally on the backup server by default.
- Switch off the Veeam vPower NFS Service if you do not plan on using the following Veeam features: Sure-Backup, Instant Recovery, or Other-OS File Level Recovery (FLR) operations.

How to remove the Veeam Backup & Replication Console

The Console can not be removed through the installer or by using Add/Remove in Windows. Open a cmd prompt with administrative access. On the command prompt type: `wmic product list brief > installed.txt` this will create a text document with all installed products and their respective Product Codes.

For uninstalling Veeam Backup & Replication Console, first de-install all Veeam Explorers:

- Veeam Explorer for Microsoft Exchange
- Veeam Explorer for Microsoft Sharepoint
- Veeam Explorer for Microsoft Active Directory
- Veeam Explorer for Microsoft SQL
- Veeam Explorer for Oracle

You can uninstall these components by using: `msiexec /x {ProductCode}`

Example for uninstalling the Veeam Backup & Replication console is: `msiexec /x {D0BCF408-A05D-45AA-A982-5ACC74ADFD8A}`

Enterprise Manager

When Enterprise Manager is not in use de-install it and remove it from your environment.

1.103.5 Console Access

The Veeam Backup & Replication console is a client-side component that provides access to the backup server. The console lets several backup operators and admins log in to Veeam Backup & Replication simultaneously and perform all kind of data protection and disaster recovery operations as if you work on the backup server.

Install the Veeam Backup & Replication console on a central management server that is, positioned in a DMZ and protected with 2-factor authentication. Do NOT install the console on the local desktops of backup & recovery admins.

1.103.6 Roles and Users

Deploy an Access Control policy, managing access to management components is crucial for a good protection. Use the *principle of least privilege*. Provide the minimal privilege needed for some operation to occur. An attacker who gained high-privilege access to backup infrastructure servers can get credentials of user accounts and compromise other systems in your environment. Make sure that all accounts have a specific role and that they are added to that specific group.

Containment to keep the attackers from moving around too easily. Some standard measures and policies are:

- Do not use user accounts for admin access, reducing incidents and accidents
- Give every Veeam admin his own admin account or add their admin account to the appropriate security group within Veeam, for traceability and easy adding and removal
- Only give out access to what is needed for the job
- Limit users who can log in using Remote Desktop and/or Veeam Backup Console
- Add 2-factor authentication to highly valuable assets
- Monitor your accounts for suspicious activity

A role assigned to the user defines the user activity scope: what operations in Veeam Backup & Replication the user can perform. Role security settings affect the following [operations](#)

Password management policy

Use a clever Password management policy, which works for your organization. Enforcing the use of strong passwords across your infrastructure is a valuable control. It's more challenging for attackers to guess passwords/crack hashes to gain unauthorized access to critical systems.

Selecting passwords of 10 characters with a mixture of upper and lowercase letters, numbers and special characters is a good start for user accounts.

For Admin accounts adding 2-factor authentication is also a must to secure the infrastructure.

And for service accounts use 25+ characters combined with a password tool for easier management. An Admin can copy and paste the password when needed, increasing security of the service accounts.

Lockout policy

Use a Lockout policy that complements a clever password management policy. Accounts will be locked after a small number of incorrect attempts. This can stop password guessing attacks dead in the water. But be careful that this can also lock everyone out of the backup & replication system for a period! For service accounts, sometimes it is better just to raise alarms fast. Instead of locking the accounts. This way you gain visibility into suspicious behavior towards your data/infrastructure.

1.103.7 Required Permissions

Use the *principle of least privilege*. Provide the minimal required permissions needed for the accounts to run. The accounts used for installing and using Veeam Backup & Replication must have the following [permissions](#).

If VMware vCenter Server is added to the backup infrastructure, an account that has administrator permissions is required. Instead of granting administrator permissions to the account, you can configure more granular permissions. Veeam has identified the minimum permissions required for the various software functions. Review the "[Required Permissions](#)" document (not changed since V9.0) and configure the accounts used by Veeam Backup & Replication to meet these requirements.

Particularly, backup proxies must be considered the target for compromise. During backup, proxies obtain from the backup server credentials required to access virtual infrastructure servers. A person having administrator privileges on a backup proxy can intercept the credentials and use them to access the virtual infrastructure.

Patching and Updates

Patch operating systems, software, and firmware on Veeam components. Most hacks succeed because there is already vulnerable software in use which is not up-to-date with current patch levels. So make sure all software and hardware where Veeam components are running are up-to-date. One of the most possible causes of a credential theft are missing guest OS updates and use of outdated authentication protocols. To mitigate risks, follow these guidelines:

- **Ensure timely guest OS updates on backup infrastructure servers.** Install the latest updates and patches on backup infrastructure servers to minimize the risk of exploiting guest OS vulnerabilities by attackers.
- **Choose strong encryption algorithms for SSH.** To communicate with Linux servers deployed as part of the backup infrastructure, Veeam Backup & Replication uses SSH. Make sure that for the SSH tunnel you use a strong and proven encryption algorithm, with sufficient key length. Ensure that private keys are kept in a highly secure place, and cannot be uncovered by a 3rd party.

1.103.8 Encryption

Backup and replica data is a highly potential source of vulnerability. To secure data stored in backups and replicas, follow these guidelines:

- **Ensure physical security of target servers.** Check that only authorized personnel have access to the room where your target servers (backup repositories and hosts) reside.
- **Restrict user access to backups and replicas.** Check that only authorized users have permissions to access backups and replicas on target servers.
- **Encrypt data in backups.** Use Veeam Backup & Replication inbuilt encryption to protect data in backups. To guarantee security of data in backups, follow [Encryption Best Practices](#).

Backup and replica data can be intercepted in-transit, when it is communicated from source to target over a network. To secure the communication channel for backup traffic, consider these guidelines:

- **Isolate backup traffic.** Use an isolated network to transport data between backup infrastructure components — backup server, backup proxies, repositories and so on. (also see segmentation)
- **Encrypt network traffic.** By default, Veeam Backup & Replication encrypts network traffic traveling between public networks. To ensure secure communication of sensitive data within the boundaries of the same network, you can also encrypt backup traffic in private networks. For details, see [Enabling Network Data Encryption](#).

1.103.9 Backup & Replication Database

The Backup & Replication configuration database stores credentials to connect to virtual servers and other systems in the backup & replication infrastructure. All passwords stored in the database are encrypted. However, a user with administrator privileges on the backup server can decrypt the passwords, which presents a potential threat.

To secure the Backup & Replication configuration database, follow these guidelines:

- **Restrict user access to the database.** Check that only authorized users can access the backup server and the server that hosts the Veeam Backup & Replication configuration database (if the database runs on a remote server).
- **Encrypt data in configuration backups.** Enable data encryption for configuration backup to secure sensitive data stored in the configuration database. For details, see [Creating Encrypted Configuration Backups](#).

1.103.10 Segmentation

Add local protection mechanics, in addition to the border firewalls, intrusion detection, patching and such. You can make use of local mechanisms, like up-to-date anti-malware, firewalls and network segmentation. This way you create different rings-of-defense slowing an attacker down. A great way to strategically use segmentation is by implementing [Zones](#).

A good practice is to place the backup repositories in a special segment not accessible by any user. Like for instance the production storage is only available to the virtual infrastructure components and application servers. Not directly accessible by any user!

To segment your infrastructure and Veeam Backup & Replication components, make sure the firewalls on the local server installations have the correct [Ports](#) opened.

You can also deploy [VMware NSX](#) as a counter measure with micro-segmentation to make sure the attack surface is as narrow as possible without blocking everyone to use the services. Visibility into the network and all data flows is crucial to help you protect all different rings/cells within your infrastructure. You can add the Veeam components to NSX policies to make sure they can communicate with each other without opening it up to any user.

Ports

Try not to use obscure ports and other tricks to try and hide Veeam ports and protocols in use, while this may look like a good choice. In practice this often makes the infrastructure harder to manage which opens other possibilities for attackers. Obscurity is not security!

You can check which ports are in use by which service on a Windows system by using:

```
netstat -bona > portlist.txt
```

you can open the text file with for instance notepad portlist.txt

1.103.11 Visibility

To know when you are under attack or have been breached it is vital to have visibility in the whole data flow path. You should be able to know what is 'normal behavior' and what is NOT. Monitor your accounts and Veeam infrastructure for suspicious activity. Place virtual trip-wires, like e.g. creating a non-used admin account with alarms tied to it. When any activity on that account is observed, it will trigger a red alert instantly. There are several systems out there that can help you by alerting suspicious behavior so you get aware that someone is snooping around and is trying to gain access to your infrastructure. Visibility is Key!

It is important to get alerts as soon as possible while defending against other attacks like viruses, malware and ransomware. The biggest fear of these attacks is that they may propagate to other systems fast. Having visibility into for e.g. potential ransomware activity is a big deal.

Example Systems that could help you create visibility are:

- A system that detects possible ransomware activity is [Veeam ONE 9.5](#). There is a pre-defined alarm called "Possible ransomware activity." This alarm will trigger if there is a high CPU utilization combined with lots of writes to disk.
- VMware vRealize Network Insight can take VMs, objects, groupings and their physical elements and easily fingerprint the application and determine the internal and external flows, the client connections, etc. this way you get an analysis of what is 'normal' behavior and what is not.
- VMware vCenter with alerts that are triggered on virtual trip-wires.

1.103.12 Recovery Strategy

Have a recovery strategy in place, before you find out your infrastructure is breached you should know what to do when being compromised through attacks. Backup your data and make sure the backups cannot be accessed by an attacker to wipe them out. An offsite copy (air-gap) or read-only on any media is highly recommended to survive any attack.

The 3-2-1-0 backup rule

The 3-2-1 rule is very general and it works for all data types (individual and corporate) and all environment types (physical and virtual). When backing up VMware or Hyper-V environments with Veeam, this rule becomes the “3-2-1-0 backup rule” where 0 means “0 errors” during the automatic recoverability verification of every backup with Veeam’s *SureBackup*.

Veeam Backup & Replication™ can help you to fulfill all 3-2-1-0 backup rule requirements.

- **Have at least three copies of data:** Setup Backup Jobs to create several backups for each of your VMware or Hyper-V VMs.
- **Store the copies on two different media:** Veeam is storage-agnostic, meaning it supports tapes, disks, the cloud and more. You can store your backups to any of the listed media.
- **Keep one backup copy offsite:** Setup Backup Copy Jobs to transfer your backup offsite faster with built-in WAN acceleration, or use Veeam Backup Cloud Edition to store your backups to one of 15 public clouds, including Windows Azure, Amazon Glacier, Google Cloud Storage and more.

Educate your Staff

By deploying an employee awareness training you make sure that your employees are aware of strange behavior and of their critical roles in protecting the organization’s services and data. This is not only for the IT department, but for everyone within the organization, because every organization is becoming an IT company rapidly.

[^1]: KISS is an acronym for “Keep it simple, stupid” as a design principle noted by the U.S. Navy in 1960. The KISS principle states that most systems work best if they are kept simple rather than made complicated; therefore simplicity should be a key goal in design and unnecessary complexity should be avoided. A simple design is easier to overview and to secure as a whole. [Wikipedia](#)

1.104 Segmentation using Zones

Ultimately, all security is about protecting a valuable asset - in this case it is **Data** – but that protection involves a defence-in-depth strategy that includes all layers. To do a defence-in-depth, you should identify the most valuable data and build layers of defence around it to protect its availability, integrity and confidentiality.

A zone is an area having a particular characteristic, purpose, use and/or subject to particular restrictions. By using zones, you have an effective strategy for reducing many types of risks. While securing your environment much granular and better, you will also lower costs associated with it. Instead of protecting everything with the same level of protection, you associate systems and information to specific zones. As a side effect, systems that are subject to regulatory compliance can be grouped in subzones to limit the scope of compliance checking and therefore, reduce costs and time needed to complete long-winded audit processes.

Think about the importance of the data and systems in that particular zone and who should have access to it. Communication is only allowed between systems in adjacent zones. A common data classification for a zone is about shared availability, confidentiality, integrity, access controls, audit, logging and monitoring requirements.

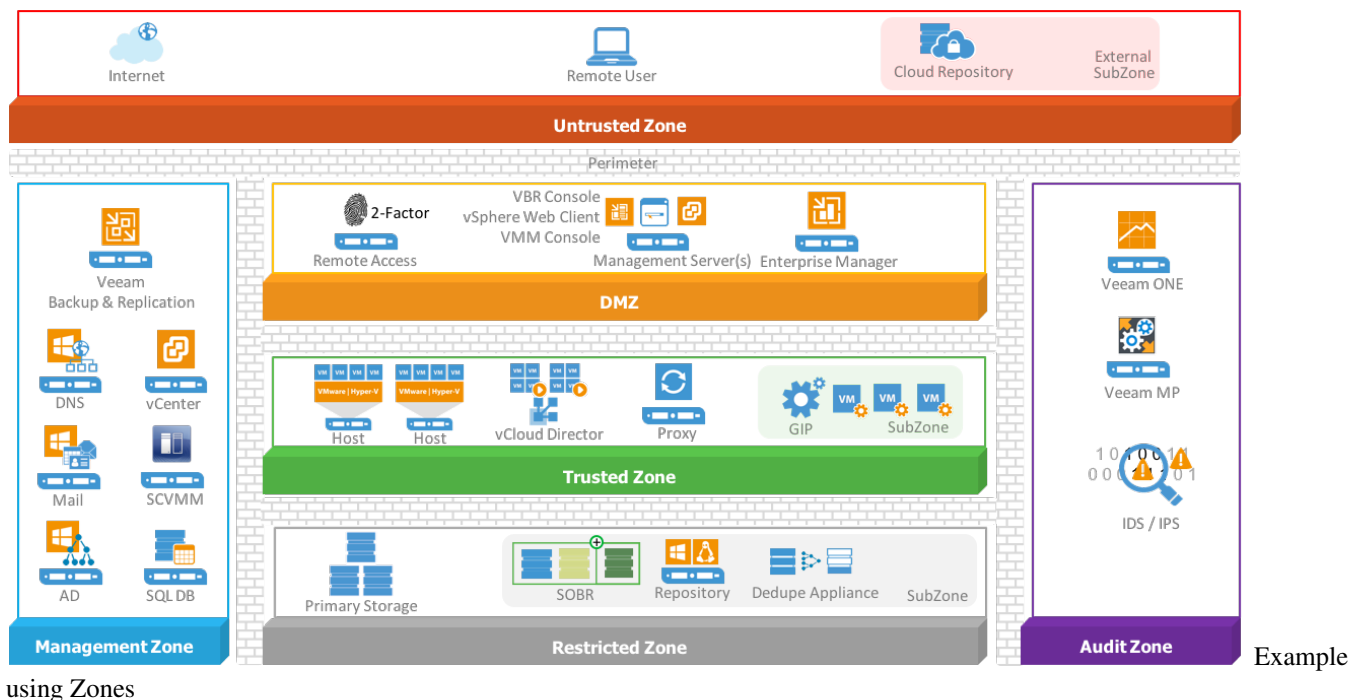
These common characteristics and requirements inherently lead to some level of isolation, but this isolation occurs not just between zones, but also within zones called subzones.

The attack surface of data and systems within a zone can be significantly reduced by exposing a limited number of services through the zone's perimeter and implementing strict access controls to limit access to specific groups of users. A potential attacker would have to gain access to all of the outer zones before getting to the restricted zone where the critical data is stored, reducing the likelihood of data theft or data mutilation. In addition, you are increasing the availability of these critical systems.

You could use a zone model as a strategic defence model which divides the different Veeam components into separate zones. Keep the following rules in mind while designing:

1. Secure by Design
2. Know what is important to secure and rank it
3. Know your attack vectors and possible ways to secure them
4. Use the principle of least privilege
5. Have insight in costs and benefits

Important: Be aware that there is no silver bullet that will solve all your security needs at once! There are numerous ways to achieve your goal. Security is a state of mind and needs to be looked after every single day. If you think you are secure, because you followed all best practices you got a false sense of protection! Look at your organization needs and then choose the best way that fits your organization taking into consideration money (budget), risks (attack vectors) and possible outcome (how does it fit in, what would be the damage).



using Zones

Implementing zones can be done in numerous ways depending on the approach you choose. But keep in mind that most of the threats nowadays are coming from the inside. Dividing your infrastructure into zones is a great way to provide better visibility into parts of greater importance. Without visibility it is sheer impossible to gain control and detect threats early. For hardening the Veeam Availability infrastructure components we place them in several logical zones.

One of the highest sought-after attack vector will be gaining access to management accounts and components. This will allow an attacker to gain access to most parts of the infrastructure instantly. While overlooking the major Veeam Backup & Replication components you will notice that there are three management components available.

The Veeam Backup & Replication Console also referred to as Console, the Veeam Backup & Replication Server which is the core component orchestrating all different jobs and ordering movement of data through the infrastructure and the Veeam Backup Enterprise Manager who federates multiple Backup Servers into a single pane of glass. Let's place all major Veeam Availability components into the defined zones.

1.104.1 Untrusted Zone

To keep a balance between security and operational efficiency you do not want to install the Veeam Backup & Replication Console on any system outside your organization infrastructure. But for operational efficiency you want to give your administrators the ability to connect to the infrastructure from any device and any location through remote access with only keyboard, mouse and video to their disposal.

For operational efficiency, you do not want to install Veeam Backup Console on machines on poor connections/long distance, there can be between 50-400 MB of data transferred between the console and backup repository when starting the console. If the first file mount is performed over a slow connection, it may take a considerable time to load the file-level recovery wizard. If there is significant latency between the backup repository and console, it is recommended to deploy an instance of the console on or closer to the repository server.

Deploy a firewall on the perimeter between the untrusted zone and the DMZ zone. On the firewall and/or dedicated RDS Gateway server add 2-factor authentication for remote administrators to access the RDS Gateway. Deny the mapping of drives, printers, clipboard etc. on the RDS Gateway to secure your infrastructure against dropping of content or files from any remote machine.

1.104.2 DMZ

The DMZ houses systems that require exposure to the untrusted zone. This zone proxies access between systems in the DMZ and the Management Zone. Also, all traffic should be funneled through systems in the DMZ to reach Internet resources. The systems deployed in this zone should be tightly controlled and hardened to reduce attack surface.

The Veeam Backup & Replication console is a client-side component that provides access to the backup server. The console lets several backup operators and admins log in to Veeam Backup & Replication simultaneous and perform all kind of data protection and disaster recovery operations as if you work on the backup server.

Install the Veeam Backup & Replication console on a central management server that is positioned in the DMZ zone and make sure its protected with 2-factor authentication. You can also install other infrastructure tools on this management server like for instance the Microsoft VMM Console and/or VMware vSphere Client to manage your hypervisor deployment.

The Veeam Enterprise Manager will also be in the DMZ zone, because it serves as a Self-Service portal for specific user-groups in the organization.

1.104.3 Management Zone

In the management zone, you place infrastructure services like DNS, Active Directory and SMTP. But also, the VMware vCenter server and/or Microsoft System Center Virtual Machine Manager (SCVMM). From the Veeam components the Veeam Backup & Replication Server(s) will be in this Management zone. The Veeam Backup Server will orchestrate all jobs and update all Veeam components in the different zones from a central location.

The Microsoft SQL Database server, which is needed to host the Veeam Backup Database and the Veeam Enterprise Backup Database should be placed in this zone if it is dedicated just for Veeam. It is a good practice to use a dedicated SQL server which hosts the different SQL instances for infrastructure components and a different SQL server for SQL instances for business processes. The Veeam Backup & Replication server is a heavy user of the SQL server and by placing the SQL database server close by gains you operational efficiency.

The VMware vCloud Director is part of a subzone within the management zone and controls the vAPP's running in subzones within the Trusted Zone.

The management zone requires secure and controlled access to the internet to download licenses and updates for different components in the infrastructure. It is highly recommended to use an Internet Proxy or Reverse Proxy situated in the DMZ as a controlled gateway to the internet.

All types of Cloud Repositories should be placed in subzones within the Untrusted zone. Organization data is leaving the security boundaries so make sure that, as an extra precaution, data towards these cloud repositories is encrypted during transport and when stored in the cloud repository. The Veeam Backup & Replication server will communicate with the Cloud Gateway service for transport of data to the Cloud Provider, Azure Proxy or AWS deployment.

1.104.4 Trusted Zone

The trusted zone will be populated with hypervisor hosts like VMware ESXi and/or Microsoft Hyper-V hosts. All components in the Trusted zone will need access to different services in the Management zone. The Veeam Proxy servers, which are the data movers, are part of the trusted zone.

Veeam Proxies can back up the VMs without having access to the Guest OSes themselves. If you back up or replicate running VMs, you can enable guest processing options. Guest processing options are advanced tasks that require Veeam Backup & Replication to communicate with the VM guest OS. When VMs are separated in subzones you can deploy and leverage the Veeam Guest Interaction Proxy (GIP) in the Trusted Subzone, which will have secure access and deploys the needed runtime in the VM for guest processing tasks.

In the case that different business units or customers are running in the trusted zone you should think about running them in subzones of the trusted zone. But be aware that overly complex designs can be counterproductive and give a misplaced feeling of being safe.

VMware vCloud Director vAPP's are also part of the Trusted Zone and would normally be divided in subzones per business unit or tenant. Veeam can capture whole vApps and vCloud Director configurations within the backup jobs.

1.104.5 Restricted Zone

Primary storage, where production data and VM's reside, but also other components which store data should be placed in this restricted zone. This zone should never be accessible by any user directly. Only available to the virtual infrastructure components and application servers and administrators with strict rights. Also, the Veeam Scale Out Backup Repository (SOBR), Simple Repository, Deduplication devices or Cloud Repository when used in combination with Veeam Cloud Connect for Enterprise (VCC-E) should be part of this zone. For organizations using VCC-E it is possible to define cloud repositories on top of their SOBR or as separate defined cloud repositories in a Restricted Zone subzone.

1.104.6 Audit Zone

Visibility is key to protect, detect and contain threats early. In this zone monitoring solutions like Veeam ONE and/or Veeam Management Pack in combination with Microsoft System Center are placed. Also IDS and IPS systems should be placed in this Audit zone.

1.105 Hardening Backup Repository - Linux

Veeam Backup & Replication, even if it's mainly Windows based software, can also consume Linux servers as its backup repositories. The requirements are bash shell, SSH and Perl. Please check the full list of required Perl modules here: <https://www.veeam.com/kb2216>.

Important: 64-bit edition of Linux must be able to run 32-bit programs. Pure 64-bit Linux editions are not supported (Perl installation must support 32-bit variables).

Best Practices for Hardening Veeam Backup Repositories based on Linux are: 0. **K.I.S.S. design** - Keep It Simple and Straightforward.

1. Make sure the servers are physical secured.
2. *Create a dedicated repository account* for Veeam, that can access the folder where you store backups.
3. *Set permissions on the repository directory* to only that account.
4. You do not need Root to use a Veeam Linux Repository. Also do not use SUDO.
5. *Modify the Firewall*, with dedicated rules for Veeam to allow access to specific ports.
6. Use *Veeam encryption* while storing backups on the repository.

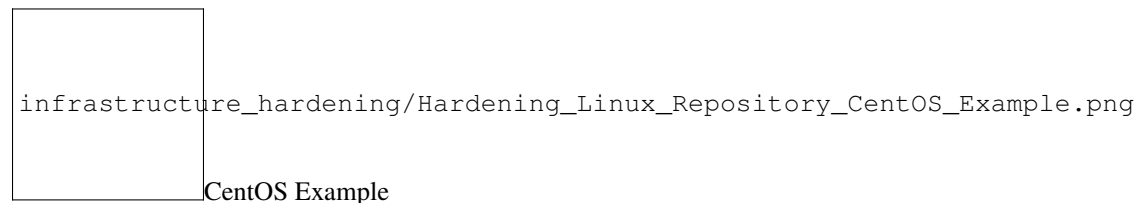
**** Note:**** In the example below CentOS is used as linux distribution, please adapt the different commands to your own distribution if needed.

1.105.1 Create a Dedicated Repository Account

Veeam only needs a regular user that has sufficient permissions to the folder where you want to store backups. Not even sudo is required. Besides, it is generally not considered best practice to provide sudo access to accounts used for Linux repositories. Far better is to create a restricted user and set the permissions on the repository directory to only that user.

Actually, the only real reason Veeam may need a root account at all is to initially modify sudoers, but if people are willing to add the Veeam user account to sudoers manually (or via some configuration management) then we don't need a root account as we'll just use a regular account and sudo when required for things like file restore.

CentOS allows to create a new regular user directly during the installation process:



Let's say we didn't create any user yet, so we only have the root account in this machine. We first create a new dedicated user for our backups:

```
useradd -d /home/repouser -m repouser
passwd repouser
```

1.105.2 Set Permissions on the Repository Directory

In this new Veeam Linux Repository we mounted a new backup volume as `/mnt/veeamrepo` with 200GB of free space.

```
[root@linuxrepo ~]# df -hT
```

Filesystem	Type	Size	Used	Avail	Use%	Mounted on
/dev/mapper/cl_linuxrepo-root	xfs	8.0G	1.5G	6.5G	19%	/
devtmpfs	devtmpfs	1.9G	0	1.9G	0%	/dev
tmpfs	tmpfs	1.9G	0	1.9G	0%	/dev/shm
tmpfs	tmpfs	1.9G	8.5M	1.9G	1%	/run
tmpfs	tmpfs	1.9G	0	1.9G	0%	/sys/fs/cgroup
/dev/sda1	xfs	1014M	186M	829M	19%	/boot
/dev/rbd0	xfs	200G	33M	200G	1%	/mnt/veeamrepo
tmpfs	tmpfs	380M	0	380M	0%	/run/user/0

Mounted

Example

Let's set the folder permissions so the newly created user is only allowed access to this folder /mnt/veeamrepo

```
chown repouser.repouser veeamrepo/
```

```
chmod 700 veeamrepo
```

With these commands we changed the ownership of the folder to the user `repouser`, and we gave full permissions to this user only, over the folder. Only this user has `rwX` permissions. All other accounts would be denied access.

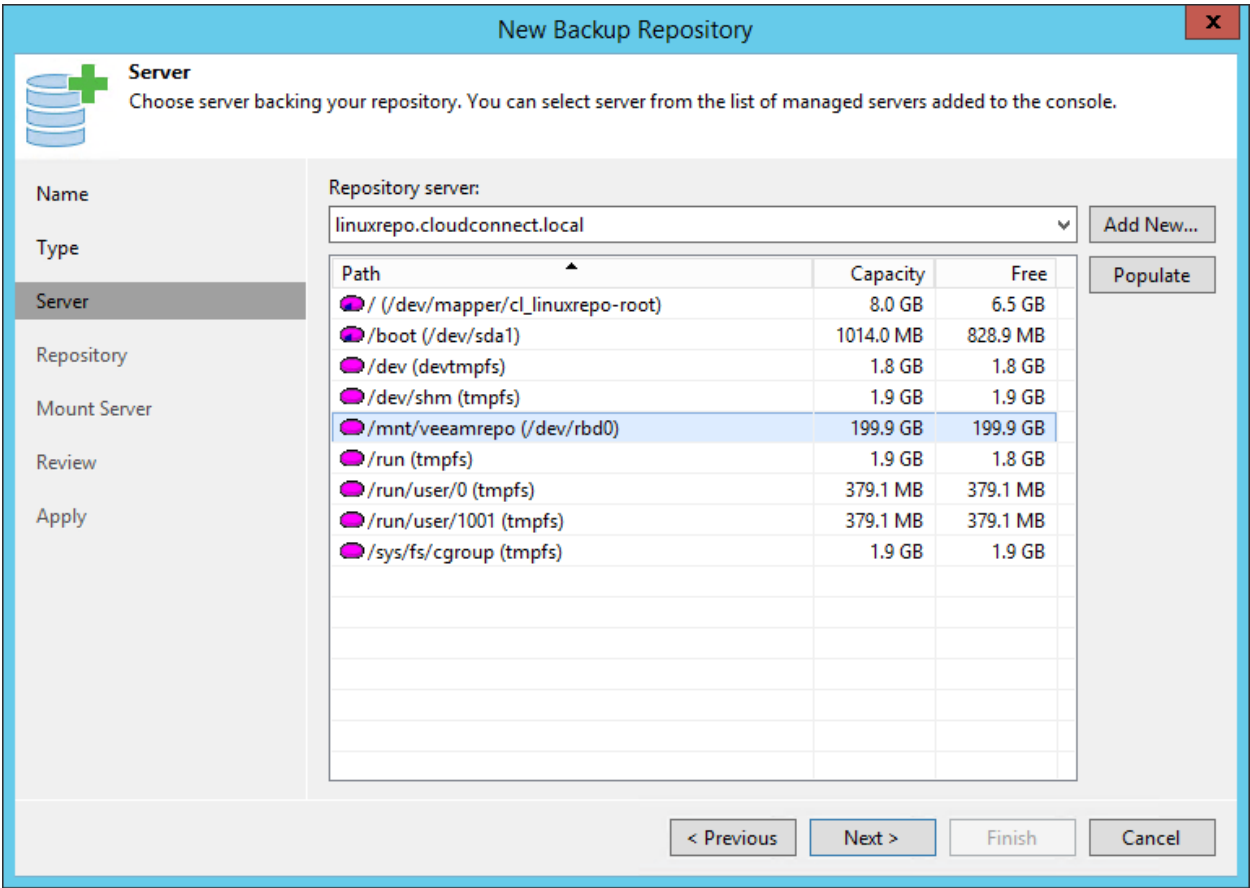
1.105.3 Configure the Linux Repository in Veeam

Open the Veeam Backup & Replication console and add a Linux Repository. At the credentials step, register the username you created before, with its password:

Credentials

Note: Before you can populate the list of available folders, remember you need to have the required Perl modules installed.

If the software prerequisites are all satisfied, you will see the volume among the available ones:



AddRepo

Select the volume and complete the wizard and have your Linux repository ready to be used.

1.105.4 Modify the Firewall

Before starting any backup, there's one more thing you need to configure: just because you were able to connect through ssh, you may think that the Linux firewall is not enabled, but in reality, it is enabled. So, if you just try to run a backup, at the *initializing storage* step, you will get an error:

ACTION	DURATI...
✓ Queued for processing at 10/19/2017 12:50:21 AM	
✓ Required backup infrastructure resources have been assigned	
✓ VM processing started at 10/19/2017 12:50:27 AM	
✓ VM size: 40.0 GB	
✓ Storage initialized	0:00:19
✗ Error: A connection attempt failed because the connected party did not proper...	
✓ Network traffic verification detected no corrupted blocks	
✗ Processing finished with errors at 10/19/2017 12:50:54 AM	

Error

The error says, *A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond 10.10.51.51:2500*. This error says that the proxy tried to connect to the repository over port 2500 (one of the dynamic RPC ports Veeam uses) but this port was not reachable. This is because the firewall is still up and running.

You can test if the firewall was enabled by running these two commands:

```
systemctl disable firewalld
systemctl stop firewalld
```

Run the backup again and if it did not fail this time you know that you have to create some dedicated rules for Veeam in the firewall.

Rules that need to be added are:

Source	Target	Protocol	Port	Notes
Backup Server	Backup Repository (Linux)	TCP	22	Port used as a control channel from the console to the target Linux host.
Backup Server	Backup Repository (Linux)	TCP	2500 - 5000	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.
Backup Repository (Linux)	Backup Server	TCP	2500 - 5000	Default range of ports used as data transmission channels. For every TCP connection that a job uses, one port from this range is assigned.
Backup Proxy	Backup Repository (Linux)	TCP	22	Port used as a control channel from the console to the target Linux host.
Backup Proxy	Backup Repository (Linux)	TCP	2500 - 5000	Default range of ports used as transmission channels for replication jobs. For every TCP connection that a job uses, one port from this range is assigned.
Backup Repository (Linux)	Backup Proxy	TCP	2500 - 5000	Default range of ports used as transmission channels for replication jobs. For every TCP connection that a job uses, one port from this range is assigned.
Backup Repository (Windows)	Backup Repository (Windows)	TCP	2500 - 5000	Default range of ports used as transmission channels for backup copy jobs. For every TCP connection that a job uses, one port from this range is assigned.
Backup Repository (Windows)	Backup Repository (Linux)	TCP	2500 - 5000	Default range of ports used as transmission channels for backup copy jobs. For every TCP connection that a job uses, one port from this range is assigned.
Backup Repository (Linux)	Backup Repository (Windows)	TCP	2500 - 5000	Default range of ports used as transmission channels for backup copy jobs. For every TCP connection that a job uses, one port from this range is assigned.
Backup Repository (Linux)	Backup Repository (Linux)	TCP	2500 - 5000	Default range of ports used as transmission channels for backup copy jobs. For every TCP connection that a job uses, one port from this range is assigned.

Firewall

Rules

1.105.5 Use Veeam Encryption

Regarding keeping root out of the backup folder on the Linux Repository, there is really no practical way to do this. Some would say you can create a SELinux/Apparmor policy, but, the problem is, the user that is root can almost certainly reboot the system with these policies disabled and/or change these policies.

Otherwise, in every other scenario like the one described, root can access the folder as much as the dedicated user. The normal way in the Linux world is, if you want to protect your files from root, would be to use per-user encryption. This is why many Linux distributions ask you to setup home directory encryption during install. The root user can still access the files, but all of the data is encrypted and cannot be read without the passphrase. Veeam recommends using [Veeam encryption](#) for this use case to provide the same level of protection.

1.106 Hardening Backup Repository - Windows

A good way of hardening the backup repository is by running it on a standalone Windows Server with storage attached to it. Create/Use a local account with administrative access and make sure only this (newly created) account has access rights to the location where the backup files are being stored. Veeam needs a local account with administrative access to function properly.

Best Practices for Hardening Veeam Backup Repositories based on Windows are:

1. [K.I.S.S. design](#) - Keep It Simple and Straightforward.
2. Use a [standalone Windows Server](#) which is not part of any Active Directory Domain.
3. Make sure the repository servers are [physical secured](#).

4. *Use a local account with administrative access*
5. *Set permissions on the repository directory* to only that local account.
6. *Modify the Firewall*, with dedicated rules for Veeam to allow access to specific ports.
7. *Disable remote RDP services* to the repository servers.
8. Use **Veeam encryption** while storing backups on the repository.

1.106.1 Standalone and Physical secured

When protecting the whole environment you do not want the Veeam repository to be tied to the same Windows Active Directory domain you are protecting with the backup. Otherwise if everything is lost you could have a chicken and egg problem around accounts wanting to authenticate against a domain which is no longer available.

Furthermore if a Domain Admin account is compromised you do not want that account to be able to overrule a backup repository account password so the hacker gets access to the backup files together with access to the whole environment.

Place the repository servers in a Restricted Zone, because these servers contain a 100% copy of your production environment! The repository servers should be physical secured, and have appropriate access control systems in place. This way access is restricted, who does have access is registered and monitored at certain specified levels.

1.106.2 Local Account with administrative access

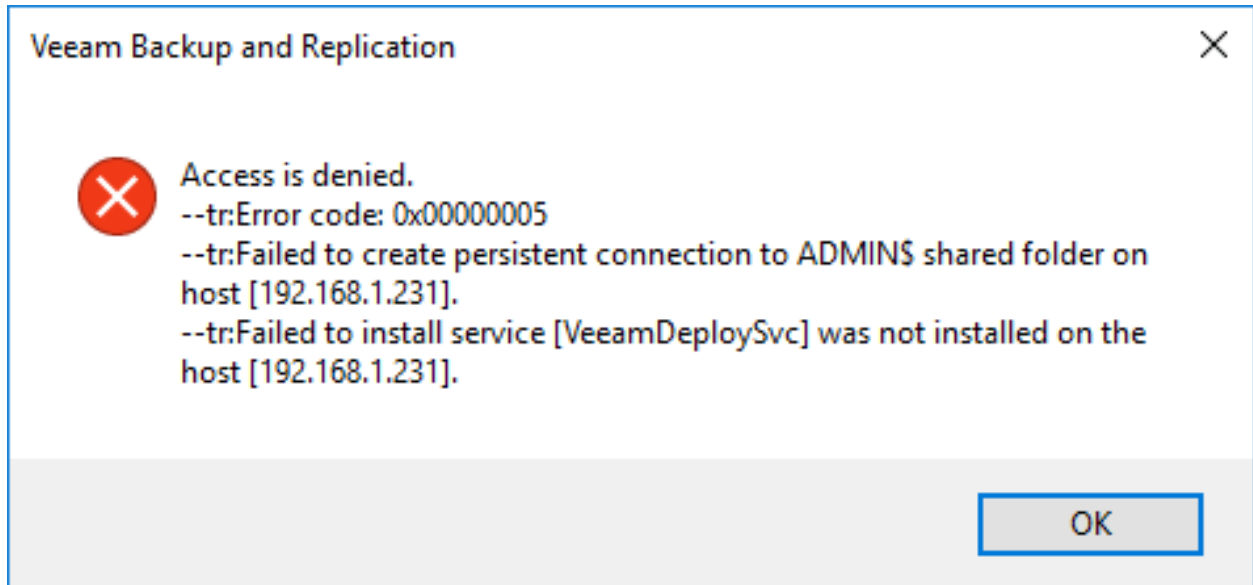
The easiest and best way to leverage a local account with administrative access to the repository server is by using the builtin Local Administrator account. As an extra precaution make sure you rename the account so a potential hacker has to guess the account name *and* the password. By using local Account specific per Veeam Backup Repository server you increase the level of protection. In the event that one of those accounts get compromised the other repository servers stay secure.

When your organisation does *not allow* you (e.g. global security policy) to use the builtin local administrator account, you can create a new local account and give it administrative access. Make sure the Local Administrator account is highly secure in this case.

Note: UAC affects connections for nondomain/local user accounts. If you connect to a remote computer using a nondomain/local user account included in the local Administrators group of the remote computer, then you must explicitly grant remote DCOM access, activation, and launch rights to the account. User Account Control (UAC) access-token filtering can affect which operations are allowed or what data is returned. Under UAC, all accounts in the local Administrators group run with a standard user access token, also known as UAC access-token filtering. An administrator account can run a script with an elevated privilege “Run as Administrator”. Some securable objects may not allow a standard user to perform tasks and offer no means to alter the default security. In this case, you may need to disable UAC so that the local user account is not filtered and instead becomes a full administrator. One important thing to know is that UAC is not a security boundary. UAC helps people be more secure, but it is not a cure all. UAC helps most by being the prompt before software is installed. This part of UAC is in full force when the “Notify me only when...” setting is used. UAC also prompts for other system wide changes that require administrator privileges which, considered in the abstract, would seem to be an effective counter-measure to malware after it is running, but the practical experience is that its effect is limited. For example, clever malware will avoid operations that require elevation. Be aware that for security reasons, *disabling UAC should be a last resort*.

The downside of creating a newly administrative local account is that you will need to disable Remote User Account Control (UAC) because this Windows function prevents local accounts from running in an elevated mode when connecting from the network. Veeam accesses the ADMIN\$ and C\$ through the Installer Service with the local account you presented while adding the Windows server to Infrastructure in Veeam Backup & Replication.

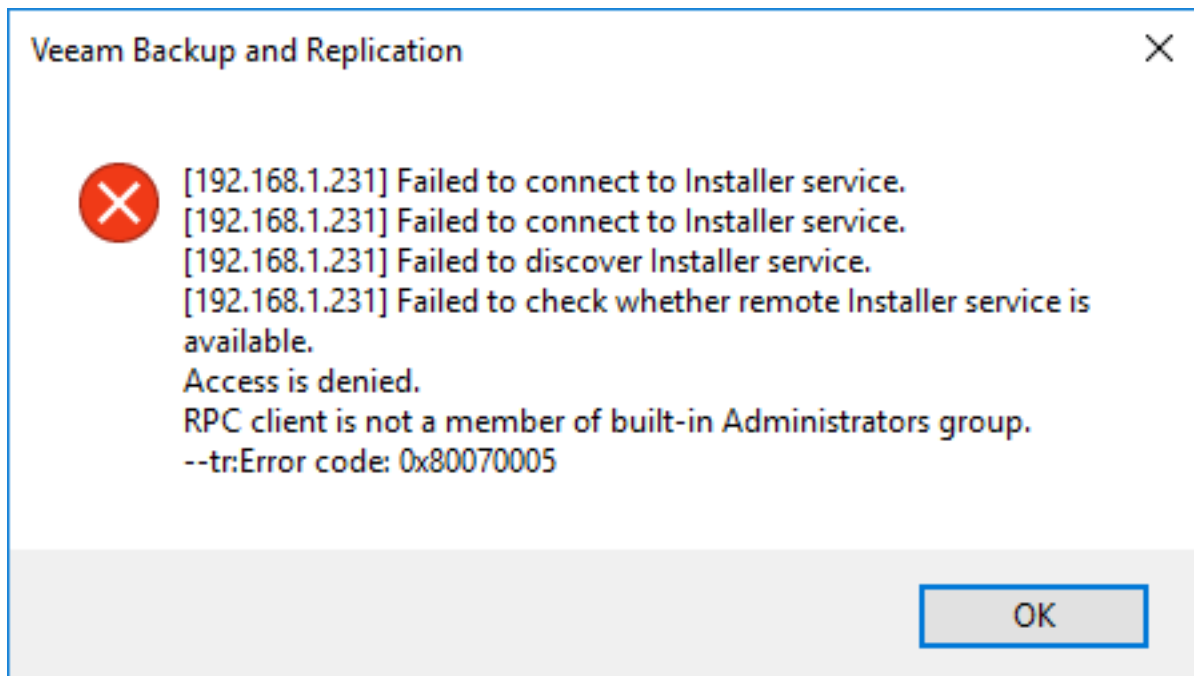
The connection will fail with the following error message: *Access is denied --tr:Error code: 0x00000005[^1] --tr:Failed to create persistent connection to ADMIN\$ shared folder on host [host name or ip-address] --tr:Failed to install service [VeeamDeploySvc] was not installed on the host [host name or ip-address] when Remote UAC is Enabled on the Windows Server.*



UAC

Error 0x00000005

or with the error message: *RPC Client is not a member of built-in Administrators group. --tr:Error code: 0x80070005 when the server was already added as a Veeam Backup Repository through Infrastructure within Veeam Backup & Replication.*



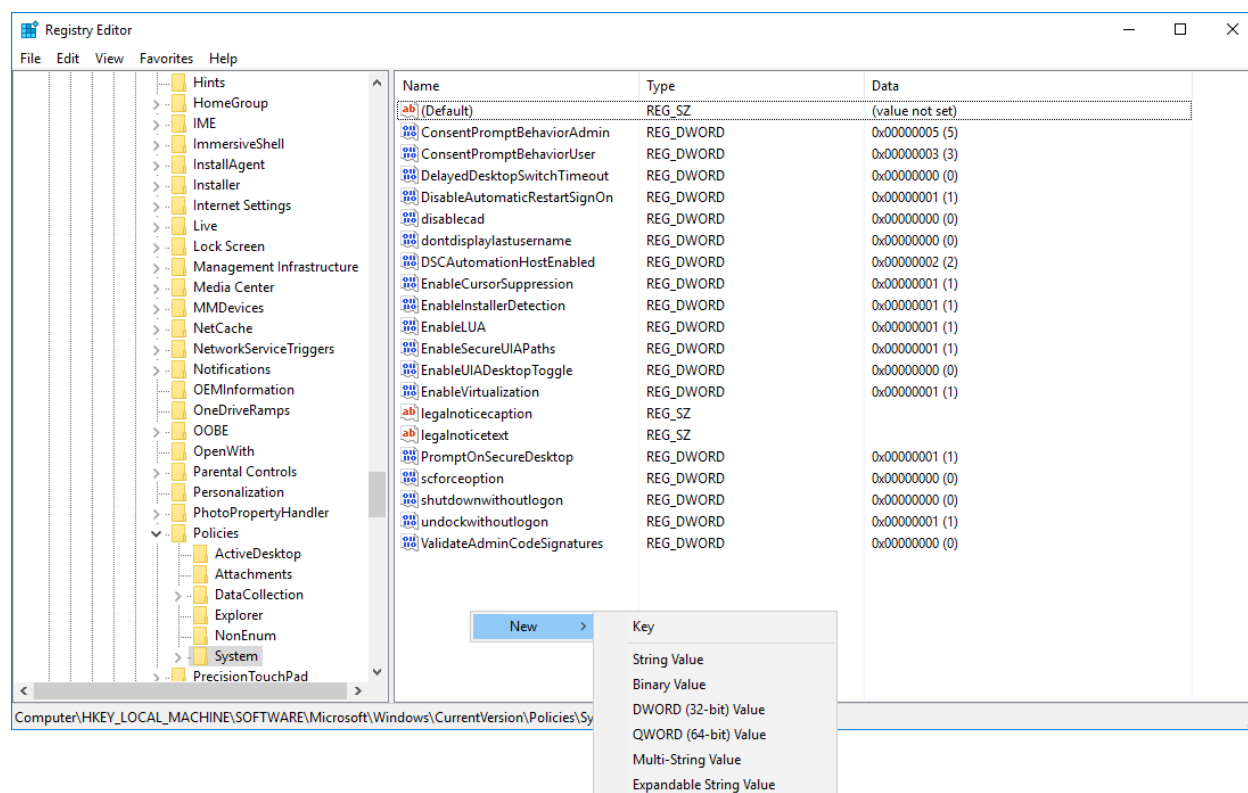
RPC

Error 0x80070005

The Veeam Installer service pushes the Veeam binaries through the ADMIN\$ and C\$ share on the target machine. It also uses administrative shares later on for other jobs.

You can disable Remote UAC on the repository server by using REGEDT32 to navigate to the following registry path:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System



LocalAccountTok

Add a new Key with type DWORD (32-bit) Value and name it LocalAccountTokenFilterPolicy give it a value of 1. No restart is needed.

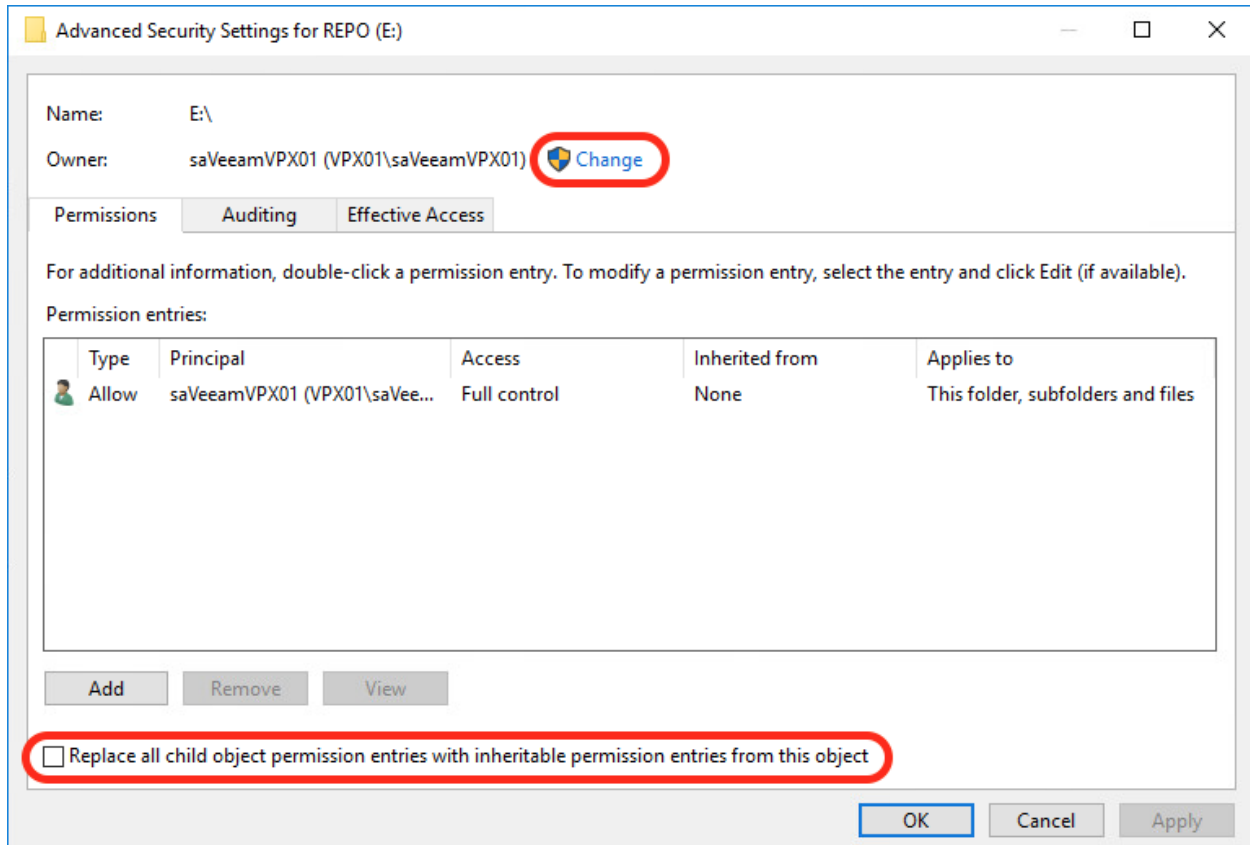
1.106.3 Set permissions on the repository directory

Login with the newly created local account or with the renamed local administrator and open File Explorer, locate the disk(s) where the backup files will be placed (or are already there in an existing deployment). Open the properties of the disk and Add the used account and give it Full access. Tick all Allow boxes.

Remove all accounts except the SYSTEM and the account you are using.

Important: the SYSTEM group account can also be removed, *but* then the Veeam services need to start with the local administrative account used instead of Local System otherwise the backups will fail. Keep the KISS principle in mind here.

After adding the used administrative account on the security tab of the disk(s) where backups will reside. Open the advanced security settings and Change the Owner. When there are already backup files on this disk make sure to tick the box: *Replace all child objects permissions entries with inheritable permissions entries from this object.*



AdvancedSecurity

1.106.4 Modify the Firewall

You have three options to make the first install of Veeam components, pushed from the Veeam Backup & Replication server, a success. From most preferred to least preferred option:

1. Keep Windows Firewall On and add three new firewall rules.
2. Keep Windows Firewall On and manual install the Veeam Installer Service (VeeamDeploySvc)
3. Switch Windows Firewall Off and enable File and Printer Sharing during the first install

Option 1 - Windows Firewall On and add three new firewall rules From a command prompt run the following three commands to add three new rules to the Windows Firewall:

```
netsh advfirewall firewall add rule name="Veeam (DCOM-in)" dir=in action=allow
protocol=TCP LocalPort=135 enable=yes program="%systemroot%\system32\svchost.
exe" service=RPCSS remoteip=<VBR Server IP-address>
```

```
netsh advfirewall firewall add rule name="Veeam (SMB-in)" dir=in action=allow
protocol=TCP LocalPort=445 enable=yes program="System" remoteip=<VBR Server
IP-address>
```

```
netsh advfirewall firewall add rule name="Veeam (WMI-in)" dir=in action=allow
protocol=TCP LocalPort=RPC enable=yes program="%systemroot%\system32\svchost.
exe" service=winmgmt remoteip=<VBR Server IP-address>
```

After adding these firewall rules nothing else has to be done to the Windows server to be added to the Veeam Infrastructure components. You also do not have to switch on File and Printer Sharing specifically.

Tip: You can also store these three commands in a windows bat file and run that on every Windows server you are preparing to use as a Veeam Infrastructure component.

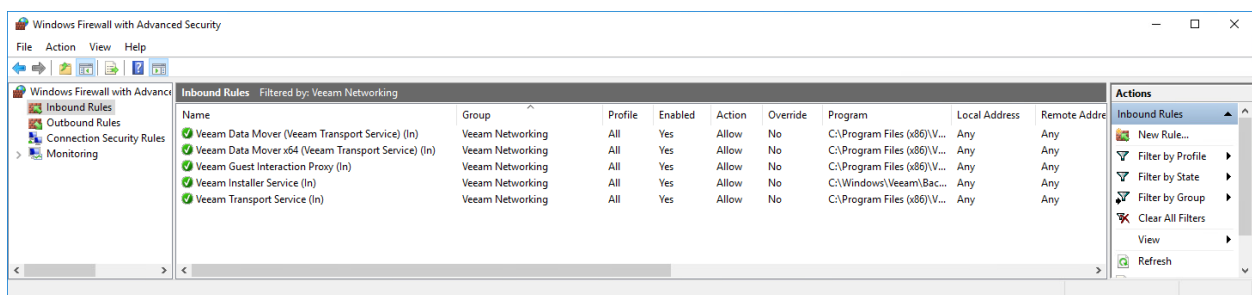
Option 2 - Windows Firewall On and manual install of Veeam Deployment Service Open the CMD utility on the repository server and create a folder C:\Windows\Veeam\Backup

```
mkdir C:\Windows\Veeam\Backup
```

Copy two files named: VeeamDeploymentDll.dll & VeeamDeploymentSvc.exe from the Veeam Backup & Repository server path C:\Program Files\Veeam\Backup and Replication\Backup\Packages

Tip: Use TAB key for auto completion.

Run on the Veeam repository server in the directory C:\Windows\Veeam\Backup through CMD the following command: VeeamDeploymentSvc.exe -install this way the Veeam installer service will be installed. Veeam will add Firewall rules for Veeam during installation, which are visible as *Veeam Networking* in the firewall under Allowed apps and features.



Veeam

Network Firewall Rules

Tip: this manual install process can be interesting for so called 'Dark Sites'. With the command: VeeamDeploymentSvc.exe -uninstall you can remove the installation services.

Option 3 - Windows Firewall Off and enable File and Printer Sharing Disable the Windows Firewall for the Private Networks during the initial Veeam installation. This way the right binaries gets pushed to the Windows repository server. Veeam will add Firewall rules for Veeam during installation, which are visible as *Veeam Networking* in the firewall under Allowed apps and features. After the process completed successful make sure you enable the Windows Firewall again!

1.106.5 Disable remote RDP services

Veeam Backup Repositories are (most) often physical. An extra security measure is to disable any remote RDP access in Windows and use a KVM-over-IP switch to access this machine remotely in the datacenter.

[^1]: Error code 0x00000005 refers to Remote UAC and local administrative account but not the original local administrator, code 0x00000040 refers to Server service stopped/crashed no administrative shares available, 0x00000057 multiple same usernames in Veeam credentials manager with different passwords

1.107 Backup & Replication Anatomy

You might have a basic understanding of how Veeam Backup & Replication components interact, but do you know what happens in detail with each component when you backup a VM, do a standard VM restore, an Instant VM Restore, a Windows File-Level restore, or replicate a VM? The next sections are dedicated to explaining in detail what actually happens during these processes.

1.108 Backup

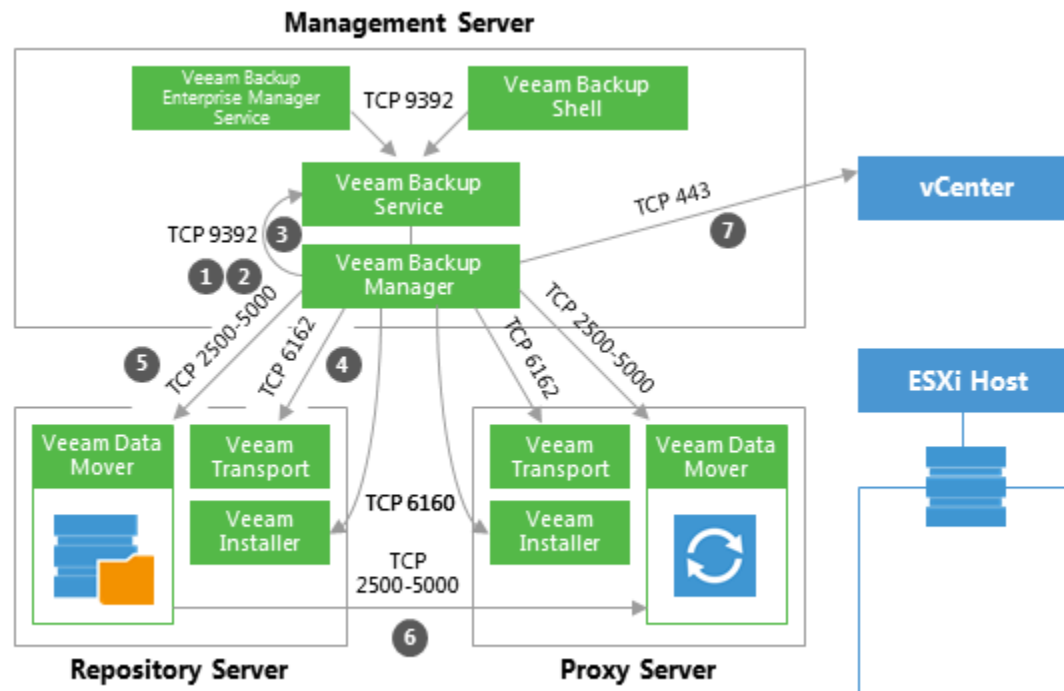
This section provides a step-by-step description of a VMware virtual machine backup process implemented in Veeam Backup & Replication.

1.108.1 1. Initialization Phase

A backup job can be started automatically or manually in the Veeam Backup & Replication console, Veeam Backup Enterprise Manager web console, by means of PowerShell, RESTful API and other.

In the initialization phase, Veeam Backup & Replication prepares resources necessary for a backup job. To help you better understand firewall settings and connection initiation flow, the process is illustrated by the diagram (see below):

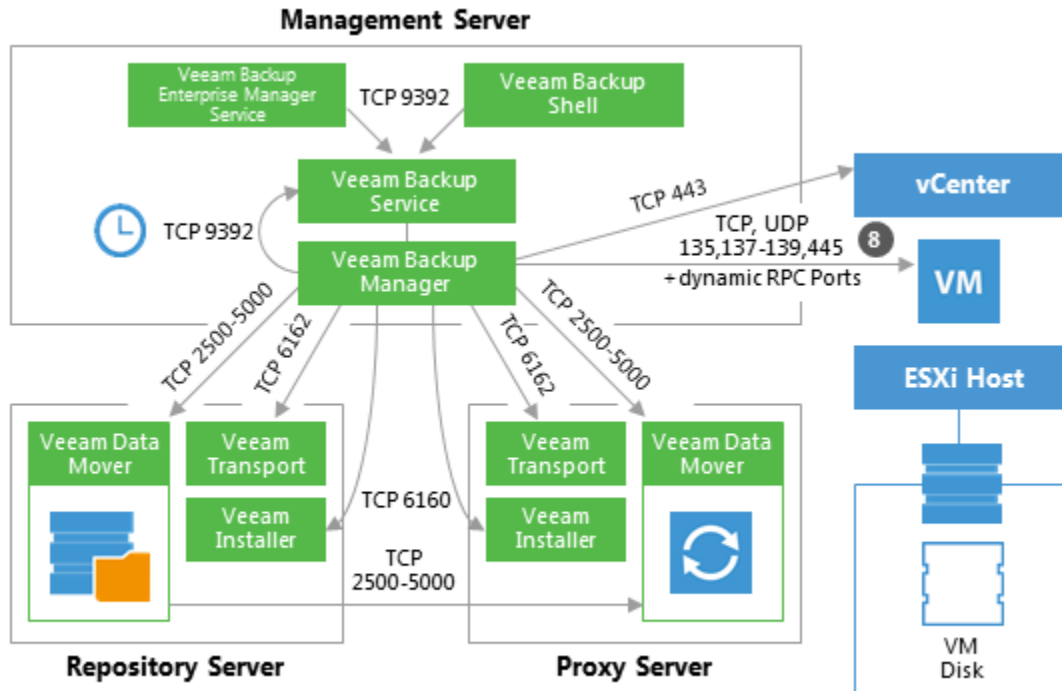
1. When a backup job is initialized, the Veeam Backup Manager process is started on the Veeam backup server.
2. Veeam Backup Manager reads job settings from the Veeam Backup configuration database and creates a list of VM tasks to process (one task stands for one VM disk).
3. Veeam Backup Manager connects to the Veeam Backup Service. The Veeam Backup Service includes a resource scheduling component for managing all tasks and resources in the backup infrastructure. The resource scheduler checks what resources are available, and assigns backup proxies and repositories to process that job tasks using Veeam's load balancing.
4. After the necessary backup infrastructure resources have been assigned, Veeam Backup Manager connects to the Transport Services on the target repository and on the backup proxy. The Transport Services, in their turn, start the Veeam Data Movers. On the backup proxy, a new Veeam Data Mover is started for each task that the proxy is processing.
5. Veeam Backup Manager establishes a connection with Veeam Data Movers on the backup repository and backup proxy, and sets a number of rules for data transfer (such as network traffic throttling rules, and so on).
6. Veeam Data Movers on the backup proxy and repository establish a connection with each other for data transfer.
7. Veeam Backup Manager connects to the vCenter Server or ESXi host and gathers metadata about VMs and hosts engaged in the backup process. At this step, no connection between the Veeam backup server and VM guest networks is established.



1.108.2 2a. Guest Processing for Windows-Based VMs

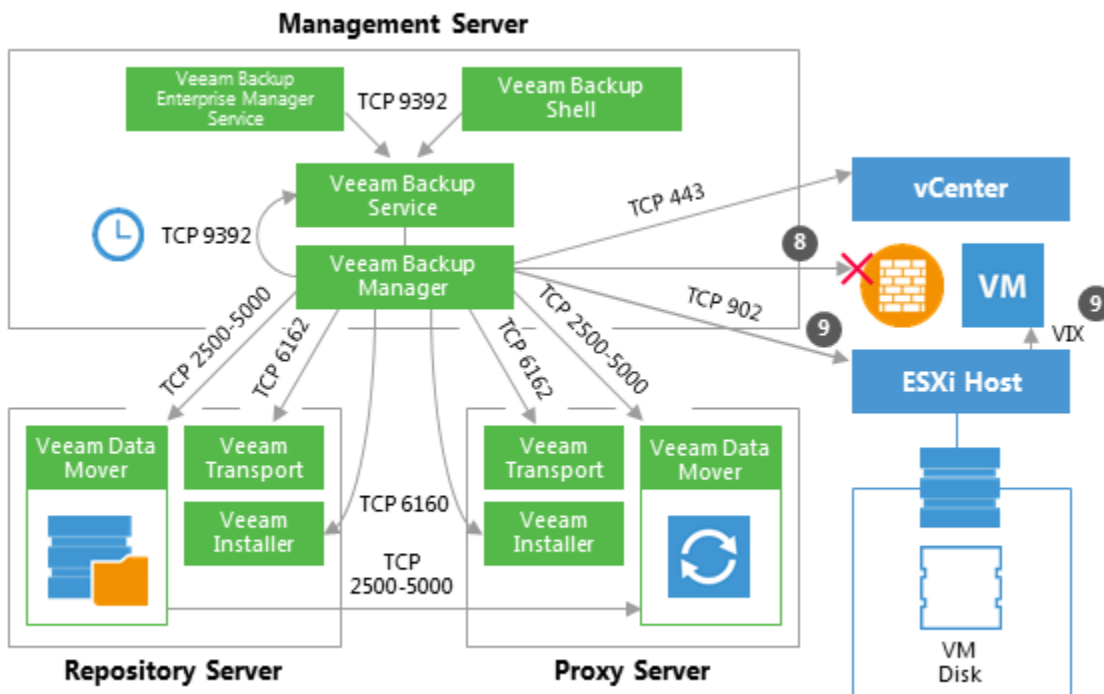
For VMs with Microsoft Windows guest OS, Veeam Backup & Replication obtains information about the guest's IP addresses from VMware Tools. Veeam uses these IP addresses to connect to the guest OS and perform in-guest processing tasks (if application-aware image processing is enabled).

If it is not possible to connect to the guest OS or the connection is blocked by a firewall, Veeam Backup & Replication tries to establish a connection using VIX, as described in section 2b.



1.108.3 2b. Guest Processing for Windows-Based VMs (VIX)

If there is no network connectivity to the VM guest OS, Veeam Backup & Replication uses the communication channel provided by VMware Tools (VIX) to interact with the guest OS and perform in-guest processing tasks.



1.108.4 2c. Guest Processing for Linux/Unix-Based VMs

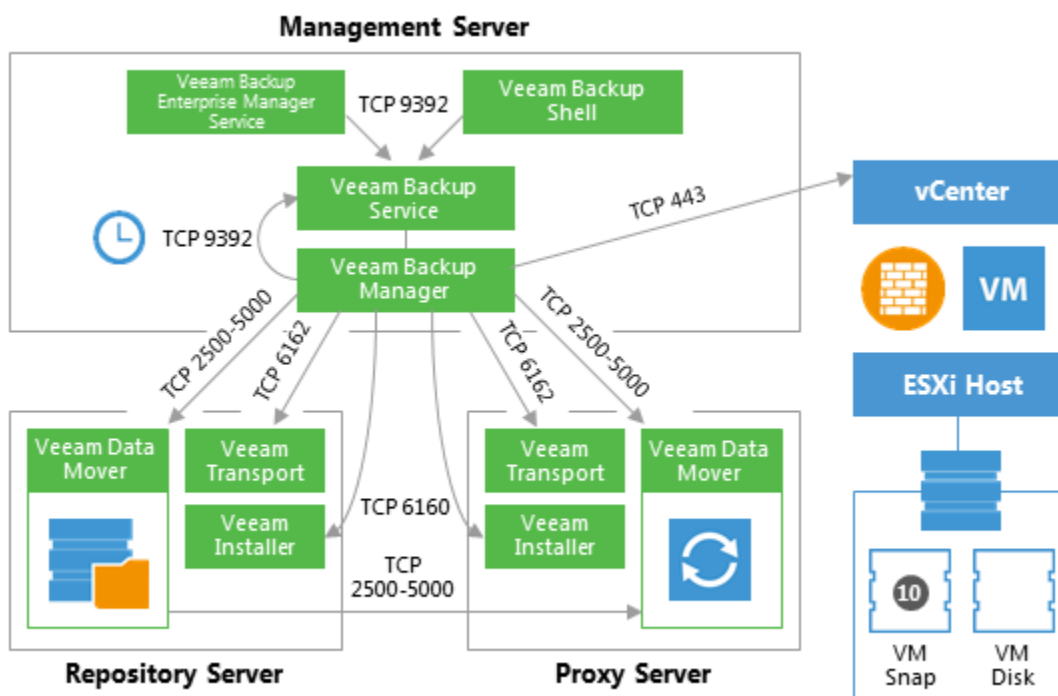
If pre-freeze and post-thaw scripts are enabled in the backup job properties, Veeam Backup & Replication obtains information about the guest's IP address from VMware Tools. Veeam uses this IP address to connect to the guest network over SSH and perform in-guest processing tasks. Scripts reside on the backup server and are injected in the guest OS at the time of backup.

If there is no network connectivity with a Linux-based VM, Veeam Backup & Replication will not fail over to the VIX communication channel. In such cases, as an alternative method, you can use VMware Tools quiescence and let VMware Tools run the necessary scripts that will need to be created inside the guest OS (see location details for Windows / Linux guest at: https://pubs.vmware.com/vsphere-50/topic/com.vmware.datarecovery.admin.doc_20/GUID-6F339449-8A9F-48C0-BE70-91A2654A79D2.html).

However, it is recommended to use Veeam's functionality to call pre-freeze and post-thaw scripts, as this method is more controllable by the Veeam code: all errors that occur during the backup process are written to Veeam logs (not VMware Tools).

1.108.5 3. Creating a VM Snapshot

Now, Veeam Backup & Replication requests the vCenter Server or ESXi host to initiate a VM snapshot creation. A VM snapshot is required to use VMware VADP backup methods and leverage features like VMware Changed Block Tracking (CBT).



1.108.6 4. Releasing the Guest OS Activities

Right after the VM snapshot is taken, all quiesced disk I/O activities in the guest OS are resumed.

1.108.7 5. VM Data Transport

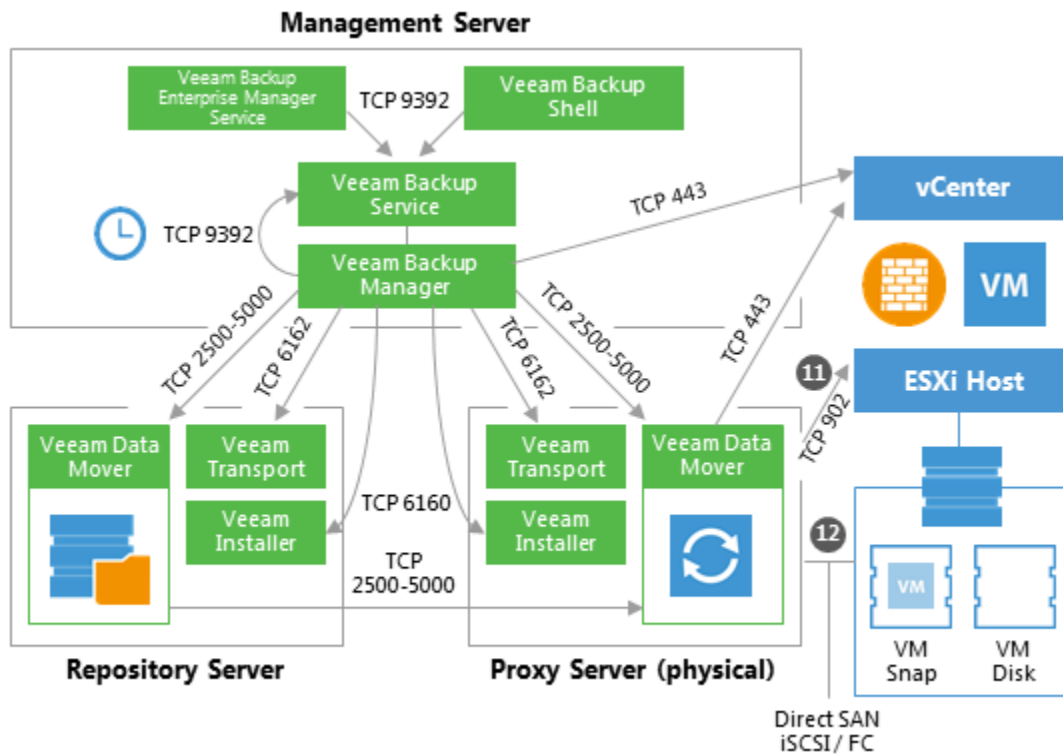
To read and transfer data from the VM snapshot, Veeam Backup & Replication can use one of the following transport modes:

- Direct SAN Access
- Virtual Appliance (HotAdd)
- Network (NBD)

For more information about each transport mode, see [Veeam Backup & Replication User Guide](#) or a corresponding section below.

1.108.8 5a. Direct SAN Access Data Transport Mode

In the Direct SAN Access mode, Veeam backup proxy connects to the ESXi host where the VM resides, and reads the necessary VM configuration files (such as *.vmx). Backup proxies use VM configuration details to read VM data directly from the SAN.

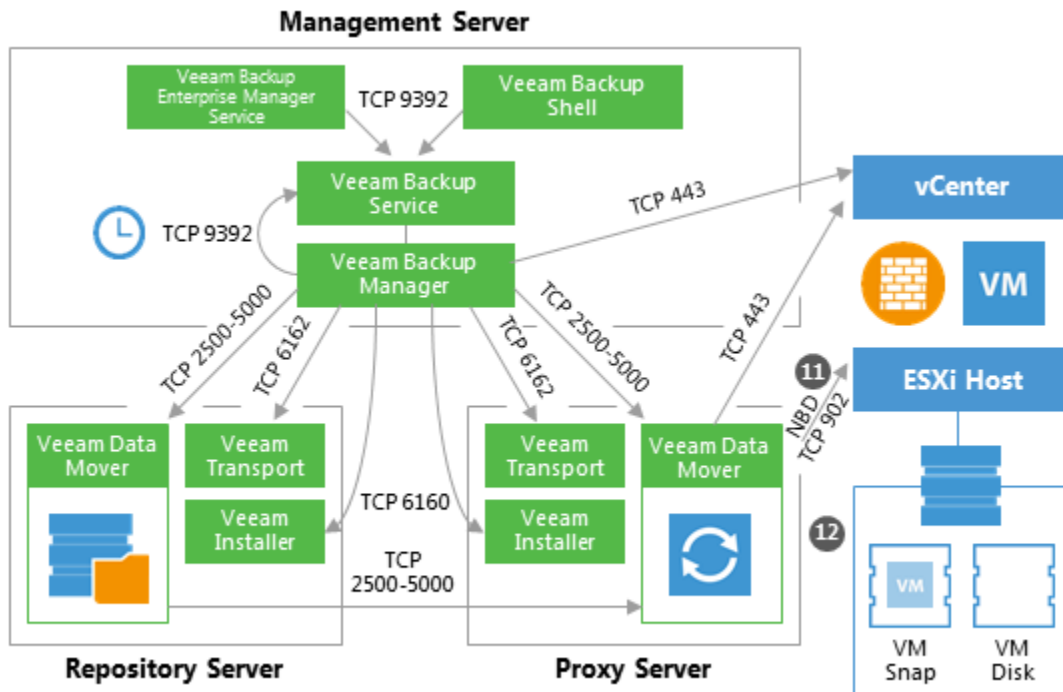


1.108.9 5b. Virtual Appliance Data Transport Mode

In the Virtual Appliance transport mode, Veeam backup proxy connects to the ESXi host where the VM resides, and reads the necessary VM configuration files (such as *.vmx). VM disks as of the snapshot state are hot-added to a virtualized Veeam backup proxy. The proxy reads VM data and unmaps the VM disks when finished.

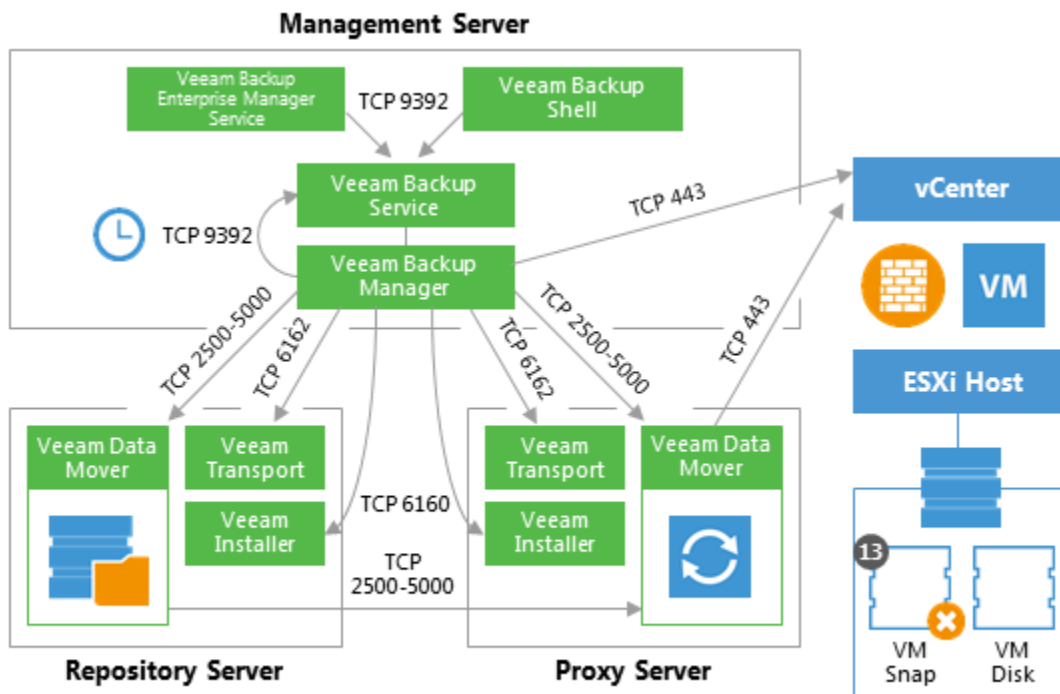


In the Network transport mode, Veeam backup proxy connects to the ESXi host where the VM resides, and reads the necessary VM configuration files (such as *.vmx). In this mode, the same data channel is used to read VM disk data, too.



1.108.11 6. Committing VM Snapshot

After Veeam backup proxy finishes reading VM data, Veeam backup server requests the vCenter Server or ESXi host to initiate a VM snapshot commit.



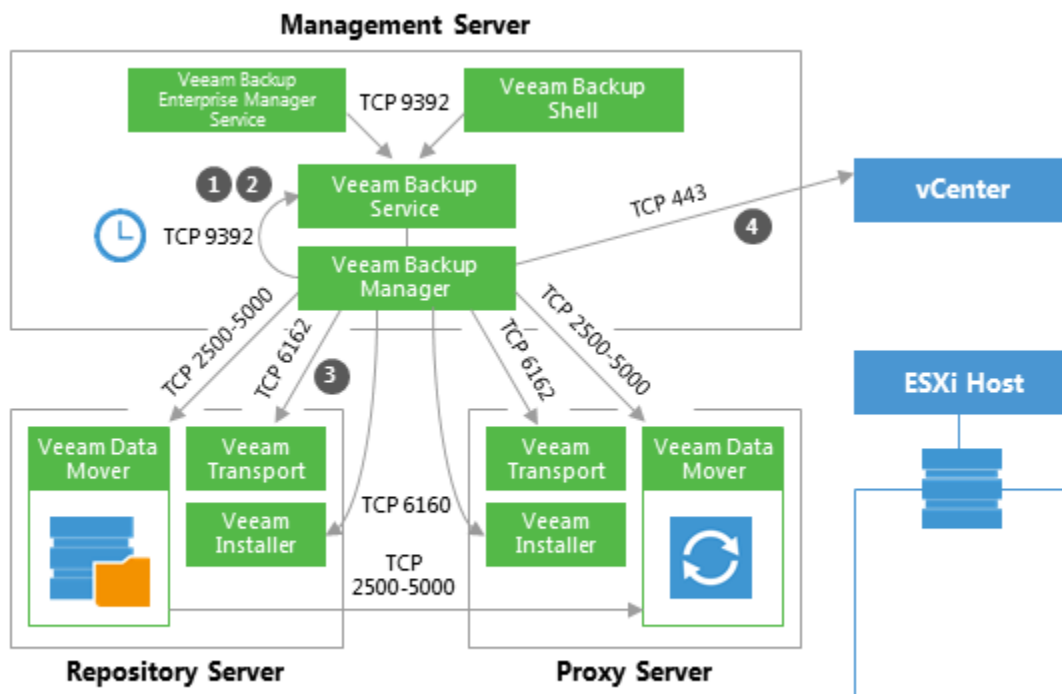
1.109 VM Restore

This section provides a step-by-step description of a full virtual machine restore process implemented in Veeam Backup & Replication.

1.109.1 1. Initialization Phase

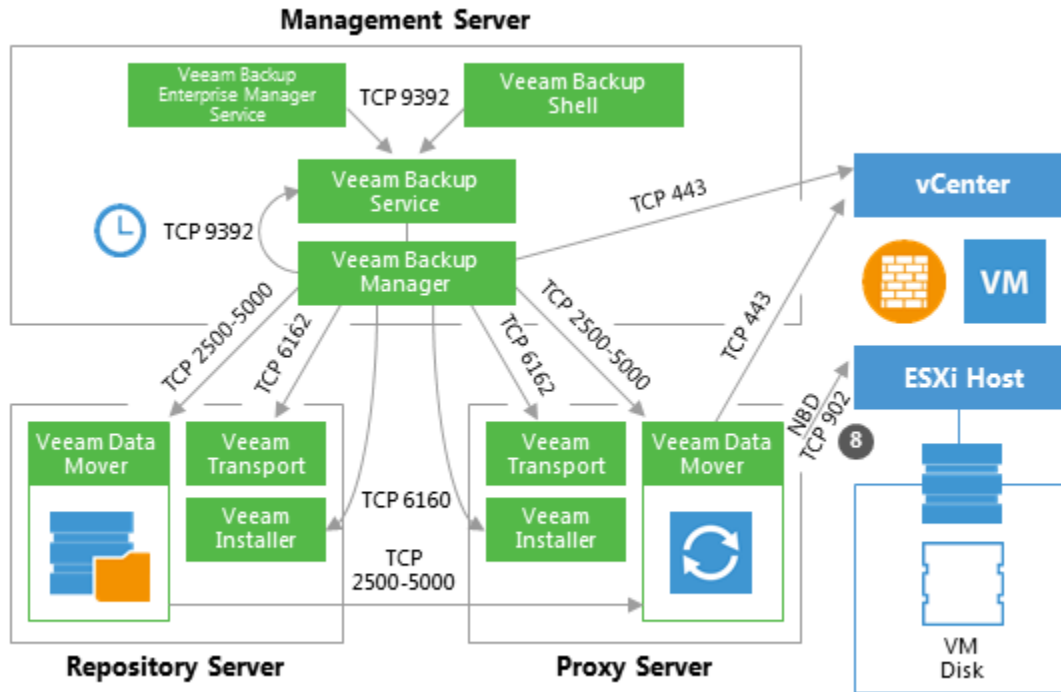
In the initialization phase, Veeam Backup & Replication prepares the resources necessary for full VM recovery. It performs the following steps:

1. Starts the necessary processes on the Veeam backup server.
2. Checks available backup infrastructure resources and assigns a proxy server for transferring restored VM data to the target host/datastore.
3. Communicates with Transport Services on the backup proxy and backup repository where the backup files reside. Transport Services, in their turn, start Veeam Data Movers. Veeam Data Movers on the backup proxy and repository establish a connection with each other for data transfer.
4. Connects to the vCenter Server or ESXi host where the restored VM will be registered.



1.109.2 2. Restoring VM Configuration

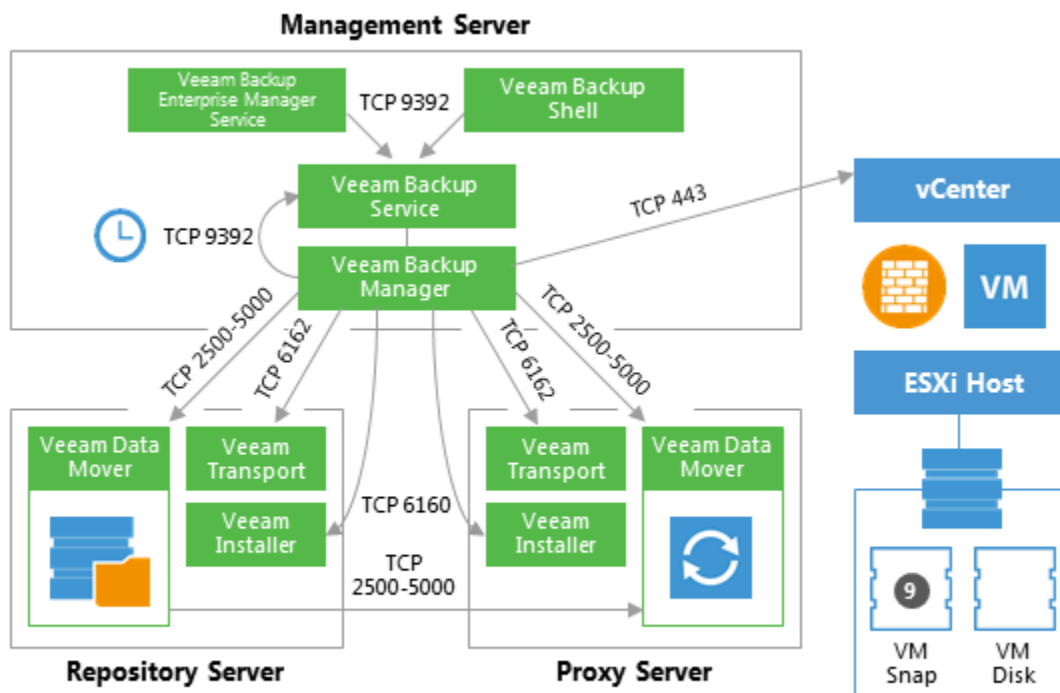
Veeam Backup & Replication retrieves VM configuration data from the backup and restores it on the chosen ESXi host/datastore. Next, it instructs VMware vSphere to register the restored VM on the host. If a user selects to change VM configuration (for example, disk format or network settings) during restore, Veeam makes the necessary amendments.



1.109.3 3. Creating VM Snapshot

Veeam Backup & Replication requests the vCenter Server or ESXi host to initiate a VM snapshot creation on the restored VM.

Important! A snapshot is not taken if a VM is restored to a VVOL datastore due to vSphere VDDK limitations (see https://pubs.vmware.com/Release_Notes/en/developer/vddk/65/vsphere-vddk-650b-release-notes.html).



1.109.4 4. VM Data Transport

Veeam Backup Manager instructs VMware vSphere to create virtual disks for the VM.

To write VM disk data to the target datastore, Veeam Backup & Replication can use one of the 3 transport modes:

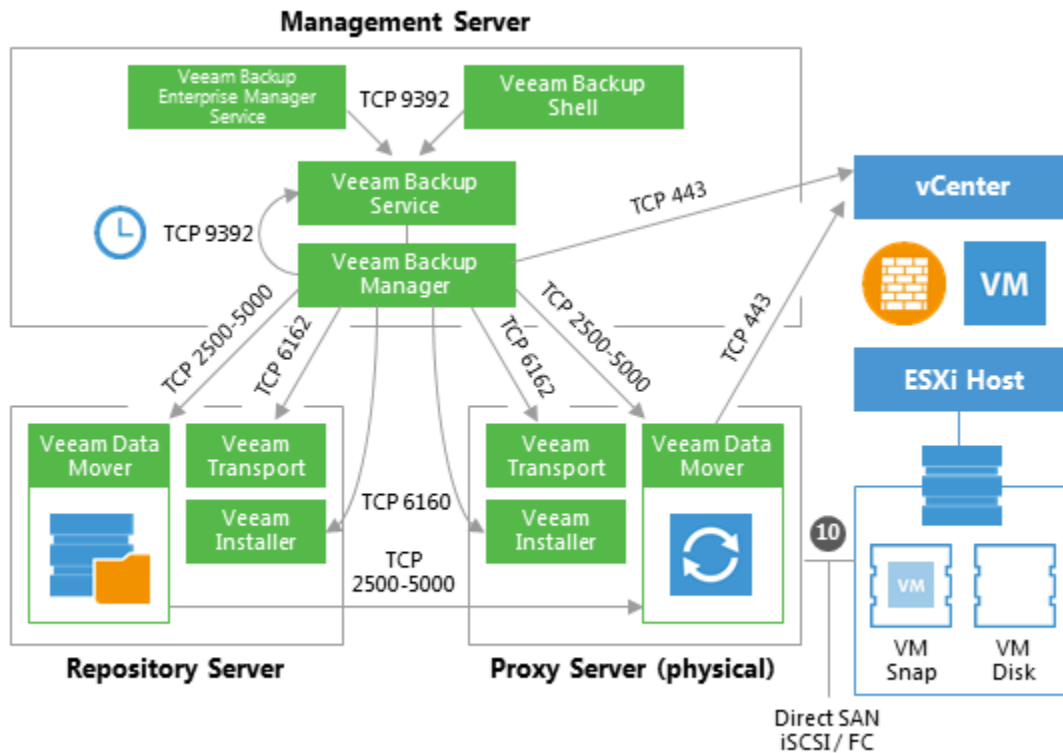
- Direct SAN Access
- Virtual Appliance (HotAdd)
- Network (NBD)

For more information about each transport mode, see [Veeam Backup & Replication User Guide](#) and the corresponding sections of this document.

1.109.5 4a. Direct SAN Access Data Transport Mode

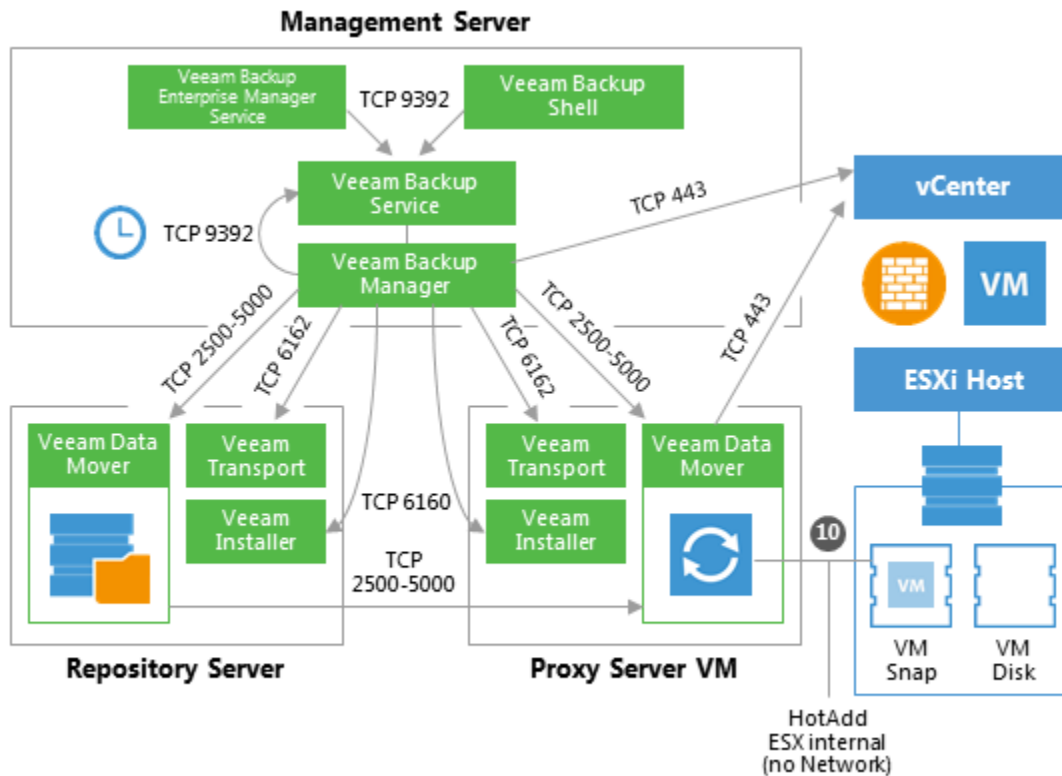
This mode is available only for VMs that have all disks in thick provisioning.

In the Direct SAN Access mode, Veeam Backup & Replication connects to the ESXi host where the restored VM is registered. The ESXi host locates the VM disks, retrieves metadata about the disk layout on the storage, and sends this metadata to the backup proxy. The backup proxy uses this metadata to copy VM data blocks to the datastore via SAN.



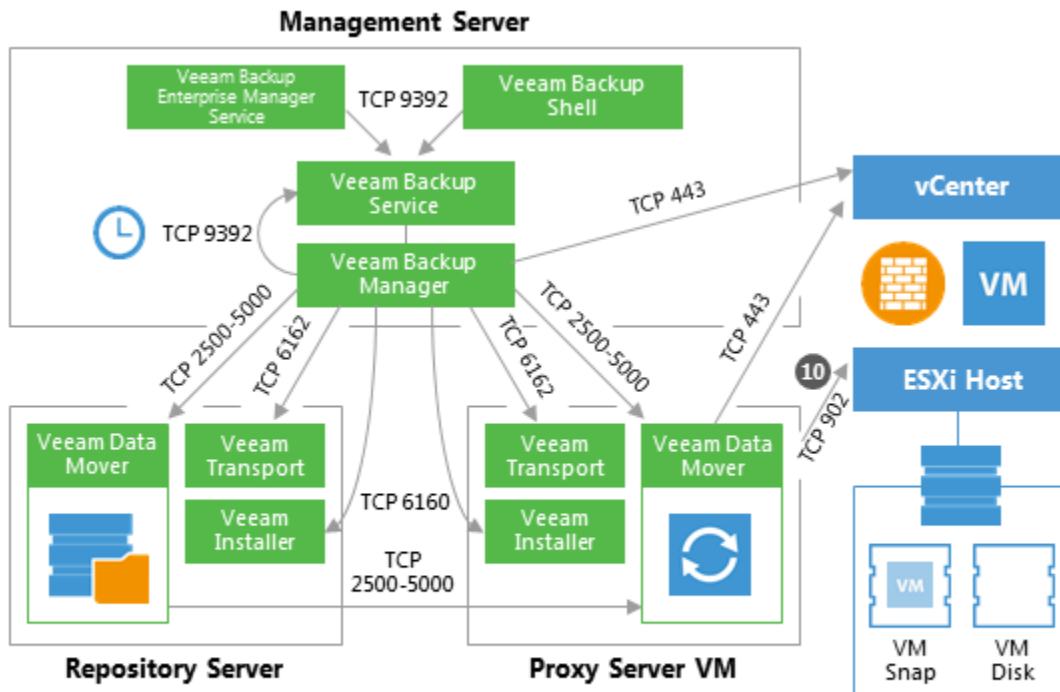
1.109.6 4b. Virtual Appliance Data Transport Mode

In the Virtual Appliance transport mode, VM disks from the backup are hot-added to a virtualized Veeam backup proxy. The proxy connects to the ESXi host where the restored VM resides and transfers disk data to the target datastore through the ESX(i) I/O stack. When the data transfer process is finished, disks are unmapped from the backup proxy.



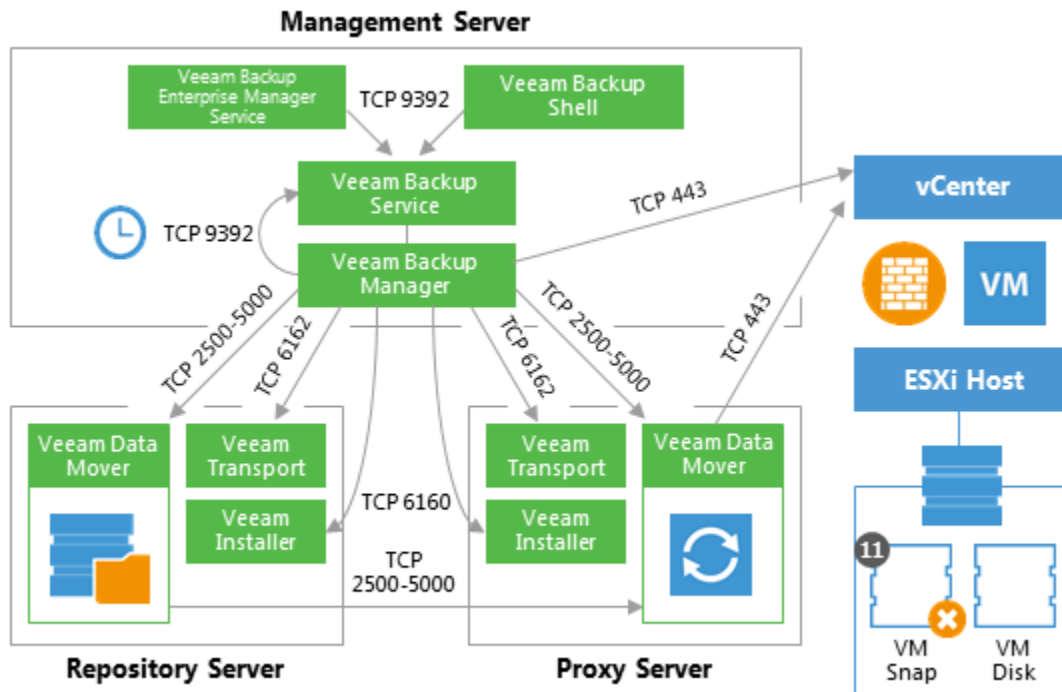
1.109.7 4c. Network Data Transport Mode

In the Network transport mode, Veeam backup proxy connects to the ESXi host where the restored VM resides, and writes VM disk data to the target datastore through the LAN channel.



1.109.8 5. Committing VM Snapshot

After the proxy finishes writing VM disk data, Veeam Backup & Replication requests the vCenter Server or ESXi host to initiate a snapshot commit for the restored VM.



1.110 Instant VM Recovery

1.110.1 Step by step description of the IVMR process implemented in Veeam Backup and Replication

1. Initialization Phase

In the initialization phase, Veeam Backup & Replication prepares resources necessary for Instant VM Recovery. It performs the following steps:

- Starts the Veeam Backup Manager process on the Veeam backup server.
- Checks with the Veeam Backup Service whether the necessary backup infrastructure resources are available for instant VM Recovery.
- Communicates with the Transport Service on the backup repository to start Veeam Data Mover.

2. NFS Mapping

When backup infrastructure resources are prepared, Veeam Backup & Replication maps an empty NFS datastore to the selected ESXi host. It uses the Veeam vPower NFS Service for this purpose.

Next, Veeam Backup & Replication creates in the Veeam NFS datastore VM configuration files and links to virtual disk files. Virtual disk files remain in the backup on the repository, while all changes to these files are written to the cache file.

3. Registering and Starting VM

The VM runs from the Veeam NFS datastore. VMware vSphere treats the Veeam NFS datastore as any regular datastore. For this reason, with the recovered VM you can perform all actions that vCenter Server/ESXi supports for regular VMs.

4. Migrating guest to production datastore

To migrate VM disk data to a production datastore, use VMware Storage vMotion or Veeam Quick Migration. For details, see [Veeam Backup & Replication User Guide](#).

1.110.2 Performance concerns

Read pattern

Usually reserved for the guests requiring the best possible RTOs, the IVMR process is read intensive and its performance is directly related to the performance of the underlying repository. Very good results can be obtained from standard drives repositories (sometimes even offering faster boot time than the production guest) while deduplication appliances might be considered carefully for such kind of use.

Keep in mind that when working on its backup files to start the guest, Veeam Backup and Replication needs to access the metadatas, which is generating some random small blocks read pattern on the repository.

Write redirections

Once booted, the guest will read existing blocks from the backup storage and write/re-read new blocks on the configured storage (whether being a datastore or a temporary file on the vPower NFS server local drive in the folder “%AL-LUSERSPROFILE%\Veeam\Backup\NfsDatastore”). To ensure consistent performances during the IVMR process, it is recommended to redirect the writes of the restored guest on a production datastore.

1.111 Windows File-Level Restore

This section provides a step-by-step description of Microsoft Windows file-level restore process for a VMware virtual machine implemented in Veeam Backup & Replication.

1.111.1 1. Initialization Phase

In the initialization phase, Veeam Backup & Replication prepares resources necessary for Microsoft Windows file-level restore. It performs the following steps:

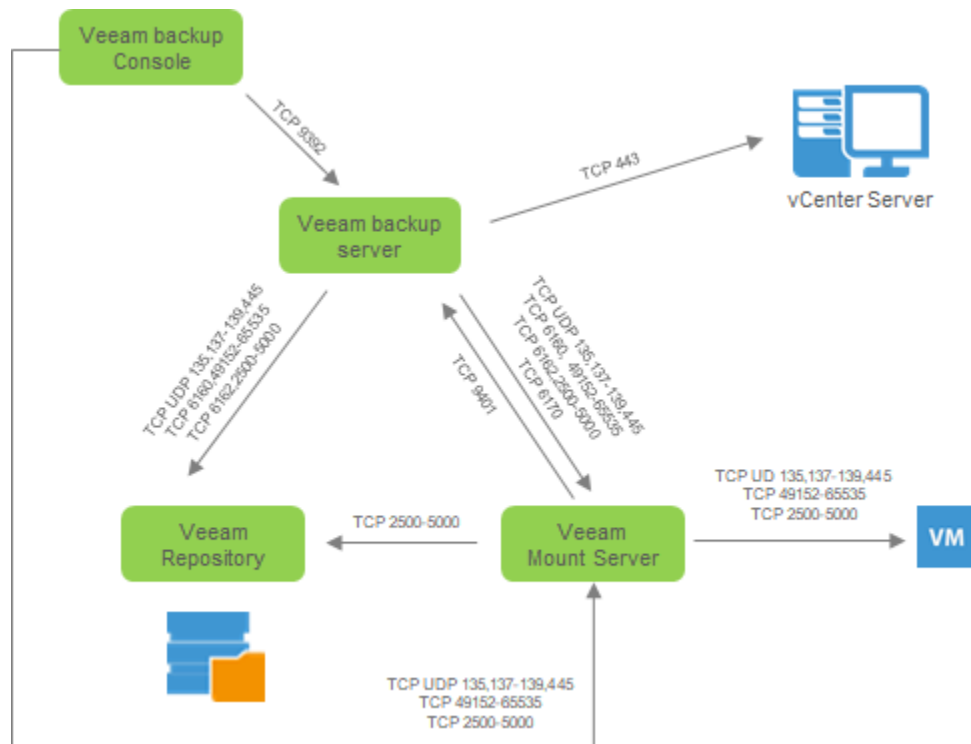
1. Checks with the Veeam Backup Service whether the necessary backup infrastructure resources are available for Microsoft Windows file-level restore.
2. Starts Veeam Data Movers on the Veeam backup server and backup repository.
3. Mounts the content of backup files to the mount server with the help of Veeam's proprietary driver.

The backup files remain on the backup repository. Guest files inside the backup can be accessed in Veeam Backup browser or Microsoft Windows File explorer on the backup server, mapped by default in the *C:\VeeamFLR* folder (which can be changed via registry key under support supervision).

1.111.2 2a. Restoring Windows Guest OS Files (Network-Based)

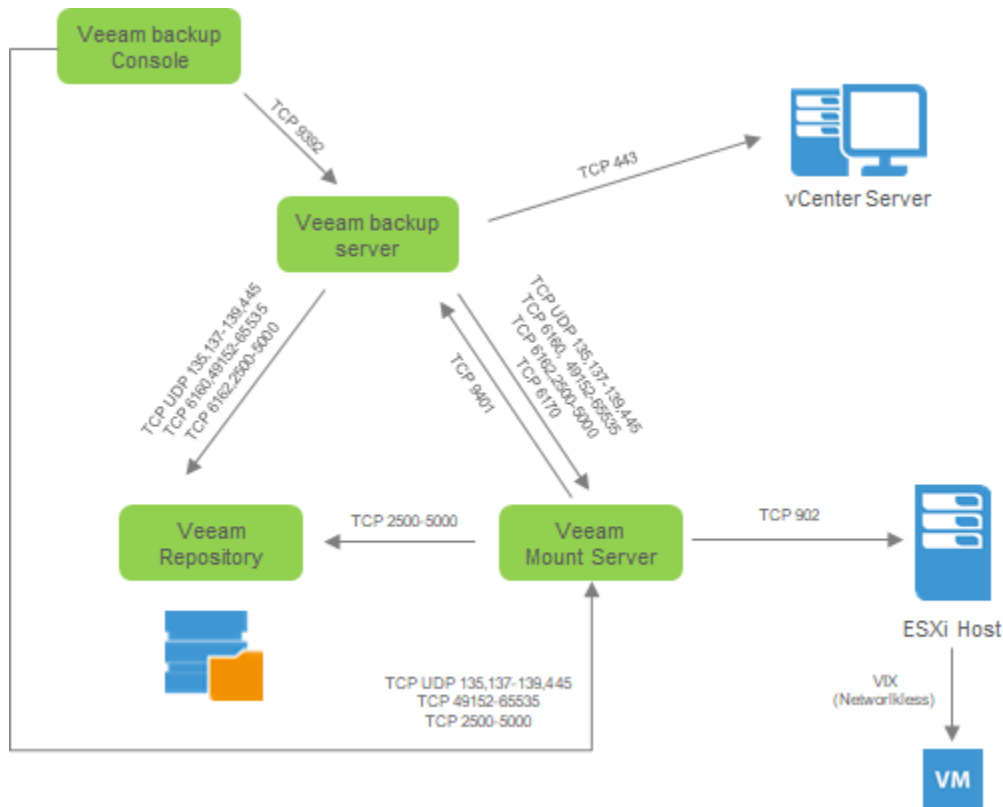
To restore guest files back to the original VM, Veeam Backup & Replication establishes a connection with the VM Guest OS. It obtains information about the guest IP address from currently running VMware Tools. Veeam uses this IP address to connect to the guest OS and perform in-guest file recovery.

If the guest has been protected using any kind of guest interaction option, the user specified at the time of the backup will be automatically invoked. In any other situation, the restore operator will be asked to input a valid set of credentials necessary to connect to the VM as specified in the [user's guide required permissions](#) section.



1.111.3 2b. Restoring Windows Guest OS Files (Networkless)

If there is no network connectivity with the VM guest OS, Veeam Backup & Replication uses the communication channel provided by VMware Tools (VIX) to interact with the guest OS and perform in-guest file recovery.



1.111.4 3. Dismounting Backup Content

After all restore activities are completed and the user closes the Veeam Backup explorer (or the explorer is closed by timeout), the content of the backup files is dismounted from the backup server.

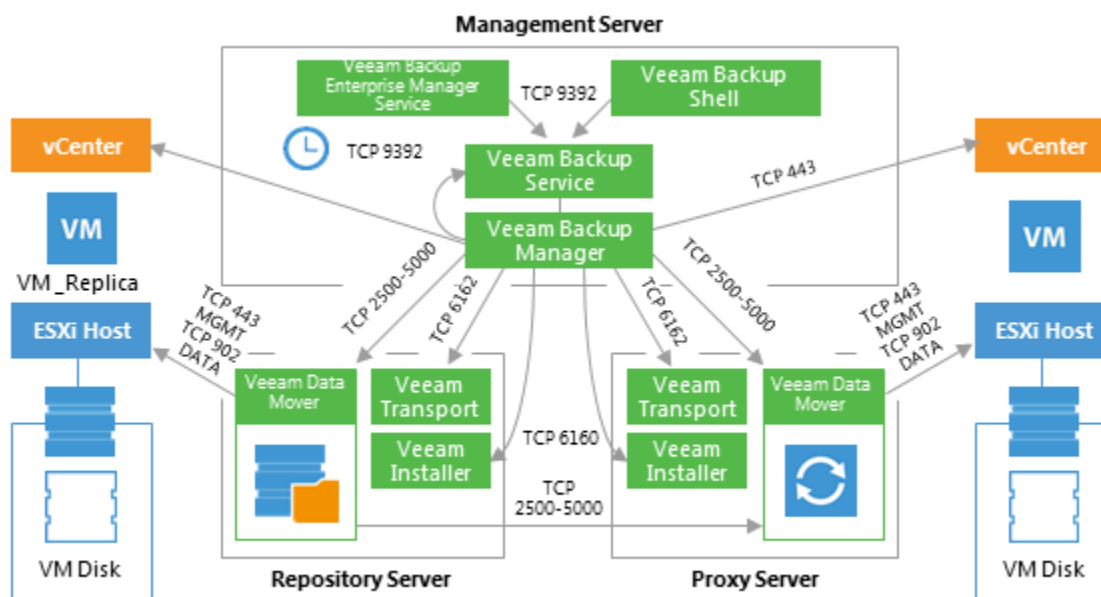
1.112 Replication

This section provides a step-by-step description of a VMware virtual machine replication process implemented in Veeam Backup & Replication.

In many aspects, the replication initialization phase is similar to the initialization phase of the backup process. Veeam Backup & Replication starts the necessary processes, builds the list of VMs to replicate, assigns backup infrastructure resources for the job and starts Veeam Data Movers on two backup proxies (source and target) and the backup repository that is used for storing replica metadata.

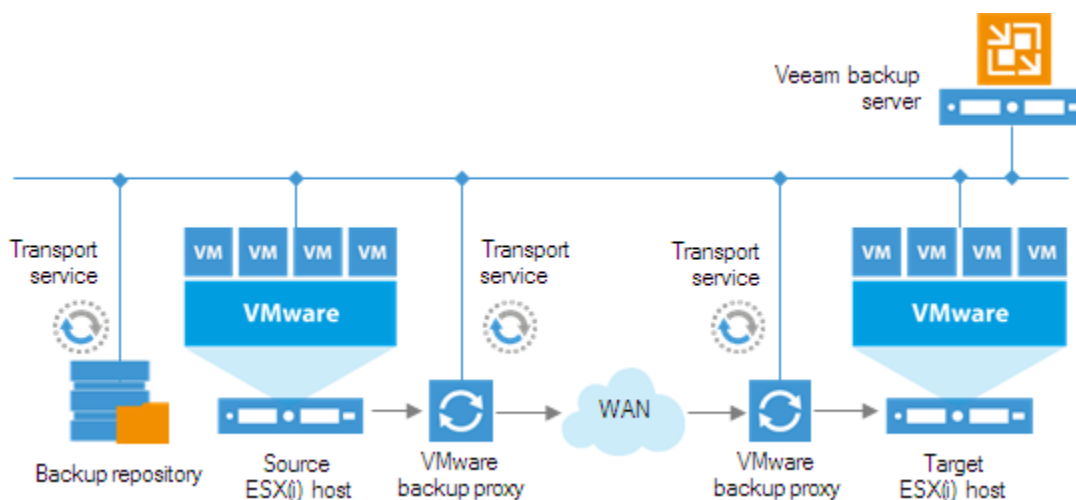
Next, Veeam Backup & Replication performs in-guest processing tasks, triggers VM snapshot creation, registers a replica VM on the target host and performs data transfer from the source host and datastore to the target host and datastore. The source and target proxies can use one of 3 available data transport modes for reading data from source and writing data to target.

This diagram illustrates the replication process with the NBD transport mode used for reading and writing VM data. For examples of the Direct SAN/NFS Access and HotAdd transport modes, see the “Backup Anatomy” section above in this Appendix.



Note that Veeam uses backup repository to store replica metadata.

The following diagram illustrates a possible placement of the Veeam Backup & Replication components in a distributed environment, with a WAN link between the production and DR sites.

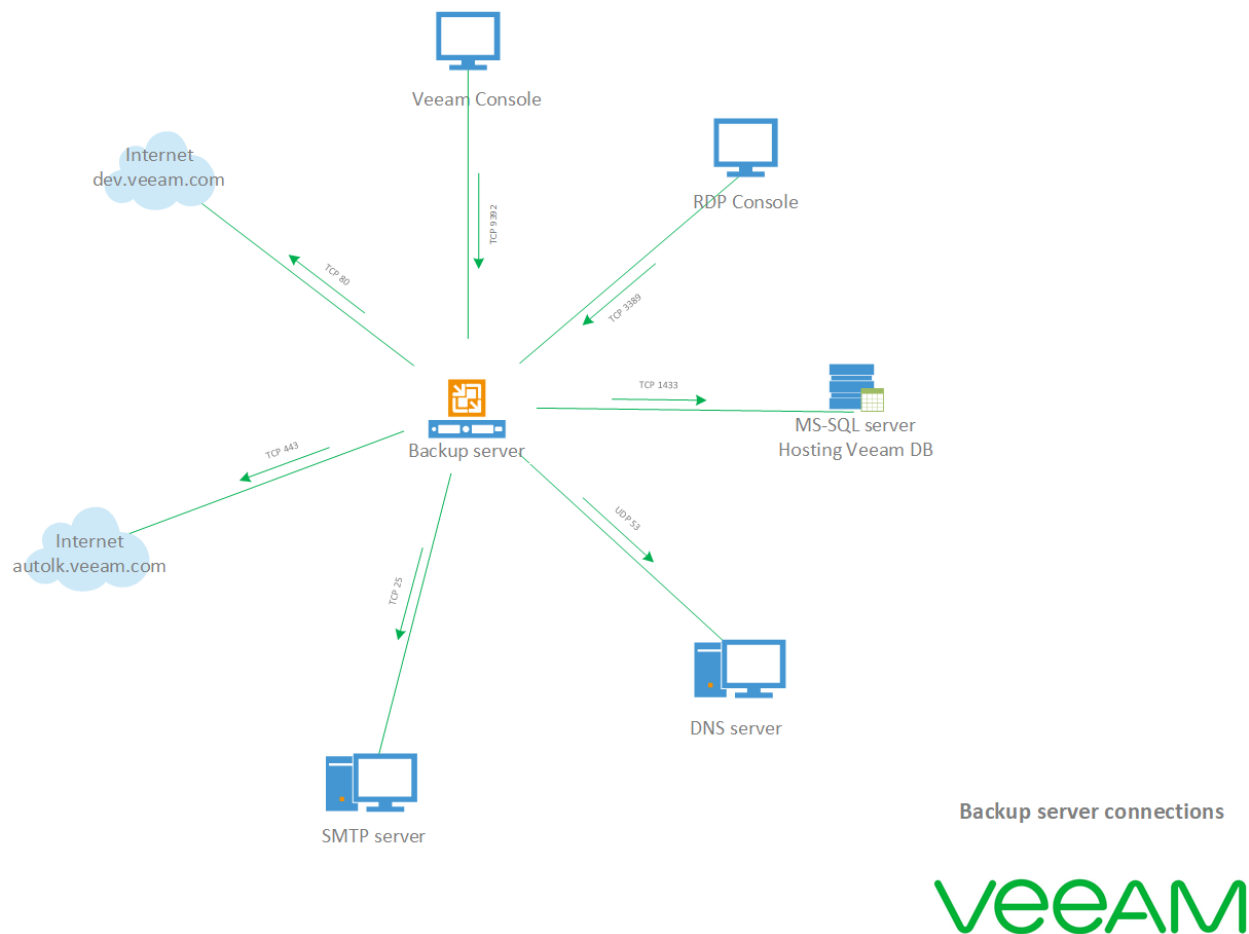


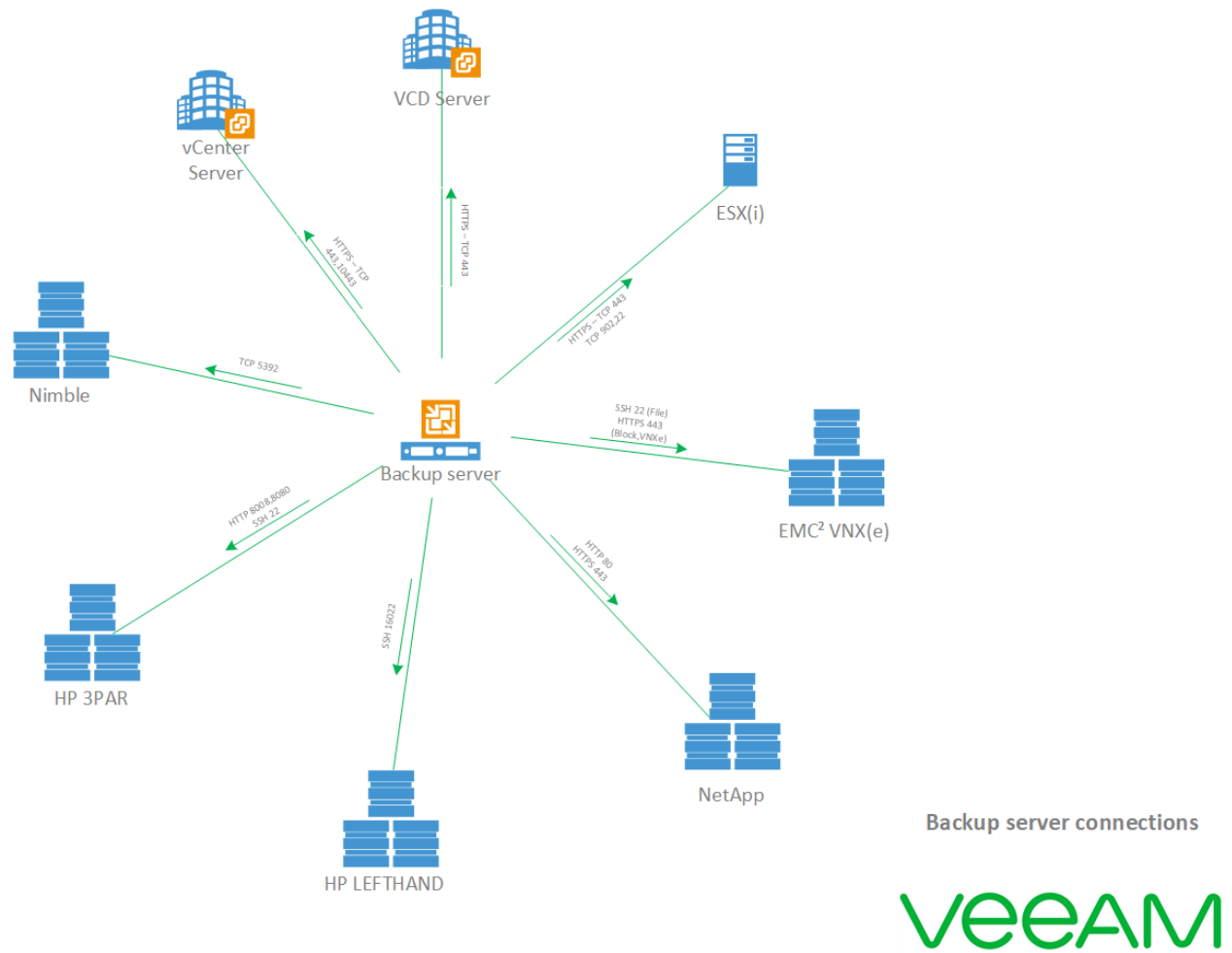
1.113 Networking Diagrams

There is a detailed list of ports used by Veeam Backup & Replication available in the [User Guide](#), but sometimes a more visual approach is helpful – you can use the diagrams below for that purpose.

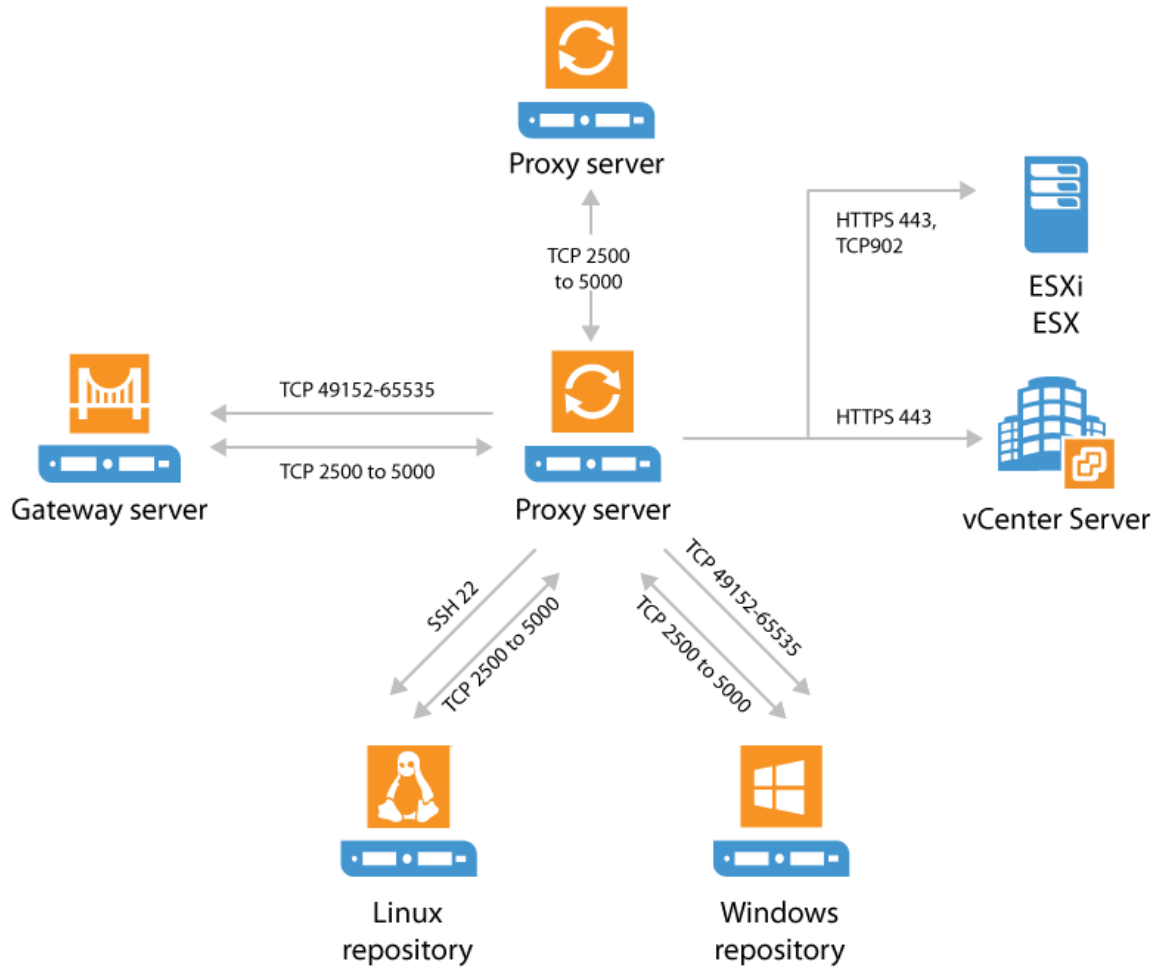
1.114 Backup Server

The following ports are required for B&R





The following ports are required for the proxy server.

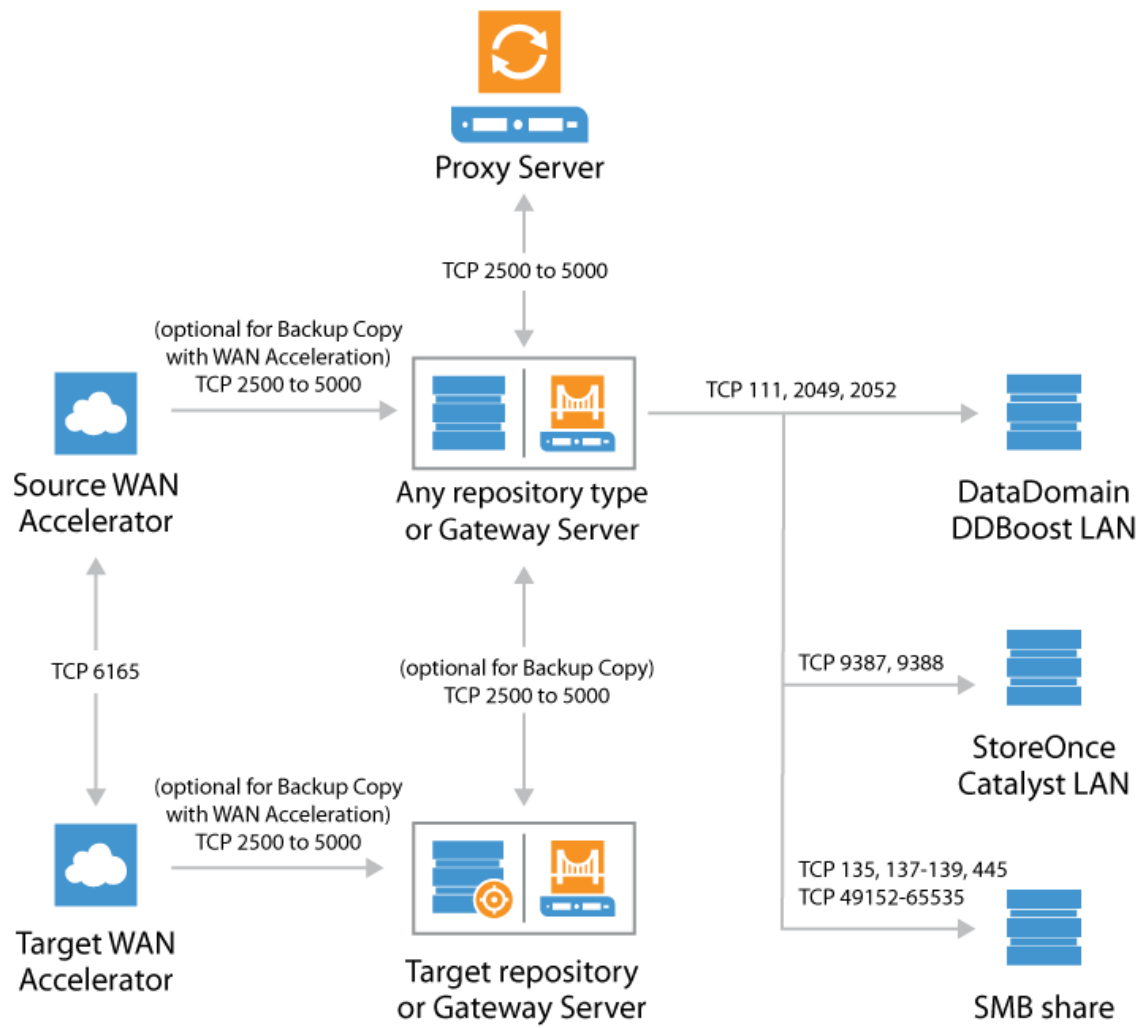


Server

Proxy

1.116 Repository Server

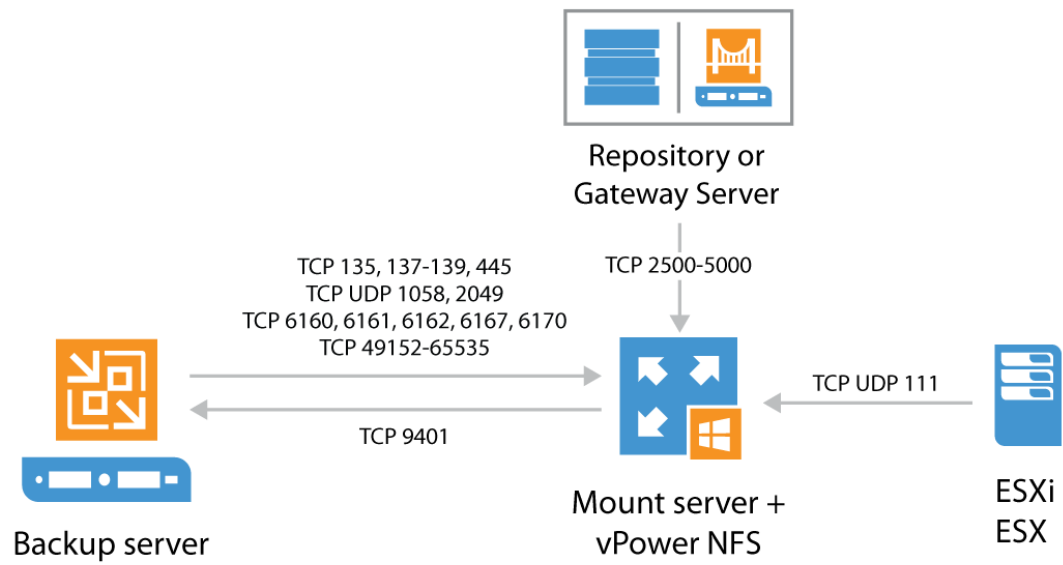
The following ports are required for the repository server.



Server

The following ports are required for vPower NFS.

Repository

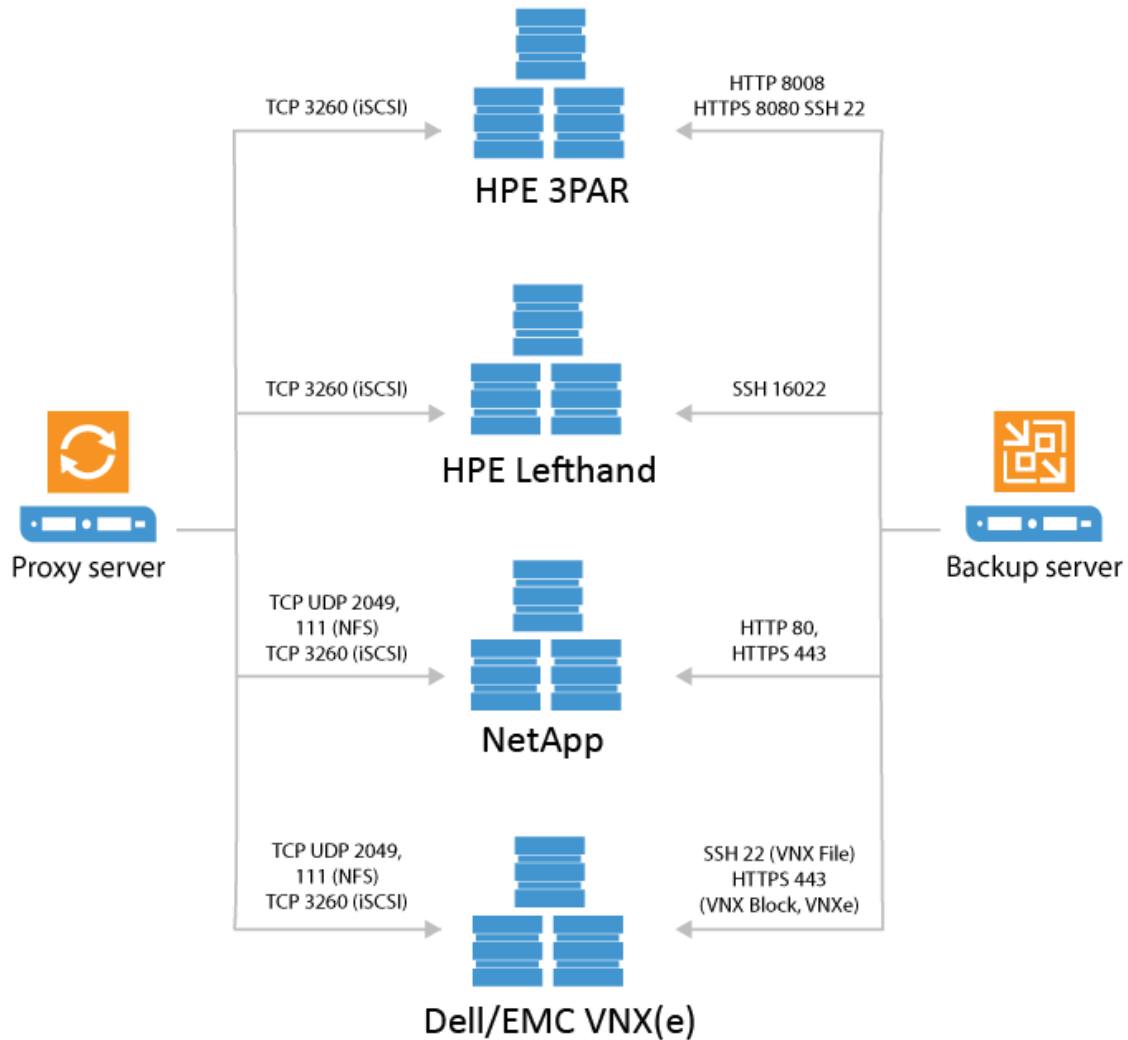


NFS

vPower

1.117 Storage Integrations

The following ports are required for integrated storage.

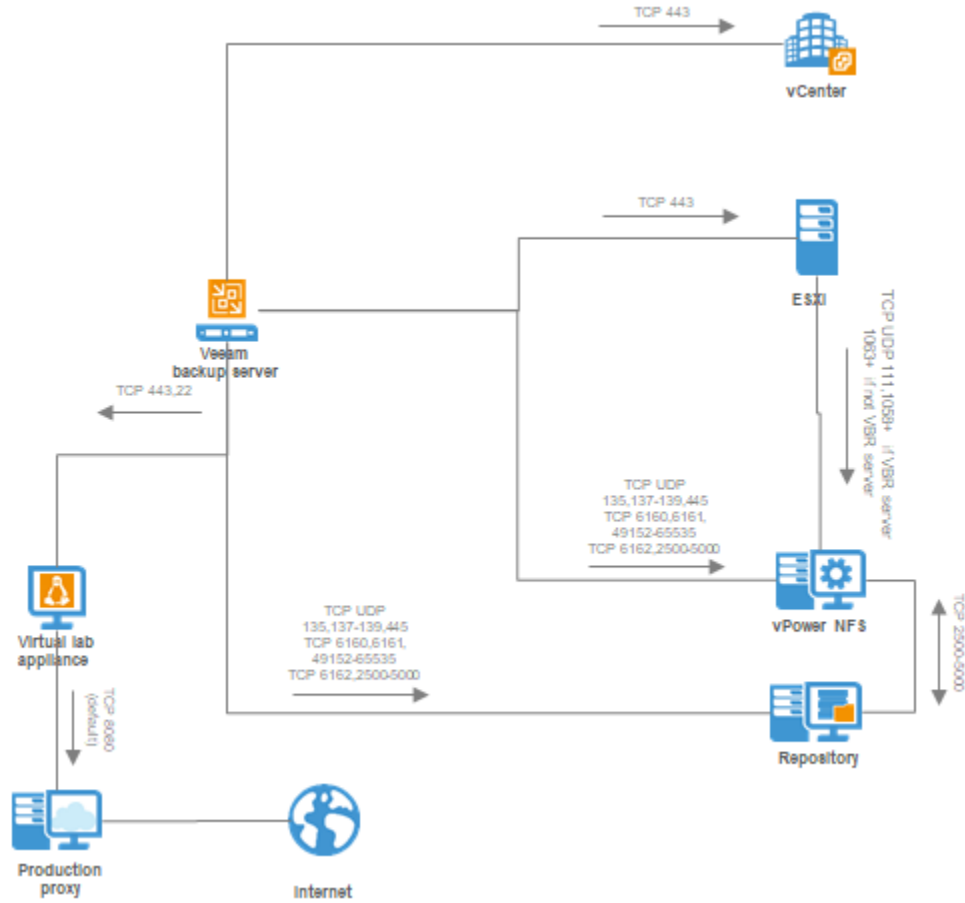


storage

Integrated

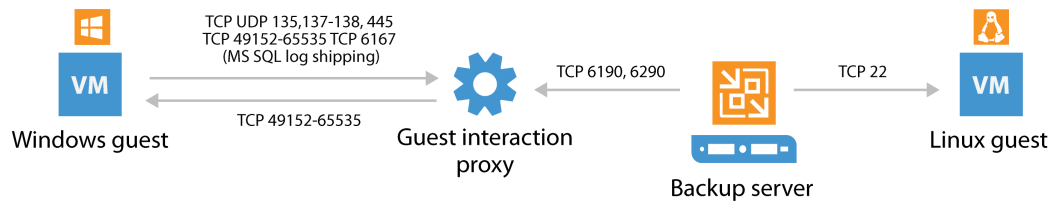
1.118 Data Validation

The following ports are required, when using SureBackup, SureReplica, or On-demand Sandbox from Storage Snapshots, repository related ports being used only for SureBackup jobs.



1.119 Application-aware Image Processing

The following ports are required for application-aware image processing over the network. If network ports are not available, the backup server will failover to using VIX via VMware Tools.

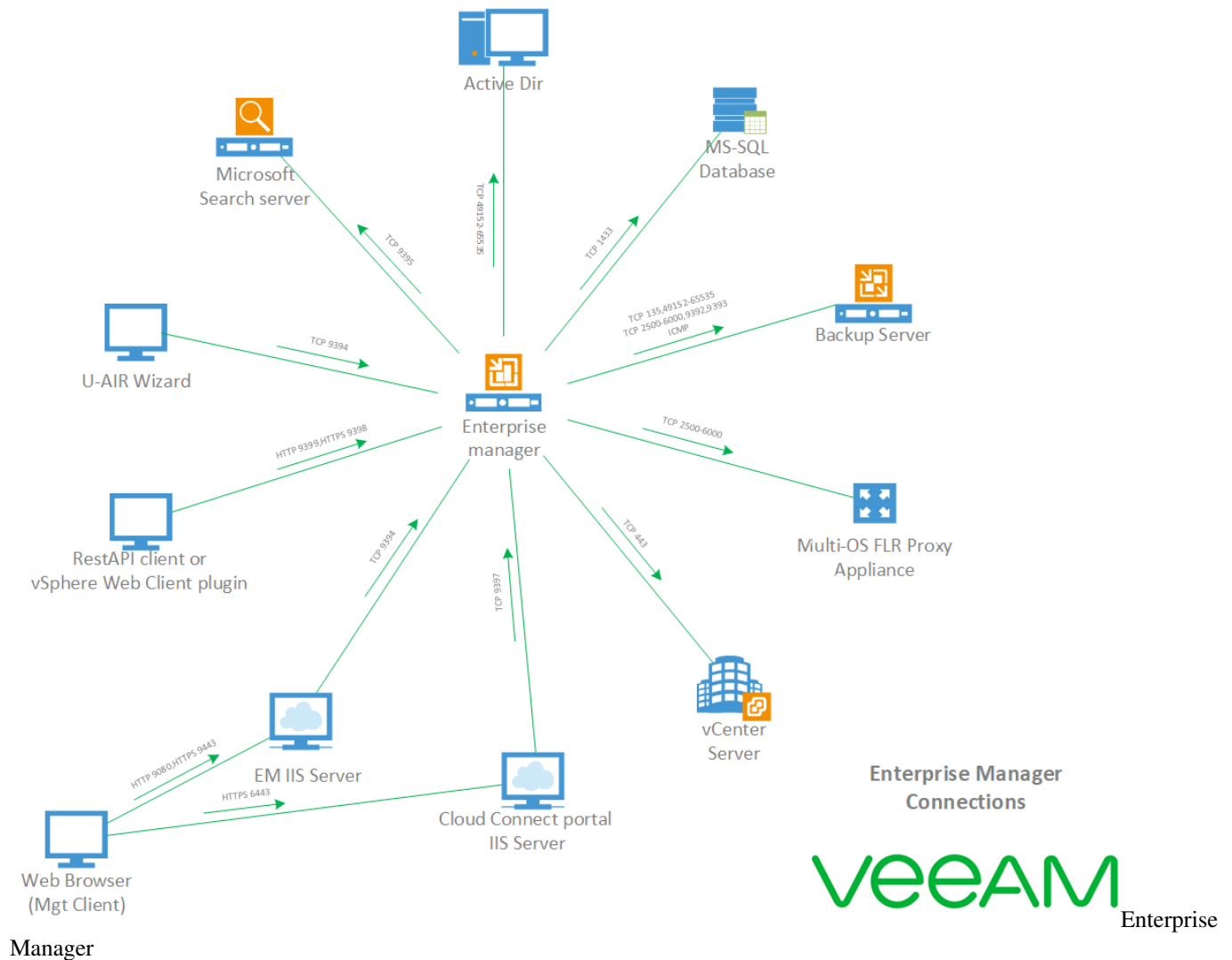


Application-aware Image Processing

Application-

1.120 Enterprise Manager

The following ports are required for Enterprise Manager



1.121 Sizing and System Requirements Appendix

This appendix is a cumulative section on base sizing metrics, there is much more to sizing a Veeam Infrastructure and performing to the highest level. These figures here are guidelines to follow as a starting point. Each section is in much more detail in its relative chapter in the guide, please read each section first and you will gain an insight as to why these numbers are recommended.

Sizing with Veeam is cumulative in respect to configurations, if you want to create an all-in-one appliance (Appliance Model) add all the resource requirements together (CPU + Memory) to understand what in total you will need, the same goes if you only wish to have proxy and repository in one host.

Please also bear in mind that these figures reflect Veeam's resource requirement, you must take the hosts system requirements into your calculation, this will depend on what you are using which is why we have not detailed it here.

1.121.1 Veeam Backup and Replication management server resources.

Recommended Veeam backup server resource configuration is:

Minimum Resources

- The minimum Compute is 2 CPU cores.
- Minimum memory, 8 GB RAM.
- Minimum HDD space is 60GB (inclusive of Logs, vPowerNFS, VBR software) Recommendations for sizing.
- 1 CPU core (physical or virtual) and 4 GB RAM per 10 concurrently running jobs.
- For per job backup files: 30 VMs per job
- For per VM backup files: 300 VMs per job
- Base HDD is 40GB for software install location
- Plan for 3 GB log file space per 100 virtual machines, with a 24 hour RPO
- vPowerNFS location with reserve capacity of 10GB (100GB per TB of space if you plan to do many recoveries or planning SureBackup tests running many vm's at the same time)
- Extra space for guest indexing processing a windows host: 100MB per 1Million files (temp file space)
- Extra space for guest indexing processing a Linux host: 50MB per 1Million files (temp file space)
- Storage space for Guest indexing before Enterprise manager flush: 2MB per 1 million files (compressed)

1.121.2 Proxy Server Resources

When sizing a proxy server remember, the ability to execute a task on the proxy will be affected by the repositories ability to process all the tasks from the proxies in infrastructure. If a repository has 20 cores, then the maximum processed tasks will be no more than 20 tasks from any proxy or group of proxies in the backend fabric of Veeam.

Recommended Veeam Proxy Servers configurations is:

- 1 CPU core per task (a task is a virtual hard drive)
- 2GB RAM per task
- Minimum of 500MB of HDD working space per task

This is based on a rounded figure offering approximately 30 VMs in a single backup job which will finish around an 8 hours backup window if in a per job backup, if a per VM repository is used more can be added. Please read the sizing and repository section for a full detailed description of parallelization of workloads in a Proxy.

1.121.3 Repository Server Resources

This is not about sizing for capacity of your repository but the resources required to accommodate the workloads form backups and restores.

When sizing a repository server remember, the ability to execute a task on the repository will be affected by the proxy's ability to process all the tasks from the proxy's. If a repository has 20 cores, then the maximum processed tasks will be no more than 20 tasks from any proxy or group of proxies in the backend fabric of Veeam to that repository.

Recommended Veeam Repository Server configurations is:

- 1 core per task
- 4GB per task
- Hard drive space is calculated based off retention points, type of backup used (full, Incremental, synthetic, forever forward incremental or reverse incremental.)

There is a much more detailed section in the guide.

1.121.4 SQL Server Database Sizing Guide

Veeam Backup & Replication may consume high amounts of CPU and RAM while processing backup or replication jobs. To achieve better performance and load balancing it is necessary to provide sufficient RAM and CPU resources. If possible, follow these guidelines:

Concurrent Jobs | CPUs | Memory ————— | ————— | ————— Up to 25 | 2CPUs | 4GB RAM Up to 50 | 4CPUs | 8GB RAM Up to 100 | 8CPUs | 16GB RAM

Note: Concurrently running jobs include any job type with a continuous schedule such as Backup Copy Jobs. When running more than 100 jobs concurrently increase compute resources in line with the table above to meet the resource need of the workload. Veeam installation package includes SQL server 2012 Express Edition, the basic limitations of this software are as follows:

- Each instance uses only up to 1 GB of RAM
- Each instance uses only up to 4 cores of the first CPU
- Database size cannot exceed 10 GB

If any of the below apply consider using SQL standard or Enterprise editions

- When protecting more than 500 VMs
- When using Files to Tape jobs extensively
- When unable to configure an external staging server
- When databases are using advanced features of Microsoft SQL Server

CHAPTER 2

Indices and tables

- `genindex`
- `modindex`
- `search`