## Contents

1. Introduction .............................................................................................................. 1  
   1.1. Course Overview .............................................................................................. 1  
2. Overview of Veeam Products ................................................................................. 3  
   2.1. Veeam Products ............................................................................................... 3  
      2.1.1. Veeam Backup & Replication ...................................................................... 3  
      2.1.2. Veeam ONE ................................................................................................. 3  
      2.1.3. Veeam Management Pack for System Center ............................................. 4  
      2.1.4. Veeam plug-in for vSphere Web Client ...................................................... 4  
      2.1.5. The Veeam Backup & Replication Add-on for Kaseya ............................. 4  
      2.1.6. Veeam Backup & Replication Plug-in for LabTech ................................... 5  
      2.1.7. Veeam Endpoint Backup FREE ................................................................. 5  
   2.2. Veeam Availability Suite ................................................................................ 6  
      2.2.1. Veeam Availability Suite Capabilities ...................................................... 6  
   2.3. Key Concepts .................................................................................................. 7  
      2.3.1. Key Concepts ............................................................................................. 7  
3. Deployment ............................................................................................................ 9  
   3.1. Core Components and Their Interaction ....................................................... 9  
      3.1.1. Veeam Backup Server .............................................................................. 9  
      3.1.2. Backup Proxy (VMware) ............................................................................ 10  
      3.1.3. Off-host Backup Proxy (Hyper-V) .............................................................. 16  
      3.1.4. Backup Repository .................................................................................... 19  
   3.2. Optional Components ..................................................................................... 23  
      3.2.1. Veeam Backup Enterprise Manager ........................................................... 23  
      3.2.2. U-AIR Wizard ............................................................................................ 24  
      3.2.3. Mount Server ........................................................................................... 24  
      3.2.4. Veeam Backup Search ............................................................................. 25  
   3.3. Deployment Scenarios ..................................................................................... 25  
      3.3.1. Simple Deployment ................................................................................... 25  
      3.3.2. Advanced Deployment ............................................................................ 27  
      3.3.3. Distributed Deployment .......................................................................... 29  
      3.3.4. Distributed Architecture ......................................................................... 30  
   3.4. Prerequisites ................................................................................................... 32  
      3.4.1. Requirements .......................................................................................... 33  
      3.4.2. Platform Support ........................................................................................ 33  
      3.4.3. System Requirements ............................................................................... 34  
      3.4.4. Required Permissions ............................................................................. 45  
   3.5. Upgrading Veeam Backup & Replication ....................................................... 46  
      3.5.1. Before You Upgrade ............................................................................... 46  
      3.5.2. After You Upgrade ................................................................................ 46  
   Labs for Module 3: Deployment .............................................................................. 49  
4. Initial Configuration .............................................................................................. 51  
   4.1. Adding Servers ............................................................................................... 51  
   4.2. Adding a VMware Backup Proxy ................................................................... 52  
   4.3. Adding a Hyper-V Off-host Backup Proxy ................................................... 52  
   4.4. Adding Backup Repositories ......................................................................... 53  
   4.5. Performing Configuration Backup and Restore ............................................ 53
# Table of Contents

4.5.1. Creating Configuration Backups ................................................................. 53  
4.5.2. Creating Encrypted Configuration Backups .................................................. 54  
4.5.3. Restoring Configuration Data ................................................................. 55  

## 4.6. Managing Network Traffic

4.6.1. Setting Network Traffic Throttling Rules ..................................................... 56  
4.6.2. Managing Data Transfer Connections ......................................................... 56  
4.6.3. Preferred Networks .................................................................................. 56  
4.6.4. Network Traffic Encryption ...................................................................... 56  

## 4.7. Global Notification Settings

4.7.1. Specifying E-Mail Notification Settings ....................................................... 57  
4.7.2. Specifying Other Notification Settings ......................................................... 57  

## 4.8. Getting to Know User Interface

4.8.1. Main Menu .............................................................................................. 58  
4.8.2. Navigation Pane ....................................................................................... 58  
4.8.3. Ribbon and Tabs ...................................................................................... 58  
4.8.4. Views .................................................................................................... 59  
4.8.5. Working Area ......................................................................................... 60  

### Labs for Module 4: Initial Configuration

<table>
<thead>
<tr>
<th>Labs for Module 4: Initial Configuration</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Protect ..................................................</td>
<td>63</td>
</tr>
</tbody>
</table>

## 5. Protect

### 5.1. Creating Backup Jobs

5.1.1. Before You Begin ................................................................................. 63  
5.1.2. Backup Methods .................................................................................. 64  
5.1.3. Changed Block Tracking (CBT) ............................................................. 74  
5.1.4. Data size optimization ....................................................................... 75  
5.1.5. Data Encryption ................................................................................ 77  
5.1.6. Transaction Consistency .................................................................... 79  
5.1.7. Scheduling ......................................................................................... 84  

### 5.2. Creating Restore Points with VeeamZIP and Quick Backup

5.2.1. VeeamZIP .......................................................................................... 86  
5.2.2. Quick Backup .................................................................................... 87  

## 5.3. Backup Copy

5.3.1. 3-2-1 rule ......................................................................................... 88  
5.3.2. Backup Copy Job .............................................................................. 89  
5.3.3. WAN Acceleration ............................................................................. 94  

## 5.4. Replication

5.4.1. Replication Overview .......................................................................... 95  
5.4.2. Insight into replication ...................................................................... 97  
5.4.3. Reducing Amount of Transferred Data .................................................. 97  
5.4.4. Resume on Disconnect ...................................................................... 98  

## 5.5. Creating VM/File Copy Jobs

5.5.1. VM copy .......................................................................................... 99  
5.5.2. File Copy ......................................................................................... 99  

### Labs for Module 5: Protect

<table>
<thead>
<tr>
<th>Labs for Module 5: Protect</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Labs for Module P: Preparation for day 2</td>
<td>103</td>
</tr>
</tbody>
</table>

## 6. Verification

### 6.1. SureBackup Recovery Verification

6.1.1. How It Works .................................................................................... 105  
6.1.2. Recovery Verification Tests ............................................................... 107  
6.1.3. Backup File Validation ........................................................................ 107  

Veeam Certified Engineer v9 . Textbook
# Table of Contents

6.1.4. Application Group ................................................................. 108
6.1.5. Virtual Lab ................................................................. 109
6.1.6. SureBackup Job ................................................................. 118
6.1.7. Manual Recovery Verification ................................................................. 120
6.2. SureReplica Recovery Verification ................................................................. 120
6.3. On-Demand Sandbox ................................................................. 122
**Labs for Module 6: Verification** ................................................................. 125
7. Entire VM Recovery ........................................................................ 127

<table>
<thead>
<tr>
<th>7.1. Data Recovery</th>
<th>127</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1.1. Data Recovery Scenarios Overview</td>
<td>127</td>
</tr>
<tr>
<td>7.1.2. Instant VM Recovery</td>
<td>127</td>
</tr>
<tr>
<td>7.1.3. Full VM Recovery</td>
<td>129</td>
</tr>
<tr>
<td>7.1.4. VM File Recovery</td>
<td>130</td>
</tr>
</tbody>
</table>

| 7.2. Working with Veeam Backup & Replication Utilities | 131 |

<table>
<thead>
<tr>
<th>7.3. Insight into Recovery from Replica</th>
<th>131</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.3.1. Failover</td>
<td>131</td>
</tr>
<tr>
<td>7.3.2. Failback</td>
<td>132</td>
</tr>
<tr>
<td>7.3.3. Failover Plan</td>
<td>133</td>
</tr>
<tr>
<td>7.3.4. Planned Failover</td>
<td>134</td>
</tr>
</tbody>
</table>

**Labs for Module 7: Entire VM Recovery** ................................................................. 137

8. Objects Recovery ........................................................................ 139

<table>
<thead>
<tr>
<th>8.1. Item-Level Recovery</th>
<th>139</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1.1. Restoring Microsoft Exchange, SQL, SharePoint and Active Directory Objects</td>
<td>139</td>
</tr>
<tr>
<td>8.1.2. Universal Application-Item Recovery (U-AIR)</td>
<td>144</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8.2. Guest OS File Recovery</th>
<th>146</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.1. Guest OS File Recovery</td>
<td>146</td>
</tr>
<tr>
<td>8.2.2. Windows File-Level Recovery</td>
<td>147</td>
</tr>
<tr>
<td>8.2.3. Multi-OS File-Level Recovery</td>
<td>147</td>
</tr>
<tr>
<td>8.2.4. File-Level Recovery for Any File System</td>
<td>148</td>
</tr>
</tbody>
</table>

**Labs for Module 8: Objects Recovery** ................................................................. 149

9. Advanced Data Protection ........................................................................ 151

<table>
<thead>
<tr>
<th>9.1. Tape Device Support</th>
<th>151</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1.1. Tape Job Encryption</td>
<td>154</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9.2. SAN Storage Systems Support</th>
<th>155</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2.1. SAN Storage Systems Support Overview</td>
<td>155</td>
</tr>
<tr>
<td>9.2.2. HPE Storage Systems</td>
<td>156</td>
</tr>
<tr>
<td>9.2.3. NetApp Storage Systems</td>
<td>156</td>
</tr>
<tr>
<td>9.2.4. EMC Storage Systems</td>
<td>159</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9.3. Support for Deduplicating Storage Systems</th>
<th>159</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.3.1. ExaGrid</td>
<td>159</td>
</tr>
<tr>
<td>9.3.2. HPE StoreOnce</td>
<td>159</td>
</tr>
<tr>
<td>9.3.3. EMC Data Domain Boost</td>
<td>161</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9.4. Veeam Cloud Connect</th>
<th>164</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.4.1. Lease and Quota</td>
<td>166</td>
</tr>
<tr>
<td>9.4.2. Licensing for Cloud Repositories</td>
<td>166</td>
</tr>
<tr>
<td>9.4.3. v9 Cloud Connect Enhancements</td>
<td>167</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>9.5. Veeam Backup Enterprise Manager</th>
<th>169</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.5.1. Required Permissions</td>
<td>169</td>
</tr>
<tr>
<td>9.5.2. Restore of Application Items</td>
<td>170</td>
</tr>
</tbody>
</table>
Table of Contents

9.5.3. Self-restore portal ........................................................................................................... 170
9.5.4. Managing Encryption Keys ............................................................................................. 170
9.5.5. Decrypting Data without a Password ................................................................................ 171
9.5.6. Veeam Backup Enterprise Manager RESTful API ............................................................ 172
9.6. Standalone Console ............................................................................................................ 173
9.7. vCloud Director Support ..................................................................................................... 174
Labs for Module 9: Advanced Data Protection ......................................................................... 175

10. Veeam ONE Features and Functionality ............................................................................. 177

10.1. Introduction to Veeam ONE .............................................................................................. 177
10.2. Auto Discovery of Backup and Virtual Infrastructure ......................................................... 177
10.3. Veeam ONE components .................................................................................................. 178
  10.3.1. Monitoring and Alerting .............................................................................................. 178
  10.3.2. Reporting and Dashboards .......................................................................................... 180
  10.3.3. Business Categorization ............................................................................................ 182
10.4. Veeam ONE Deployment .................................................................................................. 182
  10.4.1. Typical deployment ..................................................................................................... 183
  10.4.2. Advanced deployment ................................................................................................ 183
10.5. Veeam ONE Assessment Tool .......................................................................................... 185
  10.5.1. Veeam ONE Assessment Tool Content ....................................................................... 185
Labs for Module 10: Veeam ONE Features and Functionality .................................................. 187

11. Product Editions ..................................................................................................................... 189

11.1. Product Editions Comparison ............................................................................................. 189
11.2. Full and Free Functionality Modes .................................................................................... 192

12. Troubleshooting ..................................................................................................................... 195

12.1. How to Identify the Problem .............................................................................................. 195
12.2. Review and Analyze the Issue ............................................................................................ 195
12.3. Search for Additional Information ...................................................................................... 196
12.4. Veeam Support .................................................................................................................. 197
  12.4.1. Support Programs ....................................................................................................... 197
  12.4.2. Response Time SLA .................................................................................................... 198
  12.4.3. Contacting Customer Support ..................................................................................... 199
  12.4.4. Product Lifecycle ......................................................................................................... 201
  12.4.5. Third Party Software Support ....................................................................................... 202

13. Training Summary .................................................................................................................. 203

13.1. Key Points .......................................................................................................................... 203
13.2. Useful Resources ............................................................................................................... 205
13.3. Contacts ............................................................................................................................. 205
1. Introduction

This section provides a brief overview of the course and its learning objectives.

1.1. Course Overview

Keeping your business up and running at all times is critical. Businesses today require 24/7 access to data, efficient management of exploding data growth, and little tolerance for downtime and data loss. With Veeam® Availability Suite™, Veeam has created a new solution category and thus a new market: Availability for the Modern Data Center™ to enable the Always-On Business™:

- **High-Speed Recovery**: Rapid recovery of what you want, the way you want it
- **Data Loss Avoidance**: Near-continuous data protection and streamlined disaster recovery
- **Verified Recoverability**: Guaranteed recovery of every file, application or virtual server, every time
- **Leveraged Data**: Low-risk deployment with a production-like test environment
- **Complete Visibility**: Proactive monitoring and alerting of issues before operational impact

Veeam Backup & Replication delivers backup, recovery and replication for VMware and Hyper-V. This #1 VM Backup™ solution helps organizations meet RPOs and RTOs, save time, eliminate risks and dramatically reduce capital and operational costs. Veeam Availability Suite™ combines Veeam Backup & Replication with advanced monitoring and reporting capabilities to help organizations of all sizes protect virtualization, increase administrator productivity and mitigate daily management risks.

By the end of this course you should be able to:

- Understand basic and advanced backup terminology
- Understand Veeam Backup & Replication architecture, backup methods, transport modes and other mechanisms
- Install and set up Veeam Backup & Replication, Veeam ONE, Veeam Backup Enterprise Manager to prepare your infrastructure for assessment and backup deployment
- Create, edit and set up backups
- Create replications and perform their failovers, set up failover plans
- Verify restore points using such mechanisms as: SureReplica and SureBackup
- Restore Windows, Linux and other guest OS files, Exchange, Oracle, AD, SQL and SharePoint objects using different mechanisms provided by Veeam Backup & Replication
- Take backups off and archive backups to tape using native tape support and backup copy option
- Install, set up and work with WAN Accelerator
- Leverage SAN Snapshots for backups and restores
2. Overview of Veeam Products

This module will provide you with a brief overview of the range of Veeam products, introduce the purpose and idea behind the Veeam Availability Suite solution and help you get acquainted to some of the concepts that are important for the rest of the course.

Veeam Backup & Replication provides a set of features for building and maintaining a flexible backup infrastructure, performing data protection tasks (such as, regular backup and replication of VMs), and carrying out disaster recovery procedures. This section contains a high-level overview of Veeam Backup & Replication, its architecture and features, as well as data protection and disaster recovery concepts necessary to understand Veeam Backup & Replication background operations and processes.

2.1. Veeam Products

This topic will provide you with a brief overview of the range of Veeam products so you have a better understanding of the business problems they cover.

2.1.1. Veeam Backup & Replication

Veeam Backup & Replication is an availability, data protection and disaster recovery solution for VMware vSphere and Hyper-V virtual environments of any size and complexity.

To provide the most comprehensive protection of your virtual infrastructure, Veeam Backup & Replication complements image-based backup with image-based replication. You can back up any VM, VM container or VM disk, as well as replicate VMs onsite for high availability (HA) or offsite for disaster recovery (DR), across local area and wide area networks.

By leveraging the latest technological advancements of the virtualization technology, Veeam Backup & Replication delivers unprecedented replication speed. It provides near-continuous data protection (or near-CDP) at a fraction of the cost of traditional CDP systems – you can capture changes and update VM images as often as every few minutes as the replication job can be set to run Continuously.

Veeam Backup & Replication offers vPower – Veeam’s technology that allows you to:

- Immediately recover a failed VM, thus reducing downtime of production VMs to the minimum (see Instant VM Recovery).
- Verify recoverability of every backup by starting and testing VMs directly from VM backups in an isolated environment.
- Restore items from any virtualized applications with Veeam Explorers and U-AIR.
- Restore guest OS files with Multi-OS File-Level Recovery.

2.1.2. Veeam ONE

Veeam ONE delivers powerful, easy-to-use and affordable monitoring, reporting and capacity
planning for virtual and backup infrastructures:

- **Real-time monitoring** – 24x7 real-time monitoring and alerting, with built intelligence for fast troubleshooting and problem resolution
- **Documentation and management reporting** – pre-deployment analysis of backup requirements, complete documentation of the structure and state of your virtual and backup infrastructures, plus automated and on-demand reporting
- **Capacity planning** – trend analysis, provisioning recommendations, what-if modeling and more
- **Business categorization** – technical- and business-oriented views of your virtual environment

### 2.1.3. Veeam Management Pack for System Center

**Veeam Management Pack for System Center** supports both vSphere and Hyper-V virtual environments, offering the same features for monitoring, reporting and capacity planning for both hypervisors.

Veeam Management Pack extends System Center’s monitoring capabilities to include Hyper-V and vSphere virtual machines and hosts, the hardware, storage and network resources they run on, as well as the Veeam Backup & Replication infrastructure. Veeam MP automatically integrates System Center’s native monitoring of critical applications like Microsoft Exchange and SQL Server and provides drill-down view from the application to virtualization layer and further to the hardware sensors data.

### 2.1.4. Veeam plug-in for vSphere Web Client

Monitor your backup infrastructure directly from the **vSphere Web Client**, VMware’s next-generation administrative interface for vSphere. This plug-in delivers at-a-glance and detailed views of job status and backup resources, and also simplifies capacity planning and identification of unprotected VMs.

**Note:** The vSphere Web Client plug-in is installed from the vCenter Servers page of Configuration view in **Veeam Backup Enterprise Manager**.

### 2.1.5. The Veeam Backup & Replication Add-on for Kaseya

The **Veeam Backup Add-on for Kaseya** bridges the Kaseya platform with Veeam Backup & Replication and allows Managed Service Providers to remotely monitor their Veeam backup infrastructures and estimate data protection efficiencies for the managed virtual environments.

With the add-on, you can perform the following operations from within the Kaseya web interface:

- Audit the state and performance of Veeam backup infrastructure components
- Analyze VM data protection for managed customer virtual environments and ensure that critical VMs have valid backup and replica restore points that meet established RPO requirements
- See an overview of all types of jobs managed by Veeam backup servers and monitor job completion results
- Receive informative alerts about critical situations around the backup infrastructure components
and data protection operations
- Generate reports based on data collected from Veeam backup servers and protected VMs
- Monitor backup infrastructure machines and protected VMs, perform basic maintenance, troubleshoot and fix problems with Kaseya Live Connect

2.1.6. Veeam Backup & Replication Plug-in for LabTech

This Veeam plugin for LabTech is designed for Service Providers and IT Departments using the LabTech Remote Monitoring and Management (RMM) platform and Veeam Backup & Replication. With the Veeam Backup & Replication Plug-in for LabTech, you get a single pane of glass view of your Veeam backup activity from inside the LabTech Control Center, providing complete visibility into your virtual infrastructure.

You can perform the following from within the LabTech Control Center:
- Manage, view and monitor all backup jobs managed by Veeam backup servers including the ability to start, stop, retry and disable jobs
- Analyze protected and unprotected VMs to ensure critical VMs have valid backup and replica restore points
- Receive critical alerts and automatically raise tickets and alarms
- Perform day-to-day maintenance, troubleshoot and fix problems based off a pre-defined list of reports, monitors and data views with zero configuration required
- Generate reports based on data collected from the Veeam backup servers and associated VMs

2.1.7. Veeam Endpoint Backup FREE

Veeam Endpoint Backup FREE provides a simple solution for backing up Windows-based desktops and laptops. It is a free data protection and disaster recovery solution for physical machines. Veeam Endpoint Backup can be used to protect different types of computers and devices: desktops, laptops and tablets. The solution can be installed on any computer that runs the following OSes:
- Microsoft Windows 7 SP1 or later
- Microsoft Windows 2008 R2 SP1 or later

Veeam Endpoint Backup offers a variety of data protection. It allows to:
- Create a Veeam Recovery Media on an external hard drive, CD/DVD/BD, or create an ISO file with the Veeam Recovery Media on disk.
- Create an entire system image backup, back up specific computer volumes or individual folders with files. Backups can be stored on an external hard drive, in a network shared folder or on a Veeam backup repository.

In case of a disaster, the following restore operations can be performed:
- Start the OS from the Veeam Recovery Media and use Veeam Endpoint Backup and standard Microsoft Windows tools to diagnose and fix problems.
- Perform bare-metal restore.
- Restore necessary data from backups to its original location or a new location.

Veeam Endpoint Backup integrates with Veeam Backup & Replication. Backup administrators who use Veeam Backup & Replication in their VMware vSphere or Microsoft Hyper-V virtual environment, are able to take full advantage of Veeam backup repositories as target locations for the Veeam Endpoint Backup FREE jobs, which are stored in a separate folder for each endpoint protected. They can also perform advanced tasks with Veeam Endpoint backups: restore files and disks from backups and manage Veeam Endpoint backup jobs or backups created with these jobs right from Veeam Backup & Replication interface.

**Important!** Integration with Veeam Backup & Replication requires Veeam Backup & Replication 8.0 Update 2 or later.

### 2.2. Veeam Availability Suite

This section will overview Veeam Availability Suite and its purpose. Veeam Availability Suite combines the industry leading backup, restore and replication capabilities of Veeam Backup & Replication with the advanced monitoring, reporting and capacity planning functionality of Veeam ONE.

#### 2.2.1. Veeam Availability Suite Capabilities

In today’s interconnected and global business environment, customers, partners, suppliers and employees expect access to information and applications at any time and from any device, with no tolerance for downtime or data loss. IT organizations must therefore make data and applications available to all stakeholders every minute of every day. This is the era of the Always-On Business™.

Achieving non-stop service and continuous protection has traditionally required a significant investment in fully redundant systems with instant failover capabilities. These kinds of investments could only be justified for a few applications, so the vast majority of workloads were served with lower performing, legacy backup solutions allowing recovery time objectives and recovery point objectives (RTO and RPO) of several hours or days. These low performance levels fail to meet the requirements of the Always-On Business, creating a significant availability gap.

Veeam® bridges this availability gap by leveraging the capabilities of the modern data center – including virtualization, new storage integration and cloud capabilities – to provide five key enabling capabilities. These enabling capabilities in turn allow for a recovery time and point objective (RTPO™) of <15 minutes for the majority of workloads, bridging the availability gap and enabling the Always-On Business.

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>High-Speed Recovery</td>
<td>Enables low recovery time objectives (RTOs) of &lt;15 minutes; enables rapid recovery of the data customers want, in the form that they want it</td>
</tr>
</tbody>
</table>
### Benefit Description

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Loss Avoidance</strong></td>
<td>Avoids data loss by enabling low recovery point objectives (RPOs) of &lt;15 minutes, and by facilitating off-site data protection</td>
</tr>
<tr>
<td><strong>Verified Recoverability</strong></td>
<td>Ensures that files, applications, and virtual servers can be reliably restored when needed; ensures business resiliency through automated backup and DR testing</td>
</tr>
<tr>
<td><strong>Leveraged Data</strong></td>
<td>Eliminates the risks associated with application deployment, configuration changes, and other testing scenarios; allows testing of changes in a production-like environment before actually deploying them</td>
</tr>
<tr>
<td><strong>Complete Visibility</strong></td>
<td>Provides monitoring and alerting tools so that you can discover and be alerted to issues and potential problems in your IT environment before they have a significant impact on your operations</td>
</tr>
</tbody>
</table>

### 2.3. Key Concepts

In the “key concepts” topic, concepts like RTO and RPO will be defined, and their relation to Business Continuity and Disaster Recovery will be explained.

### 2.3.1. Key Concepts

<table>
<thead>
<tr>
<th>Concept</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business Continuity</strong> (BC)</td>
<td>An activity performed by an organization to ensure that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions.</td>
</tr>
<tr>
<td><strong>Disaster Recovery</strong> (DR)</td>
<td>A process, policies and procedures that are related to preparing for recovery or continuation of technology infrastructure which are vital to an organization after a natural or human-induced disaster.</td>
</tr>
<tr>
<td><strong>Recovery Point Objective</strong> (RPO)</td>
<td>The maximum tolerable period in which data might be lost from an IT service due to a major incident. Essentially, it is the acceptable time period data can be backdated to a restore.</td>
</tr>
<tr>
<td><strong>Recovery Time Objective</strong> (RTO)</td>
<td>The duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. Essentially, it is the amount of time allowable between off-line due to disaster and on-line from recovery.</td>
</tr>
</tbody>
</table>
3. Deployment

Veeam Backup & Replication is a modular solution which allows flexible scalability for environments of different sizes and configuration. The installation package of Veeam Backup & Replication includes a set of components used to configure your backup infrastructure. Some of them are mandatory and provide core functionality; some of them are optional and can be installed to provide additional functionality for your business and deployment needs. You can consolidate Veeam Backup & Replication components on the same machine, either physical or virtual, or you can set them up separately for a more scalable approach.

3.1. Core Components and Their Interaction

Veeam Backup & Replication comprises the following components. Some of the components are installed using a setup file and others are configured while working with the product.

3.1.1. Veeam Backup Server

The Veeam backup server is a Windows-based physical or virtual machine on which Veeam Backup & Replication is installed. It is the core component in the backup infrastructure that fills the role of the “configuration and control center”. The Veeam backup server performs all types of administrative activities including:

- Coordinating backup, replication, recovery verification and restore tasks
- Controlling job scheduling and resource allocation
- Setting up and managing backup infrastructure components as well as specifying global settings for the backup infrastructure

In addition to its primary functions, a newly deployed Veeam backup server also performs the roles of the default backup proxy, which manages the data handling, and the default backup repository, which handles the data storing tasks.

The Veeam backup server uses the following services and components:

<table>
<thead>
<tr>
<th>Veeam Backup Service</th>
<th>Veeam Installer Service</th>
<th>Veeam Backup Catalog Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manages scheduled jobs, serves Veeam Backup Enterprise Manager requests.</td>
<td>Enables installing, updating and configuring Veeam Backup &amp; Replication components.</td>
<td>Manages guest OS file system indexing for VMs and replicates system index data files to enable search through guest OS files.</td>
</tr>
</tbody>
</table>
### 3.1.2. Backup Proxy (VMware)

When Veeam Backup & Replication is initially installed, the Veeam backup server coordinates all job activities and, until you deploy a Backup Proxy, handles data traffic itself.

That is, when you run a backup, replication, VM copy, VM migration job or perform restore operations, VM data is moved from source to target through the Veeam backup server. So, by default Veeam backup server plays backup proxy role. This scenario is acceptable for virtual environments where few backup jobs are performed; in large-scale environments, however, the workload on the Veeam backup server will be significant.

To take the workload off the Veeam backup server, Veeam Backup & Replication uses backup proxies. A backup proxy is an architecture component that sits between data source and target and is used to process jobs and deliver backup traffic. In particular, the backup proxy tasks include retrieving VM data from the production storage, compressing and sending it to the backup repository (for example, if you run a backup job) or another backup proxy (for example, if you run a replication job). As the data handling task is assigned to the backup proxy, the Veeam backup server becomes the “point of control” for dispatching jobs to proxy servers.

The role of a backup proxy can be assigned to a dedicated Windows server (physical or virtual) in your virtual environment. You can deploy backup proxies both in the primary site and in remote sites. To optimize performance of several concurrent jobs, you can use a number of backup proxies. In this case, Veeam Backup & Replication will distribute the backup workload between available backup proxies.

Using backup proxies lets you easily scale your backup infrastructure up and down based on your demands. Backup proxies run light-weight services that take a few seconds to deploy. Deployment is fully automated – Veeam Backup & Replication installs the necessary components on a Windows-based server when you add it to the product console. As soon as you assign the role of a backup proxy to the added server, Veeam Backup & Replication starts the required services on it.

The primary role of the backup proxy is to provide an optimal route for backup traffic and enable efficient data transfer.
Transport Modes (VMware)

Efficiency of a backup job and time required for its completion in many respects depends on the transport mode. The following section will review various transport modes Veeam Backup & Replication uses to process VMware vSphere virtual machines.

Transport Modes (VMware)

The transport mode is a method that is used by the Veeam Data Mover Service to read VM data from the source and write VM data to the target.

Depending on the type of backup proxy and your backup architecture, the backup proxy can use one of the following data transport modes: Direct Storage Access, Virtual Appliance or Network. If the VM disks are located on the SAN storage and the SAN storage is added to the Veeam Backup & Replication console, the backup proxy can also use the Backup from Storage Snapshots mode. You can explicitly select the transport mode or let Veeam Backup & Replication automatically choose the mode.

For reading data, Veeam Backup & Replication offers the following modes (starting with the most efficient):

- Direct Storage Access
- Virtual Appliance
- Network

The Veeam Data Mover (transport) service is responsible for reading data on a backup proxy server. The transport mode can be defined in the settings of the backup proxy that performs the job. When configuring backup proxy settings, you can manually select a transport mode or let Veeam Backup & Replication select the most appropriate mode automatically. If you use automatic mode selection, Veeam Backup & Replication will scan the backup proxy configuration and its connection to the VMware infrastructure to choose the optimal transport mode. If multiple transport modes are available for the same proxy, Veeam Backup & Replication will choose the mode in the following order: Direct Storage Access → Virtual Appliance → Network.

For writing data to the target destination, Veeam Backup & Replication normally uses the Network mode. In some cases, such as VM replication or full VM recovery, Veeam Backup & Replication also supports the Virtual Appliance mode and the Direct Storage Access mode (for restore operations where the backup proxy is engaged, for example, full VM restore, VM disk restore and replica failback). You cannot select the transport mode for writing data – Veeam Backup & Replication selects it automatically, based on the backup proxy configuration.

For all transport modes, Veeam Backup & Replication leverages VMware vStorage APIs for Data Protection (VADP). VADP can be used for VMware vSphere starting from v4.

Applicability and efficiency of each transport mode primarily depends on the type of datastore used by the source host (local or shared), and on the backup proxy server type (physical or virtual). The table below shows recommendations for installing the backup proxy, depending on the storage type and desired transport mode.
<table>
<thead>
<tr>
<th>Production Storage Type</th>
<th>Direct SAN Access</th>
<th>Virtual Appliance</th>
<th>Network Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fiber Channel (FC) SAN</td>
<td>Install the backup proxy on a physical server with direct FC access to the SAN.</td>
<td>Install the backup proxy on a VM running on an ESX(i) host connected to the storage device.</td>
<td>Not recommended</td>
</tr>
<tr>
<td>iSCSI SAN</td>
<td>Install the backup proxy on a physical or virtual server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NFS storage</td>
<td>Install a backup proxy on a physical or virtual server.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local storage</td>
<td>Not supported</td>
<td>Install backup proxies on VMs in every ESX(i) host.</td>
<td>Install the backup proxy on one physical or virtual server in the environment.</td>
</tr>
</tbody>
</table>

Veeam Backup & Replication processes VM disks one by one or in parallel, depending on the data processing settings you select. If VM disks are located on different storages (for example, on the SAN and local storage subsystem), Veeam Backup & Replication will use different transport modes to process VM disks. In such scenario, it is strongly recommended that you select the **Failover to network mode if primary transport modes fail or are unavailable** option when configuring the mode settings for the necessary backup proxy.

**Direct Storage Access**

In the Direct storage access mode, Veeam Backup & Replication reads/writes data directly from/to the storage system where VM data or backups are located. This mode unites two transport modes:

- Direct SAN access
- Direct NFS access

**Direct SAN Access**

This mode is recommended if the ESX(i) host uses shared storage. The backup proxy leverages VADP to retrieve VM data directly from FC or iSCSI storage in the Storage Area Network (SAN). To retrieve data blocks from SAN LUN, the backup proxy uses metadata about the layout of VM disks on the SAN. Since data blocks are not retrieved over the Local Area Network (LAN), this mode minimizes disruptions to your production network during backup.
The process of data retrieval in *Direct SAN Access* mode includes the following steps:

1. The backup proxy sends a request to the ESX(i) host to locate the necessary VM on the datastore (1).
2. The host locates the VM and retrieves metadata about the layout of virtual disks on the SAN (that is, physical addresses of data blocks) and sends this metadata to the backup proxy (2, 3, 4).
3. The backup proxy uses the metadata to copy data blocks directly from the SAN and sends them to the target (5, 6).

**Important!** The backup proxy using Direct SAN Access mode must be connected directly into the SAN fabric. If no “Failover to the network mode” option is chosen and a direct SAN connection is not configured or not available when a job or task starts, the job or task will fail.

Veeam Backup & Replication allows you to switch to the Network mode and retrieve VM data through the ESX(i) host over the LAN if the SAN becomes inaccessible. This option is selected by default to ensure that backup jobs can be completed in any case. However, it puts additional load on your production network and thus may potentially affect performance if you are running backup and replication jobs during business hours.

**Important!** If you install Veeam Backup & Replication in a VM and plan to use the Direct SAN access mode without adding any Backup Proxy, you need to make sure that the Veeam Backup Server has direct access to the production storage or that you deploy a Backup Proxy that has direct access to the production storage.

Additionally, you can use the Direct SAN Access mode for those restore operations where the backup proxy is engaged, for example, full VM restore, VM disk restore and replica failover. The Direct SAN Access transport mode can be used to restore VMs with thick disks only. Before VM data is restored, the ESX(i) host needs to allocate space for the restored VM disk on the datastore:
When thick disks are restored, the ESX(i) host allocates space on disk before writing VM data. When thin disks are restored, the ESX(i) host attempts to allocate space on the fly, as requests for data blocks restore are received.

As a result, restore of thin disks involves extra allocation overhead if compared to restore of thick disks, which results in decreased performance.

To restore VMs with thin disks, you can use the Virtual Appliance mode or the Network mode. If you plan to process a VM that has both thin and thick disks, you can select the Direct SAN Access transport mode and choose to failover to the Network mode if SAN becomes inaccessible. In this case, Veeam Backup & Replication will use the Direct SAN Access transport mode to restore thick disks and the Network transport mode to restore thin disks. Alternatively, you can restore all VM disks as thick.

Direct NFS Access

The Direct NFS access is a recommended transport mode for VMs whose disks are located on NFS datastores.

The Direct NFS access mode provides an alternative to the Network mode. When Veeam Backup & Replication processes VM data in the Network mode, it uses VMware VDDK to communicate with the ESX(i) host. This produces additional load on the ESX(i) host. In the Direct NFS access mode, Veeam Backup & Replication bypasses the ESX(i) host and reads/writes data directly from/to NFS datastores. To do this, Veeam Backup & Replication deploys its native NFS client on the backup proxy and uses it for VM data transport. VM data still travels over the LAN but there is no load on the ESX(i) host.

The Direct NFS access mode can be used for all operations where the backup proxy is engaged:

- Backup
- Replication
- Full VM restore
- VM disk restore
- Replica failback
- Quick migration
The backup proxy used for VM data processing must have access to the NFS datastore(s) where VM disks are located.

Direct NFS access transport mode can be also used for data restores.

If you enable the Enable VMware tools quiescence option in the job settings, Veeam Backup & Replication will not use the Direct NFS transport mode to process running Microsoft Windows VMs that have VMware Tools installed.

If a VM has some disks that cannot be processed in the Direct NFS access mode, Veeam Backup & Replication processes these VM disks in the Network transport mode.

Virtual Appliance

This mode is recommended and can only be used if the backup proxy is deployed on a VM. The Virtual Appliance (also referred to as Hot-Add) mode uses the SCSI hot-add capability of ESXi hosts to attach disks of the backed up VM to the backup proxy VM. In this mode, VM data is retrieved directly from storage through the ESXi I/O stack, instead of going through the network stack, which improves performance.

Important! To ensure that a VM can be backed up using Virtual Appliance mode, it's important to make sure the ESX(i) host on which the backup proxy VM resides has access to the storage where disks of a backed up VM are located.

Network Mode

This mode can be used with any infrastructure configuration. However, when an alternative transport mode is applicable, the Network mode is not recommended because it has the lowest data retrieval speed. It is the only applicable mode when the backup proxy is a physical machine and the host uses local storage. In this mode, data is retrieved via the ESX (i) host over the LAN using Network Block Device protocol (NBD).
The process of data retrieval in Network mode includes the following steps:

1. The backup proxy sends a request to the ESX(i) host to locate the necessary VM on the datastore.
2. The host locates the VM, copies blocks of data and sends them to the backup proxy over the LAN.
3. VM files are exposed over the network and the data copy is performed.
4. Data blocks are sent to the backup proxy over the LAN.
5. The backup proxy transfers the data to target.

The Network mode is not recommended in case of low traffic throughput via the LAN (the copy of the VM disk usually contains a lot of data).

### 3.1.3. Off-host Backup Proxy (Hyper-V)

By default, when you perform backup, replication or VM copy jobs in the Hyper-V environment, VM data is processed directly on the source Hyper-V host where VMs reside and then moved to the target. However, VM data processing can produce unwanted overhead on the production Hyper-V host and impact performance of VMs running on this host. To take data processing off the production Hyper-V host, the off-host backup mode can be used.

The off-host mode shifts the backup and replication load to a dedicated machine – an off-host backup proxy. The off-host backup proxy functions as a “data mover” which retrieves VM data from the source datastore, processes it and transfers it to the destination.

**Backup Modes (Hyper-V)**

| Veeam Backup & Replication offers two modes for processing volume shadow copies – on-host backup and off-host backup. The difference between the two modes lies in the location where VM data is processed. |
On-host Backup

During on-host backup, VM data is processed on the source Hyper-V host where the VMs you want to back up or replicate reside. All processing operations are performed directly on the source Hyper-V host. For this reason, on-host backup may result in high CPU usage and network overhead on the host system.

The on-host backup process includes the following steps:

1. Veeam Backup & Replication triggers a snapshot of the necessary volume.
2. The Veeam data mover service uses the created volume snapshot to retrieve VM data; it then processes the VM data and copies it to the destination.
3. Once the backup process is complete, the volume snapshot is deleted.

Off-host Backup

In the off-host backup mode, backup processing shifts from the source Hyper-V host to a dedicated machine – an off-host backup proxy. The off-host backup proxy acts as a “data mover” – the Veeam Data Mover (also called “transport”) service running on it retrieves VM data from the source datastore, processes it and transfers to the destination. This type of backup does not impose load on the Hyper-V host – while resource intensive backup operations are performed on the off-host backup proxy, production hosts remain unaffected.

To perform off-host backup, Veeam Backup & Replication uses transportable shadow copies. The transportable shadow copy technology enables you to create a snapshot of a data volume on one server and import, or mount, it onto another server within the same subsystem (SAN) for backup and other purposes. The transport process is accomplished in a few minutes, regardless of the amount of the data. The process is performed at the SAN storage layer so it does not impact the host CPU usage or network performance.

In order to perform off-host backup, you must meet the following requirements:

- You must configure an off-host backup proxy. The role of an off-host backup proxy can be assigned only to a Microsoft Windows 2008 Server R2 machine with the Hyper-V role enabled, to a Microsoft Windows Server 2012 machine with the Hyper-V role enabled, or to a Microsoft Windows Server 2012 R2 machine with the Hyper-V role enabled.

**Note:** The version of the Hyper-V host and off-host backup proxy should match. For example, if you use a Microsoft Windows 2008 Server R2 machine with the Hyper-V role enabled as a Hyper-V host, you should deploy the off-host backup proxy on a Microsoft Windows 2008 Server R2 machine with the Hyper-V role enabled.

- In the properties of a backup or replication job, you must select the off-host backup method. If necessary, you can point the job to a specific proxy.
- The source Hyper-V host and the off-host backup proxy must be connected (through a SAN configuration) to the shared storage.
- To create and manage volume shadow copies on the shared storage, you must install and properly configure a VSS hardware provider that supports transportable shadow copies on the
off-host proxy and Hyper-V host. Typically, when configuring a VSS hardware provider, you need to specify a server controlling the LUN and disk array credentials to provide access to the array.

- If you back up VMs whose disks reside on a CSV with Data Deduplication enabled, make sure that you use a Microsoft Windows 2012 R2 machine as an off-host backup proxy and enable the Data Deduplication option on this off-host backup proxy. Otherwise, off-host backup will fail.

The off-host backup process includes the following steps:

1. Veeam Backup & Replication triggers a snapshot of the necessary volume on the production Hyper-V host.
2. The created snapshot is split from the production Hyper-V server and mounted to the off-host backup proxy.
3. The Veeam data mover running on a backup proxy uses the mounted volume snapshot to retrieve VM data; the VM data is processed on the proxy server and copied to the destination.
4. Once the backup process is complete, the snapshot is dismounted from the off-host backup proxy and deleted on the SAN.

**Important!** If you plan to perform off-host backup for a Hyper-V cluster with CSV, make sure you deploy an off-host backup proxy on a host that is NOT a part of a Hyper-V cluster. When a volume snapshot is created, this snapshot has the same LUN signature as the original volume. Microsoft Cluster Services do not support LUNs with duplicate signatures and partition layouts. For this reason, volume snapshots must be transported to an off-host backup proxy outside the cluster. If the off-host backup proxy is deployed on a node of a Hyper-V cluster, a duplicate LUN signature will be generated, and the cluster will fail during backup or replication.

**Services and Components for Backup Proxy (VMware) and Offhost Backup proxy (Hyper-V)**

The backup proxy uses the following services and components:

- **Veeam Installer Service** is an auxiliary service that is installed and started on any Windows server once it is added to the list of managed servers in the Veeam Backup & Replication console. This service analyzes the system, installs and upgrades necessary components and services depending on the role selected for the server.
- **Veeam Data Mover Service** is responsible for deploying and coordinating executable modules that act as "data movers" and perform main job activities on behalf of Veeam Backup & Replication, such as communicating with VMware Tools, copying VM files, performing data deduplication and compression and so on. It is installed and started on any Windows server once it is added to the list of managed servers in the Veeam Backup & Replication console as well.
- **Veeam Hyper-V Integration Service** (Hyper-V only) is responsible for communicating with the VSS framework during backup, replication and other jobs, and performing recovery tasks. It also deploys a driver that handles changed block tracking for Hyper-V.
Both Veeam Data Mover Service and Veeam Installer Service are always present at the Windows server added to the Veeam Backup & Replication UI. Some other services may also be there, depending on the role which this server is configured for.

### 3.1.4. Backup Repository

A backup repository is a location used by Veeam Backup & Replication jobs to store:

- backup chains
- copies of VMs
- metadata for replicated VMs.

Technically, a backup repository is a folder on the backup storage. By assigning different repositories to jobs and limiting the number of parallel jobs for each one, you can balance the load across your backup infrastructure.

In the Veeam backup infrastructure, you can use one of the following repository types:

- **Windows server with local or directly attached storage.** The storage can be a local disk, directly attached disk-based storage (such as a USB hard drive), or iSCSI/FC SAN LUN in case the server is connected into the SAN fabric.

  On a Windows repository, Veeam Backup & Replication deploys *Veeam data mover service* (when you add a Windows-based server to the product console, Veeam Backup & Replication installs a set of components including the Veeam data mover service on that server). When any
job addresses the repository, the Data Mover Service on the repository establishes a connection with the source-side Data Mover Service on the backup proxy, enabling efficient data transfer over LAN or WAN.

Windows repositories can be configured to function as vPower NFS Servers (VMware only). In this case, Veeam Backup & Replication will run the **Veeam vPower NFS Service** directly on the backup repository (namely, on the managing Windows server to which storage is attached) and provide ESX(i) hosts with transparent access to backed up VM images stored on the repository.

- **Linux server with local, directly attached storage or mounted NFS.** The storage can be a local disk, directly attached disk-based storage (such as a USB hard drive), NFS share, or iSCSI/FC SAN LUN in case the server is connected into the SAN fabric.

On the Linux repository, Veeam Backup & Replication deploys and starts the Veeam data mover (transport) service when a job addressing this repository is launched. This Data Mover Service establishes a connection with the source-side Data Mover Service on the backup proxy, enabling efficient data transfer over LAN or WAN.

- **CIFS (SMB) share.** This type of repository does not support Veeam data mover services, therefore data to the SMB share is written from a Windows-based gateway server. By default, this role performs a backup proxy that is utilized by the job for data transport.

However, if you plan to move VM data to an offsite SMB repository over a WAN link, it is recommended that you deploy an additional Windows gateway server in the remote site, closer to the SMB repository.

Veeam Backup & Replication will deploy a Veeam data mover service on that proxy server, which will improve data transfer performance.

- **Deduplicating storage appliance.** Veeam Backup & Replication supports the following deduplicating storage appliances:
  - EMC Data Domain
  - ExaGrid
  - HPE StoreOnce

**Note:** You can configure a backup repository to use rotated drives. This scenario can be helpful if you want to store backups on several external hard drives (for example, USB or eSATA) and plan to regularly swap these drives between different locations. If you are using rotated drives for a backup repository, select the **At rotated drives** check box when setting up a job.

**Offsite backup**

The common requirement for **offsite backup** is that one Veeam data mover service runs in the production site (closer to the source datastore), and the other Veeam data mover service runs in the remote target site (closer to the repository). During backup, Veeam data mover services maintain a stable connection, which allows for uninterrupted operation over WAN or slow links.
If you choose to back up to an offsite Windows or Linux repository, Veeam Backup & Replication will start the target-side Veeam data mover service on the Windows or Linux repository server. The source-side Veeam data mover service can be hosted either on the source host or on a dedicated off-host backup proxy, depending on the backup mode you use (onhost or off-host). Backup data is sent from the source to the repository over WAN.

If you choose to back up to an offsite SMB share in the onhost mode, you should deploy an additional Windows-based proxying server in the remote site and point the SMB share to this proxying server in the backup repository settings. In this scenario, Veeam Backup & Replication starts the target-side Veeam data mover service on the proxying server. The source-side Veeam data mover service can be hosted either on the source host or on a dedicated off-host backup proxy in the source site, depending on the backup mode you use (onhost or off-host).
Scale-Out Backup Repository

Prior to Veeam Backup & Replication version 9, each backup repository used a single dedicated container to store data. This approach led to constrains for configuring bigger backup jobs (e.g., for vCenter backup) due to limited physical capacity. V9 introduces a new logical entity – extendable, or scale-out backup repository. It embraces several repositories (extents), summarizing their capacity and offering flexible options for keeping massive backups.

An extent is a standard Veeam backup repository of any supported type (except for cloud) which was added to the scale-out repository.

A scale-out repository can be used for backup job; files stored in scale-out repository can be used for all types of restores, for SureBackup and backup copy jobs. It can also be utilized as a staging repository when performing restore from tape media; in this case, files will be placed to repository extents according to data placement policy configured for scale-out repository (see the next section for details). Integration with Veeam Endpoint Backup FREE is also supported.

When planning for a scale-out repository, consider the following limitations:

- A scale-out repository cannot be used as target for configuration backup jobs, replication jobs and VM copy jobs.
- A scale-out repository cannot be added to another scale-out repository as an extent.
- After adding a repository to a scale-out repository as an extent, it cannot be utilized as a stand-alone repository.

The following backup files placement policies are available:

- Data locality – all dependent backup files are placed on the same extent. For example, all VIBs...
are where possible placed together with their corresponding VBK. Built-in logic determines where the first VBK will be placed, based on several criteria: extent status (online/offline), free space and number of slots. When job processing starts, extent scheduler requests free space from the extents, and then estimates the required space to store the backup – it assumes that VBK will become avg. 50% less, and VIB will be 10% less (due to compression).

- Performance – for this mode, VBK and VIB are placed separately. Note that in this case network must support fast read/write operations.

If you decide to change the policy settings, consider that the new options will be applied starting from the next job run. Similarly, extent settings you specified on the previous step (in particular, per-VM files placement) will be updated starting from the next full backup creation.

To discover the extent where a particular VM data was stored, examine job session data.

**Important!** After you add an extent, you will not be able to use it as a standalone repository until you remove it from the scale-out repository.

You can remove an extent from scale-out repository by selecting the required scale-out repository and clicking **Edit Repository** on the toolbar or using the **Properties** command from the shortcut menu. After that, you can choose to keep the backups in the extent after it becomes a standalone repository or manually evacuate them.

### 3.2. Optional Components

**This topic defines some of the additional components of Veeam Backup & Replication and gives you an understanding of their functionality.**

#### 3.2.1. Veeam Backup Enterprise Manager

**Veeam Backup Enterprise Manager** is an optional component intended for distributed enterprise environments with multiple backup servers. Veeam Backup Enterprise Manager federates Veeam backup servers and offers a consolidated view of these servers through a web browser interface. You can centrally control and manage all jobs through a “single pane of glass”, edit and clone jobs, monitor job state, and get reporting data across all backup servers. Veeam Backup Enterprise Manager also enables you to search for Windows guest OS files in all current and archived backups across your backup infrastructure, and restore these files in one click.

Veeam Backup Enterprise Manager can be installed on a physical or virtual machine. You can deploy it on the Veeam backup server or use a dedicated machine.

Veeam Backup Enterprise Manager uses the following services and components:

- Veeam Backup Enterprise Manager coordinates all operations of Veeam Backup Enterprise Manager, aggregates data from multiple Veeam backup servers and provides control over these servers.
- Veeam Enterprise Manager Enterprise SQL Database is used by Veeam Backup Enterprise
Manager for storing data. The database instance can be located on an SQL Server installed either locally (on the same machine as Veeam Backup Enterprise Manager Server) or remotely.

- Veeam Backup Catalog Service on Veeam Backup Enterprise Manager works as a global, federal catalog service. It communicates with Veeam Backup Catalog services on Veeam backup servers connected to Veeam Backup Enterprise Manager and performs the following tasks:
  - Replicates indexing data from Veeam backup servers to create a global catalog for the whole backup infrastructure. By default, the Veeam Backup Catalog folder is located in the C:\VBRCatalog folder on the Veeam Backup Enterprise Manager server.
  - Maintains indexing data retention.
  - Lets you search for VM guest OS files in current and archived backup file.

### 3.2.2. U-AIR Wizard

*Universal Application Item-Level Recovery* (or *U-AIR*) addresses one of the most common IT problem – it enables you to restore individual objects from virtualized applications (for example, email messages, database records, directory objects and so on) for rare applications – when there is no suitable *Veeam Explorer*.

For recovery of application objects, U-AIR leverages the vPower technology. It starts the application and all components required for its proper work in an isolated virtual lab directly from compressed and deduplicated backup files. Once the VM is started, U-AIR provides transparent access to the backed up VM image through a proxy appliance that has visibility of both the virtual lab and production environment. Users can then extract the necessary application objects from the earlier VM images and bring them back to the production environment. U-AIR Universal wizard is a standalone component that can be installed and updated independent of the product on any machine in the production environment from which the restore process must be performed.

### 3.2.3. Mount Server

This component allows for reducing restore traffic when restoring to remote site: when restoring a VM to original location, it is reasonable to use the restore point stored in the backup repository located close to original (production) VM. This approach includes mount of the VM file system for browsing purposes (a staging system can be used) and for restore on target server. Thus, mount server must have access to backup repository and original (production) VM.

You should specify mount server that will work with repository data at restore in Veeam console when configuring repository settings. By default, the mount server running on Veeam backup server will be used.

Mount server comprises several components, one of them is *Veeam Mount Service* which is deployed on the repository (requires .NET).

Veeam needs to communicate with VM guest for remote mount operations:

- For Windows-based systems, Veeam uses iSCSI initiator to deploy Veeam Installer service (instead of deploying and removing drivers) on target machine. It prepares VM disks for file system emulation when mounting a VM from backup.
For Linux-based systems, Veeam uses FUSE driver that supports communication with VM guest.

Data communication between repository and *Mount Server* is performed using *Veeam data movers*. Mount server can work with different Veeam backup servers, as well as with Remote Shell.

### 3.2.4. Veeam Backup Search

In Veeam Backup & Replication, search for guest OS files in backups is performed with Veeam Backup Enterprise Manager. However, if you frequently need to search through a great number of backups, it is recommended to install Veeam Backup Search from the installation package on a machine running Microsoft Search Server. Veeam Backup Search is an optional component in the backup infrastructure that is used for the purpose of search performance optimization.

The *Veeam Backup Search* server runs the MOSS Integration Service that invokes updates of index databases on Microsoft Search Server. The service also sends search queries to Microsoft Search Server which processes them and returns necessary search results to Veeam Backup Enterprise Manager.

### 3.3. Deployment Scenarios

Veeam Backup & Replication can be used in virtual environments of any size and complexity right out of the box. The architecture of the solution supports onsite and offsite data protection, operations across remote sites and geographically dispersed locations. Veeam Backup & Replication provides flexible scalability and easily adapts to the needs of your virtual environment.

Before installing Veeam Backup & Replication, it is strongly advised to familiarize yourself with common deployment scenarios and carefully plan your backup infrastructure layout.

### 3.3.1. Simple Deployment

In a simple deployment scenario, one instance of Veeam Backup & Replication is installed on a physical or virtual Windows-based machine. This server is referred to as a *Veeam backup server*.

*Simple deployment* for VMware implies that the Veeam backup server fills three major roles:

- It functions as a management point, coordinates all jobs, controls their scheduling and performs other administrative activities.
- It acts as the default backup proxy for handling job processing and transferring backup traffic. All components necessary for the backup proxy functionality are installed on the Veeam backup server locally.
- It is used as the default backup repository. By default, backup files are stored to the `\backup` folder on the drive of the Veeam backup server which is judged to have the largest capacity to store them at the moment of the installation – the most amount of free disk space.
Simple deployment for Hyper-V implies that the Veeam backup server fills two major roles:

- It functions as a management point, coordinates all jobs, controls their scheduling and performs other administrative activities.
- It is used as the default backup proxy. During installation, Veeam Backup & Replication checks volumes of the machine on which you install the product and identifies a volume with the greatest amount of free disk space. On this volume, Veeam Backup & Replication creates the Backup folder that is used as the default backup repository.

In this scenario, source Hyper-V host acts as a backup proxy, handling job processing and transferring backup traffic directly to the target. All necessary backup proxy services are installed on source Hyper-V servers.

If you decide to use a simple deployment scenario in the Hyper-V environment, you can install Veeam Backup & Replication right on the Hyper-V host where VMs you want to work with reside. However, to use this Hyper-V host as the source for backup and replication, you will still need to add it to the Veeam Backup & Replication console.

If you plan to back up and replicate only a small number of VMs or evaluate Veeam Backup & Replication, this configuration is enough to get you started. Veeam Backup & Replication is ready for use right out of the box – as soon as it is installed, you can start using the solution to perform backup and replication operations. To balance the load of backing up and replicating your VMs, you can schedule jobs at different times.
In the environments that require a large number of backup or replication activities, the simple deployment scenario is not appropriate for the following reasons:

- The Veeam backup server might not have enough disk capacity to store the required amount of backup data.
- A significant load is placed on production servers that combine the roles of backup proxies and source hosts.

3.3.2. Advanced Deployment

For mid-size and large-scale environments with a great number of backup and replication jobs, the load on the Veeam Backup Server is heavy. In this case, it is recommended to use the advanced deployment scenario which moves the backup workload to dedicated backup proxies and backup repositories.

Advanced Deployment for VMware

The essence of the advanced deployment is that the backup proxy takes off a part of Veeam backup server activities (namely, it collects and processes data and moves backup traffic from source to target). In addition, the Veeam backup server no longer acts as a storage location – the backup proxy transports VM data to a dedicated backup repository which is the location for keeping backup files, VM copies, metadata and so on. The Veeam backup server in this scenario functions as a "manager" for deploying and maintaining backup proxies and repositories.

To deploy a backup proxy and/or a backup repository, you should add a server to Veeam Backup & Replication and assign a proxy and/or repository role to it. Veeam Backup & Replication will automatically install light-weight components and services onto these servers. A backup proxy does not require a separate SQL database – all settings are stored centrally, within the Veeam backup server’s SQL database.
With the advanced deployment scenario, you can easily meet your current and future data protection requirements. You can expand your backup infrastructure horizontally in a matter of minutes to match the amount of data you want to process and available network throughput. Instead of growing the number of backup servers or constantly tuning job scheduling, you can install multiple backup proxies and repositories and distribute the backup workload among them. The installation process is fully automated, which simplifies deployment and maintenance of the backup infrastructure in your virtual environment.

Veeam Backup & Replication assigns backup proxies to VMs included in the backup job one by one. Before processing a new VM in the VM list, Veeam Backup & Replication checks available backup proxies. If more than one backup proxy is available, Veeam Backup & Replication analyzes transport modes that the backup proxies can use to retrieve VM data and the current workload on the backup proxies to select the most appropriate one for VM processing.

The advanced deployment scenario can be a good choice for backing up and replicating off site. You can deploy a backup proxy in the production site and another one in the DR site, closer to the backup repository to avoid saturating the connection. When a job is performed, backup proxies on both sides establish a stable connection, allowing for efficient transport of data over a slow network connection or WAN.

**Note:** To regulate backup load, you can specify the maximum number of concurrent tasks per proxy and set up throttling rules to limit proxy bandwidth. The maximum number of concurrent tasks can also be specified for a backup repository in addition to the value of the read and write data rates for it.

Another advantage of the advanced deployment scenario is that it contributes to high availability — jobs can migrate between proxies if one of them becomes overloaded or unavailable.

**Advanced Deployment for Hyper-V**

In the advanced deployment scenario, data processing shifts from the Hyper-V Server to an off-host backup proxy — a dedicated machine that is deployed on the source side, closer to the source Hyper-V Host. The off-host backup proxy functions as a “data mover”, processing VM data and mediating the backup traffic from source to target. Therefore, the job processing overhead and data transport is offloaded from the source Hyper-V Host.

Backup data is no longer stored to the Backup Repository on the Veeam Backup Server. Instead, data is transported to dedicated backup repositories. The Veeam backup server becomes a “manager” for off-host Backup proxies and backup repositories.
### Component Description

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Virtual infrastructure servers</strong></td>
<td>Hyper-V hosts are used as source and target for backup and replication.</td>
</tr>
<tr>
<td><strong>Veeam backups server</strong></td>
<td>A configuration and control center for the backup infrastructure.</td>
</tr>
<tr>
<td><strong>Off-host backup proxy</strong></td>
<td>The component functions as a “data mover” and is used to retrieve VM data from the source datastore, process it and deliver to the target.</td>
</tr>
<tr>
<td><strong>Backup repository</strong></td>
<td>A location used to store backup files, VM copies and auxiliary replica files.</td>
</tr>
</tbody>
</table>

#### 3.3.3. Distributed Deployment

The *distributed deployment* scenario is recommended for large, geographically dispersed virtual environments with multiple Veeam backup servers installed across different sites. These backup servers are federated under Veeam Backup Enterprise Manager – an optional component that provides centralized management and reporting for these servers through a web interface.
Veeam Backup Enterprise Manager collects data from Veeam backup servers and enables you to run backup and replication jobs across the entire backup infrastructure through a “single pane of glass”, edit them, and clone jobs using a single job as a template.

Using indexing data consolidated on one server, Veeam Backup Enterprise Manager provides advanced capabilities to search for guest OS files of Windows-based VM backups created on all Veeam backup servers (even if they are stored in repositories on different sites), and recover them in a single click.

With flexible delegation options and security roles, IT administrators can delegate the necessary file restore or VM restore rights to authorized personnel in the organization – for example, allow database administrators to restore Oracle or SQL server VMs.

If you use Veeam Backup Enterprise Manager in your backup infrastructure, you do not need to install licenses on every Veeam backup server you deploy. Instead, you can install one license on the Veeam Backup Enterprise Manager server and it will be applied to all servers across your backup infrastructure. This approach simplifies tracking license usage and license updates across multiple Veeam backup servers.

In addition, VMware administrators will benefit from Veeam’s plug-in for vSphere Web Client that can be installed using Veeam Backup Enterprise Manager setup. They can analyze cumulative information on used and available storage space view and statistics on processed VMs, review success, warning, and failure counts for all jobs, easily identify unprotected VMs, and perform capacity planning for repositories, all directly from vSphere.

### 3.3.4. Distributed Architecture

**Veeam Backup & Replication provides enterprise scalability through the distributed architecture and automatic intelligent load balancing.**

**Distributed Architecture**

Distributing backup processing across multiple proxy servers and repositories:

- Makes it easier for you to scale your Backup & Replication deployment
- Enables you to achieve higher availability and redundancy: if a proxy goes down, another one
can still complete the task – no more single point of failure
- Reduces the impact from backups on the production infrastructure through intelligent load balancing
- Dramatically simplifies job scheduling (by automatically controlling the desired tasks concurrency)
- Controls backup storage saturation (for when the backup storage is too slow)

With automatic intelligent load balancing, Veeam Backup & Replication picks the best proxy server (best in terms of connectivity to VM data, as well as least loaded with other tasks) to perform the backup for a VM each time the job runs.

Built-in mechanisms of resource scheduling enable Veeam Backup & Replication to automatically select and use optimal resources to run configured jobs. Resource scheduling is performed by the Veeam Backup Service running on the Veeam backup server. When a job starts, it communicates with the service to inform it about the resources it needs. The service analyzes job settings, parameters specified for backup infrastructure components, current load on the components, and automatically allocates optimal resources to the job.

### Enabling Parallel Processing

![Options](image)

Multiple VMs and VM disks can be processed in parallel, optimizing your backup infrastructure performance and increasing the efficiency of resource usage; each data processing task within a job requires one CPU core – consider this value when configuring job settings.

**Note:** This is a global setting, so if configured, it will take effect for all backup, backup copy & replication jobs.

If you have *parallel processing* enabled and several proxies/repositories in the infrastructure, you can:
• Distribute backup processing across multiple proxy servers to make it easier for you to scale your Backup & Replication deployment
• Achieve higher availability and redundancy: if a proxy goes down, another one can still complete the task – no more single point of failure
• Reduce the impact from backups on the production infrastructure through intelligent load balancing
• Dramatically simplify job scheduling (by automatically controlling the desired tasks concurrency)
• Control backup storage saturation (for when the backup storage is too slow)

Backup I/O control

At the same time, it’s important to keep production storage availability from being impacted by too much load from parallel backup tasks. Backup I/O Control is a new, global setting that lets you set limits on how much latency is acceptable for any VMware or Hyper-V datastore. Those values are customizable.

For the Enterprise Plus Edition, Backup I/O Control can be used to set the latency on a per-datastore basis, rather than a single global setting. This is especially useful if you have datastores that need a higher/lower setting based on workload or importance, for example higher latency is usually acceptable for test/development workloads.

3.4. Prerequisites

Before you begin the installation process, take the following steps to prepare for deployment:

<table>
<thead>
<tr>
<th>Check Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform-specific and system requirements</td>
<td>Make sure the computer on which Veeam Backup &amp; Replication is to be installed meets the system requirements</td>
</tr>
<tr>
<td>Account permissions</td>
<td>Make sure all accounts you will be using have sufficient permissions. You will not be able to use Veeam Backup &amp; Replication successfully if the accounts do not have required permissions.</td>
</tr>
<tr>
<td>Ports</td>
<td>Communication between components requires a number of ports to be open. Carefully plan your backup strategy and infrastructure layout.</td>
</tr>
</tbody>
</table>

Also, note the following:

1. Veeam Backup & Replication requires .NET Framework 4. If it is not available, the Veeam Backup & Replication setup will install it on your computer.
2. Veeam Backup & Replication uses an SQL Server instance installed either locally or remotely. In case it is not installed, the Veeam Backup & Replication setup will install Microsoft SQL Server 2012 R2 Express on your computer. If a Microsoft SQL Server instance has already been installed by the previous version, Veeam Backup & Replication will connect to the existing database, upgrade it (if necessary) and use it for work.
3.4.1. Requirements

This section covers the list of system requirements for VMware vSphere and Microsoft Hyper-V environments, Veeam Backup & Replication console, virtual machines and backup targets, necessary rights and permissions, as well provides information on ports used by Veeam Backup & Replication.

**Important!** Pay attention on whether the architecture at the machine you are planning use for using for a particular role in your backup infrastructure is 64 or 32-bit.

The following components require 64-bit version of the operation system ONLY:

- Veeam backup server
- WAN Accelerator
- Veeam Explorers

3.4.2. Platform Support

Veeam Backup & Replication provides full support for the VMware vSphere virtualization platform.

**Virtual Infrastructure**

<table>
<thead>
<tr>
<th>Specification</th>
<th>VMware Requirement</th>
<th>Hyper-V Requirement</th>
</tr>
</thead>
</table>
| Platform                 | - VMware vSphere 6.0  
- VMware vSphere 5.x  
- VMware vSphere 4.x | Microsoft Hyper-V                                |
| Hypervisor               | - ESXi 6.0  
- ESXi 5.x  
- ESX(i) 4.x  
Free ESXi is not supported | - Microsoft Windows Server Hyper-V  
2012 R2  
- Microsoft Windows Server Hyper-V  
2012  
- Microsoft Windows Server Hyper-V  
2008 R2 SP1  
Microsoft Hyper-V Server (free hypervisor version) is supported |
| Management Server        | - vCenter Server 6.0  
- vCenter Server 5.x  
- vCenter Server 4.x | - Microsoft System Center Virtual Machine Manager 2008 R2 SP1  
- Microsoft System Center Virtual Machine Manager 2012 SP1  
- Microsoft System Center Virtual Machine Manager 2012 R2 |

**Important!** Please note free ESXi is not supported by Veeam Backup & Replication due to the
technical limitation: host?level snapshot backups are not supported with free ESXi.

Virtual Machines

<table>
<thead>
<tr>
<th>Specification</th>
<th>VMware Requirement</th>
<th>Hyper-V Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>All types and versions of virtual hardware are supported, including 62TB VMDK. VMs with disks engaged in SCSI bus sharing are not supported because VMware does not support snapshotting such VMs. RDM virtual disks in physical mode, independent disks, and disks connected via in-guest iSCSI initiator are not supported, and are skipped from processing automatically.</td>
<td>All types and versions of virtual hardware are supported, including Generation 2 virtual machine hardware and 64TB VHDX. Pass-through virtual disks and disks connected via in-guest iSCSI initiator are not supported, and are skipped from processing automatically.</td>
</tr>
<tr>
<td>OS</td>
<td>All operating systems supported by VMware. Application-aware processing is supported for Microsoft Windows 2003 and later. Microsoft Windows file-level restore option is supported for NTFS, FAT, FAT32 and ReFS file systems (ReFS is supported only if Veeam Backup &amp; Replication is installed on Microsoft Windows Server 2012 or Microsoft Windows Server 2012 R2). To restore files from non-Microsoft Windows guests (Linux, Solaris, BSD, Novell Netware), use the Multi-OS File Level Restore wizard.</td>
<td>All operating systems supported by Microsoft Hyper-V. Application-aware processing is supported for Microsoft Windows 2003 and later. Microsoft Windows file-level restore option is supported on NTFS, FAT, FAT32 and ReFS file systems (ReFS is supported only if Veeam Backup &amp; Replication is installed on Microsoft Windows Server 2012 or Microsoft Windows Server 2012 R2). To restore files from non-Microsoft Windows guests (Linux, Solaris, BSD, Novell Netware), use the Multi-OS File Level Restore wizard.</td>
</tr>
</tbody>
</table>
| Software      | - VMware Tools  
- All latest OS service packs and patches (required for application-aware image-level processing) | Microsoft Hyper-V Integration Services |

vCloud Director

<table>
<thead>
<tr>
<th>Specification</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Director (optional)</td>
<td>vCloud Director 5.x</td>
</tr>
</tbody>
</table>

3.4.3. System Requirements

Make sure that servers on which you plan to deploy backup infrastructure components meet
the following system requirements:

**Veeam Backup Server**

<table>
<thead>
<tr>
<th>Specification</th>
<th>VMware Requirement</th>
<th>Hyper-V Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>CPU: modern x86-64 processor (minimum 2 cores or vCPUs). Memory: 4 GB RAM plus 500 MB RAM for each concurrent job. Disk Space: 2 GB for product installation. 10 GB per 100 VM for guest file system catalog folder (persistent data). Sufficient free disk space for Instant VM Recovery cache folder (non-persistent data, at least 10 GB recommended). Network: 1 Gbps LAN for on-site backup and replication, and 1 Mbps WAN for off-site backup and replication recommended. High latency and reasonably unstable WAN links are supported.</td>
<td></td>
</tr>
<tr>
<td>OS</td>
<td>64-bit version of the following operating systems is supported: - Microsoft Windows Server 2012 R2 - Microsoft Windows Server 2012 - Microsoft Windows Server 2008 R2 SP1 - Microsoft Windows Server 2008 SP2 - Microsoft Windows 8.x - Microsoft Windows 7 SP1</td>
<td></td>
</tr>
</tbody>
</table>
### Specification

<table>
<thead>
<tr>
<th>Vmware Requirement</th>
<th>Hyper-V Requirement</th>
</tr>
</thead>
</table>
| During setup, the installer will perform system configuration check to determine if all prerequisite software is available on the machine where you plan to install Veeam Backup & Replication. If some of the required software components are missing, the setup wizard will offer you to install missing software automatically. This refers to:  
- Microsoft .NET Framework 4.0  
- Windows Installer 4.5  
- Microsoft SQL Server Management Objects  
- Microsoft SQL Server System CLR Types  
- Microsoft Visual C++ 2010 Service Pack 1 redistributable package  
| The following software needs to be installed manually:  
- Microsoft PowerShell 2.0 (required for PowerShell snap-in).  
- Internet Explorer 9.0 or later.  
- System Center Virtual Machine Manager 2012 R2/2012/2008 R2 Admin UI (optional, to be able to register SCVMM server with Veeam Backup & Replication infrastructure).  
- RDP client version 7.0 and later installed on the Veeam backup server (required to open the VM console during SureBackup recovery verification of Hyper-V VMs). The RDP client is pre-installed on Microsoft Windows 7/Windows Server 2008R2 OS and later. |

### SQL Database

Local or remote installation of the following versions of Microsoft SQL Server are supported:  
- Microsoft SQL Server 2014  
- Microsoft SQL Server 2012 (Full and Express Edition. Microsoft SQL Server 2012 Express Edition is included in the setup.)  
- Microsoft SQL Server 2008 R2 (Full and Express Edition)  
- Microsoft SQL Server 2008 (Full and Express Edition)  
- Microsoft SQL Server 2005 (Full and Express Edition)  

Due to its limitations, Microsoft SQL Server Express Edition should only be used for evaluation purposes or in the case of a small-scale production environment. For environments with a lot of VMs, it is necessary to install a fully-functional commercial version of Microsoft SQL Server.
**Note:** If you plan to back up VMs running Microsoft Windows Server 2012 R2 and Data Deduplication is enabled for some of VM volumes, it is recommended to deploy the Veeam Backup & Replication console on a machine running Microsoft Windows Server 2012 R2 with Data Deduplication feature enabled. Otherwise, certain types of restore operations for these VMs (such as Windows File Level Recovery) may fail.

### Backup Proxy

<table>
<thead>
<tr>
<th>Specification</th>
<th>VMware Backup Proxy Requirement</th>
<th>Off-host Backup Proxy Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware</strong></td>
<td>CPU: modern x86 processor (minimum 2 cores or vCPUs). Using multi-core processors improves data processing performance and allows for more tasks to be processed concurrently by the backup proxy. Memory: 2 GB RAM plus 200 MB for each concurrent task. Using faster memory (DDR3) improves data processing performance. Disk Space: 300 MB. Network: 1 Gbps LAN for on-site backup and replication and 1 Mbps WAN for offsite backup and replication recommended. High latency and reasonably unstable WAN links are supported.</td>
<td></td>
</tr>
</tbody>
</table>

**Important!** To protect VMware VMs running on ESXi 5.5 or newer, you must deploy backup proxies on machines running a 64-bit version of Microsoft Windows. VDDK 5.5 does not support 32-bit versions of Microsoft Windows.
## Backup Repository

<table>
<thead>
<tr>
<th>Specification</th>
<th>VMware Requirement</th>
<th>Hyper-V Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware</strong></td>
<td>CPU: x86 processor (x86-64 recommended). Memory: 4 GB RAM plus 2 GB RAM for each concurrent job. Disk space: 200 MB for Veeam Backup &amp; Replication components and sufficient disk space to store backup files and replicas (high-RPM drives and RAID10 configuration recommended). Network: 1 Gbps LAN for onsite backup and replication and 1 Mbps WAN for offsite backup and replication recommended. High latency and reasonably unstable WAN links are supported.</td>
<td></td>
</tr>
<tr>
<td><strong>OS</strong></td>
<td>Both 32-bit and 64-bit versions of the following operating systems are supported: - Microsoft Windows Server 2012 R2 - Microsoft Windows Server 2012 - Microsoft Windows Server 2008 R2 SP1 - Microsoft Windows Server 2008 SP2 - Microsoft Windows Server 2003 SP2 - Microsoft Windows 8.x - Microsoft Windows 7 SP1 - Microsoft Windows Vista SP2 - Linux (SSH and Perl required)</td>
<td></td>
</tr>
</tbody>
</table>

## Tape Server

<table>
<thead>
<tr>
<th>Specification</th>
<th>VMware Requirement</th>
<th>Hyper-V Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware</strong></td>
<td>CPU: x86 processor (x86-64 recommended). Memory: 2 GB RAM plus 200MB for each concurrent task. Using faster memory (DDR3) improves data processing performance. Disk Space: 300 MB. Network: 1 Gbps LAN.</td>
<td></td>
</tr>
<tr>
<td><strong>OS</strong></td>
<td>Both 32-bit and 64-bit versions of the following operating systems are supported: - Microsoft Windows Server 2012 R2 - Microsoft Windows Server 2012 - Microsoft Windows Server 2008 R2 SP1 - Microsoft Windows Server 2008 SP2 - Microsoft Windows Server 2003 SP2 - Microsoft Windows 8.x - Microsoft Windows 7 SP1 - Microsoft Windows Vista SP2</td>
<td></td>
</tr>
</tbody>
</table>
WAN Accelerator

<table>
<thead>
<tr>
<th>Specification</th>
<th>VMware Requirement</th>
<th>Hyper-V Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td>CPU: x86-64 processor. Using multi-core processors improves data processing performance and is highly recommended on WAN links faster than 10 Mbps. Memory: 8 GB RAM. Using faster memory (DDR3) improves data processing performance. Disk Space: Global cache size as defined by user, plus 20GB per each 1TB of source VM data. SSD storage is highly recommended on WAN links faster than 10 Mbps.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network: 1 Gbps or faster for onsite backup and replication and 1 Mbps or faster for offsite backup and replication. High latency and reasonably unstable WAN links are supported.</td>
<td></td>
</tr>
<tr>
<td>OS</td>
<td>Only 64-bit versions of the following operating systems are supported:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows Server 2012 R2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows Server 2012</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows Server 2008 R2 SP1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows Server 2008 SP2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows Server 2003 SP2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows 8.x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows 7 SP1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows Vista SP2</td>
<td></td>
</tr>
</tbody>
</table>

Cloud Gateway

Same system requirements as for Tape Server are applicable.

Backup Target

Backup can be performed to the following disk-based storage targets:

- **Local (internal) storage** of the backup repository server.
- **Direct Attached Storage (DAS)** connected to the backup repository server, including external USB/eSATA drives and raw device mapping (RDM) volumes.
- **Storage Area Network (SAN)**. The backup repository server must be connected into the SAN fabric via a hardware or virtual HBA or software iSCSI initiator, and the corresponding volumes must be mounted in the guest operating system of the backup repository server.
- **Network Attached Storage (NAS)** able to represent itself as an SMB (CIFS) share (direct operation) or NFS share (must be mounted on a Linux backup repository server).
- **EMC Data Domain** (DD OS version 5.4, 5.5 or 5.6) with DDBoom license. Both Ethernet and Fibre Channel (FC) connectivity is supported.
- **ExaGrid** (firmware version 4.7 or later).
- **HPE StoreOnce** (via SMB or NFS share).
Storage Integration

Backup from Storage Snapshots and Veeam Explorer for Storage Snapshots for VMware vSphere is supported for the following storage devices:

- **HPE 3PAR StoreServ**
  - Fibre Channel (FC) or iSCSI connectivity.
  - 3PAR OS 3.1.2 or later.
- **HPE StoreVirtual (LeftHand / P4000 series) and StoreVirtual VSA**
  - iSCSI connectivity only.
  - SAN/iQ version 9.5 or later.
- **NetApp FAS, FlexArray (V-Series), Edge VSA and IBM N Series (NetApp FAS OEM)**
  - NFS, Fibre Channel (FC) or iSCSI connectivity.
  - Data ONTAP version 8.1, 8.2 or 8.3
  - 7-mode or cluster-mode
- **EMC VNX, VNX2 and VNXe**
  - NFS, Fibre Channel (FC) or iSCSI connectivity (depending on applicable storage device)

**Note:** Hyper-V has native integration with storage snapshots for backup via Hardware VSS, so the list of storage devices the integration is possible for listed above is relevant only for vSphere.

Tape

<table>
<thead>
<tr>
<th>Specification</th>
<th>VMware Requirement</th>
<th>Hyper-V Requirement</th>
</tr>
</thead>
</table>
| Hardware      | Veeam Backup & Replication supports Linear Tape-Open tape libraries starting from 3rd generation (LTO3) or later:  
- Physical libraries and standalone drives, virtual tape libraries.  
- Partitions of the physical or virtual tape libraries presented to the Veeam backup server.  
**Important!** If you plan to run both Veeam Backup & Replication and 3rd party tape-recording software (for example, in your evaluation lab), consider that Veeam Backup & Replication by default will periodically lock the drive to perform rescan, preventing other software from recording. |  |
### Module 3: Deployment

#### Veeam Certified Engineer v9 . Textbook

<table>
<thead>
<tr>
<th>Specification</th>
<th>VMware Requirement</th>
<th>Hyper-V Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Software</strong></td>
<td>Tape Drive(s):</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- If multiple driver installation modes are supported for your storage device, make sure the driver is installed in the mode that allows for multiple open handles from a host to a drive to exist at the same time.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- VMware does not support tape drives connected directly to ESX(i) 4.x and later.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Device-specific, vendor-supplied OEM driver for Microsoft Windows must be installed for tape drive(s). Tape drives appearing in Microsoft Windows Device Manager as Unknown or Generic are not supported.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- If multiple driver installation modes are available for your tape device, use the one that allows for multiple open handles from a host to a drive to exist at the same time. For example, if your tape vendor provides “exclusive” and “non-exclusive” drivers, you should install the “non-exclusive” one.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- The tape device can be connected to only a single server (Veeam Backup Server or Tape Server)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tape Library:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- It is recommended that you use tape devices with original equipment manufacturer (OEM) drivers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Veeam supports medium changers that have no Windows drivers available, such device is recognized as the unknown medium changer in the Microsoft Device Manager list.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- If using a Tape Library and there is no Windows driver available for the Media Changer, Native SCSI Commands will be used instead.</td>
<td></td>
</tr>
</tbody>
</table>

#### Veeam Backup Enterprise Manager Server

<table>
<thead>
<tr>
<th>Specification</th>
<th>VMware Requirement</th>
<th>Hyper-V Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware</strong></td>
<td>Processor: x86-64 processor. Memory: 2 GB RAM. Hard Disk Space: 2 GB for product installation plus sufficient disk space to store guest file system catalog from connected backup servers (according to data retention policy). Network: 1 Mbps or faster connection to Veeam backup servers.</td>
<td></td>
</tr>
<tr>
<td><strong>OS</strong></td>
<td>64-bit version of the following operating systems is supported:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows Server 2012 R2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows Server 2012</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows Server 2008 R2 SP1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows Server 2008 SP2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows Server 2003 SP2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows 8.x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft Windows 7 SP1</td>
<td></td>
</tr>
<tr>
<td><strong>Software</strong></td>
<td>- Microsoft Internet Information Services 7.0 or later</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft .NET Framework 4.0 (included in the setup)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Windows Installer 4.5 (included in the setup)</td>
<td></td>
</tr>
</tbody>
</table>
### Module 3: Deployment

<table>
<thead>
<tr>
<th>Specification</th>
<th>VMware Requirement</th>
<th>Hyper-V Requirement</th>
</tr>
</thead>
</table>
| **Client Software** | - Microsoft Internet Explorer 9.0, Mozilla Firefox 22.0, Google Chrome 27.0 or later versions.  
- Microsoft Excel 2003 or later (to view Excel reports). | |
| **SQL Database** | Local or remote installation of the following versions of Microsoft SQL Server are supported:  
- Microsoft SQL Server 2014  
- Microsoft SQL Server 2012 (Full and Express Edition. Microsoft SQL Server 2012 Express Edition is included in the setup.)  
- Microsoft SQL Server 2008 R2 (Full and Express Edition)  
- Microsoft SQL Server 2008 (Full and Express Edition)  
- Microsoft SQL Server 2005 (Full and Express Edition) | |

#### Veeam Backup Search

<table>
<thead>
<tr>
<th>Specification</th>
<th>VMware Requirement</th>
<th>Hyper-V Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hardware</strong></td>
<td>Refer to corresponding Microsoft Search Server version system requirements</td>
<td></td>
</tr>
<tr>
<td><strong>OS</strong></td>
<td>Refer to corresponding Microsoft Search Server version system requirements</td>
<td></td>
</tr>
</tbody>
</table>
| **Software** | - Microsoft Search Server 2008 (including Express edition)  
- Microsoft Search Server 2010 (including Express edition) | |

#### Veeam Explorer for Microsoft Exchange

<table>
<thead>
<tr>
<th>Specification</th>
<th>VMware Requirement</th>
<th>Hyper-V Requirement</th>
</tr>
</thead>
</table>
| **Microsoft Exchange** | Veeam Explorer for Microsoft Exchange supports mailbox database (EDB) files created with 64-bit versions of the following Microsoft Exchange systems:  
- Microsoft Exchange 2010 SP1, SP2 or SP3  
- Microsoft Exchange 2013  
- Microsoft Exchange 2013 SP1  
- Microsoft Exchange 2016  
To open mailbox databases, Veeam Explorer for Microsoft Exchange requires a service dynamic link library (ESE.DLL) that is installed together with Microsoft Exchange. | |
| **Software** | Microsoft Outlook 2013 or 2010 (64-bit) for PST exports (optional) | |
Veeam Explorer for Microsoft SharePoint

<table>
<thead>
<tr>
<th>Specification</th>
<th>VMware Requirement</th>
<th>Hyper-V Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SharePoint</td>
<td>- Microsoft SharePoint 2013</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft SharePoint 2010</td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td>Veeam Explorer for Microsoft SharePoint is installed on</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the machine running Veeam Backup &amp; Replication. All</td>
<td></td>
</tr>
<tr>
<td></td>
<td>editions including Veeam Backup Free Edition are</td>
<td></td>
</tr>
<tr>
<td></td>
<td>supported.</td>
<td></td>
</tr>
<tr>
<td>Staging SQL Server</td>
<td>1. The staging Microsoft SQL Server can run on the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>machine where Veeam Explorer for Microsoft SharePoint</td>
<td></td>
</tr>
<tr>
<td></td>
<td>is installed (Veeam backup server) or on a remote server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. The staging system must run the same or later version</td>
<td></td>
</tr>
<tr>
<td></td>
<td>of Microsoft SQL Server as the server that hosts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>restored Microsoft SharePoint content databases. For</td>
<td></td>
</tr>
<tr>
<td></td>
<td>example, if the Microsoft SharePoint server uses</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Microsoft SQL Server 2008, the staging system can run</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Microsoft SQL Server 2008 or later.</td>
<td></td>
</tr>
</tbody>
</table>

Veeam Explorer for Microsoft SQL

<table>
<thead>
<tr>
<th>Specification</th>
<th>VMware Requirement</th>
<th>Hyper-V Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft SQL Server</td>
<td>- Microsoft SQL Server 2014</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft SQL Server 2012</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft SQL Server 2008 R2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft SQL Server 2008</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Microsoft SQL Server 2005 SP4</td>
<td></td>
</tr>
<tr>
<td>Staging SQL Server</td>
<td>For export scenarios and restore to the state before a</td>
<td></td>
</tr>
<tr>
<td></td>
<td>selected transaction, Veeam Explorer for Microsoft SQL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Server uses a staging Microsoft SQL Server. By default,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>local Microsoft SQL Server deployed with Veeam backup</td>
<td></td>
</tr>
<tr>
<td></td>
<td>server will be used as a staging system, but it is also</td>
<td></td>
</tr>
<tr>
<td></td>
<td>supported to use a remote staging server. This Microsoft</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SQL Server must have the same or later version as the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>original Microsoft SQL Server.</td>
<td></td>
</tr>
</tbody>
</table>
Veeam Explorer for Oracle

<table>
<thead>
<tr>
<th>Specification</th>
<th>VMware Requirement</th>
<th>Hyper-V Requirement</th>
</tr>
</thead>
</table>
| Oracle System | The following versions of Oracle Database are supported as source/target systems for database backup and restore:  
- Oracle Database 12c (for Windows or Linux OS)  
- Oracle Database 11g (for Windows or Linux OS)  
  Automatic Storage Management (ASM) is supported for Oracle 11g and later, requires ASMlib present.  
  Oracle Real Application Clusters (RAC) are not supported.  
  **Note:** Currently, Oracle Database Express Edition (XE) is supported for Windows-based machines only. | |

Staging server is used to fine-tune the restore point in case a user needs to restore database to the state before specific transaction. At the first launch of Veeam Explorer it tries to obtain the staging Oracle server settings using the built-in algorithm. You can specify another staging server, either local (for Windows VMs only) or remote (for both Windows and Linux VMs).

The following requirements apply to staging server:

1. A staging server must have the same Oracle database version as the source (original) and target Oracle server.
2. If you plan to restore databases with Automatic Storage Management enabled, the staging and target servers should have ASM enabled, too.
3. Oracle Database Express Edition (XE) cannot be used as a staging system.

Veeam Explorer for Microsoft Active Directory

<table>
<thead>
<tr>
<th>Specification</th>
<th>VMware Requirement</th>
<th>Hyper-V Requirement</th>
</tr>
</thead>
</table>
| Microsoft Active Directory Domain Controllers | - Microsoft Windows Server 2012 R2  
- Microsoft Windows Server 2012  
- Microsoft Windows Server 2008 R2  
- Microsoft Windows Server 2008  
- Microsoft Windows Server 2003 SP2  
Minimum supported domain and forest functional level is Windows 2003. Veeam Explorers can be only installed on a 64-bit Windows operating system. | |
### Software

- Veeam Backup & Replication 8.0 or 9.0 (any edition).
- Microsoft PowerShell 2.0.
- To open database files, Veeam Explorer for Microsoft Active Directory uses a service dynamic link library (esent.dll) that is installed together with Microsoft Active Directory Domain Services and can be found in the system directory at `%SystemRoot%`.
- Esent.dll should be of the same version as Microsoft Active Directory Domain Services used to create database files.
- To restore account passwords, Veeam Explorer for Microsoft Active Directory uses the registry database. If you plan to restore passwords, make sure that System registry hive is available (default location is `%systemroot%\System32\Config`). If you restore Active Directory database from Active Directory backup using Veeam file-level restore, the registry hive will be located automatically. Otherwise (for example, if you restore from an imported backup or from VeeamZIP file) make sure that the System registry hive is located in the same folder as the DIT file.

### Note

Database files created by a domain controller can be open only if Veeam Explorer is installed on a Windows machine with OS version same or above the version of that domain controller's OS.

### 3.4.4. Required Permissions

The accounts used for installing and using Veeam Backup & Replication should have the following permissions:

<table>
<thead>
<tr>
<th>Account</th>
<th>VMware Requirement</th>
<th>Hyper-V Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup Account</td>
<td>The account used for product installation must have the Local Administrator permissions on the Veeam backup server to install Veeam Backup &amp; Replication.</td>
<td></td>
</tr>
<tr>
<td>Target/Source Host Permissions</td>
<td>Root permissions on the source ESX(i) host Root (or equivalent) permissions on Linux backup repository Write permission on the target folder and share If vCenter Server is used, administrator credentials are required</td>
<td>Local Administrator permissions on the source Hyper-V server Root (or equivalent) permissions on Linux backup repository Write permission on the target folder and share</td>
</tr>
<tr>
<td>Account</td>
<td>VMware Requirement</td>
<td>Hyper-V Requirement</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SQL Server</td>
<td>The account used to run Veeam Backup Management Service must have the database owner role for the VeeamBackup database on the SQL Server instance.</td>
<td>The account used to run Veeam Backup Enterprise Manager must have the database owner role for the VeeamBackupReporting database on the SQL Server instance.</td>
</tr>
<tr>
<td>Veeam Backup Enterprise Manager</td>
<td>Local Administrator permissions on the Veeam Backup Enterprise Manager server to install Veeam Backup Enterprise Manager To be able to work with Veeam Backup Enterprise Manager, users should be assigned the Portal Administrator, Restore Operator or Portal User role.</td>
<td></td>
</tr>
<tr>
<td>Veeam Backup Search</td>
<td>Local Administrator permissions on the Microsoft Search Server to install Veeam Backup Search</td>
<td></td>
</tr>
<tr>
<td>Veeam Explorer for Exchange</td>
<td>Full access to Microsoft Exchange database and its log files for item recovery The account you plan to use for recovery should have both read and write permissions to all files in the folder with the database. Access rights can be provided through impersonation.</td>
<td></td>
</tr>
<tr>
<td>Veeam Explorer for SharePoint</td>
<td>The account used for working with Veeam Explorer for SharePoint requires membership in the sysadmin fixed server role on the staging Microsoft SQL Server. The account used for connection with target SharePoint server where document item(s)/list will be restored needs the following: - If permissions of the item being restored are inherited from the parent item (list) – <strong>Full Control</strong> for that list is required. - If permissions are not inherited, and restored item will replace an existing item – then <strong>Contribute</strong> for the item and <strong>Full Control</strong> for its parent list are required.</td>
<td></td>
</tr>
</tbody>
</table>

### 3.5. Upgrading Veeam Backup & Replication

**To perform upgrade, run the Veeam Backup & Replication setup file. For details on the upgrade procedure, refer to Veeam Backup & Replication Release Notes.**

### 3.5.1. Before You Upgrade

When you upgrade the product, the Veeam Backup & Replication database gets upgraded, too, and becomes available for usage with the newly installed version. It is strongly recommended that you perform configuration backup of the Veeam Backup & Replication database before upgrading the product. In this case, you will be able to easily go back to a previous version in case of issues with upgrade.

### 3.5.2. After You Upgrade

When upgrade is complete, it is recommended that you check all existing jobs, backup infrastructure...
components and make changes to the default upgrade configuration if necessary. Consider the following:

- During upgrade to Veeam Backup & Replication 9.0, backup files and VM replicas that were created with previous versions are not impacted in any way.
- The Credentials Manager will be populated with credentials that were used for connecting to virtual infrastructure servers, Microsoft Windows servers, Microsoft SMB3 servers, Linux servers and credentials used for guest processing.
Labs for Module 3: Deployment

This module gets you acquainted with the components that make up Veeam Backup & Replication architecture and explains how to choose between Veeam Backup & Replication deployment scenarios.

The corresponding labs provide you with an opportunity to dive into the Veeam Backup & Replication and Veeam Backup Enterprise Manager installation.

Get into the Lab

<table>
<thead>
<tr>
<th>Lab</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Analyze Veeam Backup &amp; Replication installation</td>
<td>In live instructor-led trainings, Veeam Backup &amp; Replication has already been pre-installed to save time - Simply review the Veeam Backup &amp; Replication installation process. You will later in the class install a second Veeam Backup &amp; Replication deployment.</td>
</tr>
<tr>
<td>3.2</td>
<td>Analyze Veeam Backup Enterprise Manager installation</td>
<td>In live instructor-led trainings, Veeam Backup Enterprise Manager has already been pre-installed to save time - simply review the Veeam Backup Enterprise Manager installation process.</td>
</tr>
<tr>
<td>3.3</td>
<td>Adding Veeam Backup &amp; Replication to Veeam Backup Enterprise Manager</td>
<td>Add Veeam Backup &amp; Replication server to Veeam Backup Enterprise Manager console to control and manage all the Veeam Backup &amp; Replication jobs through a single &quot;pane of glass&quot;.</td>
</tr>
<tr>
<td>3.4</td>
<td>Setting up Veeam ONE (part one)</td>
<td>Add VMware vSphere and Microsoft Hyper-V hosts to Veeam ONE interface and schedule data collection.</td>
</tr>
</tbody>
</table>
4. Initial Configuration

In this module you will learn how to configure all components of Veeam Backup & Replication product, including backup server, backup proxy and backup repository. We will also review about global settings and how they improve the product’s performance and Veeam Backup & Replication user interface.

4.1. Adding Servers

For building your backup infrastructure in a VMware vSphere environment, Veeam Backup & Replication supports the following types of servers:

- VMware Server
- Windows Server
- Linux Server
- vCloud Director

For building your backup infrastructure in a Hyper-V environment, Veeam Backup & Replication supports the following types of servers:

- Hyper-V Server
- Windows Server
- Linux Server
- SMB v3 Server

Managed servers are physical or virtual machines that are used as source and target hosts, backup proxies, repositories and other servers included in the backup infrastructure. The table below shows which roles can be assigned to the different types of servers managed by Veeam Backup & Replication.

<table>
<thead>
<tr>
<th>Server Type</th>
<th>Source</th>
<th>Replication Target</th>
<th>Backup Proxy</th>
<th>Backup Repository</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Server (standalone ESX(i) host or vCenter Server) / Hyper-V Server (standalone Hyper-V Server, SCVMM or Hyper-V cluster)</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Windows Server</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Linux Server</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>vCloud Director</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
</tbody>
</table>

Any ESXi host is essentially a Linux server. Thus, you can add ESXi hosts both as virtualization servers and as standard file servers, depending on the role you wish to assign them. Note that if you plan to use the same host as an ESXi host and Linux server, you should add it to Veeam Backup & Replication twice.
Similarly, any Hyper-V Server is essentially a Windows server. Thus, you can add Hyper-V hosts both as virtualization servers and as standard file servers, depending on the role you wish to assign them. Note that if you plan to use the same host as a Hyper-V server and Windows server, you should add it to Veeam Backup & Replication twice.

**Note:** If there is a vCenter server in the infrastructure, it is recommended that you add vCenter server instead of separate ESX(i) hosts to provide more flexibility at work.

**Note:** When you create a credential record for the user account that you plan to use to connect to a Linux server or VM running Linux OS, you can either choose a root account, or specify a non-root account and use the Non-root account section to grant sudo rights to this account. Then, to provide a non-root user with root account privileges, select the Elevate account to root check box and to add the user account to sudoers file, select the Add account to the sudoers file automatically check box. If you do not enable this option, you will have to manually add the user account to the sudoers file.

4.2. Adding a VMware Backup Proxy

In the backup infrastructure, a backup proxy acts as a “data mover.” While the backup server fills the role of the job manager, the backup proxy actually performs main data handling – it retrieves data, processes it and transfers to the target destination. Using backup proxies enables you to take the job processing off the backup server and allows for better scalability of your backup infrastructure.

Proxy deployment recommendations depend on a particular configuration of your virtual infrastructure.

To add a backup proxy to your backup infrastructure, you should assign this role to a Windows server that is already added to the list of managed servers.

By default, Veeam Backup & Replication adds the Veeam backup server to the list of backup proxies. A local backup proxy may be sufficient for the simplest backup or replication scenarios; however, for larger VMware environments, you will need to deploy a number of additional VMware proxy servers to offload the Veeam backup server.

4.3. Adding a Hyper-V Off-host Backup Proxy

If you plan to perform backup or replication operations in the off-host mode, you should add Hyper-V off-host backup proxies. In the backup infrastructure, a backup proxy acts as a “data mover.” While the backup server fills the role of the job manager, the off-host backup proxy actually performs main data handling – it retrieves VM data from the source storage, processes it and transfers to the target destination. Using off-host backup proxies enables you to take the job processing off the source Hyper-V host.

To add an off-host backup proxy to your backup infrastructure, you should assign this role to a Windows server that is already added to the list of managed servers. When deploying an off-host
backup proxy, make sure that you meet the requirements.

4.4. Adding Backup Repositories

Backup repository is a location for storing backup data and auxiliary files. You can assign the role of a backup repository to any Windows or Linux server added to the list of managed servers in Veeam Backup & Replication, or to any shared CIFS folder to which the backup server has access. Windows-based backup repositories can also perform the role of the Veeam vPower NFS server, enabling advantages of the vPower technology for multi-OS file-level restore, Instant VM Recovery, SureBackup and U-AIR capabilities.

**Note:** You can permanently remove a backup repository from the backup infrastructure. When you remove a backup repository, Veeam Backup & Replication unassigns the backup repository role from the server and this server is no longer used as a backup repository.

Veeam Backup & Replication does not remove backup files and other data stored on the backup repository. You can re-connect the backup repository at any time and import backups from this backup repository to Veeam Backup & Replication.

**Important!** The remove operation has the following limitations: you cannot remove a backup repository that is used by any backup or replication job (including Configuration Backup). To remove such backup repository, you first need to delete a reference to this backup repository in the job settings.

4.5. Performing Configuration Backup and Restore

With Veeam Backup & Replication, you can create a configuration backup of the Veeam backup server.

When you create a configuration backup, you export the configuration data from the Veeam Backup SQL database and save it into a backup file on the repository. If the Veeam backup server fails for some reason, you can re-install it and then quickly restore its configuration from the backup file. Alternatively, you can apply the configuration of one Veeam backup server to any other Veeam backup server in your backup infrastructure.

It is recommended that you regularly create a configuration backup for every Veeam backup server in your backup infrastructure. Periodic configuration backups reduce the possibility of data loss and minimize the administrative overhead if any problem with Veeam backup server(s) occurs.

4.5.1. Creating Configuration Backups

When you perform a configuration backup, Veeam Backup & Replication retrieves configuration data
for the Veeam backup server from the SQL database, writes this data into a set of .xml files and archives these .xml files to a .bco file.

Veeam Backup & Replication exports configuration data for all Veeam Backup & Replication objects:

<table>
<thead>
<tr>
<th>Object</th>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup infrastructure configuration data</td>
<td>vSphere hosts, HPE SAN storages, backup proxies, backup repositories, virtual labs, and other</td>
</tr>
<tr>
<td>Jobs configuration</td>
<td>Backup, replication and other jobs, registered backups, replicas, restore points, and other</td>
</tr>
<tr>
<td>Veeam Backup &amp; Replication settings</td>
<td>User roles, SMTP settings, and so on</td>
</tr>
<tr>
<td>Dynamic objects</td>
<td>Folders in the server hierarchy or snapshots in the SAN storage topology and other dynamic data.</td>
</tr>
</tbody>
</table>

**Note:** When storing credentials for the infrastructure objects, Veeam Backup & Replication does not keep passwords if encryption is not enabled. During the restore process, you will have to specify passwords manually. If by the time of restore passwords for credentials records have changed, you can specify new values for these records.

The configuration backup is job-driven. Just like any other job, you can schedule it to run regularly or start it manually. You can choose the backup repository to which the configuration backup should be stored and specify the necessary retention policy settings.

By default, Veeam Backup & Replication is configured to create a configuration backup daily. The resulting configuration backup file is stored in the `\VeeamConfigBackup\%BackupServer%` folder in the default backup repository. However, for security’s sake, it is recommended that you store configuration backups on the backup repository other than the default one. In this case, configuration data of the Veeam backup server(s) will be available for recovery even if the Veeam backup server fails.

**Note:** When you configure a new backup repository, Veeam Backup & Replication offers you to change the configuration backup file location from the default backup repository to the new backup repository. Click **Yes**, and Veeam Backup & Replication will automatically change the backup target in the configuration backup job properties and will use this target in future. Configuration backups that were created before the target change will remain in the default backup repository. You can manually copy them to the new backup repository to have all restore points of the configuration backup in one place.

### 4.5.2. Creating Encrypted Configuration Backups

Veeam Backup & Replication requires that you encrypt the configuration backup if you have created at least one password in the Password Manager on the backup server.
When you encrypt jobs or tapes with passwords, Veeam Backup & Replication creates a set of keys that are employed in the encryption process. Some of encryption keys, for example, storage keys and metakeys, are stored in the Veeam Backup & Replication database. If a configuration backup was non-encrypted, data from it could be freely restored on any backup server. The encryption keys would be saved to the Veeam Backup & Replication database, and the content of encrypted files might become accessible for unintended audience.

If the Password Manager contains at least one password and you do not enable encryption for the configuration backup, Veeam Backup & Replication disables configuration backup. To enable the configuration backup, you must configure encryption settings in the configuration backup job properties.

4.5.3. Restoring Configuration Data

If a Veeam backup server fails, you can re-deploy it, restore configuration data from the backup and apply it to the re-built server. Alternatively, you can apply configuration data to any other Veeam backup server in your backup infrastructure. In this case, you can use the configuration backup to migrate the settings of one Veeam backup server to another Veeam backup server. After the restore process is finished, the Veeam backup server is ready for work. In terms of configuration, you get a replica of the Veeam backup server you had, without additional adjustments or fine-tuning.

During the restore process, Veeam Backup & Replication retrieves configuration data from the .bco file and writes it to the Veeam Backup & Replication SQL database used by the target Veeam backup server.

There are two restore modes available:

- **Select Restore** if you want to restore data from the configuration backup on the same Veeam backup server where this backup was created. In this case, Veeam Backup & Replication will retrieve configuration data from the backup, store it to the specified database and, if necessary, perform a rescan of hosts, servers, VM replicas, backup repositories and tape libraries that were initially connected to the Veeam backup server.

- **Select Migrate** if you want to restore data from the configuration backup on a new Veeam backup server. In this case, Veeam Backup & Replication will simply retrieve configuration data from the backup and store it to the specified database. No rescan operation will be performed.

**Note:** When restoring the configuration, stop all jobs that are currently running. During restore of configuration, Veeam Backup & Replication temporary stops the Veeam Backup services and jobs.

4.6. Managing Network Traffic

If you plan to perform offsite backup or replicate VMs to a remote DR site, you can manage network traffic with the following options:
4.6.1. Setting Network Traffic Throttling Rules

You can apply network throttling rules to limit the maximum throughput of traffic going from source to target. In Veeam Backup & Replication, network traffic throttling rules are created and enforced globally, at the level of the Veeam backup server. Rules are set not for a single IP address, but for a pair of IP address ranges, on the source side and on the target side. Throttling rules are checked against backup infrastructure components between which VM data is transferred over the network: more specifically, on which Veeam data mover services engaged in the job are started.

4.6.2. Managing Data Transfer Connections

By default, for every job session, Veeam Backup & Replication uses multithreaded data transfer. VM data from source to target is transferred over five TCP/IP connections. However, when several jobs are scheduled to run at the same time, the load on the network may be heavy. If the network capacity is not sufficient to support multiple data transfer connections, you can configure network traffic throttling rules or disable multithreaded data transfer.

4.6.3. Preferred Networks

You can select a network over which VM data must be transported during data protection and disaster recovery tasks. This option can be helpful if you have a non-production network and want to route the VM traffic over this network instead of the production network.

To select networks for data transfer, you must create a network priority list. Veeam Backup & Replication will use networks from this list for VM data transport. If a connection over a priority network cannot be established for some reason, Veeam Backup & Replication will automatically fail over to a production network.

4.6.4. Network Traffic Encryption

You can enable network traffic encryption (in flight encryption) for data going between the primary site and disaster recovery site. Network traffic encryption helps you raise the security level for your data. If encrypted data is intercepted in the middle of data transfer, the eavesdropper will not be able to decrypt it or get access to it.

Network data encryption for different subnets is enabled by default. If you want to enable data encryption within the same subnet, you must create a network traffic rule for this subnet and select the data encryption option for the rule. As a result, the traffic going between servers that fall into the source and target IP addresses ranges will be encrypted according to the 256-bit Advanced Encryption Standard (AES-256).

4.7. Global Notification Settings

Notifications help ensure visibility for the processes that are happening within Veeam
Backup and Replication.

4.7.1. Specifying E-Mail Notification Settings

With Veeam Backup & Replication, you can select to receive email messages in the case of success or failure of a created backup or replication job. To be able to receive email messages, you should configure general email notification settings and select to receive a notification when creating a corresponding job.

**Tip:** To receive email notification about all jobs performed on the Veeam backup server in one email, configure email notification settings in Veeam Backup Enterprise Manager.

4.7.2. Specifying Other Notification Settings

You can configure Veeam Backup & Replication to automatically notify you about the following events:

- Low disk space
- Support contract expiration
- New product versions and available updates

When you run a job, Veeam Backup & Replication checks disk space on the target backup repository and production storage. If the disk space is below a specific value, Veeam Backup & Replication will display a warning message in the job session details.

By default, email recipients specified in global notification settings are informed about the support expiration date in every received email notification. Veeam Backup & Replication starts sending such notifications 14 days before the expiration date. Expiration information is also shown on the splash screen and on the License Information window.

You can configure Veeam Backup & Replication to automatically check for new product versions and updates available on the Veeam website. When a new version of the product or a new product update becomes available on the website, Veeam Backup & Replication displays an icon in the system tray. An icon is displayed once a week.

For Microsoft Hyper-V environments, Veeam Backup & Replication also notifies about updates that should be installed on Microsoft Hyper-V hosts and off-host backup proxies: if a Microsoft Hyper-V host or an off-host backup proxy connected to the Veeam backup server misses important fixes/patches, it can potentially hinder work of Veeam Backup & Replication.

**Important!** To get notified about updates and patches, make sure that the Veeam backup server is connected to the Internet. In the opposite case, update notification will not work.

If you do not want to get notified about available updates, you can disable this option. However, it is recommended that you leave update notifications enabled not to miss critical updates and patches.
4.8. Getting to Know User Interface

The user interface of Veeam Backup & Replication is designed to let you quickly find commands you need and perform necessary data protection and disaster recovery tasks. This section will familiarize you with elements of the application user interface.

4.8.1. Main Menu

The main menu in Veeam Backup & Replication contains commands related to general application settings. The following operations can be performed:

- Update components installed on servers connected to Veeam Backup & Replication
- Start PuTTY
- Set up user roles
- Configure traffic throttling rules
- Manage credentials
- Enable and disable SAN plug-ins
- Perform configuration backup and restore
- Define general application options
- View program help, work with licenses and program logs
- Exit Veeam Backup & Replication

4.8.2. Navigation Pane

The navigation pane, located on the left side of the window, provides centralized navigation and enables you to easily access Veeam Backup & Replication items organized in views.

The navigation pane is made up of two areas:

- The upper, or the inventory pane, displays a hierarchy or a list of all items relevant for a specific view. The content of the inventory pane is different for different views. For example, in the **Infrastructure** view, the inventory pane displays a list of backup infrastructure components – virtual infrastructure servers, backup proxies and backup repositories. In the **Virtual Machines** view, the inventory pane displays a list of servers connected to Veeam Backup & Replication.
- The lower pane contains a set of buttons that enables you to switch between Veeam Backup & Replication views.

4.8.3. Ribbon and Tabs

Operation commands in Veeam Backup & Replication are organized into logical groups and collected together under tabs on the ribbon. The ribbon is displayed at the top of the main application window; it contains the **Home** tab that is always present, and context-sensitive tabs.
The Home tab provides quick access to the most commonly performed operations. It enables you to create different types of jobs, perform restores, and import operations. This tab is always displayed, no matter which view is currently open.

Context-sensitive tabs contain commands specific for certain items and appear when these items are selected. For example, if you open the Backup & Replication view and select a backup job in the working area, the Jobs tab containing buttons for operations with jobs will appear on the ribbon. In a similar manner, if you open the Files view and select a file or folder, the File tab containing buttons for operations with files will appear on the ribbon.

**Note:** Commands for operations with items in Veeam Backup & Replication are also available from the shortcut menu.

### 4.8.4. Views

Veeam Backup & Replication displays its items in views. When you click the button of a specific view in the navigation pane, its content is displayed in the working area of Veeam Backup & Replication.

Veeam Backup & Replication offers the following views:

<table>
<thead>
<tr>
<th>Views</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup &amp; Replication</td>
<td>Used for work with all kind of jobs. It also displays a list of created backups and replicas that can be used for various restore operations, and provides statistics on recently performed jobs.</td>
</tr>
<tr>
<td>Virtual Machines</td>
<td>Displays the inventory of your virtual infrastructure. The inventory can be presented from different perspectives: Compute, Storage, VM Folders and VM Tags. This view is used to work with VMs and VM containers.</td>
</tr>
<tr>
<td>Files</td>
<td>Displays a file tree for servers connected to Veeam Backup &amp; Replication, and is primarily used for file copying operations.</td>
</tr>
<tr>
<td>Backup Infrastructure</td>
<td>Displays a list of all backup infrastructure components: servers, hosts, backup proxies, backup repositories and WAN accelerators. This view is used to set up the backup infrastructure that will be used for various data protection and disaster recovery tasks.</td>
</tr>
<tr>
<td>Storage Infrastructure</td>
<td>Displays a list of storage systems, volumes and snapshots. This view is used to restore data from storage snapshots (available only for VMware VMs).</td>
</tr>
</tbody>
</table>
4.8.5. Working Area

The working area of Veeam Backup & Replication displays a list of items relevant to a specific view. The working area looks different depending on the view that is currently open. For example, if you open the History view, the working area will display a list of job sessions and restore tasks performed with Veeam Backup & Replication. If you open the Virtual Machines view, the working area will display a list of virtual machines that reside on servers connected to Veeam Backup & Replication.
Labs for Module 4: Initial Configuration

Before proceeding to the day-to-day operation sections, we need to configure the backup infrastructure for the lab.

Get into the Lab

<table>
<thead>
<tr>
<th>Lab</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Connecting Virtual Infrastructure Servers</td>
<td>Add vSphere host and Hyper-V host to Veeam Backup &amp; Replication.</td>
</tr>
<tr>
<td>4.2</td>
<td>Configuring a Backup Proxy</td>
<td>Review the default backup proxy settings to understand its specifics.</td>
</tr>
<tr>
<td>4.3</td>
<td>Configuring a Backup Repository</td>
<td>Configure a main scale-out backup repository and a remote backup repository for off-site transfers.</td>
</tr>
<tr>
<td>4.4</td>
<td>Setting Up Notifications</td>
<td>Set up notifications to receive email notifications with results on jobs performed on the Veeam backup server.</td>
</tr>
</tbody>
</table>
5. Protect

5.1. Creating Backup Jobs

To perform backup of VMs, you should create a backup job by means of the New Backup Job wizard. This section will guide you through all steps of the wizard and provide explanations for available options.

5.1.1. Before You Begin

Prior to creating a backup job, make sure you have set up all necessary backup infrastructure components for the job.

During every job run, Veeam Backup & Replication checks disk space on the destination storage. If the disk space is below a specific threshold value, Veeam Backup & Replication will display a warning in the job session log. To specify the disk space threshold, select **Options** from the main menu. On the **Notifications** tab, specify the amount of free disk space required in a percentage.

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

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

You must also make assumptions on compression and deduplication ratios, change rates, and other factors. The following figures are typical for most sites; however, it is important to understand your environment if there are exceptions:

- Compression and deduplication savings 2:1 or more; typical is 3:1 or better, but always be conservative when estimating required space.
- Typical change rate of 5% day; this can vary tremendously per server and some include additional space for one-off full backups, and so on.

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

**Note:** With Veeam ONE, you can use the **VM Change Rate Estimation** report from the Infrastructure Assessment pack as a ballpark pre-deployment assessment of the potential amount of free space that should be available on the target repositories.

When adding the VMs to the job, to quickly find the necessary object, you can use the search field at the bottom of the Add Objects window. The available options are:

- Everything, Folder, Cluster, Host, Resource pool, VirtualApp or Virtual machine for the vSphere
infrastructur e.
• Everything, Folder, Host Group, SCVMM, Cluster, Host or Virtual machine for the Hyper-V infrastructure.

5.1.2. Backup Methods

Veeam Backup & Replication provides the following methods for creating regular backup files:

• Reverse incremental backup – recommended for disk-to-disk backup
• Incremental backup – recommended for disk-to-disk-to-tape and remote site backups
  • Forward incremental backup
  • Forever forward incremental backup

Retention Policy

Every successful job run creates a new restore point that lets you return your data to an earlier point in time. When you define retention policy, you specify how many restore points you want to keep and thus how ‘far’ you want to be able to roll back. Once the specified number is exceeded, the earliest restore point will be automatically removed. So if the retention policy is set to three and you already have three restore points, the fourth successful job run will generally delete the restore point created during the first job run.

**Note:** When the allowed number of restore points in the backup chain is exceeded, Veeam Backup & Replication deletes the whole backup file, not separate VMs from it. For this reason, in some situation a certain VM may have fewer restore points in the backup chain than is specified in the retention policy settings. This can happen if a backup job processes a number of VMs or VM containers and some VMs or VM containers fail to be processed in some job sessions.

Reverse Incremental Backup

Reverse incremental backup implies that during the first run of a backup job, a full backup of a VM is created. VM data is copied block by block, compressed at an appropriate compression level, and stored in a resulting full backup file (.vbk). All subsequent backups are incremental (that is, Veeam Backup & Replication copies only those data blocks that have changed since the last job run). During reverse incremental backup, Veeam Backup & Replication “injects” changes into the .vbk file to rebuild it to the most recent state of the VM. It also creates a reverse incremental backup file (.vr b) containing data blocks that are replaced when the full backup file is rebuilt. Therefore, the most recent restore point is always a full backup, and it gets updated after every backup cycle.
This backup method lets you perform forever-incremental backups and save disk space because you only have to store one full backup on the backup repository. If the number of restore points allowed by the retention policy is exceeded, Veeam Backup & Replication will simply delete the oldest reverse increment.

Reverse incremental backup enables you to immediately restore a VM to the most recent state without extra processing because the most recent restore point is a full backup file. If you need to restore a VM to a particular point in time, Veeam Backup & Replication will apply the required .vrb files to the .vbk file to get to the required restore point.

**Retention for Reverse Incremental Backup**

Using reverse incremental backup, Veeam Backup & Replication immediately deletes the earliest reverse increment as soon as it meets the retention policy. For example, if the retention policy is set to three restore points, two latest reverse increments and a full backup will be retained.

**Incremental Backup**

During the first run of an *incremental backup*, Veeam Backup & Replication creates a full backup file (.vbk). During subsequent backups, it only gets changes that have taken place since the last performed backup (whether full or incremental) and saves them as incremental backup files (.vib) next to the full backup.
<table>
<thead>
<tr>
<th><strong>Forward Incremental Backup</strong></th>
<th><strong>Forward Incremental-Forever Backup</strong></th>
</tr>
</thead>
</table>
| **Backup Chain**              | The first and only full backup and a set of forward incremental backups following it.
|                                | synthetic full and/or active full backups. |
| **How to set up**             | Select the Incremental backup mode in the job settings. Enable synthetic full backups and/or active full backups. |
| **Specifics**                 | Select the Incremental backup mode in job settings. Do not enable synthetic full backups and/or active full backups. |
|                               | - No synthetic operations – only write |
|                               | - The full backup chain is removed only after the last increment in the chain meets the retention policy |
|                               | - The best choice if company regulation and policies require you to regularly move a created backup file to tape or a remote site |
|                               | - Always the indicated amount of restore points |
|                               | - More load on storage (because when applying retention policy, the changes are injected to full backup – see Retention Policy for more details) |

**Forever Forward Incremental Backup**

![Forever Forward Incremental Backup Diagram]

**Note:** With Veeam Backup & Replication, you can easily switch between backup methods. Veeam Backup & Replication will not transform the previously created chain. Instead, it will create a new chain next to the existing one in the following manner:

1. If you switch from the reverse incremental method to the forward incremental method, Veeam Backup & Replication will create a set of incremental backups next to the reverse incremental chain. The full backup in the reverse incremental chain will be used as a starting point for produced increments.
2. If you switch from the forward incremental method to the reverse incremental method, Veeam Backup & Replication will first create a full backup next to the incremental backup chain. At subsequent job cycles, Veeam Backup & Replication will transform this full backup and add reverse incremental backups to the chain.
Forward Incremental Backup

Retention for Forever Forward Incremental Backup

If the number of restore points in forever forward incremental backup chains exceeds the retention policy settings, Veeam Backup & Replication transforms the backup chain to make room for the most recent restore point.

**For example:** The retention policy is set to seven restore points.

When Veeam Backup & Replication detects that the number of allowed restore points is exceeded, it starts the transform process. Veeam Backup & Replication merges data blocks from the incremental backup copied on Monday into the full backup copied on Sunday. This way, the full backup file 'moves' one step forward – from Sunday to Monday.

The incremental backup copied on Monday becomes redundant and is removed from the chain.
As a result, you have a chain of a full backup as of Monday and six incremental backups Tuesday through Sunday. That way, 3x I/O are performed: first the incremental backup is written to the repository on Sunday, then one read and one more write are executed in order to perform the transform process.

Retention for Forward Incremental Backup

To be able to restore from a forward incremental backup, you need to have a full backup and a chain of subsequent increments on disk. If you delete a full backup, the whole chain of increments will become useless. In a similar manner, if you delete any increment before the restore point to which you want to roll back, you won’t be able to restore your data (since later increments depend on earlier increments).

For this reason, if you select forward incremental backup, in some days there will be more restore points on the disk than specified by your retention policy. Veeam Backup & Replication will remove the full backup chain only after the last increment in the chain meets your retention policy (which will happen once the retention policy reaches the next full backup).

For example: The retention policy is set to three restore points.

A full backup is performed on Sunday, incremental backups are performed Monday through Saturday, and a synthetic full backup is scheduled on Thursday. Although the policy is already breached on Wednesday, the full backup is not deleted because without it the chain of increments would be useless, leaving you without any restore point at all. Thus, Veeam Backup & Replication will wait for the next full backup and two increments to be created, and only then delete the whole previous chain consisting of the full backup and increment, which will happen on Saturday.

Active and Synthetic Full Backups

To let you get the most out of incremental backup, Veeam Backup & Replication enables you to create active full backups and schedule the creation of synthetic full backups on specific days. This may help you avoid long chains of increments, ensure safety of backup data, and allow you to meet the requirements of your retention policy.
Active Full Backup

In some cases, you need to regularly create a full backup. For example, your corporate backup policy may require that you create a full backup on weekends and run incremental backup on work days. To let you conform to these requirements, Veeam Backup & Replication offers the ability to periodically perform active full backups.

The **active full backup** produces a full backup of a VM, just as if you ran the backup job for the first time. Veeam Backup & Replication retrieves data for the whole VM from the source, compresses and deduplicates it, and stores it to the full backup file – `.vbk`.

The active full backup resets the chain of increments: all subsequent increments use the latest active full backup as a new starting point. A previously used full backup file remains on disk until it is automatically deleted according to the backup retention policy.

You can create active full backups manually or schedule a backup job to create active full backups with a certain periodicity.

- To create an active full backup manually, use the **Active Full** command from the shortcut menu of a corresponding backup job.
- To schedule active full backups, specify scheduling settings in the **Advanced** section of a corresponding backup job. You can schedule active full backups to run weekly, for example, every Saturday, or monthly, for example, every fourth Sunday of a month.

Having active fulls together with the forward incremental backup methods is generally a good method when the backup repository performance is weak – that way, only sequential writes to the backup repository are performed – no transforms. However, additional time and load at the production storage are involved in that case as creating a full backup might be time, network bandwidth and resources consuming.

Synthetic Full Backup

In some situations, running active full backups periodically may not be an option. Active full backups are very resource-intensive and consume considerable amount of network bandwidth. As an alternative, you can create synthetic full backups.

In terms of data, the **synthetic full backup** is identical to an active full backup. The synthetic full backup is a `.vbk` file that contains data from the whole VM. The difference between these two backup
types lies in the way VM data is retrieved:

<table>
<thead>
<tr>
<th>Active Full Backup</th>
<th>Synthetic Full Backup</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veeam Backup &amp; Replication retrieves VM data from the source datastore (volume) where the VM resides, compresses and deduplicates it, and writes it to the .vbk file on the backup repository.</td>
<td>Veeam Backup &amp; Replication does not retrieve VM data from the source datastore (volume). Instead, it “synthesizes” a full backup from data you already have on the backup repository. Veeam Backup &amp; Replication accesses the previous full backup file and a chain of subsequent increments on the backup repository, consolidates VM data from these files and writes consolidated data into a new full backup file. As a result, the created synthetic full backup file contains the same data you would have if you created a full backup in a regular manner.</td>
</tr>
</tbody>
</table>

That way, you can minimize the load on the production storage during backup process, while still maximizing the number of available restore points if any backup file should become corrupt.

Veeam Backup & Replication treats a synthetic full backup as a regular full backup. As well as any other full backup, the synthetic full backup resets the chain of increments. All subsequent increments use the created synthetic full backup as a new starting point. A previously used full backup file remains on disk until it is automatically deleted according to the backup retention policy.

The synthetic full backup has a number of advantages:

- Does not use network resources: It is created from backup files you already have on disk.
- Imposes less load on the production environment: It is created right on the backup repository.

With Veeam Backup & Replication, you can schedule creation of synthetic full backups on specific days.

**For example:** You can configure a backup job to perform daily forward incremental backups and schedule synthetic fulls on Thursday.

Veeam Backup & Replication will perform incremental backups Sunday through Wednesday as usual. On Thursday it will perform a synthetic full backup in the following way:

1. Veeam Backup & Replication will first perform incremental backup in the regular manner.
2. At the end of the backup job, the Veeam data mover service on the backup repository will build a new synthetic full backup from the backup files you already have on disk: the full backup created on Sunday and a chain of increments, Monday through Wednesday plus the new increment created on Thursday.
3. The Veeam data mover service will delete the increment created on Thursday.

As a result, you will have a backup chain consisting of the full backup created on Sunday, three increments created on Monday through Wednesday and a synthetic full backup created on Thursday.
Every next run of the backup job will create an incremental backup starting from the synthetic full backup until next Thursday. On the next Thursday, Veeam Backup & Replication will create a new synthetic full backup.

**Note:** Veeam Backup & Replication creates a synthetic full backup only once a day on which it is scheduled. If you run the backup job again on Thursday, Veeam Backup & Replication will perform incremental backups in the regular manner.

**Note:** You can schedule to perform a synthetic full backup from time to time for an incremental backup method. This is why incremental backup is more preferable for remote backups - with reverse incremental you’d have to perform an active full from time to time, which is a bigger load on the network.

**Transforming Incremental Backup Chains into Reversed Incremental Backup Chains**

If you select to create *synthetic full backups*, you can additionally choose to transform a previous forward incremental backup chain into a reverse incremental backup chain. In this case, Veeam Backup & Replication will transform the latest backup chain consisting of the `.vbk` and `.vib` files into reverse incremental backups – `.vrb` files.

The transform option lets you dramatically reduce the amount of space required to store backups. Instead of two full backups – the regular full backup and the synthetic full backup – you will have only one synthetic full backup on disk. Note, however, that the transform process takes more time than simply creating a periodic synthetic full backup.

**For example:** You have configured a backup job to perform daily forward incremental backups and scheduled synthetic fulls on Thursday.

Additionally, you have selected to transform the incremental backup chain into the reverse incremental backup sequence. The backup job starts on Sunday. In this case, Veeam Backup & Replication will perform backup in the following way:

1. On Sunday, Veeam Backup & Replication will create a full backup; Monday through Wednesday Veeam Backup & Replication will create incremental backups and add them to the
backup chain.
2. On Thursday, Veeam Backup & Replication will first create an incremental backup in the regular manner and add it to the backup chain.
3. After that, Veeam Backup & Replication will transform the incremental backup chain into the reverse incremental chain. As a result, you have a full backup “created” on Thursday and a set of reverse increments Sunday through Wednesday.
4. When you run the backup job next time, Veeam Backup & Replication will add a new incremental backup to the chain; the synthetic full backup will be used as a starting point.

Veeam Backup & Replication always transforms only the latest incremental backup chain. For example, you have a backup chain that consists of one full backup file and set of increments. In the middle of the chain, you create an active full backup. When you run a transformation task, Veeam Backup & Replication will transform the most recent active full backup plus increments that follow it. All backups that precede the active full backup will stay intact.

Note: The transform process is accounted for as an active backup repository task. Make sure you properly plan for use of backup repository resources when you schedule backup jobs.

Retention Policy for Deleted VMs

In some situations, after you configure and run backup jobs in Veeam Backup & Replication, you may want to change something in your virtual environment or even in your backup strategy. For example, you may remove some VMs from the virtual infrastructure or move them to some other location. You may also exclude some VMs from jobs that have already been running for some time.
By default, when you remove a VM protected by Veeam Backup & Replication from the virtual infrastructure or exclude it from a job, its backup files still remain on the backup repository. To avoid keeping redundant data on disk, you can select to control retention policy for deleted VMs.

The retention policy for deleted VMs is an option in the backup job settings. By default, this option is disabled. To use this option, you need to select the Remove deleted VMs data from backup after check box and specify the desired period of time for which the data must be retained on the backup repository.

With this option enabled, Veeam Backup & Replication will check the list of VMs included in the job when a job starts. If a VM is no longer available, for example, it was deleted or moved to another location, Veeam Backup & Replication will keep its data in the backup file for the specified period only. As soon as the specified retention period is over, data from the deleted VM will be removed from backup files on the backup repository. When Veeam Backup & Replication removes data for deleted VMs, it does not free up space in the backup repository. It marks the space as available to be overwritten, and this space is overwritten during subsequent job sessions or the backup file compact operation.

**Important!** Retention policy for deleted VMs is applied to reverse incremental backup chains, forever forward incremental backup chains and forward incremental backup chains for which synthetic full backups with subsequent transform is enabled.
5.1.3. Changed Block Tracking (CBT)

To perform incremental backups, Veeam Backup & Replication needs to know which data blocks have changed since the previous job run.

For VMware

For VMware VMs with hardware version 7 or later, Veeam Backup & Replication employs VMware vSphere Changed Block Tracking (CBT) – a native VMware feature. Instead of scanning VMFS, Veeam Backup & Replication queries CBT on vSphere through VADP and gets the list of blocks that have changed since the last run of this particular job. Using CBT increases the speed and efficiency of block-level incremental backups. CBT is enabled by default; if necessary, you can disable it in the settings of a specific backup job.

In some situations, Veeam Backup & Replication cannot leverage VMware vSphere CBT due to VMware limitations. Whenever Veeam Backup & Replication cannot leverage VMware vSphere CBT (for example, if your VMs run an earlier version of virtual hardware or CBT is disabled at the ESXi host level), the filtering is still performed. Instead of tracking changed blocks of data, Veeam Backup & Replication filters out unchanged data blocks. During backup, Veeam Backup & Replication consolidates virtual disk content, scans through the VM image and calculates a checksum for every data block. Checksums are stored as metadata to backup files next to VM data. When incremental backup is run, Veeam Backup & Replication opens all backup files in the chain of previous full and incremental backups, reads metadata from these files and compares it with checksums calculated for a VM in its current state. If a match is found (which means the block already exists in the backup), the corresponding block is filtered out. The time of processing using Veeam filtering mechanism will increase though compared to the time of processing when using vSphere CBT.

For Microsoft Hyper-V

To keep track of changing data blocks for Hyper-V, Veeam & Backup & Replication uses its proprietary Hyper-V changed block tracking mechanism (CBT).

The CBT mechanism is implemented as a file system filter driver. Veeam CBT driver is installed on every Hyper-V host that is added to the list of managed servers in Veeam Backup & Replication. The driver is activated when the host is first addressed by a job with enabled CBT.

The Veeam CBT driver keeps track of changing data blocks in virtual disks. Information on data blocks that have changed is registered in special .ctp files. When a job is run, Veeam Backup & Replication uses .ctp files to learn what blocks of data have changed since the last run of this particular job, and copies only changed data blocks from the disk image. The .ctp files are stored in the C:\ProgramData\Veeam\CtpStore folder on standalone Hyper-V hosts or on every node of the Hyper-V cluster.
5.1.4. Data size optimization

To decrease traffic and disk space required for storing backup files, Veeam Backup & Replication provides mechanisms of compression and deduplication.

Compression

*Compression* decreases the size of created backups but affects the duration of the backup procedure. Veeam Backup & Replication allows you to select one of the following compression levels:

<table>
<thead>
<tr>
<th>Level</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>When using storage devices with hardware compression and deduplication tools to store created backups</td>
</tr>
<tr>
<td>Dedupe-friendly</td>
<td>Optimized compression level for very low CPU usage. Recommended if you want to decrease the proxy load.</td>
</tr>
<tr>
<td>Optimal (default setting)</td>
<td>Recommended compression level that provides the best ratio between the size of the backup file and time of the backup procedure.</td>
</tr>
<tr>
<td>High</td>
<td>Provides additional 10% compression ratio over Optimal, but at the cost of about 10x higher CPU usage. May reduce overall backup performance.</td>
</tr>
<tr>
<td>Extreme</td>
<td>Provides the smallest size of the backup file but reduces backup performance. We recommend running backup proxies on computers with modern multi-core CPUs (6 cores recommended) if you intend to use the extreme compression.</td>
</tr>
</tbody>
</table>

Deduplication

You can apply *deduplication* when backing up multiple VMs that have similar data blocks (for example, if VMs were created from the same template) or great amount of free space on their logical disks. Veeam Backup & Replication does not store zero byte blocks or space that has been preallocated but not used. With deduplication, identical blocks or blocks of free space are eliminated, which decreases the size of the created backup file. Thus the disk space required for backups is reduced.

Depending on the type of storage you select as a backup target, Veeam Backup & Replication uses data blocks of different size to process VMs, which optimizes the size of a backup file and job performance. If you’re using storage devices with hardware compression and deduplication tools to store created backups, it is recommended to select "None" level.

You can choose one of the following storage optimization options:
<table>
<thead>
<tr>
<th>Option</th>
<th>When recommended</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local target (16 TB + backup size)</td>
<td>Recommended for backup jobs that can produce very large full backup files – larger than 16 TB</td>
<td>If you select to use small data blocks to deduplicate a large backup file, the backup file will be cut into a great number of data blocks. As a result, Veeam Backup &amp; Replication will produce a very large deduplication metadata table which can potentially overgrow memory and CPU resources of your backup repository. With this option selected, Veeam Backup &amp; Replication will use data blocks of 4 MB. Large data blocks produce a smaller metadata table that requires less memory and CPU resources to process. Note, however, that this storage optimization option will provide the lowest deduplication ratio and the largest size of incremental backup files.</td>
</tr>
<tr>
<td>Local target</td>
<td>Recommended for backup to SAN, DAS or local storage</td>
<td>The SAN identifies larger blocks of data (1024 KB) and therefore can process large amounts of data at a time. This option provides the fastest backup job performance but reduces the deduplication ratio, because with larger data blocks it is less likely to find identical blocks.</td>
</tr>
<tr>
<td>LAN target</td>
<td>Recommended for backup to NAS and onsite backup</td>
<td>This option provides a better deduplication ratio and reduces the size of a backup file because of reduced data block sizes (512 KB).</td>
</tr>
<tr>
<td>WAN target</td>
<td>Recommended if you are planning to use WAN for offsite backup</td>
<td>Veeam Backup &amp; Replication will use small data blocks (256 KB), which will result in the maximum deduplication ratio and the smallest size of backup files, allowing you to reduce the amount of traffic over the WAN connection.</td>
</tr>
</tbody>
</table>

**Note:** Changing the compression level and deduplication settings in an existing job will not have any effect on previously created backup files. It will affect only those backups that will be created after you set the new settings:

- New compression settings are applied at the next run of the job.
- New deduplication settings are applied only after a new active full backup is created

**Note:** Note: If you upgrade to Veeam Backup & Replication 9.0 from a previous product version, this option will be displayed as Local target (legacy 8MB block size) in the list and will still use block size of 8MB. 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.
Zeroing Out Dirty Blocks

When Veeam Backup & Replication performs backup or replication, it copies data of the VM image at the block level. The copied data contains all data of the VM, including data blocks that are marked as deleted on the VM guest OS. Such blocks are also known as dirty blocks or Deleted File Blocks.

**Important!** Veeam Backup & Replication can exclude deleted file blocks only on the VM guest OS with Microsoft NTFS.

This option is enabled by default and excluding deleted file blocks in backup or replica leads to:

- Reduced size of backup or replica.
- Possible increase in the job performance.

If you do not want to exclude deleted file blocks from backups or replicas, you can disable the Exclude deleted file blocks option in the backup or replication job settings.

With this option enabled, Veeam Backup & Replication performs the following operations during the job session:

1. Veeam Backup & Replication accesses the MFT file on the VM guest OS to identify deleted file blocks, and zeros out these blocks.
2. Veeam Backup & Replication processes and transports data blocks of the VM image in the following manner:
   - If a data block of the VM image contains only the deleted file blocks, Veeam Backup & Replication does not read this data block from the source volume.
   - If a data block of the VM image contains zeroed out blocks and other data, Veeam Backup & Replication copies this block to the target. Due to data compression, data blocks that are marked as deleted are compressed, and the size of the resulting backup or replica file reduces.

**Note:** If you enable or disable the Exclude deleted file blocks setting for the existing job, Veeam Backup & Replication will apply the new setting from the next job session.

5.1.5. Data Encryption

Data security is an important part of the backup strategy. You must protect your information from
Unauthorized access, especially if you back up sensitive VM data to offsite locations or archive it to tape. To keep your data safe, you can use data encryption. The following types of encryption are used in Veeam Backup & Replication:

<table>
<thead>
<tr>
<th>At source</th>
<th>In flight</th>
<th>At rest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who does the encryption</td>
<td>Data Mover Service at the source proxy</td>
<td>Data Mover Service at the source proxy</td>
</tr>
<tr>
<td>Process</td>
<td>Reads the data and encrypts the files that are sent to the repository, which writes the files as it receives them (already encrypted)</td>
<td>Source Data Mover Service encrypts before sending, target decrypts when receiving</td>
</tr>
</tbody>
</table>

**Note:** In Veeam Backup & Replication, encryption works at the job level and can be enabled for the following types of jobs: backup job, backup copy job, tape jobs (backup to tape job and file to tape job), and VeeamZIP.

Veeam Backup & Replication uses the following industry-standard data encryption algorithms:

- To encrypt data blocks in backup files and files archived to tape, Veeam Backup & Replication uses the 256-bit AES with a 256-bit key length in the CBC-mode.
- To generate a key based on a password, Veeam Backup & Replication uses the Password-Based Key Derivation Function, PKCS #5 version 2.0. Veeam Backup & Replication uses 10,000 HMAC-SHA1 iterations and a 512-bit salt.
- For Microsoft Windows-based repositories, Veeam Backup & Replication uses the Windows Crypto API, complying with the Federal Information Processing Standards (FIPS 140).
- For Linux-based repositories, Veeam Backup & Replication uses a statically linked OpenSSL encryption library, without the FIPS 140 support.

To encrypt data in backups and files, Veeam Backup & Replication employs a symmetric key encryption algorithm. The symmetric, or single-key encryption algorithm, uses a single, common secret key to encrypt and decrypt data. Before data is sent to target side, it is encoded with a secret key. To restore encrypted data, you must have the same secret key. Users who do not have the secret key cannot decrypt data and get access to it.

When you enable encryption for a job, you must define a password to protect data processed by this job, and define a hint for the password. The password and the hint are saved in the job settings. Based on this password, Veeam Backup & Replication generates a user key.

During the encryption process, Veeam Backup & Replication saves a hint for the password to the encrypted file. When you decrypt a file, Veeam Backup & Replication displays a hint for the password that you must provide. After you enter the password, Veeam Backup & Replication derives a user key.
from the password and uses it to unlock the storage key for the encrypted file.

According to the security best practices, you must change passwords for encrypted jobs regularly. When you change a password for the job, Veeam Backup & Replication creates a new user key and uses it to encrypt new restore points.

**Important!** You must always remember passwords set for jobs or save these passwords in a safe place. If you lose or forget the password, you can restore data from a backup file by issuing a request to Veeam Backup Enterprise Manager.

### 5.1.6. Transaction Consistency

When you perform backups of a running VM, it is necessary to quiesce (or ‘freeze’) it to bring the file system and application data to a consistent state suitable for backup. Backing up a VM without quiescence produces a crash-consistent backup. Restoring a crash-consistent backup is essentially equivalent to rebooting a server after a hard reset. In contrast to it, restoring transactionally consistent backups (produced with VM data quiesced) ensures the safety of data for applications running on VMs.

**VMware vSphere**

To create transactionally consistent backup images of VMware vSphere VMs, Veeam Backup & Replication provides two options: application-aware processing (utilizing Windows VSS framework) and VMware Tools quiescence, leveraging ESXi snapshot capabilities.

**Important!** VMware Tools quiescence does not support log truncation recommended for highly-transactional applications like Exchange Server or SQL Server. That is why application-aware processing utilizing Windows VSS as the recommended option to use for backup and replication of Exchange Server, Active Directory and other VSS-aware applications.

**Persistent Snapshots**

As it was mentioned earlier, during application-aware processing, Veeam Backup & Replication utilizes a VSS writer for a corresponding application to freeze application data and bring it to a consistent state suitable for backup.

According to Microsoft limitations, the application freeze cannot take longer than 60 seconds (20 seconds for Microsoft Exchange). If the VSS writer does not manage to freeze application data within this period of time, a VSS processing timeout occurs, and Veeam Backup & Replication fails to create a transactionally consistent backup for the VM.

**For example:** The VSS processing timeout is a common problem for highly transactional applications such as Microsoft Exchange.
To overcome this limitation, Veeam Backup & Replication utilizes the Microsoft VSS persistent snapshots technology for backup of Microsoft Exchange VMs. If Microsoft Exchange fails to be frozen within the allowed period of time, Veeam Backup & Replication automatically fails over to the persistent snapshot mechanism. The backup operation is performed in the following way:

1. Veeam Backup & Replication triggers the Microsoft VSS framework to prepare Microsoft Exchange inside the VM for backup.
2. The Microsoft VSS writer attempts to quiesce Microsoft Exchange. If the Microsoft VSS writer fails to do it within the allowed period of time, the control is passed to the native Veeam VSS writer. The Veeam VSS writer holds the freeze operation for the necessary amount of time.
3. After Microsoft Exchange data is brought to a consistent state, the control is passed to the Microsoft VSS provider. The Microsoft VSS framework creates a persistent VSS snapshot for VM disks except system VM disks.
4. The rest of the backup operation is performed in a regular way.
5. After the backup operation is complete, Veeam Backup & Replication triggers Microsoft VSS to remove a persistent VSS snapshot on the production VM. The persistent VSS snapshot holding consistent application data still remains inside the created VM backup.

During full VM restore, Veeam Backup & Replication recovers data from the VM backup and reverts VM disks to the persistent VSS snapshot inside the backup. As a result, the Microsoft Exchange VM is restored from the backup in a consistent state without any data loss.

**Snapshot Hunter**

The *Snapshot Hunter* (available for VMware vSphere) is a Veeam technology used to detect and remove orphaned snapshots that may remain after backup or replication job sessions. The Snapshot Hunter addresses the problem of “phantom” snapshots. Under some circumstances, VMware vSphere can report a successful removal of a snapshot but the snapshot actually remains on the datastore. Phantom snapshots can take substantial space on the datastore or impact VM performance. They can even cause the production VMs to stop if the datastore runs out of free space.

To solve the problem of phantom snapshots, Veeam Backup & Replication starts the Snapshot Hunter during each backup or replication job session. The Snapshot Hunter looks for snapshot files not registered in vSphere. If there are no orphaned files, the Snapshot Hunter stops. If orphaned snapshot files are detected, the Snapshot Hunter removes them in the background mode.

The Snapshot Hunter runs in jobs that use VMware VM snapshots:

- Backup jobs: regular backup, backup from storage snapshot, vCloud Director backup
- Replication jobs (the source VM snapshot): regular replication, replication from storage snapshot
- VeeamZIP

**Guest Interaction Proxy**

To interact with the VM guest OS during the backup or replication job, Veeam Backup & Replication needs to deploy a runtime process in each VM. Guest OS interaction is performed if you enable the following options:
• Application-aware processing
• Guest file system indexing
• Transaction logs processing

Previously, the runtime process was deployed by the backup server. This could potentially cause the following problems:

• Increased load on the backup server.
• Decrease in the job performance if the connection between two sites was slow.
• Inability to process VMs to which the backup server had no network connection.

Since v9 the task of deploying the runtime process in a Microsoft Windows VM is performed by the guest interaction proxy. The guest interaction proxy is a backup infrastructure component that sits between the backup server and processed VM. The guest interaction proxy deploys the runtime process in the VM and sends commands from the backup server to the VM.

Note: Veeam Backup & Replication does not deploy persistent agents inside VMs. Instead, it uses a runtime coordination process on every VM that is started once the backup operation is launched, and removed as soon as it is finished. This helps avoid agent-related drawbacks such as pre-installing, troubleshooting and updating. Runtime coordination process is used for both Linux and Windows VMs.

The guest interaction proxy allows you to communicate with the guest OS even if the backup server and processed VM run in different networks. As the task of runtime process deployment is assigned to the guest interaction proxy, the backup server only has to coordinate job activities.

During the job session with Microsoft Windows VM guest OS interaction, Veeam Backup & Replication performs the following operations:

1. The backup server defines the machine that will perform the guest interaction proxy role.
2. The guest interaction proxy accesses the Microsoft Windows VM and deploys a runtime process responsible for guest OS interaction.
3. The VM processing proceeds with the usual scenario.
4. Once the job session completes, the backup server instructs the guest interaction proxy to delete the runtime process from the VM.

In case network connection breaks when the job is running, Veeam Backup & Replication will make attempts to reconnect.
Important! The guest interaction proxy deploys the runtime process only in a Microsoft Windows VM. In a VM with another guest OS, the runtime process will be deployed by the backup server.

To perform the role of guest interaction proxy, the machine must meet the following requirements:

- It must be a Microsoft Windows machine (physical or virtual).
- You must add it to the Veeam Backup & Replication console as a managed server.
- It must have a LAN or VIX connection to the VM that will be backed up or replicated.

Important! The guest interaction proxy functionality is available in the Enterprise and Enterprise Plus Editions of Veeam Backup & Replication.

Guest Interaction Proxy Selection

When you add a Microsoft Windows machine to the backup infrastructure, Veeam Backup & Replication deploys the Data Mover Service on it. The Data Mover Service includes the components responsible for runtime process deployment during guest OS interaction.

To assign a guest interaction proxy for the job, you must select a Microsoft Windows machine that will perform the role of the guest interaction proxy at the Guest Processing step of the backup or replication job wizard. You can assign the guest interaction proxy manually, or let Veeam Backup & Replication do it automatically. Veeam Backup & Replication uses the following priority rules to select the guest interaction proxy:

1. A machine in the same network as the protected VM that does not perform the backup server role.
2. A machine in the same network as the protected VM that performs the backup server role.
3. A machine in another network that does not perform the backup server role.
4. A machine in another network that performs the backup server role.

If Veeam Backup & Replication finds several available machines of equal priority, it selects the less loaded machine. The load is defined by the number of tasks that the machine already performs.

If the guest interaction proxy fails to connect to a Microsoft Windows VM, the guest interaction proxy
Module 5: Protect

Veeam Certified Engineer v9 . Textbook

will not be able to access the VM and deploy a runtime process in it. In this case, the backup server will take over the role of guest interaction proxy and deploy the runtime process in the VM.

Microsoft Hyper-V

To create a transactionally consistent backup of Hyper-V VMs, Veeam Backup & Replication uses the VSS framework. The Hyper-V VSS writer coordinates its operations with the Hyper-V Integration Services running inside the backed up VM to quiesce VM operations and create a stable shadow copy of the volume. This approach is also known as Hyper-V online backup.

Veeam Backup & Replication performs host-based backups of Hyper-V VMs. In contrast to traditional backup tools that deploy an agent inside the VM guest OS and back up from within the VM, Veeam Backup & Replication uses a Veeam data mover service running on the Hyper-V host or a Veeam data mover service running on the off-host backup proxy. A VM is treated as an object from the perspective of the Hyper-V host – Veeam Backup & Replication captures the VM configuration and state along with VM VHD/VHDXs and creates an image-based backup of the VM.

To perform backups of Hyper-V VMs, Veeam Backup & Replication leverages the VSS framework and Hyper-V VSS components. It acts as a VSS requestor and communicates with the VSS framework. Veeam Backup & Replication obtains from VSS information about available VSS components, prescribes what components should be used, identifies volumes where files of the necessary VMs are located, and triggers the VSS coordinator to create volume snapshots.

Before a snapshot of a volume is created, VMs on the volume must be prepared for the snapshot – that is, data in the VM must be in a state suitable for backup. Veeam Backup & Replication uses three methods to quiesce Hyper-V VMs on the volume: online backup, offline backup and crash-consistent backup.

Whenever possible, Hyper-V VSS uses online backups to quiesce VMs. If online backups cannot be performed, one of the other two methods is used to prepare a VM for a volume snapshot. By default, Veeam Backup & Replication fails over to the crash-consistent backup if online backup is not possible. However, you can configure your backup jobs to use the offline backup method instead.

Pre-Freeze and Post-Thaw Scripts

If you plan to back up VMs running applications that do not support VSS, you can instruct Veeam Backup & Replication to run custom pre-freeze and post-thaw scripts for these VMs. Pre-freeze scripts quiesce the VM file system and application data to bring the VM to a consistent state before Veeam Backup & Replication triggers a VMware VM snapshot. After the VM snapshot is committed, post-thaw scripts bring the VM and applications to their initial state.

To run pre-freeze and post-thaw scripts, you must create them beforehand and specify paths to them in the job settings. When the job starts, Veeam Backup & Replication will upload these scripts to the VM guest OS and execute them. Scripts for Microsoft Windows VMs are uploaded over the network or VIX, if Veeam Backup & Replication fails to connect to the VM guest OS over the network. Scripts for Linux VMs are uploaded over SSH.
Truncation of transaction logs

If you are performing a backup of database systems that use transaction logs, for example, Microsoft Exchange or Microsoft SQL or Oracle you can select to truncate transaction logs so that logs do not overflow the storage space. Veeam Backup & Replication provides the following options of transaction logs handling:

<table>
<thead>
<tr>
<th>What</th>
<th>Result</th>
<th>When</th>
</tr>
</thead>
<tbody>
<tr>
<td>Truncate transaction logs upon successful backup.</td>
<td>If a backup job completes successfully, Veeam Backup &amp; Replication produces a VM backup file and truncates transaction logs on the production database system.</td>
<td>You can recover a database to the point in time when the backup file was created. For a non-SQL VM and when it’s not required to be able to restore to any point of time between backups.</td>
</tr>
<tr>
<td>Do not truncate transaction logs</td>
<td>Veeam Backup &amp; Replication produces a backup file and does not trigger transaction log truncation.</td>
<td>You can use transaction logs to restore the VM to any point in time between backups. If together with Veeam Backup &amp; Replication, you use another backup tool to maintain consistency of the database state.</td>
</tr>
<tr>
<td>Back up transaction logs with Veeam Backup &amp; Replication (for Oracle and Microsoft SQL only)</td>
<td>Veeam Backup &amp; Replication creates a backup of a VM and additionally ships transaction logs and saves them to the backup repository next to the VM backup.</td>
<td>You can use transaction logs to restore the VM to any point in time between backups. When you are backing up a Microsoft SQL or Oracle VM with no other backup tool and you want to be able to restore to any point of time between backups.</td>
</tr>
</tbody>
</table>

**Important!** To be able to back up the SQL transaction logs make sure that Full or Bulk-logged recovery model is enabled for that server and no other backup tool truncates the SQL server logs files. To be able to back up the Oracle transaction logs make sure that ARCHIVELOG mode is enabled for the Oracle database.

5.1.7. Scheduling

When you create a job, you can simply start it manually whenever it is necessary. However, as the number of backup and replication jobs increases, it may become hard to keep track of them. Veeam Backup & Replication provides a number of job scheduling options which enables you to set up automatic startup schedules for jobs, automatic retries for failed jobs, and a backup window to limit...
the time when jobs are performed.

**Automatic Startup Schedule**

To perform a job on a regular basis, you can schedule it to start automatically. The Veeam Backup Service running on the backup server continuously checks configuration settings of jobs and starts them in accordance with their schedules.

Jobs can also be scheduled to run continuously, that is, in a non-stop manner. Technically, a job running continuously is launched as soon as previous job processing is complete. With Veeam Backup & Replication, you can run backup jobs and replication jobs continuously or with an interval as low as one minute to implement near-continuous data protection (near-CDP) for the most critical applications and workloads.

Even if you have scheduling set up for a job, you can still start it manually at any moment.

**Note:** For a scheduler, periodic jobs have priority over regular jobs, e.g. if you have a monthly and a daily job scheduled to run at the same time, in case there are only enough resources to launch one of them, the monthly job will be started.

**Automatic Job Retry**

Veeam Backup & Replication can be configured to retry a job for a certain number of times if the initial job pass fails. By default, Veeam Backup & Replication automatically retries a failed job three times within one job session. If necessary, however, you can change the number of retries in the job settings.

Veeam Backup & Replication retries a job only if the previous job session has failed and one or several VMs in the job have not been processed. Veeam Backup & Replication does not perform a retry if a job session has finished with the *Success* or *Warning* status. During the job retry, Veeam Backup & Replication processes only those VMs that have failed.

Veeam Backup & Replication creates only one backup file within one job session. That is, if a job includes several VMs and some of them fail to be processed during the first job pass, Veeam Backup & Replication will create a backup file containing data for those VMs that have been successfully processed. At the job retry, Veeam Backup & Replication will attempt to process failed VMs; in the case of success, Veeam Backup & Replication will write data of the processed VMs to the backup file that was created at the previous job pass.

**Important!** Veeam Backup & Replication does not perform automatic retry for jobs started manually.

In some situations, Veeam Backup & Replication may fail to process VMs during all job retries. In this case, failed VMs will be processed within the next job session; its data will be written to the backup file created within the current job session.
Backup Window

To prevent a backup or replication job from overlapping with production hours and ensure it does not provide unwanted overhead on your virtual environment, you can limit all jobs to a specific backup window. A backup window is a period of time on week days when backup and replication jobs are permitted to run. If the job exceeds the allowed window, it will be automatically terminated.

Stopping Job Session

You can stop the job session:

- With the Stop option – terminates the job session before Veeam Backup & Replication creates the restore points for the VMs that are currently processed.
- With the Stop after current VM option – terminates the job session after creating restore points for the VMs that are currently processed.

The VMs that Veeam Backup & Replication succeeded to process will have new restore points.

5.2. Creating Restore Points with VeeamZIP and Quick Backup

If you need to quickly create a restore point for selected VM, VeeamZIP (full backup) or Quick Backup (incremental backup) can be used.

5.2.1. VeeamZIP

With Veeam Backup & Replication, you can quickly perform backups of one or several VMs with VeeamZIP. You can also VeeamZIP files for VMware vSphere and Hyper-V VMs with Veeam Backup Free Edition.

VeeamZIP is similar to full VM backup. The VeeamZIP job always produces a full backup file (.vbk) that acts as an independent restore point. You can store the backup file to a backup repository, to a local folder on the Veeam backup server, or to a network share.

When you perform backups with VeeamZIP, you do not have to configure a backup job and schedule it, only minimum setting are required. Instead, you can start the backup process for selected VMs immediately. Veeam Backup Free Edition offers the following advanced options for VeeamZIP files creation:

- **Data encryption.** To create an encrypted VeeamZIP file, you must enable the encryption option and specify a password in VeeamZIP task options.
- **Retention settings.** You can specify retention settings for the created VeeamZIP file: define if the file must remain on the target storage or must be deleted with time (autoretention).
- **Data compression** – similar to the levels used for regular backup jobs.
- **VM guest OS quiescence.** VeeamZIP uses VMware Tools quiescence for VMware VMs and native Hyper-V quiescing mechanisms for Hyper-V VMs to capture VM data. VeeamZIP

---

Veeam Certified Engineer v9. Textbook
quiesces, or freezes, a running VM to bring its file system and application data to a consistent state suitable for backup. Restoring a transactionally consistent VeeamZIP file ensures successful recovery of VM applications without any data loss.

The VeeamZIP was in versions prior to v9 not registered in the database used by Veeam Backup & Replication and the backup file produced with it is not available under the Backups node in the Backup & Replication view. However since v9, VeeamZIP backups are now registered in the configuration database and shown under Backups > Disk (VeeamZIP) node to more easily track them. You can easily see the location using the Location column, showing the corresponding backup’s location, such as local path, backup repository or storage snapshot.

5.2.2. Quick Backup

Quick Backup lets you perform on-demand incremental backups for VMs. You can use Quick Backup if you want to produce an additional restore point for one or more VMs in a backup job and do not want to configure a new job or modify the existing one. Quick Backup can be run for both incremental and reverse incremental backup chains.

**Note:** Quick Backup is not supported for separate vCloud Director VMs as vCD job process vApps as integral units.

Quick Backup is an incremental backup task – and similarly, Quick Backup can only be run for VMs that have been successfully backed up at least once and has a full restore point.

To perform Quick Backup, Veeam Backup & Replication uses an existing backup job. When you start a Quick Backup task for a VM, Veeam Backup & Replication verifies that a backup job processing this VM exists on the Veeam backup server. If such job is detected, Veeam Backup & Replication triggers a job and creates an incremental restore point for the VM. If a backup job for the VM does not exist, Quick Backup is terminated.

**Note:** If many jobs exist for the same VM, the one with the most recent restore point at the repository will be selected.
When you perform Quick Backup, Veeam Backup & Replication creates a partial incremental restore point, which contains data only for a specific VM. A partial restore point is not regarded as a full-fledged restore point in the backup chain. From the retention policy perspective, a partial restore point is grouped with a regular restore point following it. When Veeam Backup & Replication needs to delete a partial restore point by retention, it waits for the next regular restore point to expire, and deletes two restore points at once.

5.3. Backup Copy

To let you adopt the 3-2-1 rule: you must have three copies of your data on two different types of media, and at least one copy of that data offsite, Veeam Backup & Replication offers backup copying capabilities. Backup copying allows you to create several instances of the same backup file in different locations, whether onsite or offsite. Copied backup files have the same format as those created by backup jobs and you can use any data recovery option for them.

5.3.1. 3-2-1 rule

The main purpose of backup is to protect your data against disasters and VM failures. However, having one copy of a backup file does not provide the necessary level of safety. A backup file may get corrupted or lost, leaving you with not data to restore at all.

Backup experts claim that to build a successful data protection and disaster recovery plan, you must follow the 3-2-1 rule:

3: You must have three copies of a data in different locations.
2: You must use two different types of media to store copies of a backup file, for example, disk storage and tape.
1: You must keep at least one copy of a backup file offsite, for example, in the cloud or in the remote site.
Thus, according to the first statement of the 3-2-1 backup strategy, you must have 2 different copies of a backup file in different locations, plus your production VM data. In case a disaster strikes, multiple backup copies increase your chances in data restore.

### 5.3.2. Backup Copy Job

To let you adopt the 3-2-1 backup strategy, Veeam Backup & Replication offers backup copying capabilities. Backup copying allows you to create several instances of the same backup file in different locations, whether onsite or offsite. Copied backup files have the same format as those created by backup jobs and you can use any data recovery option for them.

**Backup copy** is a job-driven process. Veeam Backup & Replication fully automates the backup copying process and lets you specify retention policy settings to maintain the desired number of restore points for copied backups.

Backup data is copied per VM at the block level. When the backup copying process starts, Veeam Backup & Replication accesses VM backup files in the source backup repository, retrieves data blocks for a specific VM from the backup file, copies them to the target backup repository, and composes copied blocks into a backup file in the target backup repository. Therefore, the backup copying process does not affect virtual infrastructure resources, require an additional snapshot of a VM, or produce any load on VMs whose backups are copied.

In the target backup repository, the backup copy job creates a chain of restore points using the incremental backup method. The target backup repository always contains only one active incremental backup chain. Restore points in the chain are rotated according to the specified retention policy.

The backup chain on the target backup repository is created in the following manner:

1. The first synchronization interval of the backup copy job always produces a full backup file. The full backup file is created in the following way:
   a. From the backup chain on the source backup repository, Veeam Backup & Replication copies data blocks that are necessary to build a full backup of a VM as of the most recent state. Data blocks can be copied from one or several backup files in the chain, the retention policy for a backup copy job can be different than the retention period of its related backup job, or backup jobs. If the backup chain on the source backup repository was created using the reverse incremental backup method, Veeam Backup & Replication simply copies data blocks of the latest full backup.

If the backup chain on the source backup repository was created using the forward incremental backup method, Veeam Backup & Replication copies data blocks from the
first full backup and a set of incremental backups to form a full backup of a VM as of the most recent state.

b. On the target backup repository, Veeam Backup & Replication writes all copied data blocks to the same full backup file.

2. At every synchronization interval, when a new restore point appears on the source backup repository, Veeam Backup & Replication copies incremental changes from this most recent restore point and transfers them to the target backup repository. On the target backup repository, Veeam Backup & Replication writes the copied data blocks to the incremental backup file.

The backup copy job can be created for one VM or several VMs, which can be backed up by one backup job or several backup jobs. If the backup copy job is created for several VMs, you can define the order in which the VMs should be processed. Veeam Backup & Replication will sequentially process VMs one by one in the defined order. If any VM cannot be processed for some reason, for example, when a new restore point for this VM is not yet available, Veeam Backup & Replication will pass to the next VM. Once this VM is processed, Veeam Backup & Replication will attempt to copy the unprocessed VM once again.

Even if a backup copy job processes several VMs, it creates one backup file on the target backup repository and stores the data for all VMs processed by the job.

**Note:** With v9, backup copy jobs will now process multiple VMs in parallel, just like primary backup jobs. This improves the backup copy and retention processing performance due to removing "dead time" between each VM, and will further speed up processing when per-VM backup file chains are enabled on the target backup repository.

To minimize the amount of traffic going over the network, Veeam Backup & Replication uses data compression and deduplication technologies. And if you plan to copy VM restore points over the WAN and slow connections, you can also use backup mapping. Backup mapping can only be used if you already have a full backup file for the VM you plan to process with the backup copy job on the target
backup repository. In this case, you can point the backup copy job to this backup file. This full backup file will be used as a “seed” for the backup copy job and you will need to copy only small incremental changes over the network.

When changing backup storage settings such as encryption or block size, v9 offers a new ability to trigger a manual Active Full in Backup Copy Jobs. This is also useful in troubleshooting scenarios.

**Note:** Veeam Backup & Replication does not copy restore points if the block size of the restore point on the source backup repository differs from the block size of restore points on the target backup repository. The data block size for restore points on the target backup repository is set at the first synchronization cycle of the backup copy job. This size is taken from the corresponding settings of the primary backup job — the backup job that creates the backup chain on the source backup repository. If after the first synchronization cycle you add to the backup copy job new sources that use a different data block size, Veeam Backup & Replication will detect such restore points and display the **Restore point is located in backup file with different block size** message.

### GFS retention policy

Sometimes, simple backup retention policy is not enough. You cannot store an unlimited number of restore points on the target backup repository forever because it is not rational and is resource consuming. If you want to retain VM data for longer periods of time, it is recommended that you use the GFS retention policy scheme.

The **GFS**, or **Grandfather-Father-Son retention policy** is a backup rotation scheme intended for long-term archiving. It lets you keep backups of VMs for an entire year using minimum amount of storage space. GFS is a tiered retention policy scheme. It uses a number of cycles to maintain backups at different tiers:

- Regular backup cycle performed according to the specified synchronization interval
- Weekly backup cycle
- Monthly backup cycle
- Quarterly backup cycle
- Yearly backup cycle

Weekly/monthly/quarterly/yearly backups are always full backups containing data of the whole VM image as of specific date. When you define retention policy settings for a weekly/monthly/quarterly/yearly backup cycle, you specify how many weekly backups you want to retain per month, monthly per year, etc. and define the day on which a full backup must be created.

These backups are not created in a separate task. Veeam Backup & Replication re-uses a full backup created in the regular backup cycle and propagates it to the required tier. After the retention is met and the .vbk “passes” the scheduled date, the full backup created in a backup copy job for each GFS retention point will be deleted.

Additionally, we can improve local backup copy performance and reduce the load on deduplication appliances with the new option for active full Grandfather-Father-Son (GFS) backups in Backup Copy jobs. The data rehydration requirement is eliminated on the deduplication appliance with this option.
enabled – and instead, the entire restore point is copied over from source backup files. This effectively turns the Backup Copy workload from random to streaming, really broadening our support for the deduplication appliance that can serve as the target for Backup Copy jobs to any storage at all.

**Maintenance Settings**

To specify settings for backup files stored in the target backup repository:

1. At the Target step of the wizard, click Advanced.
2. If you want to periodically perform a health check of the most recent restore point in the backup chain, select the Perform backup files health check check box and specify the time schedule for the health check. By default, the health check is performed on the last Saturday of every month. An automatic health check allows you to avoid a situation when a restore point gets corrupted, making all further increments corrupted, too. If Veeam Backup & Replication detects corrupted data blocks in the restore point during the health check, it will transfer these data blocks to the target backup repository during the next synchronization interval and store them in the newly copied restore point. For more information, see Health Check for Copied Backups.
3. Select the Remove deleted VMs data after <N> days check box and specify the retention policy settings for deleted VMs. If a VM is no longer processed by a job for some reason (for example, it was excluded from the job, removed from the virtual infrastructure and so on), its data may still be kept in backups on the target backup repository. To avoid this situation, you can define the number of days for which data for deleted VMs must be retained. By default, the deleted VM retention period is 30 days. Do not set the deleted VM retention period to 1 day or a similar short interval. In the opposite case, the backup copy job may work not as expected and remove VM data that you still require.

**Important!** When Veeam Backup & Replication removes data for deleted VMs, it does not free up space in the backup repository. It marks the space as available to be overwritten, and this space is overwritten during subsequent job sessions or the backup file compact operation.

4. To periodically compact a full backup, select the Defragment and compact full backup file check box and specify the schedule for the compacting operation. By default, the compact operation is performed on the last Sunday of every month. The compact option can be enabled only if you have not specified the GFS settings. During the compacting operation, Veeam Backup & Replication creates a new empty VBK file and copies to it all data blocks from the full backup file. As a result, the full backup file gets defragmented, its size reduces and the speed of writing and reading to/from the file increases.

**Note:** The Remove deleted VMs data after <N> days option applies only to regular backup chains. Veeam Backup & Replication does not remove data for deleted VMs from weekly, monthly, quarterly and yearly backups.

**Compact of Full Backup File**

The backup copy job constantly transforms the full backup file in the backup chain to meet retention
policy settings. The transformation process, however, has a side effect. In the long run, the full backup file grows large and gets badly fragmented. The file data occurs to be written to non-contiguous clusters on disk, and operations of reading and writing data from and to the backup file slow down.

To resolve the fragmentation problem, you can instruct Veeam Backup & Replication to compact the full backup file periodically. During the file compact operation, Veeam Backup & Replication creates a new empty VBK file and copies to it all data blocks from the full backup file. As a result, the full backup file gets defragmented, its size reduces and the speed of reading and writing from and to the file increases.

To compact the full backup file periodically, you must enable the Defragment and compact full backup file option in the backup copy job settings and define the compact operation schedule. By default, the compact operation is performed on the last Saturday of every month. You can change the compact operation schedule and instruct Veeam Backup & Replication to perform it weekly or monthly on specific days.

The full backup file compact has the following limitations:

- The Defragment and compact full backup file option can be enabled only for the simple retention policy scheme.
- The target backup repository must have enough space to store a file of the full backup size. During the compact process, Veeam Backup & Replication creates an auxiliary VBK file that exists in the backup repository until the end of the compact operation.
- If the full backup file contains data for a VM that has only one restore point and this restore point is older than 2 days, during the compact operation Veeam Backup & Replication will not copy data for such VM to the newly created full backup file. Veeam Backup & Replication will extract data for this VM from the full backup file and write this data to a separate backup file. The file will be displayed under the Backups > Disk (imported) node in the Backup & Replication view. This mechanism helps remove data for VMs that are no longer processed with the backup copy job from the full backup file and reduce the size of the full backup file.
  - The mechanism works if the following conditions are met:
    - The Remove deleted VMs data option is not enabled in the backup copy job settings.
    - The Use per-VM backup files option is not enabled in the settings of the target backup repository.

Active Full Backup Copies

You can manually create an ad-hoc full backup for the backup copy job — active full backup copy, and add it to the backup chain on the target backup repository. To do this, you can use the Active Full button on the ribbon or the Active Full command from the shortcut menu.

Active full backup copy can be helpful if you want to change backup copy job settings, for example, define a new encryption password. Veeam Backup & Replication will apply new settings starting from this full backup.

Veeam Backup & Replication treats archive full backups created with the active full backup method as regular backups and applies regular retention policy rules to maintain the necessary number of restore points.
If you create active full backups for backup copy jobs, Veeam Backup & Replication handles restore points in the previous backup chain in the following way:

1. During the copy interval when an active full backup is created, Veeam Backup & Replication does not merge restore points in the previous backup chain.
2. During the next copy interval, Veeam Backup & Replication merges 2 restore points in the previous backup chain at a time.
3. At subsequent copy intervals, Veeam Backup & Replication merges 1 point in the previous backup chain at a time.

If you additionally use the GFS retention scheme for the backup copy job, Veeam Backup & Replication merges restore points in the previous backup chain up to the restore point that must be marked as an archive backup. The archive restore point is then set aside by standard backup copy rules.

5.3.3. WAN Acceleration

Offsite backup and replication always involves moving large volumes of data between remote sites. The most common problems that backup administrators encounter during are the following:

- Insufficient network bandwidth to support VM data traffic
- Transmission of redundant data

To solve these problems, Veeam Backup & Replication offers the WAN acceleration technology that helps optimize data transfer over the WAN. To enable WAN acceleration and data deduplication technologies, you must deploy a pair of WAN accelerators in your backup infrastructure: on the source site and one on the target site.

The **WAN acceleration** technology is specific for remote jobs: backup copy jobs and replication jobs. Being a built-in feature, Veeam’s WAN acceleration does not add complexity to the backup infrastructure and does not require agents. On each WAN accelerator Veeam Backup & Replication, creates the VeeamWAN folder containing the following data:

<table>
<thead>
<tr>
<th>Source WAN</th>
<th>Target WAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Files with digests required for global deduplication.</td>
<td>Global cache data.</td>
</tr>
</tbody>
</table>

To deploy a WAN accelerator, you should assign this role to a Microsoft Windows machine added to the list of managed servers in Veeam Backup & Replication. The Microsoft Windows machine must meet the following requirements:

1. You can use either physical or virtual Microsoft Windows machine as a WAN accelerator. The role can be assigned to backup proxies and backup repositories existing in your backup infrastructure as well.
2. You can use only 64-bit Microsoft Windows machines as WAN accelerators. 32-bit versions of Microsoft Windows are not supported.
**Note:** WAN acceleration operations are resource intensive. When creating a WAN accelerator, allocate appropriate CPU and RAM resources to the Microsoft Windows machine that you plan to use. It is recommended to assign this role to machines with 8 GB RAM and more. Otherwise the WAN acceleration process may fail.

**Note:** When you run a first session of a remote job, the global cache is empty, and the whole amount of VM data needs to be transferred over the WAN. It is recommended that you populate the global cache before you start a remote job for the first time. You can manually pre-populate the global cache to avoid the situation when the cache remains empty. As a result, by the time a remote job starts, the global cache will contain data blocks that can be used for data deduplication.

### 5.4. Replication

With Veeam, you can not only back up, but also replicate your VMs. When you replicate a VM, Veeam Backup & Replication creates an exact copy of a production VM in the native format on a spare host and maintains this copy in sync with the original VM. If the primary VM goes down for some reason, you can immediately fail over to the VM replica, and restore critical services with minimum downtime.

#### 5.4.1. Replication Overview
Just like backup, replication is a job-driven process. During the first run of a replication job, Veeam Backup & Replication copies the whole VM image and registers a replicated VM on the target host. During subsequent runs of a job, Veeam Backup & Replication copies only incremental changes, and creates restore points for a VM replica – so you can recover your VM to the necessary state. Every restore point is in fact a 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 a full VM replica. The number of restore points in the chain depends on your retention policy settings.

To provide extremely fast incremental replication for VMware, Veeam Backup & Replication leverages the vSphere functionality – ESXi Changed Block Tracking (or CBT). With CBT, you can replicate much faster as the replication job can be set to run Continuously. So you get near-CDP at only a fraction of the cost of traditional CDP solutions.

As for Hyper-V, Veeam & Backup & Replication uses its proprietary Hyper-V changed block tracking mechanism (CBT). The CBT mechanism is implemented as a file system filter driver. Veeam CBT driver is installed on every Hyper-V host added to the list of managed servers in Veeam Backup & Replication. The driver is activated when the host is first addressed by a job with enabled CBT. The Veeam CBT driver keeps track of changing data blocks in virtual disks. Information on data blocks that have changed is registered in special .ctp files. When a job is run, Veeam Backup & Replication uses .ctp files to learn what blocks of data have changed since the last run of this particular job, and copies only changed data blocks from the disk image.

When replicating, you can select a path for VM data transfer:

- Direct: To transport data directly from the backup proxy to the target host.
- Through built-in WAN accelerators: To transport VM data via WAN accelerators.

With Veeam Backup & Replication, you can perform both onsite replication for HA and offsite replication for DR scenarios. For replication over WAN or slow links, Veeam Backup & Replication provides a number of means to optimize data transmission – it performs inline deduplication and compresses replica traffic. You can also configure network throttling rules to prevent replication jobs from consuming the entire bandwidth in your environment, and perform replica seeding.
Replication generally provides the best RTOs and RPOs as you actually have a copy of your VM in a ready-to-start state. If a primary VM goes down, you just need start a VM replica to recover the VM. That is why replication is most commonly used for VMs running tier 1 applications.

**Note:** When using Veeam Replication to achieve business continuity, there will be networking and DNS challenges that must be overcome for a working solution. You may want to consult your network architect to define those changes.

### 5.4.2. Insight into replication

To create replicas, Veeam Backup & Replication uses VMware/Hyper-V VM snapshot capabilities. Snapshot replica is similar in many respects to forward incremental backup. During the first run of a replication job, Veeam Backup & Replication copies the VM running on the source host and creates its full replica on the target host. All subsequent replication jobs are incremental: Veeam Backup & Replication copies only those data blocks that have changed since the last replication cycle. For each new incremental run of the replication job, Veeam Backup & Replication triggers a regular snapshot of the replica. Thus, the created replica snapshot acts as a new restore point.

As a result, for every replicated VM, Veeam Backup & Replication produces a full replica and a chain of snapshots, or restore points.

All replication infrastructure components engaged in replication make up a data pipe. VM data is moved over this data pipe block by block, with multiple processing cycles. For vSphere, it’s important that there is a proxy at the destination side, so that the target data mover service could write data directly to the target storage, not passing it over network.

Veeam Backup & Replication creates and maintains the following types of replica files:

- Full VM replica (a set of VM configuration files and virtual disks)
- Replica restore points (VM snapshot files)
- Replica metadata (.vbm files) that stores VM replica digests (used to quickly detect changed blocks of data between two replica states)

The full VM replica along with its restore points is stored in a dedicated folder on the target datastore. Replica metadata files are stored on a backup repository.

### 5.4.3. Reducing Amount of Transferred Data

A replication job helps to avoid data loss. It is generally desired that low RPO is enabled and offsite data protection is facilitated. To reduce the amount of traffic sent over the network during replication, one of the following options can be used:
### 5.4.4. Resume on Disconnect

A dropped network connection used to be one of reasons for replication job failures. If a connection was interrupted even for several seconds in the middle of data transfer, the replication job failed reporting a connection reset error. In such situation, a failed job would have to be retried or re-run and the data transfer process would start from the very beginning.

<table>
<thead>
<tr>
<th>Source of data for the first run</th>
<th>Source of data for the subsequent runs</th>
<th>VM state</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>A backup chain on the backup repository</td>
<td>Production VM</td>
<td>Point in time when the backup was created</td>
<td>Reduces the workload on the production environment</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Remote replica from backup</th>
<th>Replica seeding</th>
<th>Replica mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>The backup file placed at the remote site</td>
<td>Already existing VM in the DR site</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Resume on Network Disconnect</th>
<th>Resume on WAN Disconnect</th>
</tr>
</thead>
<tbody>
<tr>
<td>When it happens</td>
<td>If a network connection drops for a short period of time during the replication process</td>
</tr>
<tr>
<td>Characteristics</td>
<td>- Dramatically improves the reliability of remote replication</td>
</tr>
<tr>
<td></td>
<td>- Reduces the backup window</td>
</tr>
<tr>
<td></td>
<td>- Minimizes the network/WAN link load</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>How it works</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Veeam Backup &amp; Replication does not create a new restore point upon resume: VM data is written to the same restore point that was created for the current replication session.</td>
<td>- After a WAN connection is resumed, Veeam Backup &amp; Replication starts a new data transfer cycle: data transported with every new cycle is written to a new working snapshot on a VM replica.</td>
</tr>
<tr>
<td>- In order to avoid keeping long snapshot chains, Veeam Backup &amp; Replication merges earlier snapshots and maintains only two working snapshots for a VM replica.</td>
<td>- Once all of the VM data is transferred to the target host, the two working snapshots are also merged to create one fully functional VM restore point.</td>
</tr>
</tbody>
</table>
Note: Resume on network disconnect is offered for the replication, backup, backup copy, full VM restore processes and all Cloud Connect-related activities. It is not available for tape operations.

5.5. Creating VM/File Copy Jobs

This topic will cover Veeam Backup & Replication VM copy and file copy jobs, which will enable you to:

- move your data center or mirror your production environment to test lab storage with VM copying
- deliver image files to hosts, make backup copies of existing VMs and exchange VMs and templates between servers or move backups across repositories using a file copy job.

5.5.1. VM copy

With a VM copy job, you can create a fully-functioning copy of a VM that will require no manual editing or adjustments. VM copying can be helpful if you want to move your data center, mirror your production environment to test lab storage, and so on. Just like backup and replication jobs, a VM copy job can be performed using the Direct SAN Access, Virtual Appliance, or Network transport modes, supports VSS options, and can be run on demand or scheduled.

This section will guide you through all steps of the VM Copy wizard and provide explanations for available options.

Prior to creating a VM copy job, make sure you have set up all the necessary infrastructure components. Open the Infrastructure view and check that source and destination hosts are available under the Managed servers node in the management tree and that backup proxies and backup repositories are available under the Backup Proxies and Backup Repositories nodes and properly configured. You will not be able to add VM copy infrastructure components or change their configuration once the VM Copy Job wizard is launched.

During every job run, Veeam Backup & Replication checks disk space on the destination storage. If the disk space is below a specific threshold value, Veeam Backup & Replication will display a warning in the job session log. To specify the disk space threshold, select Options from the main menu. On the Notifications tab, specify the amount of free disk space required in a percentage.

5.5.2. File Copy

Veeam Backup & Replication includes file copy possibilities which provides a natural way to deliver image files to hosts, make backup copies of existing VMs, and exchange VMs and templates between servers or move backups across repositories. Using Veeam Backup & Replication, you can copy files...
and folders between and within servers connected to the Veeam Backup Server.

**Note:** When the file copy destination is located on a server managed by Veeam Backup & Replication, traffic compression can be used to minimize network bandwidth and improve performance of file copy activities.
Labs for Module 5: Protect

Now you need to deliver the promised value. To reliably protect the data center, this module’s labs will showcase how to configure backup and replication jobs using the advanced settings based on the infrastructure and business continuity plan requirements and complement successful data protection with a disaster recovery plan while complying with the 3-2-1 Rule by copying your backups off site.

Get into the Lab

<table>
<thead>
<tr>
<th>Lab</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Creating Backups</td>
<td>Create a set of backup jobs to protect the virtual machines used in the lab environment.</td>
</tr>
<tr>
<td>5.2</td>
<td>Creating Backups with VeeamZIP</td>
<td>Quickly create a point-in-time copy of one of your virtual machines using VeeamZIP.</td>
</tr>
<tr>
<td>5.3</td>
<td>Creating Offsite Backup Copy Job</td>
<td>Create an offsite backup copy job using WAN Accelerator to provide the necessary level of safety by complying with the 3-2-1 rule.</td>
</tr>
<tr>
<td>5.4</td>
<td>Creating Replicas</td>
<td>Ensure efficient data protection in your virtual environment with the best RTO and RPO by setting up a VM replica for several of the VMs in the infrastructure.</td>
</tr>
</tbody>
</table>
Labs for Module P: Preparation for day 2

This module must be performed before you start other labs of day 2. You will delete a VM from the datastore to recover it later in the course flow, deploy a second Veeam Backup & Replication instance and review the backups and replicas created overnight.

Get into the Lab

<table>
<thead>
<tr>
<th>Lab</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>P.1</td>
<td>Day 1 Overview</td>
<td>Make sure the retention policy was applied correctly.</td>
</tr>
<tr>
<td>P.2</td>
<td>Deploying a second Veeam backup server</td>
<td>Install a second Veeam Backup &amp; Replication instance. We will use it later on in the course to showcase Configuration Restore and Decryption Without Password.</td>
</tr>
<tr>
<td>P.3</td>
<td>Deleting VMs</td>
<td>Delete a VM to test out Veeam Backup &amp; Replication restore capabilities later in the course.</td>
</tr>
<tr>
<td>P.4</td>
<td>Deleting SQL table</td>
<td>Delete a SQL table to force creation of transaction logs to test out Veeam Backup &amp; Replication restore capabilities later in the course.</td>
</tr>
</tbody>
</table>
6. Verification

To guarantee recoverability of your data, Veeam Backup & Replication offers the SureBackup technology.

6.1. SureBackup Recovery Verification

SureBackup is intended to automate and simplify the backup verification process – one of the most crucial parts of data management and protection. SureBackup lets validate backups of your VMs without impacting the production infrastructure. You can automatically verify every created restore point of every VM and ensure that they will function as expected in case a disaster strikes.

6.1.1. How It Works

SureBackup is Veeam’s technology that lets you test a VM backup and ensure that you will be able to recover data from it. To validate a VM backup, Veeam Backup & Replication performs its “live” verification: it automatically boots the VM from the backup in the isolated environment, performs tests against it, and then powers the VM off and creates a report on the VM backup state. You can verify a VM from the latest backup or from any necessary restore point. A SureBackup job also can be scheduled to be executed immediately after a specific backup job completes.

Note: SureBackup, or automatic recovery verification, is available in Enterprise and Enterprise Plus Editions of Veeam Backup & Replication. If you use the Standard Edition, you can manually verify VM backups with Instant VM Recovery.

SureBackup recovery verification uses a regular image-based backup created with Veeam Backup & Replication. The procedure of the VM verification is the following:

1. Veeam Backup & Replication leverages the Instant VM Recovery technology to publish a VM in the isolated virtual environment. The VM is started directly from the compressed and deduplicated backup file residing on the backup repository.
2. Veeam Backup & Replication performs a number of tests against the verified VM.
3. When the recovery verification process is over, Veeam Backup & Replication unpublishes the VM and creates a report on its state. The report is sent to the backup administrator by email.
During verification, a backed up VM image remains in read-only state. All changes that take place when a VM is running are written to redo log files that are stored on a selected datastore in the production environment. Once the recovery verification process is complete, the redo logs are removed.

To perform VM verification, you need to create the following entities:

1. **Application group.** During recovery verification, the verified VM is not started alone: it is started together with VMs on which it is dependent. Starting the verified VM in conjunction with other VMs enables full functionality of applications running inside the VM and lets you run these applications just like in the production environment.

2. **Virtual lab.** SureBackup leverages the virtual lab technology to verify a VM backup. The virtual lab is the isolated virtual environment in which the verified VM and VMs from the application group are started and tested.

3. **SureBackup job.** The SureBackup job is a task to run the recovery verification process. You can run the SureBackup job manually or schedule it to run automatically according to some schedule.

### Veeam vPower NFS Service

The Veeam **vPower NFS Service** is a Windows service that runs on a Windows backup repository server and enables it to act as an NFS server. vPower NFS allows Veeam Backup & Replication to mount a compressed and deduplicated backup file as a regular VMDK file directly to the ESX(i) host via NFS, so ESX(i) hosts get transparent access to backed up VM images.

If you store backups on a Windows repository, it is highly recommended to enable the vPower NFS Server on this repository. In this case, the vPower NFS Service will run on the managing Windows server.

Besides Windows-based backup repository servers, Veeam vPower NFS Service can run on any Windows server you choose, including the Veeam backup server itself. However, in this case, performance may be much lower because instead of a direct connection between the ESX(i) host and the backup repository, the connection will be split into two parts: ESX(i) host to NFS server and NFS...
The vPower technology is used to enable the following features:

- SureBackup: Recovery Verification
- Instant VM Recovery
- Multi-OS File-Level Recovery
- Universal Application-Item Recovery (U-AIR)

vPower-Specific Settings

To be able to successfully connect an ESXi host to the NFS server, you should make sure that the ESXi host has a proper network interface configuration and can access the server on which Veeam vPower NFS Service is running.

When connecting to the NFS server, the ESXi host uses a VMkernel interface. That is why the ESXi host you use must have a VMkernel interface. Otherwise, vPower NFS mounting on ESXi host will fail.

6.1.2. Recovery Verification Tests

To verify a VM started in the virtual lab, you can run Veeam’s predefined tests or perform your own tests against VMs. The predefined tests include the following ones:

1. **Heartbeat test.** As soon as the VM is started, Veeam Backup & Replication performs a heartbeat test. It waits for a heartbeat signal from VMware Tools/Hyper-V Integration Services installed inside the VM to determine that the guest OS inside the VM is running. If the signal comes regularly at specific time intervals, the test is passed.

2. **Ping test.** During the ping test, Veeam Backup & Replication checks if the VM in the virtual lab can respond to the ping requests. If VM responds to ping requests from the Veeam backup server, the test is passed.

3. **Application test.** Veeam Backup & Replication waits for applications to start inside the VM and runs a script that checks application-specific network ports. For example, to verify a Domain Controller, Veeam Backup & Replication probes port 389 for a response. If the response is received, the test is passed.

Beside these predefined tests, you can use custom scripts to verify the VM backup.

**Important!** To run ALL the recovery verification tests, you must have VMware Tools/Hyper-V Integration Services installed inside the vSphere VM you start from the backup and Hyper-V Integration Services for the Hyper-V VM. Otherwise these tests will be skipped; Veeam Backup & Replication will display a warning in the SureBackup job session results.

6.1.3. Backup File Validation

In addition to recovery verification tests, Veeam Backup & Replication allows you to perform backup
file validation (also referred to as backup file verification) – a CRC check that runs for backup files of VMs verified by the SureBackup job. The option to validate backup files is selected in the recovery verification job settings. You can also optionally validate backup files for VMs from the application group.

For validation of a backup file, Veeam Backup & Replication uses the checksum algorithm. When Veeam Backup & Replication creates a backup file for a VM, it calculates a checksum for every data block in the backup file and stores this data together with VM data. During the backup file validation test, Veeam Backup & Replication de-compresses the backup file, re-calculates checksums for data blocks in the uncompressed backup file, and compares them with initial checksum values. If the results match, the test is passed.

**Note:** The result of the backup file validation test impacts the state of the SureBackup job session. If the validation tests are completed successfully but the backup validation is not passed, Veeam Backup & Replication marks the SureBackup job session with the **Warning** status.

### 6.1.4. Application Group

In most cases, a VM works in cooperation with other services and components. To verify such VMs, you first need to start all services and components on which the VM is dependent. To this aim, Veeam Backup & Replication uses the notion of the application group.

The application group creates the “surroundings” for the verified VM. The application group contains one or several VMs on which the verified VM is dependent. These VMs run applications and services that must be started to enable fully functional work of the verified VM. Typically, the application group contains at least a domain controller, DNS server and DHCP server.
When you set up an application group, you specify the role of every VM, its boot priority and boot delay. Additionally, you specify what tests must be performed for VMs in the application group.

When a SureBackup job is launched, Veeam Backup & Replication first starts in the virtual lab VMs from the application group in the required order (as specified in the application group settings) and performs necessary tests against them. This way, Veeam Backup & Replication creates the necessary environment to start the verified VM. After all the VMs from the application group are started and tested, Veeam Backup & Replication starts the verified VM in the virtual lab.

You can add a VM just from the infrastructure, so it doesn’t have to have any valid restore points at this stage yet.

An application group may contain start one or more VMs from backups, VM replicas or VMs from storage snapshots.

For example: If you want to verify a Microsoft Exchange Server, you need to test its functionality in cooperation with other components: domain controller and DNS server. Subsequently, you must add to the application group a virtualized domain controller and DNS server. When Veeam Backup & Replication runs a SureBackup job, it will first start and verify the domain controller and DNS server in the virtual lab to make verification of the Exchange Server possible.

Note: All VMs added to the application group must belong to the same platform – VMware or Hyper-V. Mixed application groups are not supported.

6.1.5. Virtual Lab

The virtual lab is an isolated virtual environment in which Veeam Backup & Replication verifies VMs. In the virtual lab, Veeam Backup & Replication starts a verified VM and VMs from the application
The virtual lab is used not only for the SureBackup verification procedure, but also for U-AIR and On-Demand Sandbox processing.

**Note:** On-Demand Sandbox refers to using the Virtual Lab to run as an isolated environment for patch deployment testing or troubleshooting.

A virtual lab does not require provisioning of additional resources. You can deploy it on the existing ESX(i) host in your virtual environment.

The virtual lab is fully fenced off from the production environment. The network configuration in the virtual lab mirrors the network configuration of the production environment.

**For example:** If verified VMs are located in two logical networks in your production environment, the virtual lab will also have two networks. The networks in the virtual lab will be mapped to corresponding production networks.

**Tip:** You can optionally connect VMs to the same network in the virtual lab, even if corresponding VMs in the production environment are connected to different networks.

VMs in isolated networks have the same IP addresses as in the production network. This lets VMs in the virtual lab function just as if they would in the production environment.
Proxy Appliance

To enable communication between the production environment and the isolated networks in the virtual lab, Veeam Backup & Replication uses a proxy appliance. The proxy appliance is a Linux-based auxiliary VM created on the host where the virtual lab is created. The proxy appliance VM is assigned an IP address from the production network and placed in the dedicated virtual lab folder and resource pool created on the host.

The proxy appliance is connected to the production network and to the isolated network so it has visibility of the production environment and the virtual lab. In essence, the proxy appliance acts as a gateway between the two networks, routing requests from the production environment to VM replicas in the virtual lab.

The proxy appliance connects to isolated networks using network adapters. Veeam Backup & Replication adds to the proxy appliance one network adapter per each isolated network.

For example: If there are two networks in the virtual lab, Veeam Backup & Replication will add two network adapters to the proxy appliance. The network adapter gets an IP address from the isolated network. Typically, this IP address is the same as the IP address of the default gateway in the corresponding production network.

Note: The proxy appliance is an optional component. Technically, you can create a virtual lab without a proxy appliance. However, in this case, you will not be able to perform automatic recovery verification of VMs. VMs will be simply started from backups in the virtual lab; you will have to access them using the VM console and perform necessary tests manually.
IP Masquerading

To let the traffic into the virtual lab, Veeam Backup & Replication uses masquerade IP addressing. Every VM in the virtual lab has a masquerade IP address, along with the IP address from the production network. The masquerade IP address resembles the IP address in the production network: for example, if the IP address of a VM is 172.16.1.13, the masquerade IP address may be 172.18.1.13.

The masquerade IP address can be thought of as an entry point to the VM in the virtual lab from the production environment. When you want to access a specific VM in the virtual lab, Veeam Backup & Replication addresses it by its masquerade IP address.

The rules routing requests to VMs in the virtual lab are specified in the routing table on the server from which you want to access VMs in the virtual lab. The routing table can be updated on the following servers:

- Veeam backup server. Veeam Backup & Replication automatically creates the necessary static route in the routing table on the Veeam backup server the moment you launch a SureBackup job and Veeam Backup & Replication starts the virtual lab.
- Client machine. If you want to provide your users with access to VMs in the virtual lab, you need to manually update routing tables on their machines and add a new static route.

The added static route destines the masquerade network traffic to the proxy appliance. The proxy appliance here acts as a NAT device: it resolves the masquerade IP address, replaces it with the “real” IP address of a VM from the production network and then directs the request to the necessary VM in the virtual lab. The static route is non-persistent: when you power off the virtual lab, the route is removed from the routing table on the Veeam backup server or client machine.
For example: When trying to access a VM with IP address 172.16.10.10 in the isolated network during recovery verification, Veeam Backup & Replication sends a request to the masquerade IP address 172.18.10.10. According to the routing rule added to the IP routing table, all requests are first sent to the next hop – the proxy appliance. The proxy appliance performs address translation, substitutes the masquerade IP address with the IP address in the isolated network, and forwards the request to the necessary VM in the isolated network – in the given example, to 172.16.10.10.

Static IP Mapping

Sometimes it is necessary to provide many clients with access to a restored VM, especially for user-directed application item-level recovery.

For example: You may want to provide your users with access to the Exchange Server started in the virtual lab using web-based access (like Outlook Web Access). Technically, you may update the routing table on every client machine; however, this will demand a lot of administrative effort. For such situations, Veeam Backup & Replication enables you to get access to a VM in the virtual lab directly from the production environment. To be able to access to a VM in the virtual lab, you should reserve a static IP address in the pool of production IP addresses and map this IP address to the IP address of a VM in the virtual lab.

The static IP address is assigned to the proxy appliance network adapter connected to the production network. IP traffic directed to the specified static IP address is routed by the proxy appliance to the
VM powered on in the isolated network.

For example: For a VM with IP address 192.168.1.20 in the isolated network, you can reserve IP address 192.168.1.99 (a free IP address from the production network). As a result, you will be able to use IP address 192.168.1.99 to access the VM in the virtual lab from the production side.

You can also register an alias record in the production DNS server for the reserved IP address. For example, you can register backup.exchange.local as an alias for the IP address 192.168.1.99.

Virtual Lab Configuration

For SureBackup recovery verification, Veeam Backup & Replication offers two types of the virtual lab configuration:

- Basic single-host virtual lab
- Advanced single-host virtual lab

However, when verifying VM replicas that are located on different hosts, you cannot use the single-host virtual lab configuration (either basic or advanced) as it has specific configuration limitations. So for SureReplica recovery verification, Veeam Backup & Replication offers three types of the virtual lab configuration:

- Basic single-host virtual lab
- Advanced single-host virtual lab
- Advanced multi-host virtual lab
Basic Single-Host Virtual Labs

The basic single-host virtual lab (formerly known as the virtual lab with basic networking configuration) should be used if all the VMs you want to verify, VMs from the application group, and the Veeam backup server are connected to the same network.

For the basic single-host virtual lab, Veeam Backup & Replication creates one virtual network that is mapped to the corresponding production network.

Advanced Single-Host Virtual Labs

The advanced single-host virtual lab (formerly known as the virtual lab with advanced networking configuration) should be used if the VMs you want to verify and/or the VMs from the application group are connected to different networks.

In the advanced single-host virtual lab, Veeam Backup & Replication creates several virtual networks for the virtual lab. The number of virtual networks corresponds to the number of production networks to which verified VMs are connected. Networks in the virtual lab are mapped to corresponding production networks.

When you create an advanced single-host virtual lab, Veeam Backup & Replication configures basic settings for networks that should be created in the virtual lab. You need to review these settings and manually adjust them if needed.
Limitations of Single-Host Virtual Labs (VMware)

If VM replicas are located on different hosts, you cannot use the single-host virtual lab configuration (either basic or advanced). A single-host virtual lab, both basic and advanced, uses standard vSwitches (vSS) that have specific configuration limitations.

When you create or edit a virtual lab, Veeam Backup & Replication creates a new port group for each isolated network in the virtual lab. All VMs from the isolated network are added to this port group. Such configuration helps differentiate the traffic passing through the VSS to the isolated network in the virtual lab.

However, the VSS has a specific restriction: it is “limited” to a certain ESX(i) host. A VSS is configured on a specific ESX(i) host. The configuration of the VSS, such as information about port groups, resides on the ESX(i) host where it is configured. Other ESX(i) hosts in the virtual environment do not have access to this information.

Therefore, the single-host configuration can only be used if all VM replicas are registered on the same ESX(i) host. If you start VM replicas registered on different ESX(i) hosts in the single-host virtual lab, VMs from different port groups will not be able to “see” each other and communicate with each other.
Advanced Multi-Host Virtual Labs (VMware)

The advanced multi-host virtual lab configuration should be used if your DR site is configured in the following way:

- All VM replicas you want to verify are located on the different ESX(i) hosts
- VM replicas you want to verify are connected to one or several networks

Note: DVS is limited to one datacenter. For this reason, all verified VM replicas and VM replicas from the application group that you plan to start in the virtual lab must belong to the same datacenter. If VM replicas belong to different datacenters, you will still be able to start them in the virtual lab, but Veeam Backup & Replication will not be able to automatically verify them with SureBackup.

To verify VM replicas registered on different ESX(i) hosts, you should use the advanced multi-host configuration of the virtual lab. The advanced multi-host virtual lab leverages the VMware Distributed vSwitch (DVS) technology.

When you configure an advanced multi-host virtual lab, you should select an ESX(i) host on which the proxy server will be created and a DVS on which Veeam Backup & Replication will create isolated network(s). Veeam Backup & Replication does not offer an option to automatically configure the DVS. The DVS you plan to use must be pre-configured in your virtual environment.

The DVS port groups created on the DVS must be isolated from the production environment. To isolate port groups, you can use one of the following methods:

1. Connect DVS uplinks to an isolated network. You can link the DVS you plan to use for recovery verification to an external, isolated network using uplink adapters. Note that these network configurations must be performed manually by the backup administrator.
2. Use VLAN tagging. This method can be used only if your router supports VLAN ID tagging. When specifying settings for isolated networks in Veeam Backup & Replication, you can define different VLAN IDs for different isolated networks. Setting VLAN IDs restricts communication of VM replicas in the isolated network with the production environment.

With Veeam Backup & Replication, you can optionally connect VMs from different production networks to one network in the isolated virtual lab. In this case, all VM replicas in the virtual lab will be...
started in the same network.

6.1.6. SureBackup Job

A SureBackup job is a task for VM backup recovery verification. The SureBackup job aggregates all the settings and policies of a recovery verification task, such as the application group and virtual lab, VM backups that should be verified in the virtual lab, and so on. The SureBackup job can be run manually or be scheduled to run automatically.

When a SureBackup job runs, Veeam Backup & Replication first creates an environment for VM backup verification:

1. Veeam Backup & Replication starts the virtual lab.
2. In the virtual lab, it starts VMs from the application group in the required order. VMs from the application group remain running until the verified VMs are booted from backups and tested. If Veeam Backup & Replication does not find a valid restore point for any of VMs from the application group, the SureBackup job will fail.

Once the virtual lab is ready, Veeam Backup & Replication starts verified VMs from the necessary restore point, tests and verifies them one by one or, depending on the settings, creates several streams and tests a number of VMs simultaneously. If Veeam Backup & Replication does not find a valid restore point for any of the verified VMs, verification fails, but the job continues to run.

By default, when using the Linked Jobs option in a SureBackup job, you can start and test up to three VMs at the same time. You can also increase the number of VMs to be started and tested simultaneously. Keep in mind that if these VMs are resource-intensive, performance of the SureBackup job as well as performance of the ESX(i) host holding the virtual lab may decrease.

Once the verification process is complete, VMs from the application group are powered off. Optionally, you can leave the VMs from the application group running to perform manual testing or enable user-directed application item-level recovery. This should be indicated when you configure a SureBackup job.

Note: In some cases, the SureBackup job schedule may overlap with the schedule of the backup job linked to it. The backup file may be locked by the backup job and the SureBackup job will be unable to verify it. In this situation, Veeam Backup & Replication will not start the SureBackup job until the corresponding backup job is over. To overcome job overlapping, you may chain the backup and SureBackup jobs.

SureBackup Job Processing

The recovery verification process includes the following steps:

1. Getting virtual lab configuration. Veeam Backup & Replication gets information about the configuration of the virtual lab where verified VMs should be started.
2. Starting the virtual lab routing engine. Veeam Backup & Replication starts a proxy appliance used as a gateway to provide access to the virtual lab.
3. Publishing. Veeam Backup & Replication creates an NFS datastore with a VM backup and registers it on the selected ESX server. Veeam Backup & Replication does not deploy the whole VM from the backup file, it deploys VM configuration files only. Virtual disks are deployed per force and per required data blocks.

4. Reconfiguring. Veeam Backup & Replication updates configuration files for VMs that should be run in the isolated network.

5. Registering. Veeam Backup & Replication registers the verified VM on the selected ESX(i) host.

6. Configuring DC. If a verified VM has the Domain Controller or Global Catalog role, the VM is reconfigured.

7. Powering on. Veeam Backup & Replication powers on the verified VM in the isolated network (using the order of priority as specified in the application group settings).

8. Running the heartbeat test. Veeam Backup & Replication checks whether or not the VMware Tool/Hyper-V Integration Services s heartbeat signal (green or yellow) is coming from the VM. If the VM has no VMware Tools, the test will not be performed, and a notification will be written in the session details.

9. Running ping tests. Veeam Backup & Replication checks if the VM responds to the ping requests. If the VM has no NICs and mapped networks for them and/or has no VMware Tools/Hyper-V Integration Services installed, the ping test will not be performed, and a notification will be written in the session details.

10. Application initialization. Veeam Backup & Replication waits for the applications installed in the VM (for example, SQL Server, web server, mail server) to start. The application initialization period is defined in the corresponding properties of the SureBackup job, and by default equals to 120 sec. However, depending on the software installed in a VM, the application initialization process may require more time than specified in the SureBackup job settings. If applications installed in a VM are not initialized within the specified period of time, test scripts can be completed with errors. If such an error situation occurs, you will need to increase the application initialization timeout value and start the job once again.

11. Running test scripts. Veeam Backup & Replication runs scripts to test whether or not the applications installed in the VM is working correctly. If the VM has no VMware Tools/Hyper-V Integration Services installed and/or there are no NICs and mapped networks for them, Veeam Backup & Replication will skip tests that use variables %vm_ip% and %vm_fqdn% as the IP address and fully qualified domain name of the VM cannot be determined.

12. Powering off. After all tests have been performed, Veeam Backup & Replication powers off the verified VM.

13. Unregistering. Veeam Backup & Replication unregisters the verified VM on the selected ESX(i) host.

14. Clearing redo logs. Veeam Backup & Replication deletes redo logs that were created at the datastore specified in Virtual Lab settings to store changes made to the VM while it was running from the backup file.

15. Unpublishing. Veeam Backup & Replication unpublishes the content of the backup file on the ESX(i) host.

**Stabilization Algorithm**

In order to perform tests for a verified VM without errors, Veeam Backup & Replication needs to know that the VM is ready for testing. To determine this, Veeam Backup & Replication waits for the VM to reach a stabilization point: that is, it waits for the VM to boot completely and report it is ready for tests. After the stabilization point has been established, Veeam Backup & Replication can start performing heartbeat tests, ping tests and running test scripts against the VM.
Veeam Backup & Replication establishes the stabilization point with the help of the VMware parameters that it gets from the VM. It can use one of three algorithms to do that, depending on the VM configuration:

- **Stabilization by IP.** This algorithm is used if the VM has VMware Tools installed and there are NICs and mapped networks for these NICs. In this case, Veeam Backup & Replication waits for the IP address of the VM for mapped networks, which is sent by VMware Tools running in the VM. The sent IP address should be valid and should not change for a specific period of time.
- **Stabilization by heartbeat.** This algorithm is used if the VM has VMware Tools installed but there are no vNICs or mapped networks for them. In this case Veeam Backup & Replication waits for a corresponding heartbeat signal (green or yellow) to come from the VM. Just like in the first case, the signal is sent by VMware Tools running in the VM.
- **Stabilization by Maximum allowed boot time.** This algorithm is used if the VM has neither VMware Tools installed, nor NICs and mapped networks for them. In this case, Veeam Backup & Replication will simply wait for the time specified in the **Maximum allowed boot time** field, which is considered to be a stabilization period for the VM. Once this time interval is exceeded, Veeam Backup & Replication will consider that the VM is successfully booted and is ready for testing.

### 6.1.7. Manual Recovery Verification

Beside automatic recovery verification, you can also perform manual verification of VM backups. **Manual verification** can be performed with all editions of Veeam Backup & Replication.

- To perform a VM boot test, you can go through the Instant VM Recovery wizard and power the VM on without connecting it to the production network.
- To perform the application recovery test, you should first create an isolated network. After that, you need to pass through the Instant VM Recovery wizard to restore a VM from the backup. At the **Network** step of the wizard, you should connect the VM to the created isolated network.

The same procedure should be followed for all VMs that run applications on which a verified VM is dependent, such as domain controller and DNS. All VMs must be connected to the same isolated network and started in the correct order: for example, DNS → domain controller → verified VM.

### 6.2. SureReplica Recovery Verification

To guarantee recoverability of your data, Veeam Backup & Replication complements the SureBackup recovery verification technology with SureReplica. SureReplica is similar to the SureBackup recovery verification in many respects. It lets you validate your DR environment without impacting the production infrastructure: you can automatically verify every created restore point of every VM replica and ensure that they are functioning as expected when you set up a SureReplica recovery verification to be triggered automatically after a replica job creates a new restore point.

**Important!** SureReplica is only available for VMware vSphere - it is not available for Microsoft Hyper-V.
The SureReplica technology is not limited only to VM replica verification and, similar to SureBackup, provides the following capabilities:

<table>
<thead>
<tr>
<th>Capability</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>SureReplica</td>
<td>Automated VM replica verification</td>
</tr>
<tr>
<td>On-Demand Sandbox</td>
<td>An isolated environment for testing VM replicas, training and troubleshooting</td>
</tr>
<tr>
<td>U-AIR</td>
<td>Recovery of individual items from applications running on VM replicas</td>
</tr>
</tbody>
</table>

**Note:** As there is no need to publish the VM from the backup file, the SureReplica processing is typically faster than SureBackup. Correspondingly, the U-AIR and On-Demand Sandbox operations are faster, too.

The procedure of the VM replica verification is the following:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Veeam Backup &amp; Replication triggers a protective snapshot for a VM replica.</td>
<td>All changes made to the VM replica are written to delta files.</td>
</tr>
<tr>
<td>2</td>
<td>Veeam Backup &amp; Replication starts the VM replica in the isolated virtual environment.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Veeam Backup &amp; Replication performs a number of tests against the verified VM replica.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>When the verification process is over, Veeam Backup &amp; Replication: 1. Removes delta files from the VM replica snapshot 2. Powers off the VM replica 3. Creates a report on its state</td>
<td>The report is sent to the backup administrator by email.</td>
</tr>
</tbody>
</table>

**Note:** Veeam Backup & Replication verifies only VM replicas that are in the Normal state. If a VM replica is in the Failover or Failback state, the verification process will fail. When Veeam Backup & Replication verifies the VM replica, it puts the VM replica to the SureBackup state. You cannot perform failback or failover operations for a VM replica in the SureBackup state until the recovery verification or U-AIR process is over and the VM replica returns to the Normal state.

To perform VM replica verification, the same wizard is used as for backup verification. You need to create the following similar entities:
During recovery verification, the VM replica is started with VMs on which the VM replica is dependent. This enables full functionality of applications running inside the VM replica and allows you to start required applications just like in the production environment.

The *virtual lab* is an isolated virtual environment in which the VM replica and VMs from the application group are started and tested. *SureReplica* leverages the virtual lab technology to verify the VM replica.

The *SureBackup* job is a task which runs the replica verification process. This kind of SureBackup job is often referred to as a SureReplica job. It can be run manually or scheduled to run automatically.

To verify a VM replica started in the virtual lab, you can run Veeam’s predefined tests or perform your own tests against VMs.

The predefined tests include the following:

<table>
<thead>
<tr>
<th>Heartbeat test</th>
<th>Ping test</th>
<th>Application test</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>When performed</strong></td>
<td>As soon as the VM replica is started</td>
<td>As soon as the VM replica is started (after heartbeat test)</td>
</tr>
<tr>
<td><strong>How it works</strong></td>
<td>Waits for a heartbeat signal from VMware Tools installed inside the VM to determine that the guest OS inside the VM replica is running</td>
<td>Sends ping requests to the VM replica started in the virtual lab</td>
</tr>
<tr>
<td><strong>How results are measured</strong></td>
<td>Passed: The yellow and green signals display. Failed: The red signal displays.</td>
<td>If the VM replica can respond to ping requests from the Veeam backup server, the test is passed.</td>
</tr>
<tr>
<td><strong>Notes</strong></td>
<td>You must have VMware Tools installed inside the VM being verified. Otherwise all tests will be skipped; Veeam Backup &amp; Replication will display a warning in the SureBackup job session results.</td>
<td></td>
</tr>
</tbody>
</table>

Beside these predefined tests, you can use custom scripts to verify the VM replica.

### 6.3. On-Demand Sandbox

If you need to perform tests for production VMs, you can create and use an *On-Demand Sandbox™*. The On-Demand Sandbox is an isolated virtual environment where you can start one or more VMs.
from backups, VM replicas or VMs from storage snapshots. You can use the On-Demand Sandbox to perform the following tasks:

- Troubleshoot problems with VMs
- Test software patches and upgrades
- Install new software

To create the On-Demand Sandbox, you must configure the following objects:

- A **virtual lab** in which VMs will be started.
- An **application group**. The application group must include all VMs and/or VM replicas that you want to start in the On-Demand Sandbox. This can be one VM or a group of VMs that work together. Veeam Backup & Replication supports mixed application groups. You can add to the same application groups both VMs from backups and VMs from replicas. Keep in mind that all VMs from the application group must belong to the same platform – VMware or Hyper-V, and must have at least one valid restore point created by the time the SureBackup job starts.
- A **SureBackup job**. The virtual lab and application group must be linked to this job.

The difference between using these three entities for automated verification purposes and for On-Demand Sandbox purposes is that for On-Demand sandbox purposes you should enable the Keep the application group running once the job completes check box when configuring a SureBackup job. With this option enabled, the lab will not be powered off when the SureBackup job completes and you will be able to manually test VMs started in the virtual lab.

You can also choose to move the VMs straight to production from the Virtual Lab (e.g if the upgrade works as expected) with a one time replication job.

---

**Note:** The source backup or replication job has a higher priority than the SureBackup job. If a backup or replication job starts when the SureBackup job is running, and this job requires to modify the restore point from which the VM is started (i.e create a new snapshot on the replica, or perform a transform operation), Veeam Backup & Replication automatically powers off VMs in the virtual lab and terminates the SureBackup job.
Labs for Module 6: Verification

After completing the theoretical part of Module 6: Verification you are familiar with configuring application group, Virtual Lab and SureBackup jobs and you can name the interactions that happen throughout the backup or replica verification.

It’s time to try out setting up the reviewed validation processes in the lab.

Get into the Lab

<table>
<thead>
<tr>
<th>Lab</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>Preparing Infrastructure</td>
<td>Familiarize yourself with the components you need to create in the interface so you can automatically validate VM backups without affecting the production infrastructure.</td>
</tr>
<tr>
<td>6.2</td>
<td>Using SureBackup</td>
<td>Configure a backup verification process for one of the VMs of the infrastructure.</td>
</tr>
<tr>
<td>6.3</td>
<td>Using SureReplica</td>
<td>Verify a replica of a VM to review the specifics of the process, especially when compared with the backup verification.</td>
</tr>
</tbody>
</table>
7. Entire VM Recovery

7.1. Data Recovery

If a production VM has failed and you need to recover it from the backup, Veeam Backup & Replication offers a number of recovery options for various disaster recovery scenarios.

7.1.1. Data Recovery Scenarios Overview

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instant VM Recovery</td>
<td>Instantly start a VM directly from a backup file</td>
</tr>
<tr>
<td>Full VM Recovery</td>
<td>Recover a VM from a backup file to its original or another location</td>
</tr>
<tr>
<td>VM file Recovery</td>
<td>Recover separate VM files (virtual disks, configuration files and so on)</td>
</tr>
<tr>
<td>Windows File-Level Recovery</td>
<td>Recover individual Windows guest OS files (from FAT, NTFS and ReFS file systems)</td>
</tr>
<tr>
<td>MultiOS File-Level Recovery</td>
<td>For most commonly used file systems on Windows, Linux, Solaris, BSD, Novell Netware, Unix and Mac machines</td>
</tr>
<tr>
<td>Veeam Explorers</td>
<td></td>
</tr>
<tr>
<td>Universal Application-Item Recovery (U-AIR)</td>
<td>Recover application objects directly from backup files</td>
</tr>
</tbody>
</table>

Note: For VMware vSphere, restores are done via network or VIX (VMware Tools VIX Channel), if Veeam Backup & Replication fails to connect to the VM guest OS over the network. Also, if your backup proxy is a VM with HotAdd access to the source datastore, during the full VM restore, Veeam Backup & Replication will use the Virtual Appliance transport mode to write the VM data from the backup proxy back to the datastore. This speeds up the restore process and reduces the load on the network.

7.1.2. Instant VM Recovery

With Instant VM Recovery, you can immediately restore a VM into your production environment by running it directly from the compressed and deduplicated backup file. Instant VM Recovery helps improve recovery time objectives and minimize disruption and downtime of production VMs. It’s like having a ‘temporary spare’ for a VM: users remain productive while you troubleshoot issues with the failed VM.
VMware

When *Instant VM Recovery* is performed, Veeam Backup & Replication uses the *Veeam vPower* technology to mount a VM image to an ESX(i) host directly from a compressed and deduplicated backup file. Because there is no need to extract the VM from the backup file and copy it to production storage, you can restart a VM from any restore point (incremental or full) in a matter of minutes.

The archived image of the VM remains in read-only state to avoid unexpected modifications. By default, all changes to virtual disks that take place while the VM is running are logged to auxiliary redo logs residing on the NFS server (Veeam backup server or backup repository). These changes are discarded as soon as a restored VM is removed, or merged with the original VM data when VM recovery is finalized.

To improve I/O performance for a restored VM, you can redirect VM changes to a specific datastore. In this case, instead of using redo logs, Veeam Backup & Replication will trigger a snapshot and put it in the Veeam IR directory on the selected datastore along with metadata files holding changes to the VM image.

Either original location or different one can be selected for restore. To finalize Instant VM Recovery, you have to migrate it to production with one of the following options:

- **Use VMware Storage vMotion** to quickly migrate the restored VM to the production storage without any downtime. In this case, original VM data will be pulled from the NFS datastore to the production storage and consolidated with VM changes while the VM is still running. VMware Storage vMotion, however, can only be used if you select to keep VM changes on the NFS datastore without redirecting them. Please note that VMware Storage vMotion is only available with VMware Enterprise licenses and above.
- **Use replication or VM copy** functionality of Veeam Backup & Replication to create a copy of a VM and fail over to it during the next maintenance window. In contrast to VMware Storage vMotion, this approach requires you to schedule some downtime while you clone or replicate the VM, power it off, and then power the cloned copy or replica on.
- **Use Quick Migration** to perform a two-stage migration procedure – instead of pulling data from the vPower NFS datastore, it will restore the VM from the backup file on the production server, then move all changes and consolidate them with the VM data.

Beside disaster recovery matters, instant VM recovery can also be used for testing purposes. Instead of extracting VM images to the production storage to perform regular DR testing, you can run a VM directly from the backup file, boot it and make sure the VM guest OS and applications are functioning properly.

Hyper-V

In the Hyper-V environment, *Instant VM Recovery* is performed in the following way:

1. Veeam Backup & Replication reads the VM configuration from the backup file in the repository and creates a dummy VM with the same settings and empty disks on the destination host.
2. Veeam Backup & Replication initiates the creation of a protective snapshot for the dummy VM and the VM is started. If the Instant VM Recovery process fails for some reason, the protective snapshot guarantees no data is lost.
3. On the backup repository and on the destination host, Veeam Backup & Replication deploys a pair of Veeam data mover services that are used to mount the VM disks from the backup file to the dummy VM.

4. On the destination host, Veeam Backup & Replication starts a proprietary Veeam driver. The driver redirects requests to the file system of the recovered VM (for example, when a user accesses some application) and reads the necessary data from the backup file on the backup repository via the pair of Veeam data mover services which maintain the disk mount.

To finalize VM recovery, you can migrate the VM to the production storage. When you begin the migration process, Veeam Backup & Replication starts another pair of Veeam data mover services on the backup repository and on the destination host. The second pair of Veeam data mover services copies the recovered VM's data from the backup repository to the destination host in the background, and populates disks of the VM started on the destination host.

The driver on the destination host knows which data has already been restored permanently and does not redirect requests to it, reading it directly from the disks of the restored VM. Thus, performance of the instantly recovered VM will increase as more of the data is copied. When the VM is restored completely, all Veeam data mover services are stopped.

**Important!** Before you start the Instant VM Recovery in the Hyper-V environment, make sure that Changed Block Tracking is enabled for a host to which you plan to restore a VM. If Changed Block Tracking is disabled for the host, the driver required for work of Instant VM Recovery will be disabled.

If you do not perform VM migration, all operations on the file system of the recovered VM will be carried out via the disk mount connection. This is helpful if you will only need the instantly recovered VM for a short period of time, to perform one or two tasks (for example, look up some information stored on the backed up VM).

### 7.1.3. Full VM Recovery

With Veeam Backup & Replication, you can restore an entire VM from a backup file to the latest state or to any good-to-know point in time if the primary VM fails.

In contrast to Instant VM Recovery, Full VM Restore (also referred to as Entire VM restore) requires you to fully extract the VM image to the production storage. Though Full VM Restore takes more resources and time to complete, you do not need to perform extra steps to finalize the recovery process. Veeam Backup & Replication pulls the VM data from the backup repository to the selected...
storage, registers the VM on the chosen ESXi or Hyper-V host and, if necessary, powers it on.

A VM can be restored to its original location or to a new location. And you can restore several VMs at once. When you restore a VM to its original location, the primary VM is automatically turned off and deleted before the restore. This type of restore ensures the quickest recovery and minimizes the number of mistakes which can potentially be caused by changes in VM settings.

### Incremental Restore

For VMware vSphere, when you restore a full VM or VM hard disk to the original location, Veeam Backup & Replication performs incremental restore (Quick Rollback) by default, leveraging VMware Changed Block Tracking technology. Instead of restoring an entire VM or VM disk from a backup file, Veeam Backup & Replication recovers only those data blocks that are necessary to revert the VM or VM disk to an earlier point in time. Incremental restore:

- Significantly reduces the recovery time.
- Has little impact on the production environment.

It is recommended that you use quick rollback if you restore a VM after a problem that has occurred at the level of the VM guest OS: for example, there has been an application error or a user has accidentally deleted a file on the VM guest OS. Do not use incremental restore if the problem has occurred at the VM hardware level, storage level or due to a power loss.

Requirements for incremental restore:

1. VM is restored to its original location.
2. The backup file from which you plan to restore a VM is created with the Changed block tracking option enabled.

There are also some limitations for incremental restore. You cannot run two incremental restore sessions subsequently. After you perform incremental restore for a VM, the CBT on the original VM is reset. You must perform at least one incremental backup to be able to perform incremental restore again.

### 7.1.4. VM File Recovery

Veeam Backup & Replication can help you to restore specific VM files (.vmdk, .vmx/.vhd, .vhdx, .xml and others) if any of these files are deleted or the datastore/volume is corrupted. This option provides a great alternative to Full VM Restore, for example, when your VM configuration file is missing and you need to restore it. Instead of restoring the whole VM image to the production storage, you can restore the specific VM file only.

When you perform VM file restore, VM files are restored from regular image-level backups. Veeam data mover (also referred to as “transport”) services deployed on the backup repository and the backup proxy retrieve VM data from the backup file and send it to the original VM location, or to a new location specified by the user.
7.2. Working with Veeam Backup & Replication Utilities

Veeam Backup & Replication comes with an extract utility that can be used to recover VMs from a full backup file – VBK. The utility can be used as an independent tool on Linux and Windows computers as it does not require any interaction with Veeam Backup & Replication. The extract utility can be helpful; for example, if it is written to the tape next to backup files, you can possibly recover VMs from backups even if backups are removed from Veeam Backup & Replication or the application is uninstalled.

The extract utility can be utilized via two interfaces:

- Graphic user interface (can be started on Microsoft Windows machines only)
- Command-line interface working in the interactive or regular mode

The installation folder of Veeam Backup & Replication (by default: %PROGRAMFILES%\Veeam\Backup and Replication\Backup) contains three files for the extract utility:

- Veeam.Backup.Extractor.exe – The utility working via the graphic user interface (Microsoft Windows machines only)
- extract.exe – The utility working via the command-line interface (version for Microsoft Windows)
- extract – The utility working via the command-line interface (version for Linux)

Important! The extract utility always restores a VM from the full backup file.

7.3. Insight into Recovery from Replica

The next section will familiarize you with the various ways that you can utilize replicas for the disaster recovery or other scenarios.

7.3.1. Failover

If a primary VM in the production site becomes unavailable, you can quickly restore services by failing over to its replica. When you perform failover, the VM replica takes over the role of the original VM and you switch from the production VM to its replica and shift your I/O and processes from the production host to a secondary host. As a result, you have your VM up and running within minutes, and your users can access the services and applications they need with minimum disruption.

In Veeam Backup & Replication, you can fail over to the latest state of a replica or to any of its good to know restore points.

Failover itself is an intermediate step that needs to be finalized. Depending on the disaster recovery scenario, you can do one of the following:
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Switch from the original VM to a VM replica and use this replica as the original VM.</td>
<td>Switch back to the original VM after the problem in the production site is eliminated.</td>
<td>Switch back to the original VM and work with it in the normal operation mode.</td>
</tr>
<tr>
<td>How changes to VM replica are handled</td>
<td>No transferring because all changes are initially made to a replica VM</td>
<td>Transferred to the original VM</td>
<td>Discarded</td>
</tr>
<tr>
<td>Replica Site Location</td>
<td>Same as original VM</td>
<td>Disaster Recovery (DR)</td>
<td>Testing environment (e.g. dedicated resource pool)</td>
</tr>
<tr>
<td>When this scenario is recommended</td>
<td>This is best when the original VM and a VM replica are located in the same site, and hosts and storage are nearly equal in terms of resources. In this case, your users will not experience any latency in ongoing operations.</td>
<td>This is best when the VM replica is located in a DR site and is running on a lower tier host and storage, which is not intended for continuous operations.</td>
<td>This is best when you want to perform some testing and troubleshooting of the VM replica without affecting the production environment in any way.</td>
</tr>
</tbody>
</table>

**Note:** Veeam Backup & Replication supports failover and failback operations for one VM or for a number of VMs at the same time. If you have a problem with an ESXi host, you can restore its work with minimum downtime.

### 7.3.2. Failback

Veeam Backup & Replication streamlines and automates disaster recovery by providing replica failback capabilities.

**Failback** is the process of switching from the VM replica to the production VM. During failback, Veeam Backup & Replication uses the working replica to recover the original VM and switch back to it.

If you managed to restore the operation of the source host, you can switch back to the original VM on the source host. However, if the source host is not available, you can restore the original VM to a new location and switch back to it. Veeam Backup & Replication offers three failback options:

- Failback to a VM in the original location on the source host
- Failback to a VM that has been restored up-front from a backup in a new location
- Failback to an entirely new location by transferring all replica files to the selected destination
The first two options help you decrease recovery time and network traffic, as Veeam Backup & Replication will transfer only differences between the two VMs. The third option is used in cases when there is no way to use the original VM or restore the VM before performing failback.

During failback, Veeam Backup & Replication protects a running VM replica with a failback snapshot. The snapshot acts as a restore point and saves the pre-failback state of a replica to which you can return afterwards.

In Veeam Backup & Replication, failback is considered a temporary stage that should be further finalized. That is, after you test the recovered original VM and make sure it is running correctly, you should take another step to commit failback. However, while the replica is still in the failback state, you also have the option to undo failback and return the replica to the failover state.

<table>
<thead>
<tr>
<th>Commit failback</th>
<th>Undo failback</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scenario</strong></td>
<td>You want to finalize recovery of the original VM in the production site.</td>
</tr>
<tr>
<td><strong>Operations flow</strong></td>
<td>Veeam Backup &amp; Replication removes the protective snapshots and unlocks replica disk files. The original VM in the production site or at a new location starts to perform the role of the primary VM.</td>
</tr>
<tr>
<td><strong>VM replica state after the operation</strong></td>
<td>The VM replica returns to the normal state.</td>
</tr>
</tbody>
</table>

### 7.3.3. Failover Plan

If you have a number of VMs running interdependent applications, you need to failover them one by one, as a group. To do this automatically, you can prepare a failover plan.

In a failover plan, you set the order in which the VMs should be processed and the delay time needed to start each VM. The delay time helps to ensure that some VMs, such as a DNS server, are already running at the time the dependent VMs start.

The failover plan should be created in advance. In case the primary VM group goes offline, you start the corresponding failover plan manually. When you start the procedure, you can choose to fail over to the latest state of a replica or to any of its good known restore points.
Because failover is a temporary intermediate step that needs to be finalized, the finalizing options for a group failover are similar to a regular failover: undoing failover, permanent failover or failback.

If you decide to commit failover or failback, you need to process every VM individually, although you can undo failover for the whole group using the undo failover plan option.

Undoing the failover switches the replica back to the primary VM, discarding all changes that were made to the replica while it was running. When you undo group failover, Veeam Backup & Replication uses the list of VMs that were failed over during the last failover plan session and switches them back to the primary VMs. If some of the VMs were already failed back, manually by a user, they are skipped from processing.

### 7.3.4. Planned Failover

If you know that your primary VMs are going to go offline (e.g. you plan to have the production host patched), you can proactively switch the workload to their replicas. A **planned failover** is a smooth manual switch from a primary virtual machine to its replica with minimum interrupting in operation. You can use the planned failover, for example, to perform maintenance or software upgrades to the primary VMs, or in case you have an advance notice of a disaster approaching that will require taking the primary servers offline. When starting the planned failover:

1. The failover process triggers the replication job to perform an incremental backup and copy the un-replicated changes to the replica.
2. The VM is powered off.
3. The failover process triggers the replication job to perform another incremental backup run and copy the portion of last-minute changes to the replica. The replica becomes fully synchronized with the source VM.
4. The VM is failed over to its replica.
Because the procedure is designed to transfer the current workload to the replica, it does not suggest selecting a restore point to switch.

During the planned failover, Veeam Backup & Replication creates 2 helper restore points that are not deleted afterwards. These restore points will appear in the list of restore points for this VM; you can use them later to roll back to the necessary VM replica state.

When your primary host is online again, you can switch back to it. The finalizing options for a planned failover are similar to those of an unplanned failover: undoing failover, permanent failover or failback.
Labs for Module 7: Entire VM Recovery

You should now be able to use the methods covered in Module 7 to restore the entire VM with Veeam Backup & Replication in disaster recovery scenarios. Choosing from Instant VM Recovery or failing over to a VM replica, will depend on the situation. In the lab, we will simulate production failure by deleting some of the VMs from disk and then we will restore them, using previously created backups and replicas.

Get into the Lab

<table>
<thead>
<tr>
<th>Lab</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>Instant VM Recovery</td>
<td>Perform Instant VM Recovery to restore a VM directly from a backup in just a few clicks.</td>
</tr>
<tr>
<td>7.2</td>
<td>Full VM Recovery</td>
<td>Perform full VM recovery to distinguish the ways the full VM recovery option differs from Instant VM Recovery and what its use cases are.</td>
</tr>
<tr>
<td>7.3</td>
<td>Using Extract Utility</td>
<td>Restore a VM via Veeam Extract Utility to get acquainted with the ways you can use it in case of disaster or for troubleshooting.</td>
</tr>
<tr>
<td>7.4</td>
<td>Bringing Replica Back</td>
<td>Perform failover and failback, commit failback of a replica, undo failover to familiarize you with the various ways that you can utilize replicas for the disaster recovery or other scenarios.</td>
</tr>
<tr>
<td>7.5</td>
<td>Failover Plan</td>
<td>Configure and run a failover plan to failover a group of VMs running interdependent applications.</td>
</tr>
<tr>
<td>7.6</td>
<td>Perform Planned Failover</td>
<td>Perform a planned failover to minimize data loss and downtime when you know in advance you are going to need a failover.</td>
</tr>
</tbody>
</table>
8. Objects Recovery

There are plenty of situations when, instead of restoring an entire VM, you would prefer to recover an individual file or an individual application item from a backup file or replica to the most recent state or to any point in time in just a few seconds. In this module you will learn how to use the Veeam Backup & Replication features that allow file- and item-level restore.

8.1. Item-Level Recovery

Veeam Explorers allow the user to browse the database of a certain application and restore items to production without fully restoring the VM from the backup. This topic details each of the Veeam Explorers, and explains:

- The technical process behind the user interface
- The specifics and benefits of each Veeam Explorer

8.1.1. Restoring Microsoft Exchange, SQL, SharePoint and Active Directory Objects

Veeam Explorer for Exchange

Veeam Explorer for Microsoft Exchange is a free tool available to users of Veeam Backup & Replication. It allows you to browse Microsoft Exchange database files and restore necessary items, such as mailboxes, folders, messages, tasks, contacts and so on. Starting with version 8, Veeam Backup & Replication supports recovery of hard deleted items, including those from public folders and mailboxes, and recovery of items from/to Archive mailbox. Instead of fully restoring and starting the VM with the Microsoft Exchange Server, you can use Veeam Backup & Replication capabilities to extract the necessary Microsoft Exchange database from the backup file and then use Veeam Explorer for Exchange to browse and restore items.

You can use granular browsing and searching capabilities to find any item or a bunch of items stored in any number of Microsoft Exchange database files. Restore options include:

- Exporting mailbox folders and items as Personal Folder Files (.pst)
- Saving mailbox items as Microsoft Exchange Mail Documents (.msg)
- Sending mailbox items as attachments via email
- Restoring mailbox folders and items (available only with Veeam Backup & Replication Enterprise and Enterprise Plus Editions)
- Starting with version 8.0, Veeam supports recovery from/to Online Archive mailbox.
**Note:** Veeam Explorer for Exchange requires full access to Microsoft Exchange database files for item recovery. This level of access is usually granted to a very limited number of employees within the organization. If you would like to allow less privileged users to perform recovery of Microsoft Exchange items from backups, you can use the Application-Item Recovery (AIR) wizard for Microsoft Exchange.

Make sure Veeam Explorer for Microsoft Exchange is aware of the Extensible Storage Engine location. Extensible Storage Engine is required to access the Exchange mailbox database (.EDB). It runs as a special dynamic link library ese.dll supplied by Microsoft.

Specify path to the ese.dll in Veeam Explorer for Microsoft Exchange configuration settings:

1. In the Options window, open the Extensible Storage Engine tab.
2. Click Browse and specify the path to the ese.dll file. The file can be found on the Microsoft Exchange Server distribution CD at X:\Setup\ServerRoles\Common\ese.dll, or in the installation directory of Microsoft Exchange Server. For example:
   - for Microsoft Exchange 2010 default path is: %ProgramFiles%\Microsoft\Exchange Server\V14\Bin
   - for Microsoft Exchange 2013 and Microsoft Exchange 2016 default path is: %ProgramFiles%\Microsoft\Exchange Server\V15\Bin

**Veeam Explorer for SharePoint**

*Veeam Explorer for SharePoint* allows you to browse Microsoft SharePoint content and recover items (such as library documents, images, webpages and so on) without needing to fully restore and start the virtual machine hosting the SharePoint content database. Instead, you can use Veeam Backup & Replication data recovery options to quickly extract the necessary Microsoft SharePoint content database file (.MDF) from the virtualized server image-level backup, and then use Veeam Explorer for SharePoint to find and restore the Microsoft SharePoint documents you need.

Available with all editions of Veeam Backup & Replication, *Veeam Explorer for SharePoint* provides granular browsing and searching capabilities to find any item or a bunch of items stored in any number of Microsoft SharePoint content databases. You can save items/lists to a local folder or network drive, or send restored items as e-mail attachments.

With Veeam Backup & Replication Enterprise and Enterprise Plus edition, you can also use *Veeam Explorer for SharePoint* to restore Microsoft SharePoint items in the way you need; authorized users (for example, Microsoft SharePoint administrators) can also import content database files (exported by *Veeam Explorer for SharePoint*) to SharePoint database using PowerShell cmdlets.

**Note:** If there is a SharePoint server which has a database larger than 10GB, you’ll need fully functional (commercial) version of Microsoft SQL Server, Express version is not going to be able to mount this database.
Note: All of Veeam Explorers can be launched both from Veeam Backup & Replication UI and independently, from the server menu.

Veeam Explorer for Microsoft Active Directory

*Veeam Explorer for Microsoft Active Directory* is a new tool that extends the functionality of Veeam Backup & Replication, allowing you to browse Active Directory database and recover items (objects and containers) and their attributes from domain controller backup into production. For that, you do not need to fully restore and start the virtual machine hosting the domain controller. Instead, you can use Veeam Backup & Replication data recovery options to quickly extract the necessary Active Directory database file (.DIT) from the virtualized DC image-level backup, and then use Veeam Explorer for Microsoft Active Directory to find and restore the required objects:

- Use Veeam Explorer for Microsoft Active Directory granular browsing and searching capabilities to find any object/container stored in Active Directory database.
- Export objects/containers to a local folder or network drive.
- Restore them to the original or different location.

Note: Veeam Explorer for Microsoft Active Directory requires full access to Active Directory database files for item recovery. This level of access is usually granted to a very limited number of employees within the organization. If you would like to allow less privileged users to perform recovery of Active Directory objects from backups, you can use the Application-Item Recovery (AIR) wizard.

When viewing the backup in Veeam Explorer for Microsoft Active Directory browser, it’s possible to detect the attributes that were changed, moved, or deleted since the Active Directory backup via Compare with Original menu command that allows you to compare Active Directory objects in the backup with those in the production database.
Veeam Explorer for Microsoft SQL Server

Veeam Explorer for Microsoft SQL Server is a tool that extends the functionality of Veeam Backup & Replication, allowing you to view and recover databases from within Microsoft SQL server VM backup. For that, you do not need to fully restore and start the virtual machine hosting the SQL server. Instead, you can use Veeam Backup & Replication data recovery options to mount the selected restore point (image-level backup or replica) of the Microsoft SQL server VM to the Veeam backup server and then specify how you want your database to be restored. Veeam Explorer for Microsoft SQL Server offers the following capabilities:

- Browsing SQL server instances and databases
- Exporting the database to a local folder or network drive, including quick and easy 1-Click Export
- Restoring the database to the original server or different server
- Restoring SQL tables

Veeam supports database restore to the current restore point (that is, to the state when the backup or replica that is currently mounted to the Veeam backup server was created), restore to the certain point in time (transaction log replay will bring the database to the desired state), and restore to the state before selected transaction.

Note: Availability of these options depends on Microsoft SQL server VM logging and recovery settings and on the backup job settings. Consider that log backups are required to restore your database to the certain point in time or to a state before the selected transaction. Log files are copied from the repository to the Windows machine hosting the target SQL server, and log replay is performed to bring the database to the desired state. Log backups functionality is available in
Enterprise and Enterprise *Plus* version of Veeam Backup & Replication.

### SQL Server Logs Backup and Restore

For highly transactional servers and applications, many organizations need to back up both the application VM and its transaction logs in order to ensure recoverability to any point in time. Among such VMs there are, for example, Microsoft Exchange server and SQL server. Another important requirement is that backup process does not affect the production infrastructure.

Veeam Backup & Replication supports transaction log backups for the following systems:

- Microsoft SQL Server 2005
- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014

**Important!** To provide for recoverability of your SQL server, make sure that Full or Bulk-logged recovery model is enabled for that server. Then all the changes to the SQL server state will be written to transaction logs, and you will be able restore from any previous state backup to the current state by applying a sequence of logged transactions (*transaction log replay*).

You can specify the frequency at which you want your database transaction logs to be processed when setting up a job. In the backup repository, logs are stored as `.VLB` files (Veeam proprietary format) co-located with corresponding SQL server VM backups (`.VBK`, `.VIB`, `.VRB` files).

### Veeam Explorer for Oracle

*Veeam Explorer for Oracle* extends the functionality of Veeam Backup & Replication, allowing you to view and recover databases from within Oracle server VM backup. Veeam Explorer can restore databases from backups created by backup jobs, from imported backups and from storage. Both Windows-based and Linux-based VMs are supported.

For database-level recovery, you do not need to fully restore and start the virtual machine hosting your Oracle system. Instead, you can use Veeam recovery capabilities to mount the selected restore point of Oracle server VM to Veeam backup server and then specify how you want your database to be restored.

*Veeam Explorer for Oracle* offers the following capabilities:

- Browsing Oracle system hierarchy
- Restoring databases to the original server or different server, including quick and easy 1-Click Restore
- Veeam supports several database restore options:
  - To the current point in time (that is, to the moment when currently selected Oracle VM backup was created)
- To the selected point in time (here log replay will bring the database to the desired point)
- To the state before selected transaction

**Note:** Availability of these scenarios depends on Oracle database logging mode and on the VM backup.

Veeam Explorer for Oracle is installed together with Veeam backup server and management console or with the Standalone Console. The basic procedures of restoring Oracle database with Veeam Explorer for Oracle are very similar for restore to current restore point and for restore to point in time or selected transaction.

When restoring to the state as of selected restore point, the following takes place:

1. Administrator uses Veeam Backup & Replication console to initiate mount of Oracle VM file system from the backup stored in the repository.
2. Mount is performed using Veeam Mount Server associated with this repository. Typically, target (production) Oracle server is used as a staging system. When a VM is mounted to the specified server, c:\VeeamFLR folder is created on it.
3. Veeam Explorer for Oracle obtains Oracle system hierarchy information and presents it to user. A user chooses the database to restore and specifies target location (original or another server) and settings required to access that server. Database files are copied from the repository to the target machine, database is ‘re-created’ on the Oracle server and becomes ready for use.

**Note:** User account that you specify for guest processing of the Oracle VM in the backup job requires the SYSDBA rights on that Oracle system. For Linux system – the root account or account included in sudoers file can be used. During the restore process, this account will be automatically assigned privileges for database restore; after the restore process is finished, these privileges will be automatically recalled.

**Oracle Logs Backup and Restore**

Restore to the selected point in time or to the state before selected transaction requires Oracle transaction log replay, so make sure the backup was created with appropriate log processing settings:

- ARCHIVELOG mode is enabled for the Oracle database
- Transaction logs are not truncated due to VM backup job settings

**8.1.2. Universal Application-Item Recovery (U-AIR)**

For recovery of application objects, U-AIR leverages the vPower technology. It starts the application and all required components in an isolated virtual lab directly from compressed and deduplicated backup files. Once the VM is started, U-AIR provides transparent access to the backed up VM image through a proxy appliance that has visibility of both the virtual lab and production environment. Users can then extract the necessary application objects from the earlier VM images and bring them back to the production environment.
U-AIR does not require any special backups or additional tools – the application is started directly from the image-level backup file and users can restore application objects with the native management tools.

U-AIR offers a universal wizard, that is, Veeam Backup & Replication starts the application and all required components in the virtual lab so that users can connect to that application with the native management tools and restore items manually. U-AIR wizards are standalone components that can be installed and updated independent of the product. You can install U-AIR wizards on any machine in your production environment from which you plan to perform the restore process.

To perform the U-AIR process, you can follow a typical workflow or a simplified workflow. Note that in both cases you need your application group, virtual lab and SureBackup job configured.

<table>
<thead>
<tr>
<th>Typical Workflow</th>
<th>Simplified Workflow</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commonly, the restore procedure requires specific knowledge and is performed by application administrators or users working with applications. At the same time, management tasks are controlled by Veeam Backup administrators who know about all available resources in the backup infrastructure and user access permissions. For this reason, in the typical U-AIR workflow, two groups of users are engaged: - Users who need to restore specific items from applications - Veeam Backup administrators who work with Veeam Backup &amp; Replication and Veeam Backup Enterprise Manager. To help users who requested virtual labs manage their requests, Veeam Backup &amp; Replication offers a special tool – Virtual Lab Manager. Virtual Lab Manager runs on the machine from which the user sends the request and on which the user plans to perform application-item recovery.</td>
<td>If you plan to restore application items in a small environment or use U-AIR for evaluation purposes, you can use a simplified U-AIR workflow. In this case, you can skip the step of creating and approving the virtual lab request and immediately start working with the necessary U-AIR wizard. To be able to use simplified workflow, make sure that the necessary U-AIR wizard is installed on the Veeam Backup server, and that a corresponding SureBackup job is configured on that server.</td>
</tr>
</tbody>
</table>

Veeam Certified Engineer v9 . Textbook
The typical restore procedure includes the following steps:
1. The user who needs to restore an application item downloads the necessary U-AIR wizard and installs it on his or her machine. The user starts the U-AIR wizard and submits a virtual lab request. The submitted request is sent over to Veeam Backup Enterprise Manager and is registered there. (1)
2. The Veeam Backup Enterprise Manager Administrator receives an e-mail about a new lab request submitted by the user. The e-mail is sent automatically once a new request is registered at Veeam Backup Enterprise Manager. (1)
3. The Veeam Backup Enterprise Manager Administrator makes sure that the user who submitted the request is eligible to access application data from the corresponding backup.
4. The Veeam Backup Enterprise Manager Administrator approves or denies access to requested data using Veeam Backup Enterprise Manager. If the request is approved, the administrator uses the request approval wizard to select the necessary SureBackup job that should be started in order to create the required virtual lab. The SureBackup job that the administrator selects should be pre-configured on one of Veeam Backup servers connected to Veeam Backup Enterprise Manager. (2,3)
5. If necessary, the Administrator can manage virtual labs. For example, the Administrator can extend the time for the virtual lab lease or stop the lab leased by the user to let somebody else perform emergency restore using the same virtual lab.
6. Once the lab is ready, the user receives a notification from Virtual Lab Manager. (4)
7. The user can now start application-item recovery. If necessary, the user can extend the time for which the virtual lab should be running. (5)
8. After the recovery process is finished, the administrator can manually power off the virtual lab. If this does not happen, the virtual lab will be powered off automatically once the time for virtual lab lease is exceeded.

8.2. Guest OS File Recovery

The Guest OS File Recovery topics shows you how the guest VM OS files are restored by Veeam Backup & Replication depending on the operating system they belong to.

8.2.1. Guest OS File Recovery

With Veeam's Instant File-Level Recovery (IFLR), you can recover an individual file from a backup file or replica to the most recent state or to any point in time in just a few seconds. IFLR does not require you to extract a VM image to the local drive or to start up the VM prior to restore – you can recover
files directly from a regular image-level backup or replica.

IFLR is available for any virtualized file system, although, Veeam Backup & Replication provides different approaches for different file systems:

- For Windows-based VMs with NTFS, FAT and ReFS file systems, Veeam Backup & Replication uses built-in Windows file-level recovery.
- For the most commonly used file systems on Windows, Linux, Solaris, BSD, Novell Netware, Unix and Mac (OS X) machines, Veeam Backup & Replication offers multiOS file-level recovery.
- For any other file system, Veeam Backup & Replication enables you to leverage Instant VM Recovery to perform manual file-level recovery.

### 8.2.2. Windows File-Level Recovery

For FAT, NTFS and ReFS guest OS systems, Veeam Backup & Replication uses built-in file-level restore functionality.

When you perform file-level recovery, the VM image is not extracted from the backup file. The content of the backup file is mounted directly to the Veeam backup server and displayed in the built-in Veeam Backup Browser. For mounting file systems of VM guest OSs, Veeam Backup & Replication uses its proprietary driver. After that you can restore the necessary files and folders to the original location (and specify overwrite options in case the file exists in the target folder), copy them to your local machine drive, save them anywhere within the network or simply point any applications to the files and use them normally. The backup file (or replica) remains in read-only state no matter what you do.

### 8.2.3. Multi-OS File-Level Recovery

Because Windows cannot read other file systems natively, Veeam Backup & Replication additionally provides multiOS file-level recovery that allows reading data from different file systems:

<table>
<thead>
<tr>
<th>OS</th>
<th>Supported File Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>FAT</td>
</tr>
<tr>
<td></td>
<td>ReFS</td>
</tr>
<tr>
<td></td>
<td>NTFS</td>
</tr>
<tr>
<td>Linux</td>
<td>ext</td>
</tr>
<tr>
<td></td>
<td>ext2</td>
</tr>
<tr>
<td></td>
<td>ext3</td>
</tr>
<tr>
<td></td>
<td>ext4</td>
</tr>
<tr>
<td></td>
<td>ReiserFS</td>
</tr>
<tr>
<td></td>
<td>JFS</td>
</tr>
<tr>
<td></td>
<td>XFS</td>
</tr>
<tr>
<td></td>
<td>Btrfs</td>
</tr>
<tr>
<td>BSD</td>
<td>UFS</td>
</tr>
<tr>
<td></td>
<td>UFS2</td>
</tr>
</tbody>
</table>
### 8.2.4. File-Level Recovery for Any File System

With the vPower technology, Veeam extends its IFLR to any file system, not just Windows FAT, NTFS, ReFS and those restored with the multiOS file-level recovery wizard.

This type of file-level restore is not wizard-driven. You should leverage instant VM recovery to publish VMDK from a backup on the vPower NFS datastore (without actually starting the VM). With the VMDK files readily available, you can mount these VMDKs to any VM that can read the corresponding file system (including the original VM), and restore the required files using native OS file management tools. Alternatively, you can mount the VMDK to a Windows VM, and use a tool such as Portlock Explorer.

---

<table>
<thead>
<tr>
<th>OS</th>
<th>Supported File Systems</th>
</tr>
</thead>
</table>
| Mac | HFS  
HFS+ |
| Solaris | ZFS (up to pool version 23) |
| Novell Netware, Novell Open Enterprise Server | Novell Storage Services (NSS file/folder permissions are not restored). |

In addition to basic disks, MultiOS file-level recovery understands Linux LVM (Logical Volume Manager) and Windows LDM (Logical Disk Manager) partitions and ZFS pools.

MultiOS file-level recovery is a wizard-driven process. To restore files from a VM guest OS, Veeam Backup & Replication utilizes its patent-pending approach using a special FLR helper. The FLR helper is a virtual appliance running a stripped down Linux kernel that has a minimal set of components. The appliance is very small – around 20 MB and takes only 10 seconds to boot.

The FLR helper appliance is created directly on the selected Hyper-V host. Whenever you perform file-level restore, Veeam Backup & Replication automatically starts the appliance and mounts the VMDK files to the FLR appliance as virtual hard drives. VMDK files are mounted directly from backup files, without prior extraction of the backup content.

Once the restore process is complete, the wizard displays the file browser window, providing you with direct access to the VM file system. You can then copy the necessary files and folders to your local machine drive or save them anywhere within the network. Alternatively, you can allow users to restore files on their own through enabling an FTP server on the virtual appliance.

If you plan to restore VM guest OS files to their initial location, VMware Tools must be installed on the target VM.

**Tip:** When you perform recovery directly to a Linux host, you can recover files with correct permissions.
Labs for Module 8: Objects Recovery

A lot of daily disaster recoveries do not require an entire VM to be restored. Veeam Backup & Replication enables you to save time and network bandwidth by performing item-level and file-level restore. Try them on your own using the lab environment.

Get into the Lab

<table>
<thead>
<tr>
<th>Lab</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1</td>
<td>Perform Microsoft Exchange Items Recovery</td>
<td>Restore Microsoft Exchange items from the backups created with Veeam Backup &amp; Replication.</td>
</tr>
<tr>
<td>8.2</td>
<td>Perform Microsoft SharePoint Items Recovery</td>
<td>Restore Microsoft SharePoint items from the backups created with Veeam Backup &amp; Replication.</td>
</tr>
<tr>
<td>8.3</td>
<td>Perform Oracle Items Recovery</td>
<td>Restore Oracle items from the backups created with Veeam Backup &amp; Replication.</td>
</tr>
<tr>
<td>8.4</td>
<td>Perform Microsoft Active Directory Items Recovery</td>
<td>Restore Microsoft Active Directory items from the backups created with Veeam Backup &amp; Replication.</td>
</tr>
<tr>
<td>8.5</td>
<td>Perform Microsoft SQL Server Items Recovery</td>
<td>Restore Microsoft SQL server databases from the backups created with Veeam Backup &amp; Replication.</td>
</tr>
<tr>
<td>8.6</td>
<td>Guest Files Recovery</td>
<td>Restore Windows and Linux guest files.</td>
</tr>
</tbody>
</table>
9. Advanced Data Protection

At this point, you’ve learned most of the basic data protection and disaster recovery features of Veeam Backup & Replication. You are now able to perform backup and replication, verify it and restore entire VMs and granular objects, such as files, Exchange and SharePoint items, and some other options.

In addition to those crucial features, Veeam Backup & Replication provides a few more advanced options that allow you to comply with your data protection strategy while improving your RTPO to better protect your data and VMs.

9.1. Tape Device Support

With Veeam Backup & Replication, you can archive to tape both backup files created in backup repositories by a backup or a backup copy job, and regular files you might want to write to tape, such as Windows and Linux files. 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.

Veeam offers the following archiving options:

<table>
<thead>
<tr>
<th>Backup to tape jobs</th>
<th>Files to tape jobs</th>
</tr>
</thead>
<tbody>
<tr>
<td>This option allows you to archive to tape media backups created by Veeam Backup &amp; Replication. Using backup to tape jobs, you can implement the ‘3-2-1’ backup approach (3 copies, 2 types of media, 1 off-site location) considered as a best practice for data protection and disaster recovery. Veeam Backup &amp; Replication provides flexible retention and scheduling settings that help automate backup archiving. You can also archive Endpoint backups to tape.</td>
<td>This option allows you to archive to tape media files from Windows and Linux servers connected to the Veeam backup server. You can create both full and incremental backups of files on tape.</td>
</tr>
</tbody>
</table>

**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.

Veeam Backup & Replication uses the MTF (*Microsoft Tape Format*) industry format to write data to tape.

Veeam Backup & Replication offers multiple options for restoring data from tape:

| Restoring backup files from tape to disk | You can also restore full backups or even backup chains to a repository or any location of your choice. The restored backup is registered in the Veeam Backup & Replication console so that you can work with it and use it for any restore scenario later on. |

Veeam Certified Engineer v9 . Textbook
You can restore an entire VM from a backup archive on tape. Veeam Backup & Replication supports all options available for regular full VM recovery, including selecting a restore point, choosing a target location, changing VM configuration settings and so on.

Flexible recovery options allow you to recover files or folders back to the original location or another server, preserving ownership and access permissions.

To back up data to the tape media and restore from tape archives, Veeam Backup & Replication uses several components:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>The source is the initial location where backup files or regular files you want to archive to tape reside. This can be a backup repository where Veeam backups are stored or a Windows or Linux server hosting files that should be archived. Regular backup or backup copy job can also be leveraged as a source.</td>
</tr>
<tr>
<td>Data path</td>
<td>During archiving and restore processes, data is transferred between two terminal points. This process is controlled by two Veeam data mover services: - Source-side Data Mover Service communicates with the source (backup repository or server hosting the files) and initiates reading data from that source. - Target-side Data Mover Service runs locally on the Veeam backup server machine to which a tape device is connected; it initiates writing data to the tape device.</td>
</tr>
<tr>
<td>Veeam backup server</td>
<td>The core component in the backup infrastructure that manages all operations and schedules and executes the jobs.</td>
</tr>
<tr>
<td>Tape device</td>
<td>The tape device is a physical tape library, a virtual tape library or a stand-alone tape drive.</td>
</tr>
<tr>
<td>Tape server</td>
<td>The tape server is a network appliance that sits between data source and tape device and is used to create a communication channel and route traffic to tape devices – a Microsoft Windows server running the Data Mover Service. The Data Mover Service talks to the Veeam Backup server on one side and backup infrastructure components on the other side, and represents a communication point over which all data between the tape device and the backup repositories or file servers is transferred. All the drivers are installed on the machine that will perform the role of the tape server for the tape library to be visible.</td>
</tr>
</tbody>
</table>
## Component Description

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| Veeam backup database | This component is used to store the following tape-related data:  
- **Tape Catalog** stores files/folders archived to tape media, as well as VBK and VIB backup files. It is updated during file-to-tape and VM-to-tape jobs. The content of the Tape Catalog can be examined under the Tape node in the Files view.  
- **Backup Catalog** stores information about VMs whose backups were archived to tape media. The content of the Backup Catalog is updated during VM-to-tape jobs and can be examined under the Backups → Tape node in Backup & Replication view. |

---

To manage the tapes, Veeam Backup & Replication uses the following entities:

<table>
<thead>
<tr>
<th>Entity</th>
<th>Description</th>
</tr>
</thead>
</table>
| Media Pools  | Media pools are logical units that distribute free tapes for writing data and store information about data that was archived to them. To start archiving data, you must create and configure at least one media pool that will serve as a target for tape jobs. The following predefined media pools are available:  
- Free – a media pool containing empty tapes. You can use this media pool to replenish custom pools with new tapes when needed.  
- Unrecognized – a media pool containing tapes that were loaded to a tape device. They need further identification by a user which can be done by running the inventory or catalog job.  
- Imported – a media pool containing non-empty tapes. These are tapes identified by the tape catalog job.  
- Retired – a media pool containing retired tapes that reached the maximal number of re-writes. This media pool may also contain tapes with some mechanical breakdown.  
The Veeam GFS media pools are special media pools that store data to tape with the GFS, or the Grandfather-Father-Son backup storage scheme. |
| Media Sets    | Media sets are separate sets of tapes with data continuously written to them. Use media sets to split your tape archive into distinctly separated groups of tapes. |
| Backup Sets   | Backup sets are sets of files written to tape within one tape job session. |
| Media Vaults  | Media vaults are logical containers for visualizing data stored offline. Create and use media vaults for convenient managing of offline tapes. |
| Data Retention| Data retention is a user-defined period of time set to protect data from overwriting. When this period ends, the tape can be reused. |

In case you have a long chains of increments, for example, if you rarely use forever-incremental backup or create a full backup, restoring from tape may require loading a large number of tapes. To “split” the tape set into shorter series and streamline the restore process, you can schedule a virtual full backup for tape jobs (also referred to as virtual synthesized full backup). When you schedule synthetic full for tape, the tape job creates the synthetic full backup directly on tape and does not require disk space for storing additional full backup files on backup repositories. To create a virtual synthesized full backup, Veeam Backup & Replication uses a small temporary file of the .vsb (Veeam
Synthetic Backup) format. The .vsb file does not contain data blocks themselves; instead, it contains pointers to data blocks in restore points of the backup chain.

Generally, you use retention settings to set the overwrite protection period for tapes. The retention period is set for a media pool and is applied to all tapes that belong to this pool. However, some tapes may contain data for which you may want to set a longer protection. To do this, you can use tape protection. *Tape protection* is an option that sets an endless retention period for particular tapes selected by the user. The protection option overrides the retention settings of the media pool. You can single out tapes that, for example, contain particularly valuable data, and set the never overwrite retention period for them without modifying the settings of the media pool, which would affect other tapes. If the tape protection is no longer needed, it can be switched off at any time.

If your tape library has multiple drives, you can enable tape multistreaming. *Tape multistreaming* allows you to use several drives simultaneously for processing tape data. This option is useful if you have a lot of file to tape jobs running at the same time.

This option is enabled for custom media pools. You can set a maximum number of drives that a media pool can use simultaneously. Tape jobs occupy the allowed number of drives and process several file to tape jobs in parallel. For each drive, Veeam selects a tape with maximum free space and starts a new media set. Restore points that refer to one file are always written to one media set.

**Note:** You cannot set multistreaming for a GFS media pool.

### 9.1.1. Tape Job Encryption

Veeam Backup & Replication supports two types of *encryption* for tape media:

- **Hardware level:** Library- and driver-managed encryption mechanisms provided by the tape vendor
- **Software level:** The encryption mechanism provided by Veeam Backup & Replication

Hardware encryption has a higher priority. If hardware encryption is enabled for the tape media, Veeam Backup & Replication automatically disables its software encryption mechanism for such tape libraries. The Veeam encryption mechanism can only be used if hardware encryption is disabled at the tape device level or not supported.

To use the Veeam encryption mechanism, you need to enable encryption at the media pool level. Encryption is supported for both types of tape jobs: backup to tape jobs and file to tape jobs.

Backup to tape jobs allow double encryption. A backup to tape job uses a backup file as a source of data. If the backup file is encrypted with the initial backup job and the encryption option is enabled for the backup to tape job, too, so the resulting backup file will be encrypted twice. To decrypt such backup file, you will need to subsequently enter two passwords:

- Password for a backup to tape job
- Password for the primary backup job
9.2. SAN Storage Systems Support

This topic explores using image-based backups and replicas from storage snapshots, with little to no impact on your production environment. You will become acquainted with supported storage vendors and specifics for each of them.

9.2.1. SAN Storage Systems Support Overview

When Veeam Backup & Replication is used for VMware vSphere environments, you can take advantages of SAN storage snapshots to build your data protection and disaster recovery plan. Veeam Backup & Replication integrates with your SAN storage system and offers two technologies that will help you decrease impact of backup and replication operations on your production environment and significantly improve RPOs:

- **Backup from Storage Snapshots**: You can use storage snapshots to create backups and replicas of VMware VMs residing on SAN storage volumes. Backup from Storage Snapshots reduces the impact of VMware snapshot removal on the production environment.
- **Veeam Explorer for Storage Snapshots**: You can restore VMware VM data directly from storage snapshots. Veeam Explore for Storage Snapshots automates the process of VM data recovery and reduces recovery time in 10 times or even more. Restore options with Veeam Explorer for Storage Snapshots include:
  - Instant VM Recovery
  - VM guest OS files restore (Windows, Linux, FreeBSD and other)
  - Restore of Microsoft Exchange objects
  - Restore of Microsoft SharePoint objects
  - Restore of Microsoft SQL Server objects
  - Restore of Microsoft Active Directory objects

Without the use of storage snapshots, VM backup images must be created using VMware snapshots alone. When VMware snapshots are used to backup heavily utilized VMs, performance of the hosts, storage system, the VM, and its applications can be seriously impacted. With Backup from Storage Snapshots, the hypervisor snapshot is used briefly to create an application-consistent state for the storage snapshot. The hypervisor snapshot is then released after the storage snapshot is taken. This hardware-level storage snapshot then becomes the source of the VM backup, independent of the production VM.

The storage snapshot is read by a Veeam proxy as the backup source. The VM's CBT map is queried for fast incremental backup of quiesced VMs from the snapshot clone to disk without mounting the storage snapshot to the hypervisor or registering the VM with the host.

Veeam Backup & Replication supports the following storage systems:

- NetApp
- HPE 3PAR StoreServ 7000
- HPE StoreVirtual P4000 series and HPE StoreVirtual VSA (Virtual Storage Appliance)
- EMC VNX, VNX2 and VNxe
To create storage snapshots for backup and restore operations, Veeam Backup & Replication leverages native APIs and technologies provided by SAN storage vendors. The technologies and procedures of snapshot creation vary for different SAN storage systems.

### 9.2.2. HPE Storage Systems

For **HPE storage systems**, Veeam Backup & Replication uses the following technologies:

- Volume snapshot for Backup from Storage Snapshots on HPE StoreVirtual storage systems
- SmartClone for restore from storage snapshots on HPE StoreVirtual storage systems
- Virtual Copy for HPE StoreServ storage systems

Volume snapshots, SmartClones and VirtualCopies are created at the per-volume basis. They produce near instantaneous, point-in-time copies of volumes on which VM data is located. As a result, Veeam Backup & Replication can safely perform backup and restore operations without having to risk altering data on the production SAN storage or volume snapshot.

**Important!** The license for the HPE StoreServ storage system must support 3PAR Virtual Copy. Otherwise, you will not be able to perform backup and restore from storage snapshots.

### 9.2.3. NetApp Storage Systems

For **NetApp storage systems**, Veeam Backup & Replication uses the following NetApp technologies:
<table>
<thead>
<tr>
<th>Requirements</th>
<th>Backup from Storage Snapshots</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Traditional LUN Cloning</strong></td>
<td>Veeam Backup &amp; Replication first triggers NetApp to create a backing snapshot of the LUN that holds data for the necessary VM. After that, NetApp creates a clone of the LUN based on this backing snapshot.</td>
<td>In case of traditional LUN cloning, LUN clones created by Veeam Backup &amp; Replication may be locked or may fail to be deleted automatically by cleanup operations.</td>
</tr>
</tbody>
</table>
| - NetApp storage system works over iSCSI or FC.  
- NetApp storage system runs in the 7-mode.  
- The FlexClone license is not installed on the NetApp storage system. | | |
| **FlexClone** | Veeam Backup & Replication first triggers NetApp to create a base snapshot of the LUN that holds data for the necessary VM. After that, NetApp creates a FlexClone of the LUN based on this snapshot. | FlexClones can be created in seconds and require little space on the storage. Unlike traditional LUN clones, FlexClones are not coupled with backing volume snapshots and do not require you to manage these snapshots or delete them. |
| - NetApp storage system works over iSCSI or FC.  
- The FlexClone license is installed on the NetApp storage system. | | |
| **SnapRestore** | Veeam Backup & Replication triggers NetApp to create a clone of a LUN or NFS share via SnapRestore. To do that, NetApp restores LUN data to a new location on the volume where the original LUN or NFS share is located. As a result, a read-write copy of the LUN or NFS share holds VM data and can be used for backup and restore operations. | When you perform SnapRestore, NetApp does not physically copy data from the storage snapshots. Instead, it updates pointers to data blocks. As a result, the restore procedure is very fast and takes a few seconds to complete. |
| - The NetApp storage system runs over NFS.  
- The NetApp storage system runs in the C-mode over iSCSI or Fibre Channel and does not have the FlexClone license installed. | | |
### Requirements

<table>
<thead>
<tr>
<th>NFS share copying</th>
<th>The NetApp storage system runs over NFS.</th>
</tr>
</thead>
</table>

### Backup from Storage Snapshots

During the backup process, Veeam Backup & Replication creates a snapshot of a volume on which the NFS share with VM data resides. The created volume snapshot is used as a source of data.

### Considerations

To be able to restore data from storage systems running over NFS, you must have a SnapRestore/FlexClone license installed or the ndmp protocol enabled. In the opposite case, VM data processing will fail.

---

## Integration with NetApp SnapMirror and SnapVault

If the primary NetApp storage array is associated with a secondary array – NetApp SnapMirror and/or SnapVault, you can use the secondary storage array as a data source during backup. Backup from storage snapshots on NetApp SnapMirror or SnapVault reduces impact on the production storage. During backup, operations on VM data reading are performed on the side of NetApp SnapMirror or SnapVault, and the primary NetApp storage array is not affected.

To back up VMs from storage snapshots on NetApp SnapMirror and SnapVault, you must configure the backup job to build a snapshot chain on the secondary storage array and instruct Veeam Backup & Replication to use the created snapshots as a data source.

Before you perform backup from storage snapshots, check the following prerequisites:

- NetApp SnapMirror or SnapVault must be configured for the primary NetApp storage array where VMs that you plan to back up reside.
- A license for storage snapshot export must be installed on NetApp SnapMirror or SnapVault.
- For NetApp storage systems working over NFS, VMs that you plan to back up must not have VMware snapshots. VMs with VMware snapshots will be skipped from processing.
- A license for Veeam Backup & Replication Enterprise Plus edition must be installed on the backup server.
- A properly configured backup proxy must be added to the backup infrastructure. The backup proxy must have access to the backup server and secondary storage array.

The host with VMs whose disks are located on the storage system, the primary NetApp storage and NetApp SnapMirror/SnapVault must be added to Veeam Backup & Replication.

To configure backing up VMs from storage snapshots on NetApp SnapMirror and SnapVault at the Secondary Target step of the wizard, click Add and select NetApp SnapMirror or NetApp SnapVault. You may specify the number of storage snapshots that you want to maintain in the snapshot chain on the secondary storage in the **Number of snapshot copies to retain** field. When this number is exceeded, Veeam Backup & Replication will trigger NetApp to remove an earlier snapshot from the chain. Then select the **Use as the data source** check box.
9.2.4. EMC Storage Systems

EMC VNX, EMC VNX2 and EMC VNXe families of arrays are supported. This integration includes both the Veeam Explorer for Storage Snapshots recovery technique and Backup from Storage snapshots.

9.3. Support for Deduplicating Storage Systems

For disk-to-disk backups, you can use a deduplicating storage system as a target. Veeam Backup & Replication supports the following deduplicating storage appliances:

- EMC Data Domain
- ExaGrid
- HPE StoreOnce

9.3.1. ExaGrid

Veeam Backup & Replication lets you use ExaGrid deduplicating storage appliance as backup repository.

Veeam Backup & Replication works with ExaGrid as with a Linux-based backup repository: the backup repository architecture for the ExaGrid appliance resembles the Linux-based backup repository scenario. To communicate with ExaGrid, Veeam Backup & Replication deploys the Veeam data mover service on the ExaGrid appliance. The data mover (transport) service establishes a connection with the source-side Data Mover Service on the backup proxy and enables efficient data transfer over LAN or WAN.

**Important!** ExaGrid deduplicating appliances achieve less deduplication when multi-task processing takes place within a Veeam job: processing only a single task at a time within each Veeam backup job produces the best deduplication. If you decide to use ExaGrid as a backup repository, all tasks executed within a Veeam job should be processed sequentially, one by one – by limiting the maximum concurrent tasks (one task per VM disk) to 1 in the Veeam repositories used with ExaGrid appliances. To accomplish maximum ingest (hence shortest backup times), configure multiple Veeam backup jobs, each with its own Veeam repository; these jobs can then be scheduled to run concurrently.

9.3.2. HPE StoreOnce

You can use HPE StoreOnce storage appliances as a backup repository. Depending on the storage configuration and type of backup target, HPE StoreOnce can perform source-side or target-side data
deduplication.

<table>
<thead>
<tr>
<th>Source-Side Data Deduplication</th>
<th>Target-Side Data Deduplication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements</td>
<td>Requirements</td>
</tr>
<tr>
<td>- You have an HPE StoreOnce Catalyst license installed.</td>
<td>- You use a Catalyst store as a backup repository.</td>
</tr>
<tr>
<td>- You use a Catalyst store as a backup repository.</td>
<td>- The Catalyst store is configured to work in the Low Bandwidth mode.</td>
</tr>
<tr>
<td>Description</td>
<td>Description</td>
</tr>
<tr>
<td>To deduplicate data on the source side, HPE StoreOnce uses the HPE StoreOnce Catalyst agent. The HPE StoreOnce Catalyst agent is a component of the HPE StoreOnce Catalyst software; it is installed on the gateway server communicating with the HPE StoreOnce appliance. HPE StoreOnce deduplicates data on the source side before writing it to target. During the first backup job session, HPE StoreOnce analyzes data incoming to the HPE StoreOnce appliance in chunks and computes a hash value for every data chunk. Hash values are stored in an index on disk. During subsequent backup job sessions, the HPE StoreOnce Catalyst agent on the gateway server calculates hash values for data chunks in a new data flow and sends these hash values to target. HPE StoreOnce identifies which data blocks are already saved on disk, and the HPE StoreOnce Catalyst agent sends only unique data blocks to target. As a result, the load on the network reduces, the backup job performance improves and you can save on disk space.</td>
<td>During the first backup job session, HPE StoreOnce analyzes data incoming to the HPE StoreOnce appliance in chunks and creates a hash value for every data chunk. Hash values are stored in an index on the target side. During subsequent backup job sessions, HPE StoreOnce analyzes VM data transported to target and replaces identical data chunks with references to data chunks that are already saved on disk. As a result, only new data chunks are written to disk, which helps save on disk space.</td>
</tr>
<tr>
<td>Scheme</td>
<td>Scheme</td>
</tr>
<tr>
<td>![Gateway server diagram]</td>
<td>![Gateway server diagram]</td>
</tr>
<tr>
<td>![Gateway server diagram]</td>
<td>![Gateway server diagram]</td>
</tr>
<tr>
<td>How Veeam works with it</td>
<td>How Veeam works with it</td>
</tr>
<tr>
<td>For source-side deduplication, Veeam Backup &amp; Replication leverages the HPE StoreOnce Catalyst technology and two HPE StoreOnce components.</td>
<td>Veeam Backup &amp; Replication works with HPE StoreOnce as with a shared folder backup repository. To communicate with HPE StoreOnce, Veeam Backup &amp; Replication uses two Data Mover Services.</td>
</tr>
</tbody>
</table>

The gateway server is a backup infrastructure component that “bridges” the backup server and HPE StoreOnce storage system. The gateway server must meet the following requirements:

- The server must run a 64-bit version of Microsoft Windows.
- The server must be added to the backup infrastructure.
- The server must have access to the backup server and HPE StoreOnce appliance.
If you plan to use HPE StoreOnce as a backup repository, consider the following limitations:

- Backup files on HPE StoreOnce are locked exclusively by a job or task. If you start several tasks at a time, a task with a higher priority will terminate a task with a lower priority. In Veeam Backup & Replication, tasks have the following priority levels (starting with the top priority):
  - restore task → backup job → backup copy.
- The length of backup chains (chains that contain one full backup and a set of subsequent incremental backups) on HPE StoreOnce cannot be greater than 7 restore points. The recommended backup job schedule is the following: not more that 1 incremental backup once a day, not less than one full backup (active or synthetic) once a week.
- HPE StoreOnce does not support the reverse incremental backup method.
- When you create a backup job targeted at HPE StoreOnce, Veeam Backup & Replication will offer you the option to switch to optimized job settings and use the 4 MB size of data block for VM data processing. It is recommended that you use optimized job settings. Large data blocks produce a smaller metadata table that requires less memory and CPU resources to process.
- A gateway server working with HPE StoreOnce must run a 64-bit version of Microsoft Windows.
- The Catalyst store used as a backup repository must be configured to work in the Low Bandwidth mode (Secondary Transfer Policy). If the Catalyst store is configured to work in the High Bandwidth mode, HPE StoreOnce Catalyst will perform target-side deduplication instead of source-side deduplication.
- HPE StoreOnce cannot be used as a cloud repository.
- Catalyst stores and items cannot be added to the file copy jobs.

### 9.3.3. EMC Data Domain Boost

Veeam Backup & Replication provides support for *EMC Data Domain* storage systems with Data Domain Boost (DD Boost). The DD Boost technology offers a set of features for advanced backup.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Distributed Segment Processing | With Distributed Segment Processing enabled, operations on data segmentation, filtering and compression are performed on the side of the backup application. The Data Domain system receives only unique data blocks and writes them to disk. Distributed Segment Processing provides the following benefits:  
- Improved network throughput: only unique data blocks are transmitted across the network  
- Reduced backup window  
- Increased backup job performance |
| Advanced Load Balancing       | Advanced Load Balancing and Link Failover allow you to balance data transfer load and perform automatic link failover in case of network outage problems. |
| Link Failover                 | Virtual Synthetic Fulls lets you synthesize a full backup without physically copying data. To construct a full backup file, the Data Domain uses pointers to existing data segments on the storage system. Virtual Synthetic Fulls reduce the workload on the network and backup infrastructure components and increase the backup job performance. |
| Virtual Synthetics            | Managed File Replication is not supported.                                                                                                     |

To support the DD Boost technology, Veeam Backup & Replication leverages two EMC Data Domain components that communicate with each other:

- DD Boost server is a target-side component running on the Data Domain OS on the Data Domain storage system.
- DD Boost library is a source-side component integrated with Veeam Backup & Replication.

The DD Boost library is embedded into the Veeam Data Mover Service setup. When you add a Microsoft Windows server to Veeam Backup & Replication, the DD Boost Library is automatically installed on the added server with the Veeam Data Mover Service. To communicate with the Data Domain storage appliance, Veeam Backup & Replication uses the DD Boost library deployed on a **gateway server**. The gateway server is a proxying backup infrastructure component that "bridges" the Veeam backup server and the Data Domain storage system.
Veeam Backup & Replication supports EMC Data Domain storage systems working over the following protocols:

- **TCP/IP protocol:** Veeam Backup & Replication communicates with the EMC Data Domain server by sending commands over the network.
- **Fibre Channel protocol:** Veeam Backup & Replication communicates with the EMC Data Domain Fibre Channel server by sending SCSI commands over Fibre Channel. DD Boost is required to use Fiber Channel.

**Important!** The length of forward incremental and forever forward incremental backup chains that contain one full backup and a set of subsequent incremental backups cannot be greater than 60 restore points. To overcome this limitation, schedule full backups (active or synthetic) to split the backup chain into shorter series. For example, to perform backups at 30-minute intervals, 24 hours a day, you must schedule synthetic fulls every day. In this scenario, intervals immediately after midnight may be skipped due to the duration of synthetic processing. If the 60-points limit is exceeded, you will not be able to restore VM data from the backup chains.

When configuring backup jobs to land on the backup repository that supports EMC Data Domain Boost, the critical decision on backup jobs will be whether to do an active full backup or leverage synthetic full backups. For most environments, it is recommended to do synthetic full backups when leveraging EMC Data Domain Boost. This will save stress on primary storage for the vSphere and Hyper-V VMs and the Boost-enabled synthesizing is very fast.

If a Backup Copy job is going to be used and GFS retention (Monthly, Weekly, Quarterly and/or Annual restore points) implemented as well, the first consideration is to ensure that the gateway server is closest to the Data Domain server, since the Backup Copy job frequently involves an offsite transfer. When the Data Domain server is designated in the repository setup, ensure that consideration is given to the gateway server if it is being used off site as GFS transformations can leverage EMC Data Domain Boost for quicker processing during synthetic full backup file creation.

There are supplementary benefits to using DD Boost with Veeam Availability Suite that provide performance and resiliency improvements in other areas of the VM backup process. The first of these applies to VMs that may have multiple backup jobs and will land on the same DD Boost Storage Unit. The first time that VM is backed up with the first of the two (or more) jobs, it will function like a full backup as expected. The next time that VM is backed up with the second job, it will have to perform a
full backup as it is the first time the Veeam job is called. Because the first job has the bulk of the blocks of the vSphere or Hyper-V VM on the DD Boost Storage Unit, it will only need to transfer metadata and any possible changed blocks. This can be a significant improvement on the active full backup process when there is a fast source storage resource in place. Still, the time of recovery can be somewhat longer when using a deduplicating appliance due to the transform operations combined with deduplication.

Additionally when using EMC Data Domain Boost, there is Advanced Load Balancing and Link Failover for connectivity to the Data Domain server. When multiple network interfaces are in use, the Data Domain server will distribute connections from Veeam components over these links. This provides improved data transfer performance with Veeam jobs operating in parallel and additional resiliency by transparently switching failed links to active links if there is an interruption in connectivity.

9.4. Veeam Cloud Connect

Service providers (SP) can use Veeam Backup & Replication to deliver backup as a service (BaaS) to their customers (tenants). Veeam Backup & Replication lets SPs set up the cloud storage so that tenants can send their VM data offsite in an easy and secure way.

Veeam Backup & Replication does not create its own cloud for storing VM data. Instead, it uses SP storage resources to configure cloud repositories – storage locations in the cloud. Tenants who want to keep their data in the cloud can connect to the SP and write their VM backups to cloud repositories. Cloud repositories can be used as primary storage locations and secondary storage locations to follow the 3-2-1 backup strategy.

All data protection and disaster recovery tasks targeted at the cloud repository are performed by tenants on their own. Tenants set up necessary jobs and perform tasks using Veeam backup servers deployed on their side. Tenants can perform the following operations:

- Back up VMs to the cloud repository
- Copy VM backup files to the cloud repository
- Restore VM data from the cloud repository (Full VM, VM hard disk, VM files and VM guest OS files restore for Windows)
- Perform file copy operations between tenant’s side and the cloud repository (Manual operations only. Scheduled file copy jobs are not supported.)

Veeam Backup & Replication establishes a secure channel to transfer data to and from the cloud repository and offers data encryption capabilities to protect tenants’ data stored in the cloud.

![Diagram of Veeam cloud connect infrastructure]

<table>
<thead>
<tr>
<th>SP</th>
<th>Tenant</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Definition</strong></td>
<td>An organization that provides the cloud repository service to tenants</td>
</tr>
</tbody>
</table>
| **Roles** | - Configuring the Veeam cloud connect infrastructure as the environment needed to provide BaaS to tenants. As part of this process, the SP takes the following steps:  
- Decides what backup repositories must be used as cloud repositories  
- Sets up SSL certificates to enable secure communication in the Veeam cloud connect infrastructure  
- Creates cloud gateways.  
- Registers user accounts for tenants  
- Managing tenants’ accounts and data to ensure flawless work of the Veeam cloud connect infrastructure | - Connect to the Veeam cloud connect infrastructure to be able to use cloud repositories  
- Configure and run jobs and perform restore tasks targeted at cloud connect repositories |
| **Cloud connect components** | - SP Veeam backup server  
- Cloud repository  
- Cloud gateway (a network appliance that resides on the SP side and acts as a communication point in the cloud)  
- [Optional] Target WAN accelerator | - Tenant’s Veeam backup server  
- [Optional] Source WAN accelerator |
<table>
<thead>
<tr>
<th>SP</th>
<th>Tenant</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veeam license type</td>
<td>Cloud Connect Provider license</td>
</tr>
</tbody>
</table>

**Note:** Tenants can perform one backup or backup copy job and one restore task targeted at the cloud repository at time. Parallel processing is not supported. For example, if a tenant starts a backup job while another backup job is running, the second backup job will wait for the first one to complete and will run only after that.

### 9.4.1. Lease and Quota

When the SP configures a user account for a tenant, the SP assigns quota and, optionally, lease settings for the tenant. Lease and quota settings help the SP control how tenants consume storage resources on the cloud repository.

**Quota** is the amount of space (specified in GB or TB) assigned to one tenant on one cloud repository. It is a chunk of storage resources that the tenant can use for storing backups on the cloud repository. The SP can assign quotas on different cloud repositories to one tenant. A quota can be valid for indefinite time or can be restricted in time. To limit the quota lifetime, the SP must set a lease for the tenant.

**Lease** is a period of time for which tenants have access to their quotas on the cloud repository. The lease settings help the SP restrict for how long a tenant should be able to use cloud repository resources.

### 9.4.2. Licensing for Cloud Repositories

To enable the cloud repository functionality, the SP must install the *Cloud Connect* Provider license on the SP Veeam backup server. The cloud repository functionality is licensed per VM. The SP must obtain a license for the total number of VMs that all tenants working with this SP plan to back up.

The Cloud Connect Provider license is consumed only by active VMs. An active VM is a VM that has been successfully backed up or copied by an active (not disabled) tenant with an active lease period (if lease is set up). The number of restore points created by tenants or the number of jobs that process VMs do not consume the license. For example, if a tenant processes the same VM with several jobs, this VM is considered as 1 active VM.

The total number of active VMs must not exceed the total number of VMs in the license. Depending on the number of active VMs, the SP license can be in one of the following states:

- **Normal:** The total number of active VMs does not exceed the total number of VMs in the license. SP tenants can freely back up and copy existing and new VMs to the cloud repository.
- **Grace (valid for 7 days):** After the total number of active VMs exceeds the total number of VMs in the license, the license is put to the Grace state. Tenants can still back up and copy existing and new VMs to the cloud repository.
Can Backup Only Old Valid VMs: The total number of active VMs exceeds the total number of VMs in the license and the grace period has expired. Tenants can back up and copy only those VMs that have already been backed up and copied in the Normal state.

Recovery: During the Grace period, the SP may return to the license limits. This can happen if the SP can performs the following actions:

- Installs a new license for a greater number of VMs. The number of active VMs must not exceed the number of VMs in a new license.
- Reduces the number of active VMs (SP disables/removes a tenant or resets a storage quota for the tenant)

In this situation, the license it put to the Recovery state. Tenants can back up and copy existing and new VMs to the cloud repository.

9.4.3. v9 Cloud Connect Enhancements

Veeam Availability Suite v9 is bringing Veeam Cloud Connect Replication, a fast, secure cloud-based disaster recovery (DR) solution. DR is a great solution to increase the availability of modern datacenter, and does so by leveraging replication technologies and creating an off-site replica of virtual machines. When end users want to design and create a DR site, they are facing a problem: the capital expenses of building and maintaining the secondary site. In a second location, owned or rented, they need to deploy new hardware and software according to the size of their production environments, configure it and even manage it, virtually doubling their IT infrastructure efforts. Also, because production workloads are running for the most part within the primary site, the secondary one is rarely used, thus its cost it’s even higher when compared to its value.

This is the situation where a cloud-based solution fits perfectly. By renting resources from a service provider on a pay-as-you-go model, end users have the same final result (CPU, ram, storage and networking resources available for failover operations) without any capital costs and the burden of designing and deploying the DR site.
Furthermore, VM replication through Veeam Cloud Connect is easy-to-use and simple to set-up, there’s no need to set up and maintain VPN connections, or open multiple ports in firewall.

The end user, upon subscribing to the service and connecting to a service provider, will see a virtual cloud host, a multi-tenant view of the assigned DR site resources with CPU, RAM, storage and networking resource allocation. Basically, a cloud host serves as the replication target for the replication jobs set up by the end user. A service provider assigns a hardware plan to a tenant defines the CPU, memory, storage and network resources available to them.

Failover has multiple options:

- Full site failover
- Partial site failover. With that, end users are able to failover to the DR site just a part of their workloads, while other VMs will still be running in the production site. This advanced capability is available thanks to built-in network extension appliances that will simplify networking complexity and preserve communication between running VMs regardless of physical location.

Disaster recovery-as-a-service (DRaaS) is no doubt one of the most requested services by end users. With Veeam Cloud Connect Replication, service providers have a complete solution to quickly create and deliver DRaaS services for VMware vSphere and Microsoft Hyper-V environments. The software, thanks to its native multi-tenancy capabilities, allows a complete isolation of end users hosted on the same hardware, as well as built-in network connectivity management for all failover types – all without the need to license, learn and maintain any additional 3rd party software.

There are a few more essentials pieces:

- Ease of use: once end users register a service provider, they will see the new virtual host added to their B&R. Replicating VMs to the service provider’s infrastructure is similar to setting up a replication job pointing to this cloud host as the target.
- Ease of networking configuration. The Network Extension appliances preserve communications with and between running replica VMs during full and partial failovers regardless of their location – without having to make any changes to replica TCP/IP settings before, during or after failover.
• Fully automated upgrade of network extensions appliances with product updates installation.
• Bandwidth-friendliness. Seeding, compression, replication from backup, Built-in WAN Acceleration are all provided as a part of Cloud Connect Replication to allow customers with slow or unreliable WAN connections, or large amounts of data, to protect their workloads with RPOs that was never before possible with their available bandwidth.
• Self-service. This is critical to any cloud service, and Veeam Cloud Connect is not an exception. A web portal is offered, running at the service provider and accessible to the end user from any device and from any location. Using this portal, the end user is able to login and start any failover plan on their own, without requiring any intervention from the service provider.

9.5. Veeam Backup Enterprise Manager

Veeam Backup Enterprise Manager implements security by limiting access to web management website features and data based on user roles. This empowers administrators to delegate permissions in a very granular way, on an as-needed basis, to the individuals who will complete the restore process. It is possible, for example, to delegate permissions to recover files without actually being able to see the contents of the files. Delegations can be made to users which allows for recovery across the virtual spectrum from individual files all the way through to the recovery of the entire VM.

9.5.1. Required Permissions

To be able to log in to the Veeam Backup Enterprise Manager website, the user must be assigned either the Portal Administrator, Restore Operator or Portal User role.

• Portal Administrators have full access to all administrative functions and configuration settings; they can browse, search and restore all VMs (please note that such actions as Instant VM Recovery and restores from the replica are not available though), files, and application items.
• The Configuration area is not accessible to Restore Operators and Portal Users.
• Portal Users and Restore Operators can access their restore scope – a list of VMs that can be recovered by appropriate personnel. For example, database administrators can restore database servers (SQL, Oracle, or other) – this is their restore scope. Exchange administrators’ restore scope will include Exchange server VM, and so on. Depending on the role configuration, non-administrative users can access the VMs and/or Files tab of Enterprise Manager website.

Important! Restore scope (list of available VMs) can be customized if you have Enterprise Plus edition of Veeam Backup & Replication. In other editions, this list includes all VMs and cannot be customized. However, you can delegate recovery of entire VMs, guest files, or selected file types.

• Restore Operators can access VMs from their restore scope in VMs and/or Files tab and perform restore operations as permitted by their settings.
• Portal Users can access VMs from their restore scope in VMs and/or Files tab, as well as reports for these VMs; they also can perform restore operations as permitted by their settings.
9.5.2. Restore of Application Items

Now authorized personnel, for example, restore operators at Help Desk, can restore the necessary Exchange items (emails, tasks, calendars) and the necessary SQL databases from backups created with Veeam Backup & Replication using Enterprise Manager.

**Note:** To recover items from your Exchange or SQL database, make sure you have an application-consistent backup (with VSS enabled) of your server VM. Also, if you plan to restore the SQL database to a certain point in time (not necessarily the restore point), then transaction log processing should be configured as described in Truncation of transaction logs section.

<table>
<thead>
<tr>
<th>Exchange items</th>
<th>SQL items</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role that needs to be assigned to a responsible user</td>
<td>At least Restore Operator</td>
</tr>
<tr>
<td>Permissions that need to be assigned to a corresponding user</td>
<td>Exchange Administrator rights and Administrator rights for all mailboxes</td>
</tr>
</tbody>
</table>

**Note:** If your organization’s policy does not allow for administrative rights assignment to restore operators, it is recommended that Application Item Restore wizard (U-AIR) is used.

9.5.3. Self-restore portal

Veeam Backup Enterprise Manager allows users with local administrative rights for infrastructure VMs to browse, search and restore guest OS files within restore points of the those VMs. This capability is supported by Veeam’s runtime process, which perform guest system indexing and also identifies local administrative accounts.

This approach streamlines delegation of restore capabilities: Instead of multiple role assignments and restore scope fine-tuning, the Enterprise Manager administrator can simply provide users with a link to web UI displaying exactly the controls required for file-level restore of their VMs. Communication with that personalized web page is performed using HTTPS or HTTP.

Enterprise Managers can access both the *Enterprise Manager web UI* and the *self-restore page*. All other users will be forwarded to the self-restore page upon the login.

9.5.4. Managing Encryption Keys

Enterprise Manager keys help you to restore encrypted data in case of a lost or forgotten password used for encryption. For safety’s sake, it is recommended to periodically generate new Enterprise Manager keys for the encryption process. Regularly changing the encryption keys raises the encryption security level.

When you create new Enterprise Manager keys, Veeam Backup Enterprise Manager generates a
keyset of two matching keys:

- *Public Enterprise Manager* key that encrypts storage keys on Veeam backup servers connected to Veeam Backup Enterprise Manager
- *Private Enterprise Manager* key that decrypts storage keys in case a password for encrypted backup or tape is lost

Enterprise Manager keys are created in the inactive state. To make the keys active and use them for encryption and decryption, you need to activate the keys.

In some cases, government regulations and internal company policies require that you regularly change encryption keys. The shorter the lifetime of an encryption key, the smaller the amount of data encrypted with that key. And the smaller the amount of data encrypted with a single encryption key, the higher the level of encryption security.

The lifetime of Enterprise Manager keys is controlled by a *key retention period*. The key retention period defines for how long Enterprise Manager keys must remain in effect and used for encryption and decryption.

You can specify a retention period for an Enterprise Manager keyset. Once the retention period is over, the keyset is marked as inactive and is no longer used for encryption or decryption.

It is important to regularly back up your Enterprise Manager keys or save their copies in a safe place. If you lose a password for an encrypted backup or tape, you can unlock this backup or tape with the private Enterprise Manager key and the Enterprise Keys Restore wizard.

However, in some situations, a matching private Enterprise Manager key may be not available. This can happen, for example, if your Veeam Backup Enterprise Manager database has failed or you use a new installation of Veeam Backup Enterprise Manager and a new database. In this case, Veeam Backup Enterprise Manager will not find a matching private Enterprise Manager key in the database and will be unable to unlock the backup or tape encrypted with the public Enterprise Manager key.

You can create a backup copy of an Enterprise Manager keyset with the export operation in Veeam Backup Enterprise Manager. The exported keyset is saved as a PEM file and contains private and public Enterprise Manager keys. You can save the exported keyset on the local disk or on a network share. An exported keyset can be imported back to Veeam Backup Enterprise Manager any time you need.

*Important!* Create backup copies of Enterprise Manager keysets and keep them in a safe place. If your installation of Veeam Backup Enterprise Manager goes down for some reason, you will lose private Enterprise Manager keys. As a result, you will not be able to use the Veeam Backup Enterprise Manager functionality to recover data from backups and tapes.

### 9.5.5. Decrypting Data without a Password

If you have lost or forgotten a password, you can unlock an encrypted file with the help of Veeam
Backup Enterprise Manager.

You can restore data without a password only if your backup infrastructure meets the following requirements:

2. The Veeam backup server on which you encrypted the data are added to Veeam Backup Enterprise Manager.
3. The Veeam backup server on which you generated a request for data decryption is added to Veeam Backup Enterprise Manager.

To decrypt data without a password, connect the Veeam backup servers to Veeam Backup Enterprise Manager. In this case, Veeam Backup & Replication will employ Enterprise Manager keys in the encryption process, which will let you recover data from encrypted backups and tapes even if the password is lost or forgotten.

9.5.6. Veeam Backup Enterprise Manager RESTful API

Veeam Backup Enterprise Manager exposes its objects via the Web Service API based on the REST (Representational State Transfer) framework. Veeam Backup Enterprise Manager RESTful API lets developers communicate with Veeam Backup Enterprise Manager to query information about objects and perform basic operations with them using HTTP and HTTPS protocols and the principles of REST. Since the HTTP protocol is very popular and widespread, REST API is platform-agnostic and can be used with practically any programming language.

REST API relies on the client-server model:

1. The client makes requests to the server, Veeam Backup Enterprise Manager, over the HTTP protocol.
2. The server processes the request and returns either a successful operation status or error. In case of success, the server returns a response in the form of an XML document.
3. The client accepts the response, parses it and retrieves the information it needs from the response.

To work with Veeam Backup Enterprise Manager RESTful API, you can use any browser or client application that supports HTTP and HTTPS protocols.

Veeam Backup Enterprise Manager additionally offers its own client, Veeam Backup Enterprise Manager Web Client that you can use to evaluate and test capabilities of Veeam Backup Enterprise
Manager RESTful API. Veeam Backup Enterprise Manager Web Client is a web-based client. It can be accessed via the Internet browser on the machine where Veeam Backup Enterprise Manager is installed by the following URL:
http://<enterprise-manager>:9399/web

### 9.6. Standalone Console

**Veeam Backup & Replication Console** is a separate client-side part that allows you to access Veeam backup server. You can use the console locally, or install it in a standalone mode on a device running Microsoft Windows to access Veeam Backup & Replication remotely over the network. The console logs you in to Veeam Backup & Replication, allowing you to perform all kind of operations.

You can install as many standalone consoles as you need so that multiple users can access Veeam simultaneously. The number of multiple connections is not limited, however a maximum of 3 to 4 simultaneous sessions are recommended.

The client side provides remote access and remote PowerShell capabilities. It also acts as a **restore proxy** in remote restore scenarios that involve mounting of backups locally.

**Important!** To log in to Veeam Backup & Replication via the console, the user must be added to the Local Users group on the backup server or a group of domain users who have access to the backup server. The user can perform the scope of operations permitted by his or her role in Veeam Backup & Replication.

For each session, the Veeam backup service generates an authentication token that contains the user's permissions. Veeam uses the token to authenticate the user for each request to the server and to check their permissions.

Multiple users can work with Veeam Backup & Replication simultaneously. When multiple users need to access the Veeam database concurrently, Veeam preserves database records from being modified simultaneously on the following events:

- Modifying infrastructure.
- Modifying credentials.
- Modifying a job.

For example if user A modified a job and successfully saved it while it was open for modification by user B, when user B will try to save her modifications, a warning message prompting to reopen the job for modification will appear.

The Veeam Backup & Replication console has no direct access to the backup infrastructure components or Veeam database. It communicates with Veeam Backup & Replication via the Veeam backup service.

For each session, Veeam creates a satellite process that maintains the connection. If the connection fails, the satellite is able to reconnect to the server within 5 minutes without additional logging. The Veeam backup service acts as a router for satellites.
9.7. vCloud Director Support

Backup and restore of vCloud Director vApps and VMs has always been a hot topic. Up to now, backup tools offered no backup option in the vCloud Director environment. The only way was to perform backup at the level of the underlying vCenter Server. For restore, the administrators would first need to restore VMs to the vCenter Server level and then import them to vCloud Director.

Veeam Backup & Replication provides support for vCloud Director. It uses vCloud Director API to help you back up vApps and VMs and restore them directly to the vCloud Director hierarchy.

The main entity with which Veeam Backup & Replication works during backup is a vApp. A vApp is a virtual system that contains one or more individual VMs along with parameters that define operational details – vApp metadata. When Veeam Backup & Replication performs a backup of VMs, it captures not only data from the VMs, but also vApp metadata.

As a result, you can restore vCloud Director objects back to the vCloud Director hierarchy and do not need to perform any additional actions on import and VM configuration.
Labs for Module 9: Advanced Data Protection

At this point, you’ve learned most of the basic data protection and disaster recovery features of Veeam Backup & Replication. You are now able to perform backup and replication, verify it and restore entire VMs and granular objects, such as files, Microsoft Exchange, Oracle, Microsoft Active Directory, Microsoft SQL Server and Microsoft SharePoint items.

In addition to those crucial features, Veeam Backup & Replication provides a few more advanced options that allow you to comply with your data protection strategy while improving your RTPO to better protect your data and VMs. The next set of labs provides you with hands-on experience on taking your backups off site to tape, advanced integration with SAN storage arrays, Veeam Backup Enterprise Manager, Veeam Backup & Replication Standalone Console and Veeam PowerShell Snap-In.

Get into the Lab

<table>
<thead>
<tr>
<th>Lab</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1</td>
<td>Working with SAN Storage Snapshot</td>
<td>Configure a SAN storage so that backup and restore using SAN snapshots can be used.</td>
</tr>
<tr>
<td>9.2</td>
<td>Using Backup to Tape</td>
<td>Connect a tape device to your Veeam Backup &amp; Replication installation. Create a backup job to get backups offsite.</td>
</tr>
<tr>
<td>9.3</td>
<td>Configuring Hyper-V Backup to Run in Off-host Mode</td>
<td>Add an off-host proxy so that the load of data processing is taken from the Hyper-V host.</td>
</tr>
<tr>
<td>9.4</td>
<td>Working with Veeam Backup Enterprise Manager</td>
<td>Review the capabilities of Veeam Backup Enterprise Manager and try them out.</td>
</tr>
<tr>
<td>9.5</td>
<td>Standalone Console</td>
<td>Install Veeam Backup &amp; Replication Standalone Console.</td>
</tr>
<tr>
<td>9.6</td>
<td>Veeam Configuration Backup and Restore</td>
<td>Backup Veeam server configuration and perform a configuration restore using a Migrate scenario to copy infrastructure configuration from one Veeam Backup &amp; Replication server to another.</td>
</tr>
<tr>
<td>9.7</td>
<td>Introducing Veeam PowerShell Snap-In</td>
<td>Operate the product through PowerShell cmdlets.</td>
</tr>
</tbody>
</table>
10. Veeam ONE Features and Functionality

Veeam ONE is a management solution for virtual environments of any scale and complexity. It delivers real-time monitoring on health and performance of virtual environments, helps analyze the efficiency of data protection implemented with Veeam Backup & Replication, provides intelligent reporting and offers business-based views of the virtual infrastructure topology to simplify management and expedite decision-making.

10.1. Introduction to Veeam ONE

Veeam ONE incorporates three components:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veeam ONE Monitor</td>
<td>Veeam ONE Monitor is the primary tool used for monitoring your virtual environment and Veeam Backup &amp; Replication infrastructure. In the Veeam ONE Monitor console, you can manage, view and interact with alarms and monitoring data as well as analyze performance of virtual infrastructure and backup infrastructure components. You can also keep an eye on the efficiency of data protection operations and troubleshoot issues that occur in your virtual environment, generate reports, and administer monitoring settings.</td>
</tr>
<tr>
<td>Veeam ONE Reporter</td>
<td>Veeam ONE Reporter helps you verify configuration issues, optimize resource allocation and utilization, and track implemented changes. You can also plan capacity growth and track whether mission-critical VMs are properly protected in the virtualized datacenter.</td>
</tr>
<tr>
<td>Veeam ONE Business View</td>
<td>Veeam ONE Business View allows you to group your virtual infrastructure objects into categories like SLA, business unit, purpose, or configuration entity. Your business categorization model is further applied to the monitoring and reporting functionality to simplify management and ensure transparency of operations for your business across large virtual environments.</td>
</tr>
</tbody>
</table>

10.2. Auto Discovery of Backup and Virtual Infrastructure

To allow Veeam ONE to collect information about your virtual infrastructure and track the efficiency of VM data protection, you need to connect to VMware, vCloud Director or Hyper-V virtual management servers and Veeam backup servers. You can connect to servers either during installation or configure connections later via the Veeam ONE Monitor console. Configured connection settings are automatically propagated to all Veeam ONE components.

For example: If you connect a vCenter Server to Veeam ONE Monitor, it automatically becomes available in Veeam ONE Reporter and Veeam ONE Business View. Therefore, there’s no need to configure connections to virtual servers and backup servers for every Veeam ONE component individually.

When you:
- Change connection settings for a server, the changes are adapted across all components.
- Remove a server from Veeam ONE Monitor, Veeam ONE automatically removes the server connection from all other components.

Veeam ONE provides a convenient way of gathering data from VMware vSphere servers, vCloud Director servers, SCVMM servers, failover clusters, Hyper-V hosts and Veeam backup servers. You can choose to collect data periodically according to the defined schedule or run data collection manually. Veeam ONE collects data agentlessly, putting no additional load on virtual servers. Veeam ONE leverages built-in monitoring means: it uses network connection to get data via a set of API calls and OS subsystems.

Retrieved data is stored to the SQL database. You can choose the necessary point in time to generate reports that describe the state of the virtual infrastructure and data protection activities at the chosen moment in the past.

10.3. Veeam ONE components

Veeam ONE Reporter and Veeam ONE Monitor integrate with Veeam ONE Business View out of the box. Veeam ONE Business View categorization model and category values assigned to virtual infrastructure objects are stored to the shared Veeam ONE database. Veeam ONE Monitor and Veeam ONE Reporter access and use this data for business-oriented monitoring and reporting. Therefore, you don’t need to perform any additional steps for Veeam ONE components integration.

10.3.1. Monitoring and Alerting

Veeam ONE Monitor – a part of an integrated Veeam ONE solution – is the primary tool for monitoring your VMware and Microsoft Hyper-V environment and Veeam Backup & Replication infrastructure. With Veeam ONE Monitor, you can manage, view and interact with alarms and monitoring data, analyze performance of virtual infrastructure objects, keep an eye on the efficiency of data protection implemented with Veeam Backup & Replication, generate reports and administer monitoring settings. Veeam ONE Monitor provides complete visibility of your virtual and backup infrastructure and helps you speed up troubleshooting and quickly isolate root causes of performance issues before users and services are affected.

Veeam ONE Monitor features the following functionality:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration with Veeam Backup &amp; Replication</td>
<td>Veeam ONE Monitor offers advanced possibilities for monitoring the efficiency of VM data protection in your virtual environment. Veeam ONE Monitor collects real-time statistics from connected Veeam backup servers and allows you to quickly review the latest status of backup, replication, SureBackup, backup copy and backup to tape jobs. You can also examine configuration and performance of your backup infrastructure components and instantaneously react to potentially dangerous situations with VM data protection.</td>
</tr>
<tr>
<td>Feature Description</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Support for heterogeneous virtual environments</strong></td>
<td>Veeam ONE Monitor is designed for professional use in Microsoft Hyper-V and VMware vSphere virtual environments. Monitoring and alerting capabilities for Microsoft Hyper-V and VMware vSphere virtual environments are available from a single console, which eliminates the need to deploy and use multiple monitoring solutions for adopted virtualization platforms.</td>
</tr>
<tr>
<td><strong>Support for SCVMM, failover clusters and hosts</strong></td>
<td>Veeam ONE Monitor allows you to gather monitoring information from large virtual deployments with multiple SCVMM servers, failover clusters and standalone hosts.</td>
</tr>
<tr>
<td><strong>Integrated or standalone monitoring</strong></td>
<td>Veeam ONE Monitor connects to SCVMM and failover clusters to provide you with cluster-aware monitoring of your virtual machines. If a VM is moved to another server in the cluster by means of Live Migration or manually, Veeam ONE Monitor will continue gathering performance data from it. Veeam ONE Monitor allows you to gather monitoring information from large virtual deployments with multiple SCVMM servers or failover clusters – all from a single console. For small datacenters or development labs running without SCVMM or failover clusters, Veeam ONE Monitor can provide monitoring, alerting and reporting for multiple standalone hosts.</td>
</tr>
<tr>
<td><strong>Client/Server architecture</strong></td>
<td>Veeam ONE Monitor supports multi-admin access to performance data without affecting virtual environment performance or changing the access policy. It agentlessly gathers all performance information into a Microsoft SQL Server database, allowing users to access infrastructure-wide performance data as needed.</td>
</tr>
<tr>
<td><strong>Alarms</strong></td>
<td>With Veeam ONE Monitor alarms, you can easily set up email notifications and SNMP traps or run custom notification scripts for important events such as VM power off, CPU utilization level excess, and so on. SNMP traps can be used to feed alarm data into other popular system monitors, such as CA Unicenter, BMC Patrol, IBM Tivoli or HPE OpenView. Alarm modelling allows you to estimate the number of alarms that you will receive and adjust alarms settings in case important information is not received or too many false positive alarms are triggered. Alarm suppressing makes it possible to eliminate sending multiple alarms during specific activities in your virtual infrastructure (for example, backup).</td>
</tr>
<tr>
<td><strong>Advanced monitoring options</strong></td>
<td>To provide enhanced control over the virtual environment, Veeam ONE Monitor features a number of advanced monitoring options: viewing and managing in-guest processes and services running on a host or VM and logging on to the VM console directly from Veeam ONE Monitor.</td>
</tr>
<tr>
<td><strong>CSV, SMB and local storage monitoring</strong></td>
<td>Veeam ONE Monitor keeps you aware of the local storage, Cluster Shared Volumes (CSV) and SMB file shares state. To trace the storage state, it uses specific alarms, reports and charts. Direct and indirect CSV workloads are differentiated in charts to help you understand the impact of each type of workload on a datastore and determine whether an issue is hardware- or configuration-based.</td>
</tr>
</tbody>
</table>
### Feature Description

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Historical reports</td>
<td>To obtain a point-in-time view of your virtual environment, you can create reports right from the Veeam ONE Monitor console. With a couple of clicks, you can generate HTML reports that describe your virtual infrastructure, summarize performance statistics and help you analyze the efficiency of data protection in your virtual environment. If you need to create reports with custom parameters, you can easily switch to the Veeam ONE Reporter console.</td>
</tr>
<tr>
<td>Business view categorization</td>
<td>Veeam ONE Monitor enables both technical- and business-oriented monitoring of the virtual infrastructure. It uses categorization data from Veeam ONE Business View to build a business topology of your virtual infrastructure and provide you with a possibility to monitor and alert of your environment presented in business terms.</td>
</tr>
</tbody>
</table>

With *Veeam ONE Monitor*, you can configure and use alarms that will inform you about important events and changes in your virtual environment. The ability to be alerted of changes in your virtual environment allows for faster response to critical issues and helps to maintain the overall health of the virtual infrastructure.

Out of the box, Veeam ONE Monitor comes with a set of predefined alarms including:

- 150+ predefined alarms for monitoring VMware vSphere environments and vCloud Director operations framework. Predefined alarms are based on best practices for a common virtual environment.
- Veeam Backup & Replication alarms that alert on connection status of backup infrastructure components, job state and duration, insufficient space on backup repositories, and Veeam Backup & Replication license issues.
- Internal alarms that alert on data collection issues, problems with connection to virtual servers, insufficient space for Veeam ONE database, and license concerns.

All predefined alarms include an extensive knowledge base. When a problem occurs, you will not only be alerted, but will also have all the necessary information for troubleshooting and finding the root cause of the issue.

Depending on your requirements to the virtual environment, you can adjust settings of predefined alarms, or create new alarms that will analyze performance and alert on errors at any level of the virtual infrastructure. Veeam ONE Monitor offers an extensive set of rules and different severity levels, allowing you to create your own elaborate alarm model.

### 10.3.2. Reporting and Dashboards

*Veeam ONE Reporter* – part of an integrated Veeam ONE solution – is designed for documenting and reporting on your Veeam Backup & Replication infrastructure and virtual environment. Veeam ONE Reporter allows you to automatically discover and collect information about your VMware vSphere, vCloud Director environment, its components, configuration settings, performance and track the efficiency of data protection performed with Veeam Backup & Replication. Veeam ONE Reporter offers comprehensive visual reports and dashboards for documentation, analysis, decision-making, change tracking, capacity planning and optimization of resource utilization.
**Veeam ONE Monitor** also offers a set of summary dashboards for monitoring your virtual environment and data protection infrastructure. Summary dashboards serve as the "launch point" for monitoring and troubleshooting. They show the summary of health state, list the most recent alarms and highlight key performance and configuration metrics in a single view. Summary dashboards are particularly helpful if you want to quickly check the overall health and reveal hotspots in your environment.

Virtual infrastructure Summary dashboards are the start-off point for monitoring your virtual environment. The dashboards reflect the aggregate health state for all components at a specific level of your virtual infrastructure and show summary details for a selected virtual infrastructure object:

- Virtual Infrastructure Summary
- Host Summary
- Virtual Machine Summary
- Local Storage Summary
- SMB Share Summary
- Cluster Shared Volume Summary

The Veeam ONE Reporter reports can be launched within the Veeam ONE Monitor interface. The following reports are among ones available with **Veeam ONE Reporter**:

<table>
<thead>
<tr>
<th>Report Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Inventory</td>
<td>Provides inventory information for your Veeam Backup &amp; Replication infrastructure</td>
</tr>
<tr>
<td>Capacity Planning for Backup Repositories</td>
<td>Analyzes the amount of free space on backup repositories and estimates the projected date when the repositories will run out of available storage capacity</td>
</tr>
<tr>
<td>Job Configuration Change Tracking</td>
<td>A record of the backup jobs’ configuration changes that occurred during a specified period</td>
</tr>
<tr>
<td>Backup Job Historical Information</td>
<td>Provides advanced information on completed backup and replication job sessions</td>
</tr>
<tr>
<td>Veeam Cloud Connect User Report</td>
<td>An overview of the storage utilization trends for Cloud Connect customers, listing key details and providing capacity availability outlook</td>
</tr>
<tr>
<td>SQL Job</td>
<td>Tracks the progress of SQL server backup jobs, providing the necessary details to verify that critical databases are properly backed up</td>
</tr>
<tr>
<td>Restore Operator Activity</td>
<td>Audits information on all types of restore actions performed across the selected Veeam Backup &amp; Replication servers</td>
</tr>
<tr>
<td>Protected VMs</td>
<td>Examines which VMs in your environment have been bolstered by up-to-date restore points by validating their RPO compliance</td>
</tr>
<tr>
<td>Report Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Orphaned VMs</td>
<td>Discovers the VMs that are present in existing backup files, but are missing from any pending backup, replication or backup to tape jobs</td>
</tr>
<tr>
<td>VMs Backed Up by Multiple Jobs</td>
<td>Zeroes in on the VMs that are backed up by several discrete jobs</td>
</tr>
<tr>
<td>VM Failover Plan Overview</td>
<td>Dissects the configuration of a failover plan, including the list of designated VMs and the amount of storage data allocated to them</td>
</tr>
<tr>
<td>VMs with no Archive Copy</td>
<td>Lists the VMs whose backups are not complemented by an existing archive copy</td>
</tr>
</tbody>
</table>

### 10.3.3. Business Categorization

While the SCVMM and Failover Cluster Manager consoles offer a set of views presenting virtual infrastructure hierarchy from a technical perspective (clusters, hosts, VMs and so on), Veeam ONE Business View builds a different categorization model – it presents data about VMs, hosts, storages and clusters in business terms, as they are categorized in your virtual infrastructure. Such insight from the enterprise perspective allows you to control, analyze and plan constantly developing and changing virtual environment.

vSphere tags are becoming increasingly popular with vSphere administrators, as they provide much more flexibility than a single dimension of VM folders. In fact, both Veeam Backup & Replication and Veeam ONE support vSphere tags. Once the rules are defined in Business View, the appropriate tags are then automatically set in vSphere. This means that you can create automatic rules in Business View to tag VM's and then setup backup jobs in Veeam Backup & Replication to use the vSphere tags. This will work with any product that uses vSphere tags.

As a result, Veeam ONE Business View can be used to create a tag for all mission critical VMs. This tag can be later used in Veeam ONE Reporter and Veeam ONE to assign special alarms and reports to that group, or in Veeam Backup & Replication to configure backup or replication jobs to automatically include any VMs with the given tag.

### 10.4. Veeam ONE Deployment

Veeam ONE supports two deployment scenarios: Typical and Advanced (Advanced scalability). Depending on the size of the managed virtual environment, you can choose of the following Veeam ONE installation types:

- **Typical** – this type of installation is recommended for small to medium environments, with up to 100 hosts and 1500 VMs
- **Advanced Scalability** – this type of installation is recommended for large environments with more than 100 hosts and 1500 VMs
Module 10: Veeam ONE Features and Functionality

Installation type is defined by a set of configuration parameters that determine Veeam ONE behavior in a number of areas, such as data collection and other. Choosing the appropriate installation type allows you to optimize monitoring and reporting performance and improve user experience in Veeam ONE. Note, that Veeam ONE provides support for multi-tenant environments.

10.4.1. Typical deployment

The typical deployment scenario is ideal if you want to consolidate the entire product functionality in one place by installing all product components on a single machine (physical or virtual). This scenario is preferable for small- to medium-scale deployments.

In the typical deployment scenario, all Veeam ONE components (Veeam ONE Server, Veeam ONE Web UI, and Veeam ONE Monitor Client) are installed altogether on a single machine (either physical or virtual).

To store data retrieved from connected servers, a local or remote SQL Server instance is required as a supporting system. If you have an SQL Server instance that meets the Veeam ONE system requirements, you can adopt it for Veeam ONE usage. Otherwise, you can install a new SQL Server instance during the product installation – Veeam ONE setup package includes SQL Server 2012 Express.

To enable multi-user access to real-time performance statistics and configurable alarms, you can additionally install several instances of Veeam ONE Monitor Client on separate machines. Thus, you will be able to access Veeam ONE functionality either from the local machine or from remote computers.

10.4.2. Advanced deployment

The advanced deployment scenario is more suitable if you want to separate client/server roles by installing structural components on different machines. It is more suitable to accommodate the need of the large environments.
In the advanced deployment scenario, the following Veeam ONE components are installed on separate machines:

- **Veeam ONE Server**
- **Veeam ONE Web UI**

To enable user access to real-time performance statistics and configurable alarms, you need to install one or several instances of Veeam ONE Monitor Client.

To store data retrieved from connected servers, a local or remote SQL Server instance is required as a supporting system. If you already have an SQL Server instance that meets the Veeam ONE system requirements, you can adopt it for your deployment. Otherwise, you can install a new SQL Server instance during the product installation – Veeam ONE setup package includes SQL Server 2012 Express.

The advanced installation utilizes a client-server model for data collection and communication, which includes three components:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Collects data from virtual infrastructure servers, vCloud Director servers and Veeam Backup &amp; Replication servers and stores aggregated data in the SQL database</td>
</tr>
<tr>
<td>Web UI</td>
<td>Communicates with the SQL database allowing users to access collected data for generating reports and managing business categorization</td>
</tr>
<tr>
<td>Monitor Client</td>
<td>Communicates with Veeam ONE Server directly to obtain real-time virtual infrastructure performance data and data protection statistics</td>
</tr>
</tbody>
</table>

Therefore, for a successful advanced deployment of Veeam ONE, it is essential that the client components are aware of the Veeam ONE Server and SQL database locations and can connect to them in order to process and manipulate data.
10.5. Veeam ONE Assessment Tool

Veeam ONE offers the Infrastructure Assessment Reports pack which helps ensure your VMs are ready to be properly backed up. Infrastructure assessment reports analyze your environment for incompatibilities and configuration errors that can potentially prevent or complicate future backup operations. The report pack helps you predict the amount of future changes on virtual disks that may have an influence on the frequency of backup jobs, consumed backup capacities and necessary WAN bandwidth allocated for replication jobs.

10.5.1. Veeam ONE Assessment Tool Content

Reports included into the pack are:

- **VM Change Rate Estimation** – tracks the amount of data changed on virtual disks to find VMs that grow too fast. The report analyzes rates at which data was written to virtual disks during the selected reporting interval, and displays top N virtual machines that grew faster and slower than other VMs. The details table provides information on total and daily amount of changes for each VM. This report helps you assess future needs for repository free space.

- **VM Configuration Assessment** – helps you to assess VMs readiness for performing backup with Veeam Backup & Replication. The report analyzes configuration of VMs in your virtual environment, and shows potential issues and possible limitations that could cause backup process to fail or prevent VMs from being properly backed up – for example, VMware Tools are not installed at the VM, or the VM has independent virtual disks in its configuration (Veeam Backup & Replication does not support independent disks; these disks are skipped from processing automatically). This report allows you to obtain a list of VMs in your virtual environment that could experience potential issues with backups, and to get guidance on how to resolve these issues.

**Note:** The VM Configuration Assessment report is available for VMware vSphere environments only.
Labs for Module 10: Veeam ONE Features and Functionality

It is crucial to have the right monitoring tools to maintain complete visibility into your virtual environment and backup and replication infrastructure to maintain an Always-On Business. Proper visibility in both layers helps provide efficient detection of potential issues before operational impact.

You are now welcome to try out the corresponding labs on Veeam ONE and its capabilities. You will have an opportunity for a hands-on experience when working with Veeam ONE, from setting it up to performing infrastructure assessment, before Veeam Backup & Replication installation.

Get into the Lab

<table>
<thead>
<tr>
<th>Lab</th>
<th>Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1</td>
<td>Analyze Veeam ONE installation.</td>
<td>To save time, Veeam ONE has already been pre-installation.</td>
</tr>
<tr>
<td>10.2</td>
<td>Setting up Veeam ONE (part two)</td>
<td>Add Veeam backup server to the Veeam ONE interface and schedule data collection.</td>
</tr>
<tr>
<td>10.3</td>
<td>Creating a Custom Veeam ONE Reporter Dashboard</td>
<td>Create a Veeam ONE Reporter dashboard to make working with the VMs from the course easier and more comfortable.</td>
</tr>
<tr>
<td>10.4</td>
<td>Customizing Veeam ONE Monitor Alerting Options</td>
<td>Set up e-mail notifications to ensure that you do not miss critical changes or events that occur in your environment.</td>
</tr>
<tr>
<td>10.5</td>
<td>Veeam ONE: Creating a Business View Category and Group</td>
<td>Set up VMs categorization.</td>
</tr>
<tr>
<td>10.6</td>
<td>Veeam ONE Backup Reporting</td>
<td>Run the Protected VMs report to analyze backup protection of VMs in your virtual environment.</td>
</tr>
<tr>
<td>10.7</td>
<td>Performing Infrastructure Assessment</td>
<td>Analyze the environment for incompatibilities and configuration errors that can potentially prevent or complicate future backup operations.</td>
</tr>
</tbody>
</table>
11. Product Editions

Veeam Backup & Replication is available in Standard, Enterprise and Enterprise Plus editions. The Enterprise and Enterprise Plus editions include additional features to accommodate the requirements of large enterprise environments.

11.1. Product Editions Comparison

The differences in features for Standard, Enterprise and Enterprise Plus editions applicable to VMware vSphere and Microsoft Hyper-V environments are shown in the table below.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>VMware</td>
<td>Hyper-V</td>
<td>VMware</td>
</tr>
<tr>
<td>Backup copy job</td>
<td>Available</td>
<td>Support for copying jobs to remote locations over WAN (direct operations only)</td>
<td>Available</td>
</tr>
<tr>
<td>Built-in WAN acceleration</td>
<td>Not available</td>
<td>Available</td>
<td>Only support for Veeam Cloud Connect</td>
</tr>
<tr>
<td>Backup from storage snapshots</td>
<td>Not available</td>
<td>Not available</td>
<td>Not available</td>
</tr>
<tr>
<td>Native tape support</td>
<td>Limited</td>
<td>File to Tape jobs only</td>
<td>Full support</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------</td>
<td>--------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td>VMware</td>
<td>Hyper-V</td>
<td>VMware</td>
</tr>
<tr>
<td>Support for vCloud Director</td>
<td>Limited Visibility of vCloud Director (vCD) infrastructure, backup via VeeamZIP (including backup of vApp and VM meta data and attributes)</td>
<td>Not available</td>
<td>Full support</td>
</tr>
<tr>
<td>Universal Application-Item Recovery (U-AIR)</td>
<td>Not available</td>
<td>Available Includes specialized universal wizard for any application</td>
<td>Available</td>
</tr>
<tr>
<td>SureBackup recovery verification</td>
<td>Manual Verify the recoverability of backup files by mounting VM disks from backup files using Instant VM Recovery and manually testing them</td>
<td>Automated You can select to perform automatic recovery verification jobs after every backup and verify any restore point.</td>
<td>Available</td>
</tr>
<tr>
<td>SureReplica recovery verification</td>
<td>Not available</td>
<td>Not available</td>
<td>Available</td>
</tr>
<tr>
<td>On-Demand Sandbox</td>
<td>Not available</td>
<td>Limited support Run one or several VMs from backup or replicas in an isolated environment, providing a working copy of the production environment for troubleshooting, testing, training and so on</td>
<td>Available</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------</td>
<td>--------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td></td>
<td>VMware</td>
<td>Hyper-V</td>
<td>VMware</td>
</tr>
<tr>
<td>File system indexing</td>
<td>Restricted</td>
<td>Not restricted</td>
<td>Not restricted</td>
</tr>
<tr>
<td></td>
<td>Browse and search for files in backups which are currently on disk</td>
<td>Browse and search for files in both current and archived backups (for example, backups which have been moved to tape storage)</td>
<td></td>
</tr>
<tr>
<td>1-Click Restore</td>
<td>Not available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Allows help desk administrators to restore VMs and guest files through the Veeam Backup Enterprise Manager web UI</td>
<td>Available</td>
</tr>
<tr>
<td>Delegation and self-recovery of VMs and guest files</td>
<td>Not available</td>
<td>Not available</td>
<td>Available</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Allows authorized users to restore VMs and guest files through the web UI</td>
<td></td>
</tr>
<tr>
<td>Job cloning and editing via the web UI</td>
<td>Not available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Clone existing jobs and edit their settings from the Veeam Backup Enterprise Manager web UI</td>
<td></td>
</tr>
<tr>
<td>Veeam Explorers</td>
<td>Limited support</td>
<td>Full support</td>
<td>Full support</td>
</tr>
<tr>
<td></td>
<td>Browse and restore mail items via save, send and export</td>
<td>Includes restore to original location</td>
<td></td>
</tr>
<tr>
<td>Scale-Out Backup Repository</td>
<td>Not available</td>
<td>Limited 3 extents maximum</td>
<td>Available</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Available Unlimited extents</td>
<td></td>
</tr>
<tr>
<td>Backup from NetApp SnapMirror and SnapVault</td>
<td>Not available</td>
<td>Not available</td>
<td>Available</td>
</tr>
<tr>
<td>Guest Interaction Proxy</td>
<td>Not available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td></td>
<td>Application-Aware Processing is still possible, but runtime will be injected by Veeam Backup Server instead of a Guest Interaction Proxy.</td>
<td></td>
<td>Available</td>
</tr>
<tr>
<td>Mount Server</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Available</td>
<td>Available</td>
</tr>
</tbody>
</table>
### Module 11: Product Editions

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct NFS access</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>Standalone console</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>Data Domain Boost and HPE StoreOnce Support</td>
<td>Not available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>Veeam Power-Shell snap-in</td>
<td>Available</td>
<td>Available</td>
<td>Available</td>
</tr>
<tr>
<td>Veeam Backup Enterprise Manager Web API</td>
<td>Not available</td>
<td>Not available</td>
<td>Available</td>
</tr>
</tbody>
</table>

All editions are installed with the same setup file, however, the extra functionality becomes available only after installing a full license for Veeam Backup & Replication Enterprise Edition or Enterprise Plus Edition. You can install the license for the necessary version during the setup process and change the license file later. You can also change the type of license used.

### 11.2. Full and Free Functionality Modes

Veeam Backup & Replication can operate in two functionality modes: full mode and free mode.

- **When you run Veeam Backup & Replication in the full functionality mode**, you get a commercial version of the product that provides access to all functions.
- **When you run Veeam Backup & Replication in the free functionality mode**, you get a free version that provides a number of powerful utilities for managing virtual machines (VMs). It also provides flexible recovery, with the ability to restore the entire VM or individual VM files, guest files, and Microsoft Exchange, SharePoint, SQL Server and Active Directory items directly from the backup. Veeam Backup Free Edition does have a number of limitations, including (but not limited to):
  - Full backups of individual VMs only — no scheduled, incremental or multi-VM backups
  - No vPower capabilities (however, you can import VeeamZIP™ backups into the paid editions and use vPower capabilities there)
  - No VM replication

If you have a valid license installed, Veeam Backup & Replication operates in the full functionality mode. As soon as your license expires, you will be offered to install a new license or switch to the free functionality mode. To switch to the free mode, select **View → Free functionality only** from the main menu.

To switch back to the full mode, do either of the following:

- Install a valid license: select **Help → License** from the main menu. In the displayed window, click **Install License** and select the necessary license file.
- Select **View → Full functionality (advanced)** from the main menu. Note that if you do not have a valid license installed, you will not be able to use the functionality provided by the full mode.

**Note:** You cannot switch to the free functionality mode if a valid trial or paid license is installed on the Veeam backup server. In this case, the View menu item will be hidden in the main menu.
12. Troubleshooting

In this section you will explore:

- How to identify issues
- How to review and analyze issues

12.1. How to Identify the Problem

The first stage of the process is to identify the problem.

Listed here are some of the most common problems.

<table>
<thead>
<tr>
<th>Category</th>
<th>Common Problems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Error messages</td>
<td>- Backup job error</td>
</tr>
<tr>
<td></td>
<td>- Pop up messages in GUI / program</td>
</tr>
<tr>
<td></td>
<td>- Errors During restore</td>
</tr>
<tr>
<td>Unexpected infrastructure behavior</td>
<td>- Slow performance on the server / poor server performance (Stunned or slow work of the server / High load on the server)</td>
</tr>
<tr>
<td></td>
<td>- Non responsive GUI</td>
</tr>
<tr>
<td></td>
<td>- Non responsive Veeam Server</td>
</tr>
<tr>
<td></td>
<td>- Veeam services or other services not starting</td>
</tr>
<tr>
<td></td>
<td>- BSOD (Windows Blue Screen)</td>
</tr>
<tr>
<td></td>
<td>- Incorrect information</td>
</tr>
<tr>
<td>Other Environmental challenges</td>
<td>- Too fast /too heavy/poorly tuned Veeam</td>
</tr>
</tbody>
</table>

12.2. Review and Analyze the Issue

Once the problem has been identified, the next step is to analyze the issue. To begin, you should always check if it’s a common issue or limitation. See below for the most common issues or limitations.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>Free ESX(i) is not supported</td>
<td>When starting a backup or replication job, it fails with an error: “Current license or ESXi version prohibits execution of the requested operation.” Solution: Please upgrade to a paid version of ESX(i). Free ESX(i) Version doesn’t have API which is used by Veeam Backup &amp; Replication. For further information please visit <a href="http://www.veeam.com/kb1435">http://www.veeam.com/kb1435</a>.</td>
</tr>
<tr>
<td>Issue</td>
<td>Cause</td>
</tr>
<tr>
<td>-------</td>
<td>-------</td>
</tr>
</tbody>
</table>
| Licensing issues | You can mark a support case as licensing-related when you open a case in the Customer Portal. Here are some other helpful support resources:  
- [http://www.veeam.com/kb1470](http://www.veeam.com/kb1470)  
- [http://www.veeam.com/kb1718](http://www.veeam.com/kb1718)  
- [http://www.veeam.com/kb1191](http://www.veeam.com/kb1191) |
| Restore challenges | Some common restore challenges:  
- Restore Speeds  
- Restore Failures  
- Alternative Restore options when primary restore option fails  
Most inquiries around Restore Challenges are focused in online forums. |
| Bottleneck detectors | In our backup jobs we have bottleneck statistics that can teach us about where the jobs are slowing down. This can be source/network/target/proxy. The bottleneck statistics does not necessarily mean that you have a problem in your backup infrastructure; it simply informs you about the weakest component in the data path. However, if you feel that the job performance is low, you may try taking some measures to resolve the bottleneck. |

### 12.3. Search for Additional Information

<table>
<thead>
<tr>
<th>Resource</th>
<th>Link</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community Forums</td>
<td><a href="http://forums.veeam.com/">http://forums.veeam.com/</a></td>
<td>These forums are maintained and moderated by the Veeam Product Management Team and contain product-specific information. By registering, users will receive our Weekly Community Digest.</td>
</tr>
</tbody>
</table>
12.4. Veeam Support

12.4.1. Support Programs

We offer two support response programs (Basic and Production) to our customers and one program (Evaluation) for 60 days if you are evaluating our software.

Evaluation Support

Evaluation Support program provides software support services during business hours (Monday through Friday) as defined below during the defined evaluation period.
Basic Support

Basic Support program provides software support services during business hours as defined below along with upgrades and updates to the products. One year of Basic Support is included with product license purchase.

Production Support

Production Support program provides 24/7 software support services and fast response times for critical issues. To receive Production Support, all production licensed sockets for a product must be licensed at Production Support levels, otherwise support defaults to Basic Support levels.

Support Programs Comparison

<table>
<thead>
<tr>
<th>Service</th>
<th>Evaluation Support</th>
<th>Basic Support</th>
<th>Production Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product updates</td>
<td>NA</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Product upgrades</td>
<td>NA</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Technical Support</td>
<td>Phone/Web</td>
<td>Phone/Web</td>
<td>Phone/Web</td>
</tr>
<tr>
<td>Business Hours (customer local time)</td>
<td>Mon-Fri 8 am – 5 pm</td>
<td>Mon – Fri 8 am – 8 pm</td>
<td>24x7x365</td>
</tr>
</tbody>
</table>

12.4.2. Response Time SLA

<table>
<thead>
<tr>
<th>Severity</th>
<th>Description</th>
<th>Target Production Response SLA</th>
<th>Target Basic Response SLA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity 1</td>
<td>A business critical software component or a Veeam managed system is inoperable or unavailable; production system is down; or there is an emergency condition. Requires an immediate workaround or solution. Examples: Excessive abnormal terminations impacting all monitoring, backups and schedules or a down/offline production system cannot be restored; application or system failure caused by Veeam product.</td>
<td>1 hour</td>
<td>2 hours</td>
</tr>
</tbody>
</table>
### Module 12: Troubleshooting

<table>
<thead>
<tr>
<th>Severity</th>
<th>Description</th>
<th>Target Production Response SLA</th>
<th>Target Basic Response SLA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity 2</td>
<td>Adversely impacting Production operations, but the production system is not down; product operates, but is seriously restricted. Examples: Production application response times or system performance are slow, system is available. Some monitoring or backups are impacted.</td>
<td>3 hours</td>
<td>8 business hours</td>
</tr>
<tr>
<td>Severity 3</td>
<td>A non-production issue; the majority of functions are still usable, a limited condition that can be readily circumvented. Example: non-Production application response times or system performance are slow, system is available. Some monitoring or backups are impacted.</td>
<td>6 hours</td>
<td>12 business hours</td>
</tr>
<tr>
<td>Severity 4</td>
<td>Minor issue or question that does not affect the product function, and can be readily circumvented. For example: “How to” questions; the text of a message, or page of documentation is worded poorly or misspelled, General Feedback, Feature Requests.</td>
<td>8 hours</td>
<td>24 business hours</td>
</tr>
</tbody>
</table>

### 12.4.3. Contacting Customer Support

This section will detail Veeam Support services, contact information and best practices for contacting support to ensure a quick response and issue resolution.

**Contacting Customer Support**

The customer should designate a few representatives responsible for opening cases with Veeam, and receiving maintenance information. They should have the appropriate technical skills and system level access to work with Veeam Support Engineers in resolving open issues. These support contacts will be your interface to Veeam Support, and should be notified of all issues that surface within your organization. They will escalate issues to Veeam Support as necessary.

Customer should be prepared to provide the following information:

- Name, company name, and telephone number with extension
- Case number (if applicable)
- Product name, release level, and any maintenance applied to the product

It is strongly recommended to attach product logs as the case is created.
Logging a Case

Any information you can provide regarding the issue can have a significant impact on how fast the issue is diagnosed and resolved. You will be asked to provide the following information:

- Issue description, impact on your system and business operations, issue severity, and the exact text of error messages and diagnostic details
- Steps to reproduce the problem, known workarounds
- Contact number where you can be reached
- Best time to reach you, and contact method (i.e. email/phone)

Submitting a Support Case

To file a case, you may use any method below. We encourage you to set the initial severity level for the problem when submitting a case and highly recommend using phone to submit Severity 1 issues.

Via the Web

You can file a case using a web browser in Customer Portal: http://cp.veeam.com/. Please follow the new case wizard to open a case. Upon submitting the case, you will receive an electronic confirmation with a unique case number sent to your email address. You will also be able to see the case in the open cases management tab.

Via the Phone

To open a case using the phone, call one of the phone numbers mentioned in Contacts at the Customer Portal. After you log the case with the customer representative, your case will be assigned a unique number given to you over the phone. If required and depending on license type, support offering and severity level, your call will be transferred to an appropriate support engineer to resolve your issue over the phone.

Following Up

A support engineer will contact you by phone and/or email or a combination of both as appropriate during the resolution process. Severity levels may be adjusted with customer consent and mutual agreement on the degree of the impact based on the Severity definitions.

Customer Support Issue Resolution

Veeam Support provides resources to research and resolve issues on a timely basis. While an issue is open, the support team will keep you informed of the resolution status, and will notify you when a reported issue has been resolved. If at any point during the resolution process, you become dissatisfied with the handling of your issue, simply contact the case owner and request an escalation.
to the manager. This allows us to understand your concerns and make adjustments in resources if necessary.

We will make three attempts, on separate business days, to contact you for updates or information on an open case. If we are unable to make contact with you, we may close the case without your consent. If the issue continues to exist, you may open a new case and reference the old one.

Resolution of a support case can include any of the following actions:

- Software that provides a fix for the problem (case closed)
- Permanent business or system workaround (case closed)
- Temporary business or system workaround (case severity level is reduced)
- Action plan for the development of a fix or workaround: milestones and dependencies are set, communicated, and tracked (case severity level might be changed)
- Issue is a customer-specific customization or enhancement, and is not covered under maintenance (customer notification, case closed)

### 12.4.4. Product Lifecycle

Level of support services provided depends on the lifecycle phase determined for specific versions of the product. Current versions of the products are eligible for full support, including support services and updates/fixes, while support for older versions may be limited. A list of known workarounds or existing fixes and assistance with upgrading to a supported version is available for customers using old or discontinued versions.

The list is updated each time there is a release, for the current list of products and their status, please see the product release matrix located at [http://www.veeam.com/support/releasestatus.pdf](http://www.veeam.com/support/releasestatus.pdf)

#### Support of Releases

1. **New Releases** – All new products are issued for General Availability (GA).
2. **Current Releases** – To maximize the quality of our service, Veeam limits technical support to the products listed on the release matrix.
3. **Releases designated as End of Fixes** – Support is available, existing program fixes are available, but no new fixes will be created and no enhancements will be made.
4. **Releases designated as End of Support or Withdrawal from the Market** – No support is available.
   - For unsupported releases, new product enhancements and fixes will not be available. Veeam does not have an obligation to provide support for software that has been publicly designated End of Support, Withdrawn from the Market, or similarly designated.

#### Product Maintenance

Our goal is to go beyond quickly solving problems, and actually preventing problems from occurring in the first place. As a result, stringent quality control procedures are built into the development and release cycle of new products and releases.
Issues sometimes occur with complex software operating in equally complex and demanding environments. Fixes and resolutions are often rolled into the next product release, and others are included as part of the next maintenance release, and the most urgent issues are addressed with a hotfix that can be applied on a specific product version. When applicable, we announce the availability of new releases on the web and through e-mail.

**12.4.5. Third Party Software Support**

We will assist the customer in problem analysis to determine whether the issue is caused by third party software or hardware. In order to isolate the problem and if Veeam support engineer believes they have reason, they may ask the customer to remove third party software or hardware product.

If it is impossible to identify the cause of the problem, Veeam may contact the third party vendor using TSANet or ask the customer to open support case with third party vendor support organization.
13. Training Summary

This section summarizes main Veeam Certified Engineer training points.

13.1. Key Points

Veeam Backup & Replication delivers a powerful, affordable and easy-to-use solution for backup, recovery and replication for both VMware and Hyper-V.

Veeam Backup & Replication is a modular solution which allows flexible scalability for environments of different sizes and configuration. Some of the following Veeam Backup & Replication components are installed using a setup file and others are configured while working with the product.

- Veeam Backup Server
- Backup Proxy
- Backup Repository
- Veeam Backup Enterprise Manager
- Veeam Backup Search
- Mount Server
- Veeam Explorers

Veeam Backup & Replication offers Standalone Console which is a separate client-side part that allows you to access Veeam backup server. You can use the console locally, or install it in a standalone mode on a device running Microsoft Windows to access Veeam Backup & Replication remotely over the network. The console logs you in to Veeam Backup & Replication, allowing you to perform all kind of operations.

For a virtual environment management solution, Veeam offers Veeam ONE, which delivers real-time monitoring on health and performance of virtual environments, helps analyze the efficiency of data protection implemented with Veeam Backup & Replication, provides intelligent reporting, and offers business-based views of the virtual infrastructure topology to simplify management and expedite decision-making.

Veeam Backup & Replication is the best solution for very different infrastructures. It can be deployed using different scenarios:

- **Simple deployment** is when Veeam Backup & Replication is installed on a physical or virtual Windows-based machine. This installation is referred to as a Veeam backup server.
- **Advanced deployment** is when the backup workload moves to dedicated backup proxies and backup repositories (in case of using VMware) or to an off-host backup proxy (in case of using Hyper-V).
- **Distributed deployment** is when virtual environments are large and geographically dispersed with multiple Veeam backup servers installed across different sites. In this case, Veeam Backup Enterprise Manager centralizes management and reporting for these servers.

With Veeam Backup & Replication, it is easy to create backups. It is a job-driven process where one backup job can be used to process one or more VMs. Essentially, the job defines when, what, how and where to back up. It indicates what VMs should be processed, what components should be used for retrieving and processing VM data, what backup options should be enabled, and where to save
the resulting backup file. Jobs can be started manually by the user or scheduled to run automatically. The resulting backup file stores compressed and deduplicated VM data. All backup files created by the job are located in a dedicated job folder on a backup repository.

To ensure efficient and reliable data protection in your virtual environment, Veeam Backup & Replication complements image-based backup with image-based replication. Replication is the process of copying a VM from its primary location (source host) to a destination location (redundant target host). Veeam Backup & Replication creates an exact copy of the VM (replica), registers it on the target host and maintains it in sync with the original VM. Replication is also a job-driven process with one replication job used to process one or more VMs. You can start the job manually every time you need to copy VM data or, if you want to run replication unattended, create a schedule to start the job automatically. It's possible to create a replica using backup file as a source, thus reducing the load at the production environment.

To guarantee recoverability of your data, Veeam Backup & Replication offers the SureBackup technology and complements the recovery verification technology with SureReplica for VMware vSphere. SureBackup lets you validate backups of your VMs without impacting the production infrastructure. You can automatically verify every created restore point of every VM and ensure that they will function as expected in case a disaster strikes. SureReplica is similar to the SureBackup recovery verification in many respect. It lets you validate your DR environment without impacting the production infrastructure: You can automatically verify every created restore point of every VM replica and ensure that they are functioning as expected.

Veeam Backup & Replication offers a number of recovery options for various disaster recovery scenarios:

- Instant VM Recovery enables you to instantly start a VM directly from a backup file.
- Full VM Recovery enables you to recover a VM from a backup file to its original or another location.
- VM File Recovery enables you to recover separate VM files (virtual disks, configuration files and so on).
- Virtual drive restore enables you to recover a specific hard drive of a VM from the backup file, and attach it to the original VM or to a new VM.
- Windows file-level recovery enables you to recover individual Windows guest OS files (from FAT, NTFS and ReFS file systems).
- MultiOS file-level recovery enables you to recover files to from many different guest OS file systems.
- Veeam Explorers and Universal Application-Item Recovery (U-AIR) enables you to recover application objects (such as, AD entries, SharePoint and Exchange items, Oracle and SQL database objects and so on) directly from backup files.

Veeam Backup & Replication uses the same image-level backup for all data recovery operations. You can restore VMs, VM files and drives, application objects and individual guest OS files to the most recent state or to any available restore point.

Veeam Backup & Replication lets you leverage HPE, NetApp and EMC SAN snapshots as a part of a comprehensive backup and recovery strategy, where SAN snapshots and image-level backups complement each other. With Veeam Backup & Replication, you can:

- Perform backup from storage snapshots
- Restore data directly from storage snapshots
To solve the problems of insufficient network bandwidth to support VM data traffic and transmission of redundant data, Veeam Backup & Replication offers the WAN acceleration technology that helps optimize data transfer over the WAN. The WAN acceleration technology is specific for backup copy and replication jobs. Being a built-in feature, Veeam’s WAN acceleration does not add complexity or cost to the backup infrastructure and does not require agents. The technology has been developed for copying backup files, with consideration of the VM backup file content.

### 13.2. Useful Resources

If you have any questions or need additional information about Veeam Backup & Replication, you can use the following resources:

<table>
<thead>
<tr>
<th>Resource</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge Base</td>
<td><a href="http://www.veeam.com/kb_search_results.html">http://www.veeam.com/kb_search_results.html</a></td>
</tr>
<tr>
<td>Latest Updates</td>
<td><a href="http://www.veeam.com/updates.html">http://www.veeam.com/updates.html</a></td>
</tr>
<tr>
<td>Community forums</td>
<td><a href="http://www.veeam.com/forums">http://www.veeam.com/forums</a></td>
</tr>
<tr>
<td>Veeam University for End Users</td>
<td><a href="http://www.veeam.com/university.html">http://www.veeam.com/university.html</a></td>
</tr>
<tr>
<td>Customer Portal</td>
<td><a href="https://cp.veeam.com/">https://cp.veeam.com/</a></td>
</tr>
</tbody>
</table>

### 13.3. Contacts

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

For the most up to date information about company contacts and offices location, please visit [www.veeam.com/contacts.html](http://www.veeam.com/contacts.html).