CONTENTS

CONTACTING VEEAM SOFTWARE .............................................................................................................. 4
ABOUT THIS GUIDE ...................................................................................................................................... 5
INTRODUCTION TO VEEAM AVAILABILITY SUITE .................................................................................. 6
REFERENCE ENVIRONMENT AND EVALUATION LAB ............................................................................ 7
PREREQUISITES ............................................................................................................................................ 7
Supported Platforms ................................................................................................................................. 7
INSTALLATION PROCESS ......................................................................................................................... 8
ADDING SERVERS TO SCOPE .................................................................................................................. 10
EXAMPLE .................................................................................................................................................... 12
COLLECTING DATA FROM INFRASTRUCTURE .......................................................................................... 13
EVALUATION CASES AND PROCEDURES ............................................................................................... 14
CASE 1. INFRASTRUCTURE ASSESSMENT ................................................................................................. 14
Step 1. Identify and Resolve Potential Issues .......................................................................................... 14
Step 2. Estimate VM Change Rate ......................................................................................................... 16
Step 3. Datastore Performance Assessment .......................................................................................... 18
CASE 2. BACKUP INFRASTRUCTURE SETUP AND OPTIMIZATION ...................................................... 20
Option for VMware VMs: Using Tags ...................................................................................................... 23
CASE 3. IDENTIFYING UNPROTECTED VMs ............................................................................................. 24
Step 1. Reporting on Unprotected VMs ................................................................................................. 24
Step 2. Monitoring for Unprotected VMs in Real Time .......................................................................... 27
CASE 4. RECOVERY VERIFICATION ......................................................................................................... 29
CASE 5. CONTROLLING BACKUP REPOSITORY ...................................................................................... 31
Step 1: Setting Up Availability Monitoring ............................................................................................ 31
Step 2: Setting Up Free Space Monitoring ............................................................................................. 33
Step 3: Capacity Planning for Repository ............................................................................................. 35
CASE 6. PERFORMING RESTORE OPERATIONS ....................................................................................... 37
Step 1. Performing Full VM Restore ...................................................................................................... 37
Step 2. Restoring Windows Guest OS File ............................................................................................... 38
Step 3. Restoring Application Items ....................................................................................................... 39
Step 4. Examining Restore Operator Activity ........................................................................................ 41
CASE 7. AUDITING AND COMPLIANCE ................................................................................................... 42
Step 1. Tracking Job Configuration Changes .......................................................................................... 42
Step 2. Examining Delegated Restore Permissions ............................................................................... 44
Step 3. Assessing VM Backup Compliance ............................................................................................ 46
Step 4. Identifying Orphaned VMs ......................................................................................................... 48
Step 5. Identifying VMs with no Archive Copies ................................................................................... 50
CASE 8. VIRTUAL INFRASTRUCTURE MONITORING AND ALERTING .................................................... 51
CASE 9. ADVANCED CAPACITY PLANNING AND “WHAT-IF” MODELLING ........................................... 53
CONTACTING VEEAM SOFTWARE

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.

Customer Support
Should you have a technical concern, suggestion or question, please visit our Customer Center Portal at cp.veeam.com to open a case, search our knowledge base, reference documentation, manage your license or obtain the latest product release.

Company Contacts
For the most up to date information about company contacts and offices location, please visit www.veeam.com/contacts.html.

Online Support
If you have any questions about Veeam Availability Suite and its components, you can use the following resources:

- Community forum at http://forums.veeam.com/
ABOUT THIS GUIDE

This guide provides information about main features and use of Veeam Availability Suite. The document applies to solution version 8.0 and all subsequent versions until the document is replaced by a new edition.

The guide is intended for anyone who wants to evaluate Veeam Availability Suite and its components. It is primarily aimed at IT administrators, but can also be helpful for other users who plan to work with the solution.

Document Revision History

<table>
<thead>
<tr>
<th>Revision #</th>
<th>Date</th>
<th>Description of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revision 1</td>
<td>14/04/2015</td>
<td>Initial version of the document for Veeam Availability Suite 8.0</td>
</tr>
</tbody>
</table>
INTRODUCTION TO VEEAM AVAILABILITY SUITE

Veeam Availability Suite integrates Veeam Backup & Replication with the built-in intelligence and powerful capabilities of Veeam ONE to offer extended monitoring, reporting and capacity planning support for backup.

Veeam Backup & Replication provides fast, flexible and reliable recovery of virtualized applications and data, offering the following features:

- **2-in-1: backup and replication** — unify backup and replication in a single data protection solution.
- **Built-in deduplication** — cut backup storage requirements up to 75% by compressing backup and network traffic and eliminating duplicate blocks of data.
- **Near-continuous data protection** — capture changes and update VM images as often as every few minutes for on-site and off-site replication.
- **Backup verification and data recovery capabilities** — automatically verify every backup, use agentless recovery of VMs, guest files and individual objects for any virtualized application.

Veeam ONE delivers a single, integrated solution for virtual environments with multiple standalone hosts, management servers, and Failover Clusters. Its powerful capabilities are extended to the backup infrastructure to provide advanced monitoring, reporting and capacity planning for Veeam Backup & Replication:

- **Real-time monitoring** — well-informed, unattended 24x7 monitoring of your entire backup and virtual infrastructures, alerting you of backup and performance issues before applications and users are affected, speeding up troubleshooting with alarm dashboards and built-in intelligence for faster resolution; these features are provided by Veeam ONE Monitor component.
- **Capacity planning** — trend analysis, what-if modeling, recommendations for making well-informed decisions to manage the growth of your virtual and backup infrastructures. This functionality, as well as documentation and reporting, is supported by Veeam ONE Reporter component.
- **Documentation and management reporting** — automatically discover and document your infrastructure for you; a wealth of predefined reports can be generated automatically and delivered to dashboards, email, web portals and folders.
- **Business categorization** — offers technical- and business-oriented views of your virtual environment. This functionality is supported by Veeam ONE Business View component.

In this document you will find a set of self-guided evaluation exercises that you should follow to familiarize yourself with Veeam Availability Suite and evaluate its capabilities in a lab. Each evaluation exercise provides an evaluation case and step procedure; some also include validation of the results.

For detailed documentation about each component of the solution, you can refer to Veeam Help Center available at [http://www.veeam.com/documentation-guides-datasheets.html](http://www.veeam.com/documentation-guides-datasheets.html).
REFERENCE ENVIRONMENT AND EVALUATION LAB

To carry out evaluation procedures, you will need to configure an evaluation lab. Sample lab description is provided later in this document.

Prerequisites

Veeam Availability Suite supports VMware and Hyper-V in a single solution, so you can protect and manage all your VMs from the same console. See the list of Supported Platforms that can be used in the evaluation lab.

Since evaluation cases described in this guide assume “all-in-one” deployment, including both Veeam Backup server and Veeam ONE server and client installed on the same machine, consider that this machine must be running 64-bit operating system.

Note: However, in production environment Veeam ONE Monitor client can be installed on a 32-bit OS; for detailed system requirements see Veeam ONE and Veeam Backup & Replication Release Notes at http://www.veeam.com/documentation-guides-datasheets.html.

Detailed software and hardware requirements, necessary permissions and ports are listed in the Release Notes for Veeam Backup & Replication and Veeam ONE, as well as in the product documentation available at http://www.veeam.com/documentation-guides-datasheets.html.

Supported Platforms

<table>
<thead>
<tr>
<th>VMware Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platforms</td>
</tr>
<tr>
<td>vSphere 5.x</td>
</tr>
<tr>
<td>vSphere 4.x</td>
</tr>
<tr>
<td>Hosts</td>
</tr>
<tr>
<td>ESXi 5.x</td>
</tr>
<tr>
<td>ESX(i) 4.x</td>
</tr>
<tr>
<td>Note: Free vSphere Hypervisor (free ESXi) is not supported.</td>
</tr>
<tr>
<td>Software</td>
</tr>
<tr>
<td>vCenter Server 5.x (optional)</td>
</tr>
<tr>
<td>vCenter Server 4.x (optional)</td>
</tr>
<tr>
<td>vCloud Director 5.1, 5.5 (optional)</td>
</tr>
<tr>
<td>Virtual machines</td>
</tr>
<tr>
<td>All operating systems supported by VMware</td>
</tr>
<tr>
<td>Any application</td>
</tr>
<tr>
<td>Any file system</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Microsoft Hyper-V Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platforms</td>
</tr>
<tr>
<td>Windows Server 2012 R2</td>
</tr>
<tr>
<td>Windows Server 2012</td>
</tr>
<tr>
<td>Windows Server 2008 R2 SP1</td>
</tr>
<tr>
<td>Hosts</td>
</tr>
<tr>
<td>Windows Server Hyper-V 2012 R2</td>
</tr>
<tr>
<td>Windows Server Hyper-V 2012</td>
</tr>
<tr>
<td>Windows Server Hyper-V 2008 R2 SP1</td>
</tr>
<tr>
<td>Microsoft Hyper-V Server (free hypervisor) is supported</td>
</tr>
<tr>
<td>Hosts must have all relevant Windows Server hot fixes installed</td>
</tr>
<tr>
<td>Software</td>
</tr>
<tr>
<td>Microsoft System Center Virtual Machine Manager 2012 R2 (optional)</td>
</tr>
</tbody>
</table>
Installation Process

For evaluation and test purposes, you can use the trial version of Veeam Availability Suite that includes Veeam Backup & Replication 8.0 and Veeam ONE 8.0, available at http://www.veeam.com/downloads.html. Trial license has no functional limitations, providing the full set of capabilities (Veeam Backup & Replication Enterprise Plus edition is included); trial license keys are valid for 30 days.

You can use a simple deployment scenario:

- All Veeam ONE components can be installed altogether on a single machine, either physical or virtual. Veeam ONE architecture and components are shown in the figure below.

- The same or another machine — physical or virtual — will host Veeam Backup & Replication components and, optionally, Veeam Backup Enterprise Manager. Veeam Backup & Replication architecture and components are shown in the figure below.
An example of a deployment where both products are installed together is provided in the description of a test lab used for this guide.

Before you start installing the solution, check if your lab configuration meets minimal system requirements (refer to http://www.veeam.com/veeam_backup_8_0_release_notes_rn.pdf and http://www.veeam.com/veeam_one_8_0_release_notes_rn.pdf). Make sure the accounts you plan to use for solution installation and operation have sufficient access rights.

To install the solution, do the following:

2. Mount the product ISO and use autorun, or run the Setup.exe file.
3. Install Veeam Backup & Replication (you can also install Veeam Backup Enterprise Manager as an optional component).
   a) Accept the terms of Veeam Backup & Replication License Agreement to install the product.
   b) Provide setup program with your trial license file.
   c) Specify the installation folder and select the required components to install.
   d) The setup program will perform pre-requisite check and install any missing components.
   e) On the Default Configuration step, review default installation settings and make sure the Let me specify different settings check box is cleared. Click

4. Have the setup locally install Microsoft SQL Server 2012 Express Edition to host the VeeamBackup database. Setup will install a named (VEEAMSQL2012) instance of SQL Server.

5. Install Veeam ONE, as described in the Veeam ONE Deployment Guide; when following the setup wizard, consider the following:
   a) On the Setup Type step, select Typical to deploy all components with default settings on a single server.
   b) On the SQL Server Instance step, select the Use existing instance of SQL server option and specify VEEAMSQL2012 as the instance. This will instruct the setup to co-locate VeeamONE database and VeeamBackup database.
   c) On the Virtual Infrastructure Type step, select Skip Virtual Infrastructure Configuration. You will perform this operation later on.

Adding Servers to Scope

The figure below shows solution components’ interactions in the evaluation lab:

- As you can see, Virtual Infrastructure servers communicate with both Veeam ONE server and Veeam backup server, thus, they should be added to both Veeam ONE scope and Veeam Backup & Replication scope.
Veeam Backup & Replication metrics, events, configuration and topology are collected by Veeam ONE server, thus, Veeam backup server should be added to Veeam ONE scope.

Do the following:

1. Use Veeam Backup & Replication console to add a VMware server (vCenter or ESX host) and/or a Hyper-V server to Veeam Backup & Replication scope as managed servers. For details, please refer to the corresponding section of Veeam Backup & Replication Help (http://helpcenter.veeam.com/backup/80/vsphere/index.html?add_vmware_server.html and http://helpcenter.veeam.com/backup/80/hyperv/index.html?add_hyperv_server.html).

**Note:** Consider that some evaluation cases are applicable to VMware environment only.

2. Open Veeam ONE Monitor console and click Add Server on the toolbar to start Add Server Wizard:

- **VMware server**: Add vCenter server (recommended), or standalone vSphere Hypervisor (ESXi/ESX).
- **VMware vCloud Director**: Add VMware vCloud Director.
- **Hyper-V server**: Add SCVMM server, Failover Cluster or standalone Hyper-V host.
- **Veeam Backup & Replication server**: Add Veeam Backup & Replication server or Veeam Backup Enterprise Manager.
3. With this wizard, you should add both Veeam backup server and Virtual Infrastructure servers (VMware vCenter, ESX host, or a Hyper-V server) that were added to Veeam Backup & Replication scope at step 1.

**Note:** You should be adding exactly the same Virtual Infrastructure servers to both Veeam Backup and Veeam ONE scope, using the same naming (either domain name or IP address), otherwise, creation of some reports may fail.

For details on using the wizard, please refer to Connecting Veeam Backup & Replication Servers, Connecting VMware vSphere Servers, and Connecting Microsoft Hyper-V Servers.

**Note:** Veeam ONE can be used in the environments with more than one Veeam Backup & Replication servers installed. In this case, a common scenario involves deploying Veeam Backup Enterprise Manager – to facilitate centralized job management, on-going statistics analysis, license management, delegated restore, and other operations. For this deployment scenario, consider adding Enterprise Manager server to Veeam ONE monitoring and reporting scope. It will become a single source of data for all backup servers, and you will not need to connect several backup instances to Veeam ONE console manually. However, to avoid duplicated data, you should only be adding either Veeam Backup Enterprise Manager server or Veeam Backup server (not both).

### Example

To carry out evaluation procedures described in this guide, a test lab with the following configuration has been used:

- Veeam Backup & Replication and all components of Veeam ONE were co-installed on a virtual machine (VMware platform) with 64-bit version of Windows Server 2012 as guest OS, and appropriate virtual hardware (4GB memory, x64 2-core vCPU).
- Microsoft SQL Server 2012 Express Edition (included in the setup) was installed locally to host all product databases.
- Other required software components were installed automatically after system configuration check during the solution setup.
- Veeam backup server also operates as a proxy server (by default); default backup repository is local Windows server.

Data flow for lab deployment is shown in the figure below.
Collecting Data from Infrastructure

Information on your virtual and backup infrastructure topology is stored in the VeeamOne database on the SQL Server specified during the setup; commonly, data collection runs periodically on schedule – by default, on weekdays, at 3:00 a.m. If necessary, you can change data collection schedule for specific servers, or start data collection manually when needed.

Note: This refers to configuration data; performance and real-time monitoring data is collected in real time.

To change data collection schedule for specific servers, do the following in Veeam ONE Reporter:

1. Open the Configuration view in web UI and click Servers on the left.
2. Select the server for which you want to change data collection schedule and click Scheduling on the toolbar.
3. Adjust data collection schedule appropriately.

Besides, you can start data collection manually when needed. For that, do the following:

1. In Veeam ONE Reporter, switch to the Configuration view.
2. Select Servers, choose the server for which you want to collect data, then click Start on the toolbar:

For more information on Veeam ONE configuration and data collection settings, please refer to Veeam ONE Deployment Guide at http://helpcenter.veeam.com/one/80/deployment/.
**EVALUATION CASES AND PROCEDURES**

Each evaluation exercise provides an evaluation case and step procedure; some also include validation of the results.

- **Case 1. Infrastructure Assessment**
- **Case 2. Backup Infrastructure Setup and Optimization**
- **Case 3. Identifying Unprotected VMs**
- **Case 4. Recovery Verification**
- **Case 5. Controlling Backup Repository**
- **Case 6. Performing Restore Operations**
- **Case 7. Auditing and Compliance**
- **Case 8. Virtual Infrastructure Monitoring and Alerting**
- **Case 9. Advanced Capacity Planning and “What-if” Modelling**

**Case 1. Infrastructure Assessment**

This evaluation case will help you understand how to use data collection and reporting capabilities to carry out the following tasks:

- Assess your virtual infrastructure readiness for backup
- Plan for network and storage resources for Veeam Backup & Replication deployment in production

The evaluation procedure should be performed before you launch your first backup job.

**Step 1. Identify and Resolve Potential Issues**

To identify potential problems that may prevent VMs from being protected with Veeam, use the **VM Configuration Assessment** report (currently available for VMware only).

This report scans the VMs deployed across the VMware environment and locates the VMs that cannot be backed or will experience difficulties during the backup process due to hardware issues, configuration errors or incompatibilities.

Take the following steps:

1. Before running this report, prepare a test VM that has its virtual disk configured as independent disk.
2. Run data collection for the corresponding VMware server, as described in **Collecting Data from Infrastructure** (for the new VM to be included in reporting scope).
3. In Veeam ONE Monitor Client, open **Infrastructure view** and click **Reports > VM > Configuration Assessment** or **Reports > Configuration > Configuration Assessment**.
4. Veeam ONE Reporter will be launched to help you generate the report. Leave the default parameters (Virtual Infrastructure option as Scope, and Skip Backup Replicas check box selected), then click Create report under Actions on the right.

5. Use search to make sure the VM from step 1 is listed in the corresponding sub-category (in the Potential Issue column) of the Virtual Disk issue category.
6. Change that VM's disk type to any supported type.
7. Run data collection again (see Collecting Data from Infrastructure).
8. Generate the VM Configuration Assessment report anew. Make sure the VM from step 1 is no longer included in the list in the Virtual Disk category.

**Note:** It is recommended that after you identify all VMs with possible problems and fix the issues, you then add these VMs to a separate backup or replication job and run this job to ensure the VMs are protected.

### Step 2. Estimate VM Change Rate

When estimating the amount of disk space required for your backup repository, you should consider a number of factors, including total size of VMs being backed up, backup method, backup frequency, and retention period. You also need to make assumptions on compression and deduplication ratios, change rates, and other factors.

To analyze your VMs’ change rate and calculate the potential amount of space required on the target repository, use the **VM Change Rate Estimation** report. This report calculates the anticipated amount of VMs’ changed blocks by extrapolating the VMs’ historical write data rate.

Take the following steps:

1. In Veeam ONE Monitor Client, open Infrastructure view and click **Reports > VM > VM Change Rate Estimation**.
2. Specify the required **Scope** for which VM data will be reported, **Reporting period** you need (for example, current week or certain dates), and **Top** – this is the number of VMs with the biggest/least change rate.
3. After that, click **Create report** under **Actions** on the right and wait for the report generation to complete. Review the amount of data written during the specified observation interval (for example, weekly). You can access the detailed write performance statistics for each VM’s virtual disk – for that, click the name of the target machine shown in the chart.

### VM Change Rate Estimation

**Description**

This report predicts the number of changed blocks (measured in GB) for virtual disks based on virtual machines write rate.

**Report Parameters**

**Scope:** Virtual Infrastructure

**Period Type:** Current week (11/17/2014 - 11/23/2014)

**Top N:** 5

**Report Created:** 11/26/2014 7:28:02 AM

---

### Summary

**Top 5 VMs with Largest Change Rate (GB)**

<table>
<thead>
<tr>
<th>Name</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Thursday</th>
<th>Friday</th>
<th>Saturday</th>
<th>Sunday</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evd01</td>
<td>295.65 GB</td>
<td>369.03 GB</td>
<td>327.08 GB</td>
<td>70.44 GB</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>963.05 GB</td>
</tr>
<tr>
<td>Evd02</td>
<td>189.37 GB</td>
<td>94.75 GB</td>
<td>83.89 GB</td>
<td>21.26 GB</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>398.87 GB</td>
</tr>
<tr>
<td>Evd03</td>
<td>74.60 GB</td>
<td>99.56 GB</td>
<td>46.59 GB</td>
<td>&lt; 1 GB</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>180.37 GB</td>
</tr>
<tr>
<td>Evd04</td>
<td>78.34 GB</td>
<td>26.78 GB</td>
<td>25.57 GB</td>
<td>7.39 GB</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>64.27 GB</td>
</tr>
<tr>
<td>Evd05</td>
<td>55.60 GB</td>
<td>19.64 GB</td>
<td>17.66 GB</td>
<td>6.16 GB</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>88.96 GB</td>
</tr>
<tr>
<td>Evd06</td>
<td>&lt; 1 GB</td>
<td>1.28 GB</td>
<td>35.19 GB</td>
<td>&lt; 1 GB</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>36.19 GB</td>
</tr>
<tr>
<td>Evd07</td>
<td>8.54 GB</td>
<td>9.56 GB</td>
<td>6.56 GB</td>
<td>2.68 GB</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>26.04 GB</td>
</tr>
<tr>
<td>Evd08</td>
<td>35.29 GB</td>
<td>9.77 GB</td>
<td>2.07 GB</td>
<td>&lt; 1 GB</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>25.77 GB</td>
</tr>
<tr>
<td>Evd09</td>
<td>2.62 GB</td>
<td>10.92 GB</td>
<td>2.77 GB</td>
<td>1.43 GB</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>23.75 GB</td>
</tr>
<tr>
<td>Evd10</td>
<td>6.10 GB</td>
<td>6.87 GB</td>
<td>6.35 GB</td>
<td>1.90 GB</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>21.03 GB</td>
</tr>
<tr>
<td>Evd11</td>
<td>1.49 GB</td>
<td>3.67 GB</td>
<td>15.06 GB</td>
<td>&lt; 1 GB</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>20.26 GB</td>
</tr>
<tr>
<td>Evd12</td>
<td>2.24 GB</td>
<td>2.04 GB</td>
<td>10.87 GB</td>
<td>0.00 GB</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>17.17 GB</td>
</tr>
<tr>
<td>Evd13</td>
<td>4.40 GB</td>
<td>5.06 GB</td>
<td>4.43 GB</td>
<td>1.51 GB</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>15.52 GB</td>
</tr>
<tr>
<td>Evd14</td>
<td>3.69 GB</td>
<td>4.89 GB</td>
<td>5.46 GB</td>
<td>&lt; 1 GB</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>13.96 GB</td>
</tr>
<tr>
<td>Evd15</td>
<td>4.21 GB</td>
<td>3.89 GB</td>
<td>4.28 GB</td>
<td>1.23 GB</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>13.61 GB</td>
</tr>
</tbody>
</table>

**Top 5 VMs with Lead Change Rate (GB)**

---

### Details

You can then utilize this information to estimate the amount of free space that should be available on the target repositories, as well as for the bandwidth requirement estimation.

### Example

A test environment includes 10 VMs, 100GB each, 80GB avg/used, with 5% daily change rate and 2:1 estimated compression/deduplication. With the reverse incremental backup method in use by daily backup and 30 days retention, the following estimations can be made:

**Estimated Full Backup Size:**

\[
10 \times 80\text{GB (Used space)} \times 50\% (2:1\ \text{Compression}) = 400\text{GB}
\]
Estimated Reverse Incremental Size:
10 * 80GB * 50% (2:1 Comp) * 5% (Change Rate) * 29 (reverse incremental restore points) = 580GB

Estimated total Backup Size:
400GB + 580GB = 980GB

Step 3. Datastore Performance Assessment

When carrying out your virtual infrastructure assessment, you should thoroughly analyze your datastore performance to ensure the datastore can cope with multiple VM snapshot commit operations triggered simultaneously. Use the Datastore Performance Assessment report that provides information on datastore performance, detecting whether datastores can sustain the current workload, and highlighting potential issues that can be met during the backup process.

For datastore performance assessment, you can take the following steps:

1. Open Veeam ONE Reporter.
2. Go to the Workspace tab and select VMware monitoring > Datastore Performance Assessment report.
3. Specify report parameters:
   • **Scope** – by default, Veeam will analyze data for all virtual infrastructure; you can click the link to narrow report scope
   • You can also use the Datastores list to analyze certain datastores
   • Select the Reporting interval you need (for example, current week or certain dates)
   • If necessary, specify threshold values – maximum allowed read latency and write latency (in milliseconds); optionally, use the Max. allowed reads and Max. allowed writes options, specifying the number of operations per second
4. Click Preview to generate the report.
5. Examine the displayed data:
The Assessment Results table shows the number of hosts connected to each datastore included in the report scope, the number of VMs that store data on the datastores, the number of virtual disks, and the average latency/IOPS values for each datastore. The Details section shows performance charts with IOPS and latency statistics for each datastore, and details tables with latency and IOPS.
values for every host connected to the datastore. The report also provides recommendations on actions to be taken to meet the defined parameters.

Consider that in v8 Veeam Backup & Replication introduces Backup I/O Control, a new capability that allows you to define latency thresholds for any datastore. The **Enable storage latency control** options are implemented as global settings (that is, applicable to all datastores) in Enterprise edition, and can be specified on per-datastore basis in Enterprise Plus edition:

Here:

- **The Stop assigning new tasks to datastore at <N> ms** setting instructs backup server not to assign new data processing tasks when primary storage latency reaches the specified value; backup job will wait for the datastore to become free before starting VM data processing.

- **The Throttle I/O existing tasks at** setting is designed for situations when a backup job is already running and latency becomes an issue due to an external load. For example, if a SQL maintenance process starts in a VM, using the same datastore as the backup job, then the backup job will automatically throttle its read I/O so that latency goes below the specified threshold.

To learn more about controlling storage latency, refer to the "Specifying Veeam Backup & Replication Options > Specifying Data Processing Settings" section of Veeam Backup & Replication User Guide.

**Case 2. Backup Infrastructure Setup and Optimization**

After you have set up your backup infrastructure as described in the User Guide (added servers, configured repository settings, and so on), you can configure your backup and replication jobs. For detailed information, please refer to the Veeam Backup & Replication User Guide available at [http://www.veeam.com/documentation-guides-datasheets.html](http://www.veeam.com/documentation-guides-datasheets.html).

To verify your Veeam Backup & Replication deployment against known best practices from Veeam experts, and to optimize the performance of your backup jobs, use the **Veeam Backup & Replication infrastructure assessment** report. This report analyzes your backup infrastructure against a set of recommended baseline settings and implementations, identifies VMs that cannot be properly backed up due to the certain reasons, verifies problem areas and helps mitigate the issues.
Note: Currently, this report is available for VMware environment only.

Take the following steps:

1. In Veeam ONE Monitor Client, open Data Protection view, select Backup Infrastructure in the navigation tree, and click Reports > Audit > Backup Infrastructure Assessment or Reports > Backup > Backup Infrastructure Assessment.

2. Specify report parameters:
   a. **Scope** — by default, report will analyze data about the whole backup infrastructure; in case you are interested in the certain Veeam backup server(s) and related configuration, click the Backup Infrastructure link and in the infrastructure tree select the server(s) you need.
   a. If you want to analyze the infrastructure against the requirements for 1-Click file level restore, select the corresponding check box.
   b. If necessary, select the Required Backup Window check box and define an interval for daily backup sessions that should be assessed.

3. After that, click Create report and wait for the report generation to complete. Backup infrastructure will be examined, as described in the Veeam ONE for VMware documentation section.

4. Review the summary of verification results. Click a criterion in the output table to drill down to recommendations for resolving the issue.
Backup Infrastructure Assessment

Description
This report helps you to assess your backup configuration and identify potential configuration improvements.

Report Parameters
Scope: Backup Infrastructure
Required Backup Window: From 12:00 AM To 8:00 AM
1-Click live level restores: True

Summary

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Verification Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application-aware image processing for Windows servers</td>
<td>Passed</td>
</tr>
<tr>
<td>VMware Tools Quiescence for Live/ Pause VMs</td>
<td>Warning</td>
</tr>
<tr>
<td>VMWare Tools Status</td>
<td>Passed</td>
</tr>
<tr>
<td>VMs verification</td>
<td>Warning</td>
</tr>
<tr>
<td>Job performance optimization</td>
<td>Passed</td>
</tr>
<tr>
<td>Parallel virtual disk processing</td>
<td>Passed</td>
</tr>
<tr>
<td>Virtual stand-by proxy server</td>
<td>Passed</td>
</tr>
<tr>
<td>Proxy server on the remote site</td>
<td>Passed</td>
</tr>
<tr>
<td>Direct SAN access for entire performance tweaks</td>
<td>Not required</td>
</tr>
<tr>
<td>Pending Backup Window</td>
<td>Passed</td>
</tr>
<tr>
<td>Backup job processing mode optimizations</td>
<td>Passed</td>
</tr>
<tr>
<td>Backup infrastructure configuration</td>
<td>Passed</td>
</tr>
<tr>
<td>VMs failed over to network processing mode</td>
<td>Passed</td>
</tr>
<tr>
<td>Backup server protection</td>
<td>Passed</td>
</tr>
<tr>
<td>SQL Server optimization</td>
<td>Passed</td>
</tr>
<tr>
<td>Repository free space</td>
<td>Passed</td>
</tr>
<tr>
<td>Storage latency control</td>
<td>Passed</td>
</tr>
<tr>
<td>file level restores</td>
<td>Passed</td>
</tr>
</tbody>
</table>

VMs failed over to network processing mode

Recommendation: Your Veeam Backup & Replication installation meets all known best practices.

Parallel virtual disk processing

Recommendation: Your Veeam backup & replication installation meets all known best practices.

Virtual stand-by proxy server

Recommendation: Install virtual backup proxy server on esx20.amst.local, esx22.amst.local, esx23.amst.local to avoid running full VM restores via ESXi network stack.

<table>
<thead>
<tr>
<th>Backup Server</th>
<th>vCenter Server</th>
<th>Target for Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>esx20.tw</td>
<td>vcenter51</td>
<td>esx20.amst.local</td>
</tr>
<tr>
<td>vcenter51</td>
<td>esx22.amst.local</td>
<td></td>
</tr>
<tr>
<td>vcenter53</td>
<td>esx23.amst.local</td>
<td></td>
</tr>
</tbody>
</table>

Report created: 1/21/2014 1:20:46 AM
Option for VMware VMs: Using Tags

With VMware vSphere 5.x, you can create and assign tags to facilitate your VMs grouping and searching. To learn more about tags, refer to VMware documentation [here](http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.vcenterhost.doc/GUID-E8E854DD-AA97-4E0C-8419-CE84F93C4058.html).

Veeam Availability Suite 8.0 supports vSphere tags: in addition to working with tagged VMs in Veeam Backup & Replication (for example, add them to jobs), you can also use Veeam ONE Business View to tag VMs and communicate these to VMware vSphere. So, you can create automatic rules in Business View to tag VMs and then setup backup jobs in Veeam Backup & Replication to use the vSphere tags.

Veeam ONE Business View supports automatic categorization based on static rules or dynamic groups, utilizing VM attributes (such as name, location or resource allocations).
To learn more about Business View categorization, refer to Veeam ONE documentation:

- To learn how to configure categories based on your own criteria, see [http://helpcenter.veeam.com/one/80/hyperv/index.html?configuring_categorization_scheme.html](http://helpcenter.veeam.com/one/80/hyperv/index.html?configuring_categorization_scheme.html)

Once the rules are defined in Business View, the appropriate tags are then automatically set in vSphere.

Note: Note that the tags you have configured in Veeam ONE will work with any product that uses vSphere tags.

### Case 3. Identifying Unprotected VMs

Consider that if object selection for a backup or replication job is performed based on VI containers (such as folders, hosts or datastores), or with complex exclusion parameters, some VMs can be missing backup or replica. Also, a VM backup can be outdated, missing the required RPO.

This evaluation case will help you understand how to check if the existing backups and replicas meet your stated RPO requirements:

#### Step 1. Reporting on Unprotected VMs

The Protected VMs report from Veeam ONE’s Veeam Backup & Replication report pack lists all protected and unprotected VMs including their last backup state, and allows you to identify the machines with outdated or missing backup or replicas.

Take the following steps:

1. Run your backup jobs. You can launch a job manually by selecting the job and using the Start menu command in the Backup & Replication view.
2. Wait for the jobs to complete. You can watch the results in the Last 24 hours history:

3. In Veeam ONE Reporter, run data collection for the Veeam backup server and VI server(s), as described in Collecting Data from Infrastructure. Wait for the process to complete.

4. Generate the Protected VMs report with the default parameter settings.

   To create the report, Veeam ONE retrieves and analyzes data from the following sources:
   - Historical data on backup and replication job sessions for the specified RPO period (pulled from Veeam Backup & Replication servers)
   - List of VMs in virtual inventory (pulled from VMware vSphere, Microsoft Hyper-V management servers and vCloud Director)
A VM is labeled “protected” if at least one valid backup or replica restore point meeting the designated RPO exists for it.

Note: For report to be created properly using correct data sets, make sure VI servers included in report scope are added to both Veeam Backup & Replication and to Veeam ONE (for details on adding servers, see “Adding Servers to Scope” section of this guide, and product documentation at http://www.veeam.com/documentation-guides-datasheets.html)

5. Then you can export the report in Excel format and filter out the unprotected machines.
6. In the Veeam Backup & Replication console, create one or more backup jobs that include these reported unprotected VMs.
7. Run the new job(s).
8. Repeat steps 3 and 4 from above. In the new Protected VMs report you create, make sure the listed VMs are reported as “protected”. 
Step 2. Monitoring for Unprotected VMs in Real Time

In addition to periodic reporting on unprotected VMs, it is recommended that you monitor in real time for your critical servers that may fall out of the required RPO for any reason. Veeam Availability Suite 8.0 offers real-time monitoring and alerting for missing the required RPO of your virtualized servers. This workflow is implemented by tracking the latest backup state for each VM and using predefined alarm for backup infrastructure. Moreover, right out of the box, Veeam groups all VMs based on their latest backup date in the corresponding Business View groups. This allows you to instantly obtain the list of VMs that have fallen out of the required RPO, eliminating the manual process of searching through the backup job session.

To evaluate these capabilities, do the following:

1. Create a test VM and do not include it in any backup or replication job. This VM should be listed as unprotected in the report you generate at Step 1.
2. In Veeam ONE Monitor, go to the Infrastructure view.
3. Select your test VM in the navigation tree on the left, and open the Summary tab on the right pane. Make sure the VM is included in the tagged group Last backup: no backup.
4. Switch to Business View and make sure your test VM is displayed under Virtual Machines > Last Backup Date > VMs with no backups group.
5. Then switch to **Alarm Management** view, expand **VMware > Virtual Machine** in the navigation tree, and find the **VM with no backups** alarm in the preview pane.

6. In the list of actions on the right, click **Enable** to activate this alarm. By default, alarm is assigned (will be applied) to all virtual infrastructure, so your VM will be in the scope.

7. Switch to the **Infrastructure View** and make sure the alarm was generated for your test VM, indicating no proper backup for it.

8. Open Veeam Backup & Replication management console and create a backup job that should process your test VM. Run the job when finished.
9. In Veeam ONE Monitor, open **Business View** and make sure that the test VM is no longer included in the list of VMs with no backups; in the **Infrastructure View**, browse for this VM and check that VM with no backups alarm is no longer issued for it.

**Tip:**
You can automatically trigger a backup job if alarm identifies unprotected VM. For that, configure the alarm to run a script that will run a backup job – open the **Alarm Management view**, select the necessary alarm, click **Edit** under **Actions** on the right, and on the **Actions** tab select **Run script** from the **Actions** list. For more information, refer to Veeam ONE User Guide (http://helpcenter.veeam.com/one/80/vsphere/index.html?alarm_action_settings.html).

---

**Case 4. Recovery Verification**

Recovery verification is one of the most crucial parts of data management and protection. SureBackup is a patented Veeam technology that lets you verify the recoverability of every VM backup, without additional hardware or administrative time and effort, ensuring that each VM can be safely recovered and reliably started on the host when necessary.

To test VM backups with SureBackup recovery verification, you will need to do the following in the Veeam Backup & Replication console:

1. Create an **application group** for a verified VM; it should comprise one or several VMs on which the verified VM is dependent. These are VMs running applications and services required to enable fully functional work of the verified VM. For example, to verify a virtualized Exchange server, you will need a domain controller, a DNS server and Global Catalog. For detailed information on application groups, refer to the "Verifying Backups and Replicas with SureBackup" and "Creating an Application Group" sections of Veeam Backup & Replication User Guide.

2. Create a **virtual lab** in which a verified VM from the backup or VM replica will be tested. This 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 group. 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 detailed information on virtual lab, refer to the "Verifying Backups and Replicas with SureBackup" and "Creating a Virtual Lab" sections of the Veeam Backup & Replication User Guide.

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

3. Create and start a SureBackup job. This job comprises all settings and policies configured for recovery verification of required VMs, such as application group and virtual lab to be used, VM backups that should be verified in the virtual lab and so on. A SureBackup job can be started manually or on schedule. When it runs, the following takes place:

   a. First, Veeam Backup & Replication creates an environment for VM backup verification: it starts the virtual lab, and within the lab the VMs from the application group are started in the specified order.

   b. 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 specified settings, creates several streams and tests a number of VMs simultaneously (ping, heartbeat and script execution tests can be performed for each VM). If Veeam Backup & Replication does not find a valid restore point for any of verified VMs, verification of this VM fails.

**Note:** VMs from the application group and verified VMs must belong to the same platform — VMware or Microsoft Hyper-V. Mixed scenarios are not supported.
For detailed information, refer to the "SureBackup Recovery Verification" and "Creating a SureBackup Job" sections of the Veeam Backup & Replication User Guide for VMware (or corresponding sections for Hyper-V platform).

The SureBackup Jobs Overview report helps you to discover issues in recovery verification of your VMs. Based on SureBackup job session history data, it delivers a comprehensive insight on the configuration and status of SureBackup jobs so that you can fine-tune your existing settings or include other critical VMs in verification process.

- When running this report, choose Backup Infrastructure as report scope, and Backup as job type (replica verification process is different and available for VMware platform only; see Veeam Backup & Replication for VMware documentation for details).
- Reporting period includes last 7 days (built-in value).

The Summary diagrams reveal the state of SureBackup jobs, including Success, Running and Failed, and show the detailed information on VMs that were subject to verification:

SureBackup Jobs Overview

Description

This report provides information about Veeam Backup & Replication SureBackup job and verified VMs latest status.

Report Parameters

Scope: Virtual Infrastructure
Job Type: All

Summary

The Summary diagrams reveal the state of SureBackup jobs, including Success, Running and Failed, and show the detailed information on VMs that were subject to verification.

Note: The SureBackup job status is set to Failed if no valid restore point can be found for a VM being verified (or for any VM from the application group).
Case 5. Controlling Backup Repository

This evaluation case will help you understand how to configure the backup infrastructure monitoring to fire alarms on a repository that becomes unavailable due to connection failure; you will also learn how Veeam ONE facilitates repository capacity planning.

Step 1: Setting Up Availability Monitoring

Proper network connectivity between various infrastructure components is a need for data transfer and management operations. Any firewalls that exist between various infrastructure components may require ports being opened to allow for appropriate proper communications (see the "Used Ports" section of the Veeam Backup & Replication User Guide). However, the Veeam backup server may lose connection to the repository due to any of the possible reasons: firewall issues, disconnected network cable, network card failure, repository service failure, or power state. A person in charge needs to be timely notified of the problem and resolve it or escalate properly.

Take the following steps:

1. In Veeam ONE Monitor, configure the e-mail notification settings. For that, use the property tabs available after you select Options > Server Settings in Veeam ONE Monitor toolbar:
   - Specify SMTP server settings, as well as sender and recipient address.
   - Add the recipient to default email notification group by clicking Configure and typing in e-mail address. Make sure this group includes a mailbox that you have access to.

   ![Configure Email Notification Group]

   - Leave the default e-mail notification policy settings (to be notified on mission-critical alarms for the virtual infrastructure right after they are triggered).
   - You can use the default email notification template – the subject line will start with [Veeam ONE Monitor] Alarm and contain alarm details.

2. Open the **Alarm Management** view in Veeam ONE Monitor. You can either search for the alarms on the backup repository, or select the **Backup repository connection failure** alarm from the navigation tree under **Backup & Replication > Repository**.

3. Click **Edit** in the **Actions** list on the right.

4. On the **General** alarm property tab, make sure the **Enable this alarm** check box is selected.

5. On the **Rule** tab, make sure the **Enabled** check box is selected.

6. On the **Actions** tab, make sure the **Send email to a default group** is selected – this should be the group you have populated when setting up for case 2 above. Ensure it includes a mailbox that you have access to.

7. Click **OK** to close the dialog.

Now you can proceed with imitating a repository connection failure.

On a Windows repository, Veeam Backup & Replication deploys a local 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 Backup Proxy service with Veeam Data Mover service, on that server). When any job addresses the repository, the transport service on the repository establishes a connection with the source-side transport service on the backup proxy, enabling efficient data transfer over LAN or WAN. For more details on Windows-based repository and its operation, please refer to Veeam Backup & Replication User Guide.

So, to imitate repository connection failure, you can stop the Veeam Data Mover service (in case of all-in-one deployment, it is co-located with Veeam Backup service).

Take the following steps:

1. Use the Windows **Services** management snap-in to stop **Veeam Data Mover service**.

2. Open the mailbox you have configured as a default recipient for alarm notifications. The mailbox should contain the item from the corresponding sender (veeam_one@mycompany.com in our example) with the subject line containing **[Veeam ONE Monitor] Alarm – Backup repository connection failure for <repository_server_name>** and alarm details and KB.
3. In Veeam ONE Monitor, open **Data Protection** view and on the **Alarms** tab make sure the **Backup repository connection failure** alarm has been issued by the machine hosting your repository.

4. Use the **Services** snap-in to start Veeam Backup service on the repository server.

**Step 2: Setting Up Free Space Monitoring**

Another matter of great importance is repository sizing and capacity planning. It requires consideration of two primary factors, space and I/O performance. So, it is recommended that you have a mechanism in place that allows you to configure a threshold for repository free space and automatically notifies you before the situation becomes critical. With no headroom for new backups and recoveries, your DR strategy may become compromised. Also, a means for capacity planning will be of use – it can help you to analyze the historical and current storage utilization data and estimate the amount of additional space that needs to be provisioned to accommodate the necessary restore points.

A backup administrator should track free space available on the backup repository and get notified of decreased space before the limit is reached. Veeam ONE Monitor allows you to automate this course of action.

Take the following steps:

1. In Veeam ONE Monitor, open the **Alarm Management** view. You can either search for the alarms on backup repository, or select the **Backup repository free space** alarm from the navigation tree under **Backup & Replication > Repository**.
2. Click Edit in the Actions list on the right.
3. On the General alarm property tab, make sure the Enable this alarm check box is selected.
4. On the Rule tab, make sure the Enabled check box is selected. In the Rule parameters section, you can configure the threshold value for repository free space to trigger a warning and an error state (measured as a percentage of overall repository capacity). Default values are:
   - 10% free space left – for warning
   - 5% free space left – for error

For evaluation purposes, you can set these limits, for example, to 30% and 20%. After finishing the evaluation case reset them to defaults — for smooth test lab operation.
5. On the Actions tab, make sure the Send email to a default group is selected – this should be the group you have populated when setting up for Step 1: Setting Up Availability Monitoring above. Ensure it includes a mailbox that you have access to.

6. Click OK to close the dialog.

Backup repositories tend to run out of free space due to poor sizing, or if the retention policy is too relaxed – outdated restore points clutter the datastore and decrease storage capacity depletion.

1. To populate the repository, you can, for example, create a backup job for a large-sized VM; you can use the backup job settings to modify retention so that it includes more restore points. You can also use the backup import feature and other possibilities to saturate the repository.

2. Open the mailbox you have configured as default recipient for alarm notifications. The mailbox should contain the item from the corresponding sender (veeam_one@mycompany.com in our example), with the subject line containing [Veeam ONE Monitor] Alarm – Backup repository free space from <repository_server_name> and alarm details and KB.

3. In Veeam ONE Monitor, open Data Protection view and on the Alarms tab and make sure the Backup repository free space failure alarm has been issued by the machine hosting your repository.

Step 3: Capacity Planning for Repository

This report analyzes the amount of free space on backup repositories and estimates the projected date when the repository will run out of available storage capacity. The report provides recommendations on how to adjust the allocated storage resources in order to meet the future demand for backup storage. Furthermore, it calculates the amount of additional space that needs to be provisioned to accommodate the necessary restore points.

Take the following steps:

1. In Veeam ONE Monitor Client, open Data Protection view and click Reports > Datastore > Capacity Planning for Backup Repositories or Reports > Forecasting > Capacity Planning for Backup Repositories.
2. Configure the following report parameters:
   a. **Scope** – check that **Backup Infrastructure** is selected
   b. **Space Utilization Limit (%)** – set to **90**
   c. **Ensure there is enough capacity for selected number of days** – set to **30**

3. Click **Preview** and wait for the report to be generated.

The report helps you analyze configuration and disk space usage on backup repositories and forecast how many days remain before the repository reaches its full capacity. The report also provides the summary of your backup infrastructure configuration, including the total number of associated repositories, the number of jobs and the number of VMs included in backups.

### Capacity Planning for Backup Repositories

#### Description

This report shows the dynamics of backup repository free space usage and identifies the date when the repository will run out of free space.

#### Report Parameters

<table>
<thead>
<tr>
<th><strong>Scope</strong></th>
<th><strong>Backup Infrastructure</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Space utilization limit:</strong></td>
<td>90.0 %</td>
</tr>
<tr>
<td><strong>Ensure there is enough capacity for selected number of days:</strong></td>
<td>30 day(s)</td>
</tr>
</tbody>
</table>

#### Summary

<table>
<thead>
<tr>
<th><strong>Backup Infrastructure:</strong></th>
<th><strong>Physical Resources:</strong></th>
<th><strong>Capacity Planning:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of repositories:</td>
<td>Total capacity: 1.6 TB</td>
<td>Min days left: 0</td>
</tr>
<tr>
<td>Number of jobs:</td>
<td>Total free space: 0.7 TB</td>
<td>Space required: 1.7 TB</td>
</tr>
<tr>
<td>Number of VMs stored:</td>
<td>Utilization ratio: 54.66%</td>
<td></td>
</tr>
</tbody>
</table>

#### Top 5 Utilized Repositories (GB)

#### Top 5 Repositories by Days Left

#### Details

<table>
<thead>
<tr>
<th>Days Left</th>
<th>Repository</th>
<th>Backup server</th>
<th>Type</th>
<th>Capacity (GB)</th>
<th>Free Space (GB)</th>
<th>N of VMs</th>
<th>Days Left</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 30 days</td>
<td>CIFS on 1487</td>
<td>172.16.21.144</td>
<td>CIFS Share</td>
<td>323.92</td>
<td>148.96</td>
<td>14</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Default Repository</td>
<td>172.16.21.144</td>
<td>Windows</td>
<td>88.99</td>
<td>14.78</td>
<td>0</td>
<td>17</td>
</tr>
</tbody>
</table>

The last section of the report includes recommendations on repository planning - for example, you may need to target some of your backup jobs to other location.
Case 6. Performing Restore Operations

This evaluation case will help you understand how to carry out, analyze and report on restore operations performed within the backup infrastructure. Veeam Availability Suite offers data collection and reporting on the following actions:

- Restoration through the Veeam Backup & Replication console by backup operators
- Recovery through Veeam Backup Enterprise Manager conducted by the virtualization administrators
- Software restore capabilities through PowerShell and RestfulAPI

The evaluation procedure below describes how to audit the restore operations activity performed via the Veeam Backup & Replication console.

Note: Another option to delegate restore rights to authorized personnel and to configure restore restrictions is to deploy Veeam Backup Enterprise Manager and use its security roles. To read more about security settings and restore operations, please refer to the Enterprise Manager User Guide.

The evaluation procedure includes the following steps:

1. Performing a Full VM restore from the Veeam Backup & Replication console (see Step 1. Performing Full VM Restore)
2. Restoring guest OS files restore from the Veeam Backup & Replication console (see Step 2. Restoring Windows Guest OS File)
3. Restoring SQL Server database with Veeam Explorer for Microsoft Exchange (see Step 3. Restoring Application Items)
4. Creating a report on restore operations using Veeam ONE (see Step 4. Examining Restore Operator Activity)

Note: Before you perform full VM restore, make sure that the VM you plan to recover has been successfully backed up at least once. For that, open the Backup & Replication view, select the Backups node in the inventory pane; expand the backup job and check if there is at least one restore point available for the VM.

Also, make sure that the original VM is powered off. If the original VM is running, Veeam Backup & Replication will not be able to restore the VM from the backup to the original location.

Step 1. Performing Full VM Restore

1. Open the Backup & Replication view and select the Backups node. In the working area, expand the backup job you have run, right-click the VM to restore and select Restore entire VM to start the wizard.
2. On the Virtual Machines step of the wizard, click Next.
3. On the Restore Mode step, check that Restore to the original location option is selected; click Next.
4. On the Reason step, enter the restore reason, for example, “Recovery capability evaluation”. Click Next.
5. Check specified settings for full VM recovery of a VM and click Finish. Veeam Backup & Replication will restore selected VMs in the specified destination.
6. Connect to the destination host and make sure the VM has been restored to the specified location and powered on.
Step 2. Restoring Windows Guest OS File

When recovering guest OS files from Windows-based VMs, Veeam Backup & Replication does not extract the VM image from the backup. Instead, it mounts the content of a backup file directly to the Veeam Backup server and displays the file tree in the built-in file browser. You can copy the files you need and save them locally or anywhere on the network.

Consider that the VM’s file systems supported by Veeam Backup & Replication file-level recovery capabilities include Microsoft Windows file systems: FAT, NTFS, and ReFS.

1. Open the Backup & Replication view and select the Backups node. In the working area, expand the backup job you have run, right-click the VM to restore and select Restore guest files (Windows).
2. On the Restore Point step of the wizard, choose the restore point for VM to recover and click Next.
3. On the Restore Reason step, enter “File restore”.
4. On the Summary step, review the information about the recovered VM and click Finish.
5. Wait while the VM backup is mounted to Veeam Backup server; Windows file system tree will be displayed in Backup Browser like shown below. Browse to the file you want to restore:

   ![Backup Browser Screenshot]

   6. Right-click the selected file and choose Copy to; enter c:\backup\restored. You can also select to Preserve permissions and ownership. Click OK.

   ![Choose Folder Screenshot]

   When the process is complete, browse the specified folder (c:\backup\restored) for the recovered file.
Step 3. Restoring Application Items

Veeam Backup & Replication allows you to restore business application items without a need to fully recover corresponding application server VM:

- Microsoft Exchange mailbox items
- Microsoft SQL Server databases
- Microsoft Active Directory objects
- Microsoft SharePoint documents and lists

For details, refer to the Veeam Explorers guide.

The following example explains how to evaluate Microsoft SQL Server database restore capabilities.

Example: Microsoft SQL Server Database Restore

To provide for recoverability of SQL server database, make sure you have an application-consistent backup (with VSS enabled) of your SQL server VM created successfully. Also, if you plan to restore the database to its state as of the certain point in time (not necessarily the restore point, that is, backup or replica), then transaction log processing should be configured, as described in the "Required Microsoft SQL Server Backup Job Settings" section of Veeam Explorers guide.

For the sake of simplicity, this example describes the recovery of SQL server database to the selected restore points. By default, it has Simple recovery model - this setting supports for database restore to selected restore point. To learn about prerequisites and settings required for other restore scenarios, refer to the "Working with Veeam Explorer for Microsoft SQL Server" section of the Veeam Explorers guide.

You can do the following:

1. Prepare an SQL server VM backup - for instance, you can set up a test VM that meets requirements for Veeam Backup Enterprise Manager, and install Enterprise Manager there, using SQL Server Express shipped with the setup. Setup will create a database named VeeamBackupReporting that will keep configuration data collected from added Veeam backup server(s), so remember to add your Veeam backup server to Enterprise Manager and run data collection.

   Note: For information on installation and initial configuration of Enterprise Manager, see Installing Veeam Backup Enterprise Manager and Initial Configuration sections of the User Guide.

2. In Veeam Backup & Replication management console, create a backup job including the Enterprise Manager server VM.

3. On the Guest processing step of the wizard, select the Enable application-aware image processing check box.

4. Click the Applications button, then in the dialog displayed, select the Enterprise Manager server VM from the list and click Edit.

   a) On the General tab, make sure you have the Require successful application processing option selected in the Applications section.
b) Make sure the **Process transaction logs with this job (recommended)** option is selected - this makes the SQL tab settings available.

c) On the SQL tab, you can select any log processing option, as this example assumes the database will be restored to the state as of the SQL server restore point, and this scenario does not require transaction logs.

5. Click **OK** to save the settings and close the dialog.

6. On the **Job schedule** step of the job wizard, make sure the scheduled run is enabled for the job.

7. Finish the wizard and launch the job.
8. When you have server backup created successfully, launch Veeam Explorer for Microsoft Exchange - for that, in Veeam Backup & Replication, open the Backup & Replication view, select the Backups node, then in the right pane expand the backup job with the SQL server. Select the server VM, and click Application items > Microsoft SQL Server on the toolbar.

9. You will pass to the Restore Point step of the Microsoft SQL Server Database Restore wizard. Make sure the default option Restore from the latest available backup is selected.

10. Next, enter the reason for database restore (optional), review the restore summary, and finish the wizard.

11. After that, Veeam Explorer for Microsoft SQL Server will be launched, with the SQL server hierarchy automatically added to its scope and shown in the navigation tree. Then you can use Veeam Explorer for Microsoft SQL Server 1-Click Restore functionality for VeeamBackupReporting database.

Step 4. Examining Restore Operator Activity

The report delivers information on all files, application-level and VM restore activities conducted by authorized users. This information includes initiating user, name of the item or VM being recovered, the intended restore destination and the status of the completed job. Data is arranged by type of restore action performed. To examine restore operator activity, do the following:

1. In Veeam ONE Reporter, run data collection for your Veeam backup server.

2. In Veeam ONE Monitor Client, open Data Protection View, click Reports on the toolbar and select Audit > Restore Operator Activity.

3. Configure the following report parameters:
   a. Scope – check that Backup Infrastructure is selected
   b. Users – select All
   c. Restore Type – select All
   d. Reporting Period – you can select Current week or Current day.
4. Click **Create report** under **Actions** on the right and wait for report to be generated.

5. When the report is ready, review the **Restores by User** chart and check that account you used to work with Veeam Backup & Replication and carry out restore procedures (see the previous sections) is displayed in the list of user accounts. Also, check the following:

   - The **Full VM Restore** and **Guest Files Restore** operations for selected VM are included in report data
   - The **Initiator** column contains the account you used when accessing Veeam Backup management console to perform the restore
   - The **Restored Item** column contains the corresponding VM (for full VM restore) and file (for guest file restore)

---

**Case 7. Auditing and Compliance**

This evaluation case includes several steps illustrating how to use Veeam Availability Suite to meet auditing and compliance requirements for your infrastructure.

**Step 1. Tracking Job Configuration Changes**

Since jobs can be configured from the Veeam Backup & Replication console, Veeam Backup Enterprise Manager console, using PowerShell scripts or through REST API, in large environments with multiple backup administrators it is often hard to tell who, when and what changed.
The **Job Configuration Change Tracking** report provides detailed information on job configuration changes performed within the reporting period including the exact time and the user account name who did the change.

Take the following steps:

1. In the Veeam Backup & Replication console, select any of existing jobs, and from its shortcut menu select **Edit**.
2. In the job wizard, proceed to the **Schedule** step and select (or clear, if selected) the **Run this job automatically** checkbox:

   ![Edit Backup Job](image)

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

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

   - **Run the job automatically**
   - **Daily at this time:**
   - **Monthly at this time:**
   - **Periodically every:**
   - **After this job:**

   - **Automatic retry**
   - **3 times**
   - **Wait before retry attempts for:**
   - **10 minutes**

   - **Backup window**
   - **Terminate job if exceeds allowed backup window**

   - **Details** table lists the modified jobs (grouped by Veeam backup server), displaying modified property, its old and new values, as well as modification date and initiator.

3. Click **Finish** to close the wizard.
4. In Veeam ONE Reporter, run data collection for the Veeam backup server where you have modified the job.
5. In Veeam ONE Monitor Client, open **Data Protection View**, click **Reports** on the toolbar and select **Audit > Job Configuration Change Tracking**.
6. Configure the following report parameters:
   a. **Scope** – check that **Backup Infrastructure** is selected
   b. **Period** – specify reporting period you need (for this example, it should include current day)
   c. **User** – default setting is **All items**
   d. **Job Type** – select what job types you want to be included in the report on configuration changes; by default, **All items** (jobs of all types) will be reported.
7. Click **Create report** under **Actions** on the right and wait for the report to be generated.

   The **Job Modifications by User** and **Modifications by Day** charts displays the number of job configuration changes performed by each authorized user and the daily number of changes.

   The **Details** table lists the modified jobs (grouped by Veeam backup server), displaying modified property, its old and new values, as well as modification date and initiator.
8. Then locate the job you have modified (use the search field in the UI, if necessary). Make sure the IsScheduleEnabled property is included in Property changes, with corresponding data in the Previous Setting, New Setting, Modification Time and Modified By columns.

Step 2. Examining Delegated Restore Permissions

Veeam Backup & Replication supports for delegation of restore permissions to users and groups in a granular way on as-needed basis. It is possible, for example, to delegate permissions to recover files without actually being able to see the contents of the files, or to recover only Microsoft Exchange items, or to restore entire VM.

On one hand, this feature allows users to service their own needs, providing for greater efficiency and less cost to the business. On the other hand, auditing of such granular restore permissions manually can be quite a challenge, especially for large environments with dozens of restore operators. This may cause inefficient resource usage and unwarranted or uncoordinated restores.

This evaluation task will help you understand how restore permissions can be delegated and then audited, using Veeam Availability Suite.
Do the following:

1. If not present, create a test user account on the server where your test lab is deployed.
2. Open Veeam Backup Enterprise Manager web UI and log in with administrative account (this can be the account under which you ran the setup).
3. Go to **Configuration** and select **Roles**, then click **Add** to create a new role assignment.
4. Specify **User** as **Account type**, then enter the account you created at step 1.
5. From the **Role** list, select **Restore Operator**.
6. Specify **All virtual machines** as restore scope.
7. Select the corresponding check boxes to allow this account to perform full VM restore and guest files restore.

8. Click **OK** to save the settings and close the dialog. The newly created role will be displayed in the list. You can click **Rebuild roles** to refresh the scope.
9. In Veeam ONE Monitor, make sure you have Veeam Backup Enterprise Manager server added to the list of managed servers (see “Adding Servers to Scope” section for more information).
10. In Veeam ONE Reporter, go to the **Configuration** tab and run data collection for Veeam Backup Enterprise Manager server (see “Collecting Data from Infrastructure” section for more information). Wait for the process to complete.
11. In Veeam ONE Monitor Client, open **Data Protection View**, select Enterprise Manager server from the navigation tree, then click Reports on the toolbar and select Audit > **Delegated Restore Permissions** Overview report.
12. Specify report **Scope** - select Veeam Backup Enterprise Manager server; you can also specify how you want report data to be grouped.
13. Click **Create report** under **Actions** on the right and wait for report to be generated.
14. Examine the report and make sure the account you configured at steps 3-8 is included in the list, with proper delegated restore permissions.
Step 3. Assessing VM Backup Compliance

This evaluation case will help you understand how to detect the VMs that do not comply with '3-2-1' approach and how to take corrective measures. It will use the VM Backup Compliance Overview report to check if there are any VMs with insufficient number of backup copies.

Note: A backup copy in this context refers to a VM’s restore point created by a successful run of a backup/replication/backup copy/tape archiving job. For example, if a VM is included into a backup job and into a VM-to-tape archiving job, both completed successfully at least once, this means that there are 2 backup copies. However, if a VM-to-tape job has created no restore points for a VM (that is, the job failed), you will have only 1 backup copy reported.

Having identified these non-compliant machines, you can appropriately modify existing job settings, add these VMs to new jobs, or dynamically adjust your retention policies.

Take the following steps:

1. Run data collection for your Veeam backup server.
2. In Veeam ONE Monitor Client, open Data Protection View, click Reports on the toolbar and select VM > VM Backup Compliance Overview.
3. Configure the following report parameters:
   a. Scope – check that VI is selected
   b. Required Number of Copies – set to 2
   c. Exclusion mask – specify a mask for VMs to be excluded from the report (if any)
4. Click Create report under Actions on the right and wait for the report to be generated.
5. Save the list of non-compliant VMs and actual number of copies by exporting the report into the file format you prefer.

After that you can open the Protected VMs report (see Case 3 above) to identify which backup jobs process these non-compliant VMs. Take the following steps:

1. Specify the following parameters for running this report:
   - **Scope** – Virtual Infrastructure
   - **Job type** – backup and replication jobs

2. Create the report.

3. In the Protected VMs section, look for VMs you need, and in the Backup Job column find the corresponding job name.

Now let’s modify the job settings so that it creates a required number of backup copies.


5. Then in the Backup & Replication view, select Jobs>Backup in the navigation tree, and in the right pane, locate the job that processes VM(s) from the list you have saved.

6. Right-click the job and select **Edit**.

7. Proceed to the Storage step of the job wizard. Select the Configure secondary destination for this job check box.
8. On the **Secondary Target** step, click **Add** and select the backup copy job.

9. Complete the wizard, saving the changes.

10. Start the modified job and wait for its completion.

11. In Veeam ONE Reporter, run data collection for your Veeam backup server to collect the latest information on the completed job. Wait for it to complete.

12. Run the **VM Backup Compliance Overview** report again, following the above step procedure.

13. Make sure the VM previously reported as non-compliant is no longer in the list.

### Step 4. Identifying Orphaned VMs

Another problem that can occur during a daily backup job management is when a VM is no longer backed up, but still present in the backup files and in need of protection. This may happen due to an error or oversight, job misconfiguration or some automatic procedures (for example, when the VM migrated to an unprotected host through vMotion).

Veeam ONE's **Orphaned VMs** report conveniently lists all the VMs that are missing in the backup job but have existing restore points in the backup files to properly identify the VMs that need backed up. It discovers VMs that are present in existing backup files, but are missing in backup, replication or backup to tape jobs. This data will help you to decide whether to modify the backup job settings for the VM if it is a mission critical one, or to delete the VM from the backup if it is no longer necessary.

Take the following steps:

1. In Veeam Backup & Replication management console, select any existing backup job and click **Edit** on the toolbar to start the job wizard.

2. Proceed to the **Virtual Machines** step, select a VM and click **Remove**. The virtual machine will be no longer backed up by the job.
3. Finish the wizard.

4. In the backup repository (default is local C:\backup folder on the Veeam backup server), make sure the folder with that VM backup still exists.

5. In Veeam ONE Reporter, run data collection for your Veeam backup server.

6. In Veeam ONE Monitor Client, open Data Protection View, click Reports on the toolbar and select VM > Orphaned VMs.

7. Configure the following report parameters:
   a. Scope – use Backup Infrastructure
   b. Group by – is set to Type of protection

8. Click Create report and wait for the report to be generated.
   The report enumerates all found VMs and provides details on the type of VM protection, the number of restore points accommodating the VM, the backup location and the date of the most recent backup session. Additionally, it states when the backup will be deleted according to the current file retention policy.

9. Make sure the VM you removed from backup job at Step 2 is listed in the report.
Step 5. Identifying VMs with no Archive Copies

To build a successful data protection and disaster recovery plan, industry best practices recommend that you have at least three copies of your data, for example, production data, backup and its copy - and two different types of media to store copies of your data, for example, disk storage and tape. This approach represents the 3-2-1 backup strategy.

The **VMs with no Archive Copy** report allows you to identify whether your VMs are protected with backup copies stored on secondary backup repositories and on tape. Since this evaluation case assumes there is no tape devices configured in your backup infrastructure, the report is expected to display no VMs backed up to tape media.

Take the following steps:

1. In Veeam ONE Reporter, run data collection for your Veeam backup server.
2. In Veeam ONE Monitor Client, open **Data Protection View**, click **Reports** on the toolbar and select **VM > VMs with no Archive Copy**.
3. Configure the following report parameters:
   a. **Scope** – check that **Virtual Infrastructure** is selected
   b. **Exclusion mask** – specify a mask for VMs to be excluded from the report (if any)
   c. **Reporting Interval** – is set to **Last Month**
4. Click **Create report** and wait for the report to be generated.

   The **VMs by Archive Status** chart displays the number of VMs with and without archive copies.

   The **VMs per Backup Location** chart depicts the locations of backup copies (primary or secondary repository or tape).
The **Details** table contains information on the location of a primary and secondary VM copy, availability of tape backups for the listed VMs and the date of the most recent VM backup. Make sure the **Tape Media Set** column does not contain any data.

### VMs with no Archive Copy

**Description**

This report highlights all VMs that do not have archive copy.

**Report Parameters**

- **Scope:** Virtual Infrastructure
- **Excluded VMs:**
- **Reporting Interval:** Last Month

**Summary**

**VMs by Archive Status**

- **5** VMs with at least 1 archive
- **3** VMs with no archives

**VMs per Backup Location**

- **12** VMs

### Details

<table>
<thead>
<tr>
<th>Location</th>
<th>VMs</th>
<th>Main Backup Repository</th>
<th>Secondary Backup Repository</th>
<th>Tape Media Set</th>
<th>Last Backup Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mar2101</td>
<td>5</td>
<td>Backup1</td>
<td></td>
<td></td>
<td>1/22/2016 12:07 AM</td>
</tr>
<tr>
<td>sn04</td>
<td></td>
<td>Backup Repository on SRV01</td>
<td></td>
<td></td>
<td>1/22/2016 12:07 AM</td>
</tr>
<tr>
<td>s04</td>
<td></td>
<td>Backup1</td>
<td></td>
<td></td>
<td>1/22/2016 12:07 AM</td>
</tr>
<tr>
<td>web01</td>
<td>6</td>
<td>Backup1</td>
<td></td>
<td></td>
<td>1/22/2016 12:07 AM</td>
</tr>
<tr>
<td>weber01</td>
<td></td>
<td>Backup Repository on SRV01</td>
<td></td>
<td></td>
<td>1/22/2016 12:07 AM</td>
</tr>
<tr>
<td>vms01</td>
<td></td>
<td>Backup1</td>
<td></td>
<td></td>
<td>1/22/2016 12:07 AM</td>
</tr>
<tr>
<td>sn04</td>
<td>4</td>
<td>Backup Repository on SRV01</td>
<td></td>
<td></td>
<td>1/22/2016 12:07 AM</td>
</tr>
<tr>
<td>sn04</td>
<td></td>
<td>Shared Vol</td>
<td></td>
<td></td>
<td>1/22/2016 12:07 AM</td>
</tr>
</tbody>
</table>

**Case 8. Virtual Infrastructure Monitoring and Alerting**

This evaluation case will help you understand how to configure virtual infrastructure monitoring rules to produce alarms on health and performance issues that may occur in your virtual infrastructure and to send notification on the triggered alarm rule.

For example, **Latest snapshot age** alarm is triggered if the current snapshot is older than a specified number of hours. The alarm helps monitor forgotten snapshots that are consuming valuable storage space and degrading performance of virtual machines.

Follow these steps to see how it works:

1. In Veeam ONE Monitor, make sure you have e-mail notification settings configured (refer to the corresponding sections of this document and Veeam ONE User Guide for details).
2. Go to the Alarm Management view.
3. In the navigation tree, select VMware > Virtual Machine > Latest Snapshot Age alarm.

4. From the list of Actions on the right, select Edit.
5. In the alarm properties, go to the Rules tab and in the Rule Parameters section, set VM snapshot age (Hours) value to 1:
6. Click **OK** to save the settings.
7. Create a snapshot of a test VM by VMware means.
8. Wait for 60 minutes, then look through the mailbox you specified as the email recipient for alarm notification. The mailbox should contain the item from the corresponding sender (veeam_one@mycompany.com in our example), with the subject line containing **[Veeam ONE Monitor] Alarm – Latest snapshot Age from <VM name>** and alarm details and KB.
9. Then in Veeam ONE Monitor, open the **Infrastructure** view, switch to the **Alarms** tab and look for the alarm from the test VM as a **Source**:

![Alarm Console Example](image)

---

**Case 9. Advanced Capacity Planning and "What-if" Modelling**

Veeam ONE deployment projects allow you to predict future resource utilization and plan resource reservations in your virtual environment, using automated "what-if" calculations and reporting. Deployment projects compare the projected resource capacities against the future resource demand, help identify potential resource shortages and provide practical recommendations that an administrator should undertake to succeed with the actual deployment.

This evaluation case explains how to model host and VMs deployment scenario, using Veeam ONE deployment project. The deployment project estimates resource usage against specified thresholds after adding required physical resources. It is considered successful if future resource utilization and performance metrics do not breach these thresholds. Take the following steps:

1. In Veeam ONE Reporter, go to the **Workspace** tab and in the navigation tree, select **All deployment projects**.
2. In the preview pane on the right, click the **Add** button. In the **Add project** dialog, enter the new project name.
3. Click the link next to the **Container Name** and select the host where the planned infrastructure should be deployed. This can be a standalone host or a cluster.

4. Click the link next to the **Datastore** fields in order to choose the resources for the estimation.

5. After that you need to model the deployment scenario you want to implement, populating the list of hosts and/or VMs you plan to deploy. For that, click the **Edit** button. In the dialog displayed, click **Add** to configure the virtual machine or the host you want to include in the deployment. In this example, the scenario includes deployment of one host and four virtual machines.

6. Select **Host** and click **Next**.

7. In the **Configuration** page, provide host configuration settings:
   - To use custom configuration settings, you can select **Host Configuration** and enter the necessary values for **CPU** and **Memory**.
To use any existing host from the infrastructure as a sample for the new host you plan to deploy, select **Existing Host** and click the link to select the machine you need. The "what-if" model will assume that a newly added host is of the same configuration as your selection.

8. Click **Finish** to save the settings and close the dialog.

9. Back in the **Edit scenario** dialog, click **Add** and follow similar steps to add virtual machines: select **Virtual Machine** and click **Next**.

10. In the **Configuration** page, select **VM Configuration** for custom settings, or select **Existing VM** and use the link to choose the sample infrastructure VM. With VM Configuration option selected, specify values for **CPU, Memory, and Storage**.
11. After finishing, return to Edit scenario dialog. Here you can adjust the number of VMs, using the Count value.

12. Click OK to save the settings and close the dialog.

13. Next, specify the date when you plan your deployment project to be implemented, and click OK to finish deployment project creation. The new project will appear in the list of projects in the preview pane, with its State as Needs to be calculated.

14. Click Thresholds to review the default threshold values for physical resource usage; you can modify them as necessary. For this example, the default values will be used.
15. Finally, run the automated report on ‘what-if’ modeling by clicking the **Build** button. Project **State** will be updated, and you can then click **View report** to examine the forecast data and recommendations on your deployment project:

- The estimation result figures out constrained resources (if any), displaying them in the **Report Parameters** section.

- The report also contains modelling results for compute resources (CPU, vCPU and memory) and for storage resources, estimating whether the selected host and datastore are capable of maintaining suggested infrastructure.

- The **Recommendations** section explains what the shortcomings of the estimated scenario are, and what resources should be provided to support your suggested deployment.
Deployment Scenarios Modelling

**Description**

This report helps you to model different VM deployment scenarios and estimate resource usage after adding or removing physical resources.

**Report Parameters**

**Project Name:** Infrastructure modernization

**Modelling Result:**

<table>
<thead>
<tr>
<th>Constrained Resource</th>
<th>Estimated Usage (%)</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage</td>
<td>1.56 GB</td>
<td>1.56 GB</td>
</tr>
</tbody>
</table>

**Scope:** esx1, esx2, esx3

**Datastores:** Datastore1

**Deployment Dates:** 1/1/2015

**CPU Usage Threshold:** 80.00%

**vCPU Per Core:** 4

**Memory Usage Threshold:** 90.00%

**Storage Space Usage Threshold:** 90.00%

**Project Details**

<table>
<thead>
<tr>
<th>Action</th>
<th>Object Type</th>
<th>Name</th>
<th>Number</th>
<th>CPU (%)</th>
<th>vCPU/Cores</th>
<th>Memory Allocated/Used (MB)</th>
<th>Storage (GB)</th>
<th>Disk Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Host</td>
<td>esx1, esx2, esx3</td>
<td>1 2 3</td>
<td>20.00</td>
<td>2</td>
<td>4.00 / 4.00</td>
<td>100.00</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Virtual Machines</td>
<td>server1</td>
<td>1</td>
<td>60.00</td>
<td>4</td>
<td>4.00 / 4.00</td>
<td>100.00</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>server2</td>
<td>1</td>
<td>60.00</td>
<td>4</td>
<td>4.00 / 4.00</td>
<td>100.00</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hypervisor</td>
<td>1</td>
<td>60.00</td>
<td>2</td>
<td>5.45 / 8.42</td>
<td>3234.47</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>dhall</td>
<td>1</td>
<td>60.00</td>
<td>4</td>
<td>4.00 / 4.00</td>
<td>100.00</td>
<td>1</td>
</tr>
</tbody>
</table>

**Total Usage Profile**

**Modelling results for Compute resources**

- **CPU (GHz):**
  - Average: 0.00%
  - Peak: 0.00%
  - Full (95%): 0.00%

- **vCPU:**
  - Average: 44.52%
  - Peak: 29

**Modelling results for Storage resources**

**Datastores affected by current project**

- **Warning:**
  - Datastore1 (Vdisk1) (Vdisk2) (Vdisk3) (Vdisk4) (Vdisk5) (Vdisk6) (Vdisk7) (Vdisk8) (Vdisk9) (Vdisk10) (Vdisk11)

**Provisioned virtual disks**

- **VM Name:** vcenter1
  - 2
  - 500.00 GB

- **Logically Mirrored**
  - 1
  - 500.00 GB

**Physical Storage**

- **Storage:**
  - 203.16

**Recommendation**

To deploy your current project and keep capacity under chosen thresholds add: 2 Datastore(s) like datastore1 with Capacity: 1860.75 GB

---

58 | Veeam Availability Suite | EVALUATOR’S GUIDE | REV 1
16. Return to your deployment project in the preview pane and click **Edit**.

17. Implement the recommendations provided in the report. For this example, two datastores were added to increase the capacity under default thresholds.

18. Save the modified scenario and click **Build**. Check that value in the **State** column has changed to **Passed**.

19. Click **View report** and make sure the updated scenario has no failures reported. Save the report, for example, by exporting it in PDF format.

20. After you have run a simulation based on a deployment project and saved the report with the modelling results, you can flag the project as **Completed**. This will instruct Veeam ONE to assume that all resources tied up to the project can be released and made available for calculation of the concurrent projects. Make sure the check box next to the project name is selected; click the **Complete** button and confirm the operation.

21. Check that the project status has changed to **Completed** and that is has been removed from the list of **Active** deployment projects – for that, apply filter in the preview pane, in the top right corner.