Nutanix Best Practices
Veeam Backup and Replication v8 on VMware
1 Executive Summary

The Nutanix Virtual Computing Platform is a scalable virtualization platform for desktop, server, and big data deployments. This document provides recommendations for the optimization and scaling of Veeam Backup & Replication v8, part of Veeam Availability Suite, with Nutanix and VMware vSphere. It shows the scalability of the Nutanix Virtual Computing Platform and provides configuration information on the scale-out capabilities of both Veeam Backup & Replication and Nutanix.

Customers can easily back up large-scale Nutanix deployments with the most reliable transport method using Veeam network backup mode and the Nutanix 10Gb NICs. Depending on their requirements and available hardware, network mode lets customers to choose between using either type of proxy server.

About Nutanix

The Nutanix Virtual Computing Platform consists of modular “blocks” that include compute, storage, and network. This design greatly reduces costs while increasing performance and scalability, enabling fast, efficient, and reliable backups. The Nutanix Distributed File System (NDFS), the core of Nutanix architecture, pools and tethers high-performance, solid-state storage to virtual machines while delivering the large capacity that the high capacity HDD tier provides through its adaptive data tiering capabilities. (You can learn more at www.nutanix.com or follow us on Twitter @nutanix.)

About Veeam

Veeam recognizes the new challenges companies across the globe face in enabling the Always-On Business™, a business that must operate 24/7/365. To address this, Veeam has pioneered a new market of Availability for the Modern Data Center™ by helping organizations meet recovery time and point objectives (RTPO™) of less than 15 minutes for all applications and data, through a fundamentally new kind of solution that delivers high-speed recovery, data loss avoidance, verified protection, leveraged data and complete visibility. Veeam Availability Suite™, which includes Veeam Backup & Replication™, leverages virtualization, storage, and cloud technologies that enable the modern data center to help organizations save time, mitigate risks, and dramatically reduce capital and operational costs.

Founded in 2006, Veeam currently has 29,000 ProPartners and more than 135,000 customers worldwide. Veeam’s global headquarters are located in Baar, Switzerland, and the company has offices throughout the world. To learn more, visit http://www.veeam.com.

Product Versions

The solution and testing provided in this document was completed with Veeam Backup & Replication v8 Patch 1 on Windows Server 2012 R2, deployed on VMware vSphere 5.5 on the Nutanix Virtual Computing Platform.
2 Introduction

2.1 Audience

This best practices document is part of the Nutanix Solutions Library and is intended for use by individuals responsible for the architecture, design, management, and support of Veeam Backup & Replication on Nutanix systems. Consumers of this document should be familiar with concepts pertaining to VMware vSphere, Veeam Backup & Replication v8, and Nutanix.

2.2 Purpose

This document covers the high level best practices for Veeam Backup & Replication v8 and Nutanix using NFS datastores with VMware vSphere 5.x. This best practices guide is focused on an optimized disk-to-disk backup architecture. A best practices checklist is included in this document to help ensure you implement all of the applicable best practices.

2.3 Synergistic Technologies

The web-scale Nutanix solution and its data locality technology are strongly complimented by the distributed and scale-out architecture of Veeam Backup & Replication v8. The combined solution leverages the strengths of both products to provide crash, OS, or even application consistent network-efficient backups, helping organizations achieve their recovery point objective (RPO) and recovery time objective (RTO) requirements. The architecture is flexible enough to enable the use of either 100% virtualized Veeam components or a combination of virtual and physical components, depending on customer requirements and available hardware.
3 Architecture

Performing backups in a VMware environment requires the interaction of several components, including the usage of VADP (VMware vStorage APIs for Data Protection). The Nutanix solution can leverage the Veeam scale-out proxy architecture by using multiple virtual Veeam proxies or one or more physical proxies. Physical proxies would offload the CPU workload from the Nutanix cluster. All of the components involved in the backup process are described in the following sections.

3.1 Component Overview

Tables 1 and 2 highlight the different components and virtualization/guest OS related technologies for the joint solution.

Table 1: Backup Components

<table>
<thead>
<tr>
<th>Backup Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nutanix Controller VM</td>
<td>The CVM is what runs the Nutanix Distributed File Server and serves all of the I/O operations for the hypervisor and all VMs running on that host. The CVM pools and exports storage to the hypervisor as a NFS datastore.</td>
</tr>
<tr>
<td>Veeam Backup Server</td>
<td>As the “brain” of the solution, Veeam Backup Server is responsible for job management and scheduling, indexing tasks, and general orchestration of the backup and replication environment. The Backup Server can be virtualized to leverage the full capabilities of the vSphere and Nutanix systems.</td>
</tr>
<tr>
<td>Veeam Backup Proxy</td>
<td>A backup proxy is a lightweight Veeam architecture component that sits between the data source and target and is used to process jobs and deliver backup traffic. In particular, backup proxy tasks include retrieving VM data from the production storage, compressing, deduplicating, and sending it to the backup repository. The use of more than one virtualized backup proxy lets you easily scale your backup infrastructure up based on the size of your Nutanix system. For large environments, multiple physical proxy servers may be required.</td>
</tr>
<tr>
<td>Veeam Repository</td>
<td>These systems provide the “memory”, storing backup archives for future restores and important metadata used during backup and replication. A repository may be a Windows or Linux server, or a third-party NAS device. Repositories can be either virtual or physical, depending on requirements and available hardware. If the repository is virtual, then it should not be stored in the same Nutanix cluster as production data to provide fault domain isolation.</td>
</tr>
</tbody>
</table>
Table 2: Backup Technologies

<table>
<thead>
<tr>
<th>Technology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware VADP</td>
<td>VMware vStorage APIs for Data Protection (VADP) was introduced with vSphere 4.0 and is available in all licensed editions. It is the next-generation backup framework that enables agent-free backups in an efficient manner. Veeam Backup &amp; Replication v8 uses the VADP framework for high performance backups.</td>
</tr>
<tr>
<td>VMware CBT</td>
<td>Changed Block Tracking (CBT) is a component of VADP that enables efficient incremental virtual machine backups. It enables Veeam Backup &amp; Replication to only backup changed data blocks, thus greatly increasing backup performance and reducing network bandwidth. Read operations are performed locally, eliminating the load on the network and other Nutanix nodes.</td>
</tr>
<tr>
<td>Microsoft VSS</td>
<td>Microsoft VSS is the built-in Microsoft framework for application-consistent backups. Built into Windows, VSS enables the creation of a consistent snapshot of application data, such as Microsoft Exchange, SQL, Active Directory, or the NTFS file system. Veeam can leverage VSS to ensure application-consistent backups for VSS-aware applications.</td>
</tr>
</tbody>
</table>

3.2 Veeam Component Sizing

Sizing the Veeam Backup & Replication servers is dependent on the number of concurrent jobs, total number of VMs, and the estimated size of the repository. The sizing guidelines in Table 3 are the minimums recommended by Veeam. The virtual Veeam Proxy servers should not need additional resources as the scale-out model based on the total number of VMs is recommended.

A general rule of thumb for a physical proxy is 1 core per 50 VMs. But this number is greatly dependent on the size of VMs and number of concurrent backups. Proper testing for your environment is critical to ensure backup windows and RPO values can be met. The Veeam Backup & Repository server may need to be upsized for your environment. (Refer to the Veeam Backup & Replication v8 documentation for additional details on sizing.)

Table 3: Veeam Sizing Recommendations

<table>
<thead>
<tr>
<th>Component</th>
<th>Sizing Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veeam Backup Proxy</td>
<td>Sizing should be tested in the customer environment to verify the backup window and RPO values can be met. ( V_{\text{Virtual}}: ) 1 vCPU per every 50 VMs (recommended minimum 2 vCPUs) 4GB RAM, 300MB disk space for installed components, and VMXNET3 NIC. No CPU/memory reservations are required. ( V_{\text{Physical}}: ) 1 CPU core for every 250 VMs. 2GB of RAM for each concurrent VMDK backup.</td>
</tr>
</tbody>
</table>
### Veeam Backup Server

4GB of RAM plus 500MB of RAM for each concurrent job. Disk space: 2GB for product, plus 10GB per 100 VMs for guest file system catalog, and at least 10GB for VM recovery cache folder. No CPU/memory reservations are required. Additional sizing considerations should be applied if the backend SQL server is deployed on this server. (See the Veeam documentation for additional guidance.)

### Veeam Repository

The Veeam Repository can be co-located with the backup server role for small deployments, or on a dedicated server (physical or virtual Windows/Linux server, NAS device, or dedicated backup appliance), and requires sufficient free space to store all backup job data. If a virtual machine is used, it is recommended to use the VMware PVSCSI controller for the disk(s) which will be storing backup data. The use of vSphere 5.5 enables disks larger than 2TB to be used, which may be advantageous for a repository server. If virtualized on Nutanix, the repository should reside in a secondary Nutanix cluster.

#### 3.3 Deployment Models

As shown in Figure 1, Veeam supports the repository server using a variety of targets, including a secondary Nutanix cluster, existing physical servers, NAS, or dedicated backup appliances. The following two sections provide guidance for two of the scenarios: 1) 100% virtualized solution on Nutanix; and 2) Using a physical backup/proxy server. A hybrid scenario is also viable where there is a physical Veeam repository server (when tape vaulting is required, for example), but virtualized proxy and management VMs are used. This can be a good approach if physical hardware is limited, as performance can be easily determined. The defined backup window may be a big factor in determining how much, if any, of the Veeam infrastructure to virtualize.

In all cases, Veeam and Nutanix recommend using the “network” backup mode and not virtual appliance mode. This enables large-scale environments to perform reliable backups. Network mode works by connecting to the ESXi management VMKernel port and transferring backup data to the proxy. For the best performance, this should be done using the Nutanix dual 10Gb NIC interfaces. If the ESXi management interfaces are using the 1Gb NICs, then the backup speed will be limited to 30-40MB/s per ESXi host, which is far from...
ideal. The network performance is not dependent on the VMware switch type, but rather the NIC speed that management traffic is using.

### 3.3.1 Virtualized Veeam on Nutanix

Figure 2 shows a 100% virtualized solution for Veeam Backup & Replication on Nutanix. One or more Nutanix nodes has a lightweight Windows Veeam Proxy VM. All VM data is read via “network” mode over the 10Gb NICs via VADP. It leverages CBT to reduce read operations to only new blocks of data. The compressed and deduplicated data is then sent over the network to the Veeam Repository server located on a secondary Nutanix system (partial shown).

![Figure 2 Virtualized Veeam Deployment Model](image)

If a 100% virtualized solution on Nutanix is deployed, then placing the Veeam repository server in a secondary Nutanix cluster is recommended. This provides maximum protection from a complete production cluster failure and allows scaling out the backup repository independent of the production VMs. Nutanix is the ideal solution if your organization has multiple remote locations that need to be replicated to a centralized repository.

### 3.3.2 Veeam Server

As an alternative to deploying a virtualized Veeam repository, Figure 3 shows a notional topology for a physical Veeam configuration. In this example, all Veeam roles (backup, proxy, and repository) are co-located on a single server. This topology can be used when tape backup is required because that requires a physical server to hold the dedicated "Tape server" role. Additional hybrid deployments are possible where just the repository and tape roles are deployed on physical nodes, while the Veeam server and proxies are virtual machines.

As stated previously, each Nutanix node should have the ESXi management interface configured to use the 10Gb NICs. This enables optimal backup performance compared to using the 1Gb NICs. The physical Veeam server should also have dual 10Gb NICs and be connected to the same layer two network as the ESXi management network. The physical server should meet the minimum Veeam sizing requirements, based on the number of VMs you are backing up and concurrent jobs. In larger environments, multiple Veeam physical machines may be required to meet backup window or storage capacity requirements.
3.4 Veeam Restore Options

The joint Nutanix and Veeam Backup & Replication solution offers a variety of options to easily recover and verify your backups and replicas. These features are implemented using Veeam vPower technology.

The Veeam vPower NFS service is a Windows service that runs on a Windows-based 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 VMware VM images. The vPower technology is used to perform the following tasks:

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

Nutanix and Veeam Backup & Replication enables you to perform both image-level and file-level restores of backups and replicas. You can restore a virtual machine as a whole to start it on the target ESX server, recover only VM hard disks, VM files (.vmdk .vmx and so on), or VM guest OS files and folders and save them on your local machine. VMs or files can be restored at any of the available restore points. All restores are performed via the network and no special procedures are required to restore your data on the Nutanix platform.
4 Best Practice Checklist

The Veeam Backup & Replication v8 on Nutanix best practices can be summarized into the following items:

**General**
- When deploying Veeam Backup & Replication servers, use the latest supported Windows operating system for your environment. Nutanix and Veeam recommend using Windows Server 2012 R2, but this is not required.
- Configure the ESXi management interface on the Nutanix nodes to use the 10Gb NICs, not the 1Gb NICs. The 1Gb NICs could be configured as standby to provide management resilience. The following figure shows two active 10Gb NICs and two standby 1Gb NICs for the ESXi management interface. This is not a required configuration and only an example of one of the many possibilities.

<table>
<thead>
<tr>
<th>Name</th>
<th>Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmnic2</td>
<td>10000 Full</td>
</tr>
<tr>
<td>vmnic3</td>
<td>10000 Full</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmnic0</td>
<td>1000 Full</td>
</tr>
<tr>
<td>vmnic1</td>
<td>1000 Full</td>
</tr>
</tbody>
</table>

- If you have ESXi Enterprise Plus and are using the DVS, consider using load-based teaming for the 10Gb interfaces.
- If using a physical Veeam proxy, use dual 10Gb NICs and place the server on the same layer two network as the ESXi management interfaces.
- Start with a PoC, test, optimize, iterate, and scale.

**Veeam Components**
- Use Veeam Backup & Replication v8 patch 1 (build 8.0.0.971) or later.
- Prefer the new forever forward incremental backup method. In general, avoid active full backups.
- Use network mode for all Veeam proxies to enable the most reliable backups.
- Do not backup the Nutanix CVMs or any virtual Veeam servers.
- Configure the Veeam jobs to back up more than one VM to enable parallel processing and enhanced deduplication ratios.

**Nutanix Components**
- Upgrade clusters to 3.5.3.1 (or later) for optimized NFS and snapshot performance.
5 Configuration Details

This section provides specific instructions on how to configure Veeam Backup & Replication to follow best practices for a deployment on the Nutanix Virtual Computing Platform. A basic familiarity with Veeam and VMware is assumed. When deploying the Veeam servers, use the latest approved 64-bit Windows operating system for your environment. Nutanix and Veeam recommend using Windows Server 2012 R2, but this is not required.

5.1 Veeam Configuration Optimization

1. Install Veeam Backup & Replication v8 patch 1 (or later) on the backup server, version 8.0.0.971. (See Veeam KB1982 for more details.)

2. If you are using a virtualized repository server, use a second SCSI controller configured with the VMware PVSCSI controller. This can reduce CPU load on the ESXi host and optimizes disk performance.

3. If you are using a physical backup/proxy server, use dual 10Gb NICs and put the server on the same layer 2 network as the ESXi management interfaces. This optimizes the backup traffic and avoids potential bottlenecks created by routing.

5.2 Veeam Backup Proxy Configuration

1. If virtualizing the proxies, provision a new Windows Server VM with appropriate virtual hardware specifications, per section 3.2.

2. Launch Veeam Backup & Recovery and navigate to the Backup Infrastructure window. Right click on Backup Proxies and select Add VMware Backup Proxy.
3. Click on **Add New** and enter the DNS name of the first proxy. If not already configured, add a **Managed Account** which has local administrator rights on the Veeam backup proxy.

4. If a firewall is running on the Veeam Proxy host, verify that 137/UDP, 138/UDP and 139/TCP are open. If you are using the Windows firewall, enable the following three rules shown in green:

   - File and Printer Sharing (NB-Name-In)  File and Printer Sharing
   - Network Discovery (NB-Name-In)  Network Discovery
   - File and Printer Sharing (NB-Datagram-In)  File and Printer Sharing
   - Network Discovery (NB-Datagram-In)  Network Discovery
   - File and Printer Sharing (NB-Session-in)  File and Printer Sharing

5. Click through the rest of the wizard and wait for the proxy to be installed.

6. After the backup proxy is installed, change the Transport mode to **Network**. Leave the **Max concurrent tasks** at 2 if using a virtual proxy. This can be increased for physical proxy servers.

   ![Transport mode](image)

   - **Transport mode:** Network
   - **Connected datastores:** Automatic detection (recommended)
   - **Max concurrent tasks:** 2

7. Accept the defaults for the remainder of the wizard.

### 5.3 Veeam Backup Methods

Veeam and Nutanix recommend using the new forever forward incremental backup method. This is the new default method for newly created jobs in Veeam Backup & Replication v8 and can be selected also for existing jobs if upgrading from previous versions. In this scenario, a full backup is performed on day one, then incremental backups
are performed for all subsequent days. The day-one backup may have lower throughput, due to reading all of the VM data that may be in the storage tier, versus the performance SSD or RAM tiers. However, through the use of CBT, all subsequent backups will only read changed blocks. These changed blocks are likely on Nutanix performance tiers.

![Advanced Settings](image.png)

**Figure 4: Forever Forward Incremental Backup**

This backup method offers the ability to execute forever incremental backups on the production storage, thus lowering at a minimum the load on the Nutanix cluster. At the same time, it offers the best space utilization on backup repository, since only one full backup file is stored at any time. When reaching the desired retention period, the oldest incremental file is injected into the full backup file. This additional disk activity is created into the backup repository itself, while any vSphere snapshot has already been removed. In this way, no additional load is created on the production Nutanix cluster. Refer to the Veeam documentation on the other advanced settings for Backup & Replication v8 including the options for vSphere integration for consistency.

### 5.4 Veeam Job Configuration

When configuring your backup jobs, exclude the Nutanix CVMs and all Veeam Backup and proxy servers (when virtualized) from the schedule. These VMs do not need to be backed up; you only need to save Veeam Backup Configuration using a specific configuration option inside Veeam Backup Server which is enabled by default. Configure your jobs to backup multiple VMs so that parallel processing can be enabled increasing backup performance. Also, Veeam-native deduplication can be higher with an increased number of VMs inside the same job. There is no need to manually configure which proxy is used for VM backup operations. Veeam Backup Server will automatically distribute the VMs to be processed to all available proxies.
5.5 Nutanix Configuration

No special Nutanix configuration is required, however upgrading the cluster(s) to 3.5.3.1 (or later) is recommended. NFS optimizations were incorporated into this release that increase snapshot performance and reliability.
6 Conclusion

The Nutanix and Veeam Backup & Replication v8 solution provides the best of many worlds: industry-leading performance with the ability to scale out your backup solution as you grow your Nutanix solution. Of the converged architectures in the market today, only Nutanix can truly provide the optimal configuration for all workloads and allow scale-out backup performance.

As part of its determination to always deliver the best possible solutions, Nutanix will continue to research into the following areas:

- Benchmarks
- Performance Optimizations
- Scale Testing
7 References

Table of Figures

Figure 1 Veeam Backup & Replication Repository Options .......................................................... 8
Figure 2 Virtualized Veeam Deployment Model............................................................................. 9
Figure 3 Veeam Server Topology ................................................................................................... 10
Figure 4: Forever Forward Incremental Backup .............................................................................. 14

Table of Tables

Table 1: Backup Components ........................................................................................................... 6
Table 2: Backup Technologies .......................................................................................................... 7
Table 3: Veeam Sizing Recommendations ......................................................................................... 7
8 About the Authors

**Derek Seaman** is a senior solutions and performance engineer at Nutanix, Inc., VMware Certified Design Expert (VCDX) #125, and a multi-year VMware vExpert. In this role, Derek helps design architectures combining applications with the Nutanix platform, creating solutions that help solve critical business needs and requirements while disrupting the infrastructure space.

Prior to joining Nutanix, Derek was an IT architect at the global leader in wireless chip technology, where he was focused on deploying secure infrastructure solutions to support the development of solutions for the U.S. Government. In these spaces, he has developed methodologies, reference architectures, and frameworks focusing on the design and transformation to agile, scalable, and cost-effective infrastructures which can be consumed in a service-oriented or cloud-like manner.

Follow Derek on Twitter at @vDerekS

**Luca Dell’Oca** is an EMEA evangelist at Veeam Software. Based in Italy, Luca is a popular blogger and an active member of the virtualization community. At Veeam, Luca creates and publishes valuable information about the latest technologies and business trends in virtualization, with a deep focus on VMware, storage, and data protection for service providers and large enterprises. He engages customers and peers during webinars and public events to help them learn about modern data protection, and how Veeam solutions can help them.

Luca's career started in information security before focusing on virtualization. Prior to joining Veeam, Luca was a data protection manager and virtualization architect at a service provider, where he refined his skills and knowledge about always-on business and the requirements of such demanding environments, while helping customers to embrace the “cloud revolution”.

Luca holds VCAP5-DCD and CISSP certifications, and he has become the first worldwide VMCE (Veeam Certified Engineer).

Follow Luca on Twitter at @Dellock6
@nutanix