



Backup as a Service and Disaster Recovery to the Cloud

Cornel Popescu
Veeam Systems Engineer, South East Europe



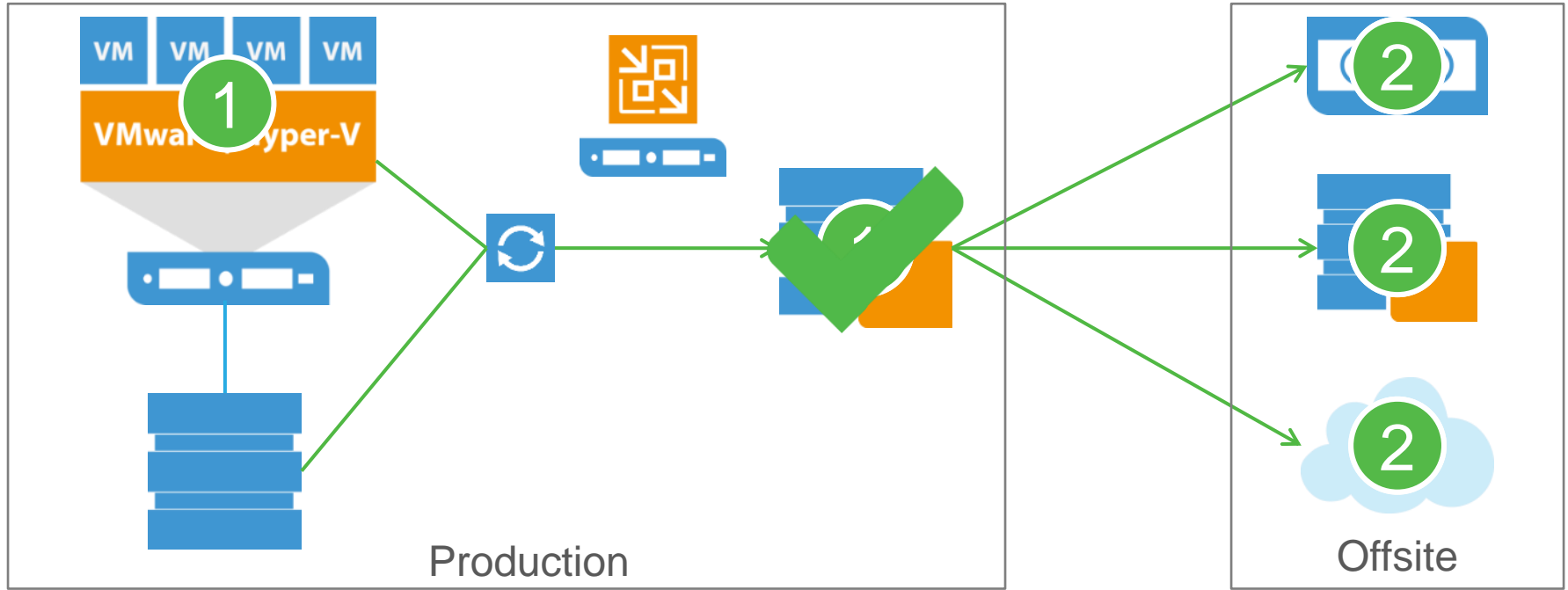
IBS IT Compass
Sofia, November 28th 2017



Agenda

- Data Protection Strategy – the 3-2-1 Rule
- Why to use Cloud for Availability
- How to use Cloud Resources with Veeam
- Backup using Cloud Resources
- Disaster Recovery using Cloud Resources

3-2-1-0 Data Protection Strategy



3

Copies of the data

2

Separate media

1

Offsite

0

Errors

Why to use Cloud resources
for Data Protection?

Top 3 reasons - why to use cloud resources for availability?

1. Cost and usage - Cloud has a different cost model, usually is pay-per-usage, no investment needed, usage on demand
2. Management - Easier to manage, you don't need to build and manage, easier to consume
3. Availability – Cloud can easily solve the problem of the offsite location, 3-2-1 becomes easy to implement

Concerns and fears of Cloud

Top 3 concerns and fears of using Cloud

1. Security – is it secure?
2. Security – is it safe?
3. Security – did I mention security?
4. Data localization – Data might be regulated by law or company policies, to be kept in a specific location
5. Management – Cloud needs to provide users with the tools to control and manage data. User should decide policies.

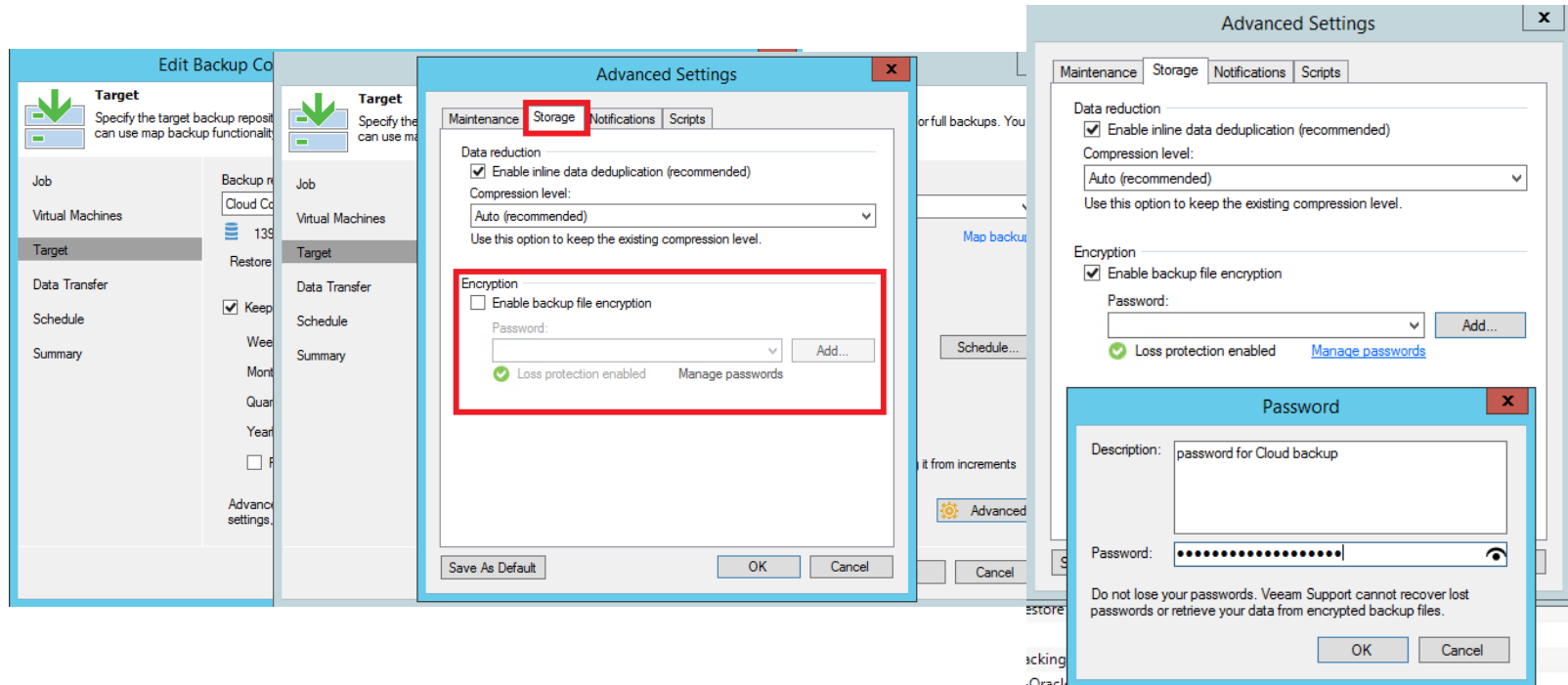
Security in Veeam Availability Suite

– Data at Rest

- Veeam has built-in AES 256-bit encryption, giving you the ability to encrypt backup files
- Veeam backup file is encrypted by a randomly generated encryption key.
- Each backup encryption key has two passwords. A backup job password created by the admin and a public key automatically generated behind the scenes by the Veeam Enterprise Manager and pushed out to all backup servers.
- If someone forgets the backup job password, using a challenge/response system in Enterprise Manager you can still access your data without sacrificing security.
- More info - https://helpcenter.veeam.com/backup/vsphere/data_encryption.html

Security in Veeam Availability Suite

– Data at Rest



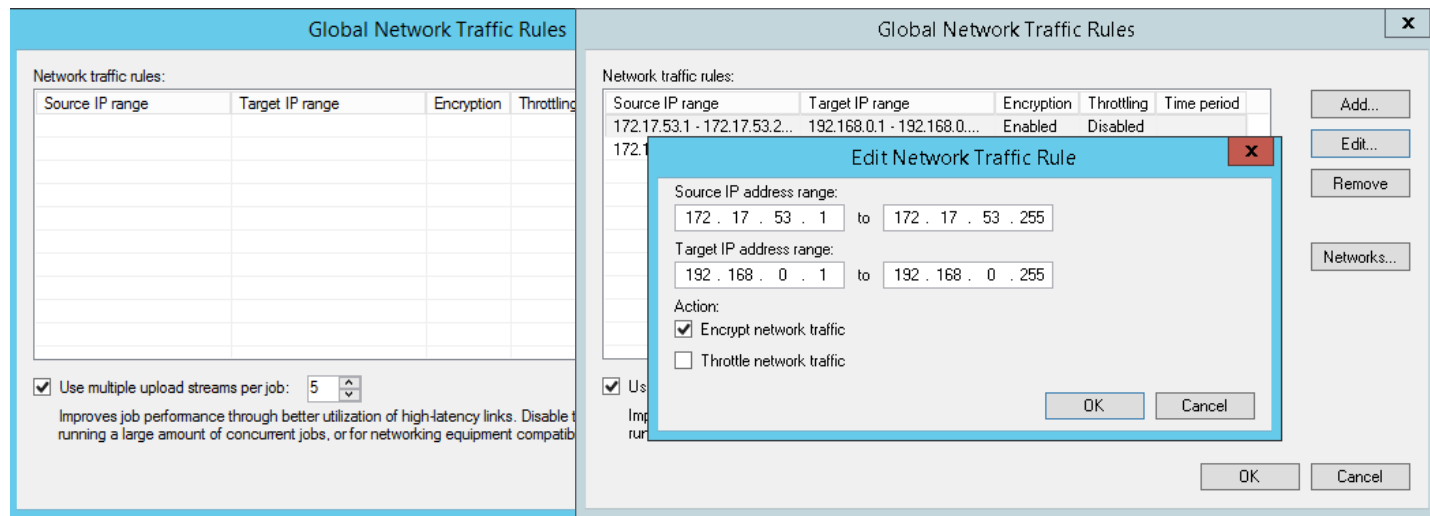
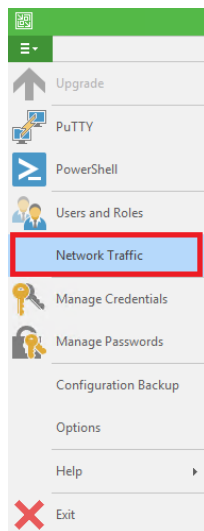
Security in Veeam Availability Suite

– Data in Transit

- You can enable network traffic encryption for data going between the source side and target side.
- If encrypted data is intercepted in the middle of data transfer, the eavesdropper will not be able to decrypt it and get access to it.
- Veeam Backup & Replication encrypts the network traffic with 256-bit Advanced Encryption Standard (AES)
- **Data transferred between public networks is encrypted by default**

Security in Veeam Availability Suite

– Data in transit



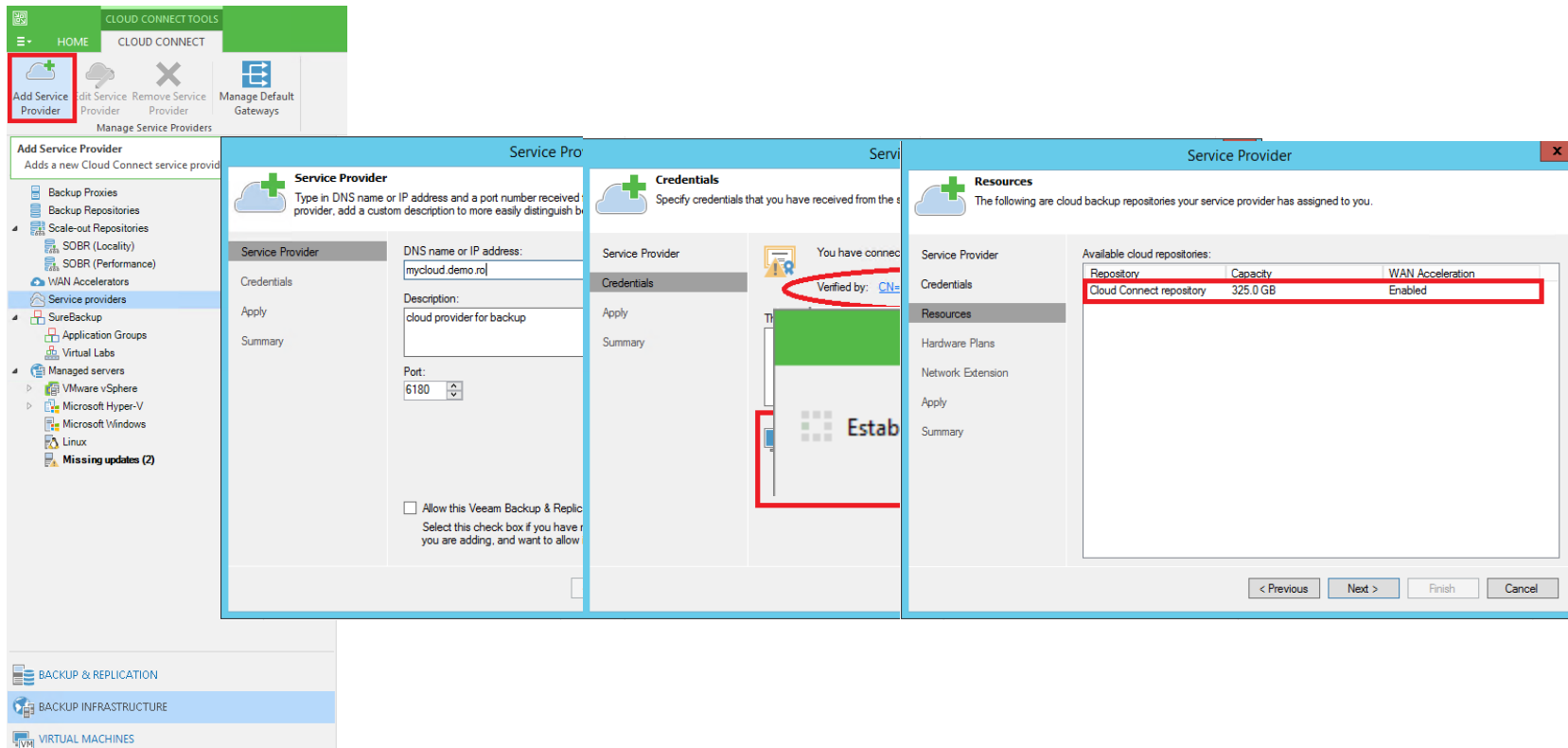
Backup in Cloud

Backup in Cloud

How to implement with Veeam B&R

1. Subscribe to a cloud backup provider
2. Add Cloud Provider Backup Repository
3. Configure connection traffic and security settings
4. Define Backup Copy Jobs
5. Configure security for Backup Copy Jobs

Backup in Cloud – adding Cloud SP



The screenshot displays the Veeam Backup & Replication console interface. The top navigation bar includes 'HOME' and 'CLOUD CONNECT' tabs. The 'Add Service Provider' button is highlighted with a red box. The main window shows the 'Add Service Provider' wizard with three tabs: 'Service Provider', 'Credentials', and 'Resources'.


Service Provider Tab:

- Service Provider:** DNS name or IP address: mycloud.demo.ro | Description: cloud provider for backup | Port: 6180
- Credentials:** Service Provider: mycloud.demo.ro | Credentials: Verified by: CN= | Summary: Estab
- Resources:** Available cloud repositories table:


Repository	Capacity	WAN Acceleration
Cloud Connect repository	325.0 GB	Enabled

The 'Cloud Connect repository' row is highlighted with a red box. The bottom of the wizard shows navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'.


Backup in Cloud – Backup Copy

**Job**


Backup copy data. Type in

**Target**

Specify the target location where the backup can map to

**Data Transfer**

Choose how VM data is transferred

**Schedule**

Specify when this job is allowed to transfer data over the network. Backup copy jobs run continuously, starting data transfers according to copy interval and/or as the new VM restore points appear.

Job

Virtual Machines

Target

Data Transfer

Schedule

Summary

Job

Virtual Machines

Target

Data Transfer

Schedule

Summary

Job

Virtual Machines

Target

Data Transfer

Schedule

Summary

Job

Virtual Machines

Target

Data Transfer

Schedule

Summary

This job can transfer data:

☐ Any time (continuously)

☒ During the following time periods only:

12 • 2 • 4 • 6 • 8 • 10 • 12 • 2 • 4 • 6 • 8 • 10 • 12

All	12	2	4	6	8	10	12	2	4	6	8	10	12
Sunday													
Monday													
Tuesday													
Wednesday													
Thursday													
Friday													
Saturday													

☐ Enable
☒ Disable

Sunday through Friday from 10:00 AM to 6:59 PM

< Previous

Next >

Finish

Cancel

Backup in Cloud – Restore

The screenshot displays the Veeam Backup & Replication interface. On the left, the 'HOME' tab is active, and the 'Cloud' option under 'Backups' is highlighted with a red box. The main window shows the 'Restore Points' dialog for a VMware backup job. The 'Available restore points for demo-AD:' section lists several backup jobs, with the 'VMware - Backup Copy to Cloud Connect' job selected and its restore points highlighted by a red box. The restore points are as follows:

Job	Type	Media set
VMware - Backup Copy to ExaGrid		
VMware - Backup Copy to DataDomain		
VMware - Backup to Exagrid		
VMware - Backup Copy to StoreOnce		
VMware - Backup Copy to Cloud Connect		
1 day ago (9:49 AM Wednesday 9/21/2016)	Increment	
2 days ago (11:01 PM Monday 9/19/2016)	Increment	
3 days ago (11:02 PM Sunday 9/18/2016)	Increment	
4 days ago (11:02 PM Saturday 9/17/2016)	Increment	
5 days ago (11:02 PM Friday 9/16/2016)	Increment	
6 days ago (11:02 PM Thursday 9/15/2016)	Increment	
7 days ago (11:03 PM Wednesday 9/14/2016)	Full	
VMware - Veeam Explorers		
VMware - Backup to DataDomain		
VMware - Backup from 3PAR Snapshot		
VMware - Backup Copy to Cloud Connect with WA...		
Pakistan VClub Test		

The 'OK' and 'Cancel' buttons are visible at the bottom right of the dialog.

Backup in Cloud – Things to remember

1. You can use cloud backup repository to perform recovery to on-prem
2. You can set retention policy on Backup Copy Job options for data archival (not on cloud repository itself)
3. The feature of using cloud repository is included in all Veeam B&R editions; it needs a subscription from a service provider for consumed cloud resources

Disaster Recovery in Cloud

Disaster Recovery (DR) in Cloud

How to implement with Veeam Availability Suite

1. Subscribe to a cloud provider
2. Add Cloud Provider Replication Resources
3. Configure connection traffic and security settings
4. Define Replication Jobs
5. Configure security for Replication to Cloud Jobs

Veeam Cloud Connect

Multi-tenant

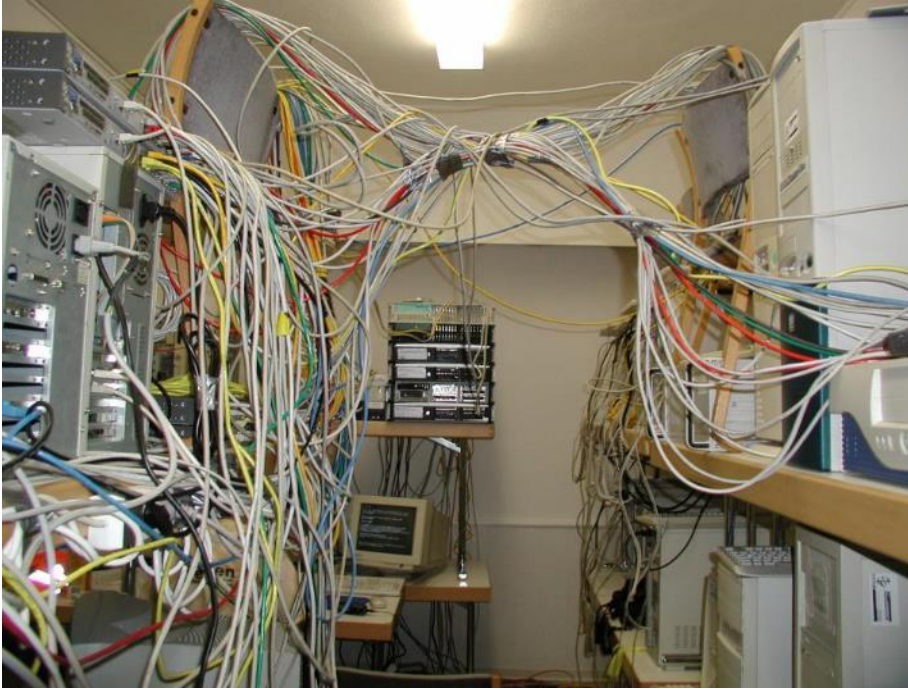
Single port

SSL/TLS (no VPN required)

Transparent networking



Traditional DR is complex

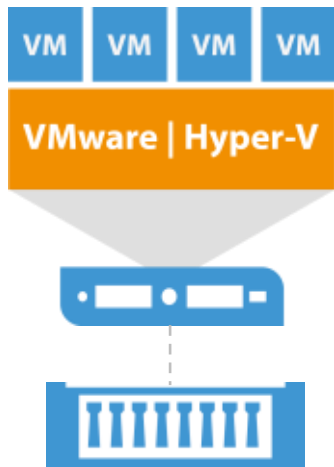


Networking

- Need to reconfigure routing
- Complex VPNs
- Custom rules
- Network overlaps
- Other...

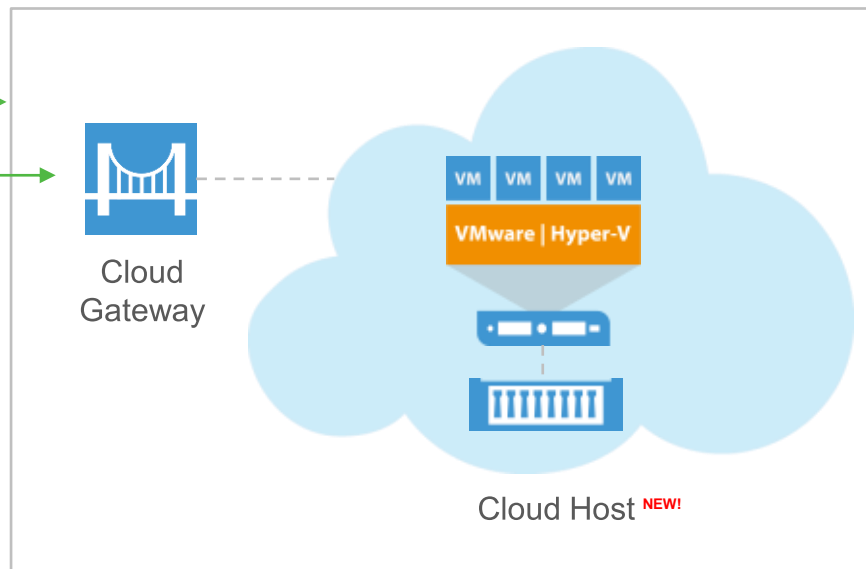
Overview – how it works

Customer On-Premises
Infrastructure



Production Host

Service Provider
Infrastructure



SSL/TLS

VM Replication **NEW!**

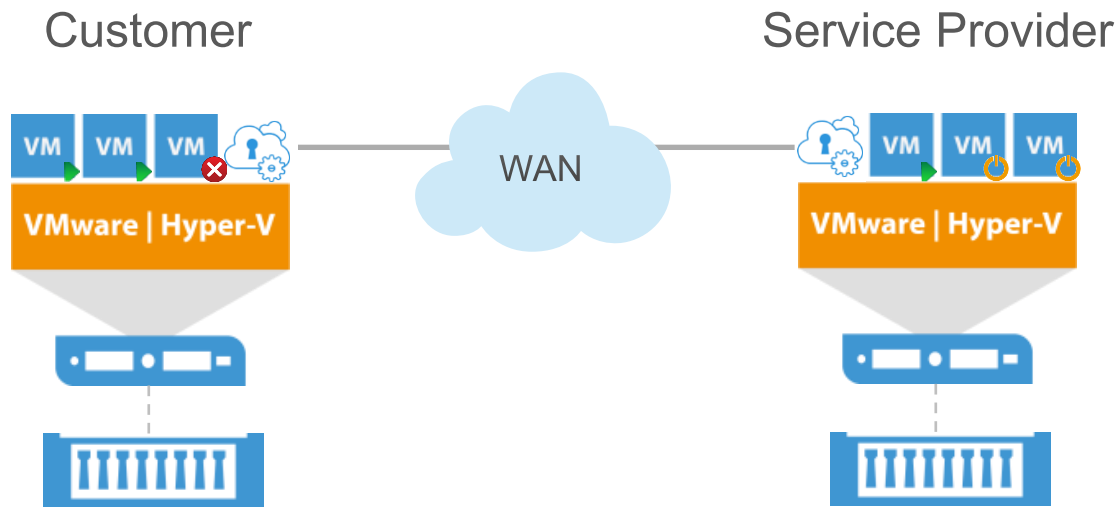


WAN Acceleration
(optional)

Cloud
Gateway

Cloud Host **NEW!**

Network extension appliance



DR in Cloud – adding Cloud SP

Service Provider

Type in DNS name or IP address and a port number received from the provider, add a custom description to more easily distinguish between providers.

Service Provider

DNS name or IP address: mycloud.demo.ro

Description: cloud provider for backup

Port: 6180

☐ Allow this Veeam Backup & Replication to connect to the provider. Select this check box if you have a provider you are adding, and want to allow Veeam Backup & Replication to connect to the provider.

Network Extension

Configure network extension appliances to enable partial site failover functionality.

Network extension appliances:

Name	Host	Production network	IP address
cloudconnect2.de...	esx3.democe...	dpg-vmnetwork-17	172.21...

Network extension appliances will be used during partial site failover to preserve network communication with failed over VMs. You must add one network extension appliance per production IP network.

< Previous Next > Finish Cancel

DR in Cloud - Replication

Edit Replication Job [VMware - Replication to Cloud Connect]

Name Specify the name of the replication job.	Destination Specify where the VM data should be replicated to.	Data Transfer Choose how VM data should be transferred to the target site.
Name	Name	Name
Virtual Machines	Virtual Machines	Virtual Machines
Destination	Destination	Destination
Job Settings	Job Settings	Job Settings
Data Transfer	Data Transfer	Data Transfer
Guest Processing	Guest Processing	Guest Processing
Schedule	Schedule	Schedule
Summary	Summary	Summary

When replicating between remote sites, we highly recommended that you deploy at least one backup proxy server locally in both sites to allow for direct access to storage.

Source proxy:

Target proxy:

☐ **Direct**
Best for local and off-site replication over fast links.

☒ **Through built-in WAN accelerators**
Best for off-site replication over slow links due to significant bandwidth savings.

Source WAN accelerator:

Target WAN accelerator:

< Previous Next > Finish Cancel

DR in Cloud – Recovery Failover

The screenshot displays the VMware vSphere interface with the 'Edit Cloud Failover Plan' dialog open. The dialog is titled 'Edit Cloud Failover Plan Failover everything to Cloud Connect Replica'. It features a sidebar on the left with a tree view containing 'Jobs', 'Backups', 'Replicas', and 'Running (5)'. The 'Replicas' section is highlighted with a red box. The main area of the dialog is divided into four tabs: 'Failover Plan', 'Virtual Machines', 'Default Gateways', and 'Public IP Addresses'. The 'Public IP Addresses' tab is selected, showing a table with columns for 'Failover Plan', 'Type in a', 'Add met', 'Spec site', and 'Assign public IP address a VM from the internet'. A red box highlights the 'Public IP Address Mapping Rule' sub-dialog, which is open over the 'Public IP Addresses' tab. This sub-dialog contains fields for 'Replica VM:' (set to 'demo-AD'), 'Public IP address:', 'Port:', 'Internal IP address of replica VM:', and 'Port:'. The 'Public IP address:' and 'Port:' fields are highlighted with a red box. The 'Internal IP address of replica VM:' and 'Port:' fields are also highlighted with a red box. The 'Description:' field is empty. The 'OK' and 'Cancel' buttons are at the bottom right of the sub-dialog. The 'Previous', 'Next', 'Finish', and 'Cancel' buttons are at the bottom of the main dialog.

ORIGINAL LOCATION

- cloudconnect2.democenter.int/Small Hardware Plan
- vc5a.democenter.int/demo-cluster
- hv7.democenter.int
- cloudconnect2.democenter.int/Hyper-V Small Hardw...

DR in Cloud – Execute Failover Plan

The screenshot shows the Veeam Backup & Replication console. The left sidebar displays the 'Failover Plans' section under 'Jobs'. The main area shows a list of failover plans. A context menu is open for the 'Hyper-V - Failover everything to Cloud Connect Replica' plan, showing options like 'Restore', 'Import', and 'Failover Plan'. A tooltip for 'Add Cloud Failover Plan' is also visible.

Failover Plans Table:

NAME	PLATFORM	STATUS	NUMBER OF VMS
Failover everything to Cloud Connect	VMware	Ready	2
Failover Exchange to Cloud Connect	Hyper-V	Ready	1
Failover Exchange to DR Replica			
Hyper-V - Failover everything to Cloud Connect Replica	Hyper-V	Ready	1

Disaster Recovery in Cloud – Things to remember

1. You can use cloud replicas to recover data
2. You can Failover and Failback to Cloud
3. While you are in Failover (partial or full failover) state, the workload is running in the Cloud
4. Veeam allows full and partial failover, without complex network settings
5. For failover purposes, public IPs and DNS should be planned

Questions?

Thank you!

veeam