Customer Documentation

Dynamic Services for Infrastructure with vCloud (DSI vCloud)

Version: 3.9, valid from March 2020

Imprint

Publisher

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main

WEEE-Reg.-Nr. DE50335567

Hereinafter referred as – Telekom –

https://www.t-systems.com/de/en/compulsory-statement

1. TABLE OF CONTENTS

2. LIST OF FIGURES

3. LIST OF TABLES

4. INTRODUCTION

DSI vCloud is based on the standard VMware functionality. Comprehensive technical trainings, manuals, administrator guides, tutorials and further detailed information is provided by VMware and is publicly available: https://docs.vmware.com/en/vCloud-Director/index.html

Contractually relevant information in regard to DSI vCloud is solely included in the service specifications and further contract documents but is not part of this manual. This document shall provide the customer additional information in regard to Telekom specific configurations, circumstances, restrictions and options as well as answer to the most frequently asked questions when using the DSI vCloud service.

It is assumed that the reader of this document has deep technical knowledge of the usage of VMware's vCloud, of virtualization and network technology and of the usage and administration of Windows Server, SuSE and RedHat Linux operating systems.

Important general note: In case Backup as a Service is used to backup and restore virtual machines, it is recommended to respect the special characters disallowed by Veritas NetBackup. VM names should not include those characters:
https://www.veritas.com/content/support/en_US/doc/21902280-127283730-0/v50329751-127283730

5. QUICK GUIDANCE ON SPECIFIC CUSTOMER DUTIES

Please regularly review the contractual customer duties to cooperate which are defined in the terms and conditions document, the service specification or your contract in order to get an exhaustive overview. Independent from that, please find key takeaways for the day to day use of DSI vCoud in the following list:

- User management – Please be aware that you are responsible for the management of the users whom are granted access to the self-service portals and your virtual machines. Please ensure to evaluate carefully to whom access is granted, apply strong password policies and review access control lists regularly.
- Default passwords – In this document you'll find information about initial login credentials created during the deployment process of virtual machines. Please change the initial password as soon as possible after the VM is deployed in order to minimize potential security risks.
- Backups – Even if there is an exception when using BIS (Backup Integrated Storage), in general your data and virtual machines are not backed up and cannot be restored in the self-service portal by default. Please ensure that you configure appropriate backups using the BaaS (Backup as a Service) portal. It is also recommended that you review the BaaS (Backup as a Service) portal regularly to ensure that all the machines that require backups are appropriately protected.
- Disaster Recovery – Even though the Telekom twin core data center solution enables you to setup disaster recovery solutions, your DSI vCloud environment is not disaster recovery ready. If desired, please implement an appropriate disaster recovery solution incl. your application layer.
- Firewall and other network configuration – Please be aware that you are responsible for management of the firewall rules and other network relevant configuration on the Edge Service Gateway for your virtual organization. Please ensure to implement strict and secure rule sets and settings to minimize security risks.
- Patch management – Even though Telekom provides distribution of software patches via central software distribution server, the patches must be installed via self-service. Please ensure that your

operating systems and application software are always up to date and use the flexibility provided to determine when your organisation can best tolerate any down time from patch installation.

- Capacity Management – Please be aware that even though Telekom is managing the overall capacity of the IaaS platform this does not include capacity management of any quotas that are set against your virtual organization or virtual data center. Please set up appropriate capacity management processed processes in order to minimize the operational risk of disruption if your current quotas are over-subscribed.
- Commissioned data processing – Please verify if you process personal data of any kind within DSI vCloud. If so, please sign a commissioned data processing agreement and send it over to Telekom.
- In case you are using self-managed operating systems based on Telekom licenses, you have to ensure 3rd party support and maintenance for Microsoft operating systems by your own. You are not able to directly contact Microsoft for support reasons, as no support contract is included in those licenses.

6. SELF-SERVICE PORTAL

Note: The following information are needed for the DSI vCloud Private platforms only. There is no need to change anything in order to access the portal of DSI vCloud Hybrid.

DSI vCloud Private portal VIP (Virtual IP address) pools

As the portal of DSI vCloud Private is reachable via private address ranges only, the following VIPs (Virtual IP addresses) and SNAT ranges are used.

Data Centre Location Frankfurt am Main	
The Virtual IP address of the vCloud Portal & API	217.150.159.1
The Virtual IP address of the vCloud Console	217.150.159.2
The Virtual IP address of the BaaS Portal	217.150.159.3
The Virtual IP address of the vCloud Availability Public API Service	217.150.159.7

Table 1 Overview of VIPs FFM

Data Centre Location Houston	
The Virtual IP address of the vCloud Portal & API	217.150.159.8
The Virtual IP address of the vCloud Console	217.150.159.9
The Virtual IP address of the BaaS Portal	217.150.159.10
The Virtual IP address of the vCloud Availability Public API Service	217.150.159.14

Table 2 Overview of VIPs HOU

Data Centre Location Singapore	
The Virtual IP address of the vCloud Portal & API	217.150.159.16
The Virtual IP address of the vCloud Console	217.150.159.17
The Virtual IP address of the BaaS Portal	217.150.159.18

The Virtual IP address of the vCloud Availability Public API Service	217.150.159.22

Table 3 Overview of VIPs SIN

DSI vCloud Private portal Links for Frankfurt am Main:

vCloud (vCloud Director) Portal

- Link (URL): https://vcloud-ffm-private.t-systems.de/cloud/org/[customer vOrg]/
- Link (IP): https://217.150.159.1/cloud/org/[customer vOrg]/

BaaS Portal

- Link (URL): https://baas-ffm-private.t-systems.de
- Link (IP): https://217.150.159.3

DSI vCloud Private portal Links for Houston:

vCloud (vCloud Director) Portal

- Link (URL): https://vcloud-hou-private.t-systems.com/cloud/org/[customer vOrg]/
- Link (IP): https://217.150.159.8/cloud/org/[customer vOrg]/

BaaS Portal

- Link (URL): https://baas-hou-private.t-systems.com
- Link (IP): https://217.150.159.10

DSI vCloud Private portal Links for Singapore:

vCloud (vCloud Director) Portal

- Link (URL): https://vcloud-sin-private.t-systems.com/cloud/org/[customer vOrg]/
- Link (IP): https://217.150.159.16/cloud/org/[customer vOrg]/

BaaS Portal

- Link (URL): https://baas-sin-private.t-systems.com
- Link (IP): https://217.150.159.18

Important note: The customer specific information like the individual URLs and users are shared within the welcome e-mail. For the communication via the URL, the customer has to create a local DNS entry within his customer DNS. As an

alternative, the customer can create entries in the local host file: (These URLs should also be added to the Trusted Zone when using the Internet Explorer)

Frankfurt am Main

217.150.159.1	vcloud-ffm-private.t-systems.de
217.150.159.2	vcloudcon-ffm-private.t-systems.de
217.150.159.3	baas-ffm-private.t-systems.de
217.150.159.7	vcav-ffm-pri.t-systems-service.com

Houston

217.150.159.8	vcloud-hou-private.t-systems.com
217.150.159.9	vcloudcon-hou-private.t-systems.com
217.150.159.10	baas-hou-private.t-systems.com
217.150.159.14	vcav-hou-pri.t-systems-service.com

Singapore

217.150.159.16	vcloud-sin-private.t-systems.com
217.150.159.17	vcloudcon-sin-private.t-systems.com
217.150.159.18	baas-sin-private.t-systems.com
217.150.159.22	vcav-sin-pri.t-systems-service.com

In order to access the vCloud portal, some pre-requisites must be fulfilled. In addition to the Flash Player and Client Integration Plugin installation, the complete vCloud portal server's certificate hierarchy of the "vcloud-ffm-private.t-systems.de" certificate should be imported (root-certificate, intermediate certificate and URL certificate). Additionally the VMware specific browser configuration, as outlined in the vCloud Director user manual, should be considered.

7. TEMPLATE MECHANISMS

Within the vCloud Director portal Telekom provides a public catalogue which includes standard vApp templates for Windows Server, RedHat and SuSE operating systems. These vApp templates are, in addition to the different operating systems, divided into two categories of vApp templates (Screen shot below):

"MANAGED" : The operating systems are managed by Telekom (Managed OS) including monitoring and incident management, antivirus protection for Windows operating systems and more (Details about the Managed OS key features can be found in the service descriptions).

"SELFMANAGED" : The operating systems are solely managed by the Customer (Self-Managed OS).

Note: A catalogue can be mounted within the same data center only. You can't mount a catalogue from data centre A in data centre B.

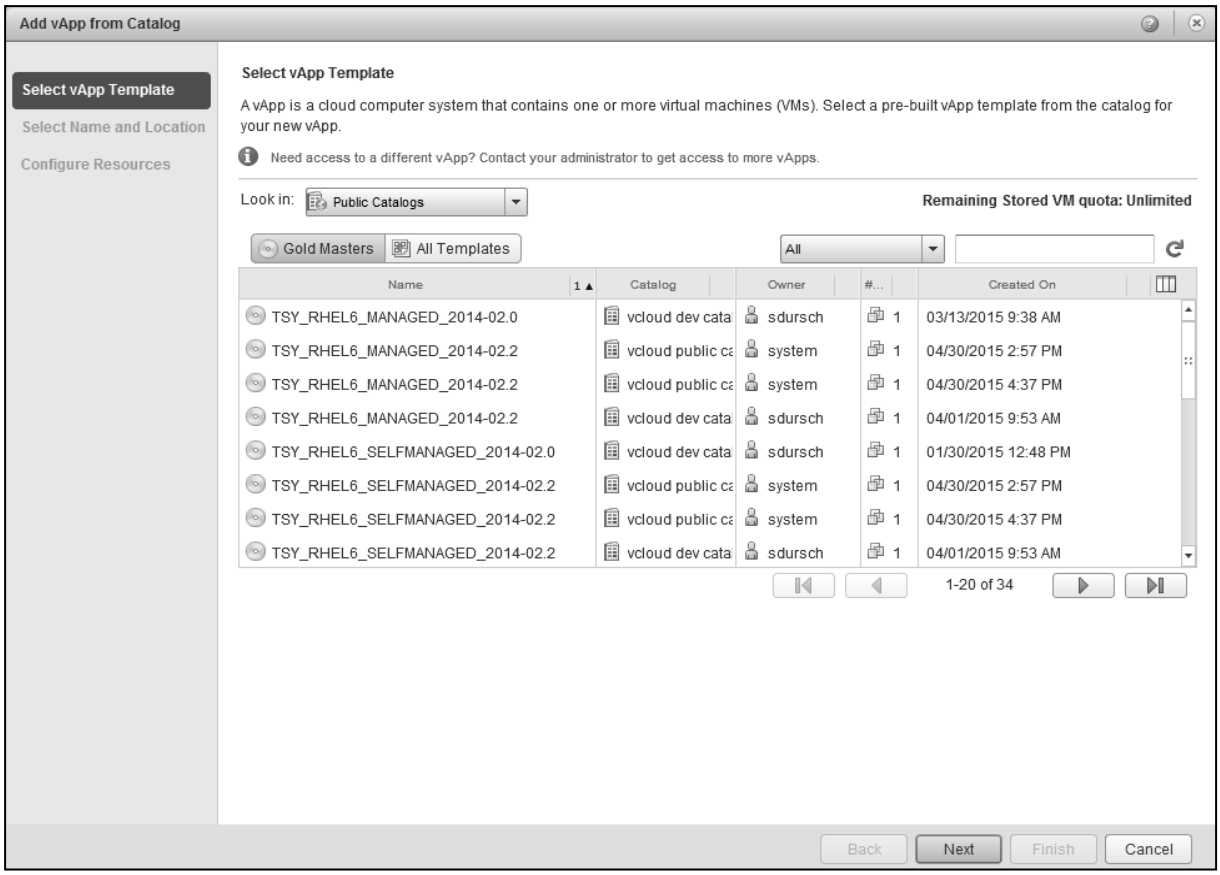


Figure 1: Example of the public catalogue provided within the vCloud Director portal

8. MANAGED OS

Initial deployment – mandatory Admin LAN configuration

In order to enable Telekom to integrate the Managed OS VMs into the necessary backend systems and to connect to the central management infrastructure (e.g. Monitoring systems), it is mandatory to attach a “Admin LAN Interface” as NIC 0 to the virtual machine (see screenshot below):

- As soon as the step “network configuration” is reached, the first NIC (NIC 0) of the virtual machine must be configured with the “TSY-AdminLAN Interface”.
- The enhanced network configuration checkbox must be activated.
- DHCP must be selected for the IP assignment.
- The second NIC (NIC 1) must be configured as “CustomerNetwork” with an static or dynamic IP-Pool and set as Primary NIC.

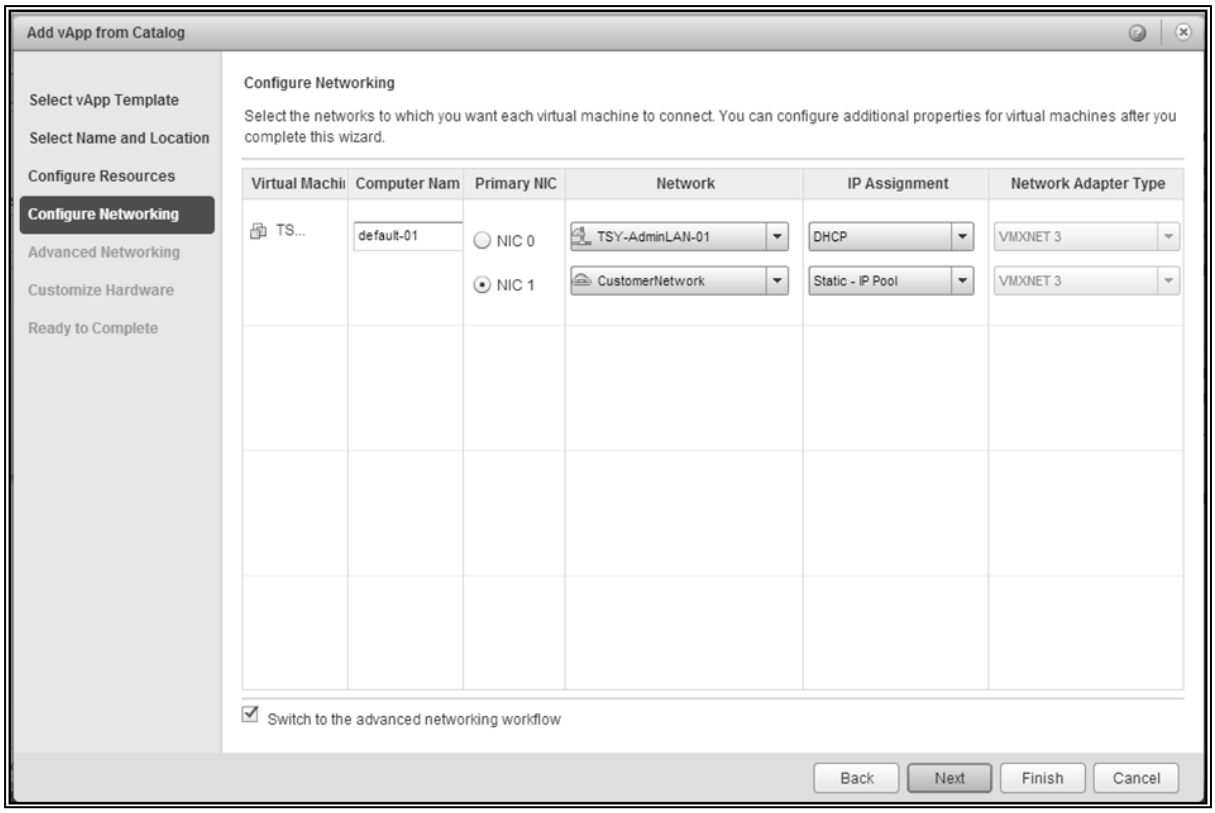


Figure 2: Example configuration of the LAN interfaces during the deployment

Important note: In case the customer doesn't configure the Admin LAN and Customer LAN interface as described above, the deployment process will fail with a network configuration error, the virtual machine can't be started and the operating systems won't be managed by Telekom.

Please take also note, that managed OS systems can be deployed on Backup Integrated Disk Storage (BIS) only in order to ensure daily automated backups, which can be used by Telekom to recover the operating system in case of failure.

The public catalogue is available for vCloud Director Users with the role "vApp-Author (Public Catalog Access)" only. If the customer would like to restrict access to the customer specific catalogue for some users, the standard role "vApp-Author" can be assigned and these users won't be able to use the public catalogue.

Deployment process

After the virtual machine is initially deployed, several Telekom specific background tasks are started in order to integrate the virtual machine into the Telekom backend infrastructure (e.g. Monitoring, Antivirus protection and more). The progress of the backend integration is shown in the overview of virtual machines within the accordant vApp.

Figure 3: Example of the progress information of the managed OS backend integration

Important note: The customer mustn't log-on to the virtual machine until the backend integration is finished and the virtual machine reached the final status "powered-on".

8.1. INITIAL LOGIN

Telekom provides a default user for each Managed OS.

Windows

Username: dsi

Password: qZ!ZwZo?

Linux

Username: dsi

Password: R?FY+oKO

Important note: The customer is asked to change the initial password as soon as the system is deployed and ready for use.

8.2. TEMPORARY PRIVILEGED ACCESS ("ROOT ACCESS")

Important note: The duration for the root access is 14 days. The console input and output will be logged in order to retrace the changes in case of failure.

How to request administrative access:

Windows

Within the Windows Managed OS VMs, the customer can request temporary administrative access by using the desktop icon.

After console login, double click "Request Privileged Access"

Accept the disclaimer about conditions while using administrative rights on a Windows Managed OS

Define the user for which administrative rights shall be granted. Optionally – but preferred - please enter a short description of the intended activities / changes while administrative access is granted.

Wait while the request is queried and one of 3 possible status messages is shown.

Figure 4: Screenshots of the request process - Windows Managed OS VMs

Important note: The customer mustn't configure/create additional local users with administrative rights.

Active Revoke Option

Linux

Within the Linux Managed OS VMs, the customer can request temporary administrative access by executing the Shell-Script “tsy-dsi_request-root.sh”. In order to do so, the default user (“dsi”) is in a special group called “dsi_request_rootsh”.

After console login, execute tsy-dsi_request-root.sh

Accept the disclaimer about conditions while using administrative rights on a Linux Managed OS

Define the user for which administrative rights shall be granted. Optionally – but preferred - please enter a short description of the intended activities / changes while administrative access is granted.

Wait while the request is queried and the user is included in the local sudoers file.

```
[dsi@dcplnx12345678 ~]$ sudo /usr/local/sbin/tsy-dsi_request-root.sh -h
tsy-dsi_request-root version 2_0-4 date 14.07.2017
Copyright (C) 2017 by T-Systems Internation GmbH

tsy-dsi_request-root This shell script is used to request root for a DSIvCloud systems.

Usage: tsy-dsi_request-root.sh [OPTIONS]

Options:
       -h             Print this [h]elp message.
       -d             [D]ebug mode on.
       -n             Enable Dryru[n] mode.
       -f             [F]orce mode on.
       -v             Print script [v]ersion.
       -u [USER]      [U]ser that should be used.
       -c [COMMENT]   [C]omment that should be used.
       -e [E-MAIL]    [E]-mail address that should be used. Instead of @ character (at)
can be used.
       -s             Check [s]tatus.
       -r             [R]evoke adminrights from user.
```

Following commands are equivalent, whereas the first one needs interactive input for Username, Comment and Mail. Force option (-f) will auto-accept the agreement.

```
[dsi@dcplnx12345678 ~]$ sudo /usr/local/sbin/tsy-dsi_request-root.sh
[dsi@dcplnx12345678 ~]$ sudo /usr/local/sbin/tsy-dsi_request-root.sh -u dsi -c “request
root test” -e “ ”

Please note, all activities will be audited during the administrative access. This may
also
include personal information or login credentials. The customer is not allowed to
configure
administrative privileges for additional local users.

The customer must not alter the operating system configuration in any way with the
exception of
mandatory changes for the application installation or administration.

While the customer has administrative access, the SLAs will be suspended. During this
time period,
the customer is responsible for all failures and outages which are not caused by T-
Systems.
T-Systems reserves the right to charge the efforts induced by failures or
Outages caused by the customer. The monitoring will automatically be suspended during
customer
administrative access and T-Systems reserves the right to investigate the changes
performed by
the customer. Once the administrative access has been revoked and the result of the
investigation
```

Important note: Users using the vCloud WebMKS console and an English keyboard layout must enter the "(at)" character for the email address instead of the "@" character.

```
has been positive, the monitoring will automatically be reinstated. If the realized
changes
cant be approved by T-Systems, but the customer wants T-Systems to manage the operating
system
furthermore, T-Systems reserves the right to restore the VM from the last valid snapshot
backup.

This temporary (for the duration of 14 days) administrative access request will be
invoiced.
For more details refer to the respective service description.

Do you agree with this? [yes|(no)]: yes
Please enter the user the action shall be performed for [dsi]. dsi
Please enter the request comment []. request root test
Please enter your e-mail address []. marcel.wiederer@t-systems.com

Resolve dependencies. ............................................ [   OK    ]
INFO    - Checking connection to apiserver
INFO    - OK: Connection Test was successful
INFO    - Requesting information from apiserver for users with admin rights
INFO    - There is no root access active for this system.
INFO    - Request was sent to registration server

The script will loop now, till the request is implemented.
You can cancel the execution with CTRL+C and use the -s option to check the status later.

INFO    - The Request has been successfully implemented.
```

Figure 5: Screenshots of the request process - Linux Managed OS VMs

Important note: The customer mustn't configure/create additional local users with administrative rights. The customer must ensure that the local administrator account (used by Telekom' for support matters) is not altered in any way and also system management service accounts must not be changed by the customer in any way.

RE-Request Root Access

If a user has already root rights on this system, running tsy-dsi_request-root.sh again will lead to following output:

```
…
Do you agree with this? [yes|(no)]: yes
Please enter the user the action shall be performed for [dsi].
Please enter the request comment []. redo order
Please enter your e-mail address []. tsi(at)t-systems.de

Resolve dependencies. ............................................ [   OK    ]
INFO    - Checking connection to apiserver
INFO    - OK: Connection Test was successful
INFO    - Requesting information from apiserver for users with admin rights
INFO    - User dsi has root access from: 2017-08-17 12:47:02 until: 2017-08-17 13:47:02.
ERROR   - User dsi already has sudo rights, can't order sudo rights for another user!
```

Active Revoke Option

Before the root rights are revoked automatically after 14 days, the user with root rights or user dsi can revoke the root rights actively:

```
[root@dcplnx12345678 ~]# /usr/local/sbin/tsy-dsi_request-root.sh -r
INFO    - Checking connection to apiserver
INFO    - OK: Connection Test was successful
INFO    - Requesting information from apiserver for users with admin rights
INFO    - User newroot has root access from: 2017-08-17 13:39:45 until: 2017-08-17
14:39:45.

If you continue root access for user newroot will be revoked.

Do you want to continue? [yes|(no)]: yes
Please enter the request comment []. revoke
Please enter your e-mail address [].

Resolve dependencies. ............................................ [   OK    ]
INFO    - Trying to revoke admin rights.
INFO    - Admin rights for newroot will be revoked shortly.
INFO    - Server answered: VMA1000I: queued

The script will loop now, till the request is implemented.
You can cancel the execution with CTRL+C and use the -s option to check the status later.
INFO    - The Request has been successfully implemented.
```

8.3. USER MANAGEMENT

In addition to the initial default user, the customer is able to administrate additional customer specific users.

Windows

The customer has two possibilities to establish the customer specific user management. Either local users are created as needed, or the Managed OS VM is joined to the customer active directory domain. Both options can be configured with the temporary privileged access (For details please refer to the section “Temporary privileged access (“Root Access”)”. In case local users shall be created the customer can optionally get in contact with the Telekom support to get the local users administrated. It is not allowed to configure/create additional local users with administrative rights.

Important note: For the customer to add a Managed OS Windows VM to their own Active Directory, an Organisational Unit (OU) must be created for all Managed OS VMs with “block inherited rights” set at the root as well as “block GPO inheritance” to be set. The customer must ensure that the local administrator account (used by Telekom’ for support matters) is not overruled or restricted by any OU policies. System management service accounts must not be changed by customer policies in any way.

Linux

The default user (“dsi”) is in a special group “dsi-usermanager”, which allows the customer to administrate local customer specific users. In order to do so, the customer can execute the Shell-Script “tsy-dsi_usermanagement”.

1) Usage

```
Usage: tsy-dsi_usermanagement.sh [OPTINS]

Options:
        -h              Print this [h]elp message.
        -d              [D]ebug mode on.
        -n              Enable Dryru[n] mode.
        -f              [F]orce mode on.
        -v              Print script [v]ersion.
        -u [USER]       User Name
        -a              [A]dd user
        -c              [C]hange user
        -e              D[e]lete user
        -r              Allow User to [r]equest root access.
        -p              Allow User to [p]atch the OS.
        -m              Allow User to [m]anage other users.
        -s              Allow User to connect via [s]sh to the
    customer interface.
        -w              Set or reset the pass[w]ord of a user.
        -l              List all customer users.
        -o              Rem[o]ve home directory of a user.
```

2) Example

```
sudo /usr/local/sbin/tsy-dsi_usermanagement.sh -u testuser -a -s
```

Figure 6: Example usage of the user management shell script

Important note: In order to allow specific users specific rights, these users should be added to the following groups as needed:

- All users in dsi_request_rootsh are allowed to execute tsy-dsi_request-root.sh via sudo.
- All users in dsi_usermanager are allowed to execute tsy-dsi-usermanagement.sh via sudo.
- All users in dsi_patchmanager are allowed to execute tsy-update-os.sh via sudo.
- All users in dsi_allow_cstssh are allowed to connect via ssh to the customer interface.

8.4. PATCH MANAGEMENT

How to get the current patch status and how to install according updates:

Windows

As soon as the customer logs on to the console, the customer will be informed about the availability of new patches via the Microsoft Windows notification service. The message includes a link to the related assistant to apply the patch bundle via standard Microsoft tools.

Linux

As soon as the customer logs on to the console with the default user ("dsi") or any other user which is in the group "dsi_patchmanager", the customer will be informed about the availability of new patches and the information how to install them (Patches can be installed by using the command "sudo tsy-update-os.sh start" if the accordant user is in the necessary group as described in the section "User Management".).

8.5. ADDITIONAL RECOMMENDATIONS AND REGULATIONS

In order to reduce complexity as far as possible, there are some recommendation in regard to the configuration of local disks within a Managed OS.

Windows

The common way to add additional storage for applications is the provisioning of new virtual disks for the related Managed OS VM. The disk needs to be configured within the operating system and the file system must be NTFS, following the Telekom security standard. The new disk should be assigned with the next drive letter to the primary operating system disk (usually D:\).

In some cases it can be necessary to enlarge existing file systems or mount a new storage partition underneath an existing folder structure. This is supported in general but not recommended as it adds complexity.

Important Note: Customer own applications should be only installed on a additional storage drive (usually D:\). The only exception is a Microsoft SharePoint installation.

Linux

The common way to add additional storage for applications is the provisioning of new virtual disks for the related Managed OS VM and it should be configured using the logical volume manager (LVM) in order to be flexible in case of necessary file system extensions for example. It is mandatory to use a separate volume group with own disks for customer own application installations. The customer is free to decide on appropriate names within any volume manager object.

The default file system is depending on the selected Linux distribution and it is recommended to use it in order to reduce complexity and ensure as fast as possible fault resolution processes. (Nevertheless also other file systems are supported of course.). The default file systems of the current Linux operating systems distributions are:

- SuSE Linux Enterprise Server 11: ext3
- RedHat Enterprise Linux 6: ext4

Important note: The SSH for managed operating systems is defined as port 10022.

8.6. FAQ

Q: How long does it take for the request to being processed?

A: Normal processing takes 1-3 minutes. If the process takes longer than 15 minutes, the user will be informed.

Q: How many users can be privileged?

A: Only 1 user can have privileged access at one time. If another user needs to have admin rights the currently granted privileged access must be revoked first.

Q: Is there a time when the rights will be revoked automatically?

A: Yes. The rights will automatically be revoked after 14 days.

9. SELF-MANAGED OS

7

9.1. DEPLOYMENT PROCESS

After the virtual machine is initially deployed, the operating system is configured finally and the virtual machine is rebooted once again.

Important note: The customer shouldn't log-on to the virtual machine before the final reboot finished. Otherwise it might be the case that changes are lost during the reboot.

9.2. PATCH MANAGEMENT AND LICENSE ACTIVATION

Important note: The Telekom infrastructure systems are available as soon as the VMs are connected to a vOrg network and Edge Service Gateway. The routing to the accordant Telekom network is configured by default.

Windows

If Telekom licenses are used, the Self-Managed OS must be activated at the central KMS server. The updates (security updates only) can be reached via the central WSUS server and installed by using standard Microsoft tools and procedures. Actual information for both systems (KMS and WSUS) are provided up to date on the desktop of each Windows VM. The customer can retrieve the information by clicking on the desktop icon "vCloud Customer Information".

Patch Management (WSUS)

Below are the list of the Windows Update Server

Location	IPv4 address	IPv6 address
Munich (DE)	6.204.32.132 (Managed OS) 6.204.72.17 (Selfmanaged OS)	2a00:da9:6:1::2077:7410
Frankfurt (DE)	6.204.128.132 (Managed OS) 6.204.72.17 (Selfmanaged OS)	2a00:da9:6:2101:00ee:0:2104:1607
Singapore (SG)	6.204.120.132 (Managed OS) 6.204.72.17 (Selfmanaged OS)	2a00:da9:6:4101:00ee:0:2112:5566
Houston (US)	6.204.112.132 (Managed OS) 6.204.72.17 (Selfmanaged OS)	2a00:da9:6:1101:00ee:0:2120:7776
London (UK)	6.208.128.132 (Managed OS 6.204.72.17 (Selfmanaged OS)	2a00:da9:6:5001:ff34::2204:9326

Linux

The Linux patch management of the Self-Managed OS is configured automatically and updates can be installed by using Linux standard tools and procedures.

In case the customer is using own SLES 11, RHEL6 or 7 images (Non T-Systems self-managed or managed images) the subscriptions for those unmanaged VMs can be activated by using the following shell scripts:

- wget http://6.204.72.10/pub/unmanaged/tsy-dsi_unmanaged.sh
- chmod +x tsy-dsi_unmanaged.sh

- bash tsy-dsi_unmanaged.sh

```
[root@dsivcloud ~]# wget http://6.204.72.10/pub/unmanaged/tsy-dsi_unmanaged.sh
--2017-01-24 10:25:24--  http://6.204.72.10/pub/unmanaged/tsy-dsi_unmanaged.sh
Connecting to 6.204.72.10:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4932 (4.8K) [application/x-sh]
Saving to: 'tsy-dsi_unmanaged.sh.1'

100%[=====================================================================================================

2017-01-24 10:25:24 (177 MB/s) - 'tsy-dsi_unmanaged.sh.1' saved [4932/4932]

[root@dsivcloud ~]# chmod +x tsy-dsi_unmanaged.sh
[root@dsivcloud ~]# bash tsy-dsi_unmanaged.sh
Download successful tsy_lib-generic.noarch.rpm from DOWNLOAD_SERVER=[6.204.72.10].
Download successful md5.txt from DOWNLOAD_SERVER=[6.204.72.10].
Get /etc/hosts. ..................................................... [   OK    ]
Get tsy-dsi_configure-patchmanagement_unmanged.sh. ................ [   OK    ]
Configure Patchmanagement ........................................... [ working ][59392.237915] systemd[1]: Reloading.
[59392.261387] systemd[1]: [/usr/lib/systemd/system/microcode.service:10] Trailing garbage, ignoring.
[59392.262880] systemd[1]: microcode.service lacks both ExecStart= and ExecStop= setting. Refusing.
[   OK    ]
[root@dsivcloud ~]#
```

Figure 7: Example usage of the license/subscription shell script

9.3. USER MANAGEMENT

Windows

Credentials for the administrator must be configured in the guest customization section of the VM properties in the vCloud Director.

Linux

Username: dsi

Password: BwN!9D$G

Important note: The customer is asked to change the initial password as soon as the system is deployed and ready for use.

9.4. ADDITIONAL RECOMMENDATIONS AND REGULATIONS

In order to fully utilize the self-service functionalities, Self-Managed OS VMs should not be deployed on Backup Integrated Disk Storage (BIS) as a restore is only possible via the Telekom support. Self-Managed systems are recommended to be deployed on online (non-BIS) storage and the backup and restore should be done via the self-service portal of the Backup as a Service solution. For Backup as a Service a granular reporting is included but such a reporting is not available for BIS.

10. ONLINE SNAPSHOTS VON VMS/VAPPS AND BACKUP-AS-A-SERVICE

The customer of DSI vCloud has multiple options to cover Data Protection.

It is possible to use the VMware snapshot function to create an online copy of a VM that is then stored as a template in the catalog and/or can be copied to the backup catalog. To ensure that the backup locations are separated here, the customer must use two vDCs, one must be ordered in data center A and the other in data center B. In this case, VMs from data center A should be backed up into a catalog in data center B, and vice versa.

- Usage of Backup-integrated-Storage (BIS) . This storage includes the build-in lowlevel snapshots which are invisible for the vCloud UI, API and VMs above. Here it's also possible to restore a VM from the filer's snapshot, however this is a manual task that needs to be performed by the Telekom operating team. Therefore it's not recommended for daily restore needs, but rather a fallback solution.
- Optionally the customer has the possibility to use Backup-as-a-Service, which offers policy based and fully automated backups and restores in customer repsonsibility (self-service).

- The customer can also use his own backup solution, with backup services either located on DSI vCloud or backup data shipped to an environment outside of DSI vCloud. E.g., via the private customer network directly to a backup infrastructure in the customer data center.
- Use application or database build-in features for data protection / replication, and dump the data to a backup store of his choice. E.g. another system on another Datacenter. This case is similar to the previous one.

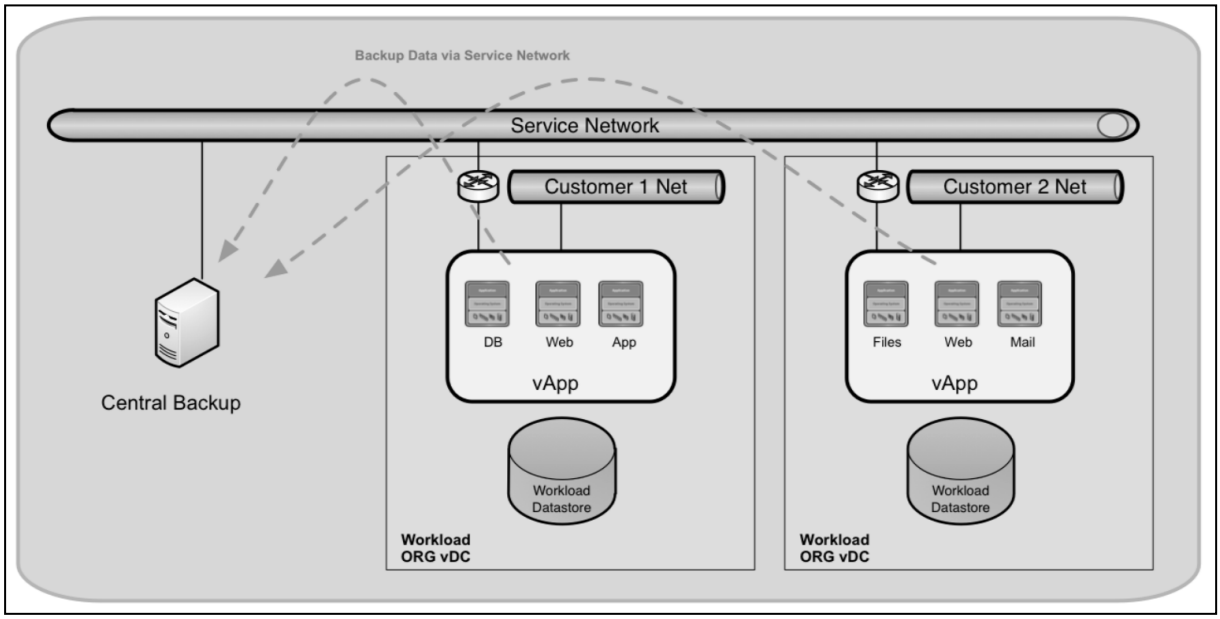


Figure 8: Schematic backup design

The customer should proceed carefully when copying and re-providing existing VMs. In some cases IPs or system names/IDs may be duplicated with such activities, for example. This may cause problems on the other systems or applications. With regard to this difficult task, DSI vCloud provides the customer with the following options:

Implementation of VMs in so-called "isolated" networks that either are not connected to the surrounding environment or are shielded behind a virtual firewall with NAT functionality.

Changing of the system identity (e.g., name or ID) before provisioning.

Scripting execution before and after system provisioning in order to adjust the VM configuration.

10.1. BACKUP-AS-A-SERVICE (BAAS)

10.1.1 GENERAL

Access to BaaS is granted via a separate self-service portal (available in up to 20 different languages) with an own user management, which offers the customer an overview of his configured backups for his DSI vCloud workloads. The fully independent self-service portal with own user management offers customers the possibility to keep their organizational separation of online and backup administrators in order to avoid concurrent deletion of online and backup data by accident.

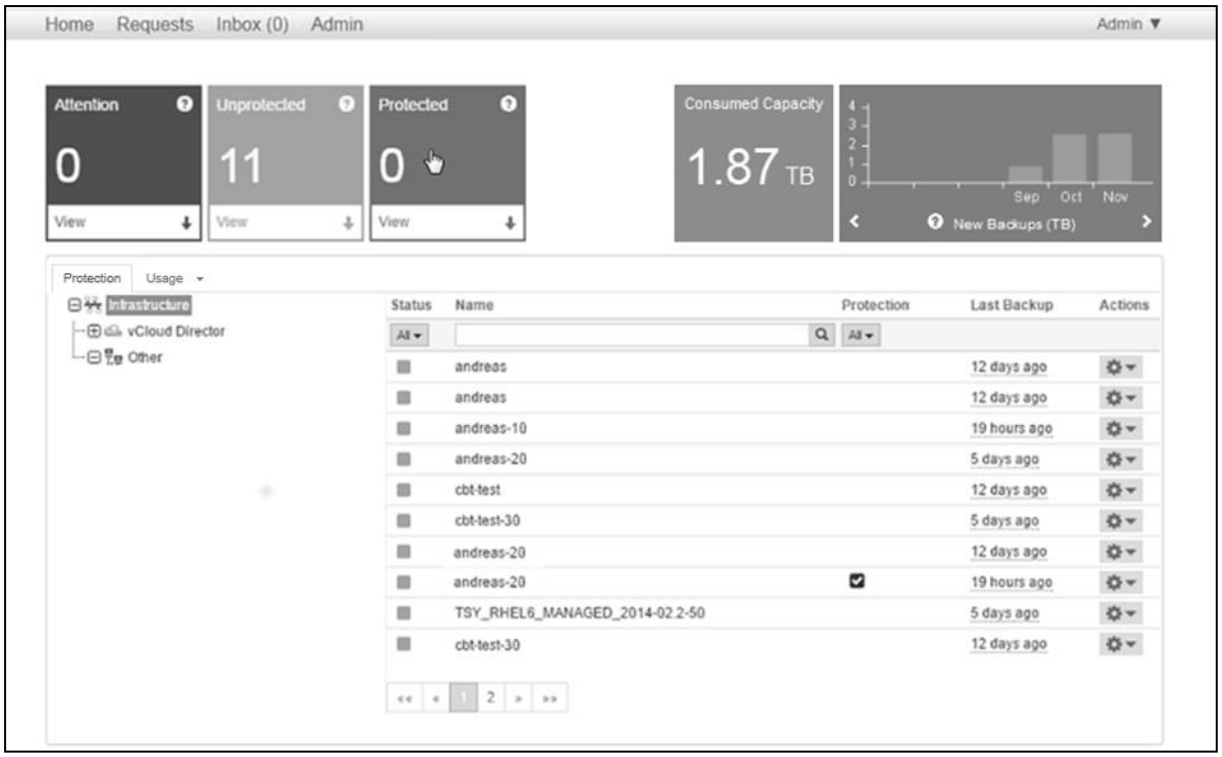


Figure 9: BaaS Customer Dashboard

Within DSI vCloud Hybrid the self-service portal is available via the Internet, whereas within DSI vCloud Private the self-service portal is only available via the customer Intranet (private network).

Besides one-time backups (backup now) and individual restores, the BaaS offers the possibility to shedule policy-based and fully automated backups for single VMs, vApps and even whole vDCs.

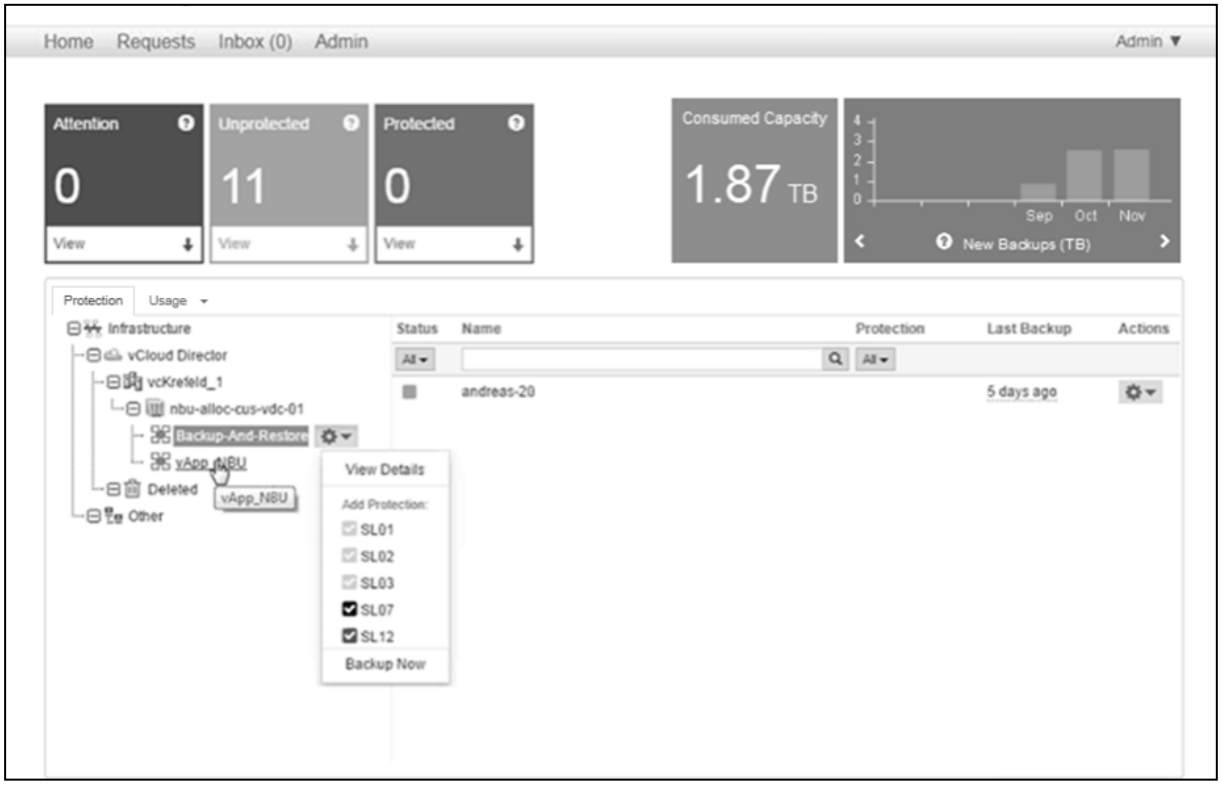


Figure 10: Protect machine and Backup now on vApp level

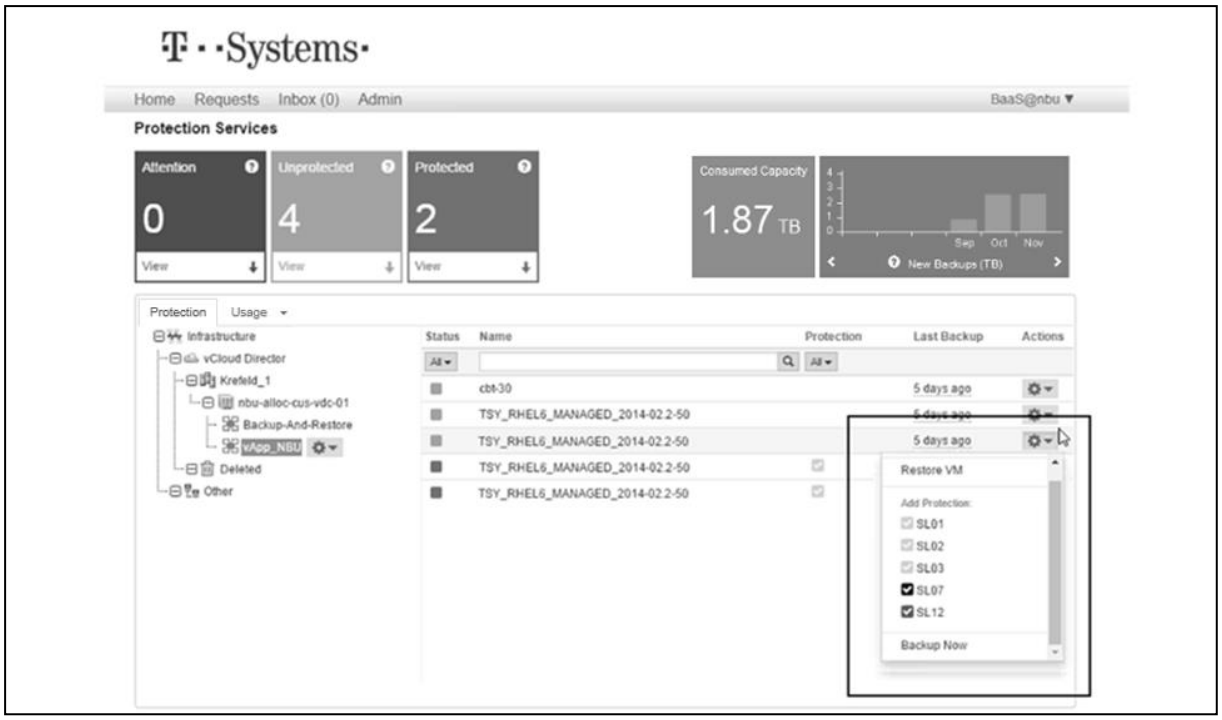


Figure 11: Protect machine and Backup now on VM level

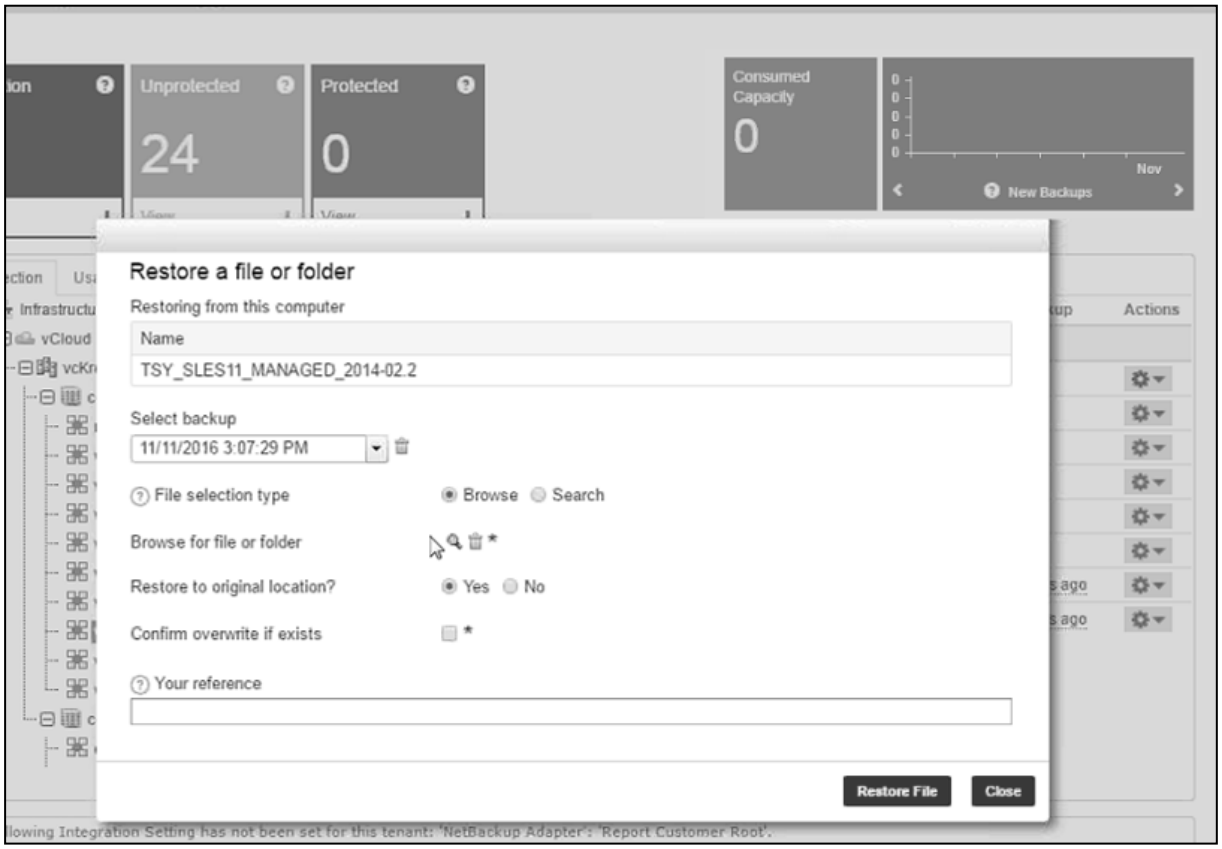


Figure 12: Restore VM

The backup solution doesn't need any installation of agents within the VMs and backups the data via the backend-infrastructure, without having any influence on the performance of VMs. Crash consistency is reached by using VADP in combination with the VMware tools that should be installed within the guest operating system of each VM. To reduce storage volumes the backups are done per default with blocklevel incrementall copies. Backups are stored on a separate backend infrastructure within the same physical twin-core data center as the customer vCloud based VMs are hosted. They are subsequently mirrored to the other physical data center of the twin core.

Note: The maximum disk size for VMs that can be backed up with BaaS is limited according to the following rules. For VM sizes not following this rules a proper backup can't be ensured.

SL01 to SL06 and SL16 to SL21: maximum disk size attached to a VM in total is limited to 1 TB.

SL07 to SL15 and MF3Y to YF12Y: maximum disk size attached to a VM in total is limited to 4 TB.

While backups are initially stored to disk storage, backups older than one month can be outsourced to tape libraries. Independent from that, the restore can be triggered via the self-service portal.

Important note: The long term retention backup feature is offered for the duration of the contract. In case of termination of the service it is the customers duty to restore and download the data as outlined in the terms and conditions. Please be aware, that for backups with a retention period greater than one year, the VM may no longer be technically compatible with the DSI vCloud version. In case the VMware technology will change in a way that the currently known VM format (VMDK) is not used and not supported anymore, it is not ensured that Backups can be restored successfully. In such cases, and if Telekom did get prior notice from the vendor, Telekom will inform the customer in advance. Customers should evaluate if the solution fulfills their technical and compliance requirements.

10.1.2 CORE FUNCTIONALITIES

Backup Now (one-time): With this functionality it is possible to process an one-time backup of a VM, vAPP or vDC within a few steps. The retention time can be chosen based on pre-configured profiles (2 weeks, 1 month, 2 months, 3 months, 6 months,12 months, 3 years, 7 years, 10 years, 12 years)

Protect Machine (regular): This functionality offers the customer the possibility to configure regulare, rule-based and fully automated backups for VMs, vApps or vDCs. Based on pre-configured profiles it is possible to decide on backup frequency, as well as the retention period. After the first full backup of an object is done all further backups are done block-level incrementell.

Restore VM: With this functionality the customer is able to restore a single VM including meta data based on an backup done before. It is possible to restore the VM into the original vApp or to decide to restore into a different vApp, which was deployed especially for this restore for exemple.

Attention: Once the option "overwrite" is chosen, the VMs is restored to its original location and the original VM (for the case it is still up and running) will be irrevocably deleted. If a VM is restored into a different vApp it is recommended to enable guest customization to avoid e.g. doubled SIDs, system names, IP-addresses and therefore negative influence on existing application landscapes. In both cases the restore will be always done to the standard storage class that is defined in the vDC where the restore is performed to. It is important that there is enough storage capacity of this class available in the vDC, otherwise the restore will fail. In general the restrictions and recommendations of the software products used within a VM have to be considered. Telekom recommends the customer to develop his own backup and restore concept and to test properly.

Unprotect Machine: This enables the customer to deconfigure the rule-based backups for his VMs, vApps and vDCs.

Attention: The backup data for previously protected machines remains in the system according to the selected retention and will therefore expire over time. The remaining backup data will be charged as long as the retention time has not expired. Same is valid for deleted VMs within the vCloud Director.

Request Monitoring / Auditing: For every customer initiated request (e.g. initiated backup-now), it is possible to get an detailed overview on the current status. After a manual backup or restore process was started the customer can optionally decide to be informed on the status via e-mail.

Backup reporting: Detailed backup reportings are available for download as PDFs in this area and via the Usage tab

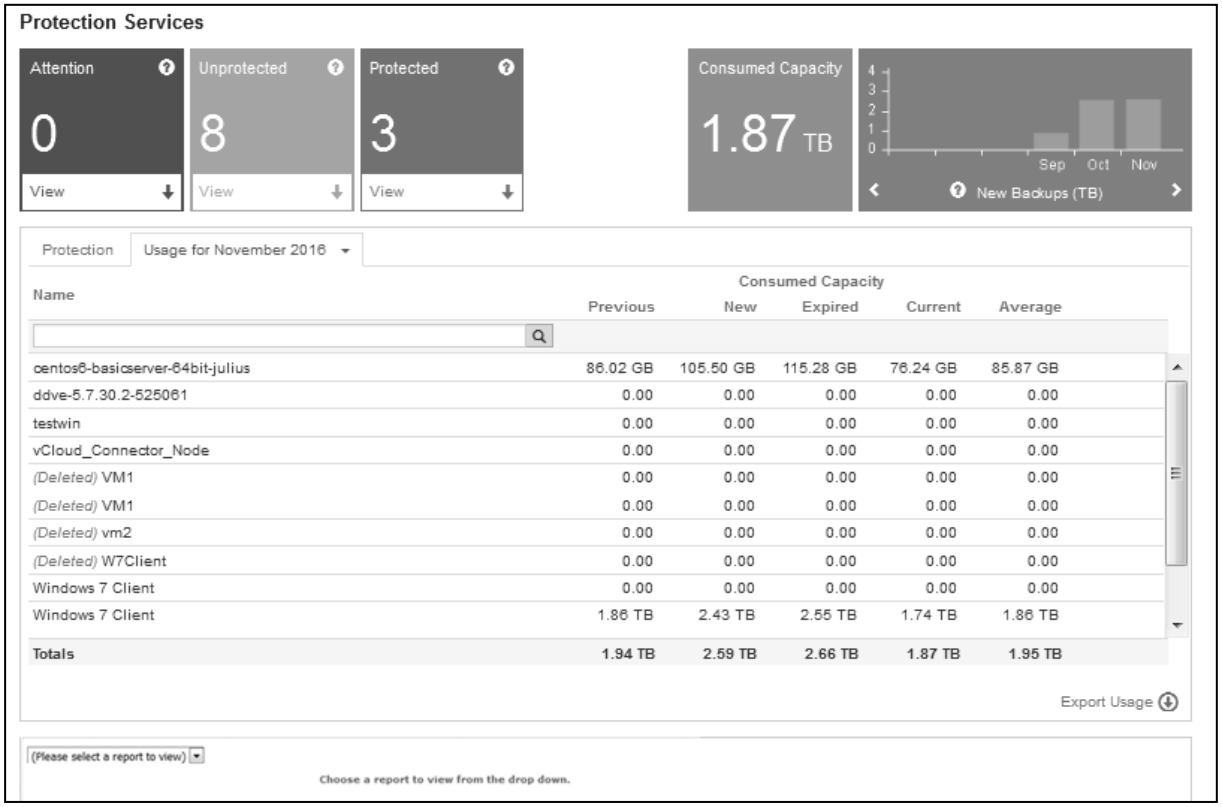


Figure 13: Backup reporting

Usage: This function shows the usage in GB for the selected month. This information is only technical without any commercial impact or relevance. The following relationship exists for each row in the table:

Current = Previous + New – Expired

Current= Backup volume of the current period

New = New Backup volume of the current period

Expired = Backup volume which expired during the current period

Previous = Backup volume of the previous period

Average = Average Backup volume of the current period. The average size is calculated as total backup space for the month divided by the number of days in the respective month (1-31).

The refresh cycle for this reporting is at present once per day (per default at 7:30 a.m. local time) and the statistics reflect the values collected up to the refresh cycle. In case the backup for a particular VM was in progress whily the refresh was ongoing, these additional volumes won't be reflected in here (only completed backups).

An export of the information is possible to a .txt file via the export usage link.

Note: The information under the usage tab is only relevant from a capacity perspective. If virtual machines where backed up with a previous version of BaaS, without the usage tab in the portal, then the utilization calculation is repeated to include data from the past. But this update functionality has limitations as the utilization of new, already deleted or expired virtual machines can't be updated.

User management: Customer can managed existing users (e.g. password resets) and create new backup users.

Available backup profiles:

Backup as a Service offers different profiles for the regular backup functionality, that differ in backup frequency and retention period. The current backup profiles as well as the information about current starting times of scheduled backups are listed in the self-service portal. Telekom reserves the right to change existing backup profiles especially the backup start window to be able to manage capacity in the backend infrastructure.

Note: All your full backups of the policies SL01 – SL06 are stored one period longer as described in the policy.

This enables you to restore from all your incremental backups until the latest full backup of this period expired.

All vApps which are additional copied with the same name in a private catalogue will be automaticly backed up.

Please set a new name for the catalog to secure the consistency of the backups.

Name	Description	Availability
SL01 (Will be discontinued)	Weekly full (Sunday), daily incremental, 2 weeks retention, start 20:00	World wide
SL02 (Will be discontinued)	Weekly full (Monday), daily incremental, 1 month retention, start 20:00	World wide
SL03 (Will be discontinued)	Weekly full (Tuesday), daily incremental, 2 months retention, start 20:00	World wide
SL04 (Will be discontinued)	Weekly full (Wednesday), daily incremental, 3 months retention, start 20:00	World wide
SL05 (Will be discontinued)	Weekly full (Thursday), daily incremental, 6 months retention, start 20:00	World wide
SL06 (Will be discontinued)	Weekly full (Friday), daily incremental, 1 year retention, start 23:00	World wide
SL07	Weekly full, 1 month retention, start 00:00	World wide
SL08	Weekly full, 2 months retention, start 00:00	World wide
SL09	Weekly full, 3 months retention, start 00:00	World wide
SL10	Weekly full, 6 months retention, start 04:00	World wide
SL11	Weekly full, 1 year retention, start 08:00	World wide
SL12	Monthly full, 2 months retention, start 00:00	World wide
SL13	Monthly full, 3 months retention, start 00:00	World wide
SL14	Monthly full, 6 months retention, start 04:00	World wide
SL15	Monthly full, 1 year retention, start 08:00	World wide
SL16	Daily full, Retention 14 days, Start 03:00	World wide
SL17	Daily full, Retention 1 month, Start 03:00	World wide
SL18	Daily full, Retention 2 months, Start 03:00	World wide
SL19	Daily full, Retention 3 months, Start 03:00	World wide
SL20	Daily full, Retention 6 months, Start 03:00	World wide
SL21	Daily full, Retention 1 year, Start 03:00	World wide
MF3Y-1	Monthly full (from 1st of each month), 3 year retention, start 04:00	Munich
MF7Y-1	Monthly full (from 1st of each month), 7 year retention, start 04:00	Munich
MF10Y-1	Monthly full (from 1st of each month), 10 year retention, start 04:00	Munich
MF12Y-1	Monthly full (from 1st of each month), 12 year retention, start 04:00	Munich
YF3Y-3	Yearly full (from 3rd of January), 3 year retention, start 04:00	Munich
YF7Y-3	Yearly full (from 3rd of January), 7 year retention, start 04:00	Munich
YF10Y-3	Yearly full (from 3rd of January), 10 year retention, start 04:00	Munich
YF12Y-3	Yearly full (from 3rd of January), 12 year retention, start 04:00	Munich

Figure 14: Overview of backup profiles within the self-service portal

Customer API and vendor documentation:

Please check the API documentation and the vendor documentation under following link:

https://www.veritas.com/support/en_US/article.000024782

11. CENTRAL LOGGING

8

11.1. PRE-DEFINED LOG/NAT CONFIGURATION

Important note: The customer mustn't change the LOG/NAT settings on the Edge Service Gateway device as the central logging will be disabled in case of a wrong configuration. How to enable the logging which is usable by the customer is described below.

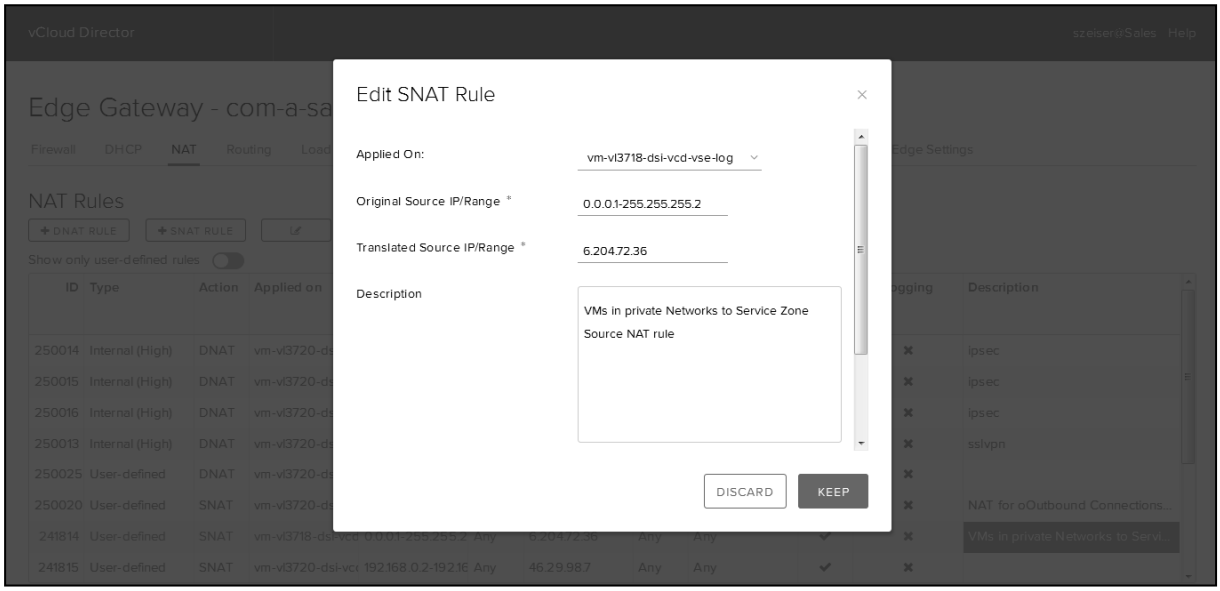


Figure 15: LOG/NAT configuration on the Edge Service Gateway Device

In addition the customer mustn't use the Telekom Admin-LAN. Any change in regard to the Telekom Admin-LAN is not supported and will be deleted.

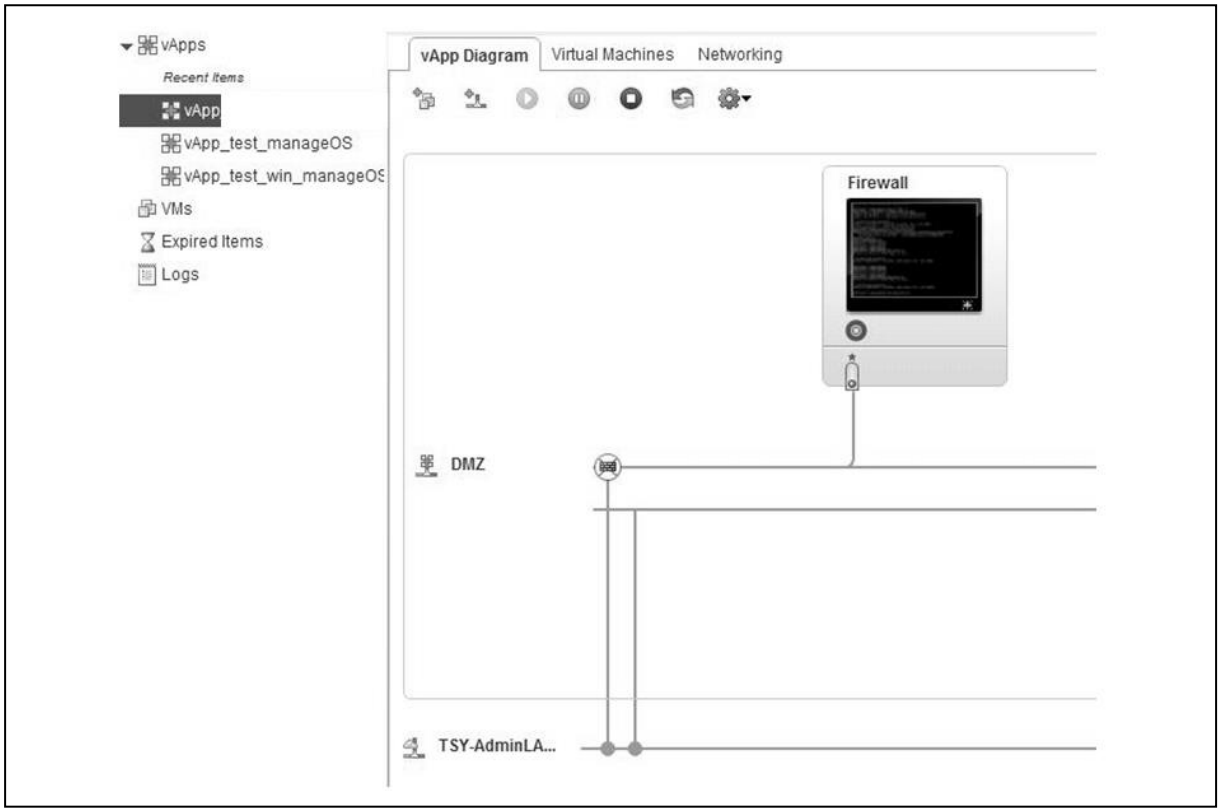
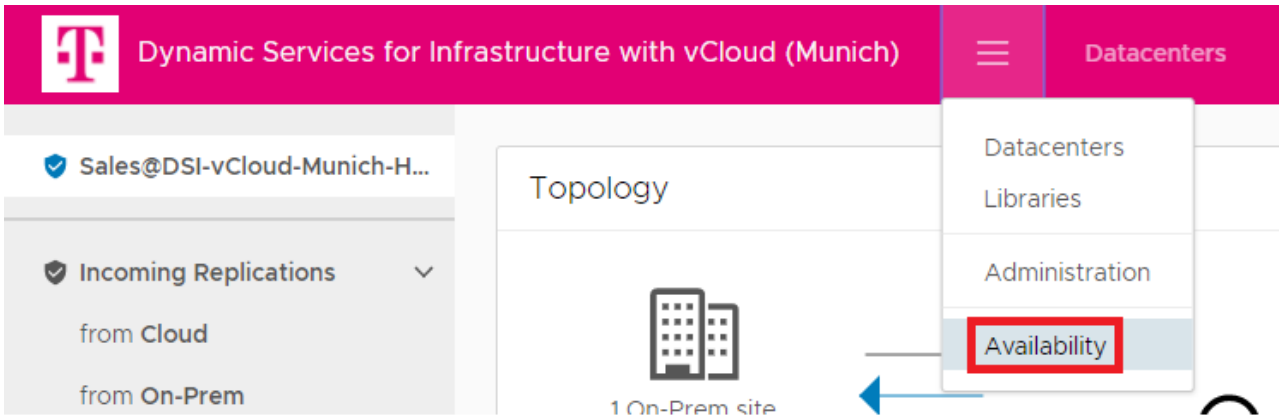


Figure 16: Example of an unsupported connection from the DMZ to the Telekom Admin-LAN

12. VCLOUD AVAILABILITY

vCloud Availability is a simple, secure and self-service product offered by Telekom for DSI vCloud. The product offers cost-effective onboarding, migration and disaster recovery services between DSI vCloud and your on-premise vSphere infrastructure with minimal downtime. vCloud Availability uses vSphere Replication which allows for workloads to be failed over, failed back and migrated between DSI vCloud and your on-prem infrastructure. Further VMware Tools integration allows for agentless, application consistent replication to the cloud. Recovery Point Objective (RPO) can be set on a per VM basis to ensure minimal data loss in the event of a failure and multiple point in time recovery allows you to retain up-to 24 restore points for flexible recovery. All communications from on-premises to the Cloud is secured end-to-end using TLS encryption and the product does not require any inbound ports to be opened to your on-premise site. The product can also be used to replicate and migrate VMs and vApps within DSI vCloud.

The service can be accessed from the vCloud Director Tenant Portal by selecting **Availability.**



To leverage the on-prem to Cloud functions of this service, you must deploy and configure additional on-premise appliances in your on-premise vSphere infrastructure and connect to the vCloud Availability Service. Documentation for the product including a User Guide is available from https://docs.vmware.com/en/VMware-vCloud-Availability/index.html

The following Public API service endpoints are required during the configuration of on-premise vCloud Availability appliance:

Site	Public API Endpoint Address
DSI vCloud Hybrid – Munich, DE	https://vcav-muc.t-systems.de:443
DSI vCloud Private – Frankfurt, DE	https://vcav-ffm-pri.t-systems-service.com:443 **
DSI vCloud Hybrid – London, UK	https://vcav-lon-hyb.t-systems-service.com:443
DSI vCloud Private – Houston, USA	https://vcav-hou-pri.t-systems-service.com:443 **
DSI vCloud Private – Singapore, SG	https://vcav-sin-pri.t-systems-service.com:443 **

** DSI vCloud Private API Endpoints addresses are not resolvable via public DNS nor are they Internet routable, ensure that the IP addresses listed under Self-Service Portal are configured to route correctly on your on-premises network and that the service addresses are all resolvable using your internal DNS infrastructure or other name resolution strategy.

Table 4 vCloud Availability Service Endpoints

The following firewall rules are required on your on-premise environment for the on-prem to cloud service to function:

On-Premise Appliance	Traffic Flow	Destination	Port & Protocol
vCloud Availability appliance	On-Prem Egress	DSI vCloud Availability Public API Endpoint	tcp/443

Table 5 vCloud Availability Customer-side firewall rules

Limitations and Caveats

Please review and consider the following important limitations and caveats before using this service. Please also review the Known Issues section outlined below

General

- This product is not a backup product. Customers should perform backups of their virtual machines with the BaaS product or similar
- VMs disks can not be added/removed or changed whilst a VM is protected by vCloud Availability. In order to change the disk configuration of a VM you must first un-protect a machine, perform the operation and then reprotect the machine.
- Virtual machine snapshots are not replicated as part of a protection
- You should not protect a VM which has existing snapshots as reverting to a snapshot that was taken before the virtual machine was protected by vCloud Availability will cause the replication to become corrupt.
- vCloud Availability supports replication of virtual machines with disks on the non-default Storage Policies however the replica virtual machines will all be placed on a single Storage Policy defined during the protection.
- vCloud Availability creates Independent Disk objects in your Org vDC (destination vDC); these are used by the service for internal pruposes and should not be removed or tampered with for the product to work as designed.
- Virtual machine disks are locked during synchronization for virtual machines that are powered off. If a disk is locked you will be unable to Power On the virtual machines until the Sync operation completes.
- If using MPIT (multiple point in time) recovery points, you should ensure that you have at least 2 times the capacity (size of the VM) available in the destination OrgVDC to accommodate these snapshots and prevent overallocation of storage.

Managed OS

- Managed OS virtual machines are not supported or compatible with vCloud Availability. Managed OS machines should not be Protected with vCloud Availability.

Backup-as-a-Service (BaaS)

- BaaS can be used to backup virtual machines protected by vCloud Availability
- For Windows based virtual machines the “Ensure application-level consistency prior to creating an instance” option in vCloud Availability is not supported when a virtual machine is also protected with Backup-as-a-Service (BaaS). This is due to a known issue which in rare circumstances may lead to a virtual machine becoming unresponsive if both services trigger guest OS quiesce operations in parallel. As there is no predictable way to prevent this condition it is not recommended to enable this option in vCloud Availability if a workload meets this criteria.
- If a machine that is assigned a BaaS policy is failed over or migrated to another Org VDC (or failed back) the BaaS policy assignment will be lost; you must re-assign a BaaS policy to the machine after any failover/migration operation
- If restoring a virtual machine protected by vCloud Availability from a BaaS backup (with the overwrite option selected), you must first unprotected the machine in vCloud Availability and reprotect after the restore has been completed.

Known Issues

- **Metadata out-of-date after failover:** In rare cases, if the VM meta data has been recently updated after a VM Failover or Test Failover is performed the vApp is failed over the vApp/VM metadata (Name, Start Order or Meta Data) is out of date.

Workaround: There is currently no workaround for this issue however this issue does not affect the data at the VM level only the assosicated meta data. This issue is caused by a vCloud metadata update not being applied to the vCloud Availability database. T-Systems are working with VMWare to develop a solution for this limitation.

13. PERFORMANCE OPTIMIZED VDC

While performance optimized vDCs can be used for multiple use cases, they are also designed for SAP Hana workload as NUMA-awareness is achievable with the appropriate VM sizing and as the underlying hardware is generally certified for SAP Hana. Please always refer to the official SAP Hana on VMware vSphere best practices guide and white paper, while specific recommendations regarding SAP Hana on DSI vCloud are outlined here.

General recommendations:

- Use the storage class "Very High" for highest performance
- Use Paravirtual SCSI Controllers and Network Adapters
- Use VMware Snapshots only during non-peak times and never snapshot VM with memory
- Remove unused virtual hardware
- Always use latest VM Hardware version
- Configure guest filesystems with the appropriate offset on the partitions for VMware virtualization
- Don't use CPU or memory HotAdd functionalities.
- Respect the recommended vCPU to RAM ratio for the sizing of VMs in order to respect a reasonable NUMA Node configuration.

VM sizing recommendations:

The sizing recommendations for virtual machines below are based on the current blades, considering a reasonable host respectively virtualization overhead and the NUMA-awareness.

NUMA config	vCPUs (CPU cores)	GB RAM
½ NUMA Node	10	230 GB
1 NUMA Node	20	460 GB
2 NUMA Node	40	920 GB

Table 6 SAP Hana VM sizing

14. HOW TO SECTION

14.1. HOW TO SUBSTITUTE A CLIENT INTEGRATION PLUGIN BY A NEWER VERSION

In case a new vCloud Director version comes along with a new Client Integration Plugin (used to access the virtual machine consoles) the old plugin of previous vCloud director versions must be uninstall and the new plugin must be installed. Below you can find a short instruction how to clean up the old installation and upgrade to the new plugin:

1. **Remove any previously created ovftool configuration file:**
   Windows: Delete “ovftool.cfg” from "C:\Users*<username>*\AppData\Roaming\VMware"
   Linux: Delete ".ovftool" from the user's home directory (also for the user root)

2. **Delete the file .csp_ovftool_settings.js from the user's home directory:**
   Windows: C:\user*<username>*
   Linux: /*<home directory path>*/*<username>* (also for the user root)

3. **Remove any previously created ovftool settings file:**
   Windows: Delete “.csp_ovftool_settings” from “C:\Users*<username>*\AppData\Roaming\VMware"
   Linux: Delete ".csp_ovftool_settings" from the user's home directory (also for the user root)

4. **Uninstall the previously installed Client Integration Plugin:**
   Windows: Uninstall VMware Client Integration Plug-in 5.5.0 from Control Panel via “add/remove programs”.
   Linux: Execute "*<Client Integration Plugin Directory>*/VMware-ClientInegrationPlugin-*<version>*.x86_64.bundle –uninstall-component=vmware-cip-*<version>*" on 64bit machines
   or "*<Client Integration Plugin Directory>*/VMware-ClientInegrationPlugin-*<version>*.i386.bundle –uninstall-component=vmware-cip-*<version>*" on 32bit machines

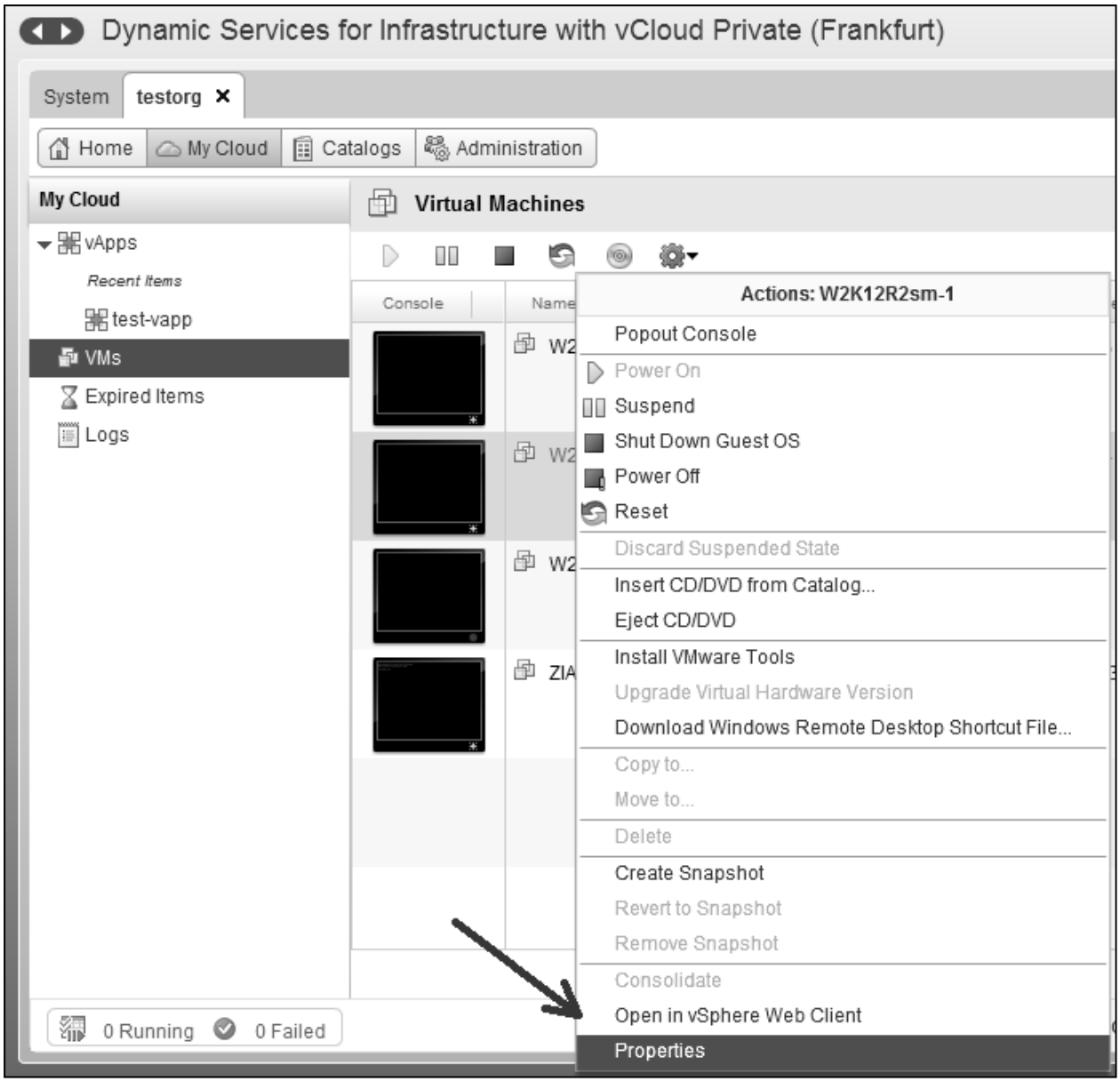
5. **Open the vCloud Director URL and download the new Client Integration Plugin:**
   Either click on a virtual machine to open a VM console or upload/download a catalog template

6. **Follow the instructions in the portal and install the Client Integration Plugin.**

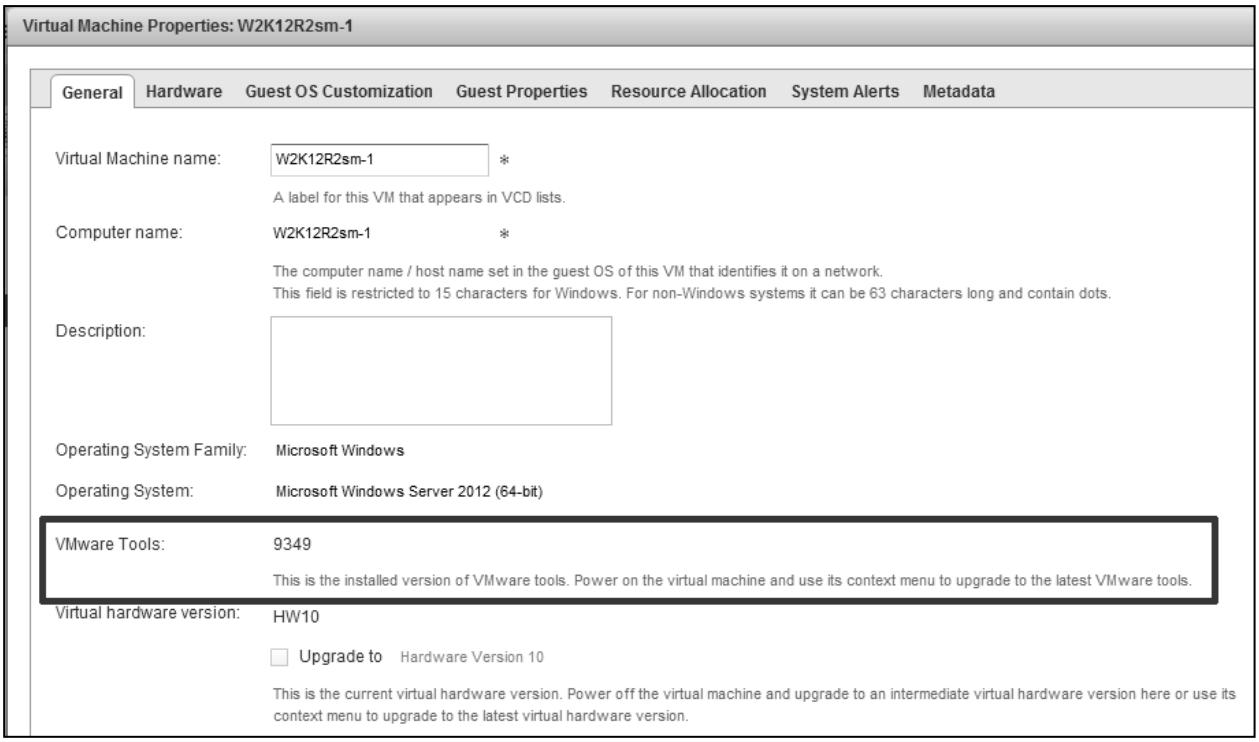
14.2. HOW TO VERIFY THE VMWARE TOOLS / OPEN-VM TOOLS VERSION

In order to verify the current version of the installed VMware tools, please follow the steps below:

- Login to the vCloud Director and open the relevant vApp
- List the existing VMs of that vApp
- Open the properties by right clicking on the VM and selecting “properties”



- Check the version of the VMware Tools



- In case of out-dated versions, follow the install guideline in the next chapter

14.3.HOW TO INSTALL THE VMWARE TOOLS / OPEN-VM TOOLS

Important note: It is very important that you install VMware Tools (in case of Linux, optionally the Open-VM tools which are provided by the respective Linux vendor) within the guest operating system of the VM as it contains a series of utilities to improves the performance and management of the VM. As an example the tools contain driver for the virtual hardware and support the optimization of the underlying infrastructure and hardening in case of outages (e.g. configuration of mandatory 180 seconds time out values for the disks). Without the tools, it's not possible for T-Systems to identify if a virtual machine needs further support after infrastructure incidents (e.g. VM reboot necessary as the disks are mounted read-only). The T-Systems MANAGED OSs are pre-installed with the tools already. You mustn't uninstall the tools in that case. In case you are using SELF-MANGED OSs the tools must be installed timely after the initial deployment.

The installers for VMware Tools for Linux and Windows guest operating systems are built into vCloud as ISO image files and appear as CR-ROM to your guest OS as soon as you selected the installation via the vCloud Director (e.g. A CD-ROM is shown within the Windows Explorer). Below you can find a short instruction how to proceed:

- Select the installation of VMware tools by right clicking on the virtual machine in vCloud Director:

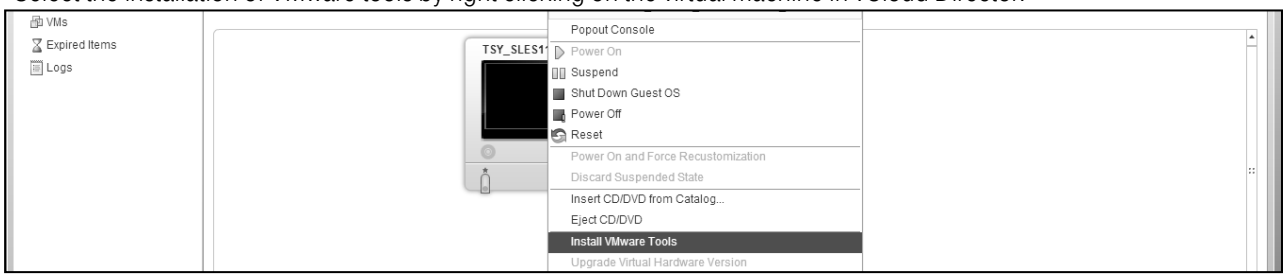


Figure 17: Install VMware Tools via vCloud Director

(In case you want to install the Open-VM tools for your Linux guest OS, you can obtain the installation sources from the respective Linux vendor.)
- The ISO image will be provided automatically to your guest OS

- Logon to the virtual machine and start the installation process of the VMware tools

Important note: the platform offers the minimum version of VMware tools that is necessary for workloads to properly run on DSI vCloud. However, there might be newer versions available directly from VMware. Installing these newer versions within a VM is fully supported and recommended for cases where you see unexpected VM behaviour (e.g. crashes, performance issues) that potentially might be caused by a bug in VMware tools.

The installation process does then vary, depending on which operating system you are using.

More details about the installation of VMware tools can also be found online in different VMware Channels like https://www.youtube.com/user/VMwareKB or https://www.youtube.com/user/vmwaretv

14.4. HOW TO ACCESS THE EDGE SERVICE GATEWAY SYSLOG EVENTS

In order to enable the customer to retrieve syslog events of the Edge Service Gateways, the Edge Service Gateway is logging to two IP addresses per default. One IP address out of the Telekom network and one IP address reachable from the customer network (Syslog-Server 2). The information can be found within the syslog server tab of the Edge Service Gateway.

Figure 18: Example of the pre-configured Edge Service Gateway syslog IP addresses and networks

The customer can retrieve the logging events via a self-managed syslog server:

Create a routed vOrg network, with the IP address of the “Syslog-Server 2”.

Deploy a virtual machine which should be used as syslog server (e.g. „TSY_RHEL6_SELFMANAGED*“) and assign the “Syslog-Server 2” IP address.

Configure syslog within the syslog server (e.g. the standard rsyslog within the RedHat machine).

Allow the network connection from the Edge Service Gateway to the syslog server via UDP Port 514. (e.g. IPtables within the RedHat VM).

-

Important note: In order to retrieve all logging events all the time, multiple syslog server must be configured per Edge Service Gateway and per routed vOrg network. Alternatively one syslog server can be deployed and as soon as an analysis of syslog events of a specific Edge Service Gateway Device is required, the syslog server is attached to the respective network.

14.5. HOW TO IDENTIFY THE EXTERNAL INTERNET FACING IP ADDRESSES

In case the customer ordered internet access, the customer can get the external IP-addresses from the vCloud Director self-service portal.

- Go to the "Administrator tab"
- Select the desired vDC for which internet access was ordered
- Select the "Edge Gateways" tab
- Right click on the Edge Gateway and select "Properties"
- Select the "Configure IP Settings" tab within the pop up window
- Verify the assigned "inet-flex" related external IP addresses on the right hand side

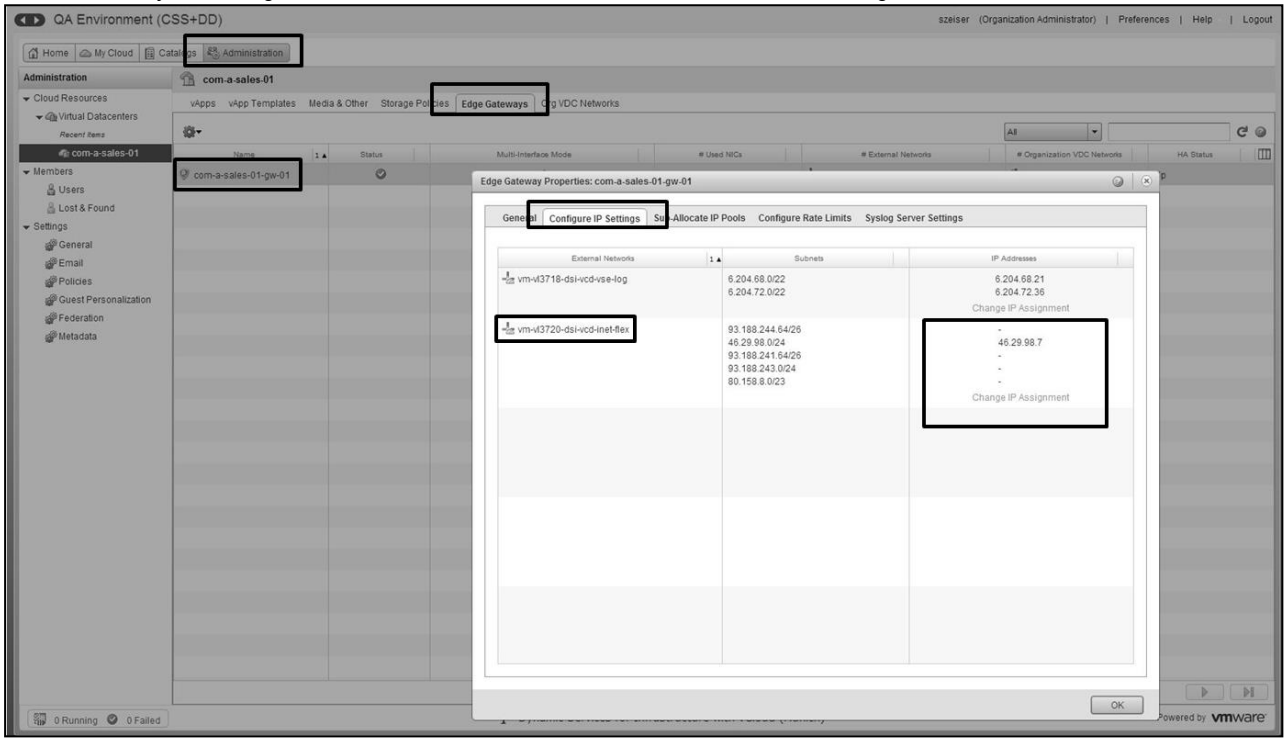


Figure 19: Identification of the assigned internet facing IP addresses

- **Note:** All external IP addresses (Flexible internet access, Secure internet access) ordered via T-Systems will remain as Static IP in the Edge Service Gateway until terminated

14.6. HOW TO CONFIGURE APPROPRIATE NAT AND FIREWALL RULES IN ORDER TO USE INTERNET ACCESS

- First of all, create a routed Org VDC Network via the "Administration" tab within the "Org VDC Networks" tab
- Afterwards go to the "Edge Gateways" tab, right click on the Edge Gateway and select "Edge Gateway
- Services..."
- Enable DHCP within the "DHCP" tab and add the previously created IP address pool of the Org VDC Network, Alternative you can use static IPs without DHCP.
- Move to the "NAT" tab and create a Source (SNAT) and Destiation (DNAT) NAT rule for the external IP and the previously created Org VDC Network
- For outgoing internet traffic, add a SNAT rule from the internal source network (previously created Org VDC Network) range to the external internet IP or external IP address range.
- For incoming internet traffic, add the DNAT rule from the external internet IP or IP address range to the internal IP address (within the previously created Org VDC Network).

- Go to the “Firewall” tab and create the desired firewall rules for the incoming connections (e.g. allow port 80 for HTTP to the internet IP address) as well as the outgoing connections (e.g. from all internal to all external IP addresses).
- Afterwards the customer can deploy a virtual machine within the Internet Access enabled vOrg VDC Network and user outbount internet access, respectively configure appropriate internet facing services within the virtual machine.

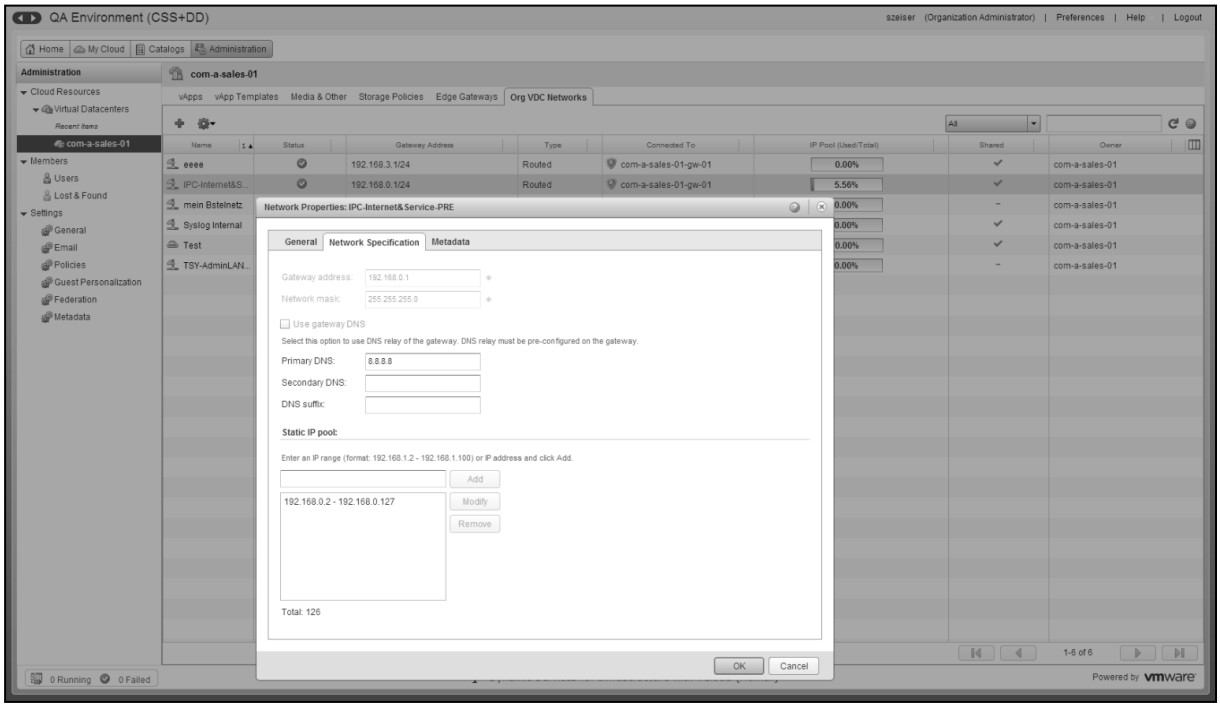


Figure 20: Example of a vOrg VDC Network

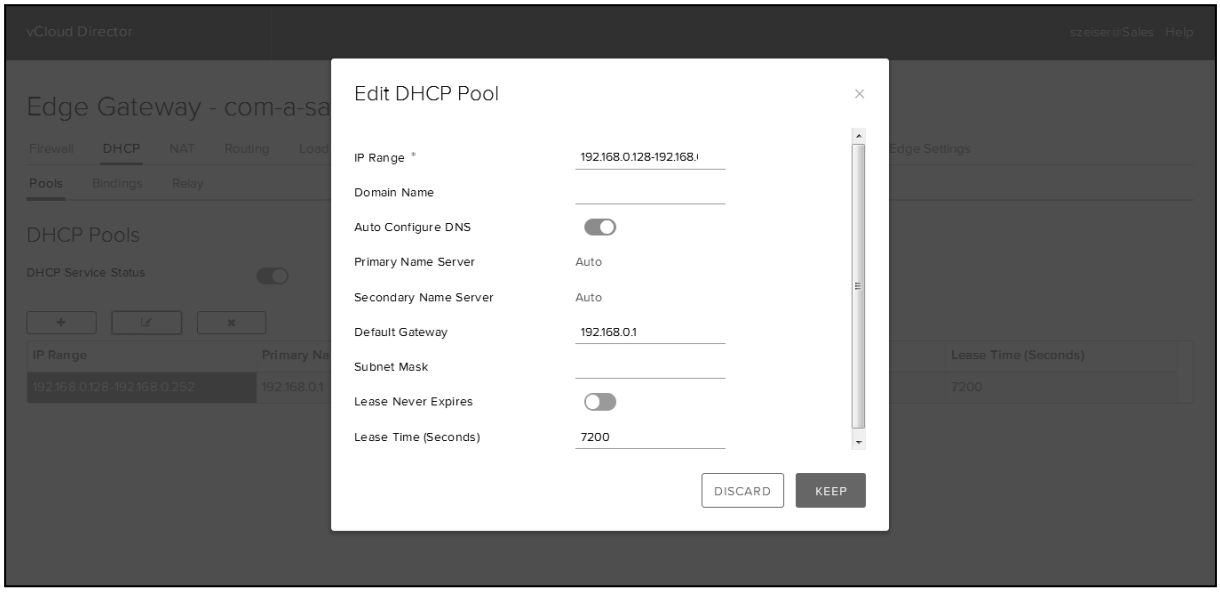


Figure 21: DHCP configuration example

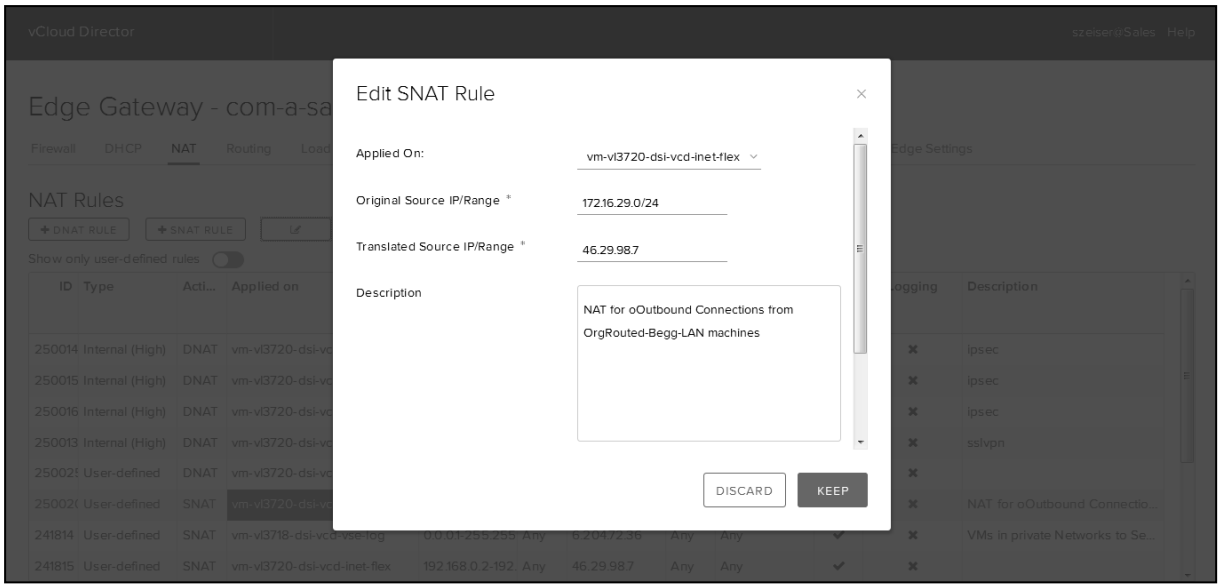


Figure 22: Example of a SNAT rule

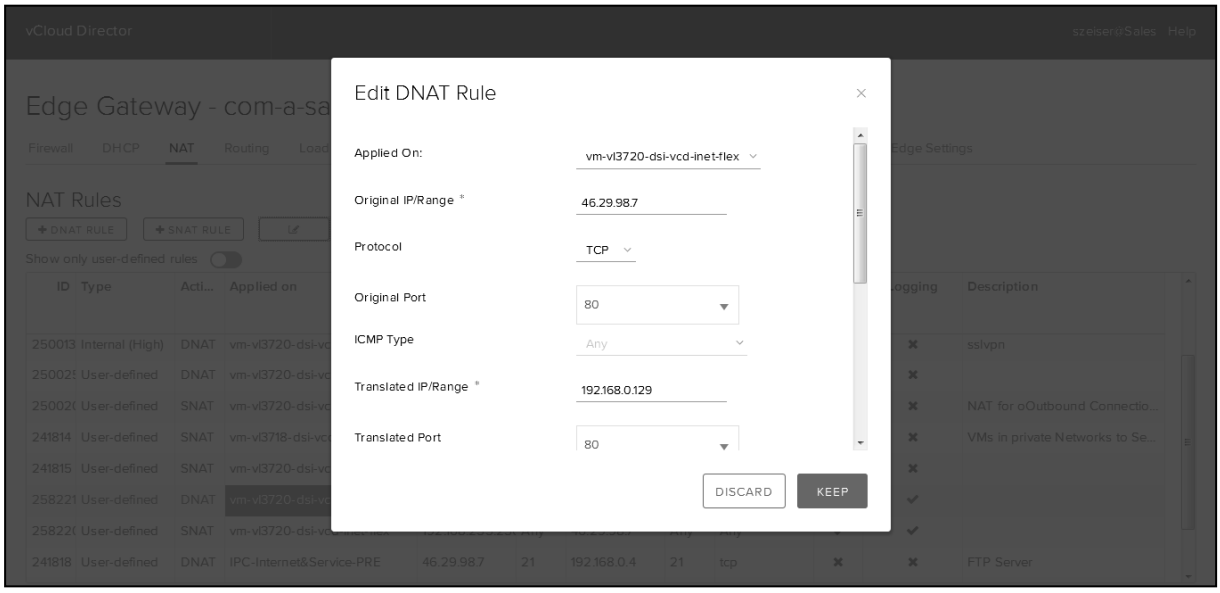


Figure 23: Example of a DNAT rule

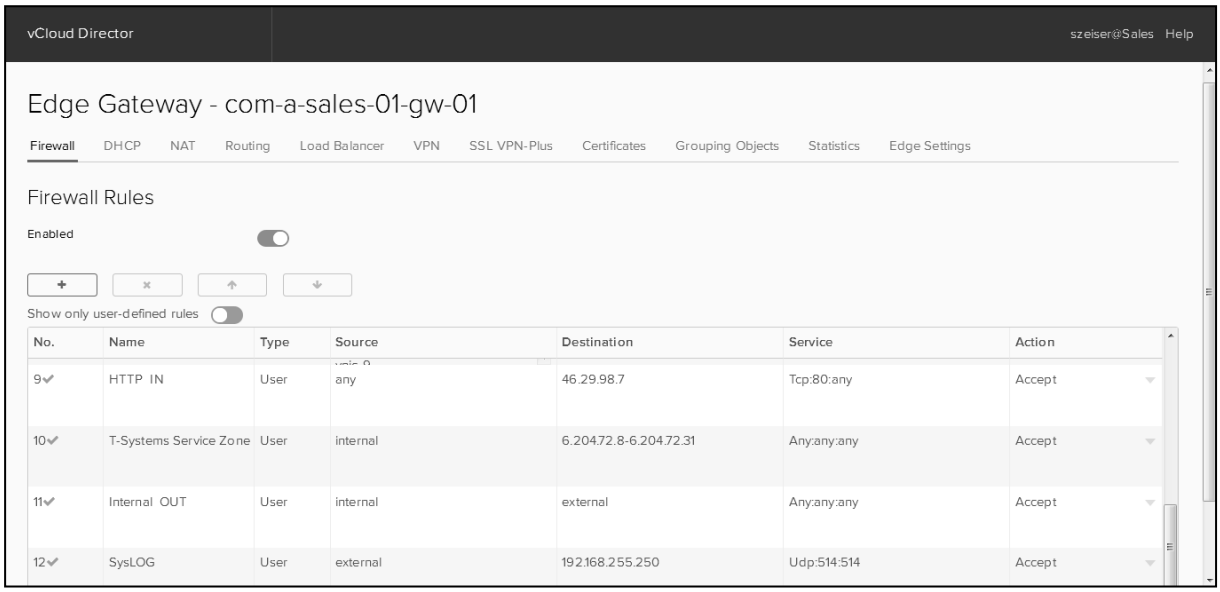


Figure 24: Example of firewall rules

14.7. HOW TO INITIATE A L2VPN CONNECTION

1. Create a vOrg network as "Create as subinterface"

Create a new vOrg network which should be extended to the vCloud. It is important to select the item "Create as sub-interface" so that the network appears later in the VPN configuration.

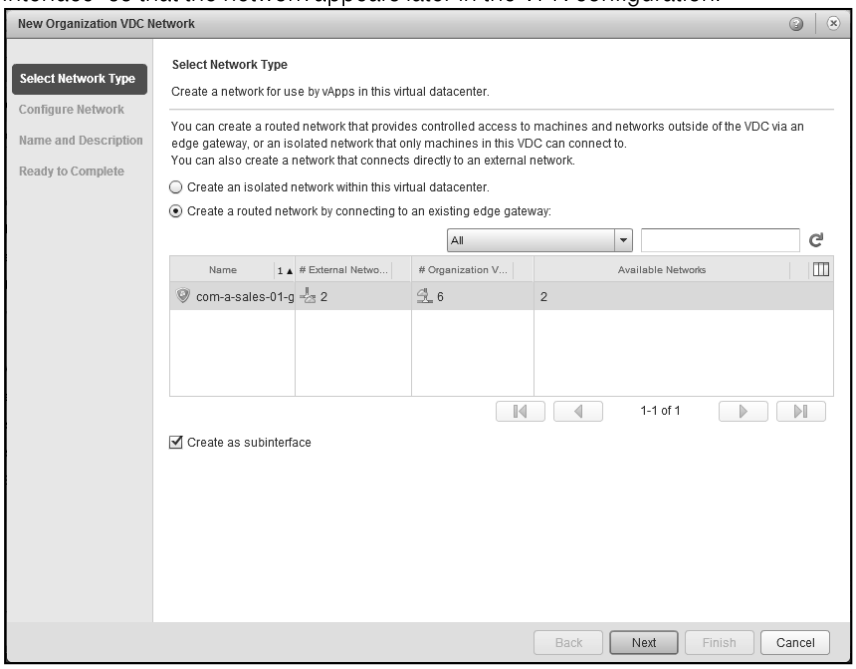


Figure 25: Create vOrg network

- Set network parameters

Note: The gateway address may not be the same as the gateway address on the customer side.

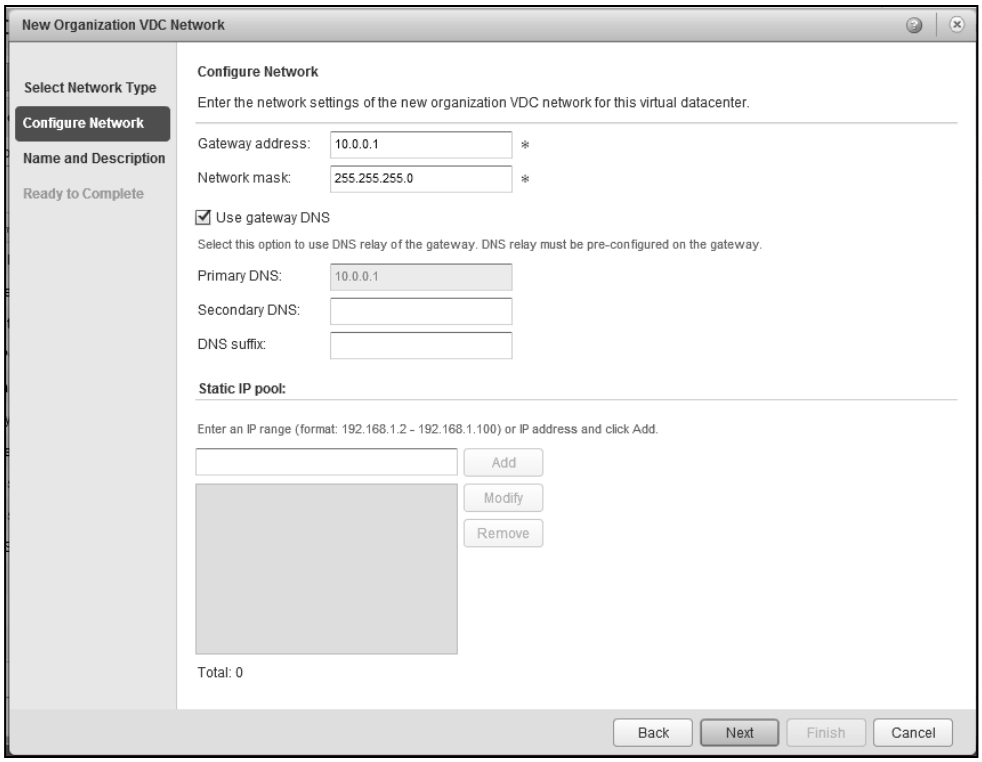


Figure 26: Configure network settings

2. Tenant portal client configuration

Select VPN and L2-VPN in the Tenant Portal and enter the following parameters.
If vCloud was **defined as a client**.

- Select client
- Enter server address (external IP of the gateway on the customer side)
- Enter the service port defined on the customer side.
- Select encryption algorithm defined on the customer side.
- Select subinterface (referenced on the Orgnetz, which was defined in the first step)
- Enter the user and password defined on the customer side.
- Apply all settings

Figure 27: define client settings

The “statistic” tab shows the status of the tunnel.

Figure 28: Statistics

3. Tenant portal server configuration

If vCloud has been defined **as a server** define the following parameters:

- Select external IP (Listener IP)
- Define listener port
- Define encryption

Figure 29: L2VPN server configuration 1

Add **server site** configuration:

- Set name
- Define user and password
- Select sub interface

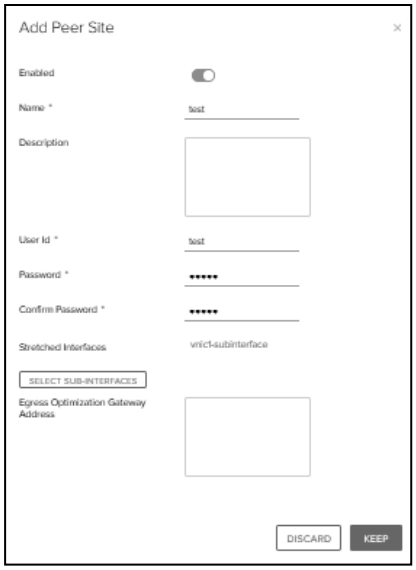


Figure 30: L2VPN server configuration 2

After the configuration has been completed, the tunnel must be given the status "UP". For communication between the VMs, you may need to define firewall rules on both sides.

Note: This https://kb.vmware.com/s/article/2150142 shows you the VMware supported L2VPN versions

14.8. HOW TO INITIATE A SSLVPN CONNECTION

SSL VPN is one-way client communication (roadwarrior) to vCloud (connection from server to client not possible). In the edge service gateway, you can create an SSL VPN in self-service. You can reach this function under the tab SSL VPN Plus.

1. Set the following general Settings

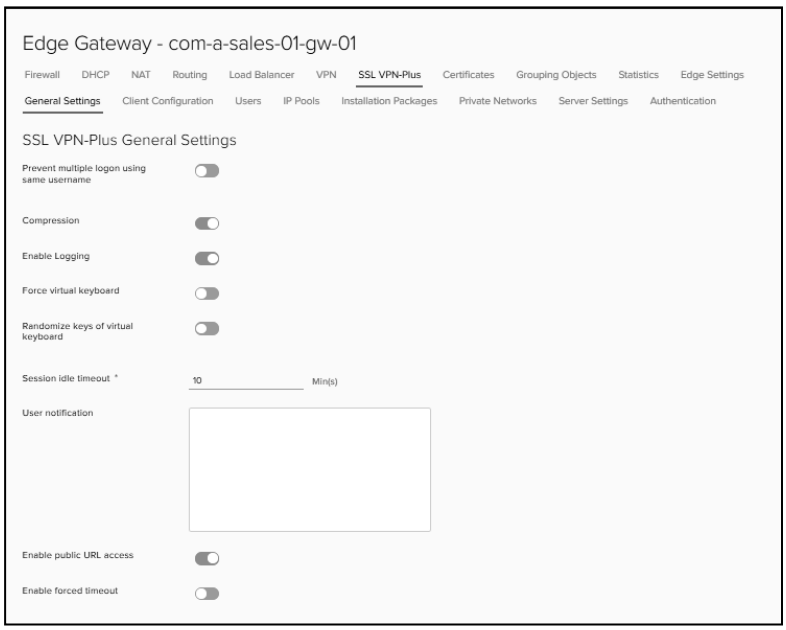


Figure 31: SSL VPN general configuration

2. Setup of the Tunneling mode

The Tunneling Mode refers always to the client. It defines whether everything should be routed via VPN or only the traffic to the connected network.

Figure 32: SSL VPN client configuration

3. Create a user (note that this is not a user but a user for the VPN client).

Please check the example user in the screen below: vpnuser.

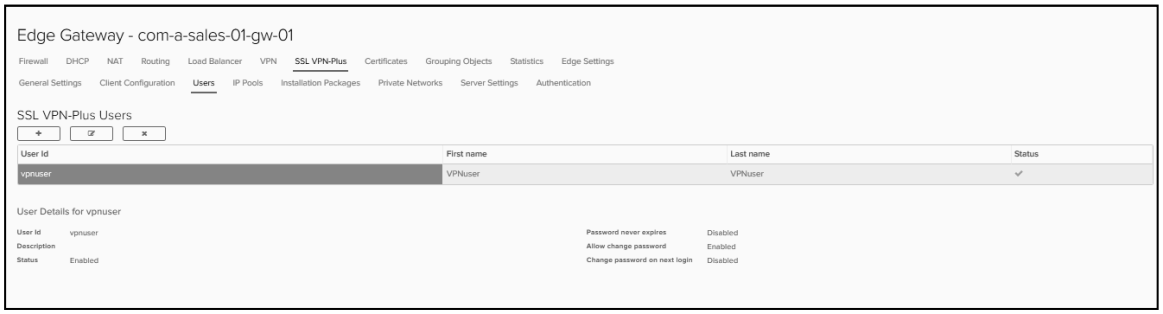


Figure 33: SSL VPN user configuration

4. Create an IP pool for the VPN client.

Note: Do not use the same network as the destination network.

Figure 34: SSL VPN IP Pools

5. Create a client package

The Gateway IP address is the external IP of the Edge Gateway Service + Port which must also be used in the server configuration.

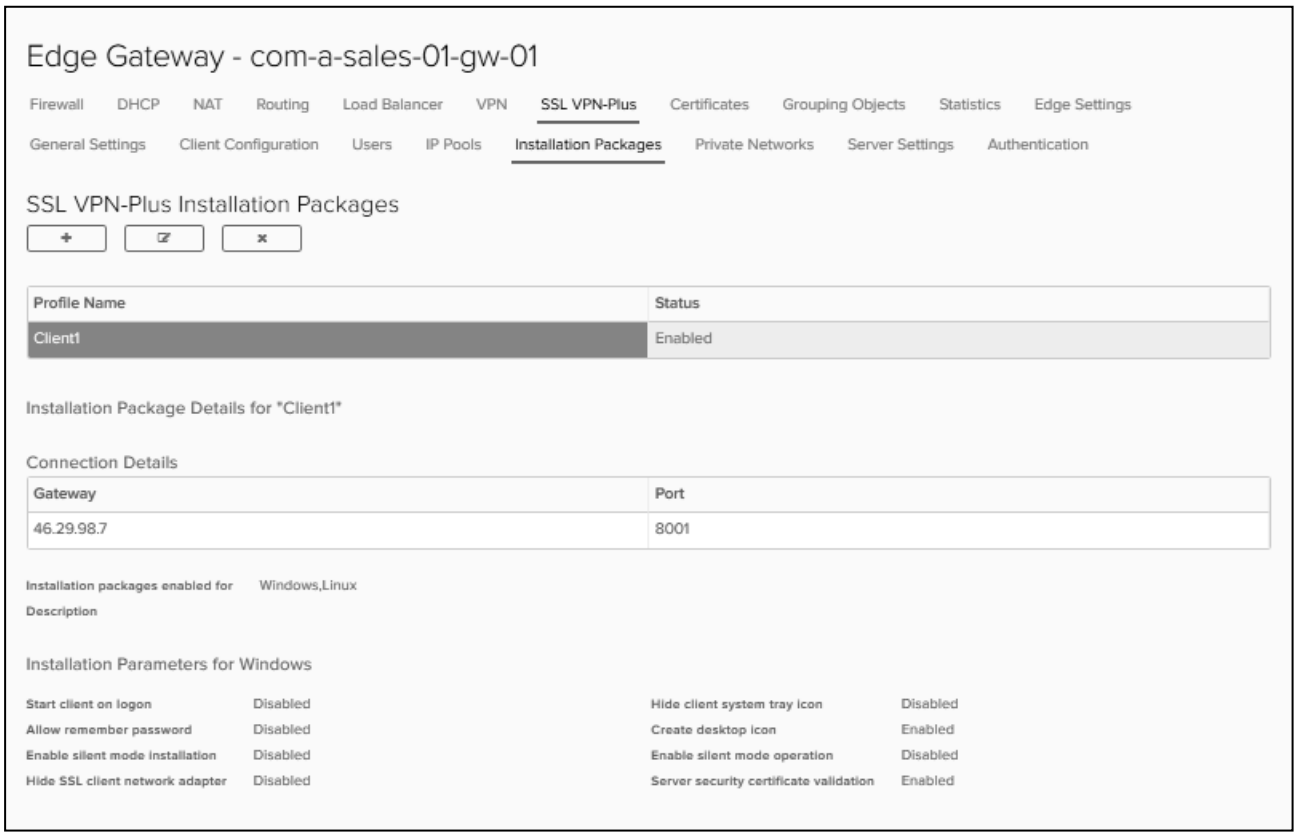


Figure 35: SSL VPN Installation Packages

6. Specify the internal vOrg network or IP on which the VPN client should be granted access

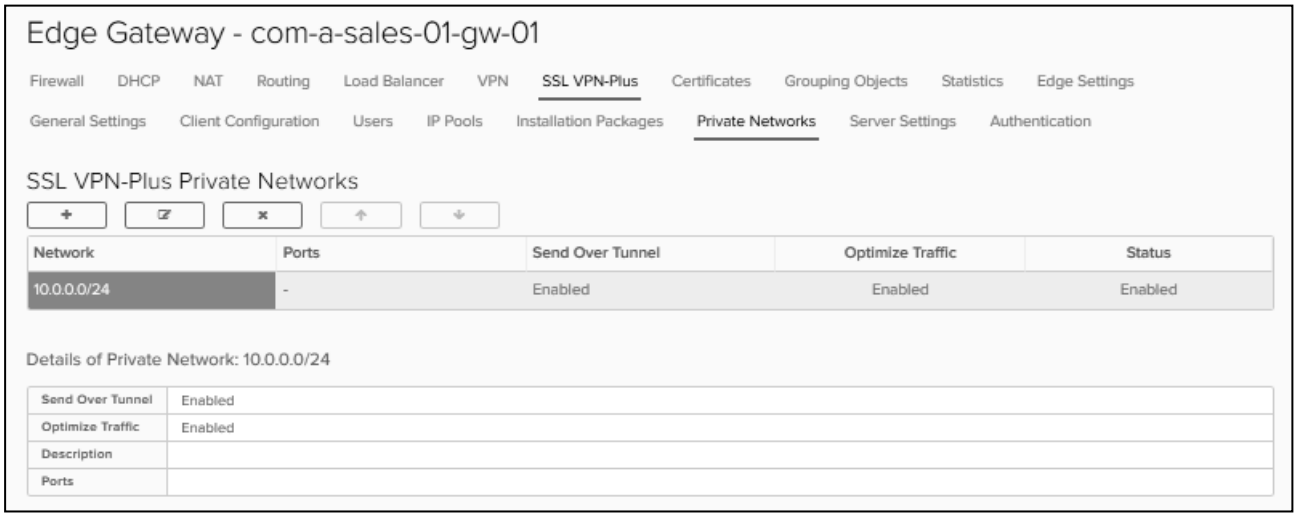


Figure 36: SSL VPN Private Network

7. Create server configuration

Select ext IP of the Edge Gateway service and define port (a firewall rule will automatically be created).

Figure 37: SSL VPN Server Settings

8. Configuration of the authentication server

Navigate to the Authentication tab and set the following configurations.

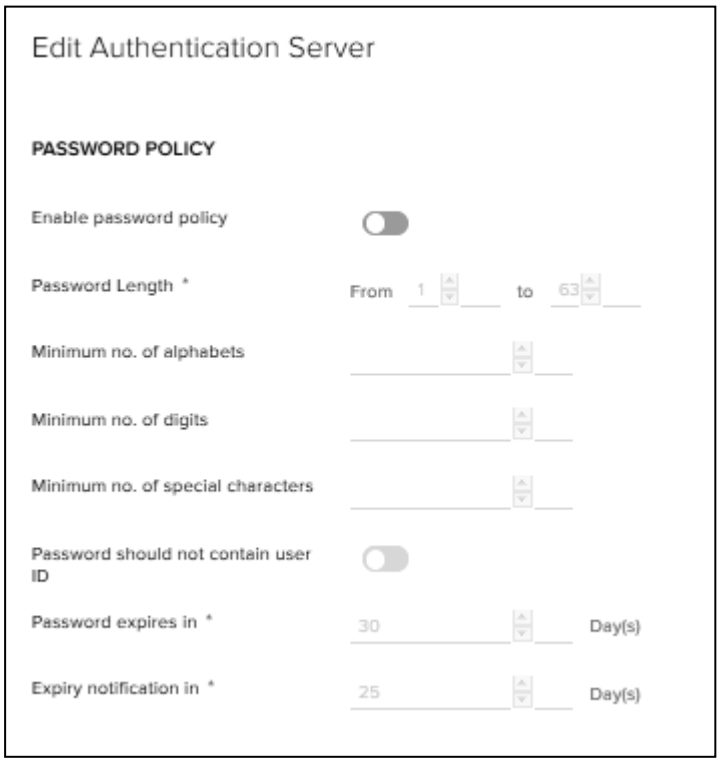


Figure 38: SSL VPN Authentication Settings 1

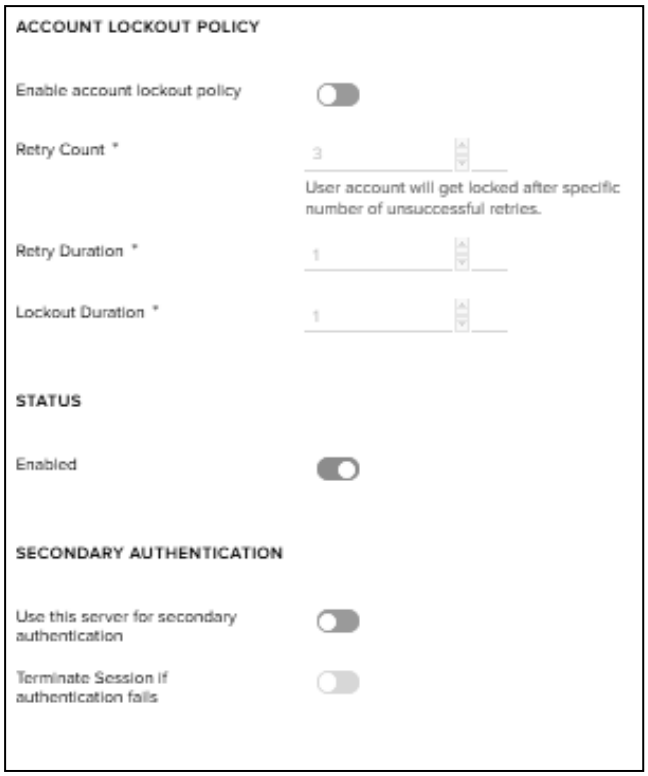


Figure 39: SSL VPN Authentication Settings 2

9. Download the VPN client

- Use the external IP address + Port of the Edge Service Gateway which was previously selected.

For example https://46.x.x.x: 8001

- Log in with the defined vpnuser

- download VPN client and install.

- The client is installed under C: \ Program Files (x86) \ VMware \ SSL VPN-Plus Client.
- Connect via icon in the tray (start bar)

•

Note: The Firewall rules for the SSL VPN is created automatically on the Edge Service Gateway.

14.9. HOW TO UP-&DOWNLOAD TEMPLATES (E.G. OVA, OVF AND ISO) VIA COMMAND LINE INTERFACE

In addition to the up- and download functionality via the self-service portal it is also possible to use the VMware ovftool on command line. This tools is automatically installed as part of the client integration plug-in and can be found in a respective sub-folder named “ovftool”.

VMware regularly releases new versions of the ovftool on their website. If you are facing issues we recommend to update to the latest version from the VMware homepage.

For detailed information on how to use the ovftool please have a look at the VMware user guide https://www.vmware.com/support/developer/ovf/

Note: When uploading larger files (more than 500 MB), we recommend uploading with the Command Line Interface.

Examples:

Upload a local ISO-file to vCloud catalog:

ovftool –sourceType="ISO" –X:logToConsole –X:logLevel=verbose *file* "vcloud://*username*:*password*@vcloud-muc.t-systems.de:443?org=*vOrg-name*&vdc=*vDC-name*&media=media-*name*&catalog=*catalog-name*"

Upload a local OVF-files to vCloud catalog:

ovftool –X:logToConsole –X:logLevel=verbose *file* "vcloud://*username*:*password*@vcloud-muc.t-systems.de:443?org=*vOrg-name*&vdc=*vDC-name*&vappTemplate=template-name&catalog=*catalog-name*"

Download a template from vCloud catalog as OVF-files:

ovftool –acceptAllEulas –X:logToConsole –X:logLevel=verbose "vcloud://*username*:*password*@vcloud-muc.t-systems.de:443?org=*vOrg-name*&vdc=*vDC-name*&vappTemplate=template-name&catalog=*catalog-name*" *file*

Downloads are done in a two step approach:
1. Export, conversion and compression of the vAPP vCloud internally to a transfer share
2. Download of the OVF file over the external network

Depending on the vApp size the export can take several hours and the ovftool might run into a time out.

Therefore we recommend to set the following time out parameters within the ovftool command. The parameters set the time out values to 24 hours:
–X:vCloudTimeout=86400

–X:vCloudKeepAliveTimeout=1440

Uploads are also done in a two steps approach:

1. Upload to transfer share
2. Import in vCloud

After the upload of each file (e.g. VMDKs) the SHA1-checksum is calculated and verified against the manifest file (.mf). For large files this checksum calculation may take very long and therefore lead to a timeout situation and error message in the ovftool.

Therefore we recommend to set the following parameter within the ovftool command if larger files should be uploaded:

–X:skipManifestCheck

Remarks

– = two hyphens, without a blank in between.
file = path and name of file, e.g. c:\xxx\centOS.iso or c:\xxx\centOS.ova

username = vCloud username, e.g. administrator

password = vCloud password for respective user

vOrg-name = vORG, e.g. xxx_10000876

vDC-name = vDC-name, e.g. com-a-xxx_10000876-01

media-name = name that should be used within the catalog for that file. Name must not exist for upload.

template-name = name that should be used within the catalog for that template. Name must not exist for upload.

catalog-name = name of catalog within vCloud, where the file should be stored or downloaded from. Catalog has to exist.

Important note: there is currently a known bug in OVF tool 4.3.0 and below, that causes a HTTP400 error when trying to upload OVF/OVA-files or ISO-images to DSI vCloud. This bug will be solved with OVF tool version 4.3.1. Until this is available, please add the following switch to your commands: –X:skipContentLength

14.10. HOW TO REQUEST A CUSTOMER DRIVEN PENETRATION TEST

A penetration test carried out by the customer must be officially displayed at T-Systems at least 4 weeks before the execution. T-Systems checks this requirement and reserves the right to refuse the test.

Please send your request for further instructions to: FMB DD-Cloud-SDM

14.11. HOW TO SOLVE PERFORMANCE ISSUES

If you are facing performance issues with a single VM or a vAPP, please check the following parameters, before opening a support ticket:

1. Ensure that latest version of VMware tools or OpenVM tools is installed within the guest operating system (for VMware tools: take the version that can be directly downloaded from VMware, as this might be already newer as the minimum version offered in the platform)
2. Ensure that your VM is running on the latest virtual hardware version that is offered from the platform.
3. Ensure that you have the latest updates for your guest operating system installed.
4. Ensure that VMs with the same load profile (e.g. webservers serving behind a loadbalancer) are distributed to different hosts by using vCloud Director Anti-Affinity Rules (it doesn't make sense to loadbalance in the frontend by having worst case all VMs on the same physical host).
5. Check that you have enough PU, RAM and storage capacity within your vDC available if you are using Committed or Dedicated vDCs.
6. If you are facing performance issues with compute performance (PU) ensure that the PUs (Ghz) available in your vDC are really deployed (vCPUs used) by increasing the vCPU speed (Ghz) in your vDC. Just having spare capacity in the vDC available will allow you to deploy additional vCPUs, but it will not really help the vCPUs that are already deployed to get more performance reserved.
7. Check performance statistics within the guest operating system and add additional vCPUs, RAM or storage to your VM if necessary.
8. If you are facing storage performance issues, check that the choosen storage class fullfills your IOPS demands and if necessary move your VM to a higher storage class (e.g. from Disk Storage normal to Disk Storage Very High)
9. If you are still facing storage performance issues, ensure that your disk layout is set up according VMware best practices – e.g. using dynamic disks in Windows is not recommended as it is known to cause performance issues in viruatlized environments.
10. If you are facing network performance issues, ensure that your network adapters are configured according the VMware best practices, e.g. use network adapter type VMXNET3.

15. GENERAL DSI VCLOUD LIMITATIONS AND CONFIGURATION REQUIREMENTS

Please consider the following limits within DSI vCloud:

Max number of vCPUs per VM	40
Max RAM per VM	For Basic / Committed vDC: 326 GB RAM For Performance Optimized vDC: 920 GB RAM
Max storage size of a VM	10 TB

Max storage size of a VM to be backed up with BaaS	1 TB or 4 TB (depending on chosen policy)
Max number of disks displayed in the BIOS*	8
Minimum virtual HW version	9 (Security relevant, due to Intel vulnerabilities)
Recommended virtual HW version	13
Min SCSI time out value **	180 seconds
Nested Virtualization ***	May encounter significant performance limitations (See notes below)
Managed Firewall Throughput (per slice)	Up to 30 Mbit/s
Managed Firewall VPN throughput (per slice)	Up to 2 Mbit/s
Managed Firewall concurrent session (per slice)	Up to 1,000 sessions

Table 7 General limits

* If you have more than 8 disks, some disks will not be visible in the BIOS and your boot drive may jump to last in the list and become "invisible" in the BIOS. In these cases, the only way to set the correct boot order is to manually force the correct drive in VMware configuration files.

** In order to cope with potential storage time outs (e.g. during failover) the SCSI time out values must be adjusted to 180 seconds. By installing and using the native VMware Tools, the value is adjusted automatically. When using Open VM-Tools, the value must be adjusted manually in the appropriate udev rules. More details can be found in the following VMware https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1009465.

*** Nested Virtualization is not recommended on DSI vCloud due to performance limitations introduced by security specific configuration. T-Systems has implemented Hypervisor-Specific mitigations for Machine Check Error on Page Size Change (MCEPSC) Speculative-Execution vulnerability which is known to cause performance degradation to workloads running nested virtualization such as Microsoft Hyper-V or Nested ESXi. More details are outlined in VMware Knowledge Base Article (https://kb.vmware.com/s/article/76050).

Please consider the following limits for the vCloud Availability Service:

Maximum Size of Protected VM	10 TB
Maximum number of simultaneous operations (Protect, Test Failover, Reverse Protect, Test Failback, and Failback)	20

Table 8 vCloud Availability limits

16. FURTHER SUPPORT AND CONSULTING

If the customer needs further assistance, Telekom offers the required consulting services on a hourly basis. For further information the customer is advised to either get in contact with their Service Delivery Manager or lookup the available information online:

https://cloud.telekom.de/

17. DSI VCLOUD GLOSSARY

Abbreviation	Explanation
API	Application Programming Interface
BaaS	Backup as a Service
BIS	Backup Integrated Disk Storage
BYOL	Bring your own license
CPU	Central Processor Unit
DHCP	Dynamic Host Configuration Protocol
DMTF	Distributed Management Task Force
DNS	Domain Name System
DR	Disaster Recovery
DSI	Dynamic Services For Infrastructure
EXT3	third extended filesystem
EXT4	fourth extended filesystem
FFM	Frankfurt am Main
FQDN	Fully Qualified Domain Name
GB	Gigabyte
Ghz	Gigahertz
GPO	Group Policy Object
GUI	Graphical User Interface
HTML	Hypertext Mark-up Language
ID	Identifier
IP	Internet Protocol
KMS	Key Management Service
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LVM	Logical Volume Manager
MPIT	Multiple Point-in-Time Snapshots
NAT	Network Adress Translation
NIC	Network Interface Card
NTFS	New Technology File System
OS	Operating Systems
OU	Organizational Unit
OVF/OVA	Open Virtualization Format
PU	Performance Unit
RAM	Random Access Memory
REST	Representational State Transfer

RHEL	RedHat Enterprise Linux
SAML	Secure Assertion Markup Language
SNAT	Secure Network Adress Translation
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
tpmC	Transactions Per Minute, Type C
UDP	User Datagram Protocol
URL	Uniform Resource Locator
vApp	Virtual Application
vCAV	vCloud Availability
vCC	vCloud Connector
vDC	Virtual Data Centre
VIP	Virtual IP address
VM	Virtual Machine
VMDK	Virtual Machine Disk
VMRC	VM Remote Console
vOrg	virtual Organisation
VxLAN	Virtual Extensible Local Area Network
WSUS	Windows Server Update Service
vOrg	Virtual Organisation

Table 9 Glossary