Solution domain

Frequently Asked Questions (FAQ) vContainer

Date	19/12/2014
Sensitivity	Confidential
E-mail	Click here to enter text.

Table of contents

1. Introduction

This document describes the Frequently Asked Questions (FAQ) in configuring and using the Proximus Cloud vContainer solution. For the start up and generic configurations, please refer to the vContainer User Manual. Specific questions related to the Network and Security aspects are covered in the Network and Security Whitepaper.

2. Accessing vCloud Interface

The access to the vContainer management Web Inteface is currently allowed from any ip address.

The web interfaces uses Java and Adobe Flash Player installed on your local computer. Since Java 7 update 51 (released on Jan 14 2014), Oracle/SUN has increased the security features. As a result a lot of websites and applications may possibly not work correctly, including the vContainer web interface.

To ensure the correct functioning of several components of the web interface (Image and ISO upload for example) Proximus encourages the customers to add an exception to their Java security:

1. Open the Java Control Panel.
2. Click the Security tab.
3. Click Edit Site List and add the address of the product in this format: https://FQDN

Include the port number if required, for example: https://FQDN:port

Afterwards close and reopen all browser sessions.

The webinterface is tested and is working correctly with IE versions up to 9 (for higher IE versions use compatibility mode), Firefox version 34.0 and Google Chrome 39.0. Linux or MAC operating systems with other browser types are untested and not guaranteed to always work correctly.

3. Working with VMs

You can deploy a pre-installed template with Microsoft Windows 2008R2, 2012, 2012R2 or CentOs 5.5. This delivers you a fully working Virtual Machine (VM) within 5 to 10 minutes. The default Administrator password for the Windows templates is 'Belgacom1'. Proximus encourages the use of 'Guest OS Customization' (also known as Sysprep) to change the system SID and administrator password at the first boot of the VM.

There is no root password on the CentOS template. You should boot it into runlevel 1 (single mode) and specify a root password during the first boot.

It is also possible to choose the 'new virtual machine' option when creating a VM. This option will not deploy a template but it creates an empty machine with the specified settings. You can then attach an ISO to the VM (either from the public media files or from your own uploaded catalog) and follow the OS installation setup. Available ISO files from the public catalog include Windows 2008R2, Windows 2012, Windows 2012R2 and CentOs 6.5.

4. Backup and Restore

We will discuss following subjects

1. **Setup** : How are backups taken
2. **Restoring VM's** : How are restores handeld
3. **Startup problems** : Problems starting VM's after restore

4.1 Setup : How are backups taken

The backups of the vContainer platform are taken through a storage proxy server and use a deduplication process. This means that only the changed blocks of the data since last backup will be backupped. For this reason there could be a slight impact on performance of a VM during backup hours. The backup process starts every day at 20h00 Belgian time and runs untill finished. No specific backup times can be configured for individual machines

To ensure a consistent backup, a snapshot of the virtual machine is taken before the backup starts. If your operating system supports snapshotting (vss) and vmtools are installed, vmtools will inform the OS to go into snapshot mode. This mechanism will ensure the most consistent backup possible. After the backup is done the snapshot will be deleted.

4.2 Restoring VMs

Due to the nature of how backups are taken, as explained here above, it is only suited for total disaster recovery. No individual file restores can be done, only full VM restores, which, depending on the size, will take some time. There is no SLA given on restore time, only on the start of the restore.

It is therefore advised to deploy your own file-based backup solution for critical files or databases to ensure fast business recovery times.

Any request for a restore is handled as standard change (RFC) and will be executed within maximum 3 business days. You can send a email to ict-servicedesk@Proximus.com, call 0800 14 888 or use your esupport portal to register a restore request. Please indicate clearly the name of the VM to be restored and from which date the restore should be. Backups are stored on the Proximus infrastructure for 28 days.

VM restores are completed to your vContainer and can be added to a vApp of your choice.

After this you would need to adapt the network settings, else it is possible that the VM won't start due to a duplicate ip.

Important remarks :

- It is your responsability to have enough resources (CPU, mem, disk) in your vContainer to accomodate a restore.
- Proximus is not responsible for corrupt files/databases when restoring virtual machines !

4.3 Problems starting restored VM

After the restore process is completed, it is possible that your restored VM doesn't start.

This is the case when the original machine is still present. This is because the VM is restored as it was including all details: the mac address and ip addres are the same.

Before atempting to boot your VM, edit your machine first and delete your network adaptor, then add a new one together with a new ip. (or reset it's mac address and change the ip).

5. Email

Proximus offers a shared mail relay platform that you can use to relay outgoing mail coming from your vContainer. Customers are not obliged to use it. Customers may use their own or any other 3rd party email relay service.

You need to open a change request to request access to this relay service.

Then you can configure 'vcrelay.belbone.be' as your outgoing email server, on port 25.

This are the restrictions on the mailrelay platform:

- max concurrent connections from one source ip : 3
- max connection/timeframe : 100
- max messages/timeframe : 500
- max recipients/timeframe : 1500
- Timeframe : 5min

Proximus can revoke your access to this relay service without prior notice at any time if misuse is detected!

Please make sure to adapt your vShield Edge firewall when using the shared vContainer email relay platform from a VM behind a routed network!

Instructions can be found in the vContainer manual.

6. Functionality

We will discuss following subjects

1. Console access
2. Web Interface Language
3. Federation certificate

6.1 Console access

To access the console of your virtual machines through the webinterface, your browser requires a plugin.

This plugin works with IE 7, 8, 9. Make sure you have enough permissions on your computer to install the plugin, called VMRC (VMWare Remote Console). For higher IE versions, you can try to run the webpage in IE compatibility mode.

There can be several reasons why the VMRC is not connecting:

- Incompatible version of Adobe Flash Player. Currently, vContainer interface requires the 32-bit version of Adobe Flash Player 10.2 or later.
- Incompatible version of Java. Currently vContainer clients must have JRE 1.6.0 update 10 or later installed and enabled. Only the 32-bit version is supported. See the note about Java 7 Update 51 above in chapter 2.
- Firewall Rules restricting console traffic. Ensure that port 443 outbound is open for VMRC connections.

NOTE : Other browsers are working but some might lack functionality.

6.2 Web Interface Language

The vContainer management interface language is automatically detected and uses your brower's default language settings. Please consult the manual of your browser to change your preferred language. If your language is not available it will be English per default.

NOTE : You cannot overwrite this in the web interface.

6.3 Federation Certificate

With the creation of your vContainer, a federation certificate will be generated automatically.

It will expire in 1 year : you will receive a warning that it will expire. You will need to renew the certificate before the end of term, else access to the user interface will be denied.

If you are not using your own active directory authentication for login to the vContainer user inferface you can safely ignore this message.

7. Limitations

There are some limitations to the vContainer platform.

CPU: Currently we are only allowing a maximum of 24 vCPUs in one machine, Proximus recommends starting a VM with 1 vCPU and adding where the need rises. More vCPUs does not necessary mean better performance.

vCPU Speed: The vCPU speed of 1 or 2 GHz in your vContainer defines what a virtual machine with one vCPU will consume at maximum when running within your VDC at 100% CPU usage in worst case. The operating system you install might report the real speed of the physical CPUs of the vContainer platform (which is 2.2GHz).

The number of vCPUs multiplied by the vCPU speed allocated to your vContainer defines the upper limit of CPU GHz of your vContainer. This means for example the following in a vContainer with 10x CPU and 1GHz vCPU speed:

- You can in total allocate 10 vCPUs to virtual machines. Either 1 machine with all vCPUs, or 10 machines with each one vCPU (not taken into account the overhead).
- A machine with one vCPU will be able to consume the physical 2.2Ghz clockspeed, as long as the total consumation of your vContainer does not exceed 10Ghz (10 vCPU multiplied by 1GHz vCPU speed). When four machines with each one vCPU are already running at 100% CPU load, the total consumation of the vContainer will be 4*2.2GHz = 8.8GHz. As starting a fifth machine with load 100% would exceed the maximum vContainer allocation of 10GHz (5*2.2GHz=11GHz), each machine will be throttled down to +-2GHz so the total consumation will not exceed the 10GHz limit.
- A machine with 10 vCPUs and loaded at 100% will consume 1GHz per vCPU, as it's total consumation cannot exceed 10GHz.

All this means that the 1 or 2 GHz vCPU speed assigned to your vContainer will only the **worst case allocation** if all the resources are being actively used.

Memory: A maximum of 128 GB per VM will be allowed. For every Gigabyte of memory assigned to a VM, the same amount will be consumed in diskspace too. So a VM with 100 GB diskspace and 32 GB memory will consume 132 GB of diskspace from your allocated storage profile. The note that more does not necessary mean betters is also applicable here!

Storage: A maximum of 1,8 TB per VM can be allocated. VMs cannot use multiple storage profiles at the same time. You can however migrate an entire VM to another storage profiles while it is running. You can do this by changing the 'storage profile' dropdown box on the General tab of the VM properties window.

Networking: A maximum of 10 NICs can be added to a VM. This also applies to the Edge Gateway appliance. Proximus encourages the use of the 'VMXNET3' network adapter type.

8. Networking

We will explain the different network configurations and options

1. Direct connect network
2. Vapp network
3. Organizational network (Routed network)
4. Vmxnet3 Adaptor

8.1 Direct Connect

The direct connect network is referred to as 'external network' in the manual or setup documentation. This is in the range of 10.190.*.*. You cannot change or delete this network!

Any public ip is NATed (both in- and outgoing) to an IP of this direct connect network. You can find the specific NATing in your vContainer setup documentation.

This NAT on the Proximus managed firewall can be modified by creating a change request.

8.2 Vapp network

A vApp network is similar to the (routed) organisational network, but with limited functionallity.

This network will be started when you start your vapp en will stop when the vapp stops.

You cannot use this network to connect multiple vapps because it is limited to one vapp.

Proximus does not recommend the use of this kind of network for throughput or high session VMs, because the underlying technology is limited in resources. It is however very well suited for backend HA links between VMs in the same vApp.

8.3 Organizational network

This is a private network that is routed behind the Edge Gateway device.

You can create up to 9 of these networks on one edge. A second edge needs to be deployed by Proximus if you plan to use more than 9 organisation networks.

If you want to access VMs that are in this network, you will need to configure natting and the firewall on the edge gateway device. Please make sure to select your direct connect network in the 'Apply To' dropdown box when creating any SNAT or DNAT rule!

You also need this kind of network when you want to configure a site 2 site vpn.

This kind of network allows you to have the most flexibility as you can manage firewall rules yourself.

8.4 Vmxnet3 Adaptor

There are many types of network adaptors available for your VM. Proximus recommends to use the latest vmxnet3 adaptors. Networking problems are possible when using other adaptors than this one.

All Proximus templates use these vmxnet3 nics.

9. Windows Activation

You can consult the vContainer manual for a step by step overview of activating your Windows operating system. All supported activation keys are also listed.

When using the vContainer Edge gateway, please make sure you add a correct SNAT and firewall rule to allow your machines to communicate with the Proximus KMS activation server. These rules must remain in place during the whole lifetime of a VM! It is essential that your servers can remain in contact with the activation server at all times, otherwise your VM can become unlicenced again!

10. Vcloud connector (vCC)

Anything that is not in this FAQ can be found in the install or user manual of vmware.

http://www.vmware.com/products/datacenter-virtualization/vcloudconnector/overview.html

You require to have a vcenter and a vCC-Server. The vcenter doesn't need to contain anything, it is just needed for the connectivity and the functions. If you see any fault or point of improvement please fill in the feedback form.

10.1 Connector server

In the current setup only connector 2.6 is supported and vcenter 5.0 or higher.

Deploy the vCC-Server ovf in your vcontainer. It is available in the public catalog. If you have your own vcenter you can deploy the vCC-Server there also. Then register the deployed vCC-Server in your vcenter.

NOTE : ! Please make sure all the required ports are open(your site and connection to our nodes) ! We do not offer support on onsite servers !

10.2 Install vCloud Connector Server in vcontainer

Procedure :

1. Log in to your vContainer.

2. Deploy the vcc server from the public catalog.

3. Proceed through the wizard. You can either use the Networking step in the wizard to set basic network properties or you can wait and set those properties when you configure your server.

4. Power on the vCC Server.

5. Take a note of the ipsettings of your vcc server, you will need this to register it in vcenter

10.3 Configure Vcloud Connector Server

Surf to https://ipofvcloudserver:5480 and login with 'admin' and password 'vmware'

Set the correct time zone in the systems tab.

Make sure you have a primary and alternate dns server configured.

10.4 Register vCloud Connector Nodes with vCloud Connector Server

You use the vCC Server admin Web console to register vCC Nodes

Prerequisites :

The vCC Server admin Web console interface is open. You can open this webinterface through an other server in your cloud.

Procedure

1 Click the Nodes tab.

The Manage Nodes page that opens displays the list of Nodes that are currently registered.

2 Click Register Nodes and complete the required information.

- Name : Enter a name for the cloud where the vCC Node is installed. This name is the display name in the vCC UI.
- Type : Select the type of cloud. This is a vCloud Director cloud, so use the Organization URL, such as https://cloud.company.com/cloud/org/orgid
- Public : Select if the cloud is a public cloud outside of the firewall where your vCC Server is installed.
- Use Proxy :Select if the vCC Server needs to use a proxy to reach the vCC Node you are registering.
- Ignore SSL Certificate Check
- IP Address : Type the IP address of the vCC Node to register.
- Username :Type an administrative username for the Node admin Web console. The default is admin.

- Password : Enter the password for the username: the default is vmware.

3 Click Register.

11. Vmtools

You should always install vmtools in every VM and keep them up to date.

! Without correctly running vmtools Proximus cannot guaranty a good performance and consistent backup !

12. VPNs

We will explain the different network configurations/options

12.1 Vpn to Remote Network

Points to consider when configuring VPN between a hardware based Firewall and a vShield (Edge Firewall)

12.1.1 IKE Phase 1 and Phase 2

IKE is a standard method used to arrange secure, authenticated communications.

12.1.1.1 Phase 1 Parameters

Phase 1 sets up mutual authentication of the peers, negotiates cryptographic parameters, and creates session keys.

The Phase 1 parameters used by the vShield Edge are:

- Main mode [No Aggressive Mode]
- TripleDES / AES [Configurable]
- SHA-1
- MODP group 2 (1024 bits)
- pre-shared secret [Configurable]
- SA lifetime of 28800 seconds (eight hours) with no kbytes rekeying

12.1.1.2 Phase 2 Parameters

IKE Phase 2 negotiates an IPSec tunnel by creating keying material for the IPSec tunnel to use (either by using the IKE phase one keys as a base or by performing a new key exchange).

The IKE Phase 2 parameters supported by vShield Edge are:

12.1.1.2 TripleDES / AES [Will match the Phase 1 setting]

- SHA-1 (Integrity Algorithm)
- ESP tunnel mode
- MODP* group 2 (1024 bits)
- Perfect forward secrecy for rekeying (PFS)
- SA lifetime of 3600 seconds (one hour) with no kbytes rekeying
- Selectors for all IP protocols, all ports, between the two networks, using IPv4 subnets

* More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)

Source: http://www.vmware.com/pdf/vshield_51_admin.pdf

Important: When configuring IPsec VPN between hardware based firewall and a virtual firewall (Edge/vShield) you need to take into account that as standard the local and remote IDs are being used in the Phase2 negotiation process.

Those IDs are used by Edge/vShield as standard.

For example, imagine that you have the following topology:

FW-SSG550 (public ip 1.1.1.1) <----IPsec VPN---> Edge (External private IP: 10.10.10.1)

The following has to be configured in the FW-SSG550

- Local id: 1.1.1.1
- Remote id: 10.10.10.1

The same but in the vice versa order is configured as standard in the Edge/V-Shield:

- Local id: 10.10.10.1
- Remote id: 1.1.1.1

12.2 Vpn to different vcontainer platform

Proximus only offers support when connecting to other Proximus cloud products. For example, vContainer demo and vContainer1 platform.

12.3 Vpn to other routed network on same vcloud platform

You will be required to have 2 edge gateway's, with each a routed network to begin this process.

- Give it a name
- Select the peer edge
- Select the starting network
- Select the destination network
- Unless you have multiple external networks, select for local and peer your external network
- Select and excryption protocol and shared key
- Leave the mtu at 1500
- Finished, wait a few minutes for the vpn to connect

12.4 VPN - Nat / Firewall Configuration

The following requirements must be met in order to build the tunnel:

1. The following ports must be opened:
    - IP Protocol ID 50 (ESP)
    - IP Protocol ID 51 (AH)
    - UDP port 500 (IKE)
    - UDP port 4500
2. The IP range used on the different organization networks must not overlap
3. The edge gateway must contain the correct source and destination nat rules

12.5 Vpn Tunnel Phase 1 & 2

Phase1

- Peer: host public ip address (mip)
- Local id: own public ip address
- Remote id: edge gateway private ip address
- Authentication method: Preshare-key
- Hashing/authenticatie: sha-1
- Keygroup: Diffie-Hellman group 2
- Encryption: aes-256
- Lifetime: standard (28800)

Phase2

- Protocol: esp
- Encryption: Aes-256
- Perfect Forward Secrecy: Diffie-Hellman group 5
- Authentication: sha-1
- Lifetime: standard (3600)