How to Identify the VPN URLs relevant for your Organization

Description

This article describes how to identify the VPN URLs relevant for your Organization, which are required to establish a secure client-to-site VPN connection to your Cloud Servers on the CaaS infrastructure.

Connection through a VPN is necessary in order to access or administer your virtual servers via SSH or Windows Remote Desktop (RDP) protocols using the server's private IP address.

The CloudControl UI will indicate whether Single-Factor VPN Authentication or Multi-Factor VPN Authentication is required for a given VPN URL. For further information see Introduction to Single-Factor and Multi-Factor Client-to-Site VPN Authentication.

Please refer to How to Establish a Secure VPN Connection to Access your Cloud Network and Servers for the complete set of requirements, summary of steps and links to appropriate instructions.

Prerequisites:

1. Any of your users can identify the VPN URLs relevant for your Organization but only users with the VPN role can connect to the VPN and access their Organization's cloud resources.
    a. To add the VPN Role to a user, see How to Manage the Primary Administrator User and other Sub-Administrators

Content / Solution:

1. **How to identify the VPN links relevant for your Organization**
    a. **From the Home screen, click on the Compute button, and select Support and Additional URLs from the drop-down menu:**

    b. **The Support and Additional URLs dashboard will be displayed. Click on the VPN Links tab:**

Important!

Every VPN link will have a tooltip indicating whether or not it requires **Single-factor VPN Authentication** or **Multi-factor VPN Authentication** (see Introduction to Single-Factor and Multi-Factor Client-to-Site VPN Authentication) and this applies to both of the **two** distinct types of VPN links:

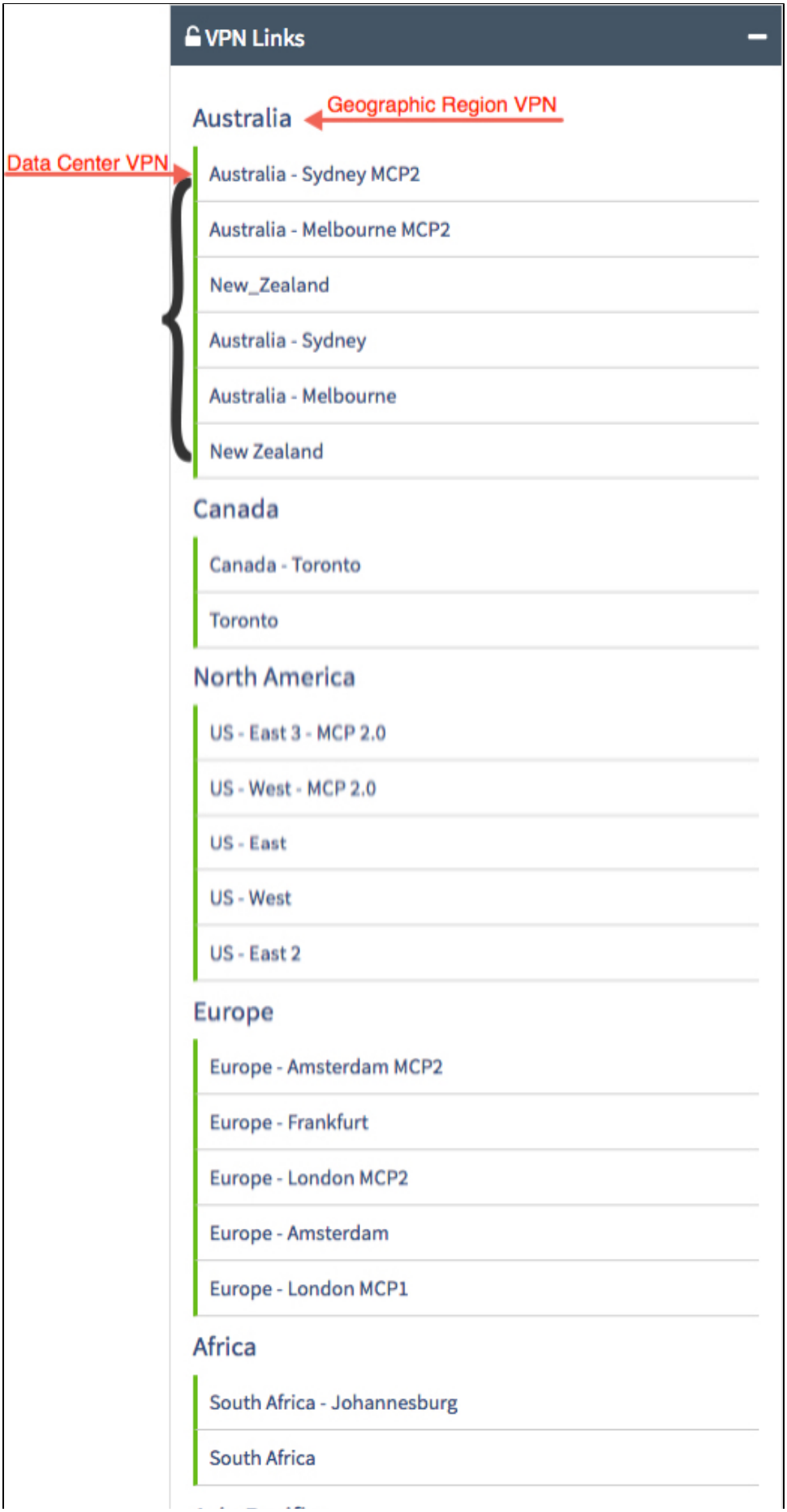
1. Geographic Region VPN

The first link with the name of the Geographic Region (in this case Australia) provides a link to the **Geographic Region VPN.** Often referred to in abbreviated form as the "Region VPN", the Geographic Region VPN connects you to all of your Cloud Network Domains/Cloud Networks in all data centers in the Geographic Region. This provides additional convenience. However, all such VPN traffic is routed through the primary data center in the Geographic Region (i.e. EU1, NA1, AU1, AP1, etc.), which reduces performance when connecting to other data center locations in the region.

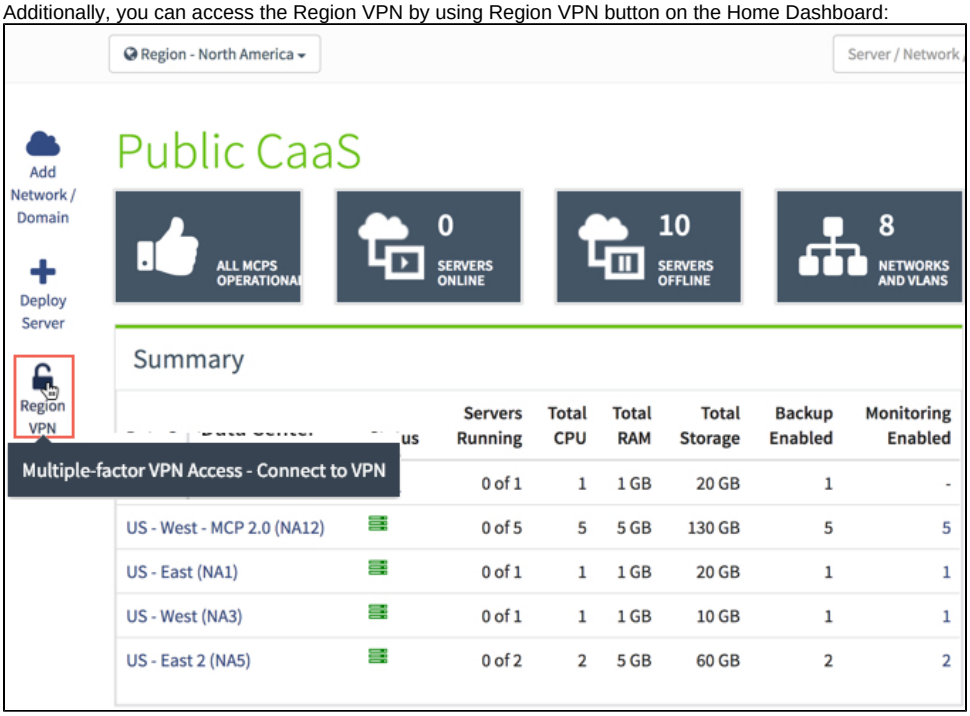
2. Data Center Location VPN

The second type of link is to the **Data Center VPN** (in this case Australia - Sydney, Australia - Melbourne etc). The Data Center VPN connects you with a secure link directly to the private IP addresses associated with the Cloud Network Domains (MCP 2.0) or Cloud Networks (MCP 1.0) in that specific data center. This provides the best link performance but requires that you switch to a different VPN if you wish to access Cloud Network Domains/Cloud Networks in a different data center location. For more information on data center locations, see Introduction to Multiple Data Center Locations in the same Geographic Region.

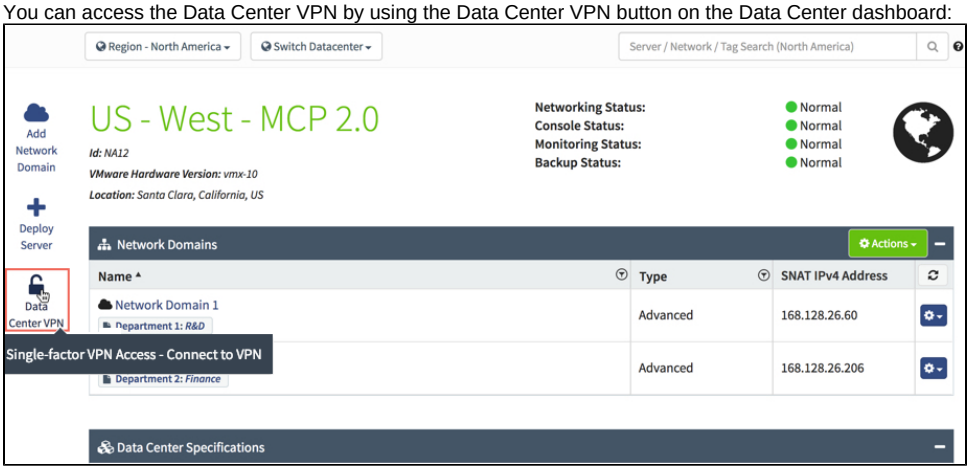
NOTES: For performance reasons, there is no "global" VPN that connects you to data center locations in different Geographic Regions.


VPN Links
Australia
Geographic Region VPN
Data Center VPN
Australia - Sydney MCP2
Australia - Melbourne MCP2
New_Zealand
Australia - Sydney
Australia - Melbourne
New Zealand
Canada
Canada - Toronto
Toronto
North America
US - East 3 - MCP 2.0
US - West - MCP 2.0
US - East
US - West
US - East 2
Europe
Europe - Amsterdam MCP2
Europe - Frankfurt
Europe - London MCP2
Europe - Amsterdam
Europe - London MCP1
Africa
South Africa - Johannesburg
South Africa

c. Additionally, you can access the Region VPN by using Region VPN button on the Home Dashboard:



d. You can access the Data Center VPN by using the Data Center VPN button on the Data Center dashboard:



Recently Updated

- How to Move a Client Image between User-Manageable Clusters
- How do I Identify Hardware Specifications and Capabilities Available in a Data Center Location
- Introducing the New Red Hat Update Infrastructure

- Introduction to Tagging, Tag Keys and Tag Values
- How to Deploy a VLAN on a Network Domain