Maidenhead Bridge

Cloud Security Connector - GRE

Models Single & Cluster

Administrator Guide

Software Version 2.6

(August 2019)

Table of Contents

1 Introduction

The Cloud Security Connector (CSC) GRE allows to connect securely to Zscaler Cloud Security Services up to 1 Gbps without hassle.

The main purpose of the CSC GRE family is simplicity: You don't need to re-architect your network. The CSC GRE is a direct replacement of your current Web Security Appliance. You can place the CSC GRE on the same network segment that you current appliance and the CSC will redirect the traffic to Zscaler.

No configuration is required. Simply filling a form with your IP addressing, download the CSC (VM) and power it on.

The CSC GRE comes with all parameters to work with Zscaler. As soon you lunch the CSC at the location, the CSC will automatically connect to the best Zscaler nodes. The CSC GRE contains the perfect configuration for GRE tunnels, firewall rules and routing tables that are necessary.

You can run the CSC GRE on any virtual software: Vmware, Hyper-V, KVM, etc; and a hardware version is also available on request.

All Zscaler functionalities are available. Internal IPs are completely visible on the Zscaler GUI.

Simple to install with full management from Amazon AWS, Rundeck or SSH.

2 Key benefits of the Cloud Security Connector GRE

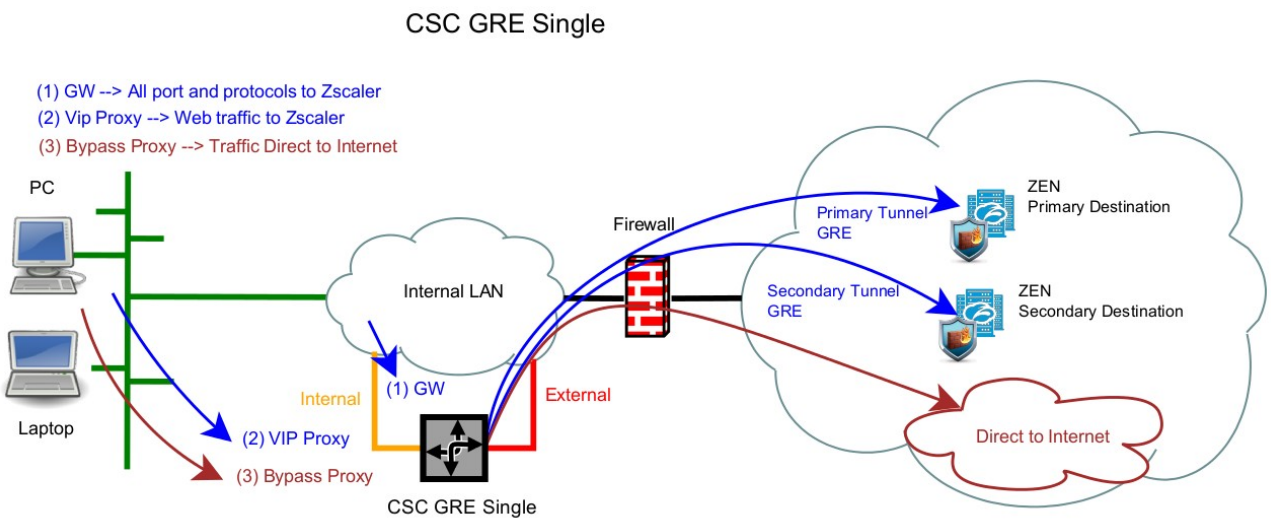
- No Networking knowledge required. No configuration.
- Direct replacement of your current appliance Web Security Appliance.
- Enables any Location to be connected to Zscaler Cloud Security Services up to 1 Gbps.
- Full tunnel redundancy.
- VIP proxy to direct the traffic to Zscaler.
- Bypass Proxy to send the traffic direct to Internet.
- Easy configuration: After you buy the CSC, you will need to fill a form indicating your IPs and GWs. After the form is submitted, you will receive the OVA file to install.
- All parametrization required for Zscaler is already configured with the optimal values.
- All Zscaler functionalities can be used: Firewall and Web Security.
- Full visibility of internal IPs.
- No operational burden for Administrators.

- Full hardened device.
- Works behind a NAT
- All virtual platform supported: Vmware, Hyper-V, KVM, etc. Hardware version available if required.
- One click Status and Configuration. This shows 25 values and does 14 checks.
- Amazon AWS management
- Zscaler API Ready
- MTR (MyTraceRoute) test to the Zscaler nodes and in the reverse path as well.
- Speedtest.net integrated
- Works with No default Route Scenarios.
- Small OVA instance: 2 CPU, 4 GB RAM, 8 GB Disk

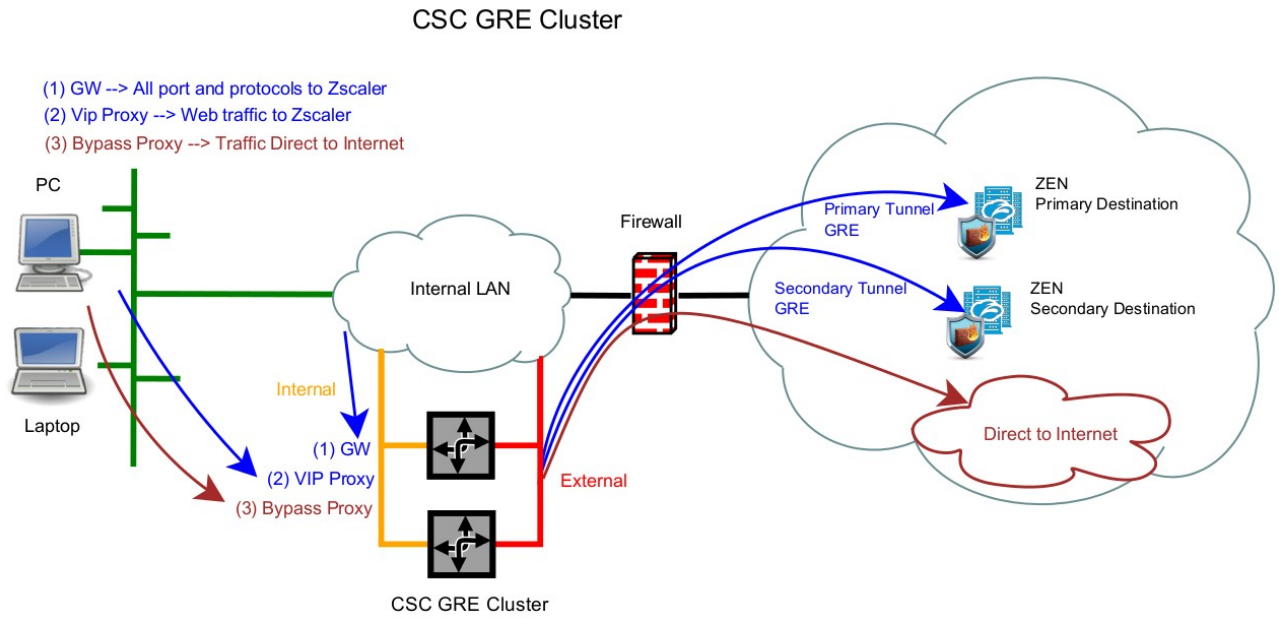
3 Cloud Security Connector GRE: Network Diagrams

Both CSC GRE Single and Cluster has two interfaces: Internal and External. The External interface provides complete isolation from Internal. It is required to use different VLANs (or dedicated interface) for each one.

3.1 CSC GRE Single



3.2 CSC GRE Cluster

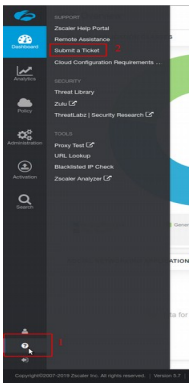


4 Creating the CSC GRE

To create the CSC GRE is very easy. Just filling a form with your IP addressing and the GRE tunnels IPs.

4.1 Submit a ticket to Zscaler Support for GRE Instructions

➔ From the GUI, Go to: Help > Submit a Ticket



➔ You will be redirected to the Submit Ticket Page:

Here you need to specify your GRE Public IP

Important: You need to specify the **<city>, <state>** and **<country>** where the IP is located. This allows Zscaler Support to indicate the best ZEN nodes for your location.

➔ After the ticket is submitted, you will receive an email with the GRE information, like this one:

We have provisioned the GRE on IP 109.151.174.156.

```
Tunnel Source IP:     109.151.174.156
Internal Range:   172.17.6.232-172.17.6.239

Primary Destination:     165.225.72.38
Internal Router IP:     172.17.6.233/30
Internal ZEN IP:     172.17.6.234/30

Secondary Destination:     104.129.194.38
Internal Router IP:     172.17.6.237/30
Internal ZEN IP:     172.17.6.238/30
```

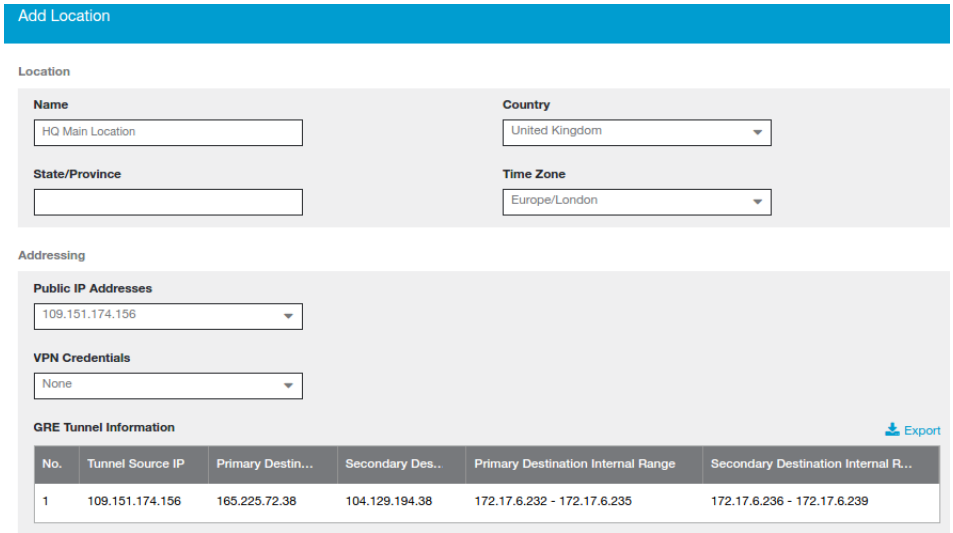
GRE Public IP

Please, note that Tunnel Source IP = <GRE Public IP> and the values remarked in green will be requested when filling the "CSC GRE Form"

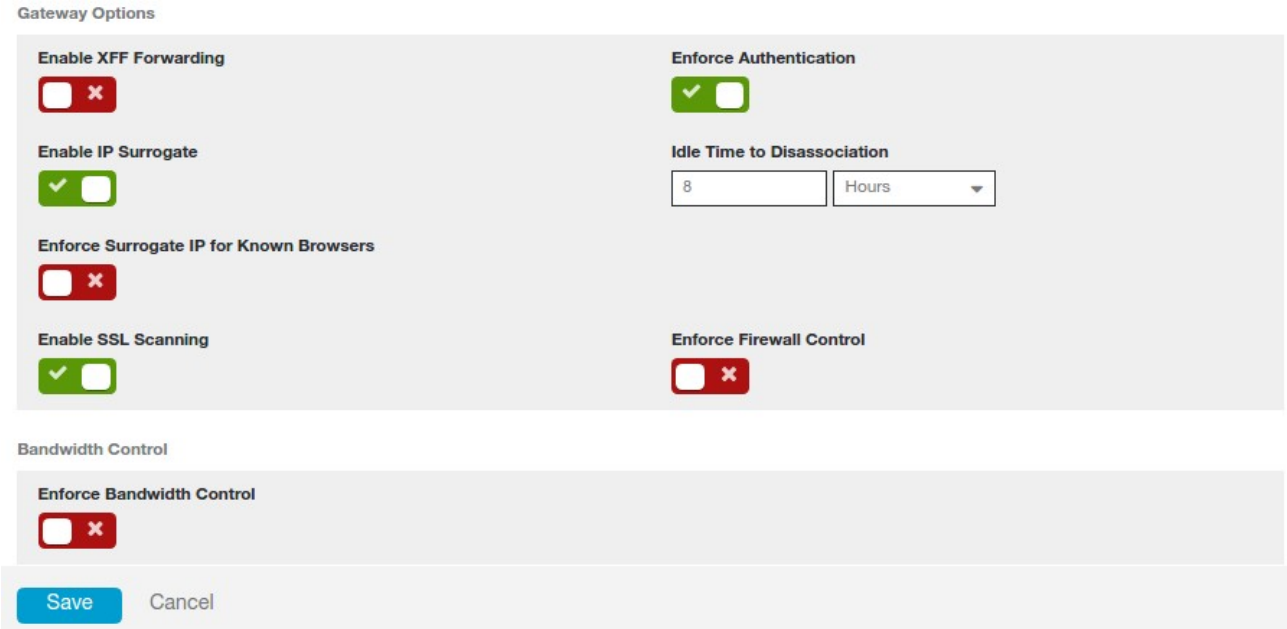
4.2 Create the Location on Zscaler GUI

On the Zscaler GUI, go to Administration > Location > Add Location

➔ ***Mandatory:*** Put Name, Country and Time Zone. Select the Public IP requested for the location.

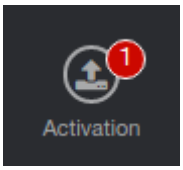


➔ ***Optional:*** Select additional options for the Location according your design, like Enforce Authentication, SSL inspection, Surrogate IP, etc.



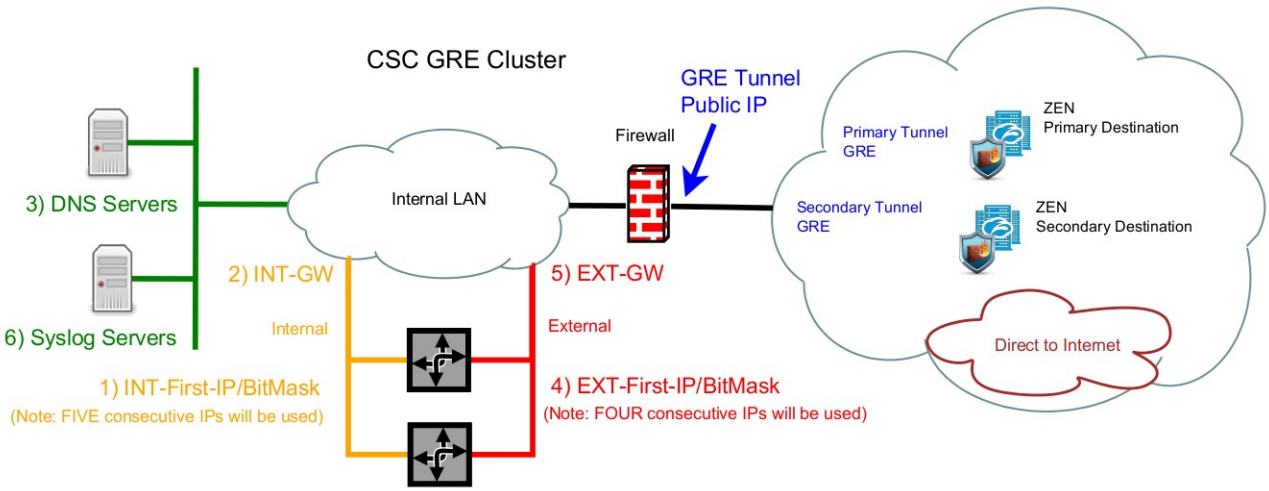
➔ Click “Save”

➔ and “Activate”. Click the RED indication on the top right of the screen and activate the changes.



4.3 Filling the Form

After you buy the CSC, you will receive a Welcome Email with the indication about to fill the a form with your data. Here a partial view of the form:



We have provisioned the GRE on IP 109.151.174.156.

```
Tunnel Source IP:    109.151.174.156
Internal Range:  172.17.6.232-172.17.6.239

Primary Destination:    165.225.72.38
Internal Router IP:    172.17.6.233/30
Internal ZEN IP:    172.17.6.234/30

Secondary Destination:    104.129.194.38
Internal Router IP:    172.17.6.237/30
Internal ZEN IP:    172.17.6.238/30
```

GRE Public IP

The form is very easy to fill. The values that you need to ingress are:

1. Email
2. Company Name
3. Zscaler Company ID
4. Zscaler Cloud Name
5. Your domain

6. Location Name
7. Internal Interface: First IP / Bitmask (*) and Gateway.
8. External Interface First IP/Bitmask (**) Gateway.
9. DNS Servers.
10. Syslog Servers and TCP port
11. Input your GRE tunnel information.

(*) The CSC GRE Single uses 3 x IPs. The CSC GRE Cluster uses 5 x IPs.

(**) The CSC GRE Single uses 2 x IPs. The CSC GRE Cluster uses 4 x IPs.

4.4 CSC files: OVA, URL/Bypass PAC example.

After filling the form, you will receive an email containing links to download two files:

- cgcxxx-v-y-z.ova (your Open Virtual Appliance file to install in your virtual infrastructure)
- cgcxxxxx-url-bypass-pac.txt (Instructions to create the “Bypass PAC” to feed your CSCs Bypass List. It contains your Bypass PAC URL already configured on the CSCs)

5 Firewall Requirements

5.1 CSC GRE Cluster

5.1.1 Mandatory Firewall Rules:

External IP#	Source	Protocol	Ports / Service	Destination
First	Tunnel IP	GRE (47)	None.([1])	Zscaler Nodes
Second	Bypass Proxy Egress IP	TCP	80, 443	Internet
			1024-65535 ([2])	Internet
Third	CSC IP(eth0) -a	TCP	80, 433	Zscaler Nodes Zscaler PAC Servers
Fourth	CSC IP(eth0) -b			

5.1.2 Optional Firewall Rules:

5.1.2.1 If using external DNS (on the internet)

External IP#	Source	Protocol	Ports / Service	Destination
Third	CSC IP(eth0) -a	TCP, UDP	53	Public DNS Servers
Fourth	CSC IP(eth0) -b			

5.1.2.2 If using AWS management

External IP#	Source	Protocol	Ports / Service	Destination
Third	CSC IP(eth0) -a	TCP	443	AWS SSM Agent URLs: ([3]) ssm.<**AWS region**>.amazonaws.com ec2messages.<**AWS region**>.amazonaws.com
Fourth	CSC IP(eth0) -b			

5.1.2.3 For MyTraceroute test when tunnels are down.

External IP#	Source	Protocol	Ports / Service	Destination
Third	CSC IP(eth0) -a	ICMP	echo-request	Zscaler Nodes Zscaler PAC files
Fourth	CSC IP(eth0) -b			
	Zscaler Nodes Zscaler PAC files	ICMP	echo-reply time-exceeded	CSC IP(eth0) -a CSC IP(eth0) -b

1 GRE is protocol and has not ports (like protocol TCP or UDP)
2 This ports are optional but are required for Web sites that are using this particular ports, for example: http://www.example.com:8080
3 The URL of the AWS SSM agent are different depending the AWS region. For example, Ireland is “eu-west1”

5.2 CSC GRE Single

5.2.1 Mandatory Firewall Rules:

External IP#	Source	Protocol	Ports / Service	Destination
First	Tunnel IP	GRE (47)	None.([4])	Zscaler Nodes
		TCP	80, 443	Zscaler Nodes Zscaler PAC Servers
Second	Bypass Proxy Egress IP	TCP	80, 443	Internet
			1024-65535 ([5])	Internet

5.2.2 Optional Firewall Rules:

5.2.2.1 If using external DNS (on the internet)

External IP#	Source	Protocol	Ports / Service	Destination
First	Tunnel IP	TCP, UDP	53	Public DNS Servers

5.2.2.2 If using AWS management

External IP#	Source	Protocol	Ports / Service	Destination
First	Tunnel IP	TCP	443	AWS SSM Agent URLs: ([6]) ssm.<**AWS region**>.amazonaws.com ec2messages.<**AWS region**>.amazonaws.com

5.2.2.3 For MyTraceroute test when tunnels are down.

External IP#	Source	Protocol	Ports / Service	Destination
First	Tunnel IP	ICMP	echo-request	Zscaler Nodes Zscaler PAC files
	Zscaler Nodes Zscaler PAC files	ICMP	echo-reply time-exceeded	CSC IP(eth0) -a CSC IP(eth0) -b

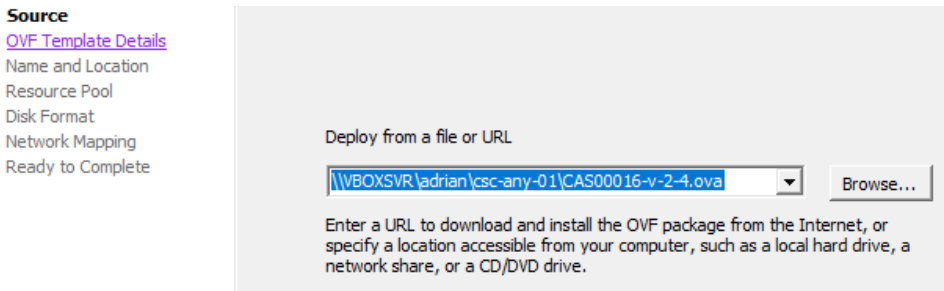
4 GRE is protocol and has not ports (like protocol TCP or UDP)
5 This ports are optional but are required for Web sites that are using this particular ports, for example: http://www.example.com:8080
6 The URL of the AWS SSM agent are different depending the AWS region. For example, Ireland is “eu-west1”

6 Installing the OVA file in your Virtual Platform.

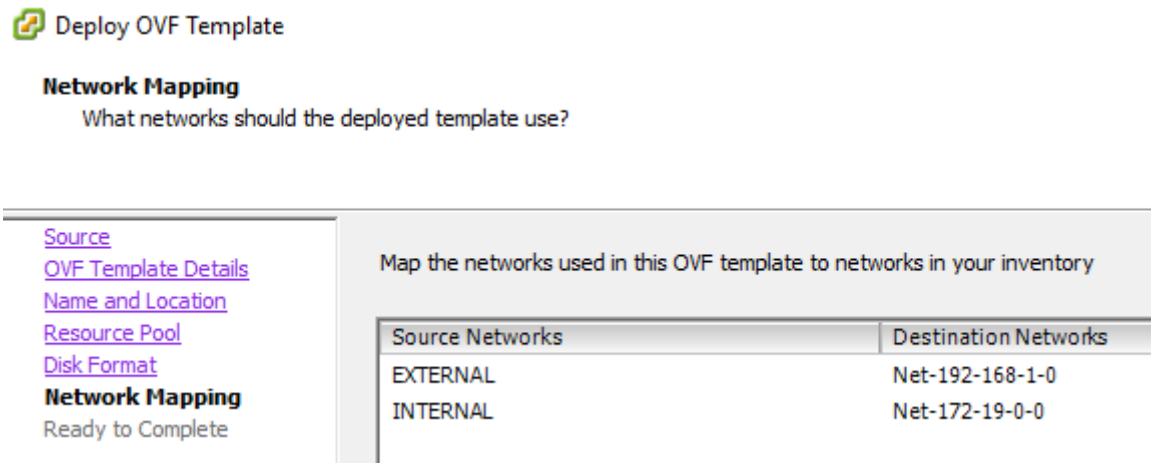
The following examples shows the installation on Vmware and Hyper-V.

6.1 Using VMware 5.x

1. Go to vSphere, File > Deploy OVF template
2. Select the OVA File:



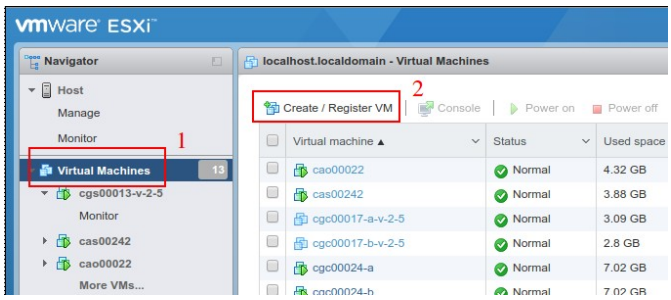
3. OVF Template Details: Click Next
4. Name and Location: Put the Name you want.
5. Resource Pool: Place the VM where you want.
6. Disk Format: Click Next
7. **Network Mapping: Please map the interfaces EXTERNAL and INTERNAL to your interfaces. Here an example:**



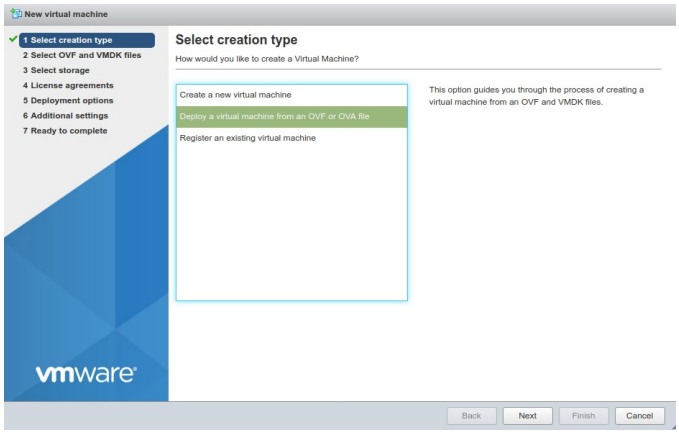
8. Click “Next”
9. Click “Finish”

6.2 Using VMware 6.x

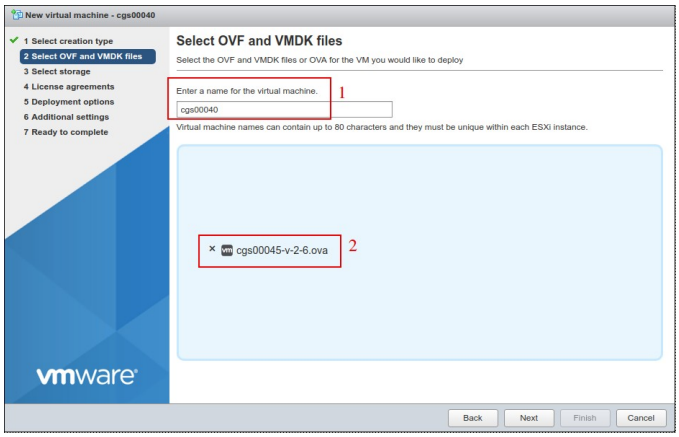
1. Go to Virtual Machines → Create/Register VM



2. Deploy a virtual machine from an OVF or OVA file

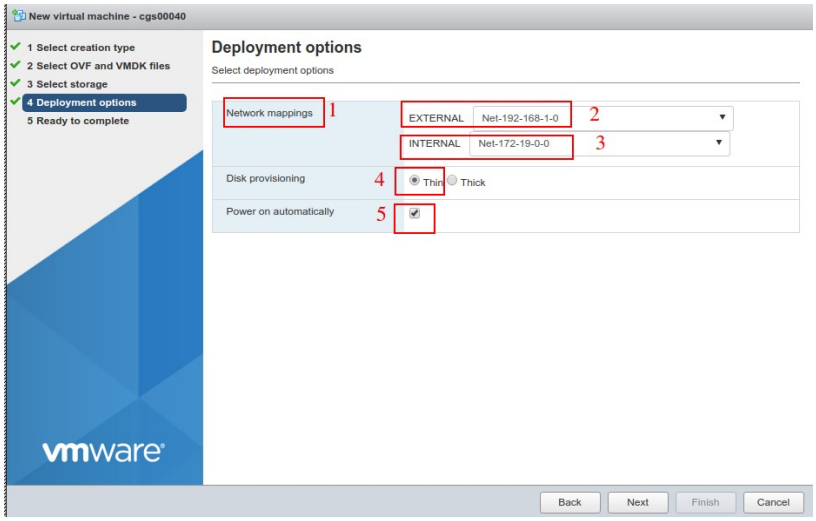


3. Click “Next”
4. Put a “Name” and “Select the OVA File”

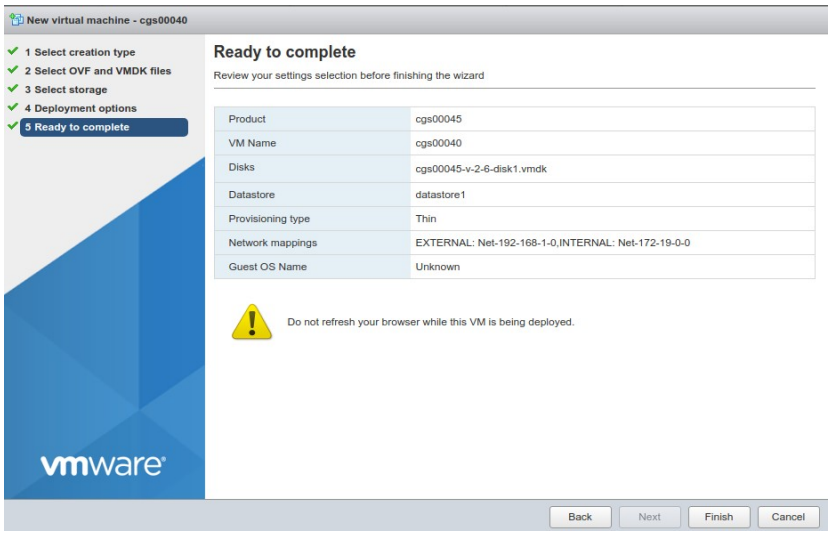


5. Click “Next”
6. Select Storage and click Next

7. On “Deployment options”, Select:
   a) “Network Mappings” → Select “EXTERNAL” and “INTERNAL” interfaces of the CSC.
   b) Disk Provisioning: Thin
   c) Power on Automatically



8. Click “Next”
9. The next screen will show all values:

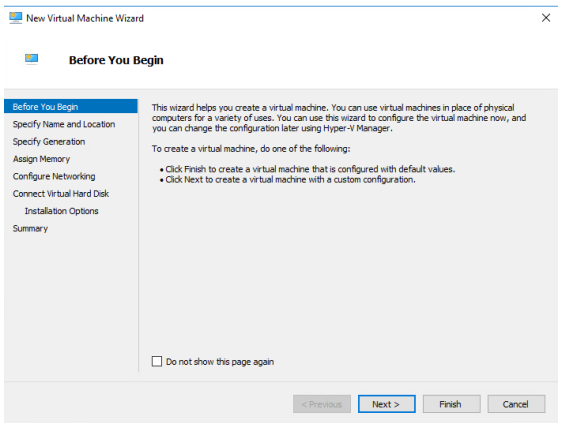


10. Click “Finish”

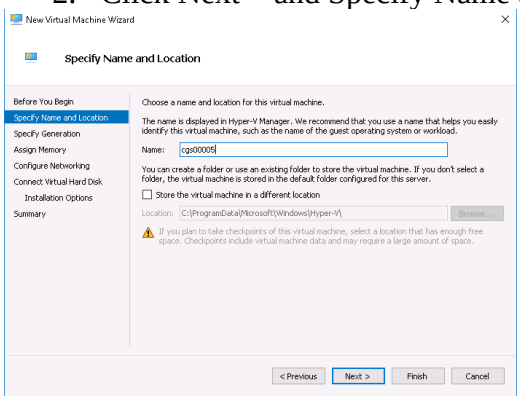
6.3 Using Hyper-V

Before to start: You will receive the CSC disk (.vhdx) on zip format. Please unzip it and place it on your Virtual Machine directory before to start this wizard.

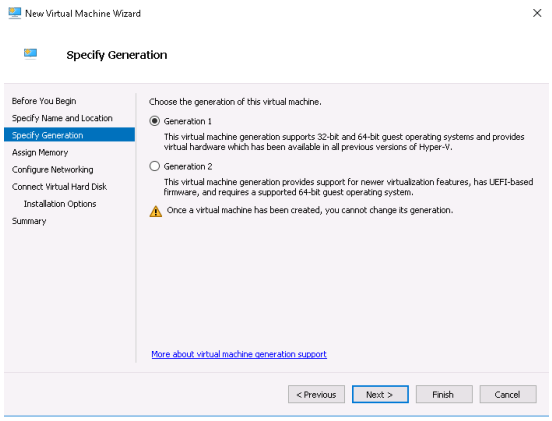
1. Go to Hyper-V and Click → Action → New



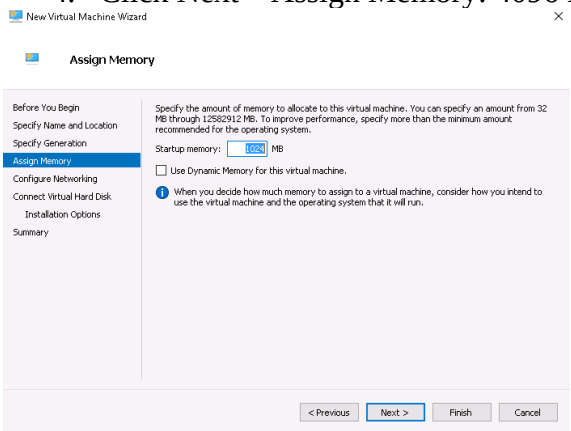
2. Click Next > and Specify Name and Storage



3. Click Next > Select “Generation 1”

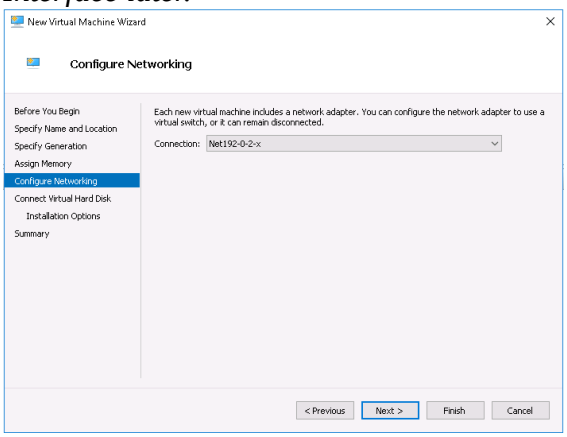


4. Click Next > Assign Memory: 4096 MB



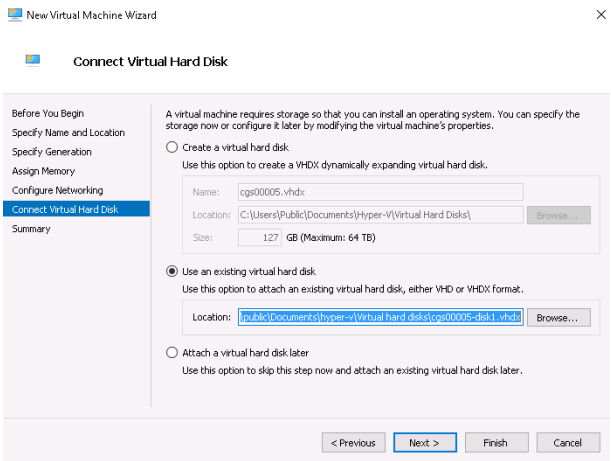
5. Click Next > Configure Networking

IMPORTANT: *This is the EXTERNAL interface of the CSC. We are going to add the Internal Interface later.*



6. Click Next > Connect Virtual Hard Disk

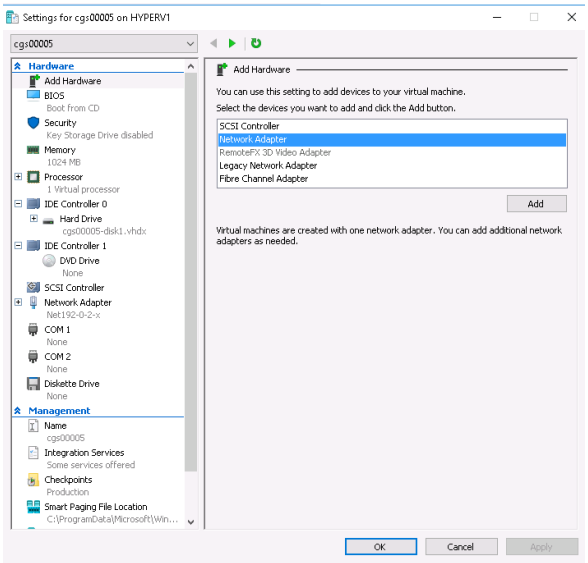
Select the unzipped disk on "Use an existing virtual disk"



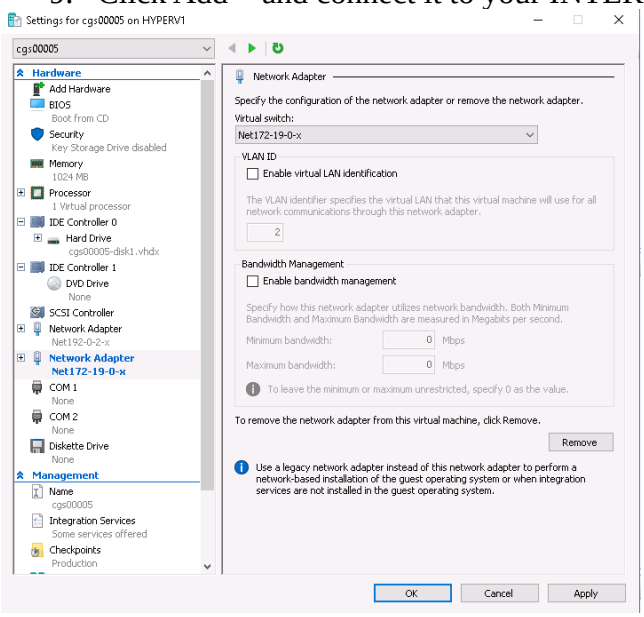
7. Click Next > Summary > Finish .

The machine will be created but we need to add the INTERNAL Interface.

8. Right Click the machine created > Settings > Add Hardware > Network Adapter



9. Click Add > and connect it to your INTERNAL virtual switch



10. Click Apply and OK

7 Powering up the CSC GRE

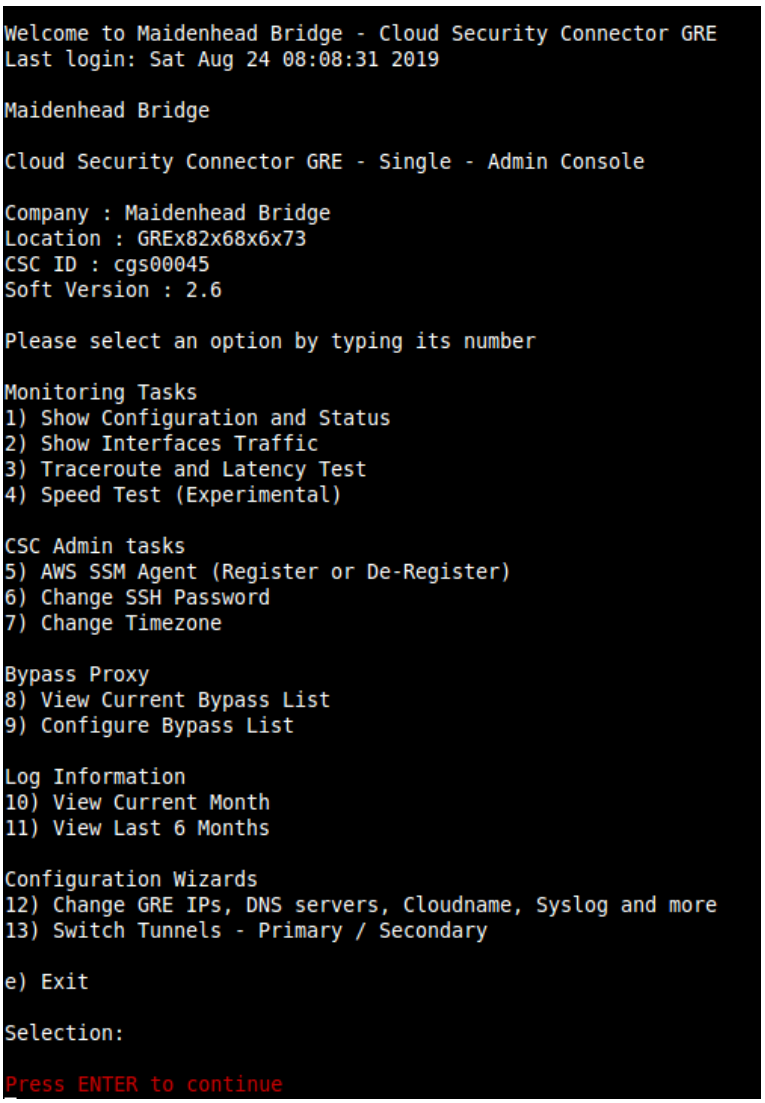
1. Power on the Virtual Machine
2. SSH to the CSC using : ssh cscadmin@<First Internal IP> for the GRE Single. On the CSC GRE Cluster you need to SSH the 4th (csc-gre-a) and 5th (csc-gre-b) internal IPs respectively.

When prompted, put the following username and password to login on the CSC Console:

Username: **cscadmin**

Password: **maidenheadbridge**

Note: SSH to the EXTERNAL interface IP is not allowed.



```
Welcome to Maidenhead Bridge - Cloud Security Connector GRE
Last login: Sat Aug 24 08:08:31 2019

Maidenhead Bridge

Cloud Security Connector GRE - Single - Admin Console

Company : Maidenhead Bridge
Location : GREx82x68x6x73
CSC ID : cgs00045
Soft Version : 2.6

Please select an option by typing its number

Monitoring Tasks
1) Show Configuration and Status
2) Show Interfaces Traffic
3) Traceroute and Latency Test
4) Speed Test (Experimental)

CSC Admin tasks
5) AWS SSM Agent (Register or De-Register)
6) Change SSH Password
7) Change Timezone

Bypass Proxy
8) View Current Bypass List
9) Configure Bypass List

Log Information
10) View Current Month
11) View Last 6 Months

Configuration Wizards
12) Change GRE IPs, DNS servers, Cloudname, Syslog and more
13) Switch Tunnels - Primary / Secondary

e) Exit

Selection:

Press ENTER to continue
```

3. Select 1) Show Configuration and Status check “Tunnel Status”

```
Selection: 1

GENERAL INFORMATION
Company : Maidenhead Bridge
Location : GREx82x68x6x73
CSC ID : cgs00045
CSC date: Sat 24 Aug 07:10:24 UTC 2019
Soft version : 2.6

INTERFACES INFORMATION
External: Tunnel IP (eth0): 192.168.1.152/24 | Bypass Proxy Egress IP: 192.168.1.153 | Network Gateway: 192.168.1.240 is Alive
Internal: CSC GW IP (eth1): 172.19.0.152/24 | Network Gateway: 172.19.0.88 is Not reachable (ping failure)

TRAFFIC REDIRECTION Options
To Zscaler: VIP Proxy: 172.19.0.153:80 (or :9400) | Route all traffic via CSC GW IP | Zscaler Global Proxies (port 80/9400) via CSC GW IP
Direct to Internet: Bypass Proxy: 172.19.0.154:3128 | Zscaler Global Proxies (port 3128) via CSC GW IP

DNS INFORMATION
DNS Server (1) IP: 172.19.0.100 is Alive
DNS Server (2) IP: 172.19.0.134 is Alive

ZSCALER INFORMATION
Zscaler Cloud:  zscalerthree
GRE tunnels egress Public IP: 82.68.6.73
Primary Tunnel:
                ZEN Public IP: 165.225.16.36
                Tunnel IPs (local/zen): 172.17.4.209 / 172.17.4.210
Secondary Tunnel:
                ZEN Public IP: 165.225.76.39
                Tunnel IPs (local/zen): 172.17.4.213 / 172.17.4.214

TUNNEL STATUS
Primary Tunnel (reachability):
                              Layer 7 Keepalive is: Alive
                              GRE ZEN Tunnel IP is: Alive
Secondary Tunnel (reachability):
                              Layer 7 Keepalive is: Alive
                              GRE ZEN Tunnel IP is: Alive

Tunnel Status: Primary tunnel is active since: Sat 24 Aug 07:08:56 UTC 2019

HTTP://IP.ZSCALER.COM PAGE STATUS
You are accessing this host via a Zscaler proxy hosted at London III in the zscalerthree.net cloud.
Your Gateway IP Address is 82.68.6.73

BYPASS PROXY - EGRESS INTERFACE STATUS
Bypass Proxy Egress Interface 192.168.1.153 can reach test page (http://pac.zscalerthree.net)

AWS SSM AGENT
AWS SSM Agent is not registered

SYSLOG INFORMATION
SYSLOG Server (1) IP: 172.19.0.199 is Alive
SYSLOG Server (2) IP is not configured
SYSLOG TCP Port: 514

Press ENTER to continue
```

4. Congratulations! You are connected to Zscaler.
5. Now, you can forward your traffic through the CSC using the following methods:
    - Zapp in Tunnel and Local Proxy (recommended)
    - PAC files: Traffic to Zscaler via VIP Proxy, Traffic direct to internet via Bypass Proxy
    - Explicit proxy: via VIP Proxy.
    - All port and protocols: If you are using Zscaler Cloud Firewall, you can use the Internal Cluster IP as your default Gateway to Zscaler and to send all ports and protocols.

Take a look of next section for more details.

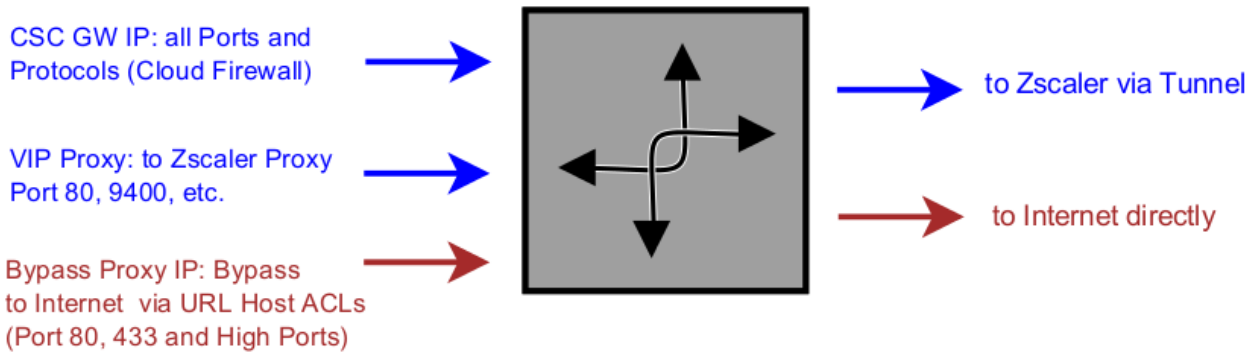
8 How to Redirect traffic to the CSC

The objective of the Cloud Security Connectors of Maidenhead Bridge is to provide a simple architecture, 100% proven that works, to connect to Zscaler.

Every member of the CSC family follows the principle of "three IPs" on the internal side:

- **CSC GW IP**: To be used as Default Gateway for internal devices behind the CSC redirecting all ports and protocols to Zscaler when using Cloud Firewall.
- **VIP Proxy (*):** This Virtual IP Proxy translates the packets directly to the Zscaler proxy. To be used when Zapp / PAC files are implemented or explicit proxy.
- **Bypass Proxy(**):** The Bypass Proxy enables a simple way to do Direct Bypasses to Internet.

Here an illustration about this:



(*) Alternatively you can use Zscaler Global Proxies to send the traffic to Zscaler using port 80/9400

(**) Alternatively you can use Zscaler Global Proxies to send the traffic to Internet using port 3128

You can download a PAC file Example from here: Click here

8.1 Obtain your traffic redirection IPs

The "Show Configuration and Status" menu provides the information of Traffic redirection options.

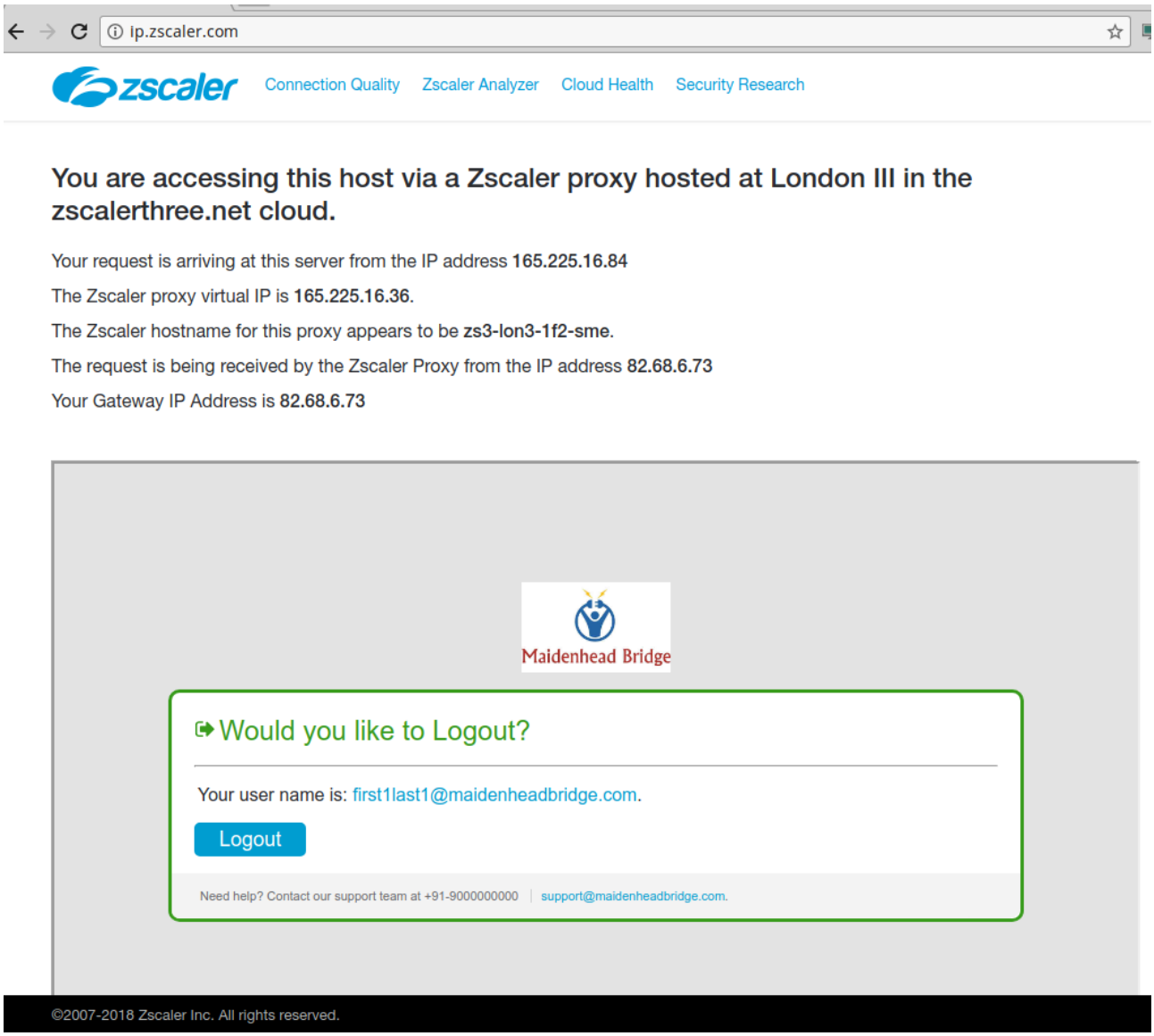
```
TRAFFIC REDIRECTION Options
To Zscaler: VIP Proxy: 172.19.0.153:80 (or :9400) | Route all traffic via CSC GW IP | Zscaler Global Proxies (port 80/9400) via CSC GW IP
Direct to Internet: Bypass Proxy: 172.19.0.154:3128 | Zscaler Global Proxies (port 3128) via CSC GW IP
```

Please, contact us at http://support.maidenheadbridge.com and we will provide the best method to your situation.

8.2 Verifying that your reaching Zscaler properly

8.2.1 Using a PC

Go to the following page: ip.zscaler.com from your PC



This page shows:

(values of this example between brackets [])

- Cloud name: [Zscaler Three]
- Node: [London III]
- Zscaler internal values [165.225.16.84, 165.225.16.36, zs3-lon3-1f2-sme]
- Your Gateway IP addresses [82.68.6.73. This is your public IP]

- The name or logo of your organization [Maidenhead Bridge]
- The Username (if Authentication was enabled on the location) [first1last1@maidenheadbridge.com]

8.2.2 Using the “Show Configuration and Status” menu

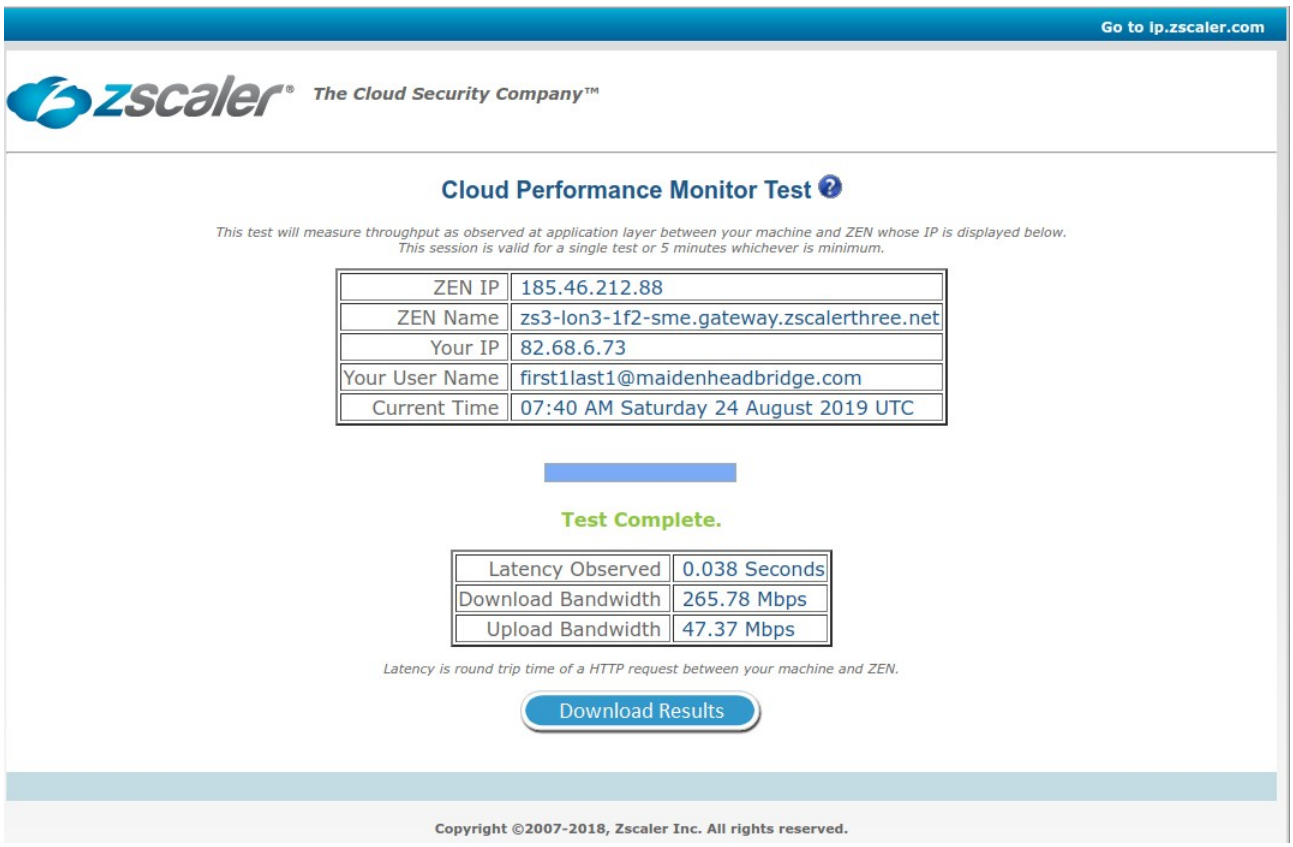
This menu also goes to http://ip.zscaler.com .

```
HTTP://IP.ZSCALER.COM PAGE STATUS
You are accessing this host via a Zscaler proxy hosted at London III in the zscalerthree.net cloud.
Your Gateway IP Address is 82.68.6.73
```

8.3 Checking Connection Quality

8.3.1 Using a PC

On the page ip.zscaler.com, click on “Connection Quality” and “Start Test”



8.3.2 Using “Speed Test” menu

The CSC runs the Speedtest.net. This function is experimental due to we need to rely on third party tools.

```
Selection: 4

SPEED TEST
This is experimental. We are using third party tools. (Speedtest.net)
Results can be inaccurate or none. The test takes a while

Retrieving speedtest.net configuration...
Testing from Zscaler (165.225.16.67)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by QTS Data Centers (London) [2.56 km]: 11.165 ms
Testing download speed.................................................
Download: 286.02 Mbit/s
Testing upload speed...................................................
Upload: 53.13 Mbit/s


Press ENTER to continue
```

9 CSC GRE – Admin Console

The CSC GRE has an Admin Console that allows to do different tasks. When you access to the Admin Console, the following information appears on top:

```
Maidenhead Bridge

Cloud Security Connector GRE - Single - Admin Console

Company : Maidenhead Bridge
Location : GREx82x68x6x73
CSC ID : cgs00045
Soft Version : 2.6
```

And you can select the following tasks:

9.1 Monitoring Tasks:

```
Monitoring Tasks
1) Show Configuration and Status
2) Show Interfaces Traffic
3) Traceroute and Latency Test
4) Speed Test (Experimental)
```

9.1.1 Show Configuration and Status

1. Show Configuration and Status. This menu show all parameters configured on the CSC GRE and does several checks.

In total, 22 parameters are showed and 16 checks are done. All in one shot.

```
GENERAL INFORMATION
Company : Maidenhead Bridge
Location : GREx82x68x6x73
CSC ID : cgs00045
CSC date: Sat 24 Aug 07:48:09 UTC 2019
Soft version : 2.6

INTERFACES INFORMATION
External: Tunnel IP (eth0): 192.168.1.152/24 | Bypass Proxy Egress IP: 192.168.1.153 | Network Gateway: 192.168.1.240 is Alive
Internal: CSC GW IP (eth1): 172.19.0.152/24 | Network Gateway: 172.19.0.88 is Not reachable (ping failure)

TRAFFIC REDIRECTION Options
To Zscaler: VIP Proxy: 172.19.0.153:80 (or :9400) | Route all traffic via CSC GW IP | Zscaler Global Proxies (port 80/9400) via CSC GW IP
Direct to Internet: Bypass Proxy: 172.19.0.154:3128 | Zscaler Global Proxies (port 3128) via CSC GW IP

DNS INFORMATION
DNS Server (1) IP: 172.19.0.100 is Alive
DNS Server (2) IP: 172.19.0.134 is Alive

ZSCALER INFORMATION
Zscaler Cloud:  zscalerthree
GRE tunnels egress Public IP: 82.68.6.73
Primary Tunnel:
                ZEN Public IP: 165.225.16.36
                Tunnel IPs (local/zen): 172.17.4.209 / 172.17.4.210
Secondary Tunnel:
                ZEN Public IP: 165.225.76.39
                Tunnel IPs (local/zen): 172.17.4.213 / 172.17.4.214

TUNNEL STATUS
Primary Tunnel (reachability):
                              Layer 7 Keepalive is: Alive
                              GRE ZEN Tunnel IP is: Alive
Secondary Tunnel (reachability):
                              Layer 7 Keepalive is: Alive
                              GRE ZEN Tunnel IP is: Alive

Tunnel Status: Primary tunnel is active since: Sat 24 Aug 07:08:56 UTC 2019

HTTP://IP.ZSCALER.COM PAGE STATUS
You are accessing this host via a Zscaler proxy hosted at London III in the zscalerthree.net cloud.
Your Gateway IP Address is 82.68.6.73

BYPASS PROXY - EGRESS INTERFACE STATUS
Bypass Proxy Egress Interface 192.168.1.153 can reach test page (http://pac.zscalerthree.net)

AWS SSM AGENT
AWS SSM Agent is not registered

SYSLOG INFORMATION
SYSLOG Server (1) IP: 172.19.0.199 is Alive
SYSLOG Server (2) IP is not configured
SYSLOG TCP Port: 514
```

Here the detail of the information provided. Test are marked in ***bold***

9.1.1.1 GENERAL INFORMATION

Here is general information about the device.

- Company Name
- Location
- CSC ID
- CSC Date
- Soft Version

9.1.1.2 INTERFACES INFORMATION

This menu shows the following according each model:

CSC GRE Single:

```
INTERFACES INFORMATION
External: Tunnel IP (eth0): 192.168.1.152/24 | Bypass Proxy Egress IP: 192.168.1.153 | Network Gateway: 192.168.1.240 is Alive
Internal: CSC GW IP (eth1): 172.19.0.152/24 | Network Gateway: 172.19.0.88 is Not reachable (ping failure)
```

- External:
  - Tunnel IP (eth0): <IP/Mask>
  - Bypass Proxy Egress: <IP>
  - Network Gateway: <IP> **(Alive or Not reachable)**
- Internal:
  - CSC GW IP (eth1): <IP/Mask>
  - Network Gateway: <IP> **(Alive or Not reachable)**

CSC GRE Cluster:

```
INTERFACES INFORMATION
External: Tunnel IP: 192.168.1.102 | Bypass Proxy Egress IP: 192.168.1.103 | CSC IP(eth0): 192.168.1.104/24 | Network Gateway: 192.168.1.133 is Alive
Internal: CSC GW IP: 172.19.0.103 | CSC IP(eth1): 172.19.0.106/24 | Network Gateway: 172.19.0.133 is Alive
```

- External:
  - Tunnel IP: <IP>
  - Bypass Proxy Egress: <IP>
  - CSC IP (eth0): <IP/Mask>
  - Network Gateway: <IP> **(Alive or Not reachable)**
- Internal:
  - CSC GW IP: <IP>
  - CSC IP(eth1): <IP/Mask>
  - Network Gateway: <IP> **(Alive or Not reachable)**

9.1.1.3 TRAFFIC REDIRECTION Options

This menu shows the following:

```
TRAFFIC REDIRECTION Options
To Zscaler: VIP Proxy: 172.19.0.153:80 (or :9400) | Route all traffic via CSC GW IP | Zscaler Global Proxies (port 80/9400) via CSC GW IP
Direct to Internet: Bypass Proxy: 172.19.0.154:3128 | Zscaler Global Proxies (port 3128) via CSC GW IP
```

- To Zscaler:
  - VIP Proxy: <IP:Port> (80/9400)
  - Route all traffic via CSC GW IP
  - Zscaler Global Proxies (port 80/9400) via CSC GW IP
- Direct to Internet:
  - Bypass Proxy: <IP:Port> (3128)
  - Zscaler Global Proxies (port 3128) via CSC GW IP

9.1.1.4 DNS INFORMATION

This menu shows the following:

```
DNS INFORMATION
DNS Server (1) IP: 172.19.0.100 is Alive
DNS Server (2) IP: 172.19.0.134 is Alive
```

- DNS Server (1) IP: <IP> **(Alive or Not reachable)**
- DNS Server (2) IP: <IP> **(Alive or Not reachable)**

9.1.1.5 ZSCALER INFORMATION

Here the values configuration values of the GRE Tunnel . (Cloud, Public IP, Primary Tunnel, Secondary Tunnel)

```
ZSCALER INFORMATION
Zscaler Cloud:  zscalerthree
GRE tunnels egress Public IP: 82.68.6.73
Primary Tunnel:
                ZEN Public IP: 165.225.16.36
                Tunnel IPs (local/zen): 172.17.4.209 / 172.17.4.210
Secondary Tunnel:
                ZEN Public IP: 165.225.76.39
                Tunnel IPs (local/zen): 172.17.4.213 / 172.17.4.214
```

- Zscaler Cloud: <Cloud Name>
- GRE tunnels egress Public IP: <IP>
- Primary Tunnel:
  - ZEN Public IP: <IP>

  - Tunnel IPs (local/zen): <IP> / <IP>
- Secondary Tunnel:
  - ZEN Public IP: <IP>
  - Tunnel IPs (local/zen): <IP> / <IP>

9.1.1.6 TUNNEL STATUS

This menu shows the status of : Layer 7 Keepalives, Tunnel Keepalives and Tunnel status. This values are particularly important to troubleshoot firewall rules (NAT and Allow Rules)

```
TUNNEL STATUS
Primary Tunnel (reachability):
                              Layer 7 Keepalive is: Alive
                              GRE ZEN Tunnel IP is: Alive
Secondary Tunnel (reachability):
                              Layer 7 Keepalive is: Alive
                              GRE ZEN Tunnel IP is: Alive

Tunnel Status: Primary tunnel is active since: Sat 24 Aug 07:08:56 UTC 2019
```

- Primary (/Secondary) Tunnel (reachability):
  - Layer 7 Keepalive is: **Alive or Not reachable (check port 80 from < CSC Ext IP > to <ZEN Node IP>)**
  - GRE ZEN Tunnel IP is: **Alive or Not reachable (check GRE protocol 47 from <CSC Ext IP> to <ZEN Node IP> and/or if the Location was created on the Zscaler GUI)**
- Tunnel Status:
  - Primary tunnel is active since: <date / time>
  - In transition (when switching tunnels)
  - No active tunnel since: <date / time>
  - Secondary tunnel is active since: <date / time>
    - -> (Note 1: Primary tunnel is under test. After 10 minutes of stability of Primary ZEN, the CSC will return to it)
    - -> (Note 2: If Secondary tunnel fails, the CSC will return to Primary tunnel instantly)

Important: When the CSC is using the Secondary tunnel, is checking the quality of the Primary all time. When the Primary is on good quality for more than 10 minutes, the CSC returns automatically to the Primary.

9.1.1.7 HTTP://IP.ZSCALER.COM PAGE STATUS

This test is what Zscaler support always recommends to do to validate that you are effectively using Zscaler. The CSC is going to the page http://ip.zscaler.com and is retrieving the following information:

```
HTTP://IP.ZSCALER.COM PAGE STATUS
You are accessing this host via a Zscaler proxy hosted at Paris II in the zscalerthree.net cloud.
Your Gateway IP Address is 82.68.6.73
```

- The Cloud and Node that you are using when connected. If you are not connected this value is blank.
- Your Gateway IP (this is your public IP in use)

9.1.1.8 BYPASS PROXY – EGRESS INTERFACE STATUS

This test validates if the bypass proxy egress IP can reach the external page pac.<cloudname>.net This test helps to troubleshoot if the firewall rules for the egress interface are correct.

```
BYPASS PROXY - EGRESS INTERFACE STATUS
Bypass Proxy Egress Interface 192.168.1.153 can reach test page (http://pac.zscalerthree.net)
```

Result when successful:

- Bypass Proxy Egress Interface <Bypass Egress IP> can reach test page (http://pac.<cloudname>.net)

Result when fails:

- Bypass Proxy Egress Interface cannot reach test page (http://pac.zscalerthree.net)
  - Please, verify connectivity from <Bypass Proxy Egress IP> to Internet

9.1.1.9 CLUSTER STATUS (Only GRE Cluster)

This test shows what CSC is the Cluster Active or Cluster Stand by.

```
CLUSTER STATUS
This CSC (cgc00024-a) is Cluster ACTIVE
```

- This CSC (CSC ID) is Cluster ACTIVE (or Stand By)

9.1.1.10 AWS SSM Agent

This section shows the Status of the AWS SSM Agent. It helps to identify the CSC managed instance on AWS, showing the instance ID and the region where the CSC was registered.

Values when AWS SSM Agent not registered

```
AWS SSM AGENT
AWS SSM Agent is not registered
```

Value when registered.

```
AWS SSM AGENT
AWS SSM Agent is active (running) since Fri 2019-06-28 18:26:02 BST; 1 months 26 days ago
Registration values: {"ManagedInstanceID":"mi-0052a5bb707749e33","Region":"eu-west-1"}
```

- AWS SSM Agent is active (running) since <date / time>; <year/month/days> ago
- Registration values: {"ManagedInstanceID":"<mi-xxxx>","Region":"<AWS Region>"}

9.1.1.11 SYSLOG INFORMATION

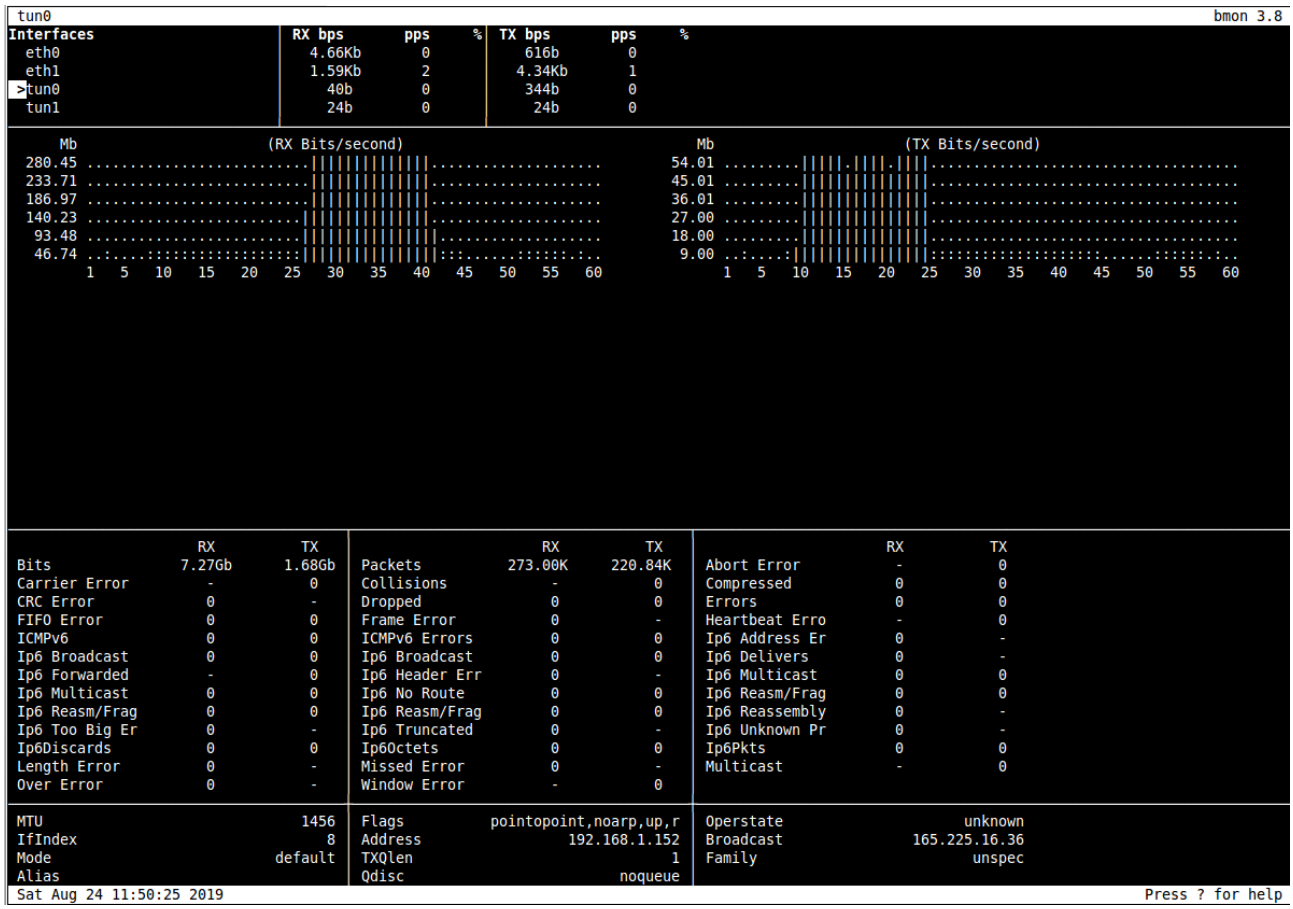
This section shows the values of the Syslogs servers IPs and Port in use.

```
SYSLOG INFORMATION
SYSLOG Server (1) IP: 172.19.0.199 is Alive
SYSLOG Server (2) IP is not configured
SYSLOG TCP Port: 514
```

- SYSLOG Server (1) (/2): <IP> **is “Alive” or “not reachable” or “is not configured”**
- SYSLOG TCP Port: <TCP port>

9.1.2 Show Interfaces Traffic

2. Show Interfaces Traffic: This selection shows the traffic information on all interfaces.



IMPORTANT:

- Press “q” to quit
- Press “?” for help

9.1.3 Traceroute and Latency Test

This test is particular important to check your internet path to Zscaler nodes and the quality of your link.

This Test does a MTR (MyTraceRoute) Tests to the Primary ZEN, Secondary ZEN, Zscaler PAC files and if the tunnel is UP, it check the reverse path from your ZEN active to your public IP (you don’t need to open a ticket to Zscaler requesting this any more)

9.1.3.1 Traceroute and Latency Test with the tunnel "Not Active"

If the tunnel is active, the MTR test will run through the tunnel. In some cases, you may want to do this test direct from your Location without the tunnel. In order to do this test, use the CSC that is "Cluster Stand By" (or block the Keepalives on CSC Single)

```
CLUSTER STATUS
This CSC (cgc00024-b) is Cluster STANDBY
```

Here an example of the test:

- Testing Primary ZEN

```
Selection: 3

My TraceRoute (MTR) Test Report
This test does 10 probes to the Primary ZEN, Secondary ZEN and Zscaler PAC Servers
Notes:
- When the tunnel is UP, this test runs through the tunnel
- When the tunnel is UP, a Reverse Path test from the active ZEN to your Public IP is performed
- Max Hops is equal 30. This test can take a while

Testing Primary ZEN
Start: Sat Aug 24 11:54:46 2019
HOST: cgc00024-b                                                    Loss%   Snt   Last   Avg  Best  Wrst StDev
  1. AS???   192.168.1.133                                           0.0%    10    1.2   1.4   1.1   2.5   0.0
  2. AS13037 82-68-6-78.dsl.in-addr.zen.co.uk (82.68.6.78)           0.0%    10    2.3   2.4   1.7   3.0   0.0
  3. AS???   ???                                                    100.0    10    0.0   0.0   0.0   0.0   0.0
  4. AS13037 ae-7.cor2.lond2.ptn.zen.net.uk (51.148.73.13)           0.0%    10    6.8   6.8   6.4   7.2   0.0
  5. AS13037 ae-21.agg3.lond2.ptn.zen.net.uk (51.148.73.40)          0.0%    10    7.0   7.0   6.6   7.4   0.0
  6. AS???   ge-2-1-0.mpr1.lhr2.uk.above.net (195.66.224.76)         0.0%    10    6.6   7.0   6.6   7.7   0.0
  7. AS6461  ae13.mpr3.lhr3.uk.zip.zayo.com (64.125.30.54)           0.0%    10    6.8   6.9   6.5   7.7   0.0
  8. AS6461  ae27.cs1.lhr15.uk.eth.zayo.com (64.125.30.234)          0.0%    10   17.6  17.4  16.7  18.7   0.3
  9. AS6461  ae2.cs1.ams10.nl.eth.zayo.com (64.125.29.16)            0.0%    10   17.5  17.2  16.9  17.5   0.0
 10. AS6461  ae0.cs1.ams17.nl.eth.zayo.com (64.125.29.81)            0.0%    10   16.9  17.3  16.8  18.4   0.0
 11. AS6461  ae2.cs1.fra6.de.eth.zayo.com (64.125.29.58)             0.0%    10   17.2  17.7  16.8  20.4   0.9
 12. AS6461  ae0.cs1.fra9.de.eth.zayo.com (64.125.29.55)             0.0%    10   24.1  26.0  17.1  39.7   8.6
 13. AS6461  ae27.mpr1.fra4.de.zip.zayo.com (64.125.30.255)          0.0%    10   22.4  19.4  16.8  30.2   4.2
 14. AS6461  94.31.30.234.IPYX-069051-765-ZYO.zip.zayo.com (94.31.30.234)  0.0%  10   16.4  17.1  16.4  18.9   0.5
 15. AS22616 165.225.72.39                                           0.0%    10   16.8  16.7  16.0  17.2   0.0
```

- Testing Secondary ZEN

```
Testing Secondary ZEN
Start: Sat Aug 24 11:55:04 2019
HOST: cgc00024-b                                                    Loss%   Snt   Last   Avg  Best  Wrst StDev
  1. AS???   192.168.1.133                                           0.0%    10    0.9   1.2   0.9   2.3   0.0
  2. AS13037 82-68-6-78.dsl.in-addr.zen.co.uk (82.68.6.78)           0.0%    10    2.5   2.4   2.2   2.8   0.0
  3. AS???   ???                                                    100.0    10    0.0   0.0   0.0   0.0   0.0
  4. AS13037 ae-7.cor2.lond2.ptn.zen.net.uk (51.148.73.13)           0.0%    10   13.2  11.5   6.7  31.5   8.4
  5. AS13037 ae-21.agg3.lond2.ptn.zen.net.uk (51.148.73.40)          0.0%    10    7.5  11.8   6.9  41.3  10.6
  6. AS???   ge-2-1-0.mpr1.lhr2.uk.above.net (195.66.224.76)         0.0%    10    6.7   6.8   6.3   8.3   0.5
  7. AS6461  ae11.mpr2.lhr2.uk.zip.zayo.com (64.125.30.52)           0.0%    10   22.3   8.5   6.7  22.3   4.8
  8. AS6461  ae27.cs1.lhr11.uk.eth.zayo.com (64.125.30.236)          0.0%    10   77.0  77.4  77.0  77.9   0.0
  9. AS6461  ae5.cs1.lga5.us.eth.zayo.com (64.125.29.126)            0.0%    10   80.6  89.7  77.5 106.0   9.9
 10. AS6461  ae4.cs1.dca2.us.eth.zayo.com (64.125.29.203)            0.0%    10   77.4  77.4  76.8  78.1   0.0
 11. AS6461  ae7.mpr3.iad2.us.zip.zayo.com (64.125.25.9)             0.0%    10   77.2  79.8  76.8 100.5   7.3
 12. AS6461  64.125.41.159                                           0.0%    10   77.3  77.3  76.9  77.6   0.0
 13. AS22616 104.129.194.39                                          0.0%    10   77.2  77.1  76.7  77.4   0.0
```

- Testing Zscaler PAC file Servers

```
Testing Zscaler PAC file servers
Start: Sat Aug 24 11:55:21 2019
HOST: cgc00024-b                                          Loss%   Snt   Last   Avg  Best  Wrst StDev
  1. AS???    192.168.1.133                                0.0%    10    1.3   1.6   1.0   4.2   0.7
  2. AS13037 82-68-6-78.dsl.in-addr.zen.co.uk (82.68.6.78)  0.0%    10    1.9   2.2   1.9   2.9   0.0
  3. AS???    ???                                        100.0    10    0.0   0.0   0.0   0.0   0.0
  4. AS13037 ae-7.cor2.lond2.ptn.zen.net.uk (51.148.73.13)  0.0%    10   19.7  27.8   6.4  42.2  13.1
  5. AS13037 ae-21.agg3.lond2.ptn.zen.net.uk (51.148.73.40) 0.0%    10    7.4  10.6   6.4  20.9   5.4
  6. AS???    ge-2-1-0.mpr1.lhr2.uk.above.net (195.66.224.76) 0.0%  10    7.2   7.2   5.8   9.6   1.1
  7. AS6461   ae11.mpr2.lhr2.uk.zip.zayo.com (64.125.30.52)  0.0%    10    7.1   7.0   6.5   7.9   0.0
  8. AS6461   ae27.cs1.lhr11.uk.eth.zayo.com (64.125.30.236) 0.0%    10   88.5  89.6  88.5  93.5   1.4
  9. AS6461   ae5.cs1.lga5.us.eth.zayo.com (64.125.29.126)   70.0%    10   88.8  94.4  88.8 104.3   8.6
 10. AS6461   ae3.cs3.ord2.us.eth.zayo.com (64.125.29.209)   80.0%    10   89.8  89.9  89.8  90.0   0.0
 11. AS6461   ae10.er6.ord7.us.zip.zayo.com (64.125.28.177)  0.0%    10   88.7  89.1  88.2  93.5   1.5
 12. AS6461   64.125.46.73                                   0.0%    10   88.7  88.9  88.5  90.0   0.3
 13. AS22616 104.129.197.230                                 0.0%    10   88.7  89.2  88.4  92.4   1.2
```

- Reverse Path Test

```
Reverse Path Test
No active tunnel. Reverse Path Test runs only when tunnel is active

Press ENTER to continue
```

9.1.3.2 Traceroute and Latency Test with the tunnel "Active"

When the tunnel is active the test runs from inside the tunnel. This is particular useful to see path from the Zscaler Cloud and to see the Reverse Path from the active node to your Public IP.

First, Check that the tunnel is active from the "Show Configuration and Status" menu.

```
CLUSTER STATUS
This CSC (cgc00024-a) is Cluster ACTIVE
```

And run the "Traceroute and Latency Test" after:

- Testing Primary ZEN

```
Selection: 3

My TraceRoute (MTR) Test Report
This test does 10 probes to the Primary ZEN, Secondary ZEN and Zscaler PAC Servers
Notes:
- When the tunnel is UP, this test runs through the tunnel
- When the tunnel is UP, a Reverse Path test from the active ZEN to your Public IP is performed
- Max Hops is equal 30. This test can take a while

Testing Primary ZEN
Start: Sat Aug 24 12:00:07 2019
HOST: cgc00024-a            Loss%   Snt   Last   Avg  Best  Wrst StDev
  1. AS62044 165.225.72.39   0.0%    10   22.1  19.6  17.2  25.3   2.4
```

- Testing Secondary ZEN

```
Testing Secondary ZEN
Start: Sat Aug 24 12:00:22 2019
HOST: cgc00024-a                    Loss%   Snt   Last   Avg  Best  Wrst StDev
  1. AS22616 104.129.194.39          0.0%    10   17.9  19.4  16.8  27.3   3.9
```

- Testing Zscaler PAC file Servers

```
Testing Zscaler PAC file servers
Start: Sat Aug 24 12:00:37 2019
HOST: cgc00024-a                                                  Loss%   Snt   Last   Avg  Best  Wrst StDev
  1. AS???    172.17.7.58                                          0.0%    10   19.3  19.4  16.7  23.6   2.3
  2. AS62044 165.225.72.2                                          0.0%    10   25.0  21.9  17.2  30.1   4.5
  3. AS3257  ae25.cr10-fra2.ip4.gtt.net (213.254.196.241)          0.0%    10   24.7  29.3  18.4  86.0  20.2
  4. AS3257  xe-9-2-4.cr1-chi1.ip4.gtt.net (213.200.112.138)       0.0%    10  130.3 125.2 117.8 145.0   7.9
  5. AS3257  zscaler-gw.ip4.gtt.net (77.67.71.210)                 0.0%    10  115.2 115.6 113.6 119.2   1.9
  6. AS22616 165.225.254.243                                       0.0%    10  113.9 115.5 113.7 119.1   2.0
  7. AS22616 104.129.197.230                                       0.0%    10  114.2 116.6 113.6 127.4   4.1
```

- Reverse Path Test

```
Reverse path from: 165.225.72.38 to your Public IP: 82.68.6.76
Start: Sat Aug 24 12:00:53 2019
HOST: cgc00024-a                                                  Loss%   Snt   Last   Avg  Best  Wrst StDev
  1. AS???    172.17.7.58                                          0.0%    10   17.0  19.3  16.9  23.9   2.6
  2. AS22616 165.225.72.3                                          0.0%    10   21.2  21.9  17.9  25.3   2.6
  3. AS6461  ae33.mpr1.fra4.de.zip.zayo.com (94.31.30.233)         0.0%    10   17.7  21.3  17.4  28.0   3.3
  4. AS6461  ae8.mpr1.fra3.de.zip.zayo.com (64.125.26.233)         0.0%    10   21.7  23.8  17.8  37.7   5.7
  5. AS6461  ae27.cs1.fra6.de.eth.zayo.com (64.125.31.216)         0.0%    10   27.7  30.5  27.6  35.2   3.1
  6. AS6461  ae2.cs1.ams17.nl.eth.zayo.com (64.125.29.59)          0.0%    10   31.5  31.3  27.3  40.0   3.6
  7. AS6461  ae0.cs1.ams10.nl.eth.zayo.com (64.125.29.80)          0.0%    10   39.1  31.8  27.4  39.1   3.9
  8. AS6461  ae2.cs1.lhr15.uk.eth.zayo.com (64.125.29.17)          0.0%    10   34.2  40.6  29.1  56.9   9.9
  9. AS6461  ae1.mcs1.lhr15.uk.eth.zayo.com (64.125.29.129)        0.0%    10   27.1  30.9  27.1  42.0   4.8
 10. AS???    lonap-1.zen.net.uk (5.57.80.48)                      0.0%    10   30.1  33.1  27.8  42.0   4.9
 11. AS13037 vl-50.ae43.agg2.lond1.ptn.zen.net.uk (51.148.73.54)   0.0%    10   33.7  31.3  29.0  33.7   1.7
 12. AS13037 ae-9.cor2.lond1.ptn.zen.net.uk (51.148.73.17)         0.0%    10   53.0  47.9  28.4 167.1  42.5
 13. AS13037 82-68-6-78.dsl.in-addr.zen.co.uk (82.68.6.78)         0.0%    10   31.5  35.4  31.5  40.2   3.6
 14. AS???    ???                                                 100.0    10    0.0   0.0   0.0   0.0   0.0
```

9.2 CSC Admin Tasks

```
CSC Admin tasks
5) AWS SSM Agent (Register or De-Register)
6) Change SSH Password
7) Change Timezone
```

5. AWS SSM Agent (Register or De-Register)

6. Change SSH Password: Allows to change the password of the CSC.

7. Change Timezone: In case if needed, you can select your Timezone here.

9.2.1 AWS SSM Agent (Register / De-Register)

The CSC GRE can be integrated as "Managed Instance" with Amazon Cloud (AWS).

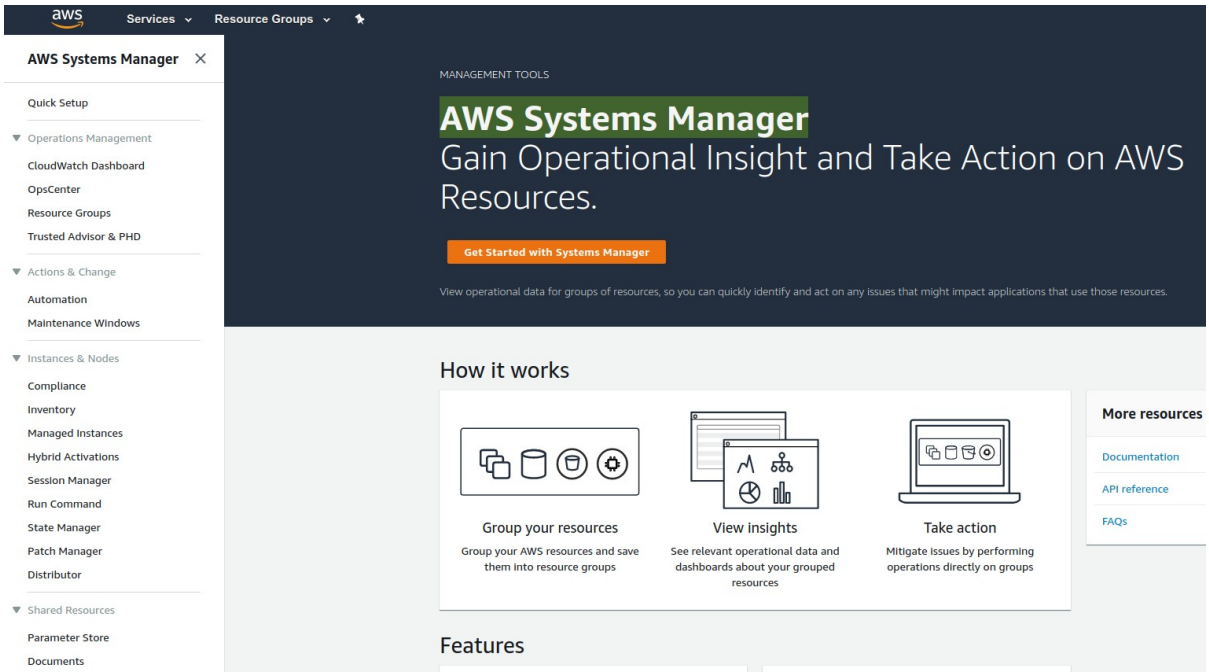
Amazon AWS offers on the Free Tier Account (https://aws.amazon.com/free) the capability to add up to 1000 managed instances.

The steps required to add the CSC to AWS are two:

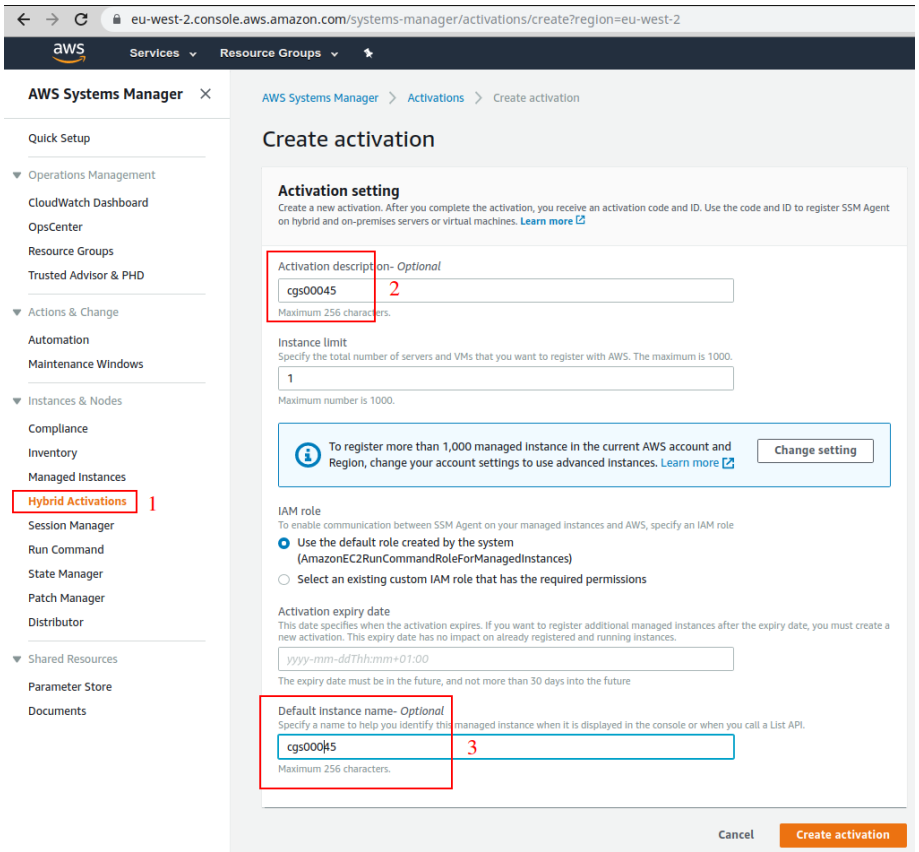
1. Create the Keys to register using "Hybrid Activation".
2. Register the CSC with the Keys

9.2.1.1 Create the Key using "Hybrid Activations"

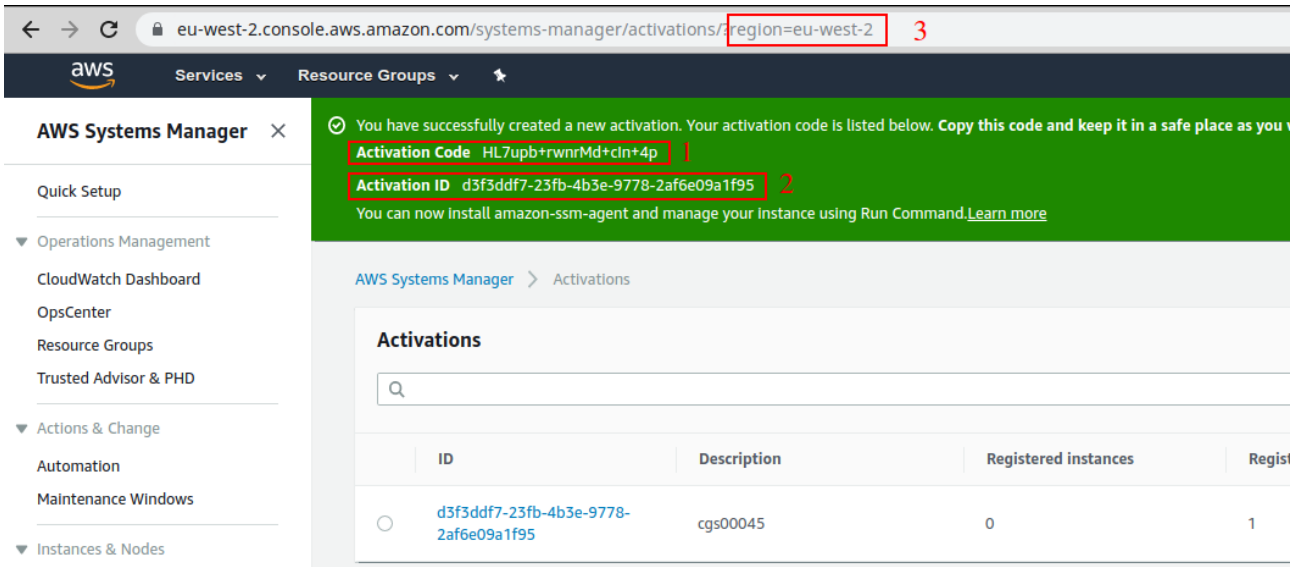
1. Open your AWS console and go to: "AWS Systems Manager"



2. Click “Hybrid Activations”. We recommend to put the name to identify the CSC on “Activation Description” and “Default Instance Name”. In this example is cgs00045



3. Click “Create activation” to generate the Keys. Please, also note the AWS Region



9.2.1.2 Register the CSC on AWS

Using the Keys and Region from the Step before, register the CSC.

1. From the CSC Admin Tasks Menu, select “5) AWS SSM Agent (Register or De-Register)”

```
CSC Admin tasks
5) AWS SSM Agent (Register or De-Register)
6) Change SSH Password
7) Change Timezone
```

2. Register using the Keys and region:

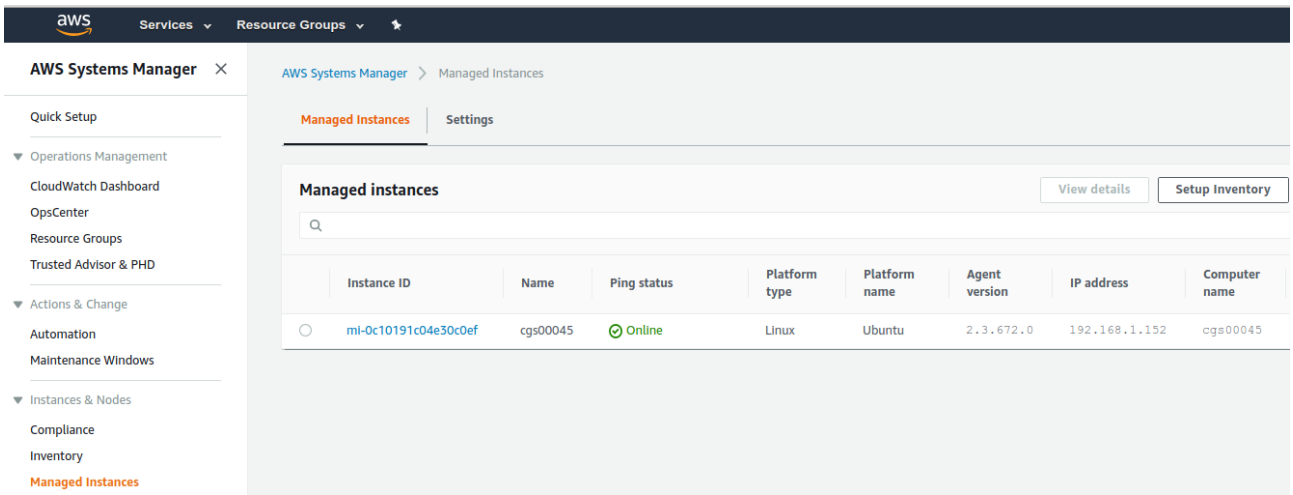
```
Selection: 5   1

AWS SSM Agent is not registered

Do you want to Register (start) the AWS SSM Agent (y/n) y   2
Please, ingress Activation Code, Activation ID and Region (example: eu-west-1)
Activation Code :HL7upb+rwnrMd+cIn+4p   3
Activation ID :d3f3ddf7-23fb-4b3e-9778-2af6e09a1f95   4
Region :eu-west-2   5
                                                                          6
AWS SSM Agent is active (running) since Sat 2019-08-24 14:35:57 UTC; 22ms ago
Registration values: {"ManagedInstanceID":"mi-0c10191c04e30c0ef","Region":"eu-west-2"}
```

Done! You have the CSC integrated with AWS now with the instance-id “mi-xxxxxxxxx” (“mi-0c10191c04e30c0ef” in this example).

Go to AWS System Manager → Managed Instances you will be able to see your CSC.



9.2.1.3 Checking the status of the AWS SSM agent

The “Show Configuration and Status” Menu shows the status of the AWS SSM agent at the bottom.

```
AWS SSM AGENT
AWS SSM Agent is active (running) since Sat 2019-08-24 14:35:57 UTC; 7min ago
Registration values: {"ManagedInstanceID":"mi-0c10191c04e30c0ef","Region":"eu-west-2"}
```

IMPORTANT: Go to Appendix B to learn how to “Run Commands” from the AWS console to monitoring the CSC and Update Bypass Lists.

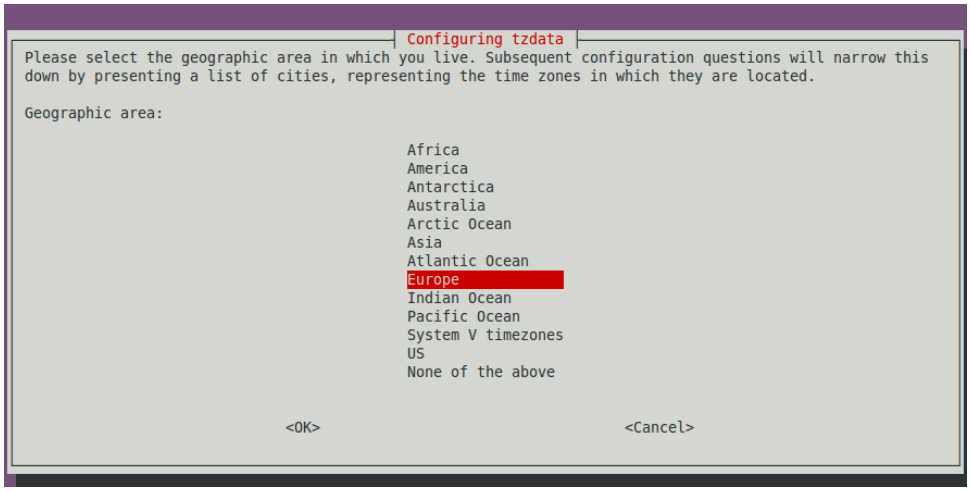
9.2.2 Change SSH Password

From this menu, you can change the SSH Password of the Admin Console.

```
Selection: 6
Changing password for cscadmin.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

9.2.3 Change Timezone

You can change the Timezone from following this Menu:



9.3 Bypass Proxy

The Bypass Proxy allows you to connect certain allowed Domains direct to Internet when using PAC files (or Zapp on Tunnel and Local Proxy).

By default, all domains are blocked and you need to insert the domains that you want to allow to go direct.

```
Bypass Proxy
8) View Current Bypass List
9) Configure Bypass List
```

Important about domains and wildcards. The CSC uses the same nomenclature than Zscaler, but the PAC files are different. Please note the following examples:

CSC	PAC file
Www.example.com	Www.example.com
.example.com	*.example.com
Important! Be careful not to create an "Open Proxy" setting something like ".com" that will allow to pass all domains ending on ".com"	

9.3.1 View Current Bypass List

This commands shows the current domains and subdomains allows to go direct to Internet

9.3.2 Configure Bypass List

In order to configure the Bypass List you have two options:

```
Selection: 9

Please, select method to configure Bypass List

1) Auto - Bypass PAC URL
2) Manual
3) Quit
Enter your choice:
```

9.3.2.1 1) Auto – Bypass PAC URL

This is the recommended method to use. You need to create a "Bypass PAC file" on your Zscaler console. The CSC will read the "Bypass List" from the "Bypass PAC file".

By default, the CSC has configured this PAC URL:

*http://pac.<**yourcloudname**>.net/<**yourdomain**>/cscbypass.pac*

** You can change this URL via console menu. You can use an internal URL if you want.*

The idea of the "Bypass PAC file" is to act a central repository of all bypasses required. Moreover, if you are managing the CSCs using AWS, you can update all CSCs in your network doing one AWS Run Command.

Example of "Bypass PAC file"

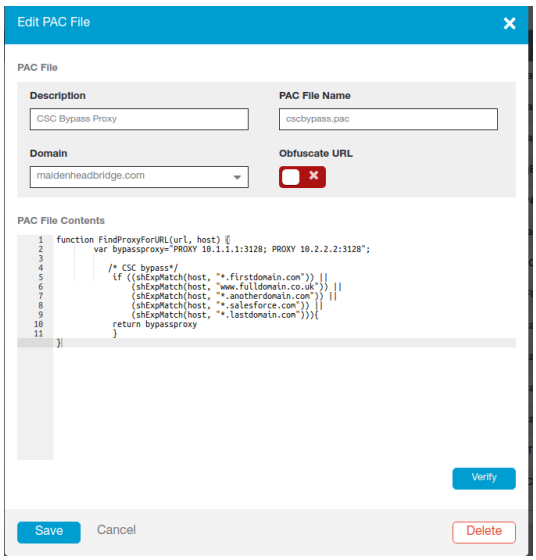
```
function FindProxyForURL(url, host) {
      var bypassproxy="PROXY 1.1.1.1:3128; PROXY 2.2.2.2:3128";

        //* CSC bypass*/
         if ((shExpMatch(host, "*.firstdomain.com")) ||
                        (shExpMatch(host, "www.fulldomain.co.uk")) ||
                        (shExpMatch(host, "*.anotherdomain.com")) ||
                        (shExpMatch(host, "*.salesforce.com")) ||
                        (shExpMatch(host, "*.lastdomain.com"))){
                return bypassproxy
                }
}
```

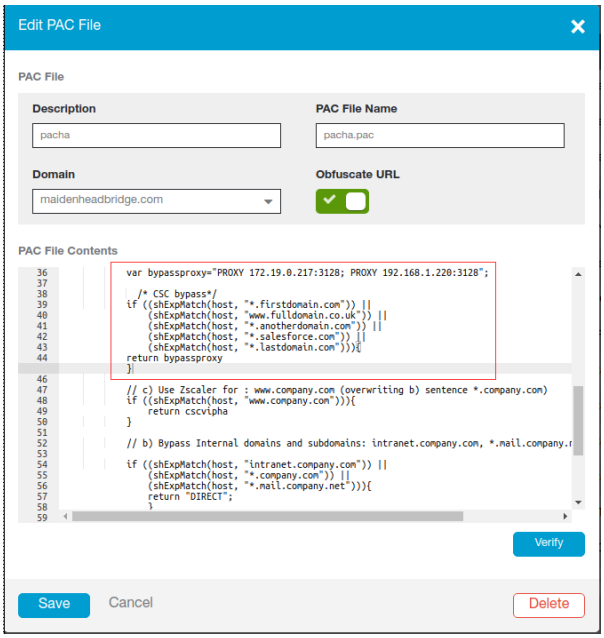
Important Note: It is mandatory to use this function and format. Feel free to add lines but don't change the format. We recommend to start filling the first line and the last line. Use middle lines for copy/paste.

*Note: You can use the lines in **bold** to copy/paste in your production pac file. Please, pay attention to replace 1.1.1.1 and 2.2.2.2 for your real Bypass proxy addresses.*

Bypass Proxy on the Zscaler Console:



For example, here is a production pac file with the bypasses added:



Important: Proxy Bypass is reachable only on port TCP 3128

Configuration Steps:

1. Select 1) Auto – Bypass PAC URL, you are invited to change the Bypass PAC URL, here an screenshoot:

```
Enter your choice: 1

Your current Bypass PAC URL is http://pac.zscalerthree.net/maidenheadbridge.com/cscbypass.pac

1) Update Bypass List
2) Change Bypass PAC URL
3) Quit
Enter your choice:
```

2. From here you can:

   (a) 1) Update Bypass List

   - Select 1)
   - Yes to Refresh Bypass List. The CSC will download and display the PAC file content.
   - Say “y” (yes) to apply the changes.
   - Verify that “Bypass List updated successfully” or correct errors.

```
1) Update Bypass List
2) Change Bypass PAC URL
3) Quit
Enter your choice: 1   1

Do you want to refresh Bypass List? (y/n)? y   2

This is your current Bypass List

.firstdomain.com
www.fulldomain.co.uk
.anotherdomain.com
.salesforce.com
.lastdomain.com


Do you want apply changes? (y/n)? y   3

Bypass List updated sucessfully   4
```

Or

(b) 2) Change Bypass PAC URL

Using this Menu you can change the PAC URL and to refresh the bypass list.

```
2) Change Bypass PAC URL
3) Quit
Enter your choice 2   1

Please, ingress Bypass PAC URL
Bypass PAC URL:http://pac.zscalerthree.net/maidenheadbridge.com/cscbypass.pac   2


Your current Bypass PAC URL is: http://pac.zscalerthree.net/maidenheadbridge.com/cscbypass.pac

Do you want to refresh Bypass List? (y/n)? y   3

This is your current Bypass List

.firstdomain.com
www.fulldomain.co.uk
.anotherdomain.com
.salesforce.com
.lastdomain.com


Do you want apply changes? (y/n)? y   4

Bypass List updated sucessfully   5
```

IMPORTANT: Go to Appendix B to learn how to Update Bypass List from AWS

9.3.2.2 2) Manual

If you want to update manually your bypass list, follow this steps

1. Select Option 2)

```
2) Manual
3) Quit
Enter your choice: 2

Please, read the instructions carefully:

You are going to edit the list using NANO editor

The following formats are accepted:

Full Domains:  'www.example.com'
Wildcard for subdomains: '.example.com' - This will allow all subdomains of example.com

To save, press CTRL-X and 'Yes'

Paid attention to ERROR messages if any. ERRORs must be corrected before to continue

Do you want to continue? (y/n)?
```

2. Ingress “y”

```
  GNU nano 2.5.3                    File: domains                          Modified

.firstdomain.com
www.fulldomain.co.uk
.anotherdomain.com
.salesforce.com
.lastdomain.com
.maidenheadbridge.com

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     ^Y Prev Page
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line  ^V Next Page
```

3. Add / Delete / Modify your full domains and subdomains
4. Please, CTL+X and “Yes” (and after next prompt Enter) to Save
5. The modified Bypass List will be displayed.

```
This is your current Bypass List

.firstdomain.com
www.fulldomain.co.uk
.anotherdomain.com
.salesforce.com
.lastdomain.com
.maidenheadbridge.com


Do you want apply changes? (y/n)?
```

6. Apply Changes (y) or discard (n). If “y” you will receive the following message:

```
Do you want apply changes? (y/n)? y

Bypass List updated sucessfully


Press ENTER to continue
```

9.4 Log Information

This section shows the tunnel logs (UP/DOWN) and the Cluster changes on the CSC GRE Cluster.

It is possible to view the current month and the last 6 months logs.

```
Log Information
10) View Current Month
11) View Last 6 Months
```

9.4.1 SysLog Server information examples:

CSC GRE Single

```
Selection: 10

Current Month (August 2019) Logs for cgs00045

Aug  5 19:43:39 root: (MHB-CSC)(DOWN) No active tunnel since: Mon  5 Aug 19:43:39 UTC 2019
Aug 24 07:08:56 root: (MHB-CSC)(UP) Primary tunnel is active since: Sat 24 Aug 07:08:56 UTC 2019
Aug 24 10:23:42 root: (MHB-CSC)(DOWN) No active tunnel since: Sat 24 Aug 10:23:42 UTC 2019
Aug 24 10:29:51 root: (MHB-CSC)(UP) Secondary tunnel is active since: Sat 24 Aug 10:29:51 UTC 2019
Aug 24 10:44:07 root: (MHB-CSC)(UP) Primary tunnel is active since: Sat 24 Aug 10:44:07 UTC 2019

Press ENTER to continue
```

CSC GRE Cluster:

```
Selection: 10

Current Month (August 2019) Logs for cgc00024-a

Aug  8 10:14:11 root: (MHB-CSC)(STANDBY) cgc0000x-b is Cluster StandBy - No active tunnels
Aug  8 12:04:26 root: (MHB-CSC)(STANDBY) cgc00024-a is Cluster StandBy - No active tunnels
Aug  8 11:51:47 root: (MHB-CSC)(UP) Primary tunnel is active since: Thu  8 Aug 11:51:47 UTC 2019
Aug  8 11:51:47 root: (MHB-CSC)(ACTIVE) cgc00024-a is Cluster Active
Aug  9 19:52:48 root: (MHB-CSC)(DOWN) No active tunnel since: Fri  9 Aug 19:52:48 UTC 2019
Aug  9 19:53:19 root: (MHB-CSC)(UP) Secondary tunnel is active since: Fri  9 Aug 19:53:19 UTC 2019
Aug  9 20:03:39 root: (MHB-CSC)(UP) Primary tunnel is active since: Fri  9 Aug 20:03:39 UTC 2019
Aug  9 20:22:11 root: (MHB-CSC)(DOWN) No active tunnel since: Fri  9 Aug 20:22:11 UTC 2019
Aug  9 20:22:43 root: (MHB-CSC)(UP) Secondary tunnel is active since: Fri  9 Aug 20:22:43 UTC 2019
Aug  9 20:33:02 root: (MHB-CSC)(UP) Primary tunnel is active since: Fri  9 Aug 20:33:02 UTC 2019
Aug 13 12:23:17 root: (MHB-CSC)(STANDBY) cgc00024-a is Cluster StandBy - No active tunnels
Aug 13 12:23:35 root: (MHB-CSC)(DOWN) No active tunnel since: Tue 13 Aug 12:23:35 UTC 2019
Aug 13 12:38:18 root: (MHB-CSC)(STANDBY) cgc00024-a is Cluster StandBy - No active tunnels
Aug 13 12:28:00 root: (MHB-CSC)(UP) Primary tunnel is active since: Tue 13 Aug 12:28:00 UTC 2019
Aug 13 12:28:00 root: (MHB-CSC)(ACTIVE) cgc00024-a is Cluster Active
Aug 13 15:46:25 root: (MHB-CSC)(DOWN) No active tunnel since: Tue 13 Aug 15:46:25 UTC 2019
Aug 13 16:01:01 root: (MHB-CSC)(STANDBY) cgc00024-a is Cluster StandBy - No active tunnels
Aug 13 15:48:15 root: (MHB-CSC)(UP) Primary tunnel is active since: Tue 13 Aug 15:48:15 UTC 2019
Aug 13 15:48:15 root: (MHB-CSC)(ACTIVE) cgc00024-a is Cluster Active

Press ENTER to continue
```

9.5 Configuration Wizards

This section allows to:

```
Configuration Wizards
12) Change GRE IPs, DNS servers, Cloudname, Syslog and more
13) Switch Tunnels - Primary / Secondary
```

9.5.1 Change GRE IPs, DNS, Cloudname, Syslog

If you want to change this parameters, go to Menu 12) and follow the Wizard.

Menu “12) Change GRE IPs, DNS servers, Cloudname, Syslog and more” will show the current values configured and will allow change all of them.

```
Selection: 12

Welcome to the CSC GRE Configuration Wizard

Before to start you need have the following values ready:

1) Cloudname: zscloud, zscalertwo, zscaler,etc. Check your Zscaler Admin URL https://admin.<cloud name>.net to find it
2) DNS Servers IPs
3) GRE Tunnel IPs: To obtain it, please submit a ticket to Zscaler Support asking for GRE tunnel IPs from Public IP 82.68.6.73
4) (Optional) Bypass Proxy PAC URL
5) (Optional) Syslog / SIEM Server/s IP/s and TCP port

Current Values Configured:
-------------------
Cloudname: zscalerthree
-------------------
DNS Servers: 172.19.0.100 ; 172.19.0.134
-------------------
Tunnel Source IP:    82.68.6.73 (* this is your Tunnel Source Public IP)

Primary Destination:    165.225.16.36
Internal Router IP:    172.17.4.209/30
Internal ZEN IP:    172.17.4.210/30

Secondary Destination:    165.225.76.39
Internal Router IP:    172.17.4.213/30
Internal ZEN IP:    172.17.4.214/30
-------------------
Bypass Proxy PAC URL
Your current Bypass PAC URL is http://pac.zscalerthree.net/maidenheadbridge.com/cscbypass.pac
-------------------
Syslog / SIEM information

Your current Syslog / SIEM configuration is:

Primary Syslog / SIEM IP: 172.19.0.199
Secondary Syslog / SIEM IP: Not configured
Syslog / SIEM TCP port: 514
-------------------
Are you ready to continue? (y/n)
```

Please, note that a reboot may be required after changing this values.

9.5.2 Switch Tunnels

In certain conditions, it is desired to switch Primary ↔ Secondary tunnel values. Using this Menu 13) you will be able to do it on one step.

Please, note that a reboot is required after this change.

```
13) Switch Tunnels - Primary / Secondary

e) Exit

Selection: 13    1

-------------------
ZSCALER INFORMATION
Zscaler Cloud:  zscalerthree
GRE tunnels egress Public IP:
Primary Tunnel:
                ZEN Public IP: 165.225.16.36
                Tunnel IPs (local/zen): 172.17.4.209 / 172.17.4.210
Secondary Tunnel:                                                    2
                ZEN Public IP: 165.225.76.39
                Tunnel IPs (local/zen): 172.17.4.213 / 172.17.4.214

TUNNEL STATUS
Primary Tunnel (reachability):
                              Layer 7 Keepalive is: Alive
                              GRE ZEN Tunnel IP is: Alive
Secondary Tunnel (reachability):
                              Layer 7 Keepalive is: Alive
                              GRE ZEN Tunnel IP is: Alive

Tunnel Status: Primary tunnel is active since: Sat 24 Aug 10:44:07 UTC 2019

HTTP://IP.ZSCALER.COM PAGE STATUS
You are accessing this host via a Zscaler proxy hosted at London III in the zscalerthree.net cloud
Your Gateway IP Address is 82.68.6.73
-------------------                                   ZEN Node
Do you want to Switch Primary / Secondary Tunnel?
Selecting Yes will reboot the CSC

1) Yes
2) No
Enter your choice: 1    3
The CSC will reboot now!
Connection to 172.19.0.152 closed by remote host.
Connection to 172.19.0.152 closed.
```

And after the reboot, you can check that the tunnel where switched

```
ZSCALER INFORMATION
Zscaler Cloud:  zscalerthree
GRE tunnels egress Public IP: 82.68.6.73
Primary Tunnel:
                ZEN Public IP: 165.225.76.39
                Tunnel IPs (local/zen): 172.17.4.213 / 172.17.4.214
Secondary Tunnel:                                                    1
                ZEN Public IP: 165.225.16.36
                Tunnel IPs (local/zen): 172.17.4.209 / 172.17.4.210

TUNNEL STATUS
Primary Tunnel (reachability):
                              Layer 7 Keepalive is: Alive
                              GRE ZEN Tunnel IP is: Alive
Secondary Tunnel (reachability):
                              Layer 7 Keepalive is: Alive
                              GRE ZEN Tunnel IP is: Alive

Tunnel Status: Primary tunnel is active since: Sat 24 Aug 16:03:21 UTC 2019
                                                      ZEN Node
HTTP://IP.ZSCALER.COM PAGE STATUS
You are accessing this host via a Zscaler proxy hosted at Paris II in the zscalerthree.net cloud.
Your Gateway IP Address is 82.68.6.73
```

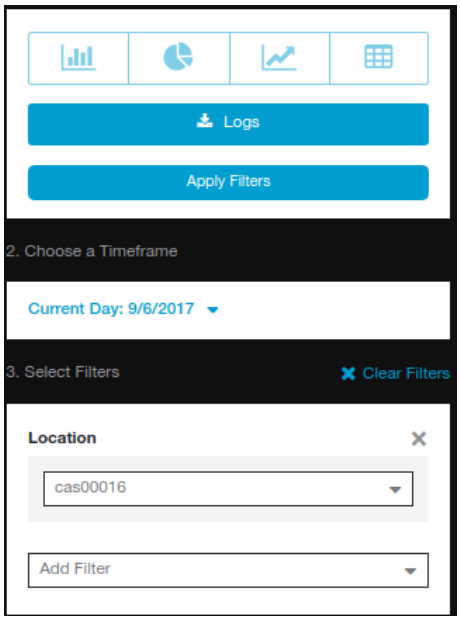
10 Checking full visibility of the transaction on the Zscaler GUI

The most important thing when doing tunnels to the Zscaler Cloud is to do not NAT the connections to the cloud. This allows to see the internal IPs on the Zscaler logs. Having visibility of the internal IPs is a must for full Security and Control.

10.1 Web Logs

Go to Analytics > Web Insights

Click Logs and Filter by Location [cas00016 in this example is the name of the Location]



Apply Filters:

Web Insights

No.	Logged Time	User	URL	Policy Action	URL Category	Client IP	Server IP
158	Wednesday, September 06, 2017 7:24:20 ...	first1last1@maidenheadbri...	www.bbc.co.uk:443	Allowed	News and Media	172.19.0.140	212.58.246.93
159	Wednesday, September 06, 2017 7:24:20 ...	first1last1@maidenheadbri...	edigitalsurvey.com:443	Allowed	Professional Services	172.19.0.140	46.236.9.36
160	Wednesday, September 06, 2017 7:24:20 ...	first1last1@maidenheadbri...	edigitalsurvey.com:443	Allowed	Professional Services	172.19.0.140	46.236.9.36
161	Wednesday, September 06, 2017 7:24:20 ...	first1last1@maidenheadbri...	edigitalsurvey.com:443	Allowed	Professional Services	172.19.0.140	46.236.9.36
162	Wednesday, September 06, 2017 7:24:20 ...	first1last1@maidenheadbri...	homepage.files.bbci.co.uk:443	Allowed	News and Media	172.19.0.140	172.227.98.43
163	Wednesday, September 06, 2017 7:24:20 ...	first1last1@maidenheadbri...	ssl.bbc.co.uk:443	Allowed	News and Media	172.19.0.140	212.58.244.114
164	Wednesday, September 06, 2017 7:24:20 ...	first1last1@maidenheadbri...	search.files.bbci.co.uk:443	Allowed	News and Media	172.19.0.140	172.227.98.43
165	Wednesday, September 06, 2017 7:24:20 ...	first1last1@maidenheadbri...	nav.files.bbci.co.uk:443	Allowed	News and Media	172.19.0.140	172.227.98.43
166	Wednesday, September 06, 2017 7:24:20 ...	first1last1@maidenheadbri...	static.bbc.co.uk:443	Allowed	News and Media	172.19.0.140	172.227.98.43

As you can see, you have full visibility of the Client IP [172.19.0.140 in this case]

More in detail:

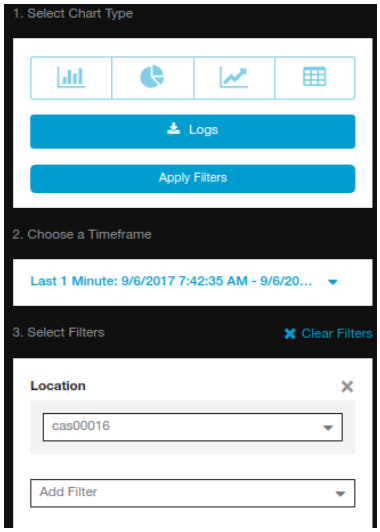
Client IP	Server IP
172.19.0.140	212.58.246.93
172.19.0.140	46.236.9.36
172.19.0.140	46.236.9.36
172.19.0.140	46.236.9.36
172.19.0.140	172.227.98.43

10.2 Firewall Logs

Same than before, with the CSC you will have full visibility on Firewall Logs of your internal IPs.

Go to Analytics > Firewall Insights

Click Logs and Filter by Location [cas00016 in this example is the name of the Location]



Apply Filters

Firewall Insights

No.	Logged Time	DNAT Rule N...	User	Location	Client Source IP	Server Destination IP	Rule Name	Network Service	Network A
16	Wednesday, September 06, 2017 7:42:39 ...	None	first1last1@maidenhead...	cas00016	172.19.0.140	8.8.4.4	Default Firewa...	DNS	DNS
17	Wednesday, September 06, 2017 7:42:42 ...	None	first1last1@maidenhead...	cas00016	172.19.0.140	91.190.217.135	Default Firewa...	TCP	TCP
18	Wednesday, September 06, 2017 7:42:43 ...	None	first1last1@maidenhead...	cas00016	172.19.0.140	157.55.56.164	Default Firewa...	TCP	TCP
19	Wednesday, September 06, 2017 7:42:49 ...	None	first1last1@maidenhead...	cas00016	172.19.0.140	91.190.217.135	Default Firewa...	TCP	TCP
20	Wednesday, September 06, 2017 7:42:56 ...	None	first1last1@maidenhead...	cas00016	172.19.0.140	74.125.133.188	Default Firewa...	TCP	TCP
21	Wednesday, September 06, 2017 7:43:00 ...	None	first1last1@maidenhead...	cas00016	172.19.0.140	91.190.217.135	Default Firewa...	TCP	TCP

More in detail:

Client Source IP	Server Destination IP
172.19.0.140	8.8.4.4
172.19.0.140	91.190.217.135
172.19.0.140	157.55.56.164
172.19.0.140	91.190.217.135
172.19.0.140	74.125.133.188
172.19.0.140	91.190.217.135

11 Troubleshooting

11.1 If the tunnels are not connecting

The "Configuration and Status" menu is providing all information required and is doing all checks for you. Start doing this command to verify everything, from configuration to reachability of gateways, DNS and Zscaler nodes.

According our experience, the most common issues are related to this:

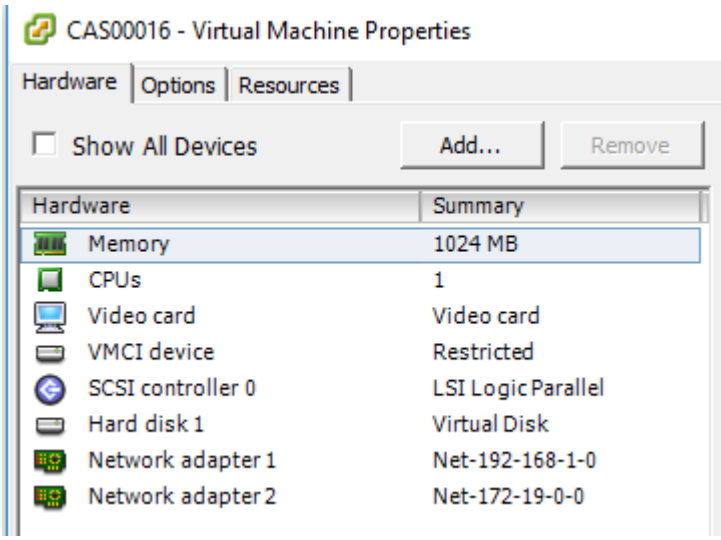
1. ***GRE NAT and firewall rules in general. GRE is not TCP. GRE is a protocol (number 47). In order to do NAT you will required to do a STATIC SOURCE NAT and to allow protocol 47 in both directions.***
2. ***Are Vmware interfaces are properly mapped?***

Please, note that the **first interface** is **EXTERNAL** and the **second** is **INTERNAL.**

In this example:

- Network adapter 1 (EXTERNAL interface) is mapped to Net-192-168-1-0.

- Network adapter 2 (INTERNAL interface) is mapped to Net-172-19-0-0.



3. ***Are the configuration values correct? Check all values again using "Configuration and Status" menu.***

11.2 Proxy Bypass

11.2.1 How to check if the Proxy Bypass is active?

Open a browser, type the IP of your proxy bypass plus (:) proxy port 3128, here the format:

http://<your bypass proxy ip>:3128

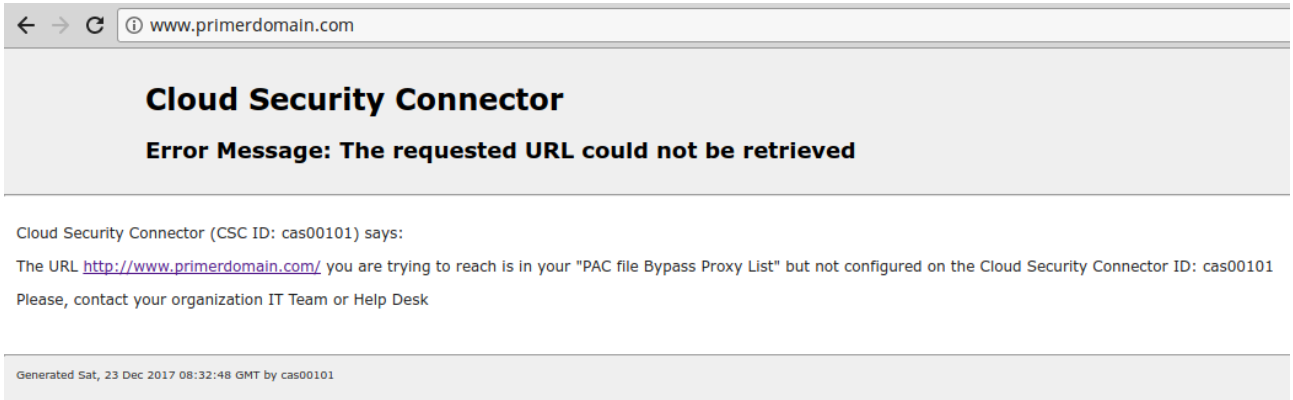
For example: http://172.19.0.217:3128/

and you will received the following page:

Please, note that the CSC ID is showed in this notification. This helps administrators to identify the CSC in case is needed.

11.2.2 If you added the bypass in the PAC but forgot to update the CSC

In the case the bypass Domain Host is in your production PAC file but not configured on the CSC, the user will received the following message:

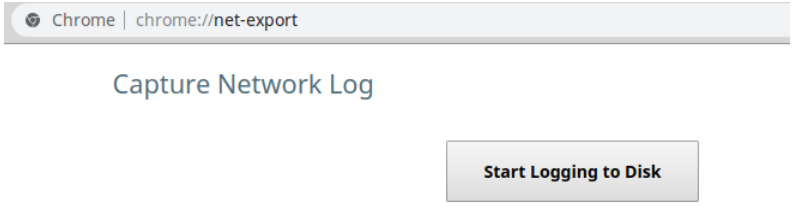


11.3 PAC file troubleshooting

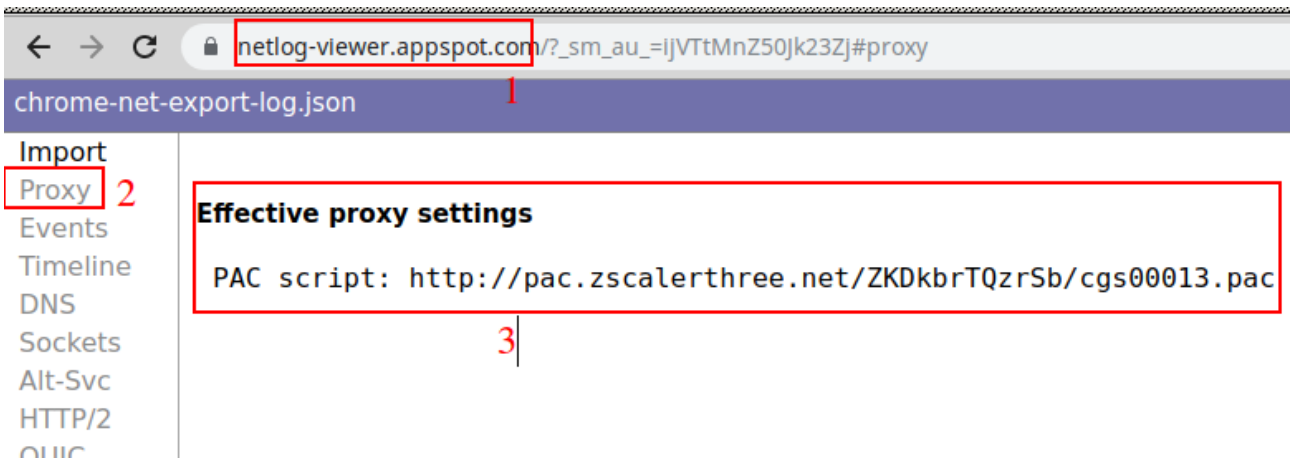
Please, for all this test use “Google Chrome”

11.3.1 How to check what PAC file URL is applied? (Effective Proxy Settings)

1. Using Google Chrome, go to: chrome://net-export/



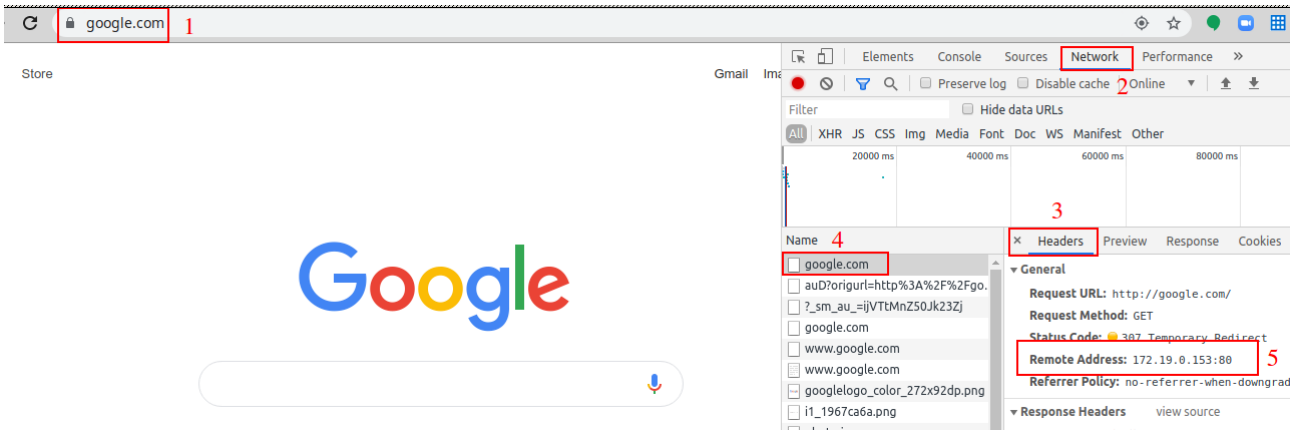
2. Start Logging to Disk. Select a destination file and “Stop Logging”
3. Go to https://netlog-viewer.appspot.com, choose file and go to “proxy”



11.3.2 How to Check if the Domain destination is using VIP Proxy or Bypass Proxy?

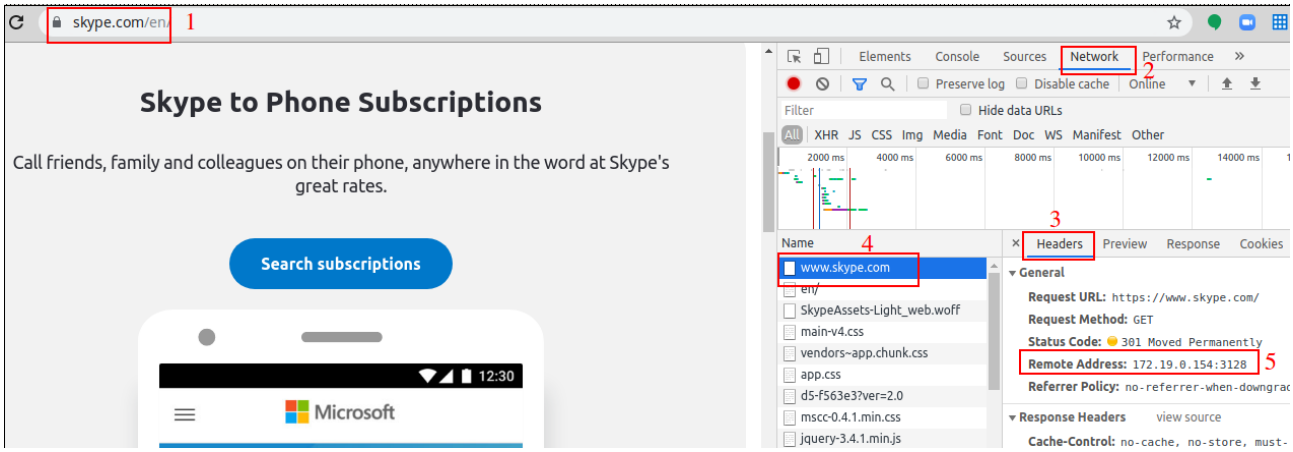
Using Google Chrome, do the following steps:

1. Open Developer Tools (More Tools → Developer Tools or CTRL+SHIFT+I)
2. Type the URL you want to check, for example "www.google.com"
3. Select "Network" → "Headers" and click on the URL. See picture below:



Check "Remote Address". In this case is using 172.19.0.153:80 that is the VIP Proxy IP of the CSC. In this case, the traffic is going via the tunnels.

4. Now go to a URL that you want to check if is going direct to Internet via the Bypass Proxy. In this example, we will use "salesforce.com"



In this case, "Remote Address" is 172.19.0.154:3128 that is the Bypass Proxy IP:Port (:3128) . All Skype traffic is going direct to Internet and not via the tunnels.

```
TRAFFIC REDIRECTION Options
To Zscaler: VIP Proxy: 172.19.0.153:80 (or :9400) | Route all traffic via CSC GW IP | Zscaler Global Proxies (port 80/9400) via CSC GW IP
Direct to Internet: Bypass Proxy: 172.19.0.154:3128 | Zscaler Global Proxies (port 3128) via CSC GW IP
```

12 Maidenhead Bridge Contact Information

Website: www.maidenheadbridge.com

Sales enquiries: sales@maidenheadbridge.com

Support: http://support.maidenheadbridge.com

13 Appendix A – PAC File Example

Click here to obtain a PAC file example that will help to redirect traffic to Zscaler and to do Local Bypasses or Direct bypasses to Internet.

14 Appendix B – “Run Commands” from AWS to monitor the CSC

When you have your CSC registered on AWS as “managed instance” you can execute the “Monitoring Tasks” and also to “Update Bypass List”. This is particular important if you have several CSC and you want to update all in one task.

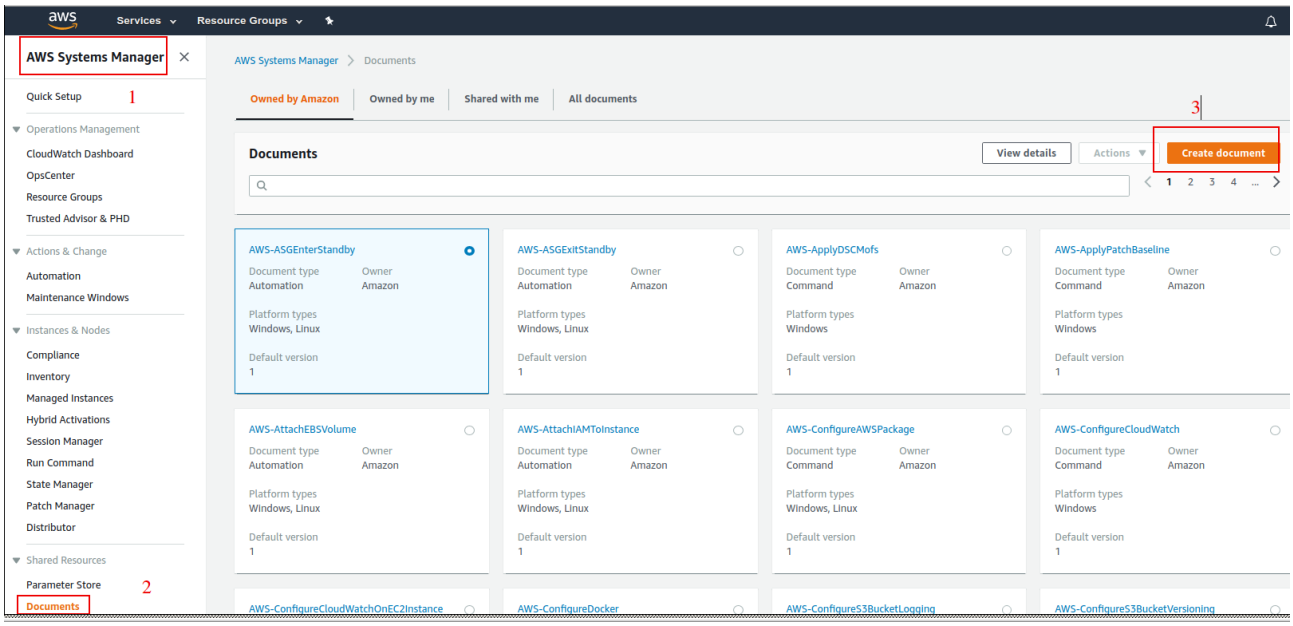
14.1 Documents

To execute “Run Commands” you need to have “Documents”. “Documents” contains a series of commands to execute. For simplicity purposes, we provide the “Documents” required for the operations of the CSC.

To obtain the Documents required you can open a ticket to http://support.maidenheadbridge.com (indicating your AWS Account ID) or to create them manually Copying/Pasting the information that follows.

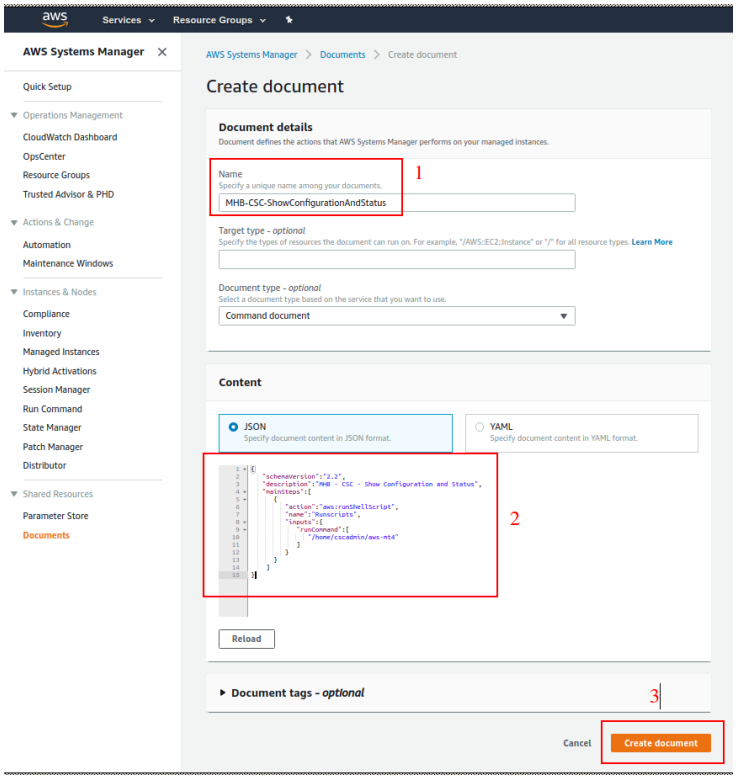
14.1.1 Creating a Document

From AWS System Manager → Document → Create Document

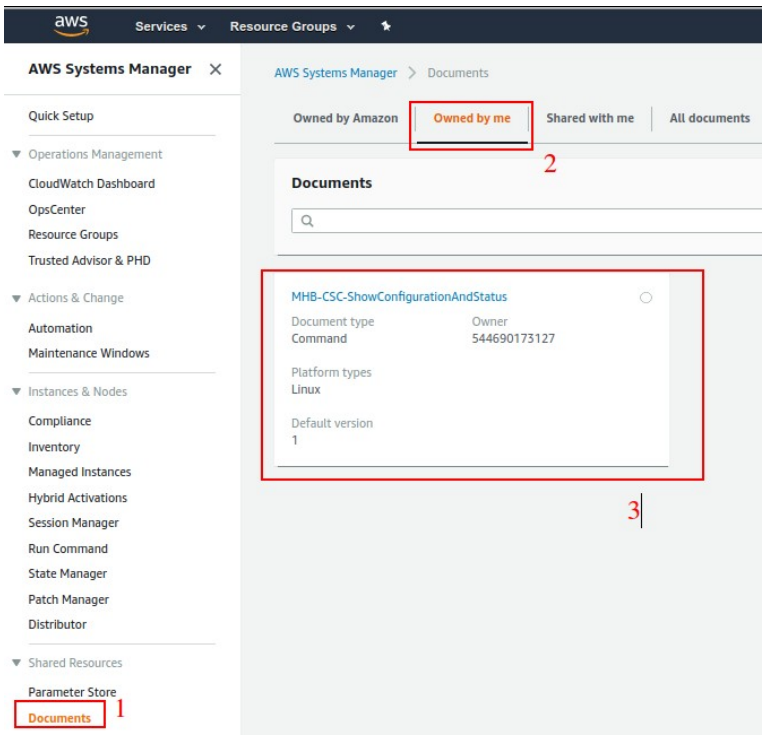


Next steps are:

1. Put the Name of the Document
2. Copy/Paste the content
3. Click “Create document”



Check the document created going to “Owned by me”



On the following section you will find all documents with Name and Content. Please, create all of them on your console.

14.1.2 List of Documents

Please, create the “Documents” using this values:

Name	MHB-CSC-ShowConfigurationAndStatus

Content	{
	"schemaVersion":"2.2",
	"description":"MHB - CSC - Show Configuration and Status",
	"mainSteps":[
	{
	"action":"aws:runShellScript",
	"name":"Runscripts",
	"inputs":{
	"runCommand":[
	"/home/cscadmin/aws-mt4"
	]
	}
	}
	]
	}

Name	MHB-CSC-SpeedTest

Content	{
	"schemaVersion":"2.2",
	"description":"MHB - CSC - Speed Test",
	"mainSteps":[
	{
	"action":"aws:runShellScript",
	"name":"Runscripts",
	"inputs":{
	"runCommand":[
	"/home/cscadmin/aws-mt7"
	]
	}
	}
	]
	}

Name	MHB-CSC-TraceRouteAndLatencyTest

Content	{
	"schemaVersion":"2.2",
	"description":"MHB - CSC - TraceRoute and Latency Test",
	"mainSteps":[
	{
	"action":"aws:runShellScript",
	"name":"Runscripts",
	"inputs":{
	"runCommand":[
	"/home/cscadmin/aws-mt6"
	]
	}
	}
	]
	}

Name	MHB-CSC-UpdateBypassList

Content	{
	"schemaVersion":"2.2",
	"description":"MHB - CSC - Update Bypass List",
	"mainSteps":[
	{
	"action":"aws:runShellScript",
	"name":"Runscripts",
	"inputs":{
	"runCommand":[
	"/home/cscadmin/aws-bp-refresh-list"
	]
	}
	}
	]
	}

Name	MHB-CSC-ShowLogCurrentMonth

Content	{
	"schemaVersion":"2.2",
	"description":"MHB - CSC - Show Log Current Month",
	"mainSteps":[
	{
	"action":"aws:runShellScript",
	"name":"Runscripts",
	"inputs":{
	"runCommand":[
	"/home/cscadmin/aws-l-current-month"
	]
	}
	}
	]
	}

Name	MHB-CSC-ShowLogCurrentMonth-2500Characters

Content	{
	"schemaVersion":"2.2",
	"description":"MHB - CSC - Show Log Current Month - (last 2500 characters)",
	"mainSteps":[
	{
	"action":"aws:runShellScript",
	"name":"Runscripts",
	"inputs":{
	"runCommand":[
	"/home/cscadmin/aws-l-current-month-2500"
	]
	}
	}
	]
	}

Name	MHB-CSC-ShowLogLastSixMonths

Content	{
	"schemaVersion":"2.2",
	"description":"MHB - CSC – Show Log Last Six Months",
	"mainSteps":[
	{
	"action":"aws:runShellScript",
	"name":"Runscripts",
	"inputs":{
	"runCommand":[
	"/home/cscadmin/aws-l-last-6-months"
	]
	}
	}
	]
	}

Name	MHB-CSC-SwitchTunnels

Content	{
	"schemaVersion": "2.2",
	"description": "MHB - CSC - Show Configuration and Status",
	"mainSteps": [
	{
	"action": "aws:runShellScript",
	"name": "Runscripts",
	"inputs": {
	"runCommand": [
	"/home/cscadmin/aws-tun-switch"
	]
	}
	}
	]
	}

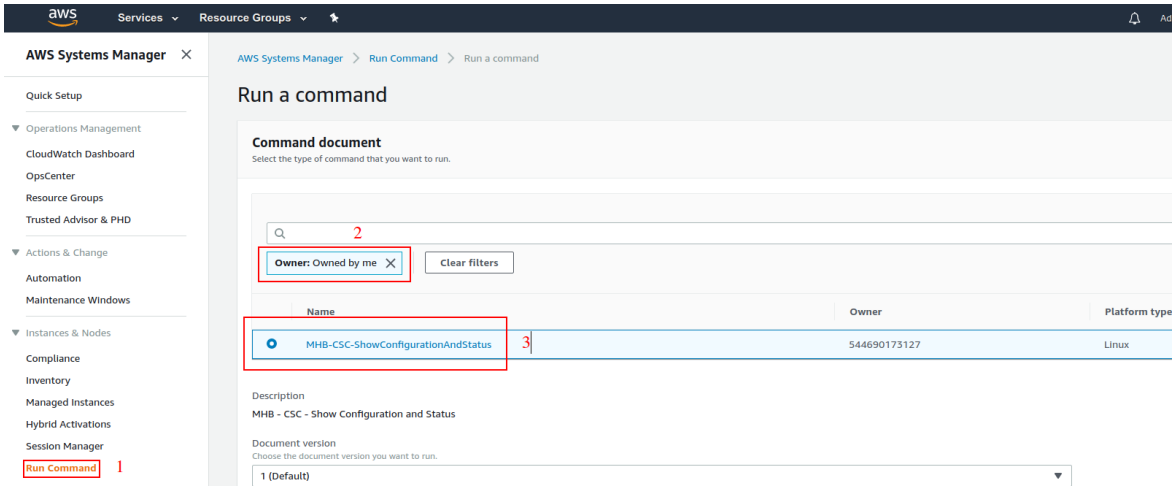
14.2 Run Commands

After you created the Documents, you are ready to Run Commands on the CSC.

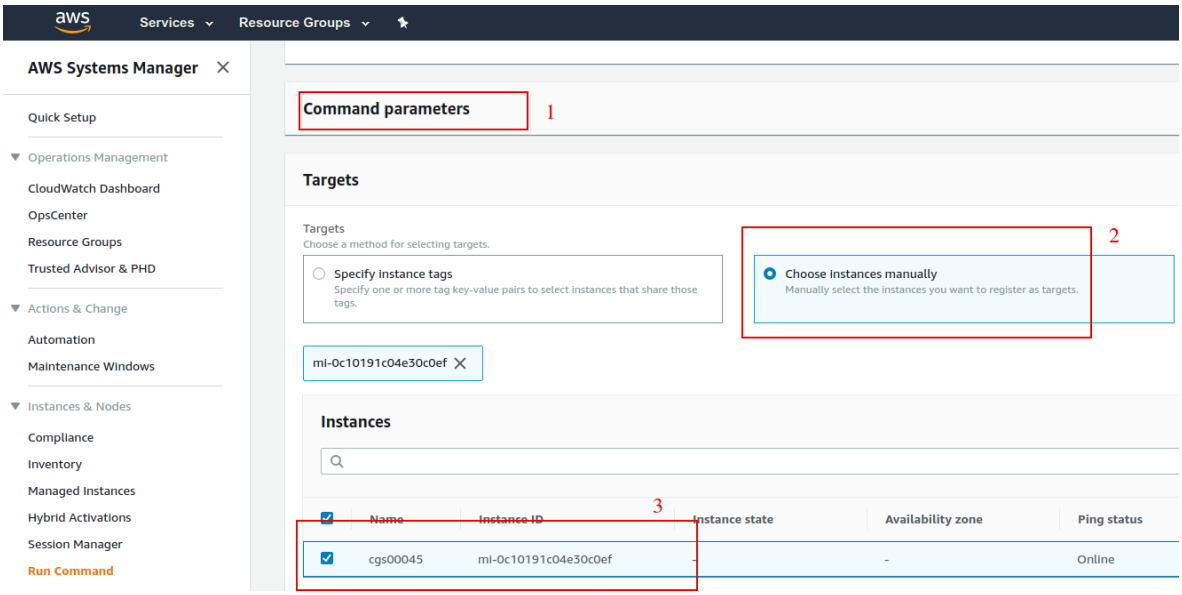
You can see the results of the operation on the “Output” section or to store the results on a S3 Buckets for further inspection.

Note: The “Output” Section allows only 2500 characters. The Traceroute and Latency Test uses more than 2500. We recommend to store this command on a S3 bucket directly.

1. To Run Commands go to: AWS Systems Manager → Run Command and Select the “Command Document”

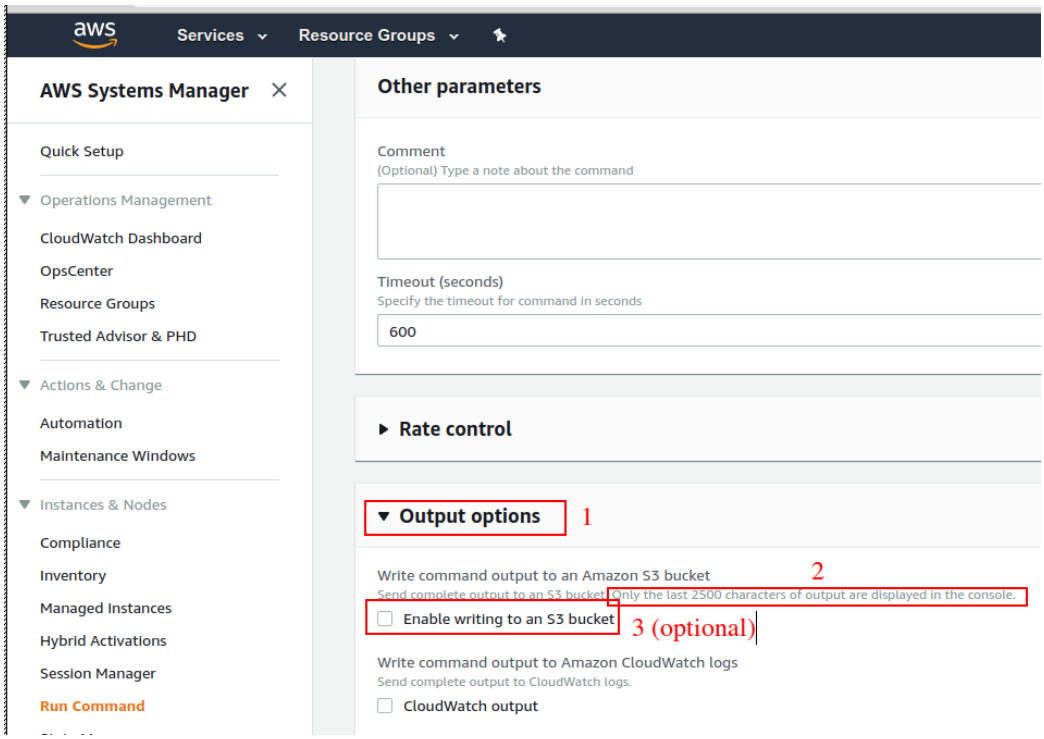


2. Scroll Down and Select the Instance:

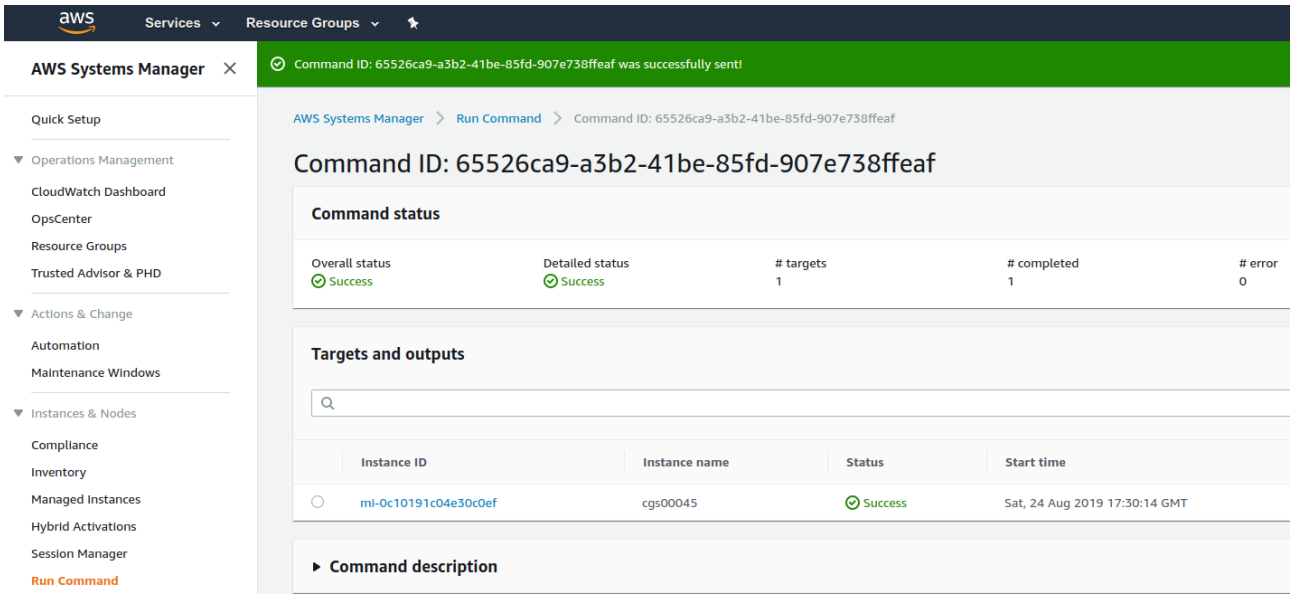


3. Scroll more down and Select “Output Options”

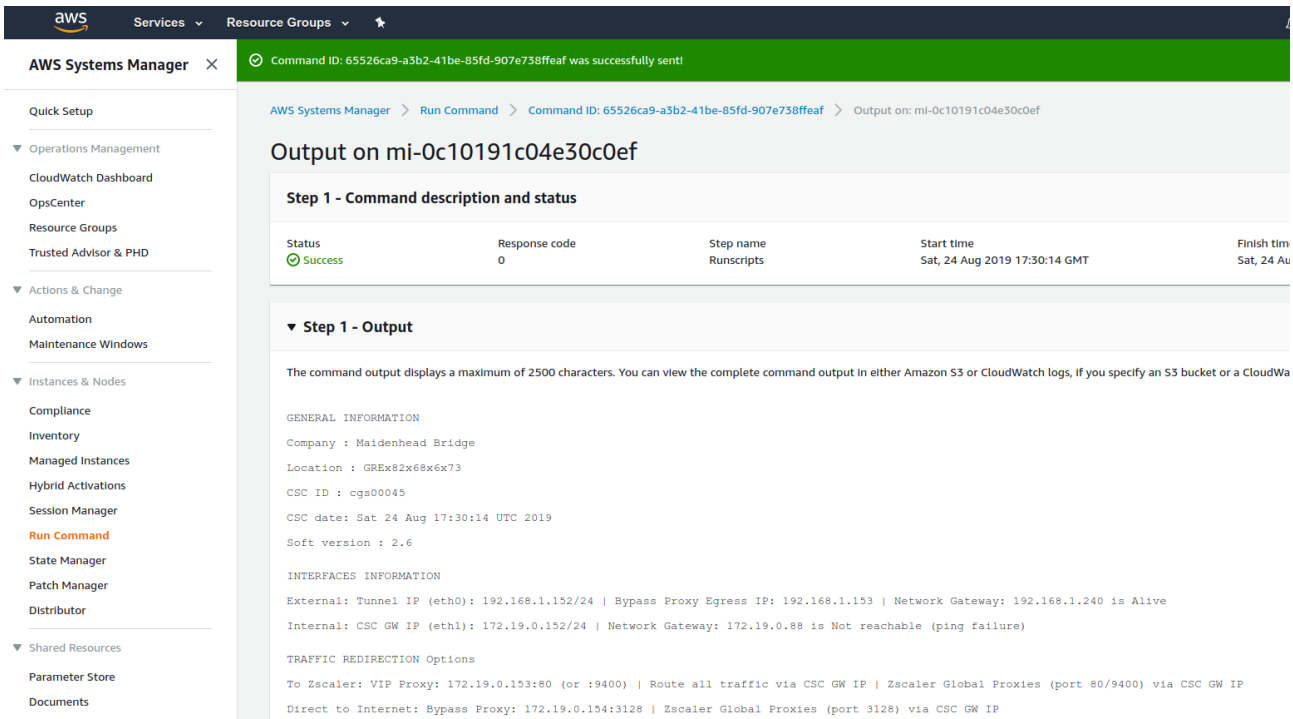
Here you can send to the Output to the console (up to 2500 characters) or to an S3 bucket or other options.



4. Finally, Click “Run”
5. Wait to complete (Success)



6. Click “Instance ID” and expand “Output”



7. Scroll down the “Output” to see the complete result of the command.

15 APPENDIX C: Release Notes

Version 2.6 comes with the following enhancements:

- NEW! Configuration Wizard. It is possible now to change via SSH Console the following parameters: GRE credentials, DNS servers, Cloudname and Syslog servers.
- NEW! Switch tunnels. It is possible now to switch Primary / Secondary via SSH console.
- Change: The default template of the OVA file requires 2 x CPU, 4 GB RAM, 8 GB disk. This increase was done due to the intensive use of the Bypass Proxy functionality by our customers. If you are sending most of the traffic to via tunnels, you can reduce it to 1 x CPU, 1 GB RAM.

Version 2.5 comes with the following enhancements:

- NEW! Zscaler Global Proxies accepted for Bypass Proxy (port :3128). Now, on the CSC, it is possible to use the Zscaler Global Proxies IPs (Ranges 185.46.212.88-93 and 185.46.212.97-98) to redirect traffic to the CSC Bypass Proxy. You need to point your bypass URLs to (example) : PROXY 185.46.212.88:3128 . This feature was requested by several customers in order to create a unique global pac file using the Zscaler Global Proxies.
- Some cosmetic menu changes.

Version 2.3 comes with the following enhancements:

- Logs to Syslog server. On version 2.3 you can setup one or two Syslog servers where to send the information about Tunnel and Cluster.
- Menu Changes: Two new options added to see the last month logs or last 6 months.

Version 2.2 comes with the following enhancements:

- DNS Resolver timeout reduced to improve response of time of Bypass Proxy when Primary DNS fails or is slow.
- Cosmetic changes on "Show Configuration and Status" menu.

Version 2.1 comes with the following enhancements:

- Watchdog application added. This watchdog will prevent any potential deviation behaviour or memory leak of the process running on the CSCs.
- Bypass proxy allows tunnelling to non standard HTTPS ports. This was requested by several customers using Cloud Services like SAP.

Version 2.0 comes with the following enhancements:

- New! Bypass Proxy functionality : The Bypass Proxy solves the problem when is required to send traffic direct to internet and not via Zscaler ZEN nodes.The most common case is when destination web site accepts only traffic coming from a specific public IP.Without the Bypass Proxy, customers where obligated to have an internal proxy or to configure several firewall rules and routes to the destinations required to be bypassed.The Bypass Proxy simplifies this task: using the Zscaler PAC files servers as repository of your bypasses and automating the task with AWS, you can easily get up to date all your bypasses in all CSC instances.The Bypass Proxy acts as Web Firewall. It only allows to reach domains hosts defined by the Administrator.
- Resilient Algorithm: When returning to the Primary ZEN, Resilient Algorithm checks if the Primary ZEN was stable for 10 minutes before to change nodes.
- Timers: Timers were adjusted to better support locations with long delays (more than 250 ms) to the ZEN Nodes.
- Internal IPs: The CSC GRE Cluster is using now five consecutive IPs for the Internal side. The first one is the Internal Cluster IP, the second the VIP Proxy, the third is the Bypass proxy, the fourth is the interface of the csc-gre-a and the fifth the csc-gre-a.
- External IPs: The CSC GRE Cluster is using now fourth consecutive IPs for the External side. The first one is the External Cluster IP, the second the Egress Bypass, the third is the interface of the csc-gre-a and the fourth the csc-gre-a.
- New! Monitoring Tasks Menu: Traceroute and Latency Test. This Test does a MTR (MyTraceRoute) test to Primary & Secondary ZEN and Google DNS. In addition to this, if the tunnel is UP, this test does a MTR test on Reverse from the Zscaler node active to your public IP. This test is similar than the one provided on the Zscaler Analyzer tool with the advantage that has the ability to analyse the reverse path as well.
- New! Monitoring Tasks Menu: Speed Test (Experimental). This test uses a third party tool: speedtest.net . This test provides the Ping delay, Download and Upload Speed.
- New! "Configuration and Status" Menu. Using this menu, in one shot you will retrieve 32 configuration parameters and will do 16 status checks.
- New! AWS Management. Now, you can manage the CSC Anywhere from AWS as "Managed Instance"