



# Maidenhead Bridge

## Cloud Security Connector for Azure

Enabling Zscaler for Azure customers

Administrator Guide

Version 2.5

(February 2021)

## Table of Contents

1 Introduction.....	4
2 Key benefits of the Cloud Security for Azure.....	4
3 The CSC on the Azure architecture.....	5
3.1 Single CSC.....	5
3.2 Redundant deployment.....	6
3.2.1 Example of Routes to Manage.....	6
3.2.2 Example PAC Load Balancing.....	7
4 Deploy the Cloud Security Connector.....	9
4.1 Prerequisites.....	9
4.2 Launching the CSC from Azure Marketplace.....	9
4.2.1 Deploying “CSC 250 Mbps – No HA Infrastructure required”.....	11
4.2.2 Deploying “CSC 250 Mbps – HA Using Availability Sets”.....	14
4.2.3 Deploying “CSC 250 Mbps – HA Using Availability Zones”.....	15
5 Accessing for first time to your CSC.....	16
6 Initial Wizard Configuration.....	17
6.1 Short Version.....	17
6.2 Long Version (with Example).....	17
6.2.1 VPN Credential creation.....	18
6.2.2 Create the Location on the Zscaler Console.....	19
6.2.3 Run the Wizard.....	20
7 Cloud Security Connector Admin Console:.....	25
7.1 Monitoring Tasks.....	26
7.1.1 Show Configuration and Status.....	26
7.1.1.1 GENERAL INFORMATION.....	27
7.1.1.2 INTERFACES INFORMATION.....	27
7.1.1.3 TRAFFIC REDIRECTION Options.....	27
7.1.1.4 PUBLIC IP Address INFORMATION.....	28
7.1.1.5 DNS INFORMATION.....	28
7.1.1.6 ZSCALER INFORMATION.....	29
7.1.1.7 TUNNEL INFORMATION.....	29
7.1.1.8 CREDENTIALS INFORMATION.....	29
7.1.1.9 http://ip.zscaler.com INFORMATION.....	29
7.1.1.10 BYPASS PROXY – EGRESS INTERFACE STATUS.....	29
7.1.1.11 AWS SSM AGENT.....	30
7.1.1.12 SYSLOG INFORMATION.....	30
7.1.1.13 HIGH AVAILABILITY Information.....	30
7.1.2 Show Interfaces Traffic.....	31
7.1.3 Traceroute and Latency Test.....	31
7.1.4 SPEED TEST.....	32
7.2 CSC Admin Tasks.....	33
7.2.1 AWS SSM Agent (Register / De-Register).....	33
7.2.1.1 Checking the status of the AWS SSM agent.....	36
7.2.2 Change Timezone.....	36
7.3 Bypass Proxy.....	36
7.3.1 View Current Bypass List.....	37

---

7.3.2 Configure Bypass List.....	37
7.3.2.1 1) Auto – Bypass PAC URL.....	37
7.3.2.2 2) Manual.....	42
7.4 Log Information.....	44
7.5 Configuration Wizards.....	44
7.5.1 Change Cloud, Nodes, VPN Credentials, DNS, Syslog and more.....	44
7.5.2 Switch Tunnels - Primary / Secondary.....	45
7.5.3 High Availability changing Route/s.....	46
8 Appendix A: High Availability to Zscaler using CSCs.....	47
8.1 Introduction.....	47
8.2 Pre-requisites.....	48
8.3 Configuration example:.....	49
8.3.1 Route Information.....	49
8.3.2 CSC Information.....	49
8.3.3 Identity.....	49
8.3.4 IAM Role.....	50
8.4 Running the configuration wizard.....	52
9 Appendix B – PAC File Example.....	53
9.1.1 Example PAC Load Balancing.....	53
10 Appendix C – AWS Systems Manager “Run Commands” to monitor the CSC.....	54
10.1 AWS Systems Manager: Documents.....	54
10.1.1 Creating a Document.....	54
10.1.2 List of Documents.....	55
10.1.3 Run Commands.....	58
11 Appendix D: Release Notes.....	61
11.1 Version 2.5.....	61
11.2 Version 2.0.....	61
11.3 Version 1.5.....	61
11.4 Version 1.3.....	61
11.5 Version 1.0.....	62

# 1 Introduction

The Cloud Security Connector (CSC) for Azure is a Virtual Machine appliance that allows to connect internal Azure resources to Zscaler Internet Access (ZIA) at 250 Mbps.

***IMPORTANT: If you need to connect to Zscaler at speeds more than 250 Mbps, please search Azure Marketplace for “CSC Mux (1 or 2 Gbps) for Zscaler (ZIA) using Availability Set” or “CSC Mux (1 or 2 Gbps) for Zscaler (ZIA) using Availability Zones”***

The CSC for Azure comes with all configuration required. After launching the CSC from the Azure Marketplace using the ARM templates provided, your only task is to put your VPN Credentials. The CSC will select automatically the best Zscaler Nodes to connect. (You can choose the nodes manually if your prefer)

Simple to install and not further management required.

All Zscaler functionalities are available: Cloud Firewall and Web Security. Internal IPs are completely visible on the Zscaler Gui.

In addition to this, the CSC provides and easy way to manage direct bypasses to trusted sites.

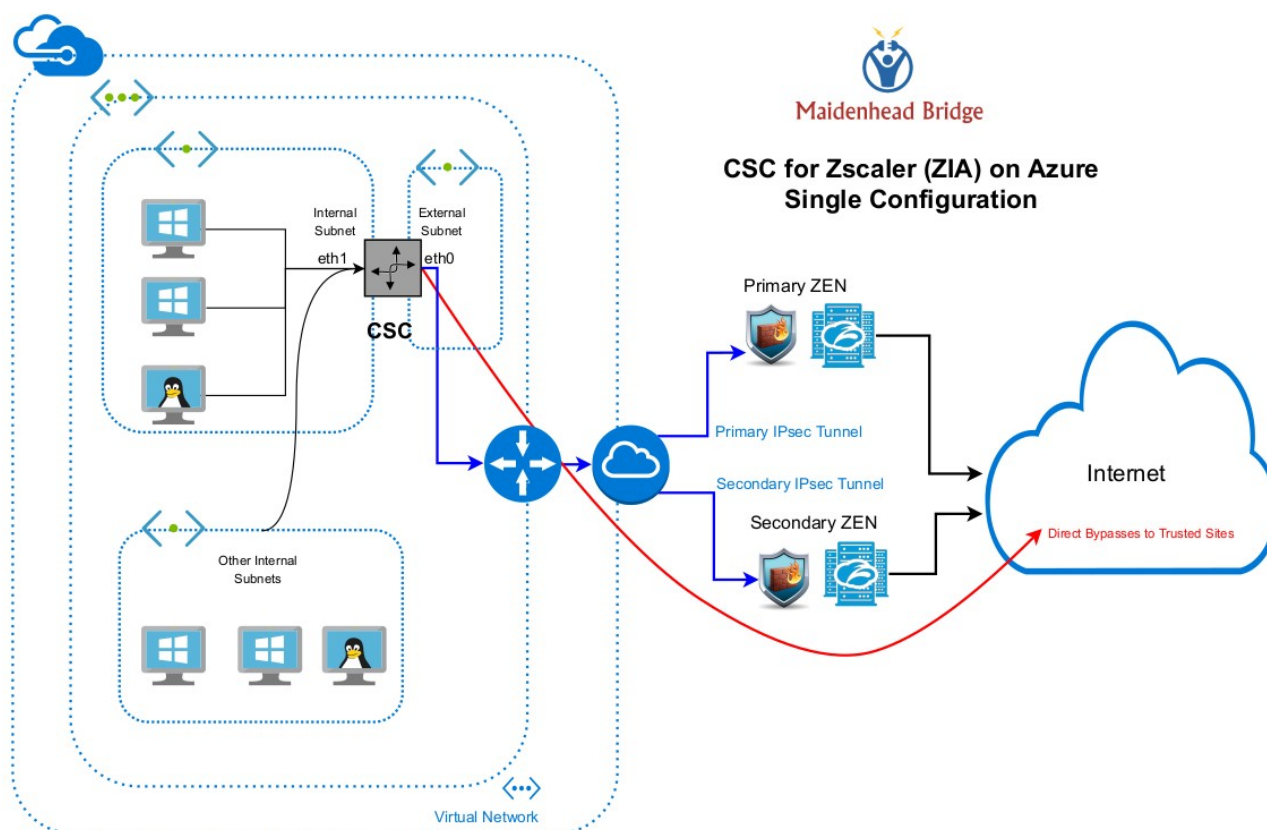
## 2 Key benefits of the Cloud Security for Azure

- Enables to connect any Azure internal resources to Zscaler Cloud Security Services.
- Automated deployment using ARM template on Availability Sets, Availability Zones or without infrastructure redundancy.
- Easy Configuration: Just insert your VPN Credentials.
- Full tunnel redundancy.
- High Availability via automatic Route configuration.
- All parametrization required for Azure and Zscaler is already configured with the optimal values according Zscaler Best practices.
- All Zscaler functionalities can be used: Firewall and Web Security.
- Full visibility of internal IPs.
- Easy way to do Bypasses to trusted sites.
- No operational burden for Administrators.
- It runs on a cheap Azure image size: Standard B1s (1 vcpus, 1 GB memory)

## 3 The CSC on the Azure architecture

### 3.1 Single CSC

The following network diagram shows where the CSC is located inside the Azure architecture:

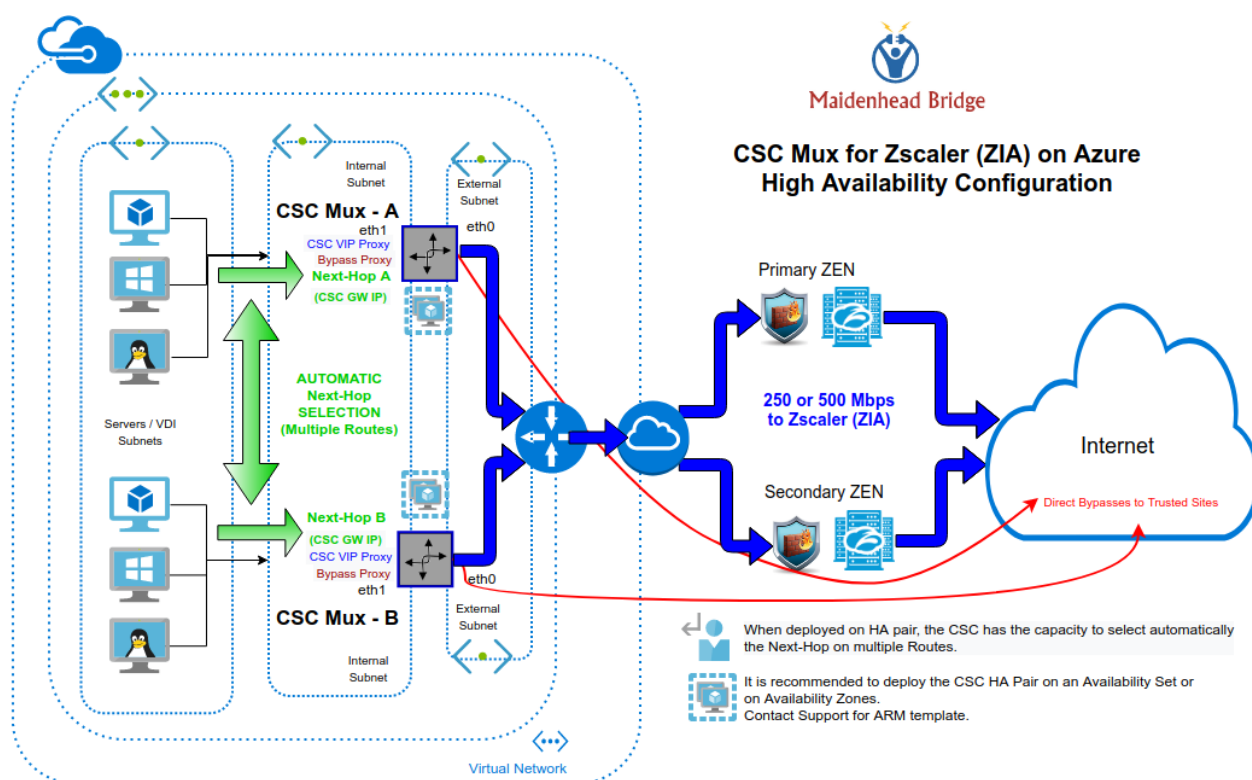


As you can see on the image, eth0 is the “external” interface and eth1 the “internal” interface. In the following chapter we are explaining how to create and install the CSC for Azure.

## 3.2 Redundant deployment

The CSC in redundant mode can be deployed on Availability Zones, Availability Set or without infrastructure redundancy.

When deployed as HA pair, the CSC pair will manage the **Next Hop of the routes configured** and you can achieve 500 Mbps for Web Traffic via PAC load balancing.



*Note: Attach both CSCs to the same “Location” on the Zscaler console. The easiest way is to configure the same VPN credentials on both CSCs.*

### 3.2.1 Example of Routes to Manage

When deployed as HA pair, the CSC has the ability to control the next-Hop on multiple routes.

Common destinations to manage are:

**Default Route to Internet** → 0.0.0.0/0

**Zscaler Global ZEN IP addresses** → 185.46.212.88/32, 185.46.212.89/32, 185.46.212.90/32, 185.46.212.91/32, 185.46.212.92/32, 185.46.212.93/32, 185.46.212.97/32, 185.46.212.98/32.

Routes examples:

All traffic to Zscaler:

Routes		
<input type="text" value="Search routes"/>		
Name	↑↓ Address prefix	↑↓ Next hop
CSC-Zscaler-Default	0.0.0.0/0	172.31.200.17

To Zscaler Global ZENs:

Routes		
<input type="text" value="Search routes"/>		
Name	↑↓ Address prefix	↑↓ Next hop
server-farm-1	185.46.212.88/32	172.31.200.17

### 3.2.2 Example PAC Load Balancing

If you want to use both CSC at the same time to duplicate your bandwidth for Web Traffic, this simple PAC file will do the job.

Please, note that you need to put the IP values of csc1vip, csc2vip, csc1bypass and csc2bypass. You can read this values from “Show Configuration and Status Menu”

**Load Balancing PAC file.**

```

function FindProxyForURL(url, host) {
    // =====
    // Section 1: Zscaler standard PAC values

    var privateIP = /^(0|10|127|192\.168|172\.[6789]|172\.2[0-9]|172\.3[01]|169\.254|192\.88\.[99])\.([0-9.]+)$/;
    var resolved_ip = dnsResolve(host);

    /* Don't send non-FQDN or private IP auths to us */
    if (isPlainHostName(host) || isInNet(resolved_ip, "192.0.2.0", "255.255.255.0") || privateIP.test(resolved_ip))
        return "DIRECT";

    /* FTP goes directly */
    if (url.substring(0, 4) == "ftp:")
        return "DIRECT";

    /* test with ZPA */
    if (isInNet(resolved_ip, "100.64.0.0", "255.255.0.0"))
        return "DIRECT";

    // =====
    // Section 2: Load Balancing: 2 x Cloud Security Connectors
    // Azure: 500 Mbps

    // Get NIC IP address
    nicIp = myIpAddress();

    // Assigning values to "tozscaler" and "bypass"
    if (isInNet(nicIp, "0.0.0.0", "0.0.0.1")) {
        var tozscaler = "PROXY csc1vip:80; PROXY csc2vip:80";
        var bypass = "PROXY csc1bypass:3128; PROXY csc2bypass:3128";
    }

    if (isInNet(nicIp, "0.0.0.1", "0.0.0.1")) {
        var tozscaler = "PROXY csc2vip:80; PROXY csc1vip:80";
        var bypass = "PROXY csc2bypass:3128; PROXY csc1bypass:3128";
    }

    // =====
    // Section 3: Bypass via Cloud Security Connectors

    // Bypass via CSC Public IPs
    if ((shExpMatch(host, "*.okta.com")) ||
        (shExpMatch(host, "*.oktacdn.com")) ||
        (shExpMatch(host, "*.okta-emea.com")) ||
        (shExpMatch(host, "login.mydomain.com")) ||
        (shExpMatch(host, "portquiz.net"))) {
        return bypass
    }

    // =====
    // Section 4: Default Traffic

    /* Default Traffic Forwarding. Forwarding to Zen on port 80, but you can use port 9400 also */
    return tozscaler
}

```



## 4 Deploy the Cloud Security Connector

### 4.1 Prerequisites

Before to launch the CSC you need to have this elements ready:

1. **(Optional) SSH Key** if you want to access the CSC using SSH keys. If not, you will be prompted a Password during the installation.
2. **Virtual Network**
3. **External Subnet:** The External Subnet must be on the same Virtual Network than the Internal Subnet.
4. **Internal Subnet:** The Internal Subnet must be on the same Virtual Network than the External Subnet.

### 4.2 Launching the CSC from Azure Marketplace

- Go to Azure Marketplace and search for Cloud Security Connector for Zscaler (ZIA):

Microsoft | Azure Marketplace Apps ▾ Search Marketplace More ▾

Products > Cloud Security Connector for Zscaler (ZIA)

**Cloud Security Connector for Zscaler (ZIA)** Save to my list

Maidenhead Bridge

★★★★★ (0) Write a review

Overview Plans Reviews

The easiest way to connect to Zscaler Internet Access (ZIA) at 250 Mbps

*(IMPORTANT Note: If you need more speed than 250 Mbps to Zscaler (ZIA), please use models "CSC Mux 1 or 2 Gbps using Availability Set" or "CSC Mux 1 or 2 Gbps using Availability Zones")*

- The Cloud Security Connector will allow to protect your Web traffic in compliance with the best practices for Zscaler Internet Access.
- The Cloud Security Connector provides tunnel redundancy and High Availability via automatic Route/s selection.
- No manual configuration required: everything is automated with the perfect configuration. Simply input your VPN Credentials and you will be connected to Zscaler ZIA.
- The Cloud Security Connector offers a simple way to do direct bypasses to internet. The Cloud Security Connector has the capacity to read the bypasses from PAC files and to apply the rules automatically.
- The Cloud Security Connector operates like a firewall and provides a robust isolation of your internal infrastructure with the intelligence required for High Availability connectivity to Zscaler Enforcement Nodes (ZENs).
- Maidenhead Bridge offers a broad portfolio of Cloud Security Connectors for Zscaler (ZIA) on virtual platforms (Hyper-V, VMware, etc) and public clouds (Azure, AWS).

Learn more

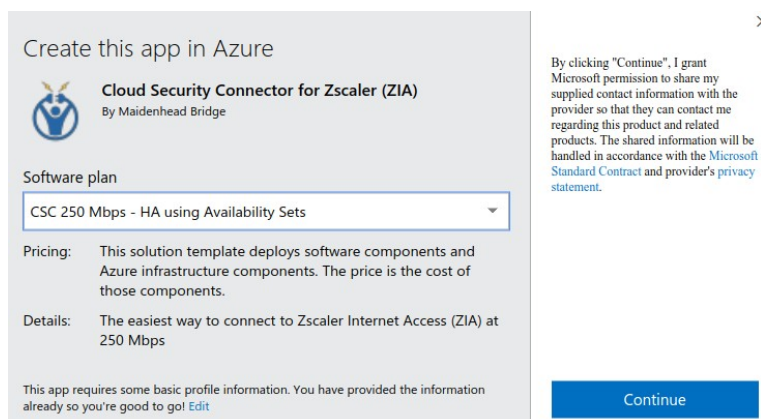
[Quick Installation Guide](#)  
[Support Portal](#)  
[Administrator Guide](#)

**CSC for Zscaler (ZIA) on Azure High Availability Configuration**


The diagram illustrates a high availability configuration for the Cloud Security Connector (CSC) on Azure. It shows two CSC instances, CSC-A and CSC-B, each with its own Virtual Network (VNet) and Subnet. Both CSCs are connected to Zscaler Enforcement Nodes (ZENs) via Primary and Secondary IPsec Tunnels. The ZENs are connected to the Internet. The diagram also shows the internal network structure with Virtual Machines (VMs) and their connection to the CSCs. A note indicates that when deployment is in progress, the CSC has the capacity to select automatically the best path to the ZENs. It is recommended to deploy the CSC with Pair on the same Availability Set.

- Click “GET IT NOW”

➤ Select the Plan:



Create this app in Azure

 **Cloud Security Connector for Zscaler (ZIA)**  
By Maidenhead Bridge

Software plan  
CSC 250 Mbps - HA using Availability Sets

Pricing: This solution template deploys software components and Azure infrastructure components. The price is the cost of those components.

Details: The easiest way to connect to Zscaler Internet Access (ZIA) at 250 Mbps

This app requires some basic profile information. You have provided the information already so you're good to go! [Edit](#)

By clicking "Continue", I grant Microsoft permission to share my supplied contact information with the provider so that they can contact me regarding this product and related products. The shared information will be handled in accordance with the [Microsoft Standard Contract](#) and provider's [privacy statement](#).

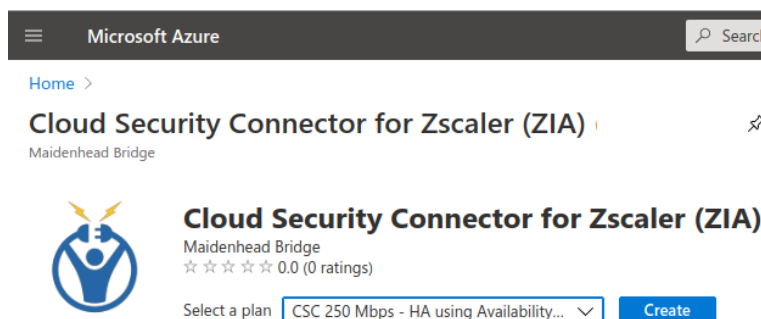
Continue

- CSC 250 Mbps – No HA Infrastructure required
- CSC 250 Mbps – HA Using Availability Sets
- CSC 250 Mbps – HA Using Availability Zones.

*NOTE 1: We recommend always to use Availability Sets or Zones.*

*NOTE 2: In all plans you can deploy 1xCSC or 2xCSCs.*


➤ Click “Continue”. You will be redirected to the Azure Portal



Microsoft Azure

Home >

**Cloud Security Connector for Zscaler (ZIA)**  
Maidenhead Bridge

 **Cloud Security Connector for Zscaler (ZIA)**  
Maidenhead Bridge  
☆☆☆☆ 0.0 (0 ratings)

Select a plan: CSC 250 Mbps - HA using Availability... [Create](#)

- You can select your plan here again.
- Click “Create”

## 4.2.1 Deploying “CSC 250 Mbps – No HA Infrastructure required”

Microsoft Azure

Home > Cloud Security Connector for Zscaler (ZIA) (preview) >

### Create Cloud Security Connector for Zscaler (ZIA)

1 Basics 2 Virtual Machine Settings 3 Networking 4 Review + create

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ Pay-As-You-Go

Resource group \* ⓘ CSC-East-US

[Create new](#)

**Instance details**

Location \* ⓘ East US

Select Single or HA configuration \*

☐ Deploy Single (1x) CSC

☒ Deploy High Availability (2x) CSCs

CSC\_Name \* ⓘ csc-zscaler

Admin Username ⓘ cscadmin

Authentication type \* ⓘ

☒ Password

☐ SSH Public Key

Password \* ⓘ

Confirm password \*

< Previous Next

- Insert the values requested (\*): Subscription, Resource group, Location, Single or HA configuration, CSC\_Name, Authentication type, SSH or Password.

**NOTE:** The Admin Username of the CSC is “cscadmin”. This value cannot be changed.

- Click “Next”

Microsoft Azure

Home > Cloud Security Connector for Zscaler (ZIA) (preview) >

## Create Cloud Security Connector for Zscaler (ZIA)

1 Basics 2 Virtual Machine Settings 3 Networking 4 Review + create

Virtual machine size \* ⓘ 1x Standard B1s  
1 vcpu, 1 GB memory  
[Change size](#)

CSC VM Disk storage account type \* ⓘ Standard\_LRS

- Select “Virtual Machine size” and “CSC VM Disk storage account type”. Default values presented are OK. If you are going to do a heavy use of the bypass functionality, please, use 2 x CPU and 4 GB RAM.
- Click “Next”

Microsoft Azure

Home > Cloud Security Connector for Zscaler (ZIA) (preview) >

## Create Cloud Security Connector for Zscaler (ZIA)

1 Basics 2 Virtual Machine Settings 3 Networking 4 Review + create

Configure virtual networks

VNET\_Name \* ⓘ VNET-East-US  
[Create new](#)

EXTERNAL\_Subnet\_Name \* ⓘ csc-external-East-US (10.2.1.0/24)  
[Manage subnet configuration](#)

INTERNAL\_Subnet\_Name \* ⓘ csc-internal-East-US (10.2.2.0/24)  
[Manage subnet configuration](#)

- Select the Virtual Network, External and Internal Subnet.
- Click “Create”

[Home](#) > [Cloud Security Connector for Zscaler \(ZIA\) \(preview\)](#) >

## Create Cloud Security Connector for Zscaler (ZIA)

✓ Validation Passed

✓ Basics   ✓ Virtual Machine Settings   ✓ Networking   **4 Review + create**

### PRODUCT DETAILS

Cloud Security Connector for Zscaler  
(ZIA)  
by Maidenhead Bridge  
[Microsoft Enterprise Contract](#) | [Privacy policy](#)

### TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

### Basics

Subscription	Pay-As-You-Go
Resource group	CSC-East-US
Location	East US
Select Single or HA configuration	Deploy High Availability (2x) CSCs
CSC_Name	csc-zscaler
Admin Username	cscadmin
Password	*****

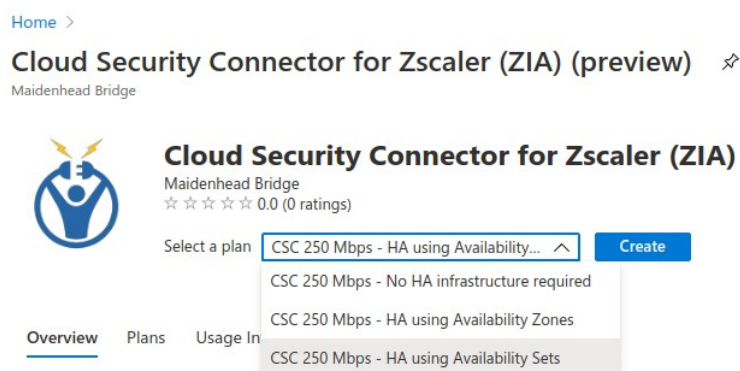
### Virtual Machine Settings

[Create](#)[< Previous](#)[Next](#)[Download a template for automation](#)

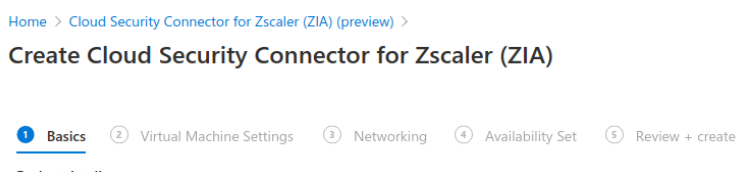
- Check "Validation Passed" and Click "Create"
- Follow the instructions on next chapter: "Next steps"

## 4.2.2 Deploying “CSC 250 Mbps – HA Using Availability Sets”

- Select plan “CSC 250 Mbps – HA using Availability Sets”



- Click “Create”
- The steps “Basics”, “Virtual Machine Settings” and “Networking” are the same than before. Step 4 “Availability Set” is the addition to this Plan:



- Fill steps 1 to 3 as example above and on step 4, select or create the “Availability Set”

**NOTE:** Please, put the name of the Availability Set and Fault and Update domains values. If the Availability Set doesn't exist, this template will create a new one using the entered values

- Click “Next”, wait for “Validation passed” and click “Create”

### 4.2.3 Deploying “CSC 250 Mbps – HA Using Availability Zones”

- Select plan “CSC 250 Mbps – HA using Availability Sets”



Microsoft Azure

Home >

Cloud Security Connector for Zscaler (ZIA) (preview)

Maidenhead Bridge

 **Cloud Security Connector for Zscaler (ZIA)**  
Maidenhead Bridge  
☆☆☆☆ 0.0 (0 ratings)

Select a plan: CSC 250 Mbps - HA using Availability... **Create**

CSC 250 Mbps - No HA infrastructure required

CSC 250 Mbps - HA using Availability Zones

CSC 250 Mbps - HA using Availability Sets

Overview Plans Usage In

- Click “Create”

#### Create Cloud Security Connector for Zscaler (ZIA)

1 Basics 2 Virtual Machine Settings 3 Networking 4 Review + create

**Project details**


Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*

Resource group \*

**Instance details**


Location \*

 Please, check if the Location (Region) selected previously supports Availability Zones (see: <https://docs.microsoft.com/en-us/azure/availability-zones/az-region>).

Select Single or HA configuration \*

☐ Deploy Single (1x) CSC

☒ Deploy High Availability (2x) CSCs

 Choose the Availability Zones for each Cloud Security Connector.

First CSC Availability Zone \*

Second CSC Availability Zone \*

CSC\_Name \*

Admin Username

Authentication type \*

☒ Password

☐ SSH Public Key

Password \*

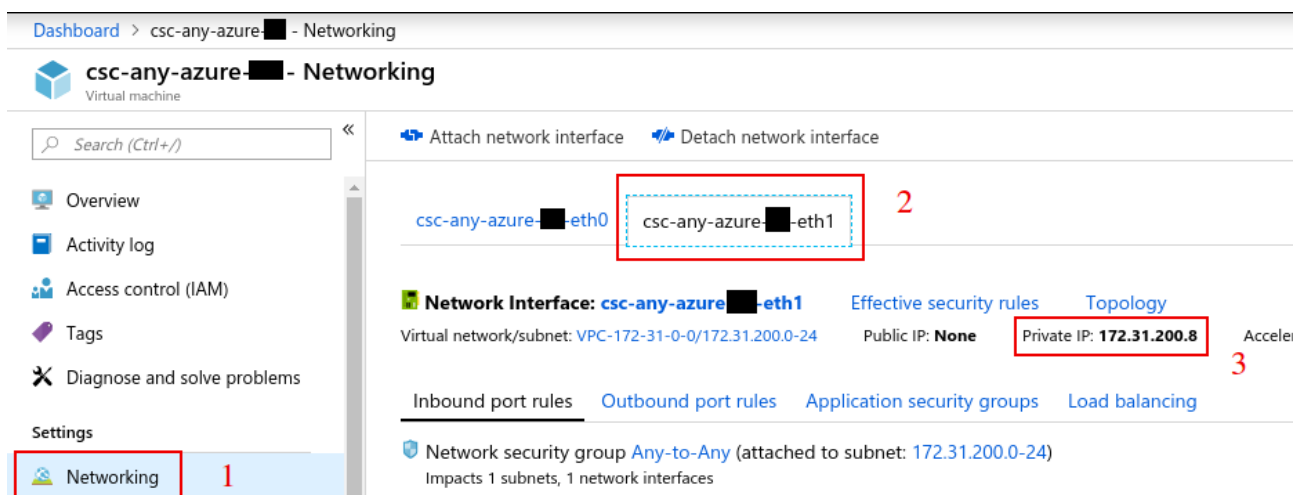
Confirm password \*

< Previous Next

- In this case, you need the only specific to select for this plan is the Availability Zone for each CSC. The rest is the same than before.

## 5 Accessing for first time to your CSC

1. Go to your Azure Dashboard → Select the VM created → Networking → eth1 and check “Private IP”



2. In this example, “Private IP” is: 172.31.200.8

3. From a machine inside the Virtual Network, ssh the CSC using the Key, like:

ssh -i <keyname.pem> cscadmin@<eth1 Private IP> or ssh cscadmin@<eth1 Private IP> if using password.

**Important: Please, wait 2 minutes before to SSH the CSC to allow all processes to complete.**

```

Welcome to Maidenhead Bridge - Cloud Security Connector Anywhere for Azure
Last login: Tue Feb  5 09:13:49 2019 from 172.31.200.7

*****IPsec tunnel information was never configured*****

Welcome to the CSC Anywhere Configuration Wizard

1) Configuration required on your Zscaler Console: VPN credentials and Location
--> VPN Credentials creation: Go to > Administration > VPN Credentials > Add VPN Credential -> Select Authentication Type = FQDN and configure 'User ID' and 'Pre-Shared Key'
--> Location creation: Go to > Administration > Location > Add Location. Put your Location values and select 'VPN Credentials' created in the step before
2) Run the Wizard on the CSC and Select Cloud, Nodes, ingress VPN Credentials, DNS Servers, Bypass PAC URL and Syslog Servers

Current Values Configured:
-----
ZSCALER INFORMATION
Zscaler Cloud:
Primary ZEN node: | Hostname: | IP:
Secondary ZEN node: | Hostname: | IP:
-----
CREDENTIALS INFORMATION
User ID: | Pre-Shared Key:
-----
DNS Server: Azure DNS server 168.63.129.16
-----
Bypass Proxy PAC URL
Your current Bypass PAC URL is http://pac.<cloudname>.net/something/<pacname>.pac
-----
SYSLOG / SIEM information
Syslog / SIEM servers are not configured
-----
Are you ready to continue? (y/n) █

```

4. Your CSC is ready for the initial configuration. Just follow the instructions of the Configuration Wizard.



## 6 Initial Wizard Configuration

Please, follow this instructions to run the initial configuration of the CSC for Azure:

### 6.1 Short Version

Configuration required on your Zscaler Console: VPN credentials and Location

1. VPN Credentials creation: Go to > Administration > VPN Credentials > Add VPN Credential -> Select Authentication Type = FDQN and configure 'User ID' and 'Pre-Shared Key'
2. Location creation: Go to > Administration > Location > Add Location. Put your Location values and select 'VPN Credentials' created in the step before
3. Run the Wizard. Insert the values. Confirm and reboot.
4. Done!

### 6.2 Long Version (with Example)

In this Example, after the CSC was launched, the values of my CSC are:

The screenshot displays the Zscaler Cloud Management Console interface. On the left, the 'Networking' tab is selected and highlighted with a red box and the number '1'. The main panel shows the configuration for a network interface named 'csc-any-azure-eth1', which is highlighted with a red box and the number '2'. Below this, the 'Network Interface' section shows 'csc-any-azure-eth1' with 'Effective security rules' and 'Topology' links. The 'Virtual network/subnet' is 'VPC-172-31-0-0/172.31.200.0-24'. The 'Public IP' is 'None', and the 'Private IP' is '172.31.200.8', which is highlighted with a red box and the number '3'. The 'Network security group' is 'Any-to-Any' (attached to subnet: 172.31.200.0-24). The 'Inbound port rules', 'Outbound port rules', 'Application security groups', and 'Load balancing' tabs are visible at the bottom.

The internal IP (eth1) is 172.31.200.8. Doing and SSH from a machine on subnet 172.31.200.0/24 to the CSC, the initial wizard appear.

In this example:

*Username: cscadmin (use always "cscadmin")*

*CSC IP: 172.31.200.8*

\$ ssh [cscadmin@172.31.200.8](mailto:cscadmin@172.31.200.8)

*(Please, Wait 2 minutes after power on or reboot to SSH the CSC)*

```

Welcome to Maidenhead Bridge - Cloud Security Connector Anywhere for Azure
Last login: Tue Feb  5 09:13:49 2019 from 172.31.200.7

****IPsec tunnel information was never configured****

Welcome to the CSC Anywhere Configuration Wizard

1) Configuration required on your Zscaler Console: VPN credentials and Location
--> VPN Credentials creation: Go to > Administration > VPN Credentials > Add VPN Credential -> Select Authentication Type = FDQN and configure 'User ID' and 'Pre-Shared Key'
--> Location creation: Go to > Administration > Location > Add Location. Put your Location values and select 'VPN Credentials' created in the step before
2) Run the Wizard on the CSC and Select Cloud, Nodes, ingress VPN Credentials, DNS Servers, Bypass PAC URL and Syslog Servers

Current Values Configured:
-----
ZSCALER INFORMATION
Zscaler Cloud:
Primary ZEN node: | Hostname: | IP:
Secondary ZEN node: | Hostname: | IP:
-----
CREDENTIALS INFORMATION
User ID: | Pre-Shared Key:
-----
DNS Server: Azure DNS server 168.63.129.16
-----
Bypass Proxy PAC URL
Your current Bypass PAC URL is http://pac.<cloudname>.net/something/<pacname>.pac
-----
SYSLOG / SIEM information
Syslog / SIEM servers are not configured
-----
Are you ready to continue? (y/n) █

```

## 6.2.1 VPN Credential creation.

Go to > Administration > VPN Credentials > Add VPN Credential -> Select Authentication Type = FDQN and configure 'User ID' and 'Pre-Shared Key'

Click “Save” and “Activation”

## 6.2.2 Create the Location on the Zscaler Console

Location creation: Go to > Administration > Location > Add Location. Put your Location values and select 'VPN Credentials' created in the step before

**Add Location**

**LOCATION**

**Name**  
csc-any-azure-02 1

**Country**  
United Kingdom

**State/Province**

**Time Zone**  
Europe/London

**Group**  
None

**ADDRESSING**

**Static IP Addresses**  
None

**VPN Credentials**  
csc-azure-02@maidenheadbridge.com 2

**GATEWAY OPTIONS**

**Enable XFF Forwarding**  
☒

**Enable IP Surrogate**  
☒

**Enforce Surrogate IP for Known Browsers**  
☐

**Enable SSL Scanning**  
☒

**Enforce Authentication**  
☒

**Idle Time to Disassociation**  
8 Hours

**Enforce Firewall Control**  
☒

**Save** **Cancel**

Fill other values on the Location, click “Save” and “Activate”

### 6.2.3 Run the Wizard

The initial values are empty.

```
Current Values Configured:
-----
ZSCALER INFORMATION
Zscaler Cloud:
Primary ZEN node: | Hostname: | IP:
Secondary ZEN node: | Hostname: | IP:
-----
CREDENTIALS INFORMATION
User ID: | Pre-Shared Key:
-----
DNS Server: Azure DNS server 168.63.129.16
-----
Bypass Proxy PAC URL
Your current Bypass PAC URL is http://pac.<cloudname>.net/something/<pacname>.pac
-----
SYSLOG / SIEM information
Syslog / SIEM servers are not configured
-----
Are you ready to continue? (y/n) █
```

1. Select your cloud

```
Are you ready to continue? (y/n) y
-----
ZSCALER INFORMATION

You current Zscaler Cloud and Nodes are:

Zscaler Cloud:
Primary ZEN node: | Hostname: | IP:
Secondary ZEN node: | Hostname: | IP:

Do you want to change these values? (y/n) y

-----
Please, select your Cloud

1) zscalerthree
2) zsccloud
3) zscalertwo
4) zscaler
5) zscalerone
6) zscalerbeta
7) Not in the list? Ingress Manually
8) Quit
Enter your choice: █
```

2. Select the Nodes: Auto or Manual. (Auto will detect the nearest nodes via DNS resolution.)  
We recommend to select Manually the nodes. You will be asked to select Primary and Secondary.

```
-----
Please, select Manual or Auto Node Selection

1) Manual
2) Auto
3) Quit
Enter your choice: 1

-----
Please, select your Primary Node on 'zscalerthree'
Nodes marked with (-NRU) may be Not Ready for Use. Check http://ips.zscalerthree.net

1) Europe,Amsterdam
2) Europe,Brussels
3) Europe,FrankfurtIV
4) Europe,LondonIII
5) Europe,MilanII
6) Europe,OsloII
7) Europe,ParisII
8) Europe,TelAviv
9) Europe,Warsaw
10) US&Canada,AtlantaII
11) US&Canada,Chicago
12) US&Canada,DallasI
13) US&Canada,SanFranciscoIV
14) US&Canada,Seattle
15) US&Canada,TorontoII
16) US&Canada,WashingtonDC
17) Asia,Auckland
18) Asia,HongKongIII
19) Asia,MumbaiII
20) Asia,SeoulIII
21) Asia,Shanghai
22) Asia,SingaporeIV
23) Asia,SydneyIII
24) Asia,TokyoIV
25) Africa,JohannesburgII
26) Not in the list? Ingress Manually
27) Quit
Enter your choice: █
```

After Primary and Secondary is selected the following screen appear:

```
-----
You have chosen the following:

Cloudname: zscalerthree
Primary node: LondonIII (lon3-vpn.zscalerthree.net)
Secondary Node: Amsterdam (ams2-vpn.zscalerthree.net)
-----
```

## 3. Enter your VPN Credentials

```
-----  
CREDENTIALS INFORMATION  
You current VPN Credentials are:  
User ID: | Pre-Shared Key:  
Do you want to change these values? (y/n) y  
Please, ingress VPN Credentials (Email and Pre Shared Key)  
Email: csc-azure-02@maidenheadbridge.com 1  
Pre Shared Key: 2  
Do you want to display the Pre Shared Key? (y/n)? y  
PSK = 12345678
```

## 4. Enter DNS values. You can use Azure DNS or setup your own DNS servers

```
-----  
DNS Configuration  
You are using Azure DNS server 168.63.129.16  
Do you want to change the DNS servers? (y/n) y  
Do you want to use Azure DNS 168.63.129.16? (y/n)n  
Primary DNS Server (IP): 1.1.1.1  
Secondary DNS Server (IP): 8.8.8.8  
-----
```

## 5. Enter Bypass PAC URL if you are using Bypass Proxy functionality.

```
-----
Bypass Proxy Configuration
Your current Bypass PAC URL is http://pac.<cloudname>.net/something/<pacname>.pac

Do you want to change the Bypass PAC URL?
1) Yes
2) No
Enter your choice: 1

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

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

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

This is your current Bypass List

.ubuntu.com
www.fullldomain.co.uk
.anotherdomain.com
.salesforce.com
```

(truncated content)

```
.mstea.ms
.office.net
.windows.net
.windows.com
.microsoftonline.com
.microsoftazuread-sso.com
.microsoftonline-p.net
.microsoftonline-p.com

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

Bypass List updated sucessfully
```

## 6. Enter Syslog / SIEM information

```
-----
Syslog / SIEM Configuration

Your current Syslog / SIEM configuration is:

Syslog / SIEM servers are not configured

Do you want to change Syslog / SIEM Servers values?

1) Yes
2) No
3) Reset default values
Enter your choice: 1

Primary Syslog Server (IP): 172.31.200.7
(Optional) Do you want to configure a Secondary Syslog Server (y/n)n
Please enter Syslog TCP port: 514
```

7. You will be asked to confirm the values. Verify and confirm. The CSC will reboot.

```
Please confirm this values:
-----
Cloudname: zscalerthree
Primary node: LondonIII (lon3-vpn.zscalerthree.net)
Secondary Node: Amsterdam (ams2-vpn.zscalerthree.net)
-----
VPN Credentials
User ID: csc-azure-02@maidenheadbridge.com | Pre-Shared Key: 12345678
-----
DNS Servers: 1.1.1.1 ; 8.8.8.8
-----
Bypass Proxy PAC URL
Your current Bypass PAC URL is http://pac.zscalerthree.net/maidenheadbridge.com/cscbypass.pac
-----
Primary Syslog / SIEM server IP: 172.31.200.7
Syslog / SIEM TCP port IP: 514
-----
Do you want to implement this values? (y/n)?
```

```
Do you want to implement this values? (y/n)?y
Validating Configuration
Your Cloud is: zscalerthree
Checking Node LondonIII hostname lon3-vpn.zscalerthree.net
Hostname lon3-vpn.zscalerthree.net has IP 165.225.16.38
Node LondonIII is Alive
Checking Node Amsterdam hostname ams2-vpn.zscalerthree.net
Hostname ams2-vpn.zscalerthree.net has IP 165.225.28.14
Node Amsterdam is Alive
Are this values correct? (y/n)? y
The system will be configured and rebooted
Connection to 172.31.200.8 closed by remote host.
Connection to 172.31.200.8 closed.
```

Done! You CSC is ready for Production.



## 7 Cloud Security Connector Admin Console:

The CSC Console was created to simplify admin tasks and to keep simple the operation showing what is important to administrators for operation and troubleshooting. In addition to this, all monitoring tasks are able to be done via AWS Systems Manager. Simply register the CSC instance on AWS as managed instance and you are ready to manage the CSC using the best management in the world.

Accessing the console via SSH, you will receive the Admin Console. For example:

```
ssh cscadmin@172.31.200.14
```

```
Maidenhead Bridge

Cloud Security Connector Anywhere - Single - Admin Console

Name : csc-v-2-0-A
Azure Zone : ukwest

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) Reserved for future use
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 Cloud, Nodes, VPN Credentials, DNS, Syslog and more
13) Switch Tunnels - Primary / Secondary
14) High Availability changing Route/s
15) Update ZEN Nodes Database

e) Exit

Selection: █
```

The Main Sections are:

- Monitoring Tasks: To check status.
- CSC Admin Tasks: To register the CSC for AWS management, and timezone.
- Bypass Proxy: To manage the Bypass PAC URL or to enter manually the Bypasses.
- Configuration Wizard: Allows to run the initial wizard, to switch tunnels, to configure High Availability and to updated ZEN nodes databases.

## 7.1 Monitoring Tasks

### 7.1.1 Show Configuration and Status

```

GENERAL INFORMATION
Name: csc-v-2-0-A
Location: ukwest | SubscriptionId: ffde02fb-c38f-45fb-9e31-89e5303be5f1 | vmSize: Standard_B1s
CSC date: Sat May 16 07:19:29 UTC 2020
Soft version : 2.0

INTERFACES INFORMATION
External: Tunnel IP (eth0): 172.31.96.8/24 | Bypass Proxy Egress IP 172.31.96.9 | Network Gateway: 172.31.96.1
Internal: CSC GW IP (eth1): 172.31.200.14/24 | Network Gateway: 172.31.200.1

TRAFFIC REDIRECTION Options
To Zscaler: VIP Proxy: 172.31.200.15:80 (or :9400) | Route all traffic via CSC GW IP | Zscaler Global Proxies (port 80/9400) via CSC GW IP
Direct to Internet: Bypass Proxy: 172.31.200.16:3128 | Zscaler Global Proxies (port 3128) via CSC GW IP

PUBLIC IP Address INFORMATION
IPsec tunnels Public IP: 51.140.225.106
Bypass Proxy Public IP: 51.140.254.28

DNS INFORMATION
Using Azure DNS: 168.63.129.16

ZSCALER INFORMATION
Zscaler Cloud: zscalerthree
Primary ZEN node: ManchesterI | Hostname: man1-vpn.zscalerthree.net | IP: 165.225.196.35 is Alive
Secondary ZEN node: LondonIII | Hostname: lon3-vpn.zscalerthree.net | IP: 165.225.16.38 is Alive

TUNNEL INFORMATION
The Node active is the: ManchesterI
IPsec uptime: 9 hours, since May 15 22:05:44 2020
Last Security Association: ESTABLISHED 90 minutes ago

CREDENTIALS INFORMATION
Username: csc-azure@maidenheadbridge.com | PSK: Not shown. Please, read it from 'Configuration Wizards' Menu

http://ip.zscaler.com INFORMATION
You are accessing the Internet via Zscaler Cloud: Manchester I in the zscalerthree.net cloud.
Your Gateway IP Address is 51.140.225.106

BYPASS PROXY - EGRESS INTERFACE STATUS
Bypass Proxy Egress Interface 172.31.96.9 can reach test page (http://pac.zscalerthree.net)

AWS SSM AGENT
AWS SSM Agent is active (running) since Fri 2020-05-15 11:09:37 UTC; 20h ago
Registration values: {"ManagedInstanceID":"mi-0a4aad85d0f080a57","Region":"eu-west-1"}

SYSLOG INFORMATION
SYSLOG Server (1) IP: 172.31.200.7 is Alive
SYSLOG Server (2) IP is not configured
SYSLOG TCP Port: 514

HIGH AVAILABILITY Information
The HA service is: active (running) since Fri 2020-05-15 11:08:32 UTC; 20h ago
Identity Type: SystemAssigned
Route to Zscaler using Next Hop: 172.31.200.14 of VM: csc-v-2-0-A (this CSC)
Current values configured are:
  Route/s (Qty)= 3
    Route 1: myroute (Route Table=csc-rt-1, Resource Group=Development)
    Route 2: server-farm-1 (Route Table=csc-rt-for-servers, Resource Group=Development)
    Route 3: CSC-Zscaler-Default (Route Table=Csc-Routing-table, Resource Group=Development)
  Computer Name of other CSC in the pair: csc-v-2-0-B (Resource Group=Development)

Press ENTER to continue

```

### 7.1.1.1 GENERAL INFORMATION

This section contains general information about the Virtual Machine. To be used for troubleshooting purposes if needed.

```
GENERAL INFORMATION
Name: csc-v-2-0-A
Location: ukwest | SubscriptionId: ffde02fb-c38f-45fb-9e31-89e5303be5f1 | vmSize: Standard_B1s
CSC date: Sat May 16 07:19:29 UTC 2020
Soft version : 2.0
```

### 7.1.1.2 INTERFACES INFORMATION

This section contains the interfaces information: IPs and Gateways.

```
INTERFACES INFORMATION
External: Tunnel IP (eth0): 172.31.96.8/24 | Bypass Proxy Egress IP 172.31.96.9 | Network Gateway: 172.31.96.1
Internal: CSC GW IP (eth1): 172.31.200.14/24 | Network Gateway: 172.31.200.1
```

### 7.1.1.3 TRAFFIC REDIRECTION Options

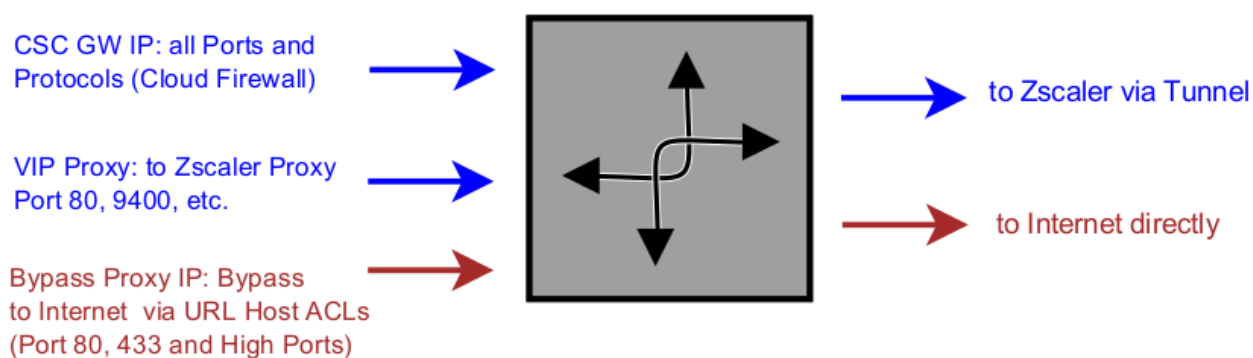
```
TRAFFIC REDIRECTION Options
To Zscaler: VIP Proxy: 172.31.200.15:80 (or :9400) | Route all traffic via CSC GW IP | Zscaler Global Proxies (port 80/9400) via CSC GW IP
Direct to Internet: Bypass Proxy: 172.31.200.16:3128 | Zscaler Global Proxies (port 3128) via CSC GW IP
```

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 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:



How to Redirect your traffic:

1. Sending all traffic using CSC GW IP as default gateway to internet for all internal devices.
2. Using a PAC File: You can download a PAC file Example from here: [Click here](#)

*Note:*

*The CSC Anywhere for Azure accepts the option to use the Zscaler Global Proxies to send traffic to Zscaler Cloud and for the Bypass as well.*

*Your task is to route the Zscaler Global Proxies IPs via the CSC GW IP and to create a return statement on your PAC file like:*

*Traffic to Zscaler → return “PROXY 185.46.212.88:80”; (you can use port 9400 as well)  
 Traffic via Bypass Proxy → return “PROXY 185.46.212.88:3128”;*

*List of Zscaler Global Proxies:*

185.46.212.88	185.46.212.89	185.46.212.90	185.46.212.91
185.46.212.92	185.46.212.93	185.46.212.97	185.46.212.98

#### 7.1.1.4 PUBLIC IP Address INFORMATION

This section displays the Public IP in use for the tunnel and for the bypass proxy functionality.

```
PUBLIC IP Address INFORMATION
IPsec tunnels Public IP: 51.140.225.106
Bypass Proxy Public IP: 51.140.254.28
```

#### 7.1.1.5 DNS INFORMATION

This section displays the DNS information. You can use the default DNS server from Azure or to setup your own DNS servers.

```
DNS INFORMATION
Using Azure DNS: 168.63.129.16
```

### 7.1.1.6 ZSCALER INFORMATION

This section shows the Cloud and Nodes in use and if they are reachable or not.

```
ZSCALER INFORMATION
Zscaler Cloud: zscalerthree
Primary ZEN node: ManchesterI | Hostname: man1-vpn.zscalerthree.net | IP: 165.225.196.35 is Alive
Secondary ZEN node: LondonIII | Hostname: lon3-vpn.zscalerthree.net | IP: 165.225.16.38 is Alive
```

### 7.1.1.7 TUNNEL INFORMATION

This section shows the Node Active, Ipsec uptime and last Security Association.

```
TUNNEL INFORMATION
The Node active is the: ManchesterI
IPsec uptime: 9 hours, since May 15 22:05:44 2020
Last Security Association: ESTABLISHED 90 minutes ago
```

### 7.1.1.8 CREDENTIALS INFORMATION

This section shows the User ID in use:

```
CREDENTIALS INFORMATION
Username: csc-azure@maidenheadbridge.com | PSK: Not shown. Please, read it from 'Configuration Wizards' Menu
```

### 7.1.1.9 <http://ip.zscaler.com> INFORMATION

Zscaler recommend to check the page <http://ip.zscaler.com> to validate that you are using Zscaler and to see your Zscaler Node, Cloud and IP address. The CSC does this test for you.

```
http://ip.zscaler.com INFORMATION
You are accessing the Internet via Zscaler Cloud: Manchester I in the zscalerthree.net cloud.
Your Gateway IP Address is 51.140.225.106
```

### 7.1.1.10 BYPASS PROXY – EGRESS INTERFACE STATUS

This sections validates if the Bypass Proxy can access internet directly going to <http://pac.<cloudname>.net>

```
BYPASS PROXY - EGRESS INTERFACE STATUS
Bypass Proxy Egress Interface 172.31.96.9 can reach test page (http://pac.zscalerthree.net)
```

### 7.1.1.11 **AWS SSM AGENT**

This section shows the status of the AWS SSM Agent.

```
AWS SSM AGENT
AWS SSM Agent is active (running) since Fri 2020-05-15 11:09:37 UTC; 20h ago
Registration values: {"ManagedInstanceID":"mi-0a4aad85d0f080a57","Region":"eu-west-1"}
```

### 7.1.1.12 **SYSLOG INFORMATION**

This section shows the Syslog Servers configured and TCP port.

```
SYSLOG INFORMATION
SYSLOG Server (1) IP: 172.31.200.7 is Alive
SYSLOG Server (2) IP is not configured
SYSLOG TCP Port: 514
```

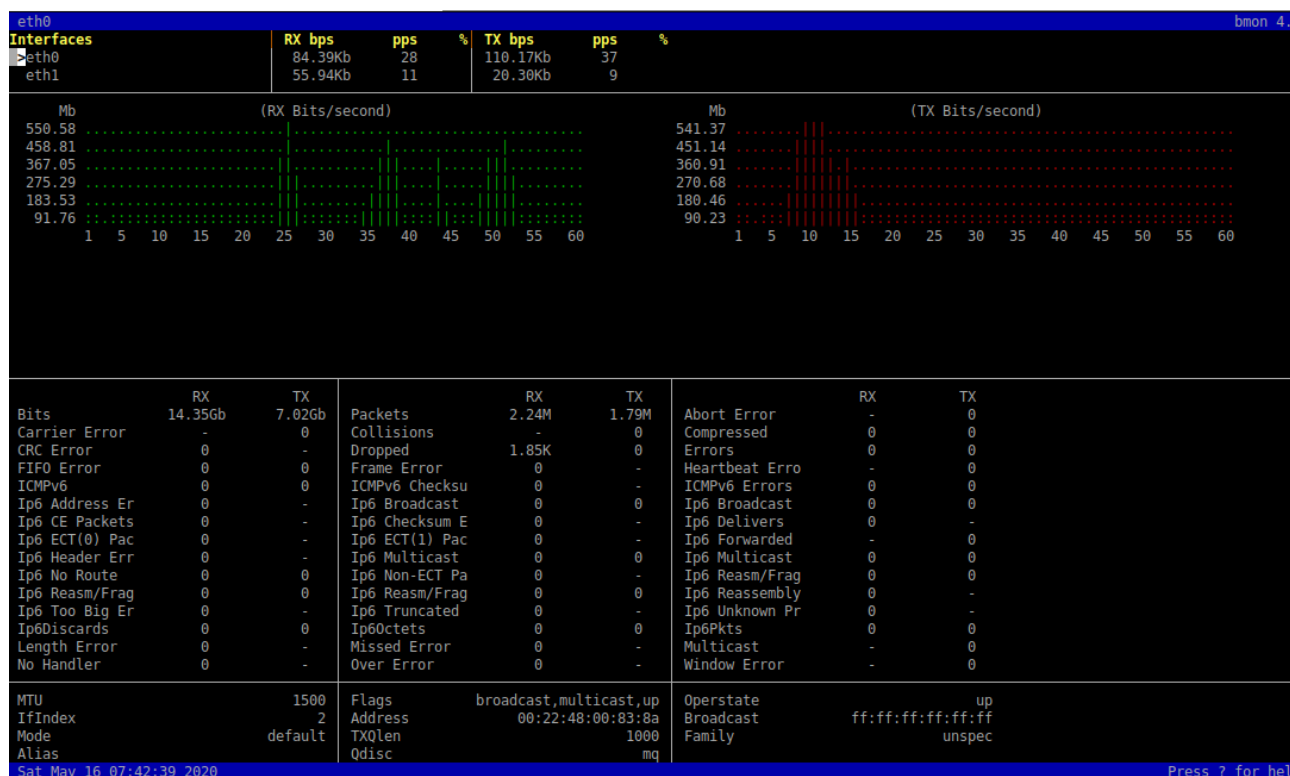
### 7.1.1.13 **HIGH AVAILABILITY Information**

This section shows the status and configuration of the High Availability. It shows all Routes under the management of the CSC pair and the current “Next-Hop” in use.

```
HIGH AVAILABILITY Information
The HA service is: active (running) since Fri 2020-05-15 11:08:32 UTC; 20h ago
Identity Type: SystemAssigned
Route to Zscaler using Next Hop: 172.31.200.14 of VM: csc-v-2-0-A (this CSC)
Current values configured are:
  Route/s (Qty)= 3
    Route 1: myroute (Route Table=csc-rt-1, Resource Group=Development)
    Route 2: server-farm-1 (Route Table=csc-rt-for-servers, Resource Group=Development)
    Route 3: CSC-Zscaler-Default (Route Table=Csc-Routing-table, Resource Group=Development)
  Computer Name of other CSC in the pair: csc-v-2-0-B (Resource Group=Development)
```

## 7.1.2 Show Interfaces Traffic

You can use this section to see the traffic in real time.



## 7.1.3 Traceroute and Latency Test

This test can validate the quality of the Internet path between your location and Zscaler. You can run it with tunnels down or up. When the tunnels are up, it does a “Reverse Path” test from your active ZEN node to your location. This is very useful to check if there is any packet loss at some point.



```

Selection: 3

My TraceRoute (MTR) Test Report
This test does 10 probes to the Primary ZEN, Secondary ZEN, Google DNS 8.8.8.8
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: ManchesterI : man1-vpn.zscalerthree.net > 165.225.196.35
Start: 2020-05-16T07:44:34+0000
HOST: csc-v-2-0-A
  1. AS62044 165.225.196.35 0.0% 10 17.7 17.2 16.4 20.0 1.1

Testing Secondary ZEN: LondonIII : lon3-vpn.zscalerthree.net > 165.225.16.38
Start: 2020-05-16T07:44:49+0000
HOST: csc-v-2-0-A
  1. AS??? ??? 100.0 10 0.0 0.0 0.0 0.0 0.0
  2. AS62044 165.225.16.38 0.0% 10 22.3 24.6 19.7 32.1 3.9

Testing Google DNS 8.8.8.8
Start: 2020-05-16T07:45:29+0000
HOST: csc-v-2-0-A
  1. AS??? ??? 100.0 10 0.0 0.0 0.0 0.0 0.0
  2. AS62044 165.225.196.219 0.0% 10 21.0 22.3 18.4 30.6 4.0
  3. AS62044 165.225.196.3 0.0% 10 22.3 25.0 19.3 33.4 4.0
  4. AS3257 46.33.77.237 0.0% 10 18.0 25.0 18.0 35.5 5.2
  5. AS3257 ae22.cr10-lon1.ip4.gtt.net (89.149.185.49) 0.0% 10 28.7 32.1 26.2 41.3 4.5
  6. AS15169 72.14.221.145 0.0% 10 28.4 31.0 25.4 37.4 4.4
  7. AS15169 216.239.48.217 0.0% 10 30.8 33.7 27.8 40.3 4.9
  8. AS15169 172.253.68.219 0.0% 10 26.1 28.9 25.3 33.9 3.0
  9. AS15169 dns.google (8.8.8.8) 0.0% 10 31.8 27.1 23.1 31.8 2.8

Reverse path from: ManchesterI to your Public IP: 51.140.225.106
Start: 2020-05-16T07:46:10+0000
HOST: csc-v-2-0-A
  1. AS??? ??? 100.0 10 0.0 0.0 0.0 0.0 0.0
  2. AS62044 165.225.196.222 0.0% 10 23.9 21.6 18.4 26.3 3.1
  3. AS22616 165.225.196.3 0.0% 10 20.0 24.4 18.4 35.2 4.6
  4. AS3257 46.33.77.237 0.0% 10 21.3 22.3 18.7 26.6 2.7
  5. AS3257 et-10-1-0.cr0-dub2.ip4.gtt.net (141.136.107.49) 0.0% 10 31.9 34.8 27.5 66.4 11.3
  6. AS3257 microsoft-gw.ip4.gtt.net (46.33.92.70) 0.0% 10 33.5 33.8 29.7 38.8 3.1
  7. AS8075 ae21-0.icr01.dub07.ntwk.msn.net (104.44.236.63) 0.0% 10 37.1 36.9 32.3 46.8 4.4
  8. AS8075 be-100-0.ibr01.dub07.ntwk.msn.net (104.44.11.61) 0.0% 10 41.9 38.8 33.9 44.1 3.6
  9. AS8075 be-8-0.ibr01.lon22.ntwk.msn.net (104.44.17.85) 0.0% 10 39.2 41.3 37.6 46.5 2.8
  10. AS8075 be-4-0.ibr01.cwl20.ntwk.msn.net (104.44.18.93) 0.0% 10 34.2 37.1 33.8 41.5 2.4
  11. AS8075 ae102-0.icr02.cwl20.ntwk.msn.net (104.44.20.184) 0.0% 10 38.4 39.8 34.0 45.4 3.6
  12. AS??? ??? 100.0 10 0.0 0.0 0.0 0.0 0.0

```

### 7.1.4 SPEED TEST

This test is experimental due to we are using third party tools (speedtest.net) but it works fine in most cases.

Note: May be will be required to add the “.speedtest.net” on your SSL Exemption list on your Zscaler console.



```
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 (165.225.196.231)...
Retrieving speedtest.net server list...
Selecting best server based on ping...
Hosted by Airband Community Internet Ltd (Manchester) [4.81 km]: 26.792 ms
Testing download speed.....
Download: 727.88 Mbit/s
Testing upload speed.....
Upload: 135.45 Mbit/s
```

Note: Zscaler imposes a “soft limit” of 200 Mbps on ipsec tunnels.

## 7.2 CSC Admin Tasks

```
CSC Admin tasks
5) AWS SSM Agent (Register or De-Register)
6) Reserved for future use
7) Change Timezone
```

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

6. Reserved for future use.

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

### 7.2.1 AWS SSM Agent (Register / De-Register)

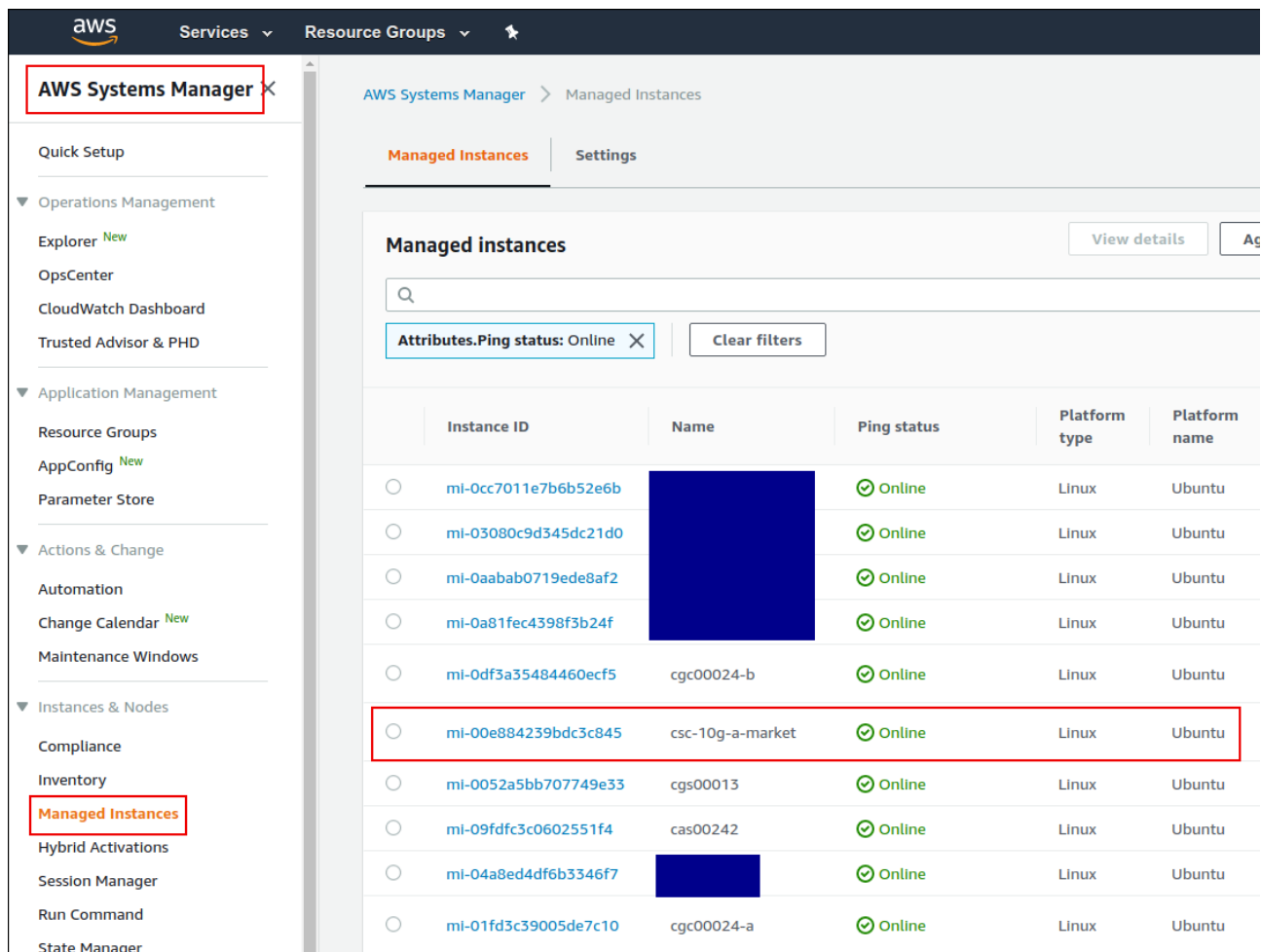
The CSC AWS has installed the AWS SSM Agent that allows you to check remotely the status of the CSC via “AWS Systems Manager” and “Run Commands”.

*Note: You can learn more about “Run Commands” on Appendix B*

*Important (\*): It is advisable to manage all CSC (for Hyper-V, AWS, KVM, Vmware, Azure, etc) from the same AWS availability zone.*

*Important (\*\*): Azure Cloud has a function to “Run Commands”.*

## AWS Systems Manager:



The screenshot shows the AWS Systems Manager console. The left sidebar contains the navigation menu with 'AWS Systems Manager' at the top. Under 'Instances & Nodes', 'Managed Instances' is highlighted. The main content area shows the 'Managed instances' page with a search bar and a filter 'Attributes.Ping status: Online'. A table lists the managed instances.

	Instance ID	Name	Ping status	Platform type	Platform name
<input type="radio"/>	mi-0cc7011e7b6b52e6b		Online	Linux	Ubuntu
<input type="radio"/>	mi-03080c9d345dc21d0		Online	Linux	Ubuntu
<input type="radio"/>	mi-0aabbab0719ede8af2		Online	Linux	Ubuntu
<input type="radio"/>	mi-0a81fec4398f3b24f		Online	Linux	Ubuntu
<input type="radio"/>	mi-0df3a35484460ecf5	cgc00024-b	Online	Linux	Ubuntu
<input type="radio"/>	mi-00e884239bdc3c845	csc-10g-a-market	Online	Linux	Ubuntu
<input type="radio"/>	mi-0052a5bb707749e33	cgs00013	Online	Linux	Ubuntu
<input type="radio"/>	mi-09dfdc3c0602551f4	cas00242	Online	Linux	Ubuntu
<input type="radio"/>	mi-04a8ed4df6b3346f7		Online	Linux	Ubuntu
<input type="radio"/>	mi-01fd3c39005de7c10	cgc00024-a	Online	Linux	Ubuntu

Please, note that in this example the availability zone is eu-west-1. Check your availability Zone when doing this.

The steps required to register the AWS SSM Agent are two:

1. From your EC2 Console (\*\* in the zone selected for management), go to AWS Systems Manager > Hybrid Activations > Create an activation

Note: We recommend to create an Activation per CSC and on “Default instance name” to put the name of the CSC instance (or CSC ID or the name of your “Location” for easy identification)

**AWS Systems Manager** X

Quick Setup

Operations Management

- Explorer *New*
- OpsCenter
- CloudWatch Dashboard
- Trusted Advisor & PHD

Application Management

- Resource Groups
- AppConfig *New*
- Parameter Store

Actions & Change

- Automation
- Change Calendar *New*
- Maintenance Windows

Instances & Nodes

- Compliance
- Inventory
- Managed Instances
- Hybrid Activations** 1
- Session Manager
- Run Command
- State Manager
- Patch Manager
- Distributor

### Activation setting

Create a new activation. After you complete the activation, you receive an activation code and ID. Use the code and ID to register SSM Agent on hybrid and on-premises servers or virtual machines. [Learn more](#)

Activation description- *Optional*

CSC-NAME 2

Maximum 256 characters

Instance limit

Specify the total number of servers and VMs that you want to register with AWS. The maximum is 1000.

1

Maximum number is 1000.

To register more than 1,000 managed instances in the current AWS account and Region, change your account settings to use advanced instances. [Learn more](#) [Change setting](#)

**IAM role**

To enable communication between SSM Agent on your managed instances and AWS, specify an IAM role

☒ Use the default role created by the system  
(AmazonEC2RunCommandRoleForManagedInstances)

☐ Select an existing custom IAM role that has the required permissions

**Activation expiry date**

This date specifies when the activation expires. If you want to register additional managed instances after the expiry date, you must create a new activation. This expiry date has no impact on already registered and running instances.

yyyy-mm-ddThh:mm-00:00

The expiry date must be in the future, and not more than 30 days into the future

Default instance name- *Optional*

Specify a name to help you identify this managed instance when it is displayed in the console or when you call a List API.

CSC-NAME 3

Maximum 256 characters.

4

Cancel **Create activation**

When you click “Create an Activation” you will receive the following information:

✓ You have successfully created a new activation. Your activation code is listed below. **Copy this code and keep it in a safe place as you will not be able to access it again.**

**Activation Code** ws1NljbgCM5pR1jbbUcU

**Activation ID** 7c4198bc-e89a-4f95-993e-b17a4934c4a4

You can now install amazon-ssm-agent and manage your instance using Run Command. [Learn more](#)

Please, keep copy this values on a safe place. You will need this to register the AWS SSM client on the CSC.

- From the CSC Admin Tasks Menu, select “5) AWS SSM Agent (Register or De-Register)”. You will asked for the Activation Code, Activation ID and AWS Region where to register the CSC. (Check your AWS URL <https://eu-west-1.console.aws.amazon.com/ec2/v2/home?region=eu-west-1#>)

```

Do you want to Register (start) the AWS SSM Agent (y/n) y
Please, ingress Activation Code, Activation ID and Region (example: eu-west-1)
Activation Code :2C9+dZ9+DYyCnp6LXaZh
Activation ID :a2317499-ca3c-4574-860d-92d587911fa3
Region :eu-west-1

AWS SSM Agent is active (running) since Thu 2019-02-07 12:15:12 UTC; 37ms ago
Registration values: {"ManagedInstanceID":"mi-0b5653473976667f0","Region":"eu-west-1"}

Press ENTER to continue

```

Done! You have the CSC integrated with AWS now with the instance-id “mi-0b5653473976667f0” in this case).

### 7.2.1.1 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 Thu 2019-02-07 12:15:12 UTC; 7min ago
Registration values: {"ManagedInstanceID":"mi-0b5653473976667f0","Region":"eu-west-1"}

```

## 7.2.2 Change Timezone

The CSC automatically takes the time and timezone from the virtual platform but you can change if it is not correct or you want another value.

## 7.3 Bypass Proxy

The Bypass Proxy allows you to connect certain allowed Domains direct to Internet. 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 pay attention to following examples:

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

### 7.3.1 View Current Bypass List

This commands shows the current domains and subdomains allows to go direct to Internet. By default the list is “blank” blocking all traffic.

```
Selection: 8  
  
This is the list of current Domains configured:  
  
Press ENTER to continue
```

### 7.3.2 Configure Bypass List

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

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

#### 7.3.2.1 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/something/<pacname>.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.fullldomain.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:

The screenshot shows the 'Edit PAC File' interface in the Zscaler console. It includes a form with the following fields:

- Description:** CSC Bypass Proxy
- PAC File Name:** cscbypass.pac
- Domain:** maidenheadbridge.com
- Obfuscate URL:** Unchecked

Below the form is a section titled 'PAC File Contents' containing a code editor with the following JavaScript code:

```
1 function FindProxyForURL(url, host) {
2     var bypassproxy="PROXY 10.1.1.1:3128; PROXY 10.2.2.2:3128";
3
4     /* CSC bypass*/
5     if ((shExpMatch(host, "*.firstdomain.com")) ||
6         (shExpMatch(host, "www.fullldomain.co.uk")) ||
7         (shExpMatch(host, "*.anotherdomain.com")) ||
8         (shExpMatch(host, "*.salesforce.com")) ||
9         (shExpMatch(host, "*.lastdomain.com"))){
10         return bypassproxy
11     }
12 }
```

At the bottom of the window are buttons for 'Save', 'Cancel', 'Verify', and 'Delete'.

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

Edit PAC File

PAC File

Description

pacha

PAC File Name

pacha.pac

Domain

maidenheadbridge.com

Obfuscate URL

☒

PAC File Contents

```
36 var bypassproxy="PROXY 172.19.0.217:3128; PROXY 192.168.1.220:3128";
37
38 /* CSC bypass*/
39 if ((shExpMatch(host, "*.firstdomain.com")) ||
40     (shExpMatch(host, "www.fulldomain.co.uk")) ||
41     (shExpMatch(host, "*.anotherdomain.com")) ||
42     (shExpMatch(host, "*.salesforce.com")) ||
43     (shExpMatch(host, "*.lastdomain.com"))){
44     return bypassproxy
45 }
46
47 // c) Use Zscaler for : www.company.com (overwriting b) sentence *.company.com)
48 if ((shExpMatch(host, "www.company.com"))){
49     return cscvpha
50 }
51
52 // b) Bypass Internal domains and subdomains: intranet.company.com, *.mail.company.r
53
54 if ((shExpMatch(host, "intranet.company.com")) ||
55     (shExpMatch(host, "*.company.com")) ||
56     (shExpMatch(host, "*.mail.company.net"))){
57     return "DIRECT";
58 }
59
```

Verify

Save

Cancel

Delete

**Important: Proxy Bypass is reachable only on port TCP 3128**

CSC for Azure – Administrator Guide

Page 39

Date 14/02/2021

## Configuration Steps:

The console has a help included. Select “See PAC Bypass Example” to see it.

```

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 Cloud, Nodes, VPN Credentials, DNS, Syslog and more
13) Switch Tunnels - Primary / Secondary

e) Exit
Selection: 9

Please, select method to configure Bypass List

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

Your current Bypass PAC URL is http://pac.<cloudname>.net/something/<pacname>.pac

1) Update Bypass List
2) Change Bypass PAC URL
3) See PAC Bypass Example
4) Quit
Enter your choice: 3

Instructions when using Bypass PAC:

1) Create the http://pac.<cloudname>.net/something/<pacname>.pac using the Template example on your Zscaler console.

Template example for PAC Bypass:
-----
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.fullldomain.co.uk")) ||
        (shExpMatch(host, "*.anotherdomain.com")) ||
        (shExpMatch(host, "*.salesforce.com")) ||
        (shExpMatch(host, "*.lastdomain.com"))){
        return bypassproxy
    }
}
-----

2) Replace with your values and Copy this information to your production PAC files
3) On your CSC, add your Bypass PAC URL like, http://pac.<cloudname>.net/something/<pacname>.pac
3) Update the Bypass List on the CSC via SSH or AWS Run Command.

```

After the creation of the PAC file for Bypasses, go to :

- Menu 9: Configure Bypass List
  - 1) Auto – Bypass PAC URL



```
Selection: 9
Please, select method to configure Bypass List
1) Auto - Bypass PAC URL
2) Manual
3) Quit
Enter your choice: 1
Your current Bypass PAC URL is http://pac.<cloudname>.net/something/<pacname>.pac
1) Update Bypass List
2) Change Bypass PAC URL
3) See PAC Bypass Example
4) Quit
Enter your choice: 2
Please, ingress Bypass PAC URL
Bypass PAC URL:http://pac.zscalerbeta.net/maidenheadbridge.com/cscbypassdoc.pac
Your current Bypass PAC URL is: http://pac.zscalerbeta.net/maidenheadbridge.com/cscbypassdoc.pac
Do you want to refresh Bypass List? (y/n)? y
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
Bypass List updated sucessfully
Press ENTER to continue
```

Steps:

1. Select 2) Change Bypass PAC URL
2. Ingress your Bypass PAC URL value
3. Refresh the Bypass List. At this point the CSC is retrieving the URL (hosts) to bypass from the Zscaler PAC servers.
4. The list is showed for your acceptance.
5. Apply changes.

Done!

Verify the Bypass list:

```
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 Cloud, Nodes, VPN Credentials, DNS, Syslog and more
13) Switch Tunnels - Primary / Secondary

e) Exit

Selection: 8

This is the list of current Domains configured:

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

Press ENTER to continue
```

### 7.3.2.2 2) Manual

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

1. Select Option 2)

```
Please, select method to configure Bypass List

1) Auto - Bypass PAC URL
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
.firstdomain.com
www.fulldomain.co.uk
portquiz.net
.salesforce.com
.lastdomain.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
portquiz.net
.salesforce.com
.lastdomain.com

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

6. Apply Changes (y) or discard (n). If “y” you will receive the following message
7. Bypass List update successfully.

```
Do you want apply changes? (y/n)? y
Bypass List updated sucessfully
```

## 7.4 Log Information

This section shows the Tunnel information and when the CSC was powered up.

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

You can see the current month or last six months. Here the Current Month for our device under test:

```
Selection: 10
Current Month (February 2019) Logs for csc-any-azure-02
Feb  5 09:45:11 root: (MHB-CSC)(DOWN) No active tunnel since Tue Feb  5 09:45:11 UTC 2019
Feb  5 09:45:42 root: (MHB-CSC)(UP) Primary tunnel is active since Tue Feb  5 09:45:42 UTC 2019
```

## 7.5 Configuration Wizards

```
Configuration Wizards
12) Change Cloud, Nodes, VPN Credentials, DNS, Syslog and more
13) Switch Tunnels - Primary / Secondary
14) High Availability changing Route/s
15) Update ZEN Nodes Database
```

### 7.5.1 Change Cloud, Nodes, VPN Credentials, DNS, Syslog and more

In this section you can run the initial configuration wizard to change Cloud & Zscaler Nodes, VPN Credentials, DNS servers, Bypass URL and Syslog Servers.

```
Welcome to the CSC Anywhere Configuration Wizard
1) Configuration required on your Zscaler Console: VPN credentials and Location
--> VPN Credentials creation: Go to > Administration > VPN Credentials > Add VPN Credential -> Select Authentication Type = FQDN and configure 'User ID' and 'Pre-Shared Key'
--> Location creation: Go to > Administration > Location > Add Location. Put your Location values and select 'VPN Credentials' created in the step before
2) Run the Wizard on the CSC and Select Cloud, Nodes, input VPN Credentials, DNS Servers, Bypass PAC URL and Syslog Servers

Current Values Configured:
-----
ZSCALER INFORMATION
Zscaler Cloud: zscalerthree
Primary ZEN node: ManchesterI | Hostname: man1-vpn.zscalerthree.net | IP: 165.225.196.35
Secondary ZEN node: LondonIII | Hostname: lon3-vpn.zscalerthree.net | IP: 165.225.16.38
-----
CREDENTIALS INFORMATION
User ID: csc-azure@maidenheadbridge.com | Pre-Shared Key: <Run the Wizard to see it>
-----
DNS Server: Azure DNS server 168.63.129.16
-----
Bypass Proxy PAC URL
Your current Bypass PAC URL is http://pac.zscalerthree.net/maidenheadbridge.com/bypass.pac
-----
SYSLOG / SIEM information
Primary Syslog / SIEM IP: 172.31.200.7
Secondary Syslog / SIEM IP: Not configured
Syslog / SIEM TCP port: 514
-----
Are you ready to continue? (y/n) █
```

Details of configuration on Chapter 6.

## 7.5.2 Switch Tunnels - Primary / Secondary

In case you want to switch the Primary / Secondary tunnel you can do it from this menu.

```
Selection: 13
-----
ZSCALER INFORMATION

You current Zscaler Cloud and Nodes are:

Zscaler Cloud:  zscalerthree
Primary ZEN node: ManchesterI | Hostname: man1-vpn.zscalerthree.net | IP: 165.225.196.35
Secondary ZEN node: LondonIII | Hostname: lon3-vpn.zscalerthree.net | IP: 165.225.16.38

Do you want to switch these values? (y/n) y

Validating Configuration

Your Cloud is: zscalerthree

Checking Node LondonIII hostname lon3-vpn.zscalerthree.net
Hostname lon3-vpn.zscalerthree.net has IP 165.225.16.38
Node LondonIII is Alive

Checking Node ManchesterI hostname man1-vpn.zscalerthree.net
Hostname man1-vpn.zscalerthree.net has IP 165.225.196.35
Node ManchesterI is Alive

Are this values correct? (y/n)? (answering 'y' will reboot the CSC):
```

## 7.5.3 High Availability changing Route/s

```

Selection: 14

This Wizard is for High Availability scenarios when changing Next-Hop on Routes via CSC.

-----
How to configure:

Recommended: Use the same Resource Group for both CSCs and Route Tables. This is to avoid permission problems with IAM roles.

The following instructions are considering that all resources are on the same Resource Group:

1) Deploy a pair of CSCs with the following conditions:
  1.1) There is connectivity each other via their internal interfaces.
  1.2) On each CSC VM, go to Identity -> System Assigned and Turn ON status. (and Save).
2) Go to Resource Group -> Access Control (IAM) and Click '+ Add'
  2.1) Select 'Add role assignment'
  2.2) Input the following values:
      -> Role: Contributor
      -> Assign Access to: Virtual Machine
      -> Select: <Select both CSC's VMs> (and Save)
3) Create (or move) the Route Tables inside the same Resource Group than the CSCs.
  3.1) Go to Routes (inside the Route Table) and create the Routes that will be controlled by the CSC HA group:
      -> Route name: <any name you want>
      -> Address prefix: <Subnet/Mask>
          Examples: 0.0.0.0/0 (if you want to send all traffic via Zscaler) or 185.46.212.88/32 (when using PAC files and/or Explicit Proxy)
      -> Next hop type: Virtual Appliance
      -> Next hop address: <Input GW (eth1, first IP) of any CSC>
  3.2) Go to Subnets and associate the Subnet with the Route Table.
  3.3) Repeat the process if you want to add more Routes. The CSC HA functionality can manipulate multiple Routes.
4) Obtain the following values and Run the Wizard
  4.1) Route, Route Table, Resource Group
  4.2) Computer Name and Resource Group of each CSC

How it works:

The CSCs on the HA pair will automatically select the Next-Hop for the Route/s configured.

-----

The HA service is: active (running) since Fri 2020-05-15 11:08:32 UTC; 21h ago

Identity Type: SystemAssigned

Current values configured are:

Route/s (Qty)= 3
Route 1: myroute (Route Table=csc-rt-1, Resource Group=Development)
Route 2: server-farm-1 (Route Table=csc-rt-for-servers, Resource Group=Development)
Route 3: CSC-Zscaler-Default (Route Table=Csc-Routing-table, Resource Group=Development)

Computer Name of other CSC in the pair: csc-v-2-0-B (Resource Group=Development)

Do you want to change this values?

1) Yes
2) No
3) Restart HA Service
4) Reset to default values
Enter your choice:

```

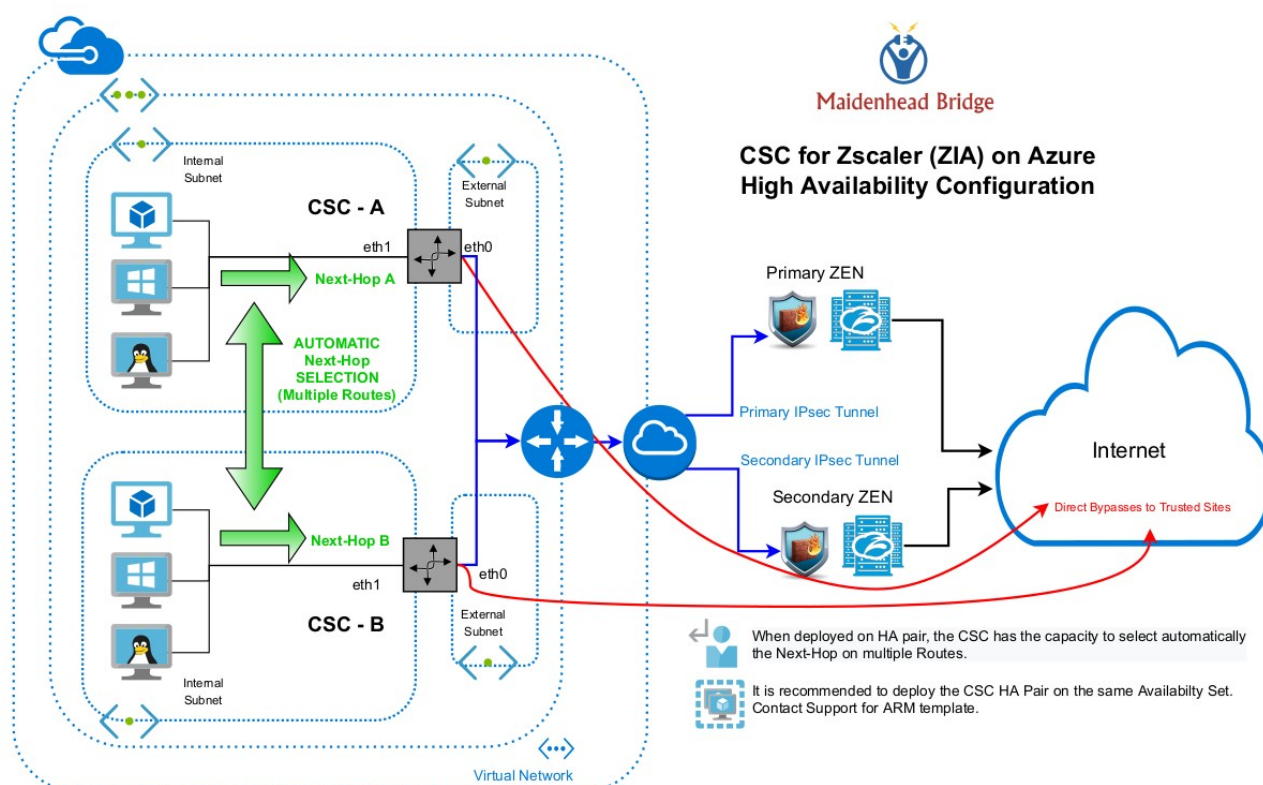
See Appendix A for a detailed configuration with examples.

## 8 Appendix A: High Availability to Zscaler using CSCs

### 8.1 Introduction:

When deployed on HA pair, the CSC has the capability to manage the “Next-Hop” of the route/s configured.

There is no limit of the amount of routes that can be configured. This allows to manipulate routes to Zscaler on more than one Route-Table.



## 8.2 Pre-requisites

The help provided on by the Configuration Wizard contains the pre-requisites:

This Wizard is for High Availability scenarios when changing Next-Hop on Routes via CSC.

-----  
How to configure:

Recommended: Use the same Resource Group for both CSCs and Route Tables. This is to avoid permission problems with IAM roles.

The following instructions are considering that all resources are on the same Resource Group:

- 1) Deploy a pair of CSCs with the following conditions:
  - 1.1) There is connectivity each other via their internal interfaces.
  - 1.2) On each CSC VM, go to Identity -> System Assigned and Turn ON status. (and Save).
- 2) Go to Resource Group -> Access Control (IAM) and Click '+ Add'
  - 2.1) Select 'Add role assignment'
  - 2.2) Input the following values:
    - > Role: Contributor
    - > Assign Access to: Virtual Machine
    - > Select: <Select both CSC's VMs> (and Save)
- 3) Create (or move) the Route Tables inside the same Resource Group than the CSCs.
  - 3.1) Go to Routes (inside the Route Table) and create the Routes that will be controlled by the CSC HA group:
    - > Route name: <any name you want>
    - > Address prefix: <Subnet/Mask>

Examples: 0.0.0.0/0 (if you want to send all traffic via Zscaler) or 185.46.212.88/32 (when using PAC files and/or Explicit Proxy)

    - > Next hop type: Virtual Appliance
    - > Next hop address: <Input GW (eth1, first IP) of any CSC>
  - 3.2) Go to Subnets and associate the Subnet with the Route Table.
  - 3.3) Repeat the process if you want to add more Routes. The CSC HA functionality can manipulate multiple Routes.
- 4) Obtain the following values and Run the Wizard
  - 4.1) Route, Route Table, Resource Group
  - 4.2) Computer Name and Resource Group of each CSC

How it works:

The CSCs on the HA pair will automatically select the Next-Hop for the Route/s configured.

-----



## 8.3 Configuration example:

### 8.3.1 Route Information

In this example, we are going to put under control of the CSC HA pair two routes:

1. **Route: CSC-Zscaler-Default** (Route Table=Csc-Routing-table, Resource Group=Development): This route has destination (Address Prefix): 0.0.0.0/0 and belongs to a route-table with subnets associated to Virtual Desktops. In this case, I want to send all traffic to Zscaler.

Routes

Search routes

Name	↑↓ Address prefix	↑↓ Next hop
CSC-Zscaler-Default	0.0.0.0/0	172.31.200.17

2. **Route: server-farm-1** (Route Table=csc-rt-for-servers, Resource Group=Development): This route has destination (Address Prefix): 185.46.212.88/32 and belongs to a route-table with subnets associated to Servers. In this case, I want to send only Web traffic setting the Proxy IP: 185.46.212.88 (Zscaler Global Proxy).

Routes



Search routes

Name	↑↓ Address prefix	↑↓ Next hop
server-farm-1	185.46.212.88/32	172.31.200.17

### 8.3.2 CSC Information

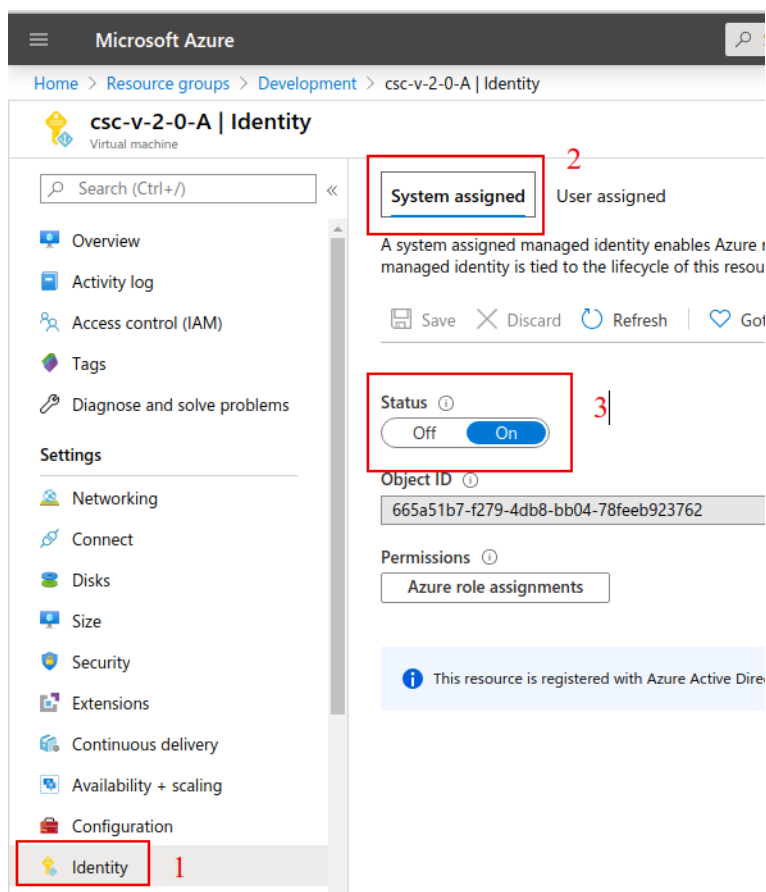
We need to obtain the “Computer Name” and Resource Group of each CSC on the pair. In this example will be:

- csc-v-2-0-A
- csc-v-2-0-B

<input type="checkbox"/>	 csc-v-2-0-A	Virtual machine
<input type="checkbox"/>	 csc-v-2-0-B	Virtual machine

### 8.3.3 Identity

On each CSC, Go to: Identity → System Assigned and turn ON status:



### 8.3.4 IAM Role

*Note: In this example, the VMs and Route Tables are under the same Resource Group. For this reason, I am going to enable the IAM Role to the Resource Group and the IAM Role will be inherited.*

*If you have the Route Tables on different Resource Group, please, apply the proper permissions.*

Go to:

1. Resource Group
2. Access control (IAM)
3. Click “Add”
4. Add role assignment:
  - 4.1. Role: Contributor
  - 4.2. Assign Role to: Virtual Machine.
5. Select the CSCs

Now, Check Roles assignments:

Name	Type	Role	Scope
<input type="checkbox"/> Contributor			
<input type="checkbox"/> csc-v-2-0-A /subscriptions/ffde02fb-c38f-45fb-9e31-8...	Virtual Machine	Contributor	This resource
<input type="checkbox"/> csc-v-2-0-B /subscriptions/ffde02fb-c38f-45fb-9e31-8...	Virtual Machine	Contributor	This resource

and, when checking the Route Table → Access Control → Role assignments:

Name	Type	Role	Scope
<input type="checkbox"/> Contributor			
<input type="checkbox"/> csc-v-2-0-A /subscriptions/ffde02fb-c38f-45fb-9e31-89e5303be5f1/r...	Virtual Machine	Contributor	Resource group (Inherited)
<input type="checkbox"/> csc-v-2-0-B /subscriptions/ffde02fb-c38f-45fb-9e31-89e5303be5f1/r...	Virtual Machine	Contributor	Resource group (Inherited)

You can see that the CSCs are able to manage this Route Table.

## 8.4 Running the configuration wizard

Enter the Route (Route-tables / Resource Group) values and other CSC Computer Name (+Resource Group)

```

Do you want to change this values?
1) Yes
2) No
3) Restart HA Service
4) Reset to default values
Enter your choice: 1

Identity Type: SystemAssigned    The Wizard checks Identity

Please, input the Route/s values:    Enter your first ROUTE
Route Name= CSC-Zscaler-Default
Route Table= Csc-Routing-table
Resource Group= Development

Do you want to add another Route? (y/n)? y    Add next ROUTE
Route Name= server-farm-1
Route Table= csc-rt-for-servers
Resource Group= Development

Do you want to add another Route? (y/n)? n

Please, input values of other CSC in the pair    Put "Other CSC" Computer Name
Computer Name= csc-v-2-0-B
Resource Group= Development

Values to configure are:    Confirm values to configure
Route/s (Qty)=2
Route 1: CSC-Zscaler-Default (Route Table=Csc-Routing-table, Resource Group=Development)
Route 2: server-farm-1 (Route Table=csc-rt-for-servers, Resource Group=Development)
Computer Name of other CSC in the pair: csc-v-2-0-B (Resource Group=Development)

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

CSC HA is : active (running) since Sat 2020-05-16 20:38:25 UTC; 27ms ago

```

Now, do the same on the Other CSC.

Finally, check the status of the HA using “Show Configuration and Status” menu.

```

HIGH AVAILABILITY Information
The HA service is: active (running) since Sat 2020-05-16 20:38:25 UTC; 1h 28min ago
Identity Type: SystemAssigned
Route to Zscaler using Next Hop: 172.31.200.14 of VM: csc-v-2-0-A (this CSC)
Current values configured are:
Route/s (Qty)= 2
Route 1: CSC-Zscaler-Default (Route Table=Csc-Routing-table, Resource Group=Development)
Route 2: server-farm-1 (Route Table=csc-rt-for-servers, Resource Group=Development)
Computer Name of other CSC in the pair: csc-v-2-0-B (Resource Group=Development)

```

## 9 Appendix B – 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.

### 9.1.1 Example PAC Load Balancing

If you want to use both CSC at the same time to duplicate your bandwidth for Web Traffic, this simple PAC file will do the job.

Please, note that you need to put the IP values of csc1vip, csc2vip, csc1bypass and csc2bypass. You can read this values from “Show Configuration and Status Menu”

#### Load Balancing PAC file.

```
function FindProxyForURL(url, host) {
// =====
// Section 1: Zscaler standard PAC values

var privateIP = /^(0|10|127|192\.168|172\.[1|6|7|8|9]|172\.2[0-9]|172\.3[01]|169\.254|192\.88\.[0-9])\.+$/;

var resolved_ip = dnsResolve(host);

/* Don't send non-FQDN or private IP auths to us */
if (isPlainHostName(host) || isInNet(resolved_ip, "192.0.2.0", "255.255.255.0") || privateIP.test(resolved_ip))
    return "DIRECT";

/* FTP goes directly */
if (url.substring(0, 4) == "ftp:")
    return "DIRECT";

/* test with ZPA */
if (isInNet(resolved_ip, "100.64.0.0", "255.255.0.0"))
    return "DIRECT";

// =====
// Section 2: Load Balancing: 2 x Cloud Security Connectors
// Azure: 500 Mbps

// Get NIC IP address
nicIp = myIpAddress();

// Assigning values to "tozscaler" and "bypass"
if (isInNet(nicIp, "0.0.0.0", "0.0.0.1")) {
    var tozscaler = "PROXY csc1vip:80; PROXY csc2vip:80";
    var bypass = "PROXY csc1bypass:3128; PROXY csc2bypass:3128";
}

if (isInNet(nicIp, "0.0.0.1", "0.0.0.1")) {
    var tozscaler = "PROXY csc2vip:80; PROXY csc1vip:80";
    var bypass = "PROXY csc2bypass:3128; PROXY csc1bypass:3128";
}

// =====
// Section 3: Bypass via Cloud Security Connectors

// Bypass via CSC Public IPs
if ((shExpMatch(host, "*.okta.com")) ||
    (shExpMatch(host, "*.oktacdn.com")) ||
    (shExpMatch(host, "*.okta-emea.com")) ||
    (shExpMatch(host, "login.mydomain.com")) ||
    (shExpMatch(host, "portquiz.net"))) {
    return bypass
}

// =====
// Section 4: Default Traffic

/* Default Traffic Forwarding. Forwarding to Zen on port 80, but you can use port 9400 also */
return tozscaler
}
```

## 10 Appendix C – AWS Systems Manager “Run Commands” 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 CSCs.

### 10.1 AWS Systems Manager: Documents

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

You can create Documents for CSC, Copying/Pasting the information that follows.

#### 10.1.1 Creating a Document

From AWS Systems Manager > Shared Resources > Documents → Click “Create Document”

Put the “Name”, “Document Type” = Command and fill “Content”

**Document details**  
Document defines the actions that AWS Systems Manager performs on your managed instances.

**Name**  
Specify a unique name among your documents.  
MHB-CSC-ShowConfigurationAndStatus  
Between 3 and 128 characters. Alphanumeric, "-", ".", "/", or "\*" only.

**Target type - optional**  
Specify the types of resources the document can run on. For example, "AWS::EC2::Instance" or "\*" for all resource types. [Learn More](#)

**Document type - optional**  
Select a document type based on the service that you want to use.  
Command document

**Content**

☒ JSON  
Specify document content in JSON format.

☐ YAML  
Specify document content in YAML format.

```

1 {
2   "schemaVersion": "2.2",
3   "description": "MHB - CSC - Show Configuration and Status",
4   "macros": {
5     "action": "aws:runShellScript",
6     "name": "RunScript",
7     "inputs": {
8       "runCommand": [
9         "/home/cscadmin/aw-nt4"
10      ]
11     }
12   }
13 }
  
```

Reload

Document tags - optional

Cancel Create document

Click “Create Document”

## 10.1.2 List of Documents

Please, create the “Documents” using this values:

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

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

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

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

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

Name	MHB-CSC-ShowLogCurrentMonth-2500Characters
Content	<pre>{   "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"         ]       }     }   ] }</pre>



Name	MHB-CSC-ShowLogLastSixMonths
Content	<pre>{   "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"         ]       }     }   ] }</pre>

Name	MHB-CSC-SwitchTunnels
Content	<pre>{   "schemaVersion": "2.2",   "description": "MHB - CSC – Switch Tunnels",   "mainSteps": [     {       "action": "aws:runShellScript",       "name": "Runscripts",       "inputs": {         "runCommand": [           "/home/cscadmin/aws-tun-switch"         ]       }     }   ] }</pre>

### 10.1.3 Run Commands

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

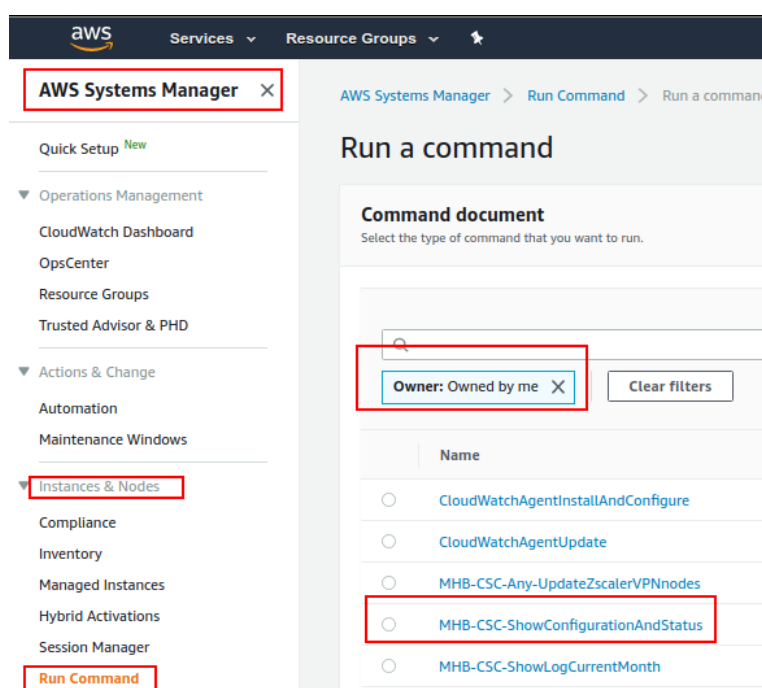
You can see the results of the operation on the “Output” section or to store the results on a S3 Buckets for further inspection.

*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.*

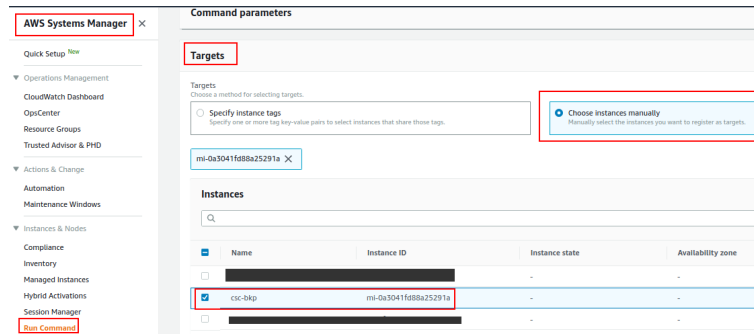
To Run Commands go to: AWS Systems Manager > Instances & Nodes > Run Command

Here an example of Running: MHB-CSC-ShowConfigurationAndStatus

1. Run a Command
2. Select the Document created (Tip: Select “Owned by me”)

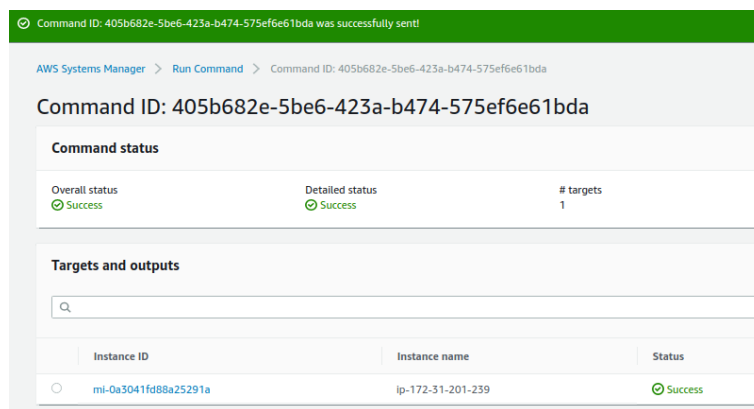


3. Scroll down and Select the Instances
4. We are selecting only one instance, but you can select as much as you want.



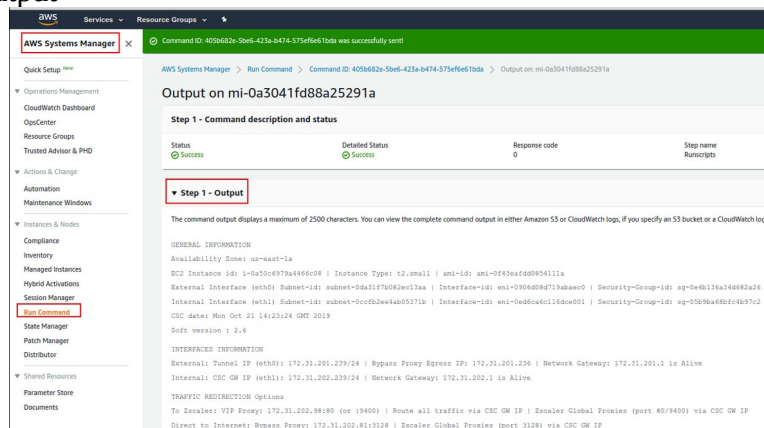
5. Click Run

Next Screen is:



6. Click “Instance ID” (mi-0a3041fd88a25291a)

7. Expand “Output”



[Commands](#) > [Output](#)

### Output for Runscripts

```
GENERAL INFORMATION
Availability Zone: us-east-1d
EC2 Instance Id: i-073558fb385b61521 | Instance Type: t2.small | ami-id: ami-b8ac8cc5
External Interface (eth0) Subnet-id: subnet-818c8ddb | Interface-id: eni-0bc01b4a28b2b6f79 | Security-Group-id: sg-0ff18e7644d1c6ed
Internal Interface (eth1) Subnet-id: subnet-8368ec49 | Interface-id: eni-03f9d912627c65975 | Security-Group-id: sg-0d63fe7212b966de
CSC date: Wed May 2 20:30:28 BST 2018
Soft version : 2.1

INTERFACES INFORMATION
External Interface (eth0) IP: 172.31.96.125/24 | External Gateway: 172.31.96.1 is Alive
Internal Interface (eth1) IP: 172.31.200.191/24 | Internal Gateway: 172.31.200.1 is Alive
VIP Proxy: 172.31.200.220
Bypass Proxy: 172.31.200.112 (--> Bypass Proxy Egress IP 172.31.96.121)

ELASTIC (PUBLIC) IPs INFORMATION
GRE tunnels Public IP: 35.171.35.22
Bypass Proxy Public IP: 35.171.56.120

DNS INFORMATION
Using AWS IP: 169.254.169.253

ZSCALER INFORMATION
Zscaler Cloud: zscalerbeta
GRE tunnel's egress Public IP: 35.171.35.22
Primary Tunnel:
    ZEN Public IP: 104.129.194.38
    Tunnel IPs (local/zem): 172.17.8.113 / 172.17.8.114
Secondary Tunnel:
    ZEN Public IP: 199.168.148.131
```

Only 2500 characters of the output is shown above. If you have logged your output to a S3 bucket, you can view the full output in your S3 bucket.

## **11 Appendix D: Release Notes**

### **11.1 Version 2.5**

This version has the following enhancements:

- The base OS was upgraded to Ubuntu 20.04
- Corrected update of Zscaler Nodes database at first boot.
- When deployed in Zone redundancy, Public IPs (Public IP: Standard SKU) are displayed now on "Show Configuration and Status" test.

### **11.2 Version 2.0**

This version has the following enhancements:

- New! High Availability changing routes to Zscaler. When deployed as HA pair, the CSC for Azure has the capacity to select the best route/s to Zscaler. You can manage multiple routes for any destination. For example, you can configure the default route (0.0.0.0/0) and/or the Zscaler Global ZEN IP address (.i.e. 185.46.212.88/32) and the CSCs on the HA pair will set up the Next Hop automatically.
- "Show Configurations and Status" show the HA Status.

### **11.3 Version 1.5**

This version has the following enhancements:

- The CSC is using now Ubuntu 18.04 as base OS
- Solved a problem when Zscaler Databases are not reachable at start up.
- The menu "Show configuration and status" shows the Public IPs in use for Tunnel and Bypass Proxy.

### **11.4 Version 1.3**

This version has the following enhancements:

- Solved problem when starting the CSC related to a delayed response of the Azure API.
- Solved problem when the Azure/WALinux Agent takes some time to respond after booting the CSC.
- Solved the problem when using subnets other than full subnets (/8, /16, /24)
- Automatically update of ZEN databased at first start up.

- “Show Configurations and Status” shows the statuses for Syslog Servers.

## **11.5 Version 1.0**

This version 1.0 of the Cloud Security Connector (Anywhere) for Azure is initial version based on the version 4.4 of the Cloud Security Connector Anywhere for virtualisation. (Hyper-V, Vmware, etc.)