Maidenhead Bridge

Cloud Security Connector for Azure

Enabling Zscaler ZIA for Azure customers at 250 Mbps

Quick Installation Guide

Version 2.0

(February 2021)

Table of Contents

1 Introduction....3
2 Key benefits of the Cloud Security for Azure....3
3 The CSC on the Azure architecture....4
3.1 Single CSC:....4
3.2 Redundant deployment....5
3.2.1 Example of Routes to Manage....5
3.2.2 Example PAC Load Balancing....6
4 Deploy the Cloud Security Connector....8
4.1 Prerequisites....8
4.2 Launching the CSC from Azure Marketplace....8
4.2.1 Deploying “CSC 250 Mbps – No HA Infrastructure required”....10
4.2.2 Deploying “CSC 250 Mbps – HA Using Availability Sets”....13
4.2.3 Deploying “CSC 250 Mbps – HA Using Availability Zones”....14
5 Next steps:....15

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.

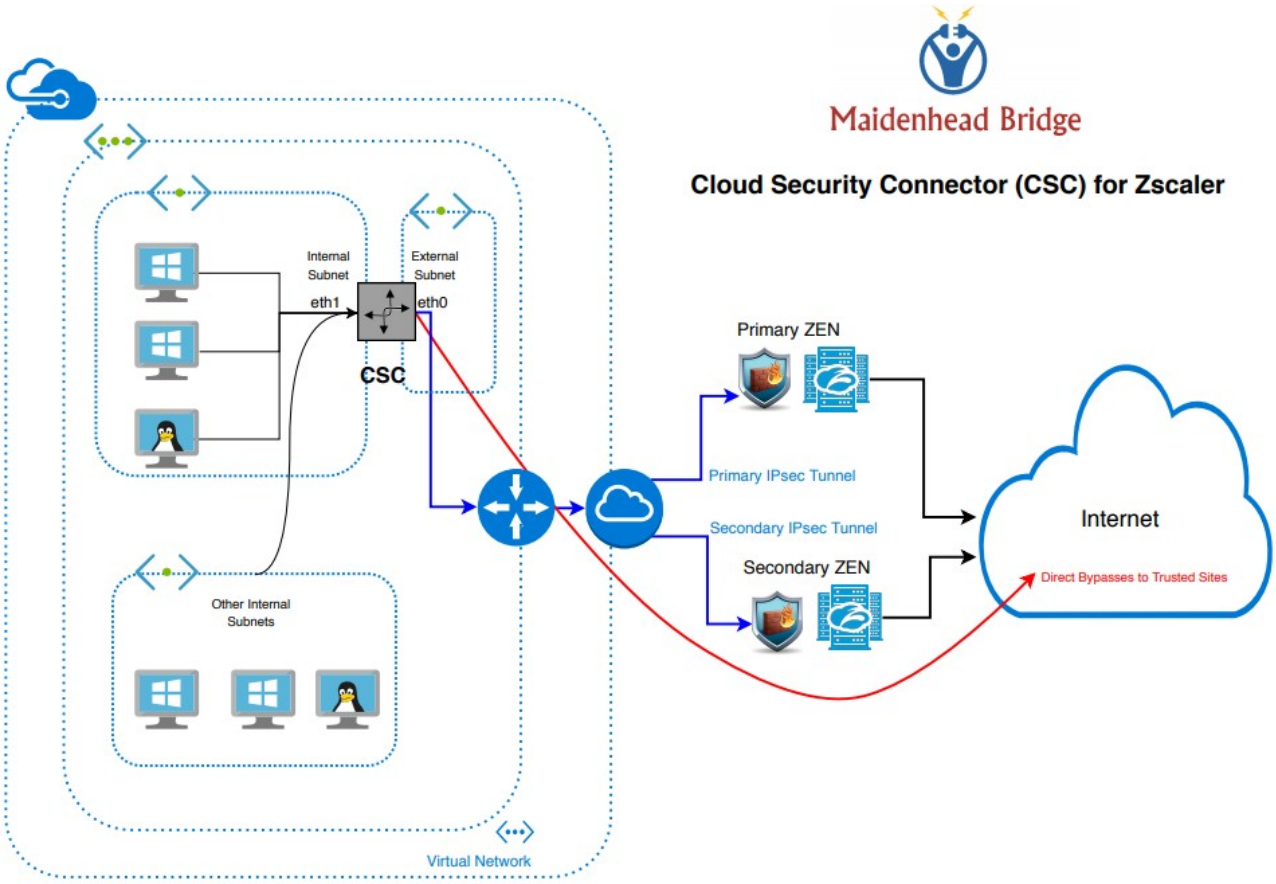
2 Key benefits of the Cloud Security for Azure

- 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:

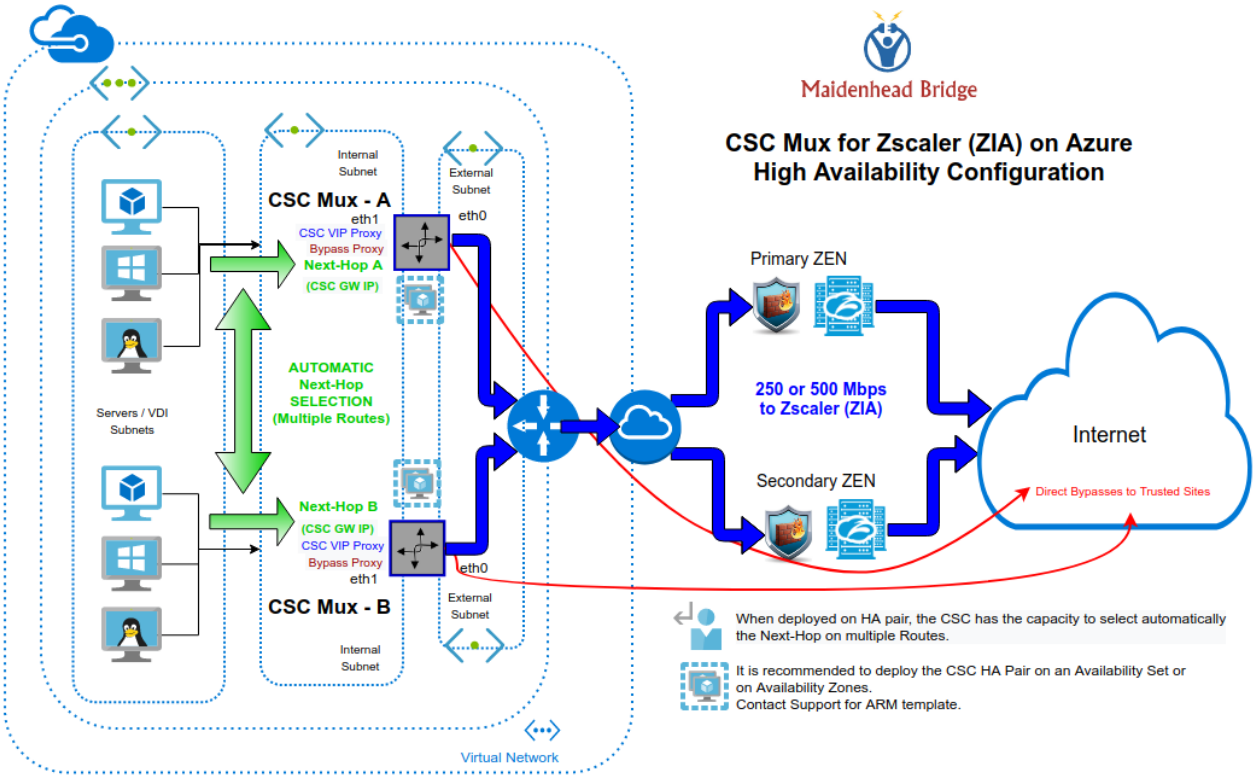


As you can see on the image, eth0 is the “external” interface and eth1 the “internal” interface. In the following chapter we are explaining how to create and install the CSC for Azure.

3.2 Redundant deployment

The CSC in redundant mode can de 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.

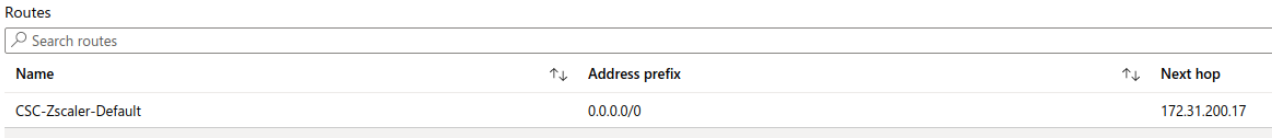
Common destinations to manage are:

Default Route to Internet → 0.0.0.0/0

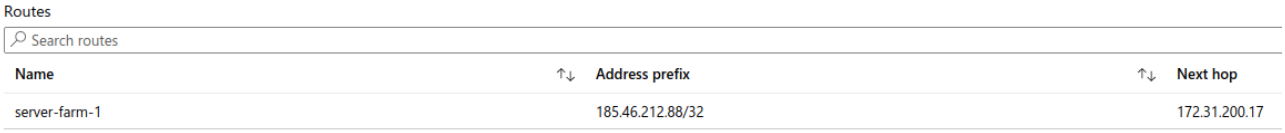
Zscaler Global ZEN IP addresses → 185.46.212.88/32, 185.46.212.89/32, 185.46.212.90/32, 185.46.212.91/32, 185.46.212.92/32, 185.46.212.93/32, 185.46.212.97/32, 185.46.212.98/32.

Routes examples:

All traffic to Zscaler:



To Zscaler Global ZENs:



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\.1[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

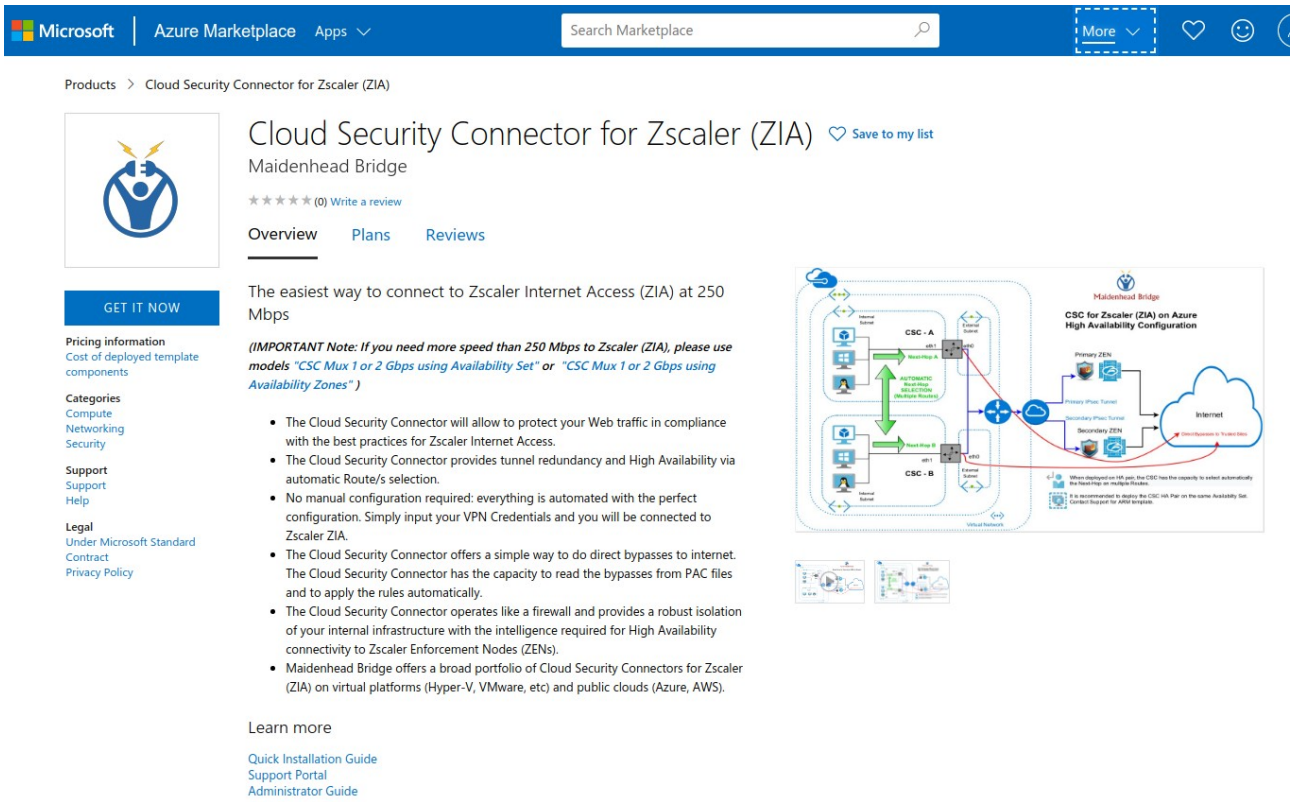
4.1 Prerequisites

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

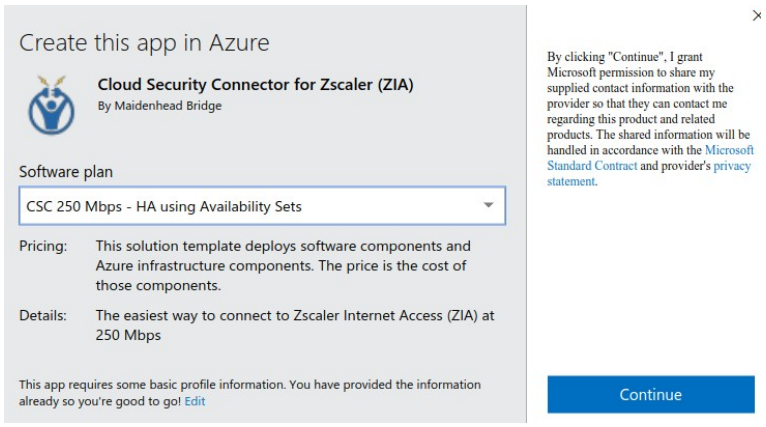
1. **(Optional) SSH Key** if you want to access the CSC using SSH keys. If not, you will we prompted a Password during the installation.
2. **Virtual Network**
3. **External Subnet:** The External Subnet must be on the same Virtual Network than the Internal Subnet.
4. **Internal Subnet:** The Internal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



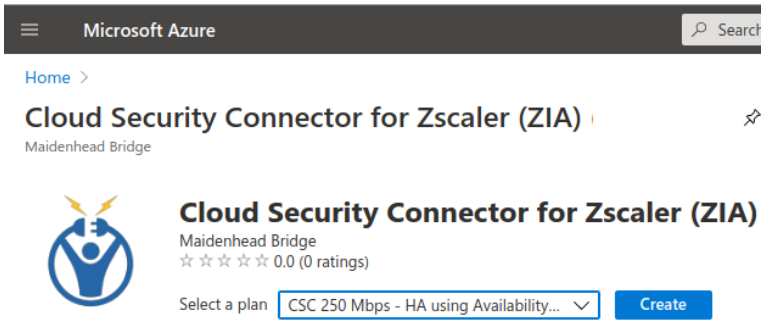
- Click “GET IT NOW”
- Select the Plan:



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

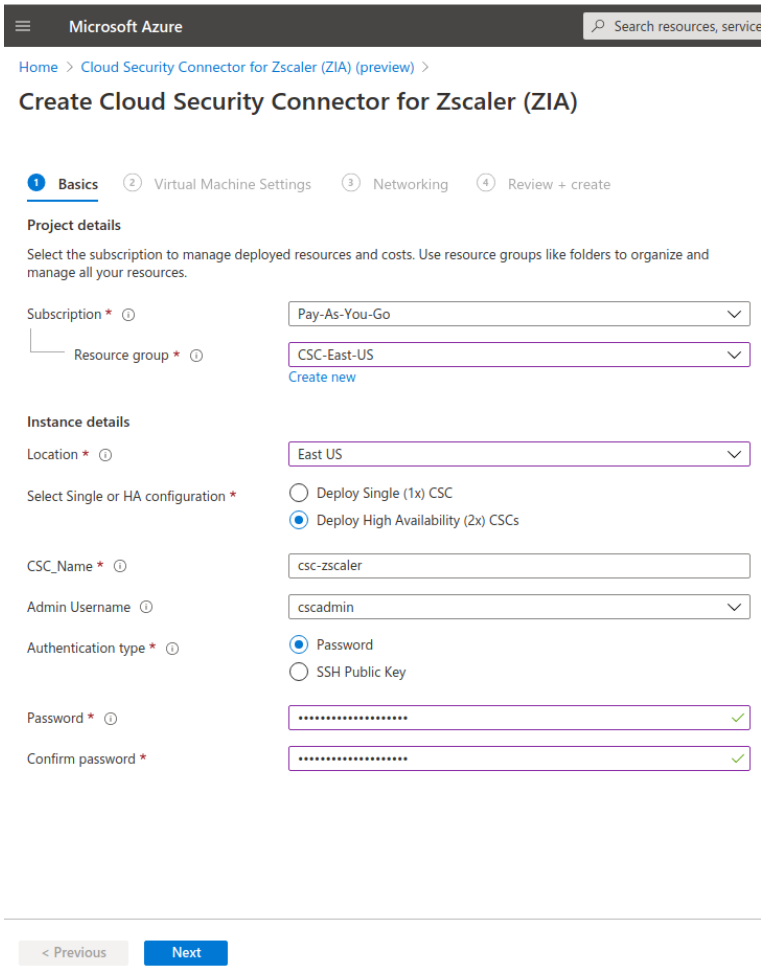
NOTE 1: We recommend always to use Availability Sets or Zones.
NOTE 2: In all plans you can deploy 1xCSC or 2xCSCs.

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



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

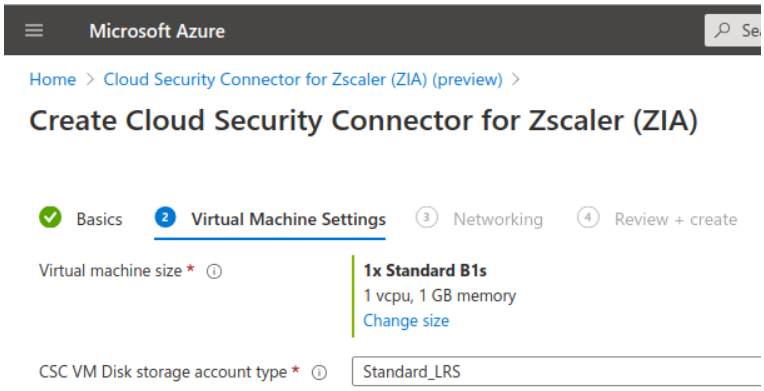
4.2.1 Deploying “CSC 250 Mbps – No HA Infrastructure required”



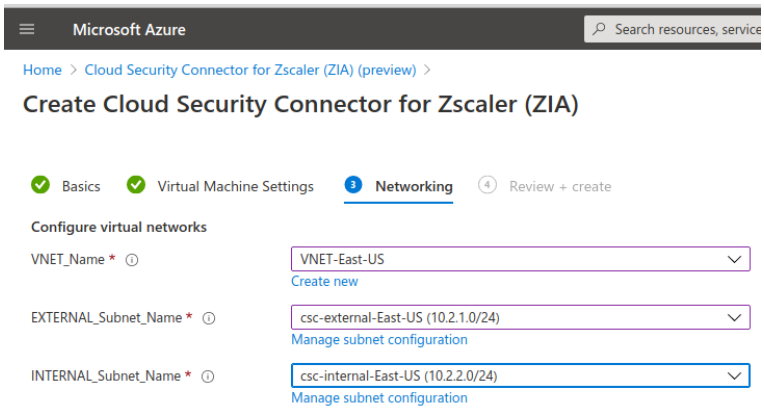
- Insert the values requested (*): Subscription, Resource group, Location, Single or HA configuration, CSC_Name, Authentication type, SSH or Password.

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

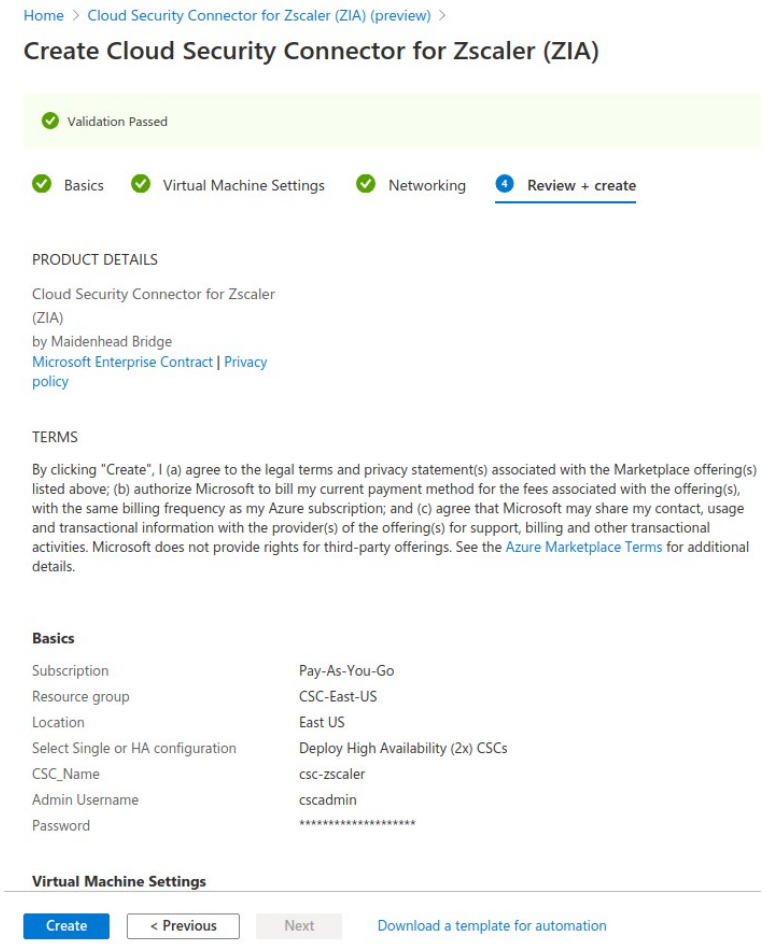
- Click "Next"



- 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"



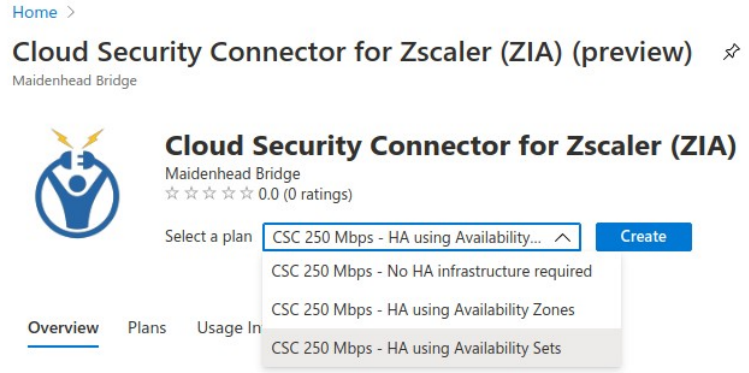
- Select the Virtual Network, External and Internal Subnet.
- Click "Create"



- 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"

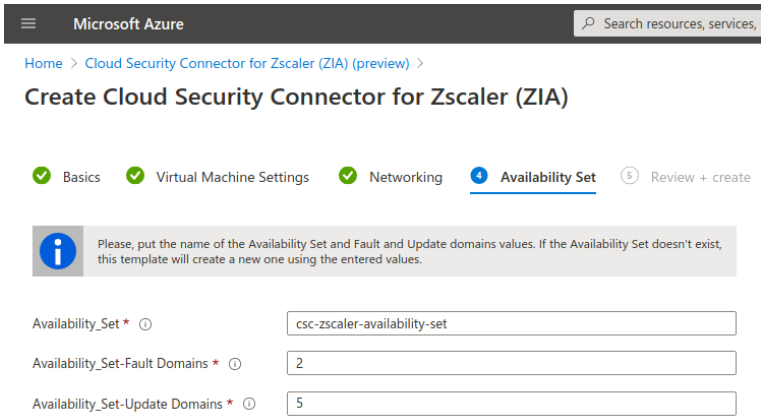


- Click "Create"
- The steps "Basics", "Virtual Machine Settings" and "Networking" are the same than before. Step 4 "Availability Set" is the addition to this Plan:



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

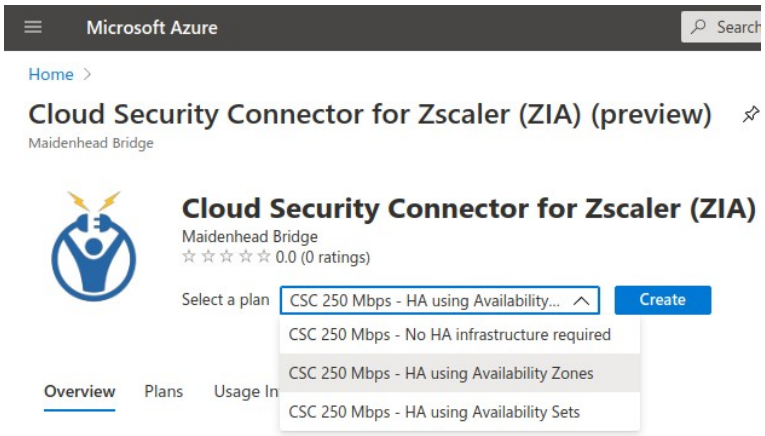
NOTE: Please, put the name of the Availability Set and Fault and Update domains values. If the Availability Set doesn't exist, this template will create a new one using the entered values



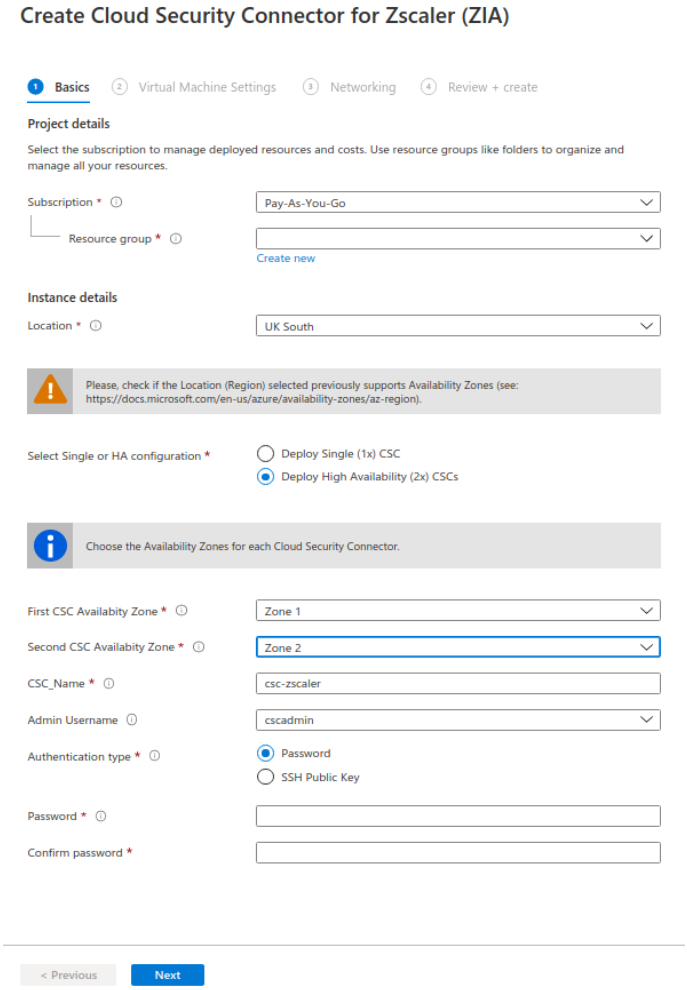
- Click "Next", wait for "Validation passed" and click "Create"

4.2.3 Deploying "CSC 250 Mbps – HA Using Availability Zones"

- Select plan "CSC 250 Mbps – HA using Availability Sets"



- Click "Create"



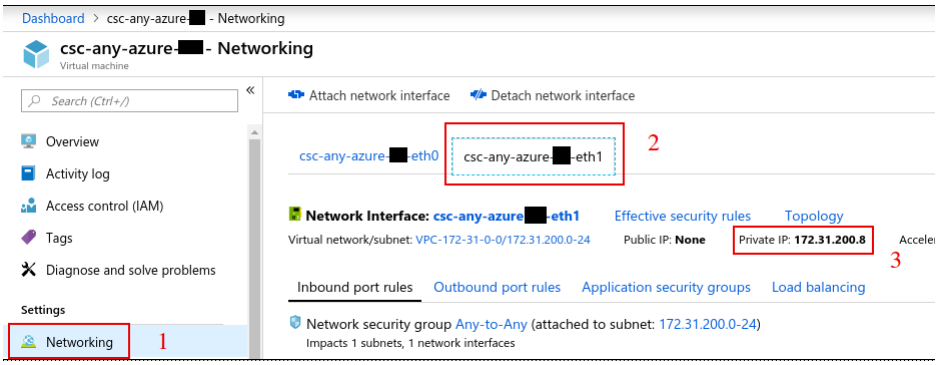
- In this case, you need the only specific to select for this plan is the Availability Zone for each CSC. The rest is the same than before.

5 Next steps:

- On your Zscaler console, create:
  - VPN Credentials
  - Location using the VPN Credentials.
- On you Azure Console, select the Virtual Machine created and find the IP of the Internal Interface (<vmname>-**eth1**)
- SSH the CSC (**cscadmin**@<IP Eth1>) and follow the Initial Wizard Menu. You will be asked for the VPN Credentials, to select the Zscaler nodes Primary and Secondary, etc.
- After running the initial wizard the CSC will be ready for Production.

*Important: The username to access the CSC is: "**cscadmin**"*

Example of how to obtain the IP of the Internal Interface



Initial Configuration Wizard:

```
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)
```

Please, Check "Administration Guide" for full documentation.