



Cloud Security Connector Mux (1/2/4/8) – Azure

with Private Cloud Private Access

(For Azure Cloud)

ilini

quaquagniti



Table of Contents

1 Introduction to Cloud Security Connectors for Zscaler	7
2 Key benefits of the Cloud Security Connector Mux for Azure	8
3 Network Diagrams	9
3.1 CSC Mux for Azure – Single deployment	9
3.2 CSC Mux for Azure – High Availability Deployment	.10
3.3 Traffic Forwarding: Routing and Proxying all together	.11
3.4 High Availability using Azure Load Balancer	.12
3.5 Private Cloud Private Access (PriCPA)	.13
4 Understanding the CSC Mux with PriCPA	.14
4.1 What problem the CSC Multiplex solves?	.14
4.2 What does the CSC Multiplex do?	.15
4.3 The CSC Mux 1, 2, 4 and 8 in action	.16
4.3.1 Speed Test with CSC Mux 1	.16
4.3.2 Speed Test with CSC Mux 2	.16
4.3.3 Speed Test with CSC Mux 4	.16
4.3.4 Speed Test with CSC Mux 8	.16
4.3.5 Iperf test using PriCPA	.17
5 Creating the CSC Mux for Zscaler with PriCPA	.18
5.1 Prerequisites	.18
5.2 Launching the CSC Mux for Azure Marketplace	.18
6 Accessing for first time to your CSC	.27
6.1 SSH to the Admin Console using CSC GW IP	.27
6.1.1 Initial Screen when using configUserData.json file	.28
6.1.2 Initial screen wihout using configUserData.json file	.29
6.1.2.1 Running the initial wizard	.29
7 Zscaler console: create VPN Credentials and Location	.32
7.1 VPN Credential creation	.32
7.2 Create the Location on the Zscaler Console	.32
7.3 Checking tunnel statuses on the CSC console	.33
8 Resources creates by the ARM template	.34
9 The Cloud Security Connector Admin Console:	.36
9.1 Monitoring Tasks	.38
9.1.1 Show Configuration and Status	.38
9.1.1.1 GENERAL INFORMATION	.39
9.1.1.2 INTERFACES INFORMATION	.39
9.1.1.3 TRAFFIC REDIRECTION Options	.39
9.1.1.4 PUBLIC IP Address INFORMATION	.40
9.1.1.5 DNS INFORMATION	.41
9.1.1.6 ZSCALER INFORMATION	.41
9.1.1.7 LOAD BALANCING INFORMATION	.41
9.1.1.8 IPSEC INFORMATION	.41
9.1.1.9 CREDENTIALS INFORMATION	.41

Maidenhead Bridge

9.1.1.10 http://ip.zscaler.com INFORMATION	
9.1.1.11 PRUXY BYPASS	
9.1.1.12 ROUTED BYPASS	
9.1.1.14 SYSLOG INFORMATION	
9.1.1.14.1 System Logs example:	
9.1.1.14.2 Trainic Logs example:	
9.1.1.15 HIGH AVAILABILITY INformation	
9.1.2 Show Interfaces Indific	45
9.1.3 Tepdump	45 //E
9.1.3.1 Tepaulip	45
0.1.4 SDEED TEST	
9.1.4 SPEED TEST	
9.2 CSC Admin Tasks	
9.2.1 AWS SSIM Agent (Register Of De-Register)	
9.2.1.1 Create a Tryblid Activation Trom Aws console	
9.2.1.2 Register the Coc	
9.2.1.5 View the Registered CSC of AWS Systems Manager	50 51
9.2.2 Manage Administrators; escadmin and esceli	
9.2.2.1 Manage Administrators. escadmin and escention	
9.2.2.1.1 Cscautini settings	
9 2 2 1 3 Managing the SSH Key of a User	
9 2 2 2 Restrict SSH Access	
9.2.2.2 Restrict SSIT Access	
9 2 3 Change Timezone	56
9 3 Proxy Bynass	
9 3 1 Proxy Bypass - Traffic Flow	57
9 3 2 View Current Proxy Bynass List	57
9 3 3 Configure Proxy Bypass List	57
9.3.3.1 Auto - Proxy Bypass PAC URI	58
9.3.3.2 Manual Proxy Bypass Configuration.	
9.4 Routed Bypass.	
9.4.1 Routed Bypass - Traffic Flow	
9.4.2 View Current Routed Bypass List	62
9.4.2.1 Compact	63
9.4.2.2 Json	63
9.4.3 Configure Routed Bypass List	64
9.4.3.1 Routed Bypass URL	64
9.4.3.2 Manual (Paste Routed Bypass JSON file)	65
9.5 System and Traffic Logs	66
9.5.1 View System Logs	66
9.5.2 Configure Syslog and Traffic Logs	66
9.6 Configuration Wizards	67
-	

9.6.1 Configure Zscaler Nodes, VPN Credentials, DNS servers and SNMP	67
9.6.1.1 Zscaler Nodes and VPN Credentials	67
9.6.1.2 DNS servers	69
9.6.1.3 SNMP	69
9.6.1.3.1 Configure SNMP attributes	69
9.6.1.3.2 SNMP v2c configuration	70
9.6.1.3.3 SNMP Networks	70
9.6.1.3.4 SNMP v3 configuration	71
9.6.1.3.5 What can you do with SNMP?	72
9.6.1.3.5.1 Node Information	72
9.6.1.3.5.2 Node Availability	72
9.6.1.3.5.3 Node Interfaces (IP & SNMP)	73
9.6.1.3.5.4 Node Statistics (CPU, Memory, etc)	73
9.6.1.3.5.5 Interfaces Traffic	74
9.6.2 Switch Tunnels - Primary / Secondary	75
9.6.3 High Availability configuration	76
10 Traffic Forwarding to Zscaler ZIA with the CSC Mux for Azure	83
10.1 CSC Mux in HA Pair	84
10.1.1 Network Diagram	84
10.1.2 Prerequisites	84
10.1.3 Real Case Scenario: Routing, Explicit Proxy and PAC files	84
10.1.3.1 Routing and Explicit proxy: Solving Case 1 and 2	85
10.1.3.2 Case 1, 2 and 3: Routed Bypasses - Layer 4	86
10.1.3.3 PAC files: Solving requirements Case 3	
10.2 CSC Mux in HA with Azure Load Balancer	92
10.2.1 Network Diagram	92
10.2.2 Azure Load Balancer configuration	92
10.2.2.1 Create a Standard Load Balancer	92
10.2.2.2 Front End IP Configuration	92
10.2.2.3 Backend pools	93
10.2.2.4 Health Probes	93
10.2.2.5 Load Balancing rules	94
10.2.2.5.1 Load Balancing Rule for CSC VIP in detail	95
10.2.2.5.2 Load Balancing Rule for Proxy Bypass in detail	95
10.3 Testing traffic to Zscaler	96
10.3.1 ip.zscaler.com	96
10.3.2 https://ip.maidenheadbridge.com	97
10.3.3 SpeedTest	
11 Private Cloud Private Access	99
11.1 What is Private Cloud Private Access (PriCPA)?	
11.2 PriCPA Network Diagrams	99
11.2.1 High Level Network Diagram	99
11.2.2 Low Level Network Diagram – PriCPA only	
11.3 Configuring PriCPA	

11.3.1 Create the Local configuration (First node of the HA pair or Single deploy	/ment)102
11.3.1.1 Using configUserData.json file	102
11.3.1.2 Manual Configuration	
11.3.2 Create the Local configuration (second node of HA Pair)	105
11.3.3 Create the Private Access Peers JSON file	107
11.3.3.1 Full mesh Private Access Peers JSON file	
11.3.3.2 Understanding "privateApps" configuration and values	112
11.3.3.3 Example of "privateApps" for a Windows Domain controller	
11.3.3.4 Example of "privateApps" for Internal Web Server	114
11.3.4 Load the "Private Access Peers JSON file" to the CSCs	115
11.3.4.1 Using "Private Access Peers URL"	115
11.3.4.2 Manual: Copy and Paste "Private Access Peers Json file"	120
11.4 Show Configurations and Status Private Access	121
11.4.1 Using SSH Admin console	
11.4.1.1 Show Peer/s Status	121
11.4.1.2 Show Peers Json file (active)	122
11.4.1.3 Show Local Configuration	124
11.4.1.4 Show Firewall Local Rules	
11.4.2 Using AWS Systems Manager or Rundeck	125
11.4.2.1 AWS Systems Manager	125
11.4.2.2 Rundeck	125
11.5 Configure CSC Remote Management via Private Access	126
12 Remote Management	127
12.1 Azure "Run Command"	127
12.1.1 Using Azure Portal	127
12.1.2 Using Azure CLI	
12.1.3 Commands table	128
12.2 AWS Systems Manager	129
12.2.1 Create Documents	
12.2.2 Run Commands	130
12.2.3 List of Documents available for "Run Command"	
12.3 Rundeck	136
12.3.1 Jobs	
12.3.2 Running job "Show Configuration and Status"	137
13 DevOps operations	
13.1 routedBypassRulesFile.json	139
13.2 privateAccessPeersConfig.json	141
13.3 highAvailability.json file	143
14 Appendixes	145
14.1 Appendix A: Release Notes	145
14.1.1 Version 4.0.4 (June 2023)	
14.1.2 Version 4.0 (June 2023)	145
14.1.3 Version 3.1 (July 2021)	146
14.1.4 Version 3.0 (October 2020)	146

14.2 Appendix B: configUserData.json file	148
14.2.1 Parameters	148
14.2.2 configUserData.json file (blank)	148
14.2.3 configUserData.json file: Example	150
14.2.3.1 zscalerInformation	151
14.2.3.2 awsSsmAgent	151
14.2.3.3 dns	151
14.2.3.4 syslog	152
14.2.3.5 bypasses	152
14.2.3.6 priCPA	152
14.2.3.7 sshRestrictions	153
14.2.3.8 adminManagement	153
14.3 Appendix C: JSON formatters (Visual Code, Notepad ++)	154
14.3.1 Visual Code	154
14.3.2 Notepad ++	155
14.4 Appendix D: Securing an AWS Bucket by source IP	157

1 Introduction to Cloud Security Connectors for Zscaler.

The Cloud Security Connector (CSC) is a device that enables easy deployments of the Zscaler ZIA solution in any customer environment. There are CSC models for Virtual Platforms (VMware, Hyper-V) and Public Clouds (Azure, AWS, etc.).

The Cloud Security Connector Multiplex (CSC Mux) for Azure is a virtual machine connecting internal Azure resources to Zscaler ZIA.

The CSC Mux for Azure lets you connect securely to Zscaler ZIA up to 6.4 Gbps without hassle.

The primary purpose of the CSC family is simplicity. The CSC for Azure comes with all configurations required.

After launching the CSC Mux from the Azure Marketplace using the ARM template provided, the CSC Mux will automatically select the best Zscaler nodes and do IPsec tunnels to Primary and Secondary Zscaler Nodes.

The CSC Mux comes in 4 models:

- 1. CSC Mux 1 with PriCPA: 1 x IPSec to Zscaler (400 Mbps)
- 2. CSC Mux 2 with PriCPA: 2 x IPSec to Zscaler (800 Mbps)
- 3. CSC Mux 4 with PriCPA: 4 x IPsec to Zscaler (1,6 Gbps)
- 4. CSC Mux 8 with PriCPA: 8 x IPsec to Zscaler (3,2 Gbps)

The CSC Mux contains the perfect configuration for IPsec tunnels, firewall rules, and necessary routing tables.

All Zscaler functionalities are available, providing complete visibility of all Internet traffic.

In addition to this, the CSC Mux provides high availability changing the default route to Zscaler when configured as High Availability pair, and an easy way to manage direct bypasses to trusted sites using your public IP.

Includes Private Cloud Private Access (PriCPA) functionality that allows you to create a full mesh among the CSCs communicating your private traffic on a Zero Trust model.

Simple to install with complete management using DevOps change management tools like Amazon Systems Manager, Rundeck, Ansible, etc; and SSH.

2 Key benefits of the Cloud Security Connector Mux for Azure

• No Networking knowledge is required.

- Automated deployment from Marketplace, ARM template or your tool of choice. (i.e. Terraform)
- Enables any Location to be connected to Zscaler up to 6,4 Gbps.
- With Private Cloud Private Access you can connect all sites securely on a Zero Trust model. The CSC secures your Private Traffic between your physical and cloud locations.
- The CSC comes with the optimal values to work with Zscaler ZIA.
- Full tunnel redundancy.
- High Availability with automatic "Next-Hop" selection on multiple routes.
- All traffic steering options supported:
 - Route all traffic to Zscaler (or http/s only).
 - Use of PAC files.
 - Use of Explicit Proxy.
 - No default Route scenarios.
- Multiple options to Bypass Traffic via dedicated Public IP:
 - Layer 7 Proxy Bypass to Trusted Web Sites.
 - Layer 4 Routed Bypass: TCP, UDP and ICMP per source/destination Network and Port (UDP/TCP)
- Cloud Firewall and Cloud Web Security.
- Complete visibility of internal IPs on Zscaler Console.
- No operational burden for Administrators.
- Full hardened device.
- Multiple tools for testing and troubleshooting included: Traffic Logs. TCPDump, Speed Test, MTR (MyTraceRoute), Keepalives statuses, Etc.
- Allow the internal communication between your locations with Private Cloud Private Access.
- Management via SSH, AWS Systems Manager, Rundeck or similar. (Ansible, Salt, Etc.)



3.1 CSC Mux for Azure – Single deployment



Maidenhead Bridge

3.2 CSC Mux for Azure – High Availability Deployment



Maidenhead Bridge



3.3 Traffic Forwarding: Routing and Proxying all together.

The most significant benefit of the Cloud Security Connector for Zscaler is that it covers all possible scenarios (routed traffic, PAC files, explicit proxy, Etc.) for any device on your organization: Laptops, Desktops, Servers, IoT devices, Virtual Desktops, Etc.

The following picture shows the CSC working will all scenarios combined.



The function of each internal IP is the following:

IP	Туре	Function
CSC GW	Gateway	Used as Gateway for traffic to Zscaler and bypasses using "Routed Bypass" (Layer 4) functionality.
CSC Vip Proxy	Proxy	Used as Proxy for traffic to Zscaler.
CSC Proxy Bypass	Proxy	User as Proxy for bypasses using "Proxy Bypass" (Layer 7) functionality.

3.4 High Availability using Azure Load Balancer





3.5 Private Cloud Private Access (PriCPA)

With the CSCs for Zscaler, you can create your Private Cloud for connecting all your internal devices in a Zero Trust model from your physical and cloud locations.



Cloud Security Connector Mux for Azure | 13

4 Understanding the CSC Mux with PriCPA

4.1 What problem the CSC Multiplex solves?

GRE tunnels are the recommended method to forward traffic to Zscaler, but Azure cloud doesn't support GRE (Generic Router Encapsulation) packets. From: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-faq

What protocols can I use within VNets?

You can use TCP, UDP, and ICMP TCP/IP protocols within VNets. Unicast is supported within VNets, with the exception of Dynamic Host Configuration Protocol (DHCP) via Unicast (source port UDP/68 / destination port UDP/67) and UDP source port 65330 which is reserved for the host. Multicast, broadcast, IP-in-IP encapsulated packets, and Generic Routing Encapsulation (GRE) packets are blocked within VNets.

IPSec tunnels to Zscaler can go up to 400 Mbps only. If you need more bandwidth to Zscaler, you need to aggregate multiple tunnels to Zscaler from different Public IPs, as this article says: From: https://help.zscaler.com/zia/configuring-ipsec-vpn-tunnel

Zscaler IPSec tunnels support a limit of 400 Mbps for each public source IP address. If your organization wants to forward more than 400 Mbps of traffic, Zscaler recommends configuring more IPSec VPN tunnels with different public source IP

addresses. For example, if your organization forwards 800 Mbps of traffic, you can configure two primary VPN tunnels and two backup VPN tunnels. If your organization forwards 1200 Mbps of traffic, you can configure three primary VPN tunnels and three backup VPN tunnels.

Suppose you want to create a setup of Gigabits per second to Zscaler with discrete elements. In that case, you will find that it is impossible in most cases or extremely expensive. You will need to implement and configure several components: Firewall, Load balancers, Routers, VPN Concentrators, Etc.

The CSC Multiplex has everything ready to work. You don't need to worry about the complexity of the solution.

The CSC Multiplex provides connectivity to all ports and protocols to Zscaler without restrictions and interacts with the Azure fabric to provide High Availability.

Your only task is to input the IPsec VPN credential.

Problem solved. You can quickly overcome the limitation of IPsec tunnels to Zscaler and reach speeds up to 6.4 Gbps or more.

Maidenhead Bridge

4.2 What does the CSC Multiplex do?

The CSC Multiplex does the job of multiple devices: Firewall, Load Balancer, VPN Concentrator, Router and Proxy, and there are 4 models:

- 1. CSC Mux 1 with PriCPA: 1 x IPSec to Zscaler (400 Mbps)
- 2. CSC Mux 2 with PriCPA: 2 x IPSec to Zscaler (800 Mbps)
- 3. CSC Mux 4 with PriCPA: 4 x IPsec to Zscaler (1,6 Gbps)
- 4. CSC Mux 8 with PriCPA: 8 x IPsec to Zscaler (3,2 Gbps)

IMPORTANT: PriCPA can reach 1 Gbps for private traffic in all models.

VNET CSC Multiplex Internal Subnet Router Security Group VPN / Tunnel Security Concentrator Group Internal X External Public IP #1 Firewall eth1 IPsec #1 Load Balancer eth1 eth0 1) CSC GW IP Public IP #2 -O\$ IPsec #2 2) CSC VIP Proxy Public IP #3 Bypass Proxy IP IPsec #3 Firewall eth0 Public IP #n (4 or 8) IPsec #n (4 or 8) PriCPA Public IP -Bypass Proxy Trusted Site Layer 4 Layer 7 AC PriCPA 1) CSC GW IP When in full routing n ute to sent all traffic to this IP. (i.e. Route 0.0.0.0/0 -> Next Hop Type: Virtual Appliance -> Next Hop Address: <CSC GW IP>) 2) CSC VIP Proxy When using PAC Files, point the Default Traffic to Zscaler to this IP as PROXY <CSC VIP Proxy >:80 (or :9400) 3) Bypass Proxy IP When using PAC Files, point the Bypass Traffic to this IP as PROXY < bypass Proxy IP>:3128 and configure the PAC URL on the CSC to automatically create the Layer 7 ACLs from the PAC file. Private Traffic

The following diagram shows the internal architecture of the CSC Multiplex:

PriCPA uses Wireguard protocol. "WireGuard" and the "WireGuard" logo are registered trademarks of Jason A. Donenfeld.

4.3 The CSC Mux 1, 2, 4 and 8 in action

4.3.1 Speed Test with CSC Mux 1

Selection: 4

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

Aggregated Bandwidth Download: 862.19 Mbps

4.3.2 Speed Test with CSC Mux 2

Selection: 4 SPEED TEST This is experimental. We are using third party tools. (Speedtest.net) Results can be inaccurate or none. The test takes a while

Aggregated Bandwidth Download: 1343.78 Mbps

4.3.3 Speed Test with CSC Mux 4

Speed expected: 1600 Mbps

Selection: 4 SPEED TEST This is experimental. We are using third party tools. (Speedtest.net) Results can be inaccurate or none. The test takes a while

Aggregated Bandwidth Download: 2472.33 Mbps

4.3.4 Speed Test with CSC Mux 8

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

Aggregated Bandwidth Download: 4363.72 Mbps

Maidenhead Bridge

Selection: 4



4.3.5 Iperf test using PriCPA

This Iperf test is between a CSC on Azure and another CSC on AWS. Both are located in the US East region.

PriCPA provides 1 Gbps throughput.

ubuntu-ds-01@ubuntu-d	ds-01:~\$ iperf -c 10.3.200.16 -p 5500 -t 60	
Client connecting to TCP window size: 1.62	10.3.200.16, TCP port 5500 2 MByte (default)	
[3] local 10.2.3.5 [ID] Interval [3] 0.0-60.0 sec	port 56046 connected with 10.3.200.16 port 550 Transfer Bandwidth 6.43 GBytes 921 Mbits/sec	0



5 Creating the CSC Mux for Zscaler with PriCPA

5.1 Prerequisites

Before launching the CSC Mux 1, 2, 4 or 8 for Azure, you need to have these elements ready:

- 1. **(Optional) SSH Key:** If you want to access the CSC using SSH keys. If not, you can use a password during the installation.
- 2. Virtual Network
- 3. **External Subnet:** The External Subnet must be on the same Virtual Network as the Internal Subnet.
- 4. **Internal Subnet:** The Internal Subnet must be on the same Virtual Network as the External Subnet.

5.2 Launching the CSC Mux for Azure Marketplace

Go to Azure Marketplace, search for "Maidenhead Bridge", and select **"CSC Mux for Zscaler with PriCPA - Model (1, 2, 4 and 8)"**.

(https://azuremarketplace.microsoft.com/en-us/marketplace/apps/maidenhead-bridge.zs-cscmux-azure-application?tab=Overview)



 \rightarrow Click "Get it Now"



 \rightarrow Select "Software Plan" and click "Continue". You will be redirected to your Azure Portal.

≡ м	Nicrosoft Azure
Home >	
CSC N	Mux for Zscaler with PriCPA - (Models 1, 2, 4 and 8)
Maidenhead	id Bridge
٢	CSC Mux for Zscaler with PriCPA - (Models 1, 2, 4 and 8) Maidenhead Bridge Azure Application
	Plan
	CSC Mux 8 - No infrastructure required V Create
	search for model
Overvie	ew CSC Mux 4 - No infrastructure required Ratings + Reviews
	CSC Mux 4 - Availability Set select deployment type
Offered	I undi CSC Mux 4 - Availability Zones
The Clou (ZIA) and	ud Security Connector Multiplex (CSC Mux 1, 2, 4 and 8) allows you to protect your Internet traffic in compliance with the best practices for Zscaler Internet Access d and communicate private Cloud Workloads.
The Key	Benefits of the CSC Mux are:
• Si	Solves the limitation of speed to Zscaler (ZIA) when using IPsec tunnels. The CSC Mux comes in four models: CSC Mux 1 (1 x IPsec, 400 Mbps to Zscaler, 1 Gbps PriCPA) CSC Mux 2 (2 x IPsec, 800 Mbps to Zscaler, 1 Gbps PriCPA) CSC Mux 4 (4 x IPsec, 1.6 Gbps to Zscaler, 1 Gbps PriCPA) CSC Mux 4 (4 x IPsec, 1.6 Gbps to Zscaler, 1 Gbps PriCPA) CSC Mux 4 (8 x IPsec, 3.2 Gbps to Zscaler, 1 Gbps PriCPA) CSC Mux 9 (8 x IPsec, 3.2 Gbps to Zscaler, 1 Gbps PriCPA) CSC Mux 9 (8 x IPsec, 3.2 Gbps to Zscaler, 1 Gbps PriCPA)

Includes Private Cloud Private Access (PriCPA) functionality that allows you to create a full mesh among the CSCs communicating your private traffic on a Zero Trust
model at Gigabit speeds.

• The primary purpose of the CSC Mux family is simplicity. The CSC comes with the optimal values to work with Zscaler (ZIA).

 \rightarrow Please, Check the Plan and click "Create".

	riCPA - (Models 1, 2, 4 and 8)		
Create CSC Mux for 2	Zscaler with PriCPA - (Models	s 1, 2, 4 and 8)	
1 Basics ② Virtual Machine	e Settings (3 Networking 👍 configUser	Data.json File 💿 Review + create	
Project details			
Select the subscription to manage dep manage all your resources.	ployed resources and costs. Use resource groups like for	olders to organize and	
Subscription * ①	МНВ	\sim	
Resource group * ①	CSC-East-US	\sim	
	Create new 1		
Instance details			
Location * 🛈	East US	\sim	
Please, check if the Location (Reg https://docs.microsoft.com/en-us	ion) selected previously supports Availability Zones (see: s/azure/availability-zones/az-region).		
Please, check if the Location (Reg https://docs.microsoft.com/en-us Select Single or HA configuration *	ion) selected previously supports Availability Zones (see: vazure/availability-zones/az-region). Deploy Single (1x) CSC Deploy High Availability (2x) CSCs		
Please, check if the Location (Reg https://docs.microsoft.com/en-us Select Single or HA configuration * (Choose the Availability Zones for	ion) selected previously supports Availability Zones (see: (azure/availability-zones/az-region). Deploy Single (1x) CSC Deploy High Availability (2x) CSCs each Cloud Security Connector.		
Please, check if the Location (Reg https://docs.microsoft.com/en-us Select Single or HA configuration * Choose the Availability Zones for	ion) selected previously supports Availability Zones (see: vazure/availability-zones/az-region). Deploy Single (1x) CSC Deploy High Availability (2x) CSCs each Cloud Security Connector.		
Please, check if the Location (Reg https://docs.microsoft.com/en-us Select Single or HA configuration * (Choose the Availability Zones for First CSC Availabity Zone * ()	ion) selected previously supports Availability Zones (see: vazure/availability-zones/az-region). Deploy Single (1x) CSC Deploy High Availability (2x) CSCs Concernent Cloud Security Connector.		
Please, check if the Location (Reg https://docs.microsoft.com/en-us Select Single or HA configuration * (Choose the Availability Zones for First CSC Availabity Zone * () Second CSC Availabity Zone * ()	ion) selected previously supports Availability Zones (see: vazure/availability-zones/az-region). Deploy Single (1x) CSC Deploy High Availability (2x) CSCs each Cloud Security Connector.		
Please, check if the Location (Reg https://docs.microsoft.com/en-us Select Single or HA configuration * (Choose the Availability Zones for First CSC Availabity Zone * (Second CSC Availabity Zone * (CSC_Name * ()	ion) selected previously supports Availability Zones (see: vazure/availability-zones/az-region). Deploy Single (1x) CSC Deploy High Availability (2x) CSCs each Cloud Security Connector. 4 Zone 1 Zone 2 zs-csc-mux-4-az-doc 5		
Please, check if the Location (Reg https://docs.microsoft.com/en-us Select Single or HA configuration * (Choose the Availability Zones for First CSC Availabity Zone * (Second CSC Availabity Zone * (CSC_Name * () Admin Username ()	ion) selected previously supports Availability Zones (see: vazure/availability-zones/az-region). Deploy Single (1x) CSC Deploy High Availability (2x) CSCs each Cloud Security Connector. 4 Zone 1 Zone 2 Zs-csc-mux-4-az-doc 5 cscadmin		
Please, check if the Location (Reg https://docs.microsoft.com/en-us Select Single or HA configuration * (Choose the Availability Zones for First CSC Availabity Zone * (Second CSC Availabity Zone * (CSC_Name * () Admin Username () Authentication type * ()	ion) selected previously supports Availability Zones (see: vazure/availability-zones/az-region). Deploy Single (1x) CSC Deploy High Availability (2x) CSCs each Cloud Security Connector. 4 Zone 1 Zone 2 Zs-csc-mux-4-az-doc 5 cscadmin Password		
Please, check if the Location (Reg https://docs.microsoft.com/en-us Select Single or HA configuration * (Choose the Availability Zones for First CSC Availabity Zone * (Second CSC Availabity Zone * (CSC_Name * (Admin Username () Authentication type * ()	ion) selected previously supports Availability Zones (see: vazure/availability-zones/az-region). Deploy Single (1x) CSC Deploy High Availability (2x) CSCs each Cloud Security Connector. 4 Zone 1 Zone 2 Zs-csc-mux-4-az-doc 5 cscadmin Password SSH Public Key 6		
Please, check if the Location (Reg https://docs.microsoft.com/en-us Select Single or HA configuration * (Choose the Availability Zones for First CSC Availabity Zone * (Second CSC Availabity Zone * (CSC_Name * (Admin Username () Authentication type * () Password * ()	ion) selected previously supports Availability Zones (see: vazure/availability-zones/az-region). Deploy Single (1x) CSC Deploy High Availability (2x) CSCs each Cloud Security Connector. 4 Zone 1 Zone 2 Zs-csc-mux-4-az-doc 5 cscadmin Password SSH Public Key 6		
Please, check if the Location (Reg https://docs.microsoft.com/en-us Select Single or HA configuration * () Choose the Availability Zones for First CSC Availabity Zone * () Second CSC Availabity Zone * () CSC_Name * () Admin Username () Authentication type * () Password * () Confirm password *	ion) selected previously supports Availability Zones (see: v/azure/availability-zones/az-region). Deploy Single (1x) CSC Deploy High Availability (2x) CSCs each Cloud Security Connector. 4 Zone 1 Zone 2 Zs-csc-mux-4-az-doc 5 cscadmin Password SSH Public Key		
Please, check if the Location (Reg https://docs.microsoft.com/en-us Select Single or HA configuration * (a) Choose the Availability Zones for First CSC Availabity Zone * (a) Second CSC Availabity Zone * (a) CSC_Name * (a) Admin Username (b) Authentication type * (c) Password * (c) Confirm password *	ion) selected previously supports Availability Zones (see: vazure/availability-zones/az-region). Deploy Single (1x) CSC Deploy High Availability (2x) CSCs each Cloud Security Connector.		

No.

Fill the values on "Basics"

- 1. Resource Group.
- 2. Location.
- 3. Single deployment or High Availability (2 x CSC).
- 4. Select Availability Zone for the first and second CSC. (Note: if the deployment is using Availability Sets, the menu will offer the corresponding options).
- 5. Put a name to the CSC VM. (Note: the ARM template will append a digit to the name. For example, if you deploy 2 x CSCs, the names will be <name>-1 and <name-2>)
- 6. For the username "cscadmin", choose to use Password or SSH key.

 \rightarrow Click "Next".

Microsoft Azure			
Home > CSC Mux for Zscaler with PriCPA	A - (Models 1, 2, 4 and 8)	>	
Create CSC Mux for Zscaler with PriCPA - (Models 1, 2, 4 and 8)			
create csc max for zscaler with ther A (models 1, 2, 4 and 6)			
🤣 Basics 🛛 🝳 Virtual Machine Set	tings ③ Networking	(4) configUserData.json File	③ Review + create
Virtual machine size * ①	1x Standard F4s v2		
	4 vcpus, 8 GB memory		
	Change size		
CSC VM Disk storage account type *	Dramium LPS		
Coe vin blac storage account type	Fremum_cros		¥

 \rightarrow Select the Virtual Machine size and Storage. We recommend using the Virtual Machine Size suggested.

Note: Microsoft created the VM Size "Standard Fx" family for Virtual Appliances. We recommend using the "Standard Fx" series for the CSC Mux 2 (Standard F2), 4 (Standard F4) and 8 (Standard F8). In the case of the CSC Mux 1, you can use Standard B1s or similar.

 \rightarrow Click "Next"

ome > CSC Mux for Zscaler wit	h PriCPA - (Models 1, 2, 4 and 8)
reate CSC Mux fo	r Zscaler with PriCPA - (Models 1, 2, 4 and 8)
🕗 Basics 🛛 🕢 Virtual Mach	ine Settings 🚯 Networking 🕘 configUserData ison File 🚯 Review + create
Configure virtual networks	
Configure virtual networks	
Configure virtual networks	VNET-East-US
Configure virtual networks	VNET-East-US
Configure virtual networks	VNET-East-US V Create new
Configure virtual networks	VNET-East-US Create new Create new
Configure virtual networks VNET_Name * CONTROL Subnet_Name * CONTR	VNET-East-US Create new csc-external-East-US (10.2.1.0/24)
Configure virtual networks VNET_Name * C EXTERNAL_Subnet_Name *	VNET-East-US Create new Csc-external-East-US (10.2.1.0/24)
Configure virtual networks VNET_Name * ① EXTERNAL_Subnet_Name * ①	VNET-East-US V Create new Creaternal-East-US (10.2.1.0/24) Manage subnet configuration
Configure virtual networks VNET_Name * C EXTERNAL_Subnet_Name * INTERNAL_Subnet_Name * C	VNET-East-US V Create new V Create new V Manage subnet configuration V csc-internal-East-US (10.2.2.0/24) V

-> Select the VNET, External and Internal Subnet for the CSC and click "Next".

(Optional) -> Paste configUserData.json file.

≡ Microsoft Azure			
Home > CSC Mux for Zscaler with PriCP.	A - (Models 1, 2, 4 and 8) >		
Create CSC Mux for Zscaler with PriCPA - (Models 1, 2, 4 and 8)			
🕑 Basics 🛛 🤡 Virtual Machine Set	tings 📀 Networking 🧕 configUserDatajson File 💿 Review + create		
(Optional) Paste here configUserData.j	son file:		
configUserData.json file 🕕	{ "model": "csc-mux-zs-azure", "type": "configUserData", "versi 🗸		
I	Paste here configUserData.json file		

IMPORTANT: See Appendix B for format and examples of the configUserdata.json file.

Via configUserData.json file, you can pass values to parameters during the installation of the CSC. You can setup:

- Zscaler Information: CloudName (zscloud, zscalerthree, zscalertwo; etc.), Nodes (autodiscovery or manual selection), vpnCredentials "domain". (Using "domain" the CSC automatically creates the FQDN (<vmName@domain> and Pre shared keys for IPsec.)
- 2. AWS SSM agent registration values.
- 3. DNS servers
- 4. Syslog servers and traffic log configuration.
- 5. Bypasses: Proxy Bypass PAC URL and Routed Bypass URL
- 6. PriCPA Local configuration values, Peers URL and Remote Management Networks.

Maidenhead Bridge

- 7. SSH Restrictions via eth1 and wg0.
- 8. Admin Management: Enable csccli user and SSH Key.

configUserData.json (blank)

The fields in **bold** are not configurable. So please, do not modify.

configUserData.json
{ "model": "csc-mux-zs-azure", "two": "config: logrData"
type : conligueridata ,
Version : 1.0 , "accalarinformation": /
"cloudName": ""
"vonNodes": {
"autoDiscovery": "ves"
"nrimary"· {
"hostName". ""
}.
"secondary": {
"hostName": ""
}
},
"vpnCredentials": {
"domain": ""
}
},
"awsSsmAgent": {
"enable": "no",
"activationCode": "",
"activationId": "",
"awsRegion": ""
},
"ans": {
useciouadons : yes ,
prinaryonsip . , "cocondaryOpela": ""
j, "svslog": {
"enable": "no".
"primaryServer": {
"ip": "",
"port": ""
},
"secondaryServer": {
"ip": "",
"port": ""
},
"trafficLogs": {
"enable": "no"
}, "humanana" (
bypasses : {
proxyBypass : {
},

```
"routedBypass": {
      "jsonUrl": ""
   }
  },
  "priCPA": {
    "enable": "no",
    "nodeName": "",
    "location": "",
    "description": "",
    "publicUdpPort": "51280",
    "privateCirdIp": "",
    "persistentKeepAlive": "no",
    "peersJsonFileUrl": "",
    "remoteManagementNetworks": []
 },
"sshRestrictions": {
    "eth1": {
      "enable": "no",
      "allowedNetworks": []
    },
    "wg0": {
      "enable": "no",
      "allowedNetworks": []
    }
  },
  "adminManagement": {
    "csccli": {
      "enable": "no",
      "sshPublicKey": ""
   }
 }
}
```

 \rightarrow Click Next.

Microsoft Azure	
ome > CSC Mux for Zscaler with P	riCPA - (Models 1, 2, 4 and 8) >
reate CSC Mux for 7	Accelor with DriCPA (Models 1.2.4 and 8)
reate CSC IVIUX IOI 2	scaler with FICFA - (Models 1, 2, 4 and 6)
Validation Passed Che	eck
Basics 🕜 Virtual Machine	Settings 🖉 Networking 🧖 configliserData icon File 5 Peview + create
Price	
CSC Mux for Zscaler with PriCPA -	
Models 1, 2, 4 and 8)	
y Maidenhead Bridge	
erms of use Privacy policy	
TEDMS	
IERIVIS	
By clicking "Create", I (a) agree to the listed above: (b) authorize Microsoft to	egal terms and privacy statement(s) associated with the Marketplace offering(s) 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
nd transactional information with the	provider(s) of the offering(s) for support, billing and other transactional
ctivities. Microsoft does not provide i letails.	ights for third-party offerings. See the Azure Marketplace Terms for additional
lame	
Preferred e-mail address	
referred phone number	
and an	
Sasics	
Subscription	МНВ
Resource group	CSC-East-US
ocation	East US
elect Single or HA configuration	Deploy High Availability (2x) CSCs
irst CSC Availabity Zone	Zone 1
econd CSC Availabity Zone	Zone 2
SC_Name	zs-csc-mux-4-az-doc
assword	CSC0011111
/irtual Machine Settings	
listual machine size	Standard Ede v2
SC VM Disk storage account type	Dremium LBS
LOC YM DISK Storage account type	Freihun_LC3
Networking	
(itselection)	VALET From LIC
/irtual network	VNET-East-US

 \rightarrow Check "Validation Passed" and click "Create". Wait up to "Your deployment is complete".



-> Click "Go to resource group" and you will see the components created.

Home > maidenhead-bridge.zs-csc-mub	-azure-application-pr-20230611162522 Overview > 	
CSC-East-US 🖉 🖈		
Resource group		
🔎 Search 🛛 «	🕂 Create 🚳 Manage view 🗸 📋 Delete resource group 🖒 Refresh 🞍 Export to CSV 😽	Open query 🕴 🙆 Ass
() Overview	↑ Essentials	
Activity log	Subscription (move) : MHB	
Access control (IAM)	Subscription ID : ffde02fb-c38f-45fb-9e31-89e5303be5f1	
Tags	Tags (edit) : Click here to add tags	
🛧 Resource visualizer	Deserves Deserves defines (2)	
Events	Resources Recommendations (2)	
Settings	zs-csc-mux-4-az-dod Type equals all \times Location equals all \times $^{+}\gamma$ Add filter	
Deployments	Showing 1 to 22 of 22 records. Show hidden types ①	
Security	Name 1	
Policies	VM	
Properties 1		
🔒 Locks		
Monitoring		
Insights (preview)	zs-cc-mix-4-az-doc-et/0-0-2ubliclp.1	
Alerts	z-cc-mux-4-az-doc-eth0-0-Publiclo-2	
Metrics	S-csc-mux-4-az-doc-eth0-1	
Diagnostic settings	zs-csc-mux-4-az-doc-eth0-1-PublicIo-1	
P Logs	zs-csc-mux-4-az-doc-eth0-1-PublicIo-2	
Advisor recommendations	s-csc-mux-4-az-doc-eth0-2	
Workbooks	zs-csc-mux-4-az-doc-eth0-2-PublicIo-1	
Automation	zs-csc-mux-4-az-doc-eth0-2-Publiclp-2	
Export template	zs-csc-mux-4-az-doc-eth0-3-Publiclp-1	
Support + troubleshooting	zs-csc-mux-4-az-doc-eth0-3-Publiclp-2	
New Support Request	zs-csc-mux-4-az-doc-eth0-4-PublicIp-1	
A new support nequest	zs-csc-mux-4-az-doc-eth0-4-Publiclp-2	
	s-csc-mux-4-az-doc-eth0-NSG-1	
	zs-csc-mux-4-az-doc-eth0-NSG-2	
	s-csc-mux-4-az-doc-eth1-1	
	s-csc-mux-4-az-doc-eth1-2	
	s-csc-mux-4-az-doc-eth1-NSG-1	
	C C C C C C C C C C C C C C C C C C C	

< Previous Page 1 V of 1 Next >

 \rightarrow Done! Your CSCs Mux for Azure are deployed.

6 Accessing for first time to your CSC

6.1 SSH to the Admin Console using CSC GW IP

1. Go to your Azure Dashboard \rightarrow Select the VM created \rightarrow Networking \rightarrow eth1 and check "NIC Private IP". (CSC-GW-IP (Primary))

ZS-CSC-MUX-4-as-d-1	Networking 🛪 ···
✓ Search «	$ otag Freedback \mathscr{S}$ Attach network interface $\mathscr{S}^{\!\mathcal{Q}}$ Detach network interface
 Overview Activity log 	zs-csc-mux-4-as-d-eth0-1 zs-csc-mux-4-as-d-eth1-1 2
Access control (IAM)	IP configuration () CSC-GW-IP (Primary) V
Diagnose and solve problems	Steele St
Settings 1	Virtual network/subnet: VNET-East-US/csc-internal-East-US NIC Public IP: - NIC Private IP: 10.2.2.15 4
Networking	Inbound port rules Outbound port rules Application security groups Load balancing

- 2. In this example, "NIC Private IP" is: 10.2.2.15
- 3. From a machine inside the Virtual Network or via remotely via PriCPA, ssh the CSC using username "cscadmin" and key or password:

ssh -i <keyname.pem> cscadmin@<eth1 Private IP>

ssh cscadmin@<eth1 Private IP>

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

6.1.1 Initial Screen when using configUserData.json file

When passing Zscaler information via configUserData.json file, the CSC will automatically configure the Cloud, Nodes and VPN Credentials.

configUserData.json example:



Initial screen:

Maidenhead Bridge	
CSC MUX 4 (1.6 Gbps) for Zscaler with PriCPA - Admin Console	
Reminder: Configuration required on your Zscaler Console: VPN credentials and Location	
> VPN Credentials creation: Go to > Administration > VPN Credentials > Add VPN Credential -> Select Authentication	n Type = FDQN and configure:
User ID: zs-csc-mux-4-as-d-1@maidenheadbridge.com Pre-Shared Key: ztyckrj6viyAWWzkdWpl3gg0SM7QJjAm	
> Location creation: Go to > Administration > Location > Add Location. Put your Location values and select 'VPN C	redentials' created in the step before
Did you created the VPN Credentials and Location on the Zscaler console? Please, confirm.	
1) Yes 2) No Enter your choice: 🗌	

You need to add the VPN credentials on your Zscaler console and to associate it with a Location.

6.1.2 Initial screen wihout using configUserData.json file

In this case, the initial screen presents the Wizard to configure manually the Zscaler Information.



6.1.2.1 Running the initial wizard

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'
- 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!

Example:

1. Select Cloud and Nodes:

Do you want to change these values?
1) Yes 2) No Enter your choice: 1
Please, select your Cloud
1) zscalerthree
2) zscloud
3) ZSCALEFTWO
5) zscalerone
6) zscalerbeta
7) zscalergov
8) Not in the list? Input Manually
9) Quit
Enter your choice: 1
Please, select Manual or Auto Node Selection
1) Manual
2) Auto
3) Quit
Enter your choice: 2
You have chosen the following:
Cloudname: zscalerthree
Primary node: AutoPrimary (vpn.zscalerthree.net) Secondary Node: AutoSecondary (secondary.vpn.zscalerthree.net)

- 2. Input VPN Credentials:
- 3. Confirm Vavlues



4. The CSC will validate the configuration and will ask to confirm.

Validating Configuration
Your Cloud is: zscalerthree
Checking Node AutoPrimary hostname vpn.zscalerthree.net Hostname vpn.zscalerthree.net has IP 165.225.8.35 Node AutoPrimary is Alive
Checking Node AutoSecondary hostname secondary.vpn.zscalerthree.net Hostname secondary.vpn.zscalerthree.net has IP 165.225.38.52 Node AutoSecondary is Alive
Do you want to apply this values? (y/n)?:y
(MHB-CSC)(INFO) CSC:zs-csc-mux-4-as-d-2 connected to Zscaler Cloud: zscalerthree (MHB-CSC)(INFO) Primary Zscaler Node using: AutoPrimary, hostname: vpn.zscalerthree.net (IP: 165.225.8.35) on CSC:zs-csc-mux-4-as-d-2 (MHB-CSC)(INFO) Secondary Zscaler Node using: AutoSecondary, hostname: secondary.vpn.zscalerthree.net (IP: 165.225.38.52) on CSC:zs-csc-mux-4-as-d-2 (MHB-CSC)(INFO) VPN Credentials using FQDN: zs-csc-mux-4-as-d-2@maidenheadbridge.com on CSC:zs-csc-mux-4-as-d-2
Rebooting after initial configuration
Connection to 10.2.2.18 closed by remote host. Connection to 10.2.2.18 closed.

5. Done! The CSC is ready.

7 Zscaler console: create VPN Credentials and Location

7.1 VPN Credential creation.

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

Add VPN Credential	×
VPN CREDENTIAL	
Authentication Type 1 FODN XAUTH IP	
User ID csc-azure-02	2 🗸
New Pre-Shared Key Confirm New Pre-Shared Key	3
Comments	
Credentials for CSC on Azure	
4 Save Cancel	

Click "Save" and "Activation"

7.2 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		ountry nited Kingdom
State/Province	Th	me Zone urope/London
Group None ~		
ADDRESSING		
Static IP Addresses None V		
VPN Credentials 2 csc-azure-02@maidenheadbridge.com ~		
GATEWAY OPTIONS		
Enable XFF Forwarding	Er	nforce Authentication
Enable IP Surrogate	Id	le Time to Disassociation Hours
Enforce Surrogate IP for Known Browsers		
Enable SSL Scanning	Er	nforce Firewall Control
Save Cancel		

Fill other values on the Location, click "Save" and "Activate"

7.3 Checking tunnel statuses on the CSC console.

 \rightarrow SSH the CSC and Run: "Show Configuration and Status". Check the Load Balancer and Tunnel information.

LOAD BALANCING INFORMATION Last change: Tue 30 May 11:04:23 UTC 2023 (UP) Ztun1 is active, using primary. (UP) Ztun2 is active, using primary. (UP) Ztun3 is active, using primary. (UP) Ztun4 is active, using primary.
TPSEC INFORMATION
Ztuni connected to: AutoPrimary, IPsec uptime uptime: 6 minutes, since May 30 11:03:13 2023, Last Security Association: ESTABLISHED 6 minutes ago
Ztun2 connected to: AutoPrimary, IPsec uptime uptime: 6 minutes, since May 30 11:03:13 2023, Last Security Association: ESTABLISHED 6 minutes ago
Ztun3 connected to: AutoPrimary, IPsec uptime uptime: 6 minutes, since May 30 11:03:14 2023, Last Security Association: ESTABLISHED 6 minutes ago
Ztun4 connected to: AutoPrimarý, IPsec uptime uptime: 6 minutes, since May 30 11:03:14 2023, Last Security Association: ESTABLISHED 6 minutes ago
CREDENTIALS INFORMATION Username: zs-csc-mux-4-as-d-2@maidenheadbridge.com PSK: Not shown. Please, read it from 'Configuration Wizards' Menu
http://ip.zscaler.com INFORMATION
Ztunl Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 136.226.68.253, via Public IP: 74.235.175.176
Ztun2 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 136.226.51.16, via Public IP: 20.163.185.99
Ztun3 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 165.225.9.19, via Public IP: 74.235.173.170
Ztun4 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 136.226.51.20, via Public IP: 20.163.185.151

8 Resources creates by the ARM template

The following resources are created by the ARM template:

1. Virtual Machine

zs-csc-mux-4-as-d-1	☆☆…			
₽ Search «	💋 Connect 🕞 Start	<	ile 🖗 Feedback 😹	CLI / PS
Overview	A Frankish			
Activity log	Sessentials			
Access control (IAM)	Resource group (move)	: CSC-EAST-US	Operating system	: Linux (ubuntu 22.04)
	Status	: Running	Size	: Standard F4s v2 (4 vcpus, 8 GiB memory)
lags	Location	: East US	Public IP address	: 74.235.173.100
Diagnose and solve problems	Subscription (move)	: MHB	Virtual network/subnet	: VNET-East-US/csc-external-East-US
Settings	Subscription ID	: ffde02fb-c38f-45fb-9e31-89e5303be5f1	DNS name	: Not configured
Retworking			Health state	(
Ø Connect	Tags (<u>edit</u>)	: Click here to add tags		

2. Interfaces External and Internal.

👧 zs-csc-mux-4-as-d-1 | Networking 🔅 😁

Virtual machine				
₽ Search	« Reedback Ø Attach network interfa	ce ග් Detach network interface		
📮 Overview	A			
Activity log	zs-csc-mux-4-as-d-eth0-1 zs-csc-m	ux-4-as-d-eth1-1		
Access control (IAM)	IP configuration ①			
🔷 Tags	Ztun1 (Primary)	~		
Diagnose and solve problems	Filter the ip configurations	-eth0-1 Effective security rules	Troubleshoot VM connection issues	Topology
Settings	Ztun1 (Primary)	ernal-East-US NIC Public IP: 74.235.	173.100 NIC Private IP: 10.2.1.24	Accelerated networking: Enabled
Networking	Ztun2	es Application security groups	Load balancing	
💋 Connect	Ztun3	as-d-eth0-NSG-1 (attached to network	interface: zs.csc.muv.4.as.d.ath0.1)	
a Disks	Ztun4	and card rate relations	interface. 25 ese max 4 as a caro i j	
Ciza	Bypass-and-PriCPA	Port	Protocol	Source De

Depending the model, the ARM template creates 1, 2, 4 or 8 x Public IP (Ztunx) for the IPsec tunnels, and 1 x Public IP used by Bypass functionality and Private Access.

- 3. Security Group for External Interface.¹²
 - 3.1. Inbound Rules

Inbound port rules	Outbound port rules Application securit	y groups Load balar	icing				
Network security group zs-csc-mux-4-as-d-eth0-NSG-1 (attached to network interface: zs-csc-mux-4-as-d-eth0-1) Impacts 0 subnets, 1 network interfaces						Add inbound port rule	
Priority	Name	Port	Protocol	Source	Destination	Action	
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow 	
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	 Allow 	
65500	DenyAllInBound	Any	Any	Any	Any	O Deny	

¹ The CSC contains Firewall Rules on each interface that are more specific in some cases. For example, the CSC only allows reaching the configured Zscaler Nodes for IPsec traffic. Therefore, there is double protection: The Azure Security Group and the internal Firewall Rules of the CSC.

² When using Private Access (PriCPA), the CSC automatically updates the internal FW rules and Security Groups to allow Peers to communicate with each other.

3.2. Outbound Rules

Inbound port rules	Outbound port rules Application	security groups Load b	palancing					
Network security group zs-csc-mux-4-as-d-eth0-NSG-1 (attached to network interface: zs-csc-mux-4-as-d-eth0-1) Impacts 0 subnets, 1 network interfaces						Add outboun	Add outbound port rule	
Priority	Name	Port	Protocol	Source	Destination	Action		
4000	AllowPing	Any	ICMP	Any	Any	 Allow 		
4010	AllowUDP500	500	UDP	Any	Any	 Allow 		
4020	AllowUDP4500	4500	UDP	Any	Any	 Allow 		
4030	AllowHTTP	80	TCP	Any	Any	 Allow 		
4040	AllowHTTPS	443	TCP	Any	Any	 Allow 		
4050	AllowPublicDNS	53	UDP	Any	Any	 Allow 		
4060	AllowNTP	123	UDP	Any	Any	 Allow 		
4070	DenyAllOutbound	Any	Any	Any	Any	Oeny		
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow 		
65001	AllowInternetOutBound	Any	Any	Any	Internet	 Allow 		
65500	DenvAllOutBound	Any	Any	Any	Any	O Denv		

4. Security Group for Internal Interface.

4.1. Inbound Rules

Inbound port rules	Outbound port rules Application security	groups Load balan	cing				
Network security group zs-cs:-max-4-as-d-eth1-NSG-1 (attached to network interface: zs-csc-max-4-as-d-eth1-1) Impacts 0 subnets, 1 network interfaces						Add inbound	l port rule
Priority	Name	Port	Protocol	Source	Destination	Action	
4000	AllowNet-10.0.0.0-8	Any	Any	10.0.0/8	Any	 Allow 	
4010	AllowNet-172.16.0.0-12	Any	Any	172.16.0.0/12	Any	 Allow 	
4020	AllowNet-192.168.0.0-16	Any	Any	192.168.0.0/16	Any	 Allow 	
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow 	
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	 Allow 	
65500	DenyAllInBound	Any	Any	Any	Any	Oeny	

4.2. Outbound Rules

Inbound port rules	Outbound port rules Application	security groups Load ba	lancing				
Network security Impacts 0 subnets,	group zs-csc-mux-4-as-d-eth1-NSG-1 (1 network interfaces	attached to network interfac	e: zs-csc-mux-4-as-d-eth1-	1)		Add outbound	l port rule
Priority	Name	Port	Protocol	Source	Destination	Action	
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow 	
65001	AllowInternetOutBound	Any	Any	Any	Internet	 Allow 	
65500	DenyAllOutBound	Any	Any	Any	Any	O Deny	

Maidenhead Bridge

9 The Cloud Security Connector Admin Console:

The CSC's SSH Console simplifies administrative tasks showing what is essential to administrators for operation and troubleshooting.

When accessing the console via SSH (using the CSC GW IP), you will receive the Admin Console.

```
Maidenhead Bridge
CSC MUX 4 (1.6 Gbps) for Zscaler with PriCPA - Admin Console
VM Name : zs-csc-mux-4-as-d-1
Azure Region : eastus
Soft Version : 4.0
Please select an option by typing its number
Monitoring Tasks

    Show Configuration and Status

2) Show Interfaces Traffic
Tcpdump, Traceroute and Latency Test

    Speed Test (Experimental)

CSC Admin tasks
5) AWS SSM Agent (Register or De-Register)
6) Manage Administrators, Restrict SSH access and Radius Configuration.
7) Change Timezone
Proxy Bypass
View Current Proxy Bypass List
9) Configure Proxy Bypass List
Routed Bypass
10) View Current Routed Bypass List
11) Configure Routed Bypass List
System and Traffic Logs
12) View System Logs
13) Configure Syslog and Traffic Logs
Configuration Wizards
14) Configure Zscaler Nodes, VPN Credentials, DNS servers and SNMP.
15) Switch Zscaler Tunnels - Primary / Secondary.
16) High Availability configuration.
Private Cloud Private Access (PriCPA)
17) Show Configuration and Status PriCPA.
18) Configure PriCPA (Local and Peers Configuration).
19) Configure CSC Remote Management via PriCPA.
e) Exit
Selection:
```
The Main Sections are:

- **Monitoring Tasks:** To check configuration, statuses, real-time traffic, tcpdump, traceroute and speed..
- **CSC Admin Tasks:** To register the CSC for AWS management, manage administrators, restrict SSH, configure radius and change timezone.
- **Proxy Bypass:** View and configure Proxy Bypass (Layer 7) functionality.
- Routed Bypass: View and configure Routed Bypass (Layer 4) functionality
- System and Traffic Logs: Shows Systems logs, configure Syslog Servers and enable/disable traffic logs.
- **Configuration Wizards:** Configure Zscaler Nodes, VPN Credentials, DNS servers, SNMP, switch tunnels and configure High Availability.
- **Private Cloud Private Access (PriCPA):** Show configuration and statuses, create local coniguration, priCPA peers and add remote management networks,

9.1 Monitoring Tasks

9.1.1 Show Configuration and Status

Selection: 1
GENERAL INFORMATION Name: zs-csc-mux-4-as-d-1 Region: eastus SubscriptionId: ffde02fb-c38f-45fb-9e31-89e5303be5f1 vmSize: Standard_F4s_v2 CSC date: Sat 3 Jun 19:38:06 UTC 2023 Soft version: 4.6 CSC Model: CSC MUX 4 (1.6 Gbps) for Zscaler with PriCPA Azure Cloud: AzureCloud
INTERFACES INFORMATION External: Tunnel IPs (eth0): 10.2.1.24-[25,26,27]/24 Bypass Proxy Egress IP 10.2.1.28 Network Gateway: 10.2.1.1 Internal: CSC GW IP (eth1): 10.2.2.15/24 Network Gateway: 10.2.2.1
TRAFFIC REDIRECTION Options To Zscaler: VIP Proxy: 10.2.2.16:80 (or :9400) Route all traffic via CSC GW IP Zscaler Global Proxies (port 80/9400) via CSC GW IP Direct to Internet: Bypass Proxy: 10.2.2.17:3128 Zscaler Global Proxies (port 3128) via CSC GW IP
PUBLIC IP Address INFORMATION IPsec tunnels Public IP: 74,235.173.100, 74,235.171.133, 74.235.171.132, 20.163.185.222 Bypass Public IP: 74.235.173.171
DNS INFORMATION DNS Server (1): 1.1.1.1 is Alive DNS Server (2): 8.8.8.8 is Alive
ZSCALER INFORMATION Zscaler Cloud: zscalerthree Primary ZEN node: NewYorkIII Hostname: nyc3-vpn.zscalerthree.net IP: 165.225.38.52 is Alive Secondary ZEN node: WashingtonDC_2 Hostname: was1-2-vpn.zscalerthree.net IP: 165.225.8.35 is Alive
LOAD BALANCING INFORMATION Last change: Sat 3 Jun 19:24:54 UTC 2023 (UP) Ztun1 is active, using primary. (UP) Ztun2 is active, using primary. (UP) Ztun3 is active, using primary. (UP) Ztun4 is active, using primary.
IPSEC INFORMATION Ztunl connected to: NewYorkIII, IPsec uptime uptime: 14 minutes, since Jun 03 19:23:43 2023, Last Security Association: ESTABLISHED 14 minutes ago Ztun2 connected to: NewYorkIII, IPsec uptime uptime: 14 minutes, since Jun 03 19:23:43 2023, Last Security Association: ESTABLISHED 14 minutes ago Ztun3 connected to: NewYorkIII, IPsec uptime uptime: 14 minutes, since Jun 03 19:23:43 2023, Last Security Association: ESTABLISHED 14 minutes ago Ztun4 connected to: NewYorkIII, IPsec uptime uptime: 14 minutes, since Jun 03 19:23:43 2023, Last Security Association: ESTABLISHED 14 minutes ago Ztun4 connected to: NewYorkIII, IPsec uptime uptime: 14 minutes, since Jun 03 19:23:43 2023, Last Security Association: ESTABLISHED 14 minutes ago
CREDENTIALS INFORMATION Username: zs-csc-mux-4-as-d-l@maidenheadbridge.com PSK: Not shown. Please, read it from 'Configuration Wizards' Menu
http://ip.zscaler.com INFORMATION Ztunl Node: New York III in the zscalerthree.net cloud. ZEN Instance IP: 165.225.39.99, via Public IP: 74.235.171.100 Ztun2 Node: New York III in the zscalerthree.net cloud. ZEN Instance IP: 165.225.39.126, via Public IP: 74.235.171.133 Ztun3 Node: New York III in the zscalerthree.net cloud. ZEN Instance IP: 165.225.221.4, via Public IP: 74.235.171.132 Ztun4 Node: New York III in the zscalerthree.net cloud. ZEN Instance IP: 165.225.39.121, via Public IP: 74.235.171.132
PROXY BYPASS Proxy Bypass URL is: https://pac.zscalerthree.net/RdwNltSPqBFN/az-csc-bypass.pac Proxy Bypass Rules configured via URL: 8 Proxy Bypass Egress Interface 10.2.1.28 can reach test page (https://ip.maidenheadbridge.com) via Public IP 74.235.173.171
ROUTED BYPASS Routed Bypass URL is: https://mhb-csc-pac.s3.amazonaws.com/routedBypassRulesFile.json Routed Bypass Rules configured via URL: 12 Routed Bypass URL https://mhb-csc-pac.s3.amazonaws.com/routedBypassRulesFile.json is reachable
AWS SSM AGENT AWS SSM Agent is active (running) since Sat 2023-06-03 00:22:49 UTC; 19h ago Registration values: {"ManagedInstanceID":"mi-055ab68d5af2fd09e","Region":"us-east-1"}
SYSLOG INFORMATION Primary Syslog / SIEM (IP/TCP PORT): 172.19.0.5/5514 is Alive Secondary Syslog / SIEM IP: Not configured Traffic Logs (IP packets) are enabled.
HIGH AVAILABILITY Information The HA service is: active (running) since Sat 2023-06-03 00:22:49 UTC; 19h ago Identity Type: SystemAssigned Route to Zscaler using Next Hop: 10.2.2.18 of VM: zs-csc-mux-4-as-d-2 (the other CSC in the pair) Current values configured are: Route (Oty) = 2 Route 1: Server-default-route (Route Table=Servers-Route-Table, Resource Group=RouteTables-East-US) Route 2: Zscaler-Global-GW (Route Table=Servers-Route-Table, Resource Group=RouteTables-East-US) Computer Name of other CSC in the pair: zs-csc-mux-4-as-d-2 (Resource Group=RouteTables-East-US)
Private Access Public IP= 74.235.173.101

9.1.1.1 GENERAL INFORMATION

This section contains general information about the instance:

```
GENERAL INFORMATION
Name: zs-csc-mux-4-as-d-1
Region: eastus | SubscriptionId: ffde02fb-c38f-45fb-9e31-89e5303be5f1 | vmSize: Standard_F4s_v2
CSC date: Tue 30 May 16:26:50 UTC 2023
Soft version: 4.0 | CSC Model: CSC MUX 4 (1.6 Gbps) for Zscaler with PriCPA
Azure Cloud: AzureCloud
```

9.1.1.2 INTERFACES INFORMATION

This section contains the interfaces information:

```
INTERFACES INFORMATION
External: Tunnel IPs (eth0): 10.2.1.24-[25,26,27]/24 | Bypass Proxy Egress IP 10.2.1.28 | Network Gateway: 10.2.1.1
Internal: CSC GW IP (eth1): 10.2.2.15/24 | Network Gateway: 10.2.2.1
```

9.1.1.3 TRAFFIC REDIRECTION Options.

The section contains information about how to steer traffic to Zscaler.

TRAFFIC REDIRECTION Options To Zscaler: VIP Proxy: 10.2.2.16:80 (or :9400) | Route all traffic via CSC GW IP | Zscaler Global Proxies (port 80/9400) via CSC GW IP Direct to Internet: Bypass Proxy: 10.2.2.17:3128 | 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 when connecting 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. Traffic routed via CSC GW IP can be bypassed from Zscalerusing "Routed Bypasses" (Layer 4).
- **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 IP:** The Bypass Proxy enables a simple way to do Layer 7 Bypasses to the Internet. To be used when PAC files are implemented.

(*) On Azure Routes, the value to use as a "Next-Hop" is the CSC GW IP.

Note:

The CSC Mux for Azure accepts the option using the Zscaler Global Proxies to send traffic to Zscaler Cloud and via the Proxy Bypass.

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 \rightarrow *return "PROXY* 185.46.212.88:**80**"; (you can use port 9400 as well) *Traffic via Bypass Proxy* \rightarrow *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

Important: Please, see Chapter 10 for detailed information about traffic redirection (with examples)

9.1.1.4 PUBLIC IP Address INFORMATION

This section shows the Public IP used to initiate the tunnels to Zscaler and the Public IP used for the Bypass Proxy functionality.

```
PUBLIC IP Address INFORMATION
IPsec tunnels Public IP: 74.235.173.100, 74.235.171.133, 74.235.171.132, 20.163.185.222
Bypass Public IP: 74.235.173.101
```

9.1.1.5 DNS INFORMATION

This section displays the DNS information. You can use the default DNS server from Azure and Google or set up your DNS servers.

```
DNS INFORMATION
Using Azure DNS (168.63.129.16) and Google DNS (8.8.8.8, 8.8.4.4)
```

9.1.1.6 ZSCALER INFORMATION

This section shows the IPsec tunnels information and if the Zscaler's nodes are reachable.



9.1.1.7 LOAD BALANCING INFORMATION

The CSC Mux has the capacity to aggregate multiple IPsec tunnels and has a Load Balancer that distributes the load evenly among each tunnel. This section shows the status of the Load Balancer of a CSC Mux 4.

LOAD	BALANCI	NG I	NFOF	RMAT	LON			
Last	change:	Thu	25	May	02:08	:59	UTC	2023
(UP)	Ztun1	is	acti	ive,	using	pri	imary	/.
(UP)	Ztun2	is	acti	ive,	using	pr	imary	/.
(UP)	Ztun3	is	acti	ive,	using	pr	imary	/.
(UP)	Ztun4	is	acti	ive,	using	pr	imary	/.

9.1.1.8 IPSEC INFORMATION

This section shows the status of each IPsec tunnel.

IPSEC INFORMATION Ztun1 connected to: AutoPrimary, IPsec uptime uptime: 5 days, since May 25 02:08:01 2023, Last Security Association: ESTABLISHED 105 minutes ago Ztun2 connected to: AutoPrimary, IPsec uptime uptime: 5 days, since May 25 02:08:01 2023, Last Security Association: ESTABLISHED 107 minutes ago Ztun3 connected to: AutoPrimary, IPsec uptime uptime: 5 days, since May 25 02:08:01 2023, Last Security Association: ESTABLISHED 107 minutes ago Ztun4 connected to: AutoPrimary, IPsec uptime uptime: 5 days, since May 25 02:08:01 2023, Last Security Association: ESTABLISHED 2 hours ago Ztun4 connected to: AutoPrimary, IPsec uptime uptime: 5 days, since May 25 02:08:02 2023, Last Security Association: ESTABLISHED 2 hours ago

9.1.1.9 CREDENTIALS INFORMATION

This section shows the User ID in use:

```
CREDENTIALS INFORMATION
```

Username: zs-csc-mux-4-as-d-1@maidenheadbridge.com | PSK: Not shown. Please, read it from 'Configuration Wizards' Menu

Maidenhead Bridge

Cloud Security Connector Mux for Azure | 41

9.1.1.10 http://ip.zscaler.com INFORMATION

Zscaler recommends checking the page <u>http://ip.zscaler.com</u> to validate that you are using Zscaler and see Zscaler Node connected, Cloud and IP address. The CSC does this test for you on each tunnel.

```
http://ip.zscaler.com INFORMATION
Ztun1 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 136.226.49.17, via Public IP: 74.235.173.100
Ztun2 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 136.226.53.25, via Public IP: 74.235.171.133
Ztun3 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 136.226.53.23, via Public IP: 74.235.171.132
Ztun4 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 136.226.49.4, via Public IP: 74.235.171.132
```

9.1.1.11 PROXY BYPASS

This sections shows the Proxy Bypass PAC URL, validates if the Proxy Bypass can access internet directly going to <u>https://ip.maidenheadbridge.com</u> and shows the amounts of proxy bypass rules configured.

```
PROXY BYPASS
Proxy Bypass URL is: https://pac.zscalerthree.net/RdwNltSPqBFN/az-csc-bypass.pac
Proxy Bypass Rules configured via URL: 8
Proxy Bypass Egress Interface 10.2.1.28 can reach test page (https://ip.maidenheadbridge.com) via Public IP 74.235.173.101
```

9.1.1.12 ROUTED BYPASS

This section shows the configuration of Routed Bypasses and check if the routed bypass URL is reachable.

```
ROUTED BYPASS
Routed Bypass URL is: https://mhb-netskope-pac-files.s3.eu-west-1.amazonaws.com/routedBypassRulesFile.json
Routed Bypass Rules configured via URL: 12
Routed Bypass URL https://mhb-netskope-pac-files.s3.eu-west-1.amazonaws.com/routedBypassRulesFile.json is reachable
```

9.1.1.13 AWS SSM AGENT

This section shows the status of the AWS SSM Agent.

```
AWS SSM AGENT
AWS SSM Agent is active (running) since Thu 2023-05-25 01:51:37 UTC; 5 days ago
Registration values: {"ManagedInstanceID":"mi-055ab68d5af2fd09e","Region":"us-east-1"}
```

9.1.1.14 SYSLOG INFORMATION

When configured, this section will show the IP/s and TCP port of your Syslog/SIEM server.



All CSC's logs are tagged with (MHB-CSC)(<action>). The values of <action> are:

SystemLogs:

- UP
- DOWN
- INFO
- ALERT
- ERROR

Traffic Logs:

- ALLOW
- BLOCK

9.1.1.14.1 System Logs example:

To obtain your System Logs, you can search by CSC name plus the following TAG. For example:

Using GrayLog Server: source:zs\-csc\-mux\-4\-as\-d\-1 AND ("UP" OR "DOWN" OR "INFO" OR "ALERT" OR "ERROR")

• From: 2 days ago	Until: Now		Select streams the search show	ld Include. Searches in all strea	ms if empty.		▼ ► Not
Q source:zs\-csc\-mux\-4\-as\-d\-1 AND	("UP" OR "DOWN" OR "INFO"	' OR "ALERT" OR "ERROR")			ę 🔶	Save 🗅 Load 🎥 S
Message Count							0
0							
60						_	
40			_			_	
20							
00:00 Jun 2, 2023	06:00	12:00	18:00	00:00 Jun 3, 2023	06:00	12:00	18:
All Mossage							
. An messages							11
mestamp TF							course 12
imestamp 17							source 17
imestamp TF 2023-06-03 19:52:59.000 :s-csc-mux-4-as-d-1 root: (MHB-CSC)(INFO) Private	e Access - Management Networ	k 172.19.0.0/24 was adde	ed on zs-csc-mux-4-as-d-1				source 17 zs-csc-mux-4-as-d-
Imestamp TF 1023-06-03 19:52:59.000 Ls-csc-mux-4-as-d-1 root: (MHB-CSC)(INFO) Private 2023-06-03 19:52:59.000	e Access - Management Networ	k 172.19.0.0/24 was adde	ed on zs-csc-mux-4-as-d-1				source 17 zs-csc-mux-4-as-d- zs-csc-mux-4-as-d-
Imestamp TF 2023-06-03 19:52:59.000 scose-mux-4-as-d-1 root: (MHB-CSC)(INFO) Private 2023-06-03 19:52:59.000 zs-csc-mux-4-as-d-1 root: (MHB-CSC)(INFO) Private	e Access - Management Networ e Access - Management Networ	k 172.19.0.0/24 was adde k 192.168.1.0/24 was add	ed on zs-csc-mux-4-as-d-1 ded on zs-csc-mux-4-as-d-1				source 17 zs-csc-mux-4-as-d- zs-csc-mux-4-as-d-
Unmestamp 17 2023-06-0319:52:53:000 2s-csc-mux-4-as-d-1 root: (MHB-CSC)(INFO) Private 2023-06-0319:52:53:000 2023-06-0319:52:53:000	e Access - Management Networ e Access - Management Networ	k 172.19.0.0/24 was adde k 192.168.1.0/24 was add	ed on zs-csc-mux-4-as-d-1 ded on zs-csc-mux-4-as-d-1				source 17 zs-csc-mux-4-as-d- zs-csc-mux-4-as-d- zs-csc-mux-4-as-d-
Imestamp IF 2023-06-03 19:52:59:000 2023-06-03 19:52:59:000 2023-06-03 19:52:59:000 Es-csc-mux-4-as-d-1 root: (MHG-CSC)(IMFO) Private 2023-06-03 19:52:59:000 Es-csc-mux-4-as-d-1 root: (MHB-CSC)(IMFO) Private	e Access - Management Networ e Access - Management Networ e Access - Management Networ	k 172.19.8.8/24 was adde k 192.168.1.8/24 was add k 192.168.6.8/24 was add	ed on zs-csc-mux-4-as-d-1 ded on zs-csc-mux-4-as-d-1 ded on zs-csc-mux-4-as-d-1				source 17 zs-csc-mux-4-as-d- zs-csc-mux-4-as-d- zs-csc-mux-4-as-d-
Immediating 17 2022-06-213-252-259.000 2023-06-2013-252-59.000 2023-06-2013-52:59.000 2023-000 2023-000 2023-000 2023-000 2023-000 2023-000 2023-000 2023-000 2023-000 2023-000 2023-000 2023-000 2023-000 20	> Access - Management Networ > Access - Management Networ > Access - Management Networ	k 172.19.0.0/24 was adde k 192.168.1.0/24 was add k 192.168.6.0/24 was add	ed on zs-csc-mux-4-as-d-1 ded on zs-csc-mux-4-as-d-1 ded on zs-csc-mux-4-as-d-1				source 17 zs-csc-mux-4-as-d- zs-csc-mux-4-as-d- zs-csc-mux-4-as-d- zs-csc-mux-4-as-d-
Immetation pt 7) Access - Management Networ) Access - Management Networ) Access - Management Networ ute to Zscaler Changed to Ne	k 172.19.0.0/24 was adde k 192.168.1.0/24 was add k 192.168.6.0/24 was add k 192.168.6.0/24 was add	ed on zs-csc-mux-4-as-d-1 ded on zs-csc-mux-4-as-d-1 ded on zs-csc-mux-4-as-d-1 2: zs-csc-mux-4-as-d-1				source 17 zs-csc-mux-4-as-d- zs-csc-mux-4-as-d- zs-csc-mux-4-as-d- zs-csc-mux-4-as-d- zs-csc-mux-4-as-d-
mentamp 17 2020-00-31952259.000 2020-00-31952259.000 2020-00-31952259.000 2020-00-31952259.000 2020-00-31952259.000 2020-00-31952259.000 2020-00-31952259.000 2020-00-31952259.000 2020-00-31952259.000 2020-00-3195259.000 2020-00-3192659.000 2020-00-3192659.000 2020-00-3192659.000 2020-00-3192659.000 2020-00-3192659.000 2020-00-3192659.000 2020-00-3192659.000 2020-00-3192659.000 2020-00-3192659.000 2020-00-3192659.000 2020-00-3192659.000 2020-00-3192659.000 2020-00-3192659.000 2020-00-3192659.000 2020-00-3192659.000 2020-00-319269.000 2020-000	 Access - Management Networ 	k 172.19.0.0/24 was add k 192.168.1.0/24 was add k 192.168.6.0/24 was add xt Hop: 10.2.2.15 of CSC upp on: Sat 3 Jun 10:24:	ed on zs-csc-mux-4-as-d-1 ded on zs-csc-mux-4-as-d-1 ded on zs-csc-mux-4-as-d-1 D: zs-csc-mux-4-as-d-1 S4 UFC 2023				source 17 zs-csc-mux-4-as-d- zs-csc-mux-4-as-d- zs-csc-mux-4-as-d- zs-csc-mux-4-as-d- zs-csc-mux-4-as-d-
mentamp IF 2020-00 1932:259.000 0220-00 1932:259.000 0220-00 31932:259.000 0220-00 31932:259.000 0220-00 31932:259.000 0220-00 31932:253.000 3=cdc=mux-4as-d-1rot: (MHC-CG)(IMFO) Rev 0220-00 31932:253.000 3=cdc=mux-4as-d-1 rot: (MHC-CG)(IMFO) Rev 0220-00 31932:253.000 1=cdc=mux-4as-d-1 rot: (MHC-CG)(IMFO) Rev 0220-00 31932:253.000 1=cdc=mux-4as-d-1 rot: (MHC-CG)(IMFO) Rev 0=cdc=mux-4as-d-1 rot: (p Access - Management Networ p Access - Management Networ p Access - Management Networ recess - Management Networ rte to Zscaler Changed to Ne incer: Balanced tunnels channer	k 172.19.0.0/24 was add k 192.160.1.0/24 was add k 192.160.6.0/24 was add xt Hop: 10.2.2.15 of CS4 xt Hop: 10.2.2.15 of CS4	ad on zs-csc-mux-4-as-d-1 ded on zs-csc-mux-4-as-d-1 ded on zs-csc-mux-4-as-d-1 D: zs-csc-mux-4-as-d-1 S: urc 2023				source 17 zs-csc-mux-4-as-d- zs-csc-mux-4-as-d- zs-csc-mux-4-as-d- zs-csc-mux-4-as-d- zs-csc-mux-4-as-d- zs-csc-mux-4-as-d-
mentamp 17 2020-00-31952259.000 2020-00-31952259.000 2020-00-31952259.000 2020-00-31952259.000 2020-00-31952259.000 2020-00-31952259.000 2020-00-31952259.000 2020-00-31952259.000 2020-00-31952459.000 2020-00-31952459.000 2020-00-31952459.000	Access - Hanagement Networ a Access - Hanagement Networ p Access - Hanagement Networ rate to Zacaler Changed to Ne uncer: Balanced tunnels chan ancer: ZtunZ is active since	k 172.19.8.8/24 was add k 192.168.1.0/24 was add k 192.168.6.0/24 was add xt Hop: 18.2.2.15 of CSC uge on: Sat 3 Jun 19:24:1 1: Sat 3 Jun 19:24:54 UTC	ed on ze-esc-mux-4-as-d-1 ded on ze-esc-mux-4-as-d-1 ded on zs-esc-mux-4-as-d-1 z: zs-esc-mux-4-as-d-1 54 UTC 2023 C 2023 using primary node				source 17 zs-cscmux-4as-d zs-cscmux-4as-d zs-cscmux-4as-d zs-cscmux-4as-d zs-cscmux-4as-d zs-cscmux-4as-d
mentamp 17 2022-06-31952259.000 2022-06-31952259.000 2022-06-31952259.000 2022-06-31952259.000 2022-06-31952259.000 2022-06-31952259.000 2022-06-31952259.000 2022-06-31952259.000 2022-06-3192255.000 2022-06-31922454.000 2022-06-31922454.000 2022-06-31922454.000	» Access - Management Networ » Access - Management Networ » Access - Management Networ ute to Zecaler Changed to Ne uncer: Blanced tunnels chan uncer: Zturd is active since	k 172.19.0.0/24 was add k 192.168.1.0/24 was add k 192.168.6.0/24 was add nxt Hop: 10.2.2.15 of CSK nyge on: Sat 3 Jun 19:24:54 UTC :: Sat 3 Jun 19:24:54 UTC	ed on ze-esc-mux-4-as-d-1 ded on ze-esc-mux-4-as-d-1 ded on ze-esc-mux-4-as-d-1 2: ze-esc-mux-4-as-d-1 54 UTC 2823 2 2823 using primery mode				source III zs-csc-mux-4-as-d zs-csc-mux-4-as-d zs-csc-mux-4-as-d zs-csc-mux-4-as-d zs-csc-mux-4-as-d zs-csc-mux-4-as-d zs-csc-mux-4-as-d
mentamp IF 2023-06-0135253.000 2023-06-015253.000 2023-06-0152553.000 2023-06-0152555.000 2023-000 2023-000 2023-000 2023-000	Access - Management Networ p Access - Management Networ r Access - Mana	k 172.19.0.0/24 was add k 192.168.1.0/24 was add k 192.168.6.0/24 was add k 192.168.6.0/24 was add yst Hop: 10.2.2.15 of CSG yst On: Sat 3 Jun 19:2454 UTC : Sat 3 Jun 19:24154 UTC : Sat 3 Jun 19:24154 UTC	ed on zs-ese-mux-4-as-d-1 ded on zs-ese-mux-4-as-d-1 ded on zs-ese-mux-4-as-d-1 21: zs-ese-mux-4-as-d-1 34: UTC 2023 2: 2023 using primary node 2: 2023 using primary node				source 17 IS-SIC-mux-4-as-d- IS-SIC-mux-4-as
Immetation 17 Im	Access - Hanagement Networ a Access - Hanagement Networ p Access - Hanagement Networ ret to Zscaler Changed to Ne ancer: Balanced tunnels chan ancer: Ztund is active since ancer; Ztund is active since	k 172.19.0.0/24 was adds k 192.168.1.0/24 was add k 192.168.6.0/24 was add out Hop: 10.2.2.15 of CS ge on: Sat 3 Jun 19:24:15 : Sat 3 Jun 19:24:154 UTC	ed on ze-esc-mux-4-as-d-1 ded on ze-esc-mux-4-as-d-1 ded on ze-esc-mux-4-as-d-1 z: ze-esc-mux-4-as-d-1 ded on ze-esc-mux-4-as-d-1 z: ze-esc-mux-4-as-d-1 c: ze-ze-mux-4-as-d-1 c: ze-ze-mux-4-as-d-1 c: ze-ze-mux-4-as-d-1 z: ze-ze-mux-4-as-d-1 c: ze-ze-mux-4-as-d-1 c				source IF zs-cs:mux-4-as-d zs-cs:mux-4-as-d zs-cs:mux-4-as-d zs-cs:mux-4-as-d zs-cs:mux-4-as-d zs-cs:mux-4-as-d zs-cs:mux-4-as-d zs-cs:mux-4-as-d

Maidenhead Bridge

Cloud Security Connector Mux for Azure | 43

9.1.1.14.2 Traffic Logs example:

Using GrayLog Server: source:zs\-csc\-mux\-4\-as\-d\-1 AND ("ALLOW" OR "BLOCK")



9.1.1.15 HIGH AVAILABILITY Information

This section show all the information when the CSC Mux is configured on HA:

```
HIGH AVAILABILITY Information

The HA service is: active (running) since Sat 2023-06-03 00:22:49 UTC; 19h ago

Identity Type: SystemAssigned

Route to Zscaler using Next Hop: 10.2.2.15 of VM: zs-csc-mux-4-as-d-1 (this CSC)

Current values configured are:

Route/s (Qty)= 2

Route 1: Server-default-route (Route Table=Servers-Route-Table, Resource Group=RouteTables-East-US)

Route 2: Zscaler-Global-GW (Route Table=Servers-Route-Table, Resource Group=RouteTables-East-US)

Computer Name of other CSC in the pair: zs-csc-mux-4-as-d-2 (Resource Group=CSC-EAST-US)

Private Access Public IP= 74.235.173.101
```

- If HA service is active.
- The Identity Type in use.
- The current "Next Hop" active for all "Route/s" configured.
- Amount of Routes configured.
- The Route names.
- Which is the VM Name of other CSC on the HA pair.
- Private Access Public IP.

9.1.2 Show Interfaces Traffic

Use this section to see the traffic in real time.



9.1.3 Tcpdump, Traceroute and Latency Test



9.1.3.1 Tcpdump

The objective of this test is to have detailed visibility of any type of traffic via any interface.



You can repeat the last command or running a new command. Example running a new command:

- Select the options:



- The test will show the resulting tcpdump command and will show the traffic captured.

COMMAND: sudo timeout 30 tcpdump -n -l -c 10 -i eth1 host 10.2.9.4 and tcp port 22 tcpdump: verbose output suppressed, use -v[v] for full protocol decode listening on eth1, link-type ENIOMB (Ethernet), snapshot length 262144 bytes 17:48:12.8771 IP 10.2.2.15.22 - 10.2.9.4.33304: Flags [-], sea 375339517:3253839705, ack 2539124923, win 501, options [nop,nop,TS val 4053139764], length 0 17:48:12.838167 IP 10.2.9.4.33304 > 10.2.2.15.22: Flags [.], ack 188, win 501, options [nop,nop,TS val 3660662977 ecr 4053139764], length 0 17:48:12.838167 IP 10.2.9.4.33304 > 10.2.2.15.22: Flags [.], ack 188, win 501, options [nop,nop,TS val 4053139564], length 0 17:48:12.931384 IP 10.2.9.4.33304 > 10.2.2.15.22: Flags [.], ack 41, win 501, options [nop,nop,TS val 405313958 ecr 36606632977], length 356 17:48:13.021197 IP 10.2.9.4.33304 > 10.2.2.15.22: Flags [.], ack 414, win 501, options [nop,nop,TS val 4053139958], length 0 17:48:13.021137 IP 10.2.9.4.33304 > 10.2.2.15.22: Flags [.], ack 414; win 501, options [nop,nop,TS val 4053139958] ecr 3660683071], length 32 17:48:13.021137 IP 10.2.2.15.22 > 10.2.9.4.33304; Flags [P.], seq 544:876, ack 1, win 501, options [nop,nop,TS val 4053139948] ecr 3660683071], length 32 17:48:13.02533 IP 10.2.2.15.22 > 10.2.9.4.33304; Flags [P.], seq 544:876, ack 1, win 501, options [nop,nop,TS val 4053139948] length 0 17:48:13.025439 IP 10.2.2.15.22 > 10.2.9.4.33304; Flags [P.], seq 876:1208, ack 1, win 501, options [nop,nop,TS val 4053149052] ecr 366068310[1], length 332 17:48:13.225332 IP 10.2.2.15.22 > 10.2.9.4.33304; Flags [P.], seq 1208:1540, ack 1, win 501, options [nop,nop,TS val 4053149052] ecr 3660683216[1], length 332 17:48:13.229322 IP 10.2.2.15.22 > 10.2.9.4.33304; Flags [P.], seq 1208:1540, ack 1, win 501, options [nop,nop,TS val 405314052], length 0 17:48:13.229322 IP 10.2.2.15.22 > 10.2.9.4.33304; Flags [P.], seq 1208:1540, ack 1, win 501, options [nop,nop,TS val 405314056326 ecr 3660683265], length 332 17:48:13.229322 IP 10.2.2.15.22 > 10.2.9.4.33304 + Flags [.], ack 1	Enter your choice: 2
tcpdump: verbose output suppressed, use -v[v] for full protocol decode Listening on eth1, link-type ENIOM® (Ethernet), snapshot length 262144 bytes 17:48:12.83771 IP 10:2.15.22 > 10:2.94.33304: Flags [-], set 188:544, act], win 501, options [nop,nop,TS val 4653139764], length 0 17:48:12.838167 IP 10:2.9.4.33304 > 10:2.2.15.22 + Flags [], ack 188, win 501, options [nop,nop,TS val 3660682977 ecr 46531393764], length 0 17:48:12.93277 IP 10:2.9.4.33304 > 10:2.2.15.22 + Flags [], ack 188, win 501, options [nop,nop,TS val 3660682977], length 0 17:48:12.93277 IP 10:2.9.4.33304 > 10:2.2.15.22 + Flags [], ack 544, win 591, options [nop,nop,TS val 3660682977], length 356 17:48:12.932277 IP 10:2.9.4.33304 > 10:2.2.15.22 + Flags [], ack 544, win 591, options [nop,nop,TS val 3660683071 ecr 4053139958], length 0 17:48:13.021197 IP 10:2.2.15.22 > 10:2.9.4.33304: Flags [P.], seq 188:544, ack 1, win 501, options [nop,nop,TS val 4053139948 ecr 3660683071], length 332 I7:48:13.021137 IP 10:2.9.4.33304 > 10:2.2.15.22: Flags [], ack 544, win 501, options [nop,nop,TS val 4053139948], length 0 17:48:13.021137 IP 10:2.9.4.33304 > 10:2.2.15.22: Flags [], ack 876, win 501, options [nop,nop,TS val 4053139948 ecr 3660683071], length 332 I7:48:13.02134 IP 10:2.9.4.33304 > 10:2.2.15.22: Flags [], ack 876, win 501, options [nop,nop,TS val 4053139948], length 0 17:48:13.025393 IP 10:2.9.4.33304 > 10:2.2.15.22: Flags [], ack 10:0, win 501, options [nop,nop,TS val 405314092 ecr 3660683101], length 332 I7:48:13.02540 IP 10:2.9.4.33304 > 10:2.2.15.22: Flags [], ack 12:0, win 501, options [nop,nop,TS val 4053140952 ecr 3660683205[], length 0 17:48:13.229322 IP 10:2.9.4.33304 > 10:2.2.15.22: Flags [], ack 12:0, win 501, options [nop,nop,TS val 4053140952 ecr 3660683205], length 332 17:48:13.229322 IP 10:2.9.4.33304 > 10:2.2.15.22: Flags [], ack 12:0, win 501, options [nop,nop,TS val 4053140952 ecr 3660683205], length 332 17:48:13.231098 IP 10:2.9.4.33304 > 10:2.2.15.22: Flags [], ack 12:0, win 501, options [nop,nop,TS val 4053140	COMMAND: sudo timeout 30 tcpdump -n -l -c 10 -i eth1 host 10.2.9.4 and tcp port 22
	tcpdump: verbose output suppressed, use -v[v] for full protocol decode Listening on eth1, link-type ENIOM® (Ethernet), snapshot length 262144 bytes 17:48:12.83771 IP 10:2.2.15.22 > 10:2.9.4.33304: Flags [F], seq 1253339517:3253839705, ack 2539124923, win 501, options [nop,nop,TS val 4053139764], length 0 17:48:12.838167 IP 10:2.9.4.33304 > 10:2.2.15.22: Flags [], ack 186, win 501, options [nop,nop,TS val 3660682977], length 138 17:48:12.931384 IP 10:2.9.4.33304 > 10:2.2.15.22: Flags [], ack 186, win 501, options [nop,nop,TS val 3660682977], length 356 17:48:12.932277 IP 10:2.9.4.33304 > 10:2.2.15.22: Flags [], ack 544, win 501, options [nop,nop,TS val 4053139586], length 6 17:48:12.932277 IP 10:2.9.4.33304 > 10:2.2.15.22: Flags [], ack 544, win 501, options [nop,nop,TS val 4053139948 ecr 3660682971], length 356 17:48:13.022134 IP 10:2.9.4.33304 > 10:2.2.15.22: Flags [], ack 544, win 501, options [nop,nop,TS val 4053139948], length 6 17:48:13.022134 IP 10:2.9.4.33304 > 10:2.2.15.22: Flags [], ack 544, win 501, options [nop,nop,TS val 4053139948], length 6 17:48:13.022134 IP 10:2.9.4.33304 > 10:2.2.15.22: Flags [], ack 186, win 501, options [nop,nop,TS val 4053139948], length 6 17:48:13.022134 IP 10:2.9.4.33304 > 10:2.2.15.22: Flags [], ack 186, win 501, options [nop,nop,TS val 4053149948], length 6 17:48:13.022134 IP 10:2.9.4.33304 > 10:2.2.15.22: Flags [], ack 186, win 501, options [nop,nop,TS val 4053149952 ecr 3660683161], length 32 17:48:13.022134 IP 10:2.9.4.33304 > 10:2.2.15.22: Flags [], ack 186, win 501, options [nop,nop,TS val 4053149052 ecr 3660683265], length 32 17:48:13.223927 IP 10:2.9.4.33304 > 10:2.2.15.22: Flags [], ack 186, win 501, options [nop,nop,TS val 4053149052 ecr 3660683265], length 32 17:48:13.223927 IP 10:2.9.4.33304 > 10:2.2.15.22: Flags [], ack 186, win 501, options [nop,nop,TS val 4053149052 ecr 3660683265], length 332 17:48:13.23098 IP 10:2.9.4.33304 > 10:2.2.15.22: Flags [], ack 1540, win 501, options [nop,nop,TS val 4053149156], length 6 10 packets captured 10

9.1.3.2 Traceroute and Latency Test

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

- **IMPORTANT**: It is required to allow ICMP Time exceeded (type 11) on the Inbound rule of the Security Group of eth0 to destination IP: x.x.x.x (\leftarrow This IP is Ztun1)

Without this security rule added, you will not able to see the results of middle hops.

- When the Ztun1 is UP, a Reverse Path test from the active ZEN to Ztun1 Public IP is performed

- Max Hops is equal 30. This test can take a while.

Example of temporary ICMP Rule required:

csc-mux-3-2Gbps-v	m-eth0-1 csc-mux-3-2Gbps-vm-eth1-1								
IP configuration ① Ztun1 (Primary)	~								
Network Interface: csc-mux-3-2Gbps-vm-eth0-1 Effective security rules Troubleshoot VM connection issues Topology Virtual network/subnet: VNET-East-US/csc-external-East-US NIC Public IP: 52.188.172.172 NIC Private IP: 10.2.1.13 Accelerated networking: Enabled									
Network securit Impacts 0 subnet	y group csc-mux-3-2Gbps-vm-eth0-NSG-1 (attached : s, 1 network interfaces	o network interface: csc-mux	-3-2Gbps-vm-eth0-1)			Add inbou	ind port rule		
Priority	Name	Port	Protocol	Source	Destination	Action			
100	temporary-icmp-rule	Any	ICMP	Any	10.2.1.13	Allow	•••		
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	•••		
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow	•••		
65500	DenyAllinBound	Any	Any	Any	Any	Oeny			

My TraceRoute	(MTR) Test Report									
This test doe	5 10 probes DIRECT to Primary / Secondary ZEN and	d a Rever	se tes	t via i	Ztun1	to Ztu	n1 Pub	ic IP		
Notes:										
- IMPORTANT:	It is required to allow ICMP Time exceeded (type	11) on t	he Inb	ound ru	ule of	the Se	ecurit	Group of eth0 1	to destination IP	P: 10.2.1.24
Without thi	s security rule added, you will not able to see i	the resul	TS OT	middle	nops.	formo	d			
- Max Hons is	equal 30 This test can take a while	EN LO ZLU	III PUD		IS he	TUTILE	u			
Hux Hops 13	equal 50. This cest can take a white									
Testing Prima	ry ZEN: AutoPrimary : vpn.zscalerthree.net > 165	.225.48.1	0							
Start: 2023-0	5-30T17:41:51+0000									
HOST: zs-csc-	nux-4-as-d-1	Loss%	Snt	Last	Avg	Best	Wrst	StDev		
1. AS???	???	100.0	10	0.0	0.0	0.0	0.0	0.0		
2. AS???	???	100.0	10	0.0	0.0	0.0	0.0	0.0		
3. AS???	777	100.0	10	0.0	0.0	0.0	0.0	0.0		
4. AS???	222	100.0	10	0.0	0.0	0.0	0.0	0.0		
5. A5!!! 6. A\$222	222	100.0	10	0.0	0.0	0.0	0.0	0.0		
7. AS8075	ae34-0.ash-96che-1a.ntwk.msn.net (104.44.233.19)) 0.0%	10	1.0	3.1	1.0	13.7	4.0		
8. AS???	egix-was1-r2.zscaler9.net (206.126.237.212)	10.0%	10	299.2	291.3	280.3	309.1	8.8		
9. AS22616	165.225.254.30	50.0%	10	287.0	295.0	287.0	302.2	5.6		
10. AS22616	165.225.48.10	0.0%	10	1.4	1.7	1.4	3.2	0.5		
Testing Secon	dary ZEN: AutoSecondary : secondary.vpn.zscalert	hree.net	> 165.	225.38	. 52					
Start: 2023-0	5-30T17:42:11+0000									
HOST: zs-csc-	nux-4-as-d-1	Loss%	Snt	Last	Avg	Best	Wrst	stDev		
1. AS????	222	100.0	10	0.0	0.0	0.0	0.0	0.0		
2. A5((([[[222	100.0	10	0.0	0.0	0.0	0.0	0.0		
4 AS222	222	100.0	10	0.0	0.0	0.0	0.0	0.0		
5. AS???	???	100.0	10	0.0	0.0	0.0	0.0	0.0		
6. AS???	???	100.0	10	0.0	0.0	0.0	0.0	0.0		
7. AS8075	be-144-0.ibr03.bl7.ntwk.msn.net (104.44.32.32)	0.0%	10	7.9	7.4	6.9	8.4	0.4		
8. AS8075	be-10-0.ibr01.ewr30.ntwk.msn.net (104.44.16.8)	0.0%	10	6.9	7.0	6.8	7.6	0.2		
9. AS8075	ae25-0.ear04.ewr30.ntwk.msn.net (104.44.33.204)	0.0%	10	6.8	8.6	6.3	12.4	2.3		
10. AS8075	ae27-0.ier01.teb31.ntwk.msn.net (104.44.239.19)	0.0%	10	6.5	6.6	6.3	7.0	0.2		
11. AS22616	165.225.250.79	0.0%	10	6.5	6.5	6.2	6.7	0.2		
12. AS22616	165.225.38.52	0.0%	10	7.2	7.0	6.6	8.0	0.4		
Reverse nath	from: AutoPrimary to your Public IP: 74 235 173	100								
Start: 2023-0	5-30T17:42:32+0000	100								
HOST: ZS-CSC-	nux-4-as-d-1 Loss% Snt Last Avg	Best Wrs	t StDe	v						
1. AS???	??? 100.0 10 0.0 0.0	0.0 0.	0 0.	0						
2. AS22616	136.226.49.23 0.0% 10 2.3 2.2	1.7 3.	ΘΘ.	4						
3. AS22616	136.226.48.2 50.0% 10 304.3 299.4 28	87.1 304.	37.	0						
4. AS22616	165.225.250.62 90.0% 10 2.2 2.2	2.2 2.	2 0.	0						
5. AS8075	104.44.51.17 0.0% 10 4.9 11.4	2.3 64.	3 18.	8						
6. AS???	100.0 10 0.0 0.0	0.0 0.	ο Θ.	0						

9.1.4 SPEED TEST

This test is experimental because we use third-party tools (speedtest.net), but it works fine in most cases. Here the result using a CSC Mux 4.



Note: At the moment of writing this documentation, Zscaler provides 400 Mbps per IPsec tunnel. When running a single test without production traffic, it is possible to obtain aggregates speeds of more than 1.6 Gbps, but with production traffic, Zscaler will rate limit the traffic to 400 Mbps.

9.2 CSC Admin Tasks

```
CSC Admin tasks
5) AWS SSM Agent (Register or De-Register)
6) Manage Administrators, Restrict SSH access and Radius Configuration.
7) Change Timezone
```

9.2.1 AWS SSM Agent (Register or De-Register)

The CSC AWS has installed the AWS SSM Agent that allows you to check remotely the status of the CSC and "Run Commands" using AWS Systems Manager. You can manage all CSCs models³ using AWS Systems Manager.

Note: You can learn more about "Run Commands" on Appendix B

Steps to create a "Hybrid Activation" and "Register the CSC".

9.2.1.1 Create a "Hybrid Activation" from AWS console.

On your AWS Console, go to Services \rightarrow Systems Manager \rightarrow Node Management \rightarrow Hybrid Activations and click "Create". Fill the values on shown below:

AWS Systems	envices, teatures, blogs, docs, and more [Att+5] AW5 Systems Manager > Activations > Create activation
Manager	
Quick Setup	Create activation 3
Operations Management Explorer	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-premites servers or virtual machines. Learn more IP
OpsCenter	Activation description- Optional 4 - Put a name to the activation
CloudWatch Dashboard	csc-gre-for-netskope-on-aws-a
PHD	Maximum 256 characters.
Incident Manager New	Instance limit Specify the total number of servers and VMs that you want to register with AWS. The maximum is 1000.
Application Management	1
Application Manager New	Maximum number is 1000.
AppConfig	
Parameter Store	To register more than 1,000 managed instances in the current XWS account and Change setting Region, change your account settings to use advanced instances. Learn more
Change Management	IAM role To enable communication between SSM Agent on your managed instances and AW5, specify an IAM role
Change Manager New	Use the default role created by the system (AmazonEC2BunCommandBoleEorManagedInstances)
Automation	Select an existing custom IAM role that has the required permissions
Change Calendar Maintenance Windows	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 numing instances.
	yyyy-mm-ddThh::mm-00:00
Node Management	The expiry date must be in the future, and not more than 30 days into the future
Fleet Manager	Default Instance name- Optional
Compliance	Specify a name to help you identify this managed instance when it is displayed in the console or when you call a List API.
inventory 2	csc-gre-tor-netskope-on-aws-a
Hybrid Activations 2	Presentition 250 characters. 5 - Repeat the name
Session Manager	0
Kun Command	Cancel Create activation
State Manager	

3 For Vmware, Hyper-V, KVM, Azure, Gcloud and AWS.



\rightarrow Click "Create Activation"

$\leftarrow \rightarrow$	C a a	onsole.aws.amazo	on.com/systems-manager/activations/aregion=us-east-1 2
aws	Services	Q Search for se	rvices, features, blogs, docs, and more [Alt+S]
AWS Mana	Systems ager	×	⊘ 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 MI]+cpTwxKxht2]VAxza
Quick	Setup		Activation ID Caba407C-56C7-4Ca1-5655-E506401 (ab56 You can now install amazon-ssm-agent and manage your instance using Run Command. Learn more 13

The vaules of Actication Code, Activation ID and Region are required to register the CSC. Keep this values on a safe place.

9.2.1.2 Register the CSC



9.2.1.3 View the Registered CSC on AWS Systems Manager

aws	Services Q. Search for services, features, blogs, docs, and more [Alt+5]	Ð	\$	Ø	ŀ
=	AWS Systems Manager 🍐 Fleet Manager				
	Fleet Manager Info				
	Managed nodes Settings				
	Managed nodes C 🛛 Download report New Node ac	ctions 1	•	Account	m
	Q Filter 1 match				<
	SSM Agent ping status = Online X Clear filters Total: 29 nodes Last fetched at: 12:48 PM				
	Node ID V Node name V IP address V SSM Agent ping st V Platform type V Operating System V Platform version V	▽ (Compute	er name	
	□ mi-0fc0d5394a2bfefed csc-gre-for-netskope-on-aws-a 172.31.96.172 ⑦ Online Linux Ubuntu 20.04 2.3.814.0	-	ip-172-3	31-96-17	2

9.2.2 Manage Administrators, Restrict SSH access and Radius Configuration

IMPORTANT: This section can be accessed only by the "cscadmin" user.



9.2.2.1 Manage Administrators: cscadmin and csccli

The CSC Mux for AZure has 2 users configured: cscadmin (for SSH Administrator Console Access), csccli (standard user, disabled by default.).

From this menu, you can edit the SSH Keys or Password.



Note: the user "cscadmin" cannot be disabled.

9.2.2.1.1 "cscadmin" settings



Maidenhead Bridge

Cloud Security Connector Mux for Azure | 51

9.2.2.1.2 "csccli" settings

Note: the "csccli" user allows console access to the CSC. If you are managing the CSC using Rundeck, or Ansible, you will need to enabled the "csccli" user and to setup the SSH Key.

1) cscadmin 2) csccli 3) Quit Enter your choice: 2
User 'csccli' is not enabled.
Do you want to enable user 'csccli'?
1) Yes 2) No Enter your choice: 1
User 'csccli' was enabled via console.
Please, input a SSH Key for user 'csccli'
This Menu allows to add/delete the SSH Public keys using Nano editor.
To save, press CTRL+S and to exit Nano, press CTRL+X
Do you want to continue?
1) Edit SSH Keys 2) Quit Enter your choice:

9.2.2.1.3 Managing the SSH Key of a User

You can add/remove keys for a User using "nano editor" when selecting the user from the previous menu.

9.2.2.2 Restrict SSH Access

This functionality allows administrators to restrict SSH access to the CSC. You can setup restrictions for the Internal (eth1) and the PriCPA (wg0) interface. SSH to external (eth0) interface is always blocked.

IMPORTANT (1): DEFAULT VALUES.

-> Internal Interface (eth1): SSH the CSC to CSC GW IP (<IP>) is allowed from any Host or Subnet.

-> External Interface (eth0): SSH the CSC to any eth0 IP is permanently blocked and cannot be changed.

-> PriCPA Interface (wg0): SSH the CSC to wg0 IP (<IP>) is allowed from any other PriCPA node that belongs to the PriCPA Subnet. (<Subnet>/<Bitmask>)

IMPORTANT (2): If the Host or Subnet is reachable via PriCPA interface and not Internal Interface eth1, you must add these Hosts or Subnets as Management Networks on PriCPA configuration.

Example of configuration:



9.2.2.3 Radius Configuration

This functionality enables Radius Authentication for users accessing the Admin Console. The configuration requires the Radius Server IP and Secret. Optionally, you can add a secondary radius server as backup.

-> Configuration on the CSC: Add Radius Server and User:



-> Example Configuration Windows NPS

1 - Create Network Policy

In this particular case we are allowing users on the Security Group = Radius Users to authenticate using radius protocol. Please, note the Authentication method required.

Network Policy Server						-	
File Action View Help							
🗢 🤿 🙋 📰 🚺							
NPS (Local) RADIUS Clients and Servers ADDUS Clients and Servers	Network Policies	ecionate who is authorized to	connect	to the network and t	he circumstance	e under wh	ich they
RADIUS Clients	or cannot connect.	calginate who is dationized to	Connect	to the network and t			ion they
Connection Request Po	Policy Name 2		Status	Processing Order	Access Type	Source	
Network Policies	LinuxAuthenticator		Enabled	1	Grant Access	Unspecifie	ed
Networking	Connections to Microsoft Routing an	d Remote Access server	Enabled	2	Deny Access	Unspecifie	ed
🗸 📑 Templates Management	Connections to other access servers		Enabled	3	Deny Access	Unspecifie	ed
Shared Secrets							
RADIUS Clients							
Remote RADIUS Servers							
IP Filters							
	LinuxAuthenticator						
	Conditions - If the following conditions	are met:					
	Condition Value						
	User Groups MAIDENHEADBRIDG	RadiusUsers 4					
		· ·					
	Settings - Then the following settings	are applied:					
	Setting	Value					
	Seuing	value					
	Access Permission	Grant Access					
	Extensible Autnentication Protocol M	EAP OR Upercents	assword (EAP-MOUTAP V2)	3		
	Framed-Protocol	PPP	a authenti	cauon (FAP, SPAP)			
	Service-Type	Framed					
		- Harried					

2 - Add the CSC as Radius Clients:

Note: The traffic will arrive to the NPS with source IP: CSC GW IP



9.2.3 Change Timezone

Use this menu to select the timezone of the CSC.

<0K>

WARNING: Some SIEM/SYSLOG software will show the logs in the past or future if the Time Zone is incorrect. In most circumstances, UTC is the best choice.

election: 7
our current Time Zone is UTC +0000 ARNING: Some SIEM/SYSLOG software will show the logs in the past or future if the Time Zone is incorrect. In most circumstances, UTC is the best choice.
o you want to change the Time Zone?) Yes) No nter your choice:

Configuring tzdata | Please select the geographic area in which you live. Subsequent configuration questions will narrow this down by presenting a list of cities, representing the time zones in which they are located. Geographic area:

Africa
America
Antarctica
Australia
Arctic Ocean
Asia
Atlantic Ocean
Europe
Indian Ocean
Pacific Ocean
System V timezone
US
None of the above

<Cancel>

9.3 Proxy Bypass

The Proxy Bypass functionality allows doing layer 7 bypasses. This functionality works in conjunction with PAC files.



9.3.2 View Current Proxy Bypass List

This menu displays the current Proxy Bypass List. For example:



9.3.3 Configure Proxy Bypass List

This menu allows to configure the Proxy Bypass List.



9.3.3.1 Auto - Proxy Bypass PAC URL

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

The "Proxy Bypass PAC file" URL acts is a central repository of all Layer 7 bypasses required. Moreover, if you manage the CSCs using AWS Systems Manager (or another tool), you can update all CSCs in your network doing one command.

Example of Proxy Bypass PAC:



Note 1: 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 2: The Bypass Proxy port is 3128

Configuring the Proxy Bypass PAC URL and Refresh the List

Selection: 9
Please, select method to configure Proxy Bypass List
1) Auto - Proxy Bypass PAC URL 2) Manual 3) Quit Enter your choice: 1
Please, select method to configure Proxy Bypass List
1) Configure Proxy Bypass PAC URL and/or Update Proxy Bypasses 2) See PAC Proxy Bypass Example 3) Quit
Enter your choice: 1 Proxy Bypass Configuration
Your current Proxy Bypass PAC URL is https://pac.zscalerthree.net/RdwNltSPqBFN/az-csc-bypass.pac
Do you want to change the Proxy Bypass PAC URL? 1) Yes 2) No Enter your choice: 2
Do you want to refresh Proxy Bypass List? 1) Yes 2) No Enter your choice: 1
This is your current Proxy Bypass List
.okta.com .oktacdn.com .okta-emea.com login.mydomain.com login.microsoftonline.com login.microsoft.com login.windows.net ip.maidenheadbridge.com
Do you want apply changes?
2) No Enter your choice: 1
(MHB-CSC)(INFO) Proxy Bypass List updated sucessfully.

9.3.3.2 Manual Proxy Bypass Configuration.

If you want to update manually your Proxy Bypass list, follow this steps.

1. Select Option 2)



2. Input "y"

GNU nano 4.8			domains			Modified
.okta.com						
.oktacdn.com						
.okta-emea.com						
login.mydomain.	com					
login.microsoft	conline.com					
login.microsoft						
login.windows.n	let					
portquiz.net manualAdded.com	.					
	L .					
C Cot Holp	AD Write Out	Where Tr	AV Cut Text	Al Justify	Cur Pos	M-II Undo
^X Exit	^R Read File	^\ Replace	^U Paste Text	^T To Spell	^ Go To Line	M-E Redo

- 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	Proxy	Bypass	List				
.okta.com .oktacdn.com .okta-emea.com login.mydomain.com login.microsoftonline.com login.microsoft.com login.windows.net portquiz.net manualAdded.com										
Do ya 1) Ye 2) Na Enter	ouv es o ryo	want a our ch	apply cha noice: []	anges?						

6. Apply Changes Yes or No. If "1" you will receive the following message:



9.4 Routed Bypass

When routing all traffic via the CSC GW IP, the Routed Bypass functionality allows you to connect specific destinations (IP/Subnet) direct to the Internet using your Public IP. By default, all destinations will travel via the tunnels to Zscaler. If you want to bypass the tunnel, you need to create a Routed Bypass Rule.

Rout	ted Bypass	
10)	View Current Routed Bypass List	
11)	Configure Routed Bypass List	

9.4.1 Routed Bypass - Traffic Flow



9.4.2 View Current Routed Bypass List

You can select to view the Routed Bypass Rules in Compact format or JSON.



9.4.2.1 Compact

Enter	your	choice: 1				
Curren	t Va	lues configur	ed are:			
Index:	0,	Protocol: icm	, SourceIP	: 0.0.0.0/0	, DestinationIP:	: 1.1.1.1/32, FromPort: , To Port: , Description: "Test ICMP"
Index:	1,	Protocol: tcp	SourceIP:	0.0.0.0/0,	DestinationIP:	20.190.128.0/18, FromPort: 443, To Port: 443, Description: "0365 Login URLs 2"
Index:	2,	Protocol: tcp	SourceIP:	0.0.0.0/0,	DestinationIP:	40.126.0.0/18, FromPort: 80, To Port: 80, Description: "0365 Login URLs 3"
Index:	З,	Protocol: tcp	SourceIP:	0.0.0.0/0,	DestinationIP:	52.47.209.216/32, FromPort: 80, To Port: 80, Description: "portquiz.net"
Index:	4,	Protocol: tcp	SourceIP:	0.0.0.0/0,	DestinationIP:	40.126.0.0/18, FromPort: 443, To Port: 443, Description: "0365 Login URLs 4"
Index:	5,	Protocol: udp	SourceIP:	0.0.0.0/0,	DestinationIP:	13.107.64.0/18, FromPort: 3478, To Port: 3481, Description: "Skype and Teams UDP 1"
Index:	6,	Protocol: udp	SourceIP:	0.0.0.0/0,	DestinationIP:	52.112.0.0/14, FromPort: 3478, To Port: 3481, Description: "Skype and Teams UDP 2"
Index:	7,	Protocol: udp	SourceIP:	0.0.0.0/0,	DestinationIP:	52.120.0.0/14, FromPort: 3478, To Port: 3481, Description: "Skype and Teams UDP 3"
Index:	8,	Protocol: tcp	SourceIP:	0.0.0.0/0,	DestinationIP:	216.239.38.21/32, FromPort: 443, To Port: 443, Description: "ip.maidenheadbridge.com 1"
Index:	9,	Protocol: tcp	SourceIP:	0.0.0.0/0,	DestinationIP:	216.239.36.21/32, FromPort: 443, To Port: 443, Description: "ip.maidenheadbridge.com 2"
Index:	10,	Protocol: tc), SourceIP	: 0.0.0.0/0	, DestinationIP:	: 216.239.34.21/32, FromPort: 443, To Port: 443, Description: "ip.maidenheadbridge.com 3"
Index:	11,	Protocol: tc	, SourceIP	: 0.0.0.0/0	, DestinationIP:	: 216.239.32.21/32, FromPort: 443, To Port: 443, Description: "ip.maidenheadbridge.com 4"

9.4.2.2 Json

```
Selection: 10
Please, Select 'Compact' or 'Json' format

    Compact

Json
3) Quit
Enter your choice: 2
  "routedBypassRules": [
    ł
       "description": "Test ICMP",
       "ipProtocol": "icmp",
"sourceCirdIp": "0.0.0.0/0",
       "destinationCirdIp": "1.1.1.1/32",
       "fromPort": "",
"toPort": ""
    },
{
       "description": "0365 Login URLs 2",
       "ipProtocol": "tcp",
"sourceCirdIp": "0.0.0.0/0",
       "destinationCirdIp": "20.190.128.0/18",
       "fromPort": "443",
"toPort": "443"
    },
     {
       "description": "0365 Login URLs 3",
       "ipProtocol": "tcp",
"sourceCirdIp": "0.0.0.0/0",
       "destinationCirdIp": "40.126.0.0/18",
       "fromPort": "80",
"toPort": "80"
```



9.4.3 Configure Routed Bypass List

There are two methods to configure the Routed Bypass List: Routed Bypass URL and Manual. The recommended method is to use Routed Bypass URL.



9.4.3.1 Routed Bypass URL

Routed Bypass URL is the recommended method. Create an AWS bucket or Azure Blob and place your JSON file on it. Here an example:

https://mhb-csc-pac.s3.amazonaws.com/routedBypassRulesFile.json



9.4.3.2 Manual (Paste Routed Bypass JSON file)

Another option to configure Routed Bypass Rules is to paste the JSON file using the following menu:



and paste the JSON file. The JSON file will be displayed, and if no errors are found, you can apply the changes:



9.5 System and Traffic Logs

In this section you can view System Logs, configure Syslog Servers and enable/disable traffic logs.



9.5.1 View System Logs



9.5.2 Configure Syslog and Traffic Logs



Maidenhead Bridge

Cloud Security Connector Mux for Azure | 66

9.6 Configuration Wizards

In this section, you can run the Configuration Wizard to change Zscaler Nodes, VPN Credentials, DNS servers, SNMP, Switch tunnels, and configure High Availability.

```
Configuration Wizards
14) Configure Zscaler Nodes, VPN Credentials, DNS servers and SNMP.
15) Switch Zscaler Tunnels - Primary / Secondary.
16) High Availability configuration.
```

9.6.1 Configure Zscaler Nodes, VPN Credentials, DNS servers and SNMP.



9.6.1.1 Zscaler Nodes and VPN Credentials

This wizard allows you to change the current values configured. It is the same wizard that runs at the initial deployment of the CSC when not using the configUserData.json file to pass User Data.

In this section we are going to show how to select Zscaler Nodes manually.



Selecting the Nodes:

Enter your choice: I					
Please, select your Cloud					
1) zscalerthree 2) zscloud 3) zscalertwo 4) zscalerone 6) zscalerone 7) zscaleropa 8) Not in the list? Input Manually 9) Ouit Enter your choice; 1					
Please select Manual or Auto Node	Selection				
1) Manual 2) Auto 3) Quit Enter your choice: 1					
Please, select your Primary Node on Nodes marked with (-NRU) may be Not	'zscalerthree' Ready for Use. Check http://ips.zsca	lerthree.net			
1) DHCA_Assicredma 2) DHCA_AssicredmaII 2) DHCA_fructedmaII 3) DHCA_fructedmaII 4) DHCA_(DobmAII 5) DHCA_NobmAII 5) DHCA_NobmAII 6) DHCA_NobmAII 5) DHCA_NOBMAIII 5) DH	12) BFK.4 LapelI 13) GFK.4 doAlH 14) GFK.4 ModrAdHI 15) GFK.4 MonCesterf 16) EFK.4 MonCesterf 16) BFK.4 MonCesterf 17) BFK.4 MinI 10) BFK.4 MonCest 10) BFK.4 MonCest 11) BFK.4	 BFEA, Rouent BFEA, Stockholmilli BFEA, TolkAviv BFEA, TolkAviv	54) Averics, DollastI 55) Averics, DowerTI 56) Averics, DowerTI 57) Averics, NeuroCity 38) Averics, NeuroCity 39) Averics, NeuroCity 39) Averics, NeuroCity 40) Averics, Sofaulot 42) Averics, Sofaulot 43) Averics, Seatle	 Aneri (av. Vancouver) Aneri (av. Vancouver) Aneri (av. NankingtroßC An	56) AAC, NeuGelbiI 27] AAC, GoedbiI 28] AAC, Soull 39] AAC, Shanghai 40) AAC, Shanghai 10] AAC, Shanghai 10] AAC, Shanghai 10] AAC, Shanghar 10] AAC, Shanghar 40] AAC, TokyaTV 65] Not in the list? Input Manually 66] Outt
Please, select your Secondary Node Nodes marked with (-NRU) may be Not	on 'zscalerthree' Ready for Use. Check http://ips.zsca	lerthree.net			
1) DHEA.Amsterdam 2) DHEA.Amsterdam1 3) DHEA.Consequent 3) DHEA.Consequent 3) DHEA.Consequent 3) DHEA.Consequent 3) DHEA.Consequent 3) DHEA.Fanakfurt1 3) DHEA.Fanakfurt1 3) DHEA.Fanakfurt1 3) DHEA.Fanakfurt1 3) DHEA.Consequent 3) DHEA.Conseq	12) DHEA,LagoSII 13) DHEA,LondonIII 15) DHEA,MancketterI 16) DHEA,MancketterI 16) DHEA,MancketterI 17) DHEA,MislanIII 18) DHEA,MonscowIII 19) DHEA,Monichi 20) DHEA,Monichi 20) DHEA,ApilSII 21) DHEA,PariSII 22) DHEA,PariSII 23) DHEA,PariSII 24) DHEA,PariSII 25) DHEA,PariSII 26) DHEA,PariSII 27) DHEA,PA	23) DHEA,Roueni 24) DHEA,StockholmIII 25) DHEA,Harki 25) DHEA,Harki 27) DHEA,MarsawII 28) DHEA,Tarish 29) Americas,AtlantII 30) Americas,BostonI 31) Americas,Ghicago 1 32) Americas,Ghicago 2 33) Americas,Ghicago 2	34) Americas, DallasII 35) Americas, DenveriII 36) Americas, DenveriII 37) Americas, Notospetes 38) Americas, Nevrol XIII 40) Americas, Nevrol XIII 40) Americas, Samfranciscol 2 42) Americas, Samfranciscol 2 43) Americas, Samfranciscol 2 44) Americas, ForentoIII	45) Americas, Vancouveri 46) Americas, Mushingtomb, 46) Americas, Mushingtomb, 40) Americas, Mushingtomb, 40) Americas, Busingtin 40) Americas, Busingtin 51) Americas, Busingtin 52) Americas, Busingtin 53) Americas, Busingtin 53) Americas, Busingtin 53) Americas, Busingtin 53) Americas, Busingtin 55) Americas, Busingtin 56) Americas, Busingtin 57) Americas, Busingtin 58) Americas, Busingtin 59) Americas, Busingtin 50) Americas, Busing	56) APAC, NewGelhiI 59, PAK, Goakal 59, PAK, Goakal 59, PAK, Sanophai 60) APAC, Shanophai 61) APAC, SingaporelY 62) APAC, Chyapper 63) APAC, Taippei 64) APAC, Taippei 63) Not in the List? Input Manually 65) Outi

Next, you can change VPN credentials and to confirm the values.



9.6.1.2 DNS servers



9.6.1.3 SNMP

The CSC Mux uses Ubuntu Server as its OS and offers all SNMP values of a standard Ubuntu Server. The CSC Mux supports SNMP v2c or v3. No special MIBs are required.

SNMP Traps are not supported. For information about tunnels up/down and other changes, please, use Systems Logs to trigger alarms or events.

9.6.1.3.1 Configure SNMP attributes



9.6.1.3.2 SNMP v2c configuration

SNMP version 2c requires the "read only community" and the IP or Subnet of the SNMP platform.

In this example, our SNMP server has IP: 172.19.0.8/32 and the rocommunity is "public".



9.6.1.3.3 SNMP Networks

The CSC blocks all SNMP request by default. You need to enable the source IPs (or Subnets) that will query the CSC using SNMP. This setting is mandatory for SNMP v2c and v3.



Maidenhead Bridge

Cloud Security Connector Mux for Azure | 70

9.6.1.3.4 SNMP v3 configuration

SNMP attributes and Networks are standard settings of SNMP v2c and SNMP v3. This section will show the specific values required for SNMP v3.

- 1. Security Name (or UserName) : <string>
- 2. Security Level: noAuthNoPriv|authNoPriv|authPriv
- 3. Authentication Passphrase: <string>
- 4. Authentication Protocol: MD5|SHA|SHA-512|SHA-384|SHA-256|SHA-224
- 5. Privacy Passphrase: <string>
- 6. Privacy Protocol: DES | AES





9.6.1.3.5 What can you do with SNMP?

Here some examples of monitoring the CSC Mux via SNMP, using OpenNMS.

9.6.1.3.5.1 Node Information

Open NMS Horizon ²	023-06-03T18:50:59+00:00 💢	٩	Search	2x û
Home / Search / Node				
Node: zs-csc-mux-4-as-d-1 View Events View Alarms View Ou	(≣ 38) (IIII snmpv2) (IIIII 1685660140309) (P Defa utages Asset Info Meta-Data Hardware Info M	ult Availability SSH HT	TPS Resource Graphs	Rescan Admir
SNMP Attributes				
Name	zs-csc-mux-4-as-d-1			
sysObjectID	.1.3.6.1.4.1.8072.3.2.10			
Location	Azure East US			
Contact	support@maidenheadbridge.com			
Description	Zscaler Mux 4 on Azure East			

9.6.1.3.5.2 Node Availability

🐼 Ор	enNMS Horizon	2023-05-03T18:53:31+00:00 🎉		Q Search	2x 1		Search	info • Status	 Reports * 	Dashboards *	Maps * He	lp∗ ≜admin	00 0	0° UI Preview
Home /	Search / Node / Ava	ilability												
Node	e: zs-csc-mu	ıx-4-as-d-1 (ID: 38)												
Availab	iity													
Availabil	ity (last 24 hours)													99.863%
10.2.2.1	5 58 19 28 19 58 20 28	20,58 21,28 21,58 22,28 22,58 28,28 28,58 00,2	18 00,58 03,28 66,58 02,28	02 58 08 28 08 58 04 28 0	HİSƏ OSİZƏ OSİSƏ OBİZƏ	oejsa ozjas ozjas oejas o	ojsa agiza agi	58 2028 2058	11/29 11/59 12	29 1259 1829 1	150 2420 2450	15 28 15 58 16	19 26 58 27 28 :	1758 1828 99.863%
ICM														99.863%
SNN	IP III III III III													99.863%
SSH		(هرهره بعر هر هر هر هر												99.863%
			OpenNINS Committee 0.2	002-2022 The Onephills	Group Inc OpenNMS	a repistered tradem	ark of The On	anNMS Group	Inc Mercian	- 20.0.2				
9.6.1.3.5.3 Node Interfaces (IP & SNMP)

Node Interfaces					
	IP Interfaces		SNM	P Interfaces	
Search/Filter SNMP	Interfaces				Q
SNMP ifIndex \downarrow_z^A	SNMP ifDescr	SNMP ifName	SNMP ifAlias	SNMP ifSpeed	
1	lo	lo	N/A	1000000	
2	eth0	eth0	N/A	N/A	
3	eth1	eth1	N/A	N/A	
4	eth2	eth2	N/A	N/A	
5	eth3	eth3	N/A	N/A	
6	zum1	zum1	N/A	N/A	
8	ztun1a	ztun1a	N/A	1000000000	
10	ztun2a	ztun2a	N/A	1000000000	
12	ztun3a	ztun3a	N/A	1000000000	
14	ztun4a	ztun4a	N/A	1000000000	
First Previous 1	2 Next Last				

9.6.1.3.5.4 Node Statistics (CPU, Memory, etc)





9.6.1.3.5.5 Interfaces Traffic

You can see the traffic per physical interfaces (eth0, eth1), tunnel interfaces (Ztunx), and PriCPA interface (wg0).



Example of real time traffic on PriCPA interface:



9.6.2 Switch Tunnels - Primary / Secondary.

This Wizard allows to Switch Tunnels Primary to Secondary and vice-versa.





9.6.3 High Availability configuration

When deployed as High Availability pair, the CSCs can manage the "Next-Hop" of the route/s configured.

The CSC active will assign its CSC GW IP as the "Next-Hop" of the routes configured. You can configure several routes; there is no limit.

For example, you can control the default route to the internet, 0.0.0/0 or any other destination via the CSCs.

Selection: 16
This Wizard is for High Availability scenarios when changing Next-Hop on Routes via CSC HA Pair.
How to configure:
 'Deployment': Deploy a pair of CSCs with the following conditions: There is connectivity each other via their internal interfaces. (Optional, but Recommended) Deploy the CSCs on Availability Zones or Availability Sets. 'Identity': On each CSC VM (Go to 'Identity -> System Assigned' and 'Turn ON' status. (and Save). (Go to 'Identity -> System Assigned' and click 'Azure role assignments' and add the following Roles:
 3) "Noures" 3.1) Go to Routes (inside the Route Table) and create the Routes that the CSC HA group will control: Route name: <any name="" want="" you=""></any> Routess prefix: <subnet mask=""></subnet> Address prefix: <subnet mask=""></subnet> Examples: 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 (eth1,="" any="" csc="" csc-gw-ip="" first="" ip)="" of=""/> 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. 4.1) Route Table, Resource Group. 4.2) Computer Name and Resource Group of each CSC. 5) This Wizard will create a JSON file. You can use this JSON file to configure the Other CSC in the pair.
How it works:
The CSCs on the HA pair will automatically select the Next-Hop for the Route/s configured.
The HA service in NOT Active
Do you want to configure it?
1) Yes 2) No Enter your choice:

Help provided:

How to configure:

1) 'Deployment': Deploy a pair of CSCs with the following conditions:

- 1.1) There is connectivity each other via their internal interfaces.
- 1.2) (Optional, but Recommended) Deploy the CSCs on Availability Zones or Availability Sets.

2) 'Identity': On each CSC VM

2.1) Go to 'Identity -> System Assigned' and 'Turn ON' status. (and Save).

Maidenhead Bridge

Cloud Security Connector Mux for Azure | 76

Example:

Search	System assigned User assigned
Overview	A system assigned managed identity is restricted to one per resource a
Activity log	managed identity is authenticated with Azure AD, so you don't have to
Access control (IAM)	Save X Discard 🕐 Refresh 🛛 🖗 Got feedback?
Tags	3
Diagnose and solve problems	Status ()
ings	Off On 2
Networking	Object (principal) ID 🔘
Connect	d9c706f5-0805-4bfc-b1e0-fd62d67fb48d
Disks	Permissions ①
Size	Azure role assignments
Microsoft Defender for Cloud	
Advisor recommendations	This resource is registered with Azure Active Directory. The managed
extensions + applications	in failures. <u>Ceant more</u>
wailability + scaling	
Configuration	
comgulation	

Note: Repeat the same step on the other CSC on the HA Pair.

2.2) Go to 'Identity -> System Assigned' and click 'Azure role assignments' and add the following Roles:

- -> Role: Contributor, Resource Group: <CSCs VMs Resource Group/s>
- -> Role: Contributor, Resource Group: <Route Tables Resource Group/s>
- -> Role: Network Contributor, Resource Group: <CSC Subnets (VNET) Resource Group>

Example:

Search System assigned User assigned A cystem assigned A cystem assigned A cystem assigned A cystem assigned A cystem assigned A cystem assigned A cystem assigned A cystem assigned A cystem assigned A cystem assigned B agoose and solve problems Satisping A noncose Connect D bisks D bisks B bisks B bisks B bisks Configuration Microsoft Defender for Cload A dystor nearmediations B bisks h>Sresc-mux-4-as-</th> <th>d-1 Identity ☆ …</th> <th></th> <th></th> <th></th>	Sresc-mux-4-as-	d-1 Identity ☆ …			
○ Overview ▲ Activity log ▲ Activity log ▲ Activity log ▲ Access control (AM) ● Tags Diagnose and solve problems Settings ● Diagnose and solve problems Settings ● Networking ● Connect ● Disks ● Activisor Defender for Cloud ● Activisor Tecommendations ■ Extensions + applications ● Activisor 1 ● Activisor 1 ● Activisor 1 ● Activisor 1 ● Activisor 1 ● Activisor 1 ● Activisor 2 ● Activisor 3 ● Activisor 2 ● Activisor 2 ● Activisor 2 ● Activisor 2 ● Activisor 2 ● Activisor 2 ● Activisor 2 ● Activisor 2 ● Activisor 2 ● Activisor 2 ● Activisor 2 ● Activisor 2 ● Activisor 2 ● Activisor 2 ● Activ	₽ Search	System assigned User assig	ned		
Activity log Imaged identity is authenticated with Azure AD, so you don't have to st Imaged identity is authenticated with Azure AD, so you don't have to st Imaged identity is authenticated with Azure AD, so you don't have to st Imaged identity is authenticated with Azure AD, so you don't have to st Imaged identity is authenticated with Azure AD, so you don't have to st Imaged identity is authenticated with Azure AD, so you don't have to st Imaged identity is authenticated with Azure AD, so you don't have to st Imaged identity is authenticated with Azure AD, so you don't have to st Imaged identity is authenticated with Azure AD, so you don't have to st Imaged identity is authenticated with Azure AD, so you don't have to st Imaged identity is authenticated with Azure AD, so you don't have to st Imaged identity is authenticated with Azure AD, so you don't have to st Imaged identity is authenticated with Azure AD, so you don't have to st Imaged identity is authenticated with Azure AD, so you don't have to st Imaged identity is authenticated with Azure AD, so you don't have to st Imaged identity is authenticated with Azure AD, so you don't have to st Imaged identity is authenticated with Azure AD, so you don't have to st Imaged identity is authenticated with Azure AD, so you don't have to st Imaged identity is authenticated with Azure AD, so you don't have to st Imaged identity is authenticated with Azure AD, so you don't have to st Imaged identity is authenticated with Azure AD, so you don't have to st Imaged identity is authenticated with Azure AD, so you don't have to	👤 Overview	A system assigned managed iden	tity is restricted to one per resource and		
S Access control (IAM) I Tags I Disgnose and solve problems Settings Settings Settings I Networking I Connect Disks Size I Microsoft Defender for Cloud Advisor recommendations E Stemsions + applications Availability + scaling Configuration I Merity I Permissions Compared to the busice to the busi	Activity log	managed identity is authenticated	d with Azure AD, so you don't have to sto		
<pre> Tags Diagnose and solve problems Settings Object (principal) ID discroter to the discroter to the discreter to the discreter to the discreter to the discretere to th</pre>	Access control (IAM)	🔚 Save 🗙 Discard 💍 R	efresh 🛛 🖗 Got feedback?		
Settings Settings Settings Settings Settings Object (principal) ID © ddc20685-0805-4bfc-b180-dd62d5/fb48d Disks Size Nicrosoft Defender for Cloud Advisor recommendations Extensions + applications Configuration Image: Setting and the provide setting and th	🗳 Tags				
Settings © Ketworking © Connect © Disks © Disks © Nicrosoft Defender for Cloud A Advisor recommendations © Extensions + applications © Availability + scaling © Configuration • Advisor recommendations • Mariability + scaling • Configuration • Advisor recommendations to recommendations • Advisor recommendations • Advisor assignments - • Advisor assignments - • Advisor recommendations • Advisor recommendations • Advisor recommendations • Advisor assignments - • Advisor recommendations • Advisor recommendations • Advisor recommendations • Advisor recommendations • Advisor scaling and the provide to the	Diagnose and solve problems	Status 🕕			
Image: Networking Object (principal) ID O Image: Object (principal)	Settings	Off On			
Image: Connect Disks Size Microsoft Defender for Cloud Advisor recommendations Extensions + applications Availability + scaling Configuration Image: Conf	2 Networking	Object (principal) ID 💿			
Permissions ① 2 Size ② Microsoft Defender for Cloud ④ Advisor recommendations ③ Extensions + applications ③ Availability + scaling ③ Configuration ③ Identity 1	Ø Connect	d9c706f5-0805-4bfc-b1e0-fd62	d67fb48d 🗅		
Size Microsoft Defender for Cloud Advisor recommendations Extensions + applications Availability + scaling Configuration Identity Configuration Identity Active role assignments Active operations Recurse New Comparison Recurse Type Asigned To Contiduate Recurse Type Asigned To Contiduate Contiduate Contiduate Recurse Type Recurse Type Asigned To Contiduate Contiduate Recurse Group Science4-ad-11 Nore 	a Disks	Permissions ①			
Microsoft Defender for Cloud Advisor recommendations Extensions + applications Availability + scaling Configuration Image: Status Image: Status Aurile close assignments Image: Status Image:	📮 Size	Azure role assignments	2		
Advisor recommendations Extensions + applications Availability + scaling Configuration Image: Configuration <th>Ø Microsoft Defender for Cloud</th> <th></th> <th>•</th> <th></th> <th></th>	Ø Microsoft Defender for Cloud		•		
Image: Statestions + applications Image: Availability + scaling Image: Configuration Image: Statestion - Image: Sta	Advisor recommendations	This resource is registered w	ith Azure Active Directory. The managed ide		
Navailability + scaling Configuration lentity 1 Hore > Acure role assignments Hole Solution to read, they won't be shown in the list. Learn more Subscription* Hole Solution to read, they won't be shown in the list. Learn more Subscription* Main Note Role Role Resource Name Resource Type Assigned To Contributor Image: Contributor	Extensions + applications				
i configuration i dentity Home > Acture role assignments in the second assignments in the second assignment (Proview) i Refree If this dentify has role assignment bat you don't have permission to read, they won't be shown in the list. Learn more Subscription * MBE Role Resource Name Resource Type Assigned To Contributor iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	Availability + scaling				
Image: Second Secon	💼 Configuration				
Home > Azure role assignments ···· + Add role assignment (Preview) C Refresh If this identity has role assignments that you don't have permission to read, they won't be shown in the list. Learn more Subscription * MHB Role Resource Name Resource Type Asigned To Condition Contributor Condition Resource Group zs-csc-mux-4-as-d-1 None Network Contributor Resource Group zs-csc-mux-4-as-d-1 None	🐒 Identity 🛛 1				
Azure role assignments ··· 4 Add role assignment (Preview) C Refresh If this identity has role assignments that you don't have permission to read, they won't be shown in the list. Learn more Subscription * MIRE Mole Resource Name Resoure Type Asigned To Condition Contributor Condition Resource Group zs-csc-mux-4-as-d-1 None Network Contributor Resource Group zs-csc-mux-4-as-d-1 None					
Add role assignment (Preview) Referesh If this identify has role assignments that you don't have permission to read, they won't be shown in the list. Learn more Subscription * MIB Role Resource Name Assigned To Condition Contributor © CSC-East-US Resource Group zs-csc-mux-4-as-d-1 None Contributor @ RouteFables-East-US Resource Group zs-csc-mux-4-as-d-1 None Network Contributor @ Networks-East-US Resource Group zs-csc-mux-4-as-d-1 None	Azure role assignments				
If this identity has role assignments that you don't have permission to read, they won't be shown in the list. Learn more Subscription * MHB Resource Name Resource Type Asigned To Condition Contributor © CSC-East-US Resource Group zs-csc-mux-4-as-d-1 None Contributor @ RouteFables-East-US Resource Group zs-csc-mux-4-as-d-1 None Network Contributor @ Networks-East-US Resource Group zs-csc-mux-4-as-d-1 None	+ Add role assignment (Preview) 🕐 Refresh				
Subscription * MHB Condition Role Resource Name Resource Type Asigned To Condition Contributor © CSC-East-US Resource Group zs-csc-mux-4-as-d-1 None Network Contributor @ Networks-East-US Resource Group zs-csc-mux-4-as-d-1 None	If this identity has role assignments that you don't have permissi	on to read, they won't be shown in the list. Learn more			
Role Resource Type Assigned To Condition Contributor © CSC-East-US Resource Group zs-csc-mux-4-as-d-1 None Contributor @ RouteTables-East-US Resource Group zs-csc-mux-4-as-d-1 None Network Contributor @ Networks-East-US Resource Group zs-csc-mux-4-as-d-1 None	Subscription *	~			
Contributor © CC-East-US Resource Group zs-csc-mux-4-as-d-1 None Contributor @ RouteTables-East-US Resource Group zs-csc-mux-4-as-d-1 None Network Contributor @ Networks-East-US Resource Group zs-csc-mux-4-as-d-1 None	Role	Resource Name	Resource Type	Assigned To	Condition
Contributor Resource Group zs-csc-mux-4-as-d-1 None Networks-Contributor Networks-East-US Resource Group zs-csc-mux-4-as-d-1 None	Contributor	CSC-East-US	Resource Group	zs-csc-mux-4-as-d-1	None
Network Contributor 😥 Networks-East-US Resource Group zs-csc-mux-4-as-d-1 None	Contributor	RouteTables-East-US	Resource Group	zs-csc-mux-4-as-d-1	None
	Network Contributor	Networks-East-US	Resource Group	zs-csc-mux-4-as-d-1	None

Note: Repeat the same step on the other CSC on the HA Pair.

3) 'Routes'

3.1) Go to Routes (inside the Route Table) and create the Routes that the CSC HA group will control:

- -> Route name: <any name you want>
- -> Address prefix: <Subnet/Mask>

Examples: 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 CSC-GW-IP (eth1, first IP) of any CSC>

Example:

Servers-Route-Table	e ☆ ☆ …									
Route table	Route Table N	lame								
₽ Search «	$ ightarrow$ Move \lor 📋 Dele	te 🖒 Refresh 🕂	Give	feedback						
🔁 Overview	∧ Essentials									
Activity log	Resource group (move)	RouteTables-East-US	F	Route Table Resource Group		Associations	: 7 subnet associations			
Access control (IAM)	Location :	East US								
🗳 Tags	Subscription (move) :	MHB								
Diagnose and solve problems	Subscription ID :	ffde02fb-c38f-45fb-9e31-	-89e5	5303be5f1						
	Tags (<u>edit</u>) :	Click here to add tags								
Settings	Routes									
Configuration	$\mathcal P$ Search routes									
🔽 Routes	Name	Ŷ	ĻΨ	Address prefix	\uparrow_{\downarrow}	Next hop type		\uparrow_{\downarrow}	Next hop IP a	ddress
Subnets	Local-VNET			10.2.0.0/16		Virtual network			-	
Properties Route Name	Server-default-route			0.0.0.0/0		Virtual appliance			10.2.2.15	1
🔒 Locks	Zscaler-Global-GW			185.46.212.88/32		Virtual appliance			10.2.2.15	
Monitoring	Subnets	_						CS	C GW IP	1
🛤 Alerts	✓ Search subnets									
Automation	Name	ŕ	,†	Address range	\uparrow_{\downarrow}	Virtual network		\uparrow_{\downarrow}	Security group	р
🖧 Tasks (preview)	fw-internal			10.2.9.0/24		VNET-East-US			-	
😨 Export template	servers-East-US			10.2.3.0/24		VNET-East-US			-	
Support + troubleshooting	wvd1-East-US			10.2.4.0/24		VNET-East-US	Subnets Assoc	ciate	ed	
Effective routes	wvd2-East-US			10.2.5.0/24		VNET-East-US			-	
New Support Request	wvd4-East-US			10.2.7.0/24		VNET-East-US			-	
A new support nequest	wvd3-East-US			10.2.6.0/24		VNET-East-US			-	
	csc-internal-East-US			10.2.2.0/24		VNET-East-US			-	
L										

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.

Example:

First CSC on the HA Pair – Manual Configuration:



5) This Wizard will create a JSON file. You can use this JSON file to configure the Other CSC in the pair.



Example:

Second CSC on the HA Pair – (paste) JSON Configuration:



How it works:

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

Check HA using Show Configuration and Status:



Note: The HA wizard automatically selects the Floating IP for Private Access.

Logs generated by High Availability:

may	31	22:42:45	root: ((MHB-CSC)(INFO)	High Availability	JSON FILE (highAvailability.json) integrity is ok
May	31	22:42:51	root: ((MHB-CSC)(INFO)	High Availability:	IAM Identity in use: SystemAssigned
May	31	22:43:01	root: ((MHB-CSC)(INFO)	High Availability:	Route Server-default-route (Route Table=Servers-Route-Table, Resource Group=RouteTables-East-US) configured
May	31	22:43:01	root: ((MHB-CSC)(INFO)	High Availability:	Route Zscaler-Global-GW (Route Table=Servers-Route-Table, Resource Group=RouteTables-East-US) configured.
May	31	22:43:01	root: ((MHB-CSC)(INFO)	High Availability	is active (running) since Wed 2023-05-31 22:43:01 UTC; 14ms ago.
May	31	22.11.11	cecadmi	in: (MHR.CSC)(T	NEO) Route to Zecal	er using Next Hope 10 2 2 15 of CSC, zs-csc-mux-4-as-d-1

10 Traffic Forwarding to Zscaler ZIA with the CSC Mux for Azure.

In Chapter 3 of this Administrator Guide, we showed the Network Diagrams of different scenarios of traffic forwarding.

When connecting Virtual Machines, Virtual Desktops, etc., to Zscaler using the CSC Mux, you have two options for traffic forwarding: routing and proxying.

The options are not mutually exclusive. You can use both at the same time. Moreover, when the CSC Mux is on a HA pair, you can use both simultaneously, duplicating the capacity for Web Traffic.

In both cases, it is possible to bypass traffic from the tunnel to Zscaler and send it directly via a dedicated Public IP, using the "routed" and "proxied" bypass functionalities.

As shown in a previous chapter, the CSC offers multiple options for traffic forwarding:



The function of each internal IP is the following:

IP	Туре	Function
CSC GW	Gateway	Used as Gateway for traffic to Zscaler and bypasses using "Routed Bypass" (Layer 4) functionality.
CSC Vip Proxy	Proxy	Used as Proxy for traffic to Zscaler.
CSC Proxy Bypass	Proxy	User as Proxy for bypasses using "Proxy Bypass" (Layer 7) functionality.

This chapter will dig into more detail about the configuration required, showing examples when the CSC Mux is on High Availability as HA Pair and when using Azure Load Balancer.

10.1 CSC Mux in HA Pair

10.1.1 Network Diagram



10.1.2 Prerequisites

- 1. Deploy 2 x CSC Mux as HA Pair. (See section "9.6.3 High Availability configuration")
- 2. Create the Routed Bypasses. (See section "9.4 Routed Bypass")
- 3. Obtain the VIP Proxy and Bypass Proxy of each CSC running "Show Configuration and Status" from SSH console or AWS Systems Manager.
- 4. Created the Proxy Bypasses. (See section "9.3 Proxy Bypass")

10.1.3 Real Case Scenario: Routing, Explicit Proxy and PAC files.

Suppose a customer with the following requirements:

• Case 1): Send all ports and protocols to Zscaler and reach Trusted Sites using your Public IP (Routed Bypass - Layer 4).

- Case 2): To provide redundancy to servers that do not support PAC files. Only Explicit Proxy (Single IP) can be configured and reach Trusted Sites using your Public IP (Routed Bypass).
- Case 3): To provide the maximum bandwidth available to Virtual Desktops (or any device that can use PAC file) using both CSC simultaneously for Web Traffic and reach Trusted Sites using your Public IP. (Routed Bypass Layer 4 or Proxy Bypass Layer 7).

10.1.3.1 Routing and Explicit proxy: Solving Case 1 and 2

To solve requirements 1) and 2), the CSC Mux on HA pair will manage the Routes on the Routing Tables to select the best exit to Zscaler.

In the case of 1) the CSC Mux Hair Par will control de default routes Next-Hop to Zscaler for the server farm.

Default Route to Internet $\rightarrow 0.0.0.0/0$

All traffic to Zscaler:

Routes				
Name	\uparrow_{\downarrow}	Address prefix	\uparrow_{\downarrow}	Next hop
CSC-Zscaler-Default		0.0.0.0/0		172.31.200.17

In the case of 2), we are going to use the Zscaler Global Proxy IP as Explicit Proxy on the servers.

You can use any of this values:

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.

The CSC Mux HA pair will control this routes to Zscaler Global ZEN IP address.

To Zscaler Global ZENs:

Routes				
Name	\uparrow_{\downarrow}	Address prefix	\uparrow_{\downarrow}	Next hop
server-farm-1		185.46.212.88/32		172.31.200.17

The CSC on the HA Pair will manage the Next Hop this this Address Prefix: 185.46.212.88/32

IMPORTANT: The Next-Hop IP is the CSC GW IP.

10.1.3.2 Case 1, 2 and 3: Routed Bypasses - Layer 4

Routed Bypasses works in a similar way to an outbound Azure Security Group. You can create rules per Source IP, Destination IP, Protocol (UDP / TCP) and destination port.

The configuration file for Routed Bypasses is a JSON file with the following format:

{	
"rou	itedBypassRules": [
ı	"description": "O365 Login URLs 1", "ipProtocol": "tcp", "sourceCirdlp": "0.0.0/0", "destinationCirdlp": "20.190.128.0/18", "fromPort": "80", "toPort": "80"
},	
1	"description": "O365 Login URLs 2", "ipProtocol": "tcp", "sourceCirdlp": "0.0.0.0/0", "destinationCirdlp": "20.190.128.0/18", "fromPort": "443", "toPort": "443"
}, {	
t	"description": "O365 Login URLs 3", "ipProtocol": "tcp", "sourceCirdlp": "0.0.0./0", "destinationCirdlp": "40.126.0.0/18", "fromPort": "80", "toPort": "80"
}, ,	
ı	"description": "portquiz.net", "ipProtocol": "tcp", "sourceCirdIp": "0.0.0/0", "destinationCirdIp": "52.47.209.216/32", "fromPort": "80", "toPort": "80"
},	
ĩ	"description": "O365 Login URLs 4", "ipProtocol": "tcp", "sourceCirdIp": "0.0.0/0", "destinationCirdIp": "40.126.0.0/18", "fromPort": "443", "toPort": "443"
}, {	
ι	"description": "Skype and Teams UDP 1", "ipProtocol": "udp", "sourceCirdlp": "0.0.0.0/0", "destinationCirdlp": "13.107.64.0/18", "fromPort": "3478", "toPort": "3481"
},	
ı	"description": "Skype and Teams UDP 2", "ipProtocol": "udp", "sourceCirdIp": "0.0.0/0", "destinationCirdIp": "52.112.0.0/14", "fromPort": "3478", "toPort": "3481"
}, {	
ĩ	"description": "Skype and Teams UDP 3", "ipProtocol": "udp", "sourceCirdIp": "0.0.0.0/0", "destinationCirdIp": "52.120.0.0/14", "fromPort": "3478", "toPort": "3481"
}	

To configure Routed Bypasses on the CSC, you paste the JSON file directly via the SSH console or configure an URL from where the CSC can retrieve the JSON file. You can create an object on a Blob container and configure the URL of the object on the CSC.

Routed Bypasses for Case 1 - Sending all ports and protocols via the CSC GW.

The rules of Routed Bypass will inspect any traffic routed by the CSC GW IP. You can bypass any TCP or UDP traffic from Zscaler, for example, O365 Authentication URLs for Conditional Access rules and MFA, and Skype UDP real-time traffic. In this case, there is nothing to configure on the internal devices.

Routed Bypasses for Case 2 - Servers with Explicit Proxy

In this case, the traffic sent via the Routed Bypass is configured on "Exceptions" (Windows) or "no proxy" (Linux). Here is an example for each one.

Windows:



Linux (Ubuntu):

Dynamic setting:

export http_proxy="http://185.46.212.88:9400" export ftp_proxy="http://185.46.212.88:9400" export https_proxy="http://185.46.212.88:9400" export no_proxy=localhost,127.0.0.0/8,10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,*.local, login.microsoftonline.com, login.microsoft.com, login.windows.net

Maidenhead Bridge

Cloud Security Connector Mux for Azure | 87

Remove Dynamic Settings:

unset ftp_proxy unset https_proxy unset no_proxy	unset http_proxy		
unset https_proxy unset no_proxy	unset ftp_proxy		
unset no_proxy	unset https_proxy		
	unset no_proxy		

Make settings permanent:

sudo nano /etc/environment

http_proxy="http://185.46.212.88:9400" ftp_proxy="http://185.46.212.88:9400" https_proxy="http://185.46.212.88:9400" no_proxy=localhost,127.0.0.0/8,10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,*.local,login.microsoftonline.com,login.mic rosoft.com,login.windows.net

Routed Bypasses for Case 3 - Devices with PAC files.

In this case, you need to create a section on the PAC file to send "DIRECT" the traffic via the Routed Bypass.

For example:

In the following section, we are talking about all options when using PAC files.

10.1.3.3 PAC files: Solving requirements Case 3

In Case 3, the Virtual Desktops support PAC files. Due to both CSCs on the HA pair being active simultaneously, we can duplicate the bandwidth to Zscaler, achieving maximum throughput. In addition, using the Bypass functionality of the CSCs, it is possible to reach Trusted Sites via your Public IP and not Zscaler's IPs.

The CSC allows "Routed Bypasses" (Layer 4) and "Proxy Bypasses" (Layer 7).

As shown in previous pictures, the CSC has 3 Internal IPs:

CSC GW IP	Default Gateway for Routed traffic - On the PAC file, anything with "return DIRECT" will travel via this GW.
CSC VIP Proxy	Proxy to Zscaler.
CSC Bypass Proxy	Proxy for "Proxy Bypass" traffic.

PAC File for Virtual Desktops:

The following PAC file shows how to achieve 6.4 Gbps using the CSC Mux 3.2 Gbps as HA pair.

```
function FindProxyForURL(url, host) {
 // Section 1: Zscaler standard PAC values
 var privatelP = /(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: Routed Bypass: Destination IPs / Networks going "DIRECT"
 // Routed Bypass for O365 Login destinations: 20.190.128.0/18 and 40.126.0.0/18
 if ((isInNet(host, "20.190.128.0", "255.255.192.0") ||
   isInNet(host, "40.126.0.0", "255.255.192.0"))) {
 return "DIRECT";
 }
 // Section 3: Load Balancing: 2 x CSC Mux
 // Get NIC IP address
 niclp = mylpAddress();
 // 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(niclp, "0.0.0.1", "0.0.0.1")) {
   var tozscaler = "PROXY csc2vip:80; PROXY csc1vip:80";
   var bypass = "PROXY csc2bypass:3128; PROXY csc1bypass:3128";
```

Maidenhead Bridge

Cloud Security Connector Mux for Azure | 89



·	
Section 1:	Zscaler Standard PAC values to: Do not send Private IPs to Zscaler or ZPA or FTP traffic.
Section 2:	Shows Destinations IP / Networks sent DIRECT that you want to reach using your Public IP using Routed Bypasses. (L4)
Section 3:	Section 2 does the load balancing between both CSC on the HA pair. As you can see, we are reading the source IP of the VDI (nicIp = myIpAddress();), and we are load balancing by odd/even IP, using different primary/secondary cscvip and cscbypass for odd/even IPs.
Section 4:	Section 4 shows examples of URLs to bypass from Zscaler to reach the destination website with your Public IP. Examples of required URLs for OKTA (for Location rules) and O365 (for Conditional Access) are shown. One common use of these examples is not asking for MFA (Multi-factor Authentication) for VDIs.
Section 5:	Default traffic will go via Zscaler.

Sections Explained:

Proxy Bypass: PAC file for the CSCs

function FindProxyForURL(url, host) { // This value of bypass on the PAC file for the CSC can be any. // We need to assigned a value just to pass the "Validation" of the PAC on Zscaler console. var bypass = "PROXY 1.1.1.1:3128; PROXY 2.2.2.2:3128"; // Section 3: Bypass via Cloud Security Connectors // Bypass via CSC Public IPs (Examples) // Okta Domains (for Location Rules) if ((shExpMatch(host, "*.okta.com")) || (shExpMatch(host, "*.oktacdn.com")) || (shExpMatch(host, "*.okta-emea.com")) || // Trusted Sites (shExpMatch(host, "trusted.domain.com")) || (shExpMatch(host, "trusted2.domain.com")) || (shExpMatch(host, "*.trusted-domain.com")) || // O365 Domains for ConditionalAccess (shExpMatch(host, "login.microsoftonline.com")) || (shExpMatch(host, "login.microsoft.com")) || (shExpMatch(host, "login.windows.net")) || // IP / Port test page (shExpMatch(host, "ip.maidenheadbridge.com"))) { return bypass; } return bypass

Maidenhead Bridge

}

10.2 CSC Mux in HA with Azure Load Balancer

The CSC Mux can be balanced using Azure Load Balancer. In this chapter, we will present how to use the Azure Load Balancer's Front End IPs as a Proxy for traffic to Zscaler and Proxy Bypass.



10.2.1 Network Diagram

10.2.2 Azure Load Balancer configuration

10.2.2.1 Create a Standard Load Balancer

	Microsoft Azure			and docs (G+/)				Σ	Ģ		÷	୭ ନି	ti DEF#
Hom	> Load balancing												
	Load balancing Loa	ad Balancer 🛷 …											
₽ s	earch «	+ Create 🛛 Manage view 🗸 💍 Ref	resh 🞍 Export to CSV 😤 Op	pen query 🛛 🖉 Assign tags									
🔋 c	verview	Filter for any field Subscriptio	n equals all (from active filter)	Resource group equals all $ imes$	Location equals all $ imes$	+ Add filter							
Load	Balancing Services	Showing 1 to 1 of 1 records.							Ē	No group	ping		\sim
🚸 A	pplication Gateway	□ Name ↑		Reso	urce group 1		Location 1		_	S	ubscript	ion_↑∟	
🔷 F	ront Door and CDN profiles				ance group		5						
🔶 U	oad Balancer	🔲 👽 ib-csc-mux		CSC-	East-US		East US			N	инв		
🔞 т	raffic Manager												

10.2.2.2 Front End IP Configuration

The first task is to create the Front End IP. In this example, we will create two: One for traffic "to Zscaler" and another for "Proxy Bypasses".

IMPORTANT: The Front End IPs must be located in the Internal Subnet of the CSC.

≡ Microsoft Azure		\mathcal{P} Search resources, services, and docs (G-	+/)
Home > Ib-csc-mux ib-csc-mux Fronter Load balancer	nd IP configuration \star …		
Search	+ Add 🕐 Refresh 🖗 Give feedback		
Access control (IAM) Tags Disappee and solve problems	Name TU csc-vip-front-end-ip csc-bypass-front-end		10.2.2.13 10.2.2.14
Settings 1	2		
Backend pools Health probes Load balancing rules			

10.2.2.3 Backend pools

Create a Backend with the CSC VIPs and another with the CSC Bypass Proxy IPs.

			ces, and docs (G+/)		
Home > Ib-csc-mux ib-csc-mux Backen Load balancer	nd pools 😤 …				
	+ Add 🕐 Refresh 🔗 Give fee	dback			
Overview					
Activity log	Group by Backend pool 🗸 🔎	7	7 Add filter		
Access control (IAM)					
Tags	✓ Backend pool	Resource Name	Resource Status	IP address	Network interface
Diagnose and solve problems					
Settings	 v csc-bypass-pool (2) 			Ву	pass Proxy IPs
Frontend IP configuration	csc-bypass-pool	zs-csc-mux-4-as-d-1	Running	10.2.2.17	zs-csc-mux-4-as-d-eth1-1
Backend pools	csc-bypass-pool	zs-csc-mux-4-as-d-2	Running	10.2.2.20	zs-csc-mux-4-as-d-eth1-2
Health probes Load balancing rules	 csc-pool-vip (2) 				
Inbound NAT rules	csc-pool-vip	zs-csc-mux-4-as-d-1	Running	10.2.2.16 C	sc VIP IPs zs-csc-mux-4-as-d-eth1-1
Properties Locks	csc-pool-vip	zs-csc-mux-4-as-d-2	Running	10.2.2.19	zs-csc-mux-4-as-d-eth1-2

10.2.2.4 Health Probes

You need to create a Health Probe for the CSC VIPs and another for the Proxy Bypasses.

- CSC VIP Health Probe: TCP / 59400
- CSC Proxy Bypass Health Probe: TCP / 53128

IMPORTANT: Health Probe TCP ports are for probe test purposes only. These ports cannot be used as proxy ports. Both Health probes stop answering when the Zscaler tunnels are down.

=	Microsoft Azure					 D. (ş 🖉
Home	e > Ib-csc-mux						
P	Ib-csc-mux Health	probes 🛪 …					
₽ Si	earch «	+ Add () Refresh 🖗 Give feedback					
0	verview						
a	ctivity log	Type to start filtering					
⁸ R A	ccess control (IAM)	,					
🔶 Ta	ags	Name	Protocol	Port	Path	User	d By
PD	iagnose and solve problems			-			
Settin	gs	hp-bypass	Тср	53128	•	lb-c	sc-bypass
E Fr	rontend IP configuration	hp-csc-vip	Тср	59400		lb-c	sc-vip
S Bi	ackend pools	L					
Ф. Н	lealth probes						

10.2.2.5 Load Balancing rules

On the Load Balancing rules you need to associate the Front End, Health Probes, Backend Pools and to define the Port to use. In this case, you need to create two Load Balance Rules, one for the CSC VIP and another for the Proxy Bypass. The TCP ports allowed are:

- To Zscaler: You can use TCP 80, 9400, 9480, 443 and 8080.
- Bypass Proxy: You can use TCP 3128

≡ Microsoft Azure	<u>۶</u>	Search resources, services, and docs (G+/)		
Home > Ib-csc-mux				
Similar State	alancing rules \star …			
	🕂 Add 💍 Refresh 🛛 Refresh			
Overview				
Activity log	P Filter by name			
Access control (IAM)	Name	Load balancing rule	Backand nool	Health probe
🗳 Tags		Loud building fac	buckenta poor	neural probe
Diagnose and solve problems	lb-csc-bypass	lb-csc-bypass (TCP/3128)	csc-bypass-pool	hp-bypass
Settings	lb-csc-vip	lb-csc-vip (TCP/80)	csc-pool-vip	hp-csc-vip
Frontend IP configuration	· · · · · · · · · · · · · · · · · · ·	• • •	• •	
Backend pools	L			
Health probes				
š≡ Load balancing rules				

IMPORTANT: Use Session Persistence "Client IP and Protocol"

Test using CURL command:

ubuntu-ds-01@ubuntu-ds-01:~\$ curl -k --proxy http://10.2.2.13:80 https://ip.maidenheadbridge.com 20.163.185.99, 136.226.68.254 via Zscaler ubuntu-ds-01@ubuntu-ds-01:~\$ curl -k --proxy http://10.2.2.14:3128 https://ip.maidenheadbridge.com 74.235.173.101 via Proxy Bypass

10.2.2.5.1 Load Balancing Rule for CSC VIP in detail.

≡ Microsoft Azure	Search resources, services, and do
Home > Ib-csc-mux Load bala	ncing rules >
lb-csc-vip	
lb-csc-mux	
A load balancing rule distributes in backend pool instances. Only backe	coming traffic that is sent to a selected IP address and port combination across a group of and instances that the health probe considers healthy receive new traffic.
Name *	lb-csc-vip
IP Version *	IPv4
Frontend IP address * 🛈	csc-vip-front-end-ip (10.2.2.13)
Backend pool * 🕡	csc-pool-vip 🗸
High availability ports 🛈	
Protocol	• тср
Port *	80
Backend port * 🛈	80
Health probe * 🛈	hp-csc-vip (TCP:59400)
	Create new
Session persistence (i)	
Idle timeout (minutes) * 🕞	4
Enable TCP Reset	
Enable Floating IP 🛈	

10.2.2.5.2 Load Balancing Rule for Proxy Bypass in detail.

	> Search resources, services, and
Home > Ib-csc-mux Load balancing ru	les >
Ib-csc-bypass	
A load balancing rule distributes incoming t backend pool instances. Only backend insta	traffic that is sent to a selected IP address and port combination across a group of inces that the health probe considers healthy receive new traffic.
Name *	lb-csc-bypass
IP Version *	IPv4
	O IPv6
Frontend IP address * 🛈	csc-bypass-front-end (10.2.2.14)
Backend pool * 🕢	csc-bypass-pool
High availability ports 🛈	
Protocol	• ТСР
	OUDP
Port *	3128
Backend port * 🕡	3128
Health probe * 🛈	hp-bypass (TCP:53128)
	Create new
Session persistence ()	Client IP and protocol
Idle timeout (minutes) * 🗊	4
Enable TCP Reset	
Enable Floating IP 🛈	

10.3 Testing traffic to Zscaler

10.3.1 ip.zscaler.com

The page ip.zscaler.com shows the Location values.

Using the browser:

Connection Quality Zscaler Analyzer Cloud Health Security Research

You are accessing the Internet via Zscaler Cloud: Washington DC in the zscalerthree.net cloud.

Your request is arriving at this server from the IP address 136.226.68.254

The Zscaler proxy virtual IP is 136.226.68.35.

The Zscaler hostname for this proxy appears to be zs3-was1-6b5-sme.

The request is being received by the Zscaler Proxy from the IP address 20.163.185.99

Your Gateway IP Address is 20.163.185.99

Using curl command from CMD or Terminal

Proxy environment:

Command	Windows: curl -sproxy http:// <csc vip=""></csc> :80 ip.zscaler.com findstr "You" Linux: curl -sproxy http:// <csc vip=""></csc> :80 ip.zscaler.com grep "You"
Expected Result	ubuntu-ds-01@ubuntu-ds-01:-\$[curl -\$oroxv http://10.2.2.13:80 ip.zscaler.com oreo "You" <div accessing="" are="" class="headline" cloud.<="" cloud:="" dc="" div="" in="" internet="" the="" via="" washington="" you="" zscaler="" zscalerthree.net=""> <div class="details" style="margin-top: 20px">Your request is arriving at this server from the IP address 136.226.68.254</div> <div \$your="" <span="" address="" class="detail0utput" gateway="" ip="" is="">20px">Your Gateway IP Address is 136.226.68.254</div></div>

Routed environment:

Command	Windows: curl -s ip.zscaler.com findstr "You" Linux: curl -s ip.zscaler.com grep "You"
Expected Result	ubuntu-ds-D1@ubuntu-ds-01:-\$ curl -s ip.zscaler.com grep "You" <div class="headline">You are accessing the Internet via Zscaler Cloud: Washington DC in the zscalerthree.net cloud.</div> <div class="headline">You are accessing the Internet via Zscaler Cloud: Washington DC in the zscalerthree.net cloud.</div> <div class="details">You for accessing the Internet via Zscaler Cloud: Washington DC in the zscalerthree.net cloud.</div> <div class="details">Your Gateway IP Address is 20: 103: 185.99</div>

10.3.2 https://ip.maidenheadbridge.com

Maidenhead Bridge provides a HTTPS page to check the IP.

Using the Browser:



20.163.185.99, 136.226.68.254

Using curl command from CMD or Terminal

(Note: the switch "-k" on curl command is to avoid SSL certificate validation)

Proxy environment:

Command	curl -kproxy http:// <csc vip=""></csc> :80 https://ip.maidenheadbridge.com
Expected Result	ubuntu-ds-01@ubuntu-ds-01:~\$ curl -s -kproxy http://10.2.2.13:80 https://ip.maidenheadbridge.com 20.163.185.99, 136.226.68.254

Routed environment:

Command	curl -k https://ip.maidenheadbridge.com
Expected Result	ubuntu-ds-01@ubuntu-ds-01:~\$ curl -s -k https://ip.maidenheadbridge.com 20.163.185.99, 136.226.69.5

10.3.3 SpeedTest

The CSC contains the SpeedTest client. You can run it from the SSH console or using any Management tool (AWS Systems Manager, Rundeck, , Ansible, etc.)



This test is experimental because we use third-party tools (speedtest.net), but it works fine in most cases. Here the result using a CSC Mux 4.



Note: At the moment of writing this documentation, Zscaler provides 400 Mbps per IPsec tunnel. The CSC Mux 4 can aggregate 4 x IPsec tunnels (~ 1.6 Gbps total).

11 Private Cloud Private Access

11.1 What is Private Cloud Private Access (PriCPA)?

Private Cloud Private Access (PriCPA) is a new functionality of the Cloud Security Connector. PriCPA allows you to create a Private Cloud among all CSCs for private traffic. In a matter of minutes, you can build a full mesh encrypted topology between your locations for private traffic with Zero Trust. After making the Private Cloud, you can set up your policies to define who will talk with who inside your Private Cloud.

11.2 PriCPA Network Diagrams

11.2.1 High Level Network Diagram



11.2.2 Low Level Network Diagram – PriCPA only

The following network diagram shows the IP addressing for PriCPA.



Steps to design your Private Cloud:

- 1. Select a Subnet for your Private Cloud. The example above is 192.168.7.0/24. Due to the Subnet is /24, up to 255 CSCs can participate in this Private Cloud.
- 2. Assign a Cloud Private IP to each CSC. In this example, we are assigning 192.168.7.1 to 192.168.7.4
- 3. The Public IP to be used will be the same assigned to the Bypass of each CSC. You can choose the UDP port to use at each location. For simplicity, it is recommended to use the same port at all locations.
- 4. Gather the information of the private Subnets behind each CSC. This information will be required when configuring the Peers.
- Firewall Rules (or Security Groups Rules): The CSC for Azure, AWS and Gcloud will implement the firewall rules automatically. Manual FW rules are required when the CSC is "On-Premises". The CSC provides a JSON file with the rules required.

11.3 Configuring PriCPA

The Main Menu has a section for Private Access:

```
Private Cloud Private Access (PriCPA)
17) Show Configuration and Status PriCPA.
18) Configure PriCPA (Local and Peers Configuration).
19) Configure CSC Remote Management via PriCPA.
```

The configuration of PriCPA is four simple steps:

Selection: 18
Private Access Configuration Wizard
Steps to configure Private Access:
 A) Assign 'Identity' to the VM: A.1) Go to 'Identity -> System Assigned' and 'Turn ON' status. (and Save). A.2) Go to 'Identity -> System Assigned' and click 'Azure role assignments' and add the following Roles: -> Role: Contributor, Resource Group: <cscs group="" resource="" s="" vms=""></cscs> -> Role: Contributor, Resource Group: <route group="" resource="" s="" tables=""> (optional, but required for HA)</route> -> Role: Network Contributor, Resource Group: <csc (vnet)="" group="" resource="" subnets=""></csc> B) Create Private Access Local Configuration. (This selection also allows to change Local Configuration) C) (optional, if HA is enabled.) Copy Local Configuration to the other CSC in the HA pair. D) Load Private Access Peers JSON configuration file.
 Create (or change) Private Access Local Configuration Load Private Access Peers JSON configuration file Quit Enter your choice:

- 1. Assign "Identity" to the CSC (and to the "other CSC" if HA is enabled).
- Create the Local Node configuration. This step will initialize and enable Private Access on the Node. The result of this operation will show a "Token" and "Private Access Local JSON file".
- 3. (HA Pair only) Initialize the second Node of the HA pair using the "Token" and "Private Access Local JSON file".
- 4. Create and distribute the Private Access Peers JSON file to all nodes.

IMPORTANT: We strongly recommend using software with a JSON formatter to create the Peers JSON file, like Visual Code or Notepad ++ . See Appendix C for more detail about how to install these programs and the plugins required.

11.3.1 Create the Local configuration (First node of the HA pair or Single deployment)

11.3.1.1 Using configUserData.json file

You can pass the Local configuration parameters via configUserData.json file during the initial deployment.

Here an example:



The CSC will read this information and create the Local configuration on the First node of the HA deployment or when it is a single deployment. As a result, the Local Configuration for PriCPA will be ready:



Maidenhead Bridge

Cloud Security Connector Mux for Azure | 102

11.3.1.2 Manual Configuration

→ From Main Menu, select "18) Configure Private Access."

→ Select "1) Create (or change) Private Access Local Configuration"



 \rightarrow Select "1) Manual Configuration" and input the values requested.



Maidenhead Bridge

Cloud Security Connector Mux for Azure | 103

Apply values



IMPORTANT: The "Token" and "Private Access Local Config JSON file" will be used to create the local configuration on the second node of the HA pair. Please, keep these values in a safe place. You can use these values to reconfigure any node of the HA Pair if necessary in the future. For example, if you want to change the IPs or descriptions.

11.3.2 Create the Local configuration (second node of HA Pair)

SSH the second node of the HA Pair and input the "Token" and "Private Access Local Config JSON file".

Go to 18) Configure Private Access. \rightarrow 1) Create (or change) Private Access Local Configuration \rightarrow 2) Token and JSON





11.3.3 Create the Private Access Peers JSON file

The Private Access Peers JSON file contains:

- 1. The Local configuration of each Peer.
- 2. The "networks" behind each Peer.
- 3. The "privateApps" allowed to be reached on each Peer.

Here some examples.

11.3.3.1 Full mesh Private Access Peers JSON file

Consider the following example:

We have 3 nodes and we want to allow full communication between sites for all port and protocols.

The Local Config JSON file of each node is:

ns-cgc00001

```
{
    "peers": [
    {
        "nodeName": "ns-cgc00001",
        "description": "Node on VMware Server 1",
        "location": "HQ",
        "publicKey": "yAnz5TF+IXXJte14tji3zIMNq+hd2rYUIgJBgB3fBmk=",
        "publicIpAndUdpPort": "200.1.1.1:51821",
        "privateCirdIp": "192.168.7.1/24",
        "persistentKeepAlive": "no",
        "networks": [],
        "privateApps": []
    }
]
```

ns-cgc00002

}

```
{
    "peers": [
    {
        "nodeName": "ns-cgc00002",
        "description": "Node on VMware Server 2",
        "location": "Datacentre 2",
        "publicKey": "xTIBA5rboUvnH4htodjb6e697QjLERt1NAB4mZqp8Dg=",
        "publicIpAndUdpPort": "200.1.1.2:51821",
        "privateCirdlp": "192.168.7.2/24",
        "persistentKeepAlive": "no",
        "networks": [],
        "privateApps": []
    }
]
```

ns-cgc00003
{
"peers": [
{
"nodeName": "ns-cgc00003",
"description": "Node on VMware Server 3",
"location": "Branch",
"publicKey": "TrMvSoP4jYQlY6RlzBgbssQqY3vxl2Pi+y71lOWWXX0=",
"publicipAndUdpPort": "200.1.1.3:51821",
"privateCirdIp": "192.168.7.3/24",
"persistentKeepAlive": "no",
"networks": [],
"privateApps": []
}
]
}

Firstly, we need to create our "basic" Peers Configuration JSON file: It contains the Local Configuration of each Node plus the "networks" behind each node.

```
Basic Peers Configuration JSON file
{
 "peers": [
   {
      "nodeName": "ns-cgc00001",
      "description": "Node on VMware Server 1",
      "location": "HQ",
      "publicKey": "yAnz5TF+IXXJte14tji3zIMNq+hd2rYUIgJBgB3fBmk=",
      "publicIpAndUdpPort": "200.1.1.1:51821",
      "privateCirdIp": "192.168.7.1/24",
      "persistentKeepAlive": "no",
      "networks": [
        "10.1.1.0/24",
        "10.1.2.0/24"
      ],
      "privateApps": []
   },
   {
      "nodeName": "ns-cgc00002",
      "description": "Node on VMware Server 2",
      "location": "Datacentre 2",
      "publicKey": "xTIBA5rboUvnH4htodjb6e697QjLERt1NAB4mZqp8Dg=",
      "publicIpAndUdpPort": "200.1.1.2:51821",
      "privateCirdIp": "192.168.7.2/24",
      "persistentKeepAlive": "no",
      "networks": [
        "10.2.1.0/24",
        "10.2.2.0/24"
      ],
      "privateApps": []
```

Maidenhead Bridge

Cloud Security Connector Mux for Azure | 108
}, { "nodeName": "ns-cgc00003", "description": "Node on VMware Server 3", "location": "Branch", "publicKey": "TrMvSoP4jYQIY6RIzBgbssQqY3vxI2Pi+y71IOWWXX0=", "publicIpAndUdpPort": "200.1.1.3:51821", "privateCirdIp": "192.168.7.3/24", "persistentKeepAlive": "no", "networks": ["10.3.1.0/24", "10.3.2.0/24" "privateApps": [] }] }

In this "Basic Peers Configuration JSON file" we have:

- Green: The Local values generated at each node.
- Yellow: The Subnets behind each node
- Red: Nothing. No private Apps configured.

If you deployed this "Basic Peers Configuration JSON file" to all CSCs, you have created the Private Cloud. All Peers will be visible to each other, but no traffic between subnets will be allowed because there is no "privateApps" configured.

If we want to allowed traffic any to any between subnets, we need to add the corresponding "privateApps" to each node. For example for node: "ns-cgc00001"



Maidenhead Bridge

Cloud Security Connector Mux for Azure | 109

"sourceCirdlp": [
"0.0.0/0"	
L	
"destinationCirdIp": [
"10.1.1.0/24",	
"10.1.2.0/24"	
],	
"destinationSinglePorts": [
],	
"destinationPortRange": {	
"fromPort": "",	
"toPort": ""	
}	
}	
},	

In this case, we added a "privateApp" that allows any source IPs (0.0.0/0) to reach the "networks" (10.1.1.0/24 and 10.1.2.0/24) using "all" protocols ("ipProtocol" : "all".)

Now, completing our "Peers Configuration JSON file":



Maidenhead Bridge

Cloud Security Connector Mux for Azure | 110



Done! Your task is to implement this JSON file on all CSCs and you will have full connectivity any to any for all protocols.

11.3.3.2 Understanding "privateApps" configuration and values

Question 1: Where to configure the "privateApps"?

Only on the node that has the "destinationCirdIp": [], that belongs to its "networks".

Example: I want to allow access to "destinationCirdIp": ["10.1.1.50/32"]. The rule must be created on node ns-cgc00001 that has "networks": ["10.1.1.0/24","10.1.2.0/24"]

Question 2 : What about the values to configure?

On "privateApps" section there are two types of values to input:

Accepts single value only -> ""

Accepts single or multiple values -> []

Examples:

Single value (""):

"description": " Intranet Servers", "ipProtocol": "tcp",

Single or Multiple values ([]):

```
"sourceCirdIp": ["0.0.0.0/0"],
```

"destinationCirdIp": ["10.1.1.100/32", "10.1.2.100/32"], "destinationSinglePorts": ["80", "443"],

The following table shows all fields and values accepted:

Field	Value Type	Values to configure	Example
"description": "",	Single	String	"description": "Intranet Server Access",
"ipProtocol": "",	Single	tcp,udp,icmp or all	"ipProtocol": "tcp",
"sourceCirdlp": [],	Single or Multiple	Networks in the range of: 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 and 0.0.0.0/0	"sourceCirdIp": ["10.2.1.0/24", "10.2.2.0/24", "10.3.1.0/24", "10.3.2.0/24"],
"destinationCirdIp": [],	Single or Multiple	Networks in the range of ⁴ : 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	"destinationCirdIp": ["10.1.1.100/32", "10.1.1.200/32"],
"destinationSinglePorts": [],	Single or Multiple	Single Port of the range 1 to 65535	"destinationSinglePorts": ["80", "443"],
"destinationPortRange": { "fromPort": "", "toPort": "" }	Single	Single Port of the range 1 to 65535	"destinationPortRange": { "fromPort": "3780", "toPort": "3784" }

IMPORTANT: For PriCPA, 0.0.0.0/0 represent the private network segments: 10/8, 172.16/12, 192.168/16 and not the entire internet addresses.

⁴ The expected value here is a value that belongs to the "network" defined behind the CSC. For example, of the network behind the CSC is 10.1.1.0/24, any destination configured must belong to 10.1.1.0/24, like 10.1.1.100/32.

11.3.3.3 Example of "privateApps" for a Windows Domain controller

The following example shows how to create rules to allow access to your Domains Controllers.

The port information was taken from this article:

https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/config-firewall-for-ad-domains-and-trusts

```
Example: Domain Controllers IPs: "10.2.1.100/32" and "10.2.2.100/32" on Node ns-cgc00002 of previous example
"privateApps": [
           "description": "Domain Controllers TCP",
           "ipProtocol": "tcp",
           "sourceCirdIp": [ "0.0.0.0/0" ],
           "destinationCirdIp": [ "10.2.1.100/32", "10.2.2.100/32" ],
           "destinationSinglePorts": [ "135", "464", "389", "636", "3268", "3269", "53", "88", "445" ],
           "destinationPortRange": { "fromPort": "49152", "toPort": "65535" }
         },
         {
           "description": "Domain Controllers UDP",
           "ipProtocol": "udp",
           "sourceCirdIp": [ "0.0.0.0/0" ],
           "destinationCirdIp": [ "10.2.1.100/32", "10.2.2.100/32" ],
           "destinationSinglePorts": [ "123", "464", "389", "53", "88" ],
           "destinationPortRange": { "fromPort": "", "toPort": "" }
         },
         {
           "description": "Domain Controllers Ping",
           "ipProtocol": "icmp",
           "sourceCirdIp": [ "0.0.0.0/0" ],
           "destinationCirdIp": [ "10.2.1.100/32", "10.2.2.100/32" ],
           "destinationSinglePorts": [],
           "destinationPortRange": { "fromPort": "", "toPort": "" }
        }
      ]
```

11.3.3.4 Example of "privateApps" for Internal Web Server.

In this example, we are showing how to configure access to users on ns-cgc00001 to an Internal Web server located behind node Node ns-cgc00003.

11.3.4 Load the "Private Access Peers JSON file" to the CSCs.

After the Local Configuration is done and the "Private Access Peers JSON file" is created, the next task is to distribute and apply it on each CSC.

There are three methods available:

- 1. URL: (Recommended) Using "Private Access Peers URL" and running the command "Refresh Private Access Peers URL" using AWS Systems Manager, Rundeck or Azure CLI commands.
- 2. DevOps: Distribute the JSON file on all CSC and run the command "Reload Private Access Peers URL" using AWS Systems Manager or Rundeck.
- 3. Manual: Copy/Paste the JSON file on each CSCs.

In this section we are going to explain two methods: URL and Manual Copy. The DevOps method is explained on Section12: DevOps operations.

11.3.4.1 Using "Private Access Peers URL"

This is the recommended method. The steps to configure are:

 Place the Private Access Peers JSON file on an internal web server or an AWS bucket⁵ or similar. Obtain the download URL.

Example of AWS bucket:

Amazon S3 > mhb-netskope-private > privateAccessPeersConfig-LAB2.json	
privateAccessPeersConfig-LAB2.json Info	C Copy S3 URI Download Open [2] Object act
Properties Permissions Versions	
Object overview	
Owner sales AWS Region EU (Ireland) eu-west-1 Last modified November 20, 2021, 10:26:09 (UTC+00:00) Size 6.6 KB	S3 URI S3 URI S3 URI S3://mhb-netskope-private/privateAccessPeersConfig-LAB2.json Amazon Resource Name (ARN) am:aws:s5:::mhb-netskope-private/privateAccessPeersConfig-LAB2.json Entity tag (Etag) d d3aeba11009b98bf5622d9b948f151d9 Object URL
Type json Key O privateAccessPeersConfig-LAB2.json	https://mhb-netskope-private.s3.eu-west-1.amazonaws.com/privateAccessPeersConfig-LAB2.json

2. Configure the URL on each CSC.

Ssh the each CSC and go to Main Menu -> 18) Configure Private Access

⁵ See Appendix D to learn how to secure an AWS S3 bucket by Source IP.



At this moment, you have the option to review the privateApps to configure in Compact or JSON format and to apply the values.

Do you want to apply this values? 1) Yes 2) No Enter your choice: 1
<pre>Creating Private Apps: (MHB-CSC(INFO) Private Access - [Index: 0, Node: zs-csc-mux-4-as-d) Private App 'Allow all to Azure' was created succesfully. (MHB-CSC(INFO) Private Access - [Index: 0, Node: zs-csc-mux-4-as-d) Private App 'SHH and BDP from MGMT Network's was created succesfully. (MHB-CSC(INFO) Private Access - [Index: 2, Node: pricpa-gcloud-v-0-2-a) Private App 'SHH and BDP from MGMT Network's was created succesfully. (MHB-CSC(INFO) Private Access - [Index: 2, Node: pricpa-gcloud-v-0-2-a) Private App 'Allow all to Google Cloud.' not applicable to this node. (MHB-CSC(INFO) Private Access - [Index: 2, Node: pricpa-gcloud-v-0-2-a) Private App 'MAs - istp' not applicable to this node. (MHB-CSC(INFO) Private Access - [Index: 3, Node: ns-csc-gre-v-1-0e) Private App 'MAs - istp' not applicable to this node. (MHB-CSC(INFO) Private Access - [Index: 3, Node: ns-csc-gre-v-1-0e) Private App 'MAs - istp' not applicable to this node. (MHB-CSC(INFO) Private Access - [Index: 3, Node: ns-csc-gre-v-1-0e) Private App 'Allow iperf tcp' not applicable to this node. (MHB-CSC(INFO) Private Access - [Index: 3, Node: ns-csc-gre-v-1-0e) Private App 'Allow SH and RDP to 10.3.200.0/24' was created succesfully. (destinationSinglePorts) (MHB-CSC)(INFO) Private Access - [Index: 4, Node: ns-csc-gre-ws-v-0-4) Private App 'Allow SH and RDP to 10.3.200.0/24' was created succesfully. (destinationSinglePorts) (MHB-CSC)(INFO) Private Access - [Index: 4, Node: ns-csc-gre-ws-v-0-4) Private App 'Allow SHP to 10.3.200.0/24' was created succesfully. (destinationSinglePorts) (MHB-CSC)(INFO) Private Access - [Index: 4, Node: ns-csc-gre-ws-v-0-4) Private App 'Allow iperf up' was created succesfully. (destinationSinglePorts) (MHB-CSC)(INFO) Private Access - [Index: 4, Node: ns-csc-gre-ws-v-0-4) Private App 'Allow iperf up' was created succesfully. (destinationSinglePorts) (MHB-CSC)(INFO) Private Access - [Index: 5, Node: ns-csc-gree-ws-v-0-4) Private App 'Allow iperf up' was created succesfully. (destinationSinglePorts) (MHB-CSC)(INFO) Private A</pre>
Adding Peers: (MHB-CSC)(INFO) Private Access - Node: ns-csc-mux-4-as added successfuly. (MHB-CSC)(INFO) Private Access - Node: ns-csc-grev-1-0e added successfuly. (MHB-CSC)(INFO) Private Access - Node: ns-csc-grev-1-0e added successfuly. (MHB-CSC)(INFO) Private Access - Node: ns-csc-grevas-v-0-4 added successfuly. (MHB-CSC)(INFO) Private Access - Node: ns-csc00006 added successfuly. (MHB-CSC)(INFO) Private Access - Node: ns-csc00006 added successfuly. (MHB-CSC)(INFO) Private Access - Node: ns-csc00006 added successfuly. (MHB-CSC)(INFO) Private Access - Node: ns-cgc00006 added successfuly. (MHB-CSC)(INFO) Private Access - Private Access - Private-access-051820, mhb-csc-private-access-051821' added to Security Group 'zs-csc-mux-4-as-d-eth0-NSG-1' (MHB-CSC)(INFO) Private Access - Private Access Peers List updated succesfuly.
Changes Security Group External: Private Access - Inbound Port Rules 'mhb-csc-private-access-I51280' added to Security Group 'zs-csc-mux-4-as-d-eth0-NSG-1' Private Access - Outbound Port Rules 'mhb-csc-private-access-O51820, mhb-csc-private-access-O51821' added to Security Group 'zs-csc-mux-4-as-d-eth0-NSG-1' (MHB-CSC)(INFO) Private Access - Private Access Peers List updated succesfully.

3. The next time you want to refresh the Private Access Peers JSON file, update the file, deploy it on the same location URL and Run Command: "Refresh Private Access Peers URL" using AWS SSM Agent or Rundeck.

AWS System Manager:

Go to AWS Systems Manager -> Run Command -> and Select "MHB-CSC-Refresh-Private-Access-Peers-URL"

AWS Systems Manager > Run Command > Run a command
Run a command
Command document Select the type of command that you want to run.
Q Search by keyword or filter by tag or attributes
Name
Copy-AWS-RunShellScript
MHB-CSC-Refresh-Private-Access-Peers-URL
MHB-CSC-Refresh-Proxy-Bypass-URL

Move down the screen and select all CSCs:

Targets Choose a m	ethod for selecting targe	ts. 1			2	
Spectrage	cify instance tags cify one or more tag key- c.	value pairs to select instances that s	hare those	Choose Instan Manually select	ces manually the instances you war	nt to register as tar
mi-0f38	37028ad9fcdf8 🗙	mi-0b9178c22b03ce2bf	X mi-0e234	4f4278cd74e27 🗙	mi-Obeef6eaa7	1c2f0bf X
Insta	nces					
Q						
Ping	status: Online 🗙	Clear filters 3				
	Name	Instance ID	Instance stat	e Availat	oility zone	Ping status
	ns-cgc00006-b	mI-0f3837028ad9fcdf8		-		Online
	ns-cgc00004-b	ml-0b9178c22b03ce2bf		-		Online
	ns-cgc00005-a	ml-0e234f4278cd74e27		-		Online
	ns-cgc00004-a	mI-0beef6eaa71c2f0bf	-	-		Online
	ns-cgc00006-a	mi-08c465d750d2689ae	-	-		Online
	ns-cgc00005-b	mi-0650bce2872f405c0	-	-		Online
4						

Go to the bottom of the page and click "Run". The next page shows the status of the command on each CSC.

Command ID: e7c8bfa2-e045-4df0-8216-4721be8d4249 was successfully senti						
WS Systems Manager 📏 Run Command 🏷 Command ID: e7c8bfa2-e045-4df0-8216-4721be8d4249						
Comr	Command ID: e7c8hfa2_e045_4df0_8216_4721he8d4249					
com		5142 0045 4410 02	10 4721500	44243		
Comm	nand status					
Overall status Detaile		Detailed status Success	# targets 6	# completed 6		
Targe	ts and outputs					
	Instance ID	Instance name	Status	Detailed Status		
	Instance ID	Instance name	Status	Detailed Status		
	Instance ID mI-0650bce2872f405c0 mI-08c465d750d2689ae	Instance name ns-cgc00005-b ns-cgc00006-a	Status Success Success	Detailed Status Ø Success Ø Success		
	Instance ID mi-0650bce2872f405c0 mi-08c465d750d2689ae mi-0beef6eaa71c2f0bf	Instance name ns-cgc00005-b ns-cgc00006-a ns-cgc00004-a	Status Status Success Success Success	Detailed Status O Success O Success O Success O Success		
	Instance ID ml-0650bce2872f405c0 ml-08c465d750d2689ae ml-0beef6eaa71c2f0bf ml-0e234f4278cd74e27	Instance name ns-cgc00005-b ns-cgc00006-a ns-cgc00004-a ns-cgc00005-a	Status Status Success Success Success Success Success Success	Detailed Status O Success Success Success Success Success Success Success		
	Instance ID mi-0650bce2872f405c0 mi-08c465d750d2689ae mi-0beef6eaa71c2f0bf mi-0e23ff4278cd74e27 mi-0b9178c22b03ce2bf	Instance name ns-cgc00005-b ns-cgc00006-a ns-cgc00004-a ns-cgc00005-a ns-cgc00005-a ns-cgc00005-a	Status Success Success Success Success Success Success Success	Detailed Status Detailed Status Success Success		

To see the individual result, right click on the Instance ID and open it on a new TAB. Check the "Output"



Using Rundeck

➢ Go to the Project <name> -> All Jobs -> Run " Refresh Private Access Peers URL"



Select ALL nodes and click Run.

Execute Job		×
Refresh Priv	rate Access Peers URL the Peers from the URL and applies the changes.	
Nodes	Change the Target Nodes (6) Select Nodes (6) Select All C Select None	
Cancel	Follow execution Nodes V	

> Wait to succeeded. You can click on "command" to see the results node by node.

NS-CSC-MGMT	Access Peers URL	Succeeded № 0.00.38 of 10.57 pm > Lyou
Log Output »		
100% 6/6 COMPLETE	0 FAILED	0 INCOMPLETE Start time
∨ a ns-cgc00004-a	All Steps O	ĸ
🗸 🚬 Command	ок	10:56:35 pm
22:56:39 22:56:39 22:56:39 22:56:42 22:56:44 22:56:44 22:56:44 22:56:44 22:56:51 22:56:51 22:56:51 22:56:54 22:56:54 22:56:54 22:56:54 22:57:68 22:57:68	Private Access - Private Access Peers JSON : Creating Private Apps Private Access - [Index: 0, Node: ns-cgc0000 Private Access - [Index: 2, Node: ns-cgc0000 Private Access - [Index: 2, Node: ns-cgc0000 Private Access - [Index: 2, Node: ns-cgc0000 Adding Peers: Private Access - Node: ns-cgc0000 added sup Private Access - Node: ns-cgc0000 added sup	'ile imported successfully. (He imported successfully. (destinationSinglePorts) (H) Private App 'Domain Controllers TCP' was created succesfully. (destinationSinglePorts) (H) Private App 'Domain Controllers TCP' was created succesfully. (destinationPortBange) (H) Private App 'Domain Controllers PUN' was created succesfully. (destinationPortBange) (H) Private App 'Domain Controllers PUN' was created succesfully. (destinationSinglePorts) (H) Private App 'Syslog server' was created succesfully. (destinationSinglePorts) (H) Private App 'Syslog server' was created succesfully. (destinationSinglePorts) (H) Private App 'All protocol 192.168.6.6/24' was created succesfully. (destinationSinglePorts) (B) Private App 'BH - SSH and RDP' was created succesfully. (destinationSinglePorts) (cessfuly.
> ms-cgc00004-b > ms-cgc00005-a > ms-cgc00005-b > ms-cgc00006-a	All Steps O All Steps O All Steps O All Steps O	К К К

11.3.4.2 Manual: Copy and Paste "Private Access Peers Json file"

From Main Menu, go to 18) Configure Private Access, follow the steps below and Paste the Private Access Peers Json File:



Done!

11.4 Show Configurations and Status Private Access.

11.4.1 Using SSH Admin console

From Main Menu, go to 17) Show Configurations and Status Private Access.

Private Cloud Private Access (PriCPA)
Show Configuration and Status PriCPA.
Configure PriCPA (Local and Peers Configuration).
Configure CSC Remote Management via PriCPA.
e) Exit
Selection: 17

11.4.1.1 Show Peer/s Status

In this menu you can see "All Peers Status" or by peer "Select Peer".



1. Show All Peers Status



IMPORTANT: This section show is the Peer is Alive and the "Source Port" that arrives at this node from the Peer. The Source Port information is essential to validate that the NAT on the Remote Peer is correct or if the FW on the other end is changing the Source Port. Please, correct the NAT on the remote Peer if you see that the Source Port differs from the expected.

2. Select Peer

This section shows a more detailed information about the Peer.

Maidenhead Bridge

Cloud Security Connector Mux for Azure | 121

Please, select an option:	
1)_Show ALL Peers Status	
2) Select Peer	
3) Quit	
Enter your choice: 2	
Please, select a Peer	
1) "ns-csc-mux-4-as"	
2) "pricpa-gcloud-v-0-2-a"	
3) <u>"ns-csc-gre-y-1-0e"</u>	
4) "ns-csc-gre-aws-v-0-4"	
6) "ns-cgc00004"	
7) "ns-cqc00006"	
8) Quit	
Enter your choice: 4	
Peer Status: Peer '"ns-csc-gre-aws-v-0-4"' (52.4.62.40:51820) -> 192.16	8.7.88 is Alive. Source Port OK. Using '51820'
Peer Counters: Latest Communication: Thu 1 Jun 21:00:06 UTC 2023 Transfer: 1.2Gi received, 5.9Mi sent	
Peer Configuration:	
"location": "vpc-10-3-0-0".	
"description": "Node en US east VPC 10.3.0.0/24",	
"publicKey": "mU4StCAt4sW13xVXaMXcRZjZTuP9G9l/OSL2bsFCh2o=",	
"publicIpAndUdpPort": "52.4.62.40:51820",	
"privatelirdip": "192.108.7.88/24", "persistentKeenAlive": "po"	
"networks": [
"10.3.200.0/24"	
1,	
"privateApps":	
<pre> 'description': "Allow SSH and RDP to 10.3 200 0/24". </pre>	
"ipProtocol": "tcp",	
"sourceCirdIp": [

11.4.1.2 Show Peers Json file (active)

This menu shows the active Private Access Peers Json file.

```
Selection: 17
Show Configuration and Status Private Access
Please, select an option:
1) Show Peer/s Status
Show Peers Json file (active)
3) Show Local Configuration
Show Firewall Local Rules
5) Quit
Enter your choice: 2
ł
   "peers": [
     peers : 1
{
    "nodeName": "zs-csc-mux-4-as-d",
    "location": "Azure US East",
    "description": "CSC MUX 4 AS D",
    "publicKey": "4QJ7QPswdTx+mrLMbgLBube0/rw9sSunY780kljTZ1g=",
    "publicIpAndUdpPort": "74.235.173.101:51280",
    "privateCirdIp": "192.168.7.16/24",
    "persistentKeepAlive": "no",
    "networks": [
             "10.2.2.0/24",
"10.2.3.0/24",
"10.2.4.0/24"
          ],
          "privateApps": [
                "description": "Allow all to Azure",
"ipProtocol": "all",
                 "sourceCirdIp": [
                1,
                 "destinationCirdIp": [
                 ],
                 "destinationSinglePorts": [
```

11.4.1.3 Show Local Configuration

This menu shows the Local configuration of the node.



11.4.1.4 Show Firewall Local Rules

This menu shows in JSON format the Rules required on the Security Group of the external interface of the CSC.

Note: The CSC does the refresh of the External Security Group every time you update the Peers configuration. No manual configuration is required.



11.4.2 Using AWS Systems Manager or Rundeck

In this case, the information provided is only "Show ALL Peer Status"

11.4.2.1 AWS Systems Manager

Go to AWS Systems Manager and Run Command: "MHB-CSC-Show-Private-Access-ALL-Peers-Status" and select the Nodes. The result will show:

AWS Systems Manager > Run Command > Command ID: caa5bcf8-3946-4408-b394-d92dd45cb49e > Output on: mi-08c465d750d2689ae			
Output on mi-08c465d750d2689ae			
Step 1 - Command description and status			
Status ⊘ Success Step name Runscripts	Detailed status Success Start time Sun, 21 Nov 2021 09:46:15 GMT		
▼ Output			
The command output displays a maximum of 48,000 characters. You can vie	w the complete command output in either Amazon S3 or CloudWatch I		
Peer 'ns-cgc00004' -> 192.168.7.11 is Alive. Source Port (Peer 'ns-cgc00005' -> 192.168.7.21 is Alive. Source Port (K. Using '51821' K. Using '51820'		

11.4.2.2 Rundeck

On Rundeck, run Job: "Show Private Access ALL Peers Status". Select the nodes. The output will show:

Show Private Access ALL Peers Status				
Log Output »				
100% 6/6 COMPLETE 0 FAILED Node	0 1			
✓ ➡ ns-cgc00004-a All Steps OK				
Command OK 09:50:20 99:50:21 99:50:21 Peer 'ns-cgc00005' -> 192.168.7.21 is Alive. Source Port 0K. Using '51820' 99:50:22 Peer 'ns-cgc00006' -> 192.168.7.20 is Alive. Source Port 0K. Using '51820'				
✓ 🚔 ns-cgc00004-b All Steps OK				
> ■ command OK > ■ ns-cgc00005-a All Steps OK				
> ▲ ns-cgc00005-b All Steps OK				
> ans-cgc00006-b All Steps OK > ans-cgc00006-b All Steps OK				

11.5 Configure CSC Remote Management via Private Access.

When the CSC is in HA pair, only the active node belongs to the Private Cloud. For this reason, if you want to reach "the Other CSC" node using SSH, you must configure Remote Management on both CSCs of the HA pair.

The configuration is via SSH Main Menu. You need to add the "Management Networks". For example, in your primary Datacentre, you have the Subnet 172.19.0.0/24, and from that Subnet, you want to reach ALL CSCs on the Private Cloud.

The configuration will be:

18) Configure PriCPA (Local and Peers Configuration).
19) Configure CSC Remote Management via PriCPA.
e) Exit Selection: 19
WARNING! You can isolate this node if the configuration is wrong. Be careful with this settings. We recommend to be precise with the Host or Subnet configured here. Subnet Prefixes less than /17 are not accepted.
No Management Networks are configured.
Do you want to configure Management Networks?
1) Yes 2) No 3) Reset to Default Enter your choice: 1
Input Management Network (IP/Subnet Prefix): 172.19.0.0/24
Do you want to add another Management Network?
1) Yes 2) No Enter your choice: 2
Management Networks to configure:
Management Networks Qty = 1 Management Network= 172.19.0.0/24
Do you want to apply changes?
1) Yes 2) No Enter your choice: 1 Private Access - Management Network 172 19 A A/24 was added on zs.csc.mux-4-as-d-1
Trace Access Hunagement Network 172.15.0.0/24 was added on 23-csc-max-4-as-u-1

12 Remote Management

You can use several tools to Remote Manage the CSC. In this chapter, we are showing how to use Azure "Run Command", AWS Systems Manager (Fleet Manager) and Rundeck.

12.1 Azure "Run Command"

12.1.1 Using Azure Portal

Azure portal allows to "Run Command" per VM. "Run Command" is particularly useful if you want to do a quick check, not SSH the CSC. Unfortunately, it is still very buggy and sometimes doesn't work.

Instructions: Select the VM go to Run Command \rightarrow RunShellScript and on "Linux Shell Script" put the command showed in the below table.



12.1.2 Using Azure CLI

The command to execute is the following:

Linux:

```
$az vm run-command invoke -g <ResourceGroup> -n <VmName> --command-id RunShellScript --
scripts <CSC Command> | jq -r .value[].messag
```

Please, note that we are using the program "jq" to extract "message" information and to present it to the Linux terminal.

Example:

Enable succeeded: [stdout] f1 wn5ize: Standard_F4s_v2 CSC date: Sun 4 Jun 10:27:46 UTC 2023 Soft version: 4.0 CSC MOdel: CSC MUX 4 (1.6 Gbps) for Zscaler with PriCPA Azure Cloud: AzureCloud
INTERFACES INFORMATION External: Tunnel IP5 (eth0): 10.2.1.24-[25,26,27]/24 Bypass Proxy Egress IP 10.2.1.28 Network Gateway: 10.2.1.1 Internal: CS GW IP (eth1): 10.2.2.15/24 Network Gateway: 10.2.2.1
TRAFFIC REDIRECTION Options To Zscaler: VIP Proxy: 10.2.2.16:80 (or :9400) Route all traffic via CSC GW IP Zscaler Global Proxies (port 80/9400) via CSC GW IP Direct to Internet: Bypass Proxy: 10.2.2.17:3128 Zscaler Global Proxies (port 3128) via CSC GW IP
PUBLIC IP Address INFORMATION IPsec tunnels Public IP: 74.235.173.100, 74.235.171.133, 74.235.171.132, 20.163.185.222 Bypass Public IP: 74.235.173.171
DNS INFORMATION DNS Server (1): 1.1.1 is Alive DNS Server (2): 8.8.8 is Alive
ZSCALER INFORMATION Zscaler Cloud: zscalerthree primary ZEN mode: WashingtonDC_2 Hostname: was1-2-vpn.zscalerthree.net IP: 165.225.8.35 is Alive Secondary ZEN mode: NewYorkIII Hostname: nyc3-vpn.zscalerthree.net IP: 165.225.38.52 is Alive
LOAD BALANCING INFORMATION Last change: Sat 3 Jun 22:02:08 UTC 2023 (UP) Ztun1 is active, using primary. (UP) Ztun2 is active, using primary. (UP) Ztun4 is active, using primary.
IPSEC INFORMATION Ztuni connected to: WashingtonDC 2, IPsec uptime uptime: 12 hours, since Jun 03 22:00:56 2023, Last Security Association: ESTABLISHED 4 hours ago Ztun2 connected to: WashingtonDC 2, IPsec uptime uptime: 12 hours, since Jun 03 22:00:56 2023, Last Security Association: ESTABLISHED 4 hours ago Ztun3 connected to: WashingtonDC 2, IPsec uptime uptime: 12 hours, since Jun 03 22:00:57 2023, Last Security Association: ESTABLISHED 4 hours ago Ztun4 connected to: WashingtonDC 2, IPsec uptime uptime: 12 hours, since Jun 03 22:00:57 2023, Last Security Association: ESTABLISHED 4 hours ago

12.1.3 Commands table

Test #	Descritption	CSC Command
1	MHB-CSC-ShowConfigurationAndStatus	/home/cscadmin/aws-mt4
2	MHB-CSC-SpeedTest	/home/cscadmin/aws-mt7
3	MHB-CSC-TraceRouteAndLatencyTest	/home/cscadmin/aws-mt6
4	MHB-CSC-Refresh-Proxy-Bypass-URL	/home/cscadmin/aws-bp-refresh-list
5	MHB-CSC-ShowLogCurrentMonth	/home/cscadmin/aws-l-current-month
6	MHB-CSC-Refresh-Routed-Bypass-URL	/home/cscadmin/aws-refresh-routed-bypass-url
7	MHB-CSC-ShowLogLastSixMonths	/home/cscadmin/aws-I-last-6-months
8	MHB-CSC-SwitchTunnels	/home/cscadmin/aws-tun-switch
9	MHB-CSC-Reload-High-Availability	/home/cscadmin/aws-reload-high-availability-json
10	MHB-CSC-Reload-Routed-Bypass-json	/home/cscadmin/aws-reload-routed-bypass-json
11	MHB-CSC-Refresh-Private-Access-Peers-URL	/home/cscadmin/aws-refresh-private-access-peers-url
12	MHB-CSC-Reload-Private-Access-JSON-file	/home/cscadmin/aws-reload-private-access-peers-json
13	MHB-CSC-Show-Private-Access-ALL-Peers-Status	/home/cscadmin/aws-show-private-access-all-peers-status
14	MHB-CSC-Update-Nodes-Database	/home/cscadmin/aws-node-region-update

12.2 AWS Systems Manager

The easiest and accessible way to manage the Cloud Security Connectors is to use AWS Systems Manager. AWS official documentation is available here: <u>https://aws.amazon.com/systems-manager/</u>. The CSC has preinstalled the SSM Agent. You need to register the CSC using "Hybrid Activations" and "Run Documents" afterwards.

With AWS Systems Manager, you can manage the CSC remotely. To do it, you need to create "Documents" in advance. "Documents" are a series of commands used by the "Run Command" functionality.

This section explains how to create the "Documents" and "Run Commands".

12.2.1 Create Documents

We provide a CloudFormation template to create all "Documents" in one shot.

Steps:

1. Download the CloudFormation template from:

https://maidenheadbridge.freshdesk.com/support/solutions/articles/33000280930-createdocuments-to-manage-the-csc-via-aws-systems-manager

2. Deploy Stack. Go to Cloudformation \rightarrow Create Stack \rightarrow Upload a template file

Services V	Q Search for services, features, marketplace products, and docs [Alt+S]
CloudFormation > Stacks > Create stack	
Step 1 Specify template	e stack
Step 2 Prereq Specify stack details	uisite - Prepare template
Step 3 Configure stack options 2	template K based on a template. A template is a JSON o WAML. Rie that contains configuration information about the AWS resources you want to include in the stack. emplate is ready O Use a sample template O trace template in Designer
Step 4 Review Specifi A templat	y template It is a SON or YAMI. file that describes your stack's resources and properties.
Templat Selecting	e source tampate generates an Amazon 53 URL where it will be stored. nazon 53 URL Upload a template file
4 Upload a	template file see file MHB-CSC-AWS-Systems-Manager-Documents-v-1-0/son AMI formatted file
S3 URL: ger-Docu	https://sius-east-2.amazonaws.com/cf-templates-zo3c488/4wul-us-east-2/20211752Uf-MH8-CSC-AWS-Systems-Mana View in uments-v-1-0.json Designer
	5 Cancel Ne

- 3. Click next.
- 4. Put the Stack Name

_		
	aws Services 🔻	Q Search for services, features, marketplace products, and docs [Alt+S]
≡	CloudFormation $>$ Stacks $>$	Create stack
	Step 1 Specify template	Specify stack details
	Step 2 Specify stack details	Stack name
	Step 3 Configure stack options	Stack name MH8-CSC-Documents-for-SSM-Agent Stack name can include letters (J-2 and a-2, numbers (D-9), and dashes (-).
	Step 4 Review	Parameters
		Parameters are defined in your template and allow you to input custom values when you create or update a stack.
		No parameters There are no parameters defined in your template
		Cancel Previous Next

- 5. Click Next -> Next -> Create Stack.
- 6. Wait the Stack to complete.

av	Services V		Q Search for services, features, marketplace products, and docs
Ξ	CloudFormation > Stacks > MHB-CSC-	Documents-for-SSM-A	gent
	⊡ Stacks (1)	C	MHB-CSC-Documents-for-SSM-Agent
	Q Filter by stack name		Stack info Events Resources Outputs Parameters Ter
	Active View nested	< 1 >	Events (41)
	MHB-CSC-Documents-for-SSM-Agent 2021-06-24 10:39:55 UTC+0100 CREATE_COMPLETE	0	Q Search events

 Now go to Services -> Systems Manager -> and click "Documents" and choose "Owned by me"

aws Services -	Q Search for services, features, marketplace products, and docs [Alt+5]	🔯 👃 Adrian Larsen 🔻 Ohio 🔻
Application Management Application Management Application Management Application Management Application Application Decements Decements Decements	Shared with me All documents	Preferences Actions ▼ Create document ▼
Change Management Change Management Change Management	attributes 3 - Documents	< 1 2)
Automation Melli-CSC-Any-UpdateZicaler/Phinodes Change Calendar Document type Owner Maintenance Windows Command 544690173122	MHB-CSC-Refersh-Prozy-Bypass-URL MHB-CSC-Refersh-Prozy-Bypass-URL Document type Owner Document type Owner Command 544690175127	URL MHB-CSC-Reload-Config-ion Document type Owner Command \$44690173127
Vide Management Unix Vide Manager Rev Default version Compliance 1	Platform types Platform types Unix Unix Default version Default version 1 1 1	Platform types Linux Default version 1
Investmentary Myhol Actuation Myhol Actuation Media CSC Medica Migh-Availability Beacon Manager Braic Command Command Command Set469017312 Sate Manager Patch Manager Patch Manager Lina	Hell-CSC-Relax8-Rooted Bypass-jon Mell-CSC-Relax8-Rooted Bypass-jon Command Outer Command S44890173127 Pattern types Linux Linux	tatus O MHB-CSC-ShowConfigurationAndStatus-WS O Document type Owner S127 Command S44690173127 Platform types Linex
Distributor Default version 1	Default version 1 1	Default version 1

8. Done!

12.2.2 Run Commands

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

You can see the operation results on the "Output" section or store the results on S3 Buckets for further inspection.

To "Run Commands", go to AWS Systems Manager \rightarrow Instances & Nodes \rightarrow Run Command.

Here is 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

aws Services V		Q Search for s	ervices, features, marketpl	lace products, and docs	[Alt+S]	
olorer	Command parameter	5				
sCenter						
tch Dashboard	Targets					
	Targets					
n Management	Targets Choose a method for selecting ta	roets				
n Management		igea.		Channel Instances and all live		
ager	Specify one or more tag k	ey-value pairs to select instances that	t share those	Manually select the instances you	want to register as targets.	
	tags.					
e						
	mi-0160555d766bf22c6	X mi-0100c70a3ad29e8b	5 ×			
nagement						
ager New	Instances					
	0					
r	4					
ndows	Ping status: Online 🗙	Clear filters				
agement	Name Name	Instance ID	Instance state	Availability zone	Ping status	Last pir
ner New					-	
	ns-cgc00002-a	mI-0160555d766bf22c6	-	-	Online	14/10/
	ns-cgc00002-b	mi-0100c70a3ad29e8b5	-		Online	14/10/
ivations	•					
mager						

4. Click "Run" . Wait for the Command Status "success"

aws Services v		Q Search for services, featur	res, marketplace products, o	and docs [/
Explorer .	Ocommand ID: 17f0c6ea-d610-43cd-a90	D-3eOd12af4dc0 was successfully ser	nt!	
CloudWatch Dashboard PHD	AWS Systems Manager > Run Comma	nd > Command ID: 17f0c6ea-d61	0-43cd-a900-3e0d12af4c	
	Command ID: 17f0c	bea-d610-43cd-a9	00-3e0d12a1	-4dc0
Application Management Application Manager New	Command status			
AppConfig Parameter Store	Overall status ⊘ Success	Detailed status Success	# targets 2	
Change Management Change Manager New	Targets and outputs			
Automation Change Calendar	Q			
Maintenance Windows	Instance ID	Instance name	Status	Detailed Statu
▼ Node Management	o mi-0100c70a3ad29e8b5	ns-cgc00002-b	⊘ Success	⊘ Success
Fleet Manager New	O mi-0160555d766bf22c6	ns-cgc00002-a	⊘ Success	⊘ Success
Compliance				

5. Right click on Instance ID (mi-xxxx) and open in new tab. Check Output.

aws iii Services Q Search	[Alt+:	5]	D 🕹 🕅 N. California	
AWS Systems × Manager	Command ID: 9860586a-6645-4844-b422-96740a9fa59b	was successfully senti		
Oulck Setup	AWS Systems Manager > Run Command > Comman	d ID: 9860586a-6645-4844-b422-96740a9fa59b > Output on: mi-065b5204	b5d721644	
	Output on mi-065b5204b5d	721644		
Operations Management				
Explorer	Step 1 - Command description and status	5		
OpsCenter	Status	Detailed status	Response code	
CloudWatch Dashboard	Success	⊘ Success	0	
Incident Manager	Step name Runscripts	Start time Sun, 04 Jun 2023 06:21:23 GMT	Finish time Sun, 04 Jun 2023 06:21:30 GMT	
Application Management	▼ Output			
AppConfig The command output displays a maximum of 48,000 characters. You can view the complete command output in either Amazon S3 or CloudWatch Logs, if you specify an S3 bucket or a lo		r CloudWatch Logs, if you specify an 53 bucket or a logs group when you run the comma		
	GENERAL INFORMATION		Copy	
Change Management	Name: zs-csc-mux-4-as-d-2			
Change Manager	Region: eastus SubscriptionId: ffde02fb-c	Region: eastus SubscriptionId: ffde02Fb-c38F-45Fb-9e31-89e5303be5F1 vmSize: Standard_F4s_v2		
Automation	CSC date: Sun 4 Jun 06:21:24 UTC 2023	CSC date: Sun 4 Jun 06:21:24 UTC 2023		
Change Calendar	Soft version: 4.0 CSC Model: CSC MUX 4 (1	Soft version: 4.0 CSC Model: CSC MUX 4 (1.6 Gbps) for Zscaler with PriCPA		
Mariatan and Miladau	Azure Cloud: AzureCloud		Ψ	

6. Done! (Note: You can copy the output and to display on a text editor for more visibility)

File Edit View Search Tools Documents Help *Unsaved Document 1 × GENERAL INFORMATION Name: zs-csc-mux-4-as-d-2 Region: eastus | SubscriptionId: ffde02fb-c38f-45fb-9e31-89e5303be5f1 | vmSize: Standard_F4s_v2 CSC date: Sun 4 Jun 06:21:24 UTC 2023 Soft version: 4.0 | CSC Model: CSC MUX 4 (1.6 Gbps) for Zscaler with PriCPA Azure Cloud: AzureCloud INTERFACES INFORMATION Internal: CSC GW IP (eth): 10.2.1.19-[20,21,22]/24 | Bypass Proxy Egress IP 10.2.1.23 | Network Gateway: 10.2.1.1 Internal: CSC GW IP (eth): 10.2.2.18/24 | Network Gateway: 10.2.2.1 TRAFFIC REDIRECTION Options To Zscaler: VIP Proxy: 10.2.2.19:80 (or :9400) | Route all traffic via CSC GW IP | Zscaler Global Proxies (port 80/9400) via CSC GW IP Direct to Internet: Bypass Proxy: 10.2.2.20:3128 | Zscaler Global Proxies (port 3128) via CSC GW IP PUBLIC IP Address INFORMATION IPsec tunnels Public IP: 74.235.175.176, 20.163.185.99, 74.235.173.170, 20.163.185.151 Bypass Public IP: 74.235.173.101 DNS INFORMATION Using Azure DNS (168.63.129.16) and Google DNS (8.8.8.8, 8.8.4.4) ZSCALER INFORMATION Zscaler Cloud: zscalerthree Primary ZEN node: AutoPrimary | Hostname: vpn.zscalerthree.net | IP: 165.225.8.35 is Alive Secondary ZEN node: AutoSecondary | Hostname: secondary.vpn.zscalerthree.net | IP: 165.225.38.52 is Alive LOAD BALANCING INFORMATION (UP) Ztun2 is active, using primary. Ztun3 is active, using primary. Ztun4 is active, using primary. (UP)(UP) IPSEC INFORMATION Ztun1 connected to: AutoPrimary, IPsec uptime uptime: 10 hours, since Jun 03 19:53:19 2023, Last Security Association: ESTABLISHED 2 hours ago Ztun2 connected to: AutoPrimary, IPsec uptime uptime: 10 hours, since Jun 03 19:53:19 2023, Last Security Association: ESTABLISHED 2 hours ago Ztun3 connected to: AutoPrimary, IPsec uptime uptime: 10 hours, since Jun 03 19:53:19 2023, Last Security Association: ESTABLISHED 2 hours ago Ztun4 connected to: AutoPrimary, IPsec uptime uptime: 10 hours, since Jun 03 19:53:19 2023, Last Security Association: ESTABLISHED 2 hours ago Ztun4 connected to: AutoPrimary, IPsec uptime uptime: 10 hours, since Jun 03 19:53:19 2023, Last Security Association: ESTABLISHED 2 hours ago CREDENTIALS INFORMATION Username: zs-csc-mux-4-as-d-2@maidenheadbridge.com | PSK: Not shown. Please, read it from 'Configuration Wizards' Menu http://ip.zscaler.com INFORMATION Ztun1 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 136.226.68.253, via Public IP: 74.235.175.176 Ztun2 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 136.226.69.27, via Public IP: 20.163.185.99 Ztun3 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 165.225.9.19, via Public IP: 74.235.173.170 Ztun4 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 136.226.51.20, via Public IP: 20.163.185.151

12.2.3 List of Documents available for "Run Command"

- 1. "MHB-CSC-ShowConfigurationAndStatus": Executes "Show Configuration and Status"
- 2. "MHB-CSC-SpeedTest": Performs speedtest.net on the CSC.
- 3. "MHB-CSC-TraceRouteAndLatencyTest": Performs MyTraceRoute test against the Primary and Secondary ZEN. It also does a Reverse Test from the tunnel active to your Public IP if the tunnel is up.
- 4. "MHB-CSC-Refresh-Proxy-Bypass-URL": Refresh the Proxy Bypass list using the values of the Proxy Bypass PAC file stored in the URL configured.
- 5. "MHB-CSC-Refresh-Routed-Bypass-URL": Refresh the Routed Bypass list using the values of the JSON file stored in the URL configured.
- 6. "MHB-CSC-ShowLogCurrentMonth": Shows current month logs.
- 7. "MHB-CSC-ShowLogLastSixMonths": Shows last six month logs.
- 8. "MHB-CSC-SwitchTunnels": Switch tunnels.
- 9. "MHB-CSC-Reload-Config-json": Reloads the values of config.json file. (not implemented on the CSC Mux for Azure)
- 10. "MHB-CSC-Reload-High-Availability": Reloads the values of highAvailability.json file. (for CSC on AWS, Azure and Gcloud. Not in use on CSC for Virtual Platforms.
- 11. "MHB-CSC-Reload-Routed-Bypass-json": Reloads the values of routedBypassRulesFile.json.
- 12. "MHB-CSC-Update-Nodes-Database": Updates the Zscaler Node Database.
- 13. "MHB CSC Refresh Private Access Peers URL": Refresh the Private Access Peers list using the values of the JSON file stored in the URL configured.
- 14. "MHB CSC Reload Private Access Peers JSON file": Reloads the values of privateAccessPeersConfig.json
- 15. "MHB CSC Show Private Access ALL Peers status": Show the Status of all Private Access Peers.

12.3 Rundeck

Rundeck (https://www.rundeck.com/) is an open-source software Job scheduler and Run Book Automation system for automating routine processes across development and production environments. It combines task scheduling multi-node command execution workflow orchestration and logs everything that happens.

Installation Steps:

- 1. Install Rundeck. Intructions at: https://www.rundeck.com/open-source
- 2. Create a Project.
- 3. Enable user "csccli" and setup the SSH Public key on each CSC.
- 4. On the Project, setup the SSH Private and define the nodes:

ll,	S-CSC-MGMT V Proje	ect
Dasheoard	Edit Nodes File 2 /home/rundeck/06/rundeck/NS-CSC-MGMT-NODES.json	
JOBS	Source 2. File Rea	ds a file containing node definitions in a supported format
	Format	
	Description /home/rund	deck06/.rundeck/NS-CSC-MGMT-NODES.json
	Soft Wrap	
₩ WEEHHOOKS	<pre> ""</pre>	3
	Cancel Save	

5. Create the jobs. Please, contact Support at http://support.maidenheadbridge.com for the latest Job List.

Maidenhead Bridge

Cloud Security Connector Mux for Azure | 136

12.3.1 Jobs

The following screen shows the list of Jobs available.

Э.	NS-CSC-MGMT V
Ê	17 All Jobs
ASHBOARD	Expand All Collopse All
joes	▶ Check CSC Status - Netskope This test checks L7 Keepalives on CSCs using Netskope Cloud ③ in 11m
÷.	Refresh Proxy Bypass URL
NODES	Refresh Proxy Bypass URL - CSCs with tags:active This job executes Refresh Proxy Bypass List command on all CSCs with tags:active
>_	Refresh Routed Bypass URL This job updates the Routed Bypass Configuration on the CSC using the Routed Bypass URL.
COMMANDS	Fafresh Routed Bypass URL - CSCs with tags:active This job updates the Routed Bypass Configuration on the CSCs with tags:active using the Routed Bypass U
5	Reload Config Json File This job reloads the values of the config json file onto the CSC.
ACTIVITY	Reload High Availability Json File This job is valid only for CSCs on AWS, Azure and Gcloud.
#	Reload Routed Bypass Json File
WEBHOOKS	Show Configuration and Status This job provides all configuration and statuses information of the CSC.
	Show Configuration and Status - CSC with tag:active This job executes Show Configuration and Status command on all CSCs with tag:active
	► Show Logs Current Month
	Show Logs Last 6 Months
	Speed Test This job executes Speed Test from the CSC to speedtest.net
	Switch Tunnels This Job Switches tunnels Primary / Secondary
	Test Email Use this job to check that you are receiving olerts via email.
	Traceroute and Latency Test Use this Job to check the quality of the path to the Cloud - hop by hop
	Update Nodes Database

12.3.2 Running job "Show Configuration and Status"

S-CSC-MGMT	~				
Show Configu	ration and Status - CSC with tags:active =	Succeeded № 0.00.09 at 7:38 pm > Lyou			
Log Output »					
100% 2/2 COMPLETE	0 FAILED	0 INCOMPLETE	0 NOT STARTED		
Node			Start time Dure		
✓ ➡ ns-cqc00002-a	All Steps OK		0.00		
	OK		7:38:08 pm 0.00		
command	UK CK		7.50.00 pm		
18:38:11					
18:38:11	GENERAL INFORMATION				
18:38:11	company : Maidennead Bridge				
18:38:11	Location : HUKVM				
18:38:11	CSC ID : hs-cgc00002-a				
10:30:11	CSC date: Inu 14 Oct 19:38:10 BSI 2021				
10:30:11	Solt Version : 1.0				
10:30:11	THTEREACEC THEORMATTON				
10.30.11	INTERFACES INFORMATION				
10:30:11	External: Jumiet 17: 192.100.1.00 bypass P104y Egless 17: 192.100.1.01 CSL 17(EUR); 192.100.1.02/24 WEUWIK Odleway: 192.100.1.240 15 ALIVE Totarnal: CSC 6W TO: 172 10 A 60 CSC 10(ath): 172 10 A 63/24 Naturek Gataway: 177 10 A 13 i. Alive				
10.30.11	Incentat: CSC 0W IP: 1/2.15.0.00 CSC IP(eth1): 1/2.15.0.03/24	Network Galeway: 172.15.0.155 15 Active			
10.30.11	TRAFFIC REDITRECTION Options				
10.30.11	To Netskope, VID Broxy, 172 19 0 61,90 Boute all traffic via C	SC GW TD Netskape Global Dravy TD, 163 116 128 80.80	VID CSC GW TR		
18.38.11	Direct to Internet: Nunas Provide 10 (0) + 62-3128 (NetSchoe Global Provy Pr. 163-116-128 via (SC GW P				
18:38:11	biteet to internet. bypass rroxy. 1/2.15.0.02.5120 wetskope of	354C 110Xy 11. 105.110.120.00.5120 V14 CSC 0W 11			
18:38:11	DNS_TNEORMATION				
18:38:11	DNS Server (1) TP: 172 19 A 1AA is Alive				
18:38:11	DNS Server (2) IP: 1.1.1.1 is Alive				
18:38:11					
18:38:11	NETSKOPE INFORMATION				
18:38:11	GRE tunnels earess Public IP: 82.68.6.74				
18:38:11					
18:38:11	Primary Tunnel:				
18:38:11	Node : GB.London.LON1				
18:38:11	Node Public IP: 163.116.162.36				
18:38:11	Node Probe: 10.162.6.209				
18:38:11	Secondary Tunnel:				

13 DevOps operations

The CSC is delivered will all configurations and is ready for production. Even so, during the life cycle of the CSC, some parametrization may be required to be changed or modified. For this reason, we provide some configuration utilities that will help with further parametrization and change management.

The CSC offers an option to do some changes using JSON config files. The operation is simple and is three steps:

- 1. Obtain the current JSON file from the CSC.
- 2. Download the modified JSON file to the CSC.
- 3. "Run Command" (AWS Systems Manager) of the specific "reload" document. (or use Rundeck Job or Azure Run Command)

The JSON files are available are:

- 1. **routedBypassRulesFile.json**: Allows administrators to manually configure Routed Bypass Rules if not using the Routed Bypass URL method.
- 2. **privateAccessPeersConfig.json:** Use this Json file to configure "networks" and "privateApps" on your Private Cloud.
- 3. highAvailability.json: Allows administrators to configure the CSC on HA pair.

In this chapter, we are going to explain the procedures.

13.1 routedBypassRulesFile.json

You can use this file to create Routed Bypass Rules manually instead of using the automatic method via Routed Bypass URL.

1. Obtain the current "routedBypassRulesFile.json" from the CSC, running "Run Command" (AWS-RunShellScript.). For example:

```
cat /usr/local/etc/mhb-csc/routedBypassRulesFile.json
   "routedBypassRules": [
      {
         "description": "O365 Login URLs 1",
          "ipProtocol": "tcp",
         "sourceCirdIp": "0.0.0.0/0",
"destinationCirdIp": "20.190.128.0/18",
         "fromPort": "80",
"toPort": "80"
      },
      {
         "description": "O365 Login URLs 2",
"ipProtocol": "tcp",
          "sourceCirdIp": "0.0.0.0/0",
          "destinationCirdIp": "20.190.128.0/18",
         "fromPort": "443",
"toPort": "443"
      },
      {
         "description": "O365 Login URLs 3",
          "ipProtocol": "tcp",
         "sourceCirdIp": "0.0.0.0/0",
"destinationCirdIp": "40.126.0.0/18",
         "fromPort": "80",
"toPort": "80"
      },
      {
         "description": "portquiz.net",
"ipProtocol": "tcp",
          "sourceCirdIn": "0 0 0 0/0"
          "destinationCirdIp": "52.47.209.216/32",
         "fromPort": "80",
"toPort": "80"
      },
      {
         "description": "O365 Login URLs 4",
         "ipProtocol": "tcp",
"sourceCirdIp": "0.0.0.0/0",
"destinationCirdIp": "40.126.0.0/18",
         "fromPort": "443",
"toPort": "443"
      }
      {
         "description": "Skype and Teams UDP 1",
         "ipProtocol": "udp",
"sourceCirdIp": "0.0.0.0/0",
         "destinationCirdlp": "13.107.64.0/18",
"fromPort": "3478",
"toPort": "3481"
      },
      {
         "description": "Skype and Teams UDP 2",
"ipProtocol": "udp",
"sourceCirdIp": "0.0.0.0/0",
"destinationCirdIp": "52.112.0.0/14",
"fromPort": "3478",
"toPort": "3481"
      }
      {
         "description": "Skype and Teams UDP 3",
"ipProtocol": "udp",
"sourceCirdIp": "0.0.0.0/0",
         "destinationCirdlp": "52.120.0.0/14",
"fromPort": "3478",
"toPort": "3481"
      }
  1
```

- 2. Create a AWS bucket (or other place) and place on it the modified "routedBypassRulesFile.json" file.
- 3. Download the file to the CSC. Run Command "AWS-RunShellScript"

wget <Your bucket file URL> -O /usr/local/etc/mhb-csc/routedBypassRulesFile.json

4. Run Document "MHB-CSC-Reload-Routed-Bypass-json" to apply the changes.

13.2 privateAccessPeersConfig.json

You can use this file to create Private Access Peer Rules manually instead of using the automatic method via Private Access Peers URL.

1. Obtain the current "privateAccessPeersConfig.json" from the CSC, running "Run Command" (AWS-RunShellScript.). For example:

```
cat /usr/local/etc/mhb-csc/privateAccessPeersConfig.json
   "peers": [
    {
        "nodeName": "ns-cgc00001".
        "description": "Node on VMware Server 1",
       "location": "HQ",
"publicKey": "yAnz5TF+IXXJte14tji3zIMNq+hd2rYUIgJBgB3fBmk=",
        "publicIpAndUdpPort": "200.1.1.1:51821",
        "privateCirdIp": "192.168.7.1/24".
        "persistentKeepAlive": "no",
        "networks": ["10.1.1.0/24", "10.1.2.0/24" ],
        "privateApps": [
             "description": "Allow all traffic to this site",
"ipProtocol": "all",
              "sourceCirdIp": [ "0.0.0.0/0" ],
              "destinationCirdIp": [ "10.1.1.0/24", "10.1.2.0/24" ],
              "destinationSinglePorts": [ "
                                                "],
             "destinationPortRange": { "fromPort": "", "toPort": "" }
          }
       ]
    }
    {
        "nodeName": "ns-cgc00002",
"description": "Node on VMware Server 2",
        "location": "Datacentre 2",
       "publicKey": "xTIBA5rboUvnH4htodjb6e697QjLERt1NAB4mZqp8Dg=",
"publicIpAndUdpPort": "200.1.1.2:51821",
        "privateCirdIp": "192.168.7.2/24",
        "persistentKeepAlive": "no"
        "networks": [ "10.2.1.0/24", "10.2.2.0/24" ],
        "privateApps": [
          {
             "description": "Allow all traffic to this site",
"ipProtocol": "all",
"sourceCirdIp": [ "0.0.0.0/0" ],
              "destinationCirdlp": [ "10.2.1.0/24", "10.2.2.0/24" ],
              "destinationSinglePorts": [ "" ],
              "destinationPortRange": { "fromPort": "", "toPort": "" }
       1
       "nodeName": "ns-cgc00003",
"description": "Node on VMware Server 3",
"location": "Branch",
        "publicKey": "TrMvSoP4jYQIY6RIzBgbssQqY3vxI2Pi+y71IOWWXX0=",
       "publicIpAndUdpPort": "200.1.1.3:51821",
"privateCirdIp": "192.168.7.3/24",
        "persistentKeepAlive": "no",
"networks": [ "10.3.1.0/24", "10.3.2.0/24" ],
"privateApps": [
             "description": "Allow all traffic to this site",
"ipProtocol": "all",
"sourceCirdIp": [ "0.0.0.0/0" ],
              "destinationCirdIp": [ "10.3.1.0/24", "10.3.2.0/24" ],
              "destinationSinglePorts": [ "" ],
              "destinationPortRange": { "fromPort": "", "toPort": "" }
       1
    }
  1
```

2. Create a AWS bucket and place on it the modified "privateAccessPeersConfig.json" file.

Maidenhead Bridge

Cloud Security Connector Mux for Azure | 141



3. Download the file to the CSC. Run Command "AWS-RunShellScript"

wget <Your bucket file URL> -O /usr/local/etc/mhb-csc/privateAccessPeersConfig.json

4. Run Document "MHB-CSC-Reload-Private-Access-JSON-file" to apply the changes.

13.3 highAvailability.json file

You can configure High Availability via downloading the highAvailability.json file and "Run Command" using the "MHB-CSC-Reload-High-Availability" AWS SSM document.

Steps:

1. Obtain the current "highAvailability.json" from the CSC, running "Run Command" (AWS-RunShellScript.)

The fields in **bold** are not configurable. So please, do not modify.



2. Create a AWS bucket and place on it the modified "highAvailability.json" file. For example:

The fields in **bold** are not configurable. So please, do not modify.

{
"model": "csc-mux-zs-azure",
"type": "highAvailability",
"version": "1.0",
"highAvailability": {
"haEnable": true,
"halamRole": "SystemAssigned",
"haFirstCsc": {
"vmName": "zs-csc-mux-4-as-d-1",
"vmResourceGroup": "CSC-East-US",
"haBypassPublicIp": "74.235.173.101"
<u>}.</u>
"haSecondCsc": {
"vmName": "zs-csc-mux-4-as-d-2",
"vmResourceGroup": "CSC-EAST-US",
"haBypassPublicIp": "74.235.173.171"
},
"haPrivateAccessPublicIp": "74.235.173.101",
"haRoutes": [
{
"routeName": "Server-default-route",
"routeTable": "Servers-Route-Table",
"resourceGroup": "RouteTables-East-US"
λ.
{
"routeName": "Zscaler-Global-GW",
"routeTable": "Servers-Route-Table",
"resourceGroup": "RouteTables-East-US"
}
}

3. Download the file to the CSC. Run Command "AWS-RunShellScript"

wget <Your bucket file URL> -O /usr/local/etc/mhb-csc/highAvailability.json

4. Apply the IAM Role to the CSC via AWS Console and Run Document "MHB-CSC-Reload-High-Availability" to apply the changes.
14 Appendixes

14.1 Appendix A: Release Notes

14.1.1 Version 4.0.4 (June 2023)

Version 4.0.4 of the CSC Mux for Azure has the following enhancements:

- Change to Standard SKU for Public IPs when deploying the CSC on Availability Set and No Infrastructure.
- The Radius timeout was adjusted to allow more time for MFA authentication.
- Azure WAAGENT agent goes direct instead via the tunnel. This change allows running "Run Commands" even if the Zscaler tunnels are down.
- Manage Administrators menu restricted to "cscadmin" user only. This change avoids a clash of configurations when multiple admins are manipulating the settings.
- Solved a problem when passing User Data (via configUserData.json file) at initial deployment with wrong values on the Zscaler nodes section. The CSC will try once and stop if the entered Zscaler node information is invalid.

14.1.2 Version 4.0 (June 2023)

Version 4.0 of the CSC Mux for Azure has the following enhancements:

- Product renaming: The Cloud Security Connectors for Azure have been renamed according to the amount of IPsec tunnels to Zscaler: CSC Mux 1 (1 x IPsec, 400 Mbps), CSC Mux 2 (2 x IPsec, 800 Mbps), CSC Mux 4 (4 x IPsec, 1,6 Gbps) and CSC Mux 8 (8 x IPsec, 3.2 Gbps). The following list shows the old and new names.
 - CSC Anywhere for Azure \rightarrow CSC Mux 1 for Azure with PriCPA.
 - New $! \rightarrow$ CSC Mux 2 for Azure with PriCPA.
 - ° CSC Mux 1.6 Gbps → CSC Mux 4 for Azure with PriCPA.
 - ° CSC Mux 3.2 Gbps → CSC Mux 8 for Azure with PriCPA.
- New! Private Cloud Private Access: PriCPA is a new functionality of the Cloud Security Connector. PriCPA allows you to create a Private Cloud among all CSCs for private traffic. In a matter of minutes, you can build a full mesh encrypted topology between your locations for private traffic with Zero Trust. After making the Private Cloud, you can set up your policies to define who will talk with who inside your Private Cloud.
- New! Traffic Logs: The CSC can send all traffic logs to a Syslog/SIEM server. The Traffic Logs
 provide visibility of all IP communications to Zscaler, Routed and Proxy Bypasses, PriCPA,
 and Local received and generated traffic. This functionality is essential to customers with a
 basic Zscaler Cloud Firewall license.

- New! SNMP support: The CSC Mux for Azure can be monitored via SNMP v2c and v3.
- New! Radius integration: You can access the Admin console using your username and authenticating via Radius protocol to a Radius Server.
- New! The "csccli" user can be enabled and configured via the Admin console, allowing terminal access to the CSC using SSH keys.
- New! SSH access can be restricted per Subnet or IP. It applies to the CSC's Internal (eth1) and PriCPA interface. It is not required anymore to set up external security groups.
- TCPdump functionality is provided via the Admin console for easy troubleshooting of IP traffic.
- New! Azure Load Balancer support. The CSC answers Azure LB Health probes on the CSC VIP IP (port 59400) and CSC Bypass IP (port 53128) when the tunnels to Zscaler are up. If the tunnels to Zscaler are down, the CSC stops answering the probes.
- New! Config User Data support. When launching the CSC, you can insert the configUserData.json file as VM's User Data to pass configuration parameters to the CSC, such as Zscaler Cloud, Zscaler Nodes, DNS Servers, AWS Systems Manager Credentials, Syslog configuration, Bypass (routed and proxy) configuration, PriCPA values and more.

14.1.3 Version 3.1 (July 2021)

Version 3.1 of the CSC Mux for Azure has the following enhancements:

- New! CSC Mux 1.6 Gbps (ex CSC Mux 1G). The CSC Mux with 4 x IPsec tunnels can deliver now 1.6 Gbps.
- New! CSC Mux 3.2 Gbps (ex CSC Mux 2G). The CSC Mux with 8 x IPsec tunnels can deliver now 3.2 Gbps.
- New! Routed Bypass functionality Added. The Routed Bypass allows you to bypass Zscaler for specific destinations when routing all traffic via the CSC Mux using your Public IP.

14.1.4 Version 3.0 (October 2020)

The CSC Mux for Azure was created merging two existing products: the CSC for Azure + CSC Mux for Vmware/Hyper-V.

This version contains all the features of the CSC for Azure (single) plus the following enhancements:

- The CSC Mux is using Ubuntu 20.04 as base OS
- The CSC Mux 1 Gbps can aggregate 4 x IPsec tunnels to deliver 1 Gbps to Zscaler.
- The CSC Mux 2 Gbps can aggregate 8 x IPsec tunnels to deliver 1 Gbps to Zscaler.
- Speedtest runs in parallel in all tunnels and returns; as a result, the sum of all tests.

Maidenhead Bridge

Cloud Security Connector Mux for Azure | 147

14.2 Appendix B: configUserData.json file

14.2.1 Parameters

Via configUserData.json file, you can pass values to parameters during the installation of the CSC. You can setup:

- Zscaler Information: CloudName (zscloud, zscalerthree, zscalertwo; etc.), Nodes (autodiscovery or manual selection), vpnCredentials "domain". (Using "domain" the CSC automatically creates the FQDN (<vmName@domain> and Pre shared keys for IPsec.)
- 2. AWS SSM agent registration values.
- 3. DNS servers
- 4. Syslog servers and traffic log configuration.
- 5. Bypasses: Proxy Bypass PAC URL and Routed Bypass URL
- 6. PriCPA Local configuration values, Peers URL and Remote Management Networks.
- 7. SSH Restrictions via eth1 and wg0.
- 8. Admin Management: Enable csccli user and SSH Key.

14.2.2 configUserData.json file (blank)

configUserData.json (blank)

The fields in **bold** are not configurable. So please, do not modify.



Maidenhead Bridge

Cloud Security Connector Mux for Azure | 148

```
"enable": "no",
        "primaryServer": {
"ip": "",
"port": ""
        },
"secondaryServer": {
"ip": "",
"port": ""
      },
"trafficLogs": {
"enable": "no"
    },
"bypasses": {
        "proxyBypass": {
"pacUrl": ""
      },
"routedBypass": {
"jsonUrl": ""
  },
"priCPA": {
    "enable": "no",
    "nodeName": "",
    "location": "",
    "description": "",
    "avbitIdeDot": "",

       "description": "",
"publicUdpPort": "51280",
"privateCirdlp": "",
"persistentKeepAlive": "no",
"peersJsonFileUrl": "",
"remoteManagementNetworks": []
    },
    "sshRestrictions": {
"eth1": {
             etn1 : {
"enable": "no",
"allowedNetworks": []
    },
"wg0": {
"enable": "no",
"allowedNetworks": []
    "adminManagement": {

"csccli": {
            "enable": "no",
"sshPublicKey": ""
       }
   }
}
```

14.2.3 configUserData.json file: Example

```
configUserData.json
   "model": "csc-mux-zs-azure".
   "type": "configUserData",
   "version": "1.0",
"zscalerInformation": {
     "cloudName": "zscalerthree",
      "vpnNodes": {
         "autoDiscovery": "yes",
        "primary": {
"hostName": ""
        },
"secondary": {
           "hostName": ""
        }
     }.
      "vpnCredentials": {
         "domain": "maidenheadbridge.com"
     }
  },
"awsSsmAgent": {
    "enable": "yes",
    ````tonCode'
 "activationCode": "ic/L9H7p+floBF5vVefe",
"activationId": "6ba05125-0bfc-42e7-9535-7f523746e752",
"awsRegion": "us-east-1"
 "dns": {
 "useCloudDns": "yes",
"primaryDnslp": "",
"secondaryDnslp": ""
 },
 "syslog": {
"enable": "yes",
 "primaryServer": {
"ip": "172.19.0.5",
 "port": "5514"
 },
 "secondaryServer": {
 "ip": "",
"port": ""
 },
 "trafficLogs": {
"enable": "yes"
 }
 "bypasses": {
 proxyBypass": {
 "proxyBypass": {
 "pacyIrl": "https://pac.zscalerthree.net/RdwNltSPqBFN/az-csc-bypass.pac"

 },
 "routedBypass": {
 "jsonUrl": "https://mhb-zscaler-pac-files.s3.eu-west-1.amazonaws.com/routedBypassRulesFile.json"
 }
 },
"priCPA": {
 "enable": "yes",
"nodeName": "zs-csc-mux-4-as-d",
 "location": "Azure US East",
 "description": "CSC MUX 4 AS D",
"publicUdpPort": "51280",
"privateCirdlp": "192.168.7.16/24",
 "persistentKeepAlive": "no"
 "peersJsonFileUrl": "https://mhb-zscaler-private.s3.eu-west-1.amazonaws.com/privateAccessPeersConfig-LAB2.json",
 "remoteManagementNetworks": [
"172.19.0.0/24",
 "192.168.1.0/24",
 "192.168.6.0/24"
]
 },
"sshRestrictions": {
 "eth1": {
 "enable": "yes",
"allowedNetworks": [
 "10.2.0.0/16",
"172.19.0.0/24",
 "192.168.1.0/24",
 "192.168.6.0/24"
 1
 },
"wg0": {
 "enable": "yes",
 "allowedNetworks": [
"10.2.0.0/16",
 "172.19.0.0/24",
```

**Maidenhead Bridge** 

Cloud Security Connector Mux for Azure | 150

"192.168.1.0/24"
h.
"adminManagement": {
"csccii": {
"enable": "yes",
"sshPublicKey": "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDPm+99wX1/ZhtDIKWh+Uv4TrEYboLoLJIRV6NZctrrkbpq/
WuSCtY9ghL456s4jmSSaNzSSCZ5ywpa3LxmYZ60huoUvYEXBR+lj7MX+trVsifYUe6aJgjPzH8q3x2X72bS20jBQovrNoeN6DZRWWLzLZ4xyczOF+samsm6l/
O3jop68KG6+FydfxFM4DddlJrw29sMi9BJmOzA0Ejl2r3x/
Niz+PWqgbvg5Aq9+uPbJsd6t5egsBsXsKi62bIv2rX5hMyZQbxpjcq7BUAc4QcxwZH76X2Y3QVkGnjKXjkFJMcLd6qzN6Su3yYqn41H8ffN2C0rSKD38fvwNDDJTkmZ93PW9mWQweNuWMvLxQTG14z0qR9
VDnlkMtxiJCZyJpUYe6RQDga0nweFIOGB07N9fA/KzA8r/GjI52E5KIEQQ725pQXcjHZHFjzTeiD12jjEBAURUx0DLldBTsO/oisGUT+pZNQAx6gmX/YxDE/le7qdjuf48aHjwH+uGL1/Q0= cscadmin"
}
}

### 14.2.3.1 zscalerInformation



In this case, the CSC automatically discover the nearest primary and secondary node of Zscaler Three and creates the VPN Credentials. (FQDN: <vmName>@<domain>, PSK: <autogenerated>)

If you want to set up the nodes manually, select "autodiscovery": "no" and put the primary and secondary node host names. You can obtain the VPN hostname from the page: https://ips.<cloudname>.net

#### 14.2.3.2 awsSsmAgent



Insert here the values for the activation of the AWS SSM agent. See section 9.2.1 for more details.

#### 14.2.3.3 dns

```
"dns": {

useCloudDns": "yes",

"primaryDnslp": "",

"secondaryDnslp": ""

}
```

Select "UserCloudDns": "yes" if you want to use Azure DNS (primary) and Google DNS (secondary)

Select "UserCloudDns": "no" and put the values of "primaryDnsIp" and "secondaryDnsIp" if you want to use your own DNS servers.

#### 14.2.3.4 syslog



Configure "enable": "yes" and put a value on "primaryServer", "ip" and "port". The secondary servers is optional.

If you want the CSC to collect traffic logs, put "trafficLogs", "enable": "yes"

#### 14.2.3.5 bypasses

```
"bypasses": {
 "proxyBypass": {
 "pacUrl": "https://pac.zscalerthree.net/RdwNltSPqBFN/az-csc-bypass.pac"
 },
 "routedBypass": {
 "jsonUrl": "https://mhb-zscaler-pac-files.s3.eu-west-1.amazonaws.com/routedBypassRulesFile.json"
 },
 }
```

In this section, you can configure the Proxy Bypass PAC URL and the Routed Bypass URL that contains the routeBypassRulesFile.json

#### 14.2.3.6 priCPA



In this section, you can configure the Local values for PriCPA, the Peers URL and the Remote Management Networks. See section 11 for more details.

## 14.2.3.7 sshRestrictions

"sshRestrictions": {     "eth1": {     "eth2": {     "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {         "eth2": {	
endule : yes ;	
"10.2.00/16",	
"172.19.0.0/24",	
"192.168.1.0/24",	
"192.168.6.0/24"	
}.	
"wg0": {	
"enable": "yes",	
"allowedNetworks": [	
"10.2.0.0/16",	
"172.19.0.0/24",	
"192.168.1.0/24"	

In this section, you can configure from which networks you can access the CSC via SSH. You can configure when the traffic arrives from the local internal interface (eth1) or via PriCPA (wg0).

## 14.2.3.8 adminManagement

"adminManagement": {     "sccli": {
"enable": "yes",
"sshPublicKey": "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDPm+99wX1/ZhtDlKWh+Uv4TrEYboLoLJIRV6NZctrrkbpq/
VuSCtY9ghL456s4jmSSaNzSSCZ5ywpa3LxmYZ60huoUvYEXBR+lj7MX+trVsifYUe6aJgjPzH8q3x2X72bS20jBQovrNoeN6DZRWWLzLZ4xyczOF+samsm6l/
)3jop68KG6+FydfxFM4DddIJrw29sMi9BJmOzA0Ejl2r3x/
liz+PWqgbvg5Aq9+uPbJsd6t5egsBsXsKi62blv2rX5hMyZQbxpjcq7BUAc4QcxwZH76X2Y3QVkGnjKXjkFJMcLd6qzN6Su3yYqn41H8ffN2C0rSkD38fvwNDDJTkmZ93PW9mWQweNuWMvLxQTG14z0qR9
<pre>/DnlkMtxiJCzyJpUYe6RQDga0nweFIOGB07N9fA/KzA8r/Gjl52E5KIEQQ725pQXcjHZHFjzTeiD12jjEBAURUx0DLldBTsO/oisGUT+pZNQAx6gmX/YxDE/le7qdjuf48aHjwH+uGL1/Q0= cscadmin"</pre>
}
}

In this section, you can enable access to the terminal console using the "csccli" user. You need to add here the SSH Public Key.

# 14.3 Appendix C: JSON formatters (Visual Code, Notepad ++)

We strongly recommend using Software that can show errors on your JSON file and also can format (beautify) the file for better visibility. Below two examples.

# 14.3.1 Visual Code



- 1. Download : https://code.visualstudio.com/download
- 2. Select your platform and install.
- 3. Create your JSON.
  - 3.1. Visual Code will show the errors in RED.
  - 3.2. To "Beautify" your JSON file press:
    - 3.2.1. On Windows: "Shift + Alt + F"
    - 3.2.2. On MAC: "Shift + Option + F"
    - 3.2.3. On Linux: " Ctrl + Shift + I"

## 14.3.2 Notepad ++



- 1. Download: https://notepad-plus-plus.org/downloads/
- 2. Install JSON Viewer Plug in.

20	\Progra	am Files\Notepad	++\change.log - Notepad++		1						
File	Edit	Search View I	Encoding Language Settings	Tools Macro Run	Plugins Window ?						
		🖻 🗟 🕞 🚔	l k n n jo c la 😽	🔍 🔍 🖪 🖬	5 1 <b>F B B G A B O I</b>						
- ch	ange lo										
	a ongong ta j										
2	NO	Notepad++ V0 Plugins Admin									
3	1.	Fix a regr	Available Updates Installed								
4	2.	Fix a regr									
5	з.	Make Funct	Search: ison		Nevt	3 Install					
6	4.	Make UDL g	1001		. Here	2110100					
7	5.	Fix phante	Dhumin	Venter		\$					
8	۰.	Enable bad	Plugin	version							
10			jN Notepad++ Plugin	2.2.185.6							
11	Not	tepad++ v8.1	SON Viewer	1.40	2						
12			JSTool	1.2107.2							
13	1.	Fix empty	LanguageHelp	1.7.5							
14	2.	Fix langua	Linefilter3	1							
15			Linter	0.1							
16			Location Navigate	0.4.8.1							
17	NO	cepad++ vs	LuaScript	0.11							
19	1.	Fix confid	-								
20	2.	Workaround	200N viewer that dealays the only	stad 200N atriag in a tra	s view						
21			Author: Kapil Ratnani	ected 550W string in a de	e view.						
22			Homepage: https://github.com/ka	pilratnani/JSON-Viewer							
23	Not	tepad++ v8.1									
24						~					
25	1.	Fix empty									
20	2.	Fix white									
28	4.	Fix "Run n									
29	5.	Fix toolti									
30	6.	Fix dockir			Close						
31											
32											
1 00			A here discours								

- 3. Create your JSON file.
- 4. To Check your JSON file go to: Plugins -> JSON Viewer -> Show JSON Viewer.

un Plu	Plugins Window ?						
9	MIME Tools						
	Converter	>					
- r	NppExport	>		-			
	JSON Viewer	>	[	Show JSON Viewer	Ctrl+Alt+Shift+J		
Plugins Admin				Format JSON	Ctrl+Alt+Shift+M		
on	Open Plugins Fold	er		Compress JSON	Ctrl+Alt+Shift+C		
": "y	Anz5TF+1XXJte1	4tji3zlM		About			
ndUdp	Port": "200.1.	1.1:51821	L",				
rd Troll	. #102 169 7 1	/248					

5. To format ("Beautify") your JSON go to: Plugins -> JSON Viewer -> Format JSON

# 14.4 Appendix D: Securing an AWS Bucket by source IP.

- On your AWS console create a bucket with default values for permissions: "Block *all* Public Access = on"
- 2. On Bucket Policy, add your Public IPs in "aws:SourceIp":[]



```
"Version": "2012-10-17",
 "Id": "S3PolicyId1",
 "Statement": [
 {
 "Sid": "IPAllow",
 "Effect": "Allow",
 "Principal": "*",
 "Action": "s3:*",
 "Resource": "arn:aws:s3:::mhb-zscaler-private/*",
 "Condition": {
 "IpAddress": {
 "aws:Sourcelp": [
 "200.1.1.1/32",
 "200.1.1.2/32",
 "200.2.0.0/24"
]
 }
 }
 }
]
}
```

3. Done!