NetScaler VPX Deployment with XenDesktop and XenApp on Microsoft Azure

Deployment Guide
Table of contents

Azure and NetScaler
   Azure Requirements 3
   NetScaler Implementation Scenarios 3
   Deployment Infrastructure 4

NetScaler Load Balancer
   VPX on Azure 5
   Setting and Basic Features 6
   Authentication (LDAP) 7
   SSL Certificates 9
   Load Balancing Monitoring for StoreFront 15
   Load Balancing 15

NetScaler Content Switching
   Content Switching VIP 20

Azure Load Balancer
   External LB 23
   Internal LB 26

NetScaler Gateway
   Create a Gateway Virtual Server 29
   Add Certificates/Authentication 31
   Create XenDesktop Policies/Profiles and bind to Gateway Virtual Server 33
   Add XenDesktop STA Server 37

Appendix
   XenDesktop StoreFront 40
   NetScaler Configuration (NetScaler Primary) 44
**Azure and NetScaler**
This document delivers prescriptive guidance on how to deploy NetScaler with XenApp/ XenDesktop. **It's highly recommended to follow the exact steps during the configuration.** The general information about NetScaler VPX on Azure and the deployment guide can be found here.

**Azure Pre-Requisites**
Leveraging existing XenDesktop infrastructure including Active Directory, LDAP, StoreFront, and Desktop Delivery Controller (DDC) on same Azure network

- Azure Cloud Storage and container (vhd storage)
- Virtual network and subnets configuration
- Create an image from a VHD
- Create a NetScaler VPX from image gallery and apply proper NetScaler and Gateway licenses
- Create another NetScaler VPX in the same cloud service

**NetScaler Implementation Scenarios**
NetScaler generally can be deployed in Azure environment in following three scenarios. **It's highly recommended to follow the exact steps during the configuration.** If your deployment is different from these scenarios and you need assistance, please contact Citrix support team. The following configuration examples use XenDesktop and XenApp. There may be difference in GUI if other versions of XenDesktop and XenApp are used.

- **Scenario 1:** Active-Active: two NetScaler VPXs running independently under Azure Load balancer
- **Scenario 2:** Active-Standby: NetScaler High Availability feature mode
- **Scenario 3:** Azure internal load balancer is utilized to load balance internally between VMs (in this XenDesktop environment case, VMs can be NetScaler load balancing virtual servers)
Deployment Infrastructure

Network Topology

This document primarily covers scenario 3 deployment. In this environment, two NetScaler VPXs will be load balanced by Azure external load balancer as well as internal load balancer, and send XenDesktop requests to two StoreFront servers before handing the traffic to XenDesktop Desktop Delivery Controllers.

Flow Diagram

External HTTP request is coming from Internet to a secured domain using SSL, port 443. Then it will be load balanced to primary of NetScaler Gateway VIPs (port 15000) which will deliver to local content switching VIP, port 1500 then send the request to load balance VIP, port 80 internally. Each load balancing VIP will be connected to two StoreFront backend servers via HTTP on IIS port 80.
**NetScaler Load Balancer**

**VPX on Azure**

Two VPXs will be used in this environment. They should be built under a same cloud service, or DNS NAME.

Two VPXs will be running HA under Active-Standby mode. The following steps can be performed to achieve properly adding a secondary (standby) node and automatic synchronization. In Active-Active mode, meaning that two VPX will be running independently, it is critical to ensure both VPXs have the same configuration.

**System>High Availability>Nodes>Add**

Once NetScaler HA is properly set, when you log into a standby node, you will get a warning message that any configuration changes made in standby node will not be propagated to primary node.
Settings and Basic Features
This environment will be utilizing following four basic features—SSL Offloading, Load Balancing, Content Switching and NetScaler Gateway which need to be enabled under Settings.

System>Settings>Configure Basic Features
Authentication – LDAP
In order to accomplish Single-Sign-On access through NetScaler Gateway and StoreFront servers, LDAP server will be configured based on pre-existing LDAP credential and added into as a policy to be used with VIP.

System>Authentication>LDAP>Servers
Choose LDAP server which was just added above and \textit{NS\_TRUE} for Expression.

\textit{System} > \textit{Authentication} > \textit{LDAP} > \textit{Policies}

\textbf{SSL Certificates}

To generate and install a public SSL certificate, complete the following procedures:

- Creating a RSA Key
- Creating a Certificate Signing Request (CSR)
- Copy CSR over to your certificate authority to get approval and server certificate
- Installing the server certificate
- Creating a Certificate-key pair
Creating a RSA Key

Traffic Management>SSL>SSL Keys>Create RSA Key
Creating a Certificate Signing Request (CSR)
Use your external FQDN in Common Name.

Traffic Management>SSL>SSL Certificates>Create CSR
Copy CSR over to your certificate authority to get approval and server certificate
Choose your CSR request file under Manage Certificates then View File to copy the content:

_Traffic Management>SSL>Tools>Manage Certificates/Keys/CSRs_
Installing the server certificate (Example)
Enter your CSR request to your certificate authority server, to receive server certificate file.

Creating a Certificate-key pair
Traffic Management>SSL>SSL Certificates

Create a Certificate-Key pair file to install Certificates on NetScaler:
Create a Certificate-Key pair file to install CA Certificates on NetScaler:
Load Balancing Monitoring for StoreFront
Enter your Monitor name and choose Type as STOREFRONT. Then add your Store Name under Special Parameters.

Traffic Management>Load Balancing>Monitors>Add

Load Balancing
Traffic Management>Load Balancing>Virtual Servers>Add
Pick an unused, non-routable IP address for internal communication, such as **192.168.10.101** and port **80**
Add Monitors
Deployment Guide

NetScaler VPX Deployment with XenDesktop and XenApp on Microsoft Azure

Monitors Table:
- Name: ping-default, State: Enabled, Type: PING
- Name: tcp-default, State: Enabled, Type: TCP
- Name: arp, State: Enabled, Type: ARP
- Name: nd6, State: Enabled, Type: ND6
- Name: ping, State: Enabled, Type: PING
- Name: tcp, State: Enabled, Type: TCP
- Name: http, State: Enabled, Type: HTTP
- Name: tcp-ecv, State: Enabled, Type: TCP-ECV
- Name: http-ecv, State: Enabled, Type: HTTP-ECV
- Name: udp-ecv, State: Enabled, Type: UDP-ECV
- Name: dns, State: Enabled, Type: DNS
- Name: ftp, State: Enabled, Type: FTP
- Name: tcps, State: Enabled, Type: TCP
- Name: https, State: Enabled, Type: HTTP
- Name: tcps-ecv, State: Enabled, Type: TCP-ECV
- Name: https-ecv, State: Enabled, Type: HTTP-ECV
- Name: ldns-ping, State: Enabled, Type: LDNS-PING
- Name: ldns-tcp, State: Enabled, Type: LDNS-TCP
- Name: ldns-dns, State: Enabled, Type: LDNS-DNS
- Name: xdm, State: Enabled, Type: CITRIX-XDM
- Name: xnc, State: Enabled, Type: CITRIX-XNC-ECV

Service Load Balancing Monitor Binding:
Add Persistence

Virtual Servers on both VPX nodes:

On NetScaler Primary:

On NetScaler Secondary:
NetScaler Content Switching
Content Switching enables the NetScaler appliance to direct requests sent to the same Web host to different servers with different content. In this set up, we are leveraging NetScaler content switching feature to enable NetScaler HA to share a load balancing VIP on Azure environment.

Traffic Management>Content Switching>Virtual Servers>Add
Add **CS Policy Binding** to add **Load Balancing Virtual Server**.

CS-VIP is up.

On NetScaler Primary:

On NetScaler Secondary:
**Azure Load Balancer**

**External LB**

Create an External Load Balancer

Azure external load balancer can be added via either Azure Management Portal Interface (web browser) or Azure PowerShell. This guide will be focusing on using command line via PowerShell.

```powershell
> Add-AzureAccount

> $vm1 = "NSVPX1"
> $vm2 = "NSVPX2"
> $svc = "NSVPX"
> $lbsetname = "DemoLB"
> $epname = "E-VIP"

```
Set up Persistency
Set the Azure Distribution mode on a load balanced endpoint set to add a persistency.

> Get-AzureVM –ServiceName $ServiceName | grep AzureEndPoint –Name $Name

Confirm your LBSetName name and LoadBalancerDistribution is not set.

Add sourceIP to LoadBalancerDistribution on your LBSetName.

> Set-AzureLoadBalancedEndpoint –ServiceName $ServiceName –LBSetName $LBSetName –LoadBalancerDistribution "sourceIP"
Confirm LoadBalancerDistribution is set to sourceIP.

```
Internal LB
Create an Internal Load Balancer
> $svc = “NSVPX”
> $ilb = “VPX-iLB”
> $subnet = “Subnet-1”
> Add-AzureInternalLoadBalancer –ServiceName $svc –InternalLoadBalancerName $ilb –SubnetName $subnet

Add VMs and assign ports on Internal Load Balancer
> $vm1 = “NSVPX1”
> $vm2 = “NSVPX2”
> $epname = “I-VIP”
> $prot = “TCP”
> $locport = “1500”
> $pubport = “80”
> $lbsetname = “Demo-iLB”
```
> Get-AzureVM -Name $vm2 -ServiceName $svc | Add-AzureEndpoint -LBSetName $lbsetname -Name $epname -Protocol $prot -Localport $locport -PublicPort $pubport -InternalLoadBalancername $ilb -ProbeProtocol TCP -ProbePort 9000 -ProbeIntervalInSeconds 5 | Update-AzureVM

Confirm your Internal Load Balancer IP Address

> Get-AzureService -ServiceName $svc | Get-AzureInternalLoadBalancer
Set up Persistency
Set the Azure Distribution mode on a load balanced endpoint set to add a persistency.

> Get-AzureVM -ServiceName $ServiceName | grep AzureEndPoint –Name $Name

Confirm your LBSetName name and LoadBalancerDistribution is not set.

Add `sourceIP` to `LoadBalancerDistribution` on your LBSetName.

> Set-AzureLoadBalancedEndpoint -ServiceName $ServiceName -LBSetName $LBSetName -LoadBalancerDistribution "sourceIP"
Confirm **LoadBalancerDistribution** is set to **sourceIP**.

![NetScaler Gateway configuration command output](image)

**NetScaler Gateway**

NetScaler Gateway will be configured to provide external users to access internal application (in this deployment, it will be XenDesktop infrastructure) via SSL VPN. The following steps to be completed in order to provide SSL VPN service via NetScaler Gateway:

- Create a Gateway Virtual Server
- Add Certificates/Authentication
- Create XenDesktop Policies/Profiles and bind to Gateway Virtual Server
- Add XenDesktop STA server
Create a Gateway Virtual Server

NetScaler Gateway>Virtual Servers>Add
Ensure to use the same port (e.g. 15000) which was used as a local port in Azure External Load Balancer configuration.

Add Certificates/Authentication
Server Certificate and CA certificate along with LDAP configuration which were created in previous chapter will be added into Gateway (VPN) Virtual Server as following.

Add Certificates
Add Authentication (LDAP)

VPN Virtual Server

Basic Settings

Name: Demo-VIP
IP Address: 10.10.0.13
Port: 15000
Max Users
Max Login Attempts
Failed Login Timeout
State: true
ICA Only: false
Enable Authentication: true
Double Hop: false
Down State Flush: false
DTLS: false
AppFlow Logging: false
ICA Proxy Session Migration: false
Enable Device Certificate: false

Certificates

1 Server Certificate
No CA Certificate

Authentication

To add, please click on the + icon

Choose Type

Choose Policy
LDAP
Choose Type
Primary

Continue Cancel
Create XenDesktop Policies/Profiles and bind to Gateway Virtual Server

NetScaler Gateway Session Profiles then Policies will be created in order to be attached to Gateway Virtual Server.

Add Policies

*NetScaler Gateway* > *Policies* > *Session*
### NetScaler VPX Deployment with XenDesktop and XenApp on Microsoft Azure

**Client Experience**

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting Policy</td>
<td></td>
</tr>
<tr>
<td>Home Page</td>
<td></td>
</tr>
<tr>
<td>URL for Web-Based Email</td>
<td></td>
</tr>
<tr>
<td>Split Tunnel*</td>
<td>OFF</td>
</tr>
<tr>
<td>Session Time-out (mins)</td>
<td>30</td>
</tr>
<tr>
<td>Client Idle Time-out (mins)</td>
<td></td>
</tr>
<tr>
<td>Clientless Access*</td>
<td>Allow</td>
</tr>
<tr>
<td>Clientless Access URL Encoding*</td>
<td>Obscure</td>
</tr>
<tr>
<td>Clientless Access Persistent Cookie*</td>
<td>DENY</td>
</tr>
<tr>
<td>Plug-in Type*</td>
<td>Windows/MAC OS X</td>
</tr>
<tr>
<td>Single Sign-on to Web Applications</td>
<td><strong>On</strong></td>
</tr>
<tr>
<td>Credential Index*</td>
<td>PRIMARY</td>
</tr>
</tbody>
</table>

*Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.*
Create NetScaler Gateway Session Profile

Name
XD-CR-Profile

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Override Global

Default Authorization Action
ALLOW

Secure Browse

Advanced Settings

Create
Close

Configure NetScaler Gateway Session Profile

Name
xd-cr-profile

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Override Global

ICA Proxy
ON

Web Interface Address
http://192.168.10.101/Citrix/DemoW

Web Interface Address Type
IPV4

Web Interface Portal Mode
NORMAL

Single Sign-on Domain
citrixonazure

Citrix Receiver Home Page

Account Services Address

OK
Close
Add Policies

Add XenDesktop STA Server

Typically, XenDesktop STA server will be your XenDesktop Desktop Delivery Controller.

Add STA server under Published Applications

Confirm NetScaler Gateway Virtual Server State is up.
Access to External Load Balancer

Access to Internal Load Balancer

Appendix
StoreFront
The latest StoreFront Configuration is available at Citrix Product Documentation at:


Use your StoreFront FQDN (of Azure iLB) or IP address and proper port in Base URL.
Choose *User name and password*, and *Pass-through from NetScaler* under *Authentication*.
Under Enable Remote Access, choose your NetScaler Gateway. If there is none, skip and perform *Add NetScaler Gateway Appliance* in next step then come back to add here.
NetScaler Configuration (NetScaler Primary)

# NS10.5 Build 51.1045.e
# Last modified Tue Apr 21 16:16:42 2015
set ns config -IPAddress 10.10.0.12 -netmask 255.255.240.0
enable ns feature WL SP LB CS SSL SSLVPN
enable ns mode MBF USNIP PMTUD
set system parameter -natPcbForceFlushLimit 4294967295
set system user nsroot 1de06ff012a8dd274d519ad30139c3d395dbc4ae7b92051a6 -encrypted
add system user azureuser 1851e4917a15611503371c1395f8139ee22e8fc719ae7f371 -encrypted
set rsskeytype -rsstype ASYMMETRIC
set lacp -sysPriority 32768 -mac 00:0d:3a:32:10:8b
set ns hostName NSVPX1
set interface 0/1 -throughput 0 -bandwidthHigh 0 -bandwidthNormal 0 -intftype "Hyper v" -ifnum 0/1
set interface LO/1 -haMonitor OFF -throughput 0 -bandwidthHigh 0 -bandwidthNormal 0 -intftype Loopback -ifnum LO/1
add ns ip6 fe80::20d:3aff:fe32:108b/64 -scope link-local -type NSIP -vlan 1 -vServer DISABLED -mgmtAccess ENABLED -dynamicRouting ENABLED
set ipsec parameter -lifetime 28800
set nd6RAvariables -vlan 1
set snmp alarm SYNFLOOD -timeout 1
set snmp alarm HA-VERSION-MISMATCH -time 86400 -timeout 86400
set snmp alarm HA-SYNC-FAILURE -time 86400 -timeout 86400
set snmp alarm HA-NO-HEARTBEATS -time 86400 -timeout 86400
set snmp alarm HA-BAD-SECONDARY-STATE -time 86400 -timeout 86400
set snmp alarm APPFW-START-URL -timeout 1
set snmp alarm APPFW-DENY-URL -timeout 1
set snmp alarm APPFW-REFERER-HEADER -timeout 1
set snmp alarm APPFW-CSRF-TAG -timeout 1
set snmp alarm APPFW-COOKIE -timeout 1
set snmp alarm APPFW-FIELD-CONSISTENCY -timeout 1
set snmp alarm APPFW-FIELD-FORMAT -timeout 1
set snmp alarm APPFW-BUFFER-OVERFLOW -timeout 1
set snmp alarm APPFW-FIELD-FORMAT -timeout 1
set snmp alarm APPFW-SAFE-COMMERCE -timeout 1
set snmp alarm APPFW-SAFE-OBJECT -timeout 1
set snmp alarm APPFW-POLICY-HIT -timeout 1
set snmp alarm APPFW-VIOLATIONS-TYPE -timeout 1
set snmp alarm APPFW-XSS -timeout 1
set snmp alarm APPFW-XML-XSS -timeout 1
set snmp alarm APPFW-SQL -timeout 1
set snmp alarm APPFW-XML-SQL -timeout 1
set snmp alarm APPFW-XML-ATTACHMENT -timeout 1
set snmp alarm APPFW-XML-DOS -timeout 1
set snmp alarm APPFW-XML-VALIDATION -timeout 1
set snmp alarm APPFW-XML-WSI -timeout 1
set snmp alarm APPFW-XML-SCHEMA-COMPILE -timeout 1
set snmp alarm APPFW-XML-FAULT -timeout 1
set snmp alarm DNSKEY-EXPIRY -timeout 1
set snmp alarm HA-LICENSE-MISMATCH -timeout 86400
set snmp alarm CLUSTER-NODE-HEALTH -time 86400 -timeout 86400
set snmp alarm CLUSTER-NODE-QUORUM -time 86400 -timeout 86400
set snmp alarm CLUSTER-VERSION-MISMATCH -time 86400 -timeout 86400
set snmp alarm PORT-ALLOC-FAILED -time 3600 -timeout 3600
set ns tcpProfile nstcp_default_profile -WS ENABLED -SACK ENABLED -TimeStamp ENABLED
set ns tcpProfile nstcp_default_Mobile_profile -frto ENABLED
add server 10.10.0.10 10.10.0.10
add service SF1 10.10.0.10 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp ON -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO
add ssl certKey self -cert self.cert -key self.key
add ssl certKey democertkey -cert netscalercloud_com.crt -key "/nsconfig/ssl/demokey"
add ssl certKey democa -cert COMODORSADomainValidationSecureServerCA.crt
add ssl certKey democa2 -cert COMODORSAAddTrustCA.crt
add ssl certKey democa3 -cert AddTrustExternalCARoot.crt
add authentication ldapAction demoldap -serverIP 10.10.10.10 -ldapBase "dc=ctixonazure,dc=local" -ldapBindDn ad_min@ctixonazure.local -ldapBindDnPassword ff35055272967070b0db -encrypted -ldapLoginName samAccountName -groupAttrName memberOf -subAttributeName CN
add authentication ldapPolicy demoldap NS_TRUE demoldap
set lb parameter -sessionsThreshold 150000
add lb vserver LBVIP HTTP 192.168.10.101 80 -persistenceType COOKIEINSERT -timeout 0 -cltTimeout 180
add cs vserver CSVIP HTTP 10.10.0.12 1500 -cltTimeout 180
set cache parameter -via “NS-CACHE-10.0: 13”
set aaa parameter -maxAAAUsers 5
add vpn vserver AGVIP SSL 10.10.0.12 15000 -downStateFlush DISABLED
set ns rpcNode 10.10.0.12 -password 8a7b474124957776a0cd31b862cbe4d72b5cb5d59868a136d4bde56cf03b28 -encrypted -srcIP 10.10.0.12
bind cmp global ns_adv_nocmp_xml_ie -priority 8700 -gotoPriorityExpression END -type RES_DEFAULT
bind cmp global ns_adv_nocmp_mozilla_47 -priority 8800 -gotoPriorityExpression END -type RES_DEFAULT
bind cmp global ns_adv_cmp_mscss -priority 8900 -gotoPriorityExpression END -type RES_DEFAULT
bind cmp global ns_adv_cmp_msapp -priority 9000 -gotoPriorityExpression END -type RES_DEFAULT
bind cmp global ns_adv_cmp_content_type -priority 10000 -gotoPriorityExpression END -type RES_DEFAULT
set responder param -undefAction NOOP
add ca action NOOP_CA -type noop
bind lb vserver LBVIP SF1
bind cs vserver CSVIP -lbvserver LBVIP
set ns diameter -identity netscaler.com -realm com
set smpp param
set ns tcpParam -WS ENABLED -SACK ENABLED
set ns tcpbufParam -memLimit 200
set dns parameter -dns64Timeout 1000
add dns nsRec . a.root-servers.net -TTL 3600000
add dns nsRec . b.root-servers.net -TTL 3600000
add dns nsRec . c.root-servers.net -TTL 3600000
add dns nsRec . d.root-servers.net -TTL 3600000
add dns nsRec . e.root-servers.net -TTL 3600000
add dns nsRec . f.root-servers.net -TTL 3600000
add dns nsRec . g.root-servers.net -TTL 3600000
add dns nsRec . h.root-servers.net -TTL 3600000
add dns nsRec . i.root-servers.net -TTL 3600000
add dns nsRec . j.root-servers.net -TTL 3600000
add dns nsRec . k.root-servers.net -TTL 3600000
add dns nsRec . l.root-servers.net -TTL 3600000
add dns nsRec . m.root-servers.net -TTL 3600000
add dns addRec l.root-servers.net 199.7.83.42 -TTL 3600000
add dns addRec b.root-servers.net 192.228.79.201 -TTL 3600000
add dns addRec d.root-servers.net 199.7.91.13 -TTL 3600000
add dns addRec j.root-servers.net 192.58.128.30 -TTL 3600000
add dns addRec h.root-servers.net 128.63.2.53 -TTL 3600000
add dns addRec f.root-servers.net 192.5.5.241 -TTL 3600000
add dns addRec k.root-servers.net 193.0.14.129 -TTL 3600000
add dns addRec a.root-servers.net 198.41.0.4 -TTL 3600000
add dns addRec c.root-servers.net 192.33.4.12 -TTL 3600000
add dns addRec m.root-servers.net 202.12.27.33 -TTL 3600000
add dns addRec i.root-servers.net 192.36.148.17 -TTL 3600000
add dns addRec g.root-servers.net 192.112.36.4 -TTL 3600000
add dns addRec e.root-servers.net 192.203.230.10 -TTL 3600000
set lb monitor ldns-dns LDNS-DNS -query . -queryType Address
add lb monitor SFMON STOREFRONT -scriptId nssf.pl -dispatcherIP 127.0.0.1
             dispatcherPort 3013 -LRTM DISABLED -storename Demo
bind service SF1 -monitorName SFMON
add route 0.0.0.0 0.0.0.0 10.10.0.1
set ssl service nshttps-::1l-443 -eRSA ENABLED -sessReuse DISABLED -tls11 DISABLED -tls12 DISABLED
set ssl service nsrpcs-::1l-3008 -eRSA ENABLED -sessReuse DISABLED -tls11 DISABLED -tls12 DISABLED
set ssl service nsrnatsip-127.0.0.1-5061 -eRSA ENABLED -sessReuse DISABLED -tls11 DISABLED -tls12 DISABLED
set ssl service nskrpcs-127.0.0.1-3009 -eRSA ENABLED -sessReuse DISABLED -tls11 DISABLED -tls12 DISABLED
set ssl service nshttps-127.0.0.1-443 -eRSA ENABLED -sessReuse DISABLED -tls11 DISABLED -tls12 DISABLED
set ssl service nsrpcs-127.0.0.1-3008 -eRSA ENABLED -sessReuse DISABLED -tls11 DISABLED -tls12 DISABLED
set ssl vserver AGVIP -tls11 DISABLED -tls12 DISABLED
add vpn sessionAction CR-action -defaultAuthorizationAction ALLOW -SSO ON -icaProxy ON
add vpn sessionAction NCR-action -defaultAuthorizationAction ALLOW -SSO ON -icaProxy ON
add vpn sessionPolicy CR-pol “REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver” CR-action
add vpn sessionPolicy NCR-pol “REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
             && REQ.HTTP.HEADER Referer EXISTS” NCR-action
set vpn parameter -forceCleanup none -clientOptions all -clientConfiguration all
bind system user azureuser superuser 101
bind vpn vserver AGVIP -staServer “http://10.10.10.131”
bind vpn vserver AGVIP -policy demoldap -priority 100
bind vpn vserver AGVIP -policy CR-pol -priority 100
bind vpn vserver AGVIP -policy NCR-pol -priority 100
bind vpn vserver AGVIP -policy _cacheTCVPNStaticObjects -priority 10 -gotoPriorityExpression END -type REQUEST
bind vpn vserver AGVIP -policy _cacheOCVPNStaticObjects -priority 20 -gotoPriorityExpression END -type REQUEST
bind vpn vserver AGVIP -policy _cacheVPNStaticObjects -priority 30 -gotoPriorityExpression END -type REQUEST
bind vpn vserver AGVIP -policy _noCacheRest -priority 40 -gotoPriorityExpression END -type REQUEST
bind ssl vserver AGVIP -certkeyName democertkey
bind ssl vserver AGVIP -certkeyName democa -CA -ocspCheck Optional
bind ssl vserver AGVIP -certkeyName democa2 -CA -ocspCheck Optional
bind ssl vserver AGVIP -certkeyName democa3 -CA -ocspCheck Optional
bind ssl vserver AGVIP -eccCurveName P_256
bind ssl vserver AGVIP -eccCurveName P_384
bind ssl vserver AGVIP -eccCurveName P_224
bind ssl vserver AGVIP -eccCurveName P_521
set L3Param -icmpErrGenerate DISABLED
set ns encryptionParams -method AES256 -keyValue ff0e316156e61427d39d6ebe1a5b9a156d0c5d6c5fefd144aa1d4859ab89807a1bba39088c18c8556b41c50e975e712b8 -encrypted
set rise param -indirectMode ENABLED
set ip6TunnelParam -srcIP ::
set ptp -state ENABLE
Done