Load Balancing Exchange 2013 With Citrix NetScaler 11

Configuring Exchange 2013 CSS Load Balancing & ActiveSync Client Certificate Authentication Using Kerberos Constrained Delegation for Single Sign-on.

Ted Joffs
HTTP://WWW.TEDJOFFS.COM

Overview

This configuration guide is written and intended to be guide for Load Balancing Microsoft Exchange 2013 via **Citrix NetScaler 11 Build 64.34** and newer with the following expectations:

- Provide Load Balancing (LB) to all Exchange services.
- Provide ActiveSync Kerberos Constrained Delegation to function with iPhone, iPad (iOS Configuration Utility or AirWatch), Android (TouchDown Mail Client or AirWatch), or Windows Phone (AirWatch).
- Provide service monitors that are in line with Microsoft best practices.
- Provide all Exchange services via Content Switching Services (CSS) to only use one IP address.
- Utilize responder and rewrite policies and actions to automatically redirect unsecured and root URL connections.
- All communication from the client through to the Exchange 2013 servers will be secured.

The following caveats, expectations, and prerequisites apply:

- Security is your responsibility. There are some security optimizations in this guide, however they should be taken with a grain of salt, validated, verified, optimized, and enhanced. You agree that by continuing with this configuration, you are aware that you are responsible for the security of your environment and that you hold the author blameless should your deployment or environment be compromised – for any reason, at any time.
- The most critical component in Kerberos is time. If you do not have a stable time environment in your network, this won't work – no exceptions.
- This guide is NOT based on the Graphical User Interface (GUI) environment; it is expected that the Command Line Interface (CLI) will be used for the deployment of this configuration.
- It is expected that the NetScaler be installed, networked, and pre-configured with basic settings prior to proceeding.
- It is expected that the Exchange 2013 environment be installed and functional, users do not need to migrated to the environment yet.
- It is expected that you have a working internal Certificate Authority (CA) server capable of serving client certificates.
- It is expected that the SSL Certificates have been installed and the appropriate key-pairs have been generated and linked.
- It is expected that your environment will not be identical to this configuration and/or requirements setup, so a fundamental knowledge of NetScaler and Microsoft Exchange 2013 is suggested. This configuration will work for Exchange 2007 and Exchange 2010 with changes to the service monitoring configurations, but that is not covered in this guide. It is expected that this configuration will work with Exchange 2016, but there are no guarantees.

About the Author

Ted Joffs, is a Citrix Certified Associate & Professional for NetScaler and has deployed a myriad of NetScaler deployments for Load Balancing for Exchange, SharePoint, Websites, VMware Horizon View as well as deployments for GSLB, KCD, Link Load Balancing, XenApp/XenDesktop Gateway, VPN Gateway, and Traffic Acceleration. He works in the industry as a consultant, however this configuration guide and any statements of the author do not reflect the opinions or viewpoints of his employer, Citrix, VMware, Microsoft, or any other entities mentioned.

About You

It is recommended that you be familiar with Citrix NetScalers, Microsoft Exchange, and various authentication mechanisms to deploy this type of environment. While this guide can be used to deploy Microsoft Exchange via a NetScaler, the reality is that you will need to understand the terminology, command parameters, and other aspects of technology quite well if you are going to deploy this in your own environment. If you do not have that understanding, I would advise contacting Citrix or a consultant you feel comfortable with to deploy your NetScaler based Exchange environment to ensure that it meets your needs.

Acknowledgments

A significant portion of this document related to KCD/SSO is based on community provided works from Rafyel G. Brooks published on August 8, 2014.

Notes

- For this guide, the following SSL Certificate key-pairs were installed:
  - PUB-ROOT-CA
  - PUB-INTER-CA
  - PUB-SSL-WILD
  - PRIV-ROOT-CA
  - PRIV-INTER-CA
  - PRIV-SSL-WILD (Installed; Not Used)
- For this guide, the following URLs are used and DNS entries have been pre-created for them. These do not exist outside the lab environment. There are different ways to configure these, your requirements may vary. Note, the KCD/AAA URL is NOT externally facing in this configuration.
  - External & Internal Exchange URL: webmail.tedjoffs.com (VIP: 172.16.10.50)
  - External Exchange URL: autodiscover.tedjoffs.com (VIP: 172.16.10.50)
  - Internal KCD/AAA URL: kcdaaa.tedjoffs.com (VIP: 172.16.10.11)
- It is important to note that the configuration for the following Exchange Virtual Directories should be case sensitive when configured in Exchange. While the NetScaler is intended to not be case sensitive in CSS policies we are defining here, experience has shown the opposite with certain code versions. If you have a monitor failing, check these. The default cases used for this configuration are:
  - /owa (Outlook Web Access)
  - /ecp (Exchange Control Panel)
  - /ews (Exchange Web Service)
  - /Microsoft-Server-ActiveSync (ActiveSync Service)
  - /oab (Offline Address Book)
  - /rpc (Outlook Anywhere)
  - /Autodiscover (Autodiscover Service)
- The following IP Address were used for this configuration:
  - 172.16.10.50 – Exchange CSS/Redirect VIP
  - 172.16.10.11 – KCD AAA VIP
  - 172.16.10.10 – DNS VIP
  - 10.150.10.10 – Internal DNS Server & AD Server
  - 10.150.10.11 – Internal DNS Server & AD Server
  - 10.150.10.20 – Internal Exchange CAS Server
  - 10.150.10.21 – Internal Exchange CAS Server

Configuration

Configure Global Parameters

Generally, in deploying a NetScaler, they are configured with basic TCP/HTTP performance baselines. As a best practice, configure the NetScalers for:

- Selective Acknowledgement (SACK); optimize TCP retransmits.
- Window Scaling; optimize effective bandwidth in TCP streams.
- Nagle's Algorithm; optimize small packets. Proceed cautiously here. This can impact LAGRE data stream transmissions.
- Drop Invalid Requests; basic Layer 7 DDoS attack prevention and optimization.

Note: As an alternative, you can create custom TCP profiles to apply to your LB VIPs. That is not covered here.

Commands:

```
set ns tcpProfile nstcp_default_profile -WS ENABLED -SACK ENABLED -WSVal 8 -nagle ENABLED -bufferSize 81900 -sendBuffsize 81900
set ns httpProfile nshttp_default_profile -dropInvalReqs ENABLED
```

Enable Features

To deploy this configuration, you will need to have the following features enabled:

- AAA
- CS
- LB
- REWRITE
- RESPONDER
- SSL

Commands:

```
enable ns feature LB CS AAA REWRITE RESPONDER SSL
```

Configure Firewall(s)

To make this stuff work, the firewalls have to be configured correctly. Use the following table to configure your firewall. Actual commands to perform these configurations are way beyond the scope of this document.

Port	Protocol	Purpose	Source	Destination
53	UDP & TCP	DNS	SNIP	Internal DNS Servers
88	UDP & TCP	Kerberos	SNIP	AD Servers
123	UDP	NTP	SNIP	Time Servers
135	TCP	RPC Endpoint Mapper	SNIP	AD, DNS, Time, & Exchange Servers
137	UDP	NetBIOS Name Service	SNIP	AD, DNS, & Exchange Servers
139	TCP	NetBIOS Session*	SNIP	AD & Exchange Servers
389	UDP & TCP	LDAP**	SNIP	AD Servers
445	TCP	SMB TCP	SNIP	AD & Exchange Servers
464	UDP & TCP	Kerberos Password Updates	SNIP	AD Servers
3268	TCP	LDAP GC**	SNIP	AD Servers
80	HTTP	Web Traffic	Internet	CSS VIP IP
443	HTTPS	Secure Web Traffic	Internet	CSS VIP IP
443	HTTPS	Secure Web Traffic	Internet	External AAA VIP IP

*Do NOT open this port from the Internet to anything.
**If using LDAP SSL, this will be different.

Configure DNS A-Records

Create DNS A-Records for your internal domain name; one for each DNS server you are using. In this configuration the internal and external domain name are the same; they may not be in your configuration.

Commands:

```
add dns addRec tedjoffs.com 10.150.10.10
add dns addRec tedjoffs.com 10.150.10.11
```

Configure NTP

It may have been mentioned above, but time is the most critical component to making Kerberos work. Make certain your time is in sync through your domain/network and make sure the time on the NetScaler is correct along with the time zone. The NTP server information is NOT stored in the standard NetScaler configuration file; only the time zone is.

Commands:

```
set ns param -timezone "GMT-05:00-CDT-America/Phoenix"
add ntp server 10.150.10.10 -minpoll 6 -maxpoll 10
add ntp server 10.150.10.11 -minpoll 6 -maxpoll 10
enable ntp sync
```

Configure Exchange CAS Servers

To actually make Kerberos Constrained Delegation (KCD) work, there need to be a few changes in Exchange. Perform these changes, as appropriate, in your environment. Every deployment and environment is slightly different, so you will need to make the appropriate configurations for your setup as noted here. Each change MUST be completed on all the CAS servers in the deployment that will be part of this solution.

- Configure OWA ActiveSync Virtual Directory for Integrated Windows Authentication
- Setup Client Certificate Mapping for ActiveSync (IIS)
- Enable 'Negotiate,NTLM' Providers (IIS)

Create KCD Service Account(s)

You will need at least one KCD Service Account in the AD with the appropriate permissions configured. If you are running multiple sites (e.g. Global Site Load Balancing) you may want a separate KCD account for each site for security, tracking, and logging purposes. The service account you create in Active Directory will need to be a standard user account; Domain Administrator rights are no longer required. For this deployment, the account 'SVCKCDUser' was created.

Configure SPN/Delegation Rights

Perform the following steps to configure the SPN/Delegation rights for the KCD Service Account(s).

- Logon to a Domain Controller; launch an Administrative Command Prompt.
- Create an SPN that will enable the Delegation tab on the KCD Service Account(s) in Active Directory with the command:
    - *setspn -A host/webmail.tedjoffs.com tedjoffs.com\SVCKCDUser*
- Open the user account(s) in Active Directory Users and Computers.
- On the Delegation tab, select the radio buttons 'Trust this user for delegation to specified services on' and 'Use any authentication protocol'.
- Click the Add button and enter the name of each of your Exchange CAS servers that will be servicing ActiveSync for that site with the service type as "HTTP".
- Click OK to close the window.

Generate Keytab File

A Keytab is a file containing pairs of Kerberos principals and encrypted keys derived from the Kerberos password. This is used to authenticate to various remote systems using Kerberos without entering a password for a user or computer account. For this deployment, we are using a user account type, however this can be configured using a computer account should it be desired. Keytab files are a potential security risk if left in the wild, so it is important to secure any copies of the Keytab file for security purposes. To generate the Keytab file, the follow tasks should be performed.

- Edit the following script to fit your environment, and run it on a Domain Controller in and Administrative Command Prompt:
    - *ktpass /princ host/webmail.tedjoffs.com@tedjoffs.com / type KRB5_NT_PRINCIPAL /mapuser tedjoffs.com\SVCKCDUser /pass Password1 -out C:\kcdvserver.keytab*
- Once run, copy the C:\kcdvserver.keytab file to the /nsconfig/krb directory on the NetScaler using WinSCP.

Create NetScaler KCD Account

Command:

```
add aaa kcdAccount SVCKCDUser -keytab "/nsconfig/krb/ns_kcd_msync.keytab"
```

Create Base Policies

Traffic Management

add tm sessionAction SPRO-KCD-SSO -sessTimeout 43829 -defaultAuthorizationAction ALLOW -SSO ON -ssoCredential PRIMARY -ssoDomain TEDJOFFS.COM -httpOnlyCookie YES -kcdAccount SVCKCDUser -persistentCookie ON -persistentCookieValidity 43828
add tm sessionPolicy SPOL-KCD-SSO ns_true SPRO-KCD-SSO

Responder

add responder action RA-EXCH-REDIRECT redirect "\"https://\" + HTTP.REQ.HOSTNAME.HTTP_URL_SAFE + HTTP.REQ.URL.PATH_AND_QUERY.HTTP_URL_SAFE" -responseStatusCode 302
add responder action RA-EXCH-REDIRECT-OWA redirect "\"/owa\"" -responseStatusCode 302
add responder policy RP-EXCH-REDIR HTTP.REQ.IS_VALID RA-EXCH-REDIRECT RESET
add responder policy RP-EXCH-REDIR-OWA "HTTP.REQ.URL.PATH.EQ(\"/\")" RA-EXCH-REDIRECT-OWA RESET
set responder param -undefAction NOOP

Create Servers

Exchange

The Exchange CAS servers you add to the NetScaler MUST be DNS based, and not IP based for the ActiveSync to work. The exchange servers in this configuration are tkjex01 (10.150.10.21) and tkjex02 (10.150.10.21); they should have DNS entries created that can be resolved from the NetScaler.

Commands:

add server SRV-TKJEX01 TKJEX01.TEDJOFFS.COM
add server SRV-TKJEX01 TKJEX01.TEDJOFFS.COM

DNS

add server SRV-TKJDNS01 10.150.10.10
add server SRV-TKJDNS02 10.150.10.11

Create Custom Monitors

DNS

Command:

add lb monitor DNS-TCP MON-DNS-TCP -query . -queryType Address -LRTM DISABLED

Exchange

Commands:

add lb monitor MON-EXCHANGE-OWA HTTP-ECV -send "GET /owa/healthcheck.htm" -recv "200 OK" -LRTM ENABLED -interval 30 -resptimeout 5 -secure YES
add lb monitor MON-EXCHANGE-ECP HTTP-ECV -send "GET /ecp/healthcheck.htm" -recv "200 OK" -LRTM ENABLED -interval 30 -secure YES
add lb monitor MON-EXCHANGE-EWS HTTP-ECV -send "GET /ews/healthcheck.htm" -recv "200 OK" -LRTM ENABLED -interval 30 -secure YES
add lb monitor MON-EXCHANGE-OAB HTTP-ECV -send "GET /oab/healthcheck.htm" -recv "200 OK" -LRTM ENABLED -interval 30 -secure YES
add lb monitor MON-EXCHANGE-RPC HTTP-ECV -send "GET /rpc/healthcheck.htm" -recv "200 OK" -LRTM ENABLED -interval 30 -secure YES
add lb monitor MON-EXCHANGE-EAS HTTP-ECV -send "GET /microsoft-server-activesync/healthcheck.htm" -recv "200 OK" -LRTM ENABLED -interval 30 -secure YES
add lb monitor MON-EXCHANGE-AUT HTTP-ECV -send "GET /autodiscover/healthcheck.htm" -recv "200 OK" -LRTM ENABLED -interval 30 -secure YES
add lb monitor MON-EXCHANGE-EAS HTTP-ECV -send "GET /microsoft-server-activesync/healthcheck.htm" -recv "200 OK" -LRTM ENABLED -interval 30 -secure YES

Local Ping

This monitor will be used for redirection of the root path and non-secure traffic.

Command:

add lb monitor MON-LOCAL-PING PING -LRTM DISABLED -destIP 127.0.0.1

Create and Bind Service Groups & Services

This can also be done with individual services, should you desire more work.

DNS

Commands:

add serviceGroup SGV-DNS-UDP DNS -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport NO -cltTimeout 120 -svrTimeout 120 -CKA NO -TCPB NO -CMP NO
add serviceGroup SGV-DNS-TCP DNS_TCP -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO
bind serviceGroup SGV-DNS-UDP SRV-TKJDNS01 53
bind serviceGroup SGV-DNS-UDP SRV-TKJDNS02 53
bind serviceGroup SGV-DNS-UDP -monitorName dns
bind serviceGroup SGV-DNS-TCP SRV-TKJDNS01 53
bind serviceGroup SGV-DNS-TCP SRV-TKJDNS02 53
bind serviceGroup SGV-DNS-TCP -monitorName DNS-TCP

Exchange

Commands:

```
add serviceGroup SG-EXCHANGE-OWA SSL -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP YES
add serviceGroup SG-EXCHANGE-ECP SSL -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP YES
add serviceGroup SG-EXCHANGE-EWS SSL -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP YES
add serviceGroup SG-EXCHANGE-OAB SSL -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP YES
add serviceGroup SG-EXCHANGE-RPC SSL -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP YES
add serviceGroup SG-EXCHANGE-AUT SSL -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP YES
add serviceGroup LB-EXCHANGE-EAS SSL -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO
bind serviceGroup SG-EXCHANGE-OWA SRV-TKJEX01 443
bind serviceGroup SG-EXCHANGE-OWA SRV-TKJEX02 443
bind serviceGroup SG-EXCHANGE-OWA -monitorName MON-EXCHANGE-OWA
bind serviceGroup SG-EXCHANGE-ECP SRV-TKJEX01 443
bind serviceGroup SG-EXCHANGE-ECP SRV-TKJEX02 443
bind serviceGroup SG-EXCHANGE-ECP -monitorName MON-EXCHANGE-ECP
bind serviceGroup SG-EXCHANGE-EWS SRV-TKJEX01 443
bind serviceGroup SG-EXCHANGE-EWS SRV-TKJEX02 443
bind serviceGroup SG-EXCHANGE-EWS -monitorName MON-EXCHANGE-EWS
bind serviceGroup SG-EXCHANGE-OAB SRV-TKJEX01 443
bind serviceGroup SG-EXCHANGE-OAB SRV-TKJEX02 443
bind serviceGroup SG-EXCHANGE-OAB -monitorName MON-EXCHANGE-OAB
bind serviceGroup SG-EXCHANGE-RPC SRV-TKJEX01 443
bind serviceGroup SG-EXCHANGE-RPC SRV-TKJEX02 443
bind serviceGroup SG-EXCHANGE-RPC -monitorName MON-EXCHANGE-RPC
bind serviceGroup SG-EXCHANGE-AUT SRV-TKJEX01 443
bind serviceGroup SG-EXCHANGE-AUT SRV-TKJEX02 443
bind serviceGroup SG-EXCHANGE-AUT -monitorName MON-EXCHANGE-AUT
bind serviceGroup LB-EXCHANGE-EAS SRV-TKJCHIEX01 443
bind serviceGroup LB-EXCHANGE-EAS SRV-TKJCHIEX02 443
bind serviceGroup LB-EXCHANGE-EAS -monitorName MON-EXCHANGE-EAS
```

Local Ping/Always Up

Command:

```
add service SV-ALWAYS-UP 1.2.3.4 HTTP 80 -maxClient 0 -maxReq 0 -cip DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP YES
bind service SV-ALWAYS-UP -monitorName MON-LOCAL-PING
```

Create and Bind Load Balancing VIP Servers

DNS

The DNS VIPs are created with IP addresses assigned. They should be assigned in the DMZ space, but should not be NATed through from the public side of the firewall.

Commands:

```
add lb vserver LB-DNS-UDP DNS 172.16.10.10 53 -persistenceType NONE -cltTimeout 120
add lb vserver LB-DNS-TCP DNS_TCP 172.16.10.10 53 -persistenceType NONE -cltTimeout 180
bind lb vserver LB-DNS-UDP SGV -DNS-UDP
bind lb vserver LB-DNS-TCP SGV-DNS-TCP
```

Authentication

Commands:

```
add authentication certAction AAA-CA-KCD -userNameField SubjectAltName:PrincipalName
add authentication certPolicy AAA-CPOL-KCD ns_true AAA-CA-KCD
add authentication vserver AAA-LB-EXCH-KCD SSL 172.16.10.11 443 -AuthenticationDomain TEDJOFFS.COM
add authentication authnProfile AAA-AP-KCD -authnVsName AAA-LB-EXCH-KCD -AuthenticationHost kcdaaa.tedjoffs.com -AuthenticationDomain TEDJOFFS.COM
bind authentication vserver AAA-LB-EXCH-KCD -policy AAA-CPOL-KCD -priority 130
bind authentication vserver AAA-LB-EXCH-KCD -policy SPOL-KCD-SSO -priority 100
```

Exchange

Because the Exchange services will be managed by a Content Switching LB VIP, they are created without IPs, meaning that they are not directly accessible. The Content Switching LB VIP will be responsible for delivering the traffic to the standard Load Balancing VIPs.

Commands:

```
add lb vserver LB-EXCHANGE-OWA SSL 0.0.0.0 0 -persistenceType NONE -cltTimeout 180
add lb vserver LB-EXCHANGE-ECP SSL 0.0.0.0 0 -persistenceType NONE -cltTimeout 180
add lb vserver LB-EXCHANGE-EWS SSL 0.0.0.0 0 -persistenceType NONE -cltTimeout 180
add lb vserver LB-EXCHANGE-OAB SSL 0.0.0.0 0 -persistenceType NONE -cltTimeout 180
add lb vserver LB-EXCHANGE-RPC SSL 0.0.0.0 0 -persistenceType NONE -cltTimeout 180
add lb vserver LB-EXCHANGE-AUT SSL 0.0.0.0 0 -persistenceType NONE -cltTimeout 180
add lb vserver LB-EXCHANGE-REDIR HTTP 172.16.10.50 80 -persistenceType NONE -cltTimeout 180
add lb vserver LB-EXCHANGE-EAS SSL 0.0.0.0 0 -persistenceType SOURCEIP -timeout 30 -backupPersistenceTimeout 540 -cltTimeout 180 -authn401 ON -authnVsName AAA-LB-EXCH-KCD
bind lb vserver LB-EXCH-REDIR SV-ALWAYS-UP
bind lb vserver LB-EXCHANGE-OWA SG-EXCHANGE-OWA
bind lb vserver LB-EXCHANGE-ECP SG-EXCHANGE-ECP
bind lb vserver LB-EXCHANGE-EWS SG-EXCHANGE-EWS
bind lb vserver LB-EXCHANGE-OAB SG-EXCHANGE-OAB
bind lb vserver LB-EXCHANGE-RPC SG-EXCHANGE-RPC
bind lb vserver LB-EXCHANGE-AUT SG-EXCHANGE-AUT
bind lb vserver LB-EXCHANGE-EAS LB-EXCHANGE-EAS
bind lb vserver LB-EXCH-REDIR -policyName RP-EXCH-REDIR -priority 100 -gotoPriorityExpression END -type REQUEST
```

Create and Bind Content Switch Load Balancing VIP Server

The Content Switch LB VIP is the key to making everything work. To make the Content Switch VIP first create the policies and actions then bind them to the newly created CSS LB VIP.

Note: This build differs from most configurations available on the Internet as the configuration here does not use the standard 'hostname' based policy for autodiscover. This is done to avoid case sensitivity and to provide the ability for autodiscover to be more discoverable.

Policies and Actions

Commands:

```
add cs action CSA-EXCHANGE-OWA -targetLBVserver LB-EXCHANGE-OWA
add cs action CSA-EXCHANGE-ECP -targetLBVserver LB-EXCHANGE-ECP
add cs action CSA-EXCHANGE-EWS -targetLBVserver LB-EXCHANGE-EWS
add cs action CSA-EXCHANGE-OAB -targetLBVserver LB-EXCHANGE-OAB
add cs action CSA-EXCHANGE-RPC -targetLBVserver LB-EXCHANGE-RPC
add cs action CSA-EXCHANGE-AUT -targetLBVserver LB-EXCHANGE-AUT
add cs action CSA-EXCHANGE-EAS -targetLBVserver LB-EXCHANGE-EAS
add cs policy CSP-EXCHANGE-OWA -rule "HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE).CONTAINS(\"/owa\")" -action CSA-EXCHANGE-OWA
add cs policy CSP-EXCHANGE-ECP -rule "HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE).CONTAINS(\"/ecp\")" -action CSA-EXCHANGE-ECP
add cs policy CSP-EXCHANGE-EWS -rule "HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE).CONTAINS(\"/ews\")" -action CSA-EXCHANGE-EWS
add cs policy CSP-EXCHANGE-OAB -rule "HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE).CONTAINS(\"/oab\")" -action CSA-EXCHANGE-OAB
add cs policy CSP-EXCHANGE-RPC -rule "HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE).CONTAINS(\"/rpc\")" -action CSA-EXCHANGE-RPC
add cs policy CSP-EXCHANGE-AUT -rule "HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE).CONTAINS (\"/AutoDiscover\")" -action CSA-EXCHANGE-AUT
add cs policy CSP-EXCHANGE-EAS -rule "HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE).CONTAINS(\"/Microsoft-Server-ActiveSync\")" -action CSA-EXCHANGE-EAS
```

Content Switching LB VIP

Commands:

```
add cs vserver CS-GLOBAL-HTTPS SSL 172.16.10.50 443 -cltTimeout 180 -caseSensitive OFF
bind cs vserver CS-GLOBAL-HTTPS -policyName RP-EXCH-REDIR-OWA -priority 10 -gotoPriorityExpression END -type REQUEST
bind cs vserver CS-GLOBAL-HTTPS -policyName CSP-EXCHANGE-OWA -priority 100
bind cs vserver CS-GLOBAL-HTTPS -policyName CSP-EXCHANGE-AUT -priority 110
bind cs vserver CS-GLOBAL-HTTPS -policyName CSP-EXCHANGE-ECP -priority 130
bind cs vserver CS-GLOBAL-HTTPS -policyName CSP-EXCHANGE-EWS -priority 140
bind cs vserver CS-GLOBAL-HTTPS -policyName CSP-EXCHANGE-OAB -priority 160
bind cs vserver CS-GLOBAL-HTTPS -policyName CSP-EXCHANGE-RPC -priority 170
bind cs vserver CS-GLOBAL-HTTPS -policyName CSP-EXCHANGE-EAS -priority 180
```

Bind SSL Certificates

Now that everything is built, it is necessary to bind the SSL Certificates to the LB VIPs, Content Switches, and Authentication VIP.

Commands:

```
bind ssl vserver LB-EXCHANGE-OWA -certkeyName PUB-SSL-WILD
bind ssl vserver LB-EXCHANGE-ECP -certkeyName PUB-SSL-WILD
bind ssl vserver LB-EXCHANGE-EWS -certkeyName PUB-SSL-WILD
bind ssl vserver LB-EXCHANGE-OAB -certkeyName PUB-SSL-WILD
bind ssl vserver LB-EXCHANGE-RPC -certkeyName PUB-SSL-WILD
bind ssl vserver LB-EXCHANGE-AUT -certkeyName PUB-SSL-WILD
bind ssl vserver LB-EXCHANGE-EAS -certkeyName PUB-SSL-WILD
bind ssl vserver LB-EXCHANGE-EAS -certkeyName PRIV-INTER-CA -ocspCheck Optional
bind ssl vserver LB-EXCHANGE-EAS -certkeyName PRIV-ROOT-CA -CA -ocspCheck Optional
bind ssl vserver AAA-LB-EXCH-KCD -certkeyName PUB-SSL-WILD
bind ssl vserver AAA-LB-EXCH-KCD -certkeyName PRIV-INTER-CA -CA -ocspCheck Optional
bind ssl vserver AAA-LB-EXCH-KCD -certkeyName PRIV-ROOT-CA -CA -ocspCheck Optional
bind ssl vserver CS-GLOBAL-HTTPS -certkeyName PUB-SSL-WILD
```

Security Enhancements

Everything should be working now, provided that the appropriate IP Addresses, Domain Names, SSL Certificates, and Service Accounts were used. There is however some final security work that should be done to enhance the security and protect the environment from known issues – specifically with SSL.

Cipher Groups

The best practice is to create and bind an A-Plus cipher group. The A-Plus cipher group in this document is the best list known to the author at the time of publication. You should, no, MUST VERIFY this and only use secure ciphers.

Commands:

```
add ssl cipher A-PLUS
bind ssl cipher A-PLUS -cipherName TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 -cipherPriority 1
bind ssl cipher A-PLUS -cipherName TLS1.2-ECDHE-RSA-AES128-GCM-SHA256 -cipherPriority 2
bind ssl cipher A-PLUS -cipherName TLS1.2-ECDHE-RSA-AES-256-SHA384 -cipherPriority 3
bind ssl cipher A-PLUS -cipherName TLS1.2-ECDHE-RSA-AES-128-SHA256 -cipherPriority 4
bind ssl cipher A-PLUS -cipherName TLS1-ECDHE-RSA-AES256-SHA -cipherPriority 5
bind ssl cipher A-PLUS -cipherName TLS1-ECDHE-RSA-AES128-SHA -cipherPriority 6
bind ssl cipher A-PLUS -cipherName TLS1.2-DHE-RSA-AES256-GCM-SHA384 -cipherPriority 7
bind ssl cipher A-PLUS -cipherName TLS1.2-DHE-RSA-AES128-GCM-SHA256 -cipherPriority 8
bind ssl cipher A-PLUS -cipherName TLS1-DHE-RSA-AES-256-CBC-SHA -cipherPriority 9
bind ssl cipher A-PLUS -cipherName TLS1-DHE-RSA-AES-128-CBC-SHA -cipherPriority 10
bind ssl cipher A-PLUS -cipherName TLS1-AES-256-CBC-SHA -cipherPriority 11
bind ssl cipher A-PLUS -cipherName TLS1-AES-128-CBC-SHA -cipherPriority 12
bind ssl cipher A-PLUS -cipherName SSL3-DES-CBC3-SHA -cipherPriority 13
bind ssl vserver LB-EXCHANGE-OWA -cipherName A-PLUS
bind ssl vserver LB-EXCHANGE-ECP -cipherName A-PLUS
bind ssl vserver LB-EXCHANGE-EWS -cipherName A-PLUS
bind ssl vserver LB-EXCHANGE-OAB -cipherName A-PLUS
bind ssl vserver LB-EXCHANGE-RPC -cipherName A-PLUS
bind ssl vserver LB-EXCHANGE-AUT -cipherName A-PLUS
bind ssl vserver LB-EXCHANGE-EAS -cipherName A-PLUS
bind ssl vserver AAA-LB-EXCH-KCD -cipherName A-PLUS
```

Disable SSLv3

There are various security problems with SSLv3 so this configuration disables that SSL protocol by default. Again, this document is NOT a guarantee; you MUST verify this along with any and all other ciphers, protocols, and configurations deployed as part of this configuration and as part of your NetScaler in general!

Commands:

```
set ssl vserver LB-EXCHANGE-OWA -ssl3 DISABLED
set ssl vserver LB-EXCHANGE-ECP -ssl3 DISABLED
set ssl vserver LB-EXCHANGE-EWS -ssl3 DISABLED
set ssl vserver LB-EXCHANGE-OAB -ssl3 DISABLED
set ssl vserver LB-EXCHANGE-RPC -ssl3 DISABLED
set ssl vserver LB-EXCHANGE-AUT -ssl3 DISABLED
set ssl vserver LB-EXCHANGE-EAS -sessReuse ENABLED -sessTimeout 1800 -clientAuth ENABLED -clientCert Mandatory -ssl3 DISABLED
set ssl vserver AAA-LB-EXCH-KCD -clientAuth ENABLED -clientCert Mandatory -ssl3 DISABLED
set ssl vserver CS-GLOBAL-HTTPS -ssl3 DISABLED
```

Test

At this point, you should be able to test your configuration for ActiveSync (based on user certificate KCD), OWA, AutoDiscover, and HTTPS over RPC.