

Deployment Guide

AX Series with Microsoft Exchange Server 2010





Table of Contents

DEPLOYMENT GUIDE

AX Series with Microsoft Exchange Server 2010

1.	Intr	oduction	
	1.1	Prerequisites and Assumptions	4
2.	AX	Deployment for Exchange Server 2010 Roles	5
	2.1	Lab diagram	6
	2.2	AX Configuration Summary	7
		2.2.1 AX Configuration Summary - Exchange Client Access Roles	7
		2.2.2 AX Configuration Summary - Exchange Edge Transport Server Role	9
	2.3	Exchange Client Access Role - Outlook Web App	
		2.3.1 AX Configuration	
		2.3.2 Configuration Validation	
	2.4	Exchange Client Access Role – Exchange Control Panel	
		2.4.1 AX Configuration	24
		2.4.2 Configuration Validation	
	2.5	Exchange Client Access Role - Outlook Anywhere	25
		2.5.1 AX Configuration	25
		2.5.2 Configuration Validation	
	2.6	Exchange Client Access role – Exchange ActiveSync	
		2.6.1 AX Configuration	
		2.6.2 Configuration Validation	
	2.7	Exchange Client Access Roles – RPC	
		2.7.1 AX Configuration	
		2.7.2 Configuration Validation	42
	2.8	Exchange Client Access Roles – POP3	43
		2.8.1 AX Configuration	43
		2.8.2 Configuration Validation	47
	2.9.	Exchange Client Access Roles – IMAP4	49
		2.9.1 AX Configuration	49
		2.9.2 Configuration Validation	53
	2.10	Exchange Client Access role – Exchange Web Services	54
		2.10.1 AX Configuration	54
		2.10.2 Configuration Validation	54
	2.11	Exchange Client Access role – Autodiscover	55
		2.11.1 AX Configuration	55
		2.11.2 Configuration Validation	55
	2.12	Exchange Client Access role – Offline Address Book distribution	56
		2.12.1 AX Configuration	56
		2.12.2 Configuration Validation	56
	2.13	Exchange Edge Transport Server Role - SMTP	57
		2.13.1 AX Configuration	57
		2.13.2 Configuration Validation	60
	2.14	Multiple Exchange Services with a Single VIP	62

	2.14.1	AX Configuration with 1 VIP for OWA + OA + EAS Services Hosted on the	
		Same Exchange Servers	62
	2.14.2	AX Configuration with 1 VIP for OWA + OA + EAS Services Hosted on	
		Different Exchange Servers	64
	2.14.3	Configuration Validation	69
3. Sur	nmar	y and Conclusion	70
A. Ap	pend	ix - AX configuration	71
A.1.	Exchan	ge Client Access Role – Outlook Web App	
A.2.	Exchan	ge Client Access Role – Exchange Control Panel	72
A.3.	Exchan	ge Client Access Role – Outlook Anywhere	73
A.4.	Exchan	ge Client Access Role – Exchange ActiveSync	74
A.5.	Exchan	ge Client Access Role – RPC	75
A.6.	Exchan	ge Client Access Role – POP3	76
A.7.	Exchan	ge Client Access Role – IMAP4	77
A.8.	Exchan	ge Client Access Role – Exchange Web Services	78
A.9.	Exchan	ge Client Access Role – Autodiscover	79
A.10). Exchan	ge Client Access Role – Offline Address Book distribution	80
A.11	L. Exchan	ge Client Access Role – SMTP	80
A.12	2. Exchan	ge Client Access Role – Multiple Exchange Services with a Single VIP (OWA + OA + EAS +	
	and so	on on same servers)	81
A.13	3. Exchan	ge Client Access Role – Multiple Exchange Services with a Single VIP (OWA + OA + EAS	
	and so	on on different servers)	82
A.14	1. Exchan	ge Client Access Role – Multiple Exchange Services with a Single VIP (OWA + OA + EAS +	
	RPC + S	SMTP on on same servers)	83
A.15	5. aFleX so	ript to block specific services(Optional)	86
A.16	5. aFleX p	ersistence script(Optional)	87



1. Introduction

Microsoft Exchange Server is the cornerstone of Microsoft's Unified Communications solution, offering a flexible and reliable messaging platform. Exchange's major features consist of electronic mail, calendaring, contacts and tasks; support for mobile and web-based access to information; and support for data storage.

To reply to the different enterprise needs, Exchange Server has different roles:

- Client Access Server a front-end server that receives end-user requests (Outlook, webmail clients, mobile devices, etc.)
- Edge Transport server role handles all Internet-facing mail flow to minimize the attack surface
- Hub Transport roles responsible for all internal mail flows
- · Mailbox role Exchange databases within which the user mailboxes are contained
- Unified Messaging role merge VoIP infrastructure with your Exchange organization

For more information on Microsoft Exchange Server, visit: http://www.microsoft.com/exchange/2010/en/us/default.aspx

Adding the **AX Series** to all your Microsoft Exchange Server deployments provides the following benefits:

- Higher Scalability enterprises can provide Exchange services to a very high number of employees, load balancing them among multiple Exchange servers in parallel
- High Availability Exchange services are guaranteed even if an Exchange Server goes offline
- Higher Performance end users access their Exchange services faster thanks to multiple Exchange server optimizations such as, but not limited to, compression and SSL offload
- · Higher Security protects services from DDoS attacks
- · Higher flexibility different Exchange services can be accessible via the same public VIP

This deployment guide contains configuration procedures for AX Series application delivery controllers and server load balancers, to support a Microsoft Exchange Server 2010 solution.

1.1 Prerequisites and Assumptions

- The A10 Networks AX Series device should be running software version 2.4.3 or later.
- It is assumed that readers have some basic configuration familiarity with both the AX Series and Microsoft Exchange Server.
- All AX integration modes are supported (routed mode, one-arm mode and transparent modes). The examples in this deployment guide use routed mode.
- Both IPv4 and IPv6 are supported. The examples in this deployment guide use IPv4. Note: There are some limitations on IPv6 support for Microsoft Exchange 2010: http://technet. microsoft.com/en-us/library/gg144561.aspx



2. AX Deployment for Exchange Server 2010 Roles

Exchange has two roles when front ending end users, the Client Access Server role and the Edge Transport server role.

The Client Access Server role accepts connections to your Exchange 2010 server from different clients such as, but not limited to, Microsoft Outlook.

The five Client Access modes are:

- Outlook Web App (OWA) access your email from any Web browser
- Outlook Anywhere access your email from the Internet using Microsoft Outlook Messaging API (MAPI) over HTTP
- ActiveSync synchronize email between your mobile phone and Exchange 2010
- Remote Procedure Call (RPC) Client Access access your email via Microsoft Outlook MAPI
- · POP3/IMAP4 access your email from standard email clients

And the Client Access mode also offers different services:

- Exchange Web Services (EWS) offers web services API
- · Autodiscover simplify user's profile configuration
- Offline Address Book (OAB) distribution OAB access via web-based distribution for Outlook clients

The Edge Transport server role performs anti-spam and antivirus filtering, and applies messaging and security policies to messages in transport.

This chapter gives you step-by-step procedures for each mode.



2.1 Lab diagram

The following diagram shows the network used for the configuration procedures.



Figure 1: AX – Exchange Server 2010 lab diagram



2.2 AX Configuration Summary

2.2.1 AX Configuration Summary - Exchange Client Access Roles

The following table summarizes the AX configuration for each Exchange Client Access role. For more information on step-by-step configuration, see the configuration sections later in this document.

Client Access Role	Real Servers	Health Moni- tor	VIP	Other
Outlook Web App	IP: Exchange Server Port: 443 (no SSL offload) 80 (with SSL offload)	HTTPS (no SSL offload) HTTP (with SSL offload)	 IP: IP accessed by clients Type: HTTPS Port: 443 Persistence: Cookie 	 Optional: Enable HTTP compression Exchange OWA SSL offload HTTP VIP listen to port 80 and transparently redirect HTTP clients to HTTPS Transparently add the "/owa" to requests
Exchange Control Panel	IP: Exchange Server Port: 443 (no SSL offload) 80 (with SSL offload)	HTTPS (no SSL offload) HTTP (with SSL offload)	 IP: IP accessed by clients Type: HTTPS Port: 443 Persistence: Cookie 	 Optional: Enable HTTP compression Exchange ECP SSL offload HTTP VIP listen to port 80 and transparently redirect HTTP clients to HTTPS
Outlook Anywhere	IP: Exchange Server Port: 443 (no SSL offload) 80 (with SSL offload)	HTTPS (no SSL offload) HTTP (with SSL offload)	 IP: IP accessed by clients Type: HTTPS Port: 443 Persistence: either aFleX script with persist uie, or Source-IP 	Optional: • Exchange OA SSL offload
Exchange ActiveSync	IP: Exchange Server Port: 443 (no SSL offload) 80 (with SSL offload)	HTTPS (no SSL offload) HTTP (with SSL offload)	 IP: IP accessed by clients Type: HTTPS Port: 443 Persistence: either aFleX script with persist uie, or Source-IP 	Optional: • Exchange EAS SSL offload



RPC	IP: Exchange Server Port: 0 (all TCP)	TCP (port 135)	 IP: IP accessed by clients Type: TCP Port: 0 (wildcard) Persistence: Source-IP 	 Increase TCP aging to a minimum of 3600 seconds (1 hour), or a maximum of 28,800 seconds (8 hours). En- able Reset Forward and Reset Receive Optional:
				 Limit the ports numbers on AX (via ACL) and Exchange servers
POP3	IP: Exchange Server Port: 995 (no SSL offload) 110 (with SSL offload)	ТСР	IP: IP accessed by clients Type: TCP (no SSL offload) SSL-Proxy (with SSL offload) Port: 995 Parsistance: No need	Optional: • Exchange POP3 SSL offload
IMAP4	IP: Exchange Server Port: 993 (no SSL offload) 143 (with SSL offload)	ТСР	IP: IP accessed by clients Type: TCP (no SSL offload) SSL-Proxy (with SSL offload) Port: 993 Persistence: No need	Optional: • Exchange IMAP4 SSL offload
Exchange Web Services (EWS)	IP: Exchange Server Port: 443 (no SSL offload) 80 (with SSL offload)	НТТР	 IP: IP accessed by clients Type: HTTP Port: 80 Persist: Cookie 	 Optional: Enable HTTP compression Exchange EWS SSL offload
Autodiscover	IP: Exchange Server Port: 443 (no SSL offload) 80 (with SSL offload)	НТТР	 IP: IP accessed by clients Type: HTTP Port: 80 Persist: No need 	 Optional: Enable HTTP compression Exchange SSL offload
Offline Address Book (OAB) distribution	See Client Access RPC	See Client Access RPC	See Client Access RPC	See Client Access RPC



Same VIP for multiple services using	IP: Exchange Server Port: 443 (no SSL	HTTPS (no SSL offload)	IP: IP accessed by clients	Optional: Exchange SSL offload
same servers	offload)	HTTP (with SSL offload)	Type: HTTPS	
	80 (with SSL offload)	,	Port : 443	
			Persistence: Source IP	
Same VIP	IP: Exchange Server	HTTPS (no	IP: IP accessed by	Optional:
for multiple services using	Port: 443 (no SSL	SSL offload)	clients	Exchange SSL offload
different	offload)	HTTP (with SSL offload)	Type: HTTPS	
3017013	80 (with SSL		Port: 443	
	onioad)		Persistence: Source-IP	
			aFleX: Select specific service group per client access	

2.2.2 AX Configuration Summary - Exchange Edge Transport Server Role

The following table summarizes the AX configuration for the Exchange Edge Transport Server role. For more information on step-by-step configuration, see the Edge section later in this document.

Client Access Role	Real Servers	Health Moni- tor	VIP	Other
Edge Transport Server	IP: Exchange Server Port: 25	SMTP	 IP: IP accessed by clients Type: TCP Port: 25 Persist: No need 	Optional : Exchange SMTP TLS (STARTTLS) offload



2.3 Exchange Client Access Role - Outlook Web App

Outlook Web App (OWA) offers Exchange mailboxes access through a web browser via HTTPS.

AX provides the following benefits:

· Load Balancing and High Availability of Exchange OWA servers

And can also provide the following optional benefits:

- · HTTP Compression to reduce remote end user response time and data center bandwidth usage
- · SSL offload to reduce CPU and memory usage on Exchange OWA servers
- Transparently redirect HTTP clients to HTTPS
- Transparently add the "/owa" to requests that do not have it

2.3.1 AX Configuration

Note: If the same virtual IP address (VIP) will to be used for Outlook Anywhere or Exchange ActiveSync services, see "2.14 Multiple Exchange Services with a Single VIP".

a. Create Exchange OWA Real Servers

• Create a real server for each Exchange OWA real server. Enter the OWA Name, IP address, and add the Protocol TCP Port 443

General		
Name: *	Exchange1	
IP Address/Host: *	10.0.2.161	IPv4 IPv6
GSLB External IP Address:		
Weight:	1	

• Via Web GUI: Config Mode > Service > SLB > Server

Port:	- 4	43	Proto	col: TCP	• W	leight(\	<u>N):* 1</u>		No SSL	_		O Add
Conn	ectio	n Limit(C	<u>CL):</u> 800000	0 VLog	ing		Connect	tion Resume	e(<u>CR</u>):			🥥 Update
Serve	er Po	rt Templ	ate(SPT):	default		•	Stats Da	ata(<u>SD</u>): •	Enabled OD	isabled		Delete
Healt	h Mo	nitor(<u>HM</u>):	ault)		OF	Follow Por	t	TCP	-		📀 Enable
Exten	ded	Stats(ES): O Enab	led 💿 Disat	led							🖸 Disable
		Port	Protocol	CL	CR	W	No SSL	SPT	HM	SD	ES	
-	-				_	_					-	

Via CLI: AX(config)#slb server Exchange1 10.0.2.161
 AX(config-real server)#port 443 tcp



b. Create Exchange OWA Health Check

- Create a health monitor template to test the availability of the Exchange OWA servers. Enter the health monitor template **Name** and select **Type** HTTPS with **URL** "GET /"
 - Via Web GUI: Config Mode > Service > Health Monitor

Health Monitor		
Name: *	hm-owa-https	
Retry:	3	
Method		
Override IPv4:		
Override IPv6:		
Override Port:		
Method:	Internal © External	
Туре:	HTTPS	
Port:	443	
Host:		
URL:	GET 🔻 /	

 Via CLI: AX(config)#health monitor hm-owa-https AX(config-health:monitor)#method https



c. Create Exchange OWA Service Group

- Create a TCP service group for the Exchange OWA servers. Enter a Name for the service group, select TCP from the Type drop-down list, select the Least Connection load balancing Algorithm, and select the OWA Health Monitor. Assign each Exchange OWA Server to the service group with Port 443
 - Via Web GUI: Config Mode > Service > SLB > Service Group

Service Group				
Name: *	Exchange-OWA-	https		
Туре:	TCP	•		
Algorithm:	Least Connectio	on 🔻		
Health Monitor:	hm-owa-https	*		
Min Active Members:				
Server				
IPv4/IPv6:	IPv4 O IPv6			
Server: *	Exchange2	 Port: * 	443	O Add
Server Port Template(SPT):	default	 Priority: 	1 🔹	🥥 Update
Stats Data:	Enabled Oisab	led		Delete
Server	Port	SPT	Priority Stats Data	🔮 Enable
Exchange1	443	default	1	😢 Disable
Excitative i	440		· · · · · · · · · · · · · · · · · · ·	

 Via CLI: AX(config)#slb service-group Exchange-OWA-https tcp AX(config-slb svc group)#method least-connection AX(config-slb svc group)#health-check hm-owa-https AX(config-slb svc group)#member Exchange1:443 AX(config-slb svc group)#member Exchange2:443

d. Create Exchange OWA Persistence

- Create a cookie persistence template to guarantee each end user will always go to the same Exchange OWA. Enter the persistence template **Name** and select match type server
 - Via Web GUI: Config Mode > Service > Template > Persistent > Cookie Persistence

Cookie Persistence		
Name: *	persist-owa	
Expiration:		Seconds
Cookie Name:		

• Via CLI: AX(config) # slb template persist cookie persist-owa



e. Import the IIS Server Public Certificate/Private Key onto the AX

Note: To export a certificate/key from Microsoft IIS, see http://technet.microsoft.com/en-us/library/ cc731386%28WS.10%29.aspx

- Import the IIS public certificate / private key onto the AX device. Enter a Name for the certificate, select the import method (Local or Remote), and select the Format. Enter or select download settings. (These depend on whether you select Local or Remote)
 - Via Web GUI: Config > Service > SSL Management > Certificate

Import	
Name: *	owa-cert-key
Import Certificate from:	Iccal Remote Text
Certificate Format:	PFX 🔻
Password:	•••
Certificate Source:	C:\Temp\IIS-OWA.pfx Browse_

- Via CLI: AX(config)#slb ssl-load certificate OWA-cert-key type pfx password al0 tftp://10.0.1.10/IIS-OWA.pfx
- Create a client-SSL template. Enter a **Name** for the template, select the **Certificate** and **Key** files, and enter the **Pass Phrase**
 - Via Web GUI: Config > Service > Template > SSL > Client SSL

Client SSL		
Name: *	OWA-Client-Side	
Certificate Name:	owa-cert-key	•
Chain Cert Name:		•
Key Name:	owa-cert-key	+
Cache Size:	0	
Pass Phrase:	•••	
Confirm Pass Phrase:	•••	

- Via CLI: AX(config)#slb template client-ssl OWA-Client-Side AX(config-client ssl)#cert OWA-cert-key AX(config-client ssl)#key OWA-cert-key passphrase al0
- Create a server-SSL template. Enter a Name for the template
 - Via Web GUI: Config > Service > Template > SSL > Server SSL



Server SSL		
Name: *	OWA-Server-Side	
Certificate Name:		•
Key Name:		-
CA Cert Name:		-
TLS/SSL Version:	•	

 $\circ~$ Via CLI: AX(config) # slb template server-ssl OWA-Server-Side

f. Create Exchange OWA VIP

- · Create the virtual IP address (VIP), which is the IP address that end users will access
 - Enter a Name for the VIP, and enter the IP address
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server

General			
Name: *	Exchange-OWA		Wildcard
IP Address or CIDR Subnet: *	10.0.1.74		IPv4 IPv6
Status:	. Enabled	O Disabled	

- Via CLI: AX(config)#slb virtual-server Exchange-OWA 10.0.1.74
- Add port Type HTTPS Port 443 and select the Service Group, Client-SSL Template, Server-SSL template and Persistence Template
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port



Virtual Server Port	
Virtual Server:	Exchange-OWA
Type: *	HTTPS 🗸
Port: *	443
Service Group:	Exchange-OWA-https 👻
Connection Limit:	🖾 8000000 💿 Drop 💿 Reset 🗹 Logging
Client-SSL Template:	OWA-Client-Side
Server-SSL Template:	OWA-Server-Side 🔻
Connection Reuse Template:	
TCP-Proxy Template:	▼
Persistence Template Type:	Cookie Persistence Template 🔹
Cookie Persistence Template:	persist-owa

• Via CLI: AX(config-slb vserver) #port 443 https

```
AX(config-slb vserver-vport)#service-group Exchange-OWA-https
AX(config-slb vserver-vport)#template client-ssl OWA-Client-Side
AX(config-slb vserver-vport)#template server-ssl OWA-Server-Side
AX(config-slb vserver-vport)#template persist cookie persist-owa
```

g. (Optional) Enable HTTP Compression

Create a HTTP template to compress HTTP content. Enter the HTTP template **Name** and enable
 Compression

Note: Keep the **Level** at 1. Increasing the level increases AX CPU usage without much compression benefit.

• Via Web GUI: Config Mode > Service > Template > Application > HTTP

нттр				
Name: *		tp-compress		
Failover URL:				
Strict Transaction Switchin	ıg:	Enabled	Disabled	
Compression				
Compression:	Enabled	Oisabled		
Keep Accept Encoding:	© Enabled	Disabled		
Level:	1(least comp	ression, fastest)	-	

- Via CLI: AX(config)# slb template http tp-compress AX(config-http)#compression enable
- Assign the HTTP compression template to the virtual server
 - Via Web GUI: Config > Service > SLB > Virtual Server > Port



HTTP T	emplate:	tp-compress	+
Via CLI:	AX(config)#slb virtua	al-server Excha	nge-OWA
	AX(config-slb vserve	r)#port 443 htt	ps

AX(config-slb vserver-vport)#template http tp-compress

h. (Optional) Offload SSL on Exchange OWA Servers

With this option end users still use HTTPS to connect to their OWA service, but the AX connects to the OWA servers via HTTP, thus offloading SSL from the servers.

- Create the Port 80 for each Exchange OWA real server
 - Via Web GUI: Config Mode > Service > SLB > Server

	1.511												
Nam	e: *			Excha	ange	1							
IP Ad	dres	ss/Host	*	10.0.2	2.161	1			IP	v4 ◎ IPv6			
GSLE	BExt	ernal II	P Address	s:									
Weig	ght:			1									
Port:	80)	Protoc	col: TCP	,	• We	eight(<u>\</u>	<u>N):</u> 1		No SSL			O Add
Port: Conne Serve	80 ection er Por) h Limit(<u>(</u> t Templ	Protoc (L):800000 ate(<u>SPT</u>):	col: TCP	oggi	• We	eight(\	M): 1 Connect Stats Da	tion Resume ata(<u>SD</u>):	No SSL e(<u>CR</u>): Enabled O D)isabled		 Add Update Delete Stacklash
Port: * Conne Serve Health	80 ection er Por h Mon) h Limit(<u>C</u> t Templa hitor(<u>HM</u>	Protoc <u>(L):</u> 800000 ate(<u>SPT</u>):): (defa	col: TCP 00 VL default ault)	.oggi	• We	eight(<u>\</u> • © F	M): 1 Connect Stats Da Follow Por	tion Resume ata(<u>SD</u>):	No SSL e(<u>CR</u>): Enabled O D)isabled		 Add Update Delete Enable
Port: Conne Serve Health Extend	80 ection r Por h Mon ded S) t Limit(<u>C</u> t Templi itor(<u>HM</u> Stats(<u>E S</u>	Protoc <u>(1):800000</u> ate(<u>SPT</u>): (defi): Enab	col: TCP)0 VL default ault) led OD	oggi	• We	eight(<u>)</u> • © F	W: 1 Connect Stats Da Follow Por	tion Resume ata(<u>SD</u>):	No SSL e(<u>CR</u>): Enabled O D)isabled		 Add Update Delete Enable Disable
Port: * Conne Serve Health Exten	ection r Por h Mon ded S) t Limit(<u>C</u> t Templi hitor(<u>HM</u> Stats(<u>ES</u> Port	Protoc L):800000 ate(<u>SPT</u>):): (defi (defi): Enab Protocol	col: TCP 00 IL default ault) CL	.oggi isable	• We ng • ed CR	eight() • © F	M): 1 Connect Stats Da Follow Por	tion Resum ata(<u>SD</u>): t: SPT	No SSL e(CR): Enabled © D TCP)isabled 	ES	 Add Update Delete Enable Disable
Port: Conne Serve Health Exten	ection r Por h Mon ded S) t Limit(<u>C</u> t Temple hitor(<u>HM</u> Stats(<u>ES</u> Port 443	Protoc CL):800000 ate(<u>SPT</u>):): (defi (defi): Enab Protocol TCP	col: TCP 0 V L default ault) led O Di CL 8000000	isable	• We ng • ed CR	v € V F	M): 1 Connect Stats Da Follow Por No SSL	tion Resum ata(<u>SD</u>): t: SPT default	No SSL e(CR): Enabled © D TCP HM (default))isabled 	ES O	 Add Update Delete Enable Disable

 Via CLI: AX(config)#slb server Exchange1 AX(config-real server)#port 80 tcp

- Create a health monitor template to test the availability of the Exchange OWA servers. Enter the health monitor template Name and select Type HTTP with URL "GET /"
 - Via Web GUI: Config Mode > Service > Health Monitor

Health Monitor	
Name: *	hm-owa-http
Retry:	3



S Method			
Override IPv4:			
Override IPv6:			
Override Port:			
Method:	Internal	External	
Туре:	HTTP		•
Port:	80		
Host:			
URL:	GET 👻 /		

- Via CLI: AX(config) #health monitor hm-owa-http AX(config-health:monitor)#method http
- Create a TCP service group with Exchange OWA servers. Enter a Name for the service group, select TCP from the Type drop-down list, select the load balancing Algorithm Least Connection, and select the OWA Health Monitor. Assign each Exchange OWA Server to the service group with Port 80
 - Via Web GUI: Config Mode > Service > SLB > Service Group

Service Group	
Name: *	Exchange-OWA-http
Туре:	TCP
Algorithm:	Least Connection 👻
Health Monitor:	hm-owa-http 🔻
Min Active Members:	

0	Serve	r								
	IPv4/I	Pv6:		IPv4	IPv6					
	Serve	ег: *		Exchange2		-	Port: *	80		🛈 Add
	Serve	er Por	t Template(<u>SPT</u>):	default		-	Priority:	1	•	🥥 Update
	Stats	Data	:	Enabled	O Disable	ed				Oelete
			Server		Port	SPT		Priority	Stats Data	🔮 Enable
		0	Exchange1		80	default		1	0	😣 Disable
		0	Exchange2		80	default		1	Ø	

 Via CLI: AX(config)#slb service-group Exchange-OWA-http tcp AX(config-slb svc group)#method least-connection AX(config-slb svc group)#health-check hm-owa-http AX(config-slb svc group)#member Exchange1:80 AX(config-slb svc group)#member Exchange2:80



- In the OWA VIP, select the Service Group with HTTP servers
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port

	Service Group:	Exchange-OWA-http 🗸
• Via	A CLI: AX(config AX(config AX(config)#slb virtual-server Exchange-OWA -slb vserver)#port 443 https -slb vserver-vport)#service-group Exchange-OWA-http
In the C	WA VIP remove th	e Server-SSL Template since the AX device will communicate with
the OW	A servers via HTTF a Web GUI: Config I	hinstead of HTTPS Mode > Service > SLB > Virtual Server > Port

- Via CLI: AX(config)#slb virtual-server Exchange-OWA AX(config-slb vserver)#port 443 https AX(config-slb vserver-vport)#no template server-ssl OWA-Server-Side
- Enable SSL offload on the Exchange OWA servers; see http://social.technet.microsoft.com/wiki/contents/articles/how-to-configure-ssl-offloading-in-exchange-2010.aspx

i. (Optional) Transparently Redirect HTTP Clients to HTTPS

By default, end users accessing the Exchange OWA service via HTTP cannot connect since that service must be accessed via HTTPS. With this option, end users accessing the Exchange OWA service via HTTP are transparently redirected to HTTPS.

- Create an HTTP template to redirect all end users to the HTTPS Exchange OWA service. Enter the HTTP template Name and the Failover URL with your Exchange OWA HTTPS access
 - Via Web GUI: Config Mode > Service > Template > Application > HTTP

нттр	
Name: *	tp-redirect-owa-https
Failover URL:	https://mail.example.com/owa
Strict Transaction Switching:	© Enabled

 Via CLI: AX(config)# slb template http tp-redirect-owa-https AX(config-http)# failover-url https://mail.example.com/owa



- In the existing Exchange OWA Virtual Server, add port Type HTTP Port 80 with no Service Group and select the failover HTTP template
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server

Virtual Server Port	
Virtual Server:	Exchange-OWA
Type: *	HTTP 🗸
Port: *	80
Service Group:	
Connection Limit:	🛛 8000000 🔍 Drop 🔍 Reset 🗹 Logging
HTTP Template:	tp-redirect-owa-https

 Via CLI: AX(config-slb vserver)#port 80 http AX(config-slb vserver-vport)#template http tp-redirect-owa-https

j. (Optional) Transparently Add "/owa" to the Requests That Are Without It

By default, end users accessing the Exchange OWA service without specifying "/owa" in the request (i.e., "<u>https://mail.example.com</u>") will access the default IIS page instead of the Exchange OWA service. The AX can transparently add the "/owa" to the requests so they always access the Exchange OWA service.

• Create an aFleX policy to insert the "/owa" in the request if not present. The aFleX policy is:

```
when HTTP_REQUEST {
    # transparently insert "/owa" if not already present
    if {not ([HTTP::uri] starts_with "/owa")} {
        HTTP::uri /owa[HTTP::uri]
    }
}
```

• Via Web GUI: Config > Service > aFleX

aFleX	
Name: *	insert_owa
	<pre>when HTTP_REQUEST { if {not ([HTTP::uri] starts_with "/owa")} { HTTP::uri /owa[HTTP::uri] } }</pre>

 Via CLI: AX(config) #import aflex insert _ owa tftp://10.0.1.10/insert _ owa. txt



- Assign the aFleX policy to the virtual server
 - Via Web GUI: Config > Service > SLB > Virtual Server > Port

aFleX:	insert owa 🔻 🔲 Multiple
Via CLI:	AX(config)#slb virtual-server Exchange-OWA AX(config-slb vserver)#port 443 https AX(config-slb vserver-vport)#aflex insert _owa

2.3.2 Configuration Validation

a. Validate AX Deployment for Exchange OWA Without SSL Offload

Validate the status of the VIP and that its members are UP.

• Via Web GUI: Monitor > Service > SLB > Virtual Server

	Mama		Connections		Packets		Bytes		
~	Name		Current 🏻 🍦	Total 🏻 🍦	Forward 🏻 🍦	Reverse 🍦	Forward 🏻 🍦	Reverse 🍦	
\mathbf{O}	Exchange-OWA/10.0.1.74	Ξ	0	0	0	0	0	0	$\underline{\boxtimes}$
0	HTTPS/443	Ξ	0	0	0	0	0	0	$\underline{\mathbb{X}}$
\odot	443 (Exchange2)		0	0	0	0	0	0	
•	443 (Exchange1)		0	0	0	0	0	0	

• Via CLI: AX#show slb virtual-server Exchange-OWA AX#show slb service-group Exchange-OWA-https AX#show slb server [Exchange1 | Exchange2]



Validate the AX deployment:

Access the Exchange OWA via https://mail.example.com/owa



b. Validate AX Deployment for Exchange OWA with HTTP Compression

Validate there is HTTP compression. Check that the **Total Data After Compression** is lower than the **Data Before Compression**

• Via Web GUI: Monitor > Service > Application > Proxy > HTTP

Statistics for HTTP		Disabl	ed 🔻 💝 Refresh	TClear
	Control CPU	Data CPU1	Data CPU2	Total
Curr Proxy Conns	0	1	1	2
Total Proxy Conns	0	103	100	203
HTTP Requests	0	138	145	283
HTTP Requests(succ)	0	136	143	279
Data Before Compression	0	6.2K	107.5K	113.7K
Data After Compression	0	2.5K	41.8K	44.3K

• Via CLI: AX#show slb http-prox



c. Validate AX deployment for Exchange OWA with SSL Offload

Validate the status of the VIP and that its members are UP.

• Via Web GUI: Monitor > Service > SLB > Virtual Server

	Nama		Connections		Packets		Bytes		
~	name	~	Current 🛛 🍦	Total 🏻 🍦	Forward 🏻 🍦	Reverse 🍦	Forward 🏻 🍦	Reverse 🍦	
\mathbf{O}	Exchange-OWA/10.0.1.74	Ξ	0	0	0	0	0	0	$ \infty $
0	HTTPS/443	Ξ	0	0	0	0	0	0	$[\underline{\mathbb{N}}]$
0	80 (Exchange1)		0	0	0	0	0	0	
\odot	80 (Exchange2)		0	0	0	0	0	0	

• Via CLI: AX#show slb virtual-server Exchange-OWA AX#show slb service-group Exchange-OWA-https AX#show slb server [Exchange1 | Exchange2]

Validate the AX deployment:

• Access the Exchange OWA via <u>https://mail.example.com/owa</u> Same as "Validate AX deployment for Exchange OWA without SSL offload"

d. Validate AX Deployment with Transparent Redirect HTTP Clients to HTTPS

Validate the AX deployment:

Access the Exchange OWA via http://mail.example.com/owa
The end user will be transparently redirected to https://mail.example.com/owa

Technical Note:

The VIP port 80 is associated to no Service Group. So it is expected to have its status under monitor. *Note: The screenshot is from an AX deployment with SSL offload (VIP port 443 is using Exchange OWA servers on port 80).*

• Via Web GUI: Monitor > Service > SLB > Virtual Server

	Nama	4	Conne	ctions	Pack	kets	Byt	es	
V	Name	×	Current 🛛 🍦	Total 🏻 🍦	Forward 🏻 🍦	Reverse 🍦	Forward 🏻 🍦	Reverse 🍦	
0	Exchange-OWA/10.0.1.74	Ξ	0	0	0	0	0	0	$\underline{\boxtimes}$
\mathbf{O}	HTTPS/443	Ξ	0	0	0	0	0	0	$ \infty $
\mathbf{O}	80 (Exchange1)		0	0	0	0	0	0	
\mathbf{O}	80 (Exchange2)		0	0	0	0	0	0	
O	HTTP/80	Ŧ	0	0	0	0	0	0	$ \infty $

• Via CLI: AX#show slb virtual-server Exchange-OWA



e. Validate Exchange OWA access with requests without "/owa"

Validate the AX deployment:

 Access the Exchange OWA via <u>https://mail.example.com</u> and validate you still have access to the Exchange OWA service



2.4 Exchange Client Access Role – Exchange Control Panel

Exchange Control Panel (ECP) is a component of OWA that offers the ability to do Exchange administrative tasks via HTTPS.

AX provides ECP with the same benefits as OWA; in this case:

· Load Balancing and High Availability of Exchange ECP servers

AX can also provide these optional benefits:

- · HTTP Compression to reduce remote end user response time and data center bandwidth usage
- SSL offload to reduce CPU and memory usage on Exchange ECP servers
- Transparently redirect HTTP clients to HTTPS

2.4.1 AX Configuration

Note: If the same VIP will be used for the Outlook Anywhere or Exchange ActiveSync services, see "2.14 Multiple Exchange Services with a Single VIP".

· Same as "Exchange Client Access roles - Outlook Web App"

2.4.2 Configuration Validation

 Same as "Exchange Client Access roles - Outlook Web App" Note: Access "https://mail.example.com/ecp:.



2.5 Exchange Client Access Role - Outlook Anywhere

Outlook Anywhere offers Microsoft Outlook end users with access to their mailboxes via HTTPS when MAPI access is blocked.

AX provides the following benefits:

· Load Balancing and High Availability of Exchange Anywhere servers

And can also provide the optional benefits:

• SSL offload to reduce CPU and memory usage on Exchange Anywhere servers

2.5.1 AX Configuration

Note: If the same VIP will be used for the Client Access Role Outlook Web App or Exchange ActiveSync services, see "2.14 Multiple Exchange Services with a Single VIP".

a. Create Exchange OA real servers

· Same as "Exchange Client Access roles - Outlook Web App"

b. Create Exchange OA health check

 Same as "Exchange Client Access roles - Outlook Web App" Note: Use the Name "hm-oa-https".

c. Create Exchange OA service group

 Same as "Exchange Client Access roles - Outlook Web App" Note: Use the Name "Exchange-OA-https", Algorithm Round-Robin and Health Monitor "hm-oa-https".



d. Create Exchange OA persistence

Note: Outlook is not a standard web browser and does not support cookies. So we cannot use cookie stickiness. The three possible persistency options for Exchange OA are no persistence, Source-IP persistence and aFleX UIE persistence.

No persistence can be selected, but at the cost of performance on the Client Access Servers (<u>http://tech-net.microsoft.com/en-us/library/ff625248.aspx</u>).

aFleX UIE persistence offers better granularity (multiple clients coming through the same proxy with the same IP address will use different servers), but requires Basic Authentication (under Exchange Management Console > Server Configuration > Client Access > Properties):

WIN-1C415FT18MQ Properties				
General System Settings Outlook Anywhere				
To change the state of Outlook Anywhere, click the enable or disable Outlook Anywhere link in the action pane.				
Status: Enabled				
External host na <u>m</u> e:				
mail.dimi.fr				
Client authentication method: Basic authentication NILM authentication Negotiate Ex authentication				
✓ Allow secure channel (SSL) offloading				
OK Cancel Apply Help				

If you can accept Basic authentication for OA, use aFleX UIE persistence, otherwise use source IP persistence.



aFleX UIE persistence configuration:

 Create an aFleX policy to define the Exchange OA persistence rule. The aFleX policy is:

```
when HTTP_REQUEST {
  # Set up variables automatically
  set Authent [HTTP::header "Authorization"]
  # Check if the client has been active in the past 30 minutes
  # Note: AX looks at the HTTP header "Authentication"
  set p [ persist lookup uie $Authent all ]
  if { $p ne "" } {
    # That client has been found in the table
   persist uie $Authent
  } else {
    # That's a new client
  }
}
when HTTP_RESPONSE {
  # Update persist uie table with Client Authent information
 persist add uie $Authent 1800
  log "Add persist entry for client $Authent"
}
```

• Via Web GUI: Config > Service > aFleX

Name: *	persist-oa
Definition: *	<pre>when HTTP_REQUEST { # Set up variables automatically set Authent [HTTP::header "Authorization"] # Check if the client has been active in the past 30 minutes # Note: AX looks at the HTTP header "Authentication" set p [persist lookup uie \$Authent all] if { \$p ne "" } { # That client has been found in the table persist uie \$Authent } else { # That's a new client } }</pre>

• Via CLI: AX(config) #import aflex persist-oa tftp://10.0.1.10/persist-oa.txt



Source IP persistence configuration:

- Create a Source-IP persistence template to guarantee each end user will always go to the same Exchange OA. Enter the persistence template **Name** and increase the **Timeout**
 - Via Web GUI: Config Mode > Service > Template > Persistent > Source IP Persistence

Source IP Persistence	
Name: *	persist-oa
Match Type:	Port 👻
Timeout:	30 Minutes

e. Import the IIS server public certificate / private key onto the AX

Note: You can access your mailboxes even if you do not have a trusted signed certificate with Outlook Web App. (You simply accept the presented untrusted certificate in your browser.) But Outlook will not accept the connection to mail boxes via Outlook Anywhere if the presented certificate is not trusted. So you must have a trusted certificate with Outlook Anywhere.

• Same as "Exchange Client Access roles - Outlook Web App" Note: Use the Certificate Name "oa-cert-key", Client-SSL Template Name "OA-Client-Side" and Server-SSL Template Name "OA-Server-Side".

f. Create Exchange OA VIP

- Create the virtual IP address (VIP), which is the IP address that end users will access
 Enter a Name for the VIP, and enter the IP address
- Via Web GUI: Config Mode > Service > SLB > Virtual Server

General		
Name: *	Exchange-OA	Wildcard
IP Address or CIDR Subnet: *	10.0.1.75	
Status:	. Enabled Disabled	

• Via CLI: AX(config)#slb virtual-server Exchange-OA 10.0.1.75



Via CLI: AX(config)#slb template persist source-ip persist-oa
 AX(config-source ip persist)#timeout 30

- Add port Type HTTPS Port 443 and select the Service Group, aFleX or Source IP Persistence Template, Client-SSL Template, and Server-SSL template
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port

Virtual Server Port	
Virtual Server:	Exchange-OA
Type: *	HTTPS 🔻
Port: *	443
Service Group:	Exchange-OA-https
Connection Limit:	🖾 8000000 💿 Drop 💿 Reset 🗹 Logging
Client-SSL Template:	OA-Client-Side
Server-SSL Template:	OA-Server-Side ▼

If aFleX iue persistency is selected

ariex: persist-oa

If Source IP persistency is selected

Persistence Template Type:	Source IP Persistence Template 🔻
Source IP Persistence Template:	persist-oa 🔹

• Via CLI: AX(config-slb vserver)#port 443 https

AX(config-slb vserver-vport)#service-group Exchange-OA-https AX(config-slb vserver-vport)#template client-ssl OA-Client-Side AX(config-slb vserver-vport)#template server-ssl OA-Server-Side

If aFleX UIE persistence is selected

AX(config-slb vserver-vport)#aflex persist-oa

If Source-IP persistence is selected

AX(config-slb vserver-vport)#template persist source-ip persist-oa



g. (Optional) Offload SSL on Exchange OA servers

With this option, end users still use HTTPS to connect to their Exchange OA service, but the AX connects to the OA servers via HTTP, offloading SSL from the servers.

- Create the port 80 for each Exchange OA real server
 - Same as "Exchange Client Access roles Outlook Web App"
- Create a health monitor template to test the availability of the Exchange OA servers. Enter the health monitor template Name and select Type HTTP with URL "GET /"
 - Same as "Exchange Client Access roles Outlook Web App" Note: Use the Name "hm-oa-http".
- Create a TCP service group with Exchange OA servers. Enter a Name for the service group, select TCP from the Type drop-down list, select the load balancing Least Connection Algorithm, and select the OA Health Monitor. Assign each Exchange OA Server to the service group with Port 80
 - Same as "Exchange Client Access roles Outlook Web App" Note: Use the Name "Exchange-OA-http" and Health Monitor "hm-oa-http".
- In the OA VIP, select the Service Group with HTTP servers
 - Same as "Exchange Client Access roles Outlook Web App" Note: Use the Service Group "hm-oa-http".
- In the OA VIP, remove the Server-SSL Template since the AX will communicate with the OA servers via HTTP instead of HTTPS.
 - · Same as "Exchange Client Access roles Outlook Web App"
- Enable SSL offload on Exchange OA servers; see <u>http://social.technet.microsoft.com/wiki/con-tents/articles/how-to-configure-ssl-offloading-in-exchange-2010.aspx</u>



2.5.2 Configuration Validation

a. Validate AX deployment for Exchange OA without SSL offload

Validate the status of the VIP and the its members are UP.

• Via Web GUI: Monitor > Service > SLB > Virtual Server

	Name 🗧		Connections		Pacl	(ets	Byt		
~			Current 🏻 🍦	Total 🏻 🍦	Forward 🏻 🍦	Reverse 🍦	Forward 🏻 🍦	Reverse 🍦	
\mathbf{O}	Exchange-OA/10.0.1.75	Ξ	0	0	0	0	0	0	×
0	HTTPS/443	Ξ	0	0	0	0	0	0	\mathbb{R}
•	443 (Exchange1)		0	0	0	0	0	0	
\mathbf{O}	443 (Exchange2)		0	0	0	0	0	0	

• Via CLI: AX#show slb virtual-server Exchange-OA AX#show slb service-group Exchange-OA-https AX#show slb server [Exchange1 | Exchange2]

Validate the AX deployment:

 Access the Exchange OA via Outlook Anywhere mode.
 For more information on how to configure Microsoft Outlook, see <u>http://technet.microsoft.com/</u> <u>en-us/library/cc179036.aspx</u>

b. Validate AX deployment for Exchange OA with SSL offload

Validate the status of the VIP and that its members are UP.

• Via Web GUI: Monitor > Service > SLB > Virtual Server

	🔷 Name 🔶		Connections		Pack	kets	Bytes		
- V			Current 🛛 🍦	Total 🏻 🍦	Forward 🏻 🍦	Reverse 🍦	Forward 🏻 🍦	Reverse 🍦	
\mathbf{O}	Exchange-OA/10.0.1.75	Ξ	0	0	0	0	0	0	×
0	HTTPS/443	Ξ	0	0	0	0	0	0	\mathbb{R}
•	80 (Exchange1)		0	0	0	0	0	0	
•	80 (Exchange2)		0	0	0	0	0	0	

• Via CLI: AX#show slb virtual-server Exchange-OA AX#show slb service-group Exchange-OA-http AX#show slb server [Exchange1 | Exchange2]

Validate the AX deployment:

· Access the Exchange OA via Outlook Anywhere mode



2.6 Exchange Client Access role – Exchange ActiveSync

Exchange ActiveSync offers end users with low bandwidth and high-latency devices such as cell phones a way to access their mailboxes via HTTPS.

AX provides the following benefit:

• Load Balancing and High Availability of Exchange ActiveSync servers

And can also provide the optional benefit:

• SSL offload to reduce CPU and memory usage on Exchange ActiveSync servers

2.6.1 AX Configuration

Note: If the same VIP will be used for Outlook Web App or Outlook Anywhere services, see "2.14 Multiple Exchange Services with a Single VIP".

a. Create Exchange EAS Real Servers

· Same as "Exchange Client Access roles - Outlook Web App"

b. Create Exchange EAS Health Check

 Same as "Exchange Client Access Roles - Outlook Web App" Note: Use the Name "hm-eas-https".

c. Create Exchange EAS Service Group

• Same as "Exchange Client Access roles - Outlook Web App" Note: Use the **Name** "Exchange-EAS-https" and **Health Monitor** "hm-eas-https".



d. Create Exchange EAS Persistence

Note: Most cell phones support cookies with ActiveSync, but some may not. We could use Source-IP persistence instead; however, in the case where multiple clients come through the same Service Provider, the load balancing would not be fair. This is why we recommend aFleX UIE persistence. But aFleX UIE persistence requires Basic Authentication (under Exchange Management Console > Server Configuration > Client Access > Properties):

Microsoft-Server-ActiveSync (Default Web Site) Properties	×
General Authentication Remote File Servers	
Select the authentication method or methods that this virtual directory accepts. To enable authentication between the Exchange server and a mobile phone, either Basic authentication or Client certificate authentication is required. Basic authentication (password is sent in clear text)	
Client certificate authentication:	
Ignore client certificates	
C Accept client certificates	
C <u>B</u> equire client certificates	
To configure SSL settings for this ActiveSync virtual directory, use the Internet Information Services (IIS) snap-in.	
OK Cancel Apply Help	

If you can accept Basic authentication for AS, use aFleX UIE persistence, otherwise use source-IP persistence.

aFleX UIE persistence configuration:

 Same as "Exchange Client Access roles - Outlook Anywhere" Note: Use the aFleX Name "persist-eas".

Source IP persistence configuration:

 Same as "Exchange Client Access roles - Outlook Anywhere" Note: Use the aFleX Name or Source-IP persistence Name "persist-eas".



e. Import the IIS server Public Certificate/Private Key onto the AX

Note: You can access your mailboxes even if you do not have a trusted signed certificate with Outlook Web App. (You simply accept the untrusted certificate presented in your browser.) However, some cell phones and carriers do not let you accept the untrusted certificate. So you must have a trusted certificate with Outlook Anywhere.

 Same as "Exchange Client Access Roles - Outlook Web App" Note: Use the Certificate Name "eas-cert-key", Client-SSL Template Name "EAS-Client-Side" and Server-SSL Template Name "EAS-Server-Side".

f. Create Exchange EAS VIP

- · Create the virtual IP address (VIP), which is the IP address that end users will access
 - Enter a Name for the VIP, and enter the IP address
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server

General		
Name: *	Exchange-EAS	Wildcard
IP Address or CIDR Subnet: *	10.0.1.76	IPv4 O IPv6
Status:	Enabled Disabled	

- Via CLI: AX(config)#slb virtual-server Exchange-EAS 10.0.1.76
- Add port Type HTTPS Port 443 and select the Service Group, aFleX, Client-SSL Template, and Server-SSL template
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port

Virtual Server Port	
Name:	Exchange-EAS
Type: *	HTTPS 🗸
Port: *	443
Service Group:	Exchange-EAS-https 🔹
Connection Limit:	■ 8000000
Client-SSL Template:	EAS-Client-Side 🗸
Server-SSL Template:	EAS-Server-Side

If aFleX iue persistency is selected

aFIeX: persist-eas	- 51 - 34			
	aFleX:		persist-eas	

If Source IP persistency is selected

Persistence Template Type:	Source IP Persistence Template	•
Source IP Persistence Template:	persist-eas	•



• Via CLI: AX(config-slb vserver)#port 443 https

AX(config-slb vserver-vport)#service-group Exchange-EAS-https AX(config-slb vserver-vport)#template client-ssl EAS-Client-Side AX(config-slb vserver-vport)#template server-ssl EAS-Server-Side

If aFleX UIE persistence is selected

AX(config-slb vserver-vport)#aflex persist-eas

If Source-IP persistence is selected

```
AX(config-slb vserver-vport)#template persist source-ip persist-eas
```

g. (Optional) Offload SSL on Exchange EAS Servers

With this option, end users still use HTTPS to connect to their Exchange EAS service, but the AX connects to the EAS servers via HTTP, offloading SSL from the servers.

- Create the port 80 for each Exchange EAS real server
 - · Same as "Exchange Client Access Roles Outlook Web App"
- Create a health monitor template to test the availability of the Exchange EAS servers. Enter the health monitor template Name and select Type HTTP with URL "GET /"
 - Same as "Exchange Client Access roles Outlook Web App" Note: Use the Name "hm-eas-http".
- Create a TCP service group with Exchange EAS servers. Enter a Name for the service group, select TCP from the Type drop-down list, select the Least Connection load balancing Algorithm, and select the EAS Health Monitor. Assign each Exchange EAS server to the Service group and Port 80
 - Same as "Exchange Client Access roles Outlook Web App" Note: Use the Name "Exchange-EAS-http" and Health Monitor "hm-eas-http".
- In the EAS VIP, select the Service Group with HTTP servers
 - Same as "Exchange Client Access Roles Outlook Web App" Note: Use the Service Group "hm-eas-http".
- In the EAS VIP, remove the Server-SSL Template, since the AX will communicate with the EAS servers via HTTP
 - Same as "Exchange Client Access Roles Outlook Web App"
- Enable SSL offload on Exchange EAS servers; see http://social.technet.microsoft.com/wiki/con-tents/articles/how-to-configure-ssl-offloading-in-exchange-2010.aspx



2.6.2 Configuration Validation

a. Validate AX Deployment for Exchange EAS Without SSL Offload

Validate the status of the VIP and that its members are up.

• Via Web GUI: Monitor > Service > SLB > Virtual Server

	Name 🔶		Connections		Pack	(ets	Bytes		
~			Current 🏻 🍦	Total 🍦	Forward 🏻 🍦	Reverse 🍦	Forward 🏻 🍦	Reverse 🍦	
\mathbf{O}	Exchange-EAS/10.0.1.76	Ξ	0	0	0	0	0	0	\boxtimes
0	HTTPS/443	Ξ	0	0	0	0	0	0	∞
•	443 (Exchange1)		0	0	0	0	0	0	
\mathbf{O}	443 (Exchange2)		0	0	0	0	0	0	

• Via CLI: AX#show slb virtual-server Exchange-EAS AX#show slb service-group Exchange-EAS-https AX#show slb server [Exchange1 | Exchange2]

Validate the AX deployment:

- Access the Exchange EAS via ActiveSync
 - For more information on how to configure ActiveSync, see your device user guide.

b. Validate AX Deployment for Exchange EAS with SSL Offload

Validate the status of the VIP and that its members are up.

• Via Web GUI: Monitor > Service > SLB > Virtual Server

A Namo 4		Connections		Pack	kets	Bytes		
~	name 🚽	Current 🏻 🍦	Total 🍦	Forward 🏻 🍦	Reverse 🍦	Forward 🏻 🍦	Reverse 🍦	
\mathbf{O}	Exchange-EAS/10.0.1.76	0	0	0	0	0	0	×
\mathbf{O}	HTTPS/443	0	0	0	0	0	0	×
\mathbf{O}	80 (Exchange1)	0	0	0	0	0	0	
•	80 (Exchange2)	0	0	0	0	0	0	

• Via CLI: AX#show slb virtual-server Exchange-EAS AX#show slb service-group Exchange-EAS-http AX#show slb server [Exchange1 | Exchange2]

Validate the AX deployment:

Access the Exchange EAS via ActiveSync


2.7 Exchange Client Access Roles – RPC

Exchange RPC access offers end users with Microsoft Outlook access to their mailboxes via the native Microsoft Outlook Messaging API (MAPI) protocol.

AX provides the following benefits:

· Load Balancing and High Availability of Exchange RPC servers

Technical Note:

Outlook using the MAPI protocol contacts the Exchange server via TCP port 135 first and then opens a dynamic port between 1024 and 65535. Since by default any dynamic port number can be used, this requires a wildcard VIP on the AX that listens on all TCP ports. This is the configuration shown below.

For security reasons, it is possible and recommended by Microsoft to specify the dynamic port Outlook will open; see the following:

- <u>http://technet.microsoft.com/en-us/library/ff625248.aspx#ipports</u>
- <u>http://www.msexchange.org/articles_tutorials/exchange-server-2007/planning-architecture/uncov-ering-new-rpc-client-access-service-exchange-2010-part2.html</u>

If you limit the dynamic ports for MAPI, you can limit the ports open on AX via an ACL.

2.7.1 AX Configuration

A10 Netw

a. Create Exchange RPC Real Servers

- Create a real server for each Exchange RPC real server. Enter the RPC Name and IP address, and add Protocol TCP port 0 with no Health Monitor
 - Via Web GUI: Config Mode > Service > SLB > Server

IP Addres		Excha	ange1							
	ss/Host: *	10.0.2	2.161			◎ IPv	4 © IPv6			
GSLB Ext	ernal IP Addr	ess:								
Weight:		1								
Server Port Health Monit	t Template(<u>SPT</u> itor(<u>HM</u>):): default	•	• © F	Stats Da	ta(<u>SD</u>):	nabled O	Disabled		 Delete Enable
Health Moni	Itor(<u>HM</u>):	ablad D	•	01	ollow Pon		ICP	Ψ.		O Enable
	Port Protor	col CL	CR	W	No SSL	SPT	HM	SD	ES	
	0 TCP	8000000	0	1	0	default		0	0	

b. Create Exchange RPC Health Check

- Create a health monitor template to test the availability of the Exchange RPC servers. Enter the health monitor template Name, select Type TCP with Port 135 and Override Port 135
 - Via Web GUI: Config Mode > Service > Health Monitor

Health Monitor	
Name: *	hm-rpc-135
Retry:	3
Method	
Override IPv4:	
Override IPv6:	
Override Port:	135
Method:	Internal © External
Туре:	TCP 🔻
Port: *	135
HalfOpen:	False © True

• Via CLI:AX(config)#health monitor hm-rpc-135 AX(config-health:monitor)#method tcp port 135 AX(config-health:monitor)#override-port 135

c. Create Exchange RPC Service Group

- Create a TCP service group with Exchange RPC servers. Enter a Name for the service group, select TCP from the Type drop-down list, select the Round Robin load balancing Algorithm, and select the RPC Health Monitor. Assign each Exchange RPC Server to the service group with Port 0
 - Via Web GUI: Config Mode > Service > SLB > Service Group

Service Group		
Name: *	Exchange-RPC	
Туре:	TCP	.
Algorithm:	Round Robin	•
Health Monitor:	hm-rpc-135	*
Min Active Members:		



0	Serve	r								
	IPv4/I	Pv6:		IPv4	IPv6					
	Serve	er: *		Exchange2		-	Port: *	0		🛈 Add
	Serve	er Por	t Template(<u>SPT</u>):	default		-	Priority:	1	-	🥥 Update
	Stats	Data	:	Enabled	O Disable	ed				Oelete
			Server		Port	SPT		Priority	Stats Data	🔇 Enable
		0	Exchange1		0	default		1	0	😢 Disable
		0	Exchange2		0	default		1	0	

 Via CLI: AX(config)#slb service-group Exchange-RPC tcp AX(config-slb svc group)#method least-connection AX(config-slb svc group)#health-check hm-rpc-135 AX(config-slb svc group)#member Exchange1:0 AX(config-slb svc group)#member Exchange2:0

d. Create Exchange RPC Persistency

- Create a Source-IP persistence template to guarantee each end user will always go to the same Exchange RPC. Enter the persistence template **Name**, select **Match Type** server, and increase the **Timeout**
 - Via Web GUI: Config Mode > Service > Template > Persistent > Source IP Persistance
 - Via CLI: AX(config)#slb template persist source-ip persist-rpc AX(config-source ip persist)#match-type server AX(config-source ip persist)#timeout 480

Source IP Persistence	
Name: *	persist-rpc
Match Type:	Server Scan All Members
Timeout:	480 Minutes

e. Create TCP Aging Time Template

 Create a TCP template to guarantee each RPC end connection will not be discarded even with end-user inactivity. Enter the TCP template Name, and increase the Idle Timeout to a minimum of 3600 seconds (1 hour) to a maximum of 28,800 seconds (8 hours).

Note: Having an Idle timeout that is to short can cause a user to re-authenticate.

• Via Web GUI: Config Mode > Service > Template > L4 > TCP

тср	
Name: *	TCP-Aging-Time-rpc
Idle Timeout:	28800 Seconds
Force Delete Timeout:	
Initial Window Size:	
Half-closed Idle Timeout:	
Reset Forward:	Enabled Disabled
Reset Receive:	Enabled Disabled Disabled
Fast TCP ACK on LAN:	Enabled O Disabled



 Via CLI: AX(config)# slb template tcp TCP-Aging-Time-rpc AX(config-l4 tcp)# idle-timeout 28800 AX(config-l4 tcp)# reset-fwd AX(config-l4 tcp)# reset-rev

f. Create Exchange RPC VIP

- · Create the virtual IP address (VIP), which is the IP address that end users will access
 - Enter a Name for the VIP, and enter the IP address
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server

General		
Name: *	Exchange-RPC	Wildcard
IP Address or CIDR Subnet: *	10.0.1.74	
Status:	• • Enabled Oisabled	

- Via CLI: AX(config)#slb virtual-server Exchange-RPC 10.0.1.74
- Add port Type TCP Port 0 and select the Service Group, and Persistence Template
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port

Virtual Server Port	
Virtual Server:	Exchange-RPC
Type: *	TCP
Port: *	0
Service Group:	Exchange-RPC 🔹
Connection Limit:	8000000 Orop Reset Logging
TCP Template:	TCP-Aging-Time-rpc
Persistence Template Type:	Source IP Persistence Template 🔻
Source IP Persistence Template:	persist-rpc 🔻

• Via CLI: AX(config-slb vserver)#port 0 tcp

AX(config-slb vserver-vport)#service-group Exchange-RPC

AX(config-slb vserver-vport)#template persist source-ip persist-rpc

AX(config-slb vserver-vport)#template tcp TCP-Aging-Time-rpc

g. (optional) Create an ACL to limit the number of ports open on AX

• Create an ACL that authorizes only the Exchange TCP ports configured Note: The example below refers to an Exchange configuration with the ports are 135 +50000-51000.

Enter an **ID** for the ACL, **Action** Permit, **Protocol** TCP, and enter the **Destination Port** • Via Web GUI: Config Mode > Network > ACL > Extended



Extended	
ID: *	100 C Remark
Action: *	Deny ermit
Log:	
Protocol: *	TCP -
Source Address: *	 Any Host: Address: Mask: (0:apply, 1:ignore)
Source Port:	
Destination Address: *	 Any Host: Address: Mask: (0:apply, 1:ignore)
Destination Port:	Ø Operator: = ▼ Port: 135

And

Extended	
ID: *	100 Cemark Entry
Action: *	Deny ermit
Log:	
Protocol: *	TCP 👻
Source Address: *	 Any Host: Address: Mask: (0:apply, 1:ignore)
Source Port:	
Destination Address: *	 Any Host: Address: Mask: (0:apply, 1:ignore)
Destination Port:	Operator: Range From: 50000 To: 51000

• Via CLI: AX(config)#access-list 100 permit tcp any any eq 135 AX(config)#access-list 100 permit tcp any any range 50000 51000



Associate the ACL to the RPC VIP port

Enter an ID for the ACL, Action Permit, Protocol TCP, and enter the Destination Port

Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port



2.7.2 Configuration Validation

a. Validate AX deployment for Exchange without SSL offload

Validate the status of the VIP and that its members are up

• Via Web GUI: Monitor > Service > SLB > Virtual Server

	🔶 Name 🔶		Connections		Pack	kets	Bytes		
~			Current 🛛 🍦	Total 🏻 🍦	Forward 🏻 🍦	Reverse 🍦	Forward 🛛 🍦	Reverse 🍦	
\mathbf{O}	Exchange-RPC/10.0.1.74	Ξ	0	0	0	0	0	0	\mathbb{N}
0	TCP/0	Ξ	0	0	0	0	0	0	\mathbb{N}
•	0 (Exchange1)		0	0	0	0	0	0	
•	0 (Exchange2)		0	0	0	0	0	0	

• Via CLI: AX#show slb virtual-server Exchange-RPC AX#show slb service-group Exchange-RPC AX#show slb server [Exchange1 | Exchange2]

Validate the AX deployment:

Access the Exchange RPC via Microsoft Outlook



2.8 Exchange Client Access Roles – POP3

Exchange POP3 offers end users a way to access their mailboxes via many different email clients, for example Mozilla Thunderbird.

AX provides the following benefits:

· Load Balancing and High Availability of Exchange POP3 servers

And can also provide the optional benefit:

· SSL offload to reduce CPU and memory usage on Exchange POP3 servers

2.8.1 AX Configuration

a. Create Exchange POP3 Real Servers

- Create a real server for each Exchange POP3 real server. Enter the POP3 Name and IP address, and add the Protocol TCP port 995 (SSL over POP3)
 - Via Web GUI: Config Mode > Service > SLB > Server

General		
Name: *	Exchange1]
IP Address/Host: *	10.0.2.161	IPv4 IPv6
GSLB External IP Address:		
Weight:	1]

Port:	. 9	95	Protoc	col: TCP	٠	Weight(V	<i>[</i>): 1		No SSL			O Add
Conn	ectio	on Limit(CL): 800000	0 🛛 Log	ging		Connect	tion Resum	e(<u>CR</u>):			🥥 Update
Serve	er Po	rt Templ	ate(SPT):	default		-	Stats Da	ita(<u>SD</u>):	Enabled O D	isabled		Delete
Healt	h Mo	nitor(HN]): • (def:	ault)		• 0 F	ollow Por	t:	TCP	-		🕗 Enable
Exter	nded	Stats(ES): O Enab	led 💿 Disal	bled							🕄 Disable
		Port	Protocol	CL	CR	W	No SSL	SPT	HM	SD	ES	

 Via CLI: AX(config)#slb server Exchange1 10.0.2.161 AX(config-real server)#port 995 tcp



b. Create Exchange POP3 Health Check

AX supports the POP3 health checks. However, we will not use a POP3 health check here because we assume the Exchange servers are configured to support only POP3S (SSL over POP3).

The Exchange POP3 servers will be tested via TCP health checks on port 995. There is no need to create a specific health monitor to test the server TCP stack. This is done within the Real Server with the default health monitor:

Port:	• 9	95	Protoc	col: TCP	•	Weight(<u>V</u>	<u>v);* 1</u>		No SSL			O Add
Conn	ectio	n Limit(C	L): 800000	0 VLo	gging		Connect	ion Resume	e(<u>CR</u>):			🥥 Update
Serve	er Po	rt Templa	ate(SPT):	default		-	Stats Da	ta(<u>SD</u>):	Enabled OD	isabled		🤤 Delete
Healt	h Mo	nitor(HM): 🤨 (defz	sult)	- 8	• 0F	ollow Port	:	TCP	+		🔮 Enable
roun												
Exter	nded	Stats(ES): O Enab	led 🔍 Dis	abled							🖸 Disable
Exter	nded	Stats(ES): C Enab	led [©] Dis CL	abled CR	W	No SSL	SPT	HM	SD	ES	Oisable

c. Create Exchange POP3 Service Group

- Create a TCP service group with Exchange POP3 servers. Enter a Name for the service group, select TCP from the Type drop-down list, and select the Least Connection load balancing Algorithm. Assign each Exchange POP3 Server to the service group with Port 995
 - Via Web GUI: Config Mode > Service > SLB > Service Group

Service Group							
Name: *	Exchange-PC	P3S					
Туре:	TCP			•			
Algorithm:	Least Conne	ction		•			
Health Monitor:				•			
Min Active Members:							
Server							
IPv4/IPv6:	IPv4	IPv6					
Server: *	Exchange2		-	Port: *	995	j	🛈 Add
Server Port Template(SPT):	default		-	Priority:	1	•	🥥 Update
Stats Data:	Enabled	O Disable	ed				Oelete
Server		Port	SPT		Priority	Stats Data	📀 Enable
📃 📀 Exchange1		995	default		1	0	😢 Disable
📃 📀 Exchange2		995	default		1	0	

 Via CLI: AX(config)#slb service-group Exchange-POP3S tcp AX(config-slb svc group)#method least-connection AX(config-slb svc group)#member Exchange1:995 AX(config-slb svc group)#member Exchange2:995



d. Create Exchange POP3 Persistence

Exchange POP3 service does not require any persistence.

e. Create Exchange POP3 VIP

- · Create the virtual IP address (VIP), which is the IP address that end users will access
 - Enter a Name for the VIP, and enter the IP address
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server

General		
Name: *	Exchange-POP3S	Wildcard
IP Address or CIDR Subnet: *	10.0.1.74	
Status:	Enabled Oisabled	

- Via CLI: AX(config)#slb virtual-server Exchange-POP3S 10.0.1.74
- Add port Type TCP Port 995 and select the Service Group
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port

Virtual Server Port	
Virtual Server:	Exchange-POP3S
Type: *	TCP 👻
Port: *	995
Service Group:	Exchange-POP3S 🔹
Connection Limit:	■ 8000000 ● Drop ● Reset ✓ Logging

• Via CLI: AX(config-slb vserver)#port 995 tcp AX(config-slb vserver-vport)#service-group Exchange-POP3S

f. (Optional) Offload SSL on Exchange POP3 Servers

With this option, end users still use POP3S to connect to their Exchange POP3 service, but the AX connects to the POP3 servers via POP3, offloading SSL from the servers.

- Create the port 110 for each Exchange POP3 real server
 - Replace server port 995 with 110 in "step a"
- Create a health monitor template to test the availability of the Exchange POP3 servers.
 AX supports the POP3 health checks

Important Note: The POP3 health check can be used only if the Exchange POP3 servers are configured with Authentication "Plain text login (Basic Authentication)" (under Exchange Management Console > Server Configuration > Client Access > POP3 > Properties):



POP3 Properties
General Binding Authentication Connection Retrieval Settings
Logon Method
Specify the security settings to use for incoming connections.
 Plain text logon (Basic authentication). No TLS connection is required for the client to authenticate to the server.
Plain text authentication logon (Integrated Windows authentication). No TLS connection is required for the client to authenticate to the server.
Secure logon. A TLS connection is required for the client to authenticate to the server.
∑.509 certificate name:
Exchange

This is not the default Exchange configuration and we will not use the POP3 health check in this example. Instead, the Exchange POP3 servers will be tested via TCP health checks on port 110. There is no need to create a specific health monitor to test the server TCP stack. This is done within the Real Server with the default health monitor.

- Create a TCP service group with Exchange POP3 servers. Enter a **Name** for the service group, select TCP from the **Type** drop-down list, and select the Least Connection load balancing **Algorithm.** Assign each Exchange POP3 **Server** to the service group with **Port** 110
 - Replace the Name "Exchange-POP3S" with "Exchange-POP3" and Port "995" with "110" in "step c"
- Import the POP3S server public certificate/private key onto the AX Note: Since this VIP will be accessed by applications that may accept only trusted certificates, you must have a trusted certificate.
 Note: To export a certificate/key from Exchange POP3, see http://technet.microsoft.com/en-us/library/bb676455.aspx
 - Same as "Exchange Client Access roles Outlook Web App" Note: Use the Certificate Name "pop3-cert-key", Client-SSL Template Name "POP3-Client-Side" and no Server-SSL Template Name



- Create Exchange POP3 VIP
 - Replace the VIP Port created in "step e" with port Type SSL-Proxy, Port 995; select the Service Group and Client-SSL Template
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port

Virtual Server Port	
Virtual Server:	Exchange-POP3S
Type: *	SSL-Proxy 💌
Port: *	995
Service Group:	Exchange-POP3 🗸
Connection Limit:	🔲 8000000 💿 Drop 💿 Reset 🗹 Logging
Client-SSL Template:	POP3-Client-Side
Server-SSL Template:	▼

• Via CLI: AX(config-slb vserver)#port 995 ssl-proxy AX(config-slb vserver-vport)#service-group Exchange-POP3 AX(config-slb vserver-vport)#template client-ssl POP3-Client-Side

2.8.2 Configuration Validation

a. Validate AX deployment for Exchange without SSL Offload

Validate the status of the VIP and that its members are up

• Via Web GUI: Monitor > Service > SLB > Virtual Server

		Nama	-	Conne	ctions	Pack	kets	Byt	es	
Ľ	×	Name	\vee	Current 🏻 🍦	Total 🍦	Forward 🏻 🍦	Reverse 🍦	Forward 🍦	Reverse 🍦	
	0	Exchange-POP3S/10.0.1.74		0	0	0	0	0	0	\boxtimes
	0	TCP/995		0	0	0	0	0	0	$\underline{\mathbb{N}}$
	•	995 (Exchange1)		0	0	0	0	0	0	
	•	995 (Exchange2)		0	0	0	0	0	0	

• Via CLI: AX#show slb virtual-server Exchange-POP3S AX#show slb service-group Exchange-POP3S AX#show slb server [Exchange1 | Exchange2]

Validate the AX deployment:

· Access the Exchange POP3 with your email POP3 client



b. Validate AX deployment for Exchange with SSL offload

Validate the status of the VIP and that its members are up

• Via Web GUI: Monitor > Service > SLB > Virtual Server

		Nama	4	Connee	ctions	Pack	kets	Byt	es	
	V	name	×	Current 🛛 🍦	Total 🏻 🍦	Forward 🏻 🍦	Reverse 🍦	Forward 🏻 🍦	Reverse 🍦	
1	\mathbf{O}	Exchange-POP3S/10.0.1.74	Ξ	0	0	0	0	0	0	1
	0	SSL-Proxy/995	Ξ	0	0	0	0	0	0	$\underline{\mathbb{X}}$
	•	110 (Exchange1)		0	0	0	0	0	0	
	•	110 (Exchange2)		0	0	0	0	0	0	

• Via CLI: AX#show slb virtual-server Exchange-POP3S AX#show slb service-group Exchange-POP3 AX#show slb server [Exchange1 | Exchange2]

Validate the AX deployment:

• Access the Exchange POP3 with your email POP3 client



2.9 Exchange Client Access Roles – IMAP4

Exchange IMAP4 offers end users a way to access their mailboxes via many different email clients, for example Mozilla Thunderbird.

AX provides the following benefits:

· Load Balancing and High Availability of Exchange IMAP4 servers

And can also provide the optional benefit:

· SSL offload to reduce CPU and memory usage on Exchange IMAP4 servers

2.9.1 AX Configuration

a. Create Exchange IMAP4 Real Servers

- Create a real server for each Exchange IMAP4 real server. Enter the IMAP4 Name and IP address, and add Protocol TCP port 993 (SSL over IMAP4)
 - Via Web GUI: Config Mode > Service > SLB > Server

General		
Name: *	Exchange1	
IP Address/Host: *	10.0.2.161	IPv4 IPv6
GSLB External IP Address:		
Weight:	1	

Port:	• 9	93	Protoc	col: TCP		We	eight(<u>\</u>	<u>N):* 1</u>		No SSL			🔾 Add
Conn	ectio	n Limit((CL): 800000	0	oggir	ng		Connect	tion Resum	e(<u>CR</u>):			🥥 Update
Serve	er Po	rt Templ	ate(SPT):	default		1.11		Stats Da	ata(<u>SD</u>): •	Enabled O D	isabled		Delete
Healt	h Mo	nitor(<u>HM</u>): • (def	ault)			OF	ollow Por	ti	TCP	-		🖉 Enable
Exter	nded	Stats(ES): O Enab	led 🔍 Dis	able	d							🖸 Disable
	1	Port	Protocol	CL	(R	W	No SSL	SPT	HM	SD	ES	
10000	0	003	TCP	8000000	0	_	1	0	default	(default)	0	0	

Via CLI: AX(config)#slb server Exchange1 10.0.2.161
 AX(config-real server)#port 993 tcp



b. Create Exchange IMAP4 Health Check

AX supports IMAP4 health checks. But we will not use that type of health check in this example because we assume the Exchange servers are configured to support only IMAP4S (SSL over IMAP4). The Exchange IMAP4 servers will be tested via TCP health checks on port 993. There is no need to create a specific health monitor to test the server TCP stack. This is done within the Real Server with the default health monitor:

Port:	9	93	Protoc	col: TCP	• We	ight(<u>\</u>	<u>N):* 1</u>		No SSL			O Add
Conn	ectio	n Limit(Cl): 800000	0 🛛 🗹 Logg	ing		Connect	ion Resume	(<u>CR</u>):			🥥 Update
Serve	er Po	rt Templa	te(<u>SPT</u>):	default			Stats Da	ta(<u>SD</u>): • I	Enabled 💿 D	isabled		Delete
Healt	h Mo	nitor(<u>HM</u>):	(defi	ault)		OF	ollow Port	:	TCP	-		Enable
		en l'un es	Const	lod O Disab	led							🔁 Disable
Exter	ded	Stats(ES)	C Ellap	ieu e Diado								
Exter	ded	Port	Protocol	CL	CR	W	No SSL	SPT	HM	SD	ES	

c. Create Exchange IMAP4 Service Group

- Create a TCP service group with Exchange IMAP4 servers. Enter a **Name** for the service group, select TCP from the **Type** drop-down list, and select the Least Connection load balancing **Algorithm.** Assign each Exchange IMAP4 Server to the service group with **Port** 993
 - Via Web GUI: Config Mode > Service > SLB > Service Group

Service Group		
Name: *	Exchange-IMAP4S	
Туре:	TCP	-
Algorithm:	Least Connection	-
Health Monitor:		-

0	Serve	F								
	IPv4/I	Pv6:		IPv4	IPv6					
	Serve	er: *		Exchange2		-	Port: *	993	3	🛈 Add
	Serve	er Por	t Template(<u>SPT</u>):	default		•	Priority:	1	•	🥥 Update
	Stats	Data	:	Enabled	O Disabl	ed				\ominus Delete
			Server		Port	SPT		Priority	Stats Data	📀 Enable
		0	Exchange1		993	default		1	0	😣 Disable
		0	Exchange2		993	default		1	0	

 Via CLI: AX(config)#slb service-group Exchange-IMAP4S tcp AX(config-slb svc group)#method least-connection AX(config-slb svc group)#member Exchange1:993 AX(config-slb svc group)#member Exchange2:993



d. Create Exchange IMAP4 Persistence

Exchange IMAP4 service does not require any persistence.

e. Create Exchange IMAP4 VIP

Create the virtual IP address (VIP), which is the IP address that end users will access

- Enter a Name for the VIP, and enter the IP address
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server

General		
Name: *	Exchange-IMAP4S	Wildcard
IP Address or CIDR Subnet: *	10.0.1.74	
Status:	Second Seco	

- Via CLI: AX(config)#slb virtual-server Exchange-IMAP4S 10.0.1.74
- Add port Type TCP Port 995 and select the Service Group
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port

Virtual Server Port	
Virtual Server:	Exchange-IMAP4S
Type: *	TCP 🗸
Port: *	993
Service Group:	Exchange-IMAP4S 👻
Connection Limit:	🖾 8000000 💿 Drop 💿 Reset 🗹 Logging

• Via CLI: AX(config-slb vserver)#port 993 tcp AX(config-slb vserver-vport)#service-group Exchange-IMAP4S

f. (Optional) Offload SSL on Exchange IMAP4 servers

With this option, end users still use IMAP4S to connect to their Exchange IMAP4 service, but the AX connects to the IMAP4 servers via IMAP4, offloading SSL from the servers.

- Create the port 143 for each Exchange IMAP4 real server
 - Replace the server port 993 with 143 in "step a"

Create a health monitor template to test the availability of the Exchange IMAP4 servers.

AX supports IMAP4 health checks.

Important Note: The IMAP4 health check can be used only if the Exchange IMAP4 servers are configured with Authentication "Plain text login (Basic Authentication)" (under Exchange Management Console > Server Configuration > Client Access > IMAP4 > Properties):



IMAP4 Properties	<
General Binding Authentication Connection Retrieval Settings	1
Logon Method	l
Specify the security settings to use for incoming connections.	L
Plain text logon (Basic authentication). No TLS connection is required for the client to authenticate to the server.	
Plain text authentication logon (Integrated Windows authentication). No TLS connection is required for the client to authenticate to the server.	l
O Secure logon. A TLS connection is required for the client to authenticate to the server.	l
≚.509 certificate name:	
Exchange	l
	Т

This is not the default Exchange configuration and we will not use IMAP health checking in this step. Instead, the Exchange IMAP4 servers will be tested via TCP health checks on port 143. There is no need to create a specific health monitor to test the server TCP stack. This is done within the Real Server with the default health monitor.

- Create a TCP service group with Exchange IMAP4 servers. Enter a **Name** for the service group, select TCP from the **Type** drop-down list, and select the Least Connection load balancing **Algorithm.** Assign each Exchange IMAP4 Server to the service group with **Port** 143
 - Replace the Name "Exchange-IMAP4S" with "Exchange-IMAP4" and Port "993" with "143" in "step c"
- Import the IMAP4S server public certificate/private key onto the AX Note: Since this VIP will be accessed by applications that may accept only trusted certificates, you must have a trusted certificate.

Note: To export certificate/key from Exchange IMAP4, see <u>http://technet.microsoft.com/en-us/library/</u><u>bb676455.aspx</u>

- Same as "Exchange Client Access roles Outlook Web App" Note: Use Certificate Name "imap4-cert-key", Client-SSL Template Name "IMAP4-Client-Side" and no Server-SSL Template Name
- Create Exchange IMAP4 VIP
 - Replace the VIP Port created in "step e" with port Type SSL-Proxy, Port 993; select the Service Group, and Client-SSL Template
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port

Virtual Server Port	
Virtual Server:	Exchange-IMAP4S
Type: *	SSL-Proxy 👻
Port: *	993
Service Group:	Exchange-IMAP4 👻
Connection Limit:	🖾 8000000 💿 Drop 💿 Reset 🗹 Logging



Client-SSL Template:	IMAP4-Client-Side 🔹
Server-SSL Template:	•

 Via CLI: AX(config-slb vserver)#port 993 ssl-proxy AX(config-slb vserver-vport)#service-group Exchange-IMAP4 AX(config-slb vserver-vport)#template client-ssl IMAP4-Client-Side

2.9.2 Configuration Validation

a. Validate AX Deployment for Exchange Without SSL offload

Validate the status of the VIP and that its members are up

• Via Web GUI: Monitor > Service > SLB > Virtual Server

	Nama		Connection		s Packets			Bytes		
~	name		Current 🛛 🍦	Total 🏻 🍦	Forward 🏻 🍦	Reverse 🍦	Forward 🏻 🍦	Reverse 🍦		
\mathbf{O}	Exchange-IMAP4S/10.0.1.74	Ξ	0	0	0	0	0	0	1	
0	TCP/993	Ξ	0	0	0	0	0	0	\mathbb{X}	
•	993 (Exchange1)		0	0	0	0	0	0		
•	993 (Exchange2)		0	0	0	0	0	0		

• Via CLI: AX#show slb virtual-server Exchange-IMAP4S AX#show slb service-group Exchange-IMAP4S AX#show slb server [Exchange1 | Exchange2]

Validate the AX deployment:

· Access the Exchange POP3 with your email IMAP4 client

b. Validate AX deployment for Exchange AS with SSL offload

Validate the status of the VIP and that its members are up

• Via Web GUI: Monitor > Service > SLB > Virtual Server

	Nama		Connections		Pack	ets	Byt		
~	name	×	Current 🛛 🍦	Total 🏻 🍦	Forward 🏻 🍦	Reverse 🍦	Forward 🏻 🍦	Reverse 🍦	
\mathbf{O}	Exchange-IMAP4S/10.0.1.74	Ξ	0	0	0	0	0	0	\boxtimes
\mathbf{O}	SSL-Proxy/993	Ξ	0	0	0	0	0	0	$\underline{\mathbb{N}}$
\mathbf{O}	143 (Exchange2)		0	0	0	0	0	0	
0	143 (Exchange1)		0	0	0	0	0	0	

• Via CLI: AX#show slb virtual-server Exchange-IMAP4S AX#show slb service-group Exchange-IMAP4 AX#show slb server [Exchange1 | Exchange2]

Validate the AX deployment:

Networks //

· Access the Exchange POP3 with your email IMAP4 client

2.10 Exchange Client Access role – Exchange Web Services

Exchange Web Services (EWS) is a component that offers web services API for Exchange.

AX provides EWS with the same benefits as OWA; in this case:

• Load Balancing and High Availability of Exchange EWS servers

AX can also provide these optional benefits:

- HTTP Compression to reduce remote end user response time and data center bandwidth usage
- SSL offload to reduce CPU and memory usage on Exchange EWS servers

2.10.1 AX Configuration

Note: If the same VIP will be used for the Outlook Anywhere or Exchange ActiveSync services, see "2.14 Multiple Exchange Services with a Single VIP".

· Same as "Exchange Client Access roles - Outlook Web App"

2.10.2 Configuration Validation

• Same as "Exchange Client Access roles - Outlook Web App" Note: Access your web services via the VIP "https://mail.example.com".



2.11 Exchange Client Access role – Autodiscover

Autodiscover allows you to automatically configure Outlook 2007/2010 clients.

AX provides Autodiscover with the same benefits as OWA; in this case:

· Load Balancing and High Availability of Exchange Autodiscover servers

AX can also provide these optional benefits:

- · HTTP Compression to reduce remote end user response time and data center bandwidth usage
- SSL offload to reduce CPU and memory usage on Exchange EWS servers

2.11.1 AX Configuration

Note: If the same VIP will be used for the Outlook Anywhere or Exchange ActiveSync services, see "2.14 Multiple Exchange Services with a Single VIP".

• Same as "Exchange Client Access roles - Outlook Web App" Note: There is no persistence need (skip step d.)

2.11.2 Configuration Validation

See http://technet.microsoft.com/en-us/library/bb123573.aspx



2.12 Exchange Client Access role – Offline Address Book distribution

An offline address book (OAB) is a copy of a collection of address lists that has been downloaded so that a Microsoft Outlook user can access the information it contains while disconnected from the server.

There are two methods by which the OAB is distributed to client computers:

- Web-based distribution
- Public folder distribution

AX provides Autodiscover with the same benefits as OWA; in this case:

· Load Balancing and High Availability of Exchange Autodiscover servers

Note: Appendix A15 is an aFleX script that blocks all Exchange services except OWA and OAB distributions. The script is very useful for Exchange administrators that control Exchange services originating from external access.

2.12.1 AX Configuration

- · For web-based distribution: Same as "Exchange Client Access roles Outlook Web App"
- · For public folder distribution: Same as "Exchange Client Access roles -RPC"

2.12.2 Configuration Validation

See http://technet.microsoft.com/en-us/library/bb124351.aspx



2.13 Exchange Edge Transport Server Role - SMTP

Exchange Edge Transport Server role performs anti-spam and antivirus filtering, and applies messaging and security policies to messages in transport.

AX provides the following benefits:

· Load Balancing and High Availability of Exchange Anywhere servers

And can also provide the optional benefit:

• TLS (STARTTLS) offload to reduce CPU and memory usage on Exchange SMTP servers

2.13.1 AX Configuration

a. Create Exchange SMTP real servers

· Same as "Exchange Client Access roles - Outlook Web App"

b. Create Exchange SMTP Health Check

- Create a health monitor template to test the availability of the Exchange SMTP servers. Enter the health monitor template Name and select Type SMTP with its Domain
 - Via Web GUI: Config Mode > Service > Health Monitor

Health Monitor		
Name: *	hm-smtp	
Retry:	3	
Method		
Override IPv4:		
Override IPv6:		
Override Port:		
Method:	Internal	External
Туре:	SMTP	
Port:	25	
Domain: *	example.com	

 Via CLI: AX(config)#health monitor hm-smtp AX(config-health:monitor)#method smtp domain example.com



c. Create Exchange SMTP Service Group

 Same as "Exchange Client Access roles - Outlook Web App" Note: Use the Name "Exchange-SMTP" and Health Monitor "hm-smtp".

d. Create Exchange SMTP persistence

Exchange SMTP service does not require any persistence.

e. Create Exchange SMTP VIP

- · Create the virtual IP address (VIP), which is the IP address that end users will access
 - Enter a Name for the VIP, and enter the IP address
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server

General		
Name: *	Exchange-SMTP	Wildcard
IP Address or CIDR Subnet: *	10.0.1.74	
Status:	Enabled Observed	

- Via CLI: AX(config)#slb virtual-server Exchange-SMTP 10.0.1.74
- Add port Type TCP Port 25 and select the Service Group
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port

Virtual Server Port	
Name:	Exchange-SMTP
Type: *	TCP 🔻
Port: *	25
Service Group:	Exchange-SMTP 🔹
Connection Limit:	🖾 8000000 💿 Drop 💿 Reset 🗹 Logging

• Via CLI: AX(config-slb vserver)#port 25 tcp AX(config-slb vserver-vport)#service-group Exchange-SMTP

f. (Optional) Offload TLS on Exchange SMTP servers

With this option, AX can offer or enforce TLS access for end users connecting to the Exchange SMTP service. However Exchange servers are still configured with no TLS for SMTP.

- · Create the SMTP template to define the TLS (STARTTLS) SMTP access
 - Enter a **Name** for the template, specify whether STARTTLS is optional or enforced, and enter the **Server Domain**
 - Via Web GUI: Config Mode > Service > Template > Application > SMTP



SMTP	
Name: *	STARTTLS-SMTP
STARTTLS:	Disabled Enforced Optional
Command Disabled:	EXPN TURN VRFY
Server Domain:	example.com
Service Ready Message:	

- Via CLI: AX(config)#slb template smtp STARTTLS-SMTP AX(config-smtp)#server-domain example.com AX(config-smtp)#starttls optional
- Import the certificate/private key onto the AX to use for SMTP
 Note: You can access your mailboxes even if you do not have a trusted signed certificate with
 Outlook. (You simply accept the untrusted certificate presented in Outlook.) However, clients may
 use other software than Outlook and will not give you the option to accept the untrusted certificate. Therefore, we recommend that you use a trusted certificate with TLS on SMTP.
 - Same as "Exchange Client Access roles Outlook Web App" Note: Use the Certificate Name "smtp-cert-key" and Client-SSL Template Name "SMTP-Client-Side"
- In the SMTP VIP, replace the TCP port 25 with:
 - Add port Type SMTP Port 25, select the Service Group, the Client-SSL template and SMTP Template
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port

Virtual Server Port	
Name:	Exchange-SMTP
Type: *	SMTP 👻
Port: *	25
Service Group:	Exchange-SMTP -
Connection Limit:	■ 8000000
Client-SSL Template:	OWA-Client-Side
SMTP Template:	STARTTLS-SMTP 🔻

- Via CLI: AX(config-slb vserver)#port 25 smtp
 - AX(config-slb vserver-vport)#service-group Exchange-SMTP AX(config-slb vserver-vport)#template client-ssl OWA-Client-Side AX(config-slb vserver-vport)#template smtp STARTTLS-SMTP



2.13.2 Configuration Validation

a. Validate AX Deployment for Exchange SMTP without TLS offload

Validate the status of the VIP and that its members are up

• Via Web GUI: Monitor > Service > SLB > Virtual Server

	Name 🔶		Connections		Packets		Bytes		
~			Current 🔶	Total 🏻 🍦	Forward 🏻 🍦	Reverse 🍦	Forward 🏻 🍦	Reverse 🍦	
\mathbf{O}	Exchange-SMTP/10.0.1.74	Ξ	0	1	18	18	2.3K	3.1K	1
\mathbf{O}	TCP/25	Ξ	0	1	18	18	2.3K	3.1K	\mathbb{N}
•	25 (Exchange1)		0	8	100	90	8.5K	10.3K	
•	25 (Exchange2)		0	7	115	107	11.2K	12.8K	

• Via CLI: AX#show slb virtual-server Exchange-SMTP AX#show slb service-group Exchange-SMTP AX#show slb server [Exchange1 | Exchange2]

Validate the AX deployment:

 Send email via SMTP via Outlook or any mail client Note: If Exchange accepts only TLS connections for the SMTP service, enable TLS on the Client. For instance, on Outlook 2007, this is under "Tools > Account Settings > Edit email > More Settings > Advanced":

Internet E-mail Settings
General Outgoing Server Connection Advanced
Server Port Numbers
Incoming server (POP3): 995 Use Defaults
This server requires an encrypted connection (SSL)
Outgoing server (SMTP): 25
Use the following type of engrypted connection:
Server Timeouts
Short Long 1 minute
Delivery
✓ Leave a copy of messages on the server
Remove from server after 10 ays
Remove from server when deleted from 'Deleted Items'
OK Cancel



b. Validate AX deployment for Exchange SMTP With SSL Offload

Validate the status of the VIP and that its members are up

• Via Web GUI: Monitor > Service > SLB > Virtual Server

	Name 🔶		Connections		Packets		Bytes		
~			Current 🛛 🍦	Total 🏻 🍦	Forward 🏻 🍦	Reverse 🍦	Forward 🏻 🍦	Reverse 🍦	
\mathbf{O}	Exchange-SMTP/10.0.1.74	Ξ	0	0	0	0	0	0	1
\mathbf{O}	SMTP/25	Ξ	0	0	0	0	0	0	\mathbb{R}
•	25 (Exchange1)		0	8	100	90	8.5K	10.3K	
0	25 (Exchange2)		0	7	115	107	11.2K	12.8K	

• ViaCLI: AX#show slb virtual-server Exchange-SMTP AX#show slb service-group Exchange-SMTP AX#show slb server [Exchange1 | Exchange2]

Validate the AX deployment:

• Send email via SMTP via Outlook or any mail client Note: If Exchange accepts only TLS connections for the SMTP service, enable TLS on the Client.



2.14 Multiple Exchange Services with a Single VIP

Microsoft Exchange uses different TCP ports for their different services (RPC, POP3, and so on). However for five services, the same TCP port 443 access is used:

- Outlook Web App (and its optional service Exchange Control Panel)
- Outlook Anywhere
- Exchange ActiveSync
- Exchange Web Services
- Autodiscover

By using different VIP access methods for these client access roles, enterprises can manage each service independently and use specific security, monitoring and load balancing settings. However, some organizations may need to use the same VIP for these Exchange services.

AX supports such deployment and provides the following benefits:

· Load Balancing and High Availability of Exchange servers

And can also provide the optional benefit:

• SSL offload to reduce CPU and memory usage on Exchange servers

Note: With this deployment, AX will not provide the following benefits:

- HTTP Compression
- Transparent redirection of HTTP clients to HTTPS for OWA + ECP
- Transparent addition of "/owa" to OWA requests that do not have it

2.14.1 AX Configuration with 1 VIP for OWA + OA + EAS Services Hosted on the Same Exchange Servers

a. Create Exchange Real Servers

· Same as "Exchange Client Access roles - Outlook Web App"

b. Create Exchange Health Check

 Same as "Exchange Client Access roles - Outlook Web App" Note: Use the Name "hm-exchange-https".

c. Create Exchange Service Group

• Same as "Exchange Client Access roles - Outlook Web App" Note: Use the **Name** "Exchange-https" and **Health Monitor** "hm-exchange-https".



d. Create Exchange Persistence

Note: Since this VIP will be accessed by some devices that support cookies and others that do not, we recommend using Source-IP persistence.

 Same as "Exchange Client Access roles - Outlook Anywhere" Note: Use the Source-IP Persistence Name "persist-exchange-https".

e. Import the IIS server public certificate / private key onto the AX

Note: Since this VIP will be accessed by devices supporting only trusted certificates, you must have a trusted certificate.

- Same as "Exchange Client Access roles Outlook Web App"
 - Note: Use the **Certificate Name** "exchange-https-cert-key", **Client-SSL Template Name** "exchange-https-Client-Side", and **Server-SSL Template Name** "exchange-https-Server-Side"

f. Create Exchange VIP

- Same as "Exchange Client Access roles Outlook Anywhere" Note: Use the Name "Exchange" and add the port Type HTTPS Port 443 and select the Service Group "Exchange-https", Source IP Persistence Template "persist-exchange-https", Client-SSL Template "exchange-https-Client-Side", and Server-SSL template "exchange-https-Server-Side"
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port

Virtual Server Port	
Name:	Exchange-OWA
Type: *	HTTPS 🗸
Port: *	443
Service Group:	Exchange-https
Connection Limit:	🖾 8000000 💿 Drop 💿 Reset 🗹 Logging
Client-SSL Template:	Exchange-https-Client-Side
Server-SSL Template:	Exchange-https-Server-Side
Connection Reuse Template:	▼
TCP-Proxy Template:	
Persistence Template Type:	Source IP Persistence Template 🔻
Source IP Persistence Template:	persist-exchange-https

0	Via CLI:	AX(config-slb vserver)#port 443 https
		AX(config-slb vserver-vport)#service-group Exchange-https
		AX(config-slb vserver-vport)#template client-ssl Exchange-
		https-Client-Side
		AX(config-slb vserver-vport)#template server-ssl Exchange-
		https-Server-Side
		AX(config-slb vserver-vport)#template persist source-ip per
		sist-exchange-https



g. (Optional) Offload SSL on Exchange Servers

With this option, end users still use HTTPS to connect to their Exchange service, but the AX connects to the Exchange servers via HTTP, offloading SSL from the servers.

- Create the port 80 for each Exchange OWA/OA/EAS real server
 - Same as "Exchange Client Access roles Outlook Web App"

Create a health monitor template to test the availability of the Exchange OWA/OA/EAS servers. Enter the health monitor template **Name** and select **Type** HTTP with **URL** "GET /"

- Same as "Exchange Client Access roles Outlook Web App" Note: Use the Name "hm-exchange-http".
- Create a TCP service group with Exchange OWA/OA/EAS servers. Enter a Name for the service group, select TCP from the Type drop-down list, select the Least Connection load balancing Algorithm, and select the Health Monitor. Assign each Exchange OWA/OA/EAS Server to the service group and Port 80
 - Same as "Exchange Client Access roles Outlook Web App"
 Note: Use the Name "Exchange-http" and Health Monitor "hm-exchange-http".
- In the OWA/OA/EAS VIP, select the **Service Group** with HTTP servers and remove the **Server-SSL Template**, **since the AX will** communicate with the OWA/OA/EAS servers via HTTP
 - Same as "Exchange Client Access roles Outlook Web App" Note: Use the Service Group "Exchange-http".
- Enable SSL offload on Exchange OWA/OA/EAS servers; see http://social.technet.microsoft.com/wiki/contents/articles/how-to-configure-ssl-offloading-in-exchange-2010.aspx

2.14.2 AX Configuration with 1 VIP for OWA + OA + EAS Services Hosted on Different Exchange Servers

a. Create Exchange Real Servers for Each Service

- Outlook Web app
 - Same as "Exchange Client Access Roles Outlook Web App"
- Outlook Anywhere
 - Same as "Exchange Client Access Roles Outlook Anywhere"
- Exchange ActiveSync
 - Same as "Exchange Client Access Roles Exchange ActiveSync"



b. Create Exchange Health Check for Each Service

- Outlook Web app
 - Same as "Exchange Client Access Roles Outlook Web App"
- Outlook Anywhere
 - Same as "Exchange Client Access Roles Outlook Anywhere"
- Exchange ActiveSync
 - Same as "Exchange Client Access Roles Exchange ActiveSync"

c. Create Exchange Service Group

- Outlook Web app
 - Same as "Exchange Client Access Roles Outlook Web App"
- Outlook Anywhere
 - · Same as "Exchange Client Access Roles Outlook Anywhere"
- Exchange ActiveSync
 - Same as "Exchange Client Access Roles Exchange ActiveSync"

d. Create Exchange Persistence

Each client access (OWA, OA, EAS) must use specific servers:

aFleX will be used to redirect specific client accesses to their specific Exchange servers.

 Create an aFleX policy to redirect specific clients to their specific service group. The aFleX policy is:

```
when HTTP_REQUEST {
    # Outlook Anywhere Clients
    if { [HTTP::header "User-Agent"] contains "MSRPC" } {
        pool Exchange-OA-https
    # Exchange ActiveSyncActiveSync Clients
    } elseif { [HTTP::uri] contains "Microsoft-Server-Active-Sync" } {
        pool Exchange-EAS-https
        # Outlook Web Apps Clients
    } else {
        pool Exchange-OWA-https
    }
}
```



• Via Web GUI: Config > Service > aFleX

aFleX	
Name: *	persist-https-per-access
Definition: *	<pre>when HTTP_REQUEST { # Outlook Anywhere Clients if { [HTTP::header "User-Agent"] contains "MSRPC" } { pool Exchange-QA-https # Exchange Active Sync Clients } elseif { [HTTP::uri] contains "Microsoft-Server-Active-Sync" } { pool Exchange-EAS-https # Outlook Web Apps Clients } else { pool Exchange-OWA-https } }</pre>

 Via CLI: AX(config)#import aflex persist-https-per-access tftp://10.0.1.10/ persist-https-per-access.txt

Server persistence for each client

Note: Since this VIP will be accessed by some devices that support cookies and others that do not, we recommend using Source-IP persistence.

- Same as "Exchange Client Access roles Outlook Anywhere" Note: Use the Source-IP Persistence **Name** "persist-exchange-https".
- To achieve better load distribution across Exchange server using persistence, refer to Appendix A16.

e. Import the IIS Server Public Certificate/Private Key onto the AX

Note: Since this VIP will be accessed by devices supporting only trusted certificates, you must have a trusted certificate.

• Same as "Exchange Client Access roles - Outlook Web App" Note: Use the **Certificate Name** "exchange-https-cert-key", **Client-SSL Template Name** "exchange-https-Client-Side" and **Server-SSL Template Name** "exchange-https-Server-Side".

f. Create Exchange VIP

 Same as "Exchange Client Access roles - Outlook Anywhere" Note: Use the Name "Exchange", add port Type HTTPS Port 443 and select the Service Group "Exchange-https", aFleX "persist-https-per-access", Source IP Persistence Template "persistexchange-https", Client-SSL Template "exchange-https-Client-Side", and Server-SSL template "exchange-https-Server-Side"



Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port

Virtual Server Port	
Name:	Exchange-OWA
Type: *	HTTPS 🔹
Port: *	443
Service Group:	Exchange-https
Connection Limit:	■ 8000000
aFleX:	persist-https-per-access
Client-SSL Template:	Exchange-https-Client-Side
Server-SSL Template:	Exchange-https-Server-Side
Connection Reuse Template:	▼
TCP-Proxy Template:	▼
Persistence Template Type:	Source IP Persistence Template 🔹
Source IP Persistence Template:	persist-exchange-https

• Via CLI: AX(config-slb vserver)#port 443 https

AX(config-slb vserver-vport)#service-group Exchange-https AX(config-slb vserver-vport)#aflex persist-https-per-access AX(config-slb vserver-vport)#template client-ssl Exchangehttps-Client-Side AX(config-slb vserver-vport)#template server-ssl Exchangehttps-Server-Side AX(config-slb vserver-vport)#template persist source-ip per sist-exchange-https

g. (Optional) Offload SSL on Exchange Servers

With this option, end users still use HTTPS to connect to their Exchange service, but the AX connects to the Exchange servers via HTTP, offloading SSL from the servers.

- Create the port 80 for each Exchange OWA/OA/EAS real server
 - Outlook Web app
 - Same as "Exchange Client Access Roles Outlook Web App"
 - Outlook Anywhere
 - · Same as "Exchange Client Access Roles Outlook Anywhere"
 - Exchange ActiveSync
 - Same as "Exchange Client Access Roles Exchange ActiveSync"



- Create a health monitor template to test the availability of the Exchange OWA/OA/EAS servers. Enter the health monitor template **Name** and select **Type** HTTP with **URL** "GET /"
 - Outlook Web app
 - Same as "Exchange Client Access Roles Outlook Web App"
 - Outlook Anywhere
 - Same as "Exchange Client Access Roles Outlook Anywhere"
 - Exchange ActiveSync
 - Same as "Exchange Client Access Roles Exchange ActiveSync"
- Create a TCP service group with Exchange OWA/OA/EAS servers. Enter a Name for the service group, select TCP from the Type drop-down list, select the Least Connection load balancing Algorithm, and select the Health Monitor. Assign each Exchange OWA/OA/EAS Server to the service group and Port 80
 - Outlook Web app
 - Same as "Exchange Client Access roles Outlook Web App"
 - Outlook Anywhere
 - · Same as "Exchange Client Access roles Outlook Anywhere"
 - Exchange ActiveSync
 - Same as "Exchange Client Access roles Exchange ActiveSync"
- Update the aFleX "persist-https-per-access" with the new pools of servers "Exchange-OWAhttp", "Exchange-OA-http", and "Exchange-EAS-http"
- In the OWA/OA/EAS VIP, select the **Service Group** with HTTP servers, and remove the **Server-SSL Template** to communicate to the OWA/OA/EAS servers via HTTP
 - Same as "Exchange Client Access roles Outlook Web App" Note: Use the Service Group "Exchange-http".
- Enable SSL offload on Exchange OWA/OA/EAS servers; see http://social.technet.microsoft.com/wiki/contents/articles/how-to-configure-ssl-offloading-in-exchange-2010.aspx



2.14.3 Configuration Validation

a. Validate AX deployment for Exchange without SSL offload

- Validate Exchange Outlook Web App
 - Same as "Exchange Client Access roles Outlook Web App"
- Validate Exchange Control Panel
 - Same as "Exchange Client Access roles Exchange Control Panel"
- Validate Exchange Outlook Anywhere
 - Same as "Exchange Client Access roles Outlook Anywhere"
- Validate Exchange ActiveSync
 - Same as "Exchange Client Access roles ActiveSync"

b. Validate AX deployment for Exchange with SSL offload

- Validate Exchange Outlook Web App
 - Same as "Exchange Client Access roles Outlook Web App"
- Validate Exchange Control Panel
 - Same as "Exchange Client Access roles Exchange Control Panel"
- Validate Exchange Outlook Anywhere
 - Same as "Exchange Client Access roles Outlook Anywhere"
- Validate Exchange ActiveSync
 - Same as "Exchange Client Access roles ActiveSync"



3. Summary and Conclusion

The AX Series Advanced Traffic Manager enhances Microsoft Exchange service by providing:

- Higher Scalability enterprises can provide Exchange services to a very high number of employees, load balancing them among multiple Exchange servers in parallel
- High Availability Exchange services are guaranteed even if an Exchange Server goes offline
- Higher Performance end users access their Exchange services faster thanks to multiple Exchange server optimizations; for example, compression and SSL offload
- Higher Security protects services from DDoS attacks
- More Deployment flexibility different Exchange services can be accessible via the same public VIP

For more information about AX Series products, please refer to: http://a10networks.com/products/axseries.php http://a10networks.com/resources/solutionsheets.php http://a10networks.com/resources/casestudies.php



A. Appendix - AX configuration

A.1. Exchange Client Access Role – Outlook Web App

Note: The configuration below is with the following options:

- HTTP Compression
- SSL offload
- Transparent Redirect HTTP Clients to HTTPS
- · Transparently add "/owa" to the requests that are without it

```
slb server Exchangel 10.0.2.161
   port 80 tcp
!
slb server Exchange2 10.0.2.162
   port 80 tcp
!
health monitor hm-owa-http
method http
!
slb service-group Exchange-OWA-http tcp
    method least-connection
    health-check hm-owa-http
    member Exchange1:80
    member Exchange2:80
!
slb template client-ssl OWA-Client-Side
   cert OWA-cert-key
   key OWA-cert-key
1
slb template persist cookie persist-owa
!
slb template http tp-compress
   compression enable
!
slb template http tp-redirect-owa-https
   failover-url https://OWA-cert-key/owa
T.
slb virtual-server Exchange-OWA 10.0.1.74
   port 443 https
      service-group Exchange-OWA-http
      template http tp-compress
```



!

```
template client-ssl OWA-Client-Side
template persist cookie persist-owa
aflex insert_owa
port 80 http
template http tp-redirect-owa-https
```

A.2. Exchange Client Access Role – Exchange Control Panel

```
Note: The configuration below is with the following options:

    HTTP Compression

    SSL offload

    Transparent Redirect HTTP Clients to HTTPS

slb server Exchangel 10.0.2.161
   port 80 tcp
!
slb server Exchange2 10.0.2.162
   port 80 tcp
!
health monitor hm-owa-http
method http
!
slb service-group Exchange-OWA-http tcp
    method least-connection
    health-check hm-owa-http
    member Exchange1:80
    member Exchange2:80
!
slb template client-ssl OWA-Client-Side
   cert OWA-cert-key
   key OWA-cert-key
!
slb template persist cookie persist-owa
!
slb template http tp-compress
   compression enable
T.
slb template http tp-redirect-owa-https
   failover-url https://OWA-cert-key/owa
```


```
!
slb virtual-server Exchange-OWA 10.0.1.74
port 443 https
    service-group Exchange-OWA-http
    template http tp-compress
    template client-ssl OWA-Client-Side
    template persist cookie persist-owa
    port 80 http
    template http tp-redirect-owa-https
!
```

A.3. Exchange Client Access Role – Outlook Anywhere

```
Note: The configuration below is with the following options:
```

```
· SSL offload

    aFleX uie persistence

slb server Exchangel 10.0.2.161
   port 80 tcp
!
slb server Exchange2 10.0.2.162
   port 80 tcp
!
health monitor hm-oa-http
method http
!
slb service-group Exchange-OA-http tcp
    health-check hm-oa-http
    member Exchange1:80
    member Exchange2:80
!
slb template client-ssl OA-Client-Side
   cert OWA-cert-key
   key OWA-cert-key
!
slb virtual-server Exchange-OA 10.0.1.75
   port 443 https
      service-group Exchange-OA-http
      template client-ssl OA-Client-Side
      afleX persist-oa
```

```
All Networks
```

!

A.4. Exchange Client Access Role – Exchange ActiveSync

```
    SSL offload

    aFleX uie persistence

slb server Exchangel 10.0.2.161
   port 80 tcp
!
slb server Exchange2 10.0.2.162
   port 80 tcp
1
health monitor hm-eas-http
method http
1
slb service-group Exchange-EAS-http tcp
    method least-connection
    health-check hm-oa-http
    member Exchange1:80
    member Exchange2:80
!
slb template client-ssl EAS-Client-Side
   cert OWA-cert-key
   key OWA-cert-key
!
slb virtual-server Exchange-EAS 10.0.1.76
   port 443 https
      service-group Exchange-EAS-http
      template client-ssl EAS-Client-Side
      aFleX persist-eas
!
```



A.5. Exchange Client Access Role – RPC

```
slb server Exchangel 10.0.2.161
  port 0 tcp
      no health-check
1
slb server Exchange2 10.0.2.162
  port 0 tcp
      no health-check
!
health monitor hm-rpc-135
override-port 135
method tcp port 135
!
slb service-group Exchange-RPC tcp
   health-check hm-rpc-135
   member Exchange1:0
   member Exchange2:0
!
slb template persist source-ip persist-rpc
  match-type server
  timeout 480
!
slb template tcp TCP-Aging-Time-rpc
   idle-timeout 28800
   reset-fwd
   reset-rev
slb virtual-server Exchange-RPC 10.0.1.74
  port 0 tcp
      service-group Exchange-RPC
      template persist source-ip persist-rpc
      template tcp TCP-Aging-Time-rpc
!
```



A.6. Exchange Client Access Role – POP3

```
    POP3 healthcheck

slb server Exchangel 10.0.2.161
  port 110 tcp
!
slb server Exchange2 10.0.2.162
  port 110 tcp
1
health monitor hm-pop3
method pop3 username user1 password a10
1
slb service-group Exchange-POP3 tcp
    method least-connection
    health-check hm-pop3
    member Exchange1:110
    member Exchange2:110
!
slb template client-ssl POP3-Client-Side
   cert OWA-cert-key
   key OWA-cert-key
!
slb virtual-server Exchange-POP3S 10.0.1.74
   port 995 ssl-proxy
      service-group Exchange-POP3
      template client-ssl POP3-Client-Side
!
```



A.7. Exchange Client Access Role – IMAP4

Note: The configuration below is with the following options: • SSL offload • IMAP4 healthcheck

```
slb server Exchangel 10.0.2.161
   port 143 tcp
!
slb server Exchange2 10.0.2.162
   port 143 tcp
1
health monitor hm-imap4
method imap username user1 password a10
1
slb service-group Exchange-IMAP4 tcp
    method least-connection
    health-check hm-imap4
    member Exchange1:143
   member Exchange2:143
!
slb template client-ssl IMAP4-Client-Side
   cert OWA-cert-key
   key OWA-cert-key
!
slb virtual-server Exchange-IMAP4S 10.0.1.74
   port 993 ssl-proxy
      service-group Exchange-IMAP4
      template client-ssl IMAP4-Client-Side
!
```



A.8. Exchange Client Access Role – Exchange Web Services

```
    HTTP Compression

    · SSL offload
slb server Exchangel 10.0.2.161
  port 80 tcp
!
slb server Exchange2 10.0.2.162
  port 80 tcp
1
health monitor hm-owa-http
method http
1
slb service-group Exchange-OWA-http tcp
    method least-connection
    health-check hm-owa-http
    member Exchange1:80
   member Exchange2:80
!
slb template client-ssl OWA-Client-Side
  cert OWA-cert-key
  key OWA-cert-key
!
slb template persist cookie persist-owa
1
slb template http tp-compress
  compression enable
!
slb virtual-server Exchange-OWA 10.0.1.74
  port 443 https
      service-group Exchange-OWA-http
      template http tp-compress
      template client-ssl OWA-Client-Side
      template persist cookie persist-owa
!
```



A.9. Exchange Client Access Role – Autodiscover

```
    HTTP Compression

    · SSL offload
slb server Exchangel 10.0.2.161
  port 80 tcp
!
slb server Exchange2 10.0.2.162
  port 80 tcp
1
health monitor hm-owa-http
method http
1
slb service-group Exchange-OWA-http tcp
    method least-connection
    health-check hm-owa-http
    member Exchange1:80
   member Exchange2:80
!
slb template client-ssl OWA-Client-Side
  cert OWA-cert-key
  key OWA-cert-key
!
slb template persist cookie persist-owa
1
slb template http tp-compress
  compression enable
!
slb virtual-server Exchange-OWA 10.0.1.74
  port 443 https
      service-group Exchange-OWA-http
      template http tp-compress
      template client-ssl OWA-Client-Side
      template persist cookie persist-owa
!
```



A.10. Exchange Client Access Role – Offline Address Book distribution

Note:

- · For Web Based distribution: Same as OWA
- · For public folder distribution: Same as RPC

A.11. Exchange Client Access Role – SMTP

```
Note: The configuration below is with the following options:

• TLS (STARTTLS) offload
```

```
slb server Exchangel 10.0.2.161
   port 25 tcp
!
slb server Exchange2 10.0.2.162
   port 25 tcp
!
health monitor hm-smtp
 method smtp domain example.com
!
slb service-group Exchange-SMTP tcp
    method least-connection
    health-check hm-smtp
    member Exchange1:25
    member Exchange2:25
!
slb template client-ssl SMTP-Client-Side
   cert OWA-cert-key
   key OWA-cert-key
!
slb template smtp STARTTLS-SMTP
   server-domain example.com
   starttls optional
!
slb virtual-server Exchange-SMTP 10.0.1.74
   port 25 smtp
      service-group Exchange-SMTP
      template smtp STARTTLS-SMTP
      template client-ssl SMTP-Client-Side
!
```



A.12. Exchange Client Access Role – Multiple Exchange Services with a Single VIP (OWA + OA + EAS on same servers)

Note: The configuration below is with the following options: SSL offload slb server Exchangel 10.0.2.161 port 80 tcp ! slb server Exchange2 10.0.2.162 port 80 tcp 1 health monitor hm-exchange-http method http 1 slb service-group Exchange-http tcp health-check hm-exchange-http member Exchange1:80 member Exchange2:80 ! slb template persist source-ip persist-exchange-https timeout 30 ! slb template client-ssl exchange-https-Client-Side cert OWA-cert-key key OWA-cert-key 1 slb virtual-server Exchange-HTTPS 10.0.1.74 port 443 https service-group Exchange-http template client-ssl exchange-https-Client-Side template persist source-ip persist-exchange-https 1



A.13. Exchange Client Access Role – Multiple Exchange Services with a Single VIP (OWA + OA + EAS on different servers)

```
    SSL offload

slb server Exchangel-OWA 10.0.2.161
  port 80 tcp
!
slb server Exchange2-OWA 10.0.2.162
  port 80 tcp
1
slb server Exchange1-OA 10.0.2.163
  port 80 tcp
1
slb server Exchange2-OA 10.0.2.164
  port 80 tcp
!
slb server Exchange1-AS 10.0.2.165
  port 80 tcp
!
slb server Exchange2-AS 10.0.2.166
  port 80 tcp
1
health monitor hm-owa-http
method http
1
health monitor hm-oa-http
method http
1
health monitor hm-as-http
method http
1
slb service-group Exchange-OWA-http tcp
    method least-connection
    health-check hm-owa-http
    member Exchange1-OWA:80
    member Exchange2-OWA:80
!
slb service-group Exchange-OA-http tcp
    method least-connection
```



```
health-check hm-oa-http
   member Exchange1-OA:80
   member Exchange2-OA:80
1
slb service-group Exchange-AS-http tcp
   method least-connection
   health-check hm-as-http
   member Exchange1-AS:80
   member Exchange2-AS:80
!
slb template client-ssl exchange-https-Client-Side
  cert OWA-cert-key
  key OWA-cert-key
!
slb template persist source-ip persist-exchange-https
  timeout 30
!slb virtual-server Exchange-HTTPS 10.0.1.74
  port 443 https
      service-group Exchange-OWA-http
      template client-ssl exchange-https-Client-Side
      aflex persist-https-per-access
      template persist source-ip persist-exchange-https
!
```

A.14. Exchange Client Access Role – Multiple Exchange Services with a Single VIP (OWA + OA + EAS + RPC + SMTP on on same servers)

```
    SSL offload
    TLS (STARTTLS) offload
    slb server Exchangel 10.0.2.161
    port 80 tcp
    port 25 tcp
```

```
port 0 tcp
```

```
no health-check
```

```
!
slb server Exchange2 10.0.2.162
port 80 tcp
```



```
port 25 tcp
   port 0 tcp
      no health-check
1
health monitor hm-exchange-http
method http
1
health monitor hm-smtp
method smtp domain example.com
1
health monitor hm-rpc-135
override-port 135
method tcp port 135
!
slb service-group Exchange-http tcp
    health-check hm-exchange-http
    member Exchange1:80
    member Exchange2:80
!
slb service-group Exchange-SMTP tcp
    method least-connection
    health-check hm-smtp
    member Exchange1:25
   member Exchange2:25
1
slb service-group Exchange-RPC tcp
    health-check hm-rpc-135
   member Exchange1:0
   member Exchange2:0
!
slb template smtp STARTTLS-SMTP
   server-domain example.com
   starttls optional
!
slb template persist source-ip persist-exchange-https
   timeout 30
1
slb template client-ssl exchange-https-Client-Side
   cert OWA-cert-key
```



```
key OWA-cert-key
!
slb template client-ssl SMTP-Client-Side
  cert OWA-cert-key
  key OWA-cert-key
!
slb template persist source-ip persist-rpc
  match-type server
  timeout 480
!
slb template tcp TCP-Aging-Time-rpc
   idle-timeout 28800
  reset-fwd
   reset-rev
slb virtual-server Exchange-HTTPS 10.0.1.74
  port 0 tcp
      service-group Exchange-RPC
      template persist source-ip persist-rpc
      template tcp TCP-Aging-Time-rpc
  port 25 smtp
      service-group Exchange-SMTP
      template smtp STARTTLS-SMTP
      template client-ssl SMTP-Client-Side
!
  port 443 https
      service-group Exchange-http
      template client-ssl exchange-https-Client-Side
      template persist source-ip persist-exchange-https
```



A15. aFleX script to block specific services(Optional):

The aFleX script below is an example showing how to block all Exchange services except OWA and OAB distributions.

```
when HTTP REQUEST {
switch -glob [string tolower [HTTP::uri]] {
 "/owa*" { return }
 "/oab*" { return }
 "/ews*" { drop ; return }
  "/rpc*" { drop ; return }
 "/microsoft-server-activesync*" { drop ; return }
 "/public*" { drop ; return }
 "/rpcwithcert*" { drop ; return }
 "/autodiscover*" { drop ; return }
 "/powershell*" { drop ; return }
}
if { [HTTP::uri] equals "/"} {
HTTP::uri /owa
}
}
```



A16. aFleX persistence script(Optional):

Some Exchange services can only support cookie persistence. The aFleX script shown below is an example of how to use persistence to achieve better load distribution across Exchange services.

```
when HTTP REQUEST {
switch -qlob [string tolower [HTTP::uri]] {
  "/ews*" { set cookie 1 ; pool CAS-80 ; return }
  "/rpc*" { persist uie [IP::client addr] ; pool CAS-80 ; return }
  "/microsoft-server-activesync*" { persist uie [IP::client addr] ;
pool CAS-80 ; return }
  "/owa*" { set cookie 1 ; pool CAS-80 ; return }
  "/oab*" { persist uie [IP::client addr] ; pool CAS-80 ; return }
  "/public*" { persist uie [IP::client addr] ; pool CAS-80 ; return }
"/rpcwithcert*" { persist uie [IP::client_addr] ; pool CAS-80 ; re-
"/autodiscover*" { persist uie [IP::client_addr] ; pool CAS-80 ; re-
  "/powershell*" { persist uie [IP::client_addr] ; pool CAS-80; return
}
}
if { not([HTTP::uri] starts with "/owa") } {
HTTP::uri /owa[HTTP::uri]
set cookie 1
pool CAS-80
}
}
when HTTP RESPONSE {
if { not($cookie == 1) } {
persist add uie [IP::client addr] 1800
}
}
```

