DEPLOYMENT GUIDE

Microsoft Exchange 2013

Table of Contents

Disclaimer

This document does not create any express or implied warranty about A10 Networks or about its products or services, including but not limited to fitness for a particular use and noninfringement. A10 Networks has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks for current information regarding its products or services. A10 Networks' products and services are subject to A10 Networks' standard terms and conditions.

Introduction

Microsoft Exchange has reached another milestone with the release of Exchange 2013, which has achieved status as the leading global Unified Communication Solution. While Microsoft has released exemplary versions of Exchange over the years, the 2013 edition is far less complex compared to previous versions. Exchange 2013 builds upon the previous Exchange Server 2010 architecture but is redesigned for simple installation, ease-of-management, minimized complexity and to scale.

Exchange's major features consist of electronic mail, calendaring, integration support for Lync and SharePoint, contacts and tasks, support for mobile and web-based information access, and support for data storage. This deployment guide contains configuration procedures for A10 Networks® Thunder® ADC line of Application Delivery Controllers to support a Microsoft Exchange Server 2013 solution.

Deployment Guide Prerequisites

This Microsoft Exchange 2013 Thunder ADC integration example has the following prerequisites (based on tested configuration):

- The A10 Thunder ADC must be running A10 Networks Advanced Core Operating System (ACOS®) version 2.6.x or higher.
- Microsoft Exchange 2013 has been tested with A10 hardware and virtual appliances.
- Thunder ADC can be deployed in routed mode, one-arm mode and transparent mode.

For a list of additional deployment modes that the Thunder ADC can support, please visit the following URL: https://www.a10networks.com/resources/deployment-guides

- Both IPv4 and IPv6 are supported. The examples in this deployment guide use IPv4.
- Windows Server 2008 R2 Standard, Enterprise and Datacenter Editions or higher, or Windows Server 2012.
- Exchange 2013 supported clients:
  - Outlook 2013 Preview
  - Outlook 2010 SP1 with April 2012 Cumulative Update
  - Outlook 2007 SP3 with July 2012 Cumulative Update
  - Entourage 2008 for Mac, Web Services Edition
  - Outlook for Mac 2011
  - Eudora 7.1 email client

Deployment Notes and Updates

1. Exchange 2013 Cumulative Update 5 can now support SSL Offload deployments.

http://technet.microsoft.com/en-us/library/jj907309(v=exchg.150).aspx

http://blogs.technet.com/b/exchange/archive/2014/05/27/released-exchange-server-2013-cumulative-update-5.aspx

2. For MAPI over HTTP support you must use only Source IP Persistence instead of Cookie Persistence.

http://technet.microsoft.com/en-us/library/dn635177%28v=exchg.150%29.aspx

Note: *Refer to the support and configuration notes section for feature support updates.*

Exchange Server Roles

In Microsoft Exchange Server 2010 and Exchange Server 2007, multiple server roles were available. These included roles such as Client Access, Mailbox, Hub Transport, and Unified Messaging. For Exchange Server 2013, the new architecture consolidates the number of server roles from four to two: the Client Access Server (CAS) role and the Mailbox Server (MS) role. To understand the new features of Exchange 2013, refer to the following URL:

http://technet.microsoft.com/en-us/library/jj150540%28v=exchg.150%29.aspx

In Exchange 2013, the Client Access Array (CAA) and the Database Availability Group (DAG) are able to provide load balancing, high availability and fault tolerance to the Exchange service.

Additionally, the Client Access Servers serve as a proxy for Microsoft Office Outlook, Outlook Web App, Mobile Devices, POP and SMTP. The Client Access Servers also can perform authentication and redirection.

Accessing the Thunder ADC Device

This section describes how to access the Thunder ADC from a Command Line Interface (CLI) or Graphical User Interface (GUI):

- CLI – The CLI is a text-based interface in which you type commands on a command line. You can access the CLI directly through the serial console or over the network using either of the following protocols:
  - Secure protocol – Secure Shell (SSH) version 2
  - Unsecure protocol – Telnet (if enabled)
- GUI – This is a web-based interface in which you click buttons, menus and other graphical icons to access the configuration or management pages. From these pages, you can type or select values to configure or manage the device. You can access the GUI using the following protocol:
- Secure protocol – Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)

Note: HTTP requests are redirected to HTTPS by default on the Thunder ADC.

Default Access Information:

- Default Username: "admin"
- Default password: "a10"
- Default IP Address of the device: "172.31.31.31"

(For detailed information on how to access the Thunder ADC, refer to the System Configuration and Administration Guide.[1])

Architecture Overview

The diagram below provides an architectural overview of how Exchange 2013 can be optimized with ACOS.

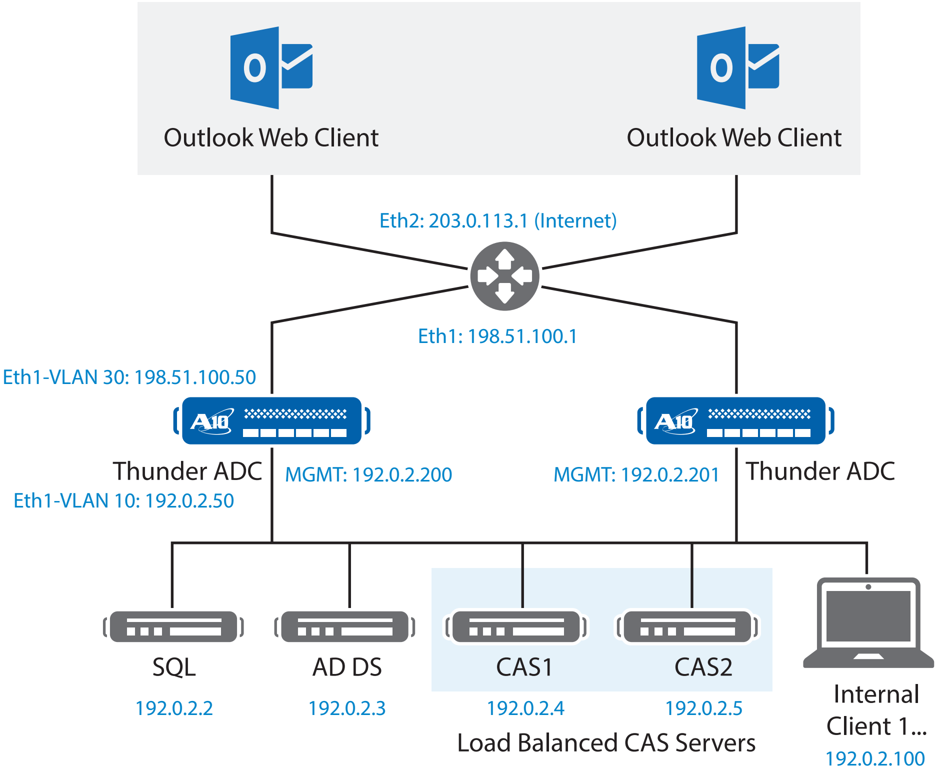


Figure 1: Exchange 2013 lab overview

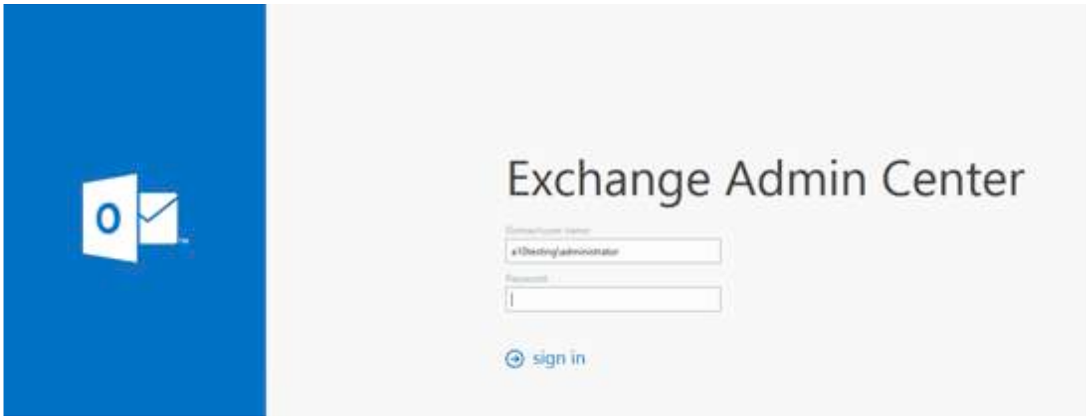
[1] https://files.a10networks.com/support-axseries/hardware-install-guides/index.html?_ga=1.84701273.1796516912.1400535969#thunder (site requires registration)

Validating Exchange 2013 Configuration

Before you start making configuration changes from the Thunder ADC, use this section to validate the Exchange 2013 server configuration.

1. Open a web browser and navigate to one of the Exchange CAS devices.
2. Navigate to https://CAS-IP-Address/ecp

   This step navigates to the Exchange Control Panel, which is also known as Exchange Admin Center, on the Exchange 2013 server.
3. Log in with a domain administrator credentials.



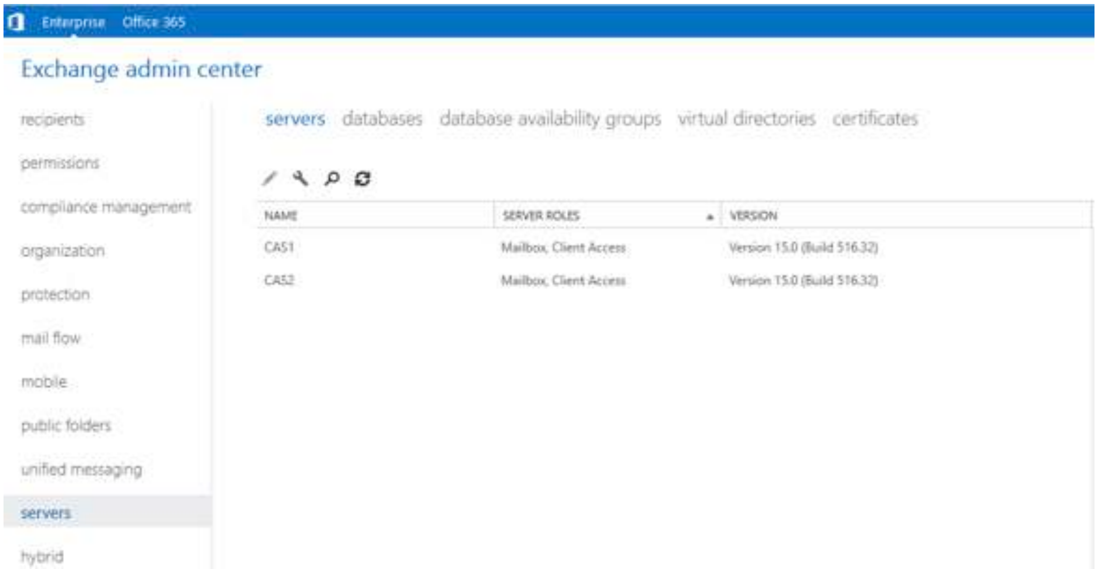
Exchange Admin Center

Domain\user name: a10testing\administrator

Password:

Figure 2: Exchange Admin Center portal

4. On the left menu panel, click Servers and on the top panel select Servers again. The menu provides a list of CAS servers deployed within Exchange 2013. These are the CAS servers that will be configured as real servers on the Thunder ADC and are referenced by a virtual IP (VIP) address.

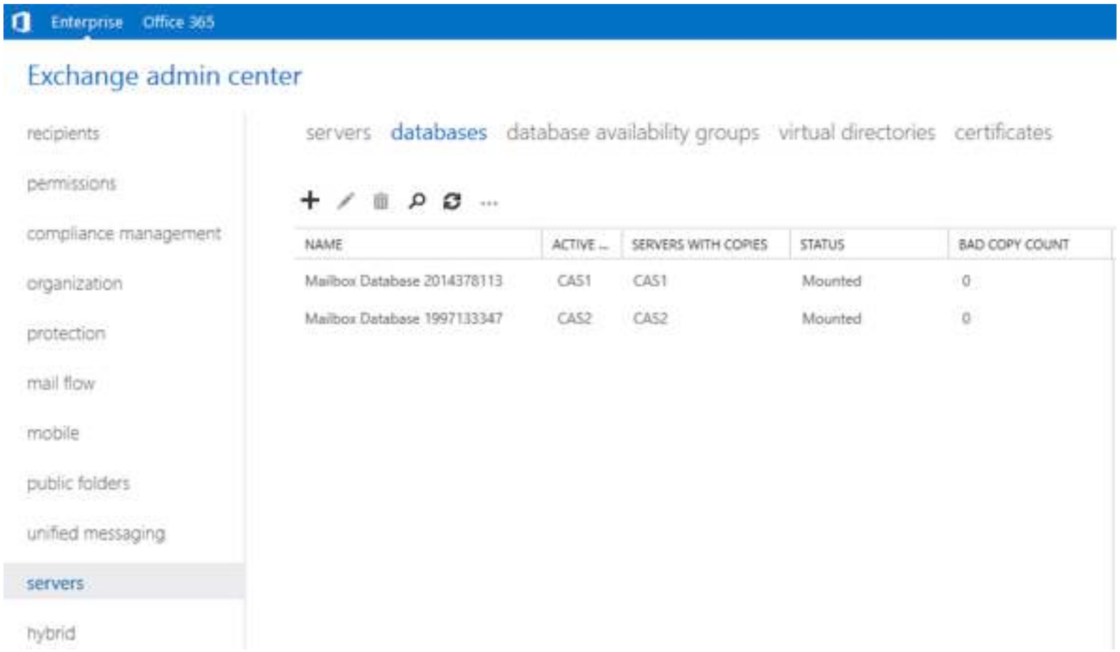


NAME	SERVER ROLES	VERSION
CAS1	Mailbox, Client Access	Version 15.0 (Build 516.32)
CAS2	Mailbox, Client Access	Version 15.0 (Build 516.32)

Figure 3: Exchange 2013 configuration

In the top menu, select Databases. A menu appears, listing the databases configured in your solution. The databases must be configured within database availability groups (DAGs) for redundancy purposes. To understand how to configure DAGs in Exchange 2013, refer to the following URL:

http://technet.microsoft.com/en-us/library/dd351172%28v=exchg.150%29.aspx



NAME	ACTIVE ...	SERVERS WITH COPIES	STATUS	BAD COPY COUNT
Mailbox Database 2014378113	CAS1	CAS1	Mounted	0
Mailbox Database 1997133347	CAS2	CAS2	Mounted	0

Figure 4: Exchange 2013 DAG setup

Once the prerequisites are configured, verify that incoming and outgoing mail can be received or sent before adding the Thunder ADC to the solution. Do not begin deployment of the ACOS solution unless Exchange 2013 is functioning correctly.

Deployment Options

This deployment guide provides steps for the following deployment options:

- **Single VIP, multiple services:** Layer 4 one-to-many mapping of a single VIP to multiple services. With this option, the Thunder ADC is configured with a single VIP bound to multiple Exchange services such as OWA, ECP, ActiveSync (Mobile), Offline Address Book (OAB), Outlook Anywhere and Autodiscover. This option provides support for Layer 4 SLB features only.
- **Multiple VIPs, multiple services:** Layer 7 one-to-one mapping of a separate VIP to each service. With this option, the Thunder ADC is configured with multiple VIPs that each are bound to a separate Exchange service. This option provides support for Layer 4 and Layer 7 SLB features.

A10 Pre-staging Considerations

It's highly recommended to configure Health Monitor and Source Network Address Translation (SNAT) since they provide more flexibility for network and server farm design, and also more your network resiliency. If your network topology is based on "one-arm" deployment, and internal clients reside on the same subnet as the VIP address for the Exchange 2013 server, SNAT is required.

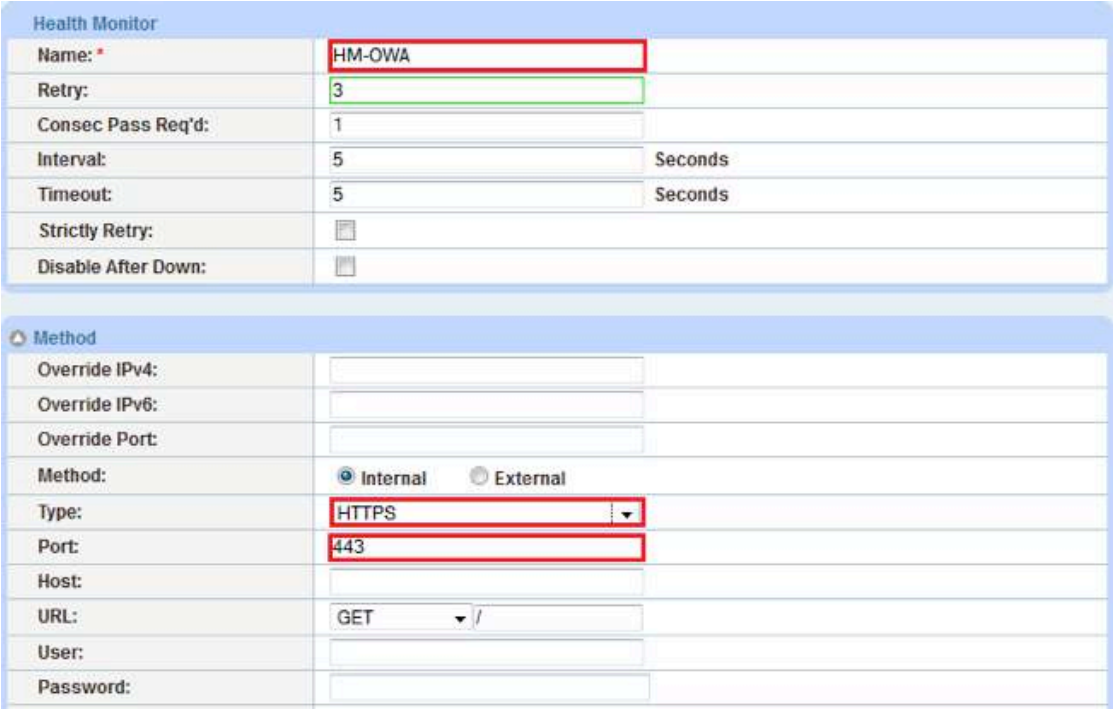
Note*: The Virtual Server is also known as the "Virtual IP" (or "VIP") that a client accesses during an initial request.*

Health Monitor Configuration (Optional)

ACOS can be configured to automatically initiate health status checks for real servers and service ports. Health checks are used to assure that all requests are sent to functional and available servers. If a server or service does not respond appropriately to a health check, the server is removed from the list of available servers until it responds to the health checks appropriately. At this point, the server is automatically added back to the list of available servers.

To configure a health check on the Thunder ADC:

1. Navigate to Config Mode > SLB > Health Monitor > Health Monitor.
2. Select Add.
3. In the Name field, enter "HM-OWA".
4. Select Method "HTTPS".
5. Click OK, and then proceed to the next section to configure the service group.



Health Monitor

Name: *	HM-OWA	
Retry:	3	
Consec Pass Req'd:	1	
Interval:	5	Seconds
Timeout:	5	Seconds
Strictly Retry:	□	
Disable After Down:	□	

Method

Override IPv4:	
Override IPv6:	
Override Port:	
Method:	● Internal ○ External
Type:	HTTPS
Port:	443
Host:	
URL:	GET /
User:	
Password:	

Figure 5: Health monitor configuration

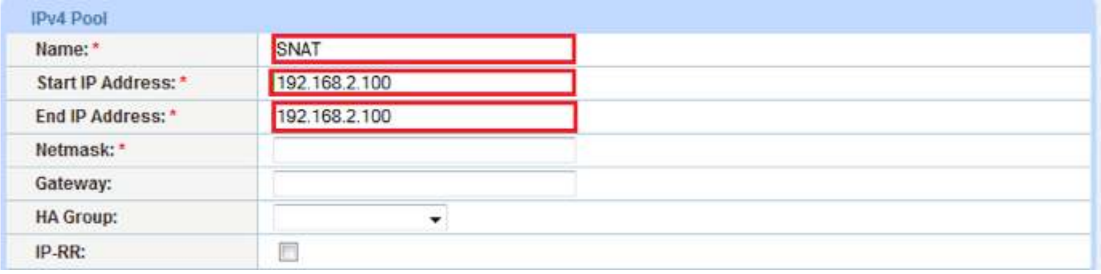
Note: All Exchange 2013 health checks must use the HTTPS (port 443 option), since clients connect to the CAS servers using HTTPS. The health check can be used with either deployment option.

Source NAT Configuration

This section shows how to configure the IP address pool to be used for IP Source Network Address Translation (SNAT). When traffic from a client accesses the VIP address (for example: 192.168.2.100), the client requests are "source NAT-ed", which means that the Thunder ADC replaces the client's source IP address with an address from a pool of source NAT addresses. SNAT is required for "one-arm" mode deployments and if the internal clients reside on the same subnet as the VIP.

Follow the procedure below to configure the address pool used in Source NAT.

1. Navigate to Config Mode> IP Source NAT > IPv4 Pool.
2. Click Add.
3. Enter the following:
   a. NAT: "SNAT"
   b. Start IP Address: "192.0.2.100"
   c. End IP Address: "192.0.2.100"
   d. Netmask: "255.255.255.0"



IPv4 Pool

Name: *	SNAT
Start IP Address: *	192.168.2.100
End IP Address: *	192.168.2.100
Netmask: *	
Gateway:	
HA Group:	
IP-RR:	□

Figure 6: Source NAT pool configuration

4. Click **OK**, then click **Save** to save the configuration.

Note: *In the Virtual Service configuration section, you can apply the Source NAT pool to the VIP.*

Note: *When using the Thunder ADC in a High Availability (HA) configuration, an HA Group must be selected to prevent duplicate IP addresses from occurring within the Source NAT Pool.*

HTTP-to-HTTPS Redirect (Optional)

This section explains how to redirect HTTP (80)-based traffic to use HTTPS (443), by using A10 Networks® aFleX® Deep Packet Inspection (DPI) Scripting Technology. aFleX is based on a standard scripting language, TCL, and enables the Thunder ADC to perform Layer 7 deep-packet inspection (DPI). For examples of aFleX scripts, please refer to the following URL for additional aFleX script examples:

https://www.a10networks.com/products/aflex-advanced-scripting-layer-4-7-traffic-management

For this feature, the Thunder ADC must have virtual server port 80 configured. The aFleX script must be bound to the virtual port.

To configure a transparent HTTPS redirect using aFleX:

1. Navigate to **Config Mode** > **SLB** > **Service** > **Virtual Service**.
2. Configure a VIP with virtual service HTTP (port 80).
3. Under the aFleX option, select "Redirect1".

Note: *"Redirect1" aFleX is a preconfigured aFleX script to redirect all HTTP (Port 80) traffic to HTTPS (Port 443).*

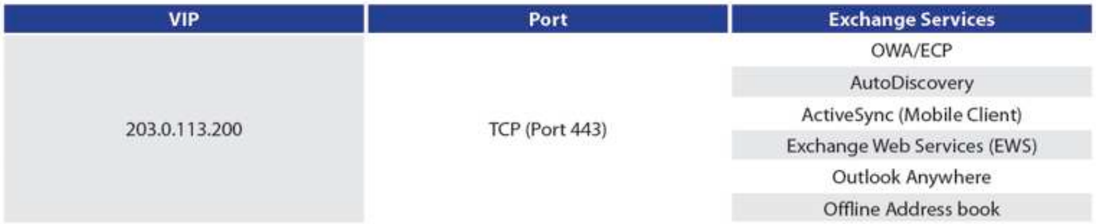
Redirect Script Content:

```
when HTTP_REQUEST {
HTTP::redirect https://[HTTP::host][HTTP::uri]
}
```

Layer 4 One-to-Many Option

This section of the deployment guide provides a basic load balancing solution for Exchange 2013. Health checks and IP Source NAT option are required, depending on preference and deployment architecture.

All Exchange 2013 traffic in this deployment option is destined for a single Virtual IP (VIP) that uses service type TCP. The port number is mapped to all the Exchange services.

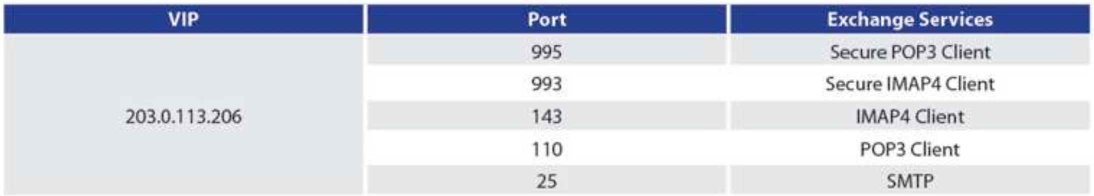


VIP	Port	Exchange Services
203.0.113.200	TCP (Port 443)	OWA/ECP
		AutoDiscovery
		ActiveSync (Mobile Client)
		Exchange Web Services (EWS)
		Outlook Anywhere
		Offline Address book

Figure 7: Exchange 2013 Layer 4 Configuration

Optional VIP Configuration

You can also apply the following optional ports to be enabled in the same (or even a different) VIP for non-compliant email client support:



VIP	Port	Exchange Services
203.0.113.206	995	Secure POP3 Client
	993	Secure IMAP4 Client
	143	IMAP4 Client
	110	POP3 Client
	25	SMTP

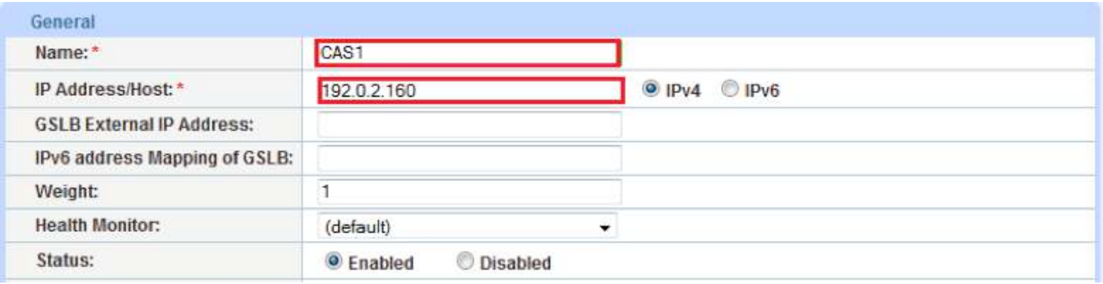
Figure 8: Exchange 2013 optional ports

Server Confguration

Follow the procedure below to configure the Exchange CAS servers on the Thunder ADC:

1. Navigate to Config Mode > SLB > Service > Server.
2. Click Add to add a new server.
3. Within the Server section, enter the following required information:
   a. Name: "CAS1"
   b. IP address /Host: "192.0.2.160"

Note: Enter additional servers if necessary.

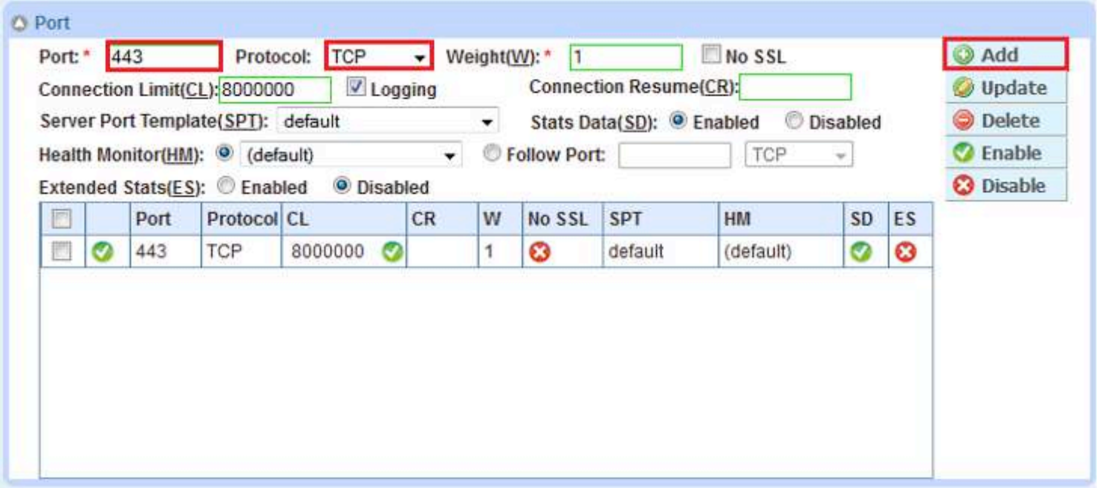


General

Name: *	CAS1
IP Address/Host: *	192.0.2.160 ● IPv4 ○ IPv6
GSLB External IP Address:	
IPv6 address Mapping of GSLB:	
Weight:	1
Health Monitor:	(default)
Status:	● Enabled ○ Disabled

Figure 9: Server configuration

4. To add a port to the server configuration:
   a. Enter the port number in the **Port** field.
   b. Select the **Protocol**.
   c. Click **Add**.
   d. Repeat the steps if you have any other ports/protocols to add (For an example, see Figure 8: Exchange 2013 optional ports)



Port: * 443 Protocol: TCP Weight(W): * 1 □ No SSL

Connection Limit(CL): 8000000 ☑ Logging Connection Resume(CR):

Server Port Template(SPT): default Stats Data(SD): ● Enabled ○ Disabled

Health Monitor(HM): ● (default) ○ Follow Port: TCP

Extended Stats(ES): ○ Enabled ● Disabled

□		Port	Protocol	CL	CR	W	No SSL	SPT	HM	SD	ES
□	✓	443	TCP	8000000 ✓		1	✗	default	(default)	✓	✗

Figure 10: Server port configuration

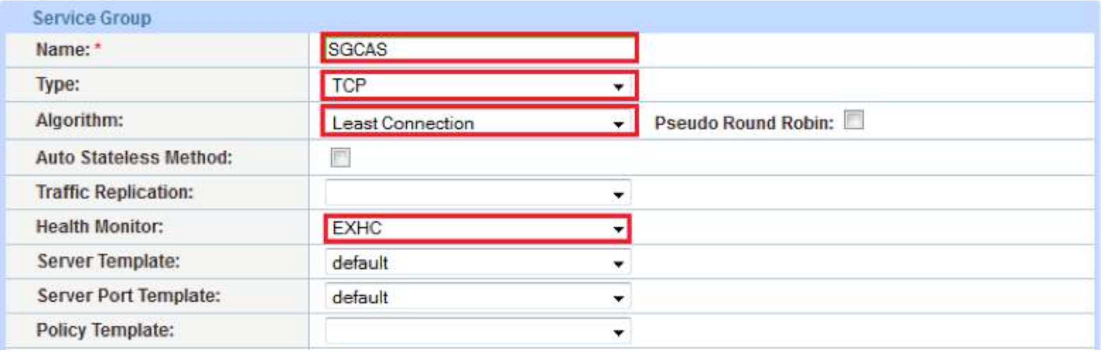
Repeat the steps if you have multiple servers.

5. Click OK, and then click **Save** to save the configuration.

Service Group Configuration

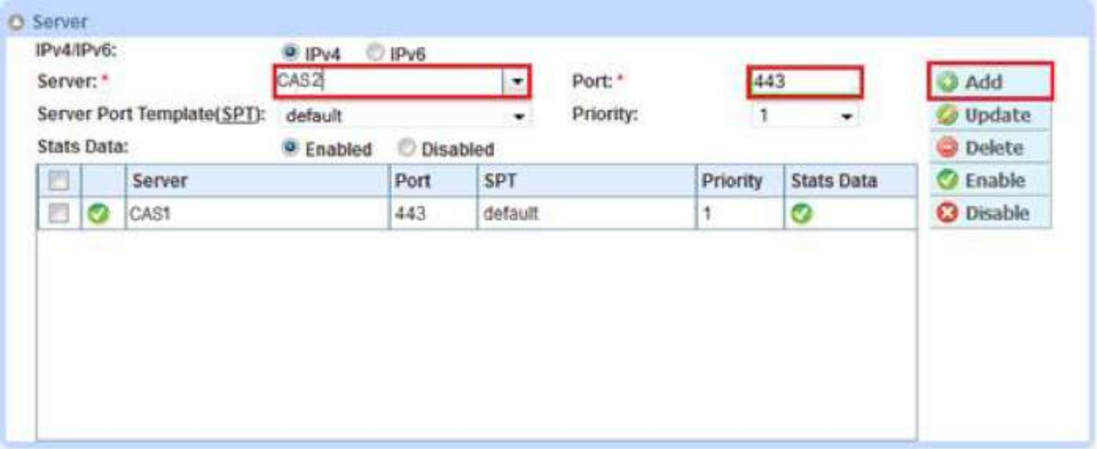
Follow the procedure below to configure a service group.

1. Navigate to **Config Mode > SLB > Service > Service Group.**
2. Click **Add**.
3. Enter or select the following values:
   a. **Name**: "SGCAS"
   b. **Type**: "TCP"
   c. **Algorithm**: "Least Connection"
   d. **Health Monitor**: "EXHC"
4. In the Server section, select a server from the Server drop-down list and enter "443" in the **Port** field.
5. Click **Add**. Repeat for each server.



Name: *	SGCAS
Type:	TCP
Algorithm:	Least Connection Pseudo Round Robin: □
Auto Stateless Method:	□
Traffic Replication:	
Health Monitor:	EXHC
Server Template:	default
Server Port Template:	default
Policy Template:	

Figure 11: Service group configuration



Server

IPv4/IPv6: ● IPv4 ○ IPv6

Server: * CAS2

Port: * 443

Server Port Template(SPT): default

Priority: 1

Stats Data: ● Enabled ○ Disabled

□		Server	Port	SPT	Priority	Stats Data
□	✓	CAS1	443	default	1	✓

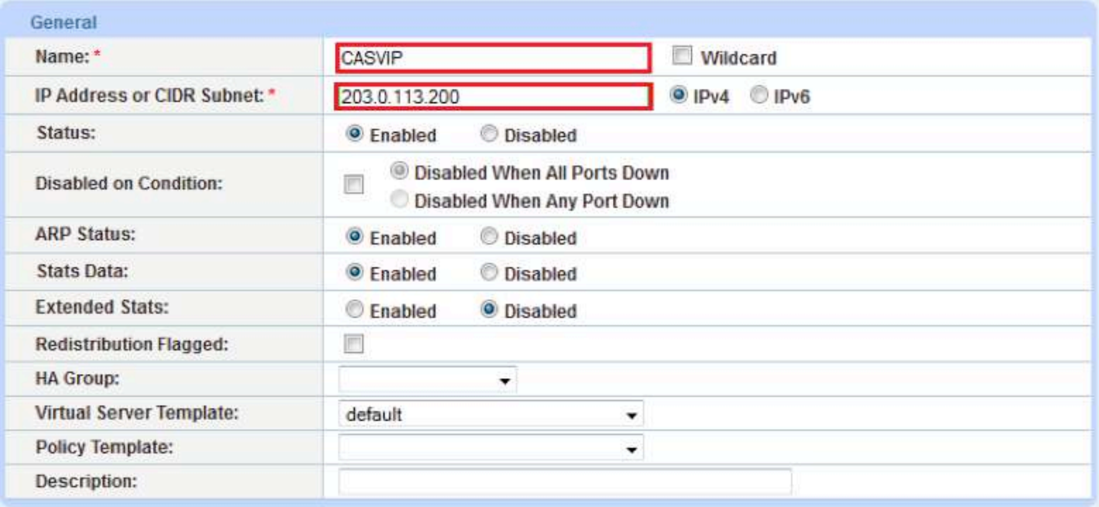
Figure 12: Server configuration

6. Repeat the steps if you have more protocols/ports or service-group to add.
7. Click **OK**, then click **Save** to save the configuration.

Virtual Server Configuration

This section contains the basic configuration for a Virtual Server. The Virtual Server is also known as the "Virtual IP" ("VIP") and is the IP address that a client accesses during an initial request.

1. Navigate to **Config Mode > SLB > Service > Virtual Service.**
2. In the General section, enter the name of the VIP and its IP address:
   a. **Name**: "CASVIP"
   b. **IP Address**: "203.0.113.200"

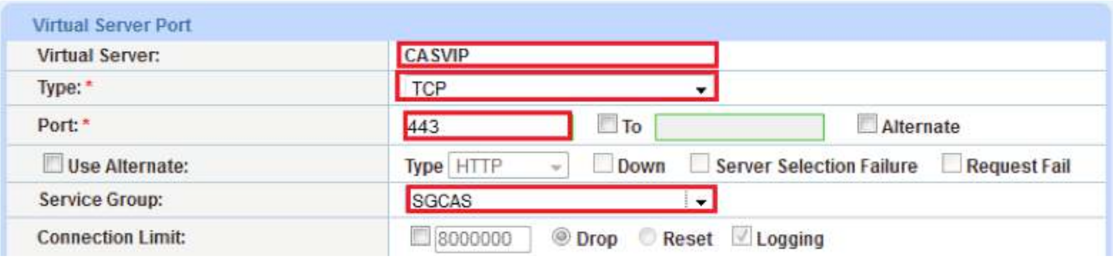


General

Name: *	CASVIP □ Wildcard
IP Address or CIDR Subnet: *	203.0.113.200 ● IPv4 ○ IPv6
Status:	● Enabled ○ Disabled
Disabled on Condition:	□ ● Disabled When All Ports Down ○ Disabled When Any Port Down
ARP Status:	● Enabled ○ Disabled
Stats Data:	● Enabled ○ Disabled
Extended Stats:	○ Enabled ● Disabled
Redistribution Flagged:	□
HA Group:	
Virtual Server Template:	default
Policy Template:	
Description:	

Figure 13: Virtual server (VIP) configuration

3. In the Port section, click **Add**.



Virtual Server Port

Virtual Server:	CASVIP
Type: *	TCP
Port: *	443 □ To □ Alternate
□ Use Alternate:	Type HTTP □ Down □ Server Selection Failure □ Request Fail
Service Group:	SGCAS
Connection Limit:	□ 8000000 ● Drop ○ Reset ☑ Logging

Figure 14: Virtual-server port configuration

4. Select the following values:

   a. **Virtual Server:** "TCP"

Note: *The port number will be pre-selected after selecting the protocol type.*

   b. **Port**: 443

   c. **Address**: "MISVIP"

   d. **Service Group**: "SGCAS"

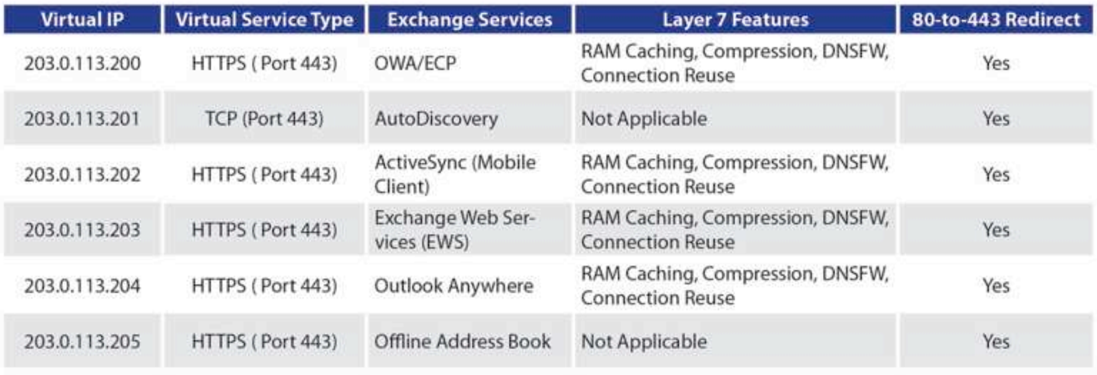
5. Repeat the steps if you have more VIPs to create.
6. Click **OK**, then click **Save** to save the configuration.

Layer 7 One-to-One Option

This section shows an advanced configuration for the Thunder ADC with Exchange 2013 CAS Servers. The advanced configuration increases server performance with features such as Compression, RAM Caching, and DNS Application Firewall.

The first step in the advanced configuration is to predefine all the optimization and performance features in configuration templates. Once all the performance features are defined in the templates, you can bind the features to the VIP.

Note: *This section moves directly from the basic configuration into advanced configuration, based on the assumption that you are already familiar with the basics of configuring the servers, service group, VIP, and virtual service. In addition, the VIP must have port 80 and 443 configured for 80-to-443 redirect to function.*

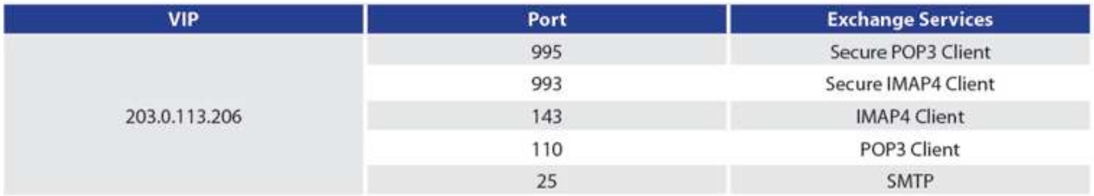


Virtual IP	Virtual Service Type	Exchange Services	Layer 7 Features	80-to-443 Redirect
203.0.113.200	HTTPS (Port 443)	OWA/ECP	RAM Caching, Compression, DNSFW, Connection Reuse	Yes
203.0.113.201	TCP (Port 443)	AutoDiscovery	Not Applicable	Yes
203.0.113.202	HTTPS (Port 443)	ActiveSync (Mobile Client)	RAM Caching, Compression, DNSFW, Connection Reuse	Yes
203.0.113.203	HTTPS (Port 443)	Exchange Web Services (EWS)	RAM Caching, Compression, DNSFW, Connection Reuse	Yes
203.0.113.204	HTTPS (Port 443)	Outlook Anywhere	RAM Caching, Compression, DNSFW, Connection Reuse	Yes
203.0.113.205	HTTPS (Port 443)	Offline Address Book	Not Applicable	Yes

Figure 15: Exchange 2013 Option 2 setup

Optional VIP Configuration

You can apply the following optional ports to be enabled in any existing VIP configured above or new separate VIP for non-compliant email client support:



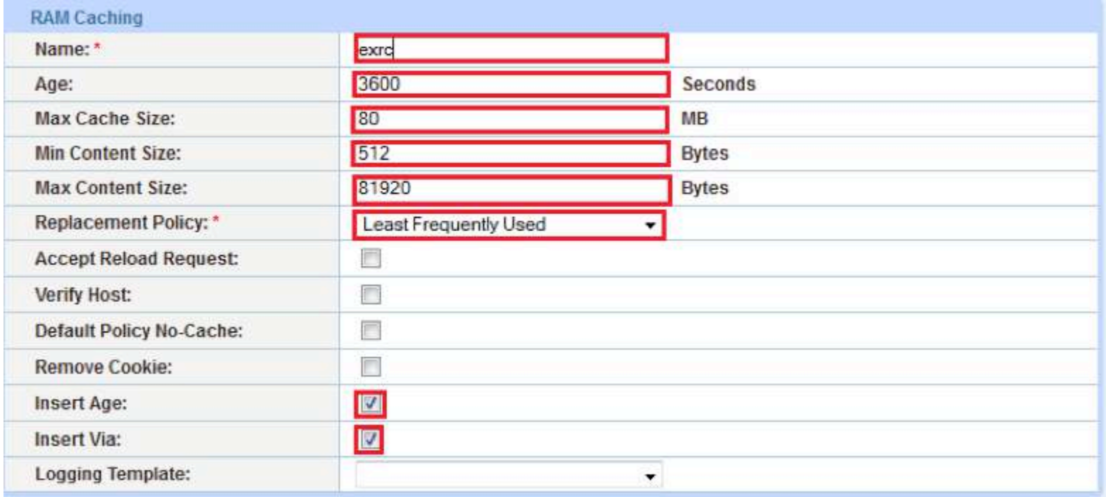
VIP	Port	Exchange Services
203.0.113.206	995	Secure POP3 Client
	993	Secure IMAP4 Client
	143	IMAP4 Client
	110	POP3 Client
	25	SMTP

Figure 16: Exchange 2013 optional ports

RAM Caching Template

RAM Caching stores cacheable data from the servers on the Thunder ADC, thus reducing overhead and increasing capacity for the Exchange CAS servers. RAM Caching reduces the number of connections and server requests that need to be processed. To create a RAM Caching template, follow the steps below:

1. Navigate to **Config Mode** > **SLB** > **Service** > **Template** > **Application** > **RAM Caching**.
2. Click **Add**.
3. Enter the following values:
   a. **Name**: "exrc".
   b. **Age**: 3600 seconds
   c. **Max Cache Size**: 80 MB
   d. **Min Content Size**: 512 Bytes
   e. **Max Content Size**: 81920 Bytes
   f. **Replacement Policy**: Least Frequently Used
4. Select the **Insert Age** and **Insert Via** checkboxes to enable these options.
5. Click **OK** and then click **Save** to store your configuration changes.



RAM Caching

Name: *	exrc	
Age:	3600	Seconds
Max Cache Size:	80	MB
Min Content Size:	512	Bytes
Max Content Size:	81920	Bytes
Replacement Policy: *	Least Frequently Used ▾	
Accept Reload Request:	□	
Verify Host:	□	
Default Policy No-Cache:	□	
Remove Cookie:	□	
Insert Age:	☑	
Insert Via:	☑	
Logging Template:	▾	

Figure 17: Exchange 2013 RAM Caching template

Note: *The RAM Caching policy option is not required unless you have specific data that requires caching, no caching or invalidate. These policy options can be configured in the policy form of the RAM Caching template. For additional information on RAM caching policy, please refer to the Application Delivery and Server Load Balancing Guide.*

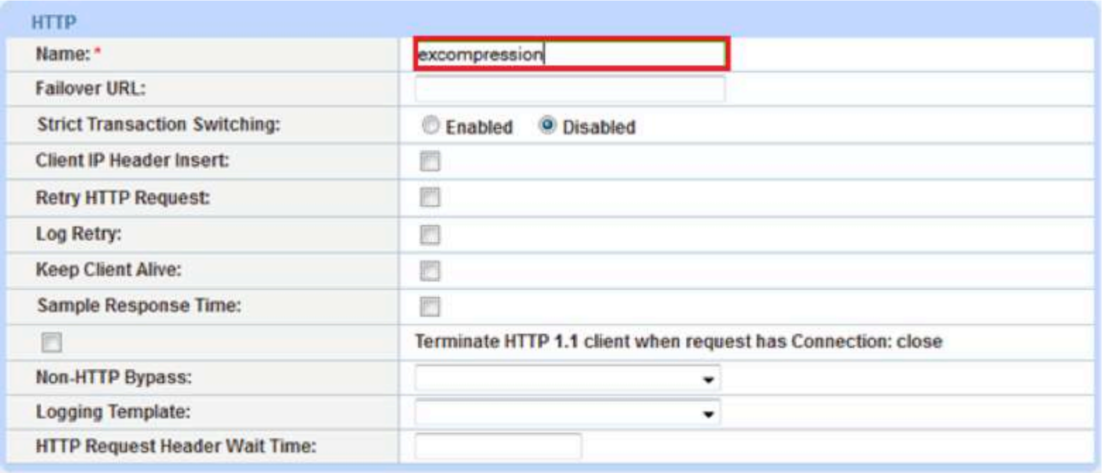
6. Click **OK** and **Save** the configuration.

Compression Template

Compression is a bandwidth optimization feature that condenses the HTTP objects that are requested from a web server. The purpose of compression is to transmit the requested data more efficiently (less data transmitted) and to provide faster response times to the client.

To create a template that can be bound to an HTTPS VIP, follow the instructions below:

1. Navigate to Config Mode > SLB > Service > Template > Application > HTTP.
2. Click Add.
3. Enter the Name: "excompression"

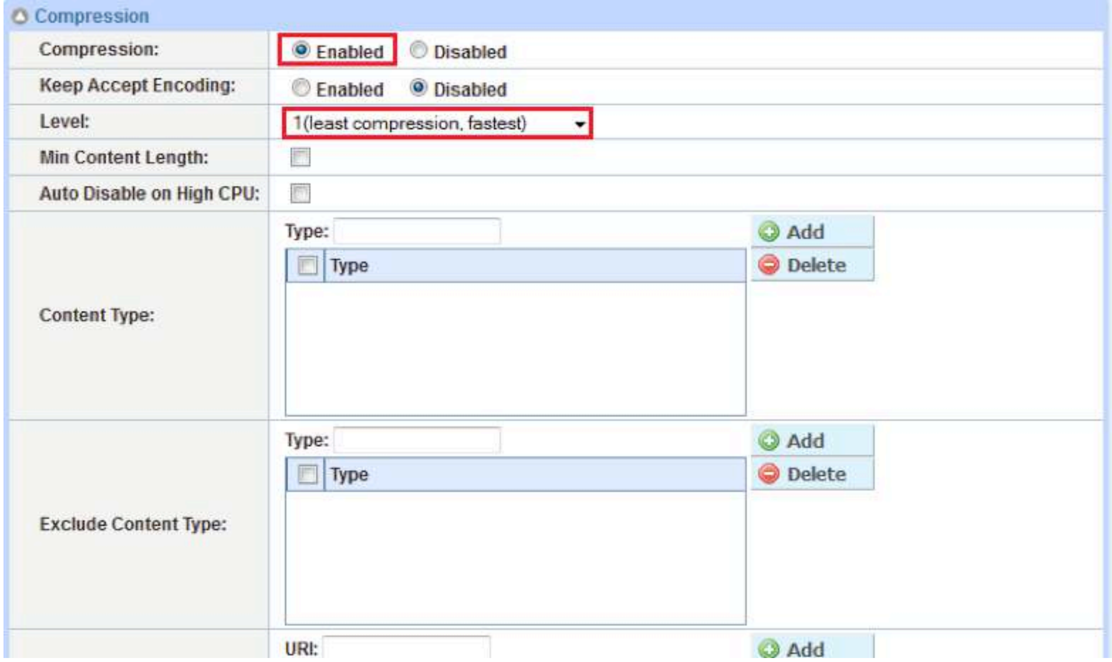


HTTP

Name: *	excompression
Failover URL:	
Strict Transaction Switching:	○ Enabled ● Disabled
Client IP Header Insert:	□
Retry HTTP Request:	□
Log Retry:	□
Keep Client Alive:	□
Sample Response Time:	□
□	Terminate HTTP 1.1 client when request has Connection: close
Non-HTTP Bypass:	
Logging Template:	
HTTP Request Header Wait Time:	

Figure 18: Compression interface

4. Expand the Compression section to display compression options.
5. Enable Compression.
6. Select the compression level (the default value is recommended).



Compression

Compression:	● Enabled ○ Disabled
Keep Accept Encoding:	○ Enabled ● Disabled
Level:	1(least compression, fastest)
Min Content Length:	□
Auto Disable on High CPU:	□
Content Type:	Type: Add □ Type Delete
Exclude Content Type:	Type: Add □ Type Delete
	URI: Add

Figure 19: A10 device Compression interface

7. Once completed, select OK and Save to save the configuration.

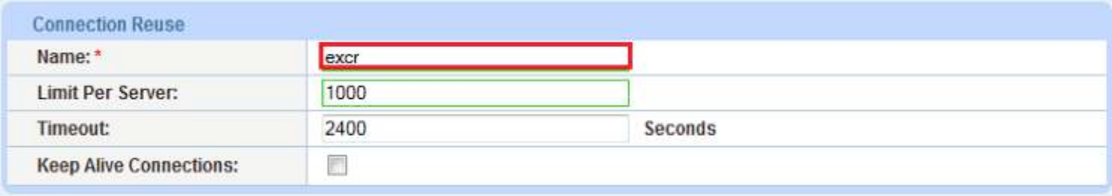
Note: Compression is disabled by default.

TCP Connection Reuse

Connection Reuse reduces the overhead associated with setting up TCP connections (3-way handshake), by establishing persistent TCP connections with Exchange CAS servers and then multiplexing client TCP requests over those connections. This feature offers a significant benefit as it eliminates the need of opening new connections for every single client connection.

Connection Reuse terminates all client connections on the Thunder ADC, maintains persistent connections to the CAS servers, and sends all client requests on the same persistent connections.

1. Navigate to **Config Mode** > **SLB** > **Service** > **Template** > **Connection Reuse**.
2. Click **Add**.
3. Enter the **Name**: "excr".



Connection Reuse

Name: *	excr	
Limit Per Server:	1000	
Timeout:	2400	Seconds
Keep Alive Connections:	□	

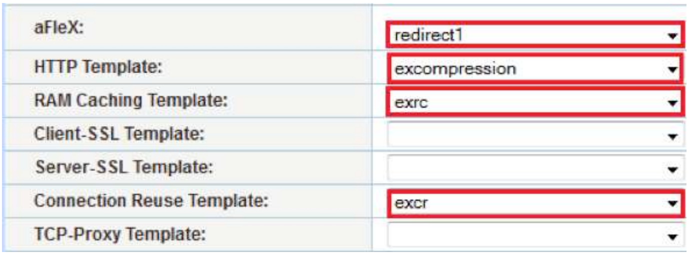
Figure 20: TCP Connection Reuse template

4. Click **OK**, then click **Save** to save the configuration.

Apply Optimization and Acceleration Feature Templates

After configuring templates for optimization and acceleration features, you must bind the templates to the virtual port on the VIP to place the features into effect.

1. Navigate to **Config Mode** > **SLB** > **Service** > **Virtual Service**.
2. Click on the virtual service name.
3. Apply the features by selecting the templates from the applicable drop-down lists.



aFleX:	redirect1
HTTP Template:	excompression
RAM Caching Template:	exrc
Client-SSL Template:	
Server-SSL Template:	
Connection Reuse Template:	excr
TCP-Proxy Template:	

Figure 21: Applying features

4. Click **OK**, then click **Save** to save the configuration.

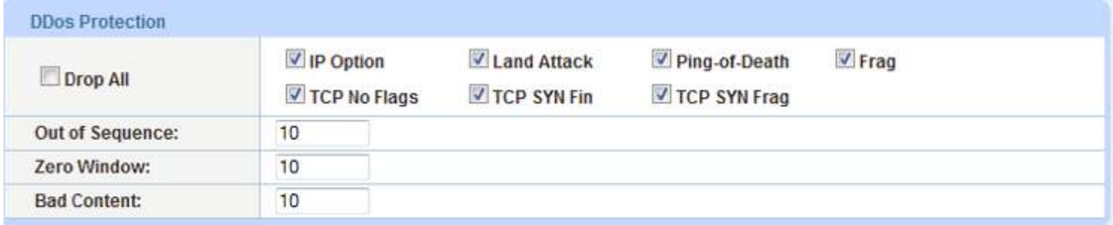
DDoS Mitigation (Optional)

ACOS provides an additional security layer for load balanced servers and applications. Adding to an in-depth defense strategy, key protections are architected into ACOS hardware and software.

ACOS provides high-performance detection and prevention against distributed denial-of-service (DDoS) and protocol attacks that can cripple servers and take down applications. Since the Thunder ADC is placed between the routers and data center resources, it is ideally positioned to detect and stop attacks directed at any data center server or application. Using specialized ASICs in select models, ACOS can continue to inspect, stop, and redirect all application traffic at network speeds.

To install a standard set of DDoS Mitigation features:

1. Navigate to Config Mode > SLB > Service > Global > DDoS Protection.
2. Select all DDoS Protection features you would like to activate.



DDos Protection

□ Drop All	☑ IP Option	☑ Land Attack	☑ Ping-of-Death	☑ Frag
	☑ TCP No Flags	☑ TCP SYN Fin	☑ TCP SYN Frag	
Out of Sequence:	10			
Zero Window:	10			
Bad Content:	10			

Figure 22: DDoS Mitigation

3. Click OK and then click Save to store your configuration changes.

Note*: Additional traffic security features are described in the Application Access Management and DDoS Mitigation Guide.*

Summary and Conclusion

With the release of Exchange 2013, Microsoft has again reached another major milestone in the unified messaging world. Installation and testing of Exchange 2013 in the A10 lab was far easier compared to the previous versions. Exchange 2013 includes major architectural changes that have made installation and setup of the Thunder ADC solution much easier.

A10 Thunder ADC, powered by ACOS, enhances Microsoft Exchange 2013 by providing the following:

- Higher Scalability – Enterprises can easily scale Exchange 2013 by load balancing traffic across multiple CAS servers.
- Higher Performance – Higher connection counts, faster end-user responsiveness and reduced IIS server CPU utilization are realized by using advanced ACOS features: HTTP Compression, RAM Caching and Connection Reuse.
- High Availability – Exchange service availability is verified through periodic health checks.
- Higher Security – ACOS protects services from DDoS attacks.

For more Information about Thunder ADC solutions, please visit the following:

https://www.a10networks.com/products/thunder-series/thunder-application_delivery_controller

https://www.a10networks.com/resources/solution-briefs

https://www.a10networks.com/resources/case-studies

Support and Configuration Updates

1. Exchange 2013 Cumulative update 5 can now support SSL Offload deployments.

http://technet.microsoft.com/en-us/library/jj907309(v=exchg.150).aspx

http://blogs.technet.com/b/exchange/archive/2014/05/27/released-exchange-server-2013-cumulative-update-5.aspx

2. For MAPI over HTTP support you must use only Source IP Persistence instead of Cookie Persistence

http://technet.microsoft.com/en-us/library/dn635177%28v=exchg.150%29.aspx

Sample Configuration

```
ip nat pool SNAT 192.0.2.157 192.0.2.157 netmask /24
health monitor HM-OWA-HTTPS
 method https
health monitor HM-OA-HTTPS
 method https
health monitor HM-OWA
 method https
health monitor HM-AS
 method https
health monitor HM-EWS
health monitor HM-OAB
health monitor HM-OA
health monitor SG-AD
health monitor EXHC
 method http
slb template server-ssl SRV-SSL
slb server SRV-Exchange1 192.0.2.160
   health-check ping
   port 443  tcp
   port 80  tcp
   port 110  tcp
   port 995  tcp
   port 25  tcp
   port 993  tcp
   port 143  tcp
slb server SRV-Exchange2 192.0.2.161
   health-check ping
   port 443  tcp
   port 80  tcp
   port 110  tcp
   port 995  tcp
   port 25  tcp
   port 993  tcp
   port 143  tcp
slb service-group SG-OWA tcp
    method least-connection
    health-check HM-OWA
    member SRV-Exchange1:443
    member SRV-Exchange2:443
slb service-group SG-AS tcp
    method least-connection
    health-check HM-AS
    member SRV-Exchange1:443
    member SRV-Exchange2:443
slb service-group SG-EWS tcp
```

```
    method least-connection
    health-check HM-EWS
    member SRV-Exchange1:443
    member SRV-Exchange2:443
slb service-group SG-OAB tcp
    method least-connection
    health-check HM-OAB
    member SRV-Exchange1:443
    member SRV-Exchange2:443
slb service-group SG-OA tcp
    method least-connection
    health-check HM-OA
    member SRV-Exchange1:443
    member SRV-Exchange2:443
slb service-group SG-AD tcp
    method least-connection
    health-check SG-AD
    member SRV-Exchange1:443
    member SRV-Exchange2:443

slb template connection-reuse External-OWA
slb template connection-reuse excr
slb template cache exrc
slb template http excompression
   compression enable
slb template client-ssl Test-SSL
   cert ms-cert
   key ms-cert
slb virtual-server VIP-Exchange-OWA 203.0.113.200
   port 443  https
      name _203.0.113.200_HTTPS_443
      source-nat pool SNAT
      service-group SG-OWA
      template cache exrc
      template client-ssl Test-SSL
      template server-ssl SRV-SSL
      template persist cookie Persist-OWA
slb virtual-server VIP-Exchange-AS 203.0.113.201
   port 443  https
      service-group SG-AS
      template client-ssl Test-SSL
   port 80  http
      service-group SG-AS
      aflex redirect1

slb virtual-server VIP-Exchange-POP3 203.0.113.202
```

```
   port 995  tcp
      service-group SG-AS
   port 110  tcp
      service-group SG-AS
slb virtual-server VIP-Exchange-IMAP4 203.0.113.203
   port 993  tcp
      service-group SG-AS
   port 143  tcp
      service-group SG-AS
slb virtual-server VIP-Exchange-AOB 203.0.113.205
   port 80  http
      service-group SG-OAB
      aflex redirect1
slb virtual-server VIP-Exchange-AW 203.0.113.206
   port 80  tcp
      service-group SG-OAB
   port 443  https
      service-group SG-OA
end
```

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Part Number: A10-DG-16103-EN-02
Dec 2015

Worldwide Offices

North America
sales@a10networks.com

Europe
emea_sales@a10networks.com

South America
brazil@a10networks.com

Japan
jinfo@a10networks.com

China
china_sales@a10networks.com

Taiwan
taiwan@a10networks.com

Korea
korea@a10networks.com

Hong Kong
HongKong@a10networks.com

South Asia
SouthAsia@a10networks.com

Australia/New Zealand
anz_sales@a10networks.com

To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at: **www.a10networks.com/contact** or call to talk to an A10 sales representative.