A10 Thunder ADC with Oracle E-Business Suite 12.2

Table of Contents

Disclaimer

1 Introduction

This deployment guide describes an optimized architecture for deploying Oracle E-business Suite 12 using A10 Networks® Thunder® ADC line of Application Delivery Controllers . The tested, high-performance architecture offers significant advantages when deploying the Oracle E-Business Suite, as the Thunder ADC offers application performance acceleration, optimization, security, scalability and improved application uptime.

2 Deployment Prerequisites

This guide provides detailed instructions on how the Thunder ADC is configured through the Graphical User Interface (GUI); a complete list of Command Line Interface (CLI) entries is located in Appendix A.

Deployment Prerequisites

Tested environment:

- A10 Networks Advanced Core Operating System (ACOS®) 4.0.1 build 214 or higher (supported with virtual or hardware-based Thunder ADC appliances) Thunder Series hardware or virtual ADC appliance support
- Oracle Application Server E-Business Suite 12.2 or higher
- Oracle 11g Release 2
- Linux Operating System (OS)
- Client browser (tested)
  - Web-based (HTML)
  - Forms-based (Java-based)

***Note**: Generally, if the Virtual IP (VIP) is accessed from an external client, the Thunder ADC device would be deployed in a routed mode. If the Oracle Application Servers (OASs) are accessed internally, the Thunder ADC device would be deployed in one-armed mode. If the OASs are accessed from both internal and external clients, the Thunder ADC device would be deployed in one-arm mode.*

***Note**: For additional supported deployment modes of the Thunder ADC, please visit the following URL:*

https://www.a10networks.com/products/load-balancing

3 Oracle E-Business Topology

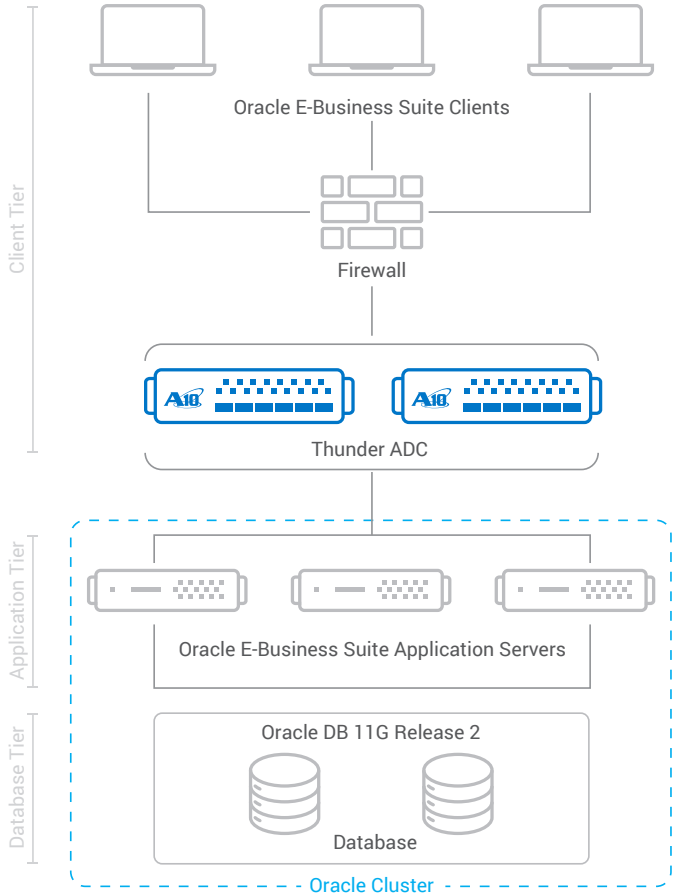

Figure 1: Configuration overview

4 Accessing the Thunder ADC Application Delivery Controller

This section describes how to access the Thunder ADC device. The device can be accessed either from a Command Line Interface (CLI) or Graphical User Interface (GUI):

- CLI – Text-based interface in which you type commands on a command line. The CLI is accessible 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 – Web-based interface in which you click to access configuration or management pages and type or select values to configure or manage the device. The GUI is accessible 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 device.*

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 device, refer to the *Thunder ADC System Configuration and Administration Guide*.)

5 Basic Configuration

This section explains how the Thunder ADC device is configured to load balance Oracle Application Servers. This section contains detailed instructions for installing the real servers, service group, and virtual services in a basic OAS configuration. Before the basic configuration is created, health monitors and source NAT must be configured.

5.1 Health Monitor Configuration

The Thunder ADC can automatically initiate health status checks for real servers and service ports. Health checks assure that all requests go to functional and available servers. If a server or a port does not respond to a health check appropriately, the server is temporarily removed from the list of available servers. Once the server is restored and starts responding appropriately to the health checks, the server is automatically added back to the list of available servers.

1. Navigate to **ADC > Health Monitor.**
2. Click **Create.**
3. Enter the following:
   a. **Name**: "OASHC"
   b. **Method**: "HTTP"
4. Click **Create Monitor.**

See the next section to continue with the service group configuration.

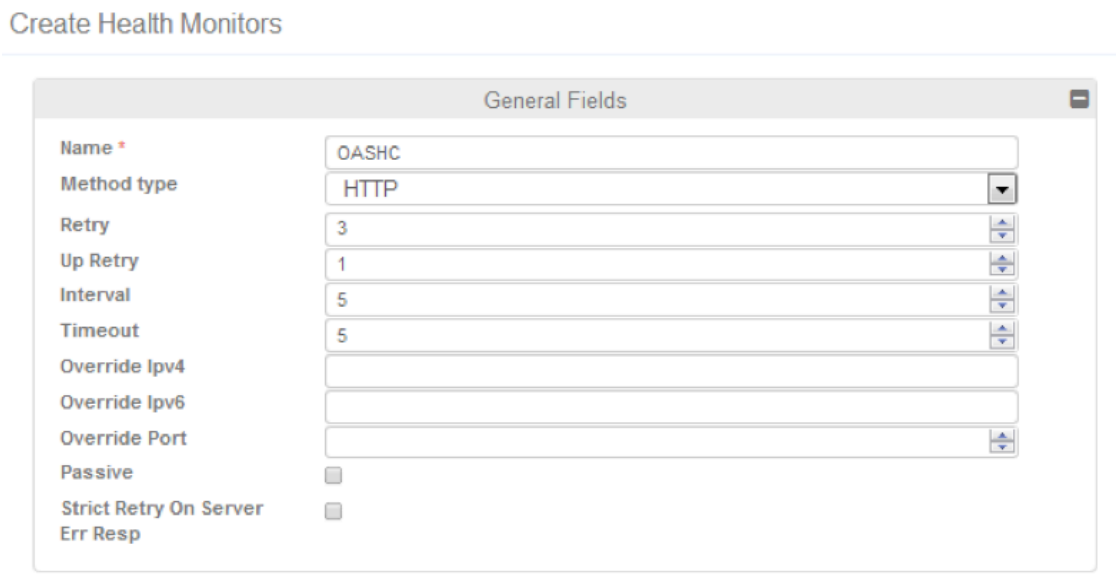

Figure 2: Health monitor configuration

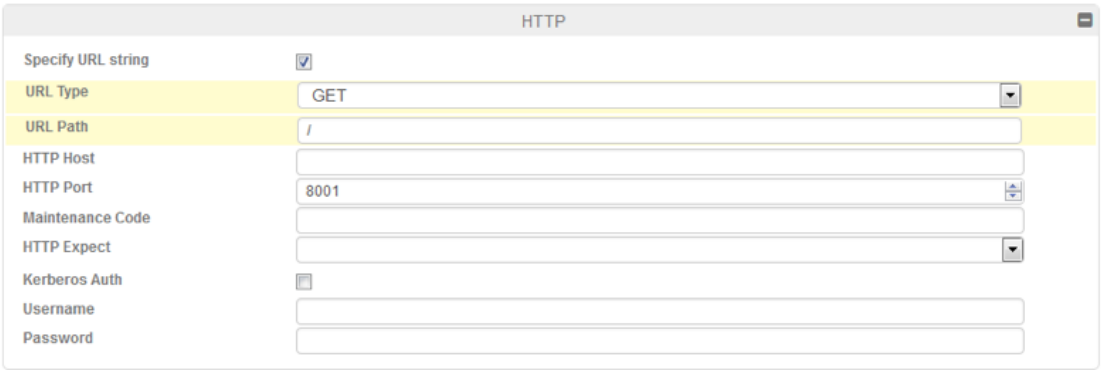

Figure 3: Health monitor HTTP configuration

5.2 IP Source NAT Configuration

This section configures the IP address pool to be used for IP Source Network Address Translation (SNAT). When incoming traffic from a client accesses the VIP address (for example: 192.0.2.200), the client requests are "source NATed", which means that the Thunder ADC device replaces the client's source IP address based on the configured address pool of the source NAT. SNAT is required when your network topology is based on "one-arm" deployment and if you have internal clients that reside on the same subnet as the VIP. The Source NAT template must be applied to the virtual server port for the NAT to take effect.

1. Navigate to **ADC > IP Source NAT > IPv4 Pools.**
2. Click **Create**.
3. Enter the following:
   a. **NAT**: "SNAT"
   b. **Start IP Address**: "192.0.2.250"
   c. **End IP Address**: "192.0.2.250"
   d. **Netmask**: "255.255.255.0"

Figure 4: IP Source NAT pool configuration

4. Click **Create**, then click the Save icon at the top of the GUI window to save the configuration.

***Note**: When you are in the virtual service configuration section, you can apply the "Source NAT" template that was created under the source NAT pool section.*

Note: *When using the Thunder ADC device in a High Availability (HA) configuration, an HA group must be selected. This will prevent duplicate IP addresses from occurring in the source NAT pool.*

5.3 Server Configuration

This section demonstrates how to configure the OASs on the Thunder ADC.

1. Navigate to **ADC > SLB > Server.**
2. Click **Add** to add a new server.
3. Within the Server section, enter the following required information:
   a. **Name**: "OAS1"
   b. **IP address /Host**: 192.0.2.5

***Note**: Enter additional servers if necessary.*

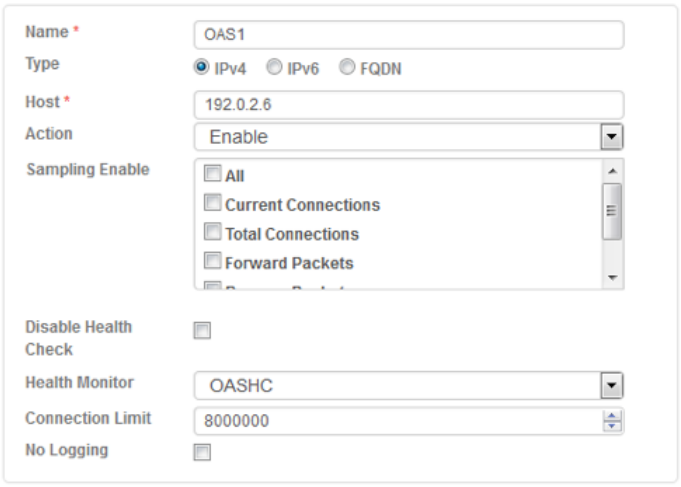

Figure 5: Server configuration

4. Add a port to the server configuration:
   a. Enter the "8001" in the **Port** field.
   b. Select the "TCP" for the **Protocol**.
   c. Click **Create**.

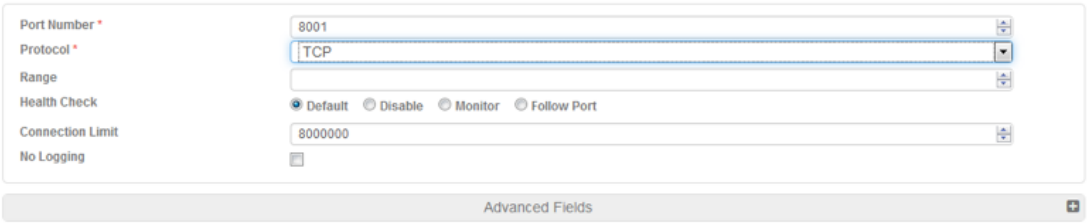

Figure 6: Server port configuration

5. Click **Create**, then click the Save icon at the top of the GUI window to save the configuration.

***Note**: Enter additional Oracle Application Servers by repeating the same procedure above*

5.4 Service Group Configuration

This section describes how to configure a service group.

1. Navigate to **ADC > SLB > Service Group**.
2. Click **Create**.
3. Enter or select the following values:
   a. **Name**: "SG8001"
   b. **Type**: "TCP"
   c. **Algorithm**: "Least Connection"
   d. **Health Monitor**: "OASHC"
4. In the Server section, select a server from the **Server** drop-down list and enter "8001" in the **Port** field.
5. Click **Create**. Repeat for each server.

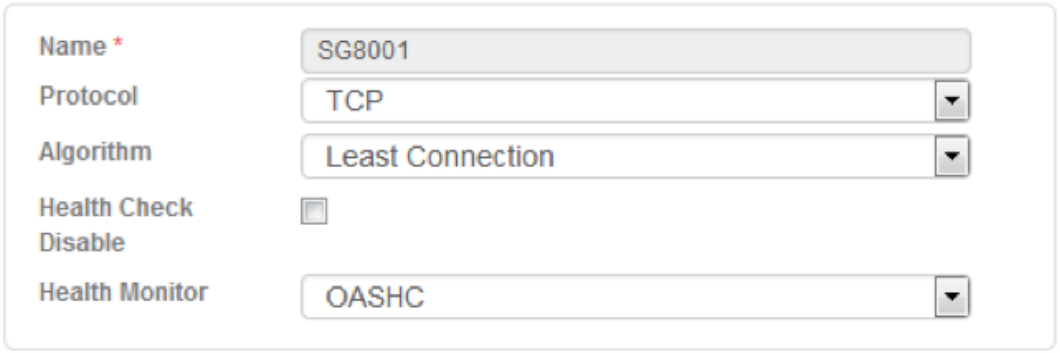

Figure 7: Service group configuration

6. Add the Servers to the Service Group called "SG8001".

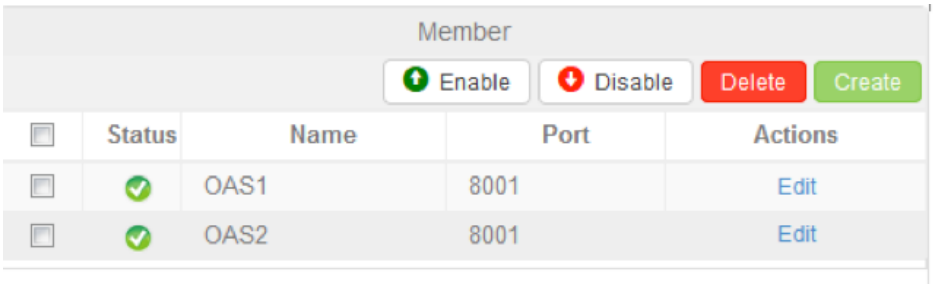

Figure 8: Server configuration

7. Click **Create**, then click the Save icon at the top of the GUI window to save the configuration.

5.5 Virtual Server Configuration

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

1. Navigate to **ADC > SLB > Virtual Service > Create.**
2. In the General section, enter the name of the VIP and its IP address:
   a. **Name**: "OASVIP"
   b. **IP Address**: 192.0.2.200

Figure 9: Virtual server configuration

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

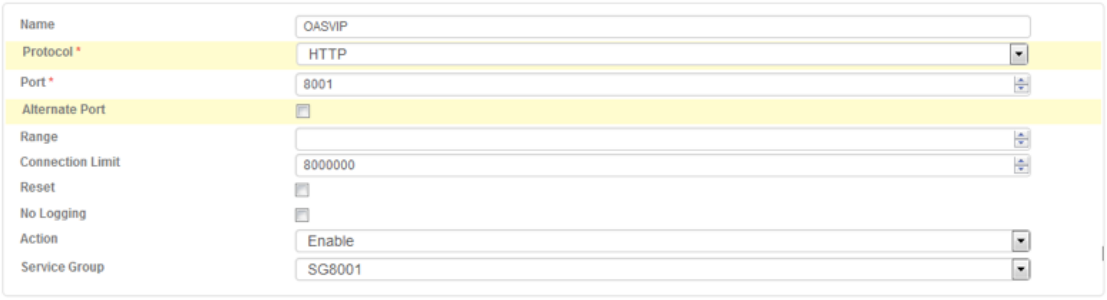

Figure 10: Virtual-server port configuration

4. Select the following values:
   a. **Virtual Server**: "HTTP"
   b. **Service Group**: "SG8001"

***Note**: The port number automatically will be selected after you select the protocol type*

5. Click **Create**, then click the Save icon at the top of the GUI window to save the configuration.

6 Advanced Configuration

This section presents the advanced configuration options of the Thunder ADC device with Oracle Application Servers. The advanced configuration increases server performance with features such as SSL Offload, HTTP Compression, HTTP Connection Reuse, Cookie Persistence, and RAM Caching.

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, the features are linked to the VIP.

***Note**: This advanced section moves directly to advanced configuration with minimal changes from the basic configuration.*

6.1 SSL Offload

SSL Offload relieves a webserver farm from the burden of encrypting and decrypting SSL traffic, which is a very CPU-intensive task. SSL Offload is a performance optimization that enables a server to offload the SSL traffic to the Thunder ADC.

To configure SSL Offload with Oracle Application Servers, navigate to the OAS application virtual service on the Thunder ADC device, and change the virtual service port and type from 8001 (HTTP) to 8443 (HTTPS).

1. Navigate to Config **ADC > SLB > Virtual Services**.
2. Click on the service name.
3. Select "HTTPS" from the **Port** drop-down list.

***Note**: It is good practice to correlate the server name with the virtual port. As an example, the "_192.0.2.200_HTTP_8001" service should be renamed "_192.0.2.200_HTTPS_8443" if the virtual port is updated to use the HTTPS service type.*

***Note**: Leave the port 8001 configuration in the service group and on the server(s). SSL Offload is configured as HTTPS (8443) from the front end but is HTTP (8001) to the backend servers/server pool.*

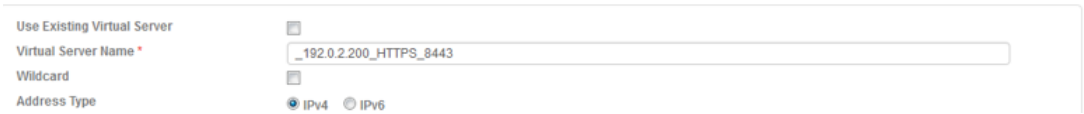

Figure 11: Virtual service configuration

6.2 Server Certificate

Since the Thunder ADC device acts as an HTTPS proxy for the Oracle Application Web servers, the server certificate for each server must be imported onto, or generated on the Thunder ADC device.

There are two options when installing an SSL template on the Thunder ADC:

- **Option 1**: Generate a self-signed certificate.
- **Option 2**: Import an SSL certificate and key signed by a Certificate Authority (CA).

6.2.1 Generate a Self-Signed Certificate

1. Navigate to **ADC > SSL Management > SSL Certificates.**
2. Click **Create**.
3. Enter the **File Name** of the certificate, "OASWS".
4. Enter the following values:
   a. **Common Name**: "OASWS"
   b. **Division**: "A10"
   c. **Organization**: "A10"
   d. **Locality**: San Jose
   e. **State or Province**: "CA"
   f. **Country**: "United States"
   g. **Email Address**: "admin@example.com"
   h. **Valid Days:** "730" (Default)
   i. **Key Size (Bits)**: "2048"

***Note**: The Thunder ADC supports 512-, 1024-, 2048-, and 4096-bit keys. The required CPU processing power increases exponentially, with the increase of key size.*

Figure 12: Self-signed certificate configuration

5. Click **Create**, then click the Save icon at the top of the GUI window to save the configuration.

6.2.2 Import the Certificate and Key

1. Navigate to **Config Mode > Service > SSL Management > Certificate**.
2. Click **Import**.
3. Enter the **Name**, "OASCert".
4. Select "**Certificate**".
5. Select "**Local**" or "Remote", depending on the file location.
6. 6. SSL or CA Certificate: Select "**SSL Certificate".**
7. Enter the certificate **Password** (if desired).

8. Certificate Format: Select "**PEM**".
9. Enter or select certificate source:
10. Click **Import**.

***Note**: When importing a CA-signed certificate for which the Thunder ADC device generated the CSR, there is no need to import the key. The key is automatically generated on the Thunder ADC device together with the CSR.*

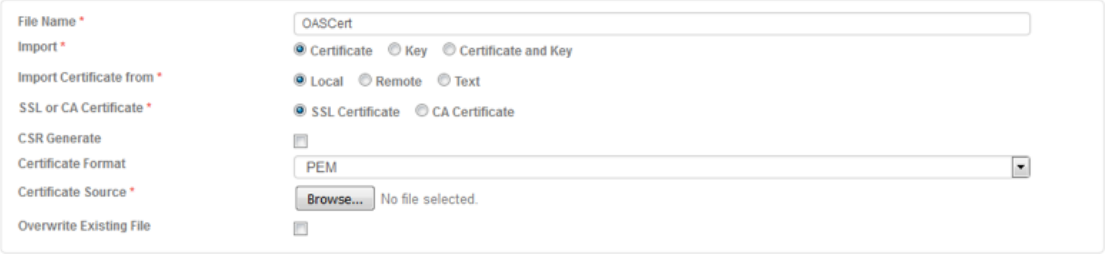

Figure 13: SSL certificate import

11. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

6.2.3 Configure and Apply Client-SSL Template

This section describes how to configure a client-SSL template and apply it to the VIP.

1. Navigate to **ADC > Templates > SSL**
2. Click **Create SSL** template.
3. Enter or select the following values:
   a. **Name**: "ClientOAS"
   b. **Certificate Name**: "OASWS"
   c. **Key Name**: "OASWS"
   d. **Pass Phrase**: "example"
   e. **Confirm Pass Phrase:** "example"

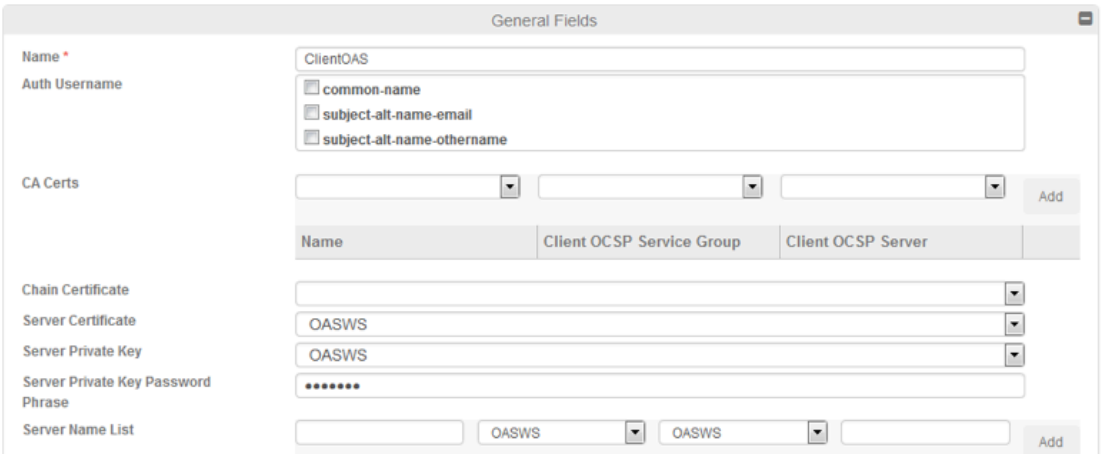

Figure 14: Client SSL template

4. Click **OK.**
5. After the client-SSL template is completed, link the template to the HTTPS VIP (port 8443):
   a. Navigate to **ADC > SLB > Virtual Server**.
   b. Click on the virtual server name.

c. Select "8443" and click **Edit**.

d. Apply the client-SSL template created by selecting it from the **Client-SSL Template** drop-down list.

Figure 15: Client SSL template selection

6. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

6.3 HTTP Compression

HTTP Compression is a bandwidth optimization feature that compresses the requested HTTP objects from a webserver. If a web site uses lots of bandwidth, enabling HTTP Compression provides faster transmission between the browser and the webserver. The purpose of compression is to transmit the requested data more efficiently and with faster transport times to the client. HTTP Compression makes HTTP transactions much faster by transmitting less data.

6.3.1 Create HTTP Compression Template

1. Navigate to **ADC > Templates > Layer 7.**
2. Click **Create**.
3. Enter a **Name**, "HTTP Compression".
4. Click **Compression** to display the compression configuration options.

***Note**: Compression is disabled by default. When compression is enabled, the compression options will have the default values shown in following example:*

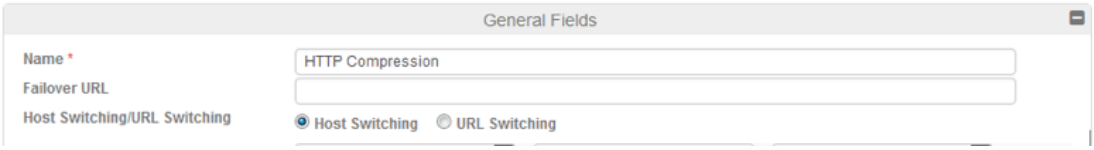

Figure 16: HTTP compression template

5. Select "Enabled" next to **Compression**.

***Note**: The Thunder ADC offers various compression levels, ranging from level 1 (least compression) through level 9 (maximum compression). Level 1 is the recommended compression setting.*

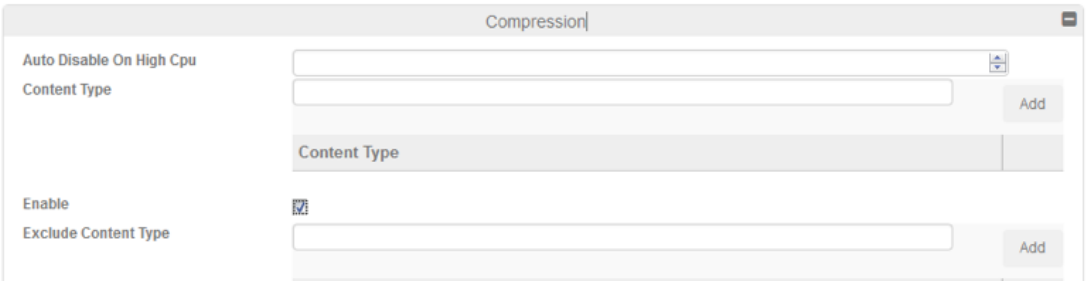

Figure 17: Compression configuration column

6. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

6.4 Cookie Persistence

Cookie Persistence enables the Thunder ADC to persist sessions with a particular server, by sending a cookie response to the client. To configure Cookie Persistence, create a template first:

1. Navigate to **ADC > Service > Persistence > Persist Cookie.**
2. Click **Create** to add a new cookie persistence template.
3. Enter the following values:
   a. **Name**: "OASPersistence"
   b. **Expiration**: 86400 seconds
   c. **Cookie Name:** "OASPersistence"
   d. **Insert Always**: Selected

Figure 18: Cookie persistence template

4. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

6.5 TCP Connection Reuse

1. Navigate to **ADC > Application > Connection Reuse.**
2. Click **Create**.
3. Enter a **Name** (for example, "OASCR").

Figure 19: TCP connection reuse template

4. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

6.6 RAM Caching

RAM Caching reduces the number of connections and server requests that need to be processed by the real servers. Cacheable data is cached within the Thunder ADC device, thus reducing overhead on the Oracle Application Servers transactions. To configure RAM Caching:

1. Navigate to **ADC > Templates > Applications > RAM Caching.**
2. Click **Create**.
3. Enter or select the following values:
   a. **Name**: "OASRC"
   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

***Note**: The RAM Caching policy option is not required, unless there is specific data that requires caching, no-cache, or invalidation. These policy options can be configured in the policy section of the RAM Caching template. For additional information on RAM Caching policies, please refer to the Thunder ADC Application Delivery and Server Load Balancing Guide.*

Figure 20: RAM caching template

6.6.1 Custom RAM Caching Policy

Under the RAM Cache policy, this section explains how to configure dynamic RAM caching, which overrides and augments standard HTTP behavior.

To configure a RAM Caching policy:

1. In the **URI** field, enter the portion of the URI string to match on.
2. Select Cache from the **Action** drop-down list. The **Duration** field appears.
3. By default, the content is cached for the number of seconds specified in the **Age** field of the RAM Caching section. To override the aging period, specify the number of seconds in the **Duration** field

***Note**: The policy allows the choice to "no-cache" or "invalidate". To use either of these options, go to the **Action** menu and select the option from the drop-down list.*

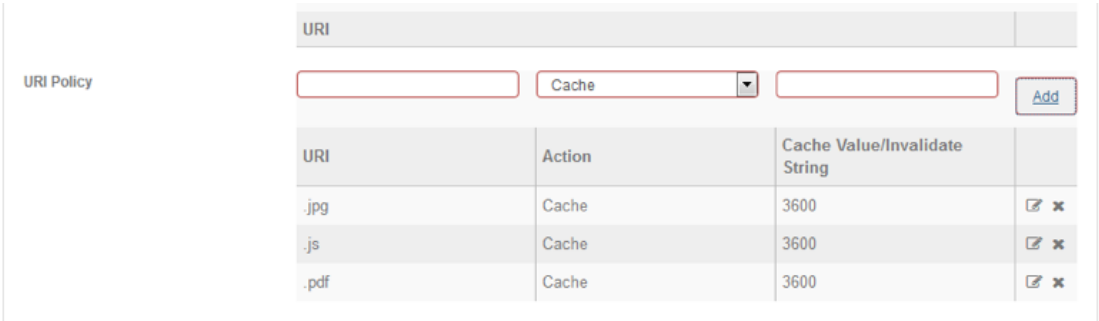

Figure 21: RAM caching policy

4. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

6.7 HTTP-TO-HTTPS Redirect

This section explains how to redirect OAS traffic that originates from HTTP to HTTPS using the Thunder ADC devices' aFleX® scripts. A10 Networks aFleX Deep Packet Inspection (DPI) Scripting Technology is based on standard TCL scripting language, and enables the Thunder ADC device to perform Layer 7 deep-packet inspection (DPI). For samples of aFleX scripts, please refer to the following URL:

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

As an example, one of the most commonly used aFleX scripts is the "HTTP redirect to HTTPS traffic" script:

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

Additional aFleX script examples can be downloaded from the URL listed above.

To configure a transparent HTTPS redirect using aFleX:

1. Navigate to **ADC > SLB > Virtual Services > Templates.**
2. Select the Virtual Service.
3. Click on the virtual service name and navigate to the General Fields.
4. Navigate to the aFleX Scripts selection and select "redirect1" from the drop down menu.

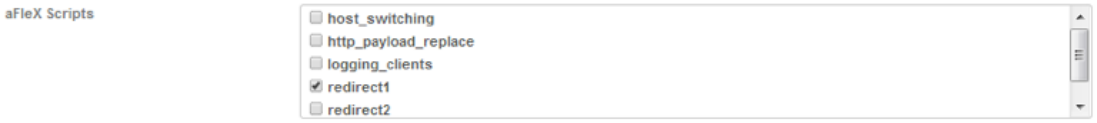

Figure 22: aFleX options

5. Click **Update**.

***Note**: The aFleX script must be bound to virtual-server port 8001.*

6.8 Optimization and Acceleration Templates

When the optimization and acceleration features are configured, they must be bound to the port on the VIP to make them into operational.

6. Navigate to **Config Mode > SLB > Virtual Service.**
7. Click on the virtual service name.

Apply the features by selecting the templates from the applicable drop-down lists.

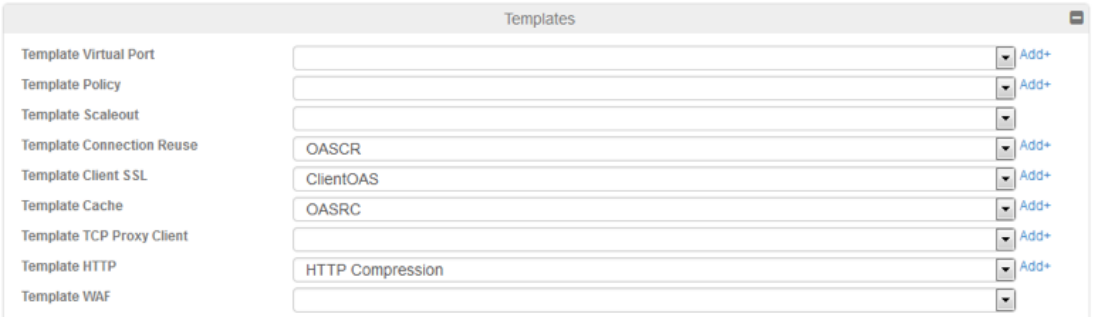

Figure 23: Applying features

8. Click **OK**, then click the Save icon at the top of the GUI window to save the configuration.

7 Summary and Conclusion

The sections above show how to deploy the Thunder ADC device for optimization of Oracle Application Servers (OAS). By using the Thunder ADC device to load balance a pool of OAS web servers, the following key advantages are achieved:

- High availability for Oracle Application Servers to prevent application failure
- Seamless distribution of client traffic across multiple Oracle Application Servers to provide seamless scalability
- Higher connection counts, faster application responsiveness, and reduced Oracle Application Server CPU utilization by initiating SSL Offload, HTTP Compression, RAM Caching and Connection Reuse
- Improved application performance and reliability for end-users

For more information about Thunder ADC products, please refer to the following URLs:

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

Appendix A. CLI Commands for Basic Configuration

This section shows the CLI commands for implementing the basic configuration described above.

```
ip nat pool SNAT 192.0.2.250 192.0.2.250 netmask /24
health monitor OASHC
 method http port 8001
slb server OAS1 192.0.2.5
   port 8001  tcp
slb server OAS2 192.0.2.6
   port 8001  tcp
slb server OAS3 192.0.2.7
   port 8001  tcp
slb service-group SG8001 tcp
    method least-connection
    health-check OASHC
    member OAS1:8001
    member OAS2:8001
    member OAS3:8001

slb template client-ssl SWSE
   cert SWSE
   key SWSE
slb virtual-server OASVIP 192.0.2.200
   port 8001  http
      name _192.0.2.200_HTTP_8001
      source-nat pool SNAT
      service-group SG8001
end
```

Appendix B. CLI Commands for Advanced Configuration

This section shows the CLI commands for implementing the advanced configuration described above.

```
ip nat pool SNAT 192.0.2.250 192.0.2.250 netmask /24
health monitor OASHC
 method http port 8001
slb server OAS1 192.0.2.5
   port 8001  tcp
slb server OAS2 192.0.2.6
   port 8001  tcp
slb server OAS3 192.0.2.7
   port 8001  tcp
slb service-group SG8001 tcp
    method least-connection
    health-check OASHC
    member OAS1:8001
    member OAS2:8001
    member OAS3:8001
slb template connection-reuse OASCR
slb template cache OASRC
   policy uri .jpg cache
   policy uri .js cache
   policy uri .png cache
   policy uri .pdf cache
slb template http "HTTP Compression"
   compression enable
slb template client-ssl ClientOAS
   cert OASWS
   key OASWS pass-phrase encrypted
04nAX4xU1tgIH3fBJznxEjwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn
slb template persist cookie OASPersistence
   expire 86400
   insert-always
slb template persist source-ip OASPersistence
slb virtual-server OASVIP 192.0.2.200
   port 8001  http
      name _192.0.2.200_HTTP_8001
      source-nat pool SNAT
service-group SG8001
      aflex redirect1
   port 8443  https
      name _192.0.2.200_HTTPS_8443
      source-nat pool SNAT
      service-group SG8001
      template http "HTTP Compression"
      template cache OASRC
      template client-ssl ClientOAS
      template connection-reuse OASCR
      template persist cookie OASPersistence
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-16113-EN-01
Feb 2016

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam_sales@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com
Hong Kong
HongKong@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@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.