DEPLOYMENT GUIDE

VMware View 5.0 and Horizon View 6.0

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.

1 Introduction

This deployment guide contains configuration procedures for A10 Networks® Thunder™ ADC and AX™ Series line of high-performance Application Delivery Controllers (ADCs) to support VMware View 5.0 (also known as VMware Horizon View 6.0).

VMware View is a desktop virtualization solution that simplifies IT manageability and control while delivering the highest fidelity end-user experience across devices and networks.

For more information on VMware View 5.0 and Horizon View 6.0, visit: http://www.vmware.com/products/view/overview.html

The A10 Thunder ADC and AX Series ADCs is built upon A10 Networks Advanced Core Operating System (ACOS®) platform, and is designed specifically for applications such as VMware View, providing more robust response in failover situations, offloading security processing, and performing intelligent load sharing for VMware View servers.

1.1 ACOS Prerequisites and Assumptions

The following are prerequisites for this solution:

- It is assumed that users have some basic configuration familiarity with both the A10 ADC and VMware View.
- The various VMware View servers are already installed and in good working order.
- The A10 ADC is running ACOS Release 2.4.3 or higher (Tested with AX Series).

Note: While the AX Series ADC is referenced throughout this guide, the A10 Thunder ADC appliance can be used as well.

Products and versions tested:

- AX Series: version 2.6.1-P1
- VMware View: version 5.0 and Horizon View 6.0

2 ACOS Deployment for VMware View

The AX Series fully supports VMware View and provides the following benefits:

- Load Balancing and High Availability of VMware Connection Servers
- Usage of VMware Connection Servers in private networks (not directly reachable from outside)

The AX Series also can provide the following optional benefit: SSL offload on VMware Connection Servers

3 Lab Presentation

The following lab was used to build the AX VMware View 5.0 configuration:

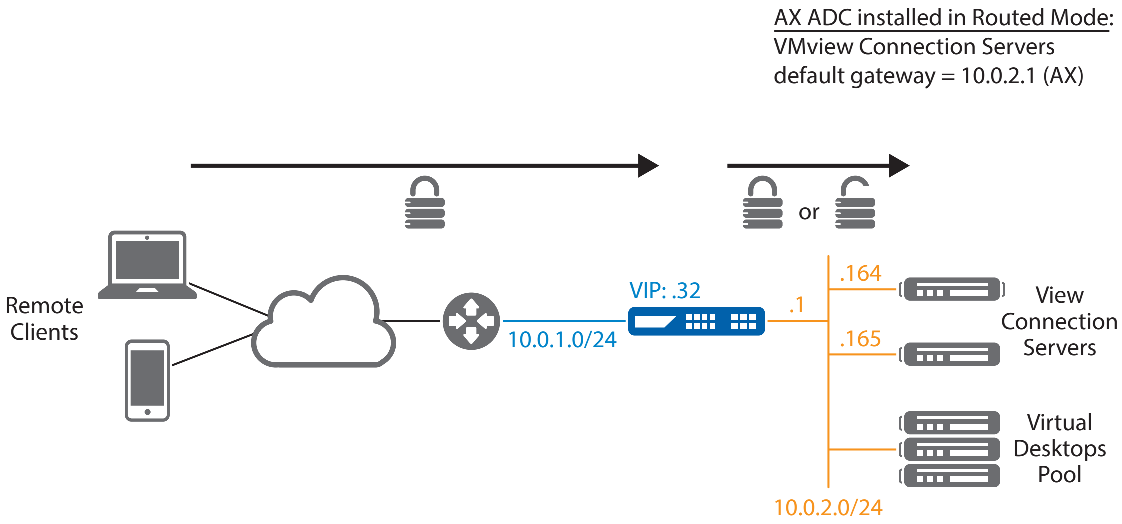


Figure 1: VMware View 5.0 deployment lab

4 Configuration

This section describes how to configure the VMware View / AX Series deployment shown in Figure 1.

4.1 VMware View Administration Configuration

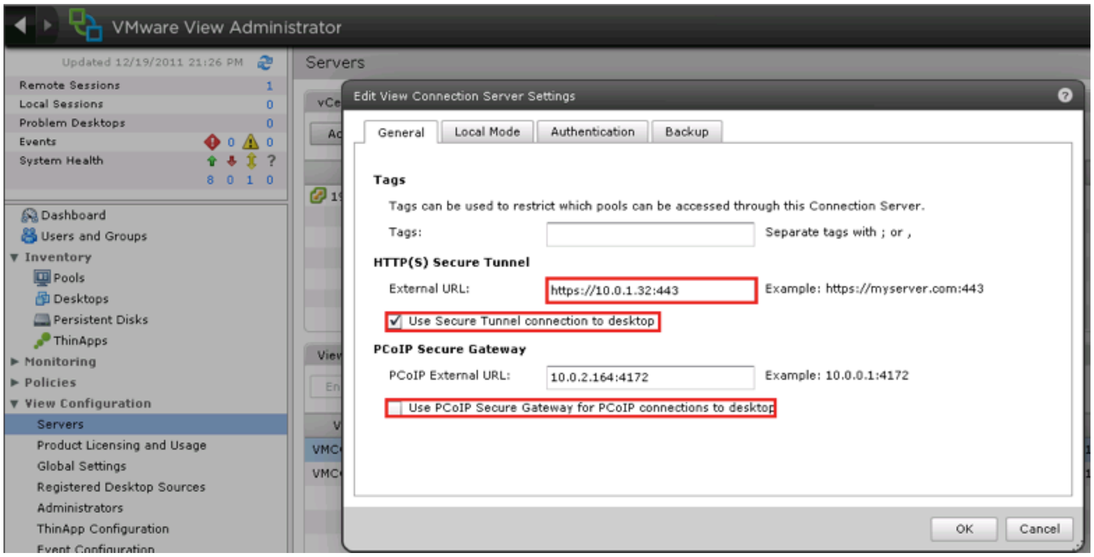
VMware View Clients access their desktops over PC-over-IP (PCoIP), which uses an encrypted UDP protocol, or Remote Desktop Protocol (RDP), which is encrypted using SSL.

- For RDP access, the AX Series can offload servers from doing the SSL encryption.
- For PCoIP access, the AX Series cannot offload servers from doing the UDP encryption. If you decide to use PCoIP for end users' desktop access, A10 recommends that you bypass the AX Series device, to enable direct connections to the desktops for PCoIP.

4.1.1 Update the VMware View Administrator

- To direct View Clients through AX Series VIP for RDP access (required to provide the SSL off load)
- To direct View Clients directly to the desktop servers for PCoIP access

1. Log on to VMware View Administrator.
2. Navigate to View Configuration > Servers > View Connection Servers.
3. Change the **External URL** to the AX Series VIP IP address or FQDN DNS name.
4. Deselect "**Use PCoIP Secure Gateway for PCoIP connections to desktop**."



Edit View Connection Server Settings

Tags

Tags can be used to restrict which pools can be accessed through this Connection Server.

Tags: Separate tags with ; or ,

HTTP(S) Secure Tunnel

External URL: https://10.0.1.32:443 Example: https://myserver.com:443

☑ Use Secure Tunnel connection to desktop

PCoIP Secure Gateway

PCoIP External URL: 10.0.2.164:4172 Example: 10.0.0.1:4172

☐ Use PCoIP Secure Gateway for PCoIP connections to desktop

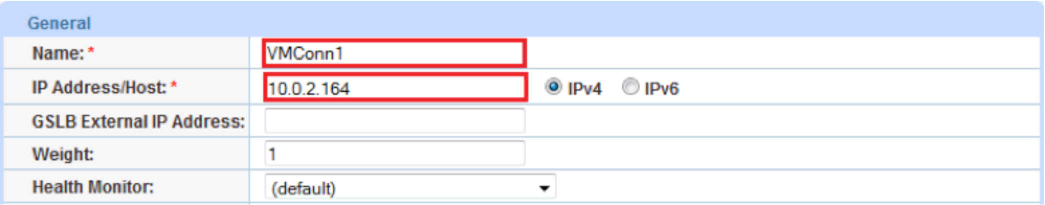
Note: Repeat for each View Connection Server.

4.2 AX Basic Configuration

4.2.1 Create View Connection Servers

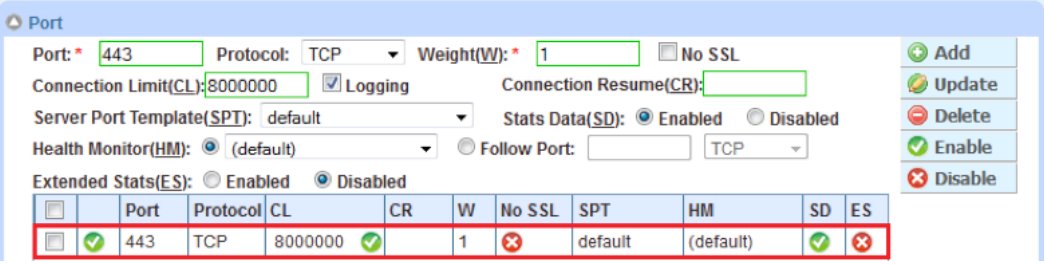
Create a real server for each View Connection Server. Enter its **Name, IP address**, and add **Protocol TCP port 443**.

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



General

Name: *	VMConn1
IP Address/Host: *	10.0.2.164 ● IPv4 ○ IPv6
GSLB External IP Address:	
Weight:	1
Health Monitor:	(default)



Port

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

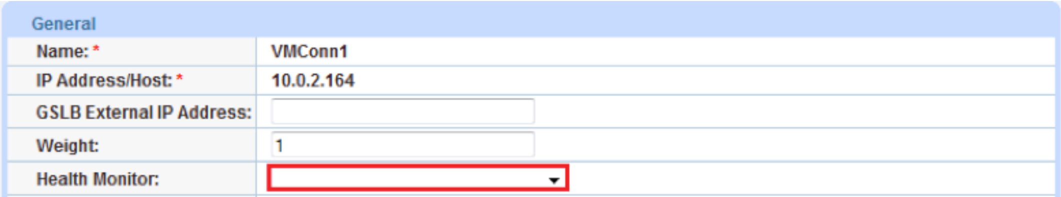
□		Port	Protocol	CL		CR	W	No SSL	SPT	HM	SD	ES
□	✓	443	TCP	8000000	✓		1	✗	default	(default)	✓	✗

- Via CLI:

```
AX(config)#slb server VMConn1 10.0.2.164
AX(config-real server)#port 443 tcp
```

Note: AX Series by default tests the server using ping and TCP handshakes. Make sure the View Connection Server Windows Firewall authorizes pings from the AX device. If not, disable the default server ping health check, as shown below.

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



General

Name: *	VMConn1
IP Address/Host: *	10.0.2.164
GSLB External IP Address:	
Weight:	1
Health Monitor:	

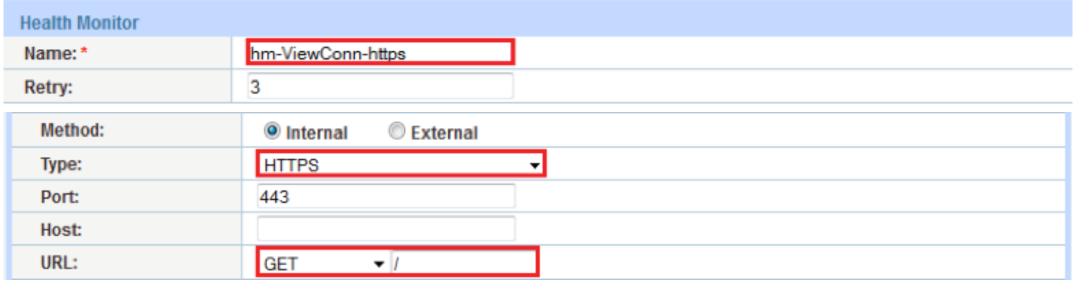
- Via CLI:= =

```
=	AX(config)#slb server VMConn1 10.0.2.164=
=	AX(config-real server)#no health-check
```

4.2.2 Create View Connection Server Health Check

Create a health monitor template to test the availability of the View Connection 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-ViewConn-https
Retry:	3
Method:	● Internal ○ External
Type:	HTTPS
Port:	443
Host:	
URL:	GET /

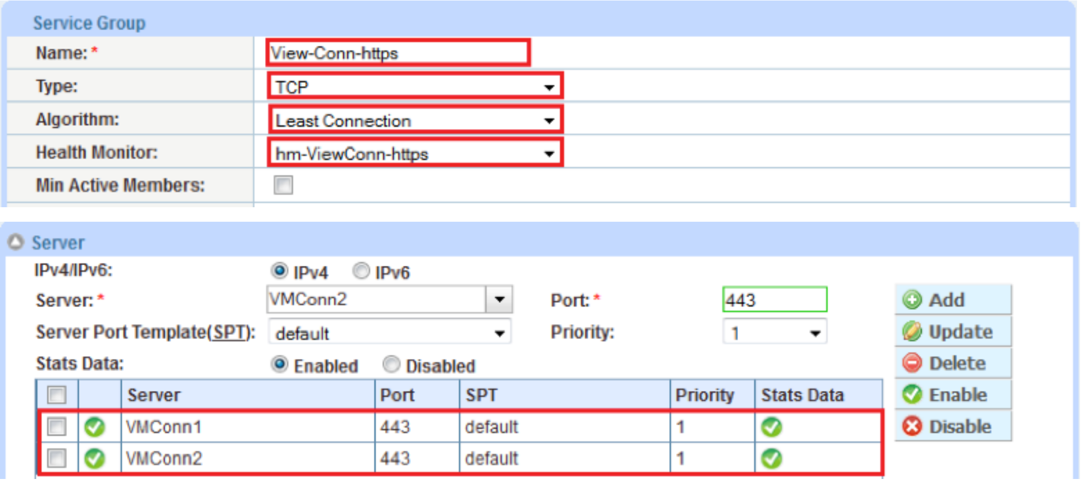
- Via CLI:

```
AX(config)#health monitor hm-ViewConn-https=
=AX(config-health:monitor)#method https
```

4.2.3 Create View Connection Service Group

Create a TCP service group for the View Connection 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 View Connection **Server Health Monitor**. Assign each View Connection Server to the service group with Port **443**.

- Via Web GUI: Config Mode > Service > SLB > Service Group



Service Group

Name: *	View-Conn-https
Type:	TCP
Algorithm:	Least Connection
Health Monitor:	hm-ViewConn-https
Min Active Members:	□

Server

IPv4/IPv6: ● IPv4 ○ IPv6

Server: * VMConn2 Port: * 443

Server Port Template(SPT): default Priority: 1

Stats Data: ● Enabled ○ Disabled

□		Server	Port	SPT	Priority	Stats Data
□	✓	VMConn1	443	default	1	✓
□	✓	VMConn2	443	default	1	✓

- Via CLI:

```
AX(config)#slb service-group View-Conn-https tcp
AX(config-slb svc group)#method least-connection
AX(config-slb svc group)#health-check hm-ViewConn-https
AX(config-slb svc group)#member VMConn1:443
AX(config-slb svc group)#member VMConn2:443
```

4.2.4 Create View Connection Persistence

Multiple end users can share the same IP address (users behind the same Proxy / firewall for instance). So persistence based on the source IP address does work, but may result in non-uniform load sharing between the View Connection Servers.

View Connection Servers use a cookie (JSESSIONID) to track users. AX Series can use the cookie information to provide persistence (using aFleX®) and thus offer uniform, even load sharing.

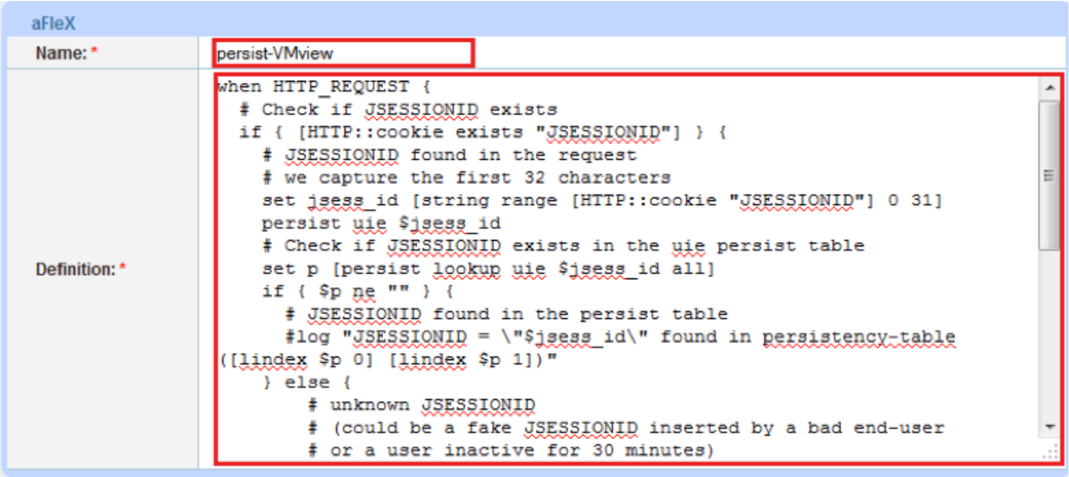
4.2.5 Create aFLEX Policy to Define View Persistence Rule

Here is the aFleX policy:

```
when HTTP_REQUEST {
  # Check if JSESSIONID exists
  if { [HTTP::cookie exists "JSESSIONID"] } {
    # JSESSIONID found in the request
    # we capture the first 32 characters
    set jsess_id [string range [HTTP::cookie "JSESSIONID"] 0 31]
    persist uie $jsess_id
    # Check if JSESSIONID exists in the uie persist table
    set p [persist lookup uie $jsess_id all]
  if { $p ne “” } {
   # JSESSIONID found in the persist table
   #log “JSESSIONID = \”$jsess_id\” found in persistency-table ([lindex $p 0] [lindex
$p 1])”
  } else {
    # unknown JSESSIONID
    # (could be a fake JSESSIONID inserted by a bad end-user
    # or a user inactive for 30 minutes)
    #log “JSESSIONID = \”$jsess_id\” not found in persistency-table”
   }
 } else {
   # JSESSIONID not found in the request
   # (could be a new client)
   #log “No JSESSIONID cookie”
  }
}

when HTTP_RESPONSE {
 if { [HTTP::cookie exists “JSESSIONID”] } {
  set jsess_cookie [HTTP::cookie “JSESSIONID”]
  persist add uie $jsess_cookie 1800
  #log “Add persist entry for JSESSIONID \”$jsess_cookie\””
 }
}
```

- Via Web GUI: Config Mode > Service > aFleX



Name: * persist-VMview

Definition: *

```
when HTTP_REQUEST {
  # Check if JSESSIONID exists
  if { [HTTP::cookie exists "JSESSIONID"] } {
    # JSESSIONID found in the request
    # we capture the first 32 characters
    set jsess_id [string range [HTTP::cookie "JSESSIONID"] 0 31]
    persist uie $jsess_id
    # Check if JSESSIONID exists in the uie persist table
    set p [persist lookup uie $jsess_id all]
    if { $p ne "" } {
      # JSESSIONID found in the persist table
      #log "JSESSIONID = \"$jsess_id\" found in persistency-table
([lindex $p 0] [lindex $p 1])"
    } else {
      # unknown JSESSIONID
      # (could be a fake JSESSIONID inserted by a bad end-user
      # or a user inactive for 30 minutes)
```

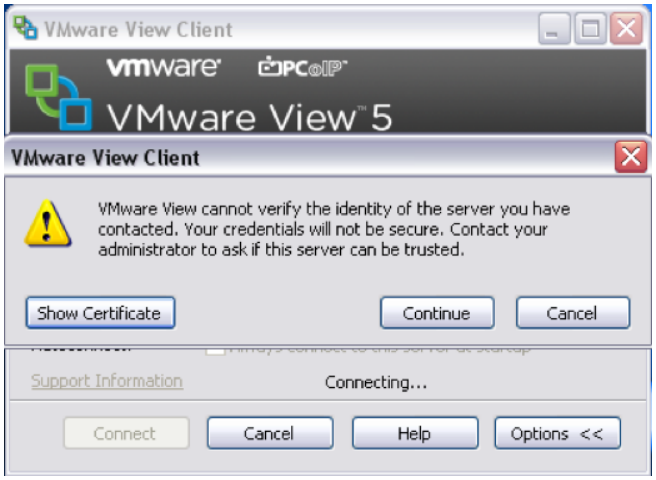
- Via CLI:

```
AX(config)#import aflex persist-VMview tftp://10.0.1.10/persist-VMview.txt
```

4.2.6 Create AX SSL Configuration

Import the View Connection Server Public Certificate / Private key onto the AX ADC device.

Note: Ask the VMware View Administrator for the certificate and key used on the View Connection Servers. For test purposes, an AX ADC self-signed cert/key can be used, but this will generate a warning message on the View Clients to accept the untrusted self-signed certificate.

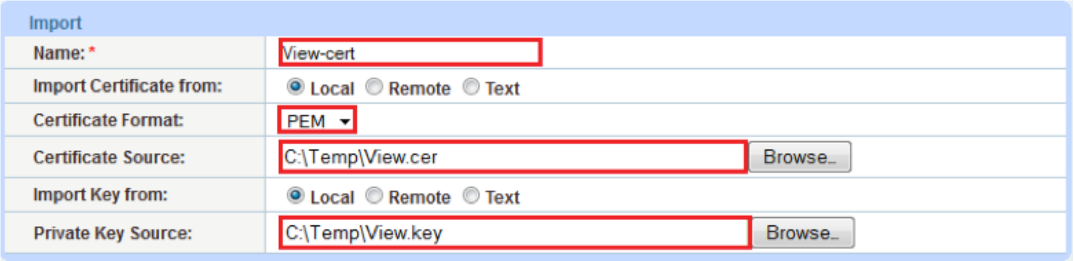


VMware View cannot verify the identity of the server you have contacted. Your credentials will not be secure. Contact your administrator to ask if this server can be trusted.

Connecting...

Import the IIS public certificate / private key onto the AX Series 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 Mode > Service > SSL Management > Certificate



Import

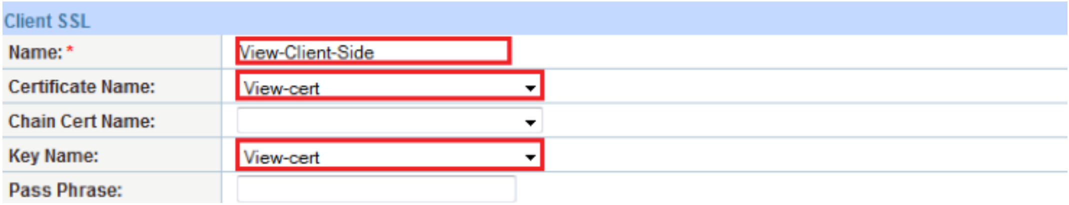
Name: *	View-cert
Import Certificate from:	● Local ○ Remote ○ Text
Certificate Format:	PEM
Certificate Source:	C:\Temp\View.cer Browse...
Import Key from:	● Local ○ Remote ○ Text
Private Key Source:	C:\Temp\View.key Browse...

- Via CLI:

```
AX(config)#slb ssl-load certificate View-cert type pem
tftp://10.0.1.10/View.cer
AX(config)#slb ssl-load private-key View-key tftp://10.0.1.10/View.key
```

Create a Client-SSL Template. Enter a Name for the Template, and Select the Certificate and Key Files.

- Via Web GUI: Config Mode > Service > SSL > Client SSL



Client SSL

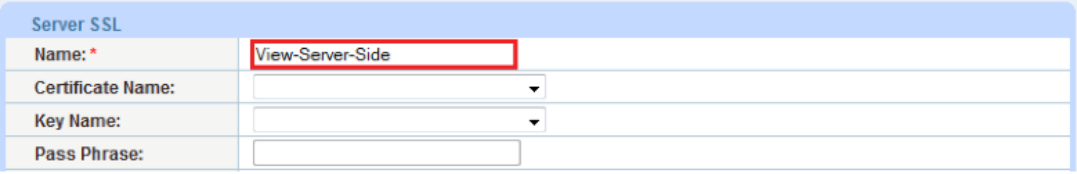
Name: *	View-Client-Side
Certificate Name:	View-cert
Chain Cert Name:	
Key Name:	View-cert
Pass Phrase:	

- Via CLI:

```
AX(config)#slb template client-ssl View-Client-Side=
AX(config-client ssl)#cert View-cert=
AX(config-client ssl)#key View-cert
```

Create a Server-SSL Template. Enter a Name for the Template.

- Via Web GUI: Config Mode > Service > SSL > Server SSL



Server SSL

Name: *	View-Server-Side
Certificate Name:	
Key Name:	
Pass Phrase:	

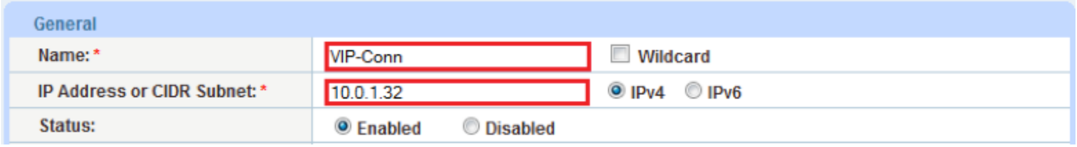
- Via CLI:

```
AX(config)#slb template server-ssl View-Server-Side
```

4.2.7 Create View Connection 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

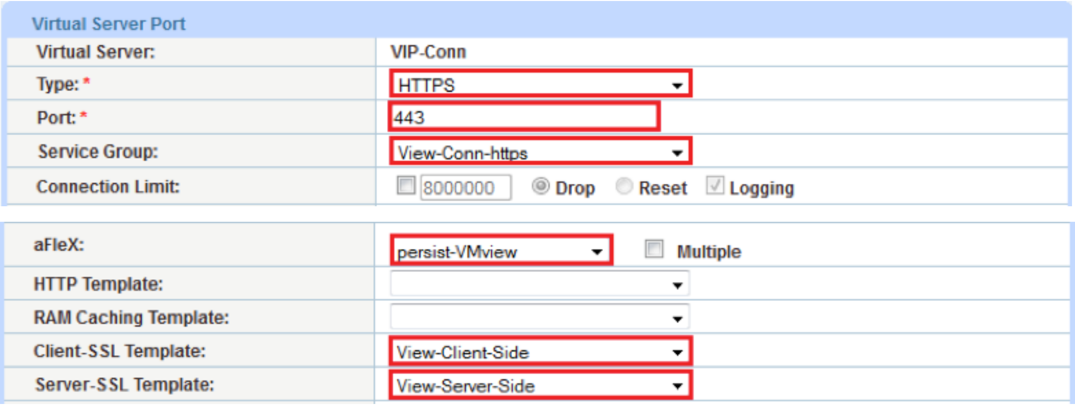
Name: *	VIP-Conn ☐ Wildcard
IP Address or CIDR Subnet: *	10.0.1.32 ● IPv4 ○ IPv6
Status:	● Enabled ○ Disabled

- Via CLI: = =

```
AX(config)#slb virtual-server VIP-Conn 10.0.1.32
```

Add port **Type** HTTPS Port 443 and select the **Service Group, Client-SSL Template, Server-SSL template and aFleX**.

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



Virtual Server Port

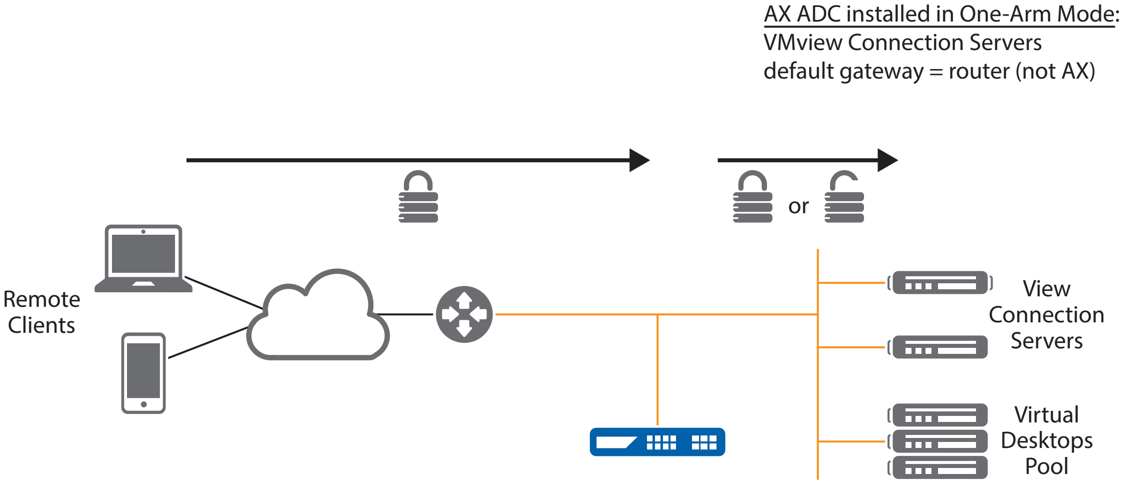
Virtual Server:	VIP-Conn
Type: *	HTTPS
Port: *	443
Service Group:	View-Conn-https
Connection Limit:	☐ 8000000 ● Drop ○ Reset ☑ Logging

aFleX:	persist-VMview ☐ Multiple
HTTP Template:	
RAM Caching Template:	
Client-SSL Template:	View-Client-Side
Server-SSL Template:	View-Server-Side

- Via CLI:

```
AX(config)#port 443 https=
AX(config-slb vserver-vport)#service-group View-Conn-https=
AX(config-slb vserver-vport)#template client-ssl View-Client-Side=
AX(config-slb vserver-vport)#template server-ssl View-Server-Side=
AX(config-slb vserver-vport)#aflex persist-VMview
```

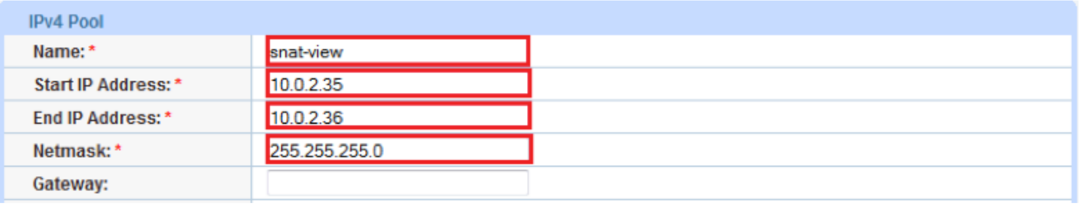
4.2.8 AX Series One-Arm Integration (Optional)


AX ADC installed in One-Arm Mode:
VMview Connection Servers
default gateway = router (not AX)
or
Remote Clients
View Connection Servers
Virtual Desktops Pool

In one-armed deployments (AX ADC is one-arm attached and the servers' default gateway is not AX ADC), you must configure IP source NAT (SNAT) to your View Connection Server VIP.

1. Create a SNAT IPv4 Pool. Enter a **Name**, a **Start-IP Address**, an **End IP address**, and a **Netmask**.

- Via Web GUI: Config Mode > Service > IP Source NAT > IPv4 Pool



IPv4 Pool

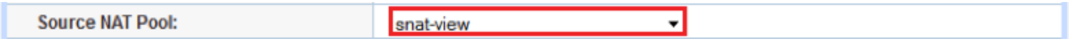
Name:*	snat-view
Start IP Address:*	10.0.2.35
End IP Address:*	10.0.2.36
Netmask:*	255.255.255.0
Gateway:	

- Via CLI:

```
AX(config)#ip nat pool snat 10.0.2.35 10.0.2.36 netmask /24
```

2. In the View Connection Server VIP, select the **Source NAT Pool**.

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



Source NAT Pool: snat-view

- Via CLI: = =

```
AX(config)#slb virtual-server Vip-Conn=
AX(config-slb vserver)#port 443 httpsö =
 AX(config-slb vserver-vport)#source-nat pool snat-view
```

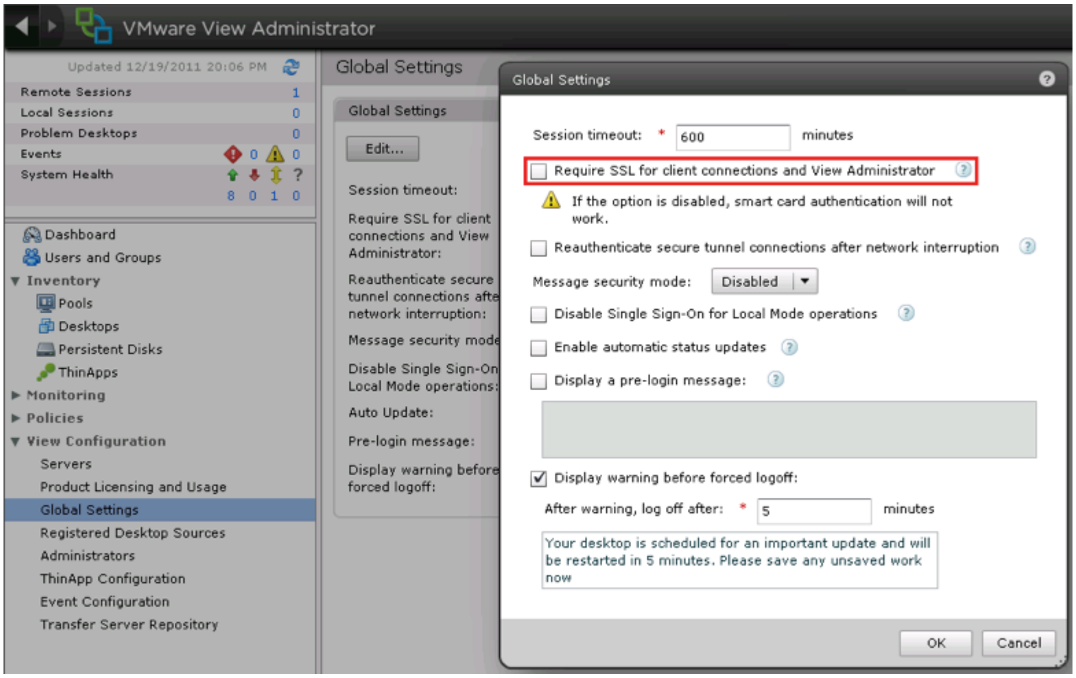
4.3 AX ADC Advanced Configuration

4.3.1 Offload SSL From the View Connection Servers Onto the AX ADC

With this option, end users will still use HTTPS to connect to their View Connection Servers. The AX ADC connects to the View Connection Servers via HTTP, this offloading CPU-intensive SSL processing from the servers onto the AX ADC.

Before starting the AX ADC configuration, update the VMware View Administrator configuration to allow access on HTTP.

1. Log on to VMware View Administrator.
2. Navigate to View Configuration > Global Settings.
3. Deselect "Require SSL for client connections and View Administrator".



Global Settings

Session timeout: * 600 minutes

□ Require SSL for client connections and View Administrator

If the option is disabled, smart card authentication will not work.

□ Reauthenticate secure tunnel connections after network interruption

Message security mode: Disabled

□ Disable Single Sign-On for Local Mode operations

□ Enable automatic status updates

□ Display a pre-login message:

☑ Display warning before forced logoff:

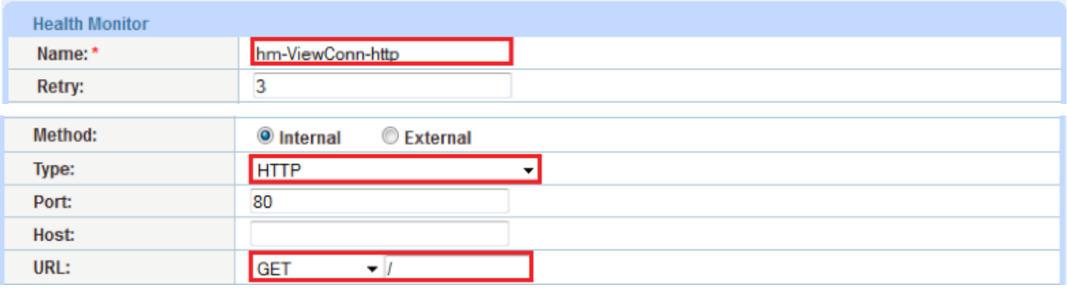
After warning, log off after: * 5 minutes

Your desktop is scheduled for an important update and will be restarted in 5 minutes. Please save any unsaved work now

4. Create port 80 for each of the View Connection servers.
   - Via Web GUI: Config Mode > Service > SLB > Server]
   - Via CLI:

```
AX(config)#slb server VMConn1 10.0.2.164=
AX(config-real server)#port 80 tcp
```

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



Health Monitor

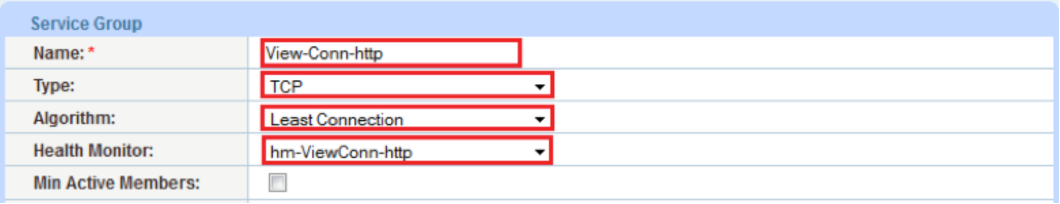
Name: *	hm-ViewConn-http
Retry:	3
Method:	● Internal ○ External
Type:	HTTP
Port:	80
Host:	
URL:	GET /

- Via CLI:

```
AX(config)#health monitor hm-ViewConn-http=
AX(config-health:monitor)#method http
```

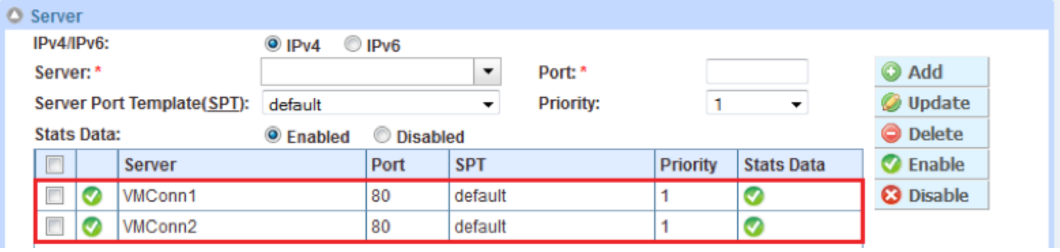
6. Create a TCP service group for the View Connection Servers. Enter a **Name** for the service group, select TCP from the **Type** drop-down list, select the Least Connection load balancing **Algorithm**, and select the View Connection Server **Health Monitor**. Assign each View Connection Server to the service group with Port 80.

- Via Web GUI: Config Mode > Service > SLB > Service Group



Service Group

Name: *	View-Conn-http
Type:	TCP
Algorithm:	Least Connection
Health Monitor:	hm-ViewConn-http
Min Active Members:	□



Server

IPv4/IPv6: ● IPv4 ○ IPv6

Server: *

Port: *

Server Port Template(SPT): default

Priority: 1

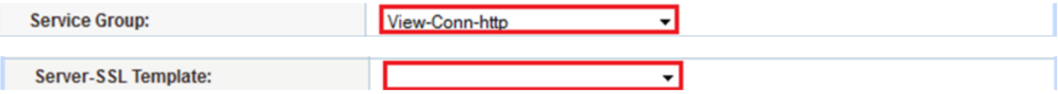
Stats Data: ● Enabled ○ Disabled

□		Server	Port	SPT	Priority	Stats Data
□	✓	VMConn1	80	default	1	✓
□	✓	VMConn2	80	default	1	✓

- Via CLI:

```
AX(config)#slb service-group View-Conn-http tcp
AX(config-slb svc group)#method least-connection=
AX(config-slb svc group)#health-check hm-ViewConn-http=
AX(config-slb svc group)#member VMConn1:80=
AX(config-slb svc group)#member VMConn2:80
```

7. In the View Connection Server VIP, select the **Service Group** with HTTP servers, and remove the **Server-SSL Template** since the AX device will communicate with the Connection View Servers through HTTP instead of HTTPS.



Service Group:	View-Conn-http
Server-SSL Template:	

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

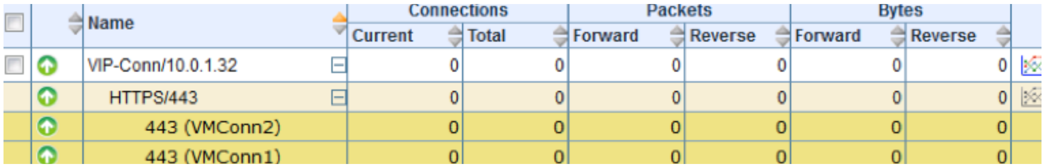
```
AX(config)#slb virtual-server Vip-Conn=
AX(config-slb vserver)#port 443 https=
AX(config-slb vserver-vport)#service-group View-Conn-http=
AX(config-slb vserver-vport)#no template server-ssl View-Server-Side
```

5 Configuration Validation

5.1 Validate Basic Deployment WIthout SSL Offload

Validate the Status of the VIP and that its Members are UP.

- Via Web GUI: Monitor Mode > Service > SLB > Virtual Server



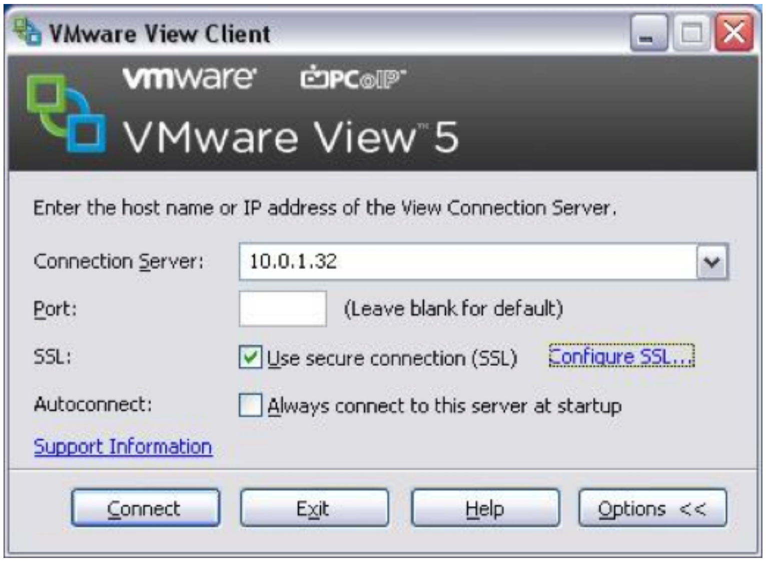
			Connections		Packets		Bytes		
☐		Name	Current	Total	Forward	Reverse	Forward	Reverse	
☐	⬆	VIP-Conn/10.0.1.32 ⊟	0	0	0	0	0	0	
	⬆	HTTPS/443 ⊟	0	0	0	0	0	0	
	⬆	443 (VMConn2)	0	0	0	0	0	0	
	⬆	443 (VMConn1)	0	0	0	0	0	0	

- Via CLI:

```
AX#show slb virtual-server VIP-Conn=
AX#show slb service-group View-Conn-https=
AX#show slb server VMConn1=
AX#show slb server VMConn2
```

Validate the Access to the VMware View Service for a VMware View Client.

Launch VMware View and connect to the VIP:



Enter the host name or IP address of the View Connection Server.

Connection Server: 10.0.1.32

Port: (Leave blank for default)

SSL: ☑ Use secure connection (SSL) Configure SSL...

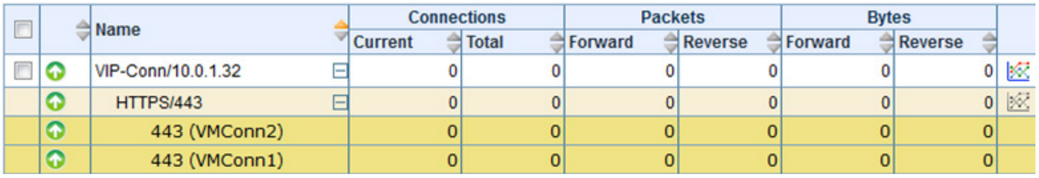
Autoconnect: ☐ Always connect to this server at startup

Support Information

5.2 Validate Advanced Deployment with SSL Offload

Validate the Status of the VIP and that its Members are UP.

- Via Web GUI: Monitor Mode > Service > SLB > Virtual Server



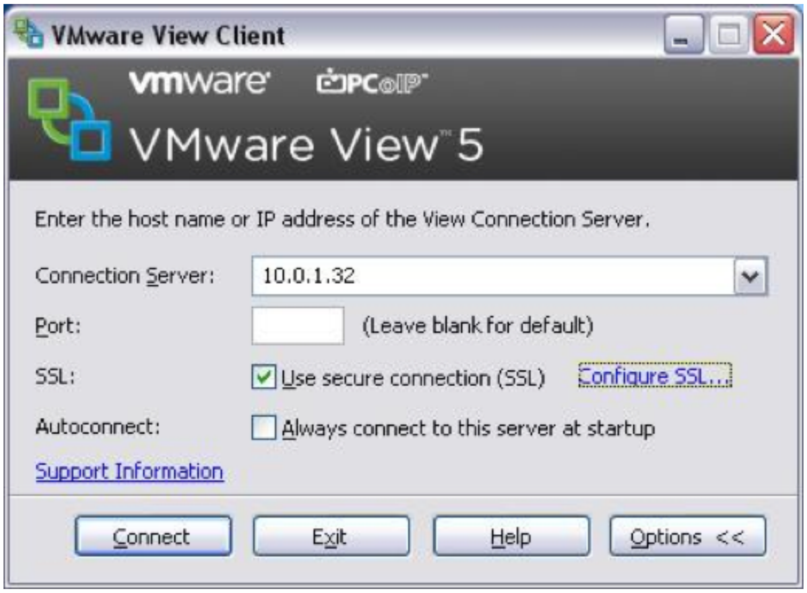
			Connections		Packets		Bytes		
☐		Name	Current	Total	Forward	Reverse	Forward	Reverse	
☐	⬆	VIP-Conn/10.0.1.32 ⊟	0	0	0	0	0	0	
	⬆	HTTPS/443 ⊟	0	0	0	0	0	0	
	⬆	443 (VMConn2)	0	0	0	0	0	0	
	⬆	443 (VMConn1)	0	0	0	0	0	0	

- Via CLI:

```
AX#show slb virtual-server VIP-Conn
AX#show slb service-group View-Conn-http
AX#show slb server VMConn1
AX#show slb server VMConn2
```

Validate the Access to the VMware View Service for a VMware View Client.

Launch VMware View and connect to the VIP:



Enter the host name or IP address of the View Connection Server.

Connection Server: 10.0.1.32

Port: (Leave blank for default)

SSL: ☑ Use secure connection (SSL) Configure SSL...

Autoconnect: □ Always connect to this server at startup

A. AX ADC Configuration

The configuration below includes the following options:

- SSL offload
- No SNAT (AX Series installed in Routed Mode)

```
slb server VMConn1 10.0.2.164
   no health-check
   port 80  tcp
slb server VMConn2 10.0.2.165
   no health-check
   port 80  tcp
health monitor hm-ViewConn-http
 method http
slb service-group View-Conn-http tcp
    method least-connection
    health-check hm-ViewConn-http
    member VMConn1:80
    member VMConn2:80
slb template client-ssl View-Client-Side
   cert View-cert
   key View-cert
slb virtual-server VIP-Conn 10.0.1.32
   port 443  https
      service-group View-Conn-http
      template client-ssl View-Client-Side
      aflex persist-VMview
```

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-16119-EN-01
Aug 2014

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam@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.

©2014 A10 Networks, Inc. All rights reserved. A10 Networks, the A10 Networks logo, A10 Thunder, Thunder, vThunder, aCloud, ACOS, and aGalaxy are trademarks or registered trademarks of A10 Networks, Inc. in the United States and in other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.