

Deployment Guide

AX Series with Microsoft Windows Server 2008 Terminal Services

Version: 1.0.1



Table of Contents

DEPLOYMENT GUIDE

AX Series with Microsoft Windows Server 2008 Terminal Services

Introduction 3 Prerequisites & Assumptions 3
AX deployment for Windows TS with RDC access
AX configuration
AX deployment valuation 10 AX deployment for Windows TS with RDC with TSG access 12 Microsoft TS Gateway configuration with load balancers such as AX
AX deployment for Windows TS with Web access20Microsoft TS Gateway configuration with load balancers such as AX20AX configuration21AX VIP status24AX deployment validation24

Summary and Conclusion	
-------------------------------	--

Introduction

This deployment guide contains configuration procedures for AX Series application delivery controllers and server load balancers to support Windows Server 2008 Terminal Services.

Microsoft Terminal Services (TS) allows users to remotely control the whole desktop or certain applications. Microsoft provides three TS access modes:

- Remote Desktop Connection (RDC)
- Remote Desktop Connection with TS Gateway (RDC with TSGW)
- Web Access

For more information on Microsoft TS 2008, visit:

http://www.microsoft.com/Windowsserver2008/en/us/ts-product-home.aspx

The AX Series with its Advanced Core Operating System (ACOS) has been designed specifically for applications such as TS, providing more robust response in failover situations, offloading security processing, and performing intelligent load sharing for all three TS access modes.

Prerequisites & Assumptions

- A10 Networks' AX platform should be running software version 2.0 or later.
- It is assumed that users have some basic configuration familiarity with both AX and Microsoft TS products.
- The AX can be configured in one-armed mode or routed mode.
- · Microsoft screenshots are from Windows 2008R2 TS servers.
- Note: A10 supports Microsoft 2008 and Windows 2003 TS servers too. The same A10 configuration can be applied for them.
- Both IPv4 and IPv6 Windows TS are supported. The examples in this deployment guides use IPv4.





AX deployment for Windows TS with RDC access

Windows 2008 enhanced TS with a new role: Session Broker. TS Session Broker provides simple load balancing and user persistency to the TS Server.

Microsoft recommends Session Broker for Terminal Server farms of two to five servers. (http://download.microsoft.com/download/b/b/5/bb50037f-e4ae-40d1-a898-7cdfcf0ee9d8/All-Up/ WS08AndWS03ComparisonFinal_En.docx.)

AX fully supports Microsoft TS and allows:

- Large TS farms
- · Granular TS load balancing and availability options
- TS in private networks (not directly reachable from outside)



Figure 1: Microsoft TS with RDC access deployment



Microsoft TS configuration with the AX Series load balancer

Note: To download a step-by-step guide for Microsoft TS, visit: http://technet.microsoft.com/en-us/library/ cc772418%28WS.10%29.aspx

As explained in the Microsoft guide, to deploy with load balancers, configure the following Remote Desktop Connection Broker settings on each TS. Navigate to Administrative Tools > Remote Desktop Services > Remote Desktop Session Host Configuration - Edit Settings / RD Connection Broker. Use the following settings:

- Deselect **Participate in Connection Broker Load-balancing**. (Load balancing is performed by the AX device.)
- Select Use token redirection. (When an end user closes their RDP connection without logging out and then reconnects, the end-user does not reconnect directly to the TS. Instead, they provide the TS IP address information in a routing token used by the load balancer to know where to redirect the end-user.)
- Select the IP address of the TS provided in the token. (This must be the Terminal Server IP address defined on the AX device.)

Pro	perties		x
G	eneral Licensing RD Co	nnection Broker BD IP Virtualization	
	ieneral Deensing		1
	Server purpose:	Member of fam	
	RD Connection Broker:	TSSB.dimi.fr	
	Farm name:	RDP-Farm1	
		Change Settings	
	Participate in Connect Relative weight of this	tion Broker Load-Balancing s server in the farm: 100	
	Use token redirection	•	
	Select token redirection use of <u>RD Connection B</u> Select IP addresses to be	only if your load balancer supports the iroker routing tokens.	
	IP Address	Network Connection	
	10.0.2.6	Local Area Connection	
	☐ fe80::100:7f.fffe ☐ fe80::5efe:10.0	Local Area Connection* 11 isatap.{E78D0145-6244-4E53-9C0 💌	
		OK Cancel Apply	



AX configuration

Note: This example shows only the required AX options. For information about other options, see the AX Series Configuration Guide, the AX Series GUI Reference, or the GUI online help.

AX configuration steps:

- 1. Create a real server for each TS. Enter the TS name and IP address, and add TCP port 3389.
 - Via Web GUI: Config Mode > Service > SLB > Server

Jeneral						_				
Name: *			TS1							
P Address	Host: *		10.0.2.6			⊙IPv	/4 ○IPv6			
SSLB Exte	rnal IP A	ddress:								
Neight:		F	1							
Port		-								lant
Port Port: * 3	389 s Linsit/(C	Protoco	ol: TCP	- Weig	jht(<u>W</u>)	:* 1	n Resume((lo SSL		O Add
Port Port: * 3 Connectio Server Po	389 n Limit(<u>C</u> t Templa	Protoco <u>L</u>):8000000 pte(SPT):	ol: TCP	🖌 Weig ng	jht(<u>W</u>)	: * 1 Connectio	n Resume(<u>C</u>	lo SSL <u>R</u>):	bled	📀 Add 🥥 Update
Port Port: * 3 Connectio Server Pol Health Mo	389 n Limit(<u>C</u> t Templa nitor(<u>HM</u>)	Protoco L):8000000 nte(<u>SPT</u>): [:	ol: TCP toggi Loggi default	Weig ng	jht(<u>W</u>) <mark>≫</mark> ○Fo	: * 1 Connectio Stats Data Ilow Port:	n Resume(<u>C</u> a(<u>SD</u>): ⊙En	lo SSL R): abled O Disa	bled	 ⊘ Add ⊘ Update ⊘ Delete ⊘ Enable
Port 3 Port: 4 3 Connectio Server Pol Health Mor	889 n Limit(<u>C</u> t Templa nitor(<u>HM</u>) Port	Protoco L): 8000000 nte(SPT): Correction Protocol	ol: TCP Loggi default sult) CL	Weig ng	jht(<u>W</u>) ♥ ○Fo W	: * 1 Connectio Stats Data Ilow Port: No SSL	n Resume(<u>C</u> a(<u>SD</u>):	lo SSL R): abled O Disa	ibled SD	 Add Update Delete Enable Disable

• Via CLI: AX(config)#slb server TS1 10.0.2.6 AX(config-real server)#port 3389 tcp

2. Create the service group (TS farm).

Enter a name for the service group, and select **TCP** from the **Type** drop-down list. Assign each TS to the service group.



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

Service Group							
Name: *	TS-Farm						
Туре:	TCP			~			
Algorithm:	Round Rob	n		~			
Health Monitor:				~			
Min Active Members:							
	Send client r	eset whe	en server s	election fails			
Stats Data:	Enabled	OD	isabled				
Description:							
Server							
IPv4/IPv6:	⊙ IPv4 C	IPv6			-		
Server: *	TS2		0	Port: *	33	89	📀 Add
Server Port Template(SPT):	default		*	Priority:	1	*	🥥 Update
Stats Data:	Enabled	ODisa	bled				🤤 Delete
Server		Port	SPT		Priority	Stats Data	🔮 Enable
🔲 🧭 TS1		3389	default		1	0	🔇 Disable
TS2		3389	default		1	0	

- Via CLI: AX(config)#slb service-group TS-Farm tcp AX(config-slb svc group)#member TS1:3389 AX(config-slb svc group)#member TS2:3389
- 3. Create the virtual IP address (VIP), which is the IP address that clients will access.
 - a. Enter a name for the VIP, and enter the IP address.
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server

General		
Name: *	TS	Uildcard Vildcard
IP Address or CIDR Subnet: *	62.52.24.31	⑧ IPv4 ○ IPv6
Status:	💿 Enabled 🛛 🔘 I	Disabled

- Via CLI: AX(config)#slb virtual-server TS 62.52.24.31
- b. Add the TCP port and select the service group.



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

Virtual Server Port	
Name:	TS
Type: *	TCP
Port: *	3389
Service Group:	TS-Farm
Connection Limit:	8000000 Orop Reset Logging

 Via CLI: AX(config-slb vserver)#port 3389 tcp AX2(config-slb vserver-vport)#service-group TS-Farm

4. Create an aFleX policy, to define the TS persistence rule:

```
when CLIENT ACCEPTED {
     # Collect client packet only if there is at least 30 bytes
     # (If there is no routing token => first packet is 19 bytes)
     TCP::collect 30
}
when CLIENT DATA {
     # Find and save the routing token in the variable "msts"
      set payload [TCP::payload]
      set index [ expr [string first "msts=" $payload] + [string length "msts="]]
      #only if there is a routing token
      if \{ and the set of the set of
            set msts [string range $payload $index end]
           # Find and save the rawip@ in the variable "rawip"
            set index2 [string first "." $msts]
            set rawip [string range $msts 0 [expr $index2 -1]]
           # Find and save the raw tcp port in the variable "rawport"
           set msts2 [string range $msts [expr $index2 + 1] end]
            set index3 [string first "." $msts2]
            set rawport [string range $msts2 0 [expr $index3 - 1]]
           # Convert and save the real tcp port in the variable "port"
            set port [ntohs [format "%d" $rawport]]
           # Convert and save the real ip@ in the variable "ipaddr"
            set bin [binary format i $rawip]
           binary scan $bin cccc a b c d
            set ipaddr "$a.$b.$c.$d"
           node $ipaddr $port
           # print the node
           # log "node= $ipaddr $port"
      }
}
```



Via Web GUI: Config Mode > Service > aFleX



- Via CLI: AX(config)#import aflex TS-persist tftp://172.31.31.12/TS-persist
- 5. Assign the aFleX policy to the virtual server.
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port

	aFleX:	TS-persist 💌
0	Via CLI:	AX(config)#slb virtual-server TS 62.52.24.31
		AX(config-slb vserver)#port 3389 tcp
		AX(config-slb vserver-vport)#aflex TS-persist

AX VIP status

Display the status of the VIP and its members:

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

	Name	4	Connee	ctions	Pack	(ets	Byt	es	
	NdHe	-	Current 🛛 🍦	Total 🍦	Forward 🛛 🍦	Reverse 🍦	Forward 🛛 🍦	Reverse 🍦	
\mathbf{O}	TS/62.52.24.31	Ξ	0	0	0	0	0	0	\boxtimes
0	HTTPS/443	Ξ	0	0	0	0	0	0	$ \infty $
•	80 (TSG1)		0	0	0	0	0	0	
\mathbf{O}	80 (TSG2)		0	0	0	0	0	0	

 Via CLI: AX#show slb virtual-server TS AX#show slb service-group TSG-Farm AX#show slb server [TSG1 | TSG2]



AX deployment validation

To validate the AX deployment:

- 1. Verify that clients can access the TS farm using RDP access via the VIP:
 - Launch RDP (mstsc.exe) and connect to the VIP.

🔁 Remote 🛙	esktop Connection	
9	Remote Desktop Connection	
<u>C</u> omputer:	62.52.24.31	
User name:	None specified	
You will be as	ked for credentials when you connect.	
	Co <u>n</u> nect Cancel <u>H</u> elp	<u>Options >></u>

- Validate that the client has access to a TS.
- Administrative Tools > Remote Desktop Services > Remote Desktop Services Manager, and go to the TS group.

🂁 Remote Desktop Service	s Manager	_ 8 ×
File Action View Help		
🗢 🔿 🔰 🔂 🗊		
Remote Desktop Services N		Actions
🛨 🚡 TSSB.dimi.fr	Manage Remote Desktop Session Host Server Group: RDF	RDP-Farm1 🔺
My Group Training RDP-Farm1	4	🚯 Add Computer
	Users Sessions Processes	🚡 Empty Group
	Corver User Cossien ID State IdleTime LogOnTime	Q Refresh
	TS2 user1 RDP-Tc 2 Active . 6/21/2010	Seset
		a

2. Verify persistence. Have one client close its RDP session (without logging out from the TS), and reconnect. The AX device should send the new connection to the same TS.



 Open an application (for instance, "Notepad") and close the RDP session without logging out from the TS.



• Establish a new RDP connection (from the same PC or another one) and log in with the same user. The new RDP connection is on the same server and the application is still there.



AX deployment for Windows TS with RDC with TSG access

Windows 2008 enhanced its TS with a new role: Gateway. TS Gateway provides RDP connection over HTTPS. The Gateway role enables remote end-users to access the TS farm, even when the RDP protocol is blocked by a firewall and only HTTP/HTTPS is authorized.

The AX device fully supports Microsoft TS Gateway and allows:

- Large TS Gateway farms
- · Granular TS Gateway loadbalancing and availability options
- TS Gateways in private networks (which are not directly reachable from outside)
- · Optional SSL offload on TS Gateways

Note: The same AX device can be used for TS with RDS (described in the previous section) and TS with RDC with TSG.



Figure 2: Microsoft TS with RDC with TSG access deployment

Microsoft TS Gateway configuration with load balancers such as AX

Note: To download a step-by-step guide for Microsoft TS Gateway, visit: http://technet.microsoft.com/enus/library/cc771530%28WS.10%29.aspx



As explained in the Microsoft guide, to deploy with load balancers, configure the following settings on each TS Gateway. (Navigate to Administrative Tools > Remote Desktop Services > Remote Desktop Gateway Manager – Edit Properties / Server Farm.)

	Add
	Add
	Add
a second scheme all se Prove	and a state of the
t to include in the farm	, and ensure that
	Details
0 This RD Gateway	server farm member is
1 This RD Gateway	server farm member is
	Remove
s	s This RD Gateway 1 This RD Gateway

When deployed with load balancers configured with no TS Gateway SSL offload, use the same server certificate for the following on all TS Gateways:

- IIS (Navigate to Administrative Tools > IIS Select Server > Sites > Default Web Site Edit Site Bindings.)
- Terminal Service Gateway (Navigate to Administrative Tools > Remote Desktop Services > Remote Desktop Gateway Manager Edit Properties / SSL Certificate) on all TS Gateways.



When deployed with load balancers that are configured with TS Gateway SSL offload, configure HTTPS-HTTP bridging on each TS Gateway. (Navigate to Administrative Tools > Remote Desktop Services > Remote Desktop Gateway Manager – Edit Properties / SSL Bridging.)

For enha	anced security,	you can configure	e RD Gateway	for use wit	h ISA Server or	a
non-Mic	rosoft product to	perform secure	sockets layer (SSL) bridgi	ng.	
🔽 Use	SSL Bridging					
C	HTTPS - HT requests)	ſPS bridging (tem	ninate SSL req	ue <mark>sts and i</mark>	nitiate new HTT	rps
¢	HTTPS - HT requests)	FP bridging (termin	nate SSL reque	ests and ini	tiate new HTTF	,
						-

AX configuration

The steps below detail the AX configuration for TS Gateway with SSL offload. If you do not want to offload SSL on TS Gateway, see the "No SSL Offload Note" in each step.

Note: This example shows only the required AX options. For information about other options, see the AX Series Configuration Guide, the AX Series GUI Reference, or the GUI online help.

AX configuration steps:

 Create a real server for each TS Gateway. Enter the TS name and IP address, and add TCP port 80.

No SSL Offload Note: Replace port 80 with 443.



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

General											
Name: *			TSG1								
IP Addres	s/Host: *		10.0.2.8			⊙ıp∖	⊙ IPv4 ○ IPv6				
GSLB Exte	ernal IP A	ddress:									
Weight:		[1								
Dort											
Port: * 8	0	Protoc	ol: TCP	~	Weigh	t(W):	* 1		No SSL		🗿 Add
Connectio	n Limit((L): 8000000	Log	ging			Connectio	n Resume(CR):		🥥 Update
Server Po	rt Templ	ate(SPT):	default	0000118	~	1	Stats Data	n(<u>SD</u>): 💿 El	nabled ODisa	abled	😂 Delete
Health Mo	nitor(<u>HM</u>): 💿 (defa	ault)		* (Fol	low Port:		TCP Y		🥝 Enable
	Port	Protocol	CL	CF	2	W	No SSL	SPT	НМ	SD	🙆 Disable
	80	TCP	8000000	0		1	8	default	(default)	0	

- Via CLI: AX(config)#slb server TSG1 10.0.2.8 AX(config-real server)#port 80 tcp
- Create a service group for the TS Gateway farm.
 Enter a name for the service group, and select TCP from the Type drop-down list. Assign each TS Gateway to the service group.

No SSL Offload Note: Replace port 80 with 443.

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

				1			
Name: *	TSG-Farm			8			
Туре:	TCP			~			
Algorithm:	Round Robi	'n		*			
Health Monitor:				*			
Min Active Members:							
	Send client r	eset wh	en server s	election fails			
Stats Data:	Enabled	OD	isabled				
Sanyar							
Server	@IDv1_0						
Server IPv4/IPv6: Server: "	● IPv4 ○ TSG2)IPv6	0	Port: *	80		Add
Server IPv44Pv6; Server: * Server Port Template(<u>SPT</u>):)IP∨6	0	Port: * Priority:	80	×	 Add Update
Server IPv4/IPv6: Server: * Server Port Template(<u>SPT</u>): Stats Data:	 IPv4 TSG2 default Enabled) IP∨6 ◯ Disa	abled	Port: * Priority:	80	×	 Add Update Delete
Server IPv4/IPv6: Server: * Server Port Template(<u>SPT</u>): Stats Data:	 IPv4 TSG2 default Enabled 	Disa O Disa	abled SPT	Port: * Priority:	80 1 Priority	Stats Data	 Add Update Delete Enable
Server IPv4.IPv6: Server: * Server Port Template(<u>SPT</u>): Stats Data: Server Server	 ● IPv4 ○ TSG2 default ● Enabled 	PV6 O Disa Port	abled SPT default	Port: * Priority:	Priority	Stats Data	 Add Update Delete Enable Disable

 Via CLI: AX(config)#slb service-group TSG-Farm tcp AX(config-slb svc group)#member TSG1:80 AX(config-slb svc group)#member TSG2:80



- 3. Create the virtual IP address (VIP), which is the IP address that clients will access.
 - No SSL Offload Note: In step b, replace port type **HTTPS** with **TCP**.
 - a. Enter a name for the VIP, and enter the IP address.
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server

General		
Name: *	TS	Uvildcard
IP Address or CIDR Subnet: *	62.52.24.31	IPv4 ○ IPv6
Status:	⊙ Enabled ○ Disabled	

- Via CLI: AX(config)# slb virtual-server TS 62.52.24.31
- b. Add the HTTPS port and select the service group.
- Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port

Virtual Server Port	
Name:	TS
Type: *	HTTPS 💙
Port: *	443
Service Group:	TSG-Farm
Connection Limit:	■ 8000000 ● Drop

- Via CLI: AX(config-slb vserver)#port 443 https AX2(config-slb vserver-vport)#service-group TSG-Farm
- 4. Import the TS Gateway certificate onto the AX device, and add it to a client-SSL template: *No SSL Offload Note: Skip this step.*
 - a. 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: *	TSG-Cert
Import Certificate from:	
Certificate Format:	PFX Y
Password:	•••••
Certificate Source:	C:\Temp\tsgw2.pfx Browse

 Via CLI: AX(config)#slb ssl-load certificate TSG-Cert type pfx password a10 tftp://10.0.1.10/tsgw2.pfx



- b. Create a client-SSL template. Enter a name for the template, select the certificate and key files, and enter the passphrase.
- Via Web GUI: Config Mode > Service > Template > SSL > Client SSL

Client SSL		
Name: *	TSG-Cert-template	
Certificate Name:	TSG-Cert	×
Chain Cert Name:		×
Key Name:	TSG-Cert	×
Cache Size:	0	
Pass Phrase:	•••••	
Confirm Pass Phrase:	•••••	

- ViaCLI: AX(config)#slb template client-ssl TSG-Cert-template AX(config-client ssl)#cert TSG-Cert AX(config-client ssl)#key TSG-Cert passphrase a10
- 5. Assign the client-SSL template to the virtual server port. No SSL Offload Note: Skip this step.
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port

Client-SSL Template:		TSG-Cert-template
• Via CLI:	AX(config)#s]	lb virtual-server TS 62.52.24.31
	AX(config-sl	b vserver)#port 443 https
	AX(config-sl	b vserver-vport)#template client-ssl TSG-Cert-ter
plate		

Note: TS Gateways do not need persistence. Each TS Gateway is aware of all user connections. When an end-user closes their RDP connection without logging out, and then reconnects, the connection may be load balanced to another TS Gateway. The TS Gateway simply forwards the end-user traffic to the correct TS Gateway.



AX VIP status

Display the status of the VIP and its members:

1. Via Web GUI: Config Mode > Service > SLB > Virtual Server

	Nama		Connec	ctions	Pack	ets	Byt		
	ndifie	-	Current 🛛 🍦	Total 🏻 🍦	Forward 🏻 🍦	Reverse 🍦	Forward 🏻 🍦	Reverse 🍦	
\mathbf{O}	TS/62.52.24.31	Ξ	0	0	0	0	0	0	×
0	HTTPS/443	Ξ	0	0	0	0	0	0	$[\underline{\mathbb{M}}]$
•	80 (TSG1)		0	0	0	0	0	0	
•	80 (TSG2)		0	0	0	0	0	0	

2. ViaCLI:AX#show slb virtual-server TS
 AX#show slb service-group TSG-Farm
 AX#show slb server [TSG1 | TSG2]



AX deployment validation

To validate the AX deployment:

- 1. Verify that clients can access the Terminal Servers using RDP with TSG access via the VIP:
 - Launch RDP (mstsc.exe) and connect to the TS with the TSG option configured. (Navigate to Options – Advanced > Settings.)

蚀 TS Gateway Server Settings	×
Remote Desktop Connection	
What is a TS Gateway server and how do I know if I need one?	
Connection settings O Automatically detect TS Gateway server settings	
O ∐se these TS Gateway server settings:	
Server name: tsgw2.dimi.fr	
Logon method: Allow me to select later	
Bypass TS Gateway server for local addresses	
○ Do not use a TS Gateway server	
Logon settings	5
User name: DIMI\administrator	
Saved credentials will be used to connect to this TS Gateway server. You can <u>edit</u> or <u>delete</u> these credentials.	
OK Cancel	

- Validate that the client has access to a TS.
- On the TS Gateway, validate that the TS Gateway is aware of the client connection. (Navigate to Administrative Tools > Remote Desktop Services > Remote Desktop Gateway Manager + Go to Monitoring.)

音 RD Gateway Manager		_ 8 ×
<u>File Action View Help</u>		
🗢 🔿 🔰 📊 🛛 🗖		
RD Gateway Manager	Monitoring	Actions
TSGW1 (Local) TSGW1 (Local)		Monitoring 🔺
Monitoring	More about Monitoring a RD Gateway Server.	Select All
	1 Connection(s) from 1 user(s) to 1 remote computer(s)	Edit Connection
	Set Automatic R	
	Connection ID User ID User Name Connected On	View 🕨
	4:1 DIMI\Administrator DIMI\Administrator 6/22/2010 4:27:26 PM	Q Refresh



AX deployment for Windows TS with Web access

Windows 2008 enhanced TS with a new role: Web Access. TS Web Access provides web access to distributed applications on TS.

End customers access the web portal that provides the list of distributed applications on TS. Then they connect to these applications via RDP to the TS.

The AX device fully supports Microsoft TS Gateway with Web access and allows:

- Large TS Gateway farms
- · Granular TS Gateway load balancing and availability options
- TS Gateways in private networks (not directly reachable from outside)
- (optional) SSL offload on TS Gateways

Note: The same AX device can be used for TS with RDS and TS with RDC with TSG.



Figure 3: Microsoft TS with Web access deployment

Microsoft TS Gateway configuration with load balancers such as AX

Note: To download a step-by-step guide for Microsoft TS Gateway, visit: http://technet.microsoft.com/enus/library/cc771354(WS.10).aspx

TS Web Access does not need any specific configuration when deployed with load balancers.



AX configuration

The steps below detail AX configuration for TS Web Access.

Note: This example shows only the required AX options. For information about other options, see the AX Series Configuration Guide, the AX Series GUI Reference, or the GUI online help.

AX configuration steps:

443

TCP

- Create a real server for each TS Gateway. Enter the TS name and IP address, and add TCP port 443.
 - Via Web GUI: Config Mode > Service > SLB > Server

General		
Name: *	TSW1	
IP Address/Host: *	10.0.2.10 💿 IPv4 🔘	IPv6
GSLB External IP Address:		
Weight:	1	
O Port Port: * 443 Prote	col: TCP 🛛 Weight(<u>W</u>): ' 1	No SSL Q Add
Connection Limit/CL/v/90000	me/CR):	
Server Port Template(SPT)	Enabled Obisabled Obisabled Obisabled Obisabled Obisabled Obisabled Obisabled Obisabled Obisable Obis	
Port Protoco	I CL CR W No SSL SPT	HM SD SD Disable

3

1

default

(default)

0

 Via CLI: AX(config)#slb server TSW1 10.0.2.10 AX(config-real server)#port 443 tcp

8000000 🧭



- 2. Create a service group for the TS Gateway farm.
 - Via Web GUI: Config Mode > Service > SLB > Service Group

Service Group					
Name: *	TSW-Farm				
Туре:	TCP	~			
Algorithm:	Round Robin	~			
Health Monitor:		~			
Min Active Members:	<u></u>				
	Send client reset who	en server selection fails			
Stats Data:		isabled			
Description:					
IPv4/IPv6:					
Server: *	TSW2	O Port: *	44	3	🔇 Add
Server Port Template(SPT):	default M Priority: 1			*	🥥 Update
Stats Data:	● Enabled				🤤 Delete
Server	Port	SPT	Priority	Stats Data	📀 Enable
🔲 🧭 TSW1	443	default	1	0	🕴 Disable
TSW2	443	default	1		and the second se

- Via CLI: AX(config)#slb service-group TSW-Farm tcp AX(config-slb svc group)#member TSW1:443 AX(config-slb svc group)#member TSW2:443
- 3. Create the virtual IP address (VIP), which is the IP address that clients will access.
 - a. Enter a name for the VIP, and enter the IP address.
 - Via Web GUI: Config Mode > Service > SLB > Virtual Server

General		
Name: *	TS	Wildcard
IP Address or CIDR Subnet: *	62.52.24.31	⑧ IPv4 ○ IPv6
Status:	Enabled Obsabled	

Via CLI: AX(config)#slb virtual-server TS 62.52.24.31



- b. Add the HTTPS port and select the service group.
- Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port

Virtual Server Port	
Name:	TS
Type: *	TCP
Port: *	443
Service Group:	TSW-Farm
Connection Limit:	8000000 Trop Reset Logging

- Via CLI: AX(config-slb vserver)#port 443 tcp AX2(config-slb vserver-vport)#service-group TSW-Farm
- 4. Configure persistence for TS Web access:
 - a. Create a source-IP persistence template. Only a name is required.
 - Via Web GUI: Config Mode > Service > Template > Persistent > Source IP Persistence

Source IP Persistence	
Name: *	srcip-persist
Match Type:	Port 💌

- Via CLI: AX(config)#slb template persist source-ip srcip-persist
- b. Assign the source-IP persistence template to the virtual server.
- Via Web GUI: Config Mode > Service > SLB > Virtual Server > Port

Course ID Descriptones Templater
Source in Persistence rempiate:

• Via CLI: AX(config)#slb virtual-server TS 62.52.24.31

AX(config-slb vserver)#port 443 tcp

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



AX VIP status

Display the status of the VIP and its members:

1. Via Web GUI: Config Mode > Service > SLB > Virtual Server

A Nama		Connections		Packets		Bytes			
	name	×	Current 🛛 🍦	Total 🏻 🍦	Forward 🛛 🍦	Reverse 🍦	Forward 🛛 🍦	Reverse 🍦	
\mathbf{O}	TS/62.52.24.31	Ε	0	0	0	0	0	0	1
0	TCP/443	Ξ	0	0	0	0	0	0	$\underline{\mathbb{N}}$
•	443 (TSW1)		0	0	0	0	0	0	
•	443 (TSW2)		0	0	0	0	0	0	

2. ViaCLI:AX#show slb virtual-server TS
 AX#show slb service-group TSW-Farm
 AX#show slb server [TSW1 | TSW2]

AX deployment validation

To validate the AX deployment:

- 1. Verify that clients can access the Terminal Servers using Web access via the VIP:
 - Launch Internet Explorer and connect to the TS Web Access servers.



· Validate that the client has access to the distributed applications.



Summary and Conclusion

The AX Series Advanced Traffic Manager provides Windows Server 2008 Terminal Services load balancing with:

- · High availability
- · High scalability
- High flexibility
- High performance
- High security

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



About A10 Networks

A10 Networks was founded in 2004 with a mission to provide innovative networking and security solutions. A10 Networks makes high-performance products that help organizations accelerate, optimize and secure their applications. A10 Networks is headquartered in Silicon Valley with offices in the United States, Europe, Japan, China, Korea and Taiwan. For more information, visit www.a10networks.com.

Performance by Design

To learn more about the AX Series Advanced Traffic Manager and how to improve application performance up to 8 times faster while enhancing reliability and security, visit A10 Networks' website at:

www.a10networks.com Or call and talk to an A10 sales representative:

Corporate Headquarters Asia Pacific Sales:

A10 Networks, Inc. 2309 Bering Drive San Jose, CA 95131 Tel: +1 408 325-8668 Fax: +1 408 325-8666

North America Sales:

+1 888 A10-6363 +1 408 325-8616

Europe, Middle East & Africa Sales:

+31 70 799-9143

China, Beijing Office:

+86 10 8515-0698

China, Shanghai Office: +86 21 6137-7850

Japan Sales: +81-3-3291-0091

Korea Office: +82-2-6007-2150 +82-2-6007-2151

Taiwan Office: +886-2-2657-3198



DG_terminal_072010

© 2010 A10 Networks, Inc. All rights reserved