

# VMware View 5.0 および Horizon View 6.0

## 目次

1	はじめに .....	2
2	VMware Horizon View/VMware View向けACOSのサポート .....	2
3	ラボ環境 .....	2
4	構成.....	3
4.1	VMware Viewの管理の構成.....	3
4.2	A10 ADCの基本的な構成.....	4
4.3	A10 ADCの高度な構成 .....	10
5	構成の確認.....	12
5.1	SSLオフロードなしの基本構成の確認.....	12
5.2	SSLオフロードありの高度な構成の確認.....	12
	添付資料A. A10 ADCの構成.....	14
	A10 Networks/A10ネットワークス株式会社について .....	15

## 免責事項

本文書はA10ネットワークスまたはその製品やサービスについて、特定の使用への適合性および他者の権利を侵害していないことを含め、明示的にも暗示的にも保証するものではありません。A10ネットワークスは本文書に含まれる情報の正確性を検証する妥当な努力はしていますが、その使用について一切責任を負いません。提供する情報はすべて「現在の状況」です。本文書に記載された製品の仕様および機能は入手可能な最新の情報に基づいています。ただし、仕様は通知せずに変更する可能性があり、特定の機能は最初の製品リリース時に利用できない可能性があります。製品とサービスに関する最新の情報については、A10ネットワークスまでお問い合わせください。A10ネットワークスの製品およびサービスには、A10ネットワークス標準の契約条件が適用されます。

## 1 はじめに

この構築ガイドでは、ハイパフォーマンスなアプリケーションデリバリーコントローラー (ADC) A10 Networks® Thunder™ および AX™ シリーズ (以下、総称して「A10 ADC」と表記) を、VMware View 5.0 (または VMware Horizon View 6.0) をサポートするよう構成する手順について説明しています。

VMware View は、IT の管理と制御を簡略化し、あらゆるデバイスおよびネットワークで期待通りの最高のエンドユーザーエクスペリエンスを提供する、デスクトップ仮想化ソリューションです。

VMware View 5.0 と Horizon View 6.0 の詳細については、次の Web ページをご覧ください：

<http://www.vmware.com/jp/products/horizon-view>

A10 ADC は、A10 ネットワークスの Advanced Core Operating System (ACOS®) プラットフォームをベースに構築され、VMware View などのアプリケーションのために特に設計された製品であり、VMware View サーバーにおけるフェイルオーバー時のより確実な対応、セキュリティ処理のオフロード、そしてインテリジェントな負荷分散を実行します。

### 1.1 ACOS の前提条件

本ソリューションの前提条件は以下のとおりです。

- ユーザーが A10 ADC と VMware View の構成について基本的な知識を備えている。
- さまざまな VMware View サーバーがすでにインストールされて正常に動作している。
- A10 ADC で ACOS リリース 2.6 以上が使用されている。

検証に使用した製品およびバージョン：

- A10 ADC : ACOS バージョン 2.6.1-GR1
- VMware View : バージョン 5.0 および Horizon View 6.0

注：本構築ガイドにおける GUI 画面イメージ、GUI 操作手順は ACOS リリース 2.7 以降のものとは異なる場合があります。

## 2 VMware Horizon View/VMware View 向け ACOS のサポート

A10 ADC は VMware View を完全にサポートしており、以下の利点を提供します。

- VMware Connection Server のロードバランシングと高可用性
- プライベートネットワーク内での VMware Connection Server の使用 (外部からの直接アクセスは不可)

また、A10 ADC は、VMware Connection Server での SSL オフロードという追加の利点も提供します。

## 3 ラボ環境

A10 ADC と VMware View 5.0 の構成には、以下のラボ環境が使用されました。

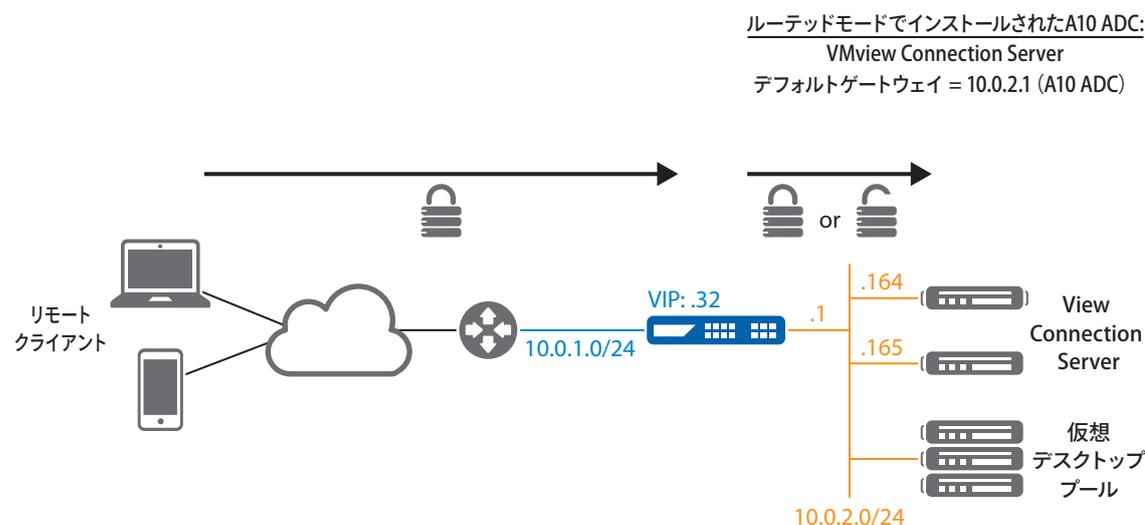


図 1: VMware View 5.0 の構築ラボ

## 4 構成

ここでは、図1で示したVMware View / A10 ADC環境を構成する方法について説明します。

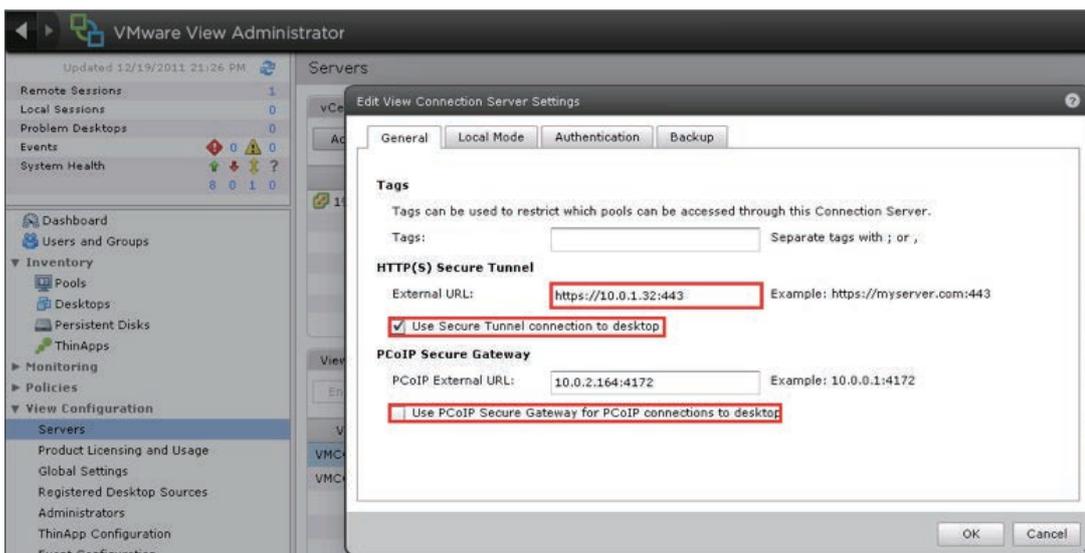
### 4.1 VMware Viewの管理の構成

VMware View Clientはデスクトップにアクセスするため、暗号化されたUDPプロトコルを使用するPC-over-IP (PCoIP)か、SSLを使って暗号化されるRemote Desktop Protocol (RDP)を使用します。

- RDPアクセスの場合、A10 ADCはSSLオフロードにより、サーバーをSSL暗号化の実行という負担から解放できます。
- PCoIPアクセスの場合、A10 ADCはSSLオフロードに対応していないため、UDP暗号化の実行という負担からサーバーを解放することはできません。エンドユーザーのデスクトップアクセスにPCoIPを使用する場合は、PCoIPがデスクトップに直接接続できるようにするため、A10 ADCのデバイスをバイパスすることをお勧めします。

#### 4.1.1 VMware View Administratorの更新

- RDPアクセスでView ClientがA10 ADCのVIPを介してアクセスするように設定する（SSLオフロードを提供するために必要）
  - PCoIPアクセスでView Clientがデスクトップサーバーに直接アクセスするように設定する
1. VMware View Administratorにログオンします。
  2. [View Configuration] > [Servers] > [View Connection Servers]へ移動します。
  3. [External URL]をA10 ADCのVIP IPアドレスまたはFQDN DNS名に変更します。
  4. [Use PCoIP Secure Gateway for PCoIP connections to desktop]の選択を解除します。



注: すべてのView Connection Serverについて、上記の手順を繰り返してください。

## 4.2 A10 ADCの基本的な構成

### 4.2.1 View Connection Serverの作成

各View Connection Serverに対してリアルサーバーを作成します。作成するサーバーの名前とIPアドレスを入力し、TCPプロトコルのポート443を追加します。

- Web GUIを使用する場合: [Config Mode] > [Service] > [SLB] > [Server]

General	
Name: *	VMConn1
IP Address/Host: *	10.0.2.164 <input type="radio"/> IPv4 <input type="radio"/> IPv6
GSLB External IP Address:	
Weight:	1
Health Monitor:	(default)

Port	
Port: *	443
Protocol:	TCP
Weight(W): *	1
<input type="checkbox"/> No SSL	
Connection Limit(CL):	8000000 <input checked="" type="checkbox"/> Logging
Connection Resume(CR):	
Server Port Template(SPT):	default
Stats Data(SD):	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Health Monitor(HM):	<input checked="" type="radio"/> (default) <input type="radio"/> Follow Port: <input type="text"/> TCP
Extended Stats(ES):	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled

<input type="checkbox"/>	Port	Protocol	CL	CR	W	No SSL	SPT	HM	SD	ES
<input checked="" type="checkbox"/>	443	TCP	8000000	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	default	(default)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

- CLIを使用する場合:

```
AX(config)#slb server VMConn1 10.0.2.164
```

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

注: A10 ADCはデフォルトで、pingとTCPハンドシェイクを使用してサーバーのテストを行います。View Connection ServerのWindowsファイアウォールがAXデバイスからのpingを許可するように設定しておく必要があります。許可しない場合は、後述のように、pingによるデフォルトのサーバーヘルスチェックを無効にしてください。

- Web GUIを使用する場合: [Config Mode] > [Service] > [SLB] > [Server]

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

- CLIを使用する場合:

```
AX(config)#slb server VMConn1 10.0.2.164
```

```
AX(config-real server)#no health-check
```

### 4.2.2 View Connection Serverのヘルスチェックの作成

View Connection Serverの可用性をテストするため、ヘルスマニターテンプレートを作成します。ヘルスマニターテンプレートの名前を入力し、タイプとして[HTTPS]を選択し、URLとして「GET /」を選択します。

- Web GUIを使用する場合: [Config Mode] > [Service] > [Health Monitor]

Health Monitor	
Name: *	hm-ViewConn-https
Retry:	3
Method:	<input checked="" type="radio"/> Internal <input type="radio"/> External
Type:	HTTPS
Port:	443
Host:	
URL:	GET /

- CLIを使用する場合:

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

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

#### 4.23 View Connection Server グループの作成

View Connection Server用のTCP サービスグループを作成します。サービスグループの**名前**を入力した後、[Type]ドロップダウンリストから[TCP]を選択し、ロードバランシング**アルゴリズム**として[Least Connection]を選択して、View Connection Serverの**ヘルスマニター**を選択します。各View Connection Serverを、このサービスグループにポート**443**で割り当ててください。

- Web GUIを使用する場合: [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:	<input type="checkbox"/>

Server																			
IPv4/IPv6:	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6																		
Server: *	VMConn2																		
Server Port Template(SPT):	default																		
Port: *	443																		
Priority:	1																		
Stats Data:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled																		
<table border="1"> <thead> <tr> <th></th> <th>Server</th> <th>Port</th> <th>SPT</th> <th>Priority</th> <th>Stats Data</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>VMConn1</td> <td>443</td> <td>default</td> <td>1</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input type="checkbox"/></td> <td>VMConn2</td> <td>443</td> <td>default</td> <td>1</td> <td><input checked="" type="checkbox"/></td> </tr> </tbody> </table>			Server	Port	SPT	Priority	Stats Data	<input type="checkbox"/>	VMConn1	443	default	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	VMConn2	443	default	1	<input checked="" type="checkbox"/>
	Server	Port	SPT	Priority	Stats Data														
<input type="checkbox"/>	VMConn1	443	default	1	<input checked="" type="checkbox"/>														
<input type="checkbox"/>	VMConn2	443	default	1	<input checked="" type="checkbox"/>														

- CLIを使用する場合:

```
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
```

#### 4.24 View Connection のパーシステンスの作成

複数のエンドユーザーが同じIPアドレスを共有することができます(たとえば同じプロキシ/ファイアウォールの背後にいるユーザー間で)。したがって、ソースIPアドレスに基づくパーシステンスは使用可能ではありますが、View Connection Server間での負荷分散が不均一になる可能性があります。

View Connection Serverは、ユーザーを追跡するためにCookie (JSESSIONID)を使用します。A10 ADCはこのCookie情報を使用してパーシステンスを提供できるため(aFlex®を使用)、均一な負荷分散を実現できます。

#### 4.25 View のパーシステンスルールを定義する aFLEX ポリシーの作成

作成するaFlexポリシーは以下のとおりです。

```
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]
  }
}
```

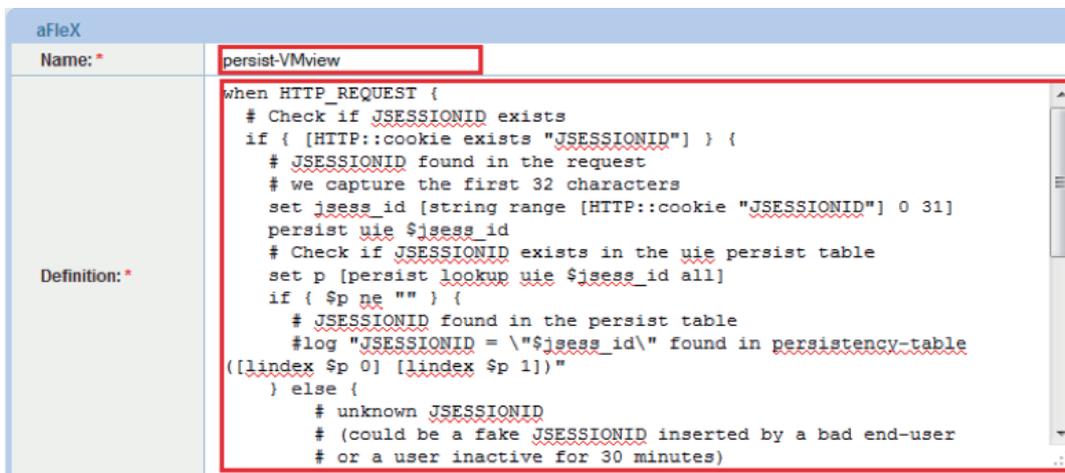
```

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\""
    }
}
}

```

- Web GUIを使用する場合: [Config Mode] > [Service] > [aFleX]



- CLIを使用する場合:  
AX(config)#import aflex persist-VMview tftp://10.0.1.10/persist-VMview.txt

## 4.26 AX SSL 構成の作成

View Connection Server の公開証明書 / 秘密鍵を A10 ADC デバイスにインポートします。

注: VMware View Administrator に対して、View Connection Server で使用する証明書と鍵を要求してください。テスト用には、A10 ADC の自己署名証明書 / 鍵を使用することもできますが、その場合は信頼されていない自己署名証明書を受け入れるために、View Client に警告メッセージが表示されます。



IIS パブリック証明書 / 秘密鍵を A10 ADC のデバイスにインポートします。証明書の **名前** を入力し、インポート方法 ([Local] または [Remote]) を選択して、**形式** を選択します。ダウンロード設定を入力します (この設定はインポート方法として [Local] と [Remote] のどちらを選択したかによって異なります)。

- Web GUI を使用する場合: [Config Mode] > [Service] > [SSL Management] > [Certificate]

Import	
Name: *	View-cert
Import Certificate from:	<input checked="" type="radio"/> Local <input type="radio"/> Remote <input type="radio"/> Text
Certificate Format:	PEM
Certificate Source:	C:\Temp\View.cer Browse...
Import Key from:	<input checked="" type="radio"/> Local <input type="radio"/> Remote <input type="radio"/> Text
Private Key Source:	C:\Temp\View.key Browse...

- CLI を使用する場合:  

```
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
```

クライアント SSL テンプレートを作成します。テンプレートの名前を入力し、証明書と鍵のファイルを選択します。

- Web GUI を使用する場合: [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:	

- CLI を使用する場合:  

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

サーバー SSL テンプレートを作成します。テンプレートの名前を入力します。

- Web GUI を使用する場合: [Config Mode] > [Service] > [SSL] > [Server SSL]

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

- CLI を使用する場合:  
AX(config)#slb template server-ssl View-Server-Side

#### 4.27 View Connection VIP の作成

エンドユーザーがアクセスする IP アドレスとなる仮想 IP アドレス (VIP) を作成します。VIP の名前を入力し、IP アドレスを入力します。

- Web GUI を使用する場合: [Config Mode] > [Service] > [SLB] > [Virtual Server]

General	
Name: *	VIP-Conn <input type="checkbox"/> Wildcard
IP Address or CIDR Subnet: *	10.0.1.32 <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Status:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled

- CLI を使用する場合:  
AX(config)#slb virtual-server VIP-Conn 10.0.1.32

ポートのタイプとして HTTPS、ポート番号として 443 を指定して、サービスグループ、クライアント SSL テンプレート、サーバー SSL テンプレート、および aFlex を選択します。

- Web GUI を使用する場合: [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:	<input type="checkbox"/> 8000000 <input checked="" type="radio"/> Drop <input type="radio"/> Reset <input checked="" type="checkbox"/> Logging

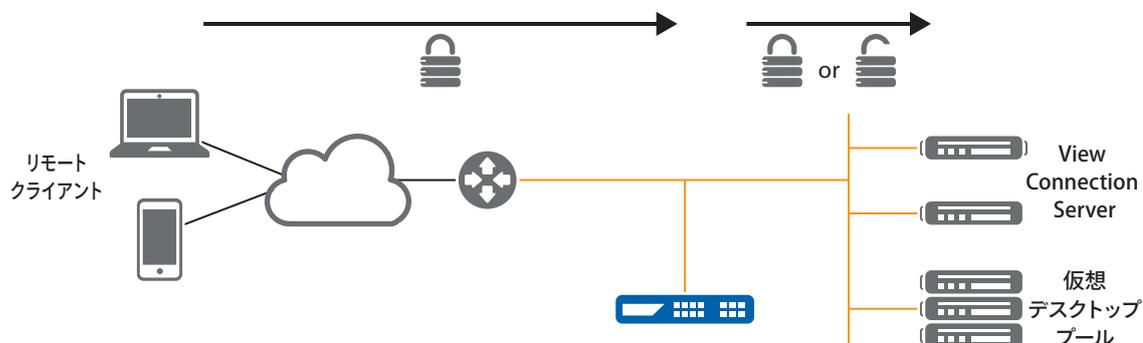
  

aFlex:	persist-VMview <input type="checkbox"/> Multiple
HTTP Template:	
RAM Caching Template:	
Client-SSL Template:	View-Client-Side
Server-SSL Template:	View-Server-Side

- CLI を使用する場合:  
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

## 4.28 A10 ADCのワンアームでの統合(オプション)

ワンアームモードでインストールされたA10 ADC:  
VMview Connection Server  
デフォルトゲートウェイ = ルーター (A10 ADC以外)



ワンアーム構成 (A10 ADCがワンアーム接続されていて、サーバーのデフォルトゲートウェイがA10 ADCではない構成) では、IP ソース NAT (SNAT) を構成する必要があります。

1. SNAT IPv4 プールを作成します。名前、開始IPアドレス、終了IPアドレス、およびネットマスクを入力します。  
– Web GUIを使用する場合: [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:	

- CLIを使用する場合:  
`AX(config)#ip nat pool snat 10.0.2.35 10.0.2.36 netmask /24`
2. View Connection ServerのVIPで、ソースNATプールを選択します。  
– Web GUIを使用する場合: [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 https |`  
`AX(config-slb vserver-vport)#source-nat pool snat-view`

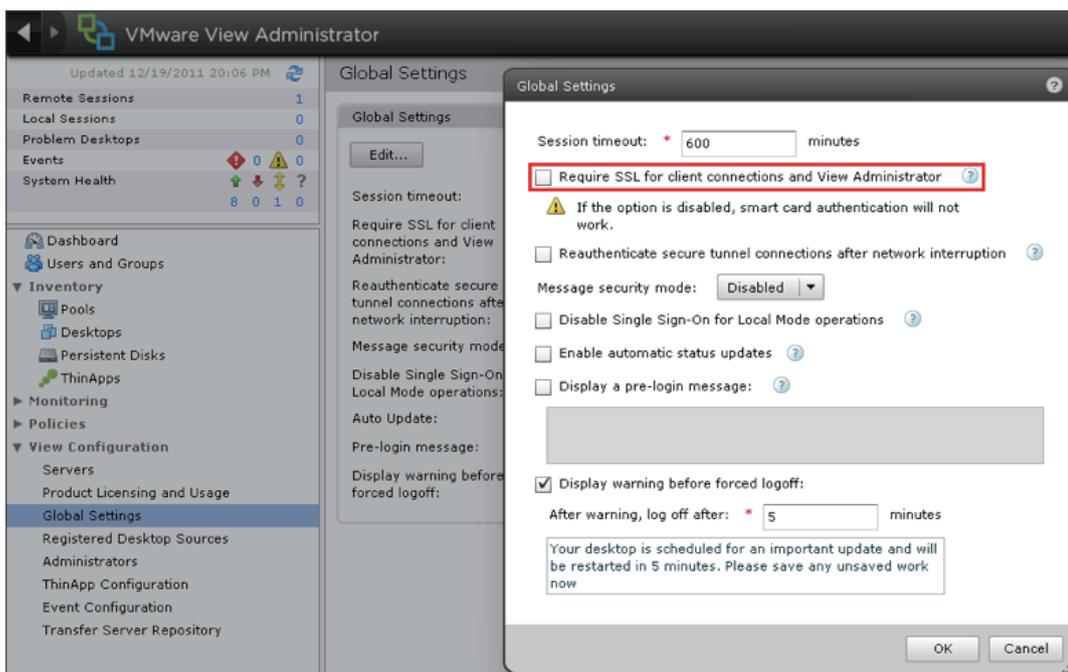
## 4.3 A10 ADCの高度な構成

### 4.31 View Connection ServerからA10 ADCへのSSLオフロード

このオプションを使用しても、エンドユーザーはHTTPSを使ってView Connection Serverに接続することになります。A10 ADCがHTTPを使ってView Connection Serverに接続することにより、CPUを集中的に使用するSSL処理がサーバーからA10 ADCへとオフロードされます。

A10 ADCの構成を始める前に、HTTPでのアクセスができるようにVMware View Administratorの構成を更新してください。

1. VMware View Administratorにログオンします。
2. [View Configuration] > [Global Settings]へ移動します。
3. [Require SSL for client connections and View Administrator]の選択を解除します。



4. 各View Connection Serverについて、それぞれポート80を作成します。
  - Web GUIを使用する場合: [Config Mode] > [Service] > [SLB] > [Server]
  - CLIを使用する場合:  
`AX(config)#slb server VMConn1 10.0.2.164`  
`AX(config-real server)#port 80 tcp`
5. View Connection Serverの可用性をテストするために、ヘルスマニターテンプレートを作成します。ヘルスマニターテンプレートの名前を入力し、タイプとして[HTTP]を選択し、URLとして「GET /」を選択します。
  - Web GUIを使用する場合: [Config Mode] > [Service] > [Health Monitor]

Health Monitor	
Name: *	hm-ViewConn-http
Retry:	3
Method:	<input checked="" type="radio"/> Internal <input type="radio"/> External
Type:	HTTP
Port:	80
Host:	
URL:	GET /

- CLIを使用する場合:

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

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

- View Connection Server用のTCPサービスグループを作成します。サービスグループの**名前**を入力した後、**[Type]**ドロップダウンリストから[TCP]を選択し、ロードバランシング**アルゴリズム**として[Least Connection]を選択して、View Connection Serverの**ヘルスマニター**を選択します。各View Connection Serverを、このサービスグループにポート80で割り当ててください。

- Web GUIを使用する場合: [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:	<input type="checkbox"/>

Server																			
IPv4/IPv6:	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6																		
Server: *	<input type="text"/>																		
Server Port Template(SPT):	default																		
Port: *	<input type="text"/>																		
Priority:	1																		
Stats Data:	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled																		
	<table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>Server</th> <th>Port</th> <th>SPT</th> <th>Priority</th> <th>Stats Data</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/></td> <td>VMConn1</td> <td>80</td> <td>default</td> <td>1</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td>VMConn2</td> <td>80</td> <td>default</td> <td>1</td> <td><input checked="" type="checkbox"/></td> </tr> </tbody> </table>	<input type="checkbox"/>	Server	Port	SPT	Priority	Stats Data	<input checked="" type="checkbox"/>	VMConn1	80	default	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	VMConn2	80	default	1	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Server	Port	SPT	Priority	Stats Data														
<input checked="" type="checkbox"/>	VMConn1	80	default	1	<input checked="" type="checkbox"/>														
<input checked="" type="checkbox"/>	VMConn2	80	default	1	<input checked="" type="checkbox"/>														

- CLIを使用する場合:

```
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
```

- View Connection ServerのVIPで、HTTPサーバーのサービスグループを選択し、

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

サーバー SSLテンプレートを削除します。これは、AXデバイスがHTTPSではなくHTTPを使用してConnection View Serverと通信することになるためです。

- Web GUIを使用する場合: [Config Mode] > [Service] > [SLB] > [Virtual Server Port]

- CLIを使用する場合:

```
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 構成の確認

### 5.1 SSL オフロードなしの基本構成の確認

VIPのステータスと、そのメンバーが稼働中であることを確認します。

- Web GUIを使用する場合: [Monitor Mode] > [Service] > [SLB] > [Virtual Server]

	Name	Connections		Packets		Bytes	
		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

- CLIを使用する場合:
 

```
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
```

VMware View ClientでのVMware View サービスへのアクセスを確認します。

VMware View を起動してVIPに接続します。



### 5.2 SSL オフロードありの高度な構成の確認

VIPのステータスと、そのメンバーが稼働中であることを確認します。

- Web GUIを使用する場合: [Monitor Mode] > [Service] > [SLB] > [Virtual Server]

	Name	Connections		Packets		Bytes	
		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

- CLIを使用する場合:
 

```
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
```

VMware View ClientでのVMware View サービスへのアクセスを確認します。

VMware View を起動してVIP に接続します。



## 添付資料 A. A10 ADCの構成

以下の構成には次のオプションが含まれています。

- SSL オフロード
- SNAT なし (A10 ADC がルーテッドモードでインストールされている)

```
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
```

## A10 Networks/A10ネットワークス株式会社について

A10 Networks (NYSE: ATEN) はアプリケーションネットワーク分野におけるリーダーとして、高性能なアプリケーションネットワークソリューション群を提供しています。世界中で数千社にのぼる大企業やサービスプロバイダー、大規模Webプロバイダーといったお客様のデータセンターに導入され、アプリケーションとネットワークを高速化し安全性を確保しています。A10 Networksは2004年に設立されました。米国カリフォルニア州サンノゼに本拠地を置き、世界各国の拠点からお客様をサポートしています。

A10 ネットワークス株式会社は台湾・東南アジア各国を含む地域統括をおこなうA10 Networksの日本子会社であり、各地域のお客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワークソリューションをご提供することを使命としています。

詳しくはホームページをご覧ください。

[www.a10networks.co.jp](http://www.a10networks.co.jp)

Facebook : <http://www.facebook.com/A10networksjapan>

### A10ネットワークス株式会社

〒105-0001  
東京都港区虎ノ門 4-3-20  
神谷町MTビル 16階  
TEL : 03-5777-1995  
FAX: 03-5777-1997  
[jinfo@a10networks.com](mailto:jinfo@a10networks.com)  
[www.a10networks.co.jp](http://www.a10networks.co.jp)

### 海外拠点

#### 北米 (A10 Networks本社)

[sales@a10networks.com](mailto:sales@a10networks.com)

#### ヨーロッパ

[emea\\_sales@a10networks.com](mailto:emea_sales@a10networks.com)

#### 南米

[latam\\_sales@a10networks.com](mailto:latam_sales@a10networks.com)

#### 中国

[china\\_sales@a10networks.com](mailto:china_sales@a10networks.com)

#### 香港

[HongKong@a10networks.com](mailto:HongKong@a10networks.com)

#### 台湾

[taiwan@a10networks.com](mailto:taiwan@a10networks.com)

#### 韓国

[korea@a10networks.com](mailto:korea@a10networks.com)

#### 南アジア

[SouthAsia@a10networks.com](mailto:SouthAsia@a10networks.com)

#### オーストラリア/ニュージーランド

[anz\\_sales@a10networks.com](mailto:anz_sales@a10networks.com)

お客様のビジネスを強化するA10のアプリケーションサービスゲートウェイ、Thunderの詳細は、A10ネットワークスのWebサイト[www.a10networks.co.jp](http://www.a10networks.co.jp)をご覧ください。A10の営業担当者にご連絡ください。

Part Number: A10-DG-16119-JA-01

August 2014

©2014 A10 Networks, Inc. All rights reserved. A10 Networks, A10 Networksのロゴ, A10 Thunder, Thunder, vThunder, aCloud, ACOS, aGalaxyはA10 Networks, Inc.の米国ならびに他の国における登録商標です。その他の商標はそれぞれの所有者の資産です。A10 Networksは本書の誤りに関して責任を負いません。A10 Networksは、予告なく本書を変更、修正、譲渡、および改訂する権利を留保します。製品の仕様や機能は、変更する場合がございますので、ご注意ください。