VMware View 5.0 および Horizon View 6.0

目次

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。

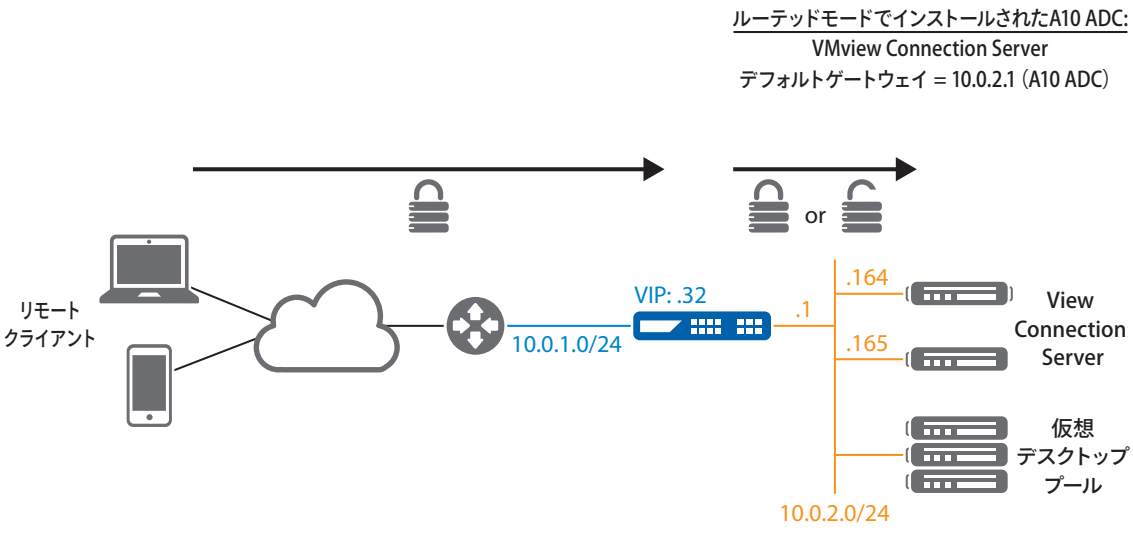


図 1: VMware View 5.0 の構築ラボ

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

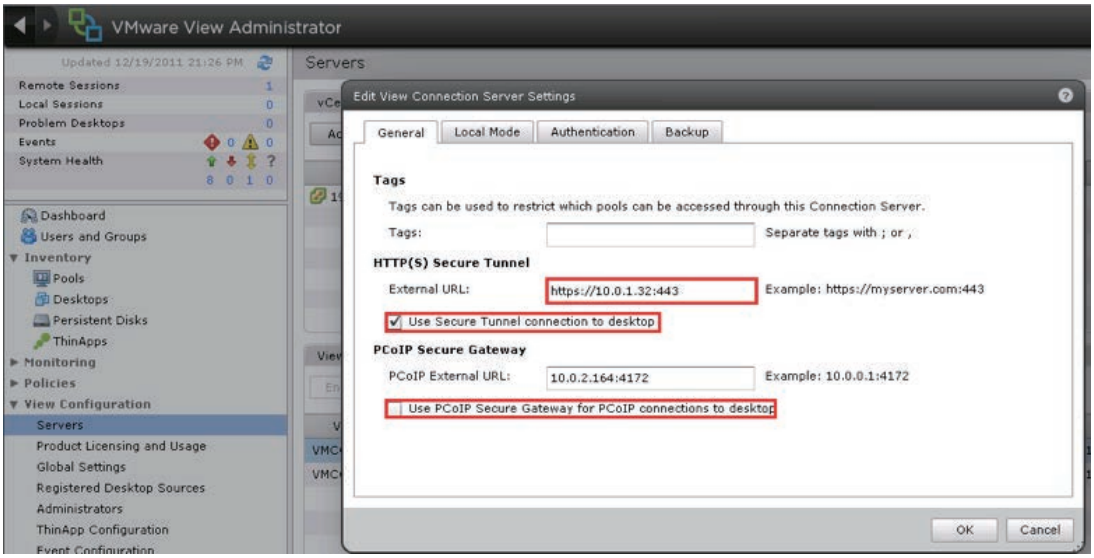
VMware View Client はデスクトップにアクセスするため、暗号化された UDP プロトコルを使用する PC-over-IP（PCoIP）か、SSL を使って暗号化される Remote Desktop Protocol（RDP）を使用します。

- 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。

4.11 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。



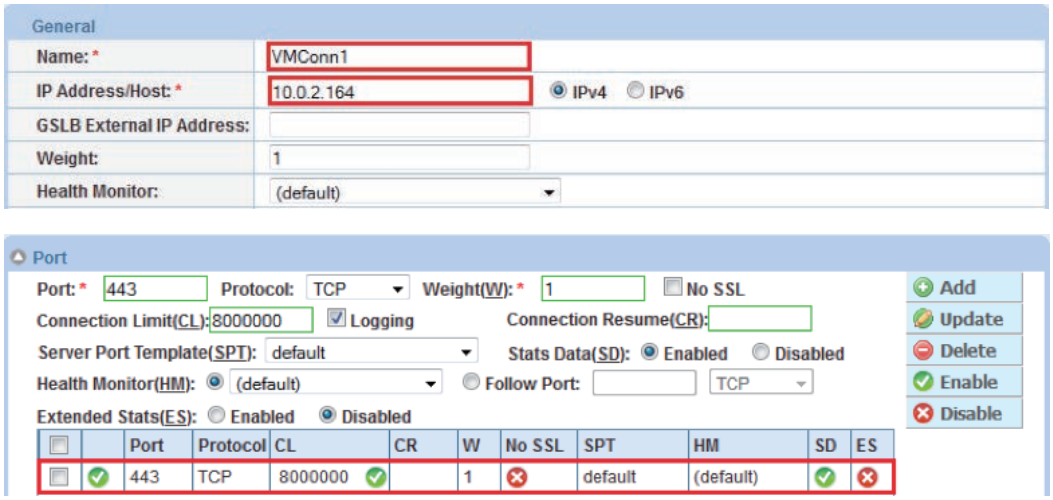
注： すべての View Connection Server について、上記の手順を繰り返してください。

4.2 A10 ADC の基本的な構成

4.21 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]



- 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 ハンドシェー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]

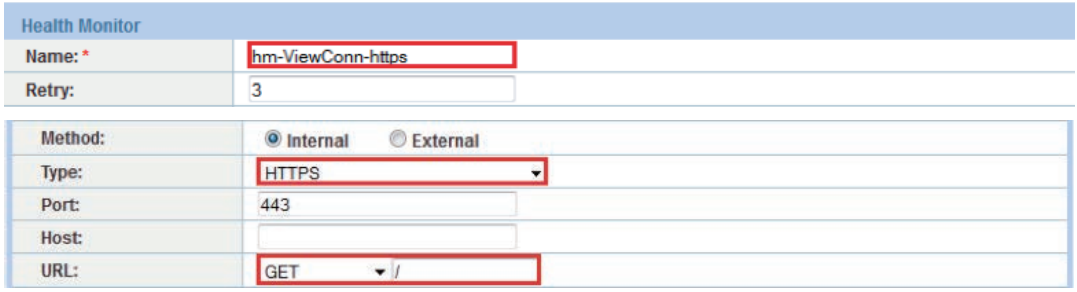
- CLI を使用する場合 :

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

4.22 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、ヘルスモニターテンプレートを作成します。ヘルスモ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]



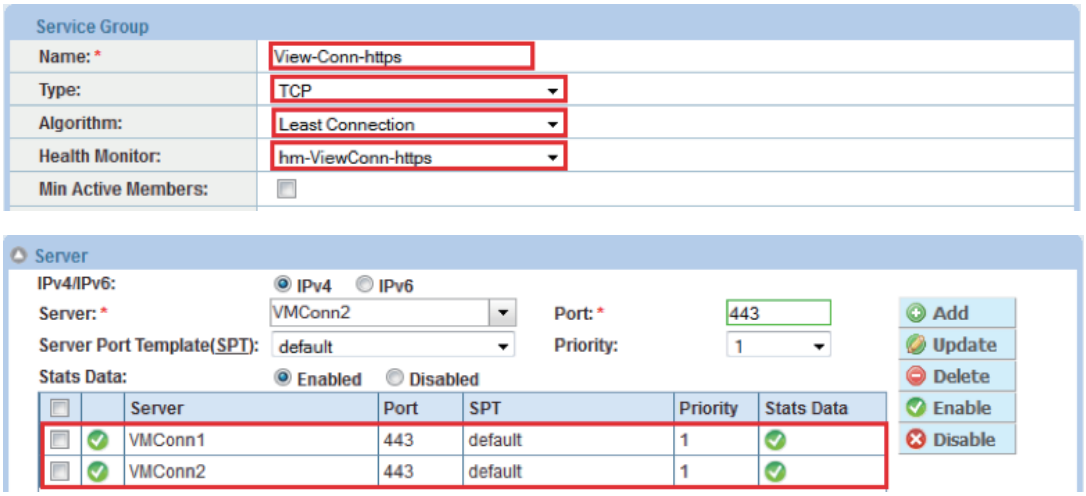
- CLI を使用する場合：

```
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**ヘルスモニター**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]



- 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ー / 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

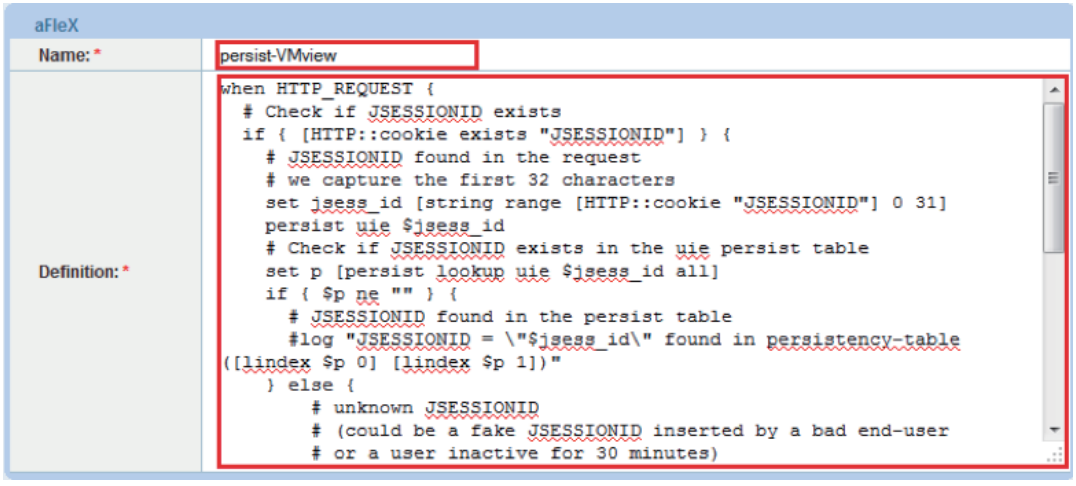
作成する aFleX ポリシーは以下のとおりです。

```
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]



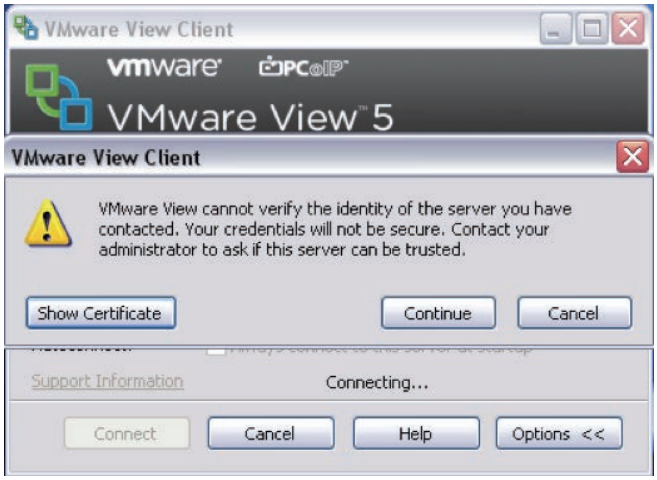
- CLI を使用する場合 :

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

4.26 AX SSL 構成の作成

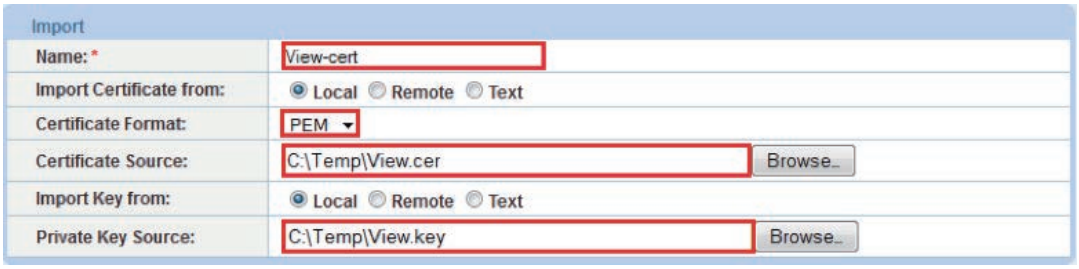
View Connection Server の公開証明書 / 秘密鍵を A10 ADC デバイスにインポートします。

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]

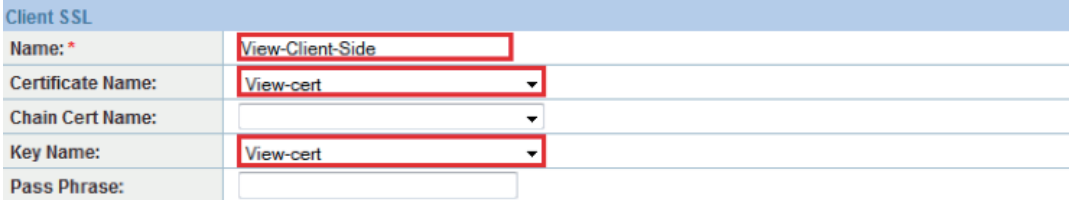


- CLI を使用する場合 :

```
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]

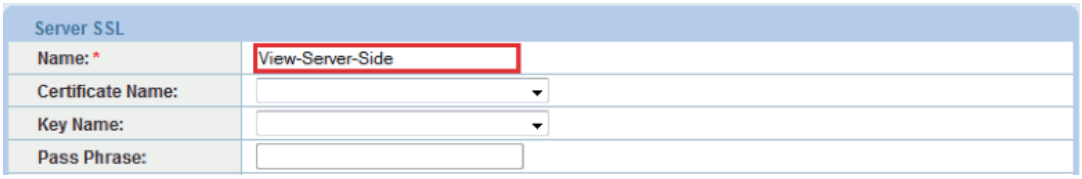


- CLI を使用する場合 :

```
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]



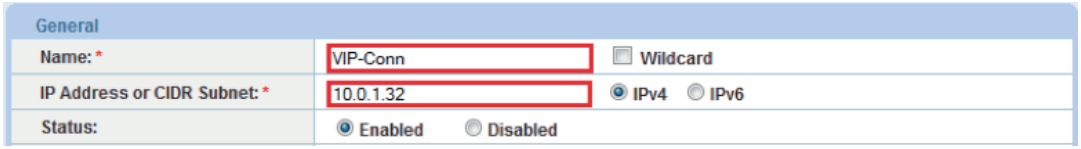
- CLI を使用する場合：

```
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]

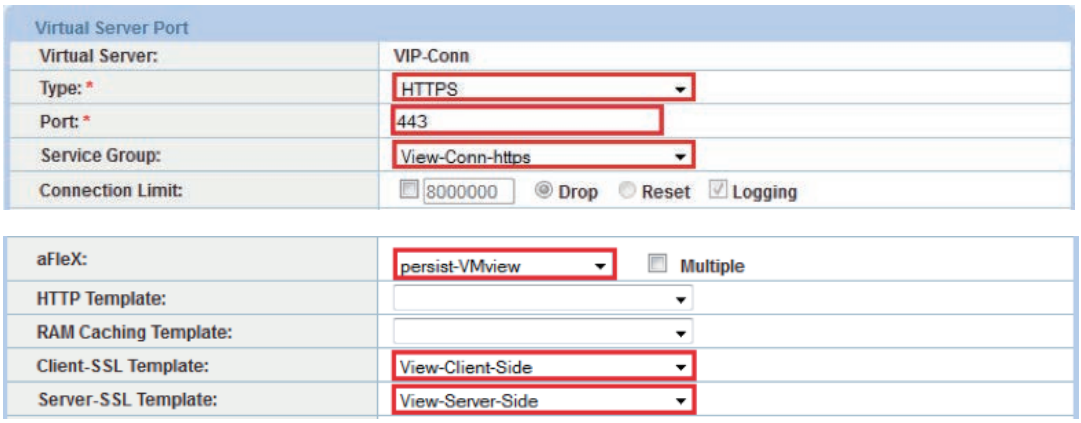


- CLI を使用する場合：

```
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。

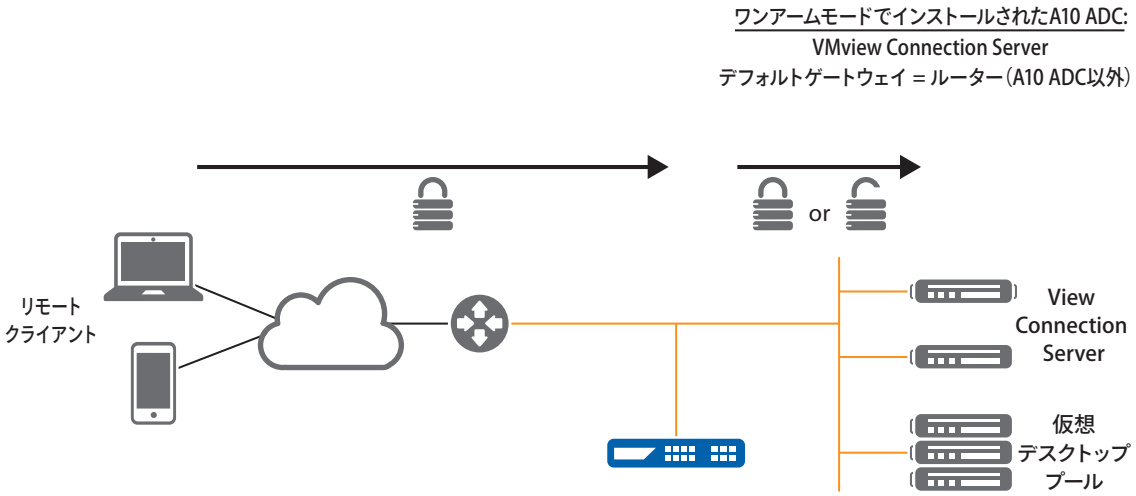
- Web GUI を使用する場合：[Config Mode] > [Service] > [SLB] > [Virtual Server] > [Port]



- CLI を使用する場合：

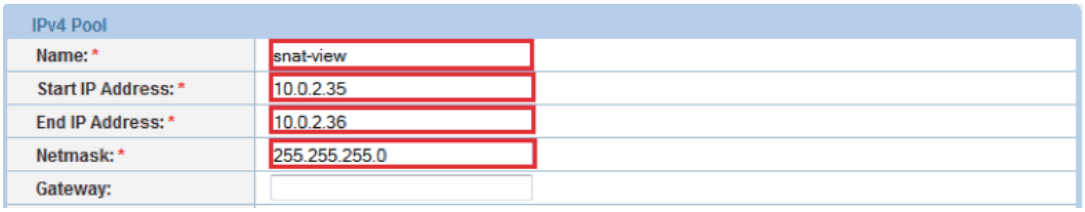
```
AX(config)#port 443 https
AX(config-slb vserver-vport)#service-group View-Conn-https
AX(config-slb vserver-vport)#template client-ssl View-Client-Side
AX(config-slb vserver-vport)#template server-ssl View-Server-Side
AX(config-slb vserver-vport)#aflex persist-VMview
```

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]



- 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]

- 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`

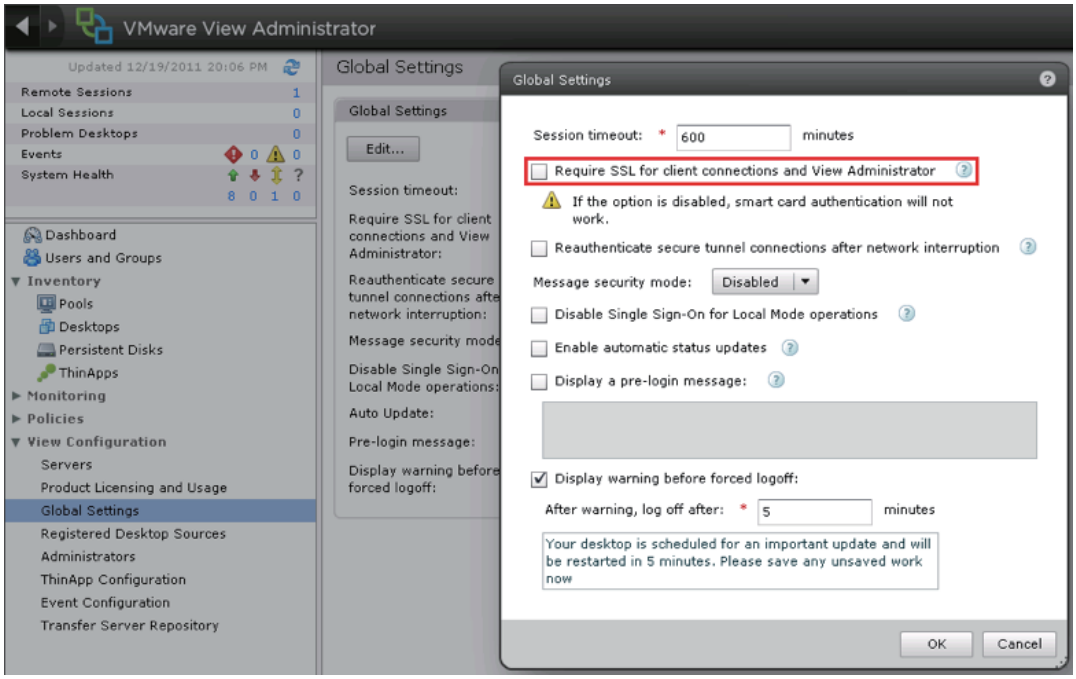
4.3 A10 ADC の高度な構成

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。

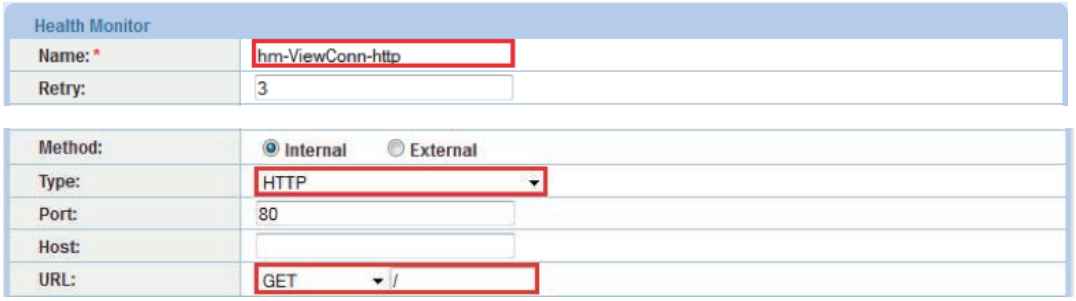
1. VMware View Administrator にログオンします。
2. [View Configuration] > [Global Settings] へ移動します。
3. **[Require SSL for client connections and View Administrator]** の選択を解除します。



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、ヘルスモニターテンプレートを作成します。ヘルスモ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]

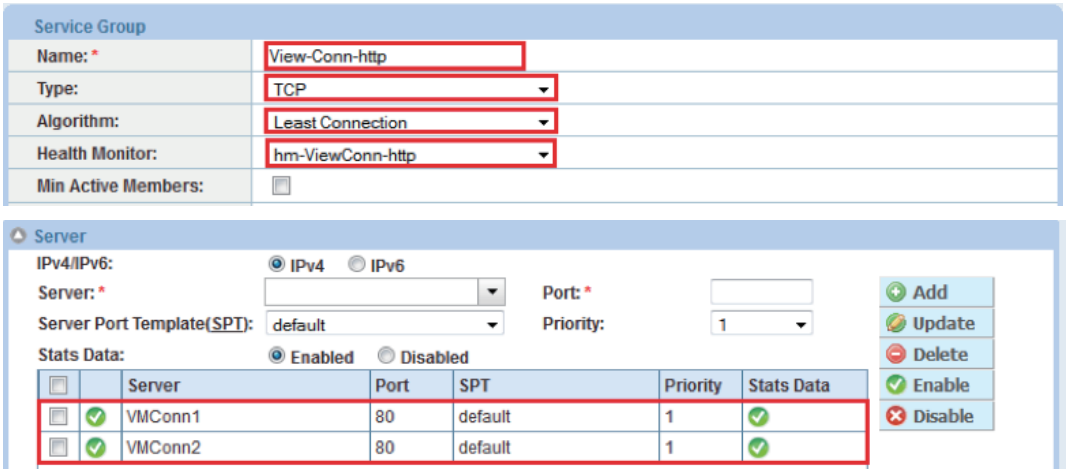


- CLI を使用する場合:

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

6. 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**ヘルスモニター**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]



- 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
```

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

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キング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キング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キング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
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
www.a10networks.co.jp

海外拠点

北米（A10 Networks本社）
sales@a10networks.com
ヨーロッパ
emea_sales@a10networks.com
南米
latam_sales@a10networks.com
中国
china_sales@a10networks.com
香港
HongKong@a10networks.com
台湾
taiwan@a10networks.com
韓国
korea@a10networks.com
南アジア
SouthAsia@a10networks.com
オーストラリア/ニュージーランド
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**をご覧になるか、A10の営業担当者にご連絡ください。

Part Number: A10-DG-16119-JA-01
August 2014