



目次

1.	はじめに3
2.	構築ガイドの概要
3.	本書の前提条件
4.	SharePoint 2010 のための AX 構築におけるサーバーの役割4
5.	AX シリーズロードバランサーへのアクセス5
6.	SharePoint 2010 の推奨インストール手順5
7.	アーキテクチャーの概要6
8.	SharePoint のための基本的な AX 構成7
8.1	サーバーの構成7
8.2	ヘルスモニターの構成9
8.3	サービスグループの構成10
8.4	バーチャルサーバー11
8.5	IP ソースパーシステンス13
8.6	IP ソース NAT
9.	サービスの確認16
10.	SharePoint のための AX の高度な機能17
10.1	構成の準備17
10.2	サービスグループのポート番号の変更18
10.3	バーチャルポートのサービスタイプの変更18
11.	SSLオフロード19
11.1	証明書のインポートまたは作成20
11.2	オプション1 : AX から自己署名 CA を作成する20
11.3	オプション2 : SSL証明書と鍵のインポート21
11.4	クライアント SSL テンプレートの構成と適用22
11.5	配備の確認23

12.	圧縮	24
12.1	HTTP 圧縮テンプレートの作成	24
12.2	VIP への HTTP 圧縮テンプレートの適用	25
12.3	配備の確認	26
13.	Cookie パーシステンス	27
13.1	COokie パーシステンステンプレートの作成	27
13.2	VIP への Cookie パーシステンステンプレートの適用	27
13.3	配備の確認	28
14.	コネクションリユース(TCP オフロード)	28
14.1	コネクションリユーステンプレートの作成	29
14.2	VIP へのコネクションリユースの適用	30
14.3	配備の確認	30
14.3 15.	配備の確認 RAM キャッシング	30 31
14.3 15. 15.1	配備の確認 RAM キャッシング RAM キャッシングテンプレートの作成	30 31 31
14.3 15. 15.1 15.2	配備の確認 RAM キャッシング RAM キャッシングテンプレートの作成 VIP への RAM キャッシングテンプレートの適用	30 31 31 32
14.3 15. 15.1 15.2 15.3	配備の確認 RAM キャッシング RAM キャッシングテンプレートの作成 VIP への RAM キャッシングテンプレートの適用 配備の確認.	30 31 31 32 33
 14.3 15.1 15.2 15.3 16. 	配備の確認 RAM キャッシング RAM キャッシングテンプレートの作成 VIP への RAM キャッシングテンプレートの適用 配備の確認. aFleX による SharePoint の保護	30 31 31 32 33 33
 14.3 15.1 15.2 15.3 16. 16.1 	配備の確認 RAM キャッシング RAM キャッシングテンプレートの作成 VIP への RAM キャッシングテンプレートの適用 配備の確認 aFleX による SharePoint の保護 Aflex スクリプトの定義	30 31 31 32 33 33 33
 14.3 15.1 15.2 15.3 16. 16.1 16.2 	配備の確認 RAM キャッシング RAM キャッシングテンプレートの作成 VIP への RAM キャッシングテンプレートの適用 配備の確認 aFleX による SharePoint の保護 Aflex スクリプトの定義 VIP への AFLEX スクリプトの適用	30 31 32 33 33 34 34
 14.3 15.1 15.2 15.3 16. 16.1 16.2 16.3 	配備の確認 RAM キャッシング RAM キャッシングテンプレートの作成 VIP への RAM キャッシングテンプレートの適用 配備の確認 aFleX による SharePoint の保護 Aflex スクリプトの定義 VIP への AFLEX スクリプトの適用 AFLEX サービスの確認.	 30 31 32 33 33 34 34 35
 14.3 15.1 15.2 15.3 16.1 16.2 16.3 17. 	配備の確認 RAM キャッシング RAM キャッシングテンプレートの作成 VIP への RAM キャッシングテンプレートの適用 配備の確認 aFleX による SharePoint の保護 Aflex スクリプトの定義 VIP への AFLEX スクリプトの適用 AFLEX サービスの確認 まとめと結論	 30 31 32 33 33 34 34 35 36

1. はじめに

Microsoft が開発した Microsoft SharePoint 2010 は、中小企業から大企業まで利用可能な最先端 の Web アプリケーションプラットフォームです。Microsoft SharePoint 2010 は、コラボレーシ ョン、コンテンツ、およびファイルを一元管理するアプリケーションソフトウェアです。オーデ ィオ、ビデオ、Silverlight アプリケーションなどをサポートするさまざまな機能があり、ユー ザーは動的な Web サイトを容易に構築できます。また、SharePoint 2010 の新しいリボンユーザ インタフェースを使うことで、配備、管理、カスタマイズをより一層簡単に行えます。それに加 えて現在は、配備を容易にするために、wiki からワークフローに至るまでさまざまなテンプレー トが用意されています。何千もの顧客をサポート可能な拡張性の高いソリューションである SharePoint は、複数サーバーの環境への導入が可能です。AX シリーズの ADC (Application Delivery Controllers:アプリケーション配信コントローラー)は、Microsoft SharePoint 2010 に高 度なロードバランシングサービスを提供します。

2. 構築ガイドの概要

本書では、Microsoft SharePoint 2010 と共に A10 ネットワークス AX シリーズデバイスを配備す る方法について説明します。このソリューションのテストは、2 台の SharePoint Web フロント エンド(WFE)サーバーのロードバランシングを行う AX シリーズデバイスで行われました。これ らの WFE サーバーのことを以降の章では Web サーバー(WS)と呼びます。本書におけるサー バーの役割については、「SharePoint 2010 のための AX 構築におけるサーバーの役割」の図 1 を参照してください。

本書は、SharePoint のための基本的な AX の構成と高度な AX の構成の 2 つの部分に分かれてい ます。基本的な AX の構成は、SharePoint と共に使用するために必要な最低限の構成です。基本 的な構成から高度な構成に変更する場合、一部の構成を変更する必要があります。変更する必要 がある構成については、エラー!参照元が見つかりません。を参照してください。

本書の内容は、Microsoft SharePoint 2003 または 2007 サーバーには該当しません。Microsoft SharePoint 2010 のインストール環境のみに該当します。

3. 本書の前提条件

本書の内容は、以下の前提条件に基づいてテストされています。

AX シリーズの要件

• A10 ネットワークス AX シリーズの ADC バージョン 2.6 以降が稼動している

Microsoft SharePoint の要件

- Microsoft SharePoint 2010 アプリケーションのテストおよび配備が完了し、内部および 外部ユーザーが SharePoint サービスを利用可能である
- Microsoft SQL Server 2008 R2 がある
- Microsoft SharePoint 2010 Server のすべてのコンポーネントが Windows 2008 (64 ビット) Enterprise Edition サーバオペレーティングシステム上で稼働している
- SharePoint クライアントが 64 ビット版の Windows 7 オペレーティングシステムを使用 している
- テストしたクライアントからのアクセス :
 - Microsoft Internet Explorer バージョン 8.0
 - o Google Chrome バージョン 10.0
 - Mozilla Firefox バージョン 4.0.1

注: VIP (Virtual IP:バーチャル IP)が外部クライアントからアクセスされる場合は、ルーテッド モードでネットワークトポロジーを構築してください。SharePoint サービスが内部からアクセス される場合は、ワンアームモードでネットワークを構築してください。SharePoint サービスが内 部および外部クライアントからアクセスされる場合は、ワンアームモード構成でネットワークト ポロジーを構築してください。

注: AX シリーズでサポート可能なその他の構築モードについては、以下の URL を参照して ください。

http://www.a10networks.com/products/axseries-load-balancing101.php

4. SHAREPOINT 2010 のための AX 構築におけるサーバーの役割

図1は、テスト環境におけるサーバーの説明です。

サーバーの役割	役割
Webサーバー	Webフロントエンドサーバー(WFE)とも言われるこのサーバーは、サーバーファームが 処理するリクエストを受け取ったときに使用するすべてのWebページ、Webパーツ、 Webサービスをホストします。
アプリケーション サーバー	このサーバーは、VisioやExcel Servicesなど、ファームで稼働しているサービス アプリケーションをホストします。
データベースサーバー	このサーバーは、構成設定、管理情報、サービスアプリケーション関連データ、ユーザー コンテンツなど、SharePoint 2010の実装に関連するデータのほとんどを保管します。
クエリサーバー	インデックスのクエリおよび一致するコンテンツの検索を行い、ユーザーに提示する コンテンツをWebサーバーに送信するアプリケーションサーバー機能です。
クロールサーバー	コンテンツソースにアクセスしてカタログし、クエリサーバーに結果を伝搬する アプリケーションサーバー機能です。クロールデータベースを使って、クロールされた すべてのソースのURLを保管します。

図1: SharePoint サーバーの役割

5. AX シリーズロードバランサーへのアクセス

このセクションでは、AX シリーズデバイスへのアクセス方法について説明します。CLI (Command Line Interface:コマンドラインインターフェイス)または GUI (Graphical User Interface:グラフィックユーザーインターフェイス)から AX にアクセスします。

- CLI コマンドラインにコマンドを入力するテキストベースのインターフェイスです。
 CLI は、シリアルコンソールから直接アクセスするか、またはネットワークを介して 以下のいずれかのプロトコルを使ってアクセスします。

 - 非セキュアプロトコル Telnet (利用可能な場合)
- GUI クリック操作によって構成または管理ページにアクセスし、デバイスを構成 または管理するための値を入力したり選択したりする Web ベースのインターフェイ スです。以下のプロトコルを使って GUI にアクセスします。
 - セキュアプロトコル HTTPS (Hypertext Transfer Protocol over Secure Socket Layer:セキュアソケットレイヤ上のハイパーテキスト転送プロトコル)

注: AX デバイスでは、デフォルトで HTTP リクエストが HTTPS にリダイレクトさ れます。

- デフォルトユーザー名: admin
- デフォルトパスワード : a10
- デバイスのデフォルト IP アドレス: 172.31.31.31

AX シリーズデバイスへのアクセス方法の詳細については、ドキュメント A10 Networks AX Series System Configuration and Administration Guide.pdf を参照してください。

6. SHAREPOINT 2010 の推奨インストール手順

- トポロジに配備するサーバーのリストを用意します。SharePoint に必要なサーバーは、 アプリケーションサーバ(AS)、Web フロントエンド(WFE)、データベースサーバ(DB)、 インデックス/検索サーバー、アクティブディレクトリー(AD)サーバー/ドメインネーム サーバ(DNS)、およびオプションのネットワークアクセスストレージ(NAS)です。
- ベースとなる Windows OS (Windows 2010 64 ビット版)をインストールし、前提条件と して必要なソフトウェアをインストールします。SQL データベースをインストールし、 SharePoint 2010 Server のデータベース作成に必要なパーミッションレベルを持つ SQL 管理者アカウントを設定します。
- 3. ネットワーク管理およびユーザプロビジョニングにはアクティブディレクトリー(AD)お よび DNS サーバーが必要です。

- 4. SharePoint 2010 Server をインストールし、サーバーの役割に基づいてサービスを構成 します。この作業は SharePoint の Web 管理 GUI から行います。
- 5. Web サーバーで AAM (Alternate Access Mapping:代替アクセスマッピング)を構成します。

注: AAMの構成方法については、以下のサイトを参照してください。

http://technet.microsoft.com/en-us/library/cc263208(office.12).aspx

6. SharePoint サイトがアクセス可能であることをテストで確認したら、AX シリーズデバ イスを配備します。

注:既存の SharePoint 2010 Server がすでにインストールされている場合は、上記の SharePoint 2010の推奨インストール手順は省略してください。



図2: SharePoint 2010の構築トポロジ

8. SHAREPOINT のための基本的な AX 構成

この章では、Microsoft SharePoint 2010 Server が実装された状態で AX シリーズを構成する方法 について説明します。この章で説明する手順では、SSL オフロードを使用しない基本的な Microsoft SharePoint 構成にリアルサーバー、サービスグループ、バーチャルサービス、および バーチャルサーバーをインストールします。

<u>基本的な SharePoint 構成</u>



図3:基本的な SharePoint 構成

最も単純な構成では、AX シリーズデバイスを使って、保護された HTTPS 接続による SharePoint トラフィックのロードバランスを行います。AX によってロードバランスが行われる のは WFE サーバのみです。これは、Microsoft SharePoint 2010 のバックエンドサーバーに独自 の冗長性およびロードバランシングメカニズムが組み込まれているためです。いかなるロードバ ランサーでもアプリケーションサーバー(AS)や他の SharePoint コンポーネントのロードバラン スは行えません。その理由については、以下の URL を参照してください。

http://social.technet.microsoft.com/Forums/en-CA/sharepoint2010setup/thread/f3ae16b1-8a3b-4ffa-a2e0-e78a48889c71

http://blogs.msdn.com/b/spses/archive/2010/01/20/sharepoint-2010-shared-service-architecture-part-1.aspx

8.1 サーバーの構成

このセクションでは、AX シリーズで SharePoint Web サーバーを構成する方法について説明 します。

- 1. [Config Mode] > [SLB] > [Server]を選択します。
- 2. [Add]をクリックし、新しいサーバーを追加します。
- 3. [Server]セクションで、以下の必須情報を入力します。
 - a. [Name:] **「WS1」**
 - b. [IP address /Host:] /172.16.1.5
 - **注**:必要に応じて、追加するサーバーについても入力してください。

General	
Name: *	WS1
IP Address/Host: *	172.16.1.5
GSLB External IP Address:	
Weight:	1
Health Monitor:	(default) 👻
Status:	Enabled Disabled
Connection Limit:	8000000 V Logging
Connection Resume:	
Slow Start:	
Spoofing Cache:	
Stats Data:	Enabled
Extended Stats:	© Enabled
Server Template:	default 👻
Description:	*

図4:リアルサーバーの構成

- サーバー構成にポートを追加するために、
 [Config] > [Service] > [SLB] > [Server] > [Port]セクションを選択します。
- 5. ポートとプロトコルのタイプを入力し、[Add]をクリックします。

01	Port												
	Port:* 443 Protocol: TCP Veight(W):* 1 No SSL										Add		
	Connection Limit(<u>CL</u>):8000000 V Logging Connection Resume(<u>CR</u>):										🥥 Update		
	Serve	er Por	t Templa	te(<u>SPT</u>):	default		-	Stats Da	ta <u>(SD</u>): 🖲 Ena	abled 🔘 Disa	bled		Delete
	Healt	h Mor	nitor(<u>HM</u>)	: 🔍 (def	ault)	•	© Fo	ollow Port	:	TCP -			🧭 Enable
	Exten	ided S	Stats(<u>ES</u>)	: 🔘 Enab	oled 💿 Disabl	led							🕴 Disable
			Port	Protocol	CL	CR	w	No SSL	SPT	нм	SD	ES	
		0	443	TCP	8000000 🥑		1	8	default	(default)	0	8	

図5:リアルサーバーのポートの構成

6. [OK]をクリックして構成を保存します。

8.2 ヘルスモニターの構成

AX シリーズでは、リアルサーバーおよびサービスポートのヘルスチェックが自動的に開始され るため、すべてのリクエストが稼動状態の利用可能なサーバーに送られることがクライアントに 保証されます。ヘルスチェックに対してサーバーまたはポートが適切に応答しない場合、その サーバーは利用可能なサーバーのリストから一時的に除去されます。サーバーが修復されてヘル スチェックに対して適切に応答するようになったら、利用可能なサーバーのリストにそのサー バーが自動的に追加されます。

- 1. [Config Mode] > [SLB] > [Server Port] > [Health Monitor]を選択します。
- 2. [Health Monitor:]ドロップダウンメニューをクリックし、[Create]を選択します。
- 3. ヘルスモニター名として「SharePoint HC」を入力します。
- 4. メソッドタイプとして[HTTP]を選択します。
- 5. [OK]をクリックし、サービスグループの構成に進みます。

Health Monitor		
Name: *	SharePoint HC]
Retry:	3]
Consec Pass Req'd:	1	
Interval:	5	Seconds
Timeout:	5	Seconds
Strictly Retry:		
Disable After Down:		
O Method		
Override IPv4:]
Override IPv6:		
Override Port:		
Method:	Internal External	
Туре:	HTTP	
Port:	80]
Host:		
URL:	GET 🗸 /	
User:]
Password:		
Expect:		Text O Code
Maintenance Code:]

図6: ヘルスモニターの構成

8.3 サービスグループの構成

このセクションでは、サービスグループ内に SharePoint Web サーバを構成する方法について説 明します。サービスグループにはリアルサーバーのセットが含まれています。AX デバイスはそ の中からクライアントリクエストに応答するためのサーバを選択します。1 つのサービスグルー プが複数の SharePoint リアルサーバーを1つの論理サーバーとしてサポートします。

- 1. [Config Mode] > [SLB] > [Service Group]を選択します。
- 2. [Add]をクリックし、新しいサービスグループを追加します。
- 3. [Service Group]セクションで、以下の必須情報を入力します。
 - a. [Name:] SharePoint Servers
 - b. [Type:]ドロップダウンメニューから[TCP]を選択します。
 - c. [Algorithm:]ドロップダウンメニューから[Round Robin]を選択します。
 - d. [Health Monitor:]ドロップダウンメニューから[SharePoint HC]を選択します。

Service Group	
Name: *	SharePoint Servers
Туре:	TCP
Algorithm:	Round Robin
Health Monitor:	SharePoint HC
Min Active Members:	
	Send client reset when server selection fails
Stats Data:	Enabled Disabled
Extended Stats:	© Enabled
Description:	h.

図7:サービスグループの構成

- 4. [Config Mode] > [Service] > [SLB] > [Service Group]を選択します。
- 5. ウィンドウの[Server]セクションで、ドロップダウンリストを使ってサーバーを1つ以上 追加します。

[Server:]ドロップダウンメニューから**[WS1]**を選択します。 [Port:]「**443**」と入力します。

6. [Add]をクリックし、利用可能なすべてのSharePoint Webサーバを入力します。

図7では、「WS1」および「WS2」というサーバー名がそれぞれポート「443」で入力されています。

Serve IPv4/I Serve	er IPv6: er: *		● IPv4 WS2	IPv6	•	Port: *	443	3	O Add
Serve	er Por	t Template(<u>SPT</u>):	default		-	Priority:	1	-	🥥 Update
Stats	Data	:	Enabled	Disable	ed				Oelete
		Server		Port	SPT		Priority	Stats Data	📀 Enable
	0	WS1		443	default		1	0	🕴 Disable
	0	WS2		443	default		1	v	

図8:サービスグループのサーバーの構成

7. 終了したら、[OK]をクリックして構成を保存します。

8.4 バーチャルサーバー

このセクションでは、AX シリーズで VIP を構成する方法について説明します。AX シリーズ内に バーチャルサーバーポートを追加すると、選択されたプロトコルのタイプに基づいてバーチャル サービスリストが生成されます。

1. [Config Mode] > [SLB] > [Virtual Server] > [一般]を選択します。

- 2. [一般]セクションで、以下の必須情報を入力します。
 - 1. [Name:] **WS-VIP**
 - 2. [IP Address or CIDR Subnet:] [172.16.1.200]

General						
Name: *	WS-VIP		🖾 Wildo	ard		
IP Address or CIDR Subnet: *	172.16.1.200		IPv4	IPv6		
Status:	Enabled	Oisabled				
ARP Status:	Enabled	Oisabled				
Stats Data:	Enabled	Oisabled				
Extended Stats:	Enabled	Oisabled				
When-All-Ports-Down:	Enabled	Oisabled				
HA Group:		-				
Virtual Server Template:	default		-			
PBSLB Policy Template:			-			
Description:					*	

図9: バーチャルサーバーまたは VIP の構成

- 3. [Config Mode] > [SLB] > [Virtual Server] > [Port]を選択します。
 - 1. [Add]をクリックします。
 - 2. バーチャルサーバーポートの情報を入力します。

a.[Type:]ドロップダウンメニューから[TCP]を選択します。

- b.[Port:] **[443]**
- c.[Service Group:]ドロップダウンメニューから[SharePoint Servers]

を選択し、バーチャルサーバーをリアルサーバーにバインドします。

Virtual Server:	WS-VIP
Type: *	TCP
Port: *	443
Service Group:	SharePoint Servers 🗸

図10:バーチャルサーバーポートの構成

d.[OK]の次に[Save]をクリックし、構成の変更を保存します。

図 11 : バーチャルポートリスト

Name		🔶 Туре	🔷 Port	🔶 IP Address or CIDR Subnet🔶
	_TCP_443	TCP	443	172.16.1.200
Select All	Unselect All			

図 12:バーチャルサービスの概要

6. [OK]をクリックして構成を保存します。

8.5 IP ソースパーシステンス

AX シリーズは、Cookie パーシステンス、宛先 IP パーシステンス、ソース IP パーシステンス、 および SSL セッション ID パーシステンスなど、さまざまなモードのパーシステンスをサポート します。パーシステンスは、同一クライアントから同一サーバーへトラフィックをダイレクトし ます。

本書では、基本的な SharePoint 構成におけるソース IP パーシステンスを重点的に説明します。 Cookie パーシステンス構成については、高度な SharePoint 構成のセクションで説明します。



図 13: ソース IP パーシステンス

8.5.1 IP パーシステンステンプレートの作成

- 1. [Config Mode] > [Template] > [Persistent] > [Source IP Persistence]を選 択します。
- 2. [Add]をクリックします。
- ソース IP パーシステンス名を入力します。
 例:「Source IP Persistence」
- 4. [Match Type]ドロップダウンメニューをクリックし、[Port]を選択します。
- 5. [Timeout]に「5」分(デフォルト)と入力します。
- 6. [OK]をクリックして構成を保存します。

Template >> Persistent >> Source	P Persistence >> Source IP Persistence
Source IP Persistence	
Name: *	Source IP Persistence
Match Type:	Port 👻
Timeout:	5 Minutes
Don't Honor Conn Rules:	
Netmask:	255.255.255.255
≪ OK X Cancel	



8.5.2 VIP への IP パーシステンスの適用

テンプレートを VIP に割り当てるには、

[Config Mode] > [Service] > [SLB] > [Virtual Server Port]を選択します。

 [Persistence template type]セクションのドロップダウンメニューから[Source IP Persistence template]を選択し、対応する作成済みのテンプレートを選択します。以 下の例では、「Source IP Persistence」がテンプレート名として使用されています。

Persistence Template Type:	Source IP Persistence Template	•
Source IP Persistence Template:	Source IP Persistence	-

図 15:パーシステンステンプレートの構成

2. [OK]をクリックして構成を保存します。

8.6 IP ソース NAT

このセクションでは、IP SNAT (Source Network Address Translation:ソースネットワークアドレス 変換)に IP アドレスプールが使用されるよう構成します。クライアントからの受信トラフィックが VIP アドレス(例: 172.16.1.200)にアクセスするとき、クライアントリクエストのソースネット ワークアドレスが変換されます。つまり、構成されたソース NAT のアドレスプールに基づいて、 AX がクライアントのソース IP アドレスを置換します。ネットワークトポロジーが**ワンアーム**構成 で、VIP と同一サブネット上に内部クライアントが存在する場合は SNAT が必要です。NAT を行 うには、バーチャルサーバーポートにソース NAT テンプレートを適用する必要があります。



図 16 : IP ソース NAT およびトラフィックフローの概要

8.6.1 IP ソース NAT テンプレートの作成

- 1. [Config Mode] > [Service] > [IP Source NAT]を選択します。
- 2. [Add]をクリックします。
- 3. IP ソース NAT 名として[Name]に「SNAT」と入力します。
- 4. [Start IP Address]に「172.16.1.250」(例)と入力します。
- 5. [End IP Address]に「172.16.1.250」(例)と入力します。
- 6. [Netmask]に「255.255.255.0」と入力します。

IPv4 Pool	
Name: *	SNAT
Start IP Address: *	172.16.1.250
End IP Address: *	172.16.1.250
Netmask: *	255.255.255.0
Gateway:	
HA Group:	▼

図 17 : IP ソース NAT の構成

- [OK]をクリックして構成を保存します。
 IP ソース NAT を~に割り当てます。
- 8. VIP にテンプレートを割り当てるには、~を選択します。

注: バーチャルサーバーポートに SNAT テンプレートを割り当ててください。 SharePoint環境が多数の同時ユーザーで構成される場合、複数の SNAT IP アドレスを構 成することをお奨めします。1 つの IP アドレスを最大 64,000 のフローに使用できます。

8.6.2 VIP への IP ソース NAT の割り当て

[Config Mode] > [Service] > [SLB] > [Virtual Server]

- 1. バーチャルサーバー名として[WS-VIP]を選択します。
- 2. ポートとして[443]を選択し、[Edit]をクリックします。
- 3. [Source NAT Pool]ドロップダウンメニューから[SNAT]を選択します。

Access List:	
Source NAT Pool:	SNAT 👻

4. [OK]をクリックして構成を保存します。

9. サービスの確認

基本的な構成が正しく機能していることを確認するには、以下の項目を選択します。

1. [Config Mode] > [Service] > [SLB] > [Server]

[Status]および[Health]が緑色の状態であることを確認します。 💿 🥝

📄 Name	🔷 De	escription 🔶	IP Address/Host 🍦	Health Monitor	Status 🍦	Health	-
🔲 WS1			172.16.1.5	SharePoint HC	0	\odot	
WS2			172.16.1.6	SharePoint HC	0	\odot	
Select All	Unselect All			:	Selected:		0

2. [Config Mode] > [Service] > [SLB] > [Virtual Server]

[Status]および[Health]が緑色の状態であることを確認します。 📀 🥝

Name	🔶 Description	IP Address or CIDR Subnet	🔷 Status	🔷 Health 🛛 🗧	HA Group	\$
🔲 🗟 ws-vip		172.16.1.200		0		
Select All	Unselect All			Selected	: (D

前述の許可されている Web ブラウザーのいずれかを起動し、VIP アドレス: 仮定: 172.16.1.200 = www.example.com を表示します。



10.SHAREPOINT のための AX の高度な機能

このセクションでは、基本的な SharePoint 構成に追加できる高度なトラフィック最適化機能に ついて説明します。これらの機能を使用することで、Web アプリケーションの高速化、 SharePoint Web サーバーパフォーマンスの最適化、および拡張性の向上を実現できます。

- SSLオフロード
- HTTP/HTTPS 圧縮
- Cookie パーシステンス
- コネクションリユース
- RAM キャッシング

10.1 構成の準備

これらの高度な機能を構成するには、基本構成に少し変更を加える必要があります。

- バーチャルサーバーでバーチャルポートのサービスタイプを TCP から HTTPS に変更する
- 既存の SharePoint Web サーバーの SSL 証明書をインポートするか、または AX から自己署 名 CA を作成する
- SSL テンプレートを作成し、SSL テンプレートを使って VIP を更新する

注:基本的な構成をまだ行っていない場合は、7 ページの手順を実行してください。前述のとおり、サービスグループのポート番号およびバーチャルポートのサービスタイプを必ず置き換えて ください。もしくは、置き換えを行わずに基本的な構成を完了し、その後、以下の手順に従って 必要な変更を行ってください。

10.2 サービスグループのポート番号の変更

- 1. [Config Mode] > [Service] > [SLB] > [Service Group]を選択します。
- 2. 基本的な構成で作成したサービスグループをクリックします。
- 3. [サーバー]セクション:

a.サーバー名の隣のチェックボックスを選択します。

b.[Port]を「443」から「80」に変更します。

c. [Update]をクリックします。

d.サーバーごとに上記手順を繰り返します。

IPv4/I	IPv6:		🖲 IPv4 🛛 🔘 IP	v6					
Serv	er:*	V	VS2		-	Port: *	80		📀 Add
Serve	er Po	ort Template(<u>SPT</u>):	default		-	Priority:	1	-	🥥 Update
Stats	Data	a: ()	Enabled	Disable	d				Delete
		Server	Po	rt SP	т		Priority	Stats Data	🔮 Enable
	0	WS1	80	de	fault		1	0	🕴 Disable
		WS2	80	de	fault		1		1

図 18:サーバーの構成

3. [OK]をクリックして構成を保存します。

10.3 バーチャルポートのサービスタイプの変更

- 1. [Config Mode] > [Service] > [SLB] > [Virtual Service]を選択します。
- 基本的な構成で作成したバーチャルサービス(_172.16.1.200_TCP_443)をクリックします。
- 3. バーチャルサービス名を「_172.16.1.200_HTTPS_443」に変更します。
- 4. [Type:]ドロップダウンメニューから[HTTPS]を選択します。

Virtual Service				
Virtual Service: *	_172.16.1.200_HTTPS_443			
Type: *	HTTPS	•		
Port: *	HTTP HTTPS			
Address *	Fast-HTTP TCP UDP BTSP	● IPv4 ◎ IPv6		
HA Group:	FTP			
Service Group:	MMS SSL-Proxy			
Connection Limit:	SMTP	set 🗹 Logging		
	SIP-TCP	n preferred method fails		
	TCP-Proxy			
	Others	election fails		
Status:	Enabled Oisabled			

図 19 : バーチャルサービスタイプの更新

5. [OK]をクリックして構成を保存します。

11.SSL オフロード

SSL オフロードは、SharePoint Web サーバーから SSL トラフィック処理の負荷を除いてサー バーを加速します。SharePoint サーバーがこれらのトランザクションを処理する代わりに、AX シリーズがすべての HTTPS トラフィックを復号化および暗号化し、(非セキュアな) HTTP 経由 で SharePoint サーバーにトラフィックを送信します。



図20:SSLオフロードの概要

この構成では、SharePoint HTTPS バーチャルサーバー用に SSL 証明書が構成されるの で、クライアントはセキュアなモードで SharePoint Web サービスにアクセスできます。



図 21: クライアント SSL の概要

11.1 証明書のインポートまたは作成

- 1. [Config Mode] > [SSL Management] > [Certificate]を選択します。
- 2. AX シリーズから SSL テンプレートをインストールするときに構成可能なオプショ ンが2種類あります。

オプション1: AX から自己署名 CA を作成する: AX シリーズから自己署名 CA を作成します。

オプション 2: SSL 証明書と鍵をインポートする: SharePoint Web サー バーから既存の CA 証明書をエクスポートし、AX シリーズデバイスにイン ポートします。

11.2 オプション1: AX から自己署名 CA を作成する

- 1. [SSL Management]から[Create]をクリックし、新しい SSL 証明書を追加し ます。
- 2. 証明書のファイル名として「WS」と入力します。
- 3. [Issuer:]ドロップダウンメニューから[Self]を選択し、以下の値を入力します。
 - i. [Common Name:] [WS]
 - ii. [Division:] [A10]
 - iii. [Organization:] [A10]
 - iv. [Locality:] [San Jose]
 - v. [State or Province:] [CA]
 - vi. [Country:] [USA]
 - vii. [Email Address:] [spadmin@example.com]
 - viii. [Valid Days:]「**730**」(デフォルト)
 - ix. [Key Size:]「2048」(ビット)

注:AX シリーズデバイスは、512、1028、2048、4096 のキーサイズをサ ポート可能です。ビットサイズが大きいほど、AX が必要とする CPU 処理量 が増加します。

4. [OK]をクリックして構成を保存します。

General	
File Name: *	WS
A Cartificate	
Issuer:	Self -
Common Name: *	A10
Division:	A10
Organization:	A10
Locality:	San Jose
State or Province:	CA
Country (C): *	United States of America US
Email Address:	spadmin@example.com
Valid Days:	730 days
O Key	
Key Size:	2048 🔻 Bits

図 22: クライアント SSL 証明書の作成

11.3 **オプション2**:SSL証明書と鍵のインポート

- 1. [SSL Management]から[Import]をクリックし、新しい SSL 証明書を追加し ます。
- 2. 証明書の名前として「WS」を入力します。
- 3. [Import Certificate from:]で[Local]を選択します(証明書の発行元に応じて 選択)。
- 4. 証明書のパスワードを入力します(該当する場合)。
- 5. 証明書のソースを入力します(該当する場合)。

注: AXデバイスを使ってCSRを生成したCA署名証明書をインポートする場合は、鍵をインポートする必要はありません。CSRを生成するときに、AXデバイスで鍵が自動的に生成されます。

Import	
Name: *	WS
Import Certificate from:	Local Remote Text Ext Ext
Certificate Format:	PFX 🗸
Password:	•••
Certificate Source:	C:\Temp\WS.pfx Browse
V OK X Cancel	

図23:SSL証明書のインポート

[OK]をクリックして構成を保存します。

11.4 クライアント SSL テンプレートの構成と適用

このセクションでは、クライアントSSLテンプレートを構成してVIPに適用する方法について説明します。

- 1. [Config Mode] > [Service] > [Template] > [SSL] > [Client SSL]を選択します。
- 2. [Add]をクリックします。
- 3. [Name:]に「Client SSL-WS」と入力します。
- 4. [Certificate Name:]に「WS」と入力します。
- 5. [Key Name:]に「**WS**」と入力します。
- 6. [Pass Phrase:]に「example」と入力します。
- 7. [Confirm Pass Phrase:]に「example」と入力します。

Client SSL		
Name: *	WS	
Certificate Name:	WS 👻	
Chain Cert Name:		
Key Name:	WS 👻	
Cache Size:	0	
Pass Phrase:	•••]
Confirm Pass Phrase:	•••]

図24: クライアントSSL

クライアント SSL テンプレートが完成したら、以下の手順でクライアント SSL を HTTPS VIP (ポート 443)にバインドする必要があります。

- [Config Mode] > [SLB] > [バーチャルサーバー]を選択します。
- 2. [Virtual Server name]をクリックします。
- 3. [443]を選択し、[Edit]をクリックします。
- 4. 作成したクライアント SSL テンプレートを適用するには、 [Client-SSL template]ドロップダウンメニューをクリック します。
- 5. ドロップダウンメニューから[WS]を選択します。

HTTP Template:	▼
RAM Caching Template:	▼
Client-SSL Template:	WS 👻
Server-SSL Template:	▼
Connection Reuse Template:	▼
TCP-Proxy Template:	▼
Persistence Template Type:	· · · · · · · · · · · · · · · · · · ·
PBSLB Policy Template:	

図 25 : クライアント SSL のバインド

6. [OK]をクリックして構成を保存します。

11.5 配備の確認

SSLオフロードが機能していることを確認するには、

[Monitor Mode] > [Service] > [Application] > [SSL]を選択します。

注:HTTPS (443)を使って SharePoint サイトを表示し、統計情報で SSL コネクションの数 および SSL コネクションの合計を確認してください。

Statistics for SSL	1 Minute 👻 🌣 Refresh 🏢 Clear
Statistics for SSL	
Number of SSL Modules:	1
Current SSL Connections:	1
Total SSL Connections:	1.2M
Failed SSL Handshakes:	0
Failed Crypto operations:	0
SSL Memory Usage:	170.8K Bytes
SSL fail CA verification:	0
No HW Context Memory:	0
HW ring full:	0
SSL Module	1
Number of Enabled Crypto Engines:	22
Number of Available Crypto Engines:	22

図26:SSLオフロードの統計情報

圧縮は帯域幅を最適化する機能です。Webサーバーから要求されたHTTPオブジェクトを凝縮し ます。圧縮の目的は、要求されたデータをより効率的に送信し(送信するデータ量を減らす)、よ り高速にクライアントに応答することです。





12.1 HTTP 圧縮テンプレートの作成

- 1. [Config Mode] > [Template] > [Application] > [HTTP]を選択します。
- 2. [Add]をクリックします。
- 3. [Name:]に「HTTP Compression」と入力します。

注:デフォルトでは圧縮は無効になっています。圧縮を有効にすると、以下のオプションにこれらのデフォルト値が設定されます。

НТТР	
Name: *	HTTP Compression
Failover URL:	
Strict Transaction Switching:	© Enabled
Client IP Header Insert:	
Retry HTTP Request:	
	Terminate HTTP 1.1 client when request has Connecton: close

図 28 : HTTP 圧縮テンプレート

- 4. [Compression]ドロップダウンメニューをクリックし、圧縮オプションを入力しま す。
- 5. テンプレートから目的の圧縮オプションを入力します。
 - 1. [Enable]を選択して圧縮を有効化します。
 - [Level:]ドロップダウンメニューから[Level 1 (Least Level Compression)]
 を選択します。

注: AX には、レベル 1 から 9 までのさまざまな圧縮レベルがあります。レベル 1 の設定をお奨めします。

Compression		
Compression:	Enabled Disabled	
Keep Accept Encoding:	© Enabled	
Level:	1(least compression, fastest)	
Min Content Length:	☑ 120	
	Туре:	O Add
	Туре	Delete
Contant Tuno:		
content type.		
	Type:	Add
	🔲 Туре	Delete
Exclude Content Type:		
	URI	O Add
		Delete
Exclude URI:		
✓ OK X Cancel		

図29: 圧縮の構成

6. [OK]の次に[Save]をクリックし、構成の変更を保存します。

12.2 VIP への HTTP 圧縮テンプレートの適用

- 1. バーチャルサーバーポート内で圧縮テンプレートを適用するには、以下の手順を実 行します。
 - 1. [Config Mode] > [SLB] > [Virtual Server]を選択します。
 - 2. バーチャルサーバー名を選択します。
 - 3. [443]を選択し、[Edit]をクリックします。
 - 4. *[HTTP Template]*ドロップダウンメニューから[HTTP Compression]を選択 し、バーチャルサーバーポートに圧縮機能を適用します。

HTTP Template:	HTTP Compression -
RAM Caching Template:	-
Client-SSL Template:	
Server-SSL Template:	
Connection Reuse Template:	
TCP-Proxy Template:	

図 30 : HTTP 圧縮テンプレート

5. [OK]をクリックして構成を保存します。

12.3 配備の確認

AX シリーズデバイスでデータが圧縮されていることを確認するには、[Monitor Mode] > [Service] > [Application] > [HTTP]を選択します。

Control								
CPU	CPU1	Data CPU2	Data CPU3	Data CPU4	Data CPU5	Data CPU6	Data CPU7	Total
0	0	0	0	0	0	0	0	0
0	132.9K	259.1K	570.8K	393.0K	5.4K	10.6K	60.2K	1.4M
0	132.9K	274.6K	787.5K	595.3K	5.4K	10.6K	60.2K	1.8M
0	132.9K	274.6K	787.5K	595.3K	5.4K	10.6K	60.2K	1.8M
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	44.6K	86.3K	189.5K	130.7K	1.8K	3.6K	20.2K	476.7K
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	-	-	FT 45-14
0	0	0	0	0	0	上稲日	1 1	上稲伐
0	0	0	0	0	0	5.60		91.6M
0	0	0	0	0	0	0	0	
0	83.5K	164.6K	384.8K	271.3K	3.9K	7.1K	37.9	953.
0	0	0	0	0	0	0	0	
0	276.0M	686.6M	2.5G	2.0G	9.8M	18.8M	128.4M	5.6
0	4.4M	11.0M	40.8M	32.8M	161.8K	308.6K	2.1M	91.6M
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
	PU 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	PU CPU1 0 0 0 132.9K 0 132.9K 0 132.9K 0 132.9K 0 132.9K 0 0	PU CPU1 CPU2 0 0 0 0 132.9K 259.1K 0 132.9K 274.6K 0 132.9K 274.6K 0 132.9K 274.6K 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 276.0M 686.6M 0 0 0 0 0 0 0	CPU1 CPU2 CPU3 0 0 0 0 0 132.9K 259.1K 570.8K 0 132.9K 274.6K 787.5K 0 132.9K 274.6K 787.5K 0 132.9K 274.6K 787.5K 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 <	PU CPU1 CPU2 CPU3 CPU4 0 0 0 0 0 132.9K 259.1K 570.8K 393.0K 132.9K 274.6K 787.5K 595.3K 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	PU CPU1 CPU2 CPU3 CPU4 CPU5 0 0 0 0 0 0 0 132.9K 259.1K 570.8K 393.0K 5.4K 132.9K 274.6K 787.5K 595.3K 5.4K 132.9K 274.6K 787.5K 595.3K 5.4K 132.9K 274.6K 787.5K 595.3K 5.4K 0 132.9K 274.6K 787.5K 595.3K 5.4K 0 132.9K 274.6K 787.5K 595.3K 5.4K 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	PUCPU1CPU2CPU3CPU4CPU5CPU6000000000132.9K259.1K570.8K393.0K5.4K10.6K0132.9K274.6K787.5K595.3K5.4K10.6K0132.9K274.6K787.5K595.3K5.4K10.6K0132.9K274.6K787.5K595.3K5.4K10.6K0132.9K274.6K787.5K595.3K5.4K10.6K000 <td>PU CPU1 CPU2 CPU3 CPU4 CPU5 CPU6 CPU7 0 0 0 0 0 0 0 0 0 0 132.9K 259.1K 570.8K 393.0K 5.4K 10.6K 60.2K 0 132.9K 274.6K 787.5K 595.3K 5.4K 10.6K 60.2K 0 132.9K 274.6K 787.5K 595.3K 5.4K 10.6K 60.2K 0 132.9K 274.6K 787.5K 595.3K 5.4K 10.6K 60.2K 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</td>	PU CPU1 CPU2 CPU3 CPU4 CPU5 CPU6 CPU7 0 0 0 0 0 0 0 0 0 0 132.9K 259.1K 570.8K 393.0K 5.4K 10.6K 60.2K 0 132.9K 274.6K 787.5K 595.3K 5.4K 10.6K 60.2K 0 132.9K 274.6K 787.5K 595.3K 5.4K 10.6K 60.2K 0 132.9K 274.6K 787.5K 595.3K 5.4K 10.6K 60.2K 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

図 31 : 圧縮の統計情報(圧縮前後)

13.COOKIE パーシステンス

Cookie パーシステンスは、ソース IP パーシステンスに比べて高い粒度の永続性を提供します。 Cookie パーシステンスを使用すると、セッションデータがユーザーのブラウザー内に保持され ます。

13.1 COOKIE パーシステンステンプレートの作成

Cookie パーシステンスを有効にするには、まず最初に以下の手順でテンプレートを作成する 必要があります。

- 1. [Config mode] > [Service] > [Template] > [Cookie Persistence]を選択します。
- 2. [Add]をクリックし、新しい Cookie パーシステンステンプレートを追加します。
- 3. [Expiration] ラジオボタンを選択し、[Seconds] フィールドに「86400」と入力します。
- 4. [Insert Always]チェックボックスを選択します。

Cookie Persistence	
Name: *	SharePoint Cookie
Expiration:	86400 Seconds
Cookie Name:	
Domain:	
Path:	
Match Type:	Service Group Port -
Insert Always:	
Don't Honor Conn Rules:	

図 32 : Cookie パーシステンステンプレート

5. [OK]の次に[Save]をクリックし、構成の変更を保存します。

SharePoint テンプレートの構成が終了すると、Cookie パーシステンスのリストにテンプ レートが表示されます。

13.2 VIP への COOKIE パーシステンステンプレートの適用

- 1. VIP 内で Cookie パーシステンスを適用するには、以下の手順を実行します。
 - a. [Config Mode] > [SLB] > [バーチャルサーバー]を選択します。
 - b. [Virtual Server name]をクリックします。
 - c. [443]を選択し、[Edit]をクリックします。
- 2. AX 機能のリストから、[Cookie Persistence Template]セクションを探します。

3. [Cookie Persistence Template]ドロップダウンメニューから、先ほど作成した [SharePoint Cookie]を選択します。

Persistence Template Type:	Cookie Persistence Template	Ŧ
Cookie Persistence Template:	SharePoint Cookie	Ŧ

図 33 : Cookie パーシステンステンプレート

4. [OK]の次に[Save]をクリックし、構成の変更を保存します。

13.3 配備の確認

Cookie パーシステンスがインストールされていることを確認するには、[Monitor Mode] > [Service] > [Application] > [Persistent]を選択します。

	Control CPU	Data CPU1	Data CPU2	Data CPU3	Data CPU4	Data CPU5	Data CPU6	Data CPU7	Total
URL Hash Persistent OK(primary)	0	19.7K	6.1K	2.3K	1.0K	461	206	15.5K	45.2K
URL Hash Persistent OK(secondary)	0	0	0	0	0	0	0	0	0
URL Hash Persistent Fails	0	0	0	0	0	0	0	0	0
Source IP Persistent OK	0	239.2K	103.6K	44.8K	19.4K	8.6K	3.9K	168.5K	588.0K
Source IP Persistent Fails	0	0	0	0	0	0	0	0	0
SSL SID Persistent OK	0	0	0	0	0	0	0	0	0
SSL SID Persistent Fails	0	0	0	0	0	0	0	0	0
Cookie Persistent OK	0	213.7K	91.3K	36.6K	14.4K	6.4K	2.8K	149.6K	514.7K
Cookie Persistent Fails	0	0	0	0	0	0	0	0	0
Persistent Cookie Not Found	0	121.6K	30.8K	12.6K	4.5K	1.6K	732	100.1K	272.0K

図 34 : Cookie パーシステンスモニタ

14.コネクションリユース(TCP オフロード)

AX シリーズのコネクションリユース機能は、SharePoint Web サーバーと TCP コネクションを 確立し、そのコネクションを複数のクライアントリクエストに再利用することで、設定されてい る TCP コネクションに関するオーバーヘッドを減らします。それにより、各 SharePoint WFE サーバーへの TCP コネクションの総数が減ります。

コネクションリユースの利点は、サーバーの TCP スタックをオフロードし、レスポンスタイム の高速化とサーバーの拡張性向上を実現できることです。コネクションリユースを有効にする場 合、ソース NAT を有効にする必要があります。構成情報については、ソース NAT を参照してく ださい。以下の*図 13*は、コネクションリユースを使用しない構成例です。*図 32 は、コネクショ* ンリユースの配備方法を示しています。 注: SharePoint サーバーで NTLM 認証が構成されている場合、コネクションリユースはサポートされません。







図 36: コネクションリユースが設定されている場合

14.1 コネクションリユーステンプレートの作成

- 1. [Config Mode] > [Template] > [Connection Reuse]を選択します。
- 2. [Add]をクリックします。
- 3. [Name:]に「SharePoint Connection」と入力します。
- 4. [OK]の次に[Save]をクリックし、構成の変更を保存します。

Connection Reuse		
Name: *	SharePoint Connection	
Limit Per Server:	1000	
Timeout:	2400	Seconds
Keep Alive Connections:		

図 37: コネクションリユースの概要

14.2 VIP へのコネクションリユースの適用

- 1. VIP 内でコネクションリユースを適用するには、以下の手順を実行します。
 - a. [Config Mode] > [SLB] > [バーチャルサーバー]を選択します。
 - b. [Virtual Server name]をクリックします。
 - c. [443]を選択し、[Edit]をクリックします。
- [Connection Reuse Template] ドロップダウンメニューで [SharePoint Connection]をクリックし、コネクションリユース機能をバーチャルサー バーポートに適用します。

HTTP Template:		•
RAM Caching Template:		•
Client-SSL Template:		•
Server-SSL Template:		•
Connection Reuse Template:	SharePoint Connection	•
TCP-Proxy Template:		Ŧ
Persistence Template Type:		•

図 38:コネクションリユーステンプレート

3. [OK]の次に[Save]をクリックし、構成の変更を保存します。

14.3 配備の確認

コネクションリユースが機能していることを確認するには、[Monitor Mode] > [Service] > [Application] > [Connection Reuse]を選択します。

Statistics for Connection Reuse					1 Min	iute	• \$ F	Refresh	👕 Clear
	Control CPU	Data CPU1	Data CPU2	Data CPU3	Data CPU4	Data CPU5	Data CPU6	Data CPU7	Total
Open Persistent	0	0	0	0	0	0	0	0	0
Active Persistent	0	0	0	0	0	0	0	0	0
Total Established	0	1.8K	1.4K	1.1K	863	628	587	1.4K	7.8K
Total Terminated	0	1.8K	1.4K	1.1K	863	628	587	1.4K	7.8K
Total Bound	0	362.5K	130.2K	52.9K	21.2K	9.1K	4.0K	271.6K	851.4K
Total Unbound	0	362.5K	130.2K	52.9K	21.2K	9.1K	4.0K	271.6K	851.4K
Total Delayed Unbindings	0	0	0	0	0	0	0	0	0
Total Long Responses	0	0	0	0	0	0	0	0	0
Total Missed Responses	0	0	0	0	0	0	0	0	0

図 39:コネクションリユースモニタ

注: SharePoint サーバーを複数の同時ユーザーが使用している環境でないと、コネクションリ ユース機能の効果が得られません。

15.RAM キャッシング

キャッシュ可能なデータを AX シリーズデバイス内にキャッシュすることで、各 WFE サーバー のオーバーヘッドを低減し、SharePoint サーバーの容量を増加します。RAM キャッシングは、 コネクションと処理する必要があるサーバーリクエストの数を減らします。



図 40: RAM キャッシングテンプレート

15.1 RAM キャッシングテンプレートの作成

- 1. [Config Mode] > [Service] > [Template] > [Application] > [RAM Caching] を選択します。
- 2. **[Add]**をクリックします。
- 3. [Name:]に「SharePoint RAM Caching」と入力します。
- 4. [Age:]に「3600」秒と入力します。
- 5. [Max Cache Size:]に「**512**」MB と入力します。
- 6. [Min Content Size:]に「10」バイトと入力します。
- 7. [Max Content Size:]に「4194303」バイトと入力します。
- [Replacement Policy]ドロップダウンメニューから[Least Frequently Used] (デフォルト)を選択します。
- 9. [OK]の次に[Save]をクリックし、構成の変更を保存します。

注: RAM キャッシングポリシーオプションは、キャッシングの要・不要または 無効化を指定する必要がある特定のデータがない限り、使用する必要はありませ ん。これらのポリシーオプションは、RAM キャッシングテンプレートのポリ シーフォームで構成できます。RAM キャッシングポリシーの詳細については、 *『AX Series System Configuration and Administration Guide』*を参照してくださ い。

RAM Caching		
Name: *	SharePoint RAM Caching	
Age:	3600	Seconds
Max Cache Size:	512	MB
Min Content Size:	10	Bytes
Max Content Size:	4194303	Bytes
Replacement Policy: *	Least Frequently Used	▼
Replacement Policy: * Accept Reload Request:	Least Frequently Used	•
Replacement Policy: * Accept Reload Request: Verify Host:	Least Frequently Used	•
Replacement Policy: * Accept Reload Request: Verify Host: Default Policy No-Cache:	Least Frequently Used	•
Replacement Policy: * Accept Reload Request: Verify Host: Default Policy No-Cache: Insert Age:	Least Frequently Used	•

図 41 : RAM キャッシングの概要

15.2 VIP への RAM キャッシングテンプレートの適用

- 1. バーチャルサーバーポート内で RAM キャッシングテンプレートを適用する には、以下の手順を実行します。
 - a. [Config Mode] > [SLB] > [Virtual Server]を選択します。
 - b. バーチャルサーバー名をクリックします。
 - c. [443]を選択し、[Edit]をクリックします。
- [RAM Caching Template] ドロップダウンメニューから [SharePoint RAM Caching]を選択し、バーチャルサーバーポートに RAM キャッシングを適用 します。

HTTP Template:	_
RAM Caching Template:	SharePoint RAM Caching 👻
Client-SSL Template:	▼
Server-SSL Template:	↓
Connection Reuse Template:	•
TCP-Proxy Template:	▼
Persistence Template Type:	

図 42: RAM キャッシングテンプレート

3. [OK]をクリックして構成を保存します。

15.3 配備の確認

RAM キャッシングが機能していることを確認するには、[Monitor Mode] > [Service] > [Application] > [RAM Caching] > [Details]を選択します。

Statistics for Cache Details				
Virtual Server: All	•	Port:	•	1 Minute 👻 💈 Refresh 🏾 🏦 Clear
Cache Hits			484	キャッシュ内にあったオブジェクトとキャッシュ
Cache Misses			50	から供給されたオブジェクトの総数
Memory Used			1121920	
Bytes Served			13376410	
Entries Cached			49	キャッシュオブジェクトの総数
Entries Replaced			0	
Entries Aged Out			0	
Entries Cleaned			0	
Total Requests			685	
Cacheable Requests			534	
No-cache Requests			44	
No-cache Responses			85	

図 43 : RAM キャッシングモニター

16.AFLEX による SHAREPOINT の保護

このセクションでは、AX aFleX スクリプトを使って、HTTP から送信された SharePoint トラフ ィックを HTTPS にリダイレクトする方法について説明します。aFleX は標準的なスクリプト言 語の TCL に基づいており、ロードバランサーによるレイヤ7の DPI (Deep Packet Inspection:デ ィープパケットインスペクション)を可能にします。aFleX スクリプトの例については、以下の URL を参照してください。

http://www.a10networks.com/products/axseries-aflex_advanced_scripting.php

「*HTTP redirect to HTTPS traffic*」は、SharePoint 2010 サーバーで使用できる最も一般的な aFleX スクリプトの一例です。aFleX スクリプトのその他の例については、以下の URL からダウ ンロードできます。

注:以下の URL にアクセスするには、A10 ネットワークスのサポートアカウントが必要です。 https://a10support.com/adc/index.php/aflex-examples-

注:HTTPS上の VIP に加えて、HTTP (ポート 80)上の VIP も構成する必要があります。HTTP 上の VIP は、HTTP トラフィックを受信すると、常にユーザーを HTTPS にリダイレクトします。 古いブラウザーのブックマークが HTTP を指しているエンドユーザーにとってはこの構成が便利 です。以下の aFleX スクリプトは、要求されたページにエンドユーザーをリダイレクトします (HTTPS を使用)。aFleX スクリプトをバーチャルサーバーポート 80 にバインドする必要があり ます。

16.1 AFLEX スクリプトの定義

- 1. [Config Mode] > [Service] > [aFleX]を選択します。
- 2. [Add]をクリックします。
- 3. [Definition]ボックス内に TCL コードを入力します。
- 4. [OK]をクリックして構成を保存します。

aFleX	
Name: *	Redirect
Definition: *	<pre>when HTTP_REQUEST { HTTP::redirect https://[HTTP::host][HTTP::uri] }</pre>

図 44 : aFleX のリダイレクト構成

以下のリダイレクトスクリプトをコピーして貼り付けます。

when HTTP_REQUEST {

HTTP::redirect https://[HTTP::host][HTTP::uri]

}

aFleX スクリプトをバーチャルサーバーポート 80 にバインドする必要があります。

16.2 VIP への AFLEX スクリプトの適用

- 1. [Config Mode] > [SLB] > [Virtual Server] > [WS-VIP] > [Port] > [80]を選択 します。
- 2. [aFleX]ドロップダウンメニューをクリックし、[Redirect]を選択します。
- 3. [OK]の次に[Save]をクリックし、構成の変更を保存します。

Source NAT Pool:	•
aFleX:	Redirect Multiple
HTTP Template:	▼
RAM Caching Template:	•

図 45 : aFleX の構成

16.3 AFLEX サービスの確認

aFleX スクリプトが機能していることを確認するには、Web ブラウザーを開いて http://example.com を表示します。ブラウザーがこの URL リクエストを受け取り、クライアント URL アドレスが「http://example.com」から「https:example.com」に変わります。



図 46 : SharePoint Web サイトの例

17.まとめと結論

本書で説明されている構成手順は、Microsoft SharePoint 2010 Server のための AX の設定方法で す。AX デバイスを使って SharePoint Web フロントエンド(WFE)サーバーのロードバランスを行 うことで、主に以下のような利点が得られます。

- SharePoint サーバーの高可用性を実現し、Web サイトの障害を防ぎます。ユーザーは悪 影響を被らずにアプリケーションにアクセスできます。
- クライアントトラフィックを複数の SharePoint WFE サーバーにシームレスに分配し、 サイトの拡張性を高めます。
- SSL オフロード、HTTP 圧縮、RAM キャッシング、コネクションリユースを開始することで、コネクションスループットの向上、エンドユーザレスポンスの高速化、WFE の CPU 使用率の低下を実現します。
- サイトのパフォーマンスとエンドユーザーからの信頼度が向上します。

AX シリーズ Advanced Traffic Manager を使用することで、すべての Microsoft SharePoint 2010 ユーザーが大きな利益を得られます。AX シリーズ製品の詳細については、以下の URL を参照し てください。

http://a10networks.com/products/axseries.php

http://a10networks.com/resources/solutionsheets.php

http://a10networks.com/resources/casestudies.php

18.付録

AX シリーズの CLI の構成例:

<u>基本的な SharePoint 構成</u>

basicconfig-ax1#show run
interfaces management
enable
hostname basicconfig-ax1
clock timezone Europe/Dublin
interface management
ip address 192.168.18.41 255.255.255.0
health monitor HTTP
method http
slb server WS1 172.16.1.5
health-check HTTP
port 443 tcp
slb server WS2 172.16.1.6
health-check HTTP
port 443 tcp
slb service-group SharePoint Servers tcp

health-check HTTP member WS1:443 member WS2:443 slb template persist source-ip "IP Persistence" timeout 10 slb virtual-server WS-VIP 172.16.1.200 port 443 https name _172.16.1.200_TCP_443 service-group SharePoint Servers template persist source-ip "IP Persistence" end

<u>高度な SharePoint 構成</u>

advconfig-ax2#show run interfaces management enable hostname advconfig-ax2 clock timezone Europe/Dublin interface management device 1 ip nat pool SNAT 172.16.1.250 172.16.1.250 netmask /24 health monitor HTTP method http url GET / enable-buff-debug slb server WS1 172.16.1.5 conn-limit 8000000 port 80 tcp conn-limit 8000000 slb server WS2 172.16.1.6 conn-limit 8000000 port 80 tcp conn-limit 8000000 slb service-group SG-80 tcp member WS1:80 member WS2:80 slb template connection-reuse "SharePoint Connection" slb template cache "SharePoint RAM Caching" max-content-size 4194303 min-content-size 10 slb template http HTTP compression enable compression minimum-content-length 120 slb template client-ssl WS cert WS key WS slb template persist source-ip "Source IP Persistence" match-type server slb virtual-server WS-VIP 172.16.1.200 port 443 https name _172.16.1.200_HTTPS_443 source-nat pool SNAT service-group SG-80

```
template tcp-proxy "TCP Proxy"
template http HTTP
template cache "SharePoint RAM Caching"
template client-ssl WS
template connection-reuse "SharePoint Connection"
template persist source-ip "Source IP Persistence"
port 80 http
name _172.16.1.200_HTTP_80
service-group SG-80
aflex Redirect
end
```



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 Email: jinfo@a10networks.com http://www.a10networks.co.jp お問い合わせ

(c) A10 Networks, Inc. and/or its affiliates. All rights reserved.