企業ユーザ用 Cisco Japan Virtualization System and Interoperability Lab（J-VSL）

Cisco Japan Virtualization System and Interoperability Lab (J-VSL) for Enterprise Customers

高可用性、フェールオーバー テスト ESXi 編

2011 年 7 月

Text Part Number: OL-24835-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

企業ユーザ用 Cisco Japan Virtualization System and Interoperability Lab（JVSL）- Phase2 Pass1 Set1 テスト

CONTENTS

はじめに

マニュアルの構成

このマニュアルの構成は、次のとおりです。

- 第 1 章「Japan Virtualization System and Interoperability Lab（J-VSL）の紹介」
- 第 2 章「設計と実装」
- 第 3 章「テスト ケース」
- 付録 A「設定」

表記法

このマニュアルでは、次の表記法を使用しています。

項目	表記法
手順で選択されるコマンド、キーワード、特殊な用語、およびオプション	**太字**
値、新規用語、または重要な用語を指定する変数	*イタリック体*
表示されるセッション情報、システム情報、パス、およびファイル名	`screen` フォント
ユーザが入力する情報	**太字の screen** フォント
ユーザが入力する変数	*イタリック体の screen* フォント
メニュー項目とボタン名	**太字**
メニュー項目を選択する順番	[Option] > [Network Preferences]

ヒント 製品を最大限に活用できる情報を示します。

（注） 「*注釈*」です。次に進む前に検討する必要がある重要情報、役に立つ情報、このマニュアル以外の参照資料などを紹介しています。

注意 「*要注意*」の意味です。機器の損傷、データの損失、またはネットワーク セキュリティの侵害を予防するための注意事項が記述されています。

警告 **ユーザの身体、ソフトウェアの状態、または機器に被害が及ぶのを防ぐために、留意する必要がある注意事項が記述されています。記載された注意事項に従わない場合に、結果として発生するセキュリティ侵害が明確に特定されています。**

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

関連資料

相互運用性テスト編のテスト レポートについては、次の URL を参照してください。
http://www.cisco.com/web/JP/partners/localization/systest/dctest/index_dctest.html

CHAPTER 1

Japan Virtualization System and Interoperability Lab（J-VSL）の紹介

Japan Virtualization System and Interoperability Lab（J-VSL）は、日本市場向けのデータセンター設計ソリューションを提供します。このフェーズで使用するデバイスは、主に、日本国内のベンダー製のストレージを搭載した Cisco サーバ（UCS）とスイッチです。

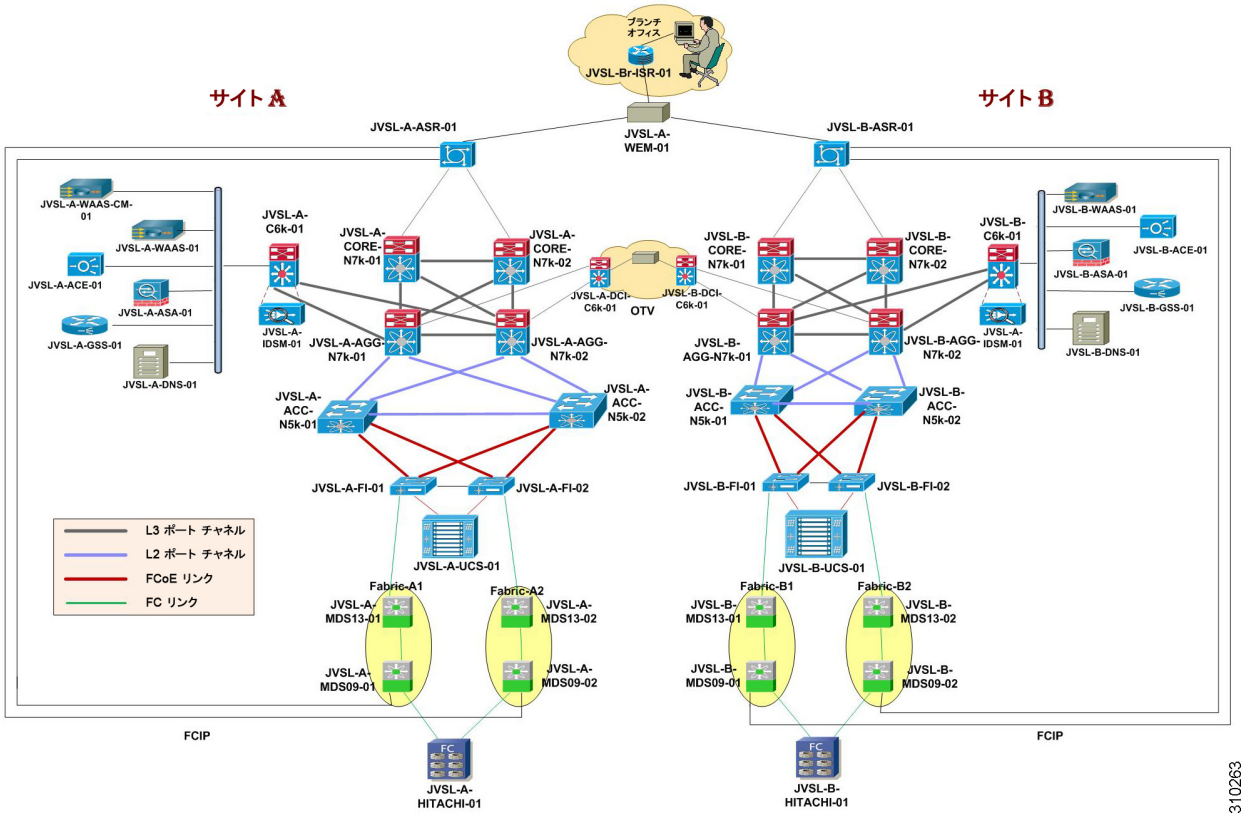
高可用性、フェールオーバー テストは、Phase1 の対象となった要素に基づいて構築されていますが、さらにデバイス、機能、範囲が追加されています。テストが実行されると、結果は観察されたとおりに報告されます。つまり、J-VSL の目標は、テストに透明性を導入し、ここに挙げる推奨設計をお客様が安心して配備できるようにすることです。

高可用性、フェールオーバー テスト ESXi 編の対象範囲は次のとおりです。

- OTV 経由の Cisco UCS サーバ間のライブ マイグレーション
- VMware ESXi 4.1 を使用した Cisco UCS 上の MS-Exchange 2010 実装
- ACE Virtual Data Center（VDC; 仮想データセンター）実装
- UCS 上の Cisco VN-Link 実装
- GSS を使用したサイト フェールオーバー

J-VSL Phase2-Pass1 のトポロジ

図 1-1　J-VSL Phase2-Pass1 のトポロジ



J-VSL Phase2-Pass1 のトポロジは、次のデバイスが設置された 2 つのサイトで構成されます。

デバイスの詳細

シスコ デバイス

No.	デバイス	モデル	オペレーティング システム/IOS
1	NEXUS	7010	NX-OS 5.1.3
2	NEXUS	5020	NX-OS 5.0(3)N1(1a)
3	MDS	9513	NX-OS 5.0(4)
4	MDS	9509	NX-OS 5.0(4)
5	CAT6K	6509	IOS 12.2(33)SXH8
6	ACE	4710	A4(1.1)
7	WAAS	7341	4.2
8	WAAS モジュール	NME-WAE-502	4.2
9	ASA	5580-20	8.4.1
10	IPS	IDSM2	7.0.2
11	ASR	1002	15.1(1)s
12	ISR	2821	12.4(15)T12
13	GSS	4492	3.1(0)

アプリケーション

No.	ベンダー	OS/アプリケーション	バージョン
1	VMWARE	ESXi	4.1E
2	VMWARE	vCenter	4.1 J
3	シスコ	Nexus 1000V	NX-OS 4.0(4)

Cisco UCS

No.	デバイス	モデル	オペレーティング システム/IOS
1	ファブリック インターコネクト	6140XP	UCS Manager 1.4(1m)
2	シャーシ	5108	
3	ファブリック エクステンダ	2104XP	
4	ブレード サーバ	B-440 M1	
		B-250 M2	
		B-200 M2	
5	インターフェイス カード	M81KR	

CHAPTER 2

設計と実装

ここで説明する内容は、次のとおりです。

OTV 経由の Cisco UCS サーバ間のライブ マイグレーション

Cisco UCS

Cisco Unified Computing System には、次の機能を実行するハイエンド ブレード サーバが含まれています。

- データセンター リソースを合理化して、総所有コストを削減します。
- サービスの提供規模を調整して、ビジネスの俊敏性を向上させます。
- セットアップ、管理、電力、冷却、およびケーブル敷設が必要なデバイスの数を大幅に削減します。

高可用性、フェールオーバー テスト ESXi 編 のトポロジのセットアップ環境では、Cisco Unified Computing System は次のコンポーネントで構築されます。

- 回線速度、低遅延、ロスレス インターコネクト スイッチを提供する、Cisco UCS 6140XP シリーズ ファブリック インターコネクト
- 6 Rack Unit（RU; ラック ユニット）の筐体内に最大 8 台の半幅ブレード サーバまたは最大 4 台の全幅ブレード サーバ、および 2 台のファブリック エクステンダを収納可能な、Cisco UCS 5108 シリーズ ブレード サーバ シャーシ
- ブレード サーバ シャーシ内でファブリックを統合して最大 4 つの 10 Gbps 接続を実現する、Cisco UCS 2104XP シリーズ ファブリック エクステンダ
- アプリケーション ニーズ、エネルギー消費、および仮想化への対応を強化できる、Cisco UCS B サーバ 現行のセットアップ環境で使用されているブレード サーバ モデルとその仕様を次に示します。

  - B-440 M1：Intel Xeon x7560、プロセッサあたり 8 コア、256GB RDIMM
  - B-250 M2：Intel Xeon x5680、プロセッサあたり 6 コア、384GB RDIMM
  - B-200 M2：Intel Xeon x5680、プロセッサあたり 6 コア、96GB RDIMM
- Cisco UCS B-Series Network Adapter M81KR（仮想化、既存のドライバ スタックとの互換性、および効率的な高性能イーサネットに最適化済み）
- 集中管理機能を提供する Cisco UCS Manager

Cisco OTV

シスコの革新的な LAN 拡張テクノロジーである Overlay Transport Virtualization（OTV）は、任意のトランスポート インフラストラクチャ上でレイヤ 2 拡張機能を提供するように設計された IP ベースの機能です。

OTV には次のようなメリットがあります。

- 分散したデータセンター全体でのレイヤ 2 アプリケーションの拡張を容易にします。
- ユーザは次のものを展開できます。
  - サイト間の Data Center Interconnect（DCI; データセンター インターコネクト）。既存のネットワーク設計を変更または再設計する必要はありません。
  - 地理的に分散したデータセンター全体にわたる仮想コンピューティング リソースとクラスタ。これにより、透過的なワークロード モビリティ、ビジネスの弾力性、コンピューティング リソースの高い効率性を実現できます。

高可用性、フェールオーバー テスト ESXi 編 のトポロジのセットアップ環境では、OTV 機能は専用の VDC に実装されます。これらの VDC は、ポイントツーポイント展開として、集約レイヤ デバイス（Nexus 7010）と DCI レイヤ デバイス（Cat 6504）の両方に接続されます。サイト A とサイト B で別々の OTV VDC（JVSL-A-OTV-01 と JVSL-B-OTV-01）が作成されます。

HSRP グループが同一の OTV VLAN が集約スイッチ内で構築されます。これは両方のサイト（サイト A とサイト B）に存在します。サイト A からサイト B への OTV VLAN 拡張は、設定によって実現されます。

VMotion

VMware vCenter の機能である VMotion は、データセンター内の ESX/ESXi ホスト間で I/O 機能を転送するための VMware 独自の能力です。VMotion を使用すれば、ESX ホスト間の仮想マシンのライブ マイグレーションが可能になります。リアルタイムでストレージを共有化しても、エンドユーザまたは移行する仮想マシンのリソースやサービスを利用しているユーザに影響はありません。

この機能を使用すれば、仮想インフラストラクチャ内の仮想マシンをシャットダウンすることなく物理 ESX/ESXi ホストを保守できるため、保守実施中もダウンタイムやパフォーマンスの低下は発生しません。

VMware VMotion に関する要件

VMware VMotion アプリケーションのモビリティは、特定のインフラストラクチャ要件に基づきます。

- 2 台の VMware vSphere サーバ間の最大遅延は 5 ミリ秒（ms）以下にする必要があります。
- 送信元 VMware ESX サーバと宛先 VMware ESX サーバは、同じ IP サブネットとブロードキャストのドメイン内のプライベート VMware VMotion ネットワークを使用します。

- 送信元 VMware ESX サーバと宛先 VMware ESX サーバから、仮想マシン内の IP サブネットにアクセスできます。仮想マシンは、宛先 VMware ESX サーバに移動しても IP アドレスを維持するため、外部（TCP クライアントなど）との通信が途絶えることはありません。
- 仮想マシンで使用されるブート デバイスなどのデータ保存場所は、常にアクティブにしておき送信元 VMware ESX サーバと宛先 VMware ESX サーバの両方からアクセスできるようにする必要があります。
- VMware vCenter サーバから VMware ESX サーバへのアクセスがサイト A とサイト B で実行可能になれば、移行は完了です。

ライブ マイグレーションの実装

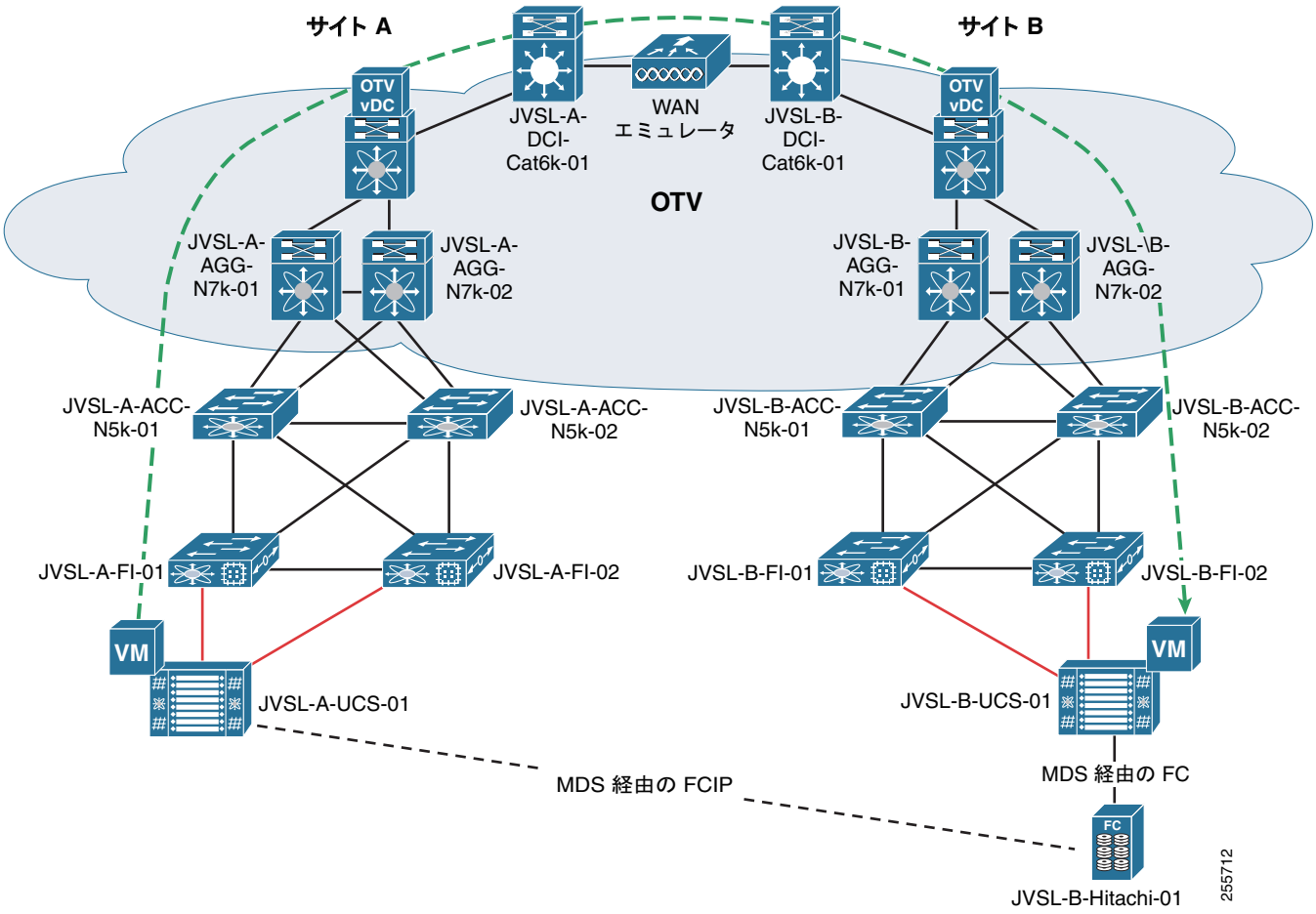
高可用性、フェールオーバー テスト ESXi 編 のトポロジのセットアップ環境で VMotion を両方のサイトに実装するには、VLAN と共有ストレージを拡張します。拡張 VLAN および共有ストレージ アーキテクチャによって、VLAN はサイト A からサイト B に拡張されますが、ストレージはサイト B に置かれます。仮想マシンをサイト A からサイト B に移行すると、アプリケーションはサイト B からストレージにアクセスします。ストレージはサイト A のデータセンター内のアプリケーションに対してプロビジョニングされません。そのため、ストレージのコピーは常に 1 つしか存在しません。

高可用性、フェールオーバー テスト ESXi 編 のトポロジのセットアップ環境では、次のデバイスが VMotion に関与します。

- VMware ESXi 4.1 と Nexus1000v がインストールされた Cisco UCS B440-M1 サーバ（サイト A）
- VMware vCenter 4.1 がインストールされた Cisco UCS B200-M2 サーバ（サイト A）
- VMware ESXi 4.1 と Nexus 1000v がインストールされた Cisco UCS B250-M2 サーバ（サイト B）
- DCI（OTV）接続用の Nexus 7010 と Cat 6504
- 単一の Hitachi USP VM ストレージがサイト A サーバとサイト B サーバでプロビジョニングされます。

図 2-1 に、このフェーズで使用される、OTV 上の物理インフラストラクチャ境界およびデータセンター全体での VMware VMotion の移行設計を示します。

図 2-1　ライブ マイグレーションの実装



実装手順は次のとおりです。

- サイト A の Cisco UCS B440-M1 とサイト B の Cisco UCS B250-M2 に、ESXi 4.1 をインストールします。
- サイト A の Cisco UCS B200-M2 に、vCenter 4.1 をインストールします。
- 両方の ESXi サーバを VMware vCenter EVC クラスタに追加して、CPU の非互換性を排除します。
- サイト B にある UCS サーバ、サイト A にある UCS サーバ、および両方のサーバに共通の LUN のためのホスト グループを、サイト B の Hitachi ストレージに作成します。
- 適切な VSAN とゾーンが設定された MDS スイッチを経由して、サイト B でサーバからストレージまでの冗長パスを作成します。
- 適切な VSAN とゾーンが設定され、FCIP リンクが確立された MDS スイッチを経由して、サイト A のサーバからサイト B のストレージまでの冗長パスを作成します。
- DCI セットアップを使用して、OTV vlan をサイト A 集約スイッチからサイト B 集約スイッチまで拡張します。
- 両方の ESXi ホストで VMotion 専用の VM カーネル インターフェイスを作成し、両方のホストの VMotion 機能をイネーブルにします。

Cisco UCS 内の MS-Exchange 2010 と VMware ESXi 4.1

MS Exchange 2010

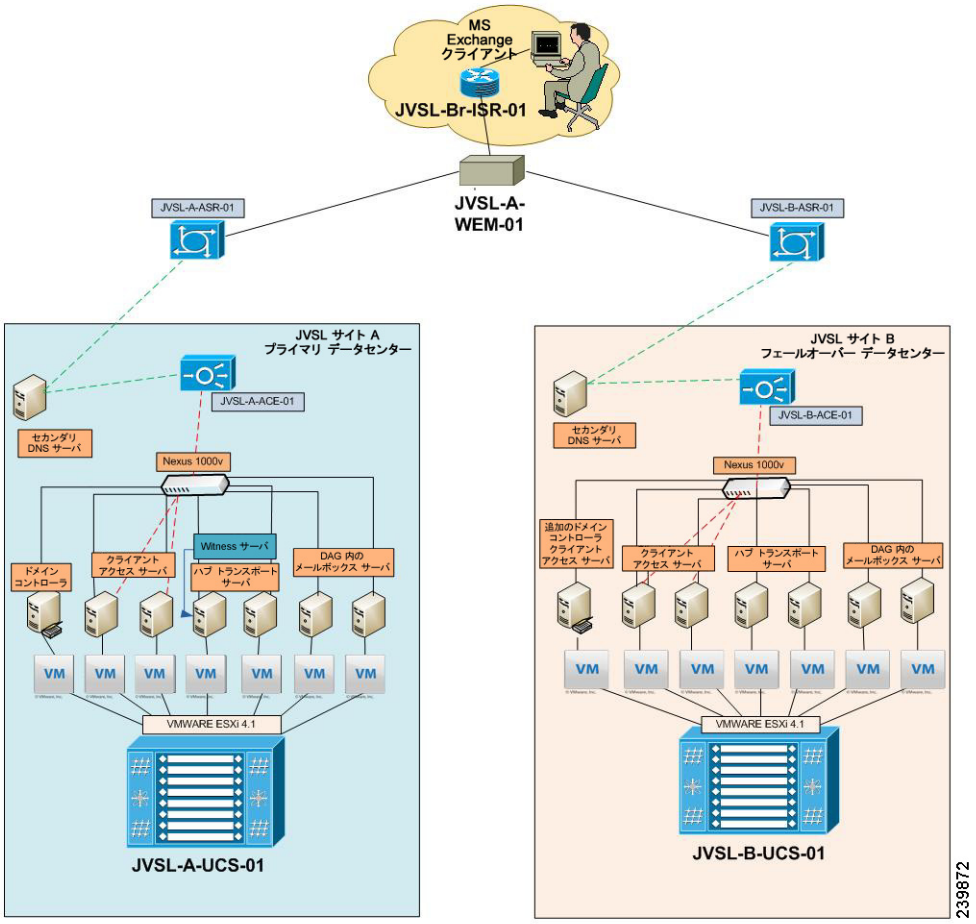
Phase2-Pass1 では、MS Exchange 2010 ログ シッピング機能とデータベース可用性グループ機能を実装し、ハイ アベイラビリティとサイト レベル フェールオーバーについてテストします。

ログ シッピング : ログ ファイルとデータベース ファイルをバックアップするプロセスです。Exchange 2010 は、SMB の代わりに TCP/IP を使用してログ ファイルのコピーとシーディングを行います。

Database Availability Group（DAG; データベース可用性グループ）: DAG は、新しいハイ アベイラビリティおよびサイト復元力機能で、Exchange 2007 の CCR/SCR/SCC に代わるものです。

実装の詳細

図 2-2　MS-Exchange 2010 の実装の詳細



J-VSL での MS EXCHANGE 2010 の実装は、J-VSL サイト A（プライマリ データセンター）と J-VSL サイト B（フェールオーバー データセンター）など、2 つのサイトで構成されます。各サイトは、7 台の仮想マシン（AD および DNS サーバ用に 1 台、クライアント アクセス サーバ、ハブ トランスポート サーバ、およびメールボックス サーバ用に 2 台ずつ）で構成されます。J-VSL サイト A では、プライマリ Active Directory サービスと DNS サービスを実行するグローバル カタログ サーバが設置され、ドメイン名（esxjvsl.com）が設定されます。フェールオーバー データセンター（サイト B）では、追加のドメイン コントローラがインストールされ、同じドメイン用に設定されます。

すべての仮想サーバが、500GB LUN を使用した UCS B-440 M1 ブレード サーバ上の ESXi 4.1 にインストールされます。これは、仮想マシンをサイト A の SAN とサイト B の UCS B-250 M2 ブレード サーバ上で起動するためです。ESXi サーバを管理するために、VCenter が同じシャーシ内の UCS B-200 M2 ブレード サーバにインストールされます。両サイトでクライアント クエリー解決用のセカンダリ DNS サーバが 2 台の外部ブレード サーバにインストールされます。

MS-Exchange コンポーネントには次のものが含まれています。

- サイトごとに 2 台のハブ トランスポート サーバが、組織内のすべてのメール フローを処理し、トランスポート ルール（ジャーナリング ポリシー）を適用し、受信者メールボックスにメッセージを配信します。ハブ トランスポートの組織内ロード バランシングが自動的に実施されます。
- 2 台のクライアント アクセス サーバは、すべての着信 / 発信クライアント接続を処理します。
- JVSLDAG という名前の同じ DAG 内に設定されたサイトごとに 2 台ずつのメールボックス サーバ
- 各メールボックス サーバに、メール データベースを保存するための 100GB LUN が搭載されています。
- 両方のクライアント アクセス サーバが、MS-Exchange トラフィックのリダイレクトとロード バランシングを実行する ACE に接続されています。
- ACE VIP の DNS クエリー解決が CAT6k に接続されたセカンダリ DNS サーバによって実行され、URL がクライアント要求に送信されます。

グローバル カタログ サーバの実装

グローバル カタログ サーバ（プライマリ AD および DNS）は、プライマリ データセンター内の Windows 2008 サーバと一緒にインストールされます。Active Directory ユーザ、コンピュータ、およびドメイン サービスがグローバル カタログ サーバによって提供されます。

プライマリ DNS サーバは、前方参照ゾーンと後方参照ゾーンの両方が同じドメイン用に設定された、グローバル カタログ サーバ上で動作します。このサーバには、Web サーバ IIS と必須機能（HTTP プロキシ上の RPC など）、リモート サーバ管理ツール、Windows パワー シェルなどもインストールされ、動作しています。Exchange ロールをインストールするすべてのメンバ サーバに、ドメイン管理権限および Exchange Trusted Subsystem アカウント権限を付与する必要があります。

セカンダリ DNS サーバの実装

セカンダリ DNS サーバは、グローバル カタログ サーバの下で動作し、プライマリ DNS サーバに対する完全な委任制御機能を備えています。セカンダリ DNS サーバはサービス スイッチ（Cat6k）に接続します。セカンダリ DNS サーバ内のすべての更新は、プライマリ DNS サーバに反映されます。これは、セカンダリ DNS サーバがプライマリ DNS サーバに対して完全な委任制御機能を備えているためです。クライアントの Outlook Web Access URL のスタティック レコードはセカンダリ DNS サーバ内で作成されます。これは、ACE の仮想サーバ IP アドレスを指します。

クライアントが URL を使用してメールボックスにアクセスすると、セカンダリ DNS サーバがそのクエリーを ACE に転送します。ACE は、ロード バランスを実施して、クライアント アクセス ロール サーバのいずれかにクエリーを転送します。Outlook Web Access URL が解決され、セカンダリ DNS サーバ経由でクライアントに送信されます。

ユーザ入力を受け取ると、クライアント アクセス ロール サーバは Active Directory でユーザ情報を検索し、そのユーザがメールボックスにアクセスできるようになります。

クライアント アクセス サーバの実装

MS Exchange 2010 のインストールに関する前提条件は、クライアント アクセス ロールのインストールを開始する前に実施する必要があります。CAS ロールのインストールはサーバ単位で行う必要があります。プライマリ データセンターの CAS サーバ名は SACAS1.ESXJVSL.COM と SACAS2.ESXJVSL.COM で、フェールオーバー データセンターの CAS サーバ名は SBCAS1.ESXJVSL.COM と SBCAS2.ESXJVSL.COM です。OWA などのクライアント アクセス URL は Exchange 管理コンソールで確認できます。プライマリ データセンターの URL は https://SACAS1.ESXJVSL.com/owa および

https://SACAS2.ESXJVSL.com/owa、フェールオーバー データセンターの URL は https://SBCAS2.ESXJVSL.com/owa および https://SBCAS2.ESXJVSL.com/owa の形式になります。インストールが完了したら、上記 URL を使用して Outlook Web Access を確認します。

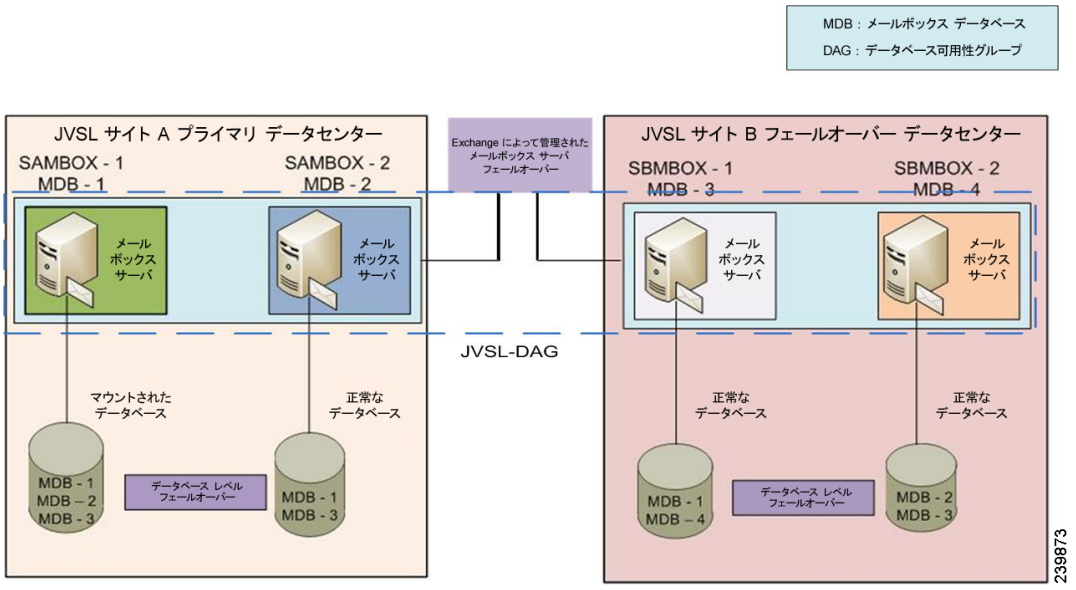
ハブ トランスポート サーバの実装

MS Exchange 2010 のインストールに関する前提条件は、ハブ トランスポート ロールのインストールを開始する前に実行する必要があります。また、ハブ トランスポート ロールのインストールは、1 つずつ実行する必要があります。プライマリ データセンターのハブ トランスポート サーバ名は SAHUB1.ESXJVSL.com と SAHUB2.ESXJVSL.com で、フェールオーバー データセンターのハブ トランスポート サーバ名は SBHUB2.ESXJVSL.com と SBHUB2.ESXJVSL.com です。

メールボックス サーバの実装

MS Exchange 2010 のインストールに関する前提条件は、ハブ トランスポート ロールのインストールを開始する前に実行する必要があります。また、メールボックス ロールのインストールは、1 つずつ実施する必要があります。両サイトのメールボックス サーバ名は、それぞれ、SAMBOX1.ESXJVSL.com と SAMBOX2.ESXJVSL.com、SBMBOX1.ESXJVSL.com と SBMBOX2.ESXJVSL.com です。メールボックス ロールが完了したら、両サイトのメールボックス サーバのメールボックス データベースは、ステータスがマウント状態で Exchange 管理コンソールに表示されます。

図 2-3　　DAG の実装



両サイトの全メールボックス サーバでメールボックス データベースがマウントされたら、DAG が作成可能です。上の図では、プライマリ データセンターとフェールオーバー データセンターの両方に JVSLDAG という名前の単一の DAG グループがあります。

作成するには、Exchange 管理シェルで次のコマンドを使用します。

```
Add-databaseavailabilitygroupserver  -identity JVSLDAG  -mailboxserver SAMBOX1
```

```
Add-databaseavailabilitygroupserver  -identity JVSLDAG  -mailboxserver SAMBOX2
Add-databaseavailabilitygroupserver  -identity JVSLDAG  -mailboxserver SBMBOX1
Add-databaseavailabilitygroupserver  -identity JVSLDAG  -mailboxserver SBMBOX2
```

DAG が作成されたら、次のコマンドを使用して、そのメンバ サーバをチェックできます。

```
Get-databaseavailabilitygroupserver JVSL DAG | fl servers
```

ここでは、スタティック IP アドレスを持つ 2 つの DAG 仮想ネットワークをレプリケーション ネットワーク用に設定します。

DAG にスタティック IP アドレスを割り当てるには、Exchange 管理シェルで次のコマンドを使用します。

```
Set-databaseavailabilitygroup -identity JVSLDAG -databaseavailabilitygroupipaddress <DAG
ip address1> <DAG ip address2>
```

新しい DAG グループが作成されたら、両方のサイトの全メールボックス サーバが Exchange 管理コンソール経由でこの DAG グループに追加されます。サイト間とサイト内のメールボックス データベースのフェールオーバーとメールボックス サーバの可用性については、メールボックス データベースのコピーをすべてのメールボックス サーバに追加します。

メールボックス データベースのコピーは、Exchange 管理シェルで次のコマンドを使用して追加できます。

```
Add-mailboxdatabasecopy -identity JVSLDAG maildatabase MDB1 -mailboxserver SAMBOX2
-activationpreference 2
Add-mailboxdatabasecopy -identity JVSLDAG maildatabase MDB1 -mailboxserver SBMBOX1
-activationpreference 3
Add-mailboxdatabasecopy -identity JVSLDAG maildatabase MDB3 -mailboxserver SBMBOX2
-activationpreference 2
Add-mailboxdatabasecopy -identity JVSLDAG maildatabase MDB3 -mailboxserver SAMBOX1
-activationpreference 2
```

Cisco ACE Virtual Data Center（VDC）の実装

AVDC は、主要なデータセンター製品を統合して、簡略化されたコスト効率の高いアプリケーション配布インフラストラクチャを提供することに重点が置かれたソリューションです。AVDC に統合された製品には、ACE モジュール、ACE アプライアンス、Nexus 7000、UCS、VMware、サード パーティ アプリケーション ベンダーなどがあります。

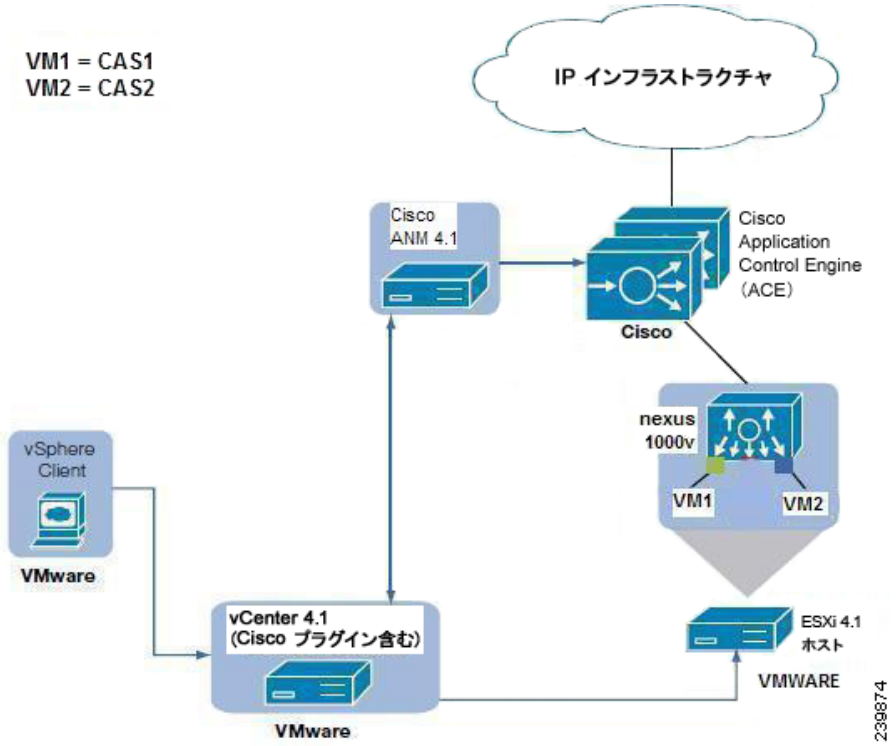
AVDC の主要機能の目的は、IT 組織が仮想データセンターで直面するアプリケーション配布の主な問題を解決することです。これらの機能には、仮想マシンのインテリジェンス、パフォーマンスとスケーラビリティ、単純化、柔軟性と協調の改善、およびサード パーティ製品（VMware vCenter など）との統合などがあります。この統合により、Cisco ACE はネットワーク内の変化に動的に対応したり、ネットワーク イベントを共有したりすることができます。

シスコでは、Cisco Data Center Business Advantage（DCBA）ソリューションの既存のポートフォリオの強化を進めており、これによって仮想データセンターの展開が可能になります。Cisco AVDC は、Cisco Data Center Business Advantage ポートフォリオの一部で、アプリケーションを使用した計算と切り替えを統一することにより、コスト効率の良い、合理化されたアプリケーション配布インフラストラクチャを実現します。

AVDC は Cisco Application Network Management（ANM）を使用します。ANM は、次の機能を実行するクライアント サーバ アプリケーションです。

- サポートされているデータセンター デバイスの機能の設定、モニタ、およびトラブルシューティング。
- 運用部門、アプリケーション オーナー、およびサーバ管理スタッフが、ネットワーク設定やトポロジの変更に関する知識や技術を使用せずに、ネットワークベースのサービスをアクティブにしたり一時的に停止したりするためのポリシーの作成。

図 2-4　AVDC の概要



AVDC を 高可用性、フェールオーバー テスト ESXi 編 で実装するのは、複数のサイトに展開された ACE を直接制御するためです。この実装は、Cisco ANM と ACE を統合し、vCenter にインストールされた vSphere クライアント経由で ACE にアクセスして行います。次のコンポーネントが、Phase2-Pass1 のセットアップ環境での Cisco AVDC 実装に含まれています。

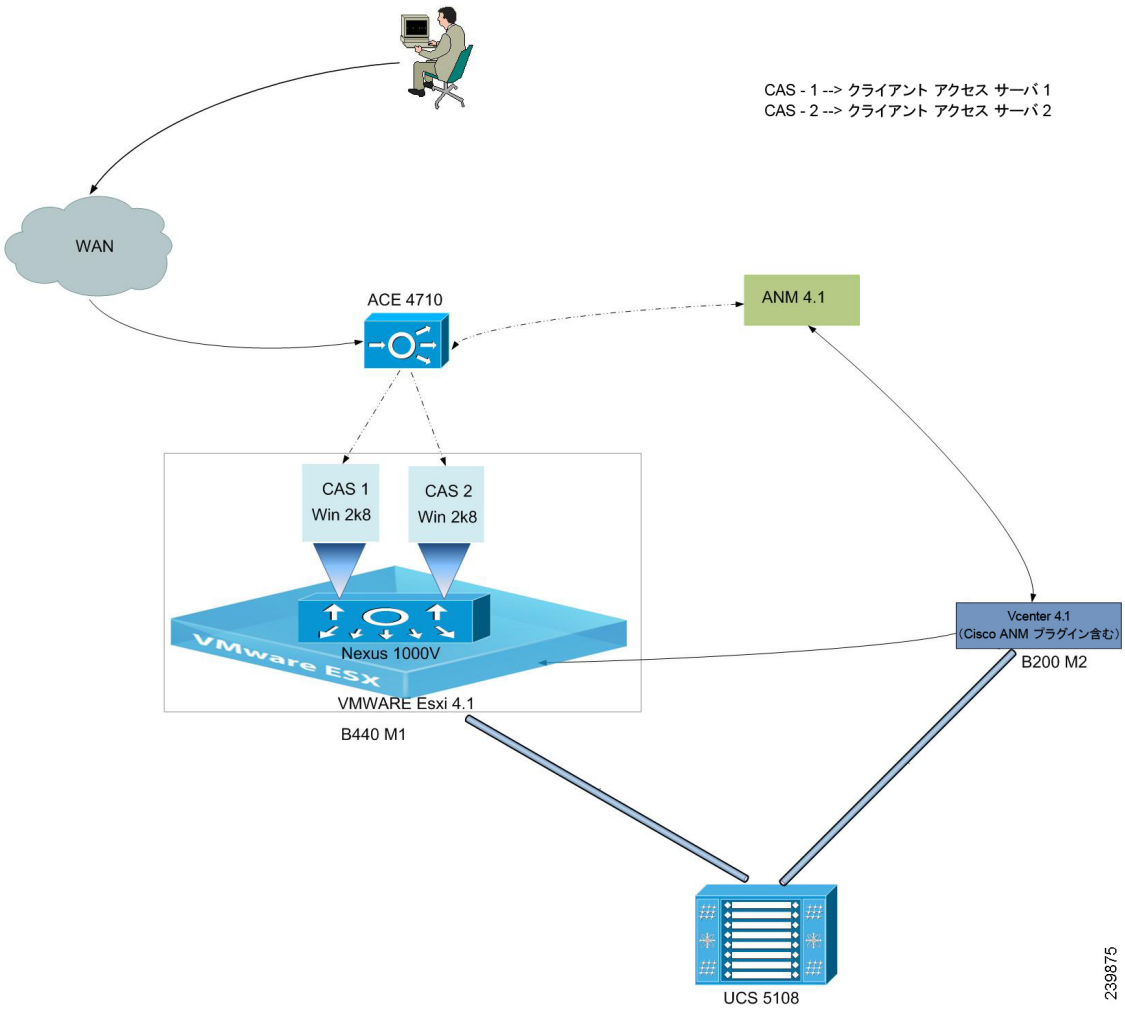
- Cisco ACE 4710 アプライアンス
- Cisco UCS ブレード サーバにインストールされた ESXi ホストを管理するための VMware vCenter 4.1
- RHEL にインストールされた Cisco ANM
- Vcenter にインストールして登録された AVDC プラグイン

Cisco AVDC のセットアップ手順を次に示します。

- Red Hat Linux に ANM 4.1 をインストールします。
- ANM GUI の [Guided setup] > [Import devices] を使用して、両サイトで VIP を使用する ACE デバイスを ANM に追加します。
- [Device] タブを使用して、ACE（JVSL-A-ACE-01 と JVSL-B-ACE-01）デバイスにアクセスできるかどうかを確認します。
- ACE をモニタするように SNMP を設定します。
- [Guided Setup] > [Import Device] タブを使用して、vCenter サーバ詳細を ANM に追加します。
- vCenter の管理者ログイン詳細を入力します。
- ここで、VMware vCenter サーバと ANM サーバの属性を指定することによって ANM プラグインを登録し、ANM が HTTPS とデフォルト ポートの 443 を使用して VMware vCenter サーバおよび vSphere クライアントと通信できるようにします。
- Cisco ANM ソフトウェアにより、VMware vCenter プラグインがインストールされます。

- vSphere クライアントから ANM GUI にアクセスできるかどうかを確認します。

図 2-5　AVDC の実装



UCS 上の Cisco VN-Link の実装

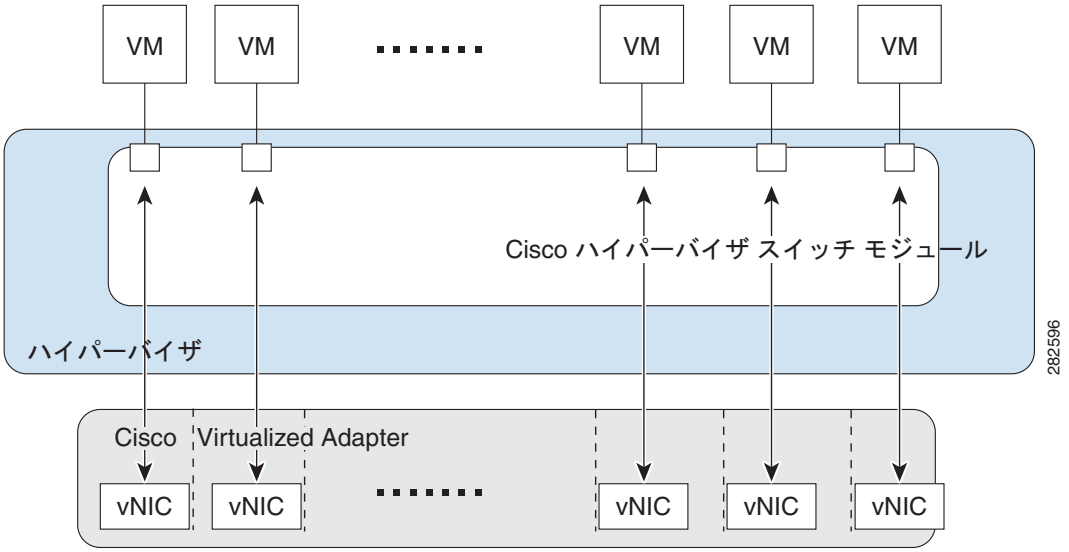
Cisco VN-Link

Cisco Virtual Network Link（VN-Link）は、仮想マシン上の vNIC と VN-Link がイネーブルにされた Cisco スイッチ間で論理リンクが構築されたことを意味します。このマッピングは、ケーブルを使用してアクセス レイヤ スイッチのネットワーク ポートに NIC を接続することと論理的に等価です。

シスコでは、Distributed Virtual Switch（DVS; 分散仮想スイッチ）フレームワークを使用して、ネットワーキング ソリューションのポートフォリオを提供しています。このポートフォリオは、分散ハイパーバイザ レイヤ内で直接動作し、他のシスコ ネットワーキング製品との互換性や一貫性を維持したフィーチャ セットと運用モデルを提供できます。このアプローチによって、サーバの仮想化に伴う新

しい要件を満たす、エンドツーエンドのネットワーク ソリューションが実現されます。具体的には、現行のネットワーク運用モデルと調和した方法で個々の仮想マシンのインターフェイスを識別、設定、モニタ、移行、診断できるようにする新しい機能セットを導入します。

図 2-6　　VN-Link のロジック



DVS フレームワークは、VIC アダプタを搭載した Cisco UCS サーバ上の仮想マシンでハードウェア内 VN リンク機能を利用できるようにします。このアプローチによって、サーバの仮想化に伴う新しい要件を満たす、エンドツーエンドのネットワーク ソリューションが実現されます。ハードウェア内 VN リンクを使用した場合、同じホスト上の 2 つの VM 間のレイヤ 2 トラフィックは DVS 上でローカルには切り替わりませんが、UCS-6100 にアップストリーム送信されることでポリシー適用と切り替えが行われます。切り替えは、ファブリック インターコネクト（ハードウェア）で行われます。これにより、ネットワーク ポリシーを仮想マシン間のトラフィックに適用できます。

次のコンポーネントが、Phase2-Pass1 のセットアップ環境での Cisco VN-Link 実装に含まれています。

- VMware ESXi 4.1 がインストールされた Cisco UCS B-200 サーバ
- ESXi ホストを管理するための VMware vCenter 4.1
- ネットワークベースの管理タスクの一部を処理するために VMware vCenter と統合された Cisco UCS 管理ソフトウェア

Cisco VN-Link のセットアップ手順を次に示します。

- ダイナミック vNIC 接続ポリシーを作成して、UCS ホストのサービス プロファイルに適用します。
- vCenter 拡張ファイルを Cisco UCS Manager から vCenter にエクスポートします。
- vCenter 拡張ファイルを VMware vCenter に登録します。拡張ファイルを VMware vCenter に登録するまで、Cisco UCS インスタンスを確認することはできません。
- UCS Manager 経由で VMware vCenter 内の分散仮想スイッチのコンポーネントを定義します。
- Cisco UCS Manager でポート プロファイルとポート プロファイル クライアントを作成します。
- vCenter サーバ上ですべてのポート プロファイルが正常に作成されていることを確認します。
- それぞれの VEM を ESX ホストにインストールします。
- VEM をインストールしたら、ESXi ホストを vNetwork 分散スイッチに追加します。
- VM が vCenter に追加され、正しいポート グループがマッピングされたら、UCS Manager/VM タブと vCenter インターフェイスで同じものを確認できるようになります。

GSS の実装

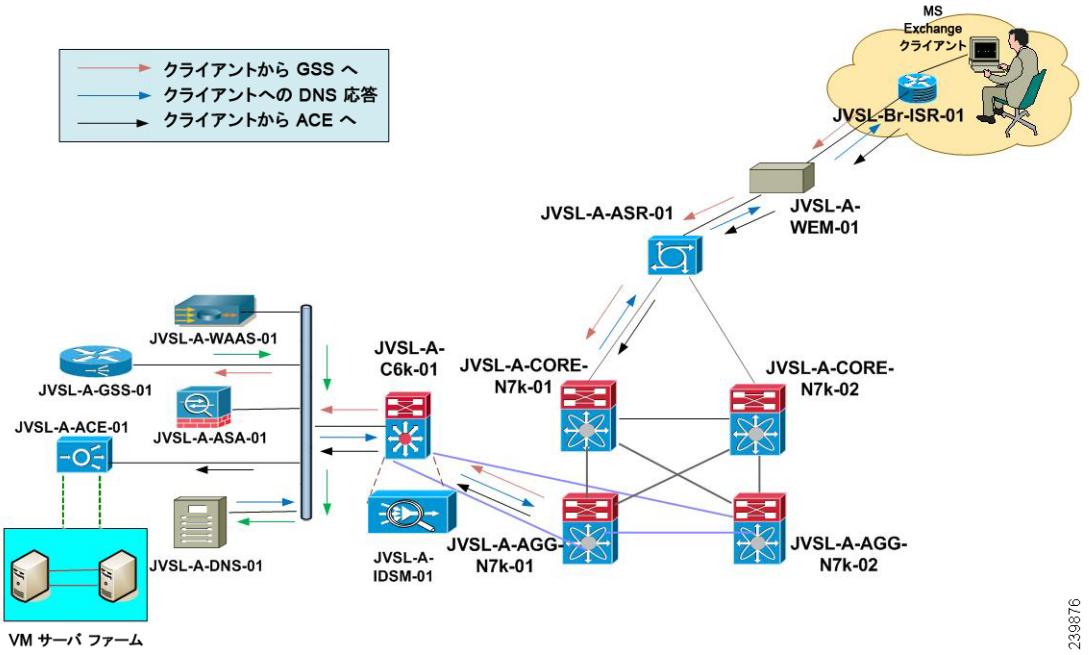
GSS

Cisco GSS デバイスとは、次世代のアプリケーション スイッチと Global Server Load Balancing（GSLB; グローバル サーバ ロードバランシング）アプライアンスを指します。これらのデバイスが Cisco ACE Application Control Engine Module と連動することによって、データセンター アプリケーションの可用性、高速化、およびセキュリティを向上させる、円滑な適用が可能なネットワーキング ソリューションが形成されます。

GSS には次の利点があります。

- 円滑な適用が可能で汎用的なビジネス継続性機能を提供することにより、アプリケーションの可用性を高めます。ネットワークが停止した場合は、GSS（Global Site Selector）が、すべてのネットワーキング トラフィックを 1 秒間に 30,000 クライアントの割合でディザスタ リカバリにリダイレクトできます。
- グローバル トラフィック管理によりアプリケーションのパフォーマンスを向上します。GSS シリーズは、複数のデータセンターにわたってすべてのデータセンター トラフィックをインテリジェントに分散します。
- 取得したテクノロジーと、GSS シリーズに統合された DNS 中心の Distributed Denial of Service（DDoS; 分散型サービス拒否）保護ソフトウェアを使用して、データセンターと重要なビジネス アプリケーションのセキュリティを強化します。
- 既存の DNS インフラストラクチャを統合します。

図 2-7　GSS の実装



実装

Phase2-Pass1 のセットアップ環境では、GSS（4492）をサイト A 内のプライマリ GSSM（JVSL-A-GSS-01）として設定します。GSS がクライアントから DNS クエリーを受け取ります。GSS がこれらの要求と DNS ルールのユーザ定義セットを照合します。

DNS ルールと一致したら、要求に対して検討すべき回答の第 1 ～ 3 候補のリストが表示されます。このトポロジでは、プライマリ DNS サーバとして JVSL-A-GSS-01 を使用し、セカンダリ DNS サーバとして JVSL-B-GSS-01 を使用するように、クライアントが設定されています。

クライアントが mail.esxjvsl.com¥owa に要求を送信すると、そのクライアントからの DNS クエリーが JVSL-A-GSS-01 に送信されます。JVSL-A-GSS-01 が到達不能の場合は、クライアント クエリーが JVSL-B-GSS-01 に配信されます。

GSS が、クライアント要求とユーザ定義 DNS ルールを照合して、DNS クエリーが一致した場合は、外部 DNS サーバ IP アドレスとして回答を送信します。その後で、GSS がそのクエリーを外部 DNS クエリーに転送して、この Exchange レコードを解決します。

クエリーが解決されたら、DNS サーバが ACE VIP アドレスを使用してクライアントに応答します。クライアントは、ACE にサーバ ロード バランシングに関するユーザ要求を送信します。

ユーザ定義 DNS クエリーは、J-VSL サイト A に対する要求を処理するときに次のように動作します。

1. 送信元アドレスが「any」と一致した場合
2. 「anything which ends with esxjvsl.com」と一致したドメインに対して
3. 回答グループが <DNS server ip> の回答から応答を選択します。
4. バランス方式として「ラウンド ロビン」を使用します。

DNS クエリーは、J-VSL サイト B に対する要求を処理するときに次のように動作します。

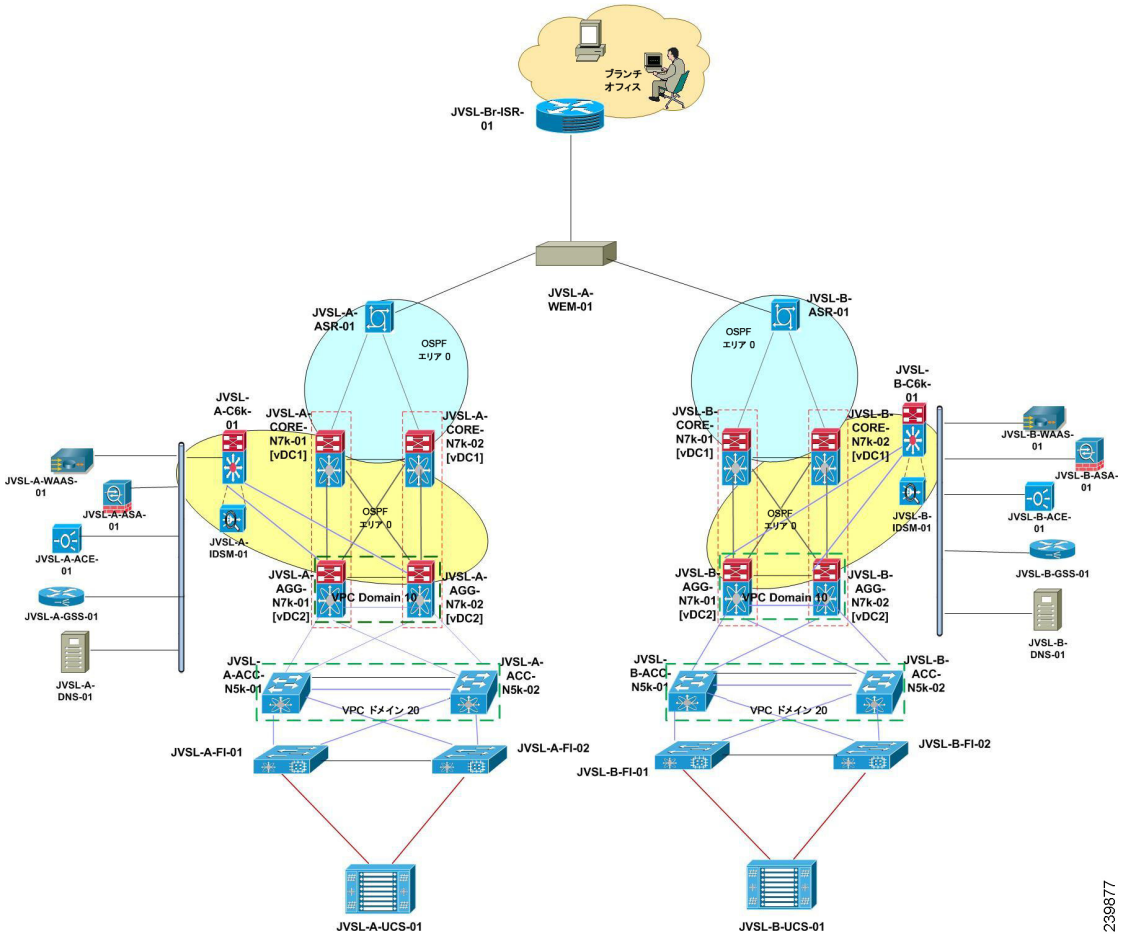
1. 送信元アドレスが「any」と一致した場合
2. 「anything which ends with esxjvsl.com」と一致したドメインに対して
3. 回答グループが <DNS server ip> の回答から応答を選択します。
4. バランス方式として「ラウンド ロビン」を使用します。

IP インフラストラクチャ

下の図に示すように、高可用性、フェールオーバー テスト ESXi 編 の IP インフラストラクチャ トポロジは両方のサイト（サイト A とサイト B）で同じです。このトポロジは、Nexus 7010 および 5020 スイッチング プラットフォームを中心にして構築されます。ブランチ オフィスで生成されたユーザ トラフィックは、WAN エミュレータに接続された ISR 経由で転送されます。両サイトの WAN エミュレータはエッジ ルータ（ASR 1002）に接続されています。コア スイッチ（Nexus 7010）は、ASR からエンド ユーザ トラフィックを受け取って、集約スイッチにルーティングします。集約スイッチは、アクセス レイヤ スイッチ（Nexus 5020）経由で UCS サーバと通信します。このサービスは、Cat 6509 に接続され、セキュリティ、サーバのロード バランス、WAN トラフィックの最適化といったさまざまな機能を実現します。

（注）　IP インフラストラクチャの使用デバイス、設計、および実装については、次の URL を参照してください。http://www.cisco.com/web/JP/partners/localization/systest/dctest/index_dctest.html

図 2-8　IP インフラストラクチャの実装



CHAPTER 3

テスト ケース

ここで説明する内容は、次のとおりです。

UCS の設定と確認

この項では、次のテスト ケースについて説明します。

ユーザ生成プールを使用した UCSM 内のサービス プロファイルの設定と確認

このテストでは、高可用性、フェールオーバー テスト ESXi 編のセットアップ環境において、UCSM のサービス プロファイル設定を確認します。

テスト手順

ユーザ生成プールを使用した UCSM 内のサービス プロファイルの設定と確認テストの手順は次のとおりです。

ステップ 1　UCSM にログインして、ナビゲーション ペインで次のプールを作成します。

a. MAC プール：[LAN] タブをクリックします。

b. WWPN プールと WWNN プール：[SAN] タブをクリックします。

c. UUID プール：[Servers] タブをクリックします。

ステップ 2　Expert Profile Creation ウィザードを使用してサービス プロファイル SP1 を作成し、次の手順を実行します。

a. [Navigation] ペインで [Server] タブをクリックします。

b. [Server] タブで、サービス プロファイルを作成する組織を選択します。

c. [Content] ペインの [Actions] メニューで、[Create Service Profile (expert)] をクリックします。

ステップ 3　サービス プロファイル SP1 に対して MAC プール、WWNN プール、UUID プールを指定し、そのプロファイルをサーバ 1 に割り当てます。

ステップ 4　サーバで、ユーザ定義プールから MAC、WWNN、および UUID が取得されたことを確認します。

予測結果

次のテスト結果が予想されます。

- サービス プロファイルのプロビジョンが成功して、ステータスが OK になります。
- サーバの MAC、WWNN、および UUID がユーザ定義プールから取得されます。

テスト結果

ユーザ生成プールを使用した UCSM 内のサービス プロファイルの設定と確認に成功しました。

ファブリック インターコネクトと Nexus 5000 間のポート チャネルの設定と確認

このテストでは、高可用性、フェールオーバー テスト ESXi 編のセットアップ環境において、ファブリック インターコネクトと Nexus 5000 間のポート チャネルを確認します。

テスト手順

ファブリック インターコネクトと Nexus 5000 接続間の PC の設定と確認テストの手順は次のとおりです。

ステップ 1　UCSM にログインして、[Navigation] ペインを選択します。

ステップ 2　[Equipment] タブをクリックして、[Fabric interconnect Expansion module] をクリックします。

ステップ 3　[Unconfigured Ethernet Ports] から [Uplink Ethernet Ports] にポートを移動します。

ステップ 4　ポート チャネルを作成して、ポートを追加し、次の手順を実行します。

a.　[LAN] タブをクリックして、[Fabric A] または [Fabric B] を選択します。

b.　新しいポート チャネル 45 を作成します。

c.　アップリンク イーサネット ポートをポート チャネル 45 に追加します。

ステップ 5　Nexus 5000 にログインして、ポート チャネルを設定し、次のコマンドを使用してイーサネット インターフェイスをバインドします。

```
interface port-channel xxx
switchport mode trunk
interface Ethernet 1/15
Channel-group xxx mode on
```

ステップ 6　UCSM と Nexus 5000 でポート チャネルのステータスを確認します。

予測結果

次のテスト結果が予想されます。

- UCSM ポート チャネルがアップして、UCS ブレード サーバが他の LAN デバイスと通信します。

テスト結果

ファブリック インターコネクトと Nexus 5000 接続間の PC の設定と確認に成功しました。

ファブリック インターコネクトと Nexus 5000 間の LAN グループへの新しい VLAN の設定と確認

このテストでは、新しい VLAN が LAN グループに追加され、その VLAN がアップリンク ポートとアップリンク ポート チャネル（高可用性、フェールオーバー テスト ESXi 編のセットアップ環境でのファブリック インターコネクトと Nexus 5000 間）で更新されることを確認します。このテストの前に、ファブリック インターコネクトと Nexus 5000 間のポート チャネルの設定と確認テストが実施されます。

テスト手順

Cisco UCS FI での新しい VLAN の設定と確認の手順は次のとおりです。

ステップ 1　UCSM にログインして、[Navigation] ペインを選択します。

ステップ 2　[LAN] タブを選択して、[LAN Cloud] と [VLANs] をクリックします。

ステップ 3　両方のファブリック インターコネクトに共通する新しい VLAN を作成します。

ステップ 4　この VLAN をいずれかのサーバ NIC に追加します。

ステップ 5　次のコマンドを使用して、VLAN が UCS FI 内のアップリンク ポート チャネルに追加されていることを確認します。

```
FI-A(nxos)# show running-config interface port-channel xx
FI-B(nxos)# show running-config interface port-channel xx
```

ステップ 6　次のコマンドを使用して、VLAN が UCS FI 内のアップリンク イーサネット ポートに追加されていることを確認します。

```
FI-A(nxos)# show running-config interface ethernet x/x
FI-B(nxos)# show running-config interface ethernet x/x
```

ステップ 7　サーバが VALN 経由でアップストリーム スイッチと通信していることを確認します。

予測結果

次のテスト結果が予想されます。

- VLAN が Cisco UCS ファブリック インターコネクト内のアップリンク ポートとアップリンク ポート チャネルに追加されます。
- サーバとアップストリーム スイッチ間の通信が正常に行われます。

テスト結果

ファブリック インターコネクトと Nexus 5000 間の LAN グループへの新しい VLAN の設定と確認に失敗しました。

発生した障害

CSCto64727 : UCS ファブリック インターコネクト内の VLAN グループに追加された新しい VLAN が更新されていません。

ファブリック インターコネクトを使用した Nexus 5000 内の vPC の設定と確認

テストの設定

アクセス（JVSL-A-ACC-N5K-01 と JVSL-A-ACC-N5K-02）スイッチとファブリック インターコネクト間で、リンクを複数接続します。アクセス スイッチとファブリック インターコネクト間のポート チャネルがアップになっていることを確認します。

テスト手順

ファブリック インターコネクトを使用した Nexus 5000 内の vPC の設定と確認テストの手順は次のとおりです。

ステップ 1　`feature vpc` コマンドを使用して vPC 機能をイネーブルにし、`show feature` コマンドを使用してイネーブルにした機能を確認します。

ステップ 2　ロール プライオリティが 5 の集約スイッチ JVSL-A-ACC-N5K-01 で vPC ドメイン 10 を作成し、そのスイッチを vPC プライマリにします。

ステップ 3　`sh vpc role` コマンドを使用して、vPC ロールを確認します。

ステップ 4　ロール プライオリティが 10 の集約スイッチ JVSL-A-ACC-N5K-02 で vPC ドメイン 10 を作成し、そのスイッチを vPC セカンダリにします。

ステップ 5　`sh vpc role` コマンドを使用して、vPC ロールを確認します。

ステップ 6　vPC-peer-keepalive リンクの宛先 IP アドレスと送信元 IP アドレスを設定し、VRF を vPC-peer-keepalive 用に設定します。

```
switch(config-vpc-domain)# peer-keepalive destination x.x.x.x source x.x.x.x
```

ステップ 7　このデバイスの vPC peer-link として使用するポート チャネルを選択し、インターフェイス コンフィギュレーション モードを開始します。

```
switch(config)# interface port-channel xxx
switch(config-if)# vpc peer-link
```

ステップ 8　インターフェイス モードで `vpc 10` コマンドを使用して、vPC メンバー ポートを vPC ドメイン 10 に追加します。

ステップ 9　`show vPC brief` コマンドを使用して vPC のステータスを確認します。

予測結果

次のテスト結果が予想されます。

- vPC がアップして実行中になります。

テスト結果

ファブリック インターコネクトを使用した Nexus 5000 内の vPC の設定と確認に成功しました。

UCS LAN 接続の設定と確認

このテストでは、UCS LAN 接続を確認します。

テスト手順

UCS LAN 接続の設定と確認テストの手順は次のとおりです。

ステップ 1　UCSM にログインして、[LAN] タブをクリックします。

ステップ 2　[LAN Cloud] と [VLANS] を選択して、[VLANs] を右クリックし、VLAN を作成します。

a.　追加する VLAN の名前と使用する VLAN ID を入力します。

ステップ 3　[Pools] を選択して右クリックすることによって、**MAC プール**を作成します。

a.　MAC プール名を入力して、MAC アドレスを追加します。

ステップ 4　[Root] 選択してから右クリックすることによって、vNIC テンプレートを作成します。

ステップ 5　VLAN、MAC アドレス プール、およびその他のポリシー（QOS、名前制御、しきい値）を vNIC に割り当てます。

ステップ 6　vNIC テンプレートをサービス プロファイルに追加して、そのテンプレートをサーバにプロビジョニングします。

ステップ 7　UCS ブレード サーバがアップストリーム LAN デバイスと通信していることを確認します。

予測結果

次のテスト結果が予測されます。

- UCS ブレード サーバとその他の LAN デバイス間の通信が行われます。

テスト結果

UCS LAN 接続の設定と確認に成功しました。

UCS SAN 接続の設定と確認

このテストでは、UCS SAN ネットワーク接続を確認します。

テスト手順

UCS SAN 接続の設定と確認テストの手順は次のとおりです。

ステップ 1　UCSM にログインして、[SAN] タブと [SAN cloud] をクリックします。

ステップ 2　[SAN cloud] を右クリックして、新しい vSAN を作成し、次のデータを入力して新しい VSAN の設定を完了します。

1. VSAN の名前
2. VSAN とインターコネクト ファブリックの相互作用
3. VSAN ID
4. FCoE VLAN

ステップ 3　[Equipment] を選択することによって、VSAN を物理 FC インターフェイスに割り当て、ターゲット FC ポートを開いて、プルダウンから必要な VSAN を選択します。

ステップ 4　[SAN] タブをクリックして、[Pools] を選択し、WWNN プールを作成します。

ステップ 5　[SAN] タブをクリックして、[Policies] と [Root] を右クリックし、vHBA テンプレートを作成します。

ステップ 6　VSAN、WWNN プール、およびその他のポリシーを割り当てます。

ステップ 7　[Equipment] タブを選択して [Fabric Interconnect Expansion module Uplink FC Ports] をクリックし、アップストリーム MDS スイッチに接続するファイバ チャネル アップリンク ポートを特定します。

ステップ 8　該当する VSAN と WWPN プールを作成して、それらをファブリック インターコネクト内の FC アップリンク ポートに割り当てます。

ステップ 9　MDS スイッチにログインして、次のコマンドを使用して NPIV モードをイネーブルにします。

```
MDS(config)# npiv enable
```

ステップ 10　MDS で VSAN を作成して、それをゾーンセットに割り当てることで、UCS ブレードがストレージ アレイ内のターゲット ファイバ チャネル ポートにアクセスできるようにします。

ステップ 11　UCSM で MDS スイッチ flogi データベースと FC アップリンク ポートのステータスを確認します。

ステップ 12　vHBA テンプレートをサービス プロファイルに追加して、そのテンプレートをサーバにプロビジョニングします。

ステップ 13　UCS ブレード サーバ ホストからターゲット ストレージにアクセスできることを確認します。

予測結果

次のテスト結果が予測されます。

- ストレージ LUN が UCS ブレード サーバから認識され、サーバとストレージが通信できます。

テスト結果

UCS SAN 接続の設定と確認に成功しました。

ストレージからの UCS SAN ブートの設定と確認

このテストでは、ストレージ LUN からの UCS SAN ブートを確認します。

テスト手順

Hitachi ストレージからの UCS SAN ブートの設定と確認テストの手順は次のとおりです。

ステップ 1　SAN ブートに必要な vHBA を使用してサービス プロファイルを作成し、UCSM を使用して該当する VSAN に配置します。

ステップ 2　該当する SAN ターゲットに vHBA をマッピングすることによって、ブート ポリシーに合わせてサービス プロファイルを変更します。

ステップ 3　ストレージ内の LUN を設定し、ホスト グループを使用して UCS サーバ vHBA にマッピングします。

ステップ 4　UCS と SAN スイッチ内の VSAN 設定を確認します。

ステップ 5　SAN スイッチ内の LUN マスキングとゾーン分割が正しいことを確認します。

ステップ 6　サービス プロファイルを適用して、サーバをリブートします。

ステップ 7　システムがリブートしたら、ブート シーケンスをモニタして、HBA にブート デバイスとして正しい LUN ID が表示されることを確認します。

予測結果

次のテスト結果が予測されます。

- UCS ブレード サーバが SAN から正常にブートします。

テスト結果

ストレージからの UCS SAN ブートの設定と確認に成功しました。

サービス プロファイルを使用した UCS 内のステートレス機能の確認

テスト手順

サービス プロファイルを使用した UCS 内のステートレス機能の確認テストの手順は次のとおりです。

ステップ 1　UCSM にログインして、ナビゲーション ペインで次のプールを作成します。

a.　MAC プール : [LAN] タブをクリックします。

b. WWPN プールと WWNN プール：[SAN] タブをクリックします。

c. UUID プール：[Servers] タブをクリックします。

ステップ 2　次の手順を実行し、Expert Profile Creation ウィザードを使用してサービス プロファイル SP_S1_test を作成します。

a. [Navigation] ペインで [Server] タブをクリックします。

b. [Server] タブで、サービス プロファイルを作成する組織を選択します。

c. [Content] ペインの [Actions] メニューで、[Create Service Profile (expert)] をクリックします。

ステップ 3　サービス プロファイル SP_S1_test に対して MAC プール、WWNN プール、UUID プールを指定し、そのプロファイルをサーバ 1 に割り当てます。

ステップ 4　サーバでユーザ定義プールから MAC、WWNN、および UUID が取得されたことを確認します。

ステップ 5　サーバ 1 を削除して、新しいサーバ（ハードウェアまたは別のモデル）を挿入します。

ステップ 6　サーバでユーザ定義プールから同じ MAC、WWNN、および UUID が取得されたことを確認します。

予測結果

次のテスト結果が予想されます。

- サービス プロファイルのプロビジョンが成功して、ステータスが OK になります。
- サーバの MAC、WWNN、および UUID がユーザ定義プールから取得されます。

テスト結果

サービス プロファイルを使用した UCS 内のステートレス機能の確認に成功しました。

UCS ハイ アベイラビリティ

この項では、次のテスト ケースについて説明します。

- 「ファブリック インターコネクトのハイ アベイラビリティの設定と確認」
- 「UCS からの冗長 FC パス障害の確認」

ファブリック インターコネクトのハイ アベイラビリティの設定と確認

このテストでは、ファブリック インターコネクトのハイ アベイラビリティを確認します。

テスト手順

ファブリック インターコネクトのハイ アベイラビリティの設定と確認テストの手順は次のとおりです。

ステップ 1　CLI 設定経由で最初のファブリック インターコネクトにログインします。

ステップ 2　管理 IP を割り当て、最初の FI（ファブリック インターコネクト）をクラスタ グループ内のプライマリとして設定します。

ステップ 3　2 つめの FI の電源をオンにして、L1 ポートを相互接続します。

ステップ 4　管理 IP を割り当て、クラスタ グループ内の下位として設定します。

ステップ 5　両方のファブリック インターコネクトでクラスタ VIP を設定します。

ステップ 6　クラスタ ステータスを確認します。

ステップ 7　プライマリ FI をリロードして、クラスタのステータスを確認します。

予測結果

次のテスト結果が予想されます。

- 下位 FI がプライマリ FI としてアップし、ファブリック インターコネクト クラスタがアップします。

テスト結果

ファブリック インターコネクトのハイ アベイラビリティの設定と確認に成功しました。

UCS からの冗長 FC パス障害の確認

このテストでは、UCS からストレージまでのセカンダリ パスが存在する場合は、UCS からストレージまでのプライマリ パスで障害が発生してもサーバ トラフィックが中断しないことを確認します。

テストの設定

冗長 vHBA をサーバのサービス プロファイル内に作成し、両方の vHBA を別々の物理 CNA に割り当てます。

テスト手順

UCS からの冗長 FC パス障害の確認テストの手順は次のとおりです。

ステップ 1　ブート順序がサービス プロファイルのブート順序に正しく記載されていることを確認します。
ステップ 2　サーバが SAN から正常にブートされることを確認します。
ステップ 3　サーバからストレージまでの vHBA リンクをシャットダウンします。
ステップ 4　冗長接続を使用してサーバからストレージにアクセスできることを確認します。

予測結果

次のテスト結果が予想されます。

- サーバは、冗長リンクを使用してストレージにアクセスできます。

テスト結果

UCS からの冗長 FC パス障害の確認に成功しました。

VN リンク

この項では、次のテスト ケースについて説明します。

- 「Cisco UCS Manager を使用した VN リンクの設定と確認」
- 「サイト サーバごとの Nexus 1000v の設定と確認」
- 「冗長 Nexus 1000v VSM の設定と確認」

Cisco UCS Manager を使用した VN リンクの設定と確認

このテストでは、VN リンクを設定して確認します。設定はすべて Cisco UCS Manager を使用して行います。

Cisco VN-Link は、VIC アダプタを使用してサーバ上の仮想マシンとのトラフィックを処理するハードウェア ベースの方法です。このアプローチによって、サーバの仮想化に伴う新しい要件を満たす、エンドツーエンドのネットワーク ソリューションが実現されます。ハードウェア内 VN リンクを使用した場合、同じホスト内の 2 つの VM 間のレイヤ 2 トラフィックはローカルでは DVS に切り替わりませんが、ファブリック インターコネクトにアップストリーム送信されることでポリシー適用と切り替えが行われます。

テストの設定

Enterprise Plus ライセンスを ESX ホストにインストールします。これは、DVS の切り替え機能に必要です。

テスト手順

Cisco UCS Manager を使用した VN リンクの設定と確認テストの手順は次のとおりです。

ステップ 1　ダイナミック vNIC を作成するサーバ リンク数に基づいて、ダイナミック vNIC 接続ポリシーを定義します。

ステップ 2　Cisco UCS Manager から vCenter 拡張ファイルを作成して、vCenter からアクセス可能なディレクトリに保存します。

ステップ 3　ステップ 2 で保存した vCenter 拡張ファイルを、新しいプラグインとして VMware vCenter に登録します。

ステップ 4　UCSM 内の vCenter Server 領域で、VMware vCenter Distributed Virtual Switch（DVS; 分散仮想スイッチ）を定義します。

ステップ 5　DVS にマッピングする適切なポート プロファイルを定義します。また、ネイティブ VLAN とともに、該当する VLAN をポート プロファイルにマッピングします。

ステップ 6　UCS Manager を使用して、ポート プロファイルと設定を vCenter Server に適用します。

ステップ 7　vCenter Server ですべてのポート プロファイルが正常に作成されていることを確認します。

ステップ 8　VEM を ESX ホストにそれぞれインストールします。これらの VEM は、シスコのソフトウェア ダウンロードから Nexus 1000v ソフトウェア パッケージとしてダウンロードできます。

ステップ 9　VEM をインストールしたら、ホストを vNetwork 分散スイッチに追加します。

ステップ 10　ダイナミック vNIC が ESXi ホスト内の VM に関連付けられていることを確認します。

予測結果

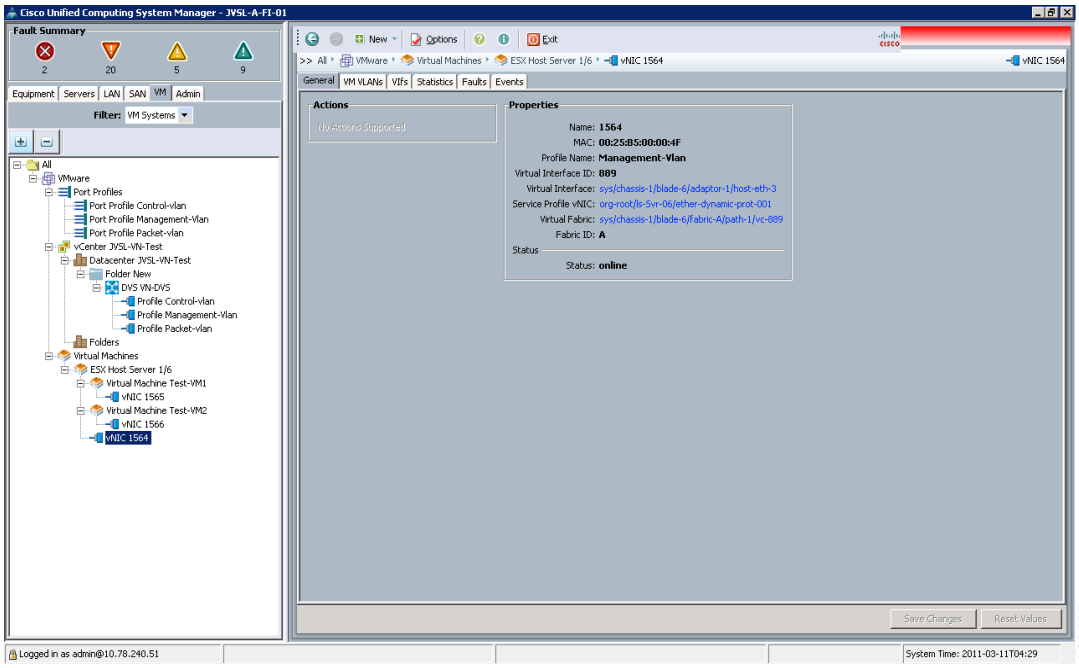
次のテスト結果が予想されます。

- VM が VC に追加され、ポート グループがそれぞれマッピングされたら、UCS Manager か VM タブと VC インターフェイスで表示できるようになります。
- VM が、作成された vNIC に正しく関連付けられます。

テスト結果

Cisco UCS Manager を使用した VN リンクの設定と確認に成功しました。

図 3-1　VN-Link の出力



サイト サーバごとの Nexus 1000v の設定と確認

このテストでは、UCS ホストにインストールされた ESXi 4.1 VMware サーバ用に、Cisco Nexus 1000V ソフトウェアを準備してインストールする方法について説明します。

テストの設定

vCenter Server を UCS ホストの 1 つにインストールし、VMware Enterprise Plus ライセンスを ESXi 4.1 ホストにインストールします。

テスト手順

サイト サーバごとの Nexus 1000v の設定と確認テストの手順は次のとおりです。

ステップ 1　ESXi ホスト内の VMware vSwitch で VSM VM 用のポート グループを 3 つ（制御 VLAN、パケット VLAN、管理 VLAN）を作成します。

ステップ 2　これらをアップストリーム スイッチ内の物理 LAN 上の対応する VLAN に関連付けます。

ステップ 3　Nexus 1000v ova ファイルを ESXi ホストに対応付けることによって、VSM をインストールします。

ステップ 4　vCenter Server で Cisco Nexus 1000v プラグインを作成します。

ステップ 5　次のコマンドを使用して、vCenter Server に接続します。

```
n1000v# config t
n1000v(config)# svs connection VC
n1000v(config-svs-conn)# connect
```

ステップ 6　Cisco Nexus 1000v で、制御 VLAN およびパケット VLAN となる VLAN を作成します。

ステップ 7　VSM と VEM 間の通信を確立するアップリンク ポート プロファイルをシステム VLAN を使用して定義する、システム ポート プロファイルを設定します。

ステップ 8　物理インターフェイスで VM トラフィックの伝送に使用されるアップリンク ポート プロファイルを定義する、アップリンク ポート プロファイルを設定します。

ステップ 9　ゲスト VM との間でトラフィックを送受信するネットワーク アダプタとして VM に提供されるデータ ポート プロファイルを定義する、データ ポート プロファイルを設定します。

ステップ 10　ESXi 4.1 ホストを DVS に追加します。

ステップ 11　次のコマンドを使用して、Nexus1000v がインストールされていることを確認します。

```
n1000v# show module
n1000v# show module vem mapping
```

予測結果

次のテスト結果が予測されます。

- Nexus 1000v が正常にホストにインストールされます。

テスト結果

サイト サーバごとの Nexus 1000v の設定と確認に成功しました。

冗長 Nexus 1000v VSM の設定と確認

このテストでは、冗長 Nexus 1000v VSM のインストールを設定して確認する方法について説明します。

テストの設定

Nexus 1000v をスタンドアロン モードでインストールします。

テスト手順

冗長 Nexus 1000v VSM の設定と確認テストの手順は次のとおりです。

ステップ 1　次のコマンドを使用して、既存のスタンドアロン VSM のロールをプライマリ VSM に変更します。

```
n1000v# system redundancy role primary
```

ステップ 2　次のコマンドを使用して、2 つめの VSM をインストールして、それにセカンダリ ロールを割り当てます。

```
n1000v# system redundancy role secondary
```

ステップ 3　両方のホストで同じパラメータを使用してデュアル VSM VM のポート グループをセットアップします。

ステップ 4　ドメイン ID をプライマリ VSM で使用されるセカンダリ VSM に割り当てます。

ステップ 5　セカンダリ VSM がインストールされると、セカンダリ VSM がリロードされ、スタンドアロン VSM としてシステムに追加されます。

ステップ 6　次のコマンドを使用して、VSM の現在のシステム冗長性ステータスを確認します。

```
n1000v# show system redundancy status
```

予測結果

次のテスト結果が予測されます。

- 冗長 VSM がインストールされ、正常に動作します。

テスト結果

冗長 Nexus 1000v VSM の設定と確認に成功しました。

ライブ マイグレーション

この項では、次のテスト ケースについて説明します。

- 「Nexus 7010（各サイトのエッジ デバイス）での OTV の設定と確認」
- 「OTV 経由のサイト A からサイト B へのトラフィック フローの設定と確認」
- 「両方のサイトでの VMware VMotion 設定」
- 「vCenter EVC クラスタ内の複数サイトでの VMware VMotion ホストの追加」
- 「サイト A からサイト B への VMotion の実行と確認」

Nexus 7010（各サイトのエッジ デバイス）での OTV の設定と確認

テストの説明

Overlay Transport Virtualization（OTV）は、クラスタや仮想化などのレイヤ 2 隣接が必要なアプリケーションに対するサポートを提供するために、トランスポート ネットワーク全体で、MAC アドレス ベースのルーティングと IP カプセル化転送を使用して、リモート ネットワーク サイト間のレイヤ 2 接続を可能にします。OTV は各サイトのエッジ デバイス上に展開されます。

テストの設定

Advanced Services Package および Transport ライセンスを使用して Nexus 7010 スイッチをインストールします。新しい OTV vDC が 7010 スイッチ（エッジ デバイス）で作成され、OTV VDC が Cat 6504（コア）デバイス経由で相互接続されます。

テスト手順

Nexus 7010 デバイスでの OTV 機能の設定と確認テストの手順は次のとおりです。

ステップ 1　feature otv コマンドを使用して、Nexus 7010 内の OTV 機能をイネーブルにします。

ステップ 2　次のコマンドを使用して、DCI 用の VDC **JVSL-OTV_VDC** を作成します。

```
switch (config) #vdc j vsl-otv_vdc
```

ステップ 3　両方のサイトで JVSL_OTV_VDC を設定します。

- OTV VDC 上の OTV 経由で拡張するように VLAN を設定します。

```
JVSL_OTV-VDC(config)# vlan 100-200,1
```

- 結合インターフェイスを設定します。

```
JVSL_OTV-VDC(config)# interface ethernet 2/2
JVSL_OTV-VDC(config-if)# description [ OTV Join-Interface ]
JVSL_OTV-VDC(config-if)# ip address xx.xx.xx.xx/30
JVSL_OTV-VDC(config-if)# ip igmp version 3
JVSL_OTV-VDC(config-if)# no shutdown
```

- 内部インターフェイスを設定します。

```
iinterface ethernet 2/10
description [ OTV Internal Interface ]
switchport
switchport mode trunk
switchport trunk allowed vlan 100-200, 1
no shutdown
```

- エッジ デバイスで `interface overlay xx` コマンドを使用してオーバーレイ インターフェイスを作成します。
- マルチキャスト グループを作成してオーバーレイ インターフェイスに対応付けます。
- `otv join-interface <interface>` コマンドを使用して、物理インターフェイスをオーバーレイ インターフェイスに割り当てます。
- サイト VLAN 範囲と拡張 VLAN 範囲を割り当てます。

ステップ 4　`show otv overlay <interface>` と `show otv adjacency` を使用して、OTV 設定を確認します。

予測結果

次のテスト結果が予測されます。

- OTV 接続がアップ状態で稼動しています。

テスト結果

Nexus 7010（各サイトのエッジ デバイス）での OTV の設定と確認に成功しました。

出力

サイト A OTV VDC からの show コマンド出力：

```
A_OTV_VDC_01# sh otv overlay 1
OTV Overlay Information
Overlay interface Overlay1
VPN name            : Overlay1
 VPN state           : UP
 Extended vlans      : 100-200 (Total:101)
 Control group       : 239.1.1.1
 Data group range(s) : 239.192.1.0/24
```

```
 Join interface(s)   : Eth7/1 (172.18.1.5)
 Site vlan           : 1 (up)

A_OTV_VDC_01# sh otv adjacency
Overlay Adjacency database
Overlay-Interface Overlay1  :
Hostname                         System-ID      Dest Addr       Up Time   State
B_OTV_VDC                        0024.f716.6641 172.18.1.13     5d20h     UP
A_OTV_VDC_01#
```

サイト B OTV VDC からの show コマンド出力：

```
B_OTV_VDC# sh otv
OTV Overlay Information
Overlay interface Overlay1
VPN name            : Overlay1
 VPN state          : UP
 Extended vlans     : 100-200 (Total:101)
 Control group      : 239.1.1.1
 Data group range(s) : 239.192.1.0/24
 Join interface(s)  : Eth7/1 (172.18.1.13)
 Site vlan          : 1 (up)

B_OTV_VDC# sh otv adjacency
Overlay Adjacency database
Overlay-Interface Overlay1  :
Hostname                         System-ID      Dest Addr       Up Time   State
A_OTV_VDC_01                     0026.51c5.9cc4 172.18.1.5      5d20h     UP
B_OTV_VDC#
```

OTV 経由のサイト A からサイト B へのトラフィック フローの設定と確認

テストの設定

Advanced Services Package および Transport ライセンスを使用して Nexus 7010 スイッチをインストールします。新しい OTV vDC が両方のサイトの 7010 スイッチ（エッジ デバイス）で作成され、Cat 6504（コア）デバイス経由で相互接続されます。

テスト手順

OTV エッジ デバイス（Nexus 7010）間の OTV トラフィック フローの確認テストの実行手順は次のとおりです。

ステップ 1　コマンドの `show otv overlay <interface>` と `show otv adjacency` を使用して、エッジ デバイス内の OTV ステータスを確認します。

ステップ 2　OTV リンクがアップ状態であることを確認します。

ステップ 3　サイト A のサーバからサイト B のサーバへの ping トラフィックを開始します。

ステップ 4　エッジ デバイスとコア デバイスでトラフィック フローを確認します。

予測結果

次のテスト結果が予測されます。

- サイト A とサイト B 間のサーバ トラフィック フローがパケット ドロップなしで転送されます。

テスト結果

OTV 経由のサイト A からサイト B へのトラフィック フローの設定と確認に成功しました。

出力

サイト A の集約スイッチからの ping コマンド出力：

```
JVSL-A-AGG-01# sh run int vlan 180

!Command: show running-config interface Vlan180
!Time: Thu May 19 08:33:52 2011

version 5.1(3)
interface Vlan180
  no shutdown
  ip address 172.16.180.2/24
  ip router ospf 10 area 0.0.0.10
  hsrp 101
    preempt delay minimum 60
    priority 150
    ip 172.16.180.1
JVSL-A-AGG-01#

JVSL-A-AGG-01# ping 172.16.180.4 count 100

PING 172.16.180.4 (172.16.180.4): 56 data bytes
64 bytes from 172.16.180.4: icmp_seq=0 ttl=254 time=1.566 ms
64 bytes from 172.16.180.4: icmp_seq=94 ttl=254 time=0.958 ms
64 bytes from 172.16.180.4: icmp_seq=95 ttl=254 time=0.971 ms
64 bytes from 172.16.180.4: icmp_seq=96 ttl=254 time=0.973 ms
64 bytes from 172.16.180.4: icmp_seq=97 ttl=254 time=0.849 ms
64 bytes from 172.16.180.4: icmp_seq=98 ttl=254 time=0.854 ms
64 bytes from 172.16.180.4: icmp_seq=99 ttl=254 time=1.1 ms
--- 172.16.180.4 ping statistics ---
100 packets transmitted, 100 packets received, 0.00% packet loss
round-trip min/avg/max = 0.809/1.301/19.981 ms
```

```
JVSL-A-AGG-01#
```

両方のサイトでの VMware VMotion 設定

2 つのサイト間で VMware VMotion 設定が実施されます。このとき、VMware vSphere が、サイト A の Cisco UCS B-440 M1 サーバとサイト B の B-250 M2 サーバにインストールされます。

テストの設定

2 つのサイト間の VLAN、およびサイト B のストレージを拡張する、拡張 VLAN および共有ストレージ アーキテクチャを使用します。仮想マシンをリモート データセンターに移行すると、アプリケーションはサイト B からストレージにアクセスします。ストレージはリモート データセンター内のアプリケーションに対してプロビジョニングされません。そのため、ストレージのコピーは常に 1 つしか存在しません。テスト中に使用されるコンポーネントは、各データセンター内の VMware VMotion を使用してイネーブルにされた VMware vSphere ESXi 4.1 サーバ、Nexus 1000V、VMware vCenter サーバ、および Data Center Interconnect（DCI; データセンター インターコネクト）WAN です。

テスト手順

両方のサイトでの VMware VMotion 設定の手順は次のとおりです。

ステップ 1　OTV セットアップがアップ状態であることを確認します。

ステップ 2　両方のサイトのサーバから認識可能な、サイト B 内の LUN を準備します。

ステップ 3　この LUN を VMotion 用の VM が設置されたサイト B 内の UCS サーバにマップします。

ステップ 4　両方のサイトで MDS 間の FCIP リンクを使用して、サイト A の UCS サーバからサイト B のストレージへのパスを構築します。

ステップ 5　ステップ 3 で使用した LUN を、VMotion 用の VM が設置されたサイト A の UCS サーバにマップします。

ステップ 6　サイト A の UCS サーバからサイト B の UCS サーバへの VMotion 専用リンクを構築します。

ステップ 7　送信元 VMware ESXi サーバと宛先 VMware ESXi サーバが相互にアクセスできることを確認します。

予測結果

次のテスト結果が予測されます。

- 送信元と宛先に到達できます。

テスト結果

両方のサイトでの VMware VMotion 設定に成功しました。

vCenter EVC クラスタ内の複数サイトでの VMware VMotion ホストの追加

VMotion に関する重要な要件の 1 つは CPU の互換性です。このテストでは、Intel Xeon x7560 が搭載された Cisco UCS B-440 M1 と Intel Xeon x5680 が搭載された B-250 M2 間で VMotion を実行します。ホスト間の CPU 非互換性を排除するために、Enhanced VMotion Compatibility（EVC）を使用して上記ホスト間の VMotion が実行されます。

テストの設定

両方のホストが、サイト A で使用可能な vCenter に到達できます。

テスト手順

vCenter EVC クラスタ内の複数サイトでの VMware VMotion の追加テストに関する手順は次のとおりです。

ステップ 1　vCenter 内のデータ センターでクラスタを作成します。

ステップ 2　クラスタ セットアップで、Intel ホストに対する EVC 機能をイネーブルにします。

ステップ 3　クラスタ作成後に、必要なホストをサイト A とサイト B に追加します。

ステップ 4　ホストが正常に追加されたことを確認します。

予測結果

次のテスト結果が予測されます。

- ホストは、CPU 非互換性の問題が発生することなく正常に追加されます。

テスト結果

vCenter EVC クラスタ内の複数サイトでの VMware VMotion ホストの追加に成功しました。

サイト A からサイト B への VMotion の実行と確認

テストの説明

アプリケーションのダウンタイムがなく瞬時に Cisco UCS B-440 M1 サーバと B-250 M2 サーバにインストールされた、2 つの VMware vSphere 間での仮想マシン モビリティを可能にする VMware VMotion テクノロジーをテストします。

テストの設定

両方のサイトで VMware VMotion 設定を実施します。

テスト手順

サイト A からサイト B への VMotion の実行と確認テストの手順は次のとおりです。

ステップ 1　ESXi サーバを vCenter ホスト クラスタに追加します。

ステップ 2　サイト A からサイト B に移行する VM を選択します。

ステップ 3　VM と同じサブネット内のホストから VM IP に対して ping コマンドを連続的に発行します。

ステップ 4　VMware Vcenter から、サイト A からサイト B にホストを移行します。

ステップ 5　移行中のパケット ドロップが最小限に抑えられたことを確認します。

ステップ 6　サイト B のホストへの移行後の VM ステータスを確認します。

予測結果

次のテスト結果が予測されます。

- ホスト移行が問題なく実行されます。

テスト結果

サイト A からサイト B への VMotion の実行と確認に成功しました。

出力

ブランチ オフィス クライアントから実行された VMotion 中の ping 出力

```
Reply from 172.16.180.20: bytes=32 time<1ms TTL=128
Reply from 172.16.180.20: bytes=32 time<1ms TTL=128
Reply from 172.16.180.20: bytes=32 time<1ms TTL=128
Reply from 172.16.180.20: bytes=32 time<1ms TTL=128
Reply from 172.16.180.20: bytes=32 time<1ms TTL=128
Reply from 172.16.180.20: bytes=32 time<1ms TTL=128
Request timed out.
Request timed out.
Reply from 172.16.180.20: bytes=32 time<1ms TTL=128
Reply from 172.16.180.20: bytes=32 time<1ms TTL=128
Reply from 172.16.180.20: bytes=32 time<1ms TTL=128
Reply from 172.16.180.20: bytes=32 time<1ms TTL=128
Reply from 172.16.180.20: bytes=32 time<1ms TTL=128
Reply from 172.16.180.20: bytes=32 time<1ms TTL=128
Reply from 172.16.180.20: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.180.20:
    Packets: Sent = 142, Received = 140, Lost = 2 (1% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 154ms, Average = 1ms
```

図 3-2　VMotion 実行前の出力

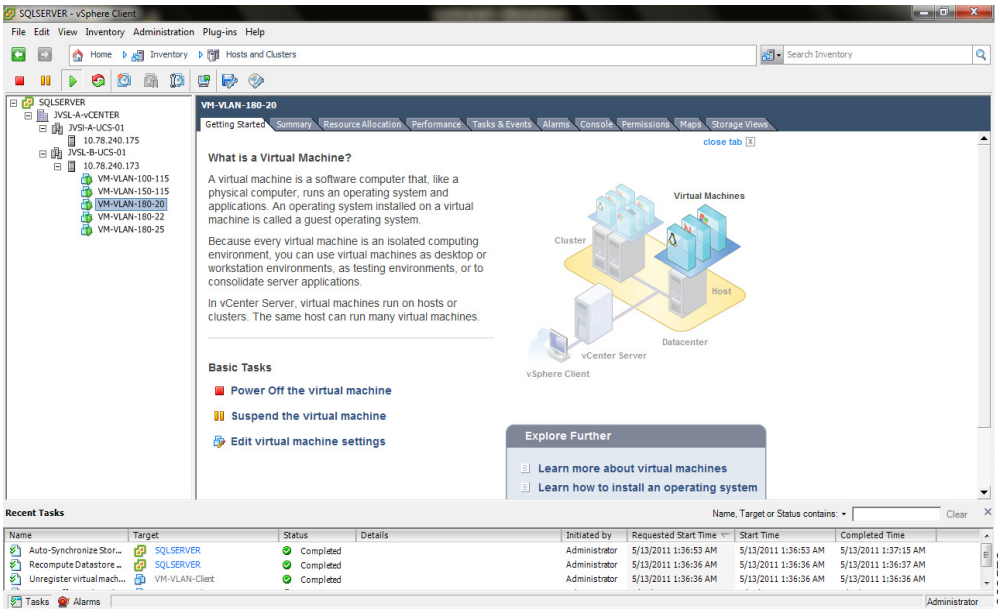
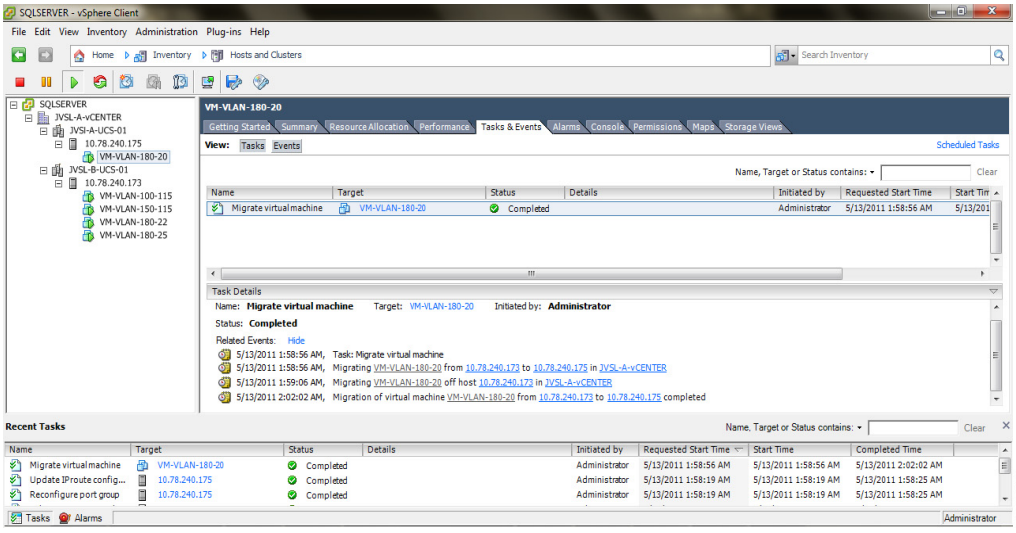


図 3-3　VMotion 実行後の出力



IP インフラストラクチャの設定と確認

この項では、次のテスト ケースについて説明します。

- 「Nexus 7010 と 5020 間の L2 ポート チャネルと、Nexus 7010 と Cat 6509 間の L3 ポート チャネルの設定と確認」
- 「コア スイッチ、集約スイッチ、サービス スイッチ、および WAN エッジ ルータでのルーティング プロトコル（OSPF）の確認」
- 「vPC 障害と STP へのフォールバックの確認」
- 「サイト A とサイト B 間の通信の確認」

Nexus 7010 と 5020 間の L2 ポート チャネルと、Nexus 7010 と Cat 6509 間の L3 ポート チャネルの設定と確認

ポート チャネルは、複数の物理イーサネット リンクを単一の論理イーサネット リンクに集約するメカニズムです。通常、ポート チャネルは、可用性を高め、帯域幅を増やすために使用します。高可用性、フェールオーバー テスト ESXi 編 では、レイヤ 2 ポート チャネルを集約スイッチとアクセス スイッチ間で構築し、L3 ポート チャネルを集約スイッチとサービス スイッチ間で構築します。

テストの設定

光ファイバ ケーブルを使用して、集約スイッチ（JVSL-B-AGG-N7k-01 と JVSL-B-AGG-N7k-02）とアクセス スイッチ（JVSL-B-ACC-N5K-01 と JVSL-B-ACC-N5K-02）を接続します。光ファイバ ケーブルを使用して、サービス スイッチ（JVSL-B-C6k-01）の 10 GB インターフェイスを集約スイッチ（JVSL-B-AGG-N7K-01）に接続します。

テスト手順

Nexus 7010 と 5020 間の L2 ポート チャネル、および Nexus 7010 と Cat 6509 間の L3 ポート チャネルの設定と確認テストの手順は次のとおりです。

ステップ 1　`switchport mode trunk` コマンドを使用して、集約スイッチ（JVSL-B-AGG-N7K-01 と JVSL-B-AGG-N7K-02）とアクセス スイッチ（JVSL-B-ACC-N5K-01 と JVSL-B-ACC-N5K-02）間のすべてのリンクをトランク ポートとして設定します。

ステップ 2　`show interface trunk` コマンドを使用して、トランク リンクのステータスを確認します。

ステップ 3　`channel-group XX mode active` コマンドを使用して、JVSL-B-AGG-N7K-01 と JVSL-B-C6k-01 間のリンクを L3 ポート チャネルとして設定します。

ステップ 4　集約スイッチ（JVSL-B-AGG-N7K-01 と JVSL-B-AGG-N7K-02）とアクセス スイッチ（JVSL-B-ACC-N5K-01 と JVSL-B-ACC-N5K-02）で、トランク モードで L2 ポート チャネル インターフェイスを作成します。

ステップ 5　`sh port-channel summary` コマンドを使用して、PortChannel のステータスを確認します。

ステップ 6　`Channel group xxx mode on` コマンドを使用して、L2 ポート チャネル グループを物理インターフェイスに割り当てます。

ステップ 7　`show port-channel summary` コマンドを使用して、ポート チャネルのステータスを確認します。

予測結果

次のテスト結果が予測されます。

- L2 ポート チャネルと L3 ポート チャネルが動作しています。

テスト結果

Nexus 7010 と 5020 間の L2 ポート チャネルと、Nexus 7010 と Cat 6509 間の L3 ポート チャネルの設定と確認に成功しました。

コア スイッチ、集約スイッチ、サービス スイッチ、および WAN エッジ ルータでのルーティング プロトコル（OSPF）の確認

このテストでは、OSPF プロトコルを確認して、さまざまなデバイスでルーティング テーブルが更新されるかどうかをチェックします。

テストの設定

コア スイッチ（JVSL-B-CORE-N7K-01 と JVSL-B-CORE-N7K-02）の WAN エッジ ポートを WAN エッジ ルータ（JVSL-B-ASR-01）の LAN ポートに接続します。光ファイバ ケーブルを使用して、コア スイッチ（JVSL-B-CORE-N7K-01 と JVSL-B-CORE-N7K-02）と集約スイッチ（JVSL-B-AGG-N7K-01 と JVSL-B-AGG-N7K-02）のポートを相互接続します。すべてのポートが L3 ポート チャネルの一部になります。

テスト手順

コア スイッチ、集約スイッチ、サービス スイッチ、および WAN エッジ ルータでのルーティング プロトコル（OSPF）の確認テストの手順は次のとおりです。

ステップ 1　コア スイッチ（JVSL-B-CORE-N7K-01 と JVSL-B-CORE-N7K-02）、WAN エッジ ルータ（JVSL-B-ASR-01）、およびサービス スイッチ（JVSL-B-C6k-01）間で L3 リンクを設定します。

ステップ 2　コア スイッチと WAN エッジ ルータで、`ip router ospf 10 area 0.0.0.0` コマンドを使用して OSPF エリア 0 を設定します。

ステップ 3　コア スイッチと集約スイッチ間の L3 ポート チャネルがアップしていることを確認し、`ip router ospf 10 area 0.0.0.10` コマンドを使用してすべての L3 ポート チャネルで OSPF エリア 10 を設定します。

ステップ 4　`show ip ospf neighbors` コマンドと `show ip ospf database` コマンドを使用して、OSPF ネイバーとデータベースを確認します。

ステップ 5　すべての OSPF ルートがルーティング テーブルに登録されていることを確認します。

予測結果

次のテスト結果が予測されます。

- OSPF データベースに正しいルートが設定されます。

テスト結果

コア スイッチ、集約スイッチ、サービス スイッチ、および WAN エッジ ルータでのルーティング プロトコル（OSPF）の確認に成功しました。

vPC 障害と STP へのフォールバックの確認

このテストでは、集約スイッチ（Nexus 7010 デバイス）とアクセス スイッチ（Nexus 5020 デバイス）で vPC 障害が発生した場合の、vPC 設定と STP テイクオーバーを確認します。

テストの設定

集約スイッチ（JVSL-B-AGG-N7K-01 と JVSL-B-AGG-N7K-02）とアクセス スイッチ（JVSL-B-ACC-N5K-01 と JVSL-B-AGG-N5K-02）間に複数のリンクを接続する必要があります。また、冗長リンクを使用して、ファブリック インターコネクトとアクセス スイッチを接続します。

テスト手順

Nexus 7010 デバイスと Nexus 5020 デバイスでの vPC 障害および STP へのフォールバックの確認テストの手順は次のとおりです。

ステップ 1　`feature vpc` コマンドを使用して vPC 機能をイネーブルにし、`show feature` コマンドを使用してイネーブルにした機能を確認します。

ステップ 2　ロール プライオリティが 5 の集約スイッチ JVSL-B-AGG-N7K-01 とアクセス スイッチ JVSL-B-ACC-N5k-01 で vPC ドメイン 10 を作成して、スイッチを vPC プライマリにします。

ステップ 3　`sh vpc role` コマンドを使用して、vPC ロールを確認します。

ステップ 4　ロール プライオリティが 10 の集約スイッチ JVSL-B-AGG-N7K-02 とアクセス スイッチ JVSL-B-ACC-N5k-02 で vPC ドメイン 10 を作成して、スイッチを vPC セカンダリにします。

ステップ 5　`sh vpc role` コマンドを使用して、vPC ロールを確認します。

ステップ 6　次のコマンドを使用して、vPC-peer-keepalive リンクの宛先 IP アドレスと送信元 IP アドレスを設定し、VRF を vPC-peer- keepalive 用に設定します。

```
switch(config-vpc-domain)# peer-keepalive destination x.x.x.x source x.x.x.x vrf vpc
```

ステップ 7　vPC peer-link として使用するポート チャネルを選択し、インターフェイス コンフィギュレーション モードを開始します。

```
switch(config)# interface port-channel XXX
switch(config-if)# vpc peer-link
```

ステップ 8　インターフェイス モードで `vpc 10` コマンドを使用して、vPC メンバー ポートを vPC ドメイン 10 に追加します。

ステップ 9　`show vPC brief` コマンドを使用して vPC のステータスを確認します。

ステップ 10　プライマリ スイッチとセカンダリ スイッチに同じロール プライオリティを設定し、`shutdown` コマンドを使用して vPC peer-link 用のポート チャネルをシャットダウンします。

ステップ 11　次のコマンドを使用して、vPC 障害が原因でループが発生しないように、スパニング ツリーの存在を確認します。

```
Show spanning-tree root
Show spanning-tree vlan
```

予測結果

次のテスト結果が予想されます。

- vPC がアップして実行中になります。

- vPC で障害が発生すると、STP がテイクオーバーします。

テスト結果

vPC 障害と STP へのフォールバックの確認に成功しました。

サイト A とサイト B 間の通信の確認

このテストでは、サイト A とサイト B の集約スイッチ間で通信が確立され、パケット損失が発生しないことを確認します。

テストの設定

集約スイッチ（JVSL-A-AGG-N7k-01 と JVSL-A-AGG-N7k-02）をコア スイッチ（JVSL-A-CORE-N7k-01 と JVSL-A-CORE-N7k-02）に接続し、そこから、WAN エッジ ルータ（JVSL-A-ASR-01）に接続します。WAN エッジ ルータの 1 GB インターフェイスを WAN エミュレータの Link1-LAN A（JVSL-A-WEM-01）ポートに接続し、Link1-LAN B を ISR（JVSL-A-ISR-01）に接続します。Link2-LAN A をサイト B の WAN エッジ ルータ（JVSL-B-ASR-01）に接続し、そこから、サイト B のコア スイッチ（JVSL-B-CORE-N7k-01 と JVSL-B-CORE-N7k-02）に接続します。コア スイッチは集約スイッチに接続します。

テスト手順

サイト A とサイト B 間の通信の確認の手順は次のとおりです。

ステップ 1　両方のサイトで WAN エッジ ルータの 1 GB インターフェイスが WAN エミュレータの LinkX-LAN A ポートに接続されており、リンクがアップしていることを確認します。

ステップ 2　1 GB インターフェイスに IP アドレスを割り当て、`ip router ospf 0 area 0.0.0.0` コマンドを使用して OSPF エリア 0 を設定します。

ステップ 3　帯域幅や遅延などの WAN エミュレータ リンク設定を構成します。

ステップ 4　ブランチ オフィス ルータのインターフェイスが WAN エミュレータの LinkX-LAN B ポートに接続されていることを確認し、`show interface` コマンドを使用してそのリンクがアップしていることを確認し、そのリンクに IP アドレスを割り当てます。

ステップ 5　`show port-channel summary` コマンドを使用して、デバイス間で設定されたすべてのポート チャネルがアップしていることを確認します。

ステップ 6　`show ip route` を使用して、ルーティング テーブルが OSPF プロトコルで更新されていることを確認します。

ステップ 7　データグラム サイズが 1000 で、繰り返し回数が 1000 の ICMP パケットをサイト A VM のいずれかからサイト B に送信して、パケット損失が発生しないことを確認します。

予測結果

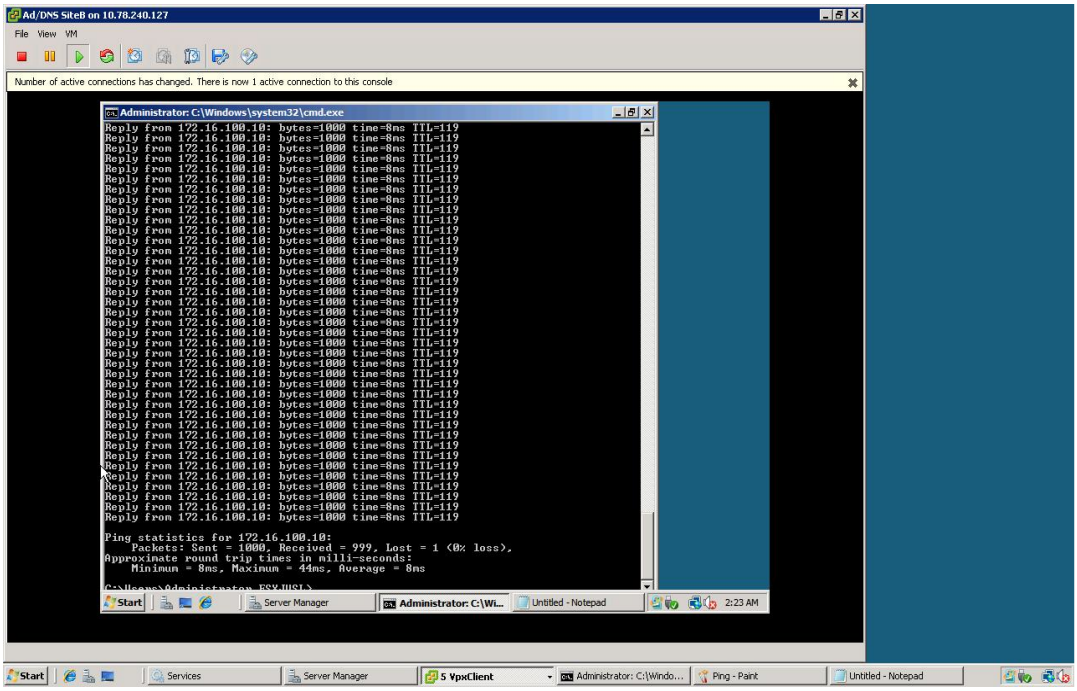
次のテスト結果が予測されます。

- サイト A とサイト B 間の通信が正常に確立され、パケット損失は発生しません。

テスト結果

サイト A とサイト B 間の通信の確認に成功しました。

図 3-4　ping の出力



MS Exchange の確認

この項では、次のテスト ケースについて説明します。

- 「基本的なメール交換の確認」
- 「データベース可用性グループ（サイト内フェールオーバー）の確認」
- 「データベース可用性グループ（サイト間フェールオーバー）の確認」
- 「ハブ トランスポート サーバのフェールオーバー（サイト内フェールオーバー）の確認」
- 「サイト フェールオーバー中のデータベース可用性の確認」
- 「グローバル カタログ サーバのフェールオーバー（サイト間）の確認」

基本的なメール交換の確認

このテストでは、高可用性、フェールオーバー テスト ESXi 編のセットアップ環境において、Microsoft Exchange アプリケーション展開の基本機能を確認します。このテストは、ブランチから J-VSL サイト A に、Outlook Web Access、Outlook アドレス帳、および Outlook Anywhere クライアント ベースのトラフィックを送信することによって確認します。ブランチと JVSL サイト A 間の接続は、帯域幅 T3 45 mbs および遅延 7 ～ 8 ms を使用して、距離が 100 km になるようにシミュレーションします。

Loadgen パラメータ

シミュレーションの長さ	10 分
シミュレーション モード	ストレス モード
ユーザ数	2
データベース数	5
予定表数	5
連絡先数	5
使用される配布リスト	既存の配布リストと動的な配布リスト
ユーザ グループ数	2

テスト手順

基本的なメール交換の確認テストの手順は次のとおりです。

ステップ 1　loadgen で MS Exchange の指定を設定します。

ステップ 2　サイト A に Exchange トラフィックを送信するように LoadGen が設定されていることを確認します。10 分間のテスト トラフィックを開始します。

ステップ 3　ユーザ 1 からユーザ 2 に対してメールの送信を開始します。

ステップ 4　相手側ユーザがメールを受信したことを確認します。

予測結果

次のテスト結果が予測されます。

- ユーザは問題なくメールを送受信できます。

テスト結果

基本的なメール交換の確認に成功しました。

データベース可用性グループ（サイト内フェールオーバー）の確認

このテストでは、アプリケーション ホスト（Exchange DAG プライマリ ホスト）フェールオーバー中の Exchange の機能を確認します。このテストは、ブランチからサイト A に 10 分間 Exchange トラフィックを送信することによって確認します。ブランチと J-VSL サイト A 間の接続は、帯域幅 T3 45 mbs および遅延 7 ～ 8 ms を使用して、距離が 100 km になるようにシミュレーションします。

Load Generator は、全長 10 分間のシミュレーション用に設定します。

テスト手順

Exchange DAG プライマリ ホスト電源障害の確認テストの手順は次のとおりです。

ステップ 1　サイト A に Exchange トラフィックを送信するように Load Gen が設定されていることを確認します。10 分間のテスト トラフィックを開始します。

ステップ 2　Exchange DAG プライマリ ホストを少なくとも 2 分間シャットダウンすることによって、DAG フェールオーバーをシミュレーションします。

ステップ 3　Load Gen から取得された結果を使用して、すべての新しい接続がサイト A のもう一方の DAG ノードにリダイレクトされることを確認します。

ステップ 4　DAG プライマリ ホストの電源をオンにします。

ステップ 5　ホストがオンライン状態に戻ったら、フェールオーバー クラスタ管理ツールを使用して、Exchange をフェールバックします。

ステップ 6　新しい接続のすべてをプライマリ DAG ホストが供給していることを確認します。

ステップ 7　トラフィックが完了したら、Load Generator のレポートを保存します。レポートから、メール データの損失が判断されます。

予測結果

次のテスト結果が予想されます。

- ホストに接続している既存のアプリケーション トラフィックが失敗します。
- フェールオーバーが発生すると、新しい接続のすべてがもう一方の DAG ノードから供給されます。
- フェールバックが発生すると、電源を再投入されたノードが新しい接続を受け入れます。

テスト結果

データベース可用性グループ（サイト内フェールオーバー）の確認に成功しました。

Load Generator のレポート

表 3-1　Microsoft Exchange Server Load Generator

テスト結果の概要	
結果：	正常
トポロジの設定	
対象のフォレスト：	ESXJVSL
ユーザ グループの総数：	2
ユーザの総数：	2
配布リストの総数：	0
動的な配布リストの総数：	0
連絡先の総数：	0
外部受信者の総数：	0

シミュレーションの統計情報	
シミュレーション開始：	2010 年 1 月 19 日午前 9 時 46 分 03 秒
スケジュール上の実行期間：	00 日：00 時間：10 分：00 秒
実際の実行期間：	00 日：00 時間：10 分：01 秒
ストレス モード：	True
リモート：	False

Load Generator のステータス

（注）　Load Generator のクライアントは、タスク カウンタがゼロであると予測されるスクリプト モジュールで、ユーザ グループを実行します。

タイプ	名称	タスクの例外	タスク キューの長さ	スキップされたタスク	完了したタスク	ディスパッチされたタスク
マスター	PC	0	0	0	31282	31282

ユーザ グループ

名称	正常	クライアント タイプ	アクション プロファイル	ユーザ数	タスク数/ユーザ日	完了したタスク
UserGroup1	正常	Outlook 2003 オンライン	Outlook_50	1	81	6487

アクティブ ユーザの統計情報

アクティブ ユーザ数	期間
1	00:10:00

タスク実行の統計

タスク名	カウント	実際の配布（%）	設定された配布（%）
AddPublicDelegateTask	0	0	0
BrowseAddressBookTask	0	0	0
BrowseCalendarTask	880	13	13
BrowseContactsTask	740	11	11
BrowsePublicFolderTask	0	0	0
BrowseTasksTask	85	1	1
CreateContactTask	100	1	1
CreateFolderTask	0	0	0
CreateTaskTask	78	1	1
DeleteMailTask	0	0	0
DownloadOabTask	97	1	1
EditRulesTask	0	0	0
EditSmartFoldersTask	70	1	0
ExportMailTask	0	0	0
InitializeMailboxTask	0	0	0
LogoffTask	232	3	3
LogonTask	0	0	0
MakeAppointmentTask	84	1	1
ModuleInitTask	1	0	0

タスク名	カウント	実際の配布（%）	設定された配布（%）
MoveMailTask	0	0	0
PostFreeBusyTask	282	4	4
PublicFolderPostTask	0	0	0
PublishCertificatesTask	0	0	0
ReadAndProcessMessagesTask	3183	49	49
RequestMeetingTask	79	1	1
SearchTask	0	0	1
SendMailTask	576	8	8
ViewContactDetailsTask	0	0	0

タスクの例外統計

タイプ	カウント
Microsoft.Mapi.MapiExceptionLogonFailed	6252

名称	正常	クライアント タイプ	アクション プロファイル	ユーザ数	タスク数/ユーザ日	完了したタスク
UserGroup1	正常	Outlook 2003 オンライン	Outlook_50	1	81	24795

アクティブ ユーザの統計情報

アクティブ ユーザ数	期間
1	00:10:00

タスク実行の統計

タスク名	カウント	実際の配布（%）	設定された配布（%）
AddPublicDelegateTask	0	0	0
BrowseAddressBookTask	0	0	0
BrowseCalendarTask	3389	13	13
BrowseContactsTask	2702	10	11
BrowsePublicFolderTask	0	0	0
BrowseTasksTask	275	1	1
CreateContactTask	299	1	1
CreateFolderTask	0	0	0
CreateTaskTask	305	1	1
DeleteMailTask	0	0	0
DownloadOabTask	310	1	1
EditRulesTask	0	0	0
EditSmartFoldersTask	328	1	0

タスク名	カウント	実際の配布（%）	設定された配布（%）
ExportMailTask	0	0	0
InitializeMailboxTask	0	0	0
LogoffTask	924	3	3
LogonTask	0	0	0
MakeAppointmentTask	289	1	1
ModuleInitTask	1	0	0
MoveMailTask	0	0	0
PostFreeBusyTask	1185	4	4
PublicFolderPostTask	0	0	0
PublishCertificatesTask	0	0	0
ReadAndProcessMessagesTask	12377	49	49
RequestMeetingTask	316	1	1
SearchTask	0	0	1
SendMailTask	2095	8	8
ViewContactDetailsTask	0	0	0

タスクの例外統計

タイプ	カウント
Microsoft.Mapi.MapiExceptionNetworkError	23868

データベース可用性グループ（サイト間フェールオーバー）の確認

このテストでは、アプリケーション ホスト（Exchange DAG ホスト）のサイト レベル フェールオーバー中の、Exchange の機能を確認します。このテストは、ブランチからサイト A に 10 分間 Exchange トラフィックを送信することによって確認します。ブランチと J-VSL サイト A 間の接続は、帯域幅 T3 45 mbs および遅延 7 ～ 8 ms を使用して、距離が 100 km になるようにシミュレーションします。

Load Generator は、全長 10 分間のシミュレーション用に設定します。

テスト手順

Exchange DAG サイト レベル障害の確認テストの手順は次のとおりです。

ステップ 1　サイト A に Exchange トラフィックを送信するように Load Gen が設定されていることを確認します。

ステップ 2　10 分間のテスト トラフィックを開始します。

ステップ 3　サイト A アクティブ メールボックス サーバを 2 分間シャットダウンすることによって、サイト フェールオーバーをシミュレーションします。

ステップ 4　Load Gen から取得された結果を使用して、新しい接続のすべてがサイト B のメールボックス サーバにリダイレクトされることを確認します。

ステップ 5　サイト A のメールボックス サーバの電源をオンにします。

ステップ 6　メールボックス サーバがオンラインに戻ったら、フェールオーバー クラスタ管理ツールを使用して、Exchange をフェールバックします。

ステップ 7　新しい接続のすべてをプライマリ DAG ホストが供給していることを確認します。

ステップ 8　トラフィックが完了したら、Load Generator のレポートを保存します。レポートから、メール データの損失が判断されます。

予測結果

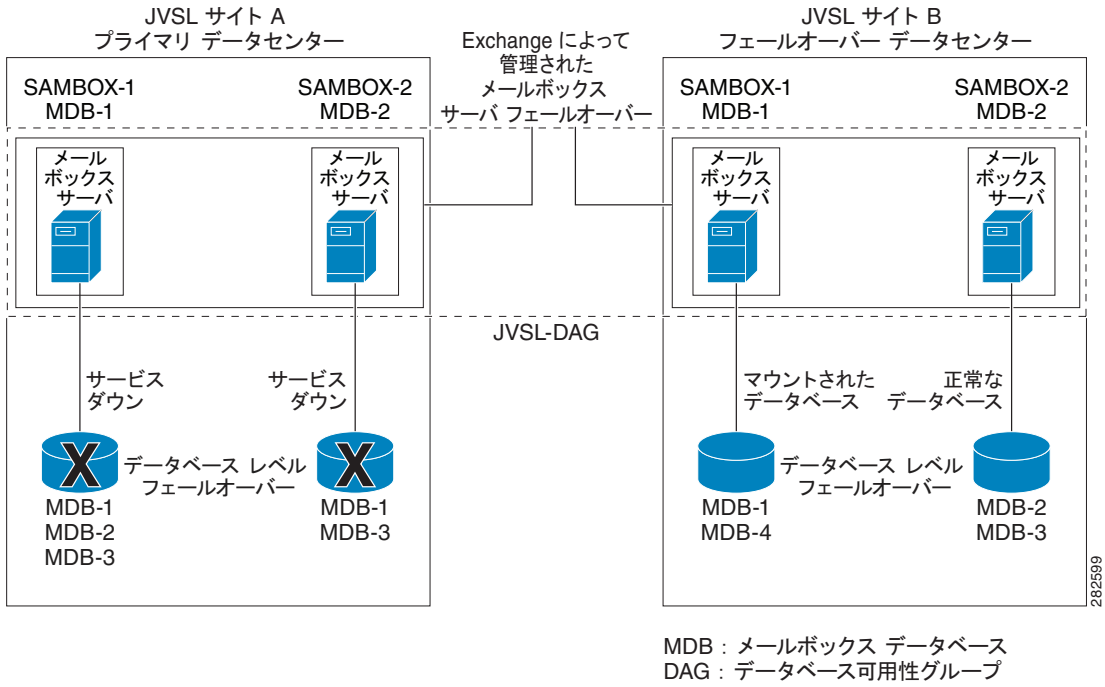
次のテスト結果が予想されます。

- ホストに接続している既存のアプリケーション トラフィックが失敗します。
- フェールオーバーが発生すると、新しい接続のすべてがもう一方の DAG ノードから供給されます。フェールバックが発生すると、電源を再投入されたノードが新しい接続を受け入れます。

テスト結果

データベース可用性グループ（サイト間フェールオーバー）の確認に成功しました。

図 3-5　サイト間フェールオーバー



MDB：メールボックス データベース
DAG：データベース可用性グループ

Load Generator のレポート

表 3-2　Microsoft Exchange Server Load Generator

テスト結果の概要	
結果：	正常
トポロジの設定	
対象のフォレスト：	ESXJVSL
ユーザ グループの総数：	2
ユーザの総数：	2

テスト結果の概要	
配布リストの総数：	0
動的な配布リストの総数：	0
連絡先の総数：	22
外部受信者の総数：	0

シミュレーションの統計情報	
シミュレーション開始：	2010 年 1 月 19 日午後 12 時 00 分 40 秒
スケジュール上の実行期間：	00 日：00 時間：10 分：00 秒
実際の実行期間：	00 日：00 時間：10 分：01 秒
ストレス モード：	True
リモート：	False

Load Generator のステータス

（注） Load Generator のクライアントは、タスク カウンタがゼロであると予測されるスクリプト モジュールで、ユーザ グループを実行します。

タイプ	名称	タスクの例外	タスク キューの長さ	スキップされたタスク	完了したタスク	ディスパッチされたタスク
マスター	PC	0	0	0	30382	30382

ユーザ グループ

名称	正常	クライアント タイプ	アクション プロファイル	ユーザ数	タスク数/ユーザ日	完了したタスク
UserGroup1	正常	Outlook 2003 オンライン	Outlook_50	1	81	5323

アクティブ ユーザの統計情報

アクティブ ユーザ数	期間
0	00:10:00

タスク実行の統計

タスク名	カウント	実際の配布（%）	設定された配布（%）
AddPublicDelegateTask	0	0	0
BrowseAddressBookTask	0	0	0
BrowseCalendarTask	732	13	13
BrowseContactsTask	604	11	11
BrowsePublicFolderTask	0	0	0
BrowseTasksTask	65	1	1

タスク名	カウント	実際の配布（%）	設定された配布（%）
CreateContactTask	68	1	1
CreateFolderTask	0	0	0
CreateTaskTask	61	1	1
DeleteMailTask	0	0	0
DownloadOabTask	60	1	1
EditRulesTask	0	0	0
EditSmartFoldersTask	68	1	0
ExportMailTask	0	0	0
InitializeMailboxTask	0	0	0
LogoffTask	201	3	3
LogonTask	0	0	0
MakeAppointmentTask	52	0	1
ModuleInitTask	1	0	0
MoveMailTask	0	0	0
PostFreeBusyTask	276	5	4
PublicFolderPostTask	0	0	0
PublishCertificatesTask	0	0	0
ReadAndProcessMessagesTask	2580	48	49
RequestMeetingTask	61	1	1
SearchTask	0	0	1
SendMailTask	494	9	8
ViewContactDetailsTask	0	0	0

タスクの例外統計

タイプ	カウント
Microsoft.Mapi.MapiExceptionLogonFailed	48
Microsoft.Mapi.MapiExceptionNetworkError	336

名称	正常	クライアント タイプ	アクション プロファイル	ユーザ数	タスク数/ユーザ日	完了したタスク
UserGroup1	正常	Outlook 2003 オンライン	Outlook_50	1	81	25059

アクティブ ユーザの統計情報

アクティブ ユーザ数	期間
1	00:10:00

タスク実行の統計

タスク名	カウント	実際の配布（%）	設定された配布（%）
AddPublicDelegateTask	0	0	0
BrowseAddressBookTask	0	0	0
BrowseCalendarTask	3451	13	13
BrowseContactsTask	2840	11	11
BrowsePublicFolderTask	0	0	0
BrowseTasksTask	294	1	1
CreateContactTask	311	1	1
CreateFolderTask	0	0	0
CreateTaskTask	312	1	1
DeleteMailTask	0	0	0
DownloadOabTask	317	1	1
EditRulesTask	0	0	0
EditSmartFoldersTask	311	1	0
ExportMailTask	0	0	0
InitializeMailboxTask	0	0	0
LogoffTask	975	3	3
LogonTask	0	0	0
MakeAppointmentTask	271	1	1
ModuleInitTask	1	0	0
MoveMailTask	0	0	0
PostFreeBusyTask	1210	4	4
PublicFolderPostTask	0	0	0
PublishCertificatesTask	0	0	0
ReadAndProcessMessagesTask	12341	49	49
RequestMeetingTask	298	1	1
SearchTask	0	0	1
SendMailTask	2127	8	8
ViewContactDetailsTask	0	0	0

タスクの例外統計

タイプ	カウント
Microsoft.Mapi.MapiExceptionNetworkError	24081

ハブ トランスポート サーバのフェールオーバー（サイト内フェールオーバー）の確認

このテストでは、プライマリ ハブ トランスポート VM が使用できない場合の Exchange トラフィックの動作を確認します。このテストは、ブランチからサイト A に 10 分間 Exchange トラフィックを送信することによって確認します。ブランチと J-VSL サイト A 間の接続は、帯域幅 T3 45 mbs および遅延 7 ～ 8 ms を使用して、距離が 100 km になるようにシミュレーションします。WAAS によって Exchange トラフィックが高速化されます。

Load Generator は、全長 10 分間のシミュレーション用に設定します。

テスト手順

ハブ トランスポート サーバ フェールオーバーの確認テストの手順は次のとおりです。

ステップ 1　サイト A に Exchange トラフィックを送信するように Load Gen が設定されていることを確認します。10 分間のテスト トラフィックを開始します。

ステップ 2　Exchange ハブ トランスポート サーバを 2 分間シャットダウンします。

ステップ 3　Load Gen から取得された結果を使用して、新しい接続のすべてが既存のハブ トランスポート サーバ経由でリダイレクトされることを確認します。

ステップ 4　2 分後に、ハブ トランスポート サーバの電源をオンにします。

ステップ 5　ホストがオンラインに戻ると、ハブ トランスポート サーバが自動的に新しい接続のロード バランスを実施します。

ステップ 6　ハブ トランスポート サーバが新しい接続のロード バランスを実施していることを確認します。

ステップ 7　トラフィックが完了したら、Load Generator のレポートを保存します。このレポートから、ハブ トランスポートのロード バランスが判断されます。

予測結果

次のテスト結果が予想されます。

- ホストに接続している既存のアプリケーションのトラフィックが失敗します。
- 新しい接続が既存のハブ トランスポート サーバから供給されます。フェールバックが発生すると、電源が再投入されたノードが新しい接続を受け入れます。

テスト結果

ハブ トランスポート サーバ フェールオーバー（サイト内フェールオーバー）の確認に成功しました。

サイト フェールオーバー中のデータベース可用性の確認

このテストでは、アプリケーション ホスト（Exchange DAG ホスト）のサイト レベル フェールオーバー中の、Exchange データベース可用性の機能を確認します。このテストは、ブランチからサイト A に 10 分間 Exchange トラフィックを送信することによって確認します。ブランチと J-VSL サイト A 間の接続は、帯域幅 T3 45 mbs および遅延 7 ～ 8 ms を使用して、距離が 100 km になるようにシミュレーションします。

Load Generator は、全長 10 分間のシミュレーション用に設定します。

テスト手順

サイト レベル障害時のデータベース可用性テストの実行手順は次のとおりです。

ステップ 1　サイト A に Exchange トラフィックを送信するように Load Gen が設定されていることを確認します。

ステップ 2　10 分間のテスト トラフィックを開始します。

ステップ 3　サイト A 内のすべてのメールボックス サーバを 2 分間シャットダウンすることによって、サイト フェールオーバーをシミュレーションします。

ステップ 4　新しい接続のすべてが、Load Gen から取得された結果を使用してマウントされる、サイト B の DAG メールボックス サーバにリダイレクトされることを確認します。

ステップ 5　最新のデータベース ファイルとログ ファイルのすべてが、サイト B のアクティブ メールボックス データベースに転送されることを確認します。

ステップ 6　サイト A のメールボックス サーバがオンラインに戻ったら、フェールオーバー クラスタ管理ツールを使用して、Exchange をフェールバックします。

ステップ 7　新しい接続のすべてをプライマリ DAG ホストが供給していることを確認します。

ステップ 8　トラフィックが完了したら、Load Generator のレポートを保存します。レポートから、メール データの損失が判断されます。

予測結果

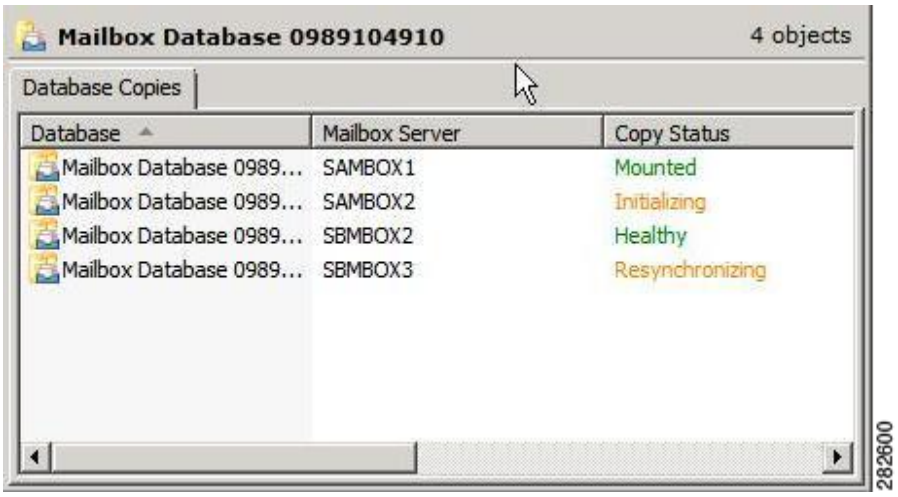
次のテスト結果が予想されます。

- ホストに接続している既存のアプリケーションのトラフィックが失敗します。
- フェールオーバーが発生すると、新しい接続のすべてがもう一方の DAG ノードから供給されます。フェールバックが発生すると、電源を再投入されたノードが新しい接続を受け入れます。

テスト結果

サイト フェールオーバー中のデータベース可用性の確認に成功しました。

図 3-6　サイト間データベース可用性



グローバル カタログ サーバのフェールオーバー（サイト間）の確認

このテストでは、グローバル カタログ サーバ（ドメイン コントローラ）のサイト レベル フェールオーバーの機能を確認します。このテストは、ブランチからサイト A に 10 分間 Exchange トラフィックを送信することによって確認します。ブランチと J-VSL サイト A 間の接続は、帯域幅 T3 45 mbs および遅延 7 ～ 8 ms を使用して、距離が 100 km になるようにシミュレーションします。

Load Generator は、全長 10 分間のシミュレーション用に設定します。

テスト手順

グローバル カタログ サーバ フェールオーバーの確認テストの手順は次のとおりです。

ステップ 1　サイト A に Exchange トラフィックを送信するように Load Gen が設定されていることを確認します。

ステップ 2　10 分間のテスト トラフィックを開始します。

ステップ 3　グローバル カタログを 2 分間シャットダウンすることによって、サイトのフェールオーバーをシミュレーションします。

ステップ 4　Load Gen から取得された結果を使用して、新しい接続のすべてがもう一方のサイトの追加ドメイン コントローラにリダイレクトされることを確認します。

ステップ 5　追加ドメイン コントローラが Active Directory ドメイン サービスを提供していることを確認します。

ステップ 6　トラフィックが完了したら、Load Generator のレポートを保存します。このレポートから、グローバル カタログ サーバのフェールオーバーとメール データの消失が確認されます。

ステップ 7　フェールバック後に、サイト B からサイト A のデータベース コピーを更新します。

ステップ 8　データベースが更新されたら、サイト A のデータベースをマウントします。

予測結果

次のテスト結果が予想されます。

- グローバル カタログ サーバの既存のドメイン サービスが失敗します。

- フェールオーバーが発生すると、新しいドメイン サービスのすべてが追加ドメイン コントローラから供給されます。フェールバックが発生すると、電源が再投入されたサーバが新しいドメイン サービスを提供します。

テスト結果

グローバル カタログ サーバ フェールオーバー（サイト間）の確認に成功しました。

ストレージ

この項では、次のテスト ケースについて説明します。

- 「サイト A とサイト B 間の FCIP セットアップ」

サイト A とサイト B 間の FCIP セットアップ

このテストでは、サイト A とサイト B の MDS 間の FCIP セットアップを確認します。Fibre Channel over IP プロトコル（FCIP）は、地理的に分散したファイバ チャネル Storage Area Network（SAN; ストレージ エリア ネットワーク）（SAN アイランド）を IP Local Area Network（LAN; ローカル エリア ネットワーク）、Metropolitan Area Network（MAN; メトロポリタン エリア ネットワーク）、および Wide Area Network（WAN; ワイド エリア ネットワーク）を介して透過的に接続するトンネリング プロトコルです。

テストの設定

IP 上での SAN 拡張パッケージ ライセンスの SAN_EXTN_OVER_IP を MDS にインストールします。

テスト手順

サイト A とサイト B 間の FCIP セットアップの確認テストの手順は次のとおりです。

ステップ 1　ギガビット イーサネット インターフェイスを設定します。

ステップ 2　FCIP プロファイルを作成してから、ギガビット イーサネット インターフェイスの IP アドレスをプロファイルに割り当てます。

ステップ 3　FCIP インターフェイスを作成し、インターフェイスにプロファイルを割り当てます。

ステップ 4　FCIP インターフェイスのピア IP アドレスを設定します。

ステップ 5　インターフェイスをイネーブルにします。

予測結果

次のテスト結果が予測されます。

- FCIP リンクが正常に確立されます。

テスト結果

サイト A とサイト B 間の FCIP セットアップに成功しました。

サービス

この項では、次のテスト ケースについて説明します。

- 「J-VSL サイト B の WAAS の設定と確認」
- 「MS-Exchange を使用した ACE サーバ ロードバランス」
- 「ANM/ACE 機能の確認」
- 「AVDC 実装の確認」
- 「vCenter から実サーバをモニタすることによる SLB の確認」
- 「Global Site Selector の障害の確認」

J-VSL サイト B の WAAS の設定と確認

このテストでは、高可用性、フェールオーバー テスト ESXi 編のセットアップ環境において、WAAS の設定を確認します。

テストの設定

WAAS がサービス スイッチ（JVSL-B-Cat6k-01）に接続されます。このデバイスは、WAAS Central Manager に登録する必要があります。

テスト手順

Exchange トラフィックを高速化するように WAAS を設定する手順は次のとおりです。

ステップ 1　WAAS が Cat6k サービス スイッチ（JVSL-B-C6k-01）に接続されていることを確認します。

ステップ 2　アプリケーション アクセラレータを初期化して、CLI プロンプトから setup コマンドを実行することによって、CLI セットアップ スクリプトを完了します。

ステップ 3　`primary-interface gigabit Ethernet 1/0` コマンドを使用して、プライマリ インターフェイスを割り当てます。

ステップ 4　デバイス モード アプリケーション アクセラレータを使用してデバイス モードを指定します。

ステップ 5　設定を保存します。

ステップ 6　WAE インターフェイスを次のように設定します。

```
waas-cm(config)# interface GigabitEthernet 1/0
waas-cm(config-if)# IP address <IP address> < mask>
waas-cm(config-if)# bandwidth 1000
waas-cm(config-if)# full-duplex
waas-cm(config-if)# no shutdown
```

ステップ 7　トラフィックを WAAS にリダイレクトするように Cat 6k を設定します。次のコマンドを使用して WCCPV2 を設定します。

```
IP wccp 61 redirect in for user access vlan
IP wccp 62 redirect in for WAN
```

ステップ 8　WAAS によって Exchange トラフィックが高速化されていることを確認します。

予測結果

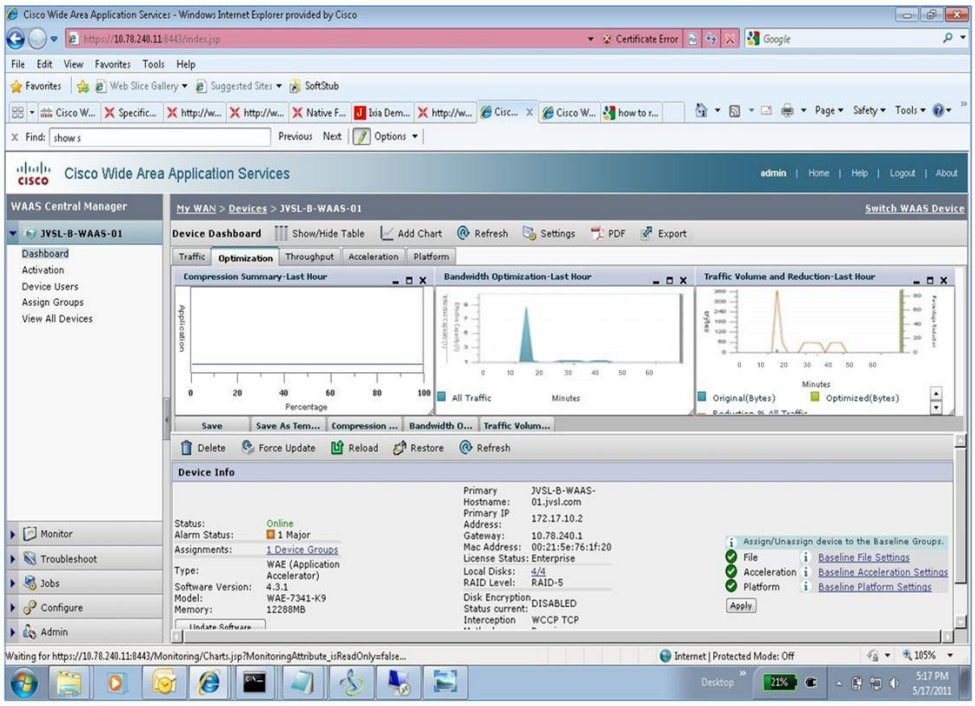
次のテスト結果が予測されます。

- WAAS は、パケットを損失することなく、Exchange トラフィックを高速化します。

テスト結果

J-VSL サイト B の WAAS の設定と確認に成功しました。

図 3-7　WAAS Central Manager GUI の出力



MS-Exchange を使用した ACE サーバ ロードバランス

このテストでは、高可用性、フェールオーバー テスト ESXi 編のセットアップ環境において、ACE サーバのロード バランスを確認します。

テスト手順

MS-Exchange を使用した ACE サーバのロード バランス テストの手順は次のとおりです。

ステップ 1　ACE が Cat6k サービス スイッチ（JVSL-B-C6k-01）に接続されていることを確認します。

ステップ 2　ACE をルーテッド モードに設定します。このモードで、クライアント VLAN とサーバ VLAN が別々の IP サブネットに属します。クライアントを VALN 30 を使用するように設定し、サーバを VLAN 200 を使用するように設定します。

ステップ 3　2 つの CAS ロールを交換するロード バランス機能を処理するように ACE を設定します。

ステップ 4　次の設定を使用して、2 つの CAS ロール用のサーバ ファームを作成します。

```
rserver host JVSL-A-UCS-01
ip address x.x.x.x
inservice
rserver host JVSL-A-UCS-02
ip address x.x.x.x
inservice
serverfarm host Server-Farm-EXh
rserver JVSL-A-UCS-01
inservice
rserver JVSL-A-UCS-02
inservice
```

ステップ 5　クラス マップを使用して、トラフィック タイプを次のように定義します。

```
policy-map type loadbalance first-match Exchange-Logic
class class-default
serverfarm Server-Farm-EXh
```

ステップ 6　次のコマンドを使用して VIP アドレスを定義します。

```
class-map match-all VIP-Server-IP
2 match virtual-address 172.17.30.5 tcp any
```

ステップ 7　ACE に対して許可されたトラフィックを次のように定義します。

```
access-list allowed-traffice-ace line 16 extended permit ip any x.x.x.x x.x.x.x
```

ステップ 8　ポリシー マップを次のように定義します。

```
policy-map multi-match exchange-policy
class VIP-Server-IP
loadbalance vip inservice
loadbalance policy Exchange-Logic
loadbalance vip icmp-reply
nat dynamic 1 vlan 200
```

ステップ 9　ポリシーを次のように適用します。

```
interface vlan 30
description Client_vlan
ip address 172.17.30.2 255.255.255.0
access-group input allowed-traffice-ace
service-policy input remote_mgmt_allow_policy
service-policy input exchange-policy
no shutdown
interface vlan 200
description Server_vlan
ip address x.x.x.x x.x.x.x
access-group input ALL
nat-pool 1 172.17.200.90 172.17.200.95 netmask 255.255.255.0 pat
service-policy input remote_mgmt_allow_policy
no shutdown
```

ステップ 10　ACE で SSL 終端機能と TCP 再利用機能をイネーブルにします。

ステップ 11　LoadGen を開始してトラフィックを生成します。

ステップ 12　次のコマンドを発行して、LoadGen 生成トラフィックから VIP へのすべての接続エントリが ACE 内に存在することを確認します。

```
show conn | inc 10.0.
```

ステップ 13　ACE が、クライアント側とサーバ側の両方のトラフィックを処理していることを確認します。

予測結果

次のテスト結果が予想されます。

- アプリケーション ホスト間の接続で ACE 負荷分散が行われます。
- 2 つの CAS インスタンス間で負荷分散が実行されるようにデータベース接続が行われます。

テスト結果

MS-Exchange を使用した ACE サーバ ロードバランシングに成功しました。

```
JVSL-B-ACE-01/Admin# sh serverfarm Server-Farm-Exchange
 serverfarm     : Server-Farm-Exchange, type: HOST
 total rservers : 2
 ---------------------------------
                                                  ----------connections-----------
       real                   weight state        current    total      failures
   ---+--------------------+------+------------+----------+----------+---------
   rserver: CAS1-SiteB
       172.17.100.15:0       8      OPERATIONAL  0          246        0
   rserver: CAS2-siteB
       172.17.100.16:0       8      OPERATIONAL  3          247        0

JVSL-B-ACE-01/Admin#


JVSL-B-ACE-01/Admin# sh service-policy int30

Status     : ACTIVE
----------------------------------------
Interface: vlan 1 30
  service-policy: int30
    class: ACE-VIP-NEW
      nat:
        nat dynamic 1 vlan 100
        curr conns       : 3        , hit count        : 497
        dropped conns    : 0
        client pkt count : 2837      , client byte count: 401410
```

```
        server pkt count : 2182      , server byte count: 668246
        conn-rate-limit      : 0         , drop-count : 0
        bandwidth-rate-limit : 0         , drop-count : 0
      loadbalance:
        L7 loadbalance policy: ACE-VIP-NEW-l7slb
        VIP ICMP Reply       : ENABLED
        VIP State: INSERVICE
        Persistence Rebalance: DISABLED
        curr conns       : 3         , hit count        : 520
        dropped conns    : 0
        client pkt count : 2873      , client byte count: 403426
        server pkt count : 2182      , server byte count: 668246
        conn-rate-limit      : 0         , drop-count : 0
        bandwidth-rate-limit : 0         , drop-count : 0
      compression:
        bytes_in  : 0
        bytes_out : 0
        Compression ratio : 0.00%

JVSL-B-ACE-01/Admin#
JVSL-B-ACE-01/Admin# sh stats

+----------------------------------------+
+------- Connection statistics ----------+
+----------------------------------------+
 Total Connections Created  : 243726
 Total Connections Current  : 3
 Total Connections Destroyed: 18436
 Total Connections Timed-out: 162
 Total Connections Failed   : 225126


+----------------------------------------+
+-------------- HTTP statistics ----------+
+----------------------------------------+
 LB parse result msgs sent : 7048       , TCP data msgs sent       : 6684
 Inspect parse result msgs : 0          , SSL data msgs sent       : 6715
                      sent
 TCP fin/rst msgs sent     : 6684       , Bounced fin/rst msgs sent: 0
 SSL fin/rst msgs sent     : 6715       , Unproxy msgs sent        : 0
 Drain msgs sent           : 6684       , Particles read           : 13732
 Reuse msgs sent           : 0          , HTTP requests            : 7048
 Reproxied requests        : 0          , Headers removed          : 0
```

```
 Headers inserted          : 0          , HTTP redirects           : 0
 HTTP chunks               : 0          , Pipelined requests       : 0
 HTTP unproxy conns        : 0          , Pipeline flushes         : 0
 Whitespace appends        : 0          , Second pass parsing      : 0
 Response entries recycled : 0          , Analysis errors          : 0
 Header insert errors      : 0          , Max parselen errors      : 0
 Static parse errors       : 0          , Resource errors          : 0
 Invalid path errors       : 0          , Bad HTTP version errors  : 0
 Headers rewritten         : 0          , Header rewrite errors    : 0


+-----------------------------------------+
+--------- HTTP Inspect statistics --------+
+-----------------------------------------+
 Total request/response   : 0
 Total allow decisions    : 0
 Total drop decisions     : 0
 Total logging decisions  : 0


+-------------------------------------------------+
+--------- HTTP Optimization statistics ---------+
+-------------------------------------------------+
 Total requests                          : 0
 Total noncondensable requests           : 0
 Total deltas                            : 0
 Total delta abandons                    : 0
 Total rebases                           : 0
 Total basefile hits                     : 0
 Total basefile misses                   : 0
 Total requested object size in bytes    : 0
 Total final response size in bytes      : 0
 Total successful transformations        : 0
 Total unsuccessful transformations      : 0
 Total transformed object requests       : 0
 Total transformed object IMS requests   : 0
 Total static object hits                : 0
 Total static object hit size in bytes   : 0
 Total static object misses              : 0
 Total static object miss size in bytes : 0
 Total refresh hits                      : 0
 Total IMS hits                          : 0
 Total IMS misses                        : 0
```

```
 Total direct requests                  : 0


+----------------------------------------+
+------- Loadbalance statistics ----------+
+----------------------------------------+
 Total version mismatch                       : 0
 Total Layer4 decisions                       : 520
 Total Layer4 rejections                      : 0
 Total Layer7 decisions                       : 7048
 Total Layer7 rejections                      : 0
 Total Layer4 LB policy misses                : 0
 Total Layer7 LB policy misses                : 0
 Total times rserver was unavailable          : 0
 Total ACL denied                             : 0
 Total IDMap Lookup Failures                  : 0
 Total Cipher Lookup Failures                 : 0
 Total Msg sent to Optimization               : 0
 Total Direct Msg received from Optimization  : 0
 Total Indirect Msg received from Optimization: 0
 Total Optimization Msg sent to Real Servers  : 0
```

ANM/ACE 機能の確認

ANM は、次の機能を実行するクライアント サーバ アプリケーションです。

- サポートされているデータセンター デバイスの機能の設定、モニタ、およびトラブルシューティング
- 運用部門、アプリケーション オーナー、およびサーバ管理スタッフが、アクティブにするためのポリシーの作成
- ネットワーク設定やトポロジの変更に関する知識や技術を使用せずに行える、ネットワークベースのサービスの一時停止

このテストでは、ANM が ACE と正しく統合されていることを確認します。

テストの設定

Red Hat Linux が搭載されたサーバに ANM 4.1 を インストールして、ACE をサービス スイッチに接続します。

テスト手順

ANM/ACE 機能の確認の手順は次のとおりです。

ステップ 1　両サイトで VIP を使用して、ANM GUI で [Guided setup] > [Import devices] をクリックすることによって、ACE デバイスを ANM に追加します。

ステップ 2　[Device] タブを使用して、ACE（JVSL-A-ACE-01 と JVSL-B-ACE-01）デバイスにアクセスできるかどうかを確認します。

ステップ 3　ACE をモニタするように SNMP を設定します。

ステップ 4　ACE 内の設定がインポートされ、ANM GUI を使用してアクセスできるかどうかを確認します。

予測結果

次のテスト結果が予測されます。

- [manage virtual server] をクリックすると、ACE サーバが ANM GUI に表示されます。

テスト結果

ANM/ACE 機能の確認に成功しました。

図 3-8　実サーバを含む ANM 出力の表示

AVDC 実装の確認

Cisco Application Control Engine 管理と VMware vCenter を統合することによって、プロビジョニングが容易になり、メンテナンス業務が合理化されます。このテストでは、VMware vCenter クライアント内の ANM 機能を確認します。

テストの設定

Red Hat Linux が搭載されたサーバに ANM 4.1 を インストールして、ACE をサービス スイッチに接続します。

テスト手順

AVDC 実装の確認テストの手順は次のとおりです。

ステップ 1　[Guided Setup] > [Import Device] をクリックして、vCenter IP を ANM に追加します。

ステップ 2　vCenter 管理者のログイン詳細を入力します。

ステップ 3　VMware vCenter サーバと ANM サーバの属性を指定することによって、ANM プラグインが登録されていることを確認します。ANM は、HTTPS とデフォルト ポートの 443 を使用して、VMware vCenter サーバおよび vCenter クライアントと通信します。

ステップ 4　Cisco ANM ソフトウェアに VMware vCenter プラグインがインストールされていることを確認します。

ステップ 5　ANM GUI が vCenter クライアントからアクセスできるかどうかを確認します。

予測結果

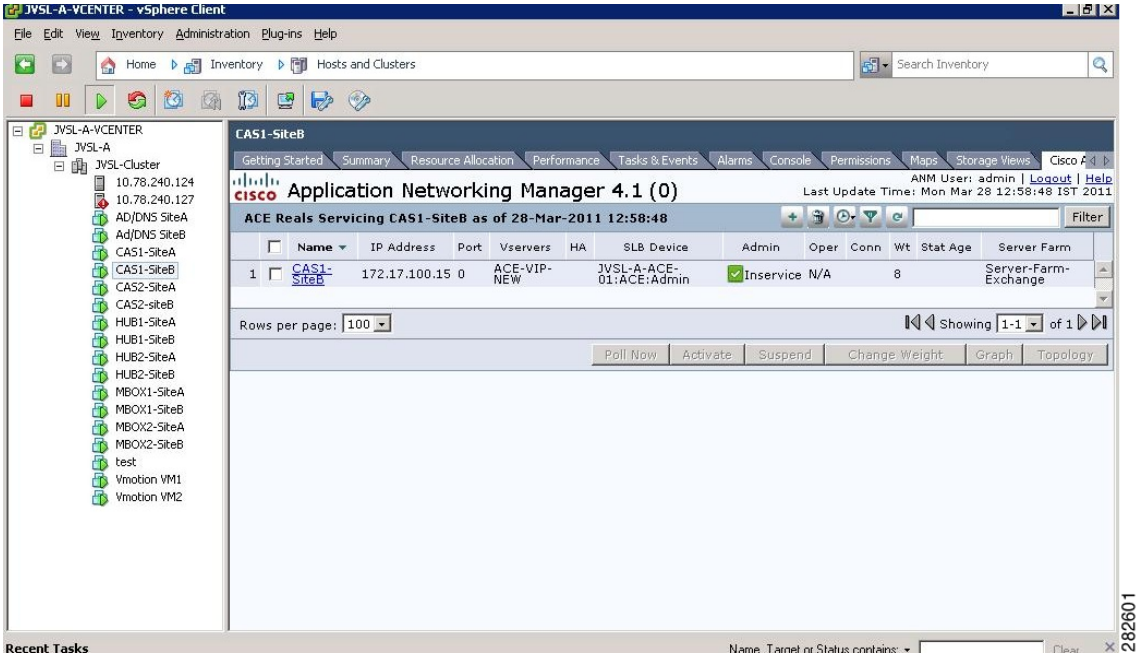
次のテスト結果が予測されます。

- ANM GUI が vCenter クライアント経由で管理されます。

テスト結果

AVDC 実装の確認に成功しました。

図 3-9　AVDC 実装



vCenter から実サーバをモニタすることによる SLB の確認

このテストでは、Exchange のロード バランス中に実サーバに関する統計情報を収集します。

テストの設定

ANM プラグインを vCenter にインストールして、各 VM で [Cisco ACE] タブが使用できるようにします。実サーバを VM に関連付けて、クライアントとサーバ間の通信を確立します。

テスト手順

vCenter から実サーバをモニタすることによる SLB の確認テストの手順は次のとおりです。

ステップ 1　VMware vCenter 内の VM ツリーから VM（CAS1-SiteB など）を選択して、[Cisco ACE] をクリックします。

ステップ 2　クライアントから OWA の URL にアクセスして、ACE 経由で OWA のロード バランスが実施されているかどうかを確認します。

ステップ 3　[Cisco ACE] で実サーバをクリックして [poll now] を選択し、グラフをクリックします。

ステップ 4　次の ACE 統計情報が表示されたグラフを使用してトラフィックをモニタします。

- Total Connections：サーバ ファーム内の実サーバに関するロード バランスが実施された接続の総数
- Connections Rate：1 秒あたりの接続数
- Dropped Connections：現在の接続数が最大許容接続数を超えた場合にドロップされる接続の総数
- Dropped Connections Rate：1 秒あたりのドロップされた接続数
- Minimum Connections：サーバ ファーム内の実サーバによってサポートされる接続の最小数
- Maximum Connections：この実サーバによってサポートされる接続の最大数

ステップ 5　ACE CLI 出力（`show conn` コマンドの発行による）と vCenter トラフィック グラフを比較します。

予測結果

次のテスト結果が予想されます。

- 実サーバ全体で Exchange トラフィックのロード バランスが実施されます。
- vCenter 内の実サーバに関する正確な統計情報が表示され、ACE CLI 出力と一致します。

テスト結果

vCenter から実サーバをモニタすることによる SLB の確認に成功しました。

図 3-10　vCenter を使用したサーバ ロード バランス

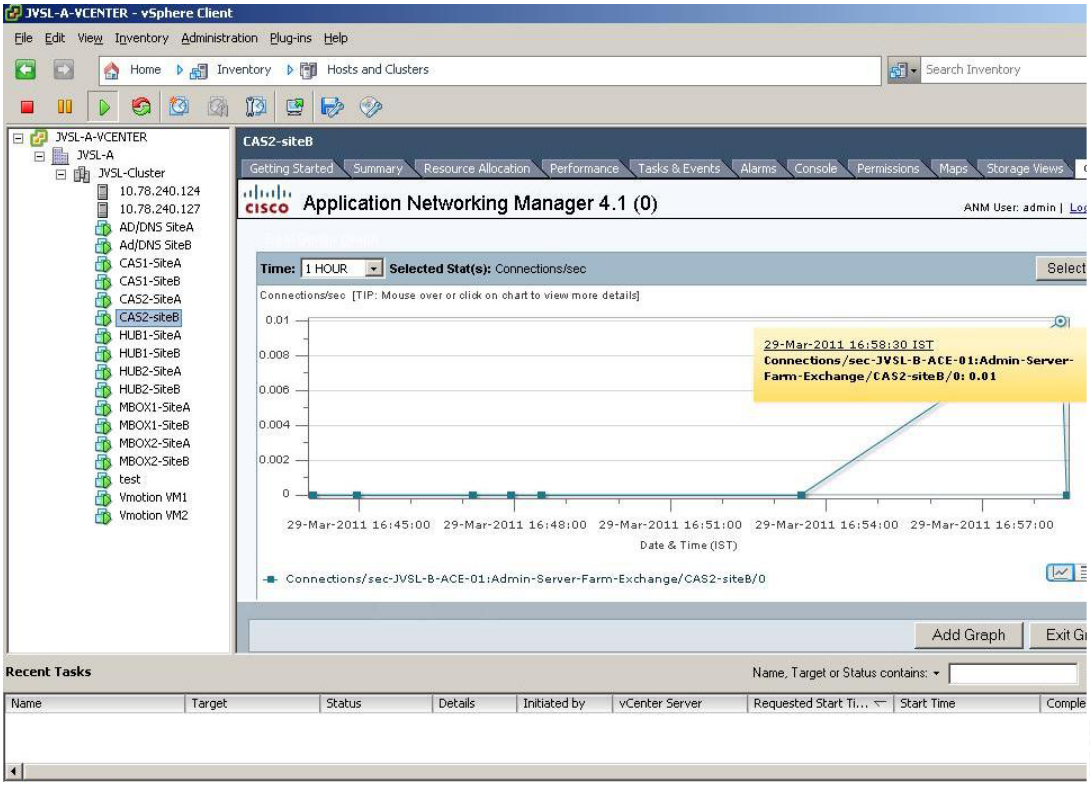
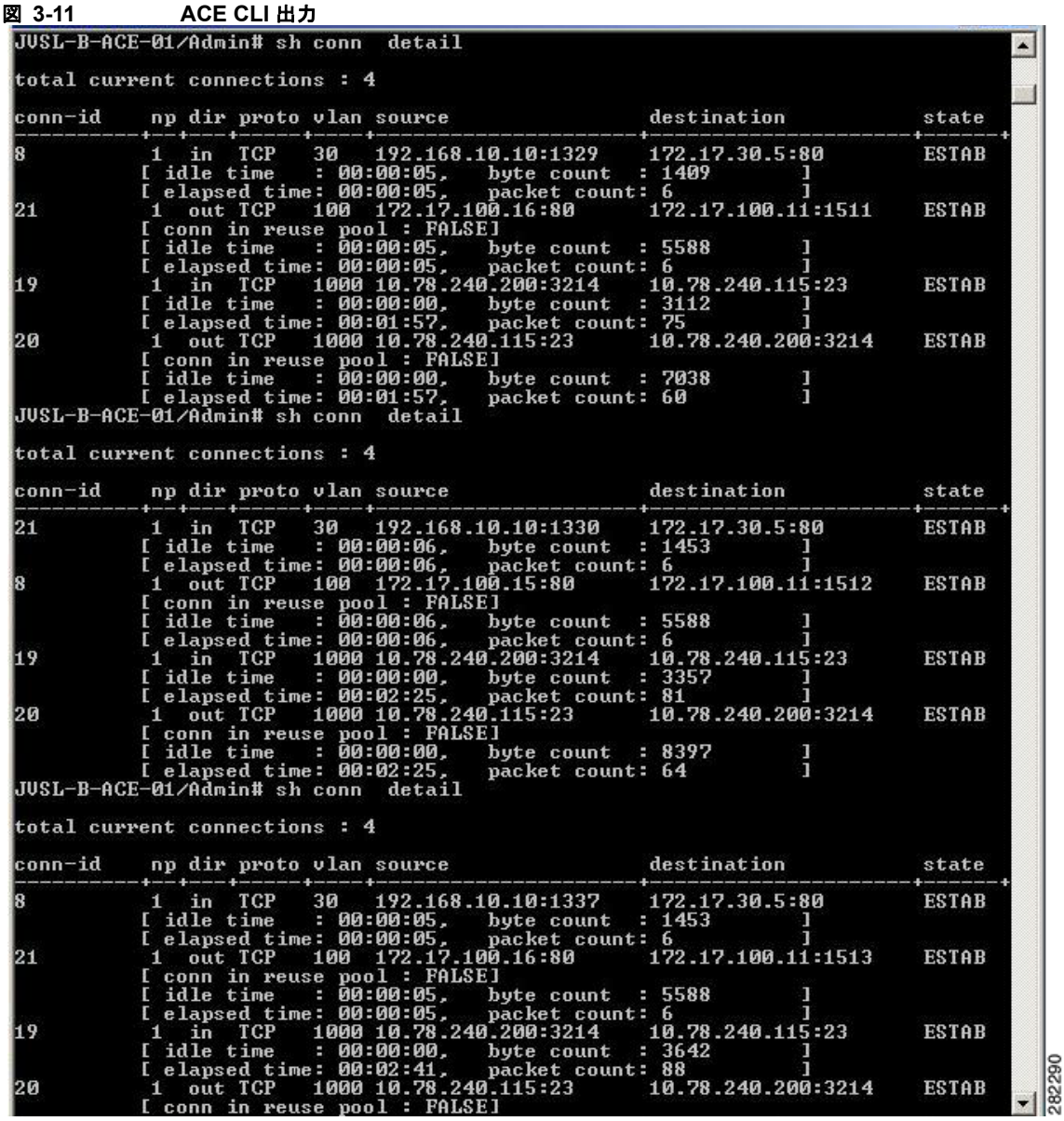


図 3-11　ACE CLI 出力



Global Site Selector の設定と確認

このテストでは、Global Site Selector で実施された設定が機能していることを確認します。

テスト手順

GSS で実施された設定の確認手順は次のとおりです。

ステップ 1　GSS をサイト A 内のプライマリ GSSM（JVSL-A-GSS-01）として設定します。

ステップ 2　x.x.x.x とドメイン（esxjvsl.com）を使用しているブランチ オフィスから DNS クエリーが届いたときに、GSS がその DNS クエリーをサイト A 内に存在する外部 DNS サーバに転送する DNS ルールを設定します。

ステップ 3　サイト A 内の GSS に対する応答は、ラウンド ロビンなどの何らかのバランシング アルゴリズムを使用するサイト A DNS サーバ（JVSL-A-DNS-01）として設定します。

ステップ 4　ブランチ オフィスからの DNS 要求をトリガーして、GSS がその要求を外部 DNS サーバに転送するかどうかを確認します。

ステップ 5　次のコマンドを発行して、クライアントが DNS サーバからの応答を受信するかどうかを確認します。

```
JVSL-A-GSS-01.cisco.com# Sh statistics dns answer-group
DNS-Answer-Group-1 totalHitCount-2
DNs-Answer-Group-1 totalHitCount-4
```

予測結果

次のテスト結果が予測されます。

- GSS が、設定されたルールどおりに、要求を外部 DNS サーバに転送します。

テスト結果

Global Site Selector の設定と確認に成功しました。

Global Site Selector の障害の確認

このテストでは、サイト A 内の GSS 障害がブランチ オフィスから届いたクエリーに影響を与えないことを確認します。これは、クエリーが他の GSS に転送されるためです。

テスト手順

サイト A での GSS 障害の確認手順は次のとおりです。

ステップ 1　JVSL-A-GSS-01 が DNS 要求を JVSL-A-DNS-01 サーバに転送し、JVSL-B-GSS-01 が DNS 要求を JVSL-B-DNS-01 に転送するように、JVSL-A-GSS-01 と JVSL-B-GSS-01 を設定します。

ステップ 2　次のコマンドを発行して、JVSL-A-GSS-01 に到達できないことを確認します。

```
JVSL-A-GSS-01.cisco.com# conf t
JVSL-A-GSS-01.cisco.com(config)#interface Ethernet 1
JVSL-A-GSS-01.cisco.com(config-eth1)#gss stop
```

ステップ 3　ブランチ オフィスのクライアントから届いたクエリーをトリガーします。クライアントが DNS サーバとして代替 JVSL-B-GSS-01 を使用するように設定され、DNS クエリーが JVSL-B-GSS-01 に配信されます。次のコマンドを発行することによって、GSS から JVSL-B-DNS-01 サーバにクライアント クエリーが転送され、応答が返されます。

```
JVSL-B-GSS-01.cisco.com# sh statistics dns answer-group
SiteB-Jvsl-Answergroup totalHitCount-1
```

予測結果

次のテスト結果が予想されます。

- クライアントが、DNS サーバとして代替 JVSL-B-GSS-01 を使用するように設定されます。DNS クエリーが JVSL-B-GSS-01 に配信され、GSS がそのクエリーを JVSL-B-DNS-01 サーバに転送してクライアント クエリーに応答します。

テスト結果

Global Site Selector の障害の確認に成功しました。

APPENDIX A

設定

ここでは、次のトピックの設定について説明します。

IP インフラストラクチャの設定

コア スイッチの設定

サイト A

```
JVSL-A-CORE-N7k-01# sh run
!Command: show running-config
!Time: Tue Mar 15 15:01:29 2011

version 5.0(3)
feature telnet
feature ospf
feature lacp

logging level aaa 5
logging level cdp 6
logging level otm 6
logging level radius 5
logging level monitor 6
logging level spanning-tree 6
logging level eth_port_channel 6
username admin password 5 $1$lwBHo9vO$SXvf74PtS6Mkih33XrQnD/  role vdc-admin
username cisco password 5 $1$k4Y8n.Ax$tCa1wPo2p74FcWJ3L5pCn/  role vdc-admin
username test password 5 $1$GajrSfmZ$YCgfSRhO8WOtW0Gpk7rBR0  role vdc-operator

banner motd #*****************************************  $ Unauthorized access
prohibited $  This system belongs to JVSL-DC team*****************************
************
```

```
#

ip domain-lookup
hostname JVSL-A-CORE-N7k-01
snmp-server user test vdc-operator auth md5 0x3aa70de12d7aa7f9e4595daeddb7a38b priv
0x3aa70de12d7aa7f9e4595daeddb7a38b localizedkey
snmp-server user admin vdc-admin auth md5 0x2a323607a1d3910babbb599e429aa31e priv
0x2a323607a1d3910babbb599e429aa31e localizedkey
snmp-server user cisco vdc-admin auth md5 0x4bb444f53704f3d53a55a815c1544170 priv
0x4bb444f53704f3d53a55a815c1544170 localizedkey
snmp-server community qwerty group vdc-operator
snmp-server community public group vdc-admin
snmp-server mib community-map qwerty context v•e
snmp-server mib community-map public context v•e

vrf context test
vrf context management
  ip route 0.0.0.0/0 10.78.240.1
vlan 1,30

interface port-channel301
  description L3_PC_TO_CORE_N7K_02
  ip address 172.16.1.13/30
  ip router ospf 10 area 0.0.0.0

interface port-channel302
  description L3_PC_TO_AGG_N7K_01
  ip address 172.16.1.17/30
  ip router ospf 10 area 0.0.0.10

interface port-channel304
  description L3_PC_TO_AGG_N7K_02
  ip address 172.16.1.25/30
  ip router ospf 10 area 0.0.0.10

interface Ethernet1/1
  description LINK_TO_CORE_N7K_02_1/1
  channel-group 301
  no shutdown

interface Ethernet1/2
  description LINK_TO_AGG_N7K_01_e1/10
  channel-group 302 mode active
  no shutdown
```

```
interface Ethernet1/3
  description LINK_TO_AGG_N7K_02_e1/11
  channel-group 304
  no shutdown

interface Ethernet1/4

interface Ethernet1/5

interface Ethernet1/6

interface Ethernet1/7

interface Ethernet1/8

interface Ethernet2/1
  description LINK_TO_ASR_G0/0/1
  ip address 172.16.1.6/30
  ip router ospf 10 area 0.0.0.0
  no shutdown

interface Ethernet2/2
  no shutdown

interface Ethernet2/3

interface Ethernet2/4

interface Ethernet2/5

interface Ethernet2/6

interface Ethernet2/7

interface Ethernet2/8

interface Ethernet7/1
  description LINK_TO_CORE_N7K_02_e7/1
  channel-group 301
  no shutdown

interface Ethernet7/2
```

```
  description LINK_TO_AGG_N7K_01_e7/10
  channel-group 302 mode active
  no shutdown

interface Ethernet7/3
  description LINK_TO_AGG_N7K_02_e7/11
  channel-group 304
  no shutdown

interface Ethernet7/4

interface Ethernet7/5

interface Ethernet7/6

interface Ethernet7/7

interface Ethernet7/8

interface mgmt0
  no snmp trap link-status
  ip address 10.78.240.3/24
logging logfile messages 6
router ospf 10

JVSL-A-CORE-N7k-02#sh run
!Command: show running-config
!Time: Tue Mar 15 15:06:51 2011

version 5.0(3)
feature telnet
feature ospf
feature lacp

username admin password 5 $1$uG2Ecslb$83uBAnLyxbf.B5cNQ3Fgh0  role vdc-admin
username cisco password 5 $1$FzHO1UgF$KOLaTJUTEaRhevdhoRXCf.  role vdc-admin

banner motd #**************************************  $ Unauthorized access
prohibited $  This system belongs to JVSL-DC team*****************************
************
#

ip domain-lookup
```

```
hostname JVSL-A-CORE-N7k-02
snmp-server user admin vdc-admin auth md5 0x5f51a94806c7dc0d4e94b790e085ecdd priv
0x5f51a94806c7dc0d4e94b790e085ecdd localizedkey
snmp-server user cisco vdc-admin auth md5 0x2dad17f0ee72c83df50d703c07e0ffd1 priv
0x2dad17f0ee72c83df50d703c07e0ffd1 localizedkey
snmp-server community public group vdc-admin
snmp-server mib community-map public context v•e

vrf context test
vrf context management
  ip route 0.0.0.0/0 10.78.240.1
vlan 1,80,100

interface port-channel301
  description L3_PC_TO_CORE_N7K_01
  ip address 172.16.1.14/30
  ip router ospf 10 area 0.0.0.0

interface port-channel303
  description L3_PC_TO_AGG_N7K_02
  ip address 172.16.1.21/30
  ip router ospf 10 area 0.0.0.10

interface port-channel305
  description L3_PC_TO_AGG_N7K_01
  ip address 172.16.1.29/30
  ip router ospf 10 area 0.0.0.10

interface Ethernet1/1
  description LINK_TO_CORE_N7K_01_e1/1
  channel-group 301
  no shutdown

interface Ethernet1/2
  description LINK_TO_AGG_N7K_01_e1/11
  channel-group 303 mode passive
  no shutdown

interface Ethernet1/3
  description LINK_TO_AGG_N7K_01_e1/11
  channel-group 305
  no shutdown

interface Ethernet1/4
```

```
  no shutdown

interface Ethernet1/5
  no shutdown

interface Ethernet1/6
  no shutdown

interface Ethernet1/7
  no shutdown

interface Ethernet1/8
  no shutdown

interface Ethernet2/1
  description LINK_TO_ASR_G0/0/2
  ip address 172.16.1.10/30
  ip router ospf 10 area 0.0.0.0
  no shutdown

interface Ethernet2/2

interface Ethernet2/3

interface Ethernet2/4

interface Ethernet2/5

interface Ethernet2/6

interface Ethernet2/7

interface Ethernet2/8

interface Ethernet7/1
  description LINK_TO_CORE_N7K_01_e7/1
  channel-group 301
  no shutdown

interface Ethernet7/2
  description LINK_TO_AGG_N7K_02_e7/10
  channel-group 303 mode passive
  no shutdown
```

```
interface Ethernet7/3
  description LINK_TO_AGG_N7K_01_e7/11
  channel-group 305
  no shutdown

interface Ethernet7/4
  no shutdown

interface Ethernet7/5
  no shutdown

interface Ethernet7/6
  no shutdown

interface Ethernet7/7
  no shutdown

interface Ethernet7/8
  no shutdown

interface Ethernet8/1

interface Ethernet8/2

interface Ethernet8/3

interface Ethernet8/4

interface Ethernet8/5

interface Ethernet8/6

interface Ethernet8/7

interface Ethernet8/8

interface mgmt0
  no snmp trap link-status
  ip address 10.78.240.5/24
logging logfile messages 6
router ospf 10
```

```
JVSL-A-CORE-N7k-02#
```

サイト B

```
JVSL-B-CORE-N7k-01# sh run

!Command: show running-config
!Time: Tue Mar 15 12:08:42 2011

version 5.1(1)
switchname JVSL-B-CORE-N7k-01

feature telnet
feature ospf
feature lacp

username admin password 5 $1$1yeXeapd$BORQEupjnHd5jFUn/XdfJ.  role vdc-admin
username cisco password 5 $1$nliWCSHk$0TNWFBiDkN.ALSXbQ15zm/  role vdc-admin

banner motd #*****************************************  $ Unauthorized access p
rohibited $  This system belongs to JVSL-DC team*********************************
*********#

ip domain-lookup
snmp-server user admin vdc-admin auth md5 0x8c3403ea5fc69c683140d8cfaf2cd793 pri
v 0x8c3403ea5fc69c683140d8cfaf2cd793 localizedkey
snmp-server user cisco vdc-admin auth md5 0x6e1e6b0dc7be6bb4b58fc83fe314265c pri
v 0x6e1e6b0dc7be6bb4b58fc83fe314265c localizedkey
snmp-server community public group vdc-admin

vrf context management
  ip route 0.0.0.0/0 10.78.240.1
vlan 1

interface port-channel301
  description L3_PC_TO_CORE_N7K_02
  ip address 172.17.1.13/30
  ip router ospf 10 area 0.0.0.0

interface port-channel302
  description L3_PC_TO_AGG_N7K_01
  ip address 172.17.1.17/30
  ip router ospf 10 area 0.0.0.10
```

```
interface port-channel304
  description L3_PC_TO_AGG_N7K_02
  shutdown
  ip address 172.17.1.25/30
  ip router ospf 10 area 0.0.0.10

interface Ethernet1/1
  description LINK_TO_CORE_N7K_02_1/1
  channel-group 301
  no shutdown

interface Ethernet1/2
  description LINK_TO_AGG_N7K_01_e1/10
  channel-group 302 mode active
  no shutdown

interface Ethernet1/3
  description LINK_TO_AGG_N7K_02_e1/11
  channel-group 304
  no shutdown

interface Ethernet1/4
  no shutdown

interface Ethernet1/5
  no shutdown

interface Ethernet1/6
  no shutdown

interface Ethernet1/7
  no shutdown

interface Ethernet1/8
  no shutdown

interface Ethernet2/1
  description LINK_TO_ASR_G0/0/1
  ip address 172.17.1.6/30
  ip router ospf 10 area 0.0.0.0
  no shutdown
```

```
interface Ethernet2/2

interface Ethernet2/3

interface Ethernet2/4

interface Ethernet2/5

interface Ethernet2/6

interface Ethernet2/7

interface Ethernet2/8

interface Ethernet7/1
  description LINK_TO_CORE_N7K_02_e7/1
  channel-group 301
  no shutdown

interface Ethernet7/2
  description LINK_TO_AGG_N7K_01_e7/10
  channel-group 302 mode active
  no shutdown

interface Ethernet7/3
  description LINK_TO_AGG_N7K_02_e7/11
  channel-group 304
  no shutdown

interface Ethernet7/4
  no shutdown

interface Ethernet7/5
  no shutdown

interface Ethernet7/6
  no shutdown

interface Ethernet7/7
  no shutdown

interface Ethernet7/8
  no shutdown
```

```
interface mgmt0
  ip address 10.78.240.103/24
line vty
router ospf 10


JVSL-B-CORE-N7k-01#




JVSL-B-CORE-N7k-01# sh run

!Command: show running-config
!Time: Tue Mar 15 12:08:42 2011

version 5.1(1)
switchname JVSL-B-CORE-N7k-01

feature telnet
feature ospf
feature lacp

username admin password 5 $1$1yeXeapd$BORQEupjnHd5jFUn/XdfJ.  role vdc-admin
username cisco password 5 $1$nliWCSHk$0TNWFBiDkN.ALSXbQl5zm/  role vdc-admin

banner motd #*****************************************  $ Unauthorized access p
rohibited $  This system belongs to JVSL-DC team*******************************
*********#

ip domain-lookup
snmp-server user admin vdc-admin auth md5 0x8c3403ea5fc69c683140d8cfaf2cd793 pri
v 0x8c3403ea5fc69c683140d8cfaf2cd793 localizedkey
snmp-server user cisco vdc-admin auth md5 0x6e1e6b0dc7be6bb4b58fc83fe314265c pri
v 0x6e1e6b0dc7be6bb4b58fc83fe314265c localizedkey
snmp-server community public group vdc-admin

vrf context management
  ip route 0.0.0.0/0 10.78.240.1
vlan 1

interface port-channel301
```

```
  description L3_PC_TO_CORE_N7K_02
  ip address 172.17.1.13/30
  ip router ospf 10 area 0.0.0.0

interface port-channel302
  description L3_PC_TO_AGG_N7K_01
  ip address 172.17.1.17/30
  ip router ospf 10 area 0.0.0.10

interface port-channel304
  description L3_PC_TO_AGG_N7K_02
  shutdown
  ip address 172.17.1.25/30
  ip router ospf 10 area 0.0.0.10

interface Ethernet1/1
  description LINK_TO_CORE_N7K_02_1/1
  channel-group 301
  no shutdown

interface Ethernet1/2
  description LINK_TO_AGG_N7K_01_e1/10
  channel-group 302 mode active
  no shutdown

interface Ethernet1/3
  description LINK_TO_AGG_N7K_02_e1/11
  channel-group 304
  no shutdown

interface Ethernet1/4
  no shutdown

interface Ethernet1/5
  no shutdown

interface Ethernet1/6
  no shutdown

interface Ethernet1/7
  no shutdown

interface Ethernet1/8
```

```
  no shutdown

interface Ethernet2/1
  description LINK_TO_ASR_G0/0/1
  ip address 172.17.1.6/30
  ip router ospf 10 area 0.0.0.0
  no shutdown

interface Ethernet2/2

interface Ethernet2/3

interface Ethernet2/4

interface Ethernet2/5

interface Ethernet2/6

interface Ethernet2/7

interface Ethernet2/8

interface Ethernet7/1
  description LINK_TO_CORE_N7K_02_e7/1
  channel-group 301
  no shutdown

interface Ethernet7/2
  description LINK_TO_AGG_N7K_01_e7/10
  channel-group 302 mode active
  no shutdown

interface Ethernet7/3
  description LINK_TO_AGG_N7K_02_e7/11
  channel-group 304
  no shutdown

interface Ethernet7/4
  no shutdown

interface Ethernet7/5
  no shutdown
```

```
interface Ethernet7/6
  no shutdown

interface Ethernet7/7
  no shutdown

interface Ethernet7/8
  no shutdown

interface mgmt0
  ip address 10.78.240.103/24
line vty
router ospf 10


JVSL-B-CORE-N7k-01#

JVSL-B-CORE-N7k-02# sh run

!Command: show running-config
!Time: Tue Mar 15 15:08:12 2011

version 5.1(1)
switchname JVSL-B-CORE-N7k-02

feature telnet
feature ospf
feature lacp

username admin password 5 $1$3QloJrRP$7X2Qe5sBczJ92WwaFYYxP/  role vdc-admin
username cisco password 5 $1$WyfjIhkv$KuG7bmKXmPlhcZqXVTrHy0  role vdc-admin

banner motd #*****************************************  $ Unauthorized access p
rohibited $  This system belongs to JVSL-DC team*********************************
*********#

ip domain-lookup
snmp-server user admin vdc-admin auth md5 0x38fec3600cbc29b1938f0be12e1fc420 pri
v 0x38fec3600cbc29b1938f0be12e1fc420 localizedkey
snmp-server user cisco vdc-admin auth md5 0x0580c0b7d1bf22227f39c04facac1f00 pri
v 0x0580c0b7d1bf22227f39c04facac1f00 localizedkey
snmp-server community public group vdc-admin
```

```
vrf context management
  ip route 0.0.0.0/0 10.78.240.1
vlan 1

interface port-channel301
  description L3_PC_TO_CORE_N7K_01
  ip address 172.17.1.14/30
  ip router ospf 10 area 0.0.0.0

interface port-channel303
  description L3_PC_TO_AGG_N7K_02
  ip address 172.17.1.21/30
  ip router ospf 10 area 0.0.0.10

interface port-channel305
  description L3_PC_TO_AGG_N7K_01
  ip address 172.17.1.29/30
  ip router ospf 10 area 0.0.0.10

interface Ethernet1/1
  description LINK_TO_CORE_N7K_01_e1/1
  channel-group 301
  no shutdown

interface Ethernet1/2
  description LINK_TO_AGG_N7K_01_e1/11
  channel-group 303 mode passive
  no shutdown

interface Ethernet1/3
  description LINK_TO_AGG_N7K_01_e1/11
  channel-group 305
  no shutdown

interface Ethernet1/4
  no shutdown

interface Ethernet1/5
  no shutdown

interface Ethernet1/6
  no shutdown
```

```
interface Ethernet1/7
  no shutdown

interface Ethernet1/8
  no shutdown

interface Ethernet2/1
  description LINK_TO_ASR_G0/0/2
  ip address 172.17.1.10/30
  ip router ospf 10 area 0.0.0.0
  no shutdown

interface Ethernet2/2

interface Ethernet2/3

interface Ethernet2/4

interface Ethernet2/5

interface Ethernet2/6

interface Ethernet2/7

interface Ethernet2/8

interface Ethernet7/1
  description LINK_TO_CORE_N7K_01_e7/1
  channel-group 301
  no shutdown

interface Ethernet7/2
  description LINK_TO_AGG_N7K_02_e7/10
  channel-group 303 mode passive
  no shutdown

interface Ethernet7/3
  description LINK_TO_AGG_N7K_01_e7/11
  channel-group 305
  no shutdown

interface Ethernet7/4
  no shutdown
```

```
interface Ethernet7/5
  no shutdown

interface Ethernet7/6
  no shutdown

interface Ethernet7/7
  no shutdown

interface Ethernet7/8
  no shutdown

interface mgmt0
  ip address 10.78.240.105/24
line vty

JVSL-B-CORE-N7k-02#
```

集約スイッチの設定

サイト A

```
JVSL-A-AGG-N7k-01#sh run
!Command: show running-config
!Time: Tue Mar 15 15:05:20 2011

version 5.0(3)
feature telnet
cfs eth distribute
feature ospf
feature isis
feature pbr
feature interface-vlan
feature hsrp
feature lacp
feature vpc

username admin password 5 $1$t0UAxiDB$Q85LIDWdVoYbKW./bvwMG0  role vdc-admin
username cisco password 5 $1$.i/DPf6e$5zOEd6zWHRzejKn5S7DKT.  role vdc-admin

banner motd #**************************************  $ Unauthorized access prohibited
$  This system belongs to JVSL-DC team*****************************
************
#

ip domain-lookup
hostname JVSL-A-AGG-N7k-01
access-list cleanup-unused-policies
snmp-server user admin vdc-admin auth md5 0x2a323607a1d3910babbb599e429aa31e priv
0x2a323607a1d3910babbb599e429aa31e localizedkey
```

```
snmp-server user cisco vdc-admin auth md5 0x2a323607a1d3910babbb599e429aa31e priv
0x2a323607a1d3910babbb599e429aa31e localizedkey
snmp-server community public group vdc-admin
snmp-server mib community-map public context v•e

vrf context vPC
vrf context test
vrf context management
  ip route 0.0.0.0/0 10.78.240.1
vlan 1,10,20,30,40,80,100
vlan 170
  name OTV_VLAN
vlan 200
spanning-tree vlan 100 priority 24576
ip prefix-list Pre_ACE seq 5 permit 192.16.10.0/24
route-map Server-to-Client-Traffic pbr-statistics
route-map Server-to-Client-Traffic permit 10
  match ip address match-Server-to-client
  set ip next-hop 172.16.1.38
route-map client_traffic_to_ACE_VIP permit 10
  match ip address match-Server-VIP
  set ip next-hop 172.16.1.38
route-map traffic_to_server pbr-statistics
route-map traffic_to_server permit 10
  match ip address match_any_toServer
  set ip next-hop 172.16.1.38
vpc domain 10
  role priority 5
  peer-keepalive destination 172.16.1.34 source 172.16.1.33 vrf vPC
  peer-gateway


interface Vlan1

interface Vlan7

interface Vlan10
  no shutdown
  description WAAS_WAN_VLAN
  no ip redirects
  ip router ospf 10 area 0.0.0.10

interface Vlan30
  no shutdown
  no ip redirects
  ip router ospf 10 area 0.0.0.10

interface Vlan80
  no shutdown
  no ip redirects
  ip router ospf 10 area 0.0.0.10

interface Vlan100
  no ip redirects
  ip address 172.16.100.2/24
  ip router ospf 10 area 0.0.0.10
  ip policy route-map Server-to-Client-Traffic
  hsrp 100
    preempt delay minimum 60
    priority 150
    ip 172.16.100.1

interface Vlan170
  no shutdown
```

```
  no ip redirects
  ip address 172.16.170.2/24
  ip router ospf 10 area 0.0.0.10
  hsrp 207
    preempt delay minimum 60
    priority 150
    ip 172.16.170.1

interface Vlan200
  no shutdown
  no ip redirects
  ip address 172.16.200.2/24
  ip ospf priority 10
  ip router ospf 10 area 0.0.0.10
  hsrp 200
    preempt delay minimum 60
    priority 150
    ip 172.16.200.1

interface port-channel176
  description L2_PC_TO_CAT6K
  ip address 172.16.1.37/30
  ip router ospf 10 area 0.0.0.10

interface port-channel201
  description L2_PC_TO_AGG_N7K_02
  switchport
  switchport mode trunk
  vpc peer-link
  switchport trunk allowed vlan 10,20,30,80,100,170,200
  spanning-tree port type network

interface port-channel202
  description L2_PC_TO_ACC_N5K_01
  switchport
  switchport mode trunk
  vpc 10
  switchport trunk allowed vlan 10,20,30,80,100,170,200

interface port-channel203

interface port-channel204
  description L2_PC_TO_ACC_N5K_02
  switchport
  switchport mode trunk
  vpc 11
  switchport trunk allowed vlan 10,20,30,80,100,170,200

interface port-channel205

interface port-channel302
  description L3_PC_TO_CORE_N7K_01
  ip address 172.16.1.18/30
  ip router ospf 10 area 0.0.0.10

interface port-channel305
  description L3_PC_TO_CORE_N7K_02
  ip address 172.16.1.30/30
  ip router ospf 10 area 0.0.0.10

interface Ethernet1/9
  description LINK_TO_AGG_N7K_02_e1/9
  switchport
  switchport mode trunk
```

```
  switchport trunk allowed vlan 10,20,30,80,100,170,200
  channel-group 201
  no shutdown

interface Ethernet1/10
  description LINK_TO_CORE_N7K_01_e1/2
  channel-group 302 mode passive
  no shutdown

interface Ethernet1/11
  description LINK_TO_CORE_N7K_02_e1/3
  channel-group 305
  no shutdown

interface Ethernet1/12
  description LINK_TO_ACC_N5K_01_e1/1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,30,80,100,170,200
  channel-group 202 mode active
  no shutdown

interface Ethernet1/13
  description LINK_TO_ACC_N5K_02_e1/2
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,30,80,100,170,200
  channel-group 204 mode active
  no shutdown

interface Ethernet1/14

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19

interface Ethernet1/20

interface Ethernet1/21
  ip address 172.18.1.5/30
  ip ospf passive-interface
  ip router ospf 10 area 0.0.0.10
  no shutdown

interface Ethernet1/22
  description "OTV_Join-int_connected_OTV01_e1/25"
  ip address 172.16.2.1/30
  ip ospf network point-to-point
  ip router ospf 10 area 0.0.0.10
  ip igmp version 3
  no shutdown

interface Ethernet1/23
  description Connected_to_OTV-01_e1/26
  switchport
  switchport mode trunk
  no shutdown
```

```
interface Ethernet1/24
  description VPC_KEEPALIVE_AGG_N7K_02
  vrf member vPC
  ip address 172.16.1.33/30
  no shutdown

interface Ethernet7/9
  description LINK_TO_AGG_N7K_02_e7/9
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,30,80,100,170,200
  channel-group 201
  no shutdown

interface Ethernet7/10
  description LINK_TO_CORE_N7K_01_e7/1
  channel-group 302 mode passive
  no shutdown

interface Ethernet7/11
  description LINK_TO_CORE_N7k_02_e7/3
  channel-group 305
  no shutdown

interface Ethernet7/12
  description LINK_TO_ACC_N5K_01_e1/3
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,30,80,100,170,200
  channel-group 202 mode active
  no shutdown

interface Ethernet7/13
  description LINK_TO_AC_N5K_01_e1/4
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,30,80,100,170,200
  channel-group 204 mode active
  no shutdown

interface Ethernet7/14

interface Ethernet7/15

interface Ethernet7/16

interface Ethernet7/17

interface Ethernet7/18

interface Ethernet7/19

interface Ethernet7/20

interface Ethernet7/21

interface Ethernet7/22

interface Ethernet7/23
  description LINK_TO_CAT6K_T1/1
  channel-group 176 mode active
  no shutdown

interface Ethernet7/24
```

```
  description LINK_TO_CAT6K_T1/2
  channel-group 176 mode active
  no shutdown

interface mgmt0
  no snmp trap link-status
  ip address 10.78.240.4/24
logging logfile messages 6
router ospf 10
ip route 172.16.30.0/24 172.16.1.38
ip route 172.16.30.2/32 172.16.1.38
JVSL-A-AGG-N7k-01#

JVSL-A-AGG-N7k-02#sh run
!Command: show running-config
!Time: Tue Mar 15 15:08:18 2011

version 5.0(3)
feature telnet
cfs eth distribute
feature ospf
feature pbr
feature interface-vlan
feature hsrp
feature lacp
feature vpc

logging level aaa 5
logging level cdp 6
logging level otm 6
logging level vpc 6
logging level hsrp 6
logging level radius 5
logging level monitor 6
logging level spanning-tree 6
logging level interface-vlan 5
logging level eth_port_channel 6
username admin password 5 $1$iDVMHN5O$Cu4kqEDIoOQjNAavnY3nh.  role vdc-admin
username cisco password 5 $1$DxRjx2hX$KkowsI1Mb1ekd34KtCmM71  role vdc-admin

banner motd #****************************************  $ Unauthorized access prohibited
$  This system belongs to JVSL-DC team*****************************
************
#

ip domain-lookup
hostname JVSL-A-AGG-N7k-02
snmp-server user admin vdc-admin auth md5 0x5f51a94806c7dc0d4e94b790e085ecdd priv
0x5f51a94806c7dc0d4e94b790e085ecdd localizedkey
snmp-server user cisco vdc-admin auth md5 0x2dad17f0ee72c83df50d703c07e0ffd1 priv
0x2dad17f0ee72c83df50d703c07e0ffd1 localizedkey
snmp-server community qwerty group vdc-operator
snmp-server community public group vdc-admin
snmp-server mib community-map qwerty context v•e
snmp-server mib community-map public context v•e

vrf context vPC
vrf context management
  ip route 0.0.0.0/0 10.78.240.1
vlan 1,10,20,30,80,100
vlan 170
  name OTV_VLAN
vlan 200
spanning-tree vlan 100 priority 28672
```

```
route-map client_traffic pbr-statistics
route-map client_traffic permit 10
  match ip address match_client_traffic
  set ip default next-hop 172.16.10.1
route-map client_traffic_to_ACE_VIP permit 10
  match ip address match-Server-VIP
  set ip next-hop 172.16.1.42
route-map traffic_to_Server pbr-statistics
route-map traffic_to_Server permit 10
  match ip address match-any-toServer
  set ip next-hop 172.16.1.42
vpc domain 10
  role priority 10
  peer-keepalive destination 172.16.1.33 source 172.16.1.34 vrf vPC
  peer-gateway


interface Vlan1

interface Vlan10
  no shutdown

interface Vlan30
  no shutdown
  no ip redirects
  ip router ospf 10 area 0.0.0.10

interface Vlan80
  no shutdown
  no ip redirects
  ip router ospf 10 area 0.0.0.10

interface Vlan100
  no shutdown
  no ip redirects
  ip address 172.16.100.3/24
  ip router ospf 10 area 0.0.0.10
  hsrp 100
    preempt delay minimum 60
    priority 110
    ip 172.16.100.1

interface Vlan170
  no shutdown
  no ip redirects
  ip address 172.16.170.3/24
  ip router ospf 10 area 0.0.0.10
  hsrp 207
    preempt delay minimum 60
    priority 120
    ip 172.16.170.1

interface Vlan200
  no shutdown
  no ip redirects
  ip address 172.16.200.3/24
  ip router ospf 10 area 0.0.0.10
  hsrp 200
    preempt delay minimum 60
    priority 110
    ip 172.16.200.1

interface port-channel201
  description L2_PC_TO_AGG_N7k_01
```

```
  switchport
  switchport mode trunk
  vpc peer-link
  switchport trunk allowed vlan 7,10,20,80,100,170,200
  spanning-tree port type network

interface port-channel203
  description L2_PC_TO_ACC_N5K_02
  switchport
  switchport mode trunk
  vpc 11
  switchport trunk allowed vlan 10,20,80,100,170,200

interface port-channel205
  description L2_PC_TO_ACC_N5K_01
  switchport
  switchport mode trunk
  vpc 10
  switchport trunk allowed vlan 10,20,80,100,170,200

interface port-channel276
  description L3_PC_to_Cat6k
  ip address 172.16.1.41/30
  ip router ospf 10 area 0.0.0.10

interface port-channel303
  description L3_PC_TO_CORE_N7K_02
  ip address 172.16.1.22/30
  ip router ospf 10 area 0.0.0.10

interface port-channel304
  description L3_PC_TO_CORE_N7K_01
  ip address 172.16.1.26/30
  ip router ospf 10 area 0.0.0.10

interface Ethernet1/9
  description LINK_TO_AGG_N7K_01_e1/9
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 7,10,20,80,100,170,200
  channel-group 201
  no shutdown

interface Ethernet1/10
  description LINK_TO_CORE_N7K_02_e1/2
  channel-group 303 mode active
  no shutdown

interface Ethernet1/11
  description LINK_TO_CORE_N7K_01_e1/3
  channel-group 304
  no shutdown

interface Ethernet1/12
  description LINK_TO_ACC_N5k_02_e1/1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 203 mode active
  no shutdown

interface Ethernet1/13
  description LINK_TO_ACC_N5K_01_e1/2
  switchport
```

```
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 205 mode active
  no shutdown

interface Ethernet1/14
  no shutdown

interface Ethernet1/15
  no shutdown

interface Ethernet1/16
  no shutdown

interface Ethernet1/17
  switchport
  switchport mode trunk
  no shutdown

interface Ethernet1/18
  no shutdown

interface Ethernet1/19
  no shutdown

interface Ethernet1/20
  no shutdown

interface Ethernet1/21
  ip address 172.18.2.5/30
  ip ospf passive-interface
  ip router ospf 10 area 0.0.0.10
  no shutdown

interface Ethernet1/22
  description "OTV_Join-int_connected_OTV02_e1/25"
  ip address 172.16.2.5/30
  ip ospf network point-to-point
  ip router ospf 10 area 0.0.0.10
  ip igmp version 3
  no shutdown

interface Ethernet1/23
  description Connected_to_OTV_e1/26
  switchport
  switchport mode trunk
  no shutdown

interface Ethernet1/24
  description VPC_KEEPALIVE_TO_AGG_N7K_01_1/24
  vrf member vPC
  ip address 172.16.1.34/30
  no shutdown

interface Ethernet7/9
  description LINK_TO_AGG_N7K_01_e7/9
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 7,10,20,80,100,170,200
  channel-group 201
  no shutdown

interface Ethernet7/10
  description LINK_TO_CORE_N7K_02_e7/2
```

```
  channel-group 303 mode active
  no shutdown

interface Ethernet7/11
  description LINK_TO_CORE_N7K_01_e7/3
  channel-group 304
  no shutdown

interface Ethernet7/12
  description LINK_TO_ACC_N5K_02_e1/3
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 203 mode active
  no shutdown

interface Ethernet7/13
  description LINK_TO_ACC_N5K_01_e1/4
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 205 mode active
  no shutdown

interface Ethernet7/14
  no shutdown

interface Ethernet7/15
  no shutdown

interface Ethernet7/16
  no shutdown

interface Ethernet7/17
  no shutdown

interface Ethernet7/18
  no shutdown

interface Ethernet7/19
  no shutdown

interface Ethernet7/20
  no shutdown

interface Ethernet7/21
  no shutdown

interface Ethernet7/22
  no shutdown

interface Ethernet7/23
  description LINK_TO_CAT6K_T1/3
  channel-group 276 mode active
  no shutdown

interface Ethernet7/24
  description LINK_TO_CAT6K_T1/4
  channel-group 276 mode active
  no shutdown

interface Ethernet8/9

interface Ethernet8/10
```

```
interface Ethernet8/11

interface Ethernet8/12

interface Ethernet8/13
  no shutdown

interface Ethernet8/14
  no shutdown

interface Ethernet8/15

interface Ethernet8/16

interface Ethernet8/17

interface Ethernet8/18

interface Ethernet8/19

interface Ethernet8/20

interface Ethernet8/21

interface Ethernet8/22

interface Ethernet8/23

interface Ethernet8/24

interface mgmt0
  no snmp trap link-status
  ip address 10.78.240.6/24
logging logfile messages 6
router ospf 10
ip access-list match-local-traffic
JVSL-A-AGG-N7k-02#
```

サイト B

```
JVSL-B-AGG-N7k-01# sh run


!Command: show running-config
!Time: Tue Mar 15 12:20:10 2011


version 5.1(1)
switchname JVSL-B-AGG-N7k-01


feature telnet
cfs eth distribute
feature ospf
feature pbr
feature interface-vlan
feature hsrp
```

```
feature lacp
feature vpc

username admin password 5 $1$nm7DABE.$5lTRIBTNOh4NVvqrf2EzH.  role vdc-admin
username cisco password 5 $1$kd.egEim$NK5QRub/bsoGbUCUsdWTd0  role vdc-admin
ip domain-lookup
snmp-server user admin vdc-admin auth md5 0x8c3403ea5fc69c683140d8cfaf2cd793 priv
0x8c3403ea5fc69c683140d8cfaf2cd793 localizedkey
snmp-server user cisco vdc-admin auth md5 0x6e1e6b0dc7be6bb4b58fc83fe314265c priv
0x6e1e6b0dc7be6bb4b58fc83fe314265c localizedkey
snmp-server community public group vdc-admin

vrf context vPC
vrf context management
  ip route 0.0.0.0/0 10.78.240.1
vlan 1,80,100
vlan 170
  name OTV_VLAN
vlan 200
vpc domain 10
  role priority 5
  peer-keepalive destination 172.17.1.34 source 172.17.1.33 vrf vPC
  peer-gateway

interface Vlan1

interface Vlan80
  no shutdown
  ip router ospf 10 area 0.0.0.10

interface Vlan100
  no ip redirects
  ip address 172.17.100.2/24
  ip router ospf 10 area 0.0.0.10
  ip policy route-map Server-to-Client-Traffic
  hsrp 100
    preempt delay minimum 60
    priority 150
    ip 172.17.100.1

interface Vlan170
  no shutdown
  no ip redirects
  ip address 172.16.170.3/24
```

```
  ip router ospf 10 area 0.0.0.10
  hsrp 207
    preempt delay minimum 60
    priority 110
    ip 172.16.170.1

interface Vlan200
  no shutdown
  no ip redirects
  ip address 172.17.200.2/24
  ip router ospf 10 area 0.0.0.10
  hsrp 200
    preempt delay minimum 60
    priority 150
    ip 172.17.200.1

interface port-channel176
  description L2_PC_TO_CAT6K
  ip address 172.17.1.37/30
  ip router ospf 10 area 0.0.0.10

interface port-channel201
  description L2_PC_TO_AGG_N7K_02
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  spanning-tree port type network
  vpc peer-link

interface port-channel202
  description L2_PC_TO_ACC_N5K_01
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  vpc 10

interface port-channel204
  description L2_PC_TO_ACC_N5K_02
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  vpc 11
```

```
interface port-channel302
  description L3_PC_TO_CORE_N7K_01
  ip address 172.17.1.18/30
  ip router ospf 10 area 0.0.0.10

interface port-channel305
  description L3_PC_TO_CORE_N7K_02
  ip address 172.17.1.30/30
  ip router ospf 10 area 0.0.0.10

interface Ethernet1/9
  description LINK_TO_AGG_N7K_02_e1/9
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 201
  no shutdown

interface Ethernet1/10
  description LINK_TO_CORE_N7K_01_e1/2
  channel-group 302 mode passive
  no shutdown

interface Ethernet1/11
  description LINK_TO_CORE_N7K_02_e1/3
  channel-group 305
  no shutdown

interface Ethernet1/12
  description LINK_TO_ACC_N5K_01_e1/1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 202 mode active
  no shutdown

interface Ethernet1/13
  description LINK_TO_ACC_N5K_02_e1/2
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 204 mode active
  no shutdown
```

```
interface Ethernet1/14
  no shutdown

interface Ethernet1/15
  no shutdown

interface Ethernet1/16
  no shutdown

interface Ethernet1/17
  no shutdown

interface Ethernet1/18
  no shutdown

interface Ethernet1/19
  no shutdown

interface Ethernet1/20
  no shutdown

interface Ethernet1/21
  ip address 172.18.1.6/30
  ip ospf passive-interface
  ip router ospf 10 area 0.0.0.10
  no shutdown

interface Ethernet1/22
  description "OTV_Join-int_connected_B-OTV01_e1/25"
  ip address 172.17.2.1/30
  ip ospf network point-to-point
  ip router ospf 10 area 0.0.0.10
  ip igmp version 3
  no shutdown

interface Ethernet1/23
  description "connected_to_B-OTV_01_e1/26"
  switchport
  switchport mode trunk
  no shutdown

interface Ethernet1/24
```

```
  description VPC_KEEPALIVE_AGG_N7K_02
  vrf member vPC
  ip address 172.17.1.33/30
  no shutdown

interface Ethernet7/9
  description LINK_TO_AGG_N7K_02_e7/9
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 201
  no shutdown

interface Ethernet7/10
  description LINK_TO_CORE_N7K_01_e7/1
  channel-group 302 mode passive
  no shutdown

interface Ethernet7/11
  description LINK_TO_CORE_N7k_02_e7/3
  channel-group 305
  no shutdown

interface Ethernet7/12
  description LINK_TO_ACC_N5K_01_e1/3
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 202 mode active
  no shutdown

interface Ethernet7/13
  description LINK_TO_AC_N5K_01_e1/4
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 204 mode active
  no shutdown

interface Ethernet7/14
  no shutdown

interface Ethernet7/15
```

```
  no shutdown

interface Ethernet7/16
  no shutdown

interface Ethernet7/17
  no shutdown

interface Ethernet7/18
  no shutdown

interface Ethernet7/19
  no shutdown

interface Ethernet7/20
  no shutdown

interface Ethernet7/21
  no shutdown

interface Ethernet7/22
  no shutdown

interface Ethernet7/23
  description LINK_TO_CAT6K_T1/1
  channel-group 176 mode active
  no shutdown

interface Ethernet7/24
  speed 10000
  duplex full
  no shutdown

interface mgmt0
  ip address 10.78.240.104/24
line vty
router ospf 10
ip route 172.16.170.0/24 172.18.1.5
ip route 172.17.30.0/24 172.17.1.38
ip route 172.17.30.2/32 172.17.1.38


JVSL-B-AGG-N7k-01#
```

```
JVSL-B-AGG-N7k-02#            sh run

!Command: show running-config
!Time: Tue Mar 15 15:10:39 2011

version 5.1(1)
switchname JVSL-B-AGG-N7k-02

feature telnet
cfs eth distribute
feature ospf
feature pbr
feature interface-vlan
feature hsrp
feature lacp
feature vpc

username admin password 5 $1$9lqLga8O$UKnb4pkax0zZvJ/6ZbFw..  role vdc-admin
username cisco password 5 $1$v759z3N9$XN8YltkgPqj0NLQEdZTiQ1  role vdc-admin

banner motd #*****************************************  $ Unauthorized access
prohibited $  This system belongs to JVSL-DC t
eam*********************************************#

ip domain-lookup
snmp-server user admin vdc-admin auth md5 0x38fec3600cbc29b1938f0be12e1fc420 priv
0x38fec3600cbc29b1938f0be12e1fc420 localize
dkey
snmp-server user cisco vdc-admin auth md5 0x0580c0b7d1bf22227f39c04facac1f00 priv
0x0580c0b7d1bf22227f39c04facac1f00 localize
dkey
snmp-server community public group vdc-admin

vrf context vPC
vrf context management
  ip route 0.0.0.0/0 10.78.240.1
vlan 1
vlan 7
  shutdown
  name OTV_extVLAN
vlan 10,20,80,100
vlan 170
  name OTV_VLAN
vlan 200
```

```
vpc domain 10
  role priority 10
  peer-keepalive destination 172.17.1.33 source 172.17.1.34 vrf vPC
  peer-gateway

interface Vlan1

interface Vlan7
  no ip redirects
  ip address 172.16.7.5/24
  ip router ospf 10 area 0.0.0.10

interface Vlan80
  no shutdown
  ip router ospf 10 area 0.0.0.10

interface Vlan100
  no shutdown
  no ip redirects
  ip address 172.17.100.3/24
  ip router ospf 10 area 0.0.0.10
  hsrp 100
    preempt delay minimum 60
    priority 110
    ip 172.17.100.1

interface Vlan170
  no shutdown
  no ip redirects
  ip address 172.16.170.4/24
  ip router ospf 10 area 0.0.0.10
  hsrp 207
    preempt delay minimum 60
    ip 172.16.170.1

interface Vlan200
  no shutdown
  no ip redirects
  ip address 172.17.200.3/24
  ip router ospf 10 area 0.0.0.10
  hsrp 200
    preempt delay minimum 60
    priority 110
```

```
    ip 172.17.200.1

interface port-channel201
  description L2_PC_TO_AGG_N7k_01
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  spanning-tree port type network
  vpc peer-link

interface port-channel203
  description L2_PC_TO_ACC_N5K_02
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  vpc 11

interface port-channel204
  shutdown

interface port-channel205
  description L2_PC_TO_ACC_N5K_01
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  vpc 10

interface port-channel276
  description L3_PC_to_Cat6k
  ip address 172.17.1.41/30
  ip router ospf 10 area 0.0.0.10

interface port-channel303
  description L3_PC_TO_CORE_N7K_02
  ip address 172.17.1.22/30
  ip router ospf 10 area 0.0.0.10

interface port-channel304
  description L3_PC_TO_CORE_N7K_01
  ip address 172.17.1.26/30
  ip router ospf 10 area 0.0.0.10

interface Ethernet1/9
```

```
  description LINK_TO_AGG_N7K_01_e1/9
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 201
  no shutdown

interface Ethernet1/10
  description LINK_TO_CORE_N7K_02_e1/2
  channel-group 303 mode active
  no shutdown

interface Ethernet1/11
  description LINK_TO_CORE_N7K_01_e1/3
  channel-group 304
  no shutdown

interface Ethernet1/12
  description LINK_TO_ACC_N5k_02_e1/1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 203 mode active
  no shutdown

interface Ethernet1/13
  description LINK_TO_ACC_N5K_01_e1/2
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 205 mode active
  no shutdown

interface Ethernet1/14
  no shutdown

interface Ethernet1/15
  no shutdown

interface Ethernet1/16
  no shutdown

interface Ethernet1/17
```

```
  no shutdown

interface Ethernet1/18
  no shutdown

interface Ethernet1/19
  no shutdown

interface Ethernet1/20
  no shutdown

interface Ethernet1/21
  ip address 172.18.2.6/30
  ip ospf passive-interface
  ip router ospf 10 area 0.0.0.10
  no shutdown

interface Ethernet1/22
  description "OTV_Join-int_connected_OTV02_e1/25"
  ip address 172.17.2.5/30
  ip ospf network point-to-point
  ip router ospf 10 area 0.0.0.10
  ip igmp version 3
  no shutdown

interface Ethernet1/23
  description Connected_to_OTV_1/26
  switchport
  switchport mode trunk
  no shutdown

interface Ethernet1/24
  description VPC_KEEPALIVE_TO_AGG_N7K_01_1/24
  vrf member vPC
  ip address 172.17.1.34/30
  no shutdown

interface Ethernet7/9
  description LINK_TO_AGG_N7K_01_e7/9
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 201
```

```
  no shutdown

interface Ethernet7/10
  description LINK_TO_CORE_N7K_02_e7/2
  channel-group 303 mode active
  no shutdown

interface Ethernet7/11
  description LINK_TO_CORE_N7K_01_e7/3
  channel-group 304
  no shutdown

interface Ethernet7/12
  description LINK_TO_ACC_N5K_02_e1/3
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 203 mode active
  no shutdown

interface Ethernet7/13
  description LINK_TO_ACC_N5K_01_e1/4
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 205 mode active
  no shutdown

interface Ethernet7/14
  no shutdown

interface Ethernet7/15
  no shutdown

interface Ethernet7/16
  no shutdown

interface Ethernet7/17
  no shutdown

interface Ethernet7/18
  no shutdown
```

```
interface Ethernet7/19
  no shutdown

interface Ethernet7/20
  no shutdown

interface Ethernet7/21
  no shutdown

interface Ethernet7/22
  no shutdown

interface Ethernet7/23
  description LINK_TO_CAT6K_T1/3
  channel-group 276 mode active
  no shutdown

interface Ethernet7/24
  no shutdown

interface mgmt0
  ip address 10.78.240.106/24
line vty
router ospf 10


JVSL-B-AGG-N7k-02#
```

アクセス スイッチの設定

サイト A

```
JVSL-A-ACC-N5k-01# sh run
!Command: show running-config
!Time: Tue Mar 15 13:06:42 2011

version 5.0(2)N2(1)
feature fcoe

feature telnet
cfs eth distribute
feature interface-vlan
```

```
feature lacp
feature vpc
feature lldp
feature fex

logging level aaa 5
logging level cdp 6
logging level radius 5
logging level monitor 6
logging level port-channel 6
logging level spanning-tree 6
snmp-server context management
role name default-role
  description This is a system defined role and applies to all users.
username admin password 5 $1$6Vlis0K7$0J9bTenZPz1MrSYpzI5HG/  role network-admin
username cisco password 5 $1$tOt2OPmU$3yO1we3/nBRWHN04kI8Cd.  role network-admin
username guest password 5 $1$68lYfzkD$Ur9/Wqk5sxWEHonIxWekj.  role network-operator
username test password 5 $1$5KqpyjJi$Lhx.t/zMB4hzBTyivnSzZ0  role vdc-operator

banner motd #****************************************  $ Unauthorized access
prohibited $  This system belongs to JVSL-DC team*****************************
************
#

ip domain-lookup
ip domain-lookup
ip host JVSL-A-ACC-N5k-01 10.78.240.7
ip host JVSL-A-ACC-N5K-01 10.78.240.7
hostname JVSL-A-ACC-N5k-01
logging event link-status default
errdisable recovery cause link-flap
errdisable recovery cause udld
errdisable recovery cause bpduguard
errdisable recovery cause loopback
errdisable recovery cause pause-rate-limit
class-map type qos class-fcoe
class-map type queuing class-all-flood
  match qos-group 2
class-map type queuing class-ip-multicast
  match qos-group 2
class-map type network-qos class-all-flood
  match qos-group 2
class-map type network-qos class-ip-multicast
```

```
  match qos-group 2
fex 100
  pinning max-links 1
  description "FEX0100"
snmp-server contact jvsl
snmp-server user admin network-admin auth md5 0x5d3817147f3acdb98f6c8a787e580cd2 priv
0x5d3817147f3acdb98f6c8a787e580cd2 localizedkey
snmp-server user cisco network-admin auth md5 0x7ab9baa6c90c053ec6c4dc4d6b3162e2 priv
0x7ab9baa6c90c053ec6c4dc4d6b3162e2 localizedkey
snmp-server user guest network-operator auth md5 0x7ab9baa6c90c053ec6c4dc4d6b3162e2 priv
0x7ab9baa6c90c053ec6c4dc4d6b3162e2 localizedkey
snmp-server host 10.78.234.117 traps version 2c public  udp-port 1163
snmp-server host 10.78.240.200 traps version 2c public  udp-port 2162
snmp-server host 171.71.7.75 traps version 2c public  udp-port 2162
snmp-server host 171.71.7.87 traps version 2c public  udp-port 2162
snmp-server host 10.78.234.117 traps version 2c public  udp-port 2162
snmp-server host 10.78.240.200 traps version 2c public  udp-port 1163
snmp-server host 10.78.240.29 traps version 2c public  udp-port 2162
snmp-server host 10.78.240.40 traps version 2c public  udp-port 2162
snmp-server enable traps entity fru
snmp-server community public group network-admin
snmp-server community qwerty group network-operator

vrf context management
  ip route 0.0.0.0/0 10.78.240.1
vlan 1,7,10,30,80,100,170,200
vlan 220
  name vMotion-vlan
vlan 300
  fcoe vsan 200
  name FCoE-vlan
vlan 500
  name Management
vlan 510
  name Control-Vlan
vlan 520
  name Packet-Vlan
vlan 530
  name Data-Vlan
vlan 600
cdp format device-id serial-number
vpc domain 20
  role priority 5
  peer-keepalive destination 10.78.240.8
```

```
vsan database
  vsan 200 name "FCoE_vsan"
fcdomain fcid database
  vsan 200 wwn 21:00:00:c0:dd:11:aa:75 fcid 0x900000 dynamic


interface Vlan1

interface Vlan7
  no shutdown
  ip address 172.16.7.22/24

interface Vlan30
  no shutdown

interface Vlan80
  no shutdown
  ip address 172.16.80.3/24

interface Vlan100
  no shutdown
  ip address 172.16.100.6/24

interface Vlan200

interface Vlan500
  no shutdown
  ip address 10.78.240.62/24

interface san-port-channel 59
  channel mode active

interface port-channel1

interface port-channel2

interface port-channel10
  description "L2_PC_TO_JVSL_A_FBS_1"
  switchport mode trunk

interface port-channel11
  switchport mode trunk
```

```
interface port-channel13

interface port-channel21

interface port-channel34

interface port-channel101
  switchport mode trunk
  vpc peer-link
  spanning-tree port type network

interface port-channel102
  switchport mode trunk
  vpc 10

interface port-channel104
  switchport mode trunk
  vpc 11

interface port-channel202
  description L2_PC_TO_AGG_N7K_01
  switchport mode trunk
  switchport trunk allowed vlan 7,10,20,30,80,100,170,200

interface port-channel205
  description L2_PC_TO_AGG_N7K_02
  switchport mode trunk

interface port-channel206
  switchport mode trunk

interface port-channel405
  switchport mode trunk
  switchport trunk allowed vlan 1,300

interface port-channel501
  description PC501_Connected_N4k
  switchport mode trunk

interface vfc4

interface vfc9
```

```
  bind interface Ethernet1/9
  no shutdown

interface vfc701
  bind mac-address 00:c0:dd:11:aa:75
  no shutdown
vsan database
  vsan 4094 interface vfc4
  vsan 200 interface vfc701
  vsan 200 interface san-port-channel 59


interface fc2/1
  channel-group 59 force
  no shutdown

interface fc2/2
  channel-group 59 force
  no shutdown

interface fc2/3

interface fc2/4

interface fc3/1

interface fc3/2

interface fc3/3

interface fc3/4

interface Ethernet1/1
  switchport mode trunk
  switchport trunk allowed vlan 7,10,20,30,80,100,170,200
  channel-group 202 mode passive

interface Ethernet1/2
  description LINK_TO_AGG_N7K_02_e1/13
  switchport mode trunk
  switchport trunk allowed vlan 7,10,20,30,80,100,170,200
  channel-group 202 mode passive
```

```
interface Ethernet1/3
  description LINK_TO_AGG_N7K_01_e7/12
  switchport mode trunk
  switchport trunk allowed vlan 7,10,20,30,80,100,170,200
  channel-group 202 mode passive

interface Ethernet1/4
  description LINK_TO_AGG_N7K_02_e7/13
  switchport mode trunk
  switchport trunk allowed vlan 7,10,20,30,80,100,170,200
  channel-group 202 mode passive

interface Ethernet1/5
  switchport mode trunk
  switchport access vlan 3555

interface Ethernet1/6
  switchport access vlan 1800

interface Ethernet1/7
  switchport mode trunk
  channel-group 206

interface Ethernet1/8

interface Ethernet1/9

interface Ethernet1/10
  description connected_2_AD
  switchport access vlan 100
  speed 1000

interface Ethernet1/11
  switchport mode trunk
  speed 1000
  channel-group 10

interface Ethernet1/12
  description test_UCS_connection
  switchport mode trunk

interface Ethernet1/13
  speed 1000
```

```
  channel-group 13 mode active

interface Ethernet1/14
  switchport access vlan 500
  speed 1000

interface Ethernet1/15
  description "connected_to_A-FI"
  switchport mode trunk
  channel-group 102 mode active

interface Ethernet1/16
  description conected to CAT6K-2/37
  switchport access vlan 500
  speed 1000

interface Ethernet1/17
  description "connected_to_A-FI"
  switchport mode trunk
  channel-group 102 mode active

interface Ethernet1/18
  description "connected _to_B-FI"
  switchport mode trunk
  channel-group 104 mode active

interface Ethernet1/19
  description "connected_to_B-FI"
  switchport mode trunk
  channel-group 104 mode active

interface Ethernet1/20
  description Reserved_for_UCS_FI_Connectivity

interface Ethernet1/21
  switchport mode trunk

interface Ethernet1/22
  switchport access vlan 800

interface Ethernet1/23

interface Ethernet1/24
```

```
  switchport mode trunk
  switchport trunk allowed vlan 500

interface Ethernet1/25
  switchport access vlan 900

interface Ethernet1/26
  switchport access vlan 1000

interface Ethernet1/27
  switchport access vlan 1200

interface Ethernet1/28

interface Ethernet1/29
  switchport access vlan 500

interface Ethernet1/30

interface Ethernet1/31

interface Ethernet1/32

interface Ethernet1/33
  description CONNECTED-TO-N4K-01-1/15
  switchport mode trunk
  switchport trunk allowed vlan 1,300
  channel-group 405

interface Ethernet1/34
  description CONNECTED-TO-N4K-01-1/16
  switchport mode trunk
  switchport trunk allowed vlan 1,300
  channel-group 405

interface Ethernet1/35
  description "connected_to_A-ACC-N5k-2_e1/35"
  switchport mode trunk
  channel-group 101 mode active

interface Ethernet1/36
  description connected_to_A-ACC-N5k-2_e1/36
  switchport mode trunk
```

```
  channel-group 101 mode active

interface Ethernet1/37
  channel-group 1 mode active

interface Ethernet1/38

interface Ethernet1/39

interface Ethernet1/40
  fex associate 100
  switchport mode fex-fabric

interface Ethernet2/1

interface Ethernet2/2

interface Ethernet2/3

interface Ethernet2/4

interface Ethernet3/1

interface Ethernet3/2

interface Ethernet3/3

interface Ethernet3/4

interface mgmt0
  ip address 10.78.240.7/24

interface Ethernet100/1/1
  description connected_FBS_BSwitch0/13
  switchport mode trunk

interface Ethernet100/1/2
  description connected_2_FBS
  switchport access vlan 500
  switchport trunk allowed vlan 80,100

interface Ethernet100/1/3
```

```
interface Ethernet100/1/4

interface Ethernet100/1/5

interface Ethernet100/1/6

interface Ethernet100/1/7

interface Ethernet100/1/8

interface Ethernet100/1/9

interface Ethernet100/1/10

interface Ethernet100/1/11

interface Ethernet100/1/12

interface Ethernet100/1/13

interface Ethernet100/1/14

interface Ethernet100/1/15

interface Ethernet100/1/16

interface Ethernet100/1/17

interface Ethernet100/1/18

interface Ethernet100/1/19

interface Ethernet100/1/20

interface Ethernet100/1/21

interface Ethernet100/1/22

interface Ethernet100/1/23

interface Ethernet100/1/24

interface Ethernet100/1/25
```

```
interface Ethernet100/1/26

interface Ethernet100/1/27

interface Ethernet100/1/28

interface Ethernet100/1/29

interface Ethernet100/1/30

interface Ethernet100/1/31

interface Ethernet100/1/32

interface Ethernet100/1/33

interface Ethernet100/1/34

interface Ethernet100/1/35

interface Ethernet100/1/36

interface Ethernet100/1/37

interface Ethernet100/1/38

interface Ethernet100/1/39

interface Ethernet100/1/40

interface Ethernet100/1/41

interface Ethernet100/1/42

interface Ethernet100/1/43

interface Ethernet100/1/44

interface Ethernet100/1/45

interface Ethernet100/1/46
```

```
interface Ethernet100/1/47

interface Ethernet100/1/48
line console
line vty
boot kickstart bootflash:/n5000-uk9-kickstart.5.0.2.N2.1.bin
boot system bootflash:/n5000-uk9.5.0.2.N2.1.bin
ip route 192.168.30.0/24 192.168.30.1
ip route 192.168.30.0/24 192.168.200.1
ip route 192.168.55.32/27 172.16.100.100
interface fc2/1
interface fc2/2
interface fc2/3
interface fc2/4
interface fc2/1
interface fc2/2
interface fc3/1
interface fc3/2
interface fc3/3
interface fc3/4
logging logfile messages 6
zoneset activate name IBM_to_EMC vsan 200


JVSL-A-ACC-N5k-01#

JVSL-A-ACC-N5k-02# sh run
version 4.1(3)N2(1a)
feature fcoe
feature telnet
feature interface-vlan
feature lacp
feature vpc
vpc domain 20
  role priority 10
  peer-keepalive destination 10.78.240.7
feature fex
logging level aaa 5
logging level cdp 6
logging level radius 5
logging level monitor 6
logging level port-channel 6
logging level spanning-tree 6
```

```
logging level interface vlan 5
snmp-server context management
role name default-role
  description This is a system defined role and applies to all users.
rule 5 permit show feature environment
  rule 4 permit show feature hardware
  rule 3 permit show feature module
  rule 2 permit show feature snmp
  rule 1 permit show feature system
username admin password 5 $1$cIeRKpwz$.uDCmDr6J3dSI2DRi8GFf/  role network-admin
username cisco password 5 $1$TtxfWI0Y$gTjof2Y2czg9rzj7uO78X/  role network-operator
username cisco role network-admin
username guest password 5 $1$8tRliPhC$9mHM48vJ8xGC0hNvGdyTF1  role network-operator

banner motd #*****************************************  $ Unauthorized access
prohibited $  This system belongs to JVSL-DC team*****************************
*************#

ip host JVSL-A-ACC-N5k-02 10.78.240.8
ip host JVSL-A-ACC-N5K-02 10.78.240.8
hostname JVSL-A-ACC-N5k-02
logging event link-status default
fex 100
  pinning max-links 1
  description FEX0100
  type "Nexus 2148T"
snmp-server user admin network-admin auth md5 0xd9908ebebe1473647f96c3acb7e0a046 priv
0xd9908ebebe1473647f96c3acb7e0a046 localizedkey
snmp-server user cisco network-operator auth md5 0x5cd317f07e1bc243609ad08bd7aaf1e2 priv
0x5cd317f07e1bc243609ad08bd7aaf1e2 localizedkey
snmp-server user cisco network-admin
snmp-server user guest network-operator auth md5 0x5cd317f07e1bc243609ad08bd7aaf1e2 priv
0x5cd317f07e1bc243609ad08bd7aaf1e2 localizedkey
snmp-server host 10.78.234.117 traps version 2c public  udp-port 2162
snmp-server host 10.78.240.200 traps version 2c public  udp-port 2162
snmp-server host 10.78.240.225 traps version 2c public  udp-port 2162
snmp-server host 171.71.7.75 traps version 2c public  udp-port 2162
port-monitor activate
snmp-server enable traps entity fru
snmp-server community qwerty group network-operator
snmp-server community public group network-operator
vrf context management
  ip route 0.0.0.0/0 10.78.240.1
vlan 1,7,80,100,170
```

```
vlan 200
  name FCoEvlan
vlan 215
  name Cluster-vlan
vlan 300
  fcoe vsan 200
vlan 500
  name Management
vlan 510
  name Control-vlan
vlan 520
  name Packet-vlan
vlan 700
  name Data
vsan database
  vsan 200
fcdomain fcid database
  vsan 200 wwn 21:00:00:c0:dd:11:aa:77 fcid 0x980000 dynamic

interface Vlan1
  no shutdown

interface Vlan7
  no shutdown
  ip address 172.16.7.21/24

interface Vlan80
  no shutdown
  ip address 172.16.80.4/24

interface Vlan100
  no shutdown
  ip address 172.16.100.4/24

interface Vlan200
  no shutdown
  ip address 172.16.200.4/24

interface Vlan250
  no shutdown

interface Vlan300
  no shutdown
```

```
  ip address 192.168.30.2/24

interface Vlan500
  no shutdown
  ip address 10.78.240.9/24

interface Vlan700

interface san-port-channel 59
  channel mode active
  no shutdown

interface port-channel10
  description "L2_PC_TO_JVSL_A_FBS_2"
  switchport mode trunk

interface port-channel11

interface port-channel101
  switchport mode trunk
  vpc peer-link
  spanning-tree port type network

interface port-channel103
  switchport mode trunk
  vpc 11

interface port-channel105
  switchport mode trunk
  vpc 10

interface port-channel203
  description L2_PC_TO_AGG_N7K_02
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200

interface port-channel204
  description L2_PC_TO_AGG_N7K_01
  switchport mode trunk

interface port-channel206
  switchport mode trunk
```

```
interface port-channel405
  switchport mode trunk

interface port-channel501
  description PC501_Connected_N4k

interface vfc500
  no shutdown

interface vfc701
  bind mac-address 00:c0:dd:11:aa:77
  no shutdown
vsan database
  vsan 200 interface vfc500
  vsan 200 interface vfc701
  vsan 200 interface san-port-channel 59

interface fc2/1
  channel-group 59 force
  no shutdown

interface fc2/2
  channel-group 59 force
  no shutdown

interface fc2/3

interface fc2/4

interface fc3/1

interface fc3/2

interface fc3/3

interface fc3/4

interface Ethernet1/1
  description LINK_TO_AGG_N7K_02_e1/12
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 203 mode passive
```

```
interface Ethernet1/2
  description LINK_TO_AGG_N7K_01_e1/13
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 203 mode passive

interface Ethernet1/3
  description LINK_TO_AGG_N7K_02_e7/12
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 203 mode passive

interface Ethernet1/4
  description LINK_TO_AGG_N7K_01_e7/13
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 203 mode passive

interface Ethernet1/5
  switchport mode trunk
  switchport access vlan 3555

interface Ethernet1/6

interface Ethernet1/7
  switchport mode trunk
  channel-group 206

interface Ethernet1/8
  switchport mode trunk
  speed 1000

interface Ethernet1/9
  switchport mode trunk
  switchport trunk allowed vlan 400,500,600,700
  speed 1000

interface Ethernet1/10
  switchport mode trunk
  speed 1000

interface Ethernet1/11
  switchport mode trunk
```

```
  switchport trunk allowed vlan 400,500,600,700
  speed 1000

interface Ethernet1/12
  description CONNECTED-TO-FI-A
  switchport mode trunk

interface Ethernet1/13
  switchport mode trunk
  switchport trunk allowed vlan 400,500,600,700
  speed 1000

interface Ethernet1/14
  switchport mode trunk
  switchport trunk allowed vlan 400,500,600,700
  speed 1000

interface Ethernet1/15
  description "conneted_to_SITEA-UCS-FI-B(sub>_3/1
  switchport mode trunk
  channel-group 103 mode active

interface Ethernet1/16
  description CONNECTED-TO-CAT65K(MGMT)
  switchport access vlan 500
  speed 1000

interface Ethernet1/17
  description Connected_to_JVSL-A-FI-01-B_eth3/3
  switchport mode trunk
  channel-group 103 mode active

interface Ethernet1/18
  description "conneted_to_SITEA-UCS-FI-b(sub)_3/2
  switchport mode trunk
  channel-group 105 mode active

interface Ethernet1/19
  description "connected_to_UCS-A-FI-a(prim>_3/4"
  switchport mode trunk
  channel-group 105 mode active

interface Ethernet1/20
```

```
interface Ethernet1/21
  switchport mode trunk

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24
  switchport mode trunk

interface Ethernet1/25
  description connected_to_N7k_A_OTV_1/25
  switchport mode trunk

interface Ethernet1/26
  description Connected_to_AGG_N7k_02_e1/26
  switchport mode trunk

interface Ethernet1/27

interface Ethernet1/28

interface Ethernet1/29

interface Ethernet1/30

interface Ethernet1/31

interface Ethernet1/32

interface Ethernet1/33
  switchport mode trunk
  channel-group 405

interface Ethernet1/34
  switchport mode trunk
  channel-group 405

interface Ethernet1/35
  switchport mode trunk
  channel-group 101 mode active
```

```
interface Ethernet1/36
  switchport mode trunk
  channel-group 101 mode active

interface Ethernet1/37

interface Ethernet1/38

interface Ethernet1/39
  shutdown

interface Ethernet1/40
  description connected_2_N2k
  switchport mode fex-fabric
  fex associate 100

interface Ethernet2/1

interface Ethernet2/2

interface Ethernet2/3

interface Ethernet2/4

interface Ethernet3/1

interface Ethernet3/2

interface Ethernet3/3

interface Ethernet3/4

interface mgmt0
  ip address 10.78.240.8/24

interface Ethernet100/1/1
  description LINK_TO_AD
  switchport mode trunk
  switchport trunk allowed vlan 80,100
  spanning-tree bpduguard disable

interface Ethernet100/1/2
  description LINK_TO_FBS
```

```
  switchport access vlan 500
  switchport trunk allowed vlan 80,100

interface Ethernet100/1/3

interface Ethernet100/1/4

interface Ethernet100/1/5

interface Ethernet100/1/6

interface Ethernet100/1/7

interface Ethernet100/1/8

interface Ethernet100/1/9

interface Ethernet100/1/10

interface Ethernet100/1/11

interface Ethernet100/1/12

interface Ethernet100/1/13

interface Ethernet100/1/14

interface Ethernet100/1/15

interface Ethernet100/1/16

interface Ethernet100/1/17

interface Ethernet100/1/18

interface Ethernet100/1/19

interface Ethernet100/1/20

interface Ethernet100/1/21

interface Ethernet100/1/22
```

```
interface Ethernet100/1/23

interface Ethernet100/1/24

interface Ethernet100/1/25

interface Ethernet100/1/26

interface Ethernet100/1/27

interface Ethernet100/1/28

interface Ethernet100/1/29

interface Ethernet100/1/30

interface Ethernet100/1/31

interface Ethernet100/1/32

interface Ethernet100/1/33

interface Ethernet100/1/34

interface Ethernet100/1/35

interface Ethernet100/1/36

interface Ethernet100/1/37

interface Ethernet100/1/38

interface Ethernet100/1/39

interface Ethernet100/1/40

interface Ethernet100/1/41

interface Ethernet100/1/42

interface Ethernet100/1/43

interface Ethernet100/1/44
```

```
interface Ethernet100/1/45

interface Ethernet100/1/46

interface Ethernet100/1/47

interface Ethernet100/1/48
line console
boot kickstart bootflash:/n5000-uk9-kickstart.4.1.3.N2.1a.bin
boot system bootflash:/n5000-uk9.4.1.3.N2.1a.bin
cfs eth distribute
ip route 192.168.200.0/24 192.168.30.1
interface fc2/1
interface fc2/2
interface fc2/3
interface fc2/4
interface fc3/1
interface fc3/2
interface fc3/3
interface fc3/4
logging logfile messages 6
zone default-zone permit vsan 1
zoneset activate name IBM_to_EMC vsan 200

JVSL-A-ACC-N5k-02#
```

サイト B

```
JVSL-B-ACC-N5k-01# sh run

!Command: show running-config
!Time: Tue Mar 15 12:51:21 2011

version 5.0(2)N2(1)
feature telnet
cfs eth distribute
feature interface-vlan
feature lacp
feature vpc
feature lldp

role name default-role
```

```
  description This is a system defined role and applies to all users.
username admin password 5 $1$qtV6C9Hw$mz3vbbGE19AkypNzYdGzi0  role network-admin
username cisco password 5 jvsl@123  role network-admin

banner motd #****************************************  $ Unauthorized access p
rohibited $  This system belongs to JVSL-DC team*********************************
*********
#

ip domain-lookup
ip domain-lookup
ip host JVSL-B-ACC-N5k-01 10.78.240.51
hostname JVSL-B-ACC-N5k-01
class-map type qos class-fcoe
class-map type queuing class-all-flood
  match qos-group 2
class-map type queuing class-ip-multicast
  match qos-group 2
class-map type network-qos class-all-flood
  match qos-group 2
class-map type network-qos class-ip-multicast
  match qos-group 2
snmp-server user admin network-admin auth md5 0x076532053f37c7c6278dd55c7c070d7b
 priv 0x076532053f37c7c6278dd55c7c070d7b localizedkey
snmp-server user cisco network-admin auth md5 0x6dd3603160deff6abe876c51e18f1ecf
 priv 0x6dd3603160deff6abe876c51e18f1ecf localizedkey
snmp-server community public group network-operator

vrf context management
  ip route 0.0.0.0/0 10.78.240.1
vlan 1,200,500
vlan 510
  name Control-vlan
vlan 520
  name Packet-vlan
vpc domain 30
  role priority 5
  peer-keepalive destination 10.78.240.108

interface Vlan1

interface Vlan80
  no shutdown
```

```
  ip address 172.17.80.3/24

interface Vlan100
  no shutdown
  ip address 172.17.100.6/24

interface Vlan200
  no shutdown
  ip address 172.17.200.5/24

interface Vlan500
  no shutdown
  ip address 10.78.240.63/24

interface port-channel101
  vpc peer-link
  spanning-tree port type network

interface port-channel102
  switchport mode trunk
  vpc 10

interface port-channel104
  switchport mode trunk
  vpc 11

interface port-channel202
  description L2_PC_TO_AGG_N7K_01
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200

interface port-channel205
  description L2_PC_TO_AGG_N7K_02
  switchport mode trunk

interface port-channel206
  switchport mode trunk

interface Ethernet1/1
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 202 mode passive
```

```
interface Ethernet1/2
  description LINK_TO_AGG_N7K_02_e1/13
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 202 mode passive

interface Ethernet1/3
  description LINK_TO_AGG_N7K_01_e7/12
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 202 mode passive

interface Ethernet1/4
  description LINK_TO_AGG_N7K_02_e7/13
  switchport mode trunk
  switchport trunk allowed vlan 10,20,80,100,170,200
  channel-group 202 mode passive

interface Ethernet1/5

interface Ethernet1/6

interface Ethernet1/7
  switchport mode trunk
  channel-group 206

interface Ethernet1/8

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15
  switchport mode trunk
  switchport trunk allowed vlan 500
```

```
interface Ethernet1/16
  switchport mode trunk
  speed 1000

interface Ethernet1/17
  description connected to UCS_B_port1
  switchport mode trunk

interface Ethernet1/18
  description "Connected_to_B-UCS-FI-b_eth3/2"
  switchport mode trunk
  channel-group 104 mode active

interface Ethernet1/19
  description Conneted_to_UCS-B-FI_3/1
  switchport mode trunk
  channel-group 104 mode active

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25

interface Ethernet1/26

interface Ethernet1/27

interface Ethernet1/28

interface Ethernet1/29

interface Ethernet1/30

interface Ethernet1/31
```

```
interface Ethernet1/32

interface Ethernet1/33

interface Ethernet1/34

interface Ethernet1/35
  description connected_to_B_ACC_N5k_02_e1/35
  channel-group 101 mode active

interface Ethernet1/36
  description "connected_to_B_ACC_N5k_02_e1/36"
  channel-group 101 mode active

interface Ethernet1/37

interface Ethernet1/38

interface Ethernet1/39

interface Ethernet1/40

interface Ethernet2/1

interface Ethernet2/2

interface Ethernet2/3

interface Ethernet2/4

interface mgmt0
  ip address 10.78.240.107/24
line console
line vty
boot kickstart bootflash:/n5000-uk9-kickstart.5.0.2.N2.1.bin
boot system bootflash:/n5000-uk9.5.0.2.N2.1.bin
ip route 0.0.0.0/0 10.78.240.1
ip route 172.17.200.0/24 172.17.200.1
JVSL-B-ACC-N5k-01#
JVSL-B-ACC-N5k-02# sh run

!Command: show running-config
!Time: Tue Mar 15 12:50:30 2011
```

```
version 5.0(2)N2(1)
feature telnet
cfs eth distribute
feature interface-vlan
feature lacp
feature vpc
feature lldp

username admin password 5 $1$F0jvyrkv$AxwA8gJntl1mSaGV0VLdM/  role network-admin
username cisco password 5 jvsl@123  role network-operator
ip domain-lookup
ip domain-lookup
ip host JVSL-B-ACC-N5k-02 10.78.240.108
hostname JVSL-B-ACC-N5k-02
class-map type qos class-fcoe
class-map type queuing class-all-flood
  match qos-group 2
class-map type queuing class-ip-multicast
  match qos-group 2
class-map type network-qos class-all-flood
  match qos-group 2
class-map type network-qos class-ip-multicast
  match qos-group 2
snmp-server user admin network-admin auth md5 0xfd41b316b65e1054a747844a7e15a704
 priv 0xfd41b316b65e1054a747844a7e15a704 localizedkey

vrf context management
  ip route 0.0.0.0/0 10.78.240.1
vlan 1,7,200,500
vlan 510
  name Control-vlan
vlan 520
  name Packet-vlan
vpc domain 30
  role priority 10
  peer-keepalive destination 10.78.240.107

interface Vlan1

interface Vlan7
  no shutdown
  ip address 172.16.7.4/24
```

```
interface Vlan80
  no shutdown
  ip address 172.17.80.4/24

interface Vlan100
  no shutdown
  ip address 172.17.100.4/24

interface Vlan200
  no shutdown
  ip address 172.17.200.4/24

interface Vlan500
  no shutdown
  ip address 10.78.240.65/24

interface port-channel101
  vpc peer-link
  spanning-tree port type network

interface port-channel102

interface port-channel103
  switchport mode trunk
  vpc 11

interface port-channel105
  switchport mode trunk
  vpc 10

interface port-channel203
  description L2_PC_TO_AGG_N7K_02
  switchport mode trunk
  switchport trunk allowed vlan 170

interface port-channel204
  description L2_PC_TO_AGG_N7K_01
  switchport mode trunk

interface port-channel206
  switchport mode trunk
```

```
interface Ethernet1/1
  description LINK_TO_AGG_N7K_02_e1/12
  switchport mode trunk
  switchport trunk allowed vlan 170
  channel-group 203 mode passive

interface Ethernet1/2
  description LINK_TO_AGG_N7K_01_e1/13
  switchport mode trunk
  switchport trunk allowed vlan 170
  channel-group 203 mode passive

interface Ethernet1/3
  description LINK_TO_AGG_N7K_02_e7/12
  switchport mode trunk
  switchport trunk allowed vlan 170
  channel-group 203 mode passive

interface Ethernet1/4
  description LINK_TO_AGG_N7K_01_e7/13
  switchport mode trunk
  switchport trunk allowed vlan 170
  channel-group 203 mode passive

interface Ethernet1/5

interface Ethernet1/6

interface Ethernet1/7
  switchport mode trunk
  channel-group 206

interface Ethernet1/8

interface Ethernet1/9

interface Ethernet1/10

interface Ethernet1/11

interface Ethernet1/12

interface Ethernet1/13
```

```
interface Ethernet1/14

interface Ethernet1/15
  switchport mode trunk
  switchport trunk allowed vlan 500

interface Ethernet1/16
  switchport mode trunk
  speed 1000

interface Ethernet1/17
  switchport mode trunk
  channel-group 103 mode active

interface Ethernet1/18
  description "connected_to_SiteB-UCS-FI-A_e3/2"
  switchport mode trunk
  channel-group 105 mode active

interface Ethernet1/19
  description "connected_to_SiteB-UCS-FI-A_e3/4"
  switchport mode trunk
  channel-group 105 mode active

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22

interface Ethernet1/23

interface Ethernet1/24

interface Ethernet1/25
  description Connected_to_UCS_FI
  switchport mode trunk

interface Ethernet1/26
  description Connected_to_AGG_N7k_02_e1/26
  switchport mode trunk
```

```
interface Ethernet1/27

interface Ethernet1/28

interface Ethernet1/29

interface Ethernet1/30

interface Ethernet1/31

interface Ethernet1/32

interface Ethernet1/33

interface Ethernet1/34

interface Ethernet1/35
  description "connected_to_B_ACC_N5k-01_e1/35"
  channel-group 101 mode active

interface Ethernet1/36
  description "connected_to_B_ACC_N5k-01_e1/36"
  channel-group 101 mode active

interface Ethernet1/37

interface Ethernet1/38

interface Ethernet1/39

interface Ethernet1/40

interface Ethernet2/1

interface Ethernet2/2

interface Ethernet2/3

interface Ethernet2/4

interface mgmt0
  ip address 10.78.240.108/24
line console
```

```
line vty
boot kickstart bootflash:/n5000-uk9-kickstart.5.0.2.N2.1.bin
boot system bootflash:/n5000-uk9.5.0.2.N2.1.bin
JVSL-B-ACC-N5k-02#
```

WAN エッジ ルータの設定

サイト A

```
JVSL-A-ASR-01#sh run
Building configuration...

Current configuration : 2895 bytes
!
! Last configuration change at 02:07:40 UTC Mon Mar 14 2011
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no platform punt-keepalive disable-kernel-core
!
hostname JVSL-A-ASR-01
!
boot-start-marker
boot system flash bootflash:asr1000rp1-adventerprise.03.02.00.S.151-1.S.bi
boot-end-marker
!
!
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
vrf definition test
 !
 address-family ipv4
 exit-address-family
!
enable secret 5 $1$Z0Tn$.uF6d.OWLeq0d8ZeTEasp.
!
no aaa new-model
!
!
!
ip source-route
!
!
!
!
!
!
!
!
```

```
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
username admin privilege 15 password 0 jvsl@123
!
redundancy
 mode none
!
!
!
ip tftp source-interface GigabitEthernet0
!
!
!
!
interface GigabitEthernet0/0/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/1
 description LINK_TO_CORE_N7K_01_eth2/1
 ip address 172.16.1.5 255.255.255.252
 ip ospf 10 area 0.0.0.0
 negotiation auto
!
interface GigabitEthernet0/0/2
 description LINK_TO_CORE_N7K_02_eth2/1
 ip address 172.16.1.9 255.255.255.252
 ip ospf 10 area 0.0.0.0
 negotiation auto
!
interface GigabitEthernet0/0/3
 no ip address
 negotiation auto
!
interface GigabitEthernet0/1/0
 description LINK_TO_WEM_LANA
 ip address 200.100.100.5 255.255.255.252
 no negotiation auto
 cdp enable
!
interface GigabitEthernet0/1/1
 ip address 172.16.2.6 255.255.255.252
 ip ospf 10 area 0.0.0.0
 negotiation auto
!
interface GigabitEthernet0/1/2
 description "connected_toMDS9509-02_e1/1"
 ip address 172.16.2.10 255.255.255.252
 negotiation auto
!
interface GigabitEthernet0/1/3
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/1/4
```

```
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/1/5
 no ip address
 negotiation auto
!
interface GigabitEthernet0/1/6
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/1/7
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 ip address 10.78.240.2 255.255.255.0
 speed 100
 no negotiation auto
!
router ospf 10
 redistribute static
 network 172.17.200.0 0.0.0.255 area 0.0.0.0
 default-information originate
!
!
ip http server
ip http authentication local
ip route 172.17.0.0 255.255.0.0 200.100.100.6
ip route 172.17.2.0 255.255.255.0 200.200.100.6
ip route 172.17.200.0 255.255.255.0 200.100.100.6
ip route 192.168.10.0 255.255.255.0 200.100.100.6
ip route 192.168.20.0 255.255.255.0 200.100.100.6
ip route 200.100.100.0 255.255.255.0 200.100.100.6
ip route 200.200.100.0 255.255.255.0 200.100.100.6
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 10.78.240.1
!
logging esm config
cdp run
!
!
!
control-plane
!
!
!
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 privilege level 15
 password jvsl@123
 login
 transport input telnet
!
end
JVSL-A-ASR-01#
```

サイト B

```
JVSL-B-ASR-01#sh run
Building configuration...

Current configuration : 2298 bytes
!
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname JVSL-B-ASR-01
!
boot-start-marker
boot-end-marker
!
vrf definition Mgmt-intf
 !
address-family ipv4
 exit-address-family
 !
address-family ipv6
 exit-address-family
!
enable secret 5 $1$QiLq$xgoyl0DXpuNm94u9dkhuK1
enable password roZes@123
!
no aaa new-model
ip subnet-zero
ip source-route
!
!
!
!
multilink bundle-name authenticated
!
!
!
redundancy
 mode none
!
```

```
!
!
!
!
!
interface GigabitEthernet0/0/0
 description LINK_TO_CORE_N7K_01_eth2/1
 ip address 172.17.1.5 255.255.255.252
 ip ospf 10 area 0.0.0.0
 negotiation auto
!
interface GigabitEthernet0/0/1
 description LINK_TO_CORE_N7K_02_eth2/1
 ip address 172.17.1.9 255.255.255.252
 ip ospf 10 area 0.0.0.0
 negotiation auto
!
interface GigabitEthernet0/0/2
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/3
 no ip address
 negotiation auto
!
interface GigabitEthernet0/2/0
 description LINK_TO_WEM_LANA
 ip address 200.200.100.5 255.255.255.252
 no negotiation auto
!
interface GigabitEthernet0/2/1
 ip address 172.17.2.6 255.255.255.252
 ip ospf 10 area 0.0.0.0
 negotiation auto
!
interface GigabitEthernet0/2/2
 description "Connected_toMDS9509-02_e1/1"
 ip address 172.17.2.10 255.255.255.252
 negotiation auto
!
interface GigabitEthernet0/2/3
 no ip address
 shutdown
```

```
 negotiation auto
!
interface GigabitEthernet0/2/4
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/2/5
 no ip address
 no negotiation auto
!
interface GigabitEthernet0/2/6
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/2/7
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0
 vrf forwarding Mgmt-intf
 ip address 10.78.240.102 255.255.255.0
 negotiation auto
!
router ospf 10
 log-adjacency-changes
 redistribute static
!
ip classless
ip route 172.16.0.0 255.255.0.0 200.200.100.6
ip route 172.16.200.0 255.255.255.0 200.200.100.6
ip route 200.100.100.0 255.255.255.0 200.200.100.6
ip route 200.200.100.0 255.255.255.0 200.200.100.6
ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0 10.78.240.1
!
no ip http server
no ip http secure-server
!
!
!
!
```

```
control-plane
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 password jvsl@123
 login
!
end


JVSL-B-ASR-01#
```

ブランチ オフィス ルータの設定

```
JVSL-Br-ISR-01>en
Password:
JVSL-Br-ISR-01#sh run
Building configuration...

Current configuration : 1924 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service linenumber
!
hostname JVSL-Br-ISR-01
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$..Ih$0vQM.bYs7fi6NfHff1ofi.
enable password jvsl@123
!
no aaa new-model
ip wccp 61
ip wccp 62
!
!
ip cef
!
!
multilink bundle-name authenticated
!
!
!
archive
 log config
  hidekeys
!
```

```
!
!
!
!
interface GigabitEthernet0/0
 description Connected_to_WAN
 ip address 200.200.100.10 255.255.255.252
 duplex full
 speed 1000
!
interface GigabitEthernet0/1
 description connected_to_WEM_LANB
 ip address 200.100.100.10 255.255.255.252
 ip wccp 62 redirect in
 duplex full
 speed 1000
!
interface FastEthernet0/0/0
 description ISR_Mgmt_port
 ip address 10.78.240.61 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/0/1
 description Connected_to_LAN
 ip address 192.168.10.1 255.255.255.0
 ip wccp 61 redirect in
 duplex auto
 speed auto
 no keepalive
!
interface Integrated-Service-Engine1/0
 ip address 192.168.20.1 255.255.255.240
 service-module ip address 192.168.20.2 255.255.255.240
 service-module ip default-gateway 192.168.20.1
 no keepalive
!
router ospf 10
 log-adjacency-changes
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.78.240.1
ip route 172.16.0.0 255.255.0.0 200.100.100.6
ip route 172.17.0.0 255.255.0.0 200.200.100.6
ip route 172.17.200.0 255.255.255.0 200.200.100.6
ip route 192.168.20.2 255.255.255.255 Integrated-Service-Engine1/0
ip route 200.100.100.0 255.255.255.0 200.100.100.9
ip route 200.200.100.0 255.255.255.0 200.200.100.9
!
!
no ip http server
!
dialer-list 1 protocol ip permit
!
!
control-plane
!
!
line con 0
line aux 0
line 66
 no activation-character
 no exec
 transport preferred none
```

```
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120
line vty 0 4
 password jvsl@123
 login
!
scheduler allocate 20000 1000
!
end

JVSL-Br-ISR-01#
```

サービスの設定

サービス スイッチの設定

サイト A

```
JVSL-A-C6k-01#sh run
Building configuration...

Current configuration : 7805 bytes
!
upgrade fpd auto
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service counters max age 5
!
hostname JVSL-A-C6k-01
!
boot-start-marker
boot system sup-bootdisk:s72033-advipservicesk9_wan-vz.122-33.SXH8.bin
boot-end-marker
!
security passwords min-length 1
enable secret 5 $1$uOmU$GWdTTw0/f3icGLUCCRYZV.
!
no aaa new-model
intrusion-detection module 3 management-port access-vlan 500
intrusion-detection module 3 data-port 1 access-vlan 60
intrusion-detection module 3 data-port 2 access-vlan 70
ip subnet-zero
```

```
ip routing protocol purge interface
ip wccp 61
ip wccp 62
!
!
no ip domain-lookup
!
call-home
 alert-group configuration
 alert-group diagnostic
 alert-group environment
 alert-group inventory
 alert-group syslog
mls netflow interface
no mls flow ip
no mls flow ipv6
no mls rate-limit unicast acl vacl-log
mls cef error action reset
!
!
!
!
!
!
!
!
redundancy
 keepalive-enable
 mode sso
 main-cpu
  auto-sync running-config
fabric timer 15
diagnostic bootup level minimal
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
!
vlan access-map IPS_Traffic 10
 match ip address traffic_to_idsm
```

```
 action forward capture
!
vlan internal allocation policy ascending
!
!
!
!
!
interface Port-channel67
 description L3_PC_to_AGG_N7k_01
 ip address 172.16.1.38 255.255.255.252
!
interface Port-channel68
 description L3_PC_to_AGG_N7K_02
 ip address 172.16.1.42 255.255.255.252
 ip wccp 62 redirect in
!
interface TenGigabitEthernet1/1
 description LINK_TO_AGG_N7K_01_7/23
 no ip address
 channel-protocol lacp
 channel-group 67 mode active
!
interface TenGigabitEthernet1/2
 description LINK_TO_AGG_N7K_01_7/24
 no ip address
 channel-protocol lacp
 channel-group 67 mode active
!
interface TenGigabitEthernet1/3
 description LINK_TO_N7K_02_ETH7/23
 no ip address
 channel-protocol lacp
 channel-group 68 mode active
!
interface TenGigabitEthernet1/4
 description LINK_TO_N7K_02_ETH7/24
 no ip address
 channel-protocol lacp
 channel-group 68 mode active
!
interface GigabitEthernet2/1
 switchport
```

```
 switchport access vlan 500
 speed 100
!
interface GigabitEthernet2/2
 no ip address
 shutdown
!
interface GigabitEthernet2/3
 description connected_2_DNSserver
 switchport
 switchport access vlan 80
 switchport mode access
!
interface GigabitEthernet2/4
 description Connected_to_DNS_server
 switchport
 switchport access vlan 80
 switchport mode access
!
interface GigabitEthernet2/5
 description Connected-to-AD
 switchport
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet2/6
 description Connected-to-AD_HP_psw
 switchport
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet2/7
 no ip address
 shutdown
!
interface GigabitEthernet2/8
 description "Connected-to-SiteB-CAT6k"
 switchport
 switchport access vlan 500
 switchport mode access
!
interface GigabitEthernet2/9
 no ip address
```

```
 shutdown
!
interface GigabitEthernet2/10
 no ip address
 shutdown
!
interface GigabitEthernet2/11
 no ip address
 shutdown
!
interface GigabitEthernet2/12
 no ip address
 shutdown
!
interface GigabitEthernet2/13
 no ip address
 shutdown
!
interface GigabitEthernet2/14
 switchport
 switchport access vlan 50
 switchport mode access
!
interface GigabitEthernet2/15
 description Connected to WAAS_WAN0_interface
 switchport
 switchport mode access
!
interface GigabitEthernet2/16
 description "Connected_to_WAAS_G1/0
 switchport
 switchport access vlan 10
 switchport mode access
!
interface GigabitEthernet2/17
 description Connected_to_ACE_Interface
 switchport
 switchport access vlan 30
 switchport mode access
!
interface GigabitEthernet2/18
 description Connected_to_ACE_Server_Interface
 switchport
```

```
 switchport access vlan 200
 switchport mode access
!
interface GigabitEthernet2/19
 description Connected_to_SiteA-ASA_inside_interface
 switchport
 switchport access vlan 40
 switchport mode access
!
interface GigabitEthernet2/20
 description Connected_to_siteA-ASA_outside_interface
 switchport
 switchport access vlan 50
 switchport mode access
!
interface GigabitEthernet2/21
 description idsm_int_inlin1
 switchport
 switchport access vlan 60
 switchport mode access
 shutdown
!
interface GigabitEthernet2/22
 switchport
 switchport access vlan 70
 switchport mode access
!
interface GigabitEthernet2/23
 no ip address
 shutdown
!
interface GigabitEthernet2/24
 ip address 172.16.90.1 255.255.255.0
!
interface GigabitEthernet2/25
 no ip address
 shutdown
!
interface GigabitEthernet2/26
 no ip address
 shutdown
!
interface GigabitEthernet2/27
```

```
 no ip address
 shutdown
!
interface GigabitEthernet2/28
 no ip address
 shutdown
!
interface GigabitEthernet2/29
 no ip address
 shutdown
!
interface GigabitEthernet2/30
 no ip address
 shutdown
!
interface GigabitEthernet2/31
 no ip address
 shutdown
!
interface GigabitEthernet2/32
 no ip address
 shutdown
!
interface GigabitEthernet2/33
 no ip address
 shutdown
!
interface GigabitEthernet2/34
 no ip address
 shutdown
!
interface GigabitEthernet2/35
 no ip address
 shutdown
!
interface GigabitEthernet2/36
 no ip address
 shutdown
!
interface GigabitEthernet2/37
 switchport
 switchport access vlan 500
!
```

```
interface GigabitEthernet2/38
 switchport
 switchport access vlan 500
 speed 100
!
interface GigabitEthernet2/39
 switchport
 switchport access vlan 500
 switchport mode access
 speed 1000
!
interface GigabitEthernet2/40
 switchport
 switchport access vlan 500
 switchport mode access
 speed 100
!
interface GigabitEthernet2/41
 no ip address
 shutdown
!
interface GigabitEthernet2/42
 no ip address
 shutdown
!
interface GigabitEthernet2/43
 no ip address
 shutdown
!
interface GigabitEthernet2/44
 no ip address
 shutdown
!
interface GigabitEthernet2/45
 no ip address
 shutdown
!
interface GigabitEthernet2/46
 no ip address
 shutdown
!
interface GigabitEthernet2/47
 description testing_connectedtoISR
```

```
 no ip address
 shutdown
 speed 100
!
interface GigabitEthernet2/48
 no ip address
 shutdown
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 description "To_WAAS_Appliance"
 ip address 172.16.10.1 255.255.255.0
!
interface Vlan20
 no ip address
 shutdown
!
interface Vlan30
 ip address 172.16.30.1 255.255.255.0
!
interface Vlan40
 ip address 172.16.40.1 255.255.255.0
 ip policy route-map return-traffic
!
interface Vlan50
 ip address 172.16.50.1 255.255.255.0
 ip policy route-map client-traffic
!
interface Vlan60
 no ip address
 shutdown
!
```

```
interface Vlan80
 ip address 172.16.80.1 255.255.255.0
!
interface Vlan100
 no ip address
 ip wccp 61 redirect in
!
interface Vlan200
 no ip address
!
interface Vlan500
 description mgmt_vlan
 ip address 10.78.240.9 255.255.255.0
!
router ospf 10
 log-adjacency-changes
 timers lsa arrival 10
 network 172.16.1.0 0.0.0.255 area 10
 network 172.16.10.0 0.0.0.255 area 10
 network 172.16.20.0 0.0.0.255 area 10
 network 172.16.30.0 0.0.0.255 area 10
 network 172.16.40.0 0.0.0.255 area 10
 network 172.16.50.0 0.0.0.255 area 10
 network 172.16.80.0 0.0.0.255 area 10
 network 172.16.90.0 0.0.0.255 area 10
 network 172.16.100.0 0.0.0.255 area 10
 network 172.16.200.0 0.0.0.255 area 10
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.78.240.1
ip route 192.168.10.0 255.255.255.0 172.16.1.18
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
dial-peer cor custom
```

```
!
!
!
!
line con 0
 password jvsl@123
 login
line vty 0 4
 password jvsl@123
 login
line vty 5 9
 password jvsl@123
 login
line vty 10 15
 login
!
exception core-file
!
no event manager policy Mandatory.go_switchbus.tcl type system
!
end

JVSL-A-C6k-01#
```

サイト B

```
JVSL-B-C6k-01#sh run
Building configuration...

Current configuration : 5038 bytes
!
upgrade fpd auto
version 12.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service counters max age 5
!
hostname JVSL-B-C6k-01
!
boot-start-marker
boot system sup-bootdisk:s72033-advipservicesk9_wan-vz.122-33.SXH8.bin
boot-end-marker
```

```
!
security passwords min-length 1
enable password jvsl@123
!
username cisco password 0 jvsl@123
no aaa new-model
ip subnet-zero
ip routing protocol purge interface
!
!
no ip domain-lookup
!
call-home
 alert-group configuration
 alert-group diagnostic
 alert-group environment
 alert-group inventory
 alert-group syslog
mls netflow interface
no mls flow ip
no mls flow ipv6
mls cef error action reset
!
!
!
!
!
!
!
!
redundancy
 keepalive-enable
 mode sso
 main-cpu
  auto-sync running-config
fabric timer 15
diagnostic bootup level minimal
diagnostic cns publish cisco.cns.device.diag_results
diagnostic cns subscribe cisco.cns.device.diag_commands
spanning-tree mode pvst
spanning-tree extend system-id
!
!
```

```
!
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
!
!
!
interface Port-channel67
 description L3_PC_to_AGG_N7k_01
 ip address 172.17.1.38 255.255.255.252
!
interface Port-channel68
 description L3_PC_to_AGG_N7K_02
 ip address 172.17.1.42 255.255.255.252
!
interface TenGigabitEthernet1/1
 description LINK_TO_AGG_N7K_01_7/23
 no ip address
 channel-protocol lacp
 channel-group 67 mode active
!
interface TenGigabitEthernet1/2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 500
 switchport mode trunk
!
interface TenGigabitEthernet1/3
 description LINK_TO_N7K_02_ETH7/23
 no ip address
 channel-protocol lacp
 channel-group 68 mode active
!
interface TenGigabitEthernet1/4
 no ip address
 shutdown
!
interface GigabitEthernet2/1
 description Connected_to_ACE_Interface
 switchport
 switchport access vlan 30
 switchport mode access
```

```
!
interface GigabitEthernet2/2
 description Connected_to_ACE_Interface
 switchport
 switchport access vlan 200
 switchport mode access
!
interface GigabitEthernet2/3
 no ip address
 shutdown
!
interface GigabitEthernet2/4
 no ip address
 shutdown
!
interface GigabitEthernet2/5
 no ip address
 shutdown
!
interface GigabitEthernet2/6
 no ip address
 shutdown
!
interface GigabitEthernet2/7
 no ip address
 shutdown
!
interface GigabitEthernet2/8
 description "Connected-to-SiteA-CAT6k"
 switchport
 switchport access vlan 500
 switchport mode access
!
interface GigabitEthernet2/9
 description "Connected to GSS"
 ip address 172.17.90.1 255.255.255.0
!
interface GigabitEthernet2/10
 description "Connected_to_WAAS_G1/0
 switchport
 switchport access vlan 10
 switchport mode access
 shutdown
```

```
!
interface GigabitEthernet2/11
 description connected_to_site B-ASA_inside_interface
 switchport
 switchport access vlan 40
 switchport mode access
!
interface GigabitEthernet2/12
 description connected_to_site B-ASA_outside_interface
 switchport
 switchport access vlan 50
 switchport mode access
!
interface GigabitEthernet2/13
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet2/14
 description "Connected_to_B-ACC-n5k02_1/15"
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet2/15
 description "MGMT_connectivity"
 switchport
 switchport access vlan 500
 switchport mode access
 speed 100
 duplex full
!
interface GigabitEthernet2/16
 description "Management connectivity"
 switchport
 switchport access vlan 500
 switchport mode access
 speed 100
 duplex full
!
interface GigabitEthernet5/1
 no ip address
 shutdown
```

```
!
interface GigabitEthernet5/2
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 description "TO_WAAS_Appliance"
 ip address 172.17.10.1 255.255.255.0
 shutdown
!
interface Vlan30
 ip address 172.17.30.1 255.255.255.0
!
interface Vlan40
 ip address 172.17.40.1 255.255.255.0
 ip policy route-map return-traffic
 shutdown
!
interface Vlan50
 ip address 172.17.50.1 255.255.255.0
 ip policy route-map client-traffic
 shutdown
!
interface Vlan200
 ip address 172.17.200.8 255.255.255.0
!
interface Vlan500
 ip address 10.78.240.109 255.255.255.0
!
router ospf 10
 log-adjacency-changes
 network 172.16.200.0 0.0.0.255 area 10
 network 172.17.1.0 0.0.0.255 area 10
 network 172.17.10.0 0.0.0.255 area 10
 network 172.17.20.0 0.0.0.255 area 10
 network 172.17.30.0 0.0.0.255 area 10
 network 172.17.40.0 0.0.0.255 area 10
 network 172.17.50.0 0.0.0.255 area 10
 network 172.17.80.0 0.0.0.255 area 10
```

```
 network 172.17.90.0 0.0.0.255 area 10
 network 172.17.100.0 0.0.0.255 area 10
 network 172.17.200.0 0.0.0.255 area 10
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.78.240.1
ip route 192.168.10.0 255.255.255.0 172.17.1.18
!
no ip http server
no ip http secure-server
!
!
!
!
!
control-plane
!
!
dial-peer cor custom
!
!
!
!
line con 0
line vty 0 4
 password jvsl@123
 login
line vty 5 15
 login
!
exception core-file
!
no event manager policy Mandatory.go_switchbus.tcl type system
!
end

JVSL-B-C6k-01#
```

ACE の設定

サイト A

```
hostname JVSL-A-ACE-01
interface gigabitEthernet 1/1
  switchport access vlan 1000
  no shutdown
interface gigabitEthernet 1/2
  description Connected_to_Cat6k_g2/1
  switchport access vlan 30
  no shutdown
interface gigabitEthernet 1/3
  description Connected_to_Cat6k_g2/2
  switchport access vlan 100
  no shutdown
interface gigabitEthernet 1/4
  shutdown


access-list ALL line 8 extended permit ip any any
access-list allow_icmp line 8 extended permit icmp any any
access-list allowed-traffice-ace line 16 extended permit ip any 172.16.0.0 255.255.0.0



probe https Exchange-Server-Probe_https
  interval 15
  passdetect interval 60
  ssl version all
  expect status 200 200
  open 1

rserver host CAS1-SiteB
  ip address 172.16.100.15
  inservice
rserver host CAS2-siteB
  ip address 172.16.100.16
  inservice


serverfarm host Server-Farm-Exchange
  rserver CAS1-SiteB
```

```
    inservice
  rserver CAS2-siteB
    inservice

class-map match-all ACE-VIP-NEW
  2 match virtual-address 172.16.30.5 tcp any
class-map type management match-any remote_access
  2 match protocol xml-https any
  3 match protocol icmp any
  4 match protocol telnet any
  5 match protocol ssh any
  6 match protocol http any
  7 match protocol https any
  8 match protocol snmp any

policy-map type management first-match remote_mgmt_allow_policy
  class remote_access
    permit

policy-map type loadbalance first-match ACE-VIP-NEW-l7slb
  class class-default
    serverfarm Server-Farm-Exchange

policy-map multi-match int30
  class ACE-VIP-NEW
    loadbalance vip inservice
    loadbalance policy ACE-VIP-NEW-l7slb
    loadbalance vip icmp-reply
    nat dynamic 1 vlan 100

interface vlan 30
  description client_vlan
  ip address 172.16.30.2 255.255.255.0
  access-group input ALL
  service-policy input remote_mgmt_allow_policy
  service-policy input int30
  no shutdown
interface vlan 80
  ip address 172.16.80.20 255.255.255.0
  no shutdown
interface vlan 100
  description server_vlan
  ip address 172.16.100.7 255.255.255.0
```

```
  access-group input ALL
  nat-pool 1 172.16.100.11 172.16.100.14 netmask 255.255.255.0 pat
  service-policy input remote_mgmt_allow_policy
  no shutdown
interface vlan 500
interface vlan 1000
  ip address 10.78.240.115 255.255.255.0
  access-group input ALL
  service-policy input remote_mgmt_allow_policy
  no shutdown

ip route 10.0.0.0 255.0.0.0 10.78.240.1
ip route 172.16.1.0 255.255.255.0 172.16.30.1
ip route 192.168.10.0 255.255.255.0 172.16.30.1

snmp-server community public group Network-Monitor


username admin password 5 $1$DNpoLpd2$K2GlbmsGEO.mV0hK2Jb3M0  role Admin domain
default-domain
username www password 5 $1$BRiU//w3$/o2PUqHI5u/kAaA83trCR.  role Admin domain de
fault-domain
ssh key rsa 1024 force
```

サイト B

```
hostname JVSL-B-ACE-01
interface gigabitEthernet 1/1
  switchport access vlan 1000
  no shutdown
interface gigabitEthernet 1/2
  description Connected_to_Cat6k_g2/1
  switchport access vlan 30
  no shutdown
interface gigabitEthernet 1/3
  description Connected_to_Cat6k_g2/2
  switchport access vlan 100
  no shutdown
interface gigabitEthernet 1/4
  shutdown


access-list ALL line 8 extended permit ip any any
```

```
access-list allow_icmp line 8 extended permit icmp any any
access-list allowed-traffice-ace line 16 extended permit ip any 172.17.0.0 255.2
55.0.0



probe https Exchange-Server-Probe_https
  interval 15
  passdetect interval 60
  ssl version all
  expect status 200 200
  open 1

rserver host CAS1-SiteB
  ip address 172.17.100.15
  inservice
rserver host CAS2-siteB
  ip address 172.17.100.16
  inservice


serverfarm host Server-Farm-Exchange
  rserver CAS1-SiteB
    inservice
  rserver CAS2-siteB
    inservice

class-map match-all ACE-VIP-NEW
  2 match virtual-address 172.17.30.5 tcp any
class-map type management match-any remote_access
  2 match protocol xml-https any
  3 match protocol icmp any
  4 match protocol telnet any
  5 match protocol ssh any
  6 match protocol http any
  7 match protocol https any
  8 match protocol snmp any

policy-map type management first-match remote_mgmt_allow_policy
  class remote_access
    permit

policy-map type loadbalance first-match ACE-VIP-NEW-l7slb
```

```
  class class-default
    serverfarm Server-Farm-Exchange

policy-map multi-match int30
  class ACE-VIP-NEW
    loadbalance vip inservice
    loadbalance policy ACE-VIP-NEW-l7slb
    loadbalance vip icmp-reply
    nat dynamic 1 vlan 100

interface vlan 30
  description client_vlan
  ip address 172.17.30.2 255.255.255.0
  access-group input ALL
  service-policy input remote_mgmt_allow_policy
  service-policy input int30
  no shutdown
interface vlan 80
  ip address 172.17.80.20 255.255.255.0
  no shutdown
interface vlan 100
  description server_vlan
  ip address 172.17.100.7 255.255.255.0
  access-group input ALL
  nat-pool 1 172.17.100.11 172.17.100.14 netmask 255.255.255.0 pat
  service-policy input remote_mgmt_allow_policy
  no shutdown
interface vlan 500
interface vlan 1000
  ip address 10.78.240.115 255.255.255.0
  access-group input ALL
  service-policy input remote_mgmt_allow_policy
  no shutdown

ip route 10.0.0.0 255.0.0.0 10.78.240.1
ip route 172.17.1.0 255.255.255.0 172.17.30.1
ip route 192.168.10.0 255.255.255.0 172.17.30.1

snmp-server community public group Network-Monitor


username admin password 5 $1$DNpoLpd2$K2GlbmsGEO.mV0hK2Jb3M0  role Admin domain
default-domain
```

```
username www password 5 $1$BRiU//w3$/o2PUqHI5u/kAaA83trCR.  role Admin domain de
fault-domain
ssh key rsa 1024 force
```

ASA の設定

サイト A

```
JVSL-A-ASA-01# show start
: Saved
: Written by enable_15 at 04:31:44.905 UTC Fri Apr 1 2011
!
ASA Version 8.4(1)
!
hostname JVSL-A-ASA-01
enable password GUd/ZZsr52VmM9ER encrypted
passwd GUd/ZZsr52VmM9ER encrypted
names
!
interface Management0/0
 nameif management
 security-level 100
 ip address 10.78.240.13 255.255.255.0
 management-only
!
interface Management0/1
 shutdown
 no nameif
 no security-level
 no ip address
 management-only
!
interface GigabitEthernet3/0
 shutdown
 nameif server-interface-inside
 security-level 100
 ip address 172.16.40.2 255.255.255.0
!
interface GigabitEthernet3/1
 shutdown
 nameif client-interface-outside
 security-level 0
 ip address 172.16.50.2 255.255.255.0
!
interface GigabitEthernet3/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet3/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet4/0
 shutdown
```

```
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet4/1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet4/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet4/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet8/0
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet8/1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet8/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet8/3
 shutdown
 no nameif
 no security-level
 no ip address
!
boot system disk0:/asa841-smp-k8.bin
ftp mode passive
access-list allow_all extended permit ip any any
access-list allowed-traffic extended permit ip any any
access-list allow-client-traffic extended permit ip 172.16.30.0 255.255.255.0 17
2.16.100.0 255.255.255.0
access-list allow-client-traffic extended permit ip any any
access-list allow-server-traffic extended permit ip 172.16.100.0 255.255.255.0 1
72.16.30.0 255.255.255.0
access-list allow-server-traffic extended permit ip any any
pager lines 24
logging enable
logging asdm informational
mtu management 1500
mtu server-interface-inside 1500
mtu client-interface-outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
```

```
icmp permit any server-interface-inside
icmp permit any client-interface-outside
asdm image disk0:/asdm-641.bin
no asdm history enable
arp timeout 14400
access-group allow_all in interface management
access-group allow-server-traffic in interface server-interface-inside
access-group allow-client-traffic in interface client-interface-outside
route management 0.0.0.0 0.0.0.0 10.78.240.1 1
route client-interface-outside 172.16.30.0 255.255.255.0 172.16.50.1 1
route server-interface-inside 172.16.100.0 255.255.255.0 172.16.40.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 10.78.240.0 255.255.255.0 management
http 10.78.0.0 255.255.0.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet 0.0.0.0 0.0.0.0 management
telnet timeout 5
ssh timeout 5
console timeout 0
!
tls-proxy maximum-session 1000
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
webvpn
username admin password ONIkFOfMEpT3E8Yu encrypted privilege 15
!
!
prompt hostname context
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DD
CEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly 14
  subscribe-to-alert-group configuration periodic monthly 14
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:dc7b9f2390e251396ed9079682ef44a9
JVSL-A-ASA-01#
```

サイト B

```
JVSL-B-ASA-01# show start
: Saved
: Written by admin at 04:27:32.719 UTC Mon Mar 7 2011
!
```

```
ASA Version 8.1(2)
!
hostname JVSL-B-ASA-01
enable password GUd/ZZsr52VmM9ER encrypted
passwd GUd/ZZsr52VmM9ER encrypted
names
!
interface Management0/0
 nameif management
 security-level 100
 ip address 10.78.240.113 255.255.255.0
 management-only
!
interface Management0/1
 shutdown
 no nameif
 no security-level
 no ip address
 management-only
!
interface GigabitEthernet3/0
 nameif server-interface-inside
 security-level 100
 ip address 172.17.40.2 255.255.255.0
!
interface GigabitEthernet3/1
 nameif client-interface-outside
 security-level 0
 ip address 172.17.50.2 255.255.255.0
!
interface GigabitEthernet3/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet3/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet4/0
```

```
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet4/1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet4/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet4/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet8/0
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet8/1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet8/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet8/3
 shutdown
```

```
 no nameif
 no security-level
 no ip address
!
ftp mode passive
access-list allow-all extended permit ip any any
access-list allowed-traffic extended permit ip any any
access-list allow-client-traffic extended permit ip 172.17.30.0 255.255.255.0 17
2.17.100.0 255.255.255.0
access-list allow-client-traffic extended permit ip any any
access-list allow-server-traffic extended permit ip 172.17.100.0 255.255.255.0 1
72.17.30.0 255.255.255.0
access-list allow-server-traffic extended permit ip any any
pager lines 24
logging enable
logging asdm informational
mtu management 1500
mtu server-interface-inside 1500
mtu client-interface-outside 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
icmp permit any server-interface-inside
icmp permit any client-interface-outside
asdm image disk0:/asdm-641.bin
no asdm history enable
arp timeout 14400
global (client-interface-outside) 101 interface
nat (management) 101 0.0.0.0 0.0.0.0
access-group allow-all in interface management
access-group allow-server-traffic in interface server-interface-inside
access-group allow-client-traffic in interface client-interface-outside
route management 0.0.0.0 0.0.0.0 10.78.240.1 1
route client-interface-outside 172.17.30.0 255.255.255.0 172.17.50.1 1
route server-interface-inside 172.17.100.0 255.255.255.0 172.17.40.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 10.78.240.0 255.255.255.0 management
```

```
http 10.78.0.0 255.255.0.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet 10.78.240.0 255.255.255.0 management
telnet 0.0.0.0 0.0.0.0 management
telnet 10.78.0.0 255.255.0.0 management
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
username admin password ONIkFOfMEpT3E8Yu encrypted privilege 15
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect sunrpc
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
!
service-policy global_policy global
```

```
prompt hostname context
Cryptochecksum:bb8c7a4cc75df4dcf5b5dafc3d6c49c6
JVSL-B-ASA-01#
```

IDSM の設定

サイト A

```
JVSL-A-IDSM2-01# sh ver
Application Partition:

Cisco Intrusion Prevention System, Version 6.0(5)E2

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S339.0                  2008-06-11
    Virus Update        V1.4                    2007-03-02
OS Version:             2.4.30-IDS-smp-bigphys
Platform:               WS-SVC-IDSM-2
Serial Number:          SAD140502B0
No license present
Sensor up-time is 18 days.
Using 1406955520 out of 1983504384 bytes of available memory (70% usage)
system is using 17.7M out of 29.0M bytes of available disk space (61% usage)
application-data is using 38.4M out of 166.8M bytes of available disk space (24%
 usage)
boot is using 38.6M out of 68.6M bytes of available disk space (59% usage)
application-log is using 528.9M out of 2.8G bytes of available disk space (20% u
sage)


MainApp          N-2008_JUN_06_02_35   (Release)   2008-06-06T03:23:18-0500   Ru
nning
AnalysisEngine   N-2008_JUN_06_02_35   (Release)   2008-06-06T03:23:18-0500   Ru
nning
CLI              N-2008_JUN_06_02_35   (Release)   2008-06-06T03:23:18-0500


Upgrade History:

  IPS-K9-6.0-5-E2   06:13:26 UTC Sat Jan 22 2011

Maintenance Partition Version 2.1(3)

Recovery Partition Version 1.1 - 6.0(5)E2

JVSL-A-IDSM2-01#

JVSL-A-IDSM2-01# sh configuration
! ------------------------------
! Current configuration last modified Wed Jan 19 07:58:38 2011
! ------------------------------
! Version 6.0(5)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S339.0   2008-06-11
```

```
!     Virus Update        V1.4     2007-03-02
! ------------------------------
service interface
inline-interfaces PAIR1
description PAIR1 = Gig0/7 & Gig 0/8
interface1 GigabitEthernet0/7
interface2 GigabitEthernet0/8
exit
bypass-mode off
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.78.240.14/24,10.78.240.1
host-name JVSL-A-IDSM2-01
telnet-option enabled
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
trusted-certificates 10.78.240.200 certificate MIIDZDCCAkygAwIBAgIEzQdDMTANBgkqh
kiG9w0BAQUFADAbMRkwFwYDVQQKExBWTXdhcmUgSW5zdGFsbGVyMB4XDTA5MTAwMTA4MTQyN1oXDTE5M
DkyOTA4MTQyN1owdjEVMBMGA1UEChMMVk13YXJlLCBJbmMuMRUwEwYDVQQLEwxWTXdhcmUsIEluYy4xI
zAhBgNVBAMTGlZNd2FyZSBkZWZhdWx0IGNlcnRpZmljYXRlMSEwHwYJKoZIhvcNAQkBFhJzdXBwb3J0Q
HZtd2FyZS5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCeFDGp0Po3DwQH/Er9QxxsL
cOGDzryf+cd8o0J3wrruPbbSOSmpWqHjlEeCk+wEyEhLBP1ngOdgzgRJrZc1VhIZMT1rqQiDBu0tm3eq
vnPPB5fUDgs6eFV77ELgvhiiT2j95jtaNbFbmig3+t6xYgRkqN1Ou1/mCQT6t5rFnBYMkQL+KskuiwEi
L/a97DDK/yVFWa3SCdUzJyeUnBbxh+g+PmiuxyGn4NZh86TKcowQhZ72/tu6XNe1QZSjH4OAvROMOeHE
z7htSBsNOhXc5l4r6mUb4Amkut4Zz23K22wicpWPohCMxWQkMiaSLVqkcA8QBbvL+jf3FKIBIR6MZWfA
gMBAAGjVTBTMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgSwMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFB
QcDAjAaBgNVHREEEzARgg9oY2wtZnBwbzhwYXpsMXcwDQYJKoZIhvcNAQEFBQADggEBAD24SBfS/f7QK
YTnrQSCJuNaTZkSNx+TlahXYhc2R4QKkdJGY6EfO293SF0uWFIaLMPQ4rQwNcNr7lBnuNiKzbz/xV+JX
6AkbCENKlRHtIEWzgTFuh7Y805e+StbyTGfRCorqKlfi0GxXpV6EOd0kNxEamTM9cvYC5GdSmVEKCwWk
ewsOZ/uXujSJSWlaGoXWionycS3gt8mPh+l7MM9yku05Gqnb63WuazE8S10Y7t3VFdyT0DfUsQnAp+MI
SHxIHtXvhfu2iCWsUuL85Os7os3WruT51GRG0VmXRG/MF3rTahfXzYHnfVhnSyphF+SuYL58VCpfl4s7
/Nm8j4X/EY=
exit
! ------------------------------
service web-server
```

```
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service analysis-engine
virtual-sensor vs0
logical-interface PAIR1
exit
exit
JVSL-A-IDSM2-01#
```

サイト B

```
ips_b# show configuration
!------------------------------
!Current configuration last modified Wed Feb 23 04:49:19 2011
!------------------------------
!Version 6.0(5)
!Host:
!     Realm Keys          key1.0
!Signature Definition:
!     Signature Update    S339.0   2008-06-11
!     Virus Update        V1.4     2007-03-02
!------------------------------
service interface
exit
!------------------------------
service authentication
exit
!------------------------------
service event-action-rules rules0
exit
!------------------------------
service host
network-settings
host-ip 10.78.240.114/24,10.78.240.1
host-name JVSL-B-IDSM2-01
telnet-option enabled
access-list 10.78.0.0/24
exit
exit
!------------------------------
service logger
```

```
exit
!------------------------------
service network-access
exit
!------------------------------
service notification
exit
!------------------------------
service signature-definition sig0
exit
!------------------------------
service ssh-known-hosts
exit
!------------------------------
service trusted-certificates
exit
!------------------------------
service web-server
exit
!------------------------------
service anomaly-detection ad0
exit
!------------------------------
service external-product-interface
exit
!------------------------------
service analysis-engine
exit
ips_b#
```

GSS の設定

サイト A

```
JVSL-A-GSS-01.cisco.com#sh run
interface ethernet 0
   ip address 10.78.240.10 255.255.255.0
   gss-communications
   duplex full
   speed 100
interface ethernet 1
   ip address 172.16.90.2 255.255.255.0

hostname JVSL-A-GSS-01.cisco.com
ip default-gateway 10.78.240.1
```

```
ip name-server 72.163.128.140

ip route 172.16.0.0 255.255.0.0 172.16.90.1
ip route 192.168.10.0 255.255.255.0 172.16.90.1
ip route 200.100.100.0 255.255.255.0 172.16.90.1

ssh enable
no ssh keys
ssh protocol version 1
telnet enable
ftp enable
snmp-server trap-source ethernet 0

no cnr enable

drp
    no enable

terminal-length 23
exec-timeout 150

logging disk enable
logging disk priority Notifications
no logging host enable
logging host priority Warnings
logging facility local5

tacacs-server timeout 5
tacacs-server keepalive-enable
```

サイト B

```
JVSL-B-GSS-01.cisco.com#sh run
interface ethernet 0
   ip address 10.78.240.110 255.255.255.0
   gss-communications
interface ethernet 1
   ip address 172.17.90.2 255.255.255.0
   duplex full
   speed 100


hostname JVSL-B-GSS-01.cisco.com
ip default-gateway 10.78.240.1
ip name-server 72.163.128.140


ip route 172.17.0.0 255.255.0.0 172.17.90.1
ip route 192.168.10.0 255.255.255.0 172.17.90.1
ip route 200.100.100.0 255.255.255.0 172.17.90.1


ssh enable
no ssh keys
no ssh protocol version 1
```

```
telnet enable
snmp-server trap-source ethernet 0

no cnr enable

drp
    no enable

terminal-length 23
exec-timeout 150

logging disk enable
logging disk priority Notifications
no logging host enable
logging host priority Warnings
logging facility local5

tacacs-server timeout 5
tacacs-server keepalive-enable
```