企業ユーザ用 Cisco Japan Virtualization System and Interoperability Lab（JVSL）

相互運用性テスト編

Cisco Japan Virtualization System and Interoperability Lab (JVSL) for Enterprise Customers

2010 年 4 月

Text Part Number: OL-23456-01-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。

CONTENTS

はじめに vii

マニュアルの構成 vii

表記法 vii

マニュアルの入手方法およびテクニカル サポート viii

CHAPTER 1 Japan Virtualization System and Interoperability Lab（J-VSL）の紹介 1-1

使用されるオペレーティング システムおよびソフトウェアのバージョン 1-3

CHAPTER 2 Japan Virtualization System and Interoperability Lab（J-VSL）の概要 2-1

IP インフラストラクチャの概要 2-1

Cisco Nexus 7000 シリーズ 2-2

Cisco Nexus 5000 シリーズ 2-2

Cisco Catalyst 6500 シリーズ 2-2

Cisco Nexus-OS 2-3

NX-OS の機能 2-3

レイヤ 4 ～ 7 サービスの概要 2-3

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス 2-4

Cisco IPS 2-4

サービス スイッチの統合 2-4

サービス シャーシ モデル（Cat6506e） 2-5

L4 ～ L7 サービスの実装 2-6

トラフィックのリダイレクション方法 2-6

Storage Area Networking（SAN）の概要 2-6

Cisco MDS 9140 2-7

Hitachi USP VM 2-7

SAN の概要 2-8

アプリケーションの概要 2-8

MS Exchange の概要 2-9

MS Exchange 2007 の主な機能 2-9

Exchange Load Generator 2-10

ブレード サーバの概要 2-10

Fujitsu PRIMERGY BX600 2-10

Cisco ブレード スイッチ 3040 2-11

CHAPTER 3 IP インフラストラクチャ 3-1
設定および確認 3-1
Nexus 7010 デバイスでの VDC 機能の設定および確認 3-2
Nexus 7010、5020、および Cat 6506e デバイス間の L2 ポート チャネルの設定および確認 3-3
Nexus 7010 デバイス間の L3 ポート チャネルの設定および確認 3-4
Nexus 7010 および Cat6506e 間の LACP プロトコルによる L2 ポート チャネルの設定および確認 3-5
Nexus 7010 および Nexus 5020 デバイス間の LACP プロトコルによる L2 ポート チャネルの設定および確認 3-6
Nexus 7010 デバイス間の LACP プロトコルによる L3 ポート チャネルの設定および確認 3-7
Nexus 7010 デバイスでの vPC の設定および確認 3-8
Nexus 7010 デバイスでの HSRP の設定および確認 3-9
Nexus 7010 デバイスでの VRF 機能の設定および確認 3-10
Nexus 7010 デバイスでの OSPF プロトコルの設定および確認 3-11
集約スイッチ（Nexus 7010）での STP 設定の確認 3-12
集約スイッチ（Nexus 7010）、アクセス スイッチ（Nexus 5020）、およびサービス スイッチ（Cat 6506e）での VLAN 設定の確認 3-13
ハイ アベイラビリティ - リンク障害 3-14
集約スイッチ（Nexus 7010）およびアクセス スイッチ（Nexus 5020）間の L2 ポート チャネルのリンク障害 3-14
コア スイッチおよび集約スイッチ（Nexus 7010）間の L3 ポート チャネルのリンク障害 3-15
Nexus 7010、5020、および Cat6506e デバイス間のポート チャネル（リンク）障害 3-16
ハイ アベイラビリティ - デバイス障害 3-18
アクセス スイッチ（Nexus5020）のリロード 3-18
集約スイッチ（Nexus 7010）のリロード 3-19

CHAPTER 4 L4 ～ L7 サービス 4-1
設定の確認 4-1
ASA 設定の確認 4-1
IPS 設定テスト 4-2
セキュリティ 4-2
ブランチ オフィス ユーザを制限する ASA の設定 4-3
SMTP 検査のイネーブル化 4-3
ハイ アベイラビリティ 4-3
IPS のリンク障害 4-4
IPS の障害 4-4

CHAPTER 5 Storage Area Networking（SAN） 5-1
MDS に関連する設定および確認 5-1
VSAN の設定（Fujitsu サーバから Hitachi ストレージへ） 5-1
ゾーンの設定（Fujitsu サーバから Hitachi ストレージへ） 5-2
IVR-with NAT 設定（Fujitsu サーバから Hitachi ストレージへ） 5-3
ホスト（Fujitsu サーバ）からストレージ（Hitachi）へのファブリック接続 5-5
マルチパスのイネーブル化 5-6
リンク障害（ケーブルを物理的に取り外す）（Fujitsu サーバから MDS へ） 5-6
リンク障害（ケーブルを物理的に取り外す）（MDS から Hitachi ストレージへ） 5-7
リンク障害（ポートのシャットダウン）（Fujitsu サーバから MDS へ） 5-8
リンク障害（ポートのシャットダウン）（MDS から Hitachi ストレージへ） 5-9
ファブリックでの VSAN の停止（VSAN SUSPEND） 5-10
マルチパスのディセーブル化 5-11
リンク障害（ケーブルを物理的に取り外す）（Fujitsu サーバから MDS へ） 5-11
リンク障害（ケーブルを物理的に取り外す）（MDS から Hitachi ストレージへ） 5-13
リンク障害（ポートのシャットダウン）（Fujitsu サーバから MDS へ） 5-14
リンク障害（ポートのシャットダウン）（MDS から Hitachi ストレージへ） 5-15
ファブリックでの VSAN の停止（VSAN SUSPEND） 5-16

CHAPTER 6 アプリケーション 6-1
基本的な Exchange の確認 6-1
基本的なメール交換の確認 6-1
ハイ アベイラビリティ 6-2
Exchange クラスタ プライマリ ホストの電源障害 6-2
Exchange クラスタ プライマリ ホストの取り外し（シャーシからのブレード サーバの取り外し） 6-3

CHAPTER 7 ブレード サーバ 7-1
基本的な接続と設定 7-1
NIC チーミング設定 7-1
Cisco ブレード スイッチ 3040 と Nexus 5020 の間のレイヤ 2 トランク設定 7-2
Cisco ブレード スイッチ 3040 と Nexus 5020 の間の L2 ポート チャネル設定 7-3
Cisco ブレード スイッチ 3040 および Nexus 5020 での LACP プロトコルによる L2 ポート チャネル 7-4
Cisco ブレード スイッチ 3040 の LST 機能 7-5
ブレード スイッチの STP 設定 7-6
ハイ アベイラビリティ 7-7
ブレード スイッチのリロード 7-7

ブレード スイッチと Nexus 5020（LST）の間のポート チャネル障害 7-8

APPENDIX A **IP インフラストラクチャの実装** A-1
レイヤ 3 トポロジの実装 A-1
レイヤ 2 トポロジの実装 A-2

APPENDIX B **Storage Area Networking（SAN）の実装** B-1
MDS 9140 の実装 B-1
Hitachi USP VM の実装 B-2

APPENDIX C **MS Exchange の実装** C-1

APPENDIX D **ブレード サーバの実装** D-1

APPENDIX E **設定** E-1
IP インフラストラクチャ コンポーネント E-1
コア スイッチの設定 E-1
集約スイッチの設定 E-9
アクセス スイッチの設定 E-21
レイヤ 4 ～ 7 サービス コンポーネント E-26
Storage Area Networking（SAN）コンポーネント E-41
ブレード スイッチ 3040 E-51
Cisco ブレード スイッチ 3040 E-56
サーバ ハードウェアおよびソフトウェアの詳細 E-61
ストレージ設定の詳細 E-61

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。

- 紹介と概要
  - 「Japan Virtualization System and Interoperability Lab（J-VSL）の紹介」
  - 「Japan Virtualization System and Interoperability Lab（J-VSL）の概要」
- テスト ケース
  - 「IP インフラストラクチャ」
  - 「L4 ～ L7 サービス」
  - 「Storage Area Networking（SAN）」
  - 「アプリケーション」
  - 「ブレード サーバ」
- 付録
  - 「IP インフラストラクチャの実装」
  - 「Storage Area Networking（SAN）の実装」
  - 「MS Exchange の実装」
  - 「ブレード サーバの実装」
  - 「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*

項目	表記法
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。

CHAPTER 1

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

相互運用性テスト編では、デバイスの全般的な機能と設定に関する基本テストを実行します。このテストでは、メール クライアントがメール サーバに到達できること、およびユーザがメールを送受信できることを確認します。

相互運用性テストは、ネットワーク、サーバ、ストレージの相互運用性テストと HA テストという 2 つの主要カテゴリに分類されます。

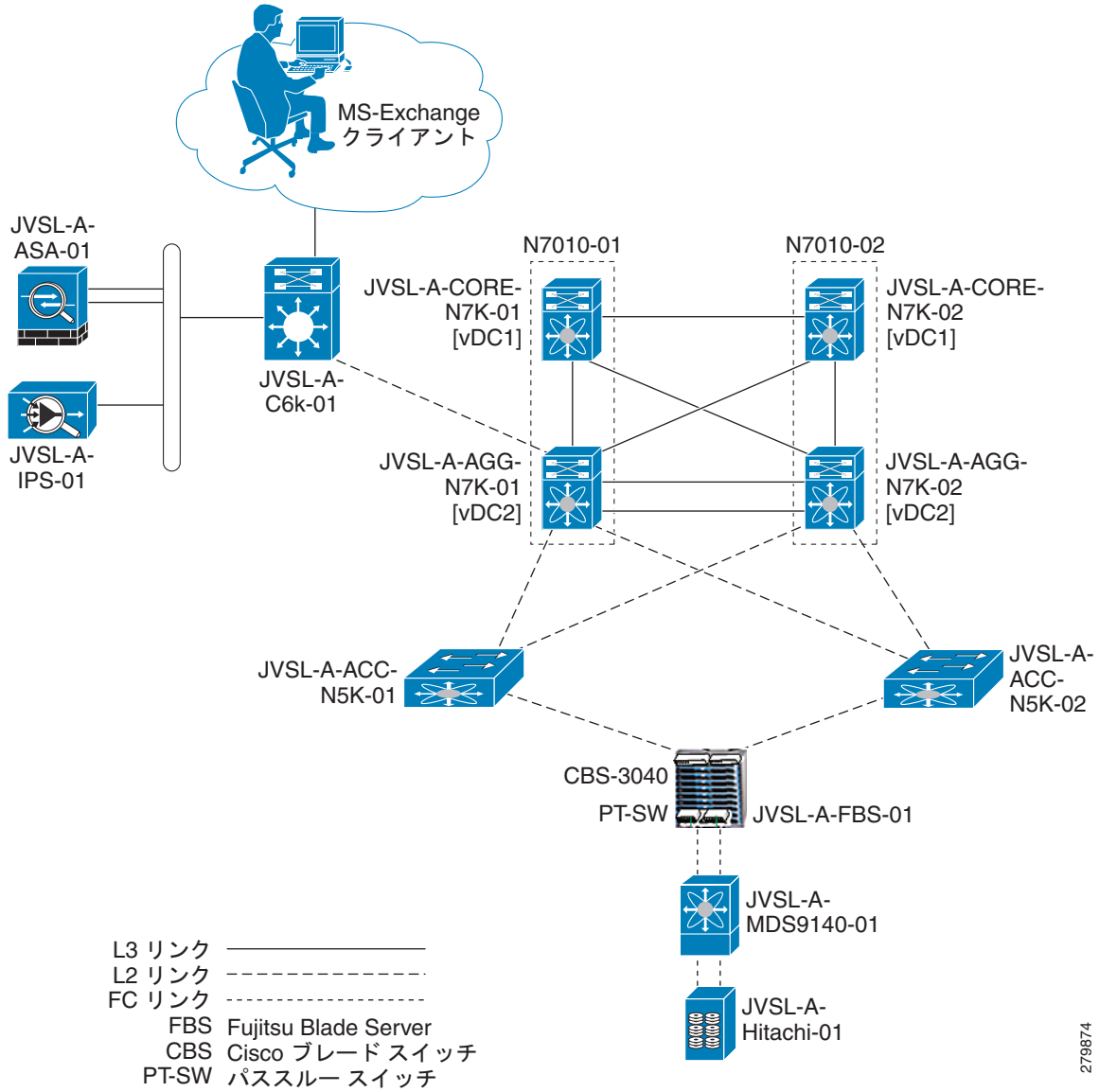
- 相互運用性テストには、クライアントからサーバにトラフィックを渡す処理、およびトラフィック フローが予測どおりであり、ストレージ デバイスがデータを受信することを確認する処理が含まれます。また、相互運用性テストには障害テストが含まれます。障害テストでは、ケーブルの引き抜き、停電、コンポーネント障害など、多様な障害条件に対する相互運用性テスト トポロジの反応を測定します。
- HA テストには、単一サイトの冗長デバイスの障害（L2 ～ L3 デバイス、SAN デバイス、およびブレード スイッチの障害など）が含まれます。

相互運用性テスト トポロジは、単一のサイトと次のカテゴリのデバイスから構成されます。

- IP インフラストラクチャ（L2 ～ L3）: Nexus 7010、5020、Cat 6506e
- サービス（L4 ～ L7）: ASA 5540、IPS 4215
- SAN：MDS 9140、Hitachi USP VM
- ブレード サーバ：Fujitsu PRIMERGY BX600 S3
- ブレード スイッチ：Cisco BS3040

なお、この次にリリース予定のテストでは、クライアントとサーバ間のトラフィックを最適化する仕組みとして WAAS、サーバのロード バランスを提供する ACE が追加されます。

図 1-1　相互運用性テスト トポロジ



相互運用性テストの設定で、MS Exchange トラフィックはクライアント ホストから生成されます。このクライアント ホストはサービス スイッチに接続されます。データセンターのスイッチである Nexus 7010 は、コアおよび集約レイヤ デバイスとして動作します。すべてのサービス アプライアンス（ASA 5540、IPS 4215）は、サービス スイッチ（Catalyst 6506E）に接続されます。このサービス スイッチは集約スイッチに接続されます。

アクセス レイヤでは、Cisco ブレード スイッチ（CBS3040）を介してブレード サーバ（Fujitsu PRIMERGY BX600）に接続する Nexus 5020 スイッチが展開されます。

FC トラフィックは、Fujitsu ブレード サーバから、Cisco Multidirector スイッチ（MDS 9140）を介してストレージ（Hitachi USP VM）に送信されます。

使用されるオペレーティング システムおよびソフトウェアのバージョン

カテゴリ	デバイス モデル	オペレーティング システムまたはソフトウェア	バージョン
IP インフラストラクチャ	Nexus 7010	NX-OS	4.2(3)
	Nexus 5020	NX-OS	4.1(3)N2(1a)
サービス	Cat6506e	Cisco IOS	12.2(17r)SX5
	ASA5540	ASA	8.0(4)
	IPS 4215	IPS	6.0(1)E1
ブレード スイッチ	CBS3040	Cisco IOS	IPBASE-M (12.2(44)SE2)
ブレード サーバ	Fujitsu BX620-S5	Windows	Windows Server 2008 SP2 Enterprise Edition
FC スイッチ	MDS 9140	NX-OS	3.3.4a
ストレージ	Hitachi USP VM	Windows	Windows Vista Business SP1
クライアント		Windows	XP（SP2）
アプリケーション		MS Exchange	2007 SP1

CHAPTER 2

Japan Virtualization System and Interoperability Lab（J-VSL）の概要

Japan Virtualization System and Interoperability Lab（J-VSL）のコンポーネントには、「はじめに」の章で一覧にしたテストが含まれます。ここでは、各テクノロジーの範囲と関連するトポロジの詳細について概要を説明します。IP インフラストラクチャ、レイヤ 4 ～ 7、ストレージ エリア ネットワーキング、アプリケーション、およびブレード サーバ テクノロジーについて、この章の各項で説明します。

- 「IP インフラストラクチャの概要」
- 「レイヤ 4 ～ 7 サービスの概要」
- 「Storage Area Networking（SAN）の概要」
- 「アプリケーションの概要」
- 「ブレード サーバの概要」

IP インフラストラクチャの概要

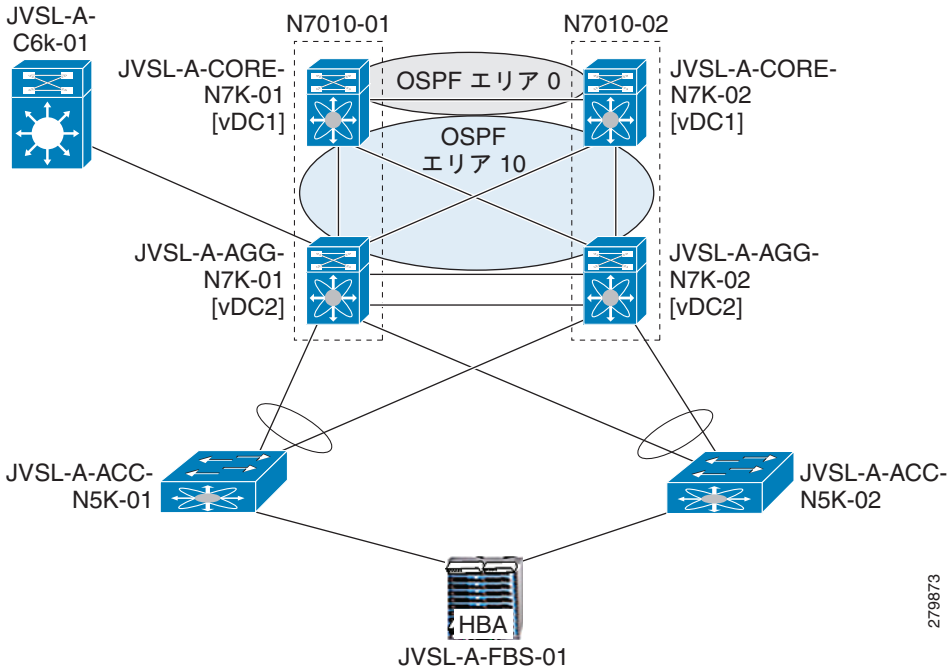
データセンターの IP インフラストラクチャ トポロジは、2 つの Nexus 7010、2 つの 5020、および 1 つの Cat6506e スイッチで構成されます。IP インフラストラクチャ トポロジは次に示す 3 つの論理レイヤに分割され、表 2-1 に示す IP インフラストラクチャ サービスを提供します。

- コア
- 集約
- アクセス レイヤ

表 2-1　論理レイヤ サービス

論理レイヤ	サービス
コア	VDC、OSPF、L3 ポート チャネル
集約	vPC、HSRP、OSPF、Rapid PVST+ Spanning-Tree、802.1Q Trunking、L2 ポート チャネル、VRF
アクセス	RPVST+ スパニングツリー、802.1Q トランキング

図 2-1　IP インフラストラクチャ トポロジ



相互運用性テスト トポロジ IP インフラストラクチャは、Nexus 7000、5000、およびスイッチング プラットフォームを中心に構築されます。

Cisco Nexus 7000 シリーズ

Cisco Nexus 7000 シリーズは、10 GB イーサネットおよび統合ファブリックをデータセンターに導入するために設計されたモジュラ スイッチング システムです。このシステムは、主にデータセンターのコア レイヤおよび集約レイヤのために設計され、ハイ アベイラビリティと高パフォーマンス（40/100 GE 対応）を提供します。

Cisco Nexus 5000 シリーズ

Cisco Nexus 5000 シリーズ スイッチは、主にアクセス レイヤのために設計され、データセンター アプリケーションのために、ライン レート、低遅延、損失のない 10 GB イーサネットおよび Fibre Channel over Ethernet（FCoE）スイッチのファミリを構成しています。また、このプラットフォームは、個別の LAN、SAN、およびサーバ クラスタ ネットワーク環境を 1 つの統合ファブリックに統合しています。

Cisco Catalyst 6500 シリーズ

Cisco Catalyst 6500 は、あらゆるお客様のネットワーク配置に適した幅広いライン カードをサポートするモジュラ シャーシ ファミリです。Cisco Catalyst 6500 のパフォーマンスは最大 400 Mbps まで拡張でき、現在の市場で最高クラスのパフォーマンスを持つスイッチ製品の 1 つです。シャーシは、3 ～ 13 スロットという幅広いシャーシ オプションをサポートしています。すべてのシャーシは、冗長電源だけでなく冗長スーパーバイザ エンジンをサポートしています。

Cisco Nexus-OS

NX-OS は Nexus プラットフォームで使用されます。Nexus プラットフォームは、モジュール性、復元力、およびサービサビリティを想定して設計されています。

NX-OS の機能

NX-OS ソフトウェアは、Virtual Device Context（VDC）をサポートしています。VDC はデバイス自体の仮想化に使用され、物理スイッチを複数の論理デバイスとして示します。相互運用性テスト トポロジでは、2 つの Nexus スイッチおよび 2 つの VDC（JVSL-A-CORE-N7k-01 と JVSL-A-AGG-N7k-01）が両方のスイッチで作成されます。

レイヤ 3 の仮想化サポートは、Virtual Route Forwarding（VRF）インスタンスの概念を使用してサポートされます。VRF は、レイヤ 3 のフォワーディングおよびルーティング テーブルの仮想化に使用されます。相互運用性テスト トポロジでは、VRF は集約スイッチに作成されます。ポート チャネルは、リンク帯域幅の集約に使用されます。レイヤ 2 およびレイヤ 3 ポート チャネルが 相互運用性テスト トポロジで使用され、スタティックな「オン」またはアクティブ モードで設定されます。

virtual Port Channel（vPC）を使用すると、2 つの異なる Nexus スイッチに物理的に接続するリンクは、その他のデバイスから単一のポート チャネルに見えるようになります。vPC によってレイヤ 2 のマルチパス処理を実行でき、ユーザは帯域幅を増やすことで冗長性を構築できるようになります。相互運用性テスト トポロジでは、vPC は集約スイッチに設定されます。

Spanning Tree Protocol（STP; スパニング ツリー プロトコル）を使用すると、レイヤ 2 で物理パスを冗長化できます。相互運用性テスト トポロジで使用する STP は Rapid PVST+ です。

トランクとは、1 つ以上のスイッチ ポートと別のネットワーキング デバイス（ルータやスイッチなど）間のポートとポートのリンクです。トランクは、単一のリンク上で複数の VLAN のトラフィックを伝送します。トランクのカプセル化は、ダイナミックにネゴシエートされるか、スタティックに設定されます。相互運用性テスト テスト トポロジでは、カプセル化はスタティックに 802.1Q に設定されています。

レイヤ 4 ～ 7 サービスの概要

相互運用性テスト テスト トポロジの一部として採用されているレイヤ 4 ～ 7 サービスがいくつかあります。たとえば、ファイアウォール処理、侵入検知、防御などです。表 2-2 に、このトポロジで使用されているレイヤ 4 ～ 7 サービスとシスコ製品ラインを示します。

表 2-2　相互運用性テストで使用されるレイヤ 4 ～ 7 ソリューション

レイヤ 4 ～ 7 サービス	J-VSL ソリューション
ファイアウォール処理	ASA
侵入防御または侵入検知	IPS

このリストのシスコ製品の一部は、サービス アプライアンスです。

- ASA：Adaptive Security Appliance（適応型セキュリティ アプライアンス）
- IPS：Intrusion Detection Services Module（侵入検知サービス モジュール）

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスは専用ソリューションであり、国際クラスのファイアウォール、ユニファイド コミュニケーション セキュリティ、VPN、Intrusion Prevention（IPS; 侵入防御）、およびセキュリティ サービスを 1 つのプラットフォームに統合しています。このシリーズは、Cisco PIX® 500 シリーズ セキュリティ アプライアンス、Cisco IPS 4200 シリーズ センサー、および Cisco VPN 3000 シリーズ コンセントレータなどの定評のあるテクノロジーに基づいています。

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスは、シスコの自己防御型ネットワークの主要コンポーネントです。Cisco ASA 5500 シリーズは、ネットワーク境界、コントロール ネットワーク、およびアプリケーション アクティビティに侵入する前に攻撃を停止する高度な脅威防御機能を備え、安全なリモート アクセスとサイト間の接続を提供します。そのため、このシリーズは強力で多機能なネットワーク セキュリティ アプライアンス ファミリであり、あらゆる規模の企業ネットワークを保護できるセキュリティの幅、正確さ、および深さを備えています。さらに、総合的なマルチレイヤ セキュリティの実装に関連する全体の導入コストと運用コストを削減できます。

Cisco IPS

セキュリティ上の脅威は複雑さを増しており、マルチギガビット環境と効率的なネットワーク侵入セキュリティ ソリューションは、高レベルの保護を維持するために欠かせません。常に警戒を怠らない保護対策によってビジネスの継続性が確保され、コストのアップにつながる侵入の影響を最小限に抑えられます。シスコの統合的なネットワーク セキュリティ ソリューションによって、企業は社内に接続しているビジネス資産を保護するとともに、侵入防御システムの効率を向上できます。Cisco IPS は Cisco Systems® ファミリの侵入検知および侵入防御（IDS/IPS）ソリューションの一部であり、他の IDS または IPS コンポーネントと連携して動作することでデータ インフラストラクチャを効率的に保護します。

Cisco IPS は、幅広く導入されている Cisco Catalyst シャーシ用のサービス モジュールです。Cisco Catalyst シャーシは数百から数千単位でインストールされており、ファイアウォール、VPN、IDS サービス、IPS サービスなどの追加サービスに適した論理プラットフォームです。この第 2 世代サービス モジュールには、IDS または IPS 攻撃の保護機能を探しているお客様に固有の利点があります。

サービス スイッチの統合

サービス シャーシは、単一 IPS（4215）および ASA（5540）と接続する JVSL-A-C6k-01 です。ASA および IPS は、ファスト イーサネットを介して接続されます。サービス スイッチは、L3 リンクを介して集約レイヤ デバイス（JVSL-A-AGG-N7K-01）に接続されます。

サービス スイッチに送られるすべてのトラフィックは、ファイアウォール サービスのために ASA に配信されます。許可されたトラフィックは IPS に配信され、プロミスキャス モードで着信トラフィックは監視されます。

図 2-2　サービス スイッチの統合

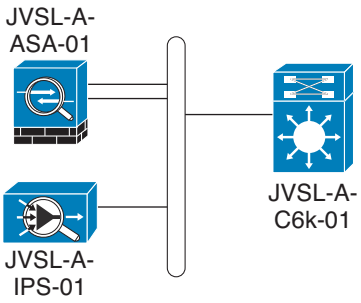
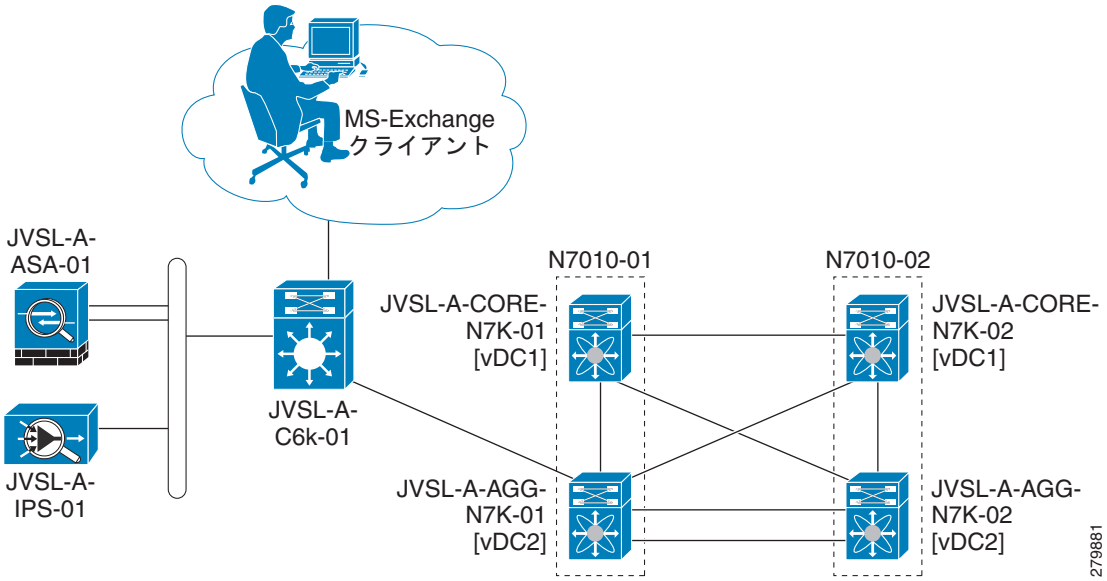


図 2-3　サービス スイッチの構成



サービス シャーシ モデル（Cat6506e）

相互運用性テスト トポロジでは、1 つの Catalyst 6500 スイッチ（JVSL-A-C6k-01）がサービス アプライアンスを格納するために配置されています。サービス スイッチに接続されたアプライアンス（ASA、IPS）は、データセンター トラフィックに対してレイヤ 4 ～ 7 のサービスを提供します。

サービス シャーシは Catalyst 6506e であり、1 つのスロットが Supervisor 720 に使用され、別のスロットが 10 GB イーサネット モジュール（WS-X6704-10GE）に使用されて集約レイヤ スイッチと接続できるようにしています。

L4 ～ L7 サービスの実装

ASA の動作モードは、ルーテッドとトランスペアレントの 2 種類です。テスト トポロジの ASA は、ルーテッド モードで動作するように設定されています。ルーテッド モードでは、ファイアウォールは、VLAN 外部から VLAN 内部およびその反対方向のトラフィックをルーティングします。相互運用性テスト トポロジでは、VLAN 外は VLAN 20 であり、VLAN 内は 30 です。クライアントのトラフィック定義は、内部の VLAN 30 上の実サーバであり、VLAN 20 にある外部からファイアウォールをヒットします。反対方向で、反対方向の処理が実行されます。

IPS はプロミスキャス モードで配置され、サービス スイッチはパケットのコピーを IPS と集約スイッチに送信します。

トラフィックのリダイレクション方法

- MS Exchange クライアントは、アプリケーション サーバに対して要求（REQ）を送信します。
- Cat6k はクライアント要求（REQ）を傍受し、FW サービスのために ASA にリダイレクトします。
- Cat6k は FW から許可されたトラフィックを受信し、パケット検査のためにパケットのコピーを IPS に送信します。
- 同時に、要求されたトラフィックは集約スイッチ JVSL-A-AGG-N7K-01 に渡されます。アクセス スイッチ JVSL-A-ACC-N5K-01 は REQ をサーバに転送します。
- サーバはクライアント要求（REQ）に対する応答（RES）を送信します。
- JVSL-A-ACC-N5K-01 はサーバから応答（RES）を受信し、集約スイッチに転送します。
- 集約スイッチは、トラフィック方向の Cat6K にトラフィックを転送します。
- クライアントは応答（RES）を受信します。

Storage Area Networking（SAN）の概要

相互運用性テスト トポロジの SAN 設計では、単一の物理 FC スイッチを使用しています。このスイッチは、コラプスド コア設計として実装されます。概念上、これはコア設計またはエッジ設計であり、単一の物理スイッチに統合されたコア ポート（非オーバーサブスクライブ）とエッジ ポート（オーバーサブスクライブ）を利用します。従来の Cisco MDS 9000 ファミリ スイッチのコラプスド コア設計では、非オーバーサブスクライブ（ストレージ）ポートとオーバーサブスクライブ（ホスト最適化）ポートの両方が使用されています。

相互運用性テスト SAN トポロジでは、Cisco MDS、業界のベスト プラクティス、およびストレージ ベンダーの実装ガイドラインを組み込み、一般的なエンタープライズ データセンター環境を代表する SAN インフラストラクチャを提供しています。トポロジには次のコンポーネントが含まれます。

- 「Cisco MDS 9140」
- 「Hitachi USP VM」

Cisco MDS 9140

Cisco MDS 9140 は、Cisco Intelligent Networking を小中規模の SAN とデータセンターのエッジ アプリケーションまで対応することで、ファイバ チャネル ファブリック スイッチの標準を高めています。Cisco MDS 9140 は、コンパクトな 1-RU フォーム ファクタにコスト、パフォーマンス、およびエンタープライズ クラスの機能を最適なバランスで組み込んでいます。Cisco MDS 9140 は、幅広いストレージ環境に必要なポート密度を提供します。クラス有数のスケーラビリティ、アベイラビリティ、セキュリティ、および管理機能を備えているため、低い TCO で高パフォーマンスの SAN を導入できます。

Cisco MDS 9140 は、小型の効率的なプロファイル スイッチング プラットフォームに豊富な機能を備えた製品で、小中規模のストレージ環境のコスト、パフォーマンス、管理の容易さ、および接続に関する要件に対応できます。

SAN トポロジには、次の仕様を持つ単一の MDS 9140 スイッチがあります。

- ポート速度：1/2 GB の自動検知（オプションで設定可能）。
- バッファ クレジット：1 つのポート（ターゲット最適化ポート）あたり最大 255。1 つのポート（ホスト最適化ポート）あたり 12
- 1 つのシャーシあたりのポート：40
- ポートの設定：32 ホスト最適化ポート、8 ターゲット最適化ポート
- ポート チャネル：最大 15 ポート

Hitachi USP VM

Hitachi Universal Storage Platform™ VM では小さな占有スペースでエンタープライズ クラスの機能を使用できるため、エントリ レベルの企業および急速に成長する中堅企業のビジネス ニーズを満たすと同時に、大企業の分散アプリケーションや部門別アプリケーションをサポートできます。

Hitachi Services Oriented Storage Solutions アーキテクチャの統合コンポーネントは Universal Storage Platform VM であり、さまざまなクラスのストレージをアプリケーション要件に合致させるための基礎となります。Hitachi Universal Storage Platform VM パッケージは、次のように重要なサービスを提供します。

- Hitachi および他のベンダーのストレージを 1 つのプールに仮想化。
- 中断なしでボリュームを拡張するための、Hitachi Dynamic Provisioning によるシン プロビジョニング。
- セキュリティ サービス、ビジネス継続サービス、およびコンテンツ管理サービス。
- アプリケーションのパフォーマンスを改善するロード バランス。
- Hitachi および他のストレージ システムからの中断のないダイナミック データ マイグレーション。

SAN の概要

相互運用性テスト SAN トポロジには、Hitachi（モデル USP VM）の FC ストレージ フレームがあります。Hitachi ストレージ フレームには、データセンターのプライマリ アプリケーション アクセスのためのデバイスが用意されています。

相互運用性テスト トポロジでは、Windows Server 2008 オペレーティング システムが Fujitsu ブレード サーバにマウントされ、4 GB Emulex によって 2 つの冗長パスがストレージ デバイスに提供されます。ホスト（Fujitsu）は Hitachi ストレージに接続され、ストレージは Windows OS の MPIO を使用します。ストレージ テストの大部分は、Windows の IOMeter で生成される I/O に基づいています。

図 2-4　　SAN テスト トポロジの概要

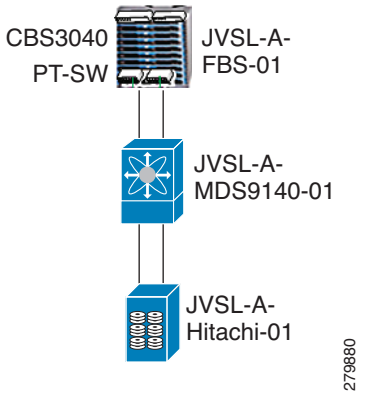


図 2-4 に、SAN トポロジ全体を示します。この図には、MDS スイッチとエンド デバイスが含まれます。

FC ファブリックは、Cisco VSAN テクノロジーを使用して実装されます。エンド デバイスにはホストとストレージ アレイが含まれます。

ホスト サーバ : ホスト サーバには、4 つのブレード サーバを搭載する Fujitsu が含まれます。この 4 つのサーバのうちの 3 つに、MS Exchange アプリケーションがインストールされます。ホスト サーバは Windows 2008 Enterprise Edition を実行し、2 つの冗長パスをストレージ デバイスに提供する 4 GB Emulex HBA があります。

ストレージ アレイ : ストレージ アレイには、SAN スイッチ接続のために 16 個の 300 GB FC ディスク ドライブと 8 個の 4 GB FC ポートを搭載した Hitachi USP VM が含まれます。

アプリケーションの概要

相互運用性テストでは、MS Windows Server 2008 Enterprise Edition Service Pack 2（英語バージョンおよび日本語バージョン）上で MS Exchange 2007 Server Enterprise Edition SP1 アプリケーションを使用しています。相互運用性テストでは、テスト トポロジでメールボックスのハイ アベイラビリティを実現するために、Exchange 2007 シングル コピー クラスタが実装されています。このアプリケーション トポロジでは、Exchange アプリケーションのために Fujitsu PRIMERGY BX600 S3 Blade Center を使用します。テストには、データセンターのデバイス（Nexus スイッチ、ブレード サーバ、ストレージなど）の接続、ブレード サーバでの Exchange アプリケーションの保持、およびクライアントからサーバへのトラフィックの転送が含まれます。

MS Exchange の概要

Microsoft Exchange Server は、Microsoft 社が開発したクライアント サーバのコラボレーション アプリケーション製品のサーバ側です。Microsoft Exchange Server はサーバ製品の Microsoft Server シリーズの一部であり、Microsoft インフラストラクチャ ソリューションを使用する企業に使用されます。MS Exchange の主な機能を次に示します。

- 電子メール
- カレンダー
- 通信とタスク
- モバイルおよび Web ベースによる情報アクセスのサポート
- データ ストレージのサポート

Microsoft Exchange Server 2007 は、これらの課題に対処し、メッセージング システムに関係するユーザのニーズに対応するために設計されています。Microsoft Exchange Server 2007 の新機能では、高度な保護ニーズと任意の場所にアクセスできる機能に対応しています。新機能は次の機能によって容易になります。

- アンチスパムおよびアンチウィルス
- ビジネスの継続性
- 機密のメッセージング、ユニファイド メッセージング、Web ベースのメッセージング、およびモバイル メッセージング
- コラボレーションと生産性
- パフォーマンス、スケーラビリティ、導入、管理、拡張性などの運用上の効率

MS Exchange 2007 の主な機能

- 保護：アンチスパム、アンチウィルス、準拠性、データ レプリケーションによるクラスタリング、改善されたセキュリティ、および暗号化。
- 改善された情報ワーカー アクセス：改善されたカレンダー、ユニファイド メッセージング、モビリティ、および Web アクセス。
- 改善された IT エクスペリエンス：64 ビットのパフォーマンスとスケーラビリティ、コマンドライン シェルおよび簡易な GUI、改善された導入、ロールの分割、および簡易なルーティング。
- Exchange Management Shell：システム管理向けの新しいコマンドライン シェルおよびスクリプティング言語（Windows Power Shell に基づきます）。
- ユニファイド メッセージング：ユニファイド メッセージングを使用すると、音声メール、電子メール、Fax をメールボックスで受信し、携帯電話や他の無線デバイスからメールボックスにアクセスできます。データベースの最大サイズ制限の増加。データベース サイズは、1 つのデータベースにつき最大 16 TB になりました。
- ストレージ グループの最大数の増加。
- Outlook は、クライアントに Microsoft Exchange Server 2007 の外部アクセスを提供するために設定されます。Microsoft Office Outlook 2007 のユーザ プロファイルは、自動検出サービスを設定して Exchange 2007 に接続するように自動的に設定されます。また、Outlook は、アベイラビリティ サービスやオフラインのアドレス帳などの Exchange サービスに対する外部アクセスも用意しています。

Exchange Load Generator

Microsoft Exchange Load Generator は、Exchange クライアントのトラフィックをシミュレートするツールです。このツールは、継続的な Exchange クライアント トラフィックを Exchange Server に送信するトポロジで使用されます。相互運用性テストでは、Load Generator は 2 人のユーザをシミュレートし、15 分間、ストレス モードでトラフィックを送信するように設定されます。

ブレード サーバの概要

相互運用性テスト トポロジでは、Fijutsu PRIMERGY BX600 S3 を使用して、テスト用の MS Exchange 2007 アプリケーションを配置します。

ブレード サーバは、物理空間とエネルギーの使用を最小限に抑えるために最適化されたモジュール式設計の軽量な装備のサーバ コンピュータです。複数のサーバを格納できるブレード ラックは、電気による冷却、ネットワーキング、多様な相互接続、管理などのサービスを提供します。ブレード自体に（ときにはラックに）格納する内容に関する原則はブレードのプロバイダーによって異なりますが、ブレードとブレード ラックの両方でブレード システムが構築されます。

Fujitsu PRIMERGY BX600

Fujitsu PRIMERGY BX600 にはサーバ、ネットワーク管理、およびストレージのインフラストラクチャが一式そろっており、モジュール式設計に統合されています。また、ビジネス データセンターに欠かせないサービスを提供するように構築されています。Fujitsu PRIMERGY BX600 S3 Blade Center は、業界標準の 19 インチ ラックへの取り付けに適した非常にコンパクトかつ省電力でスケーラブルなサーバ システムです。BX600 S3 のベース ユニットでは、ラックに 7 個の高いユニットを使用しており、最大 10 個の（モデルとバージョンが異なる）サーバ ブレードを格納できます。PRIMERGY BX600 S3 Blade Center は幅広いプロセッサ構成を使用できるため、多くの要件を満たしており、データセンター アプリケーションに使用されています。高度に開発されたハードウェアとソフトウェア コンポーネントによって、PRIMERGY BX600 S3 Blade Center はトップ クラスの信頼性とアベイラビリティを実現しています。これには、ホット スワップ サーバ ブレード、イーサネットおよびファイバ チャネル接続ブレード、管理ブレード、ホット スワップ電源ユニット、ファン モジュールが含まれます。

ネットワーク LAN 接続の場合、Cisco Catalyst Blade Switch 3040 が使用されます。Fujitsu PRIMERGY Blade System ユーザ向けの Cisco Catalyst Blade Switch 3040 は、ケーブルの複雑さを大幅に軽減する統合スイッチング ソリューションです。このソリューションは、ハイ アベイラビリティ、Quality Of Service、セキュリティなどの一貫したネットワーク サービスを提供します。

Fujitsu PRIMERGY BX600 には、ブレード システムをリモート管理する integrated Remote Management Controller（iRMC）があります。各ブレードには、管理サブネットに属する IP アドレスを持つ iRMC インターフェイスがあります。

Cisco ブレード スイッチ 3040

Fujitsu Siemens Computer（FSC）PRIMERGY Advanced Blade Ecosystem 向け Cisco Catalyst Blade Switch 3040 は、シスコのインフラストラクチャ サービスをサーバのエッジまで拡張し、既存のネットワーク投資を使用して運用コストを削減する統合スイッチです。

Cisco Catalyst Blade Switch 3040 は、10 個の内部 1000BASE ポートが PRIMERGY シャーシ バックプレーンを介してサーバに接続し、4 つの外部 10/100/1000 SFP ベースと 2 つの外部 10/100/1000BASE-T ポートが外部スイッチに接続されています。

スイッチの運用上の利点を次に示します。

- ケーブルの複雑さが大幅に軽減され、サーバと統合スイッチ間をケーブルで接続する必要がなくなります。
- 従来のサーバ ラックよりも高密度な状態で統合スイッチをシャーシ内に配置できるため、空間の要件を軽減できます。
- Cisco IOS ソフトウェアのセキュリティ機能を統合することで、アセットを保護できます。
- 共通のネットワーク サービスをサーバ エッジに統合するプラットフォームを提供することで、運用効率を強化できます。

CHAPTER 3

IP インフラストラクチャ

IP インフラストラクチャのテストは、Nexus 7010 および 5020 デバイスでの L2 および L3 プロトコルの設定およびトラフィック フローに重点を置いています。この項で使用される L2 プロトコルは、vPC、STP、および L2 ポート チャネルです。この項で使用される L3 プロトコルは、HSRP、OSPF、VRF、および L3 ポートチャネルです。

ここで説明する内容は、次のとおりです。

- 「設定および確認」
- 「ハイ アベイラビリティ - リンク障害」
- 「ハイ アベイラビリティ - デバイス障害」

設定および確認

ここで説明する内容は、次のとおりです。

- 「Nexus 7010 デバイスでの VDC 機能の設定および確認」
- 「Nexus 7010、5020、および Cat 6506e デバイス間の L2 ポート チャネルの設定および確認」
- 「Nexus 7010 デバイス間の L3 ポート チャネルの設定および確認」
- 「Nexus 7010 および Cat6506e 間の LACP プロトコルによる L2 ポート チャネルの設定および確認」
- 「Nexus 7010 および Nexus 5020 デバイス間の LACP プロトコルによる L2 ポート チャネルの設定および確認」
- 「Nexus 7010 デバイス間の LACP プロトコルによる L3 ポート チャネルの設定および確認」
- 「Nexus 7010 デバイスでの vPC の設定および確認」
- 「Nexus 7010 デバイスでの HSRP の設定および確認」
- 「Nexus 7010 デバイスでの VRF 機能の設定および確認」
- 「Nexus 7010 デバイスでの OSPF プロトコルの設定および確認」
- 「集約スイッチ（Nexus 7010）での STP 設定の確認」
- 「集約スイッチ（Nexus 7010）、アクセス スイッチ（Nexus 5020）、およびサービス スイッチ（Cat 6506e）での VLAN 設定の確認」

Nexus 7010 デバイスでの VDC 機能の設定および確認

VDC（Virtual Device Context）を設定し、VDC の機能を確認するテストを行います。

テストの設定

Nexus 7010 スイッチが、Advanced Services パッケージ ライセンスでインストールされています。

テスト手順

Nexus 7010 デバイスでの VDC 設定の確認テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　ネットワーク管理者ロールを持つユーザ名でデフォルトの VDC にログインし、`show vdc detail` コマンドを使用して VDC の詳細を確認します。

ステップ 3　`switch (config) #vdc JVSL-A-CORE-N7K-01` コマンドを使用して、コア レイヤについて JVSL-A-CORE-N7K-01 という名前の VDC を作成します。

ステップ 4　`switch (config) #vdc JVSL-A-AGG-N7K-01` コマンドを使用して、集約レイヤについて JVSL-A-AGG-N7K-01 という名前の VDC を作成します。

ステップ 5　`show vdc` コマンドを使用して、VDC の状態を確認します。

ステップ 6　次のコマンドを使用して、物理インターフェイスを Core および Aggregation VDC（JVSL-A-CORE-N7K-01 と JVSL-A-AGG-N7K-01）に割り当てます。
`switch(config-vdc)# allocate interface ethernet X/X-X`

ステップ 7　JVSL-A-CORE-N7K-01 で `show vdc membership` コマンドを使用して VDC メンバーを確認します。`switch to vdc JVSL-A-AGG-N7K-01` コマンドを使用して JVSL-A-AGG-N7K-01 VDC に切り替え、メンバーを確認します。

ステップ 8　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 9　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- VDC は動作しています。
- テスト時に CPU またはメモリに許容できない影響はありません。

結果

Nexus 7010 デバイスでの VDC 機能の設定および確認テストに合格しました。

Nexus 7010、5020、および Cat 6506e デバイス間の L2 ポート チャネルの設定および確認

このテストでは、集約スイッチおよびアクセス スイッチ間の L2 ポート チャネル設定を確認します。

テストの設定

集約スイッチ（JVSL-A-AGG-N7k-01 と JVSL-A-AGG-N7k-02）およびアクセス スイッチ（JVSL-A-ACC-N5K-01 と JVSL-A-ACC-N5K-02）が、光ファイバ ケーブルを使用して接続されています。サービス スイッチ（JVSL-A-C6k-01）の 10 GB インターフェイスが、光ファイバ ケーブルを使用して集約スイッチ（JVSL-A-AGG-N7K-01）に接続されています。

テスト手順

Nexus 7010、5020、および Cat 6506e デバイス間の L2 ポート チャネル設定テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　`switchport mode trunk` コマンドを使用して、集約スイッチ（JVSL-A-AGG-N7K-01 と JVSL-A-AGG-N7K-02）およびアクセス スイッチ（JVSL-A-ACC-N5K-01 と JVSL-A-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 3　`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 4　`switchport mode trunk` コマンドを使用して、JVSL-A-AGG-N7K-01 および JVSL-A-C6k-01 間のリンクをトランク ポートとして設定します。

ステップ 5　`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 6　集約スイッチ（JVSL-A-AGG-N7K-01 と JVSL-A-AGG-N7K-02）およびアクセス スイッチ（JVSL-A-ACC-N5K-01 と JVSL-A-ACC-N5K-02）で、トランク モードを使用して L2 ポート チャネルを作成します。

ステップ 7　`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 8　`Channel group xxx mode on` コマンドを使用して、物理インターフェイスに対して L2 ポート チャネル グループを割り当てます。

ステップ 9　集約スイッチ（JVSL-A-AGG-N7K-01）およびサービス スイッチ（JVSL-A-C6k-01）で、トランク モードを使用して L2 ポート チャネル インターフェイスを作成し、`Channel group xxx mode on` コマンドを使用して、物理インターフェイスに対して L2 ポート チャネル グループを割り当てます。

ステップ 10　`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。

ステップ 11　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 12　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がないことを確認します。

予測結果

次のテスト結果が予想されます。

- L2 ポート チャネルは動作しています。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

Nexus 7010、5020、および Cat 6506e デバイス間の L2 ポート チャネルの設定および確認テストに合格しました。

Nexus 7010 デバイス間の L3 ポート チャネルの設定および確認

このテストでは、コア スイッチと集約スイッチ間の L3 ポート チャネル設定を確認します。

テストの設定

コア スイッチ（JVSL-A-CORE-N7K-01 と N7K-02）および集約スイッチ（JVSL-A-AGG-N7K-01 と JVSL-A-AGG-N7K-02）インターフェイスが、光ファイバ ケーブルを使用して接続されています。

テスト手順

Nexus 7010 デバイス間の L3 ポート チャネルの設定および確認テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　コア スイッチ（JVSL-A-CORE-N7K-01 と JVSL-A-CORE-N7K-02）および集約スイッチ（JVSL-A-AGG-N7K-01 と JVSL-A-AGG-N7K-02）間のリンクのステータスを確認します。

ステップ 3　`interface port-channel xxx` コマンドを使用して、コア スイッチ（JVSL-A-CORE-N7K-01 と JVSL-A-CORE-N7K-02）および集約スイッチ（JVSL-A-AGG-N7K-01 と JVSL-A-AGG-N7K-02）で、IP アドレスを使用して L3 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 4　`channel-group` コマンドを使用して、物理インターフェイスに対して L3 ポート チャネル グループを割り当てます。

ステップ 5　`show port-channel summary` コマンドを使用して、L3 ポート チャネルのステータスを確認します。

ステップ 6　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 7　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がないことを確認します。

予測結果

次のテスト結果が予想されます。

- L3 ポート チャネルは動作しています。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

Nexus 7010 デバイス間の L3 ポート チャネルの設定および確認テストに合格しました。

Nexus 7010 および Cat6506e 間の LACP プロトコルによる L2 ポート チャネルの設定および確認

このテストでは、Nexus 7010 および cat6506e 間の LACP プロトコルによる L2 ポート チャネルを確認します。LACP プロトコルを使用してこのチャネルを形成する方法はいくつかあります。相互運用性テスト トポロジに使用されるチャネルは、LACP アクティブ モードを使用して設定します。このモードでは、ポートから LACP パケットを送信して他のポートとのネゴシエーションを開始します。このテストでは、集約スイッチ（JVSL-A-AGG-N7K-01）およびサービス スイッチ（JVSL-A-C6K-01）間でチャネルが適切に形成されていることを確認します。

テストの設定

サービス スイッチ（Cat6506e）10 GB インターフェイスが、光ファイバ ケーブルを使用して集約スイッチ（JVSL-A-AGG-N7K01）に接続されています。

テスト手順

Nexus 7010 および Cat6506e 間の LACP プロトコルによる L2 ポート チャネルの設定および確認テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　`show features` コマンドを使用して、LACP 機能が集約スイッチ（JVSL-A-AGG-N7k-01）でイネーブルであることを確認します。イネーブルではない場合、`feature lacp` コマンドを使用して LACP プロトコルをイネーブルにします。

ステップ 3　次のコマンドを使用して、集約スイッチ（JVSL-A-AGG-N7k-01）で L2 PortChannel を作成します。

```
interface port-channel 176
switchport
switchport mode trunk
```

LACP プロトコルを使用して、集約スイッチ（JVSL-A-AGG-N7k-01）のイーサネット 1/23 およびイーサネット 7/23 をまとめてバンドルし、ポート チャネル 176 を形成します。複数のインターフェイスをポート チャネルにバンドルするため、各インターフェイスの次の行を設定します。

```
channel-group 176 mode active
```

ステップ 4　次のコマンドを使用して、サービス スイッチ（JVSL-A-C6k-01）で L2 PortChannel を作成します。

```
interface Port-channel67
description L2_PC_TO_AGG_N7K_01
switchport
switchport trunk encapsulation dot1q
switchport mode trunk
```

LACP プロトコルを使用して、サービス スイッチ（JVSL-A-C6k-01）の 10 ギガビット イーサネット 2/2 およびイーサネット 2/3 をまとめてバンドルし、ポート チャネル 67 を形成します。複数のインターフェイスをポート チャネルにバンドルするため、各インターフェイスの次の行を設定します。

```
channel-group 67 mode active
```

ステップ 5　次のコマンドを使用して、集約スイッチ（JVSL-A-AGG-N7k-01）のポート チャネルのステータスを確認します。

```
show portchannel summary
```

ステップ 6　次のコマンドを使用して、サービス スイッチ（JVSL-A-C6k-01）のポート チャネルのステータスを確認します。

```
show etherchannel summary
```

ステップ 7　`show interfaces Port-channel 67 ether channel` コマンドをサービス スイッチで使用して、インターフェイス Te2/2 および Te2/3 の両方がバンドルされ、ポート チャネルでアクティブであることを確認します。

ステップ 8　`show port-channel database interface port-channel X176` および `sh lacp interface ethernet x/x` コマンドを集約スイッチ（JVSL-A-AGG-N7k-01）で使用して、インターフェイスがバンドルされ、ポート チャネルでアクティブであることを確認します。

ステップ 9　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 10　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がないことを確認します。

予測結果

次のテスト結果が予想されます。

- LACP によるチャネルが適切に構築されます。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

Nexus 7010 および Cat6506e 間の LACP プロトコルによる L2 ポート チャネルの設定および確認テストに失敗しました。障害番号は CSCtg47483 です。

Nexus 7010 および Nexus 5020 デバイス間の LACP プロトコルによる L2 ポート チャネルの設定および確認

このテストでは、集約スイッチ（Nexus 7010）およびアクセス スイッチ（Nexus 5020）間に、LACP プロトコルを使用するポート チャネルが適切に形成されていることを確認します。テスト中は、CPU およびメモリの使用率の安定性が監視されます。

テストの設定

集約スイッチとアクセス スイッチが、冗長ポートで相互接続されています。JVSL-A-AGG-N7k-01、JVSL-A-AGG-N7k-02、JVSL-A-ACC-N5K-01、および JVSL-A-ACC-N5K-02 スイッチ インターフェイス、10 ギガビット イーサネット x/x および 10 ギガビット イーサネット x/x がまとめてバンドルされ、ポート チャネルを形成します。

テスト手順

Nexus 7010 および Nexus 5020 デバイス間の LACP プロトコルによる L2 PortChannel の設定および確認テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　`show features` コマンドを使用して、LACP 機能が集約スイッチおよびアクセス スイッチでイネーブルであることを確認します。イネーブルではない場合、`feature lacp` コマンドを使用して LACP プロトコルをイネーブルにします。

ステップ 3　`show running-config interface` コマンドを各インターフェイスで使用して、ポート チャネルが設定されていることを確認します。

ステップ 4　次のコマンドを使用して、LACP プロトコルによる集約スイッチ（JVSL-A-AGG-N7k-01 と JVSL-A-AGG-N7k-02）およびアクセス スイッチ（JVSL-A-ACC-N5K-01 と JVSL-A-ACC-N5K-02）間で L2 ポート チャネルを設定します。

```
interface port-channel201
switchport
```

ステップ 5　複数のインターフェイスをポート チャネルにバンドルするため、各インターフェイスの次の行を設定します。`channel-group 201 mode active`

ステップ 6　`sh port-channel database interface port-channel XXX` および `sh lacp interface ethernet x/x` コマンドを集約スイッチとアクセス スイッチで使用して、インターフェイスがバンドルされ、ポート チャネルでアクティブであることを確認します。

ステップ 7　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 8　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がないことを確認します。

予測結果

次のテスト結果が予想されます。

- LACP によるチャネルが適切に構築されます。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

Nexus 7010 および Nexus 5020 デバイス間の LACP プロトコルによる L2 PortChannel の設定および確認テストに失敗しました。障害 ID は CSCtg47483 です。

Nexus 7010 デバイス間の LACP プロトコルによる L3 ポート チャネルの設定および確認

このテストでは、コア スイッチ（Nexus 7010）および集約スイッチ（Nexus 7010）間で、LACP プロトコルを使用するポート チャネルが適切に形成されていることを確認します。テスト中は、CPU およびメモリの使用率の安定性が監視されます。

テストの設定

コア スイッチおよび集約スイッチの複数のポートが、光ファイバ ケーブルを使用して相互接続されています。JVSL-A-CORE-N7k-01、JVSL-A-CORE-N7k-02、JVSL-A-AGG-N7k-01、および JVSL-A-AGG-N7k-02 スイッチ インターフェイス、10 ギガビット イーサネット x/x および 10 ギガビット イーサネット x/x がバンドルされ、ポート チャネルを形成します。

テスト手順

Nexus 7010 デバイス間の LACP プロトコルによる L3 ポート チャネルの設定および確認テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　`show features` コマンドを使用して、LACP 機能が集約スイッチおよびアクセス スイッチでイネーブルであることを確認します。イネーブルではない場合、`feature lacp` コマンドを使用して LACP プロトコルをイネーブルにします。

ステップ 3　`show running-config interface` コマンドを各インターフェイスで使用して、ポート チャネルが設定されていることを確認します。

ステップ 4　次のコマンドを使用して、LACP プロトコルによってコア スイッチ（JVSL-A-CORE-N7k-01 と JVSL-A-CORE-N7k-02）および集約スイッチ（JVSL-A-AGG-N7k-01 と JVSL-A-AGG-N7k-02）間に L3 ポート チャネルを設定します。

```
interface port-channel301
ip address xx.xx.xx.xx/xx
```

ステップ 5　`channel-group 301 mode active` コマンドを使用して、物理インターフェイスに対してポート チャネルを割り当てます。

ステップ 6　`show port-channel database interface port-channel XXX` および `show lacp interface ethernet x/x` コマンドをコア スイッチ（JVSL-A-CORE-N7k-01 と JVSL-A-CORE-N7k-02）および集約スイッチ（JVSL-A-AGG-N7k-01 と JVSL-A-AGG-N7k-02）で使用して、インターフェイスがバンドルされ、ポート チャネルでアクティブであることを確認します。

ステップ 7　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 8　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がないことを確認します。

予測結果

次のテスト結果が予想されます。

- LACP によるチャネルが適切に構築されます。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

Nexus 7010 デバイス間の LACP プロトコルによる L3 ポート チャネルの設定および確認テストに合格しました。

Nexus 7010 デバイスでの vPC の設定および確認

このテストでは、集約スイッチ（Nexus 7010 デバイス）の vPC 設定を確認します。

テストの設定

集約スイッチ（JVSL-A-AGG-N7K-01 と JVSL-A-AGG-N7K-02）およびアクセス スイッチ（JVSL-A-ACC-N5K-01 と JVSL-A-AGG-N5K-02）の間に複数のリンクが接続される必要があります。

テスト手順

Nexus 7010 デバイスでの vPC の設定および確認テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　`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について確認します。

ステップ 3　ロールのプライオリティが 5 の集約スイッチ JVSL-A-AGG-N7K-01 に vPC ドメイン 10 を作成し、スイッチを vPC プライマリにします。

ステップ 4　`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 5　ロールのプライオリティが 10 の集約スイッチ JVSL-A-AGG-N7K-02 に vPC ドメイン 10 を作成し、スイッチを vPC セカンダリにします。

ステップ 6　`sh vpc role` コマンドを使用して、vPC ロールを確認します。

vPC-peer-keepalive リンクの宛先および送信元 IP アドレスと、それらの VRF の

vPC-peer-keepalive を設定します。

```
switch(config-vpc-domain)# peer-keepalive destination 192.168.1.2 source 192.168.1.1 vrf
vpc
```

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 102
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 ステータスを確認します。

ステップ 10　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 11　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がないことを確認します。

予測結果

次のテスト結果が予想されます。

- vPC は動作しています。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

Nexus 7010 デバイスでの vPC の設定および確認テストに合格しました。

Nexus 7010 デバイスでの HSRP の設定および確認

このテストでは、集約スイッチ（JVSL-A-AGG-N7K-01 と JVSL-A-AGG-N7K-02）の HSRP 設定を確認します。

Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）は、特定のサブネットで冗長ゲートウェイ IP アドレスをクライアントに提供するために使用されます。相互運用性テスト トポロジでは、仮想 IP アドレス（ゲートウェイ）は JVSL-A-AGG-N7k-01 および JVSL-A-AGG-N7k-02 という 2 つのルータで共有されます。これら 2 つのルータは、それぞれ HSRP アクセスネットワークにつき 2 つの IP アドレスで設定します。1 つはそのルータに固有の IP アドレスで、もう 1 つはピア HSRP ルータと共有する IP アドレスです。HSRP プライオリティが高いルータはアクティブ状態を想定し、仮想 IP でのクエリーに応答します。もう一方のルータはスタンバイ状態を想定し、スタンバイ状態でこのようなクエリーを無視します。

テストの設定

2 つの集約スイッチが相互接続され、サーバはアクセス スイッチを介して集約スイッチに接続されています。

テスト手順

Nexus 7010 デバイスでの HSRP の設定および確認テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　`show feature` コマンドを使用して、HSRP 機能がイネーブルであることを確認します。イネーブルではない場合、`feature hsrp` コマンドを使用して HSRP 機能をイネーブルにします。

ステップ 3　VLAN 100 インターフェイスでプライオリティが 150 の HSRP グループ 100 を設定し、集約スイッチ 1（JVSL-A-AGG-N7K-01）で仮想 IP 172.16.100.1 を割り当てます。

ステップ 4　VLAN インターフェイスでプライオリティが 110 の HSRP グループ 100 を設定し、集約スイッチ 2（JVSL-A-AGG-N7K-02）で仮想 IP 172.16.100.1 を割り当てます。

ステップ 5　`show running-config interface Vlan100` コマンドを使用して、JVSL-A-AGG-N7K-01 および JVSL-A-AGG-N7K-02 の VLAN 100 に関する HSRP 設定を確認します。

ステップ 6　集約スイッチで `sh hsrp group 100` コマンドを実行し、アクティブおよびスタンバイの HSRP ルータ ステータスを確認します。

ステップ 7　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 8　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかったことを確認します。

予測結果

次の結果が予想されます。

- HSRP グループは、アクティブ状態およびスタンバイ状態の設定を反映します。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

Nexus 7010 デバイスでの HSRP の設定および確認テストに合格しました。

Nexus 7010 デバイスでの VRF 機能の設定および確認

このテストでは、集約スイッチの VRF 設定を確認します。

テストの設定

集約スイッチ（JVSL-A-AGG-N7K-01 および JVSL-A-AGG-N7K-02）が L3 リンクを介して接続されています。

テスト手順

Nexus 7010 デバイスでの VRF 機能の設定および確認テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　`show vrf detail` コマンドを使用して、VRF 設定を確認します。

ステップ 3　`vrf context vpc` コマンドを使用して、VPC という名前の新しい VRF を作成します。この VRF は `VPC keepalive packet sync` のためです。

ステップ 4　`vrf member vpc` コマンドを使用して、VRF VPC メンバー ポートを割り当てます。

ステップ 5　`sh vrf interface ethernet xx` コマンドを使用して、VRF メンバーの状態を確認します。

ステップ 6　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 7　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- VRF はアップ状態で、メンバーは相互に通信できます。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

Nexus 7010 デバイスでの VRF 機能の設定および確認テストに合格しました。

Nexus 7010 デバイスでの OSPF プロトコルの設定および確認

このテストでは、OSPF プロトコルの設定およびステータスを確認します。

テストの設定

コア スイッチ（JVSL-A-CORE-N7K-01 と JVSL-A-CORE-N7k-02）および集約スイッチ（JVSL-A-AGG-N7K-01 と JVSL-A-AGG-N7k-02）が相互接続される必要があります。

テスト手順

Nexus 7010 デバイスでの OSPF プロトコルの設定および確認テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　コア スイッチ（JVSL-A-CORE-N7K-01 と JVSL-A-CORE-N7K-02）間に L3 リンクを設定します。

ステップ 3　`ip router ospf 10 area 0.0.0.0` コマンドを使用して、コア スイッチ L3 リンクに OSPF エリア 0 を設定します。

ステップ 4　集約スイッチ L3 リンクに対するコア スイッチがアップ状態であることを確認し、すべての L3 リンクで OSPF エリア 10 を設定します。

ステップ 5　`show ip ospf neighbors` および `show ip ospf database` コマンドを使用して、OSPF ネイバーおよびデータベースを確認します。

ステップ 6　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 7　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- OSPF データベースには適切なルータが設定されます。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

Nexus 7010 デバイスでの OSPF プロトコルの設定および確認テストに合格しました。

集約スイッチ（Nexus 7010）での STP 設定の確認

このテストでは、集約スイッチの Spanning Tree Protocol（STP; スパニング ツリー プロトコル）設定を確認します。

テストの設定

すべての集約スイッチとアクセス スイッチが、光ファイバ ケーブルを使用して相互接続されています。また、ポートはアップ状態にあることが必要です。

テスト手順

集約スイッチ（Nexus 7010）での STP 設定の確認テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　`show running-configuration | include spanning-tree` コマンドを使用して、相互運用性テスト トポロジのすべてのレイヤ 2 デバイスのスパニングツリー設定を確認します。

ステップ 3　次のコマンドを使用して、集約スイッチ 1（JVSL-A-AGG-N7k-01）を STP ルートとして設定します。

```
spanning-tree mode rapid-pvst
spanning-tree vlan 1,10,100 priority 24576
```

ステップ 4　次のコマンドを使用して、集約スイッチ 2（JVSL-A-AGG-N7k-02）の STP を設定します。

```
spanning-tree mode rapid-pvst
spanning-tree vlan 1,10,100 priority 28672
```

ステップ 5　次のコマンドを使用して、集約スイッチおよびアクセス スイッチの STP 設定を確認します。

```
show spanning-tree root
show spanning-tree vlan
```

ステップ 6　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 7　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- スイッチは Rapid-PVST+ モードで動作し、vPC の障害時に STP が機能します。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

集約スイッチ（Nexus 7010）での STP 設定の確認テストに合格しました。

集約スイッチ（Nexus 7010）、アクセス スイッチ（Nexus 5020）、およびサービス スイッチ（Cat 6506e）での VLAN 設定の確認

このテストでは、集約スイッチ（Nexus 7010）、アクセス スイッチ（Nexus 5020）、およびサービス スイッチ（Cat 6506e）の VLAN 設定を確認します。

テストの設定

すべての集約スイッチ、アクセス スイッチ、およびサービス スイッチが相互接続されています。ブレード サーバおよびクライアントは、1 つのスイッチに接続されます。

テスト手順

集約スイッチ（Nexus 7010）、アクセス スイッチ（Nexus 5020）、およびサービス スイッチ（Cat 6506e）での VLAN 設定の確認テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　172.16.100.0 サブネット IP をサーバに割り当て、172.16.10.0 サブネット IP でクライアントを設定します。

ステップ 3　`show vlan` コマンドを使用して、既存の VLAN を確認します。次のコマンドを使用して、集約スイッチ（JVSL-A-AGG-N7k-01 と JVSL-A-AGG-N7k-02）に新しいサーバ VLAN 100 を作成し、サービス スイッチ（JVSL-A-C6k）に新しいクライアント VLAN 10 を作成します。

```
interface Vlan100
no shutdown
description FBS_Server_VLAN
ip address 172.16.100.2/24
interface Vlan10
description Client_VLAN
ip address 172.16.10.1 255.255.255.0
```

ステップ 4　それぞれのスイッチの VLAN データベースに VLAN 100 と 10 を追加します。`show vlan brief` コマンドを使用して、ステータスを確認します。

ステップ 5　次のコマンドを使用して、集約スイッチおよびサービス スイッチの VLAN に VLAN メンバー ポートを追加します。

```
interface GigabitEthernet4/13
switchport
switchport access vlan 10
```

ステップ 6　`show vlan brief` または `show vlan` コマンドを使用して、VLAN およびメンバーのステータスを確認します。

ステップ 7　VLAN のために集約スイッチおよびアクセス スイッチの必要なルーティングをイネーブルにします。クライアント PC からサーバに対する ping が成功することを確認します。

ステップ 8　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 9　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- VLAN はアップ状態で、クライアントは問題なくサーバと通信できます。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

集約スイッチ（Nexus 7010）、アクセス スイッチ（Nexus 5020）、およびサービス スイッチ（Cat 6506e）での VLAN 設定の確認テストに合格しました。

ハイ アベイラビリティ - リンク障害

ここで説明する内容は、次のとおりです。

- 「集約スイッチ（Nexus 7010）およびアクセス スイッチ（Nexus 5020）間の L2 ポート チャネルのリンク障害」
- 「コア スイッチおよび集約スイッチ（Nexus 7010）間の L3 ポート チャネルのリンク障害」
- 「Nexus 7010、5020、および Cat6506e デバイス間のポート チャネル（リンク）障害」

集約スイッチ（Nexus 7010）およびアクセス スイッチ（Nexus 5020）間の L2 ポート チャネルのリンク障害

このテストでは、各ブランチから JVSL アプリケーション トラフィックを送信します。送信後、トラフィックはシャットダウンされ、冗長リンクがアップ状態になります。各リンクは冗長性のために配置され、ダウン状態になると、集約スイッチ（JVSL-A-AGG-N7k-01 と AGG-N7k-02）およびアクセス スイッチ（JVSL-A-ACC-N5K-01 と ACC-N5K-02）間で冗長データ パスの引き継ぎが発生します。ダウン状態だったリンクがアップ状態になります。また、このテストでは、アプリケーションのエンドユーザへの影響が最小限であることも確認します。

テストの設定

すべての集約スイッチおよびアクセス スイッチが冗長リンクで相互接続され、ポート チャネルを使用して設定されています。

テスト手順

集約スイッチ（Nexus 7010）およびアクセス スイッチ（Nexus 5020）間の L2 ポート チャネルのリンク障害テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　loadsim を使用して、クライアントからサーバへの Exchange トラフィックの送信を開始します。

ステップ 3　集約スイッチ JVSL-A-AGG-N7k-01 にログインし、アクセス スイッチ（JVSL-A-ACC-N5K-01）に接続しているポート チャネル 202 の 1 つのリンクをシャットダウンします。

ステップ 4　`Show port-channel traffic` コマンドを使用して、ポート チャネルのトラフィックを確認します。

ステップ 5　JVSL-A-AGG-N7k-01 で `no shutdown` コマンドを使用して、シャットダウンしたリンクをアップ状態に戻します。

ステップ 6　`Show port-channel traffic` コマンドを使用して、ポート チャネルのトラフィックを確認します。

ステップ 7　集約スイッチ JVSL-A-AGG-N7k-02 にログインし、アクセス スイッチ（JVSL-A-ACC-N5K-02）に接続しているポート チャネル 203 の 1 つのリンクをシャットダウンします。

ステップ 8　`Show port-channel traffic` コマンドを使用して、ポート チャネルのトラフィックを確認します。

ステップ 9　JVSL-A-AGG-N7k-02 で `no shutdown` コマンドを使用して、シャットダウンしたリンクをアップ状態に戻します。

ステップ 10　`Show port-channel traffic` コマンドを使用して、ポート チャネルのトラフィックを確認します。

ステップ 11　アプリケーション トラフィックを停止し、結果を分析して、エンド ユーザ エクスペリエンスが予測どおりであることを確認します。

ステップ 12　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 13　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- 冗長リンクを介してトラフィックの迂回が発生し、リンク障害によるトラフィックの損失は最小限になります。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

集約スイッチ（Nexus 7010）およびアクセス スイッチ（Nexus 5020）間の L2 ポート チャネルのリンク障害テストに合格しました。

コア スイッチおよび集約スイッチ（Nexus 7010）間の L3 ポート チャネルのリンク障害

このテストでは、各ブランチから JVSL アプリケーション トラフィックを送信します。送信後、トラフィックはシャットダウンされ、冗長リンクはアップ状態に戻ります。

冗長性のために配置されている各リンクは、ダウン状態になると、コア スイッチ（JVSL-A-CORE-N7k-01 と JVSL-A-CORE-N7k-02）および集約スイッチ（JVSL-A-AGG-N7k-01 と JVSL-A-AGG-N7k-02）間で冗長データ パスの引き継ぎが発生します。ダウン状態だったリンクがアップ状態になります。また、このテストでは、アプリケーションのエンド ユーザへの影響が最小限であることも確認します。

テストの設定

すべて集約スイッチおよびアクセス スイッチが冗長リンクで相互接続されています。

テスト手順

コア スイッチおよび集約スイッチ（Nexus 7010）間の L3 ポート チャネルのリンク障害テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　loadsim を使用して、クライアントからサーバへの Exchange トラフィックの送信を開始します。

ステップ 3　コア スイッチ（JVSL-A-CORE-N7k-01）にログインし、集約スイッチ（JVSL-A-ACC-N5K-01）に接続しているポート チャネル 302 の 1 つのリンクをシャットダウンします。

ステップ 4　`Show port-channel traffic` コマンドを使用して、ポート チャネルのトラフィックを確認します。

ステップ 5　JVSL-A-CORE-N7k-01 で `no shutdown` コマンドを発行して、シャットダウンしたリンクをアップ状態にします。

ステップ 6　`Show port-channel traffic` コマンドを使用して、ポート チャネルのトラフィックを確認します。

ステップ 7　集約スイッチ JVSL-A-AGG-N7k-02 にログインし、コア スイッチ（JVSL-A-CORE-N7k-02）に接続しているポート チャネル 303 の 1 つのリンクをシャットダウンします。

ステップ 8　次のコマンドを使用してポート チャネルのトラフィックを確認します。
`Show port-channel traffic`

ステップ 9　JVSL-A-AGG-N7k-02 で `no shutdown` コマンドを使用して、シャットダウンしたリンクをアップ状態に戻します。

ステップ 10　`Show port-channel traffic` コマンドを使用して、ポート チャネルのトラフィックを確認します。

ステップ 11　アプリケーション トラフィックを停止し、結果を分析して、エンド ユーザ エクスペリエンスが予測どおりであることを確認します。

ステップ 12　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 13　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- 冗長リンクを介してトラフィックの迂回が発生し、リンク障害によるトラフィックの損失は最小限になります。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

コア スイッチおよび集約スイッチ（Nexus 7010）間の L3 ポート チャネルのリンク障害テストに合格しました。

Nexus 7010、5020、および Cat6506e デバイス間のポート チャネル（リンク）障害

このテストでは、多様なアクティブ冗長リンク障害の発生時のアプリケーションの機能を確認します。

このテストでは、アプリケーション トラフィックが 15 分間送信されます。冗長性のために配置されている各リンクは、ダウン状態になると、冗長データ パスの引き継ぎが発生します。ダウン状態だったリンクがアップ状態になります。また、このテストでは、アプリケーションのエンド ユーザへの影響が最小限であることも確認します。

テストの設定

すべてのコア スイッチ、集約スイッチ、アクセス スイッチ、およびサービス スイッチが、ポート チャネルを介して相互接続されています。

テスト手順

Nexus 7010、5020、および Cat6506e デバイス間のポート チャネル（リンク）障害テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　各ブランチのアプリケーション テスト トラフィックが設定されていることを確認します。

ステップ 3　15 分間のテスト トラフィックを開始します。

ステップ 4　shutdown コマンドを発行して、2 つのコア スイッチ（JVSL-A-CORE-N7k-01、JVSL-A-CORE-N7k-02）間の L3 ポート チャネルをシャットダウンします。

ステップ 5　`no shutdown` コマンドを使用して、シャットダウンした L3 ポート チャネルをアップ状態に戻します。

ステップ 6　`shutdown` コマンドを使用して、JVSL-A-CORE-N7k-01 および JVSL-A-AGG-N7k-01 間の L3 ポート チャネルをシャットダウンします。

ステップ 7　`no shutdown` コマンドを使用して、シャットダウンした L3 ポート チャネルをアップ状態に戻します。

ステップ 8　`shutdown` コマンドを使用して、JVSL-A-CORE-N7k-01 および JVSL-A-AGG-N7k-01 間の L3 ポート チャネル リンクの 1 つをシャットダウンします。

ステップ 9　`no shutdown` コマンドを使用して、シャットダウンした L3 ポート チャネルをアップ状態に戻します。

ステップ 10　shutdown コマンドを使用して、JVSL-A-AGG-N7k-01 および JVSL-A-AGG-N7k-02 間の L2 ポート チャネルの 1 つのリンクをシャットダウンします。

ステップ 11　`no shutdown` コマンドを使用して、シャットダウンしたリンクをアップ状態に戻します。

ステップ 12　`shutdown` コマンドを使用して、JVSL-A-CORE-01 および JVSL-A-AGG-01 間の L2 ポート チャネルをシャットダウンします。

ステップ 13　`no shutdown` コマンドを使用して、シャットダウンした L2 ポート チャネルをアップ状態に戻します。

ステップ 14　`shutdown` コマンドを使用して、JVSL-A-AGG-N7K-01 および JVSL-A-ACC-5K-02 間の L2 ポート チャネルをシャットダウンします。

ステップ 15　`no shutdown` コマンドを使用して、シャットダウンした L2 ポート チャネルをアップ状態に戻します。

ステップ 16　`shutdown` コマンドを使用して、JVSL-A-AGG-N7K-01 および JVSL-A-ACC-N5K-01 スイッチ間の L2 ポート チャネルをシャットダウンします。

ステップ 17　`no shutdown` コマンドを使用して、シャットダウンした L2 ポート チャネルをアップ状態に戻します。

ステップ 18　`shutdown` コマンドを使用して、JVSL-AGG-N7K-02 および JVSL-ACC-N5K-02 スイッチ間の L2 ポート チャネルをシャットダウンします。

ステップ 19　`no shutdown` コマンドを使用して、シャットダウンした L2 ポート チャネルをアップ状態に戻します。

ステップ 20　トラフィックが完了したら、結果を保存して分析し、エンド ユーザ エクスペリエンスが予測どおりであることを確認します。

ステップ 21　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 22　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- コンポーネントの障害発生後も、アプリケーション トラフィックが継続して渡されます。
- エンド ユーザに対する影響は最小限です。

結果

Nexus 7010、5020、および Cat6506e デバイス間のポート チャネル（リンク）障害テストに合格しました。

ハイ アベイラビリティ - デバイス障害

ここで説明する内容は、次のとおりです。

- 「アクセス スイッチ（Nexus5020）のリロード」
- 「集約スイッチ（Nexus 7010）のリロード」

アクセス スイッチ（Nexus5020）のリロード

このテストでは、アクセス デバイスに障害が発生したときのアプリケーションの機能を確認します。また、各ブランチから JVSL アプリケーション トラフィックを送信し、アクセス スイッチに障害が発生するテストも行います。

テストの設定

アクセス スイッチ（JVSL-A-ACC-N5K-01 と JVSL-A-ACC-N5K-02）が集約スイッチに接続されている必要があります。

テスト手順

アクセス スイッチ（Nexus5020）のリロード テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　クライアントからサーバへの通信が正常に動作していることを確認します。loadsim ツールを使用して、サーバへの Exchange クライアント トラフィックを開始します。

ステップ 3　`reload` コマンドを使用して、トラフィックをアクティブに渡しているアクセス スイッチ（JVSL-A-ACC-N5K-01）の 1 つをリロードします。

ステップ 4　トラフィックが完了したら、結果を保存して分析し、エンド ユーザ エクスペリエンスが予測どおりであることを確認します。

ステップ 5　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 6　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- デバイスの障害発生後も、アプリケーション トラフィックが継続して渡されます。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

アクセス スイッチ（Nexus 5020）のリロード テストに合格しました。

集約スイッチ（Nexus 7010）のリロード

このテストでは、集約デバイスに障害が発生したときのアプリケーションの機能を確認します。ブランチから JVSL アプリケーション トラフィックを送信し、集約スイッチに障害が発生するテストを行います。

テストの設定

相互運用性テスト トポロジ集約スイッチは VDC（JVSL-A-AGG-N7k-01）です。ユーザは、デフォルトの VDC にアクセスして reload（VDC）コマンドを実行できるようになっています。

テスト手順

集約スイッチ（Nexus 7010）のリロード テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　クライアントからサーバへの通信が正常に動作していることを確認します。loadsim ツールを使用して、サーバへの Exchange クライアント トラフィックを開始します。

ステップ 3　集約スイッチ（JVSL-A-AGG-N7k-01）をリロードします。デフォルトの VDC から reload VDC コマンドを発行することで、このスイッチからアクティブにトラフィックが渡されます。

ステップ 4　トラフィックが完了したら、結果を保存して分析し、エンド ユーザ エクスペリエンスが予測どおりであることを確認します。

ステップ 5　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 6　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- デバイスの障害発生後も、アプリケーション トラフィックが継続して渡されます。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

集約スイッチ（Nexus 7010）のリロード テストに合格しました。

CHAPTER 4

L4 ～ L7 サービス

「L4 ～ L7 サービス」の項のテストでは、Cat6506e スイッチの複数のサービスに触れるトラフィック フローに重点を置いています。この項で使用されるサービス アプライアンスは、ASA ファイアウォールと IPS です。

ここで説明する内容は、次のとおりです。

- 「設定の確認」
- 「セキュリティ」
- 「ハイ アベイラビリティ」

設定の確認

ここで説明する内容は、次のとおりです。

- 「ASA 設定の確認」
- 「IPS 設定テスト」

ASA 設定の確認

テスト手順

ASA 設定の確認テストの手順は次のとおりです。

ステップ 1 CLI route-map client-traffic を使用して、検査のためにクライアントから ASA へのトラフィックを許可するように Cat6k を設定します。FW への着信トラフィックについて VLAN 20 を設定します。

```
permit 10
match ip address 110
set ip next-hop 192.168.20.2
access-list 110 permit ip 192.168.10.0 0.0.0.255 192.168.100.0 0.0.0.255
```

ステップ 2 サーバ トラフィックのみを許可するように FW を設定します。次の設定インターフェイス Vlan100 を使用して、FW からの発信トラフィック（VLAN 30）を cat6k に配信します。

```
ip address 192.168.100.50 255.255.255.0
ip policy route-map return-traffic
route-map return-traffic permit 10
match ip address 150
```

```
set ip next-hop 192.168.30.2 Access-list 150 permit ip 192.168.100.0 0.0.0.255 host
192.168.10.10
```

ステップ 3　クライアントからのすべてのトラフィックを渡し、FW がトラフィックを検査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。

- すべての検査 CLI が設定されます。
- トラフィックがサーバに到達する前に、ASA はトラフィックを検査できます。
- CPU またはメモリに問題がありません。

結果

ASA 設定の確認テストに合格しました。

IPS 設定テスト

テスト手順

IPS 設定テストの手順は次のとおりです。

ステップ 1　IPS をプロミスキャス モードで設定します。

ステップ 2　検査のために、トラフィックの 1 コピーを IPS に渡すように Cat6k を設定します。これは FW の発信トラフィックです。

ステップ 3　アプリケーション トラフィックを渡し、検査のためにトラフィックが IPS に送信され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。

- IPS 検査の設定が指定されます。
- IPS は ASA からのすべてのトラフィックを検査します。
- CPU またはメモリに問題がありません。

結果

IPS 設定テストに合格しました。

セキュリティ

ここで説明する内容は、次のとおりです。

- 「ブランチ オフィス ユーザを制限する ASA の設定」
- 「SMTP 検査のイネーブル化」

ブランチ オフィス ユーザを制限する ASA の設定

ブランチ オフィス ユーザを制限する ASA の設定テストの手順は次のとおりです。

ステップ 1　ブランチ オフィス ユーザのみを許可するように ASA を設定します。

ステップ 2　トラフィックを渡し、ブランチ オフィス ユーザがアクセス権を持っているかどうかを確認します。ブランチ オフィスの IP アドレス以外の IP アドレスが、FW によって拒否され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。

- ブランチ オフィス クライアントはサーバにアクセスできます。
- ブランチ オフィス クライアント以外のユーザは、サーバにアクセスできません。
- CPU またはメモリに問題がありません。

結果

ブランチ オフィス ユーザを制限する ASA の設定テストに合格しました。

SMTP 検査のイネーブル化

SMTP 検査のイネーブル化テストの手順は次のとおりです。

ステップ 1　SMTP のイネーブル化設定を使用して ASA を設定します。

ステップ 2　SMTP トラフィックを渡し、SMTP トラフィックが検査されるかどうかを確認します。

予測結果

次のテスト結果が予想されます。

- SMTP がイネーブル化されます。
- トラフィックは SMTP 検査を渡します。
- CPU またはメモリに問題がありません。

結果

SMTP 検査のイネーブル化テストに合格しました。

ハイ アベイラビリティ

ここで説明する内容は、次のとおりです。

- 「IPS のリンク障害」
- 「IPS の障害」

IPS のリンク障害

IPS のリンク障害テストの手順は次のとおりです。

ステップ 1　IPS リンクがダウン状態であることを確認します。

ステップ 2　クライアントからのトラフィックを渡します。

ステップ 3　IPS リンクがダウン状態のため、トラフィック フローのブロック処理がないことを確認します。

予測結果

次のテスト結果が予想されます。

- IPS リンクがダウン状態で IPS がバイパスされるため、トラフィック フローのブロック処理がないことを確認します。
- CPU またはメモリに問題がありません。

結果

IPS のリンク障害テストに合格しました。

IPS の障害

IPS の障害テストの手順は次のとおりです。

ステップ 1　IPS がダウン状態（電源オフ）であることを確認します。

ステップ 2　クライアントからのトラフィックを渡します。

ステップ 3　IPS がダウン状態のため、トラフィック フローのブロック処理がないことを確認します。

予測結果

次のテスト結果が予想されます。

- IPS の障害で IPS がバイパスされるため、トラフィック フローのブロック処理がありません。
- CPU またはメモリに問題がありません。

結果

IPS の障害テストに合格しました。

CHAPTER 5

Storage Area Networking（SAN）

ここで説明する内容は、次のとおりです。

- 「MDS に関連する設定および確認」
- 「マルチパスのイネーブル化」
- 「マルチパスのディセーブル化」

MDS に関連する設定および確認

ここで説明する内容は、次のとおりです。

- 「VSAN の設定（Fujitsu サーバから Hitachi ストレージへ）」
- 「ゾーンの設定（Fujitsu サーバから Hitachi ストレージへ）」
- 「IVR-with NAT 設定（Fujitsu サーバから Hitachi ストレージへ）」
- 「ホスト（Fujitsu サーバ）からストレージ（Hitachi）へのファブリック接続」

VSAN の設定（Fujitsu サーバから Hitachi ストレージへ）

このテストでは、（CLI 検証を使用した）Fabric Manager を介する（Windows 2008 オペレーティング システムを搭載する）ホストとストレージ アレイ間で、ホスト（Fujitsu サーバ）からストレージ（Hitachi）に対して必要なすべての VSAN の設定およびアクティベーションを確認します。

テストの設定

Windows Enterprise 2008 Server オペレーティング システムを搭載する MS Exchange テスト ホストを作成します。2 つの異なる VSAN を作成して、単一の MDS スイッチに 2 つの個別のファブリックを作成します。ホストを 2 つのファブリックに格納します。また、ストレージ アレイをホスト ファブリックに配置します。ストレージ アレイで LUN マスキングを設定し、テスト ホストから適切な LUN にアクセスできるようにします。

テスト手順

VSAN の設定（Fujitsu サーバから Hitachi ストレージへ）の実行手順は次のとおりです。

ステップ 1 テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　次のコマンドを使用して、1 つのファブリックにつき 1 つの Windows ホストを作成します。

```
(config)# vsan database
(config-vsan-db)# vsan <1-4094>
```

ステップ 3　また、次のように、Windows ホストと対応するストレージ アレイ ファブリック ポートをメンバーとして VSAN に追加します。

```
(config-vsan-db)# vsan <1-4094> interface fc "PORT CONNECTED TO HOST"
(config-vsan-db)# vsan <1-4094> interface fc "PORT CONNECTED TO STORAGE"
```

ステップ 4　Windows ホストと対応するストレージ アレイ ファブリック ポートが、適切な Windows ホスト VSAN のファブリックおよび FC Name Server にログインしていることを確認します。

```
MDS# sh vsan <1-4094> membership
```

ステップ 5　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 6　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- Fabric Manager は、ホストとストレージ アレイ間のすべての VSAN を問題なく設定します。
- VSAN のサービスの設定および確認に問題または課題がありません。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

VSAN の設定（Fujitsu サーバから Hitachi ストレージへ）テストに合格しました。

ゾーンの設定（Fujitsu サーバから Hitachi ストレージへ）

このテストでは、ゾーン分割設定によって、（Windows オペレーティング システムを搭載する）ホストとストレージ アレイ間の通信が可能になることを確認します。ゾーンおよびゾーン セットは、（CLI 検証を使用した）Fabric Manager を介して設定および確認されます。

テストの設定

VSAN の設定が実行され、このテストを続行できることを検証されます。

テスト手順

ゾーンの設定（Fujitsu サーバから Hitachi ストレージへ）の実行手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　ファブリックごとに、次のコマンドを使用して Windows Host VSAN 用に 1 つの Windows ホスト ゾーンを作成します。

```
(config)# zone name vsan <1-4093>
```

ステップ 3　Windows ホストと対応するストレージ アレイ ファブリック ポートを、メンバーとしてゾーン（2 メンバー ゾーン）に追加します。

```
(config-zone)# member pwwn "OF HOST"
(config-zone)# member pwwn "OF STORAGE"
```

ステップ 4　ファブリックごとに、ホストのゾーン セットを作成し、作成したゾーンを追加します。

```
(config)# zoneset name Zoneset100 vsan <1-4093>
(config-zoneset)# member <ZONE_NAME>
```

ステップ 5　ゾーン セットをアクティブにし、分散します。

```
(config)# Zoneset activate name vsan
```

ステップ 6　ファブリックごとに、ファブリック全体のゾーン セットの分散とアクティベーションを確認します。

```
(config)# Zoneset activate name vsan <1-4093>
```

ゾーン セットのアクティベーションが開始されます。

ステップ 7　ゾーンのステータスを確認します。

ステップ 8　各テスト ホストから必要な LUN を参照できることを確認します。

ステップ 9　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 10　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- Fabric Manager は、ホスト間のすべてのゾーンを問題なく設定できます。
- ゾーンのサービスの設定および確認に問題または課題がありません。
- すべてのゾーンおよびゾーン メンバーがアクティベーションになり、すべてのゾーンがファブリック内のノード全体に分散されます。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

ゾーンの設定（Fujitsu サーバから Hitachi ストレージへ）テストに合格しました。

IVR-with NAT 設定（Fujitsu サーバから Hitachi ストレージへ）

このテストでは、同じスタティック ドメイン ID を持つ複数の VSAN 内でトラフィックを渡すことができるように、IVR 機能を確認します。ファイバ チャネルのトラフィック生成は、同じドメイン ID を持つ複数の VSAN 内で、ホストからストレージに対して通信できるように設定されています。すべての設定は Fabric Manager を使用して実行され、確認は CLI を介して行われます。

テストの設定

テスト ホストとストレージに接続しているエッジ VSAN ごとに 1 つのスイッチを使用して、テスト トポロジを作成します。スイッチで IVR を選択します。

テスト手順

IVR-with NAT 設定（Fujitsu サーバから Hitachi ストレージへ）テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　次のコマンドを使用して、スイッチの IVR をイネーブルにします。

```
(config)# ivr enable
```

ステップ 3　IVR トポロジを設定し、通信するすべての VSAN を含めます。

```
(config)# ivr vsan-topology database
(config-ivr-topology-db)# autonomous-fabric-id <1-64> switch-wwn vsan-ranges
(config)# ivr vsan-topology activate
```

ステップ 4　IVR トポロジをアクティブにします。

```
(config)# ivr vsan-topology activate
```

ステップ 5　IVR ゾーンを作成し、テスト ポートがアクティブで IVR ゾーン内にあることを確認します。

```
(config)# ivr zone name
(config-ivr-zone)# member pwwn vsan <1-4093> autonomous-fabric-id <1-63>
MDS# sh ivr zone active
```

ステップ 6　IVR ゾーン セットを作成し、アクティブにします。ゾーン セットのステータスを確認します。

```
(config)# ivr zoneset name
(config-ivr-zoneset)# member <ZONE_NAME>
(config)# ivr zoneset activate name
MDS# show ivr zoneset status
```

ステップ 7　テスト ホストから IOMeter ツールを使用してトラフィックを生成します。IVR 上で、ストレージ トラフィックがリモート ストレージ アレイに対して損失や問題なく配信されていることを確認します。

ステップ 8　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 9　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- トランスポート ファブリックの送信元 VSAN からリモートの宛先ファブリックに対するトラフィックを、IVR-NAT が適切にルーティングしています。
- VSAN 間ルーティングにトラフィックの損失や問題がありません。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

IVR 設定（Fujitsu サーバから Hitachi ストレージへ）テストに合格しました。

ホスト（Fujitsu サーバ）からストレージ（Hitachi）へのファブリック接続

このテストでは、トラフィック フローのテスト前に、Fujitsu ホスト、Hitachi ストレージ アレイ、および MDS ファブリック間の接続が、問題のないインフラストラクチャであることを確認します。この確認を行うには、ポート ステータスの状況をチェックします。また、すべての使用可能なリンクのエンド デバイスで、ファブリックのログインを完了します。この操作は、Fabric Manager 検証を使用した CLI を介して行います。

テストの設定

すべてのテスト ホスト、スイッチ、およびストレージ アレイが接続され、適切な VSAN とゾーンが作成されています。

テスト手順

ホスト（Fujitsu サーバ）からストレージ（Hitachi）へのファブリック接続テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　すべてのテスト ホストとストレージ アレイの接続がアクティブで、トポロジ マップに正しく表示されていることを確認します。

ステップ 3　正しい PWWN、HBA ID、およびエイリアスをチェックして、ファブリックの正常なログイン、ファイバ チャネル ネーム サーバの登録、およびデバイスのエイリアスを確認します。

ステップ 4　エラーに対して、すべてのホストとストレージ アレイ ファブリック ポートを確認します。

ステップ 5　CLI を介して Fabric Manager の情報（前の手順）を検証します。

```
MDS#show flogi database vsan
```

ステップ 6　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 7　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- Fabric Manager ファブリック ディスカバリ プロセスによって、ホストとストレージ アレイの接続情報が正確に提示されます。
- ホストと対応するファブリック ノード間のすべてのリンクがアクティブです（UP）。同様のことがストレージ アレイ リンクにも適用されます。
- すべてのテスト ホストとストレージ アレイが、ファブリックに正常にログインできます（FLOGI）。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

ホスト（Fujitsu サーバ）からストレージ（Hitachi）へのファブリック接続テストに合格しました。

マルチパスのイネーブル化

ここで説明する内容は、次のとおりです。

- 「リンク障害（ケーブルを物理的に取り外す）（Fujitsu サーバから MDS へ）」
- 「リンク障害（ケーブルを物理的に取り外す）（MDS から Hitachi ストレージへ）」
- 「リンク障害（ポートのシャットダウン）（Fujitsu サーバから MDS へ）」
- 「リンク障害（ポートのシャットダウン）（MDS から Hitachi ストレージへ）」
- 「ファブリックでの VSAN の停止（VSAN SUSPEND）」

リンク障害（ケーブルを物理的に取り外す）（Fujitsu サーバから MDS へ）

このテストでは、リンク障害に対するファブリックとホストの復元力を確認します。リンク障害は、マルチパス ソフトウェアが冗長パスがあるホストで実行されているときに、ケーブルの切断によって発生します。

テストの設定

ストレージ トラフィックが、Fujitsu ホスト（Windows）から Hitachi ストレージ アレイに対して生成されます。ホスト ポートの再接続時に、復元が完全かどうかが確認されます。すべての設定と確認は、Fabric Manager でチェックしながら CLI を介して実行されます。

テスト手順

リンク障害（ケーブルを物理的に取り外す）（Fujitsu サーバから MDS へ）テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　テスト ホストが、各パスから 1 つの LUN を参照できることを確認します。

ステップ 3　テスト ホスト（Windows）から Hitachi ストレージ アレイに対してストレージ トラフィックを生成します。

ステップ 4　テスト ホストとファブリック間のリンクを物理的に取り外します。

ステップ 5　障害が検出され、管理アプリケーションに報告されることを確認します。

ステップ 6　トラフィックが冗長パスへすべて流れることを確認します。

ステップ 7　リンクを再接続し、問題なく復元されることを確認します。

ステップ 8　ストレージ トラフィック フローが、再接続されたリンクで復元されることを確認します。

ステップ 9　リンクの復元が検出され、デバイスから管理アプリケーションに報告されることを確認します。

ステップ 10　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 11　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- リンク障害によってトラフィックは停止しません。
- 障害発生時および復元時に、トラフィックの損失はゼロか最小限です。
- 障害と復元が検出され、デバイスから管理アプリケーション サーバ（Fabric Manager）に報告されます。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

リンク障害（ケーブルを物理的に取り外す）（Fujitsu サーバから MDS へ）テストに合格しました。

リンク障害（ケーブルを物理的に取り外す）（MDS から Hitachi ストレージへ）

このテストでは、リンク障害に対するファブリックとストレージの復元力を確認します。リンク障害は、マルチパス ソフトウェアが冗長パスがあるホストで実行されているときに、ケーブルの切断によって発生します。

テストの設定

ストレージ トラフィックが、Fujitsu ホスト（Windows）から Hitachi ストレージ アレイに対して生成されます。ホスト ポートの再接続時に、復元が完全かどうかが確認されます。すべての設定と確認は、Fabric Manager でチェックしながら CLI を介して実行されます。

テスト手順

リンク障害（ケーブルを物理的に取り外す）（MDS から Hitachi ストレージへ）テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　ホストが、両方のパスから 1 つの LUN のみを参照できることを確認します。

ステップ 3　複数のテスト ホスト（Windows）から Hitachi ストレージ アレイに対するストレージ トラフィックを生成します。

ステップ 4　ファブリックおよびストレージ間のリンクを物理的に取り外します。

ステップ 5　障害が検出され、管理アプリケーションに報告されることを確認します。

ステップ 6　トラフィックが冗長パスへすべて流れることを確認します。

ステップ 7　リンクを再接続し、問題なく復元されることを確認します。

ステップ 8　ストレージ トラフィック フローが、再接続されたリンクで復元されることを確認します。

ステップ 9　リンクの復元が検出され、デバイスから管理アプリケーションに報告されることを確認します。

ステップ 10　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 11　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- マルチパス ソフトウェアが冗長ホスト リンクへのフェールオーバーを処理するため、リンク障害によってトラフィックは停止しません。
- 障害発生時および復元時に、トラフィックの損失はゼロか最小限です。
- 障害と復元が検出され、デバイスから管理アプリケーション サーバ（Fabric Manager）に報告されます。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

リンク障害（ケーブルを物理的に取り外す）（MDS から Hitachi ストレージへ）テストに合格しました。

リンク障害（ポートのシャットダウン）（Fujitsu サーバから MDS へ）

このテストでは、マルチパス ソフトウェアが冗長パスのあるホストで実行されている場合に、ポートのシャットダウンに対するファブリックおよびホストの復元力を確認します。

テストの設定

ストレージ トラフィックが、テスト ホスト（Windows）からストレージ アレイに対して生成されます。トラフィックが冗長接続に再ルーティングされることを確認するため、テスト ホストのポートに面する 1 つのホストがディセーブル化されます。ホスト ポートがイネーブル化されたときに、復元が完全かどうかが確認されます。すべての設定と確認は、Fabric Manager でチェックしながら CLI を介して実行されます。

テスト手順

リンク障害（ポートのシャットダウン）（Fujitsu サーバから MDS へ）テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　テスト ホストが、冗長パスから 1 つの LUN のみを参照できることを確認します。

ステップ 3　Fujitsu テスト ホスト（Windows）から Hitachi ストレージ アレイに対してストレージ トラフィックを生成します。

ステップ 4　テスト ホストのスイッチ リンクをシャットダウンします。

ステップ 5　シャットダウンが検出され、管理アプリケーションに報告されることを確認します。

ステップ 6　トラフィックが冗長パスへすべて流れることを確認します。

ステップ 7　リンクを再イネーブル化し、問題なく復元されることを確認します。

ステップ 8　ストレージ トラフィック フローが、再イネーブル化されたリンクで復元されることを確認します。

ステップ 9　リンクの復元が検出され、デバイスから管理アプリケーションに報告されることを確認します。

ステップ 10　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 11　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がないことを確認します。

予測結果

次のテスト結果が予想されます。

- マルチパス ソフトウェアが冗長ホスト リンクへのフェールオーバーを処理するため、リンク障害によってトラフィックは停止しません。
- 障害発生時および復元時に、トラフィックの損失はゼロか最小限です。
- ホスト ポートのリセットからシステムが完全に復元されます。
- 障害と復元が検出され、デバイスから管理アプリケーション サーバ（Fabric Manager）に報告されます。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

リンク障害（ポートのシャットダウン）（Fujitsu サーバから MDS へ）テストに合格しました。

リンク障害（ポートのシャットダウン）（MDS から Hitachi ストレージへ）

このテストでは、マルチパス ソフトウェアが冗長パスのあるホストで実行されている場合に、ポートのシャットダウンに対するファブリックおよびストレージの復元力を確認します。

テストの設定

ストレージ トラフィックが、Fujitsu ホスト（Windows）から Hitachi ストレージ アレイに対して生成されます。トラフィックが冗長接続に再ルーティングされることを確認するため、テスト ホストのポートに面する 1 つのストレージがディセーブル化されます。ホスト ポートがイネーブル化されたときに、復元が完全かどうかが確認されます。すべての設定と確認は、Fabric Manager でチェックしながら CLI を介して実行されます。

テスト手順

リンク障害（ポートのシャットダウン）（MDS から Hitachi ストレージへ）テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　ホストが、両方のパスから 1 つの LUN のみを参照できることを確認します。

ステップ 3　Fujitsu テスト ホスト（Windows）から特定のストレージ アレイに対してストレージ トラフィックを生成します。

ステップ 4　ストレージ側に面するポートのスイッチ リンクをシャットダウンします。

ステップ 5　シャットダウンが検出され、管理アプリケーションに報告されることを確認します。

ステップ 6　トラフィックが冗長パスへすべて流れることを確認します。

ステップ 7　リンクを再イネーブル化し、問題なく復元されることを確認します。

ステップ 8　ストレージ トラフィック フローが、再イネーブル化されたリンクで復元されることを確認します。

ステップ 9　リンクの復元が検出され、デバイスから管理アプリケーションに報告されることを確認します。

ステップ 10　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 11　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- マルチパス ソフトウェアが冗長ホスト リンクへのフェールオーバーを処理するため、リンク障害によってトラフィックは停止しません。
- 障害発生時および復元時に、トラフィックの損失はゼロか最小限です。
- ホスト ポートのリセットからシステムが完全に復元されます。
- 障害と復元が検出され、デバイスから管理アプリケーション サーバ（Fabric Manager）に報告されます。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

リンク障害（ポートのシャットダウン）（MDS から Hitachi ストレージへ）テストに合格しました。

ファブリックでの VSAN の停止（VSAN SUSPEND）

このテストでは、VSAN の停止によって、ファブリック ノードへの接続に切り替えられたストレージ アレイに接続するホストのパスが失われる以外に、アクティブなサービスとストレージ 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

ストレージ トラフィックが、テスト ホスト（Windows および Linux）によって生成され、ストレージ アレイにルーティングされます。ファブリック ノードの VSAN の 1 つが削除され、ストレージに接続されたホストについて、トラフィックの再ルーティングがファブリックの冗長 VSAN 上にあるパスを通過して行われることが確認されます。ファブリック ノード上のストレージに接続されたホストがチェックされ、中断のないことが確認されます。すべての確認は、CLI と Fabric Manager を介して実行されます。

テスト手順

ファブリックでの VSAN 停止（VSAN SUSPEND）テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　Fujitsu テスト ホスト（Windows）から Hitachi ストレージ アレイに対してストレージ トラフィックを生成します。

ステップ 3　ストレージ トラフィックがファブリックを通過するファブリック ノードの VSAN の 1 つを停止し、約 15 ～ 30 秒後にオンラインに戻します。

```
(config-vsan-db)# vsan <1-4093> suspend
.
.
(config-vsan-db)# no vsan <1-4093> suspend
```

ステップ 4　ファブリック ノードで VSAN の損失が検出され、管理アプリケーションに報告されることを確認します。

ステップ 5　ストレージ ポートに接続するホストに対するパスの損失以外に、トラフィック フローがファブリック ノードの損失の影響を受けていないことを確認します。

ステップ 6　問題なく復元していることを確認します。

ステップ 7　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 8　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- 冗長 VSAN があるため、ファブリック ノードの VSAN が完全に損失してから復元しても、ホストの I/O トラフィックは停止しません。
- 障害が発生した VSAN と同じファブリックでは、ホスト I/O トラフィックは影響を受けません。
- システムは、ファブリックの VSAN の損失から完全に復元されます。
- ファブリック VSAN の損失が検出され、デバイスから管理サーバ（つまり Fabric Manager）に報告されます。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

ファブリックでの VSAN の停止（VSAN SUSPEND）テストに合格しました。

マルチパスのディセーブル化

ここで説明する内容は、次のとおりです。

- 「リンク障害（ケーブルを物理的に取り外す）（Fujitsu サーバから MDS へ）」
- 「リンク障害（ケーブルを物理的に取り外す）（MDS から Hitachi ストレージへ）」
- 「リンク障害（ポートのシャットダウン）（Fujitsu サーバから MDS へ）」
- 「リンク障害（ポートのシャットダウン）（MDS から Hitachi ストレージへ）」
- 「ファブリックでの VSAN の停止（VSAN SUSPEND）」

リンク障害（ケーブルを物理的に取り外す）（Fujitsu サーバから MDS へ）

このテストでは、リンク障害に対するファブリックとホストの復元力を確認します。リンク障害は、マルチパス ソフトウェアが冗長パスがあるホストでディセーブルのときに、ケーブルの切断によって発生します。

テストの設定

ストレージ トラフィックが、Fujitsu ホスト（Windows）から Hitachi ストレージ アレイに対して生成されます。ホスト ポートの再接続時に、復元が完全かどうかが確認されます。すべての設定と確認は、Fabric Manager でチェックしながら CLI を介して実行されます。

テスト手順

リンク障害（ケーブルを物理的に取り外す）（Fujitsu サーバから MDS へ）テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　テスト ホストから、各パスについて 2 つの LUN が参照できることを確認します。

ステップ 3　テスト ホスト（Windows）から Hitachi ストレージ アレイに対してストレージ トラフィックを生成します。

ステップ 4　テスト ホストとファブリック間のリンクを物理的に取り外します。

ステップ 5　障害が検出され、管理アプリケーションに報告されることを確認します。

ステップ 6　トラフィックが冗長パスへすべて流れることを確認します。

ステップ 7　リンクを再接続し、問題なく復元されることを確認します。

ステップ 8　ストレージ トラフィック フローが、再イネーブル化されたリンクで復元されることを確認します。

ステップ 9　リンクの復元が検出され、デバイスから管理アプリケーションに報告されることを確認します。

ステップ 10　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 11　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がないことを確認します。

予測結果

次のテスト結果が予想されます。

- リンク障害によってトラフィックが停止します。
- 障害発生時と復元時のトラフィックの損失は最小限です。
- 障害と復元が検出され、デバイスから管理アプリケーション サーバ（Fabric Manager）に報告されます。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

リンク障害（ケーブルを物理的に取り外す）（Fujitsu サーバから MDS へ）テストに合格しました。

リンク障害（ケーブルを物理的に取り外す）（MDS から Hitachi ストレージへ）

このテストでは、リンク障害に対するファブリックとストレージの復元力を確認します。リンク障害は、マルチパス ソフトウェアが冗長パスがあるホストでディセーブルのときに、ケーブルの切断によって発生します。

テストの設定

ストレージ トラフィックが、Fujitsu ホスト（Windows）から Hitachi ストレージ アレイに対して生成されます。ホスト ポートの再接続時に、復元が完全かどうかが確認されます。すべての設定と確認は、Fabric Manager でチェックしながら CLI を介して実行されます。

テスト手順

リンク障害（ケーブルを物理的に取り外す）（MDS から Hitachi ストレージへ）テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　ホストが、各冗長パスから 1 つの LUN のみを参照できることを確認します。

ステップ 3　複数のテスト ホスト（Windows）から Hitachi ストレージ アレイに対するストレージ トラフィックを生成します。

ステップ 4　ファブリックおよびストレージ間のリンクを物理的に取り外します。

ステップ 5　障害が検出され、管理アプリケーションに報告されることを確認します。

ステップ 6　トラフィックが冗長パスへすべて流れることを確認します。

ステップ 7　リンクを再接続し、問題なく復元されることを確認します。

ステップ 8　ストレージ トラフィック フローが、再イネーブル化されたリンクで復元されることを確認します。

ステップ 9　リンクの復元が検出され、デバイスから管理アプリケーションに報告されることを確認します。

ステップ 10　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 11　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- リンク障害によってトラフィックは停止しません。
- 障害発生時と復元時のトラフィックの損失は最小限です。
- 障害と復元が検出され、デバイスから管理アプリケーション サーバ（Fabric Manager）に報告されます。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

リンク障害（ケーブルを物理的に取り外す）（MDS から Hitachi ストレージへ）テストに合格しました。

リンク障害（ポートのシャットダウン）（Fujitsu サーバから MDS へ）

このテストでは、マルチパス ソフトウェアが冗長パスのあるホストでディセーブルの場合に、ポートのシャットダウンに対するファブリックおよびホストの復元力を確認します。

テストの設定

ストレージ トラフィックが、テスト ホスト（Windows）からストレージ アレイに対して生成されます。トラフィックが冗長接続に再ルーティングされることを確認するため、テスト ホストのポートに面する 1 つのホストがディセーブル化されます。ホスト ポートがイネーブル化されたときに、復元が完全かどうかが確認されます。すべての設定と確認は、Fabric Manager でチェックしながら CLI を介して実行されます。

テスト手順

リンク障害（ケーブルを物理的に取り外す）（MDS から Hitachi ストレージへ）テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　テスト ホストが、各冗長パスから 2 つの LUN を参照できることを確認します。

ステップ 3　Fujitsu テスト ホスト（Windows）から Hitachi ストレージ アレイに対してストレージ トラフィックを生成します。

ステップ 4　テスト ホストのスイッチ リンクをシャットダウンします。

ステップ 5　シャットダウンが検出され、管理アプリケーションに報告されることを確認します。

ステップ 6　いくつかの最小限の損失後に、トラフィックが冗長パス上で完全に流れることを確認します。

ステップ 7　リンクを再イネーブル化し、問題なく復元されることを確認します。

ステップ 8　ストレージ トラフィック フローが、再イネーブル化されたリンクで復元されることを確認します。

ステップ 9　リンクの復元が検出され、デバイスから管理アプリケーションに報告されることを確認します。

ステップ 10　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 11　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がないことを確認します。

予測結果

次のテスト結果が予想されます。

- マルチパス ソフトウェアが冗長ホスト リンクへのフェールオーバーを処理するため、リンク障害によってトラフィックは停止しません。
- 障害発生時と復元時のトラフィックの損失は最小限です。
- ホスト ポートのリセットからシステムが完全に復元されます。
- 障害と復元が検出され、デバイスから管理アプリケーション サーバ（Fabric Manager）に報告されます。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

リンク障害（ポートのシャットダウン）（Fujitsu サーバから MDS へ）テストに合格しました。

リンク障害（ポートのシャットダウン）（MDS から Hitachi ストレージへ）

このテストでは、マルチパス ソフトウェアが冗長パスのあるホストでディセーブルの場合に、ポートのシャットダウンに対するファブリックおよびストレージの復元力を確認します。

テストの設定

ストレージ トラフィックが、Fujitsu ホスト（Windows）から Hitachi ストレージ アレイに対して生成されます。トラフィックが冗長接続に再ルーティングされることを確認するため、テスト ホストのポートに面する 1 つのストレージがディセーブル化されます。ホスト ポートがイネーブル化されたときに、復元が完全かどうかが確認されます。すべての設定と確認は、Fabric Manager でチェックしながら CLI を介して実行されます。

テスト手順

リンク障害（ポートのシャットダウン）（MDS から Hitachi ストレージへ）テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　ホストが両方の冗長パスそれぞれから 2 つの LUN を参照できることを確認します。

ステップ 3　Fujitsu テスト ホスト（Windows）から特定のストレージ アレイに対してストレージ トラフィックを生成します。

ステップ 4　ストレージ側に面するポートのスイッチ リンクをシャットダウンします。

ステップ 5　シャットダウンが検出され、管理アプリケーションに報告されることを確認します。

ステップ 6　いくつかの最小限の損失後に、トラフィックが冗長パス上で完全に流れることを確認します。

ステップ 7　リンクを再イネーブル化し、問題なく復元されることを確認します。

ステップ 8　ストレージ トラフィック フローが、再イネーブル化されたリンクで復元されることを確認します。

ステップ 9　リンクの復元が検出され、デバイスから管理アプリケーションに報告されることを確認します。

ステップ 10　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 11　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がないことを確認します。

予測結果

次のテスト結果が予想されます。

- リンク障害によってトラフィックは停止しません。
- 障害発生時と復元時のトラフィックの損失は最小限です。
- ホスト ポートのリセットからシステムが完全に復元されます。
- 障害と復元が検出され、デバイスから管理アプリケーション サーバ（Fabric Manager）に報告されます。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

リンク障害（ポートのシャットダウン）（MDS から Hitachi ストレージへ）テストに合格しました。

ファブリックでの VSAN の停止（VSAN SUSPEND）

このテストでは、VSAN の停止によって、ファブリック ノードに接続されたストレージ アレイに接続するホストのパスが失われる以外に、アクティブなサービスとストレージ 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

ストレージ トラフィックが、テスト ホスト（Windows および Linux）からストレージ アレイに対して生成されます。ファブリック ノードの VSAN の 1 つが削除され、ストレージに接続されたホストについて、トラフィックの再ルーティングがファブリックの冗長 VSAN にあるパスを通過して行われることが確認されます。ファブリック ノードのストレージに接続されたホストがチェックされ、中断のないことが確認されます。すべての確認は、CLI と Fabric Manager を介して実行されます。

テスト手順

ファブリックでの VSAN 停止（VSAN SUSPEND）テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　Fujitsu テスト ホスト（Windows）から Hitachi ストレージ アレイに対してストレージ トラフィックを生成します。

ステップ 3　ストレージ トラフィックがファブリックを通過するファブリック ノードの VSAN の 1 つを停止し、約 15 ～ 30 秒後にオンラインに戻します。

```
(config-vsan-db)# vsan <1-4093> suspend
.
.
(config-vsan-db)# no vsan <1-4093> suspend
```

ステップ 4　ファブリック ノードで VSAN の損失が検出され、管理アプリケーションに報告されることを確認します。

ステップ 5　ストレージ ポートに接続するホストに対するパスの損失以外に、トラフィック フローがファブリック ノードの損失の影響を受けていないことを確認します。

ステップ 6　問題なく復元していることを確認します。

ステップ 7　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 8　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- 冗長 VSAN があるため、ファブリック ノードの VSAN が完全に損失してから復元しても、ホストの I/O トラフィックは停止しません。
- 障害が発生した VSAN と同じファブリックでは、ホスト I/O トラフィックは影響を受けません。
- システムは、ファブリックの VSAN の損失から完全に復元されます。
- ファブリック VSAN の損失が検出され、デバイスから管理サーバ（Fabric Manager）に報告されます。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

ファブリックでの VSAN の停止（VSAN SUSPEND）テストに合格しました。

CHAPTER 6

アプリケーション

ここで説明する内容は、次のとおりです。

- 「基本的な Exchange の確認」
- 「ハイ アベイラビリティ」

基本的な Exchange の確認

ここで説明する内容は、次のとおりです。

- 「基本的なメール交換の確認」

基本的なメール交換の確認

このテストでは、Microsoft Exchange アプリケーション展開の機能を確認します。クライアントからアプリケーション サーバに対して、Microsoft Outlook クライアントベースのトラフィックを送信するテストを行います。

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 クライアントの Outlook が、メールを適切に送受信できるように設定されていることを確認します。

ステップ 2 ping を使用して、サーバに到達可能であることを確認します。

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

ユーザは問題なくメールを送受信できます。

結果

次のテスト結果が予測されます。

- 基本的なメール交換の確認テストに合格しました。

ハイ アベイラビリティ

ここで説明する内容は、次のとおりです。

- 「Exchange クラスタ プライマリ ホストの電源障害」
- 「Exchange クラスタ プライマリ ホストの取り外し（シャーシからのブレード サーバの取り外し）」

Exchange クラスタ プライマリ ホストの電源障害

このテストでは、サーバをシャットダウンすることで、物理アプリケーション ホストの電源障害が発生したときの Exchange の機能を確認します。15 分間、クライアントからアプリケーション サーバに対して Exchange トラフィックを送信するテストを行います。

テスト手順

Exchange クラスタ プライマリ ホストの電源障害テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　Exchange トラフィックをアプリケーション サーバに送信するように Loadgen が設定されていることを確認します。

ステップ 3　15 分間のテスト トラフィックを開始します。

ステップ 4　2 分間以上、Exchange クラスタ プライマリ ホストの電源を切ることで、コンポーネントの障害を発生させます。

ステップ 5　すべての新しい接続がもう一方のクラスタ 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 6　クラスタ プライマリ ホストに電源を入れます。

ステップ 7　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 8　プライマリ クラスタ ホストがすべての新しい接続を提供していることを確認します。

ステップ 9　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 10　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- 物理ホストに接続している既存のトラフィックは失敗します。
- フェールオーバーが発生すると、もう一方のクラスタ ノードによって新しい接続が提供されます。
- 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は新しい接続を受け入れます。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

Exchange クラスタ プライマリ ホストの電源障害テストに合格しました。

Exchange クラスタ プライマリ ホストの取り外し（シャーシからのブレード サーバの取り外し）

このテストでは、物理アプリケーション ホストを取り外したとき（ブレード サーバをシャーシから取り外したとき）の Exchange の機能を確認します。15 分間、クライアントからアプリケーション サーバに対して Exchange トラフィックを送信するテストを行います。2 分間、シャーシからプライマリ ホストを取り外して、トラフィックを確認します。

Exchange 2007 用の Microsoft Load Generator はストレス モードで 15 分間、2 ユーザに対して実行されるように設定されています。メールボックス サーバのハイ アベイラビリティの確保のため、MS Exchange 2007 はシングル コピー クラスタを使用して実装されています。

テスト手順

Exchange クラスタ プライマリ ホストの取り外しテストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　Exchange トラフィックをアプリケーション サーバに送信するように Loadgen が設定されていることを確認します。

ステップ 3　15 分間のテスト トラフィックを開始します。

ステップ 4　2 分間、シャーシから Exchange クラスタ プライマリ ノード（ブレード サーバ）を取り外します。

ステップ 5　すべての新しい接続がもう一方のクラスタ 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 6　2 分後、ブレード サーバをシャーシに取り付け直します。

ステップ 7　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 8　プライマリ クラスタ ホストがすべての新しい接続を提供していることを確認します。

ステップ 9　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 10　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- 物理ホストに接続している既存のトラフィックは失敗します。
- フェールオーバーが発生すると、もう一方のクラスタ ノードによって新しい接続が提供されます。
- 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は新しい接続を受け入れます。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

Exchange クラスタ プライマリ ホストの取り外しテストに合格しました。

CHAPTER 7

ブレード サーバ

ここで説明する内容は、次のとおりです。

- 「基本的な接続と設定」
- 「ハイ アベイラビリティ」

基本的な接続と設定

ここで説明する内容は、次のとおりです。

- 「NIC チーミング設定」
- 「Cisco ブレード スイッチ 3040 と Nexus 5020 の間のレイヤ 2 トランク設定」
- 「Cisco ブレード スイッチ 3040 と Nexus 5020 の間の L2 ポート チャネル設定」
- 「Cisco ブレード スイッチ 3040 および Nexus 5020 での LACP プロトコルによる L2 ポート チャネル」
- 「Cisco ブレード スイッチ 3040 の LST 機能」
- 「ブレード スイッチの STP 設定」

NIC チーミング設定

NIC チーミングとは、複数の物理 NIC を 1 つの論理 NIC にグループ化するプロセスです。この論理 NIC は、ネットワークの耐障害性と送信のロード バランスに使用できます。この NIC のグループ化プロセスはチーミングと呼ばれます。NIC チーミングの目的は、耐障害性とロード バランスです。

このテストは、NIC チーミングを Fujitsu ブレード サーバに設定する場合に使用されます。このサーバは、Intel PRO ネットワーク インターフェイス カードを搭載し、Windows Server 2008 Enterprise Edition を実行しています。NIC チーミングは、耐障害性モードで行われます。開始前に、Intel の Advance Network Service Driver がインストールされていることを確認します。

テスト手順

NIC チーミング設定テストの手順は次のとおりです。

ステップ 1 Advanced Network サービス チーミング ソフトウェアがサーバにインストールされていることを確認します。

ステップ 2 サーバ デスクトップから、[Start] > [Network] を選択します。

ステップ 3　[Network] を右クリックします。
[Properties] オプションがあるボックスが表示されます。

ステップ 4　[Properties] をクリックします。
Manage Network Connection へのリンクがある新しいウィンドウが表示されます。

ステップ 5　[Manage Network Connection] をクリックします。

ステップ 6　使用できるネットワーク接続アダプタが表示されます。

ステップ 7　ネットワーク アダプタを右クリックします。
ローカル エリア接続のプロパティ ボックスが表示されます。

ステップ 8　[Configure] タブを選択します。

ステップ 9　[Teaming] タブを選択します。

ステップ 10　[New team] をクリックします。
チーミングに使用できるすべてのアダプタが表示されます。

ステップ 11　チーミングするアダプタを選択し、アダプタの耐障害性としてチームの種類を選択します。

ステップ 12　プロセスを完了すると、論理 NIC が作成されます。

ステップ 13　IP の追加、マスク、およびゲートウェイを使用して、この論理 NIC を設定します。

ステップ 14　ping を使用してチーミングが機能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。

- NIC チーミングの設定後に論理 NIC が作成され、適切に動作します。

結果

NIC チーミング設定テストに合格しました。

Cisco ブレード スイッチ 3040 と Nexus 5020 の間のレイヤ 2 トランク設定

トランク ポートは複数の VLAN トラフィックを伝送できます。このテストでは、Cisco ブレード スイッチ 3040 とアクセス スイッチ Nexus 5020 の間を接続するポート チャネル リンクおよびポートは、L2 トランクです。このテスト ケースは、L2 トランク ポートの設定とその確認に使用されます。

テスト手順

ブレード スイッチと Nexus 5020 の間のレイヤ 2 トランク設定テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　Cisco ブレード スイッチ 3040（JVSL-A-CBS-01 と JVSL-A-CBS-02）でコマンドを発行して、インターフェイス ギガビット 0/11 および 0/13 をトランク ポートとして設定します。

```
Switchport mode trunk
switchport trunk allowed vlan 10,20,30,100
No shutdown
```

ステップ 3　コマンドを発行して、ポートがトランク ポートとして動作していることを確認します。

```
interface giga bit ethernet 0/11 switchport
interface giga bit ethernet 0/13 switchport
```

管理モードと運用モードはトランクにする必要があります。

ステップ 4　この段階でアクセス スイッチ（JVSL-A-ACC-N5K-01 と JVSL-A-ACC-N5K-02）にログインし、次のコマンドを発行して、ポート イーサネット 1/9 およびイーサネット 1/11 をトランク ポートとして設定します。また、インターフェイス速度を 1 GB に設定します。インターフェイスのデフォルト速度は 10 GB です。

```
Switchport mode trunk
switchport trunk allowed vlan 10,20,30,100
Speed 1000
```

ステップ 5　コマンドを発行して、ポートがトランク ポートとして動作していることを確認します。

```
show interface Ethernet 1/9 switchport
show interface Ethernet 1/11 switchport
```

運用モードはトランクにする必要があります。

ステップ 6　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 7　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がないことを確認します。

予測結果

次のテスト結果が予想されます。

- ブレード スイッチとアクセス スイッチ間のリンクは、トランク リンクとしてアップ状態になります。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

Cisco ブレード スイッチ 3040 および Nexus 5020 間のレイヤ 2 トランク設定テストに合格しました。

Cisco ブレード スイッチ 3040 と Nexus 5020 の間の L2 ポート チャネル設定

このテストは、ブレード スイッチ（JVSL-A-CBS-01 と JVSL-A-CBS-02）とアクセス スイッチ（JVSL-A-ACC-N5K-01 と JVSL-A-ACC-N5K-02）の間で L2 ポート チャネルを設定するために使用されます。

テスト手順

ブレード スイッチ 3040 と Nexus 5020 の間の L2 ポート チャネル設定テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　コマンドを発行して、ブレード スイッチ（JVSL-A-CBS-01 と JVSL-A-CBS-02）およびアクセス スイッチ（JVSL-A-ACC-N5K-01 and JVSL-A-ACC-N5K-02）でトランク モードを使用してポート チャネル インターフェイスを作成します。

```
switchport mode trunk
```

ステップ 3　ブレード スイッチおよびアクセス スイッチでコマンドを使用して、ポート チャネル グループにインターフェイスを割り当てます。
`channel-group number mode on`

ステップ 4　`show port-channel summary` コマンドを発行して、ポート チャネルが適切に設定されていることを確認します。このコマンドを実行すると、ポート チャネルに属するポートや、そのポートがアップ状態かダウン状態かなどの情報が表示されます。

ステップ 5　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 6　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がないことを確認します。

予測結果

次のテスト結果が予想されます。

- ブレード スイッチとアクセス スイッチ間のポート チャネルは、L2 トランク リンクとしてアップ状態になります。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

ブレード スイッチ 3040 および Nexus 5020 間の L2 ポート チャネル設定テストに合格しました。

Cisco ブレード スイッチ 3040 および Nexus 5020 での LACP プロトコルによる L2 ポート チャネル

LACP プロトコルを使用してチャネルを形成できる方法は複数あります。相互運用性テスト トポロジで使用されるチャネルは、LACP のアクティブ モードとパッシブ モードを使用して設定されます。アクティブ モード ポートは、LACP パケットを送信することで他のポートとネゴシエーションを開始します。パッシブ モード ポートは、受信した LACP パケットに応答しますが、LACP ネゴシエーションを開始しません。

このテストでは、ブレード スイッチおよびアクセス スイッチ（Nexus 5020）間で LACP プロトコルを使用するポート チャネルが正しく形成されていることを確認しました。

テスト手順

Cisco ブレード スイッチ 3040 および Nexus 5020 での LACP プロトコルによる L2 ポート チャネル テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　コマンドを発行して、ブレード スイッチ（JVSL-A-FBS-01 と JVSL-A-FBS-02）およびアクセス スイッチ（JVSL-A-ACC-N5K-01 and JVSL-A-ACC-N5K-02）でトランク モードを使用してポート チャネル インターフェイスを作成します。
`switchport mode trunk`

ステップ 3　この時点で、コマンドを使用して、インターフェイス コンフィギュレーション モードで LACP としてプロトコルを選択します。
`channel-protocol lacp`

ステップ 4　コマンドを使用して、インターフェイスをチャネル グループに割り当てます。
```
channel-group 10 mode active
```

ステップ 5　アクセス スイッチで、次のコマンドを発行してインターフェイスをポート チャネルに割り当てます。
```
channel-group 10 mode passive
```

ステップ 6　両方のブレード スイッチで次のコマンドを使用して、インターフェイスがポート チャネルでバンドルされ、アクティブであることを確認します。
```
sh port-channel summary
sh etherchannel protocol
```

ステップ 7　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 8　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- LACP によるチャネルが適切に構築されます。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

ブレード スイッチ 3040 および Nexus 5020 での LACP プロトコルによる L2 ポート チャネル テストに合格しました。

Cisco ブレード スイッチ 3040 の LST 機能

リンクステート トラッキングはレイヤ 2 トランク フェールオーバーとも呼ばれ、サーバの NIC アダプタ チーミングと併用すると、ネットワークでレイヤ 2 の冗長性を実現できる機能です。チーミングとも呼ばれるプライマリまたはセカンダリの関係でサーバのネットワーク アダプタを設定し、プライマリ インターフェイスでリンクが失われると、接続は透過的にセカンダリ インターフェイスへと切り替えられます。スイッチでレイヤ 2 トランク フェールオーバーをイネーブルにすると、内部ダウンストリーム ポートのリンク状態は、外部アップストリーム ポートの 1 つまたは複数のリンク状態にバインドされます。

内部ダウンストリーム ポートは、サーバに接続しているインターフェイスです。外部アップストリーム ポートは、外部ネットワークに接続するインターフェイスです。ダウンストリーム ポートのセットをアップストリーム ポートのセットに関連付け、すべてのアップストリーム ポートが使用できなくなると、トランクのフェールオーバーによって、すべての関連するダウンストリーム ポートが自動的に error-disabled 状態になります。その結果、サーバのプライマリ インターフェイスはセカンダリ インターフェイスにフェールオーバーします。

テスト手順

ブレード スイッチの LST 機能テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　グローバル コンフィギュレーション モードで次のコマンドを使用して、リンク状態のトラッキングのために両方のブレード スイッチを設定します。
`link state track [1-2]`

ステップ 3　次のコマンドを使用してポート チャネル 10 をアップストリーム インターフェイスに設定します。
`link state group [1-2] upstream`

ステップ 4　次のコマンドを使用して、サーバに接続するポートをダウンストリーム インターフェイスに設定します。
`link state group [1-2] downstream`

ステップ 5　次のコマンドを使用して、アップストリーム インターフェイスとダウンストリーム インターフェイスのステータスを確認します。
`sh link state group [1-2] detail`
インターフェイスのステータスがアップ状態になります。

ステップ 6　アップストリーム インターフェイスであるポート チャネル インターフェイスをシャットダウンします。ダウンストリーム インターフェイスは err-disabled 状態になります。コマンドを使用して確認します。
`sh link state group detail`

ステップ 7　no shutdown コマンドを使用して、アップストリーム リンク状態グループに設定されたアップストリーム ポート チャネルをアップ状態に戻します。

ステップ 8　次のコマンドを発行して、ダウンストリーム ポートのステータスが接続状態に戻っていることを確認します。
`show interface status`
`show link state group detail`

ステップ 9　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 10　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がないことを確認します。

予測結果

次のテスト結果が予想されます。

- アップストリーム インターフェイスがダウン状態になると、ダウンストリーム ポートの状態は err-disable 状態に変わります。
- アップストリーム インターフェイスがアップ状態になると、ダウンストリーム ポートの状態はアップ状態に戻ります。

結果

ブレード スイッチの LST 機能テストに合格しました。

ブレード スイッチの STP 設定

このテストは、Cisco ブレード スイッチ 3040 で STP の設定を確認するために使用されます。

テスト手順

ブレード スイッチの STP 設定テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　コマンドを使用して、rapid-pvst のために両方のブレード スイッチ（JVSL-A-CBS-01 と JVSL-A-CBS-02）を設定します。

```
spanning-tree mode rapid-pvst
```

ステップ 3　両方のブレード スイッチ（JVSL-A-CBS-01 と JVSL-A-CBS-02）で次のコマンドを使用して、スパニングツリー Port Fast としてサーバに接続するポートを設定します。

```
spanning-tree portfast
```

ステップ 4　コマンドを使用して、両方のブレードの STP 設定を確認します。

```
show spanning-tree vlan 100
```

集約スイッチ JVSL-A-AGG-N7k-01 はルート スイッチにする必要があります。

ステップ 5　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 6　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がないことを確認します。

予測結果

次のテスト結果が予想されます。

- スイッチは rapid-pvst モードで実行され、ルート スイッチは集約の JVSL-A-AGG-N7k-01 になります。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

ブレード スイッチの STP 設定テストに合格しました。

ハイ アベイラビリティ

ここで説明する内容は、次のとおりです。

- 「ブレード スイッチのリロード」
- 「ブレード スイッチと Nexus 5020（LST）の間のポート チャネル障害」

ブレード スイッチのリロード

このテストでは、ブレード スイッチ デバイスで障害が発生したときのアプリケーションの機能を確認します。クライアントからアプリケーション サーバに対して交換アプリケーション トラフィックを送信し、スイッチで障害を発生させるテストが行われます。

このテストでは、アプリケーション トラフィックは 15 分間実行されます。また、アクティブにトラフィックを渡すブレード スイッチの 1 つで障害が発生し、復元されます。NIC チーミングが設定されているため、トラフィックは影響を受けません。トラフィックはブレード スイッチを通過し続けるため、エンド ユーザには最小限の影響しかないことが確認されました。

テスト手順

ブレード スイッチのリロード テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　Loadgen を使用して、15 分間のテスト トラフィックを開始します。

ステップ 3　reload コマンドを発行して、アクティブにトラフィックを渡しているブレード スイッチの 1 つをリロードします。

ステップ 4　トラフィックが完了したら、結果を保存して分析し、エンド ユーザ エクスペリエンスが予測どおりであることを確認します。トラフィックには最小限の影響しかありません。

ステップ 5　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 6　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- コンポーネントの障害発生後も、アプリケーション トラフィックが継続して渡されます。
- エンド ユーザに対する影響は最小限です。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

ブレード スイッチのリロード テストに合格しました。

ブレード スイッチと Nexus 5020（LST）の間のポート チャネル障害

このテストでは、リンク状態のトラッキングの機能を確認します。ブレード スイッチとアクセス スイッチ間のポート チャネル（LS グループのアップストリーム インターフェイス）の障害時に、トラフィックは他のパスに切り替えられます。

テスト手順

ブレード スイッチと Nexus 5020（LST）の間のポート チャネル障害テストの手順は次のとおりです。

ステップ 1　テスト ネットワーク デバイスの初期ステータスを収集するバックグラウンド スクリプトを開始します。ネットワーク デバイスのメモリおよび CPU の使用率を監視します。

ステップ 2　Loadgen を使用して、クライアントからサーバへの Exchange トラフィックを開始します。

ステップ 3　ブレード スイッチで、リンク状態のトラッキングのためにアップストリーム インターフェイスであるポート チャネル インターフェイスをシャットダウンします。

ステップ 4　ダウンストリーム ポート ステータスが err-disabled 状態に変わることを確認します。

ステップ 5　ブレード サーバで、プライマリ NIC がディセーブル状態に変わり、セカンダリ NIC がアクティブ状態に変わることを確認します。すべてのトラフィックはセカンダリ NIC 経由になります。

ステップ 6　ネットワーク デバイスの最終ステータスを収集するバックグラウンド スクリプトを停止し、エラーを分析します。

ステップ 7　メモリおよび CPU に重大な影響、継続的な影響、または許容できない影響がなかっ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。

- ブレード スイッチのイネーブルなリンク状態トラッキングとアップストリーム リンクがダウン状態になっても、トラフィックのドロップはないか、最小限です。
- トラフィックは別のパスにスイッチオーバーされます。
- テスト時にデバイスの CPU またはメモリに許容できない影響がありません。

結果

ブレード スイッチと Nexus 5020（LST）間のポート チャネル障害テストに合格しました。

APPENDIX A

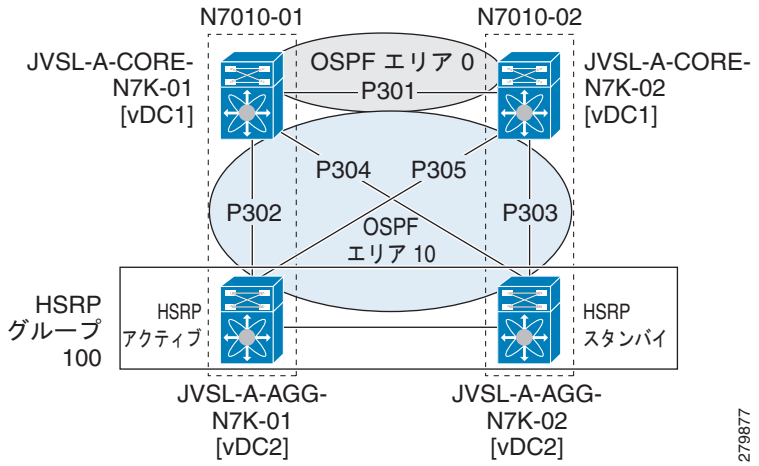
IP インフラストラクチャの実装

ここでは、レイヤ 2 およびレイヤ 3 トポロジで示す実装の詳細について説明します。

- 「レイヤ 3 トポロジの実装」
- 「レイヤ 2 トポロジの実装」

レイヤ 3 トポロジの実装

図 A-1　　レイヤ 3 トポロジ



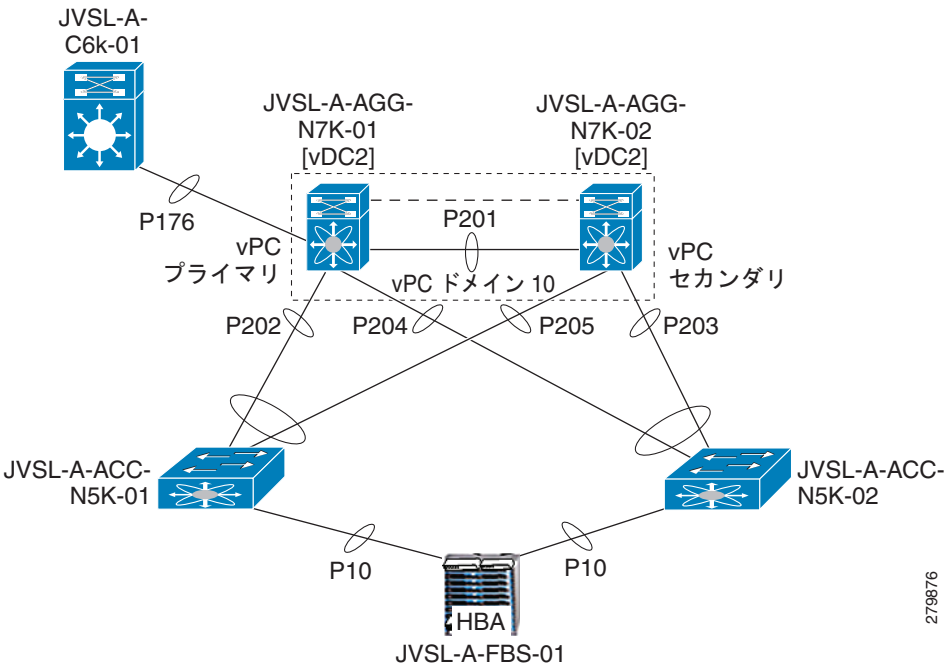
レイヤ 3 トポロジには 2 つの Nexus 7010 デバイスがあります。

- 各 Nexus 7010 スイッチで 2 つの Virtual Device Context（VDC）がイネーブルになっています。VDC はコア（JVSL-A-CORE-N7k-01、JVSL-A-CORE-N7k-02）および集約（JVSL-A-AGG-N7K-01、JVSL-A-AGG-N7K-02）レイヤ デバイスとして動作します。
- コアおよび集約レイヤ デバイスは、L3 ポート チャネルを介して接続されます。5 つの L3 ポート チャネル（P301-P305）があり、ポート チャネルの相互接続に使用されます。各 L3 ポート チャネルは、リンクの冗長性のために 2 つの 10 GB インターフェイスにグループ化されます。すべての L3 ポート チャネルのチャネリング モードはオンに設定されます。

- ルーティング プロトコル OSPF がコアおよび集約デバイスで実行されます。デバイス JVSL-A-CORE-N7K-01 および JVSL-A-CORE-N7K-02 は、エリア 0 と CORE 10 の間の Area Border Router（ABR; エリア境界ルータ）として機能します。この 2 つのコア レイヤ デバイス間のリンクは OSPF エリア 0 にあります。
- コア レイヤ デバイスおよび集約レイヤ デバイス間のリンクは、OSPF エリア 10 にあります。
- デバイス JVSL-A-AGG-N7K-01 と JVSL-A-AGG-N7K-02 は、デフォルト ゲートウェイとして動作し、Hot Standby Router Protocol（HSRP）を介して冗長性が設定されます。HSRP デフォルト ゲートウェイは、レイヤ 2 ドメインの VLAN に定義されている各サブネット用に用意されています。設定によって、JVSL-A-AGG-N7K-01 がアクティブな HSRP Router であり、JVSL-A-AGG-N7K-02 はスタンバイです。これら 2 つの各デバイスの各 VLAN にプリエンプトが設定されます。

レイヤ 2 トポロジの実装

図 A-2　レイヤ 2 トポロジ



テスト トポロジには、レイヤ 2 で動作する次の 4 つの主要デバイスがあります。

JVSL-A-AGG-N7K-01

JVSL-A-AGG-N7K-02

JVSL-A-ACC-N5K-01

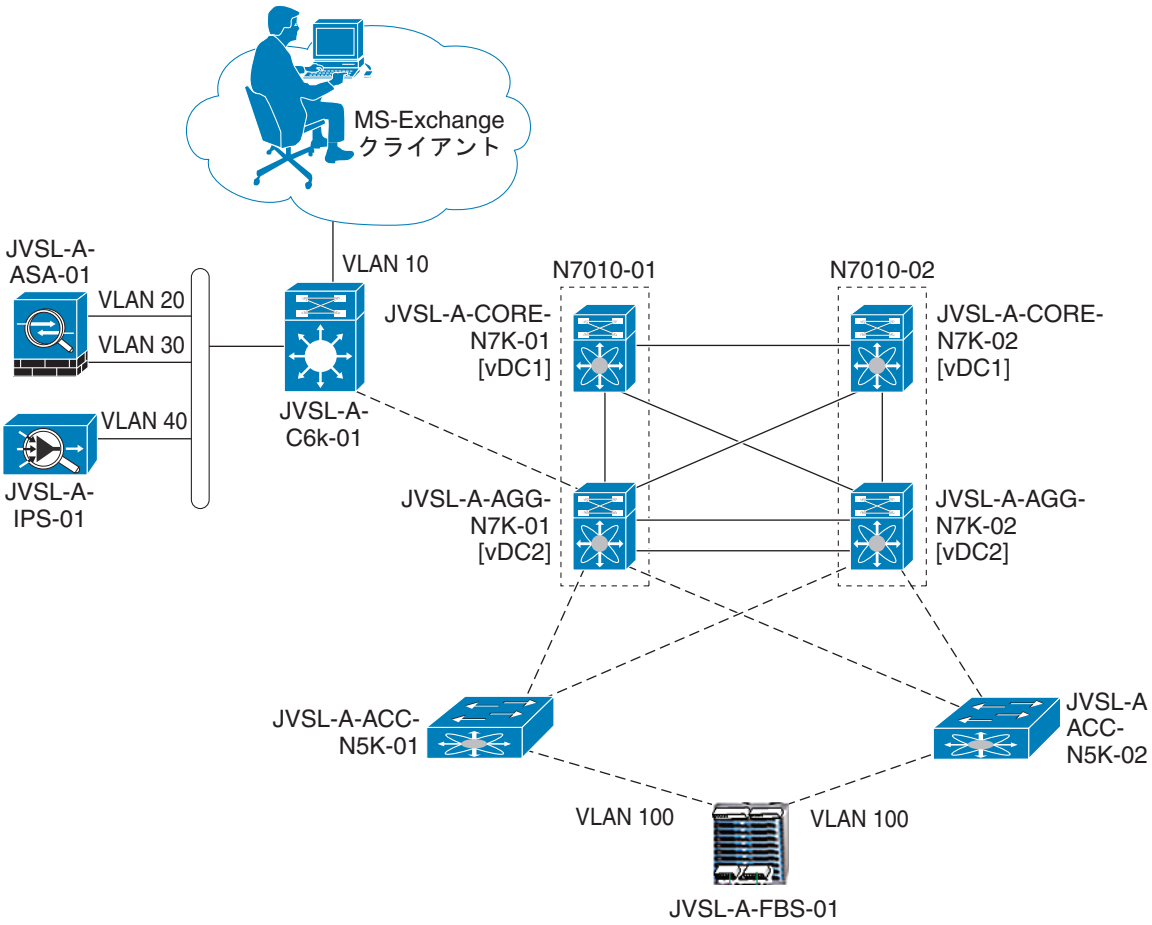
JVSL-A-ACC-N5K-02

- すべてのスイッチ間リンクは L2 ポート チャネルです。5 つの L2 ポート チャネル（P201-P205）は、L2 デバイスの相互接続に使用されます。2 つの 10 ギガビット イーサネット ポートはまとめてバンドルされ、トランク リンク（802.1Q）として設定されている L2 ポート チャネルから、複数の VLAN を伝送できます。

（注）　注意：2 つの 10 ギガビット ポートは、ポート チャネル リンクの冗長性のために使用されます。

- Virtual Port Channel（vPC）は、レイヤ 2 のマルチパスおよび冗長性のために L2 デバイスで実装されます。デバイス JVSL-A-AGG-N7K-01 と JVSL-A-AGG-N7K-02 は、vPC ドメイン 10 の vPC ピア デバイスとして設定されます。すべてのアクセス スイッチ（ACC-N5K）アップリンク L2 ポート チャネルは、vPC メンバー ポートとして動作します。
- L2 ポート チャネル（P201）は、vPC ピアリンクのために 2 つの集約スイッチ（JVSL-A-AGG-N7K-01、JVSL-A-AGG-N7K-02）の間に設定され、L3 リンクは VRF による vPC キープアライブ リンクとして設定されます。この設定により、JVSL-A-AGG-N7K-01 がプライマリ vPC ピアとなり、JVSL-A-AGG-N7K-02 がセカンダリとなります。
- STP プロトコル Rapid PVST+ は、vPC のフォールバックとしてすべてのレイヤ 2 デバイスに設定されます。集約レイヤ デバイス AGG-N7K-01 は、レイヤ 2 ドメインのすべての VLAN についてプライマリ STP として設定され、AGG-N7K-02 は、セカンダリ STP ルートとして設定されます。
- ブレード サーバ [FBS-01] は、ポート チャネル p10 を使用し、ブレード スイッチ [JVSL-A-CBS-01 と JVSL-A-CBS-02] を介してアクセス スイッチ [JVSL-A-ACC-N5K-01、JVSL-A-ACC-N5K-02] に接続されます。
- 集約レイヤ デバイスは、ネットワークのデータ トラフィックに複数のサービスを提供します。Cat6506e Service-Switch は、L2 ポート チャネル（P176）を介して集約レイヤ デバイス [JVSL-A-AGG-N7K-01] に接続します。これによってレイヤ 4 ～ 7 サービスが提供されます。
- VLAN 100 は、サーバ フォーム（ブレード サーバ HBS）データ トラフィックを提供します。
- 4 つの VLAN（VLAN10–40）は、サービス トラフィックの分離に使用されます。

図 A-3　VLAN を使用した L2/L3 トポロジの詳細



APPENDIX **B**

Storage Area Networking（SAN）の実装

ここでは、相互運用性テスト SAN トポロジで示される MDS スイッチと Hitachi ストレージの実装の詳細について説明します。

- 「MDS 9140 の実装」
- 「Hitachi USP VM の実装」

MDS 9140 の実装

図 B-1　　SAN の論理情報

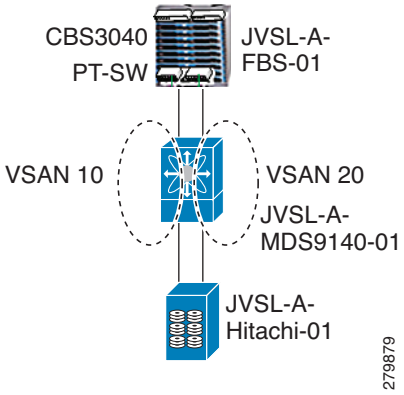


図 B-1 には、ホストとストレージの接続用の単一のスイッチにデュアル ファブリック設定を実装するために使用する Virtual SAN（VSAN; 仮想 SAN）が含まれます。個別の VSAN によって、トラフィックをストレージ フレームごとに論理的に分離しやすくなります。

Hitachi USP VM の実装

次の表に、相互運用性テストに使用される Hitachi ストレージに関する詳細情報を示します。

表 B-1　Hitachi ソフトウェア / ファームウェアの情報

プラットフォーム	ソフトウェア コンポーネント	機能	場所	バージョン
USP VM	Windows Vista Business	オペレーティング システム	フレーム	2007 SP1
	Storage Navigator	設定およびモニタリング アプリケーション インターフェイス	フレーム	60-06-12-00/00
	MPIO	マルチパス	Windows host（x86_64）	3.0

表 B-2　Hitachi ハードウェア情報

プラットフォーム	ソフトウェア コンポーネント	機能	説明
USP VM	フレーム	1	シリアル 36361
	キャッシュ	16,384 MB	
	ディスク	16@300 GB	
	ストレージ プロセッサ	2	
	ファイバ ポート	8（SP あたり 4 FC）@4Gbps	

表 B-3　Hitachi ストレージの実装

RAID レベル	合計空き容量（GB 単位）	使用可能な容量（GB 単位）
RAID 5（3D+1P）	1200（300 × 4）	900
RAID 5（7D+1P）	2400（300 × 8）	2100
RAID 5（7D+1P）		
RAID 1（2D+2D）	1200（300 × 4）	600
RAID 1（2D+2D）		

Hitachi USP VM には 16 個の FC ディスクがあり、それぞれのサイズは 300 GB です。このテストでは、ストレージを 2 つの RAID グループ（RAID 5 と RAID 1）に分割しました。さらに RAID 5 には 3D+1P と 7D+1P という 2 種類があります。この D はディスク、P はパリティを示します。

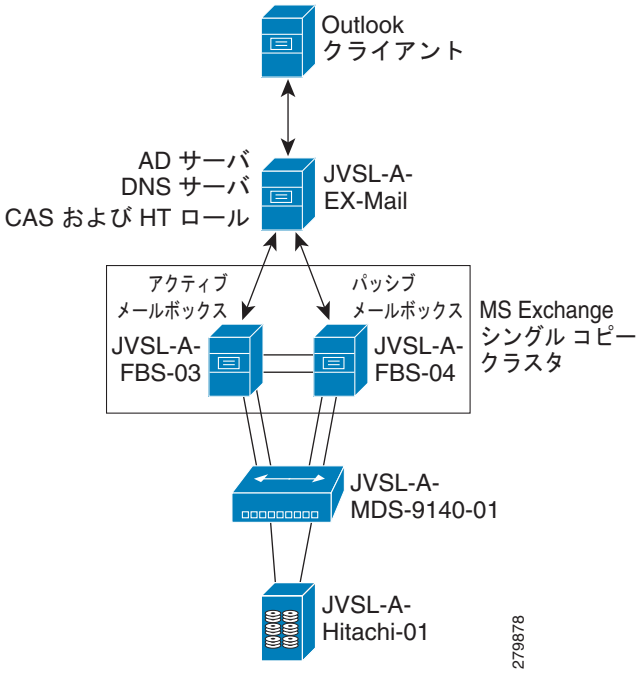
MS Exchange 実装の場合、Fujitsu ブレード サーバについて、100 GB、100 GB、および 30 GB LUN をそれぞれメール データベース、ログ ファイル、クラスタ コンフィギュレーション ファイルに関連付けました。メール データベースおよびクラスタ構成の場合、RAID 5 グループの LUN を使用しました。またログ ファイルは RAID グループ 1 の LUN に保存されました。各ブレード サーバには、同じ LUN について 2 つのパスがあります。マルチパス ソフトウェアがインストールされているため、同時に参照できるのは 1 つのパスのみです。そのため、ハードウェアまたはソフトウェアの問題によって一方のパスがダウン状態になると、もう一方のパスが引き継ぎ、接続は維持されます。

APPENDIX C

MS Exchange の実装

このトポロジは、JVSL データセンター内にシングル コピー クラスタとして実装された 1 つの Windows Exchange 2007 から構成され、これにより JVSL-EX-MBX と呼ばれるクラスタ化されたメールボックス サーバとして機能します。このクラスタ内では、JVSL-A-FBS-03 はアクティブ メールボックス サーバとして動作し、JVSL-A-FBS-04 はパッシブ メールボックス サーバとして動作します。Exchange 実装では、JVSL-A-EX-MAIL サーバは HUB Transport ロールおよび CAS ロールのインストールに使用されます。このサーバはクラスタリングの一部に含まれるわけではありませんが、メールボックス クラスタリング サーバにサービスを提供します。また、MS Exchange 2007 に対して Active Directory および DNS サービスも提供します。

図 C-1　　MS-Exchange トラフィック フロー



コンポーネントには以下が含まれます。

Microsoft Exchange Server 2007 SP1

Hub Transport ロール : 組織内および組織外のすべてのインテリジェント メッセージ ルーティング、配信、および制御について中心的な役割を果たします。

CAS ロール : OWA、Outlook Anywhere、および ActiveSync クライアントを含む多様なクライアント エンドポイントに対してメッセージング アクセスを提供します。

メールボックス ロール : メールボックス（MBX）ロールは、すべてのユーザのメッセージング データのデータベースです。Outlook など、MAPI ベースのクライアントにアクセスを提供します。MBX サーバは、ハイ アベイラビリティを提供するためにクラスタ化されます。シングル コピー クラスタはメールボックス サーバを展開するために使用されます。クラスタ化されたメールボックス サーバは「JVSL-EX-MBX」と呼ばれます。

クラスタ内のサーバには、3 つのデータ LUN に対する 2 つの冗長 FC パスがあります。LUN には、クラスタ設定、Exchange データベース、およびログ ファイルが含まれます。3 つのデータ LUN は Hitachi USP-VM ストレージからプロビジョニングされます。

Exchange データは次のように 2 つの LUN に分散されます。

- E : Exchange データベース ファイル（100 GB）
- G : Exchange ログ ファイル（100 GB）

各クラスタ ノードからは、クラスタ クォーラム制御ディスク（30 GB）とともにこれらのファイルを参照できます。Windows Server 2008 の MPIO 機能は、マルチパス ソフトウェアとして使用されます。

jvsl.com ドメインを保持する 1 つのドメイン コントローラ サーバは、ドメイン サービスを提供します。

他のブランチの Microsoft Outlook 2003 クライアントは、MAPI プロトコルを使用して MS Exchange Server にアクセスします。

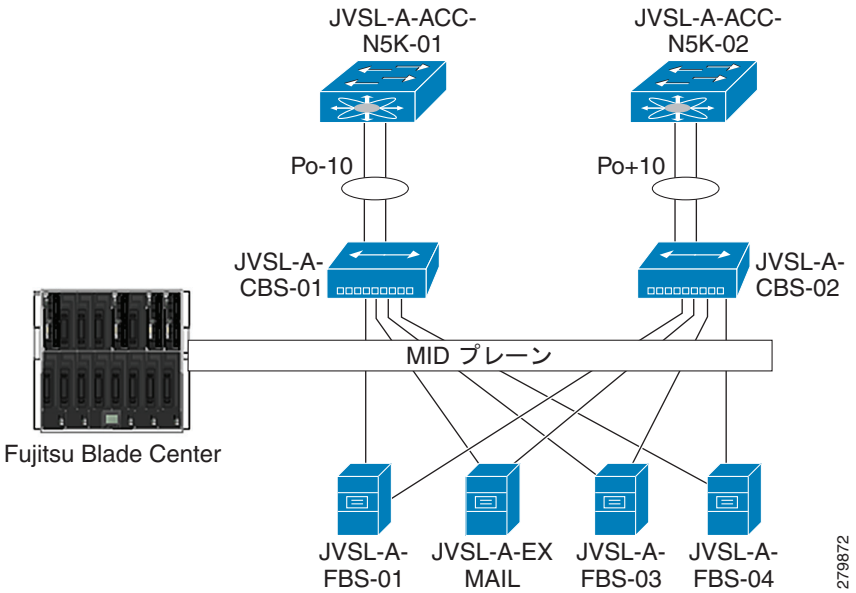
APPENDIX D

ブレード サーバの実装

Fujitsu Blade Center は 4 つの BX620 S5 ブレード サーバから構成されます。各サーバは、2 つの Intel Xeon E5560 プロセッサ 2.80 GHz、16 GB のメモリ、146GB × 2 SAS ハード ディスク、およびデュアル ポート Emulex HBA から構成されます。これらは BX600 S3 シャーシのスロット 4、5、6、および 7 に挿入されます。Windows Server 2008 Enterprise Edition SP2 を搭載した 2 つのサーバはクラスタ化され、Microsoft Exchange 2007 を実行します。NIC チーミングは、アプリケーション サーバがサーバ NIC レイヤで冗長性を提供するために使用されます。Cisco 3040 ブレード スイッチに統合された Fujitsu PRIMERGY BX600 S3 ブレード サーバは、アクセス レイヤ スイッチにネットワーク接続を提供します。各ブレード スイッチは、Access Layer Nexus 5020 スイッチに対する dual-port ether-channel を使用して設定されます。

図 D-1 に、Fujitsu Blade Center 内の Cisco ブレード スイッチを示します。これは Nexus 5020 に接続されます。

図 D-1　　ブレード サーバの実装



APPENDIX E

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 コンポーネント

コア スイッチの設定

Show Running-config

```
JVSL-A-Core-N7k-01# sh run
!Command: show running-config
!Time: Thu May  6 07:57:49 2010

version 4.2(3)
feature telnet
feature ospf
feature lacp

snmp-server context management
username admin password 5 $1$K6VUTMbk$YMdN0Cch2npju9b0rCEJh.  role vdc-admin
username cisco password 5 $1$Ji9u23jm$OirjvDB9SwY2mAAzN8HN./  role vdc-operator
username cisco role vdc-admin

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

ip domain-lookup
ip host JVSL-A-CORE-N7K-01 10.78.240.3
snmp-server user admin vdc-admin auth md5 0x4bb444f53704f3d53a55a815c1544170 pri
v 0x4bb444f53704f3d53a55a815c1544170 localizedkey
[7m--More--[m snmp-server user cisco vdc-operator auth md5
0x4bb444f53704f3d53a55a815c1544170
```

```
priv 0x4bb444f53704f3d53a55a815c1544170 localizedkey
snmp-server user cisco vdc-admin
snmp-server host 10.77.213.144 traps version 2c public
snmp-server host 10.77.202.210 traps version 2c public
snmp-server enable traps ospf
snmp-server enable traps snmp authentication
snmp-server community public group vdc-admin

vrf context management
  ip route 0.0.0.0/0 10.78.240.1
vlan 1
port-profile type port-channel L3_PC


interface port-channel301
  description L3_PC_TO_CORE_N7K_02
  ip address 172.16.1.5/30
  ip router ospf 10 area 0.0.0.0

interface port-channel302
  description L3_PC_TO_AGG_N7K_01
  ip address 172.16.1.9/30
  ip router ospf 10 area 0.0.0.10

interface port-channel304
  description L3_PC_TO_AGG_N7K_02
  ip address 172.16.1.17/30
  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
```

```
[7m--More--[m  [K
interface Ethernet1/4

interface Ethernet1/5

interface Ethernet1/6

interface Ethernet1/7

interface Ethernet1/8

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
[7m--More--[m   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
  ip address 10.78.240.3/24
logging server 10.77.213.144
logging server 10.77.202.210
router ospf 10
```

Show Version

```
JVSL-A-CORE-N7K-01# sh ver
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

Software
  BIOS:      version 3.17.0
  loader:    version N/A
  kickstart: version 4.2(3)
  system:    version 4.2(3)
  BIOS compile time:       03/23/08
  kickstart image file is: bootflash:/n7000-s1-kickstart.4.2.3.bin
  kickstart compile time:  10/26/2009 0:00:00 [12/18/2009 02:46:51]
  system image file is:    bootflash:/n7000-s1-dk9.4.2.3.bin
  system compile time:     10/26/2009 0:00:00 [12/18/2009 03:16:03]
[7m--More--[m  [K

Hardware
  cisco Nexus7000 C7010 (10 Slot) Chassis ("Supervisor module-1X")
  Intel(R) Xeon(R) CPU         with 4129600 kB of memory.
  Processor Board ID JAF1336AADS

  Device name: N7k-01
  bootflash:    2030616 kB
  slot0:              0 kB (expansion flash)

Kernel uptime is 48 day(s), 22 hour(s), 34 minute(s), 52 second(s)

Last reset at 124234 usecs after  Thu Mar 18 09:26:44 2010

  Reason: Reset Requested by CLI command reload
  System version: 4.1(4)
  Service:
```

```
plugin
  Core Plugin, Ethernet Plugin
```

Show Running-config

```
JVSL-A-Core-N7k-02# sh run
!Command: show running-config
!Time: Thu May  6 08:21:31 2010

version 4.2(3)
feature telnet
feature ospf
feature lacp

snmp-server context management
username admin password 5 $1$O3n.7OTZ$c55J0SghTy09moypUZUrR.  role vdc-admin
username cisco password 5 $1$UovWA2uP$p/cJ0FWUPJhwL2QuY4hZb1  role vdc-admin

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

ip domain-lookup
ip host JVSL-A-CORE-N7K-02 10.78.240.5
hostname JVSL-A-CORE-N7K-02
snmp-server user admin vdc-admin auth md5 0x2dad17f0ee72c83df50d703c07e0ffd1 pri
v 0x2dad17f0ee72c83df50d703c07e0ffd1 localizedkey
snmp-server user cisco vdc-admin auth md5 0x2dad17f0ee72c83df50d703c07e0ffd1 pri
v 0x2dad17f0ee72c83df50d703c07e0ffd1 localizedkey
snmp-server host 10.77.213.144 traps version 2c public
snmp-server host 10.77.202.210 traps version 2c public
snmp-server enable traps ospf
snmp-server enable traps callhome event-notify
snmp-server enable traps callhome smtp-send-fail
snmp-server enable traps cfs state-change-notif
snmp-server enable traps cfs merge-failure
snmp-server enable traps aaa server-state-change
snmp-server enable traps upgrade UpgradeOpNotifyOnCompletion
snmp-server enable traps upgrade UpgradeJobStatusNotify
snmp-server enable traps feature-control FeatureOpStatusChange
snmp-server enable traps snmp authentication
```

```
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 172.16.1.6/30
  ip router ospf 10 area 0.0.0.0

interface port-channel303
  description L3_PC_TO_AGG_N7K_02
  ip address 172.16.1.13/30
  ip router ospf 10 area 0.0.0.10

interface port-channel305
  description L3_PC_TO_AGG_N7K_01
  ip address 172.16.1.21/30
  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

interface Ethernet1/5

interface Ethernet1/6

interface Ethernet1/7
```

```
interface Ethernet1/8

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

interface Ethernet7/5

interface Ethernet7/6

interface Ethernet7/7

interface Ethernet7/8

interface mgmt0
  ip address 10.78.240.5/24
logging server 10.77.213.144
logging server 10.77.202.210
router ospf 10


JVSL-A-CORE-N7K-02#
```

Show Version

```
JVSL-A-CORE-N7K-02# sh ver
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2009, Cisco Systems, Inc. All rights reserved.
```

```
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

Software
  BIOS:      version 3.17.0
  loader:    version N/A
  kickstart: version 4.2(3)
  system:    version 4.2(3)
  BIOS compile time:       03/23/08
  kickstart image file is: bootflash:/n7000-s1-kickstart.4.2.3.bin
  kickstart compile time:  10/26/2009 0:00:00 [12/18/2009 02:46:51]
  system image file is:    bootflash:/n7000-s1-dk9.4.2.3.bin
  system compile time:     10/26/2009 0:00:00 [12/18/2009 03:16:03]


Hardware
  cisco Nexus7000 C7010 (10 Slot) Chassis ("Supervisor module-1X")
  Intel(R) Xeon(R) CPU         with 4129600 kB of memory.
  Processor Board ID JAF1336AAHP

  Device name: JVSL-A-CORE-N7K-02
  bootflash:    2030616 kB
  slot0:              0 kB (expansion flash)

Kernel uptime is 48 day(s), 19 hour(s), 34 minute(s), 28 second(s)

Last reset at 873254 usecs after  Thu Mar 18 12:46:49 2010

  Reason: Reset Requested by CLI command reload
  System version: 4.1(4)
  Service:

plugin
  Core Plugin, Ethernet Plugin
JVSL-A-CORE-N7K-02#
```

集約スイッチの設定

Show Running-config

```
JVSL-A-AGG-N7K-01# sh running-config

!Command: show running-config
!Time: Thu May  6 08:05:32 2010

version 4.2(3)
feature telnet
cfs eth distribute
feature ospf
feature bgp
feature interface-vlan
feature hsrp
feature lacp
feature vpc

snmp-server context management
role distribute
username admin password 5 $1$yd/QAwKE$hQePn682Qsc2bN.oGq5r0/  role vdc-admin
username cisco password 5 $1$AWMXfHwb$N.xM3jfa1E1dd2uxU9iqt.  role vdc-admin

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

ip domain-lookup
ip host JVSL-A-AGG-N7K-01 10.78.240.4
hostname JVSL-A-AGG-N7K-01
snmp-server user admin vdc-admin auth md5 0x4bb444f53704f3d53a55a815c1544170 pr
v 0x4bb444f53704f3d53a55a815c1544170 localizedkey
snmp-server user cisco vdc-admin auth md5 0x4bb444f53704f3d53a55a815c1544170 pr
v 0x4bb444f53704f3d53a55a815c1544170 localizedkey
snmp-server host 10.77.202.72 traps version 1 public
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 1,10,30,100
spanning-tree vlan 100 priority 24576
```

```
vpc domain 10
  role priority 5
  peer-keepalive destination 172.16.1.26 source 172.16.1.25 vrf vPC


interface Vlan1

interface Vlan10
  no shutdown

interface Vlan30

interface Vlan100
  no shutdown
  description FBS_Server_VLAN
  ip address 172.16.100.2/24
  ip router ospf 10 area 0.0.0.10
  hsrp 100
    preempt delay minimum 60
    priority 150
    ip 172.16.100.1

interface port-channel176
  description L2_PC_TO_CAT6K_01
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,30,100

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

interface port-channel202
  description L2_PC_TO_ACC_N5K_01
  shutdown
  switchport
  switchport mode trunk
  vpc 10
  switchport trunk allowed vlan 10,20,30,100
```

```
interface port-channel204
  description L2_PC_TO_ACC_N5K_02
  shutdown
  switchport
  switchport mode trunk
  vpc 11
  switchport trunk allowed vlan 10,20,30,100

interface port-channel302
  description L3_PC_TO_CORE_N7K_01
  shutdown
  ip address 172.16.1.10/30
  ip router ospf 10 area 0.0.0.10

interface port-channel305
  description L3_PC_TO_CORE_N7K_02
  ip address 172.16.1.22/30
  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 10,20,30,100
  channel-group 201
  no shutdown

interface Ethernet1/10
  description LINK_TO_CORE_N7K01_e1/2
  channel-group 302 mode passive
  no shutdown

interface Ethernet1/11
  description LINK_TO_ACC_N5K_01_e1/1
  channel-group 305
  no shutdown

interface Ethernet1/12
  description LINK_TO_ACC_N5K_01_e1/1
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,30,100
```

```
  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 10,20,30,100
  channel-group 204 mode active
  no shutdown

interface Ethernet1/14

interface Ethernet1/15
  ip router ospf 1 area 0.0.0.0

interface Ethernet1/16
  no shutdown

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19

interface Ethernet1/20

interface Ethernet1/21

interface Ethernet1/22
  switchport

interface Ethernet1/23

interface Ethernet1/24
  description VPC_KEEPALIVE_TO_AGG_N7K_02_1/24
  vrf member vPC
  ip address 172.16.1.25/30
  no shutdown

interface Ethernet7/9
  description LINK_TO_AGG_N7K_02_e7/9
  switchport
```

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

interface Ethernet7/10
  description LINK_TO_CORE_N7K01_e7/1
  channel-group 302 mode passive
  no shutdown

interface Ethernet7/11
  description LINK_TO_ACC_N5K_01_e1/2
  channel-group 305
  no shutdown

interface Ethernet7/12
  description LINK_TO_ACC_N5K_01_e1/3
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,30,100
  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 10,20,30,100
  channel-group 204 mode active
  no shutdown

interface Ethernet7/14
  no shutdown

interface Ethernet7/14.5

interface Ethernet7/14.15

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_2/3
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 10,20,30,100
  channel-group 176 mode active
  no shutdown

interface Ethernet7/24
  no shutdown

interface mgmt0
  ip address 10.78.240.4/24

interface loopback2
  ip address 2.2.2.2/32
router ospf 1
  router-id 2.2.2.2
router ospf 10
router bgp 6500
  router-id 2.2.2.2
  neighbor 192.168.10.1 remote-as 6500
    address-family ipv4 unicast
ip route 172.16.10.0/24 172.16.100.25
event manager applet MonitorInterfaceShutdown
  description "Script to Monitor Interface Shutdown"
  event cli match "shutdown"
  action 1 syslog msg "Interface is shutdown"
  action 2 cli show interface ethernet7/15
event manager applet trackscript
  event track 1 state down
  action 1 syslog msg EEM_ETHERNET7/14.11_DOWN
```

```
  action 2 cli event manager run sagay2
event manager applet sagay2
  description "Script to Test Applet"
  action 1.0 cli conf t
  action 1.5 cli interface eth7/14.33
  action 2.0 cli no shutdown
  action 2.5 cli exit
event manager applet testapplet1
  event cli match "shutdown"
  action 1.0 snmp-trap strdata "TRAP_FROM_NEXUS" event-type $_event_type policy
name $_policy_name


JVSL-A-AGG-N7K-01#
```

Show Version

```
JVSL-A-AGG-N7K-01#  sh ver
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php

Software
  BIOS:      version 3.17.0
  loader:    version N/A
  kickstart: version 4.2(3)
  system:    version 4.2(3)
  BIOS compile time:       03/23/08
  kickstart image file is: bootflash:/n7000-s1-kickstart.4.2.3.bin
  kickstart compile time:  10/26/2009 0:00:00 [12/18/2009 02:46:51]
  system image file is:    bootflash:/n7000-s1-dk9.4.2.3.bin
  system compile time:     10/26/2009 0:00:00 [12/18/2009 03:16:03]


Hardware
```

```
  cisco Nexus7000 C7010 (10 Slot) Chassis ("Supervisor module-1X")
  Intel(R) Xeon(R) CPU         with 4129600 kB of memory.
  Processor Board ID JAF1336AADS

  Device name: JVSL-A-AGG-N7K-01
  bootflash:    2030616 kB
  slot0:              0 kB (expansion flash)

Kernel uptime is 48 day(s), 22 hour(s), 39 minute(s), 37 second(s)

Last reset at 124234 usecs after  Thu Mar 18 09:26:44 2010

  Reason: Reset Requested by CLI command reload
  System version: 4.1(4)
  Service:

plugin
  Core Plugin, Ethernet Plugin
JVSL-A-AGG-N7K-01#
```

Show Running-config

```
JVSL-A-ACC-N5K-01# sh run
version 4.1(3)N2(1a)
feature fcoe
feature telnet
feature interface-vlan
feature lacp
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$8XbnUhpE$q6Y7/sdy3U3ogtxSkiojP0  role network-admin
username cisco password 5 $1$o4/x7QkC$0LtHDQV6/ujTemrSHw7Cu.  role network-admin
banner motd #*****************************************  $ Unauthorized access p
rohibited $  This system belongs to JVSL-DC team*********************************
**********#

ip host JVSL-A-ACC-N5K-01 10.78.240.7
```

```
hostname JVSL-A-ACC-N5K-01
snmp-server user admin network-admin auth md5 0x7ab9baa6c90c053ec6c4dc4d6b3162e2
 priv 0x7ab9baa6c90c053ec6c4dc4d6b3162e2 localizedkey
snmp-server user cisco network-admin auth md5 0x7ab9baa6c90c053ec6c4dc4d6b3162e2
 priv 0x7ab9baa6c90c053ec6c4dc4d6b3162e2 localizedkey
snmp-server enable traps entity fru
snmp-server community public group network-admin
vrf context management
  ip route 0.0.0.0/0 10.78.240.1
vlan 1,10,100

interface Vlan1

interface Vlan100
  no shutdown
  ip address 172.16.100.6/24

interface port-channel10
  description "L2_PC_TO_JVSL_A_FBS_1"
  switchport mode trunk
  switchport trunk allowed vlan 10,20,30,100

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

interface port-channel205
  description L2_PC_TO_AGG_N7K_02
  switchport mode trunk

interface port-channel206
  switchport mode trunk

interface Ethernet1/1
  description LINK_TO_AGG_N7K_01_e1/12
  switchport mode trunk
  switchport trunk allowed vlan 10,20,30,100
  channel-group 202 mode passive

interface Ethernet1/2
  description LINK_TO_AGG_N7K_02_e1/13
  switchport mode trunk
```

```
  switchport trunk allowed vlan 10,20,30,100
  channel-group 202 mode passive

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

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

interface Ethernet1/5
  switchport mode trunk
  channel-group 206

interface Ethernet1/6

interface Ethernet1/7
  switchport mode trunk
  channel-group 206

interface Ethernet1/8

interface Ethernet1/9
  switchport mode trunk
  switchport trunk allowed vlan 10,20,30,100
  speed 1000
  channel-group 10

interface Ethernet1/10
  switchport access vlan 100
  speed 1000

interface Ethernet1/11
  switchport mode trunk
  switchport trunk allowed vlan 10,20,30,100
  speed 1000
  channel-group 10
```

```
interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14
  speed 1000

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19

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

interface Ethernet1/36

interface Ethernet1/37

interface Ethernet1/38

interface Ethernet1/39

interface Ethernet1/40

interface mgmt0
  ip address 10.78.240.7/24
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

JVSL-A-ACC-N5K-01#
```

Show Version

```
JVSL-A-ACC-N5K-01# sh ver
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  BIOS:      version 1.2.0
  loader:    version N/A
  kickstart: version 4.1(3)N2(1a)
  system:    version 4.1(3)N2(1a)
  power-seq: version v1.0
  BIOS compile time:       06/19/08
```

```
  kickstart image file is: bootflash:/n5000-uk9-kickstart.4.1.3.N2.1a.bin
  kickstart compile time:  12/10/2009 21:00:00 [12/11/2009 05:42:02]
  system image file is:    bootflash:/n5000-uk9.4.1.3.N2.1a.bin
  system compile time:     12/10/2009 21:00:00 [12/11/2009 06:35:56]


Hardware
  cisco Nexus5020 Chassis ("40x10GE/Supervisor")
  Intel(R) Celeron(R) M CPU    with 2074284 kB of memory.
  Processor Board ID JAF1333ANTA

  Device name: JVSL-A-ACC-N5K-01
  bootflash:    1003520 kB

Kernel uptime is 14 day(s), 16 hour(s), 39 minute(s), 28 second(s)

Last reset at 445690 usecs after  Wed Apr 21 14:08:35 2010

  Reason: Reset Requested by CLI command reload
  System version: 4.1(3)N2(1a)
  Service:

plugin
  Core Plugin, Ethernet Plugin
JVSL-A-ACC-N5K-01#
```

アクセス スイッチの設定

Show Running-config

```
JVSL-A-ACC-N5K-02# sh run
version 4.1(3)N2(1a)
feature fcoe
feature telnet
feature interface-vlan
feature lacp
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$3XhGNM79$X8r2JNZtBQheXD5MvqhQw0  role network-admin
username cisco password 5 $1$8af0E.k/$H5gLrI6rzbWcWIqnQUO8P0  role network-opera
tor
username cisco role network-admin

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

ip host JVSL-A-ACC-N5K-02 10.78.240.8
hostname JVSL-A-ACC-N5K-02
snmp-server user admin network-admin auth md5 0x5cd317f07e1bc243609ad08bd7aaf1e2
 priv 0x5cd317f07e1bc243609ad08bd7aaf1e2 localizedkey
snmp-server user cisco network-operator auth md5 0x5cd317f07e1bc243609ad08bd7aaf
1e2 priv 0x5cd317f07e1bc243609ad08bd7aaf1e2 localizedkey
snmp-server user cisco network-admin
snmp-server enable traps entity fru
snmp-server community public group network-operator
vrf context management
  ip route 0.0.0.0/0 10.78.240.1
vlan 1,100

interface Vlan1

interface Vlan100
  no shutdown
  ip address 172.16.100.7/24

interface port-channel10
  description "L2_PC_TO_JVSL_A_FBS_2"
  switchport mode trunk

interface port-channel203
  description L2_PC_TO_AGG_N7K_02
  switchport mode trunk
  switchport trunk allowed vlan 10,20,30,100

interface port-channel204
  description L2_PC_TO_AGG_N7K_01
  switchport mode trunk

interface Ethernet1/1
```

```
  description LINK_TO_AGG_N7K_02_e1/12
  switchport mode trunk
  switchport trunk allowed vlan 10,20,30,100
  channel-group 203 mode passive

interface Ethernet1/2
  description LINK_TO_AGG_N7K_01_e1/13
  switchport mode trunk
  switchport trunk allowed vlan 10,20,30,100
  channel-group 203 mode passive

interface Ethernet1/3
  description LINK_TO_AGG_N7K_02_e7/12
  switchport mode trunk
  switchport trunk allowed vlan 10,20,30,100
  channel-group 203 mode passive

interface Ethernet1/4
  description LINK_TO_AGG_N7K_01_e7/13
  switchport mode trunk
  switchport trunk allowed vlan 10,20,30,100
  channel-group 203 mode passive

interface Ethernet1/5
  switchport mode trunk

interface Ethernet1/6

interface Ethernet1/7

interface Ethernet1/8

interface Ethernet1/9
  switchport mode trunk
  speed 1000
  channel-group 10

interface Ethernet1/10
  speed 1000

interface Ethernet1/11
  switchport mode trunk
  speed 1000
```

```
  channel-group 10

interface Ethernet1/12

interface Ethernet1/13

interface Ethernet1/14
  speed 1000

interface Ethernet1/15

interface Ethernet1/16

interface Ethernet1/17

interface Ethernet1/18

interface Ethernet1/19

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

interface Ethernet1/36

interface Ethernet1/37

interface Ethernet1/38

interface Ethernet1/39

interface Ethernet1/40

interface mgmt0
  ip address 10.78.240.8/24
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
```

Show Version

```
JVSL-A-ACC-N5K-02# sh ver
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software are covered under the GNU Public
License. A copy of the license is available at
http://www.gnu.org/licenses/gpl.html.

Software
  BIOS:      version 1.2.0
  loader:    version N/A
  kickstart: version 4.1(3)N2(1a)
  system:    version 4.1(3)N2(1a)
  power-seq: version v1.0
```

```
  BIOS compile time:       06/19/08
  kickstart image file is: bootflash:/n5000-uk9-kickstart.4.1.3.N2.1a.bin
  kickstart compile time:  12/10/2009 21:00:00 [12/11/2009 05:42:02]
  system image file is:    bootflash:/n5000-uk9.4.1.3.N2.1a.bin
  system compile time:     12/10/2009 21:00:00 [12/11/2009 06:35:56]


Hardware
  cisco Nexus5020 Chassis ("40x10GE/Supervisor")
  Intel(R) Celeron(R) M CPU    with 2074284 kB of memory.
  Processor Board ID JAF1336APSN

  Device name: JVSL-A-ACC-N5K-02
  bootflash:    1003520 kB

Kernel uptime is 14 day(s), 16 hour(s), 34 minute(s), 26 second(s)

Last reset at 44900 usecs after  Wed Apr 21 14:16:31 2010

  Reason: Reset Requested by CLI command reload
  System version: 4.1(3)N2(1a)
  Service:

plugin
  Core Plugin, Ethernet Plugin
JVSL-A-ACC-N5K-02#
```

レイヤ 4 ～ 7 サービス コンポーネント

Show Version

```
cat6k-services#sh ver
Cisco IOS Software, s72033_rp Software (s72033_rp-IPSERVICESK9_WAN-VM), Version
12.2(33)SXI2a, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2009 by Cisco Systems, Inc.
Compiled Tue 01-Sep-09 19:05 by prod_rel_team

ROM: System Bootstrap, Version 12.2(17r)SX5, RELEASE SOFTWARE (fc1)

 cat6k-services uptime is 2 weeks, 6 days, 27 minutes
Uptime for this control processor is 2 weeks, 6 days, 26 minutes
Time since cat6k-services switched to active is 2 weeks, 6 days, 26 minutes
```

```
System returned to ROM by s/w reset (SP by bus error at PC 0x402DF824, address 0
x0)
System image file is "sup-bootdisk:s72033-ipservicesk9_wan-vz.122-33.SXI2a.bin"
Last reload reason: Unknown reason


This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco WS-C6506-E (R7000) processor (revision 1.2) with 1040384K/8192K bytes of m
emory.
Processor board ID SAL1328TRBH
SR71000 CPU at 600Mhz, Implementation 1284, Rev 1.2, 512KB L2 Cache
Last reset from s/w reset
6 Virtual Ethernet interfaces
24 Gigabit Ethernet interfaces
4 Ten Gigabit Ethernet interfaces
1917K bytes of non-volatile configuration memory.

65536K bytes of Flash internal SIMM (Sector size 512K).
Configuration register is 0x2


Patching is not available since the system is not running from an installed imag
e.
To install, please use the "install file" command.


cat6k-services#
```

Show Running-config

```
cat6k-services#sh run
Building configuration...

Current configuration : 4615 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 cat6k-services
!
boot-start-marker
boot system flash sup-bootdisk:
boot-end-marker
!
security passwords min-length 1
enable secret 5 $1$wpn0$YAvc8wOEDValM91Jb5rdR/
enable password cisco123
!
username cisco password 0 roZes@123
no aaa new-model
ip subnet-zero
!
!
no ip domain-lookup
!
mls qos
mls netflow interface
mls cef error action reset
!
!
!
!
!
!
!
diagnostic bootup level minimal
!
```

```
power redundancy-mode combined
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
!
redundancy
 main-cpu
  auto-sync running-config
 mode sso
!
!
vlan access-map client-traffic 10
 match ip address 130 120
 action forward capture
!
vlan filter client-traffic vlan-list  100
vlan internal allocation policy ascending
vlan access-log ratelimit 2000
!
!
!
interface Port-channel67
 description L2_PC_TO_AGG_N7K_01
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
!
interface TenGigabitEthernet2/1
 no ip address
!
interface TenGigabitEthernet2/2
 description LINK_TO_AGG_N7K_01_7/23
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 channel-protocol lacp
 channel-group 67 mode active
!
interface TenGigabitEthernet2/3
```

```
 description LINK_TO_AGG_N7K_01_7/23
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,10,20,30,100
 switchport mode trunk
 shutdown
!
interface TenGigabitEthernet2/4
 no ip address
 shutdown
!
interface GigabitEthernet4/1
 description LINK_TO_ASA_01_OUTSIDE
 switchport
 switchport access vlan 20
 switchport mode access
 speed 1000
!
interface GigabitEthernet4/2
 description LINK_TO_ASA_01_INSIDE
 switchport
 switchport access vlan 30
 speed 1000
!
interface GigabitEthernet4/3
 description LINK_TO_IPS_FE1/0
 switchport
 switchport access vlan 40
 switchport mode access
 switchport capture
 switchport capture allowed vlan 100
 speed 100
!
interface GigabitEthernet4/4
 no ip address
 shutdown
 speed 100
!
interface GigabitEthernet4/5
 switchport
 switchport access vlan 100
!
interface GigabitEthernet4/6
```

```
 no ip address
 shutdown
!
interface GigabitEthernet4/7
 no ip address
 shutdown
!
interface GigabitEthernet4/8
 no ip address
 shutdown
!
interface GigabitEthernet4/9
 no ip address
 shutdown
!
interface GigabitEthernet4/10
 no ip address
 shutdown
!
interface GigabitEthernet4/11
 no ip address
 shutdown
!
interface GigabitEthernet4/12
 no ip address
 shutdown
!
interface GigabitEthernet4/13
 description LINK_TO_MS_EXCHANGE_CLIENT
 switchport
 switchport access vlan 10
 switchport mode access
 speed 1000
 spanning-tree portfast edge
!
interface GigabitEthernet4/14
 switchport
 switchport access vlan 10
 switchport mode access
 speed 1000
!
interface GigabitEthernet4/15
 switchport
```

```
 switchport access vlan 10
 switchport mode access
 speed 100
!
interface GigabitEthernet4/16
 description management_access
 ip address 10.78.240.11 255.255.255.0
 speed 100
 duplex full
!
interface GigabitEthernet5/1
 no ip address
 shutdown
!
interface GigabitEthernet5/2
 no ip address
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 172.16.10.1 255.255.255.0
 ip policy route-map client-traffic
!
interface Vlan20
 ip address 172.16.20.1 255.255.255.0
!
interface Vlan30
 ip address 172.16.30.1 255.255.255.0
!
interface Vlan100
 description FBS_Server_VLAN
 ip address 172.16.100.25 255.255.255.0
 ip policy route-map return-traffic
!
interface Vlan500
 no ip address
!
ip default-gateway 10.78.240.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.78.240.1
!
```

```
!
no ip http server
no ip http secure-server
!
access-list 10 permit any
access-list 110 permit ip 172.16.10.0 0.0.0.255 172.16.100.0 0.0.0.255
access-list 120 permit ip 172.16.10.0 0.0.0.255 172.16.100.0 0.0.0.255
access-list 130 permit ip any any
access-list 150 permit ip 172.16.100.0 0.0.0.255 172.16.10.0 0.0.0.255
!
route-map return-traffic permit 10
 match ip address 150
 set ip next-hop 172.16.30.2
!
route-map client-traffic permit 10
 match ip address 110
 set ip next-hop 172.16.20.2
!
snmp-server engineID local 800000090300002584F73A00
snmp-server user cisco admin v1
snmp-server community public RW
!
!
control-plane
!
!
dial-peer cor custom
!
!
!
!
line con 0
line vty 0 4
 access-class 10 in
 password roZes123
 login
line vty 5 15
 login
!
exception core-file
!
no event manager policy Mandatory.go_switchbus.tcl type system
!
```

```
end


cat6k-services#
```

Show Running-config

```
JVSL-A-IPS-01# sh configuration
  Generating current config: /                                          !
------------------------------ ! Current configuration last modified Thu Jul 01 04:23:49
2010 ! ------------------------------ ! Version 6.0(1) ! Host:
!    Realm Keys        key1.0             ! Signature Definition:                    !
Signature Update    S263.0   2006-12-18        Virus Update       V1.2     2005-11-24
! ------------------------------ service interface physical-interfaces FastEthernet0/1
admin-state enabled speed 100 exit physical-interfaces FastEthernet1/0  admin-state
enabled speed auto exit
physical-interfaces FastEthernet1/1  admin-state enabled speed auto exit exit  --MORE--
! ------------------------------
service authentication exit
! ------------------------------
service event-action-rules rules0 overrides deny-packet-inline  override-item-status
Disabled exit
general global-overrides-status Enabled exit
exit ! ------------------------------ service host network-settings host-ip
10.78.240.16/27,10.78.240.1 host-name JVSL-A-IPS-01 telnet-option enabled access-list
0.0.0.0/0  access-list 172.0.0.0/27  access-list 192.0.0.0/24  exit time-zone-settings
offset 0  --MORE--          standard-time-zone-name UTC exit exit
! ------------------------------ service logger exit  ! ------------------------------
service network-access exit  ! ------------------------------  service notification exit
! ------------------------------
service signature-definition sig0
signatures 2000 0  status enabled true exit exit
signatures 2004 0  engine atomic-ip event-action produce-alert exit status
 --MORE--        enabled true exit exit 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 virtual-sensor vs0
logical-interface pair1  exit  --MORE--     exit  JVSL-A-IPS-01# sh ver
Application Partition: Cisco Intrusion Prevention System, Version 6.0(1)E1 Host:
Realm Keys          key1.0
Signature Definition:
    Signature Update    S263.0                  2006-12-18
    Virus Update        V1.2                    2005-11-24
OS Version:             2.4.30-IDS-smp-bigphys
```

```
Platform:               IDS-4215
Serial Number:          88809152156
No license present
Sensor up-time is 47 days.
Using 406794240 out of 502026240 bytes of available memory (81% usage)
system is using 17.8M out of 29.0M bytes of available disk space (61% usage)
application-data is using 35.2M out of 166.8M bytes of available disk space (22% usage)
boot is using 37.6M out of 68.6M bytes of available disk space (58% usage)
application-log is using 534.4M out of 2.8G bytes of available disk space (20% usage)
MainApp          2006_Dec_11_11.57   (Release)   2006-12-11T12:44:38-0600   Running
AnalysisEngine   2006_Dec_11_11.57   (Release)   2006-12-11T12:44:38-0600   Running
CLI           2006_Dec_11_11.57   (Release)   2006-12-11T12:44:38-0600           Upgrade
History:   IPS-K9-6.0-1-E1   11:57:00 UTC Mon Dec 11 2006
 --MORE--           Recovery Partition Version 1.1 - 6.0(1)E1  JVSL-A-IPS-01#
```

Show Running-config

```
JVSL-A-ASA-01# sh run
: Saved
:
ASA Version 8.0(4)
!
hostname JVSL-A-ASA-01
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd ZyiS/yBPzhiyI7DM encrypted
names
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.20.2 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.30.2 255.255.255.0
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
```

```
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 10.78.240.15 255.255.255.0
 management-only
!
interface GigabitEthernet1/0
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/3
 shutdown
 no nameif
 no security-level
 no ip address
!
ftp mode passive
access-list 101 extended permit tcp host 172.16.10.10 host 172.16.100.10 eq smtp

access-list 101 extended permit tcp host 172.16.10.10 host 172.16.100.10 eq imap
4
access-list 101 extended permit tcp host 172.16.10.10 host 172.16.100.10 eq pop3
```

```
access-list 101 extended permit tcp host 172.16.10.10 host 172.16.100.10 eq 993
access-list 101 extended permit udp host 172.16.10.10 host 172.16.100.10 eq doma
in
access-list 101 extended permit udp host 172.16.10.10 host 172.16.100.10 eq 389
access-list 101 extended permit tcp host 172.16.10.10 host 172.16.100.10 eq ldap

access-list 101 extended permit tcp host 172.16.10.10 host 172.16.100.10 eq 445
access-list 101 extended permit udp host 172.16.10.10 host 172.16.100.10 eq 88
access-list 101 extended permit tcp host 172.16.10.10 host 172.16.100.10 eq 135
access-list 101 extended permit icmp any any echo
access-list 101 extended permit tcp host 172.16.10.10 host 172.16.100.10 eq 88
access-list 101 extended permit tcp host 172.16.10.10 host 172.16.100.10 gt 1024

access-list 102 extended permit ip 172.16.10.0 255.255.255.0 172.16.100.0 255.25
5.255.0
access-list 102 extended permit ip 172.16.100.0 255.255.255.0 172.16.10.0 255.25
5.255.0
access-list 105 extended permit ip 172.16.100.0 255.255.255.0 host 172.16.10.10
access-list 105 extended permit ip host 172.16.10.10 172.16.100.0 255.255.255.0
access-list OUT_TO_IN extended permit tcp 172.16.10.0 255.255.255.0 172.16.100.0
 255.255.255.0 eq smtp
access-list OUT_TO_IN extended permit tcp 172.16.10.0 255.255.255.0 172.16.100.0
 255.255.255.0 eq imap4
access-list OUT_TO_IN extended permit tcp 172.16.10.0 255.255.255.0 172.16.100.0
 255.255.255.0 eq pop3
access-list OUT_TO_IN extended permit tcp 172.16.10.0 255.255.255.0 172.16.100.0
 255.255.255.0 eq 993
access-list OUT_TO_IN extended permit udp 172.16.10.0 255.255.255.0 172.16.100.0
 255.255.255.0 eq domain
access-list OUT_TO_IN extended permit udp 172.16.10.0 255.255.255.0 172.16.100.0
 255.255.255.0 eq 389
access-list OUT_TO_IN extended permit tcp 172.16.10.0 255.255.255.0 172.16.100.0
 255.255.255.0 eq ldap
access-list OUT_TO_IN extended permit tcp 172.16.10.0 255.255.255.0 172.16.100.0
 255.255.255.0 eq 445
access-list OUT_TO_IN extended permit udp 172.16.10.0 255.255.255.0 172.16.100.0
 255.255.255.0 eq 88
access-list OUT_TO_IN extended permit tcp 172.16.10.0 255.255.255.0 172.16.100.0
 255.255.255.0 eq 135
access-list OUT_TO_IN extended permit icmp any any echo
access-list OUT_TO_IN extended permit tcp 172.16.10.0 255.255.255.0 172.16.100.0
 255.255.255.0 eq 88
access-list OUT_TO_IN extended permit tcp 172.16.10.0 255.255.255.0 172.16.100.0
```

```
 255.255.255.0 gt 1024
access-list OUT_TO_IN extended permit icmp any any echo-reply
access-list OUT_TO_IN extended permit tcp 172.16.10.0 255.255.255.0 172.16.100.0
 255.255.255.0 eq https
pager lines 24
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu management 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-613.bin
no asdm history enable
arp timeout 14400
access-group OUT_TO_IN in interface outside
route management 0.0.0.0 0.0.0.0 10.78.240.1 1
route outside 172.16.10.0 255.255.255.0 172.16.20.1 1
route inside 172.16.100.0 255.255.255.0 172.16.30.1 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
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.1.0 255.255.255.0 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 10.78.0.0 255.255.0.0 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
!
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 rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect icmp
  inspect http
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:7f685f1d707b83eb0dcb85875a80b8ce
: end


JVSL-A-ASA-01#
Show Version

JVSL-A-ASA-01# sh ver

Cisco Adaptive Security Appliance Software Version 8.0(4)
Device Manager Version 6.1(3)

Compiled on Thu 07-Aug-08 20:53 by builders
System image file is "disk0:/asa804-k8.bin"
Config file at boot was "startup-config"

JVSL-A-ASA-01 up 21 days 22 hours

Hardware:   ASA5540, 1024 MB RAM, CPU Pentium 4 2000 MHz
```

```
Internal ATA Compact Flash, 256MB
BIOS Flash M50FW080 @ 0xffe00000, 1024KB

Encryption hardware device : Cisco ASA-55x0 on-board accelerator (revision 0x0)
                             Boot microcode   : ?CN1000-MC-BOOT-2.00
                             SSL/IKE microcode: ?CNLite-MC-SSLm-PLUS-2.03
                             IPSec microcode  : ?CNlite-MC-IPSECm-MAIN-2.05
 0: Ext: GigabitEthernet0/0  : address is 0026.0b31.4504, irq 9
 1: Ext: GigabitEthernet0/1  : address is 0026.0b31.4505, irq 9
 2: Ext: GigabitEthernet0/2  : address is 0026.0b31.4506, irq 9
 3: Ext: GigabitEthernet0/3  : address is 0026.0b31.4507, irq 9
 4: Ext: Management0/0       : address is 0026.0b31.4508, irq 11
 5: Int: Internal-Data0/0    : address is 0000.0001.0002, irq 11
 6: Int: Not used            : irq 5
 7: Ext: GigabitEthernet1/0  : address is 0026.0bde.46c1, irq 255
 8: Ext: GigabitEthernet1/1  : address is 0026.0bde.46c2, irq 255
 9: Ext: GigabitEthernet1/2  : address is 0026.0bde.46c3, irq 255
10: Ext: GigabitEthernet1/3  : address is 0026.0bde.46c4, irq 255
11: Int: Internal-Data1/0    : address is 0000.0003.0002, irq 255

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited
Maximum VLANs                : 200
Inside Hosts                 : Unlimited
Failover                     : Active/Active
VPN-DES                      : Enabled
VPN-3DES-AES                 : Disabled
Security Contexts            : 2
GTP/GPRS                     : Disabled
VPN Peers                    : 5000
WebVPN Peers                 : 2
AnyConnect for Mobile        : Disabled
AnyConnect for Linksys phone : Disabled
Advanced Endpoint Assessment : Disabled
UC Proxy Sessions            : 2

This platform has an ASA 5540 VPN Premium license.

Serial Number: JMX1336L0U0
Running Activation Key: 0x9c3fef7c 0xdc3a0eb9 0x18527108 0x90d80c2c 0x8a2129ac
Configuration register is 0x1
Configuration last modified by enable_15 at 23:13:43.997 UTC Tue Apr 20 2010
JVSL-A-ASA-01#
```

Storage Area Networking（SAN）コンポーネント

Show Running-config

```
JVSL-MDS9140# sh run
version 3.3(4a)
vsan database
  vsan 10 name "VSAN10"
  vsan 20 name "VSAN20"
  vsan 100
  vsan 210
  vsan 220
  vsan 230
  vsan 240
  vsan 250
  vsan 260
device-alias database
  device-alias name JVSL_FBS06_HBA01 pwwn 10:00:00:00:c9:8c:9b:b6
  device-alias name JVSL_FBS06_HBA02 pwwn 10:00:00:00:c9:8c:9b:b7
  device-alias name JVSL_FBS07_HBA01 pwwn 10:00:00:00:c9:8c:9a:dc
  device-alias name JVSL_FBS07_HBA02 pwwn 10:00:00:00:c9:8c:9a:dd
  device-alias name JVSL_HITACHI_CL3A pwwn 50:06:0e:80:05:8e:09:20
  device-alias name JVSL_HITACHI_CL4A pwwn 50:06:0e:80:05:8e:09:30

device-alias commit

fcdomain distribute
fcdomain domain 100 static vsan 210
fcdomain domain 100 static vsan 220
fcdomain domain 100 static vsan 230
fcdomain domain 100 static vsan 240
fcdomain domain 100 static vsan 250
fcdomain domain 100 static vsan 260
fcdomain commit vsan 210
fcdomain commit vsan 220
fcdomain commit vsan 230
fcdomain commit vsan 240
fcdomain commit vsan 250
fcdomain commit vsan 260
fcdomain fcid database
  vsan 1 wwn 50:06:01:60:30:21:e1:e0 fcid 0xac00ef dynamic
  vsan 1 wwn 50:06:01:68:30:21:e1:e0 fcid 0xac01ef dynamic
  vsan 1 wwn 20:04:00:0d:ec:12:2a:00 fcid 0xac0200 area dynamic
```

```
  vsan 1 wwn 20:08:00:0d:ec:12:2a:00 fcid 0xac0300 area dynamic
  vsan 1 wwn 20:06:00:0d:ec:12:2a:00 fcid 0xac0400 area dynamic
  vsan 1 wwn 20:05:00:0d:ec:12:2a:00 fcid 0xac0500 area dynamic
  vsan 1 wwn 20:03:00:0d:ec:12:2a:00 fcid 0xac0600 area dynamic
  vsan 1 wwn 21:00:00:e0:8b:1d:a4:09 fcid 0xac0700 area dynamic
  vsan 1 wwn 20:07:00:0d:ec:12:2a:00 fcid 0xac0800 area dynamic
  vsan 1 wwn 50:06:01:69:30:21:e1:e0 fcid 0xac09ef dynamic
  vsan 1 wwn 50:06:01:61:30:21:e1:e0 fcid 0xac0aef dynamic
  vsan 1 wwn 50:06:01:60:30:21:d6:cf fcid 0xac0bef dynamic
  vsan 1 wwn 20:09:00:0d:ec:12:2a:00 fcid 0xac0c00 area dynamic
  vsan 1 wwn 20:19:00:0d:ec:12:2a:00 fcid 0xac0d00 area dynamic
  vsan 1 wwn 50:06:01:68:30:21:d6:cf fcid 0xac0eef dynamic
  vsan 1 wwn 50:06:01:61:30:21:d6:cf fcid 0xac0fef dynamic
  vsan 1 wwn 50:06:01:69:30:21:d6:cf fcid 0xac10ef dynamic
  vsan 1 wwn 20:1a:00:0d:ec:12:2a:00 fcid 0xac1100 area dynamic
  vsan 1 wwn 20:1e:00:0d:ec:12:2a:00 fcid 0xac1200 area dynamic
  vsan 1 wwn 20:1d:00:0d:ec:12:2a:00 fcid 0xac1300 area dynamic
  vsan 1 wwn 20:28:00:0d:ec:12:2a:00 fcid 0xac1400 area dynamic
  vsan 1 wwn 20:27:00:0d:ec:12:2a:00 fcid 0xac1500 area dynamic
  vsan 1 wwn 20:01:00:0d:ec:12:2a:00 fcid 0xac1900 area dynamic
  vsan 1 wwn 20:02:00:0d:ec:12:2a:00 fcid 0xac1a00 area dynamic
  vsan 1 wwn 50:01:43:80:06:2f:da:e8 fcid 0xac0000 dynamic
  vsan 1 wwn 10:00:00:00:c9:8c:9b:b6 fcid 0xac0001 dynamic
!            [JVSL_FBS06_HBA01]
  vsan 1 wwn 50:06:0e:80:05:8d:dd:00 fcid 0xac0002 dynamic
  vsan 1 wwn 50:01:43:80:06:2f:da:ec fcid 0xac0004 dynamic
  vsan 1 wwn 50:01:43:80:06:2f:da:ea fcid 0xac0005 dynamic
  vsan 1 wwn 50:01:43:80:06:2f:da:70 fcid 0xac0003 dynamic
  vsan 1 wwn 50:06:0e:80:05:8e:09:00 fcid 0xac0010 dynamic
  vsan 1 wwn 50:06:01:69:44:60:24:f1 fcid 0xac1bef dynamic
  vsan 1 wwn 20:1c:00:0d:ec:12:2a:00 fcid 0xac1600 area dynamic
  vsan 1 wwn 20:0c:00:0d:ec:12:2a:00 fcid 0xac1700 area dynamic
  vsan 1 wwn 50:06:01:60:44:60:24:f1 fcid 0xac1cef dynamic
  vsan 1 wwn 50:06:0e:80:05:8d:dd:10 fcid 0xac0006 dynamic
  vsan 1 wwn 50:06:0e:80:05:8e:09:10 fcid 0xac0011 dynamic
  vsan 1 wwn 50:06:01:68:44:60:24:f1 fcid 0xac1def dynamic
  vsan 1 wwn 50:06:01:61:44:60:24:f1 fcid 0xac1eef dynamic
  vsan 1 wwn 50:06:0e:80:05:8e:09:20 fcid 0xac0012 dynamic
!            [JVSL_HITACHI_CL3A]
  vsan 1 wwn 20:0a:00:0d:ec:12:2a:00 fcid 0xac1800 area dynamic
  vsan 1 wwn 50:06:0e:80:05:8e:09:30 fcid 0xac0013 dynamic
!            [JVSL_HITACHI_CL4A]
  vsan 10 wwn 50:06:0e:80:05:8e:09:20 fcid 0x890000 dynamic
```

```
!             [JVSL_HITACHI_CL3A]
  vsan 1 wwn 10:00:00:00:c9:8c:9b:ba fcid 0xac0007 dynamic
  vsan 1 wwn 50:06:0e:80:05:8d:dd:30 fcid 0xac0008 dynamic
  vsan 1 wwn 10:00:00:00:c9:8c:9a:dc fcid 0xac0009 dynamic
!            [JVSL_FBS07_HBA01]
  vsan 1 wwn 10:00:00:00:c9:8c:9b:bb fcid 0xac000a dynamic
  vsan 1 wwn 10:00:00:00:c9:8c:9b:b7 fcid 0xac000b dynamic
!            [JVSL_FBS06_HBA02]
  vsan 1 wwn 10:00:00:00:c9:8c:9a:dd fcid 0xac000c dynamic
!            [JVSL_FBS07_HBA02]
  vsan 20 wwn 50:06:0e:80:05:8e:09:30 fcid 0x410000 dynamic
!             [JVSL_HITACHI_CL4A]
  vsan 1 wwn 10:00:00:00:c9:8c:9b:91 fcid 0xac000d dynamic
  vsan 1 wwn 50:01:43:80:06:2f:da:72 fcid 0xac000e dynamic
  vsan 1 wwn 10:00:00:00:c9:8c:9b:90 fcid 0xac000f dynamic
  vsan 10 wwn 10:00:00:00:c9:8c:9b:b6 fcid 0x890001 dynamic
!             [JVSL_FBS06_HBA01]
  vsan 20 wwn 10:00:00:00:c9:8c:9b:b7 fcid 0x410001 dynamic
!             [JVSL_FBS06_HBA02]
  vsan 10 wwn 10:00:00:00:c9:8c:9a:dc fcid 0x890002 dynamic
!             [JVSL_FBS07_HBA01]
  vsan 1 wwn 50:06:0e:80:05:8d:dd:01 fcid 0xac0014 dynamic
  vsan 20 wwn 10:00:00:00:c9:8c:9a:dd fcid 0x410002 dynamic
!             [JVSL_FBS07_HBA02]
  vsan 100 wwn 50:01:43:80:06:2f:da:e8 fcid 0x7b0000 dynamic
  vsan 100 wwn 50:01:43:80:06:2f:da:ea fcid 0x7b0001 dynamic
  vsan 100 wwn 50:06:0e:80:05:8d:dd:00 fcid 0x7b0002 dynamic
  vsan 210 wwn 10:00:00:00:c9:8c:9b:b6 fcid 0x640000 dynamic
!              [JVSL_FBS06_HBA01]
  vsan 220 wwn 10:00:00:00:c9:8c:9a:dc fcid 0x640000 dynamic
!              [JVSL_FBS07_HBA01]
  vsan 230 wwn 10:00:00:00:c9:8c:9b:b7 fcid 0x640000 dynamic
!              [JVSL_FBS06_HBA02]
  vsan 240 wwn 10:00:00:00:c9:8c:9a:dd fcid 0x640000 dynamic
!              [JVSL_FBS07_HBA02]
  vsan 250 wwn 50:06:0e:80:05:8e:09:20 fcid 0x640000 dynamic
!              [JVSL_HITACHI_CL3A]
  vsan 260 wwn 50:06:0e:80:05:8e:09:30 fcid 0x640000 dynamic
!              [JVSL_HITACHI_CL4A]
vsan database
  vsan 100 interface fc1/1
  vsan 250 interface fc1/7
  vsan 260 interface fc1/8
```

```
  vsan 210 interface fc1/11
  vsan 220 interface fc1/12
  vsan 230 interface fc1/19
  vsan 240 interface fc1/20
  vsan 100 interface fc1/31
  vsan 100 interface fc1/32
fcroute 0x890001 0xffffff interface fc1/10 domain 10 metric 10  vsan 10
system default switchport trunk mode auto
interface fc1/20
  switchport speed 2000
interface fc1/32
  switchport speed 2000
interface fc1/20
  switchport mode Fx
interface fc1/32
  switchport mode Fx
interface fc1/1
interface fc1/2
interface fc1/3
interface fc1/4
interface fc1/5
interface fc1/6
interface fc1/7
  switchport mode auto
interface fc1/8
interface fc1/9
interface fc1/10
interface fc1/11
interface fc1/12
interface fc1/13
interface fc1/14
interface fc1/15
interface fc1/16
interface fc1/17
interface fc1/18
interface fc1/19
interface fc1/21
interface fc1/22
interface fc1/23
interface fc1/24
interface fc1/25
interface fc1/26
interface fc1/27
```

```
interface fc1/28
interface fc1/29
interface fc1/30
interface fc1/31
interface fc1/33
interface fc1/34
interface fc1/35
interface fc1/36
interface fc1/37
interface fc1/38
interface fc1/39
interface fc1/40
tlport alpa-cache interface fc1/9 pwwn 10:00:00:00:c9:8c:9b:91 alpa 0x1
tlport alpa-cache interface fc1/9 pwwn 50:06:0e:80:05:8e:09:00 alpa 0x4
tlport alpa-cache interface fc1/9 pwwn 50:06:0e:80:05:8e:09:10 alpa 0x8
ip default-gateway 10.78.16.1
ip route 10.0.0.0 255.0.0.0 interface mgmt0
switchname JVSL-MDS9140
role name default-role
  description This is a system defined role and applies to all users
  rule 1 permit show feature system
  rule 2 permit show feature snmp
  rule 3 permit show feature module
  rule 4 permit show feature hardware
  rule 5 permit show feature environment
username admin password 5 $1$s3UQLFoP$Y0FPPleiP.agavsp.F.Cm1  role network-admin
username topspin password 5 $1$KD0HMncu$opZ7qURjo7XZEIcBKN.Kj0  role network-ope
rator
username cisco password 5 $1$Ipwz9GNf$h4lmQtIm9AqLEHhG6W1sp0  role network-admin
ssh key rsa1 1024 force
ssh server enable
boot kickstart bootflash:/m9100-s1ek9-kickstart-mz.3.3.4a.bin
boot system bootflash:/m9100-s1ek9-mz.3.3.4a.bin
kernel core target 0.0.0.0
kernel core limit 1
ivr enable
ivr nat
ivr vsan-topology database
  autonomous-fabric-id    1 switch-wwn 20:00:00:0d:ec:12:2a:00 vsan-ranges 210,2
20,230,240,250,260
ivr vsan-topology activate
snmp-server contact odc-loca-test-dc
snmp-server community public group network-operator
```

```
snmp-server community jvsl group network-admin
snmp-server user admin network-admin auth md5 0x0275704d443e7c2bbc27ca4e6ef262ee
 priv 0x0275704d443e7c2bbc27ca4e6ef262ee localizedkey
snmp-server user cisco network-admin auth md5 0xe8def87c0d8a9e3e16ab00998b67bf70
 priv 0xe8def87c0d8a9e3e16ab00998b67bf70 localizedkey
snmp-server user topspin network-operator auth md5 0x57a880422bdc954222062128676
3a260 priv 0x57a880422bdc9542220621286763a260 localizedkey
snmp-server host 10.78.240.100 version 2c public  udp-port 2162
snmp-server host 10.78.240.200 version 2c public  udp-port 2162
snmp-server host 10.78.240.62 version 2c public  udp-port 2162
snmp-server enable traps vrrp
snmp-server enable traps license
callhome
logging level vrrp_eng 2
zone default-zone permit vsan 1
zone default-zone permit vsan 100
zoneset distribute full vsan 1
!Full Zone Database Section for vsan 10
zone name ZoneA vsan 10
    member pwwn 10:00:00:00:c9:8c:9b:b6
!               [JVSL_FBS06_HBA01]
    member pwwn 50:06:0e:80:05:8e:09:20
!               [JVSL_HITACHI_CL3A]

zone name ZoneB vsan 10
    member pwwn 10:00:00:00:c9:8c:9a:dc
!               [JVSL_FBS07_HBA01]
    member pwwn 50:06:0e:80:05:8e:09:20
!               [JVSL_HITACHI_CL3A]

zoneset name Zoneset1 vsan 10
    member ZoneA
    member ZoneB

zoneset name Zoneset100 vsan 10

zoneset activate name Zoneset1 vsan 10
!Full Zone Database Section for vsan 20
zone name ZoneC vsan 20
    member pwwn 50:06:0e:80:05:8e:09:30
!               [JVSL_HITACHI_CL4A]
    member pwwn 10:00:00:00:c9:8c:9b:b7
!               [JVSL_FBS06_HBA02]
```

```
zone name ZoneD vsan 20
    member pwwn 50:06:0e:80:05:8e:09:30
!               [JVSL_HITACHI_CL4A]
    member pwwn 10:00:00:00:c9:8c:9a:dd
!               [JVSL_FBS07_HBA02]

zoneset name Zoneset1 vsan 20
    member ZoneC
    member ZoneD

zoneset activate name Zoneset1 vsan 20
!Full Zone Database Section for vsan 100
zone name ZoneA vsan 100
    member pwwn 50:01:43:80:06:2f:da:e8
    member pwwn 50:06:0e:80:05:8d:dd:00

zone name ZoneB vsan 100
    member pwwn 50:01:43:80:06:2f:da:ea
    member pwwn 50:06:0e:80:05:8d:dd:00

zoneset name Zoneset100 vsan 100
    member ZoneA
    member ZoneB

zoneset activate name Zoneset100 vsan 100
zoneset activate name nozoneset vsan 210
zoneset activate name nozoneset vsan 220
zoneset activate name nozoneset vsan 230
zoneset activate name nozoneset vsan 240
zoneset activate name nozoneset vsan 250
zoneset activate name nozoneset vsan 260
ivr zone name IVR_ZONE_A
  member pwwn 10:00:00:00:c9:8c:9b:b6               vsan 210
!             [JVSL_FBS06_HBA01]
  member pwwn 50:06:0e:80:05:8e:09:20               vsan 250
!             [JVSL_HITACHI_CL3A]
ivr zone name IVR_ZONE_B
  member pwwn 10:00:00:00:c9:8c:9a:dc               vsan 220
!             [JVSL_FBS07_HBA01]
  member pwwn 50:06:0e:80:05:8e:09:20               vsan 250
!             [JVSL_HITACHI_CL3A]
ivr zone name IVR_ZONE_C
```

```
  member pwwn 10:00:00:00:c9:8c:9b:b7               vsan 230
!             [JVSL_FBS06_HBA02]
  member pwwn 50:06:0e:80:05:8e:09:30               vsan 260
!             [JVSL_HITACHI_CL4A]
ivr zone name IVR_ZONE_D
  member pwwn 50:06:0e:80:05:8e:09:30               vsan 260
!             [JVSL_HITACHI_CL4A]
  member pwwn 10:00:00:00:c9:8c:9a:dd               vsan 240
!             [JVSL_FBS07_HBA02]
ivr zoneset name IVR_ZONESET_1
  member IVR_ZONE_A
  member IVR_ZONE_B
  member IVR_ZONE_C
  member IVR_ZONE_D
ivr zoneset activate name IVR_ZONESET_1 force

interface fc1/1

interface fc1/2

interface fc1/3

interface fc1/4
  no shutdown

interface fc1/5
  no shutdown

interface fc1/6

interface fc1/7
  no shutdown

interface fc1/8

interface fc1/9
  no shutdown

interface fc1/10

interface fc1/11
  no shutdown
```

```
interface fc1/12
  no shutdown

interface fc1/13

interface fc1/14

interface fc1/15

interface fc1/16

interface fc1/17

interface fc1/18

interface fc1/19

interface fc1/20
  no shutdown

interface fc1/21

interface fc1/22
  no shutdown

interface fc1/23

interface fc1/24

interface fc1/25
  no shutdown

interface fc1/26

interface fc1/27

interface fc1/28

interface fc1/29

interface fc1/30

interface fc1/31
```

```
  no shutdown

interface fc1/32
  no shutdown

interface fc1/33

interface fc1/34

interface fc1/35

interface fc1/36

interface fc1/37
  no shutdown

interface fc1/38

interface fc1/39

interface fc1/40

interface mgmt0
  switchport speed 100
  ip address 10.78.240.18 255.255.255.0
no system default switchport shutdown
scheduler enable

JVSL-MDS9140#
```

Show Version

```
JVSL-MDS9140# sh ver
Cisco Storage Area Networking Operating System (SAN-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained herein are owned by
other third parties and are used and distributed under license.
Some parts of this software may be covered under the GNU Public
License or the GNU Lesser General Public License. A copy of
each such license is available at
http://www.gnu.org/licenses/gpl.html and
```

```
http://www.gnu.org/licenses/lgpl.html

Software
  BIOS:      version 1.1.0
  loader:    version 1.2(2)
  kickstart: version 3.3(4a)
  system:    version 3.3(4a)

  BIOS compile time:       10/24/03
  kickstart image file is: bootflash:/m9100-s1ek9-kickstart-mz.3.3.4a.bin
  kickstart compile time:  10/13/2009 12:00:00 [10/29/2009 14:41:59]
  system image file is:    bootflash:/m9100-s1ek9-mz.3.3.4a.bin
  system compile time:     10/13/2009 12:00:00 [10/29/2009 14:59:10]


Hardware
  cisco MDS 9100 ("1/2 Gbps FC/Supervisor")
  Intel(R) Pentium(R) III CPU with 963828 kB of memory.
  Processor Board ID JAE1011Y88K

  bootflash:  250368 kB
  slot0:           0 kB

JVSL-MDS9140   kernel uptime is 30 days 5 hours 42 minute(s) 57 second(s)

  Last reset at 698150 usecs after Thu Mar 18 12:46:49 2010
    Reason: Reset Requested by CLI command reload
    System version: 3.3(4a)
    Service:


JVSL-MDS9140#
```

ブレード スイッチ 3040

```
JVSL-A-CBS-01#sh ver
Cisco IOS Software, CBS30X0 Software (CBS30X0-IPBASE-M), Version 12.2(44)SE2, RELEASE
SOFTWARE (fc2) Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 01-May-08 13:43 by antonino
Image text-base: 0x00003000, data-base: 0x012C0000
ROM: Bootstrap program is CBS30X0 boot loader
BOOTLDR: CBS30X0 Boot Loader (CBS30X0-HBOOT-M) Version 12.2(25r)SEF2, RELEASE SO
FTWARE (fc1)
```

```
JVSL-A-CBS-01 uptime is 1 week, 6 days, 22 hours, 26 minutes
System returned to ROM by power-on
System image file is "flash:cbs30x0-ipbase-mz.122-44.SE2/cbs30x0-ipbase-mz.122-4
4.SE2.bin"

cisco WS-CBS3040-FSC (PowerPC405) processor (revision C0) with 0K/12280K bytes o
f memory.
Processor board ID FOC1320H08S
Last reset from power-on
2 Virtual Ethernet interfaces
16 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:1B:90:BC:8F:00
Motherboard assembly number     : 73-10944-01
Motherboard serial number       : FOC13202PYD
Model revision number           : C0
Motherboard revision number     : A0
Model number                    : WS-CBS3040-FSC
Daughterboard assembly number   : 73-10432-05
Daughterboard serial number     : FOC13203KJ8
System serial number            : FOC1320H08S
Top Assembly Part Number        : 800-28252-01
Top Assembly Revision Number    : D0
Version ID                      : V01
CLEI Code Number                : COUIAFKCAA
Daughterboard revision number   : A0
Hardware Board Revision Number  : 0x01


Switch Ports Model              SW Version            SW Image
------ ----- -----              ----------            ----------
*    1 16    WS-CBS3040-FSC     12.2(44)SE2           CBS30X0-IPBASE-M


Configuration register is 0xF

JVSL-A-CBS-01#
```

Show Running-config

```
JVSL-A-CBS-01#sh run
Building configuration...

Current configuration : 2736 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname JVSL-A-CBS-01
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$8lJz$jphfVgrLWUjUSuxoFTeAO.
!
no aaa new-model
system mtu routing 1500
link state track 1
ip subnet-zero
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface Port-channel10
 description "Po10 to JVSL-A-N5K-01"
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 link state group 1 upstream
!
interface GigabitEthernet0/1
 switchport access vlan 100
 speed 1000
 link state group 1 downstream
 spanning-tree portfast
!
interface GigabitEthernet0/2
```

```
 switchport access vlan 100
 speed 1000
 link state group 1 downstream
 spanning-tree portfast
!
interface GigabitEthernet0/3
 switchport access vlan 100
 speed 1000
 link state group 1 downstream
 spanning-tree portfast
!
interface GigabitEthernet0/4
 switchport access vlan 100
 speed 1000
 link state group 1 downstream
 spanning-tree portfast
!
interface GigabitEthernet0/5
 switchport access vlan 100
 speed 1000
 link state group 1 downstream
 spanning-tree portfast
!
interface GigabitEthernet0/6
 switchport access vlan 100
 speed 1000
 link state group 1 downstream
 spanning-tree portfast
!
interface GigabitEthernet0/7
 switchport access vlan 100
 speed 1000
 link state group 1 downstream
 spanning-tree portfast
!
interface GigabitEthernet0/8
 switchport access vlan 100
 speed 1000
 link state group 1 downstream
 spanning-tree portfast
!
interface GigabitEthernet0/9
 switchport access vlan 100
```

```
 speed 1000
 link state group 1 downstream
 spanning-tree portfast
!
interface GigabitEthernet0/10
 switchport access vlan 100
 speed 1000
 link state group 1 downstream
 spanning-tree portfast
!
interface GigabitEthernet0/11
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 speed 1000
 channel-group 10 mode on
!
interface GigabitEthernet0/12
 switchport access vlan 100
 switchport mode access
!
interface GigabitEthernet0/13
 switchport trunk allowed vlan 10,20,30,100
 switchport mode trunk
 channel-group 10 mode on
!
interface GigabitEthernet0/14
 no switchport
 no ip address
 no ip route-cache
!
interface GigabitEthernet0/15
 switchport access vlan 100
!
interface GigabitEthernet0/16
 switchport access vlan 100
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan100
 ip address 172.16.100.4 255.255.255.0
 no ip route-cache
```

```
!
ip default-gateway 172.16.100.1
ip classless
ip http server
!
!
control-plane
!
!
line con 0
line vty 0 4
 exec-timeout 0 0
 password 7 120B0A2D17185D5679
 login
line vty 5 15
 login
!
end

JVSL-A-CBS-01#
```

Cisco ブレード スイッチ 3040

Show Version

```
JVSL-A-CBS-02#
JVSL-A-CBS-02#sh ver
Cisco IOS Software, CBS30X0 Software (CBS30X0-IPBASE-M), Version 12.2(44)SE2, RE
LEASE SOFTWARE (fc2) Copyright (c) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 01-May-08 13:43 by antonino
Image text-base: 0x00003000, data-base: 0x012C0000

ROM: Bootstrap program is CBS30X0 boot loader
BOOTLDR: CBS30X0 Boot Loader (CBS30X0-HBOOT-M) Version 12.2(25r)SEF2, RELEASE SO
FTWARE (fc1)

JVSL-A-CBS-02 uptime is 3 weeks, 4 days, 16 hours, 36 minutes
System returned to ROM by power-on
System image file is "flash:cbs30x0-ipbase-mz.122-44.SE2/cbs30x0-ipbase-mz.122-4
4.SE2.bin"

cisco WS-CBS3040-FSC (PowerPC405) processor (revision C0) with 0K/12280K bytes o
f memory.
```

```
Processor board ID FOC1320H08H
Last reset from power-on
2 Virtual Ethernet interfaces
16 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:1B:90:BC:A1:00
Motherboard assembly number     : 73-10944-01
Motherboard serial number       : FOC13202PY5
Model revision number           : C0
Motherboard revision number     : A0
Model number                    : WS-CBS3040-FSC
Daughterboard assembly number   : 73-10432-05
Daughterboard serial number     : FOC13203KJ7
System serial number            : FOC1320H08H
Top Assembly Part Number        : 800-28252-01
Top Assembly Revision Number    : D0
Version ID                      : V01
CLEI Code Number                : COUIAFKCAA
Daughterboard revision number   : A0
Hardware Board Revision Number  : 0x01


Switch Ports Model              SW Version            SW Image
------ ----- -----              ----------            ----------
*    1 16                      WS-CBS3040-FSC     12.2(44)SE2          CBS30X0-IPBASE-M


Configuration register is 0xF

JVSL-A-CBS-02#
```

Show Running-configuration

```
JVSL-A-CBS-02#sh run
Building configuration...

Current configuration : 2355 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
service password-encryption
!
hostname JVSL-A-CBS-02
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$aQrM$dcXSlIu10S214wmifz2Lw1
!
no aaa new-model
system mtu routing 1500
link state track 1
ip subnet-zero
ip routing
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface Port-channel10
 description "L2_PC_TO_JVSL-A-N2K-02"
 switchport mode trunk
 link state group 1 upstream
!
interface GigabitEthernet0/1
 switchport access vlan 100
 link state group 1 downstream
 spanning-tree portfast
!
interface GigabitEthernet0/2
 switchport access vlan 100
 link state group 1 downstream
 spanning-tree portfast
!
interface GigabitEthernet0/3
 switchport access vlan 100
 link state group 1 downstream
 spanning-tree portfast
!
interface GigabitEthernet0/4
```

```
 switchport access vlan 100
 link state group 1 downstream
 spanning-tree portfast
!
interface GigabitEthernet0/5
 switchport access vlan 100
 link state group 1 downstream
 spanning-tree portfast
!
interface GigabitEthernet0/6
 switchport access vlan 100
 link state group 1 downstream
 spanning-tree portfast
!
interface GigabitEthernet0/7
 switchport access vlan 100
 link state group 1 downstream
 spanning-tree portfast
!
interface GigabitEthernet0/8
 switchport access vlan 100
 link state group 1 downstream
 spanning-tree portfast
!
interface GigabitEthernet0/9
 switchport access vlan 100
 link state group 1 downstream
 spanning-tree portfast
!
interface GigabitEthernet0/10
 switchport access vlan 100
 link state group 1 downstream
 spanning-tree portfast
!
interface GigabitEthernet0/11
 switchport mode trunk
 channel-group 10 mode on
!
interface GigabitEthernet0/12
 no switchport
 ip address 10.78.240.43 255.255.255.0
!
interface GigabitEthernet0/13
```

```
 switchport mode trunk
 channel-group 10 mode on
!
interface GigabitEthernet0/14
!
interface GigabitEthernet0/15
!
interface GigabitEthernet0/16
!
interface Vlan1
 no ip address
!
interface Vlan100
 ip address 172.16.100.5 255.255.255.0
!
ip default-gateway 172.16.100.1
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.100.1
ip http server
!
!
control-plane
!
!
line con 0
line vty 0 4
 password 7 00161C3C01485A545C
 login
line vty 5 15
 login
!
end

JVSL-A-CBS-02#
```

サーバ ハードウェアおよびソフトウェアの詳細

表 E-1　CAS および HT ロール サーバ

ブレード サーバ	Fujitsu BX620 S5
CPU	2 Intel Xeon E5560 2.80 GHz
メモリ	16 GB
ディスク サイズ	2 × 146 GB SAS 15K RPM（RAID-1）
RAID	RAID 1（Local ブート）
HBA	Emulex BX600-FC42E、ドライバ：7.2.20.006、ファームウェア：2.72A2
O/S	Windows Server 2008 SP2 Enterprise Edition（英語版）
MS Exchange	MS Exchange 2007 SP1

表 E-2　アクティブおよびパッシブ メール サーバ

ブレード サーバ	Fujitsu BX620 S5
CPU	2 Intel Xeon E5560 2.80 GHz
メモリ	16 GB
ディスク サイズ	2 × 146 GB SAS 15K RPM（RAID-1）
RAID	RAID 1（Local ブート）
HBA	Emulex BX600-FC42E、ドライバ：7.2.20.006、ファームウェア：2.72A2
O/S	Windows Server 2008 SP2 Enterprise Edition（英語版）
MS Exchange	MS Exchange 2007 SP1
ブレード サーバ	Fujitsu BX620 S5

ストレージ設定の詳細

次に、Exchange クラスタ ノードのパスと LUN の詳細を示します。

```
DISKPART> list disk
Disk ### Status Size Free Dyn Gpt
Disk 0 Online 136 GB 112 GB
* Disk 1 Reserved 30 GB 0 B
Disk 2 Reserved 100 GB 0 B
Disk 3 Reserved 100 GB 0 B
DISKPART> select disk 1
Disk 1 is now the selected disk.
DISKPART> detail disk
HITACHI OPEN-V Multi-Path Disk Device
Disk ID: C3719FCB
Type : FIBRE
Bus : 0
```

```
Target : 0
LUN ID : 0
Read-only : No
Boot Disk : No
Pagefile Disk : No

Hibernation File Disk : No
Crashdump Disk : No
Volume ### Ltr Label Fs Type Size Status Info
---------- --- ----------- ----- ---------- ------- --------- --------
Volume 1 D Cluster-Dis NTFS Partition 30 GB Healthy
DISKPART> select disk 2
Disk 2 is now the selected disk.
DISKPART> detail disk
HITACHI OPEN-V Multi-Path Disk Device
Disk ID: A490CC79
Type : FIBRE
Bus : 0
Target : 0
LUN ID : 1
Read-only : No
Boot Disk : No
Pagefile Disk : No
Hibernation File Disk : No
Crashdump Disk : No
Volume ### Ltr Label Fs Type Size Status Info
---------- --- ----------- ----- ---------- ------- --------- --------
Volume 2 G Log-file-di NTFS Partition 100 GB Healthy
DISKPART> select disk 3
Disk 3 is now the selected disk.
DISKPART> detail disk
HITACHI OPEN-V Multi-Path Disk Device
Disk ID: B7EF4130
Type : FIBRE
Bus : 0
Target : 0
LUN ID : 2
```