Citrix XenDesktop 5 を使用したシスコの仮想化エクスペリエンス インフラストラクチャ

「Cisco Validated Design」

2011 年 6 月 30 日

【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。

Copyright © 2011 Cisco Systems, Inc. All rights reserved

目次

目次 2
このマニュアルについて 8
マニュアルの目的 8
質問と回答 10
変更点 11
更新履歴 11
はじめに 11
仮想化：デスクトップの保護 11
プラットフォーム非依存 12
課題 12
Cisco VXI とは 13
デスクトップ仮想化 14
概要 14
仮想デスクトップ上でのユーザ エクスペリエンス 16
ユーザ入力の応答時間（マウスとキーボードの応答）16
アプリケーションの応答時間 16
表示品質 16
インタラクティブ マルチメディア 17
デスクトップ認証 18
ローカル デバイス 19
USB リダイレクト 19
印刷 20
ローカル ドライブ 20
ディスプレイ プロトコルとコネクション ブローカ 20
DV 用ハイパーバイザ 22
仮想デスクトップのホスティング 24
コンピューティング 25
ネットワーク 25
ストレージ 26
一般的な DV 導入 27
作業負荷、ピーク作業負荷、およびそれらが設計に与える影響 28
作業負荷 28
ピーク作業負荷 28
Citrix DV 29
Hosted Shared デスクトップ 31
企業の DV ポリシーとユーザ プロファイル 32
関連情報 33

導入モデル 34
Cisco VXI：新しいユーザ導入 36
集中管理された仮想ユーザ コンピューティング 38
ユーザ ネットワーク接続 39
接続の変化 39
データセンター 45
コンピューティング 48
Cisco VXI 内のコンピューティング サブシステムの最適化 50
ファブリック インターコネクトとスイッチング 51
VMware vSphere ハイパーバイザ 52
vSphere 用の仮想スイッチング：Cisco Nexus 1000v 54
vSphere 用の VM ベースのセキュリティ ゾーン：Cisco Virtual Security Gateway 55
vSphere 用の VM ベースのネットワーク最適化：Cisco vWAAS 56
ストレージ 58
ストレージ エリア ネットワーク 58
ネットワーク アタッチド ストレージ 59
共有ストレージに関する Cisco VXI の一般的なガイダンス 60
EMC Unified Storage の実装 61
NetApp FAS3170 ストレージの実装 62
直接接続ストレージ 63
ストレージとパフォーマンスの最適化用の Atlantis ILIO 63
Atlantis ILIO の検証 64
Cisco UCS サーバを使用した Atlantis ILIO の導入オプション 65
サーバ、スイッチ、ストレージ、およびハイパーバイザの統合 65
関連情報 70
VXI ネットワーク 71
VXI ネットワークについて 71
VXI ネットワーク コンポーネント 71
キャンパス 72
エンドポイントへの電力供給 73
自動ポート プロビジョニング 73
QoS 74
エンドポイント アクセスの保護 74
ロケーション：エンドポイント トラッキング 74
キャンパス アクセスの可用性 75
ブランチ内での Cisco VXI 76
Cisco VXI 内でのダイナミック VPN 76
VXI トラフィック向けの WAN 最適化 77
WAAS の導入 79
WAN の変動とパス最適化 81

ブランチ内での VXI エンドポイント アクセス サービス 82
テレワーカー 82
VXI データセンター エッジ 84
ロード バランシング、SSL オフロード、および VXI ヘルス モニタリング 84
VPN の終端 85
VXI ネットワークに関する導入と設定のベスト プラクティス 86
WAAS 86
PoE+ 87
ハイ アベイラビリティ：ISSU 87
AutoSmart ポート 87
ロケーション トラッキング 88
トラッキング 89
PfR 89
DMVPN 90
ACE 91
関連情報 93
エンドポイントとアプリケーション 94
DV エンドポイント 95
ゼロ クライアント 96
シン クライアント 96
シック クライアント 96
Cisco Virtual Experience Client デスクトップ仮想化エンドポイント 97
Cisco Cius による DV エンドポイント 98
Apple iPad による DV エンドポイント 105
DV エンドポイント管理 105
DV エンドポイントでの印刷（ネットワーク プリンタ）106
DV エンドポイントから USB 接続の周辺機器（ストレージまたはプリンタ）へのアクセス 106
DV テスト対象エンドポイント 107
Cisco VXI システム 108
Cisco Unified Communications アプリケーション 110
VXC および UC エンドポイントのシングル サインオン 113
Cisco Unified Personal Communicator、HVD、および SRST 113
Cisco VXI システム アプリケーションによる UC コラボレーションの有効化 115
関連情報 116
管理と運用 116
Cisco VXI の管理と運用のアーキテクチャ 117
スケーラビリティ 118
ハイ アベイラビリティ 118
管理トラフィック 119

デスクトップ管理 119
エンドポイント管理 121
Cisco VXI 管理ツールの概要 121
データセンターとアプリケーション 121
ネットワーク インフラストラクチャ 123
デスクトップ仮想化エンドポイント 124
ユニファイド コミュニケーション 125
Cisco VXI の管理タスクとワークフロー 126
Cisco VXI 管理ツール 133
VMware vCenter と vSphere 133
Citrix XenDesktop 5.0 管理スイート 135
Citrix XenApp Delivery Services Console 140
Cisco VXC Manager 142
Wyse Device Manager 149
Devon シン クライアント管理 152
IGEL Universal Management Suite 153
EMC Unisphere 管理スイート 154
NetApp Virtual Storage Console および StorageLink 156
Cisco NAM 157
Cisco NetFlow 161
Cisco EnergyWise Orchestrator 165
Cisco VXI 仮想デスクトップのアセスメントおよびモニタリング 172
デスクトップ管理ツール 174
Cius 管理ツール 175
関連情報 182
Cisco VXI セキュリティ 184
はじめに 184
設計上の考慮事項 186
アクセス セキュリティ 186
ネットワーク セキュリティ 188
データセンター セキュリティ 189
Cisco VXI セキュリティ コンポーネントの導入と設定のベスト プラクティス 192
ACS と連携した AnyConnect 3.0、Dot1x、MacSec、および MAB 192
エンドポイントのサポート 194
DMVPN 195
N1K 195
VSG 196
Cisco VXI のアンチウイルス ソリューション 198
関連情報 199

Quality of Service 199
QoS マーキングの表 200
データセンター 201
マーキング 201
Cisco Unified Computing System のパフォーマンスを最適化するためのキューイング 202
ネットワーク 202
エンドポイント 203
関連情報 204
パフォーマンスとキャパシティ 204
コンピューティングとストレージのキャパシティ プランニング 205
ユーザ作業負荷プロファイル 206
現在の環境でのリソース使用率 206
仮想化環境でのリソース要件の概算 207
CPU の概算 207
メモリの概算 209
サーバ キャパシティの概算 211
一般的な考慮事項 212
オペレーティング システム ディスク 215
シン プロビジョニングと シック プロビジョニング 215
ストレージ フットプリントの削減 216
パーティションの調整 216
ストレージ ネットワークの考慮事項 217
ゲスト OS の最適化 217
キャパシティの概算値の検証 218
作業負荷の考慮事項 219
単一サーバのスケールおよびパフォーマンス結果 221
作業負荷プロファイル：Cisco VXI Knowledge Worker+ 222
ESXi 上の XenDesktop 5（XD5）223
HyperV 2008 R2 上の XenDesktop 5（XD5）：Windows 7（64 ビット）228
ESXi 上の McAfee MoveAV、XD5 搭載 233
McAfee VSE サーバ統計 235
Hyper-V 2008 R2 上の XenDesktop 5（XD5）：Windows XP 239
XenServer 5.6 FP1 上の XenDesktop 5（XD5）244
アプリケーション特性評価の結果 248
XenDesktop 5 と ESXi 4.1 を使用したデスクフォン モードの Cisco Unified Personal Communicator 8.5 249
XenDesktop 5 と ESXi 4.1 を使用したデスクフォン モードの Cisco Unified Communications Integration for Microsoft Office Communicator 8.5 250
XenDesktop 5 と ESXi 4.1 を使用した Cisco UC Integration for WebEx Connect 7 251

WAN のキャパシティ プランニング 255
ネットワーク特性評価の結果 257
VDI 作業負荷の帯域幅特性：Cisco VXI KW+ 作業負荷 258
ビデオ専用 VDI 作業負荷の帯域幅特性 262
プロトコルの適応性がサーバ パフォーマンスに与える影響 265
重要事項のまとめ 267
導入後のパフォーマンス モニタリング 267
関連情報 268
略語 269
その他の資料 269
付録 1：Microsoft Hyper V 使用時の特別な考慮事項 275
Hyper-V の概要 275
Hyper-V のアーキテクチャと機能の概要 275
Hyper-V の主な機能 277
仮想マシンの管理 279
System Center Virtual Machine Manager（Virtual Machine Manager）279
Virtual Machine Manager サーバ 279
Virtual Machine ライブラリ サーバ 280
Virtual Machine Manager データベース 280
Virtual Machine Manger Administrator Console 281
仮想マシン ホスト 281
オプションの Virtual Machine Manager コンポーネントと機能 282
フェールオーバー クラスタリングと Hyper-V 282
Citrix XenDesktop 5 と Microsoft Hyper-V を使用した Cisco VXI 286
管理と運用 286
Microsoft Hyper-V 管理スイート（SCVMM）286
ハイパーバイザおよび仮想デスクトップでのリソース使用状況の監視 288
参考資料 288
付録 2：Citrix XenServer 使用時の特別な考慮事項 288
Cisco Validated Design 290

このマニュアルについて

この Cisco Validated Design ガイドでは、エンドツーエンドの Cisco® Virtualization Experience Infrastructure（Cisco VXI; Cisco 仮想化エクスペリエンス インフラストラクチャ）を導入する際の設計上の考慮事項とガイドラインについて説明します。このガイドは、Citrix XenDesktop システムを使用した Cisco 仮想化エクスペリエンス インフラストラクチャの実装を検討しているネットワーク エンジニアと設計者を対象にしています。

このガイドでは、システム全体を説明しており、章ごとにサブシステムの説明がまとめられています。これらの章では、主要な機能グループ（データセンター、ネットワーク、エンドポイントなど）と、一般的なシステム機能（管理、セキュリティ、Quality of Service など）が説明されています。

各章は、Citrix XenDesktop を使用した Cisco 仮想化エクスペリエンス インフラストラクチャをモジュール形式で説明するように編成されています。

マニュアルの目的

このマニュアルでは、エンドツーエンドの Cisco Virtualization Experience Infrastructure（Cisco VXI; Cisco 仮想化エクスペリエンス インフラストラクチャ）を導入する際の設計上の考慮事項とガイドラインについて説明します。Cisco VXI システムは、ユーザのコンピューティング環境をデータセンター内に設置することにより、さまざまなエンドポイントからのアクセスを可能にし、コラボレーション ツールと統合させ、高品質なユーザ エクスペリエンスを実現します。

システム全体が説明されており、各サブシステムの説明が、個別の章にグループ化されています。このグループ化は、主要な機能グループ（データセンター、ネットワーク、およびエンドポイント）と一般的なシステム機能（管理、セキュリティ、および Quality of Service）に沿って行われています。

各章は、Cisco VXI システムをモジュール形式で説明するように編成されています。表 1 に、各章またはモジュールの説明を示します。

表 1　　章またはモジュールの説明

章またはモジュールの見出し	説明
「はじめに」	この章では、仮想化環境の検討に至るビジネスの推進要因と Cisco VXI の使用例を結び付けます。
「デスクトップ仮想化」	この章では、Citrix XenDesktop を使用したコアの仮想デスクトップ インフラストラクチャ システムの導入に関する設計ガイダンスを示します。
「導入モデル」	この章では、導入トポロジを、ホストされるコンピューティング リソースと関連付けながらユーザ ロケーションに基づいて分類します。ネットワーク接続とコンピューティング リソースの位置の主要な特徴を示して、設計上の考慮事項を説明します。コンピューティングとネットワーキングの負荷の変化が例示されます。
「データセンター」	この章では、的確かつ限定された一連のラボラトリ ストレージ ステージングに対するテストから導かれた、ストレージ サブシステムに関する一般的な設計ガイダンスを提供します。

章またはモジュールの見出し	説明
「VXI ネットワーク」	この章では、特定の製品とテクノロジーを使用してデスクトップ仮想化エクスペリエンスを向上させるネットワークベースのサービスについて説明します。また、キャンパス WAN およびブランチ ネットワーク内で対象のネットワーク機能を導入する際のベスト プラクティスに関する具体的な推奨事項も提供します。
「エンドポイントとアプリケーション」	この章では、DV とコラボレーション エンドポイントの選択肢について明らかにし、仮想化デスクトップ内での特定のアプリケーションの導入と使用に関するガイダンスも提供します。また、デスクトップ仮想化ユーザ エクスペリエンス内への UC 機能の統合に関するガイダンスも提供します。
「管理と運用」	この章では、VXI サブシステム コンポーネントをサポートしているさまざまな管理プラットフォームを示します。また、VXI システムを運用するために必要な共通の管理タスクのワークフローも提供します。
「Cisco VXI セキュリティ」	この章では、VXI システムを保護するために実装される機能とポリシーについて重点的に説明します。
「Quality of Service」	この章では、VXI トラフィック フローの分類、優先順位付け、適切なプロビジョニングに必要な記述的なプロトコル特性についてまとめて示します。
「パフォーマンスとキャパシティ」	この章では、VXI システムのコンピューティング、ストレージ、およびネットワーキングのサイズ決定に関する設計ガイダンスを提供します。
「略語」	略語一覧。
「その他の資料」	関連情報へのリンクの一覧。
「付録 1：Microsoft Hyper V 使用時の特別な考慮事項」	Microsoft Hyper V を使用する際の特別な考慮事項。
「付録 2：Citrix XenServer 使用時の特別な考慮事項」	Citrix XenServer を使用する際の特別な考慮事項。

ここで参照として記載される Cisco VXI システムは、設計でサポートされるコンポーネント全体を表します。なお、ここで記載されるコンポーネントは、具体的に設計での使用を推奨しているわけではありません。たとえば、リファレンス アーキテクチャのテストで特定のアクセス スイッチング製品群が使用されていたとしても、それ以外のアクセス スイッチング製品が Cisco VXI システムに適合しないことを意味するわけではありません。必要な場合は、具体的なコンポーネント要件が明確に示されます。

Cisco VXI システムは、多数のサブシステムの上に構築されます。ほとんどのお客様は、これらのサブシステムの多くをすでに導入済みです。たとえば、お客様のほとんどは、ルーティングとスイッチングのインフラストラクチャをすでに設置済みであると考えられます。このマニュアルは、VXI 機能の実装に向けて既存のインフラストラクチャを増強するために必要な VXI 固有の設計ガイダンスに重点を置いています。

このマニュアルでは、ルーティング、スイッチング、セキュリティ、ストレージ、および仮想化についてすべての基本テクノロジーと参照設計を扱っているわけではありません。詳細については、それらのテクノロジーや参照設計について記載しているマニュアルを参照してください。

Cisco VXI システムは、さまざまなベンダーが提供するサブシステムの統合の上に構築されます。そのため、他のベンダーの製品およびシステムに関する参照資料が提供されています。本書の公開時点でこれらの参照資料が正確になるように最善を尽くしてはいますが、ベンダーの製品または設計ガイダンスの変更により、このガイド内の参照資料が古くなっている場合があります。そのような状態を見つけられた場合は、シスコまでご連絡ください。

質問と回答

表 2 に、Cisco VXI Certified Validated Design に関してよく寄せられる質問と、それに対して回答しているセクションへのリンクを示します。

表 2　　Cisco VXI に関してよく寄せられる質問

質問	回答
VXI システムのサイズは、ユーザ数に基づいてどのように決定されますか。	「パフォーマンスとキャパシティ」の章の「サーバ キャパシティの概算」のセクションに、CPU、メモリ、およびストレージの要件に関する設計ガイダンスが示されています。
ユニファイド コミュニケーション機能は、VXI システム内でユーザ エクスペリエンスにどのように統合されますか。	「エンドポイントとアプリケーション」の図 49 を参照してください。
Cisco WAAS は、ネットワーク フローにどのように挿入されますか。	「VXI ネットワーク」の「ACE」のセクションを参照してください。
DV エンドポイントからホステッド仮想デスクトップまでの接続に関係する主要な構成要素は何ですか。	「デスクトップ仮想化」の章の「ディスプレイ プロトコルとコネクション ブローカ」のセクションに、接続フローが説明されています。
主要なデスクトップ仮想化エンドポイント タイプは何ですか。	「エンドポイントとアプリケーション」の章の「デスクトップ仮想化エンドポイント」のセクションを参照してください。
さまざまな VXI トラフィック タイプに対してどのような Quality of Service（QoS）特性がありますか。	VXI に関連したプロトコルの QoS マーキングの詳細については、「Quality of Service」の章にある表 30 を参照してください。
デスクトップ仮想化の採用により、PC 環境の場合と比べてトラフィック フローにどのような変化が起きますか。	「導入モデル」の「集中管理された仮想ユーザ コンピューティング」のセクションを参照してください。
支店にデスクトップ仮想化ユーザを配置するために必要な WAN 帯域幅のサイズを決定する際に考慮することは何ですか。	「パフォーマンスとキャパシティ」の章を参照してください。
他にどのような VXI 関連資料がありますか。	その他の参考資料へのリンクが各章の最後にあります。また、このマニュアルの最後のセクションにもあります。
Cisco Wide Area Application Services（WAAS）によって最適化可能なトラフィック タイプは何ですか。	「VXI ネットワーク」の「VXI トラフィック向けの WAN 最適化」のセクションにある表 6 に、VXI に関連した主なトラフィック タイプが一覧され、Cisco WAAS で利用できる最適化機能が示されています。

質問	回答
データセンター内で VXI を導入する際にどのような Virtual Local Area Network（VLAN; 仮想ローカル エリア ネットワーク）設計を考慮する必要がありますか。	「データセンター」の表 4 に、VXI の導入に必要な VLAN のリストが示されています。
VXI システムのテストにはどのような作業負荷プロファイルを使用しましたか。	「パフォーマンスとキャパシティ」に、VXI システムのテストに使用されたユーザ プロファイルの詳細が説明されています。

変更点

ここで提供される情報は、最初に公開された Cisco VXI Design Guidance に関するものです。

更新履歴

このマニュアルは、2011 年 4 月 29 日に初めて公開されました。改訂が行われると、その内容がこのセクションに記載されます。

はじめに

デスクトップ仮想化の主な目的は、ユーザ エクスペリエンスの品質を損なうことなく、セキュリティを強化し、ビジネスの俊敏性を向上させながら、総所有コストを削減することです。

仮想化：デスクトップの保護

集中管理された Desktop Virtualization（DV; デスクトップ仮想化）では、ユーザのデスクトップ環境を、データセンターベースの仮想インフラストラクチャ内でホストします。

デスクトップ関連の IT 投資のほとんどが集中化されるので、企業のコンピューティング資産の管理と運用が簡素化されます。エンドポイントは、より安価で、メンテナンスが簡単になります。こうしたコストの削減は、設備投資（DV エンドポイントの購入コストは通常のラップトップやデスクトップの購入コストを下回ります）と複雑な「シック」エンドポイントの運用にまつわる運用コストの両方に適用されます。たとえば、ソフトウェア資産の追跡、ライセンス管理、パッチ適用、バックアップ（時間コスト面と帯域幅コスト面の両方）、障害回復などが簡単になります。仮想化デスクトップ環境の場合、エンドポイントの障害発生は、主としてハードウェア交換の問題となり、ユーザのファイルとデスクトップ環境はデータセンターの仮想化環境内に障害の影響を受けることなく残されます。

データ セキュリティが向上します。ユーザは、通常のデスクトップ環境を通じて接続しているかのようにデータにアクセスできます。しかし実際のデータは、ユーザのエンドポイントに配信も保管もされません。データは単にリモートで表示されているだけです。これにより、セキュリティの観点から 2 つの重要な利点がもたらされます。

- 電子データの漏洩を制御できます。ユーザのコンピューティング エンドポイントには、CD/DVD ドライブや USB 接続メモリなどの取り外し可能なストレージ メディアを装備できる場合があります。しかし、これらのデバイスをユーザが利用できるかどうかは、集中管理で適用されるポリシーによって制御されます。ユーザはファイルにアクセスする権限はあっても、そのファイルを取り外し可能な電子メディアにコピーする手段はありません。

- コンピューティング エンドポイントの紛失、破損、または盗難により、データが影響を受けることはありません。通常のラップトップには、悪用されると企業に損害を与える可能性のあるファイルが多数保管されています。また、1 台のラップトップに構想中の素晴らしいアイデアを保存している従業員は、そのラップトップが破損または盗まれると、そのラップトップの価値を超える損失を被ることになります。一方、仮想化されたエンドポイントには、企業のデータは保管されていません。したがって、紛失または破損しても、リモート コンピューティング エンドポイント内のファイルが失われたり、破壊されたり、漏洩したりすることはありません。すべての重要なデータは中央に配置されているため、エンドポイントの破損や盗難の後もその影響を受けることはありません。この利点は、ユーザのコンピューティング エンドポイントが、実際は DV クライアントを実行している「シック」ラップトップである場合でも有効です。ユーザは自分の作業を行うために従来のラップトップを必要とする場合があります。しかしその場合でも、機密性の高いコンピューティング リソースは、仮想デスクトップでリモートにホストすることができます。

プラットフォーム非依存

エンドポイントは、スマートフォン、タブレット コンピューティング プラットフォーム、ラップトップ コンピュータ、デスクトップ コンピュータなど、拡大を続けるデバイス リストの中から選択できます。これらには、多数のオペレーティング システムが含まれます。仮想化により、企業は、複数のデバイスにわたって一貫性のあるユーザ エクスペリエンスを提供できます。従業員は、日中にさまざまなエンドポイントから自分のデスクトップ環境にアクセスできるようになります。たとえば、本社で作業しているときはデスクトップ コンピュータから、リモート ブランチ オフィスに出張しているときはシン エンドポイントから、社内を移動しているときはタブレットからアクセスできます。在宅勤務の場合であっても、パーソナル コンピュータと VPN クライアントを使用することで、従業員に企業へ「接続」する手段を提供することができます。

課題

ユーザの IT 環境は、デスクトップ内にすべてが収容されているわけではありません。音声とビデオのテレフォニーや印刷サービスなどのコラボレーション ツールは、DV テクノロジーではユーザが満足するレベルで提供できない場合があります。

たとえば、音声、ビデオ、およびインタラクティブ マルチメディア リソースに仮想デスクトップ内からリモートでアクセスすると、WAN 帯域幅などの IT インフラストラクチャに対する需要が増加するとともに、パフォーマンスのレベルが低下する可能性があります。電話による通話は、リモート デスクトップ内から発信され、リモート デスクトップのディスプレイ プロトコル内で伝送される場合、ネットワークベースのトラフィックの優先順位付けが行われずに、ユーザのコンピューティング エンドポイントに接続される可能性があります。したがって、ネットワークの QoS 機能は、遅延、ジッタ、およびパケット ドロップに起因する品質の低下を防ぐために必要な特別な処理を、音声メディアに対して実質的に提供できなくなります。また、インタラクティブ マルチメディア コンテンツのストリーミングは、DV エンドポイントの帯域幅使用量を増大させる可能性があります。それにより、そのメディアの視聴者のエクスペリエンスだけでなく、同じ WAN 接続を利用している他の共存ユーザのエクスペリエンスも品質が低下する可能性があります。

Cisco VXI とは

Cisco 仮想化エクスペリエンス インフラストラクチャは、次の方法でデスクトップ仮想化を強化します。

Cisco Unified Communications への統合

ユーザは、Hosted Virtual Desktop（HVD; ホステッド仮想デスクトップ）と接続して、Cisco Unified Personal Communicator から音声コールまたはビデオ コールの発信と受信ができるようになります。Cisco Unified Personal Communicator は、ユーザのデスクフォンに対するコントローラとして機能します。電話機のコントロール プレーンは、ユーザのデスクトップに統合されます。ただし、メディア プレーンはデスクフォンの場合と同じです。メディア トラフィックは、リモート デスクトップ ディスプレイ プロトコルの外部で接続されます。したがって、ネットワークは、Real-Time Transport Protocol（RTP）パケット優先付け、コール アドミッション制御、パス最適化などの Quality of Service（QoS）機能を実行できます。たとえば、同じブランチ内の 2 人の Cisco VXI ユーザは互いに通話できます。また、コントロール（シグナリング）プレーンがデータセンター内に存在する間は、ユーザ間の音声接続がブランチから出ていくことはありません。ブランチ ネットワークではパケットの優先順位付けが RTP フローに適用され、2 台の電話機は相互に直接接続されます。音声は、データセンターに到達する必要がないため、WAN を 2 回通過する必要がなくなります。エンドポイントが音声専用であろうと、ビデオに対応していようと、これと同じアプローチが適用されます。

Cisco Unified Computing System 仮想化コンピューティング プラットフォームによって簡素化された設定

Cisco Unified Computing System™ は、通常は別々のプラットフォームに存在するコンピューティング機能、仮想化ハイパーバイザ機能、ファブリック インターコネクト機能、およびストレージ機能を統合します。こうした統合により、データセンターのパフォーマンスと管理性の両方が向上します。たとえば、Cisco Nexus® 1000V 仮想イーサネット モジュールは、スイッチング機能、トラフィック分離機能、およびポリシー挿入機能を仮想化環境内に設置します。したがって、2 台の仮想コンピュータ（レイヤ 2 ポリシーに従って接続されなければならない）は、物理的なスイッチング インフラストラクチャによってフレームをスイッチングしなくても、仮想化環境内で直接通信できます。また、特定のファイル システムにユーザが接続できないようにする場合は、シスコの仮想化スイッチング プラットフォームを使用することにより、仮想化環境内でポリシーを直接適用できます。

ネットワーク最適化

現在使用されているアプリケーションの多くは、ベースとなるネットワーク プロトコルがネットワーク帯域幅を節約するように最適化されていないため、帯域幅制限やネットワーク遅延が存在するとパフォーマンスが低下する可能性があります。Cisco Wide Area Application Services（WAAS）テクノロジーは、帯域幅使用量の削減によりアプリケーションの応答時間を改善することで、アプリケーションのパフォーマンスを向上させます。たとえば、データセンター内のユーザの仮想デスクトップから、リモート ブランチのネットワーク プリンタに対してリモート印刷動作を開始させる場合があります。WAAS は、印刷プロトコルを自動的に認識し、WAN 帯域幅使用量を削減するように印刷プロトコルを圧縮することができます。また、リモート プリンタがビジー状態であっても、印刷ファイルをリモート ブランチにスプールできます。結果として、WAN 上の帯域幅使用量が減少するとともに、ユーザに対するアプリーケンション応答時間が短縮されます。これには、ユーザ エクスペリエンスが向上すると同時に、各 WAN リンクでサービス可能なユーザ数が増加するという二重の利点があります。Cisco WAAS 機能では、その核として Transport Flow Optimization（TFO; トランスポート フロー最適化）、Data Redundancy Elimination（DRE; データ冗長性の排除）、および Lempel-Ziv（LZ）圧縮の各テクノロジーが利用されています。これらの複合効果により、帯域幅の使用効率が最大限に高められます。

セキュリティ

ネットワーク内への接続は、アクセス レイヤで制御できます。このレイヤは、デバイスが仮想インフラストラクチャに最初に接続する場所です。業界標準の 802.1X を導入して、ネットワーク アクセスをポート レベルで制御できます。したがって、シスコのアクセス スイッチは、Microsoft Active Directory などのディレクトリ サービスとの統合によって導入される資格情報ベースのアクセス コントロールと連携するだけでなく、物理レベルでセキュリティ ポリシーを適用することもできます。

テレワーカー ユーザ（ラップトップ コンピュータを使用したモバイル ユーザなど）および固定ユーザ（在宅ベースのテレワーカーなど）は、インターネット経由でエンタープライズ ネットワーク内へ接続するために、シスコの実績ある VPN テクノロジーを使用できます。ユーザの仮想デスクトップ データは、インターネットを通過するときに VPN トンネル内を暗号化されて送信されるため、完全に保護されます。このテクノロジーは、マネージド WAN を通過するトラフィックに対しても導入できます。

エンドツーエンド テスト

Cisco VXI は、エンドツーエンドのシステムであり、ネットワーク機能とコラボレーション機能を統合して仮想デスクトップ エクスペリエンスを実現します。統合されたシステム全体で設計およびテストが実施されているため、DV、コンピューティング、ネットワーキング、ストレージ、セキュリティ、最適化、ロード バランシングの各テクノロジーを孤立して導入した場合に必要となるシステム統合投資が軽減されます。

デスクトップ仮想化

概要

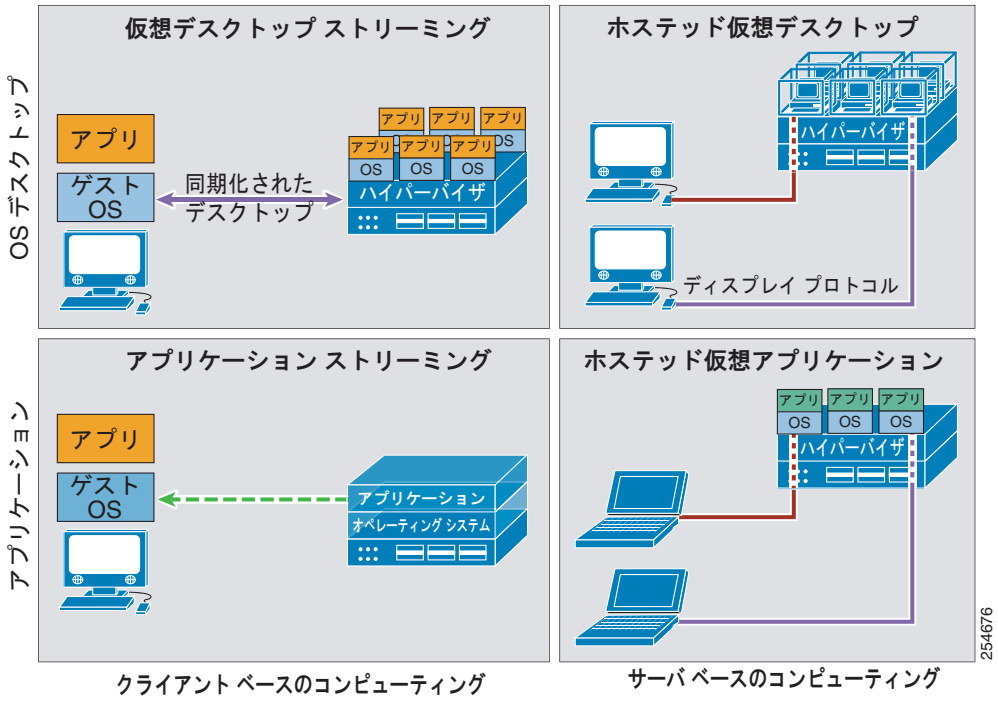
PC をベースにした現在の企業のデスクトップ環境は、高度に分散化されており、十分なコンピューティング能力とアプリケーションの柔軟性をユーザに提供しています。このようなデスクトップ モデルは、ユーザのビジネス ニーズに対して最適なものとなっています。しかし IT 部門にとっては、高い運用コスト、複雑な管理、データ セキュリティの低下という複数の課題が存在します。

Desktop Virtualization（DV; デスクトップ仮想化）テクノロジーは、IT 部門が直面している問題を、現在のユーザ エクスペリエンスを損ねることなく解決することを目指して開発されました。現在、市場ではさまざまなタイプの DV が展開されており、それぞれが異なる角度から DV に取り組んでいます。

普及している 4 つのアプローチを図 1 に示します。これらのアプローチは、処理がサーバとクライアントのいずれで行われるか、さらに、仮想化の対象がデスクトップ全体またはユーザの使用可能なアプリケーションのいずれであるかに応じて 4 つに分類されます。デスクトップ仮想化の選択が、クライアント デバイスのハードウェア要件、バックエンドのソフトウェア システムの複雑さ、ネットワーク使用率、および期待されるユーザ エクスペリエンスに強く影響します。

すべての状況に適合するものはなく、シナリオによっては複合的なアプローチも使用されますが、この Cisco Validated Design ガイドでは、主としてホステッド仮想デスクトップおよび Hosted Shared デスクトップ タイプの DV に重点を置いて説明します。Hosted Virtual Desktop（HVD; ホステッド仮想デスクトップ）と Hosted Shared Desktops（HSD; Hosted Shared デスクトップ）は、IT 部門のほとんどの要件を満たし、大多数のアプリケーションに対してローカル デスクトップと同様のユーザ エクスペリエンスを維持することから、人気が高まっています。このマニュアル内で言及しているすべての DV は、別途記載がない限り、HVD DV を意味します。この章では、主要な DV 固有のテクノロジー コンポーネントについて説明していますが、さらに説明が必要です。各コンポーネントの詳細と一般的なインストレーションの説明については、各ベンダーが提供しているドキュメントを参照してください。

図 1　デスクトップ仮想化テクノロジーの現状

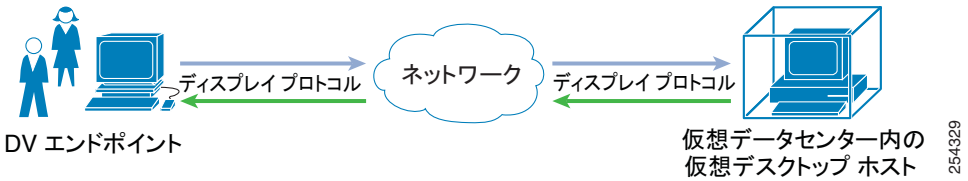


DV により、エンドユーザ エクスペリエンス（オペレーティング システム、アプリケーション、およびコンテンツ）は物理エンドポイントから抽象化されます。DV では、デスクトップ環境は、データセンター サーバ内に仮想マシンとしてホストされます。ユーザは、ラップトップ コンピュータ、シン クライアント端末、モバイル インターネット デバイス、スマートフォンを使用して、自分の仮想デスクトップにネットワーク経由でアクセスできます。どのような大規模 DV 設計でも、ユーザ アクセシビリティのニーズ、具体的なユーザ作業プロファイル、アプリケーション、および基盤となるインフラストラクチャの堅牢性を考慮する必要があります。インフラストラクチャ設計では、さらにコンピューティング、ストレージ、およびネットワーク（データセンター、キャンパス、WAN、またはインターネット）の要件も考慮します。各コンポーネントは、エンド ユーザに優れたエクスペリエンスを提供するうえで、重要な役割を果たします。

DV セッションには、エンドポイント、データセンター内の仮想マシン上で動作しているホステッド デスクトップ、および仮想デスクトップ内で動作しているソフトウェア エージェントが最低限必要です。クライアントは、仮想デスクトップ上のエージェントに対して接続を開始し、ディスプレイ プロトコルを使用してデスクトップ ユーザ インターフェイスを表示します。現実世界のシナリオでは、コネクション ブローカと呼ばれるもう 1 つのコンポーネントが、エンドポイントと仮想デスクトップの間に存在します。ブローカにより、ユーザは認証され、適切な仮想デスクトップに接続されます。

図 2 に示すように、データセンター内の仮想デスクトップとエンドポイントの間でディスプレイ データが継続的に交換され、エンドポイントと仮想化デスクトップの間でインターフェイス デバイス データ（キーボード、マウス、USB 周辺機器など）が継続的に交換されます。ネットワークは、LAN のみの環境にすることも（本社など）、WAN と LAN が混在した環境にすることもできます。一貫性のある高品質で拡張可能な DV の導入を実現するには、データセンターとデータ ネットワークを慎重に計画することが重要です。

図 2　　単純な DV セッション



仮想デスクトップ上でのユーザ エクスペリエンス

DV の重要な手順の 1 つは、優れたユーザ エクスペリエンスの主要な属性を定義することです。ユーザのタイプに応じて、実際の DV フィーチャ セットには、次の機能のサブセットが含まれます。全体的な目標は、可能な限り物理デスクトップのエクスペリエンスに近いユーザ エクスペリエンスを DV 環境内に再現することです。

ユーザ入力の応答時間（マウスとキーボードの応答）

ユーザがマウス ポインタを動かした場合、あるいはキーボードを使用して入力した場合、エンドポイント DV クライアントは、これらのコマンドをディスプレイ プロトコル内にカプセル化して送信します。HVD 内では、DV ソフトウェア エージェントがこれらのコマンドを受信し、デコードし、ゲスト オペレーティング システムに渡します。コマンドの結果（ディスプレイの変化）は、ディスプレイ プロトコルでクライアントに返送されます。HVD のコンピューティング キャパシティ、ネットワーク遅延、および帯域幅が、応答時間を目標値内に維持するうえで重要な役割を果たします。

アプリケーションの応答時間

ユーザ入力の応答時間が制限範囲内である場合、アプリケーションの応答時間は、仮想化ゲスト OS で測定される CPU、メモリ、およびストレージの Input/Output Per Second（IOPS; 1 秒あたりの I/O 処理数）の値によって決まります。物理デスクトップ上でエンドユーザが体験するのと等価なアプリケーション応答時間が、あらゆる DV 展開での目標となります。アプリケーション応答時間に非常に高い目標を設定すると、データセンター内の HVD の密度に大きく影響します。物理デスクトップ上と HVD 上のアプリケーション応答時間を比較する場合、有効な測定結果を得るには、OS のバージョンおよび基盤となるハードウェア（物理または仮想）を同じにする必要があります。

表示品質

エンド ユーザが体験する表示品質は、表示されるコンテンツ、画面解像度、および画面の更新レートに依存します。一般に DV では、解像度と更新レートが高いと、コンピューティングとネットワークの負荷が高くなります。ネットワーク内のユーザ プロファイルとユーザ ロケーションに基づいてコンピュータ リソースと帯域幅を十分に割り当てることがきわめて重要です。現在のディスプレイ プロトコルのほとんどは、複数モニタに対応しており、スパン モード（HVD から単一のディスプレイが送信され、エンドポイント上で複数のモニタに複製される）またはトゥルー マルチモニタ モード（HVD から複数のディスプレイが送信され、場合によってはそれぞれ異なる画面解像度を使用可能）を使用できます。サポートされるモードに応じて、エンドポイントや HVD のコンピューティング要件は影響を受けます。トゥルー マルチモニタ モードでは、ネットワーク帯域幅の要件の方がはるかに大きくなります。

インタラクティブ マルチメディア

現在の企業では、ビジネスの生産性を向上させるために、インタラクティブ マルチメディアが不可欠です。インタラクティブ マルチメディアには、ビデオ コンテンツの埋め込まれたコンテンツリッチな Web ページから、コラボレーションやソーシャル ネットワークのアプリケーションまで、あらゆるものが組み込まれています。コンテンツのタイプには、Flash メディア、音声、ビデオ オン デマンド、Voice over IP（VoIP）、アプリケーション ストリーミングなどがあります。DV 環境では一般に、インタラクティブ マルチメディアは、データセンター内の仮想化デスクトップから要求され、そのデスクトップ上でレンダリングされます。仮想デスクトップ上でレンダリングされた後、メディアは DV プロトコルに再び符号化され、データセンターからエンドポイントに送信されます。エンドポイントでは DV プロトコルが復号され、最終的にエンド ユーザに対して表示されます。

このシナリオでは、インタラクティブ マルチメディアが送信元からエンドポイントへ直接流れることはありません。代わりに、データセンターを経由して「ヘアピン処理」され、DV プロトコル接続によって頻繁にトンネリングされます。ストリーミング メディアとリアルタイム メディアは、インタラクティブ マルチメディアの主要な 2 つの配信手段です。データセンター内の HVD に対してそれぞれ異なる課題が存在します。

一方向のストリーミング メディアの例として、ユーザが Flash ビデオと音声の含まれる Web ページの表示を要求した場合、次の主要なイベントが発生します。

- ディスプレイ プロトコルは、少量のネットワーク帯域幅を消費して、ユーザ要求アクションを HVD に送信します。
- HVD は、ローカルのコンピューティング、メモリ、および場合によってはストレージの各リソースを消費して、ブラウザを起動します。
- Web ページをホストしている Web サーバへの接続が（おそらくインターネット経由で）開始され、ネットワーク帯域幅が消費されます。
- Web サーバから返されたコンテンツ（画像、Flash ビデオ ファイルなど）がブラウザによってダウンロードされて処理され、CPU、メモリ、ストレージの各リソースが消費されます。
- コンテンツは、HVD の仮想ディスプレイ上でレンダリングされ、DV ディスプレイ プロトコル エージェントによってキャプチャされ、エンドポイントに送信されます。これにより、コンピューティングとメモリのリソースが消費されますが、それよりも重要なこととして、ネットワーク リソース（LAN または WAN）が同じコンテンツに対して 2 回消費されるということがあります。DV ディスプレイ プロトコルは、圧縮ビデオにおいて MPEG4 などのコーデックほど効率が高くありません。そのため一般に、DV プロトコルで符号化されたビデオを再送信するために消費されるネットワーク帯域幅は、元の圧縮されたビデオ ストリームの数倍になる可能性があります。
- 最後に、エンドポイントがビデオを表示し、内蔵している音声ドライバ（サポートしている場合）を使用してインタラクティブ マルチメディアを提供します。

リアルタイム メディアには、ライブ ビデオ ストリームと双方向のビデオ/音声会議セッションがあります。例として、DV ユーザがライブ ビデオ ストリームの表示を要求した場合、次のイベントが発生します。

- ディスプレイ プロトコルは、少量のネットワーク帯域幅を消費して、ユーザ要求アクションを HVD に送信します。
- HVD は、ローカルのコンピューティング、メモリ、および場合によってはストレージの各リソースを消費して、ブラウザを起動します。
- ライブ ストリームをホストしているコンテンツ配信サーバへの接続が（おそらくインターネット経由で）開始され、データセンターのネットワーク帯域幅が消費されます。
- CDS から返されたライブ ビデオはキャッシュできません。ユーザの HVD 内の適切なビデオ コーデックを使用して復号され、CPU とメモリのリソースが消費されます。

- コンテンツは、HVD の仮想ディスプレイ上でレンダリングされ、DV ディスプレイ プロトコル エージェントによってキャプチャされ、エンドポイントに送信されます。これにより、コンピューティングとメモリのリソースが消費されるだけでなく、それよりも重要なこととして、ネットワーク リソース（LAN または WAN）が同じコンテンツに対して 2 回消費されます。DV ディスプレイ プロトコルは、圧縮ビデオにおいて MPEG4 などのコーデックほど効率が高くありません。そのため一般に、DV プロトコルで符号化されたビデオを再送信するために消費されるネットワーク帯域幅は、元の圧縮されたビデオ ストリームの数倍になる可能性があります。
- 最後に、エンドポイントがビデオを表示し、内蔵している音声ドライバ（サポートしている場合）を使用してインタラクティブ マルチメディアを提供します。

双方向のビデオ会議セッションの場合、エンドツーエンドの音声遅延とビデオ レンダリングの要件が非常に厳しくなります。ユーザの HVD では、コンテンツの受信、処理、ディスプレイ プロトコルによる送信準備といったプロセスにより、遅延がさらに増大します。満足なユーザ エクスペリエンスを実現するには、エンドツーエンドの遅延を数ミリ秒以下に抑える必要があります。HVD は、十分な CPU、メモリ、およびネットワークのリソースを確保する必要があります。これを達成するために、音声ストリームとビデオ ストリームの間の同期を緊密にする必要があります。したがって、HVD 内の追加のコンピューティング リソースとネットワーク内の厳格な QoS 保証が必要です。

ビデオの品質と複雑さおよび音声の忠実度に応じて、使用されるリソース量は大幅に変化する可能性があります。ほとんどのインタラクティブ マルチメディア コンテンツ タイプでは、コンテンツの取得とエンド ユーザへの配信に関する一般的なプロセスは、基本的に同じになります。DV 環境内でのインタラクティブ マルチメディア配信に使用されるリソースは、従来のデスクトップ環境の何倍にもなる可能性があり、このリソース使用率は、複数のコンポーネントに波及します。さらに、地理的に分散している何千ものユーザ グループ向けに記述されたモデルを拡張する場合は、最適化に重点を置くだけでなく、入念なキャパシティ プランニングが必要になります。このモデルでは、メディアはディスプレイ プロトコルに収容され、ディスプレイ プロトコルはポイントツーポイントでなければならないので、ストリーミング メディアのマルチキャストやビデオ オン デマンドなどの高度なネットワーク機能を適用できません。現在の最適化技術では、ディスプレイ プロトコルの圧縮を使用してネットワーク帯域幅を節約するか、インタラクティブ マルチメディアをディスプレイ プロトコル自体から分離します（Multimedia Redirection（MMR; マルチメディア リダイレクト））。MMR では、ローカル エンドポイントでメディアを取得し、レンダリングすることが可能になり、マルチキャスト、キャッシング、対象を絞った圧縮などの高度なネットワーク機能を活用する機会が与えられます。

より高品位なインタラクティブ マルチメディア エクスペリエンスを高遅延 / 低帯域幅のネットワークおよび WAN でサポートするためのテクノロジーは、いまだ発展途上にあります。しかし、慎重に計画を立てることにより、日常的なビジネス ニーズには現在使用可能なテクノロジーで対応できます。

デスクトップ認証

仮想デスクトップへ移行したユーザは、エンドポイント上でログインすれば、デスクトップによるサービスが提供されるものと期待します。DV 環境内では、デスクトップに到達するために、エンドポイント上、コネクション ブローカ上、そして最終的に HVD 上での認証が必要になります。コネクション ブローカはデータセンター内で既存の Active Directory インフラストラクチャと安全に統合されているので、デスクトップ認証は、ネットワークやコンピューティングにほとんど影響せずに簡単にプロビジョニングできます。ユーザ認証情報は、ディスプレイ プロトコル内のセキュア接続経由でエンドポイントからコネクション ブローカへ渡されます。

（注） HVD 内のアプリケーションは個別に認証されます。それらのメカニズムについては DV の説明の範囲外です。

ローカル デバイス

DV 環境内でのローカル デバイスと周辺機器のサポートは、ユーザの既存のデスクトップ エクスペリエンスを維持するうえで重要な役割を果たします。周辺機器には、USB 制御のデバイス、プリンタ、ローカル ドライブ アクセスなど、日々のビジネスやユーザ エクスペリエンスに不可欠なものもあります。これらの周辺機器を DV システム内に統合する決定は、ネットワーク要件とコンピューティング要件に大きく影響するため、慎重に検討する必要があります。DV の計画策定の一環として、次のことを検討する必要があります。

- どのユーザがどの周辺機器にアクセスできるか。

  アクセスは、通常、Active Directory ポリシー、コネクション ブローカ ポリシー、およびエンドポイント ハードウェアの選択によって制御されます。Active Directory グループ ポリシーベースの制御は、HVD 内のユーザ権限に適用されます。エンドポイントは、ソフトウェア クライアントによって制御されます。ソフトウェア クライアントは、コネクション ブローカと通信して具体的なポリシーを取得します。これらのポリシーにより、USB デバイスへのアクセス、内外へデータをコピーする機能、ディスプレイ プロトコルをバイパスする機能を制御できます。利用可能なほとんどのコネクション ブローカは、これらのポリシーを Active Directory グループ ポリシーから継承する機能を備えています。

- これらのユーザ グループの位置はどこか。

  位置は、どのネットワーク セグメントが影響を受けるか判断するのに役立ちます。ほとんどのローカル周辺機器は、ネットワークの制限を考慮せずに設計されており、通常は十分なハードウェア帯域幅（Peripheral Component Interconnect Express（PCIe）拡張カード経由）と動作用のローカル コンピューティング リソースを備えています。こうしたローカル周辺機器をデータセンター内の HVD から利用できるようにする場合、制限のあるネットワーク帯域幅と遅延の増大を考慮する必要があります。たとえば、LAN 上のキャンパス ユーザに USB とローカル ドライブ アクセスを提供する場合、同じアクセスを WAN ユーザに提供するよりもネットワークに与える影響は小さくなります。

収集されるデータによっては、特定のディスプレイ プロトコルが他のものよりも優れたパフォーマンスを示すことがあります。そのため、周辺機器の最適化ソフトウェアを選択する際はそのことを考慮する必要があります。

USB リダイレクト

USB 接続のプリンタ、Web カメラ、オーディオ ヘッドセット、スキャナといった多くの新しい周辺機器は、ローカル デバイス上の USB インターフェイスを使用して接続されます。これらが DV 環境内で動作するには、エンドポイント上の DV クライアントがクライアント エンドポイント上の USB データを代行受信し、HVD にインストールされているエージェントにディスプレイ プロトコルで送信します。エージェントは、この USB デバイスとデータを新しいハードウェア デバイスとして HVD に提供します。未加工の USB データ ストリーミングには、ローカル USB コントローラのソフトウェアとハードウェアのバージョンにもよりますが、480 Mbps のネットワーク帯域幅が消費される可能性があります。また、HVD 内だけでなく、エンドポイント上でも CPU サイクルが消費されます。このような高帯域幅の要件は、ローカル クライアント上で最適化と圧縮を実施しなければ、WAN リンク上で満たすことはできません。利用可能なディスプレイ プロトコル ソフトウェア クライアントは（VMware または Citrix と同様に）、ネットワーク経由で送信される USB データを圧縮および最適化できます。ただし、すべてのオペレーティング システムで互換性のあるドライバがサポートされているわけではありません。HVD OS、ローカル クライアント OS、DV クライアント/エージェント ソフトウェア、およびエンド アプリケーションの間で徹底した互換性チェックを行うことを強く推奨します。WAN リンク経由の USB リダイレクトを使用する場合は、十分な帯域幅がプロビジョニングされ、最適化が使用されるようにします。USB データ フロー ダイアグラムの詳細については、「エンドポイントとアプリケーション」の章で説明しています。Citrix HDX Plug-n-Play を使用した USB リダイレクトの制御については、http://support.citrix.com/proddocs/topic/receiver-30-windows/ica-pnp-usb-redirect.html にあるドキュメントを参照してください。

印刷

印刷は、ユーザ エクスペリエンスの重要な 1 つの要因です。また、Windows ベースの HVD 環境のパフォーマンスと安定性にも大きな影響を及ぼします。Windows ベースの印刷では、印刷プロセスを開始するアプリケーションが、Enhanced Meta File（EMF）と呼ばれるプリンタ非依存のメタファイルを作成し、Windows スプーラに送信します。その後、スプーラは、特定のプリンタ ドライバに基づいて EMF をプリンタ固有の未加工ファイルに変換し、そのファイルを USB 接続またはネットワーク接続のプリンタに送信します。DV 環境では、プリンタはエンドポイントの近くにローカルに存在しますが、これらすべてのアクションは HVD 内で実行されます。たとえば、一般的な 2 MB の EMF ファイルは 10 MB の未加工ファイルに展開される可能性があります。ユーザあたりの印刷トラフィック量を考慮すれば、DV 環境内で印刷トラフィックを最適化することを強く推奨します。Citrix XenDesktop 5 は、Universal Print Driver による新しいキャッシングおよび圧縮機能を使用して、未加工の印刷トラフィックを削減します。WAN 上では、Cisco WAAS によって過剰な印刷トラフィックがさらに削減され、印刷に特化した最適化が実行され、高度な圧縮技術が実現されます。

ローカル ドライブ

ユーザによっては、仕事でローカル ドライブにアクセスしなければならない場合があります。ほとんどのコネクション ブローカとディスプレイ プロトコルは、エンドポイントのポイントから関連 HVD へのローカル ドライブ マッピングをサポートしています。また、その使用を制御するために、Active Directory グループ ポリシーも使用できます。ただし、DV 導入の主要な推進要因の 1 つがデータ セキュリティであることから、この制御はケースバイケースで実施することが推奨されます。WAN 環境に対するネットワークの課題は、他のローカル デバイス マッピングの場合と同じです。

ディスプレイ プロトコルとコネクション ブローカ

ディスプレイ プロトコルの主要な機能は、HVD とエンドポイントの間でディスプレイやユーザ入力データを双方向に転送することです。これらの基本機能に加え、ビデオ最適化、音声転送、USB/印刷データ転送などの機能もディスプレイ プロトコルで実行されます。クライアント ソフトウェア（エンドポイント上）が接続を開始し、エージェント ソフトウェア（HVD 内）がその接続を終端します。これらのソフトウェアが、OS ドライバとのインターフェイスを提供し、満足のいくユーザ エクスペリエンスを実現する役割を担います。

クライアントと HVD では、ディスプレイ プロトコルの選択が、両方の CPU 利用率とメモリ利用率に影響を及ぼします。ディスプレイ プロトコルは、一般に複数のチャネルで構成され、各チャネルはそれぞれ特定のタイプのデータ ストリームを伝送します。新しいディスプレイ プロトコル、クライアント、およびエージェントの多くに、コンピューティング リソース使用量とネットワーク帯域幅を最適化する高度なアルゴリズムが組み込まれています。

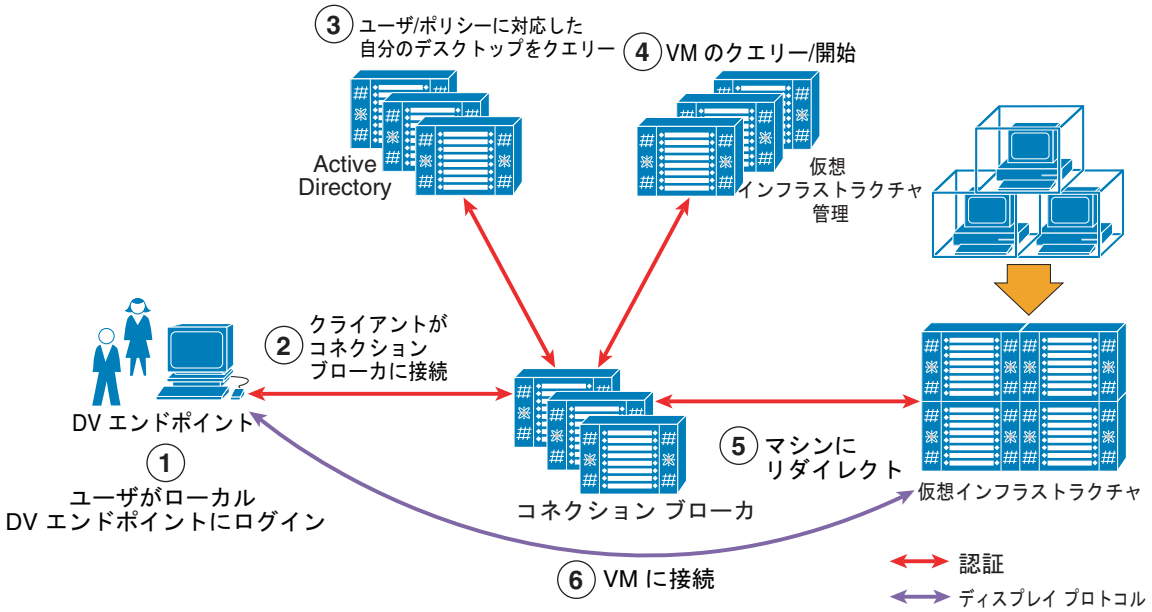
現在、市場に存在するディスプレイ プロトコルは、インタラクティブ マルチメディアの取り扱い方法の違いによって区別されます。マルチメディア リダイレクトをサポートするものから、高度でプログレッシブなディスプレイ レンダリング テクノロジーをサポートするものまであります。最も広く使用されているディスプレイ プロトコルは、Independent Computing Architecture（ICA）、PC over IP（PCoIP）、Remote Desktop Protocol（RDP）の 3 つです。ゼロ クライアントなど、エンドポイント タイプによっては、一部のディスプレイ プロトコルしかサポートされません。ディスプレイ プロトコルの選択は、ネットワークの設定方法、必要なコンピューティング能力量、ポリシーの適用、将来の互換性、そして最も重要なユーザ エクスペリエンスに大きく影響します。Citrix XenDesktop デスクトップ仮想化システムでは、クライアント接続に ICA または RDP を使用できます。Citrix XenApp は XenDesktop 5 に統合され、Microsoft Terminal Services に基づく Hosted Shared デスクトップ モデルの導入を可能にし、ディスプレイ プロトコルには ICA または RDP を使用します。XenDesktop、XenApp、およびサポートされる各種モデルの詳細については、この章で後述します。

すでに説明した多数の追加機能は、ディスプレイ プロトコルおよびコネクション ブローカの機能に依存します。図 2 に示されているようなエンドポイントから仮想デスクトップへの直接接続は、大規模な導入に対応できるだけの拡張性がありません。仮想デスクトップに対する複数のクライアント接続要求を認証し、リダイレクトするには、主要な DV コンポーネントとしてコネクション ブローカが必要です。一般にコネクション ブローカは、新しい仮想デスクトップをオンデマンドでプロビジョニングし、ユーザ資格情報をホステッド仮想デスクトップにリレーすることも行います。

高度なブローカ機能では、1 ユーザに複数のデスクトップ配備、トンネリングおよびプロキシ モードのディスプレイ プロトコル、ロード バランシング機能を備えた大規模クラスタの作成サポート、SSL 接続の終端などを使用できます。ブローカは、通常、既存の Active Directory インフラストラクチャと通信して、ユーザを認証したり、ユーザ固有のデスクトップ ポリシーを取得し、適用したりします。またコネクション ブローカは、ドロップや切断に備えて接続の状態を維持し、必要に応じてリモート デスクトップの電源オフまたは削除を行います。

図 3 に、単一エンドポイントとコネクション ブローカを使用した、簡略化された DV 環境での接続フローを示します。この基本的な接続フローは、あらゆるベンダーのすべての DV の導入に使用されます。一部のベンダーは、自社のコネクション ブローカでさまざまな機能のトンネリング モードをサポートしています。トンネリング設定は、この設計ガイドでは検証されていないため、通常はほとんどのシナリオで使用しないことを推奨します。トンネリングでは、ユーザ エンドポイントと HVD の間のディスプレイ プロトコル セッションを終端および再開始する必要があり、コネクション ブローカ上で単一の接続をサポートするために必要なコンピューティングとメモリが増加します。導入シナリオによっては、たとえば、インターネット経由で HVD にアクセスするユーザ用に Remote Desktop Protocol（RDP）over HTTPS が必要な場合、専用のトンネリングされた接続が必要になる可能性があり、設計の要因として考慮する必要があります。

図 3　　DV 接続フロー



上の図 3 に示されている DV 接続フローの手順は次のとおりです。

1. ユーザがエンドポイントにログインし、クライアント ソフトウェアにアクセスします。
2. クライアント ソフトウェアは、ブローカへの接続を開始します。
3. ブローカは、Active Directory 内でユーザを検索し、関連付けられているリモート デスクトップを決定します。

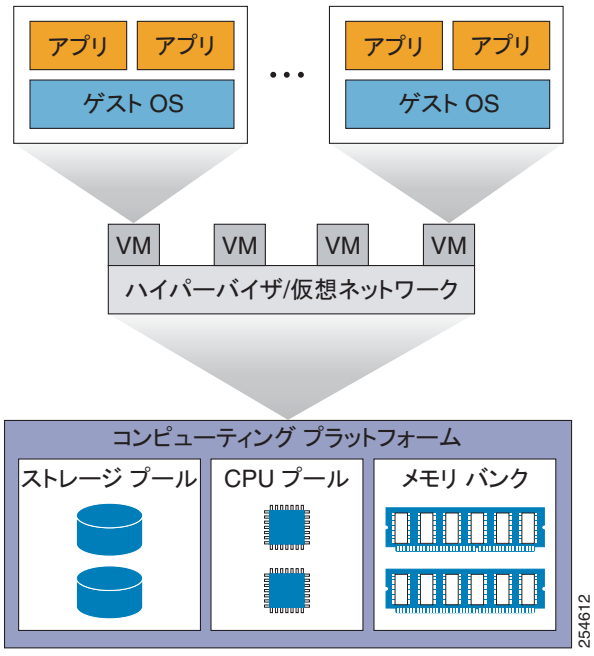
4. 必要に応じて、ブローカは、仮想インフラストラクチャ マネージャと通信して、ユーザのリモート デスクトップを作成または起動します。
5. 次に、ユーザは、該当するリモート デスクトップにリダイレクトされます。
6. それ以降、エンドポイントは、ディスプレイ プロトコルによってリモート デスクトップへ直接接続されます。

DV 用ハイパーバイザ

仮想マシンは隔離されており、ゲスト オペレーティング システムが動作する仮想ハードウェア コンテナ内で抽象化されています。この隔離設計によって、複数の仮想マシンは安全に動作し、ハードウェアにアクセスして中断のないパフォーマンスを提供することができます。こうした隔離を実行するソフトウェア レイヤをハイパーバイザと呼びます。図 4 に、HVD におけるハイパーバイザの役割を示します。

適切に設定されたハイパーバイザは、ハードウェアの抽象化のほか、すべての VM に CPU、メモリ、および I/O リソースを公平に割り当てます。ハイパーバイザが VM の内部で動作するゲスト オペレーティング システムに対して行う制御は、最小限であるか、直接的な制御は行われません。ただし、メモリ使用率を制御したり、CPU サイクルを共有したりすることで、OS の動作を間接的に制御します。Windows 7 などの仮想デスクトップは、仮想マシン内で動作します。仮想マシン自体は、ハイパーバイザによって制御されるホスト サーバ上で動作します。この Cisco Validated Design の導入には、VMware ESX/ESXi と Citrix XenServer ハイパーバイザが使用されました。ハイパーバイザ設計とインストールの重要な考慮事項について、いくつかの注意点が「データセンター」および「パフォーマンスとキャパシティ」に記載されています。インストール手順とその他の詳細については、該当する VMware および Citrix インストール ガイドを参照してください。

図 4　　HVD のコンポーネント



vCenter を搭載した VMware ESX/ESXi と XenCenter を搭載した Citrix XenServer は、データセンターで最適な仮想デスクトップ密度を実現できるツールを豊富に備えています。

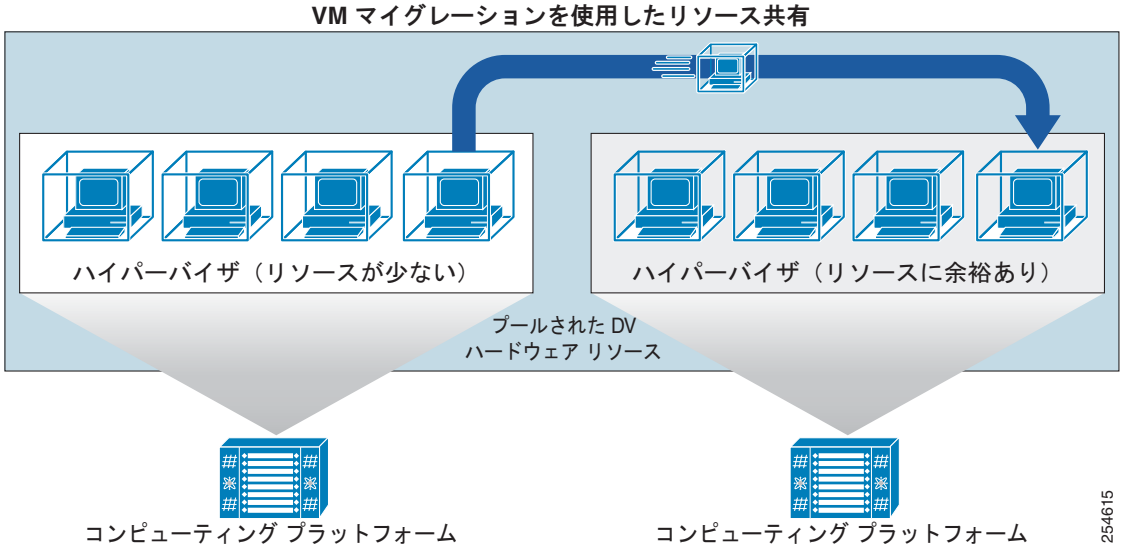
すべての仮想マシンは、単一ホスト（サーバ）上またはホスト（サーバ）プール内に存在する共通のハードウェア リソースを共有します。単一サーバ上で高密度に配置された仮想デスクトップが動作する一般的な DV の導入では、その環境内で VMware Distributed Resource Scheduler（DRS）や Citrix Workload Balancing などのリソース共有機能を適宜使用することを強く推奨します。

リソースの共有には、単一ホストへの公平な、または設定済みハードウェア リソースの配布、オーバーコミットされたホスト マシンの識別、プール内のホスト間における VM のライブ移動、プライオリティに基づいた VM 電源投入シーケンスなどが含まれます。一般的な DV シナリオの場合、通常は、プロビジョニングされたデスクトップのすべての電源が同時に投入されることはありません。これは、データセンター内の仮想化サーバの使用パターンである常時運用モードとは根本的に異なっています。さらに、企業環境内の仮想デスクトップは、勤務時間後および休日には通常使用されません。ハイパーバイザのリソース共有機能を電源管理機能と組み合わせて使用すると、特に DV の導入では、データセンターの電力使用量が削減されます。ハイパーバイザの電源管理ツールでは、すべてのアクティブな仮想デスクトップを必要最小限のホスト（サーバ）上に統合したり、アイドル状態のホストの電源をオフにしたり、設定されているプライオリティに基づいてホストの電源をオンにしたりできます。

リソース共有機能と電源管理機能は、いずれも VM マイグレーション機能（できればライブ マイグレーション）と共有 VM ストレージを必要とします。ライブ マイグレーション（稼動しながらの移行）では、物理マシン上で動作中の仮想マシンをダウンタイムなし、サービスの中断なし、トランザクションの欠落なしで別の物理サーバに移動できます。事前定義の電力使用量ポリシーとリソース使用量ポリシーに基づいてデスクトップをデータセンター内で移行できるので非常に便利です。

図 5 に、VM マイグレーションによるリソース共有の概念を示します。VMware ESX では vMotion、Citrix XenServer では XenMotion を使用してライブ マイグレーションが実行されます。このテクノロジーは継続的に強化されているため、いずれのベンダーでも制限事項、前提条件、およびベスト プラクティスが規定されています。一部の重要なベスト プラクティスについてはこのガイドで説明していますが、すべてのベスト プラクティスを記載することはこのガイドの目的の範囲外です。

図 5　　VM マイグレーションを使用したリソース共有



ESX/ESXi および XenServer は、各 HVD の接続先となるソフトウェア仮想スイッチを実装します。仮想スイッチは、仮想 Network Interface Card（NIC; ネットワーク インターフェイス カード）を HVD に提供し、ホスト マシン上の物理 NIC に接続します。HVD からのすべてのデータは、仮想スイッチにより、適切な VLAN タグを付け、QoS ポリシーを適用されて（可能な場合）、転送されます。

ESX/ESXi および XenServer によって提供される仮想スイッチは、基本的なスイッチング機能を実装します。多くのシナリオにおいて、これらの基本機能では実際の導入に十分対応できません。XenServer では、複数のネットワーク、VLAN、ロード バランシング機能を備えた物理 NIC ボンディング、および専用ストレージ NIC を作成できます。ESX/ESXi vSwitch は上記のすべての機能のほか、vCenter 管理サービスによる Distributed Virtual Switch（DVS; 分散仮想スイッチ）機能も提供します。DVS では、複数のホストに分散した複数の VM を、1 台の共有の仮想スイッチに接続できます。この機能により、DV 環境内に大量の HVD が存在する場合でも、ネットワーク設定をきわめて簡単に管理できます。XenServer は、外部のスイッチ プラットフォームに依存して分散スイッチと同等の機能を提供します。分散スイッチは、ホスト間の VM の移動を可能にします。これは、前述のリソース スケジューリング、電源管理、VM マイグレーション、HA などの高度な機能の基本要件となります。ESX/ESXi および XenServer を使用した分散仮想スイッチングでは、基本的なスイッチングは行われますが、広範囲で高度な機能は提供されません。たとえば VMware の DVS 機能には、高度な QoS、スタックド VLAN、802.1x、ポート セキュリティなど、アクセス スイッチが備えておくべき高度なネットワーキング機能はありません。Cisco Nexus の 1000V シリーズ スイッチには、これらをすべて含むさまざまな機能が用意されています。

フィーチャ セット以外にも、仮想スイッチにはホスト マシン自体の CPU サイクルを消費するという根本的な制限があります。大量の VM 間通信が発生すると、ホスト CPU の使用量が増大します。高密度の DV 導入では、キャパシティ プランニング時にこのようなリソース使用量を考慮する必要があります。さらに、ハイパーバイザにパッケージされている仮想スイッチを使用した場合、単一ホスト上のすべての VM 間通信に対する可視性が失われます。DoS 攻撃（設定の誤りによるブロードキャスト ストームも含む）など、特定の種類のセキュリティ違反は、DV 環境に深刻な影響を与える可能性があり、フローに対する可視性がないと、トラブルシューティングが困難になります。

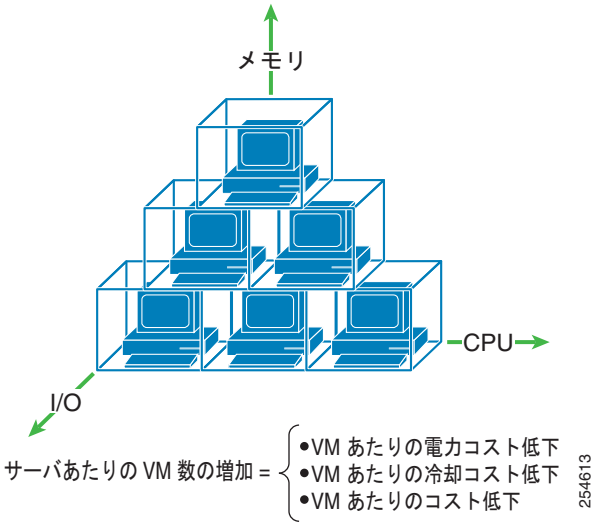
（注） 現在、Cisco Nexus 1000V シリーズは VMware ESX/ESXi ハイパーバイザでのみサポートされています。Cisco Nexus 1000V シリーズ導入の詳細については、「導入モデル」を参照してください。

仮想デスクトップのホスティング

DV が既存のデータセンターに導入されるか、新規に導入されるかに関係なく、いくつかの重要な設計基準について検討する必要があります。企業の DV 環境には、スケーラブルでセキュアな常時接続のコンピューティング、ストレージ、およびネットワーク インフラストラクチャが必要です。具体的なガイドラインは選択した DV ベンダーによって異なりますが、次の DV 導入に関する一般的な判断基準について検討する必要があります。

図 6 に示されているように、コンピューティング リソース、メモリ、および I/O が、データセンター内の DV を決定するための判断軸となります。たとえば、ある 1 つのリソースが他のリソース（たとえば CPU）よりも前に枯渇すると、プロビジョン済みのリソース、メモリ、I/O が無駄に消費されます。またその際、キャパシティ プランニングが適切に実施されていないと、ユーザ エクスペリエンスの維持とリソースの浪費回避を両立しながら、HVD の密度を最大限に高めるという目的を達成することは困難になります。以降のセクションでは、DV 環境におけるこれらのリソースの消費について、根本的に異なる点をいくつか紹介します。

図 6　　DV パフォーマンスの要因



コンピューティング

サーバはローカル デスクトップの何倍もの CPU 能力を備えています。つまり、単一のマルチコア CPU で複数の HDV を処理することができます。デスクトップ内で使用されるアプリケーションはユーザによって異なるので、各 HVD に対して必要なメモリ量を評価することは困難な場合があります。DV の導入では、仮想化サーバの導入と比べ、メモリがより中心的な役割を果たします。最も一般的な作業負荷の場合、最高の HVD 密度は、大量のメモリ バンクを提供できるコンピューティング プラットフォームを選択することで実現できます。コンピューティング要件の詳細については、「導入モデル」の章を参照してください。

ネットワーク

ディスプレイ トラフィックの場合、使用されるプロトコル、モニタの解像度と設定、作業負荷に含まれるマルチメディア コンテンツの量といった、多くの要素がネットワーク帯域幅に影響を与える可能性があります。ストリーミング型アプリケーションの同時起動もネットワーク負荷の急上昇を招きます。WAN の場合、帯域幅の制約、遅延に関する問題、およびパケット損失について検討する必要があります。DV 環境では、単一のコンピューティングおよびネットワークのインフラストラクチャでサポートされる仮想デスクトップの密度は、従来のキャンパスまたはブランチ インフラストラクチャよりもはるかに高いです。エンドポイントの集約により、ネットワークとコンピューティングの負荷が、特に使用量のピーク期間中に増加します。

DV 環境内に存在する主要なデータ フローは次のとおりです。

1. データセンター内の HVD とエンドポイントとの間のディスプレイ プロトコル トラフィック。
2. データセンター内の HVD とインターネットとの間のトラフィック。このトラフィックは、一般にエンタープライズ キャンパス ネットワーク経由でルーティングされます。
3. HVD とストレージ アレイの間のストレージ データ トラフィック（I/O Per Second（IOPS; 1 秒あたりの I/O 処理数））。このトラフィックは、通常はデータセンター内に留まります。
4. アプリケーション データ トラフィック。このトラフィックは一般にデータセンター内に留まります。

4 を除き、上記はすべて DV によって発生する新しいトラフィック フローです。大規模な導入の場合、各データ フローが、データセンター ネットワークの入口ポイントと出口ポイントで混雑する可能性があります。ディスプレイ プロトコル データなど取り扱いに注意を要するデータ フローの遅延やドロップを防止するために、適切な QoS メカニズムが必要です。

さらに、ユーザの使用パターンは予測不可能であり、仮想デスクトップごとに消費される帯域幅に悪影響を与える可能性があります。たとえば高品質の全画面ビデオは、特定の HVD 多層データセンターの帯域幅使用量が急増する原因となります。通常は十分なネットワーク キャパシティが確保されているとしても、ユーザ エクスペリエンスを維持し、将来の拡張と DV 分野における技術進歩への対応を可能にするには、エンドツーエンド ネットワーク全体を入念に設計する必要があります。従来の企業のデスクトップ展開では、ユーザ デスクトップに対してアクセス ネットワークへの接続ポイントが 1 つ存在します。このアクセス レイヤにより、ネットワークの機能と実際のコンピューティング リソースが明確に分離され、ネットワークとユーザ作業環境に対するポリシーの適用が対立しないようになっています。DV 環境では、エンドポイントは同様にキャンパス アクセス レイヤに接続しますが、それに加えてデータセンター サーバ内の HVD がサーバ内の仮想スイッチ ポートでネットワークに接続するようになります。単一ユーザ用の新しい接続ポイントの追加と仮想スイッチの位置によって、ポリシー適用の境界があいまいになり、新たなセキュリティの問題が生じます。こうした問題には、制御されたアクセス スイッチに HVD の接続ポイントを移動するか、機能の豊富な仮想スイッチを使用して制御をサーバ内部に移すことで対処できます。エンドツーエンド Cisco VXI ネットワーク要件については、「データセンター」と「VXI ネットワーク」の章で説明しています。

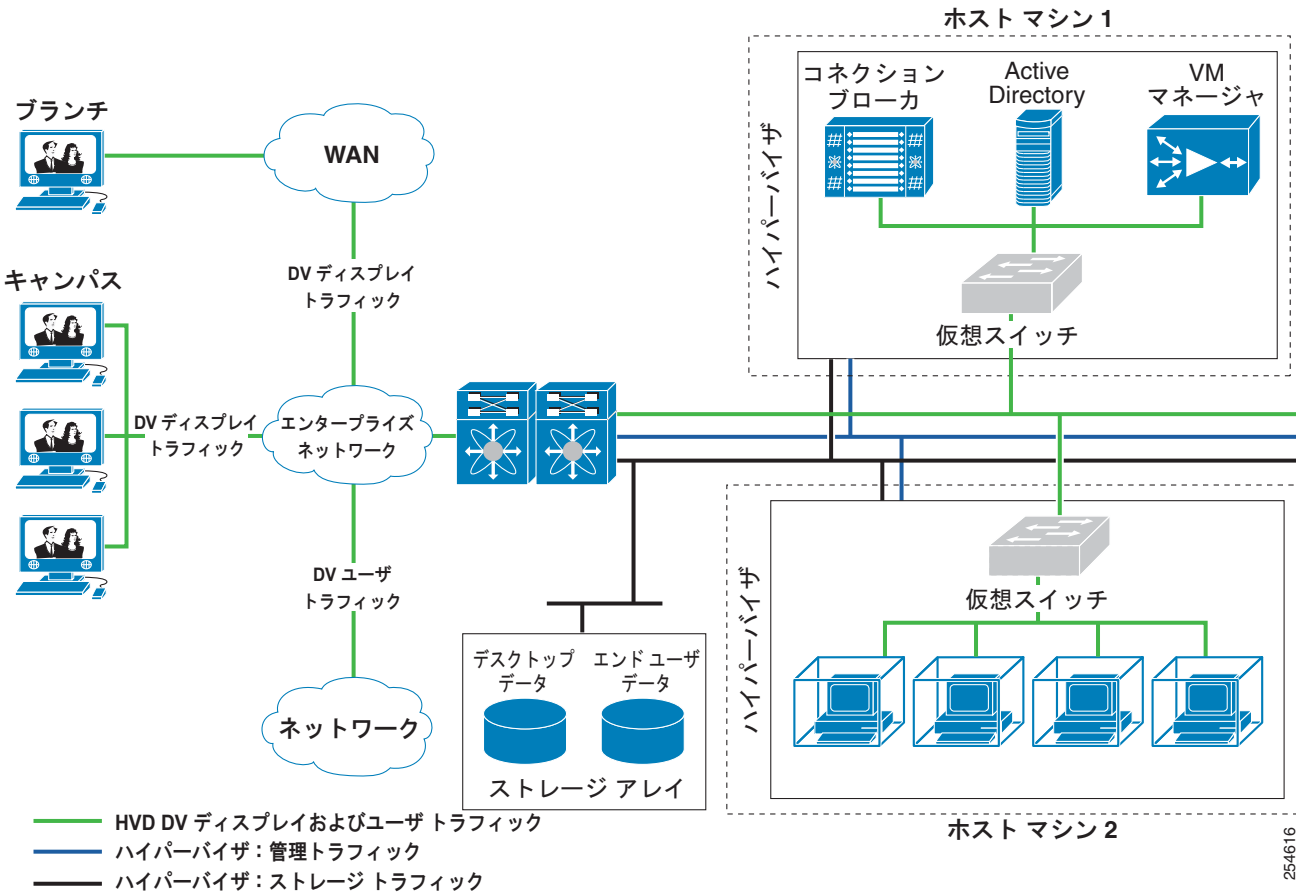
ストレージ

DV エンドポイントにはローカル ストレージがない場合があるため、関連する HVD は集中管理されたストレージ システム上に配置されます。通常、各 HVD のストレージは、デスクトップ ストアとユーザ プロファイル ストアに分割されます。デスクトップとユーザ プロファイルにストレージを分割することで、ユーザ プロファイルを残したままデスクトップを削除できるようになります。その結果、永続的デスクトップ、非永続的デスクトップ、およびデータ バックアップ（ユーザ データのバックアップのみ）がサポートされ、ストレージの要件（デスクトップの冗長性が高く、クローニングの使用が可能）が軽減されます。非永続的デスクトップを使用すると、HVD イメージに必要なストレージ キャパシティは減少しますが、必要とされる IO スループットは変わりません。したがって、高い IO スループットの達成に必要なストレージ ディスクとコントローラの数という点では、節約の程度は低くなります。解決策として、インテリジェント キャッシング ソリューションを導入することで、ハイパーバイザで生成される余分な IO を削減し、ストレージの効率性を高めるソリューションを強くお勧めします。これらのソリューションについては、このドキュメントの「データセンター」で詳しく説明しています。一定の期間に対して DV 環境内で発生する平均的なストレージ I/O 量を予測することは可能ですが、短い時間に対して予測することはほぼ不可能です。これは、サーバ環境の場合とはまったく異なります。しかし、IOPS は、OS のタイプ、OS のバージョン、および作業負荷アプリケーションの種類に強く依存します。DV 環境内では、データの重複率が非常に高くなっています（共通の OS コード ベース、同種のアプリケーションのインストールなど）。したがって、データ重複排除テクノロジーと VM クローニングは、DV ストレージにとって非常に有益です。各デスクトップのストレージ要件は、適切な制御ポリシーを適用しなければ、拡大し続ける可能性があります。HVD がクローニングされる場合、HVD を定期的に再起動し（蓄積された一時データを削除するため）、ユーザに対してディスク クォータを使用するか、直接ディスク アクセスの代わりに制御されたネットワーク ストレージを割り当てることを強く推奨します。一般的に、DV の導入はストレージ テクノロジーには依存していません。したがって、Storage Area Network（SAN; ストレージ エリア ネットワーク）または Network Attached Storage（NAS; ネットワーク アタッチド ストレージ）を組織の選択に従って使用することができます。

一般的な DV 導入

図 7 に、一般的な DV 導入をすべての主要コンポーネントおよび接続パスとともに示します。データセンターには、少なくとも HVD プール、コネクション ブローカ、Active Directory、および仮想マネージャ サーバが DV 用に収容されています。プール内の HVD はそれぞれ 1 つの VM であり、プール自体は物理的に独立した 1 台のホスト マシンです。もう 1 つのホストに、コネクション ブローカ、Active Directory、VM マネージャがインストールされた VM が収容されます。HVD プールとエンタープライズ サービスは、物理的に異なるホスト マシン上に配置することを強くお勧めします。各ホスト内のハイパーバイザは、黒色と青色に分けて示されている独立したストレージ ネットワークと管理ネットワークに接続します。キャンパスやブランチ内のエンドポイントは既存のアクセス ネットワーク インフラストラクチャに接続し、プール内の HVD はハイパーバイザ内にインストールされた仮想スイッチに接続することに注意してください。すべてのエンドポイント、HVD、および DV サーバ コンポーネントは、「緑色」のネットワーク上に存在します。緑色のネットワーク内のデバイスは、レイヤ 2 またはレイヤ 3 接続を使用して相互に到達できます。すべてのディスプレイ プロトコル トラフィックは、エンドポイントと HVD の間で生成と終端が行われます。

図 7　　DV の接続パス



（注） 図 7 に、基本的な DV 接続を示します。個々のシナリオと機能によって配置が異なる場合もあります。

（注） 図 7 は、ネットワークの観点から見て重要な Cisco VXI コンポーネントを示しており、ユーザ エクスペリエンス向上のために必要な Cisco VXI コンポーネントがすべて含まれているわけではありません。

導入の詳細については、このガイドの「導入モデル」を参照してください。

作業負荷、ピーク作業負荷、およびそれらが設計に与える影響

作業負荷

定義されている各ユーザ プロファイルに対し、既存の物理デスクトップでのエクスペリエンスに基づいて、あるいはテストを実施して、きめ細かな作業負荷パラメータを設定する必要があります。作業負荷パラメータは、ユーザ プロファイルと同様に、企業ごとに大きく異なります。これらのパラメータを早期に決定することが、DV 導入の成功と失敗の分かれ目となります。作業負荷パラメータには、アプリケーションの実行時間、アプリケーションの使用パターン、画面の平均更新レート、OS とアプリケーションのメモリ、および CPU とストレージのフットプリントを含める必要があります。作業負荷の定義には、推定平均使用率とともに、HVD 内で CPU 負荷、メモリ負荷、またはネットワーク負荷を発生させるイベント（文書の保存、電子メールの送信、ビデオの視聴、テキストの編集など）の一覧が含まれていなければなりません。各タイプの作業負荷には、IOPS の測定値で表されるさまざまなストレージ スループットの要件があるため、特に大規模な DV の導入を計画する場合は、これらの要件をきわめて正確に特定するよう注意する必要があります。このデータの大部分は試験的な DV 導入の段階で生成され、その後にフルスケールの導入用のリソース要件を推定するために使用されます。試験的導入時にネットワーク負荷、IOP 負荷、CPU 負荷、およびメモリ負荷の概算で生じたわずかな誤差が、最終的な導入時には大幅に増加していることもあります。

ピーク作業負荷

HVD はハイパーバイザによって抽象化された共有コンピューティング リソース上で稼動するため、適切なハイパーバイザ メカニズムと計画が導入時に使用されていなければ、1 つの HVD のリソース使用率が他の HVD のリソース使用率に影響を与える可能性があります。すべてのユーザは、データセンター内に集中配置されたそれぞれの HVD にアクセスするので、データセンター内への共通のセキュアなネットワーク エントリ ポイントを共有します。適切に設計されていないと、この共通のネットワーク エントリ ポイントが潜在的なボトルネックとなり、ユーザ エクスペリエンスの低下や、接続の完全な喪失さえももたらす可能性があります。ピーク作業負荷はストレージのボトルネックにもなり、デスクトップのパフォーマンスを低下させることがあります。DV 導入の計画時には、発生しうるピーク作業負荷シナリオを特定してネットワークおよびストレージ システムの規模を決定し、ピーク作業負荷に対処することが重要です。

例として、朝の数分の間に何百ものユーザがそれぞれの HVD を起動し、Microsoft Outlook を立ち上げ、それぞれの業務アプリケーションを実行する企業について考えてみます。この一連のイベントにより、DV 環境内のすべてのコンポーネントに厳しい負荷が発生する可能性があり、場合によってはネットワークを共有している非 DV アプリケーションにも影響を及ぼします。すべてのユーザ トラフィックがディスプレイ プロトコルにカプセル化されるので、同期されたユーザ アクション（何百ものユーザによるライブ社内ビデオの同時視聴など）は、ネットワークを輻輳させる可能性があります。ミッションクリティカルなアプリケーションがこれらのユーザのグループによって同時に使用されるとしても、ビデオとクリティカルなアプリケーションのトラフィックを別々に処理する QoS メカニズムはディスプレイ プロトコル内に組み込まれていません。ピーク作業負荷の他の例には、一斉に実行されるアンチウイルス チェック、アプリケーションと OS のアップデート、HVD 再起動があります。

適切なキャパシティ プランニング、十分な予備リソース、リソース スケジューリングの有効利用、耐障害性機能と High-Availability（HA; ハイ アベイラビリティ）機能、およびネットワーク キャパシティと QoS の計画は、DV 環境内のピーク作業負荷に対処するために必要不可欠です。さらに、最適な WAN/インターネット帯域利用率を慎重に検討し、計画する必要があります。

平均作業負荷、ピーク作業負荷、およびユーザ プロファイルを明確に理解することで、特定の DV 環境に必要なリソースと設定を適切に評価できます。サンプルの作業負荷を使用したリソース評価の詳細については、第 9 章のキャパシティおよびパフォーマンスに関する説明を参照してください。

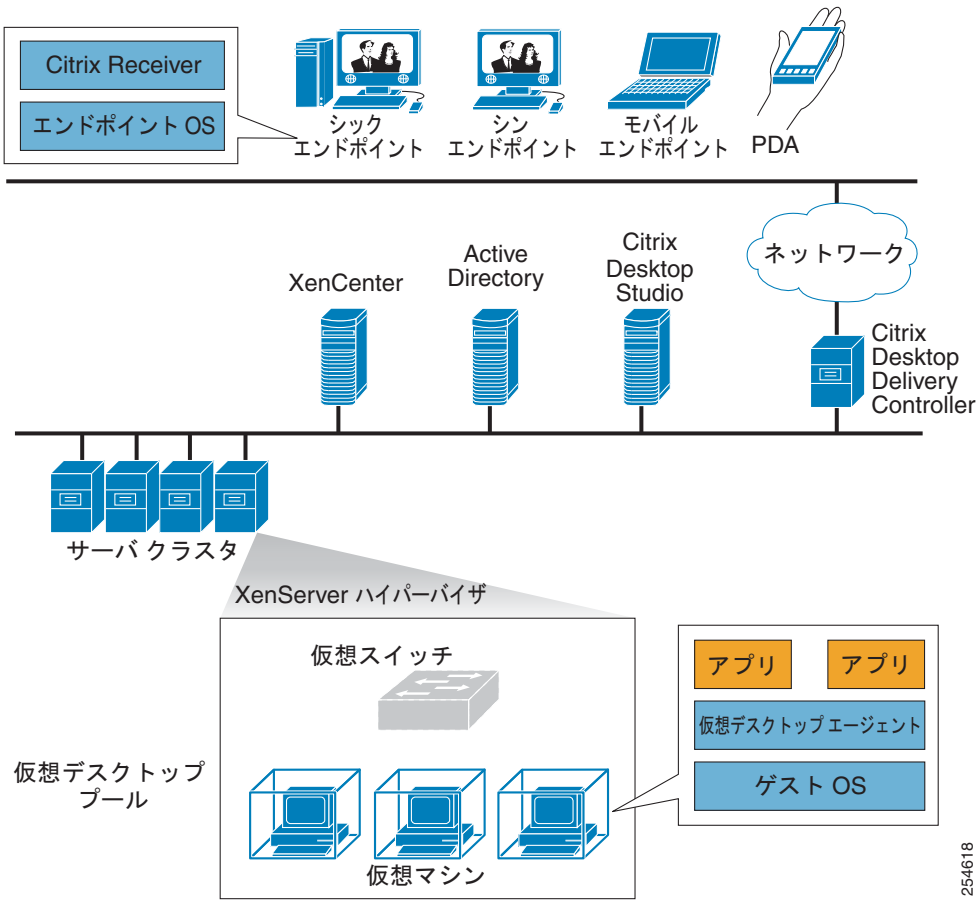
Citrix DV

ホステッド仮想デスクトップ

Citrix XenDesktop 5（XD5）環境のホステッド仮想デスクトップは、専用、プール、ストリーム、共有など複数のモードで導入することができます。これらのモードは、エンド ユーザのアクセス方法と仮想デスクトップとの関連性に基づいて区別されます。あるいは、複数のユーザ ログオンでの仮想デスクトップの状態、つまり、2 つのモードが 1 対 1 の関係にある永続的デスクトップであるか、非永続的デスクトップであるかに基づいて HVD を区別する方法もあります。永続的デスクトップは特定のユーザに関連付けられ、通常はカスタマイズされ、そのデスクトップの使用期間を通してユーザ データを保存します。非永続的デスクトップ プールでは、ユーザ間で共有するデスクトップ プールをオーバーサブスクライブすることで、拡張性を高めることができます。これらのデスクトップはログオン時にユーザに割り当てられ、個々のデータ ストア内にカスタマイズおよびユーザ データがある場合はそれらが適用され、プール内で他のユーザに解放されます。非永続的デスクトップは、さまざまなエンタープライズ アプリケーションにアクセスするための一時的なコンピューティング プラットフォームを必要とし、通常はローカルでユーザ データを保存しないタスク ワーカーに最適です。ホステッド仮想デスクトップの主なコンポーネントとその導入については後述します。

下の図 8 は、Citrix XenDesktop 5 を使用した一般的な DV 導入を示しています。Citrix 固有のコンポーネントについては、
http://support.citrix.com/proddocs/topic/xendesktop/cds-library-wrapper-rho.html の Citrix ナレッジベースを参照してください。

図 8　　Citrix XenDesktop DV 導入



仮想デスクトップ エージェント

Citrix Virtual Desktop Agent（VDA）は、各 HVD 上で動作するエージェントです。このエージェントによって、エンドポイントで動作するクライアントがデスクトップを使用できるようになります。VDA は、ポート 1494 で ICA 接続要求を受信し、デスクトップを作成し、それをクライアントへストリーミングします。VDA は、Desktop Delivery Controller（DDC）への HVD の登録も行います。バックグラウンドでは、VDA は DDC と通信してセッション ステータスを更新し、使用率の統計と現在のデスクトップの状態に関する情報を提供します。VDA はポート 8080 を使用して DDC と通信します。

Citrix Online Plug-In

VDA と連携して動作する複数のクライアント ソフトウェア オプションが Citrix から提供されています。エンドポイント ハードウェアに応じて、Citrix Receiver、Online Plug-In、または SelfService プラグインを使用できます。Citrix Online Plug-In には、ユーザがローカル デスクトップ内で仮想デスクトップを移動および拡大/縮小できるツールバー機能があります。同一デバイス上で複数の Citrix Online Plug-In セッションを使用すると、ユーザは複数のデスクトップを操作できます。その他の機能の詳細については、Citrix の製品マニュアルを参照してください。

XenDesktop 5 サーバ

XD5 は Citrix XenDesktop 5 環境の中核であり、特に重要な機能として、ユーザ認証や VM の電源管理などを行うコネクション ブローカ サービスを備えています。セッションの確立時、XD5 は ICA ポリシーを決定し、必要に応じてライセンスを適用します。クライアントと VDA 間の接続が確立されると、XD5 は VDA の支援を受けてアウトオブバンド モニタリングを実行します。XD5 を拡張すると、インストールされた単一のインスタンスで数千台のデスクトップを処理できるようになります。

さらに XD5 は、監査および DV 導入の調整に役立つデータ収集機能も実行します。XD5 サイトを作成し、そのサイトで各コントローラにデータ収集やインフラストラクチャ制御などの専門的機能を割り当てることができます。高い可用性を得るには、環境内にブローカ サービスを実行する複数の XD5 ホスト サーバを用意し、できれば Cisco ACE Application Control Engine モジュールなどのロード バランサの背後に配置することをお勧めします。XD5 のすべてのサイト メンバーは、同じ Active Directory ドメインに属していなければなりません。現在の XD5 には、仮想デスクトップをすみやかに作成およびプロビジョニングできる VM 管理サーバも組み込まれています。永続的デスクトップを必要としない DV 環境では、プロビジョニング サービスによってストレージ使用率を効率的に最適化できます。デスクトップ プロビジョニングは、単一のデスクトップ イメージからオンデマンドで仮想デスクトップを作成およびプロビジョニングして、ストレージの使用率を最適化し、ユーザがログインするたびに新しい仮想デスクトップを各ユーザに提供するコンポーネントです。デスクトップ プロビジョニングによりデスクトップ イメージも簡素化され、最高レベルの柔軟性を実現し、アプリケーションとデスクトップの両方でデスクトップの管理ポイントを削減できます。

Cisco VXI では VMware ESXi 4.1 ハイパーバイザ、Microsoft Hyper-V ハイパーバイザ、および Citrix XenServer ハイパーバイザ上で XD5 を検証しました。Citrix XD5 には、現在の市場における大手ハイパーバイザ ベンダーとの統合サポートが組み込まれています。VMware の場合、このサポートは XD5 と vCenter 間の通信を可能にする一連の API を基盤にしています。XD5 と vCenter 間の通信は HTTPS を経由するので、vCenter 証明書を XD5 にインポートする必要があります。さらに、統合を円滑に行うために、vCenter フォルダ名またはデータストア名には特殊文字を使用せず、vCenter 証明書には XD5 ホスト サーバで解決可能なドメイン名を記載します。XD5 では、仮想デスクトップを作成するためのゴールデン イメージが、分散仮想スイッチではなく ESXi 4.1 vSwitch 上に配置されている必要があります。すべての仮想デスクトップが作成され、ユーザ / ユーザ プールに初めて割り当てられたら、Power Shell を使用してそれらの仮想デスクトップを任意の分散仮想ネットワークに移動できます。上記のベスト プラクティスの手順説明については、
http://support.citrix.com/proddocs/index.jsp?topic=/xendesktop-rho/cds-vmware-rho.html と
http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/Virtualization/ucs_xd_vsphere_ntap.pdf も参照してください。

Hosted Shared デスクトップ

Hosted Shared Desktop（HSD; Hosted Shared デスクトップ）を使用すると、基盤となる同一のゲスト オペレーティング システムを複数のユーザで共有できます。これにより、最も拡張性の高い方法でユーザにデスクトップ サービスを提供できます。共有は Microsoft Terminal Services を基盤としているので、ユーザは互いに完全に孤立しているわけではありません。Hosted Shared デスクトップの最大の利点はその規模にありますが、このモデルは企業内の全ユーザに適用されるわけではありません。一般的に、大企業では HVD と HSD を組み合わせる必要があります。HSD は Citrix XenApp6 によって公開されます。必要なデスクトップを実行するサーバのファームは、各サーバ上で動作する XenApp 6 を使用して作成されます。管理を容易にするために、これらのデスクトップを仮想化することが推奨されます。ファームが作成され、必要なアプリケーションがすべてインストールされたら、XenApp 6 ファームを既存の XenDesktop 5 Web インターフェイス上で、あるいは新しい Web インターフェイスを介して公開できます。XenApp6 によって公開された仮想デスクトップは、任意のハイパーバイザ上で作成できます。Cisco VXI では、VMware ESXi および Microsoft Hyper-V を使用してアーキテクチャを検証しました。XenApp6 の各種導入モードの導入と設定、および XenDesktop 5 との統合チェックリストの詳細については、Citrix ナレッジ ベースを参照してください。

Hosted Shared デスクトップは、あらゆるユーザに最適というわけではないことに注意してください。Citrix では、ユーザ セグメンテーションを分析し、ユーザの業務に必要なアプリケーション、アプリケーションの作業負荷、およびユーザ パターンに基づいてユーザ ベースを分類することを推奨しています。Hosted Shared デスクトップは基盤となるコンピューティング環境を共有するので、1 人のユーザによってリソースが大量に消費されると、それ以外の全ユーザのリソースの可用性に影響を与えます。一般的に、MS Office やブラウザなど 1 ～ 2 種類のアプリケーションを使用するユーザには、Hosted Shared デスクトップ モードが非常に適しています。HSD で使用される共有 OS モデルに対し、すべてのアプリケーションが互換性を備えているわけではないことにも注意してください。そのようなアプリケーションには、HVD の方が適しています。

（注） 現時点で、Cisco Unified Personal Communicator は Hosted Shared デスクトップ モードではサポートされていません。一般的に、個人のリッチ メディアやコラボレーション アプリケーションは、Hosted Shared デスクトップには向いていません。

企業の DV ポリシーとユーザ プロファイル

ユーザ プロファイルの定義は、DV の導入を計画する際に最初に行う最も重要な手順の 1 つです。ユーザ プロファイルの定義は、企業全体の IT ポリシーと DV 導入の背景にあるビジネス推進要因に従って進められます。現在の企業にデスクトップ仮想化を決心させる要因は、主としてデータ セキュリティ、IT 環境の柔軟性、および総所有コストにあります。DV の導入を定める重要なポリシーの決定事項を次に一覧します。この一覧は包括的なものではありません。個別のビジネス ニーズによってさらに細かいポリシーを必要とする場合があります。

- DV に移行されるユーザ プロファイルとユーザの合計数の決定：

  ユーザ プロファイルは一般に、タスク ワーカー、ナレッジ ワーカー、およびパワー ユーザに分類されます。タスク ワーカーは特定の機能を実行し、最小限の要件で自分のデスクトップ環境を変更できます（ファイルのローカル保存、デスクトップのパーソナライズなど）。タスク ワーカーは、通常、永続的なデスクトップ（デスクトップ共有の実現）は必要なく、大規模な DV に対して最適なプロファイルです。ナレッジ ワーカーは、コンテンツを作成したリッチ メディアを使用したりするユーザで、場合によっては自分のデスクトップにアプリケーションをインストールする必要もあります（製品マネージャ、管理職、ソフトウェア プログラマなど）。通常、ナレッジ ワーカーには、ログオン中のユーザの仮想デスクトップ状態を維持できる永続的な専用デスクトップが必要です。パワー ユーザは、日々の作業で非常に高いコンピューティング能力を利用する従業員です。パワー ユーザは大量のデータを操作します。たとえば、グラフィック デザイナー、CAD デザイナー、設計者などがこれに該当します。DV の導入を成功に導くには、企業のポリシーとビジネス ニーズに基づいてユーザ プロファイルを明確に定義することが不可欠です。

- ビジネスに不可欠なアプリケーションの特定：

  アプリケーション要件は、DV 環境内のストレージ要件、コンピューティング要件、およびネットワーク要件を決定する重要な要因です。また、環境内に導入する具体的な仮想化ベンダーと仮想化ソフトウェアを決定する役にも立ちます。ビジネス要件に応じて、アプリケーションには SAP ビジネス ソフトウェア、Customer Relationship Management（CRM; 顧客関係管理）アプリケーション、Software as a Service（SaaS）、Web ブラウザ、Microsoft Office、Microsoft Outlook などが含まれます。一般に、DV 環境内に導入されたアプリケーションには、既存の IT デスクトップ ポリシーをすべて適用する必要があります。

- 地理的な位置とネットワーク内の場所に基づいたユーザのグループ化：

  ロケーション情報は、DV ユーザがどのデータセンターからサービスの提供を受けるかを決定します。また、ネットワーク、セキュリティ、ローカリゼーションの各ポリシー要件を明らかにするのにも役立ちます。

- ユーザ単位またはユーザ ロケーション単位でのアクセス レベルの定義：

多様な作業者（固定ユーザ、モバイル ユーザ、在宅勤務者、請負業者など）が存在し、既存の IT インフラストラクチャを所有する大企業では、明確に定義されたデータ アクセス ポリシーが適用されています。こうしたポリシーのほとんどは、DV 環境内にシームレスに移行できます。移行後は、ユーザが必ずしも物理的なマシンや場所に関連付けられる必要がないことに注意してください。したがって、一部の DV 導入では、ユーザ、ユーザ タイプ、ロケーション、およびネットワーク接続ポイントに基づいてデータ アクセス ポリシーを定義する必要があります。これらのポリシーは、DV インフラストラクチャと企業の AD インフラストラクチャの関係に影響を与えます。

USB リダイレクト、ローカル側での印刷、音声チャネル サポート、Single Sign On（SSO; シングル サイン オン）などの DV 固有の機能の使用を明確に指定する、ビジネス ケースに基づいたユーザ単位のユーザ プロファイル向け IT ポリシーの定義。ポリシーは、周辺機器の使用、モニタ解像度の変更、特定のディスプレイ プロトコルの選択、個人ストレージ スペースへのアクセス、HVD の再起動などを許可または拒否するために、ユーザ プロファイル単位またはユーザ単位で定義される必要もあります。DV 環境内のこれらの機能は、ネットワーク要件、ストレージ要件、およびコンピューティング要件に大きく影響します。また、すべてのユーザにこれらの機能の利用を許可すると、DV 導入の実行可能性に深刻な影響を与える可能性があります。

関連情報

表 3 に、この章で説明したハードウェアおよびソフトウェアを含む特定のベンダー情報への便利なリンクを示します。

表 3　　DV 関連のリンク

XenDesktop 4 @ Citrix ナレッジ ベース http://support.citrix.com/proddocs/index.jsp
『Best Practices for Citrix XenDesktop with Provisioning Server』 http://support.citrix.com/article/CTX119849
『Citrix XenDesktop Modular Reference Architecture』 http://support.citrix.com/article/CTX124087
『Citrix XenDesktop - Design Handbook』 http://support.citrix.com/article/CTX120760
Citrix XenServer：ドキュメント http://docs.vmd.citrix.com/XenServer/5.6.0/1.0/en_gb/

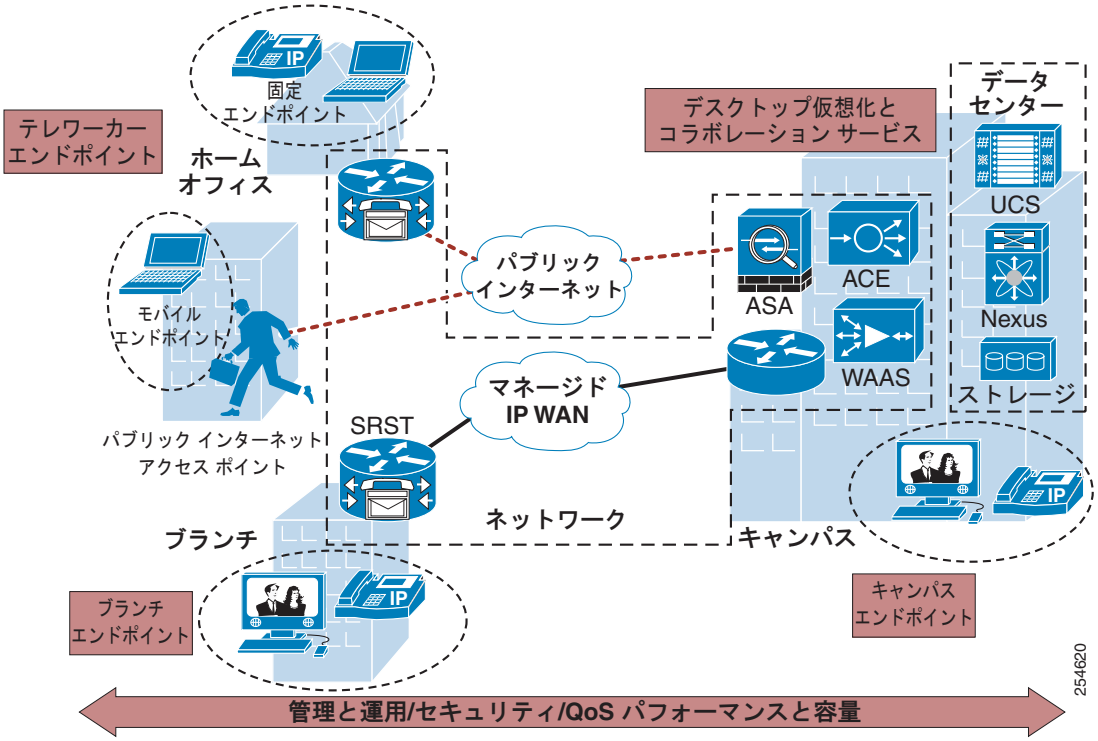
導入モデル

ネットワーク化されたユーザ エクスペリエンスをデバイス、場所、時間を問わず実現するというボーダレス ネットワークの展望は、企業の個別の需要に応じて、さまざまな方法で達成できます。仮想化は、システム設計者に新たな可能性をもたらし、コンピューティングやネットワーキングの投資場所の変化に基づいてさまざま導入モデルを使用できるようになります。

Cisco Virtualization Experience Infrastructure（Cisco VXI; Cisco 仮想化エクスペリエンス インフラストラクチャ）システムは、基本的にユーザのコンピューティング インフラストラクチャをデータセンター内に集中化することに基づいています。コンピューティング インフラストラクチャは、仮想化され、Desktop Virtualization（DV; デスクトップ仮想化）サブシステムとコラボレーション サブシステムをホストします。これらのサブシステムの連携により、デスクトップ サービスとテレフォニー サービスがネットワーク経由でさまざまな DV エンドポイントやコラボレーション エンドポイントに提供されるユーザ コミュニティが実現されます。これらのエンドポイントは、企業のネットワーク内の任意の場所に配置できます。「エンタープライズ ネットワーク」という用語は、企業の所有するネットワーキング インフラストラクチャ（企業の Virtual Private Network（VPN; バーチャル プライベート ネットワーク）ベースのインターネットへの拡張も含む）と社外で管理された他のさまざまな形態の商用ネットワークの両方を示すために使用されます。

ユーザは、さまざまな場所からコンピューティング リソースにアクセスできます。この章では、場所はネットワーク接続の条件を表し、ユーザのエンドポイントはこの条件を使用して、集中管理されたコンピューティング サービスに接続します。図 9 に示されているように、エンドポイントは、ネットワーク内でのそれらの場所に基づいて詳細に定義されます。

図 9　　Cisco VXI の全体像



キャンパス エンドポイント

キャンパス エンドポイントは、キャンパス内に導入されます。キャンパス内では、同じ場所に配置されたデータセンターがコンピューティング リソースを提供し、LAN によってネットワーク接続が提供され（通常は 100 Mbps 以上の速度）、15 ms 以下の遅延となります。

ブランチ エンドポイント

ブランチ エンドポイントは、企業のリモート ブランチ内に導入され、データセンターにマネージド WAN 経由で接続されます。この WAN では通常、事前に取り決められた Service-Level Agreement（SLA; サービス レベル契約）による帯域幅保証、遅延保証、およびジッタ保証が提供されます。また、オンネット アドレッシング（RFC 1918 に従ったプライベート アドレッシング）が提供され、ある程度のセキュリティ（インターネットと比べた場合）も備えています。エンドポイントが位置するリモート ブランチは、企業によって管理される環境であり、通常は Cisco ブランチ ルータ（Cisco サービス統合型ルータなど）を備えています。それにより、ネットワークベースのサービス（Cisco WAAS、テレフォニー ゲートウェイ、Survivable Remote Site Telephony（SRST）など）を導入して、DV サービスの特定要素（印刷など）を加速することができます。

テレワーカー エンドポイント

テレワーカー エンドポイントは、インターネットを介して導入されます。たとえば、リモート ワーカーが VPN 経由で社内のネットワーク サービスにアクセスする場合に導入されます。この接続は、パブリック インターネット上に確立された VPN 接続によって提供されます。一般に帯域幅、遅延、およびジッタの特性は不明であり、接続ごとに変化したり、同じ VPN 接続の期間内で時間とともに変動したりすることがあります。一般的な接続には Network Address Translation（NAT; ネットワーク アドレス変換）トラバーサルが 1 つ（または複数）存在し、基盤となる転送メカニズム（インターネット）は信頼できません。リモート環境は多様であり、エンドポイントのタイプはモバイル テレワーカー エンドポイントと固定テレワーカー エンドポイントにさらに分類できます。

モバイル テレワーカー エンドポイント

インターネットへの接続に公共の Wi-Fi ホットスポットが利用される場所（ホテルの客室、空港、またはその他の公共スペース）にいるユーザは、モバイル テレワーカー エンドポイントと見なされます。通常、ラップトップまたはモバイル インターネット デバイス以外に利用できる装置はありません。ユーザは基本的にデバイスの持つネットワーク機能と VPN 機能を利用することになります。複数のデバイスを使用する場合（携帯電話、タブレット コンピューティング デバイス、ラップトップ コンピュータなど）、それらはそれぞれ独自の VPN 接続を経由してエンタープライズ ネットワーク サービスに接続されます。

固定テレワーカー エンドポイント

エンドポイントは、専用のブロードバンド接続によってユーザがインターネットに接続される場合（ユーザがホーム オフィス環境内にいる場合など）、固定テレワーカー エンドポイントと見なされます。この状況は、帯域幅を除けば、モバイル テレワーカー エンドポイントに対するものとほぼ同じです。一般に、パブリック インターネット接続によって提供されるものよりも、帯域幅は大きく、その可用性は高いです。このケースでは、ユーザに Small Office Home Office（SOHO）ルータが提供される場合があります。このルータによって、ハードウェアベースの VPN 接続を確立できます。この場合、ユーザはエンドポイントや接続の選択肢が増えます。次のような選択肢があります。

- 専用のコラボレーション エンドポイント（Cisco Unified IP Phone など）。仮想デスクトップから Cisco Unified Personal Communicator を使用できるようになります（デスクフォン モードの場合）。
- ネットワーク接続プリンタ
- Cisco WAAS モジュールによる WAN 最適化機能

- Cisco Application and Content Networking System（ACNS）ネットワーク モジュールによるコンテンツ キャッシング機能

これまで明らかにしたさまざまなエンドポイントの場所は、Cisco VXI と多くの属性を共有します。これらの共通の機能属性は、この後のセクションでブランチ エンドポイントに重点を置いた説明を通じて示されます。ブランチ エンドポイントに重点を置いたのは、説明を簡素化するためです。エンドポイントの場所から生じる差異については、構成要素テクノロジーを扱っている各章で説明します。

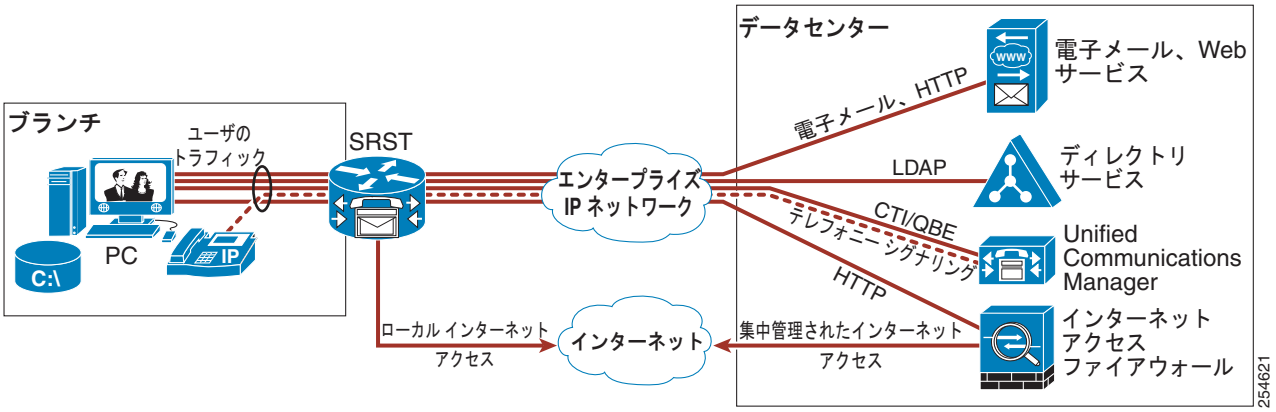
Cisco VXI：新しいユーザ導入

以降のセクションでは、集中管理された仮想化によりもたらされるユーザ コンピューティング リソース展開の根本的な変化について、従来の分散型ユーザ コンピューティングのコンピューティングおよびネットワーキング環境と、集中管理された Cisco VXI 環境を対比して説明します。

PC ベースのコンピューティング

図 10 に示されているような、一般的な PC ユーザのコンピューティング環境について考えてみます。

図 10　　PC ベースのコンピューティング環境



ユーザ コンピューティング リソース

ユーザのコンピューティング環境は、Personal Computer（PC; パーソナル コンピュータ）が中心となります。ユーザの PC は、自身のハードウェアのコンピューティング（CPU）、メモリ（RAM）、およびストレージ（ハード ドライブ）リソースを利用します。特に重要なのは、ローカルに構成されたストレージにユーザのオペレーティング システム（OS）と個人ファイルが格納される点です。このストレージ リソースは、企業の IP ネットワークを経由して、リモートで頻繁に管理（バックアップ、パッチ、設定）されなければならない IT 資産です。集中管理された仮想化では、このストレージ リソースは共有の集中配置されたストレージ システムの下に置かれます。

ユーザ ネットワーク接続

ユーザ アクションに応じて、PC からさまざまな接続が行われます。それにより、ユーザの一般的なアプリケーションがサポートされます。

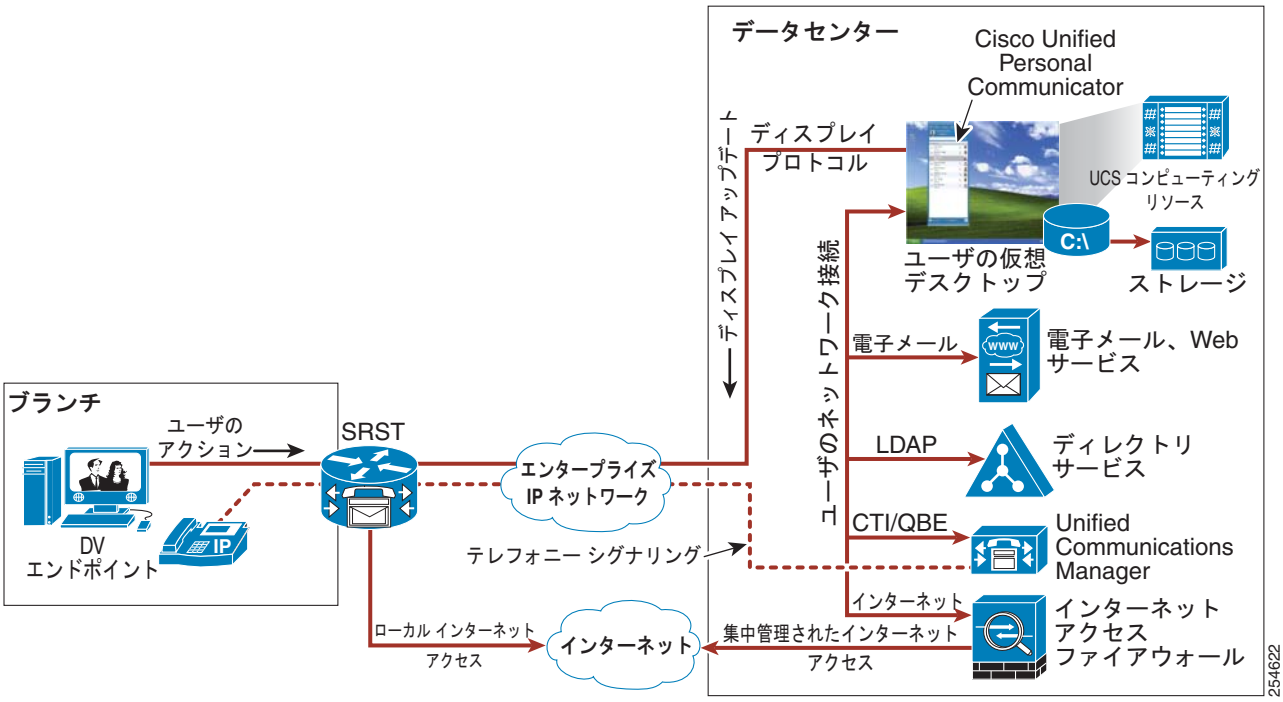
- 電子メールを使用する場合、ユーザの PC は、企業の電子メール システムへの接続を開始します。この接続は、SMTP、POP3、IMAP、Microsoft Exchange など、さまざまな電子メール プロトコルに基づくことができます。同様に、Web ベースのリソースにアクセスする場合、ユーザの PC は、オンネット（エンタープライズ内）またはオフネット（インターネット経由）のいずれかでサーバへの HTTP ベースの接続を開始します。
- Web を閲覧する場合、ユーザの PC は、インターネットへの HTTP 接続を開始します。インターネットへのアクセスは、ユーザのブランチ ロケーションから直接実行されるか、企業のメイン サイト内の集中管理されたインターネット リンクに集約されて実行されます。
- ディレクトリ アクセスは、ユーザの PC から直接開始されます。たとえば、ユーザが同僚の電話番号を社内ディレクトリで検索する場合、Lightweight Directory Access Protocol（LDAP; 軽量ディレクトリ アクセス プロトコル）クエリーがユーザの PC から開始されます。
- ユーザの電話機は、集中呼処理トポロジで導入できます。この場合、ユーザのアクション（電話の発信）は、集中管理された Cisco Unified Communications Manager にリレーされて処理されます。テレフォニー シグナリングは、Session Initiation Protocol（SIP; セッション開始プロトコル）または Skinny Call Control Protocol（SCCP）を使用して実行できます。
- Cisco Unified Personal Communicator などのコラボレーション アプリケーションにより、ユーザは、インスタント メッセージング、プレゼンス、連絡先検索、およびテレフォニー制御を 1 つのデスクトップ アプリケーションの下に集めることができます。Cisco Unified Personal Communicator は、これらの機能をサポートするために、さまざまな集中管理されたサービスへの接続を開始します。注目すべき点は、Cisco Unified Personal Communicator を使用してユーザのデスクフォンを制御するとき、Cisco Unified Communications Manager に対して Computer Telephony Integration/Quick Buffer Encoding（CTI/QBE）接続が開始されることです。

ユーザの PC 接続はすべて、該当するサービスに対して別々に開始されます。つまり、各接続は、ユーザの PC から目的のサービスへと向かう独立した IP トラフィック フローとなります。

集中管理された仮想ユーザ コンピューティング

仮想化により、ユーザのコンピューティング環境とネットワーキング環境の展開に根本的な変化がもたらされます。図 11 に、Desktop Virtualization（DV; デスクトップ仮想化）を使用したときのユーザのコンピューティング環境、接続環境、およびストレージ環境の変化を示します。

図 11　　DV ベースのコンピューティング環境



ユーザ コンピューティング リソース：集中管理、仮想

この展開では、ユーザのデスクトップは仮想化インフラストラクチャ内に配置されています。ユーザ デスクトップの OS は、コンピューティング、ストレージ、および接続の共有インフラストラクチャ上で集中管理されて稼動しています。したがって、次のようになります。

- ユーザの OS とすべてのアプリケーションは、CPU とメモリについて集中管理された共有のコンピューティング リソースを消費しています。これらの共有リソースは、複数のユーザをサポートします。
- ユーザの OS ファイルとアプリケーション ファイルは、集中管理されたストレージ システム上に保存されます。

（注） 電子メール、Web、ディレクトリ、ユニファイド コミュニケーション サービスなどのサーバ アプリケーションも仮想化できます。上の図では、ユーザ デスクトップ仮想化に重点を置いています。

ユーザ ネットワーク接続

ユーザのデスクトップ環境と各種 IT サービスの間の接続は、データセンター内で実現されるようになっています。場合によっては、ユーザのデスクトップと目的のサービスの両方が同じコンピューティング インフラストラクチャ内で仮想化されると、その接続は仮想化環境の外に出なくなります。

新しいタイプのエンドポイント

ユーザの PC は、DV エンドポイントに置き換えられています。ユーザのアプリケーションのローカル実行をサポートするために「シック」クライアントが必要な PC ベースの環境とは違い、仮想化環境では「シン」ユーザ デバイスが必要であり、ディスプレイ デバイスとユーザ入力デバイスをサポートします。ユーザ アクションは、キーボートとマウスからユーザの Hosted Virtual Desktop（HVD; ホステッド仮想デスクトップ）へディスプレイ プロトコルによってリレーされ、共有の仮想化されたコンピューティング、ストレージ、および接続のリソース上で実行されます。ユーザのアクションの視覚的な結果は、ディスプレイ プロトコルによってユーザの DV エンドポイントに返されます。

（注） エンタープライズ IP ネットワークはユーザ デスクトップごとに 1 つの接続のみを保持するようになります。この接続は、ユーザ アクションとデスクトップ GUI アップデートを伝達するルートになっています。たとえば、文字「A」を入力した場合、ディスプレイ プロトコル メッセージによってユーザのアクションが DV エンドポイントからユーザの HVD へ向けて送信され、そのデスクトップのアプリケーションによりアクションが処理されます。ユーザの画面上での文字「A」のディスプレイ アップデートは、HVD からのユーザの DV エンドポイント宛のディスプレイ プロトコル メッセージに基づいて行われます。

Cisco VXI では、豊富なデスクトップ仮想化エンドポイントのエコシステムがサポートされます。「エンドポイントとアプリケーション」の章に、Cisco VXC2200 シリーズのゼロ クライアント スタンドアロン タワー、Cisco VXC2100 シリーズのゼロ クライアント「バックパック」など、シスコの DV エンドポイント製品に関する詳細が示されています。

図 11 の環境では、Cisco VXC2200 は、Power over Ethernet（PoE）を利用可能な場合はアクセス スイッチから、そうでなければスタンドアロンの電源装置モジュールから電力が供給されるスタンドアロン DV エンドポイントとなります。

Cisco VXC2100 も同様の機能を備えていますが、シスコの IP 電話に対するアドオン モジュール形式になっています。したがって、アクセス スイッチへの電話機の接続を利用して、電力を供給し、Cisco VXC2200 へのネットワーク接続を提供できます。このアプローチにより、物理的なデスクトップに余分なデバイスのない作業スペースができます。

接続の変化

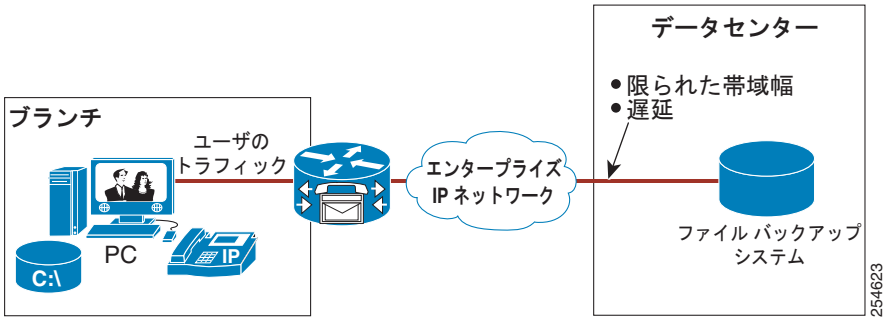
非仮想化環境では、ユーザのアクションは、多くの場合、ユーザの PC とデータセンターの間のネットワーク トラフィックになります。システム設計者が接続で常に考慮するのは、エンタープライズ ブランチが、ブランチ内の PC アプリケーションの接続ニーズに合った帯域幅で導入されるようにすることです。これらのニーズは、アプリケーションごとに異なり、実行中に帯域幅を可能な限り消費するもの（データ バックアップ アプリケーションなど）や、散発的に帯域幅を必要とするもの（Web 閲覧など）があります。キャンパス以外のすべての展開では、接続は、限られた帯域幅の WAN またはインターネット クラウドを通過します。

PC ユーザと比べた場合、DV ユーザの接続ニーズがどのように変化しているかを示す例をいくつか紹介します。

ファイル バックアップ

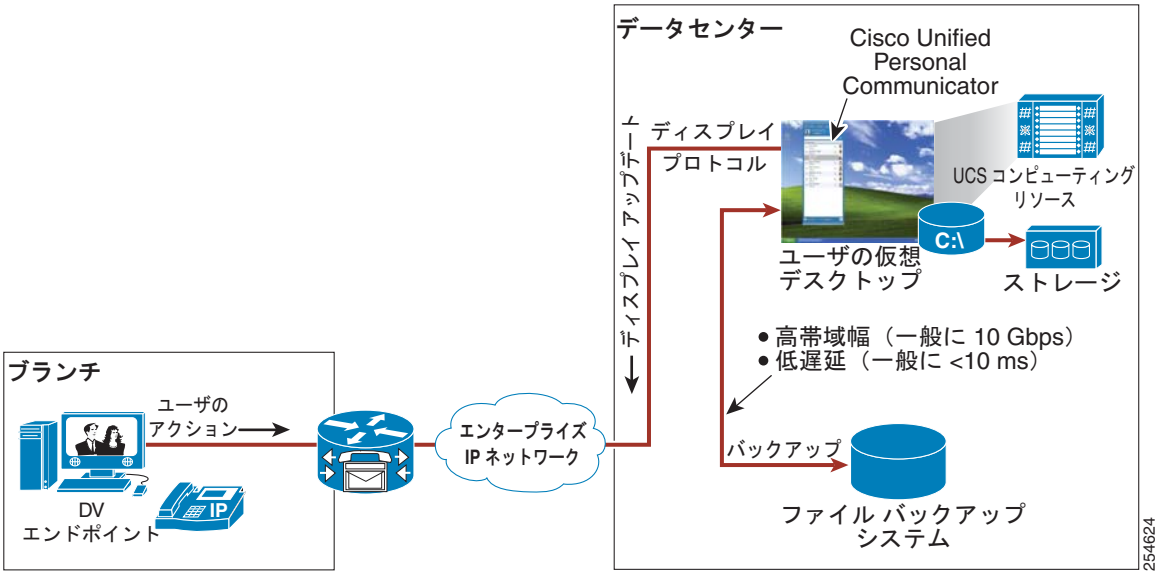
図 12 に示されているように、バックアップ アプリケーションがユーザの PC から中央のファイル ストレージ システムにファイルをコピーする場合、データ フローはエンタープライズ IP ネットワークを通過します。ユーザがブランチ オフィスにいる場合、バックアップ アクションは WAN を通過します。そのため、遅延と帯域幅がトランザクションの所要時間とコストに影響します。

図 12　　PC ベースのファイル バックアップ



集中管理されたデスクトップ仮想化環境では、ユーザのデスクトップと中央のストレージ システムは同じ場所に存在し、同じ高速 LAN によってサービスが提供されます。したがって、バックアップ アクションは、速度が向上し、コストが低下します。図 13 に、バックアップ動作の接続の変化を示します。

図 13　　DV ベースのファイル バックアップ



ファイル バックアップ システムは、それ自体が仮想化されているかどうかに関係なく、ユーザの HVD と同じ場所に存在します。したがって、バックアップ トラフィックは WAN を通過しません。この例では、データセンター内でのユーザのデスクトップの仮想化によってもたらされる接続の変化を示しています。

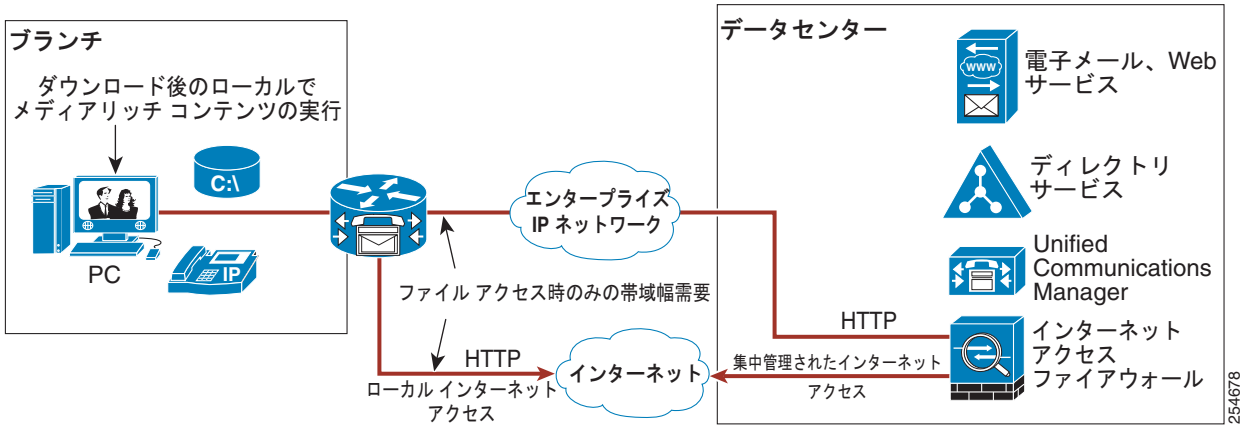
インターネット閲覧

PC のインターネット閲覧の例を図 15 に示します。ブランチ内にいる PC ユーザがインターネットにアクセスする場合について考えてみます。企業では 2 種類の接続トポロジがよく使用されます。1 つは集中管理されたインターネット アクセス ポイントがデータセンター内に配置され、もう 1 つはブランチのローカルからの接続でインターネットにアクセスします。等価な帯域幅の接続の場合、ユーザのエクスペリエンスはどちらの場合も同じです。ただし、データセンター経由のインターネット アクセスは、エンタープライズ IP WAN に対して帯域幅を要求します。

Flash ベースのビデオ ファイルの視聴など、特定のケースの PC ベースのインタラクティブ マルチメディア コンテンツの閲覧では、帯域幅の需要がファイルの再生よりも先に発生します。コンテンツは、最初にダウンロードされ、その後に再生されます。一部のストリーミング コンテンツの場合でも、メディア ファイルのバッファリングにより、コンテンツの表示が帯域幅の需要よりも後になります。

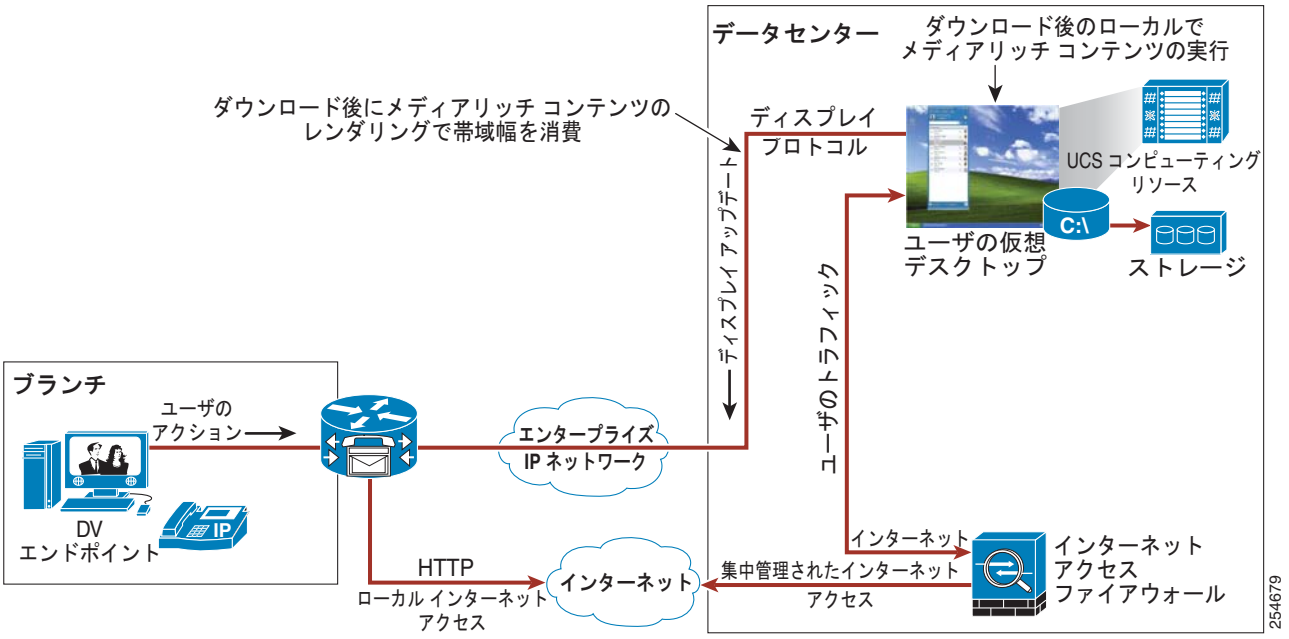
インタラクティブ マルチメディア ファイルがユーザの PC で再生され始めると（または、ストリーミング メディアの場合、バッファがファイルの最後まで到達すると）、WAN やインターネット接続に対する帯域幅の需要はなくなります。

図 14　　PC ベースのインターネット アクセス



インターネット アクセスが HVD 経由で実現される場合、接続の変化は DV エンドポイントの機能によって異なります。図 15 では、インターネット閲覧機能が本質的に HVD のブラウザによって実現されている DV エンドポイントについて考えます。この場合、マルチメディア コンテンツのダウンロード中は、ユーザの HVD とインターネットの間で中央のインターネット接続経由の帯域幅が消費されます。その後、ファイルの再生時にエンタープライズ IP WAN 上で帯域幅が消費されます。後者は、コンテンツの実行をリモート ブランチから中央のデータセンターに移したことによりもたらされた重要な結果です。視聴対象のインターネット コンテンツが HVD に配信された後も、HVD から DV エンドポイントへのディスプレイ アップデートのために WAN 帯域幅が必要です。ループしたインタラクティブ マルチメディア アニメーションの場合、コンテンツのインターネット ダウンロードは中央サイトのインターネット接続上での規則的な有限の量の帯域幅となり（数秒間に 1 Mbps など）、WAN 帯域幅に対するディスプレイ プロトコルの需要はユーザのデスクトップがそのファイルのレンダリングを止めるまで続きます。

図 15　　DV ベースのインターネット アクセス



もう 1 つの導入モデルでは（図 16 を参照）、DV エンドポイントは、前と同様にユーザのコンピュータ リソースのほとんどをデータセンター内に集中化していますが、マルチメディア ファイルをローカルに実行する機能を一部保持しています。

図 16　　リッチ メディア コンテンツへのローカル インターネット アクセス

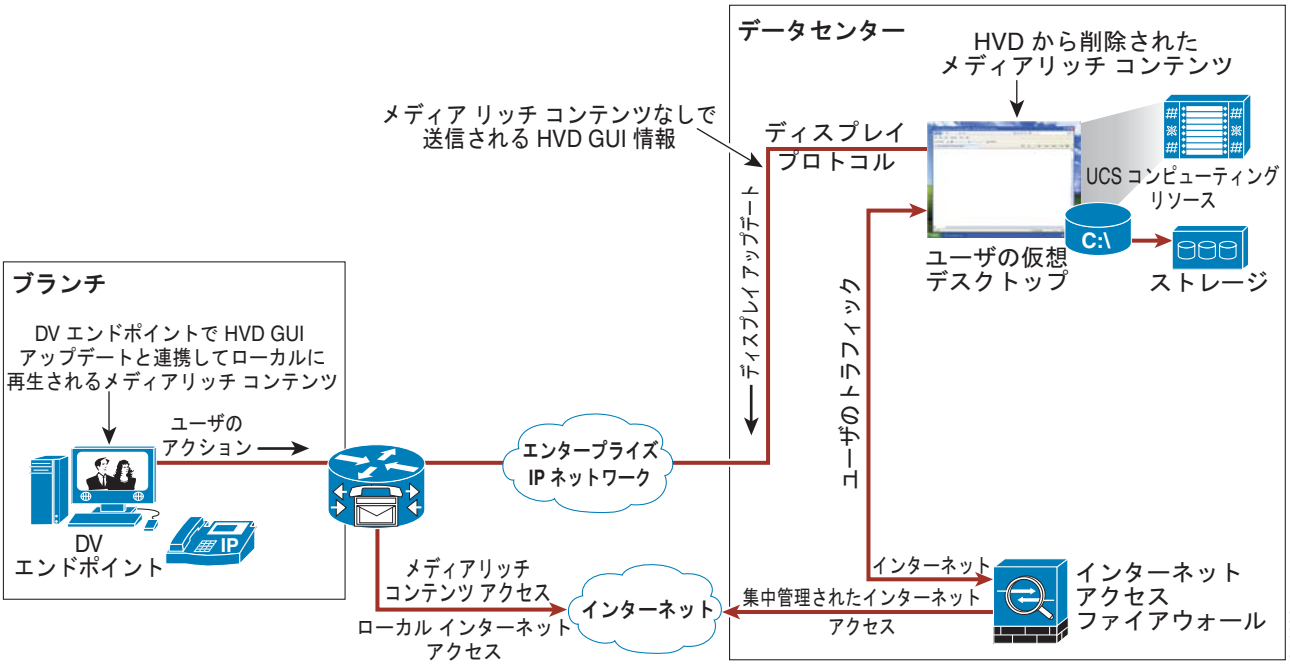
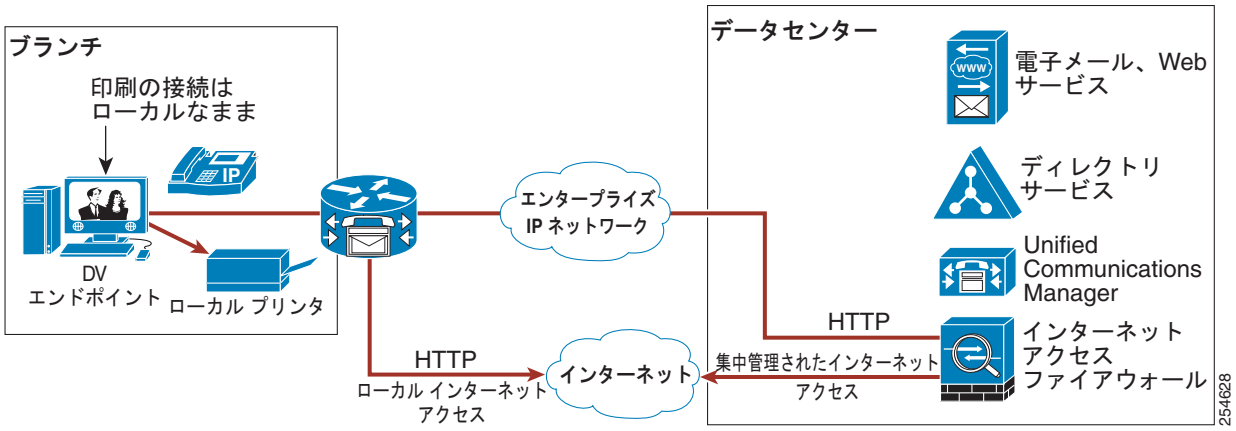


図 16 に、メディアリッチ コンテンツのローカル実行をサポートしている DV エンドポイントを示します。この導入モデルの DV エンドポイントは、ディスプレイ プロトコルや HVD の管理システムとやり取りして、一部のメディア タイプの制御を保持します。インターネット経由でインタラクティブ マルチメディア コンテンツにアクセスするとき、DV サブシステムは、DV エンドポイントがインターネットにローカル接続して視聴対象のメディア ファイルを取得するように指示します。DV エンドポイントで受信が完了した後、ユーザの HVD への WAN 接続とは無関係に、そのファイルの内容がエンドポイント上でローカルに実行されます。このアプローチでは、企業の WAN に対する帯域幅の需要を削減しながら、ユーザに対するパフォーマンスを向上させることができます。DV エンドポイントのコンテンツの閲覧機能とレンダリング機能は、DV サブシステムの機能とエンドポイントのタイプに応じて変化します。各種ベンダー オプションの詳細については、「デスクトップ仮想化」の章を参照してください。

印刷

図 17 に示されている非仮想化環境では、通常、PC ユーザの印刷アクションによってローカル ブランチ外のネットワーク トラフィックが発生することはありません。直接接続された USB プリンタへのユーザ印刷、あるいはネットワーク接続された IP プリンタへのユーザ印刷であっても、PC からプリンタへ直結したデータ フローが発生します。帯域幅の消費は、基本的にブランチ ロケーションの範囲内に収まります。

図 17　　PC ベースの印刷



集中管理された仮想化環境では、ユーザの印刷アクションは、ユーザの HVD からブランチに設置されたプリンタまでの接続に依存します。この接続は、HVD から DV エンドポイントの USB ポートまで（図 18 を参照）、またはブランチの IP ネットワーク接続プリンタまで（図 19 を参照）になります。いずれの場合でも、印刷アクションは、ユーザの HVD からブランチ ロケーションまでの接続に依存します。

図 18　　DV ベースの USB 印刷

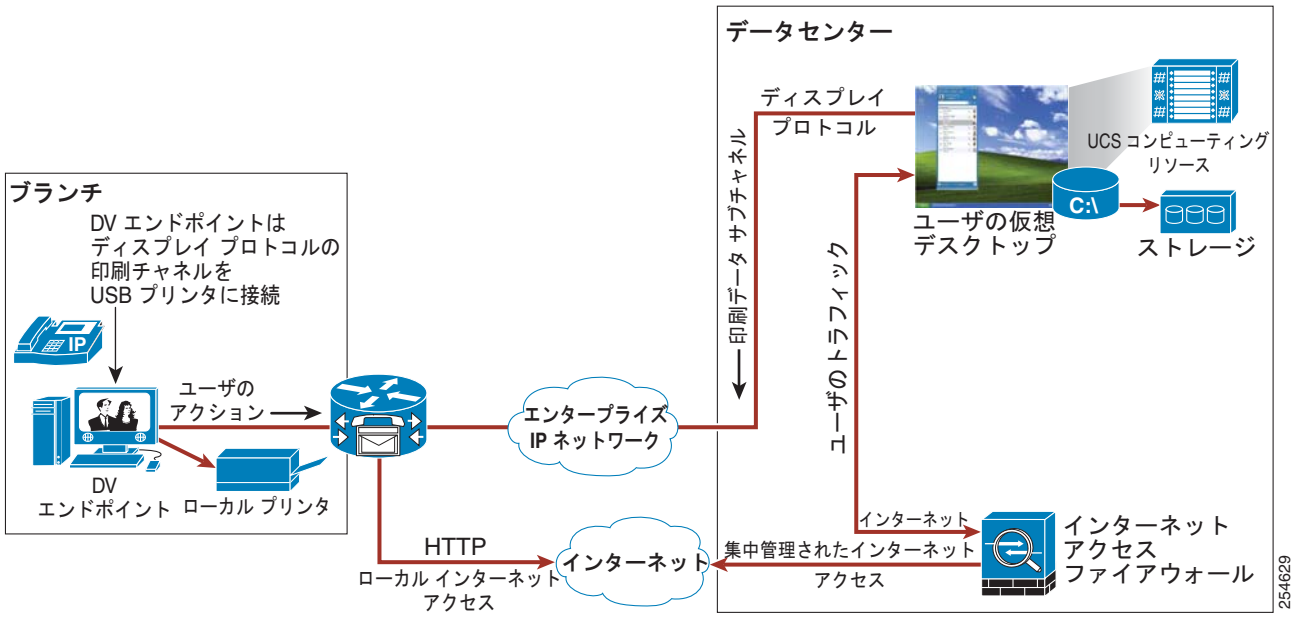
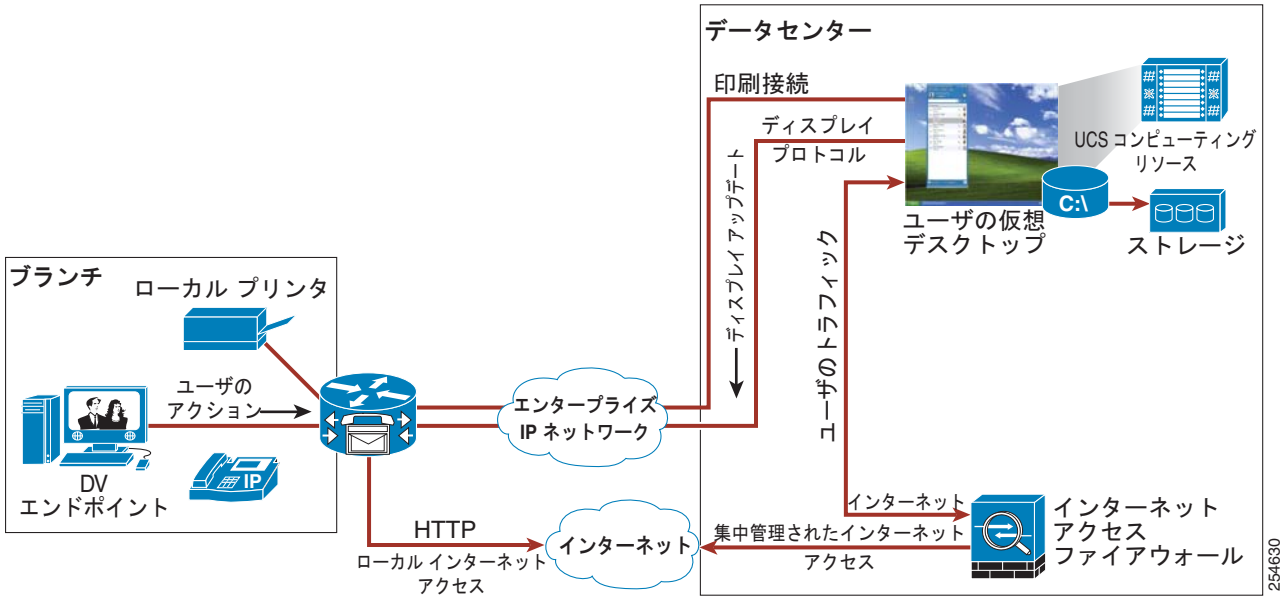


図 19　　DV ベースのネットワーク印刷



これらの図で示されているコンピューティング リソースとネットワーク リソースの機能上の考慮事項は、DV の導入全般に適用されます。Cisco VXI システムでは、DV の課題解決に向けて各サブシステムに的を絞ることにより、集中管理された仮想環境の導入が容易になっています。

- データセンター

  Cisco Unified Computing System™（UCS）ファミリのサーバおよびファブリック インターコネクト製品により、集中管理された仮想化のコンピューティング ニーズとストレージ ニーズに対して統合された管理、パフォーマンス、およびスケーラビリティが実現されます。

- ネットワーク

  Cisco Wide Area Application Services（WAAS）、Cisco Adaptive Security Appliance（ASA）、およびCisco Application Control Engine（ACE）により、ネットワーク接続に対して効率的な帯域幅の利用、セキュリティ、およびハイ アベイラビリティが提供されます。

- エンドポイント

  Cisco Unified IP Phone により、品質が保証されたビデオおよび音声のエクスペリエンスがユーザに提供されます。Cisco Unified Personal Communicator により、テレフォニー機能がデスクトップ仮想化ユーザ エクスペリエンスに統合されます。Cisco VXC エンドポイントにより、デスクトップ仮想化と、ユニファイド コミュニケーションおよびコラボレーションのユーザ エクスペリエンスが統合されます。

シスコのボーダレス ネットワーク アーキテクチャの一部として Cisco VXI システムを導入することで、デスクトップ仮想化展開は、集中管理された仮想化によるコスト面と運用面の多くの利点を享受しながら、高品質なエクスペリエンスをユーザに提供することができるようになります。

データセンター

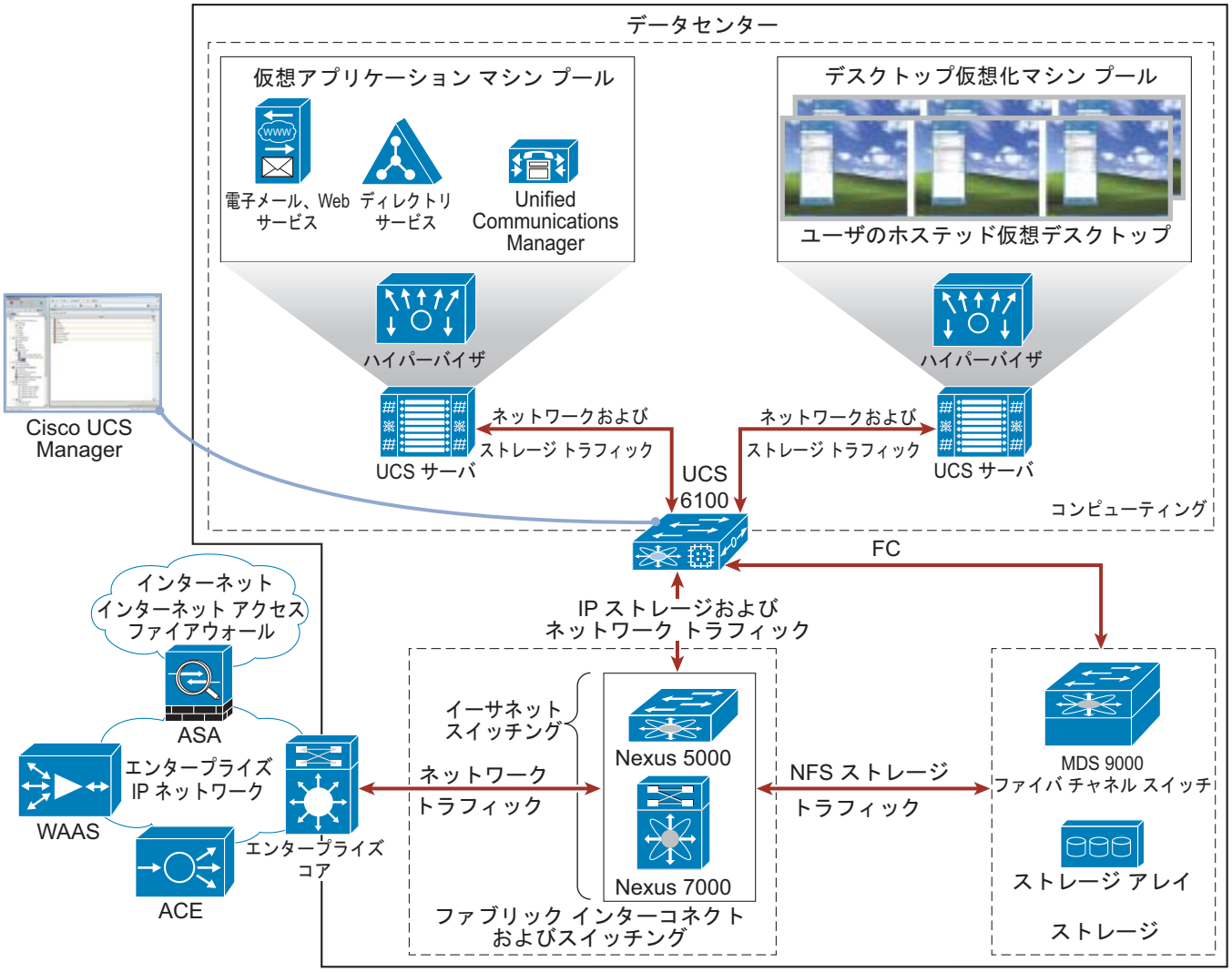
仮想化環境では、デスクトップは、データセンター内の集中管理されたサーバ上でホストされます。ユーザ数の変化は、データセンターの変化に直結します。したがって、スケーラビリティと柔軟性が不可欠になります。データセンター サーバは、(1) 高いパフォーマンスの実現、(2) 高い仮想マシン（VM）密度を可能にする十分なメモリの提供、および (3) 環境目標を達成するエネルギー効率の実現に対応できなければなりません。またデータセンターには、ハイパーバイザを、仮想リソースの適切なポリシー プロセスとセキュリティ プロセスで統合する機能も必要です。最終的に、ストレージも集中管理して、Network-Attached Storage（NAS; ネットワーク アタッチド ストレージ）、Storage Area Network（SAN; ストレージ エリア ネットワーク）、Direct-Attached Storage（DAS; 直接接続ストレージ）などの幅広いストレージ オプションに容易に対応できるようにする必要があります。

Cisco VXI 仮想化データセンターは、効率性、俊敏性、および変革可能性を併せ持つデータセンターを実現するように設計された、シスコの Data Center Business Advantage アーキテクチャをベースにしています。仮想化データセンターにより、企業は、データセンター インフラストラクチャを統合し、エネルギー コストを削減し、従業員の生産性を向上させ、ビジネス継続性を確保することが可能になります。また、きめ細かく段階的に導入することで、組織のニーズに応じたグレースフルな発展を達成することもできます。仮想化データセンター（図 20）は、ホステッド デスクトップ ソリューションを確実にサポートするために必要なコンピューティング機能、スイッチング機能、ストレージ機能、および仮想化機能を提供します。

仮想化データセンターは、(1) コンピューティング、(2) ファブリック インターコネクトとスイッチング、(3) ハイパーバイザ、および (4) ストレージからなる 4 つの基本要素で構成されます（図 20 を参照）。さらに、仮想化データセンターには、これらの要素をそれぞれ管理するために必要なツールも含まれます。

- コンピューティング要素は、Cisco Unified Computing System の上に構築されます。Cisco Unified Computing System は、Total Cost of Ownership（TCO; 総所有コスト）を削減し、ビジネスの俊敏性を高めることを目的として、コンピューティング、ネットワーク、ストレージ アクセス、仮想化、および管理を 1 つの緊密なシステムに統合する次世代データセンター プラットフォームです。Cisco VXI の検証済み設計には、B シリーズ ブレード サーバと C シリーズ ラックマウント サーバの両方の複数のモデルが含まれています。
- ファブリック インターコネクトとスイッチングのサブシステムは、Fibre-Channel と IP の両方のトラフィックが他の Cisco VXI サブシステム間で容易に移動できるようにします。Cisco UCS 6100 ファブリック インターコネクト デバイスは、このサブシステムのネットワーク接続と管理を行い、ラインレート、低遅延、ロスレスの 10 GB イーサネットおよび Fibre Channel-over-Ethernet（FCoE）機能を提供します。Cisco Nexus シリーズは、データセンター アクセス レイヤと IP ベースのネットワーク アタッチド ストレージ（NAS）接続を提供します。
- ハイパーバイザは、物理的なプロセッサ、メモリ、ストレージ、およびネットワーキングの各リソースを複数の仮想化マシン内に抽象化します。ハイパーバイザ環境は、仮想マシンの作成、管理、最適化、および移行を行う手段を提供します。この Cisco Validated Design は VMware vSphere 環境を基盤としていますが、それ以外のエコシステム パートナーのハイパーバイザをサポートすることも可能です。たとえば「付録 1：Microsoft Hyper V 使用時の特別な考慮事項」と「付録 2：Citrix XenServer 使用時の特別な考慮事項」では、Cisco VXI での Microsoft Hyper-V および Citrix XenServer の使用についてそれぞれ説明しています。
- ストレージ サブシステムには、Cisco UCS C シリーズ ラックマウントに搭載された直接接続ストレージだけでなく、EMC や NetApp などのエコシステム パートナーの NAS および SAN ストレージ ソリューションも含まれます。Cisco MDS ファミリのスイッチは、ファイバ チャネルベースのストレージ エリア ネットワーク アレイ用に接続を提供します。

図 20　　データセンターの構成要素



（注）　Cisco VXI は、Vblock™ および Flexpod™ のあらかじめパッケージ化されたインフラストラクチャ プラットフォームもサポートします。Vblock アーキテクチャの詳細については、http://www.vce.com/solutions/ を参照してください。FlexPod の詳細については、http://www.netapp.com/us/technology/flexpod/ を参照してください。

コンピューティング

Cisco VXI システムのコンピューティング構成要素は、Cisco Unified Computing System（UCS）B シリーズ ブレード サーバまたは C シリーズ ラックマウント サーバを使用して、仮想デスクトップをホストします。B シリーズ サーバと C シリーズ サーバは両方ともシスコ ユニファイド ファブリック システムをサポートします。このシステムは、コンピューティング、LAN、およびストレージのネットワーク間に 10 GB の接続を単一メディアで提供します。両方のタイプのサーバは、シスコ拡張メモリ テクノロジーもサポートします。このテクノロジーにより、パフォーマンス、キャパシティ、および VM 密度が従来のサーバと比べて向上します。UCS サーバは、エネルギー消費を削減するように設計されており、効率の高い電源と、作業負荷に合わせて消費電力を調整する Intel Xeon プロセッサを搭載しています。各サーバには、仮想化デスクトップ環境をサポートするために必要なプロセッサ、RAM、および I/O の各リソースが搭載されています。Cisco UCS サーバは、Cisco UCS Manager によって管理できます。Cisco UCS Manager は、サービス プロファイルとテンプレートを使用してロールベースおよびポリシーベースの管理を実装します。

B シリーズ サーバ

Cisco UCS B シリーズ ブレード サーバは、Cisco UCS 5108 ブレード サーバ シャーシ内に収容されます。このシャーシには、最大 8 台のハーフスロットまたは最大 4 台のフルスロット B シリーズ ブレード サーバを収容できます。この Cisco Validated Design は、次の 3 つのモデルの Cisco UCS B シリーズで検証されました。

- Cisco UCS B200 M2：ハーフ幅のブレード、最大 2 基の Intel Xeon シリーズ 5600 マルチコア プロセッサ、最大 192 GB のメモリを搭載可能な 12 DIMM スロット、最大 20 Gbps の I/O スループットに対応可能な 1 枚のメザニン カード。
- Cisco UCS B250 M2：フル幅のブレード、最大 2 基の Intel Xeon シリーズ 5600 マルチコア プロセッサ、最大 384 GB のメモリを搭載可能な 48 DIMM スロット、最大 40 Gbps の I/O スループットに対応可能な最大 2 枚のメザニン カード。
- Cisco UCS B230 M1：ハーフ幅のブレード、最大 2 基の Intel Xeon シリーズ 6500/7500 マルチコア プロセッサ、最大 256 GB のメモリを搭載可能な 32 DIMM スロット、最大 20 Gbps の I/O スループットに対応可能な 1 枚のメザニン カード。

Cisco UCS 5108 ブレード サーバ シャーシは、6 ラック ユニット構成（6RU）であり、業界標準の 19 インチ ラックでマウントできます。各シャーシは、最大 8 台のハーフ幅ブレード サーバまたは最大 4 台のフル幅ブレード サーバに対応できます。パッシブ ミッドプレーンでは、ハーフ幅ブレードあたり最大 20 Gbps の I/O 帯域幅とフル幅サーバあたり最大 40 Gbps の I/O 帯域幅が提供されます。

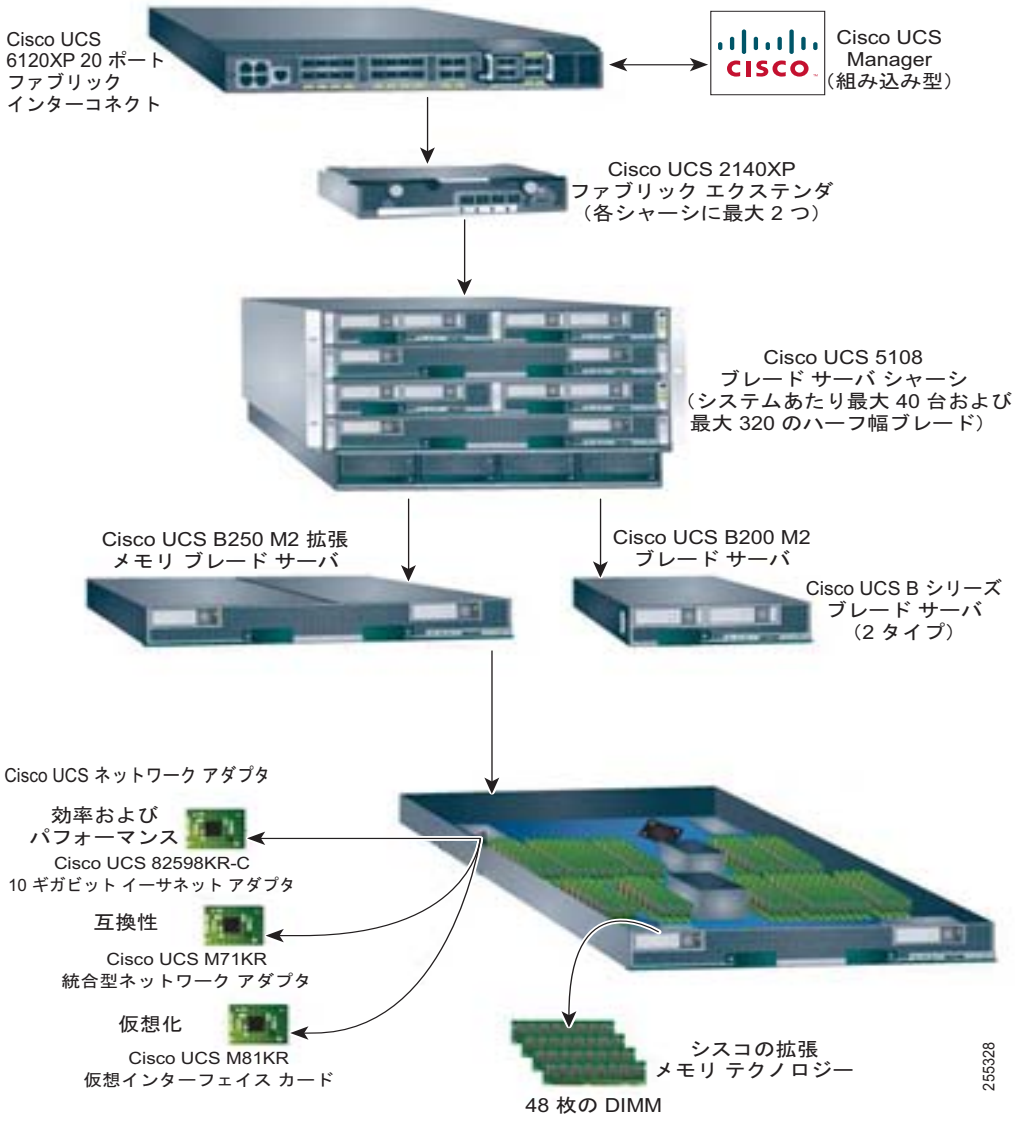
B シリーズ ブレード サーバは、統合ネットワーク アダプタを介してシャーシ ミッドプレーンに接続します。このアダプタは、各サーバにメザニン カードとして取り付けられます。これらのアダプタは、2 つのイーサネット ホスト バッファ アダプタと 2 つのファイバ チャネル ホスト バッファ アダプタをサーバ オペレーティング システムに提供し、各シャーシの背面にある Cisco UCS 2100 シリーズ ファブリック エクステンダに接続するために 2 つの 10 GB Fibre Channel over Ethernet（FCoE）ポートを提供します。ファブリック エクステンダは、統合ネットワーク アダプタからのトラフィックを集約し、最大 4 つの 10 ギガビット FCoE アップリンクで Cisco UCS シリーズ 6100 ファブリック インターコネクトのペアに転送します（図 21 を参照）。Cisco UCS 6100 は Cisco UCS Manager をホストします。Cisco UCS Manager は、コンピューティングとスイッチングの両方のファブリック リソースを管理するために使用されます。

C シリーズ サーバ

Cisco UCS C シリーズ ラックマウント サーバは、Cisco Unified Computing System™ の技術革新（シスコの拡張メモリ テクノロジーやユニファイド ネットワーク ファブリックなど）を業界標準のラックマウント フォーム ファクタに拡張したものです。C シリーズ サーバは、スタンドアロン環境でも、Cisco Unified Computing System の一部としても動作できます。C シリーズ サーバは、組織のタイミングや予算に応じて段階的に導入できます。これらのサーバは広範囲なネットワーク アダプタをサポートしており、既存のネットワークとストレージ ソリューションをすみやかに統合します。この Cisco Validated Design は、次の 2 つのモデルの Cisco UCS C シリーズで検証されました。

- Cisco UCS C200 M2 : 1 RU、2 基の Intel Xeon シリーズ 5600 マルチコア プロセッサ、最大 192 GB のメモリ、最大 4 台の内部 SAS または SATA ドライブ、2 つの統合型ギガビット イーサネット ポート、および 1 つの管理用 10/100 イーサネット ポート
- Cisco UCS C250 M2 : 2 RU、2 基の Intel Xeon シリーズ 5600 マルチコア プロセッサ、384 GB のメモリ、最大 8 台のスモール フォーム ファクタ SAS または SATA ドライブ、4 つの統合型ギガビット イーサネット ポート、2 つの管理用 10/100 イーサネット ポート

図 21　　Cisco UCS B シリーズ



Cisco VXI 内のコンピューティング サブシステムの最適化

- デスクトップ仮想化環境では、一般に、物理サーバあたりの VM 密度はアプリケーション サーバの VM 密度よりもはるかに高いです。キャパシティは、使用可能なメモリ、CPU キャパシティ、ネットワーク スループット、または仮想デスクトップ ソフトウェア自身によって制限される可能性があります。また、サーバ プールあたりの VM 数は、DV コネクション ブローカまたは管理ソフトウェアによって制限される可能性があります。「パフォーマンスとキャパシティ」の章に、タスク ワーカー プロファイルのテストに基づいた、キャパシティ プランニングに役立つガイドラインが示されています。

- 物理サーバは一般に複数のグループに分けられ、それぞれのグループが目的別に仮想マシンのニーズに応えます。たとえば、あるサーバ グループがユニファイド コミュニケーション、ディレクトリ、および電子メールの専用サーバとなる場合、他のサーバがデスクトップ仮想化ユーザのニーズに応えます。DV マシン プールは、専用の物理サーバ集合上に展開される必要があります。
- この Cisco Validated Design では、ユーザ デスクトップ VM とインフラストラクチャ VM（Microsoft Exchange Server、Web サーバ、アプリケーション サーバ、ライセンス サーバ、ユニファイド コミュニケーション、Active Directory など）に対して別々の物理サーバが導入されます。このアプローチにより、重要なインフラストラクチャ サービスは、仮想デスクトップ ユーザに関連した潜在的な負荷の集約効果や突発的な負荷の増加から保護されます。また、デスクトップ VM も、インフラストラクチャ サーバの需要ピークの影響を受けなくなります。

ファブリック インターコネクトとスイッチング

Cisco UCS 6100 ファブリック インターコネクトは、Cisco Unified Computing System 向けにネットワーク接続機能と管理機能を提供します。Cisco UCS 6100 シリーズは、ラインレート、低遅延、ロスレスの 10 GE 機能と Fibre Channel over Ethernet 機能を提供します。ファブリック インターコネクトは、一般に冗長ペアで導入されて、ネットワークとストレージの両方に対して均一なアクセスを提供します。Cisco UCS 6100 は、20 ポート モデルと 40 ポート モデルが提供されています。どちらのモデルも、高いパフォーマンスのユニファイド ファブリック、Cisco UCS Manager による集中統合管理、および VN-Link テクノロジーのサポートによる仮想マシンに最適化されたサービスを提供します。

Cisco UCS 6100 シリーズは、ブレード エンクロージャからの FCoE トラフィック フローを終端します。イーサネット トラフィックは分離され、（Cisco Nexus® 5000 および 7000 シリーズ スイッチで構成される）データセンター スイッチ ファブリックに転送されます。ファイバ チャネル トラフィックは、ファイバ チャネル アップリンク経由でファイバ チャネル Storage Area Network（SAN; ストレージ エリア ネットワーク）に転送されます。ファブリック インターコネクトとスイッチングの構成要素は、コンピューティング構成要素からのネットワーキングとストレージの両方のデータ フローをサポートします。

ファブリック インターコネクトは、UCS システムの管理を容易にする、Cisco UCS Manager を組み込んでいます。管理者は、Cisco UCS Manager を DV 管理ソフトウェアと組み合わせて使用することで、仮想マシンを導入したり、ソフトウェア アップグレードを実行したり、物理サーバ間で仮想マシンを移行したり、何千もの仮想化デスクトップに対してコンピューティング リソースを制御したりできます。さらに、Cisco UCS Manager と DV 管理ソフトウェアは、デスクトップ仮想化環境全体のモニタリングと管理を行うためのツールも提供します。

Cisco Nexus 5000 シリーズおよび 7000 シリーズ スイッチは、高速のイーサネット スイッチングを提供します。これらは一般に冗長ペアとして設置され、5000 シリーズ スイッチはアクセス レイヤに、7000 シリーズ スイッチはコアに配置されます。Nexus 5000 および 7000 シリーズ スイッチは、Cisco UCS ファブリック インターコネクトおよび Cisco Nexus 1000V シリーズ スイッチと連携して、デスクトップ仮想化をサポートするための高パフォーマンス、低遅延のインフラストラクチャを提供します。

Cisco VXI のファブリック インターコネクトとスイッチングのサブシステムの最適化

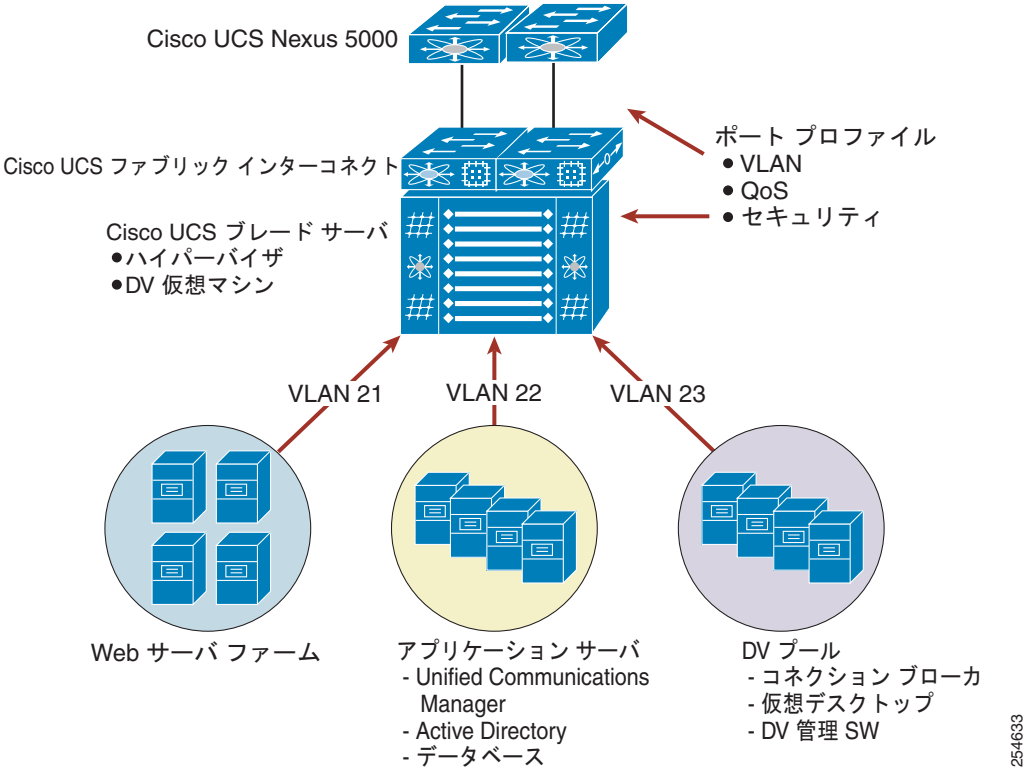
仮想デスクトップ数の増加に伴い、管理、セキュリティ、および可用性の複雑さも増します。VLAN を効果的に使用すると、スイッチング サブシステムの効率が向上します。図 22 に、複数の VLAN を使用して DV サーバ プールをセグメント化する例を示します。これらの VLAN は、会社のネットワーク ポリシーに基づいてデータセンター ルータまたはファイアウォール上で終端できます。

図 22 では、独立した 3 つのマシン プールに割り当てられる VLAN は、物理レベルでは Cisco Nexus 5000 シリーズ スイッチと Cisco UCS 6100 ファブリック インターコネクトで実装され、仮想レベルではハイパーバイザが VLAN の実装を提供します。各仮想マシン プールに示されている VLAN 番号は任意に設定されたものです。これらの VLAN 識別子は、データセンター管理者によって設定されたネットワーク ポリシーに従って割り当てる必要があります。

VLAN 21 のプールは、パブリック インターネットへのアクセスを必要とするアプリケーションを表しています。そのような仮想マシンは、一般に、VLAN 22 のプール内のサーバ上にホストされる内部アプリケーションから、ファイアウォールによって隔離されます。仮想デスクトップをホストしているサーバ プールは、VLAN 23 で表されています。このプールも、ファイアウォールで VLAN 22 のサーバから隔離される場合があります。

Cisco VXI システムの実装を成功に導くには、VLAN を多数使用して、DV、ストレージ、管理、VM マイグレーションなどのトラフィックを分離することが必要になります。VLAN の推奨リストについては、この章で後述される「ネットワークへのサーバの接続」のセクションを参照してください。

図 22　　ネットワーク接続用の物理リソースの割り当て

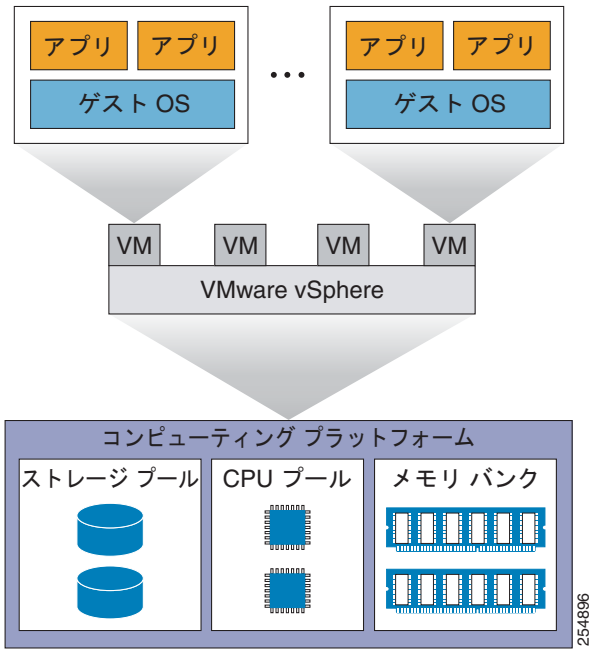


VMware vSphere ハイパーバイザ

VMware vSphere は、仮想化機能、管理機能、リソース最適化機能、可用性機能、および最適化機能を提供する製品スイートです。VMware vSphere ハイパーバイザ（ESX/ESXi とも呼ばれています）は、vSphere の主要な仮想化コンポーネントです。vSphere は Type 1 ハイパーバイザです。つまり、物理サーバ ハードウェア上で直接稼動します。vSphere は、物理サーバが所有するプロセッサ、メモリ、ストレージ、ネットワーキングの各リソースを複数の仮想マシン内に抽象化し、各 VM にそれらのリソースが適切に分配されるようにします（図 23 を参照）。VMware vCenter Server は、フロントエンドにグラフィカル ユーザ インターフェイス（GUI）を備えた高度なツール セットです。これにより、vSphere サーバおよび関連する仮想マシンが管理されます。また、高密度の実稼動環境において特に役立つ高度な機能も提供します。これらのツールにより、IT 管理者は、オーバーコミットされたホストマシンを識別したり、プールされたホスト間で VM を移行したり、電源投入シーケンスを管理したり、アクティブな VM を必要最小限のホスト上に統合したりすることが可能になります。

ハイパーバイザは、仮想化デスクトップとサーバが独立した仮想マシン（VM）として動作できるように、各 Cisco UCS サーバ上にインストールされます。物理と仮想のリソースは、複数の基準に従ってグループ化できます。仮想マシンのプールは、「タスク ワーカー」、「ナレッジ ワーカー」、「パワー ユーザ」などの作業者プロファイルの境界に沿って定義できます。また、販売、マーケティング、エンジニアリングなどの組織の境界に従ってリソースをグループ化することもできます。各プールには、同じセキュリティ ポリシーと QoS ポリシーを持つ同種の VM の集合が格納されます。仮想マシンのプールは、ハイパーバイザによって共通のリソースと関連付けられます。これらの共通リソースは、ハイパーバイザが仮想マシンの実行を選択すれば、それらの仮想マシンで常に利用できるようになります。

図 23　　VMware vSphere ハイパーバイザ



ハイパーバイザは、仮想デスクトップへのストレージ リソースの提供も行います。各仮想デスクトップは、ストレージ プールと関連付けられます。ストレージへの接続は、ハイパーバイザによって仮想領域で提供されます。このストレージは、UCS ブレード サーバ上に物理的に配置することも（ローカル ドライブ）、リモートで接続することもできます。仮想マシンの移行、クラスタリング、分散リソースのスケジューリング、およびその他の高度な仮想化機能をサポートするには、特定のユーザ集合に対するデータ ストレージが、それらのユーザの仮想デスクトップをホストしている物理サーバの集合全体で共通していなければなりません。そのため、多くの場合、DV には共有ストレージが適しています。共有ストレージは、ファイバ チャネル SAN 上に配置できます。また、Network File System（NFS）または iSCSI ベースのストレージ形式で IP ネットワーク上にも配置できます。

イーサネット データおよびネットワークベースのストレージ リソースにアクセスするために、ハイパーバイザは、物理ブレード サーバ上で使用可能な Converged Network Adapter（CNA; 統合ネットワーク アダプタ）に仮想デスクトップを接続することで、仮想領域と物理領域をブリッジします。CNA は、イーサネット NIC のペアとファイバ チャネル Host Bus Adapter（HBA; ホスト バス アダプタ）のペアに対する物理サーバ（ハイパーバイザ）アクセスを提供します。各 CNA は、イーサネット トラフィックとファイバ チャネル トラフィックを Fibre Channel over Ethernet（FCoE）トラフィックの形式でユニファイド ファブリック上に統合します。ハイパーバイザは、物理 Network Interface Card（NIC; ネットワーク インターフェイス カード）を仮想スイッチの一部として仮想 NIC にマッピングします。ファイバ チャネル トラフィック用の物理 Host Bus Adapter（HBA; ホスト バス アダプタ）は、仮想 HBA に直接ブリッジされます。

vSphere ハイパーバイザの導入のベスト プラクティス

vSphere ハイパーバイザは、可能ならば共有ストレージから起動するように設定します。これにより、ESX/VMware ESXi ソフトウェアの設定管理を一元化できるだけでなく、代替品ブレード サーバも利用できるようになります。

Cisco UCS Manager ネットワークとは異なるサブネット上に vSphere 管理イーサネット アドレスを設定します。これにより、ハイパーバイザが機能していなくても、ユーザは仮想 KVM コンソール（UCS Manager ソフトウェアの一部）にアクセスできるようになります。

ハイパーバイザの時計を外部 NTP サーバに同期させます。その後、仮想デスクトップ OS の時計をハイパーバイザの時計に同期させます。これにより、ロギング情報の時間の整合性が維持されます。この作業は、仮想デスクトップにインストールされた VMware ツールで実行できます。

詳細については、次の URL にある VMware vSphere のドキュメントのページを参照してください。
http://www.vmware.com/support/pubs/vs_pages/vsp_pubs_esxi40_i_vc40.html

vSphere 用の仮想スイッチング：Cisco Nexus 1000v

Cisco Nexus 1000v は、VMware vSphere 環境向けの仮想マシン アクセス スイッチです。Cisco Nexus 1000v は、VMware ESX または ESXi ハイパーバイザ内で動作し、Cisco VN-Link サーバ仮想化テクノロジーを活用してポリシーベースの VM 接続、VM のセキュリティとネットワーク ポリシーのモビリティ、および中断されない運用モデルを実現します。Cisco Nexus 1000v は、VM アクセス レイヤからデータセンターのネットワーク インフラストラクチャのコアに至る経路全体で、一貫性のあるネットワーキング フィーチャ セットとプロビジョニング プロセスを管理者に提供します。仮想サーバは、対応する物理サーバと同じネットワーク設定、セキュリティ ポリシー、診断ツール、および運用モデルを利用できます。

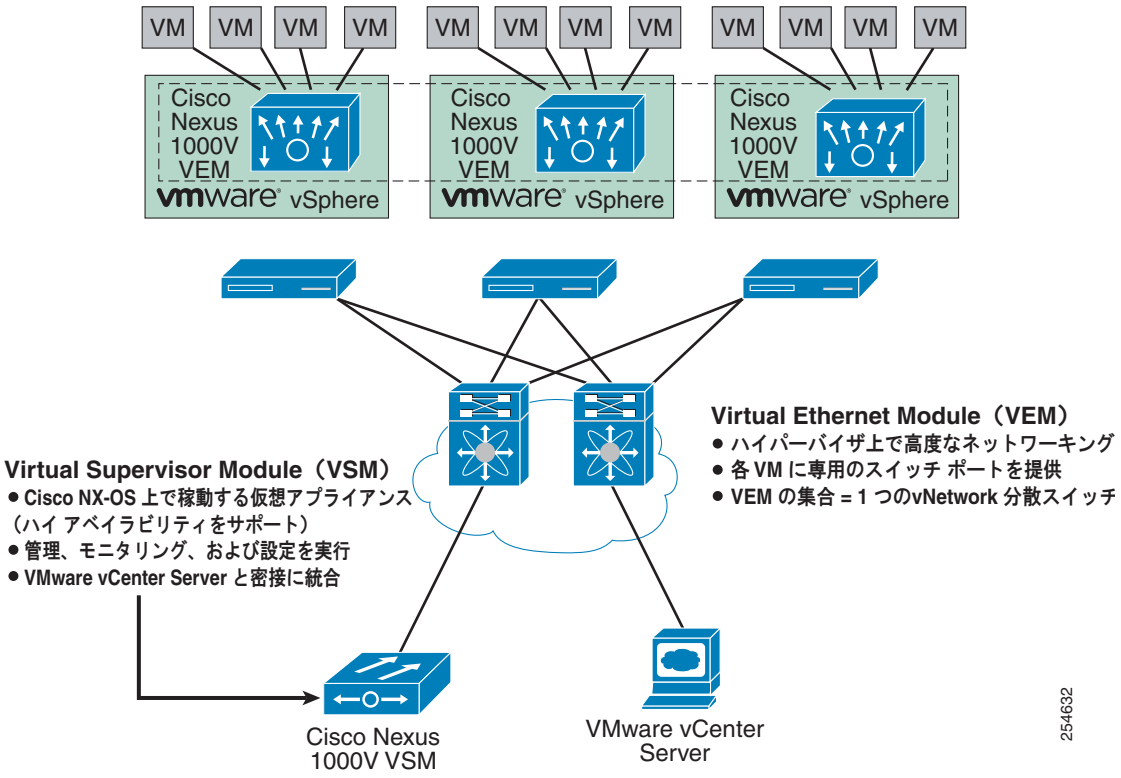
Cisco Nexus 1000v は VMware との緊密なコラボレーションを通して開発されており、VMware vSphere、vCenter、ESX、ESXi、およびその他多数の VMware vSphere 機能について互換性認定を受けています。

Cisco Nexus 1000v 仮想スイッチでは、仮想領域が 1 台の物理サーバに縛られることはありません。単一の分散仮想スイッチが、複数台の物理サーバにわたって存在できます。ポート プロファイルは、一度作成すれば、各仮想デスクトップに関連付けることができます。目的のポート プロファイルは、各タイプのユーザおよび仮想デスクトップに関連した特定の要件に従って作成できます。仮想デスクトップが移行されると、ポート プロファイルも一緒に移行されます。こうしたプロファイルは、Cisco Nexus 1000V シリーズ スイッチ内で作成され、VLAN 割り当て、QoS ポリシー、セキュリティ Access Control List（ACL; アクセス コントロール リスト）などの情報を保持します。ポート プロファイルは VMware vCenter 仮想マシン プロファイルにリンクされます。それにより、vCenter が特定の仮想デスクトップを vMotion で移行するとき、関連するポート プロファイルも移行されるようになります。

仮想デスクトップ接続に関する問題のトラブルシューティングは、内蔵の Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）プロトコルによって強化されます。最後に、セキュリティの強化は VLAN、プライベート VLAN、ポート セキュリティ、セキュリティ ACL など複数の追加機能を使用して実装されます。また、Cisco Nexus 1000V は、Cisco Virtual Security Gateway（VSG）や Cisco vWAAS などの他の仮想ネットワーキング ソリューションのための基盤も提供します。

Cisco Nexus 1000v の詳細については、このガイドの「Cisco VXI セキュリティ」の章を参照してください。

図 24　VMware ESX/ESXi と Cisco Nexus 1000V シリーズの統合



vSphere 用の VM ベースのセキュリティ ゾーン：Cisco Virtual Security Gateway

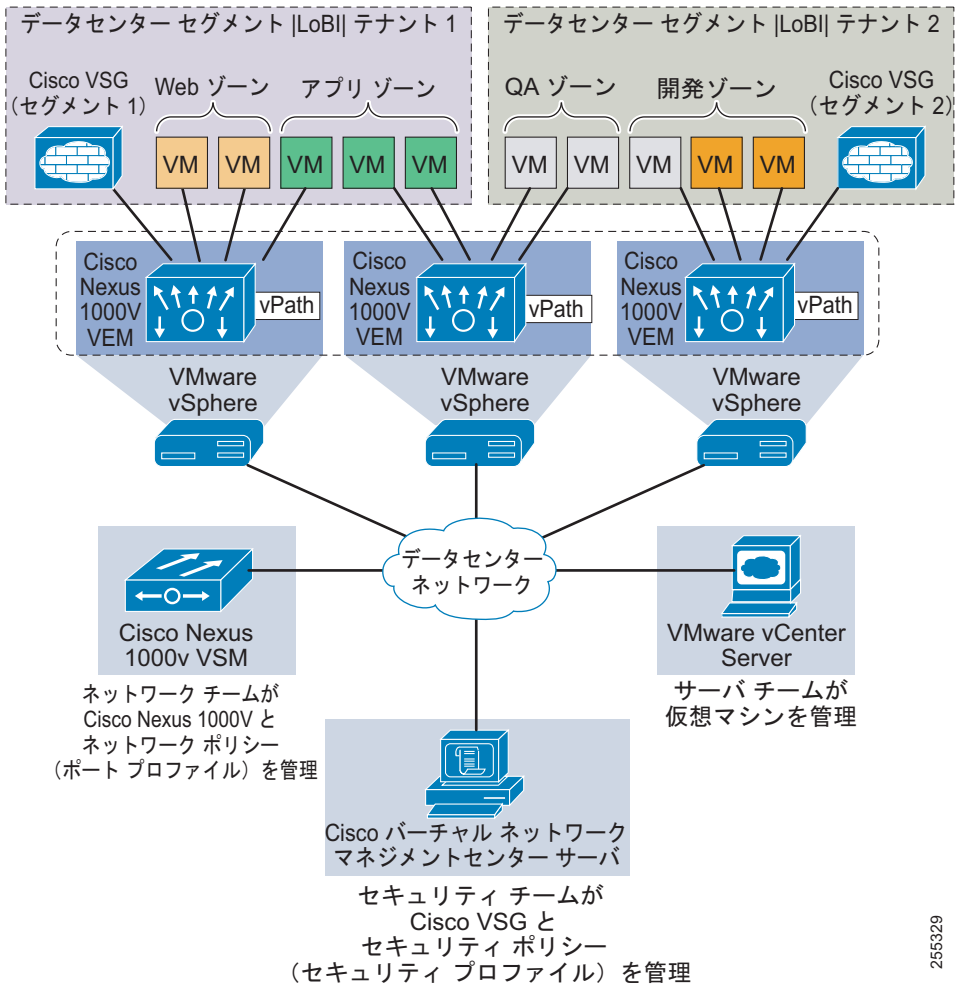
Cisco Nexus 1000v シリーズ スイッチ向け Cisco Virtual Security Gateway は、企業環境内やクラウド プロバイダー環境内の信頼ゾーンへのアクセスを制御および監視する仮想アプライアンスです。Cisco VSG は、コンテキスト連動セキュリティ ポリシーによるきめ細かなゾーンベースの制御およびモニタリングを使用して、仮想化データセンター VM のセキュアなセグメンテーションを提供します。制御は、組織的なゾーン、業種、またはマルチテナント環境に適用できます。コンテキストベースのアクセス ログが、ネットワークや VM のアクティビティ レベルで生成されます。信頼ゾーンとセキュリティ テンプレートは、VM が作成される際にオンデマンドでプロビジョニングできます。

Cisco VSG は、Cisco Nexus 1000v シリーズ仮想イーサネット モジュールに組み込まれている仮想ネットワーク サービス データ パス（vPath）テクノロジーを使用します。Cisco vPath は、指定された Cisco VSG にトラフィックを誘導してポリシーの最初の評価と適用を行います。後続のポリシーの適用は、vPath へ直接オフロードされます。Cisco VSG は、複数の物理サーバにわたって保護を提供できます。ワンアーム モードで透過的に挿入することができます。また、アクティブ/スタンバイ モードでハイ アベイラビリティを実現することもできます。

Cisco VSG は、複数の仮想マシン ゾーン、仮想化データセンター、仮想化アプリケーションにわたって展開できます。仮想の 1.5 GHz CPU、2 GB RAM、3 GB ハード ドライブ、および 3 つのネットワーク インターフェイス（データ、管理、およびハイ アベイラビリティ）が必要です。また、VMware vSphere と vCenter（4.x）、Cisco Nexus 1000v VEM と VSM、および Cisco バーチャル ネットワーク マネジメントセンターも必要です。

Cisco VSG の詳細については、このガイドの「Cisco VXI セキュリティ」の章を参照してください。

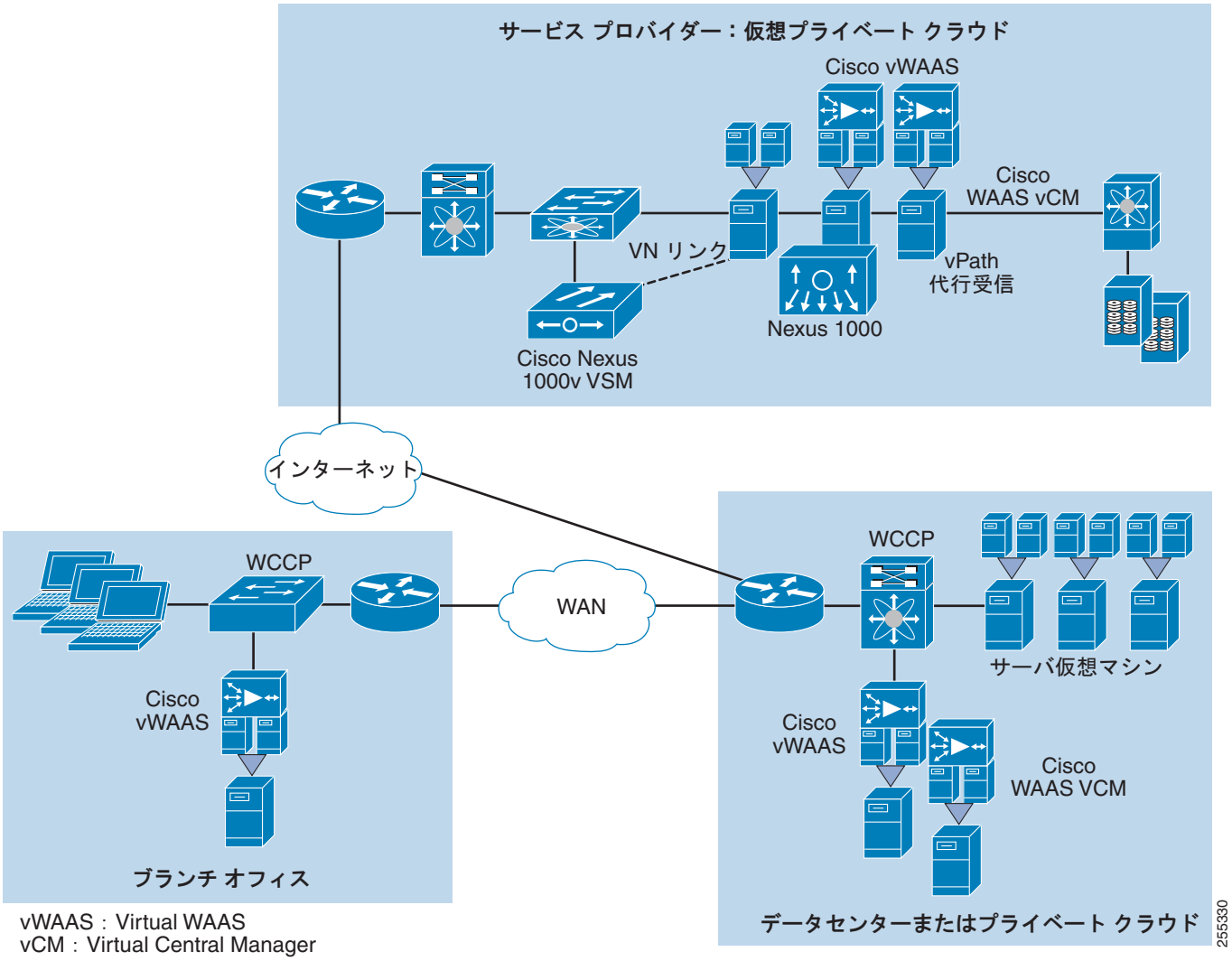
図 25　Cisco Virtual Security Gateway



vSphere 用の VM ベースのネットワーク最適化：Cisco vWAAS

Cisco Virtual WAAS（vWAAS）は、プライベート クラウドまたは仮想プライベート クラウドから提供されるビジネス アプリケーションの能力を向上させる仮想アプライアンスです。Cisco vWAAS は、Cisco UCS サーバと VMware vSphere ハイパーバイザの上で稼動し、Cisco Nexus 1000v スイッチでポリシーベースの設定を使用します。Cisco vWAAS は、インスタンス化されたり、移行されたりするアプリケーション サーバ VM と関連付けることができます。Cisco vWAAS により、クラウド プロバイダーは、設定や中断をほとんどせずに WAN 最適化サービスを迅速にプロビジョニングできます。

図 26　　Cisco vWAAS



vWAAS：Virtual WAAS
vCM：Virtual Central Manager

Cisco vWAAS では、（1）パス外代行受信による WAN エッジへの導入と（2）vPath 代行受信によるデータセンター中心部への導入という 2 つのオプションがサポートされています。WAN エッジは、最適化される WAN トラフィックを代行受信するために従来使用されている場所です。パス外モデルは、Web Cache Communication Protocol（WCCP; Web キャッシュ コミュニケーション プロトコル）を使用してトラフィックを代行受信します。このモデルでは、Cisco vWAAS 仮想マシンを搭載した VMware vSphere ホストが WCCP 対応のスイッチまたはルータに接続します。1 つのクラスタ内で複数の Cisco vWAAS VM が動作し、ルータで代行受信されたすべてのトラフィックを最適化できます。Cisco vWAAS VM は、単一または複数のサーバ全体にわたって配置できます。また、これまでの WAAS（物理）アプライアンスと vWAAS（仮想）アプライアンスが混在できます。

データセンター中心部への導入モデルでは、Cisco vWAAS VM が、同じ VMware vSphere ホスト内にあるサーバ VM の隣に配置されます。Cisco Nexus 1000v スイッチのポリシーベースの仮想サービスを使用して、Cisco vWAAS をアプリケーション単位またはサーバグループ単位で導入できます。Cisco Nexus 1000v の vPath 代行受信は、これらのサーバに対する送受信すべてのトラフィックを代行受信し、最適化のために Cisco vWAAS VM へ転送します。

Cisco vWAAS には、Data Redundancy Elimination（DRE）バイト キャッシュと Common Internet File System（CIFS）キャッシュを保存するためのストレージ アクセスが必要です。データセンター内では、直接接続ストレージまたは SAN のリモート共有ストレージのいずれかがサポートされます。vMotion、VMware Storage vMotion ®、VMware High Availability などの高度な VMware 機能を使用できるようにするために、SAN オプションを使用することを推奨します。

Cisco vWAAS の詳細については、このガイドの「VXI ネットワーク」と「パフォーマンスとキャパシティ」の章を参照してください。

ストレージ

Cisco VXI システムでは、共有ストレージ（NAS、SAN）と Direct-Attached Storage（DAS; 直接接続ストレージ）の両方がサポートされています。一般的に、共有ストレージが好まれる理由は、集中管理されたセキュリティ、高いパフォーマンス、リソース共有、および vMotion サポートにあります。それに対して DAS は、一般にパフォーマンスが低下し、vMotion が VMDK 全体をコピーする方法でしかサポートされませんが、低コストで導入できます。

共有ストレージ ソリューションは、エコシステム パートナーである EMC と NetApp から提供されます。どちらの提供ソリューションでも、NAS ベースと SAN ベースのストレージ接続を選択できます。共有ストレージは、高度なハイパーバイザ機能の利用を容易にし、デスクトップの移行に役立つため、多くの場合、仮想デスクトップ環境に適しています。ただし、初期または追加的な導入の場合や装置の設置面積を小さくする必要がある場合は、直接接続ストレージが適していることもあります。

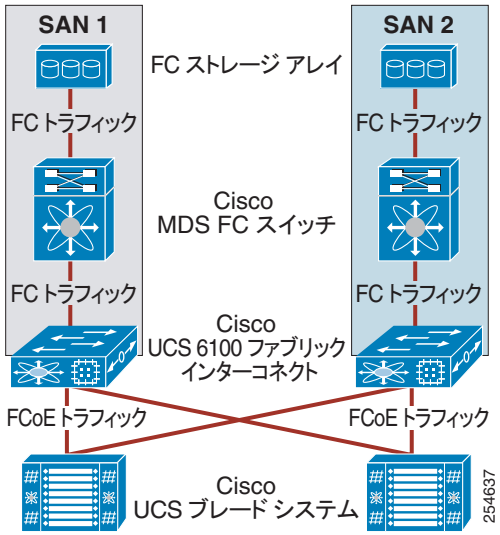
ストレージ アレイは、パーティションとも呼ばれる複数の Logical Unit Number（LUN; 論理ユニット番号）に分割されます。各 LUN は、複数のサーバ（および仮想デスクトップ）間で共有できます。しかし、セキュリティ上の理由から、およびストレージ トラフィック負荷のバランシングを容易にするため、仮想デスクトップを他の仮想サーバから隔離し、独立したストレージ プールにすることを強く推奨します。NFS アクセスの場合、アレイは、独立したファイル システムに分割されます。それぞれがハイパーバイザによってローカル ストレージ プールにマッピングされます。

ストレージ エリア ネットワーク

ファイバ チャネル ストレージ アレイは、Cisco MDS ファミリ スイッチのメンバーに接続されます。Cisco MDS スイッチにより、イーサネット スイッチの場合とほぼ同じように、複数のアレイが複数のホスト（サーバ）と通信できます。Cisco MDS スイッチは、Cisco UCS 6100 ファブリック インターコネクト上のファイバ チャネル アップリンクに接続されます。トラフィックは、Cisco UCS 6100 によって FCoE フレームにカプセル化され、サーバの Converged Network Adapter（CNA; 統合ネットワーク アダプタ）に転送されます。CNA では、ファイバ チャネル パケットが復元され、vHBA に転送されます。

ファイバ チャネル接続は、一般にアクティブまたはスタンバイ モードで動作します。SAN A がプライマリ アレイの場合、SAN B はミラー コピーとなります。場合によっては、ストレージ アレイ ベンダーにもよりますが、Cisco MDS スイッチ A と Cisco MDS スイッチ B のアップリンクが同じアレイを指し示すことがあります。ただし、特定の Logical Unit Number（LUN; 論理ユニット番号）は、それらのインターフェイスのうちの 1 つにしか同時には現れません。トラフィックのロード バランシングのために、LUN の割り当ては 2 つの SAN 間で混在させる必要があります。

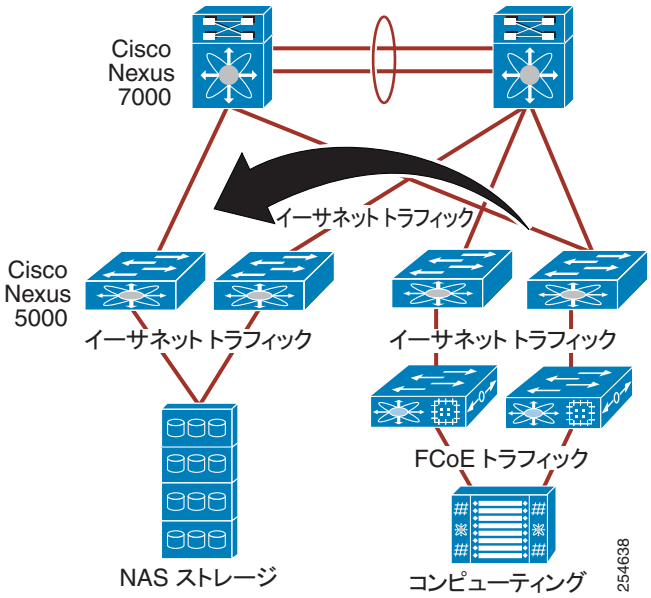
図 27　ファイバ チャネル ストレージ ネットワーク



ネットワーク アタッチド ストレージ

ネットワーク アタッチド ストレージでは、NFS サーバから送信されたトラフィックは、イーサネット トラフィックとして Cisco Nexus 5000 または 7000 シリーズ スイッチ経由でストレージ アレイにスイッチングされます。Nexus スイッチは、データセンターの多様なニーズに対応したユニバーサル プラットフォームを提供し、ネットワークの統合を容易にし、従来のテクノロジーから高度なテクノロジーへのシームレスな移行を可能にします。ファイバ チャネル接続ストレージと同様に、リモート アレイはローカル ハイパーバイザ ストレージ プールにマッピングされ、ハイパーバイザはシミュレートされたローカル ストレージを仮想デスクトップに提供します。これはイーサネットベースで実装されるので、ストレージは独立したストレージ VLAN に割り当てられます。ほとんどの場合、ストレージ アレイは同じ VLAN 内に配置されます。それにより、ハイパーバイザまたは DV 仮想マシンが、ネットワークに関する問題の発生原因となる複数のデフォルト ルートを保持する必要性が軽減されます。

図 28　　イーサネットベースのストレージ ネットワーク



共有ストレージに関する Cisco VXI の一般的なガイダンス

- ストレージ トラフィックは、統合ネットワーク アダプタの帯域幅の一部を消費します。リモート ストレージ トラフィックに対して、QoS ポリシーとキュー マッピングを使用する必要があります。詳細については、このガイドの「Quality of Service」の章を参照してください。このトラフィックを隔離するために、ストレージ VLAN を作成する必要があります。
- 多数の異なる VM が同じストレージを共有するので、集約されたトラフィックは、使用可能なリソース量を超える可能性があります。ある仮想デスクトップが大量のストレージ デバイス I/O を消費するアプリケーションを実行すると、同じ共有のストレージ リソース プールを利用する他の仮想デスクトップはリソース不足になることがあります。サーバ（Web サービス マシン等）や仮想デスクトップなどの仮想マシンのタイプに従って共有リソースを分離すると、この問題の解決に役立つ可能性があります。詳細については、このガイドの「パフォーマンスとキャパシティ」の章を参照してください。
- DV プールごとにリソース プールを別々に設定すると、ストレージ リソースの枯渇を回避できる可能性があります。汎用サーバから HVD を隔離する最良の方法は、それぞれが独立したストレージ ボリュームに割り当てられる、分離したサービス プロファイルを設定することです。
- 1 つのボリュームに割り当てられる VM の数は、その特定ボリュームに対して利用可能な I/O 帯域幅の合計を超えてはなりません。このための設定手順は、DV 管理ソフトウェア内で設定されるサーバ テンプレートに含まれます。詳細については、このガイドの「パフォーマンスとキャパシティ」の章を参照してください。
- ブート ストームを最小限に抑えるために、ステートレスな VM イメージとハイパーバイザ キャッシング テクノロジーを使用します。

EMC Unified Storage の実装

EMC Unified Storage ソリューションは、仮想デスクトップ環境に対して高度なフェールオーバーおよび完全に自動化されたストレージ階層化を提供します。EMC Unified Storage ソリューションにより、Network-Attached Storage（NAS; ネットワーク アタッチド ストレージ）、iSCSI、ファイバ チャネル Storage Area Network（SAN; ストレージ エリア ネットワーク）、および EMC Multi-Path File System（MPFS）を経由して複数のストレージ ネットワークに接続できるようになります。Cisco VXI システム テストでは、SAN の導入に対応した EMC Unified Storage ソリューションを検証しました。パフォーマンスとキャパシティの結果は、このガイドのキャパシティとパフォーマンスの章に示されています。シスコが実施した EMC Unified Storage ソリューションのテストでは、次の主要機能を有効にしました。

Fully Automated Storage Tiering for Virtual Pools（FAST VP）

EMC Fully Automated Storage Tiering for Virtual Pools（FAST VP）は、LUN 抽象化よりも下位のストレージ プール レベルで動作します。たとえば、FAST VP は 800 GB の LUN をフラッシュ ドライブに移動する代わりに、1 GB のチャンク内にあるストレージ プール全体を識別および監視します。データがアクティブになると、FAST VP はそれらの「ホット」チャンクだけを自動的にフラッシュなどの上位層に移動します。データがクール状態になると、FAST VP は下位層に移行するチャンクを正しく識別し、それらを事前に移動します。こうしたきめ細かい階層化により、ストレージの取得作業が軽減され、パフォーマンスと応答時間が向上します。『EMC FAST VP for Unified Storage Systems』を参照してください。

FAST Cache

FAST Cache により、フラッシュ ドライブをアレイの拡張キャッシュ レイヤとして使用できるようになります。FAST Cache は、アレイの FAST Cache 対応オブジェクト内で 64 KB のデータ チャンクを検証します。頻繁にアクセスされるデータは FAST Cache にコピーされ、以降のそのデータ チャンクへのアクセスは FAST Cache によって処理されます。これにより、非常にアクティブなデータをフラッシュ ドライブに迅速にプロモーションできるようになります。FAST Cache により、非常にアクティブなデータに対する応答時間が短縮され、LUN 内にホット スポットが発生する可能性が減少します。また、読み取り / 書き込みキャッシュも拡張され、ブート ストームやアンチウイルス スキャンなど読み取り中心のアクティビティと、オペレーティング システムのパッチやアプリケーションの更新など書き込み中心の作業負荷を取り込むことができます。FAST Cache テクノロジーの詳細については、http://www.emc.com/collateral/software/white-papers/h8046-clariion-celerra-unified-fast-cache-wp.pdf を参照してください。

圧縮

EMC Unified Storage では、データを圧縮し、貴重なストレージ キャパシティを再利用してストレージの効率性をさらに向上させる、Block Data Compression がサポートされています。データ圧縮はバックグラウンド タスクとして実行されるので、パフォーマンスのオーバーヘッドは最小限に抑えられます。Block Data Compression では、シン LUN もサポートされており、シック LUN が圧縮時にシン LUN へ自動的に移行されます。これにより、ストレージ キャパシティが解放されます。ブロック LUN レベルでの圧縮に加え、EMC Unified Storage ソリューションはファイル レベルの重複排除と圧縮も提供します。詳細については、http://www.emc.com/collateral/hardware/white-papers/h8198-vnx-deduplication-compression-wp.pdf を参照してください。

Citrix Machine Creation Services のサポート

EMC は Citrix Machine Creation Services（MCS）をサポートしています。Machine Creation Services（MCS）は、XenDesktop 5 で導入された新しいプロビジョニング メカニズムです。MCS は、新しい XenDesktop 管理インターフェイスである Desktop Studio と統合され、一元化された管理ポイントから実行するデスクトップのライフサイクル管理を通じて、デスクトップのプロビジョニング、管理、停止を行います。MCS では、専用マシンやプールされたマシンなど、複数のタイプのマシンを Desktop Studio のカタログ内で管理できます。MCS では Citrix XenServer 5.6 を使用する必要があります。詳細については、http://www.emc.com/collateral/software/technical-documentation/h8059-virtual-desktops-celerra-vmware-citrix-psg.pdf を参照してください。

NetApp FAS3170 ストレージの実装

NetApp FAS3100 シリーズは、SAN 展開と NAS 展開の両方をサポートする統合型ストレージ ソリューションです。Cisco VXI システム テストでは、ファイルベースのネットワーク アタッチド ストレージについて NetApp FAS3170 ソリューションを検証しました。テスト結果については、このガイドの「パフォーマンスとキャパシティ」の章で説明されています。FAS3170 は、NetApp の Data ONTAP オペレーティング システムを実行します。これにより、SAN（FCoE、ファイバ チャネル、および iSCSI）、NAS（CIFS、NFS）、プライマリ ストレージ、およびセカンダリ ストレージが単一プラットフォーム上で提供されるため、すべての仮想デスクトップ コンポーネントを同じストレージ アレイ上にホストできるようになります。シスコは、次の主要機能を有効にして NetApp FAS3170 をテストしました。

ストレージ効率

NetApp ストレージ効率テクノロジー（データ重複排除、圧縮、シン プロビジョニングなど）は、ストレージ要件の軽減を目的として設計されています。これらのテクノロジーは、デスクトップ仮想化などの高密度ソリューション アーキテクチャにおいて大きな価値をもたらします。マスター デスクトップ イメージ、ユーザ データ、ストリーミング アプリケーションなどのストレージ要件を軽減するために適用できます。

ハードウェア アクセラレーションによる VM クローニング

NetApp は、FlexClone で利用可能なアレイ ベースのゼロ コスト クローニングを提供します。仮想サーバと仮想デスクトップの迅速かつスペース効率の高い導入を行うために使用できます。FlexClone は、Citrix StorageLink と NetApp Virtual Storage Console を介して XenDesktop と統合されます。

仮想ストレージ階層化

NetApp は、I/O 需要の増加に対して仮想ストレージ階層化機能により動的に対応します。この機能により、組織は安価な市販のハード ドライブで仮想デスクトップ インフラストラクチャを導入し、従来は高価なソリッド ステート ドライブで実現されていたパフォーマンス レベルを得ることができます。VST は、重複排除に対応しており、重複排除およびハードウェア アクセラレーションによるクローニングと連携してソリューションのパフォーマンスを向上させます。VST は、モジュール方式で拡張可能であり、柔軟な設定が可能になっています。

データ保護

NetApp は、特に共有の仮想インフラストラクチャ向けに設計された、RAID-DP を提供します。RAID-DP は、RAID 10 よりも優れたデータ保護およびパフォーマンスを提供し、RAID オーバーヘッドに関して、RAID 5 よりもコストが低下します。RAID-DP では、誤ったタイプの RAID が実装される可能性が排除されるため、デスクトップのアーキテクチャの設計が簡素化されます。

仮想ストレージ コントローラ

NetApp は、仮想ストレージ アレイを vFiler 形式で提供します。vFiler では、管理者が、パフォーマンスの平準化、データセンターのメンテナンス、ハードウェアのライフ サイクル管理などを目的として、稼動中のデスクトップやユーザ環境をストレージ コントローラ間で中断させずに移行できます。仮想環境は、設定後に物理コントローラと関連付けられることはありません。vFiler では、アレイの識別情報の永続性が維持され、異なるハードウェア上で稼動するときも変化しないので、障害復旧設計も簡素化されます。

マルチプロトコルとユニファイド ファブリック アダプタ

これらのアダプタにより、さまざまなデータ セットへの接続が簡素化されます。すべての NetApp アレイは、堅牢な仮想デスクトップ展開に必要なストレージ プロトコルを FCoE から NFS、SMB2 まで多岐にわたって提供できます。

統合データ保護

NetApp アレイは、ハードウェア アクセラレーションによる迅速なスナップショット バックアップと重複排除に対応したレプリケーションの両方をサポートしています。これらの機能は、Citrix StorageLink サイト リカバリおよび Virtual Storage Console 用の NetApp バックアップ プラグインを使用して提供および統合されます。

直接接続ストレージ

直接接続ストレージでは一般に、共有ストレージ ソリューションの持つスケーラビリティや管理性が提供されないため、主としてサーバ数の限定される環境で使用されます。DAS では、各サーバのストレージは別々に管理され、各サーバ専用になります。それでも、中小企業環境（低コストで小さいストレージ設置面積が望ましい場所）では、直接接続ストレージが有用な場合があります。Cisco UCS B シリーズおよび C シリーズ サーバは、中央の共有ストレージ ソリューションを必要としない組織に対し、SAS、SATA、SSD などのさまざまな直接接続ストレージ オプションを提供します。Cisco VXI では、Cisco UCS C250 M2（合計で最大 384G をサポート）が（1）100 GB SSD X 5 と 300 GB SAS X 3 のドライブ構成および（2）300 GB SAS X 8 ドライブ構成の 2 種類の DAS 構成で検証済みです。Cisco DAS は、Atlantis ILIO アプライアンスを使用してテストされました（次のセクションを参照）。詳細については、このガイドの「パフォーマンスとキャパシティ」を参照してください。

ストレージとパフォーマンスの最適化用の Atlantis ILIO

Atlantis ILIO はストレージとパフォーマンスを最適化するソフトウェア ソリューションで、ストレージ コストの削減、IT チーム向けストレージ オプションの拡張、およびデスクトップ パフォーマンスの向上において、Desktop Virtualization（DV; デスクトップ仮想化）ソリューションとの補完的役割を果たします。Atlantis ILIO は独自かつ革新的なストレージ最適化テクノロジーであり、Microsoft Windows オペレーティング システムと設計外の共有ストレージとの連携を高度に最適化することにより、デスクトップ仮想化のスケーラビリティ特性とパフォーマンス特性を根本的に変えるものです。Atlantis ILIO は、ストレージ システム上で稼動可能な仮想デスクトップの数を増加させると同時に、デスクトップ パフォーマンスを向上させ、仮想デスクトップ イメージに必要なストレージ キャパシティを削減し、お客様がより低コストのストレージ オプションを使用できるようにします。Atlantis ILIO では、Windows オペレーティング システムで生成される IOPS のうち最大 90 % がオフロードされ、Windows NTFS プロトコル レイヤにある Atlantis ILIO 仮想アプライアンス上のソフトウェアで処理されます。これにより、お客様は HVD の導入に対応するために必要なストレージ ディスク数を低減できます。一般的な HVD 導入では、ストレージはシステムの総コストの 50 ～ 80 % を占めます。Cisco VXI アーキテクチャの一部として Atlantis ILI が導入された場合、所定のストレージ システムで稼動できるデスクトップ数は最大で 10 倍増加します。

Atlantis ILIO の検証

次の URL にある『Cisco, Citrix and Atlantis ILIO HVD Reference Architecture』（SAVBU）を参照してください。

http://www.atlantiscomputing.com/ciscocitrixatlantis

Atlantis ILIO ストレージおよびパフォーマンスの最適化テクノロジー

Atlantis ILIO は、高パフォーマンスな HVD デスクトップを安定的に導入するために必要なストレージを、2 通りの方法で削減します。Atlantis ILIO では、Windows IO トラフィックがストレージに影響を与える前に、そのトラフィックを Windows NTFS プロトコル レイヤで処理します。これにより、SAN/NAS/DAS ストレージとのインタラクションが大幅に減少するため、IO ロードの処理に必要なストレージも大きく削減されます。Atlantis ILIO は必要なストレージを大幅に（最大 90 %）削減することで、Microsoft Windows イメージがストレージに到達する前に、それらのイメージをインラインで重複排除します。Atlantis ILIO では、仮想デスクトップ イメージがストレージに到達する前に、それらのイメージに含まれている重複した情報がリアルタイムで統合されるので、仮想デスクトップは効率的にストレージを使用できます。その結果、必要なストレージ キャパシティと、Iinput/Outputs Per Second（IOPS; 1 秒あたりの入出力数）はどちらも減少します。Atlantis ILIO は、IO を仮想デスクトップと同じハイパーバイザ上でローカルに処理することで、仮想デスクトップに対する遅延と応答時間を大幅に削減します。これにより、仮想デスクトップのユーザ エクスペリエンスが向上します。

Windows NTFS プロトコル レイヤでの IO のローカル処理

Windows オペレーティング システムは、専用のローカル ドライブと連動するように設計されており、これらのドライブはストレージに頻繁にアクセスして、固有のデータの保存とは無関係のタスクを実行します。HVD 導入では、各仮想デスクトップはディスクに対して読み取りや書き込みを行うたびに、複数のスイッチを通過しなければなりません。このプロセスにより、遅延が増加し、デスクトップ パフォーマンスが低下する可能性があります。Atlantis ILIO はハイパーバイザに仮想ハード ドライブ（.VMDK または .VHD ファイル）を格納し、IO を同じハイパーバイザ上でローカルに処理することで、仮想デスクトップのハード ドライブを大幅に高速化し、最大 90 % の IOPS をストレージ システムからオフロードします。

インライン重複排除

Atlantis ILIO は、IO トランザクションがストレージ ファブリックに到達する前に、重複排除を通信線上でリアルタイムに行います。最大 90 % の IO トラフィックを除去することで、ストレージ インフラストラクチャにおける IOPS の要件も同じ割合だけ軽減されます。それと同時に、重複したデータがディスクに書き込まれないので、後処理での重複排除は不要になり、関連する IOPS とストレージ キャパシティのコスト負担は発生しません。

ストレージの選択肢の増加

Atlantis ILIO では、ストレージ キャパシティが削減され、ディスクあたりの仮想デスクトップ数が増加するだけでなく、HVD 用のストレージを、Cisco UCS ローカル ディスク（SATA、SAS、SSD）、NAS、または SAN（シスコの認定ストレージ パートナーである NetApp および EMC を含む）などの豊富なストレージ オプションから選択することができます。Atlantis ILIO を使用すると、お客様は非常に小規模な Direct Attached Storage（DAS; 直接接続ストレージ）と、Cisco UCS プラットフォーム（SATA、SAS、SSD）で使用可能なローカル ディスク オプションをオペレーティング システムとアプリケーション ベース イメージに使用しながら、共有 SAN/NAS（EMC Celera NS480、NetApp FAS3170）でユーザ データを保持することができます。Atlantis ILIO をこのハイブリッドな Cisco UCS DAS および SAN/NAS ストレージ環境で使用する場合は、基本の仮想デスクトップ イメージが低コストなローカルの SATA、SAS、または SSD ドライブに保存され、固有のユーザ データは従来の SAN/NAS ストレージに保存されるので、コスト削減幅はさらに大きくなります。

IO トラフィックの最適化：ランダムからシーケンシャル

Windows オペレーティング システムは、ディスク IO を生成するとき、データの読み込みと書き込みをディスクに対してシーケンシャルに行って全体的なシステム パフォーマンスが最大化されるようにその IO を最適化します。HVD 環境では、デスクトップのオペレーティング システムと（ローカルまたは共有ストレージ上の）物理ディスクの間に直接的な接続はありません。したがって、ディスクは他のゲスト オペレーティング システムの間で共有されるため、Microsoft Windows オペレーティング システムの独占的使用の仮定は無効になります。結果として、ハイパーバイザはシーケンシャル IO をランダム IO に変換します（IO ブレンダ効果）。ランダム IO では、ストレージとデスクトップのパフォーマンスが低下し、ストレージ キャッシュ モジュールが使用可能でもその効果は減少します。HVD では、物理サーバあたりのデスクトップ数がサーバ仮想化よりもはるかに多いため、IO ブレンダ効果がより顕著に現れます。Atlantis ILIO は、ハイパーバイザによって生成された小さいブロックのランダム IO をより大きいブロックのシーケンシャル IO に変換してストレージに送信し、ストレージ（EMC および NetApp）のパフォーマンスを向上させます。ほとんどの場合、要求されたすべてのデータはメモリからローカル配信されます。

Cisco UCS サーバを使用した Atlantis ILIO の導入オプション

Atlantis ILIO には、Atlantis ILIO On Each Server と Atlantis ILIO Top-of-Rack の 2 種類の導入オプションがあります。Cisco VXI でのテストでは、Atlantis ILIO 仮想アプライアンスを「On Each Server」式で導入するとともに、個々の仮想デスクトップにローカル DAS ストレージ（SATA、SAS、SSD）を搭載し、アプリケーションおよびオペレーティング システム ファイルの単一インスタンスを保存しました。移植性とバックアップの容易さを考慮して、ユーザ データは常に共有 SAN/NAS ストレージ システムに格納されます。Atlantis ILIO Top-of-Rack 導入モデルを含む Atlantis ILIO の導入オプションについては、以下を参照してください。

Atlantis Computing の Web ページ「Deployment Options」：
http://www.atlantiscomputing.com/products/deployment-options/

「Cisco, Citrix and Atlantis ILIO HVD Reference Architeture」（SAVBU）：
http://www.atlantiscomputing.com/ciscocitrixatlantis

『Cisco Virtualization Experience Infrastructure Configuration Guide』：
http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VXI/configuration/VXI_Config_Guide.pdf

サーバ、スイッチ、ストレージ、およびハイパーバイザの統合

図 29 に、CNA のペアが搭載されているサーバとそのサーバ内で行われる論理接続を示します。各 CNA は、サーバにファイバ チャネル ホスト バス アダプタとイーサネット NIC を提供します。vSphere ハイパーバイザがインストールされると、ファイバ チャネル HBA は仮想 HBA にマッピングされます。仮想 HBA は、リモート ストレージの接続に使用できます。Cisco Nexus 1000V シリーズは、HBA が内部の仮想イーサネット フレームワークにマッピングされないので、それらを認識しません。イーサネット インターフェイスは、Cisco Nexus 1000V 仮想スイッチにマッピングされます。Cisco Nexus 1000V シリーズは、これらをアップリンク ポートとして処理します。これらは通常、トランク ポートとして設定され、冗長性とロード バランシングを実現するために EtherChannel によって接続されます。

Cisco Nexus 1000V シリーズの内部には、複数の仮想インターフェイス（vETH）が作成されます。1 つはカーネル トラフィック（vCenter への接続）用に予約され、独立した VLAN に配置され、一意の IP アドレスが割り当てられます。さらに 1 つが、vMotion 用に予約され、同様に独立した VLAN に配置され、別の一意の IP アドレスが割り当てられます。どちらのインターフェイスも、仮想デスクトップからは認識されません。セキュリティ上の理由から、仮想デスクトップはこれらの VLAN にアクセスできません。最後にもう 1 つの予約済み vETH が、ハイパーバイザ データストアがイーサネット ベースのストレージ（NFS）によって接続される場合に作成される可能性があります。イーサネット ベースのストレージ トラフィックも、独自の VLAN に隔離される必要があります。

仮想デスクトップには、追加の VLAN が作成されます。IP アドレスは、静的に定義されるか、Dynamic Host Configuration Protocol（DHCP）で取得されます。割り当てられるアドレスとサブネット マスクは、仮想デスクトップ プールのサイズに従って作成される必要があります。仮想デスクトップは、同じプール（サブネット、VLAN など）内でのみ移行できます。各仮想デスクトップには、単一の NIC しか作成する必要はありません。異なるプールの仮想デスクトップを同じ物理サーバ上で稼動させることができます。トランク ポートの設定には、許可された仮想デスクトップのものも含め、考えられるすべての VLAN を含める必要があります。Cisco Nexus 1000V シリーズは、2 つの CNA（NIC）インターフェイスにわたって EtherChannel を作成します。そのため、各インターフェイスに対する負荷を監視して、適切なロード バランシング アルゴリズムが選択されていることを確認する必要があります。

Cisco Integrated Management Controller は、内部で UCS 6100 ファブリック インターコネクトに転送されます。Cisco UCS Manager は、そのインターフェイスの割り当てと管理を行います。Cisco Integrated Management Controller に割り当てられる IP アドレスは、UCS Manager と同じサブネット上になければなりません。これは、リモートの KVM とサーバのメンテナンスに使用されるアドレスです。

VMware vKernel インターフェイスは、vCenter との通信に使用されます。この IP アドレスは、Cisco Integrated Management Controller インターフェイスとは別の VLAN に割り当てる必要があります。この VLAN は、vCenter サーバの VLAN にルーティング可能である必要があります。

vMotion インターフェイスは、仮想デスクトップのモビリティを実現するために使用されます。このインターフェイスは、同じ仮想デスクトップ プール内のすべてのサーバと共通の独立した VLAN に割り当てることも必要です。vMotion はルーティング可能なプロトコルではないので、このネットワークはアクセス レイヤの外にまで広がる必要はありません。vCenter は、仮想デスクトップを移行するために必要なトラフィック フロー用に、サーバ上の vMotion インターフェイス（および関連する VLAN）を使用します。仮想デスクトップのストレージはリモートで維持されているため、デスクトップの RAM の内容（CPU の状態）のみが送信されます。

図 29　　Cisco VXI データセンター接続

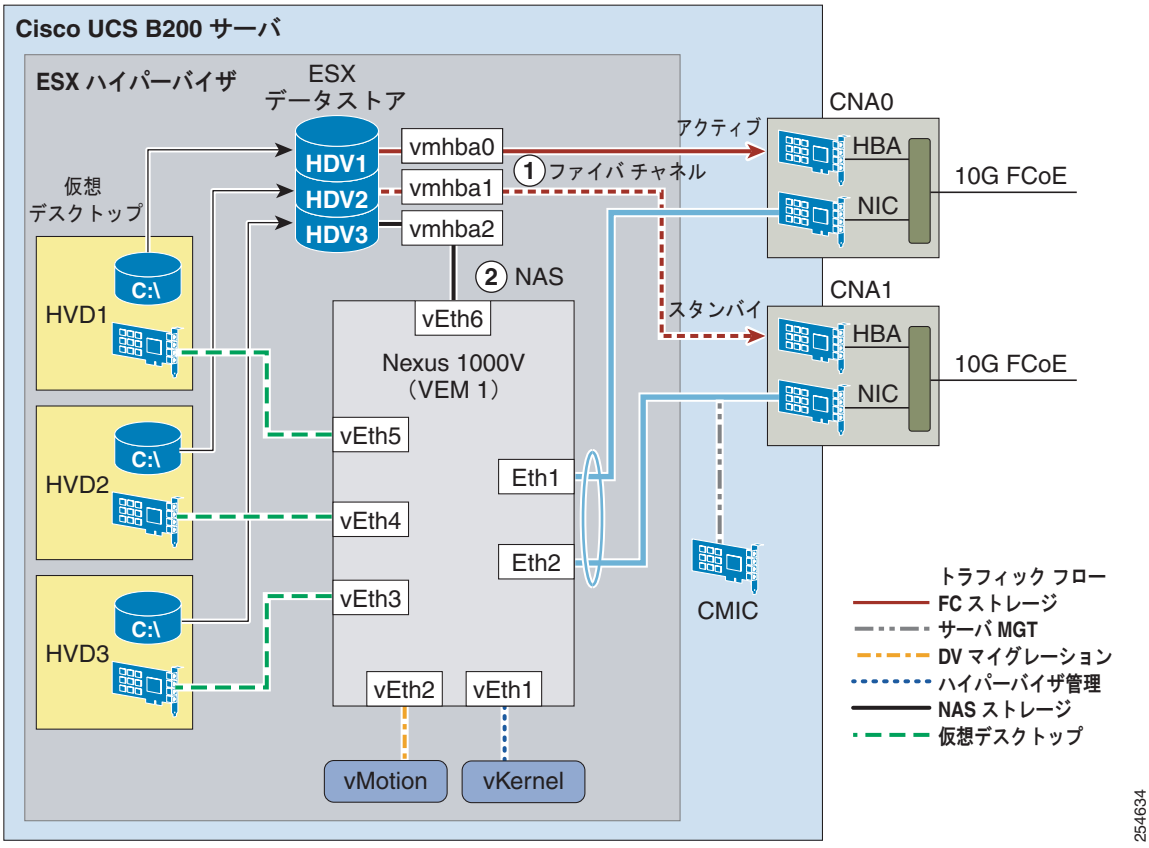


表 4　　Cisco VXI の導入に必要な VLAN のリスト

名前	デバイス	用途	説明
データセンター			
Cisco UCS Manager	Cisco UCS ブレード サーバ シャーシ、ファブリック インターコネクト、およびブレード サーバ統合管理コントローラ	すべての Cisco UCS コンポーネントのアウトオブバンド管理	この VLAN は、他の管理 VLAN と共有される場合があります。
vMgmt	ハイパーバイザ	すべてのハイパーバイザの管理	この VLAN は、特定の DV プールに固有のものです。したがって、プールごとに複数の独立した VLAN が存在する可能性があります。
vMigration	ハイパーバイザ	DV プール内での DV VM マイグレーション	vMgmt の場合と同様に、プールごとに複数の独立した VLAN が存在する可能性があります。

名前	デバイス	用途	説明
N1KControl と N1KData	Cisco Nexus 1000V シリーズ VEM および VSM	Cisco Nexus 1000V シリーズの管理	• 分散スイッチ機能を提供するすべての物理サーバに共通 • データセンター内に複数の Nexus 1000V がインストールされている可能性あり
VMData	DV 仮想マシン	ユーザのネットワーク アクセス DV ディスプレイ プロトコル	DV マシンは 1 つのインターフェイスのみが必要です。 DV プールごとに 1 つの VLAN。
VMStorage	ハイパーバイザ	ストレージ トラフィックの隔離	ファイバ チャネルまたは IP ベースのストレージ用
エンドポイント ロケーション			
データ *	DV エンドポイント	DV 仮想マシンへの接続	DV データ VLAN は、レガシー コンピューティング エンドポイント VLAN から分離される場合があります。
音声 **	ユニファイド コミュニケーションのエンドポイント	ユニファイド コミュニケーションのアクセスの提供	従来の音声 VLAN

（注） * これらの VLAN は、Cisco Nexus 1000V シリーズを導入した場合にのみ使用されます。

（注） ** エンドポイントのデータおよび音声の VLAN については、「ネットワーク」の章で説明されています。

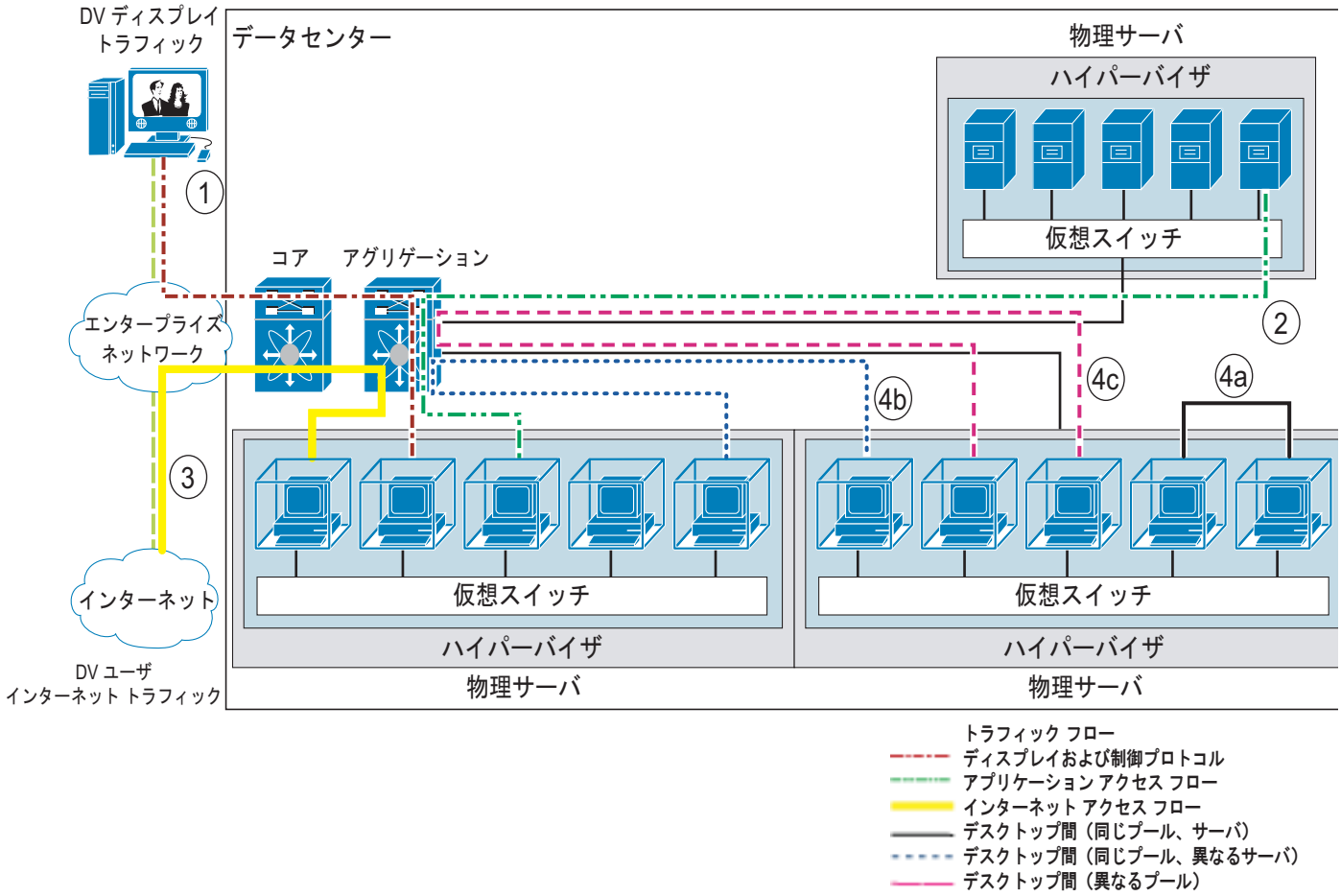
仮想デスクトップでは、図 30 に示されているように、次のトラフィック フローがあります。

1. ディスプレイ プロトコルと制御プロトコル。仮想デスクトップを送信元とし、リモート エンドポイントで終端されます。
2. データセンター内に存在するアプリケーションへのアクセスに関連したフロー。アグリゲーション レイヤ内のルータまたはファイアウォールに到達するまで L2 セグメント上を移動した後、アプリケーションを内包した別の L2 セグメントにルーティングされます。
3. インターネット アクセス フロー。仮想デスクトップを送信元としてデータセンター ネットワーク スタックを上に移動し、エンタープライズ ネットワーク内へと移り、インターネット ルータ経由で社内ネットワークの外に出ます。途中で複数のファイアウォールを経由する場合があります。
4. 仮想デスクトップ間の直接的なトラフィック（まれ）。
   a. 同じプール内で同じ物理サーバ上にあるデスクトップ間でフローが発生すると、トラフィックはそのサーバの外に出ることはありません。これを防ぐ必要がある場合、管理者はプライベート VLAN を設定できます。

b. 同じサーバ上ではないが、同じプール内にあるデスクトップ間でフローが発生すると、トラフィックはアグリゲーション レイヤ スイッチまで移動し、そこで折り返して相手の仮想デスクトップを収容しているサーバまで移動します。

c. サーバ プールではないデスクトップ間でフローが発生すると、トラフィックはネットワーク スタックを昇ってアグリゲーション レイヤにまで流れ、相手のサブネットにルーティングされ、相手の仮想デスクトップを収容しているサーバに転送されます。

図 30　　仮想および物理のトラフィック フロー



関連情報

表 5 に、この章で説明したハードウェアおよびソフトウェアを含む特定のベンダーに関する詳細情報へのリンクを示します。

表 5　　データセンター リンク

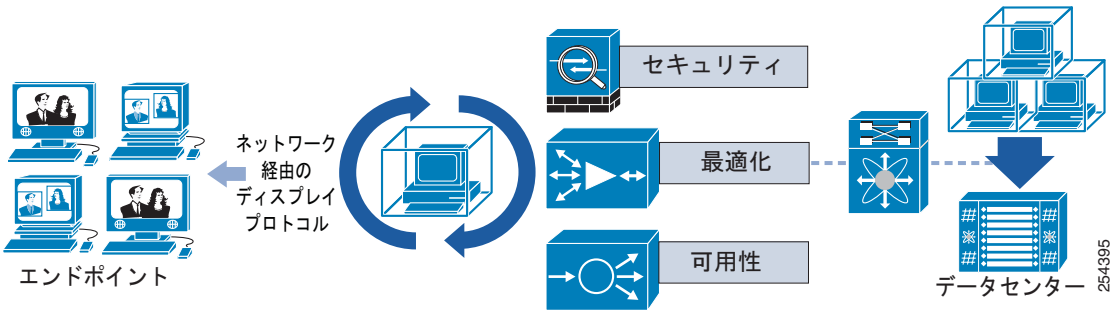
シスコのデータセンターのデザイン ゾーン
http://www.cisco.com/en/US/netsol/ns743/networking_solutions_program_home.html
『Best Practices in Deploying Cisco Nexus 1000V Series Switches on Cisco UCS B Series Blade Servers』
http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9902/white_paper_c11-558242.html
『Reference Architecture–Based Design for Implementation of Citrix XenDesktop on Cisco Unified Computing System, Citrix XenServer, and NetApp Storage』（DC の Citrix バージョン）
http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/Virtualization/ucs_xd_xenserver_ntap.pdf
『Atlantis ILIO for VDI』
http://www.atlantiscomputing.com/downloads/VDIStorage_SolBrief_020411.pdf
『EMC FAST VP for Unified Storage』
http://www.emc.com/collateral/software/white-papers/h8058-fast-vp-unified-storage-wp.pdf
『EMC Clariion, and VNX Fast Cache』
http://www.emc.com/collateral/software/white-papers/h8046-clariion-celerra-unified-fast-cache-wp.pdf
『EMC VNX Deduplication and Compression』
http://www.emc.com/collateral/hardware/white-papers/h8198-vnx-deduplication-compression-wp.pdf
『EMC Infrastructure for Virtual Desktops』
http://www.emc.com/collateral/software/technical-documentation/h8059-virtual-desktops-celerra-vmware-citrix-psg.pdf
NetApp TR-3298：『RAID-DP: NetApp Implementation of RAID Double Parity for Data Protection』
http://media.netapp.com/documents/tr-3298.pdf
NetApp TR-3347：『FlexClone Volumes: A Thorough Introduction』
http://media.netapp.com/documents/tr-3347.pdf
NetApp TR-3437：『Storage Best Practices and Resiliency Guide』
http://media.netapp.com/documents/tr-3437.pdf
NetApp TR-3505：『NetApp Deduplication for FAS, Deployment and Implementation Guide』
http://media.netapp.com/documents/tr-3505.pdf
NetApp TR-3563：『NetApp Thin Provisioning』
http://media.netapp.com/documents/tr-3563.pdf

VXI ネットワーク

VXI ネットワークについて

Cisco VXI システムのネットワーク設計は、キャンパス、WAN、およびデータセンター ネットワーク インフラストラクチャの導入に関するシスコのベスト プラクティスの上に構築されています。しかし、VXI ネットワーク設計では、ユーザがネットワーク内のどこにいるかに関係なく、より優れたユーザ エクスペリエンスを実現するために、仮想デスクトップ ディスプレイ プロトコル、UC、および周辺機器のトラフィック周りについて特に考慮する必要があります。この章では、これらのネットワークに関する考慮事項について説明します。下の図に示されているように、ネットワーク経由で配信されるディスプレイ プロトコル トラフィックには、最適化と保護が必要です。さらに、データセンター内の仮想デスクトップおよびその他のアプリケーションのハイ アベイラビリティをネットワークで提供する必要性も高まっています。特に現在では企業のあらゆる生産性がネットワークに依存するようになっているのでその傾向が強まっています。VXI システムは、仮想デスクトップ トラフィックに関する QoS のガイドラインと機能を提供することでネットワークを最適化します。また、ブランチやモバイルのアクセス シナリオに対して WAN 経由のトラフィックも最適化します。可用性は、IT 部門のビジネス目標と測定結果に基づいて定義できます。可用性の種類には、デバイス、メディア インターフェイス、およびパスの可用性、およびユーザとアプリケーションに対するネットワークの可用性があります。VXI システム内の可用性は、ダウンタイム中やアップグレード中もネットワーク パスを使用できるようにするシスコのネットワーク ベスト プラクティスを利用し、データセンター内の仮想デスクトップ サービスの健全性と可用性を保証することで実現されます。ネットワーク セキュリティについては、このガイドの「VXI セキュリティ」の章で詳しく説明します。

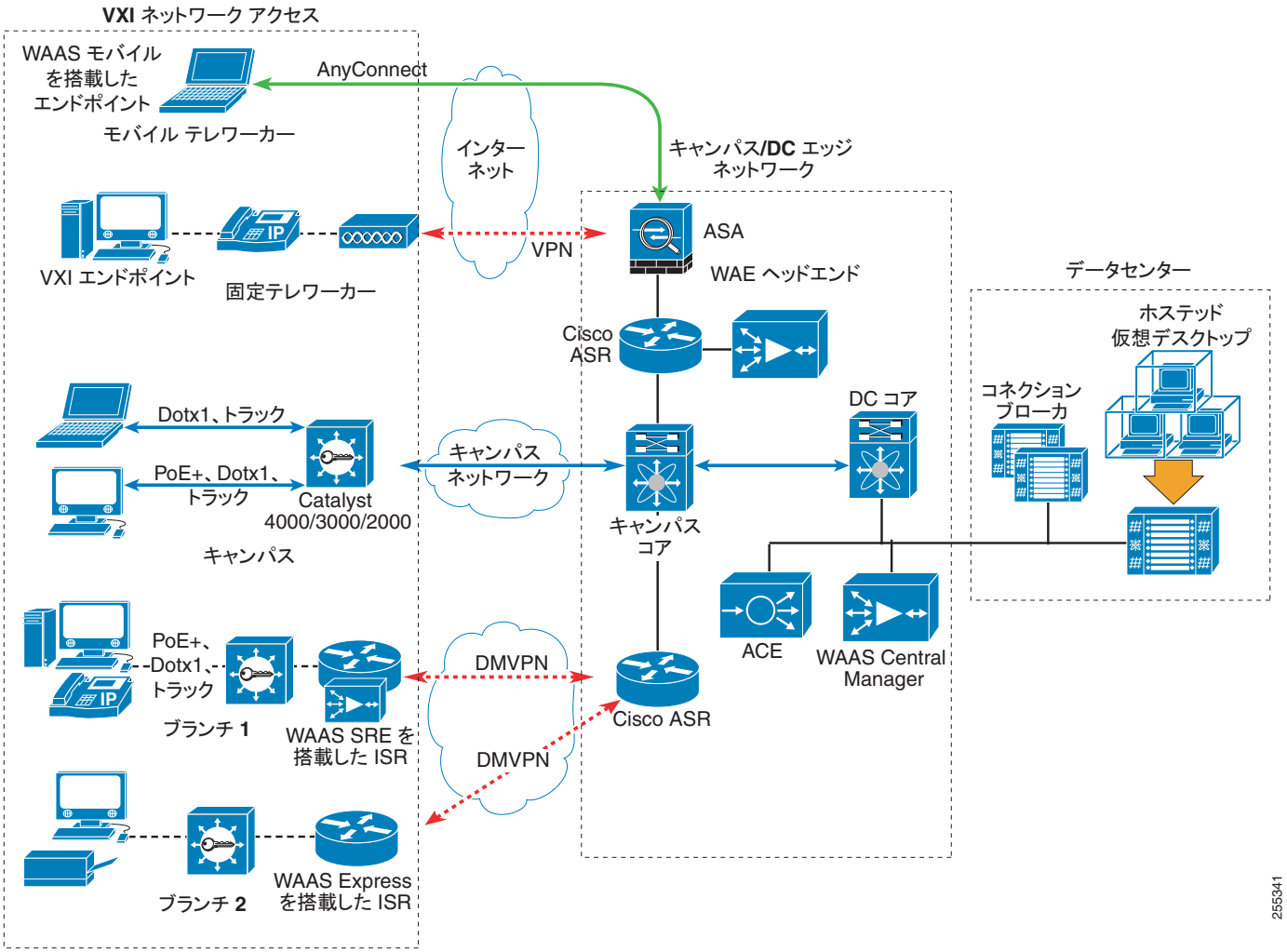
図 31　　DV ネットワークの機能フロー



VXI ネットワーク コンポーネント

下の図に、VXI の導入の 3 つの使用例を示します。仮想デスクトップ ユーザは、本社キャンパス内または小 / 中 / 大規模ブランチ内にいることも、固定またはモバイル テレワーカーになることもできます。ユーザはどこにいても、ネットワークから同じ体験を得られます。この図には、VXI 管理者が優れたユーザ エクスペリエンスを実現するために重点的に取り組まなければならないすべてのコンポーネントとネットワーク エリアも示されています。この章の残りでは、上記のシナリオの VXI 設計要件と各ロケーションでネットワークに必要なコンポーネントについて説明します。

図 32　　VXI ネットワークを実現するための主要コンポーネント



キャンパス

キャンパス ネットワークは、社内ネットワーク内のエンド ユーザとデバイスをデータセンター、WAN、およびインターネットと接続します。キャンパス ネットワークは、信頼できるエンタープライズ ネットワーク経由でのエンド ホストへのアクセスも提供します。この Cisco VXI のリリースでは、すべてのエンドポイント サービスがファースト ホップ スイッチで提供されるので、このスイッチにエンドポイントを接続するための設計のベスト プラクティスについて説明します。キャンパス ネットワークの残り部分（ファースト ホップ スイッチからデータセンター エッジに至るまでのすべて）は、シスコのエンタープライズ キャンパス 3.0 アーキテクチャを使用して導入することが推奨されます。それにより、優れた VXI ユーザ エクスペリエンスの実現に必要な高スループット、低遅延、常に利用可能な接続が提供されます。高速な接続に加え、VXI キャンパス ネットワークは、エンド ユーザおよびデバイスと直接連携して、Power over Ethernet（PoE）、IEEE 802.1x を使用したセキュアなアクセス コントロール、VXI エンドポイントを適切な QoS ポリシーとセキュリティ ポリシーで正しい VLAN に導くインテリジェントで動的なプロビジョニング、VXI エンドポイントのロケーション トラッキングの支援、トラフィックのモニタリングと管理など、豊富なサービスを提供する必要があります。上記のサービスを実現するために、キャンパス内の VXI エンドポイントは、Catalyst 4000、3000、2000 などのワイヤリング クローゼット スイッチに接続される必要があります。

エンドポイントへの電力供給

現在の Power over Ethernet テクノロジーは、ハイ アベイラビリティで高効率の管理しやすい電源を提供できることから、IP テレフォニーと最も関連付けられています。電源のハイ アベイラビリティは、E911 タイプのアプリケーションに不可欠であり、そのため PoE 経由で IP 電話に給電する多くの企業で必須になっています。PoE+ と Universal Power Over Ethernet（UPoE）対応 Cisco VXI クライアントの導入によって、企業は従業員の作業環境全体を単一の電源に移行できるようになり、配線コストとエネルギー コストの大幅な削減も見込めます。今 Cisco VXI PoE に移行しておくと、企業は将来的に Cisco EnergyWise Orchestrator や Cisco Prime LMS 4.0 などの高度な職場向け電力ポリシー アプリケーションを使用できるようになります。これらのアプリケーションの詳細については、このガイドの「管理と運用」の章を参照してください。PoE+（IEEE 802.3at、30W）のスケーラビリティを備え、PoE+ テクノロジーを 30W を超えて拡張する豊富なロードマップがあることから、Cisco VXI 用のキャンパス アクセス プラットフォームとして Cisco Catalyst 4500E、Catalyst 2000S、および Catalyst 3000-X が推奨されます。単一のケーブルですべてのデバイスにデータと電力を供給することを目指した Cisco VXI 導入には、UPoE を使用することを強く推奨します。このテクノロジーは、デバイスあたり最大 60W を供給することができます。Cisco UPOE は、業界内で飛躍的に進化したテクノロジーであり、スイッチ ポートあたり 60W の PoE を提供して、次世代の職場環境で新しい導入オプションの使用を可能にします。現在、Catalyst 4500E スイッチ上で利用できます（WS-X4748-UPOE+E ライン カード）。同時に 240 の PoE+ ポートをサポートする Catalyst 4500E は大企業に適しており、スタック サポート付きの Catalyst 3000-X と Catalyst 2000-S シリーズは中小企業向きです。

自動ポート プロビジョニング

Auto SmartPorts では、CDP によって取得されたデバイス識別情報または MAC アドレスに基づいてポートが自動的に設定されることにより、スイッチが VXI クライアントを動的にプロビジョニングできるようになります。Smartport マクロは、管理者が一般的なスイッチ ポート設定を簡単に設定できるように、シスコのベスト プラクティスに基づいて事前に作成されたカスタマイズ可能な設定スクリプトです。Auto Smartports 機能は、ネットワーク内でセキュリティ、QoS、および可用性に使用されるポリシーの一貫性を維持するのに役立ちます。

Auto Smartports では、エンドポイントのクレデンシャルに基づいてスイッチがマクロを自動的に適用します。エンドポイントへのリンクがドロップされるか、ユーザ セッションが終了されると、設定は削除されます。たとえば、スイッチによって Cisco IP Phone がポート上で検出された場合、音声 VLAN とポート セキュリティを設定し、QoS ポリシーをセットアップする IP 電話マクロが適用されます。これと同レベルの自動化を VXI エンドポイントに対して実現できます。現在のリリースでは、このプロセスは手動のみであり（静的マクロと呼ぶ）、VXI エンドポイントの自動検出のサポートは、将来のリリースで追加される予定です。自動マクロ展開には、VXI エンドポイントが自身をスイッチに識別させることが必要です。CDP を使用してこれを行う Cisco IP Phone とは異なり、現在の VXI エンドポイントでは、そのような自己識別機能はサポートされていません。VXI システムでは、Cisco IP Phone を検出するために AutoSmartPorts 機能を有効にし、VXI エンドポイントに対して静的マクロベースのマクロを作成することを推奨します。VXI システム内での自動/静的マクロの導入ガイダンスについては、次のセクションで説明します。Cisco Catalyst 4000E および Catalyst 3000-X スイッチ プラットフォームでは、両方のタイプのマクロがサポートされています。

QoS

ディスプレイ トラフィックは、ベンダー独自のプロトコルでカプセル化されます。これらのプロトコルは、パス上のネットワーク要素が解読できない非標準のプロトコルです。そのため、これらのプロトコルはネットワークに対して不透明になり、ネットワークで VXI に提供可能な重要な付加価値サービスが制限されることになります。ディスプレイ プロトコルはネットワークに対して不透明ですが、それでもある程度のレイヤ 3 レベルの QoS サービスはこのトラフィックに対して集合的に適用できます。さらに、音声トラフィックは Cisco VXI によってディスプレイ プロトコルの外に出されるので、音声トラフィックに対する QoS が、VXI システムで優れたユーザ エクスペリエンスを実現するために必要となります。エンドツーエンド VXI QoS のガイドラインの詳細については、このガイドの「Quality of Service」の章を参照してください。

エンドポイント アクセスの保護

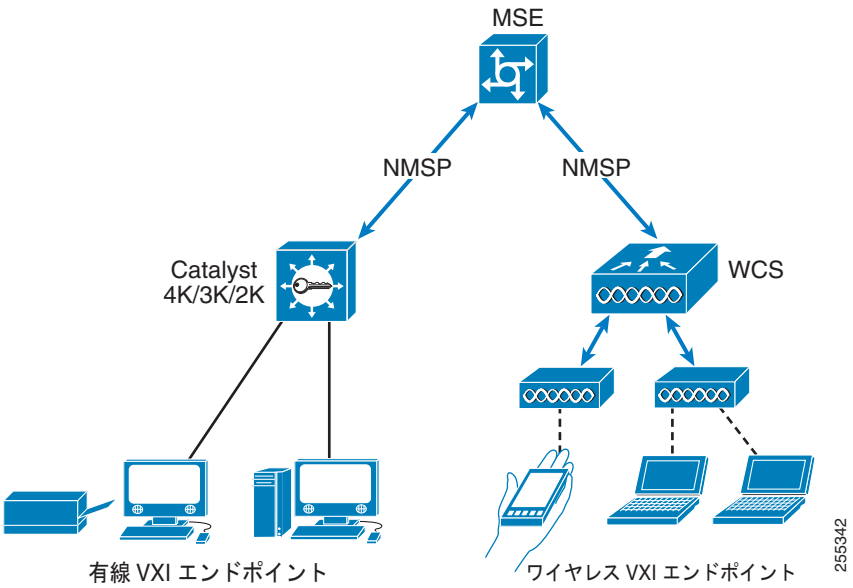
ディスプレイ プロトコルはキャンパスに対して不透明になる可能性がありますが、それでも Cisco Catalyst® ファミリのスイッチは Cisco VXI システムに対応したネットワーク内でセキュリティ機能と可用性機能を提供できます。こうした機能により、一部の DV トラフィック タイプは、ログイン特性に基づいて特徴付け、保護することが可能になります。たとえば、請負業者が自分のラップトップを使用でき、シン クライアントを使用して自分の仮想デスクトップにアクセスするとします。請負業者がネットワークに接続するとき、その請負業者はラップトップのユーザ名とパスワードを使用してログインし、802.1X を使用して認証されます。Catalyst スイッチは、VPN トラフィック用のインターネットへのアクセスと請負業者のデスクトップのみへの接続を可能にする ACL で、そのユーザを個別の請負業者 VPN にマッピングできます。Cisco Catalyst 4500 E および Catalyst 3000-X スイッチは、802.1X 機能とポート セキュリティ機能を提供してエンドポイント レベルのセキュリティを実現します。これらのセキュリティ中心の機能に関する導入および設計の詳細については、このガイドの「Cisco VXI セキュリティ」の章で説明します。

ロケーション：エンドポイント トラッキング

Network Mobility Services Protocol（NMSP; ネットワーク モビリティ サービス プロトコル）により、ネットワーク内でのホストの物理的な位置を特定できます。これにより、コンプライアンスとインベントリのために資産を追跡することができます。

アクセス スイッチ（Catalyst 4500E や Catalyst 3000-X など）は、有線のロケーション サービス機能を提供し、接続されているエンドポイントのロケーション情報を Cisco Mobility Services Engine（MSE）に送信します。Cisco MSE は、集中管理されたスケーラブルな方法で有線およびワイヤレス ネットワーク全体にモビリティ サービスを提供する、アプライアンスベースのプラットフォームです。ワイヤレス接続の場合、Access Point（AP; アクセス ポイント）が自身に接続された VXI エンドポイントのロケーション情報を追跡し、Wireless Control System（WCS）経由で MSE に送信します。WCS は、ロケーション サービス用の管理プラットフォームです。デバイスを追跡し、イベント通知のセットアップを許可し、ロケーション トリガーに基づいてアラームを発信します。スイッチと AP の実際のロケーション情報およびスイッチ上のポートは、そのスイッチと AP 自体で設定されます。

図 33　　VXI のロケーション トラッキング トポロジ



MAC アドレス、IP アドレス、シリアル番号、UDI、モデル番号などのデバイス情報は、スイッチまたは AP によって取得できます。スイッチは、接続されている VXI エンドポイントの情報を CDP/LLDP-Med または ARP スヌーピングによって学習します。AP は、前述の情報を標準的な WiFi 登録交換によって学習します。現在の VXI エンドポイントは、CDP/LLDP-Med をサポートしていません。したがって、有線スイッチ上のエンドポイントの IP アドレスと MAC アドレスおよびワイヤレス AP 上の WiFi エンドポイントの登録シーケンスを学習するために、ARP スヌーピングのみが使用されます。スイッチと AP は、デバイス カテゴリ（有線/ワイヤレス）、接続時間、動作状態（接続/切断）などの状態情報も送信します。MSE は、ロケーション データベースを保持しています。またこのリリースでは、手動でメンテナンスされる、各エンタープライズ クライアントに関連付けられた MAC アドレスのリストも保持しています。デバイス ロケーションがユーザにマッピングされる必要がある場合、別の手動でメンテナンスされる、ユーザと MAC ID のマッピング データベースが維持される必要があります。Cisco スイッチと Cisco アクセス ポイントは、すべてのモデルでロケーション サービスをネイティブ サポートしており、VXI 内で使用できます。ただし、Cisco VXI の一部として検証済みなのは、Catalyst 4500E と Catalyst 3000-X だけです。スイッチ、AP、および WCS の機能の設定方法の詳細については、「導入モデル」のセクションを参照してください。

キャンパス アクセスの可用性

VXI システム内の業務アプリケーションはすべてデータセンター内で集中管理されているため、エンド ユーザは、日常的な基本作業を行うときでさえもネットワークに完全に依存します。VXI システムでは、接続ポイント（アクセス スイッチ）から先の基盤となるネットワークが常に利用可能な状態である必要があります。わずかなダウンタイムであっても、生産性が大幅に低下する可能性があります。主要な設計要件の 1 つとして、VXI トラフィックを伝送するすべてのネットワーク コンポーネントは、機器の障害やアップグレードとダウングレード プロセスに備えて高い冗長性と可用性が必要です。

デュアル スーパーバイザによる冗長構成の Cisco Catalyst 4500E では、In-Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）機能を使用して、パケット転送を続けながら Cisco IOS ソフトウェアをアップグレードまたは修正できます。これにより、ネットワークの可用性が高まり、計画されたソフトウェア アップグレードにより生じるダウンタイムが短縮されます。ISSU 機能は、計画されたアップグレードまたは修正時に中断のないユーザ エクスペリエンスを実現できます。Supervisor 7E による ISSU プロセスは、1 行のコマンド ラインで済むようになり、トラフィック ヒットは 10 ミリ秒未満になります。ISSU プロセスの間、Power over Ethernet（PoE）とデータ プレーンにおける VXI セッションは稼動状態のままです。

ブランチ内での Cisco VXI

この Cisco VXI のリリースでは、ブランチ ネットワーク機能を VXI トラフィックに対応させることに重点を置いています。WAN には多数の課題が存在するため、企業はブランチにおいて VXI の利点を得ることができます。

Cisco VXI 内でのダイナミック VPN

ブランチからキャンパスへの WAN 接続は、多くの場合、信頼できない WAN リンクを経由する可能性があります。さらに、マルチブランチ環境内で発信されているトラフィックには、エンタープライズ ネットワーク内の別のブランチを宛先としているものが存在する可能性があります。あるブランチにいるユーザが別のブランチにいるユーザにコールするときの Cisco IP Phone トラフィックはその一例です。通常、この例での音声トラフィックは、キャンパスに転送されてから相手のブランチにルーティングされます。企業の観点からすると、これは、帯域幅コストを増加させる可能性があり、さらに重要なこととして、WAN に追加の遅延が発生することによりユーザ エクスペリエンスが悪化する可能性があります。上記の問題を踏まえ、トラフィックの宛先に基づいて暗号化トンネルを動的に作成および切断できるソリューションが必要になります。DMVPN は、パフォーマンス、スケール、アプリケーション サポート、および導入の容易さの最適な組み合わせを提供することで、このニーズを満たします。Cisco VXI システムでは、仮想デスクトップ ディスプレイ トラフィックは、ほとんどの場合、ブランチからデータセンターまでになります。また、コラボレーション トラフィックはブランチ間のピア ツーピアになる可能性があります。DMVPN では、セキュリティと最適なルート選択の両方の要件が満たされるので、その使用が推奨されます。

DMVPN ルータは、EIGRP などのダイナミック ルーティング プロトコルの使用を含め、IP ユニキャスト、IP マルチキャスト、およびブロードキャスト トラフィックをサポートする GRE ベースのトンネル インターフェイスを使用します。初期のスポークツーハブ（ブランチからキャンパス）トンネルがアクティブになった後、動的なスポーク間（ブランチ間）トンネルがトラフィック フロー要件に応じて作成されます。DMVPN は、Next Hop Resolution Protocol（NHRP）を使用して、フロー内の宛先 IP のプレフィクスに基づいて他のスポークを探します。スポーク間（ブランチ間）トンネルは、IPSec を使用して暗号化されます。過去にトラフィック フローによってブランチ間に作成された接続は、アイドル状態になるとタイムアウトされます。Internet Security Association and Key Management Protocol（ISAKMP）は、DMVPN で高速の再コンバージェンスを実現するために必要です。ISAKMP を使用したアクティブな Dead Peer Detection（DPD）がなければ、未使用のトンネルまたは孤立したトンネル（ピアのリロードの際に発生）は、タイムアウトまでに最長で 60 分の猶予があります。Network Address Translation（NAT; ネットワーク アドレス変換）を実装して DMVPN ハブがファイアウォールの内側にある場合、IPSec トンネリングも必要です。トンネルは物理インターフェイスの内側で作成されるので、DMVPN 用に設定されたブランチ ルータは、サービス プロバイダーから提供される DHCP アドレスを使用できます。ただし、初期のスポークツーハブ トンネルですべてのブランチ ルータが作成できるように、DMVPN ハブにはスタティック IP アドレスを設定する必要があります。

この章で後に説明するように、優れた Cisco VXI ユーザ エクスペリエンスを実現するには、WAN 最適化コンポーネントの使用が強く推奨されます。DMVPN と一緒に WAN 最適化を導入することは問題ありませんが、いくつかの設定に関するベスト プラクティスに従う必要があります。これらについても、この章で後に説明します。DMVPN および Cisco WAN の導入全般に関する有益な情報が下記のリンクにあります。このマニュアルの内容をよく理解してから、WAN 上での VXI の実装を始めることを推奨します。

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns982/c07-610746-02_wanDeploy.pdf

その他の Cisco DMVPN 固有の重要なリソースはすべて http://www.cisco.com/en/US/products/ps6658/index.html にあります。

VXI トラフィック向けの WAN 最適化

インタラクティブ マルチメディア（音声やビデオなど）の配信は、デスクトップ仮想化の導入における最大の課題の 1 つです。ディスプレイ プロトコルは、インタラクティブ マルチメディアの配信について最適化されません（特に WAN 環境において）。したがって、デスクトップとアプリケーションの仮想化をブランチ オフィスやテレワーカーにまで広げる際に課題が発生します。ブランチ オフィスへのホステッド仮想デスクトップの配信に伴う主要な課題は、期待されるエンドユーザ エクスペリエンスに見合う十分なパフォーマンス レベルを WAN 上で確保することです。ホステッド仮想デスクトップを WAN 経由で配信する場合、エンドユーザ トラフィックは、次の特性に対処する必要があります。

- 限られた WAN 帯域幅：ブランチ オフィスをデータセンターに接続する際の帯域幅はまだ高価です。ブランチ オフィス内のエンドユーザとアプリケーションが増加すると、帯域幅の使用が促進され、需要が高まり続けます。
- 遅延：ブランチ オフィスとデータセンターの間では、伝搬遅延が WAN 上の遅延の主な原因です。遅延は、WAN 上のすべての TCP ベースのデータ転送に影響しますが、最も影響を受けるのは、通信の多いプロトコルを使用するエンドユーザです。さらに、リアル タイム メディア トラフィックと仮想デスクトップ トラフィックは遅延の影響を非常に受けやすく、一定のしきい値を超える遅延はユーザ エクスペリエンスを悪化させ、サービス拒否さえも引き起こす可能性があります。
- パケット損失：WAN 内の輻輳によりパケットがドロップされた場合、TCP はウィンドウ サイズを小さくし、パケットを再送信します。これにより、帯域幅の効率が低下し、アプリケーションの応答時間が長くなります。パケット損失は、WAN を経由する TCP ベースのデータ転送にも影響します。DV 環境では、WAN 上でのパケット損失によって、エンドユーザ エクスペリエンスが悪影響を受ける可能性があります。

さらに、ブランチ オフィスには、最小規模のオフィスにさえもプリンタが設置されています。ほとんどのブランチ オフィスにはプリント サーバがあり、ベンダーから提供された組み込みのプリント サーバを使用しています。組み込みも含めプリント サーバが 1 台もないブランチ オフィスでは、ドキュメントをリモート オフィスで印刷しなければならないとき、レンダリング済みのドキュメントの印刷ジョブが WAN 経由でデータセンターからユーザのローカル プリンタにスプールされます。印刷トラフィックは、通信が非常に多く、ネイティブで圧縮されていなければ大量の帯域幅を消費します。このようなトラフィック タイプは、すでに量の限られている帯域幅リソースをめぐって優先度の高いリアルタイム トラフィックと競合します。VXI ブランチとテレワーカー展開には、DV トラフィック、リアルタイム トラフィック、およびその他の非優先の周辺機器トラフィックを処理可能な WAN 最適化ソリューションが必要です。

ブランチ オフィスの Cisco WAAS 展開は、データセンターの Cisco WAAS 展開と連携して、インテリジェント キャッシング、圧縮、およびプロトコル最適化を利用した WAN 最適化サービスを提供します。エンド ユーザがコネクション ブローカ経由で仮想デスクトップにアクセスした場合、Cisco WAAS は、その応答を圧縮してから、WAN 経由で高速かつ最小限の帯域幅使用量で効率よく転送します。よく使用される情報は、ブランチ オフィスとデータセンターの両方の Cisco WAAS ソリューションでキャッシュされます。それにより、サーバと WAN に対する負荷が大幅に軽減されます。

Cisco WAAS は、印刷に特化した最適化を使用して大幅な印刷パフォーマンスの向上と WAN データの削減を可能にするプリント サーバによる集中管理されたネットワーク印刷など、多様な印刷戦略をサポートするための全体的なアプローチを提供します。Cisco WAAS は、Microsoft Windows 印刷サービスを稼動することにより、ブランチ オフィス ユーザに対してローカルにプリント サーバを提供します。Cisco WAAS は、USB リダイレクトと連携して、帯域利用率を削減し、WAN 遅延を軽減することで、ブランチのクライアント デバイスにおいてローカルに接続された周辺機器（USB 接続のプリンタなど）にリダイレクトされる印刷トラフィックの最適化を提供します。既存のブランチ WAN 接続上に WAAS を導入すると、帯域幅の回収にも役立ちます。WAN 最適化は、単に VXI 向けの要件でしかないと考えるべきではありません。ほとんどの実用的な VXI の導入は、既存のブランチ ネットワーク インフラストラクチャ上でなされます。そこに WAAS を導入することにより、VXI と非 VXI の両方のトラフィックが最適化され、WAN 上の帯域幅が回収されるようになります。これにより、追加の帯域幅の購入費用が節約される可能性があります。

ネットワーク アプライアンスはプロトコルを理解し、ユーザの要求を終端することができるため、プロトコル最適化が可能です。プロトコル オプティマイザは、サーバに対して独立した接続を開設します。Cisco VXI システムで使用されるネットワーク プロトコルには、暗号化と圧縮の方式を適用するものがあります。プロトコル オプティマイザがユーザの要求を終端し、最適化できるようになるには、ネットワーク アプライアンスが、暗号化または圧縮の方式を理解する必要があります。

Cisco WAAS は、次に一覧されているテクノロジー スイートを使用して、すべての WAN 最適化機能を実現します。

- Data Redundancy Elimination（DRE; データ冗長性の排除）および Lempel-Ziv（LZ）圧縮を利用した高度な圧縮で、WAN を通過する冗長パケットを大幅に削減または排除します。WAN 帯域幅を節約し、関連するコストを削減するとともに、アプリケーションのトランザクション パフォーマンスを向上させ、同じアプリケーションで繰り返される大量転送の時間を大幅に短縮します。DRE では、アプリケーション、データ、および作業負荷に応じて 2:1 から 100:1 までの圧縮が可能です。永続的な LZ 圧縮（DRE とは別に、あるいは組み合わせて使用可能）では、使用されるアプリケーションと送信されるデータに応じて 2:1 から 5:1 までの圧縮が可能です。この圧縮は、DRE で行われた圧縮に対して追加的に行われます。
- Transport Flow Optimization（TFO; トランスポート フロー最適化）。WAN 環境内のクライアントとサーバのスループットと信頼性を向上させ、パケット損失が発生した場合に最大限のスループットを確保します。TFO では、プロトコル トラフィックが暗号化され、圧縮されていても、TCP ベースのディスプレイ プロトコルを最適化できます。
- Common Internet File System（CIFS）、Network File System（NFS）、HTTP、Secure Sockets Layer（SSL）、Messaging Application Programming Interface（MAPI）、ビデオ Real Time Streaming Protocol（RTSP; リアルタイム ストリーミング プロトコル）などのアプリケーションに特化したアクセラレータ。Cisco WAAS は、これらの通信の多い幅広い種類のアプリケーション プロトコルのパフォーマンスを向上させ、その動作を加速させます。それにより、WAN 経由でのこれらすべてのアプリケーション プロトコルの分散ユーザ アクセスを向上させ、使用可能な帯域幅にデスクトップ仮想化とリッチ メディア トラフィックのためのスペースをさらに確保します。

Independent Computing Architecture（ICA）や Remote Desktop Protocol（RDP）などのデスクトップ仮想化プロトコルの最適化は、DRE、LZ、および TFO の技術を適用して実現されます。WAAS は、将来 UDP 転送をサポートする可能性はありますが、現時点では TCP 転送にのみ対応しています。したがって、WAAS を使用しても UDP 転送を使用するプロトコルではその利点を得ることはできません。ただし、通信の多いプロトコルで消費される帯域幅が減少するので、UDP トラフィックにも良い影響を与える可能性があります。

VXI システム内で見られるさまざまなタイプのアプリケーションおよびトラフィック タイプに適用可能な WAAS テクノロジーのリストを次の表 6 に示します。

表 6　　トラフィック タイプ

トラフィック タイプ			Cisco WAAS		
アプリケーション	プロトコル	トランスポート	TFO	DRE	LZ
Citrix	ICA（基本的な暗号化）	TCP ポート 1494、TCP ポート 2598、セッションの信頼性を保証	可	可	可
USB リダイレクト		TCP ポート 32111	可	可	可
印刷	CIFS	TCP ポート 445	可	可	可
マルチメディア リダイレクト（MMR）	エンドポイント上の VDI クライアントでサポートされる MMR	TCP ポート 9427	可	可	可

インタラクティブ マルチメディア（音声やビデオなど）の配信は、デスクトップ仮想化の導入における最大の課題の 1 つです。DV ベンダーは、現在、ディスプレイ プロトコル内の音声とビデオのアプリケーションに対して優れたユーザ エクスペリエンスを実現しようと努力しています。Citrix などの DV ベンダーはインタラクティブ マルチメディアの問題に対処するために、HDX や Multimedia Redirection（MMR; マルチメディア リダイレクト）などの技術を採用しています。HDX テクノロジーは、ネットワークとパフォーマンスを最適化し、あらゆるネットワーク上で最良のユーザ エクスペリエンスを実現します。HDX と MMR は、ディスプレイ プロトコルでのインタラクティブ マルチメディア配信に対し、さらにプロトコルを最適化するオプション機能です。Cisco VXI では、使用可能な場合はこれらの機能を WAAS とともに有効にしておくことを推奨しています。

VXI の導入では、ほとんどの場合、エンタープライズ WAN 上でユーザをサポートするために WAN のアップグレードが必要になります。WAN のアップグレード コストは、Cisco WAAS の導入により 75%、場合によってはそれ以上削減することができます。

（注） Citrix XD5 では ICA 暗号化をオフにできないので、WAAS 最適化の有益性は低下します。しかし、ICA は TCP ベースのプロトコルであるため、WAAS TFO は一定のレベルで ICA を最適化します。VXI では、ディスプレイ プロトコルの範囲外であるマルチメディア トラフィックなど、すべての非ディスプレイ プロトコル トラフィックを WAAS が継続的に最適化します。Citrix XD4 を使用する場合は、WAAS による帯域幅最適化の利点を全面的に活用できるよう、ICA 暗号化をオフにすることをお勧めします。

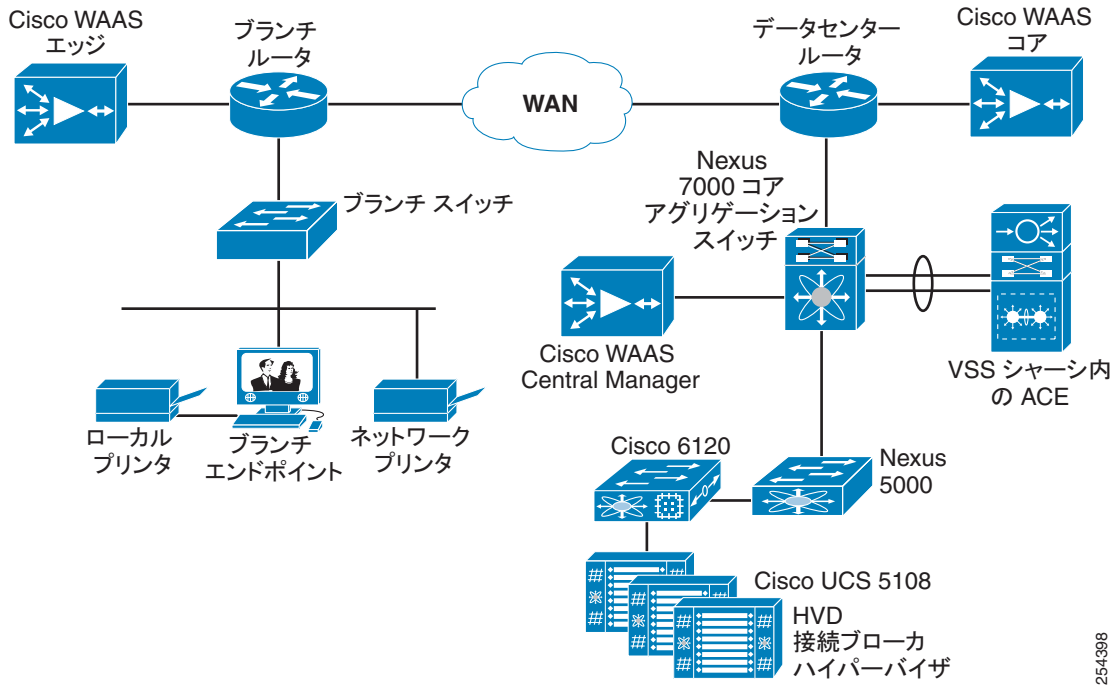
WAAS の導入

WAAS はネットワーク内では見えないので、何らかの形のネットワーク代行受信で、関連するトラフィック タイプを Cisco Wide Area Application Engine（WAE）にリダイレクトする必要があります。Cisco WAAS では、多数のネットワーク代行受信方式をサポートしています。Cisco VXI システムでは、次の 2 つの方式が推奨されます。

- 物理的インライン インターセプション：Cisco WAE は、2 つのネットワーク デバイスの間、通常はブランチ オフィス内のルータとスイッチの間に物理的に展開されます。これにより、WAN に向けてネットワークを通過するすべてのトラフィックまたは WAN から戻ってくるすべてのトラフィックが WAE を物理的に通過するようになり、それにより、トラフィックを最適化する機会が得られます。
- Web Cache Communication Protocol Version 2：Cisco WAAS デバイスでは、Web Cache Communication Protocol Version 2（WCCPv2）がサポートされています。これにより、仮想的ではありますがパス外のインライン展開が実現されます。WCCPv2 では、WAE デバイスは、ネットワーク上のアプライアンス（ネットワーク上のノードで物理的にインラインではない）として展開されます。WCCPv2 は、1 つのサービス グループ内で Cisco WAE デバイスを 32 台まで使用できるスケーラビリティ、WAE デバイス間のロード バランシング、およびすべての WAE デバイスが使用不可能になった場合のフェールスルー動作を提供します。さらに管理者がクラスタ内の WAE デバイスをほとんど中断なしで動的に追加または削除できるようにもなります。これは、VXI システム内で推奨される WAAS の導入モデルです。

次の図に示されたブランチ オフィスのセットアップ例では、Cisco WAE アプライアンスがローカル ルータ（通常は Cisco Integrated Services Router（ISR; サービス統合型ルータ））に接続されます。データセンター内では、Cisco WAAS がデータセンター WAN エッジ ルータ（通常は Aggregation Services Router（ASR; アグリゲーション サービス ルータ））に接続されます。ブランチ ルータは、VXI エンドポイントからのトラフィックを代行受信し、接続されている WAE に送信します。WAE は、最適化を行ってから、トラフィックをデータセンター WAN エッジ ルータに向けて送信します。DC WAN エッジ ルータはこのトラフィックを代行受信し、最適化のために Cisco WAAS コアへ送信します。トラフィックはこの場所からデータセンターに到達します。

図 34　　ブランチ ネットワーク内の WAAS の展開



WAAS の展開は、WAAS Central Manager または Cisco Prime LMS を使用して管理できます。VXI システムでは、その使いやすさから WAAS Central Manager の使用を推奨します。

Cisco WAAS の導入には、下に一覧されている複数のフォーム ファクタを使用できます。ネットワーク設計者は、特に注意書きがない限り、相互運用性の観点とは無関係に任意のフォーム ファクタを選ぶことができます。すべての WAAS モデルは、DC/ キャンパス WAAS WAE ヘッドエンド アプライアンスと連携して動作します。ブランチまたは DC 機器の選択は、必要な規模および選択されたソフトウェアのバージョンに基づいて行われます。WAAS の詳細なサイズ設定ガイドラインについては、http://tools.cisco.com/WAAS/sizing を参照してください。

表 7　　WAAS フォーム ファクタ

WAAS フォーム ファクタ	主要な特徴	特別な設計上の考慮事項
WAAS アプライアンス	複数のフォーム ファクタで使用可能。すべての機能をサポート。	DC 規模およびキャンパス内に適しています。
Cisco ISR G2 または Services-Ready Engine（SRE）による WAAS	ルータ統合型のアプリケーション アクセラレーション。専用のオンボード CPU、メモリ、およびハード ドライブ。	WAAS Central Manager または Cisco Prime LMS によって管理されます。 中規模から大規模のブランチに適しています。

WAAS フォーム ファクタ	主要な特徴	特別な設計上の考慮事項
WAAS Express	ISR G2 ルータの IOS 上でネイティブに稼動。 Cisco 1941、Cisco 2901、Cisco 2911、Cisco 2921、Cisco 2951、Cisco 3925、および Cisco 3945。	小規模から中規模のブランチに適用可能です。アプリケーション最適化は使用できません。 DC 内で WAAS 4.2.1 が必要です。 WAN リンクの T1、E1、3G、またはシリアル リンクに適しています。 WCS 4.3 以上が必要です。
WAAS Mobile	フットプリントが小さく、Windows アプリケーションとして動作。	WAAS モバイル マネージャが必要です。
vWAAS	仮想アプライアンス、データセンター内で稼動。WCCP リダイレクトをサポート。	Virtual Security Gateway が使用されない場所での使用を推奨します。

WAN の変動とパス最適化

サービス プロバイダーによって提供される WAN サービスの変動は、VXI のユーザ エクスペリエンスに悪影響を与える可能性があります。ブランチは、通常、複数のロード バランシングされた WAN リンクで展開され、さまざまな遅延特性、ジッタ特性、損失特性を伴うさまざまな SLA および原価基準を提供しているリンクが含まれます。VXI に必要なパフォーマンスを不規則に提供するリンクもあれば、そうでないものもあります。お客様は、所有するアプリケーションがそうしたネットワークの変動の影響を受けないようにすることに関心はありますが、一方でアクティブとスタンバイの WAN リンクをブランチに導入することには、未使用帯域幅のコストが発生することから、ためらいがあります。シスコは、VXI ユーザがネットワークの問題に影響されなくなるように、ルータ上で Performance Routing（PfR; パフォーマンス ルーティング）機能を提供しています。特に、VXI に必要な WAN パフォーマンスを提供可能な他のパスが利用可能な場合にその効果を発揮します。

Performance Routing（PfR; パフォーマンス ルーティング）は、WAN 上の最適パスを選択することで、アプリケーションのパフォーマンスを改善します。PfR は、アプリケーションの到達可能性、遅延、損失、ジッタなどのネットワーク指標を考慮に入れて、アプリケーションのニーズに基づいた最適パスを選択できます。ネットワーク パフォーマンスを測定し、それらの指標がアプリケーション ニーズを満たさない場合は、トラフィックを動的に再ルーティングします。それにより、PfR は、WAN 経由の VXI トラフィックに対してパス最適化と高度なロード バランシングを実現します。

PfR と WAAS は異なる形式の WAN 最適化を提供します。これらが連携することで、相互に補完し合い、単独の場合よりもさらに優れた VXI エクスペリエンスを WAN 上で提供できます。Cisco WAAS は、データ削減、圧縮、および TFO の各技術によりパフォーマンスを向上させ、WAN に対する帯域幅のニーズを減らすことで機能します。ただし、PfR とは異なり、WAAS はネットワーク パフォーマンスの変動には対処できず、そのため VXI のパフォーマンスはまだ影響を受ける可能性があります。さらに、コストベースのリンク ポリシーが PfR で使用されると、企業は運用コストを削減できます。

PfR には、2 つの論理コンポーネントとして、Master Controler（MC; マスター コントローラ）と Border Router（BR; 境界ルータ）が存在します。MC は、PfR の中央プロセッサおよびデータ収集ポイントとして機能し、ルータ上またはスタンドアロン モードで稼動できます。MC は、すべての BR からネットワーク指標を収集し、設定済みのポリシーに対してトラフィック クラスの適合性を判定します。この判定に基づいて、MC は BR に現在の WAN リンクに留まるか、トラフィック パスを変更する（可能な場合）ように指示できます。この実行は、当然のことながら BR 上でルート注入または動的ポリシー ベースのルーティング注入を使用して行われます。規模の小さい展開では、MC を BR 上に導入することもできます。

PfR は、次の 3 つの論理的な手順で動作します。

ステップ 1 トラフィック フローを特定し、その要件を理解します。

これは、トラフィック クラス、ポート、プロトコル、src/dst プレフィクスの情報を組み合わせて行われます。VXI トラフィックでは、TCP/UDP ポートを使用してディスプレイ プロトコル トラフィックを特定できます。あるいは、Citrix ベースの VXI 導入の場合、NBAR を Citrix 分類エンジンとともに使用することもできます。

ステップ 2 次に、ネットワーク パフォーマンスを測定し、監視します。

これは、BR 上で NetFlow ベースのモニタリングを使用することにより受動的に行われるか、ネットワーク プローブを送信して WAN リンクの健全性を測定することにより能動的に行われます。両方の方法を同時に使用して、精度を高めることもできます。

ステップ 3 最後に、ルーティングとパスの選択を行います。

これは、トラフィック クラス最適化を使用するか、リンク最適化を使用して行われます。VXI トラフィックでは、特定のトラフィック タイプのパフォーマンスを向上させることが目標なので、トラフィック クラス最適化が推奨されます。リンク ベースの最適化は、リンク コストに基づいて最適化を行います。したがって、複数のトラフィック フローが最適にロード バランシングされます。このアプローチでは、リンク コスト最適化が最も重視されます。

VXI 固有の PfR のベスト プラクティスおよび PfR の導入については、この章で後述する「VXI ネットワークに関する導入と設定のベスト プラクティス」のセクションを参照してください。

ブランチ内での VXI エンドポイント アクセス サービス

前にキャンパスのサブセクションで説明した PoE+、ロケーション トラッキング、自動ポート プロビジョニングなどのすべてのキャンパス アクセス機能はブランチ環境内でサポートされており、VXI システムでは有効にする必要があります。

テレワーカー

Cisco VXI に対応したネットワークでは、テレワーカーは固定テレワーカーとモバイル テレワーカーの 2 つに分類されます。どちらのテレワーカーも同じデータセンター内の同様の仮想デスクトップにアクセスすることが可能です。唯一の違いは、リモートユーザがどこから接続を行うかということだけです。

固定テレワーカーは、Cisco Virtual Office（CVO）などのソリューションを活用しているユーザです。Cisco Virtual Office ソリューションは、従来の社内オフィスではなく、その外部にいる作業者（フルおよびパートタイムの在宅勤務者、モバイル コントラクタ、管理職など）に安全で豊富なネットワーク サービスを提供します。データ、音声、ビデオ、およびアプリケーションを含む幅広いネットワーク サービスを提供することにより、Cisco Virtual Office は、従業員に対して包括的なオフィス環境を効果的に構築します。Cisco Virtual Office ソリューションは、次のコンポーネントで構成されます。

- Cisco 800 シリーズ Integrated Services Router（ISR; サービス統合型ルータ）と Cisco Unified IP Phone。
- VPN ルータとポリシー、設定、ID を制御するための集中管理ソフトウェアが含まれるデータセンターの存在。
- WAN 最適化は、WAAS モバイル実装をサポートするシックおよびシン VXI エンドポイントを使用したテレワーカーに提供されます。WAAS モバイルは、VPN ヘッドエンドの内側にあるデータセンター内の WAAS モバイル サーバとペアになります。
- 導入の自動化に関するガイダンスを含め、導入および統合を成功に導くシスコおよび承認済みパートナーによる導入サービスと継続的なサービス。

Cisco VXI に対応したネットワークは、CVO ソリューションを使用した固定のテレワーカーにさらに利点をもたらします。これらの機能強化には、Cisco 800 ISR の内側にある VXI エンドポイントも含まれます。エンドユーザは、Cisco 800 ISR と企業エッジ ルータの間に構築された VPN トンネルを使用することにより、各自の仮想デスクトップに安全にアクセスできます。また、WAAS モバイルによって提供される WAN 最適化テクノロジーを使用することにより、VXI トラフィックが最適化され、ユーザ エクスペリエンスが向上します。VXI 仮想デスクトップには、Cisco Unified Personal Communicator がインストールされます。ユーザは、Cisco Unified Personal Communicator アプリケーションから自分の席の IP 電話を制御できます。Cisco CVO ソリューションの詳細については、http://www.cisco.com/en/US/netsol/ns855/index.html を参照してください。

VXI のモバイル テレワーカーは、Cisco AnyConnect セキュア モビリティ クライアントと WAAS モバイルを実行可能な任意のエンドポイントから各自の仮想デスクトップに安全に接続します。モバイル テレワーカーの使用例では、Cisco IP Phone に関する要件はありません。モバイル テレワーカーは、一般に、セキュアでないネットワーク ロケーションにいます。Cisco VXI の利点の 1 つに、エンドポイントの盗難、破損、紛失があっても、データは保護されたままであるということがあります。また、WAAS モバイルによって提供される WAN 最適化テクノロジーを使用することにより、VXI トラフィックが最適化され、ユーザ エクスペリエンスが向上します。

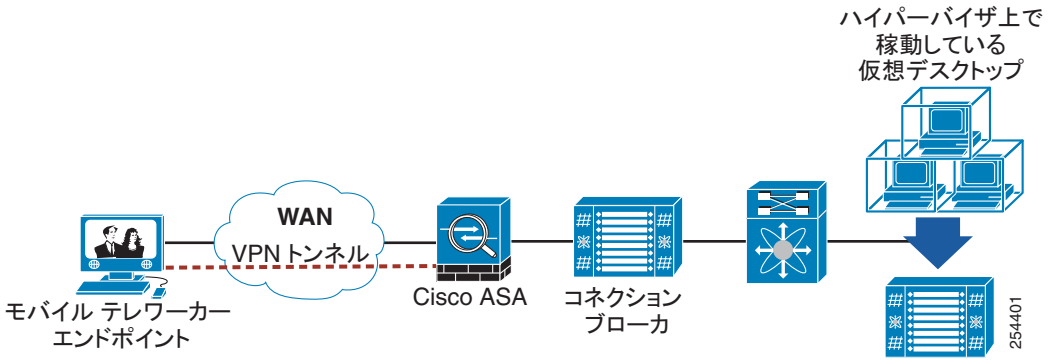
WAAS モバイル クライアントは、VPN 経由またはホーム オフィス内（CVO ルータ）で VXI データセンターに接続するエンドポイント デバイス上にインストールされます。WAAS モバイルは、フットプリントが小さく、大多数のシンおよびシック エンドポイントでサポートされています。WAAS モバイル クライアントは、VPN の内側に配置された WAAS モバイル サーバとペアになります。WAAS モバイル サーバは、WAAS ヘッドエンド アプライアンスと同一ではないことにご注意ください。つまり、SRE 製品上の WAVE、WAAS express、または WAAS とペアになることはできません。テレワーカー エンドポイントがキャンパス環境内またはブランチ環境内にある場合、WAAS モバイル機能は無効になります。これにより、より機能の豊富な WAN 最適化が可能になります。WAAS モバイル展開は、パフォーマンスの監視と ROI の測定が可能な WAAS モバイル マネージャによって管理されます。

WAAS モバイルの詳細については、http://www.cisco.com/en/US/prod/collateral/contnetw/ps5680/ps6870/data_sheet_cisco_wide_area_application_services_mobile.html を参照してください。

図 35 に、セキュアでない場所からセキュアな接続を使用してホステッド仮想デスクトップに接続しているモバイル テレワーカーを示します。

- モバイル テレワーカーは、AnyConnect クライアントを使用して ASA VPN ゲートウェイとの SSL VPN 接続を確立します。
- 次に、モバイル テレワーカーは、デスクトップ仮想化クライアントを使用してセキュア トンネル経由で企業のデータセンター内のコネクション ブローカと通信し、認証を行います。
- 認証に成功した後、コネクション ブローカは、モバイル テレワーカーに、使用可能な仮想デスクトップを提示します。
- 次に、モバイル テレワーカーは、目的の仮想デスクトップを選択して接続し、仮想デスクトップ セッションを確立します。これで、セッション全体が VPN トンネルによって保護された状態になります。

図 35　　シック クライアントを使用したテレワーカー



VXI データセンター エッジ

ロード バランシング、SSL オフロード、および VXI ヘルス モニタリング

アプリケーションのアップタイムと可用性を維持することは、IT システム管理者の主要な関心事です。Cisco VXI システム内の多くのミッションクリティカルなアプリケーションでは、システムの一部が応答しなくなった際に透過的なフェールオーバーを必要とします。サーバのアップタイムは、生産性の低下を防ぎ、ユーザが持続的に仮想デスクトップにアクセスできることを保証するうえで重要です。Cisco VXI システムは、コネクション ブローカまたは仮想デスクトップの障害を検出し、動的なアプローチを使用してこれらの障害の影響を軽減できなければなりません。仮想デスクトップ環境では、仮想デスクトップの要求がサーバに送信される前に、インフラストラクチャの複数レイヤ（コネクション ブローカ、Active Directory、サーバ、ストレージなど）を検証することが推奨されます。すべての構成要素がアクティブで使用可能なことを確認するには、ロード バランサでコネクション ブローカを検証する必要があります。コネクション ブローカは、仮想マシンとそれらをホストしているサーバを検証します。能動的なヘルス チェックで、プロトコル レイヤだけでなく、アプリケーション レイヤもテストする必要がありますCisco VXI ソリューションの Cisco ACE Application Control Engine 部分がこれらの機能を提供します。

デスクトップ仮想化は、データセンターへの常時ネットワーク接続に依存しています。過去 10 年間で、可用性はすべてのネットワーク設計に対して不可欠な要素になりました。シスコは、データセンター、キャンパス、ブランチ/WAN、インターネット エッジなど、エンタープライズ ネットワークの特定領域に重点を置いたハイ アベイラビリティ ネットワークの設計ガイダンスを提供しています。階層型ネットワーク設計は、ハイ アベイラビリティを実現するネットワークの設計において共通するテーマです。Cisco VXI システムに対応したネットワークを構築する際のハイ アベイラビリティ ネットワークの設計ガイダンスについては、次のリンクを参照してください。
http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA1_7_/configuration/device_manager/guide/UG_ha.html

既存の DV 環境の可用性とスケーラビリティの要件をさらに強化する場合は、ロード バランシング ソリューションを導入することを推奨します。

ロード バランシングと SSL オフロードでは、Cisco ACE が、ワンアーム モードを使用してデータセンター内のアグリゲーション レイヤに導入されます。ワンアーム モードでは、Cisco ACE が、クライアント要求とサーバ応答の両方を処理する単一 VLAN で設定されます。この設計では、ルーテッド ACE 導入とブリッジド ACE 導入も機能します。ワンアーム モードの場合、Client-Source NAT または Policy-Based Routing（PBR; ポリシーベース ルーティング）を設定する必要があります。それにより、Cisco ACE は、NAT を使用して実サーバに要求を送信します。サーバ応答は、元のクライアントに直接ではなく、Cisco ACE 経由で返されます。このトポロジは、Cisco ACE をネットワーク上のほぼどこにでも配置できるので便利ですが、NAT に依存するため、実現が不可能な場合もあります。なお、ルーテッドまたはブリッジ モードの場合は、すべてのユーザのディスプレイ接続に対して十分な帯域幅が存在することを確認してください。ワンアーム トポロジでは、Cisco ACE は、実サーバの「コネクション ブローカ」に独立ルータ経由で接続されるため、実サーバに対してスイッチとしてもルータとしても機能しません。クライアントは、要求を Cisco ACE 上の Virtual IP（VIP; 仮想 IP）に送信します。

少なくとも 2 台の Cisco ACE アプライアンスが必要です。Cisco ACE Application Control Engine モジュールと Cisco ACE 4170 Application Control Engine アプライアンスのどちらも使用できます。Cisco ACE モジュールを導入する場合は、マルチシャーシ EtherChannel を備えた Cisco Catalyst® 6500 Virtual Switching System（VSS; 仮想スイッチング システム）1440 などのテクノロジーを使用することが推奨されます。これにより、障害回復時に 1 秒以内のネットワーク コンバージェンスが実現され、ネットワーク設計の耐障害性を向上させることができます。Cisco ACE 4710 アプライアンスは、ポート チャネルを使用してアグリゲーション レイヤに接続され、ハイ アベイラビリティが実現されます。Cisco ACE モジュールまたは 4710 アプライアンスは、セッションの持続性を実現しながら、コネクション ブローカへの仮想デスクトップ要求をロード バランシングします。Cisco VXI システム向けに Cisco ACE 上に実装されている主要な機能は次のとおりです。

- コネクション ブローカのロード バランシング
- コネクション ブローカのヘルス モニタリング
- クライアント IP アドレスに基づいたセッションの持続性

VXI 環境内で Cisco ACE を導入するためのベスト プラクティスのガイドラインについては、このマニュアルの次のセクションを参照してください。

VPN の終端

デスクトップ サービスを提供するために、多くの IT 部門は、VPN ソリューションを利用して、ブランチ オフィスまたは固定およびモバイルのテレワーカー ロケーションから仮想デスクトップにアクセスするエンド ユーザにセキュアな接続を提供するようになっています。Cisco ASA アプライアンスや Cisco AnyConnect セキュア モビリティ クライアントなどのソリューションにより、エンド ユーザは、各自の仮想デスクトップが存在するデータセンターに対して暗号化された接続を使用できます。

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスは、クラス最高のセキュリティと VPN サービスを組み合わせた専用プラットフォームです。Cisco ASA 5500 シリーズでは、セキュア リモート アクセス（SSL/IPsec VPN）、ファイアウォール、コンテンツ セキュリティ、および侵入防御用の特別な製品エディションにより、特定の導入環境およびオプションに対するカスタマイズが可能になります。ASA は、VPN コンセントレータやファイアウォールとして機能でき、すべてのトラフィックが受信されるデータセンター エッジまたはキャンパス エッジの最初のポイントとなります。AnyConnect または IPSec に対応した ISR 800 ルータなどの VPN クライアントからのすべての VPN トンネルはここで終端します。その他のネットワーク セキュリティの懸念事項および Cisco AnyConnect セキュア モビリティ クライアントを使用した Cisco ASA アプライアンスの詳細については、「セキュリティ」の章で説明します。

VXI ネットワークに関する導入と設定のベスト プラクティス

WAAS

WAAS では、Central Manager によって、一元的なポイントから Cisco WAAS ソリューションを管理する必要があります。Cisco WAAS の Central Manager は、Cisco WAE アプライアンス上で動作します。管理者が設定またはポリシーの変更を 1 台の Cisco WAE デバイスまたはそれらのグループに適用すると、その変更は Cisco WAAS Manager によって管理対象の個々の Cisco WAE デバイスに自動的に伝播されます。各 Cisco WAE デバイスは、アプリケーション アクセラレータか Central Manager として設定できます。ベスト プラクティスでは、プライマリとスタンバイの Central Manager を導入します。

Cisco VXI 環境内の WAAS の設定

表 8 に、Cisco VXI ネットワーク上で WAAS を設定するために必要な設定情報を示します。

表 8　　Cisco WAAS の設定情報

作業内容	トラフィック タイプ	説明 / 機能	製品マニュアルへのリンク
Cisco WAAS Central Manager の設定	HTTPS		WAAS Central Manager GUI の概要
ブランチおよびデータセンターのルータ上での WCCP の設定	対象トラフィックの代行受信	WCCP をサポートしている IOS バージョン	『Configuring Traffic Interception』
アプリケーション アクセラレータの設定	Citrix ICA	ICA 暗号化および圧縮の無効化	『Configuring Application Acceleration』
ブランチおよびデータセンターの Cisco WAE の設定			『Configuring Network Settings』
Cisco WAAS を使用した印刷の最適化	CIFS		『Configuring and Managing WAAS Print Services』

WCCP を使用した WAAS 対応のトラフィック代行受信の設定

この章で前述したとおり、WCCP を使用して、「対象となる」すべてのトラフィックを代行受信し、WAAS に転送するようにルータを設定できます。WCCP サービス 61 および 62 は、インターフェイスから WCCP グループへトラフィックを再ルーティングするようにルータに指示します。サービス 61 は、入力トラフィックをリダイレクトし、サービス 62 は出力トラフィックをリダイレクトします。双方向のトラフィック フローをリダイレクトするには、サービス 61 と 62 の両方が必要です。

この設定では単一のインターフェイスを使用して着信パケットと発信パケットを代行受信するので、WAE サブネットは代行受信から除外してください。代行受信の除外が必要なのは、ルータがクライアントまたはサーバの Cisco WAE からのトラフィックを区別しないためです。ループが発生するため、Cisco WAE からのトラフィックをルータが再びリダイレクトしないようにしてください。

入力インターフェイスには WCCP 代行受信サービス 61 を、出力インターフェイスにはサービス 62 を設定します。インターフェイスからのすべての入力および出力パケットは、Cisco WAE に転送されて最適化されます。

詳細については、次のリンクにある優れた WAN 展開ガイドを参照し、WAAS のセクションをお読みください。

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns982/c07-610746-02_wanDeploy.pdf

WAAS アプライアンスと vWAAS は設計上、デバイスと VM で使用可能なすべての RAM を使用することが予想されます。これは正常な状態です。不要なメッセージを回避するため、低メモリしきい値アラートのレベルを高めに設定することが推奨されます。

Cisco VSG と Cisco vWAAS は、いずれも仮想アプライアンスであり、動作するには N1K DVS を必要とします。どちらの仮想アプライアンスも N1K でトラフィックを代行受信する必要があり、現在は同時にサポートされませんが、将来的にサポートされる予定です。対応策として、データセンターに VSG が設置されている場合は、WAAS アプライアンス フォーム ファクタを使用できます。データセンターの WAAS アプライアンスは通常、データセンター エッジでトラフィックを代行受信し、動作に N1K を必要としません。vWAAS がデータセンターにインストールされている場合は、VSG ではなく Cisco ASA を使用して HVD トラフィックのセグメント化とファイアウォール保護を行うことが強く推奨されます。

データセンターで vWAAS を使用する場合、トラフィックはデータセンター エッジの ASA を通過する必要があります。Cisco ASA/PIX Firewall で Cisco WAAS 最適化トラフィックを認識し、許可し、保護できるように、新しい Command-Line Interface（CLI; コマンドライン インターフェイス）が用意されています。Cisco ASA/PIX Firewall と Cisco WAAS の相互運用を容易にするため、この新しい CLI をクラス Modular Policy Framework（MPF）の一部として有効にしてください。

PoE+

Cisco VXC エンドポイントには 30W の電力が必要です。Cat4K のラインカードまたは Cat3K スイッチで PoE+ をサポートしている限り、特別な設定は必要ありません。コマンドの全リストとサポートされているラインカードおよびスイッチを確認するには、次の製品マニュアルを参照してください。

http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/31sg/configuration/guide/PoE.html

http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.1_19_ea1/configuration/guide/swint.html#wp1289756

ハイ アベイラビリティ：ISSU

アクセス スイッチのハイ アベイラビリティは、Cat4K シリーズのモジュラ シャーシ スイッチによってインサービス ソフトウェア アップグレードの形で提供されます。詳細な展開ガイドは、http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps4324/prod_white_paper0900aecd805e6a95.html にあります。

AutoSmart ポート

静的な Smartports マクロは、ポートに接続しているデバイスに基づいて手動で適用できるポート設定を提供します。静的マクロが適用されると、マクロに添付された CLI コマンドが既存のポート設定に追加されます。これらの設定は、ポートでリンクダウンが発生すると削除されます。

現リリースの Cisco VXI システムについては、MAC アドレス グループに MAC Operationally Unique Identifier（OUI）ベースのトリガーを設定します。MAC アドレスを組み込みマクロまたはユーザ定義のマクロにマッピングします。このマクロは、スイッチに接続している Cisco VXI エンドポイントが、上記で定義されたトリガー条件を満たしている場合に適用されます。接続しているエンドポイントがマクロをトリガーしないと、ポートは信頼できないと見なされ、デフォルトでゲスト VLAN に配置されます。ユーザ定義マクロ ファイルはリモート サーバの場所に保持することができ、ネットワーク内のすべてのアクセス スイッチで同じマクロを一貫して適用できます。これは、Cisco VXI に推奨される導入モデルです。

手動の手順は次のとおりです。

- macro auto mac-address グローバル コンフィギュレーション コマンドを使用して、MAC アドレス ベースのトリガーを設定します。
- ポート セキュリティ、Cisco VXI トラフィックに必要な QoS ポリシー、適切な VLAN、および dot1x など、Cisco VXI クライアントに必要な設定を使用して Cisco VXI マクロを作成します。
- macro auto execute グローバル コンフィギュレーション コマンドを使用して、MAC アドレス トリガーを Cisco VXI マクロに関連付けます（remote url コマンドを使用すると、マクロをリモートから検索できます）。

上記の手順は論理的に、Catalyst 4500E シリーズ スイッチと Catalyst 3000-X シリーズ スイッチの両方に適用されます。特定の設定の詳細とコマンドについては、http://www.cisco.com/en/US/docs/switches/lan/auto_smartports/12.2_55_se/configuration/guide/iosaspcg.pdf を参照してください。

ロケーション トラッキング

Cisco VXI のロケーション トラッキングの最小要件は次のとおりです。

Catalyst 4000 Switch IOS バージョン 12.2(52)SG 以降。

Catalyst 3000 Switch IOS バージョン 12.2(50)SE 以降。

MSE 3355：最大 18,000 のエンドポイントを追跡する大規模の展開に推奨されます。

MSE 3310：デバイス数が 2000 台までの小規模な Cisco VXI 導入に推奨されます。

現在、Cisco VXI 環境では、スイッチに保存されている管理タグと都市情報のみ利用できます。管理タグは、デバイスやユーザの論理グループに関連付けられた管理タグまたはサイト ロケーションです。

都市ロケーションは、RFC 4776 で説明されているとおり、通常は都市ロケーションの各種要素を示す文字列です。

設定順序：有線スイッチ

ロケーション サービスには、スイッチを設定する必要があります。これには、ロケーション データの設定と NMSP の有効化が含まれます。次に、スイッチ側の設定手順を示します。

- スロット/モジュール/ポートの設定（1/0/20）を理解します。
- 各スイッチ モデルに適した IOS バージョンを使用します。
- NMSP を有効にします。
- IP デバイス トラッキングを有効にします。
- SNMP コミュニティに読み取りおよび書き込みアクセスを設定します。
- 都市および管理タグ ロケーション識別子を設定します。
- スイッチ インターフェイスに識別子を割り当てます。

上記の手順に関する CLI コマンドや、その他の有益なデバッグ情報については、http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_50_se/configuration/guide/swlldp.html を参照してください。

設定手順：WCS の場合。ロケーション情報を WCS にリレーするための有線スイッチが必要です。

WCS では、次の手順を実行します。

- [Configure] > [Ethernet Switches] に移動します。
- イーサネット スイッチを追加します。
- IP アドレスを追加します。

- 対応するロケーションを有効にします。
- SNMP コミュニティ（読み取りおよび書き込み）を入力します。入力した SNMP コミュニティ ストリングは、Catalyst スイッチに割り当てた値に一致する必要があります。
- [Services] > [Synchronize Services] > [Switches] に移動します。
- [Assign] をクリックして、優先する MSE に割り当てます。
- スイッチを選択し、同期化します。
- [Services] > [Synchronize Services] > [Switches] に移動します。
- [System] > [Status] > [NMSP Connection] ステータスに移動します。
- スイッチごとにアクティブな NMSP ステータスを確認します。

上記の両方の設定手順が完了したら、次の操作により、WCS で有線要素を表示できます。

- [Context Aware Services] の [Wired] の下にある [Wired Switches] をクリックします。
- スイッチのリストが表示されます。
- 詳細を表示するスイッチの IP アドレスをクリックします。

詳細な設定手順や、ロケーション ベース サービス（context-aware-services とも呼ばれる）のスクリーン ショットは、次の場所にあります。

http://www.cisco.com/en/US/partner/products/ps9742/products_installation_and_configuration_guides_list.html

http://www.cisco.com/en/US/partner/docs/wireless/mse/3350/7.0/CAS/configuration/guide/CAS_70.html

トラッキング

有線および無線 Cisco VXI エンドポイントは、IP アドレス、部分 IP アドレス、MAC アドレス、部分 MAC アドレス、または VLAN ID で検索できます。エンドポイントの場所やステータスに関する特定の条件を満たしたときに通知するように、WCS を設定できます。設定に関する上記のリンクでは、トラッキングのこれらの側面を取り扱っています。同様のクイック ビデオについては、http://www.cisco.com/web/techdoc/wcs/location/client-tracking/tracking_wi-fi_clients.html?referring_site=bodynav を参照してください。

PfR

PfR 向け Cisco VXI の設計上の推奨事項は次のとおりです。

- ディスプレイ プロトコル TCP/UDP ポートを使用した PfR のトラフィック クラスのパフォーマンス最適化を有効にします。これらのポートは、この章の前半に記載されています。
- 可能な場合は NBAR 分類を ICA に使用します。
- Cisco VXI トラフィックは高度なインタラクティブ型であるため、PfR プロファイルおよびポリシーを定義する場合は、WAN における一方向の平均遅延目標を 100 ms にしてください。

PfR 機能は、Cisco ISR および Cisco ASR プラットフォームで使用できます。Cisco VXI ブランチ環境では、ブランチの ISR を使用して、データセンターの ASR に BR 機能を導入してください。データセンターの ASR では、MC を有効にしてください。

（注） PfR がルート変更をトリガーする前にパケットを処理した WAAS アプライアンスが後続のパケットを処理しないため、PfR は WAAS クラスタリングと連携して動作しません。

WAAS との PfR の展開と、DMVPN との PfR の展開はいずれも可能です。相互運用性の要件については、次のリンクを参照してください。

『Enhancing the WAN Experience with PfR and WAAS』

http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6554/ps6599/ps8787/prod_white_paper0900aecd806c5077.html

冗長な VPN ネットワークでの PfR の使用

http://www.cisco.com/en/US/products/ps8787/products_ios_protocol_option_home.html

PfR の展開には、複数の論理手順を伴います。次の表に、各フェーズとその関連文書を示します。

表 9　　PfR の展開手順

PfR の展開手順	設定に関する関連資料
トラフィック プロファイリング：トラフィック フローを識別および定義する方法。	http://www.cisco.com/en/US/docs/ios/oer/configuration/guide/pfr-profile.html
測定：前述のトラフィック フローに関するネットワーク メトリックの測定。	http://www.cisco.com/en/US/docs/ios/oer/configuration/guide/oer-trf_lnk_util.html
ポリシー：ネットワーク メトリックとしきい値およびトリガーのマッピング。処理の決定。	http://www.cisco.com/en/US/docs/ios/oer/configuration/guide/oer-cfg_ap_polcy.html
制御：ポリシーの決定に基づいたルート制御処理の実施。	http://www.cisco.com/en/US/docs/ios/oer/configuration/guide/oer-trf_rte_ctl.html
PfR の展開手順	設定に関する関連資料

DMVPN

Cisco WAN の導入ガイドは、Cisco VXI システムでの DMVPN 導入に最適なリソースです。次の URL を参照してください。

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns982/c07-610746-02_wanDeploy.pdf

DMVPN と WAAS の両方とも、トラフィックの代行受信とリダイレクトに WCCP を使用します。展開については、

次のガイドラインに従ってください。

- スポーク間の通信を有効にするには、WCCP を LAN の「in」と「out」に適用する必要があります。スポークでは、LAN およびトンネル インターフェイスの「in」方向に WCCP を適用する必要があります。ハブでは、LAN インターフェイスの「in」および「out」方向に WCCP を適用する必要があります。これは、NHRP/WCCP バグの対処策です。これ以外の設定では、TCP トラフィックはスポーク間トンネルをトリガーできません。
- EIGRP については、最初に「passive-interface default」コマンドを実行し、次に EIGRP ネイバーピアリングを確立する必要があるインターフェイスに対して「no passive-interface <int_name>」コマンドを実行することが推奨されます。
- スポーク間トンネルの動的作成をサポートするため、DMVPN ハブ ルータには、LAN インターフェイスの WCCP 62 アウトバウンドが必要です。

スポーク（ブランチ）には ISR G2 ルータ、ハブ（ヘッドエンド）には ASR/7200 シリーズ ルータを使用することが推奨されます。DMVPN 機能を取得するため、どのルータにも IOS の Security Plus ライセンスが必要です。

ACE

Cisco ACE アプリケーション コントロール エンジンは定期的に、コネクション ブローカの状態をチェックします。Cisco ACE は、プローブ情報を使用して、コネクション ブローカが最適なパフォーマンスと可用性でユーザの要求を処理できるかどうかを判断します。

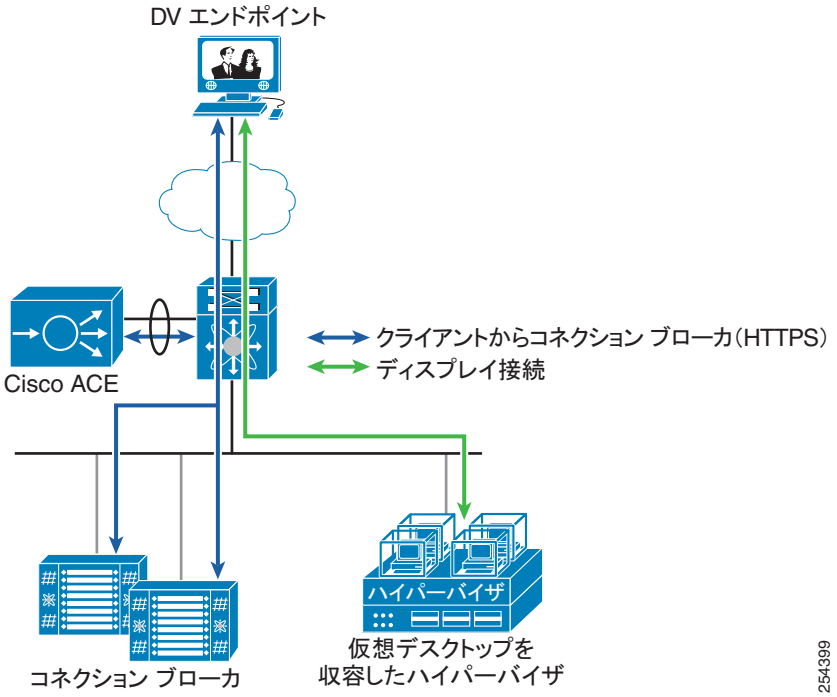
ユーザは、データセンターの仮想デスクトップにアクセスする必要がある場合、Cisco ACE で設定された仮想 IP アドレスに接続します。次に、Cisco ACE がユーザからの要求をコネクション ブローカに転送します。特定のクライアント セッションが常に同じサーバに送信されるよう、Cisco ACE では、クライアントとコネクション ブローカ間の複数のセッション持続性メカニズムをサポートしています。Cisco ACE は、クライアントの IP アドレスに基づいてセッションの持続性を実行するように設定されます。エンドポイントがプロキシ サーバを経由していると、セッションの持続性にいくつかの矛盾が生じることがあります。したがって、JSESSIONID クッキー持続性を使用することが推奨されます。Cisco ACE は、クッキーを表示する SSL セッションを終了する必要があります。

Cisco ACE とコネクション ブローカが一緒に展開されている場合のベスト プラクティスとしては、トンネルまたはダイレクト モードを使用するか、この 2 つの方法を組み合わせます。

- ダイレクト モードでは、エンドポイントはすべてのディスプレイ プロトコルのアクティビティのためにコネクション ブローカを経由する代わりに、仮想デスクトップへの接続を確立します。ダイレクト モードには、コネクション ブローカにおけるロード（CPU/ メモリ / ネットワーク）が大幅に減少するなど、多くの利点があります。コネクション ブローカはエンドポイントからの初期フェーズの接続に応答しますが、この動作にはリソースをほとんど使用しません。後続のデータは、エンドポイントと仮想デスクトップで稼動するエージェント間で直接やり取りされます。ダイレクト モードには、いくつかの欠点もあります。包括的なセキュリティ ポリシーが適用されていない場合、エンドポイントは、コネクション ブローカをバイパスして仮想デスクトップに直接接続できます。
- トンネル（プロキシ）モードでは、エンドポイントは、リモート表示データを含むすべての通信フェーズでコネクション ブローカへの接続を確立します。トンネル モードには、アクセス制御およびポリシーの適用をより厳密に行えることや、コネクション ブローカにおけるロード（CPU/ メモリ / ネットワーク）の可用性が大幅に向上することなど、いくつかの利点があります。

図 36 に、ダイレクト モードを使用した Cisco ACE 4710 アプライアンスの展開を示します。Cisco ACE 4170 アプリケーション コントロール エンジン アプライアンスは、コネクション ブローカに対するロード バランシングのみ実施します。コネクション ブローカからユーザに仮想デスクトップが割り当てられると、ディスプレイ プロトコルは Cisco ACE 4710 アプライアンスをバイパスします。Cisco ACE はワンアーム モードで設定されます。Cisco VXI システム対応のネットワークでは、ワンアーム モードが推奨されます。ディスプレイ プロトコルがエンド ユーザと仮想デスクトップの間に存在するため、トランザクションの中央に Cisco ACE は必要ありません。このため、Cisco ACE では、使用可能なデスクトップに関するコネクション ブローカからの着信エンドユーザ要求のロード バランシングを行うためのリソースを節約できます。ACE はワンアーム モードで展開されるので、Source Network Address Translation（SNAT; 送信元ネットワーク アドレス変換）を設定する必要があります。

図 36　　ネットワークにおける ACE の展開



ACE の設定作業

表 10 に、DV サーバの可用性を向上させるための詳細な設定を示します。この表には、コンテキストが示されていることがわかります。Cisco ACE が提供する仮想化デバイス環境は、コンテキストと呼ばれるオブジェクトに分けられます。各コンテキストは、独立した Cisco ACE ロード バランサのように動作し、独自のポリシー、インターフェイス、ドメイン、サーバ ファーム、実サーバ、および管理者を持ちます。また、独自の管理も存在します。Cisco ACE が展開されると、他の仮想コンテキストの管理とプロビジョニングに管理コンテキストが使用されます。VMware DV ロード バランシングという仮想コンテキストを作成することがベスト プラクティスです。

表 10　　DV サーバの設定

機能	トラフィック タイプ	説明/機能	製品マニュアル
管理コンテキストの設定	Telnet、SSH、SNMP、HTTP、HTTPS、または ICMP のみ対応	管理コンテキストを使用して次の設定を行います。 物理インターフェイス 管理アクセス リソース管理 ハイ アベイラビリティ	『Configuring Virtual Contexts』
ワンアーム モードの設定	コネクション ブローカのロード バランシングには、ワンアーム モードの使用を推奨	送信元 NAT が必要	『Configuring One-Arm Mode』

機能	トラフィック タイプ	説明 / 機能	製品マニュアル
Citrix DV に対する仮想コンテキストの設定	Citrix ICA	ICA 接続のロード バランシング：レイヤ 4 クラス マップを作成	『Configuring Virtual Server Properties』
セッションの持続性の設定		送信元 IP アドレスに基づいたセッションの持続性	『IP Address Stickiness』
ヘルス モニタリングの設定	regex チェックを使用した HTTP プローブ	HTTP プローブ内の regex ステートメント 「Citrix」を除く	『Configuring Health Monitoring for Real Servers』
ロードバランシング アルゴリズムの設定	最小負荷経路選択アルゴリズムを使用	サーバ上の最小接続数 predictor leastconns	『Load-Balancing Predictors』
送信元 NAT の設定	エンドユーザへの応答時の接続で ACE がバイパスされないよう、SNAT が必要	NAT アドレスとして仮想アドレスを使用	『ACE NAT Configuration』

関連情報

次に、この章で説明したハードウェアおよびソフトウェアを含む特定のベンダー情報の詳細へのリンクを示します。

WAAS Central Manager GUI の概要

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v421/configuration/guide/intro.html#wp1122501

『Configuring Traffic Interception』

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v4013/configuration/guide/traffic.html

『Configuring Application Acceleration』

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v4013/configuration/guide/policy.html

『Configuring Network Settings』

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v4013/configuration/guide/network.html

『Configuring and Managing WAAS Print Services』

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v4013/configuration/guide/printsvr.html

データセンター

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_3_0/DC-3_0_IPInfra.html

キャンパス

http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html

ブランチ /WAN

http://www.ciscosystems.com/en/US/docs/solutions/Enterprise/Branch/srlgbrnt.pdf

物理インターフェイス

http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA1_7_/configuration/device_manager/guide/UG_ntwk.html

管理アクセス

http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/v3.00_A1/configuration/administration/guide/access.html

リソース管理
http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA1_7_/configuration/device_manager/guide/UG_confg.html#wp2700097

ハイ アベイラビリティ
http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA1_7_/configuration/device_manager/guide/UG_ha.html

仮想コンテキストの設定
http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA1_7_/configuration/device_manager/guide/UG_confg.html

ワンアーム モードの設定
http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/vA2_3_0/configuration/getting/started/guide/one_arm.pdf

Citrix DV に対する仮想コンテキストの設定

http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA1_7_/configuration/device_manager/guide/UG_lb.html#wp1044682

セッションの持続性の設定

http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA1_7_/configuration/device_manager/guide/UG_lb.html#wp1062118

ヘルス モニタリングの設定

http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA1_7_/configuration/device_manager/guide/UG_lb.html#wp1045366

バランシング アルゴリズム

http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA1_7_/configuration/device_manager/guide/UG_lb.html#wp1045366

送信元 NAT の設定：

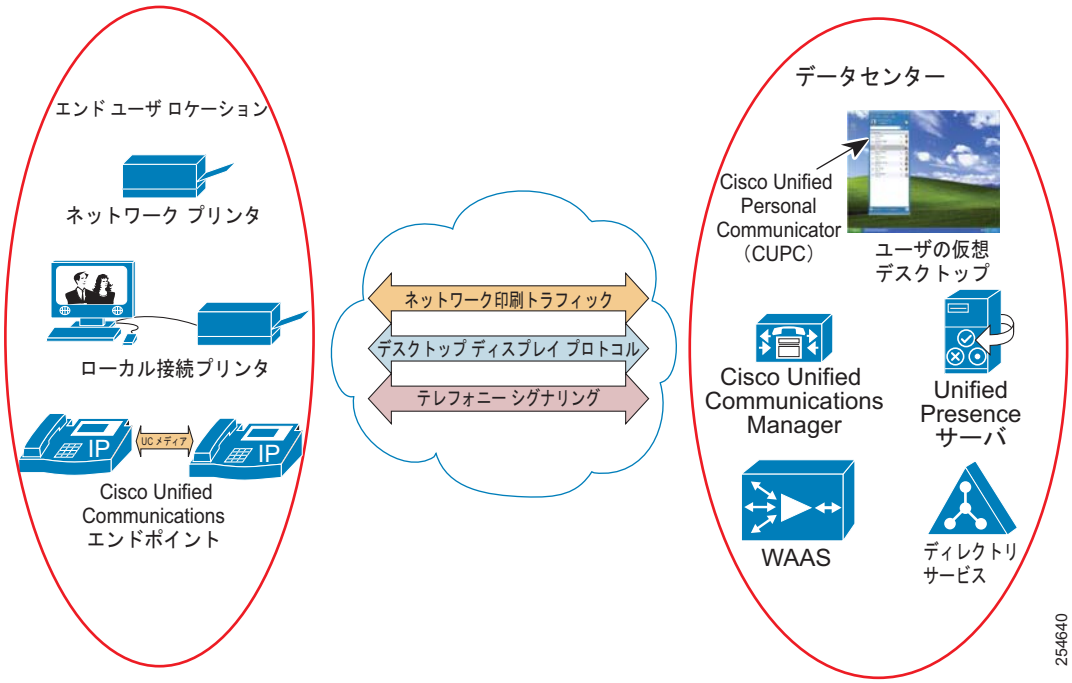
http://docwiki.cisco.com/wiki/Basic_Load_Balancing_Using_One_Arm_Mode_with_Source_NAT_on_the_Cisco_Application_Control_Engine_Configuration_Example

エンドポイントとアプリケーション

Cisco VXI システムは、Desktop Virtualization（DV; デスクトップ仮想化）およびコラボレーション サービスを提供するさまざまなエンドポイントとアプリケーションをサポートします。デスクトップ仮想化エンドポイントは、キーボード、マウス、およびタッチ スクリーン入力デバイスを介したユーザとデスクトップの対話をサポートします。また、いくつかの USB ベースの印刷およびストレージ機能も備えています。Unified Communication（UC; ユニファイド コミュニケーション）エンドポイントは、音声およびビデオ通信をサポートします。Cisco Unified Personal Communicator、UC Integration™ for Microsoft Lync、および UC Integration™ for WebEx Connect は、ユーザが自身の Hosted Virtual Desktop（HVD; ホステッド仮想デスクトップ）に配置されたソフトウェア アプリケーションを使用してデスクフォンを制御できるようにすることで、仮想デスクトップと UC エンドポイントの機能を統合します。

図 37 に、仮想デスクトップ環境の一般的なエンドポイント データ フロー図を示します。

図 37　　一般的なエンドポイント データ フロー図



（注）　VXI システム内の Cisco Unified Personal Communicator、Cisco UC Integration for Microsoft Lync（CUCILync）および Cisco UC Integration for WebEx Connect（CUCIConnect）の検証に関する詳細については、『VXI Release Notes』および「パフォーマンスとキャパシティ」の章を参照してください。VDI 環境におけるサポートを確認するには、上記の UC アプリケーションに関する製品マニュアルを参照することが推奨されます。また、これらのアプリケーションを展開する前に、使用する環境内で十分な検証を行うことが強く推奨されます。

DV エンドポイント

ユーザのエンドポイントは通常、アプリケーション要件と作業に関係するタスクに基づいて選択されます。DV エンドポイント デバイスは、ネットワーク上でユーザの HVD にアクセスするために使用され、ゼロ クライアント、シン クライアント、またはシック クライアントのいずれかのタイプで提供されます。タイプごとに提供される機能とデータ フローが異なり、ネットワーク上に配置されるロードも異なります。また、デバイスの機能に基づく各デバイス タイプは、特定のエンド ユーザ プロファイルに適しています。「デスクトップ仮想化」の章の「企業の DV ポリシーとユーザ プロファイル」のセクションにユーザ プロファイルの定義と、各プロファイルに関連付けられたワークフローとタスクの説明があります。

ゼロ クライアント

ゼロ クライアントは、最も単純なデバイスです。ゼロ クライアントには、ユーザに公開されないオペレーティング システムが組み込まれています。ゼロ クライアントではローカル機能が削減され（CPU の削減、メモリ キャパシティの縮小、ほぼ皆無のローカル ストレージなど）、ほとんど HVD 内で使用できるリソースにのみ依存します。オペレーティング システムが公開されていないので、ウイルス感染の危険がないため、ゼロ クライアントはきわめて安全です。ゼロ クライアントは通常、HVD への単一のネットワーク接続に依存するため、このクラスのデバイスのネットワーク ポリシーは非常に単純です。デバイスとの間で許容されるネットワークフローを制御する単純なセキュリティ アクセス コントロール リストを、エンドポイントのネットワーク ロケーション（subnet など）とコネクション ブローカ（および関連付けられた仮想デスクトップ プール）との間に作成できます。

セキュリティ ポリシーの一環として Network Access Control（NAC; ネットワーク アクセス コントロール）が必要な場合は、一部のゼロ クライアントで 802.1x を使用できます。シスコの Virtual Experience Client 2212（VXC-2212）および Virtual Experience Client 2112（VXC-2212）などのゼロ クライアントは、802.1x をサポートしています。

シン クライアント

シン クライアント デバイスは通常、より多くのローカル機能を備えており、多くの場合はローカルに組み込まれたカスタマイズ可能なオペレーティング システム（組み込みの Linux や Windows など）を搭載しています。シン クライアントは柔軟性に優れ、システム管理者がカスタマイズした後、ロックダウンすることが可能です。シン クライアントを固定することで、ウイルス感染の危険を最小限に抑えることができ、ユーザがエンドポイントの設定をローカルで変更することを防止できます。シン クライアントは通常、DV エンドポイントにローカルのアプリケーションが必要である場合に使用されます。たとえば、ローカル オペレーティング システム上で動作する Web ブラウザ、リッチ メディア コンテンツ プレーヤー、電子メール クライアント、オフィス自動化ツールなどが挙げられます。ゼロ クライアントと比べ、シン クライアントのトラフィック パターンはこのようなローカル アプリケーションの使用によって変わります。このため、通常はネットワーク セキュリティ ポリシーがより複雑になります。また、これはユーザのアプリケーションの選択および設定によって異なります。場合によっては、メディア リダイレクトにより、HVD を経由せずに DV エンドポイントからトラフィックを発信し、DV エンドポイントで終了できます。たとえば、ユーザがローカル ブラウザを開いた場合に生じるトラフィックは、ユーザの HVD を介してルーティングされません。

シック クライアント

シック クライアント デバイスとは、標準のオペレーティング システムを実行する個人用コンピュータ（ラップトップを含む）を指します。シック クライアントは、ローカルにインストールされた DV ソフトウェア クライアントに依存して、ユーザの HVD にデバイスを接続します。シック クライアント デバイスはオフライン作業が可能であるため、「モバイル ユーザ」の間で広く利用されています。シック クライアントのトラフィック パターンは、シン クライアントとは大きく異なる場合があります。ユーザはほとんどのアプリケーションをローカルで実行し、データセンター内の特定のアプリケーションを実行する場合のみ HVD を使用するように選択できます。たとえば、ユーザはローカルのシック クライアント上の Web ブラウザ、電子メール、およびオフィス アプリケーションを実行できますが、ローカル マシンに配置できない機密文書へのアクセスには HVD 接続を使用します。標準の PC およびラップトップをシック クライアントに変換するための多くのオプションが、デスクトップ仮想化ベンダーから提供されています。

Cisco Virtual Experience Client デスクトップ仮想化エンドポイント

Cisco VXC-2112 および VXC-2212 は、軽量の組み込み OS を実行するゼロ クライアントであり、ディスプレイ プロトコルに ICA または RDP を使用して、Citrix XenDesktop 環境に接続するための機能を提供します。

図 38　　Cisco VXC-2112

Cisco VXC-2112 エンドポイントは、Cisco 9971 または 8961 IP Phone にシームレスに接続します。この設定により、UC と DV の機能を備えた単一の統合デバイスが実現されます。たとえば、ユーザは HVD 上の Cisco Unified Personal Communicator または UC Intgeration for Webex Connect からインスタント メッセージング、ディレクトリ ルックアップ/連絡先リスト、プレゼンス、および会議を含む Cisco IP テレフォニー コントロールにアクセスする一方、ローカルの IP 電話で音声やビデオを使用することができます。

VXC-2112 には、ネットワーク アクセス用に IP 電話の PC ポートに接続するイーサネット ポートが搭載され、Cisco IP Phone 側に接続する電源ケーブルが付属しています。このアプローチにより、単一のイーサネットベース ネットワーク接続でネットワーク接続と電源の両方を UC および DV エンドポイントの両方に提供できます。VXC ネットワーク トラフィックをデータ VLAN に配置することが推奨されます。

VXC-2112 は、基本構成（つまり、キーボード、マウス、単一のモニタ接続）の場合は 802.3AT ベースのインライン パワー（PoE、25.5W）が必要ですが、USB ポート、Cisco Key Expansion Module（KEM; キー拡張モジュール）、または複数のモニタが必要とされるその他の構成では外部電源（CP-PWR-CUBE-4）が必要になります。

拡張構成に十分な電力を供給するもう 1 つの方法として、最新の Catalyst 4500E スイッチで使用できる Universal Power over Ethernet（UPoE）機能を利用します。外部電源によってエネルギー コストとケーブルの管理と複雑さが増すような展開には、このオプションが推奨されます。Cisco Catalyst 4500E の UPoE テクノロジーは、最大 60 ワットの電力を提供し、非常に幅広いエンドポイントをサポートできるほか、可用性の向上、OpEx の低下、展開の高速化という利点があります。UPoE の詳細については、www.cisco.com/go/upoe/ を参照してください。Catalyst 4500E スイッチには Cisco EnergyWise のフルサポートがあります。このサポートは、全社間の電力制御を一元化する UPoE を介して拡張されます。設計上の考慮事項について、「VXI ネットワーク」の章の「UPoE」のセクションも参照してください。

本稿執筆時点では、UPoE は最新のファームウェアを実行する 9971 電話機（VXC 2112 を装着）でのみ使用できます。

UPoE をサポートする適切な電話ロードについては、『Cisco VXI Configuration Guide』を参照してください。

VXC クライアントの設定の詳細については、http://www.cisco.com/go/vxc/ を参照してください。

図 39　　Cisco VXC-2212

VXC-2212 ゼロ クライアント エンドポイントは、スタンドアロンの DV アプライアンスであり、DV 機能を提供します。また、Cisco UC エンドポイント（Cisco 79XX IP Phone など）と連携する場合は、関連付けられた IP 電話の音声およびビデオ機能に依存しながら、ホステッド仮想デスクトップ上の Cisco Unified Personal Communicator または Cisco Webex Connect を使用して、統合化されたユーザ エクスペリエンスを実現します。

VXC-2212 は、基本構成（つまり、キーボード、マウス、単一のモニタ接続）の場合は 802.3AF ベースのインライン パワー（PoE、15W）が必要ですが、その他の構成では 802.3AT ベースのインライン電源（PoE、25.5W）または外部電源（CP-PWR-CUBE-4）が必要になります。

VXC-2212 は通常、アクセス スイッチに直接接続します。VXC-2212 のポートはデータ VLAN 内に配置することが推奨されます。セキュリティを強化する目的で、VXC-2212 は 802.1x 認証をサポートしています（802.1x 機能は Cisco ACS 5.2 で検証済み）。

VXC クライアントの設定の詳細については、http://www.cisco.com/go/vxc/ を参照してください。

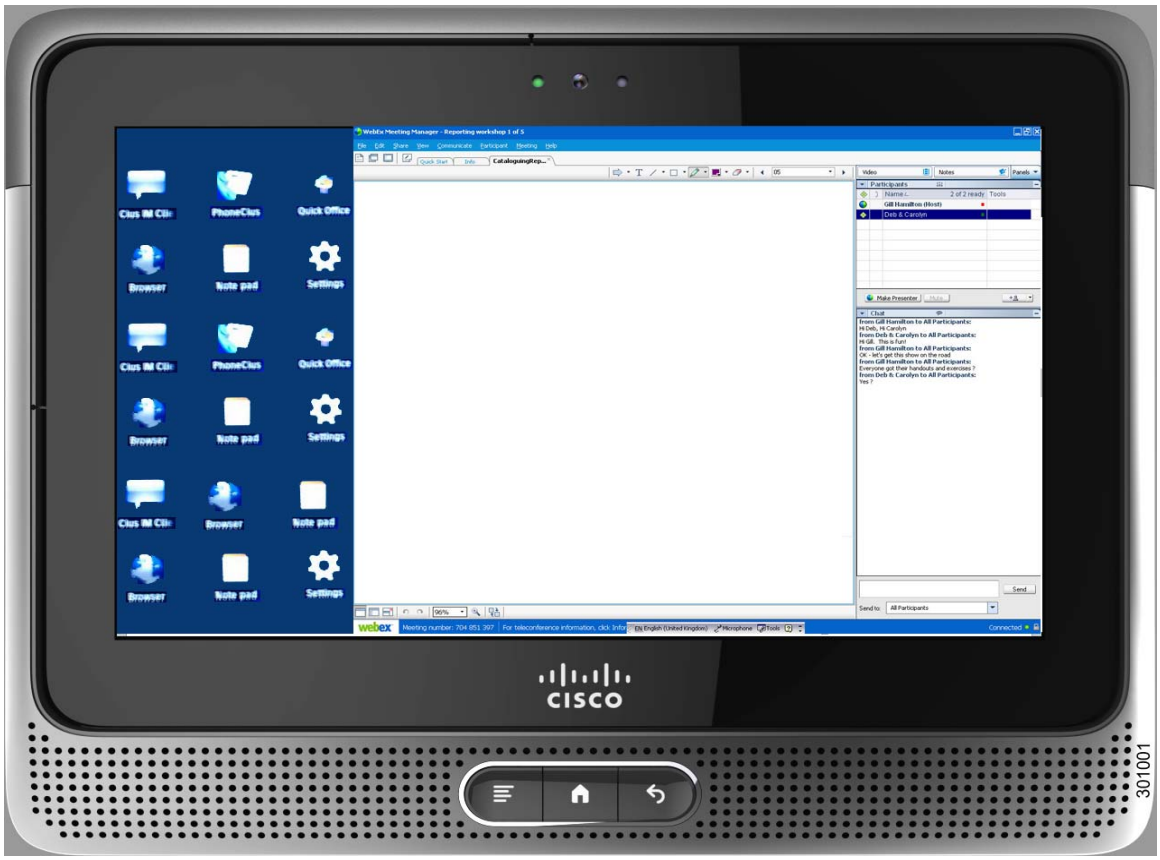
Cisco Cius による DV エンドポイント

Cius の概要

Cisco Cius は、7 インチ対角サイズの高解像度カラー タッチスクリーン タブレットです。Cius は Android オペレーティング システムで動作し、WiFi（802.11a/b/g/n）、Bluetooth 3.0、Cisco Telepresence の相互運用性を備えた HD ビデオ（720p）、および音声 / ビデオ会議、プレゼンス、インスタント メッセージング、WebEx Meeting Center へのワンクリック アクセスなどのコラボレーション アプリケーションをサポートします。Cisco Cius は、仮想デスクトップ シン クライアントとしても機能します。一元管理およびアプリケーション制御ポリシーを備えた Cius は、ナレッジ ワーカーおよびエグゼクティブ向けの初のエンタープライズ対応タブレットであり、業界内で最も包括的で信頼性が高く、セキュアなコラボレーション エクスペリエンスを提供します。Cius は、スタンドアロン デバイスとしても、コンパニオン ドッキング ステーション（Cius ドッキング ステーション）と組み合わせても使用できます。

Cius デバイスは、取り外しおよび保守の可能な 8 時間バッテリによって電力供給され、Cius バッテリの充電が可能な 5Vdc 電源アダプタが付属しています。使用可能なドッキング ステーションには、-48Vdc 電源アダプタが付属しています。Cius をドッキングしている場合、バッテリの充電には -48Vdc 電源アダプタを使用するので、5Vdc 電源アダプタは不要になります。省エネルギーおよび単一ワイヤの利便性を活かすため、Cius ドッキング ステーションでは Power-over-Ethernet（802.3AT 30W が必要）をサポートしています。Cius タブレットでは、PoE+ 接続で完全に電力供給および充電できるので、外部の電源アダプタは必要なくなります。

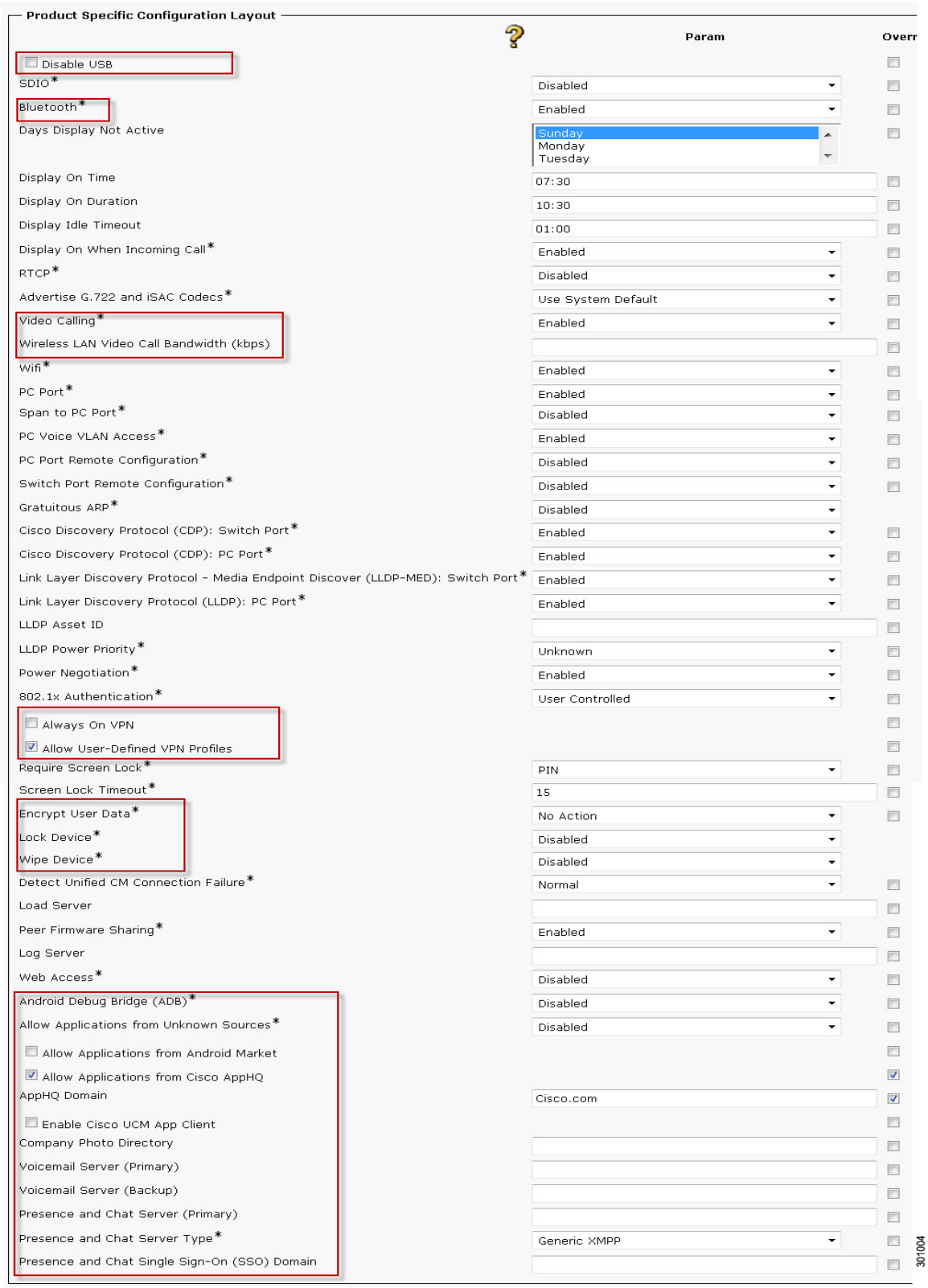
図 40　　Cisco Cius エンドポイント



Cius の管理

Cisco Cius タブレットは Cisco Unified Communications Manager（8.5 以降）を介して一元管理されるので、エンタープライズ環境にとって理想的です。管理者は、Cisco Unified Communications Manager（Cisco UCM）を利用することで、ポリシーの設定、機能の有効化、さらにはデバイスの紛失や盗難に備えたデバイスのロックやワイプを実行できます。また、管理者は、USB ポート（有効化 / 無効化）、ビデオ通話機能、Android アプリケーション マーケットへのアクセス、およびリモート VPN アクセスを制御することができます。

図 41　　Cius の管理


Product Specific Configuration Layout
Param
Overr
Disable USB
SDIO*
Disabled
Bluetooth*
Enabled
Days Display Not Active
Sunday
Monday
Tuesday
Display On Time
07:30
Display On Duration
10:30
Display Idle Timeout
01:00
Display On When Incoming Call*
Enabled
RTCP*
Disabled
Advertise G.722 and iSAC Codecs*
Use System Default
Video Calling*
Enabled
Wireless LAN Video Call Bandwidth (kbps)
Wifi*
Enabled
PC Port*
Enabled
Span to PC Port*
Disabled
PC Voice VLAN Access*
Enabled
PC Port Remote Configuration*
Disabled
Switch Port Remote Configuration*
Disabled
Gratuitous ARP*
Disabled
Cisco Discovery Protocol (CDP): Switch Port*
Enabled
Cisco Discovery Protocol (CDP): PC Port*
Enabled
Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port*
Enabled
Link Layer Discovery Protocol (LLDP): PC Port*
Enabled
LLDP Asset ID
LLDP Power Priority*
Unknown
Power Negotiation*
Enabled
802.1x Authentication*
User Controlled
Always On VPN
Allow User-Defined VPN Profiles
Require Screen Lock*
PIN
Screen Lock Timeout*
15
Encrypt User Data*
No Action
Lock Device*
Disabled
Wipe Device*
Disabled
Detect Unified CM Connection Failure*
Normal
Load Server
Peer Firmware Sharing*
Enabled
Log Server
Web Access*
Disabled
Android Debug Bridge (ADB)*
Disabled
Allow Applications from Unknown Sources*
Disabled
Allow Applications from Android Market
Allow Applications from Cisco AppHQ
AppHQ Domain
Cisco.com
Enable Cisco UCM App Client
Company Photo Directory
Voicemail Server (Primary)
Voicemail Server (Backup)
Presence and Chat Server (Primary)
Presence and Chat Server Type*
Generic XMPP
Presence and Chat Single Sign-On (SSO) Domain
301004

Cius アプリケーション

Cius アプリケーションは、4 つの方法でアクセスおよびインストールできます。アクセスは、Cisco UCM ポリシーの設定によって定義されます。管理者は、すべてのオプションを有効にすることも、組織のポリシーに応じて一部のオプションを無効にすることもできます。使用可能なアプリケーション ストアには、次のオプションがあります。

- 標準の Android マーケット ストア：このオプションを選択すると、インターネットベースの Android マーケット サイトにアクセスできます。アクセスは Cisco UCM を介して設定され、デフォルトで有効になります。
- Cisco UCM が管理する Android アプリケーション（APK ファイル）: Cisco UCM の「サービス サブスクリプション」機能を使用することで、組織は APK アプリケーションを所有し、管理できます。このオプションでも、Web パブリッシャを使用する必要があります。
- 不明な送信元 Web サーバ（一般に社内で稼動）：このオプションは、オプション 2 と似ていますが、これらのアプリケーションの管理に Cisco UCM を使用しないという点で異なります。APK アプリケーションのアクセスおよびポリシーの管理には、別個の管理ツールが使用されます。このオプションは、デフォルトで無効になります。
- Cisco App HQ：このオプションを選択すると、シスコが管理する AppStore にアクセスできます。この AppStore に登録した Cius ユーザは、使用可能なアプリケーションをダウンロードできます。Cisco App HQ へのアクセスは、Cisco UCM を介して設定され、デフォルトで有効になります。

上記のいずれかの方法で管理できるアプリケーションは、DV 対応アプリケーションの WYSE PocketCloud と VMware View Client であり、Cius ユーザはこれらのアプリケーションを利用して、VMware View 接続サーバからホステッド仮想デスクトップにアクセスできます。WYSE Pocket Cloud Pro アプリケーションは表示チャネル プロトコルとして RDP をサポートし、VMware View Client は PCoIP をサポートしています。いずれのベンダーも、Cisco Cius での動作やパフォーマンスを向上させるためにそれぞれの DV アプリケーションを最適化しています。

図 42　　Cius アプリケーション

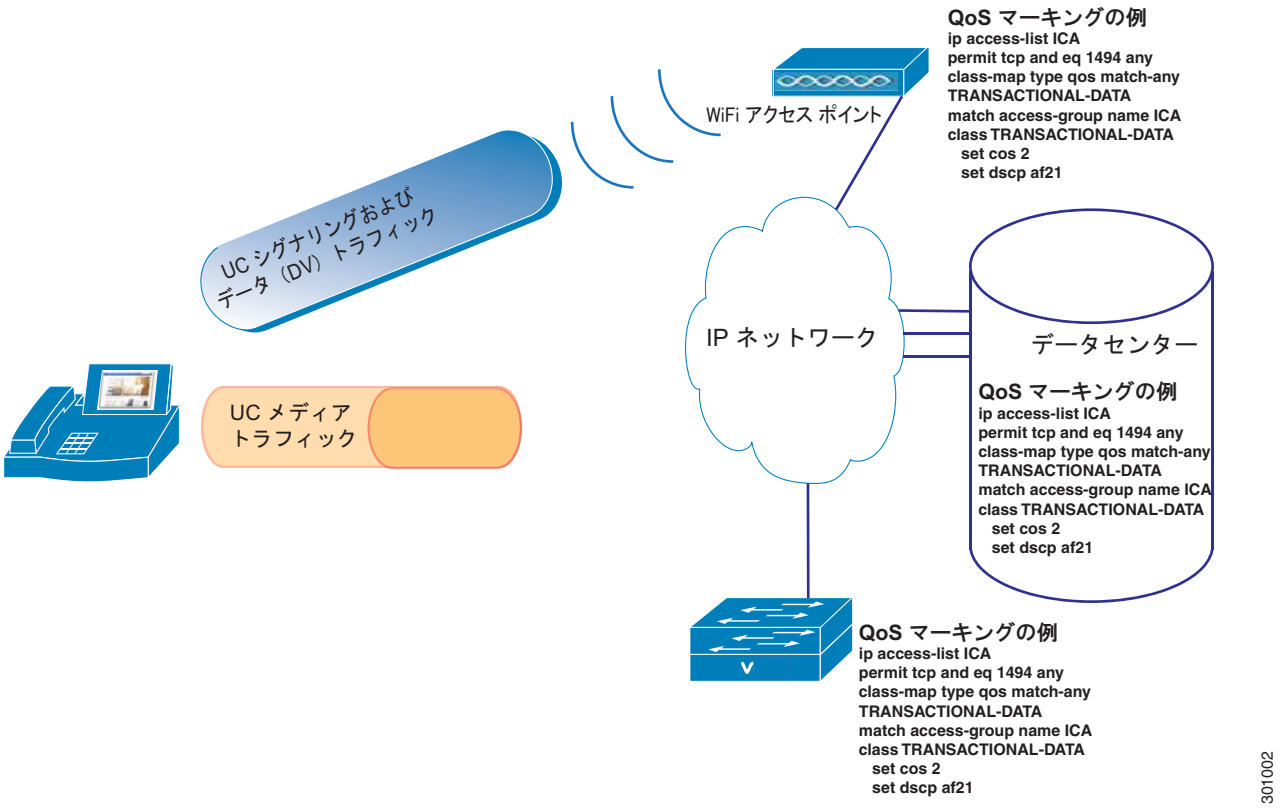
これらのアプリケーション管理機能を備えることで、IT 部門は、準拠していると思われるアプリケーションにユーザ、またはユーザのグループを制限できます。管理者は、不明なソースからのアプリケーションのインストールを無効にして、公共の Android マーケットからのアプリケーションを禁止できます。

Cius の動作モード

Cisco Cius は、スタンドアロンモードで使用できます。このモードでは、すべての接続が WiFi 接続を経由し、ユーザ インターフェイスはタッチスクリーン ディスプレイがベースとなります。また、コンパニオン ドッキング ステーションと一緒に使用し、外部のモニタ、マウス、およびキーボードに接続することもできます。ドッキング ステーションは、第 2 の有線イーサネット接続を提供します。ドッキング ステーションの使用により、Cius はタブレット コンテンツ使用デバイスから、ホステッド仮想デスクトップに接続できる全機能型デスクトップ デバイスに変わります。この機能により、Cius をすべての機能を備えた（パワーポイントやワード文書を作成する）コンテンツ作成デバイスとして使用でき、専用 PC を使用しているようなエクスペリエンスを得ることができます。

他の Desktop Virtualization（DV; デスクトップ仮想化）エンドポイントと異なり、Cisco Cius はローカルの音声およびビデオ メディア プレーンを備えています。つまり、Cisco Cius からのコールは、Cius デバイス自体に搭載された音声およびビデオのメディア チャネルによってサポートされます。メディア チャネルのフローは、ユーザのホステッド仮想デスクトップを経由せずに、宛先デバイスに直接到達する最適なネットワーク パスに従って確立されます。ドッキングされている場合、UC アプリケーション クライアントの [Cius Phone] は、WiFi ネットワーク上の UC シグナリング接続を維持しながら、UC メディア トラフィックを有線インターフェイス経由でルーティングします。このアプローチにより、ドッキングやドッキング解除の処理中もシグナリング接続を維持できるので、システムは有線と無線のアクセス ネットワークの間でメディア接続の切り替えを調整できます。

図 43　　Cius のフロー



Cisco QoS

Cisco Cius では現在、QoS に関するベストエフォート方式で、DV トラフィックを含むすべてのデータ トラフィックが処理されます。音声およびビデオ トラフィックだけがマークされ、QoS マーキングに従ってキューに入れらます。DV トラフィックが無線リンク上の他のデータ トラフィックよりも優先されるよう、管理者は、無線アクセス ポイントで QoS マーキングが実行されるように設定する必要があります（特定の DV トラフィック マーキングの推奨事項については、「QoS」の章を参照してください）。また、高品質なユーザ エクスペリエンスを実現するために、QoS マーキングをアクセス ポイントと HVD の間に一貫して適用する必要があります（詳細については、このガイドの「QoS」の章を参照してください）。Cius がドッキングされている場合、DV トラフィックと UC メディア トラフィックは別個のネットワーク パスを維持します。無線アクセスを求めたビデオおよび音声トラフィックとの競合がなくなるので、QoS マークの付いた DV トラフィックは、ネットワーク上のアクセス ポイントからデータセンターまで他のデータ トラフィックよりも優先されます。

スタンドアロン モードで使用されている（ドッキング解除されている）場合、すべてのトラフィックは WiFi インターフェイスを経由します。各種トラフィック フローの相対サイズにより、WiFi ネットワークの帯域幅がオーバーサブスクリプションになる状況が生じる可能性があります。前述のとおり、DV トラフィックが適切に優先順位付けされるように、QoS マーキングをアクセス ポイントで実行する必要があります。

テレフォニー コールでは、使用されているコーデックに対応する一定の RTP メディア フローが生成されます。たとえば、G.722 音声コールでは、コール中に（デュプレックス コールであるため）各方向で約 80 kbps が使用されます。次の表に、Cisco Cius がサポートする音声およびビデオ コーデックの公称帯域幅使用量を示します。

表 11　　コーデック / 帯域幅使用量

コーデック	帯域幅使用量
g.729	24 kbps、対称的
g.711、g.722	80 kbps、対称的
h.264	～ 768K

デスクトップ仮想化の帯域幅は、より非対称的になります。帯域幅使用量は、ユーザのホステッド仮想化デスクトップにおけるアクティビティの量にも関係します。たとえば、アイドル状態のデスクトップでは非活動的な少量のトラフィックしか生成されず、視覚的に機能豊富なアプリケーション（フラッシュ ビデオなど）を実行するデスクトップはより多くの帯域幅を使用します。

Cisco Cius タブレットがサポートするアプリケーションは、インストールされている場合にネットワーク帯域幅も使用します。たとえば、ローカル ブラウザを実行すると、DV および UC アプリケーションのトラフィック以外のトラフィック フローも生成されます。

ネットワークに対する影響を測る場合は、Cisco Cius タブレットの集約帯域幅使用量を考慮する必要があります。適切な Quality Of Service がエンドユーザに提供されるように、適切なネットワーク設計を実装してください。
http://www.cisco.com/en/US/docs/voice_ip_comm/ccmcd/deploy/9_2_1/english/ciusdply921.pdf

Cius には、（ドッキングされている場合）シグナリングおよびメディアの分離用に別個のイーサネット接続が 2 つ搭載されており、ドッキング解除またはドッキングされた構成で次の QoS マーキングがサポートされます。

表 12　Cius QoS サポート

トラフィック タイプ	DSCP	802.1p	WMM
音声	EF（46）	5	6
ビデオ	AF41（34）	4	5
呼制御	CS3（24）	3	4

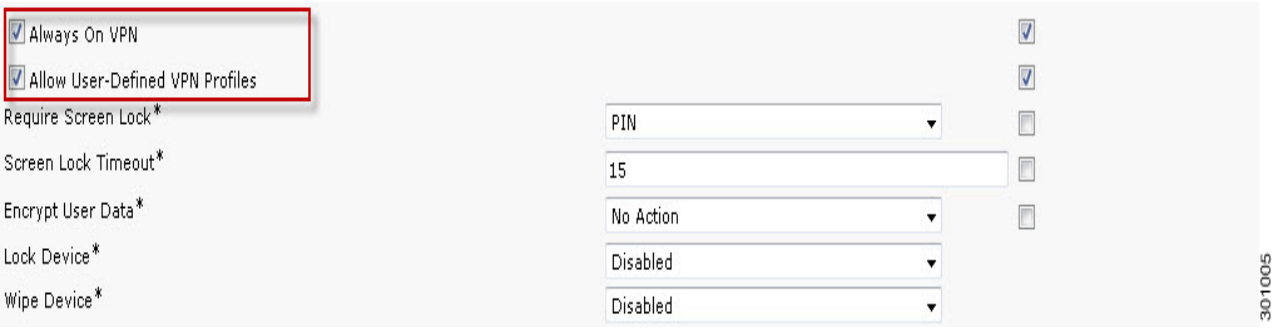
（注）　Cisco Cius は、DV トラフィックに対する QoS マーキングを実行しません。DV トラフィックのマーキングは、WiFi アクセス ポイントで設定してください。

Cius WiFi は、IEEE 802.1a/b/g/n と 20MHz および 40MHz のチャネル幅をサポートします。WiFi チャネルの詳細と、WiFi ネットワークの設計上の考慮事項については、http://www.cisco.com/en/US/docs/voice_ip_comm/ccmcd/deploy/9_2_1/english/ciusdply921.pdf を参照してください。

Cius セキュリティ

Cisco Cius は、SIP over TLS とセキュアなリアルタイムプロトコルをサポートし、UC シグナリングおよびメディア トラフィックを安全に送受信します。あらゆるタイプのトラフィックを保護するため、Cius はシスコの AnyConnect VPN をサポートし、Cisco UCM を介してネイティブにインストールおよび管理されます。AnyConnect VPN の機能により、DV および UC メディア トラフィックと、DV トラフィックを含むその他のデータは、Cius デバイスと企業のヘッドエンド セキュリティ ゲートウェイの間で安全に暗号化されます（IOS またはバージョン 8.0 以降を実行する Cisco ASA 5500 適応型セキュリティ アプライアンスが必要です）。

図 44



Apple iPad による DV エンドポイント

Apple iPad には、「Citrix Receiver for iPad」アプリケーションを実行する機能が備わっています。このアプリケーションは Apple App Store から無料で入手できます。「Citrix Receiver for iPad」を使用して、ユーザは Citrix「Store」を設定できます。この場合の Citrix「Store」は、データセンターに常駐する Citrix デスクトップ コネクション ブローカです。ユーザが Citrix Receiver アプリケーションをインストールして設定したら、そのユーザの HVD への接続を確立できます。デスクトップ仮想化デバイスとしての iPad には、キーボードのみをサポートして外部マウスはサポートしないという制限があります。Citrix Receiver ソフトウェアはこの制限に対処するため、Citrix Receiver のメニューから有効化できるタッチ スクリーン ベースのトラックパッドを提供しています。Apple iPad に Cisco AnyConnect SSL VPN アプリケーションをインストールすることで、そのデバイスを利用して、どこからでも安全にユーザの HVD にアクセスできるようになります。iPad 上で Cisco AnyConnect を使用すると、HVD トラフィックをセキュリティで保護し、iPad によって遠隔地から WiFi または 3G を介してあらゆる企業アプリケーションにアクセスすることができます。このアプリケーションの組み合わせにより、ユーザは、外出先からセキュリティを侵害することなく、自分の HVD にある重要な情報や文書を取得できます。Cisco AnyConnect および Citrix Receiver をサポートするには、Apple iPad が iOS 4.2 以降を実行している必要があります。Cisco AnyConnect for iPad は、8.0(3).1 以降を実行する ASA セキュリティ ゲートウェイでサポートされます。また、AnyConnect モバイル ライセンス機能用に Cisco ASA のライセンスを取得する必要があります。AnyConnect のライセンスに関する質問は、ac-mobile-license-request@cisco.com まで電子メールでお問い合わせください。

ASA の設定：
http://www.cisco.com/en/US/partner/docs/security/asa/asa82/configuration/guide/svc.html#wp1094561

iPad 上の AnyConnect に関するユーザ ガイド：
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect24/ios4.2-user/guide/ipad-ugac-ios4.2.html

Citrix Receiver：
http://community.citrix.com/display/ocb/2010/04/01/Top+10+Business+Uses+For+the+iPad

DV エンドポイント管理

DV エンドポイントの管理ソフトウェアは通常、エンドポイントの製造元か HVD ソフトウェア ベンダー、またはその両者から提供されます。Cisco VXC-2112 および VXC-2212 では、管理者は Virtual Experience Client Manager を使用して大規模な VXC ゼロ クライアントの導入を管理できます。Cisco Virtual Experience Client Manager は、次の機能をサポートします。

- HTTPS ベースのサーバ/クライアント通信
- HTTPS ベースのサーバ/リモート ソフトウェア リポジトリ通信
- HTTPS ベースのデバイス ソフトウェア イメージング
- 自己署名の HTTPS 証明書を認証する機能
- クライアントと正当な管理サーバとのペアリングを行うための、サーバ/クライアント ペア暗号化キー
- DMZ をインストールするために、VXC-M サーバから資産データベースを隔離する機能

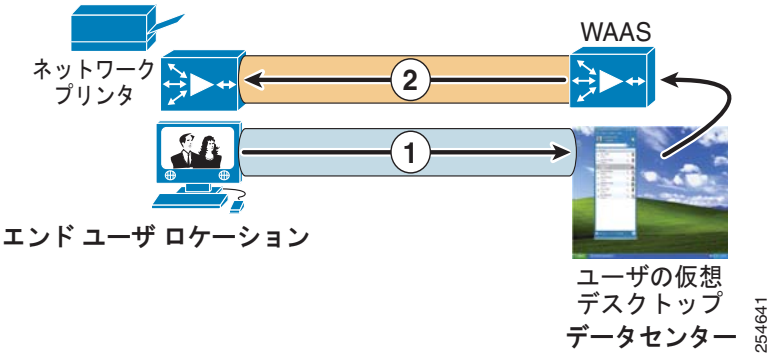
DV エンドポイント管理の詳細については、「管理と運用」を参照してください。

DV エンドポイントでの印刷（ネットワーク プリンタ）

ユーザがユーザのエンドポイントと同じ場所にあるネットワーク プリンタに文書を送信すると、その印刷フローは実際にはデータセンター内から発信されます。ネットワーク プリンタへの印刷フローは実際、デスクトップ ディスプレイ プロトコル外で伝送され、WAAS による最適化が可能です。Cisco WAAS は、印刷プロトコルを認識し、WAN 帯域幅使用量を減らすためにそれを圧縮し、生成された印刷ファイルをリモート ブランチに送信できます（図 45 を参照）。リモート プリンタが使用中の場合は、キューイング機能も提供します。この印刷の最適化とキューイングの詳細については、次の場所にある Cisco Wide-Area Application Services の設定ガイドを参照してください。

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v421/configuration/guide/cnfgbook.pdf

図 45　　ネットワーク印刷のデータ フロー



1. ローカル ネットワーク プリンタでの文書の印刷要求は、デスクトップ ディスプレイ プロトコル内で伝送されます。
2. データセンターの DV デスクトップからの印刷ジョブは、同じくデータセンター内にあるプリント サーバに送信されます。その後、プリンタにストリーム配信されます。

（注）　Cisco WAAS は、このプロトコル ストリームを認識し、最適化できます。

DV エンドポイントから USB 接続の周辺機器（ストレージまたはプリンタ）へのアクセス

多くの場合、DV エンドポイントには USB ポートが搭載されており、ストレージ デバイス（ハード ディスク、「サム（小さな）」ドライブなど）やプリンタに接続することができます。USB ポートへの物理的なアクセスによってこのような周辺機器への接続が可能になりますが、ポートの論理的な有効化を制御するのはコネクション ブローカです。

USB ポートのアクセスは、デバイスではなく、ユーザに伴うポリシーです。たとえば、あるユーザに DV エンドポイント上のストレージ機器の使用が許可されているとして、そのユーザがログアウトした後で別のユーザが同じ DV エンドポイントにログインすると、ストレージへのアクセスは無効になります。USB 周辺機器へのアクセスが特定のユーザに対して有効である場合、データセンター内の USB 周辺機器へのデータ フローはそのユーザのホステッド仮想デスクトップから発信されます。USB 周辺機器へのすべてのファイル ストレージまたは印刷操作によって生じる、DV エンドポイントへのネットワーク上のデータ フローは、ディスプレイ プロトコル内でカプセル化されます。

USB アクセスの有効化および無効化の詳細については、このマニュアルの「Cisco VXI セキュリティ」の章を参照してください。

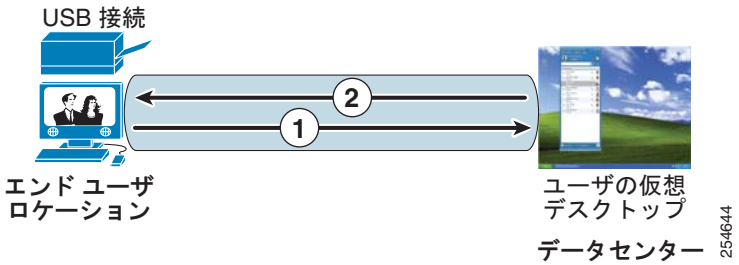
Citrix（HDX ポリシー）

Citrix XenDesktop 5 では、プロトコルが印刷アクションで使用する帯域幅を次のように調整できます。

- HDX ポリシーの使用 --> ユーザ設定によって、印刷リダイレクトの帯域幅制限を有効または無効にします。
- 全体的なセッション帯域幅制限を使用して、各ユーザ セッションで使用される帯域幅全体を制限します。このタスクは、インストールされている XenApp のバージョンに応じて、XenDesktop 5 の Desktop Studio 管理コンソール、XenDesktop 4 の Delivery Services Console、あるいは、XenApp Advanced Configuration または Presentation Server Console として知られるツールで実行できます。

http://support.citrix.com/proddocs/topic/xenapp6-w2k8-admin/ps-printing-limiting-printing-bandwidth-all.html

図 46　　USB 印刷データ フロー



1. ローカル ネットワーク プリンタでの文書の印刷要求は、デスクトップ ディスプレイ プロトコル内で伝送されます。
2. データセンター内の HVD デスクトップからの印刷ジョブは、同じデスクトップ プロトコル内でローカル プリンタ /USB デバイスに送信されます。

DV テスト対象エンドポイント

表 13 に、Cisco VXI 設計を確認するためのテストで使用されるエンドポイントのリストを示します。これは、サポートされているベンダーやデバイスの包括的なリストではありません。

表 13　　エンドポイント

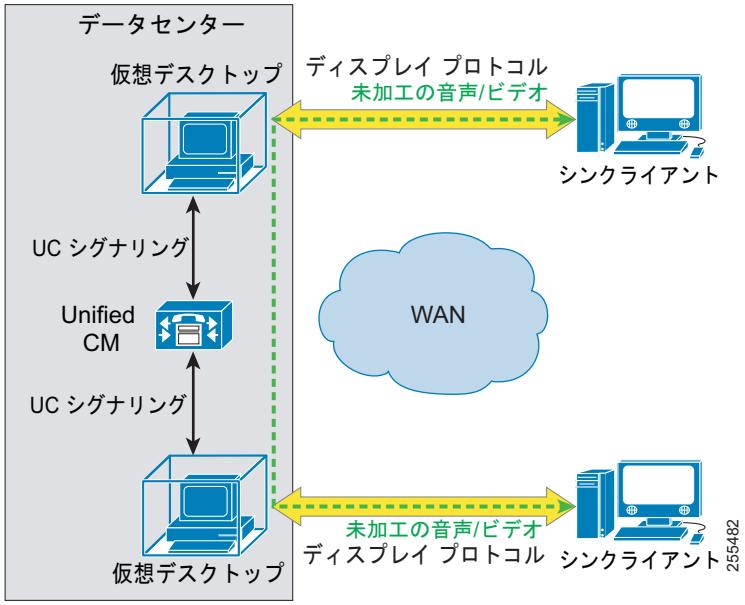
DV エンドポイント タイプ	ベンダー / デバイス	テクノロジー サポート	説明	ベンダー ページ
ゼロ	Cisco VXC-2212	Citrix HDX/RDP	Citirx Xendesktop	cisco.com
ゼロ	Cisco VXC-2112	Citrix HDX/RDP	Citirx Xendesktop	cisco.com
リッチメディア デバイス シック	Apple iPad	Citrix HDX	Citrix Receiver	cisco.com または apple.com
ゼロ	Wyse Xenith	Citrix HDX	Citrix XenDesktop	Xenith

DV エンドポイント タイプ	ベンダー / デバイス	テクノロジー サポート	説明	ベンダー ページ
シン	Wyse C10LE Wyse R90LW Wyse R90L7 Wyse X90LW Wyse Z90SW Wyse Z90DW Wyse Z90S7 Wyse Z90D7	Citrix HDX Microsoft RDP	Citrix XenDesktop	C10LE R90LW R90L7 X90L Z90SW Z90DW Z90S7 Z90D7
シン	DevonIT TC5XW DevonIT TC5DW	Citrix HDX Microsoft RDP	Citrix XenDesktop	TC5
シン	IGEL UD7	Citrix HDX Microsoft RDP	Citrix XenDesktop	UD7

Cisco VXI システム

一般的な HVD 接続は、エンドポイントと HVD 間におけるグラフィック情報、ユーザ入力（マウス、キーボードなど）情報、およびマルチメディア情報（音声およびビデオ テレフォニーなど）の伝送を IP ベースのディスプレイ プロトコル接続に依存します。このアプローチにより、あらゆる情報タイプ（音声、ビデオ、ディスプレイ アップデート、USB ベースの情報など）がエンドポイントと HVD 間の同一の IP 接続に配置されます。ディスプレイ プロトコルは、ネットワーク サービスに対して不透明であるため、QoS、CAC、およびコーデック ネゴシエーションをディスプレイ プロトコル内の個々のメディア ストリームに適用することはできず、ユーザ エクスペリエンスが最適でなくなる可能性があります。図 47 に、一般的な DV 展開を示します。

図 47　DV アプライアンス

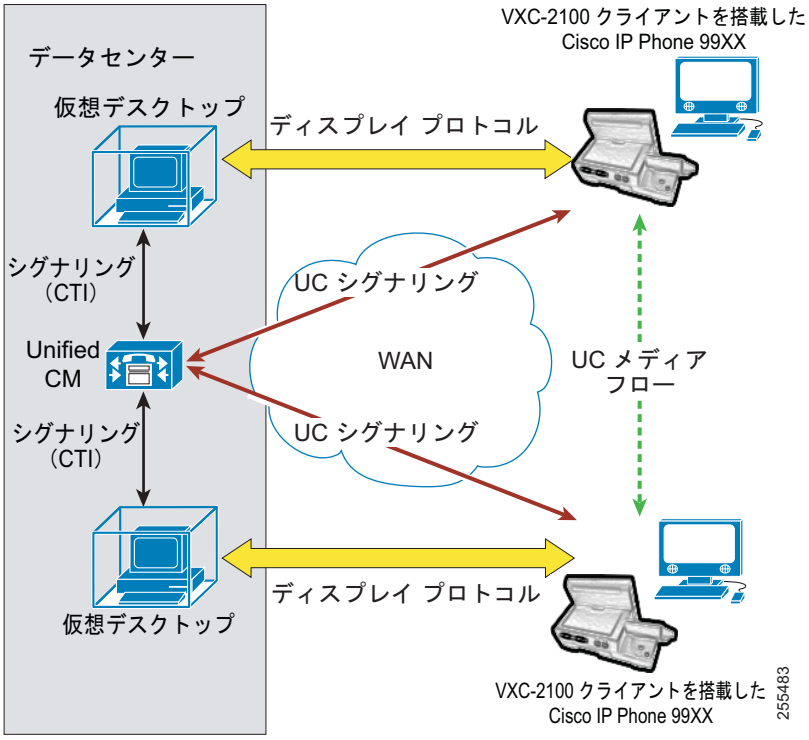


Cisco VXI システムでは、UC エンドポイントおよび DV エンドポイント アプライアンスの組み合わせを使用してメディアを分離することで、最適なユーザ エクスペリエンスを実現できます。この場合、音声およびビデオ メディア ストリームがディスプレイ プロトコルから分離され、データセンターをバイパスして UC エンドポイント間のポイントツーポイントで終了します。現在、次のネットワーク サービスを適用できます。

- メディア フローの遅延、ジッタ、およびドロップを防止する QoS
- コールの参加者間で最適化された実際のパスに基づくコール アドミッション制御
- 関連付けられた HVD ではなく、ネットワーク内におけるユーザ エンドポイントの場所に基づいた CODEC の選択

図 48 に、分離されたトラフィックのフローを示します。

図 48　分離されたトラフィックのフロー



Cisco Unified Communications アプリケーション

Cisco VXI システムでは、Cisco Client Services Framework を利用するデスクトップ アプリケーションの導入により Cisco Unified Communications がサポートされ、Cisco Unified IP Phone の制御が可能になります。このようなアプリケーションの例としては、Cisco Unified Personal Communicator、Cisco Unified Communications Integration for WebEx Connect、および Cisco Unified Communications Integration™ for Microsoft Lync が挙げられます。これらのアプリケーションは HVD 内で実行でき、ユーザのデスクトップにある電話機の制御に使用できます。Cisco Unified Personal Communicator を使用する Cisco VXI エンドユーザは、連絡先情報の管理（ディレクトリ ルックアップ）、同僚のリアルタイムの在籍状況の取得（プレゼンス）、オンライン チャット（インスタント メッセージング）、および音声とビデオによる IP テレフォニーや会議を行うことができます。

Cisco Unified Personal Communicator、UC Integration™ for Microsoft Lync、および UC Integration for WebEx Connect アプリケーションは、ソフト フォン モードかデスク フォン制御モードのいずれかで設定できます。UC メディアがディスプレイ プロトコル内に配置されるため、Cisco VXI ソリューションではソフト フォン モードはサポートされません。デスクフォン制御モードでは、物理的な Cisco Unified IP Phone を使用し、デスクトップ上のアプリケーションを介して電話機を制御できます。また、コールの音声とビデオは、DV ではなく IP 電話によって処理されます。このアプリケーションをどのように展開すべきかという点で、実際問題となるのはコールの音声ストリームとビデオ ストリームです。前のセクションで説明したとおり、ソフト フォン モードの音声ストリームとビデオ ストリームは DV の通過を試み、そのデスクトップ ディスプレイ プロトコル内で伝送されている他のアプリケーションとの区別ができないため、音声ストリームとビデオ ストリームを分離したまま、通常どおりにネットワーク内で処理できるデスクフォン制御モードで UC アプリケーションを実行することが推奨されます。

http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/admin/8_5_1/ccmsys/a08video.html

http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/docguide/8_5_1/dg851.html

サポートされている UC アプリケーションのソフトウェア バージョンについては、http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VXI/configuration/VXI_Config_Guide.pdf にある『Cisco Virtualization Experience Infrastructure Configuration Guide』を参照してください。

図 49 に、Cisco Unified Personal Communicator の一般的なコール フローを示します。

図 49　　HVD から Cisco Unified Personal Communicator コールを発信するためのデータ フロー

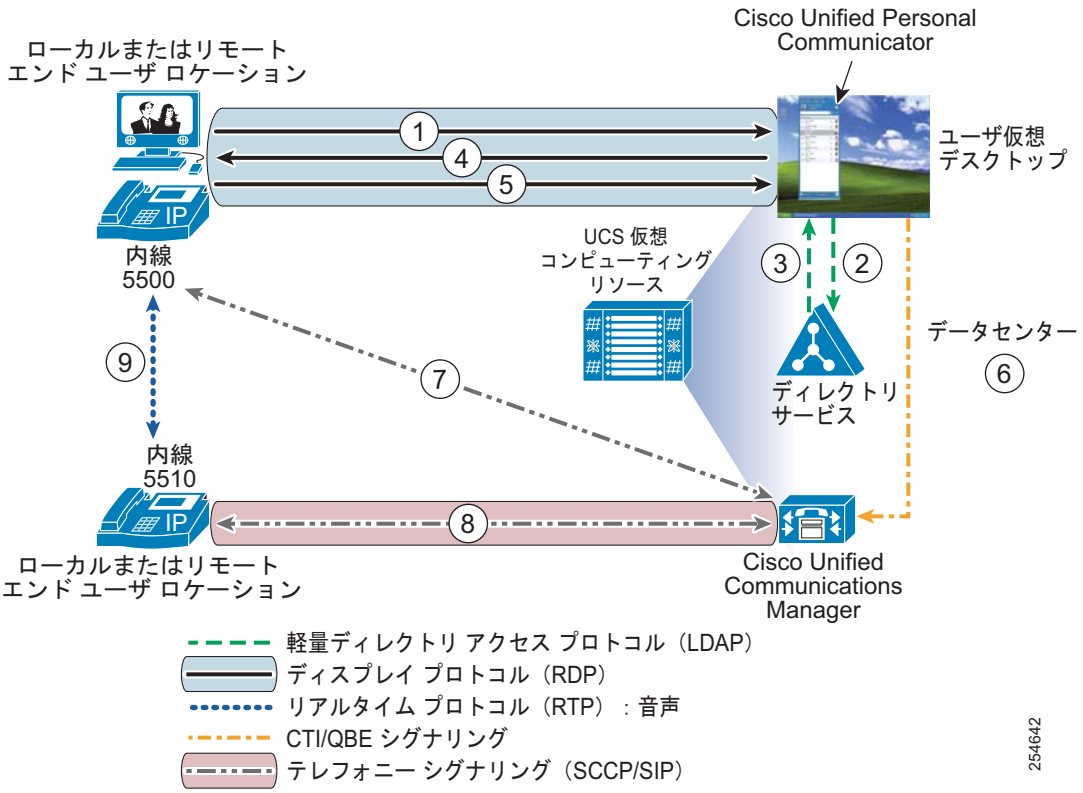


図 49 では、DV エンドポイントに各ユーザの仮想デスクトップ環境が視覚的に表示され、キーボード、マウス、またはタッチ スクリーン入力デバイスを介したユーザ入力がサポートされます。ユーザのデスクトップは、Cisco Unified Personal Communicator のインスタンスで設定され、デスク フォンを介したインスタント メッセージング、プレゼンス、ディレクトリ ルックアップ、およびテレフォニー制御が可能になります。デスク フォンは、音声およびビデオ メディアの処理を行います。

ユーザのすべてのアクションがディスプレイ プロトコル内でデータセンターの仮想デスクトップにリレーされることに注意してください。また、他の画面アップデートと同様に、Cisco Unified Personal Communicator 画面に対するすべての仮想アップデートは、ディスプレイ プロトコル内で仮想デスクトップからユーザの DV エンドポイントの画面まで伝達されます。

データセンター内の DV デスクトップにある Cisco Unified Personal Communicator でユーザ入力が処理される場合、DV は同じくデータセンター内にあり、おそらくは同じ UCS 領域内にある適切なコラボレーション サーバと通信します。デスクトップがデータセンター内のプラットフォーム上で稼動しているため、コールを制御するすべての通信がデータセンター内に留まることに注意してください。次に、このコール処理の完全なデータ フローを示します。

1. DV ユーザが、Cisco Unified Personal Communicator ウィンドウに John Doe という名前を入力します。ディスプレイ プロトコルを介して、その情報はユーザの仮想デスクトップ インスタンスにリレーされます。この入力は、ユーザがゲスト OS にローカル接続されたキーボードを利用したかのように、Cisco Unified Personal Communicator で受信されます。
2. Cisco Unified Personal Communicator は Lightweight Directory Access Protocol（LDAP; 軽量ディレクトリ アクセス プロトコル）を使用して、LDAP 互換のディレクトリ サービスに John Doe の番号を照会します。
3. 連絡先情報の照会結果が Cisco Unified Personal Communicator に戻されます。
4. Cisco Unified Personal Communicator による処理が終わると、この情報はリモート ディスプレイ プロトコルを通じてユーザのディスプレイに戻されます。
5. DV ユーザがデスクトップの Cisco Unified Personal Communicator GUI を通じて連絡先へのコールを開始すると、同様のディスプレイ プロトコルのアップデートがデータセンター内の DV インスタンスに伝送されます。
6. Computer Telephony Integration（CTI; コンピュータ テレフォニー インテグレーション）制御データが Cisco Unified Personal Communicator から Cisco Unified Communications Manager に送信され、5500 から 5510 へのコールの発信が要求されます（図 49 の 6 番）。
7. Cisco Unified Communications Manager がコール要求のダイヤル プラン処理を実行し、宛先電話機の着信番号を解決し、デスク フォンに対してコール受信者への発呼を指示します。この処理は、両方の電話機との呼制御交換によって実行されます（図 49 の 7 番と 8 番）。
8. いったん確立されたテレフォニー コールのメディアは、データセンターの仮想デスクトップを通過せずに、2 台の IP 電話機間で直接確立されます（図 49 の 9 番）。これは、ユーザ エクスペリエンスの品質維持に欠かせない側面です。ネットワークの Quality of Service（QoS）ポリシーによって、ドロップ、ジッタ、および遅延の障害からテレフォニー メディア フローが保護されます。これらの障害は、フローがディスプレイ プロトコル内でカプセル化された場合に悪影響を及ぼすことがあります。IP テレフォニー エンドポイントは、最も直接的に使用できるネットワーク パスでメディア ストリームを直接接続できることにも注意してください。

（注） コールは発信される前に、Cisco Unified Communications Manager によるコール アドミッション制御の検証を受けます。ネットワークにコールを通過させるだけの十分な帯域幅がない場合、そのコールは Cisco Unified Communications Manager の Automated Alternate Routing（AAR; 自動代替ルーティング）機能によって処理され、Cisco Unified Communications Manager のポリシー設定に従って QoS の保証なしで処理を許可されるか、ブロックされます。

（注） 発信されたコールのタイプ（音声、ビデオ）と、コールの発信に使用されるコーデックは、Cisco Unified Communications Manager のポリシー設定とエンドポイントの機能によって異なります。発信側と受信側の両方のエンドポイントがビデオ ストリーミングをサポートしている場合は、Cisco Unified Communications Manager のポリシーおよび CAC の検証に基づき、コールをビデオ コールとして発信できます。エンドポイントの機能、Cisco Unified Communications Manager のポリシー設定、またはネットワーク条件が音声コールにしか対応していない場合、コーデックは Cisco Unified Communications Manager の設定に基づいて選択されます。

VXC および UC エンドポイントのシングル サインオン

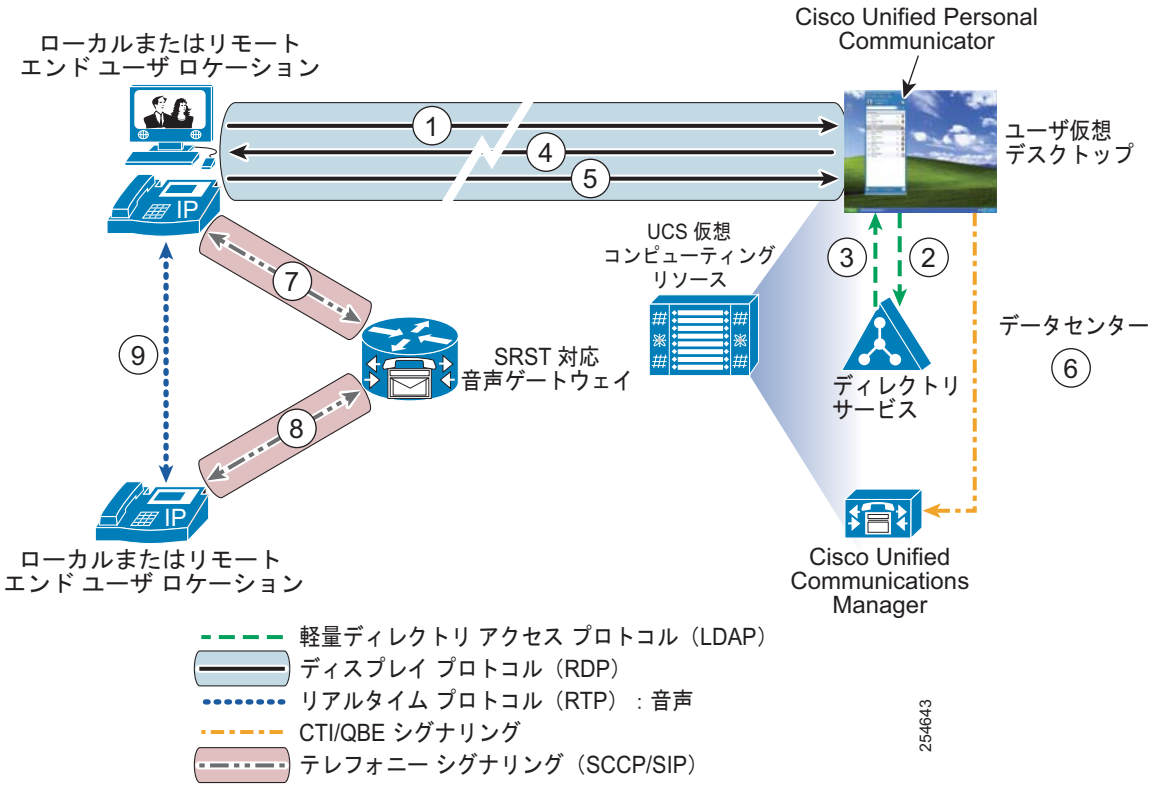
ユーザが HVD にログインする場合、シングル サインオン プロセスがサポートされ、ユーザは資格情報を 1 度入力するだけで済みます。ユーザが必要な資格情報を VXC GUI サインオン画面に入力すると、そのユーザは適切な HVD コネクション ブローカにロギングされ、HVD への接続が自動的にロギングおよび開始されます。ユーザが HVD に接続すると、Cisco Unified Personal Communicator、UC Integration™ for Microsoft Lync、または UC Integration for WebEx Connect が自動的に起動します。最初のサインオンが手動で実行されると、UC ユーザの資格情報が保存され、UC デスクフォン制御アプリケーションへの自動サインインが有効になります。HVD へのシングル サインオンは、各 Virtualization Experience Client に手動で設定するか、Virtualization Experience Client Manager を使用する 2 通りの方法でサポートされます。Virtual Experience Client-Manager（VXC-M）を使用する場合、電源を入れるとサインイン資格情報を保持する .ini ファイルが Virtual Experience Client デバイスにプッシュされます。VXC-M の詳細については、「管理と運用」の章を参照してください。

（注） HVD および UC アプリケーションのシングル サインオンは、各エンド ユーザが専用のデスクフォンまたは UC エンドポイントを所有している展開でのみサポートされます。エクステンション モビリティが実装されている場合は、シングル サインオンを利用できません。エクステンション モビリティが使用されている場合、エンドユーザは、ハード デスクフォンにログインしてから HVD 環境にログインしなければならない 2 ステップ ログイン プロセスを利用します。

Cisco Unified Personal Communicator、HVD、および SRST

SRST は、Cisco VXI でサポートされています。図 50 に、DV、UC エンドポイント、およびデータセンター間の WAN リンクが失われた場合のフェールオーバー時のコール フローを示します。Cisco Unified Personal Communicator を実行している HVD は、同じデータセンターにある Cisco Unified Communications Manager に引き続き接続します。ただし、Cisco Unified Communications Manager からハード フォンへの接続は失われます。エンドユーザの場所に SRST サービスを提供できる音声ゲートウェイが装備されている場合、電話機をそのゲートウェイに再登録できます。これにより、電話機は引き続きコールの発着信を行うことができます。

図 50　　SRST シグナリングおよびメディア フロー



データセンターへのネットワーク サービスが回復したときに、前述のハード フォン制御設定がどのように反応するかを予測することは困難です。Cisco Unified Personal Communicator アプリケーションが、Cisco Unified Communications Manager との接続を失うことはありません。接続が回復した電話機は、Cisco Unified Communications Manager との接続を再開できます。エンドユーザがデスクトップとの接続を再び確立するタイミングによって、予測不可能な動作が発生します。これが電話機と Cisco Unified Communications Manager との再接続前である場合、エンドユーザは Cisco Unified Communications Manager が電話機の存在を認識する前にハード デスク フォンの制御を試みる可能性があります。このような問題を回避する最良の方法として、オフフックにして Cisco Unified Personal Communicator のステータスの変化を確認することで、Cisco Unified Personal Communicator が電話機のステータスを正しく反映できることを確認します。まれに、このステータスが再同期されない場合があり、電話機の適切なステータスを再確立するため、HVD 内で Cisco Unified Personal Communicator を再起動しなければならない場合があります。

Cisco Unified SRST の詳細については、次の場所にある『Cisco Unified SRST Configuration Guide』を参照してください。

http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/admin/srst/configuration/guide/SRST_SysAdmin.pdf

ホステッド仮想環境でデスクフォン制御を使用し、UC ビデオおよび音声コール ソリューションを配信するための基本的な設定については、次の URL にある『Cisco Virtualization Experience Infrastructure Configuration Guide』を参照してください。

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VXI/configuration/VXI_Config_Guide.pdf

Cisco VXI システム アプリケーションによる UC コラボレーションの有効化

HVD ユーザのデスクトップにインストールされたアプリケーションに関連づけられているインストレーション、設定、およびセキュリティには、従来のデスクトップでインストールされているように、すべて同一の企業ポリシーおよび手順を適用する必要があります。これには、企業の IT インフラストラクチャの外部にあるデスクトップにアプリケーションをロードする機能も含まれます。ユーザが従来のデスクトップやラップトップ デバイスにアプリケーションをインストールできないように企業ポリシーで指示されている場合、シン クライアントのローカル OS もロックダウンする必要があります。HVD 環境で実行する個々の製品の機能に問題がなければ、データの場所をデータセンターに移動しても、ウイルス保護ポリシー、データのバックアップ手順、および企業内のパーソナル セキュリティ権限はすべてそのままにしてください。

Cisco VXI ソリューションでシスコのリッチメディア コラボレーション エクスペリエンスを実現するため、次の UC アプリケーションの検証が行われました。検証済みのアプリケーションは、Cisco Unified Personal Communicator、Cisco Unified Communications Integration™ for Microsoft Lync、Cisco Unified Communications Integration™ for WebEx Connect、および Cisco QUAD です。コンタクト センター アプリケーション用として、XenApp 仮想化環境では Cisco Agent Desktop（CAD）がサポートされています。Cisco Agent Desktop は Cisco Unified Contact Center Express 用のソフトウェア スイートで、緊密に統合された Computer Telephony Integration（CTI; コンピュータ テレフォニー インテグレーション）に対応し、生産性の向上と管理を目的としています。

XenApp を使用した Cisco CAD アプリケーションへのアクセスは、次の導入モデルでサポートされます。

1. アプリケーションのリモート処理：CAD アプリケーションは、VXC-2112 または 2212 クライアントによって XenApp ストアから直接アクセスされ、CAD ユーザ インターフェイスがクライアント画面に公開されます。
2. ホステッド仮想デスクトップからのアプリケーションのリモート処理：エージェントが専用の仮想デスクトップにログインし、HVD から CAD の XenApp インスタンスを起動します。
3. Hosted Shared 仮想デスクトップからのアプリケーションのリモート処理：エージェントは、Microsoft Terminal Services を使用して Windows OS インスタンス（Windows 7 または Windows Server）の共通インスタンスを共有します。また、共有デスクトップに接続し、そこから CAD の XenApp インスタンスを起動できます。
4. ターミナル セッション ベースの公開：上記の 3 と同様に、エージェントは共通の Windows OS インスタンスを共有します。ただし、CAD アプリケーションは共有している Windows OS インスタンスにインストールされ、HVD を共有している複数のエージェントから直接アクセスされます。ユーザ ログインが実行されたり、パーソナライゼーションが侵害されたりすることはありません。

仮想化された Cisco Agent Desktop の詳細については、http://www.cisco.com/en/US/docs/voice_ip_comm/cust_contact/contact_center/ipcc_enterprise/ipccenterprise8_0_1/design/guide/CAD-thin-client.pdf を参照してください。

（注） VXI システム内の Cisco Unified Personal Communicator、Cisco UC Integration for Microsoft Lync（CUCILync）および Cisco UC Integration for WebEx Connect（CUCIConnect）の検証に関する詳細については、『VXI Release Notes』および「パフォーマンスとキャパシティ」の章を参照してください。VDI 環境におけるサポートを確認するには、上記の UC アプリケーションに関する製品マニュアルを参照することが推奨されます。また、これらのアプリケーションを展開する前に、使用する環境内で十分な検証を行うことが強く推奨されます。

関連情報

表 14 に、この章で説明したハードウェアおよびソフトウェアを含む特定のベンダーに関する詳細情報へのリンクを示します。

表 14　　エンドポイントとアプリケーションのリンク

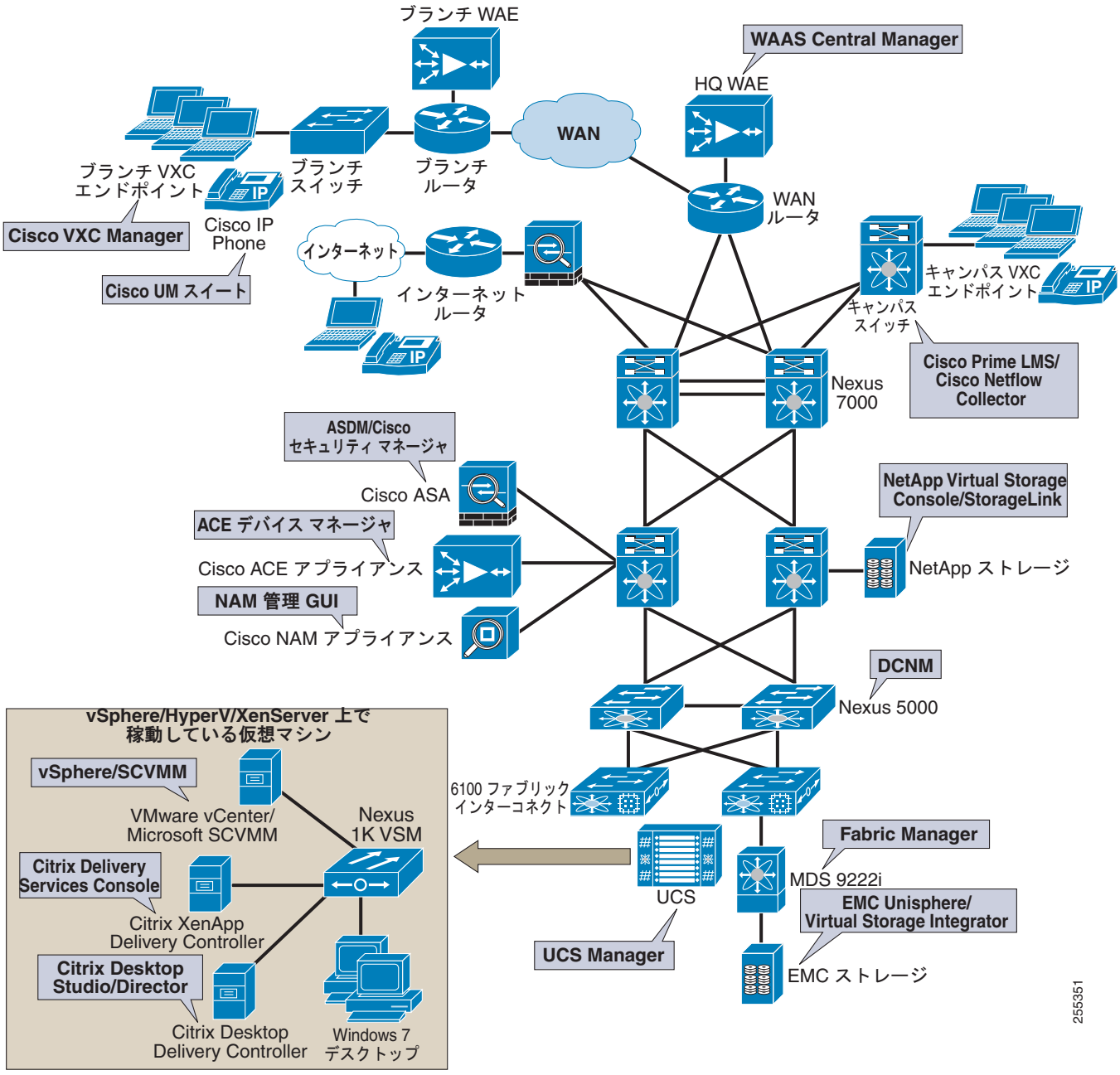
『Cisco Wide Area Application Services (WAAS) Configuration Guide』
http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v421/configuration/guide/cnfgbook.pdf
『Citrix Guide for Limiting Printing Bandwidth』
http://support.citrix.com/proddocs/index.jsp?topic=/xenapp5fp-w2k8/ps-printing-limiting-printing-bandwidth-all.html
『Cisco Unified SRST Configuration Guide』
http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/admin/srst/configuration/guide/SRST_SysAdmin.pdf
『Cisco Unified Communications 8.X SRND』
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/8x/uc8xsrnd.pdf
『Cisco Unified Personal Communicator User's Guide』
http://www.cisco.com/en/US/docs/voice_ip_comm/cupc/7_0/english/user/guide/windows/CUPC_7.0_UG_win.pdf

管理と運用

エンドツーエンドの Cisco Virtual Experience Infrastructure（Cisco VXI; シスコ仮想化エクスペリエンス インフラストラクチャ）展開には、多数のユーザに対する継続的なサービスのプロビジョニング、モニタリング、およびトラブルシューティングを可能にする総合的な管理アーキテクチャが必要です。この章では、Cisco VXI システムを管理するためのベスト プラクティスとガイドラインを示します。また、日常的な運用（展開後）に関して Cisco VXI サービスの提供に伴う主なタスクとツールについて説明します。システム管理の必要性を理解することは、市販の管理ツールを検証し、そのようなツールを社内で開発するためのベースとなります。

エンドツーエンド システム内のハードウェアおよびソフトウェア コンポーネント（キャンパス、ブランチ オフィス、およびインターネット）の数を考えると、Cisco VXI システムの管理は容易ではありません。これらのコンポーネントによって、ローカルおよびリモートのエンド ユーザや管理者にサービスが提供されます（デスクトップ仮想化、ネットワーク、ストレージ、コンピューティング、セキュリティ、ロード バランシング、WAN 高速化、およびユニファイド コミュニケーション サービスなど）。管理者には、ネットワーク、ストレージ、データベース、およびデスクトップ管理などさまざまなテクノロジーやサービスを管理することが期待されます。

図 51　Cisco VXI システムの管理に使用されるツール



Cisco VXI の管理と運用のアーキテクチャ

このセクションでは、Cisco VXI システムの管理アーキテクチャに関する主な側面について説明します。運用管理、サービス管理、サービス統計情報管理、およびプロビジョニング管理が、Cisco VXI の主な管理要素になります（表 15）。考慮すべきその他の重要な分野には、スケーラビリティ、ハイ アベイラビリティ、管理トラフィック、デスクトップ管理、およびエンドポイント管理があります。

表 15　Cisco VXI 管理アーキテクチャ

Cisco VXI 管理アーキテクチャの主要な側面
運用管理は、リアル タイムですべての要素のステータスをモニタし、診断する機能です。これには、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）、syslog、および XML ベースのモニタリングのほか、HTTP ベースのインターフェイスを使用したデバイスの管理も含まれます。また、エンドポイントと仮想デスクトップのインベントリおよび資産管理（ハードウェアとソフトウェア）も含まれます。
サービス管理は、ユーザ セッションのステータスと Quality of Experience（QoE）をモニタし、トラブルシューティングする機能です。これには、Cisco Network Analysis Module（NAM; ネットワーク解析モジュール）、NetFlow、Wireshark などのパケット キャプチャおよびモニタリング ツールを使用したセッションのモニタリングが含まれます。また、デスクトップ仮想化管理者は、エンドポイントや仮想デスクトップにリモートからアクセスし、パフォーマンスを確認して、帯域幅と遅延の測定結果を収集できるようになります。リアル タイムでコンピューティング、メモリ、ストレージ、およびネットワーク使用率を測定して、ボトルネックやサービス低下の原因を識別する機能も提供します。仮想デスクトップ セッションに関するセッション詳細レコードから、接続障害や品質の問題を知ることもできます。
サービス統計情報管理は、品質およびリソース使用率の測定結果を収集し、運用、インフラストラクチャの最適化、およびキャパシティ プランニングに役立つレポートを生成する機能です。測定結果には、システム全体にわたるセッション ボリューム、サービスの可用性、セッション品質、セッション詳細レコード、リソース使用率、およびキャパシティを含めることができます。レポートは、課金のために使用したり、サービス レベルの管理に使用したりできます。
プロビジョニング管理は、バッチ プロビジョニング ツールとテンプレートを使用してエンド ユーザ、仮想デスクトップ、およびエンドポイントのプロビジョニングを行う機能です。ベンダーから提供される API（XML）を自動およびセルフサービス プロビジョニングに使用できます。これには、エンドポイントおよび仮想デスクトップ上のソフトウェア イメージとアプリケーションの管理が含まれます。

スケーラビリティ

Command-Line Interface（CLI）を使用して各デバイスに対するプロビジョニングや管理を行う代わりに、管理ツールを使用して、中央集中化されたコントロール ポイントを介した多数のエンドポイント管理に規模を拡大できます。大規模な展開をモニタするには、ポーリング、SNMP トラップ、および syslog メッセージの使用が不可欠です。また、GUI ベースのツールは、複雑な展開をナビゲートしたり、詳細なレポートを表示したりするのに役立ちます。多くのデバイス管理ツールは、ワークフローの自動化に使用できる API または CLI も備えています。この機能は特に、多数のユーザ、デスクトップ、またはエンドポイントを追加するときに役立ちます。

ハイ アベイラビリティ

ハイ アベイラビリティを確保するには、冗長構成（プライマリ サーバとセカンダリ サーバ）で管理アプリケーションを展開し、設定とデータベースを定期的にバックアップします。また、リソースを効率的に使用し、仮想マシン マイグレーション（VMware vMotion）、VMware Distributed Resource Scheduling（DRS; 分散リソース スケジューリング）、および VMware Fault Tolerance（FT）などのハイパーバイザ インフラストラクチャが提供するハイ アベイラビリティ機能を活用するために、仮想マシンに管理アプリケーション サーバを導入します。専用サーバには多くのアプリケーションを配置する必要がありますが、可能な場合はリソースを節約するため、同じ仮想マシン上でアプリケーションとサーバを統合することを検討してください。通常、管理サーバの配置に最も適した場所は、他の重要なリソースが存在するデータセンター内です。

管理トラフィック

一般的なガイドラインとして、管理トラフィック用の IP ネットワークは別にすることが推奨されます。たとえば、リモート アクセス、SNMP、syslog、および FTP トラフィック専用の IP サブネットおよび VLAN は、必要に応じたアウト オブ バンド管理が可能です。このアプローチにより、エンドユーザおよび管理トラフィック フローが使用可能な帯域幅を奪い合ったり、妨害したりすることのないよう、また、デバイスのリセットやプロビジョニングが必要な場合にデバイスへのリモート アクセスが損なわれないようにすることができます。また、このアプローチによって、エンドユーザおよび管理トラフィックが同じインターフェイスを共有するときに起こり得る、ネットワーク セキュリティおよび可用性に対する脅威を軽減することができます。

デスクトップの仮想化によって、従来サーバや管理トラフィックのロードに使用されるインフラストラクチャにユーザ トラフィックが集中するデータセンターでは、管理およびユーザ トラフィックの隔離が特に重要です。

管理トラフィックの隔離は、一部のシステムでは実用的でない場合もあります。たとえば、エンドポイントには通常 1 つのイーサネット ポートがあり、このポートをエンドユーザ トラフィックと管理トラフィックの両方に使用しなければなりません。コストやネットワーク アドレスの節約を考えると、WAN 上の管理トラフィック用に別個のアウトオブバンド ネットワークを設定することも実用的でない場合があります。このような場合には、特定のタイプの管理トラフィック（SNMP ポーリング）が大量の帯域幅を使用する可能性があり、標準の Quality of Service（QoS）テクニックを使用して適切なスケジューリング、モニタリング、場合によってはレート制限を行う必要があることに留意してください。

各管理ツールでは、デバイスとの通信に特定のプロトコル セットを使用します。各ツールで使用されるプロトコルとポートの完全なリストについては、ベンダーのマニュアルを参照してください。これらのポートがすべての中間ルータ、スイッチ、およびファイアウォールで開かれていることを確認してください。

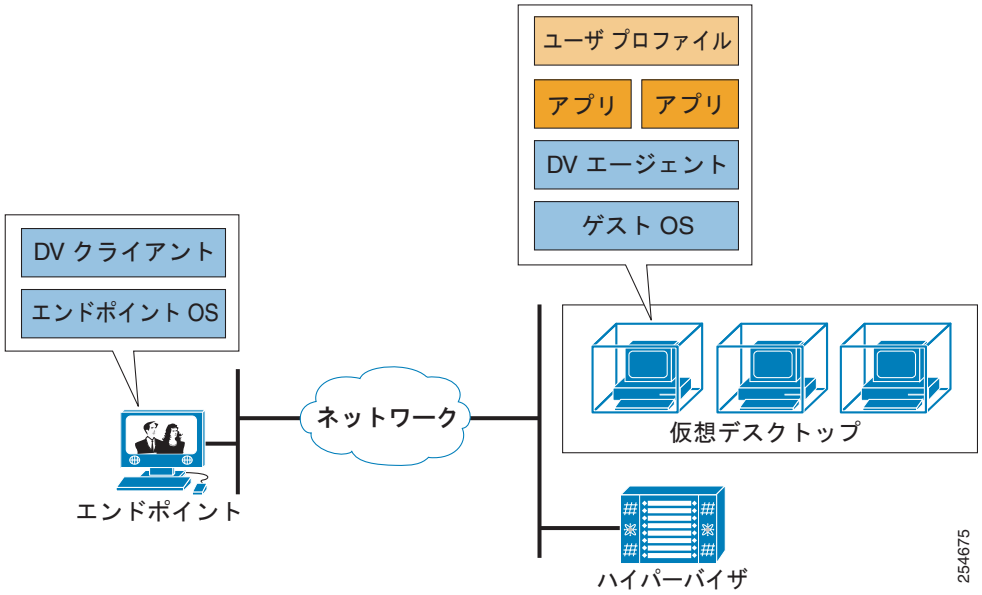
デスクトップ管理

デスクトップ仮想化環境では、エンド ユーザに関連付けられたプールに仮想デスクトップが編成されます。ユーザとプールの関連付けにより、ユーザはそのプール内のデスクトップにアクセスできるようになります。専用プールは、個人用デスクトップのように、1 人のユーザが関連付けられた 1 台のデスクトップで構成されます。共有プールには、複数のユーザが関連付けられた複数のデスクトップが含まれます。共有プールでは、ユーザに対するデスクトップの割り当てをいくつかの方法で行うことができます。

ユーザ割り当ては管理設定を通じて静的に実行することも、接続マネージャを使用して動的に実行することもできます。接続マネージャを使用すると、ランダムまたはスティッキ パターンで割り当てを行うことができるので、ユーザに常に同じデスクトップを割り当てることも、ユーザがデスクトップを選択する流動的な方法で割り当てることもできます。プール内のデスクトップは静的または動的に（オンデマンドで）生成でき、永続的に（ユーザがログオフした後に保持）することも、非永続的に（ユーザがログオフした後に削除）することもできます。デスクトップは新たに作成するか、マスター デスクトップ テンプレートからクローニングできます。

デスクトップ管理の観点から、Cisco VXI システムを管理する際はいくつかの点を考慮する必要があります（図 52）。通常、仮想デスクトップは物理デスクトップと同じ OS を実行するので、OS、アプリケーションのアップデート、Microsoft Windows ユーザ プロファイル、およびネットワーク設定には同じコンポーネント管理戦略を使用する必要があります。アプリケーションは仮想デスクトップにローカルにインストールするか、アプリケーション サーバからストリーム配信できます。永続的なデスクトップ（使用後に保持されるデスクトップ）を管理するときは、各仮想デスクトップを個別に更新する必要があります。マスター テンプレートを使用してオンデマンドで生成される非永続的なデスクトップ（使用後に削除されるデスクトップ）を管理するときは、マスターだけを更新します。新規のユーザ セッションを処理するために生成される後続のデスクトップは、更新されたマスター テンプレートからクローニングされます。

図 52　　デスクトップ管理



Cisco VXI デスクトップ管理を理解するため、次のシナリオについて考えます。

- ある Cisco VXI 展開で、管理者が個人用デスクトップを静的に作成し、日常用としてユーザに割り当てます。ユーザには、設定のカスタマイズとソフトウェアのインストールが許可されます。
- 別の Cisco VXI 展開では、共有デスクトップが動的に（オンデマンドで）作成され、タスク ワーカーであるユーザに割り当てます。ユーザには設定のカスタマイズとソフトウェアのインストールが許可されますが、デスクトップはユーザのログオフ後に削除されるので、タスク ワーカーによる変更は永続的ではありません。新規ユーザには、オンデマンドで生成される新規のデスクトップが提供されます。

仮想デスクトップの管理には利点があります。OS、アプリケーション、およびユーザがすでに設定されているマスター仮想マシン テンプレートからデスクトップをクローニングすると、新規デスクトップの作成タスク（たとえば、新規ユーザまたはアップグレードを必要とするユーザのためのオペレーティング システムやアプリケーションのインストール、およびユーザ設定のカスタマイズなど）を迅速に行うことができます。さらに、リンクド クローン機能により、クローニング操作を最適化し、高速化できます。

専用デスクトップ（永続的）へのアップデートの適用は、物理デスクトップの場合と同じ方法で行います。このシナリオでは、管理者がある程度の制御を維持することに変わりはありませんが、ユーザに関してはインストールされたアプリケーションおよびユーザ設定（パーソナライズ）に対する柔軟性が高まります。仮想デスクトップに対するソフトウェア アップデートの維持、新規ソフトウェアのダウンロードとインストール、ファイル バックアップの実行、およびウイルス対策ソフトウェアの実行といったタスクは、物理デスクトップの場合とほとんど同じです。

変更する必要があるのはマスター テンプレートだけなので、共有デスクトップ（非永続的）へのアップデートの適用は一元的な方法で行うことができます。Cisco VXI の導入により、IT は各 OS、アプリケーション、およびユーザ プロファイルの単一のインスタンスを管理することで、デスクトップ管理を大幅に簡素化できるようになりました。管理者は、デスクトップ上のイメージ バージョンおよびアプリケーション リビジョンを完全に制御できます。マスター テンプレートに対するあらゆる変更およびアップデートは管理者が行うことができ、新規ユーザ セッションにただちに反映させることができます。このプロセスは、仮想マシン テンプレートを静的にクローニングするか、動的に生成されたデスクトップの場合は VMware リンクド クローンまたは Citrix Provisioning Services を使用することによって実行できます。

ウイルス対策ソフトウェアなどの一部のアプリケーションは仮想デスクトップにローカルにインストールできますが、Microsoft Office などのその他のアプリケーションは中央リポジトリから仮想デスクトップにストリーム配信できます。ストリーム配信されたアプリケーションを更新するときは、中央アプリケーション サーバ上のマスター コピーだけを更新する必要があります。仮想デスクトップにローカルにインストールされたアプリケーションを更新するときは、デスクトップまたはマスター テンプレート デスクトップを更新する必要があります。

仮想デスクトップはデータセンター内にあり、ネットワーク プリンタの近くにない可能性があるので、デスクトップにプリンタをインストールして設定するアプリケーションに対し、適切な変更を加える必要があります。デスクトップ仮想化ベンダーのソリューションでは、エンドポイントに接続している USB デバイスへの接続をサポートしているので、USB ポートで接続しているローカル プリンタへの印刷は、エンドユーザ セッションに対して有効にします。

エンドポイント管理

エンドポイント上の OS、アプリケーション、および設定も管理する必要があります。これらのエンドポイントで Microsoft Windows の組み込みバージョンを実行している場合は、物理デスクトップとほとんど同じ方法で管理できます。エンドポイント管理ツールを使用すると、デスクトップ仮想化エンドポイントのプロビジョニングおよびモニタリングのタスクを自動化し、簡素化できます。Dynamic Host Configuration Protocol（DHCP）などのネットワークベース サービスやファイル サーバを使用して、エンドポイントのプロビジョニングと更新を行うこともできます。また、ローカル ソフトウェア リポジトリまたはキャッシング サービス（Cisco Wide Area Application Services）を使用して、デスクトップ仮想化エンドポイントにパッチやアップデートを配信できます。詳細については、デスクトップ仮想化エンドポイントの管理について説明しているセクションを参照してください。

Cisco VXI 管理ツールの概要

このセクションでは、各要素のプロビジョニングとモニタリングに使用できる Cisco VXI システム コンポーネントおよび管理ツールの概要を示します。また、関連付けられた各機能の簡単な説明と追加資料へのリンクを示します。

データセンターとアプリケーション

管理する必要のある主なデータセンター コンポーネントは、コンピューティング サーバ、ハイパーバイザ、仮想マシン、ストレージ、スイッチング ファブリック、接続マネージャ、およびネットワーク サービスを提供するサーバです。管理タスクには、エンド ユーザ、仮想デスクトップ、デスクトップ プール、ハイパーバイザ、およびストレージのプロビジョニングと、セッションおよびリソース使用（コンピューティング、メモリ、ストレージ、およびネットワーク）のモニタリングが含まれます。表 16 に、コンポーネントと管理ツールを示します。

表 16　データセンターおよびアプリケーション：管理ツール

製品	管理ツール	説明	製品マニュアルへのリンク
ESX/ESXi および仮想マシン	VMware vCenter および Vsphere クライアント	仮想マシンの作成と管理には、VMware ESX および ESXi ハイパーバイザ マネージャを使用します。	VMware vSphere ドキュメント
Microsoft Hyper-V および仮想マシン	Microsoft System Center Virtual Machine Manager（SCVMM）	Microsoft SCVMM ハイパーバイザ マネージャを使用して仮想マシンを作成および管理します。	Microsoft SCVMM ドキュメント
Citrix XenDesktop Delivery Controller 5.0	Citrix Desktop Studio および Desktop Director	仮想デスクトップのプールの作成、ユーザ権限の付与、セッションの監視を行います。	Citrix XenDesktop ドキュメント
Citrix XenApp Delivery Controller	Citrix Delivery Services Console	XenApp サーバ ファームの作成、アプリケーションの公開、ユーザ権限の付与、セッションの監視を行います。	Citrix XenApp ドキュメント
EMC ユニファイド ストレージ	EMC Unisphere 管理スイート	SAN ベースのストレージ アレイのプロビジョニングとモニタリングを行います。	EMC Unisphere 管理スイート
NetApp FAS 3170	NetApp Virtual Storage Console / StorageLink	Network-Attached Storage（NAS; ネットワーク アタッチド ストレージ）ベースのストレージ アレイのプロビジョニングとモニタリングを行います。	NetApp Virtual Storage Console NetApp StorageLink
Cisco UCS B シリーズ ブレード サーバ	Cisco UCS Manager	Cisco UCS B シリーズ ブレード サーバのプロビジョニングとモニタリングを行います。	UCS Manager

製品	管理ツール	説明	製品マニュアルへのリンク
仮想デスクトップ（ゲスト OS）	標準のエンタープライズ デスクトップおよび OS 管理ツール （Altiris、Short Message Service（SMS; ショート メッセージ サービス）、および Microsoft System Center Configuration Manager（SCCM））	仮想デスクトップのプロビジョニングとモニタリングを行います。	Altiris のリファレンス文書
Microsoft Active Directory、Domain Name System（DNS; ドメイン ネーム システム）、DHCP	標準のエンタープライズ管理ツール	エンド ユーザ プロファイルを管理し、ユーザ セッションの認証を実行します。DHCP サービスをエンドポイントに提供します。	Microsoft Active Directory およびネットワーク サービス

ネットワーク インフラストラクチャ

ネットワーク インフラストラクチャ（LAN、WAN、および SAN）内で管理が必要な主な要素は、スイッチ、ルータ、WAN 高速化デバイス、ロード バランサ、セキュリティ ゲートウェイ、およびネットワーク アナライザです。これらのコンポーネントはデータセンター、エンタープライズ コア、WAN、およびブランチ オフィスにまたがり、データおよびストレージ接続の両方を提供します。管理タスクには、これらの要素のプロビジョニングとモニタリング、およびデスクトップ仮想化セッションのモニタリング、ネットワークの使用に関するレポート作成が含まれます（表 17）。

表 17　　ネットワーク インフラストラクチャ：管理ツール

製品	管理ツール	説明	製品マニュアルへのリンク
Cisco Network Analysis Module	Cisco NAM Admin GUI	Cisco NAM のプロビジョニングとモニタリングを行います。	Cisco NAM ドキュメント
Cisco Application Control Engine（ACE）	ACE Device Manager	ACE のプロビジョニングとモニタリングを行います。	Cisco ACE ドキュメント
Cisco Wide Area Application Service	Cisco WAAS Central Manager	Cisco WAAS アプライアンスのプロビジョニングとモニタリングを行い、最適化に関する集約レポートを生成します。	Cisco WAAS ドキュメント
Cisco Adaptive Security Appliance（ASA）	Adaptive Security Device Manager	ASA のプロビジョニングとモニタリングを行います。	Cisco ASA ドキュメント
Cisco AnyConnect VPNClient	AnyConnect Profile Editor	AnyConnect VPN Client をプロビジョニングします。	Cisco AnyConnect ドキュメント

製品	管理ツール	説明	製品マニュアルへのリンク
Cisco MDS 9000	Cisco Fabric Manager	Cisco MDS 9000 ファミリ SAN スイッチのプロビジョニングとモニタリングを行います。	Cisco Fabric Manager ドキュメント
Cisco Nexus 7000/Nexus 5000	Cisco Data Center Network Manager	Nexus 7000、Nexus 5000、および MDS スイッチのプロビジョニングとモニタリングを行います。	Cisco DCNM ドキュメント
Cisco Nexus 1000v	Cisco NX-OS CLI、Cisco DCNM、および vCenter	Cisco Nexus 1000v のプロビジョニングとモニタリングを行います。	Cisco Nexus 1000v ドキュメント
Catalyst 6500、Catalyst 3560、ISR 3900/2900	Cisco Prime LAN Management Solution	Cisco ルータおよびスイッチのプロビジョニングとモニタリングを行います。	Cisco Prime ドキュメント
ルータ、スイッチ、およびセキュリティ アプライアンスに関するシスコのセキュリティ ポリシー	Cisco Security Manager	Cisco ルータ、スイッチ、およびセキュリティ アプライアンスに関するセキュリティ ポリシーのプロビジョニングとモニタリングを行います。	Cisco Security Manager ドキュメント
Cisco IOS NetFlow	Cisco NetFlow Collector	ルータおよびスイッチから収集された NetFlow データの収集、分析、およびレポート作成を行います。	Cisco NetFlow Collector ドキュメント
Cisco EnergyWise	Cisco EnergyWise Orchestrator	スイッチおよびエンドポイント デバイスに対する電力消費のモニタリングと制御を行います。	Cisco EnergyWise ドキュメント

デスクトップ仮想化エンドポイント

管理する必要のあるデスクトップ仮想化エンドポイントは、ゼロ クライアント、シン クライアント、仮想クライアント、および Web ベース クライアントです。エンドポイントの管理には、エンドポイントのプロビジョニングとモニタリング、イメージの更新、資産管理の実行、ユーザ エクスペリエンスの品質の測定、およびエンドポイントへのリモート アクセスが含まれます。デスクトップ仮想化エンドポイント OS の管理には、Altiris、Cisco VXC Manager、Wyse Device Manager、Devon Thin Client Management、IGEL Universal Management Suite などのエンタープライズ デスクトップ管理ツールや Unified CM を使用することをお勧めします。DV エンドポイントの管理ツールについては、表 18 を参照してください。

表 18　DV エンドポイント：管理ツール

製品	管理ツール	説明	製品マニュアルへのリンク
Cisco VXC エンドポイント	Cisco VXC Manager	VXC エンドポイントのイメージ、設定、資産管理、シャドウイング	Cisco VXC Manager ドキュメント
Cisco Cius タブレット	CUCM およびエンタープライズ モバイル デバイス管理ツール	モバイル DV エンドポイントのイメージ、設定、資産管理	Cisco UMS ドキュメント
Wyse DV エンドポイント	Wyse Device Manager 4.8	DV エンドポイントのイメージ、設定、資産管理、シャドウイング	Wyse Device Manager ドキュメント
Devon DV エンドポイント	Thin Client Management 3.0	DV エンドポイントのイメージ、設定、資産管理、シャドウイング	Devon IT ドキュメント
IGEL DV エンドポイント	Universal Management Suite 3	DV エンドポイントのイメージ、設定、資産管理、シャドウイング	IGEL ドキュメント
Windows ベースのエンドポイント（シック クライアント）	標準のエンタープライズ デスクトップおよび OS 管理ツール（Altiris、SMS、SCCM）	DV エンドポイントのイメージ、設定、資産管理	Altiris のリファレンス文書

ユニファイド コミュニケーション

管理する必要のある主なユニファイド コミュニケーション要素は、Cisco Unified IP Phone、Cisco Cius タブレット、Cisco Unified Personal Communicator クライアント、Cisco Unified Communications サーバ（Cisco Unified Communications Manager、Cisco Unified Presence、Cisco Unity®）です。UC 要素の管理には、IP Phone、Cisco Unified Personal Communicator クライアント、Cisco Unity アカウント、およびサーバのプロビジョニングとモニタリングのタスクが含まれます。Cisco Unified Communication サーバには、基本的なプロビジョニングおよびモニタリング タスクの実行に使用できる組み込みの Web ベース GUI 管理インターフェイスが搭載されています。高度な管理機能、スケーラビリティ、およびパフォーマンスには、Cisco Unified Communications Management スイートのツールが推奨されます（表 19）。

表 19　Unified Communications：管理ツール

製品	管理ツール	説明	製品マニュアルへのリンク
Cisco IP Phone、Cisco Cius タブレット、および Cisco Unified Personal Communicator クライアント	Cisco Unified Management Suite	CUOM、CUPM、CUSM、CUSSM	Cisco UMS ドキュメント
Unified CM、Cisco Unified Presence、Unity サーバ	Cisco Unified Management Suite	CUOM、CUPM、CUSM、CUSSM	Cisco UMS ドキュメント

Cisco VXI の管理タスクとワークフロー

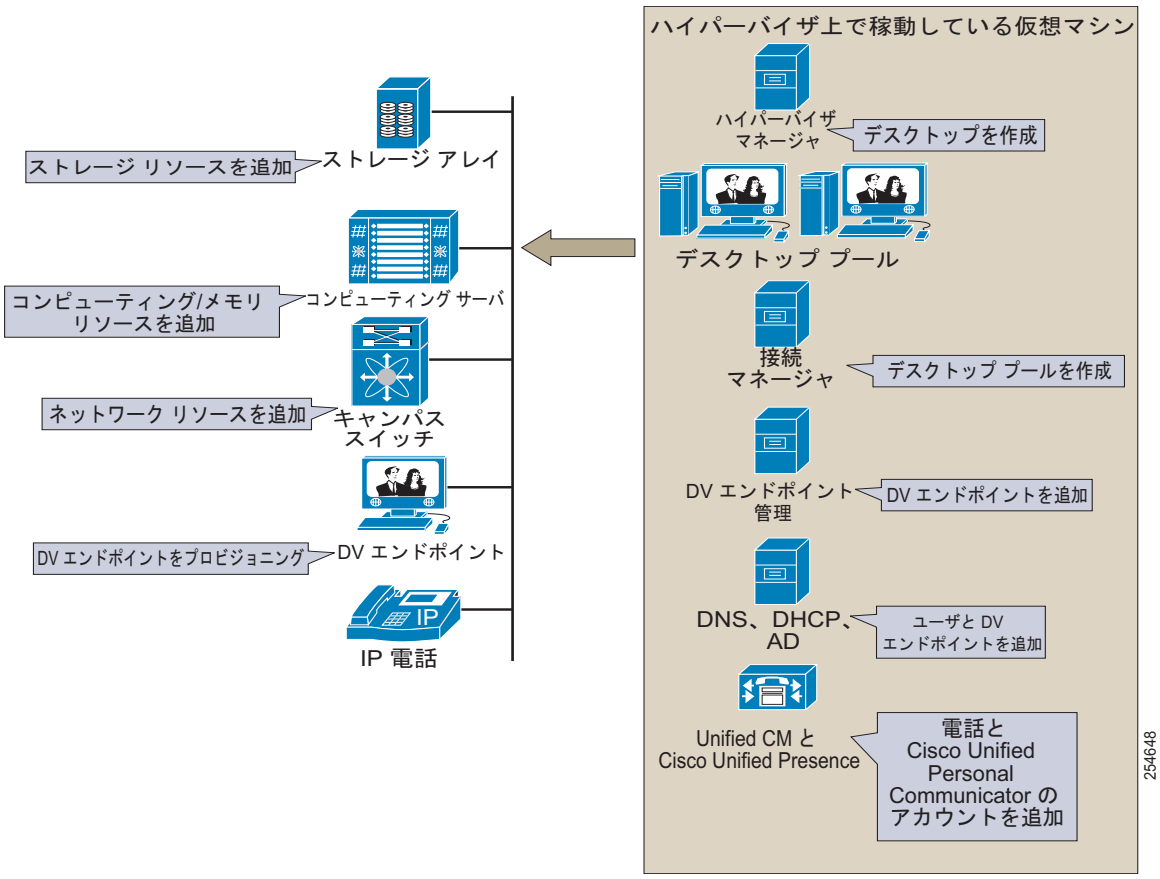
このセクションでは、IT 管理者向けの使用例と、Cisco VXI 管理者が日常的に行う最も一般的な操作のワークフローを示します。たとえば、ユーザの追加には、VMware vCenter、XenDesktop Studio、および Microsoft Active Directory における新規デスクトップ ユーザの作成、Cisco Unified Communications Manager、Cisco Unified Presence Server、および Cisco Unity での新規電話機と Cisco Unified Personal Communicator アカウントの設定、VXC Manager および DHCP サーバでの新規デスクトップ仮想化エンドポイントのプロビジョニング、および、データセンターでのストレージ、メモリ、コンピューティング、ならびにネットワーク リソースの追加を伴う場合があります。

サービス管理用の統合管理コンソールは、Cisco VXI システムにとって重要な管理ツールです。カスタマイズされたこの管理アプリケーションでは、各ベンダーが提供するインターフェイスを使用して主な Cisco VXI コンポーネントを管理します。API、プロトコル、またはプラグインによってコンポーネント固有の管理ツールと統合された市販のエンタープライズ ネットワーク マネージャを使用して、中央管理ユーティリティにあるツールのいくつかの側面と機能を公開し、管理者がツールを呼び出して全機能にアクセスできるようにすることを検討してください。

オーケストレーション ツールも、大規模な展開にとって重要な管理ツールです。このツールは、特定のワークフローに関連付けられたタスク（ユーザ、エンドポイント、仮想デスクトップの追加など）を自動化します。また、自動化インターフェイスは、各ベンダー固有の管理ツールとの統合を自動化することによって、エンド ユーザが管理者のサポートなしに仮想デスクトップをセルフプロビジョニングできるようにします。図 53 のトロポジ図に、特定のワークフローに関連するソリューション内のコンポーネントに関するアクションを示します。

IBM Network Manager など、SNMP および syslog をサポートする市販のエンタープライズ ネットワーク マネージャを使用することを検討してください。これらのプロトコルをサポートするシステム内の要素を管理するのに使用できます。システム内の異なるデバイスからのログの収集と関連付けは、ユーザ セッションのトラブルシューティングやモニタリングを行う管理者にとって非常に有益です。この機能を実行できるツールとして、Splunk を使用することを検討してください。仮想データセンターやストレージ インフラストラクチャを管理するための高度な機能を備えた VizionCore ツール スイート（仮想マシンのパフォーマンス管理やレポート作成用の vFoglight、自動化およびワークフロー管理用の vControl などのアプリケーションを含む）のツールを使用することを検討してください。Tidal ソフトウェアには、Cisco VXI システムのコンポーネントのオーケストレーションに使用できる一連の自動化ツールが備わっています。

図 53　Cisco VXI ワークフロー：ユーザの追加

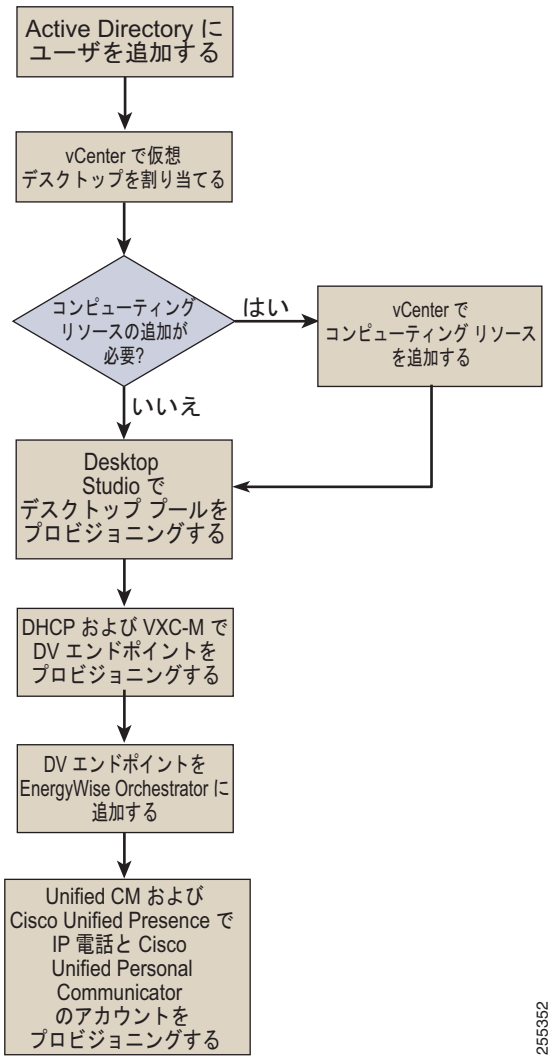


ユーザの追加

表 20　　Cisco VXI ワークフロー：ユーザの追加

タスク	考慮事項	ワークフロー
ユーザの追加：新規ユーザ用のユーザ、仮想デスクトップ、エンドポイントを追加する	• 新規ユーザ用に十分なコンピューティング、メモリ、ストレージ、およびネットワーク キャパシティがありますか。 • これは静的なデスクトップですか。それとも、動的に生成されたデスクトップですか。 • プロビジョニングも必要とされる電話機または Cisco Unified Personal Communicator はありますか。	**1.** 必要な OS/アプリケーションとデスクトップ エージェントを備えた仮想デスクトップを作成します（カスタマイズ テンプレートを使用して、仮想マシン テンプレートからクローニングできます）。 **2.** デスクトップを AD ドメインに参加させ、DNS エントリが自動的に作成されることを確認します。 **3.** コンピューティング、メモリ、ストレージ、またはネットワーク リソースが足りない場合は、必要に応じて追加します。 **4.** ユーザ名とパスワードを使用してユーザを LDAP サーバに追加します。 **5.** ユーザに適切な権限を付与するとともに、専用プール内のデスクトップをプロビジョニングします。 **6.** 必要な OS/アプリケーションおよびデバイス マネージャ エージェントとともに DV エンドポイントをプロビジョニングします。 **7.** 自動検出（オプション）を使用してデバイス マネージャに、または Energywise Orchestrator に DV エンドポイントを追加します。 **8.** DHCP サーバでネットワーク設定と接続マネージャの場所を指定します。 **9.** Cisco Unified Personal Communicator/ボイスメール アカウントを作成し、ユーザをデスク フォンに関連付けます。

図 54　　Cisco VXI ワークフロー：ユーザの追加

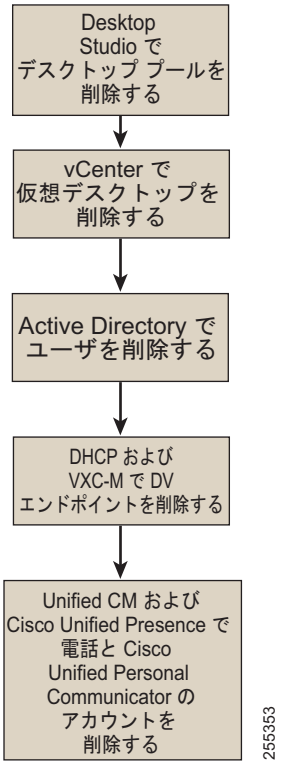


ユーザの削除

表 21　Cisco VXI ワークフロー：ユーザの削除

タスク	考慮事項	ワークフロー
ユーザの削除：ユーザ、仮想デスクトップ、エンドポイントを削除する	• コンピューティング、メモリ、ストレージ、またはネットワーク キャパシティで統合できるものはありますか。 • これは静的なデスクトップですか。それとも、動的に生成されたデスクトップですか。 • プロビジョニング解除も必要な電話機または Cisco Unified Personal Communicator はありますか。	**1.** デスクトップ プールから仮想デスクトップを削除します。 **2.** 仮想デスクトップを削除します。 **3.** LDAP サーバからユーザを削除します。 **4.** VXC-M および DHCP から DV エンドポイントを削除します。 **5.** 電話機および Cisco Unified Personal Communicator のアカウントを削除します。

図 55　Cisco VXI ワークフロー：ユーザの削除



ユーザの変更

表 22　　Cisco VXI ワークフロー：デスクトップの更新

タスク	考慮事項	ワークフロー
ユーザの仮想デスクトップの変更：仮想デスクトップ上のアプリケーションを変更する	• このデスクトップ プールは静的ですか、動的ですか。 • アプリケーションはローカルにインストールされたものですか。それともストリーム配信されたものですか。	• 静的なデスクトップの場合は、仮想デスクトップ自体を変更し、更新します。 または • 動的なデスクトップ プールの場合は、仮想マシン テンプレートを変更し、新しいデスクトップを作成します。

図 56　　Cisco VXI ワークフロー：デスクトップの更新

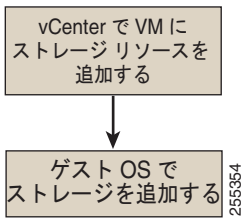
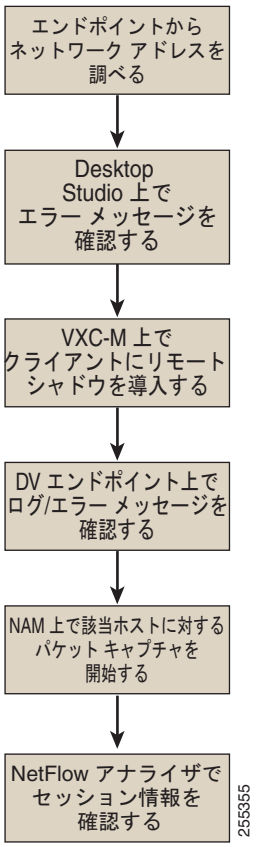


表 23　　Cisco VXI ワークフロー：デスクトップの変更

タスク	考慮事項	ワークフロー
ユーザの仮想デスクトップの変更：ストレージをデスクトップに追加する	既存のストレージのサイズを増やしますか。それとも、新しいストレージ リソースを追加しますか。 仮想デスクトップに対して、シン プロビジョニングが有効になっていますか。 ストレージは、マップされたネットワーク ドライブを介して追加できますか。	1. ストレージ リソースを追加するか、仮想マシン用の既存ストレージのサイズを増やします。 2. ゲスト OS のディスク管理ユーティリティを使用して、新しいストレージを認識します。

図 57　Cisco VXI ワークフロー：デスクトップの変更



ユーザ セッションのモニタリング / トラブルシューティング

表 24　Cisco VXI ワークフロー：ユーザ セッションのモニタリングまたはトラブルシューティング

タスク	考慮事項	ワークフロー
ユーザ セッションのモニタリング / トラブルシューティング：接続できない、または品質に問題があるユーザ セッションのトラブルシューティングを行う	• ユーザ セッションは接続できますか。 • ユーザ セッションは品質に問題がありますか。 • 接続マネージャによってリソース不足が報告されていますか。 • エンドポイント、接続マネージャ、および仮想デスクトップ間に接続はありますか。	**1.** デバイス マネージャまたは DV エンドポイント自体からネットワーク アドレスを確認します。 **2.** 接続マネージャのエラー メッセージとログをチェックします。 **3.** VXC-M リモート シャドウ Virtual Network Computing（VNC; 仮想ネットワーク コンピューティング）を使用してデスクトップ仮想化エンドポイントにアクセスし、問題のトラブルシューティングを続けます。 **4.** DV エンドポイントのエラー メッセージ、ログ、およびソフトウェア バージョンをチェックします。 **5.** 特定のホストに対するパケット キャプチャを開始します。 **6.** NetFlow アナライザで、特定のホストのセッション情報をチェックします。

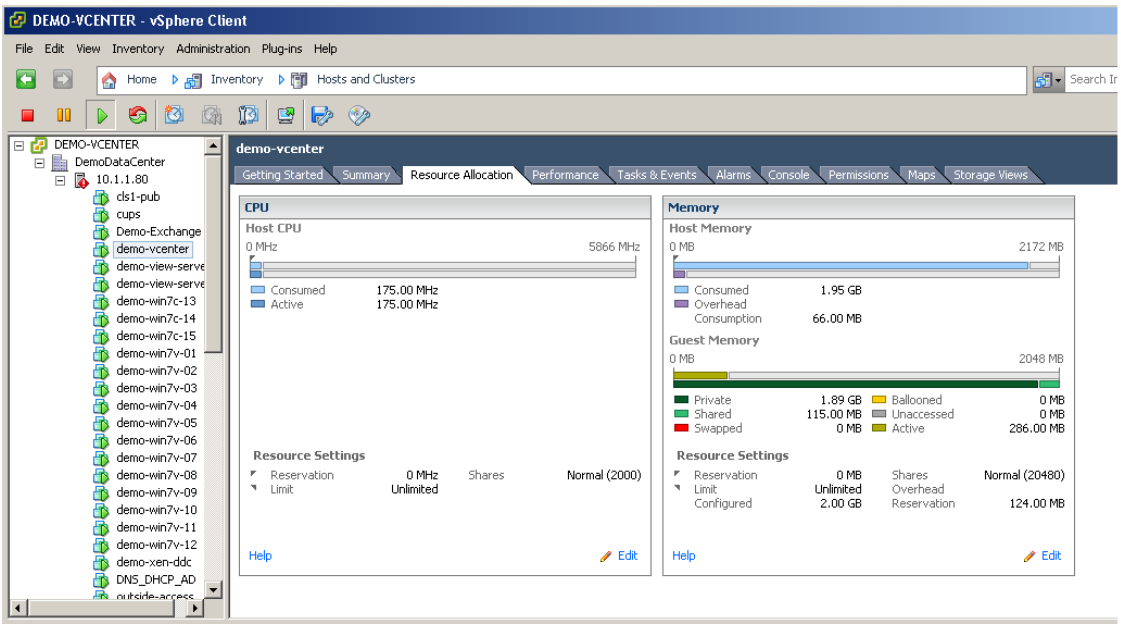
Cisco VXI 管理ツール

このセクションでは、システムのコンポーネントのプロビジョニングとモニタリングに使用できる各管理ツールの概要と簡単な説明を示します。これには、使用されるツールと実行されるタスクに関連付けられたガイドラインとベスト プラクティス、および追加資料への参照リンクも含まれます。

VMware vCenter と vSphere

VMware vCenter および vSphere 管理スイートを使用して、ホスト（物理的なコンピューティング サーバ）で動作するハイパーバイザ（VMware ESX および ESXi）を管理します。これにより、管理者は、複数のハイパーバイザ ホストの管理と、仮想マシンや仮想アプライアンスの展開および管理を行うことができます。また、この管理スイートを使用して、ホストと仮想マシン上のコンピューティング、メモリ、ストレージ、およびネットワーク リソースの使用率のモニタリング、システム イベントのモニタリング、ならびにレポートの生成を行うことができます。VMware vCenter サーバは、VMware vSphere クライアントを使用してアクセスおよび管理されます（図 58）。

図 58　　vSphere クライアント インターフェイス



Cisco VXI システムでの VMware vCenter および vSphere の使用に関するガイドライン

仮想デスクトップ

- 新規の仮想デスクトップを作成する際、管理者は仮想マシンのプロパティ、仮想 CPU の数、メモリ割り当て、ストレージのタイプと割り当て（ローカル、SAN、または NAS）、virtual Switch（vSwitch; 仮想スイッチ）への virtual Network Interface Card（vNIC; 仮想ネットワーク インターフェイス カード）の接続、およびゲスト OS（Microsoft Windows または Linux）を指定する必要があります。また、ハイパーバイザが動作している物理ホストにデスクトップを割り当てることも必要です。管理者は次に、仮想マシンへのゲスト OS のインストールに進みます。仮想マシン コンソールには VMware vSphere Client からアクセスし、ゲスト OS の追加のカスタマイズを実行できます。リモート デスクトップ セッションに対するマウスやグラフィックのパフォーマンスを向上させ、VMware vCentervSphere Client からデスクトップを管理しやすくするために、VMware ツールをゲスト OS にインストールしてください。

- 多数の仮想デスクトップを展開する場合は、必要な OS、アプリケーション、およびカスタマイズが揃っているマスター仮想デスクトップに基づいて作成されたマスター テンプレートからクローニングします。VMware 仮想マシンのカスタマイズ仕様を使用すると、複数のデスクトップのクローニング プロセスを簡素化できます。
- 動的に（オンデマンドで）作成されたデスクトップには、仮想マシン テンプレートの使用が必須です。マスター テンプレートで DHCP を有効にして、動的に生成された仮想デスクトップにおけるネットワーク アドレスの重複を回避します（クローン デスクトップのネットワーク設定は、マスター テンプレートに指定されているネットワーク設定と同じであるため）。

プロビジョニング

- 通常は VMware vSphere クライアントで実行される管理タスク（プロビジョニングやモニタリング）を自動化するため、VMware vSphere Microsoft Windows Powershell CLI を使用します。たとえば、静的に生成された永続的なデスクトップ プールに属する仮想マシンのクローニング タスクを自動化するために、CLI を使用できます。CLI は、管理者が大規模なデスクトップ プールを作成したり、エンド ユーザが仮想デスクトップをセルフプロビジョニングしたりする際に役立ちます。
- VMware ESX/ESXi ホストを VMware vCenter データセンター サーバに追加し、VMware vSphere クライアントで管理します。VMware ESXi コンソール管理インターフェイスには、物理ホストからローカルにアクセスできます。これには、管理者のパスワードやネットワーク設定のプロビジョニングに使用できるメニュー インターフェイスが表示されます。VMware ESXi ホストに VMware vSphere クライアントから直接アクセスできる場合でも、これらのホストの管理は VMware vCenter サーバを介して行ってください。VMware vCenter で直接アクセスできないように、VMware ESXi ホストをロック ダウンすることもできます。VMware ESXi にはサービス コンソールがなく、VMware ESX で使用できるサービス コンソールは非推奨であることに注意してください。
- 複数の管理者が VMware vCenter で多数の仮想マシンを管理している場合、（全権限を持つ 1 つのグローバル アカウントではなく）個々の管理者アカウントを設定して、別の管理者ユーザが行った変更を追跡し、ロギングできるようにします。また、VMware vCenter 認証を Microsoft Active Directory にリンクしてこのロギングを実行し、管理者アカウントを一元的に管理することもできます。VMware vCenter および vSphere への役割ベースのアクセスを使用して、機能、権限、およびユーザが実行できる変更の範囲を（データセンター、クラスタ、または許可された機能単位で）制限することも必要です。

（注） 永続的なデスクトップまたはマスター仮想デスクトップの定期的なスナップショットを撮り、それらを使用してデスクトップを既知の状態に復元することもできます。この手順は、デスクトップに障害が発生している（ウイルスによる攻撃を受けている）場合や、パフォーマンスに問題がある場合に役立ちます。

- VMware ESXi ホストの設定および仮想マシンを定期的にバックアップします。このバックアップには、VMware vCenter vSphereCLI（vicfg –cfgbackup コマンド）や、VMware Consolidated Backup、VMware Data Recovery、VMware vStorage API などの VMware vSphere アプリケーションを使用することが推奨されます。これらのバックアップおよびリカバリ機能の使用に関するベスト プラクティスについては、VMware のドキュメントを参照してください。
- 電力損失の場合は、物理ホストの電源が復旧した後に仮想デスクトップの電源を投入します。仮想マシンへの電源投入の順序とタイミングは、VMware vCenter で指定できます。ブートアップ時に Microsoft Windows ネットワーク サービス（DHCP、DNS、および Microsoft Active Directory）にアクセスするときの過剰なネットワークおよびサーバ ロードを回避するため、仮想デスクトップの電源投入のタイミングを調整することを検討してください。

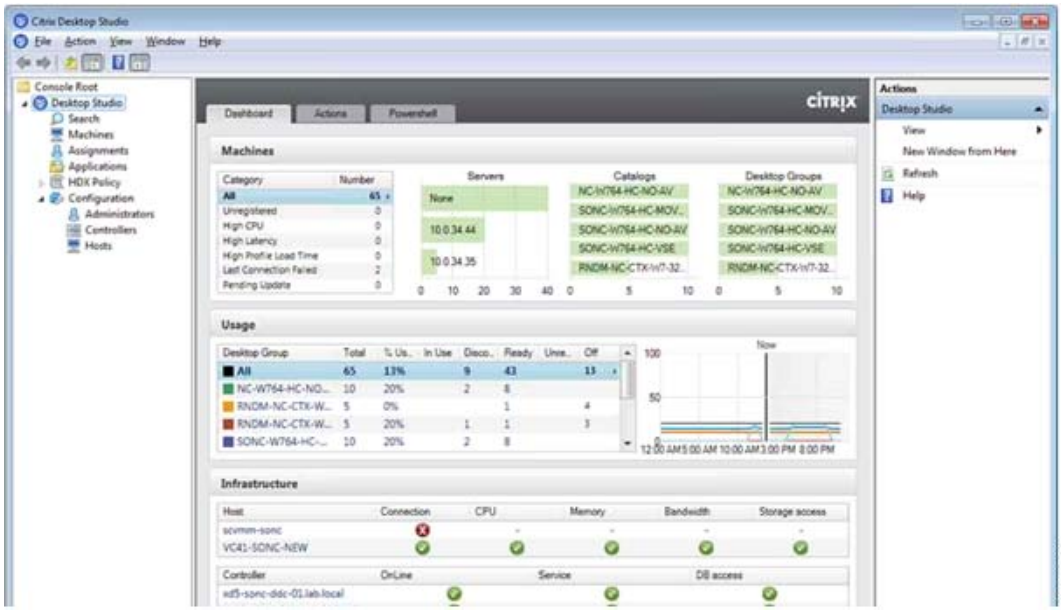
- VMware vCenter にバンドルされたデフォルトの SQL データベースは拡大できないので、規模の大きい展開には外部の Microsoft SQL または Oracle データベース エンジンを使用してください（最大 5 台のホストと 50 台の仮想マシンでの使用が対象となります）。VMware vCenter で管理できるホストと仮想マシンの数については、スケーリングと制限に関するリファレンス文書『Configuration Maximums from VMware』を参照してください。また、外部データベースに備わっているバックアップ ユーティリティを使用して、VMware vCenter データベースを定期的にバックアップする必要があります。
- 仮想マシンに VMware vCenter をインストールし、VMware vMotion、DRS、および Fault Tolerance などのハイ アベイラビリティ機能を利用することにより、アプリケーションの可用性を高めます。ハイ アベイラビリティの展開については、アクティブな役割とスタンバイの役割を確立するハートビート メカニズムを使用する冗長サーバで VMware vCenter を実行できます。大規模な展開については、リンクモード グループ機能を使用することを検討してください。このモードでは、グループ内のすべての仮想マシンへの共有アクセスを許可するよう、サーバ群の VMware vCenter を設定できます。冗長構成での VMware vCenter の展開に関するベスト プラクティスについては、VMware のドキュメントを参照してください。

Citrix XenDesktop 5.0 管理スイート

Citrix XenDesktop 5.0 管理スイートは、Cisco VXI 導入での XenDesktop コンポーネントの管理に使用されます。Citrix XenDesktop 5.0 には、仮想デスクトップと Desktop Director のプロビジョニング、設定、および管理に使用される Desktop Studio が組み込まれています。Desktop Director は、仮想デスクトップの監視とトラブルシューティング、および日常的なメンテナンス業務を行うために使用されます。これらのツールは、管理スタッフとヘルプデスクのサポート スタッフによって使用されます。

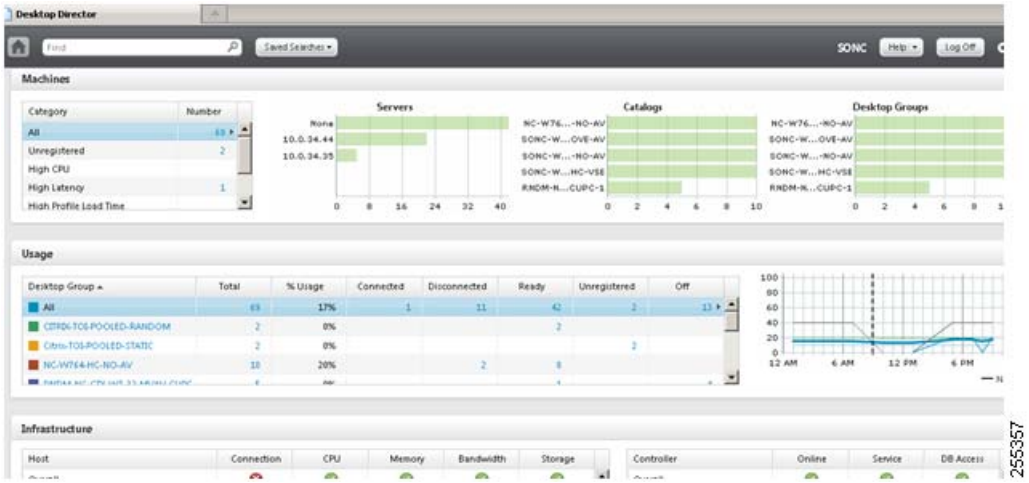
Desktop Studio は Microsoft Management Console（MMC）ベースのスナップインであり、管理者はこれを使用して、カタログによる仮想デスクトップのプロビジョニング、デスクトップ グループを使用したユーザへのデスクトップの割り当て、カタログ、デスクトップ グループ、および各デスクトップの保守、デスクトップ コントローラ環境の管理、ホストの設定、スマート カードの使用、デスクトップ ポリシーの作成を迅速に行うことができます。Desktop Studio コンソールは、プロビジョニング ワークフローを実行するためのウィザードを備えています。このウィザードはデスクトップの割り当てに使用されます。管理者はこのウィザードを使用して、ブレード PC ベースのデスクトップ、専用仮想マシンベースのデスクトップ、ユーザ グループ用にプールされたデスクトップなど、さまざまなデスクトップを異なるユーザに対して割り当てることができます。XenDesktop 5.0 の仮想デスクトップ インフラストラクチャは、サイト、デスクトップ カタログ、デスクトップ グループ、およびホストに分類されます。デスクトップ カタログには、プール、専用、既存、物理的、またはストリーム型のデスクトップを含めることができます。

図 59　　XenDesktop Studio コンソール



Desktop Director は Web ベースのツールで、IT サポート スタッフはこれを使用して、仮想デスクトップおよびホストの監視や日常的なメンテナンス業務を実行できます。Desktop Director は、サイト内のハイパーバイザやデスクトップ コントローラの稼動状態など、ホストとサーバの状態を監視するために使用されます。また、デスクトップの再起動やセッションのログオフまたは切断など、セッションとデスクトップの操作にも使用されます。さらに、Microsoft Remote Assistance でユーザ セッションを表示してこれと対話し、問題点をトラブルシューティングする場合にも使用されます。Desktop Director は、権限に関連付けられた役割ベースのアクセスをサポートしています。Desktop Studio で提供される機能に対し、Desktop Director は制限付きの読み取り専用機能を提供します。

図 60　　XenDesktop Director コンソール



Desktop Director には、リアルタイムのマシン問題、使用メトリック、ホストとコントローラの稼動状態に関する情報を集約するダッシュボードが組み込まれています。Desktop Director は、デスクトップ ユーザ セッションの監視や、帯域幅、遅延、ジッタ、ユーザ エクスペリエンス、セッション時間、HDX 機能の状態といったメトリックの確認に使用できます。また、Citrix Edgesight とともに使用すると、仮想デスクトップを監視し、CPU、メモリ、ストレージ、ネットワーク帯域幅の使用状況などを確認できます。Desktop Director を使用して、監視対象のメトリックに基づいたアラートを生成することも可能です。Desktop Director は、1 ヵ月間のユーザ アクティビティの可用性とパフォーマンスに関する SLA レポートを作成し、ヘルプデスク サポートが利用できる統計情報などリアルタイムのパフォーマンス メトリックとその履歴を提示します。Desktop Director はセッション管理をサポートしており、管理者はこれを使用して、アクティブおよび非アクティブな仮想デスクトップ接続を管理できます。管理者は、ユーザが接続しているサーバを表示し、必要に応じてユーザをログオフさせることができます。Desktop Director には、複数のソース（XenDesktop Controller、Citrix Profile Management、Windows Management Instrumentation、Active Directory）から収集された関連情報が格納されます。仮想デスクトップの起動、停止、一時停止、再起動にも Desktop Director を使用できます。

図 61　　Desktop Director のセッション モニタ

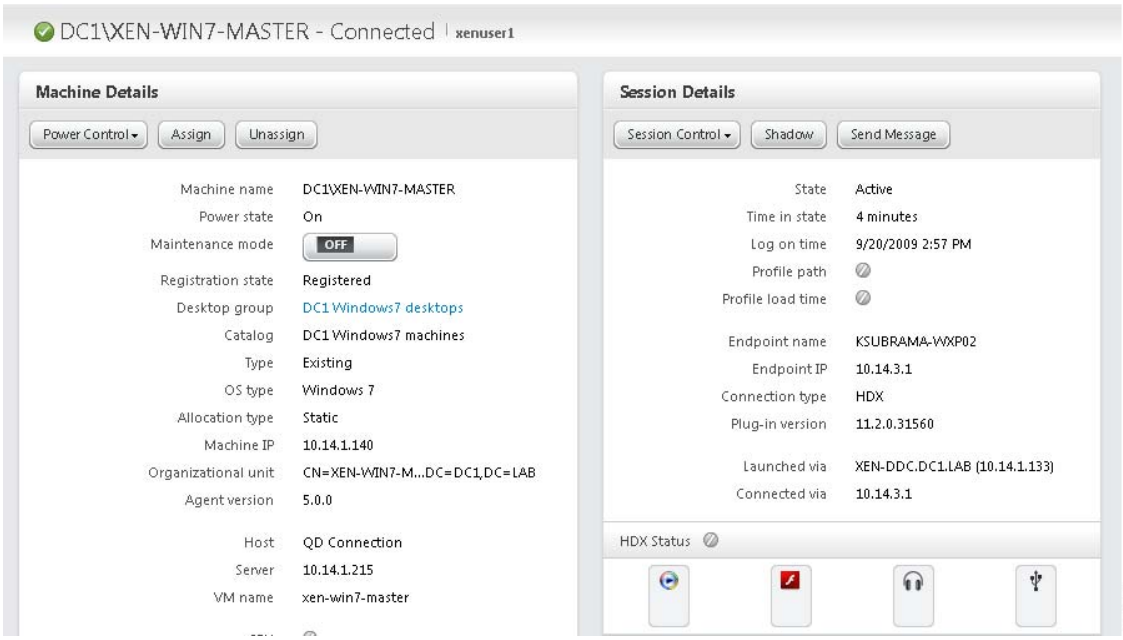


表 25　　XenDesktop 管理スイートのワークフロー

仮想デスクトップのマシン カタログの作成	1. インフラストラクチャの準備：ハイパーバイザとストレージの詳細を確認します。 2. マスター仮想デスクトップの準備：スナップショットに基づいてマスター イメージを作成します。 3. AD アカウントの作成：仮想デスクトップにコンピュータ名を割り当てます。 4. カタログの作成：ハイパーバイザ インフラストラクチャ内に仮想デスクトップを作成します。
デスクトップ グループの作成	1. デスクトップ カタログの選択 2. ユーザの割り当て：AD アカウントを指定します。

XenDesktop 管理スイートの一般的な使用例を次に示します。

- Desktop Studio を使用して Cisco VXI システムに仮想デスクトップとユーザを追加します。
- Desktop Director を使用して、デスクトップ ユーザ セッションの帯域幅、遅延、ジッタ、ユーザ エクスペリエンス、セッション時間を監視します。
- Desktop Director を使用して仮想デスクトップのリソース使用メトリックを監視します。
- Desktop Director を使用して、XenDesktop 環境のリアルタイムのパフォーマンス メトリックとその履歴を監視します。
- Desktop Director を使用して、ユーザ セッションのトラブルシューティングとレポート作成を行います。
- Desktop Director を使用して、可用性とパフォーマンスに関する SLA レポートを作成します。これにはセッションの成功率/切断率、1 ヵ月間の仮想デスクトップ使用率、およびユーザ アクティビティなどが含まれます。
- 特定の使用メトリック（ホストの CPU 使用率など）に達した場合に管理者に通知するアラートを設定します。

XenDesktop 管理スイートの使用に関するガイドライン

Desktop Studio

Desktop Studio には PowerShell バージョン 2.0 を基盤にした SDK が搭載されています。管理者はこれを使用して、通常は Desktop Studio コンソールで実行されるタスクを実行できます。SDK を使用すると、大規模な導入での複数のデスクトップのプロビジョニングを自動化することがてきます。PowerShell SDK は、旧リリースの XenDesktop に関連する SDK とは互換性がないことに注意してください。Desktop Studio コンソールには、PowerShell とデスクトップ コントローラのインタラクションについて詳細なログが保存され、これをトラブルシューティングや自動化に利用することができます。

Desktop Studio には、デスクトップ作成ウィザードを使用して複数のデスクトップを作成する機能があります。1 人のユーザがカタログ内の複数のデスクトップにアクセスでき、1 台の仮想デスクトップは単一のカタログまたはデスクトップ グループに属することに注意してください。

Desktop Studio には電源管理機能が搭載されています。これにより、時刻に基づくポリシーを使用して、デスクトップ グループ内で仮想デスクトップの電源をオンにする時刻とその台数を制御することができます。Wyse Xenith 管理スナップイン（Wyse Xenith ゼロ クライアント管理用）は、XenDesktop インストール ウィザードを使用して Desktop Studio にインストールできます。

VMware vCenter で管理される仮想デスクトップを使用してデスクトップ プールをプロビジョニングする場合は、VMware vCenter サーバで HTTP インターフェイスを有効にし、VMware vCenter サーバ URL で HTTP を指定します。あるいは、VMware vCenter サーバに信頼できる認証局の署名済み証明書をインストールし、HTTPS ベースのインターフェイスを使用します。

Desktop Director と Desktop Studio は、デフォルトではデスクトップ コントローラを実行するサーバにインストールされますが、別々のサーバにインストールすると、パフォーマンスを強化し、導入をリモート管理することができます。大規模な導入の場合は、専用サーバに Desktop Director および Studio をインストールします。小規模な導入（POC）の場合は、これらのサービスをデスクトップ コントローラと同じサーバにインストールできます。複数の XenDesktop コントローラを使用した導入では、個別のデスクトップ コントローラ コンソール スナップインを備えた単一の MMC コンソールを使用して各コントローラを管理できます。

Desktop Director

Desktop Director ダッシュボードは高度なビューを備えており、導入内の全マシンが表示されます。マシンは [All]、[Unregistered]、[High CPU]、[High Latency]（高 ICA 遅延メトリック）、[High Profile Load Time]（Profile Management ログイン時間メトリック）、[Failed Connection]、[Pending Update]（最新バージョンのディスクを使用していない Machine Creation Services によってプロビジョニングされたマシン）のカテゴリに分類されます。[High CPU]、[Latency]、[Profile Load Time] はしきい値との比較で測定され、このしきい値は管理者が設定する必要があります。[High Profile Load Time] メトリックは、Citrix Profile Management がインストールされている場合のみ表示されることに注意してください。デスクトップ リソース使用率とユーザ アプリケーション使用率を表示できるようにするには、Desktop Director と Citrix Edgesite を統合する必要があります。

Desktop Director ダッシュボードは高度なビューを備えており、各デスクトップ グループのマシン状態とサイト内の全マシンの状態について [Total]、[% Usage]（ユーザ セッションが実行されているマシンの割合）、および以下の各状態にあるマシンの数が表示されます。

- [In Use]（ユーザが接続しているマシン）
- [Disconnected]（セッションを実行中であるが接続されていないマシン）
- [Ready]（いつでも使用可能なマシン）
- [Unregistered] (動作しているがコントローラに登録されていないマシン）
- [Off]（動作していないマシン）

Desktop Director には、サイトのホストおよびコントローラのステータス アイコンなど、ホスト インフラストラクチャの健全性を表示できる高度なビューがあります。ホストの場合、vSphere または XenServer からの情報を使用して、CPU、メモリ、帯域幅（ネットワーク使用率）、ストレージ（ディスク使用率）のステータスと健全性が監視されます。コントローラの場合、サーバがオンライン状態か、すべてのサービスが稼動しているか、および、すべてのサービスがデータベースに接続されているかがアイコンで示されます。SCVMM で管理されている Hyper-V で動作するホストのステータスと健全性は表示されないことに注意してください。

Citrix Receiver

Citrix Receiver はデスクトップ仮想化エンドポイントで動作するアプリケーションで、Altiris や VXC Manager など標準的なデスクトップ ソフトウェア管理ツールを使用してインストール、更新、および管理する必要があります。エンド ユーザがデスクトップ コントローラにログオンしているときにデスクトップ プールが変更された場合、更新されたデスクトップが表示されるには、デスクトップ仮想化エンドポイントのレシーバ アプリケーションでアプリケーションを更新する必要があります。このタスクの実施方法は、デスクトップ仮想化エンドポイントのレシーバによって異なります。詳細については、ベンダーから提供されるレシーバのマニュアルを参照してください。

Citrix ツール

XenDesktop 環境の管理に使用できるその他のツールには、Citrix Profile Management ツールがあります。このツールは、Microsoft Windows OS が動作する仮想デスクトップでのユーザ パーソナライゼーション設定を管理するために使用されます。Citrix Workflow Studio には使いやすい GUI が用意されており、複数のコンポーネントを 1 つのワークフローに統合して連携させることができます。Citrix StorageLink を使用すると、ハイパーバイザ マネージャ（ vSphere など）は既存のストレージ システム（(NetApp など）のあらゆるリソースと機能を十分に活用することができます。

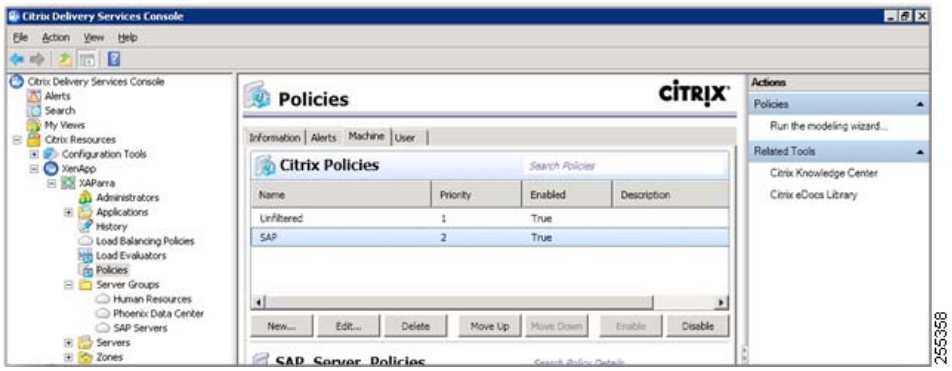
HDX Monitor は、HDX MediaStream for Flash や HDX RealTime を含む XenDesktop の HDX スタックの動作を検証するツールです。このツールを仮想デスクトップにインストールし、帯域幅使用率、セッションの設定、パフォーマンス メトリックなどの HDX エクスペリエンスについて有益な技術情報を入手します。

Citrix EdgeSight for Endpoints では、仮想デスクトップでのアプリケーション パフォーマンスが総合的に表示されます。管理者は、エンド ユーザ エクスペリエンスを監視および測定し、パフォーマンスの低いアプリケーションを特定し（アプリケーションのクラッシュとハングはすべて記録されます）、デスクトップ配信を最適化することができます。デスクトップ上で動作するエージェントによって収集されたデータは、定期的（通常はデスクトップがオフラインのとき）に Citrix EdgeSight サーバへ送信されます。

Citrix XenApp Delivery Services Console

Citrix XenApp 6.0 管理スイートを使用して、管理者は Cisco VXI 導入でのアプリケーション配信を管理できます。XenApp 6.0 には Citrix XenApp Delivery Services Console（Microsoft Management Console ベースの MMC）をはじめ、XenApp 環境を管理するための総合的なツール セットが用意されています。このツール セットを使用して、サーバ、サーバ ファーム、公開リソース、およびセッションのプロビジョニングと監視、アプリケーション アクセスの設定（Web インターフェイス と Citrix オンライン プラグインを使用）、ポリシーとプリンタの設定を行うことができます。このツール セットは、ロード バランシングの管理、アラートのトラブルシューティング、サーバ ファームの問題診断、よおび管理上の変更事項の追跡にも使用できます。さらに、サーバ パフォーマンス データの監視に使用することもできます。XenApp Delivery Services Console は、Active Directory グループ ポリシーと全面的に統合されているので、Microsoft System Center との統合も可能です。

図 62　　Citrix XenApp Delivery Services Console



Citrix XenApp では、以下のタイプのリソースを公開することで、情報とアプリケーション（コンテンツ）にアクセスできるようになります。すなわち、XenApp を実行するサーバにインストールされたアプリケーション（ユーザが公開されたアプリケーションにアクセスすると、そのアプリケーションはクライアント デバイス上でローカルに動作しているように見えます）、アプリケーション プロファイルにインストールされ、アプリケーション ハブのファイル サーバに保存されたストリーム配信アプリケーション（ユーザはプロファイルにアクセスし、各自のクライアント デスクトップ上で仮想化アプリケーションを実行します）、およびデータファイル（Web ページ、ドキュメント、メディア ファイル、スプレッドシート、URL など）です。これらのリソースは、サーバまたはデスクトップ上で仮想化できます。管理者は、XenApp Delivery Services Console の [Publish Application] ウィザードを使用してこれらすべてのリソース タイプを公開できます。

XenApp Delivery Services Console は、XenApp セッションの管理および監視に使用できます。管理者は、セッションのリセット、切断、またはログオフ、あるいはユーザへのメッセージ送信を実行することで、セッションを直接操作できます。また、コンソール ディスプレイを使用して、あるいはシャドウイングによって直接セッションを監視できます。たとえば、ユーザのクライアント デバイスに問題が発生し、アプリケーションのデータを失いたくない場合、管理者はユーザのセッションを切断できます。

XenApp Delivery Services Console では、ヘルス モニタリングと回復機能を使用して、サーバのパフォーマンスを監視できます。管理者は、ヘルス モニタリングと回復機能を使用してサーバ ファーム内のサーバをテストすることで、サーバの状態を監視し、健全性に関するリスクを発見できます。Citrix は、インポート可能なカスタマイズ済みのテストに加え、標準のテスト セットを提供します。XenApp に付属しているテストを使用して、Remote Desktop Services、XML Service、Citrix IMA Service、およびログイン/ログオフ サイクルなど複数のサービスとアクティビティを監視できます。

XenApp 管理スイートの一般的な管理目的の使用例

- XenApp へのユーザの追加
- XenApp へのサーバ デスクトップの追加
- XenApp でのアプリケーションの公開
- XenApp でのサーバ負荷の管理
- XenApp におけるユーザおよびサーバへのポリシーの適用

XenApp Delivery Services Console の使用に関するガイドライン

XenApp Delivery Services Console は Powershell 2.0 をサポートしており、自動インタラクションおよびプロビジョニングに使用できます。

コンソールの [Shadow Taskbar] を使用すると、ユーザのセッションをリモートで表示および制御したり、セッションをシャドウイングしたり、シャドウイングされた複数のセッションを切り替えたりすることができます。管理者は、Delivery Services Console を使用して ICA セッションのシャドウイングも実行できます。ローカル テキスト エコーや、低速ネットワークでのユーザ エクスペリエンスを改善するその他の機能を設定するには、SpeedScreen Latency Reduction Manager を使用します。

複数の XenApp ファームから成る導入（1 つのファームは XenApp 6 for Windows Server 2008 R2 を実行するサーバで構成され、別のファームは XenApp 5 を実行するサーバで構成されている場合など）では、個別の Delivery Services Console スナップインを備えた単一の MMC コンソールを使用して各ファームを管理できます。

コンソールの実行にはドメイン アカウントを使用することが推奨されます。ローカル管理者アカウントは使用可能ですが、ファーム内の全サーバですべてのローカル管理者のユーザ名とパスワードが同じでなければなりません。

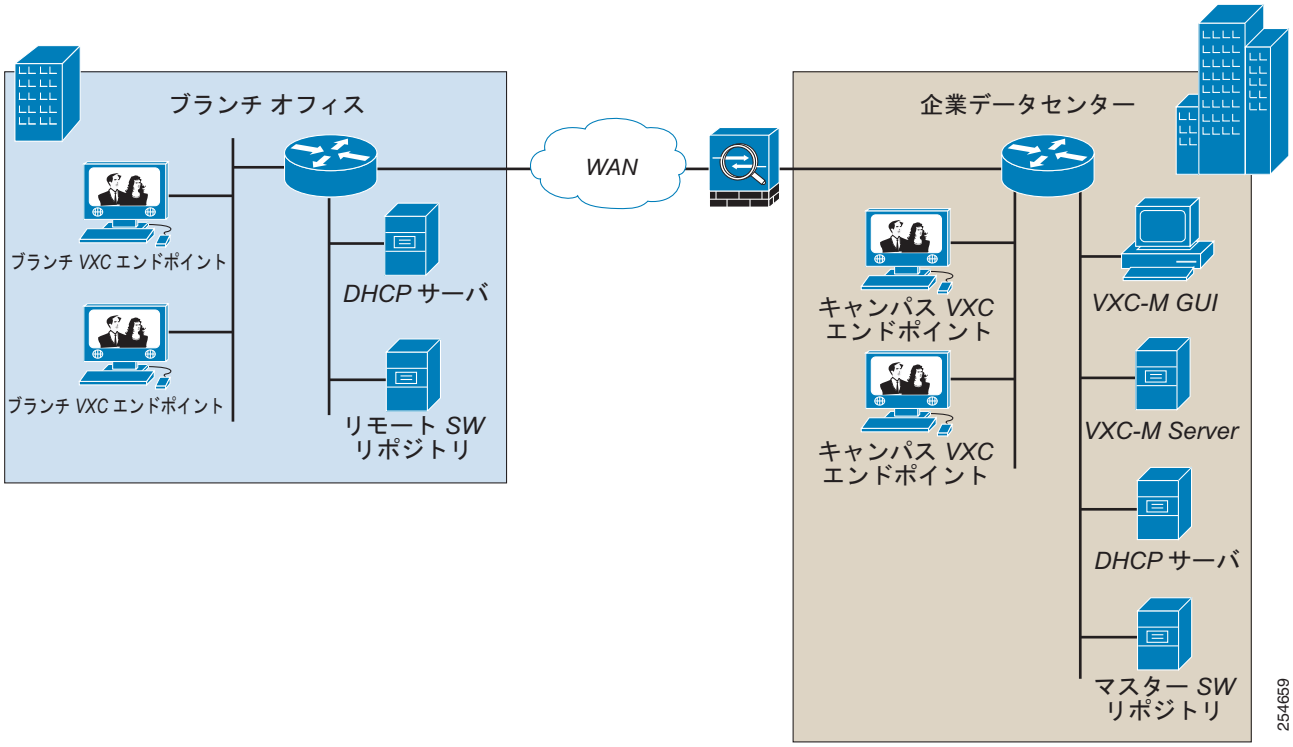
サーバ ファームおよびアプリケーションの検出は、XenApp 環境で追加または削除されたアイテム（デバイス、アプリケーションなど）をチェックする重要な作業です。XenApp 導入を検出する場合、管理対象の各ファーム内で XenApp を実行している少なくとも 1 台のサーバの名前または IP アドレスを指定します。

デフォルトでは、ファーム内のすべてのサーバでヘルス モニタリングと回復が有効になっており、付属しているテストはデータ コレクタを含む全サーバで実行されます。データ コレクタでヘルス モニタリングと回復を実行したくない場合は、この機能を手動で無効にする必要があります。

Cisco VXC Manager

Cisco VXC Manager（VXC-M）は、Cisco VXI システムにおける Cisco VXC エンドポイントのエンタープライズ規模の展開を一元的に管理するために使用します。VXC-M を使用することにより、VXC エンドポイントの効率的なプロビジョニング、モニタリング、トラブルシューティング、資産管理とインベントリの実行、デバイスのリモート制御とアクセス、エンタープライズ ポリシーに基づいたアプローチによるファームウェアや設定の更新、およびレポートの生成が可能になります。VXC-M は、高度なデバイス制御、スクリプト、およびイメージングの機能をサポートします。セキュア（HTTPS ベース）イメージング、圧縮、および帯域幅の調整による効率化、デバイスのヘルス ステータス レポート作成、シャドウイング、デバイスのリモート制御とスクリプト、およびデフォルトのデバイス設定、デバイス検出と詳細なデバイス ハードウェアおよびソフトウェア資産情報の提供、クライアント クローニング機能（管理者は、この機能を使用して参照クライアントのイメージや設定をキャプチャし、全社間に展開できます）などが、VXC-M によってサポートされます。また、イメージを展開するためのマスターおよびリモート ソフトウェア リポジトリの使用を含めた分散型のスケーラブルなアーキテクチャもサポートされます。

図 63　　VXC-M アーキテクチャ

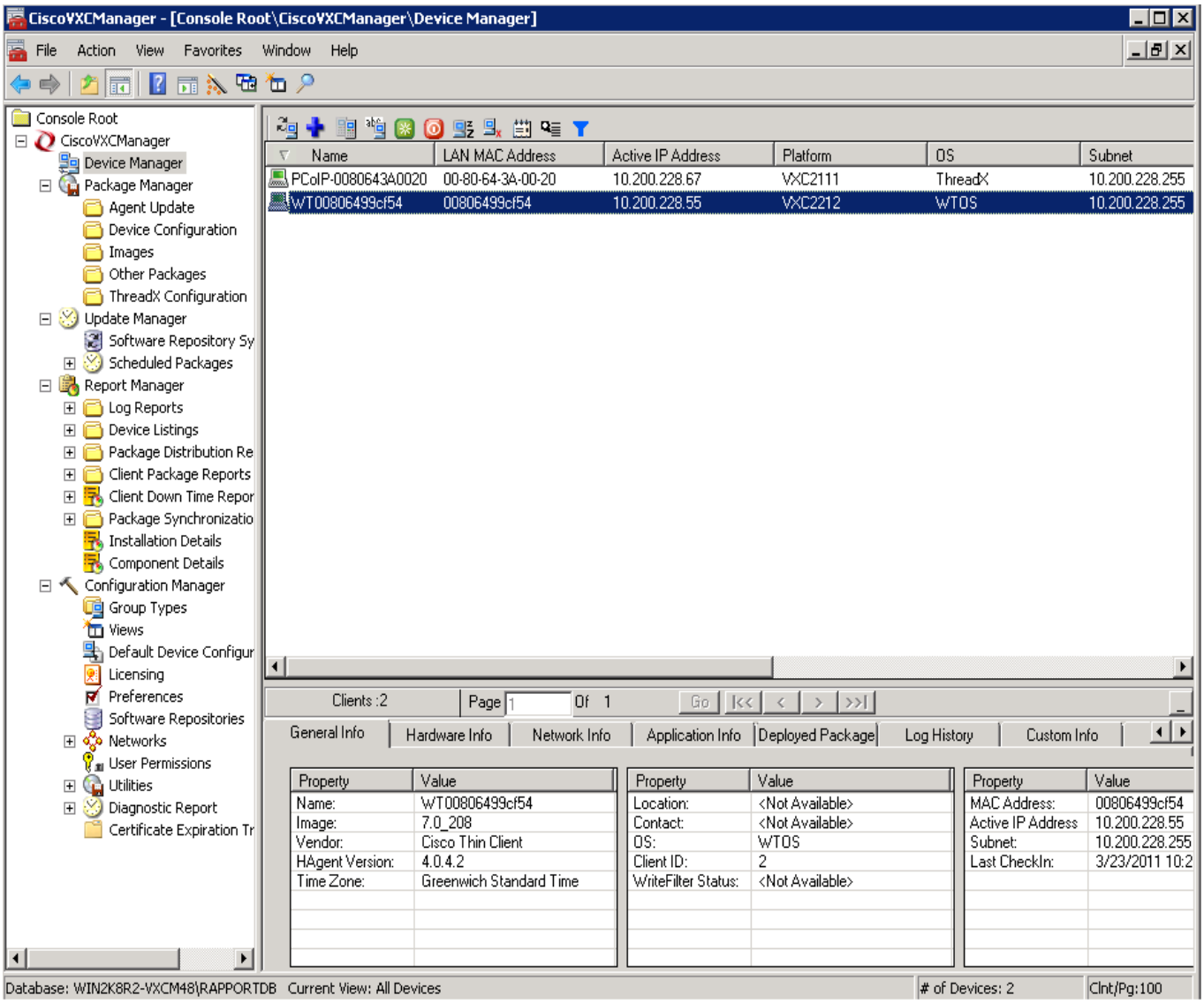


Cisco VXC Manager に含まれるコンポーネントには、管理用の管理コンソール GUI（MMC ベースのスナップイン）、エンドポイントとの通信に使用するデバイス管理サービス（HTTP、DHCP プロキシ、および TFTP のサポートを含む）、設定とデバイス情報を保存するデータベース、および、イメージ、コンフィギュレーション ファイル、パッケージ保存用のマスター ソフトウェア リポジトリがあります。VXC クライアントは、VXC-M サーバとの通信を有効にする Web エージェントを実行します。

VXC-M 管理コンソールには、デバイス、パッケージ、アップデート、レポート、およびコンフィギュレーション マネージャが含まれます。デバイス マネージャには、VXC-M サーバにチェックインするすべてのデバイスのヘルス ステータスが表示されます。デバイス ステータスは、デバイスのチェックイン ステータスによって緑色、黄色、または赤色を示します。デバイスは、デバイス ステータスを示し、アップデート（設定やファームウェアのアップデート）を確認するために、サーバに定期的にチェックインします。ICA VXC クライアントのデフォルトのデバイス チェックイン間隔は 10 分です。電源がオフになっているデバイスは、デバイス リストに赤色で表示されます。デバイス ステータスには、デバイスがアイドル状態であるか、リモート デスクトップ セッションでアクティブに使用されているかどうかという情報は含まれません。デバイス マネージャには、デバイス ハードウェアおよびソフトウェア プロファイル（OS バージョンを含む）、インストールされているソフトウェア、ネットワーク設定、およびインストールされているパッケージに関する詳細情報も含まれます。デバイスは、OS タイプ、地理的なロケーション、建物、階、部署、またはサブネットに従って論理的にグループ分けすることができます。これによって、ステータスの表示、ポリシーの適用、および特定のデバイス グループに対するパッケージの展開が容易になります。

デバイス検出機能を使用すると、デスクトップ仮想化エンドポイントをデバイス マネージャに手動で追加することも、検出機能を実行する IP アドレス範囲やサブネットを指定することでデバイス マネージャで動的に検出することもできます。VXC Manager はリブート、シャットダウン、およびウェイクアップ（Wake on LAN を使用）などの操作を含め、デスクトップ仮想化エンドポイントをリモートで制御できます。管理者はシャドウイングにより、DV エンドポイントのコンソールにリモートからアクセスし、設定の確認やリモート デスクトップ セッションのセットアップを行うことができます。シャドウイングは、エンドポイントの問題をリアル タイムでトラブルシューティングするのに役立ちます。エンドポイントで使用できる管理機能は、エンドポイントの OS またはデバイス タイプによって異なります。

図 64　　VXC-M デバイス マネージャ コンソール



パッケージ マネージャを使用して、パッケージを VXC エンドポイントに展開します。パッケージは、一連のアクション（デバイス設定の変更、設定のアップロード、ファームウェア イメージのダウンロード、シャットダウン、リセット）の実行をデバイスに支持するファイル（スクリプト、コンフィギュレーション ファイル、またはファームウェア イメージ）の集合です。VXC-M スクリプト ビルダー ユーティリティは、パッケージに組み込むスクリプトの作成に使用できます。このユーティリティを使用するときは、管理者はターゲット デバイスの OS（WTOS for ICA VXC クライアントなど）を選択する必要があります。パッケージを企業全体に展開する前に、テスト デバイスで検証することが推奨されます。パッケージ マネージャでの Web エージェントの更新は VXC クライアントに適用されないことに注意してください。VXC クライアントを実行する Web エージェントを更新するには、デバイスのファームウェアを変更します。

アップデート マネージャは、規定の時間（オフピーク時間など）にパッケージをデバイスに展開するスケジュールを組むのに使用します。スケジュールされた時間は、クライアント デバイスの時間帯に自動的に調整されます。たとえば、パッケージをデバイスのグループに展開することで、スケジュールされた時間にファームウェアを更新したり、毎日午後 6 時にユーザ セッションをクリアするためにグループ デバイスをリブートしたりすることができます。レポート マネージャを使用すると、VXC-M への管理上の変更をトラブルシューティングするためのログ レポート、管理対象のデバイス一覧が含まれたデバイス リスト レポート、およびパッケージの導入ログとステータスが含まれたパッケージ配布レポート（このレポートには、デバイスへの正常なパッケージ ダウンロードが表示されます）を生成できます。

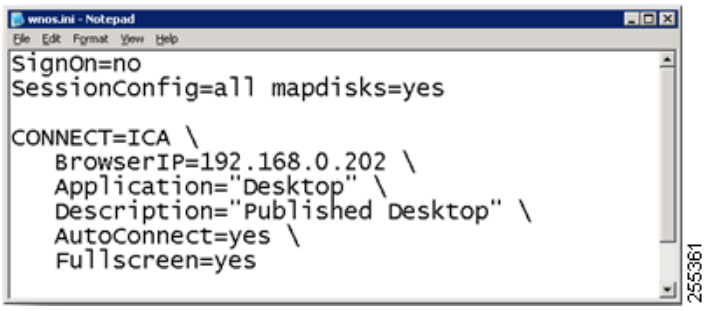
コンフィギュレーション マネージャを使用すると、VXC-M サーバ上の設定のカスタマイズ、デバイス グループの作成、サブネットと IP 範囲の設定、およびリモート ソフトウェア リポジトリのプロビジョニングを行うことができます。VXC-M 設定には、デバイスのチェックイン間隔、デバイス セキュリティの有効化、ロギング レベルの変更、タイムアウトの設定、および Default Device Configuration（DDC）の有効化が含まれます。タイムアウトの設定は、すべてのエンドポイントにグローバルに設定することも、サブネットに基づいたエンドポイントのサブセットに対して設定することもできます。たとえば、遅延の大きい WAN リンク上にあるエンドポイントに対してタイムアウトを調整できます。低帯域幅のリンク全体にわたる同時イメージ アップデートの数を制限することが推奨されます（制限することで、タイムアウトによる障害が発生するほど低速化しないようにします）。この設定は、コンフィギュレーション マネージャでプロビジョニングできます。また、VXC-M では、役割ベースのアクセスと、権限を関連付けた管理者のプロビジョニングがサポートされます。たとえば、読み取り専用権限は、特定の管理者グループに割り当てることができます。Active Directory（AD）との統合により、複数の管理ユーザを追加して、論理ビュー、エンドポイント プロパティ、OS、およびデバイスのタイプやサブネットによって編成された別個のエンドポイント プールの管理を任せることができます。

管理者は、リポジトリ作成および管理機能を使用して、配布用のソフトウェア、イメージ、およびコンフィギュレーション アップデートのリポジトリを容易に作成し、管理できます。VXC Manager サーバには、イメージおよびパッケージ サーバとして機能するマスター ソフトウェア リポジトリが含まれます。マスター リポジトリは、ブランチ オフィスに存在するリモート ソフトウェア リポジトリと同期させることができます。ブランチ オフィスなどのリモート ロケーションについては、エンドポイントに対してローカルのリモート ファイル リポジトリを使用して WAN 帯域幅を節約することが推奨されます。ファイル転送は TCP ベースのプロトコル（FTP および HTTP）を使用して実行されるので、WAN 上のファイル転送では、Cisco WAAS の高速化、キャッシング、および圧縮機能の利点が活かされます。

VXC Manager Default Device Configuration（DDC）は、ポリシー管理ツールであり、管理者はこのツールを利用して OS イメージ、スクリプト、パッケージ、およびその他の設定をシン クライアント エンドポイントに自動的に導入するルールを作成できます。管理者は DDC を使用して、デバイス グループに対するデフォルトのソフトウェアおよびデバイス設定を行い、エンドポイントの管理を簡素化し、完全に自動化することができます。たとえば、グローバル組織の管理者は DDC を使用して、サブネットを特定の国にマッピングできます。エンドポイントがネットワークに初めて接続されると、DDC はサブネット情報を使用して、DV エンドポイントに適切な言語や設定をプロビジョニングします。DDC 機能により、特定の OS を実行する特定のグループ（建物やサブネットなど）のすべてのデバイスに対して、デバイスの設定とイメージ バージョンの適合性が保証されます。この機能は、サブネット、物理的なロケーション、またはデバイス グループ内の変更に基づいて、デバイス設定の変更を自動的に実装するのに役立ちます。たとえば、デバイスやスイッチの物理ポートの VLAN 割り当てを変更するだけで、VXC クライアントを XenApp 環境から XenDesktop 環境へ容易に移行し、自動的に再設定することができます。DDC は、VXC-M サーバにチェックインするときのデバイスのブートアップ段階で、デバイスに適用されます。

ICA VXC クライアント用のパッケージにはスクリプトと、デバイスの設定が記述された INI コンフィギュレーション ファイルが含まれています。パッケージ マネージャを使用してパッケージを ICA VXC ゼロ クライアントに導入することはできません。パッケージはデバイス用の DDC に格納する必要があり、デバイスのブート フェーズまたはチェックイン時に導入されます。このアップデートは、デバイス マネージャでデバイスをリブートすることで起動できます。あるいは、デバイス マネージャでデバイスを選択し、[refresh device information] を開始してチェックインを実行してください。コンフィギュレーション マネージャでは、WTOS 設定の [return ftp/ini at checkin] を有効にする必要があります。これにより、デバイスが DHCP から取得した情報は、設定済みのファイル サーバ パスによって上書きされます。デバイスに関連付けられたネットワーク設定のサーバ パスが更新されたことを確認するには、VXC-M デバイス マネージャを使用します。

図 65　　ICA VXC クライアント用 INI コンフィギュレーション ファイルのサンプル



VXC Manager の一般的な使用例

- 自動検出を使用してエンドポイントを VXC Manager に追加する
- デバイス マネージャを使用してエンドポイントの再起動やシャットダウンを行う
- デバイスのヘルス ステータスを監視する
- アラートやロギング レポートを生成する
- リモート デスクトップ セッションで使用されているデバイスにリモート アクセスする
- パッケージ マネージャを使用してデバイス ファームウェアをアップグレードする
- パッケージ マネージャを使用してデバイスの設定を変更する

DDC for ICA VXC エンドポイント用 DDC の設定手順

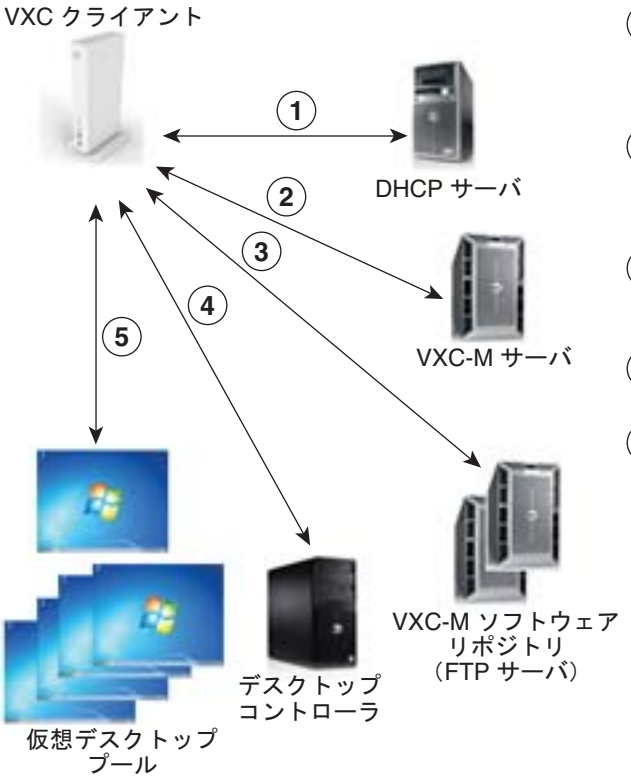
1. VXC エンドポイント用のコンフィギュレーション ファイル（ini ファイル）を作成し、VXC-M サーバのイメージ ディレクトリに保存します。
2. コンフィギュレーション ファイルが含まれたカスタム WTOS パッケージをパッケージ マネージャに登録します。
3. VXC デバイス用の DDC を作成し、カスタム パッケージを目的のデバイス グループに割り当てます。
4. VXC-M を設定し、コンフィギュレーション マネージャ設定の WTOS 設定でコンフィギュレーション ファイルの場所を指定します。
5. コンフィギュレーション マネージャ設定の [Device Manager Preferences] で DDC の適用をアクティブにします。
6. デバイス マネージャの [Refresh device information] を使用して、デバイスのチェックインを開始します。

VXC Manager の使用に関するガイドライン

多数のデスクトップ仮想化エンドポイントを展開するときは、一元的な設定アプローチが推奨されます。このアプローチによって、エンドポイントは自動的に VXC Manager やデスクトップ コントローラのロケーションを検出し、エンドポイント自体を適切なイメージと設定で更新します。エンドポイントには、ブートアップ時に、DHCP、DNS、および FTP サービスを使用してネットワーク設定、VXC-M サーバのロケーション、およびデスクトップ コントローラのロケーションがプロビジョニングされます。ここで使用する特定の DHCP オプションの詳細については、VXC クライアントおよび VXC Manager のドキュメントを参照してください。

また、ファイル サーバのロケーションから、更新されたイメージや設定をダウンロードするようにエンドポイントに指示するコンフィギュレーション ファイルを取得することもできます。DV エンドポイントは、エンド ユーザがリセットしたり、リブートしたりできます。代わりに、管理者が電源オンの VXC クライアントを一元的に管理することも（EnergyWise をサポートする PoE スイッチおよび EnergyWise Orchestrator を使用）、管理者が VXC Manager を使用してこのタスクを一元的に開始し、設定およびイメージ アップデートをエンドポイントにプッシュすることもできます。これらの設定（ファイル サーバ、VXC Manager サーバ、およびデスクトップ コントローラの場所）は、コンソールまたは Web インターフェイスを介してエンドポイントにアクセスすることにより、手動でプロビジョニングすることもできます。設定やイメージを保存するためのディレクトリ構造、および展開されるデスクトップ仮想化エンドポイントの各タイプに対応するコンフィギュレーション ファイルのフォーマットなど、マスター ファイル サーバ リポジトリの設定に関する特定の手順については、Cisco VXC のドキュメントを参照してください。

図 66　　VXC クライアントのブート プロセス



1. VXC クライアントが DHCP サーバに接続し、サーバは標準的な DHCP 情報と、カスタム オプション タグ 186 による VXC-M サーバの IP アドレスを返します。
2. VXC クライアントは VXC-M サーバにチェックインし、VXC-M ソフトウェア レポジトリ上のパスを含む DDC 設定でデバイスがアップデートされます。
3. VXC クライアントは、VXC-M ソフトウェア レポジトリに接続し、このデバイスに割り当てられている設定を検索します。
4. VXC クライアントは、INI ファイルに定義されているデスクトップ コントローラ サーバに接続します。
5. ユーザが VXC クライアントにログインし、リモート デスクトップ セッションを開始します。

ICA VXC エンドポイントを管理するには、デバイス コンソールで使用可能な画面ディスプレイを使用するか、VNC を使用してデバイス コンソールにリモート アクセスするか、DHCP オプションを使用してエンドポイントをコンフィギュレーション ファイル（INI ファイル）が保存されたファイル サーバへ誘導するか、あるいは VXC マネージャの DDC 機能を使用します。VXC エンドポイントは、DHCP オプションの使用や、サーバのロケーションを識別する標準サービス（SRV）および DNS レコードの使用を通じて、VXC-M サーバ ロケーションを学習できます。VXC-M サーバ ロケーション（IP アドレス、ポート、およびセキュア ポート）を指定するには、DHCP オプション（186、190、および 192）を使用します。または、VXC エンドポイントが DNS サーバに VXC-M サーバ ロケーションを照会します（ICA VXC クライアントではホスト名「vxcmanager」が使用されます）。DNS の使用は、DHCP サービスを変更できない展開シナリオ（たとえば、カスタマー サイトにあるブランチ ルータ上など）で役立ちます。VXC-M サーバ ロケーションを ICA VXC クライアント INI コンフィギュレーション ファイルで設定することも可能です。

（注） VXC-M サーバ ロケーションは、ICA VXC クライアント コンソール上でローカルに設定される場合もあります。

デバイスに VXC-M ロケーションを通知するもう 1 つの方法として、VXC-M デバイス マネージャでエンドポイントの手動または自動検出を使用する方法もあります。デバイスの自動検出を行うサブネットおよび IP 範囲を定義するには、サブネット マネージャを使用します。この方法は、VXC-M サーバを検出するためにデバイスをリモートからリブートできない場合に役立ちます。中央ファイル サーバ ロケーション（161：ファイル サーバ ロケーションの IP アドレス、162：ファイル サーバのルート パス）を指定する DHCP オプションを使用して、ICA VXC エンドポイントで使用される設定を制御できます。この設定では、エンドポイントの設定（ログイン画面、ICA サーバ、XenApp の設定）を指定できます。

ICA VXC デバイスの INI コンフィギュレーション ファイルの作成および変更には、テキスト エディタを使用する方法が推奨されます。コンフィギュレーション ジェネレータ ツール（フリーウェア）は、コンフィギュレーション ファイルの作成にも使用できます。

エンドポイントおよび管理コンソールと通信するには、VXC Manager が使用するネットワーク上で、VXC-M が使用するすべてのコミュニケーション ポート（HTTP が 80、280、443、FTP が 21、データベースが 1433、および VNC が 5900）が開いていることを確認してください。サーバが使用するポートの一覧については、Cisco VXC-M のドキュメントを参照してください。

VXC Manager は、1 台のサーバにインストールすることも、大規模な展開用に複数のサーバにインストールすることもできます（カスタマイズされたインストール手順を使用して、複数のサーバに分散されるサービスを利用します）。複数の管理コンソールをインストールして、複数の管理者からのリモート アクセスを容易にすることもできます。

電源管理機能を使用すると、エンドポイントの電源オン/オフをスケジュールされた時間に行ってエネルギーを節約できます。VXC-M によって電源をオンにできるのは、WoL をサポートするデバイスだけであることに注意してください。

リモート ソフトウェア リポジトリが、マスター ソフトウェア リポジトリに同期していることを確認します。Microsoft の同期化サービスを使用して、ソフトウェア リポジトリを同期させます。WAN 全体でリモート ソフトウェア リポジトリを使用するときは、ブランチにあるサブネットごとに 1 つのリモート リポジトリを展開することが推奨されます。

推奨されるトラブルシューティング ツールには、デバイスとサーバの通信を監視する Wireshark、サーバ上のイベントやエラー（ データベース通信など）をロギングする Microsoft デバッグビューア、および VXC-M サーバ ログ レポートの使用が挙げられます。

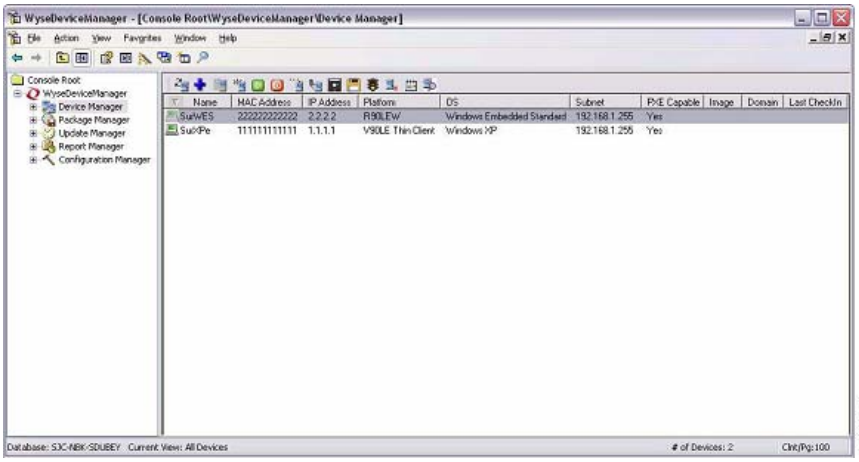
カスタム レポートは、ODBC 準拠のツール（ Crystal Reports、MS-ACCESS、MS-SQL クライアント ツールなど）や、VXC-M データベースにアクセスできるツールを使用して生成できます。

VXC Manager サーバは、IBM Tivoli NetView または CA Unicenter にアドオン モジュールとして統合できます。IT プロフェッショナルは、アドオン モジュールを使用して、IBM Tivoli NetView や CA Unicenter Network and Systems Management（NSM）など、サポートされているサードパーティの管理スイートから何千もの Cisco デスクトップ仮想化エンドポイントの整理、アップグレード、制御、およびサポートを容易に行うことができます。管理者はこのアドオン ソフトウェアにより、既存の管理フレームワークを使用して、すべてのネットワーク デバイスを包括的かつ統合的に表示できます。このアドオンは、Cisco デスクトップ仮想化エンドポイントと現在のフレームワークを統合し、管理コンソールからすべての機能へのアクセスを可能にします。この統合により、IT プロフェッショナルに必要とされる学習時間が減り、包括的なエクスペリエンスが実現します。

Wyse Device Manager

Wyse Device Manager（図 67）の使用により、管理者は Wyse デスクトップ仮想化エンドポイントのイメージ（OS）、設定、および資産管理、リモート制御、モニタリング、ならびにシャドウイングを実行できます。また、Wyse Device Manager を使用して、エンタープライズ規模のエンドポイント デバイス検出の計画と実行、エンドポイント パラメータのアップロードとダウンロード、およびエンドポイントへのソフトウェア パッケージの配布を行うことができます。シン クライアントのクローニング機能もサポートされており、管理者はこれを利用して参照先のシン クライアントのイメージと設定をキャプチャし、企業全体に展開できます。カスタマイズしたスクリプトを作成してエンドポイントに配布し、エンドポイント デバイスのセットアップと設定を自動化することも可能です。スクリプトについては、企業全体に展開する前にテスト デバイスで検証する必要があります。LAN、WAN、または無線ネットワーク全体で何千もの Microsoft Windows Embedded Standard（WES）または Compact Edition（CE）、Linux、Wyse ThinOS、または Wyse XP Embedded（XPe）シン クライアント デバイスの展開がサポートされます。Wyse Device Manager Enterprise Edition は、セキュリティ、スケーラビリティ、およびパフォーマンス機能が追加されていることから、大規模な導入に推奨されます（Workgroup Edition がサポートするエンドポイントの最大数は 750 です）。機能の一覧については、Wyse のドキュメントを参照してください。より一元的で実践的なアプローチを可能にするため、Wyse Device Manager を使用して Wyse デスクトップ仮想化エンドポイントを管理してください。

図 67　Wyse Device Manager コンソール



Wyse Device Manager の資産情報収集機能では、エンドポイントのハードウェア リビジョンと、適用されているソフトウェア OS、アプリケーション、およびアドオン バージョンを追跡できます。Wyse Device Manager は、各デバイスのすべての資産情報（ハードウェア資産情報や、各デバイスにインストールされているソフトウェアの情報を含む）を監視し、保存します。ソフトウェア情報には、オペレーティング システムと、エンドポイント デバイスに適用されているすべてのアプリケーションおよびアドオンが含まれます。Wyse Device Manager は、XPe クライアント OS を実行しているシン クライアントで書き込みフィルタのステータスを監視できます。管理されるエンドポイントのリスト、更新がスケジュールされたエンドポイント、現在のエンドポイント ソフトウェアのリビジョン レベル、サーバ ログ、およびエンドポイント アップタイムに基づいたエンドポイントの可用性を示すレポートを生成できます。

デバイス管理機能の使用により、管理者は、デスクトップ仮想化エンドポイントのステータスをリアルタイムで表示および監視できます。すべてのエンドポイントの最新ステータス情報が自動的に提供されるように、Wyse Device Manager を設定できます。エンドポイントをリモートで管理するには、エンドポイントに Wyse Device Manager エージェントをインストールする必要があります。エージェントには、Wyse Device Manager サーバのアドレスのプロビジョニングが必要です。このプロビジョニングは、デバイス検出プロセス時に自動的に実行することも、エンドポイントで手動により実行することもできます。また、エンドポイントのブートアップ時に DHCP オプションを使用するか、サーバのロケーションを識別する標準サービス（SRV）および DNS レコードを使用して実行することもできます。エンドポイントで動作するエージェントは、ハートビート メカニズムを使用してデバイス マネージャに定期的にチェックインし、アップデートの有無を調べます。また、エージェントは、ステータスの変更をサーバに報告します。デバイス検出機能を使用すると、デスクトップ仮想化エンドポイントをデバイス マネージャに手動で追加することも、検出機能を実行する IP アドレス範囲を指定することでデバイス マネージャで動的に検出することもできます。

Wyse Device Manager はリブート、シャットダウン、およびウェイクアップ（Wake on LAN を使用）などの操作を含め、デスクトップ仮想化エンドポイントをリモートで制御できます。管理者は、シャドウイング（VNC を使用）により、エンドポイントのコンソールにリモート アクセスし、設定の確認やリモート デスクトップ セッションのセットアップを行うことができます。シャドウイングは、エンドポイントの問題をリアル タイムでトラブルシューティングするのに役立ちます。管理者は、エンドポイント コンソールから設定に直接アクセスできるほか、一部のゼロ クライアントおよびシン クライアント（Viance および P20）の使用により、Web ベースの GUI を介して設定情報にリモート アクセスできます。

デスクトップ仮想化エンドポイントのアップデートには、イメージ（OS）、アプリケーション（エージェント）、および設定（ネットワークと接続）のアップデートが含まれます。これらのアップデートは、デバイス マネージャ サーバによって（ダウンタイムを減らし、オフピーク時間に移行するため）スケジュールに従って開始される場合と、デバイスがサーバにチェックインするときに開始される場合があります。管理者は、リポジトリ作成および管理機能を使用して、配布用のソフトウェア、イメージ、およびコンフィギュレーション アップデートのリポジトリを容易に作成し、管理できます。Wyse Device Manager サーバには、イメージおよびパッケージ サーバとして機能するマスター ソフトウェア リポジトリが含まれます。マスター リポジトリは、ブランチ オフィスに存在するリモート ソフトウェア リポジトリと同期させることができます。ブランチ オフィスなどのリモート ロケーションについては、WAN 帯域幅を節約するため、エンドポイントにとってローカルであるリモート ファイル リポジトリを使用してください。ファイル転送は TCP ベースのプロトコル（FTP および HTTP）を使用して実行されるので、WAN 上のファイル転送では、Cisco WAAS の高速化、キャッシング、および圧縮機能の利点が活かされます。

多数のデスクトップ仮想化エンドポイントを展開するときは、一元的な設定アプローチが推奨されます。このアプローチによって、エンドポイントは自動的にデスクトップ コントローラのロケーションを検出し、エンドポイント自体を適切なイメージと設定で更新します。エンドポイントには、ブートアップ時に DHCP を介してネットワーク設定とデスクトップ コントローラのロケーションがプロビジョニングされる必要があります。ここで使用する特定の DHCP オプションの詳細については、Wyse シン クライアントおよび Wyse Device Manager のドキュメントを参照してください。

また、ファイル サーバのロケーションから、アップデートされたイメージや設定をダウンロードするようにエンドポイントに指示する初期化ファイルを取得することもできます。手順を示す電子メール通知を使用して、エンドポイントのリセットやリブートを行うようにユーザに指示することも、管理者が Wyse Device Manager を使用してこのタスクを一元的に開始し、設定やイメージのアップデートをエンドポイントにプッシュすることもできます。これらの設定（ファイル サーバ、Wyse Device Manager サーバ、およびデスクトップ コントローラのロケーション）は、コンソールまたは Web インターフェイスを介してエンドポイントにアクセスすることにより、手動でプロビジョニングできることも覚えておいてください。設定やイメージを保存するためのディレクトリ構造、および展開されるデスクトップ仮想化エンドポイントの各タイプに対応するコンフィギュレーション ファイルのフォーマットなど、マスター ファイル サーバ リポジトリの設定に関する特定の手順については、Wyse のドキュメントを参照してください。

（注） Citrix Desktop Delivery Controller は Web サーバであるため、ファイル サーバとして使用することもできます。

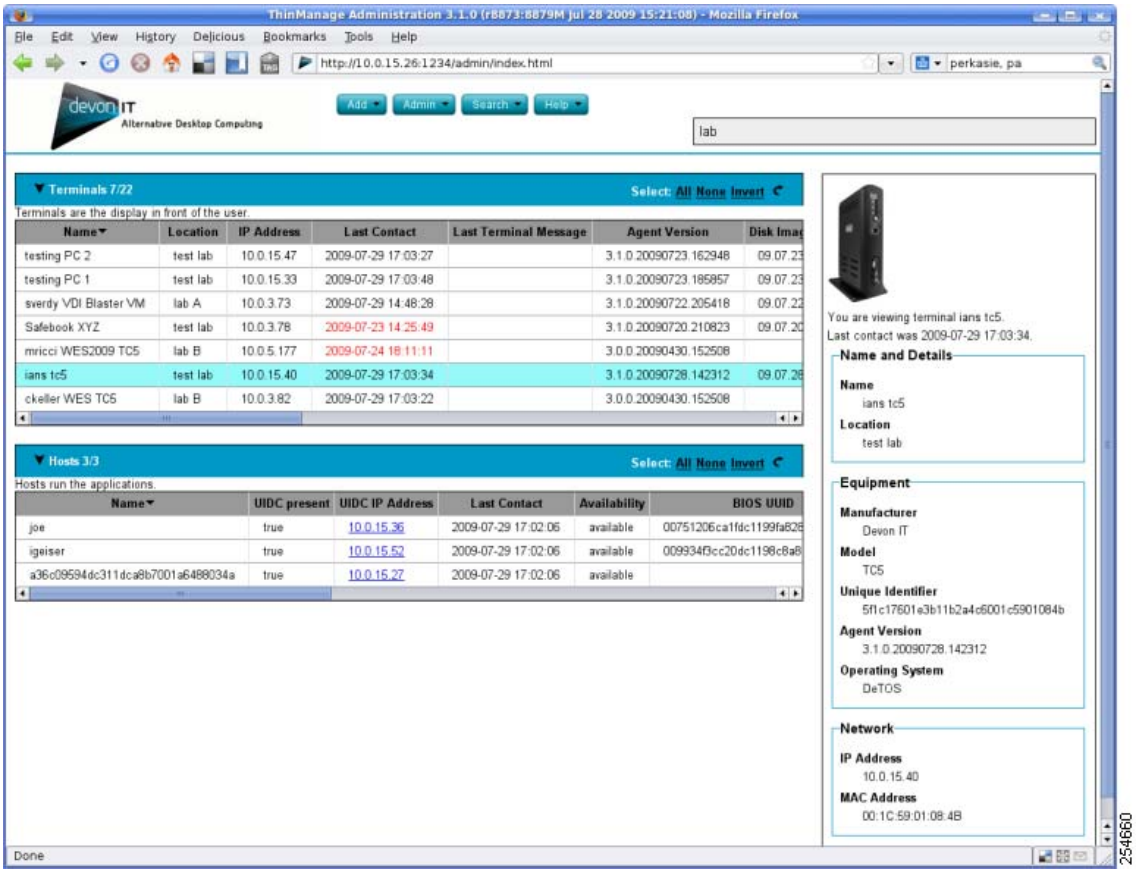
Wyse Device Manager Default Device Configuration（DDC）は、ポリシー管理ツールであり、管理者はこのツールを利用して OS イメージ、スクリプト、パッケージ、およびその他の設定をシン クライアント エンドポイントに自動的に展開するルールを作成できます。管理者は DDC を使用して、デバイス グループに対するデフォルトのソフトウェアおよびデバイス設定を行い、エンドポイントの管理を簡素化し、完全に自動化することができます。たとえば、グローバル組織の管理者は DDC を使用して、サブネットを特定の国にマッピングできます。エンドポイントがネットワークに初めて接続されると、Wyse Debvice Manager DDC はサブネット情報を使用して、シン クライアント エンドポイントに適切な言語や設定をプロビジョニングします。

Wyse Device Manager サーバは、IBM Tivoli NetView または CA Unicenter にアドオン モジュールとして統合できます。IT プロフェッショナルは、アドオン モジュールを使用して、IBM Tivoli NetView や CA Unicenter Network and Systems Management（NSM）など、サポートされているサードパーティの管理スイートから何千もの Wyse デスクトップ仮想化エンドポイントの整理、アップグレード、制御、およびサポートを容易に行うことができます。管理者はこのアドオン ソフトウェアにより、既存の管理フレームワークを使用して、すべてのネットワーク デバイスを包括的かつ統合的に表示できます。アドオンは、Wyse デスクトップ仮想化エンドポイントと現在のフレームワークを統合し、管理コンソールからすべての機能へのアクセスを可能にします。この統合により、IT プロフェッショナルに必要とされる学習時間が減り、包括的なエクスペリエンスが実現します。

Devon シン クライアント管理

Devon ThinManage Version 3 のシン クライアント管理により、管理者は、Devon デスクトップ仮想化エンドポイントのプロビジョニングと監視を行うことができます。Devon シン クライアント管理では、エンドポイント イメージとエージェントのアップデート、設定のプロビジョニング、および設定とシャドウイングを適用するためのプロファイルの使用がサポートされます。Devon ThinManage サーバは、シン クライアント マネージャと接続マネージャの両方の役割を果たします。シン クライアント エージェントはシン クライアント エンドポイントで動作し、Devon ThinManage サーバと通信します。新規機能を有効にして既知の問題を修正するには、エージェントの更新が必要になる場合があります。サーバ コンソールには、Web ブラウザを介してアクセスします（図 68）。

図 68　　DevonIT シン クライアント管理



Devon ThinManage の使用に関するガイドライン

（注）　Devon ThinManage サーバは、VMware Server または Player で動作する仮想アプライアンスとして配布されます。VMware vConverter の使用により、このサーバを VMware ESXi ホストで動作する仮想マシンに変換できます。

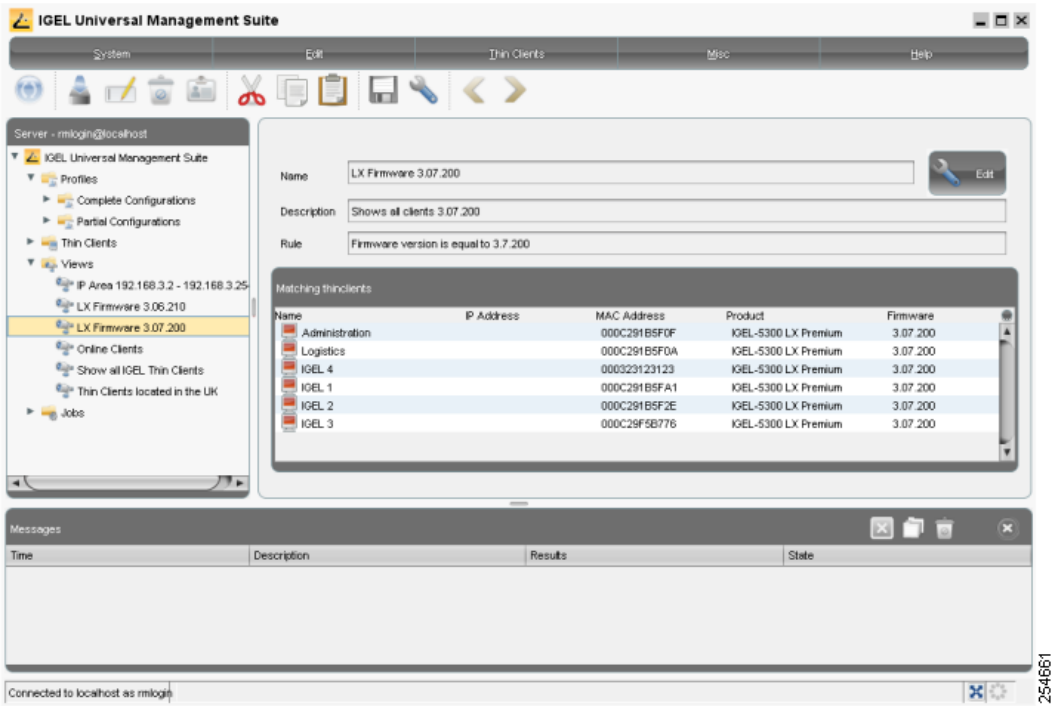
- リアル タイムでユーザをサポートしたり、問題をトラブルシューティングしたりするには、シャドウイング機能を使用してエンドポイント コンソールにリモート アクセスします。Devon ThinManage サーバは、モニタリングやトラブルシューティングに役立つイベントロギング機能をサポートします。

- Devon ThinManage サーバの使用により、デスクトップ仮想化エンドポイントの設定、接続設定、および完全なディスク イメージのクローニングが可能になります。エンドポイントの設定には、ディスプレイ、サウンド、キーボード、マウス、およびネットワーク設定が含まれます。管理者は Devon ThinManage サーバを使用して、これらの設定を 1 台のエンドポイントからクローニングし、データベースに保存してから、他のエンドポイントに適用できます。接続設定には、エンドポイントを接続サーバに接続する方法を指定するパラメータが含まれます。エンドポイント イメージは、ファイル サーバに保存し、FTP または NFS プロトコルを使用してアクセスできます。
- 復元機能を使用して後で復元できるよう、バックアップ機能を使用して現在の管理状態のスナップショットを作成します。このアプローチにより、ディザスタ リカバリのほか、イメージ アップグレード後の管理設定およびデバイス インベントリの維持が可能になります。

IGEL Universal Management Suite

IGEL Universal Management Suite（UMS）Version 3 は、IGEL デスクトップ仮想化エンドポイントの一元管理を可能にします。この管理スイートでは、エンドポイントに対する適切なプロファイル設定、イメージ管理、診断、シャドウイング、およびレポートの自動プロビジョニングがサポートされます。IGEL UMS コンソール（図 69）は、IGEL UMS サーバ用の GUI です。IGEL UMS コンソールでは、複数の IGEL UMS サーバを制御できます。Cisco VXI システムでの IGEL デスクトップ仮想化エンドポイントの大規模な展開を管理するには、IGEL UMS を使用してください。

図 69　　IGEL UMS GUI



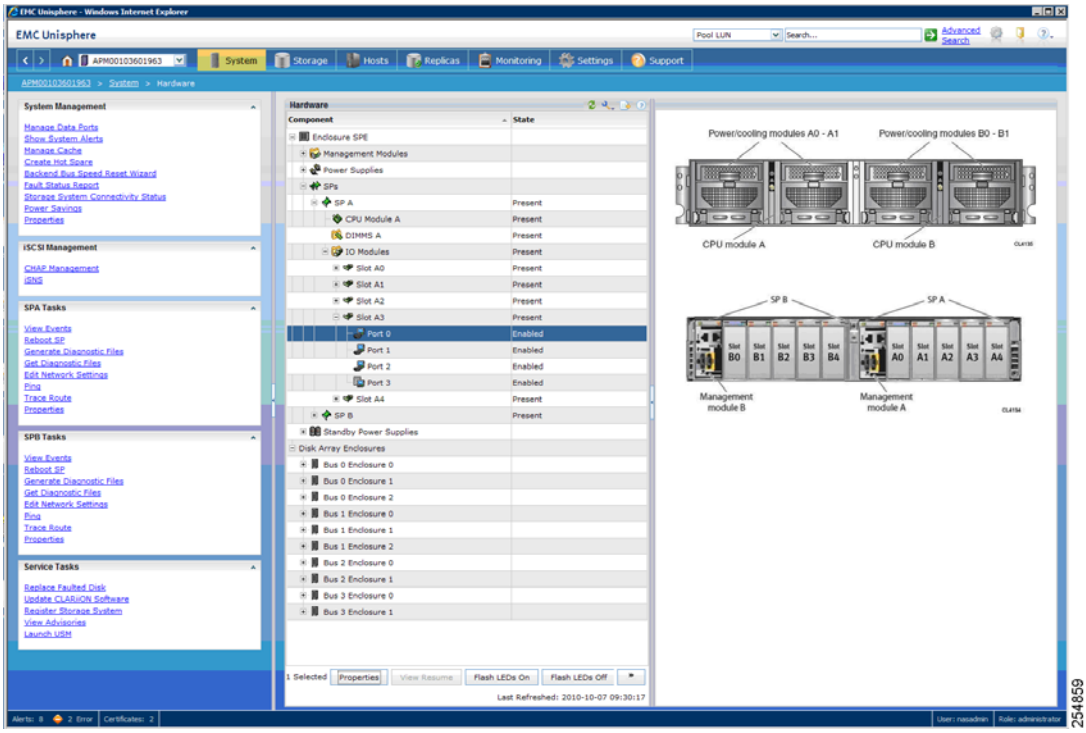
IGEL UMS の使用に関するガイドライン

- デスクトップ仮想化エンドポイントは、Lights Out 管理機能とスケジュールされたイベントを使用してリモートでシャットダウン、復帰、または起動させることができます。IT 管理者はシャドウイング機能を使用して、コンソールからエンドポイントにリモート アクセスし、診断を実行できます。エンドポイントは、DNS（標準ドメイン名）を使用して IGEL UMS サーバの場所を特定します。IGEL UMS にはレポート機能が備わっており、管理者はこの機能を使用して問題の検出に役立つ複雑なレポートを作成したり、設定変更を追跡したりすることができます。
- IGEL UMS サーバには、ローカル サーバまたは外部サーバにインストールできるデータベースが必要です。サポートされているデータベースの一覧については、IGEL のドキュメントを参照してください。サーバ、コンソール、およびデスクトップ仮想化エンドポイント間のすべての通信は暗号化されます（HTTPS および SSL を使用）。
- IGEL UMS では、イメージの配布に HTTP および FTP が使用されます。WAN 全体にデスクトップ仮想化エンドポイント イメージを配布するときは、ブランチ オフィスにある FTP サーバを使用するか、Buddy Update 機能を使用します。この機能は、更新済みの IGEL デスクトップ仮想化エンドポイントをネットワーク上にある他のローカル エンドポイント用のイメージ ソースに変換します。IGEL デスクトップ仮想化エンドポイントにはフェイルセーフ更新メカニズムが備わっており、再イメージング中に電力損失が発生した場合に、エンドポイントでは以前の設定を起動することができます。
- IGEL UMS は、複数のシステム管理者によるシステムのプロビジョニングと監視を可能にします。管理者ごとに、異なる制御範囲と権限レベルを持つことができます。このアプローチにより、組織全体にわたってサポートの責任を委ねることができます。
- 複数のエンドポイントを選択し、変更するには、IGEL UMS コンソールでグループ化とプロファイルを使用します。プロファイルをエンドポイントのグループに適用することにより、管理者は設定を効率的に変更できます。IGEL UMS サーバに登録するときに、デスクトップ仮想化エンドポイントを自動的にグループに割り当て、（MAC アドレスに基づいて）プロファイルに割り当てることができます。

EMC Unisphere 管理スイート

EMC Unisphere（図 70）管理スイートは、EMC Unified Storage デバイスのプロビジョニングと監視に使用します。Web ベースのインターフェイスが搭載され、管理者はこれを使用してストレージ システムの検出、監視、および設定を行うことができます。また、ストレージ遅延測定結果の収集や、傾向分析、レポート、およびシステム キャパシティ管理の実行にも使用できます。イベントの自動通知がサポートされるので、管理者は重要なステータス変更を予防的に管理できます。

図 70　　EMC Unisphere 管理コンソール



EMC Unisphere は仮想化に対応しています。ハイパーバイザ サーバがどのように設定されているかを視覚的に表し、どの仮想マシンが特定のストレージ リソースを使用しているかを識別します。物理ストレージとサーバのほか、VMware ESX ホストとそこに存在する仮想マシンの仮想と物理のマッピングを可能にします。管理者は、このコンソールを使用して、適切な量のストレージが仮想マシンに割り当てられていることを確認できます。

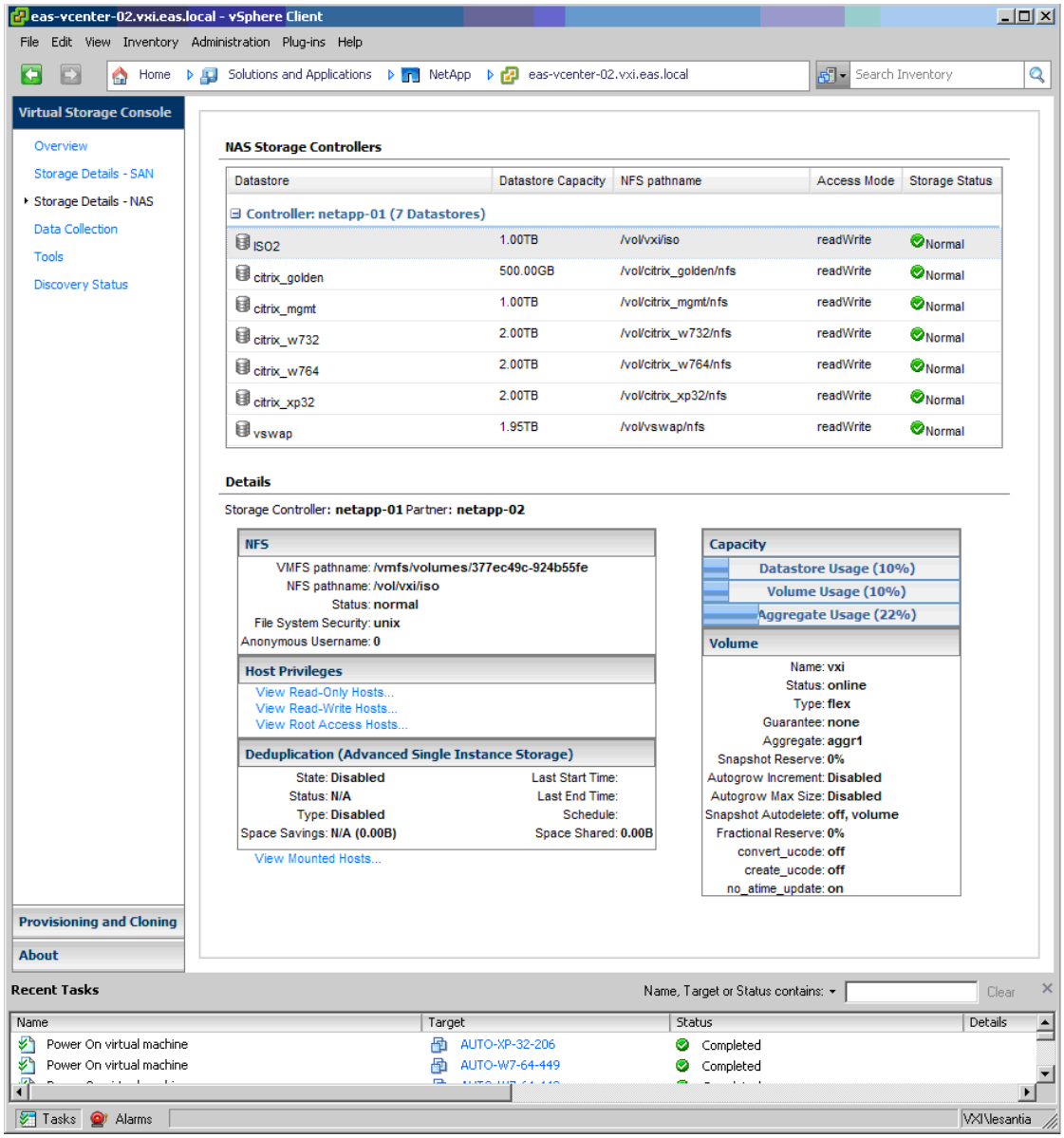
VMware 管理者は、EMC Virtual Storage Integrator（VSI）を使用して、別個のストレージ管理インターフェイスにアクセスすることなく、vSphere クライアントから一般に使用されるストレージ機能を管理できます。VSI は、EMC Unified ストレージを視覚的に表す VMware vCenter プラグインです。VSI は、vSphere データストアを EMC ストレージ上の LUN および NFS シェアにマッピングするジョブを簡素化し、アレイ上の仮想マシンと Raw デバイス マッピング ファイルのロケーションを特定するのに役立ちます。

ストレージ デバイス（NAS または SAN）は、多数のエンド ユーザ デスクトップの仮想マシン設定およびファイルを維持するので、Cisco VXI システムにおける重要なリソースとなります。ストレージ デバイス自体に組み込まれた冗長および耐障害性を使用するほか、物理的に離れた別の場所にストレージをバックアップして、障害発生時にサービスを復元できるようにしてください。

NetApp Virtual Storage Console および StorageLink

NetApp Virtual Storage Console（VSC、図 71）は、NAS デバイス NetApp FAS 3170 のプロビジョニングと監視に推奨されます。NetApp VSC は、VMware vCenter にインストールできるプラグインです。NetApp VSC のプロビジョニングおよびクローニング機能を使用して、NetApp によるスペース効率の高いクローンを展開できます。管理者は、NetApp ストレージ コンソールにログインせずに、何千もの新規仮想マシンをプロビジョニングまたは再プロビジョニングできます。VSC を使用することで、パッチやソフトウェアのアップデート、シン プロビジョニング、および重複排除管理機能の実行後に NetApp FlexClone テクノロジーを利用し、仮想マシンを再展開できます。Citrix XenServer を実行するシステムでは、NetApp StorageLink を使用して NetApp ストレージ デバイスをプロビジョニングします。NetApp StorageLink はストレージ遅延測定結果の収集にも使用できます。仮想化環境における NAS デバイスの管理に関するガイドラインとベスト プラクティスについては、NetApp のドキュメントを参照してください。

図 71　　NetApp Virtual Storage Console

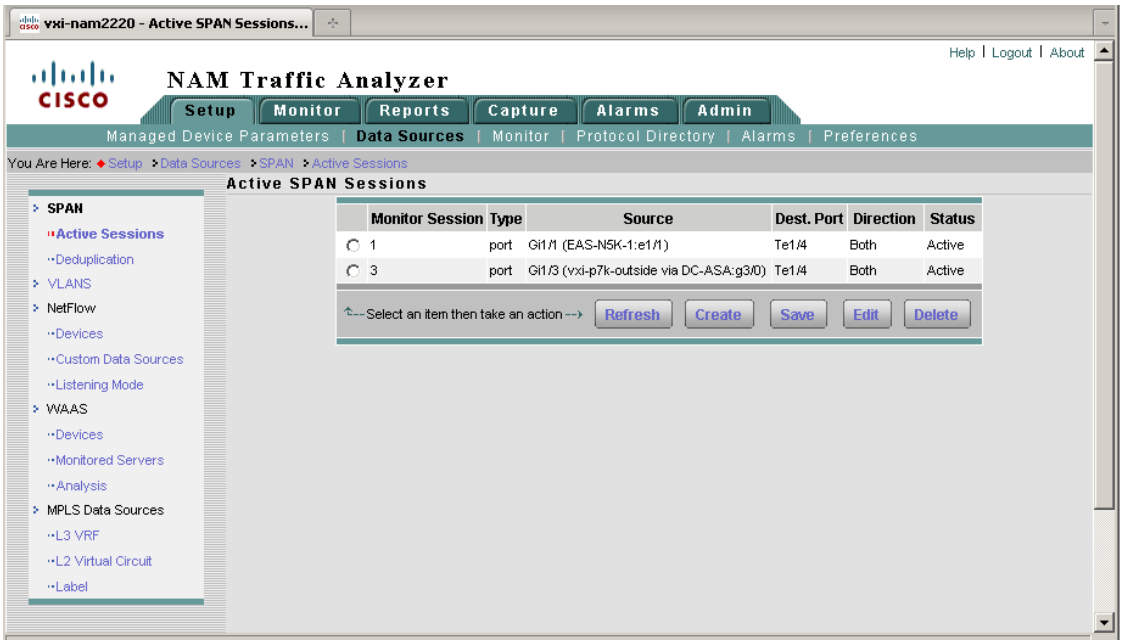


Cisco NAM

Cisco NAM Traffic Analyzer ソフトウェア（図 72）の使用により、管理者は、アプリケーションとサービスがエンド ユーザに提供される方法を監視、管理、および改善することができます。Cisco NAM は、Differentiated Services Code Point（DSCP; 差別化サービス コード ポイント）を使用したアプリケーション、ホスト、会話、およびストリームのフローベースのトラフィック分析、アプリケーション、サーバ、およびネットワーク遅延のパフォーマンスベースの測定、Voice over IP（VoIP）やビデオなどのネットワークベース サービスに対する QoE メトリック、ならびに洞察力に富むパケット キャプチャを使用した問題分析を実行します。Cisco NAM では、トラフィックの監視、パケット トレースの収集、および履歴レポートの生成が可能です。また、総合的なトラフィック分析と洞察をもたらすリアル タイムのトラブルシューティング情報が提供されるので、これらの情報を使用してネットワークとアプリケーションの効率性を高めることができます。Cisco NAM を使用して、QoS プランニングの仮定を検証することでサービス レベルの一致を確認したり、トランザクションベースの統計情報でユーザ エクスペリエンスを評価したりすることもできます。Cisco NAM を使用して Cisco VXI システムの監視やトラブルシューティングを行うときは、ここに記載されているガイドラインと推奨事項を考慮してください。

Cisco NAM には、組み込みの Web ベース トラフィック アナライザ GUI が含まれており、これを利用して設定メニューにアクセスしたり、ブラウザを介した Web、音声、およびビデオ トラフィックの使用率に関する読みやすいパフォーマンス レポートを生成したりすることができます。Cisco NAM アプライアンスの別個の管理インターフェイスを GUI へのアクセス専用にする必要があります。

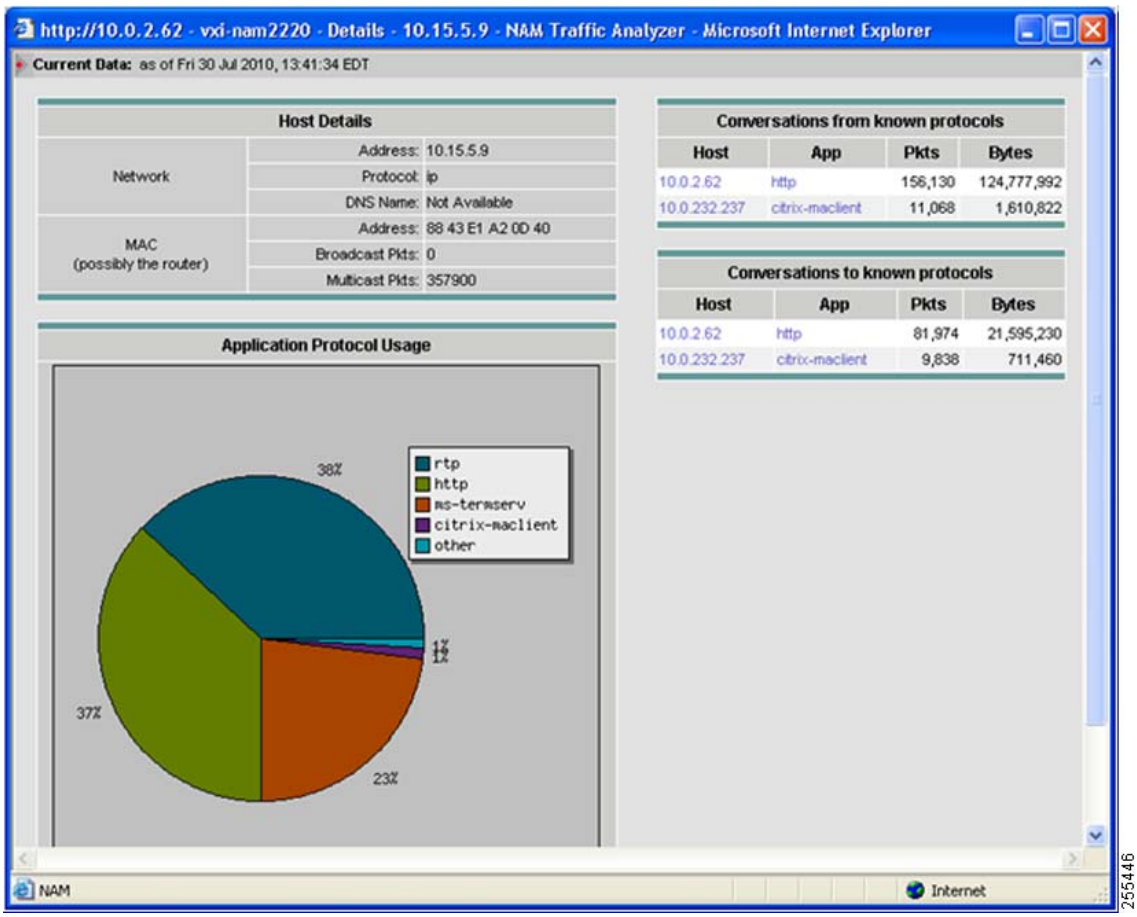
図 72　　NAM 管理 GUI



Cisco NAM はいくつかのフォーム ファクタで提供され、ネットワークのさまざまなロケーションに展開することができます。Cisco NAM プローブは、実行中の特定のタスクに適したロケーションに配置する必要があります。論理ネットワーク境界の入力ポイントまたは出力ポイントであるロケーション（アグリゲーション層、コア、またはキャンパス エッジ）では、そのパーティション内のネットワーク アクティビティに関する貴重な情報が提供されるので、Cisco NAM の展開には通常、これらのロケーションが適しています。たとえば、接続マネージャなどの重要なサーバ ファームに接続するセッションを監視するには、データセンター コアに Cisco NAM を配置します。このロケーションでは、企業ネットワークのあらゆる部分に存在するエンド ユーザが開始するセッションを監視できます。また、Cisco NAM をブランチ オフィスに配置して、WAN で接続している特定のユーザのトラブルシューティングを行うこともできます。WAN エッジは、複数のブランチ オフィスから発信されるセッションを監視するのに最適なロケーションです。ブランチ オフィスで Cisco ISR ブランチ オフィス ルータのネットワーク モジュールとして、またはコア ネットワークで Cisco Catalyst 6000 Series コア スイッチや別個のアプライアンス（Cisco NAM 2204 または 2220 アプライアンス）上のブレードとして Cisco NAM を導入できます。また、Cisco Nexus 1000V や Cisco WAAS デバイス上のソフトウェア モジュールとして Cisco NAM を導入することも可能です。データセンター コアでは、専用のハードウェアを使用して必要なレベルのパフォーマンスを提供する、別個の Cisco NAM アプライアンスを展開する必要があります。Cisco NAM の展開に関する総合的な考慮事項については、Cisco NAM 展開ガイドを参照してください。

ネットワーク トラフィック使用率レポートには、リモート ルータから Cisco NAM への NetFlow Data Export（NDE; NetFlow データ エクスポート）を使用します。NetFlow データは、Cisco WAAS アプライアンス（WAN 上のトラフィックを監視するため）、ルータ、スイッチ、または Cisco ASA アプライアンスからエクスポートできます。たとえば、Cisco WAAS からの NetQoS フロー データは、アプリケーション遅延の情報を示します。トラフィック使用率レポートは、QoS ポリシーおよび Cisco WAAS 最適化が有効となるトラフィック タイプを識別するのに役立ちます。これらの測定結果は、拡大予測やプランニングに使用することもできます（図 73）。

図 73　シスコ ネットワーク アナライザ モジュールのトラフィック使用率レポート



パケット キャプチャには、Cisco Catalyst 6000 シリーズまたは Cisco Nexus 7000 シリーズ スイッチなど、複数の送信元ポートを監視できるコア スイッチ上の Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）セッションを使用します。データセンター サーバを行き来するすべてのトラフィックを監視するには、データセンター コア スイッチ（Cisco Nexus 7000 シリーズ）の SPAN ポート（10 ギガビット イーサネット推奨）を使用します。スイッチに 2 つの SPAN セッション数制限があることに注意してください。

Cisco NAM の主な用途は、適切に設定できなかったユーザ セッションや、低品質のユーザ セッションのトラブルシューティングと分析です。特定の会話を表示するには、エンドポイント、デスクトップ コントローラ、または仮想デスクトップ ネットワーク アドレスに基づいてパケット キャプチャをフィルタリングします。また、VLAN、プロトコル（ポート）、ストリーム内の DSCP マーキングに基づいたフィルタリングも可能です。

プロトコル フォーマットが独自のものであり、暗号化される可能性があるので、Cisco NAM は現在、デスクトップ仮想化プロトコル パケットのコンテンツのデコードに対応していないことに注意してください。Cisco NAM は、使用されるポート番号に基づいてストリームを識別し、ラベル付けすることができます（図 74）。

図 74　　NAM パケット デコーダ

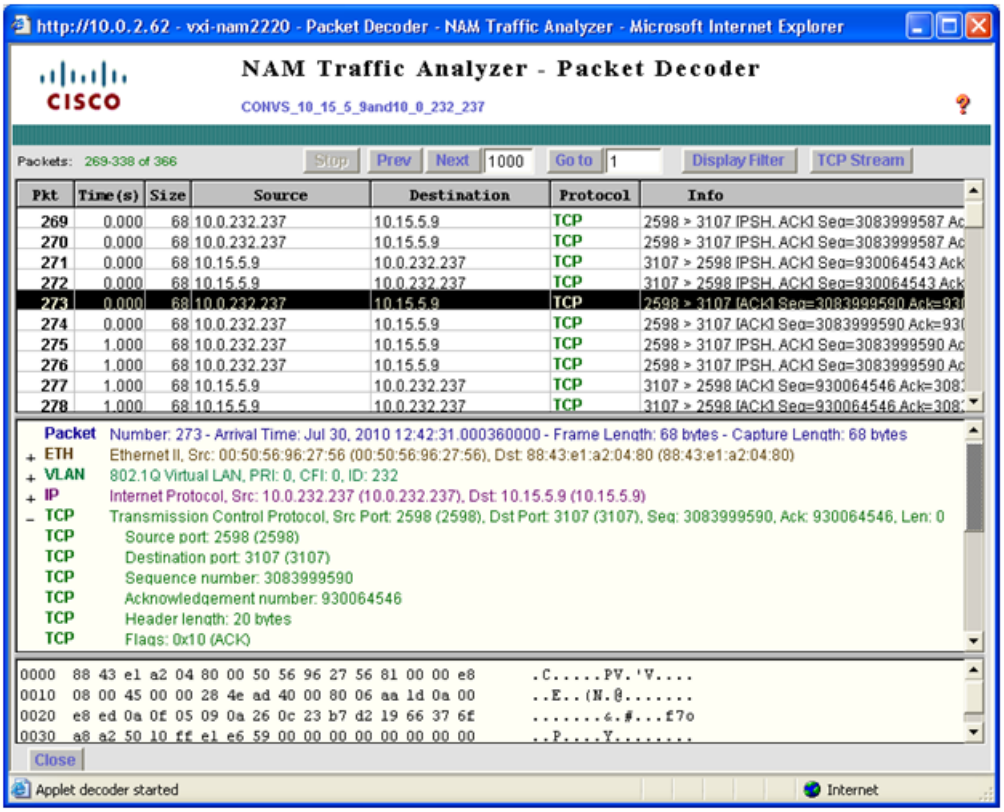


表 26 に、デスクトップ仮想化セッションで使用されるプロトコルとポートを示します。この情報を使用して、パケット キャプチャ内のユーザ ストリームを識別できます。

表 26　　プロトコル/ポート情報

DV プロトコル	プロトコル	ポート
RDP	TCP	3389/32111（USB）/9427（MMR）
ICA	TCP	1494/2598/8080

VMware vCenter サーバの VMware vSphere クライアントおよび Software Development Kit（SDK; ソフトウェア開発キット）インターフェイスでは、HTTP（80）および HTTPS（443）を使用します。VMware ESXi ホストへの VMware vCenter 通信には、TCP（ポート 902）ストリームを使用します。Citrix Desktop Delivery Controller と Citrix XenDesktop Agent 間の通信には TCP（ポート 8080）を使用します。VXC Manager は、デスクトップ仮想化エンドポイント エージェントとの通信用に HTTP（80）および HTTPS（443）をデフォルト設定します。管理者は、すべてのファイアウォール デバイスでこれらのポートが開いていることを確認する必要があります。

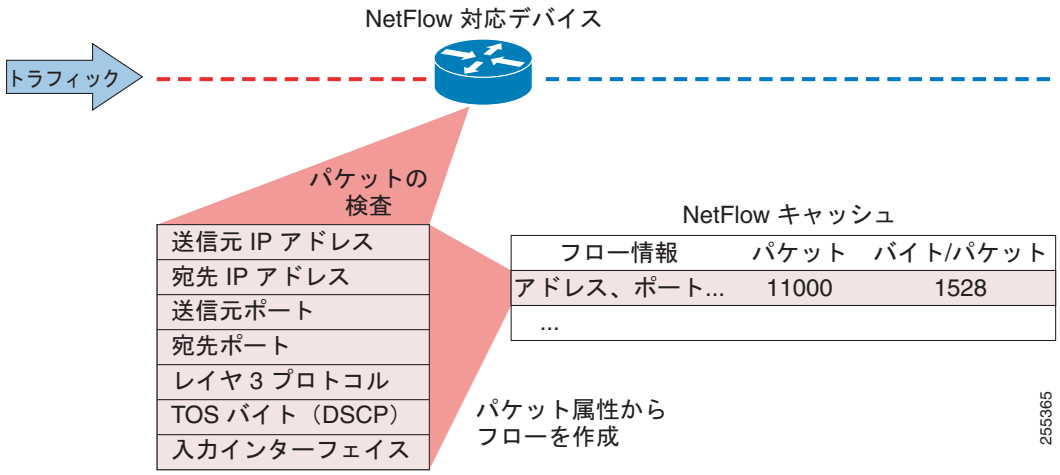
Cisco Unified Personal Communicator クライアントはデスク フォン制御モードで動作しているので、Cisco Unified Personal Communicator でアクティブなボイス コールを実行する仮想デスクトップからのトラフィックのパケット キャプチャには、Real-Time Transfer Protocol（RTP）トラフィックは含まれません。UC シグナリング トラフィックでは、SCCP TCP 2000 ポートおよび SIP TCP/UDP 5060 ポートが使用されます。

デスクトップ パケット キャプチャには、Computer Telephony Integration（CTI; コンピュータ テレフォニー インテグレーション）プロトコルを介した Cisco Unified Personal Communicator クライアントと Cisco Unified Presence および Cisco Unified Communications Manager との通信が含まれます。デスクトップ仮想化エンドポイントと同じ場所にある Cisco IP Phone のパケット キャプチャには、RTP トラフィックが含まれます。Cisco NAM は、Cisco Unified Management Suite から音声品質測定に使用される RTP メトリックも収集できます。

Cisco NetFlow

Cisco NetFlow は、ネットワーク要素（ルータおよびスイッチ）を通過するパケットの統計情報を提供し、Cisco VXI システムでのトラフィック使用率の監視に使用できます。NetFlow データは、アプリケーションやユーザのモニタリング、ネットワーク帯域幅の分析とキャパシティ プランニング、セキュリティ分析、アカウンティングと課金、トラフィック エンジニアリング、および NetFlow のデータ ウェアハウスとデータ マニングに使用できます。NetFlow をサポートするルーティングおよびスイッチング プラットフォームには、Cisco ISR および 7200、10000、12000、CRS-1 シリーズ ルータ、Catalyst4k、Cat6500、ならびに Nexus スイッチがあります。

図 75　　Cisco NetFlow による NetFlow Cache でのフロー作成



NetFlow は、IP アドレス、プロトコル、アプリケーション ポート、および DSCP や、Type of Service（ToS; タイプ オブ サービス）情報、パケット サイズ、およびカウントなどのさまざまなパケット特性を含むデータを、ネットワーク要素上の入力パケットおよび出力パケットからキャプチャします。NetFlow の主なコンポーネントは、IP フロー情報を保存する NetFlow キャッシュと、NetFlow データを Cisco NetFlow Collector などのネットワーク管理コレクタに送信する NetFlow エクスポートです。NetFlow コレクタは、エクスポートされた NetFlow レコードを集約し、ネットワーク内の IP トラフィック フローに関するモニタリングおよびレポート情報を提供します。NetFlow は、すべてのパケットを計上し（サンプル モード以外）、エンド ユーザに対して透過的に動作します。NetFlow 対応スイッチングのスケーラビリティとパフォーマンスにおいては、NetFlow キャッシュに存在するフロー単位のアカウンティング測定を動的に更新することのできる効率的なフロー キャッシュ管理と、キャッシュ エージング / フロー期限の決定が重要なポイントになります。期限の切れたフローは、NetFlow コレクタへのエクスポート用としてデータグラムにまとめられます。

NetFlow キャッシュ エントリの期限切れに関しては、次のルールがあります。

- 指定した時間の間、アイドル状態であったフローは期限切れとなり、キャッシュから削除されます。
- 長時間存続したフローは期限切れとなり、キャッシュから削除されます（デフォルトで許可されるフローの存続時間は最大 30 分です）。

- キャッシュが満杯になると、いくつかのヒューリスティックが適用され、フロー グループの同時エージングが積極的に実行されます。
- バイト ストリームの最後に到達した（FIN）、またはリセットされた（RST）TCP 接続は期限切れとなります。

ネットワーク ノードからコレクタに NetFlow レコードを伝送するための柔軟で拡張可能な手段となる、最新の NetFlow エクスポート フォーマット Version 9 を使用することが推奨されます。NetFlow Version 9 には、定義可能なレコード タイプがあり、自己記述型なので NetFlow Collection Engine の設定が容易になります。

図 76　　NetFlow Cache の例

1. フロー キャッシュ：最初の独自のパケットによりフローが作成されます。

Srcif	SrciPadd	Dstif	DstiPadd	プロトコル	TOS	Figs	パケット	送信元ポート	送信元マスク	送信元AS	宛先ポート	宛先マスク	宛先AS	ネクストホップ	バイト/パケット	アクティブ	アイドル
Fa 1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	162	/24	5	63	4	15	10.0.23.2	1528	1745	4
Fa 1/0	173.1002.3.2	Fa0/0	10.0.227.12	6	40	0	2491	15	/26	196	15	/24	15	10.0.23.2	740	41.5	1
Fa 1/0	173.1002.20.2	Fa0/0	10.0.227.12	11	80	10	10000	161	/24	180	10	/24	15	10.0.23.2	1428	1145.5	3
Fa 1/0	173.1002.6.2	Fa0/0	10.0.227.12	6	40	0	2210	19	/30	180	19	/24	15	10.0.23.2	1040	24.5	14

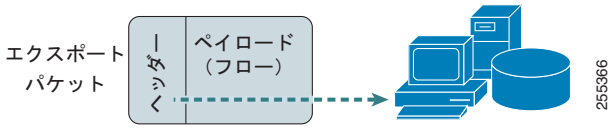
2. フロー エージング タイマー

- 非アクティブのフロー（デフォルトは 15 秒）
- 長期間のフロー（デフォルトは 30 分（1800 秒））
- RST または IN TCP フラグによるフローの終了

Srcif	SrciPadd	Dstif	DstiPadd	プロトコル	TOS	Figs	パケット	送信元ポート	送信元マスク	送信元AS	宛先ポート	宛先マスク	宛先AS	ネクストホップ	バイト/パケット	アクティブ	アイドル
Fa 1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A2	/24	15	10.0.23.2	1528	1800	4

3. エクスポート パケットでパッケージされたフロー
非集約のフロー：エクスポート バージョン 5 または 9

4. レポート サーバへの転送フロー



Cisco NetFlow の使用に関するガイドライン：

- Cisco NetFlow は、大規模な Cisco VXI の展開に対する監視、トラブルシューティング、およびキャパシティ プランニングに使用できます。複数の Cisco VXI トラフィック フローに関する NetFlow データを収集できます。このデータは集約が可能で、使用状況に関するレポートを生成できます。レポートを使用して、トラフィック タイプごとのピーク レート、平均レート、毎日 / 毎週のピーク ボリューム、毎日 / 毎週の平均ボリュームを確認できます。データは、他のネットワーク インターフェイス（WAN リンクなど）やネットワーク要素（ルータおよびスイッチ）をネットワークに追加するときのネットワーク キャパシティ プランニングに使用できます。その他の有益なタスクには、上位の Cisco VXI ユーザの識別、特定のトラフィックしきい値に達したときのアラートの設定、および Cisco VXI セッションを介してアクセスされるサービス（ 仮想デスクトップ トラフィックの監視など）に関するトラフィック分散レポートの取得があります。

- NetFlow を有効にするため、ネットワーク内のさまざまなポイントを理解し、識別するには、導入モデルの章で説明している Cisco VXI トラフィック パターンを参照してください。NetFlow は、ブランチにあるルータ（ISR など）で有効にしてデスクトップ プロトコルおよびセッション トラフィックを視覚的に表示したり、WAN エッジにある集約ルータ（ASR、7200、または WAAS など）で有効にして デスクトップ プロトコルおよびセッション トラフィックを監視したり、データセンターにあるエンタープライズ コア スイッチ（ Nexus 7000 または Catalyst 6500 など）で有効にしてデスクトップ プロトコルおよびセッション トラフィックを監視したり、仮想スイッチ（ Nexus 1000v など）で有効にしてデスクトップ プロトコルおよび仮想デスクトップ トラフィックを監視したりすることができます。すべてのネットワーク要素で NetFlow を有効にしてデータを集約すると、情報の過負荷が発生し、分析可能できる有益なデータが提供されない場合があります。代わりの戦略として、ネットワーク内の特定のポイントにあるネットワーク要素を（監視されるセッションのトラフィック パターン/パスに基づき）選択的に有効にして、分散された、または集中化されたコレクタの集合を使用してデータを収集します。
- Cisco VXI セッション トラフィックを識別するための簡単な戦略として、NetFlow レコードに含まれる IP アドレス（シン クライアントまたは仮想デスクトップ、デスクトップ コントローラ）、プロトコル タイプ（TCP/UDP）、ポート（ICA/PCoIP/RDP/HTTP/HTTPS）、および TOS 情報を使用します。対象となる特定のトラフィック フローには、エンドポイントとデスクトップ コントローラ間の Cisco VXI セッション トラフィック、エンドポイントと仮想デスクトップ間のデスクトップ プロトコル トラフィック、仮想デスクトップとデスクトップ コントローラ間のトラフィック、仮想デスクトップからサーバおよびインターネットへのトラフィック、および CTI や RTP トラフィックを含む Cisco Unified Personal Communicator 関連のトラフィック パターンが含まれます。

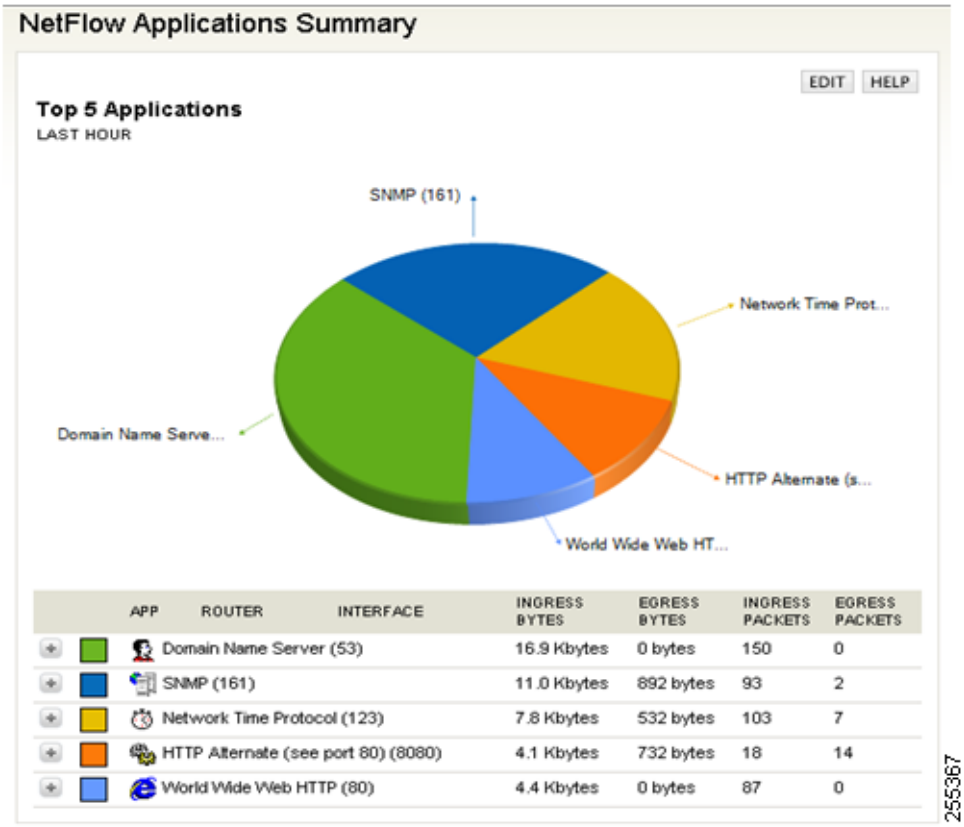
NetFlow の一般的な使用例：

- Cisco VXI セッション トラフィック フローの監視：ユーザ セッションを識別し、使用される帯域幅を測定します。
- ネットワーク トラフィックに基づいたアプリケーションの使用状況に関する仮想デスクトップ トラフィック フローの監視：仮想デスクトップを識別し、プロトコルやポートに基づいて使用される各種アプリケーションを監視します。
- Cisco VXI トラフィック フローのトラブルシューティング：低品質の問題を抱えるユーザ セッションを識別し、ネットワーク問題の原因を突き止めます。
- オーバーサブスクリプションのリンクの識別、WAN リンクで使用できる帯域幅を独占している単一ユーザの識別、および緩慢なネットワーク パフォーマンスの検出
- 各 Class of Service（CoS; サービス クラス）に適切な帯域幅が割り当てられており、オーバーサブスクリプションまたはアンダーサブスクリプションの CoS が存在しないことの確認

Cisco VXI ネットワーク ワークフローで NetFlow を有効にするための手順：

1. ネットワーク要素（ルータおよびスイッチ）に NetFlow を設定します。
   a. NetFlow コレクタの IP アドレスと NetFlow エクスポート バージョンを設定します。
   b. デバイスおよびインターフェイスで NetFlow を有効にします。
2. NetFlow コレクタを管理ステーションとしてインストールします。
   a. NetFlow コレクタに NetFlow を有効にしたルータとスイッチの IP アドレスおよび SNMP 属性をプロビジョニングします。
3. NetFlow コレクタを起動して、NetFlow データ収集を開始します。
4. 収集されたデータに対して NetFlow Analyzer レポートを実行します。

図 77　　Orion ネットワーク パフォーマンス モニタ上の NetFlow Analyzer レポート



Cisco NetFlow Collector（NFC）は、拡張性の高いデータ収集およびアグリゲーション製品であり、データ、分析、およびレポートを一元的に表示します。NFC の使用により、企業はアプリケーション配布およびネットワーク キャパシティ プランニング用にネットワーク インフラストラクチャを最適化できます。また、Cisco NAM は NetFlow コレクタおよびアナライザとして使用することができ、基本的な機能をサポートします。また、ManageEngines、Solar Winds、または NetQOS からの NetFlow アナライザは、高度なレポートおよび分析機能と大規模なデータベースをサポートします。

図 78　　NAM の NetFlow Analyzer レポート

（注）　NetFlow レコードは、ベスト エフォート方式により、ユーザ設定可能なポート上で UDP を使用してエクスポートされ、使用可能なネットワーク帯域幅を使用します。特定のルータおよびスイッチで NetFlow レコードを確実にエクスポートするには、SCTP を使用します。詳細については、Cisco ルータのドキュメントを参照してください。

（注）　NetFlow が有効になっているネットワーク要素では、CPU にごくわずかな影響があります。ルータ、コレクタ、およびネットワークに対する CPU、メモリ、およびストレージの影響を軽減するには、エージング タイマーの調整、サンプル NetFlow の使用、および Flow マスクの使用などの方法があります。その他の方法には、アグリゲーション方式、フィルタ、データ圧縮、および大きめの収集バケット サイズの使用などがあります。ネットワーク帯域幅の使用量を減らす 1 つの方法として、同じ LAN セグメント上にコレクタとルータを配置します。これらの方法の使用に関する詳細については、Cisco NetFlow のドキュメントを参照してください。

Cisco IOS ルータおよび Cisco Catalyst シリーズ スイッチでの Netflow の設定例については、次の URL にある『Cisco Virtualization Experience Infrastructure Configuration Guide』を参照してください。

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VXI/configuration/VXI_Config_Guide.pdf

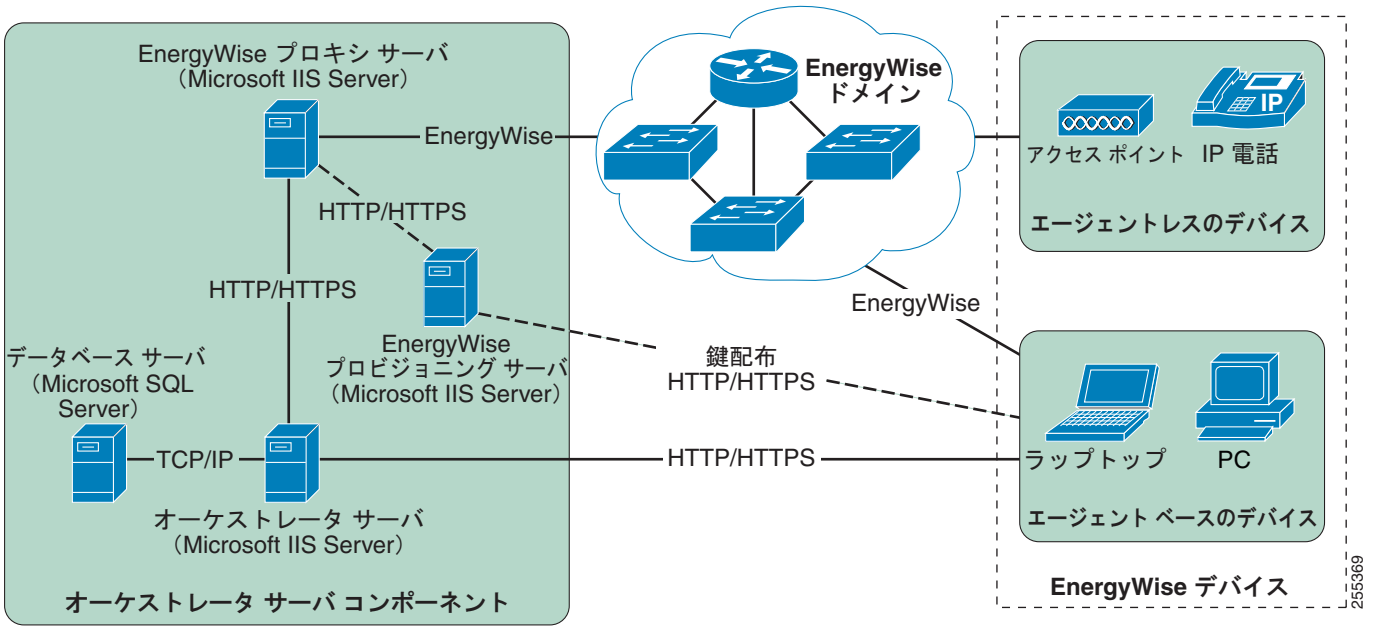
Cisco EnergyWise Orchestrator

Cisco EnergyWise Orchestrator は、Cisco VXI システムのエネルギー消費を測定、報告、および制御するための中央集中型インターフェイスを提供します。EnergyWise Orchestrator はシスコの EnergyWise テクノロジーと統合されて、DV エンドポイント、デスクトップ PC、ラップトップ、IP 電話、ルータ、スイッチ、アクセス ポイント、および EnergyWise テクノロジーをサポートするあらゆるデバイスを含む、広範囲な IT デバイスでの消費電力を管理します。省エネルギーを強化する高度なエネルギー管理ポリシーがサポートされます。省エネルギーのポリシー最適化、トラブルシューティング、およびデモンストレーションについて、有力なレポートを生成できます。エネルギー管理アーキテクチャの主要なコンポーネントとしての Enerywise Orchestrator の重要性は、エネルギー使用量とコストの削減、測定可能な Return On Investment（ROI; 投資収益率）の提供、政府規制への準拠、温室効果ガス排出量の削減、および持続可能性の全体的な向上を可能にする機能にあります。

Cisco EnergyWise Orchestrator は、エンタープライズレベルのスケーラビリティ、セキュリティ、および信頼性を実現します。また、低電力モードへの切り替え前に、デスクトップ上で動作するビジネスアプリケーションを適切に管理できます。EnergyWise Orchestrator によって、マシンにリモート（WoWAN および WoLAN）でアクセスしようとするユーザは PC アクセスが容易になります。ローカルまたはワイドエリア ネットワーク上での信頼性の高いオンデマンド ウェイクアップにより、デスクトップ パッチ管理が強化されます。

EnergyWise Orchestrator 導入には、コンポーネントとして Cisco EnergyWise Orchestrator（サーバ、プロビジョニング サーバ、プロキシ サーバ、データベース）、ルータおよびスイッチに搭載された Cisco EnergyWise テクノロジー、Cisco EnergyWise Orchestrator PC クライアント、および Cisco EnergyWise Orchestrator Sustainability Dashboard が含まれます。

図 79　　Cisco EnergyWise Orchestrator のアーキテクチャ



EnergyWise Orchestrator は、EnergyWise プロトコルを使用してすべての EnergyWise ネットワーク要素と通信し、EnergyWise API を介して PC に対する包括的な電源管理を行います。EnergyWise プロキシは、Orchestrator Server と Cisco EnergyWise プロトコル準拠デバイス間のブリッジとして機能します。EnergyWise PC エージェントは、デスクトップ PC およびラップトップ上の EnergyWise を有効にします。このエージェントは、エンド ユーザに対して透過的に動作し、Orchestrator サーバから受信する電力ポリシーを適用します。利用状況の情報は PC にローカルに保存され、定期的にサーバにリレーされます。

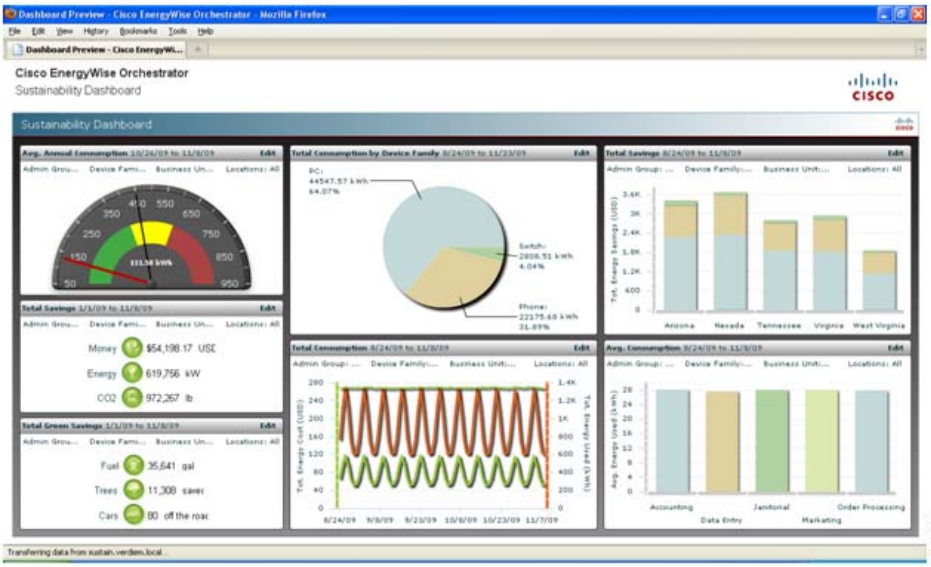
Orchestrator には、Orchestrator Administration Console（IT 管理者が使用）、Sustainability Dashboard（幹部、従業員、顧客などが使用）、およびリモート アクセス用の Wake（PC をリモートで復帰させる必要のある IT スタッフや従業員が使用）などの複数の管理インターフェイスが搭載されています。Administration Console には、デバイスの電力状態の一元的な管理、リアルタイム モニタリング、ポリシーベースの管理、インテリジェントなポリシー オーサリングに関する実際の PC 使用量のモニタリングを可能にする使いやすい Web ベースの GUI が搭載されています。役割ベースのセキュリティ権限や分析およびトラブルシューティングに関するイベント レポートを使用したグループ指向の管理がサポートされます。このコンソールを使用して、リアルタイムでデバイスの電力状態を変更または表示したり、デバイス ポリシーまたはグループ メンバーシップを手動で変更したり、デバイスまたは PC の EnergyWise 属性を編集したりすることができます。

図 80　Cisco EnergyWise Orchestrator Administration Console

企業の電力ポリシーには、デバイスがオンになるとき、または低電力モードになるときが規定されています。PC については、使用されていない場合の IDLE タイムアウトと、エンドユーザやビジネス アプリケーションに対する例外処理もポリシーで定義されます。Orchestrator は、時間ベースのグラフィカルなポリシー スケジュールを表示します。PC が低電力モードに移行した場合、管理者はユーザに対して、電力状態の変更をスキップするか、電力状態の変更を一定時間遅らせることを任意で許可することができ、状態の変更の前に PC ユーザに表示されるメッセージを指定できます。リモート ユーザが PC にログインしている場合に、ポリシーによってスリープとシャットダウンを無効にすることもできます。また、PC がスリープ状態になるかシャットダウンした場合のアプリケーションの動作もポリシーで規定します。この場合、アプリケーションを正常に終了させるか、代わりに状態の変更を中断させることができます。

EnergyWise Orchestrator Sustainability Dashboard は、Orchestrator Database を使用して省エネルギーを表示するためのカスタマイズ可能な管理レベル レポートを提供します。また、電源管理ポリシーによる節約の計算や環境に対する影響予測など、ビジネス上のメトリックに焦点を当てたインタラクティブ レポートを提供します。PC、スイッチ、IP Phone、無線アクセス ポイントを含むすべてのデバイス タイプに関する総合チャートが用意されます。Operational State レポートには、すべてのデバイスに関する電力状態の変更の傾向が示されます。システム イベント レポートには電力状態の変更、エラー、エンドユーザ インタラクションが含まれており、トラブルシューティングに役立ちます。

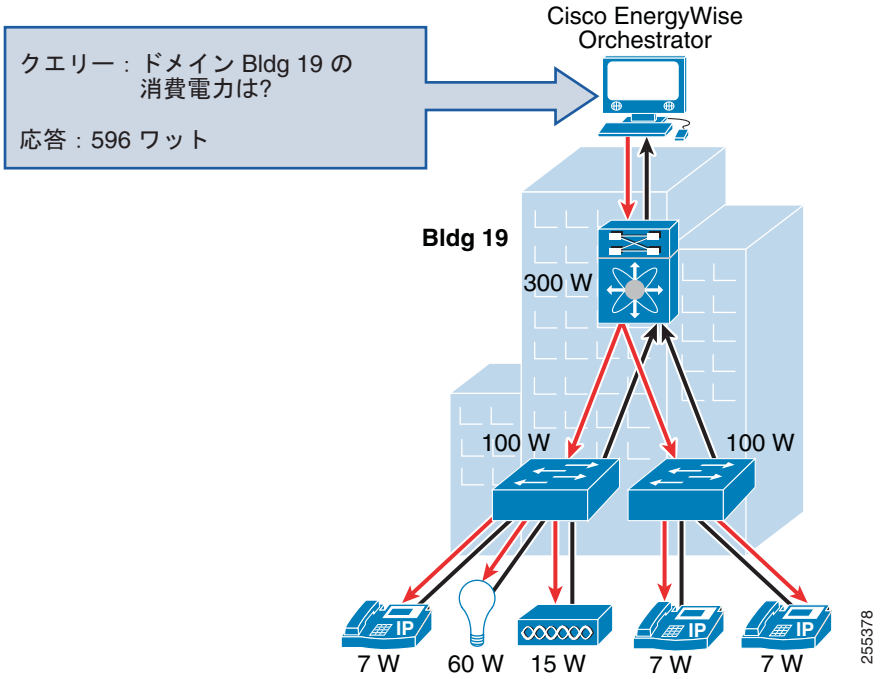
図 81　Cisco EnergyWise Orchestator Sustainability Dashboard



Cisco EnergyWise は、シスコ デバイスや接続しているすべてのエンドポイントを含む電源デバイスの消費電力を管理するための、インテリジェントなネットワークベースのアプローチに基づいたエネルギー管理アーキテクチャです。EnergyWise ドメインは、電源管理の 1 つの論理ユニットとして処理され、管理ステーション、ドメイン メンバー、およびエンドポイントで構成されます。エンドポイントは、IP Phone、アクセス ポイント、DV エンドポイント、または PC など、ネットワークに接続しているデバイスです。エンドポイントは、PoE スイッチのようなドメイン メンバーから電力供給を受けます。EnergyWise は、Catalyst 2960、3560、3750、4500、6500 シリーズ スイッチ、および Cisco ISR G2 ルータと Enhanced EtherSwitch サービス モジュールでサポートされます。

たとえば、コア ルータ、10 台のアクセス スイッチ、および電話機、アクセス ポイント、EnergyWise SDK を実行する PC などの 400 台のエンドポイントを備えた建物で、ルータとスイッチをドメイン メンバーとした MyBuilding という EnergyWise ドメインを作成できます。このドメイン メンバーは、CDP または EnergyWise UDP メッセージを使用してネイバー関係を形成し、他のメンバーやエンドポイントに EnergyWise メッセージ（クエリー）を転送します。EnergyWise プロトコルでは、メンバーと管理ステーション間の通信にポート 43440 を使用します。EnergyWise クエリーは、ドメイン メンバーとエンドポイントの電力状態に対する set、collect、save、summarize オペレーションをサポートします。ドメインを設定した後は、ドメイン メンバーの SNMP または EnergyWise API を使用して、EnergyWise Orchestrator のような中央集中型の管理ステーションから電力使用量を監視し、制御できます。電力使用量を自動的に管理するための時間帯別設定を使用するよう、繰り返しイベントまたは再発と呼ばれるルータ CLI を使用して、ドメイン メンバーにポリシーを手動で設定することもできます。EnergyWise エンドポイントの電力は、手動で（スイッチ CLI または EnergyWise クエリーを介して）制御することも、スイッチにプロビジョニングされた繰り返しイベントや Orchestrator で作成されたポリシーを介して自動的に制御することもできます。

図 82　　Cisco EnergyWise モニタリング



EnergyWise の属性は、ドメイン メンバーとエンドポイントに割り当てられるユーザ指定の値であり、組織におけるデバイスの使用方法に関するコンテキストを示します。デバイスは、組織内の重要度に基づいてキーワードを割り当て、評価できます。属性は、レポートを生成したり、ポリシーを適用したりするときに、特定の基準を満たすデバイス（2 階の財務部で使用するすべての PC など）を検索し、制御するために使用できます。重要度属性（1 ～ 100 の範囲）を使用して、ビジネス上の優先順位に基づいてデバイスを評価します。デスクの公共電話の重要度（10）よりも、ビジネスクリティカルな緊急電話（100）の重要度のほうが高くなります。たとえば、エンドポイントの IP Phone や、接続されたその他のデバイスに電力供給する PoE スイッチには、接続されたデバイスよりも高い重要度が割り当てられます。キーワード属性を使用して、デバイスまたはインターフェイスにロケーションとユーザ情報のタグを付けます。たとえば、IT、lobby、HumanResources、Accounting、router、phone、floor2 などです。役割属性は、特定の用途やデバイス機能に基づいてデバイスをグループ分けします。たとえば、interface、switch model number、Lobby、Teller、HelpDesk、または GuardDesk などです。属性が割り当てられた後は、ポリシーを使用して、午後 6 時以降は重要度 70 未満のデバイスをすべてオフにすることができます。特定のデバイス属性の設定に関する詳細なガイドラインについては、EnergyWise のドキュメントを参照してください。

EnergyWise は、標準の電力レベル（0 ～ 10 の範囲で 0 はオフ、1 ～ 10 はオン）を使用して、製造元の異なるデバイスの電力使用を一貫して管理します。これにより、エンドポイントでは、EnergyWise によって電力レベルがこれらの各標準レベルに設定されたときの適切なアクションを決定できます。次の図は、異なる電力レベルに関連付けられた動作モードをまとめたものです。

図 83　Cisco EnergyWise 電力レベル マトリックス

Mode	Color	Code	Color	Level	Label
Operational (1)		FF0000	Red	10	Full
				9	High
		FFFF00	Yellow	8	Reduced
				7	Medium
		00FF00	Green	6	Frugal
				5	Low
Standby (0)		0000FF	Blue	4	Ready
				3	Standby
		A52A2A	Brown	2	Sleep
				1	Hibernate
Nonoperational (-1)		000000	Black	0	Shut

255373

Cisco EnergyWise Orchestrator を使用して、Cisco VXI 展開における EnergyWise 対応のネットワーク要素やエンドポイントでの消費電力の監視、制御、および節約を行うことができます。Orchestrator Client を実行するシック PC やシン クライアントのような Cisco VXI デスクトップ仮想化エンドポイントは、Energywsie Orchestrator によって直接管理できます。PoE を使用する VXC クライアント（ゼロ クライアント）のような DV エンドポイントでの消費電力も、EnergyWise が有効なスイッチの接続ポートを管理することによって監視および制御できます。

Cisco VXI ユーザ電力ポリシーには、関連付けられた IP Phone、VXC エンドポイント、および仮想デスクトップなど、そのユーザに固有のすべての Cisco VXI コンポーネントに関する電力の管理を含めることができます。エネルギー ポリシーは、特定の時間帯に IP Phone、VXC エンドポイント、および仮想デスクトップをシャットダウンおよび電源投入するのに使用できます。たとえば、1 階の PC とゼロ クライアントは午前 6 時に自動的に電源投入され、午後 8 時に電源が切れます。Cisco VXI ユーザ消費電力レポートでは、先月および昨年の IP Phone、VXC エンドポイント、およびシック クライアントによるエネルギー使用が報告され、グラフ化されます。このレポートには電力の使用パターン（ピーク、平均、低）に関する情報と、指定のエネルギー ポリシーを使用したコスト削減の概要が示されます。Cisco VXI エンドポイントの電力レベルは、EnergyWise Orchestrator Administration Console で特定のデバイスの管理、現在の電力レベルの表示、および電力レベルの設定を行うことで、リアルタイムで動的に管理できます。

EnergyWise Orchestrator ワークフローにエンドポイントを追加するための手順：

1. ドメイン メンバー（ルータおよびスイッチ）で EnergyWise を設定します。
   a. エンドポイントに接続されたドメイン メンバーに、ドメインと管理パスワードを設定します。
   b. エンドポイントに接続されたデバイスとインターフェイスに、EnergyWise 属性を設定します。
2. PC エンドポイントに Orchestrator クライアントをインストールします。
3. Orchestrator サーバ（プロキシ サーバを含む）を管理ステーションとしてインストールします。
   a. プロキシ サーバにプライマリ ドメイン メンバーのドメイン、パスワード、および IP アドレスをプロビジョニングします。
4. Orchestrator サーバを起動して、EnergyWise デバイスと PC の検出を開始します。

EnergyWise Orchestrator の使用に関するガイドライン：

VXC2100 は、基本構成（1 KB+1 MS+1 モニタなど）で PoE 802.3 AT を使用できますが、その他のフル構成（1 KB+1 MS+2 USB+2 モニタなど）や中規模構成（1 KB+1 MS+2 モニタなど）には外部電源デバイスが必要です。VXC2200 では、基本構成（1 KB+1 MS+1 モニタ）に PoE 802.3 AF を使用できますが、その他の構成（フル / 中規模など）には PoE 802.3 AT が必要であることに注意してください。
VXC2100 は、4 つの電力モードをサポートし、低めの電力レベルではサポートされる周辺機器の数が少なくなります。アクセサリ（VXC2100 を含む）の電力ステータスは、関連付けられた電話機のディスプレイに示されます。電話機では、約 10 W のベース電力（アクセサリなし）が使用されることに注意してください。消費電力の詳細については、Cisco VXC クライアントのドキュメントを参照してください。

（注） VXC2100 に供給される電力は関連付けられた電話機を介して制御されますが、VXC 2200 に供給される電力は個別に制御できます。VXC エンドポイントに接続された PoE スイッチ ポートでインライン電力を有効にしても、DV エンドポイントの電源をオンにするには、ユーザ インタラクションが必要です。ただし、VXC エンドポイントに接続された PoE スイッチ ポートでインライン電力を無効にすると、エンドポイントはただちに電源オフになります。ドメインにスイッチを追加すると、デフォルトでそのスイッチとすべての PoE スイッチ ポートで EnergyWise が有効になります。Orchestrator に認識されない PoE デバイスは、不明デバイスとしてコンソールに表示されます。それらのデバイスも、Orchestrator を介して管理できます。

シスコのコンパクト スイッチ アーキテクチャを使用すると、PoE パススルーを使用する複数の PoE デバイスに電力を供給できます。エンド ユーザのロケーションに設置するように設計された Cisco Catalyst 3560-C および 2960-C コンパクト スイッチは、1 つのイーサネット ケーブルから最大 12 台のデバイスの IP サポートを提供し、最大 8 台のデバイスに PoE パススルーを提供できます。これらのスイッチでは、EnergyWise を有効にして、低電力モードをサポートすることができます。

ヒント EnergyWise アクティビティ チェック機能（スイッチで設定）を使用して、PoE ポートに接続された Cisco IP Phone がトラフィックを送受信しなくなるまで待機してから、ポートの電源をオフにするようにしてください。

現在、EnergyWise Orchestrator クライアントをサポートしているデスクトップ オペレーティング システムは、Windows 7、Windows Vista、および Windows XP（SP3）です。このクライアントは、Windows の組み込み OS を実行するシン クライアントに正常にインストールできますが、このアプリケーションは現在サポートされていません。

規模の大きい Cisco VXI 展開では、たとえば、別個の物理サーバにプロキシをインストールしたり、複数のプロキシ サーバを使用したりすることで、複数の物理サーバにまたがってサービス（サーバ、プロビジョニング、データベース、およびプロキシなど）を分散させる方法により、Orchestrator サーバを拡張できます。規模の小さい展開（ POC など）では、オーケストレータ サーバ、データベース、プロビジョニング サーバ、およびプロキシ サーバを 1 台の Windows サーバにインストールできます。

シスコから提供される EnergyWise 管理ステーションおよびエンドポイント ツールキット SDK を使用して、管理ステーションおよびエンドポイントでの EnergyWise のサポートを有効にしてください。Enerywise SDK を正常に実装するには、ドメイン メンバーが EnergyWise Phase 2 以降を実行していることが必要です。スイッチで実行している EnergyWise のバージョンを表示するには、「show energywise version」コマンドを使用します。適切な EnerygyWise バージョンをサポートするために、スイッチ ソフトウェアのアップグレードが必要になる場合があります。

（注） XenDesktop 5.0 管理スイートには、電源管理機能が搭載されています。これにより、時刻に基づくポリシーを使用して、デスクトップ グループ内で仮想デスクトップの電源をオンにする時刻と台数を制御することができます。この機能を使用して、Energywise 対応のドメイン メンバーおよびエンドポイントと整合性の取れた電源管理ポリシーを実装できます。

Cisco Prime LAN Management Solution（LMS）4.0 は、EnergyWise が有効なネットワークの管理に使用できます。サポートされる機能は、EnergyWise 対応デバイスの検出、適切な Cisco IOS ソフトウェア リリースへのデバイスの自動アップグレード、EnergyWise ドメインと属性の設定、電力使用の監視と報告、および EnergyWise のトラブルシューティングです。Cisco Prime LMS EnergyWise 機能サポートでは、ドメイン メンバー（ ルータやスイッチなどのネットワーク要素）のプロビジョニングとモニタリングに焦点を当てていますが、EnergyWise Orchestrator は、シック クライアントやデスクトップ PC のようなエンドポイントで高度な電源管理ポリシーを制御し、適用することを目的としています。

Cisco Catalyst シリーズ スイッチにおける EnergyWise の設定例については、次の URL にある『Cisco Virtualization Experience Infrastructure Configuration Guide』を参照してください。

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VXI/configuration/VXI_Config_Guide.pdf

Cisco VXI 仮想デスクトップのアセスメントおよびモニタリング

既存のデスクトップ コンピューティング インフラストラクチャの展開前の総合的なアセスメント、仮想デスクトップの実装の設計とキャパシティ プランニング、および仮想デスクトップの展開後の最適化とモニタリングは、Cisco VXI システムの実装を成功させるための重要な側面です。デスクトップ仮想化に対する組織の準備状況とその潜在的な利点を評価するには、詳細に定義された現実的なビジネスの促進要因と、現在のインフラストラクチャの明確なスナップショットを開発するのが最善の方法です。仮想デスクトップの事前アセスメント、設計、実装、モニタリング、最適化、およびキャパシティ プランニングを行うツールは、この評価の実行に不可欠です。これらのツールは、既存のデスクトップ コンピューティング リソースの使用状況とユーザ エクスペリエンスを理解するための機能、デスクトップ仮想化導入に関するキャパシティ プランニングを実行するための機能、仮想化デスクトップ リソースの使用状況とユーザ エクスペリエンスを監視するための機能、およびデスクトップ仮想化の利点を実証し、報告するための機能を提供します。アセスメントの目標は、デスクトップ仮想化に対する準備状況と要件を確認することです。デスクトップ仮想化に対するデスクトップやユーザの適合性を確認する作業は、展開の設計および計画段階の一環として行います。

大規模なデスクトップ展開では、これらのツールを使用してデスクトップ コンピューティング リソースの使用状況、アプリケーションの作業負荷、ユーザの動作、およびユーザ エクスペリエンスを視覚的に確認できます。これらのツールによる一般的な測定には、コンピューティング、メモリ、ストレージ、およびネットワーク リソースに関する使用メトリックと、アプリケーションの応答時間、ログイン時間、および遅延測定に関するデスクトップ ユーザのエクスペリエンス メトリックが含まれます。オペレーティング システム、ハードウェア プロファイル、アプリケーション、ユーザ設定、周辺機器(プリンタやスマート カード リーダーなど)、およびモニタの使用状況を含む、デスクトップの詳細なハードウェアおよびソフトウェア プロファイルも収集されます。仮想化よりも前にベースラインのユーザ エクスペリエンス アセスメントを行うことは、仮想デスクトップの展開におけるユーザ エクスペリエンスを評価するうえで重要です。

データの収集が終わると、アセスメント ツールによってレポートが生成されます。このレポートを使用して、デスクトップ仮想化の候補となる最適および準最適なデスクトップを識別します。アセスメントの目標は最終的な設計ではなく、ネットワーク インフラストラクチャ、ユーザ アプリケーション、およびデスクトップ環境を組み合わせたデスクトップ仮想化プロジェクトの実行可能性の分析にあります。仮想化の相対的な適合性を判断するには、確立前のしきい値を使用した複合メトリックに基づく客観的な適合性評価を使用します。また、アセスメント ツールを使用することで、ログイン時間の削減に基づく、またはデスクトップのハイ アベイラビリティや交換時間の削減、およびアプリケーション ロード時間の削減といった利点による生産性の向上を予測できます。

モニタリング ツールは、インタラクティブ ディスプレイ、レポート、および警告を介した仮想デスクトップのリアルタイム モニタリングを実現します。モニタリング ツールでは、サービス レベルと VDI 環境のセキュリティを検証できます。また、このツールを使用して、仮想デスクトップ環境の使用に対するサービス料を割り当てることもできます。仮想化アプリケーションの監視も可能です。

アセスメント ツールを使用するには通常、アグリゲーションおよび分析用の中央リポジトリにデータを収集し、通信するためのエージェント ソフトウェアがデスクトップにインストールされていることが必要です。エージェント ソフトウェアの動作はエンド ユーザに対して透過的であり、デスクトップのパフォーマンスに影響しません。この通信に使用されるポートが、すべての中間ネットワーク要素で開かれていることが重要です。何千ものデスクトップを監視する場合があるので、中央リポジトリ上のデータベースに十分なストレージを割り当てることも重要です。エージェント ソフトウェアは、デスクトップに手動でインストールすることも、LDAP/GPO や、デスクトップの更新に使用されるその他の標準ツール（SMS など）を使用して自動的に配布することもできます。データ収集がいったん開始されると、データは評価期間中（30 日間など）継続的に収集されます。収集されたデータを使用して、監視対象のデスクトップのマシン、アプリケーション、およびユーザ インベントリの詳細な図を作成できます。

デスクトップの低パフォーマンスを示す要素には、次のものがあります。

- [Slow User Logins] は、指定されたしきい値よりも時間がかかっているログインを示します。
- [Slow Application Load Times] は、指定されたロード時間（秒数）を超えたアプリケーションを示します。
- [Top CPU Consuming Applications] は、最も多くの CPU サイクルを使用するアプリケーションを示します。
- [Top Memory Consuming Applications] は、最も多くのメモリを使用するアプリケーションを示します。
- [Machines with High CPU Usage] は、指定されたしきい値よりも CPU 使用率の高いマシンを示します。
- [Machines with High Memory Usage] は、指定されたしきい値よりもメモリ使用率の高いマシンを示します。

アセスメントおよびモニタリング ツールは、検査データ、診断レポート、およびアセスメント レポートのリアルタイム表示を提供します。これらのツールは、グラフやチャートを使用して検査データの概要を表示し、傾向の分析や潜在的な問題の識別を支援します。これらの表示は、Cisco VXI 展開の状態を検査するときに役立ちます。特定の測定しきい値を超えたときに、電子メールまたは RSS フィードを介してアラートを送信することができます。RSS フィードのポーリングを行ったり、他のシステムにデータを渡したりするには、自動化プログラムを使用できます。データを報告しているマシンの数を示すレポートが、電子メールを介して毎日送信されるようにスケジュールを組み、データ収集が問題なく処理されていることを確認できるようにしてください。

仮想デスクトップ モニタリング ツールの使用例：

- 仮想デスクトップを監視し、SLA に関するリソースの使用率とユーザ エクスペリエンスを確認する。
- リソース使用率が高く、ユーザ エクスペリエンスが低いためにパフォーマンスが低下している仮想デスクトップ セッションをトラブルシューティングする。
- 大規模な Cisco VXI 展開を監視し、測定値の収集によってリソースの使用を特徴づける。測定値には、仮想デスクトップでのピークおよび平均負荷、仮想デスクトップの上位リソース ユーザ、履歴およびリアルタイム レポートの生成、しきい値に達したときのアラートの生成が含まれます。

仮想デスクトップの事前アセスメントおよびモニタリング ツールに関するガイドライン：

仮想デスクトップのアセスメントとモニタリングの実行に推奨されるツールは、Liquidware Labs（Stratusphere FIT/UX）および Lakeside（Systrack）提供のツールです。

仮想スイッチに接続された専用のネットワーク モニタを使用して、仮想デスクトップ ネットワーク トラフィックを監視し、アプリケーションの使用を報告することが推奨されます。適切な帯域幅を割り当て、ユーザが WAN 上の仮想デスクトップにアクセスする際の遅延を小さくするには、適切なネットワーク計画とプロビジョニングが重要です。

ハイパーバイザへのインターフェイスを備えたモニタリング ツールでは、ホスト、仮想デスクトップ、および SAN リソースの使用状況を報告できます。

移行する前に、ユーザ エクスペリエンスのベースラインを確立することが推奨されます。展開後のユーザ エクスペリエンスの測定では、展開またはパイロット時のエンド ユーザに対する影響を数値化します。アセスメントは、仮想デスクトップのプロビジョニング方法（リソース、イメージ、およびアプリケーション）、使用するデスクトップ プロトコル、および有効にするデスクトップ プロトコル機能（周辺機器など）を判断するのに役立ちます。

仮想化に適していないアプリケーションを識別することは、正常な Cisco VXI の展開に不可欠です。現在使用されているアプリケーションが正常に動作し、特に 1 台のホスト マシンで数十台の仮想デスクトップに拡張したときの仮想化環境のパフォーマンスに影響がないことを確認します。

Cisco AS は、評価を行い、アセスメント レポートと仮想化設計計画を生成する Cisco VXI の計画、設計、およびモニタリング サービスを提供します。サービスの出力には、Cisco VXI 設計書、運用準備と実装の計画、セルフサービス ガイド、PoC レポート、テスト計画、および準備状況レポートが含まれます。詳細については、次の場所にある Cisco AS の Web サイトを参照してください。
http://www.cisco.com/en/US/products/ps10374/services_segment_service_home.html

デスクトップ管理ツール

デスクトップのプロビジョニングとモニタリングは、正常な Cisco VXI システムの管理に不可欠です。このタスクについて記載されているガイドラインと推奨事項を使用してください。

デスクトップのプロビジョニング

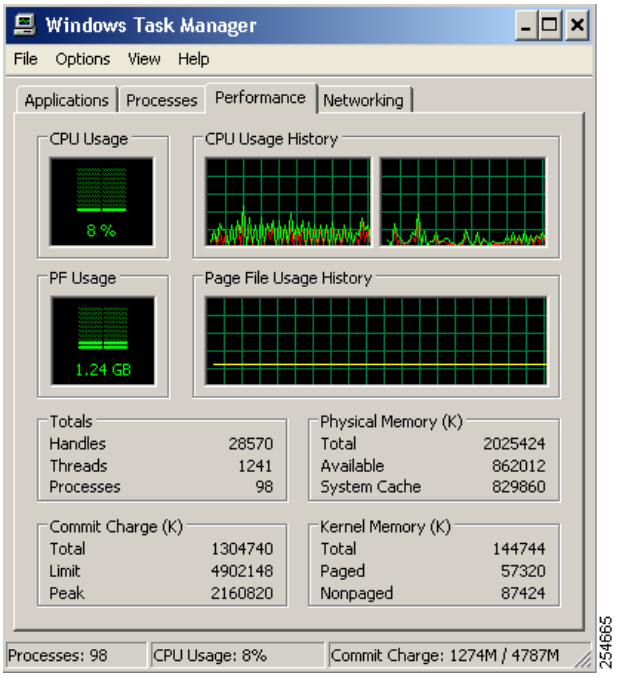
仮想デスクトップおよびデスクトップ仮想化エンドポイントは、Altiris などの標準の Microsoft Windows ソフトウェア管理ツールを使用して管理できます。これらのツールを使用して、エージェントのアップデート、OS フィックス、セキュリティのアップデート、およびアプリケーションをプッシュ アウトできます。Microsoft Windows デスクトップのユーザ プロファイルを管理し、デスクトップに適用するには、Liquidware Labs ProfileUnity、AppSense、Citrix XenDesktop profile management、および VMware Virtual Profiles などのツールを使用します。これらのデスクトップ パーソナライゼーション ツールは、ログインを高速化し、ユーザ プロファイルの破損を防止します。

ウイルス対策スキャンは、サードパーティのアプライアンスを使用してオンラインまたはオフラインのデスクトップでスケジュールし、実行できます。スケジューリングの柔軟性を高めるため、ウイルス対策スキャン アプライアンスと一緒に VMware VMsafe API を使用して、仮想デスクトップのオンラインまたはオフラインのウイルス対策スキャンを実施することを検討してください。

デスクトップのモニタリング

個々のデスクトップにおけるリソース（CPU、メモリ、ストレージ、およびネットワーク）の使用をリアル タイムで測定し、監視するには、VMware 統計情報ロギング アプリケーションを使用します。Intel IOMeter ツールと、リソース使用率およびパフォーマンス測定を表示する組み込みの Microsoft Windows Task Manager（図 84）の使用を検討してください。これらのツールは、トラブルシューティングにも役立ちます。VMware vCenter を使用すると、これらの測定値を仮想マシンごとに取得できます。

図 84　Windows Task Manager パフォーマンス モニタ



物理デスクトップのリソース使用率を測定することにより、管理者は、仮想化環境に移行する前に物理的なデスクトップ インフラストラクチャを評価できます。また、将来的なリソース増築（コンピューティング、メモリ、ストレージ、およびネットワーク リソース）用のキャパシティ プランニングや、仮想デスクトップでの展開後 QoS モニタリングが可能になります。Liquidware Labs または Lakeside 提供のツールの使用を検討してください。アクセスされているファイルやデスクトップで呼び出されているアプリケーションの監査ログも、デスクトップ使用の監視やパフォーマンス問題のトラブルシューティングに役立つ場合があります。デスクトップにインストールできるソフトウェアまたはアプリケーション プローブのほか、Microsoft Windows Performance Manager を使用することを検討してください。

Cius 管理ツール

Cisco Unified Communications Manager（CUCM）は、VXI システム内の UC および DV エンドポイントである Cius タブレット デバイスの管理に使用できます。CUCM を使用して、ファームウェアの更新とデバイス設定の適用（ファイル暗号化や VPN 設定のようなセキュリティ ポリシーを含む）、アプリケーションの管理、および一括アップデートの更新を行います。Cisco Anyconnect クライアントは、Cius に統合されており、VPN 機能を提供します。Cius の高度な管理機能をサポートするには、CUCM 8.5 が必要であることに注意してください。エンド ユーザは Cius にアプリケーションをダウンロードおよびインストールすることができ、管理者は CUCM を使用してすべてのデバイスにそれらのアプリケーションをプッシュ ダウンすることができます。アプリケーションは、CUCM アプリケーション リポジトリ、デバイス SD カード、Android マーケット、Cisco Marketplace アプリケーション リポジトリ、または企業固有のリポジトリから Cius に展開されます。Android OS 上で動作する DV クライアント アプリケーション（ Wyse PocketCloud、Citrix Receiver、VMware View Client など）を Cius にダウンロードしてインストールする必要があります。管理者は、CUCM に登録するときに、企業アプリケーションを Cius にプッシュするように指定できます。エンド ユーザは、管理者承認のリストからアプリケーションを選択することもできます。この場合、エンド ユーザは、CUCM からアプリケーション リストを要求し、そこから特定のアプリケーションの申し込みまたは申し込みの解除を行うことができます。アプリケーションの設定には、管理者が事前に設定するものと、エンド ユーザがカスタマイズするものがあります。リモート ワイプ、バックアップと復元、デバイス トラッキング、ポリシーの適用、およびウイルス保護などのより高度なモバイル デバイス管理機能は、サード パーティ ベンダーが提供するエンタープライズ モバイル デバイス管理ツールで使用できます。

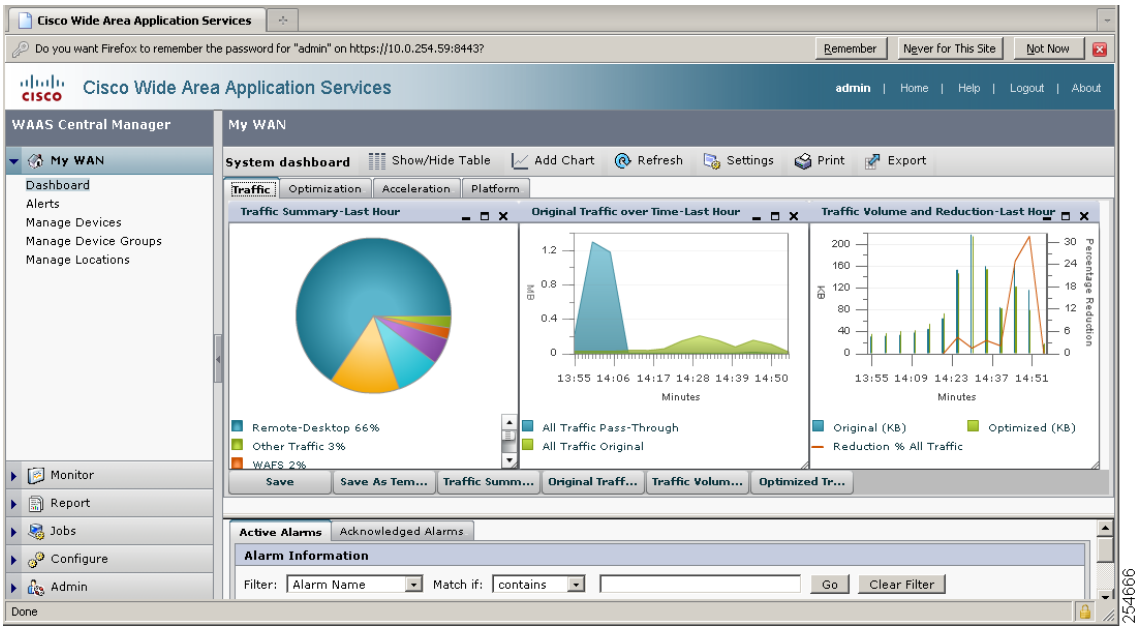
シスコ管理ツール

Cisco VXI システムの管理に欠かせないその他のシスコ ツールは、Cisco UCS Manager、Cisco Fabric Manager、Cisco DCNM、Cisco Prime LMS、Cisco ACE Device Manager、Cisco WAAS Central Manager、および Cisco Adaptive Security Device Manager（ASDM）です。このうち、Cisco UCS Manager、Cisco ACE Device Manager、Cisco WAAS Central Manager、および Cisco ASDM などの多くのツールは、管理対象デバイスに組み込まれており、ブラウザからアクセスできます。Cisco Prime LMS、Cisco Fabric Manager、および Cisco DCNM などの一部のツールは、Microsoft Windows サーバ アプリケーションであり、ブラウザまたはクライアント アプリケーションからアクセスできます。

（注） Cisco WAAS Central Manager は、専用の Cisco WAAS アプライアンス上で動作します。

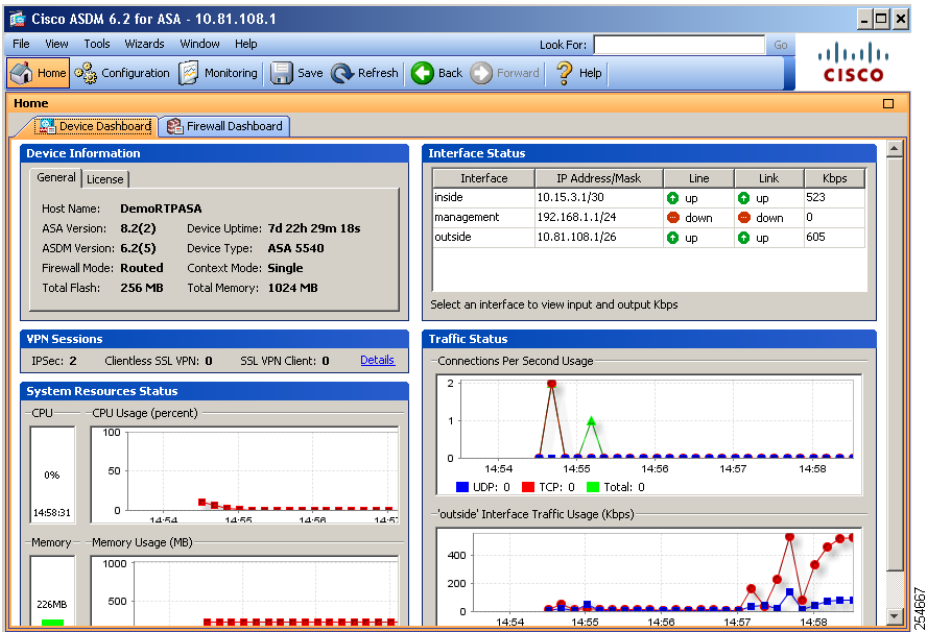
Cisco WAAS Central Manager を使用すると、WAN 上のブランチ オフィスから開始されたセッションを監視し、トラフィックの最適化に関するレポートを生成できます（図 85）。Cisco WAAS アプライアンスはインラインまたはオフラインで展開できるので、Central Manager によって生成されるトラフィックの使用率と最適化のレポートは、隣接ルータを通過するすべてのトラフィックを示すものではありません。Cisco WAAS デバイスは、オフライン設定で提供されたトラフィックのみを認識します。予備の Cisco WAAS Central Manager とステートフルな冗長性を使用して可用性を高め、その他の重要なリソースが存在するデータセンターに Cisco WAAS Central Manager を配置するようにしてください。Cisco WAAS の設定は、Cisco WAAS Central Manager で定義した後に、ネットワーク内のすべての Cisco WAAS デバイスに効率的にプッシュ アウトすることができます。

図 85　　Cisco WAAS Central Manager GUI



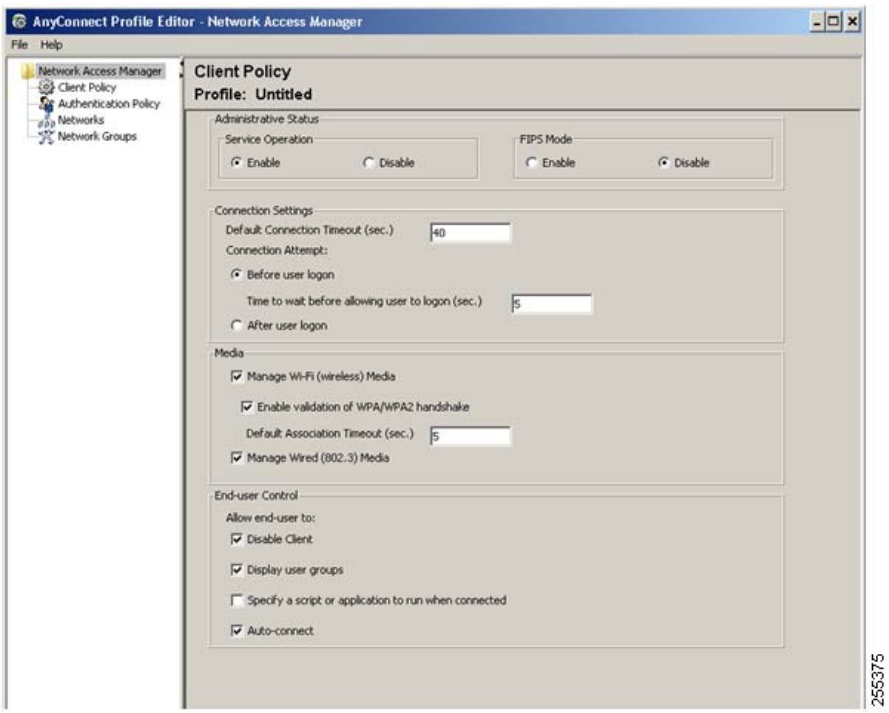
VPN クライアントを使用する企業ネットワークにアクセスするために Cisco ASA を使用しているテレワーカー（社外で作業）が開始したセッションの監視とレポート生成を行うには、Cisco ASDM を使用します。Cisco ASDM を使用すると、Cisco ASA アプライアンスのファイアウォール、Network Address Translation（NAT; ネットワーク アドレス変換）、および VPN プロファイルをプロビジョニングでき、さらに Cisco ASA のファイアウォール アクティビティ、CPU の使用状況、ネットワーク インターフェイスの使用状況、および VPN ステータスを監視できます（図 86）。

図 86　　Cisco ASDM デバイス ダッシュボード



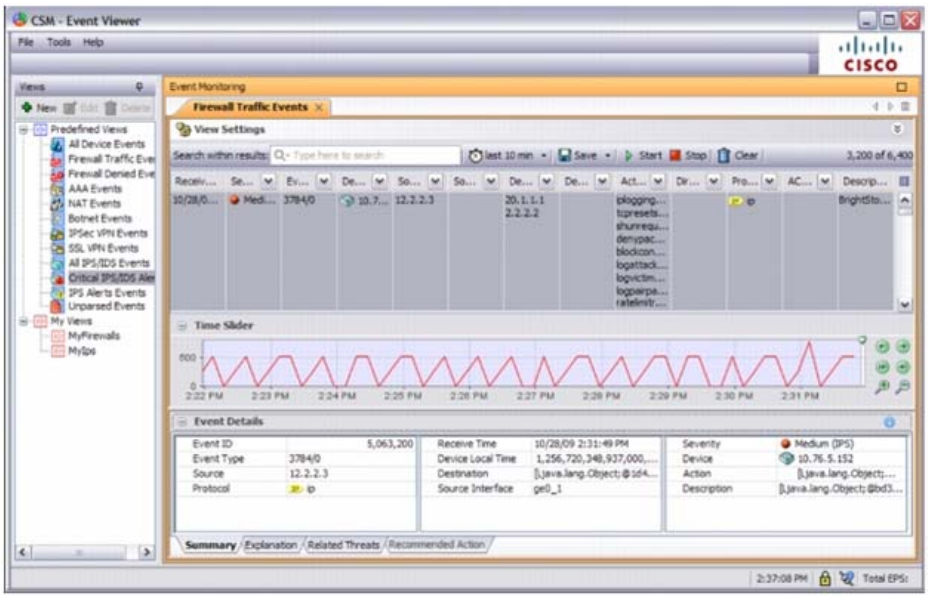
AnyConnect プロファイル エディタは、GUI ベースのコンフィギュレーション ツールです。このツールを使用して、クライアント機能を制御する設定を含む XML ファイルである AnyConnect クライアント プロファイルを設定できます。以前は、プロファイル内の XML タグを編集することにより、プロファイル設定を手動で変更するしかありませんでした。クライアント ソフトウェア パッケージが SSL VPN クライアント イメージとして ASA にロードされている場合、ASDM からプロファイル エディタを起動することもできます。これにより、管理者は、AnyConnect VPN Client、Network Access Manager（レイヤ 2 接続）クライアント、Web Security クライアント、および Telemetry クライアントに関する設定を作成できます。ACPE で生成される設定は、AnyConnect バイナリ インストール パッケージにバンドルし、SMS を介してエンドポイントにプッシュできます。

図 87　AnyConnect Profile Editor



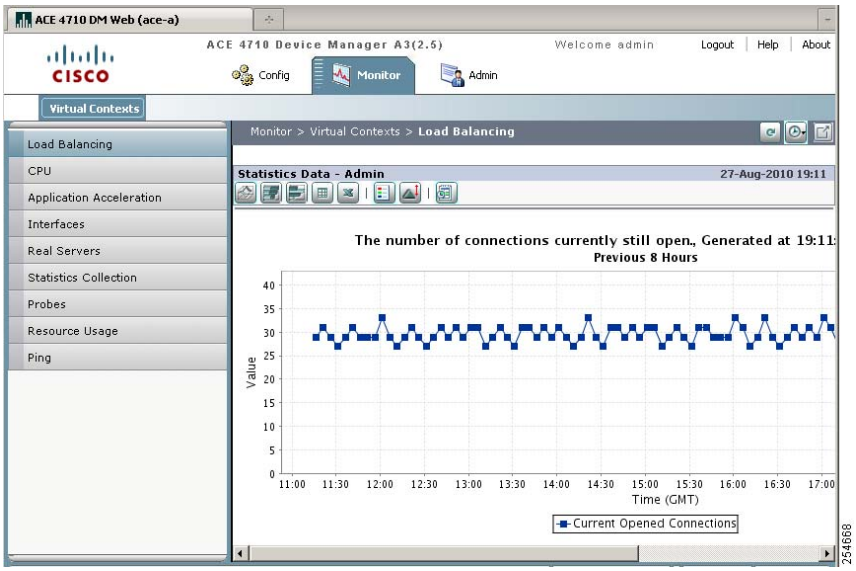
Cisco Security Manager は、シスコのセキュリティ デバイスのセキュリティ ポリシーを管理します。また、IOS ルータ、Catalyst スイッチ、ASA および PIX セキュリティ アプライアンス、ファイアウォール、VPN、および IPS に関係する Catalyst サービス モジュール、IPS アプライアンス、ならびにルータや ASA デバイス対応の各種サービス モジュール全体にわたるファイアウォール、IPS、および VPN（サイト間、リモート アクセス、および SSL）サービスの統合プロビジョニングをサポートします。Cisco VXI 展開の ISR ルータに ASA と DMVPN をプロビジョニングするには、Cisco Security Manager を使用します。

図 88　　Cisco Security Manager コンソール



Cisco ACE Device Manager を使用して、接続マネージャへのアクセスに Cisco ACE アプライアンスを使用するすべてのデスクトップ仮想化ユーザ セッションを監視し、レポートを生成します。Cisco ACE Device Manager では、データセンターに存在する接続マネージャに提供される全体的なセッション負荷のレポートを生成できます（図 89）。可用性を高めるため、ステートフルな冗長性を備えた冗長ペアで Cisco ACE を展開してください。

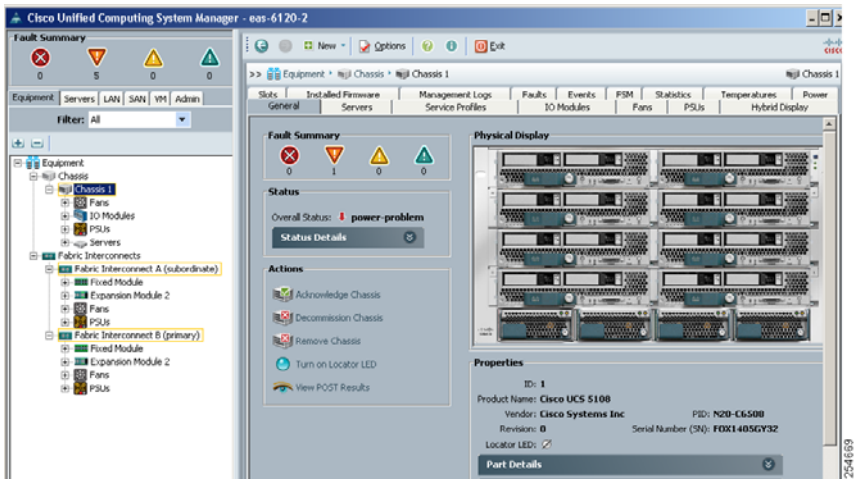
図 89　　ACE Device Manager モニタ



Cisco WAAS および Cisco ASA の管理には、Web ベースの GUI（CLI ではなく）を使用してください。GUI を利用することで、複数のデバイスの管理、複数のデバイスに対する同様の設定のプロビジョニング、複数の管理対象デバイスから収集した統計情報に基づく集約レポートの生成が可能になります。このアプローチは、多数の管理対象デバイスを抱える大規模な展開に推奨されます。

Cisco UCS ブレード サーバ（Cisco UCS 5100 シリーズ ブレード サーバ シャーシおよび Cisco UCS 6100 シリーズ ファブリック インターコネクトの両方）のプロビジョニングには、Cisco UCS Manager（図 90）を使用し、プロビジョニングは複数のシャーシにまたがった最大 320 台のブレードまで拡張可能です。管理トラフィックと仮想マシン トラフィックを区別するには、アップリンク上に別個の VLAN をプロビジョニングします。このプロビジョニングは、イーサネット アップリンク ポートおよび VMware ESXi で動作する vSwitch で実行します。すべてのブレードに同一の設定を適用するには、サービス プロファイル テンプレートのほか、vNIC および virtual Host Bus Adapter（vHBA; 仮想ホスト バス アダプタ）の特性に対応したテンプレートを使用する必要があります。また、Cisco UCS Manager は、ハードウェア交換時のダウンタイムを迅速に削減するため、ブレード スワッピングを可能にします。

図 90　　Cisco UCS Manager



Cisco DCNM を使用して、Cisco Nexus 5000 および 7000 シリーズ スイッチ（Data Center Network Manager）のプロビジョニングと監視を行います。Cisco Fabric Manager を使用して、Cisco MDS 9000 ファミリのファイバ チャネル スイッチ（Fabric Manager Web Client）を管理します。

図 91　　Data Center Network Manager

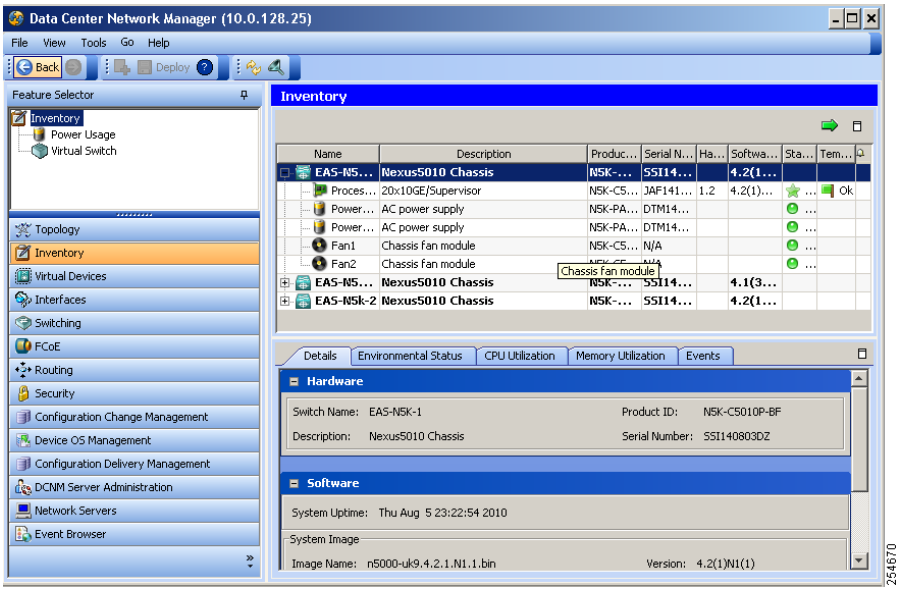
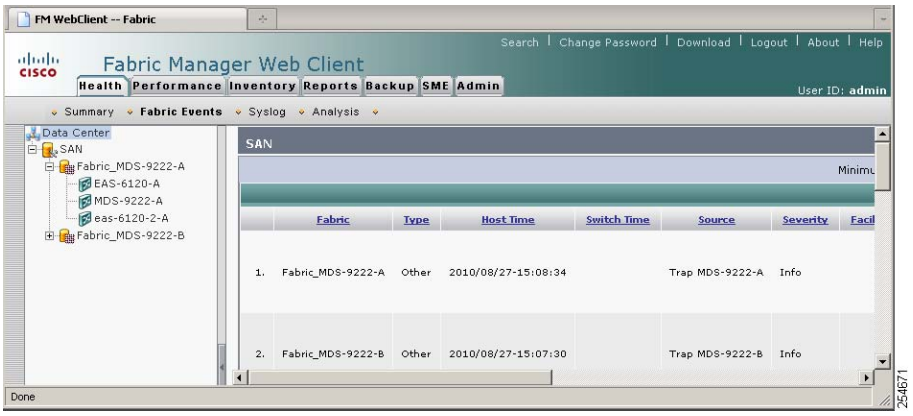
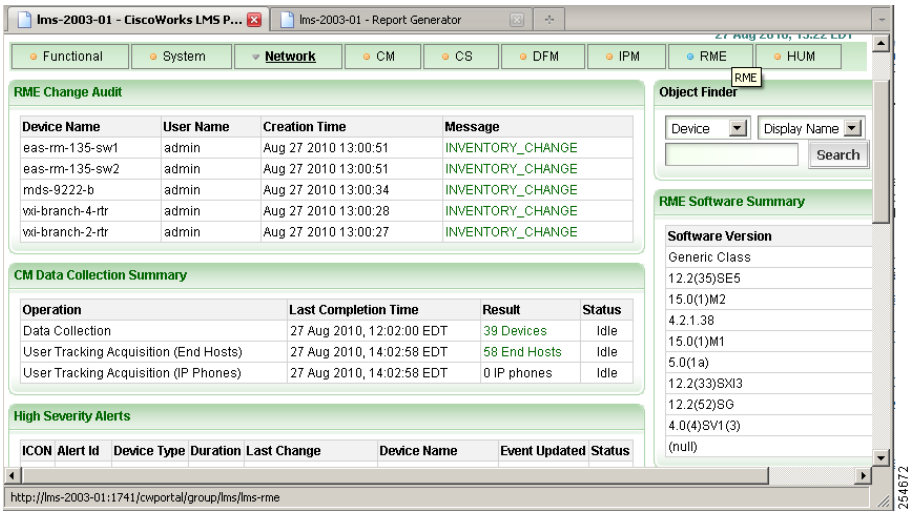


図 92　Fabric Manager Web Client



Cisco Prime LMS を使用して、エンドツーエンド システム全体を通したルータ、スイッチ、およびその他のネットワーク デバイスの監視とプロビジョニングを行います（図 93）。この機能を使用して、すべての管理対象インターフェイスにおけるネットワーク リンク使用率、遅延、およびジッタを測定できます。

図 93　Cisco Prime LMS Resource Manager Essentials



Cisco Unified Communications Management Suite は、システムに導入される Cisco Unified Communications Manager、Cisco Unified Presence、Cisco Unity サーバ、Cisco Unified Personal Communicator クライアント、Cisco Cius タブレット、および Cisco IP Phone の管理に推奨されるツールです。サーバの Cisco Unified Communications スイートで使用できる組み込みの Web ベース管理インターフェイスのほか、大規模な展開には Cisco Unified Operations Manager、Provisioning Manager、Service Monitor、および Statistics Manager で構成される Cisco Unified Communications Management Suite が推奨されます。

関連情報

次に、この章で説明したハードウェアおよびソフトウェアを含む特定のベンダー情報の詳細へのリンクを示します。

『Cisco UCS GUI Configuration Guide』

http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/1.3.1/UCSM_GUI_Configuration_Guide_1_3_1.pdf

『Cisco Unified Communications Manager Systems Guide』

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_0_2/ccmsys/accm.pdf

Citrix ドキュメント

http://support.citrix.com/proddocs/index.jsp

EMC Unisphere 管理スイート

http://www.emc.com/products/detail/software/unisphere.htm?context=storage

NetApp Virtual Storage Console

http://www.netapp.com/us/products/management-software/vsc/virtual-storage-console.html

NetApp StorageLink

http://media.netapp.com/documents/tr-3732.pdf

Altiris のリファレンス文書

http://www.symantec.com/business/theme.jsp?themeid=altiris

Microsoft Active Directory およびネットワーク サービス

http://www.microsfoft.com/

『Cisco Network Analysis Module Deployment Guide』

http://www.cisco.com/en/US/prod/collateral/modules/ps2706/white_paper_c07-505273.html#wp9000247

Cisco NAM アプライアンス ドキュメント（コマンド リファレンスおよびユーザ ガイド）

http://www.cisco.com/en/US/partner/products/ps10113/tsd_products_support_series_home.html

『Cisco Wide Area Application Services Configuration Guide (Software Version 4.1.1)』

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v411/configuration/guide/cnfg.html

『Cisco Adaptive Security Device Manager Configuration Guide』

http://www.cisco.com/en/US/products/ps6121/tsd_products_support_configure.html

Cisco ACE 4700 シリーズ アプリケーション コントロール エンジン アプライアンス ドキュメント

http://www.cisco.com/en/US/products/ps7027/tsd_products_support_series_home.html

『Cisco UCS Manager Configuration Guide』

http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html

Cisco DCNM ドキュメント

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_configure.html

Cisco Fabric Manager ドキュメント

http://www.cisco.com/en/US/partner/products/ps10495/tsd_products_support_configure.html

Cisco Nexus 1000v ドキュメント

http://www.cisco.com/en/US/partner/products/ps9902/products_installation_and_configuration_guides_list.html

Cisco Prime ドキュメント

http://www.cisco.com/en/US/partner/products/sw/cscowork/ps4565/tsd_products_support_maintain_and_operate.html

『Devon IT Echo™ Thin Client Management Software Version 3 Overview』

http://www.devonit.com/software/echo/overview

『Devon ThinManage 3.1 Admin Guide』

http://downloads.devonit.com/Website/public/Documentation/thinmanage-3-1-adminguide-rev12.pdf

『Devon IT TC5 Terminal Quick Start Guide』

http://www.devonit.com/_wp/wp-content/uploads/2009/04/tc5-quickstartguide-devonit-english.pdf

IGEL Universal Management Suite 3 の概要

http://www.igel.com/igel/live.php,navigation_id,3294,_psmand,9.html

『IGEL Universal Management Suite 3 Install Guide』

http://www.download-igel.com/index.php?filepath=manuals/english/universalmanagement/&webpath=/ftp/manuals/english/universalmanagement/&rc=emea

『IGEL Universal Management Suite 3 User Guide』

http://www.download-igel.com/ftp/manuals/english/universalmanagement/IGEL%20UMS%20User%20Guide.pdf

『IGEL Universal Desktops User Guide』

http://www.download-igel.com/ftp/manuals/english/universalmanagement/IGEL%20UMS%20User%20Guide.pdf

Cisco UMS ドキュメント

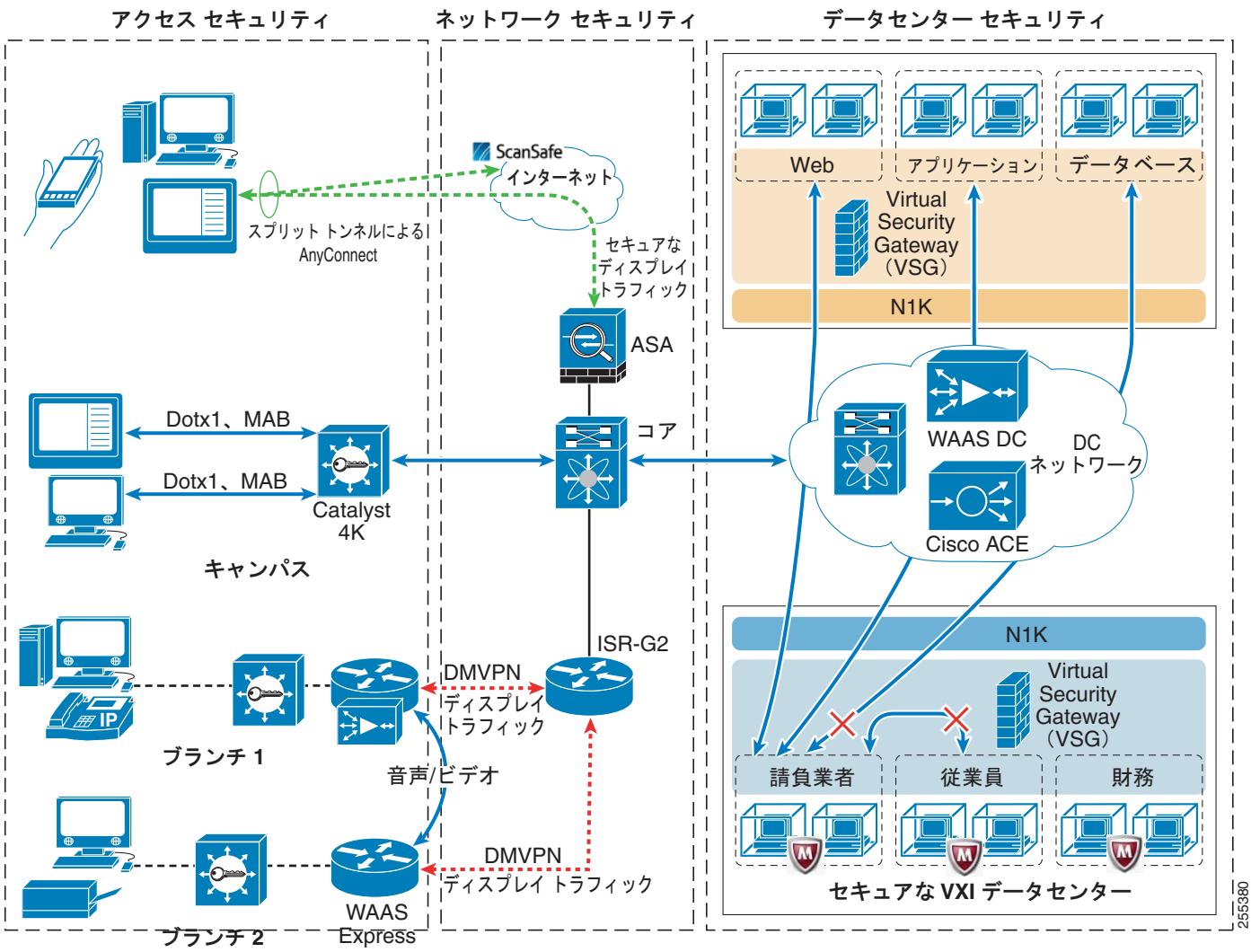
http://www.cisco.com/

Cisco VXI セキュリティ

はじめに

ユーザ エンドポイントにローカル データは存在せず、データセンターからデータが持ち出されることもないので、デスクトップ仮想化は本質的に従来のデスクトップ環境よりも安全です。ただし、デスクトップ仮想化を使用すると、いつでもどこからでもデータセンターにアクセスできるので、新たなセキュリティ問題が生まれます。IT データセンターは従来、ほとんどのシナリオでエンド ユーザがデータセンター コンポーネントに直接アクセスする必要はなく、制御されるアクセス メカニズムを介したユーザ アプリケーションだけがデータセンター内のサーバと相互作用するという考え方に基づいて構築されていました。この考え方はもはや通用せず、ユーザ デスクトップ（信頼されないコンピューティング環境）とデータセンター コンポーネントを確実に分離させることが必要です。また、現在はすべてのユーザ デスクトップが一緒にクラスタ化されているため、セキュリティが侵害された場合の影響度は従来のデスクトップ環境よりもはるかに大きくなります。Cisco VXI システムでは、一連の堅牢なセキュリティ機能とガイドラインを導入することによって、動的な仮想環境におけるセキュリティ問題に取り組んでいます。この章では、これらの機能の詳細を示し、Cisco VXI システムの保護におけるベスト プラクティスについて説明します。これらのセキュリティ メカニズムは Cisco VXI 環境だけに適用されること、また、Cisco VXI と従来のデスクトップの両方を使用している企業では、保護を完全にするため、従来および既存のセキュリティ テクノロジーが必要になります。

図 94　エンドツーエンドの Cisco VXI セキュリティ



上の図 94 に、保護する必要のある Cisco VXI システムの 3 つの論理区分を示します。これらの論理区分は、データが発信される場所と、保護を必要とする対象に基づいて分割されます。3 つの区分を合わせた焦点は、ディスプレイ プロトコル トラフィック、UC トラフィック、周辺機器トラフィック、仮想デスクトップに存在するデータの保護と、侵害されたマシンの分離です。

最初の区分はアクセスです。アクセス セキュリティの目的は、エンドポイントから最初のホップ ネットワーク要素に発信されるすべてのデータを保護することにあり、その範囲は固定/モバイル テレワーカー、ブランチ、およびキャンパス ユーザ環境に及びます。2 つ目の区分はネットワークです。ネットワーク セキュリティは、信頼されないネットワーク（インターネットなど）や信頼されるネットワーク（キャンパスなど）を移動するデータに対する Cisco VXI のセキュリティ面が対象となります。ユーザ データがデータセンターに配信された後は、データセンターまたはキャンパス エッジでデータセンター内のセキュリティ面を調べる必要があります。これらのセキュリティ面はデータセンターのセキュリティ下で扱われ、VM アクセスの保護、セグメンテーション/ゾーン分割、および仮想デスクトップ OS の保護が対象となります。この章の残りの部分では、上記の内容を中心とした Cisco VXI 固有のテクノロジーと設計戦略について説明します。

設計上の考慮事項

アクセス セキュリティ

Cisco VXI を有効にしたネットワークの実装により、アプリケーション データのロケーションがユーザ制御のデスクトップから中央集中型のデータセンターに移されます。Cisco VXI におけるアクセス セキュリティでは、エンドポイントとデータセンター間を移動しているデータと識別情報の保護に焦点を当てています。企業がサポートするアプリケーションと OS はローカルではなくデータセンターに存在するので、エンドポイントのセキュリティ侵害による影響は、データセンターに至るまでのエンドツーエンド セキュリティがどのように実装されているかにかかっています。

固定のテレワーカー環境は、最も明確に定義されています。この場合、ホーム オフィスからアクセス ルータを使用した VPN アクセスを許可する、標準の Cisco Validated Design となります。この展開では、エンドポイントからデータセンター内の仮想デスクトップへのアクセスを可能にする暗号化 VPN トンネルが構築されます。この展開を Cisco Virtual Office（CVO）と呼びます。自宅用ルータの展開は、企業セキュリティ ポリシーを従業員の自宅に拡張したものなので、アクセス ルータの背後にあるテレワーカー ローカル ネットワークは信頼できると見なすことができます。CVO の構成によっては、信頼できないエンドポイントが VPN トンネルの外側にある公共インターネットに直接アクセスできる場合があることに注意してください。このような構成では、dot1x を使用するデバイス認証や MAC アドレスに基づいた認証が推奨されます。詳細については、
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a008074f24a.pdf
を参照してください。

モバイル テレワーカー環境では、通常、信頼できない非セキュアな公共ネットワーク経由で仮想デスクトップにアクセスします。モバイル ワーカーには、ラップトップなどのシック エンドポイント、または Apple iPad などの Cisco VXI シン クライアントを使用して仮想デスクトップを表示することが期待されます。ハードフォン制御用の Cisco Unified Personal Communicator は、モバイル テレワーカー プロファイルには含まれません。このシナリオでは、ディスプレイ トラフィックの保護がエンドポイントから開始される必要があります。Cisco VXI では、企業ネットワークまで AnyConnect 3.0 経由の VPN トンネルを作成し、ディレクトリまたはネットワーク アクセス コントロール データベースで認証することを推奨しています。トンネルを確立した後は、デスクトップ クライアントを自動的に起動するように Cisco AnyConnect クライアントを設定する必要があります。設定例については、次のリンクを参照してください。
http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00808efbd2.shtml

Cisco AnyConnect 接続は通常、データセンターのインターネット アクセス エッジにある Cisco ASA 適応型セキュリティ アプライアンスで終了します。ユーザ チャレンジ（パスコード要求）が表示され、認証が実行され、従業員のアクセスを許可する暗号化トンネルが構築されます。ディスプレイ トラフィックは遅延の影響を受けやすいので、Datagram Transport Layer Security（DTLS）を使用することが推奨されます。Cisco AnyConnect クライアントおよび ASA は、プライマリ接続オプションとして DTLS を使用するように設定できます。

キャンパス環境の Cisco VXI ユーザは、信頼できるネットワーク内にあり、アクセス スイッチからデータセンターへのトラフィックは管理対象のセキュアなネットワークを経由するものと見なされます。ただし、Ciso IP Phone などの信頼できる特定のデバイスが接続されていない限り、アクセス スイッチはホスト ポートを信頼できないものと見なします。キャンパス アクセス スイッチに接続している Cisco VXI エンドポイントは、信頼できないものと見なされます。Cisco VXI システム内のエンドポイントは今後、特定のユーザに接続されることはなく、あらゆるユーザがどこからでも仮想デスクトップにアクセスできるようになります。企業は、各エンドポイントとユーザを結びつけるか、Cisco VXI 環境でエンドポイントとユーザを個別に認証することができます。いずれの場合も、エンドポイント認証メカニズムの実装が強く推奨されます。Cisco VXI システムでは、クライアント認証に IEEE 802.1x を利用します。ネイティブの IEEE 802.1x サプリカントがエンドポイントで使用できない場合は、Cisco AnyConnect 3.0 と Secure Services Client を一緒に使用できます。Cisco VXI システムで実施されたテストには、Windows XP エンドポイント上の AnyConnect 3.0 と、Windows 7 で動作する Microsoft のネイティブ サプリカントが使用されました。シン クライアントによっては、IEEE 802.1x をサポートしていても、AnyConnect 3.0 のインストールはサポートしていない場合があります。この場合、ネイティブの 802.1x 機能を使用する必要があります。展開されたエンドポイントでいずれの IEEE 802.1x サプリカントもサポートしていない場合は、アクセス スイッチの 802.1x ベース MAC Authentication By-pass（MAB; MAC 認証バイパス）機能を使用します。MAB では、ACS 5.2 で動作する RADIUS サーバに保持されている、信頼できるエンドポイントの MAC アドレスのデータベースを使用して、エンドポイントの MAC アドレスを認証します。802.1x と MAB の設定と使用の詳細については、
http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/31sg/configuration/guide/dot1x.html
を参照してください。

エンドポイントからアクセス スイッチへのすべてのディスプレイ トラフィックは、ローカル ネットワーク上を平文で送信されます。リンクのセキュリティに不安のある企業には、MACsec 準拠のホップバイホップ暗号化を使用することが推奨されます。MACsec には、MacSec を備えた dot1x サプリカントをサポートするエンドポイントと、両方をサポートするアクセス スイッチが必要です。このフェーズの Cisco VXI では、AnyConnect 3.0 を実行でき、Catalyst 3K X シリーズ スイッチポートに接続されているエンドポイントのみ、MacSec によって保護できます。将来的には、より多くのエンドポイントおよびアクセス スイッチにサポートの範囲が広がることが予測されます。ビジネス クリティカルなトラフィックはディスプレイ トラフィックであり、このトラフィックが暗号化されていない最初のホップ アクセス スイッチに到達する前にスニフィングされた場合、攻撃者はデータを視覚的に表示できますが、仮想デスクトップ テクノロジーの仕組みにより、データの操作はできないことを覚えておいてください。

ネットワーク エンティティとしてのデバイスの認証に限らず、継続的な信頼性を保つため、できるだけアクセス ポイントの近くでデバイスを監視してください。これには、この章で後述する DHCP スヌーピング、ダイナミック ARP インスペクション、および IP ソース ガードなどのポート セキュリティ対策の設定を利用します。

ブランチ アクセスは企業セキュリティの領域に属しますが、WAN リンクによって分離されます。ブランチは通常、Cisco Integrated Services Routers Generation 2（ISR G2; 第 2 世代サービス統合型ルータ）と、キャンパス/データセンターへの暗号化トンネルを使用して展開されます。キャンパスに配置されたアクセス スイッチと同様に、ブランチは一般に独自のローカル DHCP 要求に対してサービスを提供するので、アクセス層スイッチではインスペクション設定として DHCP スヌーピング、ダイナミック ARP インスペクション、および IP ソース ガードを展開する必要があります。デバイス認証用の MAB および IEEE 802.1x も、Cisco ISR 内のブランチ スイッチまたはスイッチ モジュール経由でローカルに展開する必要があります。ブランチ内のエンドポイントからブランチ アクセス スイッチへのリンクのセキュリティに不安がある企業には、MacSec のサポートが強く推奨されます。これは、帯域幅に制限のある WAN 上ではディスプレイ プロトコル トラフィック、印刷トラフィック、および UC トラフィックが、Cisco WAAS と呼ばれる WAN 高速化デバイスを使用して最適化されるためです。いずれの WAN 高速化メカニズムも、事前に暗号化されたトラフィックの最適化にはあまり効果がありません。エンドポイントから、ローカル ブランチの最初のホップ リンクを含むデータセンターまでのパスを保護するために、仮想デスクトップ クライアントの暗号化が使用されている場合、WAN 最適化のメリットを発揮できません。ブランチ環境での WAN 高速化とセキュリティのニーズのバランスを取るため、Cisco VXI では、仮想デスクトップ クライアント暗号化を MacSec ベースのリンク層暗号化に置き換えることを推奨しています。これにより、ブランチ アクセス スイッチからデータセンター ヘッドエンドへの仮想デスクトップのデータは、ブランチ ルータからキャンパス/データセンターへの IPSec トンネルで保護されたまま、さらに WAN 最適化も可能になります。Cisco VXI MacSec の展開に関する推奨事項は、キャンパス アクセスの場合と同様です。

アクセス スイッチから企業データセンターへのキャンパス ネットワークの保護に関する詳細なガイドラインについては、
http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.pdf を参照してください。

ネットワーク セキュリティ

ブランチ オフィスと本社を結ぶサイト間 VPN は、保護された IP Security（IPsec; IP セキュリティ）暗号化トンネルです。これらのトンネルは、トンネル エンドポイントの認証に証明書または事前共有パスワードを使用して導入できます。この導入モデルでは、ルート上でのデータの不用意なキャプチャを最小限に抑えるため、2 つのロケーション間の Cisco VXI データが暗号化されます。Cisco VXI では、Easy VPN と Dynamic Multipoint VPN（DMVPN; ダイナミック マルチポイント VPN）がサポートされます。デスクトップ仮想化により、時間や場所を選ばずに企業データセンターにアクセスできることは非常に重要です。これを実現するための 1 つの方法として、多数の固定テレワーカーおよびブランチを WAN 経由で企業データセンターに安全に接続できるようにします。また、ネットワーク帯域幅と管理オーバーヘッドを削減し、生産性を高めるには、なるべくデータの転送が必要なときにオンデマンドでこれらの接続を作成し、使用していないときは切断されるようにします。一般的な企業の Cisco VXI システムでは、すべてのユーザからのすべてのディスプレイ トラフィックが最も近いデータセンターに到達する必要があります。フォン トラフィックは、ユーザ間にローカルにルーティングされる必要があり、ほとんどの場合はデータセンターを経由する必要はありません。ブランチおよびテレワーカー環境には、ディスプレイ トラフィック用、および必要に応じてフォン トラフィック用に最も近いデータセンターへのセキュアな VPN トンネルを作成する機能と、2 つのブランチ間の一時的なオンデマンド トンネリングの機能を備えることが求められます。これらの推奨事項に加え、QoS マーキングと WAN 最適化をソリューション内で統合し、ユーザ エクスペリエンスを維持する必要があります。これらのニーズをすべて満たすため、Cisco VXI システムでは DMVPN テクノロジーを採用しています。このテクノロジーでは、Next Hop Resolution Protocol とマルチポイント GRE トンネルを使用して、ルーティング要件に基づいた IPSec 接続をオン デマンドで確立するとともに、WAAS によるこれらの接続の最適化を可能にします。DMVPN ソリューションでは、T1/T3、WWAN、xDSL などのさまざまな WAN リンクがサポートされています。Cisco VXI システムでこのソリューションを実装するには、各ブランチまたは固定のテレワーカー ロケーションにある ISR G2 ルータを、データセンター エッジの ASR 1000 VPN ヘッドエンドに接続するように設定します。Cisco Security Manager（CSM）を使用して、DMVPN を設定します。DMVPN の機能の詳細については、
http://www.cisco.com/en/US/products/ps6658/index.html を参照してください。

キャンパスに関する Cisco VXI ネットワーク セキュリティ要件は、既存のキャンパス環境の場合とまったく同じです。この展開の詳細については、http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/Safe-RG/SAFE_rg.pdf にある『Cisco SAFE Reference Guide』の第 8 章を参照してください。

データセンター セキュリティ

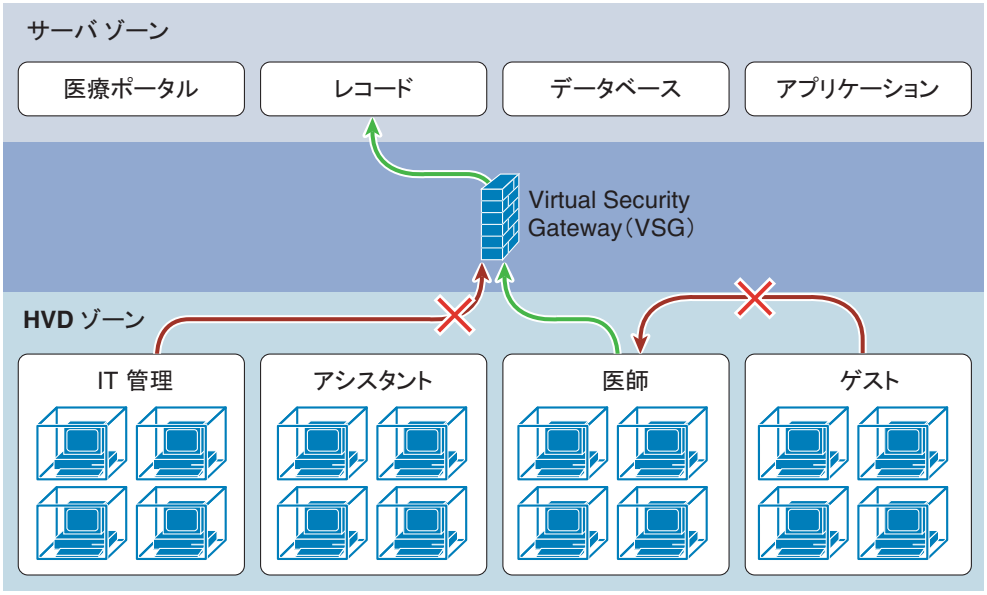
Cisco VXI ネットワークおよびアクセス セキュリティは、ユーザがデータセンター セキュリティ内の仮想デスクトップに安全に「アクセス」できるようにします。ただし、Cisco VXI データセンターの保護に関しては、設計上さらに考慮すべきことがあります。データセンターのセキュリティに関して考慮すべき重要な事柄は、次のとおりです。

- 仮想アクセス ネットワークへの仮想デスクトップ アクセスの保護
- 仮想デスクトップ間での不要なアクセスの制御
- 仮想デスクトップとアプリケーション サーバ間の不要なアクセスの制御
- 電子メールと Web セキュリティの実行
- 仮想デスクトップ密度に影響を与えないウイルス スキャン ソリューションの実装

一般に、コンピューティング デバイス（デスクトップ PC など）の認証は、ネットワーク内のアクセス レベルで行われるものと考えらえます。Cisco VXI システムでは、データセンター内にもアクセス レベルが存在します。大規模なサーバ ファームで仮想マシンを展開するということは、物理的な接続だけでなく、仮想的な接続の監視も重要であることを意味します。つまり、DV 環境に配置された仮想スイッチ内では、そのスイッチが別のネットワーク内の物理スイッチであるかのように、モニタリングを開始する必要があります。仮想デスクトップ アドレスは動的である可能性があり、データセンターの保護されたインフラストラクチャの外側にあるデスクトップ デバイスと同じレベルのサーベイランスが必要です。このスプーフィングに対する脆弱性を考慮したうえで、仮想マシンの領域にインテリジェントなレイヤ 2 仮想スイッチを実装することが推奨されます。ポート セキュリティ、DHCP スヌーピング、ダイナミック ARP インスペクション、および IP ソース ガードの保障措置を使用する機能を搭載した Cisco Nexus® 1000V シリーズ仮想スイッチを展開できます。前述したとおり、これは最初にポートに関連付けられたマシンが不正なマシンに置き換えられていないことを検証する方法として、最も効果的です。Cisco VXI システムにこれらの機能を導入する方法については、この章の後半で取り上げます。一般的な設定および導入ガイドラインについては、http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/security/configuration/guide/n1000v_security.html を参照してください。

Cisco VXI 環境では、同じデータセンター内に多数の仮想デスクトップが存在しています。多くの場合、これらの仮想デスクトップは、分散仮想スイッチを使用して複数のサーバを統合している同一の VLAN に接続します。このような環境では、仮想デスクトップとの間でやり取りされるトラフィックを互いに、あるいは既存の重要なデータセンター リソースから分離して制御する必要があります。さらに、すべての分離とアクセス制御は、トラフィックのソースに近い場所、できれば vNIC レベルで行う必要があります。これは、トラフィック制御機能を最大限に高めるため、さらには、トラフィックがインスペクションのために物理ファイアウォールへ送信されて、ネットワーク帯域幅が非効率的に使用されるのを防ぐためです。仮想デスクトップが格納された VM は、さまざまな理由でデータセンター内を移動します。こうした VM の移動は、ユーザ エクスペリエンスの観点からシームレスでなければなりませんが、ネットワーク セキュリティの面から見ても同じく重要です。Cisco VXI 環境では、vNIC レベルで適用されたセキュリティ ポリシーが VM とともに移動するよう、アトミックな移行が求められます。これらの重要なセキュリティ要件をすべて満たすには、VM のアトミックな移動を自動的に処理できる、仮想ゾーン ベースのファイアウォールが必要です。Cisco VXI では、Cisco Virtual Security Gateway を導入することで、最も効果的にファイアウォールを配置できます。この仮想ファイアウォールは、Nexus 1000v 分散仮想スイッチと緊密に統合され、あらゆる重要なセキュリティ機能を提供します。さらに、このような多階層の仮想環境では、サーバ管理者、ネットワーク管理者、およびセキュリティ管理者の管理境界があいまいになりますが、VSG と Nexus 1000V を組み合わせることで、これらの境界を明確にできます。VSG は、セキュリティ ポリシーを定義して、ネットワーク属性、VM 属性、またはカスタム属性に基づいたデスクトップ ゾーンとアクセス ルールを作成するために使用されます。その後、これらのセキュリティ ポリシーは、個々の Nexus 1000v ポート プロファイルに適用されます。Nexus 1000v ポート プロファイルはハイパーバイザで公開され、仮想デスクトップを格納した VM が接続されます。こうした階層化によって VM のアトミックな移動が可能になり、明確な管理境界も維持できます。

図 95　　Virtual Security Gateway（VSG）



上の図 95 に、医療関係の設定例における VSG ゾーン分割を示します。病院データセンターの仮想デスクトップは、共通属性（VMware または Network）を使用して、VSG によってさまざまなゾーンに配置されます。論理ゾーンは「医師」、「アシスタント（看護師）」、「ゲスト（患者）」、および病院の「IT 管理」です。この図で示すように、アプリケーション サーバも、機能とデータの重要度に基づき、VSG を使用して同様にゾーン分割されます。ゾーンが定義されたら、これらの事前定義されたゾーンを使用してセキュリティ ポリシーを定義できます。Nexus 1000v のセキュリティ プロファイルをポート プロファイルにバインドすると、セキュリティ ポリシーが適用されます。HVD で発信または着信されるすべてのトラフィックは、ポリシー評価の対象となります。

この例では、ゾーン分割ポリシーによって、ゾーン間およびゾーン内のすべてのトラフィックはブロックされます。たとえば図 95 の赤い矢印で示すように、「ゲスト」ゾーンの HVD は「医師」ゾーンの HVD にアクセスできません。さらに、「医師」ゾーンの 2 つの HVD は、明示的に許可されない限り、デフォルトでは相互に通信できません。「医師」ゾーンの一部の仮想デスクトップは、患者記録にアクセスする必要があります。図 95 の緑色の矢印で示すように、この場合は「医師」ゾーンから「レコード」ゾーンへのアクセスのみが許可されます。「IT 管理」または「ゲスト」の HVD から患者記録へのアクセスはブロックされます。VSG は、Nexus 1000v の vPath を使用してポリシーを実装します。これにより、仮想スイッチ上でポリシーの適用が可能になります。すべてのトラフィックを VSG に送信する必要はないため、パフォーマンスも向上します。セキュリティ面で推奨されるベスト プラクティスは、アクセス ポリシーをソースに最も近い場所、できればトラフィック フローのインラインで適用することであり、VSG ではまさにこの方法が実施されています。上記の例では、Nexus 1000v を管理しているネットワーク管理者は接続が正しく行われていることを確認し、サーバ管理者は VM が適切な仮想ネットワークに割り当てられていることを確認するだけですみます。両管理者は、ゾーン分割とポリシーを意識する必要はありません。これらはセキュリティ管理者が単独で、VSG を使用して管理します。

Cisco VXI 固有のゾーン分割に関する推奨事項とベスト プラクティスについては、この章の後半で取り上げます。VSG アーキテクチャと導入モデルの詳細については、https://www.myciscocommunity.com/servlet/JiveServlet/previewBody/20605-102-2-35558/Virtual_Security_Gateway_Deployment_Guide_-_v_2.9.pdf;jsessionid=05FA56FD50FAA7DB50BC995B1B397D87.node0/ を参照してください。

ユーザは各自の仮想デスクトップを使用し、ネットワークまたはインターネット内のセキュアでない領域にアクセスするので、アンチウイルス保護は引き続き必要です。従来のアンチウイルスまたはアンチマルウェア ソフトウェアは、高密度の仮想デスクトップ環境で使用するには拡張性に欠けます。アクセス スキャン、スケジュールされたディスク スキャン、ブートアップ スキャンなどで行われるでウイルス定義の更新は、メモリ、コンピューティング、および I/O リソースを大量に消費し、サポート可能な VM の密度に大きく影響します。これは対処すべき非常に重要な問題です。なぜなら、仮想デスクトップ環境全体の実現可能性は、高密度を実現しながらセキュアな仮想デスクトップ環境を維持できるかどうかに左右されるからです。一般的な環境では、大半の仮想デスクトップが同じオペレーティング システムと同種のアプリケーション セットを実行しているため、保護が必要な基本ファイル システムは非常によく似ている可能性があります。McAfee Optimized Virtual Environments Antivirus for VDI（MOVE-AV for VDI）などの中央集中型アンチウイルス ソリューションでは、この特性を利用して、拡張可能なウイルス保護製品が提供されています。高度に最適化された専用のウイルス スキャン サーバ クラスタが、リソースを大量に消費する仮想デスクトップ ファイル スキャンを実行することで、実現可能な VM 密度は大幅に増加します。基本的な考え方は、スキャンする必要がある新規ファイルを中央のウイルス スキャン サーバへ送信し、サーバはそのファイルが他の仮想デスクトップの要求によって以前にスキャンされていない場合のみスキャンを実行する、というものです。

MacAfee MOVE-AV では、次ののコンポーネントがインストールされて動作し、運用と管理が行われている必要があります。

ePolicy Orchestrator サーバおよびリポジトリ：クライアント ソフトウェアのインストール、新しいポリシーの適用、クライアント アクティビティの監視、レポートの作成、コンテンツおよびクライアント アップデートの保存および送信を行う管理ツール。このアプローチは、大規模な導入を可能にする単独の管理ソリューションです。ePolicy Orchestrator は、ePolicy Orchestrator エージェントを介して MOVE-AV クライアントと定期的にポリシー情報をやり取りします。MOVE-AV クライアントは、ポリシーの適用、イベント情報の収集、ePolicy Orchestrator への情報の返信を行います。

ePolicy Orchestrator Agent（CMA Agent）：クライアント コンピュータにインストールされ、MOVE-AV Agent クライアントと ePolicy Orchestrator コンソールおよびデータベースとの間を仲介する役割を果すサーバ エージェント。ePolicy Orchestrator サーバからクライアントへ、またはその逆方向にデータを送信します。

MOVE-AV Server：このサーバは、Virus Scan Enterprise（VSE）をホストする専用 VM マシンです。エンドポイントの仮想マシンからのオンアクセス ウイルス スキャン要求は、すべてこのコンポーネントで処理されます。

MOVE-AV Agent for Windows：VSE オンアクセス ウイルス スキャンを MOVE-AV Server へオフロードするコンポーネント。このエージェントは、Windows ベースの HVD にインストールされ、スキャン対象のファイルをポリシーに基づいて MOVE-AV へ送信します。

次のリンクにある MOVE-AV 製品ガイドで各コンポーネントが詳細に説明されています。https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/22000/PD22832/en_US/MOVE-AV-VDI_PG.pdf 導入に関する主なベスト プラクティスについては、この章の後半で取り上げます。Cisco VXI 用アンチウイルス スキャン システムを設計する場合は、ウイルス スキャン サーバ専用のサーバ リソースを割り当て、できればこれらのサーバを仮想デスクトップと同じクラスタ内に配置することをお勧めします。

Cisco VXI セキュリティ コンポーネントの導入と設定のベスト プラクティス

ACS と連携した AnyConnect 3.0、Dot1x、MacSec、および MAB

AnyConnect 3.0 は、VPN での Cisco VXI エンドポイントの配置を 3 種類のモードでサポートします。SSL VPN トンネル モード、SSL VPN クライアントレス モード、および IPSec IKEv2 を使用する VPN トンネル モードがあります。さらに AnyConnect 3.0 では、Scan Safe 用 Web セキュリティ モジュールと Dot1X 対応のネットワーク アクセス モジュールをインストールして、デバイス認証および MacSec を有効にすることができます。Cisco VXI では、エンドポイントでサポートされている場合は、常に SSL VPN トンネル モードを使用することをお勧めします。エンドポイントがシン クライアントであり、AC 3.0 のインストールには対応していないがブラウザをサポートしている場合は、SSL VPN クライアントレス モードを使用してください。Web セキュリティ モジュールは、インストールされた AC 3.0 クライアントでのみ、オプションとして使用できます。このモジュールを使用すると、VPN トンネルではなくパブリック クラウド内の Scan Safe サーバを経由する、インターネットにバインドされたすべてのトラフィックをエンドポイントで代行受信できます。ScanSafe では、悪意あるサイトの遮断、企業のインターネット アクセス ポリシーの適用、Google など人気のある検索エンジンでの Search Ahead の実行が可能です。AC 3.0 は Web インターフェイスを介して導入でき、これによってポリシーおよびソフトウェア配布を容易に管理できるようになります。AnyConnect の基本的な導入には、ASA インフラストラクチャと、プロファイル マネージャを使用した AnyConnect 用 ASA でのアクセスおよびルーティング ポリシーの設定が必要です。Cisco VXI では、Dot1X を使用してエンドポイントを認証する AAA サーバとして ACS 5.2 を使用し、Dot1x サポートを有効にした状態で 3000 または 4000 アクセス スイッチを使用する必要があります。上記のインフラストラクチャを作成する詳細な手順とスクリーンショットは、次のリンクにあります。
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/administration/guide/anyconnectadmin30.html

http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/feature/guide/anyconnect30features.html

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htwebvpn.html#wp1053858/

AnyConnect Client SSLVPN の設定は、DTLS に対応している必要があります。これは、遅延の影響を受けやすいトラフィック（音声やビデオ）に最適な転送プロトコルです。AnyConnect Client は、トンネルが確立されると、必要に応じて仮想デスクトップ クライアントが自動的に起動されるように設定する必要があります。

Dot1X 認証サポートでは、エンドポイントにインストールされた dot1x サプリカント、EAPOL メッセージを取り込んで処理できるアクセス スイッチ、および、ACS 5.2 サーバへの認証要求をリレーする機能が必要です。クライアントが Dot1x サプリカントをサポートしていない場合、アクセス スイッチの dot1x 設定のコンテキストで Mac Address Bypass（MAB）を有効にする必要があります。Cisco VXI の検証では、デバイスのポートの dot1x timeout tx-period を調整すると、複数のシン クライアントで DHCP 情報の取得に対する MAB 応答時間を改善できることが確認されました。

MACsec は、基本的には有線ネットワークで MAC レイヤを暗号化します。802.1x Extensible Authentication Protocol（EAP; 拡張認証プロトコル）フレームワークを使用して認証が正常に行われた後、MKA と MACsec が実装されます。ユーザ、従業員、契約業者、およびゲストが LAN に接続する混成グループでは、セキュアなアクセスが必要であることは明らかです。MAC レイヤの暗号化により、なりすまし、機密保持、データ改ざんを含むセキュリティ リスクの数は大幅に減少します。

現在、リンク レイヤの MacSec をサポートしているのは Catalyst 3000-X シリーズだけですが、今後は多くの Cisco スイッチが MacSec をサポートする予定です。MacSec を有効にするための要件は、Dot1x および MacSec サプリカント（ネイティブ サポートがない場合は Anyconnect 3.0 を使用可能）、ACS 5.2 RADIUS Server を使用した Dot1x 認証、および、第 1 ホップ スイッチでの MacSec サポートです。下記に示すガイドラインのほか、次のリンクでも詳細情報を入手できます。

http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/trustsec.html

http://www.cisco.com/en/US/docs/switches/lan/catalyst3750x_3560x/software/release/12.2_53_se/configuration/guide/sw8021x.html

（注） MACSec は有線メディアでのみサポートされます。

次のリンクの『Cisco Virtualization Experience Infrastructure Configuration Guide』の手順説明を使用して、AnyConnect、Dot1x、ACS5.2、および MacSec をセットアップする必要があります。

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VXI/configuration/VXI_Config_Guide.pdf

エンドポイントのサポート

次の表に、Cisco VXI システムでサポートされる各種エンドポイントと、対応する VPN およびデバイス認証方式を示します。

表 27　　Cisco VXI システムでサポートされるエンドポイント

エンドポイント	VPN およびデバイス認証	特に考慮すべき事項
シック クライアント（Win7 および XP）	SSL VPN（トンネル モード）用 AC 3.0、認証用 Dot1X	アクセス時の Catalyst 3000 または 4000 スイッチ。 AC 3.0 のインストールに関する推奨事項については、下記の「注」を参照。
Cisco VXC（2112、2212）：ICA クライアント	802.1x をネイティブでサポート	アクセス時の Catalyst 3000 または 4000 スイッチ。
Apple iPad	AnyConnect 2.5	App Store から入手可能。
Linux および MacOS シック クライアント	AnyConnect 3.0、SSL VPN リモート アクセス専用	このモードをサポートする ASA プロファイルが必要。 AC 3.0 のインストールに関する推奨事項については、下記の「注」を参照。
Windows Mobile プラットフォーム	AnyConnect 3.0、SSL VPN リモート アクセス専用	このモードをサポートする ASA プロファイルが必要。 AC 3.0 のインストールに関する推奨事項については、下記の「注」を参照。
AnyConnect 3.0 はロードできないが、dot1x をネイティブ サポートしているシン クライアント	ASA への SSL VPN クライアントレス リモート アクセス	このカテゴリのエンドポイント：Wyse ThinOS クライアント
Dot1x および AnyConnect を使用しないシン/ゼロ クライアント	ポート認証用 MAC Authentication Bypass（MAB; MAC 認証バイパス）	アクセス用 Catalyst 3000 または 4000 スイッチ

（注） 管理者は、下記のリンクの CCO から AnyConnect 3.0 をダウンロードできます。AnyConnect 3.0 を自身の ASA にアップロードしたら、それをエンドポイントにダウンロードできます。これは推奨されるオプションです。あるいは、既存のソフトウェア配布メカニズムによって配布される MSI パッケージを使用して、AC 3.0 をエンドポイントに配置することもできます。
http://www.cisco.com/cisco/software/release.html?mdfid=283000185&flowid=17001&softwareid=282364313&release=3.0.0629&rellifecycle=&relind=AVAILABLE&reltype=latest/

DMVPN

Cisco VXI は、複数のブランチ/キャンパス間 VPN オプションをサポートします。DMVPN は、QoS との統合を公式にサポートしている唯一の IPSec サイト間ソリューションです。すべてのブランチ ユーザの音声およびビデオ トラフィックを最適化するには、WAAS と QoS を各ブランチに設定する必要があります。

Cisco VXI システムで DMVPN をセットアップするには、ヘッドエンドに ASR ルータ、ブランチに ISR G2 ルータのサポート対象バージョンが配置されている必要があります。

DMVPN 導入の詳細については、「ネットワーク」のセクションを参照してください。DMVPN の設定には、Cisco Security Manager（CSM）を使用します。次のリンクにあるドキュメントも参照してください。http://www.cisco.com/en/US/products/ps6658/index.html

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a008075ea98.pdf

N1K

N1K は、高度なセキュリティ機能の中枢であり、Cisco Virtual Security Gateway を導入するための必須コンポーネントです。Cisco VXI 環境で N1K を設計および設定するためのガイドラインについては、この設計ガイドの「データセンター」の章で説明しています。VM からのトラフィックが仮想環境で正常に切り替わったら、N1K セキュリティ機能をオンにします。Cisco VXI 環境をセキュリティで保護するために、ポート セキュリティ、DHCP スヌーピング、ダイナミック ARP インスペクション、および IP ソース ガード機能を有効にしておく必要があります。これらの各機能の設定については、http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/security/configuration/guide/n1000v_security.html の『N1K Security configuration guide』を参照してください。一般的な N1K 導入ガイドは、http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9902/guide_c07-556626.html にあります。

ベスト プラクティス

- ポート セキュリティ：この機能は、制限された一連の MAC アドレスからのインバウンド レイヤ 2 アクセスを制限するために使用されます。この機能により、同じ VLAN 内で 1 つのポートから 1 つの MAC アドレスのみが許可されます。Cisco VXI システムでは、ポートのセキュリティを確保するために、スティッキ MAC アドレス ラーニング方式を有効にしておくことをお勧めします。これにより、仮想デスクトップが新規作成された場合、VM のライフサイクル中にその MAC アドレスが学習されます。さらに、可能な場合は、すべての同種の VM を同じ VLAN の 1 つのクラスタ内に配置することをお勧めします。N1K のすべての VEth ポートでは、ポート セキュリティがデフォルトで有効になっています。
- DHCP スヌーピング：このセキュリティ機能は、DHCP サーバと IP リソースが侵害されないよう、各ポートで DHCP メッセージを学習およびフィルタリングします。デフォルトでは、すべての VEth ポートは信頼されていない状態です。Cisco VXI 環境では、このデフォルト設定を変更しないでください。VEM と同じハイパーバイザに N1K 用の VSM がインストールされている場合は、その VSM ポートを信頼できるポートとして設定する必要があります。これは、前述の推奨事項における唯一の例外です。

- ダイナミック ARP インスペクション：これは、Cisco VXI 環境で強く推奨されるセキュリティ機能です。特に、侵害された仮想マシンからの 1 度の ARP スプーフィング攻撃によって、どれだけの数の仮想デスクトップが影響を受けるかを考えると、この機能が大いに推奨されます。この ARP インスペクションが機能するには、DHCP スヌーピングが必要です。ARP インスペクションを有効にする前に、信頼できるアップリンク ポートとポートチャネルを慎重に特定しなければなりません。ARP インスペクションを有効にしたら、すべてのアップリンク ポートを信頼できるモードにする必要があります。DHCP スヌーピングの場合と同様に、すべてのホスト VEth ポートは必ず信頼されていない状態にしておく必要があります。N1K に Virtual Service Domain（VSD; 仮想サービス ドメイン）を作成し、すべてのアップリンクおよびポートチャネルをその VSD 内に配置して、ポートの状態（信頼できる）が Cisco VXI の導入全体で一貫して適用されるようにしておくことをお勧めします。
- IP ソース ガード：この機能を使用すると、IP アドレスおよび MAC が DHCP スヌーピングのバインディングと一致しない IP トラフィックをすべてフィルタリングできます。この機能を有効にすると、N1K のすべての信頼できるポートで IP トラフィックのフィルタリングを開始できます。この機能を実行するには、DHCP スヌーピングが必要です。ポートを初めて起動するとき、IP トラフィックが許可されるまでに数秒かかる場合があります。これは、最初の手順で DHCP バインディングを作成するために必要な時間です。

VSG

Cisco VXI システムで VSG を正常にセットアップするために必要なコンポーネントは、二重化冗長 VSG VM、管理用 VNMC、および N1K です。設定に関する詳細なドキュメントと、最新バージョンの互換性など導入の注意点については、次のリンクを参照してください。
http://savbu.cisco.com/index.php/nexus-1000v-homepage/n1kv-sales/n1kv-sales-files/1001-nexus-1000v-virtual-security-gateway/

最新リリースの VSG では、Nexus 1000V 分散仮想スイッチのバージョン 1.4 が必要です。Nexus 1000V と VSG は、XenServer または Hyper-V 環境ではサポートされません。VSG は、Nexus OS CLI 経由ではなく Virtual Network Management Center（VNMC）によってのみ管理されます。

Nexus 1000V Virtual Supervisor Module（VSM）には、VM に導入する形式と Nexus 1010 に導入する形式の 2 種類の導入方法があります。現在 Cisco VXI システムでは、VM 上の VSM を使用する VSG のみがサポートされています。VSG VM は、今回の Cisco VXI リリースでは vMotion で移動することができず、サポートされません。VSG は、大規模なクラウドの導入向けに設計されており、マルチテナントをサポートしています。マルチテナント機能は製品でサポートされていますが、今回の Cisco VXI リリースではこの機能のテストは行われていません。さらに、今回のリリースでのみ、VSG HA のアクティブ/スタンバイ モードがサポートされます。外部からゾーン、ゾーンから外部、およびゾーン内でのアクセスは、デフォルトによりすべてブロックされます。

ベスト プラクティス

ゾーンはネットワークまたは VM 属性を使用して作成されます。推奨される名前は vm.portprofile-name です。これにより、N1K ポート プロファイルとの同期において、ロックダウンの効果を最大限に高めることができます。信頼できるゾーンは他の属性を使用して作成することもでき、Cisco VXI で検証済みです。ただし、VM の命名規則には十分注意し、命名規則の不整合によって意図しない VM のアクセスが許可されないようにしてください。さらに VM の命名規則は、通常はセキュリティ管理者の管轄外であるため、VM 名ベースの属性は Cisco VXI 環境での制御機能を低下させます。

Cisco VXI 固有のポリシーに関する推奨事項：仮想デスクトップ ゾーンのポリシーを作成する場合、最小限必要な後続の通信に VSG ファイアウォールの通過を許可する必要があります。

- 特定のディスプレイ プロトコルを介したエンドポイントから VM への接続
- VM から AD、vCenter、DNS、NetBios、および DHCP サーバへの通信（これらすべてのインフラストラクチャ サービスに対応するオブジェクト グループを作成することが推奨される）

- VM から仮想デスクトップ ブローカへの通信
- VM からインターネットへの通信（エンタープライズ インターネット ポリシーに合わせて対応）
- VM からアプリケーション サーバへの通信（Cisco VXI システム外部のアプリケーション サーバに対応するオブジェクト グループを作成することが推奨される）
- VM から UC コンポーネントへの通信（音声の場合は VM から VM、プレゼンスおよび UC 制御トラフィックの場合は VM から Unified CM および Cisco Unified Presence）

ゾーン内または異なるゾーンで HVD が他の HDV と直接通信しようとすると、デフォルトによりブロックされますが、ログも作成しておく必要があります。それには、記録可能で明示的な any-any 拒否ポリシーを作成します。VSG では、暗黙的ポリシーに関するログの作成はできません。制御機能を高め、変更も容易にできるようにするには、vCenter と仮想デスクトップ ブローカを別々のゾーンに配置することをお勧めします。

Cisco VXI HVD、および Cisco Unified Personal Communicator など Cisco VXI 固有のアプリケーションからの基本的な通信を許可するために、VSG ファイアウォールで開いておく必要があるポートを次のリストに示します。

表 28　　ポートのリスト

ポート	用途	適用される VSG ゾーン
67	BootP：UDP	HVD ゾーン：Windows ベースの VM のブートアップ時に必要
137	NetBios Name Service	HVD ゾーン：Windows ベースの VM のブートアップ時に必要
1494	ICA	HVD から外部、HVD からブローカ ゾーン
80	インターネット	HVD ゾーン：エンタープライズ ポリシーにより異なる
5222、526	Cisco Unified Personal Communicator Presence および IM：XMPP	HVD および UC ゾーン
5060、5061	Cisco Unified Personal Communicator 音声 / ビデオ：SIP	HVD および UC ゾーン
143	IMAP：Cisco Unified Personal Communicator 用	HVD および UC ゾーン
389、636	Cisco Unified Personal Communicator	HVD および UC ゾーン
69	Cisco Unified Personal Communicator：Tftp	HVD および UC ゾーン
カスタム	MOVE-AV	McAfee MOVE-AV を導入する場合は、HVD ゾーンから VSE および ePO へのカスタム ポートを開きます。

（注） Cisco VSG と Cisco vWAAS は、いずれも仮想アプライアンスであり、動作するには N1K DVS を必要とします。これらの仮想アプライアンスは、N1K でトラフィックを代行受信する必要があります。今回の CVD では、同時に両方のアプライアンスはサポートされませんが、今後サポートされる予定です。データセンターに VSG がインストールされている場合、対応策として WAAS アプライアンスを使用できます。データセンターの WAAS アプライアンスは、通常はデータセンターのエッジでトラフィックを代行受信します。データセンターに vWAAS がインストールされている場合は、Cisco ASA を使用して HVD トラフィックをセグメント化し、ファイアウォールを適用することを強くお勧めします。

Cisco VXI のアンチウイルス ソリューション

McAfee Optimized Virtual Environments Anti-Virus（MOVE-AV）

Cisco VXI 用アンチウイルス スキャン システムを設計する場合は、ウイルス スキャン サーバ専用のサーバ リソースを割り当て、できればこれらのサーバを仮想デスクトップと同じクラスタ内に配置することをお勧めします。McAfee 製品で最大限のパフォーマンスを実現するには、ハイパーバイザごとに 1 つの MOVE AV サーバを配置することをお勧めします。

数百台のサーバが仮想デスクトップをホストするような大規模な展開では、ホスト ハイパーバイザごとに 1 つの MOVE-AV サーバをインストールしない方がよい場合もあります。なぜなら、それぞれの MOVE-AV サーバ インスタンスによって、サーバのコンピューティング リソースの最大 10 % が消費される可能性があるからです。このような場合は、専用ホストに MOVE-AV Server VSE をセットアップすることができます。専用ホストに導入する場合は、MOVE-AV VSE サーバと HVD 間で使用可能なネットワーク帯域幅が十分であることと、ネットワーク遅延がごくわずかであることを確認する必要があります。HVD と MOVE-AV サーバの間に Cisco ASA などの物理ファイアウォールまたは Cisco VSG などの仮想ファイアウォールがある場合、そのファイアウォールで適切なポートが開いている必要があります。インストール時に変更されない限り、MOVE-AV VSE サーバのデフォルトの TCP ポートは 9053 です。

企業の仮想デスクトップ導入戦略に応じて、2 通りの導入シナリオが考えられます。これらのシナリオは、主として HVD のゴールデン イメージと MOVE-AV が仮想デスクトップのクラスタ間でどのように共有されているかによって区別されます。各クラスタには少なくとも 1 つの専用 MOVE-AV Server VSE があるので、2 つの導入シナリオの基本的な目標は次のようになります。

- 個々の HVD がどのマスター イメージを使用して作成されたかにかかわらず、クラスタ内のすべての HVD が正しい MOVE-AV VSE サーバの IP アドレスに到達可能であること。
- ゴールデン イメージがクラスタ間で共有されている場合でも、ePO に正しいポリシーが設定されていること。

2 つのシナリオについては、次の参照リンクで詳細に説明されています。各自の仮想デスクトップ導入戦略に適したシナリオを選択してください。

https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/23000/PD23046/en_US/MOVE-AV-VDI-DG.pdf

上記の導入ガイドラインの範囲外では、MOVE-AV コンポーネントのインストールと基本的な仮想インフラストラクチャとは無関係です。インストールの詳細な説明は、次の参照リンクで確認できます。
https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/22000/PD22831/en_US/MOVE-AV-VDI_IG.pdf

MOVE-AV の拡張ガイドラインについては、「パフォーマンスとキャパシティ」の章で説明します。

関連情報

表 29 に、この章で説明したハードウェアおよびソフトウェアを含む特定のベンダー情報の詳細を示します。

表 29　　セキュリティ関連のリンク

Cisco SAFE アーキテクチャ ガイド http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.pdf
Cisco Data Center 3.0 セキュリティ ガイド http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_3_0/dc_sec_design.pdf
Cisco Identity-Based Network セキュリティ ガイド http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/CiscoIBNS-Technical-Review.pdf
Cisco 3560 コマンド リファレンス ガイド http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_35_se/command/reference/cli1.html#wp2757193
『Cisco Business Ready Teleworker Design Guide』 http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a008074f24a.pdf
『Cisco ASA 8.x : VPN Access with the AnyConnect VPN Client Configuration Example』 http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00808efbd2.shtml
Citrix :『How to Disable USB Drive Redirection』 http://support.citrix.com/article/CTX123700
Microsoft :「Disabling Remote Desktop Services Features」 http://msdn.microsoft.com/en-us/library/aa380804%28VS.85%29.aspx

Quality of Service

Cisco® Virtual Experience Infrastructure（Cisco VXI; シスコ仮想化エクスペリエンス インフラストラクチャ）システムの Quality of Service（QoS）は、配信ネットワーク内だけでなく、データセンターでも同様に必要とされます。キャンパス ネットワークと WAN ネットワークでは、データおよびデスクトップ アプリケーションへのアクセス速度を、ユーザがラップトップおよびデスクトップ システムに対して期待している値で維持するために、QoS が使用されます。Cisco VXI データセンターには QoS が必要です。デスクトップ アプリケーションをデータセンター内に移動すると、そのアプリケーションは多数のアプリケーション サーバがアクセスしているのと同じ LAN に配置されます。それ以降、デスクトップからアプリケーション サーバへのトラフィックは、WAN を経由しなくなります。ただし、サービス ポリシーと優先順序付けは、大規模ネットワークを経由するときに適用されるものと同じにする必要があります。

Cisco VXI システムの QoS には特有の課題があります。特に、関連するプロトコルはシステム独自のもので、場合によっては暗号化されています。多くの場合、デスクトップに表示されているアプリケーションを区別することはできません。これは、それらすべてのアプリケーションがデスクトップ仮想化ディスプレイ プロトコルにカプセル化されているためです。トラフィック（ビデオなど）は別のチャネルに送られますが、それでもこれは Cisco 独自の実装であり、通常の QoS では処理できません。したがって、以前はアプリケーション固有のマーキング、トラフィックのタイプ、またはプロトコルそのものに基づいてデータを最適化できたネットワーク デバイスが、今後はそれと同等レベルの粒度を使用できなくなります。ここに記載されている情報を利用して、表示可能なトラフィックを改善できます。

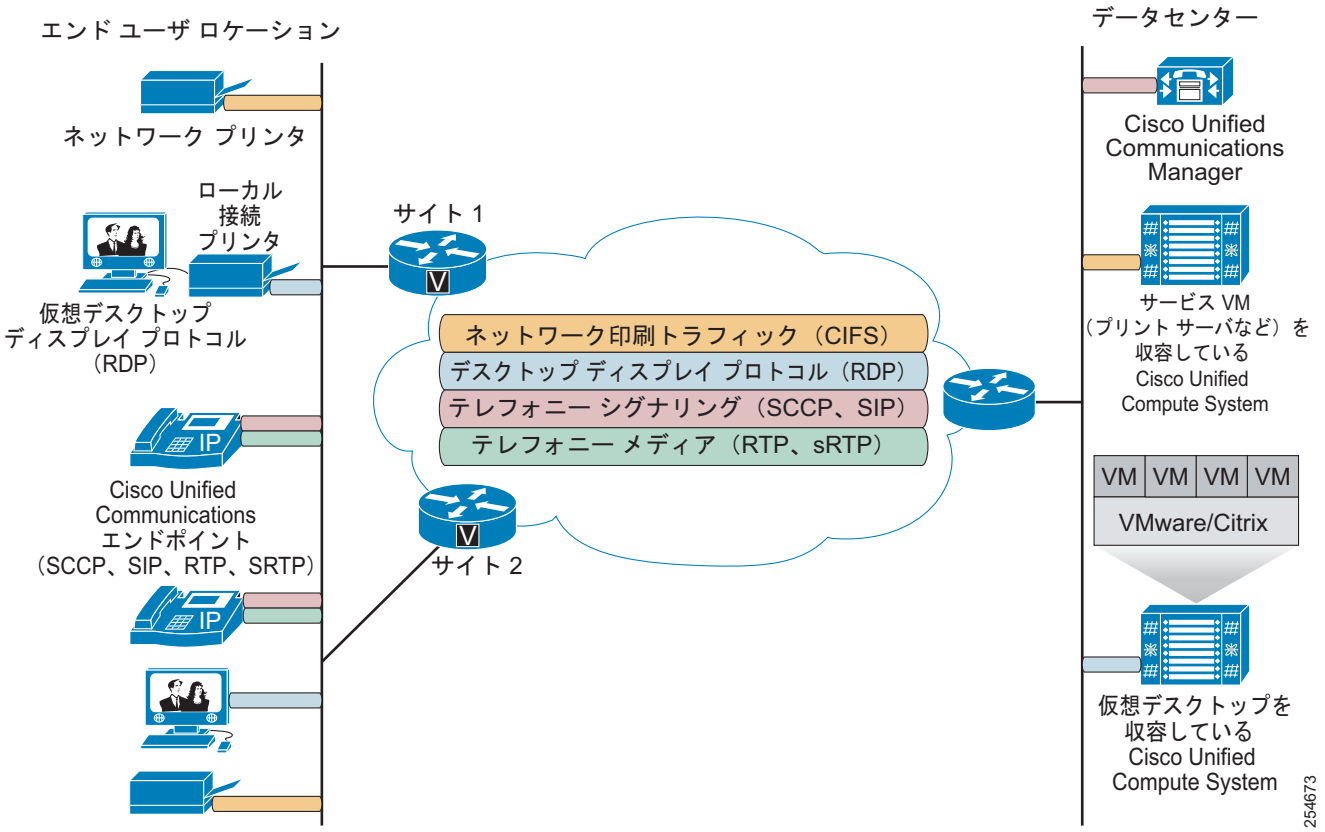
QoS マーキングの表

このセクションでは、さまざまなプロトコルについて、識別方法、Differentiated Services Code Point（DSCP; 差別化サービス コード ポイント）値の設定、およびネットワークにおけるデータ処理の最適な設定も含めて説明します。表 30 に一般的な Cisco VXI システムのプロトコルを示します。

表 30　Cisco VXI 関連プロトコルの QoS マーキング

プロトコル	TCP/UDP ポート	DSC/CoS 値
デスクトップ仮想化プロトコル		
Remote Desktop Protocol Version 7	TCP 3389	DSCP af21 および CoS2
Independent Computing Architecture（ICA） セッション セッションの信頼性 Web サービス	 TCP 1494 TCP 2598 TCP 80	 DSCP af21 および CoS2 DSCP af21 および CoS2 DSCP af21 および CoS2
USB リダイレクト（PCoIP）	TCP 32111	DSCP af11 および CoS 1
マルチメディア リダイレクト（MMR）	TCP 9427	DSCP af31 および CoS 4
Cisco VXI で使用されるその他のプロトコル		
ネットワークベースの印刷（CIFS）	TCP 445	DSCP af11 および CoS 1
ユニファイドコミュニケーション シグナリング（Skinny Client Control Protocol） ユニファイドコミュニケーション シグナリング信号（Session Initiation Protocol） ユニファイドコミュニケーション シグナリング信号（CTI）	TCP 2000 TCP 5060 TCP 2748	DSCP cs3 および CoS 3 DSCP cs3 および CoS 3 DSCP cs3 および CoS 3
ユニファイドコミュニケーション シグナリング メディア（RTP、sRTP）	UDP 16384 ～ 32767	DSCP ef および CoS 5
*PCoIP に使用するポートは、将来的には 50002 から 4172 へ移行されます。		

図 96　　Cisco VXI ネットワークのプロトコル概要



データセンター

データセンターでの分類とマーキングは、できる限りアプリケーション サーバと仮想デスクトップに近い場所で行う必要があります。その後、適切な QoS ポリシーとキューイング優先順位が設定されていることを前提に、これらのマーキングは維持され、トラフィックがネットワークで正しく処理されます。

マーキング

多くのアプリケーションでは、トラフィックが DSCP 値でマークされません。たとえマークされたとしても、そのマーキングは各企業の優先順位付けに適していない場合があります。このため、分類はソフトウェアベースではなく、（Cisco Catalyst® または Cisco Nexus® ファミリ スイッチを使用して）ハードウェアベースで行う必要があります。テストでは、可能な場合は必ず Cisco Nexus 1000V スイッチでマーキングを実装しました。入力した DSCP 値と対応するポートは、表 30 に基づいています。詳細と例については、次のリンクの『Cisco Virtualization Experience Infrastructure Configuration Guide』を参照してください。

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VXI/configuration/VXI_Config_Guide.pdf

Cisco Unified Computing System のパフォーマンスを最適化するためのキューイング

データセンター外部のネットワークを通過するトラフィックのマーキングに加えて、データセンター内部のデバイスを通過する別のトラフィックをマークする必要が生じる場合があります。たとえば、デスクトップでサービスを提供するデスクトップ仮想化トラフィックによって、Cisco Unified Computing System™ のストレージ リソースが枯渇することがないようにしなければなりません。Cisco Unified Computing System には、他のデータセンター エンティティ（ストレージなど）のパフォーマンスを高めるために、アウトバウンド パケットをマーキングおよびキューイングする独自の機能が搭載されています。Cisco Unified Computing System 固有のアクティビティに対応したキューイング戦略の詳細と推奨事項については、次のリンクの『Cisco Unified Computing System GUI Configuration Guide』を参照してください。

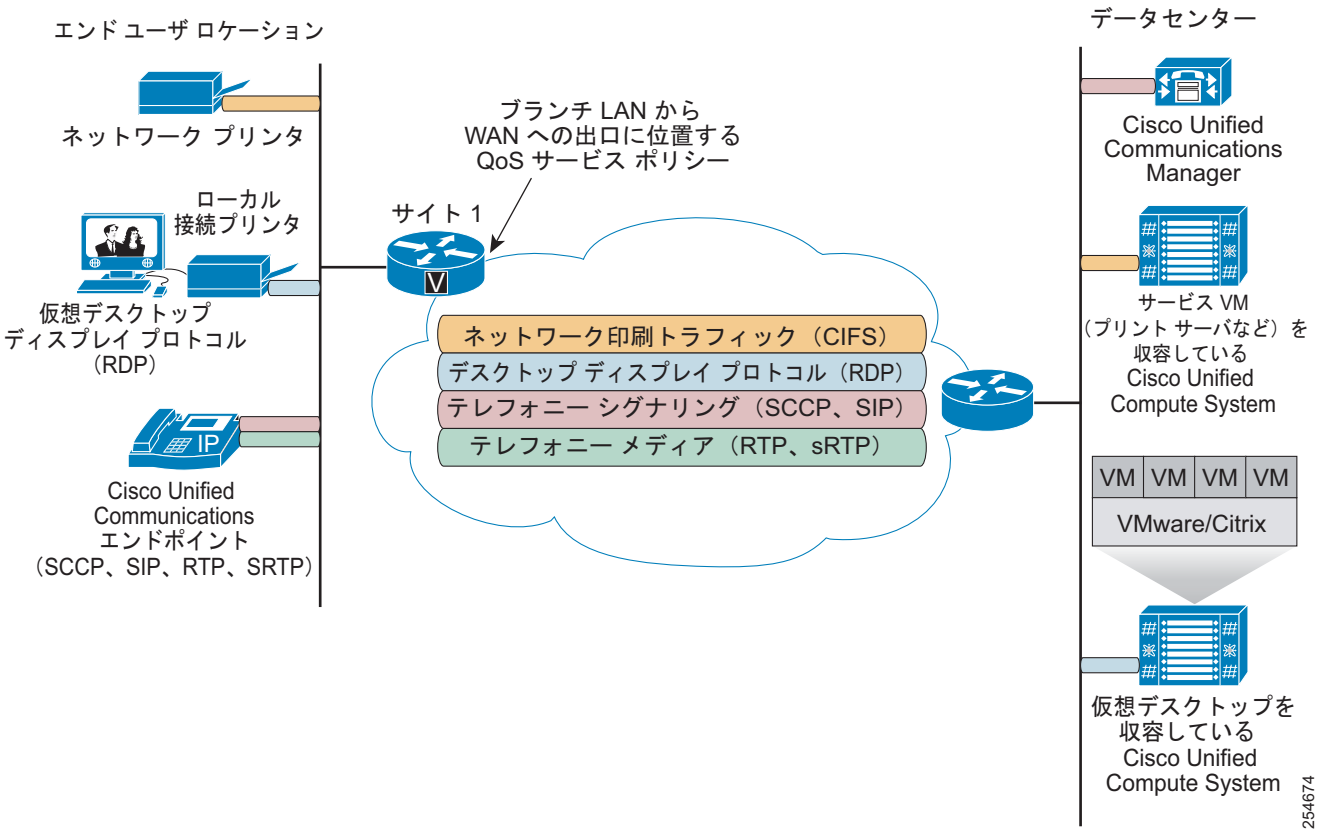
http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/1.3.1/UCSM_GUI_Configuration_Guide_1_3_1.pdf

ネットワーク

QoS に関するネットワーク デバイスの主な責務は、トラフィックを正しいキューにルーティングすることです。このとき、（ブランチ オフィスまたはデータセンターの）ローカル スイッチによって、データがトラフィックのタイプに基づいて適切にマークされていることが前提となります。正しい優先順位が付けられ、DSCP マーキングに基づいてトラフィックが転送されます。ネットワーク内ではリマーキングが実行されますが、エンドポイントの場所とデータセンターで推奨されるリマーキングの設定を適用する場合は、ネットワーク内でさらにリマーキングを行う必要はありません。

キャンパス ネットワークでは、十分な帯域幅があるため、リソースのコンテンションは最小限ですみます。ただし、ブランチ WAN ルータ ネットワークの低速な接続を確認しておく必要があります。たとえば、ブランチ オフィス LAN の高速接続から WAN の低速リンクへの出力ポイントでは、帯域幅のコンテンションが発生する可能性があります。特定のプロトコル専用の帯域幅を制限するサービス ポリシーを定義し、このポイントに適用します。Cisco VXI エンドポイントが集中する場所では、上記と同様のキューイングと帯域幅の設定を適用し、トラフィックの輻輳が発生した場合に適切に対応できるようにしておきます（図 97）。

図 97　　QoS のサービス ポリシーの場所



帯域幅サービス ポリシーの例については、次の URL にある『Cisco Virtualization Experience Infrastructure Configuration Guide』を参照してください。

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VXI/configuration/VXI_Config_Guide.pdf

エンドポイント

Cisco VXI シン クライアント エンドポイントには、通常、セッション トラフィックをマークする機能はありません。したがって、エンドポイントに代わってブランチ オフィスが、データセンター仮想マシンに戻るトラフィックに対し、アウトバウンドのデスクトップ仮想化トラフィックに対してデータセンターの Cisco Nexus1000V で実行されたのと同じマーキングを実行する必要があります。ブランチ スイッチの設定は、次の URL にある『Cisco Virtualization Experience Infrastructure Configuration Guide』に記載されている設定と似ています。

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VXI/configuration/VXI_Config_Guide.pdf

アドミッション制御は、コンテンションを低減するもう一つの方法であり、QoS を適用するために一部のアプリケーションで必要とされます。Voice-over-IP（VoIP）トラフィックは、電話機の制御に Cisco Unified Personal Communicator を使用することで、ディスプレイ プロトコルの外部でサポートされます。このトラフィックが受け付けられると、プライオリティ キューに入力されます。このプライオリティ キューのフラッディングを回避するために、アドミッション制御が必要になります。Cisco Unified Communications Manager は、ロケーションベースと Resource-Reservation Protocol（RSVP; リソース予約プロトコル）ベースの 2 種類のアドミッション制御をサポートします。

ロケーションベースの通信アドミッション制御は、多くの Cisco Unified Communications Manager のインストールで広く導入されていますが、冗長リンクやメッシュ トポロジは使用できません。RSVP ベースのアドミッション制御は、ネットワーク対応型のアドミッション制御システムです。Cisco 2800、2900、3800、および 3900 シリーズ サービス統合型ルータで動作する、RSVP エージェントと呼ばれるプロキシを使用すると、RSVP はさらに堅牢なソリューションとして、Cisco VXI の電話機を制御できます。Cisco Unified Communications Manager での RSVP ベース アドミッション制御の実装については、『Cisco Unified Communications Manager System Guide 8.0』の第 8 章、第 2 部を参照してください。

関連情報

表 31 に、この章で説明したハードウェアおよびソフトウェアを含む特定のベンダー情報の詳細へのリンクを示します。

表 31　　QoS 関連のリンク

『Cisco UCS GUI Configuration Guide』
http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/1.3.1/UCSM_GUI_Configuration_Guide_1_3_1.pdf
『Cisco Unified Communications Manager Systems Guide』
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_0_2/ccmsys/accm.pdf
『Cisco Virtualization Experience Infrastructure Configuration Guide』
http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/VXI/configuration/VXI_Config_Guide.pdf

パフォーマンスとキャパシティ

この章では、キャパシティ プランニングおよびエンドツーエンドの Cisco® Virtualization Experience Infrastructure（Cisco VXI; シスコ仮想化エクスペリエンス インフラストラクチャ）導入に使用するツールと手法について説明します。

エンタープライズ ネットワークにおけるデスクトップ仮想化サービスのパフォーマンスおよびキャパシティ プランニングには、次に示す 3 つの基本的な手順があります。

- 必要なコンピューティングおよびストレージのキャパシティ プランニング
- サービスのサポートに必要なインフラストラクチャ コンポーネントのキャパシティ プランニング
- リモート サイトにサービスを配信するための WAN キャパシティ プランニング

この章に記載されている推奨事項とテスト結果は、ユーザ プロファイルと Cisco VXI 作業負荷が最適化された、エンドツーエンドの Cisco VXI システムで実施されたテストに基づいていることに注意してください。キャパシティ プランニングの際にこの章の情報を参考にすることはできますが、各自の作業負荷と環境を慎重に検討し、自身の導入における必要性に応じて調整する必要があります。さらに、この章は Cisco VXI システムで使用されるすべてのシスコおよびサードパーティ コンポーネントに対応する包括的な指針ではありません。それらのコンポーネントについては、製品マニュアルを直接確認することが最も有効です。

コンピューティングとストレージのキャパシティ プランニング

ユーザを物理デスクトップから仮想デスクトップへ移行する場合、ユーザ ベースとそのリソース要件を CPU、メモリ、およびディスク スペースの観点から十分に把握しておくことが重要です。デスクトップ仮想化に移行する多くの企業は、それを Windows 7 へ移行する機会でもあると考えているため、そうした移行の意味合いを理解することも重要です。

このプロセスにおける重要な手順は、移行するユーザをコンピューティングおよびストレージの必要性に基づいてグループ分けし、キャパシティ プランニングをグループ レベルで実施できるようにすることです。異なるユーザ グループの概算も、個別に行う必要があります。個別に行わない場合、キャパシティが無駄に消費されたり、制限が厳しすぎたりして、結果的にユーザ エクスペリエンスが不十分になることがあります。こうしたグループ分けにより、管理者は同じオペレーティング システム、アプリケーション、使用パターンといった共通要因に基づいて、各ユーザ グループの基本プロファイルを作成できます。基本プロファイルには、CPU、メモリ、帯域幅、ディスク I/O 使用率など、グループの特徴を示すリソース使用率のメトリックも含める必要があります。それには、グループ内で統計的に有意な数のユーザから一定期間データを収集します。その後、基本プロファイルを使用して、仮想化環境のユーザ グループに必要なコンピューティングおよびストレージを概算できます。したがって、リソースの概算とキャパシティ プランニングを全体的に捉えた場合、管理者は移行するユーザ ベース全体ではなく、作業負荷と環境が同じユーザを 1 つのグループにまとめる必要があります。特に、大規模なデスクトップ仮想化の導入では、この点が重要です。

以下のセクションでは、エンドツーエンドの Cisco VXI 導入に必要なコンピューティングおよびストレージのキャパシティ プランニングの手順を詳しく説明します。キャパシティ プランニングの方法の概要は、次のとおりです。

- 物理デスクトップ環境内のユーザの基本プロファイルを作成します。これには、作業負荷プロファイルと、CPU、メモリ、ストレージ、および帯域幅の使用率など、関連するリソース使用率のメトリックが含まれます。
- 必要なコンピューティングおよびストレージに影響する共通要因（作業負荷など）に基づいてユーザをグループ分けします。
- デスクトップ仮想化の対象となるユーザ グループに必要なリソースを概算します。
- 仮想デスクトップ数の観点から、サーバごとのキャパシティを概算します。これには、関連するストレージ キャパシティと、それをサポートするために必要なパフォーマンスが含まれます。この概算では、ピーク時使用率、ログイン ストーム、および停止の影響やサーバのダウンタイムといった要因を考慮する必要があります。
- 製品導入におけるリソース使用率とパフォーマンスを改善するための最適化の手法とベスト プラクティスを評価します。
- リソースの概算値を、その環境で一般的な作業負荷を使用して検証します。
- 単一のサーバ データを基に、より大規模な Cisco VXI 導入で必要とされる全体的なコンピューティングおよびストレージ ハードウェアを推定します。

ユーザ作業負荷プロファイル

キャパシティ プランニングで使用される基本プロファイルには、アプリケーション、そのアプリケーションでのアクティビティ、および、ユーザ グループの特徴を示す使用パターンが含まれている必要があります。基本プロファイルによってグループの作業負荷プロファイルが定義されます。この作業負荷プロファイルを使用して、ユーザ グループを一般的な作業負荷プロファイルのうちのいずれかに分類できます。ベンダーは通常、これらの一般的な作業負荷を使用して、コンピューティング、ストレージ、およびネットワーキングの要件が同じユーザを特定します。ベンチマークに使用する負荷生成ツールによって対応する作業負荷が生成される際、これらの作業負荷プロファイルがパフォーマンスおよびスケーラビリティ データの基準として用いられます。作業負荷の密度は、規模とキャパシティが大幅に異なる要因となり得るので、必要なハードウェア リソースを概算するために使用されるデータにとって非常に重要です。リソース概算値の評価テストを実施する場合にも、作業負荷プロファイルは不可欠です。なぜなら、環境の規模を正確に判断するには、負荷生成ツールで使用される作業負荷プロファイルが、ユーザ グループの作業負荷プロファイルと厳密に一致する必要があるからです。つまり、作業負荷プロファイルは、導入するデスクトップ仮想化システムのキャパシティ全体において非常に重要な役割を果たします。一般的な作業負荷プロファイルについては、この章の「作業負荷の考慮事項」のセクションで詳しく説明します。

現在の環境でのリソース使用率

仮想化環境のリソース要件を概算するうえで重要な要因は、現在の物理デスクトップ環境におけるリソースの使用率です。したがって、仮想デスクトップへの移行対象となるユーザ グループについて、現在の環境を十分に理解し、次のメトリックに基づいてリソース使用率を明確にすることが重要です。

- 平均およびピーク時の CPU 使用率
- 平均およびピーク時のメモリ使用率
- ストレージ
  - 1 ユーザあたりのストレージ キャパシティ
  - I/O Operations Per Second（IOPS; 1 秒あたりの I/O 処理数）
  - スループット（毎秒のバイト数）
- LAN での帯域幅使用率

管理者は、対象となるユーザ グループの使用パターンを監視し、環境内での各グループの平均およびピーク時の使用率を把握する必要があります。監視業務では、シフト制の作業環境でのシフト交代、バックアップのタイミング、ウイルス スキャン、その他の同種のアクティビティなど、1 日の中でユーザがログオンする際に、地理的な位置によって使用パターンが変化する可能性を考慮する必要があります。

平均的な物理デスクトップ ユーザのリソース使用率は、次の方法で求めることができます。

- CPU 使用率：Microsoft Windows Perfmon や Liquidware Labs の Stratusphere などのツールを使用して、移行対象のユーザ グループの物理デスクトップから平均およびピーク時の CPU 使用率データを収集します。このデータは、統計的に有意な数のデスクトップから、作業負荷が大きい間に一定期間収集してください。収集したデータの統計的平均値を使用すると、そのグループのピーク時および平均の CPU 使用率を判断できます。
- メモリ使用率：CPU 使用率の場合と同じまたは同種のツールを使用して、物理デスクトップでのメモリ使用率に関するデータを収集します。CPU の場合と同様、有意な数のデスクトップから一定の期間に収集されたデータを分析し、そのグループの統計的平均値から、ピーク時および平均のメモリ使用率を割り出します。このデータを使用して、仮想化デスクトップを使用する際にグループが必要とするメモリを特定します。

- 物理デスクトップのストレージ キャパシティおよびパフォーマンス（IOPS とスループット）：CPU およびメモリ使用率データの収集に使用したのと同じツールを使用して、物理デスクトップの IOPS とスループットを判断できます。CPU およびメモリ使用率と同じ方法で、グループのピーク時および平均データを割り出します。このデータを使用して、そのグループの仮想化デスクトップに必要なストレージを特定します。

管理者が物理デスクトップを使用して、グループの平均およびピーク時使用率を特定したら、Cisco VXI システムへの移行に必要なコンピューティング、ストレージ、およびネットワーキングを概算するプロセスを開始できます。

仮想化環境でのリソース要件の概算

仮想化環境でのリソース要件を正確に概算するには、いくつかの要因を考慮する必要があります。このセクションでは、これらの要因のうち CPU、メモリ、ストレージの 3 点について詳しく説明します。CPU、メモリ、およびストレージについて前のセクションで収集したデータを使用して、データセンターの特定のサーバがサポートできる仮想デスクトップの数を概算できます。仮想化では別の要因も追加されるので、サーバのキャパシティを概算する前に、上記のリソース要件を調整する必要があります。その後、単一のサーバ キャパシティを使用して、大規模な導入に必要なハードウェア リソースまたはサーバを概算できます。

CPU の概算

仮想化環境で必要な CPU リソースを概算するには、物理デスクトップのデータを利用できます。次に例を示します。

- 対象となるユーザ グループの物理デスクトップでの CPU 平均使用率は 5 % です。
- これらの物理デスクトップが 2.53 GHz のシングルコア プロセッサを使用していると仮定すると、デスクトップの平均 CPU 要件は、2.53 GHz の 5 % = 126.5 MHz となります。
- VMware は、10 ～ 25 % の保護帯域幅を使用して以下の項目に対処することを推奨しています。
  - 仮想化のオーバーヘッド
  - ピーク時の CPU 使用
  - ディスプレイ プロトコルの使用に関連したオーバーヘッド
  - CPU 使用率の急増

  従来の 25 % の保護帯域幅を使用すると、そのデスクトップの全体的な CPU 要件は約 158 MHz となります。
- 仮想化デスクトップの CPU 要件と、導入用に選択されたブレード サーバの処理能力を使用して、所定のブレードでサポート可能な仮想化デスクトップ数を概算できます。Cisco UCS ブレード サーバの処理能力を表 32 に示します。

（注） 各サーバ モデルはさまざまなプロセッサ タイプをサポートしていますが、表 32 にはサーバごとに 1 タイプのみが記載されています。

表 32　　UCS サーバ モデルおよびプロセッサ

サーバ モデル	プロセッサ
Cisco UCS B200 M1 ブレード サーバ	クアッド コア Intel Xeon 5570 シリーズ 2.93GHz プロセッサ X 2
Cisco UCS B200 M2 ブレード サーバ	6 コア Intel Xeon 5680 シリーズ 3.33GHz プロセッサ X 2
Cisco UCS B250 M1 拡張メモリ ブレード サーバ	クアッド コア Intel Xeon 5570 シリーズ 2.93GHz プロセッサ X 2
Cisco UCS B250 M2 拡張メモリ ブレード サーバ	6 コア Intel Xeon 5680 シリーズ 3.33GHz プロセッサ X 2
Cisco UCS B440 M1 高性能ブレード サーバ	8 コア Intel Xeon 7560 シリーズ 2.26GHz プロセッサ X 4
Cisco UCS B230 M1 拡張メモリ ブレード サーバ	8 コア Intel Xeon 7560 シリーズ 2.26GHz プロセッサ X 2

Cisco UCS サーバ シャーシおよびブレード サーバの詳細については、「データセンター」を参照してください。

- 以下に示すように、処理能力を唯一の判断基準として使用し、所定のブレード サーバのデスクトップ仮想マシン数を計算できます。たとえば、Cisco UCS B250 M2 サーバでサポート可能な仮想デスクトップ数は、次のようになります。

```
全体的な処理能力 = 2 ソケット X 6 コア 3.33GHz = 39.96 GHz
デスクトップの CPU 平均使用率 = 最大 158MHz
1 サーバあたりの仮想デスクトップ数 = 39.96GHz/158MHz = 252 デスクトップ
```

（注）　厳密にいうと、これは理論上の計算であるため、個々の顧客の導入におけるキャパシティ プランニングでは、テストで得られた実際のデータを使用してください。

同じく Cisco UCS B200 M1 サーバでサポート可能な仮想デスクトップ数は、次のようになります。

```
全体的な処理能力 = 2 ソケット X 4 コア 2.93GHz = 23.44 GHz
デスクトップの CPU 平均使用率 = 最大 158MHz
1 サーバあたりの仮想デスクトップ数 = 23.4GHz/158MHz = 148 デスクトップ
```

（注）　この概算は、単一の要因（CPU）に基づく理論上の計算です。所定のサーバ ブレードでサポート可能な実際の仮想デスクトップ数を特定するには、他にもいくつかの要因を考慮する必要があります。

単一サーバのサイズに関する前述の概算は、物理デスクトップで測定された平均使用率によって値が増減する可能性があることに注意してください。同様に、デスクトップ仮想化の導入用に選択された Cisco UCS サーバ モデルも、Cisco Unified Computing System™ で使用可能なサーバ オプションの処理能力の違いによって、数値に影響を与える場合があります。

処理能力が制限要因であることが確認された場合は、前述のサイズの概算で得られた数値を使用して、Cisco VXI の導入における全体的なサーバ要件を概算できます。ただし、メモリとストレージを使用して同様の計算を行わない限り、このシナリオを実例と見なすことはできません。所定のサーバ ブレードに関する概算値を確定する前に、さらにいくつかの要因を考慮する必要があります。

メモリの概算

仮想化環境での全体的なメモリ要件を概算するには、CPU の概算と同じ方法を使用します。単一の仮想デスクトップに関するメモリの概算値は、以下の例で示すように、物理デスクトップから得られた統計的平均値を使用して計算できます。

- 対象となるユーザ グループの物理デスクトップでのメモリ平均使用率は、約 750 MB です。
- メモリ使用率の急増やアプリケーションの追加によって増加するメモリ需要に対応するために、概算では 25 % の増加率を使用します。したがって、全体的なメモリ要件は、約 938 MB となります。
- 仮想化デスクトップのメモリ要件と、導入用に選択されたブレード サーバで使用可能な物理メモリ リソースを使用して、所定のブレードでサポート可能な仮想化デスクトップ数を概算できます。各種 Cisco UCS サーバ モデルのメモリ キャパシティを表 33 に示します。

表 33　　Cisco UCS のメモリ キャパシティ

サーバ モデル	メモリ キャパシティ
Cisco UCS B200 M1	96 GB
Cisco UCS B200 M2	96 GB
Cisco UCS B250 M1	384 GB
Cisco UCS B250 M2	384 GB
Cisco UCS B440 M1	256 GB
Cisco UCS B230 M1	256 GB

Cisco UCS サーバ シャーシおよびブレード サーバの詳細については、この設計ガイドの「データセンター」の章を参照してください。

- 次に示すように、メモリを Cisco VXI 導入におけるハードウェア サイズ要件の唯一の判断基準として使用し、ブレード サーバがサポートできるデスクトップ仮想マシン数を計算できます。たとえば、Cisco UCS B200 M1 サーバでサポート可能な仮想デスクトップ数は、次のようになります。

```
メモリ キャパシティ = 96GB
仮想化デスクトップの平均メモリ キャパシティ = 最大 938 MB
1 サーバあたりの仮想デスクトップ数 = 96G/938 = 102 デスクトップ
```

CPU の概算と同様、概算された単一サーバの仮想デスクトップ数は、物理デスクトップから収集されたデータや導入用に選択された Cisco UCS サーバのモデルによって値が増減する可能性があります。メモリが制限要因であることが確認された場合は、このデータを使用して Cisco VXI の導入に必要なサーバの総数も推定できます。

前述の計算で使用された物理デスクトップのメモリ使用率は、所定の環境に導入されるゲスト OS およびアプリケーションによって変動することに注意してください。正確さは劣りますが、Microsoft が推奨する仮想マシンあたりの最小メモリ使用率（表 34 を参照）を使用して仮想デスクトップ数を概算する方法もあります。ただし Microsoft Windows XP の場合は、デスクトップ上で動作する Microsoft Office およびその他のアプリケーションを収容するために、ここで示す推奨最小値を 512 MB に増やす必要があります。エンドツーエンドの Cisco VXI システムの仮想デスクトップに使用されるメモリ構成も例として示します。エンドツーエンド システムで検証した作業負荷プロファイルに対し、このメモリ構成で十分良好なユーザ エクスペリエンスが得られました。

表 34　メモリ構成

Microsoft Windows OS	（Microsoft の）最小メモリ要件	Knowledge Worker+ プロファイルを使用した Cisco VXI システムのメモリ構成
Microsoft Windows XP Service Pack 3	256 MB	1 GB
Microsoft Windows 7（32 ビット）	1 GB	1.5 GB
Microsoft Windows 7（64 ビット）	2 GB	2 GB

ストレージの概算

ストレージの場合は、物理デスクトップを監視して収集された平均 IOPS およびスループット データを、仮想化デスクトップのストレージ要件として使用できます。たとえば、平均 IOPS が 5、平均スループットが 115 kbps の場合、仮想デスクトップにもこれと同じ IOPS とスループット値が期待されます。デスクトップ仮想化の導入では、ここで説明する要因も大きく影響するため、ストレージに必要なサイズを決定する際にこれらの要因を考慮する必要があります。たとえば、IOPS は以下の場合に最大になる可能性があります。

- ユーザによる起動時：ユーザが出勤して各自の仮想デスクトップをオンにすると、IOPS とスループットの値は最大になります。この状態をブート ストームと呼びます。
- ユーザのログオン時：仮想デスクトップの電源をオンにする必要がなくても、ユーザが朝に作業を開始するためログオンすると、ストレージ I/O の値が最大になります。この状態をログイン ストームと呼びます。
- その他のアクティビティ実行時：アンチウイルス スキャンやバックアップなどのアクティビティによって、必要なストレージ パフォーマンスが急増します。

顧客環境に固有のアプリケーションが、同様のストレージ I/O 急増の原因となることもあります。Cisco VXI 導入におけるストレージ環境を設計する際には、これらすべての要因を考慮する必要があります。

必要なストレージのサイズを決定する際、もう 1 つ考慮すべき点は、仮想デスクトップに割り当てるディスク スペースです。以下のアイテムに必要なストレージを合計すると、ディスク スペースを計算できます。

- オペレーティング システム、アプリケーションの基本セット
- OS およびアプリケーションによって作成されるページ ファイル、スワップ ファイル、一時ファイル
- ホストに導入された各仮想マシン用に VMware ESX および ESXi ホストで作成されるページとスワップ ファイル（仮想マシンに割り当てられるメモリに相当）
- Microsoft Windows プロファイル（デスクトップの壁紙などのユーザ設定）
- ユーザ データ（Microsoft Windows の [マイ ドキュメント] フォルダに相当）

仮想デスクトップ マシンに使用するストレージの割り当て例を表 35 に示します。View リンクド クローン デスクトップまたは Citrix ストリーム配信デスクトップをプロビジョニング サーバとともに使用してデスクトップ仮想化を導入すると、大規模なデスクトップ プールのグループが同じマスター仮想マシン イメージを共有できるので、Windows およびアプリケーションに必要なデスクトップあたりのディスク スペースが最小限に抑えられます。したがって、マスター仮想マシン イメージと、マスター VM で使用可能なディスク スペースとの差分のみを、前述の導入モデルを使用して各デスクトップに割り当てればよいことになります。ただしこの差分ディスク サイズも、OS ディスクを定期的に更新したり、非永続的デスクトップを使用したりすることで、最小限に抑えることができます。この点についても、複数のオプションがあります。

表 35　デスクトップ VM のストレージ割り当て

仮想デスクトップのゲスト OS	Windows およびアプリケーションの最小ディスクスペース	Windows ページファイルおよび一時ファイル	ハイパーバイザ スワップ ファイル	Windows ユーザ プロファイル	ユーザ データ
Windows XP	10 GB	3 GB	1 GB	2 GB	5 GB
Windows 7（32 ビット）	16 GB	4 GB	1.5 GB	2 GB	5 GB
Windows 7（64 ビット）	20 GB	4 GB	2 GB	2 GB	5 GB

サーバ キャパシティの概算

前述のとおり、サーバのパフォーマンスとスケーラビリティには複数の要因が影響します。各要因を別々に考慮すると、所定のサーバの仮想デスクトップ数の概算で異なる数値が算出される可能性があります。そのため、この章の前半の「CPU の概算」と「メモリの概算」のセクションでは、Cisco UCS B200 M1 サーバについて理論上の概算を行っています。ただし、それらのデータ（表 36 に概要を示します）はサーバの制限要因の特定に役立つとともに、その環境の具体的な作業負荷を使用して概算値を検証するためのテストを実施すれば、対象とする初期の仮想マシン密度もわかります。

表 36　キャパシティの概算値

キャパシティの決定要因	仮想化デスクトップの平均値	サーバ キャパシティ（Cisco UCS B200 M1 の理論値）
CPU	158 MHz	148
メモリ	938 MB	102

（注）　表 36 の概算値は、サーバの実際のキャパシティではありません。これらは、所定の環境内のユーザ グループに対する CPU およびメモリ使用率の仮定に基づいた、**理論上**の概算値です。

デスクトップ仮想化の導入において、作業負荷は環境内におけるサーバ上の仮想デスクトップ密度を正確に推定するために最も重要な要因です。したがって、サーバあたりのサイズを決定するために実行する概算とテストには、ユーザ グループの作業負荷と厳密に一致する作業負荷を使用する必要があります。XenDesktop で実行されたスケーラビリティ テストの実際の結果については、次のリンクを参照してください。

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns993/landing_dcVirt-vdi.html

上記のスケーラビリティ調査に加え、この設計ガイドで説明されているエンドツーエンドの Cisco VXI システムでも単一サーバのスケーラビリティ テストが実施されました。お客様がシステムを導入および使用する場合と同様に、テストは複数の導入プロファイルを使用してエンドツーエンドの Cisco VXI システムで行われました。テストはキャンパス ネットワーク内に配置されたテスト ツールを使用して行われました。これらのツールによって、データセンターでホストされている仮想デスクトップの VDI セッションが起動され、セッションは以下を経由します。

- キャンパス ネットワーク：アクセス レイヤ、ディストリビューション レイヤ、コア ネットワーク レイヤで構成され、Catalyst 3500、4500、および 6500 シリーズ レイヤ 2 およびレイヤ 3 スイッチを使用して構築されます。

- データセンター ネットワーク：同じくコア レイヤ、アグリゲーション レイヤ、アクセス レイヤで構成され、シスコが検証したデータセンター インフラストラクチャ設計に基づいて Nexus 5000 および Nexus 7000 を使用して構築されます。
- データセンター サービス アグリゲーション レイヤ：ファイアウォールを使用して、データセンターに出入りするすべてのトラフィックを制御します。ファイアウォールはデータセンター内部のアクセス レイヤでも使用され、データセンターに常駐するその他すべてのサービスおよびアプリケーション インフラストラクチャから、仮想デスクトップ間のトラフィックを制御します。冗長 ACE は、Citrix Web サーバや XenDesktop Controller などデスクトップ仮想化サービスを提供するアプリケーション サーバへのすべての接続をロード バランシングするために使用されます。
- データセンター：Nexus 1000 シリーズ アクセス スイッチに接続された B250 M2 および B200 M2 ブレード サーバ搭載の UCS 5108 B シリーズ シャーシを収容します。テストする導入プロファイルの必要性に応じて、NAS ベースと SAN ベースの両方のストレージが使用されました。

Cisco VXI 作業負荷を使用して Cisco VXI システムで実施された単一サーバ テストの結果とデータについては、この章の「作業負荷の考慮事項」のセクションを参照してください。

CPU、メモリ、およびストレージの使用率以外に、サーバの規模やキャパシティに影響を与える要因は、作業負荷のほかにもいくつかあります。これらの要因については以降のセクションで説明します。

一般的な考慮事項

ハイパーバイザの考慮事項

CPU、メモリ、ストレージのパフォーマンスを確保するために、ハイパーバイザのリソース消費を厳重に監視する必要があります。

仮想 CPU の考慮事項

Citrix では HDX を使用した 2 vCPU の導入を推奨しています。ただし、作業負荷が広範囲にわたるデスクトップ仮想化環境では、1 vCPU も一般的です。VMware では、複数の vCPU が使用され、ハイパーバイザが ESXi の場合は、単一のサーバ上に 1 vCPU と 2 vCPU を混在させないよう推奨しています。これは、リソース スケジューリングを実行すると、2vCPU デスクトップよりも 1vCPU マシンの処理が優先される可能性があるためです。リソース プールを使用して CPU 占有率を予約することはできますが、一般にリソース プールは仮想化デスクトップ環境では使用されません。VMware では、所定のホストでサポート可能な vCPU 数が表 37 の数値まで増強されました。キャパシティ プランニングの観点からみて、これらの数値は注目に値します。ただし表からもわかるとおり、多数のコアを搭載し、1 コアあたり 25 vCPU をサポートできるサーバの場合は、サポートされる 1 ホストあたりの仮想マシン数が仮想デスクトップ数の制限要因になります。表 37 のデータは、vSphere 4.0 と 4.1 の最大構成に関する VMware ドキュメントから引用したものです。完全なドキュメントへのリンクについては、この章の末尾にある「関連情報」のセクションを参照してください。

表 37　　仮想 CPU の制限

制限	VMware vSphere 4.0	VMware vSphere 4.1
コアあたりの仮想 CPU 数	25	25
ホストあたりの仮想 CPU 数	512	512
ホストあたりの仮想マシン数	320	320

（注） 1 コアにつき 25 vCPU がサポートされていても、達成可能な 1 コアあたりの CPU の数は作業負荷によって異なります。

（注） 実際にデスクトップ仮想化を導入した場合、仮想デスクトップの仮想マシン数は、おそらく 1 コアあたり 8 ～ 10 程度になります。

メモリの考慮事項

ESXi ハイパーバイザで使用可能な Transparent Page Sharing（TPS; 透過的ページ共有）機能によって、メモリ フットプリントを大幅に削減できます。特にデスクトップ仮想化の導入では、異なるデスクトップ仮想マシン間で OS およびアプリケーション データの共通点が多いため、大きな効果が得られます。TPS は、バックグラウンド プロセスを使用してメモリのコンテンツを監視し、ロードされるデータを調べて、すでにメモリ内にあるデータと同じであるかどうかを判断します。データが同じであれば、重複しているデータをロードしようとしている仮想マシンはメモリ内の既存コンテンツにリダイレクトされ、これによってメモリの共有が可能になります。TPS はメモリの重複排除機能と考えることができ、デフォルトで有効になっています。この機能の詳細については、次の URL を参照してください。

http://www.vmware.com/resources/techresources/531

Cisco VXI 環境では、透過的メモリ共有を利用することで、サーバは 1 つのブレード上により多くの仮想デスクトップを収容できるようになります。少なくとも、メモリという観点で捉えた場合、これは制限要因にはなりません。

TPS は冗長性を利用して、ホスト上で動作する仮想マシン間でメモリを共有し、その制限を回避しているので、それらの仮想マシンの作業負荷はできる限り同じでなければなりません。Cisco VXI 環境で TPS の効果を最大限利用するには、作業負荷が同程度のユーザ、たとえば同じゲスト OS（Microsoft Windows 7 および Windows XP）とアプリケーションを使用するユーザの仮想化デスクトップを 1 つのグループにまとめ、同じホストに配置します。

Cisco UCS サーバで使用される Intel Nehalem や Westmere プロセッサのように新型のハードウェア仮想化支援プロセッサ上では、TPS の動作が異なります。この新型プロセッサは、9 KB のメモリ ページを使用し、パフォーマンスを 10 ～ 20 % 改善します。TPS はデータの重複をなくすために、4 KB のページ上で動作します。これらの新型プロセッサが搭載されている場合、使用可能なメモリが最小値に達してメモリの制約を回避する必要が生じない限り、TPS の効果は発揮されません。ただし、TPS の効果が現れたことを確認するために、バックグラウンド プロセスでは引き続きメモリ ページの監視とスキャンが実行されます。新型のハードウェア仮想化支援プロセッサを使用した TPC の詳細については、次の VMware Knowledge Base の記事を参照してください。

- TPS in Hardware Memory Management Unit (MMU) Systems：
  http://kb.vmware.com/kb/1021095
- TPS Is Not Utilized Under Normal Workloads on Intel Xeon 5500 Series CPUs ：
  http://kb.vmware.com/kb/1020524

VMware の調査では、TPS がホストのパフォーマンスには影響しないことから推奨される機能であることも示されています。TPS の詳細については、VMware にお問い合わせください。

ハイ アベイラビリティの考慮事項

大規模なデスクトップ仮想化を導入する場合、仮想デスクトップのハイ アベイラビリティは大半の導入において第一の重要事項です。VMware はベスト プラクティスとして、ホストまたはサーバをクラスタ構造で配置し、VMware High Availability（HA; ハイ アベイラビリティ）、Dynamic Resource Scheduling（DRS）、Fault Tolerance、vMotion などのハイ アベイラビリティ機能を有効にすることを推奨しています。クラスタリングを行うと、サーバおよびコンピューティング リソースをプールにまとめて配置できるので、DRS を配備して、クラスタ内のホスト間で仮想デスクトップの動的ロード バランシングを実行できます。動的ロード バランシングはリソースのニーズに応じて実行したり、起動時のみ実行されるように設定したりすることができます。

ただし、サーバをクラスタ内に配置すると、VMware がサポートする最大数が変更され、制限される可能性があります。サポートされる制限は、VMware の最大構成で使用でき、新規リリースによってサポートされる制限が変更された場合に公開されます。デスクトップ仮想化導入の規模の決定に関連するデータを表 38 に示します。大規模な Cisco VXI の導入を計画する場合は、この表を参照してください。最大構成の詳細については、VMware のドキュメントを参照してください。

表 38　　最大構成

制限	VMware vSphere 4.0 Update 2	VMware vSphere 4.1
ホストあたりの仮想マシン数	320	320
ホストあたりの vCPU 数	25	25
ハイ アベイラビリティ クラスタあたりのホスト数	32	32
クラスタあたりの仮想マシン数	-	3000
ホスト数 8 以下のハイ アベイラビリティ クラスタ内のホストあたりの仮想マシン数	160	-
ホスト数 9 以上のハイ アベイラビリティ クラスタ内のホストあたりの仮想マシン数	40	
VMware vCenter サーバあたりのホスト数	1000	1000
データセンターあたりのホスト数	100	400

Microsoft Hyper-V

Cisco VXI に導入された Hyper-V Windows 2008 R2 リリースには、メモリの制限を回避する機能はありません。ただし、最近リリースされた SP1 バージョンは、動的なメモリ機能を備えています。この機能の詳細については、次の URL にある Microsoft の Web サイトで『Hyper-V Dynamic Memory Configuration Guide』を参照してください。

http://technet.microsoft.com/en-us/library/ff817651(WS.10).aspx

電源管理

デスクトップ仮想化環境で使用される電源管理ポリシーは、コンピューティング リソースに影響を与える可能性があります。Citrix XenDesktop では、使用されていない仮想デスクトップを一時停止状態にしておくことが推奨されます。リソース（CPU とメモリ）の使用を低減しつつ、ユーザ エクスペリエンスを強化するには、一時停止状態が最適な設定です。すべての仮想マシンの電源をオンにしておくと、同じサーバ上にある他の仮想マシンがホスト リソースを使用できません。永続的デスクトップを使用すると、ユーザがログオフするとただちに仮想マシンを一時停止できます。

ストレージの考慮事項

Cisco VXI システムで使用される Citrix XenDesktop5 では、プールされたデスクトップを配置できるようにし、プール内のすべてのデスクトップで共有されるメイン OS ディスクを使用することで、必要となるストレージが全体的に低減されます。Citrix XenDesktop 5 を使用した仮想デスクトップの導入については、「データセンター」を参照してください。

プールされたデスクトップを Citrix XenDesktop で使用すると、仮想化環境への移行に必要なストレージの全体的キャパシティが大幅に減少します。共有ストレージのコストは、ラップトップおよびデスクトップで個別のディスクを使用するよりもかなり高くなりますが、Citrix XenDesktop は多数のデスクトップ仮想マシンで同じ OS ディスクを共有する機能を備えているので、全体的なストレージ コストを削減できます。

オペレーティング システム ディスク

Citrix の導入における OS ディスクとは、ゲスト OS（Microsoft Windows XP または Windows 7）とアプリケーション（Microsoft Office）がインストールされている親仮想マシンの仮想ディスクを指します。この OS ディスクは、プール内のすべてのデスクトップによって読み取られます。その結果、1 つの OS ディスクを多数のデスクトップで共有でき、各デスクトップはそれぞれ専用の OS ディスクを保持する必要がないので、ストレージを大量に節約できます。ストレージと操作の両面での効率性を考えた場合、このディスクは読み取り専用にするのが理想的ですが、このディスクを読み取りおよび書き込みディスクとして使用すると、次に示す一般的なタイプの Microsoft Windows デスクトップ データを保存できます。

- Microsoft Windows プロファイル データ
- 一時ファイル（ページ ファイルを含む）
- ユーザ データ

ストレージと操作の効率性を高めるには、OS ディスクを読み取り専用ディスクにし、ここに示したデータを次のように他の場所へリダイレクトします。

- Microsoft Windows プロファイル データは、Microsoft Windows 共有またはこの目的専用の別の仮想ディスクへリダイレクトできます。これにより、OS ディスクが更新された場合にそのデータを保存できます。
- 一時ファイルを非永続的ディスクへリダイレクトし、データを更新してストレージの使用を低減することも可能です。SAN 上または Network-Attached Storage（NAS; ネットワーク アタッチド ストレージ）の一時的なボリュームの独立した場所を使用できます。
- 通常は My Documents フォルダに保存されるユーザ データは、Microsoft Windows 共有または別個のディスクへリダイレクトします。

シン プロビジョニングと シック プロビジョニング

シン プロビジョニングは、ストレージ リソースを節約し、仮想化環境でのストレージ使用率を増大させる一つの方法です。シック プロビジョニングでは、仮想マシンが導入されると、その仮想マシンに関連付けられた仮想ディスクに対し、使用の有無に関係なくすべてのストレージが割り当てられ、スペースが無駄に消費されます。シン プロビジョニングでは、仮想マシンに必要な場合のみストレージ リソースを割り当てることで、このような非効率性は軽減されます。したがって、20 GB ディスクを備えた Microsoft Windows 7 が動作する仮想デスクトップは、ストレージ システム（SAN または NAS）で 20 GB のディスク スペースを予約していませんが、この仮想デスクトップ上の Microsoft Windows およびアプリケーションは、20 GB のスペースすべてが割り当てられているかのように動作します。このように、シン プロビジョニングではストレージの制約を回避することで、基盤となるストレージ リソースを効率的に使用し、ストレージ キャパシティ全体のスケーラビリティを強化することができます。Cisco VXI 環境では、このアプローチによって、所定のストレージでサポート可能な仮想デスクトップ数が増加します。

シン プロビジョニングは、ハイパーバイザまたはストレージ システムで実行できます。NetApp や EMC などのストレージ ベンダーは、ストレージ レベルのシン プロビジョニングを提供しています。ストレージ レベルのシン プロビジョニングでは、ストレージの効率性がハイパーバイザ レベルの場合よりもさらに向上します。ストレージ シン プロビジョニングでは、実際のストレージ割り当て状態は、ストレージ システムによってハイパーバイザから隠されています。

Cisco VXI システムでのすべての検証は、ストレージ レベルまたはハイパーバイザ レベルのいずれかのシン プロビジョニングを使用して実施されました。

（注） シン プロビジョニングはストレージ リソースの超過割り当てであるため、スペース不足による問題が発生する前にストレージをデータ ストアに追加できるよう、シン プロビジョニングが行われるディスクの状態を注意深く監視する必要があります。

詳細については、この章の「関連情報」のセクションを参照してください。

ストレージ フットプリントの削減

ストレージ ベンダーは、デスクトップ仮想化導入に必要なストレージ サイズの決定に利用できる、規模の経済性を提供するテクノロジーをサポートします。このテクノロジーには、保存するデータ内の重複している情報を除去してストレージの効率性を高める、データの重複排除が含まれます。この機能は、VMware の主要ファイル システムおよびエンド ユーザ ファイル データ、およびその他の仮想化環境で使用できます。重複しているデータが他の仮想化デスクトップ仮想マシンのデータである場合、そのデータは 1 度だけ保存され、それに関連付けられたメタデータが変更されます。これにより、両方の仮想マシンがデータにアクセスできます。シン プロビジョニングの場合と同様、重複排除を使用すると、既存のストレージが多数の仮想デスクトップをサポートできるようになるため、ストレージをきわめて効率的に使用でき、デスクトップ仮想化のスケーラビリティが向上します。したがって、特に大規模なデスクトップ仮想化の導入では、重複排除機能を有効にすることを強くお勧めします。

デスクトップ仮想化環境での重複排除機能の使用方法については、EMC と NetApp のドキュメントを参照してください。

パーティションの調整

仮想化デスクトップ上で動作する Microsoft Windows ファイル システム パーティションは、基盤となるストレージ パーティションに合わせて調整する必要があります。この調整によって全体的な I/O 遅延が減少する一方、ストレージのスループットは増大するため、ストレージ パフォーマンスを強化することができます。Microsoft Windows 7（32 ビットおよび 64 ビット）ではパーティションが自動的に調整されるので、現在は Microsoft Windows XP でのみパーティションの調整が必要です。Microsoft Windows では、ドライブの先頭に 63 ブロックのメタデータが直接書き込まれるため、ディスク上に作成された最初のパーティションが正しく調整されず、問題が発生します。その結果、ドライブでは不要なデータ ブロックを余分に読み込む必要が生じ、ドライブの IOPS が増加する原因となります。このような調整の不備に対処するために、使用されるストレージ ドライブと連携するドライブに、調整済みパーティションが作成されます。この調整は、ブロックベースとファイルベースの両方のストレージ システムに有益です。Cisco VXI システムでは、EMC の SAN および NetApp の NAS ストレージと連携するために、デスクトップ プールの親仮想マシン上で 64 KB の調整済みパーティションが作成されました。詳細については、Microsoft および Citrix のドキュメントを参照してください。

ストレージ ネットワークの考慮事項

- ジャンボ フレーム：IP ベースのストレージを使用する Cisco VXI 導入では、ジャンボ フレームを有効にして、ストレージ帯域幅の使用率を増やし、I/O 応答時間を改善する必要があります。ジャンボ フレームによって、データセンターの LAN ネットワークで IP トラフィックの転送に使用されるイーサネット フレームの Maximum Transmission Unit（MTU; 最大伝送ユニット）が増大します。ジャンボ フレームを有効にすると、通常はイーサネットの MTU がデフォルト値の 1,518 バイトから 9,000 バイトに増加します。ジャンボ フレームは、仮想デスクトップをホストしているサーバと、そのサーバが使用する IP ストレージとの間の各リンクで有効にする必要があります。ジャンボ フレームは全体的なスループットを改善するだけでなく、大容量のファイルを転送するホストの CPU の負担も軽減します。
- ストレージ ネットワークの分離：ストレージ トラフィックは、LAN を使用する他のネットワーク トラフィックから物理的（推奨）または論理的に分離する必要があります。ファイバ チャネル SAN ストレージが使用される場合、Cisco Unified Computing System アーキテクチャではストレージ専用に 2 つの Host Bus Adapter（HBA; ホスト バス アダプタ）がサポートされます。
- NFS および Small Computer System over IP（iSCSI）トラフィックのストレージなど IP ベースのストレージでも、同様の物理的な分離が推奨されます。IP ストレージ トラフィックには、ホストの専用アップリンク ポートを使用して、別個の VMkernel ポートと VLAN を使用する必要があります。このように IP ストレージ トラフィックを他の IP から物理的に分離するために、Cisco Unified Computing System では 128 個の仮想アップリンク ポートをサポートする最新の Converged Network Adapters（CNA; 統合ネットワーク アダプタ）を使用します。アップリンクを専用にできない場合は、ストレージに使用される個々の VLAN によって論理的な分離が行われます。物理的分離は、アクセス レイヤで専用ポートまたはスイッチを使用してデータセンター ネットワークに拡張する必要があります。アクセス レイヤには、通常は Cisco Nexus 5000 シリーズ スイッチが配置されています。ストレージ トラフィックがデータセンターのアグリゲーション レイヤに拡張されると、通常はこのレイヤに配置される Cisco Nexus 7000 シリーズ スイッチによって、Virtual Data Center（VDC; 仮想データセンター）を介した物理的分離がサポートされます。
- ポートチャネル：可用性を損なうことなく全体的なアップリンク帯域幅を増強するには、ホストの LAN アップリンク ポートとアクセス レイヤ スイッチ（Cisco Nexus 5000 シリーズ）間でポートチャネルを使用します。Cisco VXI 導入で IP ベースのストレージを使用する場合は、必要な LAN 帯域幅が大幅に増加するため、このアプローチが重要になります。
- マルチパス化：ブロックベースの SAN ストレージと IP ベースの NAS ストレージのいずれの場合でも、マルチパス化を使用して、ホストとそのストレージ間にロード バランシングされた冗長パスを作成できます。VMware は、ストレージ デバイスに関連付けられたさまざまな物理パスを学習し、パス選択スキームを使用して所定の I/O 要求のパスを判断します。VMware でストレージ デバイスへのパスを選択するには、固定パス、直前に使用されたパス、ラウンドロビンの 3 つのオプションがあります。複数の物理パスで I/O トラフィックをロード バランシングする場合は、ラウンドロビンを使用します。マルチパス化では、ストレージの復元力が強化されることによってパフォーマンスが向上するので、ストレージ ベンダーがマルチパス化をサポートしている場合は、この機能を Cisco VXI 導入で有効にしておきます。エンドツーエンド Cisco VXI システムの EMC（ファイバ チャネル SAN）と NetApp（NFS）では、この機能がサポートされます。

ゲスト OS の最適化

Microsoft Windows を以下のように最適化し、仮想化デスクトップのパフォーマンスとスケーラビリティを強化できます。

- Microsoft Windows 仮想マシンのファイル システムを最適化し、最良の I/O パフォーマンスを実現するには、NTFS で最終アクセス日時の更新プロセスを無効にします。アプリケーションによってファイルが開かれると、Microsoft Windows は最終アクセス日時を使用してそのファイルを更新します。このオプションを無効にすると、ファイル システム内部での IOPS が減少します。

- 特に Windows 7 の導入では、Windows Best Performance を有効にすると、コンピューティングと WAN BW 使用率の両面において重要なパフォーマンスが向上します。
- 各仮想マシンが使用するメイン OS ディスクが、アンチウイルス ソフトウェアによってスキャンされないようにしてください。なぜなら、メイン OS ディスクは読み取り専用ディスクとして配置されており、仮想デスクトップの Citrix XenDesktop プールで使用されるゴールデン マスターとして認識される前に、アンチウイルス チェックが実行されているからです。この手順は、特に大規模な Cisco VXI 導入でのストレージ パフォーマンスの増強に効果的です。

仮想化デスクトップでは、複数の Windows 最適化を有効にしてパフォーマンスを強化できます。Cisco VXI システムに実装されている、Microsoft Windows XP および Windows 7 向けの主な最適化を表 39 に示します。

表 39　Microsoft Windows ゲスト OS の最適化

Microsoft Windows ゲスト OS の最適化
Microsoft Windows ゲスト OS の最適化
Microsoft Windows Hibernation の無効化
Microsoft Windows Defender の無効化（XP は適用外）
Microsoft Feeds Synchronization の無効化
Microsoft Windows Scheduled Disk Fragmentation の無効化（XP は適用外）
Microsoft Windows Registry Backup の無効化（XP は適用外）
ディスプレイの電源オプションをオフにする（PCoIP の場合）
マウス ポインタの影の無効化
書き込み専用時の McAfee アンチウイルス スキャン
Pre-fetch/Superfetch Service の無効化（XP は適用外）
Microsoft Windows Diagnostic Policy Service の無効化（XP は適用外）
「No automatic updates」の有効化
System Restore の無効化（コンポーザによって更新が実行される可能性があるため）
Microsoft Windows OS 自体のページングの無効化
不要なサービスの無効化
起動およびシャットダウン時の不要なサウンドの無効化
インデックス サービスの無効化
すべての壁紙の削除
スクリーン セーバーの無効化

キャパシティの概算値の検証

全体的なリソース プランニング プロセスの次の手順では、前のセクションで説明した要因のほか、CPU、メモリ、ストレージなどの要因に基づいたキャパシティの概算を検証します。物理デスクトップのベースライン パフォーマンス データと、導入用に選択された Cisco UCS ブレード サーバ上に展開できる仮想デスクトップ数の理論上の概算値に基づき、仮想化環境でのパフォーマンスの特定と検証を行い、以下の項目を判断します。

- サーバの CPU 平均使用率
- サーバのメモリ使用率

- サーバによって生成されるストレージ IOPS
- サーバのネットワーク帯域幅使用率
- アプリケーション応答時間

作業負荷の考慮事項

Cisco VXI 導入のためのキャパシティの概算を検証するには、1 つのオプションを使用してパイロット グループにサービスを提供し、実際のユーザのリソース概算値を検証されます。あるいは、ユーザ アクティビティ、使用されたアプリケーション、および使用パターンについて物理デスクトップから収集されたデータを使用して、環境固有の作業負荷を定義することもできます。ユーザの作業負荷がシミュレーションされるよう、カスタムの作業負荷をテスト用に自動化することができます。あるいは、スケールおよびパフォーマンス テスト用の作業負荷生成ツールで一般に使用される一般プロファイルのいずれかに、カスタムの作業負荷をマッピングすることも可能です。

作業負荷によって、ワープロ処理、プレゼンテーション、その他のオフィス用アプリケーションなど、ユーザが実際に使用するアプリケーションが明確になりますが、作業負荷にはバックアップやアンチウイルス スキャンなど、バックグラウンドのアクティビティも含まれています。社内ユーザの作業負荷は、各自の業務や職務によって異なり、組織構造（販売、マーケティング、製造など）によって違う場合もあります。作業負荷は、デスクトップ仮想化ユーザが地理的に分散している場合は特に、日時によって異なることもあります。バックアップやアンチウイルス スキャンなど、特定の時刻に開始されるバックグラウンド アクティビティも、作業負荷が増大する原因となります。

エンタープライズ ネットワークにおける作業負荷の定義およびその他の考慮事項を包括的に考察するには、「デスクトップ仮想化」の章を参照してください。

表 40　　ユーザ プロファイル

ユーザ プロファイル	説明
タスク ワーカー	• 一度に 1 つのアプリケーションを開く • 印刷機能が制限される • マウスの使用が制限される • 主な作業はテキスト編集
ナレッジ ワーカー	• 一度に複数のアプリケーションを開く • 多様なアプリケーション • マルチメディア搭載のグラフィック アプリケーション、USB 周辺機器の使用
パワー ユーザ	• 一度に複数のアプリケーションを開く • グラフィックや計算の負荷が高いアプリケーション • 場合によってはユーザに管理者権限が必要

このドキュメントで説明されているエンドツーエンドの Cisco VXI システムでは、初めの 2 つのユーザ プロファイルの変動値を使用してテストを実施しました。このプロファイルを、Cisco VXI Knowledge Worker+（KW+）プロファイルと呼びます。このプロファイルの詳細を次の表に示します。

表 41　Cisco VXI Knowledge Worker+ プロファイル

スクリプト シーケンス	作業負荷プロファイル内のアプリケーション	アプリケーションでのアクティビティ
ステップ 1	Cisco Unified Personal Communicator を起動する	1. Cisco Unified Personal Communicator アプリケーションがインストールされているかどうかを確認する 2. インストールされていない場合は次のアプリケーションへ移動する 3. インストールされている場合は Cisco Unified Personal Communicator を起動する 4. Cisco Unified Personal Communicator にログインする
ステップ 2	Internet Explorer 8 を起動し、動作を維持する	1. アプリケーションを起動する 2. キャッシュを消去する 3. 最初の Web ページ http://10.0.128.150/VXI/index.html を開く 4. 次の Web ページ http://10.0.128.150/VXI/Recipes/index.html を開く
ステップ 3	Microsoft Word を起動して閉じる	1. アプリケーションを起動する 2. 既存のファイルを開く 3. 最後のページへ移動する 4. ページを挿入する 5. 文章を書き込む 6. Word 文書を保存する 7. アプリケーションを閉じる
ステップ 4	Microsoft Outlook を起動して閉じる	1. アプリケーションを起動する 2. すべてのフォルダが最新の状態になるまで待機する 3. 送受信を実行する 4. 既存の電子メールを削除して受信箱を空にする 5. 電子メールを送信する 6. 電子メールの返信を待機する 7. 電子メールを削除する

スクリプト シーケンス	作業負荷プロファイル内のアプリケーション	アプリケーションでのアクティビティ
ステップ 5	Microsoft Excel を起動して閉じる	1. アプリケーションを起動する 2. 既存のファイルを開く 3. ズームの倍率を 100 % に設定する 4. ページを上に移動する 5. ページを下に移動する 6. 文書を保存する 7. アプリケーションを閉じる
ステップ 6	Microsoft PowerPoint を起動して閉じる	1. アプリケーションを起動する 2. 既存のファイルを開く 3. スライドショーを再生する 4. アプリケーションを閉じる
ステップ 7	Adobe Acrobat を起動して閉じる	1. アプリケーションを起動する 2. 既存のファイルを開く 3. ページ 50 へ移動する 4. ズームの倍率を 75 % に設定する 5. 表示を拡大（5 回）および縮小（5 回）する 6. アプリケーションを閉じる

- Cisco VXI では、デフォルトのスキャン プロファイルを使用して McAfee Move AV 1.5 がバックグラウンドで実行されています。
- Cisco Unified Personal Communicator と Outlook を除くすべてのアプリケーションは、作業負荷ループを複数回繰り返す中で無作為に抽出されます。
- 無作為に抽出されたタイマーが上記の各ステップで使用され、7 ～ 11 秒間停止してユーザの「思考」時間をシミュレーションします。

次のセクションでは、さまざまな導入プロファイルに対して実行された単一サーバ特性評価の結果を考察し、続いて Cisco VXI 環境でシスコのコラボレーション アプリケーションに対して実行されたアプリケーション特性評価について説明します。

単一サーバのスケールおよびパフォーマンス結果

このセクションでは、Cisco VXI の Citrix XenDesktop 5 に対して実行されたさまざまなスケールおよびパフォーマンス特性評価の結果を詳しく見ていきます。エンドツーエンドの Cisco VXI で単一サーバの観点から特性評価された領域の概要を次に示します。

- ESXi 4.1 上の XenDesktop 5、UCS B250 M2 および NetApp FAS 3170 を使用
- Hyper-V 2008 R2 上の XenDesktop 5、Windows 7（64 ビット）デスクトップ向け、UCS B230 M1 および NetApp FAS 3170 を使用
- ESXi 4.1 上の McAfee MoveAV 1.5、XenDesktop 5 搭載、UCS B250 M2 および NetApp FAS 3170 を使用

- Hyper-V 2008 R2 上の XenDesktop 5、Windows XP SP3 デスクトップ向け、UCS B250 M2 および EMC Unified Storage を使用
- XenServer 5.6 FP1 上の XenDesktop 5、Windows 7（32 ビット）デスクトップ向け、UCS B250 M2 および NetApp FAS 3170 を使用
- ESXi 4.1 上の McAfee MoveAV 1.5、XenDesktop 5 搭載、UCS B250 M2 および NetApp FAS 3170 を使用

上記のすべてのテストは、このドキュメントで前述した Cisco VXI システム アーキテクチャを基盤とするエンドツーエンドの Cisco VXI ネットワークで実施されました。

作業負荷プロファイル：Cisco VXI Knowledge Worker+

前述したとおり、使用した作業負荷は、デスクトップ仮想化環境で実施されるパフォーマンス関連の特性評価にとって非常に重要な要因です。ここに示すすべてのテスト結果には、別途記載がない限り、Cisco VXI Knowledge Worker+（KW+）の作業負荷が使用されています。このプロファイルの概要については、この章の「作業負荷の考慮事項」のセクションに記載されています。

合格基準

すべての単一サーバ テストの目的は、前述の Cisco VXI KW+ プロファイルに基づく特定の導入プロファイルに対し、所定のサーバ モデルでサポート可能な仮想デスクトップ密度を特定することです。各ケースで使用された合格基準は次のとおりです。

- アプリケーションの応答時間に基づく良好なユーザ エクスペリエンス
- 80 % または 90 % の CPU 使用率
- バルーニング（ESXi）およびスワッピングによらない 90 % のメモリ使用率

アプリケーション応答時間

次の表は、Cisco VXI システムで合格基準として使用された、アプリケーションの平均応答時間をまとめたものです。すべてのテストは、Scapa Technologies の Test and Performance Platform（TPP）を使用して実行されました。UCS サーバでホストされている各仮想デスクトップ上で、Scapa 負荷生成ツールが VDI セッションを起動し、作業負荷プロファイルで定義されたアクティビティを開始して、各デスクトップ上で作業負荷を生成します。作業負荷に含まれるアプリケーション（Cisco Unified Personal Communicator を除く）は、作業負荷ループが繰り返されるたびに起動され、閉じられます。したがって、所定のアプリケーションについて測定された平均応答時間（下記を参照）は、サーバ上で動作しているすべての HVD で測定されたアプリケーション応答時間と、各 HVD で作業負荷を繰り返し実行する間に測定された応答時間を結合したものです。下記の合格基準は、これらのアプリケーションを使用して物理デスクトップと HVD で実施されたテストと、応答時間の測定値を組み合わせて得られた数値です。各テストでは、測定された応答時間を、下記で定義されているテストに合格するための合格基準と比較します。Scapa は、データセンターでホストされている仮想デスクトップではなく、ユーザまたはエンドポイントの観点から応答時間を測定することにも注意が必要です。

表 42　　合格基準

アプリケーション	最大許容起動時間の合格基準
Cisco Unified Personal Communicator 8.5	5 秒
Outlook	10 秒
Excel	5 秒
PowerPoint	5 秒

アプリケーション	最大許容起動時間の合格基準
Acrobat	5 秒
Internet Explorer	5 秒
Word	10 秒

パフォーマンス メトリック

テストを実施した各導入プロファイルについて、サーバ パフォーマンスの次の項目が測定されました。ESXi では esxtop を使用して、5 秒のポーリング間隔でこれらのメトリックを測定しました。可能な場合は、NetApp および EMC のストレージの統計も含まれています。

- CPU 平均利用率
- メモリ平均使用率
- ストレージ
  - IOPS
  - IO 帯域幅
  - IO 遅延
- ネットワーク帯域幅使用率

ESXi 上の XenDesktop 5（XD5）

このセクションでは、XenDesktop 5 と ESXi を搭載し、W7（32 ビット）デスクトップを実行し、ストレージに NetApp を使用する UCS B250 M2 での単一サーバ スケーラビリティ テストの結果について説明します。Cisco VXI KW+ の作業負荷で実行されたテストに基づくと、このプロファイルを使用する UCS B250 M2 では 80 台の VM をサポートできます。

テスト環境とセットアップ

- ESXi 4.1 上の XenDesktop 5（Provisioning Server による Machine Creation Services の利用なし）
- HVD のプロファイル
  - Windows 7（32 ビット）、1.5 G のメモリと 20 G のディスク スペースを装備
  - 1 vCPU、永続的プール化デスクトップ
- 作業負荷プロファイル：Cisco VXI KW+（Cisco Unified Personal Communicator、IE、Microsoft Office 2007 アプリケーション、Acrobat）、デフォルト スキャン ポリシーを実行する McAfee Move AV 1.5（使用されたスキャン ポリシーについては後述する Move AV のセクションを参照）
- UCS サーバ：B250 M2、192 G のメモリを装備、2 個の 6 コア Intel Xeon（EP）5680 プロセッサ（1 基あたり 3.33 GHz）搭載
- ストレージ：NetApp FAS 3170 上の NFS、PAM2（512 G のキャッシュ）搭載
- 下記のグラフに示すすべてのデータは、IO 統計に関する NetApp ビューを除き、5 秒のポーリング間隔で resxtop を使用して収集されています。
- すべての応答時間は、前述の Scapa TPP を使用して測定されます。
- 下記のデータは、ログイン、作業負荷、およびログアウト フェーズでの数値を示しています。
- このプロファイルに関するデータは、作業負荷フェーズでのみ取得され、グラフ化されています。

アプリケーション応答時間

このプロファイルでの応答時間は、このセクションの初めに定義した合格基準の範囲内に余裕をもって納まりました。

表 43　NetApp を使用する UCS B250 M2 に搭載された ESXi 上の XD5 のアプリケーション応答時間

アプリケーション	最大許容起動時間の合格基準	平均起動時間の測定値（秒）
デスクフォン モードの Cisco Unified Personal Communicator 8.5	5 秒	3.6
Outlook	10 秒	2 秒
Excel	5 秒	6 秒
PowerPoint	5 秒	4 秒
Acrobat	5 秒	4 秒
Internet Explorer	5 秒	3 秒
Word	10 秒	7 秒

テスト結果の概要

上記の「テスト環境とセットアップ」のセクションで説明した導入プロファイルの場合、次のパフォーマンス メトリックを使用する Cisco UCS B250 M2 で 80 台の VM をサポートできます。

- CPU 平均使用率 = 90 %（定常状態）
- メモリ平均使用率 = 65 %
- ストレージ
  - IOPS = 作業負荷開始時に 6500 のピーク読み取り IOPS を測定
  - IO 帯域幅 = 作業負荷開始時に 900 Mbps のピーク読み取り BW を測定
  - IO 遅延 =15 ms 未満
- ネットワーク帯域幅使用率 = 作業負荷開始時のピーク BW 使用率 1 Gbps 超

図 98　NetApp を使用する W7（32 ビット）/XD5/ESXi 4.1 用 UCS B250M2 の CPU 使用率

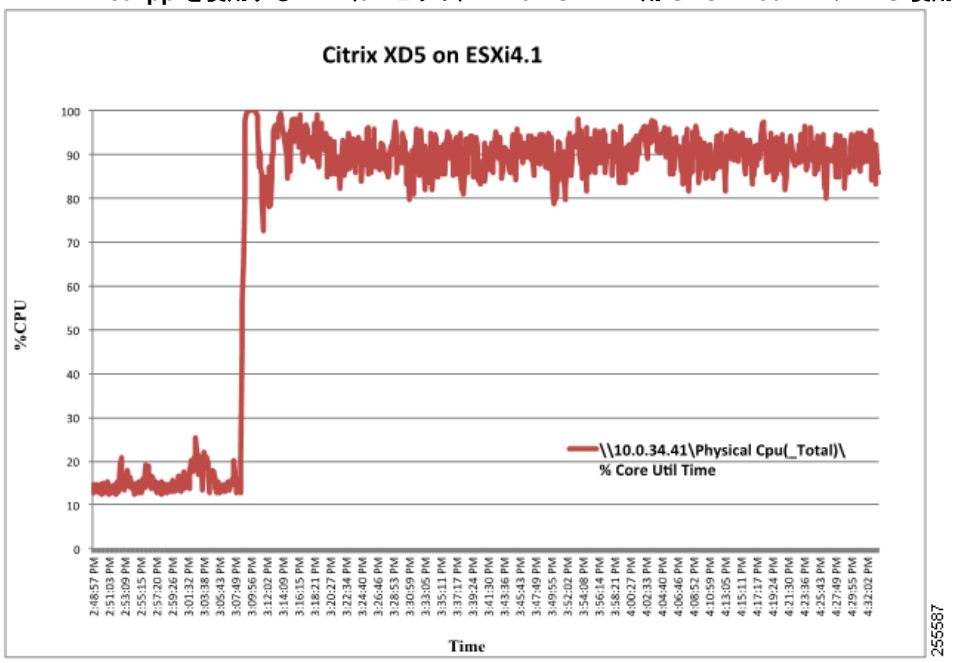


図 99　NetApp を使用する W7（32 ビット）/XD5/ESXi 4.1 用 UCS B250M2 のメモリ使用率

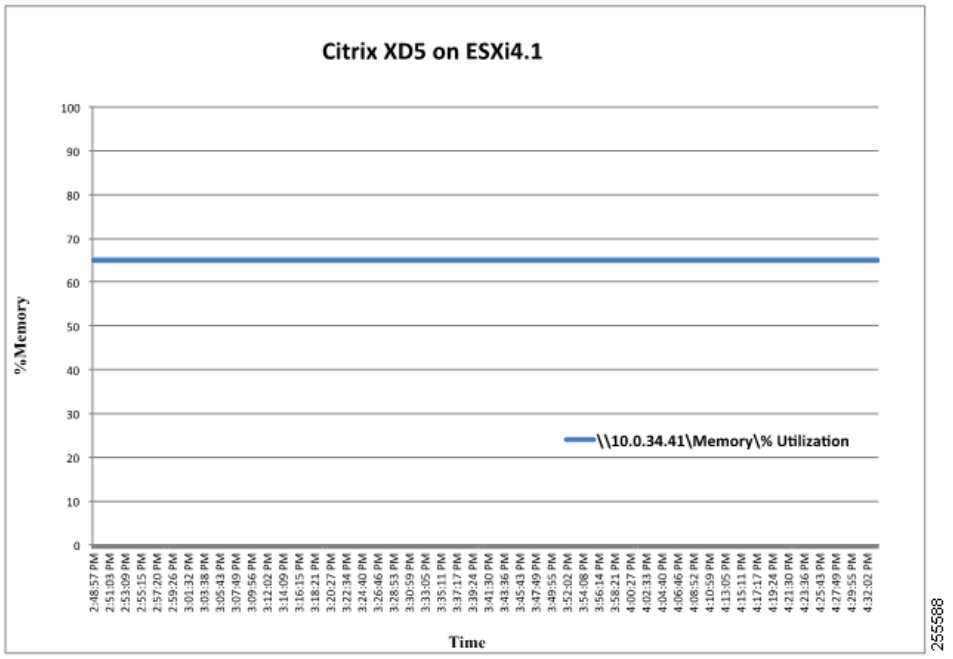


図 100　NetApp を使用する UCS B250M2 上の W7（32 ビット）/XD5/ESXi 4.1 の IOPS

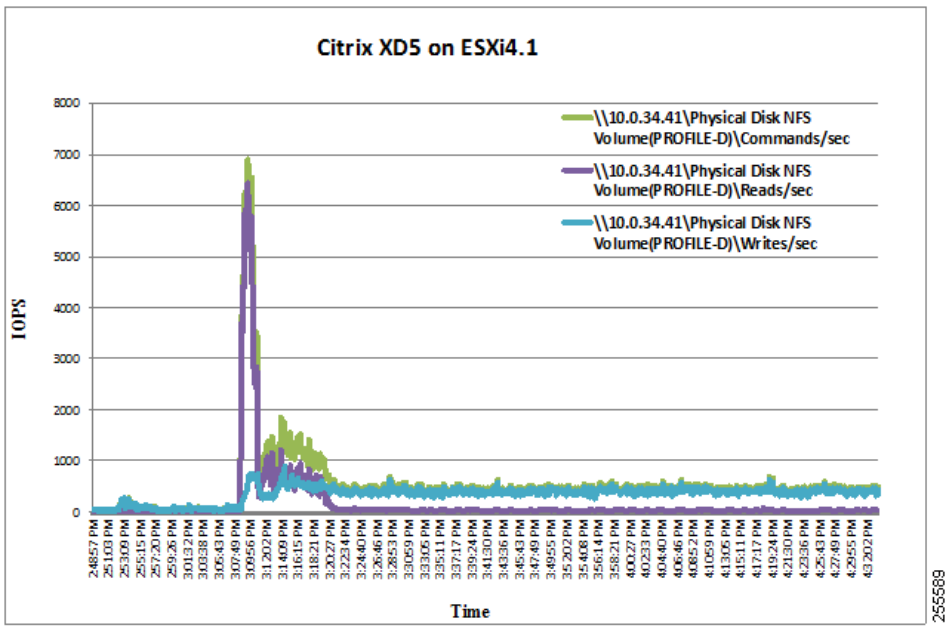


図 101　NetApp を使用する UCS B250M2 上の W7（32 ビット）/XD5/ESXi 4.1 の IO 遅延

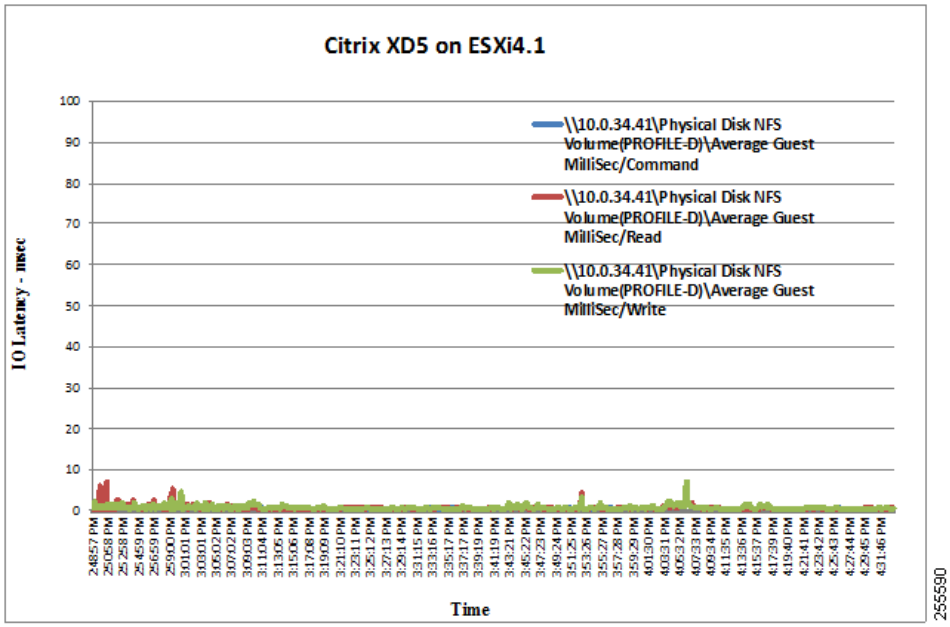


図 102　NetApp を使用する UCS B250M2 上の W7（32 ビット）/XD5/ESXi 4.1 の IO 帯域幅

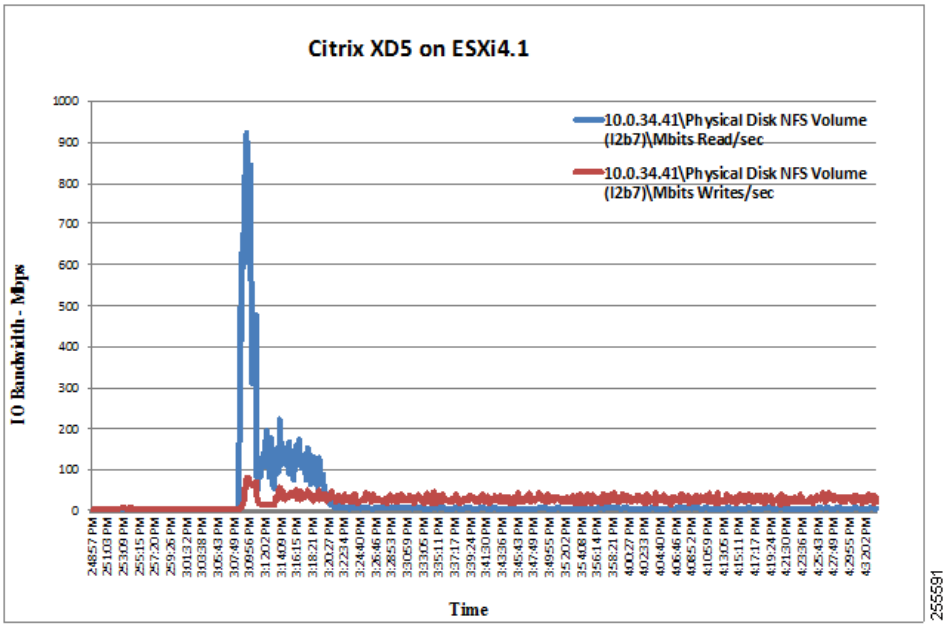


図 103　NetApp FAS 3170 の IO 統計

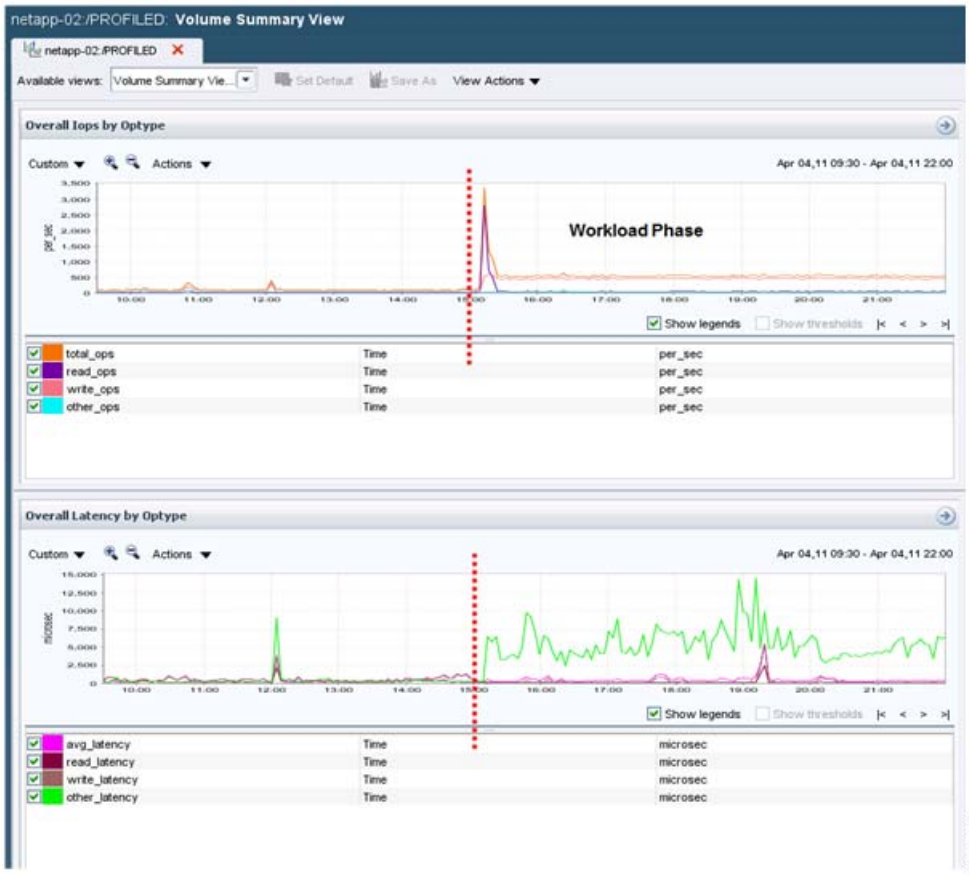
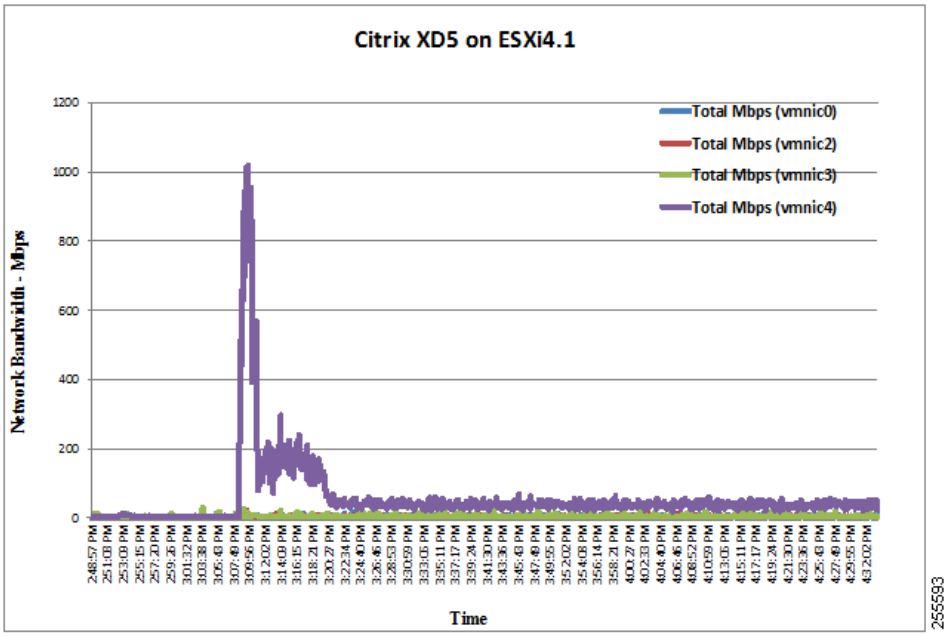


図 104　NetApp を使用する UCS B250M2 上の W7（32 ビット）/XD5/ESXi 4.1 のネットワーク帯域幅



HyperV 2008 R2 上の XenDesktop 5（XD5）：Windows 7（64 ビット）

このセクションでは、Hyper-V 2008 R2 上に XenDesktop 5 を搭載し、W7（64 ビット）デスクトップを実行し、ストレージに NetApp を使用する UCS B230 M1 での単一サーバ スケーラビリティ テストの結果について説明します。Cisco VXI KW+ の作業負荷で実行されたテストに基づくと、このプロファイルを使用する UCS B230 M1 では 70 台の VM をサポートできます。

テスト環境とセットアップ

- Hyper-V 2008 R2 上の XenDesktop 5（Provisioning Server による Machine Creation Services の利用なし）
- HVD のプロファイル
  - Windows 7（64 ビット）、2 G のメモリと 20 G のディスク スペースを装備
  - 1 vCPU、永続的プール化デスクトップ
- 作業負荷プロファイル：Cisco VXI KW+（Cisco Unified Personal Communicator、IE、Microsoft Office 2007 アプリケーション、Acrobat）、デフォルト スキャン ポリシーを実行する McAfee Move AV 1.5（使用されたスキャン ポリシーについては後述する Move AV のセクションを参照）
- UCS サーバ：B230 M1、256 G のメモリを装備、2 個の 8 コア Intel Xeon（EP）7560 プロセッサ（1 基あたり 2.26 GHz）搭載
- ストレージ：iSCSI 接続の NetApp FAS 3170、PAM2（512 G のキャッシュ）搭載
- 下記のグラフに示したすべてのデータは、perfmon を使用して収集されています。
- すべての応答時間は、前述の Scapa TPP を使用して測定されます。
- 下記のデータは、ログイン、作業負荷、およびログアウト フェーズでの数値を示しています。
- このプロファイルに関するデータは、ログイン、作業負荷、およびログアウト フェーズで取得され、グラフ化されています。

アプリケーション応答時間

このプロファイルでの応答時間は、このセクションの初めに定義した合格基準の範囲内に余裕をもって納まりました。

表 44　NetApp を使用する UCS B230 M1 に搭載された HyperV 2008 R2 上の XD5 のアプリケーション応答時間

アプリケーション	最大許容起動時間の合格基準	平均起動時間の測定値（秒）
デスクフォン モードの Cisco Unified Personal Communicator 8.5	5 秒	4.6
Outlook	10 秒	2.7 秒
Excel	5 秒	8 秒
PowerPoint	5 秒	3.2 秒
Acrobat	5 秒	6 秒
Internet Explorer	5 秒	3.2 秒
Word	10 秒	7.3 秒

テスト結果の概要

上記の「テスト環境とセットアップ」のセクションで説明した導入プロファイルの場合、次のパフォーマンス メトリックを使用する Cisco UCS B230 M1 で 70 台の VM をサポートできます。

- CPU 平均使用率 = 40 %（定常状態）
- メモリ平均使用率 = 70 %
- ストレージ
  - IOPS = 作業負荷開始時に 8000 のピーク読み取り IOPS を測定
  - IO 帯域幅 = 作業負荷開始時に 1 GBps 超のピーク読み取り BW を測定
  - IO 遅延 =15 ms 未満

ネットワーク帯域幅使用率 = 作業負荷開始時のピーク BW 使用率 1 Gbps 超

図 105　NetApp を使用する W7（64 ビット）/XD5/HyperV 用 UCS B230 M1 の CPU 使用率

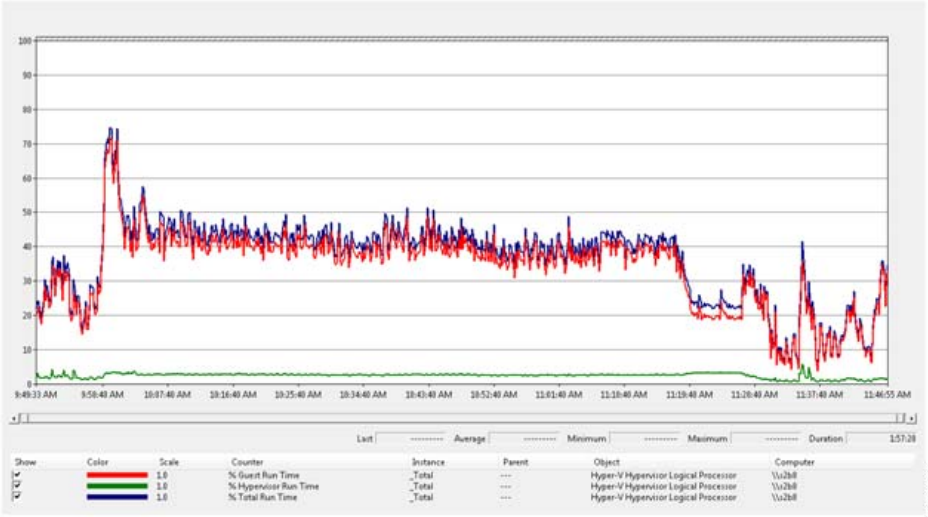


図 106　NetApp を使用する W7（64 ビット）/XD5/HyperV 用 UCS B230 M1 のメモリ使用率

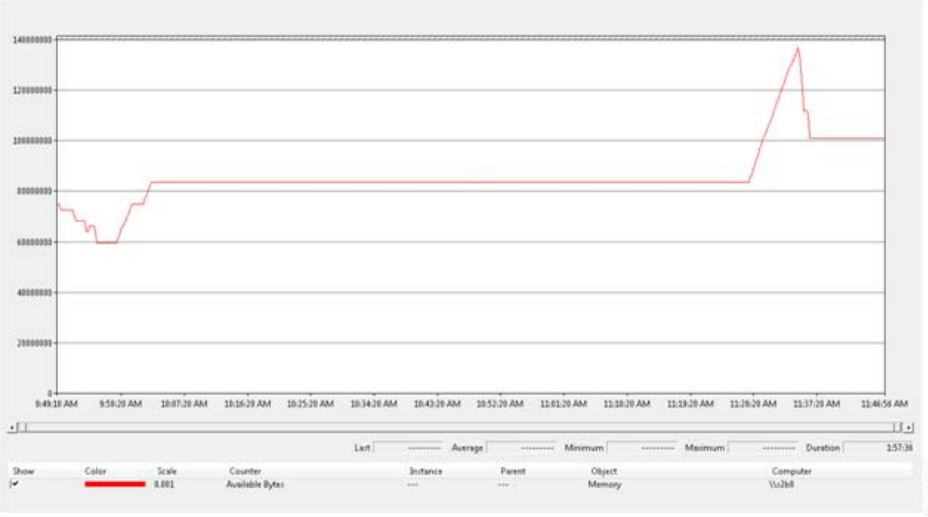


図 107　NetApp を使用する UCS B230 M1 上の W7（64 ビット）/XD5/HyperV のコンテキスト スイッチ / 秒

図 108　NetApp を使用する UCS B230 M1 上の W7（64 ビット）/XD5/HyperV の IOPS

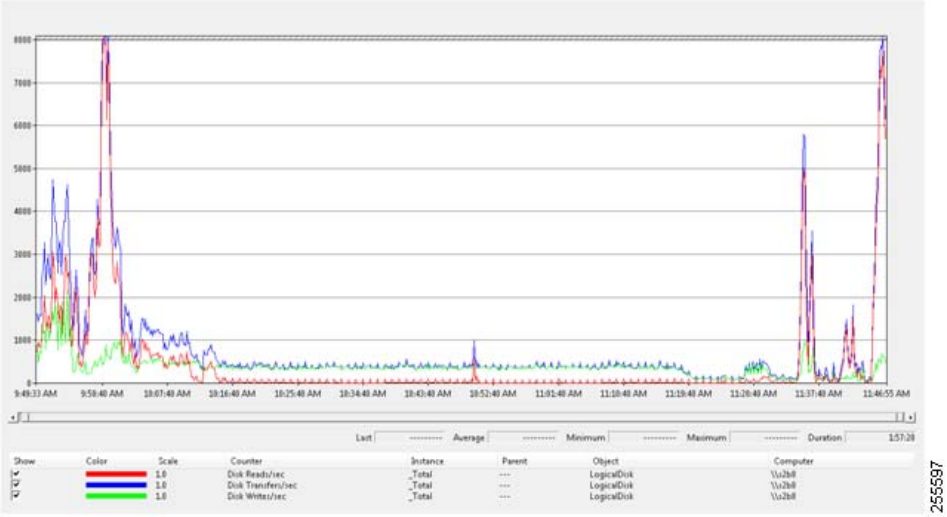


図 109　NetApp を使用する UCS B230 M1 上の W7（64 ビット）/XD5/HyperV の IO 帯域幅

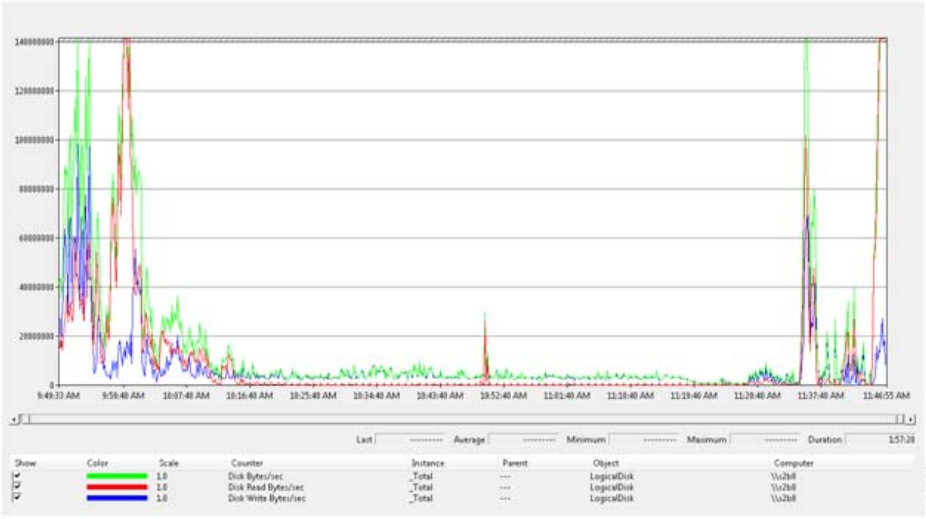


図 110　NetApp を使用する UCS B230 M1 上の W7（64 ビット）/XD5/HyperV の IO 遅延

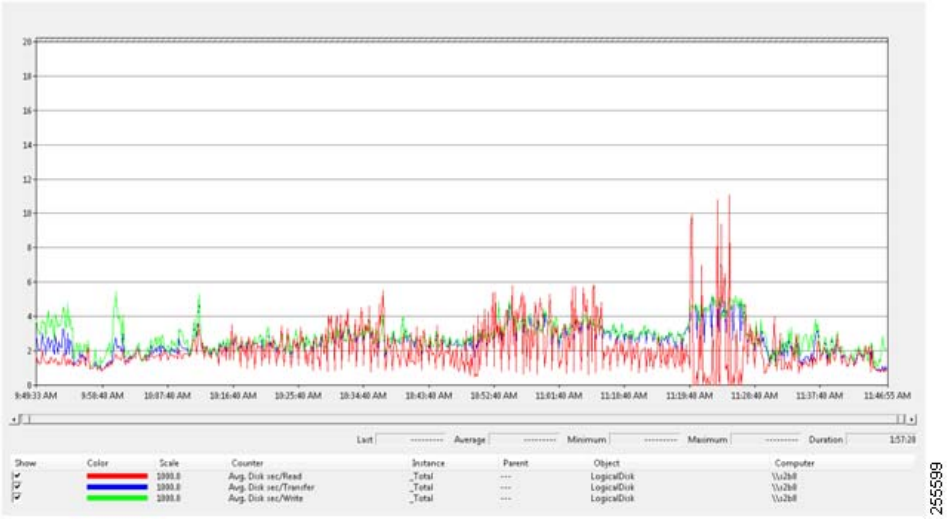
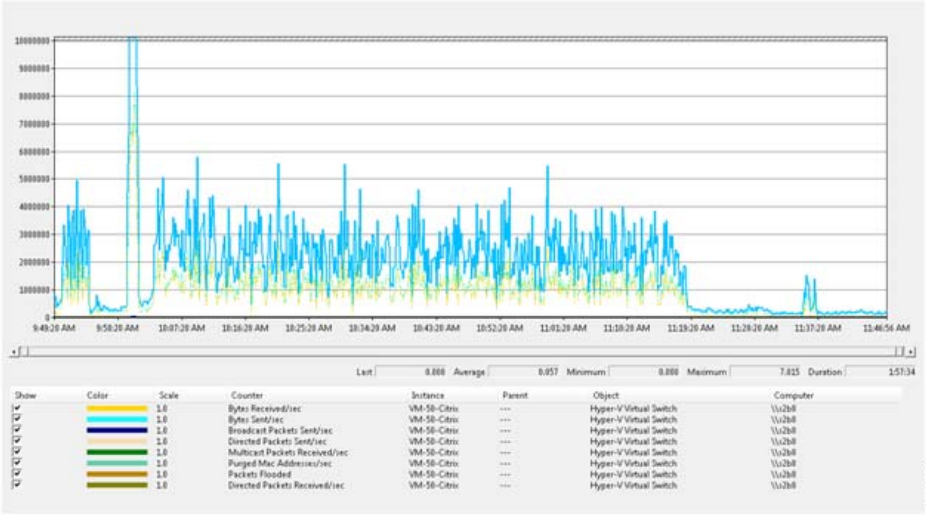


図 111　NetApp を使用する UCS B230 M1 上の W7（64 ビット）/XD5/HyperV のネットワーク帯域幅使用率



ESXi 上の McAfee MoveAV、XD5 搭載

この導入プロファイルをテストする目的は、McAfee MoveAV というアンチウイルス ソフトウェアがサーバ パフォーマンスに与える影響を VM 密度の面から把握することです。この章で取り上げている他の導入プロファイルと異なり、ここでのテストは Cisco VXI ナレッジ ワーカー プロファイルを使用して実施されました。したがって、デスクフォン モードの Cisco Unified Personal Communicator 8.5 はこのテストでは除外されています。作業負荷プロファイルに Move AV を追加することによる影響を測定するために、Move AV を使用せずにベースライン テストが実施されました。Windows 7（32 ビット）デスクトップと NetApp ストレージを使用し、XenDesktop 5 と ESXi を搭載した UCS B250 M2 上の Move AV に対して実施された SSS テストの結果を下記に示します。

このテストに基づくと、デフォルトのスキャン ポリシーが設定された Move AV を、UCS B250 M2 上で動作するナレッジ ワーカー作業負荷に追加した場合、VM 密度に与える影響は最大 10 ～ 15 % です。MoveAV を使用してこのプロファイルでサポートされる VM 密度は、80% の CPU で 100 VM です。一方、同じプロファイルとサーバを使用したベースライン テストでは、MoveAV なしで 110 VM をサポートできます。Move AV を使用したテストの結果の詳細を以下に示します。

テスト環境とセットアップ

- ESXi 4.1 上の XenDesktop 5（Machine Creation Services を使用、Provisioning Server なし）
- HVD のプロファイル
  - Windows 7（32 ビット）、1.5 G のメモリと 20 G のディスク スペースを装備
  - 1 vCPU、永続的プール化デスクトップ
- 作業負荷プロファイル：Cisco VXI KW（IE、Microsoft Office 2007 アプリケーション、Acrobat）、デフォルト スキャン ポリシー（下記を参照）を実行する McAfee Move AV 1.5
- UCS サーバ：B250 M2、192 G のメモリを装備、2 個の 6 コア Intel Xeon（EP）5680 プロセッサ（1 基あたり 3.33 GHz）搭載
- ストレージ：NetApp FAS 3170 上の NFS、PAM2（512 G のキャッシュ）搭載

- 下記のグラフに示すすべてのデータは、5 秒のポーリング間隔で resxtop を使用して収集されています。
- すべての応答時間は、前述の Scapa TPP を使用して測定されます。
- 下記のデータは、ログイン、作業負荷、およびログアウト フェーズでの数値を示しています。
- データはログイン、作業負荷、及びログアウト フェーズで取得され、グラフ化されています。

スキャン ポリシー

表 45　　McAfee Move AV スキャン ポリシー

McAfee Move AV スキャン ポリシー	
デフォルトのスキャン設定を使用。X はオンを示します。	
スキャン ファイル	X：ディスクへの書き込み時 X：ディスクからの読み取り時
	ネットワーク ドライブ上
	X：バックアップ用に開く
スキャンするファイル タイプ	X：全ファイル
除外するファイル	McAfee\Common FrameWork

アプリケーション応答時間

このプロファイルでの応答時間は、このセクションの初めに定義した合格基準の範囲内に余裕をもって納まりました。

表 46　　XD5 上の MoveAV テストのアプリケーション応答時間

アプリケーション	最大許容起動時間の合格基準	平均起動時間の測定値（秒）
デスクフォン モードの Cisco Unified Personal Communicator 8.5	このテストでは除外	このテストでは除外
Outlook	10 秒	1.6 秒
Excel	5 秒	6 秒
PowerPoint	5 秒	4 秒
Acrobat	5 秒	3 秒
Internet Explorer	5 秒	3.3 秒
Word	10 秒	8 秒

McAfee VSE サーバ統計

1 対の VSE サーバをオフロード サーバとして使用し、作業負荷の実行中にリアル タイムでスキャンを行います。下記の統計データは、スキャン要求の数（「Total av scan req」）、以前にスキャンしたアイテムに基づくキャッシュ ヒット数（「Cksum cache hit」）、およびスキャン要求に対する平均応答時間（平均 要求プロセス時間）を示しています。キャッシュ ヒット率が非常に小さいことに注意してください。これはテスト中、要求の大多数が新規要求として扱われ、スキャンするためにオフロード サーバへ送信する必要があったことを意味します。これらの要求に対する応答時間は、McAfee が推奨する 0.4 ～ 0.5 秒の範囲内に納まりました。

VS1

図 112　　McAfee VSE1 サーバ統計

VS2

図 113　　McAfee VSE2 サーバ統計

テスト結果の概要

- このプロファイルに対するパフォーマンス メトリックの概要は次のとおりです。
- CPU 平均使用率 = 80 %（定常状態）
- メモリ平均使用率 = 最大 80 %
- ストレージ
  - IOPS = ピーク書き込み IOPS は 800 以下、ピーク読み取り IOPS は 100 未満
  - IO 帯域幅 = 100 Mbps 以下
  - IO 遅延 = 10 ms 未満
- ネットワーク帯域幅使用率 = BW 平均使用率 100 Mbps 未満

図 114　MoveAV を使用する W7（32 ビット）/XD5/ESXi 4.1 用 B250M2 の CPU 使用率

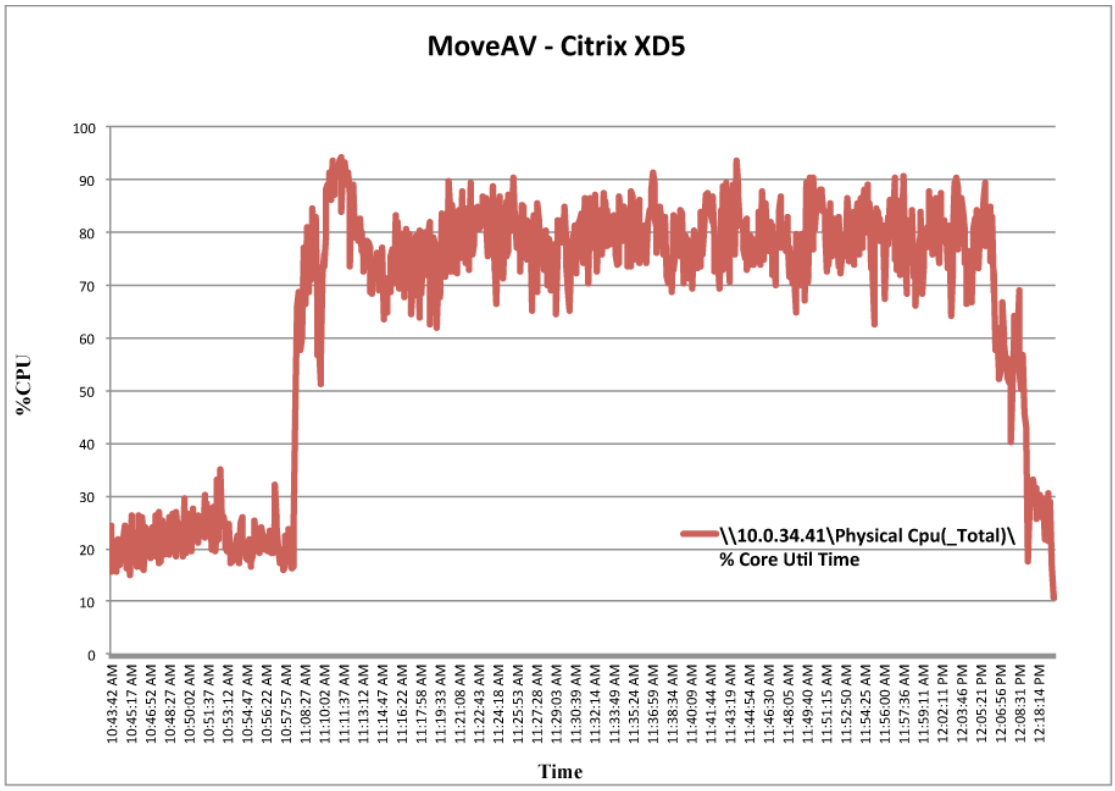


図 115　MoveAV を使用する W7（32 ビット）/XD5/ESXi 4.1 用 B250M2 のメモリ使用率

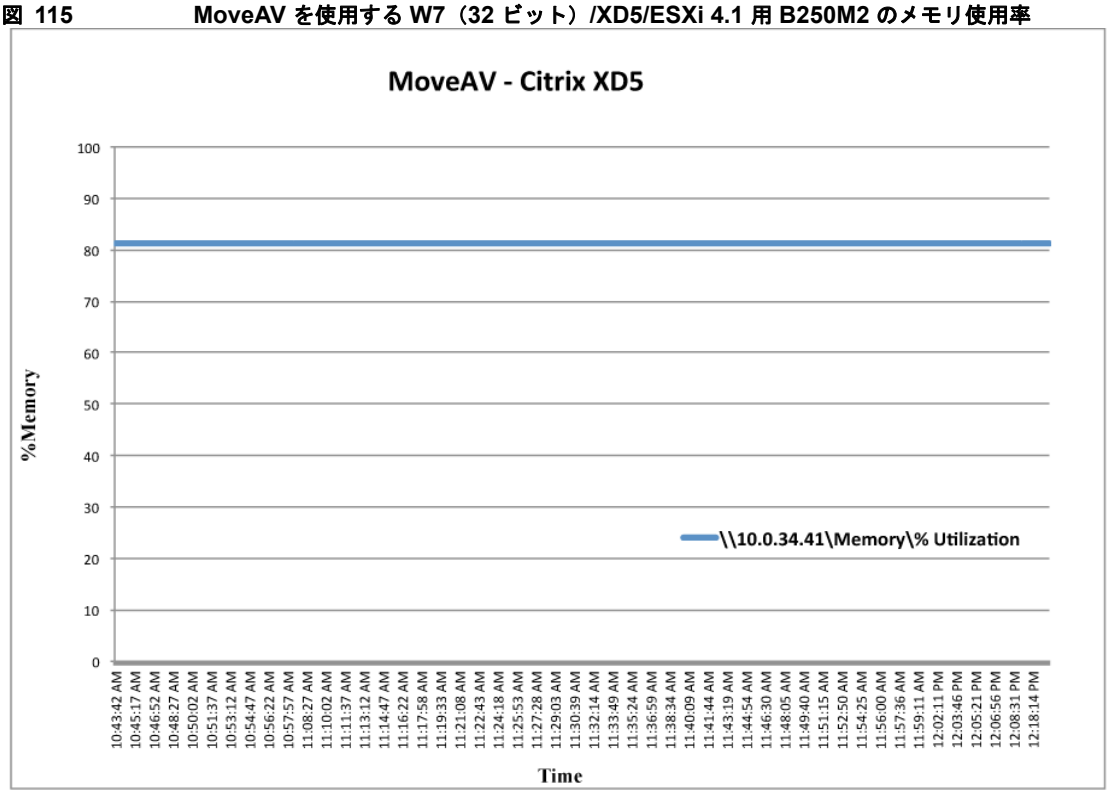


図 116　MoveAV を使用する W7（32 ビット）/XD5/ESXi 4.1 用 B250M2 の IOPS 測定値

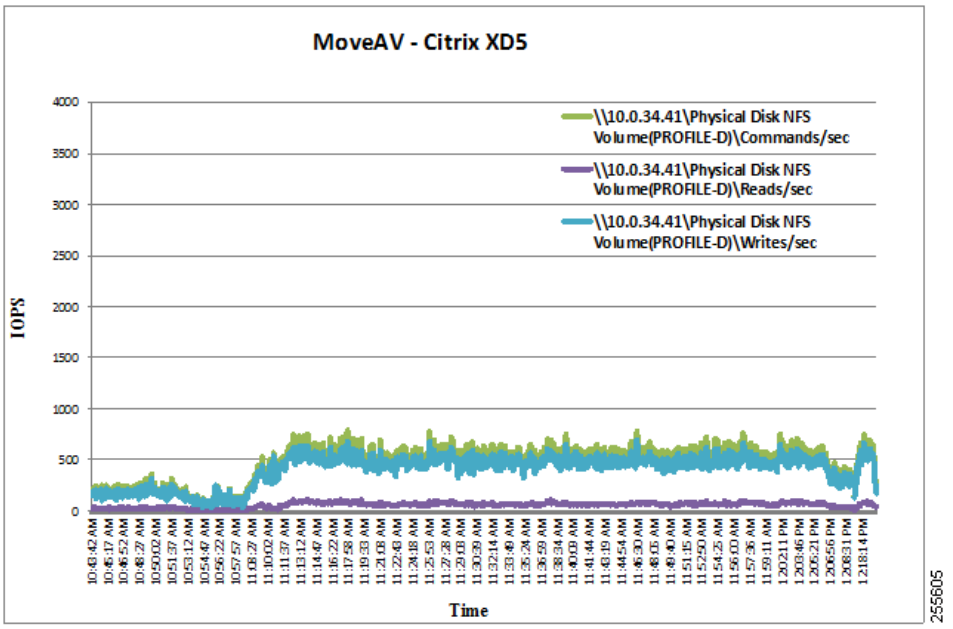


図 117　MoveAV を使用する W7（32 ビット）/XD5/ESXi 4.1 用 B250M2 の IO 帯域幅測定値

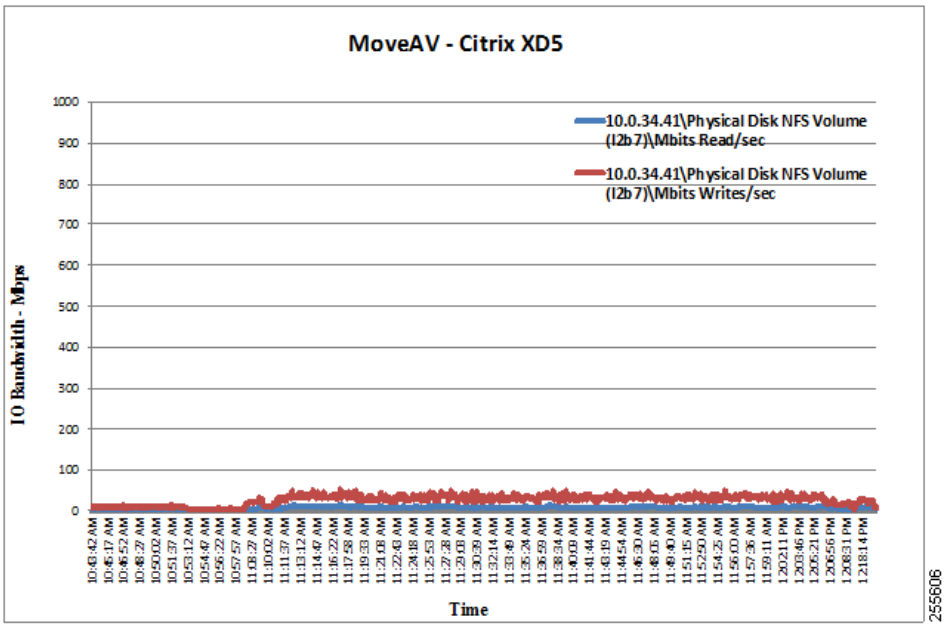


図 118　MoveAV を使用する W7（32 ビット）/XD5/ESXi 4.1 用 B250M2 の IO 遅延測定値

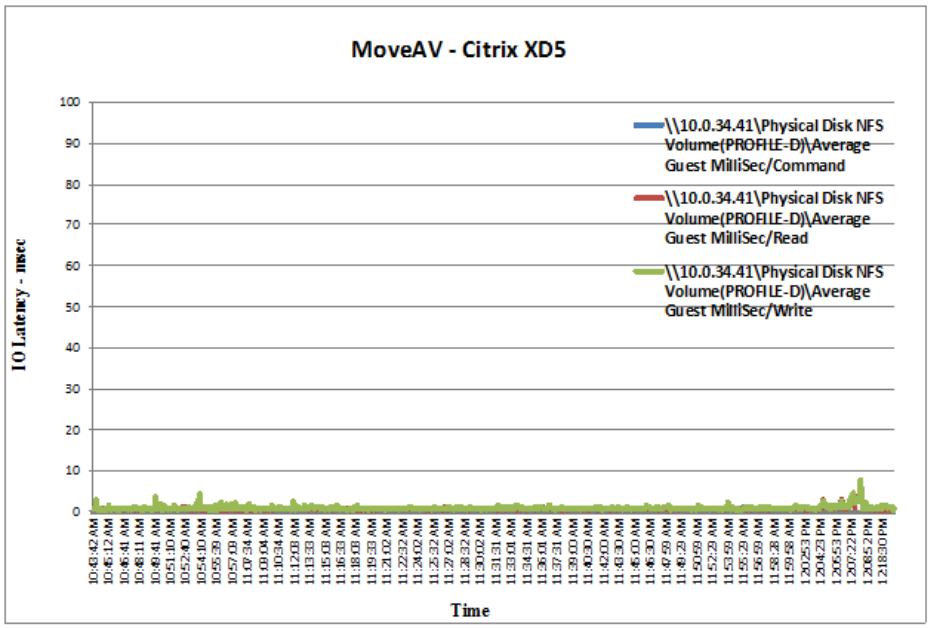


図 119　MoveAV を使用した W7（32 ビット）/XD5/ESXi 4.1 の NetApp IO 統計

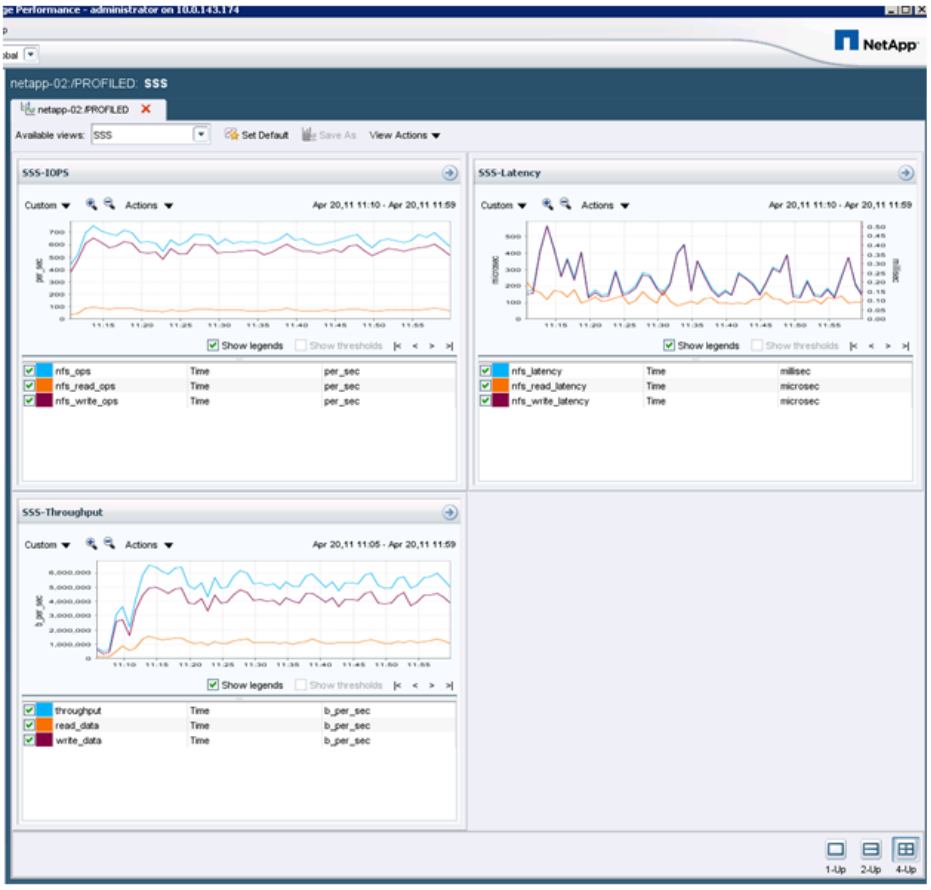
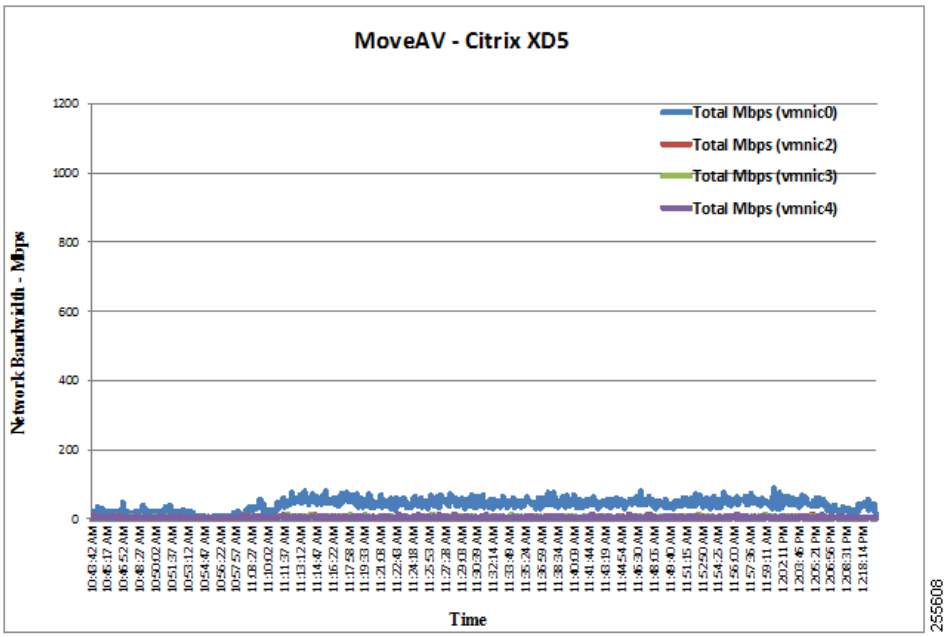


図 120　MoveAV と基本的な KW 作業負荷を使用した W7（32 ビット）/XD5/ESXi 4.1 用 B250M2 のネットワーク帯域幅測定値



Hyper-V 2008 R2 上の XenDesktop 5（XD5）: Windows XP

このセクションでは、Hyper-V 2008 R2 上に XenDesktop 5 を搭載し、Windows XP SP3 デスクトップを実行し、EMC Unified Storage を使用する UCS B250 M2 での単一サーバ スケーラビリティ テストの結果について説明します。Cisco VXI KW+ の作業負荷で実行されたテストに基づくと、この作業負荷プロファイルを使用する UCS B250 M2 では 60 台の VM をサポートできます。

テスト環境とセットアップ

- Hyper-V 2008 R2 上の XenDesktop 5（Machine Creation Services を使用）
- HVD のプロファイル
  - Windows XP SP3、1 G のメモリと 20 G のディスク スペースを装備
  - 1 vCPU、プール化デスクトップ
- 作業負荷プロファイル：Cisco VXI KW+（デスクフォン モードの Cisco Unified Personal Communicator 8.5、IE、Microsoft Office 2007 アプリケーション、Acrobat）、デフォルト スキャン ポリシーを実行する McAfee Move AV 1.5（使用されたスキャン ポリシーについては後述する Move AV のセクションを参照）
- UCS サーバ：B250 M2、192 G のメモリを装備、2 個の 6 コア Intel Xeon（EP）5680 プロセッサ（1 基あたり 3.33 GHz）搭載
- ストレージ：FCoE 接続の EMC Unified Storage
- 下記のグラフに示したすべてのデータは、perfmon を使用して収集されています。
- すべての応答時間は、前述の Scapa TPP を使用して測定されます。
- 下記のデータは、ログイン、作業負荷、およびログアウト フェーズでの数値を示しています。

アプリケーション応答時間

このプロファイルでの応答時間は、このセクションの初めに定義した合格基準の範囲内に余裕をもって納まりました。

表 47　UCS B250 M2 と EMC Unified Storage を使用する Hyper-V 2008 R2 上の XD5（Windows XP SP3）のアプリケーション応答時間

アプリケーション	最大許容起動時間の合格基準	平均起動時間の測定値（秒）
デスクフォン モードの Cisco Unified Personal Communicator 8.5	5 秒	1.5 秒
Outlook	10 秒	4.5 秒
Excel	5 秒	1.5 秒
PowerPoint	5 秒	96 秒
Acrobat	5 秒	1.5 秒
Internet Explorer	5 秒	5.3 秒
Word	10 秒	9.2 秒

テスト結果の概要

上記の「テスト環境とセットアップ」のセクションで説明した導入プロファイルの場合、次のパフォーマンス メトリックを使用する Cisco UCS B230 M1 で 70 台の VM をサポートできます。

- CPU 平均使用率 = 70 %（定常状態）
- メモリ平均使用率 = 最大 40 %
- ストレージ
  - IOPS = ピーク読み取り IOPS 1000 未満
  - IO 帯域幅 = 作業負荷開始時に 128 Mbps 超のピーク読み取り BW を測定
  - IO 遅延 = 20 ms 未満
- ネットワーク帯域幅使用率 = 作業負荷開始時のピーク BW 使用率 40 Mbps 未満

図 121　EMC Unified Storage を使用する Windows XP/XD5/Hyper-V 用 UCS B250 M2 の CPU 使用率

図 122　EMC Unified Storage を使用する Windows XP/XD5/Hyper-V 用 UCS B250 M2 の使用可能メモリ

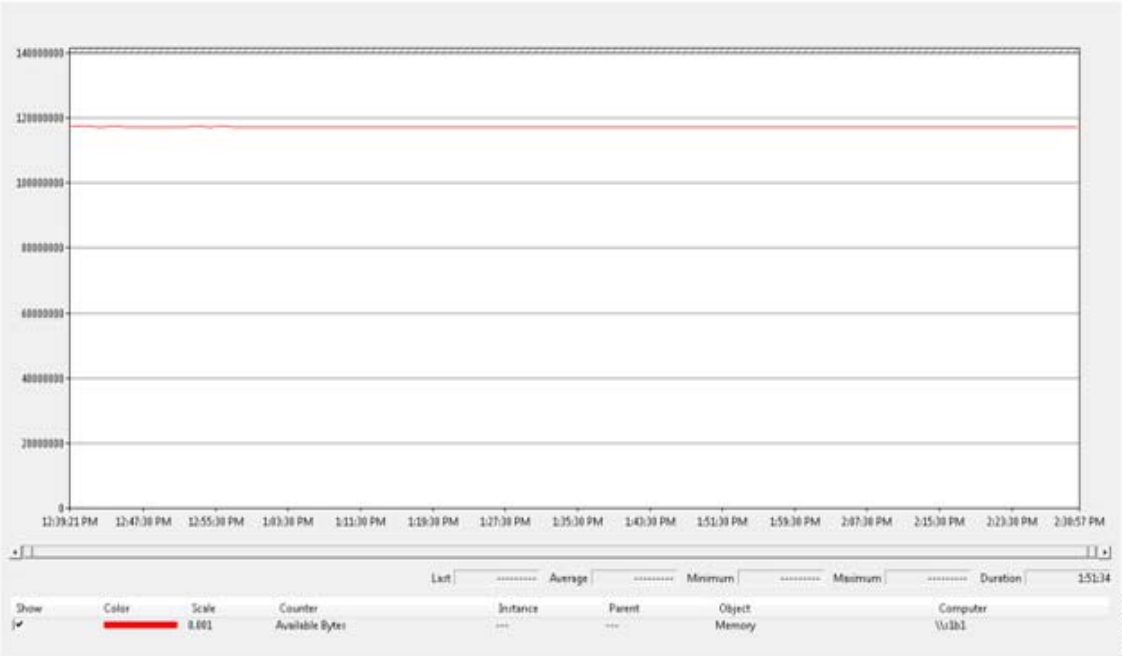


図 123　EMC Unified Storage を使用する UCS B250 M2 上の Windows XP/XD5/Hyper-V の IOPS

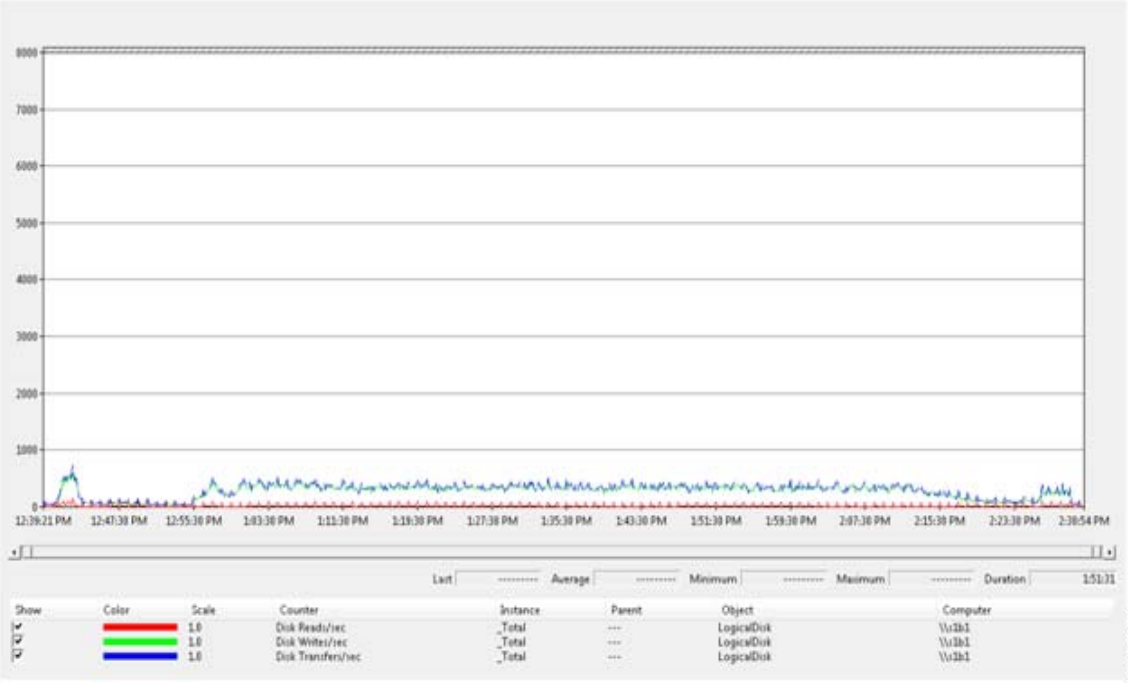


図 124　EMC Unified Storage を使用する UCS B250 M2 上の Windows XP/XD5/Hyper-V の IO 帯域幅

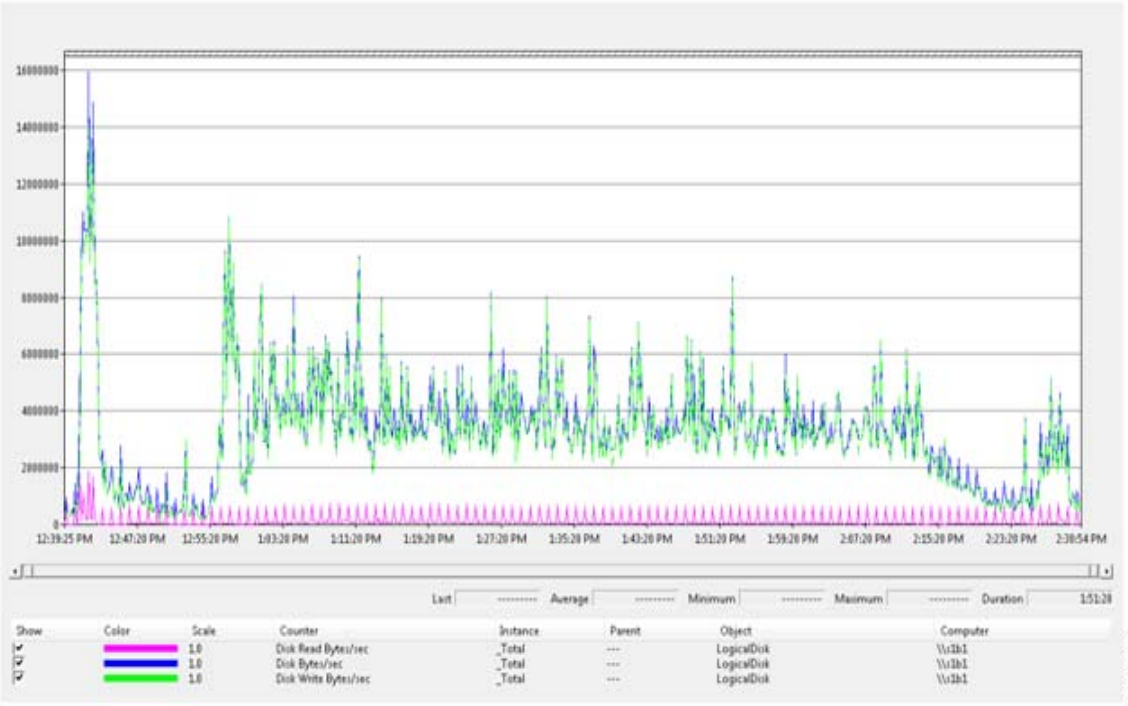


図 125　EMC Unified Storage を使用する UCS B250 M2 上の Windows XP/XD5/Hyper-V の IO 遅延

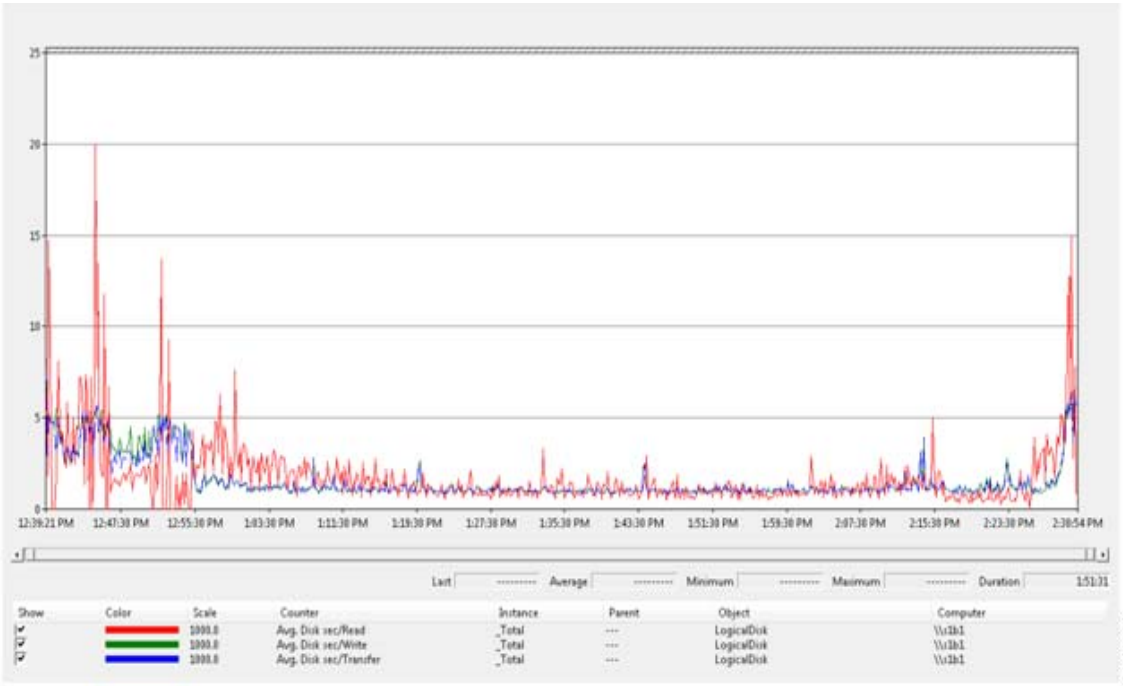


図 126　EMC Unified Storage の IO 統計

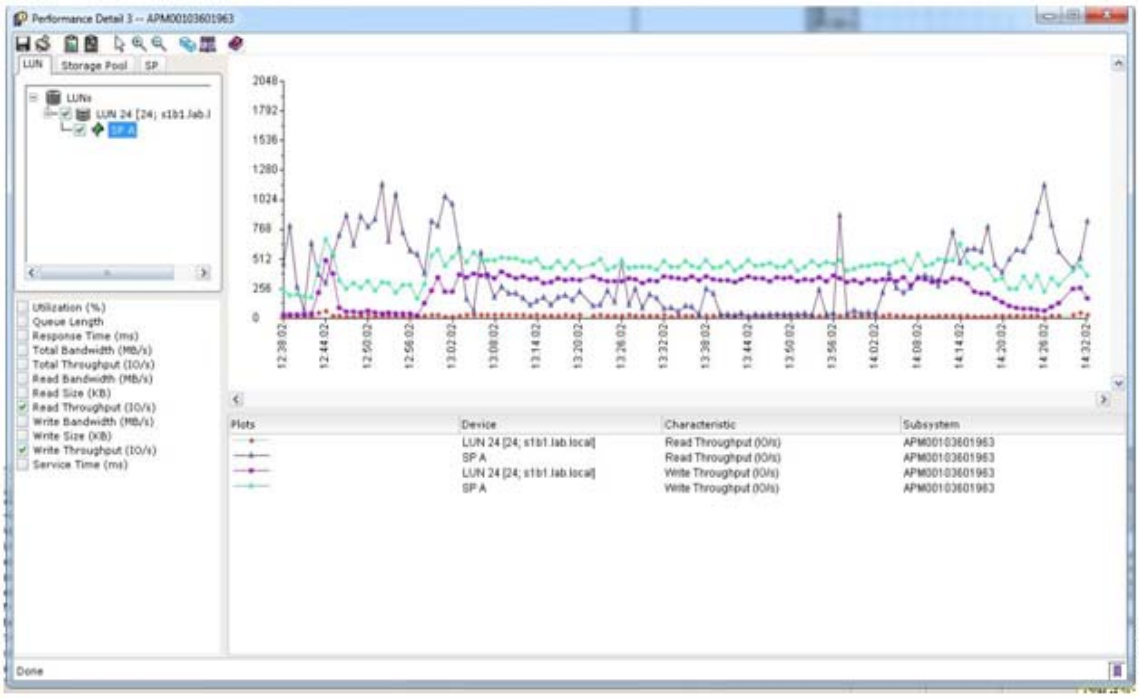
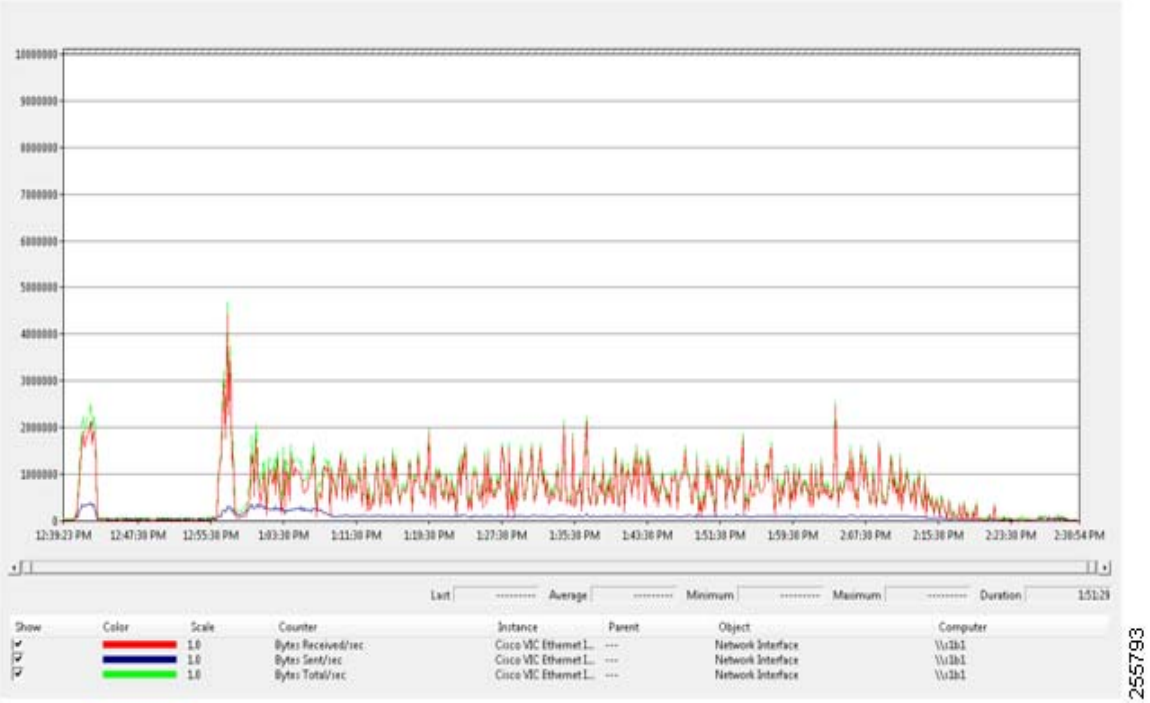


図 127　EMC Unified Storage を使用する UCS B250 M2 上の Windows XP/XD5/Hyper-V のネットワーク帯域幅使用率



XenServer 5.6 FP1 上の XenDesktop 5（XD5）

このセクションでは、XenServer 5.6 FP1 上に XenDesktop 5 を搭載し、Windows 7（32 ビット）デスクトップを実行し、ストレージに NetApp を使用する UCS B250 M2 での単一サーバ スケーラビリティ テストの結果について説明します。Cisco VXI KW+ の作業負荷で実行されたテストに基づくと、この作業負荷プロファイルを使用する UCS B250 M2 では 110 台の VM をサポートできます。

テスト環境とセットアップ

- XenServer 5.6 FP1 上の XenDesktop 5（Provisioning Services を使用）
- HVD のプロファイル
  - Windows 7（32 ビット）、1.5 G のメモリと 20 G のディスク スペースを装備
  - 1 vCPU、プール化デスクトップ
- 作業負荷プロファイル：Cisco VXI KW+（デスクフォン モードの Cisco Unified Personal Communicator 8.5、IE、Microsoft Office 2007 アプリケーション、Acrobat）、デフォルト スキャン ポリシーを実行する McAfee Move AV 1.5（使用されたスキャン ポリシーについては後述する Move AV のセクションを参照）
- UCS サーバ：B250 M2、192 G のメモリを装備、2 個の 6 コア Intel Xeon（EP）5680 プロセッサ（1 基あたり 3.33 GHz）搭載
- ストレージ：NFS 接続の NetApp FAS 3170、PAM2（512 G のキャッシュ）搭載
- すべての応答時間は、前述の Scapa TPP を使用して測定されます。
- 下記のデータは、ログイン、作業負荷、およびログアウト フェーズでの数値を示しています。

アプリケーション応答時間

このプロファイルでの応答時間は、このセクションの初めに定義した合格基準の範囲内に余裕をもって納まりました。

表 48　UCS B250 M2 と NetApp FAS 3170 を使用する XS 5.6 FP1 上の XD5 のアプリケーション応答時間

アプリケーション	最大許容起動時間の合格基準	平均起動時間の測定値（秒）
デスクフォン モードの Cisco Unified Personal Communicator 8.5	5 秒	1.4 秒
Outlook	10 秒	2.1 秒
Excel	5 秒	82 秒
PowerPoint	5 秒	54 秒
Acrobat	5 秒	50 秒
Internet Explorer	5 秒	3.1 秒
Word	10 秒	7.0 秒

テスト結果の概要

上記の「テスト環境とセットアップ」のセクションで説明した導入プロファイルの場合、次のパフォーマンス メトリックを使用する Cisco UCS B250 M2 で 110 台の VM をサポートできます。

- CPU 平均使用率 = 90 %（定常状態）
- メモリ平均使用率 = 最大 90 %
- ストレージ
  - IOPS = ピーク読み取り IOPS 1800 未満
  - IO 遅延 = 5 ms 未満
- ネットワーク帯域幅使用率 = 作業負荷開始時のピーク BW 使用率 250 Mbps 未満

図 128　NetApp FAS 3170 を使用する Windows 7（32 ビット）/XD5/XS5.6 FP1 用 UCS B250 M2 の CPU 使用率

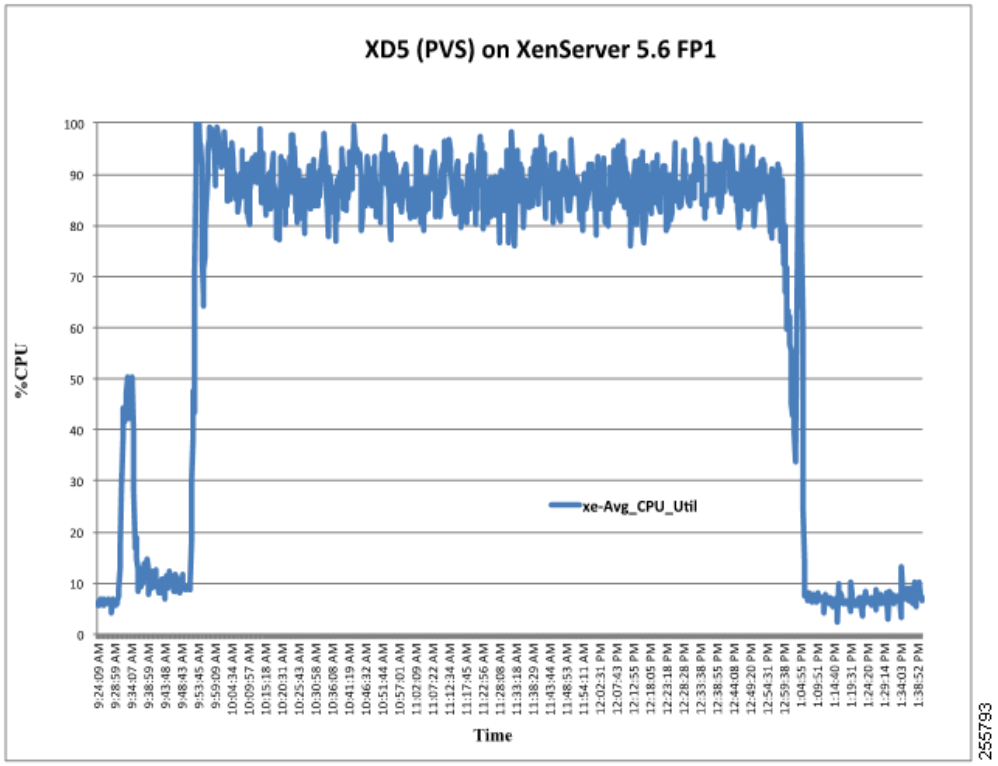


図 129　NetApp FAS 3170 を使用する Windows 7（32 ビット）/XD5/XS5.6 FP1 用 UCS B250 M2 のメモリ使用率

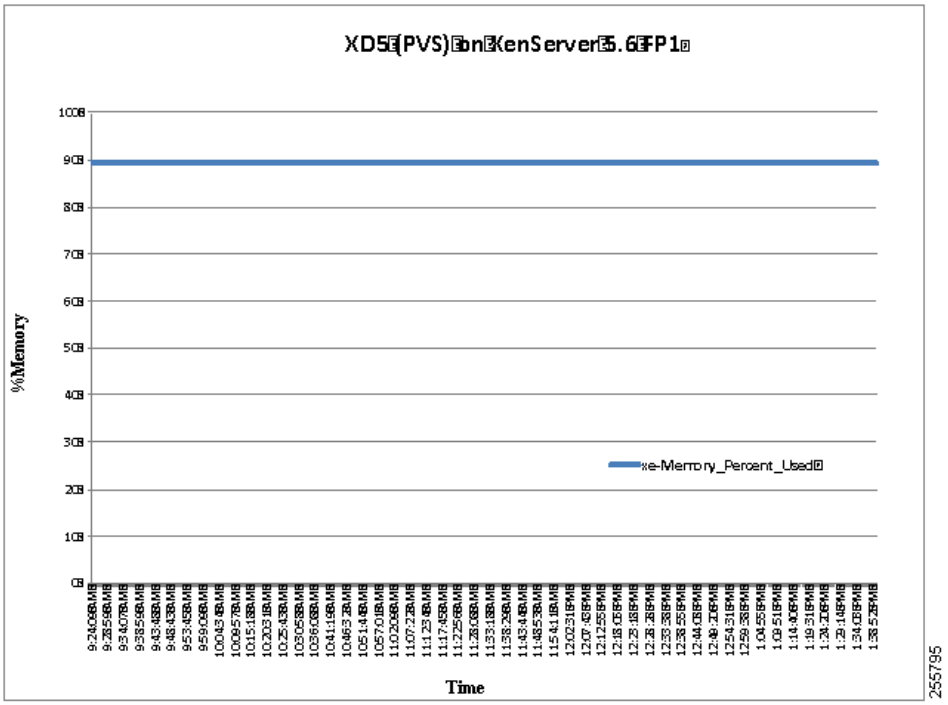


図 130　NetApp FAS 3170 を使用する Windows 7（32 ビット）/XD5/XS5.6 FP1 の IOPS

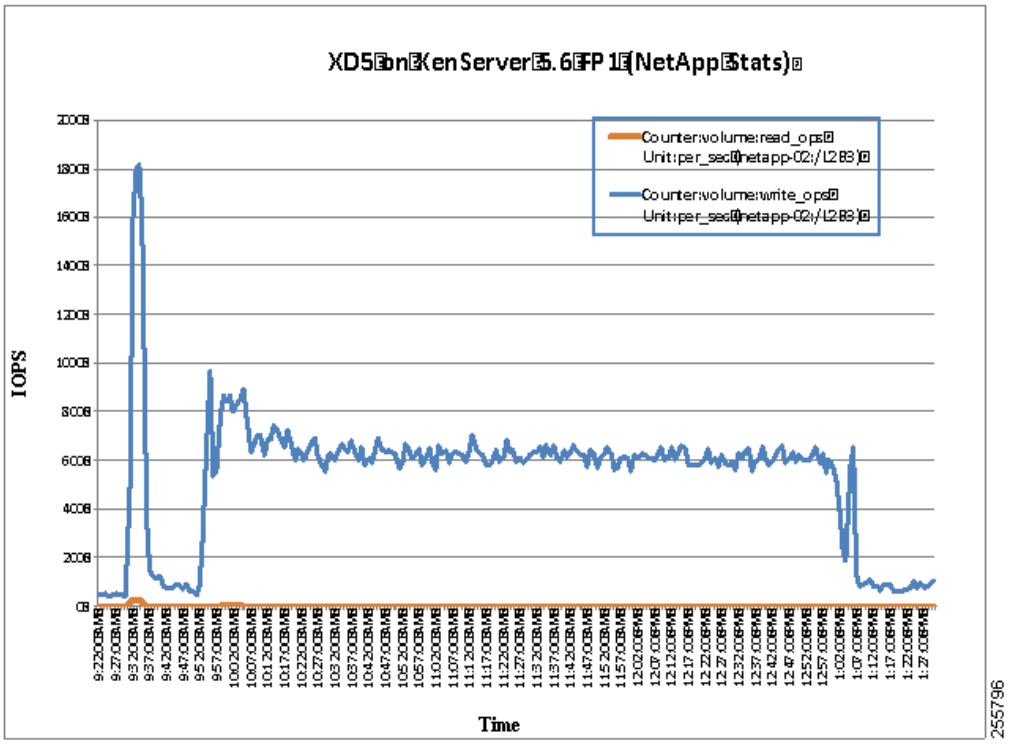


図 131　NetApp FAS 3170 を使用する Windows 7（32 ビット）/XD5/XS5.6 FP1 の IO 遅延

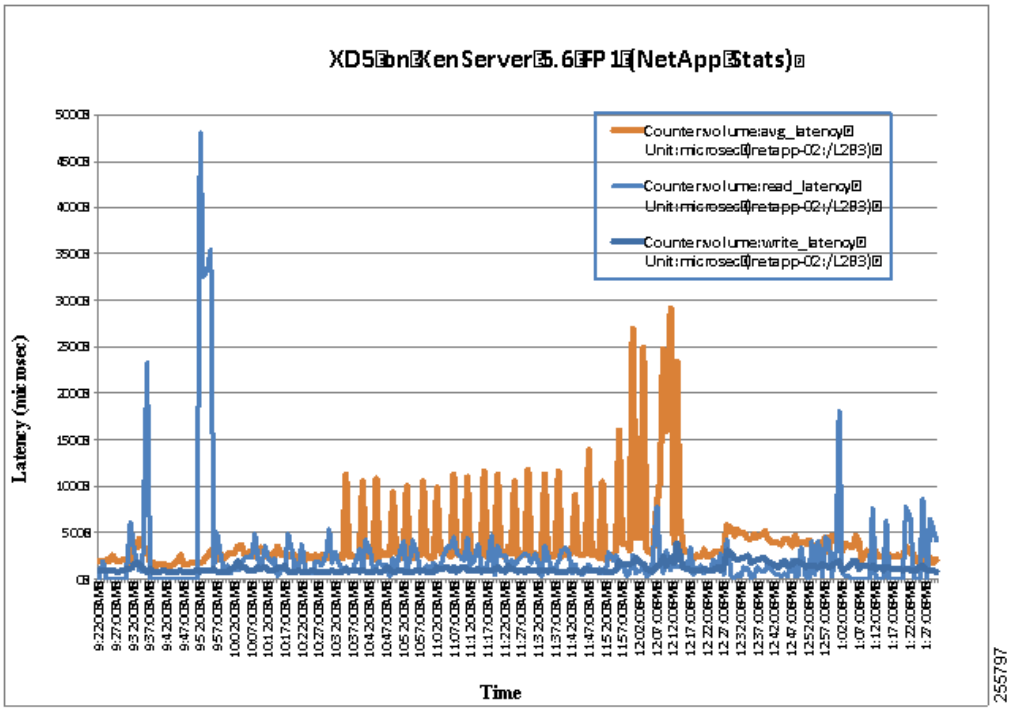
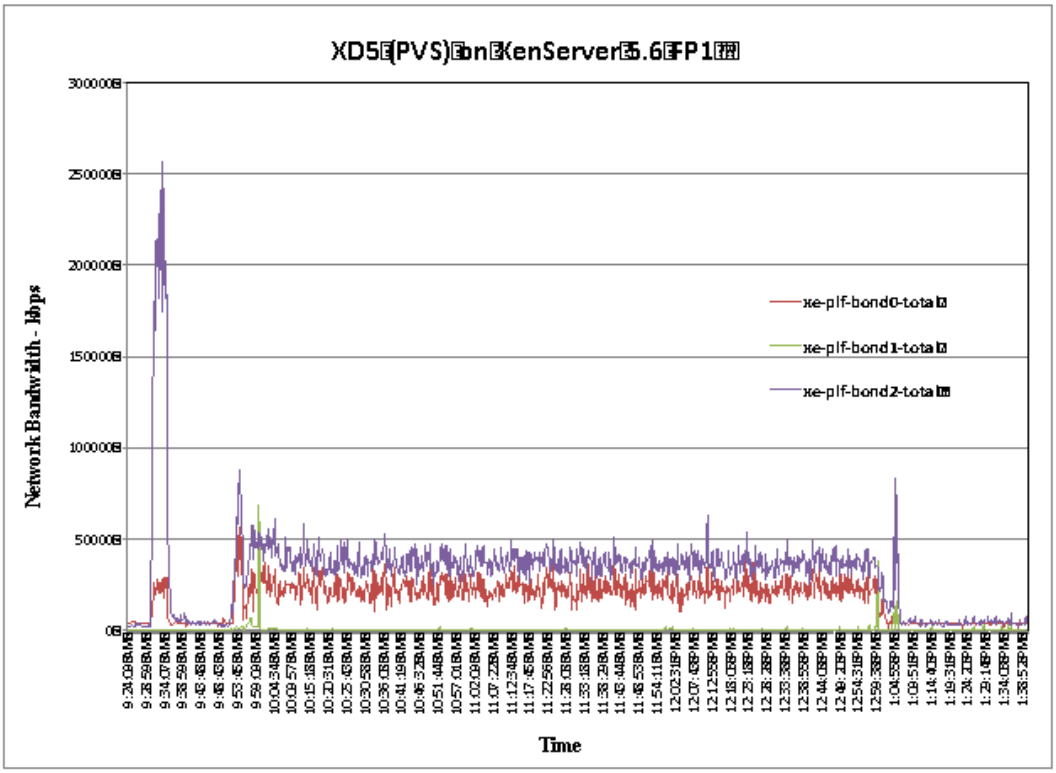


図 132　NetApp FAS 3170 を使用する Windows 7（32 ビット）/XD5/XS5.6 FP1 のネットワーク帯域幅使用率



アプリケーション特性評価の結果

このセクションでは、Citrix XenDesktop5 環境内のさまざまなシスコ コラボレーション アプリケーションについて Cisco VXI で実施されたアプリケーション特性評価の結果を詳しく説明します。エンドツーエンド Cisco VXI システムでの XenDesktop 5 に関するアプリケーション特性評価の概要を次に示します。

- デスクフォン モードの Cisco Unified Personal Communicator 8.5：Cisco UCS B250 M2 サーバ上の XenDesktop 5 と ESXi 4.1
- デスクフォン モードの Cisco Unified Communications Integration for Microsoft Office Communicator 8.5：Cisco UCS B250 M2 サーバ上の XenDesktop 5 と ESXi 4.1
- Cisco UC Integration for WebEx Connect 7：Cisco UCS B200 M2 サーバ上の XenDesktop 5 と ESXi 4.1

上記のすべてのテストは、このドキュメントで前述した Cisco VXI システム アーキテクチャを基盤とするエンドツーエンドの Cisco VXI ネットワークで実施されました。

XenDesktop 5 と ESXi 4.1 を使用したデスクフォン モードの Cisco Unified Personal Communicator 8.5

このセクションでは、UCS B250 M2 シリーズ サーバ上でデスクフォン モードの Cisco Unified Personal Communicator 8.5 を実行する XenDesktop 5 仮想デスクトップに対して実施されたアプリケーション特性評価の結果について説明します。

テスト環境とセットアップ

- ESXi 4.1 上の Citrix XenDesktop 5
- すべての HVD には、Cisco VXI Knowledge Worker+ プロファイルに含まれるアプリケーションが、バックグラウンドで実行される Move AV とともにインストールされます。
- このテストで実行されたアプリケーションは Cisco Unified Personal Communicator だけです。
- テストには 90 台の HVD が使用されました。これらはすべて、1.5 G のメモリを搭載した Windows 7（32 ビット）マシンです。90 台の HVD は、Cisco Unified Personal Communicator を実行する 90 台の HVD としてログインしました。
- UCS B250 M2（X5680、1 基あたり 3.33 GHz）、192 G の RAM を装備

テスト結果の概要

図 133　XenDesktop 5 におけるデスクフォン モードの Cisco Unified Personal Communicator 8.5 アプリケーション プロファイリング

上記のグラフは、デスクフォン モードの Cisco Unified Personal Communicator 8.5 のリソースが 90 ユーザのプールに影響し、UCS B250 M2 の CPU 使用率が 68 % 増加することを示しています。グラフの初めの部分には、ESXi で動作している 90 台の HVD による CPU 使用率（午後 3 時 15 分～ 3 時 40 分）が示され、続いて ICA を使用してログインした 90 台の HVD による使用率（午後 3 時 42 分～ 3 時 55 分）が示されています。90 ユーザがログインすると、CPU は最大 13 % の平均使用率で安定します（午後 3 時 55 分～ 4 時 00 分）。この時点で、Cisco Unified Personal Communicator のみで構成された作業負荷が、90 台すべての HVD で開始されます（午後 4 時まで）。CPU 使用率が 100 % に急増する原因は、90 ユーザ全員が Cisco Unified Personal Communicator を起動し、ログインすることにあります。CPU は、最大 81 % の平均使用率で定常状態に達します。これは、Cisco Unified Personal Communicator にログインし、このアプリケーションを実行している 90 ユーザによる使用率が 68 %（81 % - 13 %）純増することを意味します。上記のチャートは vCenter から取得されましたが、平均値の確認には resxtop で収集したデータも使用されました。

XenDesktop 5 と ESXi 4.1 を使用したデスクフォン モードの Cisco Unified Communications Integration for Microsoft Office Communicator 8.5

このセクションでは、UCS B250 M2 シリーズ サーバ上でデスクフォン モードの Cisco Unified Communications Integration for Microsoft Office Communicator 8.5 を実行する XenDesktop 5 仮想デスクトップに対して実施されたアプリケーション特性評価の結果について説明します。

テスト環境とセットアップ

- ESXi 4.1 上の Citrix XenDesktop 5
- すべての HVD には、Cisco VXI Knowledge Worker+ プロファイルに含まれるアプリケーションが、バックグラウンドで実行される Move AV とともにインストールされます。
- このテストで実行されたアプリケーションは、デスクフォン モードの Cisco Unified Communications Integration for Microsoft Office Communicator 8.5 だけです。
- テストには 90 台の HVD が使用されました。これらはすべて、1.5 G のメモリを搭載した Windows 7（32 ビット）マシンです。90 台の HVD は、デスクフォン モードの Cisco Unified Communications Integration for Microsoft Office Communicator 8.5 を実行する 90 台の HVD としてログインしました。
- UCS B250 M2（X5680、1 基あたり 3.33 GHz）、192 G の RAM を装備

テスト結果の概要

図 134　XenDesktop 5 におけるデスクフォン モードの Cisco Unified Communications Integration for Microsoft Office Communicator 8.5 アプリケーション プロファイリング

上記のグラフは、デスクフォン モードの Cisco Unified Communications Integration for Microsoft Office Communicator 8.5 のリソースが 90 ユーザのプールに影響し、UCS B250 M2 の CPU 使用率が 58 % 増加することを示しています。グラフの初めの部分には、ESXi で動作している 90 台の HVD による CPU 使用率（午後 4 時 20 分～ 5 時 01 分）が示され、続いて ICA を使用してログインした 90 台の HVD による使用率（午後 5 時 01 分～ 5 時 08 分）が示されています。90 ユーザがログインすると、CPU は 15 % まで低下します（午後 5 時 09 分まで）。この時点で、デスクフォン モードの Cisco Unified Communications Integration for Microsoft Office Communicator 8.5 のみで構成された作業負荷が、90 台すべての HVD で開始されます（午後 5 時 09 分まで）。CPU 使用率が 100 % に急増する原因は、90 ユーザ全員がデスクフォン モードの Cisco Unified Communications Integration for Microsoft Office Communicator 8.5 を起動し、ログインすることにあります。CPU は、最大 73 % の平均使用率で定常状態に達します。これは、デスクフォン モードの Cisco Unified Communications Integration for Microsoft Office Communicator 8.5 にログインし、このアプリケーションを実行している 90 ユーザによる使用率が 58 %（73 % - 15 %）純増することを意味します。上記のチャートは vCenter から取得されましたが、平均値の確認には resxtop で収集したデータも使用されました。

XenDesktop 5 と ESXi 4.1 を使用した Cisco UC Integration for WebEx Connect 7

このセクションでは、UCS B200 M2 シリーズ サーバで Cisco UC Integration for WebEx Connect 7 を実行する XenDesktop 5 仮想デスクトップに対して実施されたアプリケーション特性評価の結果について説明します。

テスト環境とセットアップ

- ESXi 4.1 上の Citrix XenDesktop 5
- すべての HVD には、Cisco VXI Knowledge Worker+ プロファイルに含まれるアプリケーションが、バックグラウンドで実行される Move AV とともにインストールされます。
- このテストで実行されたアプリケーションは、Cisco UC Integration for WebEx Connect 7 だけです。
- テストには 3 台の HVD が使用されました。これらはすべて、1.5 G のメモリを搭載した Windows 7（32 ビット）マシンです。3 台の HVD は、デスクフォン モードの Cisco Unified Communications Integration for Microsoft Office Communicator 8.5 を実行する 3 台の HVD としてログインしました。
- UCS B200 M2、96 G の RAM を装備

テスト結果の概要

下記のグラフは、3 ユーザが UCS B200 M2 で Cisco UC Integration for WebEx Connect 7 を使用した場合のリソース使用率を示しています。このグラフは、アプリケーションの起動、アプリケーションへのログイン、それに続くインスタント メッセージング、ユニキャストおよび会議タイプのチャットなど、3 ユーザが WebEx Connect でさまざまなアクティビティを実行するときの使用率を示しています。このテストは手動で行われたため、ユーザ数が制限されましたが、アプリケーションでのさまざまなアクティビティだけでなく、HVD のログインおよびログアウトについても WC7 の相対的影響が明確に示されています。

図 135　XenDesktop 5 での Cisco UC Integration for WebEx Connect 7 アプリケーション プロファイリング（CPU）：3 ユーザ

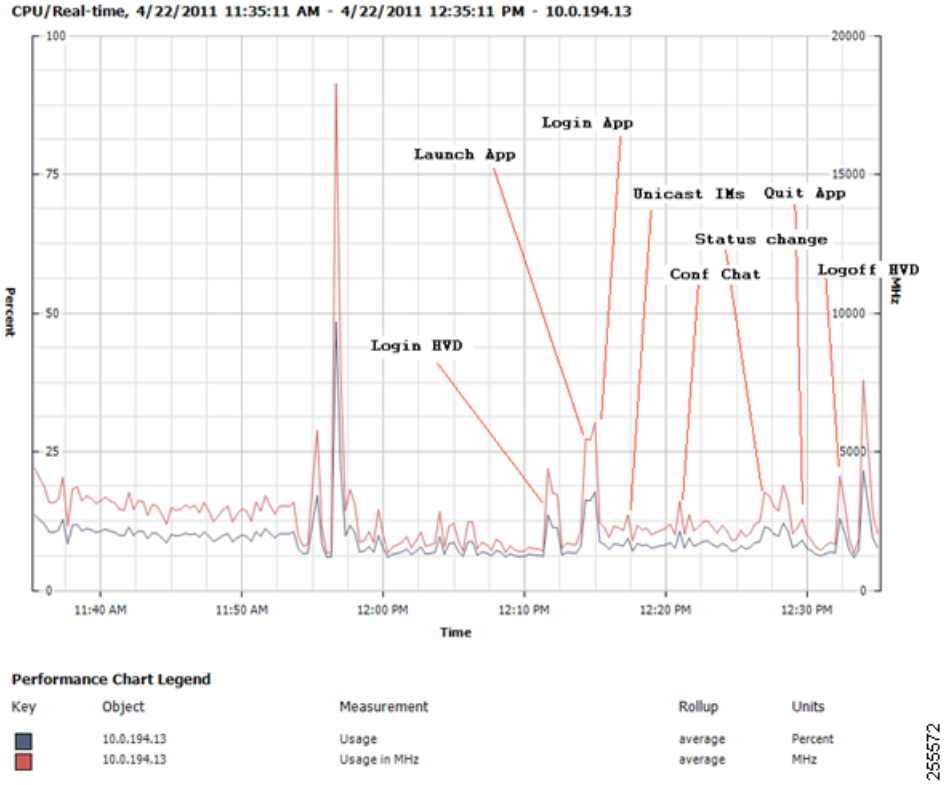


図 136　XenDesktop 5 での Cisco UC Integration for WebEx Connect 7 アプリケーション プロファイリング（メモリ）：3 ユーザ

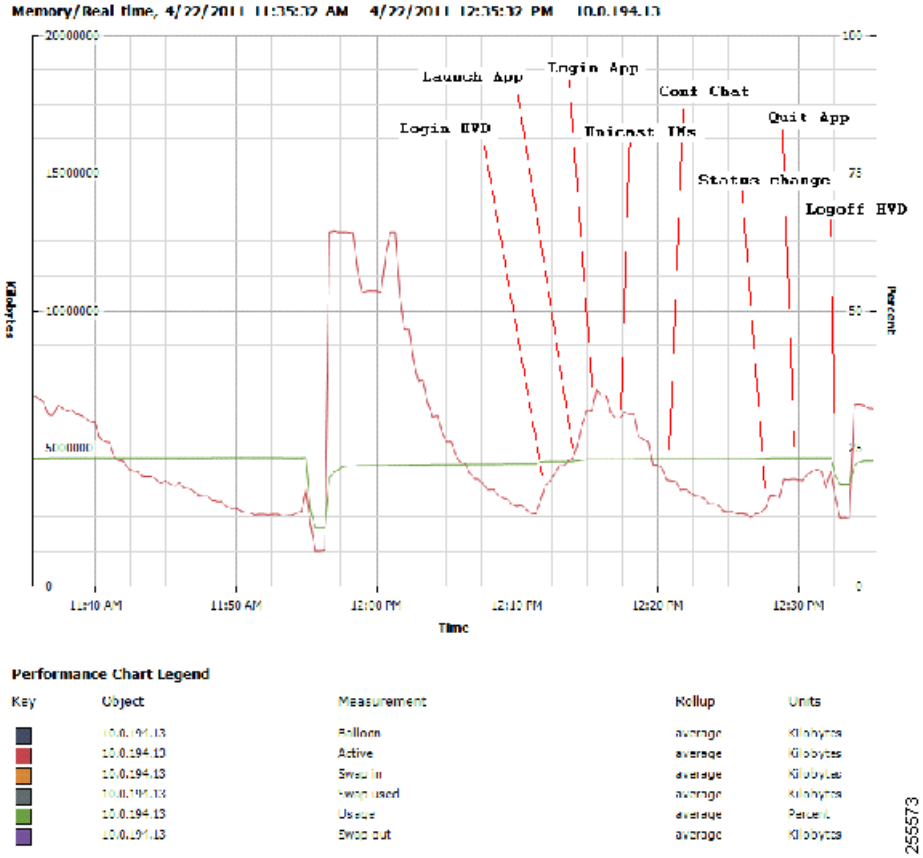


図 137　XenDesktop 5 での Cisco UC Integration for WebEx Connect 7 アプリケーション プロファイリング（データストア）：3 ユーザ

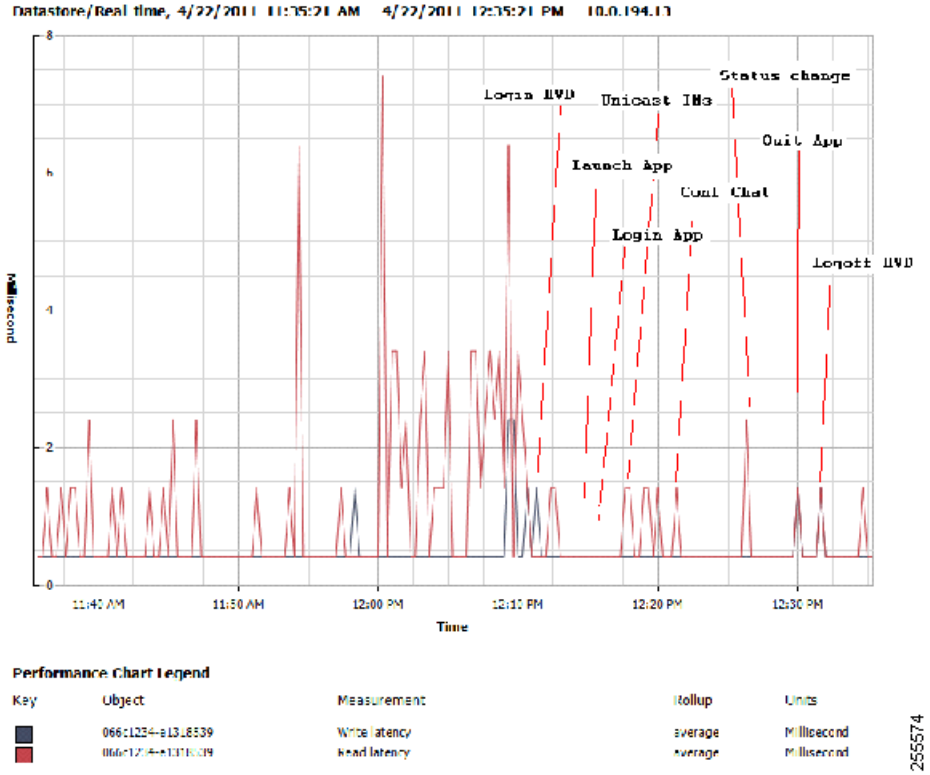
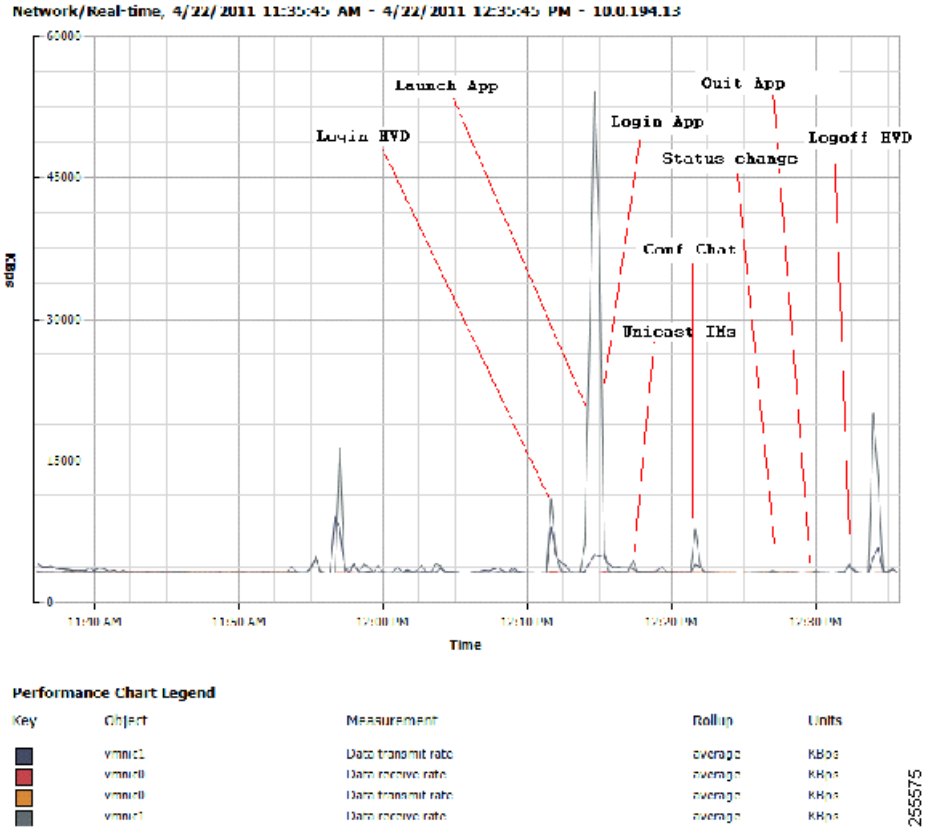


図 138　XenDesktop 5 での Cisco UC Integration for WebEx Connect 7 アプリケーション プロファイリング（ネットワーク）：3 ユーザ



WAN のキャパシティ プランニング

このセクションでは、エンタープライズ WAN と、帯域幅が制限されたリモート サイトに配置できるデスクトップ仮想化ユーザの数を決定する際に考慮すべき要因について説明します。所定の帯域幅の WAN リンクがサポートできるデスクトップ仮想化ユーザ数は、次のように表すことができます。

WAN リンクの帯域幅 / 単一のデスクトップ仮想化セッションの帯域幅

ただし、デスクトップ仮想化環境の場合、このようなサイズの決定方法には問題があります。なぜなら、単一のデスクトップ仮想化セッションの帯域幅のキャパシティは、いくつかの変動要因の影響を受ける可能性があるからです。Voice over IP（VoIP）環境では、音声コールは音声コールです。つまり、所定のコーデックに対し、トラフィックは予測可能かつ円滑であり、1 コールあたり 80 kbps で安定しています。デスクトップ仮想化セッションのトラフィックは、ユーザのネットワーク トラフィックが現在そうであるように、完全な変動要因です。音声環境では、ブランチ ロケーションで 10 個のコールを同時にサポートする必要がある場合、10 X 80 kbps = 800 kbps のトラフィックが必要です。デスクトップ仮想化では、デスクトップでの作業内容によって、2 人のユーザ間でセッションのトラフィック フローが大きく異なる場合があります。そしてこれは、セッションの帯域幅を変化させる変動要因のうちの一つにすぎません。

デスクトップ仮想化では、ユーザが開始した各アクションと、それに続く応答がネットワークを介してリレーされます。これは、データセンターのホステッド仮想デスクトップから、エンド ユーザが使用しているクライアントへ伝送される、セッション トラフィックの一部として扱われます。特定のデスクトップ仮想化セッションでは、プロトコルとベンダーに応じて、メイン デスクトップ仮想化セッションに関連付けられている他の TCP セッションでトラフィックが伝送されることがあります。あるいは、メイン デスクトップ仮想化セッションと同じ TCP または UDP セッション内の仮想チャネル（Half Duplex（HDX; 半二重）で伝送される場合もあります。Citrix XenDesktop で使用される ICA ディスプレイ プロトコルを使用すると、この情報をリレーできます。各プロトコルは、以下の点において実装方法が異なります。

- 使用される転送プロトコル
- 使用される暗号化タイプ
- 圧縮レベル
- 表示のレンダリングの処理方法（リモートまたはローカル）
- 使用可能なネットワーク帯域幅の変更に対する適応方法

ディスプレイ プロトコルそのものに加え、エンド クライアントが使用する画面解像度とモニタ数も、ネットワーク帯域幅に影響します。

アプリケーション（Microsoft Office、バックアップ、Web ブラウザ、銀行ユーザ向けの Teller アプリケーションなど）、ユーザのアクティビティ、および各ユーザの作業負荷も、常に大きな影響力を持つ変動要因です。

仮想デスクトップで一般的に使用されるゲスト OS の Microsoft Windows XP および Windows 7（32 ビットおよび 64 ビット）も、OS の違いによってデスクトップ仮想化の全体的なエクスペリエンスが異なる原因となります。したがって、デスクトップ仮想化のセッション トラフィックにも影響する場合があります。

仮想化デスクトップでビデオ トラフィックがサポートされている場合、次のようなビデオ コンテンツ以外の要素における違いが、エンドユーザ エクスペリエンスだけでなく、所定のデスクトップ仮想化セッションの帯域幅要件にも影響する可能性があります。

- ビデオの転送方式。ビデオ ストリームは個別の TCP/UDP セッションで伝送されるのか、あるいは、ビデオ ストリームはメイン デスクトップ仮想化セッションのインバンドであるのか。
- Citrix XenDesktop が導入されている場合は、HDX を使用してビデオ ストリームを伝送できます。トラフィックの最適化やユーザあたりの帯域幅の削減も、HDX によって実現できます。HDX は、遅延が 30 ms 未満の場合のみ使用できます。遅延が 30 ms を超えることが多い WAN では、HDX について考慮する必要があります。
- Adobe Flash や Microsoft Windows Media Player コンテンツなど、使用するビデオ コンテンツのタイプ。現在、Adobe Flash コンテンツは Cisco WAAS を使用して最適化できないため、Cisco WAAS を使用してユーザあたりの帯域幅要件を低減することはできません。
- Citrix XenDesktop では、Adobe Flash コンテンツは HDX によって伝送されるので、トラフィックを最適化することができます。

前述の考慮事項に加え、ビデオは帯域幅を大量に消費するうえ、損失、ジッタ、および遅延に関する要件が厳しいため、WAN リンクの計画ではビデオの QoS と割り当て帯域幅を慎重に検討する必要があります。

デスクトップ仮想化環境の印刷機能も、各セッションのトラフィックに影響することがあります。その場合、リモート サイトにあるローカル プリンタへのネットワーク印刷を使用するかどうか、あるいは、USB 印刷を使用して、個々のチャネル上の印刷トラフィックを、ユーザのメイン デスクトップ仮想化セッションと同じエンドポイントにある USB 接続プリンタへ転送するかどうか、などが要因となります。

WAN リンクのサイズ決定におけるもう一つの重要な考慮事項は、WAN 最適化を導入するかどうかです。WAN リンクを通過するアプリケーション トラフィックを最適化する場合、通常は Cisco WAAS デバイスを使用します。Cisco WAAS は、WAN リンクの帯域幅使用率をアプリケーション レベルで効率的に低減するので、所定の WAN リンクに多数のユーザを配置することが可能になります。デスクトップ仮想化導入での Cisco WAAS の使用方法については、このドキュメントの「ネットワーク」の章を参照してください。

以上のことから、デスクトップ仮想化には、セッションあたりの帯域幅使用率を変化させるさまざまな変動要因が関係していることは明白です。したがって、セッションあたりの帯域幅の概算値は、それぞれのデスクトップ仮想化導入に固有の値であり、1 つの企業内であっても、デスクトップ仮想化ユーザのアプリケーション、作業負荷、使用パターンによって大きく異なる場合があります。このため、WAN リンクのサイズ決定は些末な作業などではなく、サイズの概算は該当する環境内で検証しておく必要があります。

デスクトップ仮想化トラフィックは変動性が高いことから、WAN リンクに必要な帯域幅を特定する場合、通常はこの章の「作業負荷の考慮事項」のセクションで定義されている一般的な作業負荷プロファイルをいずれか 1 つ使用して、データの特性を評価します。ただし、個々のデスクトップ仮想化導入の特性をより的確に示す作業負荷に基づいて、概算値を調整することが重要です。さらに、ビデオや USB 印刷トラフィックのように、状況に応じてトラフィックがアウトオブバンド方式で伝送される場合は、このトラフィックも別個に特性評価する必要があります。Cisco WAAS を使用して WAN を最適化する場合、Cisco WAAS がある場合とない場合の影響についても検討する必要があります。

次のセクションでは、Cisco VXI システムで実施されたテストの結果を取り上げ、Cisco VXI システムの適切な導入に不可欠なネットワークの側面から、デスクトップ仮想化への理解を深め、その特性を評価します。

ネットワーク特性評価の結果

今回の Cisco VXI システムのリリースでは、以下の項目に重点が置かれています。

- Cisco VXI Knowledge Worker+（KW+）作業負荷など、一般的な VDI 作業負荷の Bandwidth（BW; 帯域幅）特性を理解する
- ビデオ専用の帯域幅（BW; BandWidth）特性を理解する
- ICA プロトコルの適応性がコンピューティングおよびサーバ パフォーマンスに与える影響の度合い

上記のすべてのテストは、このドキュメントで前述した Cisco VXI システム アーキテクチャを使用して構築されたエンドツーエンドの Cisco VXI ネットワークを介してブランチ サイトから実施されました。

ここに示すデータは Cisco VXI Knowledge Worker+ 作業負荷に基づいていますが、限られた帯域幅で WAN を導入する際に顧客が考慮すべき要因について、有益な見識をこのデータから得ることができます。Cisco VXI KW+ 作業負荷の詳細については、この章で前述した「作業負荷の考慮事項」のセクションを参照してください。

VDI 作業負荷の帯域幅特性：Cisco VXI KW+ 作業負荷

このセクションでは、Cisco VXI KW+ を例にとり、一般的な VDI 作業負荷の帯域幅特性について説明します。使用される作業負荷プロファイルは、Cisco VXI システムのパフォーマンスに関する特性の重要な要素です。一例を挙げると、ユーザ エクスペリエンスが良好な状態で仮想デスクトップ イベントをリモート表示するために必要な最小帯域幅があります。パフォーマンス データは使用される作業負荷プロファイルによって異なる可能性があるので、アプリケーションだけでなく使用パターンについてもユーザ ベースの特性を示す作業負荷を使用して、顧客環境で同様の評価を行うことが重要です。ただし Cisco VXI KW+ 作業負荷は、アプリケーション（Microsoft Office アプリケーション、Internet Explorer、Adobe Acrobat）とそれらのアプリケーションでの操作の両面において一般的なナレッジ ワーカーの特性を的確に表しているので、ここで示すデータは Cisco VXI 導入における WAN リンクのサイズを決定する際に有効な根拠として使用できます。

このセクションでは、以下の帯域幅データを示します。

- 所定の帯域幅と帯域幅に制限のないユーザのピーク帯域幅。このテストは、ブランチ サイトの 1 ユーザが使用する T1 リンクで実施されます。ブランチ サイトは Cisco VXI ネットワーク上にあり、HVD はデータセンターの UCS ブレードでホストされています。WAN リンクを経由するすべてのトラフィックに最大 80 ms の遅延が挿入されます。これは、米国の西海岸から東海岸で観測される一般的な遅延です。1 人のユーザが T1 帯域幅のすべてを使用できるので、特にナレッジ ワーカーの場合は、平均的な BW 使用率に十分対応できる帯域幅がありますが、ピーク時の作業負荷を処理するには不十分な場合もあります。この点に関する対処方法については、次の項目を参照してください。
- 上記と同じユーザがキャンパス ネットワーク内に存在し、そのリンクが T1 よりも高速で、ピークを処理できる十分な帯域幅がある場合、その作業負荷で測定されたピーク帯域幅使用率における違い。
- HVD のログインおよびログアウトに必要な BW など、BW 消費量のアプリケーション レベルの分析。この分析から、Word や Excel などユーザ アプリケーション間の相対的 BW 消費量のデータだけでなく、HVD のログイン/ログアウトなど VDI 固有のアクティビティに関連する消費量データも取得できます。さらにこのデータによって、アプリケーション内部のアクションと、そのアクションが帯域幅使用率に及ぼす影響に関する情報も示されます。
- 良好な EU を維持するために所定の作業負荷で必要な最小帯域幅。この帯域幅を基準にして、同様の作業負荷が発生する環境での WAN のサイズを決定できます。

テスト環境とセットアップ

- ESXi 4.1 上の XenDesktop5
- HVD のプロファイル
  - Windows 7（32 ビット）、1.5 G のメモリを装備
  - ディスプレイ プロトコル：ICA
  - 表示セッション特性

    画面解像度：1350 X 686

    カラー深度：16 ビット
  - ベスト パフォーマンス向けに最適化された Windows（すべてのオプションをオフ）
- 作業負荷プロファイル：Cisco VXI Knowledge Worker+ プロファイル、バックグラウンドで McAfee Move-AV が動作
- サーバ プロファイル：UCS B200 M2、96 G の RAM を装備。テスト中、サーバは最小負荷で動作
- このテストでは、T1 WAN リンクのブランチ サイトにある単一の HVD を使用。80 ms の遅延を挿入、ジッタなし

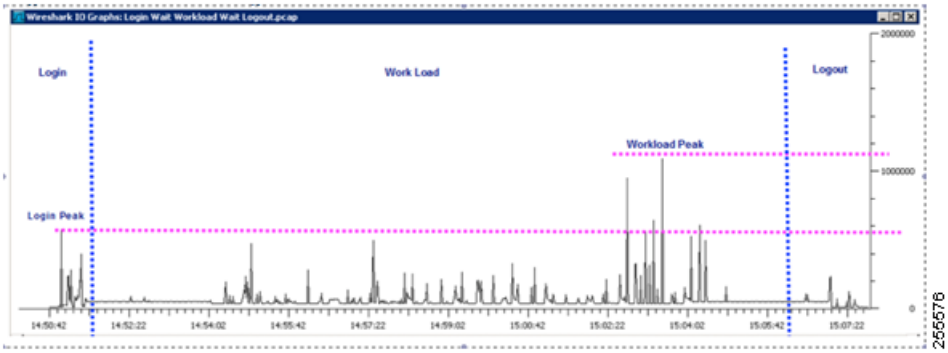
ユーザ エクスペリエンス/アプリケーション応答時間

このテストでは、追加レビューおよび分析用のセッション エクスペリエンスを WebEx 上で取り込み、自動作業負荷を使用してテストを複数回繰り返す間に、そのユーザ エクスペリエンスを観察しました。このように 1 ユーザだけが関与する特殊なテストでは、主観的測定の方が実際のユーザ エクスペリエンスを正しく評価できます。なぜなら、テスト ツールでは特定のアクティビティに対する応答時間しか取得できないのに対し、主観的測定ではセッション エクスペリエンスのあらゆる側面を把握できるからです。テストの進行中に、作業負荷に含まれるアプリケーションでの一部のアクティビティが、帯域幅制限の影響を受けやすいことが判明したため、それらのアクティビティに十分な注意が払われました。例として、PowerPoint のスライド ショー モードでの表示や Outlook での電子メールの作成が挙げられます。UE に帯域幅制限の影響が出始めた場合は、PowerPoint のスライドに情報が一括表示されるようにし、Outlook では入力中のメッセージを一括表示します。これは、ユーザ エクスペリエンスに問題がない場合の円滑なワード フローとは対照的です。以上をまとめると、このテストの結果は主観的なユーザ エクスペリエンスに基づいていますが、この場合は主観的測定とはいえ、測定された帯域幅データはより正確です。

テスト結果の概要

帯域幅：ピークおよび平均

図 139　Cisco VXI KW+ 作業負荷を使用した ICA セッションの帯域幅使用率



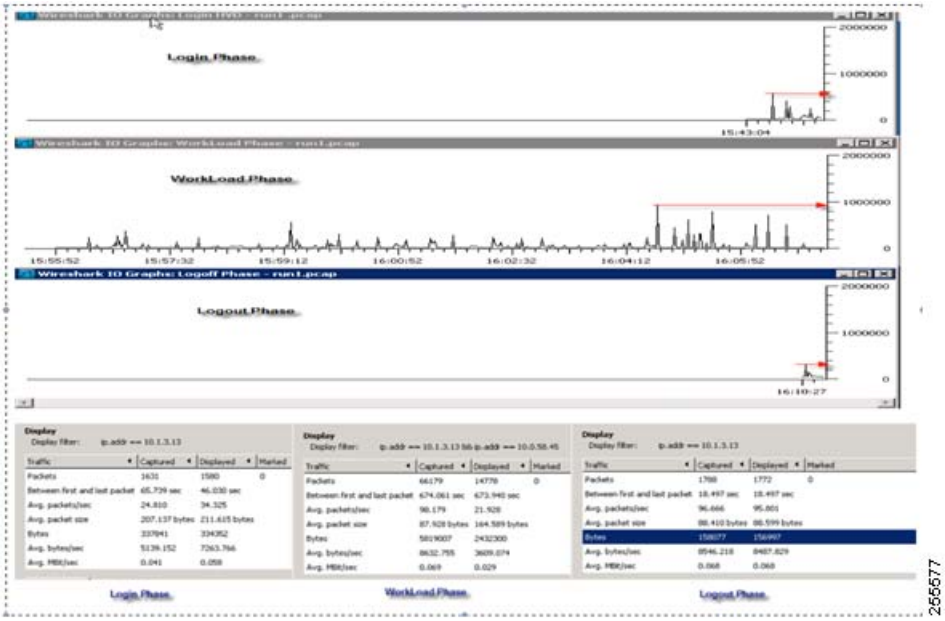
上の図に、自動化された Cisco VXI KW+ 作業負荷を 1 回繰り返す間の帯域幅を示します。ここで作業負荷は、上記の期間内のユーザのアクティビティを表しています。このデータは単一の VDI セッションを示しており、最小限必要な制御トラフィックを除き、リンク上に他のトラフィックはありません。上記のグラフは、VDI セッション トラフィックだけが表示されるようにフィルタリングされたものです。グラフには、ユーザが VDI セッションに初めてログインしたときと、ログアウトしたときの帯域幅使用率も示されています。各フェーズで使用されたピーク帯域幅を下記の表に示します。作業負荷のピークは最高値の T1 速度に達しており、その後にログイン フェーズが続いています。ログアウト フェーズは、3 つのフェーズの中で BW への影響が最も少ないようです。これらのテストには T1 WAN リンクが使用されたため、作業負荷でのイベントのリモート表示に関連するピーク帯域幅が T1 を超えることはありません。したがって、作業負荷のディスプレイ プロトコルと帯域幅要件によっては、ディスプレイ プロトコルが T1 帯域幅の制限に基づいてすでに適応している場合、ピーク帯域幅はその作業負荷での実際のピーク値と異なる場合があります。100 Mbps 以上の帯域幅を備えたキャンパス ロケーションでこれと同じテストを繰り返すと、このピーク帯域幅が作業負荷に対する実際のピーク値であるか調整後のピーク値であるかを確認できます（下記を参照）。T1 リンクによる制限があったとしても、作業負荷のピーク時にユーザ エクスペリエンスへの影響はなかったことに注意してください。

表 49　ICA と Cisco VXI KW+ 作業負荷を使用して T1 で実行された単一 VDI セッションのピーク帯域幅

ブランチ	ピーク BW 1 回目	ピーク BW 2 回目	ピーク BW 3 回目	ピーク帯域幅使用率
ログイン	600 kbps	500 kbps	600 kbps	567 kbps
作業負荷	900 kbps	1 Mbps	1 Mbps	967kbps
ログアウト	300 kbps	300 kbps	280 kbps	293 kbps

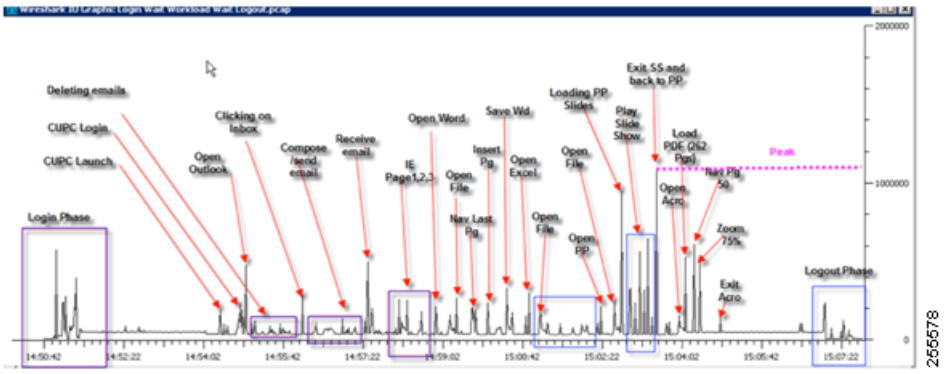
所定の作業負荷を使用する 1 ユーザに関する上記のデータを、最小 BW データとともに使用すると、良好な UE が得られる帯域幅の範囲を特定できます。このデータは、ブランチの Cisco VXI 導入で WAN リンクのサイズを決定する際、重要な要素となります。

図 140　Cisco VXI KW+ 作業負荷を使用した ICA セッションの帯域幅使用率：別図



上記の図は、各フェーズの帯域幅使用率を別の角度から捉えたものです。グラフ下の表は、このグラフのフェーズを短時間に 1 度繰り返す間の平均使用率を示しています。

図 141　　Cisco VXI KW+ 作業負荷のアプリケーション詳細図

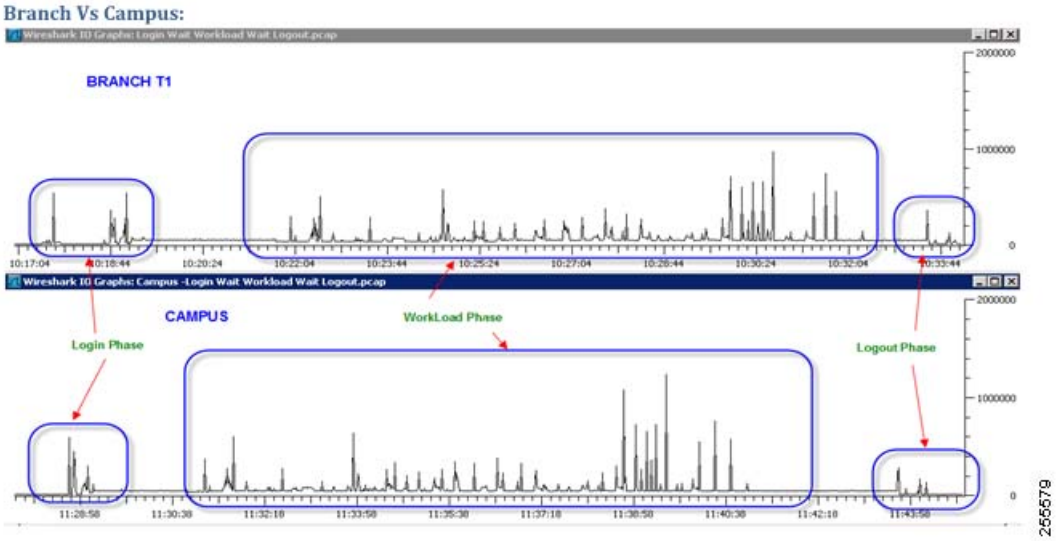


この図は、作業負荷におけるアプリケーションとアクティビティの観点から、作業負荷フェーズをさらに詳細に示したものです。このデータは、HVD での所定の操作がユーザにリモート表示されたとき、その操作が絶対的 BW と相対的 BW に与える影響を示しています。

（注）　この作業負荷でのピーク帯域幅は PowerPoint、続いて Acrobat で表示されます。ユーザ エクスペリエンスの観点からみると、使用する帯域幅が少なくても、電子メールの入力は帯域幅の輻輳に大きく影響されることにも注意が必要です。

ブランチとキャンパス

図 142　　ブランチおよび キャンパスでの ICA の帯域幅使用率



上記の図は、ユーザが 1 人の T1（遅延 80 ms）から帯域幅 100 Mbps 以上のキャンパス（遅延なし）に至るまでのピーク帯域幅使用率を示しています。このグラフから、同じ作業負荷に対し、実際のピーク帯域幅はより高い値であることがわかります。したがって、WAN リンクのサイズをピーク値に対応できる規模にする場合、あるいはピーク値の X % に設定しようとする場合は、ピークに対処できる十分な帯域幅を備えた環境でピーク帯域幅を測定することが重要です。作業負荷で使用される平均帯域幅に基づいてサイズが決定されていた場合は、T1 の単一ユーザだけが関係しているのではないことに注意してください。

以上を踏まえて、ブランチ テストのデータを次のように書き換えると、作業負荷フェーズでの実際のピーク帯域幅を反映させることができます。

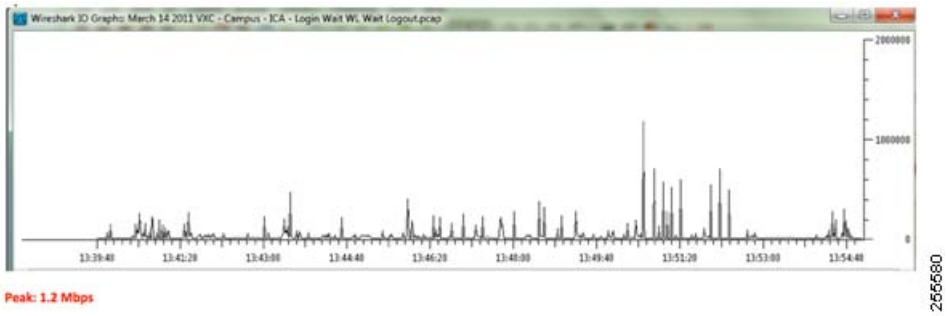
表 50　ICA と Cisco VXI KW+ 作業負荷を使用してキャンパスで実行された単一 VDI セッションのピーク帯域幅

	ブランチのピーク BW	キャンパスのピーク BW
ログオン	567 kbps	同
作業負荷	967 kbps	最大 1.3 Mbps
ログアウト	293 kbps	同

最小帯域幅

この作業負荷で良好なユーザ エクスペリエンスを得るために必要な最小帯域幅を決定するには、T1 で使用可能な帯域幅をユーザ エクスペリエンスが低下するまで減少させます。その場合、チャネライズド T1 リンクからタイムスロットを削除して、使用可能な帯域幅を削減します。その後、自動作業負荷が実行され、ユーザ エクスペリエンスが許容可能な範囲を超え始めたら、その直前にある T1 上の帯域幅を最小帯域幅と見なします。

図 143　KW+ 作業負荷を実行する Cisco VXC クライアントの ICA 最小 BW



上記の方法を使用すると、ディスプレイ プロトコルに ICA を使用する場合、この作業負荷で良好なユーザ エクスペリエンスを維持するために必要な最小帯域幅は 128 kbps となります。

ビデオ専用 VDI 作業負荷の帯域幅特性

このセクションでは、ビデオ専用 VDI 作業負荷の帯域幅特性を取り上げ、短編のビデオ クリップがブランチ サイトの帯域幅要件に及ぼす影響について説明します。これらのテストでは、WAN リンク（この場合は T1）で 1 分間のフラッシュ ビデオ クリップを使用し、輻輳が発生している場合とそうでない場合のユーザ エクスペリエンスを測定します。前述のケースと同様、VDI セッションで使用可能な帯域幅を削減して輻輳を発生させます。

テスト環境とセットアップ

- ESXi 4.1 上の XenDesktop5
- HVD のプロファイル
  - Windows 7（32 ビット）、1.5 G のメモリを装備
  - ディスプレイ プロトコル：ICA
  - 表示セッション特性

    画面解像度：1350 X 686

    カラー深度：16 ビット
  - ベスト パフォーマンス向けに最適化された Windows（すべてのオプションをオフ）

- 作業負荷プロファイル：ビデオ専用、1 分間の フラッシュ ビデオ クリップ、標準解像度 640 X 360
- このテストには単一の HVD を使用
- サーバ プロファイル：UCS B200 M2、96 G の RAM を装備。テスト中、サーバは最小負荷で動作
- このテストでは、T1 WAN リンクのブランチ サイトにある単一の HVD を使用。80 ms の遅延を挿入、ジッタなし

テスト結果の概要

帯域幅：ピークおよび平均

下の 2 つの図は、輻輳がない状態での 1 分間のビデオ クリップの帯域幅使用率を示しています。このビデオ作業負荷の平均およびピーク帯域幅は、使用可能な T1 帯域幅の最大値であることに注意してください。ビデオおよび音声品質の両方において、このテストでのユーザ エクスペリエンスは許容範囲内でした。

図 144　ビデオ専用帯域幅使用率：制限なし

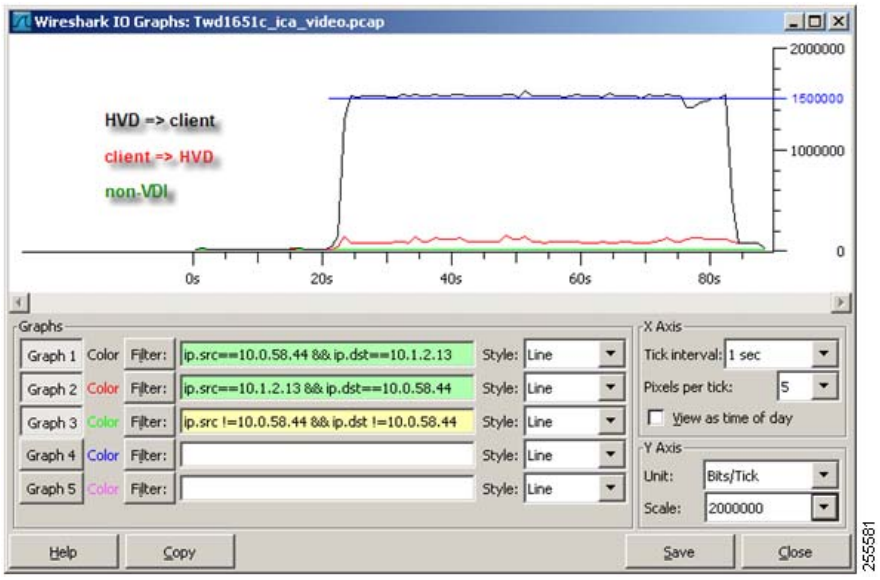
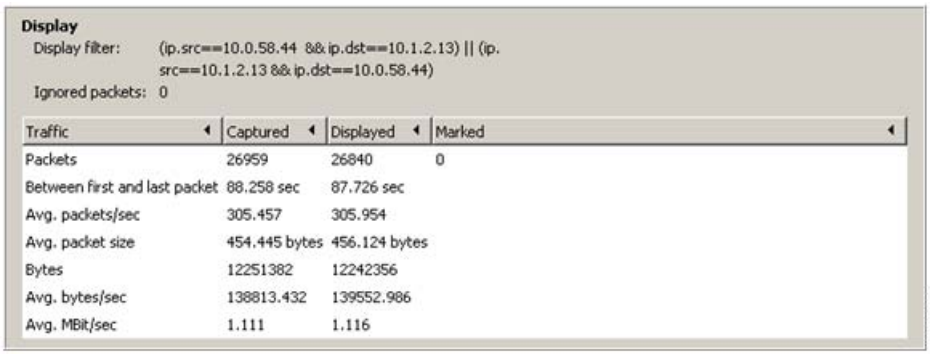


図 145　ビデオ専用帯域幅使用率に関する Wireshark 統計（制限なし）



最小帯域幅

下の 2 つの図は、輻輳が発生している状態での 1 分間のビデオ クリップの帯域幅使用率を示しています。作業負荷フェーズでの平均使用およびピーク時の使用により、使用可能な帯域幅全体が継続的に占有されていることに注意してください。このケースでは、使用可能な帯域幅は 1024 kbps に削減されました。ただし、ビデオ品質および音声品質のいずれにおいても、このレートでのユーザ エクスペリエンスは容認可能な範囲を超えていました。ビデオは不安定で理解しにくく、音声はビデオと同期していませんでした。以上を踏まえて、標準解像度（640 X 360）を使用した 1 分間のビデオ クリップに必要な最小帯域幅は、1024 kbps + 64 kbps（1 タイムスロット 64 kbps）= 約 1088 kbps となります。

図 146　　ビデオ専用帯域幅使用率：帯域幅制限あり

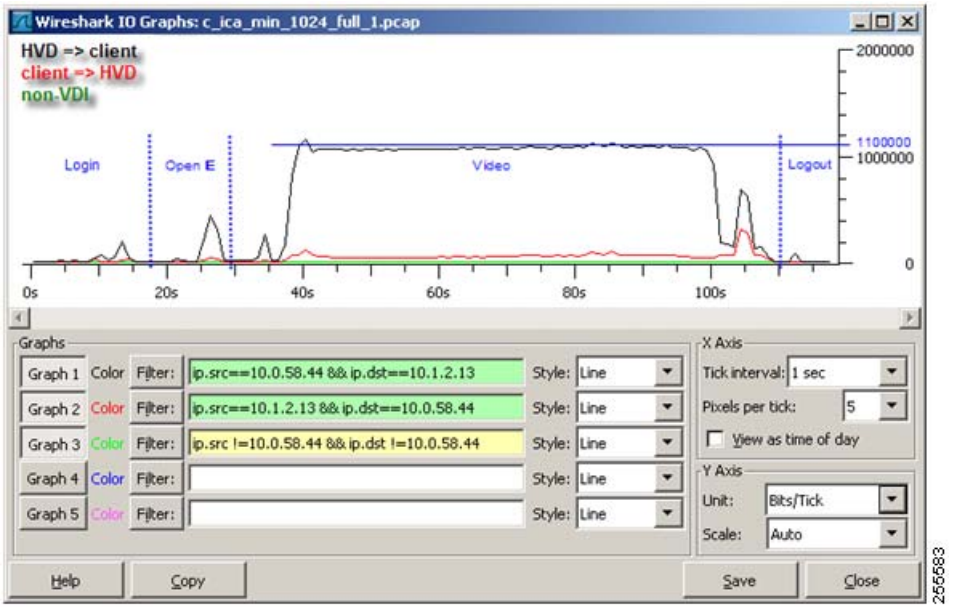
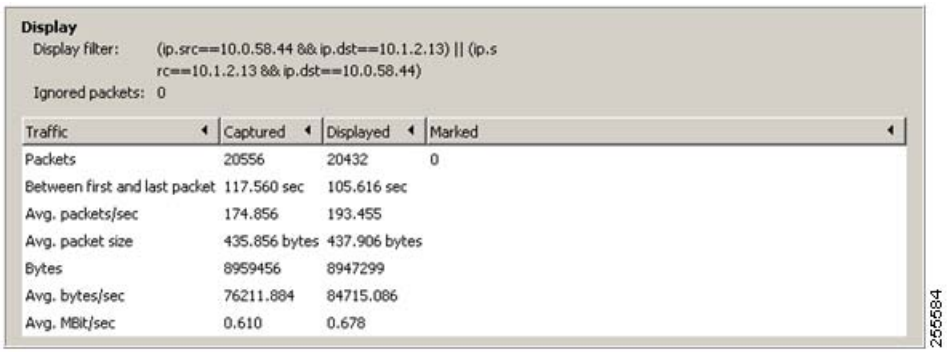


図 147　　ビデオ専用帯域幅使用率に関する Wireshark 統計（制限あり）



プロトコルの適応性がサーバ パフォーマンスに与える影響

大規模ブランチを基盤とする VDI 導入では、ディスプレイ プロトコルの適応性が、仮想デスクトップをホストしているサーバに影響を与えるかどうかを判断することが重要です。通常、サーバのスケールおよびパフォーマンスのベンチマークテストは、表示セッションで使用可能な帯域幅を制限せずに実行されます。したがってここでの目的は、すべてのユーザがブランチ サイト内に存在し、その WAN リンクで輻輳が発生している場合に、ディスプレイ プロトコルの適応性が単一のサーバに与える影響を特定することです。

テスト環境とセットアップ

- ESXi 4.1 上の XenDesktop5
- HVD のプロファイル
  - Windows 7（32 ビット）、1.5 G のメモリを装備
  - ディスプレイ プロトコル：ICA
  - 表示セッション特性

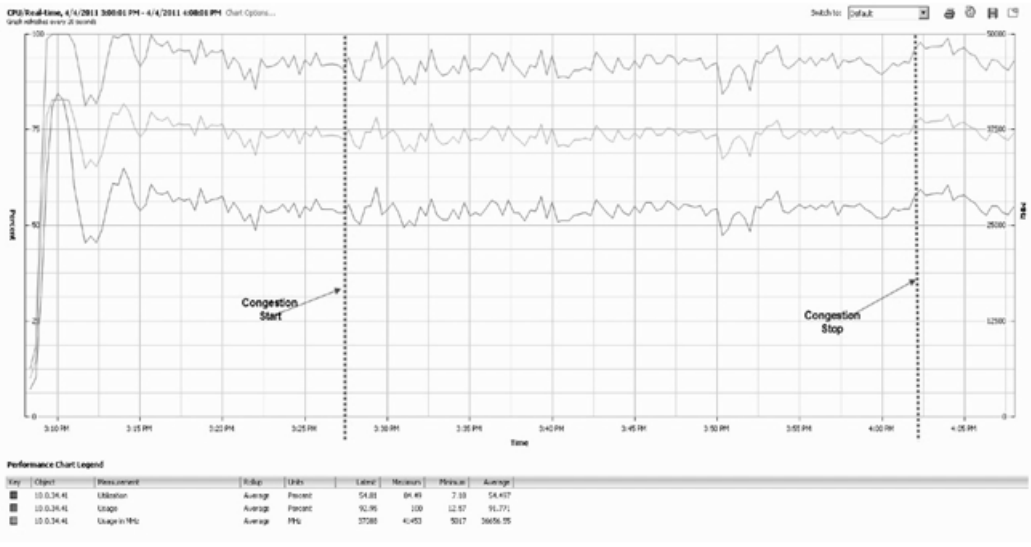
    画面解像度：1350 X 686

    カラー深度：16 ビット
  - ベスト パフォーマンス向けに最適化された Windows（すべてのオプションをオフ）
- 作業負荷プロファイル：Cisco VXI Knowledge Worker+ プロファイル、McAfee Move AV
- サーバ プロファイル：UCS B250 M2、192 G の RAM を装備、サーバは最大キャパシティまで拡張され、90 % の CPU 使用率で動作
- このテストでは、UCS サーバでホストされるすべての HVD は、T3 WAN リンクを介してブランチ サイトからアクセスされます。80 ms の遅延を挿入、ジッタなし

テスト結果の概要

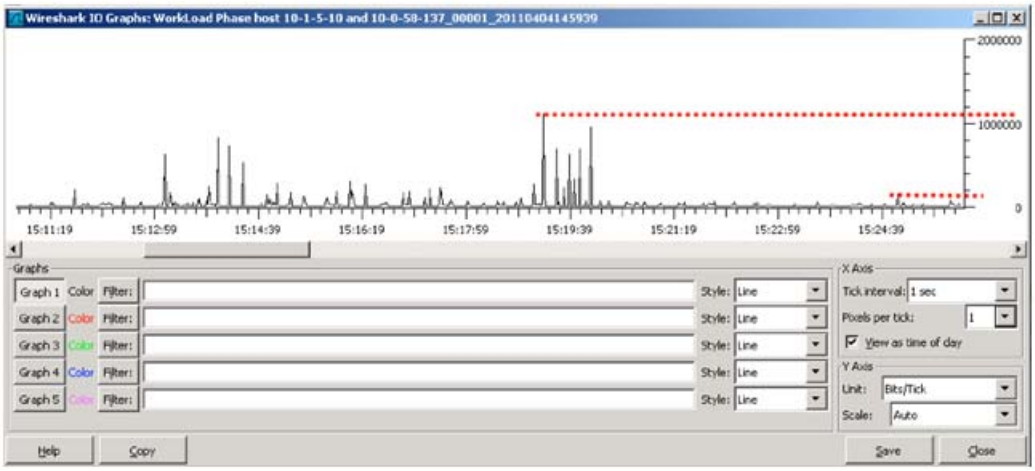
下記のグラフは、80 台の HVD をホストする Cisco UCS B250 M2 サーバの CPU 使用率を示しています。すべてのユーザは、Cisco VXI ネットワークのブランチ ネットワーク内に存在しています。CPU 使用率が最大 90 % の定常状態に達すると、トラフィック ジェネレータを使用して WAN リンクに輻輳が生成されます。この結果からは、サーバ パフォーマンスに大きな影響はないことがわかります。これは、セッションが適応して使用帯域幅を削減するからです。

図 148　　ICA を使用したサーバ/コンピューティングへの輻輳の影響



下の図は、上記のサーバでホストされているいずれかのセッションの帯域幅使用率を示しています。セッションは午後 3 時 19 分 39 秒までに、前述のピーク帯域幅の結果と同じ 1 Mbps を超えるピーク値に達しました。ただし輻輳が発生すると、セッションは他のセッションとともに適応し、200 kbps を大幅に下回る値まで帯域幅を削減しました。ここでも、最小帯域幅は 上記の測定値と同じ 128 kbps 以下です。アプリケーション応答時間でみたユーザ エクスペリエンスについては、80 セッションすべての各アプリケーションで測定され、余裕をもって許容範囲内に納まりました。

図 149　　輻輳発生時の各 VM 図



重要事項のまとめ

所定の作業負荷を使用した ICA に必要な最小帯域幅は 128 kbps、ピーク帯域幅は最大 1.3 Mbps です。このデータを使用して、WAN リンクのサイズを決定し、それらのリンクで QoS ポリシーを有効にすることができます。

アプリケーションの一部の機能または特性によってピーク帯域幅が消費されることがありますが、アプリケーション全体としての消費量はそれほど多くありません。たとえば、PowerPoint のスライド ショー モードによる BW への影響は、特定の作業負荷において最も大きくなります。

デスクフォン モードの Cisco Unified Personal Communicator 8.5 による BW への影響は大きくありませんが、PowerPoint と Acrobat は特定の作業負荷において最大の帯域幅を消費します。

導入後のパフォーマンス モニタリング

デスクトップ仮想化セッションのアプリケーション パフォーマンスだけでなく、データセンター内の全コンポーネントでキャパシティを監視する、キャパシティおよびパフォーマンス分析ツールが必要です。これにより、管理者は使用パターンとアクティビティ パターンに基づいて、必要に応じたキャパシティの増強や変更を行うことができます。キャパシティおよびパフォーマンスの監視専用に使用できるツールは次のとおりです。

- VMware esxtop ツールでは、VMware ESX サーバのリアルタイム ビューを表示できます。具体的には、以下のデータが表示されます。
  - 各仮想マシンの CPU 使用量
  - 各物理プロセッサの CPU 使用量
  - メモリ使用量
  - 仮想ディスク使用量
  - LAN およびストレージ アクセス用のネットワーク帯域幅
- データセンターに配置されたネットワーク分析モジュールを使用すると、帯域幅使用率、ドロップ、および遅延について、デスクトップ仮想化トラフィックのネットワーク パフォーマンス統計データを収集できます。
- ストレージ ベンダーが提供するストレージ パフォーマンス ツールでは、ストレージ パフォーマンスを正確に評価し、IOPS やスループットなどのメトリックを利用することができます。これらのツールは、パフォーマンスに影響する可能性がある問題の特定にも役立ちます。NetApp および EMC にはこのようなツールが用意されており、エンドツーエンド Cisco VXI システムの評価に使用されました。

エンドツーエンド Cisco VXI システムの監視に使用できるネットワーク管理ツールの詳細については、「管理と運用」の章を参照してください。

関連情報

表 51 に、この章で説明したハードウェアおよびソフトウェアを含む特定のベンダー情報の詳細を示します。

表 51　パフォーマンスとキャパシティ関連のリンク

『Reference Architecture-Based Design for Implementation of Citrix XenDesktops on Cisco Unified Computing System, and NetApp Storage』
http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/Virtualization/ucs_xd_vsphere_ntap.pdf
『Performance Best Practices for VMware vSphere 4.0』
http://www.vmware.com/pdf/Perf_Best_Practices_vSphere4.0.pdf
VMware vSphere 4.0 の最大構成
VMware vSphere 4.1 の最大構成
透過的ページ共有に関する VMware KB 記事
http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1021095
『Memory Resource Management in VMware ESX Server』
http://www.vmware.com/resources/techresources/531
『Performance Study of VMware vStorage Thin Provisioning』
http://www.vmware.com/pdf/vsp_4_thinprov_perf.pdf&rct=j&sa=X&ei=sGd3TLXvLcLflgedwqXsCw&ved=0CBoQzgQoATAA&q=VMware+and+Thin+provisioning&usg=AFQjCNHQmzBIuWlmbcVdVMhtqfDWpBu2Tg
VMware KB：「Using Thin Provisioned Disks with Virtual Machines」
http://kb.vmware.com/kb/1005418
『Workload Considerations for Virtual Desktop Reference Architectures Info Guide』
http://www.vmware.com/files/pdf/VMware-WP-WorkloadConsiderations-WP-EN.pdf
『Virtual Reality Check - Phase II version 2.0』
http://www.virtualrealitycheck.net/index.php?option=com_docman&task=doc_details&gid=11&Itemid=
『Desktop Virtualization with Xen Desktop and NetApp Storage』
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns993/landing_dcVirt-vdi.html
『Hyper-V Dynamic Memory Configuration Guide』
http://technet.microsoft.com/en-us/library/ff817651(WS.10).aspx

略語

このドキュメントで使用されている略語および省略形を表 52 に示します。

表 52　略語一覧

略語	正式表記
CNA	統合型ネットワーク アダプタ（Converged Network Adapter）
FC	ファイバ チャネル（Fibre Channel）
FCoE	Fibre Channel over Ethernet
HBA	ホスト バス アダプタ（Host Bus Adapter）
HVD	ホステッド仮想デスクトップ（Hosted Virtual Desktop）
ICA	Independent Computing Architecture
IOPS	1 秒あたりの I/O 処理数（I/O Per Second）
iSCSCI	Small Computer System Interface over IP
LAN	ローカル エリア ネットワーク（Local Area Network）
NFS	ネットワーク ファイル共有（Network File Share）
PCoIP	PC over IP
RDP	Remote Desktop Protocol
TPS	透過的ページ共有（Transparent Page Sharing）
vDC	仮想データセンター（Virtual Data Center）
VEM	仮想イーサネット モジュール（Virtual Ethernet Module）
VM	仮想マシン（Virtual Machine）
vPC	仮想ポート チャネル（Virtual Port Channel）
VSM	仮想スイッチ モジュール（Virtual Switch Module）
VoIP	Voice over IP
WAN	ワイド エリア ネットワーク（Wide Area Network）

その他の資料

次のリンクに、このマニュアルで説明したハードウェアおよびソフトウェアを含む特定のベンダー情報の詳細を示します。

デスクトップ仮想化関連のリンク

Citrix

XenDesktop 4 @ Citrix ナレッジ ベース
http://support.citrix.com/proddocs/index.jsp

『Best Practices for Citrix XenDesktop with Provisioning Server』

http://support.citrix.com/article/CTX119849

『Citrix XenDesktop Modular Reference Architecture』
http://support.citrix.com/article/CTX124087

『Citrix XenDesktop - Design Handbook』
http://support.citrix.com/article/CTX120760

Citrix XenServer：ドキュメント
http://docs.vmd.citrix.com/XenServer/5.6.0/1.0/en_gb/

データセンター関連のリンク

シスコのデータセンターのデザイン ゾーン

http://www.cisco.com/en/US/netsol/ns743/networking_solutions_program_home.html
『Best Practices in Deploying Cisco Nexus 1000V Series Switches on Cisco UCS B Series Blade Servers』

http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9902/white_paper_c11-558242.html
『Citrix XenDesktop Deployment Guide』

http://www.citrix.com/%2Fsite%2Fresources%2Fdynamic%2Fsalesdocs%2FXD_Enterprise_Design_White_Paper.pdf
Citrix XenServer 5.6 ドキュメント

http://support.citrix.com/product/xens/v5.6/
『Scalability Study for Deploying VMware View on Cisco UCS and EMC Symmetrix V-Max Systems』

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/App_Networking/vdiucswp.html

ネットワーク関連のリンク

Cisco WAAS Central Manager GUI の概要

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v421/configuration/guide/intro.html#wp1122501

『Configuring Traffic Interception』

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v4013/configuration/guide/traffic.html

『Configuring Application Acceleration』

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v4013/configuration/guide/policy.html

『Configuring Network Settings』

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v4013/configuration/guide/network.html

『Configuring and Managing WAAS Print Services』

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v4013/configuration/guide/printsvr.html

データセンター

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_3_0/DC-3_0_IPInfra.html

キャンパス

http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/HA_campus_DG/hacampusdg.html

ブランチ/WAN

http://www.ciscosystems.com/en/US/docs/solutions/Enterprise/Branch/srlgbrnt.pdf

物理インターフェイス

http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA1_7_/configuration/device_manager/guide/UG_ntwk.html

管理アクセス

http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/v3.00_A1/configuration/administration/guide/access.html

リソース管理

http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA1_7_/configuration/device_manager/guide/UG_confg.html#wp2700097

ハイ アベイラビリティ

http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA1_7_/configuration/device_manager/guide/UG_ha.html

『Configuring Virtual Contexts』

http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA1_7_/configuration/device_manager/guide/UG_confg.html

ワンアーム モードの設定

http://www.cisco.com/en/US/docs/interfaces_modules/services_modules/ace/vA2_3_0/configuration/getting/started/guide/one_arm.pdf

Citrix DV に対する仮想コンテキストの設定

http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA1_7_/configuration/device_manager/guide/UG_lb.html#wp1044682

セッションの持続性の設定

http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA1_7_/configuration/device_manager/guide/UG_lb.html#wp1062118

ヘルス モニタリングの設定

http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA1_7_/configuration/device_manager/guide/UG_lb.html#wp1045366

バランシング アルゴリズム

http://www.cisco.com/en/US/docs/app_ntwk_services/data_center_app_services/ace_appliances/vA1_7_/configuration/device_manager/guide/UG_lb.html#wp1045366

送信元 NAT の設定

http://docwiki.cisco.com/wiki/Basic_Load_Balancing_Using_One_Arm_Mode_with_Source_NAT_on_the_Cisco_Application_Control_Engine_Configuration_Example

『Cisco Enterprise Campus 3.0 Architecture』

http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/campover.html

エンドポイントとアプリケーション関連のリンク

『Cisco Wide Area Application Services (WAAS) Configuration Guide』

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v421/configuration/guide/cnfgbook.pdf

『Citrix Guide for Limiting Printing Bandwidth』

http://support.citrix.com/proddocs/index.jsp?topic=/xenapp5fp-w2k8/ps-printing-limiting-printing-bandwidth-all.html

『Cisco Unified SRST Configuration Guide』

http://www.cisco.com/en/US/docs/voice_ip_comm/cusrst/admin/srst/configuration/guide/SRST_SysAdmin.pdf

『Cisco Unified Communications 8.X SRND』

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/srnd/8x/uc8xsrnd.pdf

『Cisco Unified Personal Communicator User's Guide』

http://www.cisco.com/en/US/docs/voice_ip_comm/cupc/7_0/english/user/guide/windows/CUPC_7.0_UG_win.pdf

管理と運用関連のリンク

VMWare View 4.0 用シスコ導入ガイド

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/vmware/cisco_VMwareView.html

『Cisco UCS GUI Configuration Guide』

http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/1.3.1/UCSM_GUI_Configuration_Guide_1_3_1.pdf

『Cisco Unified Communications Manager Systems Guide』

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_0_2/ccmsys/accm.pdf

Citrix XenDesktop 4 ドキュメント

http://support.citrix.com/proddocs/index.jsp

NetApp Provisioning Manager

http://www.netapp.com/us/products/management-software/provisioning.html

Altiris のリファレンス文書

http://www.symantec.com/business/theme.jsp?themeid=altiris

Microsoft Active Directory およびネットワーク サービス

http://www.microsfoft.com/

『Cisco Network Analysis Module Deployment Guide』

http://www.cisco.com/en/US/prod/collateral/modules/ps2706/white_paper_c07-505273.html#wp9000247

Cisco NAM アプライアンス ドキュメント（コマンド リファレンスおよびユーザ ガイド）

http://www.cisco.com/en/US/partner/products/ps10113/tsd_products_support_series_home.html

『Cisco Wide Area Application Services Configuration Guide (Software Version 4.1.1)』

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v411/configuration/guide/cnfg.html

『Cisco Adaptive Security Device Manager Configuration Guide』

http://www.cisco.com/en/US/products/ps6121/tsd_products_support_configure.html

Cisco ACE 4700 シリーズ アプリケーション コントロール エンジン アプライアンス ドキュメント

http://www.cisco.com/en/US/products/ps7027/tsd_products_support_series_home.html

『Cisco UCS Manager Configuration Guide』

http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html

Cisco DCNM ドキュメント

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_configure.html

Cisco Fabric Manager ドキュメント

http://www.cisco.com/en/US/partner/products/ps10495/tsd_products_support_configure.html

Cisco Nexus 1000v ドキュメント

http://www.cisco.com/en/US/partner/products/ps9902/products_installation_and_configuration_guides_list.html

Cisco Prime ドキュメント

http://www.cisco.com/en/US/partner/products/sw/cscowork/ps4565/tsd_products_support_maintain_and_operate.html

『Wyse Device Manager Overview』

http://www.wyse.com/products/software/devicemanager/index.asp

『WDM Admin Guide (release 4.7.2)』

https://support.wyse.com/OA_HTML/cskatch.jsp?fileid=ZG9507DDFF08D288306AC95C3C3F78B52551F2D290D30D2F9F&jttst0=6_23871%2C23871%2C-1%2C0%2C&jtfm0=&etfm1=&jfn=ZG48219F51800ECBD67A914E693A1B35C69EBAE7BDBF7E5DDCF04394392EFE18816C09F686220DF682859E9756A62205A14A

『WDM Install Guide (release 4.7.2)』

https://support.wyse.com/OA_HTML/cskatch.jsp?fileid=ZG2FBE29B2F0CB4CE374726CACD3884A4E9ADCB633B42A7DA3&jttst0=6_23871%2C23871%2C-1%2C0%2C&jtfm0=&etfm1=&jfn=ZG48219F51800ECBD67A914E693A1B35C69EBAE7BDBF7E5DDCF04394392EFE18816C09F686220DF682859E9756A62205A14A

『Wyse Device Manager Integration Add-ons Admin Guide』

https://support.wyse.com/OA_HTML/cskatch.jsp?fileid=ZG1C1D43ABA80F795F39F06E7C573159728391066249DD919D&jttst0=6_23871%2C23871%2C-1%2C0%2C&jtfm0=&etfm1=&jfn=ZG48219F51800ECBD67A914E693A1B35C69EBAE7BDBF7E5DDCF04394392EFE18816C09F686220DF682859E9756A62205A14A

『Wyse® Thin Clients, Based on Microsoft® Windows® XP Embedded, Admin Guide』

https://support.wyse.com/OA_HTML/cskatch.jsp?fileid=ZG42949BF90AE7F9412C1C931422B780A1FEAB5C2D8D0D1645&jttst0=6_23871%2C23871%2C-1%2C0%2C&jtfm0=&etfm1=&jfn=ZGC29B519BFE0416A1A6FCE711FE7D993C9F7AA9C19B22F9C27470952552D8AE1777F9506FF6A0200B96E81A03AFC23839E6

『Wyse Viance Admin Guide』

https://support.wyse.com/OA_HTML/cskatch.jsp?fileid=ZG841C2F2087C671DBE3AA9E0203EC8523A6D6C2A5C8D157DD&jttst0=6_23871%2C23871%2C-1%2C0%2C&jtfm0=_0_1_0_-1_f_nv_&etfm1=&jfn=ZG0165717AA38109A13472984D2B8D94D79D98F9322001A2A71A96398EC4D334BE62DA4D17DCD2B34E7A8

『Wyse P20 Admin Guide』

https://support.wyse.com/OA_HTML/cskatch.jsp?fileid=ZG012BFCA92639876559ACEEF431B166341DBDF9D663D2886D&jttst0=6_23871%2C23871%2C-1%2C0%2C&jtfm0=_0_1_0_-1_f_nv_&etfm1=&jfn=ZG1822D032C06C7952267DE698A72D680888C4CF4D85AE20A616CFC0617832C14C20C36ACA3BEE6A94BFD

『Devon IT Echo™ Thin Client Management Software Version 3 Overview』

http://www.devonit.com/software/echo/overview

『Devon ThinManage 3.1 Admin Guide』

http://downloads.devonit.com/Website/public/Documentation/thinmanage-3-1-adminguide-rev12.pdf

『Devon IT TC5 Terminal Quick Start Guide』

http://www.devonit.com/_wp/wp-content/uploads/2009/04/tc5-quickstartguide-devonit-english.pdf

IGEL Universal Management Suite 3 の概要

http://www.igel.com/igel/live.php,navigation_id,3294,_psmand,9.html

『IGEL Universal Management Suite 3 Install Guide』

http://www.download-igel.com/index.php?filepath=manuals/english/universalmanagement/&webpath=/ftp/manuals/english/universalmanagement/&rc=emea

『IGEL Universal Management Suite 3 User Guide』

http://www.download-igel.com/ftp/manuals/english/universalmanagement/IGEL%20UMS%20User%20Guide.pdf

『IGEL Universal Desktops User Guide』

http://www.download-igel.com/ftp/manuals/english/universalmanagement/IGEL%20UMS%20User%20Guide.pdf

Cisco UMS ドキュメント

http://www.cisco.com/

Cisco VXI セキュリティ関連のリンク

Cisco SAFE アーキテクチャ ガイド

http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.pdf

Cisco Data Center 3.0 セキュリティ ガイド

http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/DC_3_0/dc_sec_design.pdf

Cisco Identity-Based Network セキュリティ ガイド

http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/CiscoIBNS-Technical-Review.pdf

Cisco 3650 コマンド リファレンス ガイド

http://www.cisco.com/en/US/docs/switches/lan/catalyst3560/software/release/12.2_35_se/command/reference/cli1.html#wp2757193

『Cisco Business Ready Teleworker Design Guide』

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns171/c649/ccmigration_09186a008074f24a.pdf

『Cisco ASA 8.x : VPN Access with the AnyConnect VPN Client Configuration Example』

http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00808efbd2.shtml

Citrix :『How to Disable USB Drive Redirection』

http://support.citrix.com/article/CTX123700

Microsoft :「Disabling Remote Desktop Services Features」

http://msdn.microsoft.com/en-us/library/aa380804%28VS.85%29.aspx

Quality of Service（QoS）関連のリンク

『Cisco UCS GUI Configuration Guide』

http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/1.3.1/UCSM_GUI_Configuration_Guide_1_3_1.pdf

『Cisco Unified Communications Manager Systems Guide』

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_0_2/ccmsys/accm.pdf

パフォーマンスとキャパシティ関連のリンク

『Reference Architecture-Based Design for Implementation of Citrix XenDesktops on Cisco Unified Computing System, VMware vSphere, and NetApp Storage』

http://preview.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/Virtualization/ucs_xd_vsphere_ntap.pdf

付録 1：Microsoft Hyper V 使用時の特別な考慮事項

Hyper-V の概要

Windows Server 2008 および Windows Server 2008 R2 の Hyper-V では、仮想化サーバ コンピューティング環境を構築できます。仮想化コンピューティング環境を使用すると、ハードウェア リソースをより有効に活用し、コンピューティング リソースの効率性を高めることができます。こうした利点は、仮想マシンとそのリソースを作成および管理できる Hyper-V の機能によって実現されます。各仮想マシンは、分離された実行環境で動作する仮想化コンピュータです。仮想マシンを使用すると、1 台の物理コンピュータ上で、同時に複数のオペレーティング システムを実行できます。

Hyper-V にはソフトウェア インフラストラクチャと基本的な管理ツールが用意されており、仮想化サーバ コンピューティング環境の構築と管理に使用できます。この仮想化環境を利用して、効率性の向上とコストの削減を目的としたさまざまな業務目標に取り組むことができます。たとえば、仮想化サーバ環境は以下のような点において有益です。

- ハードウェアの使用率を高めることで、物理サーバの運用および管理コストを削減します。サーバの作業負荷を実行するために必要なハードウェア数を低減できます。
- ハードウェアとソフトウェアのセットアップにかかる時間を短縮し、テスト環境を再現することで、開発とテストの効率性を高めます。
- 物理コンピュータのみを使用するフェールオーバー設定と同じ数の物理コンピュータを使用しなくても、サーバの可用性が向上します。

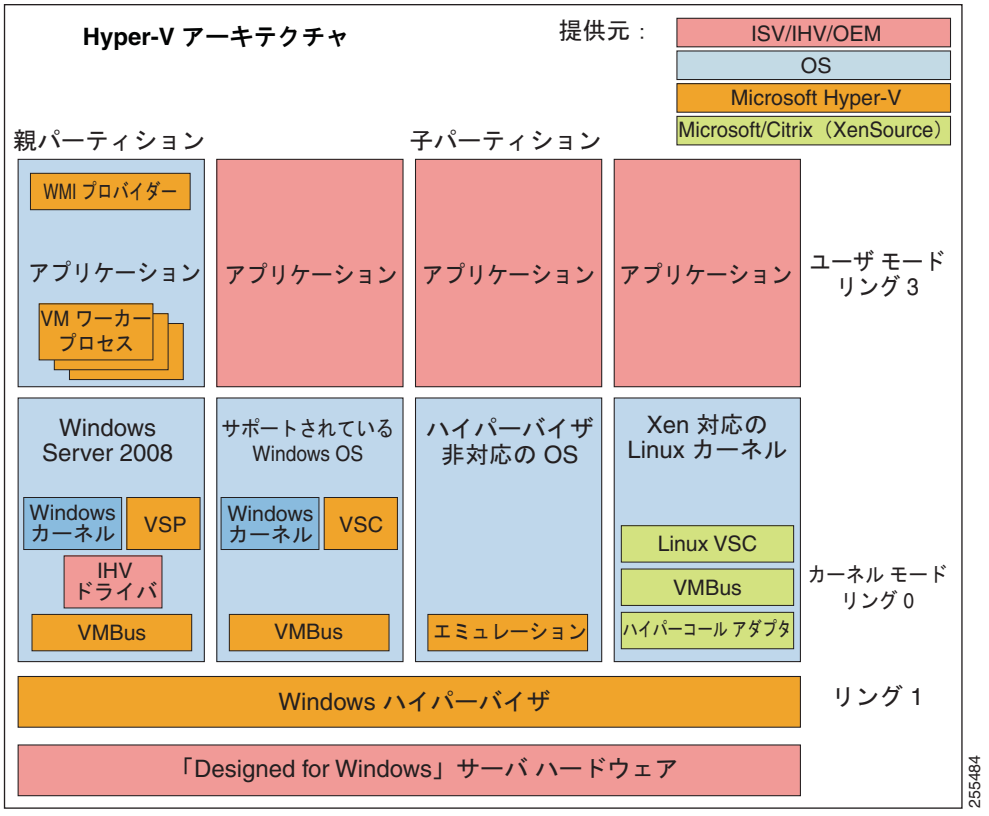
Hyper-V のアーキテクチャと機能の概要

Hyper-V™ は Windows Server® 2008 R2 の一機能で、仮想化サーバ コンピューティング環境の構築と管理に使用できるツールとサービスを提供します。この仮想化環境では、仮想マシンを作成および管理して、たとえ異なるオペレーティング システムが使用されていたとしても、1 台の物理コンピュータ上で複数のコンピュータを実行できます。仮想化環境では、仮想マシンを隔離したり、仮想マシン間および仮想マシンと外部ネットワーク間の通信方法を指定したりすることができます。Windows Server 2008 R2 Hyper-V では、初版の Hyper-V に新機能が追加されています。たとえば、Windows Server 2008 R2 Hyper-V のライブ マイグレーションでは、動作中の VM を 1 台の物理コンピュータから別のコンピュータへ移動したり、動作している VM のストレージを追加または削除したりすることができます。さらに Windows Server 2008 R2 Hyper-V では、プロセッサ サポートと物理コンピュータ ハードウェア サポートが強化されており、物理コンピュータ ハードウェアを十分に有効活用できます。

Hyper-V アーキテクチャ

Hyper-V は信頼性の高い仮想化プラットフォームが用意されており、お客様のインフラストラクチャの仮想化とコスト削減を実現します。Hyper-V は、攻撃可能領域を最小限に抑えた、軽量でマイクロカーネル化されたハイパーバイザ アーキテクチャを備えており、Server Core ロールとして利用できます。System Center 統合管理ツールを使用すると、お客様は物理リソースと仮想リソースの両方を 1 つのツール セットで管理できます。Hyper-V は、お客様の既存のパッチ、プロビジョニング、管理、およびサポート ツールとそのプロセスを活用するので、お客様の IT インフラストラクチャに容易に組み込むことができます。Hyper-V は Windows Server 2008 R2 の一機能として使用でき、お客様は Microsoft パートナー、既存の IT Pro スキル セット、および Microsoft による総合サポートから広範囲なソリューションを利用できるという点で、大きな価値があります。

図 150　　Hyper-V Architecture22 のインフラストラクチャ コンポーネント



Hyper-V の主な機能

- ライブ マイグレーション

  Windows Server 2008 R2 の Hyper-V には、たいへん待ち望まれていたライブ マイグレーション機能が搭載されています。これは、サービスを中断することなく、2 台の仮想化ホスト サーバ間で仮想マシンを移動できる機能です。Hyper-V ライブ マイグレーションは、Windows Server 2008 R2 Hyper-V および Microsoft Hyper-V Server 2008 R2 に統合されています。Hyper-V ライブ マイグレーションでは、動作中の VM を 1 台の Hyper-V 物理ホストから別のホストへ移動でき、それによってサービスが中断されたり、識別できるほどのダウンタイムが発生することはありません。Hyper-V ライブ マイグレーションを使用して、ダウンタイムなしで VM を移動すると、次のような効果が得られます。

  - 俊敏性の向上。複数の Hyper-V 物理ホストを収容しているデータセンターは、動作中の VM を最適な物理コンピュータへ移動して、ユーザに影響を及ぼすことなくパフォーマンスの強化、拡張、または最善の統合を実現できます。
  - コスト削減と生産性の向上。複数の Hyper-V 物理ホストを収容しているデータセンターは、通常の業務時間中にメンテナンスをスケジュールし、適切に制御された方法でそれらのシステムにサービスを提供できます。ライブ マイグレーションでは、メンテナンス中であっても VM をオンライン状態で維持できるので、ユーザおよびサーバ管理者の生産性が向上します。データセンターは、統合比率を動的に増やし、需要が少ない時間帯は使用されていない物理ホストをオフにすることで、消費電力を削減することもできます。

- Hyper-V 仮想マシン向けハードウェア サポートの強化

  現在、Windows Server 2008 R2 の Hyper-V では、ホスト プロセッサ プール内で最大 64 台の論理プロセッサがサポートされます。これは前バージョンからの大幅なアップグレードで、ホストあたりの VM 密度が増大するだけでなく、IT 管理者は CPU リソースをより柔軟に VM に割り当てることができます。さらに、ライブ マイグレーション向けの新機能である Hyper-V プロセッサ互換モードでは、同じプロセッサ ファミリ内の異なる CPU バージョン間で VM を移動でき（たとえば、Intel Core 2 から Intel Pentium 4、または AMD Opteron から AMD Athlon への移行など）、より広範囲なサーバ ホスト ハードウェア間での移行を実行できます。

- クラスタ共有ボリューム

  Windows Server 2008 R2 の Hyper-V は、Cluster Shared Volume（CSV; クラスタ共有ボリューム）を使用して、共有ストレージの使用法を簡素化および強化します。CSV では、全ホストのすべてのボリュームに対して 1 つの統一された名前空間を使用することで、複数の Windows Server が SAN ストレージにアクセスできます。複数のホストは、SAN ストレージの同じ Logical Unit Number（LUN; 論理ユニット番号）にアクセスできます。CSV をクラスタ構成で使用すると、ライブ マイグレーションが高速化され、Hyper-V のストレージ管理が容易になります。クラスタ共有ボリュームは、Windows Server 2008 R2 の Windows フェールオーバー クラスタリング機能の一部として使用できます。

- クラスタ ノード接続の耐障害性の向上

  CSV のアーキテクチャによって、クラスタ上で動作する VM に直接影響を与えるクラスタ ノード接続の耐障害性が強化されました。CSV アーキテクチャには、動的 I/O リダイレクトとして知られるメカニズムが実装されています。これは、接続の可否に基づいて I/O をフェールオーバー クラスタ内でルーティングできるメカニズムです。

- クラスタ検証ツールの改良
- Windows Server 2008 R2 には、フェールオーバー クラスタリングをはじめとするすべての主要サーバ ロールに使用できる Best Practices Analyzer（BPA; ベスト プラクティス アナライザ）が搭載されています。このアナライザは、クラスタおよびクラスタ ノードのベスト プラクティス構成の設定を検証します。
- 仮想データセンターの管理の強化

- 仮想化によってあらゆる効率性が向上したとしても、VM の管理は引き続き必要です。通常、仮想マシンはハードウェアを装備する必要がないため、VM の数は物理コンピュータよりも急速に増大する傾向があります。したがって、仮想データセンターの管理はこれまで以上に重要な業務です。
- 仮想ネットワーキングのパフォーマンスの向上
- 新しい Hyper-V では、Windows Server 2008 R2 に含まれる複数の新しいネットワーキング テクノロジーを活用して、VM ネットワーク全体のパフォーマンスが強化されています。
- パフォーマンスの向上と消費電力の削減

  Windows Server 2008 R2 の Hyper-V には、仮想マシンの消費電力を削減する拡張機能が追加されています。現在、Hyper-V では Second Level Address Translation（SLAT）がサポートされています。SLAT は最新型 CPU の新機能を使用して、Windows Hypervisor での処理負荷を低減すると同時に VM のパフォーマンスを向上させます。さらに、新しい Hyper-V VM では、Windows Server 2008 R2 に実装されたコア パーキング機能によって、消費電力が低減されます。
- ネットワーキング サポートの強化

  Windows Server 2008 R2 には、仮想ネットワークのパフォーマンスを向上させる 3 つの新しいネットワーキング機能が搭載されています。これまで非仮想環境で使用されていたジャンボ フレーム向けのサポートが、VM にも対応できるよう拡張されました。基盤となる物理ネットワークでジャンボ フレームがサポートされていれば、VM は最大 9014 バイトのジャンボ フレームを使用できます。ジャンボ フレームのサポートによってバイトあたりのネットワーク スタック オーバーヘッドが削減され、スループットが向上します。また、ネットワーク スタックからネットワーク ドライバへのコール数が少ないため、CPU 使用率が大幅に低減されます。

  TCP/IP 処理をネットワーク ハードウェアにオフロードできる TCP Chimney 機能は、仮想環境にも対応できるよう拡張されました。VM はネットワーク処理をハードウェアにオフロードできるようになり、特に帯域幅が 1 GB を超えるネットワークでは VM のパフォーマンスが向上します。この機能は、ファイル サーバなど大量のデータ転送を伴う役割では特に有益です。

  Virtual Machine Queue（VMQ）機能では、物理コンピュータの Network Interface Card（NIC; ネットワーク インターフェイス カード）が Direct Memory Access（DMA）を使用してパケットのコンテンツを VM メモリに直接配置でき、I/O パフォーマンスも向上します。
- 動的 VM ストレージ

  Windows Server 2008 R2 Hyper-V は、ストレージのホット プラグインとホット削除をサポートします。VM の動作中に Virtual Hard Drive（VHD; 仮想ハード ドライブ）ファイルとパススルー ディスクを追加および削除できるので、Windows Server 2008 R2 Hyper-V では作業負荷要件の変動に合わせて VM を迅速に再設定できます。この機能を使用すると、既存の VM 用 SCSI コントローラで VHD ファイルとパススルー ディスクの両方を追加および削除することができます。
- 広範囲な OS サポート

  広範囲なサポートにより、Windows や Linux など異なるサーバ プラットフォーム上で、32 ビットと 64 ビットなど種類の異なるオペレーティング システムを同時に実行できます。
- ネットワーク ロード バランシング

  Hyper-V には新しい仮想スイッチ機能が搭載されています。つまり、仮想マシンを Windows Network Load Balancing（NLB）Service と連動するように簡単に設定でき、それによって異なるサーバ上にある仮想マシン間で負荷を分散できます。
- ネットワーク ハードウェア共有アーキテクチャ

  新しい Virtual Service Provider/Virtual Service Client（VSP/VSC; 仮想サービス プロバイダー / 仮想サービス クライアント）アーキテクチャによって、Hyper-V ではディスク、ネットワーキング、ビデオなどコア リソースへのアクセスとその利用効率が改良されています。

- 仮想マシン スナップショット

  Hyper-V は動作中の仮想マシンのスナップショットを作成する機能を備えているので、容易に以前の状態に戻ることができます。また、バックアップおよび回復ソリューションも全面的に改良されています。

- 高い拡張性

  Hyper-V で標準ベースの Windows Management Instrumentation（WMI）インターフェイスおよび API を使用すると、独立系ソフトウェア ベンダーや開発者は仮想化プラットフォーム向けのカスタム ツール、ユーティリティ、拡張機能を容易に構築できます。

仮想化と Hyper-V の詳細については、http://www.microsoft.com/windowsserver2008/en/us/hyperv-technical-resources.aspx を参照してください。

仮想マシンの管理

仮想化によってあらゆる効率性が向上したとしても、仮想マシンの管理は引き続き必要です。通常、仮想マシンはハードウェアを装備する必要がないため、仮想マシンの数は物理コンピュータよりも急速に増大する傾向があります。したがって、仮想データセンターの管理はこれまで以上に重要な業務です。

仮想デーセンターの管理に役立つ Windows Server 2008 R2 の改良点を次に示します。

- Hyper-V 管理コンソールの使用によって、日常的な Hyper-V 管理タスクの負担を軽減します。
- PowerShell cmdlet の使用により、コマンドライン インターフェイスを拡張し、Hyper-V 管理タスクを自動化します。
- System Center Virtual Machine Manager 2008 の使用により、仮想データセンター環境での複数の Hyper-V サーバの管理を強化します。

System Center Virtual Machine Manager（Virtual Machine Manager）

System Center Virtual Machine Manager 2008 R2 は、仮想環境の管理と運用を一元化し、物理サーバの使用率を増やし、Virtual Machine Manager 管理者および認定セルフサービスのエンド ユーザによる新規仮想マシンのプロビジョニングを高速化します。

Virtual Machine Manager の実装は、特定の必須コア コンポーネントとオプションのコンポーネントで構成され、必要に応じてユーザの環境に実装できるのが特徴です。

Virtual Machine Manager サーバ

Virtual Machine Manager サーバは Virtual Machine Manager 実装のハブであり、他のすべての Virtual Machine Manager コンポーネントはこのサーバを介して対話と通信を行います。したがって、最初に Virtual Machine Manager サーバをインストールする必要があります。

Virtual Machine Manager サーバは、Virtual Machine Manager サービスを実行します。このサービスでは、コマンドの実行、ファイル転送、他の Virtual Machine Manager コンポーネント、すべての仮想マシン ホスト、および Virtual Machine Manager ライブラリ サーバ（これらをまとめて管理対象コンピュータと呼びます）との通信制御を行います。

Virtual Machine Manager サーバは、すべての Virtual Machine Manager の設定情報が保存された SQL Server データベースにも接続します。この情報にアクセスして Virtual Machine Manager を設定するには、Virtual Machine Manager Administrator Console または Windows PowerShell - Virtual Machine Manager コマンド シェルを使用します。Windows PowerShell - Virtual Machine Manager コマンド シェルの詳細については、スクリプトを参照してください。

デフォルトでは、Virtual Machine Manager サーバはデフォルト ライブラリ サーバでもあります。Virtual Machine Manager ライブラリを使用して、仮想ハード ディスク（保存済み仮想マシンに接続されている場合を除く）、テンプレート、ISO イメージ、PowerShell スクリプト、アンサー ファイル、仮想マシンなど、ファイルベースのリソースを保存できます。追加の Virtual Machine Manager ライブラリを設定することもできます。これは、大量のホストを管理する場合に推奨されます。

Virtual Machine ライブラリ サーバ

Virtual Machine Manager ライブラリはリソースのカタログであり、Virtual Machine Manager での仮想マシンの作成と設定に使用できます。

ライブラリには次のタイプのリソースを保存できます。

- 仮想ハード ディスク、仮想フロッピー ディスク、ISO イメージ、スクリプトなどファイルベースのリソース。Virtual Machine Manager で使用できるようにするには、ファイルをライブラリに追加しなければなりません。そのためには、指定されたライブラリ共有にあるライブラリ サーバにファイルを保存する必要があります。詳細については、『Adding File-Based Resources to the Library』を参照してください。Virtual Machine Manager ライブラリで保存可能なファイル タイプ一覧については、『File Types That Are Indexed During a Library Refresh』を参照してください。
- 標準仮想マシンの作成用に [Library] ビューで設定された仮想マシン テンプレート、ハードウェア プロファイル、およびゲスト オペレーティング システム プロファイル。これらの設定は Virtual Machine Manager データベースに保存されますが、物理的なコンフィギュレーション ファイルでは表示されません。
- 使用されていない仮想マシン。仮想マシンは [Library] ビューに表示されます。ただし、保存済み仮想マシンに対応するファイルは、新規仮想マシンの作成または設定に使用できないためライブラリでは表示されません。

Virtual Machine Manager サーバは、常にデフォルト ライブラリ サーバです。Virtual Machine Manager サーバをインストールする場合、[Setup] を使用すると、ライブラリ共有が Virtual Machine Manager サーバ上に自動的に作成されます。デフォルト ライブラリ サーバには、別のライブラリ共有を追加できます。

Virtual Machine Manager サーバのインストール後は、他のコンピュータをライブラリ サーバとして追加することができます。これについては、このトピックの後半の「オプションの Virtual Machine Manager コンポーネントと機能」で説明します。ただし、Virtual Machine Manager サーバ上のデフォルト ライブラリ サーバやそのライブラリ共有を削除したり移動したりすることはできません。したがって、Virtual Machine Manager サーバをインストールする前に、デフォルト ライブラリ共有の場所については十分考慮してください。コンピュータをライブラリ サーバとして追加すると、Virtual Machine Manager はそのコンピュータに自動的に Virtual Machine Manager エージェントをインストールします。

Virtual Machine Manager データベース

Virtual Machine Manager データベースには、Virtual Machine Manager のすべての設定情報が保存されます。Virtual Machine Manager Administrator Console を使用すると、この情報にアクセスして変更することができます。Virtual Machine Manager データベースは Virtual Machine Manager サーバのインストール時に指定します。

Virtual Machine Manager データベースには、サポートされている Microsoft SQL Server のバージョンが必要です。既存の Microsoft SQL Server データベースのローカルまたはリモート インスタンスを指定するか、あるいは [Setup] ウィザードで SQL Server 2005 Express Edition SP2 を Virtual Machine Manager サーバにインストールすることができます。[Setup Wizard] では、ローカル コンピュータでの SQL Server 2005 ツールのインストールと、MICROSOFT$Virtual Machine Manager$ という SQL Server インスタンスの作成も実行されます。

150 台を超えるホストを管理する、あるいは Operations Manager 2007 と Virtual Machine Manager を統合して Performance and Resource Optimization（PRO）のヒントとレポートを実装する計画がある場合は、SQL Server の Standard または Enterprise バージョンを使用する必要があります。サポートされる SQL Server のバージョンの詳細については、『System Requirements: Virtual Machine Manager Database』を参照してください。

Virtual Machine Manger Administrator Console

Virtual Machine Manager Administrator Console は、次の目的に使用する Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）です。

- 仮想マシンの作成、コピー、管理
- ホストおよびライブラリ サーバの監視と管理
- グローバル コンフィギュレーション設定の管理

Virtual Machine Manager サーバをインストールしたら、Virtual Machine Manager Administrator Console をインストールし、それを Virtual Machine Manager サーバに接続します。同一のコンピュータまたは別のコンピュータに、Virtual Machine Manager Administrator Console を Virtual Machine Manager サーバとしてインストールできます。Virtual Machine Manager Administrator Console は複数のコンピュータにインストールでき、それを使用して任意の Virtual Machine Manager サーバに接続し、管理することができます。Virtual Machine Manager サーバは一度に 1 台のみ接続および管理できます。

Virtual Machine Manager Administrator Console をインストールすると、[Setup] によって Windows PowerShell - Virtual Machine Manager コマンド シェルもインストールされます。これにより、コマンドラインから cmdlets を使用できるようになり、Virtual Machine Manager Administrator Console で使用可能なすべての機能を実行できます。

仮想マシン ホスト

仮想マシン ホストは、1 台または複数の仮想マシンをホストする物理コンピュータです。Virtual Machine Manager Administrator Console の [Add Hosts] ウィザードを使用すると、Virtual Machine Manager に 1 台以上のホストを追加できます。ホストを追加しない限り、Virtual Machine Manager を使用して仮想マシンを作成することはできず、Virtual Machine Manager Administrator Console の多くのアクションを利用できません。Windows Server ベースのホストを追加すると、Virtual Machine Manager はそのホストに自動的に Virtual Machine Manager エージェントをインストールします。そのホストに適切な仮想化ソフトウェアがインストールされていない場合は、これをインストールして有効化します。

Virtual Machine Manager でサポートされるホスト タイプは次のとおりです。

- Virtual Machine Manager サーバの AD ドメインと双方向の信頼関係を持たない AD ドメインに配置された Windows Server ベースのホスト。
- 境界ネットワークに配置された Windows Server ベースのホスト。
- 結合されていない名前空間に配置された Windows Server ベースのホスト。この名前空間では、Domain Name Service（DNS; ドメイン名サービス）で解決されたホストの Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）は、AD から取得した名前と同じではありません。
- ユーザ環境内の任意の場所に配置された VMware ESX Server ホスト。

オプションの Virtual Machine Manager コンポーネントと機能

Virtual Machine Manager Self-Service Portal

Virtual Machine Manager Self-Service Portal はオプションの Web ベース コンポーネントです。Virtual Machine Manager 管理者はこれをインストールし、ユーザが制限付き仮想マシン ホスト グループ内の制御された環境で、独自の仮想マシンを作成および管理できるように設定できます。Virtual Machine Manager 管理者はセルフサービス ユーザ ロールを作成し、これによって各ユーザの仮想マシンにおけるユーザ アクションの範囲が決定されます。

セルフサービス ユーザは、Virtual Machine Manager Self-Service Portal を使用して仮想マシンを作成、操作、および管理します。管理者は、どのホスト グループのセルフサービス ユーザが仮想マシンを作成できるかを決定します。セルフサービス ユーザが仮想マシンを作成すると、その仮想マシンはホストの評価に基づいて、ホスト グループ内の最も適切なホストに自動的に配置されます。

Virtual Machine Manager 管理者は、セルフサービス ユーザ ロールに仮想マシンの割り当て数を設定し、仮想マシン テンプレートで割り当てポイントを指定して、ユーザまたはグループが配置可能な仮想マシンの数を制限できます。

Performance and Resource Optimization（PRO）

Performance and Resource Optimization（PRO）では、作業負荷およびアプリケーションに配慮したリソースの最適化を仮想化環境内で実行できます。PRO では、System Center Operations Manager 2007 の PRO 対応管理パックで提供されるパフォーマンスおよびヘルス データに基づいて、自動または手動で PRO ヒントを実装できます。PRO ヒントとは、ダウンタイムを最小限に抑え、問題解決の時間を短縮するための推奨事項です。詳細については、『About Performance and Resource Optimization (PRO)』を参照してください。

フェールオーバー クラスタリングと Hyper-V

フェールオーバー クラスタは、独立したコンピュータで構成されるグループで、アプリケーションとサービスの可用性を高めるために連携して動作します。クラスタ化されたサーバ（ノードと呼ばれる）は、物理ケーブルとソフトウェアによって接続されます。いずれかのクラスタ ノードに障害が発生すると、別のノードがサービスを開始します（フェールオーバーとして知られるプロセス）。ユーザへのサービスの中断は最小限に抑えられます。Windows Server 2008 R2 の注目すべき機能の一つであるライブ マイグレーションでは、Windows Server 2008 R2 のフェールオーバー クラスタリング ロールの中で新しい Cluster Shared Volume（CSV; クラスタ共有ボリューム）機能が使用されています。

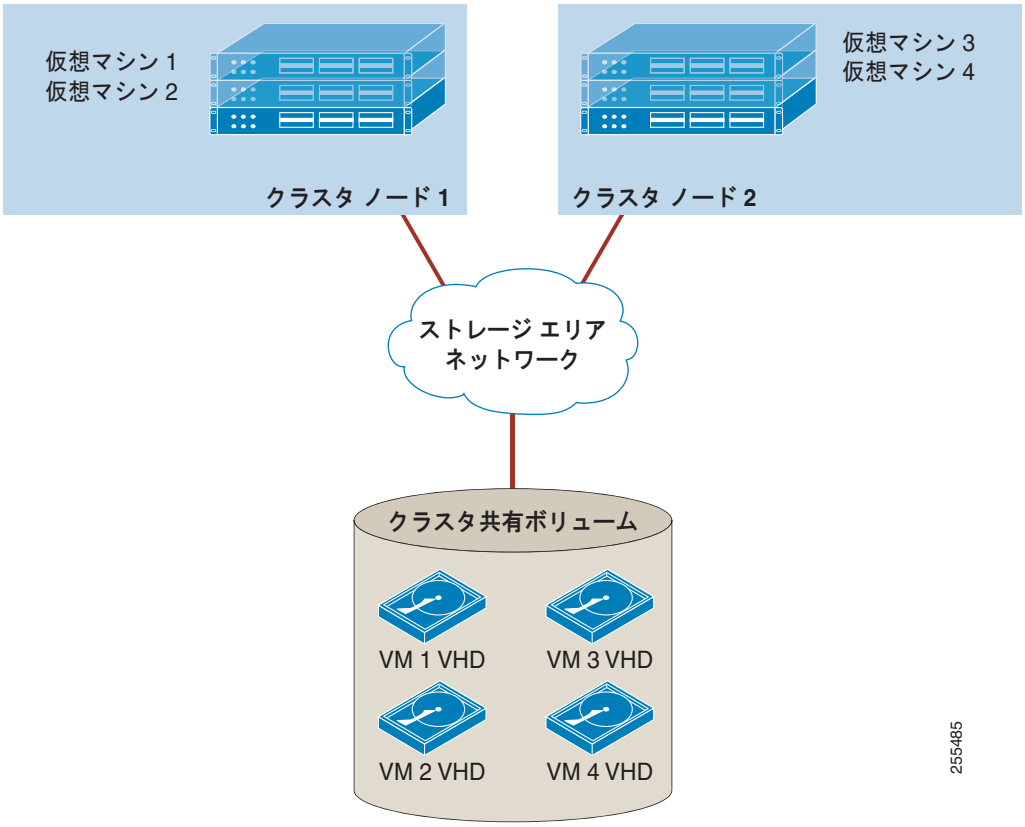
クラスタ共有ボリューム

Hyper-V 用に最適化された分散アクセス ファイル システムとして機能する Cluster Shared Volumes（CSV; クラスタ共有ボリューム）は、アーキテクチャにおける重要な技術革新であり、Microsoft Hyper-V Server 2008 R2 だけでなく、Windows Server 2008 R2 Enterprise と Windows Server 2008 R2 Datacenter のフェールオーバー クラスタリングにも組み込まれています。

Clustered File System（CFS; クラスタ化ファイル システム）と異なり、CSV は特化された専用のファイル システムを使用しません。SCV は標準の NTFS ファイル システムを使用するので、購入またはサポート後に何も追加する必要はありません。SCV では標準的なクラスタリング ストレージ デバイス、すなわちファイバ チャネル、iSCSI、またはシリアル接続 SCSI を使用できます。ただし、これらのデバイスに Windows Server 2008 R2 のロゴが表示され、完全なソリューションが [Validate a Configuration] ウィザードを通過する必要があります。

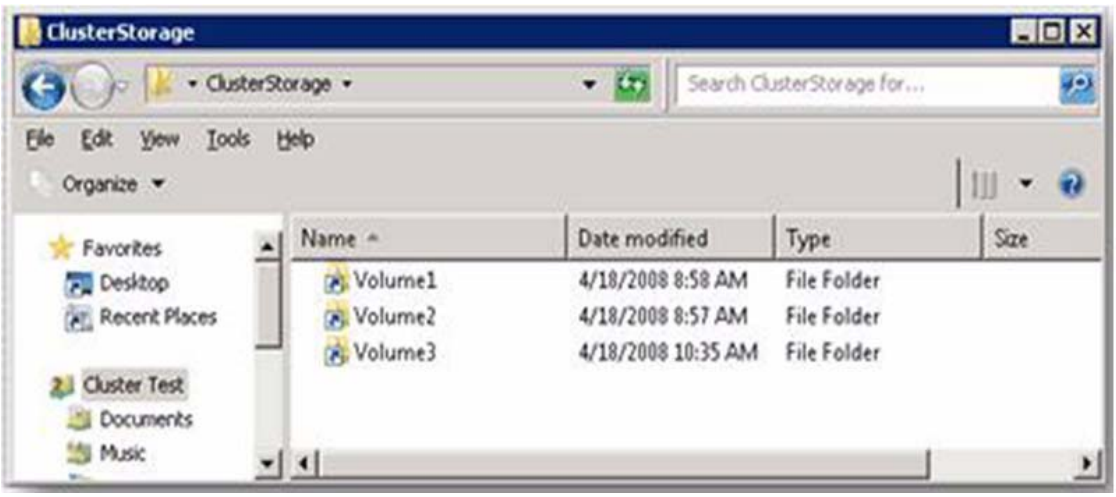
CSV を使用して、フェールオーバー クラスタ内のすべてのノードは共有ストレージにアクセスでき、仮想マシンをホストできます。ストレージを所有しているノード、あるいはストレージの NTFS を管理しているノードがどれであるかは関係ありません（図 151 を参照）。CSV には、容易なストレージ管理、強化された耐障害性、単一の LUN に多数の VM を格納できる機能など多数の利点があり、それぞれにフェールオーバー機能が備わっています。特に注目すべきは CSV のインフラストラクチャで、これによって Hyper-V 仮想マシンのライブ マイグレーションがサポートおよび強化されます。

図 151　　クラスタ共有ボリューム



CSV ではフェールオーバー クラスタ内のすべてのノードに一貫したファイル名前空間が提供されるので、CSV に保存されたファイルの名前とフェールオーバー クラスタ内のノードからのパスはすべて同じです。図 152 に示すように、CSV ボリュームは %SystemDrive%\ClusterStorage ルート フォルダの下にディレクトリおよびサブディレクトリとして保存されます。

図 152　CSV 内の単一の名前空間

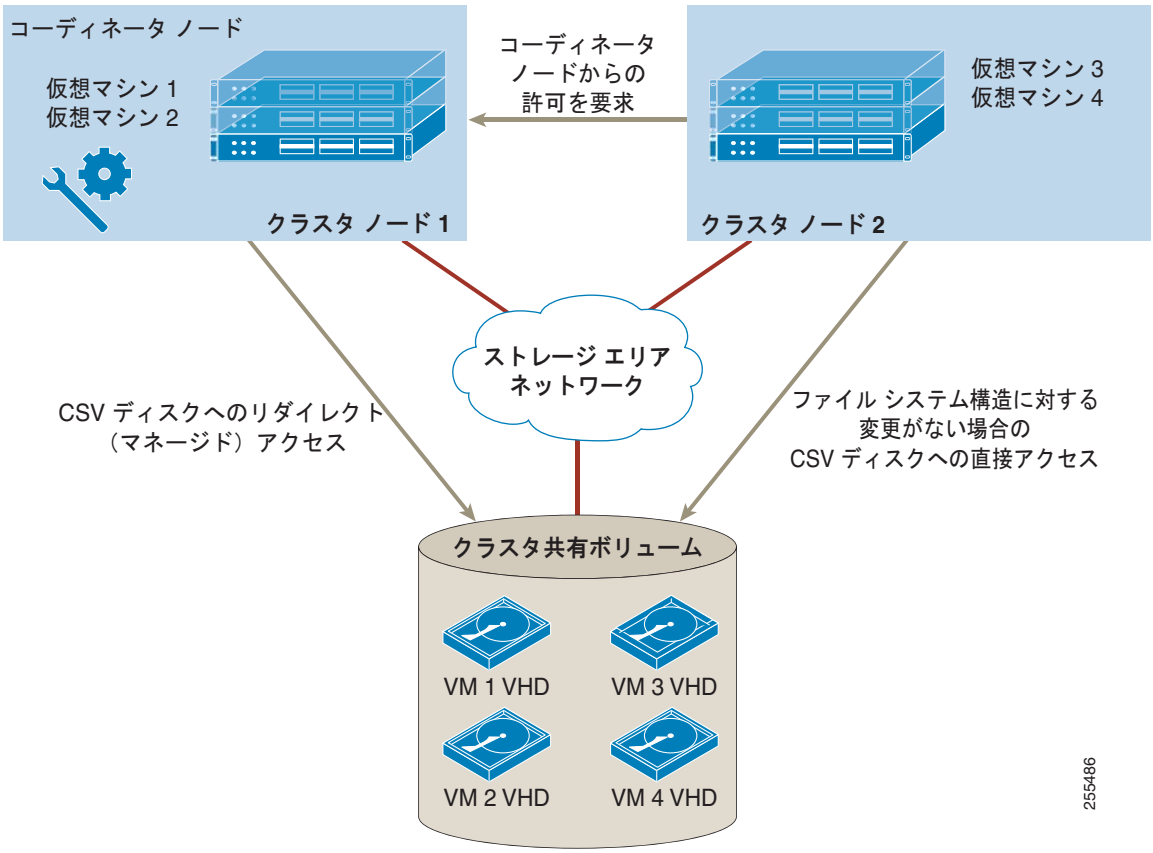


Windows Server 2008 および旧バージョンの Windows では、共有ストレージ デバイスに格納されたアプリケーション データへのクラスタからのアクセスを管理するために、各リソース グループに物理ディスク リソースが必要でした。このため、一度に 1 つのノードしかデータにアクセスできませんでした。ただし、常に 1 つのノードだけが LUN を所有できるので、LUN がフェールオーバーの最小単位でした。LUN で動作しているアプリケーションを別のノードへ移動する必要がある場合、その LUN 上のすべてのアプリケーションもフェールオーバーされます。このプロセスでは、フェールオーバー中にダウンタイムが発生することがありました。このためお客様は、多くの場合、各 LUN からアプリケーションを 1 つだけ実行し、フェールオーバー時に使用不能になるアプリケーションが 1 つですむようにしていました。このような方法はストレージ管理を非常に複雑にします。つまり、数百のリソースを持つクラスタに数百の LUN が必要になったため、導入と管理が難しくなりました。

CSV では、アプリケーション リソース（仮想マシン）とディスク リソース間の依存関係は排除されます。これにより、ディスクはフェールオーバー クラスタ内のすべてのノードでローカルに表示されるので、ディスクがどこに挿入されていても問題ありません。しかし CSV ディスク上のアプリケーションは、いつでもどのノードでも実行可能です。

CSV は、通常のクラスタ化ディスクとは異なる方法でストレージ アクセスを管理します（図 153 を参照）。フェールオーバー クラスタ内の任意のノードが調整ノードとして指定されます。CSV ディスクにデータを書き込む必要がある場合、アプリケーションは調整ノードに許可を要求します。データの書き込みによってファイル システム構造を変更する必要がなければ、調整ノードは書き込み可能ブロックのアドレスを送信し、ファイル システムに直接書き込むこと（LUN への直接アクセス）を VM に許可します。データがファイルの拡張、移動、または属性変更といったファイル システム構造の変更を必要としている場合、調整ノードはデータをディスクに書き込みます。このようにして調整ノードは NTFS ファイル システムへのアクセスを制御し、データの破損を防止します。

図 153　CSV の調整ノード



ライブ マイグレーション

Windows Server 2008 R2 のフェールオーバー クラスタリングでは、CSV によってライブ マイグレーションが改良されています。ライブ マイグレーションと CSV は別個の機能ですが、相補的なテクノロジーです。それぞれ独立して機能できますが、CSV によってライブ マイグレーションの耐障害性は向上します。こうした理由から、ライブ マイグレーションには CSV が推奨されます（必須ではありません）。CSV ボリュームを使用すると、同じフェールオーバー クラスタ内の複数のノードが同じ LUN へ同時にアクセスできます。VM 側からは、各 VM が実際に LUN を所有しているように見えますが、各 VM の .vhd ファイルは同じ CSV ボリュームに保存されています。

CSV は、Hyper-V を使用したライブ マイグレーションに有効なテクノロジーです。CSV では、物理サーバ間での仮想マシンの移動がミリ秒単位で実行され、ネットワーク接続が切断されたり、識別できるほどのダウンタイムが発生することはありません。マイグレーション操作は、接続先のユーザからは事実上不可視になります。

Hyper-V を実行する物理サーバのフェールオーバー クラスタを構築したら、いつでも自由に VM のライブ マイグレーションを実行できます。ノードに障害が発生すると、VM は別のクラスタ ノードで再起動されます。

Citrix XenDesktop 5 と Microsoft Hyper-V を使用した Cisco VXI

Citrix XenDesktop 5 と Hyper-V を基盤とする Cisco VXI 導入は、概念上はこの設計ガイドの「デスクトップ仮想化」で説明した Citrix XenDesktop 5 と VMware ESXi 4.1 の導入と同じです。XenDesktop 5 は、System Center Virtual Machine Manager（SCVMM）を介して Microsoft Hyper-V 仮想デスクトップ上で仮想デスクトップ プロビジョニング機能を実行します。この統合機能の詳細については、http://support.citrix.com/article/CTX127578 の Citrix Knowledge Center を参照してください。さらに、Cisco コンポーネントを使用した Hyper-V 環境での XenDesktop 5 の設定については、http://www.cisco.com/en/US/solutions/collateral/ns340/ns517/ns224/ns955/ns1099/cisco_usc_citrix_xd_ms_hyperV_netapp_storage.pdf を参照してください。

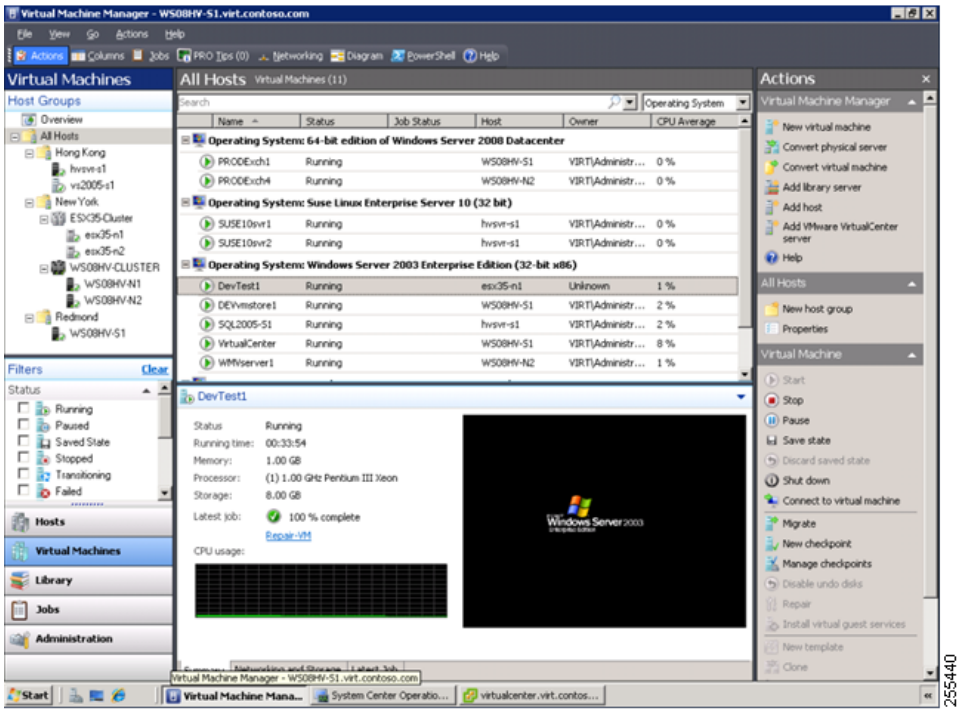
Hyper-V はスタンドアロン モードで導入することも、Microsoft Server 2008 R2 のサーバ ロールとして導入することもできます。Microsoft Server 2008 R2 バージョンを XenDesktop 5 用 Hyper-V ロールとともに使用し、クラスタ共有ボリュームだけでなくライブ マイグレーション向けのサポートを利用することをお勧めします。本稿執筆時点では、Cisco Nexus 1000v、Cisco vWAAS、および Cisco VSG は Microsoft Hyper-V でサポートされていません。したがって、仮想ゾーン ベースのファイアウォールや仮想ポート セキュリティなど、Cisco Nexus 1000v および Cisco VSG で提供される高度なネットワーキング機能は、Hyper-V ベースの導入ではサポートされません。Cisco vWAAS で提供される WAN 最適化は、データセンター エッジに Cisco WAAS WAE アプライアンスを配置することで引き続き利用できます。ネットワークに高い可用性と冗長性が求められる仮想デスクトップには、Hyper-V の NIC チーミング機能を使用することをお勧めします。ただし、Hyper-V で NIC チーミングを使用する場合、TCP Chimney と Virtual Machine Queueing（VMQ）は使用できません。TCP Chimney と VMQ は、Hyper-V ネットワーク パケット処理をハードウェアにオフロードすることで、これらのパフォーマンスを大幅に向上させます。MS Hyper-V を使用した XenDesktop の設計については、http://support.citrix.com/article/CTX124687 を参照してください。この記事では XenDesktop 4 が取り上げられていますが、XenDesktop 5 と XenApp ベースの導入にも同様に適用できます。

管理と運用

Microsoft Hyper-V 管理スイート（SCVMM）

Microsoft System Center Virtual Machine Manager™（SCVMM）には、サーバ、ライブラリ サーバ、データベース、および Administrator Console が含まれています。Administrator Console は、Cisco VXI 導入で Microsoft Hyper-V ハイパーバイザを管理するために使用されます。System Center Virtual Machine Manager 2008 R2 は、仮想化インフラストラクチャを集中管理し、サーバとデスクトップの利用効率を高め、複数の仮想化プラットフォームおよび物理プラットフォーム全体でリソースを動的に最適化します。System Center Virtual Machine Manager 2008 R2 は、Windows Server 2008 および 2008 R2 Hyper–V、Microsoft Hyper-V Server の管理に使用されます。Virtual Machine Manager（VMM）は Virtual Center の統合によって、Hyper-V プラットフォームの管理だけでなく VMware ハイパーバイザにも対応できるようになります。

図 154　SCVMM Administrator Console



SCVMM を使用すると、作業負荷を中断せずに仮想マシンのリソース設定を変更し、仮想マシンを 1 つのホストから別のホストへ移動して、物理リソースを最適化できます。作業負荷が仮想インフラストラクチャに統合されると、管理者は Virtual Machine Manager のレポートと監視データを利用できます。これらの機能は、Operations Manager 2007 との統合によって拡張可能です。SCVMM を使用すると、Microsoft Hyper-V マネージャで提供される限定的な機能を補完することができます。

Virtual Machine Manager Administrator Console は System Center Framework ユーザ インターフェイスに組み込まれており、管理者はこれを使用して仮想マシン管理の技術を急速に向上させることができます。Virtual Machine Manager は、Windows PowerShell、管理者用コマンド シェル、およびスクリプト言語と互換性があり、170 を超える標準コマンドライン ツールと一貫した構文およびユーティリティを備えています。コマンド シェル インターフェイスを使用すると、プロビジョニングのワークフローを自動化できます。

SCVMM の一般的な使用例

- 仮想デスクトップの作成
- 仮想デスクトップのクローニング
- 仮想ネットワークの作成
- Performance and Resource Optimization（PRO）ポリシーの作成

ハイパーバイザおよび仮想デスクトップでのリソース使用状況の監視

Cisco VXI 導入で SCVMM を使用するためのガイドライン

Microsoft System Center Virtual Machine Manager 2008 を XenDesktop とともに使用する場合、Hyper-V を 2 通りの方法で導入できます。すなわち、単一の Hyper-V ホストとして導入するか、複数のクラスタを持つホストとして導入します。既存のカタログを選択する代わりに XenDesktop を使用して VM を作成する場合は、特定の方法で Hyper-V 導入を設定する必要があります。要件、インストール、および設定の手順は導入によってそれぞれ異なります。詳細な手順については、Citrix XenDesktop ドキュメントのページを参照してください。

参考資料

Microsoft SCVMM ページ

http://www.microsoft.com/systemcenter/en/us/virtual-machine-manager.aspx

Microsoft SCVMM ドキュメント

http://technet.microsoft.com/en-us/library/cc917964.aspx

『Understanding Networking with Hyper-V』

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=3fac6d40-d6b5-4658-bc54-62b925ed7eea

『Microsoft Hyper-V Server 2008 Configuration Guide』

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=E1E111C9-FA69-4B4D-8963-1DD87804C04F

『Hyper-V Planning and Deployment Guide』

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=5DA4058E-72CC-4B8D-BBB1-5E16A136EF42

『Windows Server 2008 R2: Hyper-V Component Architecture』

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=5567B22A-8C47-4840-A88D-23146FD93151

『Step-by-Step Guide for Testing Hyper-V and Failover Clustering』

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=CD828712-8D1E-45D1-A290-7EDADF1E4E9C

付録 2：Citrix XenServer 使用時の特別な考慮事項

Cisco VXI システムは、Citrix XenServer ハイパーバイザとともにテスト済みです。Cisco Verified Design の各ドキュメントには、Citrix XenDesktop および Citrix XenServer を基盤とするデスクトップ仮想化システムを導入するための設計ガイダンスが示されており、次の URL で入手できます。
http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/Virtualization/ucs_xd_xenserver_ntap.pdf

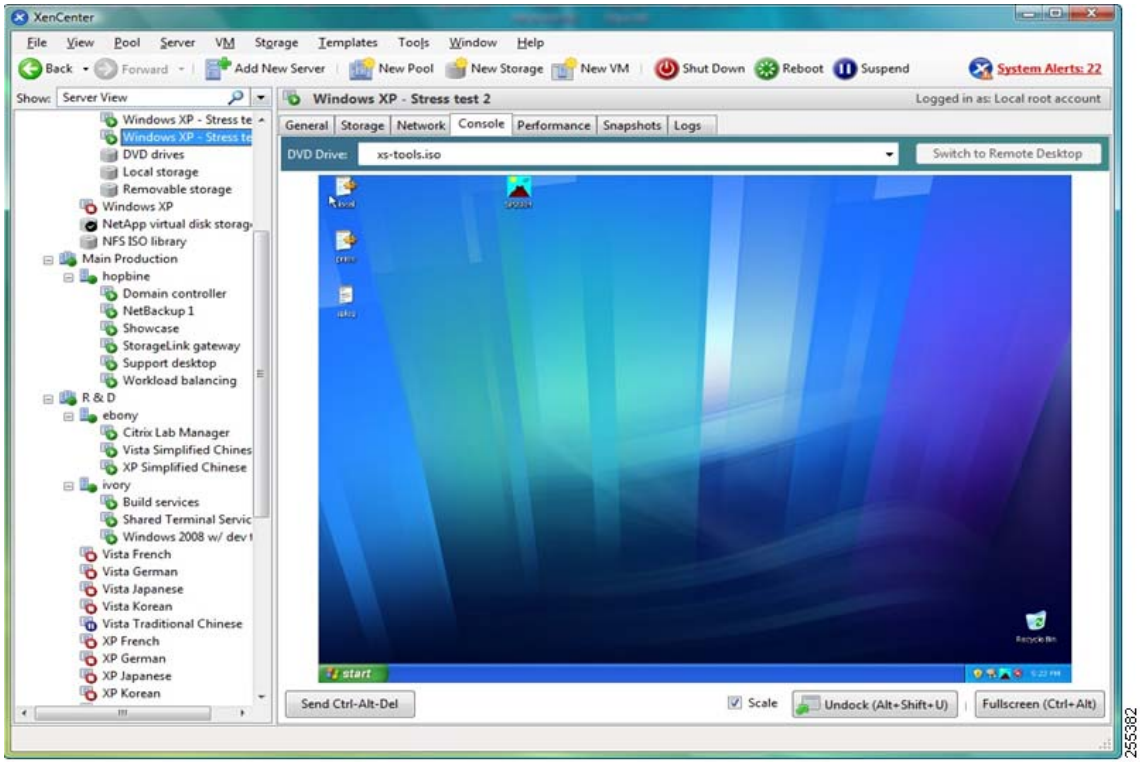
以下の製品と機能は XenServer ベースの Cisco VXI システムと互換性がないことに注意してください。

- Cisco Voice Security Gateway（VSG）
- Cisco virtual Wide Area Application Service（vWAAS）モジュール
- Cisco Nexus 1000 V 仮想スイッチ

- VNLink ベースのスイッチング
- vStorage

Citrix XenCenter 5.6 は、Citrix XenServer 管理用の Windows ベースのグラフィカル ユーザ インターフェイスです。仮想マシンのインストール、設定、およびライフサイクル管理、VM コンソールへのアクセス、NetApp および HBA（ファイバ チャネル、ハードウェア iSCSI）を含むリモート ストレージの設定、ホストのネットワーキング管理、動的メモリ管理、総合的なリソース プール管理、ハイ アベイラビリティ設定、Active Directory の統合と役割ベースのアクセス制御、VM スナップショット管理（メモリのスナップショット、VM ロールバックなど）、作業負荷の分散、作業負荷レポート、VM の自動電源管理、パフォーマンス メトリックの表示、長期のメトリック レポートと分析がサポートされています。XenServer 5.0 から 5.6 FP1 までのすべてのサーバ バージョンを管理できます。

図 155　　Citrix XenCenter Administration Console



XenCenter には、XenCenter コンソールにカスタマイズされたメニュー アイテムとタブを追加できるプラグイン機能が搭載されています。このコンソールを使用して、既存の管理ツールを XenCenter に統合できます。XenCenter には、XenServer 用のオープンソースの Web インターフェイスである xvp などのツールを使用してリモート アクセスできます。

ホワイト ペーパー『CTX122191: XenServer - Virtual Machine Backup』を参照してください。ここでは、XenServer のスナップショット機能を既存のバックアップ ソリューションと組み合わせて使用する方法など、さまざまな VM バックアップの手法について説明されています。

（注） XenDesktop 5 Machine Creation Services を Citrix XenServer とともに使用する場合は、http://support.citrix.com/proddocs/topic/xendesktop-rho/cds-sys-reqs-host-rho.html でホストとストレージの詳細な要件を確認してください。

Citrix XenServer の各リリースでの使用が認定およびサポートされているハードウェアおよびソフトウェア コンポーネントの一覧については、http://hcl.vmd.citrix.com/ を参照してください。

Cisco Validated Design

Cisco Validated Design（CVD）プログラムについて

CVD プログラムは、お客様による信頼性の高い、確実かつ予測可能な展開を容易にするために、設計、テスト、および文書化されたシステムおよびソリューションで構成されています。詳細については、www.cisco.com/go/designzone/ を参照してください。

このマニュアルに記載されているデザイン、仕様、表現、情報、および推奨事項（総称して「デザイン」）は、障害も含めて本マニュアル作成時点のものです。シスコシステムズおよびそのサプライヤは、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、一切の保証の責任を負わないものとします。いかなる場合においても、シスコシステムズおよびそのサプライヤは、このデザインの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコシステムズまたはそのサプライヤに知らされていても、それらに対する責任を一切負わないものとします。

デザインは予告なしに変更されることがあります。このマニュアルに記載されているデザインの使用は、すべてユーザ側の責任になります。これらのデザインは、シスコシステムズ、そのサプライヤ、パートナーの技術的な助言や他の専門的な助言に相当するものではありません。ユーザは、デザインを実装する前に技術アドバイザーに相談してください。シスコによるテストの対象外となった要因によって、結果が異なることがあります。

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(0809R)

© 2011 Cisco Systems, Inc. All rights reserved.