

Horizon 7 アーキテクチャの 計画

2020 年 3 月

VMware Horizon 7 7.12



vmware®

最新の技術ドキュメントは、VMware の Web サイト (<https://docs.vmware.com/jp/>) でご確認いただけます。このドキュメントに関するご意見およびご感想は、docfeedback@vmware.com までお送りください。

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴィエムウェア株式会社
105-0013 東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

Copyright © 2009-2020 VMware, Inc. All rights reserved. [著作権および商標情報](#)。

目次

Horizon 7 アーキテクチャの計画 6

1 Horizon 7 について 7

- Horizon 7 を使用する利点 7
- Horizon 7 機能 10
- コンポーネントをひとまとめにする方法 12
 - クライアント デバイス 13
 - Horizon 接続サーバ 13
 - Horizon Client 14
 - VMware Horizon ユーザー Web ポータル 15
 - Horizon Agent 15
 - Horizon Administrator 16
 - View Composer 16
 - vCenter Server 16
- Horizon 7 の統合とカスタマイズ 17

2 豊かなユーザー体験の計画 23

- Horizon Agent 機能サポーター一覧 23
- 表示プロトコルの選択 24
 - VMware Blast Extreme 24
 - PCoIP 28
 - Microsoft RDP 30
- 公開アプリケーションの使用 31
- Horizon Persona Management を使用したユーザーのデータと設定の保持 32
- リモート デスクトップおよびアプリケーションでの USB デバイスの使用 33
- Web カメラとマイクでリアルタイム オーディオ ビデオ機能を使用 34
- 3D グラフィックス アプリケーションの使用 34
- リモート デスクトップへのマルチメディアのストリーミング 35
- リモート デスクトップからの印刷 35
- シングル サインオンによるログイン 36
- モニターおよび画面解像度 37

3 中央からのデスクトップ プールとアプリケーション プールの管理 39

- デスクトップ プールの利点 39
- アプリケーション プールの利点 40
- ストレージ要件の軽減と管理 41
 - vSphere によるストレージの管理 42
 - 高パフォーマンス ストレージとポリシーベース管理での VMware vSAN の使用 43

仮想マシン中心ストレージとポリシー ベース管理のための仮想ボリュームの使用	45
Composer によるストレージ要件の低減	46
インスタント クローンによる必要ストレージの軽減	48
アプリケーション プロビジョニング	50
RDS ホストによる個々のアプリケーションの展開	51
View Composer によるアプリケーション アップデートおよびシステム アップデートのデプロイ	51
インスタント クローンでのアプリケーションおよびシステムのアップデートの展開	52
Horizon Administrator での VMware ThinApp アプリケーションの管理	52
App Volumes を使用するアプリケーションの展開と管理	53
アプリケーション プロビジョニングでの、既存のプロセスまたは VMware Mirage の使用	53
Active Directory GPO によるユーザーおよびデスクトップの管理	54
4 リモート デスクトップ展開のためのアーキテクチャ設計の要素と計画のガイドライン	56
リモート デスクトップの仮想マシン要件	57
就業者のタイプに基づく計画	57
仮想マシン デスクトップのメモリ要件の見積もり	58
仮想マシン デスクトップの CPU 要件の見積もり	60
適切なシステム ディスク サイズの選択	61
Horizon 7 ESXi ノード	62
特定のタイプのワーカーのデスクトップ プール	63
タスク ワーカー用プール	64
ナレッジ ワーカーとパワー ユーザー用プール	65
キオスク ユーザー用プール	66
デスクトップ仮想マシンの構成	68
RDS ホスト仮想マシンの構成	68
vCenter Server および View Composer 仮想マシンの構成	69
Horizon Connection Server の最大接続数と仮想マシン構成	70
vSphere クラスター	74
ストレージと帯域幅の要件	76
共有ストレージの例	76
ストレージバンド幅に関する考慮事項	79
ネットワーク バンド幅に関する考慮事項	79
View Composer パフォーマンス テストの結果	82
WAN のサポート	83
Horizon 7 ビルディング ブロック	85
Horizon 7 ポッド	86
クラウド ポッド アーキテクチャ の概要	88
ポッドで複数の vCenter Server を使用する利点	89
5 セキュリティ機能の計画	92
クライアント接続について	92

PCoIP および Blast Secure Gateway を使用するクライアント接続	93
Microsoft RDP を使用するトンネル クライアント接続	94
直接クライアント接続	95
ユーザー 認証方法の選択	95
Active Directory 認証	96
2 要素認証の使用	96
スマート カード認証	97
Windows ベースの Horizon Client で使用できる現在のユーザーとしてログイン機能を使用	97
リモート デスクトップ アクセスの制限	98
グループ ポリシー設定を使用したリモート デスクトップおよびアプリケーションのセキュリティ保護	100
スマート ポリシー の使用	100
クライアント システムのセキュリティを保護するためのベスト プラクティスの実装	101
管理者ロールの割り当て	101
セキュリティ サーバを使用するための準備	101
セキュリティ サーバ展開のベスト プラクティス	102
セキュリティ サーバのトポロジ	102
DMZ ベースのセキュリティ サーバのファイアウォール	104
通信プロトコルの概要	108
View Secure Gateway Server	110
Blast Secure Gateway	111
PCoIP Secure Gateway	111
View LDAP	112
Horizon Messaging	112
Horizon 接続サーバのファイアウォール ルール	113
View Agent または Horizon Agent のファイアウォール ルール	113
Active Directory のファイアウォール ルール	115

6 Horizon 7 環境のセットアップ手順の概要 116

Horizon 7 アーキテクチャの計画

本マニュアル『Horizon 7 アーキテクチャの計画』では、VMware Horizon™ 7 の概要について説明します。これには、主な機能および展開オプションの説明と、本番環境で一般的なコンポーネントのセットアップ方法の概要が含まれます。

このガイドは次の疑問に答えます。

- この製品は解決の必要な問題を解決してくれるのか。
- 会社はこのソリューションを実装することは可能なのか。また、コスト効率は良いのか。

エディションによっては、VMware Horizon 7 の一部の機能を使用できません。各エディションの機能セットの比較については、<http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf> を参照してください。

また、インストールの保護を支援するために、セキュリティ機能についても説明します。

対象読者

本マニュアルの情報は、IT の意思決定者、アーキテクト、管理者、およびこの製品のコンポーネントおよび機能に精通する必要があるその他の読者を対象としています。アーキテクトやプランナーはこの情報により、Windows デスクトップおよびアプリケーションを効率的かつ安全にエンド ユーザーに提供するという企業のニーズを Horizon 7 が満たすかどうかを判別できます。アーキテクチャの例が示されているため、プランナーは大規模展開のためのハードウェア要件と必要なセットアップ作業を理解できます。

Horizon 7 について

1

Horizon 7 を使用すると、IT 部門はデータセンター内でリモート デスクトップおよびアプリケーションを実行し、これらのデスクトップやアプリケーションを管理対象サービスとして従業員に提供することができます。エンド ユーザーは、社内のあらゆる場所にある任意の数のデバイスから、または自宅からアクセスできる、パーソナライズされたなじみのある環境を手にすることができます。管理者は、デスクトップ データをデータセンター内に保持できるため、制御の集中化、効率性、およびセキュリティを確保できます。

この章には、次のトピックが含まれています。

- [Horizon 7 を使用する利点](#)
- [Horizon 7 機能](#)
- [コンポーネントをひとまとめにする方法](#)
- [Horizon 7 の統合とカスタマイズ](#)

Horizon 7 を使用する利点

Horizon 7 を使用してエンタープライズ デスクトップを管理することの利点には、信頼性、セキュリティ、ハードウェアからの独立性、および利便性の向上などがあります。

信頼性とセキュリティ

デスクトップおよびアプリケーションは、VMware vSphere[®] と統合し、サーバ、ストレージ、およびネットワーク リソースを仮想化することによって、一元管理できます。デスクトップのオペレーティング システムおよびアプリケーションをデータセンター内のサーバに配置することには、次の利点があります。

- データへのアクセスを容易に制限できます。機密データがリモートの従業員の自宅コンピュータにコピーされることを防止できます。
- RADIUS がサポートされているため、2 要素認証ベンダーを柔軟に選択できます。サポート対象のベンダー製品には、特に RSA SecureID、VASCO DIGIPASS、SMS Passcode、および SafeNet があります。
- VMware Identity Manager との統合は、エンド ユーザーが SaaS、Web、および Windows アプリケーションにアクセスするために使用するのと同じ Web ベースのアプリケーション カタログを介してリモート デスクトップにオンデマンドでアクセスするという意味です。リモート デスクトップ内で、ユーザーはこのカスタム アプリケーション ストアを使用してアプリケーションにアクセスすることもできます。

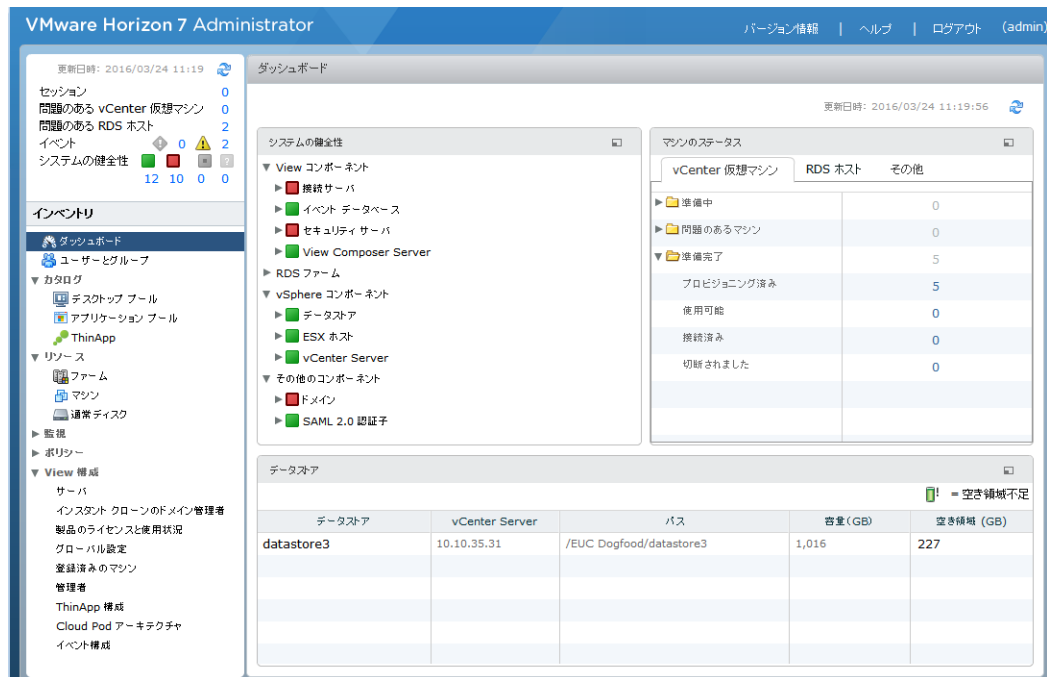
- 事前作成済みの Active Directory アカウントでリモート デスクトップをプロビジョニングする機能によって、読み取り専用のアクセス ポリシーがあるロックダウンされた Active Directory 環境の要件が解決されます。
- エンド ユーザーのシステムがいつオフになるかを気にせずに、データのバックアップをスケジュールできます。
- データセンター内でホストされるリモート デスクトップおよびアプリケーションは、ダウンタイムがほとんどないか、まったくありません。仮想マシンは VMware サーバの高可用性クラスタ上に配置できます。

仮想デスクトップをバック エンドの物理システムおよび Microsoft リモート デスクトップ サービス (RDS) ホストに接続することもできます。

利便性

最大規模で展開された Horizon 7 でも単一の管理インターフェイスで効率的に管理できるように、スケーラビリティを考慮して統合管理コンソールが組み込まれています。ウィザードとダッシュボードによってワークフローが強化され、詳細の表示や設定の変更にドリルダウン機能を活用できます。図 1-1. [ダッシュボード表示を示す管理コンソール](#) は Horizon Administrator のブラウザ ベースのユーザー インターフェイスの例です。

図 1-1. ダッシュボード表示を示す管理コンソール



他にも、VMware リモート表示プロトコル、PCoIP (PC over IP)、および Blast Extreme によって利便性が向上します。これらの表示プロトコルは、物理 PC を使用した場合の現在のエクスペリエンスに匹敵するエンドユーザーエクスペリエンスを提供します。

- LAN 上では、従来のリモート表示よりも高速かつ滑らかに表示できます。
- WAN 上では、表示プロトコルは遅延の増加またはバンド幅の減少を補って、ネットワークの状態に関わらずエンド ユーザーの生産性を維持できるようにします。

管理性

エンド ユーザー用のデスクトップおよびアプリケーションのプロビジョニングは、短時間で終わるプロセスです。各エンド ユーザーの物理 PC に 1 台ずつアプリケーションをインストールするのではなく、アプリケーションを完備した公開アプリケーションまたはリモート デスクトップにエンド ユーザーが接続します。エンド ユーザーは、さまざまな場所でさまざまなデバイスから同じリモート デスクトップまたはアプリケーションにアクセスできます。

VMware vSphere を使用して仮想デスクトップや RDS ホスト サーバをホストすることの利点には、次のようなものがあります。

- 管理の作業が削減されます。管理者はユーザーの物理 PC に手を触れることなく、アプリケーションとオペレーティング システムのパッチ適用およびアップグレードを実行できます。
- VMware Identity Manager との 統合は、IT マネージャーが Web ベースの VMware Identity Manager 管理インターフェイスを使用して、リモート デスクトップに対するユーザーおよびグループの資格を監視できることを意味します。
- リアルタイムのアプリケーション提供システムである VMware App Volumes との統合によって、企業はアプリケーションを大規模に提供して管理できます。App Volumes を使用することで、ユーザーがデスクトップにログインしているときでも、ユーザー、グループ、またはターゲット コンピュータにアプリケーションを接続できます。リアルタイムでのアプリケーションのプロビジョニング、提供、更新、および破棄も可能です。
- Horizon Persona Management によって、物理および仮想デスクトップで、ユーザー プロファイル、アプリケーション権限、ポリシー、パフォーマンス、およびその他の設定などを統合管理できます。仮想デスクトップに変換する前に、個人設定管理を物理デスクトップ ユーザーに展開します。
- エンド ユーザーは VMware User Environment Manager を使用して、自分の状況に合わせて Windows デスクトップをパーソナライズできるので、ロール、デバイス、場所などの側面に基づいて必要とされる IT リソースにアクセスできます。
- ストレージの管理が簡素化されます。VMware vSphere を使用すると、ボリュームおよびファイル システムを仮想化できるため、個別のストレージ デバイスを管理する必要がなくなります。
- vSphere 6.0 以降のリリースでは Virtual Volumes (VVols) を使用できます。この機能は、仮想ディスクとそれらの派生物、クローン、スナップショット、およびレプリカを、ストレージ システム上の仮想ボリュームと呼ばれるオブジェクトに直接マッピングします。このマッピングにより、vSphere はスナップショットの取得、クローンの作成、およびレプリケーションなど、集約的なストレージ処理をストレージ システムにオフロードできます。たとえば、以前は 1 時間かかっていたクローン作成処理も、Virtual Volumes を使用してわずか数分間で完了できるようになりました。
- vSphere 5.5 Update 1 以降のリリースでは、vSAN を使用できます。これは、ESXi™ ホストで使用可能なローカルの物理的な半導体ディスク ドライブとハード ディスク ドライブをクラスタ内のすべてのホストで共有される単一データストアに仮想化します。デスクトップ プールを作成するときは、1 つのデータストアのみを指定します。仮想マシン ファイル、レプリカ、ユーザー データ、オペレーティング システム ファイルといった各種コンポーネントは、SSD ディスクかハード ドライブ ディスクに適宜配置されます。

容量、パフォーマンス、可用性などの仮想マシン ストレージ要件は、デフォルトのストレージ ポリシー プロファイルの形式で管理します。デフォルトのストレージ ポリシー プロファイルは、デスクトップ プールを作成するときに自動的に作成されます。

- Horizon 7 Storage Accelerator を使用すると、特別なストレージ アレイ テクノロジーがなくてもより大規模なエンド ユーザー ログイン数をサポートでき、ストレージの負荷である IOPS が大幅に軽減されます。
- リモート デスクトップが vSphere 5.1 以降のバージョンで利用できる領域効率的なディスク形式を使用する場合、ゲスト OS 内の無効または削除されたデータは、自動的にワイプおよび縮小プロセスで再利用されます。

ハードウェアからの独立性

リモート デスクトップおよび公開アプリケーションは、ハードウェアに依存しません。たとえば、リモート デスクトップはデータセンター内のサーバ上で実行され、クライアント デバイスからのみアクセスされるため、クライアント デバイスのハードウェアと互換性がない可能性のあるオペレーティング システムでもリモート デスクトップで使用できます。

リモート デスクトップは、PC、Mac、シン クライアント、およびシン クライアント、タブレット、および電話として機能する PC 上で実行されます。公開アプリケーションは、これらのデバイスのサブセット上で実行されます。新しいデバイスのサポートは、四半期ごとに追加されます。

HTML Access 機能を使用すると、エンド ユーザーは、クライアント システムやデバイスにクライアント アプリケーションをインストールせずに、ブラウザ内でリモート デスクトップまたはアプリケーションを開くことができます。

Horizon 7 機能

Horizon 7 に備わる機能は、操作性、セキュリティ、集中制御、およびスケーラビリティをサポートします。

次の機能は、エンド ユーザーになじみのある体験を提供します。

- 特定のクライアント デバイス上では、仮想デスクトップからクライアント デバイスで定義されているローカルまたはネットワーク上の任意のプリンタに印刷できます。この仮想プリンタ機能を使用すると、互換性の問題が解決され、仮想マシンに追加のプリンタ ドライバをインストールする必要がなくなります。
- ほとんどのクライアント デバイス上で、ロケーションベースの印刷機能を使用して物理的にクライアント システムの近くにあるプリンタにマッピングできます。ロケーションベースの印刷では、仮想マシン上にプリンタ ドライバをインストールする必要があります。
- ローカル プリンタのリダイレクトは、次のようなユースケースで使用されます。
 - USB またはクライアントのシリアル ポートに直接接続するプリンタ。
 - クライアントに接続し、バーコード印刷やラベル印刷などを行う特別なプリンタ。
 - 仮想セッションから接続できないリモート ネットワーク上のネットワーク プリンタ。
- 複数のモニターを使用します。PCoIP および Blast Extreme 表示プロトコルを使用して複数モニターをサポートすることにより、表示解像度と回転をモニター別に調整できます。
- 仮想デスクトップを表示するローカル デバイスに接続されている USB デバイスやその他の周辺機器にアクセスします。

エンド ユーザーに接続を許可する USB デバイスのタイプを指定できます。ビデオ入力デバイスとストレージ デバイスなど複数タイプのデバイスが含まれる複合デバイスについては、デバイスを分離し、あるデバイス（たとえば、ビデオ入力デバイス）は許可し、その他のデバイス（たとえば、ストレージ デバイス）は許可しないようにできます。

- Horizon Persona Management を使用して、デスクトップが更新または再構成された後でもセッション間でユーザー設定およびデータを保持できます。Horizon Persona Management には、設定可能な間隔でユーザー プロファイルのリモート プロファイル ストア（CIFS 共有）に複製する機能があります。

Horizon 7 が管理しない物理コンピュータおよび仮想マシンでは、スタンドアロン バージョンの個人設定管理も使用できます。

Horizon 7 は、次のようなセキュリティ機能を備えています。

- RSA SecurID や RADIUS (Remote Authentication Dial-In User Service) などの 2 要素認証またはスマート カードを使用してログインします。
- Active Directory に対して読み取り専用のアクセス ポリシーを持つ環境でリモート デスクトップとアプリケーションをプロビジョニングするときに、事前作成済みの Active Directory アカウントを使用します。
- SSL/TLS トンネリングを使用して、すべての接続が完全に暗号化されるようにします。
- VMware High Availability を使用して、自動フェイルオーバーを実現します。

スケーラビリティの機能は、デスクトップとサーバの両方を管理する VMware 仮想化プラットフォームに依存します。

- VMware vSphere との統合により、コスト効率の良い密度、高水準の可用性、およびリモート デスクトップとアプリケーションのリソース割り当ての高度な制御を実現します。
- Horizon 7View Storage Accelerator 機能を使用して、同じストレージ リソースでより大規模なエンド ユーザー ログイン数をサポートします。この Storage Accelerator は、vSphere5 プラットフォームの機能を使用して共通のブロック読み取りのホスト メモリ キャッシュを作成します。
- エンド ユーザーと、それらのユーザーにアクセスが許可されているリモート デスクトップとアプリケーションとの接続を仲介するように Horizon Connection Server を構成します。
- View Composer を使用して、仮想ディスクをマスター イメージと共有するデスクトップ イメージをすばやく作成します。リンク クローンをこの方法で使用する、ディスク領域を節約でき、オペレーティング システムのパッチおよびアップデートの管理が簡素化されます。
- Horizon 7 で導入されたインスタント クローン機能を使用すると、仮想ディスクとメモリを親イメージと共有するデスクトップ イメージを迅速に作成できます。インスタント クローンは View Composer のリンク クローンの領域効率性を実現するだけでなく、オペレーティング システムの更新、再構成、再分散の必要性を排除することで、パッチとアップデートの管理をさらに簡素化します。インスタント クローンによって、デスクトップ メンテナンスの期間が完全に排除されます。

次の機能は、管理の集中化を実現します。

- Microsoft Active Directory を使用して、リモート デスクトップとアプリケーションへのアクセスを管理し、ポリシーを管理します。
- 個人設定管理を使用して、物理から仮想デスクトップへの移行を容易にし合理化します。

- Web ベースの管理コンソールを使用して、任意の場所からリモート デスクトップとアプリケーションを管理します。
- Horizon Administrator を使用して、VMware ThinApp™ でパッケージ化されたアプリケーションを配布および管理します。
- テンプレート（マスター イメージ）を使用して、デスクトップのプールをすばやく作成し、プロビジョニングします。
- ユーザーの設定、データ、または環境設定に影響を及ぼすことなく、アップデートおよびパッチを仮想マシンに送信します。
- VMware Identity Manager と統合して、エンド ユーザーが Web 上のユーザー ポータルからリモート デスクトップにアクセスし、リモート デスクトップ内のブラウザから VMware Identity Manager を使用できるようにします。
- Mirage™ と Horizon FLEX™ を統合して、ローカルにインストールされた仮想マシン デスクトップを管理し、ユーザーがインストールしたアプリケーションを上書きすることなく、専用の完全クローン リモート デスクトップのアプリケーションを展開して更新します。

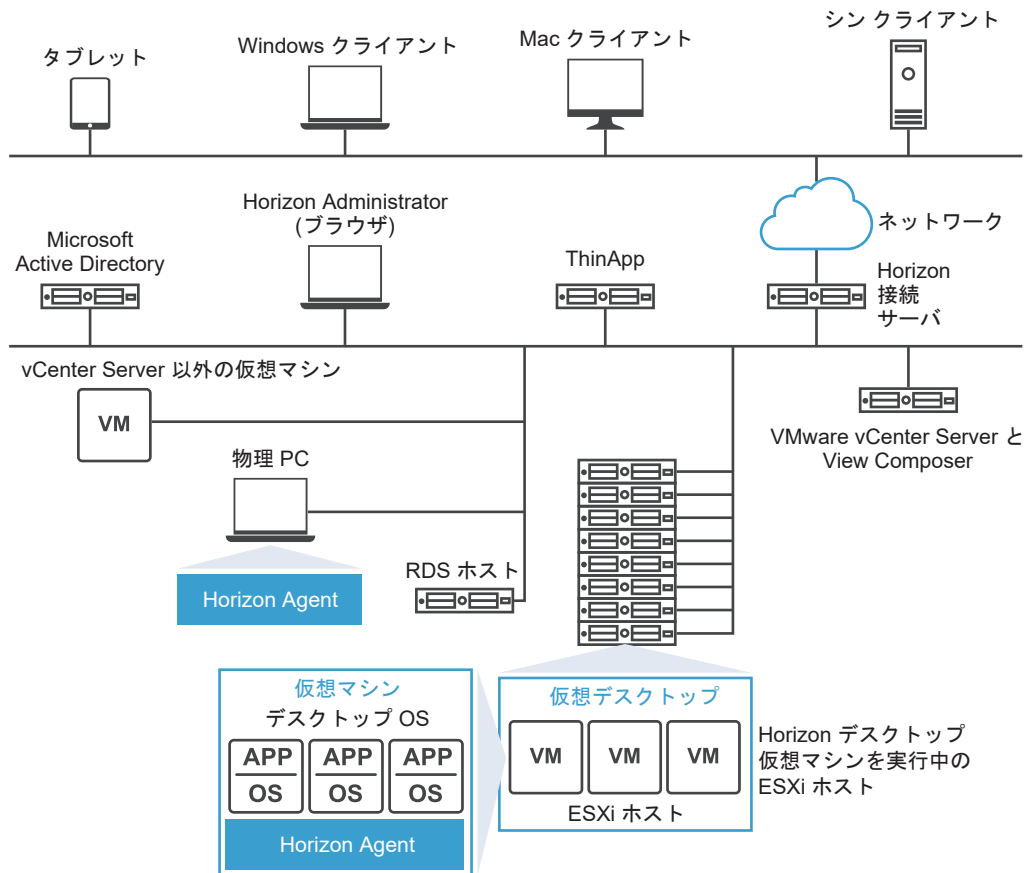
コンポーネントをひとまとめにする方法

エンド ユーザーは、Horizon Client を起動して Horizon 接続サーバにログインします。このサーバは、Windows Active Directory と統合され、VMware vSphere サーバ、物理 PC または Microsoft RDS ホストにホストされているリモート デスクトップへのアクセスを提供します。Horizon Client は、Microsoft RDS ホストの公開アプリケーションへのアクセスも提供します。

注： Horizon 7 は、Active Directory Domain Services (AD DS) ドメイン機能レベルをサポートします。サポート対象の AD DS ドメインの機能レベルについては、VMware のナレッジベース (KB) の記事、<http://kb.vmware.com/kb/2150351> を参照してください。

図 1-2. Horizon 7 環境の高水準での例 は、Horizon 7 の展開を構成する主要コンポーネントの関係を示しています。

図 1-2. Horizon 7 環境の高水準での例



クライアント デバイス

Horizon 7 を使用する主な利点は、デバイスや場所にかかわらず、リモート デスクトップおよびアプリケーションがエンド ユーザーについて回ることです。ユーザーは、会社のラップトップ、自宅の PC、シン クライアント デバイス、Mac、またはタブレットや電話機から、各自専用の仮想デスクトップまたはリモート アプリケーションにアクセスできます。

エンド ユーザーは、Horizon Client を開いて、リモート デスクトップおよびアプリケーションを表示します。クライアント デバイスは、Horizon 7 シン クライアント ソフトウェアを使用するため、ユーザーがそのデバイス上で直接起動できる唯一のアプリケーションが Horizon 7 Thin Client になるように構成できます。レガシー PC の用途を変更してシン クライアント デスクトップにすると、ハードウェアの寿命を 3 ～ 5 年延長できます。たとえば、シン デスクトップ上で Horizon 7 を使用すると、古いデスクトップ ハードウェア上で Windows 8.x などの新しいオペレーティング システムを使用できます。

HTML Access 機能を使用すると、エンド ユーザーは、クライアント システムやデバイスにクライアント アプリケーションをインストールせずに、ブラウザ内でリモート デスクトップを開くことができます。

Horizon 接続サーバ

このソフトウェア サービスは、クライアント接続のブローカーとして機能します。Horizon 接続サーバは、Windows Active Directory を介してユーザーを認証し、適切な仮想マシン、物理 PC、または Microsoft RDS ホストに要求を送ります。

接続サーバは、次の管理機能を備えています。

- ユーザーの認証
- ユーザーへの、特定のデスクトップおよびプールに対する資格の付与
- VMware ThinApp でパッケージ化されたアプリケーションの特定のデスクトップおよびプールへの割り当て
- リモート デスクトップおよびアプリケーション セッションの管理
- ユーザーとリモート デスクトップおよびアプリケーションの安全な接続の確立
- シングル サインオンの有効化
- ポリシーの設定および適用

企業ファイアウォールの内側に、2 つ以上の接続サーバ インスタンスのグループをインストールして構成します。その構成データは組み込み LDAP ディレクトリに格納され、グループのメンバー間で複製されます。

企業ファイアウォールの外部の DMZ 内で、セキュリティ サーバとして接続サーバをインストールして構成できます。また、Unified Access Gateway アプライアンスをインストールできます。DMZ 内のセキュリティ サーバおよび Unified Access Gateway アプライアンスは、企業ファイアウォールの内側の接続サーバと通信します。セキュリティ サーバおよび Unified Access Gateway アプライアンスにより、企業のデータセンターにアクセスすることができるリモート デスクトップおよびアプリケーションのトラフィックは、強力な認証を経たユーザーのトラフィックのみにすることができます。ユーザーはアクセスが許可されているリソースにのみアクセスできます。

セキュリティ サーバは View 接続サーバの機能のサブセットを提供するため、Active Directory ドメイン内に配置する必要はありません。接続サーバは、（できれば VMware 仮想マシン上の）Windows Server 2008 R2 または Windows Server 2012 R2 サーバにインストールします。Unified Access Gateway アプライアンスの詳細については、『Unified Access Gateway の導入および設定』を参照してください。

重要： 接続サーバを使用しない Horizon 7 設定を作成することは可能です。Horizon 7 Agent Direct Connect プラグインをリモート仮想マシン デスクトップにインストールすると、クライアントは仮想マシンに直接接続できます。PCoIP、HTML Access、RDP、USB リダイレクト、セッション管理などのリモート デスクトップ機能はすべて、ユーザーが接続サーバを介して接続した場合と同じように動作します。詳細については、『Horizon 7 Agent Direct-Connection プラグイン管理』を参照してください。

Horizon Client

リモート デスクトップとリモート アプリケーションにアクセスするためのクライアント ソフトウェアは、タブレット、電話、Windows、Linux、または Mac の PC またはラップトップ、シン クライアントなどで実行できます。

ユーザーはログインした後、使用を許可されているリモート デスクトップとリモート アプリケーションのリストから選択します。認証には、Active Directory の認証情報、UPN、スマート カードの PIN、または RSA SecurID またはその他の 2 要素認証トークンの使用を義務付けることができます。

管理者は、エンド ユーザーが表示プロトコルを選択できるように Horizon Client を構成できます。リモート デスクトップ用のプロトコルには、PCoIP、Blast Extreme、および Microsoft RDP が含まれます。PCoIP と Blast Extreme の速度と表示品質は物理 PC に匹敵します。

機能は、使用する Horizon Client によって異なります。このガイドは、Horizon Client for Windows について説明しています。次のタイプのクライアントについては、このガイドでは詳しく説明しません。

- タブレット、Linux クライアント、および Mac クライアント用の Horizon Client についての詳細。<https://docs.vmware.com/jp/VMware-Horizon-Client/index.html> にある Horizon Client のドキュメントを参照してください。
- ブラウザ内でリモート デスクトップを開くことを許可する HTML Access Web client についての詳細。Horizon Client アプリケーションは、クライアント システムとクライアント デバイスにインストールされません。<https://docs.vmware.com/jp/VMware-Horizon-Client/index.html> にある Horizon Client のドキュメントを参照してください。
- 様々なサードパーティ シン クライアントおよびゼロ クライアント（認定されたパートナーからの購入に限定）。
- View Open Client (VMware のパートナー認定プログラムをサポート)。View Open Client は正式なクライアント アプリケーションではないため、サポートされていません。

VMware Horizon ユーザー Web ポータル

エンド ユーザーは、クライアント デバイス上の Web ブラウザからリモート デスクトップとリモート アプリケーションに接続できます。続いて、Horizon Client がインストールされている場合はこのツールを自動的に起動でき、インストールされていない場合は Horizon Client インストーラをダウンロードできます。

ブラウザを開いて Horizon Connection Server インスタンスの URL を入力すると、Horizon Client をダウンロードするための [VMware ダウンロード サイト](#)へのリンクを含む Web ページが表示されます。ただし、Web ページ上のリンクは構成できます。たとえば、内部の Web サーバを指定するようにリンクを構成したり、独自の接続サーバで利用可能なクライアントのバージョンを制限したりできます。

HTML Access 機能を使用すると、サポートされるブラウザ内のリモート デスクトップおよびアプリケーションにアクセスするためのリンクも Web ページに表示されます。この機能を使用した場合、クライアント システムまたはデバイスに Horizon Client アプリケーションがインストールされることはありません。詳細については、<https://docs.vmware.com/jp/VMware-Horizon-Client/index.html> にある Horizon Client のマニュアルを参照してください。

Horizon Agent

Horizon Agent サービスを、リモート デスクトップとアプリケーションのソースとして使用するすべての仮想マシン、物理システム、および Microsoft RDS ホストにインストールします。仮想マシン上で、このエージェントは Horizon Client と通信して、接続の監視、仮想印刷、Horizon Persona Management、ローカルに接続された USB デバイスへのアクセスなどの機能を提供します。

デスクトップ ソースが仮想マシンの場合は、最初に Horizon Agent サービスをその仮想マシンにインストールした後、その仮想マシンをリンク クローンまたはインスタント クローンのテンプレートまたは親として使用します。この仮想マシンからプールを作成すると、エージェントがすべてのリモート デスクトップに自動的にインストールされます。

このエージェントは、シングル サインオンのオプションを有効にしてインストールできます。シングル サインオンを有効にすると、ユーザーは Horizon 接続サーバに接続したときだけログインを要求され、リモート デスクトップまたはリモート アプリケーションに接続したときには 2 回目のログインを要求されません。

Horizon Administrator

この Web ベースのアプリケーションでは、Horizon 接続サーバの構成、リモート デスクトップとアプリケーションの展開と管理、ユーザー認証の制御、およびエンド ユーザーの問題のトラブルシューティングを管理者が実行できます。

接続サーバ インスタンスをインストールすると、Horizon Administrator アプリケーションもインストールされます。このアプリケーションを使用すると、管理者は自分のローカル コンピュータにアプリケーションをインストールすることなく、任意の場所から接続サーバ インスタンスを管理できます。

View Composer

このソフトウェア サービスは、仮想マシンを管理する vCenter Server インスタンスまたは別のサーバにインストールできます。View Composer はその後、指定された親仮想マシンからリンク クローンのプールを作成できます。この戦略を採用すると、ストレージ コストが最大 90% 削減されます。

各リンク クローンは一意のホスト名および IP アドレスを持ち、独立したデスクトップのように動作しますが、リンク クローンは基本イメージを親と共有するため、ストレージの必要量ははるかに少なくなります。リンク クローン デスクトップ プールは基本イメージを共有しているため、親仮想マシンを更新するだけで、アップデートおよびパッチをすばやく展開できます。エンド ユーザーの設定、データ、およびアプリケーションは影響を受けません。

また、View Composer を使用して、エンド ユーザーに公開アプリケーションを提供するリンククローン Microsoft RDS ホストの自動ファームを作成できます。

View Composer は自身のサーバ ホストにインストールできますが、View Composer サービスは 1 つの vCenter Server インスタンスでのみ動作できます。同様に、vCenter Server インスタンスは、1 つの View Composer サービスにのみ関連付けることができます。

重要： View Composer はオプションのコンポーネントです。インスタント クローンのプロビジョニングを予定している場合は、View Composer をインストールする必要はありません。

vCenter Server

このサービスは、ネットワークに接続されている VMware ESXi サーバの集中管理者として機能します。vCenter Server によって、データセンターにおける仮想マシンの構成、プロビジョニング、および管理を一元的に行うための場が用意されます。

それらの仮想マシンを仮想マシン デスクトップ プールのソースとして使用するだけでなく、仮想マシンを使用して、Horizon Connection Server インスタンス、Active Directory サーバ、Microsoft RDS ホスト、vCenter Server、インスタンスなどの Horizon 7 のサーバ コンポーネントをホストすることもできます。

View Composer は、vCenter Server と同じサーバにも、別のサーバにもインストールできます。そして、物理サーバおよびストレージへの仮想マシンの割り当てと、仮想マシンへの CPU およびメモリ リソースの割り当てが vCenter Server によって管理されます。

vCenter Server は、VMware 仮想アプライアンスとしてインストールすることも、(できれば VMware 仮想マシン上の) Windows Server 2008 R2 サーバまたは Windows Server 2012 R2 サーバに vCenter Server をインストールすることもできます。

Horizon 7 の統合とカスタマイズ

組織内での Horizon 7 の効率を高めるために、さまざまなインターフェイスを使用して、Horizon 7 を外部アプリケーションと統合したり、コマンド ラインやバッチ モードで実行できる管理スクリプトを作成したりできます。

その他のコンポーネントとの統合

Horizon 7 は、次の VMware 製品と統合されます。

VMware Cloud on AWS

VMware Cloud on AWS を使用すると、Amazon Web Services で vSphere データセンターを作成できます。vSphere データセンターは、データセンターを管理する vCenter Server、ストレージ (vSAN)、ネットワーク (VMware NSX) から構成されます。オンプレミスのデータセンターをクラウド上の SDDC に接続し、1 つの vSphere Client インターフェイスからの両方のデータセンターを管理できます。接続された AWS アカウントを使用して、SDDC の仮想マシンから EC2 や S3 などの AWS サービスにアクセスできます。詳細については、<https://docs.vmware.com/jp/VMware-Cloud-on-AWS/index.html> にある VMware Cloud on AWS のマニュアルを参照してください。

Horizon 7 バージョン 7.5 以降では、VMware Cloud on AWS に Horizon 7 の完全クローンをデプロイできます。たとえば、オンプレミスのデータセンターと VMware Cloud on AWS のインスタンスに、クラウド ポッド アーキテクチャを使用する Horizon 7 環境を展開できます。これにより、Horizon 7 を ハイブリッドクラウド環境で簡単に実行し、SDDC インフラストラクチャの管理を VMware に任せることができます。

VMware Identity Manager

VMware Identity Manager を Horizon 7 と統合して IT マネージャやエンド ユーザーに以下の利点を提供できます。

- エンド ユーザーは、SaaS、Web、および Windows アプリケーションにアクセスするために使用するのと同じ Web 上のユーザー ポータルを介して、同じシングル サインオンの利便性でリモート デスクトップおよびアプリケーションにオンデマンドでアクセスします。

True SSO 機能を使用すると、スマート カードまたは 2 要素認証を使用して認証するユーザーは、Active Directory 認証情報を入力せずにリモート デスクトップおよびアプリケーションにアクセスできます。

- エンド ユーザーは、必要なアプリケーションを使用するために、リモート デスクトップ内から Web 上の VMware Identity Manager にアクセスできます。
- また、HTML Access も使用すると、エンド ユーザーは、クライアントシステムやデバイスにクライアント アプリケーションをインストールせずに、ブラウザ内でリモート デスクトップを開くことができます。
- IT マネージャは、VMware Identity Manager のブラウザ ベースの管理コンソールを使用してリモート デスクトップに対するユーザーおよびグループの資格を監視できます。

VMware Mirage および Horizon FLEX

Mirage および Horizon FLEX を使用すると、ユーザーがインストールしたアプリケーションやデータを上書きすることなく、専用の完全クローン リモート デスクトップでアプリケーションを展開および更新することができます。

Mirage は、以前に Horizon 7 に含まれていたローカル モード機能よりも優れたオフライン仮想デスクトップ ソリューションを提供します。Mirage には、オフライン デスクトップのための、次のようなセキュリティ機能と管理機能が含まれています。

- ローカルにインストールされた仮想マシンを暗号化し、安全なコンテナの整合性に影響を与える仮想マシン設定をユーザーが変更できないようにする。
- VMware Fusion™ Professional および VMware® Player Plus™ で使用可能なポリシー（有効期限を含む）を提供する。これは、以前のローカル モード機能で提供されていたポリシーに相当します。Fusion Pro と Player Plus は、Mirage に含まれています。
- 更新を受信するためにユーザーがデスクトップにチェックインしたりチェックアウトしたりする必要がなくなる。
- 管理者が Mirage の階層化機能、バックアップ機能、ファイル ポータルを利用できるようにする。

VMware App Volumes

VMware App Volumes は、Horizon 7 および他の仮想環境向けの統合アプリケーション提供およびユーザー管理のシステムです。App Volumes により管理されるアプリケーションとデータは、AppStack と呼ばれる特殊な VMDK または VHD に保持されます。AppStack はログインまたは再起動時に各 Windows ユーザーセッションに接続されます。この戦略により、最新のアプリケーションとデータがユーザーに確実に提供されます。App Volumes は、ユーザーがインストールする通常アプリケーションおよび設定向けに別のコンテナも提供します。書き込み可能ボリュームと呼ばれるこのコンテナも、ログインまたは再起動時にロードされます。ユーザー プロファイルおよびポリシー設定も、App Volumes プラットフォームを使用して管理できます。

VMware User Environment Manager

スマート ポリシー機能を使用して、特定のリモート デスクトップでの USB リダイレクト、仮想印刷、クリップボード リダイレクト、クライアント ドライブ リダイレクト、および PCoIP 表示プロトコル機能の動作を制御するポリシーを作成できます。User Environment Manager は、ユーザーがパーソナライズを許可される設定を IT が制御できるようにし、またネットワークや場所別のプリンタなどの環境設定もマップします。スマート ポリシーにより、特定の条件が満たされる場合にのみ有効になるポリシーを作成できます。たとえば、ユーザーが企業のネットワーク以外からリモート デスクトップに接続している場合はクライアント ドライブ リダイレクト機能を無効にするポリシーを設定できます。

VMware Unified Access Gateway

Unified Access Gateway は、企業のファイアウォールの外部からリモート デスクトップおよびアプリケーションにアクセスするユーザーのセキュア ゲートウェイとして機能します。Unified Access Gateway は、非武装地帯 (DMZ) にインストールされるアプライアンスです。確実な方法で認証されたリモート ユーザーのト

ラフィックだけを社内のデータセンターに送信するために、Unified Access Gateway を使用してください。Horizon 7 セキュリティ サーバの代わりに Unified Access Gateway アプライアンスを使用できます。詳細については、『Unified Access Gateway』ドキュメントを参照してください。

一般的なビデオ会議ソフトウェアとの統合

Horizon 7 では、次の音声会議およびビデオ会議ソフトウェアを使用できます。

Flash URL リダイレクト

Adobe Media Server からクライアント エンドポイントに Flash コンテンツを直接ストリーミングするとデータセンター ESXi ホストへの負荷が低減され、データセンターを経由する余分なルーティングが不要になり、複数のクライアント エンドポイントにライブ ビデオ イベントを同時にストリームするために必要となるバンド幅が削減されます。

Flash URL リダイレクト機能は、Web ページの管理者によって Web ページ内に組み込まれた JavaScript を使用します。仮想デスクトップ ユーザーが Web ページ内に指定された URL リンクをクリックすると、JavaScript は、ShockWave ファイル (SWF) をインターセプトし、仮想デスクトップ セッションからクライアント エンドポイントにリダイレクトします。エンドポイントは次に仮想デスクトップ セクションの外のローカル VMware Flash Projector を開き、メディア ストリームをローカルで再生します。

注： Flash URL リダイレクトを使用すれば、マルチキャストまたはユニキャストのストリームは、社内のファイアウォールの外にあるクライアント デバイスにリダイレクトされます。クライアントは、マルチキャストまたはユニキャストのストリーミングを開始する ShockWave Flash (SWF) ファイルをホストする Adobe Web サーバにアクセスする必要があります。必要に応じて、クライアント デバイスがこのサーバにアクセスすることを許可するために適切なポートを開くようにファイアウォールを構成します。

この機能を使用できるのは、一部のクライアント タイプ上だけです。この機能が特定のタイプのクライアントでサポートされるかどうかを確認するには、デスクトップまたはモバイル クライアント デバイスのそれぞれのタイプに関する「VMware Horizon Client の使用」に含まれる機能サポート マトリックスを参照してください。<https://docs.vmware.com/jp/VMware-Horizon-Client/index.html> をご覧ください。

Microsoft Lync 2013

Microsoft Lync 2013 クライアントをリモート デスクトップで使用して、Unified Communications (UC) VoIP (voice over IP) および Lync 認定の USB オーディオおよびビデオ デバイスでビデオ チャット電話に参加できます。専用の IP 電話が不要になります。

このアーキテクチャでは、リモート デスクトップに Microsoft Lync 2013 クライアントをインストールし、Windows 7 または 8 のクライアント エンドポイントに Microsoft Lync VDI プラグインをインストールする必要があります。顧客は Microsoft Lync 2013 クライアントを使用して、プレゼンス、インスタント メッセージ、Web 会議、および Microsoft Office 機能を使用できます。

Lync VoIP またはビデオ チャットが行われると、Lync VDI プラグインはデータセンター サーバからクライアント エンドポイントにすべてのメディア処理をオフロードし、すべてのメディアを Lync で最適化されたオーディオおよびビデオ codec にエンコードします。この最適化されたアーキテクチャは拡張性が高く、低いネットワークバンド幅を使用し、品質の高いリアルタイム VoIP およびビデオがサポートされたポイントツーポイントのメディア配信を提供します。詳細については、<http://www.vmware.com/files/pdf/techpaper/vmware-horizon-view-microsoft-lync-install-configure.pdf> に掲載されている VMware Horizon 6 および Microsoft Lync 2013 に関するホワイト ペーパーを参照してください。

注： オーディオ録音はサポートされません。この統合は、PCoIP または Blast Extreme 表示プロトコルでのみサポートされます。

Skype for Business

エンド ユーザーは、仮想インフラストラクチャに影響を及ぼしたり、ネットワークを過負荷状態にすることなく、仮想デスクトップ内の Skype for Business で最適な音声通話とビデオ通話を行うことができます。Skype の音声通話またはビデオ通話中は、仮想デスクトップではなくクライアント マシンですべてのメディア処理が実行されます。

Virtualization Pack for Skype for Business は、Horizon Client for Windows (4.6 以降)、Horizon Client for Linux (4.6 以降)、Horizon Client for Mac (4.7 以降) のインストーラの一部として、デフォルトでインストールされます。また、Horizon Agent のインストール時に、Horizon 管理者が VMware Virtualization Pack for Skype for Business 機能を仮想デスクトップにインストールする必要があります。詳細については、『Horizon 7 での仮想デスクトップのセットアップ』を参照してください。Skype for Business の構成方法については、『Horizon 7 でのリモート デスクトップ機能の構成』を参照してください。

Horizon 7 とビジネス インテリジェンス ソフトウェアの統合

Microsoft SQL Server や Oracle データベースにイベントを記録するように、Horizon 接続サーバを構成できます。

- ログインやデスクトップ セッションの開始などのエンド ユーザー アクション。
- 資格の追加やデスクトップ プールの作成などの管理者アクション。
- システムの障害やエラーを報告するアラート。
- 24 時間のユーザー最大数を報告するなどの統計サンプリング。

Crystal Reports、IBM Cognos、MicroStrategy 9、および Oracle Enterprise Performance Management System などのビジネス インテリジェンスのレポート エンジンを使用して、イベント データベースにアクセスして分析することもできます。

詳細については、『Horizon 7 の統合』を参照してください。

その代わりに、分析ソフトウェアがイベント データにアクセスできるようにするために、Syslog 形式で Horizon 7 イベントを生成することができます。イベントのファイル ベースのログ記録を有効にすると、イベントはローカル ログ ファイルに蓄積されます。ファイル共有を指定すると、ログ ファイルはその共有に移動されます。詳細については、『Horizon 7 のインストール』を参照してください。

Horizon PowerCLI コマンドレットによる管理スクリプトの作成

Horizon PowerCLI コマンドレットを VMware PowerCLI と一緒に使用できます。Horizon PowerCLI コマンドレットを使用して、Horizon コンポーネントに対する各種管理タスクを実行できます。

Horizon PowerCLI コマンドレットの詳細については、『VMware PowerCLI Cmdlets Reference』を参照してください。

高度な関数およびスクリプトを作成して Horizon PowerCLI と一緒に使用するための API 仕様の詳細については、[VMware Developer Center](#) の View API リファレンスを参照してください。

独自の Horizon PowerCLI スクリプトを作成するために使用できるサンプル スクリプトの詳細については、[GitHub](#) の [Horizon PowerCLI コミュニティ](#)を参照してください。

Horizon PowerCLI cmdlet を使用して、Horizon 7 コンポーネントでさまざまな管理タスクを実行することができます。

- デスクトップ プールの作成と更新。
- プールの仮想マシンに指定された IP アドレスの数を大幅に拡大するために複数のネットワーク ラベルを構成。
- 完全仮想マシンまたはリンク クローン プールへのデータセンター リソースの追加。
- リンク クローン デスクトップでの再分散、更新、再構成操作の実行。
- 一定時間における特定のデスクトップまたはデスクトップ プールの使用状況のサンプリング。
- イベント データベースのクエリ。
- サービスの状態のクエリ。

Horizon 7 での LDAP 構成データの変更

Horizon Administrator を使用して Horizon 7 の構成を変更すると、リポジトリ内の対応する LDAP データが更新されます。Horizon 接続サーバは、LDAP 互換のリポジトリに構成情報を格納します。たとえば、デスクトップ プールが追加されると、接続サーバはユーザー、ユーザー グループ、および資格に関する情報を LDAP に格納します。

VMware および Microsoft のコマンド ライン ツールを使用して、Horizon 7 との間で LDAP 構成データを LDAP データ交換形式 (LDIF) ファイルでエクスポートおよびインポートできます。これらのコマンドは、構成データの更新に Horizon Administrator や Horizon PowerCLI ではなくスクリプトを使用する上級管理者向けのコマンドです。

LDIF ファイルを使用して、いくつかのタスクを実行できます。

- 接続サーバ インスタンス間での構成データの転送。
- デスクトップ プールなどの Horizon 7 オブジェクトを多数定義した後に、それらを Horizon Administrator や Horizon PowerCLI を使用せずに View 接続サーバ インスタンスに追加。
- 接続サーバ インスタンスの復旧に使用する構成のバックアップ。

詳細については、『Horizon 7 の統合』を参照してください。

vdmadmin コマンドの使用

vdmadmin コマンド ライン インターフェイスを使用して、接続サーバ インスタンスに対するさまざまな管理タスクを実行できます。Horizon Administrator ユーザー インターフェイス内からは行えない管理タスクやスクリプトで自動的に実行する必要がある管理タスクを vdmadmin を使って行えます。

詳細については、『Horizon 7 の管理』を参照してください。

豊かなユーザー体験の計画

2

Horizon 7 は、エンド ユーザーが期待する、親しみやすくパーソナライズされたデスクトップ環境を提供します。たとえば、一部のクライアント システムでエンド ユーザーは、各自のローカル コンピュータに接続された USB デバイスやその他のデバイスにアクセスしたり、ローカル コンピュータで検出できる任意のプリンタにドキュメントを送信したり、スマート カードで認証したり、複数のディスプレイ モニターを使用したりできます。

Horizon 7 は、エンド ユーザーに提供されることが望ましい機能を多数備えています。使用する機能を決定する前に、各機能の制限および制約を理解しておく必要があります。

この章には、次のトピックが含まれています。

- [Horizon Agent 機能サポート一覧](#)
- [表示プロトコルの選択](#)
- [公開アプリケーションの使用](#)
- [Horizon Persona Management を使用したユーザーのデータと設定の保持](#)
- [リモート デスクトップおよびアプリケーションでの USB デバイスの使用](#)
- [Web カメラとマイクでリアルタイム オーディオ ビデオ機能を使用](#)
- [3D グラフィックス アプリケーションの使用](#)
- [リモート デスクトップへのマルチメディアのストリーミング](#)
- [リモート デスクトップからの印刷](#)
- [シングル サインオンによるログイン](#)
- [モニターおよび画面解像度](#)

Horizon Agent 機能サポート一覧

エンド ユーザーにどの表示プロトコルと機能を使用できるようにするかを計画する場合、以下の情報を使用して、どのエージェント（リモート デスクトップおよびアプリケーション） OS がこの機能をサポートするかを判別します。

サポートされるゲスト OS のタイプとエディションは、Windows バージョンによって異なります。サポート対象の Windows 10 オペレーティング システムの最新情報については、VMware のナレッジベースの記事 KB<http://kb.vmware.com/kb/2149393>を参照してください。Windows 10 以外の Windows オペレーティング システムの場合には、VMware のナレッジベース (KB) の記事、<http://kb.vmware.com/kb/2150295>を参照してください。

Horizon Agent がインストールされている Windows オペレーティング システムでサポートされる特定の Remote Experience 機能の一覧については、VMware のナレッジベースの記事 <http://kb.vmware.com/kb/2150305> を参照してください。

注： それぞれのクライアント デバイスのタイプでどの機能がサポートされているかについては、Horizon Client のドキュメント(<https://docs.vmware.com/jp/VMware-Horizon-Client/index.html>)を参照してください。

また、VMware のパートナー数社が、Horizon 7 のデプロイ用のシンおよびゼロ クライアント デバイスを提供しています。各シンまたはゼロ クライアント デバイスで使用可能な機能は、ベンダーおよびモデルと、企業が採用する構成によって決定されます。シンおよびゼロ クライアント デバイスのベンダーおよびモデルの詳細については、VMware Web サイトから入手可能な『[VMware 互換性ガイド](#)』（英語版）を参照してください。

表示プロトコルの選択

表示プロトコルは、データセンターに存在するリモート デスクトップまたはアプリケーションへのグラフィカル インターフェイスをエンド ユーザーに提供します。どのタイプのクライアント デバイスを使用するかによって、VMware が提供する Blast Extreme と PCoIP (PC-over-IP) または Microsoft RDP (Remote Desktop Protocol) から選択できます。

使用するプロトコルを制御するポリシー、またはエンド ユーザーがデスクトップにログインしたときにプロトコルを選択できるようにするポリシーを設定できます。

注： 一部のクライアントのタイプでは、PCoIP および RDP のいずれのリモート表示プロトコルも使用されません。たとえば、HTML Access 機能で使用可能な HTML Access クライアントを使用する場合、PCoIP または RDP ではなく Blast Extreme プロトコルが使用されます。同様に、リモートの Linux デスクトップを使用している場合は、Blast Extreme が使用されます。

VMware Blast Extreme

VMware Blast Extreme はモバイル クラウド用に最適化されており、H.264 が使用できるクライアント デバイスを最も広範囲にサポートします。表示プロトコルの中で、VMware Blast の CPU 消費は最小であり、これによりモバイル デバイスのバッテリー寿命が長くなります。VMware Blast Extreme は遅延の増加またはバンド幅の減少を補い、TCP および UDP のネットワーク転送を活用することができます。

VMware Blast 表示プロトコルは、公開アプリケーション、および仮想マシンまたは RDS ホストの共有セッション デスクトップを使うリモート デスクトップに使用できます。RDS ホストには物理マシンまたは仮想マシンを使用できます。Windows 10 RS4 以降の Enterprise Edition を除き、VMware Blast 表示プロトコルは単一ユーザーの物理コンピュータで動作しません。

注： Windows 10 RS4 を実行している物理コンピュータで、動画およびテレビのアプリケーションはサポートされません。

VMware Blast Extreme の機能

VMware Blast Extreme の主要な機能は次のとおりです。

- 会社のファイアウォールの外のユーザーは、会社の仮想プライベート ネットワーク (VPN) でこのプロトコルを使用できます。また、ユーザーは会社の DMZ のセキュリティ サーバまたは Access Point アプライアンスに対して、暗号化された安全な接続を行うことができます。
- Advanced Encryption Standard (AES) 128 ビット暗号化がサポートされており、デフォルトで有効になっています。ただし、キーの暗号化方式は AES-256 に変更できます。
- あらゆる種類のクライアント デバイスからの接続。
- LAN および WAN でのバンド幅使用を削減する最適化制御。
- Windows エージェントの PerfMon で表示されるパフォーマンス カウンタには、次のようなシステムの現状を正確に表示します。この情報は一定の間隔で更新されます。
 - Blast セッション
 - イメージング
 - オーディオ
 - CDR
 - USB : USB トラフィックが VMware 仮想チャネル (VVC) を使用するように設定されている場合、Windows エージェントの PerfMon に表示される USB カウンタは正確な値になります。
 - Skype for Business : カウンタは、制御トラフィックにのみ使用されます。
 - クリップボード
 - RTAV
 - シリアル ポートとスキャナ リダイレクト機能
 - 仮想印刷
 - HTML5 MMR
 - Windows Media MMR : この機能が VMware 仮想チャネル (VVC) を使用するように設定されている場合にのみ、パフォーマンス カウンタが表示されます。
- Windows クライアントで一時的にネットワークが切断された場合のネットワークの継続性。
- 仮想ディスプレイには 32 ビット カラーがサポートされます。
- ClearType フォントはサポートされています。
- 動的オーディオ品質調整を使用する LAN と WAN に対するオーディオのリダイレクト。
- 一部のタイプのクライアントで Webcam とマイクを使用するためのリアルタイム オーディオ ビデオ。
- 一部のクライアント上でのテキストのコピーおよび貼り付け、およびクライアントのオペレーティング システムとリモート デスクトップまたは公開アプリケーションの間でのイメージのコピーと貼り付け。その他のクライアント タイプでは、プレーン テキストのコピーおよび貼り付けのみがサポートされています。フォルダやファイルなどのシステム オブジェクトは、システム間でコピーおよび貼り付けすることができません。

- 複数のモニターは、一部のクライアント タイプでサポートされます。一部のクライアントでは、Aero が無効になっている Windows 7 リモート デスクトップに、1 つのディスプレイにつき最高 2560 x 1600 の解像度のモニターを最大 4 台、または 4K (3840 x 2160) の解像度のモニターを最大 3 台使用できます。ピボット表示および自動調整もサポートされています。

3D 機能を有効にすると、最高 1920 x 1200 の解像度のモニターが最大 2 台、または 4K (3840 x 2160) の解像度のモニター 1 台がサポートされます。

- USB のリダイレクトは、一部のクライアント タイプでサポートされます。
- MMR リダイレクトは、一部の Windows クライアント オペレーティング システムと一部のリモート デスクトップ オペレーティング システム (Horizon Agent がインストール済み) でサポートされます。
- モニターが接続されていない物理マシンへの接続は NVIDIA グラフィックス カードによりサポートされます。最高のパフォーマンスを得るために、H.264 エンコーディングをサポートするグラフィックス カードを使用してください。

アドインの GPU と組み込みの GPU がある場合、オペレーティング システムが組み込みの GPU をデフォルトに設定する可能性があります。この問題を修正するには、デバイス マネージャでデバイスを無効にするか、削除します。問題が解決しない場合には、組み込みの GPU 用の WDDM グラフィックス ドライバをインストールするか、システムの BIOS で組み込みの GPU を無効にします。組み込みの GPU を無効にする方法については、システムのドキュメントを参照してください。

注意： 組み込みの GPU を無効にすると、BIOS の設定や NT ブートローダーへのコンソール アクセスなどのアクセス機能が使用できなくなる可能性があります。

- Blast コーデックにより、より鮮明な画像とフォントが表示され、デスクトップ使用時のアダプティブ H.264 エンコーダーの機能が強化されます。このコーデックは、モーション検出、モーション ベクトル、内部予測マクロブロックを含むビデオ コーデックのように動作します。これは、次の環境でサポートされ、デフォルトでは無効になっています。
 - Windows および Linux エージェント。コーデックを有効にするには：
 - Windows エージェントの場合は、次のレジストリ キーを設定します。HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config\EncoderBlastCodecEnabled = 1
 - Linux エージェントの場合は、\etc\vmware\config の RemoteDisplay.allowBlastCodec=TRUE を設定します。
 - Windows、Linux、および MacOS のクライアントの設定で、H.264 を無効にします。モバイル クライアントと Web クライアントでは、この機能はサポートされません。
- 動的なエンコーダー スイッチを使用すると、ビデオ用に最適化されたエンコーダー (H.264 4:2:0 または H.264 4:4:4) とテキスト用に最適化されたエンコーダー (Blast コーデックとアダプティブ) を切り替えることができます。このスイッチは、帯域幅の使用量を減らし、鮮明なテキストと画像を維持するのに役立ちます。この機能を使用するには、エンコーダー スイッチを有効にします。
 - Windows エージェントの場合は、レジストリ キー HKLM\SOFTWARE\VMware, Inc.\VMware Blast\Config\EncoderSwitchEnabled = 1 を設定します。
 - Linux エージェントの場合は、\etc\vmware\config の RemoteDisplay.allowSwitchEncoder=TRUE を設定します。

- Blast コーデックを有効にします（デフォルトでは無効になっています）。Blast コーデックが有効になっていない場合、スイッチ エンコーダーはアダプティブを使用して、テキスト用に最適化されたエンコードを行います。
- Windows、Linux、および MacOS のクライアントの設定で、H.264 を有効にします。モバイル クライアントと Web クライアントでは、この機能はサポートされません。

注： エンコーダーのスイッチは、ソフトウェア H.264 のみを使用し、ハードウェア アクセラレータによるグラフィック処理はサポートされません。

どのクライアント デバイスが固有の VMware Blast Extreme 機能をサポートするかについての詳細は、<https://docs.vmware.com/jp/VMware-Horizon-Client/index.html> を参照してください。

Wake-on-LAN

Wake-on-LAN は、Windows 10 RS4 以降の Enterprise Edition が実行されている物理マシンでサポートされます。この機能を使用すると、Horizon Connection Server に接続したときに物理マシンを起動できます。Wake-on-LAN 機能には次の前提条件があります。

- Wake-on-LAN (WoL) は IPv4 環境でのみサポートされます。
- BIOS の設定とネットワーク カードの設定で Wake-on-LAN が有効になっている場合に Wake-on-LAN パケットの受信でマシンを起動するように、物理マシンが構成されている必要があります。
- Connection Server からの WoL パケットには接続先ポート 9 が使用されます。
- WoL パケットは、Horizon Connection Server から Horizon Agent に転送される IP 転送ブロードキャストパケットです。Wake-on-LAN は次のシナリオで機能します。
 - Connection Server と物理マシンの Horizon Agent が LAN 環境の同じサブネットにある。
 - 起動する物理マシンの宛先サブネットへの IP 転送ブロードキャスト パケットを許可するように、Connection Server と Horizon Agent の間のすべてのルーターが構成されている。

注： Wake-on-LAN 機能は、物理 Windows 10 エージェントのフローティング割り当てプールをサポートしていません。WoL パケットは、特定のユーザーに資格のある専用の割り当てプールにのみ送信されます。

推奨されるゲスト OS の設定

1GB 以上の RAM、および高解像度、全画面表示モード、または 720p 以上の形式のビデオの再生ではデュアル CPU が推奨される。CAD アプリケーションなどのグラフィックスを多用するアプリケーションで Virtual Dedicated Graphics Acceleration を使用するには、4GB の RAM が必要。

ビデオ品質の要件

480p 形式のビデオ

リモート デスクトップが単一の仮想 CPU を備えている場合、480p 以下のビデオをネイティブ解像度で再生できます。ビデオを HD Flash または全画面表示モードで再生する場合は、デスクトップにデュアル仮想 CPU が必要です。デュアル仮想 CPU デスクトップが搭載されていても、全画面表示モードで 360p を下回る形

式のビデオを再生する場合、特に Windows クライアントで音声が遅れる場合があります。

720p 形式のビデオ

リモート デスクトップがデュアル仮想 CPU を備えている場合、720p のビデオをネイティブ解像度で再生できます。HD または全画面表示モードで 720p のビデオを再生した場合、パフォーマンスが低下する可能性があります。

1080p 形式のビデオ

リモート デスクトップがデュアル仮想 CPU を備えている場合、メディア プレーヤーを小さいウィンドウ サイズに調整する必要がある場合がありますが、1080p 形式のビデオを再生できます。

3D レンダリング

ソフトウェア アクセラレータによるグラフィック機能またはハードウェア アクセラレータによるグラフィック機能を使用するようにリモート デスクトップを構成できます。ソフトウェア アクセラレータによるグラフィック機能を使用すると、物理的なグラフィック処理ユニット (GPU) を必要とすることなく、DirectX 9 と OpenGL 2.1 アプリケーションを実行できます。ハードウェア アクセラレータによるグラフィック機能では、仮想マシンが vSphere ホストの物理的な GPU (グラフィック処理ユニット) を共有するか、物理的な GPU を単一の仮想デスクトップの専用にすることができます。

3D アプリケーションについては、2 台までのモニターがサポートされ、最大画面解像度は 1920 x 1200 です。リモート デスクトップのゲスト OS は、Windows 7 以降が必要です。

3D 機能の詳細については、「[3D グラフィックス アプリケーションの使用](#)」を参照してください。

クライアント システムのハードウェア要件

特定のタイプのデスクトップまたはモバイル クライアント デバイスのプロセッサ要件とメモリ要件については、<https://docs.vmware.com/jp/VMware-Horizon-Client/index.html> を参照してください。

PCoIP

PCoIP (PC over IP) は、LAN 上または WAN 経由の広範なユーザーにアプリケーション、イメージ、オーディオ、ビデオ コンテンツなどの公開アプリケーションや総合的なデスクトップ環境を配信するための最適化されたデスクトップ体験を提供します。PCoIP は、レイテンシーの増加またはバンド幅の減少を補って、ネットワークの状態に関わらずユーザーの生産性を維持できるようにします。

PCoIP 表示プロトコルは、公開アプリケーションおよび、仮想マシン、Teradici ホスト カードを含む物理マシンまたは RDS ホストの共有セッション デスクトップを使用するリモート デスクトップに使用できます。

PCoIP の機能

PCoIP の主要な機能は次のとおりです。

- 会社のファイアウォールの外のユーザーは、会社の virtual private network (VPN) でこのプロトコルを使用できます。また、ユーザーは会社の DMZ のセキュリティ サーバまたは Access Point アプライアンスに対して、暗号化された安全な接続を行うことができます。

- Advanced Encryption Standard (AES) 128 ビット暗号化がサポートされており、デフォルトで有効になっています。ただし、キーの暗号化方式は AES-256 に変更できます。
 - あらゆる種類のクライアント デバイスからの接続。
 - LAN および WAN でのバンド幅使用を削減する最適化制御。
 - 仮想ディスプレイには 32 ビット カラーがサポートされます。
 - ClearType フォントはサポートされています。
 - 動的オーディオ品質調整を使用する LAN と WAN に対するオーディオのリダイレクト。
 - 一部のタイプのクライアントで Webcam とマイクを使用するためのリアルタイム オーディオ ビデオ。
 - 一部のクライアント上でのテキストのコピーおよび貼り付け、およびクライアントのオペレーティング システムとリモート デスクトップまたは公開アプリケーションの間でのイメージのコピーと貼り付け。その他のクライアント タイプでは、プレーン テキストのコピーおよび貼り付けのみがサポートされています。フォルダやファイルなどのシステム オブジェクトは、システム間でコピーおよび貼り付けすることができません。
 - 複数のモニターは、一部のクライアント タイプでサポートされます。一部のクライアントでは、Aero が無効化されている Windows 7 リモート デスクトップに、1 つのディスプレイにつき最高 2560 x 1600 の解像度のモニターを最大 4 台、または 4K (3840 x 2160) の解像度のモニターを最大 3 台使用できます。ピボット表示および自動調整もサポートされています。
- 3D 機能を有効にすると、最高 1920 x 1200 の解像度のモニターが最大 2 台、または 4K (3840 x 2160) の解像度のモニター 1 台がサポートされます。
- USB のリダイレクトは、一部のクライアント タイプでサポートされます。
 - MMR リダイレクトは、一部の Windows クライアント オペレーティング システムと一部のリモート デスクトップ オペレーティング システム (Horizon Agent がインストール済み) でサポートされます。

特定の PCoIP 機能をサポートするデスクトップ オペレーティング システムについては、「[Horizon Agent 機能サポート一覧](#)」を参照してください。

どのクライアント デバイスが固有の PCoIP 機能をサポートするかについての詳細は、<https://docs.vmware.com/jp/VMware-Horizon-Client/index.html> を参照してください。

推奨されるゲスト OS の設定

1GB 以上の RAM、および高解像度、全画面表示モード、または 720p 以上の形式のビデオの再生ではデュアル CPU が推奨される。CAD アプリケーションなどのグラフィックスを多用するアプリケーションで Virtual Dedicated Graphics Acceleration を使用するには、4GB の RAM が必要。

ビデオ品質の要件

480p 形式のビデオ

リモート デスクトップが単一の仮想 CPU を備えている場合、480p 以下のビデオをネイティブ解像度で再生できます。ビデオを HD Flash または全画面表示モードで再生する場合は、デスクトップにデュアル仮想 CPU が必要です。デュアル仮想 CPU デスクトップが搭載されていても、全画面表示モードで 360p を下回る形

式のビデオを再生する場合、特に Windows クライアントで音声が遅れる場合があります。

720p 形式のビデオ

リモート デスクトップがデュアル仮想 CPU を備えている場合、720p のビデオをネイティブ解像度で再生できます。HD または全画面表示モードで 720p のビデオを再生した場合、パフォーマンスが低下する可能性があります。

1080p 形式のビデオ

リモート デスクトップがデュアル仮想 CPU を備えている場合、メディア プレーヤーを小さいウィンドウ サイズに調整する必要がある場合がありますが、1080p 形式のビデオを再生できます。

3D レンダリング

ソフトウェア アクセラレータによるグラフィック機能またはハードウェア アクセラレータによるグラフィック機能を使用するようにリモート デスクトップを構成できます。ソフトウェア アクセラレータによるグラフィック機能を使用すると、物理的なグラフィック処理ユニット (GPU) を必要とすることなく、DirectX 9 と OpenGL 2.1 アプリケーションを実行できます。ハードウェア アクセラレータによるグラフィック機能では、仮想マシンが vSphere ホストの物理的な GPU (グラフィック処理ユニット) を共有するか、物理的な GPU を単一の仮想マシン デスクトップの専用にすることができます。

3D アプリケーションの場合は、最大 2 台のモニターがサポートされ、最大画面解像度は 1920 x 1200 です。リモート デスクトップのゲスト OS は Windows 7 以降にする必要があります。

3D 機能の詳細については、「[3D グラフィックス アプリケーションの使用](#)」を参照してください。

クライアント システムのハードウェア要件

プロセッサおよびメモリ要件の詳細については、デスクトップまたはモバイル クライアント デバイスの特定のタイプの『VMware Horizon Client の使用』を参照してください。<https://docs.vmware.com/jp/VMware-Horizon-Client/index.html> をご覧ください。

Microsoft RDP

リモート デスクトップ プロトコルは、多くのユーザーが自宅のコンピュータから職場のコンピュータにアクセスするためにすでに使用しているものと同じマルチチャネル プロトコルです。Microsoft Remote Desktop Connection (RDC) は、RDP を使用してデータを伝送します。

Microsoft RDP は、仮想マシン、物理マシン、または RDS ホスト上のセッション デスクトップを使用するリモート デスクトップにサポートされる表示プロトコルです (公開アプリケーションについては、PCoIP 表示プロトコルと VMware Blast 表示プロトコルのみがサポートされます)。Microsoft RDP は次の機能を備えています。

- RDP 7 では、最大 16 台までのモニターに対する実際の複数モニターがサポートされています。
- ローカル システムとリモート デスクトップの間で、テキストおよびシステムオブジェクト (フォルダやファイルなど) のコピーおよび貼り付けを実行できます。
- 仮想ディスプレイには 32 ビット カラーがサポートされます。
- RDP は 128 ビットの暗号化をサポートします。

- 会社のファイアウォールの外のユーザーは、会社の virtual private network (VPN) でこのプロトコルを使用できます。または、ユーザーは会社の DMZ の View セキュリティ サーバに安全で暗号化された接続ができます。

Windows 7 および Windows Server 2008 R2 への TLSv1.1 および TLSv1.2 接続をサポートするには、Microsoft 更新プログラム KB3080079 を適用する必要があります。

クライアント システムのハードウェア要件

プロセッサおよびメモリ要件の詳細については、クライアント システムの特定のタイプの『VMware Horizon Client の使用』ドキュメントを参照してください。 <https://docs.vmware.com/jp/VMware-Horizon-Client/index.html> をご覧ください。

注： モバイル クライアント 3.x デバイスは、PCoIP 表示プロトコルのみを使用します。モバイル クライアント 4.x のクライアントは、PCoIP 表示プロトコルまたは VMware Blast 表示プロトコルのみを使用します。

公開アプリケーションの使用

Horizon Client を使用すると、リモート デスクトップだけでなく、Windows ベースの公開アプリケーションにも安全にアクセスできます。

この機能を使用した場合、Horizon Client を起動して Horizon 7 サーバにログインすると、リモート デスクトップに加えてユーザーが使用する資格があるすべての公開アプリケーションが表示されます。アプリケーションを選択すると、ローカル クライアント デバイス上でそのアプリケーションのウィンドウが開きます。アプリケーションは、まるでローカルにインストールされているかのように動作します。

たとえば、Windows クライアント コンピュータでアプリケーション ウィンドウを最小化した場合、そのアプリケーションの項目はタスクバーに残り、ローカルの Windows コンピュータにインストールされている場合とまったく同じように動作します。また、ローカルにインストールされたアプリケーションのショートカットと同様に、クライアント デスクトップに表示されるアプリケーションのショートカットを作成することもできます。

次の状況では、この方法で公開アプリケーションを展開する方が完全なリモート デスクトップを展開することよりも望ましい場合があります。

- アプリケーションが複数階層化アーキテクチャで設定されていて、コンポーネントが地理的に近接しているほうが動作が向上する場合は、公開アプリケーションがよい解決方法です。

たとえば、ユーザーがデータベースにリモート アクセスする必要があるときに大量のデータを WAN 経由で送信する必要がある場合、通常はパフォーマンスに影響が出ます。公開アプリケーションを使用すると、アプリケーションのすべての部分をデータベースと同じデータセンターに配置することができるため、トラフィックが分離され、画面の更新のみが WAN 経由で送信されます。

- モバイル デバイスから個別のアプリケーションにアクセスすることは、リモート Windows デスクトップを開いてアプリケーションに移動するよりも簡単です。

この機能を使用するには、アプリケーションを Microsoft RDS ホストにインストールします。この点においては、Horizon 7 の公開アプリケーションは、他のアプリケーション リモート処理ソリューションと同様に動作します。Horizon 7 の公開アプリケーションは、最適化されたユーザー エクスペリエンスのために、Blast Extreme 表示プロトコルまたは PCoIP 表示プロトコルのいずれかを使用して提供されます。

Horizon Persona Management を使用したユーザーのデータと設定の保持

Horizon Persona Management は、リモート デスクトップだけでなく、Horizon 7 が管理しない物理コンピュータや仮想マシンでも使用できます。個人設定管理は、ユーザーがプロファイルに加えた変更を保持します。ユーザー プロファイルはユーザーが生成したさまざまな情報から構成されます。

- ユーザー固有のデータおよびデスクトップ設定。ユーザーがどのデスクトップにログインしても同じデスクトップ デザインを表示できます。
- アプリケーション データおよび設定。たとえば、ツールバーの位置や設定をアプリケーションに記憶させることができます。
- ユーザー アプリケーションによって構成された Windows レジストリ エントリ。

これらの機能を活用するため、個人設定管理では CIFS 共有でユーザーのローカル プロファイル サイズ以上のストレージが必要です。

ログオンおよびログオフ時間の最小化

個人設定管理は、デスクトップのログインおよびログオフにかかる時間を最小限に抑えます。デフォルトではログオン時に、Windows で必要なファイルのみ（ユーザー レジストリ ファイルなど）を Horizon 7 がダウンロードします。Horizon 7 はリモート デスクトップでのプロファイルの最近の変更を記録し、定期的にその変更をリモート リポジトリにコピーします。

個人設定管理では、プロファイルを管理するために Active Directory に変更を加える必要はありません。個人設定管理を構成するには、Active Directory でユーザーのプロパティを変更せずに、中央リポジトリを指定します。この中央リポジトリで、ユーザーがログオンする可能性のある他の物理マシンに影響を及ぼすことなく、1 つの環境でユーザーのプロファイルを管理できます。

個人設定管理では、VMware ThinApp アプリケーションでデスクトップをプロビジョニングする場合、ThinApp サンドボックス データもユーザー プロファイルに格納することができます。このデータはユーザーとともに移動可能で、ログオン時間には大きな影響を及ぼしません。この戦略により、データの損失や破損に対する保護が強化されます。

構成オプション

Horizon 7 個人設定は、単一のリモート デスクトップ、デスクトップ プール、OU、または展開内のすべてのリモート デスクトップなど、さまざまなレベルで構成できます。Horizon 7 が管理しない物理コンピュータおよび仮想マシンでは、スタンドアロン バージョンの個人設定管理も使用できます。

グループ ポリシー (GPO) を設定することで、個人設定に含めるファイルとフォルダを次のように細かく制御できます。ローカル設定フォルダを含めるかどうか、ログイン時にロードするファイル、ユーザー ログイン後にバックグラウンドでダウンロードするファイル、個人設定管理ではなく Windows 移動プロファイル機能により管理するユーザーの個人設定内のファイルを指定できます。

Windows 移動プロファイルと同様に、フォルダ リダイレクトを構成できます。次のフォルダをネットワーク共有にリダイレクトできます。

Contacts (連絡先)	マイ ドキュメント	Save Games (セーブ ゲーム)
Cookies (クッキー)	My Music (マイ ミュージック)	Searches (検索)
デスクトップ	My Pictures (マイ ピクチャ)	Start Menu (スタート メニュー)
ダウンロード	My Videos (マイ ビデオ)	Startup Items (スタートアップ項目)
お気に入り	Network Neighborhood (ネットワーク コンピュータ)	Templates (テンプレート)
History (履歴)	Printer Neighborhood (近くのプリンタ)	Temporary Internet Files (インターネット一時ファイル)
Links (リンク)	Recent Items (最近使った項目)	

制限

個人設定管理には、次の制限および制約があります。

- この機能は、インスタント クローン デスクトップ プールではサポートされません。
- 個人設定管理コンポーネントを含む Horizon 7 ライセンスが必要です。
- 個人設定管理には CIFS (共通インターネット ファイル システム) 共有が必要です。
- この機能は、Windows 10 のリンク クローン デスクトップ プールの永続ディスクと一緒に使用できません。

リモート デスクトップおよびアプリケーションでの USB デバイスの使用

管理者は、サム フラッシュ ドライブ、カメラ、VoIP (Voice over IP) デバイス、プリンタなどの USB デバイスを仮想デスクトップから使用できるように構成できます。この機能は USB リダイレクトと呼ばれます。仮想デスクトップでは、最大 255 個の USB デバイスに対応できます。

公開デスクトップおよびアプリケーションで使用するために、ローカルに接続された特定の USB デバイスをリダイレクトすることもできます。サポートされるデバイスのタイプについては、Horizon 7 でのリモート デスクトップ機能の構成ドキュメントを参照してください。

単一ユーザー マシンに展開されているデスクトップ プールでこの機能を使用すると、ローカル クライアント システムに接続されているほとんどの USB デバイスをリモート デスクトップで使用できるようになります。リモート デスクトップから iPad に接続して管理することもできます。たとえば、リモート デスクトップにインストールした iTunes と iPad を同期できます。Windows や Mac コンピュータなどの一部のクライアント デバイスでは、USB デバイスが Horizon Client のメニューに一覧表示されます。デバイスの接続や接続解除にもこのメニューを使用します。

ほとんどの場合、クライアント システムとリモート デスクトップの USB デバイスを同時に使用することはできません。ごく一部のタイプの USB デバイスのみ、リモート デスクトップとローカル コンピュータ間で共有できます。そのようなデバイスには、スマート カード リーダーと、キーボードやポインティング デバイスなどのヒューマン インターフェイス デバイスがあります。

管理者はエンド ユーザーに接続を許可する USB デバイスのタイプを指定できます。一部のクライアント システム上のビデオ入力デバイスとストレージ デバイスなど複数タイプのデバイスが含まれる複合デバイスについては、管理者はデバイスを分離し、あるデバイス (たとえば、ビデオ入力デバイス) は許可し、その他のデバイス (たとえば、ストレージ デバイス) は許可しないようにできます。

USB リダイレクト機能は、特定のクライアントのタイプだけで使用できます。この機能が特定のクライアントでサポートされているかどうかを確認するには、そのクライアントの Horizon Client インストールとセットアップに関するドキュメントで機能サポート一覧を参照してください。

Web カメラとマイクでリアルタイム オーディオ ビデオ機能を使用

リアルタイム オーディオビデオ機能を使用すれば、リモート デスクトップまたは公開アプリケーションでローカル クライアント システムの Web カメラまたはマイクを使用できます。リアルタイム オーディオビデオは、標準の会議アプリケーションやブラウザ ベースのビデオ アプリケーションと互換性があります。標準の Web カメラ、オーディオ USB デバイス、アナログ オーディオ入力をサポートします。

エンド ユーザーは、Skype、Webex、Google Hangouts などのオンライン会議アプリケーションをリモート デスクトップで実行できます。この機能は、USB リダイレクトを使用して達成できるよりも低いバンド幅でビデオおよびオーディオ データをエージェント マシンにリダイレクトします。リアルタイム オーディオ ビデオを使用すると、webcam イメージとオーディオ入力はクライアント上でエンコードされてからエージェント マシンに送信されます。エージェント マシンで、仮想 Web カメラと仮想マイクがストリームをデコードして再生します。これにより、サードパーティのアプリケーションで使用可能になります。

特別な構成は必要ありませんが、管理者は必要に応じてエージェント側のグループ ポリシーとレジストリ キーを使用して、フレーム レートや画像解像度を設定したり、機能をオフにすることができます。デフォルトでは、毎秒 15 フレームの場合、解像度は 320 x 240 ピクセルです。管理者は、必要に応じて、クライアント側の設定を使用して推奨する webcam またはオーディオ デバイスを設定することもできます。

注： この機能を使用できるのは、一部のクライアント タイプ上だけです。この機能が特定タイプのクライアントでサポートされているかどうかを確認するには、デスクトップまたはモバイル クライアント デバイスのタイプに応じて、インストールとセットアップに関するドキュメントに記載されている機能対応基準を参照してください。

3D グラフィックス アプリケーションの使用

Blast Extreme または PColP 表示プロトコルで利用できるソフトウェアおよびハードウェア アクセラレータによるグラフィックス機能を使用すれば、リモート デスクトップ ユーザーは、Google Earth から CAD などのグラフィックスを多用するアプリケーションに至るまでの 3D アプリケーションを実行することができます。

NVIDIA GRID vGPU（共有 GPU ハードウェア アクセラレーション）

vSphere 6.0 以降で利用可能なこの機能では、ESXi ホストの物理 GPU（グラフィック処理ユニット）が仮想マシン間で共有できます。この機能は、ハイエンドのハードウェア高速ワークステーション グラフィックスが必要な場合に使用します。

vDGA を使用する AMD Multiuser GPU

vSphere 6.0 以降で提供されるこの機能により、GPU が複数の PCI パススルーデバイスのように見えるようになり、複数の仮想マシンで AMD GPU を共有できます。この機能により、軽量の 3D タスクを処理するユーザーから、ハイエンドワークステーションでグラフィックスを処理するパワー ユーザーまで、ハードウェアで高速化された柔軟性のある 3D プロファイルを使用できるようになります。

Virtual Dedicated Graphics Acceleration (vDGA)

vSphere 5.5 Update 2 以降で提供されるこの機能を使用して、ESXi ホスト上の単一の物理 GPU を単一の仮想マシン専用にすることができます。この機能は、ハ

イエンドのハードウェア高速ワークステーション グラフィックスが必要な場合に使用します。

注： 一部の Intel vDGA カードでは、特定の vSphere 6 バージョンが必要です。
<http://www.vmware.com/resources/compatibility/search.php> にある VMware ハードウェア互換性一覧を参照してください。また、Intel vDGA の場合、他のベンダーと同様に個別の GPU ではなく、Intel 統合 GPU が使用されます。

Virtual Shared Graphics Acceleration (vSGA)

vSphere 5.5 Update 2 以降で提供されるこの機能により、ESXi ホスト上の物理的な GPU を複数の仮想マシンで共有できます。デザイン、モデリング、マルチメディアなどの処理に 3D アプリケーションを使用できます。

ソフト 3D

vSphere 5.5 Update 2 以降で提供されるソフトウェア アクセラレータによるグラフィックスで、物理的な GPU を必要とすることなく、DirectX 9 と OpenGL 2.1 アプリケーションを実行できます。この機能は、Windows Aero テーマ、Microsoft Office 2010、Google Earth など、リソース要求が少ない 3D アプリケーションで使用します。

Microsoft RDS ホスト上で実行される公開アプリケーションで NVIDIA GRID vGPU および vDGA もサポートされるようになりました。

重要： 3D レンダリングに関するさまざまな選択肢と要件の詳細については、グラフィック アクセラレーションに関する [VMware のホワイト ペーパー](#)、[NVIDIA GRID vGPU Deployment Guide for VMware Horizon 6.1](#) および [NVIDIA GRID Virtual GPU User Guide](#) を参照してください。

リモート デスクトップへのマルチメディアのストリーミング

Windows 7 および Windows 8/8.1 のデスクトップとクライアントでは、Windows Media MMR（マルチメディア リダイレクト）機能により、リモート デスクトップにマルチメディア ファイルがストリーミングされるとき、Windows クライアント コンピュータで完全に忠実な再生が実行できます。

MMR を使用すると、Windows クライアント システムでマルチメディア ストリームが処理（デコード）されます。クライアント システムはメディア コンテンツを再生し、それによって ESXi ホストの要求を開放します。Windows Media Player でサポートされるメディア フォーマットがサポートされます。たとえば、M4V、MOV、MP4、WMP、MPEG-4 Part 2、WMV 7、8 および 9、WMA、AVI、ACE、MP3、WAV などです。

注： MMR ポートをファイアウォール ソフトウェアに例外として追加する必要があります。MMR のデフォルトのポートは 9427 です。

リモート デスクトップからの印刷

仮想印刷機能を使用すると、リモート デスクトップのオペレーティング システムに追加のプリンタ ドライバをインストールする必要なく、クライアント システムのエンド ユーザーがリモート デスクトップからローカル プリンタまたはネットワーク プリンタを使用できます。ロケーション ベースの印刷機能により、リモート デスクトップを、エンドポイントのクライアント デバイスに最も近いプリンタにマッピングすることができます。

仮想印刷を使用すると、ローカル クライアント コンピュータにプリンタを追加した後で、そのプリンタが自動的に、リモート デスクトップで使用可能なプリンタのリストに自動的に追加されます。何も構成する必要はありません。この機能で使用する可能なプリンタごとに、データ圧縮、印刷品質、両面印刷、カラーなどの環境設定ができます。その場合でも、管理者権限のあるユーザーは、仮想印刷コンポーネントと競合することなくリモート デスクトップにプリンタ ドライバをインストールできます。

ローカル プリンタのリダイレクトは、次のようなユースケースで使用されます。

- USB またはクライアント デバイスのシリアル ポートに直接接続するプリンタ。
- クライアントに接続し、バーコード印刷やラベル印刷などを行う特別なプリンタ。
- 仮想セッションから接続できないリモート ネットワーク上のネットワーク プリンタ。

印刷ジョブを USB プリンタに送信するには、USB リダイレクト機能を使用するか、仮想印刷機能を使用できます。

ロケーション ベースの印刷により、IT 組織は、エンドポイントのクライアント デバイスに最も近いプリンタにリモート デスクトップをマッピングすることができます。たとえば、病院の医師が次々と部屋を移動している場合、その医師がドキュメントを印刷する度に、印刷ジョブはその医師が現在いる部屋に最も近いプリンタに送信されます。この機能を使用するには、適切なプリンタ ドライバがリモート デスクトップにインストールされている必要があります。

注： これらの印刷機能を使用できるのは、一部のタイプのクライアントのみです。印刷機能が特定のタイプのクライアントでサポートされているかどうかを確認するには、デスクトップまたはモバイル クライアント デバイスのタイプに応じて、インストールとセットアップに関するガイドに記載されている機能対応基準を参照してください。

<https://docs.vmware.com/jp/VMware-Horizon-Client/index.html> に移動します。

シングル サインオンによるログイン

シングル サインオン (SSO) 機能によって、エンド ユーザーは 1 回だけ Active Directory ログイン認証情報を入力できます。

シングル サインオン機能を使用しない場合、エンド ユーザーは 2 回ログインする必要があります。最初に Horizon 接続サーバへのログインするための Active Directory 認証情報を要求され、次にリモート デスクトップへのログインを要求されます。スマート カードも使用する場合、エンド ユーザーはスマート カード リーダに PIN を要求されたときにもログインが必要なため、3 回ログインする必要があります。

リモート デスクトップの場合、この機能には認証情報プロバイダ ダイナミックリンク ライブラリを含みます。

True SSO

True SSO 機能を使用すると、ユーザーは Active Directory 認証情報を指定する必要がなくなります。ユーザーは、Active Directory 以外の方法 (RSA SecurID または RADIUS 認証など) を使用して VMware Identity Manager にログインすると、リモート デスクトップまたはアプリケーションを使用するために Active Directory 認証情報の入力をさらに求められることはありません。

ユーザーがスマート カードまたは Active Directory 認証情報を使用して認証する場合は、True SSO 機能は必要ありませんが、このようなときも True SSO が使用されるように構成できます。これにより、ユーザーが指定する Active Directory 認証情報が無視され、True SSO が使用されます。

True SSO は、Windows ログオン プロセスで一時的な一意の証明書を作成することにより動作します。一時的な証明書をユーザーに代わって生成するには、認証局（すでに使用していない場合）と証明書登録サーバをセットアップする必要があります。登録サーバをインストールするには、接続サーバ インストーラを実行して、登録サーバのオプションを選択します。

True SSO は、アクセス（Windows デスクトップまたはアプリケーションへのアクセスなど）から認証（ユーザーの ID を検証）を分離します。ユーザーの認証情報は、電子証明書により安全性が確保されます。データセンター内では、パスワードがポルトされたり転送されたりすることはありません。詳細については、『Horizon 7 の管理』を参照してください。

モニターおよび画面解像度

リモート デスクトップを複数のモニターに展開して表示できます。高解像度モニターを使用している場合は、リモート デスクトップまたはアプリケーションを高解像度で表示できます。

[すべてのモニター] 表示モードを選択して、リモート デスクトップを複数のモニターで表示できます。[すべてのモニター] モードを使用しているときに、[最小化] ボタンをクリックしてからウィンドウを最大化すると、ウィンドウは [すべてのモニター] モードに戻ります。同様に、[全画面表示] モードを使用しているときに、ウィンドウを最小化してから最大化すると、ウィンドウは 1 台のモニターで [全画面表示] モードに戻ります。

複数のモニターがある環境における [すべてのモニター] の使用

表示プロトコルにかかわらず、リモート デスクトップで複数のモニターを使用できます。Horizon Client がすべてのモニターを使用している際にアプリケーション ウィンドウを最大化すると、アプリケーションが表示されているモニターだけでウィンドウが全画面表示に拡大します。

Horizon Client は以下のモニター設定をサポートします。

- 2 台のモニターを使用する場合、同じモードにする必要はありません。たとえば、外部モニター接続されているノートパソコンを使用している場合、外部モニターはポートレート モードまたはランドスケープ モードにできます。
- 2 台のモニターを使用している場合に限り、モニターは、並べるか 2 つずつ重ねることができます。合計の高さが 4096 ピクセル未満の場合に限り、縦に重ねることができます。
- 3D レンダリング機能を使用するには、VMware Blast 表示プロトコルまたは PCoIP 表示プロトコルを使用する必要があります。最大 1920 x 1200 の解像度で最大 2 台のモニターを使用できます。4K (3840 x 2160) の解像度の場合、1 台のモニターのみがサポートされます。
- VMware Blast 表示プロトコルまたは PCoIP 表示プロトコルでは、リモート デスクトップの 4K (3840 x 2160) の画面解像度がサポートされます。サポートされる 4K ディスプレイの数は、デスクトップ仮想マシンのハードウェア バージョンと Windows のバージョンによって異なります。

ハードウェア バージョン	Windows バージョン	サポートされる 4K ディスプレイの数
10 (ESXi 5.5.x 互換)	7、8、8.x、10	1
11 (ESXi 6.0 互換)	7 (3D レンダリング機能が無効で、Windows Aero が無効の場合)	3

ハードウェア バージョン	Windows バージョン	サポートされる 4K ディスプレイの数
11	7 (3D レンダリング機能が有効の場合)	1
11	8、8.x、10	1
13、14	7、8、8.x、10 (3D レンダリング機能が有効の場合)	1
13、14	7、8、8.x、10	4

- Microsoft RDP 7 を使用する場合、リモート デスクトップの表示に使用できるモニターは最大 16 台です。
- Microsoft RDP 表示プロトコルを使用する場合は、Microsoft リモート デスクトップ接続 (RDC) 6.0 以降がリモート デスクトップにインストールされている必要があります。

複数のモニターがある環境におけるモニター 1 台の使用

複数台のモニターがある環境で Horizon Client にその中の 1 台のモニターのみを使用させる場合、[すべてのモニター] 以外のモードでリモート デスクトップ ウィンドウを開くように選択できます。デフォルトでは、ウィンドウはプライマリ モニターで開きます。詳細については、『VMware Horizon Client for Windows のインストールとセットアップガイド』を参照してください。

高解像モードの使用

一部のクライアントのタイプで VMware Blast 表示プロトコルまたは PCoIP 表示プロトコルを使用する場合、Horizon Client では、高解像度ディスプレイが搭載されたクライアント システムの高解像度もサポートされます。高解像度モードを有効にするオプションは、クライアント システムが高解像度ディスプレイをサポートしている場合のみ表示されます。

仮想マシンで vGPU を構成すると、ハードウェア エンコードがデフォルトで有効になります。使用するビデオ メモリが 1 GB 未満で、NVENC メモリの制限でソフトウェア デコーダを使用する vGPU プロファイルを除き、サポートされるすべてのマルチモニタ設定でハードウェア エンコードが有効になります。<https://docs.nvidia.com/grid/4.3/grid-vgpu-release-notes-vmware-vsphere/index.html> で「NVENC では 1 GB 以上のフレーム バッファが必要」を参照してください。

中央からのデスクトップ プールとアプリケーション プールの管理

3

デスクトップ プールを作成する場合、含まれるリモート デスクトップは 1 つでも 100 でも 1,000 でもかまいません。デスクトップ ソースとしては、仮想マシン、物理マシン、および Windows Remote Desktop Services (RDS) ホストを使用できます。基本イメージとして 1 つの仮想マシンを作成すれば、Horizon 7 はそのイメージからリモート デスクトップのプールを生成できます。また、ユーザーにアプリケーションへのリモート アクセスを提供するアプリケーションのプールも作成できます。

この章には、次のトピックが含まれています。

- [デスクトップ プールの利点](#)
- [アプリケーション プールの利点](#)
- [ストレージ要件の軽減と管理](#)
- [アプリケーション プロビジョニング](#)
- [Active Directory GPO によるユーザーおよびデスクトップの管理](#)

デスクトップ プールの利点

Horizon 7 は、その集中管理の基盤として、デスクトップのプールを作成し、プロビジョニングする機能を備えています。

リモート デスクトップ プールは、次のいずれかのソースから作成できます。

- 物理デスクトップ PC などの物理システム。
- ESXi ホスト上でホストされ vCenter Server によって管理されている仮想マシン
- Horizon Agent をサポートする vCenter Server 以外の仮想化プラットフォームで稼動する仮想マシン。
- RDS ホストのセッション ベースのデスクトップ。RDS ホストからデスクトップ プールを作成する方法については、『Horizon 7 での公開されたデスクトップとアプリケーションのセットアップ』ドキュメントを参照してください。

vSphere 仮想マシンをデスクトップ ソースとして使用する場合は、同一の仮想デスクトップを必要な数だけ作成するプロセスを自動化できます。プールに作成される仮想デスクトップの最小数と最大数を設定できます。これらのパラメータを設定すると、すぐに使用できるリモート デスクトップの数を常に十分確保できますが、使用可能なリソースを過剰に使用するほどの数ではありません。

プールを使用してデスクトップを管理すると、プール内のすべてのリモート デスクトップに設定を適用したり、アプリケーションを展開したりすることができます。次の例は、使用可能な設定の一部を示しています。

- リモート デスクトップのデフォルトとして使用するリモート表示プロトコルと、ユーザーにデフォルトのオーバーライドを許可するかどうかの指定。
- View Composer のリンククローン仮想マシンまたは完全クローン仮想マシンについては、仮想マシンを使用していないときにパワーオフするかどうか、および完全に削除するかどうかを指定します。インスタント クローン仮想マシンは、常にパワーオンされています。
- View Composer のリンククローン仮想マシンについては、Microsoft Sysprep のカスタマイズ仕様を使用するか、または VMware の QuickPrep を使用するかを指定できます。Sysprep はプール内の各仮想マシンに一意の SID および GUID を生成します。インスタント クローンは、VMware が提供する ClonePrep と呼ばれる異なるカスタマイズ仕様を必要とします。

プール内のデスクトップにユーザーを割り当てる方法も指定できます。

専用割り当てプール

各ユーザーが特定のリモート デスクトップに割り当てられ、ログインするたびに同じデスクトップに戻ります。専用割り当てプールは、1 台のデスクトップに対して 1 人のユーザーの関係を必要とします。たとえば、100 人のユーザーを含むグループには 100 台のデスクトップを含むプールが必要となります。

フローティング割り当てプール

フローティング割り当てプールを使用すると、異なるシフトのユーザーが使用できるデスクトップのプールも作成できます。たとえば、ユーザーが一度に 100 人のシフトで勤務している場合、100 のデスクトップのプールを 300 人のユーザーが使用できます。オプションで、リモート デスクトップが使用後に毎回削除および再作成されるため、高度な制御の可能な環境が提供されます。

アプリケーション プールの利点

アプリケーション プールを使用すると、ユーザーは個人のコンピュータやデバイスではなく、データセンター内のサーバーで実行されるアプリケーションにアクセスできます。

アプリケーション プールには複数の大きな利点があります。

■ アクセシビリティ

ユーザーはネットワークの上のどこからでもアプリケーションにアクセスできます。セキュア ネットワーク アクセスも構成できます。

■ デバイスの独立性

アプリケーション プールでは、スマート フォン、タブレット、ラップトップ、シン クライアント、個人のコンピュータなどのさまざまなクライアント デバイスをサポートできます。これらのクライアント デバイスは、Windows、iOS、Mac OS、Android などのさまざまなオペレーティング システムを実行できます。

■ アクセス制御

1 人のユーザーまたはユーザーのグループに対して、アプリケーションのアクセス権を簡単かつ迅速に付与または削除することができます。

■ 展開の加速化

アプリケーション プールでは、データセンター内のサーバにのみアプリケーションを展開し、各サーバで複数のユーザーをサポートできるため、アプリケーションの展開を短期化することができます。

■ 管理性

クライアント コンピュータやデバイスに展開されているソフトウェアを管理するには、かなり多くのリソースが必要です。管理作業には、展開、構成、メンテナンス、サポート、アップグレードなどがあります。アプリケーション プールでは、ソフトウェアはデータセンター内のサーバで実行され、インストール コピーの数が少なくて済むため、企業のソフトウェア管理を簡素化できます。

■ セキュリティと規制コンプライアンス

アプリケーション プールでは、アプリケーションとその関連データがデータセンターに集約されるため、セキュリティを強化することができます。データを集約することで、セキュリティの考慮事項と規制コンプライアンスの問題に対処できます。

■ コスト削減

ソフトウェアの使用許諾契約によっては、データセンターでアプリケーションをホストすることでコスト効率を高めることができます。展開の短期化、管理性の向上などを含むその他の要因によっても、企業のソフトウェアコストを削減できます。

ストレージ要件の軽減と管理

vCenter Server によって管理される仮想マシンにデスクトップを展開すると、以前には仮想化されたサーバのみで利用できたストレージの効率性をすべて実現できます。インスタント クローンまたは Composer のリンク クローンをデスクトップ マシンとして使用することで、プール内のすべての仮想マシンが基本イメージを使用する仮想ディスクを共有するため、ストレージをより効果的に節約できます。

■ vSphere によるストレージの管理

vSphere を使用すると、ディスク ボリュームおよびファイル システムを仮想化できるため、データの物理的な格納場所を考慮に入れる必要なく、ストレージを管理および構成できます。

■ 高パフォーマンス ストレージとポリシーベース管理での VMware vSAN の使用

VMware VMware vSAN は Software-Defined Storage 階層で、vSphere 5.5 Update 2 以降のリリースで使用できます。vSphere ホストのクラスタで使用可能なローカル物理ストレージ ディスクを仮想化します。自動デスクトップ プールまたは自動ファームを作成するときにデータストアを 1 つだけ指定すると、仮想マシンのファイル、レプリカ、ユーザー データ、およびオペレーティング システムのファイルなど、さまざまなコンポーネントが適切な半導体ドライブ (SSD) ディスクまたは直接接続されたハード ディスク (HDD) に配置されます。

■ 仮想マシン中心ストレージとポリシー ベース管理のための仮想ボリュームの使用

vSphere 6.0 以降のリリースで利用可能な Virtual Volumes (VVols) を使用すると、データストアではなく、個々の仮想マシンがストレージ管理のユニットになります。ストレージ ハードウェアで仮想ディスクの内容、レイアウトおよび管理をコントロールできます。

■ Composer によるストレージ要件の低減

Composer を使用すると、仮想ディスクを基本イメージと共有するデスクトップ イメージが作成されるため、必要なストレージ容量を 50 ～ 90% 削減できます。

■ インスタント クローンによる必要ストレージの軽減

インスタント クローン機能は、vSphere vmFork テクノロジー（vSphere 6.0U1 以降で使用可能）を活用して、実行中の基本イメージまたは親仮想マシンを静止させて、仮想デスクトップのプールを迅速に作成し、カスタマイズします。

vSphere によるストレージの管理

vSphere を使用すると、ディスク ボリュームおよびファイル システムを仮想化できるため、データの物理的な格納場所を考慮に入れる必要なく、ストレージを管理および構成できます。

ファイバ チャネル SAN アレイ、iSCSI SAN アレイ、および NAS アレイは広く使用されているストレージ テクノロジーであり、データセンターのストレージのさまざまなニーズを満たすために vSphere によってサポートされています。これらのストレージ アレイは、ストレージ エリア ネットワークを介してサーバのグループに接続され、サーバのグループ間で共有されます。このような配置によってストレージ リソースを集約でき、仮想マシンに対してストレージ リソースをより柔軟にプロビジョニングできます。

互換性のある vSphere 5.5 Update 2 以降の機能

vSphere 5.5 Update 2 以降のリリースでは、vSAN を使用できます。これは、ESXi ホストで使用可能なローカルの物理的な半導体ディスク ドライブとハード ディスク ドライブをクラスタ内のすべてのホストで共有される単一データストアに仮想化します。vSAN はポリシー ベース管理による高パフォーマンス ストレージを提供します。これによって、デスクトップ プールを作成するときにデータストアを 1 つだけ指定すると、仮想マシンのファイル、レプリカ、ユーザー データ、およびオペレーティング システムのファイルなど、さまざまなコンポーネントが適切な半導体ディスク ドライブ (SSD) または直接接続されたハード ディスク (HDD) に配置されます。

vSAN では、ストレージ ポリシー プロファイルを使用して仮想マシンのストレージとパフォーマンスを管理することもできます。ホスト、ディスク、またはネットワークの障害、あるいはワークロードの変更によってポリシーが非準拠になると、vSAN は影響を受けている仮想マシンのデータを構成し直し、クラスタ全体のリソースの利用を最適化します。最大 20 台の ESXi ホストを含むクラスタにデスクトップ プールを展開できます。

vSAN は高可用性 (HA)、vMotion、および DRS などの共有ストレージを必要とする VMware 機能をサポートしますが、その一方で外部の共有ストレージは必要なくなり、ストレージ構成と仮想マシンのプロビジョニング アクティビティが簡素になります。

重要： vSphere 6.0 以降のリリースで利用可能な vSAN 機能には、多くのパフォーマンスの向上が含まれています。vSphere 6.0 では、この機能により広範囲にわたる HCL（ハードウェア互換性）サポートも含まれています。vSphere 6 以降の vSAN の詳細については、『VMware vSAN の管理』を参照してください。

注： vSAN は View Storage Accelerator 機能と互換性がありますが、ディスクのワイプおよび縮小によってディスク領域を再利用する領域効率的なディスク形式機能とは互換性がありません。

vSphere 5.5 update 2 以降のリリースでは、以下の機能を使用できます。

- View storage accelerator 機能を使用すると、仮想マシンのディスク データをキャッシュするように ESXi ホストを構成できます。

このコンテンツベースの読み取りキャッシュ (CBRC) を使用すると、多くのマシンが同時に起動してウイルス対策スキャンを実行するときに、IOPS を軽減してパフォーマンスを改善することができます。ホストは、OS 全体をストレージ システムから何度も読み取るのではなく、共通のデータ ブロックをキャッシュから読み取ることができます。

- リモート デスクトップが vSphere 5.1 以降のバージョンで使用できる領域効率的なディスク形式を使用する場合、ゲスト OS 内の無効または削除されたデータは、自動的にワイプおよび縮小プロセスで再利用されます。
- レプリカ ディスクは、VMFS5 以降のデータストアまたは NFS データストアに保存する必要があります。VMFS5 より前の VMFS バージョンにレプリカを保存する場合、クラスタは最大で 8 ホストを持つことができます。OS ディスクおよび通常ディスクは、NFS データストアまたは VMFS データストアに格納できます。

互換性のある vSphere 6.0 以降の機能

vSphere 6.0 以降のリリースでは Virtual Volumes (VVol) を使用できます。この機能は、仮想ディスクとそれらの派生物、クローン、スナップショット、およびレプリカを、ストレージ システム上の仮想ボリュームと呼ばれるオブジェクトに直接マッピングします。このマッピングにより、vSphere はスナップショットの取得、クローンの作成、およびレプリケーションなど、集約的なストレージ オペレーションをストレージ システムにオフロードできます。

仮想ボリュームでは、vSphere でストレージ ポリシー プロファイルを使用して仮想マシンのストレージとパフォーマンスを管理することもできます。これらのストレージ ポリシー プロファイルでは、仮想マシンごとにストレージ サービスに指示が行われます。このタイプの詳細なプロビジョニングでは、容量の使用率が高まります。最大 32 台の ESXi ホストを含むクラスタにデスクトップ プールを展開できます。

注： 仮想ボリュームは View Storage Accelerator 機能と互換性がありますが、ディスクのワイプおよび縮小によってディスク領域を再利用する領域効率的なディスク形式機能とは互換性ありません。

注： インスタント クローンは仮想ボリュームをサポートしません。

高パフォーマンス ストレージとポリシーベース管理での VMware vSAN の使用

VMware VMware vSAN は Software-Defined Storage 階層で、vSphere 5.5 Update 2 以降のリリースで使用できます。vSphere ホストのクラスタで使用可能なローカル物理ストレージ ディスクを仮想化します。自動デスクトップ プールまたは自動ファームを作成するときにデータストアを 1 つだけ指定すると、仮想マシンのファイル、レプリカ、ユーザー データ、およびオペレーティング システムのファイルなど、さまざまなコンポーネントが適切な半導体ドライブ (SSD) ディスクまたは直接接続されたハード ディスク (HDD) に配置されます。

vSAN はポリシー ベースのアプローチをストレージ管理に実装します。vSAN を使用する場合は、Horizon 7 によって容量、パフォーマンス、可用性などの仮想マシン ストレージ要件が、デフォルト ストレージ ポリシー プロファイルの形で定義され、vCenter Server の仮想デスクトップに自動的に展開されます。ポリシーは、ディスク (vSAN オブジェクト) ごとに自動的に適用され、仮想デスクトップのライフサイクル全体で維持されます。ストレージは、割り当てられたポリシーに従ってプロビジョニングされ、自動的に設定されます。これらのポリシーは、vCenter Server で変更できます。Horizon は、リンク クローン デスクトップ プール、インスタント クローン デスクトップ プール、完全クローンのデスクトップ プール、Horizon クラスタごとの自動ファームに vSAN ポリシーを作成します。

vSAN クラスタで暗号化を有効にすると、vSAN データストア内に保存されているすべてのデータを暗号化できます (すべての Horizon 7 デスクトップ プール タイプがサポートされます)。vSAN 暗号化は、vSAN バージョン 6.6 以降で使用できます。vSAN クラスタの暗号化の詳細については、VMware vSAN のドキュメントを参照してください。

各仮想マシンはクラスタ内の物理的な位置にかかわらず、そのポリシーを保持します。ポリシーが、ホスト、ディスク、またはネットワーク障害のために不適合になったり、ワークロードが変更される場合、vSAN は各仮想マシンのポリシーを満たすために、影響のある仮想マシンとロード バランスのデータを再構成します。

vSAN は高可用性 (HA)、vMotion、および DRS などの共有ストレージ インフラストラクチャを必要とする VMware 機能をサポートしますが、その一方で外部の共有ストレージは必要なくなり、ストレージ構成と仮想マシンのプロビジョニング アクティビティが簡素になります。

重要： vSphere 6.0 以降のリリースで使用可能な vSAN 機能には、vSphere 5.5 Update 2 で使用可能になった機能を上回る、多数のパフォーマンス上の改善が含まれています。vSphere 6.0 では、この機能により広範囲にわたる HCL (ハードウェア互換性) サポートも含まれています。また、VMware vSAN 6.0 は、キャッシングと固定ストレージの両方にフラッシュベースのデバイスを使用するオールフラッシュ アーキテクチャをサポートします。

要件および制限

vSAN 機能には、Horizon 7 展開で使用する場合に次の制限があります。

- このリリースでは、ディスクのワイプおよび縮小によってディスク領域を再利用する Horizon 7 領域効率的なディスク形式機能がサポートされていません。
- vSAN は NAS デバイスを使用しないため、vSAN は View Composer Array Integration (VCAI) 機能をサポートしません。

注： vSAN は View Storage Accelerator 機能と互換性があります。vSAN は SSD ディスクでキャッシュ レイヤーを提供し、View Storage Accelerator 機能は起動時の IOPS を削減してパフォーマンスを向上させるコンテンツベースのキャッシュ機能を提供します。

vSAN 機能には次の要件があります。

- vSphere 5.5 Update 2 以降のリリース。
- 適切なハードウェア。たとえば、VMware では容量に関する各ノードには、10GB の NIC、少なくとも 1 つの SSD、1 つの HDD を推奨しています。個別の要件については、『[VMware 互換性ガイド](#)』を参照してください。
- 少なくとも 3 つの ESXi ホストのクラスタ。vSAN ストレッチ クラスタを備える 2 台の ESXi ホストを使用した場合でも、セットアップに対応するためには十分な ESXi ホストが必要です。詳細については、『vSphere 構成の上限』ドキュメントを参照してください。
- HDD の容量の少なくとも 10% である SSD の容量。
- セットアップに対応する十分な HDD 容量。磁気ディスクの使用率が 75% を超過しないようにします。

vSAN 要件の詳細については、『vSphere 5.5 Update 2 ストレージ』ドキュメントの「vSAN の操作」を参照してください。vSphere 6 以降については、『VMware vSAN の管理』ドキュメントを参照してください。VMware vSAN の Horizon 7 仮想デスクトップ インフラストラクチャの主要コンポーネントのサイズ調整と設計のガイダンスについては、<http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf> から提供されているホワイト ペーパーを参照してください。

仮想マシン中心ストレージとポリシー ベース管理のための仮想ボリュームの使用

vSphere 6.0 以降のリリースで利用可能な Virtual Volumes (VVol) を使用すると、データストアではなく、個々の仮想マシンがストレージ管理のユニットになります。ストレージ ハードウェアで仮想ディスクの内容、レイアウトおよび管理をコントロールできます。

Virtual Volumes では、LUN または NFS 共有をベースにした伝統的なストレージ ボリュームを抽象ストレージ コンテナに置き換えます。Virtual Volumes では、仮想ディスクとその派生物、クローン、スナップショット、レプリカを仮想ボリュームと呼ばれるストレージ システム上のオブジェクトに直接マッピングします。このマッピングにより、vSphere はスナップショットの取得、クローンの作成、およびレプリケーションなど、集約的なストレージ オペレーションをストレージ システムにオフロードできます。この結果、たとえば、以前は 1 時間かかっていたクローン作成オペレーションも、仮想ボリュームを使用してわずか数分間で完了できるようになりました。

重要： 仮想ボリュームの重要なメリットのうちの 1 つは、ソフトウェア ポリシー ベース管理 (SPBM) を使用する機能です。ただし、このリリースについては、Horizon 7 は、vSAN が作成するデフォルトのきめ細かいストレージ ポリシーを作成しません。代わりに、すべての Virtual Volumes データストアに適用される vCenter Server のグローバル デフォルト ポリシーを設定できます。

Virtual Volumes には次の利点があります。

- Virtual Volumes はストレージ ハードウェアに対する多くの操作のオフロードをサポートします。これらの操作には、スナップショット、クローン作成および Storage DRS を含みます。
- Virtual Volumes で、個々の仮想マシンのレプリケーション、暗号化、重複排除および圧縮を含む先進的なストレージ サービスを使用できます。
- Virtual Volumes では、vMotion、Storage vMotion、スナップショット、リンク クローン、Flash Read Cache および DRS などの vSphere 機能がサポートされます。
- vSphere APIs for Array Integration (VAAI) をサポートするストレージ アレイで Virtual Volumes を使用できます。

要件および制限

Virtual Volumes 機能には、Horizon 7 展開で使用する場合に次の制限があります。

- このリリースでは、ディスクのワイプおよび縮小によってディスク領域を再利用する Horizon 7 領域効率的なディスク形式機能がサポートされていません。
- Virtual Volumes では View Composer Array Integration (VCAI) の使用はサポートされません。

- インスタント クローン デスクトップ プールでは、Virtual Volumes データストアはサポートされません。

注： Virtual Volumes は View Storage Accelerator 機能と互換性があります。vSAN は SSD ディスクでキャッシュ レイヤーを提供し、View Storage Accelerator 機能は起動時の IOPS を削減してパフォーマンスを向上させるコンテンツ ベースのキャッシュ機能を提供します。

Virtual Volumes 機能には以下の要件があります。

- vSphere 6.0 以降のリリース。
- 適切なハードウェア。特定のストレージ ベンダーは、vSphere の統合や Virtual Volumes のサポートができるストレージ プロバイダを供給する責任があります。すべてのストレージ プロバイダは VMware に認定され、適切に配置される必要があります。
- 仮想マシン上にプロビジョニングするすべての仮想ディスクは、1 MB の偶数倍である必要があります。

Virtual Volumes は vSphere 6.0 の機能です。要件、機能性、背景、およびセットアップ要件の詳細については、『vSphere ストレージ』ドキュメントの Virtual Volumes に関するトピックを参照してください。

Composer によるストレージ要件の低減

Composer を使用すると、仮想ディスクを基本イメージと共有するデスクトップ イメージが作成されるため、必要なストレージ容量を 50 ～ 90% 削減できます。

Composer では、基本イメージ、つまり親仮想マシンが使用され、最大 2,000 のリンク クローン仮想マシンのプールが作成されます。各リンク クローンは一意のホスト名および IP アドレスを持ち、独立したデスクトップのように動作しますが、リンク クローンの方がストレージの必要量ははるかに少なくなります。

同じデータストア上のレプリカおよびリンク クローン

Microsoft RDS ホストのリンククローン デスクトップ プールやファームを作成するときに、完全クローンが親仮想マシンから最初に作成されます。完全クローン、つまりレプリカと、それにリンクされたクローンは、同じデータストア、つまり LUN (Logical Unit Number) に配置できます。必要に応じて、再分散機能を使用してレプリカとリンククローン デスクトップ プールを 1 つの LUN から別の LUN に移動することも、リンククローン デスクトップ プールを vSAN データストアに移動することも、リンククローン デスクトップ プールを vSAN データストアから LUN に移動することもできます。

異なるデータストアにあるレプリカおよびリンク クローン

あるいは、Composer レプリカとリンク クローンをパフォーマンス特性の異なる別々のデータストアに配置することもできます。たとえば、レプリカの仮想マシンは半導体ディスク ドライブ (SSD) に格納するようにします。半導体ディスク ドライブはストレージ容量は低いものの 1 秒あたりの I/O 動作回数 (IOPS) で数万回をサポートするほどに高い読み取りパフォーマンスを備えています。リンク クローンは従来の回転メディア対応のデータストアに格納できます。このディスクはパフォーマンスは低いですが、価格が安くて格納容量が大きいので、大規模なプールに多数のリンク クローンを格納する場合に適しています。ストレージ構成を階層化すると、多数の仮想マシンを同時にリブートしたり、アンチウィルス スキャンをスケジュールして実行したりする場合のように多大の I/O が発生するシナリオを費用対効果の高い方法で処理できます。

詳細については、ベスト プラクティス ガイドである『Storage Considerations for VMware View』を参照してください。

vSAN データストアまたは Virtual Volumes のデータストアを使用する場合、レプリカ用とリンク クローン用に別々のデータストアを手動で選択することはできません。vSAN および Virtual Volumes 機能では、自動的に適切なタイプのディスクにオブジェクトが配置され、すべての I/O 操作がキャッシュされます。このため、vSAN データストアおよび Virtual Volumes のデータストアのためにレプリカ階層を使用する必要はありません。

ページングおよび一時ファイルのためのディスポーザブル ディスク

リンククローン プールやファームを作成する場合、ユーザー セッション中に生成されるゲスト オペレーティング システムのページングや一時ファイルを格納するために一時利用する仮想ディスクを別個に構成しておくこともできます。仮想マシンがパワーオフになると、ディスポーザブルディスクは削除されます。一時利用のディスクを使用することにより、リンク クローンの増加を抑えてストレージ領域を節約でき、またパワーオフ後も仮想マシンによって使用されていた領域を削減できます。

専用デスクトップのための通常ディスク

専用割り当てデスクトップ プールを作成する場合、Composer によって各仮想デスクトップ用に別個の通常仮想ディスクが作成されるようにすることもできます。その通常ディスクにエンド ユーザーの Windows プロファイルおよびアプリケーション データが保存されます。リンク クローンが更新、再構成、または再分散されても、通常仮想ディスクの内容は保たれます。Composer の通常ディスクは別のデータストアに保持することをおすすめします。その場合、通常ディスクを保持している LUN 全体をバックアップできます。

フローティング、ステートレス デスクトップのためのローカル データストア

リンク クローン デスクトップは、ESXi ホストの内部スベア ディスクにあるローカル データストアに格納できます。ローカル ストレージには、安価なハードウェア、仮想マシンの迅速なプロビジョニング、高性能の電力操作、およびシンプルな管理などの利点があります。ただし、ローカル ストレージを使用すると、利用可能な vSphere インフラストラクチャ構成オプションが制限されます。環境によってはローカル ストレージの使用が利点となる場合もありますが、不適当となる場合もあります。

注： このセクションで挙げている制限は、vSAN についての前のセクションで説明しているようにローカル ストレージ ディスクを使用するが特定のハードウェアを必要とする vSAN データストアには適用されません。

お使いの環境のリモート デスクトップがステートレスである場合には、通常、ローカル データストアを活用できます。たとえば、ステートレスなキオスクやクラスルームおよびトレーニング ステーションを展開する場合には、ローカル データストアを活用できる場合があります。

ローカル ストレージの利点を活用する場合には、次の制限事項について十分に注意してください。

- VMotion、VMware High Availability (HA)、または vSphere Distributed Resource Scheduler (DRS) を使用できません。
- Composer の再調整操作を使用して、リソース プール全体で仮想マシンのロード バランシングを行うことができません。
- 別々のデータストアに Composer のレプリカとリンク クローンを格納できません。同じボリュームにこれらを格納することを推奨します。

仮想マシンの数とそのディスクの増加を制御して、ローカル ディスク使用率を管理しており、フローティング割り当てを使用し、定期的な更新および削除操作を実行している場合、ローカル データストアにリンク クローンを正しく展開できます。

詳細については、『Horizon 7 での仮想デスクトップのセットアップ』ドキュメントのデスクトップ プールの作成に関する章を参照してください。

インスタント クローンによる必要ストレージの軽減

インスタント クローン機能は、vSphere vmFork テクノロジー (vSphere 6.0U1 以降で使用可能) を活用して、実行中の基本イメージまたは親仮想マシンを静止させて、仮想デスクトップのプールを迅速に作成し、カスタマイズします。

インスタント クローンは、作成時に仮想ディスクを親仮想マシンと共有するだけでなく、親のメモリも共有します。各インスタント クローンは一意のホスト名および IP アドレスを持ち、独立したデスクトップのように動作しますが、インスタント クローンの方がストレージの必要量ははるかに少なくなります。インスタント クローンにより、必要とされるストレージ容量は 50 ~ 90% 軽減されます。また、クローン作成時に必要なメモリの合計量も軽減されます。ストレージ要件とサイジングの制限の詳細については、VMware のナレッジベース (KB) の記事、<https://kb.vmware.com/kb/2150348> を参照してください。

Horizon 7 バージョン 7.8 以降では、インスタント クローンで、vSAN データストアの vSphere TRIM および UNMAP 機能がサポートされます。

同じデータストア上のレプリカおよびインスタント クローン

インスタント クローン デスクトップ プールを作成すると、最初にマスター仮想マシンから完全クローンが作成されます。完全クローン、つまりレプリカと、それにリンクされたクローンは、同じデータ ストア、つまり LUN (Logical Unit Number) に配置できます。

異なるデータストアにあるレプリカおよびインスタント クローン

あるいは、インスタント クローン レプリカとインスタント クローンをパフォーマンス特性の異なる別々のデータストアに配置することもできます。たとえば、レプリカの仮想マシンは半導体ディスク ドライブ (SSD) に格納するようにします。半導体ディスク ドライブはストレージ容量は低いものの 1 秒あたりの I/O 動作回数 (IOPS) で数万回をサポートするほどに高い読み取りパフォーマンスを備えています。

インスタント クローンは従来の回転メディア対応のデータストアに格納できます。このディスクはパフォーマンスは低いですが、価格が安くて格納容量が大きいので、大規模なプールに多数のインスタント クローンを格納する場合に適しています。ストレージ構成を階層化すると、スケジュールされたアンチウィルス スキャンを同時に実行したりする場合のように多大の I/O が発生するシナリオを費用対効果の高い方法で処理できます。

vSAN データストアを使用する場合、レプリカ用とインスタント クローン用に別々のデータストアを手動で選択することはできません。vSAN では、自動的に適切なタイプのディスクにオブジェクトが配置され、すべての I/O 操作がキャッシュされます。このため、vSAN データ ストアのためにレプリカ階層を使用する必要はありません。vSAN データストアでは、インスタント クローン プールがサポートされます。

ローカル データストアへのインスタンス クローンの保存

インスタンス クローン仮想マシンは、ESXi ホストの内部スベア ディスクであるローカル データストアに保存できます。ローカル ストレージには、安価なハードウェア、仮想マシンの迅速なプロビジョニング、高性能の電力操作、およびシンプルな管理などの利点があります。ただし、ローカル ストレージを使用すると、利用可能な vSphere インフラストラクチャの構成オプションが制限されます。Horizon 7 環境によってはローカル ストレージの使用が利点となる場合もありますが、不適当となる場合もあります。

注： このトピックに記載されている制限は、vSAN データストアには適用されません。このデータストアはローカル ストレージ ディスクも使用しますが、特定のハードウェアを必要とします。

お使いの環境の Horizon 7 デスクトップがステートレスである場合には、通常、ローカル データストアを使用する利点があります。たとえば、ステートレスなキオスクやクラスルームおよびトレーニング ステーションを展開する場合には、ローカル データストアを活用できる場合があります。

仮想マシンでフローティング割り当てを行う場合、個々のエンド ユーザー専用ではなく、ローカル データストアの使用を検討してください。また、定期的に（ユーザーのログオフ時など）削除または更新できます。この方法を使用すれば、データストアをまたぐ仮想マシンの移動や負荷分散を行わずに、個々のローカル データストアのディスク使用率を制御できます。

ただし、ローカル データストアの使用で Horizon 7 デスクトップまたはファーム展開に生じる次の制限について考慮する必要があります。

- VMotion を使用して Virtual Volumes を管理することはできません。
- VMware High Availability は使用できません。
- vSphere Distributed Resource Scheduler (DRS) は使用できません。

ローカル データストアを持つ単一の ESXi ホストにインスタント クローンを展開する場合には、この ESXi ホストを含むクラスタを構成する必要があります。ローカル データストアを持つ 2 台以上の ESXi ホストのクラスタがある場合は、クラスタ内の各ホストからローカル データストアを選択します。この操作を行わないと、インスタント クローンの作成が失敗します。これは、Composer リンク クローンのローカル データストアの動作とは異なります。

- 別のデータストアにレプリカやインスタント クローンを保存することはできません。
- ローカル スピニングディスク ドライブを選択する場合、市販のストレージ アレイのパフォーマンスよりも劣る可能性があります。ローカル スピニングディスク ドライブとストレージ アレイは同様の容量である可能性がありますが、ローカル スピニングディスク ドライブには、ストレージ アレイほどのスループットはありません。スピンドルの数が増えれば、スループットも向上します。直接接続のソリッド ステート ディスク (SSD) を選択する場合、ほとんどの場合、多くのストレージ アレイを超えるパフォーマンスが出ます。
- ローカル ストレージの利点を活用するのであれば、VMotion、高可用性、DRS およびその他の機能を利用できない重大性を慎重に考慮する必要があります。仮想マシンの数とディスクの増加を制御して、ローカル ディスク使用率を管理しており、フローティング割り当てを使用し、定期的な更新および削除操作を実行している場合、ローカル データストアにインスタント クローンを正しく展開できます。
- インスタント クローンのローカル データストア サポートは、仮想デスクトップと公開のデスクトップの両方で使用できます。

インスタント クローンと Composer のリンク クローンの違い

インスタント クローンはリンク クローンに比べて大幅に高速で作成できるため、インスタント クローンのプールをプロビジョニングする場合、次の機能は必要なくなります。

- インスタント クローン プールは、ゲスト オペレーティング システムのページング ファイルと一時ファイルを格納するための廃棄可能な個別の仮想ディスクの構成をサポートしません。ユーザーがインスタント クローン デスクトップからログアウトするたびに、Horizon 7 はクローンを自動的に削除し、プールが使用可能な最新の OS イメージに基づいて別のインスタント クローンをプロビジョニングしてパワーオンします。ゲスト オペレーティング システムのページング ファイルと一時ファイルは、ログアウト操作中に自動的に削除されます。
- インスタント クローン プールは、各仮想デスクトップについて個別の通常仮想ディスクの作成をサポートしません。代わりに、エンド ユーザーの Windows プロファイルおよびアプリケーション データを App Volumes のユーザー書き込み可能ディスクに格納できます。エンド ユーザーのユーザー書き込み可能ディスクは、エンド ユーザーがログインしたときにインスタント クローン デスクトップに接続されます。さらに、ユーザーがインストールしたアプリケーションを保持するために、ユーザー書き込みディスクを使用できます。
- インスタント クローン デスクトップは一時的な存在のため、インスタント クローンでは Space Efficient ディスク フォーマット (SE スパース) がサポートされていません。
- インスタント クローン デスクトップ プールは Storage vMotion と互換性があります。Composer リンク クローン デスクトップ プールは、Storage vMotion と互換性がありません。

アプリケーション プロビジョニング

Horizon 7 のアプリケーション プロビジョニングでは、従来のアプリケーション プロビジョニング手法の使用、リモート デスクトップではなく公開アプリケーションの提供、VMware ThinApp で作成したアプリケーション パッケージの配布、View Composer またはインスタント クローンの基本イメージの一部としてのアプリケーションの展開、App Volumes を使用したアプリケーションの接続といった複数のオプションを利用できます。

■ RDS ホストによる個々のアプリケーションの展開

エンド ユーザーに対してリモート デスクトップではなく公開アプリケーションを提供することも可能です。小型のモバイル デバイスでは、個々の公開アプリケーションの方が比較的ナビゲートしやすいことがあります。

■ View Composer によるアプリケーション アップデートおよびシステム アップデートのデプロイ

リンク クローン デスクトップ プールは基本イメージを共有しているため、親仮想マシンの更新により、アップデートおよびパッチをすばやくデプロイできます。

■ インスタント クローンでのアプリケーションおよびシステムのアップデートの展開

インスタント クローン デスクトップ プールは基本イメージを共有しているため、親仮想マシンをアップデートすることによってアップデートとパッチをすばやく展開できます。

■ Horizon Administrator での VMware ThinApp アプリケーションの管理

VMware ThinApp™ では、仮想化されたアプリケーション サンドボックスで実行される 1 つのファイルにアプリケーションをパッケージ化できます。この戦略を採用すると、柔軟で競合の発生しないアプリケーション プロビジョニングが可能になります。

■ App Volumes を使用するアプリケーションの展開と管理

VMware App Volumes は、オペレーティング システム上でアプリケーションを仮想化することによって、アプリケーションの管理の代替方法を提供します。この戦略により、アプリケーション、データ ファイル、設定、ミドルウェア、および構成が階層化された個別のコンテナとして動作します。

■ アプリケーション プロビジョニングでの、既存のプロセスまたは VMware Mirage の使用

Horizon 7 では、自社で現在使用しているアプリケーション プロビジョニングのテクニックをそのまま使い続けながら、Mirage も使用できます。ただし、サーバの CPU 使用率およびストレージ I/O の管理と、ユーザーにアプリケーションのインストールを許可するかどうかの決定という 2 つの考慮事項が加わります。

RDS ホストによる個々のアプリケーションの展開

エンド ユーザーに対してリモート デスクトップではなく公開アプリケーションを提供することも可能です。小型のモバイル デバイスでは、個々の公開アプリケーションの方が比較的ナビゲートしやすいことがあります。

エンド ユーザーは、以前にリモート デスクトップへのアクセスに使用したのと同じ Horizon Client を使用して Windows ベースの公開アプリケーションにアクセスできます。表示プロトコルも同じ Blast Extreme または PCoIP 表示プロトコルを使用します。

公開アプリケーションを提供するには、Microsoft リモート デスクトップ セッション (RDS) ホスト上にアプリケーションをインストールします。ファームは 1 個以上の RDS ホストから構成されます。ファーム管理者は、デスクトップ プールの作成と同様の方法でファームからアプリケーション プールを作成します。ファームのサイズ変更の推奨事項については、VMware のナレッジベース (KB) の記事、<http://kb.vmware.com/kb/2150348> を参照してください。

この方法を使用すると、アプリケーションの追加、削除、更新や、アプリケーションに対するユーザー資格の追加または削除、デバイスまたはネットワークから集約型または分散型アプリケーション ファームへのアクセスの提供が簡単になります。

View Composer によるアプリケーション アップデートおよびシステム アップデートのデプロイ

リンク クローン デスクトップ プールは基本イメージを共有しているため、親仮想マシンの更新により、アップデートおよびパッチをすばやくデプロイできます。

再構成機能を使用すると、親仮想マシンを変更し、新しい状態のスナップショットを作成して、イメージの新しいバージョンをすべてのユーザーおよびデスクトップまたはそのサブセットにプッシュすることができます。この機能は次のタスクに使用できます。

- オペレーティング システムとソフトウェアのパッチおよびアップデートの適用
- サービス パックの適用
- アプリケーションの追加
- 仮想デバイスの追加
- 使用可能メモリなど、その他の仮想マシン設定の変更

注： View Composer を使用してリンククローン Microsoft RDS ホストのファームを作成できるため、再構成機能によって、RDS ホストのゲスト OS およびアプリケーションが更新されます。

ユーザー設定やその他のユーザー生成データを格納する View Composer 通常ディスクを作成できます。この通常ディスクは再構成操作による影響を受けません。リンク クローンの削除時に、ユーザー データを保持できます。従業員が退職する際に、別の従業員が離職する従業員のユーザー データにアクセスできます。複数のデスクトップを使用しているユーザーは、1 つのデスクトップにユーザー データを統合できます。

ソフトウェアの追加、削除、または設定の変更をユーザーに許可しない場合は、更新機能を使用してデスクトップをデフォルト値に戻すことができます。この機能によって、時間の経過とともに大きくなる傾向のあるリンク クローンのサイズも削減できます。

インスタント クローンでのアプリケーションおよびシステムのアップデートの展開

インスタント クローン デスクトップ プールは基本イメージを共有しているため、親仮想マシンをアップデートすることによってアップデートとパッチをすばやく展開できます。

イメージ プッシュ機能を使用すると、親仮想マシンを変更し、新しい状態のスナップショットを作成して、イメージの新しいバージョンをすべてのユーザーおよびデスクトップにローリング方式でプッシュすることができます。更新をローリングすると、プールのメンテナンスに関連するダウンタイムを最小限に抑えることができます。ユーザーがインスタント クローン仮想デスクトップをログアウトすると、Horizon 7 はインスタント クローンを削除してイメージの最新バージョンから新しいインスタント クローンを新規に作成し、次のユーザーが新しいクローンにログインする準備が整います。

この機能は次のタスクに使用できます。

- オペレーティング システムとソフトウェアのパッチおよびアップデートの適用
- サービス パックの適用
- アプリケーションの追加
- 仮想デバイスの追加
- 使用可能メモリなど、その他の仮想マシン設定の変更

Horizon Administrator での VMware ThinApp アプリケーションの管理

VMware ThinApp™ では、仮想化されたアプリケーション サンドボックスで実行される 1 つのファイルにアプリケーションをパッケージ化できます。この戦略を採用すると、柔軟で競合の発生しないアプリケーション プロビジョニングが可能になります。

VMware ThinApp はアプリケーションの基盤となるオペレーティング システムおよびそのライブラリとフレームワークから切り離し、アプリケーション パッケージという単一の実行ファイルにバンドルすることにより、アプリケーションの仮想化を実現します。Horizon Administrator を使用して VMware ThinApp アプリケーションをデスクトップおよびプールに配布できます。

重要： デスクトップおよびプールに割り当てて ThinApps を配布する代わりに、ThinApps を Active Directory ユーザーおよびグループに割り当てる場合、VMware Identity Manager を使用できます。

VMware ThinApp で仮想化されたアプリケーションを作成してから、アプリケーションを共有ファイル サーバからストリーミングするかまたは仮想デスクトップにアプリケーションをインストールするかを選択できます。仮想化されたアプリケーションをストリーミング用に構成する場合は、アーキテクチャに関する次の考慮事項に対処する必要があります。

- アプリケーション パッケージが格納されている特定のアプリケーション リポジトリに対する特定のユーザー グループのアクセス
- アプリケーション リポジトリのストレージ構成
- ストリーミングによって生成されるネットワーク トラフィック（アプリケーションのタイプに大きく左右される）

アプリケーションをストリーミングする場合、ユーザーはアプリケーションをデスクトップ ショートカットを使用して起動できます。

仮想デスクトップにインストールされるように ThinApp パッケージ ファイルを割り当てる場合も、アーキテクチャに関して、従来の MSI ベースのソフトウェア プロビジョニングを使用する場合と類似の考慮事項があります。アプリケーションをストリーミングするにしても、リモート デスクトップに ThinApp パッケージをインストールするにしても、どちらの場合でもアプリケーション リポジトリのストレージ構成について考慮する必要があります。

App Volumes を使用するアプリケーションの展開と管理

VMware App Volumes は、オペレーティング システムの上でアプリケーションを仮想化することによって、アプリケーションの管理の代替方法を提供します。この戦略により、アプリケーション、データ ファイル、設定、ミドルウェア、および構成が階層化された個別のコンテナとして動作します。

これらのコンテナは、読み取り専用モードではアプリケーション スタック (AppStack) と呼ばれ、読み取り書き込みモードでは書き込み可能ボリュームと呼ばれます。管理者は App Volumes Manager を使用し、AppStack を作成してアプリケーション資格を割り当てたり、プロビジョニングされた AppStack をシステムまたはユーザーあるいはグループに提供したりできます。App Volumes によって提供されるアプリケーションは、ネイティブでインストールされた場合と同じように操作でき、セッションとデバイスをまたいでユーザーに追従します。管理者はリアルタイムでアプリケーションの更新と置換を実行できます。また、割り当てられたアプリケーションの削除をユーザーのログイン中に即座に実行したり、次のログインあるいは再起動時に実行したりできます。

詳細については、<https://docs.vmware.com/jp/VMware-App-Volumes/index.html> で VMware App Volumes のドキュメントを参照してください。

アプリケーション プロビジョニングでの、既存のプロセスまたは VMware Mirage の使用

Horizon 7 では、自社で現在使用しているアプリケーション プロビジョニングのテクニックをそのまま使い続けながら、Mirage も使用できます。ただし、サーバの CPU 使用率およびストレージ I/O の管理と、ユーザーにアプリケーションのインストールを許可するかどうかの決定という 2 つの考慮事項が加わります。

アプリケーションをほぼ同時刻に多数のリモート デスクトップにプッシュすると、CPU 使用率とストレージ I/O が大きく急上昇することがあります。このピーク ワークロードは、デスクトップのパフォーマンスに顕著な影響を及ぼす場合があります。ベスト プラクティスとしては、アプリケーションの更新がピーク時以外に実行されるようにスケジューリングし、可能であれば各デスクトップの更新時刻をずらしします。また、ストレージ ソリューションがそのようなワークロードをサポートできるように設計されていることを確認する必要があります。

会社がユーザーにアプリケーションのインストールを許可している場合は、現在のポリシーを継続できますが、デスクトップの更新や再構成などの View Composer の機能は活用できません。View Composer では、アプリケーションが仮想化されていないか、あるいはユーザーのプロファイルまたはデータ設定に含まれている場合、そのアプリケーションは View Composer の更新、再構成、または再分散操作が実行されるたびに破棄されます。多くの場合、インストールされるアプリケーションをこのように厳格に制御できることは、利点となります。View Composer デスクトップは既知の優れた構成とほぼ同じに保たれるため、サポートが容易です。

ユーザーの企業が、View Composer を使用してアプリケーションをプロビジョニングする代わりに、独自のアプリケーションをインストールし、リモート デスクトップの有効期間内にこれらのアプリケーションを保持する必要がある場合は、インスタント クローンを App Volumes と一緒に使用できます。または、完全クローン専用デスクトップを作成し、ユーザーがアプリケーションをインストールできるようにしてから、Mirage を使用して、ユーザーがインストールしたアプリケーションを上書きせずにデスクトップの管理と更新を行う方法もあります。

重要： Mirage は、ローカルにインストールされたオフライン デスクトップとそれらのアプリケーションの管理にも使用できます。詳細については、[「Mirage ドキュメント」](#) ページを参照してください。

Active Directory GPO によるユーザーおよびデスクトップの管理

Horizon 7 には、Horizon 7 コンポーネントとリモート デスクトップの管理および構成を集中化するためのグループポリシー管理 ADMX テンプレートが多数含まれています。

これらのテンプレートを Active Directory ディレクトリにインポートしてから、それを使用して次のグループおよびコンポーネントに適用されるポリシーを設定できます。

- ログインするユーザーにかかわらず、すべてのシステム
- ユーザーがどのシステムにログインするかにかかわらず、すべてのユーザー
- 接続サーバの構成
- Horizon Client の構成
- Horizon Agent の構成

GPO を適用すると、プロパティは指定されたコンポーネントのローカル Windows レジストリに格納されます。

GPO を使用して、Horizon Administrator ユーザー インターフェイス (UI) で選択可能なすべてのポリシーを設定できます。GPO を使用すると、UI で選択できないポリシーを設定することもできます。ADMX テンプレートで利用できる設定の詳細なリストと説明については、『Horizon 7 でのリモート デスクトップ機能の構成』を参照してください。

スマート ポリシーの使用

スマート ポリシー を使用して、特定のリモート デスクトップでの USB リダイレクト、仮想印刷、クリップボードリダイレクト、クライアント ドライブ リダイレクト、および PCoIP 表示プロトコル機能の動作を制御することもできます。この機能では User Environment Manager が必要となります。

スマート ポリシー により、特定の条件が満たされる場合にのみ有効になるポリシーを作成できます。たとえば、ユーザーが企業のネットワーク以外からリモート デスクトップに接続している場合はクライアント ドライブ リダイレクト機能を無効にするポリシーを設定できます。

通常、User Environment Manager で構成するリモート デスクトップ機能の Horizon ポリシー設定は、対応するレジストリ キーおよびグループ ポリシー設定よりも優先されます。

リモート デスクトップ展開のためのアーキテクチャ設計の要素と計画のガイドライン

4

一般的な Horizon 7 アーキテクチャ設計では、ポッド戦略を使用します。ポッド定義は、ハードウェア構成、使用されている Horizon 7 および vSphere ソフトウェアのバージョン、その他の環境固有の設計要因によって異なることがあります。

本ドキュメントの例は、企業環境および特殊な要件に適合できる標準的でスケーラブルな設計を説明しています。この章では、Horizon 7 ソリューションの展開に含まれる要素を IT アーキテクトや計画担当者が実務的に理解できるように、メモリ、CPU、ストレージ容量、ネットワーク コンポーネント、およびハードウェアの要件について詳しく説明します。

重要： この章では、次の内容については説明しません。

ホスト型アプリケーションのアーキテクチャ設計	Horizon 7 ポッドは、各ファームに RDS ホストが含まれている Microsoft RDS ホストのファームをサポートします。詳細については、「Horizon 7 での公開されたデスクトップとアプリケーションのセットアップ」を参照してください。RDS ホストの仮想マシンを使用する場合は、 RDS ホスト仮想マシンの構成 も参照してください。
Horizon 7 Agent Direct Connect プラグインのアーキテクチャ設計	このプラグインをリモート仮想マシン デスクトップで実行すると、クライアントは仮想マシンに直接接続できます。PCoIP、HTML Access、RDP、USB リダイレクト、セッション管理などのリモート デスクトップ機能はすべて、ユーザーが View 接続サーバを介して接続したかのように、同じように動作します。詳細については、『Horizon 7 Agent Direct-Connection プラグイン管理』を参照してください。

この章には、次のトピックが含まれています。

- [リモート デスクトップの仮想マシン要件](#)
- [Horizon 7 ESXi ノード](#)
- [特定のタイプのワーカーのデスクトップ プール](#)
- [デスクトップ仮想マシンの構成](#)
- [RDS ホスト仮想マシンの構成](#)
- [vCenter Server および View Composer 仮想マシンの構成](#)
- [Horizon Connection Server の最大接続数と仮想マシン構成](#)
- [vSphere クラスタ](#)
- [ストレージと帯域幅の要件](#)
- [Horizon 7 ビルディング ブロック](#)

- [Horizon 7 ポッド](#)
- [ポッドで複数の vCenter Server を使用する利点](#)

リモート デスクトップの仮想マシン要件

リモート デスクトップの仕様を計画する場合、RAM、CPU、およびディスク領域に関して行う選択は、サーバとストレージ ハードウェアの選択と費用に大きく影響します。

- [就業者のタイプに基づく計画](#)

RAM、CPU、ストレージのサイズ設定など、構成の多くの要素は、仮想デスクトップを使用する就業者のタイプと、インストールする必要があるアプリケーションによって要件が大きく変動します。

- [仮想マシン デスクトップのメモリ要件の見積もり](#)

サーバには PC よりも多くの RAM コストがかかります。RAM のコストは、サーバ ハードウェアの総コストや、必要な合計ストレージ容量の大きな部分を占めるため、デスクトップの展開を計画するには適切なメモリ割り当てを特定することがきわめて重要です。

- [仮想マシン デスクトップの CPU 要件の見積もり](#)

CPU の見積もりを行う場合は、社内の各種就業者の平均 CPU 使用率に関する情報を収集する必要があります。

- [適切なシステム ディスク サイズの選択](#)

ディスク領域を割り当てるときは、オペレーティング システム、アプリケーション、およびユーザーがインストールまたは生成する可能性のあるその他のコンテンツを格納できるだけの領域を割り当てます。通常この容量は、物理 PC に搭載されているディスクのサイズを下回ります。

就業者のタイプに基づく計画

RAM、CPU、ストレージのサイズ設定など、構成の多くの要素は、仮想デスクトップを使用する就業者のタイプと、インストールする必要があるアプリケーションによって要件が大きく変動します。

アーキテクチャの計画では、就業者をいくつかのタイプに分類できます。

タスク ワーカー

タスク ワーカーおよび事務職就業者は、一連の少数のアプリケーションで反復的な作業を行い、通常は据え置き型のコンピュータを使用します。通常それらのアプリケーションは、ナレッジ ワーカーが使用するアプリケーションのように CPU 集約型でもメモリ集約型でもありません。特定のシフトに就業するタスク ワーカーは、各自の仮想デスクトップに同時にログインする可能性があります。タスク ワーカーには、コール センターのアナリスト、小売店の従業員、倉庫作業員などが含まれます。

ナレッジ ワーカー

ナレッジ ワーカーの日常業務では、インターネットへのアクセス、電子メールの使用や、複雑なドキュメント、プレゼンテーション、およびスプレッドシートの作成などを行います。ナレッジ ワーカーには、会計士、セールス マネージャー、マーケティング リサーチ アナリストなどが含まれます。

パワー ユーザー	パワー ユーザーには、アプリケーション開発者や、グラフィックス集約型アプリケーションのユーザーが含まれます。
キオスク ユーザー	これらのユーザーは、公共の場所に置かれているデスクトップを共有する必要があります。キオスク ユーザーの例としては、教室で共有コンピュータを使用する学生、ナースステーションで勤務する看護師、就職の斡旋や求人活動に使用されるコンピュータなどがあります。これらのデスクトップでは、自動ログインが必要になります。認証は、必要に応じて特定のアプリケーションで行うことができます。

仮想マシン デスクトップのメモリ要件の見積もり

サーバには PC よりも多くの RAM コストがかかります。RAM のコストは、サーバ ハードウェアの総コストや、必要な合計ストレージ容量の大きな部分を占めるため、デスクトップの展開を計画する際には適切なメモリ割り当てを特定することがきわめて重要です。

RAM の割り当てが少なすぎると、発生する Windows ページングが多すぎるため、ストレージ I/O に悪影響を及ぼすことがあります。RAM の割り当てが多すぎると、ゲストオペレーティングシステムのページングファイルと各仮想デスクトップのスワップファイルおよびサスペンドファイルが大きくなりすぎるため、ストレージ容量に悪影響を及ぼすことがあります。

パフォーマンスに対する RAM サイズ設定の影響

RAM を割り当てるときは、低すぎる設定を選択するのは避けてください。次の点を考慮します。

- RAM の割り当てが不十分な場合、Windows ページングが過剰に発生することがあり、そのためにパフォーマンスの大幅な低下とストレージ I/O 負荷の増加を招く I/O が生成されるおそれがあります。
- VMware ESXi は、透過的なページ共有やメモリのバルーニングなどの高度なメモリ リソース管理アルゴリズムをサポートしています。そのため、一定のゲスト RAM 割り当てをサポートするために必要な物理 RAM がこれによって大幅に削減できます。たとえば、仮想デスクトップに 2 GB が割り当てられたとしても、物理 RAM の使用量はそのごく一部となります。
- 仮想デスクトップのパフォーマンスは応答時間に大きく左右されるため、ESXi ホスト上では RAM の予約設定を 0 以外の値に設定してください。いくらかの RAM を予約した場合、アイドルでも使用中のデスクトップが完全にディスクにスワップアウトされることはありません。また、ESXi スワップファイルによって消費されるストレージ領域も削減されます。ただし、予約の設定を高くすると、ESXi ホスト上でメモリをオーバーコミットできるかどうかに影響し、VMotion のメンテナンス操作にも影響する場合があります。

ストレージに対する RAM サイズ設定の影響

仮想マシンに割り当てる RAM 容量は、仮想マシンで使用される特定のファイルのサイズに直接関連します。次のリスト内のファイルにアクセスするには、Windows ゲスト OS を使用して Windows のページファイルとハイパネーションファイルを見つけ、さらに ESXi ホストのファイルシステムを使用して ESXi のスワップファイルとサスペンドファイルを見つけます。

Windows のページ ファイル	デフォルトでは、このファイルのサイズはゲスト RAM の 150% に設定されます。デフォルトでは C:\%sys にあるこのファイルは頻繁にアクセスされるため、thin provisioning されたストレージのサイズが大きくなる原因になります。View Composer のリンククローン仮想マシンでは、ページファイルと一時ファイルを、
--------------------------	---

仮想マシンがパワーオフされると削除される個別の仮想ディスクにリダイレクトすることができます。破棄可能なページ ファイルをリダイレクトするとストレージが節約されるため、リンク クローンの増大を抑えるだけでなく、パフォーマンスも向上します。このサイズは Windows 内から調整できますが、これを調整するとアプリケーションのパフォーマンスに悪影響を及ぼすことがあります。

インスタント クローンの場合、ゲスト オペレーティング システムのページング ファイルと一時ファイルはログアウト操作中に自動的に削除されるので、サイズが非常に大きくなることはありません。ユーザーがインスタント クローン デスクトップからログアウトするたびに、Horizon はクローンを削除し、プールが使用可能な最新の OS イメージに基づいて別のインスタント クローンをプロビジョニングしてパワーオンします。

ラップトップ用の Windows ハイパネーション ファイル

このファイルはゲスト RAM の 100% に相当する場合があります。このファイルは Horizon の展開には不要なため、削除しても安全です。

ESXi スワップ ファイル

.vswp 拡張子の付いたこのファイルは、予約した仮想マシンの RAM が 100% 未満の場合に作成されます。スワップ ファイルのサイズは、ゲスト RAM の予約されていない部分に等しくなります。たとえば、ゲスト RAM の 50% が予約済みで、ゲスト RAM が 2GB の場合、ESXi スワップ ファイルは 1GB です。このファイルは、ESXi ホストまたはクラスタ上のローカル データ ストアに格納できます。

ESXi サスペンド ファイル

.vmss 拡張子の付いたこのファイルは、エンド ユーザーがログオフしたときに仮想デスクトップがサスペンドされるようにデスクトップ プールのログオフ ポリシーを設定した場合に作成されます。このファイルのサイズは、ゲスト RAM のサイズに等しくなります。

PCoIP または Blast Extreme 使用時における特定のモニター構成での RAM サイズ設定

システム メモリの他に、仮想マシンでは、ビデオ オーバーヘッドのために ESXi ホストで少量の RAM も必要となります。この VRAM サイズの要件は、ディスプレイの解像度とエンド ユーザーに構成されているモニター数によって異なります。[表 4-1. PCoIP または Blast Extreme のクライアント表示オーバーヘッド](#) は、各種の構成に必要なオーバーヘッド RAM の量を示しています。各列に示したメモリ容量は、他の PCoIP または Blast Extreme 機能に必要なメモリ容量に加算されるものです。

表 4-1. PCoIP または Blast Extreme のクライアント表示オーバーヘッド

ディスプレイ解像度の標準	幅 (ピクセル単位)	高さ (ピクセル単位)	モニター 1 台でのオーバーヘッド	モニター 2 台でのオーバーヘッド	モニター 3 台でのオーバーヘッド	モニター 4 台でのオーバーヘッド
VGA	640	480	1.20 MB	3.20 MB	4.80 MB	5.60 MB
WXGA	1280	800	4.00 MB	12.50 MB	18.75 MB	25.00 MB
1080p	1920	1080	8.00 MB	25.40 MB	38.00 MB	50.60 MB
WQXGA	2560	1600	16.00 MB	60.00 MB	84.80 MB	109.60 MB
UHD (4K)	3840	2160	32.00 MB	78.00 MB	124.00 MB	170.00 MB

システム要件を計算する場合、仮想マシンでは、基本的なシステム RAM に VRAM 値が追加されます。Horizon Administrator でモニターの最大数を指定しディスプレイの解像度を選択すると、オーバーヘッド メモリが自動的に計算され構成されます。

3D レンダリング機能を使用し、Soft3D や vSGA を選択する場合、3D ゲストの VRAM を構成する Horizon Administrator コントロールの別の VRAM 値を使用して再計算できます。また、グラフィック アクセラレーションの Soft3D および vSGA 以外のタイプについては、vSphere Client を使用して VRAM を管理することを選択する場合に、VRAM の正確な量を指定できます。

デフォルトでは、複数のモニター構成がホスト トポロジと一致します。追加のトポロジ スキームに対応するために、2 台以上のモニターについては事前計算される特別なオーバーヘッドがあります。リモート セッションを開始するときにブラック スクリーンが発生する場合、Horizon Administrator で設定されるモニター数とディスプレイ解像度の値を確認し、ホスト システムを一致させるか、Horizon Administrator で [vSphere Client を使用して管理]を選択してから、合計ビデオ メモリ値を最大の 128 MB に設定し、メモリ量を手動で調整します。

特定のワークロードおよびオペレーティング システムでの RAM サイズ設定

必要な RAM 容量は就業者のタイプによって大きく異なるため、多くの企業では社内就業者のさまざまなプールに適した設定を特定するためにパイロット段階を設けています。

32 ビットの Windows 7 以降のデスクトップには 1 GB を割り当て、64 ビットの Windows 7 以降のデスクトップには 2 GB を割り当てることから開始することをお勧めします。3D ワークロード用にハードウェア高速グラフィックス機能のいずれかを使用する場合、VMware では、2 個の仮想 CPU と 4GB の RAM を推奨しています。パイロット運用中は、各種の就業者に使用されるディスク領域のパフォーマンスを監視し、就業者のプールごとに最適な設定が見つかるまで調整を行います。

仮想マシン デスクトップの CPU 要件の見積もり

CPU の見積もりを行う場合は、社内の各種就業者の平均 CPU 使用率に関する情報を収集する必要があります。

CPU 要件は、就業者のタイプによって異なります。パイロット段階で、仮想マシンの Perfmon や ESXi の esxtop、vCenter Server パフォーマンス監視ツールなどのパフォーマンス監視ツールを使用して、これらの就業者グループの平均とピークの両方の CPU 使用率レベルを把握してください。また、次のガイドラインも使用してください。

- ソフトウェア開発者や、高パフォーマンスを必要とするその他のパワー ユーザーの CPU 要件は、ナレッジ ワーカーやタスク ワーカーよりもはるかに高くなる場合があります。CAD アプリケーションの使用、HD ビデオの再生、または 4K ディスプレイ解像度など、計算処理の負荷が高いタスクを実行している 64 ビットの Windows 7 仮想マシンでは、デュアルコアまたはクアッドコアの仮想 CPU が推奨されます。
- シングル仮想 CPU は一般に、その他の場合に推奨されます。

多数の仮想マシンが 1 台のサーバ上で実行されるため、ウィルス対策エージェントなどのすべてのエージェントがまったく同じ時刻にアップデートの有無をチェックすると、CPU 使用率が急上昇するおそれがあります。パフォーマンスの問題を引き起こす可能性のあるエージェントの種類と数を特定し、それらの問題に対処するための戦略を採用します。たとえば、企業では次の戦略が有効な場合があります。

- ソフトウェア管理エージェントを使用して個別の仮想デスクトップごとにソフトウェア アップデートをダウンロードするのではなく、インスタント クローンまたは View Composer のリンク クローンを使用してイメージを更新する。

- ウィルス対策とソフトウェアの更新が、ログインしているユーザーが少ない可能性が高いオフピークの時間に実行されるようにスケジュールする。
- 更新の実行時刻をずらすか、ランダム化する。
- VMware vShield API と互換性があるアンチウイルス製品を使用します。たとえば、この API は VMware vCloud[®] Networking and Security 5.1 以降に統合されました。

まず非公式な最初のサイズ設定のアプローチとして、各仮想マシンには、保証された最小の計算能力として CPU コアの 1/8 ～ 1/10 が必要であると見なしてください。つまり、コアあたり 8 ～ 10 台の仮想マシンを使用するパイロットを計画します。たとえば、コアあたり 8 台の仮想マシンを想定したときに、2 ソケットの 8 コア ESXi ホストがある場合は、パイロット運用中にそのサーバ上で 128 台の仮想マシンをホストできます。この期間中にホスト上の全体的な CPU 使用率を監視し、使用率の急上昇に対する十分な余裕を確保するための安全マージン（たとえば、80 %）をほとんど超えることがないようにしてください。

適切なシステム ディスク サイズの選択

ディスク領域を割り当てるときは、オペレーティング システム、アプリケーション、およびユーザーがインストールまたは生成する可能性のあるその他のコンテンツを格納できるだけの領域を割り当てます。通常この容量は、物理 PC に搭載されているディスクのサイズを下回ります。

データセンターのディスク容量は通常、従来の PC 展開でのデスクトップまたはラップトップのディスク容量よりもギガバイトあたりのコストが高いため、オペレーティング システムのイメージ サイズを最適化してください。イメージ サイズを最適化するために、次の提案が有効な場合があります。

- 不要なファイルを削除します。たとえば、一時インターネット ファイルに割り当てられた領域を削減します。
- インデクサ サービス、デフラグメント サービス、および復元ポイントなどの Windows サービスをオフにします。詳細については、『Horizon 7 での仮想デスクトップのセットアップ』を参照してください。
- 将来の増加を十分見越しながらも、非現実的なほど大きくない仮想ディスク サイズを選択します。
- ユーザーが生成するコンテンツおよびユーザーがインストールするアプリケーションには、中央で管理されるファイル共有、あるいは View Composer の通常ディスク、あるいは App Volumes を使用します。
- vSphere 5.1 以降を使用している場合は、vCenter Server およびリンク クローン デスクトップ プールの領域再利用を有効にします。

仮想マシン デスクトップが vSphere 5.1 以降で使用可能な領域効率的なディスク形式を使用する場合、ゲスト OS 内の無効化されたデータ、または削除されたデータは、自動的にワイプおよび縮小プロセスで再利用されます。

必要なストレージ容量については、各仮想デスクトップで使用される次のファイルを考慮に入れる必要があります。

- ESXi サスペンド ファイルは、仮想マシンに割り当てられた RAM 容量に等しいサイズになります。
- デフォルトでは、Windows のページ ファイルは RAM の 150% に相当します。
- ログ ファイルは、各仮想マシンのために 100MB を使用できます。

- 仮想ディスク、つまり .vmdk ファイルには、オペレーティング システム、アプリケーション、将来のアプリケーション アップデートおよびソフトウェア アップデートを格納する必要があります。ローカル ユーザー データおよびユーザーがインストールするアプリケーションをファイル共有ではなく仮想デスクトップ上に配置する場合は、それらも仮想ディスクに格納する必要があります。

View Composer を使用することにより、時間の経過にともない .vmdk ファイルが大きくなりますが、View Composer の更新操作をスケジュールし、仮想マシン デスクトップ プールに対してストレージのオーバーコミット ポリシーを設定し、Windows のページ ファイルと一時ファイルを別個の読み取り専用ディスクにリダイレクトすることにより、サイズの増加量を抑制できます。

インスタント クローンを使用する場合は、ログイン セッション内で .vmdk ファイルのサイズが次第に大きくなります。ユーザーがログアウトするとインスタント クローン デスクトップは自動的に削除され、新しいインスタント クローンが作成されて次のユーザーがログインする準備が整います。このプロセスによってデスクトップは事実上更新され、元のサイズに戻ります。

ユーザーのディスク領域不足を確実に防止するため、この見積もりに 15% を加えてもかまいません。

Horizon 7 ESXi ノード

ノードとは、Horizon 7 の展開で仮想マシン デスクトップをホストする 1 台の VMware ESXi ホストです。

ESXi ホスト上でホストされるデスクトップの数を示す統合率を最大にすると、Horizon 7 のコスト効率が最大限に高まります。サーバの選択には多くの要因が影響しますが、厳密に取得価格に関して最適化する場合、処理能力とメモリが適切にバランスされたサーバ構成を見つける必要があります。

環境およびハードウェア構成のための適切な統合率を特定するには、パイロット運用などの実際の、実環境の状況の下でパフォーマンスを測定する方法に代わるものではありません。統合率は、使用パターンや環境要因によって大幅に異なる場合があります。次のガイドラインを使用してください。

- 一般的なフレームワークとして、CPU コアあたり 8 から 10 の仮想デスクトップ数の点から見た計算容量を考慮します。各仮想マシンの CPU 要件の計算については、[仮想マシン デスクトップの CPU 要件の見積もり](#)を参照してください。
- 仮想デスクトップの RAM、ホストの RAM、およびオーバーコミットメント率の点から見たメモリ容量を考慮します。CPU コアあたりの仮想デスクトップ数を 8 ～ 10 台にすることができますが、仮想デスクトップに 1 GB 以上の RAM がある場合は、物理 RAM の要件も慎重に考慮する必要があります。仮想マシンごとに必要な RAM 容量の計算については、[仮想マシン デスクトップのメモリ要件の見積もり](#)を参照してください。

物理 RAM のコストは線形ではないこと、および場合によっては DIMM チップを使用しない小型のサーバを多数購入した方がコスト効率が良いことに注意してください。別の場合には、ラック密度、ストレージの接続性、管理性、およびその他の考慮事項により、展開のサーバ数を最小限に抑えた方が適切な選択となることもあります。

- Horizon 7 では、View Storage Accelerator 機能はデフォルトでオンになっており、これによって ESXi 5.5 Update 2 以降のホストは、一般的な仮想マシンのディスク データをキャッシュできます。View Storage Accelerator を使用することで、多数の起動とウイルス対策スキャンの I/O ストームを管理する際のパフォーマンスが向上し、追加のストレージ I/O バンド幅の必要性が少なくなります。この機能では、ESXi ホスト毎に 1 GB の RAM が必要です。

- 最後に、クラスタの要件と、フェイルオーバーの要件がある場合はそれを考慮します。詳細については、[高可用性の要件の特定](#)を参照してください。

vSphere での ESXi ホストの仕様については、『VMware vSphere 構成の上限』ドキュメントを参照してください。

特定のタイプのワーカーのデスクトップ プール

Horizon 7 は、さまざまなユースケースに必要なストレージを節約したり、処理能力の量を削減したりするのに役立つ多くの機能を提供します。これらの機能の多くは、プールの設定として使用できます。

考慮すべき最も基本的な問題は、特定のタイプのユーザーにとって、ステートフル デスクトップ イメージとステートレス デスクトップ イメージのどちらが必要かという点です。ステートフル デスクトップ イメージが必要なユーザーは、保存、保守、およびバックアップする必要のあるデータをオペレーティング システム イメージ自体に保持しています。たとえば、これらのユーザーは独自のアプリケーションをいくつかインストールするか、またはファイル サーバ上やアプリケーション データベース内などの、仮想マシン自体の外部には保存できないデータを保持しています。

ステートレス デスクトップ イメージ 読み取り専用デスクトップとしても知られるステートレス アーキテクチャには、より容易なサポート、より低いストレージ コストなどの多くの利点があります。その他の利点として、仮想マシンをバックアップする必要性が低いことや、より容易で、より低価格なディザスタ リカバリおよびビジネス継続性オプションがあります。

ステートフル デスクトップ イメージ これらのデスクトップは通常のデスクトップとしても知られ、従来のイメージ管理技術が必要とする場合があります。ステートフル イメージでは、特定のストレージ システム テクノロジーとの組み合わせによりストレージ コストが低くなる場合があります。バックアップ、ディザスタ リカバリ、およびビジネス継続性のための戦略を考慮する場合は、VMware Site Recovery Manager などのバックアップ/リカバリ テクノロジーが重要です。

Horizon 7 でステートレス デスクトップ イメージを作成する方法は 2 つあります。

- フローティング割り当てプールまたはインスタント クローン仮想マシン専用の割り当てプールを作成できます。フォルダ リダイレクトと移動プロファイルをオプションで使用して、ユーザー データを格納することも可能です。
- View Composer を使用して、リンク クローン仮想マシンのフローティングまたは専用割り当てプールを作成できます。フォルダ リダイレクトと移動プロファイルを使用して、ユーザー データを格納したり、ユーザー データを保持する永続ディスクを設定できます。

Horizon 7 でステートフル デスクトップ イメージを作成する方法はいくつかあります。

- 完全クローンまたはフル仮想マシンを作成できます。一部のストレージ ベンダーは、完全クローン向けのコスト効率の良いストレージ ソリューションを提供しています。これらのベンダーは多くの場合、独自のベスト プラクティスおよびプロビジョニング ユーティリティを備えています。これらのベンダーのいずれかを使用した場合、手動の専用割り当てプールの作成が必要になることがあります。
- インスタント クローンまたはリンク クローンの仮想マシンのプールを作成し、App Volumes ユーザー書き込み可能ボリュームを使用して、ユーザー データとユーザーがインストールしたアプリケーションに接続できます。

ステートレス デスクトップとステートフル デスクトップのどちらを使用するかは、ワーカーのタイプによって異なります。

■ タスク ワーカー用プール

タスク ワーカー用のステートレス デスクトップ イメージを標準化すると、常にイメージをサポートの簡単な使い慣れた構成にすることができるため、就業者はどれでも使用可能なデスクトップにログインできるようになります。

■ ナレッジ ワーカーとパワー ユーザー用プール

ナレッジ ワーカーは、複雑なドキュメントを作成し、それらをデスクトップ上に保持する必要があります。パワー ユーザーは、独自のアプリケーションをインストールし、それらを保持する必要があります。保持する必要のある個人データの性質および量に応じて、デスクトップはステートフルまたはステートレスのどちらかになります。

■ キオスク ユーザー用プール

キオスク ユーザーには、航空会社のチェックイン ステーションにいる顧客、教室または図書館にいる学生、医療データ入力ワークステーションにいる医療スタッフ、セルフサービス地点にいる顧客などが含まれます。ユーザーはクライアント デバイスまたはリモート デスクトップを使用するためにログインする必要がないため、これらのデスクトップ プールを使用する資格はユーザーではなく、クライアント デバイスに関連付けられたアカウントに付与されます。ただし引き続き、ユーザーに、一部のアプリケーションでは認証情報を入力するよう求めることもできます。

タスク ワーカー用プール

タスク ワーカー用のステートレス デスクトップ イメージを標準化すると、常にイメージをサポートの簡単な使い慣れた構成にすることができるため、就業者はどれでも使用可能なデスクトップにログインできるようになります。

タスク ワーカーは一連の少数のアプリケーションで反復的な作業を行うため、ステートレス デスクトップ イメージを作成することで、ストレージ容量を節約し、処理要件を抑えることができます。

インスタント クローン デスクトップ プールには、次のプール設定を使用します。

- インスタント クローン プールについては、リソース使用率を最適化するために、オン デマンドのプロビジョニングを使用して、使用率に基づいてプールを拡大または縮小します。ログイン レートを満たすため、十分なスベア デスクトップを指定するようにします。
- インスタント クローン デスクトップ プールについては、ユーザーがログアウトすると Horizon 7 は自動的にインスタント クローンを削除します。新しいインスタント クローンが新規に作成され、次のユーザーがログインする準備が整います。このように、デスクトップはログアウトのたびに事実上更新されます。

View Composer リンク クローン デスクトップ プールには、次のプール設定を使用します。

- View Composer デスクトップ プールについては、ユーザーがログアウトするときどのようなアクションをとるか（必要な場合）を決定します。ディスクは、時間の経過とともに大きくなります。ユーザーがログオフするときにデスクトップを元の状態に更新すると、ディスク領域を節約できます。また、スケジュールを設定することでデスクトップを定期的に更新できます。たとえば、デスクトップが毎日、毎週、または毎月更新されるようにスケジュールを設定できます。

- 該当する場合、および View Composer のリンククローン プールを使用している場合は、ローカル ESXi データ ストアにデスクトップを格納することを検討します。この方法には、安価なハードウェア、仮想マシンの迅速なプロビジョニング、高性能の電力操作、およびシンプルな管理などの利点があります。制限事項のリストについては、[フローティング、ステートレス デスクトップのためのローカル データストア](#)を参照してください。ローカル データ ストアでは、インスタント クローン プールはサポートされません。

注： その他のタイプのストレージ オプションの詳細については、[ストレージ要件の軽減と管理](#)を参照してください。

- 個人設定管理機能を使用すると、Windows のユーザー プロファイルと同じように、ユーザーは常に好みのデスクトップの外観とアプリケーションの設定を使用できます。ログオフ時に更新または削除するように設定されているデスクトップがない場合には、ログオフ時に個人設定を削除するように構成できます。

重要： 個人設定管理は、セッション間で設定を保持したいユーザー向けのフローティング割り当てプールの実装を促進します。以前は、フローティング割り当てデスクトップの制限の一つは、エンド ユーザーがログオフすると、そのユーザーのすべての設定およびリモート デスクトップに保存したデータが失われることでした。

エンド ユーザーがログオンするたびに、デスクトップの背景はデフォルトの壁紙に設定され、ユーザーは各アプリケーションの環境設定を再度構成する必要がありました。個人設定管理を使用すると、エンド ユーザーはフローティング割り当てデスクトップのセッションと専用割り当てデスクトップのセッションの区別が付きません。

すべてのデスクトップ プールには、次の一般的なプール設定を使用します。

- 自動プールを作成して、そのプールの作成時にデスクトップが作成されるようにするか、プールの使用量に基づいてオン デマンドでデスクトップが生成されるようにすることができます。
- フローティング割り当てを使用して、使用可能なすべてのデスクトップにユーザーがログインできるようにします。全員が同時にログインする必要がない場合、この設定を行うことで、必要なデスクトップの数を削減できます。
- インスタントクローンまたは View Composer リンククローン デスクトップを作成することで、デスクトップが同じ基本イメージを共有し、データセンターで使用するストレージ容量をフル仮想マシンより少なく済むようにします。

ナレッジ ワーカーとパワー ユーザー用プール

ナレッジ ワーカーは、複雑なドキュメントを作成し、それらをデスクトップ上に保持する必要があります。パワー ユーザーは、独自のアプリケーションをインストールし、それらを保持する必要があります。保持する必要のある個人データの性質および量に応じて、デスクトップはステートフルまたはステートレスのどちらかになります。

一時的な使用を除き、ユーザーがインストールするアプリケーションを必要としないナレッジ ワーカーの場合は、ステートレス デスクトップ イメージを作成し、すべての個人データを、ファイル サーバ上やアプリケーション データベース内などの仮想マシンの外部に保存することができます。その他のナレッジ ワーカーおよびパワー ユーザーの場合は、ステートフル デスクトップ イメージを作成できます。

インスタント クローン デスクトップ プールには、次のプール設定を使用します。

- インスタント クローン デスクトップを使用する場合は、ファイル共有、移動プロファイルまたは他のプロファイル管理ソリューションを実装します。

View Composer リンク クローン デスクトップ プールには、次のプール設定を使用します。

- vSphere の仮想デスクトップで View Composer を使用する場合、vCenter Server およびデスクトップ プール用の領域再利用機能を有効にします。領域再利用機能を使用すれば、ゲスト OS 内の無効または削除されたデータは自動的にワイプおよび縮小プロセスで再利用されます。
- View Composer のリンク クローン デスクトップを使用する場合、個人設定管理、移動プロファイル、または別のプロファイル管理ソリューションを実装します。また、ユーザー プロファイルのローカル コピーを通常ディスクに保持しながら、リンククローン OS ディスクを更新および再構成できるように、通常ディスクを構成できます。
- 個人設定管理機能を使用すると、Windows のユーザー プロファイルと同じように、ユーザーは常に好みのデスクトップの外観とアプリケーションの設定を使用できます。

すべてのデスクトップ プールには、次の一般的なプール設定を使用します。

- 経理担当者、セールスマネージャ、市場調査アナリストなど、一部のパワー ユーザーおよびナレッジ ワーカーは毎回同じデスクトップにログインする必要がある場合があります。これらのユーザーについては、専用割り当てプールを作成します。
- 最初に、各デスクトップでディスクが初期の操作に必要とするストレージ容量のみが使用されように、vStorage thin provisioning を使用します。
- 独自のアプリケーションをインストールする（これにより、オペレーティング システムのディスクにデータが追加されます）必要のあるパワー ユーザーおよびナレッジ ワーカーの場合は、2 つのオプションがあります。1 つは、フル仮想マシン デスクトップを作成するオプションです。

他方のオプションは、リンク クローンまたはインスタント クローンのプールを作成し、App Volumes を使用して、ユーザーがインストールしたアプリケーションおよびユーザー データをログインをまたいで保持する方法です。

- ナレッジ ワーカーが、一時的な使用を除き、ユーザーがインストールするアプリケーションを必要としない場合は、View Composer リンククローン デスクトップまたはインスタント クローン デスクトップを作成できます。デスクトップ イメージは同じ基本イメージを共有し、フル仮想マシンより少ないストレージ容量を使用します。

キオスク ユーザー用プール

キオスク ユーザーには、航空会社のチェックイン ステーションにいる顧客、教室または図書館にいる学生、医療データ入力ワークステーションにいる医療スタッフ、セルフサービス地点にいる顧客などが含まれます。ユーザーはクライアント デバイスまたはリモート デスクトップを使用するためにログインする必要がないため、これらのデスクトップ プールを使用する資格はユーザーではなく、クライアント デバイスに関連付けられたアカウントに付与されます。ただし引き続き、ユーザーに、一部のアプリケーションでは認証情報を入力するよう求めることもできます。

ユーザーデータはオペレーティング システムのディスクに保存する必要がないため、キオスク モードで動作するように設定されている仮想マシン デスクトップはステートレス デスクトップ イメージを使用します。キオスク モードのデスクトップは、シン クライアント デバイスまたはロックダウンされた PC で使用されます。デスクトップ アプリケーションに安全なトランザクションのための認証メカニズムが実装されていること、物理ネットワークが改ざんやスヌーピングに対して安全であること、およびネットワークに接続されているすべてのデバイスが信頼できることを確認する必要があります。

ベスト プラクティスとして、専用の接続サーバ インスタンスを使用してキオスク モードのクライアントを処理し、Active Directory 内にこれらのクライアントのアカウントのための専用の組織単位とグループを作成してください。この方法により、これらのシステムが不正な侵入から保護されるだけでなく、クライアントの構成および管理が容易になります。

キオスク モードを設定するには、vdmadmin コマンドライン インターフェイスを使用し、『Horizon 7 の管理』ドキュメントのキオスク モードに関するトピックに記載されているいくつかの手順を実行する必要があります。

このセットアップの一部として、次のインスタント クローン デスクトップ プールを設定を使用できます。

- インスタント クローン デスクトップ プールを使用している場合は、ユーザーがログアウトすると Horizon 7 は自動的にインスタント クローンを削除します。新しいインスタント クローンが新規に作成され、次のユーザーがログインする準備が整います。このように、デスクトップはログアウトのたびに事実上更新されます。

このセットアップの一部として、次の View Composer リンク クローン デスクトップ プールを設定を使用できます。

- View Composer のリンククローン デスクトップを使用している場合は、デスクトップが頻繁に更新されるように、更新ポリシーを設定します。たとえば、ユーザーのログアウトのたびに毎回更新されるように設定します。
- 可能な場合には、ローカルの ESXi データストアにデスクトップを格納することを検証してください。この方法には、安価なハードウェア、仮想マシンの迅速なプロビジョニング、高性能の電力操作、およびシンプルな管理などの利点があります。制限事項のリストについては、[フローティング、ステートレス デスクトップのためのローカル データストア](#)を参照してください。ローカル データ ストアでは、インスタント クローン プールはサポートされません。

注： その他のタイプのストレージ オプションの詳細については、[ストレージ要件の軽減と管理](#)を参照してください。

このセットアップの一部として、すべてのデスクトップ プールの次の一般的な設定を使用できます。

- 自動プールを作成して、そのプールの作成時にデスクトップが作成されるようにするか、プールの使用量に基づいてオン デマンドでデスクトップが生成されるようにすることができます。
- ユーザーがプール内の任意の使用可能なデスクトップにアクセスできるように、流動割り当てを使用します。
- インスタントクローンまたは View Composer リンククローン デスクトップを作成することで、デスクトップが同じ基本イメージを共有し、データセンターで使用するストレージ容量をフル仮想マシンより少なく済むようにします。
- デスクトップに対して最も近いプリンタが使用されるように、ロケーションベースの印刷を構成するための Active Directory GPO（グループ ポリシー オブジェクト）を使用します。グループ ポリシー管理 (ADMX) テンプレートで利用できる設定の詳細なリストと説明については、『Horizon 7 でのリモート デスクトップ機能の構成』を参照してください。
- GPO またはスマート ポリシーを使用して、デスクトップが起動されたとき、またはクライアント コンピュータに USB デバイスが挿入されたときに、ローカル USB デバイスがデスクトップに接続されるかどうかを制御します。

デスクトップ仮想マシンの構成

メモリ、仮想プロセッサ数、ディスク容量などの項目の設定例は Horizon 7 に固有のものです。

必要なシステム ディスク容量は、基本イメージに必要なアプリケーションの数に依存します。当社では、8GB のディスク容量を含むセットアップを検証しています。アプリケーションには、Microsoft Word、Excel、PowerPoint、Adobe Reader、Internet Explorer、McAfee Antivirus、および PKZIP が含まれます。

ユーザー データに必要なディスク容量は、エンド ユーザーの役割と、データ ストレージに関する組織のポリシーによって変わります。View Composer を使用する場合、このデータは通常のディスクに保管されます。

次の表に示すガイドラインは、標準の Windows 7 以降の仮想マシン デスクトップ用です。

表 4-2. Windows 7 または Windows 8 のデスクトップ仮想マシンの例

アイテム	例
オペレーティング システム	32 ビットまたは 64 ビット Windows 7 以降（最新のサービス パックを適用）
RAM	1GB（3D レンダリング用のハードウェア アクセラレータによるグラフィックスがある場合は 4GB）
仮想 CPU	1(64 ビットシステムの場合、または高品位または全画面表示ビデオの再生が必要な場合は 2)
システム ディスク容量	24GB（標準よりやや少なめ）
ユーザー データの容量（通常のディスクとして）	5GB（出発点）
仮想 SCSI アダプタのタイプ	LSI Logic SAS（デフォルト）
仮想ネットワーク アダプタ	VMXNET 3

RDS ホスト仮想マシンの構成

RDS (Remote Desktop Services) ホストを使用して、公開アプリケーションとセッションベースのリモート デスクトップをエンドユーザーに提供します。

RDS ホストには物理マシンまたは仮想マシンを使用できます。この例で、以下の表に示した仕様で仮想マシンを使用します。この仮想マシンをホストする ESXi ホストは、物理サーバの障害から保護するための VMware HA クラスタに含めることができます。

表 4-3. RDS ホスト仮想マシンの例

アイテム	例
オペレーティング システム	64 ビット Windows Server 2008 R2 または Windows Server 2012 R2
RAM	24GB
仮想 CPU	4
システム ディスク容量	40 GB
仮想 SCSI アダプタのタイプ	LSI Logic SAS（Windows Server 2008 のデフォルト）
仮想ネットワーク アダプタ	VMXNET 3

表 4-3. RDS ホスト仮想マシンの例（続き）

アイテム	例
1 つの NIC	1 ギガビット
クライアント接続の合計の最大数（セッション ベースのリモート デスクトップ接続と公開アプリケーション接続を含む）	50

注： リソース仕様の最後の方に RDS ホストを構成すると、デフォルトのインストールではなく、すべての機能を使用する場合に、リソースの制約が発生する可能性があります。

RDS ホスト構成とテスト済みワークロードの詳細については、VMware Horizon 6 リファレンス アーキテクチャ ホワイト ペーパー（<http://www.vmware.com/files/pdf/techpaper/VMware-Reference-Architecture-Horizon-6-View-Mirage-Workspace.pdf>）を参照してください。

vCenter Server および View Composer 仮想マシンの構成

vCenter Server と View Composer は、同じ仮想マシンまたは別々のサーバにインストールできます。これらのサーバでは、デスクトップ仮想マシンよりも非常に多くのメモリと処理能力が必要となります。

VMware は、View Composer で vSphere 5.1 以降を使用してプール毎に 2,000 のデスクトップを作成およびロビジョニングするテストを行いました。さらに、VMware は一度に 2,000 のデスクトップで View Composer による再構成操作を行うテストも行いました。これらのテストでは、個別の仮想マシンに vCenter Server および View Composer がインストールされました。

デスクトップ プール サイズは次の要素によって制限されます。

- 各デスクトップ プールに含むことのできる vSphere クラスタは 1 つだけです。
- 一部のセットアップでは、クラスタに最大 32 ホストまで含めることができます。他のセットアップでは、クラスタは 8 ホストに限定されます。詳細については、[vSphere クラスタ](#)を参照してください。
- 各 CPU コアは 8 ～ 10 の仮想デスクトップを計算する能力があります。
- サブネットに使用できる IP アドレス数によってプール内のデスクトップ数が制限されます。たとえば、プールのサブネットに使用できる IP アドレスが 256 個しかない設定のネットワークの場合、プール サイズは 256 デスクトップに制限されます。ただし、プールの仮想マシンに割り当てる IP アドレスの数を大幅に拡張するために、複数のネットワーク ラベルを構成できます。

vCenter Server と View Composer を物理マシンにインストールすることもできますが、この例で以下の表に示す仕様を満たす個別の仮想マシンを使用します。これらの仮想マシンをホストする ESXi ホストは、VMware HA クラスタに含めて物理サーバの障害に備えることができます。

この例は、vSphere 5.1 以降および vCenter Server 5.1 以降で Horizon 7 を使用していることを想定しています。

重要： また、View Composer および vCenter Server が個別の仮想マシンにインストールされていることも想定しています。

表 4-4. vCenter Server 仮想マシンの例

アイテム	10,000 台のデスクトップを管理する vCenter Server の例	2,000 台のデスクトップを管理する vCenter Server の例
オペレーティング システム	64 ビット Windows Server 2008 R2 Enterprise	64 ビット Windows Server 2008 R2 Enterprise
RAM	48 GB	10 ～ 24 GB (vSphere バージョンによって異なります)
仮想 CPU	16	2 ～ 8 (vSphere バージョンによって異なります)
システム ディスク容量	180 GB	40 GB
仮想 SCSI アダプタのタイプ	LSI Logic SAS (Windows Server 2008 のデフォルト)	LSI Logic SAS (Windows Server 2008 のデフォルト)
仮想ネットワーク アダプタ	E1000 (デフォルト)	VMXNET 3 (ただし、E1000 のデフォルトで問題はありせん)
最大の同時 vCenter プロビジョニング操作	20	20
最大の同時電源操作	50	50

表 4-5. View Composer 仮想マシンの例

アイテム	10,000 のデスクトップを管理する View Composer の例	2,000 のデスクトップを管理する View Composer の例
オペレーティング システム	64 ビット Windows Server 2008 R2 Enterprise	64 ビット Windows Server 2008 R2 Enterprise
RAM	10 GB 以上 (vSphere バージョンによって異なります)	4 ～ 10 GB (vSphere バージョンによって異なります)
仮想 CPU	4 以上 (vSphere バージョンによって異なります)	2 ～ 4 (vSphere バージョンによって異なります)
システム ディスク容量	50 GB	40 GB
仮想 SCSI アダプタのタイプ	LSI Logic SAS (Windows Server 2008 のデフォルト)	LSI Logic SAS (Windows Server 2008 のデフォルト)
仮想ネットワーク アダプタ	VMXNET 3	VMXNET 3
View Composer の最大プール サイズ	2,000 デスクトップ	1,000 デスクトップ
最大同時 View Composer メンテナンス操作数	12	12
最大同時 View Composer プロビジョニング操作数	8	8

重要： VMware では、vCenter Server とデータベースを別の仮想マシン上に配置することを推奨しています。

Horizon Connection Server の最大接続数と仮想マシン構成

Horizon Connection Server をインストールすると、Horizon Administrator ユーザー インターフェイスもインストールされます。

Connection Server の構成

Connection Server は物理マシンにインストールできますが、この例では、「Connection Server の仮想マシンの例」に挙げている仕様の仮想マシンを使用します。この仮想マシンをホストする ESXi ホストは、物理サーバの障害から保護するための VMware HA クラスタに含めることができます。

表 4-6. Connection Server の仮想マシンの例

アイテム	例
オペレーティング システム	サポート対象のオペレーティング システムについては、Horizon 7 のインストールを参照してください。
RAM	10 GB
仮想 CPU	4
システム ディスク容量	70 GB
仮想 SCSI アダプタのタイプ	LSI Logic SAS (Windows Server 2008 のデフォルト)
仮想ネットワーク アダプタ	VMXNET 3
ネットワーク アダプタ	1Gbps NIC

Connection Server のクラスタ設計に関する考慮事項

ロード バランシングと高可用性をサポートするために、複数の複製された Connection Server インスタンスをグループで展開できます。複製されたインスタンスのグループは、LAN に接続された単一データセンター環境内のクラスタリングをサポートするように設計されています。

重要： データセンターをまたいで Horizon を展開する場合に、複製された Connection Server インスタンスのグループを WAN、MAN (metropolitan area network)、または他の LAN 以外をまたいで使用するには、クラウド ポッド アーキテクチャ 機能を使用する必要があります。詳細については、Horizon 7 でのクラウド ポッド アーキテクチャの管理を参照してください。

Connection Server の最大接続数

「リモート デスクトップ接続」では、Horizon 7 の導入で対応できる同時接続数に関するテスト済みの上限を示します。

表 4-7. リモート デスクトップ接続

展開あたりの Connection Server 数	接続のタイプ	同時接続の最大数
1 つの Connection Server	直接接続、RDP、Blast Extreme、または PCoIP	4,000 (テスト済み構成)
1 つの Connection Server	トンネル接続、RD	2,000 (デフォルト構成) 4,000 (テスト済み構成)
1 つの Connection Server	PCoIP Secure Gateway 接続	2,000 (デフォルト構成) 4,000 (テスト済み構成)
1 つの Connection Server	Blast Secure Gateway 接続	2,000 (デフォルト構成) 4,000 (テスト済み構成)
1 つの Connection Server	物理 PC への 統合アクセス	2,000 (テスト済み構成)

表 4-7. リモート デスクトップ接続 (続き)

展開あたりの Connection Server 数	接続のタイプ	同時接続の最大数
1 つの Connection Server	RDS ホストへの 統合アクセス	2,000 (テスト済み構成)
7 つの Connection Server	直接接続、RDP、Blast Extreme、または PCoIP	RDS ホスト <ul style="list-style-type: none"> ■ 10,000 (デフォルト構成) ■ 20,000 (テスト済み構成) 仮想デスクトップ <ul style="list-style-type: none"> ■ 12,000 (テスト済み構成)

注： テスト済み構成は完全対応になります。単一の Connection Server で、トンネル接続、PCoIP Secure Gateway 接続および Blast Secure Gateway 接続を使用し、テスト済み構成の最大同時接続数 4,000 を得るには、Connection Server をインストールする仮想マシンで `locked.properties` ファイルを作成します (`C:\Program Files\VMware\VMware View\Server\sslgateway\conf`)。次に、`locked.properties` ファイルで `maxConnections=4000` を設定し、Connection Server を再起動します。Unified Access Gateway で現在サポートしているセッション数は 2,000 です。したがって、20,000 セッションのテストには、14 台の Unified Access Gateway アプライアンスが使用されました。

企業ネットワークの外部からの PCoIP 接続にセキュリティ サーバまたは Unified Access Gateway アプライアンスを使用する場合は、PCoIP Secure Gateway 接続が必要です。企業ネットワークの外部からの Blast Extreme または HTML Access 接続にセキュリティ サーバや Unified Access Gateway アプライアンスを使用する場合は、Blast Secure Gateway 接続が必要です。企業ネットワークの外部からの RDP 接続、および PCoIP または Blast Secure Gateway 接続を使用する USB リダイレクトとマルチメディア リダイレクト (MMR) のアクセラレーションにセキュリティ サーバや Unified Access Gateway アプライアンスを使用する場合は、トンネル接続が必要です。複数のセキュリティ サーバを単一の Connection Server インスタンスとペアにすることができます。

1 台のセキュリティ サーバまたは Unified Access Gateway アプライアンスでは最大 2,000 の同時接続がサポートされます。Connection Server インスタンスごとに 1 台のセキュリティ サーバを使用することもできますが (2,000 セッション)、その代わりに、2 または 4 を使用することもできます。セキュリティ サーバを監視してみると、2,000 人のユーザーのアクティビティが大きすぎる場合があります。メモリと CPU 使用率の必要量からすると、Connection Server インスタンスあたりで、もっと多くのセキュリティ サーバを追加し、負荷を分散させることが必要である場合があります。たとえば、各サーバが 1,000 の接続を処理する、2 台のセキュリティ サーバを使用したり、または、各サーバが 500 接続を処理する、4 台のセキュリティ サーバを使用したりする場合があります。Connection Server インスタンスに対するセキュリティ サーバの割合は、特定の環境の要件に依存します。

Unified Access Gateway アプライアンス 1 台あたりの接続数は、セキュリティ サーバの接続数と同程度になります。Unified Access Gateway アプライアンスの詳細については、Unified Access Gateway の導入および設定を参照してください。

注： この例で、適切に構成された 5 つの Connection Server インスタンスで 20,000 の接続を処理できるものの、可用性を計画するために表では 7 という数字が示されています。これにより、企業のネットワークの内部と外部の両方からの接続に対応することができます。

たとえば、20,000 ユーザーがいて、そのうちの 16,000 ユーザーが企業ネットワーク内にいる場合は、企業のネットワーク内部に 5 つの Connection Server インスタンスが必要です。その場合、インスタンスのうち 1 つが使用不可になっても、残りの 4 つのインスタンスが負荷を処理できます。同様に、企業のネットワーク外部から 4,000 の接続がある場合、2 つの Connection Server インスタンスを使用すれば、1 つのインスタンスが使用不可になっても、負荷を処理できるインスタンスが 1 つ残っています。

これらの数値は、外部接続がゲートウェイ経由で行われることを前提としています。この例では、外部接続を処理するそれぞれの Connection Server インスタンスが 3 台のセキュリティ サーバとペアリングされ、1 台が使用できなくなった場合、残り 2 台のセキュリティ サーバで負荷が処理されます。セキュリティ サーバの代わりに Unified Access Gateway アプライアンスを使用する場合は、両方の Connection Server インスタンス間でロード バランシングを行うため、合計で 3 台が必要になります。1 台が使用できなくなった場合、残りの 2 台のアプライアンスが負荷を処理します。

いずれの場合も、Connection Server またはゲートウェイが使用不能になった場合、ユーザーは再接続する必要があります。

Unified Access Gateway と Horizon 7 を使用する場合のハードウェア要件

Horizon 7 で使用する際に最大数の接続をサポートするように、Unified Access Gateway アプライアンスには 2 つの vCPU と 4GB の RAM を使用することをお勧めします。

表 4-8. Unified Access Gateway のハードウェア要件

アイテム	例
オペレーティング システム	OVA
RAM	4 GB
仮想 CPU	2
システム ディスク容量	20 GB (デフォルトのログ レベルを変更する場合は、容量を追加する必要があります)
仮想 SCSI アダプタのタイプ	LSI Logic Parallel (OVA のデフォルト)
仮想ネットワーク アダプタ	VMXNET 3
ネットワーク アダプタ	1Gbps NIC
ネットワークのマッピング	単一 NIC のオプション

vSphere クラスタ

Horizon 7 の展開では、VMware HA クラスタを使用して物理サーバの障害に備えることができます。セットアップによりますが、クラスタにノードを最大 32 個まで含めることができます。

vSphere および vCenter Server は、仮想マシン デスクトップをホストするサーバのクラスタを管理するための豊富な機能セットを備えています。仮想マシン デスクトップ プールはそれぞれ vCenter Server リソース プールに関連付ける必要があるため、クラスタの構成も重要です。したがって、プールあたりのデスクトップの最大数は、実行を予定するサーバおよび仮想マシンのクラスタあたりの数に関連します。

非常に大規模な Horizon 7 環境では、クラスタ オブジェクトを 1 つのデータセンター オブジェクトにつき 1 つだけにすると、vCenter Server のパフォーマンスと応答性を向上させることができます。これはデフォルトの動作ではありません。デフォルトでは、vCenter Server によって、同じデータセンター オブジェクト内に新規クラスタが作成されます。

注： Horizon 7 サイジングの制限と推奨事項に関する最新情報については、VMware ナレッジベース (KB) の記事 <https://kb.vmware.com/s/article/2150348> を参照してください。

次の条件下では、vSphere クラスタに ESXi ホストまたはノードを最大 32 個まで含めることができます。

- vSphere 5.1 以降で View Composer をリンク クローン プール使用し、NFS データストアまたは VMFS5 以降のデータストアにレプリカ ディスクを格納している
- vSphere 6.0 以降を使用し、Virtual Volumes データストアにプールを格納している

vSphere 5.5 Update 1 以降を使用していて、vSAN データストア上にプールを格納している場合、vSphere クラスタには最大 20 個の ESXi ホストを含めることができます。

VMFS5 より前の VMFS バージョンに View Composer レプリカを保存する場合、クラスタは最大で 8 ホストを持つことができます。OS ディスクおよび通常ディスクは、NFS データストアまたは VMFS データストアに格納できます。

詳細については、『Horizon 7 での仮想デスクトップのセットアップ』ドキュメントのデスクトップ プールの作成に関する章を参照してください。ネットワークの要件は、サーバのタイプ、ネットワーク アダプタの数、および VMotion の構成方法に依存します。

高可用性の要件の特定

vSphere ではその効率性およびリソース管理により、サーバあたりの仮想マシン数を、業界をリードするレベルまで高めることができます。しかし、サーバあたりの仮想マシンの密度を高くすることは、サーバに障害が発生した場合に影響を受けるユーザーが多くなるということです。

高可用性の要件は、デスクトップ プールの目的に応じて大きく異なる場合があります。たとえば、ステートレス デスクトップ イメージ (フローティング割り当て) プールの目標復旧ポイント (RPO) の要件は、ステートフル デスクトップ イメージ (専用割り当て) プールとは異なる場合があります。フローティング割り当てプールの場合受容可能な解決策として、ユーザーが使用しているデスクトップが使用できなくなったとき、それらのユーザーを別のデスクトップにログインさせるという方法が考えられます。

可用性の必要性が高い場合は、VMware HA の適切な構成が不可欠です。VMware HA を使用して、サーバあたりのデスクトップ数を固定する予定の場合は、各サーバを軽減容量で稼働させます。サーバに障害が発生した場合、デスクトップが別のホスト上で再起動しても、サーバあたりのデスクトップ数の容量を超えません。

たとえば、各ホストが 128 のデスクトップを実行でき、1 台のサーバの障害に耐えることを目標とする 8 ホストのクラスタでは、そのクラスタ上で実行されるデスクトップの数を必ず $128 \times (8 - 1) = 896$ 以内にします。VMware DRS (Distributed Resource Scheduler) を使用して、8 台のホストすべてにデスクトップを均等に分散させることもできます。どのホット スペア リソースもアイドルにしておくことなく、余ったサーバ容量を最大限に利用できます。また、DRS は障害の発生したサーバがサービスに復帰した後のクラスタの再分散にも役立ちます。

サーバの障害に応答して多数の仮想マシンが一斉に再起動するために発生する I/O 負荷をサポートするため、ストレージが適切に構成されていることも確認する必要があります。ストレージの IOPS は、デスクトップがサーバの障害から復旧する速さに最も大きく影響します。

例：クラスタ構成の例

以下の表に示した設定は、Horizon 7 に固有のものです。vSphere での HA クラスタの制限については、『VMware vSphere 構成の上限』ドキュメントを参照してください。

注： 次のインフラストラクチャの例は、View 5.2 および vSphere 5.1 を使用してテストされました。この例では、インスタント クローンではなく View Composer のリンククローンが使用されていますが、これはテストが View 5.2 で実行されたためです。インスタント クローン機能は Horizon 7 で導入されています。View 5.2 では使用できなかった機能としては、他にも vSAN と Virtual Volumes があります。

表 4-9. Horizon 7 インフラストラクチャ クラスタの例

アイテム	例
仮想マシン	デスクトップ プール ソースとして使用するための vCenter Server インスタンス、Active Directory、SQL データベース サーバ、View Composer、Connection Server インスタンス、セキュリティ サーバ、親仮想マシン
ノード (ESXi ホスト)	6 Dell PowerEdge R720 サーバ (16 コア * 2 GHz; および各ホストで 192GB RAM)
SSD ストレージ	vCenter Server、View Composer、SQL データベース サーバ、および親仮想マシン用の仮想マシン
非 SSD ストレージ	Active Directory、Connection Server、およびセキュリティ サーバ用の仮想マシン
クラスタ タイプ	DRS (Distributed Resource Scheduler) /HA

表 4-10. 仮想マシン デスクトップ クラスタの例

アイテム	例
クラスタの数	5
クラスタあたりのデスクトップおよびプールの数	クラスタあたり 2,000 のデスクトップ (仮想マシン) の 1 つのプール
ノード (ESXi ホスト)	<p>以下は、各クラスタで使用できたさまざまなサーバの例です：</p> <ul style="list-style-type: none"> ■ 12 Dell PowerEdge R720 (16 コア * 2 GHz; および各ホストで 192 GB RAM) ■ 16 Dell PowerEdge R710 (12 コア * 2.526 GHz; および各ホストで 144GB RAM) ■ 8 Dell PowerEdge R810 (24 コア * 2 GHz; および各ホストで 256GB RAM) ■ 6 の Dell PowerEdge R810 + 3 PowerEdge R720
SSD ストレージ	レプリカ仮想マシン

表 4-10. 仮想マシン デスクトップ クラスターの例（続き）

アイテム	例
非 SSD ストレージ	32 のクローン用の非 SSD データストア（データストアあたり 450 GB）
クラスター タイプ	DRS (Distributed Resource Scheduler) /HA

ストレージと帯域幅の要件

仮想マシン デスクトップの共有ストレージの計画、I/O ストームに関するストレージの帯域幅要件の計画、およびネットワーク帯域幅要件の計画など、いくつかの考慮事項があります。

VMware のテスト設定で使用されたストレージおよびネットワーキング コンポーネントについての詳細は、これらの関連トピックで提供されます。

■ 共有ストレージの例

View 5.2 のテスト環境の場合、View Composer レプリカ仮想マシンは、読み取りパフォーマンスが高い半導体ディスク ドライブ (SSD) に配置され、これは秒あたりで何万もの I/O (IOPS) をサポートしています。リンク クローンは、従来の低パフォーマンスのスピニング メディアのデータストアに置かれていました。これは低価格ですが、多くのストレージ容量を提供します。この例ではインスタント クローンではなく View Composer のリンククローンが使用されていますが、これはテストが View 5.2 で実行されたためです。インスタント クローン機能は Horizon 7 で導入されています。

■ ストレージバンド幅に関する考慮事項

Horizon 7 環境では、ログオン ストームがバンド幅要件を決定するうえでの主要な考慮事項になります。

■ ネットワーク バンド幅に関する考慮事項

特定の仮想および物理ネットワーク コンポーネントは、一般的なワークロードを格納するために必要となります。

■ View Composer パフォーマンス テストの結果

これらのテスト結果を用いて、10,000 のデスクトップに View 5.2 をセットアップする方法を説明します。ここでは 1 つの vCenter Server 5.1 インスタンスが 5 つのプールを管理し、それぞれのプールに 2,000 台の仮想マシン デスクトップがあります。新しいプールのプロビジョニング、または 2,000 の仮想マシンの既存プールの再構成、更新、または再分散のために、メンテナンス期間が 1 度だけ必要でした。10,000 ユーザーのログオン ストームもテストされました。

■ WAN のサポート

WAN（ワイド エリア ネットワーク）については、バンド幅の制約と遅延の問題を考慮する必要があります。VMware が提供する PCoIP および Blast Extreme 表示プロトコルは、遅延やバンド幅が変動する状況にも適応します。

共有ストレージの例

View 5.2 のテスト環境の場合、View Composer レプリカ仮想マシンは、読み取りパフォーマンスが高い半導体ディスク ドライブ (SSD) に配置され、これは秒あたりで何万もの I/O (IOPS) をサポートしています。リンク クローンは、従来の低パフォーマンスのスピニング メディアのデータストアに置かれていました。これは低価格ですが、多くのストレージ容量を提供します。この例ではインスタント クローンではなく View Composer のリンククローン

が使用されていますが、これはテストが View 5.2 で実行されたためです。インスタント クローン機能は Horizon 7 で導入されています。

ストレージ設計に関する考慮事項は、Horizon 7 アーキテクチャを成功させるための最も重要な要素の 1 つです。アーキテクチャに最大の影響を及ぼす決定は、リンク クローン テクノロジを使用する View Composer デスクトップを採用するかどうかです。ESXi バイナリ、仮想マシンのスワップ ファイル、および親仮想マシンの View Composer レプリカは共有ストレージ システムに格納されます。

vSphere が使用する外部ストレージ システムは、ファイバ チャネルまたは iSCSI の SAN（ストレージ エリア ネットワーク）、あるいは NFS（ネットワーク ファイル システム）の NAS（ネットワーク接続ストレージ）です。vSphere 5.5 Update 1 以降で利用できる vSAN 機能では、ストレージ システムをローカル サーバ接続型ストレージに集約することもできます。

以下の例は、10,000 のデスクトップを管理する 1 つの vCenter Server の View 5.2 テスト設定で使用される階層型ストレージ戦略を説明します。

注： この例は、VMware vSAN のリリース以前に実行された View 5.2 セットアップで使用されました。VMware vSAN の View 仮想デスクトップ インフラストラクチャの主要コンポーネントのサイズ調整と設計のガイダンスについては、<http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf> から提供されているホワイト ペーパーを参照してください。

vSphere 6.0 以降のリリースで使用可能な vSAN 機能には、vSphere 5.5 Update 1 で使用可能になった機能を上回る、多数のパフォーマンス上の改善が含まれています。vSphere 6.0 では、この機能により広範囲にわたる HCL（ハードウェア互換性）サポートも含まれています。vSphere 6 以降の vSAN の詳細については、『VMware vSAN の管理』を参照してください。

物理ストレージ

- EMC VNX7500-block のみ
- 1.8TB Fast Cache (SSD)
- 8 つの 10Gbit FCoE フロント エンド接続（コントローラ当たり 4）。

SSD ストレージ層

単一 RAID5 ストレージ プール:

- 12 * 200GB EFD
- 親イメージ用に 250GB LUN
- インフラストラクチャ用に 500GB LUN
- レプリカ ストア用に 75GB LUNs（デスクトップ プール クラスタ当たり 1 つ）

仮想マシン デスクトップ ストレージ層

2 つの RAID 1/0 ストレージ プール:

プール 1 用:

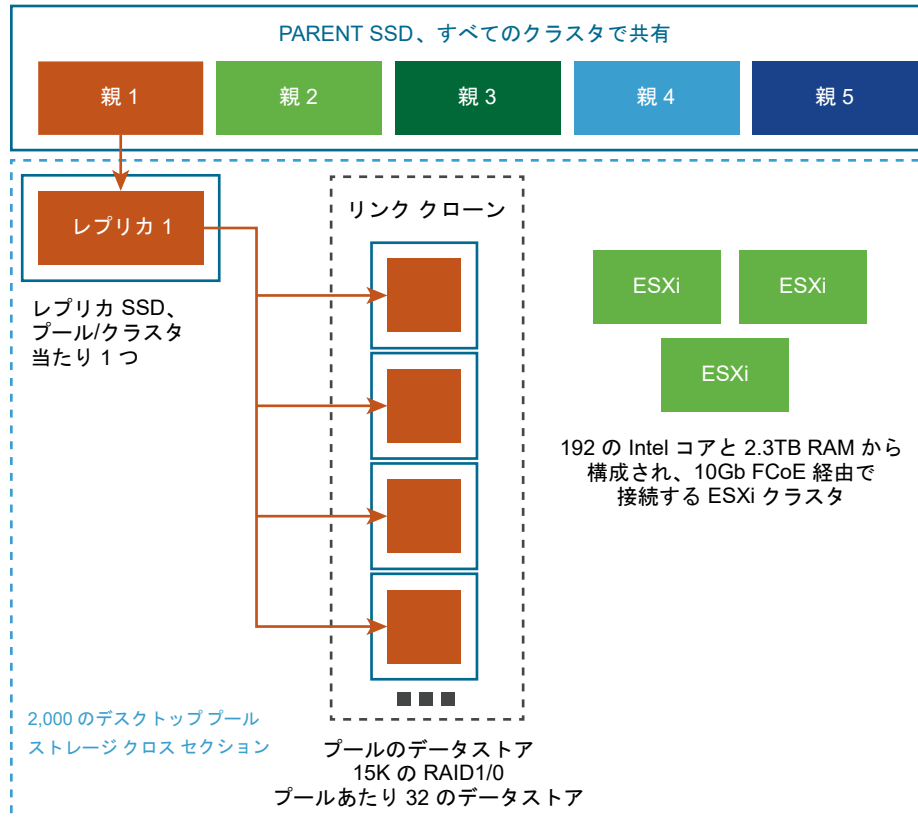
- 360 の 15K 300GB HDD（47TB を使用可能）
- デスクトップ用に 97 の 450GB LUN

プール 2 用:

- 296 の 15K 300GB HDD (39TB を使用可能)
- インフラストラクチャ用に 7 つの 450GB LUN
- デスクトップ用に 85 の 450GB LUN

このストレージ戦略は以下の図で説明されています。

図 4-1. 大規模デスクトップ プール用の階層ストレージの例



アーキテクチャの観点から見ると、View Composer では、基本イメージを共有するデスクトップ イメージが作成されるため、ストレージの必要量を 50% 以上削減できます。デスクトップを定期的に元の状態に戻し、最終更新操作以降の変更の追跡に使用される領域を回収する更新ポリシーを設定すると、さらにストレージの必要量を削減できます。

vSphere 5.1 以降の仮想マシン デスクトップで View Composer を使用する場合、領域再利用機能を使用できます。この機能を使用すれば、未使用のディスク領域の量が特定のしきい値に達すると、ゲスト OS 内の無効または削除されたデータは、自動的にワイプおよび縮小プロセスで再利用されます。vSAN データストアを使用する場合は領域再利用機能はサポートされないことに注意してください。

また、View Composer の通常ディスクまたは共有ファイル サーバをユーザー プロファイルおよびユーザー ドキュメントのプライマリ リポジトリとして使用すると、オペレーティング システムのディスク領域も削減できます。View Composer ではユーザー データをオペレーティング システムから分離できるため、通常ディスクのみをバックアップまたは複製するだけでよい場合があります、そのためにストレージの必要量がさらに削減されます。詳細については、[Composer によるストレージ要件の低減](#)を参照してください。

注： 専用ストレージ コンポーネントに関する意思決定はパイロット段階で行うのが最適です。主な考慮事項は、1 秒あたりの I/O 数 (IOPS) です。パフォーマンスおよびコスト削減を最大化するために、階層型ストレージ戦略または vSAN ストレージを試してみることもできます。

詳細については、ベスト プラクティス ガイドである『Storage Considerations for VMware View』を参照してください。

ストレージバンド幅に関する考慮事項

Horizon 7 環境では、ログオン ストームがバンド幅要件を決定するうえでの主要な考慮事項になります。

Horizon 7 環境をサポートするストレージ システムの設計には重要な要素が多数ありますが、サーバ構成の観点から見た場合、適切なストレージバンド幅の計画が不可欠です。また、ポート統合ハードウェアの影響も考慮する必要があります。

Horizon 7 環境では、すべての仮想マシンが同時にアクティビティを実行しているときに、I/O ストームの負荷が発生することがあります。I/O ストームは、ウィルス対策ソフトウェアやソフトウェア更新エージェントなどのゲストベースのエージェントによってトリガされることがあります。また、従業員全員が朝のほぼ同じ時刻にログインした場合のように、人間の動作によって I/O ストームがトリガされることもあります。VMware は、10,000 のデスクトップでログオン ストームのシナリオをテストしました。詳細については、[View Composer パフォーマンス テストの結果](#)を参照してください。

仮想マシンごとに更新の時刻をずらすなどの運用上のベスト プラクティスによって、このストーム ワークロードを最小限に抑えることができます。また、パイロット段階でさまざまなログオフ ポリシーをテストして、ユーザーがログオフした場合のサスペンドまたは電源オフによって I/O ストームが発生するかどうかを判別することもできます。View Composer レプリカを個別の高性能データストアに格納することにより、集約型の同時読み取り操作を高速化して I/O ストームの負荷に対処することができます。たとえば、次のストレージ戦略のいずれかを使用できます。

- ブール設定を手動で構成して、レプリカが別の高性能なデータストアに保存されるようにします。
- vSphere 5.5 Update 1 以降で利用可能な vSAN を使用します。これは、ソフトウェア ポリシーベースの管理を使用し、レプリカに使用するディスクの種類を決定します。
- vSphere 6.0 以降で利用可能な Virtual Volumes を使用します。Virtual Volumes ではソフトウェア ポリシーベース管理を使用し、レプリカに使用するディスクの種類を決定します。

ベスト プラクティスの特定に加え、バンド幅の平均使用量が 1Gbps の 10 分の 1 未満であっても、仮想マシン 100 台あたり 1Gbps のバンド幅を提供することをお勧めします。このように余裕をもって計画すると、ピーク時の負荷にも十分なストレージの接続性を確保できます。

ネットワーク バンド幅に関する考慮事項

特定の仮想および物理ネットワーク コンポーネントは、一般的なワークロードを格納するために必要となります。

ディスプレイ トラフィックについては、使用されるプロトコル、モニターの解像度と構成、ワークロードに含まれるマルチメディア コンテンツの量など、多くの要素がネットワーク バンド幅に影響を及ぼします。ストリーミングされた複数のアプリケーションを同時に起動した場合も、使用量が急増することがあります。

これらの問題による影響は大きく変動する場合があるため、多くの企業ではパイロット プロジェクトの一環としてバンド幅の使用量を監視しています。パイロットの出発点として、一般的なナレッジ ワーカー用に 150 ~ 200Kbps の容量を計画してください。

PCoIP または Blast Extreme 表示プロトコルでは、100Mb または 1Gb のスイッチド ネットワークを備えた企業 LAN がある場合、エンド ユーザーは次の条件の下で優れたパフォーマンスを期待できます。

- 2 台のモニター (1920 x 1080)
- Microsoft Office アプリケーションの大量の使用
- フラッシュが埋め込まれた Web ブラウズの大量の使用
- 全画面表示モードの使用が制限されたマルチメディアの頻繁な使用
- USB ベースの周辺機器の頻繁な使用
- ネットワーク ベースの印刷

詳細については、『PCoIP 表示プロトコル: 情報およびシナリオに基づくネットワーク サイジング ガイド』という情報ガイドを参照してください。

PCoIP および Blast Extreme で使用可能な最適化制御

VMware の PCoIP または Blast Extreme 表示プロトコルを使用する場合は、バンド幅の使用に影響するいくつかの要素を調整できます。

- ネットワーク輻輳期間中に使用されるイメージ品質レベルとフレーム レートを構成できます。品質レベル設定により、表示イメージ内の変更された領域の初期品質を制限できます。フレーム レートも調整できます。

この制御は、静的な画面のコンテンツを更新する必要がない場合、または一部分のみ更新する必要がある場合に有効に機能します。

- セッションのバンド幅に関しては、4 メガビット/秒のインターネット接続などのネットワーク接続のタイプに対応するため、最大バンド幅をキロビット/秒単位で構成できます。このバンド幅には、イメージ、オーディオ、仮想チャネル、USB、および PCoIP または Blast 制御のすべてのトラフィックが含まれます。

バンド幅が使用可能になるまでユーザーが待つ必要がないようにするため、セッション用に予約されるバンド幅の下限をキロビット/秒単位で構成することもできます。セッションでの UDP パケットの最大転送ユニット (MTU) サイズを 500 バイトから 1500 バイトの間で指定できます。

詳細については、『Horizon 7 でのリモート デスクトップ機能の構成』の「PCoIP の全般設定」および「VMware Blast ポリシー設定」セクションを参照してください。

ネットワーク構成の例

各プールで 2,000 台の仮想マシンのプール 5 つを管理する 1 つの vCenter Server 5.1 インスタンスがある View 5.2 テスト ポッドでは、ネットワーク要件として各 ESXi ホストには以下のハードウェアおよびソフトウェアが含まれていました。

注： この例は、VMware vSAN のリリース以前に実行された View 5.2 セットアップで使用されました。VMware vSAN の View 仮想デスクトップ インフラストラクチャの主要コンポーネントのサイズ調整と設計のガイダンスについては、<http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf> から提供されているホワイト ペーパーを参照してください。また、この例ではインスタント クローンではなく View Composer のリンククローンが使用されていますが、これはテストが View 5.2 で実行されたためです。インスタント クローン機能は Horizon 7 で導入されています。

各ホストの物理コンポーネント

- 10Gig イーサネットおよびネットワークとストレージ トラフィックのために FCoE をそれぞれ使用する Brocade 1860 Fabric Adapter。
- 6 つの VDX6720-60 スイッチで構成される Brocade VCS イーサネット ファブリックへの接続。Juniper J6350 ルーターへの 2 つの 1GB 接続がある残りのネットワークにアップリンクされたスイッチ。

vLAN 概要

- デスクトップ プール当たり 1 つの 10Gb vLAN (5 プール)
- 管理ネットワーク用に 1 つの 1Gb vLAN
- VMotion ネットワーク用に 1 つの 1Gb vLAN
- インフラストラクチャ ネットワーク用に 1 つの 10Gb vLAN

仮想 VMotion-dvswitch (ホスト当たり 1 つのアップリンク)

このスイッチは、インフラストラクチャの ESXi ホスト、親、およびデスクトップ仮想マシンで使用されました。

- Jumbo Frame (9000 MTU)
- 1 つのエフェメラル分散ポート グループ
- プライベート VLAN および 192.168.x.x アドレッシング

Infra-dvswitch (ホスト当たり 2 つのアップリンク)

このスイッチは、インフラストラクチャ仮想マシンの ESXi ホストで使用されました。

- Jumbo frame (9000 MTU)
- 1 つのエフェメラル分散ポート グループ
- インフラストラクチャ VLAN /24 (256 アドレス)

Desktop-dvswitch (ホスト当たり 2 つのアップリンク)

このスイッチは、親の ESXi ホスト、およびデスクトップ仮想マシンで使用されました。

- Jumbo frame (9000 MTU)
- 6 つのエフェメラル分散ポート グループ

- 5 台のデスクトップ ポート グループ (プール当たり 1 つ)
- 各ネットワークは /21, 2048 アドレスでした

View Composer パフォーマンス テストの結果

これらのテスト結果を用いて、10,000 のデスクトップに View 5.2 をセットアップする方法を説明します。ここでは 1 つの vCenter Server 5.1 インスタンスが 5 つのプールを管理し、それぞれのプールに 2,000 台の仮想マシンデスクトップがあります。新しいプールのプロビジョニング、または 2,000 の仮想マシンの既存プールの再構成、更新、または再分散のために、メンテナンス期間が 1 度だけ必要でした。10,000 ユーザーのログオン ストームもテストされました。

ここで提供されるテスト結果は、以下のトピックで説明されているソフトウェア、ハードウェア、およびコ設定で達成されました:

- [Horizon Connection Server の最大接続数と仮想マシン構成](#) で説明されるデスクトップおよびプール構成
- [共有ストレージの例](#) で説明される階層ストレージ コンポーネント
- [ネットワーク バンド幅に関する考慮事項](#) で説明されるネットワーキング コンポーネント

10,000 ユーザーの長時間ログオン ストームの許容量

注: この例は、VMware vSAN のリリース以前に実行された View 5.2 セットアップで使用されました。VMware vSAN の View 仮想デスクトップ インフラストラクチャの主要コンポーネントのサイズ調整と設計のガイダンスについては、<http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf> から提供されているホワイト ペーパーを参照してください。vSAN 使用時の各種ワークロードと View 操作のテスト結果については、<http://www.vmware.com/files/pdf/techpaper/vmware-horizon-view-virtual-san-reference-architecture.pdf> から提供されているリファレンス アーキテクチャ ホワイト ペーパーを参照してください。

vSphere 6.0 以降のリリースで使用可能な vSAN 機能には、vSphere 5.5 Update 1 で使用可能になった機能を上回る、多数のパフォーマンス上の改善が含まれています。vSphere 6.0 では、この機能により広範囲にわたる HCL (ハードウェア互換性) サポートも含まれています。vSphere 6 以降の vSAN の詳細については、『VMware vSAN の管理』を参照してください。

テスト設定で、以下のデスクトップおよびプール構成は、10,000 台のデスクトップのログオン ストーム シナリオで使用されました。デスクトップの電源ポリシーは常にオンに設定されました。

10,000 台のデスクトップでは、ログオン ストームは、ログオン時間の通常の配布を使用して 60 分間にわたり発生しました。仮想マシンは電源をオンにされており、ログオン ストリームが始まる前には使用できました。ログオン後は以下のアプリケーションが含まれるワークロードが開始されます。Adobe Reader、Microsoft Outlook、Internet Explorer、Microsoft Word、および Notepad。

以下は、テスト中に持続したログオン ストームの補足的な詳細です。

- +/- 2 標準偏差ウィンドウ内に発生するログオンの 95% (40 分)。
- +/- 1 標準偏差ウィンドウ内に発生するログオンの 68% (20 分)。
- ログオン率のピークは 400/min または 6.67/秒でした。

プールのプロビジョニングに必要な時間

プールを作成すると、アップフロントまたはユーザーが指定した時にオンデマンドでプロビジョニングされます。プロビジョニングとは、仮想マシンを作成し、正しいオペレーティング システム イメージおよびネットワーク設定を使用するように構成するという意味です。

それぞれ 2,000 の仮想マシンのプールを 4 つ含むテスト設定では、2,000 の仮想マシンを含む 5 番目のプールのプロビジョニングには 4 時間かかりました。すべての仮想マシンはアップフロントでプロビジョニングされました。

プールの再構成に必要な時間

オペレーティング システムのパッチの提供、アプリケーションのインストールまたはアップデート、またはプールの仮想マシンのデスクトップ ハードウェア設定の変更を行うために再構成操作を使用できます。プールの再構成の前に、新しい構成を行う仮想マシンのスナップショットをとってください。再構成操作は、そのスナップショットを使用して、プールのすべての仮想マシンをアップデートします。

それぞれ 2,000 の仮想マシンの 5 つのプールのテスト設定では、2,000 の仮想マシンの 1 つのプールの再構成に 6 時間 40 分かかりました。再構成操作の開始前、すべての仮想マシンは電源をオンにされて使用できました。

プールの更新に必要な時間

ディスクは時間とともに成長するので、ユーザーがログオフした時にデスクトップをオリジナルの状態に更新することによって、または定期的にデスクトップを更新するスケジュールを設定でき、ディスク領域を消費しすぎないようにできます。たとえば、デスクトップが毎日、毎週、または毎月更新されるようにスケジュールを設定できます。

それぞれ 2,000 の仮想マシンの 5 つのプールのテスト設定では、2,000 の仮想マシンの 1 つのプールの更新に 2 時間 40 分かかりました。更新操作の開始前、すべての仮想マシンは電源をオンにされて使用できました。

プールの再分散に必要な時間

デスクトップの再分散操作は、リンク クローン デスクトップを使用可能な論理ドライブ間で均等に再分配します。再分散操作によって、過負荷のドライブ上のストレージ領域が節約され、十分に使用されないドライブがなくなります。また、再分散操作を使用して、デスクトップ プールのすべての仮想マシンを vSAN データストアに移行したり、このデータストアから移行することができます。

それぞれ 2,000 の仮想マシンのプールを 5 つ含むテスト ポッドでは、2 つのデータストアが 1 つのテストでポッドに追加されました。他のテストでは、2 つのデータストアがポッドから削除されました。データストアが追加または削除された後、再分散操作がプールの 1 つで実行されました。2,000 の仮想マシンの 1 つのプールの再分散には 9 時間かかりました。再分散操作の開始前、すべての仮想マシンは電源をオンにされて使用できました。

WAN のサポート

WAN (ワイド エリア ネットワーク) については、バンド幅の制約と遅延の問題を考慮する必要があります。VMware が提供する PCoIP および Blast Extreme 表示プロトコルは、遅延やバンド幅が変動する状況にも適応します。

RDP 表示プロトコルを使用する場合は、支社または小規模オフィスのユーザー向けにアプリケーションを高速化する WAN 最適化製品が必要です。PCoIP および Blast Extreme では、多くの WAN 最適化技術がベース プロトコルに組み込まれています。

- WAN の最適化が有効になるのは、RDP など TCP ベースのプロトコルです。その理由は、これらのプロトコルではクライアントとサーバの間で多くのハンドシェイクが行われるためです。こうしたハンドシェイクでは、遅延が非常に大きくなることがあります。WAN アクセラレータのスプーフィングはハンドシェイクに応答するため、ネットワークの遅延はプロトコルから隠れるようになります。PCoIP および Blast Extreme は UDP ベースであるため、この形式の WAN アクセラレーションは不要となります。
- WAN アクセラレータではクライアントとサーバ間のトラフィックの圧縮も行われますが、この圧縮は通常、2:1 の圧縮率に限定されます。PCoIP および Blast Extreme では、圧縮率が大幅に高くなります。

PCoIP および Blast Extreme によるバンド幅消費を調節するために利用可能な制御については、[PCoIP および Blast Extreme で使用可能な最適化制御](#)を参照してください。

各種のユーザーのバンド幅要件

PCoIP の最小のバンド幅要件を決定する場合、次の予測値を元に計画します。

- 基本的なオフィス アプリケーションを使用するデスクトップで 100 ~ 150Kbps の平均バンド幅：ビデオ、3D グラフィックスのない典型的なオフィス アプリケーション、およびデフォルトの Windows および Horizon 7 設定。
- オフィス アプリケーションを使用する最適化されたデスクトップで 50 ~ 100Kbps の平均バンド幅：ビデオや 3D グラフィックスを使用しない通常のオフィス アプリケーションと最適化された Windows デスクトップ設定と最適化された Horizon 7。
- 複数のモニター、3D、Aero および Microsoft Office を使用する仮想デスクトップで 400 ~ 600Kbps の平均バンド幅。
- 集中的な表示変更に対応できる余裕を確保するため、500Kbps ~ 1Mbps の最小のピーク時バンド幅。通常は、平均バンド幅を使用してネットワークのサイズを設定しますが、大規模な画面変更がありイメージトラフィックが集中する状況に対応できるようにピーク時のバンド幅を考慮してください。
- 480p ビデオを実行する同時接続ユーザーごとに 2Mbps。構成されているフレーム レートの制限およびビデオタイプによって異なります。

注： 一般的なユーザーの予測値である 50 ~ 150Kbps は、すべてのユーザーが連続して操作を行い、1 日に 8 ~ 10 時間を同様のタスクを実行する状況を前提としています。50Kbps のバンド幅使用量は、可逆圧縮機能を無効にした LAN で View Planner をテストした。結果です。まったく操作を実行しないユーザーいる場合、バンド幅をほとんど消費せず、1 つのリンクでさらに多くのユーザーに対応できるので、状況が異なる場合があります。したがって、これらのガイドラインは、詳細なバンド幅を計画およびテストするための出発点となることを目的としています。

次の例は、1.5Mbps T1 回線がある支店やリモート オフィスの同時接続ユーザー数を計算する方法を示しています。

支店またはリモート オフィスのシナリオ

- ユーザーは基本的な Microsoft Office アプリケーションを使用しており、ビデオや 3D グラフィックスは使用していません。USB キーボードとマウス デバイスを使用しています。

- Horizon 7 の通常のオフィス ユーザー 1 人に必要となるバンド幅は、50 ～150Kbps です。
- T1 ネットワーク キャパシティは、1.5Mbps です。
- バンド幅利用率は 80 パーセントです（利用率の係数は .8 として計算します）。

サポートされるユーザー数を決定する式

- 最悪のケースで、ユーザーで 150Kbps が必要となります。 $(1.5\text{Mbps} \times .8) / 150\text{Kbps} = (1500 \times .8) / 150 = 8$ ユーザー
- 最高のケースで、ユーザーで 50Kbps が必要となります。 $(1.5\text{Mbps} \times .8) / 50\text{Kbps} = (1500 \times .8) / 50 = 24$ ユーザー

結果

このリモート オフィスでは、キャパシティが 1.5Mbps の T1 回線 1 つにつき 8 ～ 24 人の同時接続ユーザーをサポートできます。

重要： このユーザー密度を実現するためには、Horizon 7 と Windows デスクトップの両方の設定を最適化する必要がある場合があります。

Horizon 7 ビルディング ブロック

ビルディング ブロックは、物理サーバ、vSphere インフラストラクチャ、Horizon 7 サーバ、共有ストレージ、およびエンド ユーザー用の仮想マシン デスクトップで構成されます。ビルディング ブロックは 1 つの論理構造です。ビルディング ブロックの Horizon デスクトップの数は、2,000 個を超えないようにする必要があります。通常は最大 5 個のビルディング ブロックを Horizon 7 ポッドに含めますが、ポッドが 10,000 個のセッションと 7 個の Horizon 接続サーバ インスタンスを超えない限り、理論上は 5 個よりも多くのブロックを使用できます。

表 4-11. 2,000 台の仮想マシン デスクトップ用の LAN ベースの Horizon ビルディング ブロックの例

アイテム	例
vSphere クラスタ	1 以上
80 ポートのネットワーク スイッチ	1
共有ストレージ システム	1
同じホストで View Composer が搭載された vCenter Server	1（ブロック自体で実行可能）
データベース	MS SQL Server または Oracle データベース サーバ（ブロック自体で実行可能）
VLAN	3（各々に 1 ギガビット イーサネット ネットワーク：管理ネットワーク、ストレージ ネットワーク、および VMotion ネットワーク）

各 vCenter Server では、最大 10,000 台の仮想マシンをサポートできます。このサポートにより、2,000 台よりも多い仮想マシン デスクトップを含むビルディング ブロックを実現できます。ただし、実際のブロック サイズは、その他の Horizon 7 固有の制限事項の影響も受けます。

ポッドにビルディング ブロックが 1 つしかない場合は、冗長性を確保するために 2 つの接続サーバ インスタンスを使用します。

Horizon 7 ポッド

ポッドとは、Horizon 7 のスケーラビリティの制限によって決定される組織の単位です。

5 つのビルディング ブロックを使用したポッドの例

従来の Horizon 7 ポッドは、1 つのエンティティとして管理できる 2,000 ユーザーのビルディング ブロック 5 つを統合します。

表 4-12. 5 つのビルディング ブロックで構成された LAN ベースの Horizon 7 ポッドの例

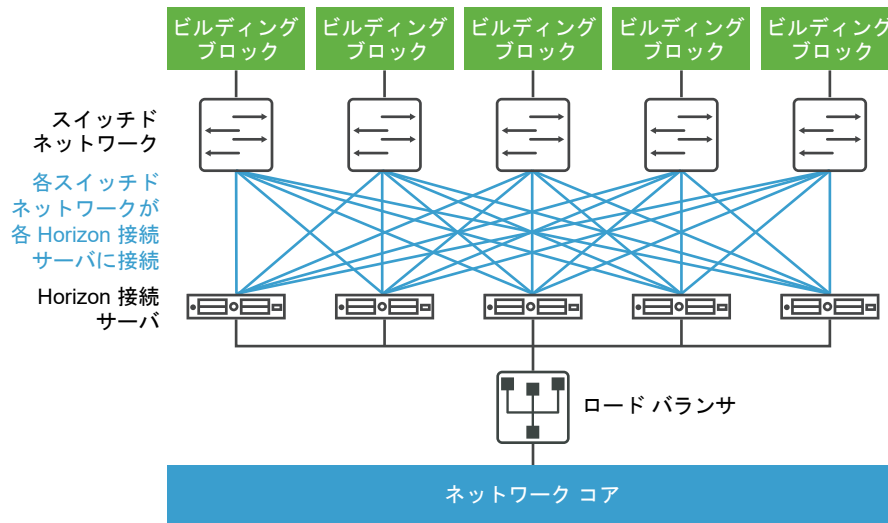
アイテム	数
1 つの Horizon 7 ポッドのビルディング ブロック	5
vCenter Server と View Composer	5 (各ビルディング ブロックに両方をホストする 1 つの仮想マシン)
データベース サーバ	5 (各ビルディング ブロックに 1 つのスタンドアロンデータベース サーバ) MS SQL Server または Oracle データベース サーバ
接続サーバ	7 (企業ネットワーク内部から 5 接続と外部から 2 接続)
vLAN	表 4-11. 2,000 台の仮想マシン デスクトップ用の LAN ベースの Horizon ビルディング ブロックの例 を参照してください。
10Gb イーサネット モジュール	1
モジュラ型ネットワーク スイッチ	1

各 vCenter Server では、最大 35,000 台の登録された仮想マシンをサポートできます。このサポートにより、2,000 台よりも多い仮想マシン デスクトップを含むビルディング ブロックを実現できます。ただし、実際のブロック サイズは、その他の Horizon 7 固有の制限事項の影響も受けます。

ここで説明する両方の例については、ネットワーク コアは接続サーバ インスタンス間の受信要求をロード バランシングできます。通常はネットワーク レベルで冗長性およびフェイルオーバーがサポートされるため、ロード バランサが単一点障害になることが防止できます。たとえば、Virtual Router Redundancy Protocol (VRRP) はロード バランサと通信して、冗長性およびフェイルオーバーの機能を追加できます。

接続サーバ インスタンスに障害が発生するか、アクティブなセッション中に応答がなくなった場合でも、ユーザーのデータは失われません。デスクトップの状態は仮想マシン デスクトップに保存されているため、ユーザーは別の接続サーバ インスタンスに接続でき、障害が発生した時点の状態からデスクトップ セッションが再開されます。

図 4-2. 10,000 の仮想マシン デスクトップのポッド ダイアグラム



1 つの vCenter Server を使用するポッドの例

前節では、Horizon 7 ポッドは複数のビルディング ブロックで構成されていました。各ビルディング ブロックは、単一の vCenter Server で 2,000 の仮想マシンがサポートされました。VMware では、顧客とパートナーから、単一の vCenter Server を使用して Horizon 7 ポッドを管理したいというご要望を多数いただきました。このご要望は、vCenter Server の単一のインスタンスが 10,000 の仮想マシンをサポートできることによるものです。ユーザーは 1 台の vCenter Server を使用して 10,000 のデスクトップ環境を管理できます。このトピックでは、単一の vCenter Server を使用して 10,000 のデスクトップを管理するアーキテクチャを説明します。

10,000 のデスクトップに対して 1 台の vCenter Server と 1 つの View Composer を使用することは可能ですが、そうすると単一点障害ができてしまいます。その単一の vCenter Server が失われると、デスクトップ展開全体が電源、プロビジョニング、および修理作業で使用できない状態になります。このため、全般的なコンポーネント回復力のための要件を満たす展開アーキテクチャを選択してください。

この例で、10,000 ユーザーのポッドは、物理サーバ、vSphere インフラストラクチャ、Horizon 7 サーバ、共有ストレージ、およびクラスタ当たり 2,000 仮想デスクトップの 5 つのクラスタで構成されます。

表 4-13. 1 つの vCenter Server がある LAN ベースの Horizon 7 ポッドの例

アイテム	例
vSphere クラスタ	6 (クラスタ当たり 1 つのリンク クローン プールのある 5 つのクラスタ および 1 つの インフラストラクチャ クラスタ)
vCenter Server	1
View Composer	1 (スタンドアロン)
データベース サーバ	1 (スタンドアロン) MS SQL Server または Oracle データベース サーバ
Active Directory サーバ	1 または 2
接続サーバ インスタンス	5

表 4-13. 1 つの vCenter Server がある LAN ベースの Horizon 7 ポッドの例（続き）

アイテム	例
セキュリティ サーバ	5
vLAN	8（デスクトップ プール クラスターで 5、そして管理、VMotion、およびインフラストラクチャ クラスターでそれぞれ 1）

クラウド ポッド アーキテクチャ の概要

データセンターをまたいで Horizon を展開する場合に、複製された接続サーバ インスタンスのグループを WAN、MAN (metropolitan area network)、または他の LAN 以外をまたいで使用するには、クラウド ポッド アーキテクチャ 機能を使用する必要があります。

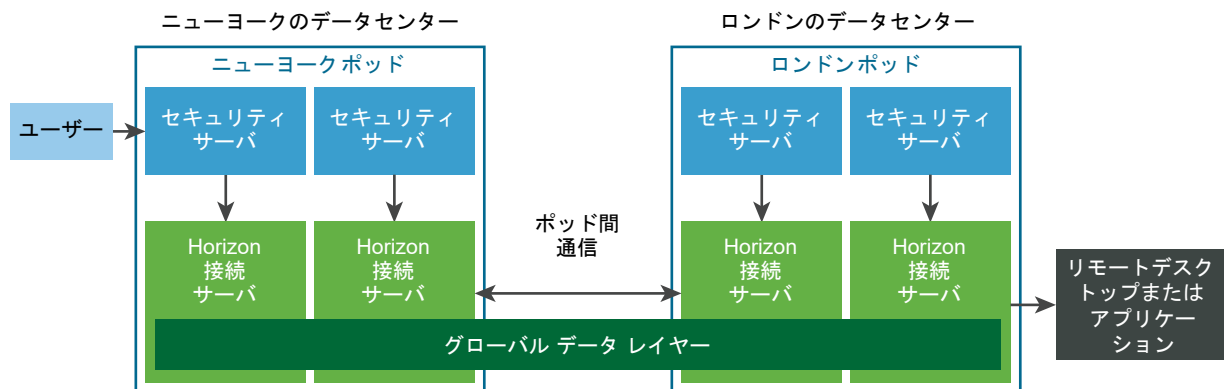
この機能は、標準の Horizon コンポーネントを使用して、複数のデータセンターにわたる管理、ユーザーとデスクトップ間のグローバルで柔軟なマッピング、高可用性デスクトップ、ディザスタ リカバリなどの機能を提供します。

クラウド ポッド アーキテクチャ トポロジは、一般に、ポッド フェデレーション内で一緒にリンクされた 2 つ以上のポッドで構成されます。ポッド フェデレーションは一定の制限を受けます。

表 4-14. ポッド フェデレーションの制限

オブジェクト	制限
セッションの合計	250,000
ポッド	50
ポッドあたりのセッション数	12,000
サイト	15
ポッドあたりの Connection Server インスタンス数	7
Connection Server インスタンスの合計	350

以下のダイアグラムは、基本的な クラウド ポッド アーキテクチャ トポロジの例です。



このトポロジの例では、以前は別々のデータセンターでスタンドアロンだった 2 つのポッドが結合され、単一のポッド フェデレーションを形成しています。この環境のエンド ユーザーは、ニューヨークのデータセンターの Connection Server インスタンスに接続して、ロンドンのデータセンターにあるデスクトップまたはアプリケーションを受け取ることができます。

クラウド ポッド アーキテクチャ機能は、IPv6 環境ではサポートされません。

詳細については、『Horizon 7 でのクラウド ポッド アーキテクチャの管理』を参照してください。

ポッドで複数の vCenter Server を使用する利点

500 台を超えるデスクトップを擁する Horizon 7 本番環境を設計する場合、いくつかの検討事項が、複数のインスタンスではなく 1 つの vCenter Server インスタンスを使用するかどうかに影響を及ぼします。

View 5.2 以降、VMware では vCenter Server 5.1 以降のサーバ 1 台を持つ 1 つの Horizon 7 ポッド内で最大 10,000 台のデスクトップ仮想マシンを管理できるようになりました。単一の vCenter Server インスタンスで 10,000 の仮想マシンを管理する前に、以下の検討事項を考慮してください。

- 会社のメンテナンス時間の長さ
- Horizon 7 コンポーネント失敗の許容量
- 電源、プロビジョニング、および修理作業の頻度
- インフラストラクチャの簡素化

メンテナンス時間の長さ

仮想マシンの電源、プロビジョニング、およびメンテナンス操作数の同時操作設定は、vCenter Server インスタンスごとに決定されます。

1 つの vCenter Server インスタンスを持つポッドの設計	<p>並行設定は、Horizon 7 ポッド全体で同時にキューに入る操作数を決定します。</p> <p>たとえば、同時実行するプロビジョニング操作を 20 に設定し、ポッドにある vCenter Server インスタンスが 1 つのみの場合、20 を超えるデスクトップ プールではプロビジョニング操作が連続操作になります。20 の同時操作をキューに入れた後、ひとつの操作は次を開始する前に完了する必要があります。大規模な Horizon 7 展開では、このプロビジョニング操作に時間がかかります。</p>
-------------------------------------	---

複数の vCenter Server インスタンスを持つポッドの設計	各インスタンスは 20 の仮想マシンを同時にプロビジョニングできます。
------------------------------------	-------------------------------------

1 つのメンテナンス期間内で同時に多くの操作を確実に完了するには、ポッドに複数の vCenter Server インスタンス（最大 5）を追加し、各 vCenter Server インスタンスが管理する vSphere クラスタに複数のデスクトップ プールを展開できます。vSphere クラスタを管理できるのは、1 度に 1 つの vCenter Server インスタンスのみです。vCenter Server インスタンス間で同時操作を行うには、デスクトップ プールを展開する必要があります。

コンポーネント失敗の許容量

Horizon 7 ポッドの vCenter Server の役割は、電源、プロビジョニング、および修理（リフレッシュ、再構成、および再分散）操作を提供することです。仮想マシン デスクトップを展開して電源を入れると、Horizon 7 は通常の操作コースでは vCenter Server に依存しません。

各 vSphere クラスタは 1 つの vCenter Server インスタンスによって管理される必要があるため、このサーバはどの Horizon 7 設計においても、単一点障害となります。このリスクは、各 View Composer インスタンスにも当てはまります。(各 View Composer インスタンスおよび vCenter Server インスタンス間に 1 対 1 のマッピングがあります。) 以下のいずれかの製品を使用して、vCenter Server または View Composer の障害による影響を少なくできます。

- VMware vSphere High Availability (HA)
- 互換性のあるサードパーティのフェイルオーバー製品

重要： これらのフェイルオーバー戦略のいずれかを使用するには、vCenter Server インスタンスを vCenter Server インスタンスが管理するクラスタの一部となる仮想マシンにインストールしないでください。

vCenter Server フェイルオーバー用にこれらを自動化するオプションに加えて、問題が発生したサーバを新しい仮想マシンや物理サーバに再構築することを選択することもできます。重要な情報の多くは、vCenter Server データベースに格納されています。

リスク許容度は、ポッド設計で vCenter Server インスタンスを 1 つ使用するか、複数使用するかを決定する上で大切な要素です。すべてのデスクトップの電源および修理を同時に行うなどのデスクトップ管理作業を実行する能力が必要である場合、複数の vCenter Server インスタンスを展開することによって、同時に停止するデスクトップの影響が広がらないようにすべきです。管理操作やプロビジョニング操作のためにデスクトップ環境を長期間に渡って使用できなくても許容できる場合や、手動の再構築プロセスを使用することを選択する場合は、ポッドに単一の vCenter Server インスタンスを展開できます。

電源、プロビジョニング、および修理作業の頻度

特定の仮想マシン デスクトップの電源、プロビジョニング、および修理作業は、管理者によってのみ開始され、通常は予測可能かつ制御可能で、あらかじめ決めたメンテナンス時間に限定できます。その他の仮想マシン デスクトップの電源および修理作業は、ログオフのリフレッシュまたはログオフのサスペンド設定を使用してユーザーによって起動され、またはアイドル状態の ESXi ホストをパワーオフするためにユーザーが介入しない時間帯に Distributed Power Management (DPM) を使用するなどのスクリプト動作により実行されます。

Horizon 7 の設計でユーザーが起動した電源および修理作業を必要としない場合、1 つの vCenter Server インスタンスで恐らく十分です。ユーザーが起動する電源操作や修理操作の頻度が高くなければ、大量の操作がキューに蓄積されることによって、vCenter Server が要求された操作を定義されている同時操作設定制限内に完了するのを待機して Horizon 接続サーバがタイムアウトになることはありません。

多くの顧客はフローティング プールを導入して、Refresh on logoff (ログオフ時に更新) 設定を選択して、以前のセッションの無効なデータを取り除いたデスクトップを常に提供します。無効なデータの例には、pagefile.sys または Windows temp ファイルでの不要なメモリ ページが含まれます。フローティング プールは、デスクトップをクリーンな状態に頻繁にリセットすることによって、マルウェアの影響を最小限にすることもできます。

一部の顧客はデスクトップが使用されていない間は電源をオフにするように Horizon 7 を構成して電気使用量を削減し、これにより vSphere DRS (Distributed Resources Scheduler) は、動作している仮想マシンを最小数の ESXi ホストに統合できます。VMware Distributed Power Management (DPM) はアイドル状態のホストの電源をオフにします。このようなシナリオでは、複数の vCenter Server インスタンスの方が、操作のタイムアウトを回避するために必要な高頻度の電源操作および修理操作に適しています。

インフラストラクチャの簡素化

大規模 Horizon 7 設計における単一の vCenter Server インスタンスには、ゴールデン マスター イメージや親仮想マシンの管理が一箇所ですむ、1 つの vCenter Server ビューが Horizon Administrator コンソール ビューに一致する、本番のバックエンド データベースおよびデータベース サーバが少なくすむ、などの魅力的な利点があります。ディザスタ リカバリ計画は、複数のインスタンスよりも 1 つの vCenter Server の方が簡素になります。メンテナンス期間や電源および修理操作の頻度などの複数の vCenter Server インスタンスの利点と、親仮想マシン イメージを管理する追加の管理オーバーヘッドや必要となるインフラストラクチャ コンポーネント数の増加などの欠点を比較して確認してください。

ハイブリッド アプローチが有益である場合があります。1 つの vCenter Server インスタンスで管理される非常に大きく相対的に静的なプールと、複数の vCenter Server インスタンスによって管理されるいくつかの小さくより動的なデスクトップ プールを選択できます。既存の大規模ポッドをアップグレードするための最適な戦略は、既存のポッドの VMware ソフトウェア コンポーネントを最初にアップグレードすることです。ポッド設計を変更する前に、最新バージョンの電源、プロビジョニング、および修理操作による改善の影響を計り、より少ない vCenter Server インスタンスにおけるより大規模なデスクトップ プールの適切なバランスを見つけるために、デスクトップ プールのサイズを増加する実験を後で行います。

セキュリティ機能の計画

5

Horizon 7 は、企業の機密データを保護するための強力なネットワーク セキュリティ機能を備えています。セキュリティを強化するため、Horizon 7 を他社製のユーザー認証ソリューションと統合したり、セキュリティ サーバを使用したり、制限付き資格の機能を実装したりできます。

重要： Horizon 6 バージョン 6.2 以降では、FIPS（米国連邦情報処理規格）140-2 準拠のアルゴリズムを使用して暗号化操作を実行できます。これらのアルゴリズムの使用を有効にするには、Horizon 7 を FIPS モードでインストールします。FIPS モードでは、一部の機能がサポートされません。詳細については、『Horizon 7 のインストール』を参照してください。

この章には、次のトピックが含まれています。

- クライアント接続について
- ユーザー認証方法の選択
- リモート デスクトップ アクセスの制限
- グループ ポリシー設定を使用したリモート デスクトップおよびアプリケーションのセキュリティ保護
- スマート ポリシー の使用
- クライアント システムのセキュリティを保護するためのベスト プラクティスの実装
- 管理者ロールの割り当て
- セキュリティ サーバを使用するための準備
- 通信プロトコルの概要

クライアント接続について

Horizon Client および Horizon Administrator は、安全な HTTPS 接続を介して Horizon 接続サーバ ホストと通信します。接続サーバ上のサーバ証明書についての情報は、クライアントとサーバ間の TLS ハンドシェイクの一部としてクライアントに伝えられます。

ユーザー認証とリモート デスクトップおよびリモート アプリケーションの選択に使用される最初の Horizon Client 接続は、ユーザーが Horizon Client を開き、接続サーバ、セキュリティ サーバ、または Unified Access Gateway ホストの完全修飾ドメイン名を入力するときに作成されます。Horizon Administrator 接続は、管理者が Web ブラウザに Horizon Administrator の URL を入力したときに作成されます。

接続サーバのインストール時に、デフォルトの TLS サーバ証明書が生成されます。デフォルトでは、TLS クライアントが Horizon Administrator などの安全なページにアクセスすると、この証明書が提示されます。

デフォルトの証明書はテストに使用できますが、できるだけ早く独自の証明書に交換する必要があります。デフォルトの証明書は、商用の証明機関 (CA) によって署名されていません。承認されていない証明書を使用すると、信頼されていないパーティにサーバを装ってトラフィックを傍受される可能性があります。

■ PCoIP および Blast Secure Gateway を使用するクライアント接続

VMware の PCoIP または Blast Extreme 表示プロトコルを使用するリモート デスクトップまたはアプリケーションにクライアントが接続された場合、Horizon Client は Horizon 接続サーバ インスタンス、セキュリティ サーバ、または Unified Access Gateway アプライアンス上の該当する Secure Gateway コンポーネントへの 2 番目の接続を確立できます。この接続によって、インターネットからリモート デスクトップとリモート アプリケーションにアクセスする場合に必要なレベルのセキュリティと接続性が提供されます。

■ Microsoft RDP を使用するトンネル クライアント接続

Microsoft RDP 表示プロトコルを使用するリモート デスクトップにユーザーが接続すると、Horizon Client は Horizon 接続サーバ ホストへの第 2 の HTTPS 接続を確立できます。この接続は、RDP データを送信するためのトンネルになるため、トンネル接続と呼ばれます。

■ 直接クライアント接続

管理者は、リモート デスクトップおよび公開アプリケーション セッションが、接続サーバ ホストをバイパスしてクライアント システムと公開アプリケーションまたはデスクトップ仮想マシンとの間で直接確立されるように Horizon 接続サーバを構成できます。このタイプの接続を直接クライアント接続といいます。

PCoIP および Blast Secure Gateway を使用するクライアント接続

VMware の PCoIP または Blast Extreme 表示プロトコルを使用するリモート デスクトップまたはアプリケーションにクライアントが接続された場合、Horizon Client は Horizon 接続サーバ インスタンス、セキュリティ サーバ、または Unified Access Gateway アプライアンス上の該当する Secure Gateway コンポーネントへの 2 番目の接続を確立できます。この接続によって、インターネットからリモート デスクトップとリモート アプリケーションにアクセスする場合に必要なレベルのセキュリティと接続性が提供されます。

セキュリティ サーバと Unified Access Gateway アプライアンスは、PCoIP Secure Gateway コンポーネントと Blast Secure Gateway コンポーネントを含みます。これには、次の利点があります。

- 企業のデータセンターに入ることができるリモート デスクトップおよびアプリケーションのトラフィックが、強力な認証を経たユーザーのトラフィックのみになります。
- ユーザーはアクセスが許可されているリソースにのみアクセスできます。
- PCoIP Secure Gateway 接続は PCoIP をサポートし、Blast Secure Gateway 接続は Blast Extreme をサポートします。どちらも、ビデオ表示パケットを TCP の代わりに UDP にカプセル化することによってネットワークの使用効率を高める、高度なリモート表示プロトコルです。
- PCoIP と Blast Extreme は、デフォルトで AES-128 の暗号化により安全性が確保されます。ただし、暗号化方式は AES-256 に変更できます。

- 表示プロトコルがいずれかのネットワーク コンポーネントによってブロックされない限り、VPN は必要ありません。たとえば、ホテルの部屋の中から自社のリモート デスクトップまたはリモート アプリケーションにアクセスを試みた場合、そのホテルが使用しているプロキシは UDP パケットを渡すように構成されていないかもしれません。

詳細については、[DMZ ベースのセキュリティ サーバのファイアウォール ルール](#)を参照してください。

セキュリティ サーバは、Windows Server 2008 R2 および Windows Server 2012 R2 オペレーティング システム上で実行され、64 ビット アーキテクチャを最大限に活用します。このセキュリティ サーバは、AES New Instructions (AESNI) をサポートし、高度に最適化された暗号化および暗号化解除のパフォーマンスを実現する Intel プロセッサの利点も活かします。

Unified Access Gateway 仮想アプライアンスの詳細については、『Unified Access Gateway の導入および設定』を参照してください。

Microsoft RDP を使用するトンネル クライアント接続

Microsoft RDP 表示プロトコルを使用するリモート デスクトップにユーザーが接続すると、Horizon Client は Horizon 接続サーバ ホストへの第 2 の HTTPS 接続を確立できます。この接続は、RDP データを送信するためのトンネルになるため、トンネル接続と呼ばれます。

トンネル接続には次の利点があります。

- RDP データが HTTPS によってトンネリングされ、SSL を使用して暗号化されます。この強力なセキュリティ プロトコルは、オンライン バンキングやクレジット カードの支払いに使用されるような他の安全な Web サイトで提供されているセキュリティに一致しています。
- クライアントは単一の HTTPS 接続を介して複数のデスクトップにアクセスできるため、プロトコル全体のオーバーヘッドが削減されます。
- それらの HTTPS 接続は Horizon 7 によって管理されるため、基盤となるプロトコルの信頼性が大幅に向上します。ユーザーが一時的にネットワーク接続を失った場合に、ネットワーク接続が復元された後、ユーザーが再接続して再度ログインしなくても HTTP 接続が再確立され、RDP 接続が自動的に再開されます。

接続サーバ インスタンスの標準展開では、HTTPS の安全な接続の終点は接続サーバになります。DMZ 展開では、HTTPS の安全な接続の終点はセキュリティ サーバまたは Unified Access Gateway アプライアンスになります。DMZ 展開とセキュリティ サーバの詳細については [セキュリティ サーバを使用するための準備](#) を参照してください。

PCoIP または Blast Extreme 表示プロトコルを使用するクライアントは USB リダイレクトおよびマルチメディア リダイレクト (MMR) のアクセラレーションのためにトンネル接続を使用できますが、他のすべてのデータについては、PCoIP では PCoIP Secure Gateway が、Blast Extreme では Blast Secure Gateway が、セキュリティ サーバまたは Unified Access Gateway アプライアンス上で使用されます。詳細については、[PCoIP および Blast Secure Gateway を使用するクライアント接続](#) を参照してください。

Unified Access Gateway 仮想アプライアンスの詳細については、『Unified Access Gateway の導入および設定』を参照してください。

直接クライアント接続

管理者は、リモート デスクトップおよび公開アプリケーション セッションが、接続サーバ ホストをバイパスしてクライアント システムと公開アプリケーションまたはデスクトップ仮想マシンとの間で直接確立されるように Horizon 接続サーバを構成できます。このタイプの接続を直接クライアント接続といいます。

直接クライアント接続でも、HTTPS 接続をクライアントと接続サーバ ホストとの間に確立し、ユーザーが認証してリモート デスクトップおよび公開アプリケーションを選択できますが、その第 2 の HTTPS 接続（トンネル接続）は使用されません。

PCoIP および Blast Extreme への直接接続には、次の組み込みのセキュリティ機能が使用されます。

- Advanced Encryption Standard (AES) 暗号化のサポート。これはデフォルトで有効になり、IP Security (IPsec) が使用されます。
- サードパーティ製 VPN クライアントのサポート

Microsoft RDP 表示プロトコルを使用するクライアントでは、展開が企業ネットワーク内に限定される場合にのみリモート デスクトップへの直接クライアント接続が適切です。直接クライアント接続を使用すると、RDP トラフィックがその接続を介してクライアントとデスクトップ仮想マシンの間で暗号化されないまま送信されます。

ユーザー認証方法の選択

Horizon 7 は、ユーザーを認証および管理するために既存の Active Directory インフラストラクチャを利用します。セキュリティを強化するために、Horizon 7 を RSA SecurID および RADIUS などの 2 要素認証ソリューションおよびスマート カード認証ソリューションと統合できます。

■ Active Directory 認証

各 Horizon 接続サーバ インスタンスは Active Directory ドメインに参加しており、ユーザーは参加しているドメインを利用するために Active Directory に対して認証されます。信頼契約の存在する追加ユーザー ドメインがある場合、ユーザーはそのドメインに対しても認証されます。

■ 2 要素認証の使用

ユーザーが RSA SecurID 認証または RADIUS (Remote Authentication Dial-In User Service) 認証を使用しなければならないように、Horizon 接続サーバ インスタンスを構成できます。

■ スマート カード認証

スマート カードは、コンピュータ チップが埋め込まれた小さなプラスチック カードです。多くの官公庁や大企業が、そのコンピュータ ネットワークにアクセスするユーザーの認証にスマート カードを使用しています。米国国防省が使用するスマート カードの 1 種には、Common Access Card (CAC) というカードがあります。

■ Windows ベースの Horizon Client で使用できる現在のユーザーとしてログイン機能を使用

Horizon Client for Windows で、ユーザーが [オプション] メニューの [現在のユーザーとしてログイン] チェックボックスを選択すると、クライアント システムへのログイン時に入力した認証情報が Horizon Connection Server インスタンスとリモート デスクトップの認証で使用されます。追加のユーザー認証は必要ありません。

Active Directory 認証

各 Horizon 接続サーバ インスタンスは Active Directory ドメインに参加しており、ユーザーは参加しているドメインを利用するために Active Directory に対して認証されます。信頼契約の存在する追加ユーザー ドメインがある場合、ユーザーはそのドメインに対しても認証されます。

たとえば、接続サーバ インスタンスがドメイン A のメンバーであり、ドメイン A とドメイン B の間に信頼契約が存在する場合、ドメイン A とドメイン B の両方のユーザーが Horizon Client を使用して View 接続サーバ インスタンスに接続できます。

同様に、ドメイン混在環境でドメイン A と MIT Kerberos レルムの間に信頼契約が存在する場合、Kerberos レルムのユーザーは Horizon Client で接続サーバに接続するときに Kerberos レルム名を選択できます。

次の Active Directory ドメインにユーザーとグループを配置できます。

- 接続サーバ ドメイン
- 接続サーバ ドメインとの双方向の信頼関係がある別のドメイン
- 一方向の外部またはレルムの信頼関係で接続サーバ ドメインによって信頼されている、接続サーバ ドメインとは異なるフォレスト内のドメイン
- 一方向または双方向の推移的なフォレストの信頼関係で接続サーバ ドメインによって信頼されている、接続サーバ ドメインとは異なるフォレスト内のドメイン

接続サーバは、ホストが存在するドメインから始めて、信頼関係をたどって、アクセスできるドメインを決定します。小規模で、接続が安定しているドメインのセットであれば、接続サーバは短時間でドメインの完全なリストを決定できますが、ドメインの数が増えたり、ドメイン間の接続が不十分であったりすると、要する時間は長くなります。リストには、リモート デスクトップおよびアプリケーションにログインしたユーザーに提供しない方がよいドメインも含まれる場合があります。

管理者は、vdmadmin コマンドライン インターフェイスを使用して、ドメインのフィルタ処理を構成できます。フィルタを使用すると、接続サーバ インスタンスが検索してユーザーに表示するドメインを制限できます。詳細については、『Horizon 7 管理ガイド』を参照してください。

ログインを許可する時間を制限したり、パスワードの失効日を設定するなどのポリシーも、Active Directory の既存の運用手順に従って処理されます。

2 要素認証の使用

ユーザーが RSA SecurID 認証または RADIUS (Remote Authentication Dial-In User Service) 認証を使用しなければならないように、Horizon 接続サーバ インスタンスを構成できます。

- RADIUS サポートは、さまざまな代替 2 要素トークン ベースの認証オプションを提供します。
- Horizon 7 は、オープン標準拡張インターフェイスも提供して、サードパーティ ソリューション プロバイダが詳細認証拡張を Horizon 7 に統合できるようにします。

RSA SecurID や RADIUS などの 2 要素認証ソリューションは、個別のサーバにインストールされた認証マネージャと連携するため、接続サーバ ホストにアクセスできるようにこれらのサーバを構成する必要があります。たとえば RSA SecurID を使用する場合、認証マネージャは RSA Authentication Manager になります。RADIUS を使用する場合、認証マネージャは RADIUS サーバになります。

2 要素認証を使用するには、認証マネージャに登録されている RSA SecurID トークンなどのトークンがユーザーごとに必要です。2 要素認証トークンは、一定の間隔で認証コードを生成するハードウェアまたはソフトウェアです。多くの場合、認証には PIN と認証コードの両方に関する知識が必要です。

接続サーバ インスタンスが複数ある場合は、一部のインスタンスで 2 要素認証を構成し、他のインスタンスでは別のユーザー認証方法を構成することができます。たとえば、インターネットを介して企業ネットワークの外からリモート デスクトップとアプリケーションにアクセスするユーザーのみに 2 要素認証を構成できます。

Horizon 7 は RSA SecurID Ready プログラムによって認定されており、新規 PIN モード、次のトークン コードモード、RSA Authentication Manager、負荷分散など、SecurID のあらゆる機能をサポートしています。

スマート カード認証

スマート カードは、コンピュータ チップが埋め込まれた小さなプラスチック カードです。多くの官公庁や大企業が、そのコンピュータ ネットワークにアクセスするユーザーの認証にスマート カードを使用しています。米国国防省が使用するスマート カードの 1 種には、Common Access Card (CAC) というカードがあります。

管理者は、個別の接続サーバ インスタンスでスマート カード認証を有効にできます。接続サーバ インスタンスでのスマート カードの使用を有効にすると、通常は信用ストアにルート証明書が追加された後、接続サーバの設定が変更されます。

スマート カード認証を使用するクライアント接続を含むすべてのクライアント接続は TLS/SSL が有効になっています。

スマート カードを使用するには、クライアント マシンにスマート カード ミドルウェアおよびスマート カード リーダが必要です。スマート カードに証明書をインストールするには、コンピュータを登録ステーションとして動作するように設定する必要があります。特定のタイプの Horizon Client でスマート カードがサポートされているかどうかについては、<https://docs.vmware.com/jp/VMware-Horizon-Client/index.html> にある Horizon Client のドキュメントを参照してください。

Windows ベースの Horizon Client で使用できる現在のユーザーとしてログイン機能を使用

Horizon Client for Windows で、ユーザーが [オプション] メニューの [現在のユーザーとしてログイン] チェックボックスを選択すると、クライアント システムへのログイン時に入力した認証情報が Horizon Connection Server インスタンスとリモート デスクトップの認証で使用されます。追加のユーザー認証は必要ありません。

この機能をサポートするため、ユーザー認証情報は Connection Server インスタンスとクライアント システムの両方に格納されます。

- Connection Server インスタンスで、ユーザー認証情報は、ユーザー名、ドメイン、オプションの UPN とともにユーザー セッションに暗号化されて保存されます。認証情報は、認証が行われると追加され、セッション オブジェクトが破棄されると削除されます。セッション オブジェクトは、ユーザーがログアウトするか、セッションがタイムアウトになるか、認証が失敗した場合に破棄されます。セッション オブジェクトは揮発性メモリに保存され、Horizon LDAP またはディスク ファイルには保存されません。

- Horizon Client の [オプション] メニューで [現在のユーザーとしてログイン] を選択したときに渡されるユーザー ID と認証情報が Connection Server インスタンスで受け入れられるように、Connection Server インスタンスで [現在のユーザーとしてのログインを受け入れる] 設定を有効にします。

重要： この設定を有効にする前に、セキュリティ リスクを理解しておく必要があります。『Horizon 7 のセキュリティ』の「ユーザー認証のセキュリティ関連のサーバ設定」を参照してください。

- クライアント システムで、ユーザー認証情報は暗号化され、Horizon Client のコンポーネントである Authentication Package のテーブルに保存されます。認証情報は、ユーザーのログイン時にテーブルに追加され、ユーザーのログアウト時にテーブルから削除されます。テーブルは揮発性メモリに存在します。

管理者は、Horizon Client のグループ ポリシー設定を使用して、[オプション] メニューの [現在のユーザーとしてログイン] を使用可能にするかどうかを制御し、そのデフォルト値を設定することができます。さらに、管理者はグループ ポリシーを使用して、ユーザーが Horizon Client の [現在のユーザーとしてログイン] をオンにした場合に渡されるユーザー ID と認証情報を受け入れる Connection Server インスタンスを指定することもできます。

現在のユーザーとしてログイン機能を使用して Connection Server にログインすると、再帰的なロック解除機能が有効になります。再帰的なロック解除機能を使用すると、クライアント マシンのロックが解除された後で、すべてのリモート セッションのロックを解除できます。管理者は、Horizon Client の [クライアント マシンのロックを解除するときにリモート セッションのロックを解除します] グローバル ポリシー設定で再帰的なロック解除機能を制御できます。Horizon Client のグローバル ポリシー設定の詳細については、[VMware Horizon Client ドキュメント Web ページ](#)にある Horizon Client ドキュメントを参照してください。

「現在のユーザーとしてログイン」機能には次の制限と要件があります。

- Connection Server インスタンスでスマート カード認証が [必須] に設定されている場合、Connection Server インスタンスに接続する際に [現在のユーザーとしてログイン] を選択したユーザーの認証が失敗します。これらのユーザーは、Connection Server にログインする際にスマート カードと PIN を使用して再認証する必要があります。
- クライアントがログインするシステムの時間と、Connection Server ホストの時間が同期している必要があります。
- クライアント システムで、デフォルトの [ネットワーク経由でコンピュータへアクセス] ユーザー権限割り当てを変更する場合は、VMware ナレッジベース (KB) の記事 1025691 の説明に従って変更する必要があります。
- クライアント マシンは、会社の Active Directory サーバと通信できる必要があります。キャッシュされた認証情報は認証に使用されません。たとえば、ユーザーが社外のネットワークからクライアント マシンにログインすると、キャッシュされた認証情報が認証に使用されます。その後、ユーザーが最初に VPN 接続を確立しないでセキュリティ サーバや Connection Server インスタンスに接続しようとすると、認証情報の入力が必要で、現在のユーザーとしてログイン機能は機能しません。

リモート デスクトップ アクセスの制限

制限付き資格の機能を使用し、ユーザーが接続する Horizon 接続サーバ インスタンスに基づいてリモート デスクトップ アクセスを制限できます。

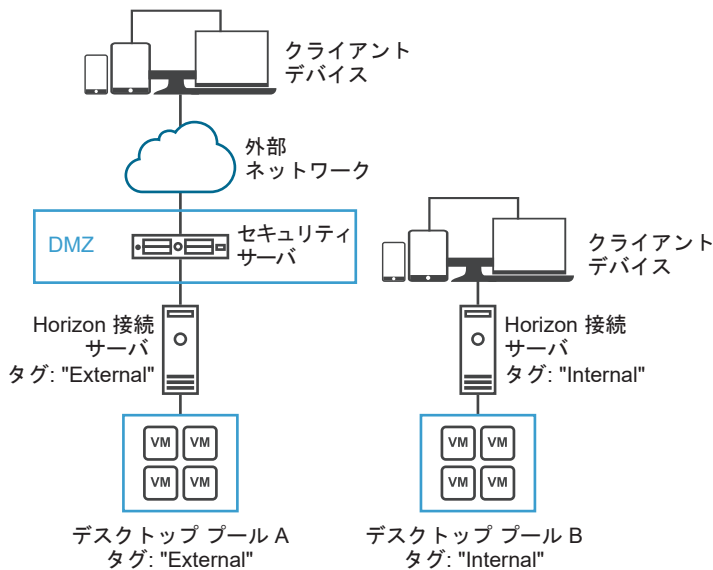
制限付き資格では、1 つ以上のタグを接続サーバ インスタンスに割り当てます。その後、デスクトップ プールを構成するときに、デスクトップ プールにアクセスできるようにする接続サーバ インスタンスのタグを選択します。ユーザーがタグ付きの接続サーバ インスタンスにログインするとき、ユーザーは少なくとも 1 つのタグが一致するか、タグがないデスクトップ プールにのみアクセスできます。

たとえば、Horizon 7 の展開に 2 つの接続サーバ インスタンスが含まれるものとしします。第 1 のインスタンスは内部ユーザーをサポートします。第 2 のインスタンスはセキュリティ サーバと対になって、外部ユーザーをサポートします。外部ユーザーが特定のデスクトップにアクセスできないようにするには、次のように制限付き資格を設定します。

- タグ「Internal」を、内部ユーザーをサポートする接続サーバ インスタンスに割り当てます。
- タグ「External」を、セキュリティ サーバと対になって外部ユーザーをサポートする接続サーバ インスタンスに割り当てます。
- 内部ユーザーのみがアクセスできるようにするデスクトップ プールに、「Internal」タグを割り当てます。
- 外部ユーザーのみがアクセスできるようにするデスクトップ プールに、「External」タグを割り当てます。

外部ユーザーは、External というタグの付いた接続サーバを使用してログインするので、Internal というタグの付いたデスクトップ プールにはアクセスできません。また、内部ユーザーは、Internal というタグの付いた接続サーバを使用してログインするので、External というタグの付いたデスクトップ プールにはアクセスできません。図 5-1. 制限付き資格の例は、この構成を示しています。

図 5-1. 制限付き資格の例



制限付き資格を使用して、特定の接続サーバ インスタンスに対して構成されているユーザー認証方法に基づいて、デスクトップ アクセスを制御することもできます。たとえば、スマート カードで認証されているユーザーのみが特定のデスクトップ プールを使用できるようにすることができます。

制限付き資格の機能は、タグの一致を適用するだけです。特定のクライアントが特定の接続サーバ インスタンスを通して接続するように、ネットワーク トポロジを設計する必要があります。

グループ ポリシー設定を使用したリモート デスクトップおよびアプリケーションのセキュリティ保護

Horizon 7 には、リモート デスクトップおよびアプリケーションのセキュリティ保護に使用できるセキュリティ関連グループ ポリシー設定を備えたグループ ポリシー管理 ADMX テンプレートが含まれています。

たとえば、グループ ポリシー設定を使用して、次のタスクを実行できます。

- ユーザーが Horizon Client for Windows の [現在のユーザーとしてログイン] チェック ボックスをオンにした場合に渡されるユーザー ID と認証情報を受け入れる接続サーバ インスタンスを指定する。
- Horizon Client でシングル サインオン スマート カード認証を有効にする。
- Horizon Client でサーバ TLS 証明書確認を構成する。
- ユーザーが Horizon Client コマンド ライン オプションによって認証情報を指定できないようにする。
- Horizon Client 以外のシステムが RDP を使用してリモート デスクトップに接続できないようにする。このポリシーは、接続が Horizon Client によって管理される必要がある、つまりユーザーがリモート デスクトップに接続するために Horizon 7 を使用する必要があることを意味します。

リモート デスクトップおよび Horizon Client グループ ポリシー設定の使用法については、『Horizon 7 でのリモート デスクトップ機能の構成』を参照してください。

スマート ポリシー の使用

スマート ポリシー は、公開デスクトップまたはアプリケーションのユーザー環境設定に使用できます。また、コンピュータの起動時またはセッションの再接続時に適用されるコンピュータ環境設定にも使用できます。

公開デスクトップまたはアプリケーションの USB リダイレクト、仮想印刷、クリップボード リダイレクト、クライアント ドライブ リダイレクト、Web および Chrome ファイル転送機能、帯域幅プロファイルの動作を制御するユーザー環境設定のポリシーを作成できます。ユーザー環境設定の Horizon スマート ポリシーはログイン時に適用されますが、セッションの再接続時に更新できます。ユーザーがセッションに再接続したときに Horizon スマート ポリシーを再適用するには、トリガされるタスクを設定できます。

エンドユーザーがコンピュータを起動したときに Dynamic Environment Manager によってコンピュータ環境設定に適用されるポリシーを作成できます。この Horizon スマート ポリシーにより、Flash マルチメディア リダイレクト、統合印刷、USB リダイレクトの動作を制御できます。コンピュータ環境設定の Horizon スマート ポリシーはコンピュータの起動時に適用されますが、セッションの再接続時に更新できます。

スマート ポリシー により、特定の条件が満たされる場合にのみ有効になるポリシーを作成できます。たとえば、ユーザーが企業のネットワーク以外からリモート デスクトップに接続している場合はクライアント ドライブ リダイレクト機能を無効にするポリシーを設定できます。

スマート ポリシー 機能では Dynamic Environment Manager が必要となります。詳細については、Horizon 7 でのリモート デスクトップ機能の構成のスマート ポリシーに関するトピックを参照してください。

クライアント システムのセキュリティを保護するためのベスト プラクティスの実装

次のベスト プラクティスを実装して、クライアント システムを保護します。

- クライアント システムが、一定期間動作していない場合にスリープ状態になり、コンピュータをアクティブにする前にユーザーがパスワードを入力する必要があるように構成されていることを確認してください。
- クライアント システムの起動時に、ユーザーはユーザー名とパスワードを入力する必要があります。クライアント システムで自動ログインを許可するように構成しないでください。
- Mac クライアント システムの場合、キーチェーンとユーザー アカウントに異なるパスワードを設定することを考慮してください。パスワードが異なる場合、システムが自動的にパスワードを入力する前に、ユーザーに入力が必要とされます。さらに、FileVault 保護を有効にすることも考慮してください。

Horizon 7 が提供するすべてのセキュリティ機能の正確なリファレンスについては、『Horizon 7 セキュリティ ガイド』を参照してください。

管理者ロールの割り当て

Horizon 7 環境の重要な管理タスクは、Horizon Administrator を使用できるユーザーとそれらのユーザーが実行可能なタスクを決定することです。

Horizon Administrator でタスクを実行する許可は、管理者ロールと権限から構成されるアクセス制御システムによって管理します。ロールは権限のコレクションです。権限は、ユーザーへのデスクトップ プールに対する資格の付与や設定の変更などの特定のアクションを実行する機能を与えます。さらに、権限は、管理者が Horizon Administrator で表示できるものも制御します。

管理者は Horizon Administrator でフォルダを作成してデスクトップ プールを再分割し、特定のデスクトップ プールの管理を別の管理者に委任できます。管理者がフォルダ内のリソースへの管理者アクセスを構成するには、そのフォルダに対するロールをユーザーに割り当てます。管理者は、ロールを割り当てたフォルダに存在するリソースのみアクセスできます。管理者がフォルダに対して持つロールによって、管理者がそのフォルダ内のリソースに対して持つアクセスのレベルが決定します。

Horizon Administrator には、一連の定義済みのロールがあります。管理者は、選択した権限を組み合わせでカスタム ロールを作成することもできます。

セキュリティ サーバを使用するための準備

セキュリティ サーバは、接続サーバ機能のサブセットを実行する、Horizon 接続サーバの特殊なインスタンスです。セキュリティ サーバを使用すると、インターネットと内部ネットワークとの間にセキュリティのレイヤを追加できます。

重要： Horizon 6 バージョン 6.2 以降のリリースでは、View セキュリティ サーバの代わりに Unified Access Gateway アプライアンスを使用できます。Unified Access Gateway アプライアンスは、安全なアクセスに対応するようにカスタマイズされた Linux アプライアンスがベースの堅牢な仮想アプライアンスとしてデプロイされます。Unified Access Gateway 仮想アプライアンスの詳細については、『Unified Access Gateway の導入および設定』を参照してください。

セキュリティ サーバは DMZ 内に存在し、信頼されるネットワーク内の接続に対してプロキシ ホストの役割を果たします。各セキュリティ サーバは接続サーバのインスタンスと対になっていて、すべてのトラフィックをそのインスタンスに転送します。複数のセキュリティ サーバを 1 台の 接続サーバ と組み合わせることができます。この設計では、公共のインターネットから接続サーバ インスタンスを遮断し、保護されていないすべてのセッション要求が強制的にセキュリティ サーバを通過するようにして、セキュリティのレイヤーを追加します。

DMZ ベースのセキュリティ サーバの展開では、クライアントが DMZ 内のセキュリティ サーバに接続できるようにファイアウォール上で数個のポートを開く必要があります。また、セキュリティ サーバと内部ネットワーク内の接続サーバ インスタンスが通信できるように、ポートを構成する必要があります。具体的なポートの詳細については、[DMZ ベースのセキュリティ サーバのファイアウォール ルール](#)を参照してください。

内部ネットワーク内からはユーザーが任意の接続サーバ インスタンスに直接接続できるため、LAN ベースの展開にはセキュリティ サーバを実装する必要はありません。

注： セキュリティ サーバは PCoIP Secure Gateway コンポーネントおよび Blast Secure Gateway コンポーネントを含むので、PCoIP または Blast Extreme 表示プロトコルを使用するクライアントは VPN ではなくセキュリティ サーバを使用できます。

PCoIP を使用するための VPN のセットアップについては、Technical Resource Center (<http://www.vmware.com/products/view/resources.html>) の「Technology Partner Resources」セクションに記載されている VPN ソリューションの概要を参照してください。

セキュリティ サーバ展開のベスト プラクティス

DMZ でセキュリティ サーバを運用する場合、次のベスト プラクティスのセキュリティ ポリシーおよび手順に従ってください。

DMZ Virtualization with VMware Infrastructure』ホワイト ペーパーに、仮想 DMZ のベスト プラクティスの例を紹介しています。このホワイト ペーパーの推奨事項の多くは、物理 DMZ にも適用されます。

フレーム ブロードキャストの範囲を制限するには、セキュリティ サーバと組み合わせた Horizon 接続サーバ インスタンスを、分離されたネットワークに展開する必要があります。このトポロジによって、内部ネットワーク上の悪意あるユーザーによるセキュリティ サーバと Horizon 接続サーバ インスタンス間の通信の監視を防止することができます。

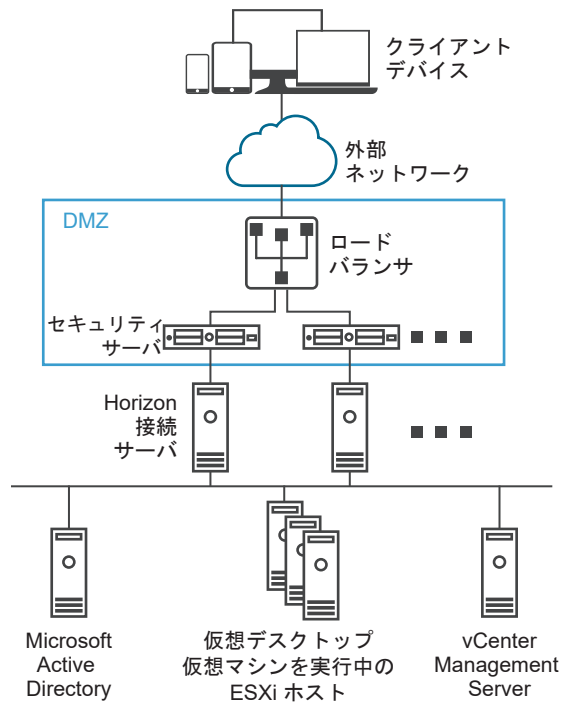
または、ネットワーク スイッチの高度なセキュリティ機能を使用して、セキュリティ サーバと Horizon 接続サーバの通信の悪意ある監視を防止し、ARP キャッシュ ポイズニングなどの監視攻撃に対して保護することもできます。詳細については、お使いのネットワーク機器の管理マニュアルを参照してください。

セキュリティ サーバのトポロジ

複数の異なるセキュリティ サーバ トポロジを実装できます。

図 5-2. DMZ 内の負荷分散されたセキュリティ サーバ のトポロジは、ロード バランスされた 2 台のセキュリティ サーバを DMZ に配置した高可用性環境を示しています。これらのセキュリティ サーバは、内部ネットワーク内の 2 つの Horizon 接続サーバ インスタンスと通信します。

図 5-2. DMZ 内の負荷分散されたセキュリティ サーバ

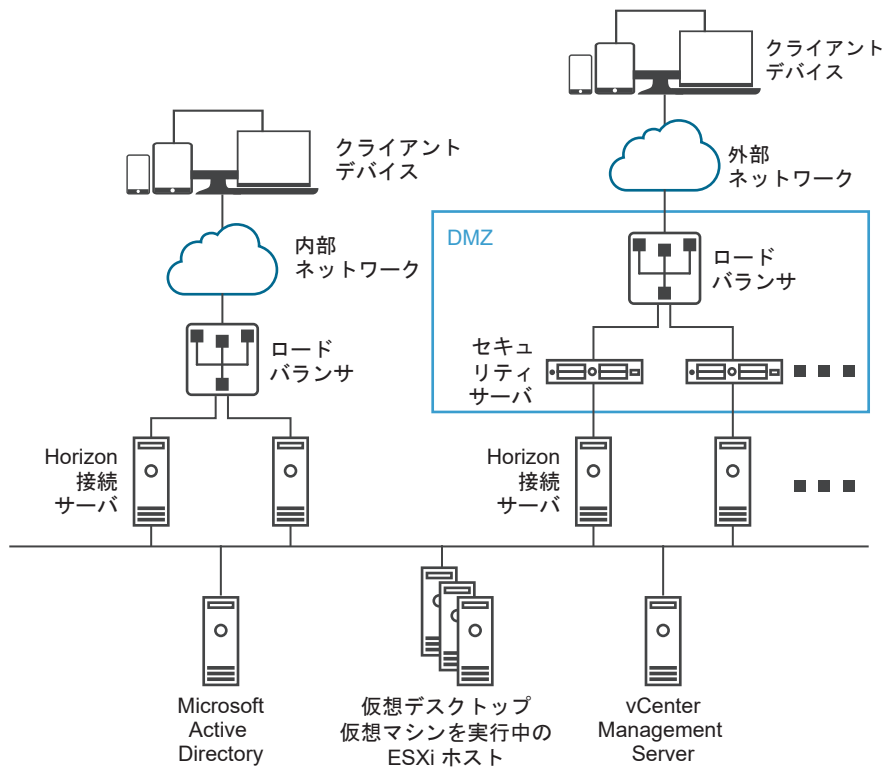


社内ネットワークの外部からユーザーがセキュリティ サーバに接続する場合、リモート デスクトップおよびアプリケーションにアクセスするには、認証に成功する必要があります。DMZ の両側に適切なファイアウォール ルールが適用されるため、このトポロジは、インターネット上のクライアント デバイスからリモート デスクトップおよびアプリケーションにアクセスする場合に適しています。

接続サーバの各インスタンスに複数のセキュリティ サーバを接続できます。DMZ 展開を標準展開と組み合わせて、内部ユーザーと外部ユーザーにアクセスを提供できます。

図 5-3. 複数のセキュリティ サーバ のトポロジは、接続サーバの 4 つのインスタンスが 1 つのグループとして機能する環境を示しています。内部ネットワーク内のインスタンスは内部ネットワークのユーザー専用であり、外部ネットワーク内のインスタンスは外部ネットワークのユーザー専用です。セキュリティ サーバと対になっている接続サーバ インスタンスで RSA SecurID 認証を有効にすると、すべての外部ネットワーク ユーザーに RSA SecurID トークンを使用した認証が義務付けられます。

図 5-3. 複数のセキュリティ サーバ



セキュリティ サーバを複数インストールする場合は、ハードウェアまたはソフトウェアのいずれかの負荷分散ソリューションを実装する必要があります。接続サーバ自体はロード バランシング機能を提供しません。接続サーバは他社製の標準的なロード バランシング ソリューションと連動します。

DMZ ベースのセキュリティ サーバのファイアウォール

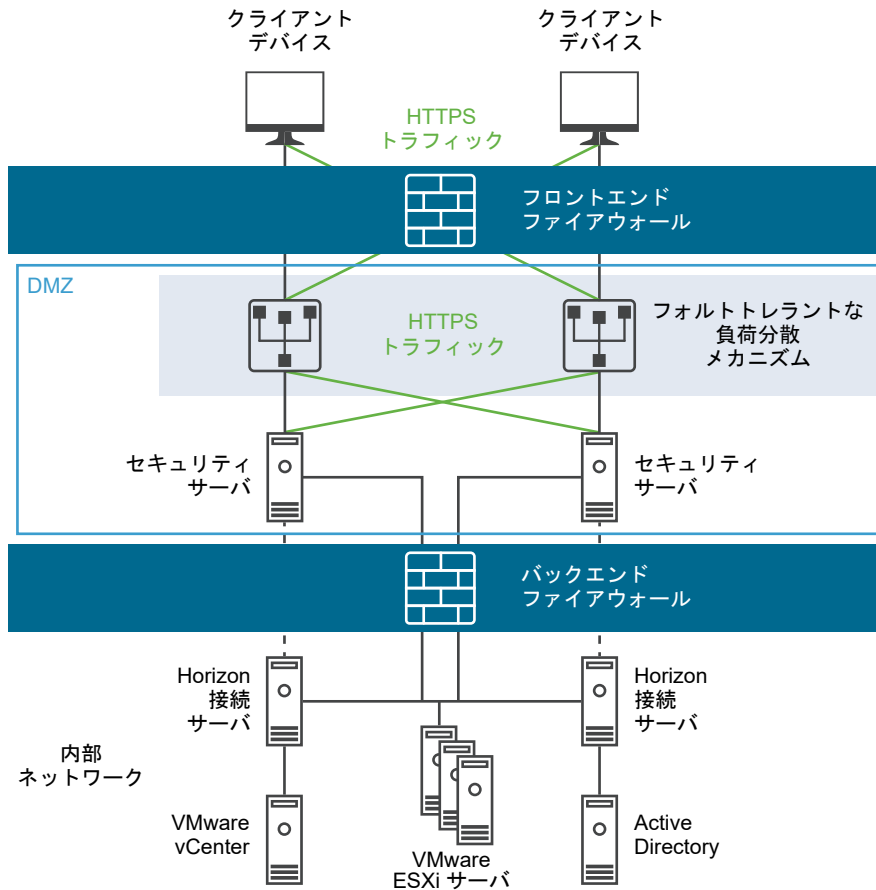
DMZ ベースのセキュリティ サーバの展開には、2 つのファイアウォールを含める必要があります。

- DMZ と内部ネットワークの両方を保護するために、外部ネットワークに接しているフロント エンド ファイアウォールが必要です。外部からのネットワーク トラフィックが DMZ に到達できるように、このファイアウォールを構成します。
- 2 つ目のセキュリティの層を提供するために、DMZ と 内部ネットワークの間のバック エンド ファイアウォールが必要です。DMZ 内のサービスから送信されたトラフィックだけを受け入れるように、このファイアウォールを構成します。

ファイアウォール ポリシーによって DMZ サービスからの受信通信が厳格に制御されるため、内部ネットワークが侵害されるリスクが大幅に軽減されます。セキュリティ サーバの構成に必要なポートの詳細については、『Horizon 7 のセキュリティ』を参照してください。

次の図は、フロントエンド ファイアウォールとバックエンド ファイアウォールを含む構成の例を示しています。

図 5-4. デュアル ファイアウォール トポロジ



DMZ ベースのセキュリティ サーバのファイアウォール ルール

DMZ ベースのセキュリティ サーバには、フロント エンド ファイアウォールとバック エンド ファイアウォールに関する特定のファイアウォール ルールが必要です。インストール中、Horizon 7 サービスは、デフォルトで特定のネットワーク ポートをリッスンするように設定されます。必要に応じて、組織のポリシーに準拠するか競合を回避するために、どのポート番号が使用されるかを変更できます。

重要： その他の詳細およびセキュリティの推奨事項については、『Horizon 7 セキュリティ ガイド』を参照してください。

フロント エンド ファイアウォールのルール

外部のクライアント デバイスが DMZ 内のセキュリティ サーバに接続できるようにするには、フロント エンド ファイアウォールで、トラフィックを特定の TCP ポートおよび UDP ポートで許可する必要があります。[表 5-1. フロント エンド ファイアウォールのルール](#) にフロント エンド ファイアウォールのルールの概要を示します。

表 5-1. フロント エンド ファイアウォールのルール

Source	デフォルト ポート	プロトコル	送信先	デフォルト ポート	注
Horizon Client	すべての TCP	HTTP	セキュリティ サーバ	TCP 80	(オプション) 外部のクライアント デバイスは、TCP ポート 80 の DMZ 内のセキュリティ サーバに接続し、自動的に HTTPS にリダイレクトされます。HTTPS ではなく HTTP を使用した接続をユーザーに許可することに関連するセキュリティ上の考慮事項については、『Horizon 7 セキュリティ ガイド』を参照してください。
Horizon Client	すべての TCP	HTTPS	セキュリティ サーバ	TCP 443	外部クライアント デバイスは、DMZ 内にあるセキュリティ サーバに TCP ポート 443 で接続して、接続サーバ インスタンスおよびリモートデスクトップやアプリケーションと通信します。
Horizon Client	すべての TCP すべての UDP	PCoIP	セキュリティ サーバ	TCP 4172 UDP 4172	外部クライアント デバイスは、DMZ 内にあるセキュリティ サーバに TCP ポート 4172 および UDP ポート 4172 で接続して、PCoIP 経由でリモートデスクトップやアプリケーションと通信します。
セキュリティ サーバ	UDP 4172	PCoIP	Horizon Client	すべての UDP	セキュリティ サーバは、UDP ポート 4172 から PCoIP データを外部クライアント デバイスに送り返します。送信先の UDP ポートは、受信した UDP パケットのソース ポートとなります。このパケットには返信データが含まれるため、通常は、このトラフィックに明示的なファイアウォール ルールを追加する必要はありません。
Horizon Client または クライアント Web ブラウザ	すべての TCP	HTTPS	セキュリティ サーバ	TCP 8443 UDP 8443	外部クライアント デバイスおよび外部 Web クライアント (HTML Access) は、リモート デスクトップと通信するために、HTTPS ポート 8443 の DMZ 内でセキュリティ サーバに接続します。

バック エンド ファイアウォールのルール

セキュリティ サーバが、内部ネットワーク内に存在する各 View 接続サーバ インスタンスと通信できるようにするには、バック エンド ファイアウォールで、受信トラフィックを特定の TCP ポートで許可する必要があります。リモート デスクトップ アプリケーションと接続サーバ インスタンスが互いに通信できるようにするために、バックエンド ファイアウォールの背後で、内部のファイアウォールが同様に構成されている必要があります。[表 5-2. バック エンド ファイアウォールのルール](#)にバックエンド ファイアウォールのルールの概要を示します。

表 5-2. バック エンド ファイアウォールのルール

Source	デフォルト ポート	プロトコル	送信先	デフォルト ポート	注
セキュリティ サーバ	UDP 500	IPSec	接続サーバ	UDP 500	セキュリティ サーバは、UDP ポート 500 で接続サーバ インスタンスと IPSec についてネゴシエートします。
接続サーバ	UDP 500	IPSec	セキュリティ サーバ	UDP 500	接続サーバ インスタンスは、UDP ポート 500 でセキュリティ サーバに応答します。
セキュリティ サーバ	UDP 4500	NAT-T ISAKMP	接続サーバ	UDP 4500	NAT がセキュリティ サーバおよびそのペアになっている接続サーバ インスタンス間で使用されている場合に必要となります。セキュリティ サーバは、UDP ポート 4500 を使用して NAT をたどって IPsec セキュリティをネゴシエートします。
接続サーバ	UDP 4500	NAT-T ISAKMP	セキュリティ サーバ	UDP 4500	接続サーバ インスタンスは、NAT が使用されている場合、UDP ポート 4500 でセキュリティ サーバに応答します。

表 5-2. バック エンド ファイアウォールのルール (続き)

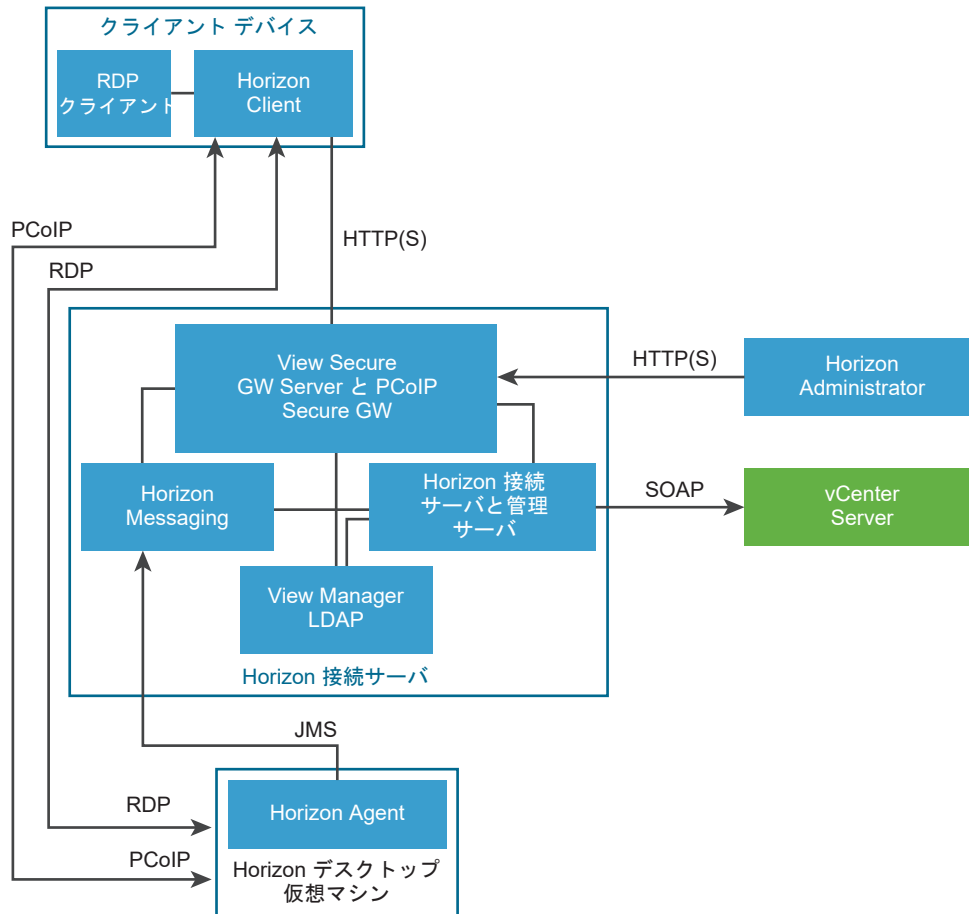
Source	デフォルト ポート	プロトコル	送信先	デフォルト ポート	注
セキュリティ サーバ	すべての TCP	AJP13	接続サーバ	TCP 8009	セキュリティ サーバは TCP ポート 8009 で接続サーバ インスタンスに接続し、外部クライアント デバイスの Web トラフィックを転送します。 IPSec を有効にすると、ペアリング後に AJP13 トラフィックは TCP ポート 8009 を使用しません。その代わりに、NAT-T (UDP ポート 4500) または ESP 上で送信されます。
セキュリティ サーバ	すべての TCP	JMS	接続サーバ	TCP 4001	セキュリティ サーバは、TCP ポート 4001 で接続サーバ インスタンスに接続し、Java Message Service (JMS) トラフィックをやりとりします。
セキュリティ サーバ	すべての TCP	JMS	接続サーバ	TCP 4002	セキュリティ サーバは、TCP ポート 4002 で接続サーバ インスタンスに接続し、保護された Java Message Service (JMS) トラフィックをやりとりします。
セキュリティ サーバ	すべての TCP	RDP	リモート デスクトップ	TCP 3389	セキュリティ サーバは、TCP ポート 3389 でリモート デスクトップに接続し、RDP トラフィックをやりとりします。
セキュリティ サーバ	すべての TCP	MMR	リモート デスクトップ	TCP 9427	セキュリティ サーバは、TCP ポート 9427 でリモート デスクトップに接続し、マルチメディアリダイレクト (MMR) とクライアント ドライブ リダイレクトに関連するトラフィックを受信します。
セキュリティ サーバ	すべての TCP UDP 55000	PCoIP	リモート デスクトップまたはアプリケーション	TCP 4172 UDP 4172	セキュリティ サーバは、TCP ポート 4172 および UDP ポート 4172 でリモート デスクトップおよびアプリケーションに接続し、PCoIP トラフィックをやりとりします。
リモート デスクトップまたはアプリケーション	UDP 4172	PCoIP	セキュリティ サーバ	UDP 55000	リモート デスクトップおよびアプリケーションは、UDP ポート 4172 からセキュリティ サーバに PCoIP データを送り返します。 送信先の UDP ポートは、受信した UDP パケットのソース ポートとなり、これは返信データであるため、通常は、これに明示的なファイアウォール ルールを追加する必要はありません。
セキュリティ サーバ	すべての TCP	USB-R	リモート デスクトップ	TCP 32111	セキュリティサーバは、TCP ポート 32111 でリモート デスクトップに接続し、外部クライアント デバイスとリモート デスクトップ間の USB リダイレクト トラフィックをやりとりします。
セキュリティ サーバ	すべての TCP または UDP	Blast Extreme	リモート デスクトップまたはアプリケーション	TCP または UDP 22443	セキュリティ サーバは、TCP および UDP ポート 22443 でリモート デスクトップおよびアプリケーションに接続し、Blast Extreme トラフィックをやりとりします。
セキュリティ サーバ	すべての TCP	HTTPS	リモート デスクトップ	TCP 22443	HTML Access を使用する場合、セキュリティ サーバはリモート デスクトップに HTTPS ポート 22443 で接続して、Blast Extreme エージェントと通信します。
セキュリティ サーバ		ESP	接続サーバ		NAT トラバーサルが必要ない場合のカプセル化された AJP13 トラフィック。ESP は IP プロトコル 50 です。ポート番号は指定されていません。
接続サーバ		ESP	セキュリティ サーバ		NAT トラバーサルが必要ない場合のカプセル化された AJP13 トラフィック。ESP は IP プロトコル 50 です。ポート番号は指定されていません。

通信プロトコルの概要

Horizon 6 と Horizon 7 のコンポーネントは、複数の異なるプロトコルを使用してメッセージを交換します。

図 5-5. セキュリティ サーバが構成されていない Horizon 6 と Horizon 7 のコンポーネントとプロトコル は、セキュリティ サーバが構成されていない場合に各コンポーネントが通信に使用するプロトコルを示しています。この場合、RDP、Blast Secure Gateway、および PCoIP Secure Gateway 用の安全なトンネルは確立されていません。この構成は一般的な LAN の展開環境で使用される可能性があります。

図 5-5. セキュリティ サーバが構成されていない Horizon 6 と Horizon 7 のコンポーネントとプロトコル



注: この図は、PCoIP または RDP を使用するクライアントへの直接接続を示しています。ただし、デフォルト設定では、PCoIP には直接接続、RDP にはトンネル接続が使用されます。

各プロトコルで使用されるデフォルト ポートについては、表 5-3. デフォルト ポート を参照してください。

図 5-6. セキュリティ サーバが構成されている Horizon 6 と Horizon 7 のコンポーネントとプロトコル は、セキュリティ サーバが構成されている場合に各コンポーネントが通信に使用するプロトコルを示しています。この構成は一般的な WAN の展開環境で使用される可能性があります。

図 5-6. セキュリティ サーバが構成されている Horizon 6 と Horizon 7 のコンポーネントとプロトコル

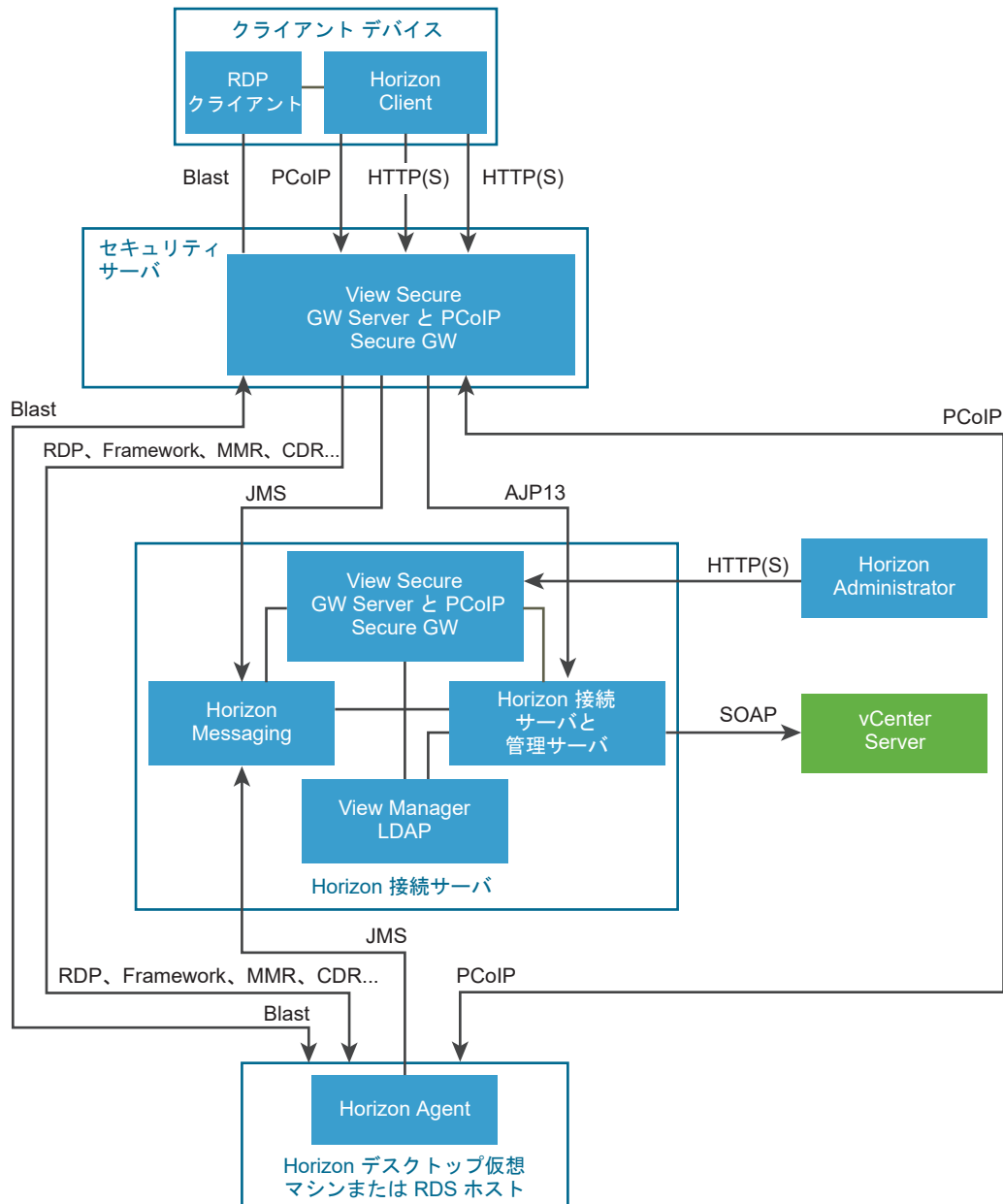


表 5-3. デフォルト ポート に、各プロトコルで使用されるデフォルト ポートを示します。必要に応じて、組織のポリシーに準拠するか競合を回避するために、どのポート番号が使用されるかを変更できます。

表 5-3. デフォルト ポート

プロトコル	ポート
JMS	TCP ポート 4001
	TCP ポート 4002
AJP13	TCP ポート 8009

注： AJP13 はセキュリティ サーバの構成のみで使用されます。

表 5-3. デフォルト ポート (続き)

プロトコル	ポート
HTTP	TCP ポート 80
HTTPS	TCP ポート 443
MMR/CDR	マルチメディア リダイレクトとクライアント ドライブ リダイレクトでは、TCP ポート 9427
RDP	TCP ポート 3389
	注： 接続サーバ インスタンスが直接クライアント接続用に構成されている場合、それらのプロトコルはクライアントからリモート デスクトップに直接接続され、View Secure Gateway Server コンポーネントを介してトンネリングされません。
SOAP	TCP ポート 80 または 443
PCoIP	TCP ポート 4172 UDP ポート 4172、50002、55000
USB リダイレクト	TCP ポート 32111。このポートはタイム ゾーンの同期にも使用されます。
VMware Blast Extreme	TCP ポート 8443、22443 UDP ポート 443、8443、22443
HTML Access	TCP ポート 8443、22443

接続サーバ間通信に使用される TCP ポート

グループ内の接続サーバ インスタンスは、互いに通信するために追加の TCP ポートを使用します。たとえば、接続サーバ インスタンスは、JMS のルーター間 (JMSIR) トラフィックを互いに送信するためにポート 4100 または 4101 を使用します。通常、ファイアウォールはグループ内の接続サーバ インスタンス間では使用されません。

View Secure Gateway Server

View Secure Gateway Server は、クライアント システムとセキュリティ サーバ、Unified Access Gateway アプライアンスまたは接続サーバ インスタンスとの安全な HTTPS 接続を実現するサーバ側コンポーネントです。

接続サーバのトンネル接続を構成すると、RDP、USB、およびマルチメディア リダイレクト (MMR) トラフィックが View Secure Gateway コンポーネントを介してトンネリングされます。直接クライアント接続を構成すると、それらのプロトコルはクライアントからリモート デスクトップに直接接続され、View Secure Gateway Server コンポーネントを介してトンネリングされません。

注： PCoIP または Blast Extreme 表示プロトコルを使用するクライアントは USB リダイレクトおよびマルチメディア リダイレクト (MMR) のアクセラレーションのためにトンネル接続を使用できますが、他のすべてのデータについては、PCoIP では PCoIP Secure Gateway が、Blast Extreme では Blast Secure Gateway が、セキュリティ サーバまたは Unified Access Gateway アプライアンス上で使用されます。

View Secure Gateway Server は、クライアントから接続サーバへの、ユーザー認証、デスクトップ選択、およびアプリケーション選択などのトラフィックを含むその他の Web トラフィックの転送も管理します。また、View Secure Gateway Server は Horizon Administrator クライアントの Web トラフィックを管理サーバ コンポーネントに渡します。

Blast Secure Gateway

セキュリティ サーバおよび Unified Access Gateway アプライアンスには、Blast Secure Gateway コンポーネントが含まれています。Blast Secure Gateway を有効にすると、認証が行われた後、Blast Extreme または HTML Access を使用するクライアントがセキュリティ サーバまたは Unified Access Gateway アプライアンスへの第 2 の安全な接続を確立できます。この接続により、クライアントはインターネットからリモート デスクトップとリモート アプリケーションにアクセスできるようになります。

Blast Secure Gateway コンポーネントを有効にすると、Blast Extreme トラフィックがセキュリティ サーバまたは Unified Access Gateway アプライアンスによってリモート デスクトップとリモート アプリケーションに転送されます。Blast Extreme を使用するクライアントで USB リダイレクト機能またはマルチメディア リダイレクト (MMR) のアクセラレーションも使用する場合は、そのデータを転送するために View Secure Gateway コンポーネントを有効にできます。

直接クライアント接続を構成した場合は、Blast Extreme トラフィックなどのトラフィックがクライアントからリモート デスクトップまたはリモート アプリケーションに直接送信されます。

自宅やモバイルの就業者などのエンド ユーザーがインターネットからデスクトップにアクセスする場合、必要なレベルのセキュリティおよび接続性がセキュリティ サーバまたは Unified Access Gateway アプライアンスによって提供されるため、VPN 接続は必要ありません。Blast Secure Gateway コンポーネントによって、企業のデータセンターに入ることができるリモート トラフィックが、強力な認証を経たユーザーのトラフィックに確実に限定されます。エンド ユーザーはアクセスが許可されているリソースにのみアクセスできます。

Blast Secure Gateway を介して動作する Blast ネイティブ クライアントの Blast セッションでは、Blast Secure Gateway で設定されている TLS 証明書によって認証された TLS 接続を想定しています。クライアントの Blast 接続で他の TLS 証明書が使用されている場合、接続がドロップされ、クライアントが証明書サムプリントの不一致を報告します。

クライアントが、クライアントと Blast Secure Gateway の間に配置された TLS 終端プロキシに接続する場合、プロキシが Blast Secure Gateway の証明書（とプライベート キー）のコピーを提供するように調整することで、クライアント証明書の要件を満たし、サムプリントの不一致エラーを回避できます。これにより、クライアントからの Blast 接続が成功します。

プロキシに Blast Secure Gateway の証明書をコピーする代わりに、プロキシに独自の TLS 証明書を提供し、クライアントが Blast Secure Gateway の証明書ではなく、プロキシの証明書を受け入れるように Blast Secure Gateway を構成することもできます。

Unified Access Gateway で Blast Secure Gateway を構成するには、Unified Access Gateway Horizon の設定の [Blast プロキシ証明書] でプロキシの証明書をアップロードします。<https://docs.vmware.com/jp/Unified-Access-Gateway/index.html> にある『VMware Unified Access Gateway の導入および設定』ドキュメントを参照してください。

注： アップロードされるのはプロキシ証明書だけです。対応するプライベート キーは Unified Access Gateway に公開されません。

PCoIP Secure Gateway

セキュリティ サーバおよび Unified Access Gateway アプライアンスには、PCoIP Secure Gateway コンポーネントが含まれています。PCoIP Secure Gateway を有効にすると、認証が行われた後、PCoIP を使用するクライ

アントがセキュリティ サーバまたは Unified Access Gateway アプライアンスへの第 2 の安全な接続を確立できます。この接続により、クライアントはインターネットからリモート デスクトップとリモート アプリケーションにアクセスできるようになります。

PCoIP Secure Gateway コンポーネントを有効にすると、PCoIP トラフィックがセキュリティ サーバまたは Unified Access Gateway アプライアンスによってリモート デスクトップとリモート アプリケーションに転送されます。PCoIP を使用するクライアントで USB リダイレクト機能またはマルチメディア リダイレクト (MMR) のアクセラレーションも使用する場合は、そのデータを転送するために View Secure Gateway コンポーネントを有効にできます。

直接クライアント接続を構成した場合は、PCoIP トラフィックなどのトラフィックがクライアントからリモート デスクトップまたはリモート アプリケーションに直接送信されます。

自宅やモバイルの就業者などのエンド ユーザーがインターネットからデスクトップにアクセスする場合、必要なレベルのセキュリティおよび接続性がセキュリティ サーバまたは Unified Access Gateway アプライアンスによって提供されるため、VPN 接続は必要ありません。PCoIP Secure Gateway コンポーネントによって、企業のデータセンターに入ることができるリモート トラフィックが、強力な認証を経たユーザーのトラフィックに確実に限定されます。エンド ユーザーはアクセスが許可されているリソースにのみアクセスできます。

View LDAP

View LDAP は View 接続サーバの組み込み LDAP ディレクトリであり、すべての Horizon 7 構成データの構成リポジトリです。

View LDAP には、各リモート デスクトップおよびアプリケーション、アクセス可能な各リモート デスクトップ、まとめて管理される複数のリモート デスクトップ、および Horizon 7 コンポーネントの構成設定を表すエントリが含まれています。

View LDAP には、他の Horizon 7 コンポーネントに自動化サービスと通知サービスを提供する、一連の Horizon 7 プラグイン DLL も含まれています。

Horizon Messaging

Horizon Messaging コンポーネントは、Horizon Connection Server コンポーネント間、および Horizon Agent と接続サーバとの間のメッセージング ルーターとして機能します。

このコンポーネントは、Horizon 7 でのメッセージングに使用される Java Message Service (JMS) API をサポートしています。

コンポーネント間のメッセージの検証では、DSA キーが使用されます。キー サイズは、デフォルトでは 512 ビットです。ただし、FIPS モードではキー サイズは 2048 ビットです。

注： メッセージ セキュリティ モードが、[拡張済み] に設定されている場合、SSL/TLS はメッセージごとの暗号化に使用するよりも JMS 接続の安全を確保することに使用されます。拡張メッセージ セキュリティ モードでは、検証は 1 つのメッセージ タイプについてのみ適用されます。拡張メッセージ モードでは、キー サイズを 2048 ビットに増やすことをお勧めします。拡張メッセージ セキュリティ モードを使用していない場合は、デフォルトを 512 ビットから変更しないことをお勧めします。これは、キー サイズを増やすことでパフォーマンスとスケーラビリティが影響を受けるためです。

すべてのキーを 1024 ビットにする場合は、最初の接続サーバ インスタンスをインストールした直後、追加のサーバやデスクトップを作成する前に、RSA キー サイズを変更する必要があります。詳細については、VMware ナレッジベース (KB) の記事 1024431 を参照してください。

Horizon 接続サーバのファイアウォール ルール

接続サーバ インスタンスおよびセキュリティ サーバ用にファイアウォールの特定のポートを開く必要があります。

接続サーバをインストールするときは、必要な Windows ファイアウォール ルールをインストール プログラムのオプションで設定できます。これらのルールは、デフォルトで使用されるポートを開きます。インストール後にデフォルト ポートを変更する場合は、更新したポートを介して Horizon Client デバイスを Horizon 7 に接続できるように Windows ファイアウォールを手動で構成する必要があります。

次の表は、インストール時に自動的に開くことができるデフォルト ポートを一覧で示しています。これらのポートは、特に記述のない限り受信ポートです。

表 5-4. Horizon 接続サーバのインストール時に開かれるポート

プロトコル	ポート	Horizon 接続サーバ インスタンスの種類
JMS	TCP 4001	標準およびレプリカ
JMS	TCP 4002	標準およびレプリカ
JMSIR	TCP 4100	標準およびレプリカ
JMSIR	TCP 4101	標準およびレプリカ
AJP13	TCP 8009	標準およびレプリカ
HTTP	TCP 80	標準、レプリカ、およびセキュリティ サーバ
HTTPS	TCP 443	標準、レプリカ、およびセキュリティ サーバ
PCoIP	TCP 4172 (受信)、 UDP 4172 (双方向)	標準、レプリカ、およびセキュリティ サーバ
HTTPS	TCP 8443 UDP 8443	標準、レプリカ、およびセキュリティ サーバ。 Horizon 7 への最初の接続が行われた後、Web ブラウザまたはクライアント デバイスは、TCP ポート 8443 で Blast Secure Gateway に接続します。Blast Secure Gateway をセキュリティ サーバまたは View 接続サーバ インスタンスで有効にして、この第 2 の接続が行われることを許可します。
HTTPS	TCP 8472	標準およびレプリカ クラウド ボッド アーキテクチャ機能の場合：ボッド間通信に使用されます。
HTTP	TCP 22389	標準およびレプリカ クラウド ボッド アーキテクチャ機能の場合：グローバル LDAP レプリケーションに使用されます。
HTTPS	TCP 22636	標準およびレプリカ クラウド ボッド アーキテクチャ 機能の場合：保護されたグローバル LDAP レプリケーションに使用されます。

View Agent または Horizon Agent のファイアウォール ルール

View Agent と Horizon Agent のインストーラは、デフォルト ネットワーク ポートを開く Windows ファイアウォール ルールをリモート デスクトップと RDS ホストにオプションで設定します。これらのポートは、特に記述のない限り受信ポートです。

View Agent と Horizon Agent のインストーラによって、ホスト OS の現在の RDP ポート（通常は 3389）に合わせて受信 RDP 接続のローカル ファイアウォール ルールが構成されます。

View Agent または Horizon Agent のインストーラに、リモート デスクトップのサポートを有効にしないように指示した場合、ポート 3389 および 32111 が開かれないため、それらのポートを手動で開く必要があります。

インストール後にこの RDP ポート番号を変更する場合は、関連するファイアウォール ルールも変更する必要があります。インストール後にデフォルトのポートを変更した場合、手動で Windows ファイアウォール ルールを再構成して更新されたポートへのアクセスを許可する必要があります。『Horizon 7 のインストール』の「View サービスのデフォルト ポートの置換」を参照してください。

RDS ホストの View Agent または Horizon Agent に関する Windows ファイアウォール ルールでは、256 個の連続した UDP ポート ブロックが受信トラフィック用に開いていることが示されます。このポートのブロックは、View Agent または Horizon Agent の VMware Blast 内部で使用されます。RDS ホストにある Microsoft が署名した特別なドライバによって、外部ソースからこれらのポートへの受信トラフィックがブロックされます。このドライバにより、Windows ファイアウォールはこれらを閉じているポートとして扱います。

仮想マシン テンプレートをデスクトップ ソースとして使用する場合は、そのテンプレートがデスクトップ ドメインのメンバーである場合にのみ、デプロイされたデスクトップにファイアウォールの例外が継承されます。Microsoft のグループ ポリシー設定を使用して、ローカルでのファイアウォールの例外を管理できます。詳細については、Microsoft のサポート技術情報 (KB) の記事 875357 を参照してください。

表 5-5. View Agent または Horizon Agent のインストール時に開かれる TCP および UDP ポート

プロトコル	ポート
RDP	TCP ポート 3389
USB のリダイレクトとタイム ゾーンの同期	TCP ポート 32111
MMR (マルチメディア リダイレクト) と CDR (クライアント ドライブ リダイレクト)	TCP ポート 9427
PCoIP	<p>RDS ホストの場合、PCoIP は TCP ポート 4172 と UDP ポート 4172 (双方向) を使用します。</p> <p>デスクトップの場合、PCoIP は、構成可能な範囲から選択したポート番号を使用します。TCP ポート 4172 から 4173、UDP ポート 4172 から 4182 がデフォルトの範囲となります。これらのファイアウォール ルールにポート番号を指定せず、各 PCoIP Server によって開かれたポートを動的に使用します。選択したポート番号が Connection Server 経由でクライアントに通知されます。</p>
VMware Blast	<p>TCP ポート 22443</p> <p>UDP ポート 22443 (双方向)</p> <p>注： Linux デスクトップでは UDP は使用されません。</p>
HTML Access	TCP ポート 22443

表 5-5. View Agent または Horizon Agent のインストール時に開かれる TCP および UDP ポート（続き）

プロトコル	ポート
XDMCP	UDP 177 注： このポートは、Ubuntu 18.04 を実行している Linux デスクトップでの XDMCP アクセスにのみ使用されます。ファイアウォール ルールにより、このポートに対する外部ホストからのアクセスはすべてブロックされます。
X11	TCP 6100 注： このポートは、Ubuntu 18.04 を実行している Linux デスクトップでの XServer アクセスにのみ使用されます。ファイアウォール ルールにより、このポートに対する外部ホストからのアクセスはすべてブロックされます。

Active Directory のファイアウォール ルール

お使いの Horizon 7 お使いの環境と Active Directory サーバの間にファイアウォールがある場合は、必要なポートがすべて開いていることを確認する必要があります。

たとえば View 接続サーバは、Active Directory グローバル カタログおよび Lightweight Directory Access Protocol (LDAP) サーバにアクセスできる必要があります。使用しているファイアウォール ソフトウェアによってグローバル カタログと LDAP のポートがブロックされると、管理者がユーザーの資格を構成する際に問題が発生します。

ファイアウォールを介して Active Directory を正常に機能させるために開く必要があるポートの詳細については、使用する Active Directory サーバのバージョンに関する Microsoft のマニュアルを参照してください。

Horizon 7 環境のセットアップ手順の概要

6

次の高水準のタスクを完了して、Horizon 7 のインストールと初期展開の構成を行います。

表 6-1. Horizon 7 のインストールおよびセットアップのチェックリスト

ステップ	タスク
1	必要な管理者ユーザーおよびグループを Active Directory で設定します。 説明：『Horizon 7 インストール ガイド』 および vSphere のマニュアル。
2	ESXi/ESX ホストおよび vCenter Server のインストールと設定をまだ行っていない場合は、行います。 説明：VMware vSphere のマニュアル。
3	(オプション) リンク クローン デスクトップを展開する場合は、View Composer を vCenter Server システムまたは別のサーバにインストールします。また、View Composer データベースをインストールします。 説明：『Horizon 7 インストール ガイド』。
4	Horizon 接続サーバをインストールして設定します。また、イベント データベースをインストールします。 説明：『Horizon 7 インストール ガイド』。
5	完全クローン デスクトップ プールのテンプレートとして、またはリンク クローン デスクトップ プールまたはインスタント クローン デスクトップ プールの親として使用できる仮想マシンを 1 台以上作成します。 手順：『Horizon 7 での仮想デスクトップのセットアップ』
6	(オプション) RDS ホストを設定し、アプリケーションをインストールして、エンド ユーザーがリモート アクセスできるようにします。 手順：『Horizon 7 での公開されたデスクトップとアプリケーションのセットアップ』
7	デスクトップ プールまたはアプリケーション プール、または両方のプールを作成します。 手順：『Horizon 7 での仮想デスクトップのセットアップ』 および 『Horizon 7 での公開されたデスクトップとアプリケーションのセットアップ』
8	デスクトップへのユーザー アクセスを制御します。 手順：『Horizon 7 でのリモート デスクトップ機能の構成』
9	エンド ユーザーのマシンに Horizon Client をインストールして、エンド ユーザーがリモート デスクトップとリモート アプリケーションにアクセスできるようにします。 手順： https://docs.vmware.com/jp/VMware-Horizon-Client/index.html にある Horizon Client のドキュメント
10	(オプション) 追加の管理者を作成して構成し、特定のインベントリ オブジェクトと設定に対して異なるレベルのアクセス権を許可します。 説明：『Horizon 7 管理ガイド』。
11	(オプション) ポリシーを構成して、Horizon 7 コンポーネント、デスクトップ プール、アプリケーション プール、およびエンド ユーザーの動作を制御します。 手順：『Horizon 7 でのリモート デスクトップ機能の構成』

表 6-1. Horizon 7 のインストールおよびセットアップのチェックリスト（続き）

ステップ	タスク
12	<p>（オプション） Horizon Persona Management を構成します。これにより、ユーザーがデスクトップにログインするたびに、個人用のデータと設定にアクセスできるようになります。</p> <p>手順：『Horizon 7 での仮想デスクトップのセットアップ』</p>
13	<p>（オプション） セキュリティを強化するために、スマート カード認証または RADIUS 2 要素認証ソリューションを統合します。</p> <p>説明：『Horizon 7 管理ガイド』。</p>