

Horizon 7 のインストール

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 © 2011-2020 VMware, Inc. All rights reserved. [著作権および商標情報](#)。

目次

Horizon 7 のインストール 7

1 サーバ コンポーネントのシステム要件 8

Horizon 接続サーバの要件 8

Horizon 接続サーバのハードウェア要件 9

Horizon Connection Server でサポートされるオペレーティング システム 9

Horizon 接続サーバの仮想化ソフトウェア要件 10

複製された Horizon 接続サーバ インスタンスのネットワーク要件 10

Horizon Administrator の要件 10

Horizon Console の要件 11

View Composer の要件 12

View Composer でサポートされるオペレーティング システム 12

スタンドアロン View Composer のハードウェア要件 13

View Composer およびイベント データベースのデータベース要件 13

2 ゲスト OS のシステム要件 14

Horizon Agent の要件と考慮事項 14

スタンドアロン Horizon Persona Management でサポートされるオペレーティング システム 15

リモート表示プロトコルとソフトウェアのサポート 15

PCoIP 16

Microsoft RDP 18

VMware Blast Extreme 18

3 IPv6 環境での Horizon 7 のインストール 23

IPv6 環境での Horizon 7 のセットアップ 23

IPv6 環境でサポートされている vSphere、データベース、および Active Directory のバージョン 24

IPv6 環境でサポートされている Horizon 7 サーバ用オペレーティング システム 24

IPv6 環境でサポートされているデスクトップおよび RDS ホスト用 Windows オペレーティング システム 25

IPv6 環境でサポートされているクライアント 25

IPv6 環境でサポートされているリモート プロトコル 25

IPv6 環境でサポートされている認証タイプ 26

IPv6 環境でサポートされているその他の機能 26

4 FIPS モードでの Horizon 7 のインストール 29

FIPS モードでの Horizon 7 のセットアップの概要 29

FIPS モードのシステム要件 30

5 Active Directory の準備 31

ドメインと信頼関係の構成	32
信頼関係とドメインのフィルタ処理	33
リモート デスクトップの OU の作成	33
キオスク モード クライアント アカウントの OU とグループの作成	33
ユーザーのグループの作成	34
vCenter Server のユーザー アカウントの作成	34
スタンドアロンの View Composer Server のユーザー アカウントの作成	34
View Composer AD 操作のユーザー アカウントの作成	34
インスタントクローン操作のユーザー アカウントの作成	36
制限されたグループ ポリシーを構成する	36
Horizon 7 グループ ポリシー管理用テンプレート ファイルの使用	37
スマート カード認証用の Active Directory を準備する	38
スマート カード ユーザーの UPN を追加する	38
信頼されたルート証明機関へのルート証明書の追加	39
中間証明機関への中間証明書の追加	40
Enterprise NTAAuth ストアにルート証明書を追加する	41
SSL/TLS における強度の弱い暗号化方式の無効化	41

6 View Composer のインストール 43

View Composer データベースの準備	43
View Composer 用の SQL Server データベースの作成	44
View Composer 用の Oracle データベースの作成	48
View Composer 向けに SSL 証明書を構成する	52
View Composer サービスのインストール	52
View Composer から vCenter および ESXi 接続で TLSv1.0 を有効にする	55
View Composer 用のインフラストラクチャの構成	56
View Composer 用の vSphere 環境の構成	56
View Composer に関する他のベスト プラクティス	56

7 Horizon 接続サーバのインストール 57

Horizon 接続サーバ ソフトウェアのインストール	57
Horizon 接続サーバのインストールの前提条件	58
新しい構成での Horizon 接続サーバのインストール	59
Horizon 接続サーバのサイレント インストール	62
Horizon Connection Server の標準インストールのサイレント インストールのプロパティ	64
接続サーバから vCenter 接続で TLSv1.0 を有効にする	65
Horizon 接続サーバの複製インスタンスのインストール	66
Horizon 接続サーバの複製インスタンスのサイレント インストール	70
Horizon 接続サーバの複製インスタンスのサイレント インストールのプロパティ	72
セキュリティ サーバのペアリング パスワードを構成する	73
セキュリティ サーバをインストールする	74

セキュリティ サーバをサイレント インストールする	78
セキュリティ サーバのサイレント インストールのプロパティ	80
セキュリティ サーバの IPsec ルールの削除	82
VPN 経由で Unified Access Gateway アプライアンスを使用する利点	83
Horizon 接続サーバのファイアウォール ルール	84
バックエンド ファイアウォールを構成して IPsec をサポートする	85
Horizon 接続サーバをバックアップ構成で再インストールする	86
Microsoft Windows インストーラ コマンド ライン オプション	88
MSI のコマンドライン オプションを使用した Horizon 7 コンポーネントのサイレント アンインストール	90

8 Horizon 7 Server 用の TLS 証明書の設定 92

Horizon 7 Server 用の TLS 証明書について	93
TLS 証明書をセットアップするためのタスクの概要	94
認証局 (CA) からの署名付き TLS 証明書の取得	95
Windows ドメインまたは Enterprise CA から署名証明書を取得する	96
新しい TLS 証明書を使用するように Horizon 接続サーバ、セキュリティ サーバ、または View Composer を構成する	97
証明書スナップインを MMC に追加する	98
署名付きサーバ証明書を Windows 証明書ストアにインポートする	99
証明書のわかりやすい名前を変更する	100
ルート証明書と中間証明書を Windows 証明書ストアにインポートする	101
View Composer が使用するポートに新規 TLS 証明書をバインドする	102
ルート証明書と中間証明書を信頼するようにクライアント エンドポイントを構成する	103
ルート証明書と中間証明書を信頼するように Horizon Client for Mac を構成	105
ルート証明書と中間証明書を信頼するように Horizon Client for iOS を構成する	105
サーバ証明書での証明書失効チェックの構成	106
新しい TLS 証明書を使用するために PCoIP Secure Gateway を構成する	107
PSG 証明書のサブジェクト名に一致するサーバ名を確認する	108
Windows 証明書ストアに PSG 証明書を構成する	108
Windows レジストリに PSG 証明書のわかりやすい名前を設定する	110
CA 署名付き証明書が PSG への接続に強制的に使用されるようにする	111
vCenter Server または View Composer 証明書を信頼するための Horizon Administrator の設定	111
認証局 (CA) によって署名された TLS 証明書を使用する利点	112
Horizon 接続サーバとセキュリティ サーバ証明書問題のトラブルシューティング	112

9 Horizon 7 の初回構成 114

vCenter Server、View Composer およびインスタント クローンのユーザー アカウントの構成	114
vCenter Server ユーザーと View Composer ユーザーを使用する場所	115
Horizon 7 および View Composer の vCenter Server ユーザーの構成	115
vCenter Server ユーザーに必要な権限	117
vCenter Server ユーザーに必要な View Composer とインスタント クローンの権限	118
初めての Horizon 接続サーバの構成	119

Horizon Administrator と Horizon Connection Server	119
Horizon Administrator へのログイン	120
製品のライセンス キーのインストール	121
vCenter Server インスタンスの Horizon 7 への追加	122
View Composer 設定を構成する	124
View Composer ドメインを構成する	125
インスタントクローンのドメイン管理者の追加	126
vSphere でリンク クローン仮想マシンのディスク領域を再利用できるようにする	126
vCenter Server 用に View Storage Accelerator を構成する	128
vCenter Server と View Composer の同時操作の制限	130
リモート デスクトップ ログオン ストームをサポートするための同時電源操作レートの設定	131
デフォルトの TLS 証明書のサムプリントを受け入れる	131
Horizon Client 接続の構成	133
PCoIP Secure Gateway および安全なトンネルの接続の構成	134
Blast Secure Gateway の構成	135
Secure Gateway 接続およびトンネル接続用の外部 URL の構成	136
Connection Server インスタンスの外部 URL を設定する	138
セキュリティ サーバの外部 URL を変更する	139
Horizon 接続サーバがアドレス情報を返したときに DNS 名を優先	140
ロード バランサでの HTML Access の許可	141
ゲートウェイでの HTML Access の許可	141
Horizon 7 サービスのデフォルト ポートの置換	142
Horizon 接続サーバ インスタンスおよびセキュリティ サーバのデフォルト HTTP ポートまたは NIC を置換する	142
Horizon 接続サーバ インスタンスおよびセキュリティ サーバ上の PCoIP Secure Gateway のデフォルト ポートまたは NIC を置換する	144
接続サーバ インスタンスおよびセキュリティ サーバ上の PCoIP Secure Gateway のデフォルト制御ポートを置換	145
View Composer のデフォルト ポートを置換する	145
接続サーバへの HTTP リダイレクト用のポート番号を変更	146
接続サーバへのクライアント接続で HTTP リダイレクトを防止	147
接続サーバ上での Horizon 7 パフォーマンス カウンタへのリモート アクセスの有効化	147
展開の規模に合わせた Windows Server 設定の調整	148
Horizon 接続サーバ用メモリのサイズ設定	148
システム ページ ファイルの設定を構成する	148

10 イベント レポートの構成 150

Horizon 7 イベント用のデータベースとデータベース ユーザーを追加する	150
SQL Server データベースをイベント レポート用に準備する	151
イベント データベースを構成する	152
Syslog サーバのイベント ログを構成する	153

Horizon 7 のインストール

『Horizon 7 のインストール』では、VMware Horizon[®] 7 サーバとクライアント コンポーネントをインストールする方法について説明します。

対象読者

この情報は、VMware Horizon 7 をインストールしようとするすべての方を対象としています。本書に記載されている情報は、仮想マシンのテクノロジーとデータセンターの操作に精通した、経験豊富な Windows または Linux システム管理者向けに書かれています。

サーバ コンポーネントのシステム要件

1

Horizon 7 のサーバ コンポーネントを実行するホストは、ハードウェアとソフトウェアの特定の要件を満たす必要があります。

この章には、次のトピックが含まれています。

- [Horizon 接続サーバの要件](#)
- [Horizon Administrator の要件](#)
- [Horizon Console の要件](#)
- [View Composer の要件](#)

Horizon 接続サーバの要件

Horizon 接続サーバはクライアント接続のブローカーとして機能し、受信したユーザーの要求を認証した後、適切なリモート デスクトップとアプリケーションに送信します。Horizon 接続サーバには、特定のハードウェア要件、オペレーティング システム要件、インストール要件、およびサポート ソフトウェア要件があります。

- [Horizon 接続サーバのハードウェア要件](#)

Horizon 接続サーバのインストールタイプ（標準、レプリカ、セキュリティ サーバ、および登録サーバのインストール）はすべて、特定のハードウェア要件を満たす専用の物理マシンまたは仮想マシンにインストールする必要があります。

- [Horizon Connection Server でサポートされるオペレーティング システム](#)

Horizon Connection Server は、サポート対象の Windows Server オペレーティング システムにインストールする必要があります。

- [Horizon 接続サーバの仮想化ソフトウェア要件](#)

Horizon 接続サーバには、特定のバージョンの VMware 仮想化ソフトウェアが必要です。

- [複製された Horizon 接続サーバ インスタンスのネットワーク要件](#)

複製された Horizon 接続サーバ インスタンスをインストールする場合、通常、物理的に同じ場所にインスタンスを構成し、高速 LAN でインスタンス間を接続する必要があります。このようにしないと、遅延の発生により Horizon 接続サーバ インスタンスの View LDAP 構成の整合性が失われる可能性があります。また、構成情報が期限切れになった Horizon 接続サーバ インスタンスに接続するときに、ユーザーがアクセスを拒否される場合があります。

Horizon 接続サーバのハードウェア要件

Horizon 接続サーバのインストールタイプ（標準、レプリカ、セキュリティ サーバ、および登録サーバのインストール）はすべて、特定のハードウェア要件を満たす専用の物理マシンまたは仮想マシンにインストールする必要があります。

表 1-1. Horizon 接続サーバのハードウェア要件

ハードウェア コンポーネント	Required	推奨
プロセッサ	Pentium IV 2.0GHz 以上のプロセッサ	4 つの CPU
ネットワーク アダプタ	100Mbps NIC	1Gbps NIC
メモリ Windows Server 2008 R2 64 ビット	4GB 以上の RAM	50 以上のリモート デスクトップを展開する場合は 10GB 以上の RAM
メモリ Windows Server 2012 R2 64 ビット	4GB 以上の RAM	50 以上のリモート デスクトップを展開する場合は 10GB 以上の RAM

上記の要件は、高可用性または外部アクセスのためにインストールする Horizon 接続サーバ（レプリカおよびセキュリティ サーバ） インスタンスにも適用されます。

重要： Horizon 接続サーバをホストする物理マシンまたは仮想マシンは、変更されない IP アドレスを持っている必要があります。IPv4 環境では、固定 IP アドレスを構成します。IPv6 環境では、変更されない IP アドレスがマシンによって自動的に取得されます。

Horizon Connection Server でサポートされるオペレーティング システム

Horizon Connection Server は、サポート対象の Windows Server オペレーティング システムにインストールする必要があります。

次のオペレーティング システムは、Horizon Connection Server のすべてのインストールタイプ（標準、レプリカ、セキュリティ サーバ）をサポートします。

表 1-2. Horizon Connection Server のオペレーティング システム サポート

オペレーティング システム	バージョン	エディション
Windows Server 2008 R2 SP1	64 ビット	Standard Enterprise Datacenter
Windows Server 2012 R2	64 ビット	Standard Datacenter
Windows Server 2016	64 ビット	Standard Datacenter
Windows Server 2019	64 ビット	Standard Datacenter

注： サービス パックなしの Windows Server 2008 R2 はサポートされません。

Horizon 接続サーバの仮想化ソフトウェア要件

Horizon 接続サーバには、特定のバージョンの VMware 仮想化ソフトウェアが必要です。

vSphere を使用している場合は、サポートされているバージョンの vSphere ESX/ESXi ホストと vCenter Server を使用する必要があります。

vCenter Server および ESXi のバージョンと互換性があるバージョンについての詳細は、http://www.vmware.com/resources/compatibility/sim/interop_matrix.php の VMware 製品の互換性一覧を参照してください。

複製された Horizon 接続サーバ インスタンスのネットワーク要件

複製された Horizon 接続サーバ インスタンスをインストールする場合、通常、物理的に同じ場所にインスタンスを構成し、高速 LAN でインスタンス間を接続する必要があります。このようにしないと、遅延の発生により Horizon 接続サーバ インスタンスの View LDAP 構成の整合性が失われる可能性があります。また、構成情報が期限切れになった Horizon 接続サーバ インスタンスに接続するときに、ユーザーがアクセスを拒否される場合があります。

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。

Horizon Administrator の要件

管理者は、Horizon Administrator を使って Horizon Connection Server の設定、リモート デスクトップおよびアプリケーションの展開と管理、ユーザー認証の制御、システム イベントの開始と調査、および分析作業を実行します。Horizon Administrator を実行するクライアント システムは、特定の要件を満たす必要があります。

Horizon Administrator は Web ベースのアプリケーションで、接続サーバをインストールするとインストールされます。Horizon Administrator は次の Web ブラウザでアクセスして使用できます。

- Internet Explorer 9 (推奨されません)
- Internet Explorer 10
- Internet Explorer 11
- Firefox (サポートされる最新バージョン)
- Chrome (サポートされる最新バージョン)
- Safari 6 以降のリリース
- Microsoft Edge (Windows 10)

Horizon Administrator を Web ブラウザで使用するには、Adobe Flash Player 10.1 以降がインストールされている必要があります。また、Adobe Flash Player をインストールできるように、クライアント システムがインターネットにアクセスできる必要があります。

Horizon Administrator を起動するコンピュータは、接続サーバをホストするサーバのルート証明書および中間証明書を信頼する必要があります。サポートされているブラウザには、よく知られているすべての証明局（CA）の証明書がすでに含まれています。証明書の発行元がよく知られていない CA である場合は、[ルート証明書と中間証明書を信頼するようにクライアント エンドポイントを構成する](#)で説明する手順に従う必要があります。

テキストを正しく表示するため、Horizon Administrator では Microsoft 固有のフォントが必要です。Web ブラウザを Linux、UNIX、Mac などの Windows 以外のオペレーティング システムで実行する場合は、Microsoft 固有のフォントがコンピュータにインストールされていることを確認してください。

現在、Microsoft の Web サイトでは Microsoft フォントが配布されていませんが、独立系の Web サイトからダウンロードできます。

Horizon Console の要件

管理者は、Horizon Console を使って Horizon Connection Server の設定、リモート デスクトップおよびアプリケーションの展開と管理、ユーザー認証の制御、システム イベントの開始と調査、および分析作業を実行します。Horizon Console を実行するクライアント システムは、特定の要件を満たす必要があります。

Horizon Console は Web ベースのアプリケーションで、Connection Server をインストールするとインストールされます。Horizon Console は次の Web ブラウザでアクセスして使用できます。

- Internet Explorer 11
- Firefox（サポートされる最新バージョン）
- Chrome（サポートされる最新バージョン）
- Safari（サポートされる最新バージョン）
- Microsoft Edge (Windows 10)

Horizon Console を起動するコンピュータは、Connection Server をホストするサーバのルート証明書および中間証明書を信頼する必要があります。サポートされているブラウザには、よく知られているすべての証明局（CA）の証明書がすでに含まれています。証明書の発行元がよく知られていない CA である場合は、[ルート証明書と中間証明書を信頼するようにクライアント エンドポイントを構成する](#)で説明する手順に従う必要があります。

テキストを正しく表示するため、Horizon Console では Microsoft 固有のフォントが必要です。Web ブラウザを Linux、UNIX、Mac などの Windows 以外のオペレーティング システムで実行する場合は、Microsoft 固有のフォントがコンピュータにインストールされていることを確認してください。

現在、Microsoft の Web サイトでは Microsoft フォントが配布されていませんが、独立系の Web サイトからダウンロードできます。

View Composer の要件

View Composer では、中央で管理される 1 つの基本イメージから複数のリンク クローン デスクトップを展開することができます。View Composer には特定のインストール要件およびストレージ要件があります。

■ View Composer でサポートされるオペレーティング システム

View Composer は 64 ビットのオペレーティング システムをサポートしますが、固有の要件と制限があります。View Composer は、vCenter Server と同じ物理マシンまたは仮想マシンにも、別のサーバにもインストールできます。

■ スタンドアロン View Composer のハードウェア要件

View Composer を vCenter Server に使用するものとは別の物理または仮想マシンにインストールする場合、特定のハードウェア要件を満たす専用のマシンを使用する必要があります。

■ View Composer およびイベント データベースのデータベース要件

View Composer には、データを格納するための SQL データベースが必要です。View Composer データベースは、View Composer Server ホスト上に存在するか、View Composer Server ホストから利用できる必要があります。Horizon イベントに関する Horizon Connection Server からの情報を記録するように、任意にイベント データベースをセットアップできます。

View Composer でサポートされるオペレーティング システム

View Composer は 64 ビットのオペレーティング システムをサポートしますが、固有の要件と制限があります。View Composer は、vCenter Server と同じ物理マシンまたは仮想マシンにも、別のサーバにもインストールできます。

表 1-3. View Composer がサポートするオペレーティング システム

オペレーティング システム	バージョン	エディション
Windows Server 2008 R2 SP1	64 ビット	Standard Enterprise Datacenter
Windows Server 2012 R2	64 ビット	Standard Datacenter
Windows Server 2016	64 ビット	Standard Datacenter
Windows Server 2019	64 ビット	Standard Datacenter

注： サービス パックなしの Windows Server 2008 R2 はサポートされません。

View Composer を vCenter Server とは異なる物理マシンまたは仮想マシンにインストールする場合は、[スタンドアロン View Composer のハードウェア要件](#) を参照してください。

Windows Server 2016 または Windows Server 2019 仮想マシンでの View Composer のインストールのトラブルシューティングについては、VMware ナレッジベースの記事 <https://kb.vmware.com/s/article/59633> を参照してください。

スタンドアロン View Composer のハードウェア要件

View Composer を vCenter Server に使用するものとは別の物理または仮想マシンにインストールする場合、特定のハードウェア要件を満たす専用のマシンを使用する必要があります。

スタンドアロン View Composer インストールは、別の Windows Server マシンにインストールされた vCenter Server、または Linux ベースの vCenter Server Appliance と連携します。VMware では、それぞれの View Composer サービスと vCenter Server インスタンスを 1 対 1 で対応させることを推奨しています。

表 1-4. View Composer のハードウェア要件

ハードウェア コンポーネント	必須	推奨
プロセッサ	1.4 GHz 以上の Intel 64 または AMD 64 プロセッサで 2 つの CPU	2 GHz 以上で 4 つの CPU
ネットワーク	1 つ以上の 10/100Mbps ネットワーク インターフェイス カード (NIC)	1Gbps NIC
メモリ	4GB 以上の RAM	50 以上のリモート デスクトップを展開する場合は 8 GB 以上の RAM
ディスク領域	40GB	60 GB

重要： View Composer をホストする物理マシンまたは仮想マシンは、変更されない IP アドレスを持っている必要があります。IPv4 環境では、固定 IP アドレスを構成します。IPv6 環境では、変更されない IP アドレスがマシンによって自動的に取得されます。

View Composer およびイベント データベースのデータベース要件

View Composer には、データを格納するための SQL データベースが必要です。View Composer データベースは、View Composer Server ホスト上に存在するか、View Composer Server ホストから利用できる必要があります。Horizon イベントに関する Horizon Connection Server からの情報を記録するように、任意にイベント データベースをセットアップできます。

vCenter Server 用のデータベース サーバがすでに存在する場合、既存のインスタンスが http://www.vmware.com/resources/compatibility/sim/interop_matrix.php の「VMware 製品の互換運用性マトリックス」にあるバージョンであれば、View Composer でそれを使用できます。データベース サーバ インスタンスがまだ存在しない場合は、インストールする必要があります。

View Composer は、vCenter Server でサポートされるデータベース サーバのサブセットをサポートします。View Composer ではサポートされないデータベース サーバを vCenter Server ですでに使用している場合は、引き続き vCenter Server でそのデータベース サーバを使用し、View Composer で使用するための別のデータベース サーバをインストールします。

重要： vCenter Server と同じ SQL Server インスタンスに View Composer データベースを作成する場合は、vCenter Server データベースを上書きしないでください。

サポートされるデータベースの最新情報については、http://www.vmware.com/resources/compatibility/sim/interop_matrix.php で VMware 製品の互換運用性マトリックスを参照してください。[ソリューション/データベースの互換運用性] について、製品とバージョンを選択した後にデータベースを追加する手順でサポートされるデータベースをすべて表示するには、[すべて] を選択して [追加] をクリックします。

ゲスト OS のシステム要件

2

Horizon Agent または Horizon Persona Management を実行しているシステムは、特定のハードウェアおよびソフトウェア要件を満たしている必要があります。

この章には、次のトピックが含まれています。

- [Horizon Agent の要件と考慮事項](#)
- [スタンドアロン Horizon Persona Management でサポートされるオペレーティング システム](#)
- [リモート表示プロトコルとソフトウェアのサポート](#)

Horizon Agent の要件と考慮事項

Horizon Agent コンポーネント（以前のリリースでは View Agent と呼ばれていた）は、セッション管理、シングル サインオン、デバイスのリダイレクトなどの機能で使用されます。すべての仮想マシン、物理システム、および RDS ホストに、Horizon Agent をインストールする必要があります。

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 (KB) の記事 <http://kb.vmware.com/kb/2150305> を参照してください。

Horizon Agent で Horizon Persona Management 設定オプションを使用するには、Horizon Agent を Windows 10、Windows 8、Windows 8.1、Windows 7、Windows Server 2012 R2、Windows Server 2008 R2、または Windows Server 2016 の仮想マシンにインストールする必要があります。このオプションは、物理コンピュータまたは RDS ホストでは動作しません。

物理コンピュータには、Horizon Persona Management のスタンドアロン バージョンをインストールできます。[スタンドアロン Horizon Persona Management でサポートされるオペレーティング システム](#)を参照してください。

注： VMware Blast 表示プロトコルを使用するには、単一セッションの仮想マシンまたは RDS ホストに Horizon Agent をインストールする必要があります。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。

セキュリティを強化するため、既知の脆弱性を除去するよう暗号化スイートを構成することをお勧めします。View Composer または Horizon Agent を実行する Windows マシン向けに暗号化スイートのドメイン ポリシーをセットアップする手順については、[SSL/TLS における強度の弱い暗号化方式の無効化](#)を参照してください。

スタンドアロン Horizon Persona Management でサポートされるオペレーティング システム

スタンドアロン Horizon Persona Management ソフトウェアでは、Horizon Agent がインストールされていないスタンドアロンの物理コンピュータと仮想マシンの個人設定管理を行うことができます。ユーザーがログインすると、そのプロファイルが、リモート プロファイル リポジトリからスタンドアロン システムに動的にダウンロードされます。

注： Horizon デスクトップ用に Persona Management を構成するには、[Persona Management] 設定オプションを使用して Horizon Agent をインストールします。スタンドアロン Persona Management ソフトウェアは、Horizon 以外のシステムのみを対象としています。

スタンドアロン Horizon Persona Management ソフトウェアでサポートされるオペレーティング システムのリストについては、VMware のナレッジベースの記事 <http://kb.vmware.com/kb/2150295> を参照してください。

スタンドアロン Persona Management ソフトウェアは、Microsoft リモート デスクトップ サービスでサポートされていません。

リモート表示プロトコルとソフトウェアのサポート

リモート表示プロトコルとリモート表示ソフトウェアで、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ます。使用されるリモート表示プロトコルは、クライアント デバイスのタイプや、リモート デスクトップとリモート アプリケーションのどちらに接続するのか、監理者がデスクトップ プールまたはアプリケーション プールをどのように構成するかなどの状況によって異なります。

■ 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。

■ 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。

■ 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。

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。
- [Horizon Agent の要件と考慮事項](#)に一覧表示されている Horizon Agent のオペレーティング システムのバージョンを実行する Windows デスクトップへの接続。
- 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 7 アーキテクチャの計画』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。

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。

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。
- [Horizon Agent の要件と考慮事項](#)に一覧表示されている Horizon Agent のオペレーティング システムのバージョンを実行する Windows デスクトップへの接続。
- 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。

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。

IPv6 環境での Horizon 7 のインストール

3

Horizon 7 は IPv4 の代用として IPv6 をサポートします。環境は IPv6 のみか、IPv4 のみのいずれかにする必要があります。Horizon 7 では、IPv6 と IPv4 の混在環境はサポートされません。

IPv4 環境でサポートされる Horizon 7 のすべての機能が IPv6 でサポートされるわけではありません。Horizon 7 は、IPv4 環境から IPv6 環境へのアップグレードはサポートしません。また、Horizon 7 は IPv4 と IPv6 間の移行もサポートしません。

重要： Horizon 7 を IPv6 環境で実行するには、すべての Horizon 7 コンポーネントのインストール時に IPv6 を指定する必要があります。

この章には、次のトピックが含まれています。

- [IPv6 環境での Horizon 7 のセットアップ](#)
- [IPv6 環境でサポートされている vSphere、データベース、および Active Directory のバージョン](#)
- [IPv6 環境でサポートされている Horizon 7 サーバ用オペレーティング システム](#)
- [IPv6 環境でサポートされているデスクトップおよび RDS ホスト用 Windows オペレーティング システム](#)
- [IPv6 環境でサポートされているクライアント](#)
- [IPv6 環境でサポートされているリモート プロトコル](#)
- [IPv6 環境でサポートされている認証タイプ](#)
- [IPv6 環境でサポートされているその他の機能](#)

IPv6 環境での Horizon 7 のセットアップ

Horizon 7 を IPv6 環境で実行するには、特定の管理タスクを実行する場合に IPv6 で固有の要件および選択肢に注意する必要があります。

Horizon 7 のインストール前に、稼働中の IPv6 環境が必要です。以下の Horizon 7 の管理タスクには、IPv6 固有のオプションがあります。

- Horizon 接続サーバのインストール。 [新しい構成での Horizon 接続サーバのインストール](#)を参照してください。

- View レプリカ サーバのインストール。 [Horizon 接続サーバの複製インスタンスのインストール](#)を参照してください。
- View セキュリティ サーバのインストール。 [セキュリティ サーバをインストールする](#)を参照してください。
- PCoIP 外部 URL の構成。 [Secure Gateway 接続およびトンネル接続用の外部 URL の構成](#)を参照してください。
- PCoIP 外部 URL の設定。 [Connection Server インスタンスの外部 URL を設定する](#)を参照してください。
- PCoIP 外部 URL の変更。 [Connection Server インスタンスの外部 URL を設定する](#)を参照してください。
- Horizon Agent のインストール。『View でのデスクトップ プールとアプリケーション プールの設定』ドキュメントにある Horizon Agent のインストールのトピックを参照してください。
- Horizon Client のインストール。 [IPv6 環境でサポートされているクライアント](#)を参照してください。

注: Horizon 7 では、管理タスクで IPv6 を入力する必要はありません。完全修飾ドメイン名 (FQDN) または IPv6 アドレスのいずれかを指定できる場合には、エラーの可能性を回避するために FQDN を指定することを強く推奨します。

IPv6 環境でサポートされている vSphere、データベース、および Active Directory のバージョン

IPv6 環境では、特定の vSphere、データベース サーバ、および Active Directory のバージョンが Horizon 7 でサポートされます。

IPv6 環境では、SQL Server 2012 以降と Oracle 11g 以降のデータベースがサポートされます。IPv6 環境でサポートされるデータベース、vSphere バージョン、Active Directory バージョンの最新情報については、http://www.vmware.com/resources/compatibility/sim/interop_matrix.php で VMware 製品の互換運用性マトリクスを参照してください。

IPv6 環境でサポートされている Horizon 7 サーバ用オペレーティング システム

IPv6 環境では、特定の Windows Server オペレーティング システムに Horizon 7 サーバをインストールする必要があります。

Horizon 7 サーバには、接続サーバ インスタンス、レプリカ サーバ、セキュリティ サーバ、および Horizon 7 インスタンスが含まれます。

オペレーティング システム	エディション
Windows Server 2016	Standard, Enterprise
Windows Server 2008 R2 SP1	Standard, Enterprise
Windows Server 2012 R2	Standard

IPv6 環境でサポートされているデスクトップおよび RDS ホスト用 Windows オペレーティング システム

IPv6 環境では、Horizon 7 はデスクトップ マシンおよび RDS ホスト用に特定の Windows オペレーティング システムをサポートします。RDS ホストは、セッションベースのデスクトップおよびアプリケーションをユーザーに提供します。

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 (KB) の記事 <http://kb.vmware.com/kb/2150305> を参照してください。

IPv6 環境でサポートされているクライアント

IPv6 環境では、Horizon 7 は特定のデスクトップ オペレーティング システム上で実行されるクライアントをサポートします。

表 3-1. サポートされている Windows オペレーティング システム

オペレーティング システム	バージョン	エディション
Windows 7、Windows 7 SP1	32 ビットまたは 64 ビット	Home、Enterprise、Professional、Ultimate
Windows 8、Windows 8.1	32 ビットまたは 64 ビット	Pro、Enterprise、および Industry Embedded
Windows 10	32 ビットまたは 64 ビット	Home、Pro、Pro for Workstations、Enterprise および IoT Enterprise

iOS デバイスでは、iOS 9.2 以降が、Horizon Client for iOS 4.1 以降でサポートされます。

macOS デバイスでは、Horizon Client for Mac 4.9 以降が必要です。

Android デバイスでは、Horizon Client for Android 4.9 以降が必要です。

Chromebook デバイスでは、Horizon Client for Android 5.1 以降が必要です。

次のクライアントはサポートされていません。

- Horizon Client for Linux、Horizon Client for Chrome、Horizon Client for Chrome OS、Horizon Client for Windows 10 UWP、Horizon Client for Windows Store
- PCoIP Zero Client

IPv6 環境でサポートされているリモート プロトコル

IPv6 環境では、特定のリモート プロトコルが Horizon 7 でサポートされます。

次のリモート プロトコルがサポートされています。

- RDP
- 安全なトンネルを使用した RDP
- PCoIP
- PCoIP Secure Gateway を経由する PCoIP
- VMware Blast
- Blast Secure Gateway を経由する VMware Blast
- Blast Extreme Adaptive Transport (BEAT)

IPv6 環境でサポートされている認証タイプ

IPv6 環境では、特定の認証タイプが Horizon 7 でサポートされます。

次の認証タイプがサポートされています。

- Active Directory を使用したパスワード認証
- スマート カード
- Single Sign-On

次の認証タイプはサポートされていません。

- SecurID
- RADIUS
- SAML

IPv6 環境でサポートされているその他の機能

IPv6 環境で、Horizon 7 はこれまでのトピックで取り扱われていない特定の機能をサポートしています。

次の機能がサポートされています。

- アプリケーション プール
- オーディオ出力
- フル仮想マシン、インスタント クローン、Horizon 7 Composer のリンク クローンを含む、自動デスクトップ プール
- Blast Extreme Adaptive Transport (BEAT)
- カスタマー エクスペリエンス向上プログラム (CEIP)
- ディスク スペース再利用
- イベント
- Horizon Performance Tracker

- HTML5 マルチメディア リダイレクト
- インスタントクローン デスクトップ プール
- LDAP バックアップ
- vCenter Server 仮想マシン、物理コンピュータ、および vCenter Server によって管理されない仮想マシンを含む、手動のデスクトップ プール
- ネイティブ NFS スナップショット (VAAI)
- 個人設定管理
- リアルタイム オーディオビデオ (RTAV)
- RDS デスクトップ プール
- RDS ホスト 3D
- ロールベースの管理
- セッション共同作業
- 現在のユーザーとしてログイン 機能を含む、シングル サインオン
- システム健全性ダッシュボード
- ThinApp
- Unity Touch
- USB リダイレクト
- Horizon 7 Composer Agent
- Horizon 7 Storage Accelerator
- Horizon 7 Composer データベースのバックアップ
- 仮想印刷
- VMware オーディオ
- VMware ビデオ
- VMware Virtualization Pack for Skype for Business (Windows のみ)

次の機能はサポートされていません。

- クライアント ドライブのリダイレクト
- クライアント IP アドレスの透過性 (64 ビットのみ)
- クラウド ポッド アーキテクチャ
- デバイス ブリッジ
- ファイルの関連付け
- Flash URL リダイレクト
- HTML Access

- Log Insight
- Lync
- RDSH インスタント クローン プールを使用する PCoIP
- スキャナ リダイレクト
- シリアル ポート リダイレクト
- Syslog
- Teradici TERA ホスト カード
- TSMMR
- URL リダイレクト
- vSAN
- Virtual Volumes
- vRealize Operations Desktop Agent

FIPS モードでの Horizon 7 のインストール

4

Horizon 7 は、FIPS (Federal Information Processing Standard) 140-2 準拠のアルゴリズムによる暗号化を実行できます。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、Horizon 7 の一部の機能がサポートされません。また、Horizon 7 では非 FIPS インストールを FIPS インストールにアップグレードすることはできません。

注： Horizon 7 を確実に FIPS モードで実行するには、すべての Horizon 7 コンポーネントをインストールするときに FIPS を有効にする必要があります。

この章には、次のトピックが含まれています。

- FIPS モードでの Horizon 7 のセットアップの概要
- FIPS モードのシステム要件

FIPS モードでの Horizon 7 のセットアップの概要

Horizon 7 を FIPS モードでセットアップするには、最初に Windows 環境で FIPS モードを有効にする必要があります。その後、すべての Horizon 7 コンポーネントを FIPS モードでインストールします。

Horizon 7 を FIPS モードでインストールするオプションは、Windows 環境で FIPS モードが有効になっている場合에만使用できます。Windows での FIPS モードの有効化に関する詳細については、<https://support.microsoft.com/en-us/kb/811833> を参照してください。

注： Horizon Administrator には、Horizon 7 が FIPS モードで実行しているかどうかが表示されません。

Horizon 7 を FIPS モードでインストールするには、次の管理タスクを実行します。

- 接続サーバをインストールするとき、FIPS モードのオプションを選択します。[新しい構成での Horizon 接続サーバのインストール](#)を参照してください。
- レプリカ サーバをインストールするとき、FIPS モードのオプションを選択します。[Horizon 接続サーバの複製インスタンスのインストール](#)を参照してください。
- セキュリティ サーバをインストールする前に、Horizon Administrator のグローバル設定である [セキュリティサーバへの接続に IPsec を使用する] の選択を解除し、手動で IPsec を構成します。<http://kb.vmware.com/kb/2000175> を参照してください。

- セキュリティ サーバをインストールするとき、FIPS モードのオプションを選択します。[セキュリティ サーバをインストールする](#)を参照してください。
- Windows システムには FIPS 処理を設定し、Horizon 7 には接続サーバとセキュリティ サーバ間の通信を IPsec で行うよう設定すると、セキュリティ サーバはインストールに失敗します。IPv4 環境では、PCoIP 外部 URL を IP アドレスとポート番号 4172 で指定します。IPv6 環境では、IP アドレスまたは完全修飾ドメイン名とポート番号 4172 を指定できます。いずれの場合も、プロトコル名を含めないでください。

たとえば、IPv4 環境の場合には、10.20.30.40:4172 になります。

クライアントは URL を使用してセキュリティ サーバにアクセスできる必要があります。
- View Composer と Horizon Agent マシンについて、強度の弱い暗号化方式を無効にします。[SSL/TLS における強度の弱い暗号化方式の無効化](#)を参照してください。
- View Composer をインストールするとき、FIPS モードのオプションを選択します。[6 章 View Composer のインストール](#)を参照してください。
- Horizon Agent をインストールするとき、FIPS モードのオプションを選択します。『Horizon 7 での仮想デスクトップのセットアップ』または『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』ドキュメントで、Horizon Agent のインストールに関するトピックを参照してください。
- Windows クライアントの場合には、クライアント オペレーティング システムで FIPS モードを有効にし、Horizon Client for Windows のインストール時に FIPS モード オプションを選択します。『VMware Horizon Client for Windows のインストールとセットアップ ガイド』ドキュメントを参照してください。
- Linux クライアントの場合には、クライアント オペレーティング システムで FIPS モードを有効にします。『VMware Horizon Client for Linux のインストールとセットアップ ガイド』ドキュメントを参照してください。

FIPS モードのシステム要件

FIPS モードをサポートするには、Horizon 7 の展開が次の要件を満たしている必要があります。

vSphere

- vCenter Server 6.0 以降
- ESXi 6.0 以降

リモート デスクトップ

- FIPS 証明書のある Windows プラットフォーム。詳細については、Microsoft TechNet Web サイトで「FIPS 140 Validation」を参照してください。
- View Agent 6.2 以降または Horizon Agent 7.0 以降（Windows プラットフォームの場合のみ）

Horizon Client

- FIPS 証明書のある Windows プラットフォーム。詳細については、Microsoft TechNet Web サイトで「FIPS 140 Validation」を参照してください。
- Horizon Client for Windows 3.5 以降

暗号化プロトコル

- TLSv1.2

Active Directory の準備

5

Horizon 7 は、ユーザーの認証と管理に既存の Microsoft Active Directory インフラストラクチャを使用します。Horizon 7 で使用するために Active Directory を準備する必要があります。

Horizon 7 は次の Active Directory Domain Services (AD DS) ドメイン機能レベルをサポートします。

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

この章には、次のトピックが含まれています。

- [ドメインと信頼関係の構成](#)
- [リモート デスクトップの OU の作成](#)
- [キオスク モード クライアント アカウントの OU とグループの作成](#)
- [ユーザーのグループの作成](#)
- [vCenter Server のユーザー アカウントの作成](#)
- [スタンドアロンの View Composer Server のユーザー アカウントの作成](#)
- [View Composer AD 操作のユーザー アカウントの作成](#)
- [インスタントクローン操作のユーザー アカウントの作成](#)
- [制限されたグループ ポリシーを構成する](#)
- [Horizon 7 グループ ポリシー管理用テンプレート ファイルの使用](#)
- [スマート カード認証用の Active Directory を準備する](#)
- [SSL/TLS における強度の弱い暗号化方式の無効化](#)

ドメインと信頼関係の構成

各 Connection Server ホストは、Active Directory ドメインに参加させる必要があります。ホストをドメイン コントローラにすることはできません。

Active Directory は、Horizon Agent マシン（単一ユーザーのマシンや RDS ホストなど）や Horizon 7 展開環境のユーザーおよびグループも管理します。Horizon Administrator では、リモート デスクトップおよびアプリケーションに対する資格をユーザーやグループに付与したり、管理者となるユーザーやグループを選択したりできます。

Horizon Agent マシン、View Composer Server、およびユーザーやグループを次の Active Directory ドメインに配置できます。

- Connection Server ドメイン
- Connection Server 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 Connection Server ドメインによって信頼されている、Connection Server 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 Connection Server ドメインによって信頼されている、Connection Server ドメインとは異なるフォレスト内のドメイン

ユーザーは、Active Directory を使用して Connection Server のドメインに対して認証され、さらに信頼契約の存在する追加ユーザー ドメインがある場合はそのドメインに対しても認証されます。

ユーザーやグループが一方向で信頼されているドメインにある場合、Horizon Administrator の管理者ユーザーに 2 番目の認証情報を提供する必要があります。2 番目の認証情報がないと、管理者は一方向で信頼されているドメインへのアクセス権を付与できません。一方向で信頼されているドメインは、外部ドメインまたは推移的なフォレストの信頼のドメインになります。

2 番目の認証情報は、エンド ユーザーのデスクトップまたはアプリケーション セッションではなく、Horizon Administrator セッションでのみ必要になります。2 番目の認証情報が必要なのは管理者ユーザーだけです。

vdmadmin -T コマンドを使用して、2 番目の認証情報を指定できます。

- 個々の管理者ユーザーに 2 番目の認証情報を構成します。
- フォレストの信頼の場合、フォレストのルート ドメインに 2 番目の認証情報を構成できます。こうすることで、Connection Server はフォレストの信頼の子ドメインを列挙できるようになります。

詳細については、『Horizon 7 の管理』ドキュメントの「-T オプションを使用した、管理者の 2 番目の認証情報の指定」を参照してください。

ユーザーのスマート カードと SAML 認証は、一方向の信頼ドメインでサポートされていません。

Horizon 7 バージョン 7.10 以降では、Horizon Client for Windows の「現在のユーザーとしてログイン」機能は、一方向の信頼ドメインでサポートされます。

注： セキュリティ サーバは、認証リポジトリ（Active Directory など）にアクセスしないため、Active Directory ドメイン内に存在する必要はありません。

信頼関係とドメインのフィルタ処理

アクセスできるドメインを判別するため、接続サーバ インスタンスは、それ自体のドメインから始めて信頼関係をたどります。

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接続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` コマンドを使用して、ドメインのフィルタ処理を設定し、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 の管理』ドキュメントを参照してください。

名前サフィックスの除外を使用してフォレストの信頼が構成されている場合、構成された除外は、フォレストの子ドメインのリストをフィルタ処理するために使用されます。`vdmadmin` コマンドで指定されたフィルタ処理に加えて、名前のサフィックスの除外によるフィルタ処理が適用されます。

リモート デスクトップの OU の作成

リモート デスクトップ固有の組織単位 (OU) を作成する必要があります。OU は、ユーザー、グループ、コンピュータ、または他の OU を含む、Active Directory 内の区画です。

デスクトップと同じドメイン内の他の Windows サーバまたはワークステーションにポリシー設定が適用されないようにするには、Horizon 7 グループ ポリシーの GPO を作成し、それをリモート デスクトップが含まれる OU にリンクします。また、サーバ オペレータや個々のユーザーなどのような従属グループに OU の制御を委任することもできます。

View Composer を使用する場合は、リモート デスクトップの OU に基づいた別の Active Directory コンテナをリンク クローン デスクトップ用に作成する必要があります。Active Directory で OU 管理者権限を持つ管理者は、ドメイン管理者権限がなくてもリンク クローン デスクトップをプロビジョニングできます。Active Directory の管理者認証情報を変更する場合は、View Composer の認証情報も更新する必要があります。

キオスク モード クライアント アカウントの OU とグループの作成

キオスク モードのクライアントは、シン クライアントまたはロックダウン PC であり、クライアント ソフトウェアを実行して接続サーバ インスタンスに接続し、リモート デスクトップ セッションを開始します。クライアントをキオスク モードで構成する場合は、キオスク モード クライアント アカウント用に専用の OU とグループを Active Directory で作成する必要があります。

キオスク モード クライアント アカウント用に専用の OU とグループを作成することで、許可されていない侵入に対してクライアント システムを分割でき、クライアントの構成と管理が簡単になります。

詳細については、『Horizon 7 の管理』ドキュメントを参照してください。

ユーザーのグループの作成

異なる種類のユーザーごとに Active Directory でグループを作成する必要があります。たとえば、エンド ユーザーに対して Horizon 7 Users という名前のグループを作成し、リモート デスクトップおよびアプリケーションを管理するユーザーに対しては Horizon 7 Administrators という名前の別のグループを作成できます。

vCenter Server のユーザー アカウントの作成

vCenter Server で使用するユーザー アカウントを Active Directory に作成する必要があります。Horizon Administrator で vCenter Server インスタンスを追加するときに、このユーザー アカウントを指定します。

vCenter Server で特定の操作を実行するための権限をユーザー アカウントに付与する必要があります。適切な権限を持つ vCenter Server ロールを作成し、そのロールを vCenter Server ユーザーに割り当てることができます。vCenter Server ロールに追加する権限リストは、View Composer ありまたはなしで Horizon 7 を使用するかどうかに応じて変わります。これらの権限の構成方法については、[vCenter Server](#)、[View Composer](#) および[インストール クローンのユーザー アカウントの構成](#)を参照してください。

vCenter Server と同じマシンに View Composer をインストールする場合、vCenter Server ユーザーを vCenter Server マシンのローカル管理者グループに追加する必要があります。この要件により、Horizon 7 で View Composer サービスの認証を行うことができます。

View Composer を vCenter Server とは別のマシンにインストールする場合、vCenter Server ユーザーを vCenter Server マシン上のローカル管理者にする必要はありません。ただし、View Composer マシン上のローカル管理者となる必要があるスタンドアロンの View Composer Server ユーザー アカウントを作成する必要があります。

スタンドアロンの View Composer Server のユーザー アカウントの作成

View Composer を vCenter Server とは別のマシンにインストールする場合、Horizon 7 がスタンドアロンのマシンで View Composer サービスへの認証に使用できるドメイン ユーザー アカウントを Active Directory で作成する必要があります。

ユーザー アカウントは、接続サーバ ホストと同じドメインまたは信頼されたドメインに存在する必要があります。ユーザー アカウントをスタンドアロンの View Composer マシンのローカル管理者グループに追加する必要があります。

Horizon Administrator で View Composer を設定し [スタンドアロン View Composer Server] を選択するとき、ユーザー アカウントを指定します。[View Composer 設定を構成する](#)を参照してください。

View Composer AD 操作のユーザー アカウントの作成

View Composer を使用する場合、View Composer が Active Directory で特定の操作を実行できるようになるユーザー アカウントを、Active Directory で作成する必要があります。View Composer では、リンク クローン仮想マシンを Active Directory ドメインに参加させるためにこのアカウントが必要です。

セキュリティのため、View Composer で使用するためのユーザー アカウントを別に作成する必要があります。別のアカウントを作成することで、他の目的のために定義されている追加権限がアカウントに付与されないようにすることができます。このアカウントには、指定された Active Directory コンテナ内のコンピュータ オブジェクトを追加および削除するために必要な最小限の権限を付与できます。たとえば、View Composer アカウントにはドメイン管理者権限は必要ありません。

手順

- 1 Active Directory で、接続サーバ ホストと同じドメインまたは信頼されたドメインにユーザー アカウントを作成します。
- 2 リンク クローン コンピュータ アカウントを中に作成する、またはリンク クローン コンピュータ アカウントを移動する先の Active Directory コンテナで、[コンピュータ オブジェクトの作成] 権限、[コンピュータ オブジェクトの削除] 権限、および [すべてのプロパティの書き込み] 権限をアカウントに追加します。

次のリストでは、ユーザー アカウントに必要なすべての権限を示します。デフォルトで割り当てられる権限も含まれます。

- 内容の一覧表示
- すべてのプロパティの読み取り
- すべてのプロパティの書き込み
- アクセス許可の読み取り
- パスワードのリセット
- コンピュータ オブジェクトの作成
- コンピュータ オブジェクトの削除

注： デスクトップ プールの[Allow reuse of pre-existing computer accounts]設定を選択する場合、必要な権限はより少なくなります。次の権限がユーザー アカウントに割り当てられていることを確認します。

- 内容の一覧表示
 - すべてのプロパティの読み取り
 - アクセス許可の読み取り
 - パスワードのリセット
-

- 3 ユーザー アカウントの権限が Active Directory コンテナおよびコンテナのすべての子オブジェクトに適用されることを確認します。

次のステップ

[vCenter Server を追加] ウィザードで View Composer ドメインを構成時、およびリンク クローン デスクトップ プールを構成して展開する際に、Horizon Administrator でこのアカウントを指定します。

インスタントクローン操作のユーザー アカウントの作成

インスタント クローンをデプロイする前に、Active Directory で一部の操作を実行する権限を持つユーザー アカウントを作成する必要があります。

インスタントクローン デスクトップ プールをデプロイする前に、インスタントクローン ドメイン管理者を追加する場合、このアカウントを選択します。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』ドキュメントの「インスタントクローンのドメイン管理者の追加」を参照してください。

手順

- 1 Active Directory で、接続サーバと同じドメインまたは信頼されたドメインにユーザー アカウントを作成します。
- 2 [コンピュータ オブジェクトの作成]、[コンピュータ オブジェクトの削除]、および [すべてのプロパティの書き込み] の許可を、インスタントクローン コンピュータ アカウントのコンテナのアカウントに追加します。

次のリストでは、ユーザー アカウントに必要な権限を示します。デフォルトで割り当てられる権限も含まれます。

- 内容の一覧表示
- すべてのプロパティの読み取り
- すべてのプロパティの書き込み
- アクセス許可の読み取り
- パスワードのリセット
- コンピュータ オブジェクトの作成
- コンピュータ オブジェクトの削除

権限が適正なコンテナおよびコンテナのすべての子オブジェクトに適用されることを確認します。

制限されたグループ ポリシーを構成する

リモート デスクトップに接続できるには、ユーザーがリモート デスクトップのローカルの Remote Desktop Users グループに属している必要があります。Active Directory の制限付きグループ ポリシーを使用して、ドメインに参加している各リモート デスクトップのローカルの Remote Desktop Users グループにユーザーまたはグループを追加することができます。

制限付きグループ ポリシーは、制限付きグループ ポリシーで定義されたメンバーシップ リスト設定と一致するように、ドメイン内にあるコンピュータのローカル グループ メンバーシップを設定します。リモート デスクトップ ユーザー グループのメンバーは、ドメインに参加している各リモート デスクトップのローカルの Remote Desktop Users グループに常に追加されます。新しいユーザーを追加するときは、リモート デスクトップ ユーザー グループに追加するだけで済みます。

これらの手順は、Horizon 7 仮想デスクトップまたは公開デスクトップとアプリケーションが参加しているドメインの Active Directory サーバに適用されます。

前提条件

Active Directory のドメインにリモート デスクトップ ユーザーのグループを作成します。たとえば、「Horizon Users」という名前のグループを作成します。

手順

- 1 Active Directory サーバで、Group Policy Management プラグインに移動します。

Active Directory のバージョン	ナビゲーション パス
Windows 2003	<ol style="list-style-type: none"> a [スタート] - [すべてのプログラム] - [管理ツール] - [Active Directory ユーザーとコンピュータ] の順に選択します。 b ドメインを右クリックして、[プロパティ] をクリックします。 c [グループ ポリシ] タブで、[開く] をクリックして Group Policy Management プラグインを開きます。 d [既定のドメイン ポリシー] を右クリックし、[編集] をクリックします。
Windows 2008	<ol style="list-style-type: none"> a [スタート] - [管理ツール] - [グループ ポリシーの管理] の順に選択します。 b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。
Windows 2012 R2	<ol style="list-style-type: none"> a [スタート] - [管理ツール] - [グループ ポリシーの管理] の順に選択します。 b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。
Windows 2016	<ol style="list-style-type: none"> a [スタート] - [管理ツール] - [グループ ポリシーの管理] の順に選択します。 b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。

- 2 [コンピュータの構成] セクションを展開し、[Windows 設定¥セキュリティ設定] を開きます。
- 3 [制限付きグループ] を右クリックし、[グループの追加] を選択し、Remote Desktop Users グループを追加します。
- 4 グループを右クリックし、新しいリモート デスクトップ ユーザー グループをグループ メンバーシップ リストに追加します。
たとえば、「Horizon Users」をリモート デスクトップ ユーザーに追加します。
- 5 [OK] をクリックして変更を保存します。

Horizon 7 グループ ポリシー管理用テンプレート ファイルの使用

Horizon 7 には、コンポーネントに固有の複数のグループ ポリシー管理用 (ADMX) テンプレート ファイルが含まれます。

Horizon 7 のグループ ポリシー設定用のすべての ADMX ファイルは、VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip に含まれています。x.x.x はバージョン番号、yyyyyyy はビルド番号です。このファイルは、<https://my.vmware.com/web/vmware/downloads> の VMware ダウンロード サイトからダウンロードできます。[Desktop & End-User Computing (デスクトップおよびエンドユーザー コンピューティング)] で VMware Horizon 7 のダウンロードを選択します。これには ZIP ファイルが含まれます。

これらのファイルのポリシー設定を Active Directory の新規 GPO または既存 GPO に追加した後、使用中のデスクトップを含む OU にその GPO を結び付けることで、リモート デスクトップを最適化し、セキュリティを強化できます。

Horizon 7 グループ ポリシー設定の使用方法については、『Horizon 7 の管理』と『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 カード認証用の Active Directory を準備する

スマート カード認証を実装するときは、Active Directory で特定のタスクを実行する必要があります。

■ スマート カード ユーザーの UPN を追加する

スマート カード ログインはユーザー プリンシパル名 (UPN) に依存するので、Horizon 7 での認証にスマート カードを使用するユーザーおよび管理者の Active Directory アカウントには有効な UPN が必要です。

■ 信頼されたルート証明機関へのルート証明書の追加

証明機関 (CA) を使用してスマート カード ログイン証明書またはドメイン コントローラ証明書を発行する場合は、Active Directory でルート証明書を信頼されたルート証明機関グループ ポリシーに追加する必要があります。Windows ドメイン コントローラがルート CA として機能する場合は、この手順を実行する必要はありません。

■ 中間証明機関への中間証明書の追加

中間証明機関 (CA) を使用してスマート カード ログイン証明書またはドメイン コントローラ証明書を発行する場合は、Active Directory で中間証明書を中間証明機関グループ ポリシーに追加する必要があります。

■ Enterprise NTAAuth ストアにルート証明書を追加する

CA を使用してスマート カード ログイン証明書またはドメイン コントローラ証明書を発行する場合は、Active Directory でルート証明書を Active Directory の Enterprise NTAAuth ストアに追加する必要があります。Windows ドメイン コントローラがルート CA として機能する場合は、この手順を実行する必要はありません。

スマート カード ユーザーの UPN を追加する

スマート カード ログインはユーザー プリンシパル名 (UPN) に依存するので、Horizon 7 での認証にスマート カードを使用するユーザーおよび管理者の Active Directory アカウントには有効な UPN が必要です。

スマート カード ユーザーが属しているドメインが、ルート証明書が発行されたドメインとは異なる場合は、ユーザーの UPN を、信頼された CA のルート証明書に含まれるサブジェクトの別名 (SAN) に設定する必要があります。ルート証明書がスマート カード ユーザーの現在のドメイン内のサーバから発行された場合は、ユーザーの UPN を変更する必要はありません。

注： 証明書が同じドメインから発行された場合であっても、組み込み Active Directory アカウントの UPN を設定することが必要な場合があります。Administrator などの組み込みアカウントには、デフォルトでは UPN は設定されません。

前提条件

- 証明書のプロパティを表示して、信頼された CA のルート証明書に含まれる SAN を取得します。

- Active Directory サーバに ADSI Edit ユーティリティがない場合は、Microsoft の Web サイトから適切な Windows Support Tools をダウンロードし、インストールします。

手順

- 1 Active Directory サーバで ADSI Edit ユーティリティを起動します。
- 2 左ペインで、ユーザーがいるドメインを展開し、CN=Users をダブルクリックします。
- 3 右ペインで、ユーザーを右クリックして [プロパティ] をクリックします。
- 4 userPrincipalName 属性をダブルクリックし、信頼された CA 証明書の SAN 値を入力します。
- 5 [OK] をクリックして属性の設定を保存します。

信頼されたルート証明機関へのルート証明書の追加

証明機関（CA）を使用してスマート カード ログイン証明書またはドメイン コントローラ証明書を発行する場合は、Active Directory でルート証明書を信頼されたルート証明機関グループ ポリシーに追加する必要があります。Windows ドメイン コントローラがルート CA として機能する場合は、この手順を実行する必要はありません。

手順

- 1 Active Directory サーバで、Group Policy Management プラグインに移動します。

Active Directory のバージョン	ナビゲーション パス
Windows 2003	<ol style="list-style-type: none"> a [スタート] - [すべてのプログラム] - [管理ツール] - [Active Directory ユーザーとコンピュータ] の順に選択します。 b ドメインを右クリックして、[プロパティ] をクリックします。 c [グループ ポリシ] タブで、[開く] をクリックして Group Policy Management プラグインを開きます。 d [既定のドメイン ポリシー] を右クリックし、[編集] をクリックします。
Windows 2008	<ol style="list-style-type: none"> a [スタート] - [管理ツール] - [グループ ポリシーの管理] の順に選択します。 b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。
Windows 2012 R2	<ol style="list-style-type: none"> a [スタート] - [管理ツール] - [グループ ポリシーの管理] の順に選択します。 b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。
Windows 2016	<ol style="list-style-type: none"> a [スタート] - [管理ツール] - [グループ ポリシーの管理] の順に選択します。 b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。

- 2 [コンピュータの構成] セクションを展開し、[Windows 設定¥セキュリティ設定¥開鍵] を開きます。
- 3 [信頼されたルート証明機関] を右クリックして、[インポート] を選択します。
- 4 ウィザードの指示に従ってルート証明書（rootCA.cer など）をインポートし、[OK] をクリックします。
- 5 [グループ ポリシー] ウィンドウを閉じます。

結果

ドメイン内のすべてのシステムの信頼されたルート ストアに、ルート証明書がコピーされます。

次のステップ

中間証明機関（CA）がスマート カードのログイン証明書またはドメイン コントローラ証明書を発行する場合は、Active Directory で中間証明機関のグループ ポリシーに中間証明書を追加します。[中間証明機関への中間証明書の追加](#)を参照してください。

中間証明機関への中間証明書の追加

中間証明機関（CA）を使用してスマート カード ログイン証明書またはドメイン コントローラ証明書を発行する場合は、Active Directory で中間証明書を中間証明機関グループ ポリシーに追加する必要があります。

手順

- 1 Active Directory サーバで、Group Policy Management プラグインに移動します。

Active Directory のバージョン	ナビゲーション パス
Windows 2003	<ol style="list-style-type: none"> a [スタート] - [すべてのプログラム] - [管理ツール] - [Active Directory ユーザーとコンピュータ] の順に選択します。 b ドメインを右クリックして、[プロパティ] をクリックします。 c [グループ ポリシ] タブで、[開く] をクリックして Group Policy Management プラグインを開きます。 d [既定のドメイン ポリシー] を右クリックし、[編集] をクリックします。
Windows 2008	<ol style="list-style-type: none"> a [スタート] - [管理ツール] - [グループ ポリシーの管理] の順に選択します。 b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。
Windows 2012 R2	<ol style="list-style-type: none"> a [スタート] - [管理ツール] - [グループ ポリシーの管理] の順に選択します。 b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。
Windows 2016	<ol style="list-style-type: none"> a [スタート] - [管理ツール] - [グループ ポリシーの管理] の順に選択します。 b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。

- 2 [コンピュータの構成] セクションを展開し、[Windows Settings\Security Settings\Public Key] のポリシーを開きます。
- 3 [中間証明機関] を右クリックして、[インポート] を選択します。
- 4 ウィザードの指示に従って中間証明書（intermediateCA.cer など）をインポートし、[OK] をクリックします。
- 5 [グループ ポリシー] ウィンドウを閉じます。

結果

ドメイン内のすべてのシステムの中間証明機関ストアに、中間証明書がコピーされます。

Enterprise NTAAuth ストアにルート証明書を追加する

CA を使用してスマート カード ログイン証明書またはドメイン コントローラ証明書を発行する場合は、Active Directory でルート証明書を Active Directory の Enterprise NTAAuth ストアに追加する必要があります。Windows ドメイン コントローラがルート CA として機能する場合は、この手順を実行する必要はありません。

手順

- ◆ Active Directory サーバで、certutil コマンドを使用して、証明書を Enterprise NTAAuth ストアに発行します。

例 : `certutil -dspublish -f ルート CA 証明書へのパス NTAAuthCA`

結果

CA がこの種の証明書の発行元として信頼されるようになります。

SSL/TLS における強度の弱い暗号化方式の無効化

より強固なセキュリティを実現するため、View Composer と View Agent または Horizon Agent を実行する Windows ベースのマシンが SSL/TLS プロトコルによる通信で弱い暗号化方式を使用しないように、ドメイン ポリシーの GPO（グループ ポリシー オブジェクト）を構成できます。

手順

- 1 Active Directory サーバで、[スタート] - [管理ツール] - [グループ ポリシー管理] を選択し、その GPO を右クリックし、[編集] を選択して編集します。
- 2 グループ ポリシー管理エディタで、[コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [ネットワーク] - [SSL 設定] に移動します。
- 3 [SSL 暗号の順位] をダブルクリックします。
- 4 [SSL 暗号の順位] ウィンドウで [有効] をクリックします。
- 5 [オプション] ペインで、[SSL 暗号] テキスト ボックスの内容全体を次の暗号リストに置き換えます。

```
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA
```

上記に示した暗号化スイートは、読みやすいように複数の行に分割されています。このリストをテキスト ボックスに追加するときは、カンマの後にスペースを入れずに 1 行の暗号化スイートとして貼り付ける必要があります。

- 6 グループ ポリシー管理エディタを閉じます。

- 7 View Composer と View Agent または Horizon Agent マシンを再起動すると、新しいグループ ポリシーが適用されます。

View Composer のインストール

6

View Composer を使用するには、View Composer データベースを作成し、View Composer サービスをインストールし、View Composer をサポートするように View インフラストラクチャを最適化します。vCenter Server と同じホスト、または別のホストに View Composer サービスをインストールできます。

View Composer はオプションの機能です。View Composer は、リンク クローン デスクトップ プールを展開する場合にインストールします。

View Composer 機能をインストールして使用するには、ライセンスが必要です。

注： View Composer をインストールする前に、Active Directory の準備が整っていることを確認してください。

注： vCenter Server 6.5 がインストールされているマシンに View Composer をインストールした場合、View Composer の動作が vCenter Server と異なることがあります。詳細については、VMware ナレッジベースの記事 <https://kb.vmware.com/s/article/2150066> 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。

- View Composer データベースの準備
- View Composer 向けに SSL 証明書を構成する
- View Composer サービスのインストール
- View Composer から vCenter および ESXi 接続で TLSv1.0 を有効にする
- View Composer 用のインフラストラクチャの構成

View Composer データベースの準備

View Composer データを格納するためのデータベースとデータ ソース名 (DSN) を作成する必要があります。

View Composer サービスにはデータベースは含まれません。ネットワーク環境にデータベース インスタンスが存在しない場合、インスタンスをインストールする必要があります。データベース インスタンスをインストールした後、View Composer データベースをそのインスタンスに追加します。

View Composer データベースは、vCenter Server データベースが配置されているインスタンスに追加できます。データベースは、ローカルまたはリモートで、ネットワーク接続された Linux、UNIX、または Windows Server コンピュータ上のいずれかで構成することができます。

View Composer データベースには、View Composer で使用される接続とコンポーネントについての情報が格納されます。

- vCenter Server の接続
- Active Directory の接続
- View Composer によって展開されるリンク クローン デスクトップ
- View Composer によって作成されるレプリカ

View Composer サービスの各インスタンスには、専用の View Composer データベースが必要です。複数の View Composer サービスで 1 つの View Composer データベースを共有することはできません。

サポートされるデータベース バージョンのリストについては、以下を参照してください：[View Composer およびイベント データベースのデータベース要件](#)。

View Composer データベースをインストール済みのデータベース インスタンスに追加するには、次のいずれかの手順を選択します。

- [View Composer 用の SQL Server データベースの作成](#)

View Composer は、リンク クローン デスクトップの情報を SQL Server データベースに格納できます。

View Composer データベースを SQL Server に追加し、それに対する ODBC データ ソースを構成することで、データベースを作成します。

- [View Composer 用の Oracle データベースの作成](#)

View Composer は、リンク クローン デスクトップの情報を Oracle 12c または 11g データベースに格納できます。View Composer データベースを既存の Oracle インスタンスに追加し、それに対する ODBC データ ソースを構成することで、データベースを作成します。新しい View Composer データベースを追加するには、Oracle Database Configuration Assistant を使用するか、SQL ステートメントを実行します。

View Composer 用の SQL Server データベースの作成

View Composer は、リンク クローン デスクトップの情報を SQL Server データベースに格納できます。View Composer データベースを SQL Server に追加し、それに対する ODBC データ ソースを構成することで、データベースを作成します。

手順

1 [View Composer データベースを SQL Server に追加する](#)

新しい View Composer データベースを既存の Microsoft SQL Server インスタンスに追加し、View Composer のリンク クローン データを格納できます。

2 (オプション) [データベース ロールの手動作成による SQL Server データベース権限の設定](#)

この推奨方法を使用して、View Composer データベース管理者は Microsoft SQL Server データベース ロールによって付与される View Composer 管理者の権限を設定できます。

3 [ODBC データ ソースを SQL Server に追加する](#)

View Composer データベースを SQL Server に追加した後、新しいデータベースへの ODBC 接続を構成して、View Composer サービスがこのデータ ソースに接続できるようにする必要があります。

View Composer データベースを SQL Server に追加する

新しい View Composer データベースを既存の Microsoft SQL Server インスタンスに追加し、View Composer のリンク クローン データを格納できます。

View Composer がインストールされるシステム上にデータベースがローカルに存在する場合は、統合 Windows 認証セキュリティ モデルを使用できます。データベースがリモート システム上にある場合は、この認証方法を使用できません。

前提条件

- サポートされているバージョンの SQL Server が View Composer をインストールするコンピュータまたはネットワーク環境にインストールされていることを確認します。詳細については、[View Composer およびイベント データベースのデータベース要件](#)を参照してください。
- SQL Server Management Studio を使用してデータベースを作成し管理することを確認します。または、次の Web サイトからダウンロードしてインストールできる SQL Server Management Studio Express を使用できます。

<http://www.microsoft.com/en-us/download/details.aspx?id=7593>

手順

- 1 View Composer コンピュータで、[スタート] - [すべてのプログラム] - [Microsoft SQL Server 2014]、[Microsoft SQL Server 2012] または [Microsoft SQL Server 2008] を選択します。
- 2 [SQL Server Management Studio] を選択し、SQL Server インスタンスに接続します。
- 3 [オブジェクト エクスプローラ] パネルで、[データベース] エントリを右クリックし、[[新しいデータベース]] を選択します。

Initial size と Autogrowth のパラメータのデフォルト値を、データベースとログ ファイルに使用できます。

- 4 [新しいデータベース] ダイアログ ボックスで、[データベース名] テキスト ボックスに名前を入力します。

例：ViewComposer

- 5 [OK] をクリックします。

SQL Server Management Studio により、[オブジェクト エクスプローラ] パネルの [データベース] エントリにデータベースが追加されます。

- 6 Microsoft SQL Server Management Studio を終了します。

次のステップ

オプションで、[データベース ロールの手動作成による SQL Server データベース権限の設定](#)の説明に従います。

以下の説明に従います。[ODBC データ ソースを SQL Server に追加する](#)

データベース ロールの手動作成による SQL Server データベース権限の設定

この推奨方法を使用して、View Composer データベース管理者は Microsoft SQL Server データベース ロールによって付与される View Composer 管理者の権限を設定できます。

この方法が推奨されるのは、View Composer をインストールしてアップグレードする View Composer 管理者の [db_owner] ロール をセットアップする必要がないからです。

この手順では、データベース ログイン名、ユーザー名、データベース ロールの独自の名前を入力できます。[[vcmpuser]], [VCMP_ADMIN_ROLE], [VCMP_USER_ROLE] は名前の例です。View Composer データベースを作成すると [dbo] スキーマが作成されます。[dbo] スキーマ名を使用する必要があります。

前提条件

- View Composer データベースが作成されていることを確認します。 [View Composer データベースを SQL Server に追加する](#) を参照してください。

手順

- 1 sysadmin (SA) として Microsoft SQL Server Management Studio セッションにログインするか、sysadmin の権限を持ったユーザー アカウントとしてログインします。
- 2 適切な SQL Server データベース権限を付与されるユーザーを作成します。

```
use ViewComposer
go
CREATE LOGIN [vcmpuser] WITH PASSWORD=N'vcmpuser!0', DEFAULT_DATABASE=ViewComposer,
DEFAULT_LANGUAGE=us_english, CHECK_POLICY=OFF
go
CREATE USER [vcmpuser] for LOGIN [vcmpuser]
go
use MSDB
go
CREATE USER [vcmpuser] for LOGIN [vcmpuser]
go
```

- 3 View Composer データベースで、データベース ロール [VCMP_ADMIN_ROLE] を作成します。
- 4 View Composer データベースで、[VCMP_ADMIN_ROLE] に権限を付与します。
 - a [ALTER]、[REFERENCES]、[INSERT] の各スキーマ権限を、[dbo] スキーマに付与します。
 - b [CREATE TABLE]、[CREATE VIEW] および [CREATE PROCEDURES] の各権限を付与します。
- 5 View Composer データベースで、[VCMP_USER_ROLE] を作成します。
- 6 View Composer データベースで、[SELECT]、[INSERT]、[DELETE]、[UPDATE]、[EXECUTE] の各スキーマ権限を、[dbo] スキーマで [VCMP_USER_ROLE] に付与します。
- 7 [VCMP_USER_ROLE] をユーザー [[vcmpuser]] に付与します。
- 8 [VCMP_ADMIN_ROLE] をユーザー [[vcmpuser]] に付与します。
- 9 MSDB データベースで、ユーザー ロール [VCMP_ADMIN_ROLE] を作成します。

10 権限を MSDB の [VCMP_ADMIN_ROLE] に付与します。

- a MSDB テーブル syscategories、sysjobsteps および sysjobs で、[SELECT] 権限をユーザー [[vcmpuser]] に付与します。
- b MSDB ストアド プロシージャ sp_add_job、sp_delete_job、sp_add_jobstep、sp_update_job、sp_add_jobserver、sp_add_jobschedule および sp_add_category で、[EXECUTE] 権限をロール [VCMP_ADMIN_ROLE] に付与します。

11 MSDB データベースで、[VCMP_ADMIN_ROLE] をユーザー [[vcmpuser]] に付与します。

12 SQL Server ログイン [vcmpuser] を使用して ODBC システムの DSN を作成します。

手順については、[ODBC データ ソースを SQL Server に追加する](#)を参照してください。

13 View Composer をインストールします。

手順については、[View Composer サービスのインストール](#)を参照してください。

14 MSDB データベースで、ユーザー [[vcmpuser]] の [VCMP_ADMIN_ROLE] を破棄します。

ロールを破棄したら、ロールを非アクティブのままにすることも、セキュリティ向上のためにロールを削除することもできます。

ODBC データ ソースを SQL Server に追加する

View Composer データベースを SQL Server に追加した後、新しいデータベースへの ODBC 接続を構成して、View Composer サービスがこのデータ ソースに接続できるようにする必要があります。

View Composer 用に ODBC DSN を構成する場合、基盤のデータベース接続を環境に適切なレベルに設定します。データベース接続の安全設定の詳細については、SQL Server のドキュメントを参照してください。

基盤のデータベース接続で SSL 暗号化を使用する場合、信頼される CA によって署名されている SSL 証明書と一緒にデータベース サーバを構成することをお勧めします。自己署名証明書を使用した場合、データベース接続は中間者攻撃を受けやすくなります。

前提条件

以下で説明する手順を実行します。[View Composer データベースを SQL Server に追加する](#)

手順

- 1 View Composer がインストールされるコンピュータで、[スタート] - [管理ツール] - [データ ソース (ODBC)] を選択します。
- 2 [システム DSN] タブを選択します。
- 3 [追加] をクリックし、リストから [SQL Native Client] を選択します。
- 4 [終了] をクリックします。
- 5 [Create a New Data Source to SQL Server (SQL Server に接続するための新規データ ソースを作成する)] セットアップ ウィザードで、View Composer データベースの名前と説明を入力します。

例：ViewComposer

- 6 [サーバ] テキスト ボックスに、SQL Server のデータベース名を入力します。

host_name>*¥server_name* の形式を使用します。*host_name* はコンピュータの名前で、*server_name* は SQL Server インスタンスです。

例：VCHOST1\VIM_SQLEXP

- 7 [次へ] をクリックします。

- 8 [SQL Server に接続して追加の構成オプションの既定設定を取得する] チェック ボックスがオンになっていることを確認し、認証オプションを選択します。

オプション	説明
統合 Windows 認証	SQL Server のローカル インスタンスを使用している場合は、このオプションを選択します。このオプションは信頼された認証とも呼ばれます。統合 Windows 認証は、SQL Server がローカル コンピュータ上で実行している場合にのみサポートされます。
SQL Server 認証	SQL Server のリモート インスタンスを使用している場合は、このオプションを選択します。Windows NT 認証はリモート SQL Server ではサポートされません。 SQL Server データベース権限を手動で設定しユーザーに割り当てている場合、そのユーザーの認証を行います。たとえば、ユーザー vcmpuser を認証します。それ以外の場合、sysadmin (SA) または sysadmin 権限を持つユーザー アカウントとして認証します。

- 9 [次へ] をクリックします。

- 10 [既定のデータベースを以下のものに変更する] チェック ボックスをオンにして、リストから View Composer データベースの名前を選択します。

例：ViewComposer

- 11 SSL を有効化して SQL Server 接続の構成を行う場合は、[Microsoft SQL Server DSN 構成] ページに移動して、[強力なデータ暗号化を使用] を選択します。

- 12 終了し、[Microsoft ODBC データ ソース アドミニストレータ] ウィザードを閉じます。

次のステップ

新しい View Composer サービスをインストールします。[View Composer サービスのインストール](#)を参照してください。

View Composer 用の Oracle データベースの作成

View Composer は、リンク クローン デスクトップの情報を Oracle 12c または 11g データベースに格納できます。View Composer データベースを既存の Oracle インスタンスに追加し、それに対する ODBC データ ソースを構成することで、データベースを作成します。新しい View Composer データベースを追加するには、Oracle Database Configuration Assistant を使用するか、SQL ステートメントを実行します。

■ View Composer データベースを Oracle 12c または 11g に追加

Oracle Database Configuration Assistant を使用すると、新しい View Composer データベースを既存の Oracle 12c または 11g インスタンスに追加できます。

■ SQL ステートメントを使用して View Composer データベースを Oracle インスタンスに追加する

■ View Composer 用に Oracle データベース ユーザーを構成する

デフォルトでは、View Composer データベースを実行するデータベース ユーザーは Oracle システム管理者権限を持ちます。View Composer データベースを実行するユーザーのセキュリティ許可を制限するには、特定の権限を持つ Oracle データベース ユーザーを構成する必要があります。

■ ODBC データ ソースを Oracle 12c または 11g に追加

View Composer データベースを Oracle 12c または 11g のインスタンスに追加した後、新しいデータベースへの ODBC 接続を構成して、View Composer サービスがこのデータ ソースに接続できるようにする必要があります。

View Composer データベースを Oracle 12c または 11g に追加

Oracle Database Configuration Assistant を使用すると、新しい View Composer データベースを既存の Oracle 12c または 11g インスタンスに追加できます。

前提条件

サポートされているバージョンの Oracle 12c または 11g がローカルまたはリモート コンピュータにインストールされていることを確認します。[View Composer およびイベント データベースのデータベース要件](#)を参照してください。

手順

- 1 View Composer データベースを追加するコンピュータで [Database Configuration Assistant] を起動します。

データベースのバージョン	アクション
Oracle 12c	[スタート] - [すべてのプログラム] - [Oracle-OraDb12c_home] - [コンフィグレーションおよび移行ツール] - [Database Configuration Assistant].
Oracle 11g	[スタート] - [すべてのプログラム] - [Oracle-OraDb11g_home] - [コンフィグレーションおよび移行ツール] - [Database Configuration Assistant].

- 2 [操作] ページで [データベースの作成] を選択します。
- 3 [データベース テンプレート] ページで、[汎用またはトランザクション処理] テンプレートを選択します。
- 4 [データベース識別情報] ページで、グローバル データベース名と Oracle システム識別子 (SID) のプレフィックスを入力します。

簡略化のため、どちらの項目にも同じ値を入力します。

- 5 [管理オプション] ページはデフォルト設定のまま [次へ] をクリックします。
- 6 [データベース資格証明] ページで、[すべてのアカウントに同じ管理パスワードを使用する] をオンにして、パスワードを入力します。
- 7 残りの構成ページはデフォルト設定のまま [次へ] をクリックします。
- 8 [作成オプション] ページで [データベースの作成] が選択されていることを確認し、[終了] をクリックします。
- 9 [確認] ページでオプションを確認し、[OK] をクリックします。

構成ツールによってデータベースが作成されます。

10 [データベース作成完了] ページで、[OK] をクリックします。

次のステップ

以下の説明に従います。[ODBC データ ソースを Oracle 12c または 11g に追加](#)

SQL ステートメントを使用して View Composer データベースを Oracle インスタンスに追加する

データベースの作成時に、データおよびログ ファイルの場所をカスタマイズできます。

前提条件

View Composer データベースは、特定のテーブルスペースや権限を持つ必要があります。SQL ステートメントを使用すると、Oracle 12c または 11g データベース インスタンス内に View Composer データベースを作成できます。

サポートされているバージョンの Oracle 12c または 11g がローカルまたはリモート コンピュータにインストールされていることを確認します。詳細については、[View Composer およびイベント データベースのデータベース要件](#)を参照してください。

手順

- 1 システム アカウントで SQL*Plus セッションにログインします。
- 2 次の SQL ステートメントを実行してデータベースを作成します。

```
CREATE SMALLFILE TABLESPACE "VCMP" DATAFILE '/u01/app/oracle/oradata/vcdb/vcmp01.dbf'
SIZE 512M AUTOEXTEND ON NEXT 10M MAXSIZE UNLIMITED LOGGING EXTENT MANAGEMENT LOCAL SEGMENT
SPACE MANAGEMENT AUTO;
```

この例では、VCMP が View Composer データベースのサンプル名、vcmp01.dbf がデータベース ファイルの名前です。

Windows インストールの場合は、Windows の規則に従って vcmp01.dbf ファイルへのディレクトリ パスを記述します。

次のステップ

特定のセキュリティ許可を使用して View Composer データベースを実行する場合は、「[View Composer 用に Oracle データベース ユーザーを構成する](#)」の手順に従います。

以下の説明に従います。[ODBC データ ソースを Oracle 12c または 11g に追加](#)

View Composer 用に Oracle データベース ユーザーを構成する

デフォルトでは、View Composer データベースを実行するデータベース ユーザーは Oracle システム管理者権限を持ちます。View Composer データベースを実行するユーザーのセキュリティ許可を制限するには、特定の権限を持つ Oracle データベース ユーザーを構成する必要があります。

前提条件

Oracle 12c または 11g インスタンス内に View Composer データベースが作成されていることを確認します。

手順

- 1 システム アカウントで SQL*Plus セッションにログインします。
- 2 次の SQL コマンドを実行することで、適切な権限を持つ View Composer データベース ユーザーを作成します。

```
CREATE USER "VCMPADMIN" PROFILE "DEFAULT" IDENTIFIED BY "oracle" DEFAULT TABLESPACE

"VCMP" ACCOUNT UNLOCK;
grant connect to VCMPADMIN;
grant resource to VCMPADMIN;
grant create view to VCMPADMIN;
grant create sequence to VCMPADMIN;
grant create table to VCMPADMIN;
grant create materialized view to VCMPADMIN;
grant execute on dbms_lock to VCMPADMIN;
grant execute on dbms_job to VCMPADMIN;
grant unlimited tablespace to VCMPADMIN;
```

この例では、ユーザー名は VCMPADMIN、View Composer データベース名は VCMP になっています。

resource ロールにはデフォルトで、create procedure、create table、および create sequence 権限が割り当てられます。resource ロールにこれらの権限が含まれていない場合は、それらを明示的に View Composer データベース ユーザーに付与してください。

ODBC データ ソースを Oracle 12c または 11g に追加

View Composer データベースを Oracle 12c または 11g のインスタンスに追加した後、新しいデータベースへの ODBC 接続を構成して、View Composer サービスがこのデータ ソースに接続できるようにする必要があります。

View Composer 用に ODBC DSN を構成する場合、基盤のデータベース接続を環境に適切なレベルに設定します。データベース接続の安全設定の詳細については、Oracle データベースのドキュメントを参照してください。

基盤のデータベース接続で SSL 暗号化を使用する場合、信頼される CA によって署名されている SSL 証明書と一緒にデータベース サーバを構成することをお勧めします。自己署名証明書を使用した場合、データベース接続は中間者攻撃を受けやすくなります。

前提条件

以下で説明した手順を実行したことを確認してください。[View Composer データベースを Oracle 12c または 11g に追加](#) または [SQL ステートメントを使用して View Composer データベースを Oracle インスタンスに追加する](#)。

手順

- 1 View Composer データベース コンピュータで、[スタート] - [管理ツール] - [データ ソース (ODBC)]を選択します。
- 2 [Microsoft ODBC データ ソース アドミニストレータ] ウィザードで、[システム DSN] タブを選択します。
- 3 [追加] をクリックし、リストから適切な Oracle ドライバを選択します。

例：OraDb11g_home

- 4 [終了] をクリックします。
- 5 [Oracle ODBC ドライバ構成] ダイアログ ボックスで、View Composer で使用する DSN、データ ソースの説明、およびデータベースに接続するユーザー ID を入力します。

特定のセキュリティ許可を持つ Oracle データベース ユーザー ID を構成した場合は、そのユーザー ID を指定します。

注： View Composer サービスをインストールするときは DSN を使用します。

- 6 ドロップダウン メニューからグローバル データベース名を選択して、[TNS サービス名] を指定します。

Oracle Database Configuration Assistant がグローバル データベース名を指定します。

- 7 データ ソースを確認するには、[接続テスト] をクリックし、[OK] をクリックします。

次のステップ

新しい View Composer サービスをインストールします。[View Composer サービスのインストール](#)を参照してください。

View Composer 向けに SSL 証明書を構成する

デフォルトでは、自己署名証明書は View Composer と一緒にインストールされます。デフォルトの証明書はテストを目的として使用できますが、本稼動用に、証明機関（CA）によって署名された証明書に置き換える必要があります。

証明書の構成は、View Composer をインストールする前にもインストールした後にもできます。View 5.1 以降のリリースでは、View Composer がインストールされている、またはインストールする予定の Windows Server コンピュータ上の Windows ローカル コンピュータ証明書ストアに証明書をインポートすることで、証明書を構成します。

- View Composer をインストールする前に CA が署名した証明書をインポートする場合、View Composer のインストール中に署名された証明書を選択できます。この手法により、インストール後にデフォルトの証明書を手作業で置き換える作業が不要になります。
- View Composer をインストールした後で既存の証明書またはデフォルトの自己署名証明書を新しい証明書に置き換える予定にしている場合、新しい証明書をインポートして SviConfig ReplaceCertificate ユーティリティを実行し、新しい証明書を View Composer によって使用されるポートにバインドする必要があります。

SSL 証明書の構成と SviConfig ReplaceCertificate ユーティリティの使用の詳細については、[8 章 Horizon 7 Server 用の TLS 証明書の設定](#)を参照してください。

vCenter Server と View Composer を同じ Windows Server コンピュータにインストールしている場合、これらは同じ SSL 証明書を使用できますが、証明書はそれぞれのコンポーネントについて個別に構成する必要があります。

View Composer サービスのインストール

View Composer を使用するには、View Composer サービスをインストールする必要があります。Horizon 7 は、View Composer を使用してリンク クローン デスクトップを作成し、vCenter Server に展開します。

vCenter Server がインストールされている Windows Server コンピュータまたは別個の Windows Server コンピュータに、View Composer サービスをインストールできます。スタンドアロン View Composer インストールは、Windows Server コンピュータにインストールされた vCenter Server および Linux ベースの vCenter Server Appliance と連携します。

View Composer ソフトウェアは、レプリカ サーバ、セキュリティ サーバ、接続サーバ、Horizon Agent、Horizon Client などの他の Horizon 7 ソフトウェア コンポーネントがインストールされている仮想マシンまたは物理マシンにインストールできません。

セキュリティを強化するため、既知の脆弱性を除去するよう暗号化スイートを構成することをお勧めします。View Composer または Horizon Agent を実行する Windows マシン向けに暗号化スイートのドメイン ポリシーをセットアップする手順については、[SSL/TLS における強度の弱い暗号化方式の無効化](#)を参照してください。

前提条件

- [View Composer の要件](#)で説明されている View Composer のインストール要件を満たしていることを確認します。
- 接続サーバ、セキュリティ サーバ、Horizon Agent、または Horizon Client など他の Horizon 7 コンポーネントが、View Composer をインストールしようとしているマシンにインストールされていないことを確認します。
- View Composer をインストールして使用するためのライセンスがあることを確認します。
- Microsoft ODBC データ ソース アドミニストレータ ウィザードで指定した DSN、ドメイン管理者のユーザー名、およびパスワードがわかるようにしておきます。View Composer サービスをインストールするときにこの情報を入力します。
- インストール中に、CA によって署名された SSL 証明書を View Composer 用に構成する場合、証明書が Windows ローカル コンピュータの証明書ストアにインポートされていることを確認します。[8 章 Horizon 7 Server 用の TLS 証明書の設定](#)を参照してください。
- View Composer コンピュータで実行されているアプリケーションが、Microsoft Secure Channel (Schannel) セキュリティ パッケージで実装される SSL バージョン 2 (SSLv2) を要求する Windows SSL ライブラリを使用していないことを確認します。View Composer インストーラにより、Microsoft Schannel 上の SSLv2 が無効になります。Java SSL を使用する Tomcat や OpenSSL を使用する Apache などのアプリケーションは、この制限による影響を受けません。
- View Composer インストーラを実行するには、そのシステムでの管理者権限を持つユーザーである必要があります。

手順

- 1 View Composer のインストーラ ファイルを VMware 製品ページ (<http://www.vmware.com/products/>) から Windows Server コンピュータにダウンロードします。

インストーラのファイル名は VMware-viewcomposer-y.y.y-xxxxxx.exe です。xxxxxx はビルド番号、y.y.y はバージョン番号です。このインストーラ ファイルは、View Composer サービスを 64 ビットの Windows Server オペレーティング システムにインストールします。

- 2 View Composer のインストール プログラムを開始するには、インストーラ ファイルを右クリックし、[管理者として実行] を選択します。

- 3 VMware のライセンス条件に同意します。
- 4 インストール先フォルダを受け入れるか、変更します。
- 5 Microsoft または Oracle の [Microsoft ODBC Data Source Administrator (Microsoft ODBC データ ソース アドミニストレータ)] ウィザードで指定した View Composer データベースの DSN を入力します。

例：VMware View Composer

注： View Composer データベースの DSN を構成しなかった場合は、[ODBC DSN のセットアップ] をクリックして、ここで名前を構成します。

- 6 [Microsoft ODBC データ ソース アドミニストレータ] ウィザードで指定したドメイン管理者のユーザー名とパスワードを入力します。

特定のセキュリティ権限がある Oracle データベース ユーザーを構成した場合は、このユーザー名を指定します。

- 7 ポート番号を入力するか、またはデフォルト値をそのまま使用します。

View 接続サーバは、このポートを使用して View Composer サービスと通信します。

- 8 SSL 証明書を指定します。

オプション	アクション
Create default SSL certificate (デフォルト SSL 証明書の作成)	View Composer サービス用にデフォルトの SSL 証明書を作成するには、このラジオ ボタンを選択します。 インストール後、デフォルトの証明書を CA により署名された SSL 証明書に置換できます。
既存の SSL 証明書を使用	View Composer サービスで使用する署名付き SSL 証明書をインストール済みの場合は、このラジオ ボタンを選択します。リストから SSL 証明書を選択します。

- 9 [インストール] をクリックし、[終了] をクリックして、View Composer サービスのインストールを完了します。

結果

VMware Horizon View Composer サービスが開始されます。

View Composer は、Windows Server オペレーティング システムによって提供される暗号化スイートを使用します。Windows Server システムで暗号化スイートを管理するには、組織のガイドラインに従う必要があります。所属する組織にガイドラインがない場合、VMware では、View Composer Server の強度の低い暗号化スイートを無効にして Horizon 7 環境のセキュリティを強化することを推奨しています。暗号化スイートの管理の詳細については、Microsoft のドキュメントを参照してください。

次のステップ

古いバージョンの vCenter Server がある場合、[View Composer から vCenter および ESXi 接続で TLSv1.0 を有効にする](#)を参照してください。

SQL Server データベース権限を手動で設定しそれらをユーザーに割り当てている場合、そのユーザーからデータベース管理者ロールを取り消すことができます。詳しくは、[データベース ロールの手動作成による SQL Server データベース権限の設定](#) に示されている手続きの最後の手順を参照してください。

View Composer から vCenter および ESXi 接続で TLSv1.0 を有効にする

Horizon 7 以降のコンポーネントでは、TLSv1.0 セキュリティ プロトコルがデフォルトで無効になっています。TLSv1.0 のみをサポートする古いバージョンの vCenter Server が展開環境に含まれている場合、View Composer 7.0 以降のリリースのインストールまたはアップグレード後に、View Composer 接続に対して TLSv1.0 を有効にすることが必要な可能性があります。

vCenter Server 5.0、5.1、および 5.5 の一部の旧メンテナンス リリースは、Horizon 7 以降のリリースではデフォルトで無効になっている TLSv1.0 のみをサポートします。vCenter Server を TLSv1.1 または TLSv1.2 をサポートするバージョンにアップグレードできない場合は、View Composer 接続に対して TLSv1.0 を有効にできます。

ESXi ホストで ESXi 6.0 U1b より前のバージョンが実行されていてアップグレードできない場合は、View Composer から ESXi ホストで TLSv1.0 接続を有効にすることが必要な可能性もあります。

前提条件

- View Composer 7.0 以降のリリースがインストールされていることを確認します。
- View Composer マシンに管理者としてログインして Windows レジストリ エディタを使用できることを確認します。

手順

- 1 View Composer をホストするマシンで、Windows レジストリ エディタ (regedit.exe) を開きます。
- 2 HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client に移動します。
このキーが存在しない場合は作成します。
- 3 値 [Enabled] が存在する場合は削除します。
- 4 [DWORD] 値 [DisabledByDefault] を編集して [0] に設定します。
- 5 VMware Horizon View Composer サービスを再起動します。
これで、View Composer から vCenter への TLSv1.0 接続が有効になりました。
- 6 View Composer マシンの Windows レジストリで、HKLM\SOFTWARE\VMware, Inc.\VMware View Composer に移動します。
- 7 文字列の値 [EnableTLS1.0] を作成または編集して [1] に設定します。
- 8 View Composer ホストが 64 ビット マシンの場合は、HKLM\SOFTWARE\WOW6432Node\VMware, Inc.\VMware View Composer に移動します。
- 9 文字列の値 [EnableTLS1.0] を作成または編集して [1] に設定します。
- 10 VMware Horizon View Composer サービスを再起動します。
これで、View Composer から ESXi ホストへの TLSv1.0 接続が有効になりました。

View Composer 用のインフラストラクチャの構成

vSphere、vCenter Server、Active Directory、およびインフラストラクチャの他のコンポーネントの機能を利用して、View Composer のパフォーマンス、可用性、信頼性を最適化できます。

View Composer 用の vSphere 環境の構成

View Composer をサポートするには、vCenter Server、ESXi、およびその他の vSphere コンポーネントをインストールして構成するときに、特定のベスト プラクティスに従う必要があります。

以下のベスト プラクティスに従うと、View Composer は vSphere 環境で効率よく動作します。

- リンク クローン仮想マシンのパスとフォルダの情報を作成した後は、vCenter Server でその情報を変更しないでください。フォルダの情報を変更するには、代わりに Horizon Administrator を使用します。

この情報を vCenter Server で変更すると、Horizon 7 は vCenter Server で仮想マシンを検索できません。

- ESXi ホストでの vSwitch 設定では、ESXi ホスト上で動作するリンク クローン仮想マシンで構成される仮想 NIC の合計をサポートするのに十分なポート数を構成するようにします。
- リンク クローン デスクトップをリソース プールで展開する場合は、必要な数のデスクトップをホストするのに十分な CPU とメモリが vSphere 環境にあることを確認してください。リソース プールでの CPU とメモリの使用状況を監視するには、vSphere Client を使用します。
- vSphere 5.1 以降では、View Composer のリンク クローンで使用されるクラスタは、レプリカ ディスクが VMFS5 以降のデータストアまたは NFS データストアに格納されている場合、8 を超える ESXi ホストを含むことができます。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。
- vSphere DRS を使用してください。DRS は、リンク クローン仮想マシンをホスト間に効果的に分散させます。

注： Storage vMotion はリンク クローン デスクトップに対してはサポートされません。

View Composer に関する他のベスト プラクティス

View Composer を効率よく動作させるには、動的ネーム サービス（DNS）が正常に動作していることを確認し、時間をずらしてウイルス対策ソフトウェアのスキャンを実行します。

DNS 解決が正しく動作するようにすることで、DNS エラーによる断続的な問題を防ぐことができます。View Composer サービスは動的な名前解決に依存して他のコンピュータと通信します。DNS の動作をテストするには、Active Directory と View 接続サーバコンピュータに名前を ping を実行します。

ウイルス対策ソフトウェアの実行時間をずらせば、リンク クローン デスクトップのパフォーマンスは影響を受けません。すべてのリンク クローンでウイルス対策ソフトウェアが同時に実行した場合は、ストレージ サブシステムで発生する 1 秒あたりの I/O 操作（IOPS）が過剰になります。この過剰な活動は、リンク クローン デスクトップのパフォーマンスに影響する場合があります。

Horizon 接続サーバのインストール

7

接続サーバを使用するには、サポートされるコンピュータにソフトウェアをインストールし、必要なコンポーネントを構成し、必要に応じてコンポーネントを最適化します。

この章には、次のトピックが含まれています。

- [Horizon 接続サーバ ソフトウェアのインストール](#)
- [Horizon 接続サーバのインストールの前提条件](#)
- [新しい構成での Horizon 接続サーバのインストール](#)
- [Horizon 接続サーバの複製インスタンスのインストール](#)
- [セキュリティ サーバのペアリング パスワードを構成する](#)
- [セキュリティ サーバをインストールする](#)
- [VPN 経由で Unified Access Gateway アプライアンスを使用する利点](#)
- [Horizon 接続サーバのファイアウォール ルール](#)
- [Horizon 接続サーバをバックアップ構成で再インストールする](#)
- [Microsoft Windows インストーラ コマンド ライン オプション](#)
- [MSI のコマンドライン オプションを使用した Horizon 7 コンポーネントのサイレント アンインストール](#)

Horizon 接続サーバ ソフトウェアのインストール

Horizon 7 のデプロイでのパフォーマンス、可用性、およびセキュリティのニーズに応じて、接続サーバの単一インスタンス、接続サーバの複製されたインスタンス、およびセキュリティ サーバをインストールできます。接続サーバのインスタンスを少なくとも 1 つはインストールする必要があります。

接続サーバをインストールするときは、インストールの種類を選択します。

標準インストール	接続サーバのインスタンスが、新しい View LDAP の構成で生成されます。
レプリカ インストール	接続サーバのインスタンスが、既存のインスタンスからコピーされた View LDAP の構成で生成されます。

セキュリティ サーバ インストール	インターネットと内部ネットワークの間に新しいセキュリティ レイヤーを追加する接続サーバのインスタンスが生成されます。
登録サーバ インストール	ユーザーが VMware Identity Manager ログインした後に、Active Directory 認証情報を入力することなくリモート デスクトップまたはアプリケーションに接続できるように、True SSO (シングル サインオン) 機能に必要な登録サーバをインストールします。登録サーバには、認証に使用する一時的な証明書が必要です。

注： この機能を使用するには、認証局を設定して、特定の構成を実行する必要もあるため、登録サーバのインストール手順は、このインストール ドキュメントではなく、『Horizon 7 の管理』ドキュメントの「認証情報を必要としないユーザー認証」の章に記載されています。

Horizon 接続サーバのインストールの前提条件

接続サーバをインストールする前に、インストール環境が特定の前提条件を満たしていることを確認する必要があります。

- Horizon 7 の有効なライセンス キーが必要です。
- 各接続サーバホストは、Active Directory ドメインに参加させる必要があります。接続サーバは、次の Active Directory Domain Services (AD DS) のドメイン機能レベルをサポートします。
 - Windows Server 2008
 - Windows Server 2008 R2
 - Windows Server 2012
 - Windows Server 2012 R2
 - Windows Server 2016

接続サーバ ホストをドメイン コントローラにすることはできません。

注： 接続サーバでは、Active Directory のスキーマまたは構成の更新を行うことも、それを必要とするものではありません。

- Windows Terminal Server の役割がインストールされているシステムには、接続サーバをインストールしないでください。接続サーバをインストールするシステムからは、Windows Terminal Server の役割を削除する必要があります。
- 他の機能または役割を実行するシステムには、接続サーバをインストールしないでください。たとえば、同じシステムを使用して vCenter Server をホストしないでください。
- 接続サーバをインストールするシステムには、変更しない IP アドレスが含まれる必要があります。IPv4 環境では、固定 IP アドレスを構成します。IPv6 環境では、変更されない IP アドレスがマシンによって自動的に取得されます。
- Horizon 接続サーバ インストーラを実行するには、そのシステムでの管理者権限を持つドメイン ユーザー アカウントを使用する必要があります。

- 接続サーバをインストールする場合は、管理者アカウントを許可します。ローカル Administrators グループ、またはドメイン ユーザー/グループのアカウントを指定できます。Horizon 7 ではこのアカウントのみに、複製された接続サーバ インスタンスをインストールする権限を含むすべての管理権限を割り当てます。ドメインのユーザーまたはグループを指定する場合は、インストーラを実行する前に、Active Directory でアカウントを作成する必要があります。

新しい構成での Horizon 接続サーバのインストール

接続サーバを単独のサーバとして、または複製された接続サーバ インスタンスのグループの最初のインスタンスとしてインストールするには、標準インストール オプションを使用します。

標準インストール オプションを選択すると、新しいローカルの View LDAP 構成が作成されます。インストールでは、スキーマ定義、ディレクトリ情報ツリー (DIT) の定義、および ACL がロードされて、データが初期化されます。

インストールの後には、Horizon Administrator を使用してほとんどの View LDAP 構成データを管理できます。接続サーバは、一部の View LDAP エントリを自動的に維持します。

接続サーバ ソフトウェアは、レプリカ サーバ、セキュリティ サーバ、View Composer、Horizon Agent、Horizon Client などを含むその他の Horizon 7 ソフトウェア コンポーネントがインストールされている仮想マシンまたは物理マシンにインストールできません。

接続サーバを新しい構成でインストールする場合は、カスタム エクスペリエンス改善プログラムに参加できます。VMware は、ユーザー要件に対する対応を向上させるために、お客様の展開に関する匿名データを収集します。企業が特定できるような情報は収集されません。インストール中にこのオプションの選択を解除すると、不参加を選択できます。インストール後に参加に関する考えが変わったら、Horizon Administrator の [製品のライセンスと使用状況] ページを編集して、プログラムに参加したり参加を取り消したりすることができます。匿名のフィールドを含め、データが収集されるフィールドのリストを確認するには、『Horizon 7 の管理』の「カスタム エクスペリエンス改善プログラムによって収集される情報」を参照してください。

デフォルトでは、接続サーバをインストールするときに、HTML Access コンポーネントが接続サーバのホストにインストールされます。このコンポーネントは、Horizon 7 ユーザー ポータル ページを構成し、Horizon Client アイコンに加えて HTML Access アイコンを表示します。ユーザーがデスクトップに接続するときに、この追加のアイコンを使用して HTML Access を選択することができます。

HTML Access の接続サーバの設定については、Horizon Client のドキュメント ページにある『VMware Horizon HTML Access のインストールとセットアップ ガイド』ドキュメントを参照してください。

前提条件

- 接続サーバをインストールする Windows Server コンピュータに、管理者権限のあるドメイン ユーザーとしてログインできることを確認します。
- [Horizon 接続サーバの要件](#)で説明されている要件をインストールが満たしていることを確認します。
- 環境をインストール用に準備します。[Horizon 接続サーバのインストールの前提条件](#)を参照してください。
- ドメインのユーザーまたはグループを管理者アカウントとして許可する場合は、ドメイン アカウントを Active Directory で作成したことを確認します。

- データ リカバリ パスワードを作成します。接続サーバをバックアップすると、View LDAP 構成が暗号化された LDIF データとしてエクスポートされます。暗号化されたバックアップ Horizon 7 構成を復元するには、データ リカバリ パスワードを入力する必要があります。パスワードは 1 文字から 128 文字の間にする必要があります。安全なパスワードの生成に関する組織のベスト プラクティスに従ってください。

重要： ビジネス継続性とディザスタ リカバリ (BCDR) シナリオで Horizon 7 の操作を継続しダウンタイムを回避するには、データ リカバリ パスワードが必要です。接続サーバをインストールするときに、パスワードにパスワード リマイダを指定することができます。

- Windows ファイアウォールで接続サーバ インスタンス用に開く必要があるネットワーク ポートについて理解します。[Horizon 接続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 サーバをこの接続サーバ インスタンスとペアにする場合、[セキュリティが強化された Windows ファイアウォール] がアクティブなプロファイルで [オン] に設定されていることを確認します。この設定はすべてのプロファイルで [オン] にすることを推奨します。デフォルトでは、IPsec ルールはセキュリティ サーバと接続サーバ間の接続を制御し、[セキュリティが強化された Windows ファイアウォール] を有効にする必要があります。
- ネットワーク トポロジにセキュリティ サーバと接続サーバ インスタンス間のバックエンドのファイアウォールが含まれている場合、IPsec をサポートするようにファイアウォールを構成する必要があります。[バックエンド ファイアウォールを構成して IPsec をサポートする](#)を参照してください。

手順

- 1 VMware ダウンロード ページ (<https://my.vmware.com/web/vmware/downloads>) から、接続サーバ インストーラ ファイルをダウンロードします。

[Desktop & End-User Computing (デスクトップおよびエンドユーザー コンピューティング)] で VMware Horizon 7 のダウンロードを選択します。これには接続サーバ ファイルが含まれます。

インストーラのファイル名は、VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe です。xxxxxx は、ビルド番号であり、y.y.y はバージョン番号です。

- 2 接続サーバのインストール プログラムを開始するには、インストーラ ファイルをダブルクリックします。

- 3 VMware のライセンス条件に同意します。

- 4 インストール先フォルダを受け入れるか、変更します。

- 5 [View スタンダード サーバ] インストール オプションを選択します。

- 6 インターネット プロトコル (IP) バージョンとして、[IPv4] または [IPv6] を選択します。

すべての Horizon 7 コンポーネントを同じ IP バージョンでインストールする必要があります。

- 7 FIPS モードを有効にするか無効にするかを選択します。

このオプションは、Windows で FIPS モードが有効になっている場合にのみ使用可能です。

- 8 ユーザーが Web ブラウザを使用して自分自身のデスクトップに接続できるようにする場合は、[HTML Access のインストール] を選択します。

[IPv4] が選択されると、この設定がデフォルトで選択されます。[IPv6] が選択されると、HTML Access は IPv6 環境でサポートされていないため、この設定は表示されません。

9 データ リカバリ パスワードを入力し、オプションでパスワード リマインダを入力します。

10 Windows ファイアウォール サービスを構成する方法を選択します。

オプション	アクション
Configure Windows Firewall automatically (Windows ファイアウォールを自動的に構成する)	インストーラで、必要なネットワーク接続を許可するように Windows ファイアウォールを構成します。
Do not configure Windows Firewall (Windows ファイアウォールを構成しない)	Windows ファイアウォール ルールを手動で構成します。 このオプションを選択するのは、組織が Windows ファイアウォールを構成するために独自の事前定義ルールを使用している場合のみです。

11 Horizon Administrator アカウントを許可します。

このアカウントのメンバーだけが、Horizon Administrator へのログイン、全管理権限の行使、複製された接続 サーバ インスタンスおよびその他の Horizon 7 サーバのインストールを行えます。

オプション	説明
ローカル Administrators グループを許可する	ローカル Administrators グループのユーザーが Horizon 7 を管理できるようにします。
特定のドメイン ユーザーまたはドメイン グループを許可する	指定したドメインのユーザーまたはグループが Horizon 7 を管理できるようにします。

12 ドメイン Horizon Administrator アカウントを指定したときに、ドメイン アカウントにアクセスできないローカル管理者や別のユーザーとしてインストーラを実行する場合は、承認されたユーザー名とパスワードでドメインにログインするための認証情報を提示します。

domain name\user name またはユーザー プリンシパル名 (UPN) 形式を使用します。UPN 形式は、*user@domain.com* となります。

13 カスタマー エクスペリエンス向上プログラムに参加するかどうかを選択します。

参加する場合は、組織の業種、規模、所在地を任意で選択できます。

14 インストール ウィザードに従って、接続サーバのインストールを終了します。

15 Windows Server コンピュータで新しいパッチをチェックし、必要に応じて Windows Update を実行します。

接続サーバをインストールする前に Windows Server コンピュータのパッチを完全に適用していたとしても、インストールによりオペレーティング システム機能が初めて有効になる場合があります。この場合、追加のパッチが必要になる場合があります。

結果

次の Horizon 7 サービスが Windows Server コンピュータにインストールされます。

- VMware Horizon 接続サーバ
- VMware Horizon View Framework コンポーネント
- VMware Horizon View Message Bus コンポーネント
- VMware Horizon View スクリプト ホスト

- VMware Horizon View Security Gateway コンポーネント
- VMware Horizon View PCoIP Secure Gateway
- VMware Horizon View Blast Secure Gateway
- VMware Horizon View Web コンポーネント
- VMware VDMDS (View LDAP ディレクトリ サービスを提供します)

これらのサービスについては、『Horizon 7 の管理』ドキュメントを参照してください。

インストール時に [HTML Access のインストール] 設定を選択した場合、HTML Access コンポーネントが Windows Server コンピュータにインストールされています。このコンポーネントにより、Horizon 7 ユーザー ポータル ページの HTML Access アイコンが構成され、Windows ファイアウォールでの [VMware Horizon View 接続サーバ (Blast-In)] ルールが有効になります。このファイアウォール ルールにより、クライアント デバイス上の Web ブラウザは、TCP ポート 8443 で接続サーバに接続できるようになります。

次のステップ

接続サーバ用の SSL サーバ証明書を構成します。8 章 [Horizon 7 Server 用の TLS 証明書の設定](#)を参照してください。

古いバージョンの vCenter Server がある場合、[接続サーバから vCenter 接続で TLSv1.0 を有効にする](#)を参照してください。

接続サーバの初期構成を行います。9 章 [Horizon 7 の初回構成](#)を参照してください。

展開に複製された接続サーバ インスタンスおよびセキュリティ サーバを含める場合は、接続サーバ インストーラ ファイルを実行して各サーバ インスタンスをインストールする必要があります。

接続サーバを再インストールしていて、パフォーマンス データを監視するようにデータ コレクタ セットを構成してある場合は、データ コレクタ セットを停止して再起動してください。

Horizon 接続サーバのサイレント インストール

Microsoft Windows インストーラ (MSI) のサイレント インストール機能を使用して、複数の Windows コンピュータで接続サーバの標準インストールを実行できます。サイレント インストールはコマンド ラインを使用して行い、ウィザードのプロンプトに対応する必要はありません。

サイレント インストールを使うと、大規模なエンタープライズに Horizon 7 のコンポーネントを効率よく展開できます。

前提条件

- 接続サーバをインストールする Windows Server コンピュータに、管理者権限のあるドメイン ユーザーとしてログインできることを確認します。
- [Horizon 接続サーバの要件](#)で説明されている要件をインストールが満たしていることを確認します。
- 環境をインストール用に準備します。[Horizon 接続サーバのインストールの前提条件](#)を参照してください。
- ドメインのユーザーまたはグループを Horizon Administrator アカウントとして許可する場合は、ドメイン アカウントを Active Directory で作成したことを確認します。

- MIT Kerberos 認証を使用して Connection Server をインストールする Windows Server 2008 R2 コンピュータにログインする場合、<http://support.microsoft.com/kb/978116> の KB 978116 に解説されている Microsoft ホットフィックスをインストールしてください。
- Windows ファイアウォールで接続サーバ インスタンス用に開く必要があるネットワーク ポートについて理解します。[Horizon 接続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 サーバをこの接続サーバ インスタンスとペアにする場合、[セキュリティが強化された Windows ファイアウォール] がアクティブなプロファイルで [オン] に設定されていることを確認します。この設定はすべてのプロファイルで [オン] にすることを推奨します。デフォルトでは、IPsec ルールはセキュリティ サーバと接続サーバ間の接続を制御し、[セキュリティが強化された Windows ファイアウォール] を有効にする必要があります。
- ネットワーク トポロジにセキュリティ サーバと接続サーバ インスタンス間のバックエンドのファイアウォールが含まれている場合、IPsec をサポートするようにファイアウォールを構成する必要があります。[バックエンド ファイアウォールを構成して IPsec をサポートする](#)を参照してください。
- 接続サーバをインストールする Windows コンピュータにバージョン 2.0 以降の MSI ランタイム エンジンがあることを確認します。詳細については、マイクロソフトの Web サイトを参照してください。
- MSI インストーラのコマンドライン オプションについて理解しておきます。[Microsoft Windows インストーラ コマンドライン オプション](#)を参照してください。
- 接続サーバの標準インストールで利用できるサイレント インストール プロパティについて理解しておきます。[Horizon Connection Server の標準インストールのサイレント インストールのプロパティ](#)を参照してください。

手順

- 1 VMware ダウンロード ページ (<https://my.vmware.com/web/vmware/downloads>) から、接続サーバ インストーラ ファイルをダウンロードします。

[Desktop & End-User Computing (デスクトップおよびエンドユーザー コンピューティング)] で VMware Horizon 7 のダウンロードを選択します。これには接続サーバ ファイルが含まれます。

インストーラのファイル名は、VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe です。xxxxxx は、ビルド番号であり、y.y.y はバージョン番号です。

- 2 Windows Server コンピュータでコマンド プロンプトを開きます。
- 3 インストール コマンドを 1 行で入力します。

```
例: VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=1
VDM_INITIAL_ADMIN_SID=S-1-5-32-544 VDM_SERVER_RECOVERY_PWD=mini
VDM_SERVER_RECOVERY_PWD_REMINDER=""First car"""
```

重要: サイレント インストールを実行する場合、データ リカバリ パスワードを含むフル コマンドラインがインストーラの vminst.log ファイルに記録されます。インストールが完了したら、このログ ファイルを削除するか、Horizon Administrator を使用してデータ リカバリ パスワードを変更します。

- 4 Windows Server コンピュータで新しいパッチをチェックし、必要に応じて Windows Update を実行します。

接続サーバをインストールする前に Windows Server コンピュータのパッチを完全に適用していたとしても、インストールによりオペレーティング システム機能が初めて有効になる場合があります。この場合、追加のパッチが必要になる場合があります。

結果

次の Horizon 7 サービスが Windows Server コンピュータにインストールされます。

- VMware Horizon 接続サーバ
- VMware Horizon View Framework コンポーネント
- VMware Horizon View Message Bus コンポーネント
- VMware Horizon View スクリプト ホスト
- VMware Horizon View Security Gateway コンポーネント
- VMware Horizon View PCoIP Secure Gateway
- VMware Horizon View Blast Secure Gateway
- VMware Horizon View Web コンポーネント
- VMware VDMDS (View LDAP ディレクトリ サービスを提供します)

インストール時に [HTML Access のインストール] 設定を選択した場合、HTML Access コンポーネントが Windows Server コンピュータにインストールされています。このコンポーネントにより、Horizon 7 ユーザー ポータル ページの HTML Access アイコンが構成され、Windows ファイアウォールでの [VMware Horizon View 接続サーバ (Blast-In)] ルールが有効になります。このファイアウォール ルールにより、クライアント デバイス上の Web ブラウザは、TCP ポート 8443 で接続サーバに接続できるようになります。

これらのサービスについては、『Horizon 7 の管理』ドキュメントを参照してください。

次のステップ

接続サーバ用の SSL サーバ証明書を構成します。8 章 [Horizon 7 Server 用の TLS 証明書の設定](#)を参照してください。

古いバージョンの vCenter Server がある場合、[接続サーバから vCenter 接続で TLSv1.0 を有効にする](#)を参照してください。

Horizon 7 を初めて構成する場合は、接続サーバの初期構成を行います。9 章 [Horizon 7 の初回構成](#)を参照してください。

Horizon Connection Server の標準インストールのサイレント インストールのプロパティ

コマンド ラインから Connection Server をサイレント インストールまたはアップグレードするときに、特定のプロパティを含めることができます。Microsoft Windows Installer (MSI) がプロパティと値を解釈できるように、*PROPERTY=value* 形式を使用する必要があります。サイレント アップグレードでは同じインストール コマンドが使用されます。

表 7-1. 標準インストールで Connection Server をサイレント インストールするための MSI のプロパティ

MSI プロパティ	説明	デフォルト値
INSTALLDIR	Connection Server ソフトウェアをインストールするパスとフォルダ。 例: INSTALLDIR=""D:\abc\my folder"" パスを囲む二重引用符によって MSI インストーラにパスの有効部分としてスペースを解釈することを許可します。	%ProgramFiles%\VMware\VMware View\Server
VDM_SERVER_INSTANCE_TYPE	Horizon Server のインストールの種類: ■ 1. 標準インストール ■ 2. レプリカ インストール ■ 3. セキュリティ サーバ インストール ■ 5. 登録サーバ インストール たとえば、標準インストールを実行するには、VDM_SERVER_INSTANCE_TYPE=1 と指定します。	1
FWCHOICE	Connection Server のインスタンスに対してファイアウォールを構成するかどうかを指定する MSI プロパティ。 値 1 はファイアウォールを構成します。値 2 はファイアウォールを構成しません。 例: FWCHOICE=1	1
VDM_INITIAL_ADMIN_SID	Horizon において全管理権限が許可されている最初の Horizon Administrator ユーザーまたはグループの SID。 デフォルト値は、Connection Server コンピュータ上のローカル Administrators グループの SID です。ドメイン ユーザー/グループ アカウントの SID を指定できます。	S-1-5-32-544
VDM_SERVER_RECOVERY_PWD	データ リカバリ パスワード。データ リカバリ パスワードが Horizon LDAP に設定されていない場合、このプロパティは必須です。 パスワードは 1 文字から 128 文字の間にする必要があります。安全なパスワードの生成に関する組織のベスト プラクティスに従ってください。	なし
VDM_SERVER_RECOVERY_PWD_REMINDER	データ リカバリ パスワードのリマインダ。このプロパティは省略可能です。	なし
VDM_IP_PROTOCOL_USAGE	Horizon コンポーネントが通信で使用する IP アドレスのバージョンを指定します。使用可能な値は IPv4 および IPv6 です。	IPv4
VDM_FIPS_ENABLED	FIPS モードを有効にするか無効にするかを指定します。値 1 は FIPS モードを有効にします。値 0 は FIPS モードを無効にします。このプロパティが 1 に設定され、Windows が FIPS モードになっていない場合、インストーラは中断されます。	0
HTMLACCESS	HTML Access アドオンのインストールを制御します。HTML Access を構成するには、このプロパティを 1 に設定します。HTML Access を必要としない場合は、プロパティを省きます。	1

接続サーバから vCenter 接続で TLSv1.0 を有効にする

Horizon 7 以降のコンポーネントでは、TLSv1.0 セキュリティ プロトコルがデフォルトで無効になっています。TLSv1.0 のみをサポートする古いバージョンの vCenter Server が展開環境に含まれている場合、接続サーバ 7.0 以降のリリースのインストールまたはアップグレード後に、接続サーバへの接続に対して TLSv1.0 を有効にすることが必要な可能性があります。

vCenter Server 5.1 および 5.5 の一部の旧メンテナンス リリースは、Horizon 7 以降のリリースではデフォルトで無効になっている TLSv1.0 のみをサポートします。vCenter Server を TLSv1.1 または TLSv1.2 をサポートするバージョンにアップグレードできない場合は、接続サーバへの接続に対して TLSv1.0 を有効にできます。

前提条件

- Horizon 7 にアップグレードする場合は、アップグレード前にこの手順を実行して、サービスの再起動回数を最小限に抑えます。接続サーバのアップグレード中にサービスが再起動され、この手順で説明されている構成の変更を適用するときに再起動が必要になります。この手順を実行する前にアップグレードを行うと、サービスをもう一度再起動する必要があります。
- お使いのバージョンの Windows オペレーティング システムでの ADSI Edit ユーティリティの使用方法については、Microsoft TechNet Web サイトを参照してください。

手順

- 1 接続サーバ ホスト上で ADSI Edit ユーティリティを起動します。
- 2 コンソール ツリーで、[接続] を選択します。
- 3 [識別名または命名規則を選択または入力] テキスト ボックスに、識別名「**DC=vdi, DC=vmware, DC=int**」を入力します。
- 4 [コンピュータ] ペインで、**localhost:389** を選択または入力するか、接続サーバ ホストの完全修飾ドメイン名 (FQDN) を入力し、続いてポート 389 を入力します。

例：**localhost:389** または **mycomputer.example.com:389**
- 5 [ADSI Edit] ツリーを展開し、[OU=Properties] を展開して [OU=Global] を選択し、右ペインで [CN=Common] をダブルクリックします。
- 6 [プロパティ] ダイアログ ボックスで、[pae-ClientSSLSecureProtocols] 属性を編集して次の値を追加します。

\LIST:TLSv1.2,TLSv1.1,TLSv1

必ず行の先頭にバック スラッシュを含めてください。
- 7 [OK] をクリックします。
- 8 新規インストールの場合に構成の変更を適用するには、各接続サーバ インスタンスで接続サーバ サービスを再起動します。

アップグレードを実行する場合は、アップグレードのプロセスによって自動的にサービスが再起動されるため、サービスを再起動する必要はありません。

Horizon 接続サーバの複製インスタンスのインストール

高可用性とロード バランシングを実現するため、既存の接続サーバ インスタンスを複製した接続サーバの追加インスタンスを 1 つ以上インストールできます。レプリカ インストールの後、接続サーバの既存インスタンスと新しくインストールしたインスタンスに違いはありません。

複製されたインスタンスをインストールするときは、Horizon 7 が既存の接続サーバ インスタンスから View LDAP 構成データをコピーします。

インストールの後、複製されたグループのすべての接続サーバ インスタンスで、同一の View LDAP 構成データが維持されます。1 つのインスタンスで構成が変更されると、更新された情報が他のインスタンスにコピーされます。

複製されたインスタンスで障害が発生した場合は、グループ内の他のインスタンスが動作を続行します。障害が発生したインスタンスが活動を再開した場合、停止中に発生した変更で構成が更新されます。

注： レプリケーション機能は、Active Directory と同じレプリケーション テクノロジを使用する View LDAP によって提供されます。

レプリカ サーバ ソフトウェアは、セキュリティ サーバ、接続サーバ、View Composer、Horizon Agent、または Horizon Client を含む他の Horizon 7 ソフトウェア コンポーネントと同じ仮想マシンまたは物理マシンにインストールすることができません。

デフォルトでは、接続サーバをインストールするときに、HTML Access コンポーネントが接続サーバのホストにインストールされます。このコンポーネントは、Horizon 7 ユーザー ポータル ページを構成し、Horizon Client アイコンに加えて HTML Access アイコンを表示します。ユーザーがデスクトップに接続するときに、この追加のアイコンを使用して HTML Access を選択することができます。

HTML Access の接続サーバの設定については、Horizon Client のドキュメント ページにある『VMware Horizon HTML Access のインストールとセットアップ ガイド』ドキュメントを参照してください。

前提条件

- ネットワークに少なくとも 1 つの接続サーバ インスタンスがインストールおよび構成されていることを確認します。
- 複製されたインスタンスをインストールするには、管理者ロールを持つユーザーとしてログインする必要があります。接続サーバの最初のインスタンスをインストールするときに、管理者ロールを持つアカウントまたはグループを指定します。ロールは、ローカル Administrators グループ、ドメイン ユーザーまたはグループのいずれかに割り当てられます。[新しい構成での Horizon 接続サーバのインストール](#)を参照してください。
- 既存の接続サーバ インスタンスが複製インスタンスとは異なるドメインにある場合、ドメイン ユーザーには、既存のインスタンスがインストールされている Windows Server コンピュータでの管理者権限も必要です。
- MIT Kerberos 認証を使用して Connection Server をインストールする Windows Server 2008 R2 コンピュータにログインする場合、<http://support.microsoft.com/kb/978116> の KB 978116 に解説されている Microsoft ホットフィックスをインストールしてください。
- [Horizon 接続サーバの要件](#)で説明されている要件をインストールが満たしていることを確認します。
- 複製された接続サーバ インスタンスをインストールしているコンピュータが、高速 LAN で接続されていることを確認します。[複製された Horizon 接続サーバ インスタンスのネットワーク要件](#)を参照してください。
- 環境をインストール用に準備します。[Horizon 接続サーバのインストールの前提条件](#)を参照してください。
- Horizon 7 5.1 以降の複製された接続サーバ インスタンスをインストールしていて、複製している既存の接続サーバ インスタンスが Horizon 7 5.0.x 以前の場合は、データ リカバリ パスワードを準備します。[新しい構成での Horizon 接続サーバのインストール](#)を参照してください。
- Windows ファイアウォールで接続サーバ インスタンス用に開く必要があるネットワーク ポートについて理解します。[Horizon 接続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 サーバをこの接続サーバ インスタンスとペアにする場合、[セキュリティが強化された Windows ファイアウォール] がアクティブなプロファイルで [オン] に設定されていることを確認します。この設定はすべてのプロファイルで [オン] にすることを推奨します。デフォルトでは、IPsec ルールはセキュリティ サーバと接続サーバ間の接続を制御し、[セキュリティが強化された Windows ファイアウォール] を有効にする必要があります。
- ネットワーク トポロジにセキュリティ サーバと接続サーバ インスタンス間のバックエンドのファイアウォールが含まれている場合、IPsec をサポートするようにファイアウォールを構成する必要があります。[バックエンド ファイアウォールを構成して IPsec をサポートする](#)を参照してください。

手順

- 1 VMware ダウンロード ページ (<https://my.vmware.com/web/vmware/downloads>) から、接続サーバ インストーラ ファイルをダウンロードします。

[Desktop & End-User Computing (デスクトップおよびエンドユーザー コンピューティング)] で VMware Horizon 7 のダウンロードを選択します。これには接続サーバ ファイルが含まれます。

インストーラのファイル名は、VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe です。xxxxxx は、ビルド番号であり、y.y.y はバージョン番号です。

- 2 接続サーバのインストール プログラムを開始するには、インストーラ ファイルをダブルクリックします。
- 3 VMware のライセンス条件に同意します。
- 4 インストール先フォルダを受け入れるか、変更します。
- 5 [View レプリカ サーバ] インストール オプションを選択します。
- 6 インターネット プロトコル (IP) バージョンとして、[IPv4] または [IPv6] を選択します。
- 7 FIPS モードを有効にするか無効にするかを選択します。

このオプションは、Windows で FIPS モードが有効になっている場合にのみ使用可能です。

- 8 ユーザーが HTML Access を使用して自分自身のデスクトップに接続できるようにする場合は、[HTML Access のインストール] を選択します。

[IPv4] が選択されると、この設定がデフォルトで選択されます。[IPv6] が選択されると、HTML Access は IPv6 環境でサポートされていないため、この設定は表示されません。

- 9 複製している既存の接続サーバ インスタンスのホスト名または IP アドレスを入力します。
- 10 データ リカバリ パスワードを入力し、オプションでパスワード リマインダを入力します。

データ リカバリ パスワードが要求されるのは、複製している既存の接続サーバ インスタンスが Horizon 7 5.0.x 以前の場合のみです。

11 Windows ファイアウォール サービスを構成する方法を選択します。

オプション	アクション
Configure Windows Firewall automatically (Windows ファイアウォールを自動的に構成する)	インストーラで、必要なネットワーク接続を許可するように Windows ファイアウォールを構成します。
Do not configure Windows Firewall (Windows ファイアウォールを構成しない)	Windows ファイアウォール ルールを手動で構成します。 このオプションを選択するのは、組織が Windows ファイアウォールを構成するために独自の事前定義ルールを使用している場合のみです。

12 インストール ウィザードに従って、複製インスタンスのインストールを終了します。

13 Windows Server コンピュータで新しいパッチをチェックし、必要に応じて Windows Update を実行します。

接続サーバをインストールする前に Windows Server コンピュータのパッチを完全に適用していたとしても、インストールによりオペレーティング システム機能が初めて有効になる場合があります。この場合、追加のパッチが必要になる場合があります。

結果

次の Horizon 7 サービスが Windows Server コンピュータにインストールされます。

- VMware Horizon 接続サーバ
- VMware Horizon View Framework コンポーネント
- VMware Horizon View Message Bus コンポーネント
- VMware Horizon View スクリプト ホスト
- VMware Horizon View Security Gateway コンポーネント
- VMware Horizon View PCoIP Secure Gateway
- VMware Horizon View Blast Secure Gateway
- VMware Horizon View Web コンポーネント
- VMware VDMDS (View LDAP ディレクトリ サービスを提供します)

これらのサービスについては、『Horizon 7 の管理』ドキュメントを参照してください。

インストール時に [HTML Access のインストール] 設定を選択した場合、HTML Access コンポーネントが Windows Server コンピュータにインストールされています。このコンポーネントにより、Horizon 7 ユーザー ポータル ページの HTML Access アイコンが構成され、Windows ファイアウォールでの [VMware Horizon View 接続サーバ (Blast-In)] ルールが有効になります。このファイアウォール ルールにより、クライアント デバイス上の Web ブラウザは、TCP ポート 8443 で接続サーバに接続できるようになります。

次のステップ

接続サーバ インスタンス用に SSL サーバ証明書を構成します。[8 章 Horizon 7 Server 用の TLS 証明書の設定](#)を参照してください。

接続サーバの複製インスタンスでは、初期の Horizon 7 構成を行う必要はありません。複製されたインスタンスは、既存の接続サーバ インスタンスから構成を継承します。

ただし、この接続サーバ インスタンス用のクライアント接続設定の構成が必要な場合があり、大規模な展開をサポートするように Windows Server 設定を調整できます。「[Horizon Client 接続の構成および 展開の規模に合わせた Windows Server 設定の調整](#)」を参照してください。

接続サーバを再インストールして、パフォーマンス データを監視するようにデータ コレクタ セットを構成してある場合は、データ コレクタ セットを停止して再起動してください。

Horizon 接続サーバの複製インスタンスのサイレント インストール

Microsoft Windows インストーラ (MSI) のサイレント インストール機能を使用して、複数の Windows コンピュータに接続サーバの複製されたインスタンスをインストールできます。サイレント インストールはコマンド ラインを使用して行い、ウィザードのプロンプトに対応する必要はありません。

サイレント インストールを使うと、大規模なエンタープライズに Horizon 7 のコンポーネントを効率よく展開できます。

前提条件

- ネットワークに少なくとも 1 つの接続サーバ インスタンスがインストールおよび構成されていることを確認します。
- 複製されたインスタンスをインストールするには、管理者アカウントにアクセスするための認証情報を持つユーザーとしてログインする必要があります。接続サーバの最初のインスタンスをインストールするときに、管理者アカウントを指定します。アカウントは、ローカル Administrators グループ、ドメイン ユーザー、グループ アカウントのいずれかになります。[新しい構成での Horizon 接続サーバのインストール](#)を参照してください。
- 既存の接続サーバ インスタンスが複製インスタンスとは異なるドメインにある場合、ドメイン ユーザーには、既存のインスタンスがインストールされている Windows Server コンピュータでの管理者権限も必要です。
- MIT Kerberos 認証を使用して Connection Server をインストールする Windows Server 2008 R2 コンピュータにログインする場合、<http://support.microsoft.com/kb/978116> の KB 978116 に解説されている Microsoft ホットフィックスをインストールしてください。
- [Horizon 接続サーバの要件](#)で説明されている要件をインストールが満たしていることを確認します。
- 複製された接続サーバ インスタンスをインストールしているコンピュータが、高速 LAN で接続されていることを確認します。[複製された Horizon 接続サーバ インスタンスのネットワーク要件](#)を参照してください。
- 環境をインストール用に準備します。[Horizon 接続サーバのインストールの前提条件](#)を参照してください。
- Windows ファイアウォールで接続サーバ インスタンス用に開く必要があるネットワーク ポートについて理解します。[Horizon 接続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 サーバをこの接続サーバ インスタンスとペアにする場合、[セキュリティが強化された Windows ファイアウォール] がアクティブなプロファイルで [オン] に設定されていることを確認します。この設定はすべてのプロファイルで [オン] にすることを推奨します。デフォルトでは、IPsec ルールはセキュリティ サーバと接続サーバ間の接続を制御し、[セキュリティが強化された Windows ファイアウォール] を有効にする必要があります。
- ネットワーク トポロジにセキュリティ サーバと接続サーバ インスタンス間のバックエンドのファイアウォールが含まれている場合、IPsec をサポートするようにファイアウォールを構成する必要があります。[バックエンド ファイアウォールを構成して IPsec をサポートする](#)を参照してください。

- MSI インストーラのコマンドライン オプションについて理解しておきます。[Microsoft Windows インストーラ コマンド ライン オプション](#)を参照してください。
- 接続サーバのレプリカのインストールで使用できるサイレント インストール プロパティについて理解しておきます。[Horizon 接続サーバの複製インスタンスのサイレント インストールのプロパティ](#)を参照してください。

手順

- 1 VMware ダウンロード ページ (<https://my.vmware.com/web/vmware/downloads>) から、接続サーバ インストーラ ファイルをダウンロードします。

[Desktop & End-User Computing (デスクトップおよびエンドユーザー コンピューティング)] で VMware Horizon 7 のダウンロードを選択します。これには接続サーバ ファイルが含まれます。

インストーラのファイル名は、VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe です。xxxxxx は、ビルド番号であり、y.y.y はバージョン番号です。

- 2 Windows Server コンピュータでコマンド プロンプトを開きます。
- 3 インストール コマンドを 1 行で入力します。

例：VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=2
ADAM_PRIMARY_NAME=cs1.companydomain.com VDM_INITIAL_ADMIN_SID=S-1-5-32-544"

View 5.1 以降の複製された接続サーバ インスタンスをインストールしていて、複製している既存の接続サーバ インスタンスが View 5.0.x 以前の場合、データ リカバリ パスワードを指定する必要があり、パスワード リマインダを追加できます。例：VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn
VDM_SERVER_INSTANCE_TYPE=2 ADAM_PRIMARY_NAME=cs1.companydomain.com
VDM_INITIAL_ADMIN_SID=S-1-5-32-544 VDM_SERVER_RECOVERY_PWD=mini
VDM_SERVER_RECOVERY_PWD_REMINDER=""First car""

重要： サイレント インストールを実行する場合、データ リカバリ パスワードを含むフル コマンド ラインがインストーラの vminst.log ファイルに記録されます。インストールが完了したら、このログ ファイルを削除するか、Horizon Administrator を使用してデータ リカバリ パスワードを変更します。

- 4 Windows Server コンピュータで新しいパッチをチェックし、必要に応じて Windows Update を実行します。

接続サーバをインストールする前に Windows Server コンピュータのパッチを完全に適用していたとしても、インストールによりオペレーティング システム機能が初めて有効になる場合があります。この場合、追加のパッチが必要になる場合があります。

結果

次の Horizon 7 サービスが Windows Server コンピュータにインストールされます。

- VMware Horizon 接続サーバ
- VMware Horizon View Framework コンポーネント
- VMware Horizon View Message Bus コンポーネント
- VMware Horizon View スクリプト ホスト
- VMware Horizon View Security Gateway コンポーネント

- VMware Horizon View PCoIP Secure Gateway
- VMware Horizon View Blast Secure Gateway
- VMware Horizon View Web コンポーネント
- VMware VDMDS (View LDAP ディレクトリ サービスを提供します)

これらのサービスについては、『Horizon 7 の管理』ドキュメントを参照してください。

インストール時に [HTML Access のインストール] 設定を選択した場合、HTML Access コンポーネントが Windows Server コンピュータにインストールされています。このコンポーネントにより、Horizon 7 ユーザー ポータル ページの HTML Access アイコンが構成され、Windows ファイアウォールでの [VMware Horizon View 接続サーバ (Blast-In)] ルールが有効になります。このファイアウォール ルールにより、クライアント デバイス上の Web ブラウザは、TCP ポート 8443 で接続サーバに接続できるようになります。

次のステップ

接続サーバ インスタンス用に SSL サーバ証明書を構成します。[8 章 Horizon 7 Server 用の TLS 証明書の設定](#)を参照してください。

接続サーバの複製インスタンスでは、初期の Horizon 7 構成を行う必要はありません。複製されたインスタンスは、既存の接続サーバ インスタンスから構成を継承します。

ただし、この接続サーバ インスタンス用のクライアント接続設定の構成が必要な場合があり、大規模な展開をサポートするように Windows Server 設定を調整できます。「[Horizon Client 接続の構成および 展開の規模に合わせた Windows Server 設定の調整](#)」を参照してください。

Horizon 接続サーバの複製インスタンスのサイレント インストールのプロパティ

コマンド ラインから Horizon 接続サーバの複製されたインスタンスをサイレント インストールするときに、特定の プロパティを含めることができます。Microsoft Windows Installer (MSI) がプロパティと値を解釈できるように、*PROPERTY=value* 形式を使用する必要があります。

表 7-2. Horizon 接続サーバの複製インスタンスをサイレント インストールする場合の MSI のプロパティ

MSI プロパティ	説明	デフォルト値
INSTALLDIR	<p>接続サーバ ソフトウェアをインストールするパスとフォルダ。</p> <p>例: <code>INSTALLDIR=""D:\abc\my folder""</code></p> <p>パスを囲む二重引用符によって MSI インストーラにパスの有効部分としてスペースを解釈することを許可します。</p> <p>この MSI プロパティはオプションです。</p>	<p>%ProgramFiles%\VMware\VMware View\Server</p>
VDM_SERVER_INSTANCE_TYPE	<p>接続サーバのインストールの種類</p> <ul style="list-style-type: none"> ■ 1. 標準インストール ■ 2. レプリカ インストール ■ 3. セキュリティ サーバ インストール <p>複製されたインスタンスをインストールするには、<code>VDM_SERVER_INSTANCE_TYPE=2</code> を指定します。</p> <p>この MSI プロパティは、レプリカ インストールの場合は必須です。</p>	1

表 7-2. Horizon 接続サーバの複製インスタンスをサイレント インストールする場合の MSI のプロパティ（続き）

MSI プロパティ	説明	デフォルト値
ADAM_PRIMARY_NAME	複製している既存の接続サーバ インスタンスのホスト名または IP アドレス。 例：ADAM_PRIMARY_NAME=cs1.companydomain.com この MSI プロパティは必須です。	なし
FWCHOICE	接続サーバのインスタンスに対してファイアウォールを構成するかどうかを指定する MSI プロパティ。 値 1 はファイアウォールを構成します。値 2 はファイアウォールを構成しません。 例：FWCHOICE=1 この MSI プロパティはオプションです。	1
VDM_SERVER_RECOVERY_PWD	データ リカバリ パスワード。データ リカバリ パスワードが View LDAP に設定されていない場合、このプロパティは必須です。 注： 複製する標準接続サーバ インスタンスが View 5.0 以前の場合は、データ リカバリ パスワードは View LDAP に設定されません。複製する接続サーバ インスタンスが View 5.1 以降の場合、このプロパティを指定する必要はありません。 パスワードは 1 文字から 128 文字の間にする必要があります。安全なパスワードの生成に関する組織のベスト プラクティスに従ってください。	なし
VDM_SERVER_RECOVERY_PWD_REMINDER	データ リカバリ パスワードのリマインダ。このプロパティは省略可能です。	なし
VDM_IP_PROTOCOL_USAGE	Horizon 7 コンポーネントが通信で使用する IP アドレスのバージョンを指定します。使用可能な値は IPv4 および IPv6 です	IPv4
VDM_FIPS_ENABLED	FIPS モードを有効にするか無効にするかを指定します。値 1 は FIPS モードを有効にします。値 0 は FIPS モードを無効にします。このプロパティが 1 に設定され、Windows が FIPS モードになっていない場合、インストーラは中断されます。	0

セキュリティ サーバのペアリング パスワードを構成する

セキュリティ サーバをインストールする前に、セキュリティ サーバのペアリング パスワードを構成する必要があります。接続サーバ インストール プログラムでセキュリティ サーバをインストールする場合、インストール中にこのパスワードの入力を求められます。

セキュリティ サーバのペアリング パスワードは、セキュリティ サーバと接続サーバ インスタンスをペアにすることを可能にする 1 回限りのパスワードです。このパスワードは、接続サーバのインストール プログラムに対して入力した後は無効になります。

注： 古いバージョンのセキュリティ サーバと現バージョンの接続サーバをペアにすることはできません。現バージョンの接続サーバでペアリング パスワードを構成し、古いバージョンのセキュリティ サーバをインストールしようとすると、ペアリング パスワードが無効になります。

手順

- 1 Horizon Administrator で、[View 構成] - [サーバ] を選択します。

- 2 [接続サーバ] タブで、セキュリティ サーバとペアにする接続サーバ インスタンスを選択します。
- 3 [その他のコマンド] ドロップダウン メニューから [セキュリティ サーバのペアリング パスワードを指定する] を選択します。
- 4 ペアリング パスワードおよび確認パスワード テキスト ボックスにパスワードを入力し、パスワードのタイムアウト値を指定します。

指定したタイムアウト期間内にパスワードを使用する必要があります。

- 5 [OK] をクリックしてパスワードを構成します。

次のステップ

セキュリティ サーバをインストールします。[セキュリティ サーバをインストールする](#)を参照してください。

重要： パスワードのタイムアウト期間内に接続サーバのインストール プログラムにセキュリティ サーバのペアリング パスワードを指定しない場合、そのパスワードは無効になり、新しいパスワードを設定する必要があります。

セキュリティ サーバをインストールする

セキュリティ サーバは、インターネットと内部ネットワークの間に新しいセキュリティ レイヤーを追加する Connection Server のインスタンスです。1 つの Connection Server インスタンスに対し、1 台以上のセキュリティ サーバをインストールして接続できます。

セキュリティ サーバ ソフトウェアは、レプリカ サーバ、Connection Server、View Composer、Horizon Agent、または Horizon Client を含む他の Horizon 7 ソフトウェア コンポーネントと同じ仮想マシンまたは物理マシンにインストールすることができません。

前提条件

- 使用するトポロジの種類を決定します。たとえば、使用するロード バランシング ソリューションを決定します。セキュリティ サーバとペアになっている接続サーバ インスタンスを外部ネットワークのユーザー専用にするかどうかを判断します。詳細については、『Horizon 7 アーキテクチャの計画』を参照してください。

重要： ロード バランサを使用する場合は、変更されない IP アドレスを持っている必要があります。IPv4 環境では、固定 IP アドレスを構成します。IPv6 環境では、変更されない IP アドレスがマシンによって自動的に取得されます。

- [Horizon 接続サーバの要件](#)で説明されている要件をインストールが満たしていることを確認します。
- 環境をインストール用に準備します。[Horizon 接続サーバのインストールの前提条件](#)を参照してください。
- セキュリティ サーバとペアにされる接続サーバ インスタンスがインストールおよび構成され、セキュリティ サーバ バージョンと互換性がある接続サーバ バージョンが実行されていることを確認します。『Horizon 7 のアップグレード』ドキュメントで「Horizon 7 コンポーネントの互換性マトリックス」を参照してください。

- セキュリティ サーバとペアにする接続サーバのインスタンスが、セキュリティ サーバをインストールする予定のコンピュータからアクセスできることを確認します。

注： 接続サーバを Horizon 7 バージョン 7.5 にアップグレードした場合、IPsec が無効になっているセキュリティ サーバを再インストールする必要があります。セキュリティ サーバの IP アドレスが変更された場合、再インストールする必要があります。セキュリティ サーバが動的 NAT の背後にある場合、セキュリティ サーバのペアリングが正しく機能しません。

- セキュリティ サーバのペアリング パスワードを構成します。 [セキュリティ サーバのペアリング パスワードを構成する](#) を参照してください。
- 外部 URL の形式を理解します。 [Secure Gateway 接続およびトンネル接続用の外部 URL の構成](#) を参照してください。
- セキュリティが強化された Windows ファイアウォール がアクティブなプロファイルで [オン] に設定されていることを確認します。この設定はすべてのプロファイルで [オン] にすることを推奨します。デフォルトでは、IPsec ルールはセキュリティ サーバと View Connection Server 間の接続を制御し、[セキュリティが強化された Windows ファイアウォール] を有効にする必要があります。
- Windows ファイアウォールでセキュリティ サーバ用に開かれている必要があるネットワーク ポートについて理解します。 [Horizon 接続サーバのファイアウォール ルール](#) を参照してください。
- ネットワーク トポロジにセキュリティ サーバと Connection Server 間のバックエンドのファイアウォールが含まれている場合、IPsec をサポートするようにファイアウォールを構成する必要があります。 [バックエンド ファイアウォールを構成して IPsec をサポートする](#) を参照してください。
- セキュリティ サーバをアップグレードまたは再インストールしている場合、セキュリティ サーバの既存の IPsec ルールが削除されていることを確認します。 [セキュリティ サーバの IPsec ルールの削除](#) を参照してください。
- Horizon 7 を FIPS モードでインストールしている場合は、Horizon Administrator のグローバル設定である [セキュリティ サーバへの接続に IPsec を使用する] の選択を解除する必要があります。これは、FIPS モードではセキュリティ サーバのインストール後に手動で IPsec を構成する必要があるためです。

手順

- 1 VMware ダウンロード ページ (<https://my.vmware.com/web/vmware/downloads>) から、接続サーバ インストーラ ファイルをダウンロードします。

[Desktop & End-User Computing (デスクトップおよびエンドユーザー コンピューティング)] で VMware Horizon 7 のダウンロードを選択します。これには接続サーバ ファイルが含まれます。

インストーラのファイル名は、VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe です。xxxxxx は、ビルド番号であり、y.y.y はバージョン番号です。

- 2 接続サーバのインストール プログラムを開始するには、インストーラ ファイルをダブルクリックします。
- 3 VMware のライセンス条件に同意します。
- 4 インストール先フォルダを受け入れるか、変更します。
- 5 [View セキュリティ サーバ] インストール オプションを選択します。

- 6 インターネット プロトコル (IP) バージョンとして、[IPv4] または [IPv6] を選択します。

すべての Horizon 7 コンポーネントを同じ IP バージョンでインストールする必要があります。

- 7 FIPS モードを有効にするか無効にするかを選択します。

このオプションは、Windows で FIPS モードが有効になっている場合にのみ使用可能です。

- 8 セキュリティ サーバとペアにする Connection Server インスタンスの完全修飾ドメイン名または IP アドレスを、[サーバ] テキスト ボックスに入力します。

セキュリティ サーバは、ネットワーク トラフィックをこの Connection Server インスタンスに転送します。

- 9 セキュリティ サーバのペアリング パスワードを [パスワード] テキスト ボックスに入力します。

パスワードの有効期限が切れている場合は、Horizon Administrator を使用して新しいパスワードを構成した後、新しいパスワードをインストール プログラムに入力できます。

- 10 [外部 URL] テキスト ボックスに、セキュリティ サーバの外部 URL を入力します。これは、使用している表示プロトコルに関係なく、すべてのクライアントで必要になります。

URL には、プロトコル識別子 (https)、クライアントが解決可能なセキュリティ サーバ名、ポート番号 (443) が含まれている必要があります。

例: https://view.example.com:443

ネットワークの外部にあるトンネル対応クライアントは、この URL を使用して、セキュリティ サーバ経由でネットワーク内のマシンに接続します。

- 11 [PCoIP 外部 URL] テキスト ボックスに、セキュリティ サーバの PCoIP ゲートウェイの外部 URL を入力します。これは、PCoIP 表示プロトコルを使用するクライアントがリモート デスクトップに接続する場合に必要なになります。

プロトコル相対 URL には、セキュリティ サーバの IP アドレスとポート番号 (4172) が含まれている必要があります。IPv4 環境では、IPv4 アドレスを使用します。IPv6 環境では、IPv6 アドレスを使用します。

IPv4 環境の例: 10.20.30.40:4172

ネットワークの外部にある PCoIP 対応クライアントは、この URL を使用して、セキュリティ サーバ経由でネットワーク内のマシンに接続します。

注: IPv6 環境の場合、ここに IPv6 アドレスを入力する必要がありますが、インストール後に、クライアントで解決可能な名前に置き換えることができます。

- 12 [Blast 外部 URL] テキスト ボックスに、セキュリティ サーバの Blast ゲートウェイの外部 URL を入力します。これは、Blast 表示プロトコルまたは HTML Access を使用するクライアントがリモート デスクトップに接続する場合に必要なになります。

URL には、プロトコル識別子 (https)、クライアントが解決可能なセキュリティ サーバ名、ポート番号 (8443) が含まれている必要があります。

例: https://myserver.example.com:8443

ネットワークの外部にある Blast 対応の HTML Access クライアントは、この URL を使用して、セキュリティ サーバ経由でネットワーク内のマシンに接続します。

13 Windows ファイアウォール サービスを構成する方法を選択します。

オプション	アクション
Configure Windows Firewall automatically (Windows ファイアウォールを自動的に構成する)	インストーラで、必要なネットワーク接続を許可するように Windows ファイアウォールを構成します。
Do not configure Windows Firewall (Windows ファイアウォールを構成しない)	Windows ファイアウォール ルールを手動で構成します。 このオプションを選択するのは、組織が Windows ファイアウォールを構成するために独自の事前定義ルールを使用している場合のみです。

14 インストール ウィザードに従って、セキュリティ サーバのインストールを終了します。

結果

セキュリティ サーバの以下のサービスが Windows Server コンピュータにインストールされます。

- VMware Horizon View セキュリティ サーバ
- VMware Horizon View Framework コンポーネント
- VMware Horizon View Security Gateway コンポーネント
- VMware Horizon View PCoIP Secure Gateway
- VMware Blast Secure Gateway

これらのサービスについては、『Horizon 7 の管理』ドキュメントを参照してください。

セキュリティ サーバが Horizon Administrator の セキュリティ サーバ ペインに表示されます。

[VMware Horizon View Connection Server (Blast-In)] ルールは、セキュリティ サーバの Windows ファイアウォールで有効にします。このファイアウォール ルールにより、クライアント デバイス上の Web ブラウザは HTML Access を使用して、TCP ポート 8443 でセキュリティ サーバにアクセスできるようになります。

注： インストールがキャンセルまたは中断された場合は、インストールをもう一度開始する前にセキュリティ サーバの IPsec ルールを削除する必要があります。IPsec ルールをすでに削除した場合であっても、セキュリティ サーバの再インストールまたはアップグレードの前に、この手順を行ってください。IPsec ルールの削除手順については、[セキュリティ サーバの IPsec ルールの削除](#)を参照してください。

次のステップ

セキュリティ サーバ用の SSL サーバ証明書を構成します。[8 章 Horizon 7 Server 用の TLS 証明書の設定](#)を参照してください。

セキュリティ サーバ用のクライアント接続設定の構成が必要な場合があり、大規模な展開をサポートするように Windows Server 設定を調整できます。[Horizon Client 接続の構成](#)および [展開の規模に合わせた Windows Server 設定の調整](#)を参照してください。

セキュリティ サーバを再インストールしていて、パフォーマンス データを監視するようにデータ コレクタ セットを構成してある場合は、データ コレクタ セットを停止して再起動してください。

セキュリティ サーバをサイレント インストールする

Microsoft Windows インストーラ (MSI) のサイレント インストール機能を使用して、複数の Windows コンピュータにセキュリティ サーバをインストールできます。サイレント インストールはコマンド ラインを使用して行い、ウィザードのプロンプトに対応する必要はありません。

サイレント インストールを使うと、大規模なエンタープライズに Horizon 7 のコンポーネントを効率よく展開できます。

前提条件

- 使用するトポロジの種類を決定します。たとえば、使用するロード バランシング ソリューションを決定します。セキュリティ サーバとペアになっている接続サーバ インスタンスを外部ネットワークのユーザー専用にするかどうかを判断します。詳細については、『Horizon 7 アーキテクチャの計画』を参照してください。

重要： ロード バランサを使用する場合は、変更されない IP アドレスを持っている必要があります。IPv4 環境では、固定 IP アドレスを構成します。IPv6 環境では、変更されない IP アドレスがマシンによって自動的に取得されます。

- [Horizon 接続サーバの要件](#)で説明されている要件をインストールが満たしていることを確認します。
- 環境をインストール用に準備します。[Horizon 接続サーバのインストールの前提条件](#)を参照してください。
- セキュリティ サーバとペアにされる接続サーバ インスタンスがインストールおよび構成され、セキュリティ サーババージョンと互換性がある接続サーババージョンが実行されていることを確認します。『Horizon 7 のアップグレード』ドキュメントで「Horizon 7 コンポーネントの互換性マトリックス」を参照してください。
- セキュリティ サーバとペアにする接続サーバのインスタンスが、セキュリティ サーバをインストールする予定のコンピュータからアクセスできることを確認します。

注： 接続サーバを Horizon 7 バージョン 7.5 にアップグレードした場合、IPsec が無効になっているセキュリティ サーバを再インストールする必要があります。セキュリティ サーバの IP アドレスが変更された場合、再インストールする必要があります。セキュリティ サーバが動的 NAT の背後にある場合、セキュリティ サーバのペアリングが正しく機能しません。

- セキュリティ サーバのペアリング パスワードを構成します。[セキュリティ サーバのペアリング パスワードを構成する](#)を参照してください。
- 外部 URL の形式を理解します。[Secure Gateway 接続およびトンネル接続用の外部 URL の構成](#)を参照してください。
- セキュリティが強化された Windows ファイアウォール がアクティブなプロファイルで [オン] に設定されていることを確認します。この設定はすべてのプロファイルで [オン] にすることを推奨します。デフォルトでは、IPsec ルールはセキュリティ サーバと接続サーバ間の接続を制御し、[セキュリティが強化された Windows ファイアウォール] を有効にする必要があります。
- Windows ファイアウォールでセキュリティ サーバ用に開かれている必要があるネットワーク ポートについて理解します。[Horizon 接続サーバのファイアウォール ルール](#)を参照してください。

- ネットワーク トポロジにセキュリティ サーバと接続サーバ間のバックエンドのファイアウォールが含まれている場合、IPsec をサポートするようにファイアウォールを構成する必要があります。[バックエンド ファイアウォールを構成して IPsec をサポートする](#)を参照してください。
- セキュリティ サーバをアップグレードまたは再インストールしている場合、セキュリティ サーバの既存の IPsec ルールが削除されていることを確認します。[セキュリティ サーバの IPsec ルールの削除](#)を参照してください。
- MSI インストーラのコマンドライン オプションについて理解しておきます。[Microsoft Windows インストーラ コマンド ライン オプション](#)を参照してください。
- セキュリティ サーバで使用できるサイレント インストールのプロパティについて理解します。[セキュリティ サーバのサイレント インストールのプロパティ](#)を参照してください。
- Horizon 7 を FIPS モードでインストールしている場合は、Horizon Administrator のグローバル設定である [セキュリティ サーバへの接続に IPsec を使用する] の選択を解除する必要があります。これは、FIPS モードではセキュリティ サーバのインストール後に手動で IPsec を構成する必要があるためです。

手順

- 1 VMware ダウンロード ページ (<https://my.vmware.com/web/vmware/downloads>) から、接続サーバ インストーラ ファイルをダウンロードします。

[Desktop & End-User Computing (デスクトップおよびエンドユーザー コンピューティング)] で VMware Horizon 7 のダウンロードを選択します。これには接続サーバ ファイルが含まれます。

インストーラのファイル名は、VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe です。xxxxxx は、ビルド番号であり、y.y.y はバージョン番号です。

- 2 Windows Server コンピュータでコマンド プロンプトを開きます。
- 3 インストール コマンドを 1 行で入力します。

```
例 : VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"/qn VDM_SERVER_INSTANCE_TYPE=3
VDM_SERVER_NAME=cs1.internaldomain.com VDM_SERVER_SS_EXTURL=https://
view.companydomain.com:443 VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40
VDM_SERVER_SS_PCOIP_TCPPORT=4172 VDM_SERVER_SS_PCOIP_UDPPORT=4172
VDM_SERVER_SS_BSG_EXTURL=https://view.companydomain.com:8443 VDM_SERVER_SS_PWD=secret"
```

結果

セキュリティ サーバの以下のサービスが Windows Server コンピュータにインストールされます。

- VMware Horizon View セキュリティ サーバ
- VMware Horizon View Framework コンポーネント
- VMware Horizon View Security Gateway コンポーネント
- VMware Horizon View PCoIP Secure Gateway
- VMware Blast Secure Gateway

これらのサービスについては、『Horizon 7 の管理』ドキュメントを参照してください。

セキュリティ サーバが Horizon Administrator の セキュリティ サーバ ペインに表示されます。

[VMware Horizon View 接続サーバ (Blast-In)] ルールは、セキュリティ サーバの Windows ファイアウォールで有効にします。このファイアウォール ルールにより、クライアント デバイス上の Web ブラウザは HTML Access を使用して、TCP ポート 8443 でセキュリティ サーバにアクセスできるようになります。

注： インストールがキャンセルまたは中断された場合は、インストールをもう一度開始する前にセキュリティ サーバの IPsec ルールを削除する必要があります。IPsec ルールをすでに削除した場合であっても、セキュリティ サーバの再インストールまたはアップグレードの前に、この手順を行ってください。IPsec ルールの削除手順については、[セキュリティ サーバの IPsec ルールの削除](#)を参照してください。

次のステップ

セキュリティ サーバ用の SSL サーバ証明書を構成します。[8 章 Horizon 7 Server 用の TLS 証明書の設定](#)を参照してください。

セキュリティ サーバ用のクライアント接続設定の構成が必要な場合があり、大規模な展開をサポートするように Windows Server 設定を調整できます。「[Horizon Client 接続の構成](#)および [展開の規模に合わせた Windows Server 設定の調整](#)」を参照してください。

セキュリティ サーバのサイレント インストールのプロパティ

コマンド ラインからセキュリティ サーバをサイレント インストールするときに、特定のプロパティを含めることができます。Microsoft Windows Installer (MSI) がプロパティと値を解釈できるように、*PROPERTY=value* 形式を使用する必要があります。

表 7-3. セキュリティ サーバをサイレント インストールするための MSI のプロパティ

MSI プロパティ	説明	デフォルト値
INSTALLDIR	<p>接続サーバ ソフトウェアをインストールするパスとフォルダ。</p> <p>例: <code>INSTALLDIR=""D:\abc\my folder""</code></p> <p>パスを囲む二重引用符によって MSI インストーラにパスの有効部分としてスペースを解釈することを許可します。</p> <p>この MSI プロパティはオプションです。</p>	<p>%ProgramFiles%\VMware\VMware View\Server</p>
VDM_SERVER_INSTANCE_TYPE	<p>接続サーバのインストールの種類</p> <ul style="list-style-type: none"> ■ 1. 標準インストール ■ 2. レプリカ インストール ■ 3. セキュリティ サーバ インストール <p>セキュリティ サーバをインストールするには、<code>VDM_SERVER_INSTANCE_TYPE=3</code> を指定します。</p> <p>この MSI プロパティは、セキュリティ サーバ インストールの場合は必須です。</p>	1
VDM_SERVER_NAME	<p>セキュリティ サーバとペアにする既存の接続サーバ インスタンスのホスト名または IP アドレス。</p> <p>例: <code>VDM_SERVER_NAME=cs1.internaldomain.com</code></p> <p>この MSI プロパティは必須です。</p>	なし
VDM_SERVER_SS_EXTURL	<p>セキュリティ サーバの外部 URL。URL には、プロトコル、外部で解決可能なセキュリティ サーバ名、およびポート番号が含まれている必要があります。</p> <p>例: <code>VDM_SERVER_SS_EXTURL=https://view.companydomain.com:443</code></p> <p>この MSI プロパティは必須です。</p>	なし

表 7-3. セキュリティ サーバをサイレント インストールするための MSI のプロパティ (続き)

MSI プロパティ	説明	デフォルト値
VDM_SERVER_SS_PWD	<p>セキュリティ サーバのベアリング パスワード。</p> <p>例: VDM_SERVER_SS_PWD=secret</p> <p>この MSI プロパティは必須です。</p>	なし
FWCHOICE	<p>接続サーバのインスタンスに対してファイアウォールを構成するかどうかを指定する MSI プロパティ。</p> <p>値 1 はファイアウォールを構成します。値 2 はファイアウォールを構成しません。</p> <p>例: FWCHOICE=1</p> <p>この MSI プロパティはオプションです。</p>	1
VDM_SERVER_SS_PCOIP_IPADDR	<p>PCoIP Secure Gateway の外部 IP アドレス。IPv6 環境では、このプロパティも PCoIP Secure Gateway の FQDN に設定できます。このプロパティがサポートされるのは、セキュリティ サーバが Windows Server 2008 R2 以降にインストールされている場合だけです。</p> <p>例: VDM_SERVER_SS_PCOIP_IPADDR=10.20.30.40</p> <p>このプロパティは、PCoIP Secure Gateway コンポーネントを使用する場合は必須です。</p>	なし
VDM_SERVER_SS_PCOIP_TCPPORT	<p>PCoIP Secure Gateway の外部 TCP ポート番号。このプロパティがサポートされるのは、セキュリティ サーバが Windows Server 2008 R2 以降にインストールされている場合だけです。</p> <p>例: VDM_SERVER_SS_PCOIP_TCPPORT=4172</p> <p>このプロパティは、PCoIP Secure Gateway コンポーネントを使用する場合は必須です。</p>	なし
VDM_SERVER_SS_PCOIP_UDPPORT	<p>PCoIP Secure Gateway の外部 UDP ポート番号。このプロパティがサポートされるのは、セキュリティ サーバが Windows Server 2008 R2 以降にインストールされている場合だけです。</p> <p>例: VDM_SERVER_SS_PCOIP_UDPPORT=4172</p> <p>このプロパティは、PCoIP Secure Gateway コンポーネントを使用する場合は必須です。</p>	なし
VDM_SERVER_SS_BSG_EXTURL	<p>Blast Secure Gateway の外部 URL。URL には、HTTPS プロトコル、外部で解決可能なセキュリティ サーバ名、およびポート番号が含まれている必要があります。</p> <p>例: VDM_SERVER_SS_BSG_EXTURL=https://view.companydomain.com:8443</p> <p>デフォルトのポート番号は 8443 です。ユーザーが Web 経由で Horizon 7 デスクトップに接続できるようにするには、セキュリティ サーバに Blast Secure Gateway をインストールする必要があります。</p>	なし
VDM_SERVER_SS_FORCE_IPSEC	<p>セキュリティ サーバとそのペアの接続サーバ インスタンス間で、強制的に IPsec が使用されるようにします。</p> <p>デフォルトでは、セキュリティ サーバを無人インストールし、IPsec が無効になった接続サーバ インスタンスとベアリングすると、ベアリングに失敗します。</p> <p>デフォルト値の 1 では、IPsec を使用してベアリングが実行されます。この値を 0 に設定すると、IPsec を使用せずにベアリングを実行できます。</p>	1

表 7-3. セキュリティ サーバをサイレント インストールするための MSI のプロパティ （続き）

MSI プロパティ	説明	デフォルト値
VDM_IP_PROTOCOL_USAGE	Horizon 7 コンポーネントが通信で使用する IP アドレスのバージョンを指定します。使用可能な値は IPv4 および IPv6 です	IPv4
VDM_FIPS_ENABLED	FIPS モードを有効にするか無効にするかを指定します。値 1 は FIPS モードを有効にします。値 0 は FIPS モードを無効にします。このプロパティが 1 に設定され、Windows が FIPS モードになっていない場合、インストーラは中断されます。	0

セキュリティ サーバの IPsec ルールの削除

セキュリティ サーバ インスタンスをアップグレードまたは再インストールする前に、セキュリティ サーバとそれとペアになっている接続サーバ インスタンス間の通信を管理する現在の IPsec ルールを削除する必要があります。この手順を実行しなければ、アップグレードまたは再インストールに失敗します。

デフォルトでは、セキュリティ サーバとそのペアの接続サーバ インスタンス間の通信は IPsec ルールによって制御されています。セキュリティ サーバをアップグレードまたは再インストールし、接続サーバ インスタンスと再びペアにする場合、新しい IPsec ルールのセットを確立する必要があります。アップグレードまたは再インストール前に既存の IPsec ルールが削除されていない場合は、ペアリングは失敗します。

セキュリティ サーバをアップグレードまたは再インストールし、IPsec を使用してセキュリティ サーバと接続サーバ間の通信を保護する場合は、この手順を実行する必要があります。

IPsec ルールを使用しなくても、最初のセキュリティ サーバ ペアリングを構成できます。セキュリティ サーバをインストールする前に、Horizon Administrator を開き、デフォルトで有効になっているグローバル設定の [セキュリティ サーバの接続に IPsec を使用] の選択を解除できます。IPsec ルールが有効でない場合は、アップグレードまたは再インストールの前に IPsec ルールを削除する必要はありません。

注： セキュリティ サーバのアップグレードまたは再インストールの前に Horizon Administrator からセキュリティ サーバを削除する必要はありません。Horizon 7 環境からセキュリティ サーバを永久的に削除したい場合にのみ、Horizon Administrator からセキュリティ サーバを削除します。

View 5.0.x および以前のリリースでは、Horizon Administrator ユーザー インターフェイス内から、または `vdmadmin -S` コマンドを使用して、セキュリティ サーバを削除できました。View 5.1 以降のリリースでは、`vdmadmin -S` を使用する必要があります。『Horizon 7 の管理』ドキュメントの「-S オプションを使用した Horizon 接続サーバ インスタンスまたはセキュリティ サーバのエントリの削除」を参照してください。

注意： アクティブ セキュリティ サーバ用の IPsec ルールを削除する場合、セキュリティ サーバのすべての通信は、セキュリティ サーバのアップグレードまたは再インストールまで失われます。そのため、ロード バランサを使用してセキュリティ サーバのグループを管理する場合、1 つのサーバでこの手順を実行し、そのサーバをアップグレードしてから、次のサーバの IPsec ルールを削除します。このように本番環境からサーバを削除して 1 つずつ再度追加することで、エンド ユーザーのダウンタイムを回避できます。

手順

- 1 Horizon Administrator で、[View 構成] - [サーバ] の順にクリックします。

- 2 [セキュリティ サーバ] タブで、セキュリティ サーバを選択し、[その他のコマンド] - [アップグレードまたは再インストールの準備] をクリックします。

セキュリティ サーバをインストールする前に IPsec ルールを無効にした場合は、この設定は無効です。この場合、再インストールまたはアップグレード前に IPsec ルールを削除する必要はありません。

- 3 [OK] をクリックします。

結果

IPsec ルールが削除され、[アップグレードまたは再インストールを準備] 設定が無効になります。つまりセキュリティ サーバを再インストールまたはアップグレードできます。

次のステップ

セキュリティ サーバをアップグレードまたは再インストールします。

VPN 経由で Unified Access Gateway アプライアンスを使用する利点

Unified Access Gateway アプライアンスは、企業のファイアウォールの外側からリモート デスクトップおよびアプリケーションに安全にアクセスできるようにするデフォルト ゲートウェイです。

Unified Access Gateway ドキュメントの最新バージョンについては、<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』を参照してください。

Unified Access Gateway アプライアンスは、ネットワークの非武装地帯 (DMZ) に配置され、信頼できるネットワーク内の接続に対してプロキシ ホストとして機能します。仮想デスクトップ、アプリケーション ホスト、サーバが公衆インターネットから隠ぺいされるため、追加のセキュリティ レイヤが実現されます。

Unified Access Gateway アプライアンスの構成

Unified Access Gateway と一般的な VPN ソリューションは、確実な方法で認証されたユーザーのためだけに内部ネットワークに確実にトラフィックが転送されるようにする点で似ています。

一般的な VPN よりも Unified Access Gateway は、次の点で優れています。

- アクセス コントロール マネージャ。Unified Access Gateway は、アクセス ルールを自動的に適用します。Unified Access Gateway は、内部接続に必要なユーザーの資格とアドレスの設定について認識しています。大半の VPN では管理者が各ユーザーまたは各ユーザー グループにネットワーク接続ルールを設定できるので、VPN でも同じ処理が行われます。最初に、これは VPN では適切に動作しますが、必要なルールを維持するためには相当な管理労力が必要となります。
- ユーザー インターフェイス。Unified Access Gateway では、簡単な Horizon Client ユーザー インターフェイスをそのまま使用できます。Unified Access Gateway では、Horizon Client が起動されると、認証されたユーザーは View 環境に配置され、デスクトップとアプリケーションへのアクセスを制御できます。VPN では、VPN ソフトウェアを最初にセットアップして、Horizon Client を起動する前に別々に認証することが求められます。

- パフォーマンス。Unified Access Gateway は、セキュリティとパフォーマンスを最大化できるように設計されています。Unified Access Gateway を使用すると、追加のカプセル化を実行しなくても、PCoIP、HTML Access、および WebSocket プロトコルのセキュリティが確保されます。VPN は、SSL VPN として実装されます。この実装は、セキュリティ要件を満たしており、Transport Layer Security (TLS) が有効である場合、安全だと考えられていますが、SSL/TLS におけるバックエンドのプロトコルは、TCP ベースに過ぎません。コネクションレスの UDP ベースの転送を利用する最新のビデオ リモートリング プロトコルでは、TCP ベースの転送を強制すると、パフォーマンス上の利点が大幅に損なわれる場合があります。SSL/TLS の代わりに DTLS や IPsec を使用して、ネットワークを運用できる場合、Horizon 7 デスクトップ プロトコルを適切に稼働させることができるので、これはすべての VPN テクノロジーで起こるわけではありません。

Unified Access Gateway による Horizon のセキュリティの強化

Unified Access Gateway アプライアンスは、ユーザー認証の他にデバイスの証明書の認証を行い、既知の良好なデバイスからのアクセスのみを許可します。これにより、仮想デスクトップ インフラストラクチャを多層的に保護しています。

注： この機能は、Horizon Client for Windows でのみサポートされます。

- <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』で、「Unified Access Gateway アプライアンスでの証明書またはスマート カード認証の構成」を参照してください。
- Unified Access Gateway で使用可能な他のユーザー認証サービスに加え、エンドポイント コンプライアンス チェック機能を使用すると、Horizon デスクトップへのアクセスに対するセキュリティが強化されます。<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』で「Horizon のエンドポイント コンプライアンス チェック」を参照してください。

重要： Unified Access Gateway アプライアンスで 2 要素認証 (RSA SecureID と RADIUS) が構成され、Windows ユーザー名の一一致が有効で、複数のユーザー ドメインがある場合は、Windows ユーザー名とパスワードで認証を行うときにユーザーが正しいドメインを選択できるように、Connection Server にドメイン リストの送信を許可する必要があります。

ダブルホップ DMZ

インターネットと内部ネットワークの間にダブルホップ DMZ が必要な場合、内側の DMZ に Unified Access Gateway を展開し、外側の DMZ に Web リバース プロキシとして Unified Access Gateway アプライアンスをデプロイすることで、ダブルホップ DMZ 構成を作成できます。トラフィックは、各 DMZ レイヤーの特定のリバース プロキシを通過しますが、DMZ レイヤーをバイパスすることはできません。構成の詳細については、『VMware Unified Access Gateway の導入および設定』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 7-4. 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 ポッド アーキテクチャ機能の場合：ポ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 ポッド 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 ポッド 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。

バックエンド ファイアウォールを構成して IPsec をサポートする

ネットワーク トポロジにセキュリティ サーバと接続サーバ インスタンス間のバックエンド ファイアウォールが含まれている場合、IPsec をサポートするにはファイアウォールに対して特定のプロトコルとポートを構成する必要があります。適切な構成が存在しない場合、セキュリティ サーバと接続サーバ インスタンス間に送信されるデータはファイアウォールを通過できません。

デフォルトでは、セキュリティ サーバと接続サーバ インスタンス間の接続は IPsec ルールによって制御されます。IPsec をサポートするために、接続サーバ インスタンスは、Horizon 7 サーバがインストールされる Windows Server ホストで Windows ファイアウォールのルールを構成できます。バック エンド ファイアウォールについては、ユーザー自身でルールを構成する必要があります。

注： IPsec の使用を強くお勧めします。代わりに、Horizon Administrator グローバル設定、[セキュリティ サーバの接続に IPsec を使用] を無効にするという方法もあります。

次のルールでは双方向のトラフィックを可能にします。ファイアウォールの受信トラフィックと送信トラフィックに対して別々のルールの指定が必要になる場合もあります。

各種ルールは、ネットワーク アドレス変換 (NAT) を使用するファイアウォールおよび NAT を使用しないファイアウォールに適用されます。

表 7-5. NAT 非対応ファイアウォールで IPsec ルールをサポートするための要件

Source	プロトコル	ポート	送信先	注
セキュリティ サーバ	ISAKMP	UDP 500	Horizon 接続サーバ	セキュリティ サーバは UDP ポート 500 を使用して IPsec セキュリティ をネゴシエートします。
セキュリティ サーバ	ESP	該当なし	Horizon 接続サーバ	ESP プロトコルは、IPsec で暗号化されたトラフィックをカプセル化します。 ESP 用のポートをルールの一部として指定する必要はありません。必要に応じて、ソースとターゲットの IP アドレスを指定して ルールの範囲を狭めることができます。

次のルールは、NAT を使用するファイアウォールに適用されます。

表 7-6. NAT 対応ファイアウォールで IPsec ルールをサポートするための要件

Source	プロトコル	ポート	送信先	注
セキュリティ サーバ	ISAKMP	UDP 500	Horizon 接続サーバ	セキュリティ サーバは UDP ポート 500 を使用して IPsec セキュリティ ネゴシエーションを開始します。
セキュリティ サーバ	NAT-T ISAKMP	UDP 4500	Horizon 接続サーバ	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。

Horizon 接続サーバをバックアップ構成で再インストールする

場合によっては、現在のバージョンの接続サーバ インスタンスを再インストールし、View LDAP 構成データを含むバックアップ LDIF ファイルをインポートすることにより既存の Horizon 7 構成を復元しなければならないことがあります。

たとえば、ビジネス継続性とディザスタ リカバリ (BC/DR) 計画の一環として、データセンターが機能を停止した場合に実行する手順を準備しておく必要があります。このような計画の最初の手順は、View LDAP 構成が別の場所にバックアップされるようにすることです。2 番目の手順では、この手順で説明するように、新しい場所に接続サーバをインストールし、バックアップ構成をインポートします。

既存の Horizon 7 構成で 2 番目のデータセンターをセットアップするときも、この手順を使用できます。あるいは、Horizon 7 の展開に含まれているのが 1 つの接続サーバ インスタンスのみで、そのサーバで問題が発生した場合も、この手順を使用できます。

複製されたグループ内に複数の接続サーバ インスタンスが存在し、1 つのインスタンスがダウンした場合は、この手順に従う必要はありません。接続サーバを複製されたインスタンスとして再インストールするだけです。インストール時に、接続情報を別の接続サーバ インスタンスに提供すると、Horizon 7 は View LDAP 構成を別のインスタンスから復元します。

前提条件

- 暗号化された LDIF ファイルに View LDAP 構成がバックアップされたことを確認します。
- vdmimport コマンドを使用して、LDIF バックアップ ファイルから View LDAP 構成を復元する方法を理解しておきます。
『Horizon 7 の管理』ドキュメントの「Horizon 7 構成データのバックアップと復元」を参照してください。
- 新しい接続サーバ インスタンスのインストール手順を理解しておきます。[新しい構成での Horizon 接続サーバのインストール](#)を参照してください。

手順

- 1 接続サーバを新しい構成でインストールします。
- 2 LDIF ファイルの暗号化を解除します。

例：

```
vdmimport -d -p mypassword
-f MyEncryptedexport.LDF > MyDecryptedexport.LDF
```

- 3 暗号化が解除された LDIF ファイルをインポートし、View LDAP 構成を復元します。

例：

```
vdmimport -f MyDecryptedexport.LDF
```

注： この段階では、Horizon 7 構成にはまだアクセスできません。クライアントは接続サーバにアクセスできないか、デスクトップに接続できません。

- 4 Windows の [プログラムの追加と削除] ユーティリティを使用して、コンピュータから接続サーバをアンインストールします。

AD LDS Instance VMwareVDMDS インスタンスと呼ばれる View LDAP 構成をアンインストールしないでください。[プログラムの追加と削除] ユーティリティを使用して、AD LDS Instance VMwareVDMDS インスタンスが Windows Server コンピュータから削除されていないことを確認できます。

- 5 接続サーバを再インストールします。

インストーラのプロンプトで、既存の View LDAP ディレクトリをそのまま使用します。

次のステップ

接続サーバ インスタンスを新しい構成でインストールした後に、接続サーバと Horizon 7 環境を自由に構成します。

Microsoft Windows インストーラ コマンド ライン オプション

Horizon 7 コンポーネントのサイレント インストールを実行するには、Microsoft Windows インストーラ (MSI) のコマンドライン オプションおよびプロパティを使用する必要があります。Horizon 7 コンポーネントのインストーラは MSI プログラムであり、MSI の標準機能を使用します。

MSI の詳細については、Microsoft の Web サイトを参照してください。MSI コマンドライン オプションについては、Microsoft Developer Network (MSDN) ライブラリの Web サイトを参照して、MSI コマンドライン オプションを検索してください。MSI コマンドラインの使用方法を確認するには、Horizon 7 コンポーネント コンピュータでコマンド プロンプトを開き、`msiexec /?` と入力します。

Horizon 7 コンポーネントのインストーラをサイレントに実行するには、まずブートストラップ プログラムを無効にします。このプログラムはインストーラを一時ディレクトリに展開し、対話型インストールを開始します。

コマンドラインで、インストーラのブートストラップ プログラムを制御するコマンドライン オプションを入力する必要があります。

表 7-7. Horizon 7 コンポーネントのブートストラップ プログラムのコマンドライン オプション

オプション	説明
<code>/s</code>	ブートストラップのスプラッシュ画面と抽出ダイアログを無効にします。これによって、対話的なダイアログは表示されません。 例: <code>VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s</code> <code>/s</code> オプションがサイレント インストールを実行するために必要です。
<code>/v"</code> <code>MSI_command_line_options"</code>	コマンドラインで入力する二重引用符で囲んだ文字列を MSI のオプションのセットとして解釈するようにインストーラに指示します。二重引用符でコマンドライン入力を囲む必要があります。 <code>/v</code> の後とコマンドラインの最後に二重引用符を配置します。 例: <code>VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /v"command_line_options"</code> スペースを含む文字列を解釈するように MSI インストーラに指示するには、その文字列を 2 組の二重引用符で囲みます。たとえば、スペースを含むインストール パス名で Horizon 7 コンポーネントをインストールするとします。 例: <code>VMware-viewconnectionserver-y.y.y-xxxxxx.exe /s /v"command_line_options INSTALLDIR=""d:\abc\my folder"""</code> この例では、MSI インストーラはインストール ディレクトリのパスをそのまま渡し、2 つのコマンドライン オプションとしての文字列の解釈を試行しません。コマンドライン全体を囲む二重引用符が末尾にあることに注意してください。 <code>/v"command_line_options"</code> オプションがサイレント インストールを実行するために必要です。

コマンドライン オプションおよび MSI プロパティ値を MSI インストーラ `msiexec.exe` に渡すことによってサイレント インストールの残りを制御します。MSI インストーラには、Horizon 7 コンポーネントのインストール コードが含まれています。このインストーラはコマンドラインに入力された値およびオプションを使用して、Horizon 7 コンポーネントに固有のインストールの選択内容およびセットアップ オプションを解釈します。

表 7-8. MSI コマンド ライン オプションおよび MSI プロパティ

MSI オプションまたはプロパティ	説明
/qn	<p>MSI インストーラにインストーラ ウィザード ページを表示しないように指示します。</p> <p>たとえば、次のように Horizon Agent のサイレント インストールを実行し、デフォルトのセットアップ オプションおよび機能のみを使用するようにすることができます。</p> <pre>VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /v"/qn"</pre> <p>あるいは、/qb を使用すると、インタラクティブではない自動インストールで基本的な進捗ダイアログ ボックスを表示できます。</p> <p>/qn または /qb オプションがサイレント インストールを実行するために必要です。</p> <p>追加の /q パラメータの詳細については、Microsoft デベロッパー センターの Web サイトを参照してください。</p>
INSTALLDIR	<p>Horizon 7 コンポーネントの代替インストール パスを指定します。</p> <p><i>INSTALLDIR=path</i> の形式で、インストール パスを指定します。Horizon 7 コンポーネントをデフォルト パスにインストールする場合は、この MSI プロパティを無視してかまいません。</p> <p>この MSI プロパティはオプションです。</p>
ADDLOCAL	<p>コンポーネント固有のインストール オプションを決定します。</p> <p>インタラクティブなインストールでは、Horizon 7 インストーラに設定または設定解除できるカスタムのセットアップ オプションが表示されます。サイレント インストールでは、ADDLOCAL プロパティを使用して、コマンド ラインでオプションを指定することで、個別のセットアップ オプションを選択的にインストールできます明示的に指定しないオプションはインストールされません。</p> <p>インタラクティブとサイレントの両方のインストールで、Horizon 7 インストーラは特定の機能を自動的にインストールします。ADDLOCAL を使用して、これらの非オプション機能をインストールするかどうかを制御できます。</p> <p>ADDLOCAL=ALL を入力して、デフォルトでインストールされるオプションやインストールを選択する必要のあるオプションを含む、インタラクティブなインストールでインストール可能なすべてのカスタム セットアップ オプションをインストールします。ただし、NGVC は対象外となります。NGVC と SVIAgent は相互に排他的です。</p> <p>次の例は Core、BlastProtocol、PCoIP、UnityTouch、VmVideo、PSG、およびゲスト OS 上でサポートされるすべての機能をインストールします。VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=ALL"</p> <p>ADDLOCAL プロパティを使用しない場合は、デフォルトでインストールされているカスタム設定オプションと、自動的にインストールされる機能がインストールされます。デフォルトでオフになっている（選択解除されている）カスタム設定オプションはインストールされません。</p> <p>次の例は Core、BlastProtocol、PCoIP、UnityTouch、VmVideo、PSG、およびゲスト OS 上でサポートされているデフォルトでオンのカスタム設定オプションをインストールします。VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /v"/qn"</p> <p>個別のセットアップ オプションを指定するには、カンマで区切ったセットアップ オプション名のリストを入力します。名前間にスペースを使用しないでください。ADDLOCAL=<i>value,value,value...</i> の形式を使用します。</p> <p>ADDLOCAL=<i>value,value,value...</i> のプロパティを使用するときは、Core を含める必要があります。</p> <p>次の例では、Core、BlastProtocol、PCoIP、UnityTouch、VmVideo、PSG、Instant Clone Agent、および仮想印刷機能とともに、Horizon Agent をインストールします。</p> <pre>VMware-Horizon-Agent-x86-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=Core,NGVC,ThinPrint"</pre> <p>前の例では、デフォルトでインタラクティブにインストールされる場合でも、他のコンポーネントはインストールしません。</p> <p>ADDLOCAL MSI プロパティはオプションです。</p>

表 7-8. MSI コマンドライン オプションおよび MSI プロパティ (続き)

MSI オプションまたはプロパティ	説明
REBOOT	REBOOT=ReallySuppress オプションを使用して、システム構成作業をシステムが再起動する前に完了することができます。 この MSI プロパティはオプションです。
/l*v <i>log_file</i>	ログ情報を詳細出力で指定したログ ファイルに書き込みます。 例: /l*v ""%TEMP%\vmmsi.log"" この例は、対話的なインストール中に生成されたログに類似する詳細なログ ファイルを生成します。 このオプションを使用して、インストールで一意的に適用するカスタム機能を記録できます。記録された情報を使用して、将来のサイレント インストールでインストール機能を指定できます。 /l*v オプションはオプションです。

MSI のコマンドライン オプションを使用した Horizon 7 コンポーネントのサイレント アンインストール

Horizon 7 コンポーネントは、Microsoft Windows Installer (MSI) のコマンドライン オプションを使用してアンインストールできます。

構文

```
msiexec.exe
/qb
/x
product_code
```

オプション

/qb オプションは、アンインストール進捗バーを表示します。アンインストール進捗バーが表示されないようにするには、/qb オプションを /qn オプションに置き換えます。

/x オプションを使用して、Horizon 7 コンポーネントをアンインストールします。

product_code 文字列は、MSI アンインストーラに対して Horizon 7 コンポーネント製品ファイルを特定します。*product_code* 文字列は、インストール時に作成される %TEMP%\vmmsi.log ファイル内の ProductCode を検索することによって確認できます。古いバージョンの Horizon 7 コンポーネントに適用する *product_code* 文字列を見つけるには、<http://kb.vmware.com/kb/2064845> にある VMware のナレッジベースの記事を参照してください。

MSI コマンドライン オプションの詳細については、[Microsoft Windows インストーラ コマンドライン オプション](#) を参照してください。

Horizon Agent のアンインストールの例

32 ビット版の Horizon Agent バージョン 7.0.2 をアンインストールするには、次のコマンドを入力します。

```
msiexec.exe /qb /x {B23352D8-AD44-4379-A56E-0E337F9C4036}
```

64 ビット版の Horizon Agent バージョン 7.0.2 をアンインストールするには、次のコマンドを入力します。

```
msiexec.exe /qb /x {53D6EE37-6B10-4963-81B1-8E2972A1DA4D}
```

コマンドに詳細ログを追加します。

```
/l*v "%TEMP%\vmmsi_uninstall.log"
```

/l オプションを明示的に渡さない場合、デフォルトの詳細ログ ファイルは %TEMP%\MSI`nnnn`.log となります。ここで、`nnnn` は 4 文字の GUID を指します。

Horizon Agent をアンインストールしても、いくつかのレジストリ キーが保持されます。これらのキーは、接続サーバの構成情報を保持するために必要であり、エージェントがアンインストールされてから再インストールされる場合でも、リモート デスクトップを接続サーバと引き続きペアリングできるようになります。これらのレジストリ キーを削除すると、ペアリングできなくなります。

次のレジストリ キーが保持されます。

- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMware Horizon View Certificates*
- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\Certificates*
- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\CRLs
- HKLM\SOFTWARE\Microsoft\SystemCertificates\VMwareView\CTLs
- HKLM\SOFTWARE\Policies\VMware, Inc.\VMware VDM*
- HKLM\SOFTWARE\Policies\VMware, Inc.\vRealize Operations for Horizon*
- HKLM\SOFTWARE\VMware, Inc.\VMware VDM*
- HKLM\SOFTWARE\Wow6432Node\Microsoft\SystemCertificates\VMware Horizon View Certificates*
- HKLM\SOFTWARE\Wow6432Node\Microsoft\SystemCertificates\VMwareView*
- HKLM\SOFTWARE\Wow6432Node\Policies\VMware, Inc.\VMware VDM*
- HKLM\SOFTWARE\Wow6432Node\Policies\VMware, Inc.\vRealize Operations for Horizon*
- HKLM\SOFTWARE\Wow6432Node\VMware, Inc.
- HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM

Horizon 7 Server 用の TLS 証明書 の設定

8

VMware では、接続サーバ インスタンス、セキュリティ サーバ、および View Composer サービス インスタンスに TLS 証明書認証を設定することを強く推奨しています。

接続サーバ インスタンス、セキュリティ サーバ、または View Composer インスタンスをインストールするとき、デフォルトの TLS サーバ証明書が生成されます。デフォルト証明書はテスト用に使用できます。

接続サーバ間の通信に使用される証明書や、Horizon Agent と接続サーバ インスタンス間の通信に使用される証明書は自動的に置換されるため、手動で置き換えることはできません。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。

重要： デフォルト証明書はできる限り早く置き換えてください。デフォルト証明書は、証明機関（CA）によって署名されていません。CA によって署名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がユーザーのサーバになりすましてトラフィックを傍受できる可能性があります。

この章には、次のトピックが含まれています。

- [Horizon 7 Server 用の TLS 証明書について](#)
- [TLS 証明書をセットアップするためのタスクの概要](#)
- [認証局 \(CA\) からの署名付き TLS 証明書の取得](#)
- [新しい TLS 証明書を使用するように Horizon 接続サーバ、セキュリティ サーバ、または View Composer を構成する](#)
- [ルート証明書と中間証明書を信頼するようにクライアント エンドポイントを構成する](#)
- [サーバ証明書での証明書失効チェックの構成](#)
- [新しい TLS 証明書を使用するために PCoIP Secure Gateway を構成する](#)
- [vCenter Server または View Composer 証明書を信頼するための Horizon Administrator の設定](#)
- [認証局 \(CA\) によって署名された TLS 証明書を使用する利点](#)
- [Horizon 接続サーバとセキュリティ サーバ証明書問題のトラブルシューティング](#)

Horizon 7 Server 用の TLS 証明書について

Horizon 7 サーバおよび関連コンポーネント用の TLS 証明書を構成する場合には、特定のガイドラインに従う必要があります。

Horizon 接続サーバとセキュリティ サーバ

サーバにクライアントを接続するには TLS が必要です。クライアント接続の接続サーバ インスタンス、セキュリティ サーバ、TLS 接続を終端させる中間サーバは、TLS サーバ証明書を要求します。

デフォルトでは、接続サーバまたはセキュリティ サーバをインストールすると、サーバ用の自己署名証明書が生成されます。ただし、次の場合は既存の証明書が使用されます。

- フレンドリ名 vdm を持つ有効な証明書が Windows 証明書ストアに存在する場合
- 以前のリリースから Horizon 7 にアップグレードし、有効なキーストア ファイルが Windows Server コンピュータで構成されている場合、インストールでキーと証明書が抽出され、Windows 証明書ストアにインポートされます。

vCenter Server と View Composer

vCenter Server と View Composer を本番環境の Horizon 7 に追加する前に、vCenter Server と View Composer が CA によって署名された証明書を使用していることを確認してください。

vCenter Server のデフォルト証明書の置換については、VMware のテクニカル ペーパー サイト (<http://www.vmware.com/resources/techresources/>) の「Replacing vCenter Server Certificates」を参照してください。

同じ Windows Server ホストに vCenter Server と View Composer をインストールする場合、同じ TLS 証明書を使用できますが、各コンポーネントで証明書を個別に構成する必要があります。

PCoIP Secure Gateway

業界または地域のセキュリティに関わる法律に準拠するため、PCoIP Secure Gateway (PSG) サービスによって生成されるデフォルトの TLS 証明書を認証局 (CA) によって署名される証明書に置き換えることができます。CA 署名付き証明書を使用するために PSG サービスを構成することを強く推奨します。特に、セキュリティ スキャナを使用して準拠テストにパスする必要がある展開です。[新しい TLS 証明書を使用するために PCoIP Secure Gateway を構成する](#)を参照してください。

Blast Secure Gateway

デフォルトでは、Blast Secure Gateway (BSG) は、BSG が動作している接続サーバ インスタンスまたはセキュリティ サーバ用に構成される TLS 証明書を使用します。CA 署名付き証明書を持つサーバのデフォルトの自己署名証明書を置き換えると、BSG も CA 署名付き証明書を使用します。

SAML 2.0 認証システム

VMware Identity Manager は SAML 2.0 認証子を使用して、セキュリティ ドメイン全体で Web ベースの認証と承認を実現します。Horizon 7 が VMware Identity Manager に認証を委任するようにする場合は、Horizon 7 を構成して、VMware Identity Manager からの SAML 2.0 認証セッションを受け入れるようにすることができます。VMware Identity Manager が Horizon 7 をサポートするように構成されている場合、VMware Identity Manager ユーザーは、Horizon ユーザー ポータルのデスクトップ アイコンを選択してリモート デスクトップに接続することができます。

Horizon Administrator では、SAML 2.0 認証システムを View 接続サーバ インスタンスで使用するように構成できます。

Horizon Administrator に SAML 2.0 認証システムを追加する前に、SAML 2.0 認証システムが CA によって署名された証明書を使用していることを確認します。

その他のガイドライン

認証局 (CA) によって署名された TLS 証明書の要求と使用に関する一般的な情報については、[認証局 \(CA\) によって署名された TLS 証明書を使用する利点](#)を参照してください。

クライアント エンドポイントが接続サーバ インスタンスまたはセキュリティ サーバに接続すると、サーバの TLS サーバ証明書と信頼チェーン内の任意の中間証明書が提示されます。サーバ証明書を信頼するには、クライアント システムに、CA が署名したルート証明書がインストールされている必要があります。

接続サーバが vCenter Server および View Composer と通信するとき、接続サーバには、TLS サーバ証明書とこれらのサーバからの中間証明書が提示されます。vCenter Server と View Composer Server を信頼するには、接続サーバ コンピュータに、CA が署名したルート証明書がインストールされている必要があります。

同様に、接続サーバ用に SAML 2.0 認証システムが構成されている場合は、接続サーバ コンピュータに、SAML 2.0 サーバ証明書用の CA が署名したルート証明書がインストールされている必要があります。

TLS 証明書をセットアップするためのタスクの概要

Horizon 7 サーバに対して TLS サーバ証明書を設定するには、高度な複数のタスクを実行する必要があります。

複製された接続サーバ インスタンスのポッドでは、ポッド内のすべてのインスタンスに対してこれらのタスクを実行する必要があります。

これらのタスクを実行する手順は、この概要の後のトピックで説明します。

- 1 認証局 (CA) から新しい署名付き TLS 証明書を取得する必要があるかどうかを判断します。

組織がすでに有効な TLS サーバ証明書を所有している場合、接続サーバ、セキュリティ サーバ、View Composer で提供されるデフォルトの TLS サーバ証明書をその証明書に置き換えることができます。既存の証明書を使用するには、それに対応するプライベート キーも必要です。

現在の状況	アクション
有効な TLS サーバ証明書が組織から提供されている。	直接、手順 2 に進みます。
TLS サーバ証明書がない。	認証局 (CA) から署名された TLS サーバ証明書を入手します。

- 2 Horizon 7 サーバ ホスト上の Windows ローカル コンピュータの証明書ストアに TLS 証明書をインポートします。
- 3 接続サーバ インスタンスとセキュリティ サーバの場合は、証明書のフレンドリ名を **vdn** に変更します。
フレンドリ名 **vdn** を、各 Horizon 7 サーバ ホストの 1 つの証明書の上に割り当てます。
- 4 接続サーバ コンピュータ上で、ルート証明書が Windows Server ホストに信頼されていない場合は、ルート証明書を Windows ローカル コンピュータの証明書ストアにインポートします。

さらに、接続サーバ インスタンスがセキュリティ サーバ、View Composer、vCenter Server ホスト用に構成された TLS サーバ証明書のルート証明書を信頼していない場合にも、これらのルート証明書をインポートする必要があります。これらの手順は、接続サーバ インスタンスでのみ実行します。View Composer、vCenter Server、またはセキュリティ サーバ ホストにルート証明書をインポートする必要はありません。
- 5 サーバ証明書が中間 CA によって署名されている場合は、中間証明書を Windows ローカル コンピュータの証明書ストアにインポートします。

クライアント構成を簡素化するには、証明書チェーン全体を Windows ローカル コンピュータの証明書ストアにインポートします。中間証明書が Horizon 7 サーバから欠落している場合、クライアントおよび Horizon Administrator を起動するコンピュータ用に中間証明書を構成する必要があります。
- 6 View Composer インスタンスの場合は、次の手順の 1 つを実行します。
 - View Composer をインストールする前に、Windows ローカル コンピュータの証明書ストアに証明書をインポートした場合は、View Composer のインストール中にこの証明書を選択できます。
 - View Composer のインストール後に、既存の証明書またはデフォルトの自己署名証明書を新しい証明書と置換する場合は、SviConfig ReplaceCertificate ユーティリティを使用して、新しい証明書を View Composer が使用するポートにバインドします。
- 7 CA が不明な場合は、ルート証明書および中間証明書を信頼するようにクライアントを構成します。

さらに、Horizon Administrator を起動するコンピュータがルート証明書および中間証明書を信頼するようにします。
- 8 証明書失効チェックを再構成するかどうかを決定します。

接続サーバは、Horizon 7 サーバ、View Composer、および vCenter Server 上で証明書失効チェックを実行します。CA によって署名された大部分の証明書には、証明書失効情報が含まれています。CA にこの情報が含まれていない場合は、証明書失効チェックを実行しないようにサーバを構成できます。

SAML 認証システムが接続サーバ インスタンスで使用されるように構成されている場合は、接続サーバは SAML サーバ証明書上でも証明書失効チェックを実行します。

認証局 (CA) からの署名付き TLS 証明書の取得

所属する組織から TLS サーバ証明書が提供されていない場合は、認証局 (CA) によって署名された新しい証明書を要求する必要があります。

いくつかの方法を使用して、新しい署名付き証明書を取得できます。たとえば、Microsoft certreq ユーティリティを使用して、証明書署名要求 (CSR) を生成し、CA に証明書要求を送信できます。

certreq でこの操作を行う方法については、『Horizon 7 の TLS 証明書設定のシナリオ』ドキュメントを参照してください。

テスト用として、信頼されていないルートによる一時的な証明書を多数の CA から無償で入手できます。

重要： 認証局 (CA) から署名入り TLS 証明書を取得するとき、特定のルールと指針に従う必要があります。

- コンピュータ上で証明書要求を作成するときは、必ずプライベート キーも作成するようにします。TLS サーバ証明書を取得し、それを Windows ローカル コンピュータの証明書ストアにインポートするときは、証明書に対応するプライベート キーが必要です。
- VMware セキュリティ推奨事項に準拠するために、クライアント デバイスがホストへの接続に使用する完全修飾ドメイン名 (FQDN) を使用します。内部ドメインの範囲内の通信にも、シンプルなサーバ名や IP アドレスは使用しないでください。
- Windows Server 2008 enterprise CA 以降のみと互換性のある証明書テンプレートを使用して、サーバの証明書を作成しないでください。
- 1024 未満の KeyLength 値を使用して、サーバ用の証明書を作成しないでください。クライアント エンドポイントは、1024 未満の KeyLength 値を使用して作成されたサーバ用の証明書を検証せず、クライアントはサーバとの接続に失敗します。接続サーバによって実行される証明書検証も失敗し、影響を受けるサーバが Horizon Administrator のダッシュボードで赤色に表示されます。

証明書取得に関する一般的な情報については、MMC への証明書スナップインにある Microsoft オンライン ヘルプを参照してください。証明書スナップインがコンピュータにインストールされていない場合は、[証明書スナップインを MMC に追加する](#)を参照してください。

Windows ドメインまたは Enterprise CA から署名証明書を取得する

Windows ドメインまたは Enterprise CA から署名証明書を取得するには、Windows 証明書ストアの Windows Certificate Enrollment ウィザードを使用できます。

この証明書要求の方法は、コンピュータ間の通信が内部ドメイン内に限られる場合に適しています。たとえば、Windows ドメイン CA からの署名証明書の取得は、サーバ間通信に適しています。

クライアントが外部ネットワークから Horizon 7 サーバに接続する場合、信頼できるサードパーティ認証局 (CA) により署名された TLS サーバ証明書を要求します。

前提条件

- クライアント デバイスがホストへの接続に使用する完全修飾ドメイン名 (FQDN) を決定します。
VMware のセキュリティ推奨事項に準拠するために FQDN を使用し、内部ドメインの範囲内であってもシンプルなサーバ名または IP アドレスは使用しません。
- 証明書のスナップインが MMC に追加されたことを確認します。[証明書スナップインを MMC に追加する](#)を参照してください。
- コンピュータまたはサービスに発行できる証明書を要求する適切な認証情報があることを確認します。

手順

- 1 Windows Server ホストの [MMC] ウィンドウで、[証明書 (ローカル コンピュータ)] ノードを展開して [個人] フォルダを選択します。
- 2 [アクション] メニューから、[すべてのタスク] - [新規証明の要求] に移動し、[証明書登録] ウィザードを表示します。
- 3 証明書登録ポリシーを選択します。
- 4 要求する証明書のタイプを選択し、[プライベート キーをエクスポート可能にする] オプションを選択して、[登録] をクリックします。
- 5 [終了] をクリックします。

結果

新しい署名の証明書が Windows 証明書ストアの [個人] - [証明書] フォルダに追加されます。

次のステップ

- サーバ証明書および証明書チェーンが Windows 証明書ストアにインポートされたことを確認します。
- 接続サーバ インスタンスまたはセキュリティ サーバの場合は、証明書のフレンドリ名を **vdm** に変更します。[証明書のわかりやすい名前を変更する](#)を参照してください。
- View Composer Server の場合、新しい証明書を View Composer により使用されるポートにバインドします。[View Composer が使用するポートに新規 TLS 証明書をバインドする](#)を参照してください。

新しい TLS 証明書を使用するように Horizon 接続サーバ、セキュリティ サーバ、または View Composer を構成する

TLS 証明書を使用するために接続サーバ インスタンス、セキュリティ サーバ、または View Composer インスタンスを構成するには、サーバ証明書と証明書チェーン全体を接続サーバ、セキュリティ サーバ、または View Composer ホストの Windows ローカル コンピュータ証明書ストアにインポートする必要があります。

複製された接続サーバ インスタンスのポッドでは、ポッド内のすべてのインスタンスでサーバ証明書と証明書チェーンをインポートする必要があります。

デフォルトでは、Blast Secure Gateway (BSG) は、BSG が動作している接続サーバ インスタンスまたはセキュリティ サーバ用に構成される TLS 証明書を使用します。デフォルトの CA 署名付き証明書のある View Server 用の自己署名証明書を置き換えると、BSG も CA 署名付き証明書を使用します。

重要： 証明書を使用するために接続サーバまたはセキュリティ サーバを構成するには、証明書のフレンドリ名を **vdm** に変更する必要があります。また、証明書にはプライベート キーが必要です。

View Composer をインストールした後に、既存の証明書またはデフォルトの自己署名証明書を新しい証明書と置換える場合には、SviConfig ReplaceCertificate ユーティリティを実行し、View Composer で使用されるポートに新しい証明書をバインドする必要があります。

手順

1 証明書スナップインを MMC に追加する

証明書を Windows 証明書ストアに追加する前に、Horizon 7 サーバがインストールされる Windows Server ホストの Microsoft 管理コンソール (MMC) に証明書スナップインを追加する必要があります。

2 署名付きサーバ証明書を Windows 証明書ストアにインポートする

TLS サーバ証明書を、接続サーバ インスタンスまたはセキュリティ サーバ サービスがインストールされている Windows Server ホスト上の Windows ローカル コンピュータの証明書ストアにインポートする必要があります。

3 証明書のわかりやすい名前を変更する

TLS 証明書を認識して使用するように、接続サーバ インスタンスまたはセキュリティ サーバを構成するには、証明書のフレンドリ名を **vdm** に変更する必要があります。

4 ルート証明書と中間証明書を Windows 証明書ストアにインポートする

接続サーバがインストールされている Windows Server ホストが署名された TLS サーバ証明書のルート証明書を信頼していない場合、ルート証明書を Windows ローカル コンピュータの証明書ストアにインポートする必要があります。さらに、接続サーバ ホストがセキュリティ サーバ、View Composer、vCenter Server ホスト用に構成された TLS サーバ証明書のルート証明書を信頼していない場合にも、これらのルート証明書をインポートする必要があります。

5 View Composer が使用するポートに新規 TLS 証明書をバインドする

View Composer をインストールした後に新しい TLS 証明書を構成する場合、View Composer が使用するポートにバインドされた証明書と置き換えるために SviConfig ReplaceCertificate ユーティリティを実行する必要があります。このユーティリティは既存の証明書のバインドを解除し、新しい証明書をポートにバインドします。

証明書スナップインを MMC に追加する

証明書を Windows 証明書ストアに追加する前に、Horizon 7 サーバがインストールされる Windows Server ホストの Microsoft 管理コンソール (MMC) に証明書スナップインを追加する必要があります。

前提条件

Horizon 7 サーバがインストールされる Windows Server コンピュータで MMC と証明書スナップインが使用可能であることを確認します。

手順

- 1 Windows Server コンピュータで、[スタート] をクリックし、**mmc.exe** と入力します。
- 2 [MMC] ウィンドウで、[ファイル] - [スナップインの追加と削除] に移動します。
- 3 [スナップインの追加と削除] ウィンドウで、[証明書] を選択し、[追加] をクリックします。
- 4 [証明書スナップイン] ウィンドウで、[コンピュータ アカウント] を選択し、[次へ] をクリックし、[ローカル コンピュータ] を選択し、[終了] をクリックします。
- 5 [スナップインの追加と削除] ウィンドウで、[OK] をクリックします。

次のステップ

TLS サーバ証明書を Windows 証明書ストアにインポートします。

署名付きサーバ証明書を Windows 証明書ストアにインポートする

TLS サーバ証明書を、接続サーバ インスタンスまたはセキュリティ サーバ サービスがインストールされている Windows Server ホスト上の Windows ローカル コンピュータの証明書ストアにインポートする必要があります。

このタスクは、View Composer サービスがインストールされている Windows Server ホストでも実行する必要があります。

証明書のファイル形式によって、キーストア ファイルに含まれる証明書チェーン全体が Windows ローカル コンピュータの証明書ストアにインポートされる場合があります。たとえば、サーバ証明書、中間証明書、ルート証明書がインポートされる場合があります。

その他のタイプの証明書ファイルについては、サーバ証明書のみが Windows ローカル コンピュータの証明書ストアにインポートされます。この場合、別の手順を行い、ルート証明書と証明書チェーン内の中間証明書をインポートする必要があります。

証明書の詳細については、MMC に対する証明書のスナップインで利用できる Microsoft オンライン ヘルプを参照してください。

注： TLS 接続を中間サーバにオフロードする場合、同じ TLS サーバ証明書を中間サーバとオフロードされる Horizon 7 Server の両方にインポートする必要があります。詳細については、『Horizon 7 の管理』ドキュメントの「TLS 接続を中間サーバにオフロードする」を参照してください。

前提条件

証明書のスナップインが MMC に追加されたことを確認します。[証明書スナップインを MMC に追加する](#)を参照してください。

手順

- 1 Windows Server ホストの MMC ウィンドウで、[証明書 (ローカル コンピュータ)] ノードを展開して [個人] フォルダを選択します。
- 2 [操作] ペインで、[追加の操作] - [すべてのタスク] - [インポート] の順に移動します。
- 3 [Certificate Import (証明書のインポート)] ウィザードで、[次へ] をクリックして証明書が格納されている場所を参照します。

- 証明書ファイルを選択して [開く] をクリックします。

証明書ファイルのタイプを表示するには、[ファイル名] ドロップダウン メニューからそのファイル形式を選択できます。

- 証明書ファイルに含まれるプライベート キーのパスワードを入力します。

- [この鍵をエクスポート可能にマークする] を選択します。

- [すべての拡張プロパティを含める] を選択します。

- [次へ] をクリックして [終了] をクリックします。

新しい証明書が [証明書 (ローカル コンピュータ)] - [個人] - [証明書] フォルダに表示されます。

- 新しい証明書にプライベート キーが含まれていることを確認します。

- [証明書 (ローカル コンピュータ)] - [個人] - [証明書] フォルダで、新しい証明書をダブルクリックします。
- [証明書情報] ダイアログ ボックスの [全般] タブで、「この証明書に対応するプライベート キーがあります。」というメッセージが表示されることを確認します。

次のステップ

証明書のわかりやすい名前を **vdm** に変更します。

証明書のわかりやすい名前を変更する

TLS 証明書を認識して使用するように、接続サーバ インスタンスまたはセキュリティ サーバを構成するには、証明書のフレンドリ名を **vdm** に変更する必要があります。

View Composer が使用している TLS 証明書のわかりやすい名前を変更する必要はありません。

前提条件

サーバ証明書が Windows 証明書ストアの[証明書 (ローカル コンピュータ)] - [個人] - [証明書] フォルダにインポートされていることを確認します。署名付きサーバ証明書を [Windows 証明書ストアにインポートする](#)を参照してください。

手順

- Windows Server ホストの MMC ウィンドウで、[証明書 (ローカル コンピュータ)] ノードを展開して [個人] - [証明書] フォルダを選択します。
- Horizon 7 サーバ ホストに発行される証明書を右クリックし、[プロパティ] をクリックします。
- [全般] タブで、[わかりやすい名前] のテキストを削除し、**vdm** と入力します。
- [適用]、[OK] の順にクリックします。
- [個人] - [証明書] フォルダのその他のサーバ証明書で、フレンドリ名が **vdm** になっていないことを確認します。
 - その他のサーバ証明書がある場合はそれを見つけて証明書を右クリックし、[個人] をクリックします。
 - 証明書のわかりやすい名前が **vdm** である場合は、その名前を削除し、[適用] をクリックして、[OK] をクリックします。

次のステップ

ルート証明書と中間証明書を Windows ローカル コンピュータの証明書ストアにインポートします。

チェーン内のすべての証明書をインポートした後で、接続サーバ サービスまたはセキュリティ サーバ サービスを再起動して変更を反映する必要があります。

ルート証明書と中間証明書を Windows 証明書ストアにインポートする

接続サーバがインストールされている Windows Server ホストが署名された TLS サーバ証明書のルート証明書を信頼していない場合、ルート証明書を Windows ローカル コンピュータの証明書ストアにインポートする必要があります。さらに、接続サーバ ホストがセキュリティ サーバ、View Composer、vCenter Server ホスト用に構成された TLS サーバ証明書のルート証明書を信頼していない場合にも、これらのルート証明書をインポートする必要があります。

接続サーバ、セキュリティ サーバ、View Composer、および vCenter Server の証明書が、接続サーバ ホストから信頼されている既知のルート CA によって署名されていて、証明書チェーン内に中間証明書がない場合、このタスクをスキップできます。一般的に使用されている証明機関は、ホストから信頼される可能性が高くなります。

信頼されていないルート証明書は、ポッド内の複製された接続サーバ インスタンスすべてにインポートする必要があります。

注： ルート証明書を View Composer、vCenter Server、またはセキュリティ サーバ ホストにインポートする必要はありません。

サーバ証明書が中間 CA によって署名されている場合、証明書チェーンのそれぞれの中間証明書もインポートする必要があります。クライアント構成を簡素化するために、中間チェーン全体を接続サーバ ホストだけでなくセキュリティ サーバ、View Composer、vCenter Server ホストにもインポートします。中間証明書が接続サーバまたはセキュリティ サーバ ホストから欠落している場合、クライアントおよび Horizon Administrator を起動するコンピュータ用にこれらを構成する必要があります。中間証明書が View Composer または vCenter Server ホストから欠落している場合、各接続サーバ インスタンス用にこれらを構成する必要があります。

証明書チェーン全体が Windows ローカル コンピュータの証明書ストアにインポートされていることをすでに確認していれば、このタスクはスキップできます。

注： SAML 認証子が接続サーバ インスタンスによって使用されるように構成されている場合、同じガイドラインが SAML 2.0 認証子についても適用されます。接続サーバ ホストが SAML 認証子用に構成されたルート証明書を信頼していない場合、または SAML サーバ証明書が中間 CA によって署名されている場合、証明書チェーンが Windows ローカル コンピュータの証明書ストアにインポートされていることを確認する必要があります。

手順

- 1 Windows Server ホストの MMC コンソールで、[証明書 (ローカル コンピュータ)] ノードを展開して、[信頼されたルート証明機関] - [証明書] フォルダに移動します。
 - ルート証明書がこのフォルダにあり、証明書チェーン内に中間証明書がない場合は、手順 7 までスキップします。
 - ルート証明書がこのフォルダになければ、手順 2 に進みます。

- 2 [信頼されたルート証明機関] - [証明書] フォルダを右クリックし、[すべてのタスク] - [インポート] をクリックします。
- 3 [証明書のインポート] ウィザードで、[次へ]をクリックしてルート CA 証明書が保存されている場所を参照します。
- 4 ルート CA 証明書ファイルを選択し、[開く] をクリックします。
- 5 [次へ] をクリックし、[次へ] をクリックし、そして [終了] をクリックします。
- 6 サーバ証明書が中間 CA によって署名されていた場合、証明書チェーンのすべての中間証明書を Windows ローカル コンピュータ証明書ストアにインポートします。
 - a [証明書 (ローカル コンピュータ)] - [中間証明機関] - [証明書] フォルダに移動します。
 - b インポートする必要がある各中間証明書で手順 3 から 6 を繰り返します。
- 7 変更を反映するため、接続サーバ サービス、セキュリティ サーバ サービス、View Composer サービス、または vCenter Server サービスを再起動してください。

View Composer が使用するポートに新規 TLS 証明書をバインドする

View Composer をインストールした後に新しい TLS 証明書を構成する場合、View Composer が使用するポートにバインドされた証明書と置き換えるために SviConfig ReplaceCertificate ユーティリティを実行する必要があります。このユーティリティは既存の証明書のバインドを解除し、新しい証明書をポートにバインドします。

View Composer をインストールする前に Windows Server コンピュータに新しい証明書をインストールする場合、SviConfig ReplaceCertificate ユーティリティを実行する必要はありません。View Composer インストールの実行時、デフォルトの自己署名の証明書ではなく CA によって署名された証明書を選択できます。インストールの際、選択された証明書は View Composer が使用するポートにバインドされます。

既存の証明書またはデフォルトの自己署名付き証明書を新しい証明書に置き換える場合、SviConfig ReplaceCertificate ユーティリティを使用する必要があります。

前提条件

View Composer がインストールされる Windows Server コンピュータの Windows ローカル コンピュータ証明書ストアに新しい証明書がインポートされたことを確認します。

手順

- 1 View Composer サービスを停止します。
- 2 View Composer がインストールされている Windows Server ホストでコマンド プロンプトを開きます。
- 3 SviConfig 実行可能ファイルに移動します。

このファイルは、View Composer アプリケーションと同じ場所にあります。デフォルト パスは C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe です。

4 SviConfig ReplaceCertificate コマンドを入力します。

例：

```
sviconfig -operation=ReplaceCertificate
          -delete=false
```

`-delete` は、置き換えられる証明書に適用される必須のパラメータです。古い証明書を Windows ローカル コンピュータ証明書ストアから削除する場合は `-delete=true` を、古い証明書を Windows 証明書ストアに保持する場合は `-delete=false` を指定する必要があります。

このユーティリティでは、Windows ローカル コンピュータ証明書ストアで使用可能な TLS 証明書の番号付きリストが表示されます。

5 証明書を選択するには、証明書の番号を入力し、Enter キーを押します。

6 View Composer サービスを再起動して変更を有効にします。

例：SviConfig ReplaceCertificate

次の例では、View Composer ポートにバインドされる証明書が置換されます。

```
sviconfig -operation=ReplaceCertificate
          -delete=false
```

ルート証明書と中間証明書を信頼するようにクライアント エンドポイントを構成する

Horizon 7 Server 証明書が、クライアント コンピュータと Horizon Administrator にアクセスするクライアント コンピュータによって信頼されていない CA によって署名されている場合、ドメイン内のすべての Windows クライアント システムをルート証明書と中間証明書を信頼するように構成できます。そのためには、Active Directory の [信頼されたルート証明機関] グループ ポリシーにルート証明書のパブリック キーを追加して、ルート証明書を Enterprise NTAAuth ストアに追加する必要があります。

たとえば、ユーザーの組織が内部の証明書サービスを使用している場合には、これらの手順を実行する必要がある場合があります。

Windows ドメイン コントローラがルート CA として機能する場合、または証明書が既知の CA によって署名されている場合は、この手順を実行する必要はありません。既知の CA については、オペレーティング システムのベンダーにより、クライアント システムにルート証明書があらかじめインストールされます。

知名度がほとんどない中間 CA によってサーバ証明書が署名されている場合には、中間証明書を Active Directory の [中間証明書機関] グループ ポリシーに追加する必要があります。

Windows 以外のオペレーティング システムを使用するクライアント デバイスについては、ユーザーがインストール可能なルート証明書と中間証明書の配布に関する次の手順を参照してください。

- Horizon Client for Mac については、[ルート証明書と中間証明書を信頼するように Horizon Client for Mac を構成](#)を参照してください。
- Horizon Client for iOS については、[ルート証明書と中間証明書を信頼するように Horizon Client for iOS を構成する](#)を参照してください。

- Horizon Client for Android については、『Android 3.0 ユーザー ガイド』などの Google Web サイトにあるマニュアルを参照してください。
- Horizon Client for Linux については、Ubuntu のマニュアルを参照してください。

前提条件

サーバ証明書が 1024 以上の KeyLength 値で生成されていることを確認します。クライアント エンドポイントは、1024 未満の KeyLength で生成されたサーバ上の証明書は検証しません。この場合、クライアントはサーバへの接続に失敗します。

手順

- 1 Active Directory サーバで、certutil コマンドを使用して、証明書を Enterprise NTAUTH ストアに発行します。

例 : `certutil -dspublish -f ルート CA 証明書へのパス NTAUTHCA`

- 2 Active Directory サーバで、Group Policy Management プラグインに移動します。

Active Directory のバージョン	ナビゲーション パス
Windows 2003	a [スタート] - [すべてのプログラム] - [管理ツール] - [Active Directory ユーザーとコンピュータ] の順に選択します。 b ドメインを右クリックして、[プロパティ] をクリックします。 c [グループ ポリシ] タブで、[開く] をクリックして Group Policy Management プラグインを開きます。 d [既定のドメイン ポリシー] を右クリックし、[編集] をクリックします。
Windows 2008	a [スタート] - [管理ツール] - [グループ ポリシーの管理] の順に選択します。 b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。
Windows 2012 R2	a [スタート] - [管理ツール] - [グループ ポリシーの管理] の順に選択します。 b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。
Windows 2016	a [スタート] - [管理ツール] - [グループ ポリシーの管理] の順に選択します。 b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。

- 3 [コンピュータの構成] セクションを展開し、[Windows 設定] - [セキュリティ設定] - [パブリック キーポリシー] に移動します。
- 4 証明書をインポートします。

オプション	説明
ルート証明書	a [信頼されたルート証明機関] を右クリックして、[インポート] を選択します。 b ウィザードの指示に従ってルート証明書 (rootCA.cer など) をインポートし、[OK] をクリックします。
中間証明書	a [中間証明機関] を右クリックして、[インポート] を選択します。 b ウィザードの指示に従って中間証明書 (intermediateCA.cer など) をインポートし、[OK] をクリックします。

5 [Group Policy (グループ ポリシー)] ウィンドウを閉じます。

結果

これで、ドメイン内のすべてのシステムの信頼されたルート証明機関のストアと中間証明機関のストアに、ルート証明書と中間証明書を信頼できるようにする証明書情報が追加されました。

ルート証明書と中間証明書を信頼するように Horizon Client for Mac を構成

Horizon Client for Mac を実行するコンピュータによって信頼されていない CA によってサーバ証明書が署名されている場合、このコンピュータをルート証明書と中間証明書を信頼するように構成できます。信頼チェーンにあるルート証明書とすべての中間証明書をクライアント コンピュータに配布する必要があります。

手順

- 1 ルート証明書と中間証明書を Horizon Client for Mac が実行しているコンピュータに配布します。

- 2 Mac コンピュータでルート証明書を開きます。

証明書によって、「今後 CA *name* によって署名される証明書をお使いのコンピュータで信頼しますか?」というメッセージが表示されます。

- 3 [常に信頼する] をクリック

- 4 ユーザー パスワードを入力します。

- 5 信頼チェーンにあるすべての中間証明書で、手順 2 から 4 を繰り返し実行します。

ルート証明書と中間証明書を信頼するように Horizon Client for iOS を構成する

サーバ証明書が Horizon Client for iOS を実行する iPad と iPhone に信頼されていない認証局 (CA) によって署名されている場合、デバイスをルート証明書と中間証明書を信頼するように構成できます。デバイスにはルート証明書と信頼チェーン内のすべての中間証明書を配布する必要があります。

手順

- 1 ルート証明書と中間証明書を電子メールの添付ファイルとして iPad に送信します。

- 2 ルート証明書の電子メール添付ファイルを開き、[インストール] を選択します。

証明書により次のメッセージが表示されます。

検証できないプロファイル。Certificate name の信頼性は検証できません。このプロファイルをインストールすると iPad の設定が変更されます。ルート証明書。Certificate name の証明書をインストールすると、iPad で信頼される証明書のリストに追加されます。

- 3 [インストール] を再度選択します。

- 4 信頼チェーン内のすべての中間証明書について手順 2 と 3 を繰り返します。

サーバ証明書での証明書失効チェックの構成

それぞれの接続サーバ インスタンスは、自身の証明書とペアにされたセキュリティ サーバの証明書について証明書失効チェックを実行します。それぞれのインスタンスは、接続を確立すると、必ず vCenter と View Composer サーバの証明書もチェックします。デフォルトでは、ルート証明書を除いてチェーン内のすべての証明書がチェックされます。ただし、このデフォルトは変更できます。

SAML 2.0 認証子が接続サーバ インスタンスによって使用されるように構成されていると、接続サーバは SAML 2.0 サーバ証明書についても証明書失効チェックを実行します。

Horizon 7 は、証明書失効リスト (CRL) や Online Certificate Status Protocol (OCSP) などのさまざまな証明書失効チェックの方式をサポートしています。CRL は、証明書を発行した CA によって公開される、失効した証明書のリストです。OCSP は、X.509 証明書の失効ステータスを取得するために使用される証明書検証プロトコルです。

CRL を使用すると、失効した証明書のリストがたいてい証明書に指定されている証明書配布ポイント (DP) からダウンロードされます。サーバは証明書に指定された CRL DP URL に定期的にアクセスし、リストをダウンロードして、サーバ証明書が失効していないかどうかを判別します。OCSP を使用すると、サーバは証明書の失効ステータスを判別するように OCSP レスポンダに要求を送信します。

サーバ証明書を他社の証明機関 (CA) から取得する場合、証明書には、たとえば CRL DP URL や OCSP レスポンダの URL を含む、失効ステータスを判別できる 1 つ以上の方式が含まれています。独自の CA があり、証明書を生成したにもかかわらず証明書に失効情報を含んでいないと、証明書失効チェックは失敗します。このような証明書の失効情報の例には、たとえば、CRL をホストするサーバ上の Web ベースの CRL DP の URL などが含まれます。

独自の CA があるにもかかわらず証明書に証明書失効情報が含まれていない、または含めることができない場合、証明書の失効をチェックしないか、チェーン内の特定の証明書のみチェックすることを選択できます。サーバで、Windows レジストリ エディタを使用して、HKLM\Software\VMware, Inc.\VMware VDM\Security の下で文字列 (REG_SZ) の値 [CertificateRevocationCheckType] を作成し、この値を次のデータ値のいずれかに設定できます。

値	説明
1	証明書失効チェックを実行しない。
2	サーバ証明書のみチェックする。チェーン内のその他の証明書についてはチェックしない。
3	チェーン内のすべての証明書をチェックする。
4	(デフォルト) ルート証明書を除くすべての証明書をチェックします。

このレジストリ値が設定されていない場合、または設定された値が有効でない（つまり、値が 1、2、3、または 4 でない）場合、ルート証明書を除くすべての証明書がチェックされます。このレジストリ値は、失効チェックを変更する予定のそれぞれのサーバで設定します。この値を設定した後でシステムを再起動する必要はありません。

注： 組織でインターネット アクセスにプロキシ設定を使用している場合、接続サーバ コンピュータでプロキシ設定を使用し、証明書失効チェックが安全なクライアント接続に使用されるセキュリティ サーバまたは接続サーバに対して実行されるように構成する必要がある場合があります。接続サーバ インスタンスがインターネットにアクセスできない場合、証明書失効チェックが失敗し、接続サーバ インスタンスまたはペアにされたセキュリティ サーバが Horizon Administrator ダッシュボードで赤色で表示される場合があります。この問題を解決するには、『Horizon 7 の管理』ドキュメントの「セキュリティ サーバ証明書失効チェックのトラブルシューティング」を参照してください。

新しい TLS 証明書を使用するために PCoIP Secure Gateway を構成する

業界または地域のセキュリティに関わる法律に準拠するため、PCoIP Secure Gateway (PSG) サービスによって生成されるデフォルトの TLS 証明書を認証局 (CA) によって署名される証明書に置き換えることができます。

Horizon 7 で、PSG サービスは、デフォルトの自己署名された TLS 証明書をサービスの開始時に作成します。PSG サービスは、自己署名証明書を、PSG に接続する Horizon Client 2.0 (または Horizon Client 5.2 for Windows) 以降のリリースが動作しているクライアントに示します。

また PSG は、PSG に接続する旧クライアントまたは以前のリリースが動作するクライアントに示されるデフォルトのレガシー TLS 証明書も提供します。

デフォルトの証明書は、クライアント エンドポイントから PSG への安全な接続を提供し、Horizon Administrator でさらに構成を行う必要はありません。ただし、CA 署名付き証明書を使用するために PSG サービスを構成することを強く推奨します。特に、セキュリティ スキャナを使用して準拠テストにパスする必要がある展開です。

これは必要ではありませんが、デフォルトの PSG 証明書を認証局 (CA) 署名付き証明書で置き換える前に、サーバ用の新しく認証局 (CA) 署名付き TLS 証明書を構成することになります。実行する手順では、PSG が動作しているサーバ用の Windows 証明書ストアに CA 署名付き証明書をすでにインポートしていることを想定しています。

注： 準拠テストでセキュリティ スキャナを使用している場合は、まずサーバと同じ証明書を使用するように PSG を設定し、PSG ポートの前に View ポートをスキャンすることができます。View ポートのスキャン中に発生する信頼または検証問題を解決し、これらの問題が PSG ポートおよび証明書のテストを無効にしないことを保証できます。次に、PSG に一意の証明書を構成して、別のスキャンを実行できます。

手順

1 PSG 証明書のサブジェクト名に一致するサーバ名を確認する

接続サーバ インスタンスまたはセキュリティ サーバがインストールされるとき、インストーラはコンピュータの FQDN を含む値でレジストリ設定を作成します。この値が、PSG ポートに到達するためにセキュリティ スキャナが使用する URL のサーバ名の部分と一致することを確認する必要があります。このサーバ名は、PSG 用に使用する TLS 証明書のサブジェクト名またはサブジェクトの別名 (SAN) と一致する必要もあります。

2 Windows 証明書ストアに PSG 証明書を構成する

デフォルトの PSG 証明書を CA によって署名された証明書で置き換えるには、PSG が動作している接続サーバまたはセキュリティ サーバ コンピュータの Windows ローカル コンピュータ証明書で、その証明書とプライベート キーを構成する必要があります。

3 Windows レジストリに PSG 証明書のわかりやすい名前を設定する

PSG は、サーバの名前および証明書のわかりやすい名前で使用される TLS 証明書を識別します。PSG が動作している接続サーバまたはセキュリティ サーバ コンピュータの Windows レジストリにわかりやすい名前を設定する必要があります。

4 (オプション) CA 署名付き証明書が PSG への接続に強制的に使用されるようにする

PSG へのすべてのクライアント接続が、デフォルトのレガシー証明書の代わりに PSG 用の CA 署名付き証明書を使用することを保証できます。この手順では、PSG 用の CA 署名付き証明書を構成する必要はありません。Horizon 7 展開で CA 署名付き証明書を強制的に使用させたい場合に限って、この手順を実行してください。

PSG 証明書のサブジェクト名に一致するサーバ名を確認する

接続サーバ インスタンスまたはセキュリティ サーバがインストールされるとき、インストーラはコンピュータの FQDN を含む値でレジストリ設定を作成します。この値が、PSG ポートに到達するためにセキュリティ スキャナが使用する URL のサーバ名の部分と一致することを確認する必要があります。このサーバ名は、PSG 用に使用する TLS 証明書のサブジェクト名またはサブジェクトの別名 (SAN) と一致する必要があります。

たとえば、スキャナが URL `https://view.customer.com:4172` で PSG に接続する場合、そのレジストリ設定は `view.customer.com` の値を持つ必要があります。インストール中に設定される接続サーバまたはセキュリティ サーバ コンピュータの FQDN は、外部のサーバ名と同じでない場合があることに注意してください。

手順

- 1 PColP Secure Gateway が動作している接続サーバまたはセキュリティ サーバ ホスト上で Windows レジストリ エディタを起動します。
- 2 `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway\SSLCertPsgSni` レジストリ設定に移動します。
- 3 `SSLCertPsgSni` 設定の値が、スキャナが PSG に接続するために使用する URL のサーバ名と一致し、そして PSG 用にインストールする TLS 証明書のサブジェクトの名前またはサブジェクトの別名が一致することを確認してください。

この値が一致しない場合、正しい値で置き換えます。

- 4 VMware Horizon View PColP Secure Gateway サービスを再起動して、変更を有効にします。

次のステップ

CA 署名付き証明書を Windows のローカル コンピュータ証明書ストアにインポートし、証明書にわかりやすい名前を付けます。

Windows 証明書ストアに PSG 証明書を構成する

デフォルトの PSG 証明書を CA によって署名された証明書で置き換えるには、PSG が動作している接続サーバまたはセキュリティ サーバ コンピュータの Windows ローカル コンピュータ証明書で、その証明書とプライベート キーを構成する必要があります。

PSG を使用して一意の証明書を使用する場合、証明書をエクスポート可能なプライベート キーと共に Windows ローカル コンピュータ証明書ストアにインポートし、適切なわかりやすい名前をつける必要があります。

PSG でサーバと同じ証明書を使用する場合、この手順に従う必要はありません。ただし、Windows レジストリでは、サーバ証明書のサブジェクトの名前に一致するサーバ名を設定し、わかりやすい名前を `[vdm]` に設定する必要があります。

前提条件

- キーの長さは少なくとも 1024 ビットであることを確認します。
- TLS 証明書が有効であることを確認します。サーバ コンピュータの現在の時間は、証明書の開始日と終了日内でなければなりません。
- 証明書のサブジェクトの名前またはサブジェクトの別名が Windows レジストリの SSLCertPsgSni 設定と一致することを確認します。[PSG 証明書のサブジェクト名に一致するサーバ名を確認する](#)を参照してください。
- 証明書のスナップインが MMC に追加されたことを確認します。[証明書スナップインを MMC に追加する](#)を参照してください。
- 証明書を Windows 証明書ストアにインポートすることを理解しておきます。[署名付きサーバ証明書を Windows 証明書ストアにインポートする](#)を参照してください。
- 証明書をわかりやすい名前に変更することを理解しておきます。[証明書のわかりやすい名前を変更する](#)を参照してください。

手順

- 1 Windows Server ホストの MMC ウィンドウで、[証明書 (ローカル コンピュータ)] - [個人] フォルダを開きます。
- 2 [その他の操作] - [すべてのタスク] - [インポート] を選択して、PSG に交付される TLS 証明書をインポートします。

[証明書のインポート] ウィザードで以下の設定を選択します:

- a [このキーをエクスポート可能にマーク]
- b [すべての拡張可能なプロパティを含む]

ウィザードを完了して、[個人] フォルダへの証明書のインポートを終了します。

- 3 以下のいずれかの手順を実行して、新しい証明書がプライベート キーを含むことを確認します:
 - 黄色のキーが証明書アイコンに表示されることを確認します。
 - 証明書をダブルクリックし、[証明書情報] ダイアログ ボックスに次の文が表示されることを確認します。この証明書に対応するプライベート キーがあります。
- 4 新しい証明書を右クリックして [プロパティ] をクリックします。
- 5 [一般] タブで、[わかりやすい名前] テキストを削除し、選択したわかりやすい名前を入力します。
次の手順で説明するように、Windows レジストリの SSLCertWinCertFriendlyName 設定に全く同じ名前を入力してください。
- 6 [適用]、[OK] の順にクリックします。

結果

PSG は CA 署名付き証明書を PCoIP でサーバに接続するクライアント デバイスに示します。

注: この手順はレガシー クライアント デバイスに影響を及ぼしません。PSG はデフォルトのレガシー証明書を PCoIP でこのサーバに接続するレガシー クライアント デバイスに引き続き示します。

次のステップ

Windows レジストリに証明書のわかりやすい名前をつけます。

Windows レジストリに PSG 証明書のわかりやすい名前を設定する

PSG は、サーバの名前および証明書のわかりやすい名前で使用する TLS 証明書を識別します。PSG が動作している接続サーバまたはセキュリティ サーバ コンピュータの Windows レジストリにわかりやすい名前を設定する必要があります。

証明書のフレンドリ名 [vdm] は、すべての接続サーバ インスタンスおよびセキュリティ サーバで使用されます。一方、自分自身の証明書を PSG 証明書用のわかりやすい名前に構成できます。正しい名前が Windows 証明書ストアに設定するわかりやすい名前と一致するように PSG を有効にするため、Windows レジストリ設定を構成する必要があります。

PSG は、PSG が動作しているサーバと同じ TLS 証明書を使用できます。サーバと同じ証明書を使用するために PSG を構成する場合、わかりやすい名前は [vdm] である必要があります。

わかりやすい名前の値は、レジストリおよび Windows 証明書ストアの両方で大文字と小文字を区別します。

前提条件

- Windows レジストリに PSG ポートに到達するために使用される正しいサブジェクトの名前が含まれ、PSG 証明書のサブジェクトの名前またはサブジェクトの別名と一致することを確認します。[PSG 証明書のサブジェクト名に一致するサーバ名を確認する](#)を参照してください。
- 証明書のフレンドリ名が Windows ローカル コンピュータ証明書ストアに構成されていることを確認します。[Windows 証明書ストアに PSG 証明書を構成する](#)を参照してください。

手順

- 1 PCoIP Secure Gateway が動作している接続サーバまたはセキュリティ サーバ コンピュータ上で Windows レジストリ エディタを起動します。
- 2 HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway レジストリ キーに移動します。
- 3 新しい文字列 (REG_SZ) 値 SSLCertWinCertFriendlyName をこのレジストリ キーに追加します。
- 4 SSLCertWinCertFriendlyName 値を変更し、PSG で使用される証明書のわかりやすい名前を入力します。
例 : [pcoip]
サーバと同じ証明書を使用する場合、その値は [vdm] である必要があります。
- 5 VMware Horizon View PCoIP Secure Gateway サービスを再起動して、変更を有効にします。

次のステップ

クライアント デバイスが PSG への接続を続行することを確認します。

準拠テストでセキュリティ スキャナを使用している場合、PSG ポートをスキャンします。

CA 署名付き証明書が PSG への接続に強制的に使用されるようにする

PSG へのすべてのクライアント接続が、デフォルトのレガシー証明書の代わりに PSG 用の CA 署名付き証明書をを使用することを保証できます。この手順では、PSG 用の CA 署名付き証明書を構成する必要はありません。

Horizon 7 展開で CA 署名付き証明書を強制的に使用させたい場合に限って、この手順を実行してください。

場合によっては、PSG は、PSG ポートの準拠テストを無効にして、CA 署名付き証明書の代わりにデフォルトのレガシー証明書をセキュリティ スキャナーに表示することがあります。この問題を解決するために、接続を試みるすべてのデバイスにデフォルトのレガシー証明書を表示しないように PSG を構成できます。

重要： この手順を実行すると、すべてのレガシー クライアントが PCoIP でこのサーバに接続しないように設定します。

前提条件

シン クライアントを含む、このサーバに接続するすべてのクライアント デバイスが Horizon Client 5.2 for Windows または Horizon Client 2.0 以降のリリースを実行していることを確認してください。レガシー クライアントをアップグレードする必要があります。

手順

- 1 PCoIP Secure Gateway が動作している接続サーバまたはセキュリティ サーバ コンピュータ上で Windows レジストリ エディタを起動します。
- 2 HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway レジストリ キーに移動します。
- 3 新しい文字列 (REG_SZ) 値 SSLCertPresentLegacyCertificate をこのレジストリ キーに追加します。
- 4 SSLCertPresentLegacyCertificate 値を [0] に設定します。
- 5 VMware Horizon View PCoIP Secure Gateway サービスを再起動して、変更を有効にします。

vCenter Server または View Composer 証明書を信頼するための Horizon Administrator の設定

Horizon Administrator ダッシュボードでは、信頼されていない vCenter Server または View Composer の証明書を信頼するように Horizon 7 を構成することができます。

VMware では、認証局 (CA) によって署名される TLS 証明書を使用するように vCenter Server と View Composer を構成することを強く推奨します。あるいは、vCenter Server または View Composer のデフォルト証明書の拇印を受け入れることもできます。

同様に、認証局 (CA) によって署名される TLS 証明書を使用するように SAML 2.0 認証システムを構成することを推奨します。あるいは Horizon Administrator ダッシュボードで、デフォルト証明書の拇印を受け入れることにより、信頼されていない SAML 2.0 サーバ証明書を信頼するように Horizon 7 を構成することもできます。

認証局 (CA) によって署名された TLS 証明書を使用する利点

CA は、証明書とその作成者の身元を保証する信頼された機関です。証明書が信頼された CA によって署名されている場合は、証明書の検証を求めるメッセージは表示されず、追加の構成をしなくてもシンクライアント デバイスから接続できます。

www.mycorp.com など、Web ドメインに特化した TLS サーバ証明書を要求できます。また、*.mycorp.com など、ドメイン全体で利用できるワイルドカード TLS サーバ証明書を要求することも可能です。複数のサーバやさまざまなサブドメインに証明書をインストールする必要がある場合は、ワイルドカード証明書を要求すれば、管理を簡素化できます。

安全なインストール環境においてはドメイン固有の証明書の使用が一般的です。また、CA は通常、ドメイン固有の証明書の紛失に対しては、ワイルドカード証明書の場合よりも保護されることを保証します。他のサービスと共有されるワイルドカード証明書を使用する場合、Horizon 7 製品のセキュリティは、その他のサービスのセキュリティにも依存します。ワイルドカード証明書を使用する場合は、プライベート キーがサーバ間を移動できるようにする必要があります。

デフォルトの証明書を独自の証明書に置き換えると、クライアントはその独自の証明書を使用してサーバ認証を行います。証明書が CA によって署名されている場合、CA 自体の証明書は、通常、ブラウザに埋め込まれるか、またはクライアントがアクセスできる信頼されたデータベースに置かれます。クライアントは、証明書を受け入れた後、応答として証明書に含まれるパブリック キーでパブリック キーされた秘密鍵を送信します。この秘密鍵を使用して、クライアントとサーバとの間のトラフィックが暗号化されます。

Horizon 接続サーバとセキュリティ サーバ証明書問題のトラブルシューティング

Horizon 7 サーバで証明書に関する問題があると、Horizon Administrator に接続できなかつたり、サーバに対して赤色の健全性インジケータが表示されたりします。

問題

問題がある接続サーバ インスタンスでは、Horizon Administrator に接続できません。同じポッドにある別の接続サーバ インスタンス上で Horizon Administrator に接続すると、問題の接続サーバ インスタンスのダッシュボード健全性インジケータが赤色で表示されています。

他の接続サーバ インスタンスから赤色の健全性インジケータをクリックすると、SSL 証明書: 無効 とステータス: (空白) が表示され、有効な証明書が見つからなかったことを示します。Horizon 7 ログ ファイルには、ERROR タイプのログ エントリと「キーストアに正規の証明書がありません」というエラー テキストが含まれます。

Horizon 7 ログ データは、接続サーバ インスタンスの C:\ProgramData\VMware\VDM\logs\log-*.txt にあります。

原因

次のような理由で証明書が Horizon 7 サーバに正常にインストールされなかった可能性があります。

- 証明書が Windows ローカル コンピュータ証明書ストアの個人フォルダ内にはない。
- 証明書ストアに証明書のプライベート キーがない。

- 証明書に [vdm] のフレンドリ名がない。
- 証明書が v3 証明書テンプレートから生成された (Windows Server 2008 以降のサーバの場合)。Horizon 7 はプライベート キーを検出できませんが、証明書スナップインを使用して Windows 証明書ストアを検証する場合、ストアにはプライベート キーがあることが示されます。

解決方法

- ◆ 証明書が Windows ローカル コンピュータ証明書ストアの個人フォルダにインポートされていることを確認します。

[署名付きサーバ証明書を Windows 証明書ストアにインポートする](#)を参照してください。

- ◆ 証明書にプライベート キーが含まれていることを確認します。

[署名付きサーバ証明書を Windows 証明書ストアにインポートする](#)を参照してください。

- ◆ 証明書に [vdm] のフレンドリ名があることを確認します。

[証明書のわかりやすい名前を変更する](#)を参照してください。

- ◆ 証明書が v3 証明書テンプレートから生成された場合は、v3 テンプレートを使用しない CA から有効な署名証明書を入手します。

[認証局 \(CA\) からの署名付き TLS 証明書の取得](#)を参照してください。

Horizon 7 の初回構成

9

Horizon 7 サーバ ソフトウェアをインストールしてサーバの SSL 証明書を構成した後、動作する Horizon 7 環境を設定するための追加のステップを実行する必要があります。

vCenter Server および View Composer のユーザー アカウントを構成し、Horizon 7 ライセンス キーをインストールし、vCenter Server および View Composer を Horizon 7 環境に追加し、PCoIP Secure Gateway および安全なトンネルを構成し、オプションで、Horizon 7 環境をサポートするために Windows Server 設定でサイズを変更します。

この章には、次のトピックが含まれています。

- [vCenter Server、View Composer およびインスタント クローンのユーザー アカウントの構成](#)
- [初めての Horizon 接続サーバの構成](#)
- [Horizon Client 接続の構成](#)
- [Horizon 7 サービスのデフォルト ポートの置換](#)
- [展開の規模に合わせた Windows Server 設定の調整](#)

vCenter Server、View Composer およびインスタント クローンのユーザー アカウントの構成

Horizon 7 で vCenter Server を使用するには、適切な vCenter Server 権限を持つユーザー アカウントを構成する必要があります。適切な権限を持つ vCenter Server ロールを作成し、そのロールを vCenter Server ユーザー アカウントに割り当てることができます。

View Composer を vCenter Server とは別のマシンにインストールする場合、Horizon 7 がスタンドアロンのマシンで View Composer サービスへの認証に使用できるユーザー アカウントを Active Directory で作成する必要があります。

View Composer を使用する場合、View Composer が Active Directory で特定の操作を実行できるようになる第三のユーザー アカウントを、Active Directory で作成する必要があります。View Composer では、リンク クローン仮想マシンを Active Directory ドメインに参加させるためにこのアカウントが必要です。[View Composer AD 操作のユーザー アカウントの作成](#)を参照してください。

インスタント クローンを使用する場合は、接続サーバが Active Directory で特定の操作を行えるよう、Active Directory 内にユーザー アカウントを 1 つ作成する必要があります。インスタント クローン仮想マシンを Active Directory ドメインに参加させるには、このアカウントが接続サーバに必要になります。[インスタントクローン操作のユーザー アカウントの作成](#)を参照してください。

要約すると、Horizon 7 を最初に構成するとき、これらのユーザー アカウントを Horizon Administrator で入力します。

- vCenter Server ユーザーにより、Horizon 7 と View Composer が vCenter Server で操作を実行できるようになります。
- スタンドアロンの View Composer Server ユーザーにより、Horizon 7 がスタンドアロン マシンで View Composer サービスへの認証を実行できるようになります。

vCenter Server と同じマシンに View Composer をインストールする場合、vCenter Server ユーザーは上記の両方の機能を実行し、ユーザーはスタンドアロンの View Composer Server ユーザーを使用しません。

- AD 操作に必要な View Composer ユーザーにより、View Composer が Active Directory で特定の操作を実行できるようになります。
- Active Directory 操作のインスタント クローン ユーザーを使用すると、接続サーバは Active Directory で特定の操作を実行できるようになります。

vCenter Server ユーザーと View Composer ユーザーを使用する場所

これらのユーザー アカウントを作成して構成した後、Horizon Administrator でユーザー名を指定します。

- vCenter Server を Horizon 7 に追加するときに、vCenter Server ユーザーを指定します。
- View Composer 設定を構成し [スタンドアロン View Composer Server] を選択するとき、スタンドアロンの View Composer サーバ ユーザーを指定します。
- View Composer ドメインを構成するとき、AD 操作に必要な View Composer ユーザーを指定します。
- リンク クローン プールを作成するとき、AD 操作に必要な View Composer ユーザーを指定します。

Horizon 7 および View Composer の vCenter Server ユーザーの構成

vCenter Server で Horizon 7 が操作を実行することを許可するユーザー アカウントを構成するには、適切な権限を持つ vCenter Server ロールをそのユーザーに割り当てる必要があります。

vCenter Server ロールに追加する必要がある権限リストは、View Composer ありまたはなしで Horizon 7 を使用するかどうかに応じて変わります。View Composer サービスは、基本的な権限の他の権限を必要とする vCenter Server での操作を実行します。

vCenter Server と同じマシンに View Composer をインストールする場合、その vCenter Server ユーザーを vCenter Server マシンのローカル システム管理者にする必要があります。この要件により、Horizon 7 で View Composer サービスの認証を行うことができます。

View Composer を vCenter Server とは別のマシンにインストールする場合、vCenter Server ユーザーを vCenter Server マシン上のローカル管理者にする必要はありません。ただし、View Composer マシン上のローカル管理者となる必要があるスタンドアロンの View Composer Server ユーザー アカウントを作成する必要があります。

前提条件

- Active Directory で、接続サーバ ドメインまたは信頼されたドメインにユーザーを作成します。[vCenter Server のユーザー アカウントの作成](#)を参照してください。
- ユーザー アカウントに必要な vCenter Server 権限について理解しておきます。[vCenter Server ユーザーに必要な権限](#)を参照してください。
- View Composer を使用する場合は、その他の必要な権限について理解しておきます。[vCenter Server ユーザーに必要な View Composer とインスタント クローンの権限](#)を参照してください。

手順

- 1 vCenter Server で、必要な権限を持つロールをユーザーに用意します。

- vCenter Server の定義済みの管理者ロールを使用できます。このロールは vCenter Server でのすべての操作を実行できます。
- View Composer を使用する場合は、接続サーバと View Composer が vCenter Server の操作を実行するために必要な最低限の権限を持つ、制限されたロールを作成することができます。

vSphere Client で、[ホーム] - [ロール] - [ロールを追加] をクリックし、

View Composer Administrator などのロール名を入力してから、ロールの権限を選択します。

このロールは、接続サーバと View Composer の両方が vCenter Server で動作するために必要なすべての権限を持っている必要があります。

- View Composer なしで Horizon 7 を使用する場合は、接続サーバが vCenter Server の操作を実行するために必要な最低限の権限を持つ、制限されたロールをさらに作成することができます。

vSphere Client で、[ホーム] - [ロール] - [ロールを追加] をクリックし、**View Manager Administrator** などのロール名を入力してから、ロールの権限を選択します。

- インスタント クローンを使用する場合は、vCenter Server の操作に接続サーバが必要とする最低限の権限を持つロールを作成できます。

vSphere Client で、[ホーム] - [ロール] - [ロールを追加] をクリックし、

View Manager インスタント クローン管理者などのロール名を入力してから、ロールの権限を選択します。インスタント クローンの権限については、[vCenter Server ユーザーに必要な View Composer とインスタント クローンの権限](#)を参照してください。

- 2 vSphere Client で、インベントリのトップ レベルで vCenter Server を右クリックして [権限を追加] をクリックし、vCenter Server ユーザーを追加します。

注： vCenter Server のレベルで vCenter Server ユーザーを定義する必要があります。

- 3 ドロップダウン メニューから、作成した管理者ロール、View Composer ロール、または View 管理者ロールを選択し、それを vCenter Server ユーザーに割り当てます。

- 4 vCenter Server と同じマシンに View Composer をインストールする場合、vCenter Server ユーザー アカウントを vCenter Server マシンのローカル システム管理者グループのメンバーとして追加する必要があります。

View Composer を vCenter Server とは別のマシンにインストールする場合は、この手順は必要ありません。

次のステップ

Horizon Administrator で、vCenter Server を Horizon 7 に追加するときに、vCenter Server ユーザーを指定します。[vCenter Server インスタンスの Horizon 7 への追加](#)を参照してください。

vCenter Server ユーザーに必要な権限

vCenter Server ユーザーには、Horizon 7 が vCenter Server で操作を実行できるように十分な権限が必要です。vCenter Server ユーザー用に必要な権限を持つ View Manager ロールを作成します。

表 9-1. View Manager ロールに必要な権限

権限グループ	有効にする権限
[フォルダ]	[フォルダの作成] [フォルダの削除]
[データストア]	[領域の割り当て]
[仮想マシン]	<p>[構成] で :</p> <ul style="list-style-type: none"> ■ [デバイスの追加または削除] ■ [詳細] ■ [デバイス設定の変更] <p>[相互作用] で :</p> <ul style="list-style-type: none"> ■ [パワーオフ] ■ [パワーオン] ■ [リセット] ■ [サスペンド] ■ [ワイプまたは圧縮操作の実行] <p>[インベントリ] で :</p> <ul style="list-style-type: none"> ■ [新規作成] ■ [既存から作成] ■ [削除] <p>[プロビジョニング] で :</p> <ul style="list-style-type: none"> ■ [カスタマイズ] ■ [テンプレートのデプロイ] ■ [カスタマイズ仕様の読み取り] ■ [テンプレートのクローン作成] ■ [仮想マシンのクローン作成]
[リソース]	[仮想マシンのリソース プールへの割り当て]
[グローバル]	<p>[vCenter Server として機能]</p> <p>View Storage Accelerator を使用しない場合でも、vCenter Server のユーザーにはこの権限が必要です。</p>

表 9-1. View Manager ロールに必要な権限（続き）

権限グループ	有効にする権限
[ホスト]	ESXi ホストのキャッシュ機能を有効にする View Storage Accelerator を実装するには、次の [ホスト] 権限が必要です。View Storage Accelerator を使用しない場合、vCenter Server のユーザーにはこの権限は必要ありません。 [構成] で： ■ [詳細設定]
[プロファイル駆動型ストレージ] (vSAN データストアまたは Virtual Volumes を使用している場合)	(すべて)

vCenter Server ユーザーに必要な View Composer とインスタント クローンの権限

View Composer またはインスタント クローンをサポートするには、Horizon 7 をサポートするために必要な権限に加えて、vCenter Server ユーザーに権限を割り当てる必要があります。

View Composer とインスタント クローンの権限では、View Manager、View Composer、およびインスタント クローンに必要な権限のスーパー セットが一覧表示されます。

表 9-2. View Composer とインスタント クローンの権限

vCenter Server の権限グループ	有効にする権限
[フォルダ]	[フォルダ作成] [フォルダ削除]
[データストア]	[領域の割り当て] [データストアを参照] [低レベル ファイル操作]
[ホスト]	[インベントリ]： ■ [クラスタの変更]
[仮想マシン]	[設定] (すべて)： [相互作用] で： ■ [パワーオフ] ■ [パワーオン] ■ [リセット] ■ [サスペンド] ■ [ワイプまたは圧縮操作の実行] ■ [デバイス接続] [インベントリ] (すべて) [スナップショット管理] (すべて) [プロビジョニング]： ■ [カスタマイズ] ■ [テンプレートのデプロイ] ■ [カスタマイズ仕様の読み取り] ■ [テンプレートのクローン作成] ■ [仮想マシンのクローン作成] ■ [ディスク アクセスを許可]

表 9-2. View Composer とインスタント クローンの権限 （続き）

vCenter Server の権限グループ	有効にする権限
[リソース]	<p>[仮想マシンのリソース プールへの割り当て]</p> <p>以下の権限は、View Composer 再分散操作を実行するために必要です。</p> <p>[仮想マシンの電源をオフにする]</p>
[グローバル]	<p>[メソッドを有効にする]</p> <p>[メソッドを無効にする]</p> <p>[システム タグ]</p> <p>[カスタム属性の管理]</p> <p>[カスタム属性の設定]</p> <p>ESXi ホストのキャッシュ機能を有効にする View Storage Accelerator を実装するには、次の権限が必要です。View Storage Accelerator を使用しない場合でも、vCenter Server のユーザーにはこの権限が必要です。</p> <p>[vCenter Server として機能]</p>
[ネットワーク]	(すべて)
[プロファイル駆動型ストレージ]	(vSAN データストアまたは Virtual Volumes を使用している場合)
[ストレージ ビュー]	[表示]
[暗号化操作]	<p>トラステッド プラットフォーム モジュール (vTPM) デバイスでインスタント クローン仮想マシンを使用する場合は、次の権限が必要です。</p> <ul style="list-style-type: none"> ■ [クローン] ■ [復号化] ■ [直接アクセス] ■ [暗号化] ■ [KMS の管理] ■ [移行] ■ [ホストの登録]

初めての Horizon 接続サーバの構成

接続サーバをインストールした後は、製品ライセンスをインストールし、vCenter Server と View Composer サービスを Horizon 7 に追加する必要があります。また、ESXi ホストでリンク クローン仮想マシンのディスク スペースを再利用できるようにして、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 ホストを構成することもできます。

セキュリティ サーバをインストールすると、これらは Horizon 7 に追加され、Horizon Administrator で自動的に表示されます。

Horizon Administrator と Horizon Connection Server

Horizon Administrator では Horizon 7 の Web ベースの管理インターフェイスが提供されます。

Horizon Connection Server は、レプリカ サーバまたはセキュリティ サーバとして機能する複数のインスタンスを持つことができます。Horizon 7 の展開環境によっては、Connection Server の各インスタンスで Horizon Administrator インターフェイスを使用できます。

Connection Server で Horizon Administrator を使用する場合は、次のベスト プラクティスを使用します。

- Connection Server のホスト名と IP アドレスを使用して、Horizon Administrator にログインします。
Horizon Administrator インターフェイスを使用して、Connection Server および関連するセキュリティ サーバやレプリカ サーバを管理します。
- ポッド環境では、すべての管理者が同じ Connection Server のホスト名と IP アドレスを使用して Horizon Administrator にログインしていることを確認します。ロード バランサのホスト名と IP アドレスを使用して、Horizon Administrator の Web ページにアクセスしないでください。
- 使用している Connection Server の CPA ポッドまたはクラスタ名を特定するには、Horizon Administrator ヘッダーと Web ブラウザ タブで名前を確認します。

注： セキュリティ サーバではなく、Unified Access Gateway アプライアンスを使用する場合は、Unified Access Gateway REST API を使用して Unified Access Gateway アプライアンスを管理する必要があります。Unified Access Gateway の以前のバージョンには、Access Point という名前が付けられます。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。

Horizon Administrator へのログイン

初期設定タスクを実行するには、Horizon Administrator にログインする必要があります。

前提条件

Horizon Administrator でサポートされている Web ブラウザを使用していることを確認します。 [Horizon Administrator の要件](#)を参照してください。

手順

- 1 Web ブラウザを開き、次の URL を入力します。*server* は、Connection Server インスタンスのホスト名です。

https://*server*/admin

注： ホスト名が解決できないときに Connection Server インスタンスにアクセスする必要がある場合は、IP アドレスを使用できます。ただし、通信するホストは、Connection Server インスタンスに対して構成された TLS 証明書に一致しないため、アクセスがブロックされたりアクセスのセキュリティが低下したりします。

Horizon Administrator へのアクセスは、Connection Server コンピュータで構成されている証明書のタイプによって異なります。Connection Server ホストで Web ブラウザを開く場合、**https://localhost** ではなく、**https://127.0.0.1** を使用して接続します。この方法で localhost 解決における潜在的な DNS 攻撃を回避することにより、セキュリティが向上します。

オプション	説明
Horizon Connection Server 用に CA によって署名された証明書を設定しています。	初めて接続するときに、Web ブラウザに [VMware Horizon 7 へようこそ] ページが表示されます。
Horizon Connection Server によって提供されたデフォルトの自己署名証明書が構成されます。	最初に接続したときに、Web ブラウザによって、アドレスに関連付けられているセキュリティ証明書が、信頼された証明機関から発行されていないことを警告するページが表示される場合があります。 [無視] をクリックして、現在の TLS 証明書の使用を続けます。

- Horizon Administrator で [起動] をクリックします。
- 管理者ロールを持つアカウントを使用してログインします。

スタンドアローンの Connection Server インスタンス、または複製されたグループにおける最初の Connection Server インスタンスをインストールするときに、管理者ロールの初期割り当てを行います。デフォルトでは、Connection Server のインストールに使用するアカウントが選択されていますが、このアカウントを Administrators ローカル グループまたはドメイン グローバル グループに変更できます。

Administrators ローカル グループを選択した場合は、このグループに追加されたドメイン ユーザーを直接またはグループ メンバーシップ経由で使用できます。このグループに追加されたローカル ユーザーは使用できません。

結果

Horizon Administrator にログインした後、[View 構成] - [管理者] を使用して、管理者ロールを持つユーザーおよびグループのリストを変更できます。

製品のライセンス キーのインストール

接続サーバを使用するには、まず製品のライセンス キーを入力する必要があります。

注： Horizon 7 サブスクリプションのライセンスがある場合、製品のライセンス キーは必要ありません。サブスクリプション ライセンスの詳細については、[#unique_129](#) を参照してください。

Horizon Administrator に初めてログインすると、[製品のライセンスと使用状況] ページが表示されます。

ライセンス キーをインストールした後は、ログインすると Horizon Administrator のダッシュボード ページが表示されます。

複製された接続サーバ インスタンスまたはセキュリティ サーバをインストールするときは、ライセンス キーを設定する必要はありません。複製されたインスタンスとセキュリティ サーバは、View の LDAP 構成に格納されている共通ライセンス キーを使用します。

注： 接続サーバには有効なライセンス キーが必要です。プロダクト ライセンス キーは 25 文字のキーです。

手順

- 1 Horizon Administrator で、[View 構成] - [製品のライセンスと使用状況] の順に選択します。
- 2 [ライセンス] パネルで、[ライセンスを編集] をクリックします。
- 3 ライセンス シリアル番号を入力し、[OK] をクリックします。
- 4 ライセンスの有効期限の日付を確認します。
- 5 お持ちの製品のライセンスによって使用資格が付与されている VMware Horizon 7 のエディションに基づいて、デスクトップ、アプリケーションのリモート処理、および View Composer ライセンスが有効または無効になっていることを確認します。

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。

vCenter Server インスタンスの Horizon 7 への追加

Horizon 7 環境内の vCenter Server インスタンスに接続するように、Horizon 7 を構成する必要があります。Horizon 7 がデスクトップ プールで使用する仮想マシンは、vCenter Server が作成し、管理します。

vCenter Server インスタンスをリンク モード グループ内で実行する場合は、各 vCenter Server インスタンスを個別に Horizon 7 に追加する必要があります。

Horizon 7 は、安全なチャネル (SSL) を使用して vCenter Server インスタンスに接続します。

前提条件

- 接続サーバの製品ライセンス キーをインストールします。
- Horizon 7 をサポートするのに必要な vCenter Server で、操作を実行する権限のある vCenter Server ユーザーを準備します。View Composer を使用するには、このユーザーに権限を追加する必要があります。

[Horizon 7 および View Composer の vCenter Server ユーザーの構成](#)を参照してください。

- TLS/SSL サーバ証明書が vCenter Server ホストにインストールされていることを確認します。本番環境で、信頼された証明機関 (CA) によって署名された有効な証明書をインストールします。

テスト環境では、vCenter Server でインストールされたデフォルト証明書を使用できますが、vCenter Server を Horizon 7 に追加する際に証明書サムプリントを受け入れる必要があります。

- 複製されたグループ内のすべての接続サーバ インスタンスが、vCenter Server ホストにインストールされているサーバ証明書のルート CA 証明書を信頼していることを確認します。ルート CA 証明書が、接続サーバ ホスト上の Windows ローカル コンピュータの証明書ストア内の [信頼されたルート証明機関] - [証明書] フォルダにあるかどうか確認します。このフォルダにない場合、ルート CA 証明書を Windows ローカル コンピュータの証明書ストアにインポートします。

[ルート証明書と中間証明書を Windows 証明書ストアにインポートする](#)を参照してください。

- vCenter Server インスタンスに ESXi ホストが含まれていることを確認します。vCenter Server インスタンスでホストが構成されていない場合、そのインスタンスを Horizon 7 に追加することはできません。

- vSphere 5.5 以降のリリースにアップグレードする場合、vCenter Server ユーザーとして使用するドメイン管理者アカウントが、vCenter Server のローカル ユーザーによって vCenter Server にログインするために明示的に指定された権限であったことを確認してください。

- Horizon 7 で FIPS モードを使用する予定の場合は、vCenter Server 6.0 以降および ESXi 6.0 以降のホストを使用していることを確認してください。

詳細については、[4 章 FIPS モードでの Horizon 7 のインストール](#)を参照してください。

- vCenter Server と View Composer の操作数の上限を決定する設定について理解しておきます。「[vCenter Server と View Composer の同時操作の制限](#)および [リモート デスクトップ ログオン ストームをサポートするための同時電源操作レートの設定](#)」を参照してください。

手順

- 1 Horizon Administrator で、[View 構成] - [サーバ] を選択します。
- 2 [vCenter Servers] タブで、[追加] をクリックします。
- 3 [vCenter Server 設定] の [サーバ アドレス] テキスト ボックスに、vCenter Server インスタンスの完全修飾ドメイン名 (FQDN) を入力します。

FQDN にはホスト名とドメイン名が含まれます。たとえば、FQDN の

myserverhost.companydomain.com で、*myserverhost* はホスト名で、*companydomain.com* はドメインです。

注： DNS 名または URL を使用してサーバを入力すると、Horizon 7 は管理者が以前に IP アドレスを使用して Horizon 7 にこのサーバを追加したかどうかを確認する DNS 検索を実行しません。vCenter Server をその DNS 名と IP アドレスの両方で追加すると、競合が発生します。

- 4 vCenter Server ユーザーの名前を入力します。
- 5 vCenter Server ユーザーのパスワードを入力します。
- 6 (オプション) この vCenter Server インスタンスの説明を入力します。
- 7 TCP のポート番号を入力します。

デフォルトのポートは 443 です。

- 8 [詳細設定] で、vCenter Server と View Composer の同時操作の制限を設定します。
- 9 [次へ] をクリックして [View Composer 設定] ページを表示します。

次のステップ

View Composer 設定を構成します。

- vCenter Server インスタンスが署名された SSL 証明書で構成されていて、接続サーバがルート証明書を信頼している場合、[vCenter Server を追加] ウィザードで [View Composer 設定] ページが表示されます。

- vCenter Server インスタンスがデフォルト証明書で構成されている場合、最初に既存の証明書のサムプリントを受け入れるかどうかを決定する必要があります。[デフォルトの TLS 証明書のサムプリントを受け入れる](#)を参照してください。

Horizon 7 で複数の vCenter Server インスタンスを使用している場合、この手順を繰り返してその他の vCenter Server インスタンスを追加します。

View Composer 設定を構成する

View Composer を使用するには、接続サーバに View Composer サービスへの接続を許可する設定をする必要があります。View Composer は独自のスタンドアロン マシンにインストールすることも、vCenter Server と同じマシンにインストールすることもできます。

VMware では、それぞれの View Composer サービスと vCenter Server インスタンスを 1 対 1 で対応させることを推奨しています。

前提条件

- vCenter Server に接続するように接続サーバを設定したことを確認します。そのためには、[vCenter Server を追加] ウィザードで [vCenter Server の情報] ページを完了する必要があります。[vCenter Server インスタンスの Horizon 7 への追加](#)を参照してください。
- この View Composer サービスがまだ別の vCenter Server インスタンスに接続するように構成されていないことを確認します。
- View Composer をスタンドアロン マシンにインストールした場合、スタンドアロンの View Composer Server ユーザー アカウントを作成したことを確認します。このドメイン ユーザー アカウントは、その View Composer マシン上のローカル管理者グループのメンバーである必要があります。

手順

- 1 Horizon Administrator で、[vCenter Server を追加] ウィザードで [vCenter Server の情報] ページを完了します。
 - a [View 構成] - [サーバ] をクリックします。
 - b [vCenter Server] タブで、[追加] をクリックして vCenter Server 設定を指定します。
- 2 [View Composer 設定] ページで、View Composer を使用していない場合、[View Composer を使用しない] を選択します。

[View Composer を使用しない] を選択した場合、その他の View Composer 設定が非アクティブになります。[\[次へ\]](#) をクリックすると、[vCenter Server を追加] ウィザードで [ストレージ設定] ページが表示されます。[\[View Composer ドメイン\]](#) ページは表示されません。

3 View Composer を使用している場合、View Composer マシンの場所を選択します。

オプション	説明
View Composer が vCenter Server と同じマシンにインストールされます。	a [View Composer を vCenter Server と一緒にインストール] を選択します。 b ポート番号が vCenter Server に View Composer サービスをインストールしたときに指定したポートと同じであることを確認します。デフォルトのポート番号は 18443 です。
View Composer が独自の個別マシンにインストールされます。	a [スタンドアロン View Composer Server] を選択します。 b View Composer Server アドレスのテキスト ボックスに、View Composer マシンの完全修飾ドメイン名 (FQDN) を入力します。 c View Composer サービスへの認証が可能なドメイン ユーザー アカウントの名前を入力します。 <p>このアカウントは、スタンドアロンの View Composer マシン上のローカル管理者グループのメンバーである必要があります。</p> <p>例: domain.com\user または user@domain.com</p> d このドメイン ユーザー アカウントのパスワードを入力します。 e ポート番号が View Composer サービスをインストールしたときに指定したポートと同じであることを確認します。デフォルトのポート番号は 18443 です。

4 [次へ] をクリックして [View Composer ドメイン] ページを表示します。

次のステップ

View Composer ドメインを構成します。

- View Composer インスタンスが署名された SSL 証明書で構成されていて、接続サーバがルート証明書を信頼している場合、[vCenter Server を追加] ウィザードで [View Composer ドメイン] ページが表示されます。
- View Composer インスタンスがデフォルト証明書で構成されている場合、最初に既存の証明書のサムプリントを受け入れるかどうかを決定する必要があります。[デフォルトの TLS 証明書のサムプリントを受け入れる](#)を参照してください。

View Composer ドメインを構成する

View Composer がリンク クローン デスクトップを展開する Active Directory ドメインを構成する必要があります。View Composer 用に複数のドメインを構成できます。最初に vCenter Server と View Composer の設定を View に追加した後で、Horizon Administrator で vCenter Server インスタンスを編集することでさらに View Composer ドメインを追加できます。

前提条件

- Active Directory 管理者は、AD 操作に必要な View Composer ユーザーを作成する必要があります。このドメイン ユーザーには、リンク クローンを含んでいる Active Directory ドメインから仮想マシンを追加または削除する権限が必要です。このユーザーに必要な権限の詳細については、[View Composer AD 操作のユーザー アカウントの作成](#)を参照してください。
- Horizon Administrator で、[vCenter Server を追加] ウィザードで [vCenter Server の情報] ページと [View Composer 設定] ページを完了していることを確認します。

手順

- 1 [View Composer ドメイン] ページで、[追加] をクリックして、AD 操作に必要な View Composer ユーザーのアカウント情報を追加します。
- 2 Active Directory ドメインのドメイン名を入力します。
例: **domain.com**
- 3 View Composer ユーザーの (ドメイン名を含む) ドメイン ユーザー名を入力します。
例: **domain.com\admin**
- 4 アカウントのパスワードを入力します。
- 5 [OK] をクリックします。
- 6 リンク クローン プールを展開する他の Active Directory ドメインでの権限を持つドメイン ユーザー アカウントを追加するには、前記の手順を繰り返します。
- 7 [次へ] をクリックして [ストレージ設定] ページを表示します。

次のステップ

仮想マシンのディスク領域再利用を有効にして、Horizon 7 用に View Storage Accelerator を構成します。

インスタントクローンのドメイン管理者の追加

インスタントクローン デスクトップ プールを作成する前に、インスタントクローン ドメイン管理者を Horizon 7 に追加する必要があります。

インスタントクローン ドメイン管理者には、特定の Active Directory ドメインの権限が必要です。『Horizon 7 のインストール』の「vCenter Server ユーザーに必要な View Composer とインスタント クローンの権限」を参照してください。

手順

- 1 Horizon Administrator で、[View 構成] - [インスタント クローンのドメイン管理者] の順に選択します。
- 2 [追加] をクリックします。
- 3 インスタントクローン ドメイン管理者のログイン名とパスワードを入力します。

vSphere でリンク クローン仮想マシンのディスク領域を再利用できるようにする

vSphere 5.1 以降では、Horizon 7 用にディスク容量再利用機能を有効にできます。vSphere 5.1 からは、Horizon 7 がリンク クローン仮想マシンを効率的なディスク形式で作成するようになりました。これにより、ESXi ホストはリンク クローン内で使用されていないディスク容量を再利用できるようになり、リンク クローンに必要なストレージ容量の合計を削減できます。

ユーザーがリンク クローン デスクトップを操作するたびに、クローンの OS ディスクが大きくなり、最終的には完全クローン デスクトップとほとんど同じディスク領域を使用する場合があります。ディスク領域再利用により、リンク クローンを更新または再構成しなくても、OS ディスクのサイズを減らすことができます。仮想マシンがパワーオンされ、ユーザーがリモート デスクトップを操作している間に、領域を再利用することができます。

ディスク領域再利用は、ログオフ時の更新などのストレージ節約戦略を利用できない展開にとって特に便利です。たとえば、ユーザー アプリケーションを専用リモート デスクトップにインストールするナレッジ ワークの場合、リモート デスクトップが更新または再構成されたときに、個人用アプリケーションが失われることがあります。Horizon 7 はディスク領域再利用により、最初にプロビジョニングされたときの小さなサイズとほぼ同じサイズにリンク クローンを保つことができます。

この機能には、効率的なディスク フォーマットとスペース再利用操作の 2 つのコンポーネントがあります。

vSphere 5.1 以降の環境では、親の仮想マシンが仮想ハードウェア バージョン 9 以降の場合、Horizon 7 は領域再利用操作が有効になっているかどうかにかかわらず、領域効率の高い OS ディスクでリンク クローンを作成します。

容量再利用操作を有効にするには、Horizon Administrator を使用して vCenter Server 用の容量再利用を有効にして、個別のデスクトップ プール用に仮想マシンのディスク容量を再利用する必要があります。vCenter Server 用の領域再利用設定には、vCenter Server インスタンスによって管理されるすべてのデスクトップ プールでこの機能を無効にするためのオプションがあります。vCenter Server 用にこの機能を無効にすると、デスクトップ プール レベルの設定が上書きされます。

以下のガイドラインは、領域再利用機能に適用されます。

- リンク クローン内の領域効率の高い OS ディスクでのみ使用できます。
- これは、View Composer 通常ディスクには影響しません。
- vSphere 5.1 以降、および仮想ハードウェア バージョン 9 以降の仮想マシンのみで機能します。
- 完全クローン デスクトップでは使用できません。
- SCSI コントローラを備えた仮想マシンで使用できます。IDE コントローラはサポートされていません。

View Composer アレイ統合 (VCAI) は、領域効率の高いディスクが使用されている仮想マシンを含むプールでサポートされていません。VCAI は、VAAI (vStorage API for Array Integration) ネイティブ NFS スナップショット テクノロジーを使用して仮想マシンのクローンを作成します。

前提条件

- vCenter Server および ESXi ホストについて、クラスタにすべての ESXi ホストが含まれ、ダウンロード パッチ ESXi510-201212001 以降を適用済みの ESXi 5.1 以降が搭載されたバージョン 5.1 であることを確認します。

手順

- 1 Horizon Administrator で、[ストレージ設定] ページの前に表示される [vCenter Server を追加] ウィザード ページを完了します。
 - a [View 構成] - [サーバ] の順に選択します。
 - b [vCenter Servers] タブで、[追加] をクリックします。
 - c [vCenter Server の情報] ページ、[View Composer 設定] ページ、[View Composer ドメイン] ページを完了します。

2 [ストレージ設定] ページで、[領域再利用を有効にする] が選択されていることを確認します。

Horizon 7 5.2 以降の新規インストールを実行している場合は、領域再利用がデフォルトで選択されています。
You must select if you are upgrading to Horizon 7 5.1 以前のリリースから Horizon 7 5.2 以降にアップグレードしている場合は、[領域再利用を有効にする] を選択する必要があります。

次のステップ

[ストレージ設定] ページで、View Storage Accelerator を構成します。

Horizon 7 でディスク領域再利用の構成を終了するには、デスクトップ プール用の領域再利用をセットアップします。

vCenter Server 用に View Storage Accelerator を構成する

vSphere 5.1 以降では、仮想マシンのディスク データをキャッシュするよう ESXi ホストを構成できます。この View Storage Accelerator と呼ばれている機能は、ESXi ホストで Content Based Read Cache (CBRC) 機能を使用します。多くの仮想マシンが起動しているかウイルス対策スキャンが一度に実行される場合に I/O ストームが発生することがありますが、View Storage Accelerator により、I/O ストーム時の Horizon 7 のパフォーマンスが向上します。この機能は、管理者またはユーザーがアプリケーションまたはデータを頻繁にロードする場合にも役立ちます。ホストは、OS 全体またはアプリケーションをストレージ 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。

ブート ストーム中の IOPS 数を減らすことにより、View Storage Accelerator によるストレージ アレイの要求が抑えられ、これにより Horizon 7 展開をサポートするためのストレージ I/O バンド幅が小さくなります。

この手順で説明しているように、Horizon Administrator の vCenter Server ウィザードで View Storage Accelerator 設定を選択することで、ESXi ホストでのキャッシュ機能を有効にします。

View Storage Accelerator がそれぞれのデスクトップ プール用にも構成されていることを確認します。デスクトップ プールで操作するには、View Storage Accelerator を vCenter Server とそれぞれのデスクトップ プールで有効にする必要があります。

View Storage Accelerator は、デフォルトでデスクトップ プール用に有効になっています。この機能は、プールを作成または編集するときに無効または有効に設定できます。デスクトップ プールを初めて作成するときにこの機能を有効にすることをお勧めします。既存のプールを編集してこの機能を有効にする場合は、リンク クローンをプロビジョニングする前に、新しいレプリカとそのダイジェスト ディスクが作成されていることを確認する必要があります。新しいレプリカは、プールを新しいスナップショットに再構成するか、プールを新しいデータストアに再分散することによって作成できます。ダイジェスト ファイルは、デスクトップ プール内の仮想マシンがパワーオフされているときにのみ構成できます。

リンク クローンを含むデスクトップ プールと、フル仮想マシンを含むプールで View Storage Accelerator を有効にすることができます。

ネイティブ NFS スナップショット テクノロジー (VAAI) は、View Storage Accelerator 用に有効にされているプールでサポートされていません。

View Storage Accelerator は、Horizon 7 レプリカ階層を使用する構成で機能するようになり、レプリカはリンククローンでなく別のデータストアに保存されます。Horizon 7 レプリカ階層で View Storage Accelerator を使用するパフォーマンスの利点は実質的には大きくありませんが、特定の容量に関わる利点は別のデータストアにレプリカを保存することによって実現できる場合があります。したがって、この組み合わせがテストおよびサポートされません。

重要： この機能を使用する計画であり、いくつかの ESXi ホストを共有する複数の Horizon 7 ポッドを使用している場合は、共有 ESXi ホストのすべてのプールについて Horizon Storage Accelerator 機能を有効にする必要があります。複数ポッドの設定に一貫性がない場合は、共有 ESXi ホストの仮想マシンが不安定になることがあります。

前提条件

- vCenter Server ホストおよび ESXi ホストのバージョンが 5.1 以降であることを確認します。
ESXi クラスタで、すべてのホストのバージョンが 5.1 以降であることを確認します。
- vCenter Server の [ホスト] > [構成] > [詳細] 設定の権限が vCenter Server ユーザに割り当てられていることを確認します。
[vCenter Server、View Composer およびインスタント クローンのユーザー アカウントの構成](#)を参照してください。

手順

- 1 Horizon Administrator で、[ストレージ設定] ページの前に表示される [vCenter Server を追加] ウィザード ページを完了します。
 - a [View 構成] - [サーバ] の順に選択します。
 - b [vCenter Servers] タブで、[追加] をクリックします。
 - c [vCenter Server の情報] ページ、[View Composer 設定] ページ、[View Composer ドメイン] ページを完了します。
- 2 [ストレージ設定] ページで、[View Storage Accelerator を有効にする] チェック ボックスがオンになっていることを確認します。
デフォルトでは、このチェック ボックスはオンになっています。
- 3 デフォルトのホスト キャッシュ サイズを指定します。
デフォルトのキャッシュ サイズは、この vCenter Server インスタンスで管理されるすべての ESXi ホストに適用されます。
デフォルト値は 1,024 MB です。キャッシュ サイズは、100 MB ～ 2,048 MB の範囲でなければなりません。
- 4 個別の ESXi ホスト向けに別のキャッシュ サイズを指定するには、ESXi ホストを選択して、[キャッシュ サイズの編集] をクリックします。
 - a [ホスト キャッシュ] ダイアログ ボックスで、[デフォルトのホスト キャッシュ サイズを上書き] のチェック ボックスをオンにします。
 - b [ホスト キャッシュ サイズ] の値を 100 MB ～ 2,048 MB の範囲で入力し、[OK] をクリックします。
- 5 [ストレージ設定] ページで、[次へ] をクリックします。

6 [終了] をクリックして、vCenter Server、View Composer、ストレージ設定を Horizon 7 に追加します。

次のステップ

PCoIP Secure Gateway、安全なトンネル、クライアント接続用の外部 URL を構成するには、「[Horizon Client 接続の構成](#)」を参照してください。

Horizon 7 で View Storage Accelerator 設定を完了するには、デスクトップ プール用に View Storage Accelerator を構成します。『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 プール用に View Storage Accelerator を構成する」を参照してください。

vCenter Server と View Composer の同時操作の制限

vCenter Server を Horizon 7 に追加する場合、または vCenter Server 設定を編集する場合には、vCenter Server と View Composer で実行される同時操作の最大数を設定するオプションをいくつか構成できます。

これらのオプションは、[vCenter Server の情報] ページの [詳細設定] パネルで構成します。

表 9-3. vCenter Server と View Composer の同時操作の制限

設定	説明
[最大同時 vCenter プロビジョニング操作数]	<p>接続サーバがこの vCenter Server インスタンスでフル仮想マシンのプロビジョニングと削除のために出すことができる同時要求の最大数を指定します。</p> <p>デフォルト値は 20 です。</p> <p>この設定はフル仮想マシンにのみ適用されます。</p>
[最大同時電源操作数]	<p>この vCenter Server インスタンス内の接続サーバによって管理されている仮想マシンで同時に実行できる電源操作（起動、シャットダウン、サスペンドなど）の最大数を決定します。</p> <p>デフォルト値は 50 です。</p> <p>この設定の値を計算するためのガイドラインについては、リモート デスクトップ ログオン ストームをサポートするための同時電源操作レートの設定を参照してください。</p> <p>この設定は、フル仮想マシンとリンク クローンに適用されます。</p>
[最大同時 View Composer メンテナンス操作数]	<p>この View Composer インスタンスによって管理されているリンク クローンで同時に実行できる、View Composer の更新、再構成、再分散などの操作の最大数を決定します。</p> <p>デフォルト値は 12 です。</p> <p>メンテナンス操作を開始する前に、アクティブなセッションが存在するリモート デスクトップからログオフする必要があります。メンテナンス操作の開始直後にユーザーを強制的にログオフさせた場合、ログオフが必要なリモート デスクトップ上の同時操作の最大数は、構成値の半分になります。たとえば、この設定を 24 に構成して、ユーザーを強制的にログオフさせた場合、ログオフが必要なリモート デスクトップ上の同時操作の最大数は 12 です。</p> <p>この設定はリンク クローンにのみ適用されます。</p>
[最大同時 View Composer プロビジョニング操作数]	<p>この View Composer インスタンスによって管理されているリンク クローンで同時に実行できる作成および削除操作の最大数を指定します。</p> <p>デフォルト値は 8 です。</p> <p>この設定はリンク クローンにのみ適用されます。</p>

リモート デスクトップ ログオン ストームをサポートするための同時電源操作レートの設定

[最大同時電源操作数] 設定は、vCenter Server インスタンスのリモート デスクトップ仮想マシンで使用可能な同時電源操作の最大数を制御します。この最大数はデフォルトで 50 に設定されています。この値は、多くのユーザーが同時にデスクトップにログインするときのピーク時パワーオン率をサポートするように変更できます。

ベスト プラクティスとして、この設定の適切な値を判断するためにパイロット段階を実施できます。プランニングのガイドラインについては、『Horizon 7 アーキテクチャの計画』ドキュメントの「アーキテクチャ設計の要素と計画のガイドライン」を参照してください。

必要な同時電源操作の数は、デスクトップがパワーオンになるピーク率と、デスクトップがパワーオンになり、起動し、接続可能になるのに要する時間に基づきます。一般的に、推奨される電源操作の最大数は、デスクトップの開始に要した合計時間にピーク時パワーオン率を掛け合わせたものです。

たとえば、平均的なデスクトップは起動に 2 ～ 3 分要します。したがって、同時電源操作の最大数はピーク時パワーオン率の 3 倍にする必要があります。デフォルト設定の 50 は、毎分 16 台のデスクトップのピーク時パワーオン率をサポートできることを見込んでいます。

システムは、デスクトップが起動するまで最大 5 分待機します。起動にこれ以上の時間を要すると、他のエラーが発生する可能性があります。万一に備えて、同時電源操作の最大数をピーク時パワーオン率の 5 倍に設定できます。控えめに考えて、デフォルト設定の 50 は、毎分 10 台のデスクトップのピーク時パワーオン率をサポートします。

ログオン、つまりデスクトップのパワーオン操作は、通常、特定の時間範囲で正規分散されて行われます。時間範囲の中間にパワーオン操作が発生し、パワーオン操作の 40% が時間範囲の 6 分の 1 で発生すると仮定して、ピーク時パワーオン率を概算することができます。たとえば、ユーザーが午前 8:00 から午前 9:00 の間にログオンすると、時間範囲は 1 時間であり、ログオンの 40% は午前 8:25 から午前 8:35 までの 10 分間に発生します。ユーザーが 2,000 人いる場合、そのうち 20% がデスクトップをパワーオフしており、400 台のデスクトップのパワーオン操作の 40% がこの 10 分間に発生することになります。ピーク時パワーオン率は、毎分 16 台のデスクトップになります。

デフォルトの TLS 証明書のサムプリントを受け入れる

vCenter Server および View Composer インスタンスを Horizon 7 に追加する場合、vCenter Server および View Composer インスタンス用に使用される TLS 証明書が有効で、接続サーバによって信頼されていることを確認する必要があります。vCenter Server および View Composer でインストールされるデフォルトの証明書が存在する場合、これらの証明書のサムプリントを受け入れるかどうかを決定する必要があります。

vCenter Server または View Composer インスタンスが CA によって署名された証明書で構成され、ルート証明書が接続サーバによって信頼される場合、この証明書のサムプリントを受け入れる必要はありません。操作は何も必要ありません。

デフォルト証明書を CA によって署名された証明書に置換するにもかかわらず接続サーバがルート証明書を信頼していない場合、証明書のサムプリントを受け入れるかどうかを決定する必要があります。サムプリントとは、証明書の暗号化ハッシュです。サムプリントは、提示された証明書が以前に受け入れられた証明書など、別の証明書と同じものであるかどうかを素早く判別するために使用されます。

注： 同じ Windows Server ホストに vCenter Server と View Composer をインストールする場合、同じ TLS 証明書を使用できますが、各コンポーネントで証明書を個別に構成する必要があります。

TLS 証明書の構成方法については、[8 章 Horizon 7 Server 用の TLS 証明書の設定](#)を参照してください。

まず、Horizon Administrator で vCenter Server の追加ウィザードを使用して、vCenter Server と View Composer を追加します。証明書が信頼されておらず、サムプリントを受け入れなければ、vCenter Server および View Composer を追加できません。

これらのサーバが追加されたら、[vCenter Server の編集] ダイアログ ボックスで再構成できます。

注： 旧リリースからアップグレードする場合、そして vCenter Server または View Composer 証明書が信頼されていない場合、または信頼されている証明書を信頼されていない証明書と置き換える場合は、証明書のサムプリントを受け入れる必要もあります。

Horizon Administrator ダッシュボードで、vCenter Server または View Composer のアイコンが赤に変わり、[無効な証明書が検出されました] ダイアログ ボックスが表示されます。Horizon Administrator で、[View 構成] - [サーバ] の順にクリックし、View Composer サービスに関連付けられた vCenter Server のエントリを編集します。vCenter Server の設定で [編集] をクリックし、プロンプトに従って自己署名証明書を確認して同意します。

同様に Horizon Administrator では、接続サーバ インスタンスごとに使用する SAML 認証システムを構成できます。SAML サーバの証明書が接続サーバによって信頼されていない場合、証明書のサムプリントを受け入れるかどうかを決定する必要があります。サムプリントを受け入れなければ、Horizon 7 で SAML 認証システムを構成できません。SAML 認証システムが構成されると、[接続サーバの編集] ダイアログ ボックスで再構成できます。

手順

- 1 Horizon Administrator で [無効な証明書が検出されました] ダイアログ ボックスが表示されたら、[証明書を表示] をクリックします。
 - 2 [証明書情報] ウィンドウで証明書のサムプリントを調べます。
 - 3 vCenter Server または View Composer インスタンス用に構成された証明書のサムプリントを調べます。
 - a vCenter Server または View Composer ホストで、MMC スナップインを開始し、Windows 証明書ストアを開きます。
 - b vCenter Server または View Composer の証明書に移動します。
 - c [証明書の詳細] タブをクリックして証明書のサムプリントを表示します。

同様に、SAML 認証システムの証明書のサムプリントを調べます。必要に応じて、SAML 認証システム ホストで上記の手順を行います。
 - 4 [証明書情報] ウィンドウのサムプリント (two occurrences) が vCenter Server または View Composer インスタンスのサムプリント (two occurrences) と一致することを確認します。
- 同様に、SAML 認証システムについてもサムプリントが一致するかどうかを調べます。

5 証明書のサムプリントを受け入れるかどうかを決定します。

オプション	説明
サムプリントが一致しています。	[許可] をクリックしてデフォルト証明書を使用します。
サムプリントが一致していません。	[拒否] をクリックします。 一致しない証明書のトラブルシューティングを行います。たとえば、vCenter Server または View Composer で正しくない IP アドレスを指定した可能性があります。

Horizon Client 接続の構成

クライアント エンドポイントは、安全な接続を介して接続サーバ ホストまたはセキュリティ サーバ ホストと通信します。

ユーザー認証およびリモート デスクトップとアプリケーションの選択に使用されるクライアントの初期接続は、ユーザーが Horizon Client にドメイン名を入力したときに HTTPS を介して作成されます。ファイアウォールおよびロード バランシング ソフトウェアがネットワーク環境内で正しく構成されている場合、この要求は接続サーバ ホストまたはセキュリティ サーバ ホストに到達します。この接続ではユーザーが認証され、デスクトップまたはアプリケーションが選択されますが、ユーザーはまだリモート デスクトップまたはアプリケーションに接続されていません。

ユーザーがリモート デスクトップおよびアプリケーションに接続すると、クライアントはデフォルトで接続サーバ ホストまたはセキュリティ サーバ ホストへの接続を再度行います。この接続は、RDP などのデータを HTTPS 上で送信するための安全なトンネルになるため、トンネル接続と呼ばれます。

ユーザーが PCoIP 表示プロトコルを使用してリモート デスクトップおよびアプリケーションに接続した場合には、クライアントはさらに接続サーバ ホストまたはセキュリティ サーバ ホスト上の PCoIP Secure Gateway に接続することができます。PCoIP Secure Gateway は、認証されたユーザーのみが PCoIP 上でリモート デスクトップおよびアプリケーションとの通信を行えるようにします。

また、VMware Blast 表示プロトコルを使用してリモート デスクトップおよびアプリケーションに接続するユーザーと、HTML Access を使用してリモート デスクトップに接続する外部ユーザーに対して、安全な接続を提供することもできます。Blast Secure Gateway は、認証されたユーザーのみがリモート デスクトップとの通信を行えるようにします。

使用しているクライアント デバイスのタイプに応じて、クライアント デバイスに USB リダイレクト データなどの他のトラフィックを送信するために、追加のチャネルが確立されます。これらのデータ チャネルは、安全なトンネルが有効な場合は安全なトンネルにトラフィックをルーティングします。

安全なトンネルおよび安全なゲートウェイが無効になっていると、デスクトップおよびアプリケーション セッションが、接続サーバ ホストまたはセキュリティ サーバ ホストをバイパスして、クライアント デバイスとリモート マシンとの間で直接確立されるようになります。このタイプの接続を直接接続といいます。

直接接続を使用するデスクトップおよびアプリケーション セッションは、接続サーバが稼動しなくなっても、接続されたままになります。

通常、セキュリティ サーバ ホストまたは接続サーバ ホストに WAN 経由で接続する外部クライアントに対して安全な接続を提供するには、安全なトンネル、PCoIP Secure Gateway、および Blast Secure Gateway を有効にします。LAN 接続された内部クライアントがリモート デスクトップとアプリケーションに直接接続できるように、安全なトンネルと安全なゲートウェイを無効にすることができます。

安全なトンネルのみまたは安全なゲートウェイ 1 つのみを有効にする場合、使用しているクライアントのタイプによっては、セッションで一部のトラフィックに直接接続を使用する一方で、その他のトラフィックを接続サーバまたはセキュリティ サーバ ホストを経由して送信する可能性があります。

SSL は接続サーバおよびセキュリティ サーバ ホストへのすべてのクライアント接続に必要です。

PCoIP Secure Gateway および安全なトンネルの接続の構成

Horizon Administrator を使用して、安全なトンネルおよび PCoIP Secure Gateway の使用を構成します。これらのコンポーネントは、認証されたユーザーのみがリモート デスクトップおよびアプリケーションとの通信を行えるようにします。

PCoIP 表示プロトコルを使用するクライアントは、PCoIP Secure Gateway を使用できます。RDP 表示プロトコルを使用するクライアントは、安全なトンネルを使用できます。

Blast Secure Gateway の構成については、[Blast Secure Gateway の構成](#)を参照してください。

重要： 外部クライアントに安全な接続を提供する一般的なネットワーク構成には、セキュリティ サーバが含まれています。セキュリティ サーバで安全なトンネルおよび PCoIP Secure Gateway を有効または無効にするには、セキュリティ サーバとペアになっている Connection Server インスタンスを編集する必要があります。

外部クライアントが Connection Server ホストに直接接続するネットワーク構成では、Horizon Administrator で Connection Server インスタンスを編集して、安全なトンネルや PCoIP Secure Gateway を有効または無効にする必要があります。

前提条件

- PCoIP Secure Gateway を有効にする場合は、Connection Server インスタンスおよびペアのセキュリティ サーバが View 4.6 以降であることを確認します。
- PCoIP Secure Gateway をすでに有効にしている Connection Server インスタンスに対してセキュリティ サーバをペアにする場合は、セキュリティ サーバが View 4.6 以降であることを確認します。

手順

- 1 Horizon Administrator で、[View 構成] - [サーバ] を選択します。
- 2 [Connection Server] パネルで、Connection Server インスタンスを選択して [編集] をクリックします。
- 3 安全なトンネルの使用を設定します。

オプション	説明
安全なトンネルを無効にする	[マシンへの安全なトンネル接続を使用する] の選択を解除します。
安全なトンネルを有効にする	[マシンへの安全なトンネル接続を使用する] を選択します。

デフォルトでは、安全なトンネルは有効になっています。

4 PColP Secure Gateway の使用を設定します。

オプション	説明
PCoIP Secure Gateway を有効にする	[マシンへの PCoIP 接続に PCoIP Secure Gateway を使用する] を選択します。
PCoIP Secure Gateway を無効にする	[マシンへの PCoIP 接続に PCoIP Secure Gateway を使用する] の選択を解除します。

デフォルトでは、PCoIP Secure Gateway は無効になっています。

5 [OK] をクリックして変更を保存します。

Blast Secure Gateway の構成

Horizon Administrator では、HTML Access、または VMware Blast 表示プロトコルを使用するクライアント接続を介してリモート デスクトップおよびアプリケーションに安全にアクセスできるように、Blast Secure Gateway の使用を構成できます。

Blast Secure Gateway には Blast Extreme Adaptive Transport (BEAT) ネットワークが含まれています。これは、速度の変化やパケット損失などのネットワーク状態に動的に適合します。

- Blast Secure Gateway は、Unified Access Gateway アプライアンスで実行されている場合にのみ、BEAT ネットワークをサポートします。
- Unified Access Gateway アプライアンス バージョン 3.3 以降に接続している場合、IPv4 を使用する Horizon Client と IPv6 を使用する Horizon Client を TCP ポート 8443 と UDP ポート 8443 (BEAT 用) で同時に処理できます。
- 一般的なネットワーク状態では、Horizon Client を接続サーバ (BSG 無効)、セキュリティ サーバ (BSG 無効) またはバージョン 2.8 以降の Unified Access Gateway アプライアンスに接続する必要があります。一般的なネットワーク状態で Horizon Client を接続サーバ (BSG 有効)、セキュリティ サーバ (BSG 有効) またはバージョン 2.8 より前の Unified Access Gateway アプライアンスに接続すると、クライアントはネットワーク状態を自動的に感知し、TCP ネットワークに戻ります。
- ネットワーク状態が良好でない場合、Horizon Client はバージョン 2.9 以降の Unified Access Gateway アプライアンス (UDP トンネル サーバ有効) に接続する必要があります。ネットワーク状態が良好でないときに Horizon Client を接続サーバ (BSG 有効)、セキュリティ サーバ (BSG 有効) またはバージョン 2.8 より前の Unified Access Gateway アプライアンスに接続すると、クライアントはネットワーク状態を自動的に感知し、TCP ネットワークに戻ります。
- ネットワーク状態が良好でないときに、Horizon Client を接続サーバ (BSG 無効)、セキュリティ サーバ (BSG 無効)、バージョン 2.9 以降の Unified Access Gateway アプライアンス (UDP トンネル サーバ無効) またはバージョン 2.8 の Unified Access Gateway アプライアンスに接続すると、クライアントはネットワーク状態を自動的に感知し、一般的なネットワーク状態に戻ります。

詳細については、<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。

注： また、セキュリティ サーバではなく、Unified Access Gateway アプライアンスを使用して、Horizon 7 サーバおよびデスクトップに安全に外部アクセスすることもできます。Unified Access Gateway アプライアンスを使用する場合、接続サーバ インスタンスで Secure Gateway を無効にして、これらのゲートウェイを Unified Access Gateway アプライアンスで有効にする必要があります。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。

Blast Secure Gateway が有効になっていない場合、クライアント デバイスおよびクライアント Web ブラウザは、VMware Blast Extreme プロトコルを使用して、リモート デスクトップ仮想マシンおよびアプリケーションに直接接続することで、Blast Secure Gateway をバイパスします。

重要： 外部ユーザーに安全な接続を提供する一般的なネットワーク構成には、セキュリティ サーバが含まれています。セキュリティ サーバで Blast Secure Gateway を有効または無効にするには、セキュリティ サーバとペアになっている接続サーバ インスタンスを編集する必要があります。外部ユーザーが接続サーバ ホストに直接接続する場合、その接続サーバ インスタンスを編集して Blast Secure Gateway を有効または無効にします。

前提条件

ユーザーが VMware Identity Manager を使用してリモート デスクトップを選択する場合、VMware Identity Manager がインストールされ、接続サーバで使用するために構成されており、接続サーバが SAML 2.0 認証サーバとペアになっていることを確認します。

手順

- 1 Horizon Administrator で、[View 構成] - [サーバ] を選択します。
- 2 [接続サーバ] タブで、接続サーバ インスタンスを選択して [編集] をクリックします。
- 3 Blast Secure Gateway の使用を構成します。

オプション	説明
Blast Secure Gateway を有効にする	[Blast Secure Gateway を使用してマシンに Blast 接続する] を選択します。
HTML Access に Blast Secure Gateway を有効にする	[HTML Access とマシンの Blast 接続にのみ Blast Secure Gateway を使用する] を選択します。
Blast Secure Gateway を無効にする	[Blast Secure Gateway を使用しない] を選択します。

Blast Secure Gateway はデフォルトで有効になります。

- 4 [OK] をクリックして変更を保存します。

Secure Gateway 接続およびトンネル接続用の外部 URL の構成

クライアント システムで安全なトンネルを使用するには、クライアントから接続サーバ ホストまたはセキュリティ サーバ ホストに到達できるようにするための IP アドレスまたは IP アドレスに解決可能な完全修飾ドメイン名 (FQDN) に、クライアント システムがアクセスする必要があります。

PCoIP Secure Gateway を使用するには、クライアントは接続サーバまたは URL を使用してセキュリティ サーバ ホストに接続します。IPv4 環境では、ホストを特定する URL に IP アドレスを使用する必要があります。IPv6 環境では、ホストを特定する URL に IP アドレスまたは FQDN のいずれかを使用できます。

Blast Secure Gateway を使用するには、ユーザーの Web ブラウザまたはコンピュータで接続サーバまたはセキュリティ サーバ ホストに到達できるようにする IP アドレスに解決できる FQDN に、ユーザーのエンドポイント デバイスでアクセスする必要があります。

外部からのトンネル接続の使用

デフォルトでは、接続サーバ ホストまたはセキュリティ サーバ ホストに接続できるクライアントは、同じネットワーク内に存在して要求されたホストを検出できるトンネル クライアントだけです。

多くの組織では、特定の IP アドレスまたはクライアントで解決可能なドメイン名と特定のポートを使用して、ユーザーが外部から接続できる必要があります。この情報は、接続サーバ ホストまたはセキュリティ サーバ ホストの実際のアドレスやポート番号に似ている場合も、似ていない場合もあります。この情報は、URL の形式でクライアント システムに提供されます。例：

- `https://view-example.com:443`
- `https://view.example.com:443`
- `https://example.com:1234`
- `https://10.20.30.40:443`

このようなアドレスを Horizon 7 で使用するには、ホストの FQDN ではなく外部 URL を返すように接続サーバまたはセキュリティ サーバ ホストを構成する必要があります。

外部 URL の構成

複数の外部 URL を構成します。1 つは、クライアント システムがトンネル接続を行えるようにするための URL です。もう 1 つは、PCoIP を使用するクライアントが PCoIP Secure Gateway 経由で安全な接続を行えるようにするための URL です。IPv4 環境では、ホストを特定する URL に IP アドレスを使用する必要があります。IPv6 環境では、ホストを特定する URL に IP アドレスまたは FQDN のいずれかを使用できます。この URL を使用すると、クライアントは外部の場所から接続が可能になります。

さらにもう 1 つは、クライアント デバイスまたは Web ブラウザから Blast Secure Gateway 経由で安全な接続を行えるようにするための URL です。

ネットワーク構成にセキュリティ サーバが含まれている場合は、セキュリティ サーバの外部 URL を提供します。セキュリティ サーバとペアになっている接続サーバ インスタンスの外部 URL は必要ありません。

外部 URL を設定する方法は、接続サーバ インスタンスとセキュリティ サーバでは異なります。

- 接続サーバ インスタンスの場合は、Horizon Administrator で接続サーバの設定を編集して外部 URL を設定します。
- セキュリティ サーバの場合は、接続サーバのインストール プログラムを実行するときに外部 URL を設定します。セキュリティ サーバの外部 URL を変更するには、Horizon Administrator を使用できます。

Connection Server インスタンスの外部 URL を設定する

Connection Server インスタンスの外部 URL を設定するには、Horizon Administrator を使用します。

安全なトンネルの外部 URL、PCoIP 外部 URL、および Blast 外部 URL は、この Connection Server に到達するためにクライアント システムで使用されるアドレスでなければなりません。

前提条件

- 安全なトンネル接続と PCoIP Secure Gateway が Connection Server インスタンス上で有効になっていることを確認します。[PCoIP Secure Gateway および安全なトンネルの接続の構成](#)を参照してください。
- Blast 外部 URL を設定するには、Blast Secure Gateway が Connection Server インスタンス上で有効になっていることを確認します。[Blast Secure Gateway の構成](#)を参照してください。

手順

- 1 Horizon Administrator で、[View 構成] - [サーバ] の順にクリックします。
- 2 [Connection Server] タブで、Connection Server インスタンスを選択して [編集] をクリックします。
- 3 [外部 URL] テキスト ボックスに安全なトンネルの外部 URL を入力します。

URL には、プロトコル、クライアントで解決可能なホスト名、およびポート番号が含まれている必要があります。

例 : `https://myserver.example.com:443`

注： ホスト名が解決できないときに Connection Server インスタンスにアクセスする必要がある場合は、IP アドレスを使用できます。ただし、通信するホストは、Connection Server インスタンスに対して構成された TLS 証明書に一致しないため、アクセスがブロックされたりアクセスのセキュリティが低下したりします。

- 4 [PCoIP 外部 URL] テキスト ボックスに、PCoIP Secure Gateway の外部 URL を入力します。

IPv4 環境では、PCoIP 外部 URL を IP アドレスとポート番号 4172 で指定します。IPv6 環境では、IP アドレスまたは完全修飾ドメイン名とポート番号 4172 を指定できます。いずれの場合も、プロトコル名を含めないでください。

IPv4 環境の例 : `10.20.30.40:4172`

クライアントは URL を使用してセキュリティ サーバにアクセスできる必要があります。

- 5 [Blast 外部 URL] テキスト ボックスに Blast Secure Gateway の外部 URL を入力します。

URL には、HTTPS プロトコル、クライアントが解決可能なホスト名、およびポート番号が含まれている必要があります。

例 : `https://myserver.example.com:8443`

デフォルトでは、URL には安全なトンネル外部 URL の FQDN およびデフォルトのポート番号 8443 が含まれます。URL には、この Connection Server ホストに到達するためにクライアント システムで使用できる FQDN とポート番号を含める必要があります。

- 6 このダイアログのすべてのアドレスによって、クライアント システムがこの Connection Server インスタンスに到達できることを確認します。
- 7 [OK] をクリックします。

セキュリティ サーバの外部 URL を変更する

セキュリティ サーバの外部 URL を変更するには、Horizon Administrator を使用します。

接続サーバ インストール プログラムにセキュリティ サーバをインストールする場合、最初にこれらの外部 URL を設定します。

安全なトンネルの外部 URL、PCoIP 外部 URL、および Blast 外部 URL は、このセキュリティ サーバに到達するためにクライアント システムで使用されるアドレスでなければなりません。

前提条件

- 安全なトンネル接続と PCoIP Secure Gateway が、このセキュリティ サーバとペアになっている接続サーバ インスタンス上で有効になっていることを確認します。[PCoIP Secure Gateway および安全なトンネルの接続の構成](#)を参照してください。
- Blast 外部 URL を設定するには、Blast Secure Gateway が、このセキュリティ サーバとペアになっている接続サーバ インスタンス上で有効になっていることを確認します。[Blast Secure Gateway の構成](#)を参照してください。

手順

- 1 Horizon Administrator で、[View 構成] - [サーバ] を選択します。
- 2 [セキュリティ サーバ] タブを選択し、セキュリティ サーバを選択して、[編集] をクリックします。
- 3 [外部 URL] テキスト ボックスに安全なトンネルの外部 URL を入力します。

URL には、プロトコル、クライアントで解決可能なセキュリティ サーバのホスト名およびポート番号が含まれている必要があります。

例 : `https://myserver.example.com:443`

注： ホスト名が解決できないときにセキュリティ サーバにアクセスする必要がある場合は、IP アドレスを使用できます。ただし、通信するホストは、セキュリティ サーバ用に構成されている TLS 証明書に対応していないため、アクセスがブロックされたりアクセスのセキュリティが低下したりします。

- 4 [PCoIP 外部 URL] テキスト ボックスに、PCoIP Secure Gateway の外部 URL を入力します。
- IPv4 環境では、PCoIP 外部 URL を IP アドレスとポート番号 4172 で指定します。IPv6 環境では、IP アドレスまたはドメイン名とポート番号 4172 を指定できます。いずれの場合も、プロトコル名を含めないでください。

IPv4 環境の例 : `10.20.30.40:4172`

クライアントは URL を使用してセキュリティ サーバにアクセスできる必要があります。

- 5 [Blast 外部 URL] テキスト ボックスに Blast Secure Gateway の外部 URL を入力します。

URL には、HTTPS プロトコル、クライアントが解決可能なホスト名、およびポート番号が含まれている必要があります。

例 : `https://myserver.example.com:8443`

デフォルトでは、URL に安全な外部 URL の FQDN とデフォルトのポート番号 8443 が含まれています。URL には、このセキュリティ サーバに到達するためにクライアント システムで使用できる FQDN とポート番号を含める必要があります。

- 6 このダイアログのすべてのアドレスでクライアント システムがこのセキュリティ サーバ ホストに到達できることを確認します。
- 7 [OK] をクリックして変更を保存します。

結果

Horizon Administrator が、更新された外部 URL をセキュリティ サーバに送信します。変更を有効にするためにセキュリティ サーバ サービスを再起動する必要はありません。

Horizon 接続サーバがアドレス情報を返したときに DNS 名を優先

デフォルトでは、デスクトップ マシンと RDS のアドレスをクライアントとゲートウェイに送信するときに、IP アドレスが Horizon 接続サーバで優先されます。この Horizon 7 LDAP 属性のデフォルト動作は、Horizon 接続サーバで DNS 名を優先するように変更できます。特定の環境では、接続サーバが DNS 名をクライアントとゲートウェイに返すことがネットワーク インフラストラクチャ設計の柔軟性の向上につながる場合があります。

注： この Horizon 7 LDAP 属性は、Horizon 6.0.x 以前のリリースのグループ ポリシー設定、Connect using DNS Name で指定されていたデスクトップごとの機能を置き換えます。

Horizon 7 LDAP 属性は、接続サーバ インスタンス（セキュリティ サーバ以外）上で Horizon Client 3.3 for Windows 以降、HTML Access 3.5 以降、および Secure Gateway を実行しているクライアントに影響します。

前提条件

お使いのバージョンの Windows Server オペレーティング システムでの ADSI Edit ユーティリティの使用方法については、Microsoft TechNet Web サイトを参照してください。

手順

- 1 接続サーバ コンピュータで ADSI Edit ユーティリティを起動します。
- 2 コンソール ツリーで、[接続] を選択します。
- 3 [識別名または命名規則を選択または入力] テキスト ボックスに、識別名「[DC=vdi, DC=vmware, DC=int]」を入力します。
- 4 [ドメインまたはサーバを選択または入力] テキスト ボックスで、**localhost:389** を選択または入力するか、接続サーバ コンピュータの完全修飾ドメイン名 (FQDN) を入力し、続いてポート 389 を入力します。

たとえば：localhost:389 または mycomputer.mydomain.com:389
- 5 オブジェクト [CN=Common, OU=Global, OU=Properties] で、[pae-PreferDNS] 属性の値を 1 に設定します。

この属性を 1 に設定すると、接続サーバは、DNS 名が使用可能で受信者が名前を解決できる場合に、DNS 名を返します。そうでない場合、接続サーバは、お使いの環境（IPv4 または IPv6）で適切なタイプの IP アドレスが使用可能な場合に、IP アドレスを返します。

この属性を設定しないか、0 に設定すると、接続サーバは、適切なタイプの IP アドレスが使用可能な場合に、IP アドレスを返します。そうでない場合、IP アドレスの互換性エラーが返されます。

ロード バランサでの HTML Access の許可

ロード バランサまたはロード バランシングされたゲートウェイのすぐ後ろに存在する接続サーバ インスタンスおよびセキュリティ サーバは、ユーザーが HTML Access を使用するときブラウザがロード バランサへの接続で使用するアドレスを知っている必要があります。

ゲートウェイのすぐ後ろに直接存在する接続サーバ インスタンスおよびセキュリティ サーバについては、[ゲートウェイでの HTML Access の許可](#) で説明する手順を実行します。

ロード バランサまたはロード バランシングされたゲートウェイの背後に存在する各 Horizon 7 サーバについて、この手順を実行する必要があります。

手順

- 1 接続サーバ ホストまたはセキュリティ サーバ ホスト上で、SSL ゲートウェイ構成フォルダ内の `locked.properties` ファイルを作成または編集します。

例: `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`
- 2 `balancedHost` プロパティを追加し、これにロード バランサのアドレスを設定します。

たとえば、ユーザーがロード バランシングされた Horizon 7 サーバのいずれかに到達するためにブラウザに `https://view.example.com` と入力する場合は、`locked.properties` ファイルに `balancedHost=view.example.com` を追加します。
- 3 `locked.properties` ファイルを保存します。
- 4 変更を反映するため、接続サーバ サービスまたはセキュリティ サーバ サービスを再起動してください。

ゲートウェイでの HTML Access の許可

Access Point などのゲートウェイのすぐ後ろに存在する接続サーバ インスタンスおよびセキュリティ サーバは、ユーザーが HTML Access を使用するときブラウザがゲートウェイへの接続で使用するアドレスを知っている必要があります。

ロードバランサまたはロード バランシングされたゲートウェイの背後に存在する接続サーバ インスタンスおよびセキュリティ サーバについては、[ロード バランサでの HTML Access の許可](#)で説明する手順を実行します。

ゲートウェイの後ろに存在する各 Horizon 7 サーバについて、この手順を実行する必要があります。

手順

- 1 接続サーバ ホストまたはセキュリティ サーバ ホスト上で、SSL ゲートウェイ構成フォルダ内の `locked.properties` ファイルを作成または編集します。

例: `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`

- 2 `portalHost` プロパティを追加し、これにゲートウェイのアドレスを設定します。

たとえば、ブラウザがゲートウェイを通じて Horizon 7 にアクセスするために使用するアドレスが `https://view-gateway.example.com` である場合には、`portalHost=view-gateway.example.com` を `locked.properties` ファイルに追加します。

接続サーバ インスタンスまたはセキュリティ サーバが複数のゲートウェイの背後に存在する場合は、次のように `portalHost` プロパティに数字を追加することによって、各ゲートウェイを指定できます。

```
portalHost.1=view-gateway-1.example.com
portalHost.2=view-gateway-2.example.com
```

1 つのゲートウェイ マシンが複数の名前で見られている場合には、複数の `portalHost` プロパティを指定する必要もあります。

- 3 `locked.properties` ファイルを保存します。
- 4 変更を反映するため、接続サーバ サービスまたはセキュリティ サーバ サービスを再起動してください。

Horizon 7 サービスのデフォルト ポートの置換

インストール時、View サービスは、デフォルトで特定のネットワーク ポートでリッスンするように設定されます。組織によっては、組織のポリシーを遵守するため、または競合を回避するために、これらのポートを変更する必要があります。接続サーバ、セキュリティ サーバ、PCoIP Secure Gateway、および View Composer サービスが使用するデフォルト ポートを変更できます。

ポートの変更は、任意の設定タスクです。展開でデフォルト ポートを変更する必要がない場合は、そのまま使用します。

Horizon 7 サーバがデフォルトで使用する TCP ポートと UDP ポートについては、『Horizon 7 のセキュリティ』ドキュメントを参照してください。

Horizon 接続サーバ インスタンスおよびセキュリティ サーバのデフォルト HTTP ポートまたは NIC を置換する

サーバ コンピュータの `locked.properties` ファイルを編集して、接続サーバ インスタンスまたはセキュリティ サーバのデフォルト HTTP ポートまたは NIC を置換できます。組織によっては、組織のポリシーに遵守するため、または競合を回避するために、これらのタスクの実行を必須にしていることがあります。

デフォルトの SSL ポートは 443 です。デフォルトの非 SSL ポートは 80 です。

安全なトンネルの外部 URL で指定されているポートは、この手順でポートを変更しても変更されることはありません。ネットワーク構成によっては、安全なトンネルの 外部 URL ポートも変更しなければならないことがあります。

サーバ コンピュータに複数の NIC がある場合は、コンピュータはデフォルトですべての NIC でリッスンします。構成されているポート上でリッスンするための NIC を 1 つ選択するには、その NIC にバインドされている IP アドレスを指定します。

インストール時に、Horizon 7 は、必要なデフォルト ポートを開くように Windows ファイアウォールを構成します。ポート番号またはリッスンで使用する NIC を変更した場合は、更新されたポートを開きクライアント デバイスがサーバに接続できるように、Windows ファイアウォールを手動で再構成する必要があります。

SSL ポート番号を変更して、HTTP リダイレクトを引き続き動作させる必要がある場合は、HTTP リダイレクトのポート番号も変更する必要があります。[接続サーバへの HTTP リダイレクト用のポート番号を変更](#)を参照してください。

前提条件

この手順でポートを変更した後も、この接続サーバ インスタンスまたはセキュリティ サーバの外部 URL で指定されているポートが引き続き有効になっていることを確認します。

手順

- 1 接続サーバ ホストまたはセキュリティ サーバ コンピュータ上で、SSL ゲートウェイ構成フォルダ内の `locked.properties` ファイルを作成または編集します。

例 : `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`
`locked.properties` ファイルのプロパティは、大文字と小文字が区別されます。

- 2 `locked.properties` ファイルに、`serverPort` または `serverPortNonSsl` プロパティ、あるいは両方のプロパティを追加します。

例 :

```
serverPort=4443
serverPortNonSsl=8080
```

- 3 (オプション) サーバ コンピュータに複数の NIC がある場合は、構成されているポート上でリッスンするための NIC を 1 つ選択します。

`serverHost` および `serverHostNonSsl` プロパティを追加して、選択された NIC にバインドされている IP アドレスを指定します。

例 :

```
serverHost=10.20.30.40
serverHostNonSsl=10.20.30.40
```

通常、SSL および非 SSL リスナは、どちらも同じ NIC を使用するように構成されています。ただし、`serverProtocol=http` プロパティを使用して、クライアント接続用の SSL をオフロードする場合、`serverHost` プロパティを個別の NIC に設定し、Horizon Administrator の起動に使用されるシステムへの SSL 接続を実現できます。

同じ NIC を使用するように SSL および非 SSL 接続を構成する場合は、SSL と非 SSL ポートは同一にしないでください。

- 4 変更を反映するため、接続サーバ サービスまたはセキュリティ サーバ サービスを再起動してください。

次のステップ

必要に応じて、更新されたポートを開くように Windows ファイアウォールを手動で構成します。

Horizon 接続サーバ インスタンスおよびセキュリティ サーバ上の PCoIP Secure Gateway のデフォルト ポートまたは NIC を置換する

接続サーバ インスタンスまたはセキュリティ サーバ上で動作している PCoIP Secure Gateway サービスによって使用されるデフォルト ポートまたは NIC を置換できます。組織によっては、組織のポリシーに遵守するため、または競合を回避するために、これらのタスクの実行を必須にしていることがあります。

クライアントが接続する TCP および UDP 接続の場合は、PCoIP Secure Gateway はデフォルトでポート 4172 でリッスンします。リモート デスクトップへの UDP 接続の場合は、PCoIP Secure Gateway はデフォルトでポート 55000 でリッスンします。

PCoIP 外部 URL で指定されているポートは、この手順でポートを変更しても変更されることはありません。ネットワーク構成によっては、PCoIP 外部 URL ポートも変更しなければならないことがあります。

PCoIP Secure Gateway が動作しているコンピュータに複数の NIC がある場合は、コンピュータはデフォルトですべての NIC 上でリッスンします。構成されているポート上でリッスンするための NIC を 1 つ選択するには、その NIC にバインドされている IP アドレスを指定します。

前提条件

この手順でポートを変更した後も、接続サーバ インスタンスまたはセキュリティ サーバ上の PCoIP 外部 URL で指定されているポートが引き続き有効になっていることを確認します。

手順

- 1 PCoIP Secure Gateway が動作している接続サーバまたはセキュリティ サーバ コンピュータ上で Windows レジストリ エディタを起動します。
- 2 HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway レジストリ キーに移動します。
- 3 このレジストリ キーに、次の文字列 (REG_SZ) 値の 1 つ以上を更新されたポート番号とともに追加します。

例：

```
ExternalTCPPort "44172"
ExternalUDPPort "44172"
InternalUDPPort "55111"
```

- 4 (オプション) PCoIP Secure Gateway が動作しているコンピュータに複数の NIC がある場合は、構成されているポート上でリッスンするための NIC を 1 つ選択します。

同じレジストリ キーに、次の文字列 (REG_SZ) 値を追加して、選択された NIC にバインドされている IP アドレスを指定します。

例：

```
ExternalBindIP "10.20.30.40"
InternalBindIP "172.16.17.18"
```

同じ NIC を使用するように外部および内部接続を構成する場合は、外部と内部の UDP ポートは同一にしないでください。

- 5 VMware Horizon View PCoIP Secure Gateway サービスを再起動して、変更を有効にします。

接続サーバ インスタンスおよびセキュリティ サーバ上の PCoIP Secure Gateway のデフォルト制御ポートを置換

接続サーバ インスタンスまたはセキュリティ サーバ上で動作している PCoIP Secure Gateway (PSG) サービスを制御するデフォルト ポートを置換できます。ポートの競合を回避するために、この操作が必要になる場合があります。

デフォルトでは、PCoIP Secure Gateway はローカル TCP ポート 50060 で制御接続を待機します。

手順

- 1 PCoIP Secure Gateway が動作している接続サーバまたはセキュリティ サーバの SSL ゲートウェイ設定フォルダに `locked.properties` ファイルを作成し、編集します。

例: `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`
`locked.properties` ファイルのプロパティは、大文字と小文字が区別されます。

- 2 `locked.properties` ファイルに `psgControlPort` プロパティを追加します。

例:

```
psgControlPort=52060
```

- 3 同じマシンで Windows レジストリ エディタを起動します。
- 4 `HKEY_LOCAL_MACHINE\SOFTWARE\Teradici\SecurityGateway` レジストリ キーに移動します。
- 5 このレジストリ キーで、次の文字列値 (`REG_SZ`) と更新したポート番号を追加します。

例:

```
TCPControlPort "52060"
```

注: `TCPControlPort` のポート番号は、`psgControlPort` のポート番号と同じです。

- 6 変更を反映するため、接続サーバ サービスまたはセキュリティ サーバ サービスを再起動してください。

View Composer のデフォルト ポートを置換する

View Composer サービスで使用される SSL 証明書は、デフォルトで特定のポートにバインドされています。`SviConfig ChangeCertificateBindingPort` ユーティリティを使用すると、デフォルト ポートを置換できます。

`SviConfig ChangeCertificateBindingPort` ユーティリティを使用して新しいポートを指定する場合、ユーティリティは、View Composer 証明書を現在のポートからアンバインドし、新しいポートにバインドします。

インストール時に、View Composer は、必要なデフォルト ポートを開くように Windows ファイアウォールを構成します。ポートを変更した場合、更新されたポートを開くように Windows ファイアウォールを手動で再構成し、View Composer サービスへの接続を確保する必要があります。

前提条件

指定したポートが利用できることを確認します。

手順

- 1 View Composer サービスを停止します。
- 2 View Composer がインストールされている Windows Server ホストでコマンド プロンプトを開きます。
- 3 SviConfig 実行可能ファイルに移動します。

このファイルは、View Composer アプリケーションと同じ場所にあります。デフォルト パスは C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe です。

- 4 SviConfig ChangeCertificateBindingPort コマンドを入力します。

例：

```
sviconfig -operation=ChangeCertificateBindingPort
          -Port=ポート番号
```

ここで、-port=*port number* は、View Composer が証明書をバインドする新しいポートです。-port=*port number* パラメータは必須です。

- 5 View Composer サービスを再起動して変更を有効にします。

次のステップ

必要に応じて、更新されたポートを開くように、View Composer server 上の Windows ファイアウォールを手動で再構成します。

接続サーバへの HTTP リダイレクト用のポート番号を変更

Horizon 7 サーバのデフォルト ポート 443 を置き換えて、ポート 80 に接続を試みる Horizon Client に HTTP リダイレクトを許可したい場合、Horizon 7 サーバの `locked.properties` ファイルで設定する必要があります。

注： この手順は、SSL を中間デバイスにオフロードしても効果はありません。SSL オフロードがインプレースで、Horizon 7 サーバの HTTP ポートはサービスをクライアントに提供します。

前提条件

デフォルトのポート番号を 443 から変更したことを確認します。インストール中に構成されるデフォルト値を使用する場合、この手順を実行して HTTP リダイレクト規則を保持する必要はありません。

手順

- 1 接続サーバ ホストまたはセキュリティ サーバ コンピュータ上で、SSL ゲートウェイ構成フォルダ内の `locked.properties` ファイルを作成または編集します。

例：`install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`
`locked.properties` ファイルのプロパティは、大文字と小文字が区別されます。

- 2 以下の行を `locked.properties` ファイルに追加します:

```
frontMappingHttpDisabled.1=5:*:moved:https::port
frontMappingHttpDisabled.2=3:/error/*:file:docroot
frontMappingHttpDisabled.3=1:/admin*:missing
frontMappingHttpDisabled.4=1:/view-vlsi*:missing
```

前行の変数 *port* は、クライアントが接続するポート番号です。

前行を追加しなければ、*port* は 443 のままです。

- 3 変更を反映するため、接続サーバ サービスまたはセキュリティ サーバ サービスを再起動してください。

接続サーバへのクライアント接続で HTTP リダイレクトを防止

HTTP 上での Horizon 7 サーバへの Horizon Client による接続は、HTTPS にサイレントでリダイレクトされます。一部の導入では、Web ブラウザでユーザーが **http://** を入力できないようにして、強制的に HTTPS を使用するようにしたい場合があります。Horizon Client に対して HTTP リダイレクトを防止するには、Horizon 7 サーバの `locked.properties` ファイルで設定する必要があります。

注： この手順は、SSL を中間デバイスにオフロードしても効果はありません。SSL オフロードがインプレースで、Horizon 7 サーバの HTTP ポートはサービスをクライアントに提供します。

手順

- 1 接続サーバ ホストまたはセキュリティ サーバ コンピュータ上で、SSL ゲートウェイ構成フォルダ内の `locked.properties` ファイルを作成または編集します。

例: `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`
`locked.properties` ファイルのプロパティは、大文字と小文字が区別されます。

- 2 以下の行を `locked.properties` ファイルに追加します:

```
frontMappingHttpDisabled.1=5:*:missing
frontMappingHttpDisabled.2=3:/error/*:file:docroot
```

- 3 変更を反映するため、接続サーバ サービスまたはセキュリティ サーバ サービスを再起動してください。

接続サーバ上での Horizon 7 パフォーマンス カウンタへのリモート アクセスの有効化

Horizon 7 パフォーマンス カウンタは接続サーバ上でローカルに使用できますが、他のコンピュータからアクセスすると 0 を返します。接続サーバ上で Horizon 7 パフォーマンス カウンタへのリモート アクセスを有効にするには、レジストリで接続サーバのフレームワーク ポートを構成する必要があります。

手順

- 1 Windows レジストリ エディタを開始します。
- 2 HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Node Manager レジストリ キーに移動します。

3 新しい文字列 (REG_SZ) 値 Management Port を追加します。

4 Management Port 値を **32111** に設定します。

展開の規模に合わせた Windows Server 設定の調整

リモート デスクトップの大規模な展開をサポートするため、接続サーバをインストールする Windows Server コンピュータを構成できます。コンピュータごとに、Windows ページ ファイルのサイズを調整できます。

Windows Server 2008 R2 および Windows Server 2012 R2 コンピュータの場合、エフェメラル ポート、TCB ハッシュ テーブル、および Java 仮想マシンの設定値はデフォルトでサイズ調整されます。これらの調整により、予想されるユーザー負荷のもとで正常に動作するための適切なリソースをコンピュータが確保します。

Horizon 接続サーバ用メモリのサイズ設定

接続サーバ コンピュータで、50 台より多くのリモート デスクトップを展開するには、10GB のメモリが必要です。10GB 以上のメモリを持つ Windows Server コンピュータは、接続サーバがサポートできる最大数である、約 2,000 の同時トンネル セッションをサポートするように自動的に構成されます。

10GB 未満のメモリは、小規模の概念実証の展開の場合にのみ構成します。4GB という必要最小メモリの構成では、約 500 の同時トンネル セッションをサポートでき、小規模の概念実証の展開をサポートするには十分です。

しかし、展開は、より多くのユーザーが環境に追加されるに従って大きくなる可能性があるため、VMware では常に 10GB 以上のメモリを構成することを推奨しています。環境が大きくなり、メモリが入手できないと分かっている場合に限り、例外とします。

接続サーバを 10GB 未満のメモリでインストールすると、インストール完了後に、Horizon 7 によって警告メッセージが生成され、推奨メモリに関する情報が表示されます。12 時間ごとにイベントがトリガされ、接続サーバ インスタンスが小容量の物理メモリで構成されていることが通知されます。

より大規模な展開をサポートするためにコンピュータのメモリを 10GB に増設する場合は、接続サーバを再起動して、JVM ヒープ サイズが自動的に推奨値に増やされたことを確認します。接続サーバを再インストールする必要はありません。

重要： 64 ビットの Windows Server コンピュータでは、JVM ヒープ サイズを変更しないでください。この値を変更すると、接続サーバの動作が不安定になる可能性があります。64 ビットのコンピュータでは、接続サーバのサービスが物理メモリに合わせて JVM ヒープ サイズを設定します。

接続サーバの追加のハードウェアおよびメモリ要件については、[Horizon 接続サーバのハードウェア要件](#)を参照してください。

大規模な展開で接続サーバを使用する場合のハードウェアおよびメモリの推奨構成については、『Horizon 7 アーキテクチャの計画』の「接続サーバの最大接続数と仮想マシン構成」を参照してください。

システム ページ ファイルの設定を構成する

接続サーバ インスタンスがインストールされている Windows Server コンピュータの仮想メモリを、システム ページ ファイルの設定を変更することで最適化できます。

Windows Server をインストールするとき、Windows はコンピュータに搭載されている物理メモリに基づいてページ ファイルの初期サイズと最大サイズを計算します。これらのデフォルト設定は、コンピュータを再起動しても変わらず維持されます。

Windows Server コンピュータが仮想マシンの場合は、vCenter Server を使用してメモリ サイズを変更できます。ただし、Windows がデフォルトの設定を使用している場合は、システム ページ ファイルのサイズは新しいメモリ サイズに合わせて調整されません。

手順

- 1 接続サーバがインストールされている Windows Server コンピュータで、[仮想メモリ] ダイアログ ボックスに移動します。

デフォルトで、[カスタム サイズ] が選択されています。ページ ファイルの初期サイズと最大サイズが表示されます。

- 2 [システム管理サイズ] をクリックします。

結果

Windows は継続的に、現在のメモリ使用と使用可能なメモリに基づいてシステム ページ ファイルのサイズを再計算します。

イベント レポートの構成

10

イベント データベースを作成し、Horizon 7 イベントについての情報を記録することができます。さらに、Syslog サーバを使用する場合、イベントを Syslog サーバに送信するか、Syslog 形式で記述されたイベントのフラット ファイルを作成するように接続サーバを構成できます。

この章には、次のトピックが含まれています。

- [Horizon 7 イベント用のデータベースとデータベース ユーザーを追加する](#)
- [SQL Server データベースをイベント レポート用に準備する](#)
- [イベント データベースを構成する](#)
- [Syslog サーバのイベント ログを構成する](#)

Horizon 7 イベント用のデータベースとデータベース ユーザーを追加する

イベント データベースは、既存のデータベース サーバに追加する方法で作成します。続いて、エンタープライズ レポート ソフトウェアを使用して、そのデータベース内のイベントを分析できます。

イベント データベース用のデータベース サーバは、専用のサーバにデプロイします。これは、プロビジョニングおよび Horizon 7 のデプロイに対して重要な他のアクティビティにイベントのログ アクティビティが影響を与えないようにするためです。

注： このデータベースのために ODBC データ ソースを作成する必要はありません。

前提条件

- サポートされている Microsoft SQL Server または Oracle データベース サーバが、接続サーバ インスタンスでアクセスできるシステム上に存在することを確認します。サポートされるデータベース バージョンのリストについては、以下を参照してください：[View Composer およびイベント データベースのデータベース要件](#)
- データベースとユーザーをデータベース サーバに作成するために必要なデータベース権限があることを確認します。
- Microsoft SQL Server データベース サーバにデータベースを作成する手順を把握していない場合は、[View Composer データベースを SQL Server に追加する](#)で手順を確認してください。

- Oracle データベース サーバにデータベースを作成する手順を把握していない場合は、[View Composer データベースを Oracle 12c または 11g に追加](#) で手順を確認してください。

手順

- 1 サーバに新しいデータベースを追加し、HorizonEvents のようなわかりやすい名前をこのデータベースに付けます。

Oracle 12c または 11g データベースの場合は、Oracle システム識別子 (SID) も指定します（この識別子は Horizon Administrator でイベント データベースを構成する際に使用します）。

- 2 これらのオブジェクトの読み書き権限の他にテーブルとビュー（Oracle の場合はトリガとシーケンスも）を作成する権限を持ったユーザーをこのデータベースに追加します。

Microsoft SQL Server データベースの場合、統合 Windows 認証セキュリティ モデルの認証方法は使用しないでください。必ず SQL Server 認証の認証方法を使用してください。

結果

データベースは作成されますが、Horizon Administrator でデータベースを構成するまでスキーマはインストールされません。

次のステップ

以下の説明に従います。[イベント データベースを構成する](#)

SQL Server データベースをイベント レポート用に準備する

Horizon Administrator を使用して Microsoft SQL Server にイベント データベースを構成する前に、正しい TCP/IP プロパティを構成し、サーバが SQL Server 認証を使用していることを確認する必要があります。

前提条件

- イベント レポート用に SQL Server データベースを作成します。[Horizon 7 イベント用のデータベースとデータベース ユーザーを追加する](#)を参照してください。
- データベースを構成するために必要なデータベース権限があることを確認します。
- データベース サーバが SQL Server 認証の認証方法を使用していることを確認します。Windows 認証は使用しないでください。

手順

- 1 SQL Server 構成マネージャを開き、[SQL Server YYYY ネットワークの構成] を展開します。
- 2 [server_name のプロトコル] を選択します。
- 3 プロトコルのリストで [TCP/IP] を右クリックし、[P プロパティ] を選択します。
- 4 [有効化] プロパティを [はい] に設定します。
- 5 ポートが割り当てられていることを確認し、必要であれば割り当てます。

静的および動的なポートおよびポートを割り当てる方法については、SQL Server 構成マネージャのオンラインヘルプを参照してください。

6 このポートがファイアウォールによってブロックされないことを確認します。

次のステップ

Horizon Administrator を使用して、データベースを接続サーバに接続します。以下の説明に従います。 [イベント データベースを構成する](#)

イベント データベースを構成する

イベント データベースには、Horizon 7 のイベントに関する情報が、ログ ファイルではなくデータベースのレコードとして格納されます。

Connection Server インスタンスをインストールした後で、イベント データベースを構成します。Connection Server グループ内で構成する必要があるホストは 1 台だけです。グループの他のホストは自動的に構成されます。

注： Connection Server インスタンスと外部データベース間のデータベース接続のセキュリティは、管理者の責任ですが、イベント トラフィックは Horizon 7 環境の 健全性に関する情報に制限されます。さらに慎重を期すのであれば、IPSec などの手段を使用してこのチャネルを保護するか、データベースを Connection Server コンピュータ上でローカルに展開することができます。

データベース テーブル内のイベントを調べるには、Microsoft SQL Server または Oracle データベース レポート ツールを使用できます。詳細については、Horizon 7 の統合を参照してください。

また、Horizon 7 イベントを Syslog 形式で生成すると、他社製分析ソフトウェアからイベント データにアクセスできます。vdmadmin コマンドと -I オプションを使用して、Horizon 7 イベント メッセージを Syslog 形式でイベント ログ ファイルに記録します。Horizon 7 の管理ドキュメントで、「-I オプションを使用した Syslog 形式での Horizon 7 イベント ログ メッセージの生成」を参照してください。

前提条件

イベント データベースを構成するには、次の情報が必要です。

- データベース サーバの DNS 名または IP アドレス。
- データベース サーバの種類 (Microsoft SQL Server または Oracle)。サポートされているデータベース サーバの詳細については、[IPv6 環境でサポートされている vSphere、データベース、および Active Directory のバージョン](#)を参照してください。
- データベース サーバへのアクセスに使用するポート番号。デフォルトは、Oracle の場合は 1521、SQL Server の場合は 1433 です。SQL Server では、データベース サーバが名前付きインスタンスの場合、または SQL Server Express を使用している場合は、ポート番号の特定が必要になる場合があります。SQL Server の名前付きインスタンスへの接続については、Microsoft のサポート技術情報 (KB) の記事 <http://support.microsoft.com/kb/265808> を参照してください。
- データベース サーバに作成したイベント データベースの名前。 [Horizon 7 イベント用のデータベースとデータベース ユーザーを追加する](#)を参照してください。

Oracle 12c または 11g データベースの場合、Horizon Administrator でイベント データベースを構成するときに Oracle System Identifier (SID) をデータベース名として使用する必要があります。

- このデータベース用に作成したユーザーのユーザー名とパスワード。 [Horizon 7 イベント用のデータベースとデータベース ユーザーを追加する](#)を参照してください。

このユーザーに対しては SQL Server 認証を使用します。統合 Windows 認証セキュリティ モデルの認証方法は使用しないでください。

- イベント データベースのテーブルのプレフィックス (VE_ など)。プリフィックスを使用することで、Horizon 7 の複数のインストール間でデータベースを共有できます。

注： 使用しているデータベース ソフトウェアで有効な文字を入力する必要があります。ダイアログ ボックスを終了するときにプレフィックスの構文はチェックされません。使用しているデータベース ソフトウェアで有効でない文字を入力した場合、Connection Server がデータベース サーバへの接続を試行したときにエラーが発生します。ログ ファイルにはすべてのエラーが記録され、このエラーや、データベース名が無効な場合にデータベース サーバから返されるその他すべてのエラーも含まれます。

手順

- 1 Horizon Administrator で、[View 構成] - [イベント構成] の順に選択します。
- 2 [イベント データベース] セクションで、[編集] をクリックし、提示されるフィールドに情報を入力して、[OK] をクリックします。
- 3 (オプション) イベントの設定 ウィンドウで、[編集] をクリックし、イベントを表示する時間の長さ、およびイベントを新規として分類する日数を変更し、[OK] をクリックします。

これらの設定は、イベントが Horizon Administrator インターフェイスに表示される期間に関係します。この時間が経過すると、イベントは履歴データベース テーブルにのみ表示されます。

Database Configuration (データベースの構成) ウィンドウに、イベント データベースの現在の構成が表示されます。

- 4 [Monitoring (監視)] - [イベント] を選択し、イベント データベースに正常に接続できることを確認します。

接続できない場合は、エラー メッセージが表示されます。SQL Express を使用している場合、または SQL Server の名前付きインスタンスを使用している場合は、前提条件にあるように、正しいポート番号の指定が必要な場合があります。

結果

[Horizon Administrator] ダッシュボードの [System Component Status (システム コンポーネント ステータス)] では、イベント データベース サーバは [Reporting Database (レポート データベース)] という見出しの下に表示されます。

Syslog サーバのイベント ログを構成する

Horizon 7 イベントを Syslog 形式で生成すると、分析ソフトウェアからイベント データにアクセスできます。

Connection Server グループ内で構成する必要があるホストは 1 台だけです。グループの他のホストは自動的に構成されます。

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、これらのログ ファイルはその共有に移動されます。

- ローカル ファイルは、構成中（多くの場合はイベント データベースが構成される前）に素早くトラブルシューティングできるようにイベントを確認するためにのみ使用します。

イベント ログのローカル ディレクトリの最大サイズは、最も古いファイルが削除される前に閉じられたログ ファイルを含めて 300 MB です。Syslog 出力のデフォルトの出力先は %PROGRAMDATA%\VMware\VDM \events\ です。

- Syslog サーバがない場合、または現在の Syslog サーバではニーズが満たせない場合は、UNC パスを使用して長期的なイベントのレコードのログ ファイルを保存します。

別の方法として、vdmadmin コマンドを使用してイベントのファイル ベースのログを Syslog 形式で構成できます。『Horizon 7 の管理』ドキュメントで、vdmadmin コマンドの -I オプションを使用した Syslog 形式での Horizon 7 イベント ログ メッセージの生成に関するトピックを参照してください。

重要： Syslog データはソフトウェア ベースの暗号化なしにネットワーク間で送信され、ユーザー名などの機密データが含まれている場合があります。VMware は、IPSEC などのリンク レイヤ セキュリティを使用して、こうしたデータがネットワーク上でモニターリングする可能性を回避することを推奨します。

前提条件

イベントを Syslog 形式で記録できるようにするか、Syslog サーバに送信できるようにする、またはその両方を実現できるように Connection Server を構成するには、以下の情報が必要です。

- Syslog サーバを使用して UDP ポートで Horizon 7 イベントをリッスンする予定にしている場合、Syslog サーバの DNS 名または IP アドレスと UDP ポート番号が必要です。デフォルトの UDP ポート番号は 514 です。
- フラット ファイル形式でログを収集する予定にしている場合は、ログ ファイルを格納するファイル共有およびフォルダまでの UNC パスが必要で、ファイル共有に書き込む権限を持つアカウントのユーザー名、ドメイン名、パスワードが必要です。

手順

- 1 Horizon Administrator で、[View 構成] - [イベント設定] の順に選択します。
- 2 （オプション） [Syslog] 領域で、イベントを Syslog サーバに送信するように Connection Server を構成するには、[Syslog サーバに送信] の隣の [追加] をクリックし、サーバ名または IP アドレスと UDP ポート番号を入力します。

- 3 (オプション) [ファイル システムへのイベント] 領域で、イベント ログ メッセージを生成してログファイルに Syslog 形式で保存するかどうかを選択します。

オプション	説明
Always	イベント ログ メッセージが常に生成され、Syslog 形式で保存されます。
エラー時にファイルにログを記録する (デフォルト)	イベント データベースまたは Syslog サーバにイベントを書き込むときに問題が発生した場合、監査イベントがログ ファイルに記録されます。このオプションは、デフォルトで有効になっています。
実行しない	イベント ログ メッセージが生成されず、Syslog 形式で保存されません。

ログ ファイルは、ファイル共有までの UNC パスを指定しない限り、ローカルで保持されます。

- 4 (オプション) Horizon 7 イベント ログ メッセージをファイル共有で格納するには、[場所にコピー] の隣の [追加] をクリックして、ログ ファイルを格納するファイル共有およびフォルダまでの UNC パスを入力し、ファイル共有に書き込む権限を持つアカウントのユーザー名、ドメイン名、パスワードを入力します。

以下は、UNC パスの例です。

```
\\syslog-server\folder\file
```