

View でのデスクトッププールの とアプリケーションプールの 設定

VMware Horizon 7 7.0



vmware®

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

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

ヴァイ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 © 2019 VMware, Inc. All rights reserved. [著作権および商標情報](#)。

目次

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 12

1 デスクトップ プールとアプリケーション プールの概要 13

ファーム、RDS ホスト、デスクトップおよびアプリケーション プール 13

デスクトップ プールの利点 14

特定のタイプのワーカーのデスクトップ プール 15

タスク ワーカー用プール 16

ナレッジ ワーカーとパワー ユーザー用プール 17

キオスク ユーザー用プール 18

アプリケーション プールの利点 19

2 非管理対象マシンの準備 21

リモート デスクトップ展開用の非管理対象マシンの準備 21

非管理対象マシンでの Horizon Agent のインストール 22

非管理対象マシン用の Horizon Agent のカスタム セットアップ オプション 23

3 クローン作成のための親仮想マシンの作成と準備 26

クローン作成のための仮想マシンの作成 27

vSphere での仮想マシンの作成 27

ゲスト OS のインストール 29

リモート デスクトップの展開のためのゲスト OS の準備 30

デスクトップで使用するための Windows Server OS の準備 32

Windows Server 2008 R2 へのデスクトップ エクスペリエンスのインストール 33

Windows Server 2012 または 2012 R2 へのデスクトップ エクスペリエンスのインストール 34

障害発生後に Windows ファイアウォール サービスを再起動させるための構成 34

仮想マシンへの Horizon Agent のインストール 35

Horizon Agent のカスタム セットアップ オプション 37

Horizon Agent のサイレント インストール 39

Microsoft Windows インストーラ コマンドライン オプション 41

Horizon Agent のサイレント インストール プロパティ 43

Horizon Agent のための複数の NIC を使用する仮想マシンの構成 46

ゲスト OS のパフォーマンスの最適化 46

Windows カスタマー エクスペリエンス向上プログラムを無効にする 48

インスタントクローンおよび View Composer リンククローン仮想マシン用の Windows のカスタマイズ 49

Windows のサービスおよびタスクを無効にした場合の利点 49

インスタント クローンおよびリンク クローンのディスクの拡大を招く Windows のサービスおよびタスク 49

Windows 親仮想マシンでのスケジュール設定されたディスクの最適化の無効化 51

Windows Update を無効にする	52
Windows 仮想マシンでの診断ポリシー サービスの無効化	53
Windows 仮想マシンでのブリフェッチとスーパーフェッチの機能の無効化	53
Windows 仮想マシンでの Windows レジストリのバックアップの無効化	54
Windows 仮想マシンでのシステムの復元の無効化	54
Windows 仮想マシンでの Windows Defender の無効化	55
Windows 仮想マシンでの Microsoft Feeds Synchronization の無効化	55
親仮想マシンの準備	56
親仮想マシンの構成	56
インスタント クローンおよび View Composer リンク クローンでの Windows のアクティベーション	58
親仮想マシンでの Windows のハイパネーションの無効化	59
View Composer リンク クローン用のローカル ストレージの構成	59
View Composer 親仮想マシンのページング ファイル サイズの記録	60
ClonePrep および QuickPrep カスタマイズ スクリプトのタイムアウト制限の引き上げ	61
仮想マシン テンプレートの作成	61
カスタマイズ仕様の作成	62

4 フル仮想マシンを含む自動デスクトップ プールの作成 63

フル仮想マシンを含む自動プール	63
フル仮想マシンを含む自動プールの作成用ワークシート	63
フル仮想マシンを含む自動プールの作成	67
自動デスクトップ プールのクローン作成	68
フル仮想マシンを含む自動プールのデスクトップ設定	69

5 リンク クローン デスクトップ プールの作成 71

リンク クローン デスクトップ プール	71
リンク クローン デスクトップ プールの作成用ワークシート	71
リンククローン デスクトップ プールの作成	80
自動デスクトップ プールのクローン作成	82
リンク クローン デスクトップ プールのデスクトップ プール設定	84
View Composer でのリンク クローンの SID およびサードパーティ アプリケーションのサポート	84
リンク クローン マシンをカスタマイズするための QuickPrep または Sysprep の選択	86
View Composer の操作時に、リモート デスクトップ セッションで使用するようプロビジョニングされたリンク クローン マシンを維持する	90
リンク クローンに既存の Active Directory コンピュータ アカウントを使用する	91

6 インスタントクローン デスクトップ プールの作成 93

インスタントクローン デスクトップ プール	93
インスタントクローン デスクトップ プールのイメージの公開および再調整	95
インスタントクローンのドメイン管理者の追加	95
インスタントクローン デスクトップ プールの作成用ワークシート	96
インスタントクローン デスクトップ プールの作成	99

ClonePrep でのゲストのカスタマイズ	100
インスタントクローン メンテナンス ユーティリティ	101

7 手動デスクトップ プールの作成 104

手動デスクトップ プール	104
手動デスクトップ プールの作成用ワークシート	104
手動デスクトップ プールの作成	106
1 つのマシンを含む手動プールの作成	107
手動プールのデスクトップ プール設定	108

8 リモート デスクトップ サービス ホストの設定 111

リモート デスクトップ サービス (RDS) ホスト	111
Windows Server 2008 R2 へのリモート デスクトップ サービスのインストール	113
Windows Server 2012 または 2012 R2 へのリモート デスクトップ サービスのインストール	114
Windows Server 2008 R2 へのデスクトップ エクスペリエンスのインストール	115
Windows Server 2012 または 2012 R2 へのデスクトップ エクスペリエンスのインストール	115
ユーザーを単一セッションに制限する	116
リモート デスクトップ サービス ホストへの Horizon Agent のインストール	117
RDS ホストに対する Horizon Agent のカスタム セットアップ オプション	118
ネストされたセッション内で起動されたリモート アプリケーションからの印刷	120
RDS デスクトップ セッションと RDS アプリケーション セッションのタイム ゾーン リダイレクトの有効化	120
アプリケーションで Windows ベーシック テーマを有効にする	121
Runonce.exe を開始するグループ ポリシーの構成	122
RDS ホスト パフォーマンス オプション	122
RDS ホスト用の 3D グラフィックスの構成	123

9 ファームの作成 125

ファーム	125
自動ファームの親仮想マシンの準備	126
RDS ホストの親仮想マシンの準備	127
リンククローン RDS ホストでの Windows のアクティベーション	129
親仮想マシンでの Windows のハイパネーションの無効化	129
手動ファーム作成用ワークシート	130
自動ファーム作成用ワークシート	131
手動ファームの作成	136
自動ファームの作成	136

10 アプリケーション プールの作成 138

アプリケーション プール	138
アプリケーション プールの手動作成用ワークシート	139
アプリケーション プールの作成	139

11 RDS デスクトップ プールの作成 141

RDS デスクトップ プールの概要 141

RDS デスクトップ プールの作成 142

RDS デスクトップ プールのデスクトップ プール設定 143

Adobe Flash のスロットルを RDS デスクトップ プール用に Internet Explorer で構成する 143

12 デスクトップ プールのプロビジョニング 144

デスクトップ プールでのユーザー割り当て 144

マシンの手動での名前付けまたは名前付けパターンの指定 145

マシン名のリストの指定 146

自動デスクトップ プールでの名前付けパターンの使用 148

マシンの名前付けの例 149

名前のリストによってプロビジョニングされる自動プールへのマシンの追加 150

マシンの手動でのカスタマイズ 151

メンテナンス モードでのマシンのカスタマイズ 151

個別マシンのカスタマイズ 152

すべてのデスクトップ プール タイプのデスクトップ プール設定 152

Adobe Flash の品質とスロットル 157

デスクトップ プールの電源ポリシーの設定 158

デスクトップ プールの電源ポリシー 158

ユーザーが切断した後にサスペンドするよう専用マシンを構成する 160

自動デスクトップ プールに対する電源ポリシーの影響 160

流動割り当てを使用する自動プールの電源ポリシーの例 161

専用割り当てを使用する自動プールの電源ポリシーの例 162

View の電源ポリシーの競合の防止 162

デスクトップ用の 3D レンダリングの構成 163

3D レンダラーのオプション 167

3D レンダリング構成のベスト プラクティス 169

vDGA 機能の準備 172

NVIDIA GRID vGPU 機能の準備 172

vDGA を使用する AMD Multiuser GPU の機能を使用する準備 173

vDGA を使用する AMD Multiuser GPU の構成 174

ESXi ホストでの GPU リソースの調査 176

View デスクトップへの RDP を使用したアクセスの防止 176

大規模なデスクトップ プールの展開 177

8 台を超えるホストを含むクラスタでのデスクトップ プールの構成 177

デスクトップ プールへの複数のネットワーク ラベルの割り当て 178

13 資格のあるユーザーとグループ 179

デスクトップまたはアプリケーション プールへの資格の追加 179

デスクトップまたはアプリケーション プールからの資格の削除 180

デスクトップまたはアプリケーション プールの資格の確認	180
リモート デスクトップ アクセスの制限	181
制限付き資格の例	181
タグ一致	182
制限付き資格に関する考慮事項と制限事項	183
View 接続サービインスタンスへのタグの割り当て	184
デスクトップ プールへのタグの割り当て	184
ネットワーク外部のリモート デスクトップ アクセスの制限	185
ネットワーク外部のユーザーの制限	185

14 リモート デスクトップ機能の構成 187

Unity Touch の構成	187
Unity Touch のシステム要件	188
Unity Touch で表示されるお気に入りアプリケーションの構成	188
マルチキャストまたはユニキャスト ストリーミング用の Flash URL リダイレクトの構成	191
Flash URL リダイレクトのシステム要件	192
Flash URL リダイレクト機能がインストールされていることの確認	194
マルチキャストまたはユニキャストのストリームを提供する Web ページの設定	194
Flash URL リダイレクト用にクライアント デバイスを設定	195
Flash URL リダイレクトを無効または有効	195
Flash リダイレクトの構成	196
Flash リダイレクトの要件	197
Flash リダイレクトのインストールと構成	198
Windows レジストリ設定を使用した Flash リダイレクトの構成	201
URL コンテンツ リダイレクトの構成	203
URL コンテンツ リダイレクトの要件と制限事項	204
URL コンテンツ リダイレクト機能ありでの Horizon Client のインストール	206
URL コンテンツ リダイレクト機能ありでの Horizon Agent のインストール	206
Active Directory への URL コンテンツ リダイレクト ADM テンプレートの追加	206
VMware Horizon URL コンテンツ リダイレクト テンプレートの設定	208
リアルタイム オーディオ ビデオの構成	211
リアルタイム オーディオ ビデオの構成の選択	212
リアルタイム オーディオビデオのシステム要件	212
リアルタイム オーディオ ビデオが USB リダイレクトの代わりに使用されることを確認	213
優先される Web カメラとマイクロフォンを選択	214
リアルタイム オーディオ ビデオ グループ ポリシ設定の構成	223
リアルタイム オーディオ ビデオの帯域幅	226
スキャナ リダイレクトの構成	227
スキャナ リダイレクトのシステム要件	227
スキャナ リダイレクトのユーザー操作	228
スキャナ リダイレクトのグループ ポリシー設定の構成	229

シリアル ポート リダイレクトの構成	232
シリアル ポート リダイレクトの要件	233
シリアル ポート リダイレクトのユーザー操作	234
シリアル ポート リダイレクトの構成に関するガイドライン	235
シリアル ポート リダイレクトのグループ ポリシー設定の構成	236
USB シリアル アダプタの構成	239
Windows Media マルチメディア リダイレクト (MMR) へのアクセスの管理	240
View でのマルチメディア リダイレクトの有効化	240
Windows Media MMR のシステム要件	241
ネットワーク遅延に基づく Windows Media MMR の使用の決定	242
クライアント ドライブ リダイレクトへのアクセスの管理	243
グループ ポリシーを使用したクライアント ドライブ リダイレクトの無効化	244
レジストリ設定を使用したクライアント ドライブ リダイレクトの構成	244
コピーおよび貼り付け操作におけるクリップボードのデータ形式の制限	246
15 リモート デスクトップおよびアプリケーションでの USB デバイスの使用	248
USB デバイス タイプに関する制限事項	249
USB リダイレクトの設定の概要	250
ネットワーク トラフィックと USB リダイレクト	251
USB デバイスへの自動接続	252
保護された View 環境での USB デバイスの展開	253
すべてのタイプのデバイスに対する USB リダイレクトの無効化	253
特定のデバイスに対する USB リダイレクトの無効化	254
ログ ファイルを使用してのトラブルシューティングと USB デバイス ID の確認	256
USB リダイレクトを制御するポリシーの使用	257
複合 USB デバイスのデバイス分割ポリシー設定の構成	257
USB デバイスのフィルタ ポリシー設定の構成	260
USB デバイス ファミリ	264
Horizon Agent の構成 ADM テンプレートの USB 設定	265
USB リダイレクトに関する問題のトラブルシューティング	268
16 ストレージ要件の軽減と管理	271
vSphere によるストレージの管理	271
高パフォーマンス ストレージとポリシー ベース管理のための Virtual SAN の使用	273
Virtual SAN データストアのデフォルトのストレージ ポリシー プロファイル	275
仮想マシン中心ストレージとポリシー ベース管理のための仮想ボリュームの使用	276
インスタント クローンによる必要ストレージの軽減	277
View Composer によるストレージ要件の軽減	278
インスタントクローンおよび View Composer リンククローン デスクトップ プールのストレージ サイズ設定	280
インスタントクローン プールとリンク クローン プールのサイズ設定ガイドライン	280
インスタントクローン プールとリンク クローン プールのサイズ設定の式	283

クローンを作成するためのサイズ設定の式（プールを編集する場合、またはレプリカを別のデータストアに格納する場合）	284
View Composer リンク クローン仮想マシンのストレージ オーバーコミット	285
リンククローン仮想マシンのストレージのオーバーコミット レベルの設定	286
View Composer リンククローン データ ディスク	287
ローカル データストアへの View Composer リンク クローンの保存	288
インスタント クローンおよび View Composer リンク クローン用の別のデータストアへのレプリカおよびクローンの格納	289
別のデータストアにレプリカを格納する際の可用性に関する考慮事項	290
View Composer リンク クローン用の View Storage Accelerator の構成	290
View Composer リンク クローンでのディスク領域の再利用	292
View Composer リンク クローン用の VAAI ストレージの使用	294
View Composer リンク クローン用の Storage Accelerator と領域再利用の停電期間の設定	296

17 デスクトップ プールとアプリケーション プールのポリシーの構成 297

View Administrator でのポリシーの設定	297
グローバル ポリシー設定の構成	298
デスクトップ プールのポリシーの構成	298
ユーザーのポリシーの構成	299
View ポリシー	299
スマート ポリシー の使用	300
スマート ポリシー の要件	300
User Environment Manager のインストール	300
User Environment Manager の構成	301
Horizon スマート ポリシー設定	302
帯域幅プロファイル リファレンス	302
Horizon スマート ポリシー定義への条件の追加	303
User Environment Manager の Horizon スマート ポリシーの作成	305
Active Directory グループ ポリシーの使用	306
リモート デスクトップの OU の作成	307
リモート デスクトップのループバック処理の有効化	307
View グループ ポリシー管理用テンプレート ファイルの使用	307
View ADM および ADMX テンプレート ファイル	308
Horizon Agent の構成 ADM テンプレートの設定	309
リモート デスクトップに送信されるクライアント システム情報	313
View デスクトップ上でのコマンドの実行	317
PCoIP ポリシー設定	317
PCoIP の一般的な設定	318
PCoIP クリップボードの設定	325
PCoIP の帯域幅設定	328
PCoIP のキーボード設定	330
PCoIP ロスレス構築機能	331

VMware Blast ポリシー設定	332
VMware Blast のロスレス圧縮の有効化	335
リモート デスクトップ サービス グループ ポリシーの使用	336
RDS CAL (接続デバイス数) ストレージの構成	336
リモート デスクトップ サービス ADMX ファイルを Active Directory へ追加	337
RDS アプリケーションの互換性の設定	338
RDS 接続の設定	340
RDS デバイスおよびリソースのリダイレクトの設定	340
RDS ライセンスの設定	340
RDS プロファイルの設定	342
RDS リモート セッション環境の設定	345
RDS セキュリティの設定	345
RDS 一時フォルダの設定	345
ロケーションベースの印刷の設定	346
ロケーションベースの印刷グループ ポリシー DLL ファイルの登録	348
ロケーションベースの印刷グループ ポリシーの構成	348
ロケーションベースの印刷グループ ポリシー設定の構文	350
Active Directory グループ ポリシーの例	351
View マシンの OU の作成	352
View グループ ポリシーの GPO の作成	352
GPO への View ADM テンプレートの追加	353
リモート デスクトップのループバック処理の有効化	354

18 View Persona Management でのユーザー プロファイルの構成 356

View でのユーザーの個人設定の提供	356
スタンドアロン システムでの View Persona Management の使用	357
View Persona Management によるユーザー プロファイルの移行	358
個人設定管理と Windows 移動プロファイル	362
View Persona Management 展開の構成	362
View Persona Management 展開の設定の概要	362
ユーザー プロファイル リポジトリ の構成	363
View Persona Management オプションを指定して Horizon Agent をインストール	365
スタンドアロン View Persona Management をインストールする	366
View Persona Management の ADM または ADMX テンプレート ファイルの追加	368
View Persona Management ポリシーを構成	371
個人設定管理を使用するデスクトップ プールの作成	373
View Persona Management 展開を構成するためのベスト プラクティス	374
ThinApp サンドボックス フォルダを含むようにユーザー プロファイルを構成	376
View Persona Management での View Composer 通常ディスクの構成	377
スタンドアロン ノート型コンピュータでのユーザー プロファイルの管理	377
View Persona Management グループ ポリシー設定	378

- 移動と同期に関するグループ ポリシー設定 379
- フォルダリダイレクトのグループ ポリシー設定 383
- デスクトップ UI のグループ ポリシー設定 386
- ログのグループ ポリシー設定 386

19 マシンとデスクトップ プールのトラブルシューティング 388

- 問題のあるマシンの表示 388
- デスクトップ ユーザーへのメッセージの送信 389
- デスクトップ プールのプロビジョニングまたは再作成に関する問題 390
 - インスタントクローンのプロビジョニングまたはイメージ プッシュの失敗 390
 - インスタント クローンのイメージ公開の失敗 390
 - インスタントクローンのプロビジョニング中の無限エラー リカバリ 390
 - 孤立したインスタント クローンを削除できない 391
 - カスタマイズ仕様が見つからない場合のプール作成の失敗 391
 - 権限の問題によるプール作成の失敗 392
 - 構成の問題によるプールのプロビジョニングの失敗 392
 - View 接続サーバ インスタンスが vCenter に接続できないことによるプールのプロビジョニングの失敗 393
 - データストアの問題によるプールのプロビジョニングの失敗 393
 - vCenter Server の過負荷によるプールのプロビジョニングの失敗 394
 - 仮想マシンのプロビジョニング状態の継続 395
 - 仮想マシンのカスタマイズ状態の継続 395
 - 孤立または削除されたリンク クローンの削除 395
 - 繰り返し削除と再作成が行われるマシンのトラブルシューティング 397
 - QuickPrep のカスタマイズに関する問題のトラブルシューティング 398
 - 未使用の View Composer レプリカの検索と保護解除 399
 - View Composer のプロビジョニング エラー 400
- ネットワーク接続に関する問題のトラブルシューティング 402
 - マシンと View 接続サーバ インスタンスの接続の問題 402
 - Horizon Client と PCoIP Secure Gateway の接続の問題 403
 - マシンと View 接続サーバ インスタンスの接続の問題 405
 - クローン マシンへの不正な IP アドレス割り当てによる接続の問題 406
- USB リダイレクトに関する問題のトラブルシューティング 406
- 資格のないユーザーのマシンおよびポリシーの管理 408
- ViewDbChk コマンドを使用したデータベース不整合の解決 409
- トラブルシューティングの追加情報 412

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

『View でのデスクトップ プールおよびアプリケーション プールの設定』では、Microsoft リモート デスクトップ サービス (RDS) のホストで実行するリモート アプリケーションのプールの作成、マシンのプールの作成とプロビジョニング方法について説明します。マシンの準備、ポリシーの構成、ユーザーおよびグループへの資格の付与、リモート デスクトップ機能の構成、View Persona Management でのユーザー プロファイルの構成に関する情報が含まれます。

対象読者

この情報は、デスクトップおよびアプリケーション プールを作成およびプロビジョニングする必要のあるユーザーを対象としています。これらの情報は、仮想マシン テクノロジーおよびデータセンターの運用に精通している経験豊富な Windows システム管理者向けに記述されています。

デスクトップ プールとアプリケーション プールの概要

1

Horizon 7 では、デスクトップ プールを作成する場合、含まれる仮想デスクトップは 1,000 台でもかまいません。仮想マシン、物理マシン、および Windows Remote Desktop Services (RDS) ホストで実行するデスクトップをデプロイできます。基本イメージとして 1 台の仮想マシンを作成すれば、Horizon 7 はそのイメージから仮想デスクトップのプールを生成できます。また、ユーザーにアプリケーションへのリモート アクセスを提供するアプリケーション プールも作成できます。

この章には、次のトピックが含まれています。

- [ファーム、RDS ホスト、デスクトップおよびアプリケーション プール](#)
- [デスクトップ プールの利点](#)
- [特定のタイプのワーカーのデスクトップ プール](#)
- [アプリケーション プールの利点](#)

ファーム、RDS ホスト、デスクトップおよびアプリケーション プール

デスクトップ プールとアプリケーション プールを作成することにより、ユーザーに仮想マシン ベースのデスクトップ、セッション ベースのデスクトップ、物理コンピュータ、およびアプリケーションへのリモート アクセスを行わせることができます。Microsoft リモート デスクトップ サービス (RDS)、VMware PC-over-IP (PCoIP)、または VMware Blast を選択しても、リモート アクセスをユーザーに提供できます。

RDS ホスト

RDS ホストは、Windows リモート デスクトップ サービスと Horizon Agent がインストールされたサーバ コンピュータです。これらのサーバは、ユーザーが遠隔地からアクセスできるアプリケーションとデスクトップ セッションをホストします。RDS デスクトップ プールまたはアプリケーションにアクセスするには、Horizon Client 3.0 以上が必要です。

デスクトップ プール

デスクトップ プールは、自動、手動、RDS の主に 3 種類があります。自動デスクトップ プールは、vCenter Server 仮想マシン テンプレートまたはスナップショットを使用して同一の仮想マシンのプールを作成します。手動デスクトップ プールは、既存の vCenter Server 仮想マシン、物理コンピュータ、またはサードパーティ仮想マシンの集まりです。自動プールまたは手動プールでは、各マシンには、一度に 1 人のユーザーがリモート アクセスできます。RDS デスクトップ プールはマシンの集まりではありません。このプールは、RDS ホストにおけるデスクトップ セッションをユーザーに提供します。RDS ホスト上のデスクトップ セッションは複数のユーザーによる同時利用が可能です。

アプリケーション プール

アプリケーション プールを利用して管理者は、多数のユーザーにアプリケーションを配布できます。アプリケーション プール内のアプリケーションは、RDS ホストのファームで実行されます。

ファーム

ファームは RDS ホストの集まりです。ファームを利用することでホストを円滑に管理できます。ファームに含める RDS ホストの数は流動的に変更でき、共通のアプリケーション セットや RDS デスクトップをユーザーに提供できます。RDS デスクトップ プールまたはアプリケーション プールを作成する場合は、ファームを指定する必要があります。ファーム内の RDS ホストは、ユーザーにデスクトップ セッションとアプリケーション セッションを提供します。

デスクトップ プールの利点

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

リモート デスクトップ プールは、次のいずれかのソースから作成できます。

- 物理デスクトップ PC や RDS ホストなどの物理システム
- ESXi ホスト上でホストされ vCenter Server によって管理されている仮想マシン
- Horizon Agent をサポートする vCenter Server 以外の仮想化プラットフォームで稼動する仮想マシン。

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

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

- リモート デスクトップのデフォルトとして使用するリモート表示プロトコルと、ユーザーにデフォルトのオーバーライドを許可するかどうかの指定。
- View Composer のリンククローン仮想マシンまたは完全クローン仮想マシンについては、仮想マシンを使用していないときにパワーオフするかどうか、および完全に削除するかどうかを指定します。インスタント クローン仮想マシンは、常にパワーオンされています。

- View Composer のリンククローン仮想マシンについては、Microsoft Sysprep のカスタマイズ仕様を使用するか、または VMware の QuickPrep を使用するかを指定できます。Sysprep はプール内の各仮想マシンに一意の SID および GUID を生成します。インスタント クローンは、VMware が提供する ClonePrep と呼ばれる異なるカスタマイズ仕様を必要とします。

プール内のデスクトップにユーザーを割り当てる方法も指定できます。

専用割り当てプール

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

流動割り当てプール

オプションで、リモート デスクトップが使用後に毎回削除および再作成されるため、高度な制御の可能な環境が提供されます。

流動割り当てプールを使用すると、異なるシフトのユーザーが使用できるデスクトップのプールも作成できます。たとえば、ユーザーが一度に 100 人のシフトで勤務している場合、100 のデスクトップのプールを 300 人のユーザーが使用できます。

特定のタイプのワーカーのデスクトップ プール

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

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

ステートレス デスクトップ イメージ

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

ステートフル デスクトップ イメージ

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

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

- インスタント クローン仮想マシンの流動割り当てプールを作成できます。フォルダ リダイレクトと移動プロファイルをオプションで使用して、ユーザー データを格納することも可能です。

- View Composer を使用して、リンク クローン仮想マシンの流動割り当てプールを作成できます。フォルダ リダイレクトと移動プロファイルをオプションでを使用して、ユーザー データを格納することも可能です。

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

- インスタント クローン仮想マシンの流動割り当てプールを作成し、App Volumes を使用してユーザー データとユーザーがインストールするアプリケーションを接続できます。フォルダ リダイレクトと移動プロファイルをオプションでを使用して、ユーザー データを格納することも可能です。
- View Composer を使用して、リンク クローン仮想マシンの専用割り当てプールを作成できます。View Composer の通常ディスクを構成できます。
- 完全クローンまたはフル仮想マシンを作成できます。一部のストレージ ベンダーは、完全クローン向けのコスト効率の良いストレージ ソリューションを提供しています。これらのベンダーは多くの場合、独自のベスト プラクティスおよびプロビジョニング ユーティリティを備えています。これらのベンダーのいずれかを使用した場合、手動の専用割り当てプールの作成が必要になることがあります。

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

タスク ワーカー用プール

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

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

- 自動プールを作成して、そのプールの作成時にデスクトップが作成されるようにするか、プールの使用量に基づいてオン デマンドでデスクトップが生成されるようにすることができます。
- インスタント クローン プールについては、リソース使用率を最適化するために、オン デマンドのプロビジョニングを使用して、使用率に基づいてプールを拡大または縮小します。ログイン レートを満たすため、十分なスベア デスクトップを指定するようにします。
- 流動割り当てを使用して、使用可能なすべてのデスクトップにユーザーがログインできるようにします。全員が同時にログインする必要がない場合、この設定を行うことで、必要なデスクトップの数を削減できます。
- インスタントクローンまたは View Composer リンククローン デスクトップを作成することで、デスクトップが同じ基本イメージを共有し、データセンターで使用するストレージ容量をフル仮想マシンより少なく済むようにします。
- View Composer デスクトップ プールについては、ユーザーがログアウトするときにどのようなアクションをとるか（必要な場合）を決定します。ディスクは、時間の経過とともに大きくなります。ユーザーがログオフするときにデスクトップを元の状態に更新すると、ディスク領域を節約できます。また、スケジュールを設定することでデスクトップを定期的に更新できます。たとえば、デスクトップが毎日、毎週、または毎月更新されるようにスケジュールを設定できます。
- インスタント クローン デスクトップ プールについては、ユーザーがログアウトすると View は自動的にインスタント クローンを削除します。新しいインスタント クローンが新規に作成され、次のユーザーがログインする準備が整います。このように、デスクトップはログアウトのたびに事実上更新されます。

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

注: その他のタイプのストレージ オプションの詳細については、[16 章 ストレージ要件の軽減と管理](#)を参照してください。

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

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

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

ナレッジ ワーカーとパワー ユーザー用プール

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

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

- 経理担当者、セールスマネージャ、市場調査アナリストなど、一部のパワー ユーザーおよびナレッジ ワーカーは毎回同じデスクトップにログインする必要がある場合があります。これらのユーザーについては、専用割り当てプールを作成します。
- 個人設定管理機能を使用すると、Windows のユーザー プロファイルと同じように、ユーザーは常に好みのデスクトップの外観とアプリケーションの設定を使用できます。
- 最初に、各デスクトップでディスクが初期の操作に必要とするストレージ容量のみが使用されるように、vStorage thin provisioning を使用します。
- 独自のアプリケーションをインストールする（これにより、オペレーティング システムのディスクにデータが追加されます）必要のあるパワー ユーザーおよびナレッジ ワーカーの場合は、2 つのオプションがあります。1 つ目のオプションは、フル仮想マシン デスクトップを作成し、Mirage を使用して、ユーザーがインストールしたアプリケーションを上書きせずにアプリケーションの展開と更新を行う方法です。

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

- ナレッジ ワーカーが、一時的な使用を除き、ユーザーがインストールするアプリケーションを必要としない場合は、View Composer リンククローン デスクトップまたはインスタント クローン デスクトップを作成できます。デスクトップ イメージは同じ基本イメージを共有し、フル仮想マシンより少ないストレージ容量を使用します。
- vSphere 5.1 以降の仮想デスクトップで View Composer を使用する場合は、vCenter Server およびデスクトップ プール用の領域再利用機能を有効にします。領域再利用機能を使用すれば、ゲスト OS 内の無効または削除されたデータは自動的にワイブおよび縮小プロセスで再利用されます。
- View Composer のリンク クローン デスクトップを使用する場合、View Persona Management、移動プロファイル、または別のプロファイル管理ソリューションを実装します。また、ユーザー プロファイルのローカル コピーを通常ディスクに保持しながら、リンククローン OS ディスクを更新および再構成できるように、通常ディスクを構成できます。
- インスタント クローン デスクトップを使用する場合は、移動プロファイルまたは他のプロファイル管理ソリューションを実装します。通常ディスクを構成する必要はありません。App Volumes を使用して、ユーザー データおよびプロファイルのコピーを保持します。

キオスク ユーザー用プール

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

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

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

キオスク モードを設定するには、vdmadmin コマンドライン インターフェイスを使用し、『View の管理ガイド』のキオスク モードに関するトピックに記載されているいくつかの手順を実行する必要があります。このセットアップの一部として、次のプールの設定を使用できます。

- 自動プールを作成して、そのプールの作成時にデスクトップが作成されるようにするか、プールの使用量に基づいてオン デマンドでデスクトップが生成されるようにすることができます。
- ユーザーがプール内の任意の使用可能なデスクトップにアクセスできるように、流動割り当てを使用します。

- インスタントクローンまたは View Composer リンククローン デスクトップを作成することで、デスクトップが同じ基本イメージを共有し、データセンターで使用するストレージ容量をフル仮想マシンより少なく済むようにします。
- View Composer のリンククローン デスクトップを使用している場合は、デスクトップが頻繁に更新されるように、更新ポリシーを設定します。たとえば、ユーザーのログアウトのたびに毎回更新されるように設定します。
- インスタント クローン デスクトップ プールを使用している場合は、ユーザーがログアウトすると View は自動的にインスタント クローンを削除します。新しいインスタント クローンが新規に作成され、次のユーザーがログインする準備が整います。このように、デスクトップはログアウトのたびに事実上更新されます。
- 可能な場合には、ローカルの ESXi データストアにデスクトップを格納することを確認してください。この方法には、安価なハードウェア、仮想マシンの迅速なプロビジョニング、高性能の電力操作、およびシンプルな管理などの利点があります。制限事項のリストについては、[ローカル データストアへの View Composer リンク クローンの保存](#)を参照してください。ローカル データ ストアでは、インスタント クローン プールはサポートされません。

注: その他のタイプのストレージ オプションの詳細については、[16 章 ストレージ要件の軽減と管理](#)を参照してください。

- デスクトップに対して最も近いプリンタが使用されるように、ロケーションベースの印刷を構成するための Active Directory GPO（グループ ポリシー オブジェクト）を使用します。グループ ポリシー管理 (ADM) テンプレートで使用できる設定の詳細なリストと説明については、[17 章 デスクトップ プールとアプリケーション プールのポリシーの構成](#)を参照してください。
- GPO またはスマート ポリシーを使用して、デスクトップが起動されたとき、またはクライアント コンピュータに USB デバイスが挿入されたときに、ローカル USB デバイスがデスクトップに接続されるかどうかを制御します。

アプリケーション プールの利点

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

アプリケーション プールには複数の大きな利点があります。

■ アクセシビリティ

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

■ デバイスの独立性

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

■ アクセス制御

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

■ 展開の加速化

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

■ 管理性

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

■ セキュリティと規制コンプライアンス

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

■ コスト削減

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

非管理対象マシンの準備

ユーザーは、vCenter Server によって管理されないマシンから配布されるリモート デスクトップにアクセスできます。これらの非管理対象マシンには、vCenter Server 以外の仮想化プラットフォームで実行される物理コンピュータおよび仮想マシンが含まれます。リモート デスクトップ アクセスを提供するには非管理対象マシンを準備する必要があります。

リモート デスクトップ サービス (RDS) ホストとして使用するマシンの準備については、[8 章 リモート デスクトップ サービス ホストの設定](#)を参照してください。

リモート デスクトップの展開に使用する Linux 仮想マシンの準備については、Horizon 7 for Linux デスクトップのセットアップを参照してください。

この章には、次のトピックが含まれています。

- [リモート デスクトップ展開用の非管理対象マシンの準備](#)
- [非管理対象マシンでの Horizon Agent のインストール](#)

リモート デスクトップ展開用の非管理対象マシンの準備

リモート デスクトップ展開のために非管理対象マシンを準備するタスクを実行する必要があります。

前提条件

- 非管理対象マシンに対して管理者権限を持っていることを確認します。
- リモート デスクトップ ユーザーが非管理対象マシンのローカルの Remote Desktop Users グループに追加されるようにするには、制限付きの Remote Desktop Users グループを Active Directory に作成します。詳細については、『View のインストール』を参照してください。

手順

- 1 非管理対象マシンをパワーオンし、View 接続サーバ インスタンスにアクセスできることを確認します。
- 2 非管理対象マシンをリモート デスクトップ用の Active Directory ドメインに参加させます。
- 3 非管理対象マシンへのリモート デスクトップ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。

次のステップ

非管理対象マシンに Horizon Agent をインストールします。[非管理対象マシンでの Horizon Agent のインストール](#)を参照してください。

非管理対象マシンでの Horizon Agent のインストール

すべての非管理対象マシンに Horizon Agent をインストールする必要があります。View では、Horizon Agent がインストールされていないと非管理対象マシンを管理できません。

Horizon Agent のサイレント インストールを実行すると、ウィザードのプロンプトに応答することなく複数の Windows 物理コンピュータに Horizon Agent をインストールできます。 [Horizon Agent のサイレント インストール](#)を参照してください。

前提条件

- 非管理対象マシンに対して管理者権限を持っていることを確認します。
- 非管理対象の Windows Server マシンを RDS ホストではなくリモート デスクトップとして使用するには、[デスクトップで使用するための Windows Server OS の準備](#)に記載されている手順を実行します。
- 非管理対象マシン用の Horizon Agent カスタム セットアップ オプションについて理解しておきます。 [非管理対象マシン用の Horizon Agent のカスタム セットアップ オプション](#)を参照してください。
- Horizon Agent インストール プログラムによってファイアウォール上で開かれる TCP ポートについて理解しておきます。詳細については、『View アーキテクチャの計画』ドキュメントを参照してください。
- マシンに Microsoft Visual C++ Redistributable パッケージがインストールされている場合、パッケージのバージョンが 2005 SP1 以降であることを確認します。パッケージのバージョンが 2005 以前の場合、パッケージのアップグレードまたはアンインストールのいずれかが可能です。
- VMware 製品ページ <http://www.vmware.com/go/downloadview> から、Horizon Agent インストーラ ファイルをダウンロードします。

手順

- 1 Horizon Agent 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。
インストーラのファイル名は、VMware-viewagent-y.y.y-xxxxxx.exe または VMware-viewagent-x86_64-y.y.y-xxxxxx.exe です。y.y.yはバージョン番号、xxxxxxはビルド番号です。
- 2 VMware のライセンス条件に同意します。
- 3 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 View 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。
- 4 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 モードが有効にされている場合にのみ使用可能です。
- 5 カスタム セットアップのオプションを選択します。
- 6 インストール先フォルダを受け入れるか、変更します。
- 7 [サーバ] テキスト ボックスに、View 接続サーバ ホストのホスト名または IP アドレスを入力します。
インストール時に、インストーラがこの View 接続サーバ インスタンスに非管理対象マシンを登録します。登録後、指定した View 接続サーバ インスタンスおよび同じ View 接続サーバ グループ内の他のインスタンスは非管理対象マシンと通信できます。

- 8 認証方式を選択して、View 接続サーバ インスタンスに非管理対象マシンを登録します。

オプション	アクション
現在ログインしているユーザーとして認証する	[ユーザー名] および [パスワード] テキスト ボックスは無効であり、現在のユーザー名とパスワードを使用して View 接続サーバ インスタンスにログインします。
管理者の認証情報を指定する	[ユーザー名] および [パスワード] テキスト ボックスに、View 接続サーバ管理者のユーザー名とパスワードを入力する必要があります。

Domain\User の形式でユーザー名を入力します。

ユーザー アカウントは、View 接続サーバ インスタンスで View LDAP にアクセスできるドメイン ユーザーでなければなりません。ローカル ユーザーは使用できません。

- 9 Horizon Agent インストール プログラムの指示に従ってインストールを終了します。
- 10 USB リダイレクト オプションを選択した場合は、非管理対象マシンを再起動して USB サポートを有効にします。

さらに、[新しいハードウェアが見つかりました] ウィザードが起動する場合があります。非管理対象マシンを再起動する前に、ウィザードの指示に従ってハードウェアを構成します。

VMware Horizon Horizon Agent サービスが非管理対象マシンで開始されます。

次のステップ

非管理対象マシンを使用してリモート デスクトップを作成します。[手動デスクトップ プール](#)を参照してください。

非管理対象マシン用の Horizon Agent のカスタム セットアップ オプション

非管理対象マシンに Horizon Agent をインストールするとき、カスタム セットアップ オプションをオンまたはオフにできます。また、Horizon Agent は特定の機能を、サポートされているすべてのゲスト OS に自動的にインストールします。これらの機能はオプションではありません。

最新の Horizon Agent バージョンをインストールした後でカスタム セットアップ オプションを変更するには、Horizon Agent をアンインストールしてから再インストールする必要があります。パッチおよびアップグレードの場合、前のバージョンをアンインストールすることなく、新しい Horizon Agent インストーラを実行して、新しいオプション セットを選択できます。

表 2-1. IPv4 環境の非管理対象マシンに対する Horizon Agent のカスタム セットアップ オプション (オプション)

オプション	説明
USB リダイレクト	<p>デスクトップにローカルに接続されている USB デバイスにユーザーがアクセスできるようにします。</p> <p>USB リダイレクトは、単一ユーザー マシンに展開されたりリモート デスクトップでサポートされます。また、USB フラッシュ ドライブとハード ディスクのリダイレクトは、RDS デスクトップとアプリケーションでサポートされます。</p> <p>デフォルトではこのセットアップ オプションは選択されていません。このオプションを選択してインストールする必要があります。</p> <p>USB リダイレクトを安全に使用するガイダンスについては、『View セキュリティ』ガイドを参照してください。たとえば、グループ ポリシー設定を使用して、特定のユーザーの USB リダイレクトを無効にすることができます。</p>
クライアント ドライブ リダイレクト	<p>これを使用すると、Horizon Client ユーザーはリモート デスクトップとローカル ドライブを共有できます。</p> <p>このセットアップ オプションがインストールされた後は、リモート デスクトップではこれ以上の構成は必要ありません。</p> <p>クライアント ドライブ リダイレクトは、管理された単一ユーザー仮想マシン上で実行されている VDI デスクトップと、RDS デスクトップおよびアプリケーションでもサポートされます。</p>
View Persona Management	<p>ローカル デスクトップのユーザー プロファイルをリモート プロファイル リポジトリと同期させて、ユーザーがデスクトップにログインするときはいつでもユーザー プロファイルにアクセスできるようにします。</p>
Smartcard リダイレクト	<p>ユーザーが、PCoIP または Blast Extreme 表示プロトコルの使用時にスマート カードを使用して認証できるようにします。</p> <p>Smartcard リダイレクトは、単一ユーザー マシンに展開されたりリモート デスクトップでサポートされますが、RDS ホストベースのリモート デスクトップではサポートされません。</p>
仮想オーディオ ドライバ	<p>リモート デスクトップに仮想オーディオ ドライバを提供します。</p>

IPv6 環境のオプション機能は、Smartcard リダイレクトのみです。

表 2-2. IPv4 環境の非管理対象マシンに自動インストールされる Horizon Agent の機能 (非オプション)

機能	説明
PCoIP エージェント	<p>ユーザーが PCoIP 表示プロトコルを使用してリモート デスクトップに接続できるようにします。</p> <p>PCoIP Agent 機能は、Teradici TERA ホスト カードを使用して構成された物理マシン上でサポートされます。</p>
Lync	<p>リモート デスクトップで Microsoft Lync 2013 クライアントをサポートします。</p>
Unity Touch	<p>タブレットおよびスマートフォン ユーザーがリモート デスクトップで実行している Windows アプリケーションを容易に操作できます。ユーザーはすべてスタート メニューまたはタスクバーを使用せずに、Windows アプリケーションやファイルの参照、検索、およびオープンを行ったり、お気に入りのアプリケーションやファイルを選択したり、実行しているアプリケーションを切り替えたりすることができます。</p>

IPv6 環境で自動インストールされる機能は、PCoIP Agent のみです。

クローン作成のための親仮想マシンの作成と準備

3

vCenter Server 仮想マシン (VM) のクローンを作成することによって、デスクトップマシンのプールを作成できます。デスクトップ プールを作成する前に、クローンの親となるこの仮想マシンを準備して構成する必要があります。

リモート デスクトップ サービス (RDS) ホストとして使用するマシンの準備については、[8 章 リモート デスクトップ サービス ホストの設定](#)を参照してください。

リモート デスクトップを展開するための Linux 仮想マシンの準備に関する情報は、『Horizon 7 for Linux デスクトップのセットアップ』ガイドを参照してください。

注:

- バージョン 7.0 以降、View Agent は Horizon Agent に名称変更され、View Administrator は Horizon Administrator に名前変更されています。
 - Horizon 7.0 以降で使用可能な表示プロトコルである VMware Blast は、VMware Blast Extreme とも呼ばれます。
-

この章には、次のトピックが含まれています。

- [クローン作成のための仮想マシンの作成](#)
- [仮想マシンへの Horizon Agent のインストール](#)
- [Horizon Agent のサイレント インストール](#)
- [Horizon Agent のための複数の NIC を使用する仮想マシンの構成](#)
- [ゲスト OS のパフォーマンスの最適化](#)
- [Windows カスタマー エクスペリエンス向上プログラムを無効にする](#)
- [インスタントクローンおよび View Composer リンククローン仮想マシン用の Windows のカスタマイズ](#)
- [親仮想マシンの準備](#)
- [仮想マシン テンプレートの作成](#)
- [カスタマイズ仕様の作成](#)

クローン作成のための仮想マシンの作成

クローン作成されたデスクトップのプールを展開するプロセスでは、最初に vSphere で仮想マシンを作成し、オペレーティング システムをインストールして構成します。

手順

1 vSphere での仮想マシンの作成

一から、または既存の仮想マシンのクローンを作成することで、vSphere で仮想マシンを作成できます。この手順では、一から仮想マシンを作成する方法について説明します。

2 ゲスト OS のインストール

仮想マシンを作成したら、ゲスト OS をインストールする必要があります。

3 リモート デスクトップの展開のためのゲスト OS の準備

リモート デスクトップの展開のためにゲスト OS を準備する特定のタスクを実行する必要があります。

4 デスクトップで使用するための Windows Server OS の準備

Windows Server 2008 R2、または Windows Server 2012 R2 仮想マシンを（RDS ホストとしてではなく）単一セッションの View デスクトップとして使用するには、Horizon Agent を仮想マシンにインストールする前に、特定の手順を実行する必要があります。Windows Server を View デスクトップ対応のオペレーティング システムとして扱うように View Administrator を構成する必要もあります。

5 Windows Server 2008 R2 へのデスクトップ エクスペリエンスのインストール

RDS デスクトップとアプリケーション、および Windows Server を実行するシングルユーザー仮想マシンに展開された VDI デスクトップの場合、スキャナ リダイレクトを使用するには、RDS ホストおよびシングルユーザー仮想マシンにデスクトップ エクスペリエンス機能をインストールする必要があります。

6 Windows Server 2012 または 2012 R2 へのデスクトップ エクスペリエンスのインストール

RDS デスクトップとアプリケーション、および Windows Server を実行するシングルユーザー仮想マシンに展開された VDI デスクトップの場合、スキャナ リダイレクトを使用するには、RDS ホストおよびシングルユーザー仮想マシンにデスクトップ エクスペリエンス機能をインストールする必要があります。

7 障害発生後に Windows ファイアウォール サービスを再起動させるための構成

シングルセッション デスクトップとしてデプロイされた一部の Windows Server 2012 R2、Windows 8.1、および Windows 10 マシンは、プロビジョニングされた後、すぐには使用可能にならない場合があります。この問題は、タイムアウトの期限が切れた後、Windows ファイアウォール サービスが再起動されない場合に発生します。デスクトップ プール内のすべてのマシンが使用可能になるように、親仮想マシンまたはテンプレート仮想マシンで Windows ファイアウォール サービスを構成できます。

vSphere での仮想マシンの作成

一から、または既存の仮想マシンのクローンを作成することで、vSphere で仮想マシンを作成できます。この手順では、一から仮想マシンを作成する方法について説明します。

前提条件

- 仮想マシンのカスタム構成パラメータについて理解しておきます。[仮想マシンのカスタム構成パラメータ](#)を参照してください。

手順

- 1 vSphere Client にログインします。
- 2 [ファイル] - [新規] - [仮想マシン]を選択し、[新しい仮想マシン] ウィザードを起動します。
- 3 [カスタム]を選択し、カスタム構成パラメータを構成します。
- 4 [完了前に仮想マシンの設定を編集]を選択し、[続行]をクリックしてハードウェア設定を構成します。
 - a CD/DVD ドライブを追加し、ISO イメージ ファイルを使用するようにメディアの種類を設定し、適切なオペレーティング システムの ISO イメージ ファイルを選択した後、[パワーオン時に接続]を選択します。
 - b [パワーオン ブート遅延]を 10,000 ミリ秒に設定します。
- 5 [終了]をクリックして仮想マシンを作成します。

次のステップ

オペレーティング システムをインストールします。

仮想マシンのカスタム構成パラメータ

リモート デスクトップの展開のための仮想マシンを作成するときは、仮想マシンのカスタム構成パラメータを基本状態の設定として使用できます。

View Administrator を使用して仮想マシンからデスクトップ プールを展開するときは、特定の設定を変更できます。

表 3-1. カスタム構成パラメータ

パラメータ	説明および推奨事項
Name and Location	仮想マシンの名前と場所。 仮想マシンをテンプレートとして使用する予定の場合は、総称的な名前を割り当てます。場所には、データセンター インベントリ内の任意のフォルダを使用できます。
Host/Cluster	仮想マシンを実行する ESXi サーバまたはサーバ リソースのクラスタ。 仮想マシンをテンプレートとして使用する予定の場合、最初の仮想マシンの場所では、テンプレートから今後作成される仮想マシンが配置される場所を指定しなくても構いません。
Resource Pool	物理 ESXi サーバ リソースがリソース プールに分割される場合は、それらを仮想マシンに割り当てることができます。
Datastore	仮想マシンと関連付けられるファイルの場所。
Hardware Machine Version	使用できるハードウェア マシン バージョンは、実行している ESXi バージョンに応じて異なります。ベスト プラクティスとして、最高の仮想マシン機能を備えた、利用可能な最新のハードウェア マシン バージョンを選びます。View 機能の中には、最小バージョンのハードウェア マシンを必要とするものもあります。
Guest Operating System	仮想マシンをインストールするオペレーティング システムの種類。
CPUs	仮想マシン内の仮想プロセッサの数。 ほとんどのゲスト OS には、1 つのプロセッサで十分です。

パラメータ	説明および推奨事項
Memory	<p>仮想マシンに割り当てるメモリの容量。</p> <p>ほとんどの場合、512 MB で十分です。</p>
Network	<p>仮想マシン内の仮想ネットワーク アダプタ (NIC) の数。</p> <p>通常、1 つの NIC で十分です。ネットワーク名は、仮想インフラストラクチャ間で一貫性を保つ必要があります。テンプレート内のネットワーク名が正しくないと、インスタンスのカスタマイズ フェーズでエラーが発生する可能性があります。</p> <p>複数の NIC を使用する仮想マシンに Horizon Agent をインストールするときは、Horizon Agent が使用するサブネットを設定する必要があります。詳細については、Horizon Agent のための複数の NIC を使用する仮想マシンの構成を参照してください。</p> <p>重要: Windows 7、Windows 8*、Windows 10、Windows Server 2008 R2、および Windows Server 2012 R2 オペレーティング システムの場合は、VMXNET 3 ネットワーク アダプタを選択する必要があります。デフォルトの E1000 アダプタを使用すると、仮想マシン上でカスタマイズ タイムアウト エラーが発生する可能性があります。VMXNET 3 アダプタを使用するには、Microsoft 修正プログラムをインストールする必要があります。</p> <p>Windows 7 SP1 では、次の修正プログラムをインストールします。</p> <ul style="list-style-type: none"> ■ http://support.microsoft.com/kb/2550978 <p>Horizon Agent をインストールする前に修正プログラムをインストールします。修正プログラムをインストールするときに Windows Update のエラー 0x80070424 が発生する場合は、https://support.microsoft.com/en-us/kb/968002 を参照してください。</p> <ul style="list-style-type: none"> ■ https://support.microsoft.com/en-au/kb/2578159 ■ https://support.microsoft.com/en-au/kb/2661332 <p>修正プログラムのインストールの詳細については、https://kb.vmware.com/kb/2073945 を参照してください。</p>
SCSI Controller	<p>仮想マシンで使用する SCSI アダプタのタイプ。</p> <p>Windows 8/8.1 および Windows 7 ゲスト オペレーティング システム の場合は、LSI Logic アダプタを指定する必要があります。LSI Logic アダプタはパフォーマンスが向上しており、汎用 SCSI デバイスで高い性能を発揮します。</p> <p>LSI Logic SAS は、ハードウェア バージョン 7 以降の仮想マシンでのみ使用できます。</p>
Select a Disk	<p>仮想マシンで使用するディスク。</p> <p>各ユーザーに割り当てることを決定したローカル ストレージの容量に基づいて新しい仮想ディスクを作成します。OS インストール、パッチ、およびローカルにインストールされているアプリケーションに十分なストレージ領域を割り当てます。</p> <p>必要なディスク領域を減らし、ローカル データの管理を軽減するために、ユーザーの情報、プロファイル、およびドキュメントはローカル ディスクではなくネットワーク共有に保存してください。</p>

ゲスト OS のインストール

仮想マシンを作成したら、ゲスト OS をインストールする必要があります。

前提条件

- ゲスト OS の ISO イメージ ファイルが ESXi サーバ上のデータストアに存在していることを確認します。
- 仮想マシンの CD/DVD ドライブがゲスト OS の ISO イメージ ファイルを参照しており、CD/DVD ドライブがパワーオン時に接続されるように構成されていることを確認します。

手順

- 1 vSphere Client で、仮想マシンが存在する vCenter Server システムにログインします。
- 2 仮想マシンを右クリックし、[パワー] を選択し、[パワーオン] を選択して仮想マシンを起動します。
CD/DVD ドライブを、ゲスト OS の ISO イメージを参照し、パワーオン時に接続されるように構成したため、ゲスト OS のインストール プロセスが自動的に開始されます。
- 3 [コンソール] タブをクリックし、オペレーティング システム ベンダによって提供されるインストール手順を実行します。
- 4 Windows のアクティベーションをします。

次のステップ

View デスクトップの展開のためにゲスト OS を準備します。

リモート デスクトップの展開のためのゲスト OS の準備

リモート デスクトップの展開のためにゲスト OS を準備する特定のタスクを実行する必要があります。

前提条件

- 仮想マシンを作成し、ゲスト OS をインストールします。
- リモート デスクトップのための Active Directory ドメイン コントローラを構成します。詳細については、『View のインストール』ドキュメントを参照してください。
- デスクトップ ユーザーが仮想マシンのローカルの Remote Desktop Users グループに追加されていることを確認するには、制限付きの Remote Desktop Users グループを Active Directory に作成します。詳細については、『View のインストール』ドキュメントを参照してください。
- リモート デスクトップ サービスが仮想マシンで開始していることを確認します。リモート デスクトップ サービスは Horizon Agent のインストール、SSO、およびその他の View 操作に必要です。デスクトップ プール設定およびグループ ポリシー設定を構成することにより View デスクトップへの RDP アクセスを無効にできます。[View デスクトップへの RDP を使用したアクセスの防止](#)を参照してください。
- ゲスト OS に対する管理者権限があることを確認します。
- Windows Server オペレーティング システムで、デスクトップで使用するオペレーティング システムを準備します。[デスクトップで使用するための Windows Server OS の準備](#)を参照してください。
- デスクトップ プールに 3D グラフィックス レンダリングを構成したい場合、仮想マシンの [3D サポートを有効にする] 設定を理解しておきます。

この設定は、Windows 7 以降のオペレーティング システムで有効になります。ESXi 5.1 以降のホストでは、ESXi ホストで 3D レンダラーがどのように管理されるかを決定するオプションを選択することもできます。詳細については、『vSphere Virtual Machine Administration』ドキュメントを参照してください。

手順

- 1 vSphere Client で、仮想マシンが存在する vCenter Server システムにログインします。
- 2 仮想マシンを右クリックし、[パワー] を選択し、[パワーオン] を選択して仮想マシンを起動します。

- 3 仮想マシンを右クリックし、[ゲスト] を選択し、[VMware Tools のインストール/アップグレード] を選択して最新バージョンの VMware Tools をインストールします。

注: 仮想印刷機能は、Horizon Agent からインストールする場合に限ってサポートされます。VMware Tools でインストールした場合、仮想印刷はサポートされません。

- 4 VMware Tools の時刻同期機能を使用して、仮想マシンが ESXi と同期されていることを確認します。

ESXi は、外部の NTP ソース（たとえば、Active Directory と同じタイム ソース）と同期している必要があります。

Windows Time サービスなど、その他の時間同期機能を無効にします。

VMware Tools のオンライン ヘルプに、ゲストとホストの間の時刻同期の構成に関する情報が提供されています。

- 5 サービス パックと更新プログラムをインストールします。

- 6 ウイルス対策ソフトウェアをインストールします。

- 7 スマート カード認証を使用する場合は、スマート カード ドライバなど、その他のアプリケーションおよびソフトウェアをインストールします。

ThinApp アプリケーションを含むカタログを提供するために VMware Identity Manager を使用する予定である場合、VMware Identity Manager for Windows をインストールする必要があります。

重要: Microsoft .NET Framework をインストールする場合は、Horizon Agent をインストールした後にインストールする必要があります。

- 8 Horizon Client デバイスが PCoIP 表示プロトコルを使用して仮想マシンに接続する場合は、[ディスプレイの電源を切る] の電源オプションを [なし] に設定します。

この設定を無効にしない場合は、省電力モードが開始されたときに、ディスプレイが最後の状態でフリーズしたように見えます。

- 9 Horizon Client デバイスが PCoIP 表示プロトコルで仮想マシンに接続する場合、[コントロール パネル] - [システム] - [詳細システム設定] - [パフォーマンス設定] の順に選択し、[視覚効果] の設定を [パフォーマンスを優先する] に設定します。

[パフォーマンスを優先する] または [コンピュータにとって何が最も優先されるかの選択を Windows に任せる] と呼ばれる設定を代わりに使用すると、Windows はパフォーマンスの代わりに外観を選択し、パフォーマンスに悪影響を及ぼします。

- 10 ネットワーク環境でプロキシ サーバが使用されている場合は、ネットワーク プロキシの設定を構成します。

- 11 ネットワーク接続のプロパティを構成します。

- a 固定 IP アドレスを割り当てるか、または DHCP サーバによって IP アドレスが割り当てられるように指定します。

View は、View デスクトップのリンク ローカル (169.254.x.x) アドレスをサポートしていません。

- b 優先および代替 DNS サーバ アドレスを Active Directory サーバ アドレスに設定します。

- 12 (オプション) 仮想マシンをリモート デスクトップ用の Active Directory ドメインに参加させます。

インスタント クローンまたは View Composer リンク クローンを作成するための親仮想マシンは、デスクトップ マシンが参加するドメインと同じ Active Directory ドメインに属するか、ワークグループのメンバーである必要があります。

- 13 仮想マシンへのリモート デスクトップ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。

- 14 (オプション) ホット プラグ PCI デバイスを無効にします。

この手順は、ユーザーが仮想マシンから仮想ネットワーク デバイス (vNIC) を誤って切断することを防ぎます。

- 15 (オプション) ユーザー カスタマイズ スクリプトを構成します。

デスクトップで使用するための Windows Server OS の準備

Windows Server 2008 R2、または Windows Server 2012 R2 仮想マシンを (RDS ホストとしてではなく) 単一セッションの View デスクトップとして使用するには、Horizon Agent を仮想マシンにインストールする前に、特定の手順を実行する必要があります。Windows Server を View デスクトップ対応のオペレーティング システムとして扱うように View Administrator を構成する必要があります。

前提条件

- Windows Server 2008 R2 または Windows Server 2012 R2 でデスクトップ エクスペリエンス機能をインストールする手順を理解しておきます。[Windows Server 2008 R2 へのデスクトップ エクスペリエンスのインストール](#) または [Windows Server 2012 または 2012 R2 へのデスクトップ エクスペリエンスのインストール](#) を参照してください。
- Windows Server 2012 R2 マシンで、障害が発生した後に Windows ファイアウォール サービスが再起動されるように構成する手順を理解しておきます。[障害発生後に Windows ファイアウォール サービスを再起動させるための構成](#)を参照してください。

手順

- 1 リモート デスクトップ サービス ロールがインストールされていないことを確認します。

リモート デスクトップ サービス ロールが存在しない場合、Horizon Agent インストーラから Horizon Agent をデスクトップ モードでインストールすることを確認するよう求められます。リモート デスクトップ サービス ロールが存在する場合、Horizon Agent インストーラはこのプロンプトを表示せず、Windows Server マシンを、単一セッションの View デスクトップではなく、RDS ホストとして扱います。

- 2 Windows Server 2008 R2 Service Pack 1 (SP1) または Windows Server 2012 R2 をインストールします。

Windows Server 2008 R2 とともに SP1 をインストールせずに Horizon Agent をインストールすると、エラーが発生します。

- 3 (オプション) 次の機能を使用する予定がある場合は、デスクトップ エクスペリエンス機能をインストールします。

- HTML Access
- スキャナ リダイレクト
- Windows Aero

- 4 (オプション) Windows Aero を Windows Server デスクトップで使用するには、テーマ サービスを開始します。

デスクトップ プールを作成または編集する際に、デスクトップの 3D グラフィックス レンダリングを構成できます。3D レンダラー設定は、Windows Aero をプール内のデスクトップで実行できるようにするソフトウェア オプションを提供します。

- 5 Windows Server 2012 R2 マシンで、障害が発生した後に Windows ファイアウォール サービスが再起動されるように構成します。
- 6 Windows Server をデスクトップ対応のオペレーティング システムとして扱うように View Administrator を構成します。

この手順を実行しなければ、View Administrator でデスクトップ用に Windows Server マシンを選択できません。

- a View Administrator で、[View 構成] - [グローバル設定] を選択します。
- b [全般] ペインで、[編集] をクリックします。
- c [Windows Server デスクトップを有効にする] チェックボックスを選択して、[OK] をクリックします。

Windows Server デスクトップを View Administrator で有効にすると、View Administrator は View 接続サーバがインストールされているマシンを含む使用可能な Windows Server マシンのすべてを、デスクトップ用の潜在的マシンとして表示します。Horizon Agent を他の View ソフトウェア コンポーネントがインストールされたマシンにインストールできません。

Windows Server 2008 R2 へのデスクトップ エクスペリエンスのインストール

RDS デスクトップとアプリケーション、および Windows Server を実行するシングルユーザー仮想マシンに展開された VDI デスクトップの場合、スキャナ リダイレクトを使用するには、RDS ホストおよびシングルユーザー仮想マシンにデスクトップ エクスペリエンス機能をインストールする必要があります。

手順

- 1 管理者としてログインします。
- 2 Server Manager を開始します。
- 3 [機能] をクリックします。
- 4 [機能の追加] をクリックします。
- 5 [機能を選択] ページで、[デスクトップ エクスペリエンス] チェックボックスを選択します。
- 6 デスクトップ エクスペリエンス機能で必要な他の機能に関する情報を確認し、[必要な機能の追加] をクリックします。
- 7 指示に従ってインストールを終了します。

Windows Server 2012 または 2012 R2 へのデスクトップ エクスペリエンスのインストール

RDS デスクトップとアプリケーション、および Windows Server を実行するシングルユーザー仮想マシンに展開された VDI デスクトップの場合、スキャナ リダイレクトを使用するには、RDS ホストおよびシングルユーザー仮想マシンにデスクトップ エクスペリエンス機能をインストールする必要があります。

Windows Server 2012 および Windows Server 2012 R2 は、RDS ホストとして使用されるマシンでサポートされています。Windows Server 2012 R2 はシングル ユーザー仮想マシンでサポートされています。

手順

- 1 管理者としてログインします。
- 2 Server Manager を開始します。
- 3 [ロールと機能を追加] を選択します。
- 4 [インストール タイプを選択] ページで、[ロールベースまたは機能ベースのインストール] を選択します。
- 5 [ターゲット サーバを選択] ページで、サーバを選択します。
- 6 [サーバ ロールを選択] ページで、デフォルトの選択を受け入れ、[次へ] をクリックします。
- 7 [機能を選択] ページで、[ユーザー インターフェイスとインフラストラクチャ] の下で [デスクトップ エクスペリエンス] を選択します。
- 8 指示に従ってインストールを完了します。

障害発生後に Windows ファイアウォール サービスを再起動させるための構成

シングルセッション デスクトップとしてデプロイされた一部の Windows Server 2012 R2、Windows 8.1、および Windows 10 マシンは、プロビジョニングされた後、すぐには使用可能にならない場合があります。この問題は、タイムアウトの期限が切れた後、Windows ファイアウォール サービスが再起動されない場合に発生します。デスクトップ プール内のすべてのマシンが使用可能になるように、親仮想マシンまたはテンプレート仮想マシンで Windows ファイアウォール サービスを構成できます。

プロビジョニング中にこの問題が発生した場合、Windows イベント ログに次のようなエラー メッセージが表示されます: Windows ファイアウォール サービスは次のサービス固有のエラーによって終了しました。タイムアウトの期限が切れたため、このオペレーションは戻されました。

この問題は、Windows Server 2012 R2、Windows 8.1、および Windows 10 マシンで発生します。その他のゲスト OS は影響を受けません。

手順

- 1 デスクトップ プールのデプロイ元となる Windows Server 2012 R2、Windows 8.1、または Windows 10 の親仮想マシンまたはテンプレート仮想マシンで、[コントロール パネル] - [管理ツール] - [サービス] を選択します。
- 2 [サービス] ダイアログ ボックスで [Windows ファイアウォール] サービスを右クリックし、[プロパティ] を選択します。
- 3 [Windows ファイアウォールのプロパティ] ダイアログ ボックスで、[リカバリ] タブをクリックします。

- 4 障害が発生した後にサービスを再起動するリカバリ設定を選択します。

設定	ドロップダウン メニュー オプション
最初の障害 :	[サービスの再起動]
2 番目の障害 :	[サービスの再起動]
それ以降の障害 :	[サービスの再起動]

- 5 [エラーで停止するようにアクションを有効化] チェックボックスを選択し、[OK] をクリックします。
- 6 親仮想マシンまたはテンプレート仮想マシンからデスクトップ プールを展開または再展開します。

仮想マシンへの Horizon Agent のインストール

接続サーバが、vCenter Server によって管理される仮想マシンと通信できるようにするには、それらの仮想マシンに Horizon Agent をインストールする必要があります。完全クローン デスクトップ プールのテンプレート、リンク クローン デスクトップ プールの親、インスタントクローン デスクトップ プールの親、および手動デスクトップ プール内のマシンとして使用するすべての仮想マシンに Horizon Agent をインストールします。

Horizon Agent のサイレント インストールを実行すると、ウィザードのプロンプトに応答することなく複数の Windows 仮想マシンに Horizon Agent をインストールできます。 [Horizon Agent のサイレント インストール](#) を参照してください。

Horizon Agent ソフトウェアは、セキュリティ サーバ、接続サーバ、View Composer など、他の Horizon 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できません。Horizon Client では共在できます。

前提条件

- リモート デスクトップの展開のためにゲスト OS を準備します。 [リモート デスクトップの展開のためのゲスト OS の準備](#) を参照してください。
- Windows Server 仮想マシンを（RDS ホストとしてではなく）リモート デスクトップとして使用するには、 [デスクトップで使用するための Windows Server OS の準備](#) に説明されている手順を実行します。
- マシンに Microsoft Visual C++ Redistributable パッケージがインストールされている場合、パッケージのバージョンが 2005 SP1 以降であることを確認します。パッケージのバージョンが 2005 以前の場合、パッケージのアップグレードまたはアンインストールのいずれかが可能です。
- VMware 製品ページ <http://www.vmware.com/go/downloadview> から、Horizon Agent インストーラ ファイルをダウンロードします。
- 仮想マシンに対して管理者権限を持っていることを確認します。
- Horizon Agent のカスタム セットアップ オプションについて理解しておきます。 [Horizon Agent のカスタム セットアップ オプション](#) を参照してください。
- Horizon Agent インストール プログラムによってファイアウォール上で開かれる TCP ポートについて理解しておきます。詳細については、『View アーキテクチャの計画』ドキュメントを参照してください。

手順

- 1 Horizon Agent 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。
インストーラのファイル名は、VMware-viewagent-y.y.y-xxxxxx.exe または VMware-viewagent-x86_64-y.y.y-xxxxxx.exe です。y.y.y はバージョン番号、xxxxxx はビルド番号です。
- 2 VMware のライセンス条件に同意します。
- 3 リモート デスクトップ サービス (RDS) ロールがインストールされていない Windows Server マシンに Horizon Agent をインストールする場合は、[VMware Horizon Agent を「デスクトップ モード」でインストール] を選択します。

このオプションを選択すると、RDS ホストとしてではなくシングルユーザー View デスクトップとして Windows Server マシンが構成されます。マシンを RDS ホストとして機能させる場合は、Horizon Agent インストールをキャンセルして、マシンに RDS ロールをインストールし、Horizon Agent インストールをもう一度開始します。
- 4 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 View 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。
- 5 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。
- 6 カスタム セットアップのオプションを選択します。

View Composer リンク クローン デスクトップをデプロイするには、[VMware Horizon View Composer Agent] オプションを選択します。インスタントクローン デスクトップをデプロイするには、[VMware Horizon Instant Clone Agent] オプションを選択します。これらのオプションを両方とも選択することはできません。
- 7 インストール先フォルダを受け入れるか、変更します。
- 8 Horizon Agent インストール プログラムの指示に従ってインストールを終了します。

注: ゲスト OS の準備中にリモート デスクトップ サポートを有効にしなかった場合は、Horizon Agent インストール プログラムから有効にするよう求められます。Horizon Agent のインストール中にリモート デスクトップ サポートを有効にしない場合は、インストールの終了後に手動で有効にする必要があります。

- 9 USB リダイレクト オプションを選択した場合は、仮想マシンを再起動して USB サポートを有効にします。

さらに、[新しいハードウェアが見つかりました] ウィザードが起動する場合があります。仮想マシンを再起動する前に、ウィザードの指示に従ってハードウェアを構成します。

次のステップ

仮想マシンが複数の NIC を使用する場合は、Horizon Agent が使用するサブネットを構成します。 [Horizon Agent のための複数の NIC を使用する仮想マシンの構成](#)を参照してください。

Horizon Agent のカスタム セットアップ オプション

仮想マシンに Horizon Agent をインストールするときには、カスタム セットアップ オプションを選択または選択解除できます。また、Horizon Agent は特定の機能を、サポートされているすべてのゲスト OS に自動的にインストールします。これらの機能はオプションではありません。

ゲスト OS でサポートされる機能については、『View アーキテクチャの計画』の「Horizon Agent の機能サポートマトリックス」を参照してください。

最新の Horizon Agent バージョンをインストールした後でカスタム セットアップ オプションを変更するには、Horizon Agent をアンインストールしてから再インストールする必要があります。パッチおよびアップグレードの場合、前のバージョンをアンインストールすることなく、新しい Horizon Agent インストーラを実行して、新しいオプションセットを選択できます。

すべてのカスタム セットアップ オプションは、シリアル ポート リダイレクト、スキャナ リダイレクト、USB リダイレクト、Flash リダイレクト、Smartcard リダイレクト、および VMware Horizon Instant Clone Agent を除き、デフォルトで選択済みです。

表 3-2. IPv4 環境での Horizon Agent のカスタム セットアップ オプション

オプション	説明
Core	コア機能をインストールします。
シリアル ポート リダイレクト	<p>クライアント システムに接続される シリアル COM ポートをリダイレクトするので、それらをリモート デスクトップで使用できます。</p> <p>デフォルトではこのオプションが選択されていません。このオプションを選択してインストールする必要があります。</p> <p>シリアル ポート リダイレクトは、単一ユーザー マシンに展開されたリモート デスクトップ でサポートされます。シリアル ポート リダイレクトは Horizon 6 バージョン 6.1.1 以降のリリースで使用できます。</p>
スキャナ リダイレクト	<p>クライアント システムに接続されるスキャン デバイスおよびイメージング デバイスをリダイレクトするので、それらのデバイスをリモート デスクトップまたはアプリケーションで使用できます。</p> <p>デフォルトではこのオプションが選択されていません。このオプションを選択してインストールする必要があります。</p> <p>スキャナ リダイレクトは Horizon 6.0.2 以降のリリースで使用できます。</p>
USB リダイレクト	<p>デスクトップにローカルに接続されている USB デバイスにユーザーがアクセスできるようにします。</p> <p>USB リダイレクトは、単一ユーザー マシンに展開されたリモート デスクトップ でサポートされます。また、USB フラッシュ ドライブとハード ディスクのリダイレクトは、RDS デスクトップとアプリケーションでサポートされます。</p> <p>デフォルトではこのオプションが選択されていません。このオプションを選択してインストールする必要があります。</p> <p>USB リダイレクトを安全に使用するガイダンスについては、『View セキュリティ』ガイドを参照してください。たとえば、グループ ポリシー設定を使用して、特定のユーザーの USB リダイレクトを無効にすることができます。</p>
VMware Horizon View Composer Agent	この仮想マシンを View Composer リンク クローン デスクトップ プールの親仮想マシンにできるようにします。このオプションを選択した場合、[VMware Horizon Instant Clone Agent] オプションは選択できません。
VMware Horizon Instant Clone Agent	この仮想マシンをインスタントクローン デスクトップ プールの親仮想マシンにできるようにします。デフォルトではこのオプションが選択されていません。このオプションを選択した場合、[VMware Horizon View Composer Agent] オプションは選択できません。
リアルタイム オーディオビデオ	クライアント システムに接続される Web カメラおよびオーディオ デバイスをリダイレクトするので、それらをリモート デスクトップで使用できます。

オプション	説明
クライアント ドライブ リダイレクト	<p>これを使用すると、Horizon Client ユーザーはリモート デスクトップとローカル ドライブを共有できます。このオプションがインストールされた後は、リモート デスクトップではこれ以上の構成は必要ありません。クライアント ドライブ リダイレクトは RDS デスクトップおよびアプリケーションと、未管理のマシンで実行される VDI デスクトップ上でもサポートされます。</p>
仮想印刷	<p>ユーザーがクライアント コンピュータで利用できる任意のプリンタに出力できるようにします。ユーザーは、デスクトップに追加のドライバをインストールする必要はありません。</p> <p>仮想印刷は次のリモート デスクトップおよびアプリケーションでサポートされます。</p> <ul style="list-style-type: none"> ■ Windows デスクトップや Windows Server マシンなど、単一ユーザーのマシンにデプロイされたデスクトップ。 ■ 仮想マシンである RDS ホストにデプロイされたデスクトップ。 ■ リモート アプリケーション。 ■ リモート デスクトップ内部の Horizon Client から起動されるリモート アプリケーション（ネストされるセッション）。 <p>仮想印刷機能は、Horizon Agent からインストールする場合に限ってサポートされます。VMware Tools でインストールしてもサポートされません。</p>
vRealize Operations Desktop Agent	vRealize Operations for View が View デスクトップを監視するための情報を提供します。
View Persona Management	ローカル デスクトップのユーザー プロファイルをリモート プロファイル リポジトリと同期させて、ユーザーがデスクトップにログインするときはいつでもユーザー プロファイルにアクセスできるようにします。
Smartcard リダイレクト	<p>ユーザーが、PCoIP または Blast Extreme 表示プロトコルの使用時にスマート カードを使用して認証できるようにします。デフォルトではこのオプションが選択されていません。</p> <p>Smartcard リダイレクトは、単一ユーザー マシンにデプロイされたりリモート デスクトップでサポートされます。</p>
VMware オーディオ	リモート デスクトップに仮想オーディオ ドライバを提供します。
Flash リダイレクト	パフォーマンスの最適化のために、Internet Explorer 9、10、または 11 ブラウザでの Flash マルチメディア コンテンツをクライアントにリダイレクトします。Horizon 7.0 では、これは Tech Preview 機能です。Horizon 7.0.1 では、この機能は完全にサポートされます。

IPv6 環境のオプション機能は、VMware Horizon View Composer Agent、VMware Horizon Instant Clone Agent、および VMware オーディオのみです。

表 3-3. 自動的にインストールされる Horizon Agent 機能（非オプション）

機能	説明
PCoIP エージェント	<p>ユーザーが PCoIP 表示プロトコルを使用して View デスクトップに接続できるようにします。</p> <p>PCoIP Agent 機能をインストールすると、Windows デスクトップでスリープモードが無効になります。ユーザーが Power Options（電源オプション）または Shut Down（シャットダウン）メニューに移動すると、スリープモードまたはスタンバイモードは非アクティブになっています。非アクティブのデフォルトの期間が過ぎても、デスクトップはスリープモードやスタンバイモードになりません。デスクトップはアクティブモードのままです。</p>
Windows Media マルチメディア リダイレクト (MMR)	Windows 7 以降のデスクトップおよびクライアントにマルチメディアリダイレクトを拡張します。この機能は、クライアントコンピュータに直接マルチメディアストリームを配信し、これによってリモート ESXi ホストの代わりにクライアントハードウェアでマルチメディアストリームを処理できます。
Unity Touch	タブレットおよびスマートフォンユーザーがリモートデスクトップで実行している Windows アプリケーションを容易に操作できます。ユーザーはすべてスタートメニューまたはタスクバーを使用せずに、Windows アプリケーションやファイルの参照、検索、およびオープンを行ったり、お気に入りのアプリケーションやファイルを選択したり、実行しているアプリケーションを切り替えたりすることができます。
仮想ビデオドライバ	リモートデスクトップに仮想ビデオドライバを提供します。

IPv6 環境で自動インストールされる機能は、PCoIP Agent のみです。

Horizon Agent 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 仮想マシンまたは物理コンピュータに Horizon Agent 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応え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 View のコンポーネントを効率よく展開できます。

自動的に、つまりデフォルトでインストールされる機能の一部がインストールされないようにする場合は、ADDLOCAL MSI プロパティを使用して個々のセットアップ オプションと機能を選択的にインストールできます。ADDLOCAL プロパティの詳細については、[表 3-5. MSI コマンドライン オプションおよび MSI プロパティ](#)を参照してください。

前提条件

- デスクトップの展開のためにゲスト OS を準備します。[リモート デスクトップの展開のためのゲスト OS の準備](#)を参照してください。
- Windows Server マシンを（RDS ホストではなく）シングルセッションのリモート デスクトップとして使用するには、[デスクトップで使用するための Windows Server OS の準備](#)に記載されている手順を実行します。
- マシンに Microsoft Visual C++ Redistributable パッケージがインストールされている場合、パッケージのバージョンが 2005 SP1 以降であることを確認します。パッケージのバージョンが 2005 以前の場合、パッケージのアップグレードまたはアンインストールのいずれかが可能です。

- VMware 製品ページ <http://www.vmware.com/go/downloadview> から、Horizon Agent インストーラ ファイルをダウンロードします。
インストーラのファイル名は、VMware-viewagent-y.y.y-xxxxxx.exe または VMware-viewagent-x86_64-y.y.y-xxxxxx.exe です。y.y.yはバージョン番号、xxxxxxはビルド番号です。
- 仮想マシンまたは物理 PC に対する管理者権限があることを確認します。
- Horizon Agent のカスタム セットアップ オプションについて理解しておきます。 [Horizon Agent のカスタム セットアップ オプション](#) 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。
- Horizon Agent 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ておきます。 [Horizon Agent のサイレント インストール プロパティ](#)を参照してください。
- Horizon Agent インストール プログラムによってファイアウォール上で開かれる TCP ポートについて理解しておきます。詳細については、『View アーキテクチャの計画』ドキュメントを参照してください。
- Horizon Agent をサイレント インストールする予定のゲスト OS に、最新の Windows Update パッチがインストールされていることを確認します。場合によっては、Windows Update パッチの保留を実行するために、管理者によるインタラクティブなインストールを行う必要があります。すべての OS 操作とその後の再起動が完了していることを確認します。

手順

- 1 仮想マシンまたは物理 PC で Windows コマンド プロンプトを開きます。
- 2 インストール コマンドを 1 行で入力します。

次の例では、Core、VMware Blast、PCoIP、Unity Touch、VmVideo、PSG、View Composer Agent、仮想印刷、USB リダイレクト、および Real-Time Audio-Video のコンポーネントとともに、Horizon Agent をインストールします。

```
VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn VDM_VC_MANAGED_AGENT=1  
ADDLOCAL=Core,SVIAgent,ThinPrint,USB,RTAV"
```

次の例では、非管理対象コンピュータに Horizon Agent をインストールし、指定した View 接続サーバ (cs1.companydomain.com) にデスクトップを登録します。また、インストーラは、Core、VMware Blast、PCoIP、Unity Touch、VmVideo、PSG、仮想印刷、および USB リダイレクト コンポーネントをインストールします。

```
VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn VDM_VC_MANAGED_AGENT=0  
VDM_SERVER_NAME=cs1.companydomain.com VDM_SERVER_USERNAME=admin.companydomain.com  
VDM_SERVER_PASSWORD=secret ADDLOCAL=Core,ThinPrint,USB"
```

Windows Server マシンに Horizon Agent をインストールし、そのマシンを RDS ホストとしてではなくシングルユーザー View デスクトップとして構成する場合は、インストール コマンドに VDM_FORCE_DESKTOP_AGENT=1 プロパティを含める必要があります。この要件は、vCenter Server によって管理されるマシンと管理対象外のマシンに適用されます。

次のステップ

仮想マシンが複数の NIC を使用する場合は、Horizon Agent が使用するサブネットを構成します。 [Horizon Agent のための複数の NIC を使用する仮想マシンの構成](#)を参照してください。

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

View 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。View 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、View コンポーネント コンピュータでコマンド プロンプトを開いて、`msiexec /?` と入力します。

View 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 3-4. View 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-viewagent-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 View 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、View 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、View 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 3-5. 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-viewagent-y.y.y-xxxxxx.exe /s /v"/qn"</pre> <p>その代わりに、/qb オプションを使用して、非対話的にウィザード ページを表示する自動インストールができます。インストールが進むとウィザード ページが表示されますが、それらに応答はできません。</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>
INSTALLDIR	<p>View 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>INSTALLDIR=<i>path</i> の形式で、インストール パスを指定します。View 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、View 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、View 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が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 SVI Agent は相互に排他的です。NGVC をインストールするには、明示的に指定する必要があります。</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: <code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn ADDLOCAL=ALL"</code></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: <code>VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn"</code></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。名前の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-viewagent-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>

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。
/!%v log_file	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: /!%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。 /!%v オプションはオプションです。

Horizon Agent のサイレント インストール プロパティ

コマンド ラインから Horizon Agent をサイレントでインストールする場合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 3-6. Horizon Agent をサイレント インストールするための MSI プロパティ は、コマンド ラインで使用できる Horizon Agent サイレント インストール プロパティを示しています。

表 3-6. Horizon Agent をサイレント インストールするための MSI プロパティ

MSI プロパティ	説明	デフォルト値
INSTALLDIR	Horizon Agent ソフトウェアがインストールされるパスおよびフォルダ。 例: INSTALLDIR=""D:\abc\my folder"" パスを 2 つの二重引用符のセットで囲むと、MSI インストーラはパス内の領域を無視します。 この MSI プロパティはオプションです。	%ProgramFiles%\VMware\VMware View Agent
RDP_CHOICE	デスクトップでリモート デスクトップ プロトコル (RDP) を有効にするかどうかを決定します。 値 1 を指定すると、RDP が有効になります。値 0 を指定すると、RDP 設定は無効のままです。 この MSI プロパティはオプションです。	1
UNITY_DEFAULT_APPS	モバイル デバイスの Unity Touch サイドバーに表示されるデフォルトのお気に入りのアプリケーションのリストを指定します。このプロパティは、Unity Touch コンポーネントをサポートするために作成されました。これは一般的な MSI プロパティではありません。 お気に入りのアプリケーションのデフォルト リストの構成およびこのプロパティで使用するための構文とフォーマットについての詳細は、 Unity Touch で表示されるお気に入りアプリケーションの構成 を参照してください。 この MSI プロパティはオプションです。	
URL_FILTERING_ENABLED	URL コンテンツ リダイレクト機能をインストールするかどうかを指定します。値に 1 を指定すると、この機能がインストールされます。次に、グループ ポリシー設定を使用して、リダイレクトする URL を構成する必要があります。 URL コンテンツ リダイレクトの構成 を参照してください。 この MSI プロパティはオプションです。	0

MSI プロパティ	説明	デフォルト値
VDM_VC_MANAGED_AGENT	Horizon Agent がインストールされる仮想マシンを vCenter Server が管理するかどうかを決定します。 値 1 を指定すると、デスクトップは vCenter Server の管理対象仮想マシンとして構成されます。 値 0 を指定すると、デスクトップは vCenter Server の非管理対象として構成されます。 この MSI プロパティは必須です。	なし
VDM_SERVER_NAME	Horizon Agent インストーラが非管理対象デスクトップを登録する View 接続サーバ コンピュータのホスト名または IP アドレス。このプロパティは、非管理対象デスクトップにのみ適用されます。 例: VDM_SERVER_NAME=10.123.01.01 非管理対象デスクトップでは、この MSI プロパティは必須です。 vCenter Server の管理対象の仮想マシン デスクトップには、この MSI プロパティを使用しないでください。	なし
VDM_SERVER_USERNAME	View 接続サーバ コンピュータの管理者のユーザー名。この MSI プロパティは、非管理対象デスクトップにのみ適用されます。 例: VDM_SERVER_USERNAME=domain\username 非管理対象デスクトップでは、この MSI プロパティは必須です。 vCenter Server の管理対象の仮想マシン デスクトップには、この MSI プロパティを使用しないでください。	なし
VDM_SERVER_PASSWORD	View 接続サーバ管理者ユーザー パスワード。 例: VDM_SERVER_PASSWORD=secret 非管理対象デスクトップでは、この MSI プロパティは必須です。 vCenter Server の管理対象の仮想マシン デスクトップには、この MSI プロパティを使用しないでください。	なし
VDM_IP_PROTOCOL_USAGE	Horizon Agent が使用する IP 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
VDM_FLASH_URL_REDIRECTION	Horizon Agent で Flash URL リダイレクト機能をインストールできるかどうかを特定します。1 を指定するとインストールが有効になり、0 を指定するとインストールが無効になります。 この MSI プロパティはオプションです。	0

サイレント インストール コマンドでは、MSI プロパティ ADDLOCAL= を使用して、Horizon Agent インストーラが構成するオプションを指定できます。

[表 3-7. Horizon Agent のサイレント インストール オプションとインタラクティブ カスタム セットアップ オプション](#)には、コマンド ラインに入力できる Horizon Agent オプションが示されます。これらのオプションには対応するセットアップ オプションがあり、それらのオプションはインタラクティブ インストールで選択解除または選択できます。カスタム セットアップ オプションの詳細については、[Horizon Agent のカスタム セットアップ オプション](#)を参照してください。

コマンド ラインで ADDLOCAL プロパティを使用しない場合、Horizon Agent はインタラクティブなインストール時にデフォルトでインストールされるすべてのオプションをインストールします（ゲスト OS でサポートされている場合）。ADDLOCAL=ALL を使用すると、Horizon Agent は次のオプションを、デフォルトでオンのものもオフのもものもすべてインストールします（NGVC を除き、ゲスト OS でサポートされている場合）。NGVC と SVIAgent は相互に排他的です。NGVC をインストールするには、明示的に指定する必要があります。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](#)にある ADDLOCAL の表のエントリを参照してください。

表 3-7. Horizon Agent のサイレント インストール オプションとインタラクティブ カスタム セットアップ オプション

サイレント インストール オプション	対話的なインストールのカスタム セットアップ オプション	インタラクティブなインストール時にデフォルトでインストールされる、または ADDLOCAL が使用されていない場合にインストールされる
Core	Core	はい
USB	USB リダイレクト	いいえ
SVIAgent	View Composer Agent	はい
NGVC	Instant Clone Agent	いいえ
RTAV	リアルタイム オーディオビデオ	はい
ClientDriveRedirection	クライアント ドライブ リダイレクト	はい
SerialPortRedirection	シリアル ポート リダイレクト	いいえ
ScannerRedirection	スキャナ リダイレクト	いいえ
FlashURLRedirection	Flash URL リダイレクト この機能は、コマンド ラインで VDM_FLASH_URL_REDIRECTION=1 プロパティを使用しない限り非表示になっています。	いいえ
ThinPrint	仮想印刷	はい
V4V	vRealize Operations Desktop Agent	はい
VPA	View Persona Management	はい
SmartCard	PCoIP スマートカード。インタラクティブなインストールで、この機能がデフォルトでインストールされることはありません。	いいえ
VmwVaudio	VMware オーディオ（仮想オーディオ ドライバ）	はい
TSMMR	Windows Media マルチメディア リダイレクト (MMR)	はい
RDP	この機能は、コマンド ラインの RDP_CHOICE=1 プロパティを使用するか、View Administrator でデスクトップ プールを作成または編集する際にデフォルトの表示プロトコルとして RDP を選択する場合に、レジストリの RDP を有効にします。 この機能はインタラクティブなインストールでは非表示になっています。	はい

ADDLOCAL を使用して機能を個々に指定、つまり ADDLOCAL=ALL を指定しない場合は、Core を常に指定しなければなりません。

表 3-8. 自動的にインストールされる Horizon Agent サイレント インストール機能

サイレント インストール機能	説明
Core	Horizon Agent の主要機能。 ADDLOCAL=ALL を指定すると、Core 機能がインストールされます。
BlastProtocol	VMware Blast
PCoIP	PCoIP プロトコル エージェント
VmVideo	仮想ビデオ ドライバ
UnityTouch	Unity Touch
PSG	この機能は、Horizon Agent が IPv4 または IPv6 を使用しているかどうかを、接続サーバに伝えるレジストリ エントリを設定します。

サイレント インストールで VDM_FLASH_URL_REDIRECTION=1 プロパティを使用することによって、Flash URL リダイレクト機能をインストールします。この機能は、インタラクティブなインストールでも、サイレント インストールで ADDLOCAL=ALL を使用した場合でもインストールされません。

例: VMware-viewagent-y.y.y-xxxxxx.exe /s /v"/qn VDM_VC_MANAGED_AGENT=1
VDM_FLASH_URL_REDIRECTION=1
ADDLOCAL=Core,SVIAgent,ThinPrint,USB,FlashURLRedirection,RTAV"

Horizon Agent のための複数の NIC を使用する仮想マシンの構成

複数の NIC を使用する仮想マシンに Horizon Agent をインストールするときは、Horizon Agent が使用するサブネットを設定する必要があります。サブネットによって、クライアント プロトコル接続のために Horizon Agent が接続サーバ インスタンスに提供するネットワーク アドレスが決まります。

手順

- ◆ Horizon Agent がインストールされている仮想マシンで、コマンド プロンプトを開き、**regedit.exe** と入力します。次に、サブネットを構成するためのレジストリ エントリを作成します。

たとえば、IPv4 ネットワークの場合は

HKLM\Software\VMware, Inc.\VMware VDM\IpPrefix = *n.n.n.n/m* (REG_SZ) のようにします。

この例で、*n.n.n.n* は TCP/IP サブネットで、*m* はサブネット マスクのビット数です。

注: Horizon 6 バージョン 6.1 よりも前のリリースでは、このレジストリ パスが

HKLM\Software\VMware, Inc.\VMware VDM\Node Manager\subnet = *n.n.n.n/m* (REG_SZ) で

した。この古いレジストリ設定は、View Agent 6.1 以降で使用されません。以前のリリースからバージョン 6.1 以降に View Agent をアップグレードする場合は、現在のレジストリ設定を使用してください。

ゲスト OS のパフォーマンスの最適化

リモート デスクトップの展開のためにゲスト OS のパフォーマンスを最適化する特定の手順を実行できます。これらの手順はすべてオプションです。

推奨事項としては、スクリーン セーバーをオフにすること、およびスリープ タイマーを指定しないことが挙げられます。組織によっては、スクリーン セーバーの使用を必須にしていることがあります。たとえば、スクリーン セーバーが起動してから一定時間後にデスクトップをロックする GPO 管理のセキュリティ ポリシーを使用している場合が考えられます。この場合は、ブランクのスクリーン セーバーを使用してください。

前提条件

- リモート デスクトップの展開のためにゲスト OS を準備します。
- Windows カスタマー エクスペリエンス向上プログラムを無効にする手順を理解しておきます。[Windows カスタマー エクスペリエンス向上プログラムを無効にする](#)を参照してください。

手順

- ◆ COM1、COM2、LPT などの未使用のポートを無効にします。
- ◆ 表示のプロパティを調整します。
 - a ベーシック テーマを選択します。
 - b 背景を単色に設定します。
 - c スクリーン セーバーを [なし] にします。
 - d ハードウェアのアクセラレーションを有効にしていることを確認します。
- ◆ 高パフォーマンスの電源オプションを選択し、スリープ タイマーを指定しません。
- ◆ インデックス サービス コンポーネントを無効にします。

注: インデックスを付けると、ファイルがカタログ化されて検索の速度が向上します。頻繁に検索を行うユーザーに対しては、この機能を無効にしないでください。

- ◆ システムの復元ポイントを削除するか、または最小限に抑えます。
- ◆ C:¥ のシステム保護をオフにします。
- ◆ 不要なすべてのサービスを無効にします。
- ◆ サウンド設定を [サウンドなし] に設定します。
- ◆ 視覚効果を [パフォーマンスを優先する] に設定します。
- ◆ Windows Media Player を開き、デフォルトの設定を使用します。
- ◆ 自動コンピュータ保守をオフにします。
- ◆ パフォーマンス設定を最高のパフォーマンスに調整します。
- ◆ C:¥ 内の \$NtUninstallKB893756\$ などの非表示のアンインストール フォルダを削除します。
- ◆ すべてのイベント ログを削除します。
- ◆ ディスク クリーンアップを実行して一時ファイルを削除し、ごみ箱を空にして、必要でなくなったシステム ファイルおよびその他の項目を削除します。
- ◆ ディスク デフラグを実行し、断片化されたデータを再配置します。

- ◆ Tablet PC コンポーネントの機能が必要でなければアンインストールします。
- ◆ IPv6 が必要でなければ無効にします。
- ◆ ファイル システム ユーティリティ (fsutil) コマンドを使用して、ファイルの最終アクセス時間を追跡する設定を無効にします。

例: `fsutil behavior set disablelastaccess 1`

- ◆ レジストリ エディタ (regedit.exe) を起動し、[HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥services¥Disk] の TimeoutValue REG_DWORD を **0x000000be(190)** に変更します。
- ◆ Windows カスタマー エクスペリエンス向上プログラムをオフにし、タスク スケジューラから関連するタスクを無効にします。
- ◆ 上記の変更を行った後で、Windows を再起動します。

次のステップ

インスタント クローンおよび View Composer リンク クローンの増大を抑えるために Windows の特定のサービスやタスクを無効にする方法の詳細については、[インスタントクローンおよび View Composer リンククローン仮想マシン用の Windows のカスタマイズ](#)を参照してください。さらに、特定のサービスおよびタスクを無効にすることによって、フル仮想マシンのパフォーマンス上の利点も得られる可能性があります。

Windows カスタマー エクスペリエンス向上プログラムを無効にする

Windows カスタマー エクスペリエンス向上プログラム、およびこのプログラムを制御する関連したタスク スケジューラのタスクを無効にすると、大規模なデスクトップ プール内の Windows 7、Windows 8/8.1、および Windows 10 のシステム パフォーマンスが向上する場合があります。

次の手順は、Windows 7 および Windows 8 に適用されます。別の Windows オペレーティング システムでは手順が異なる可能性があります。

手順

- 1 Windows 7 または Windows 8 ゲスト OS で、コントロール パネルを起動して [アクション センター] - [アクション センターの設定を変更] をクリックします。
- 2 [カスタマー エクスペリエンス向上プログラムの設定] をクリックします。
- 3 [いいえ、このプログラムに協力しません] を選択して [変更の保存] をクリックします。
- 4 コントロール パネルを起動して [管理ツール] - [タスク スケジューラ] をクリックします。
- 5 [タスク スケジューラ] ダイアログ ボックスの [タスク スケジューラ (ローカル)] ベインで [タスク スケジューラ ライブラリ] - [Microsoft] - [Windows] ノードを展開し、[Application Experience] フォルダを開きます。
- 6 [AITAgent], [ProgramDataUpdater] を無効にし、使用できる場合は [Microsoft Compatibility Appraiser] タスクを無効にします。
- 7 [タスク スケジューラ ライブラリ] - [Microsoft] - [Windows] ノードで、[Customer Experience Improvement Program] フォルダを開きます。
- 8 [Consolidator], [KernelCEIPTask]、および [UsbCEIP] タスクを無効にします。

9 [タスク スケジューラ ライブラリ] - [Microsoft] - [Windows] ノードで[Autochk]フォルダを開きます。

10 [Proxy] タスクを無効にします。

次のステップ

他の Windows 最適化タスクを実行します。 [ゲスト OS のパフォーマンスの最適化](#)を参照してください。

インスタントクローンおよび View Composer リンククローン仮想マシン用の Windows のカスタマイズ

Windows 7、Windows 8/8.1、および Windows 10 の一部のサービスとタスクを無効にすることによって、インスタント クローンと View Composer リンク クローンのディスク使用率の拡大を低減できます。さらに、特定のサービスおよびタスクを無効にすることによって、フル仮想マシンのパフォーマンス上の利点も得られる可能性があります。

Windows のサービスおよびタスクを無効にした場合の利点

Windows 7、Windows 8/8.1、および Windows 10 は、マシンがアイドル状態の場合でも、インスタント クローンおよび View Composer のリンク クローンの拡大を招く可能性のあるサービスおよびタスクをスケジュール設定します。OS ディスクが徐々に拡大することで、最初にクローンを作成したときに達成したストレージの節約が台なしになることがあります。これらの Windows サービスを無効にすることによって、ディスク サイズの拡大を低減できます。

Windows ゲスト OS により、デフォルトでディスクの最適化などのサービスの実行がスケジュール設定されます。これらのサービスは、無効にしない限り、バックグラウンドで実行されます。

OS ディスク サイズの拡大に影響するサービスは、入力/出力処理も発生させます。これらのサービスを無効にすることで、IOPS（1 秒当たりの入力/出力処理）を低減し、あらゆるタイプのデスクトップ マシンのパフォーマンスも向上できます。

Windows を最適化するためのこれらのベスト プラクティスは、ほとんどのユーザー環境に適用されます。ただし、各サービスを無効にした場合の効果は、実際のユーザー、アプリケーション、およびデスクトップについて評価する必要があります。特定のサービスをアクティブなままにしておくことが必要な場合もあります。

たとえば、Windows 更新サービスを無効にすることは、インスタント クローンの場合はユーザーがログアウトするときに毎回 OS が更新されるために有意義です。また、View Composer リンク クローンについても、定期的に更新または再構成する場合には有意義です。

インスタント クローンおよびリンク クローンのディスクの拡大を招く Windows のサービスおよびタスク

Windows 7、Windows 8/8.1、および Windows 10 の特定のサービスおよびタスクは、マシンがアイドル状態の場合でも、徐々にインスタント クローンまたは View Composer リンク クローンの OS ディスクの拡大を招く可能性があります。これらのサービスおよびタスクを無効にすると、OS ディスクの拡大を抑制できます。

また、OS ディスクの拡大に影響を与えるサービスによって、I/O 操作も生成されます。完全クローンで、これらのサービスを無効にした場合の利点を評価することもできます。

表 3-9. Windows のサービスおよびタスクが OS ディスクの拡大と IOPS に与える影響に示す Windows のサービスを無効にする前に、[ゲスト OS のパフォーマンスの最適化](#)の最適化の手順を実行したことを確認してください。

表 3-9. Windows のサービスおよびタスクが OS ディスクの拡大と IOPS に与える影響

サービスまたはタスク	説明	デフォルトの頻度または起動	OS ディスクへの影響	IOPS への影響	このサービスまたはタスクの無効化
Windows のハイバネーション	コンピュータがパワーオフされる前に、開かれているドキュメントやプログラムをファイルに格納することによって省電力状態を提供します。このファイルは、コンピュータが再起動されたときにメモリに再びロードされ、ハイバネーションが起動された時点の状態を復元します。	デフォルトの電源プラン設定では、ハイバネーションは無効になっています。	高。 デフォルトでは、ハイバネーション ファイル hiberfil.sys のサイズは、仮想マシンに搭載されている RAM と同じです。この機能は、すべてのゲスト OS に影響を与えます。	高。 ハイバネーションが起動されると、システムは、搭載されている RAM のサイズで hiberfil.sys ファイルを書き込みます。	はい 仮想環境では、ハイバネーションに利点はありません。 手順については、 親仮想マシンでの Windows のハイバネーションの無効化 を参照してください。
Windows でスケジュール設定されたディスクの最適化	ディスクの最適化は、バックグラウンド処理としてスケジュール設定されます。	1 週間に 1 回	高。 ディスクの最適化操作が繰り返されると、OS ディスクのサイズが数 GB 増える場合があります、ディスク アクセスの効率化にはほとんど役立ちません。	高	はい
Windows Update サービス	Windows やその他のプログラムの更新を検出、ダウンロード、およびインストールします。	自動スタートアップ	中～高。 更新チェックが頻繁に実行されるため、OS ディスクへの書き込みが頻繁に発生します。影響は、ダウンロードされる更新によって異なります。	中～高	インスタント クローンの場合、および更新や再構成を定期的に行う View Composer リンク クローンの場合は行う。
Windows 診断ポリシー サービス	Windows コンポーネントの問題を検出、トラブルシューティング、および解決します。このサービスを停止すると、診断が機能しなくなります。	自動スタートアップ	中～高。 このサービスは、必要に応じて起動されます。書き込みの頻度は、要求によって異なります。	低～中	デスクトップ上で診断ツールが機能する必要がある場合は行う。

サービスまたはタスク	説明	デフォルトの頻度または起動	OS ディスクへの影響	IOPS への影響	このサービスまたはタスクの無効化
プリフェッチ/スーパーフェッチ	実行するアプリケーションがより迅速に起動されるように、アプリケーションに関する特定の情報を格納します。	無効にしない限り、常に有効。	中 レイアウトおよびデータベース情報や、必要に応じて生成される個別のプリフェッチ ファイルに対する定期的な更新が発生します。	中	この機能を無効にした後のアプリケーションの起動時間が許容できる場合は行う。
Windows レジストリのバックアップ (RegIdleBackup)	システムがアイドル状態のときに、Windows レジストリを自動的にバックアップします。	10 日ごと、午前 12:00	中。 このタスクが実行されるごとに、レジストリのバックアップ ファイルが生成されます。	中。	はい。インスタント クローンと View Composer リンク クローンのどちらを使用しても、スナップショットに戻して、レジストリの復元という目標を達成できます。
システムの復元	Windows システムを以前の正常な状態に戻します。	Windows の起動時と、それ以降 1 日に 1 回。	低～中。 システムが必要と判断した場合に、システムの復元ポイントをキャプチャします。	大きな影響はありません。	はい。インスタント クローンと View Composer リンク クローンのどちらを使用しても、正常な状態に戻すことができます。
Windows Defender	スパイウェア対策機能を提供します。	Windows の起動時。1 日に 1 回、クイック スキャンを実行します。各スキャンの前に、更新をチェックします。	中～高。 定義の更新、スケジュール設定されたスキャン、および必要に応じて起動されるスキャンを実行します。	中～高。	他のスパイウェア対策ソフトウェアがインストールされている場合は行う。
Microsoft Feeds Synchronization タスク (msfeedssync.exe)	Windows Internet Explorer Web ブラウザ内の RSS フィードを定期的に更新します。このタスクは、RSS フィードの自動同期が有効になっている RSS フィードを更新します。このプロセスが Windows タスク マネージャに表示されるのは、Internet Explorer が実行されている場合だけです。	1 日に 1 回。	中。 通常ディスクが構成されていない場合は、OS ディスクの拡大に影響を与えます。通常ディスクが構成されている場合は、影響が通常ディスクに移ります。	中	ユーザーがデスクトップ上での RSS フィードの自動更新を必要としない場合は行う。

Windows 親仮想マシンでのスケジュール設定されたディスクの最適化の無効化

インスタント クローン用または View Composer リンク クローン用の親仮想マシンを準備するとき、スケジュール設定されたディスクの最適化を無効にすることを推奨します。デフォルトでは、Windows はディスクの最適化を毎

週スケジュール設定します。ディスクの最適化が実行されると、クローンの仮想ディスクのサイズが大幅に増え、インスタント クローンまたは View Composer リンク クローンのディスク アクセスが効率化されません。

クローンは親仮想マシンの OS ディスクを共有しますが、各クローンでは、ファイル システムに対する変更を個別の仮想ディスクで維持します。ディスクの最適化などのあらゆるアクティビティによって、各クローンの個別仮想ディスクのサイズが増えるため、ストレージ使用量が増加します。ベスト プラクティスとして、スナップショットを作成してプールを作成する前に、親仮想マシンのディスクの最適化を行うことをお勧めします。

次の手順は、Windows 7 および Windows 8 に適用されます。別の Windows オペレーティング システムでは手順が異なる可能性があります。

手順

- 1 vSphere Client で、親仮想マシンを選択し、[コンソールを開く] を選択します。
- 2 管理者としてログインします。
- 3 [スタート] をクリックし、**プログラムとファイルの検索** ボックスに「[デフラグ]」と入力します。
- 4 [プログラム] ペインで、ディスク デフラグ ツールをクリックします。
- 5 [ディスク デフラグ ツール] ダイアログ ボックスで、[ディスクの最適化] をクリックします。
ディスク デフラグ ツールによって、最適化されたファイルが仮想マシンのハード ディスク上に統合されます。
- 6 [ディスク デフラグ ツール] ダイアログ ボックスで、[スケジュールの構成] をクリックします。
- 7 [スケジュールに従って実行する (推奨)] の選択を解除し、[OK] をクリックします。

Windows Update を無効にする

Windows Update 機能を無効にすることで、ファイル システムに対する一部の I/O 処理を回避し、インスタント クローンまたは View Composer リンク クローンの仮想ディスクの拡大を低減できます。

Windows Update を無効にする前の環境の必要性の評価この機能を無効にする場合は、手動で親仮想マシンの更新プログラムをダウンロードし、インスタント クローンのプッシュイメージ操作または View Composer リンク クローンの再構成を使用して、すべてのクローンに更新を適用できます。

次の手順は、Windows 7 および Windows 8 に適用されます。別の Windows オペレーティング システムでは手順が異なる可能性があります。

手順

- 1 vSphere Client で、親仮想マシンを選択し、[コンソールを開く] を選択します。
- 2 管理者としてログインします。
- 3 [スタート] - [コントロール パネル] - [システムとセキュリティ] - [自動更新の有効化または無効化] をクリックします。
- 4 [重要な更新プログラム] メニューで、[更新プログラムを確認しない] を選択します。
- 5 [推奨される更新プログラムについても重要な更新プログラムと同様に通知する] の選択を解除します。
- 6 [すべてのユーザーにこのコンピューターへの更新プログラムのインストールを許可する] の選択を解除し、[OK] をクリックします。

Windows 仮想マシンでの診断ポリシー サービスの無効化

Windows 診断ポリシー サービスを無効にすることで、ファイル システムに対する一部の I/O 処理を回避し、インスタント クローンまたは View Composer リンク クローンの仮想ディスクの拡大を低減できます。

ユーザーがデスクトップに診断ツールを必要としている場合は、Windows 診断ポリシー サービスを無効にしないでください。

次の手順は、Windows 7 および Windows 8 に適用されます。別の Windows オペレーティング システムでは手順が異なる可能性があります。

手順

- 1 vSphere Client で、親仮想マシンを選択し、[コンソールを開く] を選択します。
- 2 管理者としてログインします。
- 3 [スタート] - [コントロール パネル] - [システムとセキュリティ] - [管理ツール] をクリックします。
- 4 [サービス] を選択し、[開く] をクリックします。
- 5 [Diagnostic Policy Service] をダブルクリックします。
- 6 (ローカル コンピュータ) Diagnostic Policy Service のプロパティ ダイアログで、[停止] をクリックします。
- 7 [起動タイプ] メニュー メニューで、[無効化] を選択します。
- 8 [OK] をクリックします。

Windows 仮想マシンでのプリフェッチとスーパーフェッチの機能の無効化

プリフェッチとスーパーフェッチの機能を無効にすることで、ファイル システムに対する一部の I/O 処理を回避し、インスタント クローンまたは View Composer でリンクされたクローンの仮想ディスクの拡大を低減できます。

プリフェッチとスーパーフェッチの機能を無効にするには、仮想マシンで Windows レジストリ キーを編集し、プリフェッチ サービスを無効にする必要があります。

次の手順は、Windows 7 および Windows 8 に適用されます。別の Windows オペレーティング システムでは手順が異なる可能性があります。

前提条件

Windows レジストリ エディタ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 ローカル Windows 仮想マシンで Windows レジストリ エディタを起動します。
- 2 [PrefetchParameters] という名前のレジストリ キーに移動します。
このレジストリ キーのパスは、HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters です。
- 3 [EnablePrefetcher] と [EnableSuperfetch] の値を 0 に設定します。
- 4 [スタート] - [コントロール パネル] - [システムとセキュリティ] - [管理ツール] をクリックします。

- 5 [サービス] を選択し、[開く] をクリックします。
- 6 [Superfetch] サービスをダブルクリックします。
- 7 (ローカル コンピュータ) Superfetch のプロパティ ダイアログで、[停止] をクリックします。
- 8 [起動タイプ] メニュー メニューで、[無効化] を選択します。
- 9 [OK] をクリックします。

Windows 仮想マシンでの Windows レジストリのバックアップの無効化

Windows レジストリのバックアップ機能 (RegIdleBackup) を無効にすると、ファイル システムに対する一部の I/O 操作が回避されるため、インスタント クローンの仮想ディスクまたは View Composer リンク クローンの仮想ディスクの拡大を抑えることができます。

次の手順は、Windows 7 および Windows 8 に適用されます。別の Windows オペレーティング システムでは手順が異なる可能性があります。

手順

- 1 vSphere Client で、親仮想マシンを選択し、[コンソールを開く] を選択します。
- 2 管理者としてログインします。
- 3 [スタート] - [コントロール パネル] - [システムとセキュリティ] - [管理ツール] をクリックします。
- 4 [タスク スケジューラ] を選択し、[開く] をクリックします。
- 5 左ペインで、[タスク スケジューラ ライブラリ]、[Microsoft]、[Windows] を展開します。
- 6 [Registry] をダブルクリックして、[RegIdleBackup] を選択します。
- 7 [アクション] ペインで、[無効化] をクリックします。

Windows 仮想マシンでのシステムの復元の無効化

Windows のシステムの復元機能を無効にすることで、ファイル システムに対する一部の I/O 処理を回避し、インスタント クローンまたは View Composer リンク クローンの仮想ディスクの拡大を低減できます。

システムの復元により、マシンの状態を以前の特定時点における状態に戻すことができます。インスタント クローンのプッシュ イメージ操作、および View Composer リンク クローンの再構成または更新操作を実行する場合と同じ結果を達成できます。さらに、インスタント クローンにより、ユーザーがログアウトするとマシンが再作成され、システムの復元が不要になります。

次の手順は、Windows 7 および Windows 8 に適用されます。別の Windows オペレーティング システムでは手順が異なる可能性があります。

手順

- 1 vSphere Client で、親仮想マシンを選択し、[コンソールを開く] を選択します。
- 2 管理者としてログインします。
- 3 [スタート] - [コントロール パネル] - [システムとセキュリティ] - [管理ツール] をクリックします。

- 4 [タスク スケジューラ] を選択し、[開く] をクリックします。
- 5 左ペインで、[タスク スケジューラ ライブラリ]、[Microsoft]、[Windows] を展開します。
- 6 [SystemRestore] をダブルクリックし、[SR] を選択します。
- 7 [アクション] ペインで、[無効化] をクリックします。

Windows 仮想マシンでの Windows Defender の無効化

Windows Defender を無効にすると、ファイル システムに対する一部の I/O 操作が回避されるため、インスタント クローンの仮想ディスクまたは View Composer リンク クローンの仮想ディスクの拡大を抑えることができます。

Windows Defender が仮想マシンにインストールされている唯一のスパイウェア対策ソフトウェアである場合は、環境内のデスクトップで Windows Defender をアクティブなままにすることもできます。

次の手順は、Windows 7 および Windows 8 に適用されます。別の Windows オペレーティング システムでは手順が異なる可能性があります。

手順

- 1 vSphere Client で、親仮想マシンを選択し、[コンソールを開く] を選択します。
- 2 管理者としてログインします。
- 3 [スタート] をクリックし、プログラムとファイルの検索ボックスに「**Windows Defender**」と入力します。
- 4 [ツール] - [オプション] - [管理者] をクリックします。
- 5 [このプログラムを使用する] の選択を解除し、[保存] をクリックします。

Windows 仮想マシンでの Microsoft Feeds Synchronization の無効化

Windows Internet Explorer は、Microsoft Feeds Synchronization タスクを使用して、ユーザーの Web ブラウザ内の RSS フィードを更新します。このタスクを無効にすると、ファイル システムに対する一部の I/O 操作が回避されるため、インスタント クローンの仮想ディスクまたは View Composer リンク クローンの仮想ディスクの拡大を抑えることができます。

手順

- 1 vSphere Client で、親仮想マシンを選択し、[コンソールを開く] を選択します。
- 2 管理者としてログインします。
- 3 [スタート] - [コントロール パネル] - [ネットワークとインターネット] - [インターネット オプション] をクリックします。
- 4 [コンテンツ] タブをクリックします。
- 5 [フィードと Web スライス] で、設定をクリックします。
- 6 [フィードおよび Web スライスの更新の確認を自動的に行う] の選択を解除し、[OK] をクリックします。
- 7 [インターネットのプロパティ] ダイアログで、OK をクリックします。

親仮想マシンの準備

インスタントクローンまたは View Composer リンク クローン デスクトップ プールをデプロイするには、まず親仮想マシンを準備する必要があります。

- **親仮想マシンの構成**

親として使用する予定の仮想マシンを作成した後に、Windows 環境を構成します。

- **インスタント クローンおよび View Composer リンク クローンでの Windows のアクティベーション**

Windows 7、Windows 8/8.1、Windows 10、および Windows Server クローンの適切なアクティベーションが、クローンの作成時に行われるようにするには、親仮想マシンで Microsoft ポリウム アクティベーションを使用する必要があります。ポリウム アクティベーション テクノロジーにはポリウム ライセンス キーが必要です。

- **親仮想マシンでの Windows のハイバネーションの無効化**

Windows のハイバネーション機能によって、非表示のシステム ファイル Hiberfil.sys が作成されます。このファイルは、ハイブリッド スリープに必要な情報を格納するために使用されます。ハイバネーションを無効にすると、インスタント クローンの仮想ディスクまたは View Composer リンク クローンの仮想ディスクのサイズが削減されます。

- **View Composer リンク クローン用のローカル ストレージの構成**

View Composer リンク クローン デスクトップ プールでは、仮想マシン スワップ ファイルをローカル データストアに格納するように親仮想マシンを構成できます。リンク クローンのスワップ ファイルは、ローカル ストレージに配置されます。この機能はインスタント クローンでは使用できません。

- **View Composer 親仮想マシンのページング ファイル サイズの記録**

View Composer リンク クローン デスクトップ プールを作成するとき、クローンのページング ファイルと一時ファイルを別のディスクにリダイレクトすることができます。このディスクは、親仮想マシン上のページング ファイルのサイズより大きくなるように構成する必要があります。

- **ClonePrep および QuickPrep カスタマイズ スクリプトのタイムアウト制限の引き上げ**

ClonePrep および QuickPrep 同期後スクリプトまたはパワーオフ スクリプトには、20 秒のタイムアウトがあります。親仮想マシンで Windows レジストリの値 ExecScriptTimeout を変更すると、この制限を引き上げることができます。

親仮想マシンの構成

親として使用する予定の仮想マシンを作成した後に、Windows 環境を構成します。

前提条件

- リモート デスクトップの展開のために使用する仮想マシンを準備したことを確認します。 [クローン作成のための仮想マシンの作成](#)を参照してください。

親仮想マシンは、デスクトップ マシンが参加するドメインと同じ Active Directory ドメインに属するか、またはワークグループのメンバーとなることが可能です。

- 仮想マシンがインスタント クローンまたは View Composer リンク クローンから変換されたものではないことを確認します。

重要: また、インスタント クローンまたは View Composer リンク クローンを親仮想マシンとして使用することはできません。

- 親仮想マシンに Horizon Agent をインストールするときは、インスタント クローンの [VMware Horizon Instant Clone Agent] オプション、または [VMware Horizon View Composer Agent] オプションを選択します。仮想マシンへの [Horizon Agent のインストール](#) を参照してください。

大規模な環境で Horizon Agent を更新するには、標準的な Windows 更新メカニズム (Altiris、SMS、LanDesk、BMC などのシステム管理ソフトウェア) を使用できます。プッシュ イメージまたは再構成操作を使用して、Horizon Agent を更新することもできます。

注: View Composer のリンク クローンについては、親の仮想マシンで VMware View Composer Guest Agent Server サービスのログイン アカウントを変更しないでください。デフォルトでは、これはローカル システム アカウントです。このアカウントを変更すると、この親から作成されたリンク クローンは起動しなくなります。

- Windows マシンをデプロイするには、ボリューム ライセンス キーを構成し、親仮想マシンのオペレーティング システムをボリューム アクティベーションによってアクティベーションします。 [インスタント クローンおよび View Composer リンク クローンでの Windows のアクティベーション](#) を参照してください。
- ベスト プラクティスに従ってオペレーティング システムを最適化していることを確認します。 [インスタント クローンおよび View Composer リンク クローン仮想マシン用の Windows のカスタマイズ](#) を参照してください。
- デバイス ドライバの Windows Update 検索を無効にするための手順を理解しておきます。 [http://technet.microsoft.com/en-us/library/cc730606\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc730606(v=ws.10).aspx) にある Microsoft Technet の記事「Disable Searching Windows Update for Device Drivers」を参照してください。

手順

- ◆ 親仮想マシンの DHCP リースを削除して、リースされた IP アドレスがプール内のリンク クローンにコピーされないようにします。
 - a 親仮想マシンで、コマンド プロンプトを開きます。
 - b **ipconfig /release** コマンドを入力します。
- ◆ システム ディスクにボリュームが 1 つだけ含まれていることを確認します。

複数のボリュームを含む親仮想マシンからリンク クローンを展開することはできません。複数の仮想ディスクはサポートされています。

注: View Composer のリンク クローンについては、親仮想マシンに複数の仮想ディスクが含まれている場合は、デスクトップ プールを作成するときに、親仮想マシンにすでに存在する、またはネットワーク マウントされたドライブに使用されているドライブ文字と競合する、View Composer 通常ディスクまたは廃棄可能データ ディスク用ドライブ文字は選択しないでください。

- ◆ 仮想マシンに独立ディスクが含まれていないことを確認します。

仮想マシンのスナップショットを作成するときに、独立ディスクは除外されます。クローンはスナップショットに基づくため、独立ディスクを含みません。

- ◆ View Composer リンク クローンについては、リンククローン マシンを作成するときに破棄可能データ ディスクを構成する場合に、デフォルト ユーザーの TEMP および TMP 変数を親仮想マシンから削除します。

pagefile.sys ファイルを削除して、すべてのリンク クローンでファイルを複製することを回避することもできます。親仮想マシンの pagefile.sys ファイルを残しておく、ファイルの読み取り専用バージョンがリンク クローンによって継承され、そのファイルの第 2 バージョンは破棄可能データ ディスクで使用されます。

- ◆ 各クローンの仮想ディスクのサイズを減らすには、ハイパネーション オプションを無効にします。
- ◆ 親仮想マシンのスナップショットをとる前に、デバイス ドライバの Windows Update 検索を無効にします。

この Windows 機能は、カスタマイズのプロセスに干渉する場合があります。各クローンがカスタマイズされると、Windows はインターネット上でそのクローンの最適なドライバを検索し、遅延する結果となります。

- ◆ vSphere Client で、親仮想マシンの [vApp オプション] 設定を無効にします。
- ◆ Windows 8.1、Windows Server 2008 R2、および Windows Server 2012 R2 マシンで、未使用の機能を削除することによってディスク領域を確保するスケジュール設定されたメンテナンス作業を無効にします。

例: Schtasks.exe /change /disable /tn "\\Microsoft\\Windows\\AppxDeploymentClient\\Pre-staged app cleanup"

たとえば、View Composer のリンク クローンの場合、このメンテナンス作業によりリンク クローンの作成後に Sysprep カスタマイズ スクリプトが削除され、後続の再構成操作がカスタマイズ操作のタイムアウト エラーで失敗する可能性があります。詳細については、Microsoft KB の記事 (<http://support.microsoft.com/kb/2928948>) を参照してください。

次のステップ

vSphere Client または vSphere Web Client を使用して、パワーオフ状態の親仮想マシンのスナップショットを作成します。このスナップショットは、クローンの基本イメージを提供します。

重要: スナップショットを作成する前に、親仮想マシンをシャットダウンします。

インスタント クローンおよび View Composer リンク クローンでの Windows のアクティベーション

Windows 7、Windows 8/8.1、Windows 10、および Windows Server クローンの適切なアクティベーションが、クローンの作成時に行われるようにするには、親仮想マシンで Microsoft ポリウム アクティベーションを使用する必要があります。ポリウム アクティベーション テクノロジーにはポリウム ライセンス キーが必要です。

ポリウム アクティベーションによって Windows をアクティベーションするには、キー マネージメント サービス (KMS) を使用します。これには KMS ライセンス キーが必要です。Microsoft 販売代理店に問い合わせ、ポリウム ライセンス キーを取得し、ポリウム アクティベーションを構成してください。

注: マルチプル アクティベーション キー (MAK) ライセンスはサポートされていません。

インスタントクローンまたは View Composer リンク クローン デスクトップ プールを作成する前に、ボリューム アクティベーションを使用して、親仮想マシンで Windows をアクティベーションする必要があります。

次の手順は、アクティベーションを行う方法を示しています。

- 1 既存のライセンスを削除するスクリプトを起動します。
- 2 Windows を再起動します。
- 3 KMS ライセンスを使用して Windows をアクティベーションするスクリプトを起動します。

KMS は、アクティベーション済みの各クローンを新しく発行されたライセンスを持つコンピュータとして扱います。

親仮想マシンでの Windows のハイバネーションの無効化

Windows のハイバネーション機能によって、非表示のシステム ファイル `Hiberfil.sys` が作成されます。このファイルは、ハイブリッド スリープに必要な情報を格納するために使用されます。ハイバネーションを無効にすると、インスタント クローンの仮想ディスクまたは View Composer リンク クローンの仮想ディスクのサイズが削減されます。

注意: ハイバネーションを使用不可にすると、ハイブリッド スリープは機能しません。停電が発生した場合は、データが失われる可能性があります。

手順

- 1 vSphere Client で、親仮想マシンを選択し、[コンソールを開く] を選択します。
- 2 管理者としてログインします。
- 3 ハイバネーション オプションを無効にします。
 - a [スタート] をクリックし、[検索の開始] ボックスに「**cmd**」と入力します。
 - b 検索結果のリストで、[コマンド プロンプト] を右クリックし、[管理者として実行] をクリックします。
 - c [ユーザー アカウント制御] プロンプトで、[続行] をクリックします。
 - d コマンド プロンプトで、「**powercfg.exe /hibernate off**」と入力し、Enter キーを押します。
 - e 「**exit**」と入力し、Enter キーを押します。

View Composer リンク クローン用のローカル ストレージの構成

View Composer リンク クローン デスクトップ プールでは、仮想マシン スワップ ファイルをローカル データストアに格納するように親仮想マシンを構成できます。リンク クローンのスワップ ファイルは、ローカル ストレージに配置されます。この機能はインスタント クローンでは使用できません。

この手順では、ゲスト OS のページング ファイルおよび一時ファイルではなく、仮想マシン スワップ ファイルのローカル ストレージを構成します。リンク クローン プールを作成するとき、ゲスト OS のページング ファイルと一時ファイルを別のディスクにリダイレクトすることもできます。[リンク クローン デスクトップ プールの作成用ワークシート](#)を参照してください。

手順

- 1 リンク クローン プールを展開する ESXi ホストまたはクラスタでスワップファイル データストアを構成します。
- 2 vCenter Server で親仮想マシンを作成するときは、仮想マシン スワップ ファイルをローカル ESXi ホストまたはクラスタ上のスワップファイル データストアに格納します。
 - a vSphere Client で、親仮想マシンを選択します。
 - b [編集設定] をクリックし、[オプション] タブをクリックします。
 - c [スワップファイル場所] をクリックし、[ホストのスワップファイル データストアに格納] をクリックします。

詳細な手順については、VMware vSphere のドキュメントを参照してください。

View Composer 親仮想マシンのページング ファイル サイズの記録

View Composer リンク クローン デスクトップ プールを作成するとき、クローンのページング ファイルと一時ファイルを別のディスクにリダイレクトすることができます。このディスクは、親仮想マシン上のページング ファイルのサイズより大きくなるように構成する必要があります。

破棄可能ファイルとは別のディスクで構成されているリンク クローンがパワーオフされると、ディスクが再作成されます。この機能により、リンク クローンのサイズの拡大を抑えることができます。ただし、この機能は、破棄可能ファイル ディスクをクローンのページング ファイルを保持するのに十分な大きさに構成した場合にのみ機能します。

破棄可能ファイル ディスクを構成する前に、親仮想マシンの最大ページング ファイル サイズを記録します。リンク クローンのページング ファイル サイズは親仮想マシンと同じです。

ベスト プラクティスとして、スナップショットをとる前に `pagefile.sys` ファイルを親仮想マシンから削除して、すべてのリンク クローンのファイルの重複を回避します。[親仮想マシンの構成](#)を参照してください。

注: この機能は、仮想マシン スワップ ファイルのローカル ストレージの構成とは同じではありません。[View Composer リンク クローン用のローカル ストレージの構成](#)を参照してください。

手順

- 1 vSphere Client で、親仮想マシンを右クリックし、[コンソールを開く] をクリックします。
- 2 [スタート] - [設定] - [コントロール パネル] - [システム] を選択します。
- 3 [詳細設定] タブをクリックします。
- 4 Performance (パフォーマンス) ペインで、[設定] をクリックします。
- 5 [詳細設定] タブをクリックします。
- 6 Virtual memory (仮想メモリ) ペインで、[変更] をクリックします。
Virtual Memory (仮想メモリ) ページが表示されます。
- 7 ページング ファイル サイズを、仮想マシンに割り当てられたメモリのサイズより大きい値に設定します。

重要: [最大サイズ (MB)] の設定が仮想マシンのメモリ サイズより小さい場合は、大きい値を入力し、新しい値を保存します。

- 8 選択したドライブのページング ファイル サイズ ペインで構成されている [最大サイズ (MB)] の設定を記録します。

次のステップ

この親仮想マシンからリンク クローン プールを構成するときに、ページング ファイル サイズよりも大きい破棄可能 ファイル ディスクを構成します。

ClonePrep および QuickPrep カスタマイズ スクリプトのタイムアウト制限の引き上げ

ClonePrep および QuickPrep 同期後スクリプトまたはパワーオフ スクリプトには、20 秒のタイムアウトがあります。親仮想マシンで Windows レジストリの値 ExecScriptTimeout を変更すると、この制限を引き上げることができます。

タイムアウト制限を引き上げる代わりに、カスタム スクリプトを使用して、長時間タスクを実行する別のスクリプトまたはプロセスを起動することもできます。

注: ほとんどの QuickPrep カスタマイズ スクリプトは、20 秒の制限内で実行を終了できます。制限を引き上げる前に、スクリプトをテストしてください。

手順

- 1 親仮想マシンで、Windows レジストリ エディタを起動します。
 - a [スタート]-[コマンド プロンプト]を選択します。
 - b コマンド プロンプトで、[regedit]と入力します。
- 2 Windows レジストリで、vmware-viewcomposer-ga レジストリ キーを探します。
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\vmware-viewcomposer-ga
- 3 [編集] をクリックし、レジストリ値を修正します。

```
Value Name: ExecScriptTimeout
Value Type: REG_DWORD
Value unit: milliseconds
```

デフォルト値は 2000 ミリ秒です。

仮想マシン テンプレートの作成

フル仮想マシンを含む自動プールを作成する前に、仮想マシン テンプレートを作成する必要があります。

仮想マシン テンプレートとは、新しい仮想マシンの作成およびプロビジョニングに使用できる仮想マシンのマスター コピーです。通常、テンプレートには、インストールされたゲスト OS と一連のアプリケーションが含まれています。

仮想マシン テンプレートは vSphere Client で作成します。以前に構成した仮想マシンから仮想マシン テンプレートを作成することも、以前に構成した仮想マシンを仮想マシン テンプレートに変換することもできます。

vSphere Client を使用した仮想マシン テンプレートの作成については、『vSphere 基本システム管理』を参照してください。自動プールの作成については、[フル仮想マシンを含む自動プール](#)を参照してください。

注: 仮想マシン テンプレートは、インスタントクローンまたは View Composer リンククローン デスクトップ プールを作成するためのものではありません。

カスタマイズ仕様の作成

Sysprep を使用してクローンをカスタマイズする場合は、カスタマイズ仕様を指定する必要があります。

Sysprep は、View Composer のリンク クローン デスクトップ プールおよび自動完全クローン デスクトップ プールで使用できますが、インスタントクローン デスクトップ プールでは使用できません。vSphere のカスタマイズ仕様ウィザードを使用して、カスタマイズ仕様を作成します。カスタマイズ仕様ウィザードの使用については、『vSphere Virtual Machine Administration』ドキュメントを参照してください。

デスクトップ プールを作成するために vSphere のカスタマイズ仕様を使用する前に、カスタマイズ仕様をテストすることを推奨します。Sysprep カスタマイズ仕様を使用して Windows デスクトップをドメインに参加させる場合は、Active Directory ドメインの完全修飾ドメイン名 (FQDN) を使用する必要があります。NetBIOS 名は使用できません。

フル仮想マシンを含む自動デスクトップ プールの作成

フル仮想マシンが含まれる自動デスクトップ プールでは、管理者が仮想マシン テンプレートを作成し、View がそのテンプレートを使用して各デスクトップの仮想マシンを作成します。管理者は、必要に応じて、自動プール展開を迅速に処理するためのカスタマイズ仕様も作成できます。

この章には、次のトピックが含まれています。

- [フル仮想マシンを含む自動プール](#)
- [フル仮想マシンを含む自動プールの作成用ワークシート](#)
- [フル仮想マシンを含む自動プールの作成](#)
- [自動デスクトップ プールのクローン作成](#)
- [フル仮想マシンを含む自動プールのデスクトップ設定](#)

フル仮想マシンを含む自動プール

自動デスクトップ プールを作成するために、View はプールに適用された設定に基づいてマシンを動的にプロビジョニングします。View は仮想マシンのテンプレートをプールの基準として使用します。テンプレートから、View は vCenter Server に各デスクトップ用の新しい仮想マシンを作成します。

フル仮想マシンを含む自動プールの作成用ワークシート

自動デスクトップ プールを作成するときに、View Administrator の [デスクトップ プールを追加] ウィザードで特定のオプションを構成するよう求められます。このワークシートを使用して、プールを作成する前に構成オプションを準備します。

このワークシートを印刷し、[デスクトップ プールを追加] ウィザードを実行するときに、希望する値を記入することができます。

表 4-1. ワークシート：フル仮想マシンを含む自動プールを作成するための構成オプション

オプション	説明	値をここに記入
ユーザー割り当て	<p>ユーザー割り当てのタイプを選択します。</p> <ul style="list-style-type: none"> ■ 専用割り当てプールでは、各ユーザーがマシンに割り当てられます。ユーザーは、プールにログインするたびに同じマシンを受け取ります。 ■ 流動割り当てプールでは、ユーザーは、ログインするたびに異なるマシンを受け取ります。 <p>詳細については、以下を参照してください。デスクトップ プールでのユーザー割り当て。</p>	
自動割り当てを有効にする	<p>専用割り当てプールでは、マシンはユーザーが最初にプールにログインするときに割り当てられます。マシンをユーザーに明示的に割り当てすることもできます。</p> <p>自動割り当てを有効にしない場合は、マシンを各ユーザーに明示的に割り当てる必要があります。</p> <p>自動割り当てが有効になっている場合でも、マシンを手動で割り当てることができます。</p>	
vCenter Server	プール内の仮想マシンを管理する vCenter Server を選択します。	
デスクトップ プール ID	<p>View Administrator でプールを識別する一意の名前。</p> <p>環境内で複数の vCenter Server を実行している場合は、別の vCenter Server で同じプール ID を使用していないことを確認します。</p> <p>View 接続サーバ構成は、スタンドアロンの View 接続サーバインスタンスまたは View LDAP 構成を共有する複製されたインスタンスのポッド場合があります。</p>	
表示名	クライアント デバイスからログインするときにユーザーに表示されるプール名。表示名を指定しない場合は、プール ID がユーザーに表示されます。	
アクセス グループ	<p>プールを配置するアクセス グループを選択するか、プールをデフォルトのルート アクセス グループに残します。</p> <p>アクセス グループを使用する場合は、プールの管理を特定のロールを持つ管理者に委任できます。詳細については、『View の管理』のロール ベースの委任管理についての章を参照してください。</p> <p>注： アクセス グループは、デスクトップ仮想マシンを格納する vCenter Server フォルダとは異なります。vCenter Server フォルダは、他の vCenter Server 設定とともにウィザード内で後で選択します。</p>	
ログオフ後にマシンを削除	<p>流動ユーザー割り当てを選択する場合は、ユーザーがログオフした後にマシンを削除するかどうかを選択します。</p> <p>注： このオプションは、[デスクトップ プールの設定] ページで設定します。</p>	

オプション	説明	値をここに記入
デスクトップ プールの設定	<p>デスクトップの状態、仮想マシンが使用中でないときの電源ステータス、表示プロトコル、Adobe Flash 品質などを決定する設定。</p> <p>説明については、すべてのデスクトップ プール タイプのデスクトップ プール設定を参照してください。</p> <p>自動プールに適用される設定のリストについては、フル仮想マシンを含む自動プールのデスクトップ設定を参照してください。</p> <p>電源ポリシーおよび自動プールの詳細については、デスクトッププールの電源ポリシーの設定を参照してください。</p>	
エラーによりプロビジョニングを停止	<p>仮想マシンのプロビジョニング中にエラーが発生した後で、デスクトップ プールの仮想マシンのプロビジョニングを停止するか続行するかを View に指示できます。この設定を選択した状態にしておくと、複数の仮想マシンでプロビジョニングエラーが繰り返されるのを防ぐことができます。</p>	
仮想マシンの名前付け	<p>マシン名のリストを手動で指定してマシンをプロビジョニングするか、それとも名前付けパターンとマシンの総数を指定してマシンをプロビジョニングするかを選択します。</p> <p>詳細については、以下を参照してください。マシンの手動での名前付けまたは名前付けパターンの指定。</p>	
名前を手動で指定	<p>名前を手動で指定する場合は、マシン名のリストと、必要に応じて関連するユーザー名を準備します。</p>	
名前付けパターン	<p>この名前付け方法を使用する場合は、パターンを指定します。指定したパターンをすべてのマシン名のプレフィックスとして使用し、その後に各マシンを識別するための一意の番号を付けます。</p> <p>詳細については、以下を参照してください。自動デスクトップ プールでの名前付けパターンの使用。</p>	
マシンの最大数	<p>名前付けパターンを使用する場合は、プール内のマシンの総数を指定します。</p> <p>プールを最初に作成するときに、プロビジョニングするマシンの最小数を指定することもできます。</p>	
スベアの（パワーオン状態の）マシンの数	<p>名前を手動で指定する場合、または名前付けパターンを使用する場合は、新しいユーザーのために可用性とパワーオン状態を維持しておくマシンの数を指定します。詳細については、以下を参照してください。マシンの手動での名前付けまたは名前付けパターンの指定。</p> <p>名前を手動で指定する場合、このオプションの名称は [パワーオン状態の未割り当てのマシンの数] です。</p>	
マシンの最小数	<p>名前付けパターンを使用し、必要に応じてマシンをプロビジョニングする場合は、プール内のマシンの最小数を指定します。</p> <p>プールを作成するときに、マシンの最小数が作成されます。</p> <p>必要に応じてマシンをプロビジョニングする場合、ユーザーがプールに初めて接続したとき、またはマシンをユーザーに割り当てたときに追加のマシンが作成されます。</p>	

オプション	説明	値をここに記入
vSphere Virtual SAN を使用する	可能な場合は、Virtual SAN を使用するかどうかを指定します。Virtual SAN はソフトウェア定義のストレージ階層で、ESXi ホストのクラスタで使用可能なローカル物理ストレージ ディスクを仮想化します。詳細については、 高パフォーマンス ストレージとポリシー ベース管理のための Virtual SAN の使用 を参照してください。	
テンプレート	プールを作成するために使用する仮想マシン テンプレートを選択します。	
vCenter Server folder (vCenter Server フォルダ)	デスクトップ プールが配置される vCenter Server 内のフォルダを選択します。	
Host or cluster (ホストまたはクラスタ)	仮想マシンが実行される ESXi ホストまたはクラスタを選択します。 vSphere 5.1 以降では、最大 32 台の ESXi ホストでクラスタを選択できます。	
Resource pool (リソース プール)	デスクトップ プールが配置される vCenter Server リソース プールを選択します。	
データストア	デスクトップ プールを格納するデータストアを 1 つ以上選択します。 クラスタの場合は、共有またはローカル データストアを使用できます。 注: Virtual SAN を使用する場合、データストアを 1 つのみ選択します。	
View Storage Accelerator を使用	ESXi ホストで、共通の仮想マシン ディスク データをキャッシュするかどうかを指定します。View Storage Accelerator を使用することで、多数の起動とウイルス対策 スキャンの I/O ストームを管理する際のパフォーマンスが向上し、追加のストレージ I/O 帯域幅の必要性が少なくなります。 この機能は vSphere 5.0 以降でサポートされています。 この機能は、デフォルトで有効になっています。 詳細については、以下を参照してください。 View Composer リンク クローン用の View Storage Accelerator の構成 。	

オプション	説明	値をここに記入
透過的ページ共有の範囲	<p>透過的なページ共有 (TPS) を実行できるレベルを選択します。[仮想マシン] (デフォルト)、[プール]、[ポッド]、または [グローバル] から選択します。プール、ポッド、またはグローバルですべてのマシンに対して TPS をオンにすると、ESXi ホストは、マシンが同じゲスト オペレーティング システムまたはアプリケーションを使用した結果生じるメモリ ページの余分なコピーを取り除きます。</p> <p>ページ共有は ESXi ホストで発生します。たとえば、プールレベルで TPS を有効にするが、プールが複数の ESXi ホストにまたがっている場合、同じホスト上、または同じプール内の仮想マシンのみがページを共有します。グローバルレベルでは、同じ ESXi ホスト上で View によって管理されているすべてのマシンは、マシンが置かれているプールに関係なく、メモリ ページを共有できます。</p> <p>注: TPS はセキュリティ上のリスクを招く可能性があるため、デフォルト設定ではマシン間でのメモリ ページの共有が行われません。調査では、非常に限定された構成シナリオにおいて、TPS を悪用してデータへの不許可のアクセスを取得できる可能性があることが示されています。</p>	
Guest customization (ゲストのカスタマイズ)	<p>カスタマイズ仕様 (SYSPREP) をリストから選択して、マシン上でライセンス、ドメインへの関連付け、DHCP 設定、およびその他のプロパティを構成します。</p> <p>または、マシンの作成後に、マシンを手動でカスタマイズできます。</p>	

フル仮想マシンを含む自動プールの作成

選択した仮想マシン テンプレートに基づいて自動デスクトップ プールを作成できます。View は、デスクトップを動的に展開して、vCenter Server に各デスクトップ用の新しい仮想マシンを作成します。

前提条件

- View がマシンを作成するために使用する仮想マシンのテンプレートを準備します。Horizon Agent はテンプレートにインストールされる必要があります。[3 章 クローン作成のための親仮想マシンの作成と準備](#)を参照してください。
- カスタマイズ仕様を使う予定がある場合は、仕様が正確であることを確認します。vSphere Client で、カスタマイズ仕様を使ってテンプレートから仮想マシンを展開してカスタマイズします。結果として得られた仮想マシンを完全にテストします (DHCP や認証を含む)。
- リモート デスクトップとして使用している仮想マシンに対して使用されている ESXi 仮想スイッチに十分な数のポートがあることを確認します。大規模なデスクトップ プールを作成する場合、デフォルト値では不十分なことがあります。ESXi ホスト上の仮想スイッチ ポートの数は、仮想マシンの数に、仮想マシンあたりの仮想 NIC の数をかけた数以上である必要があります。
- プールを作成するために指定する必要がある構成情報を収集します。[フル仮想マシンを含む自動プールの作成用ワークシート](#)を参照してください。

- 電源設定、表示プロトコル、Adobe Flash 品質、およびその他の設定を構成する方法を決定します。[すべてのデスクトップ プール タイプのデスクトップ プール設定](#)を参照してください。
- VMware Identity Manager からデスクトップとアプリケーションへのアクセスを提供しようとしている場合、View Administrator のルート アクセス グループで Administrators ロールを持つユーザーとしてデスクトップ プールとアプリケーション プールを作成していることを確認します。ルート アクセス グループ以外で Administrators ロールをユーザーに付与すると、VMware Identity Manager は、View で構成する SAML 認証システムを認識せず、VMware Identity Manager でプールを構成できません。

手順

- 1 View Administrator で、[カタログ] - [デスクトップ プール]を選択します。
- 2 [追加] をクリックします。
- 3 [自動化されたデスクトップ プール] を選択します。
- 4 [vCenter Server] ページで、[フル仮想マシン] を選択します。
- 5 ウィザードの指示に従って、プールを作成します。

ワークシートで収集した構成情報を使用します。ナビゲーション パネルのページ名をクリックすると、完了したウィザード ページに直接戻ることができます。

View Administrator で、[カタログ] - [デスクトップ プール] を選択すると、プールに追加されているとおりにマシンを表示できます。

次のステップ

プールにアクセスするための資格をユーザーに付与します。[デスクトップまたはアプリケーション プールへの資格の追加](#)を参照してください。

自動デスクトップ プールのクローン作成

既存のプールから自動デスクトップ プールのクローンを作成できます。プールのクローンを作成する場合、既存のデスクトップ プールの設定が [デスクトップ プールを追加] ウィザードにコピーされるため、各設定を手動で入力することなく新しいプールを作成できます。

この機能を使用すれば、[デスクトップ プールを追加] ウィザードで各オプションを入力する必要がなくなるため、プールの作成を合理化できます。ウィザードの事前入力値を使用して、デスクトップ プール属性が標準化されていることを確認できます。

フル仮想マシンまたは View Composer リンク クローンを含む自動デスクトップ プールのクローンを作成できます。インスタント クローンの自動デスクトップ プール、手動デスクトップ プール、または RDS デスクトップ プールのクローンを作成することはできません。

デスクトップ プールのクローンを作成する場合、特定の設定は変更できません。

- デスクトップ プール タイプ
- クローン タイプ（リンク クローンまたはフル仮想マシン）
- ユーザー割り当て（専用または流動）

■ vCenter Server インスタンス

前提条件

- 元のデスクトップ プールを作成するための前提条件がまだ有効であることを確認します。
たとえば、フル仮想マシンを含むプールの場合、仮想マシン テンプレートが準備されていることを確認します。
リンククローン プールの場合、親仮想マシンが準備されていて、仮想マシンのパワーオフ後にスナップショットが作成されていることを確認します。
プールのクローンを作成する場合、同じ仮想マシン テンプレートまたは親仮想マシンを使用することができますが、別の仮想マシン テンプレートまたは親仮想マシンを選択することもできます。
- 自動完全クローン プールのクローンを作成するための前提条件については、[フル仮想マシンを含む自動プールの作成](#)を参照してください。
- リンククローン プールのクローンを作成するための前提条件については、[リンククローン デスクトップ プールの作成](#)を参照してください。

手順

- 1 View Administrator で、[カタログ] - [デスクトップ プール] を選択します。
- 2 クローンを作成するデスクトップ プールを選択し、[クローン] をクリックします。
[デスクトップ プールを追加] ウィザードが表示されます。
- 3 [デスクトップ プールを追加] ページで、一意のプール ID を入力します。
- 4 [プロビジョニングの設定] ページで、仮想マシンの一意の名前を入力します。

オプション	説明
[名前付けパターンを使用]	仮想マシンの名前付けパターンを入力します。
[名前を手動で指定]	仮想マシンの一意の名前のリストを入力します。

- 5 ウィザードの他の指示に従って、プールを作成します。
必要に応じて、デスクトップ プールの設定および値を変更します。

View Administrator で、[カタログ] - [デスクトップ プール] を選択すると、プールに追加されているとおりにマシンを表示できます。

次のステップ

プールにアクセスするための資格をユーザーに付与します。[デスクトップまたはアプリケーション プールへの資格の追加](#)を参照してください。

フル仮想マシンを含む自動プールのデスクトップ設定

フル仮想マシンを含む自動プールを構成するときに、デスクトップ プールの設定を指定する必要があります。専用ユーザー割り当てを使用するプールと流動ユーザー割り当てを使用するプールには、異なる設定が適用されます。

表 4-2. フル仮想マシンを含む自動プールの設定 に、専用ユーザー割り当てを使用する自動プールおよび流動ユーザー割り当てを使用する自動プールに適用される設定を示します。

各デスクトップ プール設定の説明については、[すべてのデスクトップ プール タイプのデスクトップ プール設定](#)を参照してください。

表 4-2. フル仮想マシンを含む自動プールの設定

設定	自動プール、専用割り当て	自動プール、流動割り当て
状態	はい	はい
接続サーバ restrictions (接続サーバの制限)	はい	はい
リモート マシンの電源ポリシー	はい	はい
Automatic logoff after disconnect (切断後に自動的にログオフ)	はい	はい
ユーザーによるマシンのリセットを許可	はい	はい
ユーザーが複数のクライアント デバイスからセッションを個別に開始できるようにする		はい
ログオフ後にマシンを削除		はい
デフォルト表示プロトコル	はい	はい
ユーザーがプロトコルを選択できるようにする	はい	はい
3D レンダラー	はい	はい
Max number of monitors (モニタの最大数)	はい	はい
Max resolution of any one monitor (特定のモニタの最大解像度)	はい	はい
Adobe Flash quality (Adobe Flash の品質)	はい	はい
Adobe Flash throttling (Adobe Flash のスロットル)	はい	はい
Mirage 設定全体をオーバーライドする	はい	はい
Mirage サーバの構成	はい	はい

リンク クローン デスクトップ プールの作成

リンク クローン デスクトップ プールを使用して、View は選択した親仮想マシンに基づいてデスクトップ プールを作成します。View Composer サービスは、vCenter Server に各デスクトップ用の新しいリンク クローン仮想マシンを動的に作成します。

この章には、次のトピックが含まれています。

- [リンク クローン デスクトップ プール](#)
- [リンク クローン デスクトップ プールの作成用ワークシート](#)
- [リンククローン デスクトップ プールの作成](#)
- [自動デスクトップ プールのクローン作成](#)
- [リンク クローン デスクトップ プールのデスクトップ プール設定](#)
- [View Composer でのリンク クローンの SID およびサードパーティ アプリケーションのサポート](#)
- [View Composer の操作時に、リモート デスクトップ セッションで使用するようプロビジョニングされたリンククローン マシンを維持する](#)
- [リンク クローンに既存の Active Directory コンピュータ アカウントを使用する](#)

リンク クローン デスクトップ プール

リンク クローン デスクトップ プールを作成するために、View Composer は、親仮想マシンのスナップショットからリンク クローン仮想マシンを生成します。View は、プールに適用された設定に基づいてリンク クローン デスクトップを動的にプロビジョニングします。

リンク クローン デスクトップは基本のシステム ディスク イメージを共有するため、使用するストレージはフル仮想マシンよりも少なくなります。

リンク クローン デスクトップ プールの作成用ワークシート

リンク クローン デスクトップ プールを作成するときに、View Administrator の [デスクトップ プールを追加] ウィザードで特定のオプションを構成するよう求められます。このワークシートを使用して、プールを作成する前に構成オプションを準備します。

このワークシートを印刷し、[デスクトップ プールを追加] ウィザードを実行するときに、希望する値を記入することができます。

リンク クローン プールを作成する前に、vCenter Server を使用して、プールのために準備する親仮想マシンのスナップショットを作成する必要があります。スナップショットを作成する前に親仮想マシンをシャットダウンする必要があります。View Composer は、クローンを作成するための基本イメージとしてスナップショットを使用します。

注: 仮想マシン テンプレートからリンク クローン プールを作成することはできません。

表 5-1. ワークシート：リンク クローン デスクトップ プールを作成するための構成オプション

オプション	説明	値をここに記入
ユーザー割り当て	<p>ユーザー割り当てのタイプを選択します。</p> <ul style="list-style-type: none"> ■ 専用割り当てプールでは、各ユーザーがマシンに割り当てられます。ユーザーは、ログインするたびに同じマシンを受け取ります。 ■ 流動割り当てプールでは、ユーザーは、ログインするたびに異なるマシンを受け取ります。 <p>詳細については、以下を参照してください。デスクトップ プールでのユーザー割り当て。</p>	
自動割り当てを有効にする	<p>専用割り当てプールでは、マシンはユーザーが最初にプールにログインするときに割り当てられます。マシンをユーザーに明示的に割り当てることもできます。</p> <p>自動割り当てを有効にしない場合は、マシンを各ユーザーに明示的に割り当てる必要があります。</p>	
vCenter Server	プール内の仮想マシンを管理する vCenter Server を選択します。	
デスクトップ プール ID	<p>View Administrator でプールを識別する一意の名前。</p> <p>環境内で複数の View 接続サーバ構成を実行している場合は、別の View 接続サーバ構成で同じプール ID を使用していないことを確認します。</p> <p>View 接続サーバ構成は、スタンドアロンの View 接続サーバ インスタンスまたは View LDAP 構成を共有する複製されたインスタンスのボッド場合があります。</p>	
表示名	クライアント デバイスからログインするときにユーザーに表示されるプール名。表示名を指定しない場合は、プール ID がユーザーに表示されます。	
アクセス グループ	<p>プールを配置するアクセス グループを選択するか、プールをデフォルトのルート アクセス グループに残します。</p> <p>アクセス グループを使用する場合は、プールの管理を特定のロールを持つ管理者に委任できます。詳細については、『View の管理』のロール ベースの委任管理についての章を参照してください。</p> <p>注: アクセス グループは、デスクトップとして使用される仮想マシンを格納する vCenter Server フォルダとは異なります。vCenter Server フォルダは、他の vCenter Server 設定とともにウィザード内で後で選択します。</p>	
ログオフ時にマシンを削除または更新	<p>流動ユーザー割り当てを選択する場合は、ユーザーがログオフした後にマシンを更新するか、マシンを削除するか、または何もしないかを選択します。</p> <p>注: このオプションは、[デスクトップ プールの設定] ページで設定します。</p>	

オプション	説明	値をここに記入
デスクトップ プールの設定	<p>マシンの状態、仮想マシンが使用中でないときの電源ステータス、表示プロトコル、Adobe Flash 品質などを決定する設定。</p> <p>説明については、すべてのデスクトップ プール タイプのデスクトップ プール設定を参照してください。</p> <p>リンク クローン プールに適用される設定のリストについては、リンク クローン デスクトップ プールのデスクトップ プール設定を参照してください。</p> <p>電源ポリシーおよび自動プールの詳細については、デスクトップ プールの電源ポリシーの設定を参照してください。</p>	
エラーによりプロビジョニングを停止	<p>仮想マシンのプロビジョニング中にエラーが発生した後で、デスクトップ プールの仮想マシンのプロビジョニングを停止するか続行するかを View に指示できます。この設定を選択した状態にしておくと、複数の仮想マシンでプロビジョニング エラーが繰り返されるのを防ぐことができます。</p>	
Virtual machine naming (仮想マシンの名前付け)	<p>マシン名のリストを手動で指定してマシンをプロビジョニングするか、それとも名前付けパターンとマシンの総数を指定してマシンをプロビジョニングするかを選択します。</p> <p>詳細については、以下を参照してください。マシンの手動での名前付けまたは名前付けパターンの指定。</p>	
名前を手動で指定	<p>名前を手動で指定する場合は、マシン名のリストと、必要に応じて関連するユーザー名を準備します。</p>	
Naming pattern (名前付けパターン)	<p>この名前付け方法を使用する場合は、パターンを指定します。</p> <p>指定したパターンをすべてのマシン名のプレフィックスとして使用し、その後に各マシンを識別するための一意の番号を付けます。</p> <p>詳細については、以下を参照してください。自動デスクトップ プールでの名前付けパターンの使用。</p>	
マシンの最大数	<p>名前付けパターンを使用する場合は、プール内のマシンの総数を指定します。</p> <p>プールを最初に作成するときに、プロビジョニングするマシンの最小数を指定することもできます。</p>	
スベアの (パワーオン状態の) マシンの数	<p>名前を手動で指定する場合、または名前付けパターンを使用する場合は、新しいユーザーのために可用性とパワーオン状態を維持しておくマシンの数を指定します。詳細については、以下を参照してください。マシンの手動での名前付けまたは名前付けパターンの指定。</p> <p>名前を手動で指定する場合、このオプションの名称は [パワーオン状態の未割り当てのマシン数] です。</p>	

オプション	説明	値をここに記入
View Composer のメンテナンス操作における（プロビジョニング済み）動作可能マシンの最小数	<p>名前を手動で指定するか名前付けパターンを使用する場合は、View Composer のメンテナンス操作中に、リモート デスクトップ セッションで使用するようプロビジョニングされるマシンの最小数を指定します。</p> <p>この設定を使用すると、View Composer がプールにあるマシンを更新、再構成、または再調整するときに、ユーザーは既存の接続を維持したり、新しい接続要求を行ったりできます。この設定では、新しい接続の受け入れ準備ができていないスベア マシンと既存のデスクトップ セッションですでに接続されているマシンは区別されません。</p> <p>この値は、オンデマンドでマシンをプロビジョニングする場合に指定する [マシンの最大数] より小さくなければなりません。</p> <p>View Composer の操作時に、リモート デスクトップ セッションで使用するようプロビジョニングされたリンククローン マシンを維持するを参照してください。</p>	
<p>オンデマンドでマシンをプロビジョニング</p> <p>または</p> <p>全マシンを事前にプロビジョニング</p>	<p>名前付けパターンを使用する場合は、プールが作成されたときにすべてのマシンをプロビジョニングするか、必要に応じてマシンをプロビジョニングするかを選択します。</p> <ul style="list-style-type: none"> ■ [全マシンを事前にプロビジョニング]。プールが作成されたときに、システムは、[マシンの最大数] で指定した数のマシンをプロビジョニングします。 ■ [オンデマンドでマシンをプロビジョニング]。プールが作成されたときに、システムは、[マシンの最小数] で指定した数のマシンを作成します。ユーザーがプールに初めて接続したとき、またはマシンをユーザーに割り当てたときに追加のマシンが作成されます。 	
マシンの最小数	<p>名前付けパターンを使用し、必要に応じてデスクトップをプロビジョニングする場合は、プール内のマシンの最小数を指定します。</p> <p>システムは、プールが作成されたときに最小数のマシンを作成します。この数は、[ログオフ時にマシンを削除または更新] などの設定によってマシンが削除される場合でも保持されます。</p>	
Windows プロファイルを通常ディスクにリダイレクト	<p>専用ユーザー割り当てを選択する場合は、Windows ユーザー プロファイル データを別個の View Composer 通常ディスクに格納するか、OS データと同じディスクに格納するかを選択します。</p> <p>別個の通常ディスクを使用すると、ユーザー データおよび設定を保持できます。View Composer の更新、再構成、および再分散操作は、通常ディスクに影響を与えません。通常ディスクをリンク クローンから切断し、切断されたディスクからリンク クローン仮想マシンを再作成することができます。たとえば、マシンまたはプールが削除されたとき、通常ディスクを切断しデスクトップを再作成して、元のユーザー データおよび設定を保持することができます。</p> <p>Windows プロファイルを OS ディスクに格納する場合、ユーザー データおよび設定は、更新、再構成、および再分散操作時に削除されます。</p>	

オプション	説明	値をここに記入
Disk size and drive letter for persistent disk (通常ディスクのディスク サイズおよびドライブ文字)	<p>別個の View Composer 通常ディスクにユーザー プロファイル データを格納する場合は、ディスク サイズ (メガバイト単位) とドライブ文字を指定します。</p> <p>注: 親仮想マシンにすでに存在するドライブ文字、またはネットワーク マウントされたドライブに使用されているドライブ文字と競合するドライブ文字は選択しないでください。</p>	
ディスポーザブル ファイルのリダイレクト	<p>ゲスト OS のページング ファイルと一時ファイルを別の読み取り専用ディスクにリダイレクトするかどうかを選択します。リダイレクトする場合は、ディスク サイズをメガバイト単位で指定します。</p> <p>この構成では、リンク クローンがパワーオフされると、破棄可能ファイル ディスクは、リンク クローン プールで作成された元のディスクのコピーに置き換わります。ユーザーがデスクトップを操作するたびに、リンク クローンのサイズが増える可能性があります。破棄可能ファイルのリダイレクトにより、リンク クローンの拡大を抑えることで、ストレージ領域を節約できます。</p>	
Disk size and drive letter for disposable file disk (破棄可能ファイル ディスクのディスク サイズおよびドライブ文字)	<p>破棄可能ファイルを読み取り専用ディスクにリダイレクトする場合は、ディスク サイズ (MB) とドライブ文字を指定します。</p> <p>ディスク サイズは、ゲスト OS のページ ファイル サイズよりも大きくしてください。ページ ファイル サイズの決定については、View Composer 親仮想マシンのページング ファイル サイズの記録を参照してください。</p> <p>破棄可能ファイル ディスクのサイズを構成する場合は、フォーマットされたディスク パーティションの実際のサイズが、View Administrator で指定した値よりわずかに小さいことを考慮してください。</p> <p>破棄可能ファイル ディスクのドライブ文字は選択できます。デフォルト値の [自動] を使用すると、View でドライブ文字を割り当てます。</p> <p>注: 親仮想マシンにすでに存在するドライブ文字、またはネットワーク マウントされたドライブに使用されているドライブ文字と競合するドライブ文字は選択しないでください。</p>	
vSphere Virtual SAN を使用する	<p>可能な場合、VMware Virtual SAN を使用するかどうかを指定します。Virtual SAN はソフトウェア定義のストレージ階層で、ESXi ホストのクラスターで使用可能なローカル物理ストレージ ディスクを仮想化します。詳細については、高パフォーマンス ストレージとポリシー ベース管理のための Virtual SAN の使用を参照してください。</p>	
通常ディスクおよび OS ディスク用に別のデータストアを選択します。	<p>(Virtual SAN を使用しない場合にのみ使用可能) ユーザー プロファイルを別の通常ディスクにリダイレクトすると、通常ディスクおよび OS ディスクを別のデータストアに格納できます。</p>	

オプション	説明	値をここに記入
レプリカおよび OS ディスク用に別のデータストアを選択します	<p>(Virtual SAN または Virtual Volumes を使用しない場合にのみ使用可能) レプリカ (マスタ) 仮想マシン ディスクを高パフォーマンスのデータストアに格納し、リンク クローンを別のデータストアに格納できます。</p> <p>詳細については、以下を参照してください。 インスタント クローンおよび View Composer リンク クローン用の別のデータストアへのレプリカおよびクローンの格納。</p> <p>レプリカおよび OS ディスクを別のデータストアに格納すると、ネイティブ NFS スナップショットが使用できなくなります。NAS デバイス上のネイティブ クローン作成を実行できるのは、レプリカおよび OS ディスクが同じデータストアに格納されている場合のみです。</p>	
親仮想マシン	プールの親仮想マシンを選択します。	
スナップショット (デフォルト イメージ)	<p>プールの基本イメージとして使用する親仮想マシンのスナップショットを選択します。</p> <p>vCenter Server からスナップショットと親仮想マシンを削除しないようにしてください。ただし、プール内のリンク クローンがデフォルト イメージを使用せず、このデフォルト イメージから今後リンク クローンを作成することがない場合は削除しても構いません。システムでは、プール ポリシーに従ってプール内に新しいリンク クローンをプロビジョニングするために、親仮想マシンおよびスナップショットが必要です。親仮想マシンとスナップショットは、View Composer の保守作業にも必要です。</p>	
仮想マシンのフォルダの場所	デスクトップ プールが配置される vCenter Server 内のフォルダを選択します。	
Host or cluster (ホストまたはクラスター)	<p>デスクトップ仮想マシンが実行される ESXi ホストまたはクラスターを選択します。</p> <p>Virtual SAN データストア (vSphere 5.5 Update 1 の機能) では、最大 20 個までの ESXi ホストを持つクラスターを選択できます。</p> <p>Virtual Volumes データストア (vSphere 6.0 の機能) では、最大 32 個までの ESXi ホストを持つクラスターを選択できます。</p> <p>vSphere 5.1 以降では、レプリカが VMFS5 以降のデータストアまたは NFS データストアに保存されている場合、最大で 32 台の ESXi ホストでクラスターを選択できます。VMFS5 より前の VMFS パージョンにレプリカを保存する場合、クラスターは最大で 8 ホストを持つことができます。</p> <p>vSphere 5.0 では、レプリカが NFS データストアに保存されている場合、8 を超える ESXi ホストでクラスターを選択できます。レプリカを VMFS データストアに保存する場合、クラスターは最大で 8 つのホストを持つことができます。 8 台を超えるホストを含むクラスターのデスクトップ プールの構成を参照してください。</p>	
Resource pool (リソース プール)	デスクトップ プールが配置される vCenter Server リソース プールを選択します。	

オプション	説明	値をここに記入
データストア	<p>デスクトップ プールを格納するデータストアを 1 つ以上選択します。</p> <p>[デスクトップ プールを追加] ウィザードの [リンク クローンのデータストアを選択] ページにある表は、プールのストレージ要件を見積もるための大まかなガイドラインを提供します。これらのガイドラインは、リンク クローン ディスクを格納するための十分な大きさがあるデータストアを特定するのに役立ちます。詳細については、以下を参照してください。 インスタントクローンおよび View Composer リンククローン デスクトップ プールのストレージ サイズ設定。</p> <p>個別の ESXi ホストまたは ESXi クラスタに、共有またはローカル データストアを使用できます。ESXi クラスタでローカル データストアを使用する場合は、デスクトップの展開で課せられる vSphere インフラストラクチャの制約を考慮する必要があります。 ローカル データストアへの View Composer リンク クローンの保存 を参照してください。</p> <p>Virtual SAN データストア (vSphere 5.5 Update 1 の機能) では、最大 20 個までの ESXi ホストを持つクラスタを選択できます。</p> <p>Virtual Volumes データストア (vSphere 6.0 の機能) では、最大 32 個までの ESXi ホストを持つクラスタを選択できます。</p> <p>vSphere 5.1 以降では、VMFS5 以降または NFS であるデータストアにレプリカが保存されている場合、クラスタは 8 台を超える ESXi ホストを持つことができます。vSphere 5.0 では、レプリカが NFS データストアに保存されている場合、クラスタは 8 台を超える ESXi ホストを持つことができます。 8 台を超えるホストを含むクラスタでのデスクトップ プールの構成 を参照してください。</p> <p>リンク クローン用に作成されるディスクの詳細については、 View Composer リンククローン データ ディスク を参照してください。</p> <p>注: Virtual SAN を使用する場合、データストアを 1 つのみ選択します。</p>	
ストレージ オーバーコミット	<p>各データストアでリンク クローンを作成する際のストレージ オーバーコミット レベルを決定します。</p> <p>レベルを高くすると、データストアに割り当てられるリンク クローンの数が増加し、個々のクローンの増大に予約される領域は小さくなります。ストレージ オーバーコミットのレベルを高くすると、データストアの物理ストレージ上限を超える合計論理サイズを持つリンク クローンを作成できます。詳細については、以下を参照してください。 リンククローン仮想マシンのストレージのオーバーコミット レベルの設定。</p> <p>注: Virtual SAN を使用する場合、この設定は効果がありません。</p>	

オプション	説明	値をここに記入
View Storage Accelerator を使用	<p>ESXi ホストが共通の仮想マシン ディスク データをキャッシュできるようにする View Storage Accelerator を使用するかどうかを指定します。View Storage Accelerator を使用することで、多数の起動とウイルス対策スキャンの I/O ストームを管理する際のパフォーマンスが向上し、追加のストレージ I/O 帯域幅の必要性が少なくなります。</p> <p>この機能は vSphere 5.0 以降でサポートされています。</p> <p>この機能は、デフォルトで有効になっています。</p> <p>詳細については、以下を参照してください。View Composer リンク クローン用の View Storage Accelerator の構成。</p>	
ネイティブ NFS スナップショット (VAAI) を使用	<p>(Virtual SAN を使用しない場合にのみ使用可能) vStorage APIs for Array Integration (VAAI) をサポートする NAS デバイスが展開内に含まれている場合、ネイティブ 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できます。</p> <p>この機能を使用できるのは、VAAI を介したネイティブ クローン作成操作をサポートする NAS デバイスに存在するデータストアを選択した場合だけです。</p> <p>レプリカと OS ディスクを別々のデータストアに格納している場合、この機能は使用できません。領域効率の高いディスクのある仮想マシンでは、この機能は使用できません。</p> <p>この機能は vSphere 5.0 以降でサポートされています。</p> <p>詳細については、以下を参照してください。View Composer リンク クローン用の VAAI ストレージの使用。</p>	
VM ディスク スペースを再利用	<p>(Virtual SAN または Virtual Volumes を使用しない場合にのみ使用可能) ESXi ホストがスペース効率的なディスク形式でフォーマットされたリンク クローンの未使用ディスク領域を再利用できるようにするかどうかを決定します。領域再利用機能により、リンク クローン デスクトップに必要なストレージ容量が削減されます。</p> <p>この機能は vSphere 5.1 以降でサポートされています。リンク クローン仮想マシンは、仮想ハードウェア バージョン 9 以降である必要があります。</p> <p>詳細については、以下を参照してください。View Composer リンク クローンでのディスク領域の再利用。</p>	
仮想マシンの未使用領域が次の値を超えると再利用が開始されます。	<p>(Virtual SAN または Virtual Volumes を使用しない場合にのみ使用可能) 領域再利用のトリガーとなる、リンク クローン OS ディスク上に蓄積する必要がある未使用ディスク領域の最小量 (GB) を入力します。未使用ディスク領域がこのしきい値を超過すると、View は ESXi ホストに OS ディスク上の領域を再利用するように指示する操作を開始します。</p> <p>この値は仮想マシンごとに計測されます。未使用ディスク領域が個々の仮想マシンで指定したしきい値を超過すると、View はそのマシンで領域再利用プロセスを開始します。</p> <p>例: 2 GB。</p> <p>デフォルト値は 1 GB です。</p>	

オプション	説明	値をここに記入
停電期間	<p>View Storage Accelerator の再生成と仮想マシン ディスク領域の再利用が行われない日時を構成します。</p> <p>必要に応じて ESXi のリソースがフォアグラウンド タスク専用になるように、ESXi ホストでこれらの操作を実行しない日時を指定できます。</p> <p>詳細については、以下を参照してください。View Composer リンク クローン用の Storage Accelerator と領域再利用の停電期間の設定。</p>	
透過的ページ共有の範囲	<p>透過的なページ共有 (TPS) を実行できるレベルを選択します。[仮想マシン] (デフォルト)、[プール]、[ポッド]、または [グローバル] から選択します。プール、ポッド、またはグローバルですべてのマシンに対して TPS をオンにすると、ESXi ホストは、マシンが同じゲスト オペレーティング システムまたはアプリケーションを使用した結果生じるメモリ ページの余分なコピーを取り除きます。</p> <p>ページ共有は ESXi ホストで発生します。たとえば、プール レベルで TPS を有効にするが、プールが複数の ESXi ホストにまたがっている場合、同じホスト上、または同じプール内の仮想マシンのみがページを共有します。グローバル レベルでは、同じ ESXi ホスト上で View によって管理されているすべてのマシンは、マシンが置かれているプールに関係なく、メモリ ページを共有できます。</p> <p>注: TPS はセキュリティ上のリスクを招く可能性があるため、デフォルト設定ではマシン間でのメモリ ページの共有が行われません。調査では、非常に限定された構成シナリオにおいて、TPS を悪用してデータへの不許可のアクセスを取得できる可能性があることが示されています。</p>	
ドメイン	<p>Active Directory ドメインおよびユーザー名を選択します。</p> <p>View Composer では、リンク クローン プールを作成するために特定のユーザー権限が必要となります。ドメインおよびユーザー アカウントは、リンク クローン マシンをカスタマイズするために QuickPrep または Sysprep によって使用されます。</p> <p>このユーザーは、vCenter Server のための View Composer 設定を構成するときに指定します。View Composer 設定を構成する場合は、複数のドメインとユーザーを指定できます。[デスクトップ プールを追加] ウィザードを使用してプールを作成する場合、リストから 1 つのドメインとユーザーを選択する必要があります。</p> <p>View Composer の構成については、『View 管理』のマニュアルを参照してください。</p>	
AD コンテナ	<p>Active Directory コンテナの相対識別名を指定します。</p> <p>例 : CN=Computers</p> <p>[デスクトップ プールを追加] ウィザードを実行するとき、Active Directory ツリー内のコンテナを参照できます。</p>	

オプション	説明	値をここに記入
既存のコンピュータ アカウントの再利用を許可	<p>View Composer によってプロビジョニングされたリンク クローンで、Active Directory 内の既存のコンピュータ アカウントを使用するには、このオプションを選択します。このオプションにより、Active Directory で作成されたコンピュータ アカウントを管理できます。</p> <p>リンク クローンがプロビジョニングされたときに、既存の AD コンピュータ アカウント名がリンク クローン マシン名と一致すれば、View Composer は既存のコンピュータ アカウントを使用します。一致しない場合は、新しいコンピュータ アカウントが作成されます。</p> <p>既存のコンピュータ アカウントが、[Active Directory コンテナ] 設定で指定する Active Directory コンテナに配置されている必要があります。</p> <p>このオプションが無効になっていると、View Composer がリンク クローンをプロビジョニングするときに、新しい AD コンピュータ アカウントが作成されます。このオプションは、デフォルトで無効になっています。</p> <p>詳細については、以下を参照してください。リンク クローンに既存の Active Directory コンピュータ アカウントを使用する。</p>	
Use QuickPrep or a customization specification (Sysprep) (QuickPrep またはカスタマイズ仕様 (Sysprep) を使用)	<p>ライセンス、ドメインへの関連付け、DHCP 設定、およびその他のプロパティをマシンで構成できるようにするために、QuickPrep を使用するか、カスタマイズ仕様 (Sysprep) を選択するかを選択します。</p> <p>リンク クローンに対して Sysprep がサポートされるのは vSphere 4.1 以降のソフトウェア上だけです。</p> <p>QuickPrep または Sysprep を使用してプールを作成すると、後でそのプール内のマシンを作成または再構成するときに他のカスタマイズ方法に切り替えることはできません。</p> <p>詳細については、以下を参照してください。リンク クローン マシンをカスタマイズするための QuickPrep または Sysprep の選択。</p>	
Power-off script (パワーオフ スクリプト)	<p>QuickPrep は、リンク クローン マシンがパワーオフされる前にマシン上でカスタマイズ スクリプトを実行できます。</p> <p>親仮想マシン上のスクリプトのパスおよびスクリプト パラメータを指定します。</p>	
同期後スクリプト	<p>QuickPrep は、リンク クローン マシンが作成、再構成、および更新された後にそのマシン上でカスタマイズ スクリプトを実行できます。</p> <p>親仮想マシン上のスクリプトのパスおよびスクリプト パラメータを指定します。</p>	

リンククローン デスクトップ プールの作成

選択した親仮想マシンに基づいて自動リンク クローン デスクトップ プールを作成できます。View Composer サービスは、vCenter Server に各デスクトップ用の新しいリンク クローン仮想マシンを動的に作成します。

フル仮想マシンを含む自動プールの作成については、[フル仮想マシンを含む自動プール](#)を参照してください。

前提条件

- View Composer サービスが vCenter Server と同じホストまたは個別のホストにインストールされていて、View Composer データベースが構成されていることを確認します。『View インストール ガイド』を参照してください。
- vCenter Server の View Composer 設定が View Administrator で構成されていることを確認します。『View 管理ガイド』を参照してください。
- リモート デスクトップとして使用している仮想マシンに対して使用されている ESXi 仮想スイッチに十分な数のポートがあることを確認します。大規模なデスクトップ プールを作成する場合、デフォルト値では不十分なことがあります。ESXi ホスト上の仮想スイッチ ポートの数は、仮想マシンの数に、仮想マシンあたりの仮想 NIC の数をかけた数以上である必要があります。
- 親仮想マシンを準備したことを確認します。親仮想マシンで Horizon Agent がインストールされている必要があります。3 章 [クローン作成のための親仮想マシンの作成と準備](#)を参照してください。
- vCenter Server で親仮想マシンのスナップショットを作成します。スナップショットを作成する前に親仮想マシンをシャットダウンする必要があります。View Composer は、クローンを作成するための基本イメージとしてスナップショットを使用します。

注: 仮想マシン テンプレートからリンククローン プールを作成することはできません。

- プールを作成するために指定する必要がある構成情報を収集します。 [リンク クローン デスクトップ プールの作成用ワークシート](#)を参照してください。
- 電源設定、表示プロトコル、Adobe Flash 品質、およびその他の設定を構成する方法を決定します。 [すべてのデスクトップ プール タイプのデスクトップ プール設定](#)を参照してください。
- VMware Identity Manager からデスクトップとアプリケーションへのアクセスを提供しようとしている場合、View Administrator のルート アクセス グループで Administrators ロールを持つユーザーとしてデスクトップ プールとアプリケーション プールを作成していることを確認します。ルート アクセス グループ以外で Administrators ロールをユーザーに付与すると、VMware Identity Manager は、View で構成する SAML 認証システムを認識せず、VMware Identity Manager でプールを構成できません。

重要: リンク クローン プールが作成されている間、vCenter Server で親仮想マシンを変更しないでください。たとえば、親仮想マシンをテンプレートに変換しないでください。View Composer サービスでは、プールの作成中、親仮想マシンが静的な未変更の状態のままであることが必要です。

手順

- 1 View Administrator で、[カタログ] - [デスクトップ プール] を選択します。
- 2 [追加] をクリックします。
- 3 [自動化されたデスクトップ プール] を選択します。
- 4 [vCenter Server] ページで、[View Composer のリンク クローン] を選択します。
- 5 ウィザードの指示に従って、プールを作成します。

ワークシートで収集した構成情報を使用します。ナビゲーション パネルのページ名をクリックすると、完了したウィザード ページに直接戻ることができます。

[vCenter 設定] ページで、[参照] をクリックし、vCenter Server の設定を順番に選択する必要があります。vCenter Server の設定を省略することはできません。

- a 親仮想マシン
- b スナップショット
- c 仮想マシンのフォルダの場所
- d ホストまたはクラスター
- e リソース プール
- f データストア

View Administrator で、[カタログ] - [デスクトップ プール] を選択すると、プールに追加されているとおりにマシンを表示できます。

リンク クローンは、プロビジョニング中に 1 回以上再起動される場合があります。リンク クローンがエラー状態にある場合、View の自動リカバリ メカニズムはそのリンク クローンのパワーオン、またはシャットダウンと再起動を試みます。リカバリが繰り返し失敗すると、そのリンク クローンは削除されます。

View Composer は、リンク クローンのプロビジョニング用のマスタ イメージとして機能するレプリカ仮想マシンも作成します。領域の使用を少なくするために、レプリカはシン ディスクとして作成されます。すべての仮想マシンが再構成または削除され、レプリカにクローンが 1 つもリンクされていない場合、レプリカ仮想マシンは vCenter Server から削除されます。

別のデータストアにレプリカを格納しない場合は、View Composer によって、リンク クローンが作成される各データストアにレプリカが作成されます。

別のデータストアにレプリカを格納する場合は、リンク クローンが複数のデータストア上で作成されている場合でもプール全体に対して 1 つのレプリカが作成されます。

次のステップ

プールにアクセスするための資格をユーザーに付与します。[デスクトップまたはアプリケーション プールへの資格の追加](#)を参照してください。

自動デスクトップ プールのクローン作成

既存のプールから自動デスクトップ プールのクローンを作成できます。プールのクローンを作成する場合、既存のデスクトップ プールの設定が [デスクトップ プールを追加] ウィザードにコピーされるため、各設定を手動で入力することなく新しいプールを作成できます。

この機能を使用すれば、[デスクトップ プールを追加] ウィザードで各オプションを入力する必要がなくなるため、プールの作成を合理化できます。ウィザードの事前入力値を使用して、デスクトップ プール属性が標準化されていることを確認できます。

フル仮想マシンまたは View Composer リンク クローンを含む自動デスクトップ プールのクローンを作成できます。インスタント クローンの自動デスクトップ プール、手動デスクトップ プール、または RDS デスクトップ プールのクローンを作成することはできません。

デスクトップ プールのクローンを作成する場合、特定の設定は変更できません。

- デスクトップ プール タイプ
- クローン タイプ（リンク クローンまたはフル仮想マシン）
- ユーザー割り当て（専用または流動）
- vCenter Server インスタンス

前提条件

- 元のデスクトップ プールを作成するための前提条件がまだ有効であることを確認します。
たとえば、フル仮想マシンを含むプールの場合、仮想マシン テンプレートが準備されていることを確認します。
リンククローン プールの場合、親仮想マシンが準備されていて、仮想マシンのパワーオフ後にスナップショットが作成されていることを確認します。
プールのクローンを作成する場合、同じ仮想マシン テンプレートまたは親仮想マシンを使用することができますが、別の仮想マシン テンプレートまたは親仮想マシンを選択することもできます。
- 自動完全クローン プールのクローンを作成するための前提条件については、[フル仮想マシンを含む自動プールの作成](#)を参照してください。
- リンククローン プールのクローンを作成するための前提条件については、[リンククローン デスクトップ プールの作成](#)を参照してください。

手順

- 1 View Administrator で、[カタログ] - [デスクトップ プール] を選択します。
- 2 クローンを作成するデスクトップ プールを選択し、[クローン] をクリックします。
[デスクトップ プールを追加] ウィザードが表示されます。
- 3 [デスクトップ プールを追加] ページで、一意のプール ID を入力します。
- 4 [プロビジョニングの設定] ページで、仮想マシンの一意の名前を入力します。

オプション	説明
[名前付けパターンを使用]	仮想マシンの名前付けパターンを入力します。
[名前を手動で指定]	仮想マシンの一意の名前のリストを入力します。

- 5 ウィザードの他の指示に従って、プールを作成します。
必要に応じて、デスクトップ プールの設定および値を変更します。

View Administrator で、[カタログ] - [デスクトップ プール] を選択すると、プールに追加されているとおりにマシンを表示できます。

次のステップ

プールにアクセスするための資格をユーザーに付与します。[デスクトップまたはアプリケーション プールへの資格の追加](#)を参照してください。

リンク クローン デスクトップ プールのデスクトップ プール設定

View Composer によって作成されたリンク クローンを含む自動プールを構成するときに、マシンとデスクトップ プールの設定を指定する必要があります。専用ユーザー割り当てを使用するプールと流動ユーザー割り当てを使用するプールには、異なる設定が適用されます。

[表 5-2. 自動リンク クローン デスクトップ プールの設定](#) に、専用ユーザー割り当てを使用するリンク クローン プールおよび流動ユーザー割り当てを使用するリンク クローン プールに適用される設定を示します。

各設定の説明については、[すべてのデスクトップ プール タイプのデスクトップ プール設定](#)を参照してください。

表 5-2. 自動リンク クローン デスクトップ プールの設定

設定	リンク クローン プール、専用割り当て	リンク クローン プール、流動割り当て
状態	はい	はい
接続サーバ restrictions (接続サーバの制限)	はい	はい
リモート マシンの電源ポリシー	はい	はい
Automatically logoff after disconnect (切断後に自動的にログオフ)	はい	はい
ユーザーによるマシンのリセットを許可	はい	はい
ユーザーが複数のクライアント デバイスからセッションを個別に開始できるようにする		はい
ログオフ時にマシンを削除または更新		はい
Refresh OS disk after logoff (ログオフ後に OS ディスクを更新)	はい	
デフォルト表示プロトコル	はい	はい
ユーザーがプロトコルを選択できるようにする	はい	はい
3D レンダラー	はい	はい
Max number of monitors (モニタの最大数)	はい	はい
Max resolution of any one monitor (特定のモニタの最大解像度)	はい	はい
Adobe Flash quality (Adobe Flash の品質)	はい	はい
Adobe Flash throttling (Adobe Flash のスロットル)	はい	はい
Mirage 設定全体をオーバーライドする	はい	はい
Mirage サーバの構成	はい	はい

View Composer でのリンク クローンの SID およびサードパーティ アプリケーションのサポート

View Composer が、リンク クローン仮想マシンのローカル コンピュータ セキュリティ識別子 (SID) を生成および保持できる場合があります。サードパーティ アプリケーションが GUID を生成する方法によっては、View Composer はそのアプリケーションのグローバル意識別子 (GUID) を保持できます。

View Composer 操作が SID およびアプリケーション GUID にどのように影響するかを理解するには、リンク クローン マシンがどのように作成されてプロビジョニングされるかを理解する必要があります。

- 1 View Composer は、次の処理を行うことによってリンク クローンを作成します。
 - a 親仮想マシンのスナップショットを複製することによってレプリカを作成します。
 - b そのレプリカを親ディスクとして参照するリンク クローンを作成します。
- 2 View Composer および View は、プールの作成時に選択したカスタマイズ ツールに従って、QuickPrep または Sysprep カスタマイズ仕様によってリンク クローンをカスタマイズします。
 - Sysprep を使用する場合は、クローンごとに一意の SID が生成されます。
 - QuickPrep を使用する場合、新しい SID は生成されません。親仮想マシンの SID は、プール内のすべてのプロビジョニングされたリンク クローン マシンで複製されます。
 - 一部のアプリケーションは、カスタマイズ時に GUID を生成します。
- 3 View は、リンク クローンのスナップショットを作成します。

スナップショットには、Sysprep で生成された一意の SID または QuickPrep で生成された共通 SID が含まれます。
- 4 View は、プールの作成時に選択した設定に従ってマシンをパワーオンします。

一部のアプリケーションは、マシンが初めてパワーオンされたときに GUID を生成します。

QuickPrep によるカスタマイズと Sysprep によるカスタマイズの比較については、[リンク クローン マシンをカスタマイズするための QuickPrep または Sysprep の選択](#)を参照してください。

リンク クローンを更新すると、View Composer はスナップショットを使用してクローンを初期状態に戻します。SID は保持されます。

リンク クローンを再構成するときに QuickPrep を使用した場合は、再構成操作で同じ親仮想マシンを選択していれば、親仮想マシンの SID がそのリンク クローン上に保持されます。再構成で別の親仮想マシンを選択した場合は、新しい親の SID がクローンで複製されます。

Sysprep を使用する場合は、クローンで新しい SID が常に生成されます。詳細については、[Sysprep でカスタマイズしたリンク クローンの再構成](#)を参照してください。

表 5-3. View Composer の操作、リンク クローン SID、およびアプリケーション GUID に、View Composer の操作がリンク クローンの SID およびサードパーティ アプリケーションの GUID に与える影響を示します。

表 5-3. View Composer の操作、リンク クローン SID、およびアプリケーション GUID

SID または GUID のサポート	クローン作成	更新	再構成
Sysprep: リンク クローンの一意の SID	Sysprep カスタマイズでは、リンク クローンに対して一意の SID が生成されます。	一意の SID は保持されます。	一意の SID は保持されません。
QuickPrep: リンク クローンの共通 SID	QuickPrep カスタマイズでは、プール内のすべてのクローンに対して共通 SID が生成されます。	共通 SID は保持されます。	共通 SID は保持されます。
サードパーティ アプリケーションの GUID	アプリケーションごとに動作が異なります。 注: GUID の保持については、Sysprep と QuickPrep で結果に違いはありません。	アプリケーションが初期スナップショットが作成される前に GUID を生成する場合、GUID は保持されます。 アプリケーションが初期スナップショットが作成された後で GUID を生成する場合、GUID は保持されません。	アプリケーションが View Composer の通常ディスクとして指定されたドライブに GUID を書き込む場合を除き、再構成操作ではアプリケーション GUID は保持されません。

リンク クローン マシンをカスタマイズするための QuickPrep または Sysprep の選択

QuickPrep および Microsoft Sysprep では、リンク クローン マシンをカスタマイズするためのさまざまな方法を提供します。QuickPrep は、View Composer と効率的に連携するように設計されています。Microsoft Sysprep は、標準のカスタマイズ ツールを提供します。

リンク クローン マシンを作成する際は、仮想マシンがネットワーク上の一意のコンピュータとして機能できるように各仮想マシンを変更する必要があります。View と View Composer では、リンク クローン マシンを個人用に設定する方法が 2 つあります。

表 5-4. [QuickPrep と Microsoft Sysprep の比較](#)では、QuickPrep と、Microsoft Sysprep で作成されたカスタマイズ仕様を比較しています。

表 5-4. QuickPrep と Microsoft Sysprep の比較

QuickPrep	カスタマイズ仕様 (Sysprep)
View Composer と連携するように設計されています。 詳細については、 QuickPrep でのリンク クローン マシンのカスタマイズ を参照してください。	標準の Microsoft Sysprep ツールを使って作成できます。
プール内のすべてのリンク クローンに対して同じローカル コンピュータ セキュリティ識別子 (SID) を使用します。	プール内の各リンク クローンに対して一意のローカル コンピュータ SID を生成します。
リンク クローンのパワーオフ前、およびリンク クローンの作成、更新、または再構成後に、追加のカスタマイズ スクリプトを実行できます。	ユーザーが初めてログインしたときに追加スクリプトを実行できます。
リンク クローン コンピュータを Active Directory ドメインに参加させます。	リンク クローン コンピュータを Active Directory ドメインに参加させます。 Sysprep カスタマイズ仕様に含まれるドメインと管理者の情報は使用されません。仮想マシンは、プールの作成時に View Administrator で入力するゲストのカスタマイズ情報を使ってドメインに結合されます。

QuickPrep	カスタマイズ仕様 (Sysprep)
各リンク クローンで、一意の ID を Active Directory ドメイン アカウントに追加します。	各リンク クローンで、一意の ID を Active Directory ドメイン アカウントに追加します。
リンク クローンの更新後に新しい SID を生成しません。共通 SID が保持されます。	各リンク クローンがカスタマイズされたときに新しい SID を生成します。更新操作中は一意の SID を保持しますが、再構成または再分散操作中は保持しません。
リンク クローンの再構成後に新しい SID を生成しません。共通 SID が保持されます。	リンク クローンの再構成後に再度実行し、仮想マシンの新しい SID を生成します。 詳細については、 Sysprep でカスタマイズしたリンク クローンの再構成 を参照してください。
Sysprep より迅速に動作します。	QuickPrep よりも時間がかかることがあります。

QuickPrep または Sysprep でリンク クローン プールをカスタマイズした後、そのプール内のマシンを作成または再構成する際に別のカスタマイズ方法に切り替えることはできません。

QuickPrep でのリンク クローン マシンのカスタマイズ

QuickPrep システム ツールを使用して、親仮想マシンから作成されたリンク クローン マシンを個人用に設定できます。View Composer は、リンク クローン マシンが作成または再構成される際に QuickPrep を実行します。

QuickPrep は、次のいくつかの方法でリンク クローン マシンをカスタマイズします。

- コンピュータに、リンク クローン プールを作成するときに指定した名前を付けます。
- Active Directory 内にコンピュータ アカウントを作成し、そのコンピュータを適切なドメインに参加させます。
- View Composer の通常ディスクをマウントします。Windows ユーザー プロファイルはこのディスクにリダイレクトされます。
- 一時ファイルとページング ファイルを別のディスクにリダイレクトします。

これらの手順では、リンク クローンを 1 回以上再起動しなければならない場合があります。

QuickPrep は KMS ボリューム ライセンス キーを使用して、Windows リンククローン マシンをアクティベーションします。詳細については、『View 管理ガイド』を参照してください。

リンク クローンをさらにカスタマイズする独自のスクリプトを作成できます。QuickPrep は、あらかじめ定義されたタイミングで 2 種類のスクリプトを実行できます。

- リンク クローンが作成または再構成された後
- リンク クローンがパワーオフされる直前

QuickPrep のカスタマイズ スクリプトの使用に関するガイドラインおよびルールについては、[QuickPrep カスタマイズ スクリプトの実行](#)を参照してください。

注: リンク クローン マシンを Active Directory ドメインに参加させるには、View Composer でドメインのユーザー 一認証情報が必要です。詳細については、『View 管理ガイド』を参照してください。

QuickPrep カスタマイズ スクリプトの実行

QuickPrep ツールでは、プール内のリンク クローン マシンをカスタマイズするためのスクリプトを作成できます。2 つの事前に定義されたタイミングにカスタマイズ スクリプトを実行するように QuickPrep を構成できます。

QuickPrep スクリプトが実行される時期

同期後スクリプトは、リンク クローンが作成、再構成、または再分散され、そのクローンのステータスが [動作可能] になった後に実行されます。パワーオフ スクリプトは、リンク クローンがパワーオフされる前に実行されます。これらのスクリプトは、リンク クローンのゲスト OS で実行されます。

QuickPrep でのスクリプトの実行方法

QuickPrep プロセスは、Windows の CreateProcess API 呼び出しを使用してスクリプトを実行します。スクリプトは、CreateProcess API で作成できる任意のプロセスを呼び出すことができます。たとえば、cmd、vbscript、exe、およびバッチ ファイル プロセスは、この API で動作します。

特に QuickPrep は、スクリプトに指定されたパスを 2 番目のパラメータとして CreateProcess API に渡し、最初のパラメータを NULL に設定します。

たとえば、スクリプト パスが C:¥.cmd である場合、このパスは次のように View Composer ログ ファイル内の関数では 2 番目のパラメータとして表示されます。CreateProcess(NULL,c:¥.cmd,...)

QuickPrep スクリプトへのパスの指定

リンク クローン マシン プールを作成する場合や、プールのゲストのカスタマイズ設定を編集する場合は、QuickPrep カスタマイズスクリプトのパスを指定します。スクリプトは、親仮想マシンに配置する必要があります。ネットワーク共有の UNC パスは使用できません。

スクリプトの実行にインタープリタが必要なスクリプト言語を使用する場合は、スクリプト パスをインタープリタのバイナリで始める必要があります。

たとえば、QuickPrep カスタマイズ スクリプトとして C:¥¥.vbs を指定した場合、View Composer Agent はスクリプトを実行できません。次のように、インタープリタのバイナリ パスで始まるパスを指定する必要があります。

```
C:\windows\system32\cscript.exe c:\script\myvb.vbs
```

重要: 通常のユーザーがアクセスできないように QuickPrep カスタマイズ スクリプトを保護します。スクリプトを安全なフォルダに配置します。

QuickPrep スクリプトのタイムアウト制限

View Composer は、20 秒を経過した同期後スクリプトまたはパワーオフ スクリプトを終了します。スクリプトが 20 秒より長くかかる場合は、タイムアウトの上限を引き上げることができます。詳細については、[ClonePrep および QuickPrep カスタマイズ スクリプトのタイムアウト制限の引き上げ](#)を参照してください。

または、スクリプトを使用して、長時間タスクを実行する別のスクリプトまたはプロセスを起動できます。

QuickPrep スクリプトのアカウント

QuickPrep は、VMware View Composer Guest Agent Server サービスの実行が構成されたアカウントでスクリプトを実行します。デフォルトでは、このアカウントはローカル システムです。

このログオン アカウントは変更しないでください。変更すると、リンク クローンが起動しなくなります。

QuickPrep プロセス権限

セキュリティ上の理由から、一部の Windows OS 権限は、QuickPrep カスタマイズ スクリプトを起動する View Composer Guest Agent プロセスから削除されます。

QuickPrep カスタマイズ スクリプトは、View Composer Guest Agent プロセスから削除される権限を必要とする操作は実行できません。

次の権限は、QuickPrep スクリプトを起動するプロセスから削除されます。

```
SeCreateTokenPrivilege
SeTakeOwnershipPrivilege
SeSecurityPrivilege
SeSystemEnvironmentPrivilege
SeLoadDriverPrivilege
SeSystemtimePrivilege
SeUndockPrivilege
SeManageVolumePrivilege
SeLockMemoryPrivilege
SeIncreaseBasePriorityPrivilege
SeCreatePermanentPrivilege
SeDebugPrivilege
SeAuditPrivilege
```

QuickPrep スクリプトのログ

View Composer ログには、QuickPrep スクリプトの実行に関する情報が含まれています。このログには、実行の開始と終了や、出力またはエラー メッセージが記録されます。このログは、次の Windows の temp ディレクトリ内にあります。

C:\Windows\Temp\vmware-viewcomposer-ga-new.log

Sysprep でカスタマイズしたリンク クローンの再構成

Sysprep でカスタマイズしたリンク クローン マシンを再構成すると、View は、OS ディスクが再構成された後で Sysprep カスタマイズ仕様を再度実行します。この操作により、リンク クローン仮想マシンの新しい SID が生成されます。

新しい SID が生成されると、再構成されたリンク クローンはネットワーク上で新しいコンピュータとして機能します。システム管理ツールなどのソフトウェア プログラムは、管理対象のコンピュータを識別するために SID を使用します。これらのプログラムが、リンク クローン仮想マシンを識別または検索できない場合があります。

また、サードパーティ ソフトウェアがシステム ディスクにインストールされている場合、カスタマイズ仕様によって、再構成後にそのソフトウェアの GUID が再生成されることがあります。

再構成により、リンク クローンが元の状態（カスタマイズ仕様が初めて実行される前の状態）に戻ります。この状態のリンク クローンには、ローカル コンピュータの SID またはシステム ドライブにインストールされているサードパーティ ソフトウェアの GUID がありません。View は、リンク クローンが再構成された後で Sysprep カスタマイズ仕様を実行する必要があります。

View Composer の操作時に、リモート デスクトップ セッションで使用するようにプロビジョニングされたリンククローン マシンを維持する

ユーザーが常にリモート デスクトップにアクセスできる必要がある場合、View Composer のメンテナンス操作が行われている間でも、リモート デスクトップ セッションで使用できるようにプロビジョニングされた一定数のマシンを維持する必要があります。View Composer が、プールにあるリンククローン仮想マシンを更新、再構成、または再調整するときに、メンテナンス モードに入らないマシンの最小数を設定できます。

[View Composer のメンテナンス操作中における（プロビジョニング済み）動作可能マシンの最小数] を設定すると、View Composer がメンテナンス操作を続行する間も、指定された数のマシンが View によってプロビジョニングされたままになり、メンテナンス モードに入らなくなります。

この設定を使用すると、View Composer のメンテナンス操作時に、ユーザーは既存の接続を維持したり、新しい接続要求を作成したりできます。この設定では、新しい接続の受け入れ準備ができていないスベア マシンと既存のデスクトップ セッションですでに接続されているマシンは区別されません。

リンククローン プールを作成または編集するときに、この設定を指定できます。

以下のガイドラインがこの設定に適用されます。

- 多くのユーザーが既存のデスクトップ接続を維持できるようにし、新しい接続要求を受け入れることができるスベアの（パワーオン状態の）マシンの数を最小限にするには、[View Composer のメンテナンス操作中における（プロビジョニング済み）動作可能マシンの最小数] に、両方のマシンのセットが含まれるように、十分に大きな値を設定します。
- マシンのプロビジョニングに名前付けパターンを使用し、オン デマンドでマシンをプロビジョニングする場合、View Composer 操作時にプロビジョニングされるマシンの数は指定された [マシンの最大数] よりも小さい値に設定してください。最大数がこれよりも小さければ、プールの合計マシン数が、最終的に View Composer の操作中にプロビジョニングされた状態のままにする最小数よりも小さくなる場合があります。この場合、View Composer のメンテナンス操作が行われない可能性があります。
- 手動でマシン名のリストを指定することでマシンをプロビジョニングする場合、（マシン名を削除して）合計のプール サイズをプロビジョニングされるマシンの最小数より小さい数字まで減らさないでください。この場合、View Composer のメンテナンス操作が行われない可能性があります。
- プロビジョニングされるマシンの最小数をプール サイズに対して相対的に大きく設定すると、View Composer のメンテナンス操作が完了するまで時間がかかる場合があります。View はメンテナンス操作中にプロビジョニングされるマシンの最小数を維持しますが、操作では [最大同時 View Composer メンテナンス操作数] 設定で指定した同時制限に達しない場合があります。

たとえば、プールに 20 台のマシンが含まれていて、プロビジョニングされるマシンの最小数が 15 の場合、View Composer は最大でも同時に 5 台のマシンでしか稼動できません。同時 View Composer メンテナンス操作数の制限が 12 の場合、同時制限に達することはありません。

- この設定名では、「作動可能」という言葉は、リンククローン仮想マシンの状態に適用されるものであり、View Administrator に表示されるマシンのステータスに適用されるものではありません。仮想マシンは、プロビジョニングされてパワーオンされる準備ができていれば作動可能です。マシンのステータスは、マシンの View 管理対象状態を反映します。たとえば、マシンは 接続済み、切断されました、エージェントに到達できません、削除中などのステータスになる場合がありますが、「作動可能」と見なされます。

リンク クローンに既存の Active Directory コンピュータ アカウントを使用する

デスクトップ プールや自動ファームを作成または編集するとき、新しくプロビジョニングされたリンク クローンに Active Directory の既存のコンピュータ アカウントを使用するように View Composer を構成できます。

デフォルトでは、View Composer はプロビジョニングしたリンク クローンごとに新しい Active Directory コンピュータ アカウントを生成します。[既存のコンピュータ アカウントの再利用を許可] オプションでは、View Composer が既存の AD コンピュータ アカウントを使用できるようにすることで、Active Directory で作成されたコンピュータ アカウントを管理できます。

このオプションを有効にすると、リンク クローンがプロビジョニングされたときに、View Composer は、既存の AD コンピュータ アカウント名がリンク クローン マシン名と一致するかどうかを確認します。一致していれば、View Composer は既存の AD コンピュータ アカウントを使用します。View Composer は、一致する AD コンピュータ アカウント名を検出できない場合は、リンク クローン用の新しい AD コンピュータ アカウントを生成します。

デスクトップ プールや自動ファームを作成または編集するときに、[既存のコンピュータ アカウントの再利用を許可] オプションを設定できます。プールまたはファームを編集してこのオプションを設定した場合、この設定は、今後プロビジョニングされるリンククローン マシンに影響を与えます。すでにプロビジョニングされているリンク クローンには影響しません。

[既存のコンピュータ アカウントの再利用を許可] オプションを設定すると、デスクトップ プールまたはファームを生成する View Composer ユーザー アカウントに割り当てられる Active Directory の権限を制限できます。必要なのは次の Active Directory の権限のみです。

- 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

プロビジョニングを行うすべてのマシンに、Active Directory で既存のコンピュータ アカウントが割り当てられている場合、Active Directory 権限のみを制限できます。一致する名前が見つからなければ、View Composer は、新しい AD コンピュータ アカウントを生成します。コンピュータ オブジェクトの作成などの追加権限は、新しいコンピュータ アカウント作成するために必要です。View Composer ユーザー アカウントに必要な権限の完全なリストについては、『View 管理ガイド』を参照してください。

View Composer が現在、既存の AD コンピュータ アカウントを 1 つ以上使用している場合は、このオプションは無効にできません。

次の手順は、リンククローン デスクトップ プールに適用されます。手順は、自動ファームの場合と同様です。

前提条件

既存のコンピュータ アカウントが、[Active Directory コンテナ] 設定で指定する Active Directory コンテナに配置されていることを確認します。既存のアカウントが別のコンテナに配置されている場合、それらのアカウント名のリンク クローンではプロビジョニングは失敗し、Active Directory に既存のコンピュータ アカウントが既に存在するというエラー メッセージが表示されます。

たとえば、[既存のコンピュータ アカウントの再利用を許可] オプションを選択し、[Active Directory コンテナ] がデフォルト値 **CN=Computers** であることを指定し、既存のコンピュータ アカウントが **OU=mydesktops** に配置されると、プロビジョニングはそれらのアカウントで失敗します。

手順

- 1 Active Directory で、リンククローン マシンに使用するコンピュータ アカウントを作成します。

例: machine1, machine2, machine3

View でマシンのプロビジョニング時に生成される名前と一致するように、コンピュータ アカウント名には連続した整数を使用する必要があります。

- 2 View Administrator で、[デスクトップ プールを追加] ウィザードを使用してプールを作成するか、[編集] ダイアログ ボックスでプールを編集します。
- 3 [プロビジョニングの設定] ページまたはタブで、[名前付けパターンを使用] を選択します。
- 4 [名前付けパターン] テキスト ボックスに、Active Directory コンピュータ アカウント名と一致するマシン名を入力します。

例: machine

View は一意の番号をパターンに付加し、各マシンに固有の名前を付けます。

例: machine1, machine2, machine3

- 5 [ゲストのカスタマイズ] ページまたはタブで、[既存のコンピュータ アカウントの再利用を許可] オプションを選択します。

インスタントクローン デスクトップ プールの作成

ユーザーがインスタントクローン デスクトップにアクセスするには、インスタントクローン デスクトップ プールを作成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。

- [インスタントクローン デスクトップ プール](#)
- [インスタントクローン デスクトップ プールのイメージの公開および再調整](#)
- [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 プールの作成用ワークシート](#)
- [インスタントクローン デスクトップ プールの作成](#)
- [ClonePrep でのゲストのカスタマイズ](#)
- [インスタントクローン メンテナンス ユーティリティ](#)

インスタントクローン デスクトップ プール

インスタントクローン デスクトップ プールは、自動デスクトップ プールです。vCenter Server は、ユーザーがプール作成時に指定した設定に基づいて、デスクトップ仮想マシンを作成します。

インスタント クローンは、View Composer がリンクされたクローンと同様に親仮想マシンの仮想ディスクを共有するので、フル仮想マシンに比べてストレージの使用量が少なくなります。さらに、インスタント クローンは親仮想マシンのメモリも共有します。インスタント クローンは vmFork テクノロジーを使用して作成されます。インスタントクローン デスクトップ プールは、次のような主要な特徴があります。

- インスタント クローンのプロビジョニングは View Composer リンク クローンに比べて大幅に高速で実行されます。
- インスタント クローンは常にパワーオン状態で作成され、ユーザーが接続できる準備が整っています。ゲストのカスタマイズや Active Directory ドメインへの参加は、最初のパワーオンのワークフローの一部として完了します。
- ユーザーがログアウトするとき、デスクトップ仮想マシンが削除されます。オンデマンドまたは事前の新規クローン作成は、プロビジョニング ポリシーに従って行われます。
- プッシュイメージ操作により、親仮想マシンのスナップショットからプールを再作成できます。プッシュ イメージを使用して、オペレーティング システム およびアプリケーション パッチをロールアウトできます。

- クローンが作成されると、View はデータストアを選択して、データストア全体に最良のクローンを送信します。手動の再調整は必要ありません。
- View Storage Accelerator は自動的に有効になります。
- 透過的なページ共有は自動的に有効になっています。

View はインスタント クローンを素早く作成できるので、事前にデスクトップをプロビジョニングしたり、多くの準備の整ったデスクトップは必要はありません。View Composer がリンクされたクローンと比べて、インスタント クローンでは大規模なデスクトップの管理タスクが簡単になり、必要とされるハードウェア リソースを低減できます。

インスタント クローンには、次の互換性の要件があります。

- vSphere 6.0 Update 1 以降。
- 仮想マシン ハードウェア バージョン 11 以降。

ベスト プラクティスとして、vSphere 環境で分散仮想スイッチを構成します。

Horizon 7.0 では、インスタント クローンに次の制限があります。

- シングルユーザー デスクトップだけがサポートされます。RDS ホストはサポートされません。
- フローティング ユーザー割り当てだけがサポートされます。ユーザーは、プールからのデスクトップにランダムに割り当てられます。
- インスタントクローン デスクトップは通常ディスクを使用できません。ユーザーは、通常データを格納するために VMware App Volumes を使用できます。App Volumes の詳細については、<https://www.vmware.com/products/appvolumes> を参照してください。
- Virtual Volumes と VAAI (vStorage APIs for Array Integration) のネイティブ NFS スナップショットはサポートされません。
- デスクトップのカスタマイズでは Sysprep を使用できません。
- Windows 7 および Windows 10 ではサポートされますが、Windows 8 または Windows 8.1 ではサポートされません。
- PowerCLI はサポートされません。
- ローカル データストアはサポートされません。
- IPv6 はサポートされません。
- インスタント クローンは、Active Directory に存在するコンピュータ アカウントを再利用できません。
- 個人設定管理は使用できません。
- 3D レンダリングは使用できません。
- インスタントクローンのメンテナンス操作中は、準備（プロビジョニング）ができていないマシンの最低台数を指定できません。インスタント クローンは高速で作成され、メンテナンス操作中に一部のデスクトップがすでに使用可能になるため、この機能は必要ありません。

ユーザーがログアウトするとインスタント クローンが再作成されるので、View Composer がリンクされたクローンに利用できるディスク スペース再利用機能は必要ありません。インスタント クローンでは、仮想マシンの未使用のディスク スペースの再利用は、ストレージの使用量にあまり影響しません。

インスタントクローン デスクトップ プールのイメージの公開および再調整

インスタントクローン デスクトップ プールのクローンは、同じイメージを基準にしています。インスタント クローンが作成されるとき、デスクトップ プールは、データストア全体へ自動的に再調整されます。

イメージは、親仮想マシンのスナップショットです。インスタントクローン デスクトップ プールの作成には、次の操作が伴います。

- 1 View は、選択するイメージを公開します。vCenter Server では、4 つのフォルダ (ClonePrepInternalTemplateFolder、ClonePrepParentVmFolder、ClonePrepReplicaVmFolder、および ClonePrepResyncVmFolder) が作成され (存在しない場合)、またクローン作成に必要とされるいくつかの内部仮想マシンが作成されます。View Administrator では、デスクトップ プールの [サマリ] タブでこの処理の進捗状況を確認できます。公開中、保留しているイメージ ペインには、イメージの名前や状態が表示されます。

注: 4 つのフォルダ、またはフォルダに含まれる内部仮想マシンを変更しないでください。変更するとエラーが発生することがあります。内部仮想マシンは、必要がなくなると削除されます。通常、プールの削除またはプッシュイメージ操作を実行した後、これらの仮想マシンは 5 分以内に削除されます。ただし、場合によっては削除されるまでに最長 30 分かかることがあります。

- 2 クローンが作成されます。このプロセスは高速で実行されます。通常、クローンは 2 秒以内に作成されます。このプロセス中、View Administrator の現在のイメージ ペインには、イメージの名前や状態が表示されます。

プールが作成された後は、プッシュイメージ操作によりイメージを変更できます。『View 管理』の「インスタントクローン デスクトップ プールのイメージの変更」を参照してください。プールの作成と同様に、新しいイメージは最初に公開されます。次にクローンが再作成されます。

プールを編集してデータストアを追加したり削除したりする場合、新しいクローンが作成されるとき、仮想マシンの再調整を自動的に実行します。より高速に再分散を実行するには、次の操作を実行します。

- データストアを削除する場合は、そのデータストア上のデスクトップを手動で削除します。これにより、新しいデスクトップが残りのデータストアで作成されます。
- データストアを追加する場合は、元のデータストアから一部のデスクトップを手動で削除します。これにより、新しいデスクトップが新しいデータストアで作成されます。また、すべてのデスクトップを削除したり、または単に同じイメージを使用してプッシュ イメージを実行できます。これにより、クローンが再作成されるときに、データストア全体で均等にデスクトップが分散されます。

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 View 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。詳細については、『View のインストール』の「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。

手順

- 1 View Administrator で、[View 構成] - [インスタント クローンのドメイン管理者] を選択します。
- 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。

インスタントクローン デスクトップ プールの作成用ワークシート

インスタントクローン デスクトップ プールを作成する際、[デスクトップ プールを追加] ウィザードで特定のオプションを構成するよう求められます。このワークシートを使用して、プールを作成する前に構成オプションを記録します。

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、親仮想マシンのスナップショットを取得します。スナップショットを取得する前に、親仮想マシンをシャットダウンする必要があります。このスナップショットは、クローンの基本イメージとなります。

注: 仮想マシン テンプレートからインスタントクローン デスクトップ プールを作成することはできません。

表 6-1. ワークシート：インスタントクローン デスクトップ プールを作成するための構成オプション

オプション	説明	値をここに記入
ユーザー割り当て	[流動] を選択します。ユーザーは、プールからのデスクトップにランダムに割り当てられます。	
vCenter Server	[インスタントクローン] を選択し、インスタント クローン 仮想マシンを管理する vCenter Server を選択します。	
デスクトップ プール ID	View Administrator でプールを識別する一意の名前。 複数の接続サーバ構成が存在する場合、同じプール ID を使用する接続サーバ構成が存在していないことを確認します。接続サーバ構成は、1 台の接続サーバ、または複数の接続サーバによる構成が可能です。	
表示名	クライアントからログインするときにユーザーに表示されるプール名。名前を指定しない場合、プール ID が使用されます。	
アクセス グループ	プールに対するアクセス グループを選択するか、プールをデフォルトのルート アクセス グループに残します。 アクセス グループを使用する場合は、プールの管理を特定のロールを持つ管理者に委任できます。詳細については、『View 管理』のロール ベースの委任管理についての章を参照してください。 注: アクセス グループは、デスクトップ 仮想マシンを格納する vCenter Server フォルダとは異なります。ウィザードで vCenter Server フォルダを後で選択します。	
状態	[有効] に設定されている場合、プロビジョニング後にプールを使用する準備が整っています。 [無効] に設定されている場合、ユーザーはプールを使用できません。プロビジョニング中にプールを無効にすると、プロビジョニングは停止します。	

オプション	説明	値をここに記入
接続サーバの制限	<p>プールへのアクセスを特定の接続サーバに制限するには、[参照] をクリックして、1 台以上の接続サーバを選択します。</p> <p>VMware Identity Manager からデスクトップへのアクセスを提供することを意図して接続サーバ制限を構成すると、これらのデスクトップが実際には制限されている場合でも VMware Identity Manager アプリケーションでユーザーにデスクトップが表示されることがあります。VMware Identity Manager ユーザーはこれらのデスクトップを起動できません。</p>	
切断後に自動的にログオフ	<ul style="list-style-type: none"> ■ [直後] : ユーザーは切断時にログアウトします。 ■ [なし] : ユーザーはログオフされません。 ■ [時間が経過した後] : ユーザーが接続を切断してからこの時間が経過すると、ログオフされます。時間は分単位で入力します。 <p>ログオフ時間は今後の切断時に適用されます。ログオフ時間を設定したときにデスクトップ セッションがすでに切断されている場合、そのユーザーのログオフ経過時間が開始するのは、ログオフ時間を設定した時点となり、セッションが最初に切断された時点ではありません。たとえば、この値を 5 分に設定した場合に、セッションが 10 分前に切断されたとすると、そのセッションは値を設定してから 5 分後に View でログオフされます。</p>	
ユーザーが複数のクライアント デバイスからセッションを個別に開始できるようにする	このオプションが選択されている場合、複数のクライアント デバイスから同じデスクトップ プールに接続しているユーザーは複数のデスクトップ セッションを取得します。ユーザーは同じクライアント デバイスからのみ既存のセッションに再接続できます。この設定が選択されていない場合、使用されるクライアント デバイスに関係なく、ユーザーは常時、既存のセッションと再接続されます。	
デフォルト表示プロトコル	デフォルトの表示プロトコルを選択します。選択肢は [Microsoft RDP]、[PCoIP]、および [VMware Blast] です。	
ユーザーがプロトコルを選択できるようにする	ユーザーがデフォルト以外の表示プロトコルを選択できるかどうかを指定します。	
HTML Access	<p>ユーザーに自分の Web ブラウザからリモート デスクトップに接続することを許可するには、[有効] を選択します。この機能の詳細については、『HTML Access の 使用』(https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html から利用可能) を参照してください。</p> <p>VMware Identity Manager で HTML Access を使用するには、『View 管理 管理ガイド』の説明に従って接続サーバを SAML 認証サーバとペアにする必要があります。VMware Identity Manager をインストールして、接続サーバで使用するために構成する必要があります。</p>	
Adobe Flash quality (Adobe Flash の品質)	<p>Web ページで Adobe フラッシュ コンテンツの品質を選択します。</p> <ul style="list-style-type: none"> ■ [制御しない] : Web ページの設定により品質が決定されます。 ■ [低] : この設定は、最小限の帯域幅を使用します。品質レベルが指定されない場合、これがデフォルト レベルです。 ■ [中] : この設定は、中程度の帯域幅を使用します。 ■ [高] : この設定は、最大限の帯域幅を使用します。 <p>詳細については、Adobe Flash の品質とスロットル を参照してください。</p>	

オプション	説明	値をここに記入
Adobe Flash throttling (Adobe Flash のスロットル)	<p>Adobe Flash ムービーのフレーム レートを選択します。この設定を有効にすると、スロットル レベルを選択することによって、1 秒あたりに表示されるフレームの数を増やしたり減らしたりできます。</p> <ul style="list-style-type: none"> ■ [無効化]: スロットルは行われません。 ■ [低]: タイマー間隔は 100 ミリ秒です。この設定では、抜けるフレームの数が最も少なくなります。 ■ [中]: タイマー間隔は 500 ミリ秒です。 ■ [高]: タイマー間隔は 2,500 ミリ秒です。この設定では、抜けるフレームの数が最も多くなります。 <p>詳細については、Adobe Flash の品質とスロットル を参照してください。</p>	
エラーによりプロビジョニングを停止	エラーが発生した際に View でデスクトップ仮想マシンのプロビジョニングを停止し、そのエラーが複数の仮想マシンに影響が及ばないようにするかどうかを指定します。	
Naming pattern (名前付けパターン)	<p>すべてのデスクトップ仮想マシン名のプレフィックス（その後に一意の数字が続く）として View で使用するパターンを指定します。</p> <p>詳細については、自動デスクトップ プールでの名前付けパターンの使用を参照してください。</p>	
マシンの最大数	プール内のデスクトップ仮想マシンの総数を指定します。	
スベアの（パワーオン状態の）マシンの数	ユーザーから利用可能な状態を保つデスクトップ仮想マシンの数を指定します。詳細については、以下を参照してください。 マシンの手動での名前付けまたは名前付けパターンの指定 。	
オンデマンドでマシンをプロビジョニング マシンの最小数 全マシンを事前にプロビジョニング	<p>プールの作成時にすべてのデスクトップ仮想マシンをプロビジョニングするか、または必要に応じて仮想マシンをプロビジョニングするかどうかを指定します。</p> <ul style="list-style-type: none"> ■ [全マシンを事前にプロビジョニング]。プールが作成されると、View は [マシンの最大数] で指定した数の仮想マシンをプロビジョニングします。 ■ [オンデマンドでマシンをプロビジョニング]。プールが作成されると、View は [マシンの最小数] の値または [スベアの（パワーオン状態の）マシンの数] の値（いずれか大きい方）に基づく台数の仮想マシンを作成します。ユーザーがデスクトップに接続すると、この利用可能な仮想マシンの最小台数を維持するために、追加の仮想マシンが作成されます。 	
レプリカおよび OS ディスク用に別のデータストアを選択します	<p>インスタント クローンのデータストアとは異なるデータストアにレプリカおよび OS ディスクを格納するかどうかを指定します。</p> <p>詳細については、インスタント クローンおよび View Composer リンク クローン用の別のデータストアへのレプリカおよびクローンの格納を参照してください。</p>	
親仮想マシン	プールの親仮想マシンを選択します。	
スナップショット（デフォルト イメージ）	プールの基本イメージとして使用する親仮想マシンのスナップショットを選択します。	
仮想マシンのフォルダの場所	デスクトップ仮想マシン用の vCenter Server のフォルダを選択します。	
クラスタ	デスクトップ仮想マシン用の vCenter Server クラスタを選択します。	
Resource pool (リソース プール)	デスクトップ仮想マシン用の vCenter Server リソース プールを選択します。	
データストア	<p>デスクトップ仮想マシン用の 1 つ以上のデータストアを選択します。</p> <p>[インスタント クローンのデータストアを選択] ウィンドウは、プールのストレージ要件を評価するためのハイレベルなガイドラインを提供します。これらのガイドラインは、クローンを格納するための十分な大きさがあるデータストアを特定するのに役立ちます。[ストレージ オーバーコミット] の値は常時 [境界なし] に設定され、構成できません。</p>	

オプション	説明	値をここに記入
ドメイン	Active Directory ドメインを選択します。ドロップダウン リストには、インスタントクローン ドメイン管理者を構成したときに指定したドメインが表示されます。 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。	
AD コンテナ	Active Directory コンテナの相対識別名を指定します。 例：CN=Computers [デスクトップ プールを追加] ウィンドウで、コンテナの Active Directory ツリーを参照できます。	
Power-off script（パワーオフ スクリプト）	仮想マシンのパワーオフ前にデスクトップ仮想マシンで実行するスクリプトのパス名とスクリプト パラメータを指定します。	
同期後スクリプト	仮想マシンの作成後にデスクトップ仮想マシンで実行するスクリプトのパス名とスクリプト パラメータを指定します。	

インスタントクローン デスクトップ プールの作成

[[デスクトップ プールを追加]] ウィザードを使用すると、手順に従ってインスタントクローン デスクトップ プールを作成できます。

前提条件

- インスタントクローン仮想マシンが接続する仮想スイッチには、予想された仮想マシン数をサポートする十分なポートがあることを確認してください。仮想マシンの各ネットワーク カードには 1 つのポートが必要です。
- 親仮想マシンの準備ができていることを確認します。詳細については、[3 章 クローン作成のための親仮想マシンの作成と準備](#)を参照してください。
- プールの構成情報を収集します。[インスタントクローン デスクトップ プールの作成用ワークシート](#)を参照してください。
- View Administrator にインスタントクローンのドメイン管理者を追加したことを確認します。[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 View Administrator で、[カタログ] - [デスクトップ プール] を選択します。
- 2 [追加] をクリックします。
- 3 [自動化されたデスクトップ プール] を選択します。
- 4 [[vCenter Server]] ページで、[インスタント クローン] を選択します。
- 5 プロンプトに従って、プールを作成します。

ワークシートで収集した構成情報を使用します。ナビゲーション ペインのページ名をクリックすると、ウィザード ページに直接戻ることができます。

View Administrator で、[カタログ] - [デスクトップ プール] を選択すると、プールに追加されているとおりにデスクトップ仮想マシンを表示できます。

プールを作成した後は、プールが存在する限り、vCenter Server インベントリから親仮想マシンを削除したり、取り除いたりしないでください。vCenter Server のインベントリから仮想マシンを誤って取り除いてしまった場合は、改めて追加し、現在のイメージを使用してプッシュ イメージを実行する必要があります。

次のステップ

プールにアクセスするための資格をユーザーに付与します。[デスクトップまたはアプリケーション プールへの資格の追加](#)を参照してください。

ClonePrep でのゲストのカスタマイズ

ClonePrep は、作成プロセス中にインスタント クローンのカスタマイズします。

ClonePrep は、インスタント クローンがすべて Active Directory ドメインに参加することを確認します。クローンのコンピュータ セキュリティ ID (SID) は、親仮想マシンと同じものになります。ClonePrep は、アプリケーションのグローバル一意識別子 (GUID) も保持します。ただし、一部のアプリケーションではカスタマイズ中に新しい GUID が生成されることがあります。

インスタントクローン デスクトップ プールを追加すると、クローン作成後にすぐにスクリプトを実行し、クローンがパワーオフされる前に別のスクリプトを実行するよう指定できます。

ClonePrep でのスクリプトの実行方法

ClonePrep は、スクリプトを実行するために Windows CreateProcess API を使用します。スクリプトは、CreateProcess API で作成できる任意のプロセスを呼び出すことができます。たとえば、cmd、vbscript、exe、およびバッチ ファイル プロセスは、この API で動作します。

特に、ClonePrep は、スクリプトのパスを 2 番目のパラメータとして CreateProcess API に渡し、最初のパラメータを NULL に設定します。たとえば、スクリプト パスが `c:\myscript.cmd` の場合、CreateProcess の呼び出しは `CreateProcess(NULL, c:\myscript.cmd, ...)` となります。

ClonePrep スクリプトへのパスの指定

デスクトップ プールを作成または編集するときに、そのスクリプトを指定できます。スクリプトは、親仮想マシンに配置する必要があります。ネットワーク共有の UNC パスは使用できません。

スクリプトの実行にインタープリタが必要なスクリプト言語を使用する場合は、スクリプト パスをインタープリタの実行可能形式で始める必要があります。たとえば、`C:\script\myvb.vbs` ではなく、`C:\windows\system32\cscript.exe c:\script\myvb.vbs` と指定する必要があります。

重要: 許可されていないアクセスを防止するために、ClonePrep カスタマイズ スクリプトを安全なフォルダに入れてください。

ClonePrep スクリプトのタイムアウト制限

デフォルトでは、ClonePrep はスクリプトの実行が 20 秒を超える場合に、スクリプトを終了します。このタイムアウトの上限は引き上げることができます。詳細については、[ClonePrep および QuickPrep カスタマイズ スクリプトのタイムアウト制限の引き上げ](#)を参照してください。

あるいは、別のスクリプトを実行するスクリプトまたは実行に長時間かかるプロセスを指定できます。

ClonePrep スクリプト アカウント

ClonePrep は、VMware Horizon Instant Clone Agent サービスが使用するアカウントと同じアカウントを使用してスクリプトを実行します。デフォルトでは、このアカウントはローカル システムです。このログイン アカウントを変更しないでください。変更すると、クローンは起動に失敗します。

ClonePrep プロセスの権限

セキュリティ上の理由により、Windows オペレーティング システムの一部の権限は、ClonePrep カスタマイズ スクリプトを実行する VMware Horizon Instant Clone Agent プロセスから取り除かれます。そのスクリプトは、これらの権限を必要とするアクションを実行できません。

ClonePrep スクリプトを実行するプロセスには、次の権限がありません。

- SeCreateTokenPrivilege
- SeTakeOwnershipPrivilege
- SeSecurityPrivilege
- SeSystemEnvironmentPrivilege
- SeLoadDriverPrivilege
- SeSystemtimePrivilege
- SeUndockPrivilege
- SeManageVolumePrivilege
- SeLockMemoryPrivilege
- SeIncreaseBasePriorityPrivilege
- SeCreatePermanentPrivilege
- SeDebugPrivilege
- SeAuditPrivilege

ClonePrep スクリプトのログ

ClonePrep は、ログファイルにメッセージを書き込みます。ログファイルは、`C:\Windows\Temp\vmware-viewcomposer-ga-new.log` です。

インスタントクローン メンテナンス ユーティリティ

接続サーバには、vCenter Server のインスタントクローン仮想マシンと仮想マシンが含まれているクラスタのメンテナンスに使用できる、ユーティリティが 2 つあります。

ユーティリティは `IcMaint.cmd` と `IcUnprotect.cmd` で、`C:\Program Files\VMware\VMware View\Server\tools\bin` にあります。

IcMaint.cmd

このコマンドは、親仮想マシンを削除し、オプションでホストをメンテナンス モードにします。メンテナンスの実行後にこのコマンドを実行すると、ホストをメンテナンス モードから復帰できます。

構文：

```
IcMaint.cmd
-vc
  hostname_or_IP_address
-uid
  user_ID
-password
  password
-hostName
  ESXi_hostname
-maintenance
  ON|OFF
```

パラメータ：

- `-vc` *host name or IP address of vCenter Server*
- `-uid` *vCenter Server user ID*
- `-password` *vCenter Server user password*
- `-hostname` *ESXi host name*
- `-maintenance` *ON|OFF*

このパラメータは、親仮想マシンの削除後にメンテナンス モードを開始するかどうかを指定します。ホストがすでにメンテナンス モードの場合は、`-maintenanceOFF` に設定するとホストがメンテナンス モードから復帰します。

すべてのパラメータは必須です。

IcUnprotect.cmd

このユーティリティは、ClonePrep で作成したフォルダと仮想マシンの保護を解除します。ClonePrep は、作成プロセス中にインスタント クローンをカスタマイズするメカニズムです。

構文：

```
IcUnprotect.cmd
-vc
  hostname_or_IP_address
-uid
  user_ID
-password
  password [-clusterIdcluster_ID] [-includeFolders]
```

パラメータ :

- `-vc` *host name or IP address of vCenter Server*
- `-uid` *vCenter Server user ID*
- `-password` *vCenter Server user password*
- `-clusterId` *cluster ID*
- `-includeFolders`

このパラメータは、仮想マシンだけでなくフォルダのセキュリティも解除します。

`clusterId` および `includeFolders` を除くすべてのパラメータは必須です。`clusterId` が指定されていない場合、すべてのデータセンターにおけるすべての ClonePrep 仮想マシンの保護が解除されます。

手動デスクトップ プールの作成

手動デスクトップ プール内で、エンド ユーザーからアクセスされる各リモート デスクトップは別々のマシンです。手動デスクトップ プールを作成するときに、既存のマシンを選択します。手動デスクトップ プールを作成し、単一のマシンを選択することによって、単一のデスクトップを含むプールを作成することができます。

この章には、次のトピックが含まれています。

- [手動デスクトップ プール](#)
- [手動デスクトップ プールの作成用ワークシート](#)
- [手動デスクトップ プールの作成](#)
- [1 つのマシンを含む手動プールの作成](#)
- [手動プールのデスクトップ プール設定](#)

手動デスクトップ プール

手動デスクトップ プールを作成するために、View は既存のマシンからデスクトップをプロビジョニングします。プール内のデスクトップごとに、別のマシンを選択します。

手動プールでは複数の種類のマシンを使用できます。

- vCenter Server で管理される仮想マシン
- vCenter Server 以外の仮想化プラットフォームで実行される仮想マシン
- 物理コンピュータ

Linux 仮想マシンを使用する手動デスクトップ プールの作成に関する詳細については、Horizon 7 for Linux デスクトップのセットアップガイドを参照してください。

手動デスクトップ プールの作成用ワークシート

手動デスクトップ プールを作成するときに、View Administrator の [デスクトップ プールを追加] ウィザードで特定のオプションを構成するよう求められます。このワークシートを使用して、プールを作成する前に構成オプションを準備します。

このワークシートを印刷し、[デスクトップ プールを追加] ウィザードを実行するときに、希望する値を記入することができます。

注: 手動プールで、リモート デスクトップ アクセスを提供するための各マシンを準備する必要があります。各マシンで Horizon Agent がインストールされ、実行されている必要があります。

表 7-1. ワークシート：手動デスクトップ プールを作成するための構成オプション

オプション	説明	値をここに記入
ユーザー割り当て	<p>ユーザー割り当てのタイプを選択します。</p> <ul style="list-style-type: none"> ■ 専用割り当てプールでは、各ユーザーがマシンに割り当てられます。ユーザーは、ログインするたびに同じマシンを受け取ります。 ■ 流動割り当てプールでは、ユーザーは、ログインするたびに異なるマシンを受け取ります。 <p>詳細については、以下を参照してください。デスクトップ プールでのユーザー割り当て。</p>	
vCenter Server	<p>マシンを管理する vCenter Server。</p> <p>このオプションは、マシンが vCenter Server によって管理される仮想マシンである場合にのみ表示されます。</p>	
マシン ソース	<p>デスクトップ プールに含める仮想マシン、または物理コンピュータ。</p> <ol style="list-style-type: none"> 1 どの種類のマシンを使用するかを決定します。vCenter Server によって管理される仮想マシンまたは非管理対象の仮想マシンと物理コンピュータのいずれかを使用できます。 2 デスクトップ プールに含める、vCenter Server 仮想マシンまたは非管理対象の仮想マシンと物理コンピュータのリストを準備します。 3 デスクトップ プールに含める各マシンに Horizon Agent をインストールします。 <p>非管理対象の仮想マシンまたは物理コンピュータであるマシンで PColP を使用するには、Teradici ハードウェアを使用する必要があります。</p> <p>注: View Administrator で Windows Server デスクトップを有効にすると、View Administrator は使用可能なすべての Windows Server マシン（View 接続サーバなどの View server がインストールされているマシンなど）を潜在的なマシン ソースとして表示します。</p> <p>マシンに View server ソフトウェアがインストールされている場合、それらのマシンをデスクトップ プールに選択することはできません。Horizon Agent は、View 接続サーバ、セキュリティ サーバ、View Composer、または Horizon Client を含む他の View 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はできません。</p>	

オプション	説明	値をここに記入
デスクトップ プール ID	<p>ユーザーのログイン時に表示され、View Administrator でプールを識別するプール名。</p> <p>環境内で複数の vCenter Server を実行している場合は、別の vCenter Server で同じプール ID を使用していないことを確認します。</p>	
デスクトップ プールの設定	<p>マシンの状態、仮想マシンが使用中でないときの電源ステータス、表示プロトコル、Adobe Flash 品質などを決定する設定。</p> <p>詳細については、以下を参照してください。すべてのデスクトップ プール タイプのデスクトップ プール設定。</p> <p>手動プールに適用される設定のリストについては、手動プールのデスクトップ プール設定を参照してください。</p>	
透過的ページ共有の範囲	<p>透過的なページ共有 (TPS) を実行できるレベルを選択します。[仮想マシン] (デフォルト)、[プール]、[ポッド]、または [グローバル] から選択します。プール、ポッド、またはグローバルですべてのマシンに対して TPS をオンにすると、ESXi ホストは、マシンが同じゲスト オペレーティング システムまたはアプリケーションを使用した結果生じるメモリ ページの余分なコピーを取り除きます。</p> <p>ページ共有は ESXi ホストで発生します。たとえば、プールレベルで TPS を有効にするが、プールが複数の ESXi ホストにまたがっている場合、同じホスト上、または同じプール内の仮想マシンのみがページを共有します。グローバルレベルでは、同じ ESXi ホスト上で View によって管理されているすべてのマシンは、マシンが置かれているプールに関係なく、メモリ ページを共有できます。</p> <p>注: TPS はセキュリティ上のリスクを招く可能性があるため、デフォルト設定ではマシン間でのメモリ ページの共有が行われません。調査では、非常に限定された構成シナリオにおいて、TPS を悪用してデータへの不許可のアクセスを取得できる可能性があることが示されています。</p>	

手動デスクトップ プールの作成

既存の仮想マシンまたは物理コンピュータからデスクトップをプロビジョニングする手動デスクトップ プールを作成できます。このデスクトップ プールに含めるマシンを選択する必要があります。

vCenter Server によって管理される仮想マシンが含まれている手動プールの場合は、ユーザーがスベア マシンに接続できるように、View は必ず 1 つのスベア マシンがパワーオンされているようにします。このスベア マシンは、どの電源ポリシーが有効でもパワーオンされます。

前提条件

- リモート デスクトップ アクセスを提供するためのマシンを準備します。手動プールでは、各マシンを個別に準備する必要があります。各マシンで Horizon Agent がインストールされ、実行されている必要があります。

vCenter Server で管理される仮想マシンの準備については、[3 章 クローン作成のための親仮想マシンの作成と準備](#)を参照してください。

非管理対象の仮想マシンと物理コンピュータの準備については、[2 章 非管理対象マシンの準備](#)を参照してください。

- プールを作成するために指定する必要がある構成情報を収集します。[手動デスクトップ プールの作成用ワークシート](#)を参照してください。
- 電源設定、表示プロトコル、Adobe Flash 品質、およびその他の設定を構成する方法を決定します。[すべてのデスクトップ プール タイプのデスクトップ プール設定](#)を参照してください。

手順

- 1 View Administrator で、[カタログ] - [デスクトップ プール]を選択します。
- 2 [追加] をクリックします。
- 3 [手動デスクトップ プール] を選択します。
- 4 ウィザードの指示に従って、プールを作成します。

ワークシートで収集した構成情報を使用します。ナビゲーション パネルのページ名をクリックすると、完了したウィザード ページに直接戻ることができます。

View Administrator で、[カタログ] - [デスクトップ プール] を選択すると、プールに追加されているとおりにマシンを表示できます。

次のステップ

プールにアクセスするための資格をユーザーに付与します。[デスクトップまたはアプリケーション プールへの資格の追加](#)を参照してください。

1 つのマシンを含む手動プールの作成

ユーザーが一意的専用デスクトップを必要としている場合や、単一ホスト ライセンスしかない高価なアプリケーションに複数のユーザーが異なる時間にアクセスする必要がある場合は、単一マシンを含むプールを作成できます。

手動デスクトップ プールを作成し、単一のマシンを選択することによって、個別のマシンを独自のプールでプロビジョニングできます。

複数のユーザーが共有できる物理コンピュータを模倣するには、プールにアクセスするための資格が付与されているユーザーに対して流動割り当てを指定します。

単一のマシン プールを専用割り当てで構成しているか、流動割り当てで構成しているかにかかわらず、電源操作がセッション管理によって開始されます。仮想マシンは、ユーザーがデスクトップを要求するとパワーオンされ、ユーザーがログオフするとパワーオフされるかサスペンドされます。

[マシンは常にパワーオン] ポリシーを構成している場合、仮想マシンはパワーオンされたままです。ユーザーが仮想マシンをシャットダウンした場合、すぐに再起動されます。

前提条件

- リモート デスクトップ アクセスを提供するためのマシンを準備します。マシンで Horizon Agent がインストールされ、実行されている必要があります。

vCenter Server で管理される仮想マシンの準備については、[3 章 クローン作成のための親仮想マシンの作成と準備](#)を参照してください。

非管理対象の仮想マシン、物理コンピュータの準備については、[2 章 非管理対象マシンの準備](#)を参照してください。

- 手動プールを作成するために指定する必要がある構成情報を収集します。[手動デスクトップ プールの作成用ワークシート](#)を参照してください。
- 電源設定、表示プロトコル、Adobe Flash 品質、およびその他の設定を構成する方法を決定します。[すべてのデスクトップ プール タイプのデスクトップ プール設定](#)を参照してください。

手順

- 1 View Administrator で、[カタログ] - [デスクトップ プール]を選択します。
- 2 [追加] をクリックします。
- 3 [手動デスクトップ プール] を選択します。
- 4 ユーザー割り当てのタイプを選択します。

オプション	説明
専用	マシンは 1 人のユーザーに割り当てられます。そのユーザーだけがこのデスクトップにログインできます。
流動	マシンは、そのプールに対する資格が付与されているすべてのユーザーによって共有されます。別のユーザーがログインしていない限り、資格を持っているすべてのユーザーがこのデスクトップにログインできます。

- 5 [マシン ソース] ページで、デスクトップ プールに含めるマシンを選択します。
- 6 ウィザードの指示に従って、プールを作成します。

ワークシートで収集した構成情報を使用します。ナビゲーション パネルのページ名をクリックすると、完了したウィザード ページに直接戻ることができます。

View Administrator で、[カタログ] - [デスクトップ プール] を選択すると、プールに追加されるマシンを表示できます。

次のステップ

プールにアクセスするための資格をユーザーに付与します。[デスクトップまたはアプリケーション プールへの資格の追加](#)を参照してください。

手動プールのデスクトップ プール設定

手動デスクトップ プールの構成時に、マシンとプールの設定を指定する必要があります。すべての設定がすべての種類の手動プールに適用されるわけではありません。

[表 7-2. 手動デスクトップ プールの設定](#) に、以下のプロパティを使って構成される手動デスクトップ プールに適用される設定を示します。

- 専用ユーザー割り当て

- 流動ユーザー割り当て
- 管理対象マシン（vCenter Serve 仮想マシン）
- 非管理対象マシン

これらの設定は、単一マシンを含む手動プールにも適用されます。

各デスクトップ プール設定の説明については、[すべてのデスクトップ プール タイプのデスクトップ プール設定](#)を参照してください。

表 7-2. 手動デスクトップ プールの設定

設定	手動の管理対象プール、専用割り当て	手動の管理対象プール、流動割り当て	手動の非管理対象プール、専用割り当て	手動の非管理対象プール、流動割り当て
状態	はい	はい	はい	はい
接続サーバ restrictions（接続サーバの制限）	はい	はい	はい	はい
リモート マシンの電源ポリシー	はい	はい		
Automatically logoff after disconnect（切断後に自動的にログオフ）	はい	はい	はい	はい
ユーザーによるマシンのリセットを許可	はい	はい		
ユーザーが複数のクライアント デバイスからセッションを個別に開始できるようにする		はい		はい
デフォルト表示プロトコル	はい	はい	はい vCenter Server による非管理対象マシンで PCoIP を使用するには、マシンに Teradici ハードウェアをインストールする必要があります。	はい vCenter Server による非管理対象マシンで PCoIP を使用するには、マシンに Teradici ハードウェアをインストールする必要があります。
ユーザーがプロトコルを選択できるようにする	はい	はい	はい	はい
3D レンダラー	はい	はい		
Max number of monitors（モニタの最大数）	はい	はい		
Max resolution of any one monitor（特定のモニタの最大解像度）	はい	はい		

設定	手動の管理対象プ ール、専用割り当て	手動の管理対象プール、流動割 り当て	手動の非管理対象プール、専用 割り当て	手動の非管理対象プール、流動割 り当て
Adobe Flash quality (Adobe Flash の品質)	はい	はい	はい	はい
Adobe Flash throttling (Adobe Flash のスロットル)	はい	はい	はい	はい
Mirage 設定全体を オーバーライドする	はい	はい	はい	はい
Mirage サーバの構 成	はい	はい	はい	はい

リモート デスクトップ サービス ホストの設定

8

Microsoft リモート デスクトップ サービス (RDS) ホストにより、ユーザーがクライアント デバイスからアクセス可能なデスクトップ セッションおよびアプリケーションが提供されます。RDS デスクトップ プールまたはアプリケーション プールを作成する場合は、まず RDS ホストを設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。

- リモート デスクトップ サービス (RDS) ホスト
- Windows Server 2008 R2 へのリモート デスクトップ サービスのインストール
- Windows Server 2012 または 2012 R2 へのリモート デスクトップ サービスのインストール
- Windows Server 2008 R2 へのデスクトップ エクスペリエンスのインストール
- Windows Server 2012 または 2012 R2 へのデスクトップ エクスペリエンスのインストール
- ユーザーを単一セッションに制限する
- リモート デスクトップ サービス ホストへの Horizon Agent のインストール
- ネストされたセッション内で起動されたリモート アプリケーションからの印刷
- RDS デスクトップ セッションと RDS アプリケーション セッションのタイム ゾーン リダイレクトの有効化
- アプリケーションで Windows ベーシック テーマを有効にする
- Runonce.exe を開始するグループ ポリシーの構成
- RDS ホスト パフォーマンス オプション
- RDS ホスト用の 3D グラフィックスの構成

リモート デスクトップ サービス (RDS) ホスト

RDS ホストは、リモート アクセスのためのアプリケーションおよびデスクトップ セッションをホストするサーバ コンピュータです。RDS ホストには仮想マシンまたは物理サーバを使用できます。

RDS ホストには、Microsoft リモート デスクトップ サービス ロール、Microsoft リモート デスクトップ セッション ホスト サービスおよび Horizon Agent がインストールされています。リモート デスクトップ サービスは、かつてはターミナル サービスという名前でした。リモート デスクトップ セッション ホスト サービスを使用すると、アプリケーションおよびリモート デスクトップ セッションをサーバでホストできます。RDS ホストに Horizon Agent をインストールすることで、ユーザーは PCoIP または Blast Extreme 表示プロトコルを使用して、アプリケーションおよびデスクトップ セッションに接続できます。両方のプロトコルは、画像、オーディオ、ビデオなどのリモート コンテンツの配信について最適化されたユーザー エクスペリエンスを提供します。

RDS ホストのパフォーマンスは、多くの要因に依存します。Windows Server の異なるバージョンのパフォーマンスを調整する方法については、<http://msdn.microsoft.com/library/windows/hardware/gg463392.aspx> を参照してください。

Horizon 7 は、RDS ホスト上でユーザーごとに最大 1 つのデスクトップ セッションおよび最大 1 つのアプリケーション セッションをサポートします。

同一の RDS ホストでホストされる RDS デスクトップまたはアプリケーションから同時に印刷ジョブを実行すると、RDS ホストの ThinPrint サーバは印刷要求を同時ではなく順次処理します。そのため、一部のユーザーでは遅延が発生することがあります。印刷サーバは、印刷ジョブの完了を待機せずに次の印刷ジョブを処理します。異なるプリンタに送信された印刷ジョブの場合は、同時に印刷されます。

アプリケーションと RDS デスクトップが両方とも同一の RDS ホストでホストされている場合にこれらを起動すると、同一ユーザーのプロファイルが共有されます。デスクトップからアプリケーションを起動している場合に、両方のアプリケーションがユーザー プロファイルの同じ部分にアクセスしようとしたり、変更を加えようとしたりすると競合が発生することがあり、どちらかのアプリケーションが正しく実行されない場合があります。

アプリケーションまたはリモート アクセスのための RDS デスクトップ設定手順には、次のタスクが含まれます。

- 1 RDS ホストをセットアップします。
- 2 ファームを作成します。[9 章 ファームの作成](#)を参照してください。
- 3 アプリケーション プールまたは RDS デスクトップ プールを作成します。[10 章 アプリケーション プールの作成](#)または [11 章 RDS デスクトップ プールの作成](#)を参照してください。
- 4 ユーザーおよびグループに資格を付与します。[13 章 資格のあるユーザーとグループ](#)を参照してください。

- 5 (オプション) RDS デスクトップおよびアプリケーション セッションのタイム ゾーン リダイレクトを有効にします。[RDS デスクトップ セッションと RDS アプリケーション セッションのタイム ゾーン リダイレクトの有効化](#)を参照してください。

注: スマート カード認証が有効になっている場合は、RDS ホストでスマート カード サービスが無効になっていることを確認してください。RDS ホストでスマート カード サービスが無効になっていない場合、認証が失敗する可能性があります。デフォルトでは、このサービスは無効です。

注意: ユーザーが Web ブラウザなどのアプリケーションを起動するとき、ユーザーがそのアプリケーションをホストしている RDS ホスト上のローカル ドライブにアクセスできる可能性があります。アプリケーションで Windows Explorer を実行する機能が提供される場合、これが可能です。このような RDS ホストへのアクセスを防止するため、<http://support.microsoft.com/kb/179221> で説明されている手順に従い、アプリケーションで Windows Explorer が実行されないようにします。

<http://support.microsoft.com/kb/179221> の手順は、デスクトップおよびアプリケーション セッションの両方に影響を与えるため、デスクトップセッションが影響を受けないように、Microsoft KB 記事の手順に従う場合、同一のファームに RDS デスクトップ プールとアプリケーション プールを作成しないことを推奨します。

アプリケーションのインストール

アプリケーション プールを作成する場合、RDS ホストにアプリケーションをインストールする必要があります。Horizon 7 でインストールされたアプリケーションのリストを自動的に表示するには、すべてのユーザーが [スタート] メニューから利用できるようにアプリケーションをインストールする必要があります。アプリケーション プールを作成する前であれば、いつでもアプリケーションをインストールできます。手動でアプリケーションを指定する場合は、アプリケーション プールを作成する前または後の好きなときにアプリケーションをインストールできます。

重要: アプリケーションをインストールするときに、ファーム内のすべての RDS ホストに、かつ各 RDS ホストの同じ場所にインストールする必要があります。そうしなかった場合、健全性の警告が View Administrator ダッシュボードに表示されます。この状況でアプリケーション プールを作成すると、アプリケーションの実行時にエラーが発生する場合があります。

Horizon 7 では、アプリケーション プールを作成すると、ファームのすべての RDS ホストの [スタート] メニューから、(個々のユーザーではなく) すべてのユーザーが使用可能なアプリケーションが自動的に表示されます。このリストから任意のアプリケーションを選択できます。また、[スタート] メニューから、すべてのユーザーに利用可能ではないアプリケーションを手動で指定できます。RDS ホストにインストールできるアプリケーションの数に制限はありません。

Windows Server 2008 R2 へのリモート デスクトップ サービスのインストール

リモート デスクトップサービス (RDS) は、Windows Server で設定できるロールの 1 つです。Windows Server 2008 R2 を実行する RDS ホストをセットアップするには、このロールをインストールする必要があります。

前提条件

- RDS ホストで Windows Server 2008 R2 Service Pack 1 (SP1) が動作していることを確認します。

- RDS ホストが Horizon 7 環境の Active Directory ドメインの一部であることを確認します。
- <http://support.microsoft.com/kb/2775511> に記載されている Microsoft のホットフィックス ロールアップをインストールします。
- Microsoft 更新プログラム (<https://support.microsoft.com/en-us/kb/2973201>) をインストールします。

手順

- 1 RDS ホストに管理者としてログインします。
- 2 Server Manager を開始します。
- 3 ナビゲーション ツリーで [ロール] を選択します。
- 4 [ロールを追加] をクリックして [ロールを追加] ウィザードを起動します。
- 5 [リモート デスクトップ サービス] ロールを選択します。
- 6 [ロール サービスを選択] ページで、[リモート デスクトップ セッション ホスト] を選択します。
- 7 認証方法の指定のページで、適宜、[ネットワーク レベル認証を必要とする] または [ネットワーク レベル認証を必要としない] を選択します。
- 8 [クライアント エクスペリエンスの構成] ページで、ユーザーに提供する機能を選択します。
- 9 指示に従ってインストールを終了します。

次のステップ

HTML Access またはスキャナ リダイレクトを使用する予定がある場合は、デスクトップ エクスペリエンス機能をインストールします。デスクトップ エクスペリエンスのインストール手順は、Windows Server 2008 R2 上と Windows Server 2012 または 2012 R2 上では異なります。

ユーザーが 1 つのデスクトップ セッションのみを使用するように制限します。[ユーザーを単一セッションに制限する](#)を参照してください。

Windows Server 2012 または 2012 R2 へのリモート デスクトップ サービスのインストール

リモート デスクトップサービスは、Windows Server 2012 または 2012 R2 が持つことのできるロールの 1 つです。RDS ホストをセットアップするには、このロールをインストールする必要があります。

前提条件

- RDS ホストで Windows Server 2012 または Windows Server 2012 R2 が動作していることを確認します。
- RDS ホストが Horizon 7 展開環境用の Active Directory ドメインの一部であることを確認します。

手順

- 1 RDS ホストに管理者としてログインします。
- 2 Server Manager を開始します。
- 3 [ロールと機能を追加] を選択します。

- 4 [インストール タイプを選択] ページで、[ロールベースまたは機能ベースのインストール] を選択します。
- 5 [ターゲット サーバを選択] ページで、サーバを選択します。
- 6 [サーバ ロールを選択] ページで、[リモート デスクトップ サービス] を選択します。
- 7 [機能を選択] ページで、デフォルトを受け入れます。
- 8 [ロール サービスを選択] ページで、[リモート デスクトップ セッション ホスト] を選択します。
- 9 指示に従ってインストールを終了します。

次のステップ

HTML Access またはスキャナ リダイレクトを使用する予定がある場合は、デスクトップ エクスペリエンス機能をインストールします。デスクトップ エクスペリエンスのインストール手順は、Windows Server 2008 R2 上と Windows Server 2012 または 2012 R2 上では異なります。

ユーザーが 1 つのデスクトップ セッションのみを使用するように制限します。[ユーザーを単一セッションに制限する](#)を参照してください。

Windows Server 2008 R2 へのデスクトップ エクスペリエンスのインストール

RDS デスクトップとアプリケーション、および Windows Server を実行するシングルユーザー仮想マシンに展開された VDI デスクトップの場合、スキャナ リダイレクトを使用するには、RDS ホストおよびシングルユーザー仮想マシンにデスクトップ エクスペリエンス機能をインストールする必要があります。

手順

- 1 管理者としてログインします。
- 2 Server Manager を開始します。
- 3 [機能] をクリックします。
- 4 [機能の追加] をクリックします。
- 5 [機能を選択] ページで、[デスクトップ エクスペリエンス] チェックボックスを選択します。
- 6 デスクトップ エクスペリエンス機能で必要な他の機能に関する情報を確認し、[必要な機能の追加] をクリックします。
- 7 指示に従ってインストールを終了します。

Windows Server 2012 または 2012 R2 へのデスクトップ エクスペリエンスのインストール

RDS デスクトップとアプリケーション、および Windows Server を実行するシングルユーザー仮想マシンに展開された VDI デスクトップの場合、スキャナ リダイレクトを使用するには、RDS ホストおよびシングルユーザー仮想マシンにデスクトップ エクスペリエンス機能をインストールする必要があります。

Windows Server 2012 および Windows Server 2012 R2 は、RDS ホストとして使用されるマシンでサポートされています。Windows Server 2012 R2 はシングル ユーザー仮想マシンでサポートされています。

手順

- 1 管理者としてログインします。
- 2 Server Manager を開始します。
- 3 [ロールと機能を追加] を選択します。
- 4 [インストール タイプを選択] ページで、[ロールベースまたは機能ベースのインストール] を選択します。
- 5 [ターゲット サーバを選択] ページで、サーバを選択します。
- 6 [サーバ ロールを選択] ページで、デフォルトの選択を受け入れ、[次へ] をクリックします。
- 7 [機能を選択] ページで、[ユーザー インターフェイスとインフラストラクチャ] の下で [デスクトップ エクスペリエンス] を選択します。
- 8 指示に従ってインストールを終了します。

ユーザーを単一セッションに制限する

Horizon 7 は、RDS ホスト上でユーザーごとに最大 1 つのデスクトップ セッションおよび最大 1 つのアプリケーション セッションをサポートします。ユーザーを単一セッションに制限するように RDS ホストを構成する必要があります。Windows Server 2008 R2、Windows Server 2012、および Windows Server 2012 R2 の場合、グループ ポリシー設定の

Restrict Remote Desktop Services users to a single Remote Desktop Services session を有効にしてユーザーを単一セッションに制限することができます。この設定は、Computer Configuration \Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections フォルダにあります。Windows Server 2008 R2 の場合、次の手順を使用してユーザーを単一セッションに制限することができます。

前提条件

- [Windows Server 2008 R2 へのリモート デスクトップ サービスのインストール](#) に説明されている方法で、リモート デスクトップ サービス ロールをインストールします。

手順

- 1 [スタート] - [管理ツール] - [リモート デスクトップ サービス] - [リモート デスクトップ セッション ホストの構成] の順にクリックします。
- 2 [編集設定] ペインの [全般] で、[各ユーザーを単一セッションに制限する] をダブルクリックします。
- 3 [プロパティ] ダイアログ・ボックスの [全般] タブで、[各ユーザーを単一セッションに制限する] を選択して、[OK] をクリックします。

次のステップ

RDS ホストに Horizon Agent をインストールします。[リモート デスクトップ サービス ホストへの Horizon Agent のインストール](#)を参照してください。

リモート デスクトップ サービス ホストへの Horizon Agent のインストール

Horizon Agent は、接続サーバと通信して、表示プロトコル PCoIP および Blast Extreme をサポートします。RDS ホストに Horizon Agent をインストールする必要があります。

前提条件

- [Windows Server 2008 R2 へのリモート デスクトップ サービスのインストール](#)または [Windows Server 2012 または 2012 R2 へのリモート デスクトップ サービスのインストール](#)に説明されている方法で、リモート デスクトップ サービス ロールをインストールします。
- ユーザーが 1 つのデスクトップ セッションのみを使用するように制限します。[ユーザーを単一セッションに制限する](#)を参照してください。
- Horizon Agent カスタム セットアップ オプションについて理解しておきます。[RDS ホストに対する Horizon Agent のカスタム セットアップ オプション](#)を参照してください。
- マシンに Microsoft Visual C++ Redistributable パッケージがインストールされている場合、パッケージのバージョンが 2005 SP1 以降であることを確認します。パッケージのバージョンが 2005 以前の場合は、パッケージのアップグレードまたはアンインストールのいずれかが可能です。
- VMware 製品ページ <http://www.vmware.com/go/downloadview> から、Horizon Agent インストーラ ファイルをダウンロードします。

手順

- 1 管理者としてログインします。
- 2 Horizon Agent インストール プログラムを起動するには、インストーラ ファイルをダブルクリックします。
インストーラのファイル名は、VMware-viewagent-x86_64-y.y.y-xxxxxx.exe です。y.y.yはバージョン番号、xxxxxxはビルド番号です。
- 3 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 View 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。
- 4 カスタム セットアップのオプションを選択します。
手動ファームに置かれる RDS ホストに Horizon Agent をインストールしている場合、[View Composer Agent] オプションを選択しないでください。
- 5 [サーバ] テキスト ボックスに、接続サーバ ホストのホスト名または IP アドレスを入力します。
インストール時に、インストーラが接続サーバ インスタンスに RDS ホストを登録します。登録後、指定した接続サーバ インスタンスおよび同じ接続サーバ グループ内の他のインスタンスは RDS ホストと通信できます。

6 認証方式を選択して、接続サーバ インスタンスに RDS ホストを登録します。

オプション	説明
現在ログインしているユーザーとして認証する	[ユーザー名] および [パスワード] テキスト ボックスは無効であり、現在のユーザー名とパスワードを使用して接続サーバ インスタンスにログインします。
管理者の認証情報を指定する	[ユーザー名] および [パスワード] テキスト ボックスに、接続サーバ管理者のユーザー名とパスワードを入力する必要があります。

ユーザー アカウントは、View 接続サーバ インスタンスで View LDAP にアクセスできるドメイン ユーザーでなければなりません。ローカル ユーザーは使用できません。

7 指示に従ってインストールを終了します。

次のステップ

ファームを作成します。[9 章 ファームの作成](#)を参照してください。

RDS ホストに対する Horizon Agent のカスタム セットアップ オプション

RDS ホストに Horizon Agent をインストールする際に、カスタム セットアップ オプションを選択できます。また、Horizon Agent は特定の機能を、サポートされているすべてのゲスト OS に自動的にインストールします。これらの機能はオプションではありません。

最新の Horizon Agent バージョンをインストールした後でカスタム セットアップ オプションを変更するには、Horizon Agent をアンインストールしてから再インストールする必要があります。パッチおよびアップグレードの場合、前のバージョンをアンインストールすることなく、新しい Horizon Agent インストーラを実行して、新しいオプション セットを選択できます。

表 8-1. IPv4 環境の RDS ホストに対する Horizon Agent のカスタム セットアップ オプション

オプション	説明
USB リダイレクト	<p>ローカルで接続されている USB ストレージ デバイスにユーザーがアクセスできるようにします。</p> <p>特に、USB フラッシュ ドライブとハード ディスクのリダイレクトは、RDS デスクトップとアプリケーションでサポートされています。他のタイプの USB デバイス、およびセキュリティ ストレージ ドライブ、USB CD-ROM などの他のタイプの USB ストレージ デバイスのリダイレクトは、RDS デスクトップとアプリケーションでサポートされません。</p> <p>デフォルトではこのセットアップ オプションは選択されていません。このオプションを選択してインストールする必要があります。このオプションは、Windows Server 2012 または 2012 R2 が動作している RDS ホストで利用可能ですが、Windows Server 2008 R2 では利用できません。</p> <p>USB リダイレクトを安全に使用するガイダンスについては、『View セキュリティ』ガイドを参照してください。たとえば、グループ ポリシー設定を使用して、特定のユーザーの USB リダイレクトを無効にすることができます。</p>
HTML Access	<p>ユーザーは HTML Access を使用して RDS デスクトップおよびアプリケーションに接続できます。この設定オプションが選択されると、HTML Access エージェントがインストールされます。このエージェントは RDS ホストにインストールする必要があり、これによってユーザーは HTML Access に接続できます。</p>
3D RDSH	<p>この RDS ホストで実行されているアプリケーションで 3D グラフィックスを使用できるようにします。</p>
View Composer Agent	<p>このマシンが自動ファームを作成するための親仮想マシンの場合、このオプションを選択します。このマシンが手動ファームの RDS ホストの場合、このオプションは選択しないでください。</p>

オプション	説明
クライアント ドライブ リダイレクト	<p>これを使用すると、Horizon Client ユーザーがローカル ドライブを RDS デスクトップおよびアプリケーションと共有できます。</p> <p>この設定オプションがインストールされた後は、RDS ホストではこれ以上の構成は必要ありません。</p> <p>クライアント ドライブ リダイレクトは、単一ユーザーの仮想マシンおよび未管理のマシン上で実行されている VDI デスクトップでもサポートされます。</p>
仮想印刷	<p>ユーザーがクライアント コンピュータで利用できる任意のプリンタに出力できるようにします。ユーザーは、デスクトップに追加のドライバをインストールする必要はありません。</p> <p>仮想印刷は次のリモート デスクトップおよびアプリケーションでサポートされます。</p> <ul style="list-style-type: none"> ■ Windows デスクトップや Windows Server マシンなど、単一ユーザーのマシンにデプロイされたデスクトップ。 ■ 仮想マシンである RDS ホストにデプロイされたデスクトップ。 ■ リモート アプリケーション。 ■ リモート デスクトップ内部の Horizon Client から起動されるリモート アプリケーション（ネストされるセッション）。 <p>仮想印刷機能は、Horizon Agent からインストールする場合に限ってサポートされます。VMware Tools でインストールしてもサポートされません。</p>
vRealize Operations Desktop Agent	vRealize Operations Manager を vRealize Operations Manager for Horizon で動作させます。
スキャナ リダイレクト	<p>クライアント システムに接続されるスキャン デバイスをリダイレクトするので、そのデバイスを RDS デスクトップまたはアプリケーションで使用できます。</p> <p>このオプションを Horizon Agent インストーラでできるようにするには、RDS ホストの Windows Server オペレーティング システムにデスクトップ エクスペリエンス機能をインストールする必要があります。</p> <p>このセットアップ オプションは、Windows Server ゲスト OS にデフォルトではインストールされません。このオプションを選択してインストールする必要があります。</p> <p>スキャナ リダイレクトは Horizon 6.0.2 以降のリリリースで使用できます。</p>
VMware クライアント IP アドレスの透過性	<p>Internet Explorer へのリモート接続を有効にし、リモート デスクトップ マシンの IP アドレスの代わりにクライアントの IP アドレスを使用します。</p> <p>デフォルトではこのセットアップ オプションは選択されていません。このオプションを選択してインストールする必要があります。</p>

IPv6 環境では、オプション機能はありません。

表 8-2. RDS ホストに自動的にインストールされる Horizon Agent の機能

オプション	説明
PCoIP エージェント	<p>ユーザーが PCoIP 表示プロトコルを使用してアプリケーションと RDS デスクトップに接続できるようにします。</p> <p>ユーザーは PCoIP を使用してのみアプリケーションに接続できるため、アプリケーション プールを作成する予定がある場合は、このコンポーネントをインストールする必要があります。</p>
Windows Media マルチメディア リダイレクト (MMR)	RDS デスクトップへのマルチメディア リダイレクトを提供します。この機能は、クライアント コンピュータに直接マルチメディア ストリームを配信し、これによってリモート ESXi ホストの代わりにクライアント ハードウェアでマルチメディア ストリームを処理できます。
Unity Touch	<p>タブレット ユーザーとスマートフォン ユーザーが、リモート デスクトップで実行されている Windows アプリケーションを操作できるようになります。ユーザーは Windows アプリケーションやファイルの参照、検索、およびオープンを行ったり、お気に入りのアプリケーションやファイルを選択したり、スタート メニューまたはタスクバーを使用しなくても実行中のアプリケーションを切り替えることができます。</p>

オプション	説明
PSG エージェント	RDS ホストに PCoIP Secure Gateway をインストールし、RDS ホスト上で実行されているデスクトップ セッションおよびアプリケーション セッション用に PCoIP 表示プロトコルを実装します。
VMwareRDS	VMware でのリモート デスクトップ サービス機能の実装を可能にします。

IPv6 環境で自動的にインストールされる機能は、PCoIP Agent、PSG Agent、および VMwareRDS です。

RDS ホストでサポートされるその他の機能については、『View アーキテクチャの計画』の「Horizon Agent の機能サポート一覧」を参照してください。

ネストされたセッション内で起動されたリモート アプリケーションからの印刷

Horizon Agent のインストール中に仮想印刷を有効にすると、リモート デスクトップ（ネストされたセッション）内の Horizon Client から起動したリモート アプリケーションから、ローカル クライアント マシンにあるプリンタに印刷できます。

Horizon 7 バージョン 7.0.2 から、ネストされたセッションから起動したリモート アプリケーションから、ローカル クライアント マシンに接続するプリンタではなく、リモート デスクトップ マシンに接続するプリンタにユーザーが印刷できるようになりました。この機能を有効にするには、HKEY_LOCAL_MACHINE\SOFTWARE\ThinPrint\TPClnRDP の SiSActive の値を 0 に変更して、リモート デスクトップ マシンの Thinprint セッション イン セッション モードを変更します。

注: SiSActive がリモート デスクトップ マシンで 0 に設定されていると、ネストされたセッション内から起動されたリモート アプリケーションからローカル クライアント マシンに接続するプリンタに印刷できなくなります。デフォルトの ThinPrint セッション イン セッション モードを再度有効にするには、リモート デスクトップ マシンで HKEY_LOCAL_MACHINE\SOFTWARE\ThinPrint\TPClnRDP の SiSActive の値を 1 に変更します。

Horizon Agent インストール時に仮想印刷オプションを有効にする方法の詳細は、[RDS ホストに対する Horizon Agent のカスタム セットアップ オプション](#)を参照してください。

RDS デスクトップ セッションと RDS アプリケーション セッションのタイムゾーンリダイレクトの有効化

RDS ホストのタイムゾーンとユーザーのタイムゾーンが異なる場合、デフォルトでは、そのユーザーが RDS デスクトップに接続するときに RDS デスクトップには RDS ホストのタイムゾーンの時間が表示されます。タイムゾーンリダイレクトグループポリシー設定を有効にすることにより、RDS デスクトップにローカルタイムゾーンの時間を表示することができます。このポリシー設定はアプリケーションセッションにも適用されます。

前提条件

- Active Directory サーバでグループポリシー管理機能が使用できることを確認します。

グループポリシー管理コンソールを開く手順は、Windows 2012、Windows 2008、および Windows 2003 Active Directory の各バージョンによって異なります。[View グループポリシーの GPO の作成](#)を参照してください。

- Horizon 7 RDS ADMX ファイルが Active Directory に追加されていることを確認します。 [リモート デスクトップ サービス ADMX ファイルを Active Directory へ追加](#) を参照してください。
- グループ ポリシー設定について理解しておきます。 [RDS デバイスおよびリソースのリダイレクトの設定](#) を参照してください。

手順

- 1 Active Directory サーバで、グループ ポリシー管理コンソールを開きます。
- 2 ドメインと [グループ ポリシー オブジェクト] を展開します。
- 3 グループ ポリシー設定用に作成した GPO を右クリックし、[編集] を選択します。
- 4 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] - [Windows コンポーネント] - [Horizon View RDSH サービス] - [リモート デスクトップ セッション ホスト] - [デバイスとリソースのリダイレクト] の順に移動します。
- 5 設定 [タイム ゾーン リダイレクトの許可] を有効にします。

アプリケーションで Windows ベーシック テーマを有効にする

RDS ホスト上のデスクトップに接続したことがないユーザーが、RDS ホストでホストされているアプリケーションを起動した場合、Aero スタイル テーマをロードするように GPO 設定が構成されていても、アプリケーションに Windows ベーシック テーマは適用されません。Horizon 7 では、Aero スタイル テーマはサポートされませんが、Windows ベーシック テーマはサポートされます。アプリケーションに Windows ベーシック テーマを適用するには、別の GPO 設定を構成する必要があります。

前提条件

- Active Directory サーバでグループ ポリシー管理機能が使用できることを確認します。
グループ ポリシー管理コンソールを開く手順は、Windows 2012、Windows 2008、および Windows 2003 Active Directory の各バージョンによって異なります。 [View グループ ポリシーの GPO の作成](#) を参照してください。

手順

- 1 Active Directory サーバで、グループ ポリシー管理コンソールを開きます。
- 2 ドメインと [グループ ポリシー オブジェクト] を展開します。
- 3 グループ ポリシー設定用に作成した GPO を右クリックし、[編集] を選択します。
- 4 グループ ポリシー管理エディタで、[ユーザーの構成] - [ポリシー] - [管理用テンプレート] - [コントロール パネル] - [個人設定] に移動します。
- 5 [特定の視覚スタイル ファイルを強制するか、または Windows クラシックを強制する] という設定を有効にして、[視覚スタイルへのパス] を `%windir%\resources\Themes\Aero\ aero.msstyles` に設定します。

Runonce.exe を開始するグループ ポリシーの構成

デフォルトでは、Explorer.exe ファイルに依存する一部のアプリケーションは、アプリケーション セッションで実行できないことがあります。この問題を回避するには、runonce.exe を実行するように GPO 設定を構成する必要があります。

前提条件

- Active Directory サーバでグループ ポリシー管理機能が使用できることを確認します。
グループ ポリシー管理コンソールを開く手順は、Windows 2012、Windows 2008、および Windows 2003 Active Directory の各バージョンによって異なります。[View グループ ポリシーの GPO の作成](#)を参照してください。

手順

- 1 Active Directory サーバで、グループ ポリシー管理コンソールを開きます。
- 2 ドメインと [グループ ポリシー オブジェクト] を展開します。
- 3 グループ ポリシー設定用に作成した GPO を右クリックし、[編集] を選択します。
- 4 グループ ポリシー管理エディタで、[ユーザー構成] - [ポリシー] - [Windows 設定] - [スクリプト (ログオン/ログオフ)] に移動します。
- 5 [ログオン] をダブルクリックし、[追加] をクリックします。
- 6 スクリプト名ボックスに、**runonce.exe** と入力します。
- 7 スクリプト パラメータ ボックスに、**/AlternateShellStartup** と入力します。

RDS ホスト パフォーマンス オプション

パフォーマンス オプションを設定することで、Windows をフォアグラウンド プログラムまたはバックグラウンド サービス用に最適化できます。デフォルトでは、Horizon 7 により、サポートされている Windows Server のすべてのバージョンで、RDS ホストの特定のパフォーマンス オプションが無効になっています。

次の表に、Horizon 7 により無効になっているパフォーマンス オプションを示します。

表 8-3. Horizon 7 により無効になっているパフォーマンス オプション

Horizon 7 により無効になっているパフォーマンス オプション
ウィンドウを最大化や最小化するときにアニメーションで表示する
マウス ポインタの下に影を表示する
ウィンドウの下に影を表示する
デスクトップのアイコン名に影を付ける
ドラッグ中にウィンドウの内容を表示する

Horizon 7 により無効になっている 5 つのパフォーマンス オプションは、レジストリの 4 つの Horizon 7 設定に対応します。次の表は、Horizon 7 設定とそのデフォルトのレジストリ値を示します。レジストリ値はすべて、レジストリ サブキー HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\Configuration にあります。1 つ以上の Horizon 7 レジストリ値を **false** に設定して、パフォーマンス オプションを再度有効にすることができます。

表 8-4. Windows パフォーマンス オプション に関連する Horizon 7 設定

Horizon 7 設定	レジストリの値
カーソル シャドウを無効にする	DisableMouseShadows
フル ウィンドウ ドラッグを無効にする	DisableFullWindowDrag
リストビュー シャドウを無効にする	DisableListViewShadow
ウィンドウ アニメーションを無効にする	DisableWindowAnimation

RDS ホスト用の 3D グラフィックスの構成

RDS ホスト用の 3D グラフィックスが構成されている場合、アプリケーション プールのアプリケーションと RDS デスクトップで実行されているアプリケーションの両方で 3D グラフィックスを表示できます。

次の 3D グラフィックス オプションを使用できます。

NVIDIA GRID vGPU (共有 GPU ハードウェア アクセラレーション) ESXi ホスト上の物理 GPU は複数の仮想マシンで共有されます。ESXi 6.0 以降が必要です。

vDGA を使用する AMD Multiuser GPU ESXi ホスト上の物理 GPU は複数の仮想マシンで共有されます。ESXi 6.0 以降が必要です。

Virtual Dedicated Graphics Acceleration (vDGA) ESXi ホスト上の物理 GPU は単一の仮想マシン専用になります。ESXi 5.5 以降が必要です。

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

vDGA の場合、最大のパフォーマンスを得るために GPU 全体を 1 つのマシンに割り当てます。RDS ホストを手動ファームに含める必要があります。

vDGA を使用した AMD Multiuser GPU の場合、複数の PCI パススルー デバイスのように見せることで、複数の RDS ホストの間で AMD GPU を共有できます。RDS ホストを手動ファームに含める必要があります。

NVIDIA GRID vGPU を使用すると、各グラフィックス カードで複数の RDS ホストをサポートでき、RDS ホストを手動ファームに含める必要があります。ESXi ホストに複数の物理 GPU がある場合、ESXi ホストが仮想マシンを GPU に割り当てる方法を構成することもできます。デフォルトの場合、ESXi ホストは、すでに割り当てられている仮想マシンの数が最も少ない物理 GPU に仮想マシンを割り当てます。これはパフォーマンス モードと呼ばれます。仮想マシンが最大数に到達するまで ESXi ホストが仮想マシンを同じ物理 GPU に割り当ててから、次の物理 GPU 上に仮想マシンを配置する場合は、統合モードを選択することもできます。統合モードを構成するには、`/etc/vmware/config` ファイルを ESXi ホストで編集して、次のエントリを追加します。

```
vGPU.consolidation = "true"
```

PCoIP プロトコルまたは VMware Blast プロトコルを使用する場合、3D グラフィックスのみがサポートされます。そのため、ファームでデフォルト プロトコルとして PCoIP または VMware Blast を使用し、ユーザーがプロトコルを選択できないようにする必要があります。

3D グラフィックスの構成手順の概要

ここでは、3D グラフィックスを構成するために vSphere および Horizon 7 で実行する必要があるタスクについての概要を説明します。NVIDIA GRID vGPU の設定の詳細については、ドキュメント [VMware Horizon 6.1 向け NVIDIA GRID vGPU デプロイ ガイド](#) を参照してください。vDGA の設定の詳細については、ドキュメント [View 仮想デスクトップのグラフィックス アクセラレーション](#) を参照してください。vDGA を使用した AMD Multiuser GPU の設定の詳細については、[vDGA を使用する AMD Multiuser GPU の機能を使用する準備](#) を参照してください。

- 1 RDS ホストの仮想マシンを設定します。詳細については、[8 章 リモート デスクトップ サービス ホストの設定](#) を参照してください。
- 2 グラフィックス PCI デバイスを仮想マシンに追加します。『vSphere 仮想マシン管理』ドキュメントの「仮想マシン ハードウェアの構成」の章にある「その他の仮想マシン デバイスの構成」を参照してください。デバイスを追加するときは、必ず [すべてのメモリの予約] をクリックしてください。
- 3 仮想マシンで、グラフィックス カードのデバイス ドライバをインストールします。
- 4 RDS ホストを手動ファームに追加して、RDS デスクトップ プールを作成します。次に、PCoIP を使用してデスクトップに接続し、ディスプレイ アダプタをアクティベーションします。

View Administrator で RDS ホストの 3D グラフィックスを構成する必要はありません。Horizon Agent のインストール時に、[3D RDSH] オプションを選択すれば済みます。デフォルトではこのオプションは選択されておらず、3D グラフィックスは無効になっています。

ファームの作成

ファームは RDS ホストのグループで、一般的なアプリケーションまたは RDS デスクトップをユーザーに提供します。

この章には、次のトピックが含まれています。

- [ファーム](#)
- [自動ファームの親仮想マシンの準備](#)
- [手動ファーム作成用ワークシート](#)
- [自動ファーム作成用ワークシート](#)
- [手動ファームの作成](#)
- [自動ファームの作成](#)

ファーム

ファームを使用すると、エンタープライズ内の RDS ホスト、RDS デスクトップ、アプリケーションを管理するタスクが簡素化されます。手動ファームまたは自動ファームを作成して、異なるサイズ、または異なるデスクトップ要件あるいはアプリケーション要件を持つユーザー グループを処理できます。

手動ファームは、すでに存在する RDS ホストで構成されます。RDS ホストは、物理マシンまたは仮想マシンです。ファームを作成する場合、手動で RDS ホストを追加します。

自動ファームは、vCenter Server のリンククローン仮想マシンである RDS ホストで構成されます。View Composer は、ファームの作成時に指定したパラメータに基づいて仮想マシンを作成します。仮想マシンに必要なストレージ容量を削減するメカニズムで、1 つの親仮想マシンから複数の仮想マシンがクローン作成され、親にリンクされます。

アプリケーション プールまたは RDS デスクトップ プールを作成する場合は、ファームを 1 つだけ指定する必要があります。ファーム内の RDS ホストは、RDS デスクトップ、アプリケーション、またはその両方をホストできます。ファームでは RDS デスクトップ プールを 1 つまでしかサポートできませんが、複数のアプリケーション プールをサポートできます。ファームは、両方のタイプのプールを同時にサポートできます。

ファームを使用すると、次のような利点があります。

- 負荷分散

デフォルトでは、Horizon 7 はファーム内のすべての RDS ホストの RDS デスクトップ セッションおよびアプリケーション セッションの負荷を分散します。負荷分散スクリプトを作成して構成することにより、新しいアプリケーション セッションの配置を制御できます。詳細については、『View 管理』ドキュメントの「RDS ホストの負荷分散の構成」を参照してください。

- 冗長性

ファーム内の 1 つの RDS ホストがオフラインの場合、ファーム内の他の RDS ホストが引き続きユーザーにアプリケーションやデスクトップを提供します。

- スケーラビリティ

ファームにはさまざまな数の RDS ホストを含めることができます。さまざまなサイズのユーザー グループを処理するために、さまざまな数の RDS ホストを持つファームを作成できます。

ファームには、次のプロパティがあります。

- 1 つの Horizon 7 ポッドに、最大 200 のファームを含めることができます。
- 1 つのファームに、最大 200 の RDS ホストを含めることができます。
- ファーム内の RDS ホストでは、サポートされている任意のバージョンの Windows Server を実行できます。『View のインストール』の「ゲスト OS のシステム要件」を参照してください。
- 自動ファームでは、View Composer の再構成操作はされていますが、更新操作または再調整操作はサポートされていません。自動ファームを再構成することはできますが、ファームの RDS ホストのサブセットを再構築することはできません。

重要: Microsoft では、ファームごとに個別にユーザーの移動プロファイルを構成することを推奨しています。プロファイル ファイルをファーム間またはユーザーの物理デスクトップ間で共有することはできません。ユーザーが同じプロファイルを読み取る 2 台のマシンに同時にログインしている場合、プロファイルの破損およびデータの損失が発生する可能性があるためです。

自動ファームの親仮想マシンの準備

自動ファームを作成するには、まず親仮想マシンを準備する必要があります。View Composer は、この親仮想マシンを使用して、ファーム内の RDS ホストであるリンククローン仮想マシンを作成します。

- [RDS ホストの親仮想マシンの準備](#)

View Composer サービスには、リンク クローンの作成のための基本イメージの生成元になる親仮想マシンが必要です。

- [リンククローン RDS ホストでの Windows のアクティベーション](#)

View Composer によってリンククローン RDS ホスト上の Windows Server オペレーティング システムの適切なアクティベーションが行われるようにするには、親仮想マシンで Microsoft ボリューム アクティベーションを使用する必要があります。ボリューム アクティベーション テクノロジーにはボリューム ライセンス キーが必要です。

■ 親仮想マシンでの Windows のハイバネーションの無効化

Windows のハイバネーション機能によって、非表示のシステム ファイル Hiberfil.sys が作成されます。

このファイルは、ハイブリッド スリープに必要な情報を格納するために使用されます。ハイバネーションを無効にすると、インスタント クローンの仮想ディスクまたは View Composer リンク クローンの仮想ディスクのサイズが削減されます。

RDS ホストの親仮想マシンの準備

View Composer サービスには、リンク クローンの作成のための基本イメージの生成元になる親仮想マシンが必要です。

前提条件

- RDS ホストの仮想マシンが設定されていることを確認します。[8 章 リモート デスクトップ サービス ホストの設定](#)を参照してください。RDS ホストを設定するには、以前に View 接続サーバに登録されていた仮想マシンを使用しないようにしてください。

View Composer のために使用する親仮想マシンは、リンク クローン マシンが参加するドメインと同じ Active Directory ドメインに属するか、ローカルの WORKGROUP のメンバーになる必要があります。

- 仮想マシンが View Composer リンク クローンから変換されたものではないことを確認します。リンク クローンから変換された仮想マシンは、クローンの内部ディスクおよび状態の情報を持っています。親仮想マシンは状態の情報を持つことはできません。

重要: リンク クローンおよびリンク クローンから変換された仮想マシンは、親仮想マシンとしてサポートされません。

- 親仮想マシンに Horizon Agent をインストールするとき、[View Composer Agent] オプションを選択します。[リモート デスクトップ サービス ホストへの Horizon Agent のインストール](#)を参照してください。

大規模な環境で Horizon Agent を更新するには、標準的な Windows 更新メカニズム (Altiris、SMS、LanDesk、BMC などのシステム管理ソフトウェア) を使用できます。再構成操作を使用して Horizon Agent を更新することもできます。

注: 親の仮想マシンで VMware View Composer Guest Agent Server サービスのログイン アカウントを変更しないでください。デフォルトでは、これはローカル システム アカウントです。このアカウントを変更すると、この親から作成されたリンク クローンは起動しなくなります。

- Windows マシンをデプロイするには、ボリューム ライセンス キーを構成し、親仮想マシンのオペレーティング システムをボリューム アクティベーションによってアクティベーションします。[インスタント クローンおよび View Composer リンク クローンでの Windows のアクティベーション](#)を参照してください。
- デバイス ドライバの Windows Update 検索を無効にするための手順を理解しておきます。[http://technet.microsoft.com/en-us/library/cc730606\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc730606(v=ws.10).aspx) にある Microsoft Technet の記事「Disable Searching Windows Update for Device Drivers」を参照してください。
- RDS ホストと負荷分散機能を実装するには、『View 管理』ドキュメントの「RDS ホストの負荷分散の構成」で説明されているように RDS ホストの親仮想マシンを変更します。

手順

- ◆ 親仮想マシンの DHCP リースを削除して、リースされた IP アドレスがファーム内のリンク クローンにコピーされないようにします。

a 親仮想マシンで、コマンド プロンプトを開きます。

b **ipconfig /release** コマンドを入力します。

- ◆ システム ディスクにボリュームが 1 つだけ含まれていることを確認します。

複数のボリュームを含む親仮想マシンからリンク クローンを展開することはできません。View Composer サービスは、複数のディスク パーティションをサポートしていません。複数の仮想ディスクはサポートされていません。

- ◆ 仮想マシンに独立ディスクが含まれていないことを確認します。

仮想マシンのスナップショットを作成するときに、独立ディスクは除外されます。仮想マシンから作成または再構成されたリンク クローンには、独立ディスクは含まれません。

- ◆ 親仮想マシンから作成されたリンク クローン OS ディスクのサイズを減らすには、ハイバネーション オプションを無効にします。

- ◆ 親仮想マシンのスナップショットをとる前に、デバイス ドライバの Windows Update 検索を無効にします。

この Windows 機能は、リンク クローン マシンのカスタマイズに干渉する場合があります。各リンク クローンがカスタマイズされると、Windows はインターネット上でそのクローンの最適なドライバを検索し、検索を繰り返してカスタマイズが遅延する結果となります。

- ◆ vSphere Client で、親仮想マシンの [vApp オプション] 設定を無効にします。

- ◆ Windows Server 2008 R2 および Windows Server 2012 R2 マシンで、未使用の機能を削除することによってディスク領域を確保するスケジュール設定されたメンテナンス作業を無効にします。

例: `Schtasks.exe /change /disable /tn "\Microsoft\Windows\AppxDeploymentClient\Pre-staged app cleanup"`

有効にしておくと、リンク クローンの作成後に、このメンテナンス作業により Sysprep カスタマイズ スクリプトが削除され、後続の再構成操作がカスタマイズ操作のタイムアウト エラーで失敗する可能性があります。詳細については、Microsoft KB の記事 (<http://support.microsoft.com/kb/2928948>) を参照してください。

- ◆ Windows Server 2012 マシンに、<https://support.microsoft.com/en-us/kb/3020396> から入手可能な Microsoft のホットフィックスを適用します。

このホットフィックスによって、Sysprep が RDS のロールが有効になっている Windows Server 2012 仮想マシンをカスタマイズできるようになります。このホットフィックスを適用しないと、自動ファームにデプロイされる Windows Server 2012 リンククローン マシンで Sysprep カスタマイズが失敗します。

次のステップ

vSphere Client または vSphere Web Client を使用して、パワーオフ状態の親仮想マシンのスナップショットを作成します。このスナップショットは、親仮想マシンに関連付けられた最初のリンク クローン マシン セットのための基本状態の構成として使用されます。

重要: スナップショットを作成する前に、ゲスト OS の [シャットダウン] コマンドを使用して、親仮想マシンを完全にシャットダウンします。

リンククローン RDS ホストでの Windows のアクティベーション

View Composer によってリンククローン RDS ホスト上の Windows Server オペレーティング システムの適切なアクティベーションが行われるようにするには、親仮想マシンで Microsoft ポリウム アクティベーションを使用する必要があります。ポリウム アクティベーション テクノロジーにはポリウム ライセンス キーが必要です。

ポリウム アクティベーションによって Windows をアクティベーションするには、キー マネージメント サービス (KMS) を使用します。これには KMS ライセンス キーが必要です。Microsoft 販売代理店に問い合わせ、ポリウム ライセンス キーを取得し、ポリウム アクティベーションを構成してください。

注: View Composer は、マルチプル アクティベーション キー (MAK) ライセンスをサポートしていません。

View Composer でリンク クローン マシンを作成する前に、ポリウム アクティベーションを使用して、親仮想マシンでオペレーティング システムをアクティベーションする必要があります。

リンク クローン マシンが作成されると、リンク クローンが再構成されるたびに、View Composer Agent は親仮想マシンの KMS サーバを使用して、リンク クローンでオペレーティング システムをアクティベーションします。

KMS ライセンスの場合、View Composer は、親仮想マシンをアクティベーションするように構成された KMS サーバを使用します。KMS サーバは、アクティベーション済みのリンク クローンを新しく発行されたライセンスを持つコンピュータとして扱います。

親仮想マシンでの Windows のハイバネーションの無効化

Windows のハイバネーション機能によって、非表示のシステム ファイル `Hiberfil.sys` が作成されます。このファイルは、ハイブリッド スリープに必要な情報を格納するために使用されます。ハイバネーションを無効にすると、インスタント クローンの仮想ディスクまたは View Composer リンク クローンの仮想ディスクのサイズが削減されます。

注意: ハイバネーションを使用不可にすると、ハイブリッド スリープは機能しません。停電が発生した場合は、データが失われる可能性があります。

手順

- 1 vSphere Client で、親仮想マシンを選択し、[コンソールを開く] を選択します。
- 2 管理者としてログインします。

3 ハイバネーション オプションを無効にします。

- a [スタート] をクリックし、[検索の開始] ボックスに「**cmd**」と入力します。
- b 検索結果のリストで、[コマンド プロンプト] を右クリックし、[管理者として実行] をクリックします。
- c [ユーザー アカウント制御] プロンプトで、[続行] をクリックします。
- d コマンド プロンプトで、「**powercfg.exe /hibernate off**」と入力し、Enter キーを押します。
- e 「**exit**」と入力し、Enter キーを押します。

手動ファーム作成用ワークシート

手動ファームを作成するときに、[ファームを追加] ウィザードで特定の設定を構成するように求められます。

このワークシートを印刷し、[ファームを追加] ウィザードを実行するときに指定する値を記入することができます。

表 9-1. ワークシート：手動ファームを作成するための構成設定

設定	説明	値をここに記入
ID	View Administrator でファームを識別する一意の名前。	
説明	このファームの説明。	
アクセス グループ	このファーム内のすべてのプールを含めるアクセス グループ。 アクセス グループの詳細については、『View 管理者ガイド』のロールベースの委任管理に関する章を参照してください。	
デフォルト表示プロトコル	[VMware Blast]、[PCoIP]、または [RDP] を選択します。RDP はデスクトップ プール のみに適用されます。アプリケーション プールの表示プロトコルは、必ず [VMware Blast] または [PCoIP] になります。[RDP] を選択し、このファームを使用してアプリケーション プールをホストする予定であれば、[ユーザーがプロトコルを選択できるようにする] を [はい] に設定する必要があります。デフォルトは、[PCoIP] です。	
ユーザーがプロトコルを選択できるようにする	[はい] または [いいえ] を選択します。この設定は RDS デスクトップ プールにのみ適用されます。[はい] を選択すると、ユーザーは Horizon Client から RDS デスクトップに接続するときに表示プロトコルを選択できます。デフォルトは [はい] です。	
空のセッションのタイムアウト (アプリケーションのみ)	空のアプリケーション セッションが開かれたままにする時間を決定します。アプリケーション セッションで実行されているアプリケーションがすべて閉じられた時点で、そのセッションは空の状態です。セッションが開かれている間、ユーザーはアプリケーションを速やかに開くことができます。空のアプリケーション セッションを切断またはログオフすると、システム リソースを節約できます。タイムアウト値として、[なし] を選択するか、または分単位で数字を設定します。デフォルトは [1 分後] です。	
タイムアウトの発生時	[空のセッションのタイムアウト] 制限に達した時点で空のアプリケーション セッションを切断するか、それともログオフするかを決定します。[切断] または [ログオフ] を選択します。ログオフされたセッションはリソースを解放しますが、アプリケーションを開くのに比較的時間がかかります。デフォルトは [切断] です。	

設定	説明	値をここに記入
切断されたセッションからのログオフ	切断されたセッションをログオフするタイミングを決定します。この設定は、デスクトップセッションとアプリケーションセッションの両方に適用されます。[なし]、[直後]、または [...分後] を選択します。[直後] または [... 分後] の選択は慎重に行ってください。切断されたセッションがログオフされる時点でそのセッションは失われます。デフォルトは [なし] です。	
このファームのデスクトップとアプリケーションへの HTML Access を許可	RDS デスクトップおよびアプリケーションへの HTML Access を許可するかどうかを決定します。[有効にする] ボックスをチェックして、RDS デスクトップおよびアプリケーションへの HTML Access を許可します。ファーム作成後にこの設定を編集すると、新しいデスクトップとアプリケーションだけでなく既存のデスクトップとアプリケーションにも新しい値が適用されます。	

注: 自動ファームとは異なり、手動ファームには [RDS サーバあたりの最大セッション数] 設定がありません。手動ファームでは異なる RDS ホストを設定できるためです。手動ファームの RDS ホストの場合、個々の RDS ホストを編集し、これに相当する設定である [接続数] を変更できます。

自動ファーム作成用ワークシート

自動ファームを作成するときに、[ファームを追加] ウィザードで特定の設定を構成するように求められます。

このワークシートを印刷し、[ファームを追加] ウィザードを実行するときに指定する値を記入することができます。

表 9-2. ワークシート：自動ファームを作成するための構成設定

設定	説明	値をここに記入
ID	View Administrator でファームを識別する一意の名前。	
説明	このファームの説明。	
アクセス グループ	このファーム内のすべてのプールを含めるアクセス グループ。 アクセス グループの詳細については、『View 管理者ガイド』のロールベースの委任管理に関する章を参照してください。	
デフォルト表示プロトコル	[VMware Blast]、[PCoIP]、または [RDP] を選択します。RDP はデスクトップ プール のみに適用されます。アプリケーション プールの表示プロトコルは、必ず [VMware Blast] または [PCoIP] になります。[RDP] を選択し、このファームを使用してアプリケーション プールをホストする予定であれば、[ユーザーがプロトコルを選択できるようにする] を [はい] に設定する必要があります。デフォルトは、[PCoIP] です。	
ユーザーがプロトコルを選択できるようにする	[はい] または [いいえ] を選択します。この設定は RDS デスクトップ プールにのみ適用されます。[はい] を選択すると、ユーザーは Horizon Client から RDS デスクトップに接続するときに表示プロトコルを選択できます。デフォルトは [はい] です。	
空のセッションのタイムアウト (アプリケーションのみ)	空のアプリケーション セッションが開かれたままにする時間を決定します。アプリケーション セッションで実行されているアプリケーションがすべて閉じられた時点で、そのセッションは空の状態です。セッションが開かれている間、ユーザーはアプリケーションを速やかに開くことができます。空のアプリケーション セッションを切断またはログオフすると、システム リソースを節約できます。タイムアウト値として、[なし] を選択するか、または分単位で数字を設定します。デフォルトは [1 分後] です。	

設定	説明	値をここに記入
タイムアウトの発生時	[空のセッションのタイムアウト] 制限に達した時点で空のアプリケーション セッションを切断するか、それともログオフするかを決定します。[切断] または [ログオフ] を選択します。ログオフされたセッションはリソースを解放しますが、アプリケーションを開くの比較的長い時間がかかります。デフォルトは [切断] です。	
切断されたセッションからのログオフ	切断されたセッションをログオフするタイミングを決定します。この設定は、デスクトップセッションとアプリケーションセッションの両方に適用されます。[なし]、[直後]、または [...分後] を選択します。[直後] または [...分後] の選択は慎重に行ってください。切断されたセッションがログオフされる時点でそのセッションは失われます。デフォルトは [なし] です。	
このファームのデスクトップとアプリケーションへの HTML Access を許可	RDS デスクトップおよびアプリケーションへの HTML Access を許可するかどうかを決定します。[有効にする] ボックスをチェックして、RDS デスクトップおよびアプリケーションへの HTML Access を許可します。ファーム作成後にこの設定を編集すると、新しいデスクトップとアプリケーションだけでなく既存のデスクトップとアプリケーションにも新しい値が適用されます。	
RDS サーバあたりの最大セッション数	RDS ホストでサポートできる最大セッション数を指定します。[無制限] または [次の値以下...] を選択します。デフォルトは [無制限] です。	
プロビジョニングを有効にする	このウィザードの完了後にプロビジョニングを有効にするには、このチェックボックスを選択します。デフォルトでは、このボックスは選択されています。	
エラーによりプロビジョニングを停止	プロビジョニング エラーが発生した場合にプロビジョニングを停止するには、このチェックボックスを選択します。デフォルトでは、このボックスは選択されています。	
名前付けパターン	ブリフィックスまたは名前の形式を指定します。View により、1 から始まる自動生成番号が追加または挿入され、マシン名が形成されます。末尾に番号を追加する場合は、ブリフィックスを選択するだけです。それ以外の場合、文字列の任意の場所で [{n}] を指定すると、[{n}] が番号に置き換わります。また、[{n:fixed=<number of digits>}] を指定することもできます。[fixed=<number of digits>] はその番号に使用される桁数を示します。たとえば、[vm-{n:fixed=3}-sales] を指定すると、マシン名は vm-001-sales、vm-002-sales などのようになります。 注: 各マシン名（自動生成番号を含む）には、15 文字の制限があります。	
マシンの最大数	プロビジョニングするマシンの数。	
View Composer のメンテナンス操作中における（プロビジョニング済み）動作可能マシンの最小数	この設定により、View Composer がファームの仮想マシンを再構成している間、接続要求を受け入れることができる仮想マシンの数を指定の数に維持できます。	
vSphere Virtual SAN を使用する	可能な場合、VMware Virtual SAN を使用するかどうかを指定します。Virtual SAN はソフトウェア定義のストレージ階層で、ESXi ホストのクラスタで使用可能なローカル物理ストレージ ディスクを仮想化します。詳細については、 高パフォーマンス ストレージとポリシー ベース管理のための Virtual SAN の使用 を参照してください	
レプリカおよび OS ディスク用に別のデータストアを選択します	(Virtual SAN を使用しない場合のみ使用可能) パフォーマンスなどの理由により、レプリカおよび OS ディスクを別のデータストアに配置できます。	
親仮想マシン	リストから親仮想マシンを選択します。リストには、View Composer Agent がインストールされていない仮想マシンが含まれています。View Composer Agent は必要なので、これらのマシンを選択しないでください。仮想マシンに View Composer Agent がインストールされているかどうかがわかる命名規則を使用することをお勧めします。	

設定	説明	値をここに記入
スナップショット	<p>ファームの基本イメージとして使用する親仮想マシンのスナップショットを選択します。</p> <p>vCenter Server からスナップショットと親仮想マシンを削除しないようにしてください。ただし、ファーム内のリンク クローンがデフォルト イメージを使用せず、このデフォルト イメージから今後リンク クローンを作成することがない場合は削除しても構いません。システムでは、ファーム ポリシーに従ってファーム内に新しいリンク クローンをプロビジョニングするために、親仮想マシンおよびスナップショットが必要です。親仮想マシンとスナップショットは、View Composer の保守作業にも必要です。</p>	
仮想マシンのフォルダの場所	ファームが配置される vCenter Server 内のフォルダを選択します。	
ホストまたはクラスタ	<p>デスクトップ仮想マシンが実行される ESXi ホストまたはクラスタを選択します。</p> <p>Virtual SAN データストア (vSphere 5.5 Update 1 の機能) では、最大 20 個までの ESXi ホストを持つクラスタを選択できます。Virtual Volumes データストア (vSphere 6.0 の機能) では、最大 32 個までの ESXi ホストを持つクラスタを選択できます。</p> <p>vSphere 5.1 以降では、レプリカが VMFS5 以降のデータストアまたは NFS データストアに保存されている場合、最大で 32 台の ESXi ホストでクラスタを選択できます。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。</p> <p>vSphere 5.0 では、レプリカが NFS データストアに保存されている場合、8 を超える ESXi ホストでクラスタを選択できます。レプリカを VMFS データストアに保存する場合、クラスタは最大で 8 つのホストを持つことができます。</p>	
リソース プール	ファームが配置される vCenter Server リソース プールを選択します。	
データストア	<p>ファームを格納するデータストアを 1 つ以上選択します。</p> <p>[ファームを追加] ウィザードの [リンク クローンのデータストアを選択] ページにある表は、ファームのストレージ要件を見積もるための大まかなガイドラインを提供します。これらのガイドラインは、リンク クローン ディスクを格納するための十分な大きさがあるデータストアを特定するのに役立ちます。詳細については、以下を参照してください。 インスタントクローンおよび View Composer リンククローン デスクトップ プールのストレージ サイズ設定。</p> <p>個別の ESXi ホストまたは ESXi クラスタに、共有またはローカル データストアを使用できます。ESXi クラスタでローカル データストアを使用する場合は、デスクトップの展開で課せられる vSphere インフラストラクチャの制約を考慮する必要があります。 ローカル データストアへの View Composer リンク クローンの保存 を参照してください。</p> <p>注: Virtual SAN を使用する場合、データストアを 1 つのみ選択します。</p>	
ストレージ オーバーコミット	<p>各データストアでリンククローンを作成する際のストレージ オーバーコミット レベルを決定します。</p> <p>レベルを高くすると、データストアに割り当てられるリンク クローンの数が増加し、個々のクローンの増大に予約される領域は小さくなります。ストレージ オーバーコミットのレベルを高くすると、データストアの物理ストレージ上限を超える合計論理サイズを持つリンク クローンを作成できます。詳細については、以下を参照してください。 View Composer リンク クローン仮想マシンのストレージ オーバーコミット。</p> <p>注: Virtual SAN を使用する場合、この設定は効果がありません。</p>	

設定	説明	値をここに記入
ネイティブ NFS スナップショット (VAAI) を使用	<p>(Virtual SAN を使用しない場合にのみ使用可能) vStorage APIs for Array Integration (VAAI) をサポートする NAS デバイスが展開内に含まれている場合、ネイティブ 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できません。</p> <p>この機能を使用できるのは、VAAI を介したネイティブ クローン作成操作サポートする NAS デバイスに存在するデータストアを選択した場合だけです。</p> <p>レプリカと OS ディスクを別々のデータストアに格納している場合、この機能は使用できません。領域効率の高いディスクのある仮想マシンでは、この機能は使用できません。</p> <p>この機能は vSphere 5.0 以降でサポートされています。</p> <p>詳細については、以下を参照してください。View Composer リンク クローン用の VAAI ストレージの使用。</p>	
VM ディスク スペースを再利用	<p>(Virtual SAN または Virtual Volumes を使用しない場合にのみ使用可能) ESXi ホストがスペース効率的なディスク形式でフォーマットされたリンク クローンの未使用ディスク領域を再利用できるようにするかどうかを決定します。領域再利用機能により、リンククローン デスクトップに必要なストレージ容量が削減されます。</p> <p>この機能は vSphere 5.1 以降でサポートされています。リンク クローン仮想マシンは、仮想ハードウェア バージョン 9 以降である必要があります。</p> <p>詳細については、以下を参照してください。View Composer リンク クローンでのディスク領域の再利用。</p>	
仮想マシンの未使用領域が次の値を超えると再利用が開始されます。	<p>(Virtual SAN または Virtual Volumes を使用しない場合にのみ使用可能) 領域再利用のトリガとなる、リンククローン OS ディスク上に蓄積する必要がある未使用ディスク領域の最小量 (GB) を入力します。未使用ディスク領域がこのしきい値を超過すると、View は ESXi ホストに OS ディスク上の領域を再利用するように指示する操作を開始します。</p> <p>この値は仮想マシンごとに計測されます。未使用ディスク領域が個々の仮想マシンで指定したしきい値を超過すると、View はそのマシンで領域再利用プロセスを開始します。</p> <p>例 : 2 GB。</p> <p>デフォルト値は 1 GB です。</p>	
停電期間	<p>仮想マシン ディスク領域の再利用が行われない日時を構成します。</p> <p>必要に応じて ESXi のリソースがフォアグラウンド タスク専用になるように、ESXi ホストでこれらの操作を実行しない日時を指定できます。</p> <p>詳細については、以下を参照してください。View Composer リンク クローン用の Storage Accelerator と領域再利用の停電期間の設定。</p>	

設定	説明	値をここに記入
透過的ページ共有の範囲	<p>透過的なページ共有 (TPS) を実行できるレベルを選択します。[仮想マシン] (デフォルト)、[ファーム]、[ポッド]、または [グローバル] から選択します。ファーム、ポッド、またはグローバルですべてのマシンに対して TPS をオンにすると、ESXi ホストは、マシンが同じゲスト OS またはアプリケーションを使用した結果生じるメモリ ページの余分なコピーを取り除きます。</p> <p>ページ共有は ESXi ホストで発生します。たとえば、ファーム レベルで TPS を有効にするが、ファームが複数の ESXi ホストにまたがっている場合、同じホスト上、または同じファーム内の仮想マシンのみがページを共有します。グローバル レベルでは、同じ ESXi ホスト上で View によって管理されているすべてのマシンは、マシンが置かれているファームに関係なく、メモリ ページを共有できます。</p> <p>注: TPS はセキュリティ上のリスクを招く可能性があるため、デフォルト設定ではマシン間でのメモリ ページの共有が行われません。調査では、非常に限定された構成シナリオにおいて、TPS を悪用してデータへの不許可のアクセスを取得できる可能性があることが示されています。</p>	
ドメイン	<p>Active Directory ドメインおよびユーザー名を選択します。</p> <p>View Composer には、ファームに対する特定のユーザー権限が必要です。ドメインおよびユーザー アカウントは、リンククローン マシンをカスタマイズするために Sysprep によって使用されます。</p> <p>このユーザーは、vCenter Server のための View Composer 設定を構成するときに指定します。View Composer 設定を構成する場合は、複数のドメインとユーザーを指定できます。[ファームを追加] ウィザードを使用してファームを作成する場合、リストから 1 つのドメインとユーザーを選択する必要があります。</p> <p>View Composer の構成については、『View 管理』のマニュアルを参照してください。</p>	
AD コンテナ	<p>Active Directory コンテナの相対識別名を指定します。</p> <p>例: CN=Computers</p> <p>[ファームを追加] ウィザードを実行するとき、Active Directory ツリー内のコンテナを参照できます。</p>	
既存のコンピュータ アカウントの再利用を許可	<p>View Composer によってプロビジョニングされたリンク クローンで、Active Directory 内の既存のコンピュータ アカウントを使用するには、この設定を選択します。この設定により、Active Directory で作成されたコンピュータ アカウントを管理できます。</p> <p>リンク クローンがプロビジョニングされたときに、既存の AD コンピュータ アカウント名がリンク クローン マシン名と一致すれば、View Composer は既存のコンピュータ アカウントを使用します。一致しない場合は、新しいコンピュータ アカウントが作成されます。</p> <p>既存のコンピュータ アカウントが、[Active Directory コンテナ] 設定で指定する Active Directory コンテナに配置されている必要があります。</p> <p>この設定が無効になっていると、View Composer がリンク クローンをプロビジョニングするときに、新しい AD コンピュータ アカウントが作成されます。デフォルトでは、この設定は無効になっています。</p> <p>詳細については、以下を参照してください。 リンク クローンに既存の Active Directory コンピュータ アカウントを使用する。</p>	
カスタマイズ仕様 (Sysprep) を使用	<p>仮想マシンをカスタマイズするための Sysprep カスタマイズ仕様を指定します。</p>	

手動ファームの作成

アプリケーションまたは RDS デスクトップにユーザーがアクセスできるようにするプロセスの一部として、手動ファームを作成します。

前提条件

- ファームに属する RDS ホストを設定します。[8 章 リモート デスクトップ サービス ホストの設定](#)を参照してください。
- すべての RDS ホストが使用可能ステータスであることを確認します。View Administrator で、[View 構成] - [登録済みのマシン] を選択し、[RDS ホスト] タブの各 RDS ホストのステータスを確認します。
- ファームを作成するために指定する必要がある構成情報を収集します。[手動ファーム作成用ワークシート](#)を参照してください。

手順

- 1 View Administrator で、[リソース] - [ファーム] をクリックします。
- 2 [追加] をクリックしてワークシートで収集した構成情報を入力します。
- 3 [手動ファーム] を選択します。
- 4 ウィザードの指示に従って、ファームを作成します。

ワークシートで収集した構成情報を使用します。ナビゲーション パネルのページ名をクリックすると、完了したウィザード ページに直接戻ることができます。

- 5 ファームに追加する RDS ホストを選択して、[次へ] をクリックします。
- 6 [終了] をクリックします。

View Administrator で、[リソース] - [ファーム] をクリックすることでファームを表示できるようになりました。

次のステップ

アプリケーション プールまたは RDS デスクトップ プールを作成します。[10 章 アプリケーション プールの作成](#)または [11 章 RDS デスクトップ プールの作成](#)を参照してください。

自動ファームの作成

アプリケーションまたは RDS デスクトップにユーザーがアクセスできるようにするプロセスの一部として、自動ファームを作成します。

前提条件

- View Composer サービスがインストールされていることを確認します。『View インストール ガイド』を参照してください。
- vCenter Server の View Composer 設定が View Administrator で構成されていることを確認します。『View 管理ガイド』を参照してください。

- リモート デスクトップとして使用している仮想マシンに対して使用されている ESXi 仮想スイッチに十分な数のポートがあることを確認します。大規模なデスクトップ プールを作成する場合、デフォルト値では不十分なことがあります。ESXi ホスト上の仮想スイッチ ポートの数は、仮想マシンの数に、仮想マシンあたりの仮想 NIC の数をかけた数以上である必要があります。
- 親仮想マシンを準備したことを確認します。Horizon Agent と View Composer Agent の両方が親仮想マシンにインストールされている必要があります。 [自動ファームの親仮想マシンの準備](#)を参照してください。
- vCenter Server で親仮想マシンのスナップショットを作成します。スナップショットを作成する前に親仮想マシンをシャットダウンする必要があります。View Composer は、クローンを作成するための基本イメージとしてスナップショットを使用します。

注: 仮想マシン テンプレートからリンククローン プールを作成することはできません。

- ファームを作成するために指定する必要がある構成情報を収集します。 [自動ファーム作成用ワークシート](#)を参照してください。

手順

- 1 View Administrator で、[リソース]-[ファーム] をクリックします。
- 2 [追加] をクリックしてワークシートで収集した構成情報を入力します。
- 3 [自動ファーム] を選択します。
- 4 ウィザードの指示に従って、ファームを作成します。

ワークシートで収集した構成情報を使用します。ナビゲーション パネルのページ名をクリックすると、完了したウィザード ページに直接戻ることができます。

View Administrator で、[リソース]-[ファーム] をクリックすることでファームを表示できるようになりました。

次のステップ

アプリケーション プールまたは RDS デスクトップ プールを作成します。 [10 章 アプリケーション プールの作成](#)または [11 章 RDS デスクトップ プールの作成](#)を参照してください。

アプリケーション プールの作成

ユーザーにアプリケーションへのリモート アクセスを提供するための作業の 1 つとして、アプリケーション プールを作成します。アプリケーション プールに対する資格が付与されているユーザーは、さまざまなクライアント デバイスからアプリケーションにリモート アクセスを行うことができます。

この章には、次のトピックが含まれています。

- アプリケーション プール
- アプリケーション プールの手動作成用ワークシート
- アプリケーション プールの作成

アプリケーション プール

アプリケーション プールを使用すると、1 つのアプリケーションを多くのユーザーに配信できます。アプリケーションは RDS ホストのファームで実行されます。

アプリケーション プールを作成する場合、ユーザーがネットワーク上のどこからでもアクセスできるデータセンターにアプリケーションを展開します。アプリケーション プールの概要については、[ファーム](#)、[RDS ホスト](#)、[デスクトップおよびアプリケーション プール](#)を参照してください。

アプリケーション プールには 1 つのアプリケーションがあり、1 つのファームと関連付けられています。エラーを避けるため、ファームのすべての RDS ホストにアプリケーションをインストールする必要があります。

View では、アプリケーション プールを作成すると、ファームのすべての RDS ホストの [スタート] メニューから、(個々のユーザーではなく) すべてのユーザーが使用可能なアプリケーションが自動的に表示されます。リストから 1 つ以上のアプリケーションを選択できます。リストから複数のアプリケーションを選択すると、アプリケーションごとに個別のアプリケーション プールが作成されます。リストにないアプリケーションを手動で指定することもできます。手動で指定するアプリケーションがまだインストールされていない場合、View に警告メッセージが表示されます。

アプリケーション プールを作成する際、プールを配置するアクセス グループは指定できません。アプリケーション プールと RDS デスクトップ プールについては、ファームの作成時にアクセス グループを指定します。

アプリケーションは PColP および VMware Blast 表示プロトコルをサポートします。HTML Access を有効にするには、https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html から利用できる『HTML Access の使用』ドキュメントの「セットアップとインストール」の章の「HTML Access のためのデスクトップ、プール、ファームの準備」を参照してください。

アプリケーション プールの手動作成用ワークシート

アプリケーション プールを作成して手動でアプリケーションを指定する際、[アプリケーション プールを追加] ウィザードからアプリケーションに関する情報を入力するよう求められます。RDS ホストにアプリケーションをインストールしておく必要はありません。

このワークシートを印刷し、アプリケーションを手動で指定するときのアプリケーションのプロパティを書き留めることができます。

表 10-1. ワークシート：アプリケーション プールを手動で作成するためのアプリケーションのプロパティ

プロパティ	説明	値をここに記入
ID	View Administrator でプールを識別する一意の名前。 このフィールドは必須です。	
表示名	Horizon Client にログインする際にユーザーに表示されるプール名。表示名を指定しない場合は、[ID] と同じになります。	
バージョン	アプリケーションのバージョン。	
パブリッシャ	アプリケーションのパブリッシャ。	
パス	アプリケーションのフル パス名。例：C:\Program Files\app1.exe。このフィールドは必須です。	
開始フォルダ	アプリケーションの開始ディレクトリのフル パス名。	
パラメータ	アプリケーションの起動時にアプリケーションに渡すパラメータ。たとえば、-username user1 -loglevel 3 を指定できます。	
説明	このアプリケーション プールの説明。	

アプリケーション プールの作成

RDS ホストで動作するアプリケーションにユーザーがアクセスできるようにする処理の一部として、アプリケーション プールを作成します。

前提条件

- RDS ホストをセットアップします。[8 章 リモート デスクトップ サービス ホストの設定](#)を参照してください。
- それらの RDS ホストが含まれるファームを作成します。[9 章 ファームの作成](#)を参照してください。
- アプリケーション プールを手動で追加する場合は、アプリケーションについての情報を収集します。[アプリケーション プールの手動作成用ワークシート](#)を参照してください。

手順

- 1 View Administrator で、[カタログ] - [アプリケーション プール] をクリックします。
- 2 [追加] をクリックします。

3 ウィザードの指示に従って、プールを作成します。

アプリケーション プールを手動で追加することを選択する場合は、ワークシートで収集した構成情報を使用します。View Administrator が表示するリストからアプリケーションを選択する場合は、複数のアプリケーションを選択できます。アプリケーションごとに個別のプールが作成されます。

View Administrator で、[カタログ] - [アプリケーション プール] をクリックしてアプリケーション プールを確認できます。

次のステップ

プールにアクセスするための資格をユーザーに付与します。[13 章 資格のあるユーザーとグループ](#)を参照してください。

RDS アプリケーションのサポートに必要な Horizon Client 3.0 以降のソフトウェアにエンド ユーザーがアクセスできることを確認します。

アプリケーションを実行できる十分なリソースがある RDS ホストでのみ View 接続サーバがアプリケーションを起動するように限定するには、アプリケーション プールに非アフィニティ ルールを構成します。詳細については、『View 管理』ドキュメントの「アプリケーション プールのアンチアフィニティ ルールの構成」を参照してください。

RDS デスクトップ プールの作成

ユーザーにセッション ベース デスクトップへのリモート アクセスを提供するための作業の 1 つとして、リモート デスクトップ サービス (RDS) デスクトップ プールを作成します。RDS デスクトップ プールにより、リモート デスクトップ展開のいくつかの具体的なニーズを満たすことができます。

この章には、次のトピックが含まれています。

- RDS デスクトップ プールの概要
- RDS デスクトップ プールの作成
- RDS デスクトップ プールのデスクトップ プール設定
- Adobe Flash のスロットルを RDS デスクトップ プール用に Internet Explorer で構成する

RDS デスクトップ プールの概要

RDS デスクトップ プールは、作成可能な 3 種類のデスクトップ プールのうちの 1 つです。このタイプのプールは、以前の View リリースでは Microsoft Terminal Services プールと呼ばれていました。

RDS デスクトップ プールおよび RDS デスクトップには次の特徴があります。

- RDS デスクトップ プールは RDS ホストのグループであるファームと関連付けられます。各 RDS ホストは複数の RDS デスクトップをホストすることができる Windows サーバです。
- RDS デスクトップは RDS ホストへのセッションに基づきます。これに対し、自動デスクトップ プール内のデスクトップは仮想マシンに基づき、手動デスクトップ プール内のデスクトップは仮想マシンまたは物理マシンに基づきます。
- RDS デスクトップは RDP、PCoIP、および VMware Blast 表示プロトコルをサポートします。HTML Access を有効にするには、https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html から利用できる『HTML Access の使用』ドキュメントの「セットアップとインストール」の章の「HTML Access のためのデスクトップ、プール、ファームの準備」を参照してください。
- RDS デスクトップ プールは、RDS ロールをサポートし、View によりサポートされる Windows Server オペレーティングシステムでのみサポートされます。『View のインストール』の「ゲスト OS のシステム要件」を参照してください。
- View は、接続要求をアクティブなセッションの数が最小の RDS ホストに転送することによって、ファーム内の RDS ホストの負荷分散を提供します。
- RDS デスクトップ プールはセッションベースのデスクトップを提供するため、更新、再構成、再分散のような、リンク クローン デスクトップ プールに特有な操作はサポートされません。

- RDS ホストが vCenter Server により管理される仮想マシンの場合、基本イメージとしてスナップショットを使用できます。vCenter Server を使用してスナップショットを管理できます。RDS ホストの仮想マシンでのスナップショットの使用は、View に対して透過的です。
- RDS デスクトップは View Persona Management をサポートしません。
- HTML Access では、コピーおよび貼り付け機能がデフォルトで無効になっています。この機能を有効にするには、https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html で公開されている『HTML Access の使用』ドキュメントの「エンド ユーザー用に HTML Access を構成」の「HTML Access グループ ポリシー設定」を参照してください。

RDS デスクトップ プールの作成

RDS デスクトップへのアクセス権をユーザーに付与するプロセスの一環として、RDS デスクトップ プールを作成します。

前提条件

- RDS ホストをセットアップします。[8 章 リモート デスクトップ サービス ホストの設定](#)を参照してください。
- それらの RDS ホストが含まれるファームを作成します。[9 章 ファームの作成](#)を参照してください。
- プール設定の構成方法を決定します。[RDS デスクトップ プールのデスクトップ プール設定](#)を参照してください。

手順

- 1 View Administrator で、[カタログ] - [デスクトップ プール] を選択します。
- 2 [追加] をクリックします。
- 3 [RDS デスクトップ プール] を選択します。
- 4 プール ID、表示名、および説明を指定します。

プール ID は、View Administrator でプールを識別する一意の名前です。表示名は、ユーザーが Horizon Client にログインするときに表示される RDS デスクトップ プールの名前です。表示名を指定しない場合は、表示名はプール ID と同じになります。

- 5 プール設定を選択します。
- 6 このプールのファームを選択または作成します。

View Administrator で、[カタログ] - [デスクトップ プール] を選択すると、RDS デスクトップ プールを表示できます。

次のステップ

プールにアクセスするための資格をユーザーに付与します。[デスクトップまたはアプリケーション プールへの資格の追加](#)を参照してください。

エンド ユーザーが Horizon Client 3.0 以降のソフトウェアにアクセスできることを確認します。これは RDS デスクトップ プールをサポートするために必要です。

RDS デスクトップ プールのデスクトップ プール設定

RDS デスクトップ プールの作成時に特定のプール設定を指定できます。すべてのプール設定がすべての種類のデスクトップ プールに適用されるわけではありません。

すべてのプール設定の説明については、[すべてのデスクトップ プール タイプのデスクトップ プール設定](#)を参照してください。次のプール設定が RDS デスクトップ プールに適用されます。

表 11-1. RDS デスクトップ プールの設定

設定	デフォルト値
状態	有効
接続サーバ restrictions (接続サーバの制限)	なし
Adobe Flash quality (Adobe Flash の品質)	制御しない
Adobe Flash throttling (Adobe Flash のスロットル)	無効

Adobe Flash のスロットルを RDS デスクトップ プール用に Internet Explorer で構成する

RDS デスクトップで Adobe Flash のスロットルが Internet Explorer で確実に動作するようにするには、ユーザーがサード パーティ製のブラウザ拡張を有効にする必要があります。

手順

- 1 Horizon Client を起動し、ユーザーのデスクトップにログインします。
- 2 Internet Explorer で、[ツール] - [インターネット オプション] をクリックします。
- 3 [詳細設定] タブをクリックし、[サード パーティ製のブラウザ拡張を有効にする] を選択して、[OK] をクリックします。
- 4 Internet Explorer を再起動します。

デスクトップ プールのプロビジョニング

12

デスクトップ プールを作成するときに、プールの管理方法およびユーザーのデスクトップ操作方法を決定する構成オプションを選択します。

これらのプロビジョニング タスクは、シングルユーザー マシン上に展開されるデスクトップ プールに適用されます。RDS デスクトップ プールには適用されません。ただし、Adobe Flash の品質とスロットル設定は、RDS を含むすべてのタイプのデスクトップ プールに適用されます。

この章には、次のトピックが含まれています。

- [デスクトップ プールでのユーザー割り当て](#)
- [マシンの手動での名前付けまたは名前付けパターンの指定](#)
- [マシンの手動でのカスタマイズ](#)
- [すべてのデスクトップ プール タイプのデスクトップ プール設定](#)
- [Adobe Flash の品質とスロットル](#)
- [デスクトップ プールの電源ポリシーの設定](#)
- [デスクトップ用の 3D レンダリングの構成](#)
- [View デスクトップへの RDP を使用したアクセスの防止](#)
- [大規模なデスクトップ プールの展開](#)

デスクトップ プールでのユーザー割り当て

フル仮想マシンまたは View Composer リンク クローンの手動デスクトップ プールおよび自動デスクトップ プールの場合は、デスクトップのユーザー割り当てについて流動または専用ユーザー割り当てを選択できます。インスタントクローン デスクトップ プールの場合は、流動ユーザー割り当てのみを選択できます。

専用割り当ての場合、各デスクトップが特定のユーザーに割り当てられます。初めてログインしたユーザーは、別のユーザーに割り当てられていないデスクトップを受け取ります。その後、このユーザーはログインすると必ずこのデスクトップを受け取り、他のユーザーがこのデスクトップを使うことはできません。

流動割り当ての場合、ユーザーはログインするたびにランダムなデスクトップを受け取ります。ユーザーがログオフすると、デスクトップはプールに戻されます。

インスタント クローンでは、ユーザーのログアウト時に必ずデスクトップが現在のイメージから削除され、再作成されます。View Composer リンク クローンでは、ユーザーのログアウト時に流動割り当てマシンが削除されるように構成できます。自動削除を使用すると、同時に必要な数だけ仮想マシンを保持できます。

流動割り当てを使用すると、ソフトウェア ライセンス コストを削減できる場合があります。

マシンの手動での名前付けまたは名前付けパターンの指定

フル仮想マシンまたは View Composer リンク クローンの自動デスクトップ プールを使用すると、デスクトップ マシンの名前のリストを指定するか、名前付けパターンを指定することができます。インスタントクローン デスクトップ プールを使用すると、プールのプロビジョニング時に名前付けパターンのみを指定できます。

リストを指定してマシンに名前を付ける場合は、会社の名前付け方式を使用し、各マシン名とユーザーとを関連付けることができます。

名前付けパターンを指定する場合、View ではユーザーが必要とするときに動的にマシンを作成して割り当てることができます。

表 12-1. マシンの手動での名前付けまたはマシン名前付けパターンの指定 では、2 つの名前付け方法を比較し、それぞれの方法がデスクトップ プールの作成および管理方法にどのような影響を及ぼすかを示します。

表 12-1. マシンの手動での名前付けまたはマシン名前付けパターンの指定

機能	マシン名前付けパターンの使用	マシンの手動での名前付け
マシン名	マシン名は、番号を名前付けパターンに付加することで、生成されます。 詳細については、 自動デスクトップ プールでの名前付けパターンの使用 を参照してください。	管理者がマシン名のリストを指定します。 専用割り当てプールでは、ユーザー名とマシン名を列挙してユーザーとマシンを関連付けることができます。 詳細については、 マシン名のリストの指定 を参照してください。
プール サイズ	管理者がマシンの最大数を指定します。	マシン名のリストによってマシンの数が決まります。
プールにマシンを追加する場合	最大プール サイズを増やすことができます。	リストにマシン名を追加できます。 詳細については、 名前のリストによってプロビジョニングされる自動プールへのマシンの追加 を参照してください。
オンデマンド プロビジョニング	利用可能。 View は、ユーザーが初めてログインするとき、または管理者がユーザーにマシンを割り当てるときに、指定されている最小数およびスベア数のマシンを動的に作成してプロビジョニングします。 View は、管理者がプールを作成するときにも、すべてのマシンを作成してプロビジョニングできます。	利用不可。 View は、プールが作成されたときに、リストに指定されたすべてのマシンを作成してプロビジョニングします。
初期カスタマイズ	利用可能。 マシンのプロビジョニング時に、View は選択されたカスタマイズ仕様を実行できます。	利用可能。 マシンのプロビジョニング時に、View は選択されたカスタマイズ仕様を実行できます。

機能	マシン名前付けパターンの使用	マシンの手動での名前付け
専用マシンの手動カスタマイズ	<p>インスタント クローンでは利用不可。</p> <p>マシンをカスタマイズし、ユーザーがマシンにアクセスできるようにするには、各マシンの所有権を削除し、再度割り当てる必要があります。初回のログイン時にマシンを割り当てるかどうかによって、これらの手順の実行が 2 回必要になる場合があります。メンテナンス モードではマシンを起動できません。プールが作成された後、マシンを手動でメンテナンス モードにすることができます。</p>	<p>所有権を再度割り当てなくても、マシンをカスタマイズしてテストできます。</p> <p>プールを作成するとき、すべてのマシンをメンテナンス モードで起動して、ユーザーがアクセスできないようにすることができます。マシンをカスタマイズしたら、メンテナンス モードを終了してユーザーがアクセスできるようにします。詳細については、マシンの手動でのカスタマイズを参照してください。</p>
動的または固定プール サイズ	<p>動的。</p> <p>専用割り当てプール内のマシンからユーザー割り当てを削除した場合、マシンは使用可能なマシンのプールに返されます。</p> <p>流動割り当てプールでログオフ時にマシンを削除することを選択した場合は、プール サイズがアクティブなユーザー セッションの数に応じて拡大または縮小することがあります。</p> <p>注: インスタントクローン プールは、流動割り当てプールのみに設定できます。マシンはログオフ時に必ず削除されます。</p>	<p>固定。</p> <p>プールには、マシン名のリストで指定した数のマシンが含まれます。</p> <p>マシンに手動で名前を付けた場合は、[ログオフ時にマシンを削除する] の設定を選択できません。</p>
スベア マシン	<p>View が新しいユーザーのためにパワーオン状態を維持しておくスベア マシンの数を指定できます。</p> <p>View は、指定された数を維持するために新しいマシンを作成します。最大プール サイズに達すると、View はスベア マシンの作成を停止します。</p> <p>View は、プールの電源ポリシーが [パワーオフ] または [サスペンド] に設定されている場合、または電源ポリシーが設定されていない場合でも、スベア マシンをパワーオン状態で維持します。</p> <p>注: インスタントクローン プールには、電源ポリシーがありません。</p>	<p>View が新しいユーザーのためにパワーオン状態を維持しておくスベア マシンの数を指定できます。</p> <p>View は、指定された数を維持するための新しいスベア マシンを作成しません。</p> <p>View は、プールの電源ポリシーが [パワーオフ] または [サスペンド] に設定されている場合、または電源ポリシーが設定されていない場合でも、スベア マシンをパワーオン状態で維持します。</p>
ユーザー割り当て	<p>専用割り当ておよび流動割り当てプールに対して名前付けパターンを使用できます。</p> <p>注: インスタントクローン プールは、流動割り当てプールのみに設定できます。</p>	<p>専用割り当ておよび流動割り当てプールに対してマシン名を指定できます。</p> <p>注: 流動割り当てプールでは、ユーザー名をマシン名に関連付けることはできません。マシンは、関連付けられたユーザー専用ではありません。流動割り当てプールでは、ログインするユーザーは、現在使用されていないすべてのマシンにアクセスできます。</p>

マシン名のリストの指定

マシン名のリストを手動で指定して、自動デスクトップ プールをプロビジョニングすることができます。この命名方法では、会社の命名規則を使用してプール内のマシンを識別することができます。

マシン名を明示的に指定すると、ユーザーには、リモート デスクトップへのログイン時に会社の組織に基づくわかりやすい名前が表示されます。

マシン名を手動で指定するには、次のガイドラインに従います。

- 各マシン名は個別の行に入力します。
- マシン名には、最大 15 文字の英数字を使用できます。
- 各マシン エントリにユーザー名を追加できます。カンマを使用して、ユーザー名とマシン名を区切ります。

この例では、2 つのマシンが指定されています。2 番目のマシンはユーザーに関連付けられています。

```
Desktop-001
Desktop-002,abccorp.com\jdoe
```

注: 流動割り当てプールでは、ユーザー名をマシン名に関連付けることはできません。マシンは、関連付けられたユーザー専用ではありません。流動割り当てプールでは、ログインするユーザーは、現在使用されていないすべてのマシンにアクセスできます。

前提条件

各マシンの名前が一意であることを確認します。vCenter Server の既存の仮想マシンの名前を使用することはできません。

手順

- 1 マシン名のリストを含むテキスト ファイルを作成します。

少数のマシンを含むデスクトップ プールを作成する場合は、マシン名を直接 [デスクトップ プールを追加] ウィザードに入力できます。別のテキスト ファイルを作成する必要はありません。

- 2 View Administrator で [デスクトップ プールを追加] ウィザードを起動して、自動デスクトップ プールの作成を開始します。

- 3 プロビジョニングの設定ページで [名前を手動で指定] を選択し、[名前を入力] をクリックします。

- 4 [マシン名を入力] ページにマシン名のリストをコピーし、[次へ] をクリックします。

[マシン名を入力] ウィザードにデスクトップのリストが表示され、検証エラーが赤い [!] で示されます。

- 5 無効なマシン名を修正します。

a カーソルを無効な名前の上に置くと、ページの下部に関連するエラー メッセージが表示されます。

b [戻る] をクリックします。

c 正しくない名前を編集し、[次へ] をクリックします。

- 6 [終了] をクリックします。

- 7 (オプション) [メンテナンス モードでマシンを開始] を選択します。

このオプションにより、ユーザーがログインして使用する前にマシンをカスタマイズできます。

- 8 ウィザードの指示に従って、デスクトップ プールの作成を終了します。

View で、リスト内の名前ごとに 1 つのマシンが作成されます。エントリにマシンとユーザー名が含まれている場合、View により、そのユーザーにマシンが割り当てられます。

デスクトップ プールの作成後、追加のマシン名およびユーザーを含む別のリスト ファイルをインポートしてマシンを追加できます。『View 管理』の「名前のレストランによってプロビジョニングされる自動プールへのマシンの追加」を参照してください。

自動デスクトップ プールでの名前付けパターンの使用

名前付けパターンとプール内で必要なマシンの総数を指定して、プール内のマシンをプロビジョニングすることができます。デフォルトでは、View は、パターンをすべてのマシン名のプレフィックスとして使用し、一意の番号を付加して各マシンを識別します。

マシン名の名前付けパターンの長さ

マシン名の文字数の上限は、名前付けパターンと自動的に生成される番号も含めて 15 文字です。

表 12-2. マシン名の名前付けパターンの最大の長さ

プールで設定するマシンの数	プレフィックスの最大長
1 ~ 99	13 文字
100 ~ 999	12 文字
1,000 以上	11 文字

固定長トークンを含む名前では、長さの上限が異なります。[固定長トークンを使用する場合の名前付けパターンの長さ](#)を参照してください。

マシン名でのトークンの使用

トークンを使用して、自動生成された番号を名前に付加できます。プール名を入力するとき、トークンを指定するには「{n}」と入力します。

たとえば、「**amber-{n}-desktop**」と入力します。

マシンを作成するときに、View は **{n}** を一意の番号に置き換えます。

「**{n:fixed=桁数}**」と入力すると、固定長トークンを生成できます。

View は、トークンを指定された桁数を含む番号に置き換えます。

たとえば、「**amber-{n:fixed=3}**」と入力した場合、View は **{n:fixed=3}** を 3 桁の番号に置き換え、**amber-001**、**amber-002**、**amber-003** のようなマシン名を作成します。

固定長トークンを使用する場合の名前付けパターンの長さ

固定長トークンを含む名前の文字数の上限は、名前付けパターンとトークンの桁数も含めて 15 文字です。

表 12-3. 固定長トークンを使用する場合の名前付けパターンの最大長

固定長トークン	名前付けパターンの最大長
{n:fixed=1}	14 文字
{n:fixed=2}	13 文字
{n:fixed=3}	12 文字

マシンの名前付けの例

この例は、マシン名が同じで番号は異なる 2 つの自動デスクトップ プールを作成する方法を示しています。この例で使用する方法は、個別のユーザー目的を達成し、マシンの名前付け方法の柔軟性を示します。

目的は、VDIABC-XX などの同じ命名規則を使用する 2 つのプールを作成することです。ここで、XX は番号を表します。各プールは異なる連続番号を持ちます。たとえば、最初のプールにはマシン VDIABC-01 から VDIABC-10 が含まれます。2 つ目のプールにはマシン VDIABC-11 から VDIABC-20 が含まれます。

いずれかのマシンの名前付け方法を使用して、この目的を達成できます。

- マシンの固定セットを一度に作成するには、マシン名を手動で指定します。
- ユーザーが初めてログインするときに動的にマシンを作成するには、名前付けパターンを提供し、トークンを使用して連続番号を指定します。

手動での名前の指定

- 1 VDIABC-01 から VDIABC-10 のマシン名のリストを含む最初のプール用のテキスト ファイルを準備します。
- 2 View Administrator でプールを作成し、マシン名を手動で指定します。
- 3 [名前を入力] をクリックし、リストを [マシン名を入力] リスト ボックスにコピーします。
- 4 VDIABC-11 から VDIABC-20 の名前を使用して、2 つ目のプールに対してこれらの手順を繰り返します。

詳しい手順については、[マシン名のリストの指定](#)を参照してください。

各プールの作成後、マシンを追加できます。たとえば、最初のプールにマシン VDIABC-21 から VDIABC-30 を追加し、2 つ目のプールに VDIABC-31 から VDIABC-40 を追加できます。[名前のリストによってプロビジョニングされる自動プールへのマシンの追加](#)を参照してください。

トークンを含む名前パターンの提供

- 1 View Administrator で、最初のプールを作成し、名前付けパターンを使用してマシン名をプロビジョニングします。
- 2 名前付けパターンのテキスト ボックスに、「**VDIABC-0{n}**」と入力します。
- 3 プールの最大サイズを 9 に制限します。
- 4 2 つ目のプールに対してこれらの手順を繰り返しますが、名前付けパターンのテキスト ボックスには「**VDIABC-1{n}**」と入力します。

最初のプールにはマシン VDIABC-01 から VDIABC-09 が含まれます。2 つ目のプールにはマシン VDIABC-11 から VDIABC-19 が含まれます。

または、2 桁の固定長トークンを使用して、プールをそれぞれ最大 99 のマシンを含むように構成できます。

- 最初のプールに対して、「**VDIABC-0{n:fixed=2}**」と入力します。
- 2 つ目のプールに対して、「**VDIABC-1{n:fixed=2}**」と入力します。

各プールの最大サイズを 99 に制限します。この構成により、3 桁の連続名パターンを含むマシンが作成されます。

最初のプール：

```
VDIABC-001
VDIABC-002
VDIABC-003
```

2 つ目のプール：

```
VDIABC-101
VDIABC-102
VDIABC-103
```

名前付けパターンおよびトークンの詳細については、[自動デスクトップ プールでの名前付けパターンの使用](#)を参照してください。

名前のリストによってプロビジョニングされる自動プールへのマシンの追加

手動でマシン名を指定してプロビジョニングされる自動デスクトップ プールにマシンを追加するには、新しいマシン名の別のリストを指定します。この機能により、デスクトップ プールを拡大しても、会社の命名規則を引き続き使用できます。

Horizon 7.0 では、インスタント クローンのこの機能はサポートされていません。

マシン名を手動で追加するには、次のガイドラインに従います。

- 各マシン名は個別の行に入力します。
- マシン名には、最大 15 文字の英数字を使用できます。
- 各マシン エントリにユーザー名を追加できます。カンマを使用して、ユーザー名とマシン名を区切ります。

この例では、2 つのマシンが追加されています。2 番目のマシンはユーザーに関連付けられています。

```
Desktop-001
Desktop-002,abccorp.com/jdoe
```

注： 流動割り当てプールでは、ユーザー名をマシン名に関連付けることはできません。マシンは、関連付けられたユーザー専用ではありません。流動割り当てプールでは、ログインするユーザーは、現在使用されていないすべてのマシンにアクセスできます。

前提条件

マシン名を手動で指定してデスクトップ プールを作成したことを確認します。名前付けパターンを指定してプールを作成した場合は、新しいマシン名を指定することによってマシンを追加することはできません。

手順

- 1 追加のマシン名のリストを含むテキスト ファイルを作成します。

少数のマシンのみを追加する場合は、[デスクトップ プールを追加] ウィザードでマシン名を直接入力できます。別のテキスト ファイルを作成する必要はありません。

- 2 View Administrator で、[カタログ]-[デスクトップ プール]を選択します。

- 3 展開するデスクトップ プールを選択します。
- 4 [編集] をクリックします。
- 5 [プロビジョニングの設定] タブをクリックします。
- 6 [マシンを追加] をクリックします。
- 7 [マシン名を入力] ページにマシン名のリストをコピーし、[次へ] をクリックします。
[マシン名を入力] ウィザードによってマシンのリストが表示され、検証エラーが赤い [X] で示されます。
- 8 無効なマシン名を修正します。
 - a カーソルを無効な名前の上に置くと、ページの下部に関連するエラー メッセージが表示されます。
 - b [戻る] をクリックします。
 - c 正しくない名前を編集し、[次へ] をクリックします。
- 9 [終了] をクリックします。
- 10 [OK] をクリックします。

vCenter Server で、新しい仮想マシンの作成を監視できます。

View Administrator で、[カタログ] - [デスクトップ プール] を選択すると、デスクトップ プールに追加されているとおりにマシンを表示できます。

マシンの手動でのカスタマイズ

自動プールを作成した後、所有権を再度割り当てることなく特定のマシンをカスタマイズできます。メンテナンス モードでマシンを起動することによって、ユーザーにリリースする前にマシンを変更およびテストできます。

注: この機能は、インスタントクローン デスクトップ プールでは使用できません。

メンテナンス モードでのマシンのカスタマイズ

メンテナンス モードでは、ユーザーはデスクトップにアクセスできません。マシンをメンテナンス モードで起動した場合、View は、マシンが作成されると各マシンをメンテナンス モードにします。

専用割り当てプールでは、自分の管理者アカウントに所有権を再度割り当てなくても、メンテナンス モードを使用してマシンにログインできます。カスタマイズの終了後、マシンに関連付けられているユーザーに所有権を返す必要はありません。

流動割り当てプールでは、ユーザーにログインを許可する前に、メンテナンス モードでマシンをテストできます。

自動プール内のすべてのマシンで同じカスタマイズを実行するには、テンプレートまたは親として準備する仮想マシンをカスタマイズします。View は、すべてのマシンにカスタマイズを展開します。プールを作成するときに、Sysprep カスタマイズ仕様を使用して、すべてのマシンをライセンス情報、ドメインへの関連付け、DHCP 設定などのコンピュータ プロパティを使って構成することもできます。

注: マシンをメンテナンス モードで起動できるのは、名前付けパターンを指定してマシンに名前を付ける場合ではなく、プールのマシン名を手動で指定する場合です。

個別マシンのカスタマイズ

マシンをメンテナンス モードで起動して、プールの作成後に個別マシンをカスタマイズすることができます。

手順

- 1 View Administrator で、[デスクトップ プールを追加] ウィザードを起動して自動デスクトップ プールの作成を開始します。
- 2 プロビジョニングの設定ページで [名前を手動で指定] を選択します。
- 3 [メンテナンス モードでマシンを開始] を選択します。
- 4 [デスクトップ プールを追加] ウィザードを終了して、デスクトップ プールの作成を終了します。
- 5 vCenter Server で、個別仮想マシンにログインし、カスタマイズしてテストします。
マシンは、手動でカスタマイズすることも、Altiris、SMS、LanDesk、BMC などの標準の Windows システム管理ソフトウェアを使用してカスタマイズすることもできます。
- 6 View Administrator で、デスクトップ プールを選択します。
- 7 フィルタ ツールを使用してユーザーにリリースする特定のマシンを選択します。
- 8 [その他のコマンド] - [メンテナンス モードを終了] をクリックします。

次のステップ

デスクトップにログインできることをユーザーに通知します。

すべてのデスクトップ プール タイプのデスクトップ プール設定

フル仮想マシン、リンク クローン デスクトップ プール、手動デスクトップ プール、インスタントクローン デスクトップ プール、および RDS デスクトップ プールを含む自動プールを構成するときには、マシンとデスクトップ プールの設定を指定する必要があります。すべての設定がすべての種類のデスクトップ プールに適用されるわけではありません。

表 12-4. デスクトップ プールの設定オプション

設定	オプション
状態	<ul style="list-style-type: none"> ■ [有効化]: デスクトップ プールは作成後に有効になり、すぐに使用できます。 ■ [無効化]: デスクトップ プールは作成後に無効になり、使用できません。またプールのプロビジョニングも停止します。展開後にテストなどの標準メンテナンスのような作業を行う場合にはこの設定が適しています。 <p>この状態が有効の場合、リモート デスクトップは使用できません。</p>
接続サーバ restrictions (接続サーバの制限)	<ul style="list-style-type: none"> ■ [なし]。デスクトップ プールには、すべての接続サーバ インスタンスがアクセスできます。 ■ [タグ付き]: 1 つ以上の接続サーバ タグを選択して、これらのタグを持つ接続サーバ インスタンスのみがデスクトップ プールにアクセスできるようにします。チェック ボックスを使用して複数のタグを選択できます。 <p>VMware Identity Manager からデスクトップへのアクセスを提供することを意図して接続サーバ制限を構成すると、これらのデスクトップが実際には制限されている場合でも VMware Identity Manager アプリケーションでユーザーにデスクトップが表示されることがあります。VMware Identity Manager ユーザーはこれらのデスクトップを起動できません。</p>

設定	オプション
リモート マシンの電源ポリシー	<p>関連付けられたデスクトップからユーザーがログオフするときの仮想マシンの動作方法を決定します。</p> <p>電源ポリシー オプションの詳細については、デスクトップ プールの電源ポリシーを参照してください。</p> <p>電源ポリシーが自動プールに与える影響の詳細については、デスクトップ プールの電源ポリシーの設定を参照してください。</p> <p>インスタント クローン デスクトップ プールには適用されません。インスタント クローンは常にパワーオンされています。</p>
Automatically logoff after disconnect (切断後に自動的にログオフ)	<ul style="list-style-type: none"> ■ [直後] : ユーザーが接続を切断すると、すぐにログオフされます。 ■ [なし] : ユーザーはログオフされません。 ■ [時間が経過した後] : ユーザーが接続を切断してからこの時間が経過すると、ログオフされます。時間は分単位で入力します。 <p>ログオフ時間は今後の切断時に適用されます。ログオフ時間を設定したときにデスクトップ セッションがすでに切断されていた場合、そのユーザーのログオフ経過時間の開始は、ログオフ時間を設定したときとなり、セッションが最初に切断されたときではありません。たとえば、この値を 5 分に設定した場合に、セッションが 10 分前に切断されたとすると、そのセッションは値を設定してから 5 分後に View でログオフされます。</p>
ユーザーによるマシンのリセットを許可	<p>ユーザーによるデスクトップのリセットを許可します。</p> <p>インスタント クローン デスクトップ プールには適用されません。</p>
ユーザーが複数のクライアント デバイスからセッションを個別に開始できるようにする	<p>この設定が選択されている場合、複数のクライアント デバイスから同じデスクトップ プールに接続しているユーザーは複数のデスクトップ セッションを取得します。ユーザーが既存セッションに再接続するには、このセッションを開始したクライアント デバイスから行う必要があります。この設定が選択されていない場合、ユーザーは使用しているクライアント デバイスに関係なく、自身の既存セッションに再接続できます。</p>
ログオフ後にマシンを削除	<p>流動割り当て、フル仮想マシンを削除するかどうかを選択します。</p> <ul style="list-style-type: none"> ■ [[いいえ]]仮想マシンは、ユーザーのログオフ後にデスクトップ プールに残ります。 ■ [[はい]]仮想マシンは、ユーザーがログオフするとすぐにパワーオフされて削除されます。 <p>インスタントクローンの場合、ログオフ後に必ずマシンが削除され、再作成されます。</p>
ログオフ時にマシンを削除または更新	<p>流動割り当てのリンク クローン仮想マシンを削除するか、更新するか、またはそのまま残すかを選択します。</p> <ul style="list-style-type: none"> ■ [なし] : 仮想マシンは、ユーザーのログオフ後にデスクトップ プールに残り、更新されません。 ■ [すぐに削除] : 仮想マシンは、ユーザーがログオフするとすぐにパワーオフされて削除されます。ユーザーがログオフすると、仮想マシンはただちに削除中状態になります。 ■ [すぐに更新] : 仮想マシンは、ユーザーがログオフするとすぐに更新されます。ユーザーがログオフすると、仮想マシンはただちにメンテナンス モードになります。これは、更新操作の開始時に他のユーザーがログインできないようにするためです。 <p>インスタントクローンの場合、ログオフ後に必ずマシンが削除され、再作成されます。</p>

設定	オプション						
Refresh OS disk after logoff (ログオフ後に OS ディスクを更新)	<p>専用割り当てのリンク クローン仮想マシンの OS ディスクを更新するかどうかと、そのタイミングを選択します。</p> <ul style="list-style-type: none"> ■ [なし] : OS ディスクは更新されません。 ■ [常時] : ユーザーがログオフするたびに OS ディスクが更新されます。 ■ [間隔] : OS ディスクは、指定された日数で定期的に更新されます。日数を入力します。 <p>日数は、最終の更新から、または一度も更新されていない場合には最初のプロビジョニングから数えられます。たとえば、指定した値が 3 日で、最終更新から 3 日が経過している場合、ユーザーがログオフした後にマシンが更新されます。</p> <ul style="list-style-type: none"> ■ [このサイズのとき] : OS ディスクは、現在のサイズが最大許容サイズの指定した割合に達したときに更新されます。リンク クローンの OS ディスクの最大サイズはレプリカの OS ディスクのサイズです。割合を入力します。この割合に達すると、更新操作が実行されます。 <p>[このサイズのとき] オプションを使用すると、データストア内のリンク クローンの OS ディスクのサイズが、許容可能な最大サイズと比較されます。このディスク使用率 (%) には、マシンのゲスト OS の内部で表示される可能性のあるディスク使用量が反映されません。</p> <p>専用割り当てのリンク クローン プールで OS ディスクを更新する場合、View Composer の通常ディスクは影響を受けません。</p> <p>インスタントクローンの場合、ログオフ後に必ずマシンが削除され、再作成されます。</p>						
デフォルト表示プロトコル	<p>接続サーバがクライアントと通信するために使用する表示プロトコルを選択します。</p> <table> <tr> <td>VMware Blast</td><td>VMware Blast Extreme プロトコルは、H.264 プロトコルを基盤としており、任意のネットワーク上で、スマート フォン、タブレット、超低コスト PC、Mac などのクライアント デバイスを最も広範囲にサポートします。このプロトコルの CPU リソース使用量は最小であり、そのためモバイル デバイスのバッテリー寿命が長くなります。</td></tr> <tr> <td>PCoIP</td><td>サポートされている場合は常にデフォルト オプションです。PCoIP は、Teradici ハードウェアを備える仮想マシンおよび物理マシン用の表示プロトコルとしてサポートされます。PCoIP は、LAN 上または WAN 経由の広範なユーザーにイメージ、オーディオ、ビデオ コンテンツを配信するための最適化された PC 体験を提供します。</td></tr> <tr> <td>Microsoft RDP</td><td>Microsoft Remote Desktop Connection (RDC) は、RDP を使用してデータを伝送します。RDP は、ユーザーがコンピュータにリモート接続できるようにするマルチチャネル プロトコルです。</td></tr> </table>	VMware Blast	VMware Blast Extreme プロトコルは、H.264 プロトコルを基盤としており、任意のネットワーク上で、スマート フォン、タブレット、超低コスト PC、Mac などのクライアント デバイスを最も広範囲にサポートします。このプロトコルの CPU リソース使用量は最小であり、そのためモバイル デバイスのバッテリー寿命が長くなります。	PCoIP	サポートされている場合は常にデフォルト オプションです。PCoIP は、Teradici ハードウェアを備える仮想マシンおよび物理マシン用の表示プロトコルとしてサポートされます。PCoIP は、LAN 上または WAN 経由の広範なユーザーにイメージ、オーディオ、ビデオ コンテンツを配信するための最適化された PC 体験を提供します。	Microsoft RDP	Microsoft Remote Desktop Connection (RDC) は、RDP を使用してデータを伝送します。RDP は、ユーザーがコンピュータにリモート接続できるようにするマルチチャネル プロトコルです。
VMware Blast	VMware Blast Extreme プロトコルは、H.264 プロトコルを基盤としており、任意のネットワーク上で、スマート フォン、タブレット、超低コスト PC、Mac などのクライアント デバイスを最も広範囲にサポートします。このプロトコルの CPU リソース使用量は最小であり、そのためモバイル デバイスのバッテリー寿命が長くなります。						
PCoIP	サポートされている場合は常にデフォルト オプションです。PCoIP は、Teradici ハードウェアを備える仮想マシンおよび物理マシン用の表示プロトコルとしてサポートされます。PCoIP は、LAN 上または WAN 経由の広範なユーザーにイメージ、オーディオ、ビデオ コンテンツを配信するための最適化された PC 体験を提供します。						
Microsoft RDP	Microsoft Remote Desktop Connection (RDC) は、RDP を使用してデータを伝送します。RDP は、ユーザーがコンピュータにリモート接続できるようにするマルチチャネル プロトコルです。						
ユーザーがプロトコルを選択できるようにする	ユーザーが Horizon Client を使用してデスクトップのデフォルトの表示プロトコルをオーバーライドできるようにします。						

設定	オプション
3D レンダラー	<p>プールが Windows 7 以降のデスクトップで構成されている場合、3D グラフィックス レンダリングを有効にするかどうかを選択できます。[3D レンダラー] を構成して、ESXi 5.1 以降のホストにインストールされた物理的な GPU グラフィックス カードに基づいて、ソフトウェア レンダリングまたはハードウェア レンダリングを使用できます。</p> <p>この機能を有効にするには、プロトコルとして PCoIP または VMware Blast を選択し、[ユーザーがプロトコルを選択できるようにする] 設定を無効にする必要があります（[いいえ] を選択します）。</p> <p>ハードウェア ベースの [3D レンダラー] オプションを使用すると、ユーザーは設計、モデリング、マルチメディア用のグラフィックス アプリケーションを活用できます。ソフトウェアの [3D レンダラー] オプションを使用すると、ユーザーは AERO、Microsoft Office、Google Earth などの要求の低いアプリケーションの高度なグラフィックス機能を活用できます。システム要件については、デスクトップ用の 3D レンダリングの構成を参照してください。</p> <p>View デプロイが vSphere 5.0 以降で動作していない場合、この設定は利用できず、View Administrator でも非アクティブになります。</p> <p>この機能を選択し、[自動]、[ソフトウェア]、または [ハードウェア] オプションを選択する場合は、プールにあるマシンに割り当てられる VRAM の量を構成できます。モニタの最大数は 2 台で、最大解像度は 1920 x 1200 です。</p> <p>[vSphere Client を使用して管理] や [NVIDIA GRID vGPU] を選択する場合は、vCenter Server で 3D メモリの量とモニタ数を構成する必要があります。モニタの解像度に応じて、リモート デスクトップとして使用されるマシンに最大で 4 つのモニタを選択できます。</p> <hr/> <p>注: この設定を構成または編集したときには、新しい設定を有効にするために、既存の仮想マシンをいったんパワーオフし、それらのマシンが vCenter Server で再構成されていることを確認したうえで、マシンをパワーオンする必要があります。仮想マシンを再起動しても新しい設定は有効になりません。</p> <hr/> <p>詳細については、デスクトップ用の 3D レンダリングの構成、3D レンダラーのオプション、および 3D レンダリング構成のベスト プラクティスを参照してください。</p> <p>インスタントクローン デスクトップ プールでは使用できません。</p>
Max number of monitors (モニタの最大数)	<p>表示プロトコルとして PCoIP または VMware Blast を選択する場合は、ユーザーがデスクトップを表示できる [モニタの最大数] を選択できます。</p> <p>最大で 4 つのモニタを選択できます。</p> <p>[3D レンダラー] 設定が選択されていない場合、[モニタの最大数] の設定は、プール内のマシンに割り当てられる VRAM の量に影響を与えます。モニタ数を増やすと、関連付けられた ESXi ホスト上でより多くのメモリが消費されます。</p> <p>[3D レンダラ] 設定が選択されていない場合、Aero が無効になっている Windows 7 ゲスト OS では、最大 3 台のモニタが 3840x2160 の解像度でサポートされます。その他のオペレーティング システムまたは Aero が有効な Windows 7 では、1 台のモニタが 3840x2160 の解像度でサポートされます。</p> <p>[3D レンダラ] 設定が選択されている場合、1 台のモニタが 3840x2160 の解像度でサポートされます。モニタを複数使用する場合は、解像度を低くすると最良のサポートが得られます。解像度を高くする場合はモニタの数を少なくします。</p> <hr/> <p>注: この設定を有効にするには、既存の仮想マシンをパワーオフしてからパワーオンする必要があります。仮想マシンを再起動しても設定は有効になりません。</p> <hr/> <p>インスタントクローン デスクトップ プールでは使用できません。Horizon 7.0 では、インスタント クローンのモニタの最大数は 2 台です。</p>

設定	オプション
Max resolution of any one monitor (特定のモニタの最大解像度)	<p>表示プロトコルとして PCoIP または VMware Blast を選択する場合は、[各モニタの最大解像度] を指定する必要があります。</p> <p>デフォルトでは、[各モニタの最大解像度] は 1920x1200 ピクセルに設定されていますが、この値は構成可能です。</p> <p>[3D レンダラー] 設定が選択されていない場合、[特定のモニタの最大解像度] の設定は、プール内のマシンに割り当てられる VRAM の量に影響を与えます。この解像度を上げると、関連付けられた ESXi ホスト上でより多くのメモリが消費されます。</p> <p>[3D レンダラ] 設定が選択されていない場合、Aero が無効になっている Windows 7 ゲスト OS では、最大 3 台のモニタが 3840x2160 の解像度でサポートされます。その他のオペレーティング システムまたは Aero が有効な Windows 7 では、1 台のモニタが 3840x2160 の解像度でサポートされます。</p> <p>[3D レンダラ] 設定が選択されている場合、1 台のモニタが 3840x2160 の解像度でサポートされます。モニタを複数使用する場合は、解像度を低くすると最良のサポートが得られます。解像度を高くする場合はモニタの数を少なくします。</p> <p>注: この設定を有効にするには、既存の仮想マシンをパワーオフしてからパワーオンする必要があります。仮想マシンを再起動しても設定は有効になりません。</p> <p>インスタントクローン デスクトップ プールでは使用できません。Horizon 7.0 では、すべてのモニタの解像度が 2560 x 1600 です。</p>
HTML Access	<p>ユーザーに自分の Web ブラウザ内からリモート デスクトップに接続することを許可するには、[有効化] を選択します。ユーザーが VMware Horizon Web ポータル ページまたは VMware Identity Manager アプリケーションを使用してログインし、リモート デスクトップを選択した場合、HTML Access Agent はそのユーザーが HTTPS 経由でデスクトップに接続できるようにします。デスクトップがユーザーのブラウザに表示されます。PCoIP や RDP など、その他の表示プロトコルは使用されません。Horizon Client ソフトウェアがクライアント デバイスにインストールされている必要はありません。</p> <p>HTML Access を使用するには、View 展開に HTML Access をインストールする必要があります。詳細については、https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html で公開されている『HTML Access の使用』を参照してください。</p> <p>VMware Identity Manager で HTML Access を使用するには、『View 管理 管理ガイド』の説明に従って接続サーバを SAML 認証サーバとペアにする必要があります。VMware Identity Manager をインストールして、接続サーバで使用するために構成する必要があります。</p>
Adobe Flash quality (Adobe Flash の品質)	<p>Web ページに表示される Adobe Flash コンテンツの品質を決定します。</p> <ul style="list-style-type: none"> ■ [制御しない] : 品質は Web ページの設定で決まります。 ■ [低] : この設定では、帯域幅が最も節約されます。品質レベルを指定しないと、デフォルトで Low (低) に設定されます。 ■ [中] : この設定では、帯域幅の節約は中程度です。 ■ [高] : この設定では、帯域幅の節約は最も少なくなります。 <p>詳細については、Adobe Flash の品質とスロットル を参照してください。</p>
Adobe Flash throttling (Adobe Flash のスロットル)	<p>Adobe Flash ムービーのフレーム レートを決定します。この設定を有効にすると、レベルを選択することによって、1 秒あたりに表示されるフレームの数を増やしたり減らしたりすることができます。</p> <ul style="list-style-type: none"> ■ [無効化] : スロットルは行われません。タイマー間隔は変更されません。 ■ [低] : タイマー間隔は 100 ミリ秒です。この設定では、抜けるフレームの数が最も少なくなります。 ■ [中] : タイマー間隔は 500 ミリ秒です。 ■ [高] : タイマー間隔は 2,500 ミリ秒です。この設定では、抜けるフレームの数が最も多くなります。 <p>詳細については、Adobe Flash の品質とスロットル を参照してください。</p>

設定	オプション
Mirage 設定全体をオーバーライドする	すべてのデスクトップ プールに同一の Mirage サーバを指定するには、このプール固有設定ではなく全体的な View 構成設定を使用してください。 インスタントクローン デスクトップ プールでは使用できません。
Mirage サーバの構成	mirage://server-name:port または mirages://server-name:port という形式で Mirage サーバの URL を指定できるようにします (<i>server-name</i> は完全修飾ドメイン名)。ポート番号を指定しないと、デフォルトのポート番号 8000 が使用されます。 Mirage クライアントのインストール時に Mirage サーバを指定する代わりに、View Administrator で Mirage サーバを指定することもできます。View Administrator での Mirage サーバの指定をサポートしているのはどの Mirage バージョンかを確認するには、 https://www.vmware.com/support/pubs/mirage_pubs.html で公開されている Mirage ドキュメントを参照してください。 インスタントクローン デスクトップ プールでは使用できません。

Adobe Flash の品質とスロットル

Adobe Flash コンテンツの品質の許容される最大レベルを指定して、Web ページでの設定を上書きできます。Web ページの Adobe Flash 品質が許容される最大レベルより高い場合、品質は指定されている最大レベルまで下げられます。品質は低いほど帯域幅が節約されます。

Adobe Flash 帯域幅削減の設定を使用するには、Adobe Flash を全画面表示モードで実行してはいけません。

表 12-5. Adobe Flash の品質設定 に使用可能な Adobe Flash のレンダリング品質設定を示します。

表 12-5. Adobe Flash の品質設定

品質設定	説明
[制御しない]	品質は Web ページの設定で決まります。
[低]	この設定では、帯域幅が最も節約されます。
[中]	この設定では、帯域幅の節約は中程度です。
[高]	この設定では、帯域幅の節約は最も少なくなります。

品質の最高レベルを指定しないと、デフォルトで [低] に設定されます。

Adobe Flash はタイマー サービスを使用して、特定の時点で画面に表示されるものを更新します。一般的な Adobe Flash タイマー間隔の値は、4 ~ 50 ミリ秒の範囲です。間隔をスロットルつまり延長すると、フレーム レートを減らすことができ、それによって帯域幅を少なくできます。

表 12-6. Adobe Flash のスロットル設定 に使用可能な Adobe Flash のスロットル設定を示します。

表 12-6. Adobe Flash のスロットル設定

スロットル設定	説明
[無効]	スロットルは行われません。タイマー間隔は変更されません。
[低]	タイマー間隔は 100 ミリ秒です。この設定では、抜けるフレームの数が最も少なくなります。
[中]	タイマー間隔は 500 ミリ秒です。
[高]	タイマー間隔は 2500 ミリ秒です。この設定では、抜けるフレームの数が最も多くなります。

オーディオの速度はスロットル設定の選択に関係なく一定です。

デスクトップ プールの電源ポリシーの設定

デスクトップ プールの仮想マシンを vCenter Server で管理している場合、その仮想マシンの電源ポリシーを構成できます。ただし、インスタント クローンは除きます。インスタント クローンは常にパワーオンされています。

電源ポリシーは、関連付けられたデスクトップが使用中でないときの仮想マシンの動作方法を制御します。デスクトップは、ユーザーがログインする前と、ユーザーが切断またはログオフした後は使用中でないで見なされます。電源ポリシーは、更新、再構成、再分散などの管理タスクが完了した後の仮想マシンの動作方法も制御します。

View Administrator でデスクトップ プールを作成または編集するときに電源ポリシーを構成します。

注: 非管理対象のマシンを含むデスクトップ プールに対しては電源ポリシーを構成できません。

デスクトップ プールの電源ポリシー

電源ポリシーは、関連付けられたリモート デスクトップが使用中でないときの仮想マシンの動作方法を制御します。

デスクトップ プールを作成または編集するときに電源ポリシーを設定します。[表 12-7. 電源ポリシー](#)で、利用できる電源ポリシーについて説明します。

表 12-7. 電源ポリシー

電源ポリシー	説明
[電源操作を行わない]	<p>View は、ユーザーがログオフした後に電源ポリシーを適用しません。この設定による影響は 2 つあります。</p> <ul style="list-style-type: none"> ■ View は、ユーザーがログオフした後に仮想マシンの電源状態を変更しません。 <p>たとえば、ユーザーが仮想マシンをシャットダウンした場合、仮想マシンはパワーオフのままです。ユーザーがシャットダウンせずにログオフした場合、仮想マシンはパワーオンのままです。ユーザーがデスクトップに再接続すると、仮想マシンは電源がオフであった場合は再起動します。</p> <ul style="list-style-type: none"> ■ View は、管理タスクの完了後に電源状態を適用しません。 <p>たとえば、ユーザーがシャットダウンせずにログオフしたとします。仮想マシンはパワーオンのままです。スケジュール設定されている再構成が行われると、仮想マシンはパワーオフされます。再構成の完了後、View は仮想マシンの電源状態を変えるための操作を何も行いません。仮想マシンはパワーオフのままです。</p>
[マシンは常にパワーオン状態]	<p>仮想マシンは、未使用時でもパワーオンされたままです。ユーザーが仮想マシンをシャットダウンした場合、すぐに再起動されます。また、仮想マシンは、更新、再構成、再分散などの管理タスクが完了した後も再起動されます。</p> <p>スケジュール設定された時刻に仮想マシンに接続する必要があるバッチプロセスまたはシステム管理ツールを実行する場合は、[マシンは常にパワーオン] を選択します。</p>

電源ポリシー	説明
[サスペンド]	<p>仮想マシンは、ユーザーがログオフしたときにサスペンド状態になりますが、ユーザーが切断したときにはサスペンド状態になりません。</p> <p>ユーザーがログオフせずに切断したときに専用プールのマシンをサスペンドするように構成することもできます。このポリシーを構成するには、View LDAP に属性を設定する必要があります。ユーザーが切断した後にサスペンドするよう専用マシンを構成するを参照してください。</p> <p>複数の仮想マシンがサスペンド状態から再開すると、一部の仮想マシンのパワーオンが遅延する場合があります。遅延が発生するかどうかは、ESXi ホスト ハードウェアおよび ESXi ホストに構成される仮想マシンの数に依存します。Horizon Client からデスクトップに接続しているユーザーは、一時的にデスクトップが使用できないというメッセージを目にする場合があります。デスクトップにアクセスするために、ユーザーは再接続できます。</p>
[パワーオフ]	<p>仮想マシンは、ユーザーがログオフしたときにシャットダウンされますが、ユーザーが切断したときにはシャットダウンされません。</p>

注: マシンを手動プールに追加する場合は、[パワーオフ] または [電源操作を行わない] 電源ポリシーが選択されている場合でも、View はマシンをパワーオンして完全に構成されるようにします。構成が済んだ Horizon Agent は動作可能とマークされ、プールの通常の電源管理設定が適用されます。

vCenter Server によって管理されるマシンが含まれている手動プールの場合、ユーザーがスベア マシンに接続できるように、View は必ず 1 つのスベア マシンがパワーオンされているようにします。このスベア マシンは、どの電源ポリシーが有効でもパワーオンされます。

[表 12-8. View が電源ポリシーを適用するタイミング](#)に、構成された電源ポリシーを View が適用するタイミングを示します。

表 12-8. View が電源ポリシーを適用するタイミング

デスクトップ プールタイプ	電源ポリシーの適用
1 つのマシン（vCenter Server によって管理される仮想マシン）を含む手動プール	<p>電源操作はセッション管理によって起動されます。仮想マシンは、ユーザーがデスクトップを要求するとパワーオンされ、ユーザーがログオフするとパワーオフされるかサスペンドされます。</p> <p>注: 単一のマシン プールで流動割り当てを使用しているか、専用割り当てを使用しているか、およびマシンが割り当て済みか、未割り当てにかかわらず、[マシンは常にパワーオン] ポリシーが適用されます。</p>
専用割り当てによる自動プール	<p>未割り当てマシンに対してのみ。</p> <p>割り当て済みマシンでは、電源操作はセッション管理によって開始されます。仮想マシンは、ユーザーが割り当て済みのマシンを要求するとパワーオンされ、ユーザーがログオフするとパワーオフされるかサスペンドされます。</p> <p>注: [マシンは常にパワーオン] ポリシーは割り当て済みおよび未割り当てマシンに適用されます。</p>
流動割り当てによる自動プール	<p>マシンが使用されていないとき、およびユーザーがログオフした後。</p> <p>流動割り当てデスクトップ プールに対して [パワーオフ] または [サスペンド] 電源ポリシーを構成する場合は、セッションの破棄または孤立を防止するために [切断後に自動的にログオフ] を [直後] に設定します。</p>

デスクトップ プールタイプ	電源ポリシーの適用
専用割り当てによる手動プール	<p>未割り当てマシンに対してのみ。</p> <p>割り当て済みマシンでは、電源操作はセッション管理によって開始されます。仮想マシンは、ユーザーが割り当て済みのマシンを要求するとパワーオンされ、ユーザーがログオフするとパワーオフされるかサスペンドされます。</p> <p>注: [マシンは常にパワーオン] ポリシーは割り当て済みおよび未割り当てマシンに適用されます。</p>
流動割り当てによる手動プール	<p>マシンが使用されていないとき、およびユーザーがログオフした後。</p> <p>流動割り当てデスクトップ プールに対して [パワーオフ] または [サスペンド] 電源ポリシーを構成する場合は、セッションの破棄または孤立を防止するために [切断後に自動的にログオフ] を [直後] に設定します。</p>

View が、構成された電源ポリシーを自動プールにどのように適用するかは、マシンが使用可能かどうかによって異なります。詳細については、[自動デスクトップ プールに対する電源ポリシーの影響](#)を参照してください。

ユーザーが切断した後にサスペンドするよう専用マシンを構成する

[サスペンド] 電源ポリシーにより、ユーザーがログオフしたときに仮想マシンはサスペンドしますが、切断したときにはサスペンドしません。ユーザーがログオフせずにデスクトップから切断したときに、専用プールのマシンをサスペンドするように構成することもできます。切断時にサスペンドを使用することで、リソースを節約することができます。

専用マシンで切断時にサスペンドを有効にするには、View LDAP に属性を設定する必要があります。

手順

- 1 View 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 [ドメインまたはサーバを選択または入力] フィールドに、サーバ名として **localhost:389** を入力します。
- 4 [接続ポイント] で [識別名または命名規則を選択または入力] をクリックし、識別名として **DC=vdi,DC=vmware,DC=int** を入力して、[OK] をクリックします。
[ADAM ADSI Edit] メイン ウィンドウが表示されます。
- 5 ADAM ADSI ツリーを展開して [OU=Properties] を展開します。
- 6 [OU=Global] を選択してから、右ペインで [CN=Common] を選択します。
- 7 [アクション] - [プロパティ] の順に選択し、[pae-NameValuePair] 属性の下に新規エントリ **suspendOnDisconnect=1** を追加します。
- 8 VMware Horizon View 接続サーバ サービスまたは View 接続サーバを再起動します。

自動デスクトップ プールに対する電源ポリシーの影響

View が、構成された電源ポリシーを自動プールにどのように適用するかは、マシンが使用可能かどうかによって異なります。

自動プール内のマシンは、以下の条件を満たす場合に使用可能であると見なされます。

- アクティブである
- ユーザー セッションを含んでいない
- ユーザーに割り当てられていない

マシンで実行されている Horizon Agent サービスにより、マシンの可用性の確認が View 接続サーバに対して行われます。

自動プールを構成するときに、プロビジョニングする必要がある仮想マシンの最小数と最大数、およびいつでもパワーオン状態を維持し、使用可能にしておく必要があるスペア マシンの数を指定できます。

流動割り当てを使用する自動プールの電源ポリシーの例

流動割り当てを使用して自動プールを構成するときに、いつでも特定の数のマシンを使用可能にしておくよう指定できます。プール ポリシーがどのように設定されていても、使用可能なスペア マシンは常にパワーオンの状態になります。

電源ポリシーの例 1

表 12-9. 流動割り当てを使用する自動プールのデスクトップ プール設定の例 1 は、この例で使用される流動割り当ての自動プールを示しています。このプールは、マシン名前付けパターンを使用して、マシンのプロビジョニングと名前付けを行います。

表 12-9. 流動割り当てを使用する自動プールのデスクトップ プール設定の例 1

デスクトップ プールの設定	値
マシン数 (最小)	10
マシン数 (最大)	20
スペアのパワーオン状態のマシンの数	2
リモート マシンの電源ポリシー	パワーオフ

このデスクトップ プールがプロビジョニングされると、10 台のマシンが作成され、2 台のマシンはパワーオンされ、すぐに使用可能になり、8 台のマシンはパワーオフされます。

使用可能なスペア マシン数を維持するために、新しいユーザーがプールに接続するたびに 1 台のマシンがパワーオンになります。接続ユーザー数が 8 名を超えると、スペア マシンの数を維持するために追加マシン (最大で 20 台) が作成されます。最大数に達した後も、スペア マシンの数を維持するために、最初に切断した 2 名のユーザーのマシンはパワーオンのままになります。後続の各ユーザーのマシンは、電源ポリシーに従ってパワーオフされます。

電源ポリシーの例 2

表 12-10. 流動割り当てを使用する自動プールのデスクトップ プール設定の例 2 は、この例で使用される流動割り当ての自動プールを示しています。このプールは、マシン名前付けパターンを使用して、マシンのプロビジョニングと名前付けを行います。

表 12-10. 流動割り当てを使用する自動プールのデスクトップ プール設定の例 2

デスクトップ プールの設定	値
マシン数 (最小)	5
マシン数 (最大)	5
スベアのパワーオン状態のマシンの数	2
リモート マシンの電源ポリシー	パワーオフ

このデスクトップ プールがプロビジョニングされると、5 台のマシンが作成され、2 台のマシンはパワーオンされてすぐに使用可能になり、3 台のマシンはパワーオフされます。

このプールの 4 台目のマシンがパワーオフされると、既存のマシンのいずれかがパワーオンされます。マシンの最大数にすでに達しているため、追加マシンがパワーオンされることはありません。

専用割り当てを使用する自動プールの電源ポリシーの例

流動割り当てを使用する自動プール内のパワーオン状態のマシンとは異なり、専用割り当てを使用する自動プール内のパワーオン状態のマシンは必ずしも使用可能ではありません。マシンがユーザーに割り当てられていない場合にのみ使用可能です。

表 12-11. 専用割り当てを使用する自動プールのデスクトップ プール設定の例は、この例で使用される専用割り当ての自動プールを示しています。

表 12-11. 専用割り当てを使用する自動プールのデスクトップ プール設定の例

デスクトップ プールの設定	値
マシン数 (最小)	3
マシン数 (最大)	5
スベアのパワーオン状態のマシンの数	2
リモート マシンの電源ポリシー	マシンは常にパワーオン

このデスクトップ プールがプロビジョニングされると、3 台のマシンが作成され、パワーオンされます。vCenter Server でマシンがパワーオフされた場合、電源ポリシーに従って、マシンはすぐに再度パワーオンになります。

ユーザーがプール内のマシンに接続した後、マシンはそのユーザーに永続的に割り当てられます。ユーザーがマシンから切断した後、他のユーザーはそのマシンを使用できません。ただし、[マシンは常にパワーオン] ポリシーは適用されたままとなります。割り当て済みマシンが vCenter Server でパワーオフされた場合、すぐに再度パワーオンされます。

別のユーザーが接続すると、2 番目のマシンが割り当てられます。2 番目のユーザーが接続すると、スベア マシンの数が制限を下回るため、別のマシンが作成およびパワーオンされます。最大マシンの制限に達するまで、新しいユーザーが割り当てられるたびに、追加マシンが作成およびパワーオンされます。

View の電源ポリシーの競合の防止

View Administrator を使用して電源ポリシーを構成するときは、電源ポリシーをゲスト OS の電源オプション コントロール パネルの設定と比較することによって、電源ポリシーの競合を防止する必要があります。

仮想マシンで構成されている電源ポリシーがゲスト OS で構成されている電源オプションと互換性がない場合、仮想マシンが一時的にアクセス不能になることがあります。同じプールに他のマシンがある場合は、それらも影響を受けることがあります。

以下の構成は、電源ポリシーの競合の例です。

- View Administrator で、仮想マシンに対して [サスペンド] の電源ポリシーが構成されています。このポリシーにより、仮想マシンは未使用時にサスペンド状態になります。
- ゲスト OS の電源オプション コントロール パネルで、[コンピュータをスリープ状態にする] が 3 分に設定されています。

この構成では、View 接続サーバとゲスト OS の両方が仮想マシンをサスペンドできます。View 接続サーバで仮想マシンがパワーオンであることが必要な場合に、ゲスト OS の電源オプションが原因で仮想マシンが使用できないことがあります。

デスクトップ用の 3D レンダリングの構成

仮想マシンのデスクトップ プールを作成または編集するときに、デスクトップの 3D グラフィックス レンダリングを構成できます。デスクトップは、Virtual Shared Graphics Acceleration (vSGA)、Virtual Dedicated Graphics Acceleration (vDGA)、または共有 GPU ハードウェア アクセラレーション (NVIDIA GRID vGPU) を活用できます。vDGA と NVIDIA GRID vGPU は、ESXi ホストにインストールされている物理グラフィックス カードを使用し、仮想マシン間でグラフィック プロセッシング ユニット (GPU) リソースを管理する vSphere の機能です。

注: この機能は Horizon 7.0 のインスタント クローンでは使用できません。

エンド ユーザーは、効率的に実行するには多くの場合 GPU ハードウェアが必要になる設計、モデリング、マルチメディア用の 3D アプリケーションを活用できます。物理 GPU を必要としないユーザーは、ソフトウェア オプションによって、Windows AERO、Microsoft Office、Google Earth など、負担の少ないアプリケーションをサポートできる高度なグラフィックス機能を利用できます。次に、3D グラフィックス オプションについて簡単に説明します。

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

vSphere 6.0 以降で提供されるこの機能を使用して、ESXi ホスト上の 1 つの物理 GPU を仮想マシン間で共有できます。この機能により、軽量の 3D タスクを処理するユーザーから、ハイエンド ワークステーションでグラフィックスを処理するパワー ユーザーまで、ハードウェアで高速化された柔軟性のある 3D プロファイルを使用できるようになります。

vDGA を使用する AMD Multiuser GPU

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

Virtual Dedicated Graphics Acceleration (vDGA)

vSphere 5.5 以降で提供されるこの機能を使用して、ESXi ホスト上の単一の物理 GPU を単一の仮想マシン専用にすることができます。この機能は、ハイエンドのハードウェア高速ワークステーション グラフィックスが必要な場合に使用します。

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

Virtual Shared Graphics Acceleration (vSGA)

vSphere 5.1 以降で提供されるこの機能により、ESXi ホスト上の物理的な GPU を複数の仮想マシンで共有できます。この機能は、中間 3D 設計、モデリング、およびマルチメディア アプリケーションに適しています。

ソフト 3D

vSphere 5.0 以降で提供されるソフトウェア アクセラレータによるグラフィックスで、物理的な GPU を必要とすることなく、DirectX 9 と OpenGL 2.1 アプリケーションを実行できます。この機能は、Windows Aero テーマ、Microsoft Office 2010、Google Earth など、リソース要求が少ない 3D アプリケーションで使用します。

NVIDIA GRID vGPU、vDGA を使用する AMD Multiuser GPU、およびすべての vDGA ソリューションでは、ESXi ホストで PCI パススルーを使用するため、ライブ VMotion はサポートされません。vSGA および Soft 3D ではライブ VMotion はサポートされています。

ビデオ ゲームや 3D ベンチマークなどのアプリケーションによってディスプレイが強制的に全画面解像度で表示されると、場合によっては、デスクトップ セッションが切断される可能性があります。可能な回避策には、アプリケーションをウィンドウ モードで実行するように設定することや、View セッションのデスクトップ解像度をアプリケーションが要求する既定の解像度に合わせるなどがあります。

すべてのタイプの 3D レンダリングに対する要件

3D グラフィックス レンダリングを有効にするには、プール展開が次の要件を満たしている必要があります。

- 仮想マシンは Windows 7 以降である。
- プールでデフォルト表示プロトコルとして PCoIP または VMware Blast Extreme が使用されている。
- ユーザーにプロトコルの選択を許可しない。

重要: [3D レンダラー] 設定を構成または編集する際は、既存の仮想マシンをパワーオフし、マシンが vCenter Server で再構成されていることを確認してから、マシンをパワーオンして新しい設定を有効にする必要があります。仮想マシンを再起動しても新しい設定は有効になりません。

NVIDIA GRID vGPU のその他の要件

NVIDIA GRID vGPU を使用する場合、ESXi ホスト上の単一の物理 GPU を複数の物理マシンで共有できます。このタイプの共有 GPU ハードウェア アクセラレーションをサポートするには、プールが次の追加要件を満たしている必要があります。

- 仮想マシンが ESXi 6.0 以降のホストで実行されており、仮想ハードウェア バージョン 11 以降であり、vCenter Server 6.0 以降のソフトウェアによって管理されている必要があります。

View にデスクトップ プールを作成する前に、共有 PCI デバイスを使用するように親仮想マシンまたは仮想マシン テンプレートを構成する必要があります。詳細な手順については、『[NVIDIA GRID vGPU Deployment Guide for VMware Horizon 6.1](#)』を参照してください。

- 仮想マシンのゲスト OS に、GPU ベンダーからグラフィックス ドライバをインストールする必要があります。

注: サポートされている GPU ハードウェアのリストについては、<http://www.vmware.com/resources/compatibility/search.php> の VMware ハードウェア互換性一覧を参照してください。

- View Administrator の [3D レンダラー] オプションを [NVIDIA GRID vGPU] に設定する必要があります。

vDGA を使用する AMD Multiuser GPU のその他の要件

vDGA を使用する AMD Multiuser GPU により、GPU が複数の PCI パススルー デバイスのように見えるようになり、複数の仮想マシンで AMD GPU を共有できます。このタイプの共有 GPU ハードウェア アクセラレーションをサポートするには、プールが次の追加要件を満たしている必要があります。

- 仮想マシンが ESXi 6.0 以降のホストで実行されており、仮想ハードウェア バージョン 11 以降であり、vCenter Server 6.0 以降のソフトウェアによって管理されている必要があります。
- ESXi ホスト上で GPU パススルーを有効化し、AMD SR-IOV (Single Root I/O Virtualization) を構成して、専用 PCI デバイスを使用するように各仮想マシンを構成する必要があります。[vDGA を使用する AMD Multiuser GPU の機能を使用する準備](#) を参照してください。

注: このリリースでは、手動デスクトップ プールのみがサポートされます。

- 仮想マシンのゲスト OS に、GPU ベンダーからグラフィックス ドライバをインストールする必要があります。

注: サポートされている GPU ハードウェアのリストについては、<http://www.vmware.com/resources/compatibility/search.php> の VMware ハードウェア互換性一覧を参照してください。

- View Administrator の [3D レンダラー] オプションを [vSphere Client を使用して管理] に設定する必要があります。

vDGA を使用する場合のその他の要件

vDGA は ESXi ホスト上の単一の物理 GPU を単一の仮想マシン専用にしします。vDGA をサポートするには、プールが次の追加要件を満たしている必要があります。

- 仮想マシンが ESXi 5.5 以降のホストで実行されており、仮想ハードウェア バージョン 9 以降であり、vCenter Server 5.5 以降のソフトウェアによって管理されている必要があります。

View でデスクトップ プールが作成された後、ESXi ホスト上で GPU パススルーを有効にし、専用 PCI デバイスを使用するように各仮想マシンを構成する必要があります。vDGA に親仮想マシンまたはテンプレートを構成してからデスクトップ プールを作成することはできません。同じ物理的な GPU がプール内のすべての仮想マシン専用になるためです。グラフィックス アクセラレーションについては、『VMware ホワイト ペーパー』の「vDGA インストール」を参照してください。

リンク クローン仮想マシンでは、vDGA 設定が更新、再構成、および再分散操作後に保存されます。

- 仮想マシンのゲスト OS に、GPU ベンダーからグラフィックス ドライバをインストールする必要があります。

注: サポートされている GPU ハードウェアのリストについては、<http://www.vmware.com/resources/compatibility/search.php> の VMware ハードウェア互換性一覧を参照してください。

- [3D レンダラー] オプションを [vSphere Client を使用して管理] に設定する必要があります。

vSGA を使用する場合のその他の要件

vSGA を使用して、ESXi ホスト上の物理的な GPU を複数の仮想マシンで共有できます。vSGA をサポートするには、プールが次の追加要件を満たしている必要があります。

- 仮想マシンは ESXi 5.1 以降のホストで動作し、vCenter Server 5.1 以降のソフトウェアで管理される必要があります。
- GPU グラフィックス カードおよび関連付けられた vSphere Installation Bundles (VIB) が ESXi ホストにインストールされている。サポートされている GPU ハードウェアのリストについては、<http://www.vmware.com/resources/compatibility/search.php> の VMware ハードウェア互換性一覧を参照してください。
- Windows 7 マシンは、仮想ハードウェア バージョン 8 以降である必要があります。Windows 8 マシンは、仮想ハードウェア バージョン 9 以降である必要があります。Windows 10 マシンは、仮想ハードウェア バージョン 10 以降である必要があります。
- [3D レンダラー] オプションを、[vSphere Client を使用して管理]、[自動]、または [ハードウェア] のいずれかの設定に指定できます。[3D レンダラー用のビデオ RAM 構成オプション](#) も参照してください。

[自動] オプションでは、ESXi ホストに有効で使用可能なハードウェア GPU がある場合にハードウェア アクセラレーションが使用されます。ハードウェア GPU を使用できない場合、仮想マシンは 3D タスクにソフトウェア 3D レンダリングを使用します。

Soft 3D を使用する場合のその他の要件

ソフトウェアの 3D レンダリングをサポートするには、プールが次の追加の要件を満たしている必要があります。

- 仮想マシンは ESXi 5.0 以降のホストで動作し、vCenter Server 5.0 以降のソフトウェアで管理される必要があります。
- マシンは、仮想ハードウェア バージョン 8 以降である必要があります。
- [3D レンダラー] オプションを [ソフトウェア] に設定する必要があります。[3D レンダラー用のビデオ RAM 構成オプション](#) も参照してください。

3D レンダラー用のビデオ RAM 構成オプション

[3D レンダラー] 設定を有効にし、[自動]、[ソフトウェア]、または [ハードウェア] オプションを選択した場合、[3D ゲストの VRAM を構成] ダイアログ ボックスのスライダーを動かして、プール内の仮想マシンに割り当てられる VRAM の量を構成できます。最小の VRAM サイズは 64MB です。次のように、VRAM のデフォルト容量は仮想ハードウェアのバージョンによって異なります。

- 仮想ハードウェア バージョン 8 (vSphere 5.0) 仮想マシンの場合、VRAM のデフォルト サイズは 64 MB であり、最大サイズの 128MB に構成できます。
- 仮想ハードウェア バージョン 9 (vSphere 5.1) および 10 (vSphere 5.5 Update 1) 仮想マシンの場合、VRAM のデフォルト サイズは 96 MB であり、最大サイズの 512MB に構成できます。
- 仮想ハードウェア バージョン 11 (vSphere 6.0) 仮想マシンの場合、VRAM のデフォルト サイズは 96 MB であり、最大サイズの 128 MB に構成できます。vSphere 6.0 以降の仮想マシンでは、この設定はグラフィックスカード内のディスプレイ メモリ容量のみを示しているため、3D オブジェクトを保管するためにディスプレイ メモリとゲスト メモリの両方が含まれていた以前の仮想ハードウェア バージョンよりも、最大値の設定が低くなっています。

View Administrator で構成する VRAM 設定は、[vSphere Client を使用して管理] オプションを選択しない限り、vSphere Client または vSphere Web Client の仮想マシン向けに構成可能な VRAM 設定よりも優先されます。

[自動]、[ソフトウェア]、または [ハードウェア] 3D レンダリング オプションの詳細については、[「3D レンダラーのオプション」](#)を参照してください。

3D レンダラーのオプション

デスクトップ プール用の [3D レンダラー] 設定には、さまざまな方法でグラフィックス レンダリングを構成できるオプションがあります。

次の表は、View Administrator で使用可能なさまざまなタイプの 3D レンダリング オプションの相違を示しています。ただし、Virtual Shared Graphics Acceleration (vSGA)、Virtual Dedicated Graphics Acceleration (vDGA)、vDGA を使用する AMD Multiuser GPU、および NVIDIA GRID vGPU 用に仮想マシンや ESXi ホストを構成する方法の詳細については記載されていません。これらのタスクは、View Administrator でデスクトップ プールを作成する前に vSphere Web Client で行う必要があります。vSGA と vDGA に関するこれらのタスクの手順については、『[VMware ホワイト ペーパー](#)』のグラフィック アクセラレーションに関する項目を参照してください。NVIDIA GRID vGPU に関する手順については、『[NVIDIA GRID vGPU Deployment Guide for VMware Horizon 6.1](#)』を参照してください。vDGA を使用する AMD Multiuser GPU の詳細については、[vDGA を使用する AMD Multiuser GPU の機能を使用する準備](#)を参照してください。

表 12-12. vSphere 5.1 以降で実行されるプール用の 3D レンダラーのオプション

オプション	説明
vSphere Client を使用して管理	<p>vSphere Web Client（または vSphere 5.1 以降の vSphere Client）で設定する仮想マシン用の [3D レンダラー] オプションによって、使用される 3D グラフィックス レンダリングのタイプが決まります。View は 3D レンダリングを制御しません。</p> <p>vSphere Web Client で、[自動]、[ソフトウェア]、または [ハードウェア] のオプションを構成できます。これらのオプションは、View Administrator で設定した場合と同じ効果を持ちます。</p> <p>vDGA および vDGA を使用する AMD Multiuser GPU を構成する場合、この設定を使用します。この設定は、vSGA のオプションでもあります。</p> <p>[vSphere Client を使用して管理] オプションを選択すると、[3D ゲストの VRAM を構成]、[モニタの最大数]、[特定のモニタの最大解像度] の設定が View Administrator で非アクティブになります。vSphere Web Client でメモリ量を構成できます。</p>
自動	<p>3D レンダリングが有効です。ESXi ホストが使用される 3D レンダリングのタイプを制御します。</p> <p>たとえば、ESXi ホストは仮想マシンがパワーオンされる順番に従って GPU ハードウェア リソースを予約します。仮想マシンがパワーオンされた時点ですべての GPU ハードウェア リソースがすでに予約されている場合、ESXi はそのマシン用にソフトウェア レンダラーを使用します。</p> <p>この設定は、vSGA を構成するときのオプションです。</p> <p>ESXi ホストは、[3D ゲストの VRAM を構成] ダイアログ ボックスで設定した値に基づいて VRAM を仮想マシンに割り当てます。</p>
ソフトウェア	<p>3D レンダリングが有効です。ESXi ホストはソフトウェア 3D グラフィックス レンダリングを使用します。GPU グラフィックス カードが ESXi ホストにインストールされると、このプールはそれを使用しなくなります。</p> <p>この設定は、Soft 3D を構成するときを使用します。</p> <p>ESXi ホストは、[3D ゲストの VRAM を構成] ダイアログ ボックスで設定した値に基づいて VRAM を仮想マシンに割り当てます。</p>
ハードウェア	<p>3D レンダリングが有効です。ESXi ホストは仮想マシンがパワーオンされる順番に従って GPU ハードウェア リソースを予約します。</p> <p>この設定は、vSGA を構成するときのオプションです。</p> <p>ESXi ホストは、[3D ゲストの VRAM を構成] ダイアログ ボックスで設定した値に基づいて VRAM を仮想マシンに割り当てます。</p> <p>重要: [ハードウェア] オプションを構成する場合、次のような制約が考えられることを考慮してください。</p> <ul style="list-style-type: none"> ■ すべての GPU ハードウェア リソースが予約されている場合にユーザーがマシンに接続しようすると、仮想マシンがパワーオンされず、ユーザーにエラー メッセージが表示されます。 ■ vMotion を使用して、GPU ハードウェアが構成されていない ESXi ホストにマシンを移動すると、仮想マシンの電源はオンになりません。 <p>ハードウェア ベースの 3D レンダリングを構成すると、ESXi ホストの各仮想マシンに割り当てられた GPU リソースを調べられます。詳細については、以下を参照してください。 ESXi ホストでの GPU リソースの調査。</p>

オプション	説明
NVIDIA GRID vGPU	<p>NVIDIA GRID vGPU の 3D レンダリングが有効になります。ESXi ホストは仮想マシンがパワーオンされる順番に従って GPU ハードウェア リソースを予約します。ホスト上の他の仮想マシンによってすべての GPU ハードウェア リソースが使用されている場合にユーザーがマシンに接続しようとする、View 接続サーバはその仮想マシンをクラスタ内の別の ESXi ホストに移動させてから、電源をオンにします。</p> <p>この設定は、NVIDIA GRID vGPU を構成しているときに使用します。</p> <p>[NVIDIA GRID vGPU] オプションを選択すると、[3D ゲストの VRAM を構成]、[モニタの最大数]、および[1 台のモニタの最大解像度] の設定が View Administrator で非アクティブになります。vSphere Web Client を使用して親仮想マシンまたは仮想マシン テンプレートを構成する場合、すべてのメモリを予約するように求められます。</p> <p>重要: [NVIDIA GRID vGPU] オプションを構成する場合は、次のような制約が課せられる可能性があることを考慮してください。</p> <ul style="list-style-type: none"> ■ 仮想マシンは、サスペンドまたはレジュームできません。このため、仮想マシンをサスペンドするためのリモートマシンの電源ポリシー オプションは使用できません。 ■ vMotion を使用して、GPU ハードウェアが構成されていない ESXi ホストにマシンを移動すると、仮想マシンの電源はオンになりません。ライブ vMotion は使用できません。 ■ クラスタ内のすべての ESXi ホストがバージョン 6.0 以降であり、仮想マシンはハードウェア バージョン 11 以降である必要があります。 ■ ESXi クラスタに、NVIDIA GRID vGPU が有効になっているホストと、NVIDIA GRID vGPU が無効になっているホストが含まれている場合、それらのホストの View Administrator ダッシュボードに黄色（警告）ステータスが表示されます。ホスト上の他の仮想マシンによってすべての GPU ハードウェア リソースが使用されている場合にユーザーがマシンに接続しようとする、View 接続サーバはその仮想マシンをクラスタ内の別の ESXi ホストに移動させてから、電源をオンにします。このような場合、NVIDIA GRID vGPU が無効になっているホストを、このタイプの動的移行に使用することはできません。
無効	3D レンダリングが非アクティブです。

表 12-13. vSphere 5.0 で実行されるプール用の 3D レンダラーのオプション

オプション	説明
有効	<p>[3D レンダラー] オプションが有効です。ESXi ホストはソフトウェア 3D グラフィックス レンダリングを使用します。ソフトウェア レンダリングが構成されている場合、デフォルトの VRAM サイズは 64MB であり、これが最小サイズです。[3D ゲストの VRAM を構成] ダイアログ ボックスでは、スライダを使用して予約されている VRAM の量を増やすことができます。ソフトウェア レンダリングでは、ESXi ホストが仮想マシンごとに最大 128MB を割り当てます。それより大きい VRAM サイズを設定すると、無視されます。</p>
無効	3D レンダリングが非アクティブです。

デスクトップ プールが 5.0 より前のバージョンの vSphere で実行されている場合、[3D レンダラー] 設定が非アクティブになり、View Administrator では使用できません。

3D レンダリング構成のベスト プラクティス

3D レンダリングのオプションなどのプール設定には、さまざまな利点と問題点があります。自分の vSphere ハードウェア インフラストラクチャ、およびグラフィックス レンダリングに関するユーザーの要件に最も合ったオプションを選択してください。

注: ここでは、View Administrator で見つけたコントロールの概要について説明します。3D レンダリングにおけるさまざまな選択内容や要件の詳細については、グラフィック アクセラレーションに関する『[VMware ホワイトペーパー](#)』を参照してください。

自動オプションを選択したほうがよい状況

[自動] オプションは、3D レンダリングを必要とする多くの View 展開にとって最適な選択肢です。vSGA (Virtual Shared Graphics Acceleration) が有効な仮想マシンは、再構成しなくてもソフトウェアとハードウェア間の 3D レンダリングを動的に切り替えることができます。このオプションを使用すると、GPU リソースがすべて予約済みだったとしても、特定のタイプの 3D レンダリングを使用できます ESXi 5.1 と ESXi 5.0 ホストの混合クラスタ内でこのオプションを使用すると、たとえば、vMotion が仮想マシンを ESXi 5.0 ホストに移動していた場合であっても、仮想マシンを正常にパワーオンして 3D レンダリングを使用することができます。

[自動] オプションの唯一の問題点は、仮想マシンがハードウェアとソフトウェアのどちらの 3D レンダリングを使用するかを容易には判断できないことです。

ハードウェア オプションを選択したほうがよい状況

[ハードウェア] オプションを使用すると、GPU リソースが ESXi ホストで使用可能である限り、プール内のすべての仮想マシンがハードウェア 3D レンダリングを使用できます。このオプションは、すべてのユーザーがグラフィックス集約型アプリケーションを実行する場合の最適な選択肢です。このオプションは、vSGA (Virtual Shared Graphics Acceleration) を構成するときに使用できます。

[ハードウェア] オプションを使用した場合、vSphere 環境を厳密に制御する必要があります。すべての ESXi ホストはバージョン 5.1 以降であり、GPU グラフィックス カードがインストールされている必要があります。

ESXi ホストのすべての GPU リソースが予約されている場合、View は次にデスクトップにログインしようとしたユーザーのために仮想マシンをパワーオンすることができません。GPU リソースの割り当てと vMotion の使用を管理して、リソースがデスクトップで使用できるようにする必要があります。

vSphere Client を使用して管理するオプションを選択したほうがよい状況

[vSphere Client を使用して管理] オプションを選択すると、vSphere Web Client を使用し、さまざまなオプションや VRAM 値を設定して個々の仮想マシンを構成できます。

- vSGA (Virtual Shared Graphics Acceleration) の場合は、プール内の仮想マシンに対して 3D レンダリングと VRAM サイズを組み合わせた構成をサポートできます。
- vDGA (Virtual Dedicated Graphics Acceleration) の場合は、各仮想マシンを個別に構成して特定の PCI デバイスを ESXi ホストと共有し、すべてのメモリを予約する必要があります。詳細については、[vDGA 機能の準備](#)を参照してください。

すべての ESXi ホストはバージョン 5.5 以降であり、GPU グラフィックス カードがインストールされている必要があります。

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

- vDGA を使用する AMD Multiuser GPU の場合は、各仮想マシンを個別に構成して特定の PCI デバイスを ESXi ホストと共有し、すべてのメモリを予約する必要があります。この機能を使用すると、1 つの PCI デバイスを複数の個別の物理 PCI デバイスのように扱うことができます。これにより GPU を 2 ～ 15 人のユーザーで共有できます。詳細については、[vDGA を使用する AMD Multiuser GPU の機能を使用する準備](#)を参照してください。

すべての ESXi ホストはバージョン 6.0 以降であり、GPU グラフィックス カードがインストールされている必要があります。

このオプションは、親仮想マシンからの設定をクローンに継承させることで、クローンとリンクされたクローンのグラフィック設定を明示的に管理する場合にも選択できます。

NVIDIA GRID vGPU オプションを使用したほうがよい状況

[NVIDIA GRID vGPU] オプションを使用すると、同じパフォーマンス レベルを確保しながら、vDGA を使用した場合よりも、NVIDIA GRID vGPU が有効な ESXi ホストで仮想マシンの統合率を高めることができます。vDGA (Dedicated Virtual Graphics) の場合と同様に、ESXi および仮想マシンも NVIDIA GRID vGPU に GPU パススルーを使用します。

注: 仮想マシンの統合率を向上させるために、統合モードを使用するように ESXi ホストを設定できます。/etc/vmware/config ファイルを ESXi ホストで編集して、次のエントリを追加します。

```
vGPU.consolidation = "true"
```

デフォルトの場合、ESXi ホストは、すでに割り当てられている仮想マシンの数が最も少ない物理 GPU に仮想マシンを割り当てます。これはパフォーマンス モードと呼ばれます。仮想マシンが最大数に到達するまで ESXi ホストが仮想マシンを同じ物理 GPU に割り当ててから、次の物理 GPU 上に仮想マシンを配置するようにする場合は、統合モードを使用できます。

GPU は 1 つの特定の仮想マシン専用にする必要はないため、[NVIDIA GRID vGPU] オプションを使用して、親仮想マシンまたは仮想マシンテンプレートで NVIDIA GRID vGPU が有効になるように作成および構成し、同じ物理 GPU を共有できる仮想マシンのデスクトップ プールを作成できます。

ESXi ホスト上のすべての GPU リソースが他の仮想マシンによって使用されている場合、次のユーザーがデスクトップにログインしようとする、View はクラスタ内の別の NVIDIA GRID vGPU が有効な ESXi サーバに仮想マシンを移動し、仮想マシンの電源をオンにすることができます。すべての ESXi ホストはバージョン 6.0 以降であり、GPU グラフィックス カードがインストールされている必要があります。

詳細については、[NVIDIA GRID vGPU 機能の準備](#)を参照してください。

ソフトウェア オプションを選択したほうがよい状況

[ソフトウェア] オプションは、ESXi 5.0 ホストしかない場合、ESXi 5.1 以降のホストに GPU グラフィックス カードがインストールされていない場合、ユーザーが AERO や Microsoft Office など、ハードウェア グラフィックス アクセラレーションを必要としないアプリケーションのみを実行する場合に選択します。

GPU リソースを管理するためのデスクトップ設定の構成

その他のデスクトップ設定を構成して、ユーザーがアクティブに使用しないときに GPU リソースが無駄にならないようにできます。

流動プールについては、ユーザーがデスクトップを使用していないときにその他のユーザーのために GPU リソースが開放されるようにセッション タイムアウトを設定します。

専用プールでは、ユーザーにとって適切であれば、[切断後に自動的にログオフ] 設定を [直後] および [サスペンド] 電源ポリシーに構成できます。たとえば、長時間のシミュレーションを実行する研究者のプールについては、これらの設定を使用しないでください。[NVIDIA GRID vGPU] オプションを使用する場合は、[サスペンド] 電源ポリシーを使用できないことに注意してください。

vDGA 機能の準備

Virtual Dedicated Graphics Acceleration (vDGA) では物理 GPU へのダイレクト パススルーが提供されます。これにより、ユーザーは単一の vGPU に無制限の専用アクセスを行うことができます。vDGA 機能を持つデスクトップ プールを作成する前に、仮想マシンおよび ESXi ホストで特定の構成タスクを実行する必要があります。

ここでは、View Administrator でデスクトップ プールを作成または構成するために vSphere で実行する必要のある作業の概要を説明します。詳細な情報と手順については、『VMware ホワイト ペーパー』のグラフィック アクセラレーションに関する項目を参照してください。

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

- 1 グラフィックス カードを ESXi ホストにインストールします。
- 2 GPU vSphere Installation Bundle (VIB) をインストールします。
- 3 VT-d または AMD IOMMU が ESXi ホストで有効になっていることを確認します。
- 4 PCI デバイスを仮想マシンに追加し、適切な PCI デバイスを選択して仮想マシンで GPU パススルーを有効にします。
- 5 仮想マシンの作成時に、すべてのメモリを予約します。
- 6 仮想マシンのビデオ カード 3D 機能を構成します。
- 7 GPU ベンダーから GPU ドライバを取得し、仮想マシンのゲスト OS に GPU デバイスのドライバをインストールします。
- 8 VMware Tools と Horizon Agent をゲスト OS にインストールし、再起動します。

これらのタスクを実行した後、仮想マシンを手動デスクトップ プールに追加し、PCoIP または VMware Blast Extreme を使用してゲスト OS にアクセスできるようにする必要があります。これで、PCoIP セッションまたは VMware Blast セッションで NVIDIA、AMD、または Intel ディスプレイ アダプタをゲスト OS でアクティベーションできるようになります。

NVIDIA GRID vGPU 機能の準備

NVIDIA GRID vGPU は ESXi ホストの物理 GPU への直接アクセスを提供し、これによって複数のユーザーは、ネイティブのグラフィック カード ドライバを使用して単一の GPU を共有できます。NVIDIA GRID vGPU 機能を持つデスクトップ プールを作成する前に、仮想マシンおよび ESXi ホストで特定の構成タスクを実行する必要があります。

ここでは、View Administrator でデスクトップ プールを作成または構成するために vSphere で実行する必要のある作業の概要を説明します。詳細な情報と手順については、『[NVIDIA GRID vGPU Deployment Guide for VMware Horizon 6.1](#)』を参照してください。

- 1 グラフィックス カードを ESXi ホストにインストールします。
- 2 GPU vSphere Installation Bundle (VIB) をインストールします。
- 3 VT-d または AMD IOMMU が ESXi ホストで有効になっていることを確認します。
- 4 GPU デバイスのパススルーを ESXi ホストで有効にします。
- 5 共有 PCI デバイスを仮想マシンに追加し、適切な PCI デバイスを選択して仮想マシンで GPU パススルーを有効にします。

共有 PCI デバイスを追加すると、ESXi ホストの GPU カードから使用できる、サポートされているすべてのグラフィックス プロファイル タイプのリストが表示されます。

- 6 仮想マシンの作成時に、すべてのメモリを予約します。
- 7 仮想マシンのビデオ カード 3D 機能を構成します。
- 8 GPU ベンダーから GPU ドライバを取得し、仮想マシンのゲスト オペレーティング システムに GPU デバイスのドライバをインストールします。
- 9 VMware Tools と Horizon Agent をゲスト OS にインストールし、再起動します。

これらのタスクを実行した後、仮想マシンを手動プールの View デスクトップ プールに追加し、PCoIP を使用してゲスト オペレーティング システムにアクセスできるようにする必要があります。これで、PCoIP セッションで NVIDIA ディスプレイ アダプタをゲスト オペレーティング システムでアクティブ化できるようになります。

この時点で、仮想マシンをテンプレートとして構成したり、仮想マシンのスナップショットを取得して View Composer リンククローン プールで基本イメージとして使用したりすることができます（スナップショットを取る前に、仮想マシンの電源をオフにする必要があります）。[デスクトップ プールの追加] ウィザードを使用する場合、[3D レンダラー] に [NVIDIA GRID vGPU] オプションを選択すると、NVIDIA GRID vGPU が有効な ESXi ホストと NVIDIA GRID vGPU が有効な仮想マシンのテンプレートとスナップショットのみがウィザードの選択肢として表示されます。

vDGA を使用する AMD Multiuser GPU の機能を使用する準備

vDGA を使用する AMD Multiuser GPU では物理 GPU へのダイレクト パススルーが提供されます。これにより、ユーザーは単一の GPU に無制限の専用アクセスを行うことができます。vDGA を使用する AMD Multiuser GPU を備えたデスクトップ プールを作成する前に、仮想マシンと ESXi ホストに特定の構成タスクを実行する必要があります。

ここでは、View Administrator でデスクトップ プールを作成または構成するために vSphere で実行する必要のある作業の概要を説明します。GPU デバイスのパススルーの有効化と仮想マシンへの PCI デバイスの追加については、[VMware ホワイト ペーパー](#)のグラフィック アクセラレーションに関する項目を参照してください。

- 1 グラフィックス カードを ESXi ホストにインストールします。
- 2 GPU vSphere Installation Bundle (VIB) をインストールします。
- 3 VT-d または AMD IOMMU が ESXi ホストで有効になっていることを確認します。

- 4 `esxcfg-module` コマンドを使用して、SR-IOV (Single Root I/O Virtualization) 用にグラフィックス カードを構成します。

[vDGA を使用する AMD Multiuser GPU の構成](#)を参照してください。

- 5 ESXi ホストを再起動します。
- 6 PCI デバイスを仮想マシンに追加し、適切な PCI デバイスを選択して仮想マシンで GPU パススルーを有効にします。
- 7 仮想マシンの作成時に、すべてのメモリを予約します。
- 8 仮想マシンのビデオ カード 3D 機能を構成します。
- 9 GPU ベンダーから GPU ドライバを取得し、仮想マシンのゲスト OS に GPU デバイスのドライバをインストールします。
- 10 VMware Tools と Horizon Agent をゲスト OS にインストールし、再起動します。

これらのタスクを実行した後、仮想マシンを手動デスクトップ プールに追加し、PCoIP または VMware Blast Extreme を使用してゲスト OS にアクセスできるようにする必要があります。vSphere を使用して仮想マシンにアクセスしようとすると、ディスプレイに黒い画面が表示されます。

vDGA を使用する AMD Multiuser GPU の構成

`esxcfg-module` コマンドライン コマンドを使用して、GPU を共有できるユーザー数、各ユーザーに割り当てられるフレーム バッファ容量、およびパフォーマンス制御などのパラメータを構成します。

構文

```
esxcfg-module -s "adapter1_conf=bus#,device#,function#,number_of_VFs,FB_size,time_slice,mode" amdgpuv
```

使用上の注意

`vicfg-module` コマンドでは、ESXi ホストの VMkernel モジュール オプションを設定および取得できます。このコマンドの一般的なリファレンス情報については、<http://pubs.vmware.com/vsphere-60/topic/com.vmware.vcli.ref.doc/vicfg-module.html> を参照してください。

必須フラグ

vDGA を使用する AMD Multiuser GPU を構成する場合、いくつかのフラグを指定する必要があります。コマンドにすべての必須フラグが含まれていない場合、エラー メッセージは表示されませんが、デフォルトの単純な 4 個の SR-IOV デバイス構成になります。

表 12-14. AMD SR-IOV を構成するフラグ

フラグ	説明
<i>bus#</i>	10 進数形式のバス番号。
<i>device#</i>	<p>サポートされている AMD カードの 10 進数形式の PCIe デバイス ID。リストを表示するには、<code>lspci grep -i display</code> コマンドを使用します。</p> <p>たとえば、2 つの AMD GPU カードのあるシステムの場合、このコマンドを実行すると、次のような出力が表示されます。</p> <pre>[root@host:~] lspci grep -i display 0000:04:00.0 Display controller: 0000:82:00.0 Display controller:</pre> <p>この例では、PCIe デバイス ID は 04 と 82 です。これらの ID は 16 進数形式で表示されるため、<code>vicfg-module</code> コマンドで使用するには、10 進数形式に変換する必要があります。</p> <p>AMD S7150 カードでは、カードごとに 1 つの GPU のみがサポートされるため、これらのカードのデバイス ID と機能 ID は 0 になります。</p>
<i>function#</i>	10 進数形式の機能番号。
<i>number_of_VFs</i>	2 ～ 15 の VF（仮想機能）の数。この数は、GPU を共有するユーザー数を表します。
<i>FB_size</i>	<p>各 VF に割り当てられるフレーム バッファ メモリの容量 (MB)。サイズを求めるには、カードのビデオ メモリの総容量を取得して、VF の数で割ります。次に、その数を最も近い 8 の倍数に丸めます。たとえば、8,000 MB の AMD S7150 カードの場合、次の設定を使用できます。</p> <ul style="list-style-type: none"> ■ 2 つの VF の場合、4096 を使用します。 ■ 4 つの VF の場合、2048 を使用します。 ■ 8 つの VF の場合、1024 を使用します。 ■ 15 つの VF の場合、544 を使用します。
<i>time_slice</i>	VF スイッチ間の間隔（マイクロ秒）。この設定を使用して、SR-IOV デバイス間のコマンドのキューイングおよび処理の遅延を調整します。3,000 ～ 40,000 の値を使用します。複数の SR-IOV デスクトップがアクティブになっているときに大きな途切れが発生する場合、この値を調整します。
<i>mode</i>	有効な値は次のとおりです。0 = 再利用したパフォーマンス、1 = 改善されたパフォーマンス（パーセンテージ）。

重要: `esxcfg-module` コマンドの実行後、設定を反映するには、ESXi ホストを再起動する必要があります。

例

- 1 8 人のユーザーで共有されている PCI ID 4 の 1 つの AMD S7150 カードの場合、次のようになります。

```
esxcfg-module -s "adapter1_conf=4,0,0,8,1024,4000" amdgpuv
```

- 2 4 人のパワー ユーザーで共有されている PCI ID 4 および PCI ID 82 の 2 つの AMD S7150 カードがある単独サーバの場合、次のようになります。

```
esxcfg-module -s "adapter1_conf=3,0,0,2,4096,4000 adapter2_conf=130,0,0,2,4096,4000" amdgpuv
```

- 3 2 つの AMD S7150 カードがある単独サーバの場合、各カードに異なるパラメータを設定できます。たとえば、View 環境で 2 人のパワー ユーザーと 16 人のタスク ワーカーをサポートする必要がある場合、次のようになります。

```
esxcfg-module -s "adapter1_conf=3,0,0,2,4096,4000 adapter2_conf=130,0,0,15,544,7000" amdgpuv
```

4 ESXi ホストで、SR-IOV オプションを有効にします。

一部のホストでは、BIOS で SR-IOV を構成できます。

ESXi ホストでの GPU リソースの調査

ESXi ホストで利用できる GPU リソースをより良く管理するために、現在の GPU リソース予約を調査できます。ESXi コマンド ラインの問い合わせユーティリティである `gpubvm` は、ESXi ホストにインストールされる GPU をリストし、ホストの各仮想マシンに予約される GPU メモリ量を表示します。この GPU メモリ予約は、仮想マシンの VRAM サイズと同じではないことに注意してください。

このユーティリティを実行するには、ESXi ホスト上のシェル プロンプトから `gpubvm` と入力します。ホストのコンソールまたは SSH 接続を使用できます。

たとえば、このユーティリティによって次のような出力が表示される場合があります。

```
~ # gpubvm
Xserver unix:0, GPU maximum memory 2076672KB
  pid 118561, VM "JB-w7-64-FC3", reserved 131072KB of GPU memory.
  pid 64408, VM "JB-w7-64-FC5", reserved 261120KB of GPU memory.
GPU memory left 1684480KB.
```

同様に、`nvidia-smi` コマンドを ESXi ホストで使用して NVIDIA GRID vGPU が有効な仮想マシン、消費されたフレーム バッファ メモリの量、および仮想マシンが使用されている物理 GPU のスロット ID のリストを表示できます。

View デスクトップへの RDP を使用したアクセスの防止

特定の View 環境では、RDP 表示プロトコルを使用した View デスクトップへのアクセスを禁止することが重要な場合があります。プール設定およびグループ ポリシー設定を構成することにより、ユーザーおよび管理者が RDP を使用して View デスクトップにアクセスすることを防止できます。

デフォルトの設定の場合、ユーザーは、View デスクトップ セッションにログイン中に RDP を使用して、View の外側から仮想マシンに接続できます。RDP 接続によって View デスクトップ セッションが終了し、View ユーザーの保存されていないデータや設定は失われます。View ユーザーは、外部の RDP 接続が閉じられるまで、デスクトップにログインできません。この状況を回避するには、`AllowDirectRDP` 設定を無効にします。

注: リモート デスクトップ サービスは、プールの作成に使用する仮想マシンおよびそのプールで展開される仮想マシン上で起動している必要があります。リモート デスクトップ サービスは Horizon Agent のインストール、SSO、およびその他の View のセッション管理操作に必要です。

前提条件

Horizon Agent の構成管理用テンプレート (ADM) ファイルが Active Directory にインストールされていることを確認します。 [View グループ ポリシー管理用テンプレート ファイルの使用](#)を参照してください。

手順

- 1 View 接続サーバが Horizon Client デバイスと通信するために使用する表示プロトコルとして PCoIP を選択します。

オプション	説明
デスクトップ プールを作成する	<ol style="list-style-type: none"> a View Administrator で、[デスクトップ プールの追加] ウィザードを起動します。 b [デスクトップ プールの設定] ページで、[VMware Blast] または [PCoIP] をデフォルト表示プロトコルとして選択します。
既存のデスクトップ プールを編集する	<ol style="list-style-type: none"> a View Administrator で、デスクトップ プールを選択し、[編集] をクリックします。 b [デスクトップ プールの設定] タブで、[VMware Blast] または [PCoIP] をデフォルト表示プロトコルとして選択します。

- 2 [ユーザーがプロトコルを選択できるようにする] 設定で [いいえ] を選択します。
- 3 AllowDirectRDP グループ ポリシー設定を無効にすることにより、Horizon Client を実行していないデバイスが、RDP 経由で直接 View デスクトップに接続するのを防ぎます。
 - a Active Directory サーバ上でグループ ポリシー管理コンソールを開き、[コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [従来の管理用テンプレート (ADM)] - [VMware Horizon Agent の構成] を選択します。
 - b AllowDirectRDP 設定を無効にします。

大規模なデスクトップ プールの展開

多くのユーザーが同じデスクトップ イメージを必要とする場合、単一のテンプレートまたは親仮想マシンから 1 つの大規模な自動プールを作成できます。単一の基本イメージとプール名を使用することで、マシンを個別に管理する必要のある小規模なグループに任意で分割するのを避けることができます。この戦略により、展開と管理タスクが簡素化されます。

大規模なプールをサポートするために、最大 32 台の ESXi ホストを含む ESXi クラスタでプールを作成できます。複数のネットワーク ラベルを使用するプールを構成して、複数のポート グループの IP アドレスをプールの仮想マシンで使用可能にすることもできます。

注: 複数のネットワーク ラベルの機能は、インスタント クローンでは使用できません。

8 台を超えるホストを含むクラスタでのデスクトップ プールの構成

vSphere 5.1 以降では、最大 32 の ESXi ホストを含むクラスタでリンク クローン デスクトップ プールを展開できます。クラスタ内のすべての ESXi ホストはバージョン 5.1 以降である必要があります。ホストは VMFS または NFS データストアを使用できます。VMFS データストアは、VMFS5 以降である必要があります。

vSphere 5.0 では、8 台を超える ESXi ホストを含むクラスタでリンク クローンを展開できますが、この場合は NFS データストアにレプリカ ディスクを格納する必要があります。VMFS データストアでレプリカ ディスクを格納できるのは、8 台以下のホストを含むクラスタの場合のみです。

vSphere 5.0 で 8 台を超えるホストを含むクラスタでリンク クローン プールを構成する場合は、次のルールが適用されます。

- OS ディスクと同じデータストアにレプリカ ディスクを格納する場合は、レプリカと OS ディスクを NFS データストアに格納する必要があります。
- OS ディスクとは別のデータストアにレプリカ ディスクを格納する場合は、レプリカ ディスクを NFS データストアに格納する必要があります。OS ディスクは、NFS データストアまたは VMFS データストアに格納できます。
- View Composer 通常ディスクを別のデータストアに格納する場合、通常ディスクは NFS データストアまたは VMFS データストアで構成できます。

vSphere 4.1 以前のリリースでは、8 台以下のホストを含むクラスタでのみデスクトップ プールを展開できます。

デスクトップ プールへの複数のネットワーク ラベルの割り当て

View 5.2 以降のリリースでは、複数のネットワーク ラベルを使用するように自動デスクトップ プールを構成できます。複数のネットワーク ラベルを、リンク クローン プール、またはフル仮想マシンを含む自動プールに割り当てられます。

注: 複数のネットワーク ラベルの機能は、インスタント クローンでは使用できません。

以前のリリースでは、プール内の仮想マシンが親仮想マシンまたはテンプレートの NIC で使用されていたネットワーク ラベルを継承していました。一般的な親仮想マシンまたはテンプレートには、1 つの NIC と 1 つのネットワーク ラベルが含まれています。ネットワーク ラベルによって、ポート グループと VLAN が定義されます。1 つの VLAN のネットマスクによって、一般的に使用可能な IP アドレスの範囲が制限されます。

View 5.2 以降のリリースでは、デスクトップ プールが展開されるクラスタ内のすべての ESXi ホスト用に、vCenter Server で使用可能なネットワーク ラベルを割り当てられます。プール用に複数のネットワーク ラベルを構成することにより、プール内の仮想マシンに割り当てられる IP アドレスの数を大幅に増やすことができます。

複数のネットワーク ラベルをプールに割り当てるには、View PowerCLI cmdlet を使用する必要があります。このタスクを View Administrator で実行することはできません。

View PowerCLI を使用したこのタスクの実行の詳細については、『View の統合』の「View PowerCLI の使用」の章の「デスクトップ プールに複数のネットワーク ラベルを割り当てる」を参照してください。

資格のあるユーザーとグループ

資格を構成して、ユーザーがアクセス可能なリモート デスクトップとアプリケーションを制御することができます。制限付き資格の機能を構成して、ユーザーがリモート デスクトップを選択する際に、接続先の View 接続サーバー インスタンスに基づいてデスクトップ アクセスを制御することもできます。ネットワークの外部にいるユーザー セットがネットワーク内のリモート デスクトップやアプリケーションに接続することを制限することもできます。

Cloud Pod アーキテクチャ環境では、グローバル資格を作成して、ポッド フェデレーション内の複数のポッドをまたぐ複数のデスクトップに対してユーザーまたはグループに資格を付与します。グローバル資格を使用する場合、リモート デスクトップのローカル資格を構成および管理する必要はありません。グローバル資格および Cloud Pod アーキテクチャ環境の設定については、『View Cloud Pod アーキテクチャの管理』を参照してください。

この章には、次のトピックが含まれています。

- デスクトップまたはアプリケーション プールへの資格の追加
- デスクトップまたはアプリケーション プールからの資格の削除
- デスクトップまたはアプリケーション プールの資格の確認
- リモート デスクトップ アクセスの制限
- ネットワーク外部のリモート デスクトップ アクセスの制限

デスクトップまたはアプリケーション プールへの資格の追加

ユーザーがリモート デスクトップまたはアプリケーションにアクセスするには、デスクトップまたはアプリケーション プールを使用するための資格を付与されている必要があります。

前提条件

デスクトップまたはアプリケーション プールを作成します。

手順

- 1 デスクトップまたはアプリケーション プールを選択します。

オプション	操作
デスクトップ プールに対する資格の追加	View Administrator で、[カタログ] - [デスクトップ プール] を選択して、デスクトップ プールの名前をクリックします。
アプリケーション プールに対する資格の追加	View Administrator で、[カタログ] - [アプリケーション プール] を選択して、アプリケーション プールの名前をクリックします。

- 2 [資格] ドロップダウン メニューから [資格を追加] を選択します。
- 3 [追加] をクリックして、1 つ以上の検索基準を選択し、[検索] をクリックして検索基準に基づいてユーザーまたはグループを検索します。

注: 混在モードのドメインでは、ドメイン ローカル グループは検索結果から除外されます。ドメインが混在モードで構成されている場合は、ドメイン ローカル グループ内のユーザーに資格を付与することはできません。

- 4 プール内のデスクトップまたはアプリケーションに対する資格を付与するユーザーまたはグループを選択して、[OK] をクリックします。
- 5 [OK] をクリックして変更を保存します。

デスクトップまたはアプリケーション プールからの資格の削除

デスクトップまたはアプリケーション プールから資格を削除して、特定のユーザーまたはグループがデスクトップまたはアプリケーションにアクセスできないようにすることができます。

手順

- 1 デスクトップまたはアプリケーション プールを選択します。

オプション	説明
デスクトップ プールの資格の削除	View Administrator で、[カタログ] - [デスクトップ プール] を選択し、デスクトップ プールの名前をクリックします。
アプリケーション プールの資格の削除	View Administrator で、[カタログ] - [アプリケーション プール] を選択し、アプリケーション プールの名前をクリックします。

- 2 [資格] ドロップダウン メニューから [資格を削除] を選択します。
- 3 資格を削除するユーザーまたはグループを選択し、[削除] をクリックします。
- 4 [OK] をクリックして変更を保存します。

デスクトップまたはアプリケーション プールの資格の確認

ユーザーまたはグループが資格を付与されているデスクトップまたはアプリケーション プールを確認できます。

手順

- 1 View Administrator で、[ユーザーとグループ] を選択し、ユーザーまたはグループの名前をクリックします。

- 2 [資格] タブをクリックして、ユーザーまたはグループが資格を付与されているデスクトップまたはアプリケーション プールを確認します。

オプション	操作
ユーザーまたはグループが資格を付与されているデスクトップ プールを一覧表示する	[デスクトップ プール] をクリックします。
ユーザーまたはグループが資格を付与されているアプリケーション プールを一覧表示する	[アプリケーション プール] をクリックします。

リモート デスクトップ アクセスの制限

制限付き資格を構成して、ユーザーがデスクトップを選択する際に、接続先の View 接続サーバ インスタンスに基づいてリモート デスクトップ アクセスを制限することができます。

制限付き資格では、1 つ以上のタグを View 接続サーバ インスタンスに割り当てます。その後、デスクトップ プールを構成するときに、デスクトップ プールにアクセスできるようにする View 接続サーバ インスタンスのタグを選択します。

ユーザーがタグ付きの View 接続サーバ インスタンスを通してログインするとき、ユーザーは少なくとも 1 つのタグが一致するか、タグがないデスクトップ プールにのみアクセスできます。

注: リモート アプリケーションへのアクセスを制限するために制限付き資格の機能を構成することはできません。

■ 制限付き資格の例

この例は、2 つの View 接続サーバ インスタンスを含む View 展開を示しています。第 1 のインスタンスは内部ユーザーをサポートします。第 2 のインスタンスはセキュリティ サーバと対になって、外部ユーザーをサポートします。

■ タグ一致

制限付き資格の機能は、タグの一致を使用して、View 接続サーバ インスタンスが特定のデスクトップ プールにアクセスできるかどうかを決定します。

■ 制限付き資格に関する考慮事項と制限事項

制限付き資格を実装する前に、考慮事項と制限事項について理解しておく必要があります。

■ View 接続サーバ インスタンスへのタグの割り当て

View 接続サーバ インスタンスにタグを割り当てると、その View 接続サーバに接続するユーザーは、一致するタグを持っているか、またはタグがないデスクトップ プールにのみアクセスできます。

■ デスクトップ プールへのタグの割り当て

デスクトップ プールにタグを割り当てると、一致するタグを持つ View 接続サーバ インスタンスに接続したユーザーのみが、そのプール内のデスクトップにアクセスできます。

制限付き資格の例

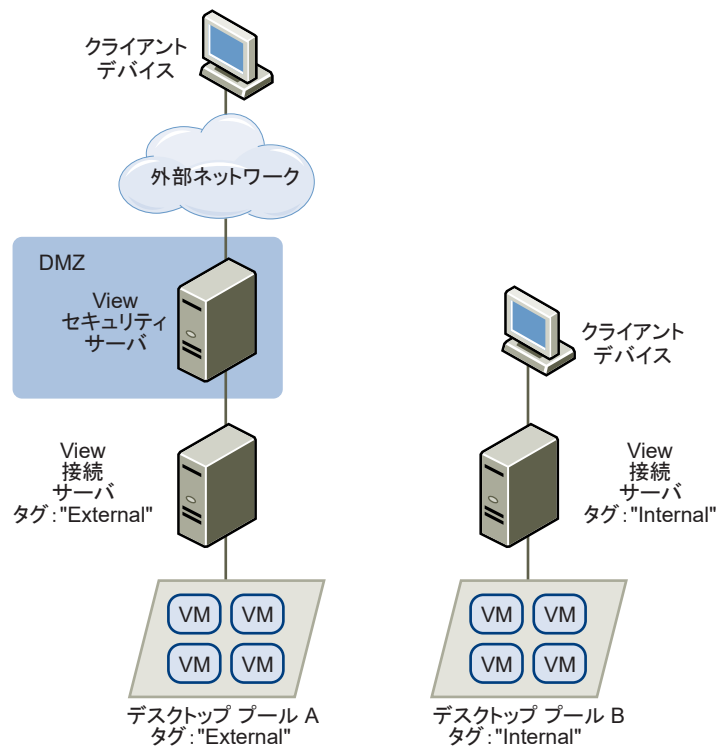
この例は、2 つの View 接続サーバ インスタンスを含む View 展開を示しています。第 1 のインスタンスは内部ユーザーをサポートします。第 2 のインスタンスはセキュリティ サーバと対になって、外部ユーザーをサポートします。

外部ユーザーが特定のデスクトップにアクセスできないようにするには、次のように制限付き資格を設定します。

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

外部ユーザーは、External というタグの付いた View 接続サーバを使用してログインするので、Internal というタグの付いたデスクトップ プールにはアクセスできません。また、内部ユーザーは、Internal というタグの付いた View 接続サーバを使用してログインするので、External というタグの付いたデスクトップ プールにはアクセスできません。図 13-1. 制限付き資格の構成 は、この構成を示しています。

図 13-1. 制限付き資格の構成



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

タグ一致

制限付き資格の機能は、タグの一致を使用して、View 接続サーバ インスタンスが特定のデスクトップ プールにアクセスできるかどうかを決定します。

最も基本的なレベルでは、タグの一致は、特定のタグを持つ View 接続サーバ インスタンスが同じタグを持つデスクトップ プールにアクセスできることを決定します。

タグの割り当てがないことも、View 接続サーバ インスタンスがデスクトップ プールにアクセスできるかどうかに影響を与える場合があります。たとえば、タグを持たない View 接続サーバ インスタンスは、やはりタグを持たないデスクトップ プールにのみアクセスできます。

表 13-1. **タグ一致のルール** では、制限された資格機能により View Connection Server がデスクトップ プールにアクセスできる時期を決定する方法について示します。

表 13-1. **タグ一致のルール**

View 接続サーバ	デスクトップ プール	アクセスの許可
タグなし	タグなし	行う
タグなし	1 つ以上のタグ	×
1 つ以上のタグ	タグなし	行う
1 つ以上のタグ	1 つ以上のタグ	タグが一致する場合のみ

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

制限付き資格に関する考慮事項と制限事項

制限付き資格を実装する前に、考慮事項と制限事項について理解しておく必要があります。

- 1 つの View 接続サーバ インスタンスまたはデスクトップ プールが、複数のタグを持つことができます。
- 複数の View 接続サーバ インスタンスおよびデスクトップ プールが、同じタグを持つことができます。
- タグを持たないデスクトップ プールには、すべての View 接続サーバ インスタンスがアクセスできます。
- タグを持たない View 接続サーバ インスタンスは、やはりタグを持たないデスクトップ プールにのみアクセスできます。
- セキュリティ サーバを使用する場合は、セキュリティ サーバと対になっている View 接続サーバ インスタンスに制限付き資格を構成する必要があります。セキュリティ サーバに制限付き資格を構成することはできません。
- あるタグがデスクトップ プールにまだ割り当てられていて、そのタグがただ 1 つの View 接続サーバ インスタンスに割り当てられている場合、その View 接続サーバ インスタンスでそのタグを変更または削除することはできません。
- 制限付き資格は、他のデスクトップ 資格またはデスクトップ 割り当てより優先されます。たとえば、ユーザーに特定のマシンが割り当てられている場合でも、デスクトップ プールのタグが、ユーザーが接続している View 接続サーバ インスタンスに割り当てられているタグと一致しない場合、ユーザーはそのマシンにアクセスできません。
- VMware Identity Manager からデスクトップ へのアクセスを提供することを意図して View 接続サーバ 制限を構成すると、これらのデスクトップ が実際には制限されている場合でも VMware Identity Manager アプリケーションでユーザーにデスクトップ が表示されることがあります。VMware Identity Manager ユーザーがデスクトップ にログインを試みると、デスクトップ プールのタグが、ユーザーが接続する View 接続サーバ インスタンスに指定されているタグと一致しなければ、デスクトップ は起動されません。

View 接続サーバ インスタンスへのタグの割り当て

View 接続サーバ インスタンスにタグを割り当てると、その View 接続サーバに接続するユーザーは、一致するタグを持っているか、またはタグがないデスクトップ プールにのみアクセスできます。

手順

- 1 View Administrator で、[View 構成] - [サーバ] を選択します。
- 2 [接続サーバ] タブをクリックし、View 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 [タグ] テキスト ボックスに 1 つ以上のタグを入力します。
複数のタグはカンマまたはセミコロンで区切ります。
- 4 [OK] をクリックして変更を保存します。

次のステップ

デスクトップ プールにタグを割り当てます。

デスクトップ プールへのタグの割り当て

デスクトップ プールにタグを割り当てると、一致するタグを持つ View 接続サーバ インスタンスに接続したユーザーのみが、そのプール内のデスクトップにアクセスできます。

デスクトップ プールを追加または編集するときに、タグを割り当てることができます。

前提条件

- 1 つ以上の View 接続サーバ インスタンスにタグを割り当てます。

手順

- 1 View Administrator で、[カタログ] - [デスクトップ プール] を選択します。
- 2 タグを割り当てるプールを選択します。

オプション	操作
新しいプールにタグを割り当てる	[追加] をクリックして [デスクトップ プールを追加] ウィザードを起動し、プールを定義して識別します。
既存のプールにタグを割り当てる	プールを選択し、[編集] をクリックします。

- 3 [デスクトップ プールの設定] ページに移動します。

オプション	操作
新しいプールのプール設定	[デスクトップ プールを追加] ウィザードで、[デスクトップ プールの設定] をクリックします。
既存のプールのプール設定	[デスクトップ プールの設定] タブをクリックします。

- 4 [接続サーバの制限] の横にある [参照] をクリックし、デスクトップ プールにアクセスできる View 接続サーバ インスタンスを構成します。

オプション	操作
プールをすべての View 接続サーバ インスタンスからアクセス可能にする	[制限なし] を選択します。
プールをこれらのタグを持つ View 接続サーバ インスタンスからのみアクセス可能にする	[次のタグに制限] を選択し、1 つ以上のタグを選択します。チェック ボックスを使用して複数のタグを選択できます。

- 5 [OK] をクリックして変更を保存します。

ネットワーク外部のリモート デスクトップ アクセスの制限

資格が付与されている特定のユーザーとグループについて外部ネットワークからのアクセスを許可し、資格が付与されている他のユーザーとグループについてはアクセスを制限することができます。資格が付与されたすべてのユーザーは、内部ネットワークにあるデスクトップおよびアプリケーションにアクセスできます。特定のユーザーによる外部ネットワークからのアクセスを制限しない場合、資格が付与されているすべてのユーザーが外部ネットワークからアクセスできるようになります。

セキュリティ上の理由で、管理者は外部ネットワークのユーザーとグループによるネットワーク内のリモート デスクトップおよびアプリケーションへのアクセスを制限する必要がある場合があります。制限されているユーザーが外部ネットワークからシステムにアクセスすると、ユーザーにシステムを使用する資格が付与されていないことを伝えるメッセージが表示されます。デスクトップおよびアプリケーション プールの資格を取得するには、ユーザーは内部ネットワークの中にいる必要があります。

ネットワーク外部のユーザーの制限

特定のユーザーとグループについてはネットワークの外部から View 接続サーバへのアクセスを許可し、その他のユーザーとグループについてはアクセスを制限できます。

前提条件

- ユーザーに資格が付与される View 接続サーバへのゲートウェイとして、Access Point アプライアンス、セキュリティ サーバ、またはロード バランサは、ネットワークの外部にデプロイする必要があります。Access Point アプライアンスのデプロイの詳細については、『Access Point の導入および設定』を参照してください。
- リモートからアクセスするユーザーには、デスクトップやアプリケーション プールへの資格を付与する必要があります。

手順

- 1 View Administrator で、[ユーザーとグループ] を選択します。
- 2 [リモート アクセス] タブをクリックします。
- 3 [追加] をクリックして、1 つ以上の検索基準を選択し、[検索] をクリックして検索基準に基づいてユーザーまたはグループを検索します。
- 4 ユーザーまたはグループにリモート アクセスを提供するには、ユーザーまたはグループを選択して、[OK] をクリックします。

- 5 特定のユーザーまたはグループからリモート アクセスを削除するには、そのユーザーまたはグループを選択して、[削除] をクリックしてから、[OK] をクリックします。

リモート デスクトップ機能の構成

Horizon Agent とともにインストールされる特定のリモート デスクトップ機能は、コア View リリースおよび Feature Pack アップデートのリリースで更新できます。これらの機能を構成して、エンド ユーザーのリモート デスクトップ エクスペリエンスを強化できます。

これらの機能には HTML Access、Unity Touch、Flash URL リダイレクト、リアルタイム オーディオ ビデオ、Windows Media マルチメディア リダイレクト (MMR)、USB リダイレクト、スキャナ リダイレクト、シリアル ポート リダイレクトなどがあります。

HTML Access の詳細については、VMware Horizon Client ドキュメントの Web ページにある『HTML Access の使用』を参照してください。

USB リダイレクトの詳細については、[15 章 リモート デスクトップおよびアプリケーションでの USB デバイスの使用](#)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。

- [Unity Touch の構成](#)
- [マルチキャストまたはユニキャスト ストリーミング用の Flash URL リダイレクトの構成](#)
- [Flash リダイレクトの構成](#)
- [URL コンテンツ リダイレクトの構成](#)
- [リアルタイム オーディオ ビデオの構成](#)
- [スキャナ リダイレクトの構成](#)
- [シリアル ポート リダイレクトの構成](#)
- [Windows Media マルチメディア リダイレクト \(MMR\) へのアクセスの管理](#)
- [クライアント ドライブ リダイレクトへのアクセスの管理](#)
- [コピーおよび貼り付け操作におけるクリップボードのデータ形式の制限](#)

Unity Touch の構成

Unity Touch を使用すれば、タブレットおよびスマートフォン ユーザーは Windows アプリケーションやファイルの参照、検索、およびオープンを簡単に行ったり、お気に入りのアプリケーションやファイルを選択したり、スタート メニューまたはタスクバーを使用せずに実行しているアプリケーションを切り替えることができます。Unity Touch サイドバーに表示されるデフォルトのお気に入りアプリケーションのリストを構成できます。

[Unity Touch を有効化] グループ ポリシー設定を構成すると、Unity Touch のインストール後に Unity Touch 機能を無効または有効にできます。 [Horizon Agent の構成 ADM テンプレートの設定](#)を参照してください。

iOS および Android デバイス向けの VMware Horizon Client ドキュメントには、Unity Touch で提供されるエンド ユーザー機能についての詳細が記載されています。

Unity Touch のシステム要件

Horizon Client をインストールする Horizon Client ソフトウェアおよびモバイル デバイスは、Unity Touch をサポートするために特定のバージョン要件を満たす必要があります。

View デスクトップ

Unity Touch をサポートため、以下のソフトウェアは、エンド ユーザーがアクセスする仮想マシンにインストールする必要があります：

- View Agent 6.0 以降をインストールすることにより、Unity Touch 機能をインストールします。 [仮想マシンへの Horizon Agent のインストール](#)を参照してください。
- オペレーティング システム：Windows 7（32 ビットまたは 64 ビット）、Windows 8（32 ビットまたは 64 ビット）、Windows 8.1（32 ビットまたは 64 ビット）、Windows Server 2008 R2 または Windows Server 2012 R2、Windows 10（32 ビットまたは 64 ビット）

Horizon Client ソフトウェア

Unity Touch は以下の Horizon Client バージョンでサポートされます：

- iOS 版 Horizon Client 2.0 以降
- Android 版 Horizon Client 2.0 以降

モバイル デバイス オペレーティング システム

Unity Touch は以下のモバイル デバイス オペレーティング システムでサポートされます：

- iOS 5.0 以降
- Android 3（Honeycomb）、Android 4（Ice Cream Sandwich）、および Android 4.1/4.2（Jelly Bean）。

Unity Touch で表示されるお気に入りアプリケーションの構成

Unity Touch 機能を使用すれば、タブレットおよびスマートフォン ユーザーは、Unity Touch スライドバーから View デスクトップ アプリケーションまたはファイルに素早く移動できます。エンド ユーザーはサイドバーにどのお気に入りアプリケーションが表示されるかを指定できますが、利便性のために管理者はお気に入りアプリケーションのデフォルト リストを構成できます。

流動割り当てデスクトップ プールを使用する場合、エンド ユーザーが指定するお気に入りのアプリケーションおよびお気に入りのファイルは、Active Directory でローミング ユーザー プロファイルを有効にしない限り、デスクトップから切断すると失われます。

お気に入りのアプリケーションのデフォルト リストは、エンド ユーザーが Unity Touch が有効になっているデスクトップに最初に接続したときに有効になります。ただし、ユーザーが自分のお気に入りのアプリケーション リストを構成すると、デフォルト リストは無視されます。ユーザーのお気に入りのアプリケーション リストは、ユーザーのローミング プロファイルに残り、流動プールまたは専用プールで別のマシンにユーザーが接続すると使用できるようになります。

お気に入りのアプリケーションのデフォルト リストを作成し、1 つ以上のアプリケーションが View デスクトップ オペレーティング システムにインストールされない場合やそれらのアプリケーションへのパスが [スタート] メニューに表示されない場合、アプリケーションはお気に入りのリストに表示されません。この動作を使用して、代替のアプリケーションの異なるセットで複数の仮想マシン イメージに適用できるお気に入りのアプリケーションのマスター デフォルト リストを設定することができます。

たとえば、Microsoft Office と Microsoft Visio が 1 台の仮想マシンにインストールされ、Windows Powershell と VMware vSphere Client が 2 台目の仮想マシンにインストールされている場合、4 つのアプリケーションすべてを含む 1 つのリストを作成できます。インストールされたアプリケーションだけが、それぞれのデスクトップにデフォルトのお気に入りのアプリケーションとして表示されます。

異なる方法を使用して、お気に入りのアプリケーションのデフォルト リストを指定できます。

- デスクトップ プール内の仮想マシンの Windows レジストリに値を追加します
- Horizon Agent インストーラから管理インストール パッケージを作成し、仮想マシンにそのパッケージを配布します
- 仮想マシンのコマンド ラインから Horizon Agent インストーラを実行します

注: Unity Touch では、[スタート] メニューの [プログラム] フォルダにアプリケーションへのショートカットが置かれていると想定しています。ショートカットが [プログラム] フォルダの外に置かれている場合、プリフィックス **Programs** をショートカット パスに追加します。たとえば、Windows Update.lnk は ProgramData \Microsoft\Windows\Start Menu フォルダに格納されています。デフォルトのお気に入りのアプリケーションとしてこのショートカットをパブリッシュするには、プリフィックス **Programs** をショートカット パスに追加します。たとえば、"Programs/Windows Update.lnk" です。

前提条件

- Horizon Agent が仮想マシンにインストールされていることを確認します。
- 仮想マシンに対して管理者権限を持っていることを確認します。この手順では、レジストリ設定を編集する必要はありません。
- 流動割り当てデスクトップ プールを使用する場合、Active Directory を使用してローミング ユーザー プロファイルを設定します。Microsoft によって提供されている手順に従ってください。

流動割り当てデスクトップ プールのユーザーには、ログインするたびにお気に入りのアプリケーションおよびお気に入りのファイルのリストが表示されます。

手順

- ◆ (オプション) Windows レジストリに値を追加してお気に入りのアプリケーションのデフォルト リストを作成します。

- a regedit を開き、HKLM\Software\VMware, Inc.\VMware Unity レジストリ設定に移動します。

64 ビット仮想マシンでは、HKLM\Software\Wow6432Node\VMware, Inc.\VMware Unity ディレクトリに移動します。

- b FavAppList と呼ばれる文字列値を作成します。
- c デフォルトのお気に入りのアプリケーションを指定します。

以下のフォーマットを使用して、[スタート] メニューで使用されるアプリケーションへのショートカット パスを指定します。

```
path-to-app-1|path-to-app-2|path-to-app-3|...
```

例 :

```
Programs/Accessories/Accessibility/Speech Recognition.lnk|Programs/VMware/VMware vSphere Client.lnk|Programs/Microsoft Office/Microsoft Office 2010 Tools/Microsoft Office 2010 Language Preferences.lnk
```

- ◆ (オプション) Horizon Agent インストーラから管理インストール パッケージを作成してお気に入りのアプリケーションのデフォルト リストを作成します。

- a コマンド ラインから、以下のフォーマットを使用して管理インストール パッケージを作成します。

```
VMware-viewagent-x86_64-y.y.y-xxxxxx.exe /s /a /v"/qn TARGETDIR=""a network share to store the admin install package"" UNITY_DEFAULT_APPS=""the list of default favorite apps that should be set in the registry"""
```

例 :

```
VMware-viewagent-x86_x64-y.y.y-xxxxxx.exe /s /a /v"/qn TARGETDIR=""\\foo-installer-share\viewfeaturepack\""" UNITY_DEFAULT_APPS=""Programs/Accessories/Accessibility/Ease of Access.lnk|Programs/Accessories/System Tools/Character Map.lnk|Programs/Accessories/Windows PowerShell/Windows PowerShell.lnk|Programs/Internet Explorer (64-bit).lnk|Programs/Google Chrome/Google Chrome.lnk|Programs/iTunes/iTunes.lnk|Programs/Microsoft Office/Microsoft SharePoint Workspace 2010.lnk|Programs/PuTTY/PuTTY.lnk|Programs/Skype/Skype.lnk|Programs/WebEx/Productivity Tools/WebEx Settings.lnk|"""
```

- b 社内で導入されている標準の Microsoft Windows Installer (MSI) 展開ツールを使用して、ネットワーク共有からデスクトップ仮想マシンに管理インストール パッケージを配布します。

- ◆ (オプション) 仮想マシンにコマンド ラインで直接 Horizon Agent インストーラを実行してお気に入りのアプリケーションのデフォルト リストを作成します。

次のフォーマットを使用します。

```
VMware-viewagent-x86_x64-y.y.y-xxxxxx.exe /s /v"/qn UNITY_DEFAULT_APPS=""the list of default favorite apps that should be set in the registry""
```

注: 上記のコマンドは、Horizon Agent のインストールと、お気に入りアプリケーションのデフォルト リストの指定を組み合わせたものです。このコマンドを実行する前に Horizon Agent をインストールする必要はありません。

次のステップ

仮想マシンでこのタスクを直接実行した場合 (Windows レジストリを編集するか、コマンド ラインから Horizon Agent をインストールすることによって)、新たに構成した仮想マシンをデプロイする必要があります。スナップショットまたはテンプレートを作成してからデスクトップ プールを作成することも、既存のプールを再構成することもできます。または、Active Directory グループ ポリシを作成して新しい構成を導入することができます。

マルチキャストまたはユニキャスト ストリーミング用の Flash URL リダイレクトの構成

Adobe Media Server およびマルチキャストまたはユニキャストを使用して仮想デスクトップ インフラストラクチャ (VDI) 環境でライブ ビデオ イベントを配信できるようになりました。VDI 環境でマルチキャストまたはユニキャストのライブ ビデオ ストリームを配信するには、メディア ストリームを、リモート デスクトップをバイパスしてメディア ソースからエンド ポイントに直接送信する必要があります。Flash URL リダイレクト機能は、リモート デスクトップからクライアント エンドポイントに ShockWave Flash (SWF) ファイルをインターセプトおよびリダイレクトすることで、この機能をサポートします。

そして、Flash コンテンツは、クライアントのローカル Flash メディア プレーヤを使用して表示されます。

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

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

Flash URL リダイレクトを構成するには、HTML Web ページおよびクライアント デバイスをセットアップする必要があります。

手順

1 Flash URL リダイレクトのシステム要件

Flash URL リダイレクトをサポートするには、View の展開が特定のソフトウェアおよびハードウェア要件を満たす必要があります。

2 Flash URL リダイレクト機能がインストールされていることの確認

この機能を使用する前に、Flash URL リダイレクト機能がインストールされ、仮想デスクトップで実行されていることを確認します。

3 マルチキャストまたはユニキャストのストリームを提供する Web ページの設定

Flash URL リダイレクトの実行を許可するには、マルチキャストまたはユニキャストのストリームにリンクを提供する MIME HTML (MHTML) Web ページに JavaScript コマンドを組み込む必要があります。ユーザーはビデオ ストリームにアクセスするために、リモート デスクトップのブラウザでこれらの Web ページを表示します。

4 Flash URL リダイレクト用にクライアント デバイスを設定

Flash URL リダイレクト機能は、リモート デスクトップからクライアント デバイスに SWF ファイルをリダイレクトします。これらのデバイスでマルチキャストまたはユニキャストのストリームから Flash ビデオの再生を許可するには、適切な Adobe Flash Player がクライアント デバイスにインストールされていることを確認する必要があります。クライアントは、メディア ソースに対する IP 接続性を持つ必要もあります。

5 Flash URL リダイレクトを無効または有効

Flash URL リダイレクトは、VDM_FLASH_URL_REDIRECTION=1 プロパティを指定して Horizon Agent のサイレント インストールを実行すると有効になります。選択されたリモート デスクトップの Windows レジストリ キーの値を設定することで、それらの仮想マシンでの Flash URL リダイレクト機能を無効にするか、または再度有効にすることができます。

Flash URL リダイレクトのシステム要件

Flash URL リダイレクトをサポートするには、View の展開が特定のソフトウェアおよびハードウェア要件を満たす必要があります。

View デスクトップ

- Flash URL リダイレクトは、View Agent 6.0 以降のサイレント インストールでコマンド ラインに VDM_FLASH_URL_REDIRECTION プロパティを指定することによってインストールします。 [Horizon Agent のサイレント インストール プロパティ](#) を参照してください。
- デスクトップは、64 ビットまたは 32 ビットの Windows 7 オペレーティングシステムで実行する必要があります。

- サポートされているデスクトップ ブラウザには、Internet Explorer 8、9、および 10、Chrome 29.x および Firefox 20.xが含まれます。

Flash メディア プレイヤー と ShockWave Flash (SWF)

Strobe Media Playback などの適切な Flash メディア プレイヤーを、お使いの Web サイトに統合する必要があります。マルチキャスト コンテンツをストリーミングするには、お使いの Web ページで `multicastplayer.swf` または `StrobeMediaPlayback.swf` を使用できます。ライブのユニキャスト コンテンツをストリーミングするには、`StrobeMediaPlayback.swf` を使用する必要があります。RTMP ストリーミングや HTTP ダイナミック ストリーミングなどの、サポートされる他の機能には、`StrobeMediaPlayback.swf` も使用できます。

Horizon Client ソフトウェア

次の Horizon Client リリースは、マルチキャストとユニキャストをサポートしています。

- Linux 版 Horizon Client 2.2 または以降のリリース
- Windows 版 Horizon Client 2.2 または以降のリリース

以下の Horizon Client リリースはマルチキャストのみをサポートしています (ユニキャストはサポートしていません)。

- Linux 版 Horizon Client 2.0 または 2.1
- Windows 版 Horizon Client 5.4

Horizon Client コンピュータ またはクライアント アク セス デバイス

- Flash URL リダイレクトは、x86 シン クライアント デバイスで Linux 版 Horizon Client を実行するすべてのオペレーティング システムでサポートされます。この機能は ARM プロセッサではサポートされません。
- Flash URL リダイレクトは、Windows 版 Horizon Client を実行するすべてのオペレーティング システムでサポートされます。詳細については、『Windows 版 VMware Horizon Client の使用』を参照してください。
- Windows クライアント デバイスでは、Internet Explorer 用の Adobe Flash Player 10.1 以降をインストールする必要があります。
- Linux シン クライアント デバイスでは、`libexpat.so.0` と `libflashplayer.so` ファイルをインストールする必要があります。[Flash URL リダイレクト用にクライアント デバイスを設定](#)を参照してください。

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

Flash URL リダイレクト機能がインストールされていることの確認

この機能を使用する前に、Flash URL リダイレクト機能がインストールされ、仮想デスクトップで実行されていることを確認します。

Flash URL リダイレクト機能は、マルチキャストまたはユニキャストのリダイレクトを使用するすべてのデスクトップにインストールしておく必要があります。Horizon Agent のインストール手順については、[Horizon Agent のサイレント インストール プロパティ](#)を参照してください。

手順

- 1 PCoIP を使用するリモート デスクトップ セッションを開始します。
- 2 タスク マネージャを開きます。
- 3 ViewMPServer.exe プロセスがデスクトップで動作していることを確認します。

マルチキャストまたはユニキャストのストリームを提供する Web ページの設定

Flash URL リダイレクトの実行を許可するには、マルチキャストまたはユニキャストのストリームにリンクを提供する MIME HTML (MHTML) Web ページに JavaScript コマンドを組み込む必要があります。ユーザーはビデオ ストリームにアクセスするために、リモート デスクトップのブラウザでこれらの Web ページを表示します。

また、Flash URL リダイレクトで問題が発生した場合にエンド ユーザーに対して表示される英語のエラー メッセージをカスタマイズできます。各国語のエラー メッセージをエンド ユーザーに対して表示する場合は、このオプションの手順を実行します。var vmwareScriptErrorMessage 構成を各国語のテキスト文字列と一緒に MHTML Web ページに埋め込む必要があります。

前提条件

swfobject.js ライブラリが MHTML Web ページにインポートされていることを確認します。

手順

- 1 MHTML Web ページに viewmp.js JavaScript コマンドを組み込みます。

例: <script type="text/javascript" src="http://localhost:33333/viewmp.js"></script>

- 2 (オプション) エンド ユーザーに送信される Flash URL リダイレクトのエラー メッセージをカスタマイズします。

例: "var vmwareScriptErrorMessage=localized error message"

- 3 ShockWave Flash (SWF) ファイルが MHTML Web ページにインポートされる前に、viewmp.js JavaScript コマンドを埋め込んだことを確認し、オプションで Flash URL リダイレクトのエラー メッセージをカスタマイズします。

ユーザーがリモート デスクトップで Web ページを表示すると、viewmp.js JavaScript コマンドがリモート デスクトップで Flash URL リダイレクト機能を起動し、デスクトップからホスティングしているクライアント デバイスに SWF ファイルをリダイレクトします。

Flash URL リダイレクト用にクライアント デバイスを設定

Flash URL リダイレクト機能は、リモート デスクトップからクライアント デバイスに SWF ファイルをリダイレクトします。これらのデバイスでマルチキャストまたはユニキャストのストリームから Flash ビデオの再生を許可するには、適切な Adobe Flash Player がクライアント デバイ스에インストールされていることを確認する必要があります。クライアントは、メディア ソースに対する IP 接続性を持つ必要もあります。

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

手順

- ◆ クライアント デバイスに Adobe Flash Player をインストールします。

オペレーティング システム	操作
Windows	Internet Explorer 用に Adobe Flash Player 10.1 以降をインストールします。
Linux	<p>a libexpat.so.0 ファイルをインストールするか、このファイルが既にインストールされていることを確認します。</p> <p>ファイルが /usr/lib または /usr/local/lib ディレクトリにインストールされていることを確認します。</p> <p>b libflashplayer.so ファイルをインストールするか、このファイルが既にインストールされていることを確認します。</p> <p>このファイルが Linux オペレーティング システムの適切な Flash プラグイン ディレクトリにインストールされていることを確認します。</p> <p>c wget プログラムをインストールするか、プログラム ファイルが既にインストールされていることを確認します。</p>

Flash URL リダイレクトを無効または有効

Flash URL リダイレクトは、VDM_FLASH_URL_REDIRECTION=1 プロパティを指定して Horizon Agent のサイレント インストールを実行すると有効になります。選択されたリモート デスクトップの Windows レジストリ キーの値を設定することで、それらの仮想マシンでの Flash URL リダイレクト機能を無効にするか、または再度有効にすることができます。

手順

- 1 仮想マシンで Windows レジストリ エディタを起動します。

2 Flash URL リダイレクトを制御する Windows レジストリ キーに移動します。

オプション	説明
Windows 7 64 ビット	HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware, Inc.\VMware ViewMP\enabled = <i>value</i>
Windows 7 32 ビット	HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware ViewMP\enabled = <i>value</i>

3 Flash URL リダイレクトを無効化または有効化する値を設定します。

オプション	値
無効	0
有効	1

デフォルトでは、値は 1 に設定されます。

Flash リダイレクトの構成

Flash リダイレクト機能を使用すると、Flash コンテンツはクライアント システムに送信され、Flash Player ActiveX バージョンを使用して Flash コンテナ ウィンドウで再生されます。

注: Horizon 7.0 では、Flash リダイレクトは技術プレビュー機能です。Horizon 7.0.1 では、完全にサポートされます。

この機能の名前は Flash URL リダイレクトと呼ばれる機能と似ていますが、次の表に示す大きな違いがあります。

表 14-1. Flash リダイレクト機能と Flash URL リダイレクトの比較

差異項目	Flash リダイレクト	Flash URL リダイレクト
サポート レベル	テクニカル サポートがない Horizon 7.0 の技術プレビュー機能です。Horizon 7.0.1 では、完全にサポートされます。	完全にサポートされます
この機能をサポートする Horizon Client のタイプ	Windows クライアントのみ	Windows クライアントおよび Linux クライアント
表示プロトコル	Horizon 7.0 では、PCoIP のみ。Horizon 7.0.1 では、PCoIP および VMware Blast。	PCoIP
ブラウザ	エージェント（リモート デスクトップ）の Internet Explorer 9、10、または 11	Horizon Client および Horizon Agent で現在サポートされるすべてのブラウザ
構成メカニズム	エージェント側の GPO を使用して、Flash リダイレクトの使用/未使用に関わらず、Web サイトのホワイト リストまたはブラック リストを指定します	Web ページのソース コードを変更して、必要な JavaScript を埋め込みます

機能制限

Flash リダイレクト機能には次の制限があります。

- Flash Player ウィンドウ内の URL リンクをクリックすると、リモート デスクトップ（エージェント側）ではなくクライアントのブラウザが開きます。
- 一部のブラウザ バージョンでは、Flash リダイレクトと連携しない Web サイトもあります。たとえば、Internet Explorer 11 を使用すると vimeo.com Web サイトは機能しません。
- Horizon 7.0 では、Flash と Java のスクリプトは期待どおりに動作しない可能性があります。
- Flash コンテンツの再生時に Horizon Client ウィンドウがフリーズする可能性があります。ただし、Windows レジストリ キーを設定してこの問題を回避できます。

32 ビット クライアントでは HKLM\Software\VMware, Inc.\VMware VDM\Client\EnableD3DRenderer 値を「FALSE」に設定し、64 ビット クライアントでは HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\EnableD3DRenderer を「FALSE」に設定します。

- YouTube Web サイトでは、再生問題を回避するために、外部インターフェイスはデフォルトで無効になります。したがって、[自動再生]、[次へ] ボタンと [前へ] ボタン、および [シアター モード] の機能は動作しません。YouTube Web サイトの最新アップデートで Flash メディアを有効にするには、[互換表示設定] から youtube.com を削除して、&nohtml5=1 をビデオの URL に手動で追加します。たとえば、https://www.youtube.com/watch?v=NwmRD25HWGE&nohtml5=1 のように追加します。
- リモート デスクトップで appMode=1 を Windows レジストリ キーとして設定していない限り、YouTube サイトでお勧めのビデオをクリックできません。
- クライアントにオーディオ デバイスがないと、YouTube フラッシュ メディアを再生するとき、エラーが発生します。
- Flash リダイレクトは、redbox.com では動作しません。
- [Flash] コンテキスト メニュー（右クリックで有効化）は無効です。
- Horizon Client バージョン 4.1 を、PCoIP で Horizon 7.0 デスクトップに接続すると、Flash リダイレクトは失敗します。Flash コンテンツは、デスクトップのネイティブ プレイヤーで再生されるか、もしくは白色の画面となります。

Flash リダイレクトの要件

Flash リダイレクトでは、Internet Explorer 9、10、または 11 の使用時に、Flash コンテンツがクライアント システムに送信されます。クライアント システムはメディア コンテンツを再生し、ESXi ホストのロードを低減します。

リモート デスクトップ

- Horizon Agent 7.0 以降が、Flash リダイレクト オプションを選択して、単一ユーザー (VDI) リモート デスクトップにインストールされている必要があります。Flash リダイレクト オプションはデフォルトで選択されていません。

[Horizon Agent のカスタム セットアップ オプション](#) を参照してください。

- 適切なグループ ポリシー設定が構成されている必要があります。[Flash リダイレクトのインストールと構成](#)を参照してください。

- Flash リダイレクトは、Windows 7、Windows 8、Windows 8.1、および Windows 10 の単一ユーザー リモート デスクトップでサポートされています。
- Internet Explorer 9、10、または 11 が、対応する Flash ActiveX プラグインとともにインストールされている必要があります。
- インストールした後に、VMware View FlashMMR Server アドオンを Internet Explorer で有効にする必要があります。

Horizon Client コンピュータまたはクライアント アクセス デバイス

- Horizon Client 4.0 以降がインストールされている必要があります Flash リダイレクト オプションはデフォルトで有効です。
『Windows 版 VMware Horizon Client の使用』の Horizon Client のインストールに関するトピックを参照してください。
- Flash リダイレクトは、Windows 7、Windows 8、Windows 8.1、および Windows 10 でサポートされています。
- Flash ActiveX プラグインがインストールされ、有効になっている必要があります

リモート セッションの表示 VMware Blast、PCoIP プロトコル

Flash リダイレクトのインストールと構成

リモート デスクトップからローカル クライアント システムの Flash Player ウィンドウに Flash コンテンツをリダイレクトするには、Flash リダイレクト機能と Internet Explorer をリモート デスクトップとクライアント システムにインストールし、この機能を使用する Web サイトを指定する必要があります。

この機能をクライアント システムにインストールするには、Horizon Client 4.0 以降のインストーラを使用する必要があります。この機能をリモート デスクトップにインストールするには、Horizon Agent 7.0 以降のインストーラを使用して、適切なインストール オプション（デフォルトでは選択されていない）を選択する必要があります。この機能を有効化し、この機能を使用する Web サイトを指定するには、グループ ポリシーを使用します。

注: または、リモート デスクトップの Windows レジストリ設定を使用して、Flash リダイレクトで使用する Web サイトのホワイト リストを構成することもできます。[Windows レジストリ設定を使用した Flash リダイレクトの構成](#)を参照してください。

前提条件

- Active Directory サーバをホストするマシンに管理者ドメイン ユーザーとしてログインできることを確認します。
- MMC およびグループ ポリシー オブジェクト エディタ スナップインが Active Directory サーバで使用できることを確認します。
- Horizon Agent の構成 ADM テンプレート（vdm_agent.adm ファイル）がリモート デスクトップの OU に追加されていることを確認します。[GPO への View ADM テンプレートの追加](#)を参照してください。

- Flash コンテンツをリダイレクトできる Web サイト、またはリダイレクトできない Web サイトのリストをコンパイルします。ホワイト リストをコンパイルして、必ずリストで指定されている URL だけが Flash コンテンツをリダイレクトできるようにします。ブラック リストをコンパイルして、必ずリストで指定されている URL が Flash コンテンツをリダイレクトできないようにします。
- Flash ActiveX がインストールされており適切に動作することを確認します。インストールを確認するには、Internet Explorer を実行して <https://helpx.adobe.com/flash-player.html> に移動します。

手順

- 1 Windows 7、Windows 8、Windows 8.1、または Windows 10 クライアント システムで、必要なバージョンの Horizon Client および ActiveX バージョンの Flash Player をインストールします。
 - Horizon Client 4.0 以降をインストールします。『VMware Horizon Client for Windows の使用』ドキュメントの Horizon Client のインストールに関するトピックを参照してください。
 - 必要に応じて、(NPAPI バージョンではなく) ActiveX バージョンの Flash Player をインストールします。Internet Explorer 10 および 11 の場合、Flash Player はデフォルトでインストールされています。Internet Explorer 9 の場合、必要に応じて <https://get.adobe.com/flashplayer/> にアクセスし、Flash Player をダウンロードしてインストールします。
- 2 Windows 7、Windows 8、Windows 8.1、または Windows 10 リモート デスクトップで、必要なバージョンの Horizon Agent および Internet Explorer (Flash Player あり) をインストールします。
 - Horizon Agent 7.0 以降をインストールし、Flash リダイレクト (試験的) のオプションを選択します。デフォルトではこのオプションが選択されていません。
 - Internet Explorer 9、10、または 11 をインストールします。
 - 必要に応じて、(NPAPI バージョンではなく) ActiveX バージョンの Flash Player をインストールします。Internet Explorer 10 および 11 の場合、Flash Player はデフォルトでインストールされています。Internet Explorer 9 の場合、必要に応じて <https://get.adobe.com/flashplayer/> にアクセスし、Flash Player をダウンロードしてインストールします。
- 3 リモート デスクトップで、Internet Explorer のメニュー バーから [ツール] - [アドオンの管理] を選択し、[VMware View FlashMMR サーバ] が表示されていて有効になっていることを確認します。

- 4 Active Directory サーバで、グループ ポリシー管理エディタを開き、[コンピュータの構成] で Flash リダイレクト ポリシー設定を編集します。

この設定は、[コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [従来の管理用テンプレート] - [VMware Horizon Agent の構成] - [VMware FlashMMR] フォルダ内にあります。

設定	説明
Flash マルチメディア リダイレクトの有効化	リモート デスクトップ (エージェント側) で Flash リダイレクト (FlashMMR) を有効にするかどうかを指定します。この機能が有効になっている場合、Flash マルチメディア データが指定の URL から TCP チャンネルを介してクライアントに転送され、クライアント システムでローカル Flash Player が起動します。この機能により、エージェント側の CPU およびネットワーク帯域幅の負荷が大幅に減少します。
長方形の最小サイズ	Flash コンテンツが再生される長方形の幅と高さの最小値をピクセル単位で指定します。たとえば、 400,300 と指定すると、幅が 400 ピクセル、高さが 300 ピクセルになります。Flash コンテンツがこのポリシーで指定した値以上になっている場合にのみ Flash リダイレクトが使用されます。GPO が構成されていない場合、デフォルト値の 320,200 が使用されます。

- 5 グループ ポリシー管理エディタの [ユーザーの構成] で Flash リダイレクト ポリシー設定を編集します。

この設定は、[ユーザーの構成] - [ポリシー] - [管理用テンプレート] - [従来の管理用テンプレート] - [VMware Horizon Agent の構成] - [VMware FlashMMR] フォルダ内にあります。

- a Flash リダイレクトで使用するホスト URL のリストの定義する [FlashMMR URL リストの使用方法的定義] の設定を開いて、[有効] ラジオ ボタンを選択します。
- b URL の使用方法的ドロップ ダウン リストで、ホワイト リストまたはブラック リストを有効にします。
 - ホワイト リストを有効にするには、[ホワイト リストを有効にする] を選択します。
 - ブラック リストを有効にするには、[ブラック リストを有効にする] を選択します。
 デフォルトでは、ホワイト リストが有効になります。
- c [FlashMMR を有効/無効にするホスト URL リスト] 設定を開いて、Flash リダイレクトを使用するまたは使用しないホスト URL リストを追加し、[有効] ラジオ ボタンを選択します。

d [表示] ボタンをクリックします。

e 前提条件としてコンパイルした完全な URL を [名前] 列に入力し、[値] 列を空白のままにします。

必ず `http://` または `https://` を含めてください。正規表現を使用できます。たとえば、

`https://*.google.com` や **`http://www.cnn.com`** を指定できます。

(Horizon 7.0) [値] 列は空白のままにします。

(Horizon 7.0.1) [値] 列では、**`requireIECompatibility=true`**、**`appMode=0`**、または両方（コンマを使用して 2 つの文字列を区切る）を自由に指定できます。

Web サイトは、デフォルトで HTML5 をサポートします。また、Flash リダイレクトはこれらの Web サイトでは動作しません。これらのサイトを動作させるには、**`requireIECompatibility=true`** を設定する必要があります。このパラメータは、YouTube Web サイトでは不要です。

Flash リダイレクトを実行すると、デフォルトで外部インターフェイスのサポートは有効になります。これによりパフォーマンスが低下します。**`appMode=0`** を設定すると、パフォーマンスが向上し、ユーザーの操作性が向上する場合があります。

6 エージェント マシンで、コマンド プロンプトを開き、次のディレクトリに変更します。

```
%Program Files%\Common Files\VMware\Remote Experience
```

7 次のコマンドを実行して、Internet Explorer にホワイト リストまたはブラック リストを追加します。

```
cscript mergeflashmmrwhitelist.vbs
```

8 Internet Explorer を再起動します。

パラメータ **`requireIECompatibility=true`** が設定されたサイトは、Internet Explorer の [互換表示] に追加されます。これを確認するには、メニュー バーから [ツール] - [互換表示設定] を選択します。

Horizon 7.0 でのみ、そのサイトも Internet Explorer の信頼済みサイトのリストに追加されます。信頼済みサイトを確認するには、Internet Explorer のメニュー バーから [ツール] - [インターネット オプション] を選択し、[セキュリティ] タブで [サイト] ボタンをクリックします。

Windows レジストリ設定を使用した Flash リダイレクトの構成

Active Directory サーバに対する管理者権限がないドメイン ユーザーは、代わりにリモート デスクトップで Windows レジストリ キーに適切な値を設定して、Flash リダイレクトを構成できます。

この手順は、Flash リダイレクトの構成に GPO 設定を使用する代わりに使用できます。

前提条件

- Web サイトのホワイト リストをコンパイルして、リストで指定されている URL だけが Flash コンテンツをリダイレクトできるようにします。ブラック リストの Web サイトをコンパイルすることはできませんが、Windows レジストリ設定を使用してブラック リストを有効にはできません。ブラック リストによって、リストで指定されている URL が Flash コンテンツをリダイレクトできなくなります。ブラック リストを有効にするには、Flash リダイレクトの GPO 設定を使用する必要があります。

- リモート デスクトップに Flash Player および Internet Explorer 9、10、または 11 とともに Horizon Agent 7.0 以降がインストールされていることを確認します。[Flash リダイレクトのインストールと構成](#)を参照してください。
- Horizon Client 4.0 以降と Flash Player ActiveX バージョンを使用していることを確認します。

手順

- 1 Horizon Client を使用してリモート デスクトップ (エージェント マシン) にアクセスします。
- 2 エージェント マシンで Windows レジストリ エディタ (regedit.exe) を開き、次のフォルダに移動して [FlashRedirection] を **1** に設定します。

```
HKLM\Software\VMware, Inc.\VMware FlashMMR
```

注: この設定により Flash リダイレクト機能が有効になりますが、HKLM\Software\Policies\VMware, Inc.\VMware FlashMMR でこの設定が無効 (0) になっている場合はドメイン全体で Flash リダイレクトが無効になるため、ドメイン管理者が機能を有効にする必要があります。

- 3 次のフォルダに移動します。

```
HKEY_CURRENT_USER\SOFTWARE\VMware, Inc.\VMware FlashMMR
```

このフォルダが存在しない場合は作成します。

- 4 VMware FlashMMR フォルダで、[UrlWhiteList] というサブキーを作成します。
- 5 [UrlWhiteList] キーを右クリックして [新規] - [文字列値] を選択し、[名前] に Flash リダイレクトを使用する Web サイトの URL を入力します。

正規表現を使用できます。たとえば、**https://*.google.com** と指定します。[データ] の値は必ず空のままにしてください。

- 6 (オプション) (Horizon 7.0.1 および 7.0.2 のみ) 新しいレジストリ値のデータフィールドで、**requireIECompatibility=true**、**appMode=0**、または両方 (コンマを使用して 2 つの文字列を区切る) を追加します。

Web サイトは、デフォルトで HTML5 をサポートします。また、Flash リダイレクトはこれらの Web サイトでは動作しません。これらのサイトを動作させるには、**requireIECompatibility=true** を設定する必要があります。このパラメータは、YouTube Web サイトでは不要です。

Flash リダイレクトを実行すると、デフォルトで外部インターフェイスのサポートは有効になります。これによりパフォーマンスが低下します。Horizon 7.0.1 以降の特定の状況下では、**appMode=0** に設定するとパフォーマンスが向上し、**appMode=1** に設定すると、ユーザーの操作性が向上する場合があります。

- 7 前の手順を繰り返して他の URL を追加し、完了したらレジストリ エディタを閉じます。
- 8 エージェント マシンで、コマンド プロンプトを開き、次のディレクトリに変更します。

```
%Program Files%\Common Files\VMware\Remote Experience
```

9 次のコマンドを実行して、Internet Explorer にホワイト リストを追加します。

```
cscript mergeflashmmrwhitelist.vbs
```

10 Internet Explorer を再起動します。

パラメータ **requireIECompatibility=true** が設定されたサイトは、Internet Explorer の [互換表示] に追加されます。これを確認するには、メニュー バーから [ツール] - [互換表示設定] を選択します。

Horizon 7.0 でのみ、そのサイトも Internet Explorer の信頼済みサイトのリストに追加されます。信頼済みサイトを確認するには、Internet Explorer のメニュー バーから [ツール] - [インターネット オプション] を選択し、[セキュリティ] タブで [サイト] ボタンをクリックします。

URL コンテンツ リダイレクトの構成

URL コンテンツ リダイレクトを使用すると、特定の URL を構成して、クライアントで常に関くか、あるいはリモート デスクトップまたはアプリケーションで開くようにすることができます。ユーザーが Internet Explorer のアドレス バーに入力する URL と、ユーザーがクリックできるアプリケーション内のリンクをリダイレクトできます。HTTP、mailto、および callto などの任意の数のプロトコルをリダイレクトするように構成できます。

URL コンテンツ リダイレクト機能は、次の方向の URL リダイレクトをサポートします。

クライアントからリモート デスクトップまたはアプリケーションへ (クライアントからエージェントへのリダイレクト)	セットアップしたルールに基づき、Horizon Client は、リモート デスクトップまたはリモート アプリケーションのどちらかを開いて、URL を処理します。デスクトップが開くと、URL に対応するプロトコルのデフォルト アプリケーションが URL を処理します。
---	--

クライアントからエージェントへのリダイレクトを使用するには、Horizon Client と Horizon Agent の両方で URL コンテンツ リダイレクト機能を有効にする必要があります。

リモート デスクトップまたはアプリケーションからクライアントへ (エージェントからクライアントへのリダイレクト)	Horizon Agent から URL が Horizon Client に送信され、URL で指定されたプロトコルに対応するデフォルト アプリケーションが開きます。 エージェントからクライアントへのリダイレクトを使用するには、Horizon Agent で URL コンテンツ リダイレクト機能を有効にする必要があります。Horizon Client では、URL コンテンツ リダイレクト機能を有効にする必要はありません。
---	---

一部の URL をリモート デスクトップまたはアプリケーションからクライアントにリダイレクトし、それ以外の URL をクライアントからリモート デスクトップまたはアプリケーションにリダイレクトできます。グループ ポリシー設定を構成して、Horizon Agent または Horizon Client での URL のリダイレクト方法をプロトコルごとに示します。

Horizon Client がリモート デスクトップにインストールされている環境、つまり Horizon Agent と Horizon Client の両方が同じマシンにインストールされている環境を作成できます。たとえば、ユーザーがシン クライアント デバイスにログインしていて、リモート デスクトップに接続しているとします。デスクトップから、ユーザーが Horizon Client を実行してリモート アプリケーションにアクセスします。このデスクトップ マシンで、ユーザーは

Horizon Agent を URL コンテンツ リダイレクト機能ありでインストールするか、Horizon Client をこの機能ありでインストールすることはできますが、両方をインストールすることはできません。このマシンでは、クライアントからエージェントへのリダイレクトまたはエージェントからクライアントへのリダイレクトのいずれかを設定できますが、両方を設定することはできません。

URL コンテンツ リダイレクトの要件と制限事項

URL コンテンツ リダイレクト機能には、いくつかの要件と制限事項があります。

URL コンテンツ リダイレクト機能の要件

URL コンテンツ リダイレクト機能には、次の要件があります。

- Horizon Client for Windows 4.0 以降。
- Horizon Client for Mac 4.2 および 4.3。URL コンテンツ リダイレクトは、エージェントからクライアントへのリダイレクトのみをサポートする Tech Preview 機能です。
- URL を入力またはクリックしたときのその URL のリダイレクトをサポートしているブラウザは、Internet Explorer 9、10、および 11 です。
- リモート セッションの表示プロトコルが VMware Blast または PCoIP である必要があります。

URL コンテンツ リダイレクト機能の制限事項

URL コンテンツ リダイレクト機能の動作によって、次のような予期しない結果が生じる場合があります。

- URL から開かれるページがロケールに基づく各国対応ページの場合、開くロケール ページは、リンクのソースによって決定されます。たとえば、リモート デスクトップ（エージェント ソース）が日本のデータセンターに存在し、ユーザーのコンピュータが米国に存在する場合、URL がエージェントからクライアント マシンにリダイレクトされると、米国のクライアントで開くページは日本語のページになります。
- ユーザーが Web ページからお気に入りを作成すると、リダイレクト後のお気に入りが作成されます。たとえば、ユーザーがクライアント マシンでリンクをクリックし、URL がリモート デスクトップ（エージェント）にリダイレクトされたとします。ユーザーがそのページのお気に入りを作成すると、エージェントにお気に入りが作成されます。ユーザーが次にブラウザをクライアント マシンで開いたときに、ユーザーは、クライアント マシンにお気に入りがあるものと考えますが、実際には、エージェント（リモート デスクトップ）にお気に入りが保存されています。
- ユーザーがダウンロードしたファイルは、URL を開くために使用されたブラウザがあるマシンにダウンロードされます。たとえば、ユーザーがクライアント マシンでリンクをクリックすると、その URL はリモート デスクトップにリダイレクトされます。そのリンクがファイルをダウンロードするためのリンクであったり、ユーザーがファイルをダウンロードするための Web ページ リンクであったりする場合、クライアント マシンではなく、リモート デスクトップにファイルがダウンロードされます。

サポートされない URL コンテンツ リダイレクト機能

URL コンテンツ リダイレクト機能は、次の状況では機能しません。

- `https://goo.gl/abc` などの短縮 URL は、フィルタリング規則に基づいてリダイレクトできますが、フィルタリングメカニズムでは、元の短縮されていない URL が参照されません。たとえば、`acme.com` が含まれた URL をリダイレクトする規則がある場合、元の URL が `http://www.acme.com/some-really-long-path` で元の URL の短縮 URL が `https://goo.gl/xyz` だとすると、元の URL はリダイレクトされますが、短縮 URL はリダイレクトされません。

回避策：URL の短縮に最も頻繁に使用されている Web サイトから URL をブロックまたはリダイレクトするルールを作成します。

- 埋め込み HTML ページでは、URL リダイレクトはバイパスされます。たとえば、URL リダイレクト ルールに一致しない URL にアクセスしたとします。ページに埋め込み HTML ページが含まれていて (iFrame またはインラインフレーム)、その URL がリダイレクト ルールに一致しないと、URL ルールは機能しません。ルールは、最上位の URL でのみ動作します。
- URL コンテンツ リダイレクトは、Internet Explorer プラグインが無効な状況、たとえば、ユーザーが Internet Explorer で InPrivate ブラウズに切り替えている状況では機能しません。(プライベート ブラウズを使用すると、Web ページや Web ページからダウンロードされたファイルは、コンピュータで閲覧やダウンロード履歴に記録されません)。URL リダイレクト機能では特定の Internet Explorer プラグインを有効にする必要がありますが、プライベート ブラウズによってこれらのプラグインが無効になるために、この制限事項が発生します。

回避策：GPO 設定を使用して、ユーザーがプラグインを無効にできないようにします。これに該当する設定は、[ユーザーによるアドオンの有効化および無効化を許可しない] と [新しくインストールされたアドオンを自動的に有効にする] です。グループ ポリシー管理エディタでは、これらの設定は、[コンピュータの構成] - [管理用テンプレート] - [Windows コンポーネント] - [Internet Explorer]の下にあります。

Internet Explorer の場合の回避策：GPO 設定を使用して、InPrivate モードを無効にします。この設定は、[InPrivate ブラウズを無効にする] という名前です。グループ ポリシー管理エディタでは、これらの設定は、[コンピュータの構成] - [管理用テンプレート] - [Windows コンポーネント] - [Internet Explorer] - [プライバシー]の下にあります。

これら 2 つの回避策は、推奨されるベスト プラクティスであり、プライベート ブラウズ以外の状況によって発生する可能性があるリダイレクトの問題を防止できます。

- リンクで指定されているプロトコルのデフォルト ハンドラが Windows 10 のユニバーサル アプリケーションである場合、URL リダイレクトが動作しません。ユニバーサル Windows プラットフォームに組み込まれ、PC、タブレット、およびスマートフォンにダウンロードできるユニバーサル アプリケーションとしては、Microsoft Edge ブラウザ、メール、マップ、フォト、Groove ミュージックなどがあります。したがって、デフォルト ハンドラがこれらのいずれかのアプリケーションとなっているリンクをクリックすると、URL はリダイレクトされません。たとえば、ユーザーがアプリケーションの電子メール リンクをクリックし、デフォルトの電子メール アプリケーションがユニバーサル アプリケーションのメールであった場合、リンクで指定された URL はリダイレクトされません。

回避策：別のアプリケーションを、リダイレクトする URL のプロトコルに対するデフォルト ハンドラにします。たとえば、Edge がデフォルト ブラウザの場合は、Internet Explorer をデフォルト ブラウザにします。

- セキュア ブートが有効であるマシンでは、URL コンテンツ リダイレクト機能が無効のままになります。これらのマシンから URL をリダイレクトすることはできません。ただし、これらのマシンに URL をリダイレクトすることはできます。

URL コンテンツ リダイレクト機能ありでの Horizon Client のインストール

クライアントからリモート デスクトップやアプリケーションへの URL コンテンツ リダイレクト（クライアントからエージェントへのリダイレクト）をサポートするには、Horizon Client を URL コンテンツ リダイレクト機能ありでインストールする必要があります。

Horizon Client for Windows では、コマンドライン オプションで Horizon Client for Windows のインストーラを使用する必要があります。インストーラ ファイルをダブルクリックする代わりにコマンド プロンプト ウィンドウで次のコマンドを実行して、インストールを開始します。例：

```
VMware-Horizon-Client-x86-y.y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1
```

指示に従ってインストールを完了した後に、`vmware-url-protocol-launch-helper.exe` ファイルと `vmware-url-filtering-plugin.dll` ファイルがディレクトリ `%PROGRAMFILES%\VMware\VMware Horizon View Client\` にインストールされているかをチェックすることで、この機能がインストールされていることを確認できます。Internet Explorer のアドオンの VMware Horizon View URL Filtering Plugin がインストールされていることも確認します。

注： Horizon Client for Mac は、クライアントからエージェントへのリダイレクトはサポートしません。

URL コンテンツ リダイレクト機能ありでの Horizon Agent のインストール

リモート デスクトップまたはアプリケーションからクライアントへの URL コンテンツ リダイレクト（エージェントからクライアントへのリダイレクト）をサポートするには、Horizon Agent を URL コンテンツ リダイレクト機能ありでインストールする必要があります。

インストーラ ファイルをダブルクリックする代わりにコマンド プロンプト ウィンドウで次のコマンドを実行して、インストールを開始します。

```
VMware-viewagent-x86_64-y.y.y-xxxxxx.exe /v URL_FILTERING_ENABLED=1
```

指示に従ってインストールを完了した後に、`vmware-url-protocol-launch-helper.exe` ファイルと `vmware-url-filtering-plugin.dll` ファイルがディレクトリ `%PROGRAMFILES%\VMware\VMware View \Agent\bin\UrlRedirection\` にインストールされているかをチェックすることで、この機能がインストールされていることを確認できます。Internet Explorer のアドオンの VMware Horizon View URL Filtering Plugin が有効になっていることも確認します。

Active Directory への URL コンテンツ リダイレクト ADM テンプレートの追加

URL コンテンツ リダイレクト ADM ファイル、`urlRedirection-enUS.adm` のポリシー設定を Active Directory のグループ ポリシー オブジェクト (GPO) に追加し、グループ ポリシー オブジェクト エディタで設定を構成できます。

前提条件

- リモート デスクトップやアプリケーションでクリックされるリンクにポリシーを設定する場合には、Horizon Agent のインストールに URL コンテンツ リダイレクト機能が含まれていることを確認します。[URL コンテンツ リダイレクトの構成](#)を参照してください。
- クライアント ブラウザやアプリケーションでクリックされるリンクにポリシーを設定する場合には、Horizon Client のインストールに URL コンテンツ リダイレクト機能が含まれていることを確認します。[URL コンテンツ リダイレクトの構成](#)を参照してください。
- URL コンテンツ リダイレクトのグループ ポリシー設定用に Active Directory GPO が作成されていることを確認します。リモート デスクトップやアプリケーションからクリックされるリンクに関するルールについては、デスクトップおよび RDS ホストを含む組織単位 (OU) に GPO がリンクされる必要があります。クライアント システム内でクリックされるリンクについては、クライアント コンピュータを含む組織単位 (OU) に GPO がリンクされる必要があります。

[Active Directory グループ ポリシーの例](#)を参照してください。

- MMC およびグループ ポリシー オブジェクト エディタ スナップインが Active Directory サーバで使用できることを確認します。
- URL コンテンツ リダイレクト グループ ポリシー設定について理解しておきます。[VMware Horizon URL コンテンツ リダイレクト テンプレートの設定](#)を参照してください。

手順

- 1 View GPO Bundle .zip ファイルを <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 GPO Bundle が含まれます。

ファイル名は VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip で、x.x.x はバージョン、yyyyyyy はビルド番号を表します。View のグループ ポリシー設定用の ADM ファイルと ADMX ファイルはすべて、このファイルで提供されています。

- 2 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip ファイルを解凍して、URL コンテンツ リダイレクト ADM ファイル urlRedirection-enUS.adm を Active Directory サーバにコピーします。
- 3 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 GPO を編集します。
- 4 グループ ポリシー オブジェクト エディタで、[コンピュータの構成] - [ポリシー] - [管理テンプレート] フォルダを右クリックして、[テンプレートの追加と削除] を選択します。
- 5 [追加] をクリックして urlRedirection-enUS.adm ファイルを参照し、[開く] をクリックします。
- 6 [閉じる] をクリックして ADM ファイルのポリシー設定を GPO に追加します。

この設定は、[コンピュータの構成] - [ポリシー] - [管理テンプレート] - [従来の管理テンプレート] - [VMware Horizon URL リダイレクト] フォルダ内にあります。

- 7 URL コンテンツ リダイレクト グループ ポリシー設定を構成します。

グループ ポリシーは、クライアント コンピュータまたは OU に含まれる RDS ホストのリモート デスクトップに対して構成されます。

VMware Horizon URL コンテンツ リダイレクト テンプレートの設定

Horizon URL コンテンツ リダイレクト ADM テンプレート ファイル (`urlRedirection-enUS.adm`) には、リモート デスクトップまたはアプリケーションで URL リンクをクライアント側またはエージェント側のどちらで開くかどうかを制御するポリシー設定が含まれます。たとえば、セキュリティを強化するために管理者がポリシーを設定し、会社のネットワーク内で働くすべての従業員に対して、社外のネットワークにアクセスするすべての URL リンクをリモート デスクトップまたはアプリケーションで開くようにできます。

この ADM ファイルは、`VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` という .zip バンドル ファイル内にあり、<https://my.vmware.com/web/vmware/downloads> 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 バンドル ファイルが含まれます。

URL コンテンツ リダイレクトは、ユーザーがブラウザや Microsoft Word の文書や電子メールなどのアプリケーションにある URL リンクをクリックしたときや、Internet Explorer 9、10、または 11 ブラウザで URL をクリックまたは入力したときなどに実行されるようにできます。URL リンクのリンク先には、Web ページ、電話番号、電子メールアドレスなどを設定可能です。

URL コンテンツ リダイレクト ルールの構文

クライアントまたはエージェントで開く URL の指定では、正規表現を使用できます。複数のエントリはセミコロンで区切ってください。エントリ間にスペースは使用できません。

例を示します。

エントリ	説明
<code>.*</code>	(ドットとアスタリスク) すべての URL をリダイレクトするよう指定します。この設定を [agentRules] オプションに使用すると、すべての URL がエージェント側にリダイレクトされるため、URL がリモート デスクトップまたはアプリケーションで開きます。この設定を [clientRules] オプションに使用すると、指定した URL がクライアントにリダイレクトされます。
<code>.*.acme.com;.*.example.com</code>	<code>.acme.com</code> または <code>example.com</code> というテキストが含まれるすべての URL をリダイレクトするよう指定します。
[スペースまたは空白]	どの URL もリダイレクトしないようにするには、スペースを使用するか、設定を空白のままにします。たとえば、[clientRules] を空白のままにすると、どの URL もクライアントにリダイレクトしないよう指定することになります。

[agentRules] の場合は、[brokerHostname] オプションも使用して、接続サーバの IP アドレスまたは完全修飾ドメイン名を指定する必要があり、さらに、[remoteItem] オプションを使用して、デスクトップまたはアプリケーション プールの View Administrator に表示される名前を指定する必要があります。

エージェントからクライアントへのリダイレクト

特定の URL をクライアントにリダイレクトするようには、このテンプレートをリモート デスクトップまたはアプリケーション プールの GPO に追加します。

たとえば、エージェントからエージェントへのリダイレクトは、リソースの節約やセキュリティ レイヤの追加に使用されることがあります。たとえば、従業員がリモート デスクトップやアプリケーションでの作業中に動画を視聴した場合であれば、それらの URL をクライアント マシンにリダイレクトすることで、データセンターに負荷がかかることはなくなります。あるいは、社内ネットワークの外で働く従業員のセキュリティを強化する目的で、社内ネットワークの外部にアクセスするすべての URL を従業員自身のクライアント マシンで開くようにしたいとします。

その場合は、たとえば、ルールを構成して、会社に関係のないコンテンツや社内ネットワークへのアクセスではない URL はすべて、クライアント マシンにリダイレクトして開くようにします。このような状況では、次の設定を正規表現を含めて使用します。

■ [agentRules] の場合： `.*.mycompany.com`

このルールは、**mycompany.com** というテキストが含まれるすべての URL がエージェントで開くことを意味します。

■ [clientRules] の場合： `.*`

このルールは、すべての URL をクライアントでデフォルトのクライアント ブラウザを使用して開くことを意味します。

この機能は、次のプロセスを使用してルールを適用します。

- 1 ユーザーがリモート アプリケーションまたはデスクトップでリンクをクリックすると、クライアント ルールが最初にチェックされます。
- 2 URL 内のパターンがクライアント ルールと一致すると、エージェント ルールが次にチェックされます。
- 3 エージェント ルールとクライアント ルールが競合する場合、リンクはローカルで開きます。つまり、この場合は、エージェント マシンで開きます。
- 4 競合がなければ、URL はクライアントにリダイレクトされます。

上記の例では、**mycompany.com** が含まれる URL はすべての URL のサブセットであるため、ルール間で競合が存在します。この競合によって、**mycompany.com** が含まれる URL はローカルで開きます。リモート デスクトップで URL の **mycompany.com** のリンクをクリックすると、URL はそのリモート デスクトップで開きます。クライアント システムから URL の **mycompany.com** のリンクをクリックすると、URL はクライアントで開きます。

クライアントからエージェントへのリダイレクト

特定の URL をリモート デスクトップまたはアプリケーションにリダイレクトするには、このテンプレートをクライアント コンピュータのグループの GPO に追加します。たとえば、セキュリティ上の目的で、社内ネットワークにアクセスするすべての URL をリモート デスクトップまたはアプリケーションで開くようにしたいとします。このような状況では、[agentRules] を次のように設定します。

```
.*.mycompany.com
```

URL をリモート デスクトップまたはアプリケーションにリダイレクトするには、使用するプールも指定する必要があります。[brokerHostname] オプションを使用して、接続サーバの IP アドレスまたは完全修飾ドメイン名を指定し、さらに、[remoteItem] オプションを使用して、デスクトップまたはアプリケーション プールの View Administrator に表示される名前を指定します。

URL がリモート デスクトップにリダイレクトされた場合、リンクはそのデスクトップのデフォルト ブラウザで開きます。URL がリモート アプリケーションにリダイレクトされた場合、リンクは指定されたアプリケーション プールを使用して開きます。指定されたデスクトップまたはアプリケーション プールを使用する権限をエンド ユーザーが持っている必要があります。

このテンプレートをエージェントとクライアントの両方の GPO に追加できますが、その場合は、両方のルールが競合しないこと、または、競合があっても意図的なものであることを確認してください。

テンプレート設定の詳細

次の表に、Horizon URL コンテンツ リダイレクト ADM テンプレート ファイルのポリシー設定の説明を記載します。このテンプレートには、コンピュータの構成設定のみが含まれます。

表 14-2. Horizon URL コンテンツ リダイレクト テンプレートの設定

設定	プロパティ
IE Policy: Users can't disable URL Redirection plugin	ユーザーが URL コンテンツ リダイレクトを無効にできるかどうかを決定します。 デフォルトでは、この設定は無効になっています。
IE Policy: Automatically activate newly installed plugins	新しくインストールされた Internet Explorer プラグインを自動的に有効にするかどうかを決定します。 デフォルトでは、この設定は無効になっています。
Url Redirection Enabled	この機能をオンにするかどうかを決定します。 デフォルトでは、この設定は有効になっています。この設定を使用すると、コンポーネントがインストールされている場合であっても、機能を無効にできます。
Url Redirection Protocol 'http'	HTTP プロトコルを使用するすべての URL について、リダイレクトする URL を指定します。 たとえば、[agentRules] を .*.mycompany.com に設定すると、"mycompany.com" が含まれるすべての URL がリモート デスクトップまたはリモート アプリケーションにリダイレクトされます。[brokerHostname] を設定することで、使用する接続サーバをさらに指定でき、[remoteItem] を設定することで、使用するデスクトップまたはアプリケーション プールの View Administrator に表示される名前を指定できます。 [clientRules] を .*.mycompany.com に設定すると、"mycompany.com" が含まれるすべての URL が Windows ベースのクライアントにリダイレクトされ、クライアントのデフォルト ブラウザで開きます。 注: ベスト プラクティスとして、HTTP プロトコルと HTTPS プロトコルに同じルールを設定します。この方法では、ユーザーが mycompany.com などの部分的な URL を Internet Explorer に入力し、そのサイトが自動的に HTTP から HTTPS にリダイレクトされると、URL コンテンツ リダイレクト機能が期待どおりに動作します。この場合、HTTP ではなく HTTPS のルールを設定すると、ユーザー入力による部分的な URL ではリダイレクトされません。 デフォルトでは、この設定は無効になっています。

設定	プロパティ
Url Redirection Protocol 'https'	<p>HTTPS プロトコルを使用するすべての URL について、リダイレクトする URL を指定します。</p> <p>このオプションは、Url Redirection Protocol 'http' の場合と同じです。</p> <p>注: ベスト プラクティスとして、HTTPS プロトコルと HTTP プロトコルに同じルールを設定します。</p> <p>デフォルトでは、この設定は無効になっています。</p>
Url Redirection Protocol 'callto'	<p>callto プロトコルを使用するすべての URL について、リダイレクトする URL を指定します。</p> <p>このオプションは、Url Redirection Protocol 'http' の場合と同じです。</p> <p>デフォルトでは、この設定は無効になっています。</p>
Url Redirection Protocol 'email'	<p>email または mailto プロトコルを使用するすべての URL について、リダイレクトする URL を指定します。</p> <p>このオプションは、Url Redirection Protocol 'http' の場合と同じです。</p> <p>デフォルトでは、この設定は無効になっています。</p>
Url Redirection Protocol '[...]'	<p>これは、追加のプロトコルについて変更が可能なテンプレートです。追加のプロトコルを構成する必要がない場合は、ADM テンプレートを Active Directory に追加する前に、このエントリを削除またはコメントアウトできます。</p>

注: クライアントからエージェントへのリダイレクトについて、デフォルトのハンドラがないプロトコルを構成する場合、このプロトコルを指定する URL がリダイレクトされるには、このプロトコルの GPO 設定を構成した後で Horizon Client を一度起動する必要があります。

リアルタイム オーディオ ビデオの構成

リアルタイム オーディオ ビデオを利用すると、View ユーザーは Skype、Webex、Google Hangouts や他のオンライン会議アプリケーションをリモート デスクトップで実行できます。リアルタイム オーディオ ビデオを使用すれば、クライアント システムにローカルで接続される webcam およびオーディオ デバイスは、リモート デスクトップにリダイレクトされます。この機能は、USB リダイレクトを使用して達成できるよりも大幅に低い帯域幅でビデオ およびオーディオ データをデスクトップにリダイレクトします。

リアルタイム オーディオ ビデオは、標準的な会議アプリケーションおよびブラウザベースのビデオ アプリケーションと互換性があり、標準的な webcam、オーディオ USB デバイス、およびアナログ オーディオ入力をサポートします。

この機能は、VMware Virtual Webcam および VMware Virtual Microphone をデスクトップ オペレーティング システムにインストールします。VMware Virtual Web カメラは、ブラウザ ベースのビデオ アプリケーションや他のサードパーティ製の会議ソフトウェアとの高度な互換性を備えたカーネル モードの Web カメラドライバを使用します。

会議アプリケーションやビデオ アプリケーションが起動すると、VMware 仮想デバイスを表示および使用します。これらの VMware 仮想デバイスは、クライアントでローカル接続されたデバイスからのオーディオ ビデオ リダイレクトを処理します。VMware Virtual Web カメラおよび VMware Virtual Microphone は、デスクトップ オペレーティング システムのデバイス マネージャに表示されます。

オーディオおよび Web カメラデバイス用のドライバは、リダイレクトを有効にするために Horizon Client システムにインストールする必要があります。

リアルタイム オーディオ ビデオの構成の選択

リアルタイム オーディオ ビデオと共に Horizon Agent をインストール後、この機能はさらに構成しなくとも View デスクトップで動作します。Web カメラ フレーム レートおよび画像解像度のデフォルト値は、ほとんどの標準デバイスおよびアプリケーションで推奨されます。

グループ ポリシ設定を構成して、これらのデフォルト値を変更して、特定のアプリケーション、Web カメラ、または環境に適応することができます。ポリシーを設定して機能をすべて無効または有効にすることもできます。ADM テンプレート ファイルにより、Active Directory または個々のデスクトップにリアルタイム オーディオ ビデオ グループ ポリシ設定をインストールできます。[リアルタイム オーディオ ビデオ グループ ポリシ設定の構成](#)を参照してください。

クライアント コンピュータに内蔵または接続されている複数の Web カメラおよびオーディオ入力デバイスがある場合、デスクトップにリダイレクトされる優先される Web カメラおよびオーディオ入力デバイスを構成できます。[優先される Web カメラとマイクロフォンを選択](#)を参照してください。

注: 優先されるオーディオ デバイスを選択できますが、他のオーディオ構成オプションは使用できません。

Web カメラ画像およびオーディオ入力がリモート デスクトップにリダイレクトされると、ユーザーはローカル コンピュータの Web カメラおよびオーディオ デバイスにアクセスできません。逆に言えば、これらのデバイスがローカル コンピュータで使用中であれば、リモート デスクトップでそれらにアクセスできません。

サポートされるアプリケーションについては、VMware ナレッジベースの記事『Guidelines for Using Real-Time Audio-Video with 3rd-Party Applications on Horizon View Desktops (リアルタイム オーディオ-ビデオを Horizon View デスクトップのサードパーティ アプリケーションで使用するためのガイドライン)』(<http://kb.vmware.com/kb/2053754>) を参照してください。

リアルタイム オーディオビデオのシステム要件

リアルタイム オーディオビデオは、標準的な webcam、USB オーディオ、およびアナログ オーディオ デバイス、そして Skype、WebEx、および Google Hangouts などの標準的な会議アプリケーションで動作します。リアルタイム オーディオビデオをサポートするには、View の展開が特定のソフトウェアおよびハードウェア要件を満たす必要があります。

View リモート デスクトップ

View Agent 6.0 以降または Horizon Agent 7.0 以降をインストールすることにより、リアルタイム オーディオビデオ機能をインストールします。RDS デスクトップとリモート アプリケーションでこの機能を使用するには、Horizon Agent 7.0.2 以降をインストールする必要があります。[仮想マシンへの Horizon Agent のインストール](#)を参照してください。

Horizon Client ソフトウェア

Horizon Client 2.2 for Windows 以降のリリース

Horizon Client 2.2 for Linux 以降のリリース。Horizon Client for Linux 3.1 以前の場合、この機能はサードパーティ ベンダーによって提供される Horizon Client for Linux のバージョンでのみ使用できます。Horizon Client for Linux 3.2 以降の場合、この機能は VMware から入手できるクライアントのバージョンでも入手できます。

Horizon Client 2.3 for Mac 以降のリリース

Horizon Client 4.0 for iOS 以降のリリース。

Horizon Client 4.0 for Android 以降のリリース。

Horizon Client コンピュータまたはクライアント アクセス デバイス

- Horizon Client for Windows を実行するすべてのオペレーティング システム。
- x86 デバイスで Horizon Client for Linux を実行するすべてのオペレーティング システム。この機能は ARM プロセッサではサポートされません。
- Mac OS X Mountain Lion (10.8) 以降。それよりも前のすべての Mac OS X オペレーティング システムでは無効になっています。
- Horizon Client for iOS を実行するすべてのオペレーティング システム。
- Horizon Client for Android を実行するすべてのオペレーティング システム。
- サポートされているクライアント オペレーティング システムの詳細については、該当するシステムまたはデバイスの VMware Horizon Client の使用を参照してください。
- webcam およびオーディオ デバイス ドライバをインストールする必要があります。webcam およびオーディオ デバイスがクライアント コンピュータで操作可能である必要があります。リアルタイム オーディオビデオをサポートするために、エージェントがインストールされているデスクトップ オペレーティング システムにデバイス ドライバをインストールする必要はありません。

View 用の表示プロトコル

- PCoIP
- VMware Blast (Horizon Agent 7.0 以降が必要)

リアルタイム オーディオビデオは、RDP デスクトップ セッションでサポートされません。

リアルタイム オーディオ ビデオが USB リダイレクトの代わりに使用されることを確認

リアルタイム オーディオ ビデオは、会議アプリケーションでの使用のために、Web カメラおよびオーディオ入力のリダイレクトをサポートします。Horizon Agent でインストールできる USB リダイレクト機能は Web カメラのリダイレクトをサポートしません。オーディオ入力デバイスを USB リダイレクト経由でリダイレクトすると、オーディオ ストリームはリアルタイム オーディオビデオ セッション中にビデオと適切に同期せず、ネットワーク帯域幅の要求を抑制する利点が失われます。Web カメラおよびオーディオ入力デバイスが USB リダイレクトではなくリアルタイム オーディオ ビデオ経由でデスクトップにリダイレクトされるように対策を講じることができます。

デスクトップが USB リダイレクトで構成されている場合、エンド ユーザーは Windows クライアント メニュー バーの [USB デバイスの接続] オプションを選択するか、または Mac クライアントの [デスクトップ > USB] メニューを選択することで、ローカルに接続されている USB デバイスに接続および表示できます。Linux クライアントはデフォルトでオーディオおよびビデオ デバイスの USB リダイレクトをブロックし、エンド ユーザーに USB デバイス オプションを提供しません。

エンド ユーザーが [USB デバイスの接続] または [デスクトップ > USB] リストから USB デバイスを選択すると、そのデバイスはビデオまたはオーディオ会議に使用できなくなります。たとえば、ユーザーが Skype 電話をかけている場合、ビデオ画像が表示されない、またはオーディオ ストリームが低下する可能性があります。エンド ユーザーが会議セッション中にデバイスを選択すると、Web カメラまたはオーディオのリダイレクトは中断されます。

これらのデバイスをエンド ユーザーに表示せず、中断の危険性を防ぐには、USB リダイレクト グループ ポリシー設定を構成し、Web カメラやオーディオ入力デバイスを VMware Horizon Client で表示できないようにします。

特に、Horizon Agent に対し USB リダイレクト フィルタ規則を作成し、**audio-in** および **video** デバイス ファミリー名を無効に指定します。グループ ポリシーの設定と USB リダイレクトに対するフィルタ規則の指定の詳細は、[USB リダイレクトを制御するポリシーの使用](#)を参照してください。

注意: USB デバイス ファミリーを無効にする USB リダイレクトのフィルタ規則を設定しない場合、エンド ユーザーに、VMware Horizon Client メニュー バーの [USB デバイスの接続] または [デスクトップ > USB] リストから Web カメラやオーディオ デバイスを選択できないことを通知してください。

優先される Web カメラとマイクロフォンを選択

クライアント コンピュータに複数の Web カメラおよびマイクロフォンがある場合、リアルタイム オーディオ ビデオがデスクトップにリダイレクトする優先 Web カメラおよびデフォルトのマイクロフォンを構成できます。これらのデバイスは、ローカル クライアント コンピュータに内蔵または接続できます。

Horizon Client for Windows 4.2 以降がインストールされている Windows クライアント コンピュータでは、Horizon Client の [設定] ダイアログ ボックスのリアルタイム オーディオビデオ設定を構成して、優先される Web カメラとマイクロフォンを選択できます。Horizon Client の以前のバージョンでは、優先する Web カメラを選択するにはレジストリ設定を変更し、デフォルトのマイクロフォンを選択するには、Windows オペレーティング システムの [サウンド] コントロールを使用する必要がありました。

Mac クライアント コンピュータでは、Mac のデフォルトのシステムを使用して、優先する Web カメラまたはマイクロフォンを指定できます。

Linux クライアント コンピュータでは、構成ファイルを編集して、優先する Web カメラを指定できます。デフォルトのマイクロフォンを選択するために、クライアント コンピュータの Linux オペレーティング システムで [サウンド] コントロールを構成できます。

リアルタイム オーディオ ビデオは、優先される Web カメラ が使用できればそれをリダイレクトします。使用できない場合、リアルタイム オーディオ ビデオはシステムによって列挙される最初の Web カメラを使用します。

Windows クライアント システムでの優先する Web カメラまたはマイクロフォンの選択

リアルタイム オーディオ ビデオ機能では、クライアント システムに複数の Web カメラやマイクロフォンがある場合、1 台だけがリモート デスクトップやアプリケーションで使用されます。Horizon Client でリアルタイム オーディオ ビデオ機能を構成して、優先的に使用する Web カメラまたはマイクロフォンを指定できます。

優先する Web カメラまたはマイクロフォンが使用できる場合は、リモート デスクトップやアプリケーションで使用され、使用できない場合は他の Web カメラまたはマイクロフォンが使用されます。

リアルタイム オーディオビデオ機能を使用すれば、ビデオ デバイス、オーディオ入力デバイス、およびオーディオ出力デバイスは USB リダイレクトを使用せずに動作し、必要となるネットワーク帯域幅の量は大幅に削減されます。アナログ オーディオ入力デバイスもサポートされます。

注: USB Web カメラやマイクロフォンを使用している場合は、Horizon Client の [USB デバイスを接続] メニューから接続しないでください。これを行うと USB リダイレクトからデバイスがルーティングされるので、デバイスはリアルタイム オーディオビデオ機能を使用できません。

この手順は、Windows 版 Horizon Client 4.2 以降のみに適用されます。それ以前のバージョンのクライアントについては、レジストリ設定を変更して優先する Web カメラを選択し、Windows オペレーティング システムの [サウンド] コントロールを使用してデフォルトのマイクロフォンを選択する必要があります。詳細については、お使いの Horizon Client バージョンの『Windows 版 VMware Horizon Client の使用』を参照してください。

前提条件

- USB Web カメラや USB マイクロフォンまたは他のタイプのマイクロフォンがインストールされ、クライアント システムで動作できる状態であることを確認します。
- リモート デスクトップやアプリケーション用に VMware Blast 表示プロトコルまたは PCoIP 表示プロトコルを使用していることを確認します。
- サーバに接続します。

手順

- 1 [設定] ダイアログ ボックスを開いて、左ペインで [リアルタイム オーディオビデオ] を選択します。

デスクトップやアプリケーション画面の右上隅にある [設定] (歯車) アイコンをクリックするか、デスクトップやアプリケーションのアイコンを右クリックして [設定] をクリックし、[設定] ダイアログ ボックスを開くことができます。
 - 2 [優先する Web カメラ] ドロップダウン メニューから優先する Web カメラを、[優先するマイクロフォン] ドロップダウン メニューから優先するマイクロフォンを選択します。

ドロップダウン メニューには、クライアント システムで利用可能な Web カメラとマイクロフォンが表示されます。
 - 3 [OK] または [適用] をクリックして、変更を保存します。
- リモート デスクトップやアプリケーションを次回起動するときに、優先するように選択した Web カメラとマイクロフォンが、リモート デスクトップやアプリケーションにリダイレクトされます。

Mac クライアント システムでのデフォルトのマイクロフォンの選択

クライアント システムに複数のマイクロフォンがある場合、リモート デスクトップで使用されるのは 1 つだけです。クライアント システムの [システム環境設定] を使用して、リモート デスクトップ用のデフォルトのマイクロフォンを指定できます。

リアルタイム オーディオ ビデオ機能を使用すれば、オーディオ入力デバイスおよびオーディオ出力デバイスは USB リダイレクトを使用せずに動作し、必要となるネットワーク帯域幅の量は大幅に削減されます。アナログ オーディオ 入力デバイスもサポートされます。

この手順では、クライアント システムのユーザー インターフェイスからマイクロフォンを選択する方法について説明します。管理者は、Mac のデフォルト システムを使用して優先するマイクロフォンを構成することもできます。

[Mac クライアント システムで優先する Web カメラまたはマイクロフォンの構成](#)を参照してください。

重要: USB マイクロフォンを使用している場合は、Horizon Client の [接続] - [USB] メニューから接続しないでください。このメニューから接続すると、デバイスは USB リダイレクトによってルーティングされるので、デバイスはリアルタイム オーディオ ビデオ機能を使用できなくなります。

前提条件

- USB マイクロフォンまたは他のタイプのマイクロフォンがインストールされ、クライアント システムで動作できる状態であることを確認します。
- リモート デスクトップ用に VMware Blast 表示プロトコルまたは PCoIP 表示プロトコルを使用していることを確認します。

手順

- 1 クライアント システムで [Apple メニュー] - [システム環境設定] を選択して、[サウンド] をクリックします。
- 2 [サウンド環境設定] の [入力] ペインを開きます。
- 3 使用するマイクロフォンを選択します。

次回、リモート デスクトップに接続して呼び出しを開始すると、クライアント システムで選択したデフォルトのマイクロフォンがデスクトップで使用されます。

Mac クライアント上でのリアルタイム オーディオビデオの構成

リアルタイム オーディオビデオ設定は、Mac のデフォルト システムを使用して、コマンド ラインで構成できます。デフォルト システムでは、ターミナル (/Applications/Utilities/Terminal.app) を使用することで、Mac ユーザーのデフォルト設定の読み取り、書き込み、および削除を行うことができます。

Mac のデフォルト設定は、ドメインに属します。ドメインは通常、個々のアプリケーションに対応します。リアルタイム オーディオビデオ機能のドメインは com.vmware.rtav です。

リアルタイム オーディオビデオを構成するための構文

次のコマンドを使用して、リアルタイム オーディオビデオ機能を構成できます。

表 14-3. リアルタイム オーディオビデオ構成のコマンド構文

コマンド	説明
<code>defaults write com.vmware.rtav scrWCamId "webcam-userid"</code>	リモート デスクトップで優先して使用する Web カメラを設定します。この値を設定しない場合、Web カメラはシステム列挙によって自動的に選択されます。クライアントシステムに接続されている（または組み込まれている）任意の Web カメラを指定できます。
<code>defaults write com.vmware.rtav srcAudioInId "audio-device-userid"</code>	リモート デスクトップで優先して使用するマイクロフォン（オーディオ入力デバイス）を設定します。この値を設定しない場合、リモート デスクトップでは、クライアントシステムで設定されているデフォルトの録音デバイスが使用されます。クライアントシステムに接続されている（または組み込まれている）任意のマイクロフォンを指定できます。
<code>defaults write com.vmware.rtav srcWCamFrameWidth pixels</code>	画像の幅を設定します。この値には、ハードコードされた値である 320 ピクセルがデフォルトとして設定されています。画像の幅は、どのようなピクセル値にも変更できます。
<code>defaults write com.vmware.rtav srcWCamFrameHeight pixels</code>	画像の高さを設定します。この値には、ハードコードされた値である 240 ピクセルがデフォルトとして設定されています。画像の高さは、任意のピクセル値に変更できます。
<code>defaults write com.vmware.rtav srcWCamFrameRate fps</code>	フレーム レートを設定します。この値には、15 fps がデフォルトとして設定されています。フレーム レートは、どのような値にも変更できます。
<code>defaults write com.vmware.rtav LogLevel "level"</code>	リアルタイム オーディオビデオ ログ ファイル（~/Library/Logs/VMware/vmware-RTAV- <i>pid</i> .log）のログ レベルを設定します。ログ レベルをトレースまたはデバッグに設定できます。
<code>defaults write com.vmware.rtav IsDisabled value</code>	リアルタイム オーディオビデオを有効にするか無効にするかを決定します。リアルタイム オーディオビデオはデフォルトで有効に設定されています（この値は適用されていません）。リアルタイム オーディオビデオをクライアント上で無効にするには、値を true に設定します。
<code>defaults read com.vmware.rtav</code>	リアルタイム オーディオビデオの構成設定を表示します。
<code>defaults delete com.vmware.rtav setting</code>	リアルタイム オーディオビデオの構成設定を削除します。以下に例を示します。 <code>defaults delete com.vmware.rtav srcWCamFrameWidth</code>

注: フレーム レートを 1 fps から最大 25 fps まで、解像度を最大 1920x1080 まで調整できます。デバイスまたは環境によっては、高速フレーム レートでの高解像度がサポートされないことがあります。

Mac クライアント システムで優先する Web カメラまたはマイクロフォンの構成

リアルタイム オーディオ ビデオ機能を使用し、クライアント システムに複数の web カメラとマイクロフォンがある場合、リモート デスクトップで利用できるのは 1 台の Web カメラと 1 台のマイクロフォンだけです。Mac のデフォルト システムを使用して、優先する Web カメラとマイクロフォンをコマンド ラインで指定します。

リアルタイム オーディオ ビデオ機能を使用すると、Web カメラ、オーディオ入力デバイス、オーディオ出力デバイスは、USB リダイレクトなしで動作し、必要なネットワーク帯域幅の量が大幅に軽減します。アナログ オーディオ入力デバイスもサポートされます。

ほとんどの環境では、優先マイクロフォンまたは Web カメラを設定する必要はありません。優先マイクロフォンを設定しない場合、リモート デスクトップでは、クライアント システムの [システム環境設定] で設定されたデフォルトのオーディオ デバイスが使用されます。以下を参照してください。 [Mac クライアント システムでのデフォルトのマイクロフォンの選択](#)。優先 Web カメラを構成しない場合、リモート デスクトップでは、列挙された順に従って Web カメラが選択されます。

前提条件

- 優先 USB Web カメラを構成する場合は、その Web カメラがクライアント システムにインストールされ、動作できる状態であることを確認します。
- 優先 USB マイクロフォンまたは他のタイプのマイクロフォンを構成する場合は、そのマイクロフォンがクライアント システムにインストールされ、動作できる状態であることを確認します。
- リモート デスクトップ用に VMware Blast 表示プロトコルまたは PCoIP 表示プロトコルを使用していることを確認します。

手順

- 1 Mac クライアント システムで Web カメラまたはマイクロフォン アプリケーションを起動して、カメラ デバイスまたはオーディオ デバイスの列挙をリアルタイム オーディオ ビデオのログ ファイルにトリガします。
 - a Web カメラまたはオーディオ デバイスを取り付けます。
 - b [アプリケーション] フォルダで [VMware Horizon Client] をダブルクリックして、Horizon Client を起動します。
 - c 呼び出しを開始し、その後呼び出しを停止します。
- 2 リアルタイム オーディオ ビデオ ログ ファイル内で、Web カメラまたはマイクロフォンのログ エントリを見つけます。
 - a リアルタイム オーディオ ビデオ ログ ファイルをテキスト エディタで開きます。
リアルタイム オーディオ ビデオ ログ ファイルには ~/Library/Logs/VMware/vmware-RTAV-*pid*.log という名前が付けられています。*pid* は現在のセッションの処理 ID です。
 - b リアルタイム オーディオ ビデオ ログ ファイルで、接続された Web カメラまたはマイクロフォンを特定するエントリを探します。

次の例では、リアルタイム オーディオ ビデオ ログ ファイルで Web カメラのエントリがどのように表示されるかを示します。

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum() - 1
Device(s) found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void VideoInputBase::LogDevEnum() -
Name=FaceTime HD Camera (Built-in)   UserId=FaceTime HD Camera (Built-in)#0xfa20000005ac8509
SystemId=0xfa20000005ac8509
```

次の例では、リアルタイム オーディオ ビデオ ログ ファイルでマイクロフォンのエントリがどのように表示されるかを示します。

```
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: int
AVCaptureEnumerateAudioDevices(MMDev::DeviceList&) -
```

```

2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum() - 2
Device(s) found
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum() -
Index=255 Name=Built-in Microphone UserId=Built-in
Microphone#AppleHDAEngineInput:1B,0,1,0:1 SystemId=AppleHDAEngineInput:1B,0,1,0:1
2013-12-16T12:18:17.404Z| vthread-3| I120: RTAV: static void AudioCaptureBase::LogDevEnum() -
Index=255 Name=Built-in Input UserId=Built-in Input#AppleHDAEngineInput:1B,0,1,1:2
SystemId=AppleHDAEngineInput:1B,0,1,1:2

```

- リアルタイム オーディオ ビデオ ログ ファイルで、優先する Web カメラまたはマイクロフォンを見つけて、そのユーザー ID をメモします。

ログ ファイルでは、ユーザー ID が文字列 `UserId=` の後に表示されます。たとえば、内蔵フェイス タイム カメラのユーザー ID は FaceTime HD Camera (組み込み) で、内蔵マイクロフォンのユーザー ID は Built-in Microphone です。

- ターミナル (/Applications/Utilities/Terminal.app) で `defaults write` コマンドを使用して、優先する Web カメラまたはマイクロフォンを設定します。

オプション	アクション
優先する Web カメラを設定する	<pre>defaults write com.vmware.rtav srcWCamId "webcam-userid"</pre> と入力します。ここで、 <code>webcam-userid</code> は、リアルタイム オーディオ ビデオ ログ ファイルで取得した、優先する Web カメラのユーザー ID です。例： <pre>defaults write com.vmware.rtav srcWCamId "HD Webcam C525"</pre>
優先するマイクロフォンを設定する	<pre>defaults write com.vmware.rtav srcAudioInId "audio-device-userid"</pre> と入力します。ここで、 <code>audio-device-userid</code> は、リアルタイム オーディオ ビデオ ログ ファイルで取得した、優先するマイクロフォンのユーザー ID です。例： <pre>defaults write com.vmware.rtav srcAudioInId "Built-in Microphone"</pre>

- (オプション) `defaults read` コマンドを使用して、リアルタイム オーディオ ビデオ機能への変更を確認します。

例：`defaults read com.vmware.rtav`

このコマンドにより、リアルタイム オーディオ ビデオ設定のすべてが表示されます。

次回、リモート デスクトップに接続して新しい呼び出しを開始すると、構成した優先 Web カメラまたはマイクロフォンが使用されます (利用可能な場合)。優先 Web カメラまたはマイクロフォンが利用できない場合、リモート デスクトップは別の利用可能な Web カメラまたはマイクロフォンを使用できます。

Linux クライアント システムでのデフォルトのマイクロフォンの選択

クライアント システムに複数のマイクロフォンがある場合、1 つだけが View デスクトップで使用されます。デフォルトで使用するマイクロフォンを指定するために、クライアント システムの [サウンド] コントロールを使用できます。

リアルタイム オーディオ ビデオ機能を使用すれば、オーディオ入力デバイスおよびオーディオ出力デバイスは USB リダイレクトを使用せずに動作し、必要となるネットワーク帯域幅の量は大幅に削減されます。アナログ オーディオ 入力デバイスもサポートされます。

この手順では、クライアント システムのユーザー インターフェイスからデフォルトのマイクロフォンを選択する方法について説明します。管理者が構成ファイルを編集して、優先するマイクロフォンを構成することもできます。

[Linux クライアント システムで優先する Web カメラまたはマイクロフォンの選択](#)を参照してください。

前提条件

- USB マイクロフォンまたは他のタイプのマイクロフォンがインストールされ、クライアント システムで動作できる状態であることを確認します。
- リモート デスクトップ用に VMware Blast 表示プロトコルまたは PCoIP 表示プロトコルを使用していることを確認します。

手順

- 1 Ubuntu グラフィカル ユーザー インターフェイスで、[システム] - [プリファレンス] - [サウンド] を選択します。または、画面の上にあるツール バーの右側の [サウンド] アイコンをクリックします。
- 2 [Sound Preferences] ダイアログ ボックスの [入力] タブをクリックします。
- 3 優先するデバイスを選択して [閉じる] をクリックします。

Linux クライアント システムで優先する Web カメラまたはマイクロフォンの選択

リアルタイム オーディオ ビデオ機能があり、クライアント システムに複数の Web カメラとマイクロフォンがある場合、1 台の Web カメラと 1 台のマイクロフォンだけを View デスクトップで使用できます。優先する Web カメラとマイクロフォンを指定するには、構成ファイルを編集します。

優先する Web カメラまたはマイクロフォンは、使用できる場合はリモート デスクトップで使用され、使用できない場合は他の Web カメラまたはマイクロフォンが使用されます。

リアルタイム オーディオ ビデオ機能を使用すれば、Web カメラ、オーディオ入力デバイスおよびオーディオ出力デバイスは、USB リダイレクトを使用せずに動作し、必要となるネットワーク帯域幅量は大幅に削減されます。アナログ オーディオ入力デバイスもサポートされます。

/etc/vmware/config ファイルにプロパティを設定し、優先するデバイスを指定するには、特定のフィールドの値を確定する必要があります。これらのフィールドの値については、ログ ファイルを検索できます。

- Web カメラについては、rtav.srcWCamId プロパティを Web カメラの UserId フィールドの値に設定し、rtav.srcWCamName プロパティを Web カメラの Name フィールドの値に設定します。

rtav.srcWCamName プロパティには、rtav.srcWCamId プロパティよりも高い優先度が設定されています。両方のプロパティでは、同じ Web カメラが指定されるはずですが、これらのプロパティが異なる Web カメラを指定する場合、rtav.srcWCamName が存在する場合、このプロパティによって指定される Web カメラが使用されます。このプロパティが存在しない場合、rtav.srcWCamId によって指定される Web カメラが使用されます。両方の Web カメラが見つからない場合、デフォルトの Web カメラが使用されます。
- オーディオ デバイスの場合、rtav.srcAudioInId プロパティを Pulse Audio device.description フィールドの値に設定します。

前提条件

優先する Web カメラ、優先するマイクロフォン、または両方のいずれを構成するかに応じて、所定の準備作業を行います。

- USB webcam がインストールされ、クライアント システムで動作できる状態であることを確認します。
- USB マイクロフォンまたは他のタイプのマイクロフォンがインストールされ、クライアント システムで動作できる状態であることを確認します。
- リモート デスクトップ用に VMware Blast 表示プロトコルまたは PCoIP 表示プロトコルを使用していることを確認します。

手順

- 1 クライアントを起動し、Web カメラまたはマイクロフォンのアプリケーションを開始して、カメラ デバイスまたはオーディオ デバイスの一覧がクライアント ログに出力されるようにします。
 - a 使用する Web カメラまたはオーディオ デバイスを接続します。
 - b `vmware-view` コマンドを使用して Horizon Client を起動します。
 - c 呼び出しを開始し、その後呼び出しを停止します。このプロセスでログ ファイルが作成されます。

2 Web カメラまたはマイクロフォンというログのエントリを探します。

a テキスト エディタでデバッグ ログ ファイルを開きます。

リアルタイム オーディオ ビデオのログ メッセージが出力されるログ ファイルは、`/tmp/vmware-
<username>/vmware-RTAV-<pid>.log` に保存されています。クライアント ログは、`/tmp/vmware-
<username>/vmware-view-<pid>.log` に保存されています。

b ログ ファイルを検索して、接続されている Web カメラおよびマイクロフォンを参照しているログ ファイルのエントリを探します。

Web カメラを抽出する例を以下に示します。

```
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - 3 Device(s) found
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=UVC Camera (046d:0819)
UserId=UVC Camera (046d:0819)#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.4/1-3.4.5
SystemId=/dev/video1
main| I120: RTAV: static void VideoInputBase::LogDevEnum() - Name=gspca main driver
UserId=gspca main driver#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.4/1-3.4.7
SystemId=/dev/video2
main| I120: RTAV: static void VideoInputBase::LogDevEnum() -
Name=Microsoft® LifeCam HD-6000 for Notebooks UserId=Microsoft® LifeCam HD-6000 for
Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6 SystemId=/dev/video0
main| W110: RTAV: static bool AudioCaptureLin::EnumCaptureDevices(MMDev::DeviceList&) -
enumeration data unavailable
```

オーディオ デバイスとそれぞれの現在のオーディオ レベルを抽出する例を以下に示します。

```
vthread-18| I120: RTAV: bool AudioCaptureLin::TriggerEnumDevices() - Triggering enumeration
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - PulseAudio Get Source (idx=1 'alsa_output.usb-
Logitech_Logitech_USB_Headset-00-Headset.analog-stereo.monitor' 'Monitor of Logitech USB
Headset Analog Stereo')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:0 vol:65536
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:1 vol:65536
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - PulseAudio Get Source (idx=2 'alsa_input.usb-
Logitech_Logitech_USB_Headset-00-Headset.analog-mono' 'Logitech USB Headset Analog Mono')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:0 vol:98304
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - PulseAudio Get Source (idx=3 'alsa_output.usb-
Microsoft_Microsoft_LifeChat_LX-6000-00-LX6000.analog-stereo.monitor' 'Monitor of Microsoft
LifeChat LX-6000 Analog Stereo')

vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioGetSourceCB(pa_context*, const
pa_source_info*, int, void*) - channel:0 vol:65536
```

選択したデバイスのいずれかのソース オーディオ レベルが PulseAudio 基準を満たしていない場合 (ソースが 100% (0dB) に設定されていない場合)、または選択したソース デバイスがミュートになっている場合は、以下の警告が表示されます。

```
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*,
const pa_source_info*, int, void*) - Note, selected device channel volume: 0: 67%
vthread-18| I120: RTAV: static void AudioCaptureLin::PulseAudioSourceInfoCB(pa_context*,
const pa_source_info*, int, void*) - Note, selected device channel is muted
```

- 3 デバイスの記述をコピーし、それを利用して /etc/vmware/config ファイルに正しくプロパティを設定します。

Web カメラの例では、Microsoft® LifeCam HD-6000 for Notebooks と Microsoft® LifeCam HD-6000 for Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6 をコピーして、優先される Web カメラとして Microsoft の Web カメラを指定し、次のようにプロパティを設定します。

```
rtav.srcWCamName = "Microsoft® LifeCam HD-6000 for Notebooks"
rtav.srcWCamId = "Microsoft® LifeCam HD-6000 for Notebooks#/sys/devices/pci0000:00/0000:00:1a.7/usb1/1-3/1-3.6"
```

この例では、rtav.srcWCamId プロパティを "Microsoft" に設定することもできます。rtav.srcWCamId プロパティは、部分および完全一致の両方をサポートします。rtav.srcWCamName プロパティは、完全一致のみをサポートします。

オーディオ デバイスの場合には、たとえば Logitech ヘッドセットを優先オーディオ デバイスとして指定するために Logitech USB Headset Analog Mono をコピーし、プロパティを次のように設定します。

```
rtav.srcAudioInId="Logitech USB Headset Analog Mono"
```

- 4 変更を保存し、/etc/vmware/config 構成ファイルを閉じます。
- 5 デスクトップ セッションをログオフして、新しいセッションを開始します。

リアルタイム オーディオ ビデオ グループ ポリシ設定の構成

View デスクトップでのリアルタイム オーディオ ビデオ (RTAV) の動作を制御するグループ ポリシ設定を構成できます。これらの設定は、仮想 webcam の最大フレーム レートおよび画像の解像度を決定します。これらの設定によって、1 人のユーザーが消費できる最大帯域幅を管理できます。追加設定は RTAV 機能を無効または有効にします。

これらのポリシ設定を構成する必要はありません。リアルタイム オーディオ ビデオは、クライアント システムの webcam に設定されるフレーム レートおよび画像の解像度で動作します。デフォルト設定がほとんどの webcam およびオーディオ アプリケーションで推奨されます。

リアルタイム オーディオ ビデオ中に使用する帯域幅の例については、[リアルタイム オーディオ ビデオの帯域幅](#)を参照してください。

これらのポリシ設定は、物理デバイスが接続されているクライアント システムではなく、View デスクトップに影響します。これらの設定をデスクトップで構成するには、Active Directory に RTAV グループ ポリシー管理テンプレート (ADM) ファイルを追加します。

クライアント システムでの設定については、VMware ナレッジベースの記事、『Setting Frame Rates and Resolution for Real-Time Audio-Video on Horizon View Clients (Horizon View Client でのリアルタイム オーディオ-ビデオのフレームレートと解像度の設定)』(<http://kb.vmware.com/kb/2053644>) を参照してください。

アクティブ ディレクトリに RTAV ADM テンプレートを追加した設定の構成

RTAV ADM ファイル、`vdm_agent_rtav.adm`、のポリシー設定を Active Directory のグループ ポリシー オブジェクト (GPO) に追加し、Group Policy Object Editor の設定を構成することができます。

前提条件

- デスクトップに RTAV 設定オプションがインストールされていることを確認します。この設定オプションはデフォルトでインストールされますが、インストール中に選択を解除することができます。この設定は RTAV がインストールされなければ効果がありません。[仮想マシンへの Horizon Agent のインストール](#)を参照してください。
- Active Directory GPO が RTAV グループ ポリシ設定で作成されることを確認します。GPO は、デスクトップを含む OU にリンクする必要があります。[Active Directory グループ ポリシーの例](#)を参照してください。
- Active Directory サーバで、Microsoft MMC およびグループ ポリシー オブジェクト エディタ スナップインが使用できることを確認します。
- RTAV グループ ポリシ設定をよく理解してください。[リアルタイム オーディオ ビデオ グループ ポリシ設定](#) を参照してください。

手順

- 1 View GPO Bundle .zip ファイルを <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 GPO Bundle が含まれます。

ファイル名は `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` で、`x.x.x` はバージョン、`yyyyyy` はビルド番号を表します。View のグループ ポリシー設定用の ADM ファイルと ADMX ファイルはすべて、このファイルで提供されています。

- 2 `VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyy.zip` ファイルを解凍して、RTAV ADM ファイル `vdm_agent_rtav.adm` を Active Directory サーバにコピーします。
- 3 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 GPO を編集します。
- 4 グループ ポリシー オブジェクト エディタで、[コンピュータの構成] - [管理テンプレート] フォルダを右クリックして、[テンプレートの追加と削除] を選択します。
- 5 [追加] をクリックして `vdm_agent_rtav.adm` ファイルを参照し、[開く] をクリックします。
- 6 [閉じる] をクリックして ADM ファイルのポリシ設定を GPO に適用します。

この設定は、[コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [従来の管理用テンプレート] - [VMware Horizon Agent の構成] - [RTAV 構成を表示] フォルダ内にあります。

7 RTAV グループ ポリシ設定を構成します。

リアルタイム オーディオ ビデオ グループ ポリシ設定

リアルタイム オーディオ ビデオ (RTAV) グループ ポリシー設定により、仮想 Web カメラの最大フレーム レートおよび画像の最大解像度を制御できます。追加設定により RTAV 機能を無効または有効にできます。このポリシー設定は View デスクトップに影響し、物理デバイスが接続されたクライアント システムには影響しません。

RTAV グループ ポリシー設定を構成しない場合、RTAV はクライアント システムに設定されている値を使用します。クライアント システムでは、デフォルトの Web カメラフレーム レートは 1 秒あたり 15 フレームです。デフォルトの Web カメラ画像の解像度は 320x240 ピクセルです。

[解像度 - 最大画像...] グループ ポリシー設定で、使用できる最大値を決定します。クライアント システムで設定されるフレーム レートと解像度は絶対値です。たとえば、RTAV 設定の画像の最大解像度を 640x480 ピクセルに構成すると、Web カメラではクライアントで設定された最大 640x480 ピクセルまでの解像度を表示します。クライアントの画像解像度を 640x480 ピクセルよりも高い値に設定すると、クライアント解像度は 640x480 ピクセルが上限となります。

構成によっては、1 秒あたり 25 フレームで 1920x1080 の解像度の最大グループ ポリシー設定を達成できない場合があります。指定された解像度に対して構成で達成できる最大フレーム レートは、使用する Web カメラ、クライアント システム ハードウェア、Horizon Agent 仮想ハードウェア、利用可能な帯域幅によって異なります。

[解像度 - デフォルト イメージ...] グループ ポリシー設定は、ユーザーによって解像度の値が設定されていない場合に使用されるデフォルト値を決定します。

グループ ポリシー設定	説明
RTAV の無効化	<p>この設定を有効にすると、リアルタイム オーディオ ビデオ機能が無効になります。</p> <p>この設定が構成されていない場合、または無効になっている場合は、リアルタイム オーディオ ビデオが有効になります。</p> <p>この設定は [RTAV 構成を表示] フォルダにあります。</p>
1 秒あたりの最大フレーム	<p>Web カメラがフレームをキャプチャできる、1 秒あたりの最大レートを決定します。この設定を使用して、低帯域幅ネットワーク環境での Web カメラ フレーム レートを制限できます。</p> <p>最小値は 1 秒あたり 1 フレームです。最大値は 1 秒あたり 25 フレームです。</p> <p>この設定が構成されていない場合、または無効になっている場合は、最大フレーム レートは設定されません。リアルタイム オーディオ ビデオはクライアント システムで Web カメラに選択されたフレーム レートを使用します。</p> <p>デフォルトでは、クライアント Web カメラのフレーム レートは 1 秒あたり 15 フレームです。クライアント システムで設定が構成されておらず、[1 秒あたりの最大フレーム] 設定が構成されていない場合、または無効になっている場合は、Web カメラは 1 秒あたり 15 フレームをキャプチャします。</p> <p>この設定は [RTAV 構成を表示] - [RTAV Web カメラ設定を表示] フォルダにあります。</p>
解像度 - ピクセル単位での画像の最大幅	<p>Web カメラによってキャプチャされる画像フレームのピクセル単位での最大幅を決定します。画像の最大幅を低く設定することで、キャプチャされるフレームの解像度を下げ、低帯域幅ネットワーク環境でのイメージングの使用環境を改善することができます。</p> <p>この設定が構成されていない場合、または無効になっている場合は、画像の最大幅は設定されません。RTAV はクライアント システムで設定された画像の幅を使用します。クライアント システムのデフォルトの Web カメラ画像の幅は 320 ピクセルです。</p> <p>Web カメラ画像の上限は 1920x1080 ピクセルです。この設定を 1920 ピクセルよりも大きい値で構成した場合、有効となる画像の最大幅は 1920 ピクセルです。</p> <p>この設定は [RTAV 構成を表示] - [RTAV Web カメラ設定を表示] フォルダにあります。</p>

グループ ポリシー設定	説明
解像度 - ピクセル単位での画像の最大の高さ	<p>Web カメラによってキャプチャされる画像フレームのピクセル単位での最大の高さを決定します。画像の最大の高さを低く設定することで、キャプチャされるフレームの解像度を下げ、低帯域幅ネットワーク環境でのイメージングの使用環境を改善することができます。</p> <p>この設定が構成されていない場合、または無効になっている場合は、画像の最大の高さは設定されません。RTAV はクライアント システムで設定された画像の高さを使用します。クライアント システムのデフォルトの Web カメラ画像の高さは 240 ピクセルです。</p> <p>Web カメラ画像の上限は 1920x1080 ピクセルです。この設定を 1080 ピクセルよりも大きい値で構成した場合、有効となる画像の最大の高さは 1080 ピクセルです。</p> <p>この設定は [RTAV 構成を表示] - [RTAV Web カメラ設定を表示] フォルダにあります。</p>
解像度 - ピクセル単位でのデフォルト イメージ解像度の幅	<p>Web カメラによってキャプチャされる画像フレームのピクセル単位でのデフォルトの解像度の幅を決定します。この設定は解像度の値がユーザーによって定義されていない場合に使用されます。</p> <p>この設定が構成されていない場合、または無効になっている場合は、デフォルト イメージの幅は 320 ピクセルになります。</p> <p>このポリシー設定によって構成された値は、View Agent 6.0 以降および Horizon Client 3.0 以降の両方が使用されている場合にのみ有効になります。View Agent または Horizon Client のバージョンが古い場合はこのポリシー設定が無効となり、デフォルト イメージの幅は 320 ピクセルになります。</p> <p>この設定は [RTAV 構成を表示] - [RTAV Web カメラ設定を表示] フォルダにあります。</p>
解像度 - ピクセル単位でのデフォルト イメージ解像度の高さ	<p>Web カメラによってキャプチャされる画像フレームのピクセル単位でのデフォルトの解像度の高さを決定します。この設定は解像度の値がユーザーによって定義されていない場合に使用されます。</p> <p>この設定が構成されていない場合、または無効になっている場合には、デフォルト イメージの高さは 240 ピクセルになります。</p> <p>このポリシー設定によって構成された値は、View Agent 6.0 以降および Horizon Client 3.0 以降の両方が使用されている場合にのみ有効になります。View Agent または Horizon Client のバージョンが古い場合はこのポリシー設定が無効となり、デフォルト イメージの高さは 240 ピクセルになります。</p> <p>この設定は [RTAV 構成を表示] - [RTAV Web カメラ設定を表示] フォルダにあります。</p>

リアルタイム オーディオ ビデオの帯域幅

リアルタイム オーディオ ビデオの帯域幅は、Web カメラの画像解像度およびフレーム レート、キャプチャされている画像やオーディオ データによって異なります。

表 14-4. Horizon Client から Horizon Agent へのリアルタイム オーディオ ビデオ データの送信の帯域幅の結果のサンプルに示すサンプルのテストは、リアルタイム オーディオ ビデオが標準的な Web カメラとオーディオ入力デバイスを含む View 環境で使用する帯域幅を測定します。このテストは Horizon Client から Horizon Agent へのビデオおよびオーディオ データの両方を送信する帯域幅を測定します。Horizon Client からデスクトップ セッションを実行するのに必要な帯域幅の合計は、この数字よりも大きくなる可能性があります。これらのテストでは、Web カメラはイメージを各画像解像度に対し毎秒 15 フレームでキャプチャします。

表 14-4. Horizon Client から Horizon Agent へのリアルタイム オーディオ ビデオ データの送信の帯域幅の結果のサンプル

画像解像度 (幅 x 高さ)	使用されている帯域幅 (Kbps)
160 x 120	225
320 x 240	320
640 x 480	600

スキャナ リダイレクトの構成

スキャナ リダイレクトを使用することで、View ユーザーはクライアント コンピュータにローカルに接続されたスキャナやイメージング デバイスを使用して、リモート デスクトップおよびアプリケーション内の情報をスキャンできます。スキャナ リダイレクトは Horizon 6.0.2 以降のリリースで使用できます。

スキャナ リダイレクトは、TWAIN および WIA 形式と互換性がある標準のスキャナやイメージング デバイスをサポートしています。

スキャナ リダイレクトのセットアップ オプションを使用して Horizon Agent をインストールすると、後から構成しなくても、リモート デスクトップおよびアプリケーションでスキャナ リダイレクトが機能します。リモート デスクトップまたはアプリケーションにスキャナ固有のドライバを構成する必要はありません。

グループ ポリシー設定を構成してデフォルト値を変更し、特定のスキニングおよびイメージング アプリケーションまたは環境に適用することができます。ポリシーを設定して機能をすべて無効または有効にすることもできます。ADM テンプレート ファイルを使用すると、スキャナ リダイレクト グループ ポリシー設定を Active Directory または個別のデスクトップにインストールできます。[スキャナ リダイレクトのグループ ポリシー設定の構成](#)を参照してください。

スキニング データがリモート デスクトップまたはアプリケーションにリダイレクトされると、ユーザーはローカル コンピュータのスキャナやイメージング デバイスにアクセスできません。逆に言えば、デバイスがローカル コンピュータで使用中であれば、リモート デスクトップでそのデバイスにアクセスできません。

スキャナ リダイレクトのシステム要件

スキャナ リダイレクトをサポートするには、View の展開が特定のソフトウェアおよびハードウェア要件を満たす必要があります。

View リモート デスクトップまたはアプリケーション

この機能は、単一ユーザーの仮想マシンに展開された RDS デスクトップ、RDS アプリケーション、および VDI デスクトップでサポートされています。

親またはテンプレート仮想マシンまたは RDS ホストに View Agent 6.0.2 以降をインストールして、スキャナ リダイレクト セットアップ オプションを選択する必要があります。

Windows デスクトップおよび Windows Server ゲスト OS では、Horizon Agent スキャナ リダイレクト セットアップ オプションがデフォルトでオフになっています。

単一ユーザーの仮想マシンおよび（記載されている場合は）RDS ホストでは、次のゲスト OS がサポートされます。

- 32 ビットまたは 64 ビットの Windows 7
- 32 ビットまたは 64 ビットの Windows 8。x
- 32 ビットまたは 64 ビットの Windows 10
- デスクトップまたは RDS ホストとして構成されている Windows Server 2008 R2

- デスクトップまたは RDS ホストとして構成されている Windows Server 2012 R2

重要: デスクトップとして構成されているか RDS ホストとして構成されているかに関係なく、Windows Server ゲスト OS にはデスクトップ エクスプレス機能をインストールしておく必要があります。

Horizon Agent がインストールされているデスクトップ オペレーティング システムにスキャナ デバイス ドライバをインストールする必要はありません。

Horizon Client ソフトウェア

Windows 版 Horizon Client 3.2 以降のリリース

Horizon Client コンピュータまたはクライアント アクセス デバイス

サポートされるオペレーティング システムは次のとおりです。

- 32 ビットまたは 64 ビットの Windows 7
- 32 ビットまたは 64 ビットの Windows 8。x
- 32 ビットまたは 64 ビットの Windows 10

スキャナ デバイス ドライバをインストールする必要があり、スキャナがクライアント コンピュータで操作可能である必要があります。

スキャン デバイスの標準

TWAIN または WIA

View 用の表示プロトコル

PCoIP

スキャナ リダイレクトは、RDP デスクトップ セッションでサポートされません。

スキャナ リダイレクトのユーザー操作

スキャナ リダイレクトを使用すると、クライアント コンピュータに接続されている物理スキャナとイメージング デバイスを、リモート デスクトップおよびアプリケーションでスキャン操作を実行する仮想デバイスとして操作できます。

ユーザーは、ローカル接続されたクライアント コンピュータ上のスキャナを使用する場合とよく似た方法で仮想スキャナを操作できます。

- Horizon Agent でスキャナ リダイレクト オプションをインストールした後、スキャナ ツール トレイ アイコン (🖨️) がデスクトップに追加されます。RDS アプリケーションでは、ツール トレイ アイコンはローカル クライアント コンピュータにリダイレクトされます。

スキャナ ツール トレイ アイコンを使用する必要はありません。スキャンのリダイレクトは何も構成しなくても機能します。アイコンを使用すると、複数のデバイスがクライアント コンピュータに接続されている場合に使用するデバイスの変更など、オプションの構成を実行できます。

- スキャナ アイコンをクリックすると、[VMware Horizon のスキャナ リダイレクト] メニューが表示されます。クライアント コンピュータに互換性のないスキャナが接続されている場合、メニュー リストにスキャナは表示されません。

- デフォルトでは、スキャン デバイスが自動選択されます。TWAIN スキャナと WIA スキャナは個別に選択されます。TWAIN スキャナと WIA スキャナは同時に 1 つずつ選択できます。
- ローカル接続されたスキャナが複数構成されている場合は、デフォルトで選択されているスキャナとは別のスキャナを選択できます。
- WIA スキャナは、リモート デスクトップの [デバイス マネージャ] メニューの [イメージング デバイス] に表示されます。WIA スキャナの名前は [VMware Virtual WIA スキャナ] です。
- [VMware Horizon のスキャナ リダイレクト] メニューで [環境設定] オプションをクリックすると、スキャナ リダイレクト メニューでの Web カメラの非表示やデフォルト スキャナの選択方法の決定などのオプションを選択できます。

また、Active Directory でスキャナ リダイレクト グループ ポリシー設定を構成して、この機能をコントロールすることもできます。[スキャナ リダイレクトのグループ ポリシー設定](#)を参照してください。

- TWAIN スキャナを操作する場合は、[VMware Horizon の TWAIN スキャナ リダイレクト] メニューに、イメージの領域を選択したり、カラー、白黒、またはグレースケールでスキャンしたり、その他の一般的な機能を選択したりするための追加のオプションが表示されます。
- デフォルトではウィンドウを表示しない TWAIN スキャン ソフトウェアの TWAIN ユーザー インターフェイス ウィンドウを表示するには、[VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスの [[スキャナ設定] ダイアログを常に表示] オプションを選択します。

ただし、ほとんどの TWAIN スキャン ソフトウェアはデフォルトで TWAIN ユーザー インターフェイス ウィンドウを表示します。このソフトウェアでは、[[スキャナ設定] ダイアログを常に表示] オプションを選択しているかどうかに関係なく、このウィンドウは常に表示されます。

注: 異なるファームでホストされている 2 つの RDS アプリケーションを実行している場合、クライアント コンピュータには 2 つのスキャナ リダイレクト ツールトレイ アイコンが表示されます。通常、クライアント コンピュータには 1 つのスキャナのみが接続されています。この場合は、両方のアイコンが同じデバイス进行操作するため、どちらのアイコンを選択してもかまいません。状況によっては、ローカル接続されたスキャナが 2 つあり、異なるファームで稼動する 2 つの RDS アプリケーションを実行している場合があります。その場合は、各アイコンを開いて、どちらのスキャナ リダイレクト メニューがどちらの RDS アプリケーションをコントロールするかを確認する必要があります。

エンド ユーザーがリダイレクトされるスキャナを操作する手順については、『Windows 版 VMware Horizon Client の使用』を参照してください。

スキャナ リダイレクトのグループ ポリシー設定の構成

View デスクトップとアプリケーションでのスキャナ リダイレクトの動作を制御するグループ ポリシー設定を構成できます。これらのポリシー設定を使用すると、ユーザーのデスクトップおよびアプリケーションの VMware Horizon スキャナ リダイレクトの [環境設定] ダイアログ ボックスで使用可能なオプションを、Active Directory から集中管理できます。

これらのポリシー設定を構成する必要はありません。スキャナ リダイレクトは、リモート デスクトップやクライアント システムのスキャナ デバイス用に構成されたデフォルトの設定で機能します。

これらのポリシー設定はユーザーのリモート デスクトップとアプリケーションには影響しますが、物理スキャナが接続されたクライアント システムには影響しません。これらの設定をデスクトップとアプリケーションで構成するには、Active Directory にスキャナ リダイレクト グループ ポリシー管理テンプレート (ADM) ファイルを追加します。

スキャナ リダイレクト ADM テンプレートを Active Directory に追加する

スキャナ リダイレクト ADM ファイル、`vdm_agent_scanner.adm` のポリシー設定を Active Directory のグループ ポリシー オブジェクト (GPO) に追加し、グループ ポリシー オブジェクト エディタで設定を構成することができます。

前提条件

- スキャナリダイレクトのセットアップ オプションがデスクトップと RDS ホストにインストールされていることを確認します。スキャナリダイレクトがインストールされていないと、グループ ポリシー設定は有効になりません。[仮想マシンへの Horizon Agent のインストール](#)を参照してください。
- スキャナリダイレクトのグループ ポリシー設定用に Active Directory GPO が作成されていることを確認します。GPO は、デスクトップと RDS ホストを含む OU にリンクする必要があります。[Active Directory グループ ポリシーの例](#)を参照してください。
- MMC およびグループ ポリシー オブジェクト エディタ スナップインが Active Directory サーバで使用できることを確認します。
- スキャナリダイレクトのグループ ポリシー設定について理解しておきます。[スキャナ リダイレクトのグループ ポリシー設定](#)を参照してください。

手順

- 1 View GPO Bundle .zip ファイルを <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 GPO Bundle が含まれます。

ファイル名は `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyyy.zip` で、`x.x.x` はバージョン、`yyyyyyyy` はビルド番号を表します。View のグループ ポリシー設定用の ADM ファイルと ADMX ファイルはすべて、このファイルで提供されています。

- 2 `VMware-Horizon-View-Extras-Bundle-x.x.x-yyyyyyyy.zip` ファイルを解凍して、スキャナ リダイレクト ADM ファイル `vdm_agent_scanner.adm` を Active Directory サーバにコピーします。
- 3 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 GPO を編集します。
- 4 グループ ポリシー オブジェクト エディタで、[コンピュータの構成] - [管理テンプレート] フォルダを右クリックして、[テンプレートの追加と削除] を選択します。
- 5 [追加] をクリックして、`vdm_agent_scanner.adm` ファイルを参照し、[開く] をクリックします。
- 6 [閉じる] をクリックして ADM ファイルのポリシー設定を GPO に適用します。

この設定は、[コンピュータの構成] - [ポリシー] - [管理テンプレート] - [従来の管理テンプレート] - [VMware View Agent の構成] - [スキャナ リダイレクト] フォルダ内にあります。

ほとんどの設定も、[ユーザー構成] - [ポリシー] - [管理テンプレート] - [従来の管理テンプレート] - [VMware View Agent の構成] - [スキャナ リダイレクト] 内の [ユーザー構成] フォルダに追加されます。

7 スキャナ リダイレクトのグループ ポリシー設定を構成します。

スキャナ リダイレクトのグループ ポリシー設定

スキャナ リダイレクトのグループ ポリシーの設定は、[VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスでユーザーのデスクトップおよびアプリケーションに対して使用できるオプションを制御します。

スキャナ リダイレクト ADM ファイルには、コンピュータの構成とユーザーの構成の両方のポリシーが含まれます。ユーザーの構成ポリシーを使用すると、VDI デスクトップ、RDS デスクトップ、RDS アプリケーションのユーザーに対してさまざまな構成を設定できます。ユーザーのデスクトップ セッションやアプリケーションが同じ RDS ホスト上で実行されている場合であっても、さまざまなユーザーの構成ポリシーを適用できます。

グループ ポリ シー設定	説明
機能を無効にする	<p>スキャナ リダイレクト機能を無効にします。</p> <p>この設定は、コンピュータの構成ポリシーとしてのみ使用できます。</p> <p>この設定を有効にすると、スキャナはリダイレクトできなくなり、ユーザーのデスクトップおよびアプリケーションのスキャナ メニューに表示されません。</p> <p>この設定を無効にすると、または構成しないと、スキャナ リダイレクトは動作し、スキャナ メニューにスキャナが表示されます。</p>
構成をロックする	<p>スキャナ リダイレクトのユーザー インターフェイスをロックし、ユーザーがデスクトップおよびアプリケーションで構成オプションを変更できないようにします。</p> <p>この設定は、コンピュータの構成ポリシーとしてのみ使用できます。</p> <p>この設定を有効にすると、ユーザーはデスクトップおよびアプリケーションのトレイ メニューから使用できるオプションを構成できません。ユーザーは [VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスを表示することはできますが、オプションが非アクティブになっていて、変更できません。</p> <p>この設定を無効にすると、または構成しないと、ユーザーは [VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスでオプションを構成できます。</p>
圧縮	<p>リモート デスクトップまたはアプリケーションへのイメージ転送時のイメージ圧縮率を設定します。</p> <p>以下の圧縮モードから選択できます。</p> <ul style="list-style-type: none"> ■ [無効化]。イメージの圧縮を無効にします。 ■ [ロスレス]。イメージの品質が低下しないロスレス (zlib) 圧縮を使用します。 ■ [JPEG]。品質の低下がある JPEG 圧縮を使用します。[JPEG 圧縮品質] フィールドでイメージ品質のレベルを指定します。JPEG 圧縮品質に指定できる値は 0 ~ 100 です。 <p>この設定を有効にすると、このポリシーが適用されるすべてのユーザーに対して選択した圧縮モードが設定されます。ただし、ユーザーは [VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスで [圧縮] オプションを変更することで、ポリシー設定をオーバーライドできます。</p> <p>このポリシー設定を無効にすると、または構成しないと、[JPEG] 圧縮モードが使用されます。</p>

グループ ポリ	
シー設定	説明
Web カメラ を非表示	<p>[VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスのスキャナ選択メニューに、Web カメラが表示されないようにします。</p> <p>この設定は、コンピュータの構成ポリシーおよびユーザーの構成ポリシーとして使用できます。</p> <p>デフォルトでは、Web カメラをデスクトップおよびアプリケーションにリダイレクトできます。ユーザーは Web カメラを選択し、仮想スキャナとして使用してイメージをキャプチャできます。</p> <p>この設定をコンピュータの構成ポリシーとして有効にすると、Web カメラは影響を受けるコンピュータのすべてのユーザーに対して表示されなくなります。ユーザーは、[VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスの [Web カメラを非表示] オプションを変更できません。</p> <p>この設定をユーザーの構成ポリシーとして有効にすると、Web カメラは影響を受けるすべてのユーザーに対して表示されなくなります。ただし、ユーザーは、[VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスの [Web カメラを非表示] オプションを変更できます。</p> <p>この設定をコンピュータの構成およびユーザーの構成の両方で有効にすると、影響を受けるコンピュータのすべてのユーザーについて、コンピュータの構成における [Web カメラを非表示] 設定によって、ユーザーの構成における対応するポリシー設定がオーバーライドされます。</p> <p>どちらかのポリシー構成でこの設定を無効にするか、または構成しないと、[Web カメラを非表示] 設定は、対応するポリシー設定（ユーザーの構成またはコンピュータの構成）または [VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスにおけるユーザーの選択によって決まります。</p>
デフォルト ス キャナ	<p>スキャナの自動選択を集中管理できるようにします。</p> <p>この設定は、コンピュータの構成ポリシーおよびユーザーの構成ポリシーとして使用できます。</p> <p>スキャナの自動選択オプションは、TWAIN スキャナと WIA スキャナで個別に選択します。以下の自動選択オプションから選択できます。</p> <ul style="list-style-type: none"> ■ [なし]。スキャナを自動的に選択しません。 ■ [自動選択]。ローカル接続されているスキャナを自動的に選択します。 ■ [前回使用]。最後に使用されたスキャナを自動的に選択します。 ■ [指定]。[指定したスキャナ] テキスト ボックスに入力したスキャナ名を選択します。 <p>この設定をコンピュータの構成ポリシーとして有効にすると、影響を受けるコンピュータのすべてのユーザーについて、この設定によりスキャナの自動選択モードが決まります。ユーザーは、[VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスの [デフォルト スキャナ] オプションを変更できません。</p> <p>この設定をユーザーの構成ポリシーとして有効にすると、影響を受けるすべてのユーザーについて、この設定によりスキャナの自動選択モードが決まります。ただし、ユーザーは、[VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスの [デフォルト スキャナ] オプションを変更できます。</p> <p>この設定をコンピュータの構成およびユーザーの構成の両方で有効にすると、影響を受けるコンピュータのすべてのユーザーについて、コンピュータの構成におけるスキャナの自動選択モードによって、ユーザーの構成における対応するポリシー設定がオーバーライドされます。</p> <p>どちらかのポリシー構成でこの設定を無効にするか、または構成しないと、スキャナの自動選択モードは、対応するポリシー設定（ユーザーの構成またはコンピュータの構成）または [VMware Horizon スキャナ リダイレクトの環境設定] ダイアログ ボックスにおけるユーザーの選択によって決まります。</p>

シリアル ポート リダイレクトの構成

シリアル ポート リダイレクトを使用すると、ユーザーは内蔵の RS232 ポートまたは USB シリアル アダプタなどの、ローカルに接続されたシリアル（COM）ポートをリダイレクトできます。プリンタ、バーコード リーダー、その他のシリアル デバイスなどのデバイスをこれらのポートに接続し、リモート デスクトップで使用できます。

シリアル ポート リダイレクトは Windows 版 Horizon Client 3.4 以降のリリースを搭載した Horizon 6 バージョン 6.1.1 以降のリリースで使用できます。

Horizon Agent をインストールし、シリアル ポート リダイレクトの機能を設定すると、この機能はそれ以上の構成なしにリモート デスクトップ上で動作できます。たとえば、リモート デスクトップ上に COM ポートがすでに存在する場合を除いて、ローカル クライアント システム上の COM1 はリモート デスクトップ上で COM1 としてリダイレクトされ、COM2 は COM2 としてリダイレクトされます。COM ポートがすでに存在する場合は、COM ポートがマップされ、競合は回避されます。たとえば、COM1 と COM2 がリモート デスクトップにすでに存在する場合、デフォルトでクライアントの COM1 は COM3 にマップされます。COM ポートを構成したり、デバイス ドライバをリモート デスクトップにインストールする必要はありません。

リダイレクトされた COM ポートをアクティブにするには、ユーザーはデスクトップ セッション中にシリアル ポート ツールトレイ アイコンのメニューから、[[接続]] オプションを選択します。また、ユーザーはリモート デスクトップへのログイン時に COM ポート デバイスが必ず自動的に接続するよう設定することも可能です。[シリアル ポート リダイレクトのユーザー操作](#)を参照してください。

デフォルトの構成を変更するには、グループ ポリシー設定を構成できます。たとえば、設定をロックして、COM ポート マッピングまたはプロパティをユーザーが変更できないようにすることができます。ポリシーを設定して機能をすべて無効または有効にすることもできます。ADM テンプレート ファイルを使用すると、ポート リダイレクト グループ ポリシー設定を Active Directory または個別のデスクトップにインストールできます。[シリアル ポート リダイレクトのグループ ポリシー設定の構成](#)を参照してください。

リダイレクトされた COM ポートがリモート デスクトップ上で開かれ使用されると、ローカル コンピュータ上のポートにアクセスすることはできません。逆に、COM ポートがローカル コンピュータ上で使用されているときは、リモート デスクトップのポートにはアクセスできません。

シリアル ポート リダイレクトの要件

この機能を使用するとユーザーは、内蔵の RS232 ポートまたは USB シリアル アダプタなど、ローカルに接続されたシリアル (COM) ポートをリモート デスクトップにリダイレクトできます。シリアル ポート リダイレクトをサポートするには、View の展開が特定のソフトウェアおよびハードウェア要件を満たす必要があります。

View リモート デスクトップ

親またはテンプレート仮想マシン上のリモート デスクトップには、View Agent 6.1.1 以降または Horizon Agent 7.0 以降をインストールし、シリアル ポート リダイレクト設定オプションを設定する必要があります。デフォルトではこの設定オプションは選択解除されています。

次のゲスト OS は単一ユーザーの仮想マシンでサポートされています。

- 32 ビットまたは 64 ビットの Windows 7
- 32 ビットまたは 64 ビットの Windows 8.x
- 32 ビットまたは 64 ビットの Windows 10
- デスクトップとして構成されている Windows Server 2008 R2
- デスクトップとして構成されている Windows Server 2012 R2

この機能は Windows Server RDS ホスト向けには現在サポートされていません。

エージェントがインストールされているデスクトップ オペレーティング システムにシリアル ポート デバイス ドライバをインストールする必要はありません。

Horizon Client コンピュータまたはクライアント アクセス デバイス

- シリアル ポート リダイレクトは、Windows 7、Windows 8.x クライアント システム、および Windows 10 でサポートされています。
- 必要なシリアル ポート デバイス ドライバをすべてインストールする必要があります。シリアル ポートがクライアント コンピュータ上で操作可能である必要があります。エージェントがインストールされているリモート デスクトップのオペレーティング システムにデバイス ドライバをインストールする必要はありません。

View 用の表示プロトコル

- PCoIP
- VMware Blast Extreme (Horizon Agent 7.0 以降が必要)

VMware Horizon シリアル ポート リダイレクトは、RDP デスクトップ セッションでサポートされません。

シリアル ポート リダイレクトのユーザー操作

ユーザーは、クライアント コンピュータに接続された物理 COM ポート デバイスを操作でき、シリアル ポートの仮想化を使用して、デバイスをリモート デスクトップに接続できます。デバイスはここでサード パーティ アプリケーションにアクセスできます。

- Horizon Agent を使用してシリアル ポート リダイレクト オプションをインストールした後、シリアル ポート ツールトレイ アイコン (🔌) がリモート デスクトップに追加されます。

このアイコンは、必要なバージョンの Horizon Agent と Windows 版 Horizon Client を使用し、PCoIP を介して接続している場合に表示されます。Mac、Linux、モバイル クライアントからリモート デスクトップに接続している場合、アイコンは表示されません。

アイコンを使用して、マップされた COM ポートの接続、切断、カスタマイズを行うためのオプションを構成できます。

- シリアル ポート アイコンをクリックすると、[VMware Horizon のシリアル COM リダイレクト] メニューが表示されます。
- デフォルトではローカルに接続された COM ポートは、リモート デスクトップ上の対応する COM ポートにマップされます。たとえば、[COM1 は COM3 にマップされます]。マップされたポートはデフォルトでは接続されません。
- マップされた COM ポートを使用するには、[VMware Horizon のシリアル COM リダイレクト]メニューで手動で[接続]オプションを選択するか、以前のデスクトップ セッション時、またはグループ ポリシー設定の構成で、[自動接続]オプションを選択しておく必要があります。[自動接続]は、リモート デスクトップ セッション開始時に、マップされたポートを自動で接続するよう構成します。
- [接続]オプションを選択すると、リダイレクトされたポートはアクティブになります。リモート デスクトップ上のゲスト オペレーティング システムの [デバイス マネージャ] で、リダイレクトされたポートは [VMware Horizon のシリアル ポート リダイレクタ (COMn)] として表示されます。

COM ポートが接続されると、サードパーティ アプリケーションでポートを開くことができ、これによってクライアント マシンに接続された COM ポート デバイスとデータを交換できます。アプリケーションでポートが開いているときは、[VMware Horizon のシリアル COM リダイレクト] メニューのポートは切断できません。

COM ポートを切断するには、その前に、アプリケーションのポートを閉じるか、アプリケーションを閉じる必要があります。その後、[切断] オプションを選択してポートを切断し、物理 COM ポートをクライアント マシンでできるようにできます。

- [VMware Horizon のシリアル COM リダイレクト] メニューで、リダイレクトされたポートを右クリックすると、[Port Properties] コマンドを選択できます。

[COM プロパティ] ダイアログ ボックスで、ポートがリモート デスクトップ セッション開始時に自動的に接続したり、[データ セット準備完了 (DSR)] 信号を無視したりするよう構成でき、また、[カスタム ポート名] ドロップダウン リストでポートを選択して、クライアントのローカル ポートがリモート デスクトップ上の異なる COM ポートにマップされるよう構成できます。

リモート デスクトップ ポートは重複して表示されることがあります。たとえば、[COM1 (重複)] のように見えることがあります。この場合、仮想マシンは ESXi ホスト上の仮想ハードウェアの COM ポートで構成されます。仮想マシン上で重複するポートにマップされている場合でも、リダイレクトされたポートを使用できます。仮想マシンは ESXi ホストを介して、またはクライアント システムから、シリアル データを受信します。

- ゲスト オペレーティング システムの [デバイス マネージャ] で、[プロパティ] - [ポートの設定] タブを使用して、リダイレクトされた COM ポートの設定を構成できます。たとえば、デフォルトのボーレートとデータビットを設定できます。ただしアプリケーションがポートの設定を指定した場合、[デバイス マネージャ] で構成した設定は無視されます。

エンド ユーザーがリダイレクトされるシリアル COM ポートを操作する手順については、『Windows 版 VMware Horizon Client の使用』を参照してください。

シリアル ポート リダイレクトの構成に関するガイドライン

グループ ポリシーの設定を使用してシリアル ポート リダイレクトを構成し、リダイレクトされた COM ポートをユーザーがどの程度カスタマイズできるかを制御できます。選択肢は社内のユーザーのロールとサードパーティ アプリケーションによって異なります。

グループ ポリシー設定の詳細については、[シリアル ポート リダイレクトのグループ ポリシー設定](#)を参照してください。

- ユーザーが同じサードパーティ アプリケーションと COM ポート デバイスを使用している場合は、リダイレクトされたポートが同じように構成されていることを確認します。たとえば、POS（販売時点情報管理）デバイスを使用する銀行や小売店では、すべての COM ポート デバイスがクライアント エンドポイントの同じポートに接続され、すべてのポートがリモート デスクトップ上の同じリダイレクトされた COM ポートにマップされていることを確認してください。

クライアント ポートをリダイレクトされたポートへマップするには、[PortSettings] ポリシー設定を設定します。各デスクトップ セッションの開始時に、[PortSettings] の [自動接続] の項目を選択し、リダイレクトされたポートが接続されていることを確認してください。ユーザーがポート マッピングを変更したり、ポートの構成をカスタマイズできないようにするには、[構成のロック] ポリシー設定を有効にします。このシナリオでは、ユーザーは手動で接続や切断を行う必要がなく、ユーザーが誤ってリダイレクトされた COM ポートがサードパーティ アプリケーションにアクセスできないようにしてしまうことを防ぎます。

- ユーザーが各種のサードパーティ アプリケーションを使用するナレッジ ワーカーで、クライアント マシンでローカルに COM ポートを使用する可能性がある場合、ユーザーがリダイレクトされた COM ポートから接続および切断を行えるようにする必要があります。

デフォルトのポート マッピングが間違っている場合は、[PortSettings] ポリシー設定を設定できます。ユーザーの要件に応じて、[自動接続] の項目を設定する場合としない場合があります。[構成のロック] ポリシー設定は有効にしません。

- サードパーティ アプリケーションがリモート デスクトップにマップされている COM ポートを開くことを確認します。
- デバイスに使用中のポーレートがサードパーティ アプリケーションが使用しようとしているポーレートと一致することを確認します。
- クライアント システムからリモート デスクトップへ最大 5 個の COM ポートをリダイレクトできます。

シリアル ポート リダイレクトのグループ ポリシー設定の構成

リモート デスクトップでのシリアル ポート リダイレクトの動作を制御するグループ ポリシー設定を構成できます。これらのポリシー設定を使用して、ユーザのデスクトップの [[VMware Horizon のシリアル COM リダイレクト]] メニューで使用するオプションを、一元的に Active Directory から制御できます。

これらのポリシー設定を構成する必要はありません。シリアル ポート リダイレクトは、リモート デスクトップやクライアント システム上のリダイレクトされた COM ポート用に構成されたデフォルトの設定で機能します。

このポリシー設定はユーザーのリモート デスクトップに影響し、物理 COM ポート デバイスが接続されたクライアント システムには影響しません。これらの設定をデスクトップで構成するには、Active Directory にシリアル ポート リダイレクト グループ ポリシー管理テンプレート (ADM) ファイルを追加します。

シリアル ポート リダイレクト ADM テンプレートを Active Directory に追加する

シリアル ポート リダイレクト ADM ファイル、vdm_agent_serialport.adm のポリシー設定を Active Directory のグループ ポリシー オブジェクト (GPO) に追加し、グループ ポリシー オブジェクト エディタで設定を構成することができます。

前提条件

- デスクトップにシリアル ポート リダイレクト設定オプションがインストールされていることを確認します。シリアル ポート リダイレクトがインストールされていないと、グループ ポリシー設定は有効になりません。[仮想マシンへの Horizon Agent のインストール](#)を参照してください。
- シリアル ポート リダイレクトのグループ ポリシー設定用に Active Directory GPO が作成されていることを確認します。GPO は、デスクトップを含む OU にリンクする必要があります。[Active Directory グループ ポリシーの例](#)を参照してください。
- MMC およびグループ ポリシー オブジェクト エディタ スナップインが Active Directory サーバで使用できることを確認します。
- シリアル ポート リダイレクトのグループ ポリシー設定について理解しておきます。[シリアル ポート リダイレクトのグループ ポリシー設定](#)を参照してください。

手順

- 1 View GPO Bundle .zip ファイルを <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 GPO Bundle が含まれます。

ファイル名は VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip で、x.x.x はバージョン、yyyyyyy はビルド番号を表します。View のグループ ポリシー設定用の ADM ファイルと ADMX ファイルはすべて、このファイルで提供されています。

- 2 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip ファイルを解凍して、シリアル ポート リダイレクト ADM ファイル vdm_agent_serialport.adm を Active Directory サーバにコピーします。
- 3 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 GPO を編集します。
- 4 グループ ポリシー オブジェクト エディタで、[コンピュータの構成] - [管理テンプレート] フォルダを右クリックして、[テンプレートの追加と削除] を選択します。
- 5 [追加] をクリックして、vdm_agent_serialport.adm ファイルを参照し、[開く] をクリックします。
- 6 [閉じる] をクリックして ADM ファイルのポリシ設定を GPO に適用します。

この設定は、[コンピュータの構成] - [ポリシー] - [管理テンプレート] - [従来の管理テンプレート] - [VMware View Agent の構成] - [シリアル COM] フォルダ内にあります。

ほとんどの設定も、[ユーザー構成] - [ポリシー] - [管理テンプレート] - [従来の管理テンプレート] - [VMware View Agent の構成] - [シリアル COM] 内の [ユーザー構成] フォルダに追加されます。

- 7 シリアル ポート リダイレクトのグループ ポリシー設定を構成します。

シリアル ポート リダイレクトのグループ ポリシー設定

シリアル ポート リダイレクトのグループ ポリシー設定は、リダイレクトされた COM ポートの構成を制御します。これにはリモート デスクトップの [VMware Horizon のシリアル COM リダイレクト] メニューで利用できるオプションが含まれます。

シリアル ポート リダイレクト ADM ファイルには、コンピュータの構成とユーザーの構成の両方のポリシーが含まれます。ユーザーの構成ポリシーによって、VDI デスクトップの指定されたユーザに異なる構成を設定できます。コンピュータの構成で構成されたポリシー設定は、ユーザーの構成で構成された対応する設定よりも優先されます。

グループ ポリシー設定	説明
PortSettings	<p>クライアント システム上の COM ポートと、リモート デスクトップ上のリダイレクトされた COM ポートの間のマッピングを決定し、リダイレクトされた COM ポートに影響する他の設定を決定します。</p> <p>リダイレクトされた 各 COM ポートを個別に構成します。[PortSettings1] から [PortSettings5] まで、5 個の [PortSettings] ポリシー設定を利用でき、最大 5 個の COM ポートをクライアントからリモート デスクトップにマップできます。構成する各 COM ポートの [PortSettings] ポリシー設定を 1 つ選択します。</p> <p>[PortSettings] ポリシー設定を有効にすると、リダイレクトされた COM ポートに影響する以下の項目を構成できます。</p> <ul style="list-style-type: none"> ■ [ソース ポート番号]の設定は、クライアント システムに接続される物理 COM ポートの数を指定します。 ■ [ターゲット仮想ポート番号]の設定は、リモート デスクトップ上のリダイレクトされた仮想 COM ポートの数を指定します。 ■ [自動接続]の設定は各デスクトップ セッションの開始時に、COM ポートをリダイレクトされた COM ポートに自動的に接続します。 ■ [IgnoreDSR] の設定では、リダイレクトされた COM ポート デバイスは [データセットの準備完了 (DSR)] 信号を無視します。 ■ [ポートを閉じる前に停止 (ミリ秒)]の設定は、ユーザーがリダイレクトされたポートを閉じた後と、ポートが実際に閉じる前に待機する時間 (ミリ秒) を指定します。特定の USB シリアル アダプタでは、転送されたデータが確実に保持するために、この遅延を必要とします。この設定はトラブルシューティングを目的としています。 ■ [Serial2USBModeChangeEnabled] の設定は、GlobalSat BU353 GPS アダプタを含め、Prolific チップセットを使用する USB シリアル アダプタに該当する問題を解決します。Prolific チップセット アダプタ用のこの設定を有効にしない場合、接続したデバイスはデータを転送できますが、データを受信することはできません。 ■ [待機マスクのエラーの無効化]の設定は、COM ポート マスクのエラー値を無効にします。このトラブルシューティング設定は特定のアプリケーション向けに必要です。詳細については、http://msdn.microsoft.com/en-us/library/windows/desktop/aa363479(v=vs.85).aspx の WaitCommEvent 機能に関する Microsoft の文書を参照してください。 ■ [HandleBtDisappear] の設定は BlueTooth COM ポートの動作をサポートします。この設定はトラブルシューティングを目的としています。 ■ [UsbToComTroubleShooting] の設定は USB シリアル ポート アダプタに該当する一部の問題を解決します。この設定はトラブルシューティングを目的としています。 <p>特定の COM ポートの [PortSettings] の設定を有効にすると、ユーザーはリダイレクトされたポートを接続したり切断したりできますが、リモート デスクトップ上のポートのプロパティを構成することはできません。たとえば、ユーザーはデスクトップへのログイン時にポートが自動的にリダイレクトされるように設定することはできません。また、DSR 信号は無視できません。これらのプロパティはグループ ポリシー設定によって制御されます。</p>
	<p>注: リダイレクトされた COM ポートは物理 COM ポートがローカルでクライアント システムに接続されている場合のみ接続されアクティブになります。クライアントに存在しない COM ポートをマップする場合、リダイレクトされたポートは非アクティブの表示になり、リモート デスクトップ上のツール トレイ メニューでは使用できません。</p>
	<p>[PortSettings] 設定が無効になっているか構成されていない場合、リダイレクトされた COM ポートはユーザーがリモート デスクトップ上で構成した設定を使用します。[VMware Horizon のシリアル COM リダイレクト] メニュー オプションはアクティブでユーザーが使用できます。</p>
	<p>この設定は、コンピュータの構成ポリシーおよびユーザーの構成ポリシーとして使用できます。</p>
ローカル設定の優先	<p>リモート デスクトップ上で構成された設定を優先します。</p> <p>このポリシーを有効にすると、ユーザーがリモート デスクトップで構成するシリアル ポート リダイレクト設定が、グループ ポリシー設定よりも優先されます。グループ ポリシー設定は、設定がリモート デスクトップで構成されていない場合のみ有効になります。</p> <p>この設定が無効になっているか構成されていない場合は、リモート デスクトップ上で構成された設定よりも、グループ ポリシー設定が優先されます。</p> <p>この設定は、コンピュータの構成ポリシーおよびユーザーの構成ポリシーとして使用できます。</p>

グループ ポリシー設定	説明
機能を無効にする	<p>シリアル ポート リダイレクト機能を無効にします。</p> <p>この設定を有効にすると、COM ポートはリモート デスクトップにリダイレクトされません。リモート デスクトップ上のシリアル ポート ツールトレイ アイコンも表示されません。</p> <p>この設定が無効になっている場合、シリアル ポート リダイレクトは機能し、シリアル ポート ツールトレイ アイコンが表示され、[VMware Horizon のシリアル COM リダイレクト] メニューに COM ポートが表示されます。</p> <p>この設定が構成されていない場合、リモート デスクトップへのローカルの設定によって、シリアル ポート リダイレクトが無効か有効かが決まります。</p> <p>この設定は、コンピュータの構成ポリシーとしてのみ使用できます。</p>
ロックの構成	<p>シリアル ポート リダイレクトのユーザー インターフェイスをロックし、ユーザーがリモート デスクトップの構成オプションを変更するのを防止します。</p> <p>この設定を有効にすると、ユーザーはデスクトップのツールトレイ メニューから使用できるオプションを構成できません。ユーザーは [VMware Horizon のシリアル COM リダイレクト] メニューを表示できますが、オプションは非アクティブで変更はできません。</p> <p>この設定が無効になっている場合、ユーザーは [VMware Horizon のシリアル COM リダイレクト] メニューのオプションを設定できます。</p> <p>この設定が構成されていない場合、リモート デスクトップのローカル プログラムの設定によって、ユーザーが COM ポート リダイレクト設定を構成できるかどうかが決まります。</p>
帯域幅の限界	<p>データ転送速度の限界を、リダイレクトされたシリアル ポートとクライアント システムの間の 1 秒あたりのキロバイト数で設定します。</p> <p>この設定を有効にすると、リダイレクトされたシリアル ポートとクライアントの間の最大データ転送速度を決定する[帯域幅の限界 (キロバイト/秒)] ボックスの値を設定できます。値「0」は帯域幅制限を無効にします。</p> <p>この設定が無効になっている場合、帯域幅の限界は設定されていません。</p> <p>この設定が構成されていない場合、リモート デスクトップのローカル プログラムの設定によって、帯域幅の限界が設定されるかどうか決定します。</p> <p>この設定は、コンピュータの構成ポリシーとしてのみ使用できます。</p>

USB シリアル アダプタの構成

シリアル ポート リダイレクト機能によって、Prolific チップセットを使用する USB シリアル アダプタを、リモート デスクトップにリダイレクトするように構成することができます。

Prolific チップセット アダプタでデータの適切な転送を確実に行うには、Active Directory または個別のデスクトップ仮想マシンのシリアル ポート リダイレクト グループ ポリシー設定を有効にします。

Prolific チップセット アダプタの問題を解決するようグループ ポリシー設定を構成しない場合、接続されたデバイスはデータを転送できますが、データを受信することはできません。

クライアント システムのポリシー設定またはレジストリ キーは構成する必要はありません。

前提条件

- デスクトップにシリアル ポート リダイレクト設定オプションがインストールされていることを確認します。シリアル ポート リダイレクトがインストールされていないと、グループ ポリシー設定は有効になりません。[仮想マシンへの Horizon Agent のインストール](#)を参照してください。
- シリアル ポート リダイレクト ADM ファイルが Active Directory またはデスクトップ仮想マシンに追加されていることを確認します。[シリアル ポート リダイレクト ADM テンプレートを Active Directory に追加する](#)を参照してください。

- [PortSettings] グループ ポリシー設定の [Serial2USBModeChangeEnabled] の項目について理解しておきます。 [シリアル ポート リダイレクトのグループ ポリシー設定](#)を参照してください。

手順

- 1 Active Directory または仮想マシン上で、[グループ ポリシー オブジェクト エディタ] を開きます。
- 2 [コンピュータの構成] - [ポリシー] - [管理テンプレート] - [従来の管理テンプレート] - [VMware View Agent の構成] - [シリアル COM] フォルダの順に移動します。
- 3 [PortSettings] フォルダを選択します。
- 4 [PortSettings] グループ ポリシー設定を選択し有効にします。
- 5 COM ポートをマップするための、ソースおよびターゲットの COM ポート番号を指定します。
- 6 [Serial2USBModeChangeEnabled] チェックボックスを選択します。
- 7 必要に応じて [PortSettings] ポリシー設定の他の項目を構成します。
- 8 [OK] をクリックし、グループ ポリシー オブジェクト エディタを閉じます。

ユーザーが次のデスクトップ セッションを開始すると、USB シリアル アダプタはリモート デスクトップにリダイレクトでき、データを正常に受信できます。

Windows Media マルチメディア リダイレクト (MMR) へのアクセスの管理

View は、単一ユーザーのマシンで実行される VDI デスクトップと、RDS デスクトップ向けの Windows Media MMR 機能を提供します。

MMR は、マルチメディア ストリームをクライアント コンピュータに直接提供します。MMR を使用すると、クライアント システムでマルチメディア ストリームが処理（デコード）されます。クライアント システムはメディア コンテンツを再生し、それによって ESXi ホストの要求を開放します。

MMR データはアプリケーション ベースの暗号化なしにネットワーク経由で送信されますが、リダイレクトされるコンテンツによっては、機密データが含まれていることもあります。このデータがネットワークで盗まれないことを保証するには、セキュア ネットワークで MMR だけを使用してください。

安全なトンネルが有効になっている場合、Horizon Clients と View Secure Gateway の間の MMR 接続は保護されますが、View Secure Gateway からデスクトップ マシンへの接続は暗号化されません。安全なトンネルが無効になっている場合、Horizon Clients からデスクトップ マシンへの MMR 接続は暗号化されません。

View でのマルチメディア リダイレクトの有効化

以下の手順によって、MMR がアクセス可能であるのは、ローカル マルチメディア デコーディングを処理するための十分なリソースを持ち、セキュア ネットワークの View に接続されている Horizon Client システムのみであることを確認できます。

デフォルトでは、View Administrator のグローバル ポリシーで、[マルチメディア リダイレクト (MMR)] は [拒否] に設定されています。

MMR を使用するには、この値を明示的に [許可] に設定する必要があります。

MMR へのアクセスを制御するには、個別のデスクトップ プール、または特定のユーザーに対してグローバルに [マルチメディア リダイレクト (MMR)] ポリシーを有効または無効にします。

View Administrator でグローバル ポリシーを設定するための手順については、[View ポリシー](#)を参照してください。

Windows Media MMR のシステム要件

Windows Media マルチメディア リダイレクト (MMR) をサポートするには、View の展開が特定のソフトウェアおよびハードウェア要件を満たす必要があります。Windows Media MMR は、Horizon 6.0.2 以降のリリースで提供されます。

View リモート デスクトップ

- この機能は、単一ユーザーの仮想マシンにデプロイされた VDI デスクトップと、RDS デスクトップでサポートされます。

RDS デスクトップでこの機能をサポートするには、View Agent 6.1.1 以降が必要です。

単一ユーザーのマシンでこの機能をサポートするには、View Agent 6.0.2 以降が必要です。
- 次のゲスト OS がサポートされています。
 - 64 ビットまたは 32 ビットの Windows 10。Windows Media Player がサポートされます。デフォルトの TV および動画プレーヤーはサポートされません。
 - Windows Server 2016 は、技術プレビュー機能です。Windows Media Player がサポートされます。デフォルトの TV および動画プレーヤーはサポートされません。
 - 64 ビットまたは 32 ビット Windows 7 SP1 Enterprise または Ultimate (単一ユーザーのマシン) Windows 7 Professional はサポートされません。
 - 64 ビットまたは 32 ビットの Windows 8/8.1 Professional または Enterprise (単一ユーザーのマシン)
 - RDS ホストとして構成されている Windows Server 2008 R2
 - RDS ホストとして構成されている Windows Server 2012 および 2012 R2
- [3D レンダリング] はデスクトップ プールで有効または無効にできます。
- ユーザーは Windows Media Player 12 以降または Internet Explorer 8 以降でビデオを再生する必要があります。

Internet Explorer を使用するには、保護モードを無効にする必要があります。
[インターネット オプション] ダイアログ ボックスで、[セキュリティ] タブをクリックし、[保護モードを有効にする] をオフにします。

Horizon Client ソフトウェア	単一ユーザーのマシンで Windows Media MMR をサポートするには、Horizon Client 3.2 for Windows 以降のリリースが必要です。
Horizon Client コンピュータまたはクライアント アクセス デバイス	<ul style="list-style-type: none"> クライアントは、64 ビットまたは 32 ビットの Windows 7、Windows 8/8.1、または Windows 10 オペレーティング システムで実行する必要があります。
サポートされるメディア フォーマット	Windows Media Player でサポートされるメディア フォーマットがサポートされます。たとえば、M4V、MOV、MP4、WMP、MPEG-4 Part 2、WMV 7/8/9、WMA、AVI、ACE、MP3、WAV などです。
<p>注: DRM で保護されたコンテンツは、Windows Media MMR 経由でリダイレクトされません。</p>	
View ポリシー	View Administrator で、[マルチメディア リダイレクト (MMR)] ポリシーを [許可] に設定します。デフォルト値は [拒否] です。
バックエンド ファイアウォール	お使いの View で DMZ ベースのセキュリティ サーバと社内ネットワークの間にバックエンド ファイアウォールが置かれている場合は、バックエンド ファイアウォールがお使いのデスクトップのポート 9427 へのトラフィックを許可していることを確認します。

ネットワーク遅延に基づく Windows Media MMR の使用の決定

デフォルトでは、Windows Media MMR は、Windows 8 以降上で実行されている単一ユーザーのデスクトップ、あるいは Windows Server 2012 か 2012 R2 以降で実行されている RDS デスクトップのネットワーク状態に適応します。Horizon Client とリモート デスクトップの間のネットワーク遅延が 29 ミリ秒以下の場合、ビデオは Windows Media MMR を使用してリダイレクトされます。ネットワーク遅延が 30 ミリ秒以上の場合、ビデオはリダイレクトされません。代わりに、ビデオは ESXi ホストでレンダリングされ、PCoIP を介してクライアントに送信されます。

この機能は Windows 8 以降の単一ユーザー デスクトップと、Windows Server 2012 または 2012 R2 以降の RDS デスクトップに適用されます。ユーザーはサポートされているクライアント システム、Windows 7、または Windows 8/8.1 を実行できます。

この機能は Windows 7 単一ユーザー デスクトップまたは Windows Server 2008 R2 RDS デスクトップには適用されません。これらのゲスト オペレーティング システムで、Windows Media MMR はネットワーク遅延と関わりなく常にマルチメディア リダイレクトを実行します。

デスクトップ上で `RedirectionPolicy` レジストリ設定を構成して、ネットワーク遅延に関係なく Windows Media MMR がマルチメディア リダイレクトを実行するように強制することで、この機能を上書きできます。

手順

- 1 リモート デスクトップで Windows レジストリ エディタを起動します。
- 2 リダイレクト ポリシーを制御する Windows レジストリ キーに移動します。

リモート デスクトップで構成するレジストリ キーは、Windows Media Player のバージョンが何ビット版かによって異なります。

オプション	説明
64 ビット版 Windows Media Player	<ul style="list-style-type: none"> ■ 64 ビット版デスクトップの場合、レジストリ キー: HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware tsmmr を使用します。
32 ビット版 Windows Media Player	<ul style="list-style-type: none"> ■ 32 ビット版デスクトップの場合、レジストリ キー: HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware tsmmr を使用します。 ■ 64 ビット版デスクトップの場合、レジストリ キー: HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware, Inc.\VMware tsmmr を使用します。

- 3 RedirectionPolicy の値を always に設定します。

```
Value name = RedirectionPolicy
Value Type = REG_SZ
Value data = always
```

- 4 Windows Media Player をデスクトップで再起動して、更新した値を有効にします。

クライアント ドライブ リダイレクトへのアクセスの管理

Horizon Client 3.5 以降と View Agent 6.2 以降またはクライアント ドライブ リダイレクト機能を実装する Horizon Agent 7.0 以降をデプロイすると、フォルダとファイルは暗号化されネットワークを介して送信されます。クライアントと View Secure Gateway 間のクライアント ドライブ リダイレクト接続と、View Secure Gateway からデスクトップ マシンへの接続の安全性は確保されています。

Horizon Client 4.2 または Horizon 7 バージョン 7.0.2 以降の場合、VMware Blast Extreme が有効になっていると、ファイルとフォルダは暗号化されて仮想チャネル間で転送されます。

以前のクライアントやエージェント リリースでは、クライアント ドライブ リダイレクトではフォルダとファイルは暗号化されずにネットワークを介して送信されており、リダイレクトされるコンテンツに、機密データが含まれる場合があります。安全なトンネルを有効にすると、Horizon Client と View Secure Gateway のクライアント ドライブ リダイレクト接続は保護されますが、View Secure Gateway からデスクトップ マシンへの接続は暗号化されません。安全なトンネルを無効にすると、Horizon Client からデスクトップ マシンへのクライアント ドライブ リダイレクト接続は暗号化されません。バージョン 3.5 よりも前の Horizon Client やバージョン 6.2 より前のエージェントを使用している場合、このデータをネットワークで監視できないようにするために、安全なネットワークでのみクライアント ドライブ リダイレクトを使用します。

エージェント インストーラの [クライアント ドライブのリダイレクト] 設定オプションは、デフォルトで選択されています。ベスト プラクティスとして、[クライアント ドライブのリダイレクト] 設定オプションは、ユーザーがこの機能を必要とするデスクトップ プールでのみ有効にします。

グループ ポリシーを使用したクライアント ドライブ リダイレクトの無効化

Active Directory 内のリモート デスクトップおよび RDS ホストで Microsoft リモート デスクトップ サービスのグループ ポリシー設定を構成して、クライアント ドライブ リダイレクトを無効にできます。

クライアント ドライブ リダイレクトの詳細については、特定のタイプのデスクトップ クライアント デバイスに関する『VMware Horizon Client の使用』ドキュメントを参照してください。 https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html をご覧ください。

注: この設定により、クライアント ドライブ リダイレクト機能を有効にするローカル レジストリおよび スマート ポリシー 設定がオーバーライドされます。

前提条件

お使いの View デプロイで DMZ ベースのセキュリティ サーバと社内ネットワークの間にバックエンド ファイアウォールが置かれている場合は、バックエンド ファイアウォールがお使いの単一ユーザーおよび RDS デスクトップのポート 9427 へのトラフィックを許可していることを確認します。クライアント ドライブ リダイレクトをサポートするには、ポート 9427 での TCP 接続が必要です。

Horizon Client 4.2 または Horizon 7 バージョン 7.0.2 以降では、クライアント ドライブ リダイレクトによって仮想チャネルを介してデータが転送されるため、VMware Blast Extreme が有効になっている場合、ポート 9427 を開く必要はありません。

手順

- 1 グループ ポリシー 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\Windows コンポーネント\リモート デスクトップ サービス\リモート デスクトップ セッション ホスト\デバイスとリソースのリダイレクト]の順に移動します。

これは、Windows Server 2012 の Active Directory におけるナビゲーションパスです。他の Windows オペレーティング システムではナビゲーション パスは異なります。

- 2 [ドライブ リダイレクトを許可しない] グループ ポリシー設定を有効にします。

レジストリ設定を使用したクライアント ドライブ リダイレクトの構成

Windows レジストリ キー設定を使用して、リモート デスクトップでのクライアント ドライブ リダイレクトの動作を制御できます。この機能には Horizon Agent 7.0 以降および Horizon Client 4.0 以降が必要です。

リモート デスクトップでのクライアント ドライブ リダイレクトの動作を制御する Windows レジストリ設定は、次のパスにあります。

```
HKLM\Software\VMware, Inc.\VMware TSDR
```

リモート デスクトップで Windows レジストリ エディタを使用して、ローカル レジストリ設定を編集できます。

注: スマート ポリシー で設定されたクライアント ドライブ リダイレクト ポリシーは、ローカル レジストリ設定よりも優先されます。

クライアント ドライブ リダイレクトの無効化

クライアント ドライブ リダイレクトを無効にするには、`disabled` という新しい文字列値を作成し、その値を `true` に設定します。

```
HKLM\Software\VMware, Inc.\VMware TSDR\disabled=true
```

デフォルトでは、この値は `false`（有効）になっています。

共有フォルダへの書き込みアクセスの防止

リモート デスクトップと共有されるすべてのフォルダへの書き込みアクセスを防止するには、`permissions` という新しい文字列値を作成し、その値を `rw` 以外の `r` で始まる任意の文字列に設定します。

```
HKLM\Software\VMware, Inc.\VMware TSDR\permissions=r
```

デフォルトでは、この値は `rw`（すべての共有フォルダが読み取り可能で書き込み可能）になっています。

特定のフォルダの共有

特定のフォルダをリモート デスクトップと共有するには、`default shares` という新しいキーを作成し、リモート デスクトップと共有する各フォルダに対して新しいサブキーを作成します。各サブキーで、`name` という新しい文字列値を作成し、その値を共有するフォルダのパスに設定します。次の例では、フォルダ `C:\ebooks` と `C:\spreadsheets` を共有しています。

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f1\name=C:\ebooks
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f2\name=C:\spreadsheets
```

`name` を `*all` に設定すると、すべてのクライアント ドライブがリモート デスクトップと共有されます。`*all` 設定は、Windows クライアント システムでのみサポートされています。

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\1st\name=*all
```

クライアントの他のフォルダ（`default shares` キーで指定されていないフォルダ）が共有されることを防止するには、`ForcedByAdmin` という文字列値を作成し、その値を `true` に設定します。

```
HKLM\Software\VMware, Inc.\VMware TSDR\ForcedByAdmin=true
```

値が `true` の場合、Horizon Client でユーザーがリモート デスクトップに接続したときに [共有] ダイアログ ボックスは表示されません。デフォルトでは、この値は `false`（クライアントの他のフォルダを共有可能）になっています。

次の例では、フォルダ `C:\ebooks` と `C:\spreadsheets` を共有して両方のフォルダを読み取り専用にし、クライアントの他のフォルダが共有されることを防止しています。

```
HKLM\Software\VMware, Inc.\VMware TSDR\ForcedByAdmin=true
HKLM\Software\VMware, Inc.\VMware TSDR\permissions=r
```

```
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f1\name=C:\ebooks
HKLM\Software\VMware, Inc.\VMware TSDR\default shares\f2\name=C:\spreadsheets
```

注: セキュリティ機能または共有制御として、`ForcedByAdmin` 機能を使用しないでください。ユーザーは、既存の共有へのリンクを作成することにより、`ForcedByAdmin=true` 設定をする必要がありません。既存の共有は、`default shares` キーで指定されていないフォルダを指定します。

コピーおよび貼り付け操作におけるクリップボードのデータ形式の制限

PCoIP および VMware Blast セッションでユーザーがデータをコピーおよび貼り付けるときに許可するクリップボードのデータ形式を制御するグループ ポリシー設定を構成できます。セキュリティ上の理由でコピーおよび貼り付け操作を制限する必要がある場合に、この機能が役立ちます。

コピーおよび貼り付け操作の方向を基準にしてクリップボードのデータ形式の制限を構成できます。たとえば、クライアント システムからリモート システムにコピーされるデータについてあるポリシー セットを構成し、リモート デスクトップからクライアント システムにコピーするデータに別のポリシー セットを構成できます。

PCoIP セッションについては、クリップボード コンテンツをフィルタするグループ ポリシー設定は PCoIP グループ ポリシー テンプレート ファイル `pcoip.adm` にあります。詳細は、[PCoIP クリップボードの設定](#)を参照してください。VMware Blast セッションについては、クリップボード コンテンツをフィルタするグループ ポリシー設定は VMware Blast グループ ポリシー テンプレート ファイル `vdm_blast.adm` ファイルにあります。[VMware Blast ポリシー設定](#)を参照してください。これらのグループ ポリシー設定は、Horizon Agent のみに適用され、バージョン 7.0.2 以降のみが対象になります。

クリップボードのデータ形式フィルタの例

次の例は、コピーおよび貼り付け操作時にクリップボードのデータ形式をフィルタするグループ ポリシー設定をどのように使用できるかを示しています。

- ユーザーがクライアント システムからリモート デスクトップに送信されるデータをコピーするときに、Wordpad など、Microsoft Office アプリケーション以外のイメージを取り除くには、`Filter images out of the incoming clipboard data` グループ ポリシー設定を有効にします。
- ユーザーがクライアント システムからリモート デスクトップに送信されるデータをコピーするときに、Microsoft Office 以外のアプリケーションと Microsoft Office アプリケーションの両方のイメージを取り除くには、`Filter Microsoft Chart and Smart Art data out of the incoming clipboard data` と `Filter images out of the incoming clipboard data` グループ ポリシー設定を有効にします。`Filter Microsoft Chart and Smart Art data out of the incoming clipboard data` グループ ポリシー設定は、イメージが含まれる場合がある、Microsoft Office のチャートと Smart Art データを取り除きます。
- ユーザーがクライアント システムからリモート デスクトップに送信されるデータをコピーするときに、Microsoft Office のチャートと Smart Art データのみを取り除くには、`Filter Microsoft Chart and Smart Art data out of the incoming clipboard data` グループ ポリシー設定のみを有効にします。

- ユーザーがクライアント システムからリモート デスクトップに、そしてリモート デスクトップからクライアント システムに送信されるデータをコピーするときに、Microsoft Word に関連するテキスト形式を取り除くには、受信に関するグループ ポリシー設定の Filter Microsoft Text Effects data out of the incoming clipboard data と Filter Rich Text Format data out of the incoming clipboard data を有効にし、送信に関するグループ ポリシー設定の Filter Microsoft Text Effects data out of the outgoing clipboard data と Filter Rich Text Format data out of the outgoing clipboard data を有効にします。
- ユーザーがクライアント システムからリモート デスクトップに、そしてリモート デスクトップからクライアント システムに送信されるデータをコピーするときに、Microsoft Word のイメージを取り除くには、受信に関するグループ ポリシー設定 Filter Rich Text Format data out of the incoming clipboard data と送信に関するグループ ポリシー設定の Filter Rich Text Format data out of the outgoing clipboard data を有効にします。Microsoft Word のイメージは、複合的な RTF 形式で保存されます。

リモート デスクトップおよびアプリケーションでの USB デバイスの使用

15

管理者は、サム フラッシュ ドライブ、カメラ、VoIP (Voice over IP) デバイス、プリンタなどの USB デバイスをリモート デスクトップから使用できるように構成できます。この機能は USB リダイレクトと呼ばれ、Blast Extreme、PCoIP、または Microsoft RDP 表示プロトコルの使用をサポートします。リモート デスクトップでは、最大 128 個の USB デバイスに対応できます。

RDS デスクトップおよびアプリケーションで使用する場合、ローカルで接続された USB サム フラッシュ ドライブとハード ディスクをリダイレクトすることもできます。他のタイプのストレージ デバイスを含め、他のタイプの USB デバイスは RDS デスクトップおよびアプリケーションでサポートされていません。

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

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

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

USB リダイレクト機能は、一部のクライアントのタイプだけで使用できます。この機能が特定のタイプのクライアントでサポートされるかどうかを確認するには、デスクトップまたはモバイル クライアント デバイスのそれぞれのタイプに関する「VMware Horizon Client の使用」に含まれる機能サポート マトリックスを参照してください。
[https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html] をご覧ください。

重要: USB リダイレクト機能を展開すると、USB デバイスに影響を及ぼす可能性のあるセキュリティ上の脆弱性から組織を保護する措置を講じることができます。保護された View 環境での USB デバイスの展開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。

- [USB デバイス タイプに関する制限事項](#)

- [USB リダイレクトの設定の概要](#)
- [ネットワーク トラフィックと USB リダイレクト](#)
- [USB デバイスへの自動接続](#)
- [保護された View 環境での USB デバイスの展開](#)
- [ログ ファイルを使用してのトラブルシューティングと USB デバイス ID の確認](#)
- [USB リダイレクトを制御するポリシーの使用](#)
- [USB リダイレクトに関する問題のトラブルシューティング](#)

USB デバイス タイプに関する制限事項

リモート デスクトップにおけるデバイスの動作を View が明示的に阻止することはありませんが、ネットワークの遅延や帯域幅などの要因で、デバイスのパフォーマンスには差があります。デフォルトでは、使用されないように一部のデバイスがフィルタリングまたはブロックされます。

Horizon 6.0.1 を Horizon Client 3.1 以降と一緒に使用すると、Windows、Linux、および Mac クライアントのクライアント マシンで USB 3.0 デバイスを USB 3.0 ポートに接続できます。USB 3.0 デバイスは、単一ストリームのみでサポートされます。複数のストリームのサポートはこのリリースで実装されていないため、USB デバイスのパフォーマンスは強化されません。常に高いスループットを出さないと適切に動作しない一部の USB 3.0 デバイスの場合、ネットワークの待機時間によって VDI セッションで動作しない可能性があります。

以前の View のリリースでは、超高速 USB 3.0 デバイスはサポートされていませんが、USB 3.0 デバイスは多くの場合、クライアント マシンの USB 2.0 ポートに接続すると動作します。ただし、クライアント システムのマザーボードの USB チップセットのタイプによっては、動作しないことがあります。

次のタイプのデバイスは、シングル ユーザー マシンに展開されているリモート デスクトップへの USB リダイレクトに適さない可能性があります。

- Web カメラは、その帯域幅要件（通常 60Mbps を超える帯域幅を使用する）上の理由で、USB リダイレクトではサポートされません。Web カメラではリアルタイム オーディオ ビデオ機能を使用できます。
- USB オーディオ デバイスのリダイレクトは、ネットワークの状態に依存し、信頼できません。一部のデバイスでは、アイドル状態のときでさえ、高いデータ スループットが必要です。リアルタイム オーディオ ビデオ機能があれば、オーディオ入出力デバイスはこの機能を使用して問題なく動作します。それらのデバイス用に USB リダイレクトを使用する必要はありません。
- USB CD/DVD の焼き付けはサポートされていません。
- 一部の USB デバイスは、ネットワークの遅延や信頼性次第でパフォーマンスが大幅に変化します。特に、WAN 経由の場合、この変化が顕著です。たとえば、USB ストレージ デバイスの 1 回の読み取り要求では、クライアントとリモート デスクトップ間のラウンドトリップを 3 回必要とします。ファイル全体の読み取りは複数の USB 読み取り操作が必要になることもあり、遅延が大きくなるほど、ラウンドトリップにかかる時間が長くなります。

ファイル構造は、ファイル形式次第でかなり大きくなることがあります。大容量 USB ディスク ドライブは、デスクトップに表示されるまでに数分かかる場合があります。USB デバイスを FAT ではなく NTFS でフォーマットすると、最初の接続時間が短縮されます。信頼性の低いネットワーク リンクは再試行を引き起こし、パフォーマンスをさらに低下させます。

同様に、USB CD/DVD リーダー、スキャナ、署名付きタブレットなどのタッチ デバイスは、WAN などの速度の遅いネットワーク上では機能しません。

- USB スキャナのリダイレクトはネットワークの状態に左右されるため、スキャンの完了には通常より時間がかかることがあります。

RDS デスクトップまたはアプリケーションには、次のタイプのデバイスをリダイレクトできます。

- USB サム フラッシュ ドライブ
- USB ハード ディスク

Horizon 7 バージョン 7.0.2 では、署名パッド、ディクテーション用フット ペダル、さらにいくつかの Wacom タブレットを RDS デスクトップやアプリケーションにリダイレクトできます。デフォルトでは、これらのデバイスは無効になっています。これらのデバイスを有効にするには、Windows レジストリ キー設定 `ExcludeAllDevices` および `IncludeFamily` を `HKLM\Software\Policies\VMware, Inc\VMware VDM\Agent\USB` のパスから削除します。

その他のタイプの USB デバイスや、セキュリティ ストレージ ドライブや USB CD-ROM などのその他のタイプの USB ストレージ デバイスを RDS デスクトップやアプリケーションにリダイレクトすることはできません。

USB リダイレクトの設定の概要

エンド ユーザーが USB フラッシュ ドライブ、カメラ、ヘッドセットなどのリムーバブル デバイスに接続できるように展開を設定するには、リモート デスクトップまたは RDS ホストとクライアント デバイスの両方に特定のコンポーネントをインストールし、View Administrator で USB デバイスのグローバル設定が有効になっていることを確認する必要があります。

このチェックリストには、企業で USB リダイレクトを設定するための必須タスクとオプション タスクの両方が含まれます。

USB リダイレクト機能は、Windows クライアント、Mac クライアント、パートナー提供の Linux クライアントなど、一部のクライアント タイプのみで使用できます。この機能が特定タイプのクライアントでサポートされるかどうかを確認するには、特定タイプのクライアント デバイスに関する「VMware Horizon Client の使用」に含まれる機能サポート一覧を参照してください。[https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html] をご覧ください。

重要: USB リダイレクト機能を展開すると、USB デバイスに影響を及ぼす可能性のあるセキュリティ上の脆弱性から組織を保護する措置を講じることができます。たとえば、グループ ポリシー設定を使用して、一部のリモート デスクトップおよびユーザーに対して USB リダイレクトを無効にしたり、リダイレクトできる USB デバイスのタイプを制限したりすることができます。保護された View 環境での USB デバイスの展開を参照してください。

- 1 リモート デスクトップ ソースまたは RDS ホストで Horizon Agent インストール ウィザードを実行するときは、必ず USB リダイレクト コンポーネントを含めてください。

デフォルトでは、このコンポーネントが選択されていません。このコンポーネントを選択してインストールする必要があります。

- 2 クライアント システムで VMware Horizon Client インストール ウィザードを実行する際は、必ず USB リダイレクト コンポーネントを含めてください。

デフォルトでは、このコンポーネントは含まれています。

- 3 View Administrator で、リモート デスクトップまたはアプリケーションから USB デバイスへのアクセスが有効になっていることを確認します。

View Administrator で、[ポリシー] - [グローバル ポリシー] に移動し、[USB アクセス] が [許可] になっていることを確認します。

- 4 (オプション)リダイレクトを許可するデバイスのタイプを指定する Horizon Agent グループ ポリシーを構成します。

[USB リダイレクトを制御するポリシーの使用](#)を参照してください。

- 5 (オプション) クライアント デバイスで、同様の設定を構成します。

Horizon Client がリモート デスクトップまたはアプリケーションに接続するとき、またはエンド ユーザーが USB デバイスを接続するときに、デバイスが自動的に接続されるかどうかも構成できます。クライアント デバイスで USB 設定を構成する方法は、デバイスのタイプによって異なります。たとえば、Windows クライアント エンドポイントの場合はグループ ポリシーを構成できますが、Mac エンドポイントの場合はコマンドライン コマンドを使用します。手順については、特定タイプのクライアント デバイスの『VMware Horizon Client の使用』を参照してください。

- 6 エンド ユーザーにリモート デスクトップまたはアプリケーションに接続し、USB デバイスをローカル クライアント システムに接続するように指示します。

USB デバイスのドライバがまだリモート デスクトップまたは RDS ホストにインストールされていない場合、物理 Windows コンピュータ上と同じように、ゲスト OS は USB デバイスを検出して適切なドライバを探します。

ネットワーク トラフィックと USB リダイレクト

USB リダイレクトは表示プロトコル (RDP または PCoIP) とは別に動作し、USB トラフィックは通常 TCP ポート 32111 を使用します。

クライアント システムとリモート デスクトップまたはアプリケーションとの間のネットワーク トラフィックは、クライアント システムが企業ネットワーク内部にあるかどうか、および管理者がセキュリティの設定をどのように選択したかにより、さまざまな経路をとる可能性があります。

- 1 クライアント システムが企業ネットワーク内部にある場合、クライアントとデスクトップまたはアプリケーションとの間に直接接続が確立されるように、USB トラフィックは TCP ポート 32111 を使用します。
- 2 クライアント システムが企業ネットワーク外部にある場合、クライアントは View セキュリティ サーバを経由して接続することができます。

セキュリティ サーバは DMZ 内に存在し、信頼されるネットワーク内の接続に対してプロキシ ホストの役割を果たします。この設計では、公衆網に接するインターネットから View 接続サーバ インスタンスを遮断し、保護されていないすべてのセッション要求が強制的にセキュリティ サーバを通過するようにして、セキュリティのレイヤを追加します。

DMZ ベースのセキュリティ サーバの展開では、クライアントが DMZ 内のセキュリティ サーバに接続できるようにファイアウォール上で数個のポートを開く必要があります。また、セキュリティ サーバと内部ネットワーク内の View 接続サーバ インスタンスが通信できるように、ポートを構成する必要があります。

特定のポートの詳細は、『View アーキテクチャの計画ガイド』の「DMZ ベースのセキュリティ サーバのファイアウォール ルール」を参照してください。

- 3 クライアント システムが企業ネットワーク外部にある場合、View Administrator を使用して HTTPS 安全なトンネルを有効にすることができます。ユーザーがリモート デスクトップまたはアプリケーションに接続するときに、クライアントは View 接続サーバまたはセキュリティ サーバ ホストへの HTTPS 接続を追加します。接続は HTTPS ポート 443 を使用してセキュリティ サーバにトンネリングされ、サーバからリモート デスクトップまたはアプリケーションへの USB トラフィックの以降の接続に TCP ポート 32111 が使用されるようになります。このトンネルを使用すると、USB デバイスのパフォーマンスがわずかに低下します。

注: ゼロ クライアントを使用している場合、USB トラフィックは、TCP 32111 経由ではなく PCoIP 仮想チャネルを使用してリダイレクトされます。データはカプセル化され、TCP/UDP ポート 4172 を使用して、PCoIP Secure Gateway により暗号化されます。ゼロ クライアントのみを使用している場合、TCP ポート 32111 を開く必要はありません。

USB デバイスへの自動接続

一部のクライアント システムでは、管理者、エンド ユーザー、またはその両方が、リモート デスクトップへの USB デバイスの自動接続を構成できます。自動接続は、ユーザーが USB デバイスをクライアント システムに差し込んだとき、またはクライアントがリモート デスクトップに接続したときに確立することができます。

スマート フォンやタブレットなどの一部のデバイスでは、アップグレード中にデバイスが再起動されて接続が切れるため、自動接続が必要となります。これらのデバイスがリモート デスクトップに自動的に再接続するように設定されていない場合、アップグレード中、デバイスの再起動後に、代わりにローカル クライアント システムに接続します。

管理者がクライアントに設定する、またはエンド ユーザーが Horizon Client メニュー項目を使用して設定する自動 USB 接続の構成プロパティは、デバイスが USB リダイレクトから除外されるように構成されている場合を除いて、すべての USB デバイスに適用されます。たとえば、一部のクライアントのバージョンでは、Web カメラとマイクロフォンはリアルタイム オーディオビデオ機能を使用する方が良好に動作するため、デフォルトで USB リダイレクトから除外されています。場合によっては、USB デバイスがデフォルトでリダイレクトから除外されておらず、管理者が明示的にデバイスをリダイレクトから除外する必要があります。たとえば、次のタイプの USB デバイスは USB リダイレクトには適しておらず、リモート デスクトップに自動的に接続してはなりません。

- USB イーサネット デバイス。USB イーサネット デバイスをリダイレクトすると、そのデバイスが唯一のイーサネット デバイスの場合、クライアント システムのネットワーク接続が切断されます。
- タッチ画面デバイス。タッチ画面デバイスをリダイレクトすると、リモート デスクトップはタッチ入力を受け付けますが、キーボード入力は受け付けません。

リモート デスクトップを USB デバイスに自動接続するように設定している場合、タッチ画面デバイスやネットワーク デバイスなどの特定のデバイスを除外するようにポリシーを構成することができます。詳細については、[USB デバイスのフィルタ ポリシー設定の構成](#) を参照してください。

Windows クライアントでは、除外されたデバイスを除くすべてのデバイスに自動的に接続する設定を使用する代わりに、Horizon Client がスマートフォンやタブレットなどの特定のデバイスもしくは特定の複数デバイスのみをリモート デスクトップに再接続するように設定する構成ファイルをクライアントで編集することができます。手順については、『Windows 版 VMware Horizon Client の使用』を参照してください。

保護された View 環境での USB デバイスの展開

USB デバイスは BadUSB と呼ばれるセキュリティ脅威に対して脆弱である可能性があり、一部の USB デバイスではファームウェアがハイジャックされたり、マルウェアに置き換えられたりする場合があります。たとえば、ネットワークトラフィックをリダイレクトしたり、キーボードをエミュレートしてキーストロークを取得したりするデバイスを作成できます。このようなセキュリティ上の脆弱性から View の展開が保護されるように USB リダイレクト機能を構成できます。

USB リダイレクトを無効にすることで、すべての USB デバイスがユーザーの View デスクトップやアプリケーションにリダイレクトされないようにできます。あるいは、特定の USB デバイスのリダイレクト機能を無効にすることで、ユーザーが自分のデスクトップやアプリケーションで特定のデバイスにしかアクセスできないようにすることができます。

組織のセキュリティ要件に従って、このような設定を施すかどうかを決定してください。これらの設定は必須ではありません。View の展開で、USB リダイレクトをインストールし、すべての USB デバイスでその機能を有効なままにしておくこともできます。少なくとも、組織がこのセキュリティ上の脆弱性に晒される可能性をどの程度まで限定する必要があるかについて、慎重に検討してください。

すべてのタイプのデバイスに対する USB リダイレクトの無効化

一部の非常にセキュリティ要件が厳しい環境では、ユーザーがクライアント デバイスに接続した可能性のあるすべての USB デバイスがリモート デスクトップおよびアプリケーションにリダイレクトされるのを回避する必要があります。すべてのデスクトップ プール、特定のデスクトップ プール、またはデスクトップ プール内の特定のユーザーの USB リダイレクトを無効にすることができます。

状況に応じて、次に示す方法の中から任意のものを使用してください。

- Horizon Agent をデスクトップ イメージまたは RDS ホストでインストールする場合、[USB リダイレクト] セットアップ オプションを選択解除してください（このオプションはデフォルトで選択されていません）。この手法では、デスクトップ イメージまたは RDS ホストから展開されるすべてのリモート デスクトップおよびアプリケーションで、USB デバイスへのアクセスが回避されます。
- View Administrator で、特定のプールに対する [USB アクセス] ポリシーを編集して、アクセスを拒否または許可します。この手法では、デスクトップ イメージを変更する必要はなく、特定のデスクトップおよびアプリケーション プールで USB デバイスへのアクセスを制御できます。

RDS デスクトップおよびアプリケーション プールには、グローバル [USB アクセス] ポリシーのみを使用できます。個々の RDS デスクトップまたはアプリケーション プールに対してこのポリシーを設定することはできません。

- View Administrator で、デスクトップまたはアプリケーション プール レベルでポリシーを設定した後、[ユーザー上書き] 設定を選択し、ユーザーを選択することで、プール内の特定のユーザーに対するポリシーを上書きできます。
- 必要に応じて、Horizon Agent 側またはクライアント側で **Exclude All Devices** ポリシーを **true** に設定します。
- スマート ポリシーを使用して、[USB リダイレクト] Horizon ポリシー設定を無効にするポリシーを作成します。この手法により、特定の条件が満たされる場合に特定のリモート デスクトップでの USB リダイレクトを無効化できます。たとえば、ユーザーが企業のネットワーク以外からリモート デスクトップに接続している場合は USB リダイレクトを無効にするポリシーを設定できます。

Exclude All Devices ポリシーを **true** に設定すると、Horizon Client はどの USB デバイスもリダイレクトされないようにします。その他のポリシー設定を使用して、特定のデバイスまたはデバイス ファミリがリダイレクトされるように変更できます。このポリシーを **false** に設定すると、Horizon Client は、その他のポリシー設定でブロックされているものを除き、すべての USB デバイスがリダイレクトされるようにします。このポリシーは、Horizon Agent と Horizon Client の両方に設定できます。次の表は、Horizon Agent と Horizon Client に設定できる **Exclude All Devices** ポリシーを組み合わせ、クライアント コンピュータに効果的なポリシーを作成する方法を示しています。デフォルトでは、ブロックされていない限り、すべての USB デバイスがリダイレクトされるようになっています。

表 15-1. Exclude All Devices（すべてのデバイスを除外する）ポリシーの組み合わせた場合の効果

Horizon Agent での Exclude All Devices（すべてのデバイスを除外する）ポリシー	Horizon Client での Exclude All Devices（すべてのデバイスを除外する）ポリシー	組み合わせた場合の効果的な Exclude All Devices（すべてのデバイスを除外する）ポリシー
false または未定義（すべての USB デバイスを含む）	false または未定義（すべての USB デバイスを含む）	すべての USB デバイスを含む
false （すべての USB デバイスを含む）	true （すべての USB デバイスを除外する）	すべての USB デバイスを除外する
true （すべての USB デバイスを除外する）	いずれか、または未定義	すべての USB デバイスを除外する

Disable Remote Configuration Download ポリシーを **true** に設定すると、Horizon Agent での **Exclude All Devices** の値が Horizon Client に渡されませんが、Horizon Agent と Horizon Client は **Exclude All Devices** のローカル値を適用します。

これらのポリシーは、Horizon Agent の構成 ADM テンプレート ファイル (`vdm_agent.adm`) に含まれています。詳細については、[Horizon Agent の構成 ADM テンプレートの USB 設定](#)を参照してください。

特定のデバイスに対する USB リダイレクトの無効化

ユーザーの中には、ローカル側で接続された特定の USB デバイスをリダイレクトして、リモート デスクトップまたはアプリケーションでそれらのデバイスがタスクを実行できるようにする必要のあるユーザーもいます。たとえば、医師は Dictaphone USB デバイスを使用して、患者の医療情報を記録しなければならない場合があります。このような場合、すべての USB デバイスへのアクセスを無効にすることはできません。グループ ポリシー設定を使用して、特定のデバイスに対して USB リダイレクトを有効または無効にすることができます。

特定のデバイスに対して USB リダイレクトを有効にする前に、会社内のクライアント マシンに接続される物理デバイスを信用できることを確認してください。サプライ チェーンを信用できることを確認します。可能であれば、USB デバイスの加工および流通過程の管理体制を追跡します。

また、従業員に不明な発行元からのデバイスを接続しないように周知します。可能な場合は、環境内のデバイスを署名付きファームウェア更新のみ、つまり FIPS 140-2 レベル 3 認定のものに限定し、現場で更新可能なすべての種類のファームウェアをサポートしないようにします。このようなタイプの USB デバイスは発行元を特定するのが困難であり、デバイスの要件によっては検出不可能である可能性があります。このような選択肢は実用的ではないかもしれませんが、検討する価値はあります。

各 USB デバイスにはコンピュータにそれ自体を認識させるためのベンダー ID と製品 ID が付けられています。Horizon Agent 構成のグループ ポリシー設定を構成することで、既知のデバイス タイプを含めるポリシーを設定できます。この手法により、不明なデバイスが環境内で使用されるリスクをなくすることができます。

たとえば、既知のデバイス ベンダー ID および製品 ID である vid/pid=0123/abcd を除くすべてのデバイスがリモート デスクトップまたはアプリケーションにリダイレクトされるのを回避できます。

```
ExcludeAllDevices    Enabled

IncludeVidPid        o:vid-0123_pid-abcd
```

注: この例の構成では保護することはできますが、感染したデバイスによって何らかの vid/pid が報告される可能性があるため、攻撃の可能性は依然としてあります。

デフォルトで、View は特定のデバイス ファミリがリモート デスクトップまたはアプリケーションにリダイレクトされるのをブロックします。たとえば、HID（ヒューマン インターフェイス デバイス）やキーボードなどはゲスト内への表示がブロックされます。出回っている一部の BadUSB コードは USB キーボード デバイスをターゲットにしています。

特定のデバイス ファミリがリモート デスクトップまたはアプリケーションにリダイレクトされるのを回避できます。たとえば、すべてのビデオ、オーディオ、および大規模ストレージ デバイスをブロックできます。

```
ExcludeDeviceFamily  o:video;audio;storage
```

反対に、ホワイトリストを作成し、すべてのデバイスがリダイレクトされないようにしても特定のデバイス ファミリのみは使用できるようにすることもできます。たとえば、ストレージ デバイスを除くすべてのデバイスをブロックできます。

```
ExcludeAllDevices    Enabled

IncludeDeviceFamily  o:storage
```

リモート ユーザーがデスクトップまたはアプリケーションにログインして、それを感染させる場合、別のリスクが発生する可能性があります。会社のファイアウォールの外側から行われたすべての View 接続への USB アクセスを回避できます。USB デバイスは内的には使用できますが、外的には使用できなくなります。

TCP ポート 32111 をブロックして USB デバイスへの外部アクセスを無効にすると、タイム ゾーン同期が動作しなくなります。これは、タイム ゾーン同期でもポート 32111 が使用されているためです。ゼロ クライアントの場合、USB トラフィックは UDP ポート 4172 の仮想チャネル内に組み込まれます。ポート 4172 は USB リダイレクトの他にディスプレイ プロトコルにも使用されるため、ポート 4172 をブロックすることはできません。必要な場合は、ゼロ クライアントに対して USB リダイレクトを無効に設定できます。詳細については、ゼロ クライアント製品パンフレットを参照するか、ゼロ クライアント ペンダーにお問い合わせください。

特定のデバイス ファミリーまたは特定のデバイスをブロックするポリシーを設定すると、BadUSB マルウェアによって感染させられるリスクを軽減できる可能性があります。これらのポリシーによってすべてのリスクが軽減されるわけではありませんが、全体的なセキュリティ戦略の一部として有効に機能する可能性があります。

ログ ファイルを使用してのトラブルシューティングと USB デバイス ID の確認

USB に有用なログ ファイルは、クライアント システムとリモート デスクトップの両方のオペレーティング システムまたは RDS ホストにあります。トラブルシューティングを行うには、両方の場所にあるログ ファイルを使用します。特定のデバイスの製品 ID を見つけるには、クライアント側のログを使用します。

USB デバイスの分割またはフィルタリングを構成しようとしている場合、または特定のデバイスが Horizon Client メニューに表示されない理由を判断しようとしている場合は、クライアント側のログを確認します。クライアント ログは USB アービトラータ (USB 仲裁デバイス) および Horizon View USB サービスのために生成されます。Windows および Linux クライアントでのログ記録はデフォルトで有効になっています。Mac クライアントでは、ログ記録はデフォルトで無効になっています。Mac クライアントでログ記録を有効にするには、『VMware Horizon Client for Mac の使用』を参照してください。

USB デバイスの分割およびフィルタリングのポリシーを構成する場合、設定する一部の値で USB デバイス用の VID (ペンダー ID) および PID (製品 ID) が必要になります。VID および PID を見つけるには、vid および pid と組み合わせられた製品名をインターネット検索できます。あるいは、Horizon Client の実行中に、USB デバイスをローカル システムに接続してクライアント側のログを調べることができます。次の表は、ログ ファイルのデフォルトの場所を示しています。

表 15-2. ログ ファイルの場所

クライアントまたはエージェン ト	ログ ファイルのパス
Windows クライアント	%PROGRAMDATA%\VMware\VDM\logs\debug-*.txt C:\Windows\Temp\vmware-SYSTEM\vmware-usbarb-*.log
Horizon Agent	%PROGRAMDATA%\VMware\VDM\logs\debug-*.txt
Mac クライアント	/var/root/Library/Logs/VMware/vmware-view-usbd-xxxx.log /Library/Logs/VMware/vmware-usbarbitrator-xxxx.log
Linux クライアント	(デフォルトの場所) /tmp/vmware-root/vmware-view-usbd-*.log

デバイスがリモート デスクトップまたはアプリケーションにリダイレクトされた後に、デバイスに関する問題が発生する場合は、クライアント側とエージェント側両方のログを調べてください。

USB リダイレクトを制御するポリシーの使用

リモート デスクトップまたはアプリケーション (Horizon Agent) と Horizon Client の両方に USB ポリシーを構成できます。これらのポリシーは、クライアント デバイスで複合 USB デバイスを個別のコンポーネントに分割してリダイレクト可能にするかどうかを指定します。デバイスを分割して、クライアントがリダイレクト可能とする USB デバイスのタイプを制限し、Horizon Agent で特定の USB デバイスがクライアント コンピュータから転送されないように防止します。

Horizon Agent または Horizon Client の以前のバージョンをインストールしている場合は、USB リダイレクト ポリシーの機能の一部を使用できません。表 15-3. USB ポリシー設定の互換性 は、Horizon Agent と Horizon Client の組み合わせに応じて View が適用するポリシーについて示しています。

表 15-3. USB ポリシー設定の互換性

Horizon Agent のバージョン	Horizon Client のバージョン	USB ポリシー設定の USB リダイレクトへの影響
5.1 以降	5.1 以降	<p>USB ポリシー設定は、Horizon Agent と Horizon Client の両方に適用されます。Horizon Agent USB ポリシー設定を使用して、USB デバイスがデスクトップに転送されないようブロックできます。Horizon Agent では、デバイス分割およびフィルタリング ポリシーの設定を Horizon Client に送信可能です。Horizon Client USB ポリシー設定を使用して、USB デバイスがクライアント コンピュータからデスクトップにリダイレクトされないよう防止できます。</p> <p>注: View Agent 6.1 以降と Horizon Client 3.3 以降では、これらの USB リダイレクト ポリシー設定が単一ユーザー マシンで実行されるリモート デスクトップに加えて、RDS デスクトップとアプリケーションにも適用されます。</p>
5.1 以降	5.0.x 以前	<p>USB ポリシー設定は、Horizon Agent にのみ適用されます。Horizon Agent USB ポリシー設定を使用して、USB デバイスがデスクトップに転送されないようブロックできます。Horizon Client USB ポリシー設定を使用して、クライアント コンピュータからデスクトップにリダイレクト可能なデバイスの選択を制御することはできません。Horizon Client では、デバイス分割およびフィルタリング ポリシーの設定を Horizon Agent から受信できません。Horizon Client による USB リダイレクトの既存のレジストリ設定は有効なままです。</p>
5.0.x 以前	5.1 以降	<p>USB ポリシー設定は、Horizon Client にのみ適用されます。Horizon Client USB ポリシー設定を使用して、USB デバイスがクライアント コンピュータからデスクトップにリダイレクトされないよう防止できます。Horizon Agent USB ポリシー設定を使用して、USB デバイスがデスクトップに転送されないようブロックすることはできません。Horizon Agent では、デバイス分割およびフィルタリング ポリシーの設定を Horizon Client に送信できません。</p>
5.0.x 以前	5.0.x 以前	<p>USB ポリシー設定は適用されません。Horizon Client による USB リダイレクトの既存のレジストリ設定は有効なままです。</p>

Horizon Client をアップグレードする場合、HardwareIdFilters など USB リダイレクトに関する既存のレジストリ設定は、Horizon Client 用に USB ポリシーを定義するまで、すべて有効なままです。

クライアントサイドの USB ポリシーをサポートしていないクライアント デバイスでは、Horizon Agent に USB ポリシーを使用してクライアントからデスクトップまたはアプリケーションへの転送を許可する USB デバイスを制御できます。

複合 USB デバイスのデバイス分割ポリシー設定の構成

複合 USB デバイスは、ビデオ入力デバイスとストレージデバイス、もしくはマイクロフォンとマウス デバイスなど、2 つ以上のデバイスの組み合わせで構成されます。1 つ以上のコンポーネントをリダイレクトに利用できるよう

にする必要がある場合は、複合デバイスをコンポーネント インターフェイスに分割し、特定のインターフェイスをリダイレクト対象から除外し、残りのインターフェイスをリダイレクトに含めることができます。

複合デバイスを自動的に分割するポリシーを設定できます。特定のデバイスで自動デバイス分割が機能しない場合や、使用しているアプリケーションで必要な結果が自動分割で得られない場合には、複合デバイスを手動で分割できます。

自動デバイス分割

自動デバイス分割を有効にすると、View は現在適用されているフィルタ ルールに従って複合デバイス内の機能もしくはデバイスを分割しようとします。たとえば、マウス デバイスをクライアントでしか使えない状態に保つために口述マイクロフォンを自動分割しても他のデバイスはリモート デスクトップに転送するというケースが考えられます。

次の表は、Horizon Client が複合 USB デバイスを自動分割するかどうかを決定する Allow Auto Device Splitting の設定値を示しています。デフォルトでは、自動分割は無効になっています。

表 15-4. Disable Auto Device Splitting（自動デバイス分割を無効にする）ポリシーを組み合わせた場合の効果

Horizon Agent での自動デバイス分割を許可するポリシー	Horizon Client での自動デバイス分割を許可するポリシー	組み合わせた場合の効果的な自動デバイス分割を許可するポリシー
Allow – Default Client Setting	false （自動分割が無効）	自動分割が無効
Allow – Default Client Setting	true （自動分割が有効）	自動分割が有効
Allow – Default Client Setting	未定義	自動分割が有効
Allow – Override Client Setting	いずれか、または未定義	自動分割が有効
未定義	未定義	自動分割が無効

注: これらのポリシーは、Horizon Agent の構成 ADM テンプレート ファイル (vdm_agent.adm) に含まれています。詳細については、[Horizon Agent の構成 ADM テンプレートの USB 設定](#)を参照してください。

デフォルトでは、View の自動分割は無効であり、複合 USB デバイスのオーディオ出力、キーボード、マウス、スマート カードのコンポーネントはすべてリダイレクト対象から除外されます。

View では、デバイス分割ポリシー設定を適用してから、フィルタ ポリシー設定をすべて適用します。自動分割を有効にしたときに、ベンダー/プロダクト ID を指定し、分割対象から複合 USB デバイスを明示的に除外しない場合は、View が複合 USB デバイスの各インターフェイスを調べ、フィルタ ポリシー設定に従って、除外するインターフェイスか、含めるインターフェイスかを判断します。自動デバイス分割を無効にしたときに、分割する複合 USB デバイスのベンダー/プロダクト ID を明示的に指定しない場合、View はデバイス全体にフィルタ ポリシー設定を適用します。

自動分割を有効にすると、Exclude Vid/Pid Device From Split ポリシーを使用して、分割対象から除外する複合 USB デバイスを指定できます。

手動デバイス分割

Split Vid/Pid Device ポリシーを使用して、分割したい複合 USB デバイスのベンダーおよびプロダクト ID を指定できます。リダイレクト対象から除外したい複合 USB デバイスのコンポーネントについては、そのインターフェイスも指定できます。このようにして除外したコンポーネントに対しては、どのフィルタ ポリシー設定も View で適用されません。

重要: Split Vid/Pid Device ポリシーを使用する場合、明示的に除外しなかったコンポーネントは、View で自動的に含まれることはありません。これらのコンポーネントを含めるには、Include Vid/Pid Device などのフィルタ ポリシーを指定する必要があります。

表 15-5. Horizon Agent でのデバイス分割ポリシー設定の分割修飾子 では、Horizon Client に同等のデバイス分割ポリシー設定が存在する場合に、Horizon Client で Horizon Agent デバイス分割ポリシー設定を処理する方法を指定する修飾子を示しています。これらの修飾子は、すべてのデバイス分割ポリシー設定に適用されます。

表 15-5. Horizon Agent でのデバイス分割ポリシー設定の分割修飾子

修飾子	説明
m (マージ)	Horizon Client は、Horizon Client デバイス分割ポリシー設定に加えて、Horizon Agent デバイス分割ポリシー設定を適用します。
o (上書き)	Horizon Client は、Horizon Client デバイス分割ポリシー設定の代わりに、Horizon Agent デバイス分割ポリシー設定を使用します。

表 15-6. デバイス分割ポリシー設定への分割修飾子の適用例 では、別の分割修飾子を指定したときに、Horizon Client で Exclude Device From Split by Vendor/Product ID の設定を処理する方法の例を示しています。

表 15-6. デバイス分割ポリシー設定への分割修飾子の適用例

Horizon Agent でのベンダー/製品 ID によりデバイスを分割から除外するポリシー	Horizon Client でのベンダー/製品 ID によりデバイスを分割から除外するポリシー	Horizon Client で使用される効果的なベンダー/製品 ID によりデバイスを分割から除外するポリシー
m:vid-XXXX_pid-XXXX	vid-YYYY_pid-YYYY	vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY
o:vid-XXXX_pid-XXXX	vid-YYYY_pid-YYYY	vid-XXXX_pid-XXXX
m:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY	vid-YYYY_pid-YYYY	vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY
o:vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY	vid-YYYY_pid-YYYY	vid-XXXX_pid-XXXX;vid-YYYY_pid-YYYY

Horizon Agent は、デバイス分割ポリシー設定を接続先で適用しません。

Horizon Client は、次の優先順序で、デバイス分割ポリシー設定を評価します。

- Exclude Vid/Pid Device From Split
- Split Vid/Pid Device

分割対象からデバイスを除外するデバイス分割ポリシー設定は、デバイスを分割するためのどのポリシー設定よりも優先されます。分割対象から除外するインターフェイスまたはデバイスを定義すると、Horizon Client は、一致するコンポーネント デバイスをリダイレクトに利用可能なデバイスから除外します。

複合 USB デバイスを分割するためのポリシーの設定例

自動分割後に、特定のベンダーおよび製品 ID のデバイスをリダイレクト対象から除外するデスクトップの分割ポリシーを設定し、そのポリシーをクライアント コンピュータに渡します。

- Horizon Agent の場合、Allow Auto Device Splitting ポリシーを Allow – Override Client Setting に設定します。
- Horizon Agent の場合、Exclude VidPid From Split ポリシーを **o:vid-xxx_pid-yyyy** に設定します (xxx と yyyy は該当する ID)。

デスクトップの自動デバイス分割を許可し、クライアント コンピュータで特定のデバイスを分割するポリシーを指定します。

- Horizon Agent の場合、Allow Auto Device Splitting ポリシーを Allow – Override Client Setting に設定します。
- クライアント デバイスの場合、Include Vid/Pid Device フィルタ ポリシーを、分割したい特定のデバイスを含めるように設定します (例: **vid-0781_pid-554c**)。
- クライアント デバイスの場合、Split Vid/Pid Device ポリシーを、指定した複合 USB デバイスを分割してインターフェイス 00 とインターフェイス 01 をリダイレクト対象から除外するように設定します (例: **vid-0781_pid-554c(exintf:00;exintf:01)**)。

USB デバイスのフィルタ ポリシー設定の構成

Horizon Agent および Horizon Client に対して構成するフィルタ ポリシー設定では、クライアント コンピュータからリモート デスクトップまたはアプリケーションまでリダイレクト可能な USB デバイスが指定されます。USB デバイス フィルタリングは、多くの場合、企業がリモート デスクトップ上の大容量ストレージ デバイスの使用を無効にしたり、クライアント デバイスをリモート デスクトップに接続する USB イーサネット アダプタのような、特定タイプのデバイスが転送されないようにブロックするために使用されます。

デスクトップまたはアプリケーションに接続すると、Horizon Client は Horizon Agent の USB ポリシー設定をダウンロードし、Horizon Client USB ポリシー設定とともにそれらの設定を使用して、クライアント コンピュータからのリダイレクトを許可する USB デバイスを決定します。

View では、デバイス分割ポリシー設定をすべて適用してから、フィルタ ポリシー設定を適用します。複合 USB デバイスを分割した場合、View では各デバイスのインターフェイスが調べられ、フィルタ ポリシー設定に従って、含めるものと含めないものが判断されます。複合 USB デバイスを分割しなかった場合、View でフィルタ ポリシー設定がデバイス全体に適用されます。

デバイス分割ポリシーは Horizon Agent の構成 ADM テンプレート ファイル (`vdm_agent.adm`) に含まれます。詳細については、[Horizon Agent の構成 ADM テンプレートの USB 設定](#)を参照してください。

エージェント適用型 USB 設定の操作

次の表に、Horizon Client に同等のフィルタ ポリシー設定が存在する場合に、Horizon Client でエージェント適用型設定の Horizon Agent フィルタ ポリシー設定を処理する方法を指定する修飾子を示します。

表 15-7. エージェント適用型設定のフィルタ修飾子

修飾子	説明
m (マージ)	Horizon Client により、Horizon Client フィルタ ポリシー設定に加えて、Horizon Agent フィルタ ポリシー設定が適用されます。プール (true/false) 設定の場合、クライアント ポリシーが設定されていなければエージェントの設定が使用されます。クライアント ポリシーが設定されている場合、Exclude All Devices 設定の場合を除き、エージェントの設定は無視されます。Exclude All Devices ポリシーがエージェント側に設定されている場合、このポリシーはクライアント設定よりも優先されます。
o (上書き)	Horizon Client は Horizon Client フィルタ ポリシー設定ではなく、Horizon Agent フィルタ ポリシー設定を使用します。

たとえば、エージェント側で次のポリシー設定を行うと、クライアント側のすべての包含ルールに優先し、デバイス VID-0911_PID-149a にのみ包含ルールが適用されます。

```
IncludeVidPid: o:VID-0911_PID-149a
```

アスタリスクをワイルドカードとして使用することもできます (例: **o:vid-0911_pid-******)。

重要: **o** または **m** 修飾子なしでエージェント側の構成を行うと、構成ルールは無効と見なされ、無視されます。

クライアント解釈型 USB 設定の操作

次の表に、クライアント解釈型設定の Horizon Agent フィルタ ポリシー設定を、Horizon Client で処理する方法を指定する修飾子を示します。

表 15-8. クライアント解釈型設定のフィルタ修飾子

修飾子	説明
Default (レジストリ設定では d)	Horizon Client フィルタ ポリシー設定が存在しない場合、Horizon Client は Horizon Agent フィルタ ポリシー設定を使用します。 Horizon Client フィルタ ポリシー設定が存在する場合、Horizon Client はそのポリシー設定を適用し、Horizon Agent フィルタ ポリシー設定は無視します。
Override (レジストリ設定では o)	Horizon Client では、同等の Horizon Client フィルタ ポリシー設定ではなく、Horizon Agent フィルタ ポリシー設定が使用されます。

Horizon Agent は、クライアント解釈型設定のフィルタ ポリシー設定を接続先で適用しません。

次の表に、別のフィルタ修飾子を指定したときに、Horizon Client で Allow Smart Cards の設定を処理する方法の例を示します。

表 15-9. クライアント解釈型設定へのフィルタ修飾子の適用例

Horizon Agent での Allow Smart Cards (スマート カードを許可する) 設定	Horizon Client での Allow Smart Cards (スマート カードを許可する) 設定	Horizon Client で使用される効果的な Allow Smart Cards (スマート カードを許可する) ポリシー設定
Disable – Default Client Setting (レジストリ設定では d:false)	true (許可する)	true (許可する)
Disable – Override Client Setting (レジストリ設定では o:false)	true (許可する)	false (無効にする)

Disable Remote Configuration Download ポリシーを **true** に設定すると、Horizon Client は、Horizon Agent から送信されるフィルタ ポリシー設定をすべて無視します。

Horizon Agent は、別のフィルタ ポリシー設定を使用するよう Horizon Client を構成しても、または Horizon Client において Horizon Agent からのフィルタ ポリシー設定のダウンロードを無効にしても、エージェント適用型設定にあるフィルタ ポリシー設定を常に接続先で適用します。Horizon Client では、Horizon Agent がデバイスの転送をブロックしていることをレポートしません。

設定の優先

Horizon Client では、優先順位に従って、フィルタ ポリシー設定が評価されます。一致デバイスがリダイレクトされないようにするフィルタ ポリシー設定は、デバイスを含む同等のフィルタ ポリシー設定よりも優先されます。デバイスを除外するフィルタ ポリシー設定が Horizon Client にない場合は、Exclude All Devices ポリシーを **true** に設定していない限り、Horizon Client ではデバイスのリダイレクトが許可されます。しかし、デバイスを除外するように Horizon Agent でフィルタ ポリシー設定を構成した場合、デスクトップまたはアプリケーションはデバイスをそれにリダイレクトしようとする試みをすべてブロックします。

Horizon Client は、Horizon Client 設定と Horizon Agent 設定に加え、Horizon Agent 設定に適用する修飾子の値を考慮し、優先順位に従いフィルタ ポリシー設定を評価します。次のリストに優先順位 (項目 1 が最優先) を示します。

- 1 Exclude Path
- 2 Include Path
- 3 Exclude Vid/Pid Device
- 4 Include Vid/Pid Device
- 5 Exclude Device Family
- 6 Include Device Family
- 7 Allow Audio Input Devices、Allow Audio Output Devices、Allow HIDBootable、Allow HID (Non Bootable and Not Mouse Keyboard)、Allow Keyboard and Mouse Devices、Allow Smart Cards、Allow Video Devices
- 8 すべての USB デバイスを除外するか含めるかが判断される、組み合わせた場合の効果的な Exclude All Devices ポリシー

Exclude Path および Include Path フィルタ ポリシー設定は、Horizon Client に対してのみ設定できます。別のデバイス ファミリー向けの Allow フィルタ ポリシー設定は、優先順位が同じです。

ベンダーおよびプロダクト ID の値に基づいてデバイスを除外するポリシー設定を構成すると、デバイスが属するファミリの Allow ポリシー設定を構成していたとしても、Horizon Client によりベンダーとプロダクト ID の値がこのポリシー設定と一致するデバイスは除外されます。

ポリシー設定の優先順位により、ポリシー設定間の競合が解決されます。スマート カードのリダイレクトを可能にするために Allow Smart Cards を構成した場合、それよりも優先順位の高い除外ポリシー設定を構成すると、このポリシーは上書きされます。たとえば、パス、ベンダー、プロダクト ID の値が一致するスマート カード デバイスを除外するよう Exclude Vid/Pid Device ポリシー設定を構成する場合があります。また、Exclude Device Family デバイス ファミリー全体も除外する smart-card ポリシー設定を構成する場合も同様です。

何らかの Horizon Agent フィルタ ポリシー設定を構成すると、Horizon Agent はリモート デスクトップまたはアプリケーション上で次の優先順位（項目 1 が最優先）に従って、フィルタ ポリシー設定を評価して適用します。

- 1 Exclude Vid/Pid Device
- 2 Include Vid/Pid Device
- 3 Exclude Device Family
- 4 Include Device Family
- 5 すべての USB デバイスを除外するか含めるかが設定されている、エージェント適用型の Exclude All Devices ポリシー

Horizon Agent は、この限定的なフィルタ ポリシー設定のセットを接続先で適用します。

Horizon Agent のフィルタ ポリシー設定を定義することで、管理されていないクライアント コンピュータのフィルタリング ポリシーを作成できます。また、この機能により、Horizon Client のフィルタ ポリシー設定でリダイレクトが許可されている場合でも、クライアント コンピュータから転送されないようデバイスをブロックすることもできます。

たとえば、Horizon Client がデバイスのリダイレクトを可能にするのを許可するポリシーを構成する場合、デバイスを除外するよう Horizon Agent のポリシーを構成すれば、Horizon Agent はデバイスをブロックします。

USB デバイスをフィルタリングするためのポリシーの設定例

これらの例で使用されるベンダー ID とプロダクト ID は、単なる例です。特定デバイスに対するベンダー ID とプロダクト ID の決定については、[ログ ファイルを使用してのトラブルシューティング](#)と [USB デバイス ID の確認](#)を参照してください。

- クライアントで特定のデバイスがリダイレクトされないようにする

```
Exclude Vid/Pid Device:    Vid-0341_Pid-1a11
```

- すべてのストレージ デバイスがこのデスクトップまたはアプリケーション プールにリダイレクトされないようにブロックします。次のエージェント側設定を使用します。

```
Exclude Device Family:    o:storage
```


- デスクトップ プールのすべてのユーザーに対してオーディオおよびビデオ デバイスをブロックし、これらのデバイスがリアルタイム オーディオビデオ機能で常時利用可能になるようにする次のエージェント側設定を使用します。

```
Exclude Device Family:      o:video;audio
```

ベンダーおよびプロダクト ID を使用して特定のデバイスを除外することもできることに注意してください。

- クライアントで 1 つの特定のデバイスを除くすべてのデバイスがリダイレクトされないようにブロックする

```
Exclude All Devices:      true
Include Vid/Pid Device:    Vid-0123_Pid-abcd
```

- エンド ユーザーに問題が起こるため、特定の企業で製造されたすべてのデバイスを除外する次のエージェント側設定を使用します。

```
Exclude Vid/Pid Device:    o:Vid-0341_Pid-*
```

- クライアントで 2 つの特定のデバイスを含め、その他すべてを除外する

```
Exclude All Devices:      true
Include Vid/Pid Device:    Vid-0123_Pid-abcd;Vid-1abc_Pid-0001
```

USB デバイス ファミリ

Horizon Client、または View Agent または Horizon Agent の USB フィルタリング規則を作成する場合にファミリを指定できます。

注: 一部のデバイスはデバイス ファミリを報告しません。

表 15-10. USB デバイス ファミリ

デバイス ファミリ名	説明
audio	すべてのオーディオ入力またはオーディオ出力デバイス。
audio-in	マイクロフォンなどのオーディオ入力デバイス。
audio-out	ラウドスピーカーおよびヘッドホンなどのオーディオ出力デバイス。
bluetooth	Bluetooth に接続されたデバイス。
comm	モデムおよび有線ネットワーク アダプタなどの通信デバイス。
hid	キーボードおよびポインティング デバイスを除くヒューマン インターフェイス デバイス。
hid-bootable	キーボードおよびポインティング デバイスを除く、起動時に使用できるヒューマン インターフェイス デバイス。
imaging	スキャナなどの画像デバイス。
keyboard	キーボード デバイス。
mouse	マウスなどのポインティング デバイス。
other	ファミリが指定されていません。
pda	携帯情報端末。

デバイス ファミリ名	説明
physical	カフィードバック ジョイスティックなどのカフィードバック デバイス。
printer	印刷デバイス。
security	指紋読み取りなどのセキュリティ デバイス。
smart-card	スマート カード デバイス。
storage	フラッシュ ドライブおよび外部ハードディスク ドライブなどの大容量ストレージ デバイス。
unknown	ファミリーが不明です。
vendor	ベンダ固有の機能のあるデバイス。
video	ビデオ入力デバイス。
wireless	無線ネットワーク アダプタ。
wusb	無線 USB デバイス。

Horizon Agent の構成 ADM テンプレートの USB 設定

Horizon Agent と Horizon Client の両方で USB ポリシー設定を定義できます。接続時に、Horizon Client は USB ポリシー設定を Horizon Agent からダウンロードし、それらを Horizon Client USB ポリシー設定と一緒に使用して、クライアント コンピュータからのリダイレクトに利用できるようにするデバイスを指定します。

Horizon Agent の構成 ADM テンプレート ファイル (`vdm_agent.adm`) には、Horizon Agent の認証および環境コンポーネントに関連するポリシー設定（USB リダイレクトなど）が含まれています。設定はコンピュータ レベルで適用されます。Horizon Agent は、コンピュータ レベルで GPO から設定を優先的に読み取ります。GPO からの読み取りがない場合は、`HKLM\Software\Policies\VMware, Inc.\VMware VDM\Agent\USB` のレジストリから設定を読み取ります。

USB デバイス分割を構成するための設定

次の表で、Horizon Agent の構成 ADM テンプレート ファイル内にある、複合 USB デバイスの分割に関する各ポリシー設定について説明します。Horizon Agent は、これらの設定を適用しません。Horizon Agent は、設定を Horizon Client に渡し、マージ (m) またはオーバーライド (o) のどちらの修飾子を指定したかに応じて、解釈と適用が行われます。Horizon Client は設定を使用して、複合 USB デバイスをコンポーネント デバイスに分割するかどうか、そしてコンポーネント デバイスをリダイレクトに利用可能なデバイスから除外するかどうかを決定します。複合 USB デバイスの分割ポリシーの View での適用方法については、[複合 USB デバイスのデバイス分割ポリシー設定の構成](#)を参照してください。

表 15-11. Horizon Agent の構成テンプレート：デバイス分割設定

設定	プロパティ
Allow Auto Device Splitting プロパティ： AllowAutoDeviceSplitting	複合 USB デバイスの自動分割を許可します。 デフォルト値は未定義で、 false と同じです。
Exclude Vid/Pid Device From Split プロパティ： SplitExcludeVidPid	ベンダーおよびプロダクト ID で指定された複合 USB デバイスは、分割対象から除外します。設定の形式： <code>{m o}:vid-xxx1_pid-yyyZ;vid-xxx2_pid-yyyZ...</code> ID 番号は 16 進数で指定する必要があります。ID の個々の数字の位置にワイルドカード文字 (*) を使用できます。 例： o:vid-0781_pid-55** デフォルト値は定義されていません。
Split Vid/Pid Device プロパティ： SplitVidPid	ベンダーおよびプロダクト ID で指定した複合 USB デバイスのコンポーネントを、別のデバイスとして扱います。設定の形式： <code>{m o}:vid-xxxx_pid-yyy(exintf:zz;exintf:ww)</code> または <code>{m o}:vid-xxxx_pid-yyy(exintf:zz;exintf:ww)</code> exintf というキーワードを使用すれば、インターフェイス番号を指定することで、コンポーネントをリダイレクトから除外することができます。ID 番号は 16 進数で指定し、インターフェイス番号は先行ゼロをすべて含む 10 進数で指定する必要があります。ID の個々の数字の位置にワイルドカード文字 (*) を使用できます。 例： o:vid-0781_pid-554c(exintf:01;exintf:02) 注： 明示的に除外しなかったコンポーネントは、View で自動的に含まれることはありません。これらのコンポーネントを含めるには、Include Vid/Pid Device などのフィルタ ポリシーを指定する必要があります。 デフォルト値は定義されていません。

Horizon Agent 適用型 USB 設定

次の表で、Horizon Agent の構成 ADM テンプレート ファイルにある、USB 用の各エージェント適用型ポリシー設定について説明します。Horizon Agent は設定を使用して、USB デバイスがホスト マシンに転送できるかどうかを判断します。Horizon Agent はまた、設定を Horizon Client に渡し、マージ (m) またはオーバーライド (o) のどちらの修飾子を指定したかに応じて、解釈と適用が行われます。Horizon Client は設定を使用して、USB デバイスがリダイレクトに利用可能かどうかを決定します。Horizon Agent は、エージェント適用型ポリシー設定を常に適用するため、Horizon Client に設定したポリシーとは逆の結果になることがあります。USB デバイスをフィルタリングするためのポリシーを View で適用する方法については、[USB デバイスのフィルタ ポリシー設定の構成](#)を参照してください。

表 15-12. Horizon Agent の構成テンプレート：エージェント適用型設定

設定	プロパティ
Exclude All Devices プロパティ： ExcludeAllDevices	<p>転送対象からすべての USB デバイスを除外します。true に設定すると、その他のポリシー設定を使用して、特定のデバイスまたはデバイス ファミリが転送されるようにすることができます。false に設定すると、その他のポリシー設定を使用して、特定のデバイスまたはデバイス ファミリが転送されるのを防止できます</p> <p>true に設定し、Horizon Client に渡すようにすると、この設定は Horizon Client での設定を常にオーバーライドします。この設定では、マージ (m) または上書き (o) の修飾子は使用できません。</p> <p>デフォルト値は未定義で、false と同じです。</p>
Exclude Device Family プロパティ： ExcludeFamily	<p>転送対象からデバイス ファミリを除外します。設定の形式：{m o}:family_name_1[,family_name_2]...</p> <p>例：o:bluetooth;smart-card</p> <p>自動デバイス分割を有効にした場合、View は複合 USB デバイスの各インターフェイスのデバイス ファミリを調べ、除外するインターフェイスを判断します。自動デバイス分割を無効にした場合、View は複合 USB デバイス全体のデバイス ファミリを調べます。</p> <p>デフォルト値は定義されていません。</p>
Exclude Vid/Pid Device プロパティ： ExcludeVidPid	<p>指定したベンダーとプロダクト ID のデバイスを、転送対象から除外します。設定の形式：{m o}:vid-xxx1_pid-yyy2[,vid-xxx2_pid-yyy2]...</p> <p>ID 番号は 16 進数で指定する必要があります。ID の個々の数字の位置にワイルドカード文字 (*) を使用できます。</p> <p>例：m:vid-0781_pid-****;vid-0561_pid-554c</p> <p>デフォルト値は定義されていません。</p>
Include Device Family プロパティ： IncludeFamily	<p>デバイス ファミリを転送対象に含めます。設定の形式：{m o}:family_name_1[,family_name_2]...</p> <p>例：m:storage</p> <p>デフォルト値は定義されていません。</p>
Include Vid/Pid Device プロパティ： IncludeVidPid	<p>指定したベンダーとプロダクト ID のデバイスを、転送対象に含めます。設定の形式：{m o}:vid-xxx1_pid-yyy2[,vid-xxx2_pid-yyy2]...</p> <p>ID 番号は 16 進数で指定する必要があります。ID の個々の数字の位置にワイルドカード文字 (*) を使用できます。</p> <p>例：o:vid-0561_pid-554c</p> <p>デフォルト値は定義されていません。</p>

クライアント解釈型 USB 設定

次の表で、Horizon Agent の構成 ADM テンプレート ファイル内にある各クライアント解釈型ポリシー設定について説明します。Horizon Agent は、これらの設定を適用しません。Horizon Agent は、Horizon Client に設定を渡し、解釈と適用が行われます。Horizon Client は設定を使用して、USB デバイスがリダイレクトに利用可能かどうかを決定します。

表 15-13. Horizon Agent の構成テンプレート：クライアント解釈型設定

設定	プロパティ
Allow Audio Input Devices プロパティ： AllowAudioIn	オーディオ入力デバイスの転送を許可します。 デフォルト値は定義されていませんが、これは true が設定されている場合に相当します。
Allow Audio Output Devices プロパティ： AllowAudioOut	オーディオ出力デバイスの転送を許可します。 デフォルト値は未定義で、 false と同じです。
Allow HIDBootable プロパティ： AllowHIDBootable	キーボードとマウス以外で、起動時に利用可能な入力デバイス（別名 HID 起動可能なデバイス）の転送を許可します。 デフォルト値は定義されていませんが、これは true が設定されている場合に相当します。
Allow Other Input Devices	HID 起動可能なデバイスや統合型ポインティング デバイス付きキーボード以外の入力デバイスの転送を許可します。 デフォルト値は定義されていません。
Allow Keyboard and Mouse Devices プロパティ： AllowKeyboardMouse	統合型ポインティング デバイス（マウス、トラックボール、タッチ パッドなど）付きキーボードの転送を許可します。 デフォルト値は未定義で、 false と同じです。
Allow Smart Cards プロパティ： AllowSmartcard	スマート カード デバイスの転送を許可します。 デフォルト値は未定義で、 false と同じです。
Allow Video Devices プロパティ： AllowVideo	ビデオ デバイスの転送を許可します。 デフォルト値は定義されていませんが、これは true が設定されている場合に相当します。

USB リダイレクトに関する問題のトラブルシューティング

Horizon Client で USB リダイレクトに関する各種の問題が発生することがあります。

問題

Horizon Client の USB リダイレクトで、ローカル デバイスをリモート デスクトップで使用可能にできなかったり、Horizon Client で一部のデバイスがリダイレクトに使用できるように表示されなかったりします。

原因

USB リダイレクトが正常に機能しない場合、または予想どおりに機能しない場合、可能性のある原因は次のとおりです。

- デバイスが複合 USB デバイスであり、含まれるデバイスの 1 つがデフォルトでブロックされています。たとえばマウスを含む読み上げデバイスはデフォルトでブロックされています。これはマウス デバイスがデフォルトでブロックされているためです。この問題を解決するには、[複合 USB デバイスのデバイス分割ポリシー設定の構成](#)を参照してください。
- USB リダイレクトは、リモート デスクトップおよびアプリケーションが展開されている Windows Server 2008 RDS ホストではサポートされません。View Agent 6.1 以降では、Windows Server 2012 RDS ホストで USB リダイレクトがサポートされますが、サポート対象は USB ストレージ デバイスのみです。USB リダイレクトは、単一ユーザー デスクトップとして使用されている Windows Server 2008 R2 および Windows Server 2012 R2 システムでサポートされます。

- RDS デスクトップおよびアプリケーションでは、USB フラッシュ ドライブとハード ディスクのみがサポートされます。その他のタイプの USB デバイスや、セキュリティ ストレージ ドライブや USB CD-ROM などのその他のタイプの USB ストレージ デバイスを RDS デスクトップやアプリケーションにリダイレクトすることはできません。
- Web カメラはリダイレクトの対象としてサポートされていません。
- USB オーディオ デバイスのリダイレクトは、ネットワークの状態に依存し、信頼できません。一部のデバイスでは、アイドル状態のときでさえ、高いデータ スループットが必要です。
- ブート デバイスでは USB リダイレクトがサポートされていません。USB デバイスからブートする Windows システムで Horizon Client を実行しており、このデバイスをリモート デスクトップにリダイレクトした場合、ローカル オペレーティング システムが応答しなかったり使用できなかったりすることがあります。<http://kb.vmware.com/kb/1021409> を参照してください。
- Windows 版 Horizon Client では、デフォルトで、キーボード、マウス、スマート カード、オーディオ出力デバイスをリダイレクト対象として選択できません。<http://kb.vmware.com/kb/1011600> を参照してください。
- RDP は、コンソール セッションの USB HID またはスマート カード リーダのリダイレクトをサポートしていません。<http://kb.vmware.com/kb/1011600> を参照してください。
- Windows Mobile デバイス センターにより、RDP セッションの USB デバイスのリダイレクトが妨げられることがあります。<http://kb.vmware.com/kb/1019205> を参照してください。
- 一部の USB HID では、マウス ポインタの位置を更新するように、仮想マシンを構成する必要があります。<http://kb.vmware.com/kb/1022076> を参照してください。
- 一部のオーディオ デバイスでは、ポリシー設定またはレジストリ設定を変更する必要がある場合があります。<http://kb.vmware.com/kb/1023868> を参照してください。
- ネットワークのレイテンシーが原因で、デバイスの相互作用が低速になったり、アプリケーションがフリーズしているように見えることがあります。これはアプリケーションがローカル デバイスと相互作用するように設計されているからです。非常に大容量の USB ディスク ドライブは、Windows エクスプローラに表示されるまでに数分かかることがあります。
- FAT32 ファイル システムでフォーマットされた USB フラッシュ カードはロードが遅くなります。<http://kb.vmware.com/kb/1022836> を参照してください。
- リモート デスクトップまたはアプリケーションに接続する前に、ローカル システムでプロセスまたはサービスがデバイスを開いていた。
- リダイレクトされた USB デバイスは、デスクトップまたはアプリケーションにそのデバイスが使用可能であることが表示されている場合でも、デスクトップまたはアプリケーション セッションを再接続すると、動作が停止します。
- View Administrator で USB リダイレクトが無効になっている。
- ゲスト上で、USB リダイレクト ドライバが存在しないか、無効になっている。

解決方法

- ◆ PCoIP が使用可能な場合は、RDP の代わりにプロトコルとして使用します。

- ◆ 一時的な切断後に、リダイレクトされたデバイスが使用できないままであるか、動作を停止した場合、デバイスを取り外し、再度接続して、リダイレクトを再試行してください。
- ◆ View Administrator で、[ポリシー] - [グローバル ポリシー] に移動して、[View ポリシー] で USB アクセスが [許可] に設定されていることを確認します。
- ◆ ゲストのログでクラス `ws_vhub` のエントリの有無、クライアントのログでクラス `vmware-view-usbd` のエントリの有無を調べます。

ユーザーが管理者でない場合、または USB リダイレクト ドライバがインストールされていないか、機能していない場合には、これらのクラスのエントリがログに書き込まれます。これらのログの場所については、[ログ ファイルを使用してのトラブルシューティングと USB デバイス ID の確認](#)を参照してください。

- ◆ ゲスト上でデバイス マネージャを開き、[ユニバーサル シリアル バス コントローラ] を展開して、VMware View 仮想 USB ホスト コントローラのドライバおよび VMware View 仮想 USB ハブのドライバが表示されない場合はそれらを再インストールし、無効になっている場合は再度有効にします。

ストレージ要件の軽減と管理

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

この章には、次のトピックが含まれています。

- [vSphere によるストレージの管理](#)
- [インスタント クローンによる必要ストレージの軽減](#)
- [View Composer によるストレージ要件の軽減](#)
- [インスタントクローンおよび View Composer リンククローン デスクトップ プールのストレージ サイズ設定](#)
- [View Composer リンク クローン仮想マシンのストレージ オーバーコミット](#)
- [View Composer リンククローン データ ディスク](#)
- [ローカル データストアへの View Composer リンク クローンの保存](#)
- [インスタント クローンおよび View Composer リンク クローン用の別のデータストアへのレプリカおよびクローンの格納](#)
- [View Composer リンク クローン用の View Storage Accelerator の構成](#)
- [View Composer リンク クローンでのディスク領域の再利用](#)
- [View Composer リンク クローン用の VAAI ストレージの使用](#)
- [View Composer リンク クローン用の Storage Accelerator と領域再利用の停電期間の設定](#)

vSphere によるストレージの管理

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

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

互換性のある vSphere 5.0 および 5.1 以降の機能

vSphere 5.0 以降のリリースでは、以下の機能を使用できます。

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

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

- リモート デスクトップが vSphere 5.1 以降のバージョンで使用できる領域効率的なディスク形式を使用する場合、ゲスト OS 内の無効または削除されたデータは、自動的にワイプおよび縮小プロセスで再利用されます。
- 特定の制限付きで、最大 32 の ESXi ホストを含むクラスタにデスクトップ プールを展開できます。

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

互換性のある vSphere 5.5 Update 1 以降の機能

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

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

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

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

互換性のある vSphere 6.0 以降の機能

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

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

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

注: インスタント クローンは仮想ボリュームをサポートしません。

高パフォーマンス ストレージとポリシー ベース管理のための Virtual SAN の使用

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

Virtual SAN はポリシー ベースのアプローチをストレージ管理に実装します。Virtual SAN を使用する場合は、View によって容量、パフォーマンス、可用性などの仮想マシン ストレージ要件が、デフォルト ストレージ ポリシー プロファイルの形で定義されます (このプロファイルは変更できます)。ストレージは、割り当てられたポリシーに従ってプロビジョニングされ、自動的に設定されます。Virtual SAN は、リンククローン デスクトップ プール、インスタントクローン デスクトップ プール、完全クローン デスクトップ プール、および自動ファームで使用できます。

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

Virtual SAN では、HA、vMotion、および DRS などの共有ストレージを必要とする VMware 機能がサポートされるとともに、外部の共有ストレージ インフラストラクチャが要らなくなり、ストレージ構成と仮想マシンのプロビジョニング アクティビティが簡素になります。

重要: vSphere 6.0 以降のリリースで使用可能な Virtual SAN 機能には、vSphere 5.5 Update 1 で使用可能になった機能を上回る、多数のパフォーマンス上の改善が含まれています。vSphere 6.0 では、この機能により広範囲にわたる HCL (ハードウェア互換性) サポートも含まれています。また、VMware Virtual SAN 6.0 は、キャッシングと固定ストレージの両方にフラッシュベースのデバイスを使用するオールフラッシュ アーキテクチャをサポートします。

View の Virtual SAN ワークフロー

- 1 vCenter Server 5.5 Update 1 以降のリリースを使用して Virtual SAN を有効にします。vSphere 5.5 Update 1 の Virtual SAN の詳細については、『vSphere ストレージ』ドキュメントを参照してください。vSphere 6 以降の Virtual SAN の詳細については、『VMware Virtual SAN の管理』ドキュメントを参照してください。
- 2 View Administrator で自動デスクトップ プールまたは自動ファームを作成する場合、[ストレージ ポリシー管理] で [VMware Virtual SAN を使用する] を選択し、使用する Virtual SAN データストアを選択します。

[VMware Virtual SAN を使用する] を選択すると、Virtual SAN データストアのみが表示されます。

デフォルトのストレージ ポリシー プロファイルは、選択するオプションに従って作成されます。たとえば、リンク クローンのフローティング デスクトップ プールを作成すると、レプリカ ディスク プロファイルとオペレーティング システムのディスク プロファイルは自動的に作成されます。リンク クローンの通常のデスクトップ プールを作成すると、レプリカ ディスク プロファイルと通常のディスク プロファイルが作成されます。自動ファームの場合、レプリカ ディスク プロファイルが作成されます。デスクトップ プールと自動ファームのどちらのタイプの場合も、仮想マシン ファイルのプロファイルが作成されます。

- 3 既存の View Composer デスクトップ プールを他のタイプのデータストアから Virtual SAN のデータストアに移動するには、View Administrator でプールを編集して古いデータストアを選択解除し、その代りに Virtual SAN のデータストアを選択し、Rebalance コマンドを使用します。自動ファームは再調整できないため、この操作は自動ファームでは実行できません。

- 4 (オプション) vCenter Server を使用してストレージ ポリシー プロファイルのパラメータを変更します。これには、許容できる障害の回数や、予約する SSD の読み取りキャッシュの量などが含まれます。

ポリシーの名前は、OS_DISK (オペレーティング システム ファイルを示す)、PERSISTENT_DISK (ユーザー データ ファイルを示す)、REPLICA_DISK (レプリカを示す)、VM_HOME (.vmx ファイルや .vmsn ファイルなどの仮想マシン ファイルを示す) です。ポリシーの変更は、デスクトップ プールまたは自動ファームに新規に作成される仮想マシンと既存の仮想マシンのすべてに伝達されます。

- 5 vCenter Server を使用して、データストアに参加する Virtual SAN クラスタとディスクを監視します。詳細については、『vSphere ストレージ マニュアル』と『vSphere 監視とパフォーマンス マニュアル』を参照してください。vSphere 6 以降については、『VMware Virtual SAN の管理』ドキュメントを参照してください。
- 6 (オプション) View Composer のリンククローン デスクトップ プールの場合は、通常のように Refresh コマンドと Recompose コマンドを使用します。自動ファームの場合、データストアのタイプに関係なく、Recompose コマンドのみがサポートされます。

要件および制限

Virtual SAN 機能には、View 展開で使用する場合に以下の制限があります。

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

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

Virtual SAN 機能には以下の要件があります。

- vSphere 5.5 Update 1 以降のリリース。
- 適切なハードウェア。たとえば、VMware では容量に関する各ノードには、10GB の NIC、少なくとも 1 つの SSD、1 つの HDD を推奨しています。個別の要件については、『[VMware 互換性ガイド](#)』を参照してください。

- 少なくとも 3 つの ESXi ホストのクラスタ。Virtual SAN 拡張クラスタを備える 2 つの ESXi ホストを使用した場合でも、セットアップに対応するためには十分な ESXi ホストが必要です。詳細については、『vSphere 構成の上限』ドキュメントを参照してください。
- HDD の容量の少なくとも 10% である SSD の容量。
- セットアップに対応する十分な HDD 容量。磁気ディスクの使用率が 75% を超過しないようにします。

Virtual SAN 要件の詳細については、『vSphere 5.5 Update 1 ストレージ』ドキュメントの「Virtual SAN の操作」を参照してください。vSphere 6 以降については、『VMware Virtual SAN の管理』ドキュメントを参照してください。VMware Virtual SAN の View 仮想デスクトップ インフラストラクチャの主要コンポーネントのサイズ調整と設計のガイダンスについては、<http://www.vmware.com/files/pdf/products/vsan/VMW-TMD-Virt-SAN-Dsn-Szing-Guid-Horizon-View.pdf> から提供されているホワイト ペーパーを参照してください。

Virtual SAN データストアのデフォルトのストレージ ポリシー プロファイル

Virtual SAN を使用する場合は、View によって容量、パフォーマンス、可用性などの仮想マシン ストレージ要件が、デフォルト ストレージ ポリシー プロファイルの形で定義されます (このプロファイルは変更できます)。ストレージは、割り当てられたポリシーに従ってプロビジョニングされ、自動的に設定されます。

デスクトップ プールの作成時に作成されるデフォルトのポリシーは、作成するプールの種類によって異なります。ポリシーの名前は、OS_DISK (オペレーティング システム ファイルを示す)、PERSISTENT_DISK (ユーザー データ ファイルを示す)、REPLICA_DISK (レプリカを示す)、VM_HOME (.vmx ファイルや .vmsn ファイルなどの仮想マシン ファイルを示す) です。たとえば、REPLICA_DISK ポリシーが作成されるのは、リンククローン プールの場合だけです。ポリシーの変更は、デスクトップ プールに新規に作成される仮想マシンと既存の仮想マシンのすべてに伝達されます。

Virtual SAN はストレージ ポリシー フレームワークを提供します。このフレームワークを使用して Virtual SAN データストア上に存在するさまざまな仮想マシン オブジェクトの動作を制御できます。Virtual SAN には、仮想ディスク (VMDK) ファイルなどのオブジェクトが含まれます。各オブジェクトには、ポリシーによって制御される 4 つの特性があります。

- [ストライプ]: データのストライプの数。ディスク ストライプの数は磁気ディスク (HDD) の数に影響を与えます。
- [復元性]: 許容する障害の数。許容するホスト障害の数は、当然ながら、使用されているホストの数によって異なります。
- [ストレージ プロビジョニング]: シックまたはシン。
- [キャッシュ予約]: 読み取りキャッシュ予約。

ストライプとキャッシュ予約の設定は、パフォーマンスの制御に使用されます。復元性の設定は可用性を制御します。ストレージ プロビジョニングの設定は容量を制御します。これらの設定が、全体として vSphere ホストと磁気ディスクの必要数に影響を与えます。

たとえば、オブジェクトあたりのディスク ストライプの数を 2 に設定すると、Virtual SAN は少なくとも 2 台の HDD にわたってそのオブジェクトのストライピングを行います。この設定と併用して、許容するホスト障害の数を 1 に設定すると、Virtual SAN は復元用としてコピーをもう 1 つ作成します。この結果、HDD が 4 台必要となります。さらに、許容するホスト障害の数を 1 に設定する場合、ESXi ホストは最低 3 台必要です（復元用に 2 台、パーティション化されている場合にタイブレークを実行するために 1 台）。

注: 矛盾する設定を誤って行った場合には、その設定の適用時に操作が失敗し、状況（十分な数のホストが存在しないことなど）を説明するエラー メッセージが表示されます。

これらのデフォルト ポリシーに関連するユーザー操作の要件はありません。ポリシーは、リンククローン デスクトップ プール、完全クローン デスクトップ プール、および自動ファームの場合に作成されます。

デフォルトのストレージ ポリシー プロファイルは、vSphere コマンドライン インターフェイス (esxcli) または vSphere Web Client を使用して変更できます。各仮想マシンはクラスタ内の物理的な位置にかかわらず、そのポリシーを保持します。ポリシーが、ホスト、ディスク、またはネットワーク障害のために不適合になったり、ワークロードが変更される場合、Virtual SAN は各仮想マシンのポリシーを満たすために、影響のある仮想マシンとロード バランスのデータを再構成します。

仮想マシン中心ストレージとポリシー ベース管理のための仮想ボリュームの使用

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

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

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

Virtual Volumes には次の利点があります。

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

- vSphere APIs for Array Integration (VAAI) をサポートするストレージ アレイで Virtual Volumes を使用できません。

要件および制限

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

- このリリースでは、ディスクのワイプおよび縮小によってディスク領域を再利用する View 領域効率的なディスク形式機能がサポートされていません。
- Virtual Volumes では View Composer Array Integration (VCAI) の使用はサポートされません。
- インスタント クローン デスクトップ プールでは、Virtual Volumes データストアはサポートされません。

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

Virtual Volumes 機能には以下の要件があります。

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

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

インスタント クローンによる必要ストレージの軽減

インスタント クローン機能は、vSphere vmFork テクノロジー (vSphere 6.0U1 以降で使用可能) を活用して、実行中の基本イメージまたは親仮想マシンを静止させてホットクローンを作成し、最大 2,000 個のインスタント クローンのプールを作成します。

インスタント クローンは、作成時に仮想ディスクを親仮想マシンと共有するだけでなく、親のメモリも共有します。各インスタント クローンは一意のホスト名および IP アドレスを持ち、独立したデスクトップのように動作しますが、インスタント クローンの方がストレージの必要量ははるかに少なくなります。インスタント クローンにより、必要とされるストレージ容量は 50 ~ 90% 軽減されます。また、クローン作成時に必要なメモリの合計量も軽減されます。

同じデータストア上のレプリカおよびインスタント クローン

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

異なるデータストアにあるレプリカおよびインスタント クローン

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

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

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

インスタント クローンと View Composer のリンク クローンの違い

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

- インスタント クローン プールは、ゲスト オペレーティング システムのページング ファイルと一時ファイルを格納するための廃棄可能な個別の仮想ディスクの構成をサポートしません。ユーザーがインスタント クローン デスクトップからログアウトするたびに、View は自動的にクローンを削除し、プールが使用可能な最新の OS イメージに基づいて別のインスタント クローンをプロビジョニングしてパワーオンします。ゲスト オペレーティング システムのページング ファイルと一時ファイルは、ログアウト操作中に自動的に削除されます。
- インスタント クローン プールは、各仮想デスクトップについて個別の通常仮想ディスクの作成をサポートしません。代わりに、エンド ユーザーの Windows プロファイルおよびアプリケーション データを App Volumes のユーザー書き込み可能ディスクに格納できます。エンド ユーザーのユーザー書き込み可能ディスクは、エンド ユーザーがログインしたときにインスタント クローン デスクトップに接続されます。さらに、ユーザーがインストールしたアプリケーションを保持するために、ユーザー書き込みディスクを使用できます。
- インスタント クローン デスクトップは一時的なものであるため、ワイプおよび縮小プロセスを含む領域を効率化するディスク形式 (SE スパース) は必要ありません。

View Composer によるストレージ要件の軽減

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

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

同じデータストア上のレプリカおよびリンク クローン

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

異なるデータストアにあるレプリカおよびリンク クローン

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

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

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

ページングおよび一時ファイルのためのディスポーザブル ディスク

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

専用デスクトップのための通常ディスク

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

インスタントクローンおよび View Composer リンククローン デスクトップ プールのストレージ サイズ設定

View には、インスタントクローンまたはリンククローン デスクトップ プールに必要なストレージの量を特定するのに役立つ大まかなガイドラインが用意されています。[デスクトップ プールを追加] ウィザードには、デスクトップ プールに必要なストレージの見積もりが示されます。

ストレージのサイズ設定の表には、OS ディスク、View Composer 通常ディスク (View Composer リンク クローン用のみ)、およびレプリカを格納するために選択するデータストア上の空き領域も表示されます。実際の空き領域をデスクトップ プールの見積もりの要件と比較することによって、どのデータストアを使用するかを決定できます。

View が使用する式は、ストレージ使用の一般的な見積もりを計算するだけです。クローンの実際のストレージの拡大は、次のような多くの要因に依存します。

- 親仮想マシンに割り当てられたメモリの量
- 更新操作の頻度 (View Composer リンク クローンのみ)
- ゲスト OS のページング ファイルのサイズ
- ページング ファイルと一時ファイルを個別のディスクにリダイレクトするかどうか (View Composer リンク クローンのみ)
- 個別の View Composer 通常ディスクを構成するかどうか (View Composer リンク クローンのみ)
- デスクトップ マシン上のワークロード (主に、ユーザーがゲスト OS で実行するアプリケーションの種類によって決まります)

注: 数百または数千のクローンが含まれている展開では、特定のデータストアのセットが特定の ESXi クラスタ専用で使用されるようにデスクトップ プールを構成します。プールをすべてのデータストアにわたってランダムに構成することは避けてください。ほとんどまたはすべての ESXi ホストが、ほとんどまたはすべての LUN にアクセスしなければならなくなります。

特定の LUN 上の OS ディスクに書き込もうとする ESXi ホストが多すぎると、競合の問題が発生して、パフォーマンスが低下し、拡張性が妨げられることがあります。大規模な展開でのデータストアの計画の詳細については、『View アーキテクチャの計画』を参照してください。

インスタントクローン プールとリンク クローン プールのサイズ設定ガイドライン

インスタントクローンまたはリンク クローン デスクトップ プールを作成または編集すると、[リンク クローンのデータストアを選択 (インスタント クローンのデータストアを選択)] ページに、ストレージのサイズ設定ガイドラインを示す表が表示されます。この表は、リンク クローン ディスクにどのデータストアを選択するかを決定するのに役立ちます。これらのガイドラインから、新しいリンク クローンに必要な容量を計算できます。

OS ディスクと通常ディスクのサイズ設定の表

表 16-1. OS ディスクと通常ディスクのサイズ設定の表の例 に、親仮想マシンに 1GB のメモリと 10GB のレプリカがある場合に、10 台の仮想マシンのプールに対して表示される、ストレージのサイズ設定に対する推奨値の例を示します。この例では、OS ディスクと View Composer 通常ディスク用に異なるデータストアが選択されています。

注: 通常ディスクの情報は、View Composer リンク クローンのみを対象にしています。インスタント クローンは通常ディスクをサポートしていません。

表 16-1. OS ディスクと通常ディスクのサイズ設定の表の例

データの種類	選択された空き領域 (GB)	推奨される最小領域 (GB)	50% Utilization (GB) (50% の使用率 (GB))	推奨される最大領域 (GB)
OS ディスク	184.23	40.00	80.00	130.00
通常ディスク	28.56	4.00	10.00	20.00

[選択された空き領域] 列は、OS ディスクなどのディスクの種類のために選択したすべてのデータストア上の使用可能な合計領域を示します。

[推奨される最小領域] 列は、プールに対して推奨されるストレージの最小の容量を示します。

[50% の使用率] 列は、ディスクが親仮想マシンの 50% に拡大したときの推奨されるストレージを示します。

[推奨される最大領域] 列は、ディスクが親仮想マシン全体のサイズに近づいたときの推奨されるストレージを示します。

OS ディスクと通常ディスクを同じデータストアに格納する場合、View は、両方のディスクの種類のストレージ要件を計算します。[データの種類] には、特定のディスクの種類ではなく [リンク クローン] または [インスタント クローン] と表示されます。

View Composer レプリカを別のデータストアに格納する場合、この表にはレプリカのストレージに対する推奨値も示され、OS ディスクに対する推奨値が調整されます。

View Composer リンク クローンのサイズ設定ガイドライン

この表は、一般的なガイドラインを示します。ストレージの計算では、クローン内の実際のストレージの拡大に影響を与える可能性のある追加の要因を考慮する必要があります。

OS ディスクの場合、サイズ設定の見積もりは、プールの更新や再構成の頻度によって異なります。

リンク クローン プールを 1 日に 1 回～1 週間に 1 回の間で更新する場合は、[選択された空き領域] が [推奨される最小領域] から [50% の使用率] の概算までの間のストレージ使用に対応できることを確認します。

プールの更新や再構成をめったに行わない場合は、リンク クローン ディスクが拡大し続けます。[選択された空き領域] が [50% の使用率] から [推奨される最大領域] の見積もりまでの間のストレージ使用に対応できることを確認します。

通常ディスクの場合、サイズ設定の見積もりは、ユーザーがデスクトップ上に生成する Windows プロファイル データの量によって異なります。更新操作や再構成操作は、通常ディスクには影響を与えません。

既存のデスクトップ プールを編集する場合のサイズ設定ガイドライン

View によって、新しいクローンに必要なストレージ容量が見積もられます。デスクトップ プールを作成する場合は、サイズ設定ガイドラインはプール全体が対象となります。既存のデスクトップ プールを編集する場合は、プールに追加する新しいクローンのみがガイドラインの対象となります。

たとえば、デスクトップ プールに 100 個のクローンを追加し、新しいデータストアを選択する場合、新しいクローン 100 個に必要な容量が View によって見積もられます。

新しいデータストアを選択する場合でもデスクトップ プールを同じサイズに保つ場合、もしくはクローンの数を減らす場合などには、サイズ設定ガイドラインは 0 と示されます。値 0 は、選択されているデータストアで新しいクローンを作成する必要がないことを意味します。既存のクローンですでに容量要件に達しています。

View でのサイズ設定に対する最小の推奨値の計算方法

OS ディスクに対する最小の推奨値を得るために、View は、各クローンが最初に作成されて起動されるときに、そのクローンのメモリ サイズの 2 倍が消費されると見積もられます。クローンに対してメモリが予約されていない場合は、クローンがパワーオンされるとすぐに、そのクローンの ESXi スワップ ファイルが作成されます。また、ゲスト OS のページング ファイルのサイズも、クローンの OS ディスクの拡大に影響を与えます。

OS ディスクに対する最小の推奨値では、View は各データストア上の 2 つのレプリカの領域も含めます。View Composer は、プールが作成されるときにレプリカを 1 つ作成します。そのプールが初めて再構成されると、View Composer はデータストア上に 2 番目のレプリカを作成し、クローンを新しいレプリカに関連付けした後、他のクローンは元のスナップショットを使用していない場合は最初のレプリカを削除します。再構成操作中、データストアには 2 つのレプリカを格納するための容量が必要です。

デフォルトでは、レプリカは vSphere Thin Provisioning を使用しますが、ガイドラインをシンプルにするために、View は親仮想マシンと同じ領域を使用する 2 つのレプリカを計算に含めます。

通常ディスクに対する最小の推奨値を得るために、View は [デスクトップ プールを追加] ウィザードの [View Composer のディスク] ページで指定されたディスク サイズの 20% を計算します。

注: 通常ディスクの計算は、静的なしきい値 (GB 単位) に基づいています。たとえば、1024MB ~ 2047MB の任意の値の通常ディスク サイズを指定した場合、View は、この通常ディスク サイズを 1GB として計算します。2048MB のディスク サイズを指定した場合、View は、このディスク サイズを 2GB として計算します。

レプリカを別のデータストアに格納するための推奨値を得るために、View は、データストア上の 2 つのレプリカのための領域を考慮します。最小と最大の使用量に対して同じ値が計算されます。

詳細については、[インスタントクローン プールとリンク クローン プールのサイズ設定の式](#)を参照してください。

View Composer リンク クローンのサイズ設定ガイドラインとストレージ オーバーコミット

注: インスタント クローンはストレージ オーバーコミットをサポートしていません。

ユーザーがストレージ要件を見積もり、データストアを選択して、プールを展開した後、View は各データストア上の空き領域と既存のクローンに基づいて、それぞれのデータストア上のリンク クローン仮想マシンをプロビジョニングします。

[デスクトップ プールを追加] ウィザードの [リンク クローンのデータストアを選択] ページで選択されたストレージ オーバーコミット オプションに基づいて、View は新しいクローンのプロビジョニングを停止し、既存のクローンのために空き領域を予約します。この動作によって、データストア上の各マシンに対してバッファを拡大できるようになります。

ストレージ オーバーコミット レベルを高く設定した場合は、見積もりのストレージ要件が、[選択された空き領域] 列に示されている容量を超える可能性があります。ストレージ オーバーコミット レベルは、View がデータストア上に実際に作成する仮想マシンの数に影響を与えます。

詳細については、[リンククローン仮想マシンのストレージのオーバーコミット レベルの設定](#)を参照してください。

インスタントクローン プールとリンク クローン プールのサイズ設定の式

ストレージのサイズ設定の式は、OS ディスク、View Composer 通常ディスク、およびレプリカのために選択するデータストア上で必要なディスク容量を見積もるのに役立ちます。

注: 通常ディスクの情報は、View Composer リンク クローンのみを対象にしています。インスタント クローンは通常ディスクをサポートしていません。

ストレージのサイズ設定の式

表 16-2. 選択されたデータストア上のクローン ディスクのためのストレージのサイズ設定の式は、プールの作成時と、クローンが次第に拡大するにつれての、ディスクの見積もりサイズを計算する式を示しています。これらの式には、クローンとともにデータストアに格納されるレプリカ ディスクのための領域が含まれています。

既存のプールを編集するか、またはレプリカを別のデータストアに格納する場合、View は別のサイズ設定の式を使用します。[クローンを作成するためのサイズ設定の式（プールを編集する場合、またはレプリカを別のデータストアに格納する場合）](#)を参照してください。

表 16-2. 選択されたデータストア上のクローン ディスクのためのストレージのサイズ設定の式

データの種類	選択された空き領域 (GB)	推奨される最小領域 (GB)	50% Utilization (GB) (50% の使用率 (GB))	推奨される最大領域 (GB)
OS ディスク	選択されたデータストア上の空き領域	仮想マシンの数 * (2 * 仮想マシンのメモリ) + (2 * レプリカ ディスク)	VM の数 * (レプリカ ディスクの 50% + VM のメモリ) + (2 * レプリカ ディスク)	仮想マシンの数 * (レプリカ ディスクの 100% + 仮想マシンのメモリ) + (2 * レプリカ ディスク)
通常ディスク	選択されたデータストア上の空き領域	VM の数 * 通常ディスクの 20%	仮想マシンの数 * 通常ディスクの 50%	仮想マシンの数 * 通常ディスクの 100%

ストレージのサイズ設定の見積もりの例

この例では、親仮想マシンに 1GB のメモリが構成されています。親仮想マシンのディスク サイズは 10GB です。1 つのプールは 10 台のマシンで作成されています。通常ディスクのサイズは 2048MB として構成されています。

OS ディスクは、現在 184.23GB の使用可能な領域があるデータストア上に構成されています。通常ディスクは、28.56GB の使用可能な領域がある別のデータストア上に構成されています。

表 16-3. 選択されたデータストア上にデプロイされているクローン ディスクのサイズ設定の見積もりの例は、サイズ設定の式で、サンプルのデスクトップ プールの見積もりのストレージ要件を計算する方法を示しています。

表 16-3. 選択されたデータストア上にデプロイされているクローン ディスクのサイズ設定の見積もりの例

データの種類	選択された空き領域 (GB)	推奨される最小領域 (GB)	50% Utilization (GB) (50% の使用率 (GB))	推奨される最大領域 (GB)
OS ディスク	184.23	$10 * (2 * 1\text{GB}) + (2 * 10\text{GB}) = 40.00$	$10 * (10\text{GB の } 50\% + 1\text{GB}) + (2 * 10\text{GB}) = 80.00$	$10 * (10\text{GB の } 100\% + 1\text{GB}) + (2 * 10\text{GB}) = 130.00$
通常ディスク	28.56	$10 * (2\text{GB の } 20\%) = 4.00$	$10 * (2\text{GB の } 50\%) = 10.00$	$10 * (2\text{GB の } 100\%) = 20.00$

クローンを作成するためのサイズ設定の式（プールを編集する場合、またはレプリカを別のデータストアに格納する場合）

既存のデスクトップ プールを編集するか、またはレプリカを別のデータストアに格納する場合、View は、プールを初めて作成する場合とは異なるサイズ設定の式で計算します。

既存のプールを編集し、そのプールのデータストアを選択した場合、View Composer は選択されたデータストア上に新しいクローンを作成します。これらの新しいクローンは既存のスナップショットに関連付けられ、既存のレプリカ ディスクを使用します。新しいレプリカは作成されません。

View は、デスクトップ プールに追加された新しいクローンのサイズ要件を見積もります。既存のクローンは計算に含めません。

レプリカを別のデータストアに格納した場合は、他の選択したデータストアは OS ディスク専用に使われます。

表 16-4. クローン ディスクのためのストレージのサイズ設定の式（プールを編集する場合、またはレプリカを別のデータストアに格納する場合） は、プールを編集したりレプリカを別のデータストアに格納する際に、クローン ディスクの見積もりサイズを計算する式を示しています。

表 16-4. クローン ディスクのためのストレージのサイズ設定の式（プールを編集する場合、またはレプリカを別のデータストアに格納する場合）

データの種類	選択された空き領域 (GB)	推奨される最小領域 (GB)	50% Utilization (GB) (50% の使用率 (GB))	推奨される最大領域 (GB)
OS ディスク	選択されたデータストア上の空き領域	新しい仮想マシンの数 * (2 * 仮想マシンのメモリ)	新しい仮想マシンの数 * (レプリカ ディスクの 50% + 仮想マシンのメモリ)	新しい仮想マシンの数 * (レ プリカ ディスクの 100% + 仮想マシンのメモリ)
通常ディスク	選択されたデータストア上の空き領域	新しい仮想マシンの数 * 通常ディスクの 20%	新しい仮想マシンの数 * 通常ディスクの 50%	新しい仮想マシンの数 * 通 常ディスクの 100%

ストレージのサイズ設定の見積もりの例（プールを編集する場合、またはレプリカを別のデータストアに格納する場合）

この例では、親仮想マシンに 1GB のメモリが構成されています。親仮想マシンのディスク サイズは 10GB です。1 つのプールは 10 台のマシンで作成されています。通常ディスクのサイズは 2048MB として構成されています。

OS ディスクは、現在 184.23GB の使用可能な領域があるデータストア上に構成されています。通常ディスクは、28.56GB の使用可能な領域がある別のデータストア上に構成されています。

表 16-5. クローン ディスクのサイズ設定の見積もりの例（プールを編集する場合、またはレプリカを別のデータストアに格納する場合）は、サイズ設定の式で、サンプルのプールの見積もりのストレージ要件を計算する方法を示しています。

表 16-5. クローン ディスクのサイズ設定の見積もりの例（プールを編集する場合、またはレプリカを別のデータストアに格納する場合）

データの種類	選択された空き領域 (GB)	推奨される最小領域 (GB)	50% Utilization (GB) (50% の使用率 (GB))	推奨される最大領域 (GB)
OS ディスク	184.23	$10 * (2 * 1\text{GB}) = 20.00$	$10 * (10\text{GB の } 50\% + 1\text{GB}) = 60.00$	$10 * (10\text{GB の } 100\% + 1\text{GB}) = 110.00$
通常ディスク	28.56	$10 * (2\text{GB の } 20\%) = 4.00$	$10 * (2\text{GB の } 50\%) = 10.00$	$10 * (2\text{GB の } 100\%) = 20.00$

View Composer リンク クローン仮想マシンのストレージ オーバーコミット

ストレージ オーバーコミット機能を使用して、フル仮想マシンで可能な数より多くのリンククローン仮想マシンをデータストアに配置することによりストレージ コストを削減できます。リンク クローンは、データストアの物理容量の数倍の論理ストレージ領域を使用できます。

注: インスタント クローンはストレージ オーバーコミットをサポートしていません。

この機能は、データストアの容量をオーバーコミットできるストレージ レベルを選択して、View が作成するリンククローン数の制限を設定する際に役立ちます。プロビジョニングが控え目すぎるためにストレージを無駄にすることや、リンククローンがディスク領域を使い果たしてオペレーティング システムまたはアプリケーションに問題が発生するような事態になるのを避けることができます。

たとえば、各仮想マシンが 10 GB の場合、100 GB のデータストアに作成できるフル仮想マシンは最大でも 10 個です。10 GB の親仮想マシンからリンク クローンを作成した場合、各クローンのサイズはその何分の 1 になります。

オーバーコミット レベルを低く設定した場合、View はクローンがデータストアの物理サイズの 4 倍を使用することを可能にし、各クローンを親仮想マシンのサイズとして測定します。100 GB のデータストアで、親が 10 GB の場合、View は約 40 個のリンク クローンをプロビジョニングします。View は、データストアに空き領域がある場合でも、追加のクローンをプロビジョニングしません。この制限により、既存のクローン用のバッファの拡大を管理します。

表 16-6. ストレージのオーバーコミット レベルに、設定できるストレージのオーバーコミット レベルを示します。

表 16-6. ストレージのオーバーコミット レベル

オプション	ストレージのオーバーコミット レベル
なし	ストレージはオーバーコミットされません。
低	データストアのサイズの 4 倍。これはデフォルトのレベルです。

オプション	ストレージのオーバーコミット レベル
中	データストアのサイズの 7 倍。
高	データストアのサイズの 15 倍。

ストレージのオーバーコミット レベルはストレージ容量を決定するための大まかな目安になります。最適なレベルを決定するため、実際の環境でリンク クローンの増加を監視してください。

OS ディスクが可能な最大サイズまで増加することがない場合は、高いレベルを設定します。オーバーコミット レベルを高くする場合は注意が必要です。リンク クローンがディスク領域を使い果たすことがないようにするには、デスクトップ プールを定期的に更新または再分散し、リンク クローンの OS データをその元のサイズに縮小します。自動ファームでは、更新または再調整はサポートされていません。自動ファームのリンク クローンにディスク領域を使い果たす危険性がある場合、オーバーコミット レベルを変更します。

たとえば、ログオフ後に仮想マシンが削除または更新されるように設定されている流動割り当てデスクトップ プールの場合は、オーバーコミット レベルを高く設定することは有効です。

各データストアのさまざまなレベルのスループットに対応するため、データストアのタイプによって、ストレージのオーバーコミット レベルを変えることができます。たとえば、NAS データストアと SAN データストアを別の設定にすることができます。

リンククローン仮想マシンのストレージのオーバーコミット レベルの設定

ストレージ オーバーコミット機能を使用して、View がデータストアにどのようにリンククローン仮想マシンを作成するかを制御できます。この機能により、データストアの物理ストレージ上限を超える合計論理サイズになるリンク クローンを作成できます。

この機能はリンククローン プールおよび自動ファームでのみ機能します。

ストレージのオーバーコミット レベルは、各クローンがフル仮想マシンであった場合に使用するデータストアの物理サイズより大きくストレージの量を見積もります。詳細については、以下を参照してください。[View Composer リンク クローン仮想マシンのストレージ オーバーコミット](#)。次の手順は、リンククローン デスクトップ プールに適用されます。手順は、自動ファームの場合と同様です。

手順

- 1 View Administrator で、[カタログ] - [デスクトップ プール] を選択します。
- 2 新しいデスクトップ プールを作成するとき、または既存のプールを編集するときは、[vCenter 設定] ページに移動します。

オプション	アクション
新しいデスクトップ プール	<ol style="list-style-type: none"> a [追加] をクリックします。 b [vCenter 設定] ページが表示されるまで、[デスクトップ プールを追加] ウィザードの処理を続行します。
既存のデスクトップ プール	<ol style="list-style-type: none"> a リンククローン プールを選択し、[編集] をクリックします。 b [vCenter 設定] タブをクリックします。

- 3 [vCenter 設定] ページで、[データストア] の横にある [参照] をクリックします。

4 [リンク クローンのデータストアを選択] ページで、データストアを選択します。

選択したデータストアの [ストレージ オーバーコミット] 列にドロップダウン メニューが表示されます。

5 ドロップダウン メニューから、ストレージ オーバーコミット レベルを選択します。

オプション	説明
なし	ストレージはオーバーコミットされません。
低	データストアのサイズの 4 倍。これはデフォルトのレベルです。
中	データストアのサイズの 7 倍。
高	データストアのサイズの 15 倍。
境界なし	View は、データストアの物理的な容量に基づいて作成されるリンククローン マシンの数を制限しません。このレベルは、すべてのマシンとそれらの将来のデータ増加に対応するために、データストアに十分なストレージ容量があることが確実である場合に限り選択してください。

6 [OK] をクリックします。

View Composer リンククローン データ ディスク

View Composer は、リンククローン仮想マシンのコンポーネントを格納するための複数のデータ ディスクを作成します。

OS ディスク

View Composer は、リンク クローンごとに OS ディスクを作成します。このディスクには、基本イメージへのリンクを維持し、一意の仮想マシンとして機能するためにクローンが必要とするシステム データが格納されます。

QuickPrep 構成データ ディスク

View Composer は、OS ディスクとともに 2 つ目のディスクを作成します。2 つ目のディスクには、更新および再構成操作時に保持する必要がある QuickPrep 構成データおよびその他の OS 関連データが格納されます。このディスクは小容量で、通常、約 20MB です。仮想マシンをカスタマイズするため、このディスクは QuickPrep または Sysprep のどちらを使用した場合でも作成されます。

ユーザー プロファイルを格納するために個別の View Composer 通常ディスクを構成する場合、各リンク クローンには、OS ディスク、2 つ目の仮想マシン ディスク、および View Composer 通常ディスクの 3 つのディスクが関連付けられます。

2 つ目の仮想マシン ディスクは、OS ディスクと同じデータストアに格納されます。このディスクを構成することはできません。

View Composer 通常ディスク

専用割り当てプールでは、Windows ユーザー プロファイル データを格納するために別個の View Composer 通常ディスクを構成できます。このディスクはオプションです。

別個の通常ディスクを使用すると、ユーザー データおよび設定を保持できます。View Composer の更新、再構成、および再分散操作は、通常ディスクに影響を与えません。通常ディスクをリンク クローンから切断し、別のリンク クローンに接続することができます。

別個の通常ディスクを構成しない場合、Windows プロファイルは OS ディスクに格納されます。ユーザー データおよび設定は、更新、再構成、および再分散操作時に削除されます。

通常ディスクは OS ディスクと同じデータストアまたは別のデータストアに格納できます。

破棄可能データ ディスク

リンク クローン プールを作成するときに、ユーザー セッション中に生成されるゲスト OS のページング ファイルと一時ファイルを格納するために別の読み取り専用ディスクを構成することができます。ディスク サイズはメガバイト単位で指定する必要があります。

このディスクはオプションです。

リンク クローンがパワーオフされると、View は破棄可能データ ディスクを、View Composer がリンク クローン プールで作成した元のディスクのコピーに置き換えます。ユーザーがデスクトップを操作するたびに、リンク クローンのサイズが増える可能性があります。破棄可能データ ディスクを使用すると、リンク クローンの拡大を抑えることでストレージ領域を節約できます。

破棄可能データ ディスクは、OS ディスクと同じデータストアに格納します。

ローカル データストアへの View Composer リンク クローンの保存

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

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

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

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

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

- VMotion を使用して、ボリュームを管理することはできません。

- リソース プール全体で仮想マシンの負荷分散を行うことはできません。たとえば、ローカル データストアに保存されたリンク クローンでは、View Composer 再分散操作を使用できません。
- VMware High Availability は使用できません。
- vSphere Distributed Resource Scheduler (DRS) は使用できません。
- View Composer レプリカがローカル データストアにある場合、異なるデータストアに View Composer レプリカまたはリンク クローンを保存できません。

ローカル データストアにリンク クローンを保存している場合、リンク クローンと同じボリュームにレプリカを保存することを強く推奨します。クラスターのすべての ESXi ホストがレプリカにアクセスできる場合、リンク クローンをローカル データストアに保存し、レプリカを共有データストアに保存することもできますが、VMware ではこの構成は推奨しません。

- ローカル スピニングディスク ドライブを選択する場合、市販のストレージ アレイのパフォーマンスよりも劣る可能性があります。ローカル スピニングディスク ドライブとストレージ アレイは同様の容量である可能性がありますが、ローカル スピニングディスク ドライブには、ストレージ アレイほどのスループットはありません。スピンドルの数が増えれば、スループットも向上します。

直接接続のソリッド ステート ディスク (SSD) を選択する場合、ほとんどの場合、多くのストレージ アレイを超えるパフォーマンスが出ます。

単一の ESXi ホストまたは単一の ESXi ホストを含むクラスターでデスクトップ プールまたはファームを構成すれば、制限なしにローカル データストアにリンク クローンを保存できます。ただし、単一の ESXi ホストを使用すると、構成可能なデスクトップ プールまたはファームのサイズが制限されます。

大容量のデスクトップ プールまたはファームを構成するには、複数の ESXi ホストを含むクラスターを選択して集合的な容量を確保し、多数の仮想マシンに対応するようにする必要があります。

ローカル ストレージの利点を活用するのであれば、VMotion、HA、DRS およびその他の機能を利用できない重大性を慎重に考慮する必要があります。仮想マシンの数とディスクの増加を制御して、ローカル ディスク使用率を管理しており、流動割り当てを使用し、定期的な更新および削除操作を実行している場合、ローカル データストアにリンク クローンを正しく展開できます。

インスタント クローンおよび View Composer リンク クローン用の別のデータストアへのレプリカおよびクローンの格納

レプリカとクローンを、パフォーマンス特性の異なる別々のデータストアに配置できます。この構成により、特に View Composer リンク クローンの場合は、プロビジョニングしたりウイルス対策を実行したりするなどのディスクを多用する操作を迅速に行うことができます。

たとえば、レプリカ仮想マシンをソリッド ステート ディスク対応のデータストアに格納できます。ソリッド ステート ディスクは、ストレージ容量が少なく、読み取りのパフォーマンスが高く、通常、1 秒あたり 20,000 I/O (IOPS) をサポートします。一般的な環境に存在するレプリカ数はわずかなため、レプリカはあまりストレージ領域を必要としません。

クローンは従来の回転メディア対応のデータストアに格納できます。これらのディスクは、パフォーマンスが低く、通常、200 IOPS をサポートします。安価で大容量のため、多数のクローンを格納する場合に適しています。

レプリカとクローンをこの方法で構成すると、特に View Composer リンク クローンの場合は、一度に多くのクローンが作成されるときに発生する I/O ストームの影響を軽減できます。たとえば、ログオフ時にマシンを削除するポリシーを使用して流動割り当てプールを展開した場合、ユーザーが同時に作業を開始すると、View はユーザー用の新しいマシンを同時にプロビジョニングする必要があります。

重要: この機能は、高パフォーマンスのディスク ソリューションを提供するベンダが使用する特定のストレージ構成向けに設計されています。ストレージ ハードウェアが高い読み取りパフォーマンスをサポートしていない場合は、レプリカを別のデータストアに保存しないでください。

レプリカとクローンを別のデータストアのプールに格納する場合は、特定の要件に従う必要があります。

- 1 つのプールに指定できる別のレプリカ データストアは 1 つだけです。
- レプリカ データストアは、クラスタ内のすべての ESXi ホストからアクセスできる必要があります。
- View Composer リンク クローンについては、ローカル データストアにクローンを配置している場合、リンク クローンと同じボリュームにレプリカを保存することを強く推奨します。クラスタのすべての ESXi ホストがレプリカにアクセスできる場合、リンク クローンをローカル データストアに保存し、レプリカを共有データストアに保存することもできますが、VMware ではこの構成は推奨しません。
- Virtual SAN データストアまたは Virtual Volumes データストアを使用する場合、この機能は使用できません。これらのタイプのデータストアでは、ソフトウェア ポリシーベース管理が使用されるため、ストレージ プロファイルにより、どのコンポーネントでどのタイプのディスクを使用するかを定義します。

別のデータストアにレプリカを格納する際の可用性に関する考慮事項

レプリカ仮想マシンを別のデータストア、またはクローンと同じデータストアに格納できます。これらの構成は、さまざまな形でプールの可用性に影響を与えます。

レプリカをクローンと同じデータストアに格納すると、可用性を向上させるために、各データストアに個別のレプリカが作成されます。データストアが使用できなくなった場合、そのデータストアのクローンのみが影響を受けます。他のデータストアのクローンは引き続き動作します。

レプリカを別のデータストアに格納すると、プール内のすべてのクローンがそのデータストアのレプリカに関連付けられます。データストアが使用できなくなった場合、プール全体が使用できなくなります。

デスクトップ プールの可用性を高めるために、レプリカを格納するデータストアに対して高可用性ソリューションを構成することができます。

View Composer リンク クローン用の View Storage Accelerator の構成

ESXi ホストが仮想マシンのディスク データをキャッシュできるよう View Composer リンク クローン デスクトップ プールを構成できます。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。View Storage Accelerator により、ブート ストーム発生時（多くのマシンが一斉に起動するか、ウイルス対策スキャンを同時に実行する場合など）の IOPS を削減し、パフォーマンスを向上させることが可能です。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。この機能を使用するには、個別のデスクトップ プールに対して View Storage Accelerator が有効であることを確認する必要があります。

注: 既存のリンククローン デスクトップ プールで View Storage Accelerator を有効にしたときに、View Storage Accelerator に対してレプリカがそれまで有効ではなかった場合、この機能はすぐに有効にならないことがあります。View Storage Accelerator は、レプリカの使用中には有効になりません。View Storage Accelerator は、デスクトップ プールを新しい親仮想マシンに再構成することで、強制的に有効にすることができます。インスタント クローン の場合、この機能は自動的に有効になり、構成できません。

仮想マシンを作成すると、View は各仮想ディスク ファイルの内容にインデックスを付けます。インデックスは仮想マシンのダイジェスト ファイルに格納されます。実行時に、ESXi ホストはそのダイジェスト ファイルを読み取り、データの共通ブロックをメモリにキャッシュします。ESXi ホストのキャッシュを最新に保つために、指定した間隔で、および仮想マシンが再構成されるときに、View でダイジェスト ファイルが再生成されます。再生成の間隔は変更可能です。

リンク クローンを含むプールと、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。

View Storage Accelerator は、デフォルトで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。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。

View Storage Accelerator は、View レプリカ階層を使用する構成で動作するために適しており、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。View 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でレプリカを保存することによって実現できます。その結果、この組み合わせはテストおよびサポートされます。

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 View 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 View 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 5.0 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 5.0 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 ユーザーに必要な View および View Composer の権限については、『View のインストール』マニュアルのトピックを参照してください。
- View Storage Accelerator が vCenter Server で有効になっていることを確認します。『View 管理ガイド』を参照してください。

手順

- 1 View Administrator で、[[詳細なストレージ]] ページを表示します。

オプション	説明
新しいデスクトップ ツール (推奨)	[デスクトップ プールを追加] ウィザードを起動して、自動デスクトップ プールの作成を開始します。ウィザードの構成に関する指示に従って、[[詳細なストレージ]] ページが表示されるまで進みます。
既存のデスクトップ プール	既存のプールを選択し、[編集] をクリックして、[詳細なストレージ] タブをクリックします。既存のデスクトップ プールの View Storage Accelerator の設定を変更すると、デスクトップ プールの仮想マシンがパワーオフするまで、変更は有効になりません。

- 2 プール用に View Storage Accelerator を有効にするには、[View Storage Accelerator を使用] 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、この設定はオンになっています。この設定を無効にするには、[View Storage Accelerator を使用] ボックスをオフにします。

- 3 (オプション) [ディスク タイプ] メニューから [OS ディスク] のみを選択するか [OS ディスクと通常ディスク] を選択することで、キャッシュするディスク タイプを指定します。

デフォルトでは、[OS ディスク] が選択されています。

フル仮想マシンに対して View Storage Accelerator を構成する場合、ディスク タイプは選択できません。View Storage Accelerator は、仮想マシン全体で実行されます。

- 4 (オプション) [次の期間後にストレージ アクセラレータを再作成] テキスト ボックスで、View Storage Accelerator ダイジェスト ファイルの再生成までの間隔を日数で指定します。

デフォルトの再生成までの間隔は、7 日間です。

次のステップ

ディスク領域再利用と View Storage Accelerator の再生成が行われない停電期間を日数および時間で構成できます。[View Composer リンク クローン用の Storage Accelerator と領域再利用の停電期間の設定](#)を参照してください。

既存のプールを編集して View Storage Accelerator 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、デスクトップ 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します。

View Composer リンク クローンでのディスク領域の再利用

vSphere 5.1 以降では、View Composer リンククローン デスクトップ プールおよび自動ファームに対してディスク領域再利用機能を構成できます。vSphere 5.1 から、View は、ESXi ホストがリンク クローン上の未使用ディスク領域を再利用できるようにする効率の良いディスク フォーマットでリンク クローン仮想マシンを作成するようになったため、リンク クローンに必要なストレージの合計領域が減少しました。

注: インスタント クローンはユーザーのログアウト時に常に再作成されるので、この機能は必要ありません。

ユーザーが仮想マシンを操作するたびに、リンク 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仮想マシン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。領域は、仮想マシンがパワーオンしていて、ユーザーがマシンを操作している間に再利用できます。

View Administrator では、ディスク領域再利用をプールに対して直接開始できません。View がディスク領域再利用を開始するタイミングを決定するには、操作をトリガーする、リンク クローン OS ディスク上に蓄積する必要がある未使用ディスク領域の最小量を指定します。未使用ディスク領域が指定したしきい値を超過すると、View は ESXi ホストにその OS ディスク上の未使用領域を再利用するように指示します。View は、しきい値をプール内の仮想マシンごとに適用します。

`vdmadmin -M` オプションを使用すると、デモまたはトラブルシューティングの目的で、特定の仮想マシンでディスク領域再利用を開始することができます。『View 管理ガイド』を参照してください。

新しいプールを作成するとき、または既存のプールを編集するときに、リンク クローン上でディスク領域再利用を構成できます。既存のプールについては、『View アップグレード ガイド』の「領域を再利用するためにプールをアップグレードする作業」を参照してください。

注: Virtual SAN データストアまたは仮想ボリューム

View Composer がリンク クローンを更新、再構成または再分散している場合、ディスク領域再利用はそのリンク クローン上では実行されません。

ディスク領域再利用は、リンク クローン内の OS ディスクのみで動作します。この機能は、View Composer の通常ディスクに影響せず、完全クローン仮想マシンでは動作しません。

ネイティブ NFS スナップショットテクノロジー (VAAI) 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。

次の手順は、リンククローン デスクトップ プールに適用されます。手順は、自動ファームの場合と同様です。

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。
- vSphere バージョン 5.1 以降で提供される VMware Tools が、プール内のすべてのリンク クローン仮想マシンにインストールされていることを確認します。
- プール内のすべてのリンク クローン仮想マシンが仮想ハードウェア バージョン 9 以降であることを確認します。
- 仮想マシンが SCSI コントローラを使用することを確認します。ディスク領域再利用は、IDE コントローラを備えた仮想マシンではサポートされていません。
- Windows 10 仮想マシンの場合、マシンが vSphere 5.5 U3 以降で実行されていることを確認します。
- Windows 8 または 8.1 仮想マシンの場合、マシンが vSphere 5.5 以降で実行されていることを確認します。ディスク領域の再利用は、vSphere 5.5 以降で実行されている Windows 8 または 8.1 仮想マシンでサポートされます。
- Windows 7 仮想マシンの場合、マシンが vSphere 5.1 以降で実行されていることを確認します。

- ディスク領域再利用が vCenter Server で有効になっていることを確認します。このオプションにより、プール内の仮想マシンは、ディスク領域再利用に必要な効率の良いディスク フォーマットで作成されるようになります。『View 管理ガイド』を参照してください。

手順

- 1 View Administrator で、[詳細なストレージ] ページを表示します。

オプション	説明
新しいデスクトップ プール	[デスクトップ プールを追加] ウィザードを起動して、自動デスクトップ プールの作成を開始します。ウィザードの構成に関する指示に従って、[[詳細なストレージ]] ページが表示されるまで進みます。
既存のデスクトップ プール	既存のプールを選択し、[編集] をクリックして、[詳細なストレージ] タブをクリックします。領域再利用をサポートするためにプールをアップグレードする場合は、『View アップグレードガイド』の「領域再利用のためのデスクトップ プールのアップグレード」を参照してください。

- 2 [VM ディスク スペースを再利用] チェック ボックスを選択します。
- 3 [仮想マシンの未使用領域が次の値を超えると再利用が開始されます] テキスト ボックスに、リンク クローン OS ディスク上に蓄積する必要がある未使用のディスク領域の最小量 (GB) を入力します。この値を超過すると、ESXi はそのディスク上で領域の再利用を開始します。

例：2 GB。

デフォルト値は 1 GB です。

次のステップ

ディスク領域の再利用と View Storage Accelerator での再生成を実行しない停電日数と停電時間数を構成できます。[View Composer リンク クローン用の Storage Accelerator と領域再利用の停電期間の設定](#)を参照してください。

View Administrator で、[カタログ] - [デスクトップ プール] を選択し、領域再利用が行われた最終時刻とデスクトップ上で最後に再利用された領域の容量を表示するマシンを選択します。

View Composer リンク クローン用の VAAI ストレージの使用

vStorage APIs for Array Integration (VAAI) をサポートする NAS デバイスがデプロイに含まれている場合、View Composer リンク クローン プールで View Composer Array Integration (VCAI) 機能を有効にすることができます。この機能では、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。

注: Horizon 7.0 では、インスタント クローンは VAAI をサポートしていません。

このテクノロジーを使用すると、ESXi ホストでデータの読み取りや書き取りをすることなく、NFS ディスク アレイで仮想マシンのクローンが作成されます。この操作で仮想マシンのクローンが作成されると、時間が短縮され、ネットワーク負荷が軽減されることがあります。

ネイティブ NFS スナップショット テクノロジーを使用する場合は、次のガイドラインに従ってください。

- この機能を使用できるのは、VAAI を介したネイティブ クローン作成操作をサポートする NAS デバイスに存在するデータストアでデスクトップ プールまたは自動ファームを構成する場合だけです。
- View Composer 機能を使用して、ネイティブ NFS スナップショット テクノロジーで作成されたリンク クローンを管理できます。たとえば、通常ディスクの更新、再構成、再分散、作成が可能です。また、作成されたクローンで QuickPrep カスタマイズ スクリプトを実行できます。
- レプリカと OS ディスクを別々のデータストアに格納している場合、この機能は使用できません。
- この機能は vSphere 5.0 以降でサポートされています。
- プールを編集し、ネイティブ NFS クローン作成機能の選択または選択解除を行っても、既存の仮想マシンは影響を受けません。

既存の仮想マシンをネイティブ NFS クローンから従来の REDO ログ クローンに変更するには、ネイティブ NFS クローン作成機能の選択を解除し、新しい基本イメージに対してプールを再構成する必要があります。プール内のすべての仮想マシンについてクローン作成方法を変更し、別のデータストアを使用するには、新しいデータストアを選択し、ネイティブ NFS クローン作成機能の選択を解除して、新しいデータストアにプールを再分散し、新しい基本イメージに対してプールを再構成する必要があります。

同様に、仮想マシンを従来の REDO ログ クローンからネイティブ NFS クローンに変更するには、VAAI をサポートする NAS データストアを選択し、ネイティブ NFS クローン作成機能を選択して、NAS データストアにプールを再分散し、プールを再構成します。詳細については、<http://kb.vmware.com/kb/2088995> を参照してください。

- ESXi クラスターの View Administrator で選択された NFS データストアでネイティブ クローン作成機能を構成するには、クラスター内のすべての ESXi ホストの VAAI でネイティブ クローン作成操作をサポートするベンダー固有の NAS プラグインをインストールしなければならない場合があります。構成要件のガイダンスについては、ストレージ ベンダーのドキュメントを参照してください。
- ネイティブ NFS スナップショット テクノロジー (VAAI) 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ではサポートされていません。
- Virtual SAN データストアまたは Virtual Volumes データストアを使用する場合、この機能は使用できません。
- View での VCAI サポートの FAQ については、VMware ナレッジベース (KB) の記事 2061611 を参照してください。

重要: NAS ストレージ ベンダーは、VAAI のパフォーマンスおよび操作に影響を及ぼす追加設定を用意している場合があります。ベンダーの推奨事項に従い、NAS ストレージ アレイと ESXi の両方で適切な設定を構成する必要があります。ベンダーの推奨設定の構成に関するガイダンスについては、ストレージ ベンダーのドキュメントを参照してください。

View Composer リンク クローン用の Storage Accelerator と領域再利用の停電期間の設定

View Composer リンク クローンでは、View Storage Accelerator のダイジェスト ファイルの再生成および仮想マシン ディスク領域の再利用で、ESXi のリソースを使用できます。必要に応じて ESXi のリソースがフォアグラウンドタスク専用になるように、ESXi ホストでこれらの操作を実行しない日時を指定できます。

注: インスタント クローンの場合、この機能は必要ありません。

たとえば、ユーザーが業務を開始する平日の午前中、起動時、ウイルス対策スキャンの I/O ストーム発生時に、停電期間を指定できます。さまざまな日の時間帯を指定することが可能です。

設定した停電期間中は、ディスク領域の再利用および View Storage Accelerator ダイジェスト ファイルの再生成は行われません。各操作に個別の停電期間を設定することはできません。

停電期間が有効な場合でも、View では、プロビジョニング ステージで新しいマシン用の View Storage Accelerator ダイジェスト ファイルを作成することができます。

次の手順は、リンククローン デスクトップ プールに適用されます。手順は、自動ファームの場合と同様です。

前提条件

- [View Storage Accelerator を有効にする] または [領域再利用を有効にする]、あるいは両方の機能が、vCenter Server で選択されていることを確認します。
- [View Storage Accelerator を使用] または [VM ディスク スペースを再利用]、あるいは両方の機能が、デスクトップ プールで選択されていることを確認します。

手順

- 1 [デスクトップ プールを追加] ウィザードの [詳細なストレージ] ページで、[停電期間] に移動し、[追加] をクリックします。
既存のプールを編集している場合は、[詳細なストレージ] タブをクリックします。
- 2 停止日数を確認し、開始時刻と終了時刻を指定します。
時刻は 24 時間制で選択します。たとえば、10:00 は午前 10:00、22:00 は午後 10:00 です。
- 3 [OK] をクリックします。
- 4 別の停止期間を追加するには、[追加] をクリックし、別の期間を指定します。
- 5 停電期間を変更または削除するには、[停電期間] リストから期間を選択し、[編集] または [削除] をクリックします。

デスクトップ プールとアプリケーション プールのポリシーの構成

17

デスクトップ プール、アプリケーション プール、マシン、およびユーザーの動作を制御するポリシーを構成できます。View Administrator を使用して、クライアント セッションのポリシーを設定できます。Active Directory グループ ポリシー設定を使用して、シングルユーザー マシン、RDS ホスト、PCoIP、または VMware Blast に影響を及ぼす、Horizon Agent の動作、Windows 用 Horizon Client の動作、および各種機能の動作を制御できます。

この章には、次のトピックが含まれています。

- [View Administrator でのポリシーの設定](#)
- [スマート ポリシー の使用](#)
- [Active Directory グループ ポリシーの使用](#)
- [View グループ ポリシー管理用テンプレート ファイルの使用](#)
- [View ADM および ADMX テンプレート ファイル](#)
- [Horizon Agent の構成 ADM テンプレートの設定](#)
- [PCoIP ポリシー設定](#)
- [VMware Blast ポリシー設定](#)
- [リモート デスクトップ サービス グループ ポリシーの使用](#)
- [ロケーションベースの印刷の設定](#)
- [Active Directory グループ ポリシーの例](#)

View Administrator でのポリシーの設定

View Administrator を使用して、クライアント セッションのポリシーを構成できます。

これらのポリシーを設定して、特定のユーザー、特定のデスクトップ プール、またはすべてのクライアント セッション ユーザーに適用できます。特定のユーザーとデスクトップ プールに適用するポリシーは、ユーザー レベルのポリシーおよびデスクトップ プール レベルのポリシーと呼ばれます。すべてのセッションとユーザーに適用するポリシーはグローバル ポリシーと呼ばれます。

ユーザー レベルのポリシーでは、対応するデスクトップ プール レベルのポリシー設定から設定が継承されます。同様に、デスクトップ プール レベルのポリシーでは、対応するグローバル ポリシー設定から設定が継承されます。デスクトップ プール レベルのポリシー設定は、対応するグローバル ポリシー設定より優先されます。ユーザー レベルのポリシー設定は、対応するグローバル ポリシー設定およびデスクトップ プール レベルのポリシー設定より優先されます。

低いレベルのポリシー設定は、対応する高いレベルの設定より、制限を厳しくすることも緩くすることもできます。たとえば、グローバル ポリシーを [拒否] に設定し、対応するデスクトップ プール レベルのポリシーを [許可] に設定することも、この逆に設定することもできます。

注: RDS デスクトップおよびアプリケーション プールでは、グローバル ポリシーのみを使用できます。RDS デスクトップおよびアプリケーション プールに対して、ユーザー レベル ポリシーまたはプール レベル ポリシーを設定することはできません。

グローバル ポリシー設定の構成

すべてのクライアント セッション ユーザーの動作を制御するグローバル ポリシーを構成できます。

前提条件

ポリシーの説明を理解しておきます。[View ポリシー](#)を参照してください。

手順

- 1 View Administrator で、[ポリシー] - [グローバル ポリシー] を選択します。
- 2 [View ポリシー] ペインで [ポリシーを編集] をクリックします。
- 3 [OK] をクリックして変更を保存します。

デスクトップ プールのポリシーの構成

特定のデスクトップ プールに影響を与えるデスクトップ レベルのポリシーを構成できます。デスクトップ レベルのポリシー設定は、対応するグローバル ポリシー設定より優先されます。

前提条件

ポリシーの説明を理解しておきます。[View ポリシー](#)を参照してください。

手順

- 1 View Administrator で、[カタログ] - [デスクトップ プール] を選択します。
- 2 デスクトップ プールの ID をダブルクリックし、[ポリシー] タブをクリックします。
[ポリシー] タブには、現在のポリシー設定が表示されます。設定が対応するグローバル ポリシーから継承されている場合は、[デスクトップ プール ポリシー] 列に [継承] と表示されます。
- 3 [View ポリシー] ペインで [ポリシーを編集] をクリックします。
- 4 [OK] をクリックして変更を保存します。

ユーザーのポリシーの構成

特定のユーザーに影響を与えるユーザー レベルのポリシーを構成できます。ユーザー レベルのポリシー設定は、常に、対応するグローバルおよびデスクトップ プール レベルのポリシー設定より優先されます。

前提条件

ポリシーの説明を理解しておきます。[View ポリシー](#)を参照してください。

手順

- 1 View Administrator で、[カタログ] - [デスクトップ プール] を選択します。
- 2 デスクトップ プールの ID をダブルクリックし、[ポリシー] タブをクリックします。
[ポリシー] タブには、現在のポリシー設定が表示されます。設定が対応するグローバル ポリシーから継承されている場合は、[デスクトップ プール ポリシー] 列に [継承] と表示されます。
- 3 [ユーザーによる上書き] をクリックし、[ユーザーの追加] をクリックします。
- 4 ユーザーを見つけるには、[追加] をクリックし、ユーザーの名前または説明を入力して、[検索] をクリックします。
- 5 リストから 1 名以上のユーザーを選択し、[OK] をクリックし、[次へ] をクリックします。
Add Individual Policy（個別のポリシーの追加）ダイアログ ボックスが表示されます。
- 6 View ポリシーを構成し、[終了] をクリックして変更を保存します。

View ポリシー

すべてのクライアント セッションに影響を与えるように View ポリシーを構成することも、特定のデスクトップ プールまたはユーザーに影響を与えるように View ポリシーを適用することもできます。

[表 17-1. View ポリシー](#) 各 View ポリシー設定について説明します。

表 17-1. View ポリシー

ポリシー	説明
マルチメディア リダイレクト (MMR)	<p>クライアント システムで MMR を有効にするかどうかを指定します。</p> <p>MMR は Windows Media Foundation のフィルタであり、マルチメディア データをリモート デスクトップ上の特定のコーデックから TCP ソケット経由で直接クライアント システムに転送します。その後、データはクライアント システム上で直接デコードされ、そこで再生されます。</p> <p>デフォルト値は [拒否] です。</p> <p>クライアント システムにローカル マルチメディアのデコードを処理する十分なリソースがない場合、設定を [拒否] のままにします。</p> <p>マルチメディア リダイレクト (MMR) データは、アプリケーション ベースの暗号化なしでネットワークを介して送信され、リダイレクトされる内容によっては機密データが含まれる場合があります。このデータがネットワークで盗まれないことを保証するには、セキュア ネットワークで MMR だけを使用してください。</p>
USB Access (USB アクセス)	<p>リモート デスクトップがクライアント システムに接続されている USB デバイスを使用できるかどうかを指定します。</p> <p>デフォルト値は [許可] です。セキュリティ上の理由のため、外部デバイスを使用できないようにするには、設定を [拒否] に変更します。</p>
PCoIP ハードウェアのアクセラレーション	<p>PCoIP 表示プロトコルのハードウェアのアクセラレーションを有効にするかどうか、および PCoIP ユーザー セッションに割り当てられるアクセラレーションの優先度を指定します。</p> <p>この設定は、リモート デスクトップをホストする物理コンピュータ上に PCoIP ハードウェアのアクセラレーション デバイスが存在する場合にのみ有効です。</p> <p>デフォルト値は [許可] で、優先度が [中] です。</p>

スマート ポリシー の使用

スマート ポリシー を使用して、特定のリモート デスクトップでの USB リダイレクト、仮想印刷、クリップボード リダイレクト、クライアント ドライブ リダイレクト、および PCoIP 表示プロトコル機能の動作を制御できます。

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

スマート ポリシー の要件

スマート ポリシー を使用するには、View 環境が特定の要件を満たす必要があります。

- スマート ポリシー で管理するリモート デスクトップに、Horizon Agent 7.0 以降と VMware User Environment Manager 9.0 以降をインストールする必要があります。
- スマート ポリシー で管理するリモート デスクトップに接続するには、ユーザーが Horizon Client 4.0 以降を使用する必要があります。

User Environment Manager のインストール

スマート ポリシーを使用して、リモート デスクトップ機能の動作を制御するには、User Environment Manager 9.0 以降をリモート デスクトップにインストールする必要があります。

User Environment Manager インストーラは、VMware ダウンロード ページからダウンロードできます。User Environment Manager を使用して管理する各リモート デスクトップに VMware UEM FlexEngine クライアント コンポーネントをインストールする必要があります。User Environment Manager 環境を管理する任意のデスクトップに User Environment Manager 管理コンソール コンポーネントをインストールできます。

リンククローン プールの場合、リンク クローンの基本イメージとして使用する親仮想マシンに User Environment Manager をインストールします。RDS デスクトップ プールの場合、RDS デスクトップ セッションを提供する RDS ホストに User Environment Manager をインストールします。

User Environment Manager のシステム要件および完全なインストール手順については、『User Environment Manager 管理者ガイド』ドキュメントを参照してください。

User Environment Manager の構成

リモート デスクトップ機能のスマート ポリシーを作成するには、User Environment Manager を構成してから使用する必要があります。

User Environment Manager を構成するには、『User Environment Manager 管理者ガイド』の構成手順に従います。次の構成手順は、上記ドキュメントの情報を補足します。

- VMware UEM FlexEngine クライアント コンポーネントをリモート デスクトップに構成するとき、FlexEngine のログオン スクリプトとログオフ スクリプトを作成します。ログオン スクリプトには **-HorizonViewMultiSession -r** パラメータを使用し、ログオフ スクリプトには **-HorizonViewMultiSession -s** パラメータを使用します。

注: リモート デスクトップの他のアプリケーションの起動にログオン スクリプトを使用しないでください。追加のログオン スクリプトにより、リモート デスクトップのログオンが最大 10 分間遅延する可能性があります。

- リモート デスクトップのユーザー グループ ポリシー設定 **Run logon scripts synchronously** を有効にします。この設定はユーザーの構成\ポリシー\管理用テンプレート\システム\スクリプト フォルダにあります。
- リモート デスクトップのコンピュータ グループ ポリシー設定 **Always wait for the network at computer startup and logon** を有効にします。この設定はコンピュータの構成\管理用テンプレート\システム\ログオン フォルダにあります。
- Windows 8.1 リモート デスクトップの場合、コンピュータ グループ ポリシー設定 **Configure Logon Script Delay** を無効にします。この設定はコンピュータの構成\管理用テンプレート\システム\グループ ポリシー フォルダにあります。
- ユーザーがデスクトップ セッションに再接続すると Horizon のスマート ポリシー設定が更新されるようにするには、User Environment Manager 管理コンソールを使用してトリガされるタスクを作成します。トリガを [セッションの再接続]、アクションを [ユーザー環境の更新] に設定し、更新に [Horizon スマート ポリシー] を選択します。

注: トリガされるタスクの作成が、ユーザーのリモート デスクトップへのログイン中に行われた場合、デスクトップからログオフして、トリガされるタスクを有効にする必要があります。

Horizon スマート ポリシー設定

User Environment Manager で Horizon スマート ポリシーを作成して、リモート デスクトップ機能の動作を制御します。

表 17-2. Horizon スマート ポリシー設定では、User Environment Manager で Horizon スマート ポリシーを定義する場合に選択できる設定について説明します。

表 17-2. Horizon スマート ポリシー設定

設定	説明
USB リダイレクト	リモート デスクトップで USB リダイレクトを有効にするかどうかを指定します。USB リダイレクト機能により、ユーザーはリモート デスクトップから小型のフラッシュ ドライブ、カメラ、プリンタなどのローカルで接続された USB デバイスを使用できます。
印刷	リモート デスクトップで仮想印刷を有効にするかどうかを指定します。仮想印刷機能により、ユーザーはリモート デスクトップからクライアント コンピュータに接続された仮想プリンタまたは USB プリンタに印刷できます。
クリップボード	<p>クリップボード リダイレクトを許可する方向を決定します。次のいずれかの値を選択できます。</p> <ul style="list-style-type: none"> ■ [無効化]。クリップボード リダイレクトは両方の方向で無効になります。 ■ [すべて許可]。クリップボード リダイレクトが有効になります。ユーザーは、クライアント システムからリモート デスクトップ、およびリモート デスクトップからクライアント システムにコピーして貼り付けることができます。 ■ [クライアントからエージェントへのコピーを許可]。ユーザーは、クライアント システムからリモート デスクトップにのみコピーして貼り付けることができます。 ■ [エージェントからクライアントへのコピーを許可]。ユーザーは、リモート デスクトップからクライアント システムにのみコピーして貼り付けることができます。
クライアント ドライブ リダイレクト	<p>リモート デスクトップでクライアント ドライブ リダイレクトを有効にするかどうかと、共有ドライブおよびフォルダを書き込み可能にするかどうかを指定します。次のいずれかの値を選択できます。</p> <ul style="list-style-type: none"> ■ [無効化]。リモート デスクトップでクライアント ドライブ リダイレクトが無効になります。 ■ [すべて許可]。クライアント ドライブおよびフォルダは、リモート デスクトップと共有され、読み取り/書き込み可能になります。 ■ [読み取り専用]。クライアント ドライブおよびフォルダは、リモート デスクトップと共有され、読み取り可能になりますが、書き込みはできません。 <p>この設定を構成しない場合、共有ドライブおよびフォルダが書き込み可能になるかどうかは、ローカル レジストリ設定によって決まります。詳細については、レジストリ設定を使用したクライアント ドライブ リダイレクトの構成を参照してください。</p>
帯域幅プロファイル	<p>リモート デスクトップの PCoIP および Blast セッションの帯域幅プロファイルを構成します。[LAN] などの事前定義帯域幅プロファイルを選択できます。事前定義帯域幅プロファイルを選択すると、エージェントはリンク容量よりも高い速度で送信を試行できなくなります。デフォルトのプロファイルを選択した場合、最大帯域幅は毎秒 90,000 kbps になります。</p> <p>詳細については、帯域幅プロファイル リファレンスを参照してください。</p>
HTML Access ファイル転送	クライアントとエージェント間の HTML ファイルの転送を決定します。

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

帯域幅プロファイル リファレンス

スマート ポリシーでは、帯域幅プロファイルのポリシー設定を使用して、リモート デスクトップ上の PCoIP または Blast セッションの帯域幅プロファイルを構成できます。

表 17-3. 帯域幅プロファイル

帯域幅プロファイル	最大セッション 帯域幅 (Kbps)	最小セッション 帯域幅 (Kbps)	BTL の有 効化	最高初期イメ ージ品質	最低イメージ 品質	最大 FPS	最大オーディ オ帯域幅 (Kbps)	イメージ品質の パフォーマンス
高速 LAN	900,000	100	はい	100	50	60	1600	50
LAN	900,000	100	はい	90	50	30	1600	50
専用 WAN	900,000	100	いいえ	80	40	30	500	50
ブロードバンド WAN	5,000	100	いいえ	70	40	20	500	50
低速 WAN	2,000	100	いいえ	70	30	15	200	25
超低速接続	1,000	100	いいえ	70	30	5	90	0

Horizon スマート ポリシー定義への条件の追加

User Environment Manager で Horizon スマート ポリシーを定義する場合、ポリシーを有効にするための必要条件を追加できます。たとえば、ユーザーが企業のネットワーク以外からリモート デスクトップに接続した場合にのみクライアント ドライブのリダイレクト機能を無効にする条件を追加できます。

同じリモート デスクトップ機能に対して複数の条件を追加できます。たとえば、ユーザーが HR グループのメンバーである場合にローカル印刷を有効にする条件や、リモート デスクトップが Win7 プールにある場合にローカル印刷を有効にする条件を追加できます。

User Environment Manager 管理コンソールで条件を追加および編集する方法の詳細については、『User Environment Manager 管理者ガイド』を参照してください。

Horizon Client プロパティ条件の使用

ユーザーがリモート デスクトップに接続するか、再接続すると、Horizon Client がクライアント コンピュータに関する情報を収集し、接続サーバがその情報をリモート デスクトップに送信します。Horizon Client プロパティ条件を Horizon ポリシー定義に追加し、リモート デスクトップが受信する情報に基づいて、ポリシーが有効になるタイミングを制御できます。

注: Horizon Client プロパティ条件は、ユーザーが PCoIP 表示プロトコルまたは VMware Blast 表示プロトコルを使用してリモート デスクトップを起動した場合にのみ有効になります。ユーザーが RDP 表示プロトコルを使用してリモート デスクトップを起動した場合、Horizon Client プロパティ条件は無効になります。

表 17-4. Horizon Client プロパティ条件の事前定義プロパティでは、Horizon Client プロパティ条件を使用するときに [プロパティ] ドロップダウン メニューから選択できる事前定義プロパティについて説明します。各事前定義プロパティは、ViewClient_ レジストリ キーに対応します。

表 17-4. Horizon Client プロパティ条件の事前定義プロパティ

プロパティ	対応するレジストリ キー	説明
[クライアントの場所]	ViewClient_Broker_GatewayLocation	<p>ユーザーのクライアント システムの場所を指定します。有効な値は以下のとおりです。</p> <ul style="list-style-type: none"> ■ Internal - ユーザーが企業のネットワークの内からリモート デスクトップに接続した場合にのみポリシーが有効になります。 ■ External - ユーザーが企業のネットワーク以外からリモート デスクトップに接続した場合にのみポリシーが有効になります。 <p>接続サーバまたはセキュリティ サーバ ホストのゲートウェイの場所の設定については、『View 管理』ドキュメントを参照してください。Access Point アプライアンスのゲートウェイの場所の設定については、『Access Point をデプロイして構成する』ドキュメントを参照してください。</p>
[起動タグ]	ViewClient_Launch_Matched_Tags	<p>1 つ以上のタグを指定します。複数のタグはカンマまたはセミコロンで区切ります。リモート デスクトップを起動できるようにしたタグが指定のタグのいずれかと一致した場合にのみポリシーが有効になります。</p> <p>タグを接続サーバ インスタンスおよびデスクトップ プールに割り当てる方法については、リモート デスクトップ アクセスの制限を参照してください。</p>
[プール名]	ViewClient_Launch_ID	<p>デスクトップ プール ID を指定します。リモート デスクトップの起動時にユーザーが選択したデスクトップ プールの ID が指定のデスクトップ プール ID と一致した場合にのみポリシーが有効になります。たとえば、ユーザーが Win7 プールを選択していて、このプロパティが Win7 に設定されている場合、ポリシーが有効になります。</p> <p>注: このプロパティを使用して、アプリケーション プールを指定することはできません。</p>

[プロパティ] ドロップダウン メニューはテキスト ボックスでもあるため、そのテキスト ボックスに ViewClient_ レジストリ キーを手動で入力できます。レジストリ キーを入力する場合、ViewClient_ プリフィックスを含めな
いください。ViewClient_Broker_URL を指定するには、「Broker_URL」と入力します。

リモート デスクトップで Windows レジストリ エディタ (regedit.exe) を使用して、ViewClient_ レジストリ キーを表示できます。Horizon Client は、クライアント コンピュータ情報を、単一ユーザー マシンにデプロイされ
たリモート デスクトップのシステム レジストリ パス HKEY_CURRENT_USER\Volatile Environment に書き込
みます。RDS セッションにデプロイされたリモート デスクトップの場合、Horizon Client は、クライアント コンピ
ュータ情報をシステム レジストリ パス HKEY_CURRENT_USER\Volatile Environment\x に書き込みます。こ
の x は RDS ホストでのセッション ID です。

その他の条件の使用

User Environment Manager 管理コンソールには、多数の条件が用意されています。次の条件は、リモート デスクトップ機能のポリシーを作成する場合に特に便利です。

グループ メンバー	この条件を使用して、ユーザーが特定のグループのメンバーである場合にのみ有効になるようにポリシーを構成できます。
リモート表示プロトコル	この条件を使用して、ユーザーが特定の表示プロトコルを選択した場合にのみ有効になるようにポリシーを構成できます。条件設定には、RDP、PCoIP、および Blast が含まれます。
IP アドレス	この条件を使用して、ユーザーが企業のネットワークの内部または外部から接続した場合にのみ有効になるようにポリシーを構成できます。条件設定を使用して、内部 IP アドレス範囲または外部 IP アドレス範囲を指定します。

注: また、Horizon Client プロパティ条件の [クライアントの場所] プロパティを使用することもできます。

使用可能なすべての条件の詳細については、『User Environment Manager 管理者ガイド』ドキュメントを参照してください。

User Environment Manager の Horizon スマート ポリシーの作成

User Environment Manager 管理コンソールを使用して、User Environment Manager の Horizon スマート ポリシーを作成します。Horizon スマート ポリシーを定義するときに、スマート ポリシーを有効にするために必要な条件を追加できます。

前提条件

- User Environment Manager をインストールして構成します。 [User Environment Manager のインストール](#) および [User Environment Manager の構成](#)を参照してください。
- Horizon スマート ポリシー設定について理解しておきます。 [Horizon スマート ポリシー設定](#)を参照してください。
- Horizon スマート ポリシー定義を追加できる条件について理解しておきます。 [Horizon スマート ポリシー定義への条件の追加](#)を参照してください。

User Environment Manager 管理コンソールの使用方法の詳細については、『User Environment Manager 管理者ガイド』ドキュメントを参照してください。

手順

- 1 User Environment Manager 管理コンソールで、[ユーザー環境] タブを選択し、ツリー ビューで [Horizon スマート ポリシー] をクリックします。

既存の Horizon スマート ポリシー定義がある場合には、[Horizon スマート ポリシー] ペインに表示されます。

- 2 [Horizon スマート ポリシー] を右クリックし、[Horizon スマート ポリシー定義の作成] を選択して新しいスマート ポリシーを作成します。

[Horizon スマート ポリシー] ダイアログ ボックスが表示されます。

- 3 [設定] タブを選択し、スマート ポリシー設定を定義します。

- a [全般設定] セクションで、[名前] テキスト ボックスにスマート ポリシーの名前を入力します。

たとえば、スマート ポリシーがクライアント ドライブ リダイレクト機能に影響する場合、CDR などのスマート ポリシー名を付けます。

- b [Horizon スマート ポリシー設定] セクションで、スマート ポリシーに含めるリモート デスクトップ機能と設定を選択します。

複数のリモート デスクトップ機能を選択できます。

- 4 (オプション) スマート ポリシーに条件を追加するには、[条件] タブを選択して [追加] をクリックし、条件を選択します。

1 つのスマート ポリシー定義に複数の条件を追加できます。

- 5 [保存] をクリックしてスマート ポリシーを保存します。

User Environment Manager は、ユーザーがリモート デスクトップに接続または再接続するたびに Horizon スマート ポリシーを処理します。

User Environment Manager は複数のスマート ポリシーをスマート ポリシー名のアルファベット順に処理します。Horizon スマート ポリシーは、[Horizon スマート ポリシー] ペインにアルファベット順に表示されます。スマート ポリシーが競合する場合、最後に処理されたスマート ポリシーが優先されます。たとえば、Sue というユーザーの USB リダイレクトを有効にする Sue というスマート ポリシーがあり、Win7 というデスクトップ プールの USB リダイレクトを無効にする Pool という別のスマート ポリシーがある場合、Sue が Win7 デスクトップ プールのリモート デスクトップに接続したときに USB リダイレクト機能が有効になります。

Active Directory グループ ポリシーの使用

Microsoft Windows グループ ポリシーを使用して、リモート デスクトップの最適化とセキュリティ保護、View コンポーネントの動作の制御、ロケーションベースの印刷の設定を行うことができます。

グループ ポリシーは、Active Directory 環境でのコンピュータとリモート ユーザーの一元化された管理および構成を提供する、Microsoft Windows オペレーティング システムの機能です。

グループ ポリシー設定は、グループ ポリシー オブジェクト (GPO) と呼ばれるエンティティに格納されます。GPO は Active Directory オブジェクトに関連付けられます。View 環境のさまざまな領域を制御するために、ドメイン全体にわたるレベルで GPO を View コンポーネントに適用できます。適用後、GPO 設定は指定されたコンポーネントのローカル Windows レジストリに格納されます。

Microsoft Windows グループ ポリシー オブジェクト エディタを使用して、グループ ポリシー設定を管理します。グループ ポリシー オブジェクト エディタは Microsoft 管理コンソール (MMC) スナップインです。MMC は Microsoft グループ ポリシー管理コンソール (GPMC) に含まれています。GPMC のインストールと使用については、Microsoft TechNet Web サイトを参照してください。

リモート デスクトップの OU の作成

Active Directory 内に、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。

リモート 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グループ ポリシー設定が適用されないようにするには、View 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。

OU および GPO の作成については、Microsoft TechNet Web サイトの Microsoft Active Directory のマニュアルを参照してください。

リモート デスクトップのループバック処理の有効化

デフォルトでは、ユーザーのポリシー設定は、Active Directory 内のユーザー オブジェクトに適用される一連の GPO から取得されます。ただし、View 環境では、ユーザーがログインするコンピュータに基づいて GPO をユーザーに適用する必要があります。

ループバック処理を有効にすると、Active Directory 内の場所には関係なく、一貫した一連のポリシーが、特定のコンピュータにログインするすべてのユーザーに適用されます。

ループバック処理を有効にする方法については、Microsoft Active Directory のマニュアルを参照してください。

注: ループバック処理は、View で GPO を処理する方法の一つにすぎません。別の方法を実装する必要がある場合もあります。

View グループ ポリシー管理用テンプレート ファイルの使用

View には、コンポーネント固有のグループ ポリシー管理用 (ADM および ADMX) テンプレート ファイルがいくつか含まれています。これらの ADM および ADMX テンプレート ファイル内のポリシー設定を Active Directory 内の新しい GPO または既存の GPO に追加することによって、リモート デスクトップとアプリケーションを最適化し、セキュリティ保護することができます。

View のグループ ポリシー設定を提供する ADM および ADMX ファイルはすべて、VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip という .zip バンドル ファイル内にあります。x.x.x はバージョン、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 バンドル ファイルが含まれます。

View の ADM および ADMX テンプレート ファイルには、コンピュータの構成とユーザーの構成の両方のグループ ポリシーが含まれています。

- コンピュータの構成ポリシーは、だれがデスクトップに接続するかにはかかわらず、すべてのリモート デスクトップに適用されるポリシーを設定します。
- ユーザーの構成ポリシーは、ユーザーが接続するリモート デスクトップやアプリケーションにはかかわらず、すべてのユーザーに適用されるポリシーを設定します。ユーザーの構成ポリシーは、対応するコンピュータの構成ポリシーより優先されます。

Microsoft Windows は、デスクトップの起動時とユーザーのログイン時にポリシーを適用します。

View ADM および ADMX テンプレート ファイル

View ADM および ADMX テンプレート ファイルでは、View コンポーネントを制御および最適化できるグループ ポリシー設定が提供されます。

表 17-5. View ADM および ADMX テンプレート ファイル

テンプレート名	テンプレート ファイル	説明
Horizon Agent 構成	vdm_agent.adm	Horizon Agent の認証および環境コンポーネントに関するポリシー設定が含まれています。 Horizon Agent の構成 ADM テンプレートの設定 を参照してください。
Horizon Client 構成	vdm_client.adm	Windows 版 Horizon Client に関するポリシー設定が含まれています。 View 接続サーバ ホスト ドメインの外部から接続するクライアントは、Horizon Client に適用されるポリシーの影響を受けません。 『Windows 版 VMware Horizon Client の使用』を参照してください。
VMware Horizon URL リダイレクト	urlRedirection-enUS.adm	URL コンテンツ リダイレクト機能に関するポリシー設定が含まれています。このテンプレートをリモート デスクトップ プールまたはアプリケーション プールの GPO に追加すると、リモート デスクトップまたはアプリケーション内でクリックされた特定の URL リンクを Windows ベースのクライアントにリダイレクトし、クライアント側のブラウザで開くことができます。 このテンプレートをクライアント側の GPO に追加すると、ユーザーが Windows ベースのクライアント システムで特定の URL リンクをクリックしたときに、リモート デスクトップまたはアプリケーションで URL を開くことができます。 VMware Horizon URL コンテンツ リダイレクト テンプレートの設定 および『Windows 版 VMware Horizon Client の使用』ドキュメントを参照してください。
View Server の構成	vdm_server.adm	View 接続サーバに関するポリシー設定が含まれています。 『View 管理』を参照してください。
View Common の構成	vdm_common.adm	すべての View コンポーネントに共通のポリシー設定が含まれています。 『View 管理』を参照してください。
View PCoIP のセッション変数	pcoip.adm	PCoIP 表示プロトコルに関するポリシー設定が含まれています。 PCoIP ポリシー設定 を参照してください。
View PCoIP クライアントのセッション変数	pcoip.client.adm	Windows 版 Horizon Client に影響を与える PCoIP 表示プロトコルに関するポリシー設定が含まれています。 『Windows 版 VMware Horizon Client の使用』を参照してください。

テンプレート名	テンプレート ファイル	説明
View Persona Management 構成	ViewPM.adm ViewPM.admx	View Persona Management に関するポリシー設定が含まれています。 View Persona Management グループ ポリシー設定 を参照してください。
View リモート デスクトップ サービス	vmware_rdsh.admx vmware_rdsh_server.admx	リモート デスクトップ サービスに関するポリシー設定が含まれています。 リモート デスクトップ サービス グループ ポリシーの使用 を参照してください。
リアルタイム オーディオビデオ構成	vdm_agent_rtav.adm	リアルタイム オーディオ ビデオ機能で使用する Web カメラに関するポリシー設定が含まれています。 リアルタイム オーディオ ビデオ グループ ポリシー設定 を参照してください。
スキャナ リダイレクト	vdm_agent_scanner.adm	リモート デスクトップおよびアプリケーションで使用するためにリダイレクトされるスキャン デバイスに関するポリシー設定が含まれています。 スキャナ リダイレクトのグループ ポリシー設定 を参照してください。
シリアル ポート リダイレクト	vdm_agent_serialport.adm	リモート VDI デスクトップで使用するためにリダイレクトされるシリアル (COM) ポートに関するポリシー設定が含まれています。 シリアル ポート リダイレクトのグループ ポリシー設定 を参照してください。

Horizon Agent の構成 ADM テンプレートの設定

Horizon Agent の構成 ADM テンプレート ファイル (vdm_agent.adm) には、Horizon Agent の認証および環境コンポーネントに関するポリシー設定が含まれています。

この ADM ファイルは、VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip という .zip バンドル ファイル内にあり、<https://my.vmware.com/web/vmware/downloads>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 バンドル ファイルが含まれます。

次の表で、USB デバイスで使用されているポリシー設定以外に、Horizon Agent の構成 ADM テンプレート ファイル内にあるポリシー設定について説明します。テンプレートには、コンピュータの構成とユーザーの構成の両方の設定が含まれています。ユーザーの構成設定は、対応するコンピュータの構成設定より優先されます。

表 17-6. Horizon Agent の構成テンプレートの設定

設定	コンピュータ	ユーザー	プロパティ
AllowDirectRDP	X		<p>Horizon Client デバイス以外のクライアントが RDP を使用してリモート デスクトップに直接接続できるかどうかを指定します。この設定が無効になっていると、エージェントでは、Horizon Client 経由での View によって管理される接続のみが許可されます。</p> <p>Horizon Client for Mac からリモート デスクトップに接続する場合は、AllowDirectRDP の設定を無効にしないでください。この設定を無効にすると、Access is denied(アクセスが拒否されました) エラーが発生して接続に失敗します。</p> <p>デフォルトの設定の場合、ユーザーは、View デスクトップセッションにログイン中に RDP を使用して、View の外側から仮想マシンに接続できます。RDP 接続によって View デスクトップ セッションが終了し、View ユーザーの保存されていないデータや設定は失われます。View ユーザーは、外部の RDP 接続が閉じられるまで、デスクトップにログインできません。この状況を回避するには、AllowDirectRDP 設定を無効にします。</p> <hr/> <p>重要: View を正しく動作させるために、Windows リモート デスクトップ サービスが各デスクトップのゲスト OS で実行されている必要があります。この設定を使用して、ユーザーが自分のデスクトップに直接 RDP 接続を作成することを不可にできます。</p> <hr/> <p>デフォルトでは、この設定は有効になっています。</p>
AllowSingleSignon	X		<p>シングル サインオン (SSO) を使用して、ユーザーをデスクトップおよびアプリケーションに接続するかどうかを決定します。この設定が有効になっていると、ユーザーはサーバにログインするときに、自分の認証情報を 1 回入力するだけで済みます。この設定を無効にすると、ユーザーはリモート接続の確立時に再認証する必要があります。</p> <p>デフォルトでは、この設定は有効になっています。</p>
CommandsToRunOnConnect	X		<p>セッションに初めて接続するときに実行されるコマンドまたはコマンド スクリプトのリストを指定します。</p> <p>詳細については、View デスクトップ上でのコマンドの実行を参照してください。</p>
CommandsToRunOnDisconnect	X		<p>セッションが切断されたときに実行されるコマンドまたはコマンド スクリプトのリストを指定します。</p> <p>詳細については、View デスクトップ上でのコマンドの実行を参照してください。</p>
CommandsToRunOnReconnect	X		<p>セッションが切断された後、再接続されるときに実行されるコマンドまたはコマンド スクリプトのリストを指定します。</p> <p>詳細については、View デスクトップ上でのコマンドの実行を参照してください。</p>
ConnectionTicketTimeout	X		<p>View 接続チケットが有効な時間 (秒) を指定します。</p> <p>Horizon Client デバイスは、エージェントに接続するときに、検証とシングル サインオンのために接続チケットを使用します。セキュリティ上の理由から、接続チケットは限られた期間のみ有効です。ユーザーがリモート デスクトップに接続するときは、接続チケットのタイムアウト期間内に認証を行う必要があります。そうでないとセッションがタイムアウトになります。この設定が構成されていない場合、デフォルトのタイムアウト期間は 900 秒になります。</p>

設定	コンピュータ	ユーザー	プロパティ
CredentialFilterExceptions	X		エージェントの CredentialFilter のロードを許可されていない実行可能ファイルを指定します。ファイル名にパスまたはサフィックスを含めることはできません。複数のファイル名を区切るにはセミコロンを使用します。
Disable Time Zone Synchronization	X	X	View デスクトップのタイム ゾーンを接続されたクライアントのタイムゾーンと同期化するかどうかを指定します。設定を有効にすると、Horizon Client の構成ポリシーの Disable time zone forwarding 設定が無効に設定されていない場合にのみ適用されます。 デフォルトでは、この設定は無効になっています。
Enable multi-media acceleration	X		View デスクトップでマルチメディア リダイレクト (MMR) を有効にするかどうかを指定します。 MMR は、TCP ソケットを介してリモート システムの固有のコーデックからマルチメディア データをクライアントに直接転送する Windows Media Foundation フィルタです。その後、データはクライアント上で直接デコードされ、そこで再生されます。クライアントがローカル マルチメディア デコーディングを処理するために十分なリソースを持たない場合は、MMR を無効にできます。 デフォルトでは、この設定は有効になっています。
Enable system tray redirection for Hosted Apps	X		ユーザーがリモート アプリケーションを実行しているときに、システムトレイのリダイレクトを有効にするかどうかを決定します。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Unity Touch およびホスト型アプリケーション フォルダ] にあります。 デフォルトでは、この設定は有効になっています。
Enable Unity Touch	X		View デスクトップで Unity Touch 機能を有効にするかどうかを決定します。Unity Touch は、View でリモート アプリケーションの配信をサポートし、モバイル デバイス ユーザーが Unity Touch サイドバーのアプリケーションにアクセスできるようにします。 この設定は、グループ ポリシー管理エディタの [VMware View Agent の構成] - [Unity Touch およびホスト型アプリケーション フォルダ] にあります。 デフォルトでは、この設定は有効になっています。
ShowDiskActivityIcon	X		この設定は、このリリースではサポートされていません。
Toggle Display Settings Control	X		クライアント セッションで PCoIP 表示プロトコルを使用するときに、[Display (画面)] コントロール パネルの [Settings (設定)] タブを無効にするかどうかを指定します。 デフォルトでは、この設定は有効になっています。

設定	コンピュータ	ユーザー	プロパティ
DPI Synchronization	X	X	<p>リモート セッションに関するシステム全体の DPI 設定を調整します。この設定が有効にされていたり、構成されていなかったりすると、リモート セッションに関するシステム全体の DPI 設定は、クライアント オペレーティング システムの対応する DPI 設定と一致するように設定されます。この設定が無効になっていると、リモート セッションに関するシステム全体の DPI 設定は決して変更されません。</p> <p>デフォルトでは、この設定は構成されていません。</p> <p>注: この設定は、バージョン 7.0.2 以降、および Horizon Client 4.2 以降がインストールされている Windows クライアントのみに適用されます。</p>
VMwareViewAgentCIT	X		<p>Internet Explorer へのリモート接続を有効にし、リモート デスクトップ マシンの IP アドレスの代わりにクライアントの IP アドレスを使用します。この設定は、次回ログインする時に有効になります。</p> <p>Horizon Agent インストーラで [VMware クライアント IP アドレスの透過性] カスタム セットアップ オプションが選択されている場合、この設定はデフォルトで有効になります。</p>
ProxyDefaultAutoDetectSettings	X		<p>[インターネットのプロパティ] と [ローカル エリア ネットワークの設定] の設定を自動的に検出するデフォルトの Internet Explorer の接続設定。</p> <p>デフォルトでは、この設定は有効ではありません。</p>
ProxyDefaultIEProxyServer	X		<p>[インターネットのプロパティ] および [ローカル エリア ネットワークの設定] で使用するプロキシ サーバーが指定されるプロキシ サーバーに関するデフォルトの Internet Explorer 接続設定。</p> <p>デフォルトでは、この設定は有効ではありません。</p>
UpdateJavaProxy	X		<p>リモート接続で Java アプレット用のリモート デスクトップ マシンの IP アドレスではなく、クライアントの IP アドレスを使用するように指定します。</p> <p>デフォルトでは、この設定は有効ではありません。</p>
FlashMMRUrlListEnableType			<p>URL での Flash リダイレクトを使用を有効または無効にするホワイト リストまたはブラック リストを指定します。ホワイト リストを使用するには、Flash リダイレクトの使用が有効になっている URL リストの URL のみが有効になるように FlashMMRUrlListEnableType=0 を設定します。ブラック リストを使用するには、URL リストの URL が Flash リダイレクトを使用できないように FlashMMRUrlListEnableType=1 を設定します。</p> <p>この設定では、ホワイト リストのがデフォルトで指定されます。</p>
FlashMMRUrlList			<p>FlashMMRUrlListEnableType の設定に基づいて Flash リダイレクトの使用を有効または無効にする URL リストを指定します。</p> <p>必ず [http://] または [https://] を含めてください。正規表現を使用できます。たとえば、 https://*.google.com や http://www.cnn.com を指定できます。</p>

注: Connect using DNS Name の設定は、Horizon 6 バージョン 6.1 リリースで削除されました。View LDAP 属性、[pae-PreferDNS] を設定して View 接続サーバが、デスクトップ マシンと RDS ホスト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は、DNS 名に環境設定を与えるようにすることができます。『View のインストール』ドキュメントの「View 接続サーバがアドレス情報を返す場合、DNS 名に環境設定を与える」を参照してください。

Horizon Agent の USB 設定

[Horizon Agent の構成 ADM テンプレートの USB 設定](#)を参照してください。

リモート デスクトップに送信されるクライアント システム情報

ユーザーがリモート デスクトップに接続するか、再接続すると、Horizon Client がクライアント システムに関する情報を収集し、接続サーバがその情報をリモート デスクトップに送信します。

Horizon Agent は、クライアント コンピュータ情報を、単一ユーザー マシンにデプロイされたりリモート デスクトップのシステム レジストリ パス HKCU\Volatile Environment に書き込みます。RDS セッションにデプロイされたりリモート デスクトップの場合、Horizon Agent は、クライアント コンピュータ情報をシステム レジストリ パス HKCU\Volatile Environment\x に書き込みます。この x は RDS ホストでのセッション ID です。

Horizon Client がリモート デスクトップ セッション内で実行されている場合、仮想マシン情報ではなくて物理クライアントの情報がリモート デスクトップに送信されます。たとえば、ユーザーがクライアント システムをリモート デスクトップに接続し、リモート デスクトップ内で Horizon Client を起動して別のリモート デスクトップに接続する場合、物理クライアント システムの IP アドレスはこのセカンド リモート デスクトップに送信されます。この機能は、ネスト モードまたはダブルホップ シナリオと呼ばれます。Horizon Client は、1 に設定されている ViewClient_Nested_Passthrough をクライアント システム情報と一緒に送信し、ネスト モード情報を送信していることを示します。

注: Horizon Client 4.1 では、最初のプロトコル接続の時に、クライアント システム情報がセカンドホップ デスクトップに渡されます。Horizon Client 4.2 以降では、ファーストホップ プロトコルの接続が切断して再接続すると、クライアント システム情報も更新されます。

Horizon Agent の CommandsToRunOnConnect、CommandsToRunOnReconnect および CommandsToRunOnDisconnect グループ ポリシー設定にコマンドを追加し、ユーザーがデスクトップに接続および再接続するときに、この情報をシステム レジストリから読み取るコマンドまたはコマンド スクリプトを実行することができます。詳細については、[View デスクトップ上でのコマンドの実行](#)を参照してください。

[表 17-7. クライアント システム情報](#)に、クライアント システム情報を含むレジストリ キーについて説明し、それらをサポートするデスクトップおよびクライアント システムのタイプを一覧表示します。[サポートされるネスト モード] 列に [はい] が表示される場合、物理クライアントの情報（仮想マシンの情報ではなく）がセカンドホップ デスクトップに送信されることを示します。

表 17-7. クライアント システム情報

レジストリ キー	説明	サポートされる ネスト モード	サポートされるデスクトップ	サポートされるクライアント システム
ViewClient_IP_Address	クライアント システムの IP アドレス。	はい	VDI (シングルユーザー マシン) RDS	Windows、Linux、Mac、Android、iOS、Windows ストア
ViewClient_MAC_Address	クライアント システムの MAC アドレス。	はい	VDI (シングルユーザー マシン) RDS	Windows、Linux、Mac、Android
ViewClient_Machine_Name	クライアント システムのマシン名。	はい	VDI (シングルユーザー マシン) RDS	Windows、Linux、Mac、Android、iOS、Windows ストア
ViewClient_Machine_Domain	クライアント システムのドメイン。	はい	VDI (シングルユーザー マシン) RDS	Windows、Windows ストア
ViewClient_LoggedOn_Username	クライアント システムへのログインに使用したユーザー名。		VDI (シングルユーザー マシン) RDS	Windows、Linux、Mac
ViewClient_LoggedOn_Domainname	クライアント システムへのログインに使用したドメイン名。		VDI (シングルユーザー マシン) RDS	Windows、Windows ストア Linux クライアントまたは Mac クライアントの場合、ViewClient_Machine_Domain を参照してください。 .ViewClient_LoggedOn_Domainname は、Linux および Mac アカウントが Windows ドメインにバインドされていないため、Linux クライアントまたは Mac クライアントでは指定されません。
ViewClient_Type	クライアント システムのシンクライアント名またはオペレーティング システムの種類。	はい	VDI (シングルユーザー マシン) RDS	Windows、Linux、Mac、Android、iOS、Windows ストア
ViewClient_Broker_DNS_Name	View 接続サーバ インスタンスの DNS 名。		VDI (シングルユーザー マシン) RDS	値は、Horizon Client により収集されるのではなく、View 接続サーバから直接送信されます。
ViewClient_Broker_URL	View 接続サーバ インスタンスの URL。		VDI (シングルユーザー マシン) RDS	値は、Horizon Client により収集されるのではなく、View 接続サーバから直接送信されます。

レジストリ キー	説明	サポートされるネスト モード	サポートされるデスクトップ	サポートされるクライアント システム
ViewClient_Broker_Tunneled	View 接続サーバのトンネル接続のステータス。true（有効）または false（無効）です。		VDI（シングルユーザー マシン） RDS	値は、Horizon Client により収集されるのではなく、View 接続サーバから直接送信されます。
ViewClient_Broker_Tunnel_URL	View 接続サーバのトンネル接続が有効になっている場合のトンネル接続の URL。		VDI（シングルユーザー マシン） RDS	値は、Horizon Client により収集されるのではなく、View 接続サーバから直接送信されます。
ViewClient_Broker_Remote_IP_Address	View 接続サーバ インスタンスから見えるクライアント システムの IP アドレス。		VDI（シングルユーザー マシン） RDS	値は、Horizon Client により収集されるのではなく、View 接続サーバから直接送信されます。
ViewClient_TZID	Olson タイム ゾーン ID。タイム ゾーンの同期を無効にするには、Horizon Agent の Disable Time Zone Synchronization グループ ポリシー設定を有効にします。		VDI（シングルユーザー マシン） RDS	Windows、Linux、Mac、Android、iOS
ViewClient_Windows_Timezone	GMT 標準時間。タイム ゾーンの同期を無効にするには、Horizon Agent の Disable Time Zone Synchronization グループ ポリシー設定を有効にします。		VDI（シングルユーザー マシン） RDS	Windows、Windows ストア
ViewClient_Broker_DomainName	View 接続サーバの認証に使用されるドメイン名。		VDI（シングルユーザー マシン） RDS	値は、Horizon Client により収集されるのではなく、View 接続サーバから直接送信されます。
ViewClient_Broker_UserName	View 接続サーバの認証に使用されるユーザー名。		VDI（シングルユーザー マシン） RDS	値は、Horizon Client により収集されるのではなく、View 接続サーバから直接送信されます。
ViewClient_Client_ID	ライセンス キーへのリンクとして使用される Unique Client HardwareId を指定します。		VDI（シングルユーザー マシン） RDS	Windows、Linux、Mac、Android、iOS、Windows ストア
ViewClient_Displays.Number	クライアントで使用されているモニターの数を指定します。		VDI（シングルユーザー マシン） RDS	Windows、Linux、Mac、Android、iOS、Windows ストア
ViewClient_Displays.Topology	クライアントのディスプレイの配置、解像度、寸法を指定します。		VDI（シングルユーザー マシン） RDS	Windows、Linux、Mac、Android、iOS、Windows ストア

レジストリ キー	説明	サポートされる ネスト モード	サポートされるデスクトップ	サポートされるクライアント システム
ViewClient_Keyboard.Type	クライアントで使用されているキーボードの種類を指定します。例：日本語、韓国語。		VDI (シングルユーザー マシン) RDS	Windows
ViewClient_Launch_SessionType	セッション タイプを指定します。指定できるタイプはデスクトップまたはアプリケーションです。		VDI (シングルユーザー マシン) RDS	値は、Horizon Client により収集されるのではなく、View 接続サーバから直接送信されます。
ViewClient_Mouse.Identifier	マウスの種類を指定します。		VDI (シングルユーザー マシン) RDS	Windows
ViewClient_Mouse.NumButtons	マウスでサポートするボタンの数を指定します。		VDI (シングルユーザー マシン) RDS	Windows
ViewClient_Mouse.SampleRate	PS/2 マウスからの入力のサンプリング レートを 1 秒あたりのレポート数で指定します。		VDI (シングルユーザー マシン) RDS	Windows
ViewClient_Protocol	使用されているプロトコルを指定します。		VDI (シングルユーザー マシン) RDS	Windows、Linux、Mac、Android、iOS、Windows ストア
ViewClient_Language	オペレーティング システムの言語を指定します。		VDI (シングルユーザー マシン) RDS	Windows、Linux、Mac、Android、iOS、Windows ストア
ViewClient_Launch_ID	デスクトップ プールの一意の ID を指定します。		VDI (シングルユーザー マシン)	Windows、Linux、Mac、Android、iOS、Windows ストア

注: 表 17-7. クライアント システム情報にある ViewClient_LoggedOn_Username および ViewClient_LoggedOn_Domainname の定義は、Horizon Client 2.2 for Windows 以降のリリースに適用されます。

Horizon Client 5.4 for Windows 以前のリリースでは、Horizon Client で入力されたユーザー名が ViewClient_LoggedOn_Username により送信され、Horizon Client で入力されたドメイン名が ViewClient_LoggedOn_Domainname により送信されます。

Horizon Client 2.2 for Windows は Horizon Client 5.4 for Windows より後のリリースです。Horizon Client 2.2 から、Windows 版のリリース番号は、他のオペレーティング システムおよびデバイスの Horizon Client リリースと整合性が取れています。

View デスクトップ上でのコマンドの実行

Horizon Agent `CommandsToRunOnConnect`、`CommandsToRunOnReconnect`、および `CommandsToRunOnDisconnect` グループ ポリシー設定を使用して、ユーザーが接続、再接続、切断するときに View デスクトップ上でコマンドおよびコマンド スクリプトを実行できます。

コマンドまたはコマンド スクリプトを実行するには、コマンド名またはスクリプトのファイル パスを、グループ ポリシー設定のコマンド リストに追加します。例：

`date`

`C:\Scripts\myscript.cmd`

コンソール アクセスが必要なスクリプトを実行するには、先頭に `-C` または `-c` オプションと領域を付加します。

例：

`-c C:\Scripts\Cli_clip.cmd`

`-C e:\procepx.exe`

サポートされているファイルのタイプには、`.CMD`、`.BAT`、`.EXE` が含まれます。`.VBS` ファイルは、`cscript.exe` または `wscript.exe` で解析されない限り実行されません。例：

`-C C:\WINDOWS\system32\wscript.exe C:\Scripts\checking.vbs`

文字列の合計の長さ（`-C` または `-c` オプションを含む）が 260 文字を超えないようにする必要があります。

PCoIP ポリシー設定

PCoIP の ADM テンプレート ファイル (`pcoip.adm`) には、PCoIP 表示プロトコルに関連するポリシー設定が含まれています。これらの設定をデフォルト値（管理者による上書きが可能）にすることも、上書きできない値にすることもできます。

この ADM ファイルは、`VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` という .zip バンドル ファイル内にあり、<https://my.vmware.com/web/vmware/downloads> 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 バンドル ファイルが含まれます。

View PCoIP のセッション変数 ADM テンプレート ファイルには、2 つのサブカテゴリが含まれています。

上書き可能な管理者デフォルト

PCoIP ポリシー設定のデフォルト値を指定します。管理者はこれらの設定を上書きできます。これらの設定は、レジストリ キーの値を `HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin_defaults` に書き込みます。

上書き不可の管理者設定

上書き可能な管理者デフォルトと同じ設定を含みますが、管理者はこれらの設定を上書きできません。これらの設定は、レジストリ キーの値を `HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin` に書き込みます。

このテンプレートには、コンピュータの構成設定のみが含まれます。

ポリシー以外のレジストリ キー

ローカル マシン設定を適用する必要がある、HKLM\Software\Policies\Teradici 下に格納できない場合は、ローカル マシン設定を HKLM\Software\Teradici 内のレジストリ キーに格納できます。HKLM\Software\Policies\Teradici にあるのと同じレジストリ キーを HKLM\Software\Teradici に入れることができます。両方の場所に同じレジストリ キーが存在する場合は、HKLM\Software\Policies\Teradici 内の設定がローカル マシン値に優先されます。

PCoIP の一般的な設定

View PCoIP ADM テンプレート ファイルには、PCoIP イメージの品質、USB デバイス、ネットワーク ポートなどの一般的な設定を構成するグループ ポリシー設定が含まれます。

表 17-8. PCoIP の一般的なポリシー設定

設定	説明
Configure PCoIP client image cache size policy	<p>PCoIP クライアントのイメージ キャッシュのサイズを制御します。クライアントは、イメージ キャッシュを使用して以前に送信された表示の一部を保存します。イメージ キャッシュにより、再送されるデータ量が削減されます。</p> <p>この設定は、Horizon Client、Horizon Agent、および View 接続サーバが View 5.0 以降のリリースの場合に、Windows、Linux および Mac クライアントのみに適用されます。</p> <p>この設定を構成しないか、無効にすると、PCoIP はデフォルトのクライアント イメージ キャッシュ サイズである 250MB を使用します。</p> <p>Horizon Client 3.1 以降のリリースでは、使用可能なメモリの量を 2 で割ったよりも小さい数値を指定した場合、キャッシュ サイズは次の式を使用して設定されます。</p> <div style="background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> $\text{user-setting} - 10 \text{ MB}$ </div> <p>Horizon Client 3.1 以降のリリースでは、使用可能なメモリを 2 で割ったよりも大きい数値を指定した場合、キャッシュ サイズは次の式を使用して設定されます。</p> <div style="background-color: #f0f0f0; padding: 5px; margin: 10px 0;"> $\text{available-memory} / 2 - 10 \text{ MB}$ </div> <p>たとえば、1,024 MB の最大キャッシュ サイズを指定すると使用可能な メモリは 1,600 MB で、最大キャッシュ サイズは 790 MB に設定されます。</p> <p>全 Horizon Client バージョンで、デフォルト サイズは 250 MB で、最小サイズは 50 MB です。</p> <p>Horizon Client 1.6 以降のリリースでは、最大サイズは 1,024 MB です。Horizon Client 1.5 以前のリリースでは、最大サイズは 300 MB です。</p>
Configure PCoIP event log cleanup by size in MB	<p>サイズ (MB) に基づく PCoIP イベント ログ クリーンアップの構成を有効にします。</p> <p>このポリシーが構成されている場合は、クリーンアップが実行される前のログ ファイルの最大サイズが設定で管理されます。m がゼロ以外に設定されている場合は、m MB より大きいファイルが自動的かつサイレントに削除されます。0 に設定されている場合は、サイズに基づくファイルのクリーンアップは行われません。</p> <p>このポリシーが無効になっているか設定されていない場合は、サイズに基づくイベント ログ クリーンアップのデフォルト値は 100 MB です。</p> <p>ログ ファイルのクリーンアップは、セッション起動時に 1 回実行されます。設定の変更は、次のセッションまで適用されません。</p>

設定	説明
Configure PCoIP event log cleanup by time in days	<p>時間（日数）に基づく PCoIP イベント ログ クリーンアップの構成を有効にします。</p> <p>このポリシーが構成されている場合は、ログ ファイルのクリーンアップが実行されるまでの日数が管理されます。n がゼロ以外に設定されている場合は、日数が n 日より長いログ ファイルが自動的かつサイレントに削除されます。0 に設定されている場合は、時間に基づくファイルのクリーンアップは行われません。</p> <p>このポリシーが無効になっているか設定されていない場合は、イベント ログ クリーンアップのデフォルトの日数は 7 日です。</p> <p>ログ ファイルのクリーンアップは、セッション起動時に 1 回実行されます。設定の変更は、次のセッションまで適用されません。</p>
Configure PCoIP event log verbosity	<p>PCoIP イベント ログの冗長性を設定します。この値は、0（最も簡素）から 3（最も詳細）です。</p> <p>この設定を有効にすると、冗長性のレベルを 0 から 3 に設定できます。設定を行わないか、無効にすると、デフォルトのイベント ログの冗長性レベルは 2 になります。</p> <p>この設定をアクティブ PCoIP セッション中に変更すると、新しい設定が直ちに反映されます。</p>
Configure PCoIP image quality levels	<p>ネットワーク輻輳期間中の PCoIP でのイメージ描画方法を制御します。[最低イメージ品質]、[最高初期イメージ品質]、および [最大フレーム レート] の値の相互作用により、ネットワーク帯域幅に制約のある環境での精密な制御が可能になります。</p> <p>帯域幅が制限されるシナリオでイメージ品質とフレーム レートのバランスをとるには、[最低イメージ品質] の値を使用します。30 から 100 までの値を指定できます。デフォルト値は 40 です。小さい値を指定するとフレーム レートが高くなりますが、表示の品質が低下する可能性があります。大きい値を指定するとイメージ品質が向上しますが、ネットワーク帯域幅に制約がある場合にフレーム レートが低下する可能性があります。ネットワーク帯域幅に制約がない場合は、この値にかかわらず、PCoIP で最高品質が維持されます。</p> <p>表示イメージ内の変更された領域の初期品質を制限することで、PCoIP に必要な最大ネットワーク帯域幅を削減するには、[最高初期イメージ品質] の値を使用します。30 から 100 までの値を指定できます。デフォルト値は 80 です。小さい値を指定するとコンテンツの変更部分のイメージ品質が低下し、必要な最大帯域幅が削減されます。大きい値を指定するとコンテンツの変更部分のイメージ品質が向上し、必要な最大帯域幅が増加します。イメージの変更されていない領域は、この値にかかわらず、プログレッシブ方式でロスレス（完全）品質まで構築されます。80 以下の値を指定すると、使用可能な帯域幅を最大限に活用できます。</p> <p>[最低イメージ品質] の値が [最高初期イメージ品質] の値を超えないようにする必要があります。</p> <p>1 秒あたりの画面の更新回数を制限して、ユーザーあたりの平均使用帯域幅を管理するには、[最大フレーム レート] の値を使用します。毎秒 1 フレームから 120 フレームまでの値を指定できます。デフォルト値は 30 です。大きい値を指定すると、使用帯域幅が増加する場合がありますが、ジッタが減少するため、ビデオなどの変化するイメージの遷移がスムーズになります。小さい値を指定すると、使用帯域幅が削減されますが、ジッタが増加します。</p> <p>これらのイメージ品質の値は、ソフト ホストにのみ適用され、ソフト クライアントには影響しません。</p> <p>この設定を無効にするか、構成しない場合は、デフォルト値が使用されます。</p> <p>この設定をアクティブ PCoIP セッション中に変更すると、新しい設定が直ちに反映されます。</p>

設定	説明
Configure frame rate vs image quality preference	<p>フレーム レートとイメージ品質の設定を 0（最大フレーム レート）から 100（最高イメージ品質）で構成します。このポリシーが無効になっているか設定されていない場合、デフォルトの設定は 50 です。</p> <p>大きい値（最大 100）を指定すると、フレーム レートが低い場合でも、高いイメージ品質が優先されます。小さい値（最小 0）を指定すると、高いイメージ品質で滑らかに表示されます。</p> <p>この設定は、Configure PCoIP image quality levels GPO と連携も可能です。この GPO は、最高初期イメージ品質レベルと最低イメージ品質レベルを指定します。Frame rate and image quality preference では各フレームのイメージ品質レベルを調整できますが、Configure PCoIP image quality levels GPO によって構成された最高/最低品質レベルのしきい値を超えて調整することはできません。実行時にこのポリシーを変更すると、変更が直ちに反映されることがあります。</p>
Configure PCoIP session encryption algorithms	<p>セッション ネゴシエーション中に PCoIP エンドポイントによってアダプタイズされる暗号化アルゴリズムを制御します。</p> <p>いずれかのチェック ボックスをオンにすると、関連付けられた暗号化アルゴリズムが無効になります。1 つ以上のアルゴリズムを有効にする必要があります。</p> <p>この設定はエージェントとクライアントの両方に適用されます。エンドポイントは、使用される実際のセッション暗号化アルゴリズムをネゴシエートします。FIPS140-2 承認モードが有効な場合は、[Disable AES-128-GCM encryption (AES-128-GCM 暗号化を無効にする)] の値が常に上書きされ、AES-128-GCM 暗号化が有効になります。</p> <p>サポートされている暗号化アルゴリズムは、SALSA20/12-256、AES-GCM-128、AES-GCM-256（優先順位順）です。デフォルトでは、サポートされているすべての暗号化アルゴリズムを、このエンドポイントのネゴシエーションに使用できます。</p> <p>両方のエンドポイントが 3 つすべてのアルゴリズムをサポートするように構成され、接続でセキュリティ ゲートウェイ (SG) が使用されない場合は、SALSA20 アルゴリズムがネゴシエートされ使用されます。ただし接続で SG が使用される場合は、SALSA20 は自動的に無効になり、AES128 がネゴシエートされ使用されます。一方のエンドポイントまたは SG が SALSA20 を無効に、もう一方のエンドポイントが AES128 を無効にすると、AES256 がネゴシエートされ使用されます。</p>

設定	説明								
Configure PCoIP USB allowed and unallowed device rules	<p>Teradici ファームウェアを実行するゼロ クライアントを使用する PCoIP セッションで使用を許可する USB デバイスと許可しない USB デバイスを指定します。PCoIP セッションで使用される USB デバイスは、USB 許可テーブルに表示されている必要があります。USB 不許可テーブルに表示されている USB デバイスは、PCoIP セッションで使用できません。</p> <p>最大 10 の USB 許可ルールと最大 10 の USB 不許可ルールを定義できます。複数のルールは縦棒 () 文字で区切ります。</p> <p>各ルールは、ベンダー ID (VID) と製品 ID (PID) の組み合わせ、または USB デバイスのクラスの記述で指定できます。クラス ルールでは、デバイス クラス全体、1 つのサブクラス、またはサブクラス内のプロトコルの許可または不許可を指定できます。</p> <p>VID/PID を組み合わせたルールの形式は、1xxxxyyyy です。ここで xxxx は 16 進数形式の VID、yyyy は 16 進数形式の PID です。たとえば、VID 0x1a2b、PID 0x3c4d のデバイスを許可またはブロックするルールは、11a2b3c4d です。</p> <p>クラス ルールの場合は、次のいずれかの形式を使用します。</p> <table> <tr> <td>すべての USB デバイスを許可する</td><td>形式：23XXXXXX 例：23XXXXXX</td></tr> <tr> <td>特定のクラス ID の USB デバイスを許可する</td><td>形式：22classXXXX 例：22aaXXXX</td></tr> <tr> <td>特定のサブクラスを許可する</td><td>形式：21class-subclassXX 例：21aabbXX</td></tr> <tr> <td>特定のプロトコルを許可する</td><td>形式：20class-subclass-protocol 例：20aabbcc</td></tr> </table> <p>たとえば、USB HID(マウスおよびキーボード) デバイス (クラス ID 0x03) と Web カメラ (クラス ID 0x0e) を許可する USB 許可文字列は 2203XXXX 220eXXXX です。USB マス ストレージ デバイス (クラス ID 0x08) を許可しない USB 不許可文字列は、2208XXXX です。</p> <p>空の USB 許可文字列は、どの USB デバイスも許可されないことを意味します。空の USB 不許可文字列は、どの USB デバイスも禁止されないことを意味します。</p> <p>この設定は、Horizon Agent にのみ、およびリモート デスクトップが Teradici ファームウェアを実行するゼロ クライアントとセッション中の場合にのみ適用されます。デバイスの使用はエンドポイント間でネゴシエートされます。</p> <p>デフォルトでは、すべてのデバイスが許可され、どのデバイスも禁止されません。</p>	すべての USB デバイスを許可する	形式： 23XXXXXX 例： 23XXXXXX	特定のクラス ID の USB デバイスを許可する	形式： 22classXXXX 例： 22aaXXXX	特定のサブクラスを許可する	形式： 21class-subclassXX 例： 21aabbXX	特定のプロトコルを許可する	形式： 20class-subclass-protocol 例： 20aabbcc
すべての USB デバイスを許可する	形式： 23XXXXXX 例： 23XXXXXX								
特定のクラス ID の USB デバイスを許可する	形式： 22classXXXX 例： 22aaXXXX								
特定のサブクラスを許可する	形式： 21class-subclassXX 例： 21aabbXX								
特定のプロトコルを許可する	形式： 20class-subclass-protocol 例： 20aabbcc								

設定	説明
Configure PCoIP virtual channels	<p>PCoIP セッションで動作できる仮想チャネルと動作できない仮想チャネルを指定します。この設定によって、PCoIP ホスト上でのクリップボードの処理を無効にするかどうかも指定されます。</p> <p>PCoIP セッションで使用される仮想チャネルは、許可仮想チャネルリストに表示されている必要があります。不許可仮想チャネル リストに表示されている仮想チャネルは、PCoIP セッションでは使用できません。</p> <p>PCoIP セッションで使用する仮想チャネルを 15 まで指定できます。</p> <p>複数のチャネル名は縦棒 () 文字で区切ります。たとえば、mksvchan と vdp_rdpvcbridge の仮想チャネルを許可する仮想チャネル許可文字列は、mksvchan vdp_vdpvcbridge です。</p> <p>チャネル名に縦棒文字またはバックスラッシュ (\) 文字が含まれる場合は、その前にバックスラッシュ文字を入れてください。たとえば、チャネル名 awk\ward\channel は awk\ ward\channel として入力します。</p> <p>許可仮想チャネル リストが空の場合は、すべての仮想チャネルが禁止されます。不許可仮想チャネル リストが空の場合は、すべての仮想チャネルが許可されます。</p> <p>仮想チャネルの設定はエージェントとクライアントの両方に適用されます。仮想チャネルを使用するには、エージェントとクライアントの両方で仮想チャネルを有効にする必要があります。</p> <p>仮想チャネルの設定には、PCoIP ホスト上でのクリップボードのリモート処理を無効にできるチェック ボックスが別にあります。この値はエージェントにのみ適用されます。</p> <p>デフォルトでは、クリップボードの処理を含め、すべての仮想チャネルが有効です。</p>
Configure the PCoIP transport header	<p>PCoIP 転送ヘッダを構成し、転送セッションの優先度を設定します。</p> <p>PCoIP 転送ヘッダは、すべての PCoIP UDP パケットに追加される 32 ビット ヘッダです (転送ヘッダが有効にされ、両側でサポートされる場合に限りです)。PCoIP 転送ヘッダによって、ネットワーク デバイスは、ネットワークの輻輳を処理するときに、より良い優先順位/QoS 決定を行うことができます。デフォルトでは、転送ヘッダは有効になっています。</p> <p>転送セッションの優先度は、PCoIP 転送ヘッダで報告される PCoIP セッション優先度を決定します。ネットワーク デバイスは、指定した転送セッション優先度に基づいてより良い優先順位/QoS 決定を行います。</p> <p>Configure the PCoIP transport header 設定を有効にすると、以下の転送セッション優先度が使用できるようになります。</p> <ul style="list-style-type: none"> ■ [高] ■ [中] (デフォルト値) ■ [低] ■ [未定義] <p>転送セッション優先度値は、PCoIP エージェントとクライアントによって取り決められます。PCoIP エージェントが転送セッション優先度値を指定する場合、セッションはエージェントが指定したセッション優先度を使用します。クライアントだけが転送セッション優先度を指定した場合、セッションはクライアントが指定したセッション優先度を使用します。エージェントとクライアントのどちらもが転送セッション優先度を指定しなければ、または[未定義の優先度] が指定された場合、セッションはデフォルト値である [中] 優先度を使用します。</p>

設定	説明
Configure the TCP port to which the PCoIP host binds and listens	<p>ソフトウェア PCoIP ホストがバインドされる TCP エージェント ポートを指定します。TCP ポートの値によって、エージェントがバインドを試行するベース TCP ポートが指定されます。TCP ポート範囲の値によって、ベース ポートが使用可能でない場合に使用を試行する追加ポートの数が指定されます。ポート範囲は 1 から 10 までの間にする必要があります。</p> <p>この範囲は、ベース ポートから、ベース ポートにポート範囲を加えた数値までになります。たとえば、ベース ポートが 4172 でポート範囲が 10 の場合、範囲は 4172 から 4182 までになります。</p> <p>リトライ ポート範囲の値を 0 に設定しないでください。この値を 0 に設定すると、PCoIP 表示プロトコルでユーザーがデスクトップにログインする時に接続に失敗します。Horizon Client は、このデスクトップの表示プロトコルは現在使用できません。システム管理者にお問い合わせください。というエラー メッセージを返します。</p> <p>この設定は Horizon Agent にのみ適用されます。</p> <p>シングル ユーザー マシンでは、View 4.5 以降でのデフォルトのベース TCP ポートは 4172 です。View 4.0.x 以前でのデフォルトのベース TCP ポートは 50002 です。デフォルトのポート範囲は 1 です。</p> <p>RDS ホストでは、デフォルトのベース TCP ポートは 4173 です。PCoIP が RDS ホストで使用される場合、ユーザー接続ごとに個別の PCoIP ポートが使用されます。リモート デスクトップ サービスによって設定されるデフォルトのポート範囲は、同時ユーザー接続の予想される最大数に対応できる十分な大きさです。</p> <hr/> <p>重要: ベスト プラクティスとして、このポリシー設定を使用して RDS ホストのデフォルトのポート範囲を変更したり、TCP ポート値をデフォルトの 4173 から変更したりしないでください。最も重要なこととして、TCP ポート値を 4172 に設定しないでください。この値を 4172 に設定すると、RDS セッション中の PCoIP パフォーマンスに悪影響を及ぼします。</p>

設定	説明
Configure the UDP port to which the PCoIP host binds and listens	<p>ソフトウェア PCoIP ホストがバインドされる UDP エージェント ポートを指定します。</p> <p>UDP ポートの値によって、エージェントがバインドを試行するベース UDP ポートが指定されます。UDP ポート範囲の値によって、ベース ポートが使用可能でない場合に使用を試行する追加ポートの数が指定されます。ポート範囲は 1 から 10 までの間にする必要があります。</p> <p>リトライ ポート範囲の値を 0 に設定しないでください。この値を 0 に設定すると、PCoIP 表示プロトコルでユーザーがデスクトップにログインする時に接続に失敗します。Horizon Client は、このデスクトップの表示プロトコルは現在使用できません。システム管理者にお問い合わせください。というエラー メッセージを返します。</p> <p>この範囲は、ベース ポートから、ベース ポートにポート範囲を加えた数値までになります。たとえば、ベース ポートが 4172 でポート範囲が 10 の場合、範囲は 4172 から 4182 までになります。</p> <p>この設定は Horizon Agent にのみ適用されます。</p> <p>シングル ユーザー マシンでは、View 4.5 以降でのデフォルトのベース UDP ポートは 4172、View 4.0.x 以前でのデフォルトのベース UDP ポートは 50002 です。デフォルトのポート範囲は 10 です。</p> <p>RDS ホストでは、デフォルトのベース UDP ポートは 4173 です。PCoIP が RDS ホストで使用される場合、ユーザー接続ごとに個別の PCoIP ポートが使用されます。リモート デスクトップ サービスによって設定されるデフォルトのポート範囲は、同時ユーザー接続の予想される最大数に対応できる十分な大きさです。</p> <p>重要: ベスト プラクティスとして、このポリシー設定を使用して RDS ホストのデフォルトのポート範囲を変更したり、UDP ポート値をデフォルトの 4173 から変更したりしないでください。最も重要なこととして、UDP ポート値を 4172 に設定しないでください。この値を 4172 に設定すると、RDS セッション中の PCoIP パフォーマンスに悪影響を及ぼします。</p>
Enable access to a PCoIP session from a vSphere console	<p>vSphere Client コンソールにアクティブな PCoIP セッションの表示およびデスクトップへの入力の送信を許可するかどうかを決定します。</p> <p>デフォルトでは、クライアントが PCoIP によって接続されている場合、vSphere Client コンソール画面は空白になり、コンソールは入力を送信できません。デフォルト設定によって、PCoIP セッションがアクティブなときに悪意あるユーザーがユーザーのデスクトップを閲覧したりホストにローカルで入力できなくなります。</p> <p>この設定は Horizon Agent にのみ適用されます。</p> <p>この設定を無効にするか、構成しない場合は、コンソール アクセスは許可されません。この設定を有効にすると、コンソールに PCoIP セッションが表示され、コンソール入力が許可されます。</p> <p>この設定を有効にした場合、Windows 7 システム上で実行している PCoIP セッションは、Windows 7 仮想マシンがハードウェア v8 である場合にのみコンソールに表示できます。ハードウェア v8 は ESXi 5.0 以降でのみ使用できます。一方、Windows 7 システムへのコンソール入力は、仮想マシンがどのハードウェア バージョンであっても許可されます。</p>

設定	説明
Enable the FIPS 140-2 approved mode of operation	<p>リモート PCoIP 接続の確立に、FIPS 140-2 で承認された暗号化アルゴリズムおよびプロトコルのみを使用するかどうかを指定します。この設定を有効にすると、AES128-GCM 暗号化を無効にする設定が上書きされます。</p> <p>この設定はエージェントとクライアントの両方に適用されます。一方または両方のエンドポイントを、FIPS モードで動作するように構成できます。FIPS モードで動作するように 1 つのエンドポイントを構成すると、セッション ネゴシエーションに使用できる暗号化アルゴリズムが制限されます。</p> <p>FIPS モードは View 4.5 以降で使用できます。View 4.0.x 以前では、FIPS モードは使用できず、この設定を構成しても効果がありません。</p> <p>この設定を無効にするか、構成しない場合は、FIPS モードが使用されます。</p>
Enable/disable audio in the PCoIP session	<p>PCoIP セッションでオーディオを有効にするかどうかを指定します。両方のエンドポイントでオーディオが有効になっている必要があります。この設定を有効にすると、PCoIP オーディオが許可されます。この設定を無効にすると、PCoIP オーディオが無効になります。この設定を構成しないと、デフォルトでオーディオが有効になります。</p>
Enable/disable microphone noise and DC offset filter in PCoIP session	<p>PCoIP セッション中にマイク入力のマイク ノイズ フィルタおよび DC オフセット フィルタを有効にするかどうかを決定します。</p> <p>この設定は Horizon Agent と Teradici オーディオ ドライバのみに適用されます。</p> <p>この設定が構成されていない場合、Teradici オーディオ ドライバは、デフォルトでマイク ノイズ フィルタおよび DC オフセット フィルタを使用します。</p>
Turn on PCoIP user default input language synchronization	<p>PCoIP セッションでのユーザーのデフォルト入力言語と、PCoIP クライアント エンドポイントのデフォルト入力言語を同期するかどうかを指定します。この設定を有効にすると、同期が許可されます。この設定を無効にするか、構成しない場合は、同期が許可されません。</p> <p>この設定は Horizon Agent にのみ適用されます。</p>

PCoIP クリップボードの設定

View PCoIP ADM テンプレート ファイルには、コピーおよび貼り付け操作に関するクリップボード設定を構成するグループ ポリシー設定が含まれます。

表 17-9. PColP クリップボード ポリシー設定

設定	説明
Configure clipboard memory size on server (in kilobytes)	<p>キロバイト単位で、サーバのクリップボードのメモリ サイズの値を指定します。クライアントにも、クリップボードのメモリ サイズの値があります。セッション設定後、サーバは自身のクリップボードのメモリ サイズの値をクライアントに送信します。有効なクリップボードのメモリ サイズは、クライアントとサーバのクリップボードのメモリ サイズの値の小さい方となります。</p> <p>指定できる最小値は 512 KB、最大値は 16384 KB です。0 を指定する場合、または値を指定しない場合、サーバのクリップボードのメモリ サイズは、デフォルトで 1024 KB になります。</p> <p>この設定は、バージョン 7.0.1 以降、および Horizon Client 4.1 以降がインストールされている Windows、Linux および Mac クライアントのみに適用されます。以前のリリースでは、クリップボードのメモリ サイズは 1 MB です。</p> <p>注: ネットワークによっては、クリップボードのメモリ サイズを大きくすると、パフォーマンスに悪影響が及ぶ場合があります。クリップボードのメモリ サイズは、16 MB を超える値に設定しないことを推奨します。</p>
Configure clipboard redirection	<p>クリップボード リダイレクトを許可する方向を決定します。次のいずれかの値を選択できます。</p> <ul style="list-style-type: none"> ■ [クライアントからエージェントの方向のみ有効] (すなわち、クライアント システムからリモート デスクトップにのみ、コピーおよび貼り付けを許可します)。 ■ [どちらの方向も無効] ■ [どちらの方向も有効] ■ [エージェントからクライアントの方向のみ有効] (すなわち、リモート デスクトップからクライアント システムにのみ、コピーおよび貼り付けを許可します)。 <p>クリップボードのリダイレクトは、仮想チャネルとして実装されます。仮想チャネルが無効になっている場合、クリップボードのリダイレクトは機能しません。</p> <p>この設定は Horizon Agent にのみ適用されます。</p> <p>この設定が無効または構成されていない場合、デフォルト値は [クライアントからエージェントの方向のみ有効] です。</p>
Filter text out of the incoming clipboard data	<p>クライアントからエージェントに送信されるクリップボード データからテキスト形式のデータを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。</p> <p>この設定はバージョン 7.0.2 以降に適用されます。</p>
Filter Rich Text Format data out of the incoming clipboard data	<p>クライアントからエージェントに送信されるクリップボード データからリッチ テキスト形式のデータを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。</p> <p>この設定はバージョン 7.0.2 以降に適用されます。</p>
Filter images out of the incoming clipboard data	<p>クライアントからエージェントに送信されるクリップボード データからイメージデータを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。</p> <p>この設定はバージョン 7.0.2 以降に適用されます。</p>

設定	説明
Filter Microsoft Office text data out of the incoming clipboard data	クライアントからエージェントに送信されるクリップボード データから Microsoft Office のテキスト形式データ (BIFF12 形式) を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。この設定はバージョン 7.0.2 以降に適用されます。
Filter Microsoft Chart and Smart Art data out of the incoming clipboard data	クライアントからエージェントに送信されるクリップボード データから Microsoft Office チャートおよび Smart Art データ (Art::GVML ClipFormat) を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。この設定はバージョン 7.0.2 以降に適用されます。
Filter Microsoft Text Effects data out of the incoming clipboard data	クライアントからエージェントに送信されるクリップボード データから Microsoft Office のテキスト エフェクト データ (HTML 形式) を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。この設定はバージョン 7.0.2 以降に適用されます。
Filter text out of the outgoing clipboard data	エージェントからクライアントに送信されるクリップボード データからテキスト形式のデータを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。この設定はバージョン 7.0.2 以降に適用されます。
Filter Rich Text Format data out of the outgoing clipboard data	エージェントからクライアントに送信されるクリップボード データからリッチ テキスト形式のデータを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。この設定はバージョン 7.0.2 以降に適用されます。
Filter images out of the outgoing clipboard data	エージェントからクライアントに送信されるクリップボード データからイメージ データを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。この設定はバージョン 7.0.2 以降に適用されます。
Filter Microsoft Office text data out of the outgoing clipboard data	エージェントからクライアントに送信されるクリップボード データから Microsoft Office のテキスト形式データ (BIFF12 形式) を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。この設定はバージョン 7.0.2 以降に適用されます。

設定	説明
Filter Microsoft Chart and Smart Art data out of the outgoing clipboard data	<p>エージェントからクライアントに送信されるクリップボード データから Microsoft Office チャートおよび Smart Art データ (Art::GVML ClipFormat) を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。</p> <p>この設定はバージョン 7.0.2 以降に適用されます。</p>
Filter Microsoft Text Effects data out of the outgoing clipboard data	<p>エージェントからクライアントに送信されるクリップボード データから Microsoft Office のテキスト エフェクト データ (HTML 形式) を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。</p> <p>この設定はバージョン 7.0.2 以降に適用されます。</p>

PCoIP の帯域幅設定

View PCoIP ADM テンプレート ファイルには、PCoIP の帯域幅特性を構成するグループ ポリシー設定が含まれます。

表 17-10. View PCoIP のセッション帯域幅変数

設定	説明
Configure the maximum PCoIP session bandwidth	<p>PCoIP セッションの最大帯域幅をキロビット/秒単位で指定します。この帯域幅には、イメージ、オーディオ、仮想チャネル、USB、および制御 PCoIP のすべてのトラフィックが含まれます。</p> <p>この値を、想定される同時並行の PCoIP セッションの数を考慮に入れたうえで、エンドポイントが接続されるリンクの合計容量に設定します。たとえば、4 メガビット/秒のインターネット接続を介して接続される単一ユーザーの VDI 構成 (単一の PCoIP セッション) では、他のネットワーク トラフィックのための余地を確保するためにこの値を 4 メガビット、またはそれから 10% 引いた値に設定します。複数の VDI ユーザーまたは RDS 構成のいずれかで構成される、複数の同時並行 PCoIP セッションでリンクを共有することを想定している場合には、設定を適宜調整することを推奨します。ただし、この値を低くすると、各アクティブ セッションの最大帯域幅が制限されます。</p> <p>この値を設定すると、エージェントがリンク容量よりも高い速度での送信を試行して、過剰なパケット損失が発生したり、ユーザーの操作性が低下したりすることがなくなります。この値は対称型です。クライアント側とエージェント側で設定されている 2 つの値のうち、小さい方の値がクライアントとエージェントで強制的に使用されます。たとえば、最大帯域幅を 4 メガビット/秒に設定すると、それがクライアント側で行われた設定でも、エージェントは強制的にそれ以下の速度で送信するようになります。</p> <p>エンドポイント上でこの設定を無効にするか、構成しない場合、エンドポイントは帯域幅を制限しません。この設定を構成する場合、その設定はエンドポイントの最大帯域幅制限としてキロビット/秒単位で使用されます。</p> <p>この設定が構成されていない場合のデフォルト値は、900000 キロビット/秒になります。この設定は Horizon Agent とクライアントに適用されます。2 つのエンドポイントの設定が異なる場合は、小さい方の値が使用されます。</p>
Configure the PCoIP session bandwidth floor	<p>PCoIP セッションによって予約される帯域幅の下限をキロバイト/秒単位で指定します。この設定では、エンドポイントの帯域幅で期待される最小送信速度が構成されます。この設定を使用してエンドポイントの帯域幅を予約すると、ユーザーは帯域幅が使用可能になるまで待つ必要がなくなるため、セッションの応答性が向上します。</p> <p>すべてのエンドポイントの合計予約帯域幅を過剰にサブスクライブしないように注意してください。また、構成内の全接続の帯域幅下限の合計がネットワークの容量を超えないように注意してください。</p> <p>デフォルト値は 0 です。これは、最小帯域幅が予約されないことを意味します。この設定を無効にするか、構成しない場合、最小帯域幅は予約されません。</p> <p>この設定は Horizon Agent とクライアントに適用されますが、構成されたエンドポイントにのみ影響します。</p> <p>この設定をアクティブ PCoIP セッション中に変更すると、変更が直ちに反映されます。</p>
Configure the PCoIP session MTU	<p>PCoIP セッションでの UDP パケットの最大転送ユニット (MTU) サイズを指定します。この MTU サイズには、IP および UDP のパケット ヘッダーが含まれます。TCP では MTU の設定に標準の MTU 検出メカニズムが使用されるため、この設定による影響を受けません。</p> <p>最大 MTU サイズは 1500 バイトです。最小 MTU サイズは 500 バイトです。デフォルト値は 1300 バイトです。</p> <p>通常、MTU サイズを変更する必要はありません。PCoIP パケットの断片化の原因となる、通常と異なるネットワーク設定を使用する場合は、この値を変更してください。</p> <p>この設定は Horizon Agent とクライアントに適用されます。2 つのエンドポイントの MTU サイズ設定が異なる場合は、小さい方のサイズが使用されます。</p> <p>この設定を無効にするか、構成しない場合、クライアントでは Horizon Agent とのネゴシエーションにデフォルト値が使用されます。</p>

設定	説明
Configure the PCoIP session audio bandwidth limit	<p>PCoIP セッションでオーディオ（サウンドの再生）に使用できる最大帯域幅を指定します。</p> <p>オーディオ処理では、オーディオに使用される帯域幅が監視されます。この処理によって、現在の帯域幅使用率で可能な最善のオーディオを提供するオーディオ圧縮アルゴリズムが選択されます。帯域幅制限が設定されている場合、帯域幅の制限内に収まるようになるまで、圧縮アルゴリズムの選択が変更されて品質が低下します。指定された帯域幅の制限内で最低品質のオーディオを提供できない場合は、オーディオが無効になります。</p> <p>圧縮なしの高品質なステレオ オーディオを再生できるようにするには、この値を 1600 キロビット/秒以上に設定します。450 キロビット/秒以上に設定すると、高品質な圧縮ステレオ オーディオを提供できます。50 ～ 450 キロビット/秒の値を設定すると、FM ラジオから電話までの品質のオーディオになります。50 キロビット/秒未満の値を設定すると、オーディオが再生されない可能性があります。</p> <p>この設定は Horizon Agent にのみ適用されます。この設定による効果を得るには、両方のエンドポイントでオーディオを有効にする必要があります。</p> <p>また、この設定は USB オーディオには影響しません。</p> <p>この設定を無効にするか、構成しない場合、デフォルトのオーディオ帯域幅制限である 500 キロビット/秒が構成され、オーディオ圧縮アルゴリズムの選択が制限されます。この設定を構成すると、値がキロビット/秒単位で計測され、デフォルトのオーディオ帯域幅制限は 500 キロビット/秒となります。</p> <p>この設定は View 4.6 以降に適用されます。それ以前のバージョンの View では影響がありません。</p> <p>この設定をアクティブ PCoIP セッション中に変更すると、変更が直ちに反映されます。</p>
Turn off Build-to-Lossless feature	<p>PCoIP プロトコルのロスレス構築機能をオフまたはオンのどちらにするかを指定します。この機能は、デフォルトでオフになっています。</p> <p>この設定を有効にするか、構成しない場合、ロスレス構築機能はオフになり、イメージやその他のデスクトップおよびアプリケーション コンテンツがロスレス状態まで構築されることはありません。帯域幅が制約されたネットワーク環境では、ロスレス構築機能をオフにすることで帯域幅を節約できます。</p> <p>この設定を無効にするとロスレス構築機能がオンになります。イメージおよびその他のデスクトップおよびアプリケーション コンテンツをロスレス状態で構築することが必要な環境では、ロスレス構築機能をオンにすることが推奨されています。</p> <p>この設定をアクティブ PCoIP セッション中に変更すると、変更が直ちに反映されます。</p> <p>PCoIP のロスレス構築機能の詳細については、PCoIP ロスレス構築機能を参照してください。</p>

PCoIP のキーボード設定

View PCoIP ADM テンプレート ファイルには、キーボードの使用方法に影響を及ぼす PCoIP の設定を構成するグループ ポリシー設定が含まれます。

表 17-11. キーボード用の View PCoIP のセッション変数

設定	説明
Disable sending CAD when users press Ctrl+Alt+Del	<p>このポリシーが有効になっている場合、PCoIP セッション中に Secure Attention Sequence (SAS) をリモート デスクトップに送信するには、Ctrl+Alt+Del ではなく Ctrl+Alt+Insert を押す必要があります。</p> <p>ユーザーがクライアント エンドポイントをロックするために Ctrl+Alt+Del を押したとき、ホストとゲストの両方に SAS が送信されるために混乱が生じる場合は、この設定を有効にすることを推奨します。</p> <p>この設定は Horizon Agent にのみ適用されて、クライアントには影響しません。</p> <p>このポリシーが構成されていない、または無効になっている場合は、Ctrl+Alt+Del または Ctrl+Alt+Insert を押して SAS をリモート デスクトップに送信できます。</p>
Use alternate key for sending Secure Attention Sequence	<p>Secure Attention Sequence (SAS) を送信するための、Insert キーの代替キーを指定します。</p> <p>この設定を使用して、PCoIP セッション中にリモート デスクトップの内部から起動された仮想マシンで Ctrl+Alt+Ins のキー シーケンスを保持できます。</p> <p>たとえば、ユーザーが PCoIP デスクトップ内から vSphere Client を起動し、vCenter Server で仮想マシンのコンソールを開くことができます。vCenter Server 仮想マシン上のゲスト オペレーティング システム内で Ctrl+Alt+Ins シーケンスを使用すると、仮想マシンに Ctrl+Alt+Del の SAS が送信されます。この設定を構成すると、Ctrl + Alt + <i>Alternate Key</i>のシーケンスで PCoIP デスクトップに Ctrl+Alt+Del の SAS を送信できます。</p> <p>この設定を有効にする場合は、代替キーをドロップダウン メニューから選択する必要があります。この設定を有効にして、値を未指定のままにすることはできません。</p> <p>この設定を無効にするか、構成しない場合は、Ctrl+Alt+Ins のキー シーケンスが SAS として使用されます。</p> <p>この設定は Horizon Agent にのみ適用されて、クライアントには影響しません。</p>

PCoIP ロスレス構築機能

PCoIP 表示プロトコルを構成して、プログレッシブ構築またはロスレス構築と呼ばれるエンコーディング方法を使用できます。この方法により、制約のあるネットワーク条件下でも全体的に最適なユーザー体験を提供できます。この機能は、デフォルトでオフになっています。

ロスレス構築機能ではロッキー イメージと呼ばれる高度に圧縮された初期イメージを提供し、その後プログレッシブに完全なロスレス状態まで構築します。ロスレス状態とは、イメージが意図したとおり完全に忠実に表示されることです。

LAN 上では、PCoIP は、テキストを常にロスレス圧縮を使用して表示します。ロスレス機能が有効になっていて、セッションあたりの使用可能帯域幅が 1Mbps を下回った場合には、PCoIP は最初にロッキー テキスト イメージを表示し、そのイメージを素早くロスレス状態に構築します。このアプローチにより、ネットワーク条件が変化する中でもデスクトップの応答が早い状態に保ち、可能な限り最高の状態のイメージを表示することで、ユーザーに最適な体験を提供できます。

ロスレス構築機能には次の特長があります。

- 動的にイメージ品質を調整
- 混雑しているネットワーク上でイメージ品質を低減
- 画面更新の待ち時間を減らすことにより、応答性を維持

■ ネットワークの混雑解消時には最大イメージ品質を回復

Turn off Build-to-Lossless feature グループ ポリシー設定を無効にして、ロスレス構築機能をオンにすることができます。PCoIP の帯域幅設定を参照してください。

VMware Blast ポリシー設定

VMware Blast グループ ポリシー テンプレート ファイルの `vdm_blast.adm` には、VMware Blast 表示プロトコルのポリシー設定が含まれています。ポリシーを適用すると、設定がレジストリ キー `HKLM\Software\Policies\VMware, Inc.\VMware Blast\config` に保存されます。

これらの設定は、HTML Access およびすべての Horizon Client に適用されます。

表 17-12. VMware Blast ポリシー設定

設定	説明
Max Session Bandwidth	VMware Blast セッションの最大帯域幅をキロビット/秒 (kbps) 単位で指定します。この帯域幅には、イメージ、オーディオ、仮想チャネル、USB、および VMware Blast 制御のすべてのトラフィックが含まれます。デフォルトは 1 Gbps です。
Min Session Bandwidth	VMware Blast セッション用に予約された最小帯域幅をキロビット/秒 (kbps) 単位で指定します。デフォルトは 256 kbps です。
Max Bandwidth Slope for the Kbps Per Megapixel	VMware Blast セッション用に予約された最大帯域幅スロープをキロビット/秒 (kbps) 単位で指定します。最小値は 100 です。最大値は 100000 です。デフォルト値は 6200 です。
Max Frame Rate	画面更新の最大レートを指定します。この設定を使用して、ユーザーが使用する平均帯域幅を管理します。デフォルトは 1 秒あたり 30 回の更新です。
UDP Protocol	UDP プロトコルまたは TCP プロトコルを使用するかどうかを指定します。デフォルトでは、UDP プロトコルを使用しません。つまり TCP プロトコルを使用します。この設定を有効にすると、UDP プロトコルが使用されます。この設定では、レジストリ キーがある Horizon Agent マシンの再起動が必要となります。この設定は、常に TCP プロトコルが使用される HTML Access には適用されません。
H264	H.264 エンコードまたは JPEG/PNG エンコードを使用するかどうかを指定します。デフォルトでは、H.264 エンコードを使用します。
PNG	この設定を有効にしない、あるいは構成しない場合、PNG エンコードをリモート セッションに利用できます。この設定を無効にすると、JPEG/PNG モードにおけるエンコードでは、JPEG エンコードのみが使用されます。H.264 エンコードが有効な場合、このポリシーは適用されません。デフォルトでは、この設定は構成されていません。この設定は 7.0.2 以降に適用されます。
Screen Blanking	デスクトップにアクティブなセッションがある場合に、デスクトップ仮想マシンのコンソールに、ユーザーに表示される実際のデスクトップを表示するか、空の画面を表示するかを指定します。デフォルトでは、空の画面を表示します。
Cookie Cleanup Interval	アクティブではないセッションに関連付けられている Cookie を削除する頻度（ミリ秒）を決定します。デフォルトは 100 ミリ秒です。

設定	説明
Image Quality	<p>リモート ディスプレイのイメージ品質を指定します。2 つの低品質設定、2 つの高品質設定、および 1 つの中品質設定を指定できます。低品質設定は、スクロール発生時など、頻繁に変化する画面の領域に適しています。高品質設定は、より静的な画面の領域に適していて、イメージ品質がより高くなります。次の設定を指定できます。</p> <ul style="list-style-type: none"> ■ [Low JPEG Quality (低品質 JPEG)] (使用可能な値の範囲：1 ～ 100、デフォルト：25) ■ [Low JPEG Chroma Subsampling (低い JPEG 彩度のサブサンプリング)] (使用可能な値の範囲：4:1:0 (最低)、4:1:1、4:2:0、4:2:2、および 4:4:4 (最高)、デフォルト：4:1:0) ■ [Mid JPEG Quality (中品質 JPEG)] (使用可能な値の範囲：1 ～ 100、デフォルト：35) ■ [High JPEG Quality (高品質 JPEG)] (使用可能な値の範囲：1 ～ 100、デフォルト：90) ■ [High JPEG Chroma Subsampling (高い JPEG 彩度のサブサンプリング)] (使用可能な値の範囲：4:1:0 (最低)、4:1:1、4:2:0、4:2:2、および 4:4:4 (最高)、デフォルト：4:4:4)
H.264 Quality	<p>H.264 エンコードを使用するように構成されたリモート ディスプレイのイメージ品質を指定します。ロスレス圧縮でイメージをどれだけ制御するかを決定する量子化の最小および最大値を指定できます。最高のイメージ品質には量子化の最小値を指定できます。最低のイメージ品質には量子化の最大値を指定できます。次の設定を指定できます。</p> <ul style="list-style-type: none"> ■ [H264maxQP] (使用可能な値の範囲：0 ～ 51、デフォルト：36) ■ [H264minQP] (使用可能な値の範囲：0 ～ 51、デフォルト：10) <p>最高のイメージ品質のためには、使用可能な値の範囲の +5 または -5 以内の量子化値を設定します。</p>
HTTP Service	<p>セキュリティ サーバまたは Access Point アプライアンスとデスクトップの間の安全な通信 (HTTPS) に使用されるポートを指定します。このポートを開くようにファイアウォールを構成する必要があります。デフォルトは 22443 です。</p>
Audio playback	<p>オーディオ再生をリモート デスクトップに対して有効にするかどうかを指定します。この設定では、オーディオ再生を有効にします。</p>
Configure clipboard redirection	<p>クリップボード リダイレクトの許容される動作を指定します。次のオプションがあります。</p> <ul style="list-style-type: none"> ■ [どちらの方向も有効] ■ [どちらの方向も無効] ■ [Enabled client to server only (クライアントからサーバの方向のみ有効)] (ユーザーはクライアントからデスクトップへのみコピー/貼り付けを実行できます。) ■ [Enabled server to client only (サーバからクライアントの方向のみ有効)] (ユーザーはデスクトップからクライアントへのみコピー/貼り付けを実行できます。) <p>デフォルトは [Enabled client to server only (クライアントからサーバの方向のみ有効)] です。</p>
Clipboard memory size on server(in kilobytes)	<p>キロバイト単位で、サーバのクリップボードのメモリ サイズの値を指定します。クライアントにも、クリップボードのメモリ サイズの値があります。セッション設定後、サーバは自身のクリップボードのメモリ サイズの値をクライアントに送信します。有効なクリップボードのメモリ サイズは、クライアントとサーバのクリップボードのメモリ サイズの値の小さい方となります。</p> <p>指定できる最小値は 512 KB、最大値は 16384 KB です。0 を指定する場合、または値を指定しない場合、サーバのクリップボードのメモリ サイズは、デフォルトで 1024 KB になります。</p> <p>この設定は、バージョン 7.0.1 以降、および Horizon Client 4.1 以降がインストールされている Windows、Linux および Mac クライアントのみに適用されます。以前のリリースでは、クリップボードのメモリ サイズは 1 MB です。</p> <p>注： ネットワークによっては、クリップボードのメモリ サイズを大きくすると、パフォーマンスに悪影響が及ぶ場合があります。クリップボードのメモリ サイズは、16 MB を超える値に設定しないことを推奨します。</p>
Keyboard locale synchronization	<p>クライアントのキーボード ロケール リストやデフォルト キーボード ロケールを、リモート デスクトップまたはアプリケーションに同期させるかどうかを指定します。この設定を有効にすると、同期が発生します。この設定は Horizon Agent のみに適用されます。</p> <p>注： この機能は、Horizon Client for Windows のみにサポートされます。</p>

設定	説明
Configure file transfer	<p>リモート デスクトップと HTML Access クライアント間のファイル転送について許可される動作を指定します。次のいずれかの値を選択できます。</p> <ul style="list-style-type: none"> ■ [アップロードとダウンロードの両方を無効にする] ■ [アップロードとダウンロードの両方を有効にする] ■ [ファイルのアップロードのみを有効にする] (ユーザーはクライアントシステムからリモート デスクトップにのみファイルをアップロードできます)。 ■ [ファイルのダウンロードのみを有効にする] (ユーザーはリモート デスクトップからクライアントシステムにのみファイルをダウンロードできます)。 <p>デフォルトは、[ファイルのアップロードのみを有効にする] です。</p> <p>この設定は、バージョン 7.0.1 以降と HTML Access 4.1 以降にのみ適用されます。</p>
Filter text out of the incoming clipboard data	<p>クライアントからエージェントに送信されるクリップボード データからテキスト形式のデータを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。</p> <p>この設定はバージョン 7.0.2 以降に適用されます。</p>
Filter Rich Text Format data out of the incoming clipboard data	<p>クライアントからエージェントに送信されるクリップボード データからリッチ テキスト形式のデータを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。</p> <p>この設定はバージョン 7.0.2 以降に適用されます。</p>
Filter images out of the incoming clipboard data	<p>クライアントからエージェントに送信されるクリップボード データからイメージ データを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。</p> <p>この設定はバージョン 7.0.2 以降に適用されます。</p>
Filter Microsoft Office text data out of the incoming clipboard data	<p>クライアントからエージェントに送信されるクリップボード データから Microsoft Office のテキスト形式データ (BIFF12 形式) を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。</p> <p>この設定はバージョン 7.0.2 以降に適用されます。</p>
Filter Microsoft Chart and Smart Art data out of the incoming clipboard data	<p>クライアントからエージェントに送信されるクリップボード データから Microsoft Office チャートおよび Smart Art データ (Art::GVML ClipFormat) を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。</p> <p>この設定はバージョン 7.0.2 以降に適用されます。</p>
Filter Microsoft Text Effects data out of the incoming clipboard data	<p>クライアントからエージェントに送信されるクリップボード データから Microsoft Office のテキスト エフェクト データ (HTML 形式) を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。</p> <p>この設定はバージョン 7.0.2 以降に適用されます。</p>
Filter text out of the outgoing clipboard data	<p>エージェントからクライアントに送信されるクリップボード データからテキスト形式のデータを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。</p> <p>この設定はバージョン 7.0.2 以降に適用されます。</p>
Filter Rich Text Format data out of the outgoing clipboard data	<p>エージェントからクライアントに送信されるクリップボード データからリッチ テキスト形式のデータを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。</p> <p>この設定はバージョン 7.0.2 以降に適用されます。</p>

設定	説明
Filter images out of the outgoing clipboard data	エージェントからクライアントに送信されるクリップボード データからイメージ データを取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。
Filter Microsoft Office text data out of the outgoing clipboard data	エージェントからクライアントに送信されるクリップボード データから Microsoft Office のテキスト形式データ (BIFF12 形式) を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。
Filter Microsoft Chart and Smart Art data out of the outgoing clipboard data	エージェントからクライアントに送信されるクリップボード データから Microsoft Office チャートおよび Smart Art データ (Art::GVML ClipFormat) を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。
Filter Microsoft Text Effects data out of the outgoing clipboard data	エージェントからクライアントに送信されるクリップボード データから Microsoft Office のテキスト エフェクト データ (HTML 形式) を取り除くかどうかを指定します。この設定が有効にされており、チェック ボックスがオンになっていると、データは取り除かれます。この設定が無効にされているか、構成されていない場合は、データは許可されます。 この設定はバージョン 7.0.2 以降に適用されます。

VMware Blast ポリシー設定の適用

クライアントのセッション中に、次の VMware Blast ポリシーの変更があった場合、Horizon Client は変更を検出し、直ちに新しい設定を適用します。

- H264
- Audio Playback
- Max Session Bandwidth
- Min Session Bandwidth
- Max Frame Rate
- Image Quality

他のすべての VMware Blast ポリシーについては、マイクロソフト GPO 更新ルールが適用されます。GPO は、手動または Horizon Agent マシンの再起動により更新できます。詳細については、Microsoft ドキュメントを参照してください。

VMware Blast のロスレス圧縮の有効化

VMware Blast 表示プロトコルを有効にして、プログレッシブ構築またはロスレス構築と呼ばれるエンコーディング アプローチを使用できます。この機能では、ロッキー イメージと呼ばれる高度に圧縮された初期イメージを提供し、その後プログレッシブに完全なロスレス状態まで構築します。ロスレス状態とは、イメージが意図したとおり完全に忠実に表示されることです。

VMware Blast のロスレス圧縮を有効にするには、エージェント マシンの Windows レジストリにある HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config フォルダの EncoderBuildToPNG キーを 1 に設定します。デフォルト値は 0（無効）で、コーデックが PNG に構築されないことになり、ロスレスのフォーマットになります。

EncoderBuildToPNG キーの設定変更は、すぐに有効になります。

注: VMware Blast のロスレス圧縮を有効にすると、帯域幅や CPU 使用率の増加の原因になります。VMware では、ロスレス圧縮が必要な場合は、VMware Blast ではなく PCoIP 表示プロトコルを使用することを推奨します。PCoIP のロスレス圧縮の構成に関する情報については、[PCoIP ロスレス構築機能](#) を参照してください。

リモート デスクトップ サービス グループ ポリシーの使用

リモート デスクトップ サービス (RDS) グループ ポリシーを使用し、RDS ホスト、RDS デスクトップ セッション、および RDS アプリケーション セッションの構成とパフォーマンスを制御できます。View には、View でサポートされる Microsoft RDS グループ ポリシーが含まれている ADMX ファイルが提供されています。

ベスト プラクティスとして、対応する Microsoft グループ ポリシーではなく View ADMX ファイルで提供されているグループ ポリシーを構成することをお勧めします。View グループ ポリシーは、View 展開をサポートすることが保証されています。

RDS CAL（接続デバイス数）ストレージの構成

CAL（接続デバイス数）ストレージ オプションを構成して、CAL の保存場所を指定できます。この機能により、CAL を保存するかどうかを指定できます。

View RDS デプロイに Windows Server 2008 システムと Windows Server 2012 システムの両方が存在するなど、CAL（接続デバイス数）の過剰使用が考えられる場合があります。この機能を有効にすると、View RDS のデプロイで CAL の使用が効率的になります。この機能は、発行されたライセンスを保存し、クライアントから RDS ホストへの接続を試みているときにライセンスを提供して、ライセンスの更新があればライセンスを再保存することで達成されます。

View Administrator で、または手動で View LDAP データベースで、RDS CAL（接続デバイス数）を構成できます。

手順

- 1 View Administrator で、[View 構成] > [グローバル設定] をクリックします。
- 2 [全般] ペインで、[編集] をクリックします。

- 3 [RDS CAL (接続デバイス数) ストレージ オプション] ドロップダウン メニューから、次のいずれかの構成を選択します。

オプション	説明
ブローカーのみに保存	CAL (接続デバイス数) はブローカーのみに保存されます。 注: LDAP エントリは、 <code>cs-enablerdslicensing=true</code> および <code>sendRdsLicense=false</code> です。
クライアントとブローカーの両方に保存	CAL (接続デバイス数) はクライアントとブローカーの両方に保存されます。 注: LDAP エントリは、 <code>cs-enablerdslicensing=true</code> および <code>sendRdsLicense=true</code> です。
CAL (接続デバイス数) を保存しない	CAL (接続デバイス数) はどこにも保存されません。 注: LDAP エントリは、 <code>cs-enablerdslicensing=false</code> および <code>sendRdsLicense=false</code> です。

- 4 [OK] をクリックします。

リモート デスクトップ サービス ADMX ファイルを Active Directory へ追加

View RDS ADMX ファイルのポリシー設定を Active Directory のグループ ポリシー オブジェクト (GPO) に追加することができます。個々の RDS ホストに RDS ADMX ファイルをインストールすることもできます。

前提条件

- RDS グループ ポリシー設定の GPO を作成し、それらを RDS ホストを含む OU にリンクさせます。
- Active Directory サーバでグループ ポリシー管理機能が使用できることを確認します。
グループ ポリシー管理コンソールを開く手順は、Windows 2012、Windows 2008、および Windows 2003 Active Directory の各バージョンによって異なります。[View グループ ポリシーの GPO の作成](#)を参照してください。

手順

- 1 View GPO Bundle .zip ファイルを <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 GPO Bundle が含まれます。

ファイル名は `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` で、`x.x.x` はバージョン、`yyyyyyy` はビルド番号を表します。View のグループ ポリシー設定用の ADM ファイルと ADMX ファイルはすべて、このファイルで提供されています。

- 2 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip ファイルを解凍して、RDS ADMX ファイルを Active Directory または RDS ホストにコピーします。
 - a vmware_rdsh.admx ファイル、vmware_rdsh_server.admx ファイル、および en-US フォルダを Active Directory または RDS ホストの C:\Windows\PolicyDefinitions フォルダにコピーします。
 - b (オプション) 言語リソース ファイル vmware_rdsh.adml および vmware_rdsh_server.adml を Active Directory または RDS ホストの C:\Windows\PolicyDefinitions\ 内の適切なサブフォルダにコピーします。
- 3 Active Directory ホストで、[グループ ポリシー管理エディタ]を開きます。

個々の RDS ホストでは、gpedit.msc ユーティリティで [ローカル グループ ポリシー エディタ]を開きます。

View RDS グループ ポリシー設定は、[コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [Windows コンポーネント] - [Horizon View RDSH サービス] - [リモート デスクトップ セッション ホスト] フォルダにインストールされています。
- 4 (オプション) [Horizon View RDSH サービス] - [リモート デスクトップ セッション ホスト] フォルダで、グループ ポリシー設定を構成します。

RDS アプリケーションの互換性の設定

RDS アプリケーションの互換性グループ ポリシー設定は、Windows インストーラの互換性、リモート デスクトップの IP 仮想化、ネットワーク アダプタの選択、RDS ホスト IP アドレスの使用などを制御します。

表 17-13. RDS アプリケーションの互換性グループ ポリシー設定

設定	説明
Turn off Windows Installer RDS Compatibility	<p>このポリシー設定は、Windows Installer RDS Compatibility が、フルインストールされたアプリケーションのユーザーごとに実行されるかどうかを指定します。Windows インストーラで一度に実行できる <code>msiexec</code> プロセス インスタンスは 1 つです。デフォルトでは、Windows Installer RDS Compatibility が有効になります。</p> <p>このポリシー設定を有効にすると、Windows Installer RDS Compatibility が無効になり、一度に実行できる <code>msiexec</code> プロセス インスタンスは 1 つになります。</p> <p>このポリシー設定を無効にするか、または構成しないままにすると、Windows Installer RDS Compatibility が有効になり、複数のユーザーごとのアプリケーションのインストール要求が待機中になり、それらが受け取られた順に <code>msiexec</code> プロセスによって処理されます。</p>
Turn on Remote Desktop IP Virtualization	<p>このポリシー設定は、リモート デスクトップの IP 仮想化を有効にするかどうかを指定します。</p> <p>デフォルトでは、リモート デスクトップの IP 仮想化は無効です。</p> <p>このポリシー設定を有効にすると、リモート デスクトップの IP 仮想化が有効になります。この設定が適用されるモードを選択できます。プログラム単位モードを使用する場合は、仮想 IP アドレスを使用するプログラムのリストを入力する必要があります。各プログラムを個別の行に入力してください（プログラム間に空の行を入れないでください）。例：</p> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <pre>explorer.exe mstsc.exe</pre> </div> <p>このポリシー設定を無効にするか、または構成しないままにすると、リモート デスクトップの IP 仮想化は無効になります。</p>
Select the network adapter to be used for Remote Desktop IP Virtualization	<p>このポリシー設定は、仮想 IP アドレスに使用されるネットワーク アダプタに対応する IP アドレスとネットワーク マスクを指定します。IP アドレスとネットワーク マスクは、Classless Inter-Domain Routing の表記で入力する必要があります。例：192.0.2.96/24。</p> <p>このポリシー設定を有効にすると、指定した IP アドレスとネットワーク マスクが使用されて、仮想 IP アドレスに使用されるネットワーク アダプタが選択されます。</p> <p>このポリシー設定を無効にするか、または構成しないままにすると、リモート デスクトップの IP 仮想化は無効になります。リモート デスクトップの IP 仮想化を機能させるためには、ネットワーク アダプタを構成する必要があります。</p>
Do not use Remote Desktop Session Host server IP address when virtual IP address is not available	<p>このポリシー設定は、仮想 IP アドレスが使用できない場合にリモート デスクトップ セッション ホスト サーバの IP アドレスをセッションが使用するかどうかを指定します。</p> <p>このポリシー設定を有効にすると、仮想 IP が使用できない場合に RD セッション ホスト サーバの IP アドレスが使用されません。このセッションではネットワーク接続が確立されていません。</p> <p>このポリシー設定を無効にするか、または構成しないままにすると、仮想 IP が使用できない場合、RD セッション ホスト サーバの IP アドレスが使用されます。</p>

RDS 接続の設定

RDS 接続グループ ポリシー設定により、CPU スケジュール設定の公平なシェアを無効にすることができます。

表 17-14. RDS 接続グループ ポリシー設定

設定	説明
Turn off Fair Share CPU Scheduling	<p>CPU スケジュール設定の公平なシェアは、同じ RD セッション ホスト サーバ上のすべてのリモート デスクトップ サービス セッション間で、セッションの数と、各セッション内でのプロセッサ時間の要求に基づき、プロセッサ時間を動的に分散します。</p> <p>このポリシー設定を有効にすると、CPU スケジュール設定の公平なシェアはオフになります。</p> <p>このポリシー設定を無効にするか、または構成しない場合、CPU スケジュール設定の公平なシェアはオンになります。</p>

RDS デバイスおよびリソースのリダイレクトの設定

RDS デバイスおよびリソース リダイレクト グループ ポリシー設定により、リモート デスクトップ サービス セッションのクライアント コンピュータのデバイスおよびリソースへのアクセスを制御します。

表 17-15. RDS デバイスおよびリソース リダイレクト グループ ポリシー設定

設定	説明
Allow time zone redirection	<p>このポリシー設定は、クライアント コンピュータがタイム ゾーン設定をリモート デスクトップ サービス セッションにリダイレクトするかどうかを決定します。</p> <p>このポリシー設定を有効にすると、タイム ゾーン リダイレクトが可能なクライアントはタイム ゾーン情報をサーバに送信します。サーバ ベースの時間は現在のセッション時間を計算するために使用されます（現在のセッション時間 = サーバ ベースの時間 + クライアント タイム ゾーン）。</p> <p>このポリシー設定を無効にする場合、または構成しない場合、クライアント コンピュータはタイム ゾーン情報をリダイレクトしません。セッション タイム ゾーンはサーバ タイム ゾーンと同じです。</p>

RDS ライセンスの設定

RDS ライセンス グループ ポリシー設定では、RDS ライセンス サーバが参照される順番、問題通知を表示するかどうか、RDS クライアント アクセス ライセンス (CAL) でユーザーごとのライセンスまたはデバイスごとのライセンスのどちらを使用するかを管理します。

表 17-16. RDS ライセンス グループ ポリシー設定

設定	説明
Use the specified Remote Desktop license servers	<p>このポリシー設定により、RD セッション ホスト サーバがリモート デスクトップ ライセンス サーバを探す順番を指定できます。</p> <p>このポリシーを有効にすると、RD セッション ホスト サーバは指定したライセンス サーバを最初に探します。指定したライセンス サーバが見つからない場合、RD セッション ホスト サーバにより自動ライセンス サーバ検出が試行されます。</p> <p>自動ライセンス サーバ検出では、Windows Server ベースのドメインの RD セッション ホスト サーバにより、次の順番でライセンス サーバへのアクセスが試行されます。</p> <ol style="list-style-type: none"> 1 リモート デスクトップ セッション ホスト 構成ツールで指定されたライセンス サーバ 2 Active Directory ドメイン サービスで公開されたライセンス サーバ 3 RD セッション ホスト サーバと同じドメインのドメイン コントローラにインストールされたライセンス サーバ <p>このポリシー設定を無効にするか、構成しなかった場合、RD セッション ホスト サーバでは、リモート デスクトップ セッション ホスト 構成ツールで指定されたライセンス サーバ検出モードが使用されます。</p>
Hide notifications about RD Licensing problems that affect the RD Session Host server	<p>このポリシー設定により、RD セッション ホスト サーバに影響する RD ライセンスに問題がある場合、RD セッション ホスト サーバに通知を表示するかどうかを決定します。</p> <p>デフォルトでは、RD セッション ホスト サーバに影響する RD ライセンスに問題がある場合、ローカル管理者としてログインした後に RD セッション ホスト サーバに通知が表示されます。RD セッション ホスト サーバのライセンス有効期間が切れるまでの日数も通知されます（該当する場合）。</p> <p>このポリシー設定を有効にすると、これらの通知は RD セッション ホスト サーバに表示されません。</p> <p>このポリシー設定を無効にするか、構成しなかった場合、ローカル管理者としてログインした後に、RD セッション ホスト サーバにこれらの通知が表示されます。</p>
Set the Remote Desktop licensing mode	<p>このポリシー設定により、この RD セッション ホスト サーバへの接続に必要なリモート デスクトップ サービス クライアント アクセス ライセンス (RDS CAL) のタイプを指定できます。</p> <p>このポリシー設定を使用して、次の 2 つのライセンス モードのうちいずれかを選択します。ユーザーごとまたはデバイスごと</p> <p>接続ユーザー数によるライセンス モードでは、この RD セッション ホスト サーバに接続する各ユーザー アカウントには、RDS CAL（接続ユーザー数）が必要になります。</p> <p>接続デバイス数によるライセンス モードでは、この RD セッション ホスト サーバに接続する各デバイスには、RDS CAL（接続デバイス数）が必要になります。</p> <p>このポリシー設定を有効にすると、ここで指定したライセンス モードは、リモート デスクトップ セッション ホストのインストール時に指定した、またはリモート デスクトップ セッション ホスト 構成ツールで指定したライセンス モードに優先します。</p> <p>このポリシー設定を無効にするか、構成しなかった場合、リモート デスクトップ セッション ホスト ロール サービスのインストール時に指定した、またはリモート デスクトップ セッション ホスト 構成ツールで指定したライセンス モードが使用されます。</p>

RDS プロファイルの設定

RDS プロファイル グループ ポリシー設定では、リモート デスクトップ サービス セッションの移動プロファイルおよびホーム ディレクトリの設定を制御します。

表 17-17. RDS プロファイル グループ ポリシー設定

設定	説明
Limit the size of the entire roaming user profile cache	<p>このポリシー設定により、ローカル ドライブ上の移動ユーザー プロファイルのキャッシュ全体のサイズを制限できます。このポリシー設定は、リモート デスクトップ セッション ホスト ロール サービスがインストールされているコンピュータにのみ適用されます。</p> <p>注: 個別のユーザー プロファイルのサイズを制限する場合は、[User Configuration\Policies\Administrative Templates\System\User Profiles] にある Limit profile size ポリシー設定を使用します。</p> <p>このポリシー設定を有効にする場合は、移動ユーザー プロファイルのキャッシュ全体の監視間隔（分単位）と最大サイズ（ギガバイト単位）を指定する必要があります。監視間隔で、移動ユーザー プロファイルのキャッシュ全体のサイズをチェックする頻度を決定します。移動ユーザー プロファイルのキャッシュ全体のサイズが指定した最大サイズを超えると、下回るまで最も古い（最も長く使われていない）移動ユーザー プロファイルが削除されます。このポリシー設定を無効にする、または構成しない場合、ローカル ドライブ上の移動ユーザー プロファイルのキャッシュ全体のサイズに制限は設定されません。</p> <p>注: [Computer Configuration\Policies\Administrative Templates\System\User Profiles] にある Prevent Roaming Profile changes from propagating to the server ポリシー設定が有効になっている場合、このポリシー設定は無視されます。</p>
Set Remote Desktop Services User Home Directory	<p>リモート デスクトップ サービスが、指定されたネットワーク共有またはローカル ディレクトリ パスを、リモート デスクトップ サービス セッションでユーザーのホーム ディレクトリのルートとして使用するかどうかを指定します。</p> <p>この設定を使用するには、[場所] ドロップダウン リストからホーム ディレクトリ（ネットワークまたはローカル）の場所を選択します。ディレクトリをネットワーク共有に置く場合は、ホーム ディレクトリのルート パスを \Computername\Sharename の形式で入力してから、ネットワーク共有をマッピングするドライブ文字を選択します。</p> <p>ホーム ディレクトリをローカル コンピュータに保持する場合は、ホーム ディレクトリのルート パスを環境変数や省略記号なしで Drive:\Path の形式で入力します。ログイン時にリモート デスクトップ サービスで自動的に追加されるため、ユーザー エイリアスのプレースホルダは指定しないでください。</p> <p>注: ローカル パスを指定する場合、[ドライブ レター] フィールドは無視されます。ローカル パスを指定することを選択したが、ホーム ディレクトリのルート パスにネットワーク共有名を入力した場合、リモート デスクトップ サービスはユーザーのホーム ディレクトリをネットワーク上の場所に配置します。</p> <p>ステータスが [有効] に設定されている場合、リモート デスクトップ サービスはユーザーのホーム ディレクトリを、ローカル コンピュータまたはネットワーク上で指定した場所に作成します。各ユーザーのホーム ディレクトリのパスは、指定されたホーム ディレクトリのルート パスおよびユーザーのエイリアスです。</p> <p>ステータスが [無効] または [構成されていません] に設定されている場合、ユーザーのホーム ディレクトリはサーバで指定されたものになります。</p>

設定	説明
Use mandatory profiles on the RD Session Host server	<p>このポリシー設定により、RD セッション ホスト サーバにリモートで接続しているすべてのユーザーについて、リモート デスクトップ サービスが必須のプロファイルを使用するかどうかを指定できます。</p> <p>このポリシー設定を有効にした場合、リモート デスクトップ サービスは Set path for Remote Desktop Services Roaming User Profile ポリシー設定で指定したパスを、必須のユーザー プロファイルのルート フォルダとして使用します。RD セッション ホスト サーバにリモートで接続しているすべてのユーザーは、同じユーザー プロファイルを使用します。</p> <p>このポリシー設定を無効にする、または構成しない場合、RD セッション ホスト サーバにリモートで接続しているユーザーは必須のユーザー プロファイルを使用しません。</p> <p>注: このポリシー設定を有効にするには、Set path for Remote Desktop Services Roaming User Profile ポリシー設定も有効にして構成する必要があります。</p>
Set path for Remote Desktop Services Roaming User Profile	<p>このポリシー設定では、リモート デスクトップ サービスが移動ユーザー プロファイルに使用するネットワーク パスを指定できます。</p> <p>デフォルトでは、リモート デスクトップ サービスはすべてのユーザー プロファイルを RD セッション ホスト サーバにローカルに保存します。このポリシー設定を使用して、ユーザープロファイルを一元的に保存できるネットワーク共有を指定できます。これにより、ユーザーはユーザー プロファイルにネットワーク共有を使用するように構成されているすべての RD セッション ホスト サーバ上のセッションで、同じプロファイルにアクセスできます。</p> <p>このポリシー設定を有効にすると、リモート デスクトップ サービスは指定されたパスをすべてのユーザー プロファイルのルート ディレクトリとして使用します。このプロファイルは、各ユーザーのアカウント名が名前として付けられたサブフォルダに含まれます。</p> <p>このポリシー設定を構成するには、ネットワーク共有へのパスを <code>\Computername\Sharename</code> の形式で入力します。ユーザーがログオンしてプロファイルが作成される際にリモート デスクトップ サービスで自動的に追加されるため、ユーザー アカウント名のプレースホルダは指定しないでください。指定したネットワーク共有が存在しない場合、リモート デスクトップ サービスにより RD セッション ホスト サーバにエラー メッセージが表示され、ユーザー プロファイルは RD セッション ホストサーバ上にローカルに保存されます。</p> <p>このポリシー設定を無効にする、または構成しない場合、ユーザー プロファイルは RD セッション ホスト サーバ上にローカルに保存されます。ユーザーのアカウントの [プロパティ] ダイアログ ボックスの [リモート デスクトップ サービス プロファイル] タブで、ユーザーのプロファイルのパスを構成できます。</p> <p>注:</p> <ol style="list-style-type: none"> 1 ポリシー設定によって有効になる移動ユーザー プロファイルは、リモート デスクトップ サービス接続にのみ適用されます。Windows 移動ユーザー プロファイルを構成させる場合もあります。リモート デスクトップ サービスの移動ユーザー プロファイルは、常にリモート デスクトップ サービス セッションで優先されます。 2 RD セッション ホスト サーバにリモートで接続しているすべてのユーザーについて、必須のリモート デスクトップ サービスの移動ユーザー プロファイルを構成するには、このポリシー設定を [Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\RD Session Host\Profiles].にある Use mandatory profiles on the RD Session Host server ポリシー設定と同時に使用します。Set path for Remote Desktop Services Roaming User Profile ポリシー設定で設定するパスには、必須のプロファイルを含める必要があります。

RDS リモート セッション環境の設定

RDS リモート セッション環境のグループ ポリシー設定では、リモート デスクトップ サービス セッションでのユーザー インターフェイスの構成を制御します。

表 17-18. RDS リモート セッション環境のグループ ポリシー設定

設定	説明
Remove Windows Security item from Start menu	<p>リモート デスクトップ クライアントの [設定] メニューから [Windows セキュリティ] の項目を削除するかどうかを指定します。この設定を使用して、未熟なユーザーがリモート デスクトップ サービスから間違えてログオフするのを防ぐことができます。</p> <p>ステータスが [有効] に設定されている場合、[スタート] メニューの [設定] に [Windows セキュリティ] は表示されません。このため、クライアント コンピュータで [Windows セキュリティ] ダイアログ ボックスを開くには、Ctrl +Alt+End などの Secure Attention Sequence (SAS) を入力する必要があります。</p> <p>ステータスが [無効] または [構成されていません] に設定されている場合、[Windows セキュリティ] は [設定] メニューに残ります。</p>

RDS セキュリティの設定

RDS Security group ポリシー設定で、ローカル管理者が権限のカスタマイズをできるようにするかどうかを制御します。

表 17-19. RDS Security Group ポリシー設定

設定	説明
Do not allow local administrators to customize permissions	<p>リモート デスクトップ セッション ホスト構成ツールで、セキュリティ権限をカスタマイズする管理者権限を無効にするかどうかを指定します。</p> <p>この設定を使用して、管理者がリモート デスクトップ セッション ホスト構成ツールの [アクセス権限] タブでユーザー グループを変更できないようにすることができます。デフォルトでは、管理者はこのような変更を行うことができます。</p> <p>ステータスが [有効] に設定されている場合、リモート デスクトップ セッション ホスト構成ツールの [アクセス権限] タブでは、接続ごとのセキュリティ記述子をカスタマイズしたり、既存のグループのデフォルトのセキュリティ記述子を変更したりすることはできません。すべてのセキュリティ記述子は読み取り専用です。</p> <p>ステータスが [無効] または [構成されていません] に設定されている場合でも、サーバ管理者にはリモート デスクトップ セッション ホスト構成ツールの [アクセス権限] タブのユーザーのセキュリティ記述子へのすべての読み取り/書き込み権限があります。</p> <p>注: ユーザーのアクセスを管理する際には、リモート デスクトップ ユーザー グループにユーザーを追加することをお勧めします。</p>

RDS 一時フォルダの設定

RDS 接続グループ ポリシー設定は、リモート デスクトップ サービス セッション用の一時フォルダの作成および削除を制御します。

表 17-20. RDS 一時フォルダのグループ ポリシー設定

設定	説明
Do not delete temp folder upon exit	<p>リモート デスクトップ サービスで、ユーザーのセッションごとの一時フォルダをログオフ時に保持するかどうかを指定します。</p> <p>この設定を使用して、ユーザーがセッションからログオフしても、リモート コンピュータ上のユーザーのセッション固有の一時フォルダを保持することができます。デフォルトでは、リモート デスクトップ サービスは、ユーザーがログオフする際にユーザーの一時フォルダを削除します。</p> <p>このステータスが [有効] に設定されている場合、ユーザーのセッションごとの一時フォルダは、ユーザーがセッションからログオフしても保持されます。</p> <p>このステータスが [無効] に設定されている場合、管理者がリモート デスクトップ セッション ホスト構成ツールで他の設定をしたとしても、一時フォルダはユーザーがログオフするときに削除されます。</p> <p>このステータスが [構成されていません] に設定されている場合、サーバ管理者が他の設定をしない限り、リモート デスクトップ サービスはログオフ時に一時フォルダをリモート コンピュータから削除します。</p> <p>注: この設定は、セッションごとの一時フォルダがサーバで使用されている場合のみ有効になります。つまり、[セッションごとの一時フォルダを使用しない] 設定を有効にした場合、この設定は無効になります。</p>
Do not use temporary folders per session	<p>このポリシー設定により、リモート デスクトップ サービスがセッション固有の一時フォルダを作成することを防止できます。</p> <p>このポリシー設定を使用して、各セッション用の別の一時フォルダをリモート コンピュータ上に作成することを無効にできます。デフォルトでは、リモート デスクトップ サービスは、ユーザーがリモート コンピュータに保持する、各アクティブ セッション用の別の一時フォルダを作成します。これらの一時フォルダは、ユーザーのプロファイルフォルダ内一時フォルダにあるリモート コンピュータ上で、sessionid という名前で作成されます。</p> <p>このポリシー設定を有効にすると、セッションごとの一時フォルダは作成されません。その代わりに、リモート コンピュータ上のすべてのセッション用のユーザーの一時ファイルが、リモート コンピュータ上のユーザーのプロファイルフォルダ内の共通の一時フォルダに保存されます。</p> <p>このポリシー設定を無効にすると、リモート デスクトップ セッション ホスト構成ツールで他の設定をしたとしても、セッションごとの一時フォルダが常に作成されます。</p> <p>このポリシー設定を構成しないと、リモート デスクトップ セッション ホスト構成ツールで他の設定をしない限り、セッションごとの一時フォルダが作成されます。</p>

ロケーションベースの印刷の設定

ロケーションベースの印刷機能は、物理的に近いクライアント システムであるプリンタを View デスクトップにマッピングして、ユーザーが View デスクトップからローカル プリンタやネットワーク プリンタに印刷できるようにします。

ロケーションベースの印刷により、IT 組織は、エンドポイントのクライアント デバイスに最も近いプリンタに対して、View デスクトップをマッピングすることができます。たとえば、病院の医師が次々と部屋を移動している場合、その医師がドキュメントを印刷する度に、印刷ジョブはその医師が現在いる部屋に最も近いプリンタに送信されます。

ロケーションベースの印刷機能は、Windows、Mac、Linux、およびモバイル クライアント デバイスで使用できます。

Horizon 6.0.1 以降の場合、ロケーションベースの印刷は次のリモート デスクトップとアプリケーションでサポートされます。

- Windows Desktop や Windows Server マシンなど、単一ユーザーのマシンに展開されたデスクトップ
- 仮想マシンである RDS ホストに展開されたデスクトップ
- ホスト型アプリケーション
- リモート デスクトップ内部の Horizon Client から起動されるホスト型アプリケーション

Horizon 6.0 以前の場合、ロケーションベースの印刷は、単一ユーザーの Windows デスクトップ マシンで展開されているデスクトップでサポートされます。

ロケーション ベースの印刷機能を使用するには、デスクトップに Horizon Agent と一緒に仮想印刷セットアップ オプションをインストールするとともに、正しいプリンタ ドライバをインストールする必要があります。

ロケーションベースの印刷を設定するには、Active Directory グループ ポリシー設定 **AutoConnect Map Additional Printers for VMware View** を設定します。この設定は、Microsoft グループ ポリシー オブジェクト エディタの [コンピュータの構成] の下の [ソフトウェアの設定] フォルダにあります。

注: AutoConnect Map Additional Printers for VMware View はコンピュータ固有のポリシーです。コンピュータ固有のポリシーは、デスクトップに接続するユーザーに関係なく、すべての View デスクトップに適用されます。

AutoConnect Map Additional Printers for VMware View は名前変換表として実装されます。表の各行を使用して、特定のプリンタを識別し、そのプリンタの一連の変換ルールを定義します。変換ルールは、プリンタが特定のクライアント システムの View デスクトップにマッピングされているかどうかを判定します。

ユーザーが View デスクトップに接続すると、View は、クライアント システムを表の各プリンタに関連付けられている変換ルールと比較します。クライアント システムがプリンタに設定されているすべての変換ルールに該当する場合、またはプリンタに変換ルールが関連付けられていない場合、View はユーザーのセッション中にプリンタを View デスクトップにマッピングします。

クライアント システムの IP アドレス、名前、および MAC アドレス、さらにユーザーの名前とグループに基づいて変換ルールを定義できます。特定のプリンタに対し、1 つの変換ルールまたは複数の変換ルールを組み合わせで指定できます。

プリンタを View デスクトップにマッピングするために使われる情報は、View デスクトップの `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\thinprint\tpautoconnect` のレジストリ エントリに保存されます。

ロケーションベースの印刷のプリンタ設定

Horizon 6.0.2 以降では、ユーザーがデスクトップからログアウトまたは切断した後も、ロケーションベースの印刷のプリンタ設定が保持されます。たとえば、白黒モードを使用するようにユーザーがロケーションベースのプリンタを設定したとします。ユーザーがデスクトップからログアウトして再度ログインした後も、ロケーションベースのプリンタでは引き続き白黒モードが使用されます。

ホスト型アプリケーションのセッション間でプリンタの設定を保存するには、ユーザーはアプリケーションの印刷ダイアログ ボックスからロケーションベースのプリンタを選択し、選択したプリンタを右クリックして、[印刷設定] を選択する必要があります。ユーザーがプリンタを選択し、アプリケーションの印刷ダイアログ ボックスで [環境設定] ボタンをクリックした場合、プリンタの設定は保存されません。

設定が、Microsoft が推奨するプリンタ ドライバの DEVMODE の拡張部分ではなく、プリンタ ドライバのプライベート空間に保存される場合、ロケーションベースのプリンタの永続設定はサポートされません。永続設定をサポートするには、プリンタ ドライバの DEVMODE 部分に設定が保存されるプリンタを展開します。

ロケーションベースの印刷グループ ポリシー DLL ファイルの登録

ロケーションベースの印刷のグループ ポリシー設定を構成する前に、DLL ファイル TPVMGPoACmap.dll を登録する必要があります。

32 ビット版と 64 ビット版の TPVMGPoACmap.dll は、VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyyy.zip というバンドル化された .zip ファイルで提供されます。x.x.x はバージョン、yyyyyyyy はビルド番号です。このファイルは、VMware Horizon の 6 ダウンロード サイトからダウンロードできます。

以前の View リリースの場合、32 ビット版と 64 ビット版の TPVMGPoACmap.dll は、View 接続サーバ ホスト上のディレクトリ `install_directory\VMware\VMware View\Server\extras\GroupPolicyFiles\ThinPrint` 内にあります。

手順

- 1 Active Directory サーバまたはグループ ポリシーの構成に使用するドメイン コンピュータに、TPVMGPoACmap.dll の適切なバージョンをコピーします。
- 2 `regsvr32` ユーティリティを使用して TPVMGPoACmap.dll ファイルを登録します。

例 : `regsvr32 "C:\TPVMGPoACmap.dll"`

次のステップ

ロケーションベースの印刷のグループ ポリシーを構成します。

ロケーションベースの印刷グループ ポリシーの構成

ロケーションベースの印刷を設定するには、AutoConnect Map Additional Printers for VMware View グループ ポリシー設定を構成します。このグループ ポリシー設定は、プリンタを View デスクトップにマッピングする名前変換表です。

前提条件

- Active Directory サーバまたはグループ ポリシーの構成に使用するドメイン コンピュータで、Microsoft MMC およびグループ ポリシー オブジェクト エディタ スナップインが使用できることを確認します。
- Active Directory サーバまたはグループ ポリシーの構成に使用するドメイン コンピュータに、DLL ファイル TPVMGPoACmap.dll を登録します。 [ロケーションベースの印刷グループ ポリシー DLL ファイルの登録](#) を参照してください。

- AutoConnect Map Additional Printers for VMware View グループ ポリシー設定の構文について理解しておきます。[ロケーションベースの印刷グループ ポリシー設定の構文](#)を参照してください。
- ロケーションベースのグループ ポリシー設定の GPO を作成し、それを View デスクトップが格納されている OU にリンクします。View グループ ポリシーの GPO の作成方法の例については、[View グループ ポリシーの GPO の作成](#)を参照してください。
- デスクトップに Horizon Agent と共に仮想印刷設定オプションがインストールされていることを確認します。確認するには、デスクトップ オペレーティング システムに TP AutoConnect サービスおよび TP VC Gateway サービスがインストールされているか確認します。
- 印刷ジョブは View デスクトップからプリンタに直接送信されるため、必要なプリンタ ドライバがデスクトップにインストールされていることを確認します。

手順

- 1 Active Directory サーバで GPO を編集します。

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 View デスクトップを格納する OU を右クリックし、[プロパティ] を選択します。 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 右ペインで、ロケーションベースの印刷グループ ポリシー設定用に作成した GPO を右クリックし、[編集] を選択します。
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、ロケーション ベースの印刷のグループ ポリシー設定で作成した GPO を右クリックして、[編集] を選択します。

[グループ ポリシー オブジェクト エディタ] ウィンドウが表示されます。

- 2 [コンピュータの構成] を展開し、[ソフトウェアの設定] フォルダを開き、[VMware View の追加のプリンタを自動接続マッピングする] を選択します。
- 3 ポリシー ペインで、[追加のプリンタの自動接続マッピングを構成する] をダブルクリックします。
[VMware View の追加のプリンタを自動接続マッピングする] ウィンドウが表示されます。
- 4 [有効化] を選択してグループ ポリシー設定を有効にします。
グループ ポリシー ウィンドウに変換表の見出しとボタンが表示されます。

重要: [無効化] をクリックすると、すべての表エントリが削除されます。念のため、後でインポートできるように構成を保存します。

- 5 View デスクトップにマッピングするプリンタを追加し、それらの関連変換ルールを定義します。
- 6 [OK] をクリックして変更を保存します。

ロケーションベースの印刷グループ ポリシー設定の構文

AutoConnect Map Additional Printers for VMware View グループ ポリシー設定を使用して、プリンタをリモート デスクトップにマッピングします。

AutoConnect Map Additional Printers for VMware View は、プリンタを識別し、関連付けられた変換ルールを定義する名前変換表です。表 17-21. 変換表の列と値 では、変換表の構文について説明します。

ロケーションベースの印刷により、ローカル プリンタがリモート デスクトップにマッピングされますが、UNC パスを使用して構成されたネットワーク プリンタのマッピングはサポートされません。

表 17-21. 変換表の列と値

列	説明
IP Range	<p>クライアント システムの IP アドレスの範囲を指定する変換ルール。</p> <p>特定の範囲の IP アドレスを指定するには、次の表記を使用します。</p> <p><i>ip_address–ip_address</i></p> <p>例： 10.112.116.0–10.112.119.255</p> <p>特定のサブネットのすべての IP アドレスを指定するには、次の表記を使用します。</p> <p><i>ip_address/subnet_mask_bits</i></p> <p>例： 10.112.4.0/22</p> <p>この表記は、10.112.4.1 から 10.112.7.254 までの使用可能な IPv4 アドレスを指定しています。</p> <p>任意の IP アドレスに一致させるには、アスタリスクを入力します。</p>
Client Name	<p>コンピュータ名を指定する変換ルール。</p> <p>例： Mary's Computer</p> <p>任意のコンピュータ名に一致させるには、アスタリスクを入力します。</p>
Mac Address	<p>MAC アドレスを指定する変換ルール。GPO エディタでは、クライアント システムで使用されている形式と同じものを使用する必要があります。例：</p> <ul style="list-style-type: none"> ■ Windows クライアントではハイフンを使用します： 01–23–45–67–89–ab ■ Linux クライアントではコロンを使用します： 01:23:45:67:89:ab <p>任意の MAC アドレスに一致させるには、アスタリスクを入力します。</p>
User/Group	<p>ユーザーまたはグループ名を指定する変換ルール。</p> <p>特定のユーザーまたはグループを指定するには、次の表記を使用します。</p> <p><i>\\domain\user_or_group</i></p> <p>例： \\mydomain\Mary</p> <p>完全修飾ドメイン名 (FQDN) は、ドメイン名の表記としてサポートされていません。 任意のユーザー名またはグループ名を指定するには、アスタリスクを入力します。</p>
Printer Name	<p>リモート デスクトップにマッピングするプリンタの名前。</p> <p>例： PRINTER–2–CLR</p> <p>マッピングされる名前は、クライアント システム上のプリンタ名と一致している必要はありません。</p> <p>プリンタはクライアント デバイスのローカル プリンタである必要があります。ネットワーク プリンタの UNC パスへのマッピングはサポートされていません。</p>

列	説明
Printer Driver	<p>プリンタで使用するドライバの名前。</p> <p>例：HP Color LaserJet 4700 PS</p> <p>重要： 印刷ジョブはデスクトップからプリンタに直接送られるため、プリンタ ドライバをデスクトップにインストールする必要があります。</p>
IP Port/ThinPrint Port	<p>ネットワーク プリンタの場合は、先頭に IP_ が付いたプリンタの IP アドレス。</p> <p>例：IP_10.114.24.1</p> <p>デフォルトのポートは 9100 です。ポート番号を IP アドレスに付加することで、デフォルト以外のポートを指定できます。</p> <p>例：IP_10.114.24.1:9104</p>
Default	プリンタがデフォルトのプリンタであるかどうかを示します。

列見出しの上に表示されるボタンを使用して、行を追加、削除、移動し、表エントリを保存およびインポートします。各ボタンには対応するキーボード ショートカットがあります。各ボタンの上にマウスを置くと、ボタンの説明とその対応するキーボード ショートカットが表示されます。たとえば、表の末尾に行を挿入するには、先頭の表ボタンをクリックするか、<Alt> + <A> を押します。表エントリをインポートして保存するには、最後の 2 つのボタンをクリックします。

表 17-22. ロケーションベースの印刷グループ ポリシー設定の例に 2 つの変換表の行の例を示します。

表 17-22. ロケーションベースの印刷グループ ポリシー設定の例

IP Range (IP 範囲)	Client Name (クライアント名)	Mac Address (Mac アドレス)	User/Group (ユーザー/グループ)	Printer Name (プリンタ名)	Printer Driver (プリンタドライバ)	IP Port/ThinPrint Port (IP ポート/ThinPrint ポート)	デフォルト
*	*	*	*	PRINTER-1-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.1	
10.112.116.140-10.112.116.145	*	*	*	PRINTER-2-CLR	HP Color LaserJet 4700 PS	IP_10.114.24.2	X

最初の行に指定されているネットワーク プリンタは、すべての変換ルール列にアスタリスクが表示されているため、すべてのクライアント システムのリモート デスクトップにマッピングされます。2 行目に指定されているネットワーク プリンタは、クライアント システムの IP アドレスが 10.112.116.140 から 10.112.116.145 の範囲である場合のみ、リモート デスクトップにマッピングされます。

Active Directory グループ ポリシーの例

View で Active Directory グループ ポリシーを実装するには、リモート デスクトップ セッションを配信する View マシンの OU を作成して、その OU に 1 つ以上の GPO をリンクします。これらの GPO を使用して、View マシンにグループ ポリシー設定を適用します。

GPO をドメインに直接リンクするには、ポリシー設定をドメイン内のすべてのコンピュータに適用します。ただし、ベスト プラクティスでは、ドメイン内のすべてのコンピュータでポリシー処理を回避するために、ほとんどの展開で GPO を個別の OU にリンクする必要があります。

Active Directory サーバまたはドメイン内の任意のコンピュータでポリシーを構成できます。次の例に、Active Directory サーバで直接ポリシーを構成する方法を示します。

注: View 環境はそれぞれ異なるため、組織固有のニーズに合わせて異なる手順の実行が必要な場合があります。

View マシンの OU の作成

同じ Active Directory ドメインのその他の Windows コンピュータに影響を与えずにリモート デスクトップ セッションを提供する View マシンにグループ ポリシーを適用するには、View マシン専用の OU を作成します。View 展開全体用に 1 つの OU を作成することや、シングルユーザー マシンおよび RDS ホスト用に個別の OU を作成することができます。

手順

- 1 Active Directory サーバで、[起動] - [すべてのプログラム] - [管理ツール] - [Active Directory ユーザーおよびコンピュータ] を選択します。
- 2 View マシンを含むドメインを右クリックし、[新規] - [組織単位] を選択します。
- 3 OU の名前を入力し、[OK] をクリックします。
左ペインに新しい OU が表示されます。
- 4 View マシンを新しい OU に追加するには：
 - a 左ペインの [コンピュータ] をクリックします。
ドメイン内のすべてのコンピュータ オブジェクトが右ペインに表示されます。
 - b 右パネルの View マシンを表すコンピュータ オブジェクトの名前を右クリックし、[移動] を選択します。
 - c OU を選択し、[OK] をクリックします。
OU を選択すると、右ペインに View マシンが表示されます。

次のステップ

View グループ ポリシーの GPO を作成します。

View グループ ポリシーの GPO の作成

View コンポーネントとロケーションベースの印刷のグループ ポリシーを格納する GPO を作成し、それらを View マシンの OU にリンクします。

前提条件

- View マシンの OU を作成します。
- Active Directory サーバでグループ ポリシー管理機能が使用できることを確認します。

手順

- 1 Active Directory サーバで、グループ ポリシー管理コンソールを開きます。

AD バージョン	ナビゲーション パス
Windows 2012	[Server Manager] - [ツール] - [グループ ポリシー管理] を選択します。
Windows 2008	[スタート] - [管理ツール] - [グループ ポリシー管理] を選択します。
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 ユーザーおよびコンピュータ] を選択します。 b View マシンを格納する OU を右クリックし、[プロパティ] を選択します。 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。

- 2 ドメインを展開し、View マシンを格納する OU を右クリックし、[このドメインに GPO を作成して、ここにリンクする] を選択します。

Windows 2003 Active Directory では、このオプションは [ここに GPO を作成してリンクする] という名前です。

- 3 GPO の名前を入力し、[OK] をクリックします。

左ペインの OU の下に新しい GPO が表示されます。

- 4 (オプション) OU の特定の View マシンにのみ GPO を適用するには

- a 左ペインで GPO を選択します。
- b [セキュリティ フィルタ処理] - [追加] を選択します。
- c View マシンのコンピュータ名を入力し、[OK] をクリックします。

[セキュリティ フィルタ処理] ペインに View マシンが表示されます。GPO の設定はこれらのマシンにのみ適用されます。

次のステップ

View ADM テンプレートをグループ ポリシーの GPO に追加します。

GPO への View ADM テンプレートの追加

View コンポーネントのグループ ポリシー設定をリモート デスクトップおよびアプリケーションに適用するには、その ADM テンプレート ファイルを GPO に追加します。

前提条件

- View コンポーネントのグループ ポリシー設定のための GPO を作成し、それらを View マシンが格納されている OU にリンクします。
- Active Directory サーバでグループ ポリシー管理機能が使用できることを確認します。

グループ ポリシー管理コンソールを開く手順は、Windows 2012、Windows 2008、および Windows 2003 Active Directory の各バージョンによって異なります。[View グループ ポリシーの GPO の作成](#)を参照してください。

手順

- 1 View GPO Bundle .zip ファイルを <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 GPO Bundle が含まれます。

ファイル名は VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip で、x.x.x はバージョン、yyyyyyy はビルド番号を表します。View のグループ ポリシー設定用の ADM ファイルと ADMX ファイルはすべて、このファイルで提供されています。

- 2 ファイルを Active Directory サーバにコピーして展開します。
- 3 Active Directory サーバで、グループ ポリシー管理コンソールを開きます。
- 4 ドメインを展開し、グループ ポリシー設定を作成した GPO を右クリックして、[[編集]] を選択します。
- 5 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: ポリシー定義] フォルダを右クリックし、[テンプレートの追加と削除] を選択します。
- 6 [追加] をクリックし、ADM テンプレート ファイルを参照して、[開く] をクリックします。
- 7 [閉じる] をクリックして、ADM テンプレート ファイルのポリシー設定を GPO に適用します。

Windows Server 2012 または 2008 Active Directory では、テンプレート名は、[管理用テンプレート] - [従来の管理用テンプレート (ADM)] の下の左ペインに表示されます。Windows Server 2003 Active Directory では、テンプレートは [管理用テンプレート] の下に表示されます。

- 8 グループ ポリシー設定を構成します。

次のステップ

View マシンのループバック処理を有効にします。

リモート デスクトップのループバック処理の有効化

通常はある特定のコンピュータに適用されるユーザーの構成設定が、そのコンピュータにログインするすべてのユーザーに適用されるようにするには、ループバック処理を有効にします。

前提条件

- View コンポーネントのグループ ポリシー設定のための GPO を作成し、それらを View マシンが格納されている OU にリンクします。
- Active Directory サーバでグループ ポリシー管理機能が使用できることを確認します。

グループ ポリシー管理コンソールを開く手順は、Windows 2012、Windows 2008、および Windows 2003 Active Directory の各バージョンによって異なります。[View グループ ポリシーの GPO の作成](#) を参照してください。

手順

- 1 Active Directory サーバで、グループ ポリシー管理コンソールを開きます。

- 2 ドメインを展開し、グループ ポリシー設定を作成した GPO を右クリックして、[編集] を選択します。
- 3 [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: ポリシー定義] - [システム] - [グループ ポリシー] に移動します。
- 4 右側のペインで、[ユーザー グループ ポリシー ループバックの処理モード] をダブルクリックします。
- 5 [有効化] を選択し、[モード] ドロップダウン メニューからループバック処理モードを選択します。

オプション	アクション
Merge (マージ)	適用されるユーザー ポリシー設定は、コンピュータ GPO とユーザー GPO の両方に含まれるものを組み合わせたものです。競合がある場合は、コンピュータ GPO が優先されます。
Replace (置き換える)	ユーザー ポリシーはコンピュータに関連付けられている GPO からすべて定義されます。ユーザーに関連付けられているすべての GPO が無視されます。

- 6 [OK] をクリックして変更を保存します。

View Persona Management でのユーザー プロファイルの構成

18

View Persona Management では、リモート プロファイル リポジトリと動的に同期するユーザー プロファイルを構成できます。この機能により、ユーザーはデスクトップにログインすればいつでも各自のデスクトップ環境にアクセスできます。View Persona Management により機能が拡張し、Windows 移動プロファイルのパフォーマンスが向上しますが、Windows 移動プロファイルの操作は必要ありません。

View Persona Management を有効にして View Persona Management 展開のさまざまな側面を管理するために、グループ ポリシー設定を構成します。

View Persona Management を有効にして使用するには、適切な VMware Horizon ライセンスが必要です。<http://www.vmware.com/download/eula> の VMware エンド ユーザー ライセンス契約 (EULA) 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 でのユーザーの個人設定の提供
- スタンドアロン システムでの View Persona Management の使用
- View Persona Management によるユーザー プロファイルの移行
- 個人設定管理と Windows 移動プロファイル
- View Persona Management 展開の構成
- View Persona Management 展開を構成するためのベスト プラクティス
- View Persona Management グループ ポリシー設定

View でのユーザーの個人設定の提供

View Persona Management 機能により、ユーザーが View デスクトップにログインするときに、ユーザーのリモート プロファイルが動的にダウンロードされます。安全な中央管理のリポジトリにユーザー プロファイルを保存するよう、View を構成することができます。View により、ユーザーが必要なときに適宜、個人設定情報がダウンロードされます。

View Persona Management は、Windows 移動プロファイルの代替機能です。View Persona Management により機能が拡張し、Windows 移動プロファイルよりもパフォーマンスが向上します。

View 内で個人設定をすべて構成し管理できます。Windows 移動プロファイルを構成する必要はありません。Windows 移動プロファイル構成がある場合、View で既存のリポジトリ構成を使用できます。

ユーザー プロファイルは、View デスクトップから独立しています。ユーザーが任意のデスクトップにログインすると、同じプロファイルが表示されます。

たとえば、ユーザーが流動割り当て、リンク クローン デスクトップ プールにログインし、デスクトップの背景と Microsoft Word の設定を変更するとします。ユーザーが次のセッションを開始すると、仮想マシンは異なりますが、ユーザーには同じ設定が表示されます。

ユーザー プロファイルはユーザーが生成したさまざまな情報から構成されます。

- ユーザー固有のデータおよびデスクトップ設定
- アプリケーション データおよび設定
- ユーザー アプリケーションで構成された Windows レジストリ エントリ

ThinApp アプリケーションでデスクトップをプロビジョニングする場合、ThinApp サンドボックス データをユーザー プロファイルに保存し、ユーザーとともに移動することが可能です。

View Persona Management で、デスクトップへのログイン、ログオフ時間を最小化します。ログイン、ログオフ時間は、Windows 移動プロファイルでは問題になる場合があります。

- ログイン時に、View により、ユーザー レジストリ ファイルのような Windows に必要なファイルのみがダウンロードされます。その他のファイルは、ユーザーやアプリケーションがローカルのプロファイル フォルダからそれらを開くときに、ローカル デスクトップにコピーされます。
- ローカル プロファイルの最近の変更は View によって通常数分に 1 回、リモート リポジトリにコピーされます。デフォルトは 10 分ごとです。ローカル プロファイルのアップロード頻度を指定することができます。
- ログオフ時には、前回のレプリケーション以降に更新されたファイルのみがリモート リポジトリにコピーされます。

スタンドアロン システムでの View Persona Management の使用

スタンドアロン バージョンの View Persona Management を、View によって管理されていない物理コンピュータおよび仮想マシンにインストールすることができます。このソフトウェアを使用すると、View デスクトップおよびスタンドアロン システム全体でユーザー プロファイルを管理することができます。

スタンドアロン View Persona Management ソフトウェアは、Windows 7、Windows 8、Windows 10、Windows Server 2008 R2、および Windows Server 2012 R2 オペレーティング システムで動作します。

スタンドアロン View Persona Management ソフトウェアを使用して、次の目標を達成することができます。

- スタンドアロン システムおよび View デスクトップ全体でユーザー プロファイルを共有します。

ユーザーは、View Persona Management を使用して、引き続きスタンドアロン システムおよび View デスクトップを使用できます。同じ View Persona Management グループ ポリシー設定を使用して View デスクトップおよび物理システムを管理する場合は、ユーザーは、レガシー コンピュータと View デスクトップのどちらを使用しているかに関わらず、ログインするたびに最新のプロファイルを受け取ることができます。

注: View Persona Management は、同時アクティブ セッションをサポートしません。ユーザーは、別のセッションにログインする前に現在のセッションからログアウトする必要があります。

- ユーザー プロファイルを物理システムから View デスクトップへ移行します。

View 展開で使用するためにレガシー物理コンピュータの目的を再設定する場合は、View デスクトップをユーザーに公開する前に、スタンドアロン View Persona Management をレガシー システムにインストールできます。ユーザーがレガシー システムにログインすると、そのプロファイルは View リモート プロファイル リポジトリに格納されます。ユーザーが初めて View デスクトップにログインすると、既存のプロファイルがユーザーの View デスクトップにダウンロードされます。

- 物理システムから View デスクトップへの段階的な移行を実行します。

段階的に展開を移行する場合、View デスクトップにまだアクセスしていないユーザーはスタンドアロン View Persona Management を使用できます。View デスクトップの各セットが展開されると、ユーザーは View デスクトップのプロファイルにアクセスでき、レガシー システムは段階的に廃止されます。このシナリオには、以前のシナリオが組み合わされています。

- ユーザーがオフラインになったときに最新のプロファイルをサポートします。

スタンドアロンのノート PC のユーザーは、ネットワークから切断することができます。ユーザーが再接続すると、View Persona Management はユーザーのローカル プロファイルの最新の変更をリモート プロファイル リポジトリにアップロードします。

注: ユーザーがオフラインになる前に、ユーザー プロファイルがローカル システムに完全にダウンロードされている必要があります。

View Persona Management によるユーザー プロファイルの移行

View Persona Management を使用して、さまざまな設定の既存のユーザー プロファイルを View デスクトップに移行できます。プロファイルの移行が完了した後にユーザーが View デスクトップにログインすると、レガシー システムで使用していた個人設定と個人データが提示されます。

ユーザー プロファイルを移行することにより、次のデスクトップの移行目標を達成することができます。

- Windows 7、Windows 8、Windows Server 2008 R2、または Windows Server 2012 R2 View デスクトップを Windows 10 View デスクトップにアップグレードできます。
- ユーザーのシステムをレガシーの Windows XP から Windows 7、Windows 8、Windows Server 2008 R2、または Windows Server 2012 R2 にアップグレードし、ユーザーを物理コンピュータから View に初めて移行することができます。
- レガシー Windows XP View デスクトップを Windows 7、Windows 8、Windows Server 2008 R2、または Windows Server 2012 R2 View デスクトップにアップグレードできます。
- オペレーティング システムをアップグレードしなくても、物理コンピュータから View デスクトップに移行することができます。

これらのシナリオをサポートするために、View Persona Management には、View Agent 5.x がインストールされていない物理マシンまたは仮想マシン用のプロファイル移行ユーティリティおよびスタンドアロン View Persona Management インストーラが用意されています。

重要: View Agent 6.1 以降のリリースでは、Windows XP および Windows Vista デスクトップはサポートされていません。これらのゲスト OS をサポートしている最後の View リリースは View Agent 6.0.2 です。Windows XP および Vista に関して Microsoft と拡張サポート契約を行っているお客様、およびこれらのゲスト OS システムに関して VMware と拡張サポート契約を行っているお客様は、View 接続サーバ 6.1 を使用して Windows XP および Vista デスクトップの View Agent 6.0.2 バージョンをデプロイできます。

View ユーザー プロファイル移行ユーティリティを使用して、レガシー Windows XP デスクトップ デプロイから、将来の View リリースで継続的にサポートされるデスクトップ デプロイへの移行で重要なタスクを実行できます。

表 18-1. ユーザー プロファイルの移行シナリオ では、さまざまな移行シナリオと、各シナリオで実行するタスクの概要を示しています。

表 18-1. ユーザー プロファイルの移行シナリオ

移行元の展開	移行先の展開	実行するタスク:
Windows 7、Windows 8、Windows Server 2008 R2、または Windows Server 2012 R2 View デスクトップ	Windows 10 View デスクトップ	<ol style="list-style-type: none"> View Persona Management を使用して、ユーザー向けの Windows 10 View デスクトップを構成します。View Persona Management 展開の構成を参照してください。 注: 手順 2 を完了するまで、Windows 10 View デスクトップをユーザーに公開しないでください。 View V2 から V5 へのプロファイル移行ユーティリティを実行します。 <ul style="list-style-type: none"> 移行元プロファイルについては、既存の Windows 7、Windows 8、Windows Server 2008 R2、または Windows Server 2012 R2 View デスクトップのリモート プロファイル リポジトリを指定します。 移行先プロファイルについては、Windows 10 View デスクトップ用に構成したリモート プロファイル リポジトリを指定します。 <p>詳細については、『View ユーザー プロファイル移行ガイド』を参照してください。</p> ユーザーが Windows 10 View デスクトップにログインできるようにします。
Windows XP 物理コンピュータ	Windows 7、Windows 8、Windows Server 2008 R2、または Windows Server 2012 R2 View デスクトップ	<ol style="list-style-type: none"> View Persona Management を使用して、ユーザー向けに Windows 7、Windows 8、Windows Server 2008 R2、または Windows Server 2012 R2 View デスクトップを構成します。View Persona Management 展開の構成を参照してください。 注: 手順 2 を完了するまで、Windows 7、Windows 8、Windows Server 2008 R2、または Windows Server 2012 R2 View デスクトップをユーザーに公開しないでください。 View V1 から V2 へのプロファイル移行ユーティリティを実行します。 <ul style="list-style-type: none"> 移行元プロファイルについては、Windows XP 物理コンピュータのローカル プロファイルを指定します。 移行先プロファイルについては、View 展開用に構成したリモート プロファイル リポジトリを指定します。 <p>詳細については、『View ユーザー プロファイル移行ガイド』を参照してください。</p> ユーザーが Windows 7、Windows 8、Windows Server 2008 R2、または Windows Server 2012 R2 View デスクトップにログインできるようにします。

移行元の展開	移行先の展開	実行するタスク:
<p>移動ユーザー プロファイル ソリューションを使用する Windows XP 物理コンピュータまたは仮想マシン。たとえば、展開で次のいずれかのソリューションを使用している場合があります。</p> <ul style="list-style-type: none"> ■ View Persona Management ■ RTO Virtual Profile ■ Windows 移動プロファイル <p>このシナリオでは、元のユーザー プロファイルはリモート プロファイル リポジトリに保持されている必要があります。</p>	<p>Windows 7、Windows 8、Windows Server 2008 R2、または Windows Server 2012 R2 View デスクトップ</p>	<ol style="list-style-type: none"> 1 View Persona Management を使用して、ユーザー向けに Windows 7、Windows 8、Windows Server 2008 R2、または Windows Server 2012 R2 View デスクトップを構成します。View Persona Management 展開の構成を参照してください。 <p>注: 手順 2 を完了するまで、Windows 7、Windows 8、Windows Server 2008 R2、または Windows Server 2012 R2 View デスクトップをユーザーに公開しないでください。</p> 2 View V1 から V2 へのプロファイル移行ユーティリティを実行します。 <ul style="list-style-type: none"> ■ 移行元プロファイルについては、Windows XP システムのリモート プロファイル リポジトリを指定します。 ■ 移行先プロファイルについては、View 展開用に構成したリモート プロファイル リポジトリを指定します。 <p>詳細については、『View ユーザー プロファイル移行ガイド』を参照してください。</p> 3 ユーザーが Windows 7、Windows 8、Windows Server 2008 R2、または Windows Server 2012 R2 View デスクトップにログインできるようにします。
<p>Windows 7、Windows 8、Windows Server 2008 R2、または Windows Server 2012 R2 物理コンピュータまたは仮想マシン。</p> <p>レガシー システムには、View Agent 5.x をインストールすることはできません。</p>	<p>Windows 7、Windows 8、Windows Server 2008 R2、または Windows Server 2012 R2 View デスクトップ</p>	<ol style="list-style-type: none"> 1 View Persona Management を使用して、ユーザー向けに Windows 7、Windows 8、Windows Server 2008 R2、または Windows Server 2012 R2 View デスクトップを構成します。View Persona Management 展開の構成を参照してください。 2 Windows 7、Windows 8、Windows Server 2008 R2 または Windows Server 2012 R2 システムに、スタンドアロン View Persona Management ソフトウェアをインストールします。スタンドアロン View Persona Management をインストールするを参照してください。 3 View デスクトップと同じリモート プロファイル リポジトリを使用するように、レガシー Windows 7、Windows 8、Windows Server 2008 R2 または Windows Server 2012 R2 システムを構成します。ユーザー プロファイル リポジトリの構成を参照してください。 <p>最も簡単なのは、Active Directory で View Persona Management の同じグループ ポリシー設定を使用して、レガシー システムと View デスクトップの両方を管理する方法です。View Persona Management の ADM または ADMX テンプレート ファイルの追加を参照してください。</p> 4 Windows 7、Windows 8、Windows Server 2008 R2 または Windows Server 2012 R2 View デスクトップをユーザーに公開します。

個人設定管理と Windows 移動プロファイル

個人設定管理 (Persona Management) が有効になっている場合は、Windows 移動プロファイル機能を使用して View ユーザーの個人設定を管理することはできません。

たとえば、デスクトップのゲスト OS システムにログインしたときに、[システムのプロパティ] ダイアログ ボックスの [詳細設定] タブに移動し、ユーザー プロファイル設定を [移動プロファイル] から [ローカル プロファイル] に変更すると、View Persona Management は、ローカル デスクトップとリモートの個人設定リポジトリ間で、ユーザーの個人設定の同期を継続します。

ただし、View Persona Management ではなく、Windows 移動プロファイル機能に管理されているユーザーの個人設定内のファイルとフォルダを指定できます。[Windows 移動プロファイルの同期] ポリシーを使用して、これらのファイルとフォルダを指定します。

View Persona Management 展開の構成

View Persona Management を構成するには、ユーザー プロファイルを格納するリモート リポジトリのセットアップ、Horizon Agent のインストール (リモート デスクトップ セッションを提供する仮想マシンで [View Persona Management] セットアップ オプションを指定)、View Persona Management グループ ポリシー設定の追加および構成、デスクトップ プールの展開を行います。

また、非 View 展開に View Persona Management を構成することもできます。スタンドアロンバージョンの View Persona Management を、ユーザーの非 View ラップトップ、デスクトップ、または仮想マシンにインストールします。またリモート リポジトリを設定して、View Persona Management グループ ポリシー設定を構成する必要があります。

View Persona Management 展開の設定の概要

View Persona Management を使用して View デスクトップ展開またはスタンドアロン コンピュータを設定するには、上位レベルの複数のタスクを実行する必要があります。

ここに示す順序でタスクを実行することが推奨されていますが、別の順序で実行することも可能です。たとえば、デスクトップ プールを展開してから、Active Directory でグループ ポリシー設定を構成または再構成することができます。

- 1 ユーザー プロファイルを格納するリモート リポジトリを構成します。

ネットワーク共有を構成することも、Windows 移動プロファイル用に構成した既存の Active Directory ユーザー プロファイル パスを使用することもできます。

- 2 デスクトップ プールの作成に使用する仮想マシンで、[View Persona Management] セットアップ オプションを指定して Horizon Agent をインストールします。

View 以外のラップトップ、デスクトップまたは仮想マシンに対して View Persona Management を構成するには、スタンドアロン View Persona Management ソフトウェアを対象となる展開の各コンピュータにインストールします。

- 3 Active Directory サーバ、または親仮想マシンのローカル コンピュータ ポリシー構成に、View Persona Management ADM テンプレート ファイルまたは View Persona Management ADMX テンプレート ファイルを追加します。

View のデプロイ環境全体または View 以外のデプロイ環境に対して View Persona Management を構成するには、ADM テンプレート ファイルまたは ADMX テンプレート ファイルを Active Directory に追加します。

1 台のデスクトップ プールに対して View Persona Management を構成するには、次の操作を行います。

- プールの作成に使用する仮想マシンに、ADM テンプレート ファイルまたは ADMX テンプレート ファイルを追加します。
 - ADM テンプレート ファイルまたは ADMX テンプレート ファイルを Active Directory に追加し、プール内のマシンを含む OU にグループ ポリシー設定を適用します。
- 4 [ユーザーの個人設定を管理] グループ ポリシー設定を有効にすることで、View Persona Management を有効にします。
 - 5 リモート プロファイル リポジトリ用のネットワーク共有を構成した場合は、[個人設定リポジトリの場所] グループ ポリシー設定を有効にし、ネットワーク共有のパスを指定します。
 - 6 (オプション) Active Directory やローカル コンピュータ ポリシー構成で、その他のグループ ポリシー設定を構成します。
 - 7 [View Persona Management] セットアップ オプションを指定して Horizon Agent をインストールした仮想マシンからデスクトップ プールを作成します。

ユーザー プロファイル リポジトリ の構成

ユーザー プロファイル内のユーザー データと設定、アプリケーション固有のデータ、およびその他のユーザー生成情報を格納するリモート リポジトリを構成できます。Windows 移動プロファイルが展開内に構成されている場合は、既存の Active Directory ユーザー プロファイルのパスを代わりに使用できます。

注: Windows 移動プロファイルを構成しなくても、View Persona Management を構成できます。

前提条件

- 共有フォルダを構成するために必要な最小限のアクセス権限について理解しておきます。[View Persona Management の共有フォルダのアクセス権の設定](#)を参照してください。
- ユーザー プロファイル リポジトリの作成におけるガイドラインについて理解しておきます。View グループ ポリシーの GPO を作成する方法の例については、[View Persona Management のネットワーク共有の作成](#)

手順

- 1 既存の Active Directory ユーザー プロファイルのパスを使用するか、ネットワーク共有にユーザー プロファイル リポジトリを構成するかを決定します。

オプション	操作
既存の Active Directory ユーザー プロファイルのパスを使用する	既存の Windows 移動プロファイル構成がある場合は、移動プロファイルをサポートする Active Directory 内のユーザー プロファイルのパスを使用できます。この手順の残りのステップはスキップできます。
ユーザー プロファイル リポジトリを格納するネットワーク共有を構成する	既存の Windows 移動プロファイル構成がない場合は、ユーザー プロファイル リポジトリ用のネットワーク共有を構成する必要があります。この手順の残りのステップに従います。

- 2 ユーザーがデスクトップ上のゲスト OS からアクセス可能なコンピュータに共有フォルダを作成します。

構成するフォルダ パスに %username% が含まれていない場合は、View Persona Management により %username%.%userdomain% がパスに追加されます。

例: \\server.domain.com\VPRepository\%username%.%userdomain%

- 3 ユーザー プロファイルを格納する共有フォルダのアクセス権限を設定します。

注意: アクセス権限が正しく構成されていることを確認します。共有フォルダのアクセス権限の不正な構成は、View Persona Management に関連する問題の最多要因です。

View Persona Management の共有フォルダのアクセス権の設定

View Persona Management および Windows 移動プロファイルには、ユーザー プロファイル リポジトリに対する特定の最小限の権限が必要です。さらに View Persona Management では、データを共有フォルダに入れるユーザーの Security group に、共有フォルダに対する読み取り属性が必要です。

ユーザー プロファイル リポジトリおよびリダイレクトされるフォルダ共有に対し必要なアクセス権限を設定します。

表 18-2. ユーザー プロファイル リポジトリおよびリダイレクトされるフォルダ共有に対し必要な最小限の NTFS 権限

ユーザー アカウント	必要な最小限の権限
作成オーナー	フル コントロール、サブフォルダおよびファイルのみ
管理者	なし。代わりに、Windows グループ ポリシー設定 [Administrators Security group を移動ユーザー プロファイルに追加] を有効にします。グループ ポリシー オブジェクト エディタで、このポリシー設定は [Computer Configuration\Administrative Templates\System\User Profiles\] にあります。
データを共有にするのに必要なユーザーの security group	List Folder/Read Data、Create Folders/Append Data、Read Attributes - このフォルダのみ
全員	権限なし
ローカル システム	フル コントロール、このフォルダ、サブフォルダおよびファイル

表 18-3. ユーザー プロファイル リポジトリおよびリダイレクトされるフォルダ共有に対し必要な共有レベル (SMB) 権限

ユーザー アカウント	デフォルトの権限	必要な最小限の権限
全員	読み取り専用	権限なし
データを共有にするのに必要なユーザーの security group	該当なし	フル コントロール

移動ユーザー プロファイル セキュリティの詳細については、Microsoft TechNet のトピック「Security Recommendations for Roaming User Profiles Shared Folders (移動ユーザー プロファイル共有フォルダのセキュリティ推奨事項)」を参照してください。 [http://technet.microsoft.com/en-us/library/cc757013\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc757013(WS.10).aspx)

View Persona Management のネットワーク共有の作成

プロファイル リポジトリとして使用するために共有フォルダを作成する場合には、特定のガイドラインに従う必要があります。

- Windows 8 デスクトップを使用していて、ネットワーク共有で EMC Isilon NAS デバイス上の OneFS ファイル システムを使用している場合、OneFS ファイル システムはバージョン 6.5.5.11 以降である必要があります。
- 共有フォルダは、サーバ上、ネットワーク接続型ストレージ (NAS) デバイス上、またはネットワーク サーバ上で作成できます。
- 共有フォルダは、View 接続サーバと同じドメインにある必要はありません。
- 共有フォルダは、共有フォルダにプロファイルを保存するユーザーと同じ Active Directory フォレストに存在させる必要があります。
- ユーザーのユーザー プロファイル情報を保存するのに十分な大きさの共有ドライブを使用する必要があります。大規模な View 展開をサポートするために、さまざまなデスクトップ プールに個別のリポジトリを構成できます。

複数のプールに対する資格が付与されているユーザーの場合、ユーザーを共有するプールは同じプロファイル リポジトリで構成されなければなりません。プロファイル リポジトリがそれぞれ異なる 2 つのプールに対する資格をユーザーに付与すると、そのユーザーは各プール内のデスクトップから同一バージョンのプロファイルにアクセスできなくなります。

- ユーザー プロファイル フォルダが作成される場所のフル プロファイル パスを作成する必要があります。パスの一部が存在しない場合は、ユーザーが最初にログインするときに Windows によって不明フォルダが作成され、ユーザーのセキュリティ上の制約がそれらのフォルダに割り当てられます。Windows は、そのパスの下に作成するすべてのフォルダに対して、同じセキュリティ上の制約を割り当てます。

たとえば、`user1` に対して、View Persona Management のパスとして `\\server\VPRepository\profiles\user1` と構成するとします。ネットワーク共有として `\\server\VPRepository` を作成した場合、`profiles` フォルダが存在しないと、`user1` がログインするときに Windows によって `\\profiles\user1` というパスが作成されます。また、`\\profiles\user1` フォルダへのアクセスが `user1` アカウントに制限されます。別のユーザーがログインし、そのプロファイル パスが `\\server\VPRepository\profiles` の場合、この 2 番目のユーザーはリポジトリにアクセスできず、ユーザーのプロファイルのレプリケーションも失敗します。

View Persona Management オプションを指定して Horizon Agent をインストール

View デスクトップで View Persona Management を使用するには、デスクトップ プールの作成に使用する仮想マシンにおいて、[View Persona Management] セットアップ オプションを指定して Horizon Agent をインストールする必要があります。

自動プールを使用する場合は、親またはテンプレートとして使用する仮想マシンにおいて、[View Persona Management] セットアップ オプションを指定して Horizon Agent をインストールします。デスクトップ プールを仮想マシンから作成すると、View Persona Management ソフトウェアが View デスクトップで展開されます。

手動プールを使用する場合は、プールでデスクトップとして使用されている各仮想マシンにおいて、[View Persona Management] セットアップ オプションを指定して Horizon Agent をインストールする必要があります。Active Directory を使用して、手動プールの View Persona Management グループ ポリシーを構成します。または、ADM テンプレート ファイルまたは ADMX テンプレート ファイルを追加し、各マシンで個別にグループ ポリシーを構成します。

前提条件

- Windows 7、Windows 8、Windows 10、Windows Server 2008 R2、または Windows Server 2012 R2 仮想マシンでインストールを実行していることを確認してください。View Persona Management は Microsoft RDS ホストでは動作しません。

[View Persona Management] セットアップ オプションを指定して Horizon Agent をインストールすると、物理コンピュータでは動作しません。物理コンピュータには、スタンドアロン View Persona Management ソフトウェアをインストールできます。[スタンドアロン View Persona Management をインストールする](#) を参照してください。

- 仮想マシンに管理者としてログインできることを確認します。
- ネイティブ RTO Virtual Profiles 2.0 が仮想マシンにインストールされていないことを確認します。ネイティブ RTO Virtual Profile 2.0 がインストールされている場合は、それをアンインストールしてから、[View Persona Management] セットアップ オプションを指定して Horizon Agent をインストールします。
- Horizon Agent のインストールについて理解しておきます。[仮想マシンへの Horizon Agent のインストール](#) または [非管理対象マシンでの Horizon Agent のインストール](#) を参照してください。

手順

- ◆ 仮想マシンに Horizon Agent をインストールするときに、[View Persona Management] セットアップ オプションを選択します。

次のステップ

Active Directory サーバ、または仮想マシン自体のローカル コンピュータ ポリシー構成に、View Persona Management ADM テンプレート ファイルまたは View Persona Management ADMX テンプレート ファイルを追加します。[View Persona Management の ADM または ADMX テンプレート ファイルの追加](#) を参照してください。

スタンドアロン View Persona Management をインストールする

View Persona Management を View 以外の物理コンピュータまたは仮想マシンで使用するには、View Persona Management のスタンドアロン バージョンをインストールします。コマンドラインでインタラクティブなインストールまたはサイレント インストールを実行できます。

スタンドアロン View Persona Management ソフトウェアを対象となる展開の各コンピュータまたは仮想マシンにインストールします。

前提条件

- Windows 7、Windows 8、Windows 10、Windows Server 2008 R2、または Windows Server 2012 R2 物理コンピュータまたは仮想マシンでインストールを実行していることを確認してください。View Persona Management は Windows Server や Microsoft RDS ホストでは動作しません。システムが『View のインストール』ドキュメントの「スタンドアロン View Persona Management でサポートされるオペレーティング システム」に記載されている要件を満たしていることを確認します。
- システムに管理者としてログインできることを確認します。
- View Agent 5.x以降がコンピュータにインストールされていないことを確認します。
- ネイティブ RTO Virtual Profiles 2.0 が仮想マシンにインストールされていないことを確認します。
- サイレント インストールを実行する場合は、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。

手順

- 1 スタンドアロン View Persona Management インストーラ ファイルを VMware 製品ページ (<http://www.vmware.com/products/>) からダウンロードします。

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

- 2 インタラクティブなインストール プログラムを実行するか、サイレント インストールを実行します。

オプション	説明
インタラクティブなインストール	<p>a 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。</p> <p>b VMware のライセンス条件に同意します。</p> <p>c [インストール] をクリックします。</p> <p>デフォルトでは、View Persona Management は C:\Program Files\VMware\VMware View Persona Management ディレクトリにインストールされます。</p> <p>d [終了] をクリックします。</p>
サイレント インストール	<p>マシンで Windows のコマンド プロンプトを開き、インストール コマンドを 1 行で入力します。</p> <p>たとえば、VMware-personamanagement-y.y.y-xxxxxx.exe /s /v"/qn /l*v ""c:\persona.log"" ALLUSERS=1" のようにします。</p> <p>重要: コマンド ラインには ALLUSERS=1 プロパティを含める必要があります。</p>

- 3 システムを再起動してインストールの変更を有効にします。

次のステップ

View Persona Management ADM テンプレート ファイルを Active Directory またはローカル グループ ポリシー 構成に追加します。

View Persona Management の ADM または ADMX テンプレート ファイルの追加

View Persona Management ADM テンプレート ファイルと View Persona Management ADMX テンプレート ファイルには、View Persona Management を構成できるグループ ポリシー設定が含まれます。ポリシーを構成する際には、ADM テンプレート ファイルまたは ADMX テンプレート ファイルをローカル システムまたは Active Directory サーバに追加する必要があります。

単一システムで View Persona Management を構成する場合は、そのローカル システムのローカル コンピュータ ポリシー構成にグループ ポリシー設定を追加できます。

デスクトップ プールの View Persona Management を構成する場合は、デスクトップ プールのデプロイにおける親またはテンプレートとして使用する仮想マシンのローカル コンピュータ ポリシー構成に、グループ ポリシー設定を追加できます。

ドメイン全体のレベルで View Persona Management を構成し、その構成を多くの View マシンまたはデプロイ環境全体に適用する場合は、Active Directory サーバのグループ ポリシー オブジェクト (GPO) にグループ ポリシー設定を追加できます。Active Directory では、View Persona Management を使用する View マシンの OU の作成、1 つ以上の GPO の作成、さらに OU への GPO のリンクを行えます。さまざまなタイプのユーザー向けに個別の View Persona Management ポリシーを構成するために、View マシンの特定セットの OU を作成し、さまざまな GPO を OU に適用できます。

たとえば、View Persona Management を使用する View マシンに OU を 1 つ作成し、スタンドアロンの View Persona Management ソフトウェアがインストールされている物理コンピュータに別の OU を作成できます。

Active Directory のグループ ポリシーの View への実装例については、[Active Directory グループ ポリシーの例](#)を参照してください。

個人設定管理 ADM テンプレートをシングル システムに追加する

シングル デスクトップ プール向けの View Persona Management を構成するには、プールを作成するために使用する仮想マシン上のローカル コンピュータ ポリシーに個人設定管理 ADM テンプレート ファイルを追加する必要があります。シングル システムで View Persona Management を構成するには、そのシステムに個人設定管理 ADM テンプレート ファイルを追加する必要があります。

前提条件

- View Persona Management セットアップ オプションを指定して Horizon Agent がシステムにインストールされていることを確認します。[View Persona Management オプションを指定して Horizon Agent をインストール](#)を参照してください。
- システムに管理者としてログインできることを確認します。

手順

- 1 View GPO Bundle .zip ファイルを <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 GPO Bundle が含まれます。

ファイル名は VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip で、x.x.x はバージョン、yyyyyyy はビルド番号を表します。View のグループ ポリシー設定用の ADM ファイルと ADMX ファイルはすべて、このファイルで提供されています。

- 2 zip ファイルを展開して、ADM ファイル ViewPM.adm をローカル システムにコピーします。
- 3 ローカル システムで [スタート] - [ファイル名を指定して実行] をクリックします。
- 4 「gpedit.msc」と入力し、[OK] をクリックします。
- 5 [ローカル コンピュータ ポリシー] ウィンドウで [コンピュータの構成] に移動し、[管理用テンプレート] を右クリックします。

注: [ユーザーの構成] の下の [管理用テンプレート] は選択しないようにしてください。

- 6 [テンプレートの追加と削除] をクリックし、[追加] をクリックします。
- 7 ViewPM.adm ファイルが含まれるディレクトリを参照します。
- 8 ViewPM.adm を選択し、[追加] をクリックします。
- 9 [テンプレートの追加と削除] ウィンドウを閉じます。

View Persona Management グループ ポリシー設定が、ローカル システムのローカル コンピュータ ポリシー構成に追加されます。この構成を表示するには、gpedit.msc を使用する必要があります。

次のステップ

ローカル システムで View Persona Management グループ ポリシー設定を構成します。[View Persona Management ポリシーを構成](#)を参照してください。

個人設定管理 ADM テンプレートの Active Directory への追加

展開用に View Persona Management を構成するために、個人設定管理 ADM テンプレート ファイルを Active Directory サーバのグループ ポリシー オブジェクト (GPO) に追加できます。

前提条件

- View 個人設定管理の展開用の GPO を作成して、View 個人設定管理を使用する View マシンを含む OU にリンクします。[Active Directory グループ ポリシーの例](#)を参照してください。
- Active Directory サーバで、Microsoft MMC およびグループ ポリシー オブジェクト エディタ スナップインが使用できることを確認します。
- Active Directory サーバにアクセス可能なシステムに、View Persona Management 設定オプションを使用して Horizon Agent がインストールされていることを確認します。[View Persona Management オプションを指定して Horizon Agent をインストール](#)を参照してください。

手順

- 1 View GPO Bundle .zip ファイルを <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 GPO Bundle が含まれます。

ファイル名は `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` で、`x.x.x` はバージョン、`yyyyyyy` はビルド番号を表します。View のグループ ポリシー設定用の ADM ファイルと ADMX ファイルはすべて、このファイルで提供されています。

- 2 zip ファイルを展開して、View 個人設定管理 ADM テンプレート ファイルの `ViewPM.adm` を Active Directory サーバにコピーします。
- 3 Active Directory サーバで、グループ ポリシー管理コンソールを開きます。
たとえば [ファイル名を指定して実行] ダイアログ ボックスで、`gpmmc.msc` と入力して [OK] をクリックします。
- 4 左側のペインで、View マシンが含まれるドメインまたは OU を選択します。
- 5 右ペインで、グループ ポリシー設定に作成した GPO を右クリックし、[編集] を選択します。
[グループ ポリシー オブジェクト エディタ] ウィンドウが表示されます。
- 6 グループ ポリシー オブジェクト エディタで、[コンピュータの構成] の下の [管理用テンプレート] を右クリックして、[テンプレートの追加と削除] を選択します。
- 7 [追加] をクリックして `ViewPM.adm` ファイルを参照し、[開く] をクリックします。
- 8 [閉じる] をクリックして、ADM テンプレート ファイルのポリシー設定を GPO に適用します。

左ペインの [管理用テンプレート] の下にテンプレート名が表示されます。

次のステップ

Active Directory サーバで View Persona Management グループ ポリシー設定を構成します。

Active Directory または単一システムへの Persona Management ADMX テンプレート ファイルの追加

Persona Management の ADMX テンプレート ファイルを Active Directory または単一システムに追加できます。

前提条件

- View Persona Management セットアップ オプションを指定して Horizon Agent がインストールされていることを確認します。[View Persona Management オプションを指定して Horizon Agent をインストールを参照してください。](#)
- `gpedit.msc` または適切なグループ ポリシー エディタが利用可能であることを確認します。

手順

- 1 View GPO Bundle .zip ファイルを <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 GPO Bundle が含まれます。

ファイル名は `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` で、`x.x.x` はバージョン、`yyyyyy` はビルド番号を表します。View のグループ ポリシー設定用の ADM ファイルと ADMX ファイルはすべて、このファイルで提供されています。

- 2 `VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip` ファイルを展開して、View Persona Management ADMX ファイルを Active Directory サーバまたは個々の Persona ホスト (単一システム) にコピーします。

a `ViewPM.admx` ファイルを `C:\Windows\PolicyDefinitions\` ディレクトリにコピーします。

b 言語リソース ファイル `ViewPM.adml` を Active Directory サーバまたは個々の Persona ホストの `C:\Windows\PolicyDefinitions\` の適切なサブフォルダにコピーします。

たとえば、英語環境であれば、`ViewPM.adml` ファイルを `C:\Windows\PolicyDefinitions\en-US\` ディレクトリにコピーします。

- 3 お使いの Active Directory ホストで、グループ ポリシー管理エディタまたは個々の Persona ホストを開いて、`gpedit.msc` ユーティリティでローカル グループ ポリシー エディタを開きます。

[コンピュータの構成] > [ポリシー] > [管理用テンプレート] > [個人設定管理] に View Persona Management グループ ポリシー設定がインストールされます。

次のステップ

(オプション) View Persona Management グループ ポリシー設定を構成します。[View Persona Management ポリシーを構成](#)を参照してください。

View Persona Management ポリシーを構成

View Persona Management を使用するには、[ユーザーの個人設定を管理] グループ ポリシー設定を有効にする必要があります。これにより、View Persona Management ソフトウェアがアクティベーションされます。Active Directory ユーザー プロファイルのパスを使用せずに、ユーザー プロファイル リポジトリをセットアップするには、[個人設定リポジトリの場所] グループ ポリシー設定を構成する必要があります。

オプションのグループ ポリシー設定では、View Persona Management 展開のその他の設定について構成できません。

Windows 移動プロファイルが展開内にすでに構成されている場合は、既存の Active Directory ユーザー プロファイルのパスを使用できます。[個人設定リポジトリの場所] の設定は、無効または未構成のままにしておくことが可能です。

前提条件

- [ユーザーの個人設定を管理] および [個人設定リポジトリの場所] グループ ポリシーの設定について理解しておきます。 [移動と同期に関するグループ ポリシー設定](#)を参照してください。
- ローカル システムでグループ ポリシーを設定する場合は、[グループ ポリシー] ウィンドウを開く方法について理解しておきます。 [個人設定管理 ADM テンプレートをシングル システムに追加する手順](#) [手順 3](#) および [手順 4](#)を参照してください。
- Active Directory サーバでグループ ポリシーを設定する場合は、グループ ポリシー オブジェクト エディタの開始方法について理解しておきます。 [個人設定管理 ADM テンプレートの Active Directory への追加](#) の手順 [手順 3](#) から [手順 5](#)を参照してください。

手順

- 1 [グループ ポリシー] ウィンドウを開きます。

オプション	説明
ローカル システム	[ローカル コンピュータ ポリシー] ウィンドウを開きます。
Active Directory サーバ	[グループ ポリシー オブジェクト エディタ] ウィンドウを開きます。

- 2 [コンピュータ構成] フォルダを展開し、[個人設定管理] フォルダに移動します。

オプション	説明
Windows 7 以降、または Windows Server 2008 以降	次のフォルダを展開します:[管理テンプレート]、[従来の管理テンプレート (ADM)]、[VMware View Agent の構成]、[個人設定管理]
Windows Server 2003	次のフォルダを展開します:[管理テンプレート]、[VMware View Agent の構成]、[個人設定管理]

- 3 [移動と同期] フォルダを開きます。
- 4 [ユーザーの個人設定を管理] をダブルクリックして、[有効化] をクリックします。
この設定にすると、View Persona Management がアクティベーションされます。この設定が無効または未構成の場合、View Persona Management は機能しません。
- 5 プロファイルのアップロード間隔を分単位で入力し、[OK] をクリックします。
プロファイルのアップロード間隔は、View Persona Management がユーザー プロファイルの変更をリモート リポジトリにコピーする頻度を決定するものです。デフォルトのアップロード間隔は 10 分です。
- 6 [個人設定リポジトリの場所] をダブルクリックして、[有効化] をクリックします。
すでに Windows 移動プロファイル展開がある場合は、リモート プロファイル リポジトリに対して Active Directory ユーザー プロファイルのパスを使用できます。[個人設定リポジトリの場所] を構成する必要はありません。
- 7 ユーザー プロファイルを格納するネットワーク ファイル サーバ共有までの UNC パスを入力します。
例: \\server.domain.com\UserProfilesRepository\%username%
ネットワーク共有は、展開内の仮想マシンまでアクセス可能でなければなりません。

Active Directory ユーザー プロファイルのパスを使用する場合、UNC パスを指定する必要はありません。

- 8 Active Directory ユーザー プロファイルのパスが展開内で構成されている場合は、このパスを使用するか、上書きするかを指定します。

オプション	アクション
ネットワーク共有を使用	[Active Directory ユーザー プロファイルのパスが構成されている場合はこれを上書きする] チェックボックスをオンにします。
存在する場合は Active Directory ユーザー プロファイルのパスを使用する	[Active Directory ユーザー プロファイルのパスが構成されている場合はこれを上書きする] チェックボックスをオフにします。

- 9 [OK] をクリックします。

- 10 (オプション) その他の View Persona Management グループ ポリシー設定を構成します。

個人設定管理を使用するデスクトップ プールの作成

View デスクトップで View Persona Management を使用するには、各マシンにインストールされている View Persona Management エージェントを使用してデスクトップ プールを作成する必要があります。

View Persona Management を、リモート デスクトップ サービス (RDS) ホストで実行している RDS デスクトップ プールで使用することはできません。

前提条件

- デスクトップ プールの作成に使用する仮想マシンに、[View Persona Management] セットアップ オプションを指定して Horizon Agent がインストールされていることを確認します。[View Persona Management オプションを指定して Horizon Agent をインストール](#)を参照してください。
- View Persona Management ポリシーをこのデスクトップ プールのみに構成する場合は、View Persona Management の ADM テンプレート ファイルを仮想マシンに追加し、ローカル コンピュータ ポリシー構成でグループ ポリシー設定を構成したことを確認します。[個人設定管理 ADM テンプレートをシングル システムに追加する](#)および [View Persona Management ポリシーを構成](#)を参照してください。

手順

- ◆ 仮想マシンからスナップショットまたはテンプレートを生成し、自動デスクトップ プールを作成します。
フル仮想マシンまたはリンク クローンを格納するプールで View Persona Management を設定できます。プールでは、専用割り当てと流動割り当てを使用できます。
- ◆ (オプション) 手動デスクトップ プールで View Persona Management を使用するには、[View Persona Management] オプションで Horizon Agent がインストールされているマシンを選択します。

注: View Persona Management を View デスクトップ プールにデプロイした後に、View マシン上の [View Persona Management] セットアップ オプションを削除したり、Horizon Agent 全体をアンインストールすると、現在ログインしていないユーザーのマシンからローカル ユーザー プロファイルが削除されます。現在ログインしているユーザーについては、アンインストール処理中にリモート プロファイル リポジトリからユーザー プロファイルがダウンロードされます。

View Persona Management 展開を構成するためのベスト プラクティス

ユーザーのデスクトップ使用環境を強化し、デスクトップのパフォーマンスを向上させ、他の View 機能とともに View Persona Management が効率よく動作するようにするには、View Persona Management を構成するためのベスト プラクティスに従ってください。

ローカル ユーザー プロファイルをログオフ時に削除するかどうかを指定

View Persona Management のデフォルトでは、ユーザーがログオフするときにローカル マシンからユーザー プロファイルは削除されません。[ログオフ時にローカルの個人設定を削除] ポリシーが無効になっています。多くの場合、デフォルト設定は、I/O 処理数を削減し、冗長な動作を回避するものであるため、ベスト プラクティスと言えます。

たとえば、流動割り当てプールを展開し、ログオフ時にマシンを更新または削除する場合、このポリシーは無効のままにします。ローカル プロファイルが削除されるのは、仮想マシンが更新または削除されるときです。流動割り当ての自動プールでは、ログオフ後にフル仮想マシンを削除できます。流動割り当てのリンク クローン プールでは、ログオフ時にクローンを更新または削除できます。

専用割り当てプールを展開する場合、ユーザーはセッションごとに同じマシンに戻るため、ポリシーを無効のままにしておくことができます。ポリシーが無効になっていると、ユーザーのログイン時に View Persona Management はローカル プロファイルで示されているファイルをダウンロードする必要がありません。専用割り当てのリンク クローン プールを通常ディスクで構成する場合は、通常ディスクからユーザー データが削除されないように、ポリシーを無効のままにします。

場合によっては、[ログオフ時にローカルの個人設定を削除] ポリシーを有効にすることがあります。

View Persona Management および Windows 移動プロファイルを含む展開への対応

Windows 移動プロファイルが構成されていて、ユーザーが、View デスクトップへのアクセスに View Persona Management を、標準デスクトップへのアクセスに Windows 移動プロファイルを使用している展開において、ベスト プラクティスは、2 つのデスクトップ環境に対して異なるプロファイルを使用することです。View デスクトップと、デスクトップが起動するクライアント コンピュータが同じドメイン内にあり、かつ Active Directory GPO を使用して Windows 移動プロファイルと View Persona Management の両方を構成する場合は、[個人設定リポジトリの場所] ポリシーを有効にして、[Active Directory ユーザー プロファイルのパスが構成されている場合はこれをオーバーライドする] を選択します。

この対応により、ユーザーがクライアント コンピュータからログオフするときに、Windows 移動プロファイルで View Persona Management プロファイルが上書きされなくなります。

既存の Windows 移動プロファイルと View Persona Management プロファイルの間でデータを共有しようとする場合は、Windows フォルダのリダイレクトを構成できます。

リダイレクト対象フォルダのパスの構成

[フォルダ リダイレクト] グループ ポリシー設定を使用する場合、フォルダ パスに %username% を含むように構成しますが、パスの最後のサブフォルダには My Videos などのリダイレクト対象フォルダ名を使用するようにします。ユーザーのデスクトップ上ではフォルダ名としてパスの最後のフォルダが表示されます。

たとえば、\\myserver\videos\%username%\My Videos というパスを構成すると、ユーザーのデスクトップに表示されるフォルダ名は My Videos になります。

パス内の最後のサブフォルダが %username% である場合、フォルダ名としてユーザの名前が表示されます。たとえば、デスクトップ上に My Videos が表示されず、ユーザー JDoe には JDoe という名前のフォルダが表示され、フォルダを簡単に識別できません。

View Persona Management 展開を監視するための Windows イベント ログの使用

展開の管理を支援するために、View Persona Management には改良されたログ メッセージ、プロファイル サイズ およびファイル、そしてフォルダ カウント トラッキングが用意されています。View Persona Management は、Windows イベント ログのリダイレクト用フォルダを提案するためにファイルおよびフォルダ カウントを使用し、これらのフォルダに統計を提供します。たとえば、ユーザーがログインすると、Windows イベント ログにフォルダをリダイレクトする次の推奨事項が表示される場合があります。

```
Profile path: \\server.domain.com\persona\user1V2
...
Folders to redirect:
\\server.domain.com\persona\user1V2 Reason: Folder size larger than 1GB
\\server.domain.com\persona\user1V2\Documents Reason: More than 10000 files and folders
```

その他のベスト プラクティス

次の推奨事項にも従うことができます。

- 多くのウイルス対策製品はデフォルトでオフライン ファイルをスキャンしません。たとえば、ユーザーがデスクトップにログインしたときに、これらウイルス対策製品では、[事前ロードするファイルとフォルダ] または [Windows 移動プロファイルの同期] グループ ポリシー設定で指定されていないユーザー プロファイルに対してのスキャンは行われません。多くの展開において、デフォルトの動作は、オンデマンドでのスキャン時にファイルをダウンロードするのに必要な I/O 処理数を削除するため、ベスト プラクティスと言えます。

リモート リポジトリからファイルを取得し、オフライン ファイルのスキャンを有効にする必要がある場合は、お使いのウイルス対策製品のマニュアルを参照してください。

- 標準的な方法で、View Persona Management がプロファイル リポジトリを保存するネットワーク シェアをバックアップすることを強くお勧めします。

注: View デスクトップにあるユーザー プロファイルをバックアップするときに、View Persona Management で、MozyPro や Windows のボリューム バックアップ サービスなどのバックアップ ソフトウェアを使用しないでください。

View Persona Management では、リモートのプロファイル リポジトリにユーザー プロファイルが確実にバックアップされるため、デスクトップのユーザー データをバックアップするために別のツールを追加する必要はありません。場合によっては、MozyPro や Windows のボリューム バックアップ サービスなどのツールが View Persona Management の正常な処理を妨げ、データが損失したり破壊されたりする可能性があります。

- View Persona Management ポリシーを設定して、ユーザーが ThinApp アプリケーションを起動したときのパフォーマンスを向上させることができます。 [ThinApp サンドボックス フォルダを含むようにユーザー プロファイルを構成](#)を参照してください。
- ユーザーが大量の個人設定データを生成するときに、更新や再構成を使用して専用割り当てのリンク クローン デスクトップを管理する場合は、個別の View Composer 通常ディスクを使用するようデスクトップ プールを構成します。通常ディスクは、View Persona Management のパフォーマンスを向上させることができます。 [View Persona Management での View Composer 通常ディスクの構成](#)を参照してください。
- View Persona Management をスタンドアロンのノート PC 用に構成する場合は、ユーザーがオフラインになったときにプロファイルの同期が維持されるようにする必要があります。 [スタンドアロン ノート型コンピュータでのユーザー プロファイルの管理](#)を参照してください。
- Windows CSC (クライアントサイド キャッシュ) を View Persona Management とともに使用しないでください。Windows CSC システムは、Windows オフライン ファイル機能をサポートするメカニズムです。このシステムがローカル システムで有効な場合、フォルダ リダイレクト、ログオン時のオフライン ファイル書き込み、バックグラウンド ダウンロード、ローカル プロファイル ファイルのリモート プロファイル リポジトリへのレプリケーションなどの View Persona Management 機能は正しく動作しません。

ベスト プラクティスとして、View Persona Management の使用を開始する前に Windows オフライン ファイル機能を無効にします。デスクトップで Windows CSC が有効になっていたために View Persona Management に問題が発生した場合には、ローカルのクライアントサイド キャッシング データベースに現在存在しているプロファイル データを同期し、Windows オフライン ファイル機能を無効にすることで問題を解決することができます。詳細な手順については、[「KB 2016416 : Windows CSC \(クライアントサイド キャッシュ\) システムが有効な場合、View Persona Management 機能が動作しない」](#)を参照してください。

ThinApp サンドボックス フォルダを含むようにユーザー プロファイルを構成

View Persona Management は、ThinApp サンドボックス フォルダをユーザー プロファイルに含めることで、ThinApp アプリケーションに関連付けられているユーザー設定を維持します。View Persona Management ポリシーを設定して、ユーザーが ThinApp アプリケーションを起動したときのパフォーマンスを向上させることができます。

View Persona Management は、ユーザーのログイン時に ThinApp サンドボックス フォルダとファイルをローカル ユーザー プロファイルに事前ロードします。ThinApp サンドボックス フォルダが作成されると、ユーザーはログオンを完了できます。パフォーマンスを向上させるために View Persona Management ではログイン時に ThinApp サンドボックス データをダウンロードしません。ただし、ユーザーのリモート プロファイル内の ThinApp サンドボックス ファイルと同じ基本属性とサイズでローカル デスクトップ上にファイルが作成されます。

ベスト プラクティスとしては、実際の ThinApp サンドボックス データをバックグラウンドでダウンロードします。[バックグラウンドでダウンロードするフォルダ] グループ ポリシー設定を有効にし、ThinApp サンドボックス フォルダを追加します。[移動と同期に関するグループ ポリシー設定](#)を参照してください。

実際の ThinApp サンドボックス ファイルは、大きい場合があります。[バックグラウンドでダウンロードするフォルダ] 設定が有効になっていると、ユーザーはアプリケーションを起動したときに大きなファイルがダウンロードされるのを待たなくて済みます。また、大きなファイルについて [事前ロードするファイルとフォルダ] 設定を使用していると、ユーザーはログイン時にファイルが事前ロードされるのを待つ必要もなくなります。

View Persona Management での View Composer 通常ディスクの構成

View Composer 通常ディスクを使用すると、リンク クローン OS ディスクの管理として更新、再構成、再分散の操作を行っているときにもユーザーのデータと設定を保持できます。通常ディスクを構成すると、ユーザーが大量の個人設定情報を生成する際の View Persona Management のパフォーマンスを向上させることができます。通常ディスクは、専用割り当てのリンク クローン デスクトップでのみ構成できます。

View Persona Management は、ネットワーク共有で構成されるリモート リポジトリにおいて、各ユーザー プロファイルを維持します。ユーザーがデスクトップにログインした後で、ユーザーの必要に応じて、個人設定ファイルが動的にダウンロードされます。

View Persona Management で通常ディスクを構成すると、リンク クローン OS ディスクを更新および再構成し、各ユーザー プロファイルのローカル コピーを通常ディスクに保存しておくことができます。

通常ディスクは、ユーザー プロファイルのキャッシュとして機能させることができます。ユーザーが個人設定ファイルが必要としたときに、ローカルの通常ディスクおよびリモート リポジトリと同じデータについては、View Persona Management でダウンロードする必要はありません。ダウンロードが必要なのは、同期されていない個人設定データのみです。

通常ディスクを構成する場合は、[ログオフ時にローカルの個人設定を削除] ポリシーを有効にしないようにしてください。このポリシーを有効にすると、ユーザーのログオフ時に通常ディスクからユーザー データが削除されます。

スタンドアロン ノート型コンピュータでのユーザー プロファイルの管理

View Persona Management を (View 以外の) スタンドアロン ノート型コンピュータにインストールする場合、ユーザーがそのスタンドアロン ノート型コンピュータをオフラインの状態にすると、ユーザー プロファイルの同期化が持続していることを確認します。

スタンドアロン ノート型コンピュータのユーザーが最新のローカル プロファイルを保有していることを確認するには、View Persona Management のグループ ポリシー設定である **Enable background download for laptops** を構成します。この設定により、ユーザー プロファイル全体がスタンドアロン ノート型コンピュータにバックグラウンドでダウンロードされます。

ベスト プラクティスとして、ネットワーク接続から外す前にユーザー プロファイルが完全にダウンロードされたことを確認するように、ユーザーに伝えてください。接続を外す前に、Background download complete(バックグラウンドでのダウンロードが完了しました)の通知がノート型コンピュータ画面に表示されるまで待つように、ユーザーに知らせてください。

ユーザーのノート型コンピュータに Background download complete(バックグラウンドでのダウンロードが完了しました)の通知を表示させるには、View Persona Management のグループ ポリシー設定である Show critical errors to users via tray icon alerts を構成します。

プロファイルのダウンロードが完了する前に、ユーザーがネットワーク接続から外した場合、ローカル プロファイルとリモート プロファイルは非同期の状態になる場合があります。オフライン状態の間では、ユーザーは全体がダウンロードされなかったローカル ファイルをアップデートする可能性があります。ユーザーがネットワークに再接続すると、ローカル プロファイルはアップロードされ、リモート プロファイルは上書きされます。元のリモート プロファイルにあったデータは失われる場合があります。

手順の例を次に示します。

前提条件

View Persona Management がユーザーのスタンドアロン ノート型コンピュータ用に構成されていることを確認します。[View Persona Management 展開の構成](#)を参照してください。

手順

- 1 スタンドアロン ノート型コンピュータを制御する Active Directory OU で、Enable background download for laptops 設定を有効にします。

グループ ポリシー オブジェクト エディタで、次のフォルダを開きます。[コンピュータの構成]、[管理テンプレート]、[従来の管理テンプレート (ADM)]、[VMware View Agent の構成]、[個人設定管理]、[移動と同期]。

[従来の管理テンプレート (ADM)] フォルダが表示されるのは、Windows 7 以降および Windows Server 2008 以降のリリースのみです。

- 2 スタンドアロン ノート型コンピュータでは、View 以外の方法を使用して、ログイン時にユーザーに通知する必要があります。

たとえば、次のようなメッセージの配信もアイデアの一つです。

個人データはログインした後に、お使いのノート型コンピュータに自動的にダウンロードされます。 ノート型コンピュータをネットワーク接続から外す前に、個人データのダウンロードが終了していることを確認してください。個人データのダウンロードが終了すると、「バックグラウンドでのダウンロードが終了しました」という通知が表示されます。

View Persona Management グループ ポリシー設定

View Persona Management ADM テンプレート ファイルと View Persona Management ADMX テンプレート ファイルには、個別のシステムまたは Active Directory サーバ上のグループ ポリシー構成に追加するグループ ポリシー設定が含まれます。グループ ポリシー設定は、View Persona Management のさまざまな機能をセットアップおよび制御するために構成する必要があります。

ADM テンプレート ファイルの名前は、ViewPM.adm です。ADMX テンプレート ファイルの名前は、ViewPM.admx です。

この ADM ファイルは、VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip という .zip バンドル ファイル内にあり、<https://my.vmware.com/web/vmware/downloads> 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 バンドル ファイルが含まれます。

ViewPM.adm または ViewPM.admx ファイルをグループ ポリシー構成に追加すると、ポリシー設定は [グループ ポリシー] ウィンドウの [個人設定管理] フォルダに表示されるようになります。

表 18-4. [グループ ポリシー] ウィンドウでの View Persona Management 設定の場所

オペレーティング システム	場所
Windows 7 以降、または Windows Server 2008 以降	[Computer Configuration (コンピュータの構成)] > [Administrative Templates (管理テンプレート)] > [Classic Administrative Templates (ADM) (従来の管理テンプレート (ADM))] > [VMware View Agent Configuration (VMware View Agent の構成)] > [Persona Management (個人設定管理)]
Windows Server 2003	[Computer Configuration (コンピュータの構成)] > [Administrative Templates (管理テンプレート)] > [VMware View Agent Configuration (VMware View Agent の構成)] > [Persona Management (個人設定管理)]

グループ ポリシー設定は、次のフォルダに含まれています。

- 移動と同期
- Folder Redirection (フォルダ リダイレクト)
- Desktop UI (デスクトップ UI)
- ログ記録

移動と同期に関するグループ ポリシー設定

移動と同期に関するグループ ポリシー設定では、View Persona Management のオンとオフの切り替え、リモート プロファイル リポジトリの場所の設定、ユーザー プロファイルに属するフォルダとファイルの指定、フォルダとファイルの同期方法の制御を行えます。

グループ ポリシー設定	説明
ユーザーの個人設定を管理	<p>ユーザー プロファイルを View Persona Management で動的に管理するか、Windows 移動プロファイルで管理するかを決定します。この設定により、View Persona Management の有効と無効が切り替わります。</p> <p>この設定が有効になっていると、View Persona Management はユーザー プロファイルを管理します。</p> <p>設定が有効になっているときは、プロファイルのアップロード間隔を分単位で指定できます。この値で、ユーザー プロファイルの変更がリモート リポジトリにコピーされる頻度が決まります。デフォルト値は 10 分です。</p> <p>この設定が無効または未構成の場合、ユーザー プロファイルは Windows で管理されます。</p>
個人設定リポジトリの場所	<p>ユーザー プロファイル リポジトリの場所を指定します。この設定により、View Persona Management で指定されているネットワーク共有を使用するか、Windows 移動プロファイルをサポートする Active Directory で構成されているバスを使用するかも決まります。</p> <p>この設定が有効になっていると、[共有バス] を使用してユーザー プロファイル リポジトリの場所を指定できます。</p> <p>[共有バス] テキスト ボックスで、View Persona Management デスクトップからアクセス可能なネットワーク共有の UNC バスを指定します。この設定により、View Persona Management でユーザー プロファイル リポジトリの場所を制御できます。</p> <p>例：\\server.domain.com\VPRepository</p> <p>構成するフォルダ バスに %username% が含まれていない場合は、View Persona Management により %username%.%userdomain% がバスに追加されます。</p> <p>例：\\server.domain.com\VPRepository\%username%.%userdomain%</p> <p>[共有バス] で場所を指定すると、Windows で移動プロファイルをセットアップしたり、Windows 移動プロファイルをサポートするために Active Directory でユーザー プロファイルのバスを構成したりする必要があります。</p> <p>View Persona Management 向け UNC ネットワーク共有の構成の詳細については、ユーザー プロファイル リポジトリの構成を参照してください。</p> <p>デフォルトでは、Active Directory ユーザー プロファイル バスが使用されます。</p> <p>厳密に言えば、[共有バス] が空白になっていると、Active Directory ユーザー プロファイル バスが使用されるということです。この設定が無効または未構成の場合、[共有バス] は空白で非アクティブとなります。この設定が有効になっていても、バスを空白にしておくことができます。</p> <p>この設定が有効になっている場合、[Active Directory ユーザー プロファイルのバスが構成されている場合はこれを上書きする] チェックボックスをオンにすれば、[共有バス] で指定されているバスが確実に View Persona Management で使用されるようになります。デフォルトでは、このチェックボックスはオフになっており、両方の場所が構成されている場合は View Persona Management で Active Directory ユーザー プロファイルのバスが使用されます。</p>
ログオフ時にローカルの個人設定を削除	<p>ユーザーがログオフするときに、ローカルに保存されている各ユーザーのプロファイルを View マシンから削除します。</p> <p>また、ユーザー プロファイルが削除されるときに、各ユーザーのローカル設定フォルダも削除する場合は、チェックボックスをオンにします。このチェック ボックスをオンにすると、AppData\Local フォルダが削除されません。</p> <p>この設定の使用に関するガイドラインについては、View Persona Management 展開を構成するためのベストプラクティスを参照してください。</p> <p>この設定が無効または未構成の場合、ローカルで保存されているユーザー プロファイル（ローカル設定フォルダを含む）は、ユーザーのログオフ時に削除されません。</p>
Roam local settings folders (ローカル設定フォルダを移動)	<p>残りの各ユーザー プロファイルとともに、ローカル設定フォルダを移動します。</p> <p>このポリシーは AppData\Local フォルダに影響を及ぼします。</p> <p>デフォルトでは、ローカル設定は移動しません。</p> <p>Microsoft OneDrive を使用する場合は、この設定を有効にする必要があります。</p>

グループ ポリシー設定	説明
事前ロードするファイルとフォルダ	<p>ユーザーのログイン時にローカル ユーザー プロファイルにダウンロードされるファイルとフォルダのリストを指定します。ファイルが変更されると、変更内容がリモート リポジトリにコピーされます。</p> <p>状況によっては、ローカルで保存されているユーザー プロファイルに特定のファイルとフォルダを事前ロードした方がよい場合があります。この設定を使用して、これらのファイルとフォルダを指定します。</p> <p>ローカル プロファイルのルートへの相対パスを指定します。パス名にドライブを指定しないでください。</p> <p>例: <code>Application Data\Microsoft\Certificates</code></p> <p>指定したファイルとフォルダが事前ロードされると、View Persona Management では、別のプロファイル データを管理する場合と同じように、ファイルとフォルダを管理します。事前ロードしたファイルとフォルダをユーザーが更新すると、View Persona Management はセッション中に、次のプロファイル アップロードの間隔で、更新されたデータをリモート プロファイル リポジトリにコピーします。</p>
Files and folders to preload (exceptions) (事前ロードするファイルとフォルダ (例外))	<p>指定したファイルとフォルダは事前ロードされないようにします。</p> <p>選択したフォルダ パスは、[事前ロードするファイルとフォルダ] 設定で指定したフォルダ内になければなりません。</p> <p>ローカル プロファイルのルートへの相対パスを指定します。パス名にドライブを指定しないでください。</p>
Windows roaming profiles synchronization (Windows 移動プロファイルの同期)	<p>標準の Windows 移動ファイルで管理されるファイルとフォルダのリストを指定します。ユーザーのログイン時に、リモート リポジトリからファイルとフォルダが取得されます。ユーザーがログオフするまで、ファイルはリモート リポジトリにコピーされません。</p> <p>指定したファイルとフォルダについては、[ユーザーの個人設定を管理] 設定の [プロファイルのアップロード間隔] で構成されるプロファイル レプリケーション間隔が View Persona Management で無視されます。</p> <p>ローカル プロファイルのルートへの相対パスを指定します。パス名にドライブを指定しないでください。</p>
Windows roaming profiles synchronization (exceptions) (Windows 移動プロファイルの同期 (例外))	<p>選択したファイルとフォルダは、[Windows 移動プロファイルの同期] 設定で指定されているパスの例外となります。</p> <p>選択したフォルダ パスは、[Windows 移動プロファイルの同期] 設定で指定したフォルダ内になければなりません。</p> <p>ローカル プロファイルのルートへの相対パスを指定します。パス名にドライブを指定しないでください。</p>
Files and folders excluded from roaming (移動対象から除外されるファイルとフォルダ)	<p>残りのユーザー プロファイルと一緒に移動しないようにするファイルとフォルダのリストを指定します。指定したファイルとフォルダはローカル システムのみに存在します。</p> <p>場合によっては、特定のファイルとフォルダについて、ローカルで保存されているユーザー プロファイルのみに存在することが求められます。たとえば、一時ファイルやキャッシュ ファイルを移動から除外できます。これらのファイルは、リモート リポジトリへのレプリケーションが不要です。</p> <p>ローカル プロファイルのルートへの相対パスを指定します。パス名にドライブを指定しないでください。</p> <p>デフォルトでは、ユーザー プロファイルの一時フォルダ、ThinApp のキャッシュ フォルダ、および Internet Explorer、Firefox、Chrome、Opera 用のキャッシュ フォルダは、移動対象から除外されます。</p>
Files and folders excluded from roaming (exceptions) (移動対象から除外されるファイルとフォルダ (例外))	<p>選択したファイルとフォルダは、[移動対象から除外されるファイルとフォルダ] 設定で指定されているパスの例外となります。</p> <p>選択したフォルダ パスは、[移動対象から除外されるファイルとフォルダ] 設定で指定したフォルダ内になければなりません。</p> <p>ローカル プロファイルのルートへの相対パスを指定します。パス名にドライブを指定しないでください。</p>

グループ ポリシー設定	説明
ノート PC に対するバックグラウンドでのダウンロードの有効化	<p>ユーザーが View Persona Management ソフトウェアがインストールされているノート PC にログインしたときに、ユーザー プロファイル内のすべてのファイルがダウンロードされます。ファイルはバックグラウンドでダウンロードされます。</p> <p>操作が完了すると、ユーザー画面に次のポップアップ通知が表示されます。バックグラウンドでのダウンロードが完了しました。この通知をユーザーのノート PC に表示するには、トレイ アイコン アラートを使用して重大なエラーをユーザーに表示設定を有効にする必要があります。</p> <p>注: この設定を有効にした場合、ベスト プラクティスとして、ネットワークから切断する前に、プロファイルが完全にダウンロードされたことを確認するようにユーザーに通知します。</p> <p>プロファイルのダウンロードが完了する前に、スタンドアロンのノート PC をオフラインにすると、ユーザーはローカル プロファイル ファイルにアクセスできなくなる場合があります。ユーザーは、オフラインの間、一部しかダウンロードされなかったローカル ファイルを開くことができません。</p> <p>スタンドアロン ノート型コンピュータでのユーザー プロファイルの管理を参照してください。</p>
バックグラウンドでダウンロードするフォルダ	<p>選択したフォルダは、ユーザーがデスクトップにログインした後で、バックグラウンドでダウンロードされます。場合によっては、特定のフォルダの中身をバックグラウンドでダウンロードすることで、View Persona Management を最適化できます。この設定が有効になっていると、ユーザーはアプリケーションを起動したときに大きなファイルがダウンロードされるのを待たなくて済みます。また、非常に大きなファイルで [事前ロードするファイルとフォルダ] 設定を使用していると、ユーザーはログイン時にファイルが事前ロードされるのを待たなくて済みます。</p> <p>たとえば、VMware ThinApp サンドボックス フォルダを [バックグラウンドでダウンロードするフォルダ] 設定に含めることができます。バックグラウンドでのダウンロードは、デスクトップでユーザーがログインするときや別のアプリケーションを使用するときのパフォーマンスに影響しません。ユーザーが ThinApp アプリケーションを起動すると、必要な ThinApp サンドボックス ファイルがリモート リポジトリからダウンロードされる可能性が高くなり、アプリケーションの起動時間が短縮されます。</p> <p>ローカル プロファイルのルートへの相対パスを指定します。パス名にドライブを指定しないでください。</p>
バックグラウンドでダウンロードするフォルダ (例外)	<p>選択したフォルダは、[バックグラウンドでダウンロードするフォルダ] 設定で指定したパスの例外となります。選択したフォルダ パスは、[バックグラウンドでダウンロードするフォルダ] 設定で指定したフォルダ内になければなりません。</p> <p>ローカル プロファイルのルートへの相対パスを指定します。パス名にドライブを指定しないでください。</p>
除外されるプロセス	<p>指定したプロセスの I/O は View Persona Management から無視されます。</p> <p>パフォーマンスの問題を回避するために、特定のウイルス対策アプリケーションを [除外されるプロセス] リストに追加しなければならない場合があります。ウイルス対策アプリケーションに、オンデマンドでのスキャン時にオフライン ファイルの取得を無効にする機能がない場合は、[除外されるプロセス] 設定により、ウイルス対策アプリケーションは不必要にファイルを取得しなくなります。ただし、View Persona Management は、除外されるプロセスによって行われるユーザー プロファイル内のファイルおよび設定に対する変更は行いません。</p> <p>プロセスを [除外されるプロセス] リストに追加するには、この設定を有効にし、[表示] をクリックし、プロセス名を入力して、[OK] をクリックします。例 : process.exe。</p>
CLFS ファイルのクリーンアップ	<p>ログオン時に <code>ntuser.dat</code> と <code>usrclass.dat</code> 用として共通ログ ファイル システム (CLFS) によって移動プロファイルから生成されるファイルを削除します。</p> <p>この設定を有効にするのは、これらのファイルに問題が起きているユーザー プロファイルを修正する必要がある場合だけに限定してください。これらのファイルに問題がない限り、設定を無効または未構成のままにしておいてください。</p>

フォルダ リダイレクトのグループ ポリシー設定

フォルダ リダイレクトのグループ ポリシー設定を使用すると、ユーザー プロファイル フォルダをネットワーク共有にリダイレクトできます。フォルダがリダイレクトされると、ユーザー セッション中にすべてのデータがネットワーク共有に直接保存されます。

この設定は、高可用性を必要とするフォルダをリダイレクトする際に使用できます。View Persona Management により、プロファイル アップロード間隔の設定値に応じて、1 分ごとに、ローカル ユーザー プロファイルからリモート プロファイルに更新がコピーされます。ただし、ローカル システムでネットワーク停止や障害が発生した場合、前回のレプリケーション以降のユーザーの更新については、リモート プロファイルに保存されないことがあります。数分間の一時的な作業データ紛失を許容できないユーザーの場合は、このような重要なデータを格納しているフォルダをリダイレクトできます。

フォルダのリダイレクトについては、次のルールとガイドラインが適用されます。

- この設定をフォルダに対して有効にすると、フォルダのリダイレクト先となるネットワーク共有の UNC パスを入力する必要があります。
- 構成するフォルダ パスに %username% が含まれていない場合は、View 個人設定管理 により %username% が UNC パスに追加されます。
- ベスト プラクティスとして、フォルダ パスに %username% が含まれるように構成しますが、パスの最後のサブフォルダには My Videos などのリダイレクト対象フォルダ名を使用するようにします。ユーザーのデスクトップ上ではフォルダ名としてパスの最後のフォルダが表示されます。詳細については、以下を参照してください。[リダイレクト対象フォルダのパスの構成](#)。
- 各フォルダに個別の設定を構成します。リダイレクト対象として特定のフォルダを選択し、それ以外をローカルの View デスクトップに残したままにすることができます。また、別のフォルダを別の UNC パスにリダイレクトすることも可能です。
- フォルダのリダイレクト設定が無効または未構成の場合、フォルダはローカルの View デスクトップに保存され、View Persona Management のグループ ポリシー設定に従って管理されます。
- View Persona Management と Windows 移動プロファイルで同一フォルダへのリダイレクトが構成されている場合は、View Persona Management のフォルダ リダイレクトが Windows 移動プロファイルよりも優先されます。
- フォルダのリダイレクトは、Windows シェル API を使用して共通フォルダ パスにリダイレクトするアプリケーションに対してのみ適用されます。たとえば、ファイルを %USERPROFILE%\AppData\Roaming に書き込むアプリケーションの場合、そのファイルはローカル プロファイルに書き込まれ、ネットワークの格納場所にはリダイレクトされません。
- デフォルトでは、Windows のフォルダ リダイレクトにより、リダイレクトされるフォルダへの排他的権限がユーザーに与えられます。新しくリダイレクトされたフォルダへのアクセスをドメイン管理者に与えるには、View Persona Management グループ ポリシー設定を使用できます。

Windows のフォルダ リダイレクトには [[ユーザーに *folder-name* に対する排他的権限を与える]] というチェックボックスがあり、リダイレクトされるフォルダにユーザー固有の排他的権限を与えます。セキュリティ対策のため、このチェックボックスはデフォルトで選択されています。このチェックボックスを選択すると、管理者はリダイレクトされたフォルダにアクセスできません。管理者がユーザーのリダイレクトされたフォルダに対するアクセス権を強制的に変更しようとする、そのユーザーに対して View Persona Management が機能しなくなります。

[リダイレクトされたフォルダに管理者グループを追加] グループ ポリシー設定を使用して、新しくリダイレクトされたフォルダにドメイン管理者がアクセスできるようにすることができます。この設定により、ドメイン管理者グループに、リダイレクトされた各フォルダへのフル コントロールを付与することができます。表 18-5. [フォルダ リダイレクトを制御するグループ ポリシー設定](#)を参照してください。

既存のリダイレクトされたフォルダについては、[既存のリダイレクト対象フォルダへのアクセスをドメイン管理者に付与する](#)を参照してください。

フォルダ リダイレクトから除外されるフォルダ パスを指定できます。表 18-5. [フォルダ リダイレクトを制御するグループ ポリシー設定](#)を参照してください。

注意: View では、View Persona Management によって管理されるプロファイルにすでにあるフォルダに対するフォルダ リダイレクトの有効化はサポートされていません。この構成により、View Persona Management で障害が発生し、ユーザー データが失われる場合があります。

たとえば、リモート プロファイル リポジトリのルート フォルダが `\\Server\%username%` であり、フォルダを `\\Server\%username%\Desktop` にリダイレクトすると、これらの設定により、View Persona Management でフォルダ リダイレクトの障害が発生し、以前は `\\Server\%username%\Desktop` フォルダにあったコンテンツが失われます。

次のフォルダをネットワーク共有にリダイレクトできます。

- Application Data (アプリケーション データ) (移動)
- Contacts (連絡先)
- Cookies (クッキー)
- デスクトップ
- ダウンロード
- お気に入り
- History (履歴)
- Links (リンク)
- マイ ドキュメント
- My Music (マイ ミュージック)
- My Pictures (マイ ピクチャ)
- My Videos (マイ ビデオ)
- Network Neighborhood (ネットワーク コンピュータ)

- Printer Neighborhood (近くのプリンタ)
- Recent Items (最近使った項目)
- Save Games (セーブ ゲーム)
- Searches (検索)
- Start Menu (スタート メニュー)
- Startup Items (スタートアップ項目)
- Templates (テンプレート)
- Temporary Internet Files (インターネット一時ファイル)

表 18-5. フォルダ リダイレクトを制御するグループ ポリシー設定

グループ ポリシー設定	説明
リダイレクトされたフォルダに管理者グループを追加	リダイレクトされた各フォルダに管理者グループを追加するかどうかを指定します。デフォルトでは、ユーザーにリダイレクトされたフォルダへの排他的権限があります。この設定を有効にすると、管理者もリダイレクトされたフォルダにアクセスできます。 デフォルトでは、この設定は構成されていません。
Files and Folders excluded from Folder Redirection (フォルダ リダイレクトから除外されるファイルとフォルダ)	選択されたファイルおよびフォルダ パスはネットワーク共有にリダイレクトされません。 場合によっては、特定のファイルとフォルダがローカル ユーザー プロファイルにとどまっている必要があります。フォルダ パスを [フォルダ リダイレクトから除外されるファイルとフォルダ] リストに追加するには、この設定を有効にして [表示] をクリックし、パス名を入力して [OK] をクリックします。 ユーザーのローカル プロファイルのルートへの相対的なフォルダ パスを指定します。例： Desktop\New Folder。
フォルダ リダイレクトから除外されるファイルとフォルダ (例外)	選択されたファイルとフォルダ パスは、[フォルダ リダイレクトから除外されるファイルとフォルダ] 設定で指定されたパスの例外となります。 フォルダ パスを [フォルダ リダイレクトから除外されるファイルとフォルダ (例外)] リストに追加するには、この設定を有効にして [表示] をクリックし、パス名を入力して [OK] をクリックします。 [フォルダ リダイレクトから除外されるフォルダ] 設定で指定されたフォルダ内にあり、ユーザーのローカル プロファイルに対して相対的なフォルダ パスを指定します。例： Desktop\New Folder\Unique Folder。

既存のリダイレクト対象フォルダへのアクセスをドメイン管理者に付与する

デフォルトでは、Windows のフォルダ リダイレクトにより、リダイレクトされるフォルダへの排他的権限がユーザーに与えられます。リダイレクトされた既存のフォルダへのアクセス権をドメイン管理者に付与するには、`icacls` ユーティリティを使用する必要があります。

View Persona Management で使用するために、新規にリダイレクトされたフォルダを設定する場合、[リダイレクトされたフォルダに管理者グループを追加] グループ ポリシー設定を使用して、ドメイン管理者が新規にリダイレクトされたフォルダにアクセスできるようにすることができます。表 18-5. フォルダ リダイレクトを制御するグループ ポリシー設定を参照してください。

手順

- 1 ファイルやフォルダで管理者の所有権を設定します。

```
icacls "\\file-server\persona-share\*" /setowner "domain\admin" /T /C /L /Q
```

```
例: icacls "\\myserver-123abc\folders\*" /setowner "mycompanydomain
\vcadmin" /T /C /L /Q
```

- 2 ファイルやフォルダの ACL を変更します。

```
icacls "\\file-server\persona-share\*" /grant "admin-group":F /T /C /L /Q
```

```
例: icacls "\\myserver-123abc\folders\*" /grant "Domain-Admins":F /T /C /L /Q
```

- 3 ユーザー フォルダごとに、管理者から該当ユーザーに所有権を戻します。

```
icacls "\\file-server\persona-share\*" /setowner "domain\folder-
owner" /T /C /L /Q
```

```
例: icacls "\\myserver-123abc\folders\*" /setowner "mycompanydomain\user1" /T /C /
L /Q
```

デスクトップ UI のグループ ポリシー設定

デスクトップ UI のグループ ポリシー設定は、ユーザーのデスクトップに表示される View Persona Management 設定を制御します。

グループ ポリシー設定	説明
Hide local offline file icon (ローカルのオフライン ファイル アイコンを非表示にする)	ユーザー プロファイルに属しているローカル保存のファイルをユーザーが表示するときに、オフライン アイコンを非表示するかどうかを指定します。この設定を有効にすると、Windows エクスプローラおよび大部分の Windows ダイアログ ボックスでオフライン アイコンが非表示になります。 デフォルトでは、オフライン アイコンは表示されません。
Show progress when downloading large files (大きなファイルのダウンロード時には進行状況を示す)	クライアントがリモート リポジトリから大きなファイルを取得する場合に、ユーザーのデスクトップに進行状況ウィンドウを表示するかどうかを指定します。 この設定を有効にすると、進行状況ウィンドウの表示を開始する最小ファイル サイズをメガバイト単位で指定できます。このウィンドウは、指定した量のデータがリモート リポジトリから取得されると View Persona Management で判断されたときに表示されます。この値は、一度に取得するすべてのファイルの集計です。 たとえば、設定値が 50 MB のときに 40 MB のファイルを取得すると、ウィンドウは表示されません。最初のファイルのダウンロード中に 30 MB のファイルを取得すると、ダウンロードの合計量が設定値を超えるため、進行状況ウィンドウが表示されます。ウィンドウは、ファイルのダウンロードが開始されるときに表示されます。 デフォルトでは、この値は 50 MB です。 デフォルトでは、この進行状況ウィンドウは表示されません。
Show critical errors to users via tray icon alerts (トレイ アイコン アラートを使用して重大なエラーをユーザーに表示)	レプリケーションまたはネットワーク接続で障害が発生したときに、重大なエラー アイコン アラートをデスクトップトレイに表示します。 デフォルトでは、このアイコン アラートは非表示になっています。

ログのグループ ポリシー設定

ログのグループ ポリシー設定は、View Persona Management ログ ファイルの名前、場所、動作を指定します。

次の表では、ログのグループ ポリシー設定についてそれぞれ説明します。

グループ ポリシー設定	説明
Logging filename (ログ ファイル名)	ローカルの View Persona Management ログ ファイルの完全パス名を指定します。 デフォルトのパスは、ProgramData\VMware\VDM\logs\ <i>filename</i> です。 デフォルトのログファイル名は、VMWVvp.txt です。
Logging destination (ログの書き込み先)	すべてのログ メッセージをログ ファイルに書き込むか、デバッグ ポートに書き込むか、その両方に書き込むかを指定します。 デフォルトでは、ログ メッセージはログ ファイルに送信されます。
Logging flags (ログ フラグ)	生成するログ メッセージのタイプを指定します。 <ul style="list-style-type: none"> ■ 情報メッセージをログに記録する。 ■ デバッグ メッセージをログに記録する。 この設定が無効になるか構成されない場合、およびデフォルトで設定が構成されている場合にと、この設定が無効にされるか構成されないと、ログ メッセージが情報レベルに設定されます。
ログの履歴の深さ	View Persona Management で維持する履歴ログ ファイルの数を決定します。 維持する履歴ログ ファイルの数を最小 1 から最大 10 まで設定可能です。 デフォルトでは、1 つの履歴ログ ファイルが維持されます。
ネットワークへのログのアップロード	View Persona Management ログ ファイルを、ユーザーがログオフする時に、指定したネットワーク共有へアップロードします。 この設定が有効になっている場合、ネットワーク共有のパスを指定します。ネットワーク共有のパスは、UNC パスである必要があります。View Persona Management では、ネットワーク共有は作成されません。 デフォルトでは、ログ ファイルはネットワーク共有にアップロードされません。

マシンとデスクトップ プールのトラブルシューティング

19

マシンおよびデスクトップ プールの作成および使用中に発生する可能性のある問題を診断および解決するために、さまざまな手順を使用できます。

ユーザーが Horizon Client を使用してデスクトップおよびアプリケーションにアクセスしているときに問題が発生することがあります。トラブルシューティングの手順を使用して問題の原因を調べ、解決を試みることも、VMware のテクニカル サポートから支援を受けることもできます。

この章には、次のトピックが含まれています。

- [問題のあるマシンの表示](#)
- [デスクトップ ユーザーへのメッセージの送信](#)
- [デスクトップ プールのプロビジョニングまたは再作成に関する問題](#)
- [ネットワーク接続に関する問題のトラブルシューティング](#)
- [USB リダイレクトに関する問題のトラブルシューティング](#)
- [資格のないユーザーのマシンおよびポリシーの管理](#)
- [ViewDbChk コマンドを使用したデータベース不整合の解決](#)
- [トラブルシューティングの追加情報](#)

問題のあるマシンの表示

動作が疑わしいとして View によって検出されたマシンのリストを表示できます。

View Administrator には、次の問題があるマシンが表示されます。

- パワーオンされているが、応答していない
- 長時間プロビジョニング状態のままである
- 作動可能状態だが、接続を受け入れていないと報告している
- vCenter Server に存在しないように見える
- コンソール上のアクティブなログイン、資格のないユーザーによるログイン、または View 接続サーバ インスタンスを経由しないで行われたログインがある

手順

- 1 View Administrator で、[リソース] - [マシン] を選択します。
- 2 [vCenter 仮想マシン] タブで、[問題のあるマシン] をクリックします。

次のステップ

必要な処置は、View Administrator が各マシンについて報告した問題によって異なります。

- リンク クローン マシンがエラー状態にある場合、View の自動リカバリ メカニズムはそのリンク クローンのパワーオン、またはシャットダウンと再起動を試みます。リカバリが繰り返し失敗すると、そのリンク クローンは削除されます。状況によって、リンク クローンが繰り返し削除されて再作成される場合があります。[繰り返し削除と再作成が行われるマシンのトラブルシューティング](#)を参照してください。
- マシンがパワーオンされているが応答しない場合は、仮想マシンを再起動します。それでもマシンが応答しない場合は、使用している Horizon Agent のバージョンがマシンのオペレーティング システムでサポートされていることを確認します。vdmadmin コマンドと -A オプションを使用して、Horizon Agent バージョンを表示できます。詳細については、『View 管理』を参照してください。
- マシンが長時間プロビジョニング状態のままになる場合は、その仮想マシンを削除して、再度クローンを作成します。マシンをプロビジョニングするために十分なディスク領域があることを確認します。[仮想マシンのプロビジョニング状態の継続](#)を参照してください。
- マシンが作動可能と報告しているが、接続を受け入れない場合は、ファイアウォール構成をチェックして、表示プロトコルがブロックされていないことを確認します。[マシンと View 接続サーバ インスタンスの接続の問題](#)を参照してください。
- マシンが vCenter Server に存在しないように見える場合は、その仮想マシンが予期された vCenter Server 上に構成されているかどうか、別の vCenter Server に移動したかを確認します。
- マシンにアクティブなログインがあるが、それがコンソールに表示されない場合、そのセッションはリモートです。ログインしているユーザーと通信できない場合は、仮想マシンの再起動によるユーザーの強制ログアウトが必要になることがあります。

デスクトップ ユーザーへのメッセージの送信

現在デスクトップにログインしているユーザーへのメッセージの送信が必要になることがあります。たとえば、マシンのメンテナンスを行う必要がある場合は、一時的にログアウトするようにユーザーに依頼したり、今後のサービス停止をユーザーに警告したりすることができます。1 つのメッセージを複数のユーザーに送信することができます。

手順

- 1 View Administrator で、[カタログ] - [デスクトップ プール] をクリックします。
- 2 プールをダブルクリックし、[セッション] タブをクリックします。
- 3 1 つ以上のマシンを選択し、[メッセージを送信] をクリックします。
- 4 メッセージを入力し、メッセージのタイプを選択して、[OK] をクリックします。
メッセージのタイプは、[情報]、[警告]、または [エラー] のいずれかになります。

メッセージは、アクティブなセッションで選択されているすべてのマシンに送信されます。

デスクトップ プールのプロビジョニングまたは再作成に関する問題

デスクトップ プールのプロビジョニングまたは再作成に関する問題を診断および解決するために、いくつかの手順を使用できます。

インスタントクローンのプロビジョニングまたはイメージ プッシュの失敗

インスタントクローン デスクトップ プールの保留中イメージが、失敗状態です。

問題

プールの作成中またはイメージ プッシュの操作中に、「Fault type is SERVER_FAULT_FATAL – Runtime error: Method called after shutdown was initiated(障害タイプ SERVER_FAULT_FATAL – ランタイム エラー:シャットダウン後に呼び出されたメソッドが開始されました)」というエラー メッセージが表示されます。

原因

これは、別の接続サーバでイメージ操作の実行中にレプリカの接続サーバが起動した場合に発生することがあります。

解決方法

- ◆ プールの作成中にエラーが発生した場合、プロビジョニングが無効であれば有効にします。これが有効になっている場合は、無効にしてから有効にします。
- ◆ イメージ プッシュの操作中にエラーが発生した場合、同じイメージで別のイメージ プッシュ操作を開始します。

インスタント クローンのイメージ公開の失敗

View Administrator はイメージ公開の失敗を示します。

問題

インスタントクローン デスクトップ プールの作成またはプッシュ イメージの開始後に処理のステータスを確認すると、View Administrator はイメージ公開の失敗を示します。

解決方法

- ◆ プロビジョニングが無効になっている場合は、再び有効にします。これが有効になっている場合は、無効にしてから有効にします。これによって、View は新規に最初の公開処理をトリガします。
- ◆ 現在のイメージに問題があると判断された場合は、異なるイメージを使用して別のプッシュ イメージ操作を開始します。

次のステップ

イメージ公開が繰り返し失敗する場合は、30 分間後に再試行します。

インスタントクローンのプロビジョニング中の無限エラー リカバリ

インスタントクローン デスクトップ プールのプロビジョニング中に、エラー リカバリが無限ループに入ります。

問題

プロビジョニング中に、インスタント クローンで、「No network connection between Agent and connection Server (Agent と接続サーバの間にネットワーク接続がありません)」というエラー メッセージが表示され、エラー状態となる場合があります。自動エラー リカバリ メカニズムによってクローンが削除されて再作成され、再作成されたクローンが同じエラー状態となって、プロセスが無期限に繰り返されます。

原因

可能性のある原因には、永続的なネットワーク エラー、カスタマイズ後スクリプトへのパスの誤りなどがあります。

解決方法

- ◆ ネットワークのエラーまたはカスタマイズ後スクリプトへのパスを修正します。

孤立したインスタント クローンを削除できない

まれに、プロビジョニング中にインスタント クローンがエラー状態になり、View Administrator からデスクトップ プールを削除できないことがあります。

問題

プールを削除するために、View は vCenter Server にクローンのパワーオフを要求します。しかし、孤立したクローンについては要求が失敗します。このため、View はプールを削除できません。

解決方法

- 1 vCenter Server から、孤立したクローンの登録を解除します。
- 2 View Administrator から、クローンを削除します。

カスタマイズ仕様が見つからない場合のプール作成の失敗

デスクトップ プールを作成しようとして、カスタマイズ仕様が見つからないと、操作が失敗します。

問題

デスクトップ プールを作成できず、イベント データベースに次のメッセージが表示されます。

```
Provisioning error occurred for Machine <varname>Machine_Name</varname>:(マシン <varname>Machine_Name</varname> でプロビジョニング エラーが発生しました:)Customization failed for Machine(マシンのカスタマイズに失敗しました)
```

原因

この問題で最も可能性の高い原因は、カスタマイズ仕様にアクセスするため、またはプールを作成するために十分な権限がないことです。もう 1 つ可能性のある原因は、カスタマイズ仕様の名前が変更されたか、カスタマイズ仕様が削除されたことです。

解決方法

- ◆ カスタマイズ仕様にアクセスするため、およびプールを作成するために十分な権限があることを確認します。
- ◆ 必要なカスタマイズ仕様の名前の変更または削除により存在しない場合は、別の仕様を選択します。

権限の問題によるプール作成の失敗

SX/ESXi ホスト、SX/ESXi クラスタ、またはデータベースに権限の問題がある場合、デスクトップ プールを作成できません。

問題

テンプレート、SX/ESXi ホスト、SX/ESXi クラスタ、またはデータセンターにアクセスできないため、View Administrator でデスクトップ プールを作成できません。

原因

この問題には、多くの原因が考えられます。

- プールを作成するために正しい権限がない。
- テンプレートにアクセスするために正しい権限がない。
- ESX/ESXi ホスト、ESX/ESXi クラスタ、またはデータセンターにアクセスするための適切な権限がない。

解決方法

- ◆ [Template Selection (テンプレートの選択)] 画面に使用可能なテンプレートが表示されない場合、テンプレートにアクセスするための十分な権限があることを確認します。
- ◆ ESX/ESXi ホスト、ESX/ESXi クラスタ、またはデータセンターにアクセスするための十分な権限があることを確認します。
- ◆ プールを作成するために十分な権限があることを確認します。

構成の問題によるプールのプロビジョニングの失敗

テンプレートが使用できないか、仮想マシン イメージが移動または削除された場合、デスクトップ プールのプロビジョニングが失敗することがあります。

問題

デスクトップ プールがプロビジョニングされず、イベント データベースに次のメッセージが表示されます。

Provisioning error occurred on Pool <varname>Desktop_ID</varname> because of a configuration problem(構成の問題のため、プール <varname>Desktop_ID</varname> でプロビジョニング エラーが発生しました)

原因

この問題には、多くの原因が考えられます。

- テンプレートにアクセスできない。
- vCenter でテンプレート名が変更されている。
- vCenter でテンプレートが別のフォルダに移動された。
- 仮想マシン イメージが ESX/ESXi ホスト間で移動したか、削除されている。

解決方法

- ◆ テンプレートにアクセスできることを確認します。
- ◆ テンプレートの名前とフォルダが正しく指定されていることを確認します。
- ◆ 仮想マシン イメージを ESX/ESXi ホスト間で移動した場合は、仮想マシンを正しい vCenter フォルダに移動します。
- ◆ 仮想マシン イメージが削除されている場合は、View Administrator でその仮想マシンのエントリを削除し、イメージを再作成または復元します。

View 接続サーバ インスタンスが vCenter に接続できないことによるプールのプロビジョニングの失敗

接続サーバが vCenter に接続できない場合、デスクトップ プールのプロビジョニングが失敗することがあります。

問題

デスクトップ プールのプロビジョニングが失敗し、イベント データベースに次のいずれかのメッセージが表示されます。

- Cannot log in to vCenter at address *VC_Address*(アドレス *VC_Address* の vCenter にログインできません)
- The status of vCenter at address *VC_Address* is unknown(アドレス *VC_Address* の vCenter のステータスが不明です)

原因

View 接続サーバ インスタンスが次のいずれかの理由で vCenter に接続できません。

- vCenter Server 上の Web サービスが停止した。
- View 接続サーバ ホストと vCenter Server の間にネットワークの問題がある。
- vCenter または View Composer のポート番号とログインの詳細が変更された。

解決方法

- ◆ vCenter で Web サービスが実行されていることを確認します。
- ◆ View 接続サーバ ホストと vCenter の間にネットワークの問題がないことを確認します。
- ◆ View Administrator で、vCenter および View Composer に構成されているポート番号とログインの詳細を確認します。

データストアの問題によるプールのプロビジョニングの失敗

データストアのディスク領域が不足しているか、データストアにアクセスする権限がない場合、デスクトップのプロビジョニングが失敗することがあります。

問題

デスクトップ プールのプロビジョニングが失敗し、イベント データベースに次のいずれかのメッセージが表示されます。

- Provisioning error occurred for Machine *Machine_Name*: (マシン *Machine_Name* でプロビジョニング エラーが発生しました:) Cloning failed for Machine (マシンのクローンの作成に失敗しました)
- Provisioning error occurred on Pool *Desktop_ID* because available free disk space is reserved for linked clones (使用可能な空きディスク領域がリンク クローン用に予約されているため、プール *Desktop_ID* でプロビジョニング エラーが発生しました)
- Provisioning error occurred on Pool *Desktop_ID* because of a resource problem (リソースの問題のため、プール *Desktop_ID* でプロビジョニング エラーが発生しました)

原因

選択したデータストアにアクセスする権限がないか、プールに使用されているデータストアのディスク領域が不足しています。

解決方法

- ◆ 選択したデータストアにアクセスするために十分な権限があることを確認します。
- ◆ データストアが構成されているディスクがいっぱいになっていないことを確認します。
- ◆ ディスクがいっぱいになっているか領域が予約されている場合は、ディスク上の領域を解放するか、使用可能なデータストアを再分散するか、データストアをより大容量のディスクに移行します。

vCenter Server の過負荷によるプールのプロビジョニングの失敗

vCenter Server が要求で過負荷になると、デスクトップ プールのプロビジョニングが失敗することがあります。

問題

デスクトップ プールのプロビジョニングが失敗し、イベント データベースに次のエラー メッセージが表示されます。

```
カスタマイズ中のタイムアウトにより、プール <varname id="varname_76C2270646664C0B89AC2F37A5F3F201">Desktop_ID</varname>
でプロビジョニング エラーが発生しました
```

原因

vCenter で要求が過負荷になっています。

解決方法

- ◆ View Administrator で、vCenter Server での同時プロビジョニング操作と同時電源操作の最大数を減らします。
- ◆ 追加の vCenter Server インスタンスを構成します。

vCenter Server の構成の詳細については、『View インストール ガイド』を参照してください。

仮想マシンのプロビジョニング状態の継続

クローンを作成した後、仮想マシンがプロビジョニング状態のままになります。

問題

仮想マシンがプロビジョニング状態のままになります。

原因

この問題の最も可能性の高い原因は、クローンの作成操作の途中で View 接続サーバ インスタンスを再起動したことです。

解決方法

- ◆ 仮想マシンを削除して、再度クローンを作成します。

仮想マシンのカスタマイズ状態の継続

クローンを作成した後、仮想マシンがカスタマイズ状態のままになります。

問題

仮想マシンがカスタマイズ状態のままになります。

原因

この問題の最も可能性の高い原因は、仮想マシンを起動するために十分なディスク領域がないことです。カスタマイズを行う前に、仮想マシンを起動する必要があります。

解決方法

- ◆ 仮想マシンを削除して、カスタマイズ状態から復旧します。
- ◆ ディスクがいっぱいになっている場合は、ディスク上の領域を解放するか、データストアをより大容量のディスクに移行します。

孤立または削除されたリンク クローンの削除

特定の条件下では、View、View Composer、および vCenter Server のリンク クローン データの同期が解除される場合があります、リンク クローン マシンをプロビジョニングまたは削除できない場合があります。

問題

- リンク クローン デスクトップ プールをプロビジョニングできません。
- リンク クローン マシンのプロビジョニングは失敗し、次のエラーが発生します。入力仕様のある仮想マシンはすでに存在しています
- View Administrator では、リンク クローン マシンは **Deleting** 状態のままになります。マシンはすでに **Deleting** 状態にあるため、View Administrator で削除コマンドを再起動できません。

原因

この問題は、View Composer データベースに、View LDAP、Active Directory、または vCenter Server の情報と一致しないリンク クローン情報が含まれている場合に発生します。次のようないくつかの状況が、不一致の原因になる場合があります。

- プールが作成された後に、vCenter Server でリンク クローン仮想マシンの名前を手動で変更したために、View Composer と vCenter Server が同じ仮想マシンを異なる名前で参照する。
- ストレージの障害や手動操作により、仮想マシンが vCenter Server から削除される。リンク クローン仮想マシン データは、引き続き View Composer データベース、View LDAP、および Active Directory に存在しています。
- View Administrator からプールが削除されている間に、ネットワーキングなどの障害が発生すると、仮想マシンが vCenter Server に残ったままになる。

デスクトップ プールをプロビジョニングした後で vSphere Client で仮想マシンの名前を変更した場合、仮想マシンの名前を、View に展開されていたときに使用されていた名前に変更します。

他のデータベース情報に不一致がある場合は、SviConfig RemoveSviClone コマンドを使用して、次の項目を削除します。

- View Composer データベースのリンク クローン データベース エントリ
- Active Directory のリンク クローン マシン アカウント
- vCenter Server のリンク クローン仮想マシン

SviConfig ユーティリティは、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。

重要: SviConfig ユーティリティは、経験豊富な View Composer 管理者のみが使用してください。このユーティリティは、View Composer サービスに関連する問題を解決するためのものです。

次の手順を実行します。

- 1 View Composer サービスが動作していることを確認します。
- 2 View Composer コンピュータの Windows コマンド プロンプトから、次の形式で SviConfig RemoveSviClone コマンドを実行します。

```
sviconfig -operation=removesviclone
          -VmName=仮想マシン名
          [-AdminUser=ローカル管理者ユーザー名]
          -AdminPassword=ローカル管理者パスワード
          [-ServerUrl=View Composer サーバ URL]
```

例 :

```
sviconfig -operation=removesviclone -vmname=MyLinkedClone
          -adminuser=Admin -adminpassword=Pass -serverurl=ViewComposerURL
```

VmName パラメータと AdminPassword パラメータは必須です。AdminUser パラメータのデフォルト値は Administrator です。ServerURL パラメータのデフォルト値は https://localhost:18443/SviService/v2_0 です。

View LDAP からの仮想マシン情報の削除に関する詳細は、VMware ナレッジベースの記事「[Manually deleting linked clones or stale virtual desktop entries from the View Composer database in VMware View Manager and VMware Horizon View \(2015112\)](#)」(VMware View Manager および VMware Horizon View の View Composer データベースからリンク クローンまたはステールの仮想デスクトップ エントリを手動で削除する (2081246)) を参照してください。

繰り返し削除と再作成が行われるマシンのトラブルシューティング

View は、エラー状態のリンク クローン マシンと完全クローン マシンを繰り返し削除し再作成することができます。

問題

リンク クローン マシンまたは完全クローン マシンは、エラー状態で作成されると、エラー状態で削除および再作成されます。このサイクルは何度も繰り返されます。

原因

大規模なデスクトップ プールがプロビジョニングされると、1 つ以上の仮想マシンがエラー状態になる場合があります。View の自動リカバリ メカニズムでは、エラー状態の仮想マシンのパワー オンが試行されます。試行が一定回数行われても仮想マシンがパワーオンしない場合、View は仮想マシンを削除します。

View は、プール サイズ要件に従って新しい仮想マシンを作成しますが、多くの場合、マシンの名前は元のマシンと同じになります。新しい仮想マシンが同じエラーでプロビジョニングされる場合、その仮想マシンは削除され、サイクルが繰り返されます。

自動リカバリは、リンク クローン マシンと完全クローン マシンで実行されます。

仮想マシンで自動リカバリの試行が失敗すると、仮想マシンがユーザーに割り当てられていない流動マシンが専用マシンである場合に限り、View はその仮想マシンを削除します。また View は、プールのプロビジョニングが無効になっている場合は仮想マシンを削除しません。

デスクトップ プールの作成に使用された親仮想マシンまたはテンプレートを調べます。仮想マシンでのエラーの原因になる可能性のある仮想マシンまたはゲスト OS のエラーを確認します。

リンク クローンの場合、親仮想マシンのエラーを解決し、新しいスナップショットを作成します。

- エラー状態のマシンが多い場合は、新しいスナップショットまたはテンプレートを使用してプールを再作成します。
- ほとんどのマシンが正常な状態である場合は、View Administrator でデスクトップ プールを選択し、[編集] をクリックします。次に [vCenter 設定] タブを選択し、デフォルトの基本イメージとして新しいスナップショットを選択して、編集内容を保存します。

新しいスナップショットを使用して、新しいリンク クローン マシンが作成されます。

完全クローンの場合は、仮想マシンのエラーを解決し、新しいテンプレートを生成し、プールを再作成します。

QuickPrep のカスタマイズに関する問題のトラブルシューティング

View Composer QuickPrep カスタマイズ スクリプトがさまざまな理由で失敗することがあります。

問題

QuickPrep 同期後スクリプトまたはパワーオフ スクリプトが実行されません。リンク クローンによって、スクリプトが正常に完了したり、失敗したりすることがあります。

原因

QuickPrep スクリプトの失敗の一般的な原因には次のものがあります。

- スクリプトがタイムアウトした
- スクリプトのパスがインタープリタを必要とするスクリプトを参照している
- スクリプトを実行するアカウントに、スクリプト タスクを実行するための十分な権限がない

解決方法

- ◆ カスタマイズ スクリプト ログを調べます。

QuickPrep カスタマイズ情報が Windows temp ディレクトリのログ ファイルに書き込まれます。

`C:\Windows\Temp\vmware-viewcomposer-ga-new.log`

- ◆ スクリプトがタイムアウトしているかどうかを判断します。

View Composer は 20 秒以上かかっているカスタマイズ スクリプトを終了させます。ログ ファイルに、スクリプトが開始されたことを示すメッセージとその後のタイムアウトを示すメッセージが表示されます。

```
2010-02-21 21:05:47,687 [1500] INFO Ready -  
[Ready.cpp, 102] Running the PostSync script:cmd /c  
C:\temp\build\composer.bat  
2010-02-21 21:06:07,348 [1500] FATAL Guest -  
[Guest.cpp, 428] script cmd /c  
C:\temp\build\composer.bat timed out
```

タイムアウトの問題を解決するには、スクリプトのタイムアウトの制限を引き上げて、再実行します。

- ◆ スクリプト パスが有効かどうかを判断します。

スクリプトの実行にインタープリタが必要なスクリプト言語を使用する場合は、スクリプト パスをインタープリタのバイナリで始める必要があります。

たとえば、QuickPrep カスタマイズ スクリプトとして `C:¥¥.vbs` を指定した場合、View Composer Agent はスクリプトを実行できません。次のように、インタープリタのバイナリ パスで始まるパスを指定する必要があります。

`C:\windows\system32\cscript.exe c:\script\myvb.vbs`

- ◆ スクリプトを実行するアカウントに、スクリプト タスクを実行するための適切な権限があるかどうかを判断します。

QuickPrep は、VMware View Composer Guest Agent Server サービスの実行が構成されたアカウントでスクリプトを実行します。デフォルトでは、このアカウントはローカル システムです。

このログオン アカウントは変更しないでください。変更すると、リンク クローンが起動しなくなります。

未使用の View Composer レプリカの検索と保護解除

特定の条件下では、View Composer レプリカが vCenter Server と関連付けられたリンク クローンを保持しなくなってもそのまま vCenter Server に残る場合があります。

問題

未使用レプリカが vCenter Server フォルダにそのまま残っています。vSphere Client を使用してもレプリカを削除することができません。

原因

View Composer の操作時にネットワークが停止したか、または適切な View コマンド使用せずに関連のリンク クローンを vSphere から直接削除した場合、vCenter Server に未使用レプリカが残る可能性があります。

レプリカは、vCenter Server 内の保護されたエンティティです。通常の vCenter Server または vSphere Client 管理コマンドではそれらを削除できません。

SviConfig FindUnusedReplica コマンドを使用して、指定したフォルダ内のレプリカを検索します。-Move パラメータを使用すると、レプリカを別のフォルダに移動することができます。-Move パラメータにより、移動前に未使用レプリカの保護が解除されます。

重要: SviConfig ユーティリティは、経験豊富な View Composer 管理者のみが使用してください。このユーティリティは、View Composer サービスに関連する問題を解決するためのものです。

SviConfig ユーティリティは、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。

開始する前に、レプリカと関連付けられたリンク クローンが存在しないことを確認します。

SviConfig FindUnusedReplica パラメータについて理解しておく必要があります。

- DsnName。データベースへの接続に使用する DSN。
- UserName。データベースへの接続に使用するユーザー名。このパラメータを指定しない場合、Windows 認証が使用されます。
- Password(パスワード)。データベースに接続するユーザーのパスワード。このパラメータが指定されておらず、Windows 認証が使用されない場合、後でパスワードの入力を求められます。
- ReplicaFolder。レプリカ フォルダの名前。ルート フォルダには空の文字列を使用します。デフォルト値は VMwareViewComposerReplicaFolder です。

- **UnusedReplicaFolder**。すべての未使用レプリカを含めるフォルダの名前。デフォルト値は **UnusedViewComposerReplicaFolder** です。Move パラメータを使用する際にこのパラメータを使用してターゲット フォルダを指定します。
- **OutputDir**。unused-replica-*.txt ファイルに保存される、未使用レプリカのリストを示す出力ディレクトリの名前が収集されます。デフォルト値は現在のワーキング ディレクトリです。
- **Move**。未使用レプリカ仮想マシンの保護を解除し、それらを指定したフォルダに移動するかどうかを決定します。UnusedReplicaFolder パラメータでは、ターゲット フォルダが指定されます。Move パラメータのデフォルト値は **false** です。

DsnName、Username、Password の各パラメータが必要です。DsnName は空の文字列にはできません。

次の手順を実行します。

- 1 View Composer サービスを停止します。
- 2 View Composer コンピュータの Windows コマンド プロンプトから、次の形式で SviConfig FindUnusedReplica コマンドを実行します。

```
sviconfig -operation=findunusedreplica
          -DsnName=DSN の名前
          -Username=データベース管理者ユーザー名
          -Password=データベース管理者パスワード
          [-ReplicaFolder=レプリカ フォルダ名]
          [-UnusedReplicaFolder=未使用のレプリカ フォルダ名]
          [-OutputDir=出力ファイル ディレクトリ]
          [-Move=true or false]
```

例：

```
sviconfig -operation=FindUnusedReplica -DsnName=SVI
          -Username=SVIUser -Password=1234 -Move=True
```

- 3 View Composer サービスを再起動します。
- 4 (オプション) レプリカを新しいフォルダに移動したら、vCenter Server からレプリカ仮想マシンを削除します。

View Composer のプロビジョニング エラー

View Composer でリンク クローン マシンのプロビジョニングまたは再構成が行われてエラーが発生する場合、エラー コードに障害の原因が示されます。エラー コードは、View Administrator のマシン ステータス列に表示されます。

表 19-1. View Composer のプロビジョニング エラー に、View Composer のプロビジョニング エラー コードを示します。

この表には、View Composer および QuickPrep によるカスタマイズに関連するエラーが一覧表示されています。View 接続サーバ、および他の View コンポーネントで、マシンのプロビジョニングに影響を及ぼす可能性のあるその他のエラーが発生することがあります。

表 19-1. View Composer のプロビジョニング エラー

エラー	説明
0	<p>ポリシーが正常に適用されました。</p> <p>注: 結果コード 0 は View Administrator に表示されません。View Composer のドメイン外で View エラーが発生した場合を除き、リンク クローン マシンは作動可能状態に移行します。この結果コードは、完全性を確保するために含められています。</p>
1	コンピュータ名の設定に失敗しました。
2	ユーザー プロファイルを View Composer 通常ディスクにリダイレクトしようとして失敗しました。
3	コンピュータのドメイン アカウント パスワードの設定に失敗しました。
4	ユーザーのプロファイル キーのバックアップに失敗しました。ユーザーが、再構成操作後に次回このリンク クローン マシンにログインすると、OS によってこのユーザーの新しいプロファイル ディレクトリが作成されます。新しいプロファイルが作成されるため、ユーザーは以前のプロファイル データを表示できなくなります。
5	ユーザーのプロファイルの復元に失敗しました。プロファイルの状態が定義されていないため、ユーザーがこの状態でマシンにログインしないようにする必要があります。
6	<p>他のエラー コードに該当しないエラー。ゲスト OS 内の View Composer Agent のログ ファイルで、これらのエラーの原因に関する詳細情報が提供されることがあります。</p> <p>たとえば、Windows プラグ アンド プレイ (PnP) タイムアウトによってこのエラー コードが生成されます。この場合、View Composer は PnP サービスによってリンク クローン仮想マシン用の新しいボリュームがインストールされるまで待機し、その後タイムアウトになります。</p> <p>プールの構成に応じ、PnP によって最大 3 つのディスクがマウントされます。</p> <ul style="list-style-type: none"> ■ View Composer 通常ディスク ■ ゲスト OS の一時ファイルおよびページング ファイルをリダイレクトするための読み取り専用ディスク ■ QuickPrep の構成およびその他の OS 関連データを格納する内部ディスク。このディスクには常にリンク クローンが構成されます。 <p>タイムアウトの長さは 10 分です。PnP によるディスクのマウントが 10 分以内に終了しないと、エラー コード 6 が生成されて View Composer が機能停止します。</p>
7	リンク クローンに接続されている View Composer 通常ディスクが多すぎます。1 つのクローンに接続できる View Composer 通常ディスクは 3 つまでです。
8	プールの作成時に選択されたデータストアに通常ディスクをマウントできませんでした。
9	View Composer が破棄可能データのファイルを読み取り専用ディスクにリダイレクトできませんでした。ページング ファイルまたは一時ファイルのフォルダがリダイレクトされませんでした。
10	指定された内部ディスク上で View Composer が QuickPrep の構成ポリシー ファイルを検出できません。
12	View Composer が QuickPrep の構成ポリシー ファイルおよびその他の OS 関連データを含む内部ディスクを検出できません。
13	複数の通常ディスクが Windows ユーザー プロファイルをリダイレクトするように構成されています。
14	View Composer が内部ディスクのマウント解除に失敗しました。
15	View Composer が構成ポリシー ファイルから読み取ったコンピュータ名が、リンク クローンの最初のパワーオン後、現在のシステム名と一致しません。
16	ゲスト OS のボリューム ライセンスがアクティブになっていないため、View Composer Agent が起動しませんでした。
17	View Composer Agent が起動しませんでした。エージェントは Sysprep が起動するまで待機している間にタイムアウトになりました。
18	View Composer Agent がカスタマイズ中にリンク クローン仮想マシンをドメインに結合できませんでした。
19	View Composer Agent は、同期後スクリプトの実行に失敗しました。

エラー	説明
20	View Composer Agent は、マシン パスワード同期イベントの処理に失敗しました。 このエラーは一時的なものである場合があります。リンク クローンがドメインに参加しているのであれば、パスワードに問題はありません。 クローンがドメインに参加できない場合には、エラーが発生した前に実行した操作を再度行ってください。クローンを再起動している場合には、再起動をもう一度行ってください。クローンを更新している場合には、更新をもう一度行ってください。それでもクローンがドメインに参加できない場合には、クローンを再構成してください。
21	View Composer Agent は、システム ディスパーザブル ディスクのマウントに失敗しました。
22	View Composer Agent は、View Composer 通常ディスクのマウントに失敗しました。

ネットワーク接続に関する問題のトラブルシューティング

マシン、Horizon Client デバイス、View 接続サーバ インスタンスとのネットワーク接続に関する問題を診断および解決するために、さまざまな手順を使用できます。

マシンと View 接続サーバ インスタンスの接続の問題

マシンと View 接続サーバ インスタンスの接続に関して、問題が発生することがあります。

問題

マシンと View 接続サーバ インスタンスとの接続に失敗した場合、イベント データベースに次のいずれかのメッセージが表示されます。

- マシン *Machine_Name* のプロビジョニング エラーが発生しました:Horizon Agent と接続サーバとのネットワーク通信がないことによるカスタマイズ エラー
- Horizon Agent のネットワークの問題により、プール *Desktop_ID* でプロビジョニング エラーが発生しました
- ユーザー *User_Display_Name* のプール *Desktop_ID* から開始できません:*Protocol* を使用してマシン *MachineName* に接続できませんでした

原因

マシンと View 接続サーバ インスタンスとの接続の問題は、さまざまな理由によって発生する可能性があります。

- マシンでの、View 接続サーバ ホストの DNS 名の参照エラー。
- JMS、RDP、または AJP13 通信用のポートがファイアウォール ルールによってブロックされている。
- View 接続サーバ ホストでの JMS ルータの障害。

解決方法

- ◆ マシンのコマンド プロンプトで、nslookup コマンドを入力します。

```
nslookup CS_FQDN
```

`CS_FQDN`は、View 接続サーバ ホストの完全修飾ドメイン名 (FQDN) です。このコマンドによって View 接続サーバ ホストの IP アドレスが返されない場合は、一般的なネットワーク トラブルシューティング テクニックを適用して DNS の構成を修正します。

- ◆ マシンのコマンド プロンプトで `telnet` コマンドを入力して、TCP ポート 4001 が機能していることを確認します。これは、Horizon Agent が View 接続サーバ ホストとの JMS 通信を確立するために使用するポートです。

```
telnet CS_FQDN 4001
```

`telnet` 接続が確立される場合は、JMS のネットワーク接続が機能しています。

- ◆ DMZ にセキュリティ サーバが展開されている場合は、TCP ポート 3389 でセキュリティ サーバと仮想マシンとの RDP 接続を許可する例外ルールが内部ファイアウォールで構成されていることを確認します。
- ◆ 安全な接続がバイパスされている場合は、クライアントが TCP ポート 3389 で仮想マシンへの直接 RDP 接続を確立すること、または TCP ポート 4172 および UDP ポート 4172 で仮想マシンへの直接 PColP 接続を確立することがファイアウォール ルールで許可されていることを確認します。
- ◆ TCP ポート 4001 (JMS) および TCP ポート 8009 (AJP13) で各セキュリティ サーバとそれに関連付けられた View 接続サーバ ホストとの接続を許可する例外ルールが内部ファイアウォールで構成されていることを確認します。

Horizon Client と PColP Secure Gateway の接続の問題

PColP を介して通信する外部ユーザーを認証するように PColP Secure Gateway が構成されている場合は、Horizon Client とセキュリティ サーバ ホストまたは View 接続サーバ ホストとの接続に関して、問題が発生することがあります。

問題

PColP を使用するクライアントが View デスクトップに接続または表示できません。セキュリティ サーバまたは View 接続サーバ インスタンスへの最初のログインは成功しますが、ユーザーが View デスクトップを選択すると接続が失敗します。この問題は、PColP Secure Gateway がセキュリティ サーバ ホストまたは View 接続サーバ ホスト上に構成されている場合に発生します。

注: 通常、PColP Secure Gateway はセキュリティ サーバ上で活用されます。外部クライアントが View 接続サーバ ホストに直接接続するネットワーク構成では、PColP Secure Gateway も View 接続サーバ上に構成できます。

原因

PColP Secure Gateway との接続の問題は、さまざまな理由で発生する可能性があります。

- Windows Firewall によって、PColP Secure Gateway に必要なポートが閉じられている。
- PColP Secure Gateway がセキュリティ サーバまたは View 接続サーバ インスタンスで有効になっていない。
- PColP 外部 URL 設定が正しく構成されていない。この設定は、クライアントがインターネットを介してアクセスできる外部 IP アドレスとして指定する必要があります。

- PCoIP 外部 URL、安全なトンネルの外部 URL、Blast 外部 URL、および他のアドレスは、異なるセキュリティ サーバまたは View 接続サーバ ホストを指すように構成されます。これらのアドレスをセキュリティ サーバまたは View 接続サーバ ホストを構成するとき、すべてのアドレスでクライアント システムが現在のホストに到達する必要がある場合があります。
- クライアントが、PCoIP Secure Gateway に必要なポートを閉じている外部 Web プロキシ経由で接続している。たとえば、ホテル ネットワーク接続やパブリック ワイヤレス接続での Web プロキシは必要なポートをブロックする可能性があります。
- PCoIP Secure Gateway が構成されているセキュリティ サーバと対になっている View 接続サーバ インスタンスのバージョンが View 4.5 以前である。セキュリティ サーバおよびそれと対になっている View 接続サーバ インスタンスのバージョンは View 4.6 以降である必要があります。

解決方法

- ◆ セキュリティ サーバ ホストまたは View 接続サーバ ホストのファイアウォール上で、次のネットワーク ポートが開いていることを確認します。

ポート	説明
TCP 4172	Horizon Client からセキュリティ サーバ ホストまたは View 接続サーバ ホスト。
UDP 4172	Horizon Client とセキュリティ サーバ ホストまたは View 接続サーバ ホスト間（双方向）。
TCP 4172	セキュリティ サーバ ホストまたは View 接続サーバ ホストから View デスクトップ
UDP 4172	セキュリティ サーバ ホストまたは View 接続サーバ ホストと View デスクトップ間（双方向）

- ◆ View Administrator で、PCoIP セキュア ゲートウェイが有効であることを確認してください。
 - a [View 構成] - [サーバ] をクリックします。
 - b [接続サーバ] タブで View 接続サーバ インスタンスを選択し、[編集] をクリックします。
 - c [マシンへの PCoIP 接続に PCoIP Secure Gateway を使用する] を選択します。
デフォルトでは、PCoIP Secure Gateway は無効になっています。
 - d [OK] をクリックします。
- ◆ View Administrator で、PCoIP 外部 URL が正しく構成されていることを確認してください。
 - a [View 構成] - [サーバ] をクリックします。
 - b 構成するホストを選択します。
 - ユーザーがセキュリティ サーバで PCoIP セキュア ゲートウェイに接続する場合、[セキュリティ サーバ] タブでセキュリティ サーバを選択します。
 - ユーザーが View 接続サーバ インスタンスで PCoIP セキュア ゲートウェイに接続する場合、[接続サーバ] タブでインスタンスを選択します。
 - c [編集] をクリックします。

- d [PCoIP 外部 URL] テキスト ボックスで、URL に、クライアントがインターネットを介してアクセスできるセキュリティ サーバまたは View 接続サーバホストの外部 IP アドレスが含まれていることを確認します。
- ポート 4172 を指定します。プロトコル名を含めないでください。

例: **10.20.30.40:4172**

- e このダイアログのすべてのアドレスでクライアント システムがこのホストに到達できることを確認します。
- [セキュリティ サーバ設定を編集] 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必要があります。[View 接続サーバ設定を編集] 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 View 接続サーバ インスタンスに到達できる必要があります。

- f [OK] をクリックします。

ユーザーが PCoIP Secure Gateway に接続する基盤となる、各セキュリティ サーバおよび View 接続サーバ インスタンスでこれらの手順を繰り返します。

- ◆ ユーザーがネットワークの外部にある Web プロキシ経由で接続していて、そのプロキシが必要なポートをブロックしている場合は、ユーザーにネットワークの別の場所から接続するように指示します。

マシンと View 接続サーバ インスタンスの接続の問題

マシンと View 接続サーバ インスタンスの接続に関して、問題が発生することがあります。

問題

マシンと View 接続サーバ インスタンスとの接続に失敗した場合、イベント データベースに次のいずれかのメッセージが表示されます。

- マシン *Machine_Name* のプロビジョニング エラーが発生しました: Horizon Agent と接続サーバとのネットワーク通信がないことによるカスタマイズ エラー
- Horizon Agent のネットワークの問題により、プール *Desktop_ID* でプロビジョニング エラーが発生しました
- ユーザー *User_Display_Name* のプール *Desktop_ID* から開始できません: *Protocol* を使用してマシン *MachineName* に接続できませんでした

原因

マシンと View 接続サーバ インスタンスとの接続の問題は、さまざまな理由によって発生する可能性があります。

- マシンでの、View 接続サーバ ホストの DNS 名の参照エラー。
- JMS、RDP、または AJP13 通信用のポートがファイアウォール ルールによってブロックされている。
- View 接続サーバ ホストでの JMS ルータの障害。

解決方法

- ◆ マシンのコマンド プロンプトで、nslookup コマンドを入力します。

```
nslookup CS_FQDN
```

`CS_FQDN`は、View 接続サーバ ホストの完全修飾ドメイン名 (FQDN) です。このコマンドによって View 接続サーバ ホストの IP アドレスが返されない場合は、一般的なネットワーク トラブルシューティング テクニックを適用して DNS の構成を修正します。

- ◆ マシンのコマンド プロンプトで `telnet` コマンドを入力して、TCP ポート 4001 が機能していることを確認します。これは、Horizon Agent が View 接続サーバ ホストとの JMS 通信を確立するために使用するポートです。

```
telnet CS_FQDN 4001
```

`telnet` 接続が確立される場合は、JMS のネットワーク接続が機能しています。

- ◆ DMZ にセキュリティ サーバが展開されている場合は、TCP ポート 3389 でセキュリティ サーバと仮想マシンとの RDP 接続を許可する例外ルールが内部ファイアウォールで構成されていることを確認します。
- ◆ 安全な接続がバイパスされている場合は、クライアントが TCP ポート 3389 で仮想マシンへの直接 RDP 接続を確立すること、または TCP ポート 4172 および UDP ポート 4172 で仮想マシンへの直接 PCoIP 接続を確立することがファイアウォール ルールで許可されていることを確認します。
- ◆ TCP ポート 4001 (JMS) および TCP ポート 8009 (AJP13) で各セキュリティ サーバとそれに関連付けられた View 接続サーバ ホストとの接続を許可する例外ルールが内部ファイアウォールで構成されていることを確認します。

クローン マシンへの不正な IP アドレス割り当てによる接続の問題

クローン マシンが固定 IP アドレスを使用している場合、それらに接続できないことがあります。

問題

Horizon Client を使用してクローン マシンに接続することはできません。

原因

DHCP を使用して IP アドレスを取得するのではなく固定 IP アドレスを使用するように、クローン マシンが不正に構成されています。

解決方法

- 1 vCenter Server のデスクトップ プールのテンプレートが、DHCP を使用してマシンに IP アドレスを割り当てるように構成されていることを確認します。
- 2 vSphere Web Client で、デスクトップ プールから仮想マシンのクローンを手動で 1 つ作成し、その IP アドレスが DHCP から正しく取得されることを確認します。

USB リダイレクトに関する問題のトラブルシューティング

Horizon Client で USB リダイレクトに関する各種の問題が発生することがあります。

問題

Horizon Client の USB リダイレクトで、ローカル デバイスをリモート デスクトップで使用可能にできなかったり、Horizon Client で一部のデバイスがリダイレクトに使用できるように表示されなかったりします。

原因

USB リダイレクトが正常に機能しない場合、または予想どおりに機能しない場合、可能性のある原因は次のとおりです。

- デバイスが複合 USB デバイスであり、含まれるデバイスの 1 つがデフォルトでブロックされています。たとえばマウスを含む読み上げデバイスはデフォルトでブロックされています。これはマウス デバイスがデフォルトでブロックされているためです。この問題を解決するには、[複合 USB デバイスのデバイス分割ポリシー設定の構成](#)を参照してください。
- USB リダイレクトは、リモート デスクトップおよびアプリケーションが展開されている Windows Server 2008 RDS ホストではサポートされません。View Agent 6.1 以降では、Windows Server 2012 RDS ホストで USB リダイレクトがサポートされますが、サポート対象は USB ストレージ デバイスのみです。USB リダイレクトは、単一ユーザー デスクトップとして使用されている Windows Server 2008 R2 および Windows Server 2012 R2 システムでサポートされます。
- RDS デスクトップおよびアプリケーションでは、USB フラッシュ ドライブとハード ディスクのみがサポートされます。その他のタイプの USB デバイスや、セキュリティ ストレージ ドライブや USB CD-ROM などのその他のタイプの USB ストレージ デバイスを RDS デスクトップやアプリケーションにリダイレクトすることはできません。
- Web カメラはリダイレクトの対象としてサポートされていません。
- USB オーディオ デバイスのリダイレクトは、ネットワークの状態に依存し、信頼できません。一部のデバイスでは、アイドル状態のときでさえ、高いデータ スループットが必要です。
- ブート デバイスでは USB リダイレクトがサポートされていません。USB デバイスからブートする Windows システムで Horizon Client を実行しており、このデバイスをリモート デスクトップにリダイレクトした場合、ローカル オペレーティング システムが応答しなかったり使用できなかったりすることがあります。<http://kb.vmware.com/kb/1021409> を参照してください。
- Windows 版 Horizon Client では、デフォルトで、キーボード、マウス、スマート カード、オーディオ出力デバイスをリダイレクト対象として選択できません。<http://kb.vmware.com/kb/1011600> を参照してください。
- RDP は、コンソール セッションの USB HID またはスマート カード リーダのリダイレクトをサポートしていません。<http://kb.vmware.com/kb/1011600> を参照してください。
- Windows Mobile デバイス センターにより、RDP セッションの USB デバイスのリダイレクトが妨げられることがあります。<http://kb.vmware.com/kb/1019205> を参照してください。
- 一部の USB HID では、マウス ポインタの位置を更新するように、仮想マシンを構成する必要があります。<http://kb.vmware.com/kb/1022076> を参照してください。
- 一部のオーディオ デバイスでは、ポリシー設定またはレジストリ設定を変更する必要がある場合があります。<http://kb.vmware.com/kb/1023868> を参照してください。
- ネットワークのレイテンシーが原因で、デバイスの相互作用が低速になったり、アプリケーションがフリーズしているように見えることがあります。これはアプリケーションがローカル デバイスと相互作用するように設計されているからです。非常に大容量の USB ディスク ドライブは、Windows エクスプローラに表示されるまでに数分かかることがあります。

- FAT32 ファイル システムでフォーマットされた USB フラッシュ カードはロードが遅くなります。<http://kb.vmware.com/kb/1022836> を参照してください。
- リモート デスクトップまたはアプリケーションに接続する前に、ローカル システムでプロセスまたはサービスがデバイスを開いていた。
- リダイレクトされた USB デバイスは、デスクトップまたはアプリケーションにそのデバイスが使用可能であることが表示されている場合でも、デスクトップまたはアプリケーション セッションを再接続すると、動作が停止します。
- View Administrator で USB リダイレクトが無効になっている。
- ゲスト上で、USB リダイレクト ドライバが存在しないか、無効になっている。

解決方法

- ◆ PCoIP が使用可能な場合は、RDP の代わりにプロトコルとして使用します。
- ◆ 一時的な切断後に、リダイレクトされたデバイスが使用できないままであるか、動作を停止した場合、デバイスを取り外し、再度接続して、リダイレクトを再試行してください。
- ◆ View Administrator で、[ポリシー] - [グローバル ポリシー] に移動して、[View ポリシー] で USB アクセスが [許可] に設定されていることを確認します。
- ◆ ゲストのログでクラス `ws_vhub` のエントリの有無、クライアントのログでクラス `vmware-view-usbd` のエントリの有無を調べます。

ユーザーが管理者でない場合、または USB リダイレクト ドライバがインストールされていないか、機能していない場合には、これらのクラスのエントリがログに書き込まれます。これらのログの場所については、[ログ ファイルを使用してのトラブルシューティングと USB デバイス ID の確認](#) を参照してください。

- ◆ ゲスト上でデバイス マネージャを開き、[ユニバーサル シリアル バス コントローラ] を展開して、VMware View 仮想 USB ホスト コントローラのドライバおよび VMware View 仮想 USB ハブのドライバが表示されない場合はそれらを再インストールし、無効になっている場合は再度有効にします。

資格のないユーザーのマシンおよびポリシーの管理

資格が削除されたユーザーに割り当てられているマシン、および資格のないユーザーに適用されているポリシーを表示できます。

資格のないユーザーが組織を完全に離れたり、長期間にわたってそのユーザーのアカウントをサスペンドしている場合があります。こうしたユーザーにはマシンが割り当てられていますが、マシン プールを使用する資格はありません。

-O または -P オプションを指定して `vdadmin` コマンドを使用し、資格のないマシンおよびポリシーを表示することもできます。詳細については、『View 管理ガイド』を参照してください。

手順

- 1 View Administrator で、[リソース] - [マシン] を選択します。
- 2 [その他のコマンド] - [資格のないマシンの表示] を選択します。

- 3 資格のないユーザーに対するマシン割り当てを削除します。
- 4 [その他のコマンド] - [資格のないマシンを表示] または [その他のコマンド] - [資格のないポリシーを表示] を適宜選択します。
- 5 資格のないユーザーに適用されているポリシーを変更または削除します。

ViewDbChk コマンドを使用したデータベース不整合の解決

ViewDbChk コマンドを使用して、自動デスクトップ プールにあるデスクトップ仮想マシンおよび自動ファームにある RDS ホストに関する情報を保管するデータベースの不整合を解決できます。

View 環境では、デスクトップ仮想マシンと自動ファームの RDS ホストの情報は、次の場所に保管されます。

- LDAP データベース
- vCenter Server データベース
- View Composer リンク クローン マシンのみ : View Composer データベース

通常、View Administrator を使用してデスクトップ仮想マシンや RDS ホストを削除またはリセットすることで、プロビジョニングまたは他の操作中に発生するエラーからリカバリできます。まれに、エラー状態になっているマシンに関するさまざまなデータベース上の情報が不整合になり、View Administrator を使用してもエラーからリカバリできない場合があります。次のいずれかの兆候が見られる可能性があります。

- 次のエラー メッセージが表示されてプロビジョニングが失敗します。入力仕様のある仮想マシンはすでに存在しています。
- 次のエラー メッセージが表示されてデスクトップ プールの再構築が失敗します Desktop Composer の障害: 入力仕様のある仮想マシンはすでに存在しています
- View Administrator が、デスクトップ マシンや RDS ホストが削除中状態のままであることを示します。
- デスクトップ プールや自動ファームは削除できません。
- デスクトップ マシンや RDS ホストは削除できません。
- View Administrator の [インベントリ] タブで、デスクトップ マシンや RDS ホストのステータスが欠落しています。

データベース不整合によってデスクトップ マシンや RDS ホストがリカバリ不可能なエラー状態になるか、View Administrator のタスクを正常に完了できない状況で、ViewDbChk コマンドを使用して不整合を解決できます。

ViewDbChk コマンドには次の特徴があります。

- View スタンダード サーバまたは View レプリカ サーバをインストールすると、ViewDbChk は自動的にインストールされます。View セキュリティ サーバをインストールするときに、ユーティリティはインストールされません。
- ViewDbChk は、Windows コマンド プロンプトまたはスクリプトから実行できるコマンドです。
- ViewDbChk は自動ファームとフル仮想マシンの自動デスクトップ プールとともに、View Composer リンク クローンをサポートしています。

- マシンを削除する場合、ViewDbChk はマシンでヘルス チェックを実行し、マシンが正常であるかどうかをさらに確認するプロンプトを表示します。
- ViewDbChk はエラーのある、または不完全な LDAP エントリを削除できます。
- ViewDbChk は国際化文字セットを使用した入力および出力をサポートします。
- ViewDbChk はユーザー データを削除しません。フル デスクトップ仮想マシンの場合、ViewDbChk はインベントリから仮想マシンを削除しますが、ディスクからは削除しません。リンククローン デスクトップ仮想マシンの場合、ViewDbChk は仮想マシンを削除し、VMFS データストアの場合はルート フォルダに、Virtual SAN および仮想ボリューム データストアの場合は archiveUDD という名前のサブフォルダに、ユーザー ディスクをアーカイブします。
- ViewDbChk は、非管理対象のデスクトップ マシンや手動ファームの RDS ホストをサポートしません。

ViewDbChk 構文

```
ViewDbChk --findDesktop --desktopName <desktop pool or farm name> [--verbose]

ViewDbChk --enableDesktop --desktopName <desktop pool or farm name> [--verbose]

ViewDbChk --disableDesktop --desktopName <desktop pool or farm name> [--verbose]

ViewDbChk --findMachine --desktopName <desktop pool or farm name> --machineName <machine name> [--verbose]

ViewDbChk --removeMachine --machineName <machine name> [--desktopName <desktop pool or farm name>] [--force] [--noErrorCheck] [--verbose]

ViewDbChk --scanMachines [--desktopName <desktop pool or farm name>] [--limit <maximum deletes>] [--force] [--verbose]

ViewDbChk --help [--commandName] [--verbose]
```

ViewDbChk パラメータ

パラメータ	説明
--findDesktop	デスクトップ プールやファームを検索します。
--enableDesktop	デスクトップ プールやファームを有効にします。
--disableDesktop	デスクトップ プールやファームを無効にします。
--findMachine	マシンを検出します。
--removeMachine	デスクトップ プールまたはファームからマシンを削除します。マシンを削除する前に、ViewDbChk はユーザーにデスクトップ プールまたはファームを無効にするように求めます。マシンを削除した後、ViewDbChk はユーザーにデスクトップ プールやファームを再度有効にするように求めます。
--scanMachines	エラー状態またはクローンエラー状態のマシン、または仮想マシンが欠落しているマシンを検出し、デスクトップ プールまたはファームごとにグループ化して問題のあるマシンをリストし、マシンを削除するオプションを提供します。マシンを削除する前に、ViewDbChk はユーザーにデスクトップ プールまたはファームを無効にするように求めます。デスクトップ プールまたはファーム内でエラーを生じたすべてのマシンを削除した後、ViewDbChk はユーザーにデスクトップ プールまたはファームを再度有効にするように求めます。

パラメータ	説明
--help	ViewDbChk の構文を表示します。
--desktopName <desktop name>	デスクトップ プールやファームの名前を指定します。
--machineName <machine name>	マシン名を指定します。
--limit <maximum deletes>	ViewDbChk が削除できるマシンの数を制限します。 デフォルトは 1 です。
--force	ユーザーの確認なしで強制的にマシンを削除します。
--noErrorCheck	エラーを生じていないマシンを強制的に削除します。
--verbose	詳細ログを有効にします。

注: すべてのパラメータ名は大文字と小文字が区別されます。

ViewDbChk の使用例

lc-pool2-2 という名前のデスクトップ マシンがエラー状態になっており、View Administrator を使用してそれを削除することはできません。 ViewDbChk を使用して View 環境からそれを削除します。

```
C:\>viewdbchk --removeMachine --machineName lc-pool2-2
Looking for desktop pool "lc-pool2" in LDAP...
  Desktop Pool Name: lc-pool2
  Desktop Pool Type: AUTO_LC_TYPE
  VM Folder: /vdi/vm/lc-pool2/
  Desktop Pool Disabled: false
  Desktop Pool Provisioning Enabled: true
Looking for machine "/vdi/vm/lc-pool2/lc-pool2-2" in vCenter...
  Connecting to vCenter "https://10.133.17.3:443/sdk". This may take some time...
Checking connectivity...
  Connecting to View Composer "https://10.133.17.3:18443". This may take some time...
The desktop pool "lc-pool2" must be disabled before proceeding. Do you want to disable the desktop
pool? (yes/no):yes
Found machine "lc-pool2-2"
  VM Name: lc-pool2-2
  Creation Date: 1/25/15 1:20:26 PM PST
  MOID: vm-236
  Clone Id: b12a9ed2-8535-44ee-a9d6-6c9b5cf6f878
  VM Folder: /vdi/vm/lc-pool2/lc-pool2-2
  VM State: ERROR
Do you want to remove the desktop machine "lc-pool2-2"? (yes/no):yes
Shutting down VM "/vdi/vm/lc-pool2/lc-pool2-2"...
Archiving persistent disks...
Destroying View Composer clone "b12a9ed2-8535-44ee-a9d6-6c9b5cf6f878"...
Removing ThinApp entitlements for machine "/vdi/vm/lc-pool2/lc-pool2-2"...
Removing machine "/vdi/vm/lc-pool2/lc-pool2-2" from LDAP...
Running delete VM scripts for machine "/vdi/vm/lc-pool2/lc-pool2-2"...
Do you want to enable the desktop pool "lc-pool2"? (yes/no):yes
```

トラブルシューティングの追加情報

トラブルシューティングの追加情報は、VMware ナレッジベースの記事に掲載されています。

VMware ナレッジベース (KB) は、VMware 製品の新しいトラブルシューティング情報が追加されて継続的に更新されています。

View のトラブルシューティングの詳細については、VMware KB の Web サイトで利用可能な KB の記事を参照してください。

<http://kb.vmware.com/selfservice/microsites/microsite.do>