

# Horizon Console の管理

2019 年 7 月

VMware Horizon 7 7.9



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](mailto:docfeedback@vmware.com) までお送りください。

VMware, Inc.  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://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](http://www.vmware.com/jp)

Copyright © 2018-2019 VMware, Inc. All rights reserved. [著作権および商標情報](#)。

# 目次

1	VMware Horizon Console の管理	10
2	VMware Horizon Console の使用	11
	サポートされている Horizon 7 機能	11
	Horizon Console を使用する利点	13
	Horizon Console のインストールと構成	13
	Horizon Console へのログイン	13
3	Horizon Console での Horizon Connection Server の設定	15
	Horizon Console での vCenter Server と Horizon Composer の設定	15
	Horizon Composer Active Directory 操作のユーザー アカウントの作成	15
	Horizon Console での製品のライセンス キーのインストール	16
	Horizon Console での vCenter Server インスタンスの Horizon 7 への追加	17
	Horizon Composer の設定	19
	Horizon Composer ドメインの設定	20
	Horizon Console でのインスタント クローンのドメイン管理者の追加	21
	vSphere でリンク クローン仮想マシンのディスク領域を再利用できるようにする	22
	vCenter Server の Horizon Storage Accelerator の設定	23
	vCenter Server と Horizon Composer の同時操作の制限数	25
	リモート デスクトップ ログオン ストームをサポートするための同時電源操作レートの設定	26
	デフォルトの TLS 証明書のサムプリントを受け入れる	27
	Horizon 7 からの vCenter Server インスタンスの削除	28
	Horizon 7 からの Horizon Composer の削除	28
	競合している vCenter Server の一意の ID	29
	Horizon Console での Horizon Connection Server のバックアップ	30
	Horizon Console でのクライアント セッションの設定	30
	Horizon Console でのクライアント セッションのグローバル設定	30
	Horizon Console のクライアント セッションと接続のグローバル セキュリティ設定	33
	Horizon Console での Horizon Connection Server の無効化または有効化	34
	Horizon Connection Server インスタンスの外部 URL の編集	35
	Horizon Console でのゲートウェイの登録	36
4	スマート カード認証の設定	37
	スマート カードを使用したログイン	37
	Horizon 接続サーバでのスマート カード認証の構成	38
	証明機関の証明書の取得	39
	Windows からの CA 証明書の取得	39
	サーバ信頼ストア ファイルへの CA 証明書の追加	40

Horizon Connection Server の構成プロパティの変更	41
Horizon Console でのスマート カードの設定	42
サードパーティ 製ソリューションでのスマート カード認証の設定	45
スマート カード認証用の Active Directory を準備する	45
スマート カード ユーザーの UPN を追加する	46
Enterprise NTAAuth ストアにルート証明書を追加する	46
信頼されたルート証明機関へのルート証明書の追加	47
中間証明機関への中間証明書の追加	47
Horizon Console でのスマート カード認証の設定の検証	48
スマート カードでの証明書失効チェックの使用	50
CRL チェックを使用したログイン	50
OCSP による証明書失効チェックを使用したログイン	51
CRL チェックの構成	51
OCSP による証明書失効チェックの構成	52
スマート カードでの証明書失効チェックのプロパティ	52

## 5 他のタイプのユーザー認証の設定 54

2 要素認証の使用	54
2 要素認証を用いたログイン	55
Horizon Console での 2 要素認証の有効化	55
RSA SecureID アクセス拒否のトラブルシューティング	57
RADIUS アクセス拒否のトラブルシューティング	58
SAML 認証の使用	58
VMware Identity Manager 統合用の SAML 認証の使用	59
Horizon Console での SAML 認証子の設定	60
VMware Identity Manager でのプロキシ サポートの設定	62
Connection Server でのサービス プロバイダ メタデータの有効期間の変更	62
Connection Server をサービス プロバイダとして使用可能にするための SAML メタデータの生成	63
複数の動的 SAML 認証子の応答時間に関する注意事項	64
Horizon Console での Workspace ONE アクセス ポリシーの設定	64
バイオメトリクス認証の構成	65

## 6 ユーザーとグループの認証 66

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	66
リモート アクセスの設定	66
非認証アクセスの構成	67
非認証アクセス ユーザーの作成	67
公開アプリケーションに対する非認証アクセス ユーザーへの資格付与	68
非認証アクセス ユーザーの削除	69
Horizon Client からの非認証アクセス	69

## 7 Horizon Console でのロールベースの委任管理の構成 71

ロールと権限の概要 71

Horizon Console でのアクセス グループを使用したプールおよびファーム管理の委任 72

異なるアクセス グループの異なる管理者 73

同じアクセス グループの異なる管理者 73

権限の概要 73

管理者の管理 74

Horizon Console での管理者の作成 75

Horizon Console での管理者の削除 76

権限の管理と確認 76

Horizon Console での権限の追加 76

Horizon Console での権限の削除 77

Horizon Console での権限の確認 78

アクセス グループの管理と確認 78

Horizon Console でアクセス グループを追加する 79

Horizon Console での別のアクセス グループへのデスクトップ プールまたはファームの移動 79

Horizon Console でのアクセス グループの削除 80

アクセス グループ内のデオブジェクトの確認 80

アクセス グループ内の vCenter 仮想マシンの確認 80

カスタム ロールの管理 81

Horizon Console でのカスタム ロールの追加 81

Horizon Console でのカスタム ロールの権限の変更 81

Horizon Console でのカスタム ロールの削除 82

定義済みのロールと権限 82

定義済みの管理者ロール 83

グローバル権限 85

オブジェクト固有の権限 85

内部権限 86

一般的なタスクに必要な権限 86

プール管理のための権限 87

マシン管理のための権限 87

通常ディスク管理のための権限 88

ユーザーと管理者の管理のための権限 88

Horizon Help Desk Tool タスクの権限 89

一般的な管理タスクと管理コマンドのための権限 89

管理者ユーザーおよびグループに関するベスト プラクティス 90

## 8 Horizon Console でのポリシーの設定 91

グローバル ポリシーの設定 91

## 9 Horizon 7 コンポーネントのメンテナンス 93

Horizon 7 構成データのバックアップと復元	93
Horizon Connection Server と Horizon Composer のデータのバックアップ	93
Horizon 7 構成バックアップのスケジュール	94
Horizon 7 構成バックアップ設定	95
Horizon Connection Server からの構成データのエクスポート	95
Horizon Connection Server と Horizon Composer の構成データのリストア	97
Horizon Connection Server への構成データのインポート	97
Horizon Composer データベースのリストア	99
Horizon Console データベースのリストアの結果コード	100
Horizon Composer データベースのデータのエクスポート	101
Horizon Composer データベースのエクスポートの結果コード	102
Horizon Console での製品ライセンス キーまたはライセンス モードの変更	102
ライセンス使用量の監視	103
ライセンス使用量データのリセット	104
カスタム エクスペリエンス向上プログラム	105

## 10 Horizon Console での仮想デスクトップ プールの作成 106

インスタントクローン デスクトップ プールの作成	106
Horizon Console でインスタント クローン デスクトップ プールを作成するためのワークシート	107
インスタントクローン デスクトップ プールの作成	112
Horizon Console でのインスタント クローン デスクトップ プールのイメージの変更	113
Horizon Console でのプッシュイメージ操作のモニタリング	113
Horizon Console でのプッシュイメージ操作の再スケジュールまたはキャンセル	114
フル仮想マシンを含む自動デスクトップ プールの作成	114
Horizon Console でフル仮想マシンを含む自動プールを作成するためのワークシート	114
フル仮想マシンを含む自動プールの作成	118
Horizon Console での完全クローン デスクトップ プールの仮想マシンの再構築	119
Horizon Console でのリンク クローン デスクトップ プールの作成	120
Horizon Console でのリンク クローン デスクトップ プールの作成用ワークシート	120
Horizon Console でのリンク 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	130
Horizon Console でのリンク クローン デスクトップ プールの作成	131
Horizon Console での手動デスクトップ プールの作成	132
Horizon Console での手動デスクトップ プールの作成用ワークシート	133
Horizon Console での手動デスクトップ プールの作成	134
Horizon Console での手動プールのデスクトップ プール設定	136
デスクトップ プールの構成	137
Horizon Console でのデスクトップ プールでのユーザー割り当て	137
マシンの手動でのカスタマイズ	144
Horizon Console でのすべてのデスクトップ プール タイプのデスクトップ プールの設定	146
Horizon Console でのデスクトップ プールと仮想デスクトップの管理	150
デスクトップ プールの管理	150

仮想マシンベースのデスクトップの管理	152
Horizon Console での外部ファイルへの Horizon 7 情報のエクスポート	154
Horizon Composer リンク クローン デスクトップ仮想マシンの管理	155
Horizon Console での管理対象外のマシンと登録済みマシンの管理	168
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	169
Horizon Console での問題のあるマシンの表示	169
デスクトップ プールのユーザー割り当ての確認	170
Horizon Console でのデスクトップの再起動と仮想マシンのリセット	170
Horizon Console でのデスクトップ ユーザーへのメッセージの送信	171
Horizon Console での資格のないユーザーのマシンおよびポリシーの管理	172

## 11 Horizon Console での公開デスクトップとアプリケーションの作成 173

Horizon Console でのファームの作成	173
Horizon Console でファームを手動で作成するためのワークシート	174
Horizon Console での手動ファームの作成	175
Horizon Console で自動インスタント クローン ファームを作成するためのワークシート	176
Horizon Console での自動インスタント クローン ファームの作成	181
Horizon Console での自動リンク クローン ファーム作成用ワークシート	182
Horizon Console での自動リンク クローン ファームの作成	187
Horizon Console での公開デスクトップ プールの作成	188
公開デスクトップ プール作成用のワークシート	188
Horizon Console での公開デスクトップ プールの作成	189
Horizon Console でのアプリケーション プールの作成	190
Horizon Console でアプリケーション プールを手動で作成するためのワークシート	191
Horizon Console でのアプリケーション プールの作成	194
Horizon Console で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	194
Horizon Console でのファームの管理	196
Horizon Console でのファームの編集	196
Horizon Console でのファームの削除	196
Horizon Console でのファームの無効化または有効化	197
Horizon Console での自動インスタント クローン ファームのメンテナンス スケジュール	197
Horizon Console でのアプリケーション プールの管理	200
Horizon Console でのアプリケーション プールの編集	200
Horizon Console でのアプリケーション プールの削除	200
公開アプリケーションのアイコンの変更	200
公開アプリケーションのアイコンの削除	201
Horizon Console での RDS ホストの管理	201
Horizon Console での RDS ホストの編集	202
Horizon Console で手動ファームに RDS ホストを追加する	202
Horizon Console でのファームからの RDS ホストの削除	202
Horizon 7 からの RDS ホストの削除	203

Horizon Console での RDS ホストの無効化または有効化	203
Horizon Console での RDS ホストのモニタリング	203
Horizon Console での RDS ホストのステータス	204
Horizon Console での公開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管理	205
<b>12 Horizon Console でユーザーとグループに資格を付与する</b>	<b>207</b>
Horizon Console での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	207
Horizon Console での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	208
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	208
資格のあるプールのショートカットの設定	209
Horizon Console でのデスクトップ プールのショートカットの作成	210
Horizon Console でのアプリケーション プールのショートカットの作成	211
デスクトップとアプリケーション プールへのクライアント制限の実装	212
<b>13 JMP Integrated Workflow スタート ガイド</b>	<b>214</b>
JMP Integrated Workflow のバージョン情報	214
JMP 統合ワークフローの開始	214
<b>14 JMP 設定の管理</b>	<b>216</b>
JMP の初期構成	216
JMP 設定の管理	219
JMP Server の設定の編集	219
Horizon 7 認証情報の編集	219
Horizon 接続サーバ URL の編集	219
Active Directory ドメインの追加	221
Active Directory ドメイン情報の編集	221
Active Directory ドメイン情報の削除	221
App Volumes 情報の追加	222
App Volumes インスタンス情報の編集	223
App Volumes インスタンス情報の削除	223
User Environment Manager 構成共有情報の追加	223
User Environment Manager 構成ファイルの共有情報の編集	224
User Environment Manager 構成共有情報の削除	225
<b>15 JMP 割り当ての管理</b>	<b>226</b>
JMP 割り当ての作成	227
JMP 割り当ての編集	228
JMP 割り当ての複製	229
JMP 割り当ての削除	230
<b>16 Horizon Console でのイベント レポートの設定</b>	<b>231</b>



- Horizon Console で Horizon 7 イベント用のデータベースとデータベース ユーザーを追加する 231
- Horizon Console で SQL Server データベースをイベント レポート用に準備する 232
- Horizon Console でのイベント データベースの設定 233
- Horizon Console での Syslog サーバのイベント ログの設定 234
- Horizon 7 でのイベントの監視 236
  - Horizon 7 イベント メッセージ 236

## 17 Horizon Console での Horizon Help Desk Tool の使用 238

- Horizon Console で Horizon Help Desk Tool を開始します。 239
- Horizon Help Desk Tool でのユーザーのトラブルシューティング 239
- Horizon Help Desk Tool のセッションの詳細 242
- Horizon Help Desk Tool のセッション プロセス 247
- Horizon Help Desk Tool のアプリケーション ステータス 247
- Horizon Help Desk Tool でのデスクトップまたはアプリケーション セッションのトラブルシューティング 248

# VMware Horizon Console の管理

『VMware Horizon Console の管理』では、Horizon Console で VMware Horizon<sup>®</sup> 7 の構成と管理、管理者の作成、ユーザー認証の設定、ポリシーの構成、管理タスクを行う方法を説明します。また、Horizon 7 コンポーネントを保守およびトラブルシューティングする方法についても説明します。

Horizon Console を使用して クラウド ポッド アーキテクチャ 環境の設定と管理を行う方法については、『Horizon 7 でのクラウド ポッド アーキテクチャの管理』を参照してください。

## 対象読者

本書に記載されている情報は、VMware Horizon 7 を構成および管理するすべての方を対象としています。本書に記載されている情報は、仮想マシンのテクノロジーとデータセンターの操作に精通した、経験豊富な Windows または Linux システム管理者向けに書かれています。

# VMware Horizon Console の使用

VMware Horizon Console は、Web インターフェイスの最新バージョンで、仮想デスクトップや公開デスクトップとアプリケーションを作成したり、管理することができます。また、Horizon Console には、VMware Horizon Just-in-Time Management Platform (JMP) 統合ワークフロー機能が統合され、ワークスペースの管理を行うことができます。

Horizon Console は、Horizon 接続サーバをインストールして構成した後に使用できます。

接続サーバの構成については、『Horizon 7 の管理』ガイドを参照してください。

JMP 統合ワークフロー機能の詳細については、[13 章 JMP Integrated Workflow スタート ガイド](#) 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。

- [サポートされている Horizon 7 機能](#)
- [Horizon Console を使用する利点](#)
- [Horizon Console のインストールと構成](#)
- [Horizon Console へのログイン](#)

## サポートされている Horizon 7 機能

Horizon Console には、Horizon 7 機能の一部が実装されています。従来の Web インターフェイスである Horizon Administrator を使用すると、Horizon Console でまだ使用できない機能にもアクセスできます。

Horizon Administrator でサポートされている Horizon 7 の詳細については、『Horizon 7 の管理』ドキュメントを参照してください。

次の機能がサポートされています。

- サーバ
  - Horizon Connection Server の設定
  - イベント データベース
- 資格
  - ユーザーとグループに対する資格
  - デスクトップに対する資格
  - アプリケーションに対する資格

- グローバル資格
- グローバル ポリシー
- 認証
  - リモート アクセス認証
  - 公開アプリケーションでの非認証アクセス
  - スマート カード認証
  - ロールベースの委任管理
- 仮想デスクトップ
  - フル仮想マシンの自動専用割り当てプール
  - 自動、インスタント クローン専用割り当て、フローティング割り当てプール
  - 自動化されたリンク クローン デスクトップ プール
  - フル仮想マシンの自動フローティング割り当てプール
  - 手動デスクトップ プール
  - 通常ディスク
- 公開デスクトップ
  - 手動ファーム
  - 自動インスタント クローン ファーム
  - 自動リンク クローン ファーム
  - RDS デスクトップ プール
- 公開アプリケーション
  - 手動アプリケーション プール
  - 既存のアプリケーションのアプリケーション プール
- 仮想マシン
  - vCenter Server で使用可能な仮想マシン
  - vCenter Server で使用できない登録済みのマシン
- クラウド ポッド アーキテクチャ

次の機能はサポートされていません。

- 自動デスクトップ プールのクローン作成
- ThinApp アプリケーション

## Horizon Console を使用する利点

Horizon Console を使用すると、デスクトップやアプリケーションのデプロイが簡単になり、ジャストイン タイムのデスクトップ配信が可能になります。セキュリティ リスクを回避するため、より安全な Web インターフェイスも利用できます。

Horizon Console Web インターフェイスを更新すると、使いやすいワークロードを使用して、デスクトップとアプリケーションのデプロイやトラブルシューティングを行うことができます。

Horizon Console には、インスタント クローン、VMware App Volumes、VMware User Environment Manager テクノロジーを統合ワークフローに組み込む JMP Integrated Workflow 機能も含まれます。この機能を使用すると、オンデマンド デスクトップをすばやくデプロイし、スケーリングできます。詳細については、[JMP Integrated Workflow のバージョン情報](#)を参照してください。

Horizon Console には HTML5 ベースの Web インターフェイスが用意されています。これにより、安全性を強化し、多くのセキュリティ リスクと脆弱性を排除できます。

## Horizon Console のインストールと構成

Horizon 接続サーバ インストーラを使用して接続サーバをインストールして構成すると、Horizon Administrator の Web インターフェイスで Horizon Console URL を使用できます。JMP Server インストーラを使用して JMP Server をインストールして構成すると、Horizon Console で JMP Integrated Workflow を使用できます。

接続サーバのインストールに関する詳細については、『Horizon 7 のインストール』ドキュメントを参照してください。

接続サーバの構成については、『Horizon 7 の管理』ドキュメントを参照してください。

JMP Server のインストールと設定の詳細については、『VMware Horizon JMP Server のインストールとセットアップ ガイド』ドキュメントを参照してください。

## Horizon Console へのログイン

デスクトップまたはアプリケーションのデプロイ タスク、トラブルシューティング タスク、JMP ワークフローの管理を実行するには、Horizon Console にログインする必要があります。Horizon Administrator Web インターフェイスを介して Horizon Console にアクセスするには、セキュア接続 (TLS) を使用します。

### 前提条件

- Horizon 接続サーバが専用コンピュータにインストールされていることを確認します。
- Horizon Administrator で Horizon Console のリンクを表示し、Horizon Console にログインするには、ユーザーに事前定義ロールまたはその組み合わせを割り当てる必要があります。ただし、ユーザーにカスタム ロールか、事前定義ロールとカスタム ロールの組み合わせが割り当てられている場合、Horizon Administrator に Horizon Console リンクは表示されません。ロール ベースのアクセスの設定方法については、『Horizon 7 の管理』ドキュメントを参照してください。
- Horizon Console でサポートされている Web ブラウザを使用していることを確認します。サポート対象 Web ブラウザの詳細については、『Horizon 7 のインストール』ドキュメントを参照してください。

## 手順

- 1 Horizon Administrator インターフェイスにログインします。

Web ブラウザを開き、次の URL を入力します。 *server* は、接続サーバ インスタンスのホスト名です。

**https://*server*/admin**

**注:** ホスト名が解決できないときに接続サーバ インスタンスにアクセスする必要がある場合は、IP アドレスを使用できます。ただし、通信するホストは、接続サーバ インスタンスに対して構成された TLS 証明書に一致しないため、アクセスがブロックされたりアクセスのセキュリティが低下したりします。

Horizon Administrator へのアクセスは、接続サーバ コンピュータで構成されている証明書のタイプによって異なります。

接続サーバ ホストで Web ブラウザを開く場合、**https://localhost** ではなく、**https://127.0.0.1** を使用して接続します。この方法で localhost 解決における潜在的な DNS 攻撃を回避することにより、セキュリティが向上します。

オプション	説明
接続サーバ用に CA によって署名された証明書を構成しています。	最初に接続するときに、Web ブラウザで Horizon Console が表示されます。
接続サーバによって提供されたデフォルトの自己署名証明書が構成されます。	最初に接続したときに、Web ブラウザによって、アドレスに関連付けられているセキュリティ証明書が、信頼された証明機関から発行されていないことを警告するページが表示される場合があります。  [無視] をクリックして、現在の TLS 証明書の使用を続けます。

- 2 管理者アカウントにアクセスするための認証情報を持つユーザーとしてログインします。

スタンドアローンの接続サーバ インスタンス、または複製されたグループにおける最初の接続サーバ インスタンスをインストールするときに、管理者ロールの初期割り当てを行います。デフォルトでは、接続サーバのインストールに使用するアカウントが選択されていますが、このアカウントを Administrators ローカル グループまたはドメイン グローバル グループに変更できます。

Administrators ローカル グループを選択した場合は、このグループに追加されたドメイン ユーザーを直接またはグループ メンバーシップ経由で使用できます。このグループに追加されたローカル ユーザーは使用できません。

- 3 Horizon Administrator で、[Horizon Console] をクリックします。

新しいタブで Horizon Console Web インターフェイスを開きます。シングル サインオンで Horizon Console にログインします。

# Horizon Console での Horizon Connection Server の設定

# 3

Horizon Connection Server をインストールし初期構成を実行後、vCenter Server インスタンスおよび Horizon Composer サービスを Horizon 7 環境に追加し、管理者責任を委任するためのロールを設定して、構成データのバックアップをスケジュールリングできます。

この章には、次のトピックが含まれています。

- [Horizon Console での vCenter Server と Horizon Composer の設定](#)
- [Horizon Console での Horizon Connection Server のバックアップ](#)
- [Horizon Console でのクライアント セッションの設定](#)
- [Horizon Console での Horizon Connection Server の無効化または有効化](#)
- [Horizon Connection Server インスタンスの外部 URL の編集](#)
- [Horizon Console でのゲートウェイの登録](#)

## Horizon Console での vCenter Server と Horizon Composer の設定

仮想マシンをリモート デスクトップとして使用するには、vCenter Server と通信するように Horizon 7 を設定する必要があります。リンク クローン デスクトップ プールを作成して管理するには、Horizon Console で Horizon Composer の設定を行う必要があります。

Horizon 7 用のストレージも構成できます。ESXi ホストに対して、リンク クローン仮想マシンでディスク容量を再利用するように構成できます。ESXi ホストで仮想マシンのデータをキャッシュできるようにするには、vCenter Server の Horizon Storage Accelerator を有効にする必要があります。

## Horizon Composer Active Directory 操作のユーザー アカウントの作成

Horizon Composer を使用する場合は、Horizon Composer が Active Directory で特定の操作を行えるよう、Active Directory 内にユーザー アカウントを 1 つ作成する必要があります。Horizon Composer では、リンク クローン仮想マシンを Active Directory ドメインに参加させるためにこのアカウントが必要です。

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

## 手順

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

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

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

---

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

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

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

## 次のステップ

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

## Horizon Console での製品のライセンス キーのインストール

Connection Server を使用するには、まず製品のライセンス キーを入力する必要があります。

---

**注:** Horizon 7 サブスクリプションのライセンスがある場合、製品のライセンス キーは必要ありません。サブスクリプション ライセンスの詳細については、『Horizon 7 のインストール』の「サブスクリプション ライセンスでの Horizon 7 の有効化」を参照してください。

---

Horizon Console に初めてログインすると、[ライセンスと使用状況] ペインが表示されます。



複製された Connection Server インスタンスまたはセキュリティ サーバをインストールするときは、ライセンス キーを設定する必要はありません。複製されたインスタンスとセキュリティ サーバは、View の LDAP 構成に格納されている共通ライセンス キーを使用します。

---

**注:** Connection Server には有効なライセンス キーが必要です。プロダクト ライセンス キーは 25 文字のキーです。

---

#### 手順

- 1 Horizon Console で、[設定] - [製品のライセンスと使用状況] の順に選択します。
- 2 [ライセンスの設定] パネルで、[ライセンスを編集] をクリックします。
- 3 ライセンス シリアル番号を入力し、[OK] をクリックします。
- 4 ライセンスの有効期限の日付を確認します。
- 5 お持ちの製品のライセンスによって使用資格が付与されている VMware Horizon 7 のエディションに基づいて、デスクトップ、アプリケーションのリモート処理、および View Composer ライセンスが有効または無効になっていることを確認します。

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

## Horizon Console での vCenter Server インスタンスの Horizon 7 への追加

Horizon 7 環境内の vCenter Server インスタンスに接続するように、Horizon 7 を構成する必要があります。Horizon 7 がデスクトップ プールで使用する仮想マシンは、vCenter Server が作成し、管理します。

vCenter Server インスタンスをリンク モード グループ内で実行する場合は、各 vCenter Server インスタンスを個別に Horizon 7 に追加する必要があります。

Horizon 7 は、安全なチャネル (TLS) を使用して vCenter Server インスタンスに接続します。

#### 前提条件

- Connection Server の製品ライセンス キーをインストールします。
- Horizon 7 をサポートするのに必要な vCenter Server で、操作を実行する権限のある vCenter Server ユーザーを準備します。Horizon Composer を使用するには、このユーザーに権限を追加する必要があります。  
  
Horizon 7 のための vCenter Server ユーザーの構成の詳細については、『Horizon 7 のインストール』ドキュメントを参照してください。
- TLS サーバ証明書が vCenter Server ホストにインストールされていることを確認します。本番環境で、信頼された証明機関 (CA) によって署名された有効な証明書をインストールします。

テスト環境では、vCenter Server でインストールされたデフォルト証明書を使用できますが、vCenter Server を Horizon 7 に追加する際に証明書サムプリントを受け入れる必要があります。

- 複製されたグループ内のすべての Connection Server インスタンスが、vCenter Server ホストにインストールされているサーバ証明書のルート CA 証明書を信頼していることを確認します。ルート CA 証明書が、Connection Server ホスト上の Windows ローカル コンピュータの証明書ストア内の [信頼されたルート証明機関] - [証明書] フォルダにあるかどうか確認します。このフォルダにない場合、ルート CA 証明書を Windows ローカル コンピュータの証明書ストアにインポートします。

『Horizon 7 のインストール』ドキュメントの「ルート証明書と中間証明書を Windows 証明書ストアにインポートする」を参照してください。

- vCenter Server インスタンスに ESXi ホストが含まれていることを確認します。vCenter Server インスタンスでホストが構成されていない場合、そのインスタンスを Horizon 7 に追加することはできません。
- vSphere 5.5 以降のリリースにアップグレードする場合、vCenter Server ユーザーとして使用するドメイン管理者アカウントが、vCenter Server のローカル ユーザーによって vCenter Server にログインするために明示的に指定された権限であったことを確認してください。
- Horizon 7 で FIPS モードを使用する予定の場合は、vCenter Server 6.0 以降および ESXi 6.0 以降のホストを使用していることを確認してください。

詳細については、『Horizon 7 のインストール』ドキュメントで「FIPS モードでの Horizon 7 のインストール」を参照してください。

- vCenter Server と Horizon Composer の操作数の上限を決定する設定について理解しておきます。

#### 手順

- 1 Horizon Console で、[設定] - [サーバ] の順に移動します。
- 2 [vCenter Server] タブで、[追加] をクリックします。
- 3 [vCenter Server 設定] の [サーバ アドレス] テキスト ボックスに、vCenter Server インスタンスの完全修飾ドメイン名 (FQDN) を入力します。

FQDN にはホスト名とドメイン名が含まれます。たとえば、FQDN の **myserverhost.companydomain.com** で、**myserverhost** はホスト名で、**companydomain.com** はドメインです。

---

**注:** DNS 名または URL を使用してサーバを入力すると、Horizon 7 は管理者が以前に IP アドレスを使用して Horizon 7 にこのサーバを追加したかどうかを確認する DNS 検索を実行しません。vCenter Server をその DNS 名と IP アドレスの両方で追加すると、競合が発生します。

---

- 4 vCenter Server ユーザーの名前を入力します。
- 5 vCenter Server ユーザーのパスワードを入力します。
- 6 (オプション) この vCenter Server インスタンスの説明を入力します。
- 7 TCP のポート番号を入力します。

デフォルトのポートは 443 です。

- 8 (オプション) VMware Cloud on AWS に vCenter Server がデプロイされている場合は、[VMware Cloud on AWS] を選択します。

VMware Cloud on AWS と Horizon 7 の統合の詳細については、『Horizon 7 の統合』を参照してください。

- 9 [詳細設定] で、vCenter Server と Horizon Composer の同時操作の制限数を設定します。
- 10 [次へ] をクリックし、指示に従ってウィザードを完了します。

#### 次のステップ

Horizon Composer の設定を行います。

- vCenter Server インスタンスが署名された TLS 証明書で設定されていて、Connection Server がルート証明書を信頼している場合、[vCenter Server を追加] ウィザードで [Horizon Composer 設定] ページが表示されます。
- vCenter Server インスタンスがデフォルト証明書で構成されている場合、最初に既存の証明書のサムプリントを受け入れるかどうかを決定する必要があります。[デフォルトの TLS 証明書のサムプリントを受け入れる](#)を参照してください。

Horizon 7 で複数の vCenter Server インスタンスを使用している場合、この手順を繰り返してその他の vCenter Server インスタンスを追加します。

## Horizon Composer の設定

Horizon Composer を使用するには、Horizon 7 が Horizon Composer サービスに接続できるように設定する必要があります。Horizon Composer は個別のホストにインストールすることも、vCenter Server と同じホストにインストールすることもできます。

それぞれの Horizon Composer サービスと vCenter Server インスタンスが 1 対 1 で対応している必要があります。1 つの Horizon Composer サービスは 1 つの vCenter Server インスタンスのみと一緒に作動できます。1 つの vCenter Server インスタンスは 1 つの Horizon Composer サービスにのみ関連付けることができます。

Horizon 7 の初期デプロイが完了した後で、Horizon 7 環境の拡張または変更に対応できるように Horizon Composer サービスを新しいホストに移行できます。初期の Horizon Composer 設定は Horizon Console で編集できますが、確実に移行を成功させるためには追加の手順を実行する必要があります。

#### 前提条件

- リンク クローンを含む Active Directory ドメインに仮想マシンを追加したり、ドメインから仮想マシンを削除したりするための権限を付与されたユーザーが Active Directory に作成されていることを確認します。[Horizon Composer Active Directory 操作のユーザー アカウントの作成](#)を参照してください。
- vCenter Server に接続するように Horizon 7 を構成したことを確認します。そのためには、[vCenter Server を追加] ウィザードで [vCenter Server の情報] ページを完了する必要があります。[Horizon Console での vCenter Server インスタンスの Horizon 7 への追加](#)を参照してください。
- この Horizon Composer サービスがまだ別の vCenter Server インスタンスに接続するように構成されていないことを確認します。

## 手順

- 1 Horizon Console で、[設定] - [サーバ] の順に移動します。
- 2 [vCenter Server] タブで [追加] をクリックします。[vCenter Server 設定] ページで、vCenter Server の情報を入力し、[次へ] をクリックします。
- 3 [Horizon Composer の設定] ページで、Horizon Composer を使用していない場合、[Horizon Composer を使用しない] を選択します。

[Horizon Composer を使用しない] を選択した場合、その他の Horizon Composer 設定が非アクティブになります。[次へ] をクリックすると、[vCenter Server を追加] ウィザードで [ストレージ設定] ページが表示されます。

- 4 Horizon Composer を使用している場合は、Horizon Composer ホストの場所を選択します。

オプション	説明
Horizon Composer が vCenter Server と同じホストにインストールされます。	<ol style="list-style-type: none"> <li>a [Horizon Composer を vCenter Server と一緒にインストール] を選択します。</li> <li>b ポート番号が vCenter Server に Horizon Composer サービスをインストールしたときに指定したポートと同じであることを確認します。デフォルトのポート番号は 18443 です。</li> </ol>
Horizon Composer が個別のホストにインストールされます。	<ol style="list-style-type: none"> <li>a [スタンドアロンの Horizon Composer Server] を選択します。</li> <li>b Horizon Composer Server アドレスのテキスト ボックスに、Horizon Composer ホストの完全修飾ドメイン名 (FQDN) を入力します。</li> <li>c Horizon Composer ユーザーの名前を入力します。 例: <b>domain.com\user</b> または <b>user@domain.com</b></li> <li>d Horizon Composer ユーザーのパスワードを入力します。</li> <li>e ポート番号が Horizon Composer サービスをインストールしたときに指定したポートと同じであることを確認します。デフォルトのポート番号は 18443 です。</li> </ol>

- 5 [次へ] をクリックして [Horizon Composer ドメイン] ページを表示します。

## 次のステップ

Horizon Composer ドメインを設定します。

- Horizon Composer インスタンスが署名された TLS 証明書で構成されていて、Connection Server がルート証明書を信頼している場合、[vCenter Server を追加] ウィザードで [Horizon Composer ドメイン] ページが表示されます。
- Horizon Composer インスタンスがデフォルト証明書で構成されている場合、最初に既存の証明書のサムプリントを受け入れるかどうかを決定する必要があります。

## Horizon Composer ドメインの設定

Horizon Composer がリンク クローン デスクトップを展開する Active Directory ドメインを構成する必要があります。Horizon Composer の複数のドメインを設定できます。vCenter Server と Horizon Composer の設定を Horizon 7 に追加した後で、Horizon Console で vCenter Server インスタンスを編集して、より多くの Horizon Composer ドメインを追加できます。

### 前提条件

- Active Directory 管理者は、Active Directory の操作に必要な Horizon Composer ユーザーを作成する必要があります。このドメイン ユーザーには、リンク クローンを含んでいる Active Directory ドメインから仮想マシンを追加または削除する権限が必要です。このユーザーに必要な権限の詳細については、[Horizon Composer Active Directory 操作のユーザー アカウントの作成](#) を参照してください。
- Horizon Console で、[vCenter Server を追加] ウィザードの [vCenter Server 設定] ページと [Horizon Composer の設定] ページを完了していることを確認します。

### 手順

- 1 Horizon Console で、[設定] - [サーバ] の順に移動します。
- 2 [vCenter Server] タブで [追加] をクリックします。[vCenter Server 設定] ページで、vCenter Server の情報を入力し、[次へ] をクリックします。
- 3 Horizon Composer を使用している場合は、[Horizon Composer の設定] ページで Horizon Composer ホストの場所を選択し、[次へ] をクリックします。

Horizon Composer の詳細については、[Horizon Composer の設定](#) を参照してください。

- 4 [Horizon Composer ドメイン] ページで、[追加] をクリックして、Active Directory の操作に必要な Horizon Composer ユーザーのアカウント情報を追加します。
- 5 Active Directory ドメインのドメイン名を入力します。

例：**domain.com**

- 6 Horizon Composer ユーザーのドメイン ユーザー名（ドメイン名を含む）を入力します。

例：**domain.com\admin**

- 7 アカウントのパスワードを入力します。
- 8 [OK] をクリックします。
- 9 リンク クローン プールを展開する他の Active Directory ドメインでの権限を持つドメイン ユーザー アカウントを追加するには、前記の手順を繰り返します。
- 10 [次へ] をクリックして [ストレージ設定] ページを表示します。

### 次のステップ

仮想マシンのディスク容量再利用を有効にして、Horizon 7 の Horizon Storage Accelerator を設定します。

## Horizon Console でのインスタント クローンのドメイン管理者の追加

インスタントクローン デスクトップ プールを作成する前に、インスタントクローン ドメイン管理者を Horizon 7 に追加する必要があります。

## 前提条件

- インスタント クローンのドメイン管理者が、必要な Active Directory ドメイン権限を持っていることを確認します。詳細については、『Horizon 7 のインストール』ドキュメントの「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 Horizon Console で、[設定] - [インスタント クローンのドメイン アカウント] の順に選択します。
- 2 [追加] をクリックします。
- 3 インスタント クローンのドメイン管理者のドメインを選択します。
- 4 ユーザー名とパスワードを入力します。

## 次のステップ

Horizon Console では、インスタント クローンのドメイン管理者を追加または削除できます。また、インスタント クローンの管理者リストを Microsoft Excel ファイルにエクスポートすることもできます。[設定] - [インスタント クローンのドメイン アカウント] の順に移動し、インスタント クローンのドメイン管理者を選択します。[編集] をクリックして、管理者のドメインとログイン情報を編集します。[削除] をクリックして、管理者を削除します。エクスポートアイコンをクリックして、インスタント クローンの管理者リストを Microsoft Excel ファイルにエクスポートします。

## vSphere でリンク クローン仮想マシンのディスク領域を再利用できるようにする

vSphere バージョン 5.1 以降では、Horizon 7 用にディスク容量再利用機能を有効にできます。Horizon 7 がリンク クローン仮想マシンを効率的なディスク形式で作成します。これにより、ESXi ホストはリンク クローン内で使用されていないディスク容量を再利用できるようになり、リンク クローンに必要なストレージ容量の合計を削減できます。

ユーザーがリンク クローン デスクトップを操作するたびに、クローンの OS ディスクが大きくなり、最終的には完全 クローン デスクトップとほとんど同じディスク領域を使用する場合もあります。ディスク領域再利用により、リンク クローンを更新または再構成しなくても、OS ディスクのサイズを減らすことができます。仮想マシンがパワーオンされ、ユーザーがリモート デスクトップを操作している間に、領域を再利用することができます。

ディスク領域再利用は、ログオフ時の更新などのストレージ節約戦略を利用できない展開にとって特に便利です。たとえば、ユーザー アプリケーションを専用リモート デスクトップにインストールするナレッジ ワークの場合、リモート デスクトップが更新または再構成されたときに、個人用アプリケーションが失われることがあります。Horizon 7 はディスク領域再利用により、最初にプロビジョニングされたときの小さなサイズとほぼ同じサイズにリンク クローンを保つことができます。

この機能には、効率的なディスク フォーマットとスペース再利用操作の 2 つのコンポーネントがあります。

vSphere バージョン 5.1 以降では、親の仮想マシンが仮想ハードウェア バージョン 9 以降の場合、Horizon 7 は領域再利用操作が有効になっているかどうかにかかわらず、領域効率の高い OS ディスクでリンク クローンを作成します。

容量再利用操作を有効にするには、Horizon Console を使用して vCenter Server 用の容量再利用を有効にして、個別のデスクトップ プール用に仮想マシンのディスク容量を再利用する必要があります。vCenter Server 用の領域再利用設定には、vCenter Server インスタンスによって管理されるすべてのデスクトップ プールでこの機能を無効にするためのオプションがあります。vCenter Server 用にこの機能を無効にすると、デスクトップ プール レベルの設定が上書きされます。

以下のガイドラインは、領域再利用機能に適用されます。

- リンク クローン内の領域効率の高い OS ディスクでのみ使用できます。
- Horizon Composer パーシステント ディスクには影響しません。
- vSphere バージョン 5.1 以降で、仮想ハードウェア バージョン 9 以降の仮想マシンでのみ機能します。
- 完全クローン デスクトップでは使用できません。
- SCSI コントローラを備えた仮想マシンで使用できます。IDE コントローラはサポートされていません。

ネイティブ NFS スナップショット テクノロジ (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。

#### 前提条件

- vCenter Server および ESXi ホストについて、クラスタにすべての ESXi ホストが含まれ、ダウンロード パッチ ESXi510-201212001 以降を適用済みの ESXi 5.1 以降が搭載されたバージョン 5.1 であることを確認します。

#### 手順

- 1 Horizon Console で、[設定] - [サーバ] の順に移動します。
- 2 [vCenter Server] タブで [追加] をクリックし、[vCenter Server を追加] ウィザードを完了して、[ストレージ設定] ページに移動します。
- 3 [ストレージ設定] ページで、[仮想マシンディスク容量を再利用] を選択します。

Horizon 7 の新規インストールを実行している場合、このオプションはデフォルトで選択されます。Horizon 7 の新しいリリースにアップグレードする場合は、[仮想マシンディスク容量を再利用] を選択する必要があります。

#### 次のステップ

[ストレージ設定] ページで、Horizon Storage Accelerator を設定します。

Horizon 7 でディスク領域再利用の構成を終了するには、デスクトップ プール用の領域再利用をセットアップします。

## vCenter Server の Horizon Storage Accelerator の設定

vSphere で、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 ホストを設定できます。この Horizon Storage Accelerator と呼ばれている機能は、ESXi ホストで Content Based Read Cache (CBRC) 機能を使用します。多くの仮想マシンが起動しているかアンチウイルス スキャンが一度に実行される場合に I/O ストームが発生することがありますが、Horizon Storage Accelerator により、I/O ストーム時の Horizon 7 のパフォーマンスが向上します。この機能は、管理者またはユーザーがアプリケーションまたはデータを頻繁にロードする場合にも役立ちます。ホストは、OS 全体またはアプリケーションをストレージ システムから何度も読み取るのではなく、共通のデータ ブロックをキャッシュから読み取ることができます。



ブート ストーム中の IOPS 数を減らすことにより、Horizon Storage Accelerator によるストレージ アレイの要求が抑えられ、これにより Horizon 7 展開をサポートするためのストレージ I/O 帯域幅が小さくなります。

この手順で説明しているように、Horizon Console の [vCenter Server を追加] ウィザードで Horizon Storage Accelerator 設定を選択することで、ESXi ホストでのキャッシュ機能を有効にします。

個々のデスクトップ プールに Horizon Storage Accelerator が設定されていることも確認します。デスクトップ プールで操作するには、Horizon Storage Accelerator を vCenter Server とそれぞれのデスクトップ プールで有効にする必要があります。

デフォルトでは、デスクトップ プールで Horizon Storage Accelerator が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 クローンを提供ジョニングする前に、新しいレプリカとそのダイジェスト ディスクが作成されていることを確認する必要があります。新しいレプリカは、プールを新しいスナップショットに再構成するか、プールを新しいデータストアに再分散することによって作成できます。ダイジェスト ファイルは、デスクトップ プール内の仮想マシンがパワーオフされているときにのみ構成できます。

リンク クローンを含むデスクトップ プールと、フル仮想マシンを含むプールで Horizon Storage Accelerator を有効にすることができます。

ネイティブ NFS スナップショット テクノロジ (VAAI) は、Horizon Storage Accelerator 用に有効にされているプールでサポートされていません。

Horizon Storage Accelerator は、Horizon 7 レプリカ階層を使用する構成で機能するようになり、レプリカはリンク クローンでなく別のデータストアに保存されます。Horizon 7 レプリカ階層で Horizon Storage Accelerator を使用するパフォーマンスの利点は実質的には大きくありませんが、特定の容量に関わる利点は別のデータストアにレプリカを保存することによって実現できる場合があります。したがって、この組み合わせがテストおよびサポートされます。

---

**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 Horizon 7 ポッドを使用している場合は、共有 ESXi ホストのすべてのプールについて Horizon Storage Accelerator 機能を有効にする必要があります。複数ポッドの設定に一貫性がない場合は、共有 ESXi ホストの仮想マシンが不安定になることがあります。

---

#### 前提条件

- vCenter Server ホストおよび ESXi ホストのバージョンが 5.1 以降であることを確認します。  
ESXi クラスタで、すべてのホストのバージョンが 5.1 以降であることを確認します。
- vCenter Server の [ホスト] > [構成] > [詳細] 設定の権限が vCenter Server ユーザに割り当てられていることを確認します。  
『Horizon 7 のインストール』ドキュメントで、vCenter Server ユーザーに必要な Horizon 7 および Horizon Composer の権限について説明しているトピックを参照してください。

#### 手順

- 1 Horizon Console で、[設定] - [サーバ] の順に移動します。
- 2 [vCenter Server] タブで [追加] をクリックし、[vCenter Server を追加] ウィザードを完了して、[ストレージ設定] ページに移動します。



- 3 [ストレージ設定] ページで、[Horizon Storage Accelerator を有効にする] を選択します。

このオプションはデフォルトで選択されています。

- 4 デフォルトのホスト キャッシュ サイズを指定します。

デフォルトのキャッシュ サイズは、この vCenter Server インスタンスで管理されるすべての ESXi ホストに適用されます。

デフォルト値は 1,024 MB です。キャッシュ サイズは、100 MB ~ 2,048 MB の範囲でなければなりません。

- 5 個別の ESXi ホスト向けに別のキャッシュ サイズを指定するには、ESXi ホストを選択して、[キャッシュ サイズの編集] をクリックします。

a [ホスト キャッシュ] ダイアログ ボックスで、[デフォルトのホスト キャッシュ サイズを上書き] のチェック ボックスをオンにします。

b [ホスト キャッシュ サイズ] の値を 100 MB ~ 2,048 MB の範囲で入力し、[OK] をクリックします。

- 6 [ストレージ設定] ページで、[次へ] をクリックします。

- 7 [設定内容の確認] ページで設定を確認したら、[送信] をクリックします。

#### 次のステップ

クライアント セッションおよび接続用の設定を構成します。『Horizon 7 の管理』の「クライアント セッションの設定」を参照してください。

Horizon 7 で Horizon Storage Accelerator の設定を完了するには、デスクトップ プールの Horizon Storage Accelerator を設定します。『Horizon 7 での仮想デスクトップのセットアップ』ドキュメントの「デスクトップ プール用に Horizon Storage Accelerator を構成する」を参照してください。

## vCenter Server と Horizon Composer の同時操作の制限数

vCenter Server を Horizon 7 に追加する場合、または vCenter Server 設定を編集する場合には、vCenter Server と Horizon Composer で実行される同時操作の最大数を設定するオプションをいくつか構成できます。

これらのオプションは、[vCenter Server を追加] ウィザードの [vCenter Server 設定] ページにある [詳細設定] パネルで設定します。

表 3-1. vCenter Server と Horizon Composer の同時操作の制限数

設定	説明
[最大同時 vCenter プロビジョニング操作数]	<p>Connection Server がこの vCenter Server インスタンスでフル仮想マシンのプロビジョニングと削除のために出すことができる同時要求の最大数を指定します。</p> <p>デフォルト値は 20 です。</p> <p>この設定はフル仮想マシンにのみ適用されます。</p>
[最大同時電源操作数]	<p>この vCenter Server インスタンス内の Connection Server によって管理されている仮想マシンで同時に実行できる電源操作（起動、シャットダウン、サスペンドなど）の最大数を決定します。</p> <p>デフォルト値は 50 です。</p> <p>この設定の値を計算するためのガイドラインについては、<a href="#">リモート デスクトップ ログオン ストームをサポートするための同時電源操作レートの設定</a>を参照してください。</p> <p>この設定は、フル仮想マシンとリンク クローンに適用されます。</p>

設定	説明
[最大同時 Horizon Composer メンテナンス操作数]	<p>この Horizon Composer インスタンスによって管理されているリンク クローンで同時に実行できる、Horizon Composer の更新、再構成、再調整などの操作の最大数を決定します。</p> <p>デフォルト値は 12 です。</p> <p>メンテナンス操作を開始する前に、アクティブなセッションが存在するリモート デスクトップからログオフする必要があります。メンテナンス操作の開始直後にユーザーを強制的にログオフさせた場合、ログオフが必要なリモート デスクトップ上の同時操作の最大数は、構成値の半分にになります。たとえば、この設定を 24 に構成して、ユーザーを強制的にログオフさせた場合、ログオフが必要なリモート デスクトップ上の同時操作の最大数は 12 です。</p> <p>この設定はリンク クローンにのみ適用されます。</p>
[最大同時 Horizon Composer プロビジョニング操作数]	<p>この Horizon Composer インスタンスによって管理されているリンク クローンで同時に実行できる作成および削除操作の最大数を指定します。</p> <p>デフォルト値は 8 です。</p> <p>この設定はリンク クローンにのみ適用されます。</p>
[インスタント クローン エンジンの最大同時操作数]	<p>この vCenter Server インスタンスによって管理されているインスタント クローンで同時に実行できる作成および削除操作の最大数を指定します。</p> <p>この設定はインスタント クローンにのみ適用されます。</p>

## リモート デスクトップ ログオン ストームをサポートするための同時電源操作レートの設定

[最大同時電源操作数] 設定は、vCenter Server インスタンスのリモート デスクトップ仮想マシンで使用可能な同時電源操作の最大数を制御します。この最大数はデフォルトで 50 に設定されています。この値は、多くのユーザーが同時にデスクトップにログインするときのピーク時パワーオン率をサポートするように変更できます。

ベスト プラクティスとして、この設定の適切な値を判断するためにパイロット段階を実施できます。プランニングのガイドラインについては、『Horizon 7 アーキテクチャの計画』ドキュメントの「アーキテクチャ設計の要素と計画のガイドライン」を参照してください。

必要な同時電源操作の数は、デスクトップがパワーオンになるピーク率と、デスクトップがパワーオンになり、起動し、接続可能になるのに要する時間に基づきます。一般的に、推奨される電源操作の最大数は、デスクトップの開始に要した合計時間にピーク時パワーオン率を掛け合わせたものです。

たとえば、平均的なデスクトップは起動に 2 ～ 3 分要します。したがって、同時電源操作の最大数はピーク時パワーオン率の 3 倍にする必要があります。デフォルト設定の 50 は、毎分 16 台のデスクトップのピーク時パワーオン率をサポートできることを見込んでいます。

システムは、デスクトップが起動するまで最大 5 分待機します。起動にこれ以上の時間を要すると、他のエラーが発生する可能性があります。万一来て、同時電源操作の最大数をピーク時パワーオン率の 5 倍に設定できます。控えめに考えて、デフォルト設定の 50 は、毎分 10 台のデスクトップのピーク時パワーオン率をサポートします。

ログオン、つまりデスクトップのパワーオン操作は、通常、特定の時間範囲で正規分散されて行われます。時間範囲の中間にパワーオン操作が発生し、パワーオン操作の 40% が時間範囲の 6 分の 1 で発生すると仮定して、ピーク時パワーオン率を概算することができます。たとえば、ユーザーが午前 8:00 から午前 9:00 の間にログオンすると、時間範囲は 1 時間であり、ログオンの 40% は午前 8:25 から午前 8:35 までの 10 分間に発生します。ユーザーが 2,000 人いる場合、そのうち 20% がデスクトップをパワーオフしており、400 台のデスクトップのパワーオン操作の 40% がこの 10 分間に発生することになります。ピーク時パワーオン率は、毎分 16 台のデスクトップになります。

## デフォルトの TLS 証明書のサムプリントを受け入れる

vCenter Server および Horizon Composer インスタンスを Horizon 7 に追加する場合、vCenter Server および Horizon Composer インスタンス用に使用される TLS 証明書が有効で、Connection Server によって信頼されていることを確認する必要があります。vCenter Server および Horizon Composer でインストールされるデフォルトの証明書が存在する場合、これらの証明書のサムプリントを受け入れるかどうかを決定する必要があります。

vCenter Server または Horizon Composer インスタンスが認証局 (CA) によって署名された証明書で設定され、ルート証明書が Connection Server によって信頼される場合、この証明書のサムプリントを受け入れる必要はありません。操作は何も必要ありません。

デフォルト証明書を CA によって署名された証明書に置換するにもかかわらず Connection Server がルート証明書を信頼していない場合、証明書のサムプリントを受け入れるかどうかを決定する必要があります。サムプリントとは、証明書の暗号化ハッシュです。サムプリントは、提示された証明書が以前に受け入れられた証明書など、別の証明書と同じものであるかどうかを素早く判別するために使用されます。

---

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

---

TLS 証明書の設定方法については、『Horizon 7 のインストール』の「Horizon 7 Server の TLS 証明書の設定」を参照してください。

まず、[vCenter Server を追加] ウィザードを使用して、Horizon Console に vCenter Server と Horizon Composer を追加します。証明書が信頼されておらず、サムプリントを受け入れなければ、vCenter Server および vCenter Server を追加できません。

これらのサーバが追加されたら、[vCenter Server を編集] ダイアログ ボックスで再設定できます。

---

**注:** 旧リリースからアップグレードする場合、そして vCenter Server または Horizon Composer 証明書が信頼されていない場合、または信頼されている証明書を信頼されていない証明書と置き換える場合は、証明書のサムプリントを受け入れる必要もあります。

---

### 手順

- 1 Horizon Console で [無効な証明書が検出されました] ダイアログ ボックスが表示されたら、[証明書を表示] をクリックします。
- 2 [証明書情報] ウィンドウで証明書のサムプリントを調べます。
- 3 vCenter Server または Horizon Composer インスタンス用に設定された証明書のサムプリントを調べます。
  - a vCenter Server または Horizon Composer ホストで、MMC スナップインを開始し、Windows 証明書ストアを開きます。
  - b vCenter Server または Horizon Composer 証明書に移動します。
  - c [証明書の詳細] タブをクリックして証明書のサムプリントを表示します。同様に、SAML 認証システムの証明書のサムプリントを調べます。必要に応じて、SAML 認証システム ホストで上記の手順を行います。

- 4 [証明書情報] ウィンドウのサムプリントが vCenter Server または Horizon Composer インスタンスのサムプリントと一致することを確認します。

同様に、SAML 認証システムについてもサムプリントが一致するかどうかを調べます。

- 5 証明書のサムプリントを受け入れるかどうかを決定します。

オプション	説明
サムプリントが一致しています。	[許可] をクリックしてデフォルト証明書を使用します。
サムプリントが一致していません。	[拒否] をクリックします。 一致しない証明書のトラブルシューティングを行います。たとえば、vCenter Server または Horizon Composer で正しくない IP アドレスを指定した可能性があります。

## Horizon 7 からの vCenter Server インスタンスの削除

Horizon 7 と vCenter Server インスタンス間の接続を削除できます。これを行うと、Horizon 7 は、vCenter Server インスタンスで作成された仮想マシンを管理しなくなります。

### 前提条件

vCenter Server インスタンスに関連付けられているすべての仮想マシンを削除します。仮想マシンの削除の詳細については、『Horizon 7 での仮想デスクトップのセットアップ』ドキュメントで「デスクトップ プールの削除」を参照してください。

### 手順

- 1 Horizon Console で、[設定] - [サーバ] の順に移動します。
- 2 [vCenter Server] タブで、vCenter Server インスタンスを選択します。
- 3 [削除] をクリックします。

Horizon 7 がこの vCenter Server インスタンスによって管理される仮想マシンにアクセスできなくなることを警告するダイアログ メッセージが表示されます。

- 4 [OK] をクリックします。

Horizon 7 は、vCenter Server インスタンスで作成された仮想マシンにアクセスできなくなります。

## Horizon 7 からの Horizon Composer の削除

vCenter Server インスタンスに関連付けられている Horizon Composer サービスと Horizon 7 との接続を削除できます。

Horizon Composer との接続を無効にする前に、Horizon Composer によって作成されたすべてのリンク クローン仮想マシンを Horizon 7 から削除する必要があります。Horizon 7 では、関連付けられたリンク クローンが残っている場合は、Horizon Composer を削除できません。Horizon Composer への接続を無効にすると、Horizon 7 で新しいリンク クローンをプロビジョニングまたは管理できなくなります。

## 手順

- 1 Horizon Composer によって作成されたリンク クローン デスクトップ プールを削除します。
  - a Horizon Console で、[インベントリ] - [デスクトップ] の順に選択します。
  - b リンク クローン デスクトップ プールを選択して、[削除] をクリックします。

リンク クローン デスクトップ プールが Horizon 7 から完全に削除されることを警告するダイアログ ボックスが表示されます。リンク クローン 仮想マシンが通常ディスクを使用して構成されている場合、通常ディスクを切断または削除できます。
  - c [OK] をクリックします。

仮想マシンが vCenter Server から削除されます。さらに、関連付けられた Horizon Composer データベース エントリと Horizon Composer によって作成されたレプリカも削除されます。
  - d Horizon Composer によって作成された各リンク クローン デスクトップ プールに次の手順を繰り返します。
- 2 [設定] - [サーバ] の順に移動します。
- 3 [vCenter Server] タブで、Horizon Composer が関連付けられている vCenter Server インスタンスを選択します。
- 4 [編集] をクリックします。
- 5 [Horizon Composer] タブの [Horizon Composer Server 設定] で、[Horizon Composer を使用しない] を選択して [OK] をクリックします。

この vCenter Server インスタンスでリンク クローン デスクトップ プールを作成することはできなくなりますが、vCenter Server インスタンスでフル仮想マシン デスクトップ プールの作成と管理を引き続き行うことができます。

## 次のステップ

別のホストに Horizon Composer をインストールし、Horizon 7 を再構成して新しい Horizon Composer サービスに接続する場合は、特定の追加手順を実行する必要があります。リンク クローン 仮想マシンがない Horizon Composer を移行する方法については、『Horizon 7 の管理』を参照してください。

## 競合している vCenter Server の一意の ID

環境内に複数の vCenter Server インスタンスが構成されている場合は、新しいインスタンスを追加しようとする、一意の ID が競合しているために失敗することがあります。

## 問題

Horizon 7 に vCenter Server インスタンスを追加しようとしています、新しい vCenter Server インスタンスの一意の ID が既存のインスタンスと競合しています。

## 原因

2 つの vCenter Server インスタンスが同一一意の ID を使用することはできません。vCenter Server の一意の ID は、デフォルトではランダムに生成されますが、編集できます。

#### 解決方法

- 1 vSphere Client で、[管理] - [vCenter Server 設定] - [ランタイムの設定] の順にクリックします。
- 2 新しい一意の ID を入力し、[OK] をクリックします。

vCenter Server の一意の ID 値を編集する方法の詳細については、vSphere のドキュメントを参照してください。

## Horizon Console での Horizon Connection Server のバックアップ

Horizon Connection Server の初期構成が完了したら、Horizon 7 と Horizon Composer の構成データの定期的なバックアップをスケジュールリングする必要があります。

Horizon 7 構成のバックアップと復元については、[Horizon Connection Server と Horizon Composer のデータのバックアップ](#)を参照してください。

## Horizon Console でのクライアント セッションの設定

Connection Server インスタンスまたは複製されたグループによって管理されるクライアント セッションおよび接続に影響を与えるグローバル設定を指定できます。セッション タイムアウトの長さを設定したり、ログイン前メッセージや警告メッセージを表示したり、セキュリティ関連のクライアント接続オプションを設定したりすることができます。

### Horizon Console でのクライアント セッションのグローバル設定

全般的なグローバル設定では、セッション タイムアウトの長さ、SSO の有効性とタイムアウト制限、Horizon Console でのステータス更新を設定します。また、ログイン前メッセージや警告メッセージを表示するかどうか、Horizon Console が Windows Server をリモート デスクトップ用にサポートされるオペレーティング システムとして扱うかどうかなども設定できます。

以下の表の設定の変更はただちに有効になります。Horizon 7 Connection Server または Horizon Client の再起動は不要です。

表 3-2. クライアント セッションの全般的なグローバル設定

設定	説明
[View Administrator セッション タイムアウト]	<p>セッションがタイムアウトする前にアイドル状態の Horizon Console セッションがどれだけ続くかを決定します。</p> <p><b>重要:</b> Horizon Console セッション タイムアウトを長く設定すると、Horizon Console が不正に使用されるリスクが増大します。アイドル状態のセッションを長時間許可する場合は用心してください。</p> <p>デフォルトでは、Horizon Console セッション タイムアウトは 30 分です。セッション タイムアウトは 1 分から 4320 分（72 時間）の間で設定できます。</p>
[ユーザーの強制切断]	<p>ユーザーが Horizon 7 にログインしてから指定した時間（分）が経過すると、すべてのデスクトップとアプリケーションが切断されます。すべてのデスクトップとアプリケーションは、ユーザーがそれらをいつ開いたかにかかわらず同時に切断されます。</p> <p>アプリケーションのリモート処理をサポートしないクライアントでは、この設定の値が [なし] または 1200 分よりも長い場合、最大タイムアウト値である 1200 分が適用されます。</p> <p>デフォルトは、[600 分後] です。</p>
[シングル サインオン (SSO)]	<p>SSO が有効な場合、Horizon 7 にはユーザーの認証情報がキャッシュされるため、ユーザーは Windows リモート セッションにログインするための認証情報を指定せずにリモート デスクトップまたはアプリケーションを起動できます。デフォルトは [有効化] です</p> <p>Horizon 7 以降で導入されている True SSO 機能を使用する場合は、SSO を有効にする必要があります。True SSO では、ユーザーが Active Directory 認証情報以外の認証形式を使用してログインする場合、ユーザーが VMware Identity Manager にログインした後に、キャッシュされた認証情報ではなく短期間の証明書が True SSO 機能によって生成されます。</p> <p><b>注:</b> デスクトップが Horizon Client から起動し、セキュリティ ポリシーに基づきユーザーまたは Windows のいずれかによりロックされた場合、デスクトップで Horizon 7 Agent 6.0 以降または Horizon Agent 7.0 以降が実行されている場合は、Horizon 7 Connection Server はユーザーの SSO 認証情報を破棄します。ユーザーはログイン認証情報を指定して新しいデスクトップまたは新しいアプリケーションを起動するか、または切断されたデスクトップまたはアプリケーションに再接続する必要があります。SSO を再度有効にするには、Horizon 7 Connection Server から切断するか、または Horizon Client を終了し、Horizon 7 Connection Server に再接続する必要があります。ただし、デスクトップが Workspace ONE または VMware Identity Manager から起動してロックされている場合、SSO 認証情報は破棄されません。</p>
[ステータスの自動更新を有効にする]	<p>ステータスの更新が、Horizon Console の左上隅にあるグローバル ステータス ペインに数分ごとに表示されるかどうかを指定します。また、Horizon Console のダッシュボード ページも数分ごとに更新されます。</p> <p>デフォルトでは、この設定は有効になっていません。</p>



設定	説明
<p>[アプリケーションをサポートするクライアント。]</p> <p>[ユーザーがキーボードとマウスを使用しなくなった場合に、アプリケーションを切断し、SSO 認証情報を破棄する:]</p>	<p>クライアント デバイスで、キーボードやマウスが使用されなくなった場合にアプリケーション セッションを保護します。[経過時間...分] に設定した場合、指定された時間 (分) ユーザーのアクティビティがないと、Horizon 7 により、すべてのアプリケーションが切断され、SSO 認証情報は破棄されます。デスクトップセッションは切断されません。ユーザーは、再度ログインして切断されたアプリケーションに再接続するか、新しいデスクトップまたはアプリケーションを起動する必要があります。</p> <p>この設定は True SSO 機能にも適用されます。SSO 認証情報が破棄されると、ユーザーは Active Directory 認証情報の入力を求められます。ユーザーが Active Directory 認証情報を使用せずに VMware Identity Manager にログイン済みで、入力すべき Active Directory 認証情報がわからない場合は、ログアウトしてから VMware Identity Manager にログインし直してリモート デスクトップとアプリケーションにアクセスできます。</p> <p><b>重要:</b> アプリケーションとデスクトップの両方が開いて、タイムアウトによりアプリケーションが切断されている場合でも、デスクトップは接続されたままになることを認識しておく必要があります。ユーザーはデスクトップの保護のためにこのタイムアウトに依存することがないようにしてください。</p> <p>[なし] に設定すると、ユーザーのアクティビティがなくても、Horizon 7 によるアプリケーションの切断や SSO 認証情報の破棄は行われません。</p> <p>デフォルトは [なし] です。</p>
<p>[その他のクライアント。]</p> <p>[SSO 認証情報の破棄:]</p>	<p>指定した時間 (分) が経過すると、SSO 認証情報は破棄されます。この設定は、アプリケーションのリモート処理をサポートしていないクライアント用です。[経過時間...分] に設定した場合、クライアント デバイスでのユーザー アクティビティにかかわらず、Horizon 7 でログイン後指定時間 (分) が経過したら、ユーザーはデスクトップへ再度ログインしてデスクトップに接続する必要があります。</p> <p>[なし] に設定すると、ユーザーが Horizon Client を閉じるまで、または [ユーザーの強制切断] タイムアウトに達するまで、このどちらが先であっても、Horizon 7 は SSO 認証情報を保存します。</p> <p>デフォルトは、[15 分後] です。</p>
[ログイン前メッセージを表示する]	<p>Horizon Client ユーザーがログインしたときに免責事項または別のメッセージを表示します。</p> <p>[グローバル設定] ダイアログ ボックスのテキスト ボックスに情報または指示を入力します。</p> <p>メッセージを表示しない場合は、チェック ボックスをオフのままにします。</p>
[強制的にログオフする前に警告を表示する]	<p>スケジュール設定された更新や、デスクトップの更新操作などの即座の更新が開始されようとしているためにユーザーが強制的にログオフされる場合、警告メッセージを表示します。この設定では、警告を表示してからユーザーがログオフするまでの待機時間も指定します。</p> <p>警告メッセージを表示するにはチェック ボックスをオンにします。</p> <p>警告を表示してからユーザーがログオフするまでの待機時間を分単位で入力します。デフォルトは 5 分です。</p> <p>警告メッセージを入力します。次のデフォルト メッセージを使用できます。</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>お使いのデスクトップは、重要なアップデートがスケジュールされているため、5 分後にシャットダウンされます。保存していない作業を今すぐ保存してください。</p> </div>
[Windows Server デスクトップを有効にする]	<p>デスクトップとして使用できる Windows Server 2008 R2 および Windows Server 2012 R2 マシンを選択できるかどうかを指定します。この設定が有効な場合、Horizon Console では、Horizon 7 Server コンポーネントがインストールされているマシンを含む、使用可能なすべての Windows Server マシンが表示されます。</p> <p><b>注:</b> Horizon Agent ソフトウェアは、セキュリティ サーバ、Horizon 7 Connection Server、Horizon 7 Composer を含む他の Horizon 7 Server 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>



設定	説明
[HTML Access のタブを閉じるときに認証情報をクリーンアップする]	<p>リモート デスクトップやアプリケーションに接続するタブや、HTML Access クライアントのデスクトップとアプリケーションの選択ページに接続するタブをユーザーが閉じるときに、キャッシュからユーザーの認証情報を削除します。</p> <p>この設定が有効である場合、Horizon 7 は、次の HTML Access クライアントのシナリオにおいても認証情報をキャッシュから削除します。</p> <ul style="list-style-type: none"> <li>■ ユーザーが、デスクトップおよびアプリケーションの選択ページやリモート セッション ページを更新する。</li> <li>■ サーバから自己署名証明書が提示されており、ユーザーがリモート デスクトップやアプリケーションを起動し、セキュリティの警告が表示されるときにユーザーがその証明書を受け入れる。</li> <li>■ リモート セッションが含まれるタブで URI コマンドをユーザーが実行する。</li> </ul> <p>この設定が無効である場合、証明書はキャッシュに残ります。デフォルトでは、この機能は無効になっています。</p> <p><b>注:</b> この機能は、Horizon 7 バージョン 7.0.2 以降で利用できます。</p>
[クライアントのユーザー インターフェイスでサーバ情報を非表示]	<p>このセキュリティ設定を有効にして、Horizon Client 4.4 以降でサーバの URL 情報を非表示にします。</p>
[クライアントのユーザー インターフェイスでドメイン リストを非表示]	<p>このセキュリティ設定を有効にして、Horizon Client 4.4 以降で [ドメイン] ドロップダウン メニューを非表示にします。</p> <p>[クライアントのユーザー インターフェイスでドメイン リストを非表示] グローバル設定が有効になっている Connection Server にユーザーがログインすると、ドメイン ドロップダウン メニューが Horizon Client で非表示になり、ユーザーはドメイン情報を Horizon Client の [ユーザー名] テキスト ボックスに指定する必要があります。たとえば、ユーザー名を domain\username または username@domain の形式で入力する必要があります。</p> <p><b>重要:</b> [クライアントのユーザー インターフェイスでドメイン リストを非表示] 設定を有効にし、Connection Server インスタンスで 2 要素認証 (RSA SecureID または RADIUS) を選択している場合は、Windows ユーザー名の一致を強制しないでください。Windows ユーザー名の一致を強制すると、ユーザーは、ユーザー名のテキスト ボックスにドメイン情報を入力できなくなり、ログインが常に失敗します。単一ユーザー ドメインの場合、これは Horizon Client バージョン 5.0 以降に適用されません。</p> <p><b>重要:</b> この設定のセキュリティと操作性に対する影響については、『Horizon 7 のセキュリティ』を参照してください。</p>

## Horizon Console のクライアント セッションと接続のグローバル セキュリティ 設定

グローバル セキュリティ設定では、中断後にクライアントを再認証するかどうか、メッセージのセキュリティ モードを有効にするかどうか、セキュリティ ステータスを拡張するかどうかを設定します。

Horizon 7 に対するすべての Horizon Client 接続と Horizon Console 接続には、TLS が必要です。Horizon 7 の展開でロード バランサまたはその他のクライアントが接続する中間サーバが使用されている場合、TLS をそれらにオフロードしてから、それぞれの Connection Server インスタンスおよびセキュリティ サーバで非 TLS 接続を構成できます。

表 3-3. クライアント セッションおよび接続のグローバル セキュリティ 設定

設定	説明
[ネットワークへの割り込み後に安全なトンネル接続を再認証する]	<p>Horizon Client がリモート デスクトップへの安全なトンネル接続を使用する場合、ネットワークへの割り込み後にユーザー認証情報を再認証する必要があるかどうかを指定します。</p> <p>この設定を選択すると、安全なトンネル接続に割り込みが入った場合に、Horizon Client では再接続する前にユーザーの再認証が必要になります。</p> <p>この設定により、セキュリティが強化されます。たとえば、ラップトップが盗まれて別のネットワークに移動された場合、認証情報を入力しなければ、ユーザーはリモート デスクトップに自動的にアクセスできません。</p> <p>この設定を選択しない場合は、クライアントがリモート デスクトップに再接続するときに、ユーザーの再認証を要求しません。</p> <p>安全なトンネルが使用されていない場合、この設定は効果がありません。</p>
[メッセージ セキュリティ モード]	<p>コンポーネント間で JMS メッセージを送信するために使用されるセキュリティ メカニズムを指定します。</p> <ul style="list-style-type: none"> <li>■ モードが [有効] に設定されている場合、Horizon 7 コンポーネント間で渡される JMS メッセージの署名と検証が行われます。</li> <li>■ モードが [拡張済み] に設定されている場合、相互認証された TLS でセキュリティが提供されます。JMS 接続とアクセスは JMS トピックで制御されます。</li> </ul> <p>新規インストールの場合、メッセージ セキュリティ モードはデフォルトで [拡張済み] に設定されています。前のバージョンからアップグレードする場合は、前のバージョンで使用されていた設定が維持されます。</p>
[拡張セキュリティのステータス] (読み取り専用)	<p>[メッセージ セキュリティ モード] が [有効] から [拡張済み] に変更された場合に表示される読み取り専用フィールド。変更は段階的に行われるため、このフィールドにはフェーズを通じた進捗が表示されます。</p> <ul style="list-style-type: none"> <li>■ [MessageBus の再起動待機中] が最初のフェーズです。この状態は、手動でポッド内のすべての接続サーバインスタンスを再起動するか、ポッド内のすべての接続サーバホストの VMware Horizon Message Bus Component サービスを再起動するまで、表示されます。</li> <li>■ 次の段階は [拡張の保留] です。すべての Horizon Message Bus コンポーネント サービスが再起動されると、すべてのデスクトップ サーバおよびセキュリティ サーバに対して、システムはメッセージ セキュリティ モードを [拡張済み] に変更する処理を開始します。</li> <li>■ 最後の段階は [拡張済み] であり、すべてのコンポーネントが [拡張済み] メッセージ セキュリティ モードを使用するようになったことを示します。</li> </ul>

## Horizon Console での Horizon Connection Server の無効化または有効化

Connection Server インスタンスを無効にして、ユーザーが仮想または公開デスクトップやアプリケーションにログインできないようにすることができます。インスタンスを無効にした後、再度有効にすることができます。

Connection Server インスタンスを無効にしても、現在デスクトップやアプリケーションにログインしているユーザーは影響を受けません。

インスタンスを無効にするとユーザーがどのような影響を受けるかは、Horizon 7 の展開によって決まります。

- 単一でスタンドアロンの Connection Server インスタンスの場合、ユーザーはデスクトップまたはアプリケーションにログインできません。Connection Server に接続できません。

- これが複製された Connection Server インスタンスの場合は、ユーザーを別の複製されたインスタンスにルーティングできるかどうかはネットワーク トポロジによって決まります。別のインスタンスにアクセスできる場合、ユーザーはデスクトップやアプリケーションにログインできます。

#### 手順

- 1 Horizon Console で、[設定] - [サーバ] の順に選択します。
- 2 [Connection Server] タブで、Connection Server インスタンスを選択します。
- 3 [無効化] をクリックします。  
[有効化] をクリックすることによって、インスタンスを再び有効にすることができます。

## Horizon Connection Server インスタンスの外部 URL の編集

Horizon Console を使用して、Connection Server インスタンスの外部 URL を編集できます。

デフォルトでは、Connection Server ホストに接続できるクライアントは、同じネットワーク内に存在するトンネルクライアントだけです。ネットワークの外部で実行されているトンネル クライアントは、クライアントで解決できる URL を使用して Connection Server ホストに接続する必要があります。

ユーザーが PCoIP 表示プロトコルを使用してリモート デスクトップに接続した場合には、Horizon Client はさらに Connection Server ホスト上の PCoIP Secure Gateway に接続することができます。PCoIP Secure Gateway を使用するには、クライアント システムが Connection Server ホストに到達するための IP アドレスにアクセスする必要があります。この IP アドレスは PCoIP 外部 URL に指定します。

さらにもう 1 つは、Blast Secure Gateway 経由で安全な接続を行えるようにするための URL です。

安全なトンネルの外部 URL、PCoIP 外部 URL、および Blast 外部 URL は、このホストに到達するためにクライアント システムで使用されるアドレスでなければなりません。

#### 手順

- 1 Horizon Console で、[設定] - [サーバ] の順に選択します。
- 2 [Connection Server] タブで、Connection Server インスタンスを選択して [編集] をクリックします。
- 3 [外部 URL] テキスト ボックスに安全なトンネルの外部 URL を入力します。

URL には、プロトコル、クライアントで解決可能なホスト名、およびポート番号が含まれている必要があります。

例 : `https://horizon.example.com:443`

---

**注:** ホスト名が解決できないときに Connection Server インスタンスにアクセスする必要がある場合は、IP アドレスを使用できます。ただし、通信するホストは、Connection Server インスタンスに対して構成された TLS 証明書に一致しないため、アクセスがブロックされたりアクセスのセキュリティが低下したりします。

---

- 4 [PCoIP 外部 URL] テキスト ボックスに、PCoIP Secure Gateway の外部 URL を入力します。  
PCoIP 外部 URL は、IP アドレスとポート番号 4172 の組み合わせとして指定します。プロトコル名は含めないでください。

例：10.20.30.40:4172

URL には、クライアント システムがこの Connection Server インスタンスに到達する際に使用できる IP アドレスとポート番号を含める必要があります。

- 5 [Blast 外部 URL] テキスト ボックスに Blast Secure Gateway の外部 URL を入力します。

URL には、HTTPS プロトコル、クライアントが解決可能なホスト名、およびポート番号が含まれている必要があります。

例：https://myserver.example.com:8443

デフォルトでは、URL には安全なトンネル外部 URL の FQDN およびデフォルトのポート番号 8443 が含まれます。URL には、このホストに到達するためにクライアント システムで使用できる FQDN とポート番号を含める必要があります。

- 6 このダイアログのすべてのアドレスでクライアント システムがこのホストに到達できることを確認します。

- 7 [OK] をクリックして変更を保存します。

外部 URL はすぐに更新されます。変更を有効にするために Connection Server を再起動する必要はありません。

## Horizon Console でのゲートウェイの登録

Horizon Client は、Horizon Console で登録したゲートウェイまたは Unified Access Gateway アプライアンスを介して接続します。

Horizon Console で、ゲートウェイの登録または登録解除ができます。ゲートウェイの登録を解除するには、ゲートウェイまたは Unified Access Gateway アプライアンスを選択して、[登録解除] をクリックします。

### 手順

- 1 Horizon Console で、[設定] - [サーバ] の順に選択します。
- 2 [ゲートウェイ] タブで [登録] をクリックします。
- 3 ゲートウェイまたは Unified Access Gateway アプライアンスの FQDN を入力します。
- 4 [OK] をクリックします。

## スマート カード認証の設定

セキュリティを強化するため、ユーザーと管理者がスマート カードを使用して認証できるように、接続サーバインスタンスまたはセキュリティ サーバを構成できます。

スマート カードは、コンピュータ チップを搭載した小型のプラスチック カードです。ミニチュア コンピュータのようなこのチップは、秘密鍵および公開鍵の証明書など、データの安全なストレージを備えています。米国国防省が使用するスマート カードの 1 種には、Common Access Card (CAC) というカードがあります。

スマート カード認証では、クライアント コンピュータに接続されたスマート カード リーダにユーザーまたは管理者がスマート カードを差し込み、PIN を入力します。スマート カード認証は、個人が持っているもの（スマート カード）と個人が知っていること (PIN) の両方を検証することによって、2 要素認証を提供します。

スマート カード認証を実装するためのハードウェア要件およびソフトウェア要件については、『Horizon 7 のインストール』を参照してください。Microsoft TechNet の Web サイトでは、Windows システム用にスマート カード認証を計画して実装する方法についての詳細情報が提供されています。

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

この章には、次のトピックが含まれています。

- スマート カードを使用したログイン
- Horizon 接続サーバでのスマート カード認証の構成
- サードパーティ製ソリューションでのスマート カード認証の設定
- スマート カード認証用の Active Directory を準備する
- Horizon Console でのスマート カード認証の設定の検証
- スマート カードでの証明書失効チェックの使用

### スマート カードを使用したログイン

ユーザーまたは管理者がスマート カード リーダにスマート カードを差し込むと、クライアント オペレーティング システムが Windows の場合、スマート カードのユーザー証明書がクライアント システムのローカル証明書ストアにコピーされます。ローカル証明書ストアの証明書は、Horizon Client を含め、クライアント コンピュータ上で実行されているすべてのアプリケーションで利用可能です。

スマート カード認証が構成されている Connection Server インスタンスまたはセキュリティ サーバへの接続をユーザーまたは管理者が開始すると、信頼された認証局 (CA) のリストがその Connection Server インスタンスまたはセキュリティ サーバからクライアント システムに送信されます。クライアント システムは信頼された CA のリストを使用可能なユーザー 証明書と照合し、適切な証明書を選択してから、ユーザーまたは管理者にスマート カード PIN の入力を要求します。有効なユーザー 証明書が複数ある場合、クライアント システムはユーザーまたは管理者に証明書の選択を求めます。

そのユーザー 証明書がクライアント システムから Connection Server インスタンスまたはセキュリティ サーバに送信され、証明書の信頼および有効期間を確認することによって証明書が検証されます。一般に、ユーザー 証明書が署名されていて有効であれば、ユーザーおよび管理者は正常に認証されます。証明書失効チェックが構成されている場合、失効した証明書を持つユーザーまたは管理者は認証できません。

環境によっては、ユーザーのスマート カード証明書を複数の Active Directory ドメインのユーザー アカウントにマップできます。ユーザーは管理者権限のある複数のアカウントを持っている場合がありますが、その場合、スマート カードでログインするときの [ユーザー名のヒント] フィールドで使用するアカウントを指定する必要があります。Horizon Client のログイン ダイアログ ボックスに [ユーザー名のヒント] フィールドを表示するには、管理者が Horizon Console の Connection Server インスタンスでスマート カード ユーザー名のヒント機能を有効にする必要があります。次に、スマート カード ユーザーは、スマート カードでログインするときに、[ユーザー名のヒント] フィールドにユーザー名または UPN を入力できます。

外部アクセスの安全を確保するために、お使いの環境で Unified Access Gateway アプライアンスを使用している場合、スマート カード ユーザー名のヒント機能をサポートするように、Unified Access Gateway アプライアンスを構成する必要があります。スマート カード ユーザー名のヒント機能は、Unified Access Gateway バージョン 2.7.2 以降でのみサポートされます。Unified Access Gateway アプライアンスでスマート カード ユーザー名のヒント機能を有効にする方法については、『Unified Access Gateway の導入および設定』ドキュメントを参照してください。

Horizon Client でのスマート カード認証では、表示プロトコルの切り替えがサポートされていません。Horizon Client でのスマート カードによる認証後に、表示プロトコルを変更するには、ユーザーはログオフして、再度ログインする必要があります。

## Horizon 接続サーバでのスマート カード認証の構成

スマート カード認証を構成するには、ルート証明書を取得してサーバ信頼ストア ファイルに追加し、接続サーバの構成プロパティを変更して、スマートカード認証を設定する必要があります。使用する環境によっては、追加の手順が必要になることがあります。

### 手順

#### 1 証明機関の証明書の取得

ユーザーまたは管理者が提示したスマート カード上のすべての信頼されたユーザー 証明書について、該当するすべての CA (証明機関) の証明書を取得する必要があります。これらの証明書にはルート証明書が含まれ、ユーザーのスマート カード証明書が中間証明機関によって発行された場合には中間証明書が含まれる場合があります。

## 2 Windows からの CA 証明書の取得

CA が署名したユーザー証明書またはそれを含むスマート カードがあり、Windows でルート証明書が信頼される場合は、そのルート証明書を Windows からエクスポートできます。ユーザー証明書の発行元が中間証明機関である場合は、その証明書をエクスポートできます。

## 3 サーバ信頼ストア ファイルへの CA 証明書の追加

信頼するすべてのユーザーおよび管理者のサーバ信頼ストア ファイルに、ルート証明書と中間証明書のいずれかまたは両方を追加する必要があります。接続サーバ インスタンスおよびセキュリティ サーバは、この情報を使用してスマート カード ユーザーおよび管理者を認証します。

## 4 Horizon Connection Server の構成プロパティの変更

スマート カード認証を有効にするには、Connection Server 構成プロパティを変更する必要があります。

## 5 Horizon Console でのスマート カードの設定

Horizon Console を使用して、スマート カード認証のさまざまなシナリオに対応する設定を指定できます。

# 証明機関の証明書の取得

ユーザーまたは管理者が提示したスマート カード上のすべての信頼されたユーザー証明書について、該当するすべての CA（証明機関）の証明書を取得する必要があります。これらの証明書にはルート証明書が含まれ、ユーザーのスマート カード証明書が中間証明機関によって発行された場合には中間証明書が含まれる場合があります。

ユーザーおよび管理者によって提示されたスマート カード上の証明書に署名した CA のルート証明書または中間証明書を持っていない場合、CA が署名したユーザー証明書またはそれを含むスマート カードから証明書をエクスポートできます。[Windows からの CA 証明書の取得](#)を参照してください。

### 手順

◆ CA の証明書は次のいずれかの発行元から取得します。

- Microsoft Certificate Services を実行する Microsoft IIS サーバ。Microsoft IIS のインストール、証明書の発行、および組織内での証明書配布の詳細については、Microsoft TechNet の Web サイトを参照してください。
- 信頼された CA の公開ルート証明書。これは、スマート カード インフラストラクチャがすでに使用されていて、スマート カードの配布および認証方法が標準化されている環境で最もよく利用されるルート証明書の発行元です。

# Windows からの CA 証明書の取得

CA が署名したユーザー証明書またはそれを含むスマート カードがあり、Windows でルート証明書が信頼される場合は、そのルート証明書を Windows からエクスポートできます。ユーザー証明書の発行元が中間証明機関である場合は、その証明書をエクスポートできます。



## 手順

- 1 ユーザー証明書がスマート カード上にある場合は、そのスマート カードをリーダに挿入して、ユーザー証明書を個人用ストアに追加します。

ユーザー証明書が個人用ストアに表示されない場合は、リーダ ソフトウェアを使用してユーザー証明書をファイルにエクスポートします。このファイルは、この操作の手順 4 で使用されます。

- 2 Internet Explorer で [ツール] - [インターネット オプション] を選択します。

- 3 [コンテンツ] タブで [証明書] をクリックします。

- 4 [個人] タブで、使用する証明書を選択し、[表示] をクリックします。

ユーザー証明書がリストに表示されない場合は、[インポート] をクリックして手動でファイルからインポートします。証明書がインポートされると、その証明書をリストから選択できます。

- 5 [証明のパス] タブで、ツリーの最上位にある証明書を選択して [証明書を表示] をクリックします。

ユーザー証明書が信頼階層の一部として署名されている場合は、署名する証明書が別の上位の証明書によって署名されていることがあります。親証明書（ユーザー証明書に実際に署名した証明書）をルート証明書として選択してください。場合によっては発行元が中間 CA となります。

- 6 [詳細] タブで [ファイルにコピー] をクリックします。

[証明書のエクスポート ウィザード] が表示されます。

- 7 [次へ] - [次へ] をクリックし、エクスポートするファイルの名前と場所を入力します。

- 8 [次へ] をクリックして、指定した場所にファイルをルート証明書として保存します。

## サーバ信頼ストア ファイルへの CA 証明書の追加

信頼するすべてのユーザーおよび管理者のサーバ信頼ストア ファイルに、ルート証明書と中間証明書のいずれかまたは両方を追加する必要があります。接続サーバ インスタンスおよびセキュリティ サーバは、この情報を使用してスマート カード ユーザーおよび管理者を認証します。

## 前提条件

- ユーザーまたは管理者が提示したスマート カード上の証明書への署名に使用したルート証明書または中間証明書を取得します。[証明機関の証明書の取得](#)および[Windows からの CA 証明書の取得](#)を参照してください。

---

**重要:** ユーザーのスマート カード証明書が中間証明機関によって発行された場合、これらの証明書には中間証明書が含まれることがあります。

---

- keytool ユーティリティが、接続サーバまたはセキュリティ サーバ ホストのシステム パスに追加されていることを確認します。詳細については、『Horizon 7 のインストール』ドキュメントを参照してください。

## 手順

- 1 接続サーバまたはセキュリティ サーバ ホストで、keytool ユーティリティを使用して、ルート証明書または中間証明書のいずれかまたは両方をサーバ信頼ストア ファイルにインポートします。

例 :

```
keytool -import -alias alias -file root_certificate -keystore truststorefile.key
```



このコマンドでは、*alias* は信頼ストア ファイル内の新しいエントリの大文字と小文字を区別する一意の名前で、*root\_certificate* は取得またはエクスポートしたルート証明書または中間証明書です。また、*truststorefile.key* はルート証明書の追加先の信頼ストア ファイルの名前です。ファイルが存在しない場合、現在のディレクトリに作成されます。

---

**注:** `keytool` ユーティリティによって、信頼ストア ファイルのパスワードの作成を求められる場合があります。後で信頼ストア ファイルにさらに証明書を追加する必要がある場合は、このパスワードの入力が求められます。

---

- 2 接続サーバまたはセキュリティ サーバ ホストの SSL ゲートウェイ構成フォルダに、信頼ストア ファイルをコピーします。

例: `install_directory\VMware\VMware View\Server\sslgateway\conf\truststorefile.key`

#### 次のステップ

接続サーバの構成プロパティを変更して、スマート カード認証を有効にします。

## Horizon Connection Server の構成プロパティの変更

スマート カード認証を有効にするには、Connection Server 構成プロパティを変更する必要があります。

#### 前提条件

信頼されたすべてのユーザー証明書の CA（認証局）証明書をサーバ信頼ストア ファイルに追加します。これらの証明書にはルート証明書が含まれ、ユーザーのスマート カード証明書が中間認証局によって発行された場合には中間証明書が含まれる場合があります。

#### 手順

- 1 Connection Server ホスト上で、TLS/SSL ゲートウェイ構成フォルダ内の `locked.properties` ファイルを作成または編集します。  
 例: `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`
- 2 `locked.properties` ファイルに `trustKeyfile`、`trustStoretype`、および `useCertAuth` プロパティを追加します。
  - a `trustKeyfile` に信頼ストア ファイルの名前を設定します。
  - b `trustStoretype` に **jks** を設定します。
  - c `useCertAuth` に **true** を設定して、証明書認証を有効にします。
- 3 Connection Server サービスを再起動して、変更を有効にします。

## 例：locked.properties ファイル

例に示すファイルでは、すべての信頼されたユーザーのルート証明書がある場所としてファイル `lonqa.key` が指定され、信頼ストアのタイプが `jks` に設定され、証明書認証が有効になります。

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
```

### 次のステップ

Connection Server インスタンスでスマート カード認証を構成した場合は、Horizon Console でスマート カード認証の設定をします。

## Horizon Console でのスマート カードの設定

Horizon Console を使用して、スマート カード認証のさまざまなシナリオに対応する設定を指定できます。

### 前提条件

- Connection Server ホストの Connection Server 構成プロパティを変更します。
- Horizon Client が Connection Server またはセキュリティ サーバのホストに対して HTTPS 接続を直接確立していることを確認します。TLS を中間デバイスにオフロードしている場合、スマート カード認証はサポートされません。

### 手順

- 1 Horizon Console で、[設定] - [サーバ] の順に選択します。
- 2 [Connection Server] タブで、Connection Server インスタンスを選択して [編集] をクリックします。

### 3 リモート デスクトップ ユーザーおよびアプリケーション ユーザーのスマート カード認証を構成するには、次の手順を実行します。

- a [認証] タブで、[Horizon 認証] セクションの [ユーザー用スマート カード認証] ドロップダウン メニューから設定オプションを選択します。

オプション	アクション
不許可	Connection Server インスタンスでのスマート カード認証が無効になります。
Optional	ユーザーはスマート カード認証またはパスワード認証を使用して Connection Server インスタンスに接続できます。スマート カード認証が失敗した場合、ユーザーはパスワードを入力する必要があります。
Required	<p>Connection Server インスタンスに接続するときにユーザーはスマート カード認証を使用する必要があります。</p> <p>スマート カード認証が必須の場合は、Connection Server インスタンスに接続する際に [現在のユーザーとしてログイン] チェック ボックスをオンにしたユーザーの認証が失敗します。これらのユーザーは、Connection Server にログインする際にスマート カードと PIN を使用して再認証する必要があります。</p> <p><b>注:</b> スマート カード認証を設定すると、Windows パスワード認証は利用できなくなりますが、他の認証は利用できます。SecurID が有効になっている場合は、ユーザーは SecurID とスマート カード認証の両方による認証を求められます。</p>

- b スマート カード取り外しポリシーを構成します。

スマート カード認証が [不許可] に設定されている場合は、スマート カード取り外しポリシーを構成できません。

オプション	アクション
ユーザーがスマート カードを取り外したら、Connection Server からユーザーを切断する。	[スマート カードを取り出すときはユーザー セッションを切断します] チェック ボックスをオンにします。
ユーザーがスマート カードを取り外しても Connection Server への接続を維持して、再認証しなくても新しいデスクトップまたはアプリケーション セッションを開始できるようにします。	[スマート カードを取り出すときはユーザー セッションを切断します] チェック ボックスをオフにします。

ユーザーが [現在のユーザーとしてログイン] チェック ボックスをオンにして Connection Server インスタンスに接続している場合は、スマート カードでクライアント システムにログインしている場合であっても、スマート カード取り外しポリシーは適用されません。

- c スマート カードのユーザー名のヒント機能を構成する。

スマート カード認証が [不許可] に設定されている場合は、スマート カードのユーザー名のヒント機能を構成できません。

オプション	アクション
ユーザーが 1 つのスマート カード証明書を 使用して、複数のユーザー アカウントを認証 できるようにする。	[スマート カード ユーザー名のヒントを許可します] チェック ボックスをオンにします。
ユーザーが 1 つのスマート カード証明書を 使用して、複数のユーザー アカウントを認証 できないようにする。	[スマート カード ユーザー名のヒントを許可します] チェック ボックスをオフにします。

- 4 Horizon Console へのログインで管理者が使用するスマート カード認証を設定するには、[Horizon Administrator 認証] セクションで [管理者用スマート カード認証] ドロップダウン メニューから設定オプションを選択します。

オプション	アクション
不許可	Connection Server インスタンスでのスマート カード認証が無効になります。
Optional	管理者はスマート カード認証またはパスワード認証を使用して Horizon Console にログインできます。スマート カード認証が失敗した場合、管理者はパスワードを入力する必要があります。
Required	管理者は Horizon Console にログインするときにスマート カード認証を使用する必要があります。

- 5 [OK] をクリックします。

- 6 Connection Server サービスを再起動します。

スマート カードの設定に対する変更を反映するには、Connection Server サービスを再起動する必要があります。1 つだけ例外があります。スマート カード認証の設定は、Connection Server サービスを再起動せずに、[オプション] と [必須] の間で変更できます。

スマート カードの設定を変更しても、現在ログインしているユーザーおよび管理者に影響はありません。

#### 次のステップ

必要に応じて、スマート カード認証のために Active Directory を準備します。 [スマート カード認証用の Active Directory を準備する](#) を参照してください。

スマート カード認証の構成を検証します。 [Horizon Console でのスマート カード認証の設定の検証](#) を参照してください。

## サードパーティ製ソリューションでのスマート カード認証の設定

ロード バランサやゲートウェイなどのサードパーティ製ソリューションは、スマート カードの X.509 証明書と暗号化された PIN が含まれる SAML アサーションを渡すことで、スマート カード認証を実行できます。

このトピックでは、証明書がパートナ デバイスによって検証された後に関連する X.509 証明書を Connection Server に提供するためのサードパーティ製ソリューションの設定に伴うタスクについて概説します。この機能では SAML 認証を使用するため、タスクの 1 つとして Horizon Console で SAML 認証子を作成します。

Unified Access Gateway でのスマート カード認証の設定については、『Unified Access Gateway』を参照してください。

### 手順

- 1 サードパーティ製ゲートウェイまたはロード バランサ用の SAML 認証子を作成します。  
[Horizon Console での SAML 認証子の設定](#)を参照してください。
- 2 Connection Server のメタデータの有効期間を延長して、リモート セッションが 24 時間経過後に終了されないようにします。  
[Connection Server でのサービス プロバイダ メタデータの有効期間の変更](#)を参照してください。
- 3 必要に応じて、Connection Server からサービス プロバイダのメタデータを使用するようにサードパーティ製デバイスを構成します。  
 サードパーティ製デバイスの製品ドキュメントを参照してください。
- 4 サードパーティ製デバイスでスマート カード設定を構成します。  
 サードパーティ製デバイスの製品ドキュメントを参照してください。

## スマート カード認証用の Active Directory を準備する

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

### ■ スマート カード ユーザーの UPN を追加する

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

### ■ Enterprise NTAAuth ストアにルート証明書を追加する

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

### ■ 信頼されたルート証明機関へのルート証明書の追加

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

## ■ 中間証明機関への中間証明書の追加

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

## スマート カード ユーザーの UPN を追加する

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

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

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

### 前提条件

- 証明書のプロパティを表示して、信頼された CA のルート証明書に含まれる SAN を取得します。
- Active Directory サーバに ADSI Edit ユーティリティがない場合は、Microsoft の Web サイトから適切な Windows Support Tools をダウンロードし、インストールします。

### 手順

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

## Enterprise NTAAuth ストアにルート証明書を追加する

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

### 手順

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

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

CA がこの種の証明書の発行元として信頼されるようになります。

## 信頼されたルート証明機関へのルート証明書の追加

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

### 手順

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

Active Directory のバージョン	ナビゲーション パス
Windows 2003	<ol style="list-style-type: none"> <li>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。</li> <li>b ドメインを右クリックして、[プロパティ] をクリックします。</li> <li>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。</li> <li>d [既定のドメイン ポリシー] を右クリックし、[編集] をクリックします。</li> </ol>
Windows 2008	<ol style="list-style-type: none"> <li>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。</li> <li>b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。</li> </ol>
Windows 2012 R2	<ol style="list-style-type: none"> <li>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。</li> <li>b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。</li> </ol>
Windows 2016	<ol style="list-style-type: none"> <li>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。</li> <li>b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。</li> </ol>

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

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

### 次のステップ

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

## 中間証明機関への中間証明書の追加

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

## 手順

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

Active Directory のバージョン	ナビゲーションパス
Windows 2003	<ol style="list-style-type: none"> <li>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。</li> <li>b ドメインを右クリックして、[プロパティ] をクリックします。</li> <li>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。</li> <li>d [既定のドメイン ポリシー] を右クリックし、[編集] をクリックします。</li> </ol>
Windows 2008	<ol style="list-style-type: none"> <li>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。</li> <li>b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。</li> </ol>
Windows 2012 R2	<ol style="list-style-type: none"> <li>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。</li> <li>b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。</li> </ol>
Windows 2016	<ol style="list-style-type: none"> <li>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。</li> <li>b ドメインを展開し、[デフォルト ドメイン ポリシー] を右クリックして、[編集] をクリックします。</li> </ol>

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

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

## Horizon Console でのスマート カード認証の設定の検証

スマート カード認証を初めて設定したとき、またはスマート カード認証が正しく動作しないときは、スマート カード認証の構成を検証する必要があります。

## 手順

- ◆ 各クライアントシステムに、スマート カード ミドルウェア、スマート カードとその有効な証明書、およびスマート カード リーダがあることを確認します。エンド ユーザーについては、Horizon Client を所有しているかを確認します。

スマート カードのソフトウェアとハードウェアの構成方法については、スマート カード ベンダから提供されているマニュアルを参照してください。



- ◆ 各クライアント システムで、[スタート] - [設定] - [コントロール パネル] - [インターネット オプション] - [コンテンツ] - [証明書] - [個人] を選択し、スマート カード認証に証明書が使用できることを確認します。

ユーザーまたは管理者がスマート カード リーダにスマート カードを差し込むと、Windows によって証明書がスマート カードからユーザーのコンピュータにコピーされます。クライアント システム上のアプリケーション (Horizon Client を含む) は、これらの証明書を使用できます。

- ◆ Connection Server またはセキュリティ サーバ ホストの `locked.properties` ファイルで、`useCertAuth` プロパティが **true** に設定されていて、スペルが正しいことを確認します。

`locked.properties` ファイルは `install_directory\VMware\VMware View\Server\sslgateway\conf` にあります。`useCertAuth` プロパティのスペルを `userCertAuth` と誤ることがよくあります。

- ◆ Connection Server インスタンスでスマート カード認証を設定した場合は、Horizon Console でスマート カード認証の設定を確認します。

a [設定] - [サーバ] の順に選択します。

b [Connection Server] タブで、Connection Server インスタンスを選択して [編集] をクリックします。

c ユーザーのスマート カード認証を構成した場合は、[認証] タブで、[ユーザー用スマート カード認証] が [オプション] または [必須] に設定されていることを確認します。

d 管理者のスマート カード認証を構成した場合は、[認証] タブで、[管理者用スマート カード認証] が [オプション] または [必須] に設定されていることを確認します。

スマート カードの設定に対する変更を反映するには、Connection Server サービスを再起動する必要があります。

- ◆ スマート カード ユーザーが属しているドメインが、ルート証明書が発行されたドメインとは異なる場合は、ユーザーの UPN が、信頼された CA のルート証明書に含まれる SAN に設定されていることを確認します。

a 証明書のプロパティを表示して、信頼された CA のルート証明書に含まれる SAN を調べます。

b Active Directory サーバで、[スタート] - [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。

c [ユーザー] フォルダでユーザーを右クリックし、[プロパティ] を選択します。

[アカウント] タブの [ユーザー ログオン名] テキスト ボックスに、UPN が表示されます。

- ◆ スマート カード ユーザーが PCoIP 表示プロトコルまたは VMware Blast 表示プロトコルを選択して、シングルセッション デスクトップに接続する場合は、Smartcard リダイレクトという名前の Horizon Agent コンポーネントが単一ユーザー マシンにインストールされていることを確認します。スマート カード機能を使用すると、ユーザーはスマート カードを使用してシングルセッション デスクトップにログインできます。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た RDS ホストでは、スマート カード機能が自動的にサポートされるため、この機能をインストールする必要はありません。

- ◆ Connection Server またはセキュリティ サーバ ホストの `drive:\Documents and Settings\All Users\Application Data\VMware\VDM\logs` にあるログ ファイルで、スマートカード認証が有効であることを示すメッセージを確認します。

## スマート カードでの証明書失効チェックの使用

証明書失効チェックを構成すると、失効したユーザー証明書を持つユーザーがスマート カードを使用して認証されるのを回避できます。証明書は、ユーザーが組織を離れたとき、スマート カードを紛失したとき、別の部門に異動したときなどに失効します。

Horizon 7 は、証明書失効リスト (CRL) およびオンライン証明書状態プロトコル (OCSP) による証明書失効チェックをサポートします。CRL は、証明書を発行した CA によって公開される、失効した証明書のリストです。OCSP は、X.509 証明書の失効ステータスを取得するために使用される証明書検証プロトコルです。

証明書失効チェックは、接続サーバ インスタンスまたはセキュリティ サーバ上で構成できます。接続サーバ インスタンスがセキュリティ サーバと対になっている場合は、セキュリティ サーバ上で証明書失効チェックを構成します。認証局 (CA) は、接続サーバまたはセキュリティ サーバ ホストからアクセスできる必要があります。

同じ接続サーバ インスタンスまたはセキュリティ サーバ上で CRL と OCSP の両方を構成できます。両方のタイプの証明書失効チェックを構成すると、Horizon 7 は最初に OCSP の使用を試行し、OCSP に失敗すると CRL にフォールバックします。Horizon 7 は、CRL が失敗した場合、OCSP にフォールバックしません。

### ■ CRL チェックを使用したログイン

CRL チェックを構成すると、Horizon 7 によって CRL が構築されて読み取られ、ユーザー証明書の失効ステータスが判別されます。

### ■ OCSP による証明書失効チェックを使用したログイン

OCSP による証明書失効チェックを構成すると、特定のユーザー証明書の失効ステータスの判別を求める要求が Horizon 7 から OCSP レスポンドに送信されます。Horizon 7 では、OCSP 署名証明書を使用して、OCSP レスポンドから受信した応答が本物であることを確認します。

### ■ CRL チェックの構成

CRL チェックを構成すると、Horizon 7 によって CRL が読み取られ、スマート カードのユーザー証明書の失効ステータスが判別されます。

### ■ OCSP による証明書失効チェックの構成

OCSP による証明書失効チェックを構成すると、スマート カードにあるユーザー証明書の失効ステータスの判別を求める検証要求が Horizon 7 から OCSP レスポンドに送信されます。

### ■ スマート カードでの証明書失効チェックのプロパティ

`locked.properties` ファイル内の値を設定して、スマート カードでの証明書失効チェックを有効化および構成します。

## CRL チェックを使用したログイン

CRL チェックを構成すると、Horizon 7 によって CRL が構築されて読み取られ、ユーザー証明書の失効ステータスが判別されます。

証明書が失効していて、スマート カード認証がオプションになっている場合は、[Enter your user name and password (ユーザー名とパスワードを入力してください)] ダイアログ ボックスが表示され、ユーザーは認証のためにパスワードを入力する必要があります。スマート カード認証が必須の場合は、エラー メッセージが表示され、ユーザーの認証が許可されません。Horizon 7 が CRL を読み取ることができない場合にも、同じイベントが発生します。

## OCSP による証明書失効チェックを使用したログイン

OCSP による証明書失効チェックを構成すると、特定のユーザー証明書の失効ステータスの判別を求める要求が Horizon 7 から OCSP レスポンダに送信されます。Horizon 7 では、OCSP 署名証明書を使用して、OCSP レスポンダから受信した応答が本物であることを確認します。

ユーザー証明書が失効していて、スマート カード認証がオプションになっている場合は、[Enter your user name and password (ユーザー名とパスワードを入力してください)] ダイアログ ボックスが表示され、ユーザーは認証のためにパスワードを入力する必要があります。スマート カード認証が必須の場合は、エラー メッセージが表示され、ユーザーの認証が許可されません。

Horizon 7 は、OCSP レスポンダからの応答がない場合、または応答が無効な場合、CRL チェックにフォールバックします。

## CRL チェックの構成

CRL チェックを構成すると、Horizon 7 によって CRL が読み取られ、スマート カードのユーザー証明書の失効ステータスが判別されます。

### 前提条件

CRL チェックに使用される `locked.properties` ファイルのプロパティを理解しておきます。[スマート カードでの証明書失効チェックのプロパティ](#)を参照してください。

### 手順

- 1 接続サーバ ホストまたはセキュリティ サーバ ホスト上で、TLS/SSL ゲートウェイ構成フォルダ内の `locked.properties` ファイルを作成または編集します。  
  
例: `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`
- 2 `locked.properties` ファイルに `enableRevocationChecking` および `crlLocation` プロパティを追加します。
  - a `enableRevocationChecking` に **true** を設定して、スマート カードでの証明書失効チェックを有効にします。
  - b `crlLocation` に CRL の場所を設定します。この値には、URL またはファイル パスを指定できます。
- 3 変更を反映するため、接続サーバ サービスまたはセキュリティ サーバ サービスを再起動してください。

### 例: `locked.properties` ファイル

例に示すファイルでは、スマート カード認証とスマート カードでの証明書失効チェックが有効になり、CRL チェックが構成され、CRL の場所の URL が指定されます。

```
trustKeyfile=longa.key
trustStoretype=jks
useCertAuth=true
enableRevocationChecking=true
crlLocation=http://root.ocsp.net/certEnroll/ocsp-R00T_CA.crl
```

## OCSP による証明書失効チェックの構成

OCSP による証明書失効チェックを構成すると、スマート カードにあるユーザー証明書の失効ステータスの判別を求める検証要求が Horizon 7 から OCSP レスポンドに送信されます。

### 前提条件

OCSP による証明書失効チェックに使用される `locked.properties` ファイルのプロパティを理解しておきます。  
[スマート カードでの証明書失効チェックのプロパティ](#)を参照してください。

### 手順

- 1 接続サーバ ホストまたはセキュリティ サーバ ホスト上で、TLS/SSL ゲートウェイ構成フォルダ内の `locked.properties` ファイルを作成または編集します。  
  
例: `install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`
- 2 `locked.properties` ファイルに `enableRevocationChecking`、`enableOCSP`、`ocspURL`、`ocspSigningCert` プロパティを追加します。
  - a `enableRevocationChecking` に **true** を設定して、スマート カードでの証明書失効チェックを有効にします。
  - b `enableOCSP` に **true** を設定して、OCSP による証明書失効チェックを有効にします。
  - c `ocspURL` に OCSP レスポンドの URL を設定します。
  - d `ocspSigningCert` に OCSP レスポンドの署名証明書を含むファイルの場所を設定します。
- 3 変更を反映するため、接続サーバ サービスまたはセキュリティ サーバ サービスを再起動してください。

### 例: `locked.properties` ファイル

例に示すファイルでは、スマート カード認証およびスマート カードでの証明書失効チェックが有効になり、CRL と OCSP の両方の証明書失効チェックが構成され、OCSP レスポンドの場所が指定され、OCSP 署名証明書を含むファイルが特定されます。

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
enableRevocationChecking=true
enableOCSP=true
allowCertCRLs=true
ocspSigningCert=te-ca.signing.cer
ocspURL=http://te-ca.lonqa.int/ocsp
```

## スマート カードでの証明書失効チェックのプロパティ

`locked.properties` ファイル内の値を設定して、スマート カードでの証明書失効チェックを有効化および構成します。

[表 4-1. スマート カードでの証明書失効チェックのプロパティ](#)は、証明書取り消し確認用の `locked.properties` のファイル プロパティをリストします。

表 4-1. スマート カードでの証明書失効チェックのプロパティ

プロパティ	説明
enableRevocationChecking	<p>このプロパティを <b>true</b> に設定すると、証明書失効チェックが有効になります。</p> <p>このプロパティを <b>false</b> に設定すると、証明書失効チェックが無効になり、他のすべての証明書失効チェック プロパティが無視されます。</p> <p>デフォルト値は <b>false</b> です。</p>
crlLocation	<p>CRL の場所を指定します。URL またはファイル パスを指定できます。</p> <p>URL を指定しない場合、または指定した URL が無効な場合に、<b>allowCertCRLs</b> が <b>true</b> に設定されているか、または指定されていないと、Horizon 7 はユーザー証明書の CRL のリストを使用します。</p> <p>Horizon 7 が CRL にアクセスできない場合は、CRL チェックが失敗します。</p>
allowCertCRLs	<p>このプロパティを <b>true</b> に設定すると、Horizon 7 はユーザー証明書から CRL のリストを抽出します。</p> <p>デフォルト値は <b>true</b> です。</p>
enableOCSP	<p>このプロパティを <b>true</b> に設定すると、OCSP による証明書失効チェックが有効になります。</p> <p>デフォルト値は <b>false</b> です。</p>
ocspURL	OCSP レスポンドの URL を指定します。
ocspResponderCert	OCSP レスポンドの署名証明書を含むファイルを指定します。Horizon 7 では、この証明書を使用して、OCSP レスポンドから受信した応答が本物であることを確認します。
ocspSendNonce	<p>このプロパティを <b>true</b> に設定すると、応答の繰り返しを回避するために OCSP 要求とともにノンスが送信されます。</p> <p>デフォルト値は <b>false</b> です。</p>
ocspCRLFailover	<p>このプロパティを <b>true</b> に設定すると、Horizon 7 は OCSP 証明書失効チェックが失敗した場合に CRL チェックを使用します。</p> <p>デフォルト値は <b>true</b> です。</p>

## 他のタイプのユーザー認証の設定

Horizon 7 は、ユーザーおよび管理者を認証および管理するために既存の Active Directory インフラストラクチャを利用します。また、スマートカードに加え、バイオメトリクス認証や、RSA SecurID、RADIUS などの 2 要素認証ソリューションなど他の形式の認証と Horizon 7 を統合して、リモート デスクトップおよびアプリケーション ユーザーを認証することもできます。

この章には、次のトピックが含まれています。

- [2 要素認証の使用](#)
- [SAML 認証の使用](#)
- [バイオメトリクス認証の構成](#)

### 2 要素認証の使用

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

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

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

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

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

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

## ■ 2 要素認証を用いたログイン

RSA SecurID 認証または RADIUS 認証が有効になっている Connection Server インスタンスにユーザーが接続すると、Horizon Client に特別なログイン ダイアログ ボックスが表示されます。

## ■ Horizon Console での 2 要素認証の有効化

Horizon Console で Connection Server の設定を変更して、Connection Server インスタンスで RSA SecurID 認証または RADIUS 認証を有効にします。

## ■ RSA SecureID アクセス拒否のトラブルシューティング

Horizon Client が RSA SecurID 認証で接続すると、アクセスが拒否されます。

## ■ RADIUS アクセス拒否のトラブルシューティング

Horizon Client が RADIUS 2 要素認証で接続すると、アクセスが拒否されます。

## 2 要素認証を用いたログイン

RSA SecurID 認証または RADIUS 認証が有効になっている Connection Server インスタンスにユーザーが接続すると、Horizon Client に特別なログイン ダイアログ ボックスが表示されます。

ユーザーは、特別なログイン ダイアログ ボックスに RSA SecurID または RADIUS 認証ユーザー名とパスコードを入力します。通常、2 要素認証パスコードは PIN とそれに続くトークン コードで構成されます。

- RSA Authentication Manager で、ユーザーが RSA SecurID ユーザー名とパスコードを入力した後に、新しい RSA SecurID PIN の入力が必要な場合は、PIN ダイアログ ボックスが表示されます。新しい PIN を設定した後、ユーザーはログインする前に次のトークン コードを待つよう求められます。システムによって生成された PIN を使用するように RSA Authentication Manager が構成されている場合は、PIN を確認するためのダイアログ ボックスが表示されます。

- Horizon 7 にログインしているときは、RADIUS 認証は RSA SecurID とほとんど同じ働きをします。RADIUS サーバがアクセス チャレンジを発行すると、Horizon Client は次のトークン コードに対し RSA SecurID プロンプトに似たダイアログ ボックスを表示します。RADIUS チャレンジの現在のサポートは、テキスト入力に対するプロンプトの表示に限られます。RADIUS サーバから送信された、いかなるチャレンジ テキストも表示されません。複数の選択肢や画像の選択など、より複雑な形式のチャレンジは、現在サポートされていません。

ユーザーが認証情報を Horizon Client に入力すると、RADIUS サーバは SMS テキスト メッセージまたは電子メール、あるいは他のアウトオブバンド機能を使用してテキストを、コードと共にユーザーの携帯電話に送信できます。ユーザーはこのテキストおよびコードを Horizon Client に入力して、認証を完了することができます。

- RADIUS ベンダーによっては Active Directory からユーザーをインポートする機能が提供されるので、エンドユーザーは、RADIUS 認証ユーザー名およびパスコードを要求される前に、Active Directory 認証情報の入力を最初に要求される場合があります。

## Horizon Console での 2 要素認証の有効化

Horizon Console で Connection Server の設定を変更して、Connection Server インスタンスで RSA SecurID 認証または RADIUS 認証を有効にします。

## 前提条件

RSA SecurID ソフトウェアや RADIUS ソフトウェアなどの 2 要素認証ソフトウェアを、認証マネージャのサーバにインストールして構成します。

- RSA SecurID 認証の場合、**sdconf.rec** ファイルを RSA Authentication Manager から Connection Server インスタンスにエクスポートします。RSA Authentication Manager のドキュメントを参照してください。
- RADIUS 認証の場合、ベンダーの構成に関するドキュメントに従ってください。RADIUS サーバのホスト名または IP アドレス、RADIUS 認証をリスンしているポート番号（通常は 1812）、認証タイプ（PAP、CHAP、MS-CHAPv1 または MS-CHAPv2）、および共有シークレットを書き留めておきます。これらの値は、Horizon Console で入力します。値をプライマリおよびセカンダリ RADIUS 認証子に入力できます。

## 手順

- 1 Horizon Console で、[設定] - [サーバ] の順に移動します。
- 2 [Connection Server] タブで、Connection Server インスタンスを選択して [編集] をクリックします。
- 3 [認証] タブで、[高度な認証] セクションの [2 要素認証] ドロップダウン メニューから、[RSA SecureID] または [RADIUS] を選択します。
- 4 RSA SecurID ユーザー名または RADIUS ユーザー名を Active Directory 内のユーザー名と強制的に一致させるには、[SecurID と Windows のユーザー名を強制的に一致させる] または [2 要素認証と Windows ユーザー名の一致の確認を強制します] を選択します。

このオプションを選択した場合、ユーザーは Active Directory 認証にも同じ RSA SecurID ユーザー名または RADIUS ユーザー名を使用する必要があります。このオプションを選択しない場合は、名前が異なってもかまいません。

- 5 RSA SecurID の場合、[ファイルのアップロード] をクリックして **sdconf.rec** ファイルの場所を入力するか、[参照] をクリックしてファイルを検索します。



## 6 RADIUS 認証の場合、残りのフィールドを入力します。

- a 最初の RADIUS 認証が、トークン コードのアウトオブバンド伝送をトリガする Windows 認証を使用し、このトークン コードが RADIUS のチャレンジの一部として使用される場合、[RADIUS と Windows 認証には同じユーザー名とパスワードを使用します] を選択します。

このチェックボックスを選択すると、RADIUS 認証で Windows のユーザー名およびパスワードを使用している場合、RADIUS 認証後にユーザーは Windows 認証情報の入力を求められません。ユーザーは RADIUS 認証後、Windows ユーザー名およびパスワードを再入力する必要はありません。

- b [認証子] ドロップダウン メニューから、[新しい認証子の作成] を選択し、ページのすべての項目に入力します。
  - RADIUS アカウンティングを有効にする必要がない限り、[アカウンティング ポート] は [0] に設定します。RADIUS サーバがアカウンティング データの収集をサポートする場合に限り、このポートをゼロ以外の数字に設定します。RADIUS サーバがアカウンティング メッセージをサポートせず、このポートをゼロ以外の数字に設定すると、メッセージが送信されて無視され、何度も再試行された結果、認証が遅延します。

アカウンティング データは、利用時間およびデータに基づいた、ユーザーへの請求に使用できます。アカウンティング データは、統計目的および一般的なネットワーク監視にも使用することができます。

- レルムのプリフィックス文字列を指定すると、RADIUS サーバに送られるときに、その文字列がユーザー名の先頭に配置されます。たとえば、Horizon Client に入力されたユーザー名が **jdoe** で、レルムのプリフィックス **DOMAIN-A\** が指定された場合、ユーザー名 **DOMAIN-A\jdoe** が RADIUS サーバに送信されます。同様に、レルムのサフィックスまたはポストフィックスに文字列 **@mycorp.com** を使用する場合、ユーザー名 **jdoe@mycorp.com** が RADIUS サーバに送信されます。

## 7 [OK] をクリックして変更を保存します。

Connection Server サービスの再起動は不要です。必要な構成ファイルが自動的に配布され、構成の設定がすぐに有効になります。

ユーザーが Horizon Client を開き、Connection Server へ認証する場合、2 要素認証が求められます。RADIUS 認証の場合、ログイン ダイアログ ボックスに、指定したトークンのラベルを含むテキスト プロンプトが表示されます。

RADIUS 認証設定への変更は、構成が変更された後で開始されるリモート デスクトップおよびアプリケーション セッションに影響を及ぼします。RADIUS 認証設定を変更しても、現在のセッションには影響ありません。

### 次のステップ

Connection Server インスタンスの複製されたグループがあり、そこでも RADIUS 認証を設定する場合、既存の RADIUS 認証子の構成を再利用することができます。

## RSA SecureID アクセス拒否のトラブルシューティング

Horizon Client が RSA SecurID 認証で接続すると、アクセスが拒否されます。

### 問題

RSA SecurID を使用した Horizon Client 接続で「アクセスが拒否されました」が表示され、RSA Authentication Manager Log Monitor にエラー「ノードの検証に失敗しました」が表示されます。

**原因**

RSA Agent ホスト ノードの秘密をリセットする必要があります。

**解決方法**

- 1 Horizon Console で、[設定] - [サーバ] の順に移動します。
- 2 [Connection Server] タブで、Connection Server インスタンスを選択して [編集] をクリックします。
- 3 [認証] タブで、[高度な認証] セクションの [2 要素認証] ドロップダウン メニューから、[RSA SecureID] を選択します。
- 4 [ノード シークレットをクリア] を選択して、[OK] をクリックします。
- 5 RSA Authentication Manager を実行しているコンピュータで、[スタート] - [RSA プログラム] - [RSA Security] - [RSA Authentication Manager ホスト モード] の順に選択します。
- 6 [エージェント ホスト] - [エージェント ホストの編集] の順に選択します。
- 7 リストから View Connection Server を選択し、[作成されたノードの秘密] チェック ボックスの選択を解除します。  
  
編集するときは、毎回デフォルトで [作成されたノードの秘密] が選択されます。
- 8 [OK] をクリックします。

## RADIUS アクセス拒否のトラブルシューティング

Horizon Client が RADIUS 2 要素認証で接続すると、アクセスが拒否されます。

**問題**

RADIUS 2 要素認証を使用して Horizon Client 接続を行うと、「アクセスが拒否されました」と表示されます。

**原因**

RADIUS は RADIUS サーバから応答を受け取ることができず、Horizon 7 がタイムアウトします。

次に、この状況を引き起こしやすい一般的な構成エラーを示します。

- Connection Server インスタンスを RADIUS クライアントとして受け入れるように RADIUS サーバが構成されていない。RADIUS を使用する各 Connection Server インスタンスは、RADIUS サーバでクライアントとして設定する必要があります。詳細は、RADIUS 2 要素認証製品のドキュメントを参照してください。
- Connection Server インスタンス上と RADIUS サーバ上の共有シークレット値が一致していない。

## SAML 認証の使用

Security Assertion Markup Language (SAML) は、さまざまなセキュリティ ドメイン間で認証情報および権限情報を記述および交換するための XML ベースの標準です。SAML は、ID プロバイダとサービス プロバイダ間において、SAML アサーションと呼ばれる XML ドキュメントでユーザーに関する情報の受け渡しを行います。

SAML 認証を使用して、Horizon 7 を VMware Workspace ONE、VMware Identity Manager、または認定のサードパーティ製ロード バランサ/ゲートウェイと統合できます。サードパーティ製デバイスの SAML を設定する場合は、ベンダーのドキュメントを参照して、Horizon 7 の設定方法を確認してください。SSO が有効になっている場合、VMware Identity Manager またはサードパーティ製のデバイスにログインしたユーザーは、第 2 のログイン手順を介さずにリモート デスクトップやアプリケーションを起動できます。SAML 認証を使用して、VMware Access Point またはサードパーティ製のデバイスにスマート カード認証を実装することもできます。

Workspace ONE、VMware Identity Manager、またはサードパーティ製のデバイスに認証の責任を委任するには、Horizon 7 で SAML 認証子を作成する必要があります。SAML 認証子には、Horizon 7 と Workspace ONE、VMware Identity Manager、またはサードパーティ製のデバイス間での信頼とメタデータの交換が含まれます。SAML 認証子を接続サーバ インスタンスと関連付けます。

## VMware Identity Manager 統合用の SAML 認証の使用

Horizon 7 と VMware Identity Manager (旧称 Workspace ONE) の統合では、SAML 2.0 標準を使用して、シングル サインオン (SSO) 機能に不可欠な相互信頼を確立します。SSO が有効になっている場合、Active Directory 認証情報を使用して VMware Identity Manager または Workspace ONE にログインしたユーザーは、第 2 のログイン手順を経ずにリモート デスクトップやアプリケーションを起動できます。

VMware Identity Manager と Horizon 7 が統合されている場合、ユーザーが VMware Identity Manager にログインしてデスクトップまたはアプリケーション アイコンをクリックするたびに、VMware Identity Manager は一意の SAML アーティファクトを生成します。VMware Identity Manager はこの SAML アーティファクトを使用して、Universal Resource Identifier (URI) を作成します。URI には、デスクトップ プールまたはアプリケーション プールが置かれている Connection Server インスタンス、起動するデスクトップまたはアプリケーション、および SAML アーティファクトについての情報が含まれます。

VMware Identity Manager は SAML アーティファクトを Horizon Client に送信し、その後、Connection Server インスタンスにアーティファクトを送信します。Connection Server インスタンスは SAML アーティファクトを使用して、VMware Identity Manager から SAML アサーションを取得します。

Connection Server インスタンスは SAML アサーションを受け取った後、アサーションを検証し、ユーザーのパスワードを復号化し、復号化されたパスワードを使用してデスクトップまたはアプリケーションを起動します。

VMware Identity Manager と Horizon 7 の統合の設定には、Horizon 7 の情報での VMware Identity Manager の構成、および VMware Identity Manager への認証責任を委任するための Horizon 7 の構成が含まれます。

VMware Identity Manager への認証責任を委任するには、Horizon 7 で SAML 認証を作成する必要があります。SAML 認証子には、Horizon 7 と VMware Identity Manager 間での信頼とメタデータの交換が含まれます。SAML 認証子を Connection Server インスタンスと関連付けます。

---

**注:** 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、Horizon Console 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、Horizon 7 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。

---

## Horizon Console での SAML 認証子の設定

リモート デスクトップおよびアプリケーションを VMware Identity Manager から起動するか、サードパーティ製ロード バランサまたはゲートウェイを通じてリモート デスクトップおよびアプリケーションを接続するには、Horizon Console で SAML 認証子を作成する必要があります。SAML 認証子には、Horizon 7 とクライアントが接続するデバイス間での信頼とメタデータの交換が含まれます。

SAML 認証子を Connection Server インスタンスと関連付けます。導入環境に複数の Connection Server インスタンスが含まれる場合は、各インスタンスに SAML 認証子を関連付ける必要があります。

1 つの静的認証子と複数の動的認証子を一度にライブにすることができます。vIDM（動的）および Unified Access Gateway（静的）の認証子を構成して、これらをアクティブ状態に保持できます。これらの認証子のいずれかを通じて接続を行うことができます。

Connection Server に複数の SAML 認証子を構成して、すべての認証子を同時にアクティブにできます。ただし、Connection Server で構成される各 SAML 認証子のエンティティ ID は異なっている必要があります。

SAML 認証子は本質的に静的な事前定義済みメタデータであるため、ダッシュボードでのステータスは常に緑色です。ステータスが赤色と緑色の間で切り替わるのは、動的認証子のみです。

VMware Unified Access Gateway アプライアンスの SAML 認証子の構成については、『Unified Access Gateway』を参照してください。

### 前提条件

- Workspace ONE、VMware Identity Manager またはサードパーティ製のゲートウェイまたはロード バランサがインストールされて構成されていることを確認します。該当製品のインストール ガイドを参照してください。
- Connection Server ホストに、SAML サーバ証明書用の認証局 (CA) が署名したルート証明書がインストールされていることを確認します。VMware では、自己署名の証明書を使用するように SAML 認証子を構成することは推奨されません。証明書認証の詳細については、『Horizon 7 のインストール』ドキュメントを参照してください。
- Workspace ONE サーバ、VMware Identity Manager サーバ、または外部に接しているロード バランサの FQDN または IP アドレスを書き留めます。
- Workspace ONE または VMware Identity Manager を使用している場合、コネクタ Web インターフェ이스の URL を書き留めます。
- SAML メタデータを生成して静的認証子を作成する必要がある Unified Access Gateway アプライアンスまたはサードパーティ製アプライアンスの認証子を作成する場合、デバイスで SAML メタデータを生成する手順を実行し、そのメタデータをコピーします。

### 手順

- 1 Horizon Console で、[設定] - [サーバ] の順に移動します。
- 2 [Connection Server] タブで、SAML 認証子を関連付けるサーバ インスタンスを選択して [編集] をクリックします。

- 3 [認証] タブで、[VMware Horizon (SAML 2.0 認証子) への認証の委任] ドロップダウン メニューの設定を選択して、SAML 認証子を有効または無効にします。

オプション	説明
無効	SAML 認証が無効です。リモート デスクトップとアプリケーションは、Horizon Client からのみ起動できます。
許可	SAML 認証が有効です。リモート デスクトップとアプリケーションは、Horizon Client と VMware Identity Manager の両方またはサードパーティ製デバイスから起動できます。
Required	SAML 認証が有効です。リモート デスクトップとアプリケーションは、VMware Identity Manager またはサードパーティ製デバイスからのみ起動できます。デスクトップまたはアプリケーションを、Horizon Client から手動で起動できません。

要件に応じて、環境内の各 Connection Server インスタンスを異なる SAML 認証設定で構成できます。

- 4 [SAML 認証子の管理] をクリックし、[追加] をクリックします。
- 5 [SAML 2.0 認証子を追加] ダイアログ ボックスで SAML 認証子を構成します。

オプション	説明
Type	Unified Access Gateway アプライアンスまたはサードパーティ製デバイスの場合、[静的] を選択します。VMware Identity Manager の場合、[動的] を選択します。動的認証子の場合、メタデータ URL および管理 URL を指定できます。静的認証子の場合、Unified Access Gateway アプライアンスまたはサードパーティ製デバイスでメタデータを生成し、メタデータをコピーして [SAML メタデータ] テキスト ボックスに貼り付けます。
ラベル	SAML 認証子を識別する一意の名前。
説明	SAML 認証子の簡単な説明。この値はオプションです。
メタデータ URL	(動的認証子の場合) SAML ID プロバイダと Connection Server インスタンス間で SAML 情報を交換するために必要な情報すべてを取得するための URL。URL <code>https://&lt;Horizon Server 名&gt;/SAAS/API/1.0/GET/metadata/idp.xml</code> で、[<Horizon Server 名>] をクリックして VMware Identity Manager サーバまたは外部接続ロード バランサ (サードパーティ製デバイス) の FQDN または IP アドレスに置換します。
管理 URL	(動的認証子の場合) SAML ID プロバイダの管理コンソールにアクセスするための URL。VMware Identity Manager の場合、この URL は VMware Identity Manager コネクタ Web インターフェイスを参照している必要があります。この値はオプションです。
SAML メタデータ	(静的認証子の場合) Unified Access Gateway アプライアンスまたはサードパーティ製デバイスから生成およびコピーしたメタデータ テキスト。
Connection Server に有効	認証子を有効にするには、このチェック ボックスをオンにします。複数の認証子を有効にできます。有効になっている認証子のみがリストに表示されます。

- 6 [OK] をクリックして SAML 認証子の構成を保存します。

有効な情報を指定した場合、自己署名の証明書を受け入れるか (推奨されません)、Horizon 7 および VMware Identity Manager またはサードパーティ製デバイスの信頼できる証明書を使用する必要があります。

[SAML 認証子の管理] ダイアログ ボックスには、新しく作成された認証子が表示されます。

### 次のステップ

Connection Server のメタデータの有効期間を延長して、リモート セッションが 24 時間経過後に終了されないようにします。[Connection Server でのサービス プロバイダ メタデータの有効期間の変更](#)を参照してください。

## VMware Identity Manager でのプロキシ サポートの設定

Horizon 7 は、VMware Identity Manager (vIDM) サーバのプロキシのサポートを提供します。ホスト名やポート番号などのプロキシの詳細は ADAM データベースで設定できます。HTTP 要求はプロキシ経由で経路指定されます。

この機能は、オンプレミスの Horizon 7 環境がクラウド内の vIDM サーバと通信できるハイブリッド環境をサポートします。

### 前提条件

#### 手順

- 1 Connection Server ホスト上で ADSI Edit ユーティリティを起動します。
- 2 ADAM ADSI ツリーで、オブジェクトパス `cd=vdi,dc=vmware,dc=int,ou=Properties,ou=Global,cn=Common Attributes` を展開します。
- 3 [アクション]-[プロパティ] の順に選択して、**pae-SAMLProxyName** エントリと **pae-SAMLProxyPort** エントリに値を追加します。

## Connection Server でのサービス プロバイダ メタデータの有効期間の変更

有効期間を変更しないと、Connection Server は 24 時間後に Unified Access Gateway アプライアンスやサードパーティ製の ID プロバイダなどの SAML 認証子から SAML アサーションを受け入れるのを停止し、メタデータの交換を繰り返す必要があります。

この手順を使用して、Connection Server が ID プロバイダから SAML アサーションを受け入れるのを停止するまでの日数を指定します。この日数は、現在の有効期間が切れるときに使用されます。たとえば、現在の有効期間が 1 日の場合に 90 日を指定すると、1 日経過後に Connection Server は有効期間が 90 日間のメタデータを生成します。

### 前提条件

お使いのバージョンの Windows オペレーティング システムでの ADSI Edit ユーティリティの使用方法については、Microsoft TechNet Web サイトを参照してください。

#### 手順

- 1 Connection Server ホスト上で ADSI Edit ユーティリティを起動します。
- 2 コンソール ツリーで、[接続] を選択します。
- 3 [識別名または命名規則を選択または入力] テキスト ボックスに、識別名「**DC=vdi, DC=vmware, DC=int**」を入力します。



- 4 [コンピュータ] ペインで、**localhost:389** を選択または入力するか、Connection Server ホストの完全修飾ドメイン名 (FQDN) を入力し、続いてポート 389 を入力します。

例: **localhost:389** または **mycomputer.example.com:389**

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

```
cs-samlencryptionkeyvaliditydays=number-of-days
cs-samlsigningkeyvaliditydays=number-of-days
```

この例で、*number-of-days* はリモート Connection Server が SAML アサーションを受け入れるのを停止するまでに経過できる日数です。この期間を過ぎると、SAML メタデータを交換するプロセスを繰り返す必要があります。

## Connection Server をサービス プロバイダとして使用可能にするための SAML メタデータの生成

使用する ID プロバイダに SAML 認証子を作成して有効にすると、Connection Server メタデータの生成が必要になる場合があります。このメタデータは、ID プロバイダである Unified Access Gateway アプライアンスまたはサードパーティ製ロード バランサでサービス プロバイダを作成するために使用します。

### 前提条件

Unified Access Gateway またはサードパーティ製ロード バランサ/ゲートウェイ ID プロバイダの SAML 認証子を作成済みであることを確認します。

### 手順

- 1 新規のブラウザ タブを開き、Connection Server の SAML メタデータを取得するための URL を入力します。

**`https://connection-server.example.com/SAML/metadata/sp.xml`**

この例で、*connection-server.example.com* は Connection Server ホストの完全修飾ドメイン名です。

このページには、Connection Server からの SAML メタデータが表示されます。

- 2 [別名で保存] コマンドを使用して Web ページを XML ファイルに保存します。

たとえば、ページを `connection-server-metadata.xml` という名前のファイルに保存することもできます。このファイルの内容は次のテキストで始まります。

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ...
```

### 次のステップ

ID プロバイダで適切な手順を使用して、Connection Server SAML メタデータ内にコピーします。Unified Access Gateway またはサードパーティ製ロード バランサ/ゲートウェイのドキュメントを参照してください。

## 複数の動的 SAML 認証子の応答時間に関する注意事項

Connection Server インスタンスで SAML 2.0 認証をオプションまたは必須として設定し、複数の動的 SAML 認証子を Connection Server インスタンスに関連付けている場合に、動的 SAML 認証子のいずれかに到達できなくなると、他の動的 SAML 認証子からリモート デスクトップを起動するための応答時間が長くなります。

他の動的 SAML 認証子でリモート デスクトップを起動するための応答時間を短縮するには、Horizon Console を使用して、到達できない動的 SAML 認証子を無効にします。SAML 認証子を無効にする方法については、[Horizon Console](#) での [SAML 認証子の設定](#) を参照してください。

## Horizon Console での Workspace ONE アクセス ポリシーの設定

Workspace ONE または VMware Identity Manager (vIDM) の管理者は、Horizon 7 で資格のある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アクセス ポリシーを設定できます。vIDM で作成したポリシーを適用するには、Horizon Client がユーザーを Workspace ONE クライアントにプッシュして資格を開始できるように、Horizon Client を Workspace ONE モードに切り替える必要があります。Horizon Client にログインすると、アクセス ポリシーにより、Workspace ONE 経由で公開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。

### 前提条件

- Workspace ONE でアプリケーションのアクセス ポリシーを設定します。アクセス ポリシーの設定の詳細については、『VMware Identity Manager 管理ガイド』を参照してください。
- Horizon Console で公開デスクトップとアプリケーションの資格をユーザーに付与します。

### 手順

- 1 Horizon Console で、[設定] - [サーバ] の順に移動します。
- 2 [Connection Server] タブで、SAML 認証子に関連するサーバ インスタンスを選択して [編集] をクリックします。
- 3 [認証] タブで、[VMware Horizon (SAML 2.0 認証子) への認証の委任] オプションを [必須] に設定します。  
[必須] オプションにより、SAML 認証が有効になります。エンドユーザーが Horizon Server に接続するには、vIDM またはサードパーティの ID プロバイダによって提供される SAML トークンを使用する必要があります。デスクトップまたはアプリケーションを、Horizon Client から手動で起動することはできません。
- 4 [Workspace ONE モードを有効にする] を選択します。
- 5 [Workspace ONE サーバ ホスト名] テキスト ボックスに Workspace ONE ホスト名の FQDN 値を入力します。
- 6 (オプション) [Workspace ONE モードをサポートしていないクライアントからの接続をブロックする] を選択して、Workspace ONE モードをサポートする Horizon Client からアプリケーションへのアクセスを制限します。

バージョン 4.5 より前の Horizon Client では、Workspace ONE モード機能がサポートされていません。このオプションを選択した場合、バージョン 4.5 より前の Horizon Client は Workspace ONE でアプリケーションにアクセスできません。Workspace ONE のバージョンがバージョン 2.9.1 よりも古い場合、Horizon 7 7.2 よりも新しいバージョンで Workspace ONE モード機能が有効になりません。



## バイオメトリクス認証の構成

バイオメトリクス認証は、LDAP データベースで `pae-ClientConfig` 属性を編集することで構成できます。

### 前提条件

お使いのバージョンの Windows サーバでの ADSI Edit ユーティリティの使用方法については、Microsoft TechNet Web サイトを参照してください。

### 手順

- 1 接続サーバ ホスト上で ADSI Edit ユーティリティを起動します。
- 2 [接続設定] ダイアログ ボックスで、[DC=vdi,DC=vmware,DC=int] を選択するか接続します。
- 3 [コンピュータ] ペインで、**localhost:389** を選択または入力するか、接続サーバ ホストの完全修飾ドメイン名 (FQDN) を入力し、続いてポート 389 を入力します。

例：**localhost:389** または **mycomputer.mydomain.com:389**

- 4 オブジェクトの [CN=Common, OU=Global, OU=Properties] で、[pae-ClientConfig] 属性を編集して値 [BioMetricsTimeout=<integer>] を追加します。

次の BioMetricsTimeout 値が有効です。

BioMetricsTimeout 値	説明
0	バイオメトリクス認証はサポートされません。これはデフォルトです。
-1	バイオメトリクス認証は時間制限なしでサポートされます。
任意の正の整数	バイオメトリクス認証はサポートされ、指定した分数の間、使用することができます。

新しい設定はただちに有効になります。接続サーバ サービスまたはクライアント デバイスを再起動する必要はありません。

## ユーザーとグループの認証

Horizon Console にログインした後、ユーザーおよびグループに認証を設定し、アプリケーションやデスクトップへのアクセスを制御できます。

ネットワーク外部からデスクトップへのユーザーまたはグループのアクセスを制限するように、リモート アクセスを構成します。非認証ユーザーが Active Directory 認証情報を使用せずに Horizon Client から公開アプリケーションにアクセスできるように設定できます。

この章には、次のトピックが含まれています。

- 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
- 非認証アクセスの構成

### 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。

### リモート アクセスの設定

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接続サーバ インスタンスへのアクセスを許可し、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接続サーバ インスタンスへのゲートウェイとして、Unified Access Gateway 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。Unified Access Gateway アプライアンスのデプロイの詳細については、『Unified Access Gateway の導入および設定』ドキュメントを参照してください。

- 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 Horizon Console 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。

---

**注:** 非認証アクセスのユーザーは検索結果に表示されません。

---

- 4 非認証アクセスのユーザーまたはグループにリモート アクセスを許可するには、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。

## 非認証アクセスの構成

管理者は、非認証ユーザーが Active Directory 認証情報を使用せずに Horizon Client から公開アプリケーションにアクセスできるように設定できます。ユーザーが自身のセキュリティ管理とユーザー管理を行うアプリケーションにシームレスにアクセスする必要がある場合には、非認証アクセスの設定を考慮してください。

ユーザーが非認証アクセスを設定した公開アプリケーションを起動すると、RDS ホストが必要に応じてローカル ユーザー セッションを作成し、ユーザーにセッションを割り当てます。

この機能を実行するには、Horizon 7 バージョン 7.1 環境のセットアップと Horizon Client バージョン 4.4 が必要です。

非認証アクセス ユーザーを構成するルールとガイドラインについては、『Horizon 7 の管理』ドキュメントを参照してください。

## 非認証アクセス ユーザーの作成

管理者は、公開アプリケーションに非認証でアクセスするユーザーを作成できます。管理者が非認証アクセスのユーザーを設定すると、ユーザーは Horizon Client から非認証アクセスでのみ接続サーバーインスタンスにログインできます。

#### 前提条件

- 管理者が作成できるユーザーは、Active Directory アカウントごとに 1 つだけです。
- 管理者は、非認証のユーザー グループを作成できません。非認証アクセス ユーザーを作成するときに、この Active Directory ユーザーに対する既存のクライアント セッションがある場合には、変更を反映するためにクライアント セッションを再起動する必要があります。
- デスクトップの使用資格を持つユーザーを選択し、ユーザーを非認証アクセス ユーザーにすると、このユーザーは資格のあるデスクトップにアクセスできなくなります。

**手順**

- 1 Horizon Console で、[ユーザーとグループ] を選択します。
- 2 [非認証アクセス] タブで [追加] をクリックします。
- 3 [認証されていないユーザーの追加] ウィザードで、1 つ以上の検索条件を選択します。[検索] をクリックして、検索条件に基づいてユーザーを検索します。
- 4 ユーザーを選択し、[次へ] をクリックします。
- 5 ユーザー エイリアスを入力します。

デフォルトのユーザー エイリアスは、Active Directory アカウントに設定されたユーザー名です。エンド ユーザーは、ユーザー エイリアスを使用して Horizon Client から接続サーバ インスタンスにログインできます。

- 6 (オプション) ユーザーの詳細を確認して、コメントを追加します。
- 7 [送信] をクリックします。

接続サーバが非認証アクセス ユーザーを作成し、ユーザー エイリアス、ユーザー名、氏名、ドメイン、アプリケーションの資格、セッションなどのユーザーの詳細を表示します。

**次のステップ**

非認証アクセスのユーザーの作成後、接続サーバで非認証アクセスを有効にして、公開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必要があります。『Horizon 7 の管理』ドキュメントで「ユーザーの非認証アクセスを有効にする」を参照してください。

**公開アプリケーションに対する非認証アクセス ユーザーへの資格付与**

非認証アクセス ユーザーの作成後、公開アプリケーションにアクセスする資格をユーザーに付与する必要があります。

**前提条件**

- RDS ホストのグループに基づいてファームを作成します。 [Horizon Console でのファームの作成](#)を参照してください。
- RDS ホストのファームで実行される公開アプリケーションのアプリケーション プールを作成します。 [Horizon Console でのアプリケーション プールの作成](#)を参照してください。

**手順**

- 1 Horizon Console で、[ユーザーとグループ] を選択します。
- 2 [資格] タブで、[資格] ドロップダウン メニューから [アプリケーションに対する資格を追加] を選択します。
- 3 [追加] をクリックして、1 つ以上の検索条件を選択します。[非認証ユーザー] チェックボックスをオンにして [検索] をクリックし、検索条件に基づいて非認証アクセス ユーザーを検索します。
- 4 プールのアプリケーションに対する資格を付与するユーザーを選択して、[OK] をクリックします。
- 5 プール内のアプリケーションを選択して、[送信] をクリックします。

### 次のステップ

非認証アクセス ユーザーを使用して、Horizon Client にログインします。 [Horizon Client からの非認証アクセス](#) を参照してください。

## 非認証アクセス ユーザーの削除

非認証アクセス ユーザーを削除する場合には、アプリケーション プールに対するユーザーの資格も削除する必要があります。

非認証アクセス ユーザーがデフォルト ユーザーの場合、このユーザーは削除できません。デフォルトのユーザーを削除すると、ユーザーが正常に削除されたことを示すメッセージと内部エラー メッセージが Horizon Console に表示されます。ただし、デフォルトのユーザーは、Horizon Console から削除されません。

---

**注:** 非認証アクセス ユーザーを削除するときに、この Active Directory ユーザーに対する既存のクライアント セッションがある場合には、変更を反映するためにクライアント セッションを再起動する必要があります。

---

### 手順

- 1 Horizon Console で、[ユーザーとグループ] を選択します。
- 2 [非認証アクセス] タブでユーザーを選択し、[削除] をクリックします。
- 3 [OK] をクリックします。

### 次のステップ

アプリケーションに対するユーザーの資格を削除します。

## Horizon Client からの非認証アクセス

非認証アクセスで Horizon Client にログインして、公開アプリケーションを起動します。

セキュリティを強化するため、非認証アクセス ユーザーには、Horizon Client へのログインに使用できるユーザー エイリアスが存在します。ユーザー エイリアスを選択する場合、ユーザーの Active Directory 認証情報または UPN を入力する必要はありません。Horizon Client にログインすると、公開アプリケーションをクリックして、アプリケーションを起動できます。Horizon Client のインストールと設定の詳細については、[VMware Horizon Client ドキュメント](#) Web ページにある Horizon Client のドキュメントを参照してください。

### 前提条件

- Horizon 7 バージョン 7.1 の接続サーバで非認証アクセスが構成されていることを確認します。
- Horizon Administrator で、非認証アクセス ユーザーが作成されていることを確認します。デフォルトの非認証ユーザーが唯一の非認証アクセス ユーザーである場合、Horizon Client はデフォルトのユーザーで接続サーバインスタンスに接続します。

### 手順

- 1 Horizon Client を開始します。
- 2 Horizon Client で、[認証されていないアクセスを使用して匿名ログイン] を選択します。
- 3 接続サーバ インスタンスに接続します。

- 4 ドロップダウン メニューからユーザー エイリアスを選択して、[ログイン] をクリックします。  
デフォルト ユーザーには "default" というサフィックスが付いています。
- 5 公開アプリケーションをダブルクリックして、アプリケーションを起動します。

# Horizon Console でのロールベースの委任管理の構成

# 7

Horizon 7 環境の重要な管理タスクは、Horizon Console を使用できるユーザーとそれらのユーザーが実行可能なタスクを決定することです。ロールベースの委任管理を使用すると、特定の Active Directory ユーザーおよびグループに管理者ロールを割り当てることによって、選択的に管理者権限を割り当てることができます。

この章には、次のトピックが含まれています。

- [ロールと権限の概要](#)
- [Horizon Console でのアクセス グループを使用したプールおよびファーム管理の委任](#)
- [権限の概要](#)
- [管理者の管理](#)
- [権限の管理と確認](#)
- [アクセス グループの管理と確認](#)
- [カスタム ロールの管理](#)
- [定義済みのロールと権限](#)
- [一般的なタスクに必要な権限](#)
- [管理者ユーザーおよびグループに関するベスト プラクティス](#)

## ロールと権限の概要

Horizon Console でタスクを実行できるかどうかは、管理者ロールおよび権限から構成されるアクセス制御システムで管理します。このシステムは vCenter Server アクセス制御システムに似ています。

管理者ロールは権限の集まりです。権限は、ユーザーにデスクトップ プールに対する資格を付与するなど、特定のアクションを実行できるようにするものです。さらに、権限は、管理者が Horizon Console で表示できるものも制御します。たとえば、管理者がグローバル ポリシーの表示または変更権限を持たない場合は、その管理者が Horizon Console にログインしてもナビゲーション パネルに [グローバル ポリシー] 設定は表示されません。

管理者権限はグローバルか、またはオブジェクト固有です。グローバル権限は、グローバル設定の表示や変更などシステム全体の操作を制御します。オブジェクト固有の権限は、特定のタイプのオブジェクトの操作を制御します。

管理者ロールは、一般に、上位レベルの管理タスクを実行するために必要な個別の権限をすべて組み合わせたものです。Horizon Console には、一般的な管理タスクの実行に必要な権限を含む定義済みのロールが用意されています。これらの定義済みのロールを管理者ユーザーおよびグループに割り当てることも、選択した権限を組み合わせて独自のロールを作成することもできます。定義済みのロールを変更することはできません。

管理者を作成するには、Active Directory ユーザーおよびグループからユーザーとグループを選択し、管理者ロールを割り当てます。ロールにオブジェクト固有の権限が含まれている場合、アクセス グループへのロールの適用が必要になる場合があります。管理者は、ロールの割り当てによって権限を取得します。権限を管理者に直接割り当てることはできません。複数のロールが割り当てられた管理者は、それらのロールに含まれるすべての権限を合わせたものを取得します。

## Horizon Console でのアクセス グループを使用したプールおよびファーム管理の委任

デフォルトでは、自動デスクトップ プール、手動デスクトップ プールおよびファームは、Horizon Console に / または Root (/) で表示されるルート アクセス グループ内に作成されます。公開デスクトップ プールおよびアプリケーション プールでは、そのファームのアクセス グループが継承されます。ルート アクセス グループの下にアクセス グループを作成し、別の管理者に特定のプールやファームの管理を委任することができます。

**注:** 公開デスクトップ プールまたはアプリケーション プールのアクセス グループを直接変更することはできません。公開デスクトップ プールまたはアプリケーション プールが属するファームのアクセス グループを変更する必要があります。

仮想または物理マシンでは、そのデスクトップ プールからアクセス グループが継承されます。接続された通常ディスクでは、そのマシンからアクセス グループが継承されます。ルート アクセス グループを含む最大 100 のアクセス グループを保持できます。

アクセス グループの管理者にロールを割り当てることにより、そのアクセス グループのリソースへの管理者アクセスを構成することができます。管理者は、ロールを割り当てられているアクセス グループのみに存在するリソースにアクセスできます。管理者が持つアクセス グループに対するロールによって、そのアクセス グループのリソースに対するアクセス レベルが決定されます。

ロールは、ルート アクセス グループから継承されるため、ルート アクセス グループに対するロールを持つ管理者は、すべてのアクセス グループに対してそのロールを持つことになります。ルート アクセス グループに対する管理者ロールを持つ管理者は、システムのすべてのオブジェクトに対するフル アクセス権を持つため、スーパー管理者になります。

ロールには、アクセス グループに適用する少なくとも 1 つのオブジェクト固有権限が含まれている必要があります。グローバル権限のみを含むロールはアクセス グループに適用できません。

Horizon Console を使用してアクセス グループを作成し、既存のデスクトップ プールをアクセス グループに移動することができます。自動デスクトップ プール、手動プールまたはファームを作成する場合、デフォルトのルート アクセス グループを受け入れるか、または別のアクセス グループを選択できます。

### ■ 異なるアクセス グループの異なる管理者

構成内の各アクセス グループを管理する異なる管理者を作成できます。



## ■ 同じアクセス グループの異なる管理者

同じアクセス グループを管理する複数の異なる管理者を作成できます。

## 異なるアクセス グループの異なる管理者

構成内の各アクセス グループを管理する異なる管理者を作成できます。

たとえば、会社のデスクトップ プールが 1 つのアクセス グループ内にあり、ソフトウェア開発者用のデスクトップ プールが別のアクセス グループ内にある場合、複数の管理者を作成してアクセス グループごとにリソースを管理することができます。

表 7-1. 異なるアクセス グループの異なる管理者 に、このタイプの構成の例を示します。

表 7-1. 異なるアクセス グループの異なる管理者

管理者	ロール	アクセス グループ
view-domain.com\Admin1	インベントリ管理者	/CorporateDesktops
view-domain.com\Admin2	インベントリ管理者	/DeveloperDesktops

この例では、Admin1 という管理者が CorporateDesktops というアクセス グループのインベントリ管理者ロールを持ち、Admin2 という管理者が DeveloperDesktops というアクセス グループのインベントリ管理者ロールを持ちます。

## 同じアクセス グループの異なる管理者

同じアクセス グループを管理する複数の異なる管理者を作成できます。

たとえば、会社のデスクトップ プールが 1 つのアクセス グループ内にある場合、それらのプールを表示および変更できる管理者と、それらの表示のみが可能な別の管理者を作成することができます。

表 7-2. 同じアクセス グループの異なる管理者 に、このタイプの構成の例を示します。

表 7-2. 同じアクセス グループの異なる管理者

管理者	ロール	アクセス グループ
view-domain.com\Admin1	インベントリ管理者	/CorporateDesktops
view-domain.com\Admin2	インベントリ管理者（読み取り専用）	/CorporateDesktops

この例では、Admin1 という管理者が CorporateDesktops というアクセス グループのインベントリ管理者ロールを持ち、Admin2 という管理者が同じアクセス グループのインベントリ管理者（読み取り専用）ロールを持ちます。

## 権限の概要

Horizon Console は、ロールの組み合わせ、管理者ユーザーまたはグループ、およびアクセス グループを権限として提供しています。ロールは実行できるアクションを定義し、ユーザーまたはグループはアクションを実行できる者を示し、アクセス グループはアクションの対象となるオブジェクトを格納します。

管理者ユーザーまたはグループ、アクセス グループ、ロールのどれを選択したかによって、Horizon Console での権限の表示が異なります。

次の表に、管理者ユーザーまたはグループを選択した場合に Horizon Console で権限がどのように表示されるかを示します。管理者ユーザーは Admin 1 という名前で、2 つの権限を持ちます。

表 7-3. Admin 1 の Administrators and Groups（管理者とグループ） タブでの権限

ロール	アクセス グループ
インベントリ管理者	MarketingDesktops
管理者（読み取り専用）	/

最初の権限は Admin 1 が MarketingDesktops というアクセス グループに対してインベントリ管理者ロールを持つことを示しています。2 番目の権限は、Admin 1 がルート アクセス グループに対して管理者（読み取り専用）ロールを持つことを示しています。

次の表に、MarketingDesktops アクセス グループを選択した場合に Horizon Console で同じ権限がどのように表示されるかを示します。

表 7-4. MarketingDesktops の Folders（フォルダ） タブの権限

Admin	ロール	継承
horizon-domain.com\Admin1	インベントリ管理者	
horizon-domain.com\Admin1	管理者（読み取り専用）	はい

最初の権限は、[表 7-3. Admin 1 の Administrators and Groups（管理者とグループ） タブでの権限](#)に示す最初の権限と同じです。2 番目の権限は、[表 7-3. Admin 1 の Administrators and Groups（管理者とグループ） タブでの権限](#)に示す 2 番目の権限から継承されています。アクセス グループはルート アクセス グループから権限を継承するため、Admin1 は MarketingDesktops アクセス グループに対する管理者（読み取り専用）ロールを持ちます。権限が継承された場合、継承された列に Yes（はい）が表示されます。

次の表に、インベントリ管理者ロールを選択した場合に [表 7-3. Admin 1 の Administrators and Groups（管理者とグループ） タブでの権限](#) の最初の権限が Horizon Console でどのように表示されるかを示します。

表 7-5. インベントリ管理者の [ロールの権限] タブの権限

Administrator	アクセス グループ
horizon-domain.com\Admin1	/MarketingDesktops

## 管理者の管理

Administrators（管理者）ロールを持つユーザーは、Horizon Console を使用して、管理者ユーザーおよびグループを追加および削除できます。

Administrators（管理者）ロールは、Horizon Console で最も強力なロールです。最初に、Administrator アカウントのメンバーに、Administrators（管理者）ロールが付与されます。Connection Server をインストールするときに、Administrator アカウントを指定します。管理者アカウントとしては、Connection Server コンピュータ上のローカル Administrators グループ (BUILTIN\Administrators)、またはドメイン ユーザー/グループのアカウントを指定できます。

**注:** デフォルトでは、Domain Admins グループはローカル Administrators グループのメンバーです。ローカル Administrators グループとして Administrator アカウントを指定した場合に、インベントリ オブジェクトおよび Horizon 7 設定に対するフル アクセス権限をドメイン管理者に与えたくないときは、ローカル Administrators グループから Domain Admins グループを削除する必要があります。

#### ■ [Horizon Console での管理者の作成](#)

管理者を作成するには、Horizon Console で Active Directory ユーザーおよびグループからユーザーまたはグループを選択し、管理者ロールを割り当てます。

#### ■ [Horizon Console での管理者の削除](#)

管理者ユーザーまたはグループを削除できます。システム内の最後のスーパー管理者は削除できません。スーパー管理者は、ルート アクセス グループに対する管理者ロールを持つ管理者です。

## Horizon Console での管理者の作成

管理者を作成するには、Horizon Console で Active Directory ユーザーおよびグループからユーザーまたはグループを選択し、管理者ロールを割り当てます。

### 前提条件

- 定義済みの管理者ロールについて理解しておきます。 [定義済みのロールと権限](#)を参照してください。
- 管理者ユーザーおよびグループを作成するためのベスト プラクティスについて理解しておきます。 [管理者ユーザーおよびグループに関するベスト プラクティス](#)を参照してください。
- 管理者にカスタム ロールを割り当てるには、カスタム ロールを作成します。 [Horizon Console でのカスタム ロールの追加](#)を参照してください。
- 特定のデスクトップ プールを管理できる管理者を作成するには、アクセス グループを作成し、デスクトップ プールをそのアクセス グループに移動します。 [アクセス グループの管理と確認](#)を参照してください。

### 手順

- 1 Horizon Console で、[設定] - [管理者] の順に移動します。
- 2 [管理者とグループ] タブで [ユーザーまたはグループの追加] をクリックします。
- 3 [追加] をクリックして、1 つ以上の検索条件を選択し、[検索] をクリックして検索条件に基づいて Active Directory ユーザーまたはグループをフィルタ処理します。
- 4 管理者ユーザーまたはグループにする Active Directory ユーザーまたはグループを選択して、[OK] をクリックし、[次へ] をクリックします。

Ctrl + Shift キーを押すと、複数のユーザーやグループを選択できます。

- 5 管理者ユーザーまたはグループに割り当てるロールを選択します。

[アクセス グループに適用] 列は、ロールをアクセス グループに適用するかどうかを示します。アクセス グループに適用されるのは、オブジェクト固有の権限を含むロールのみです。グローバル権限のみを含むロールはアクセス グループに適用されません。

オプション	アクション
選択したロールがアクセス グループに適用される	1 つ以上のアクセス グループを選択して [次へ] をクリックします。
すべてのアクセス グループにロールを適用する	ルート アクセス グループを選択して [次へ] をクリックします。

- 6 [終了] をクリックして、管理者ユーザーまたはグループを作成します。

[管理者とグループ] タブの左ペインに新しい管理者ユーザーまたはグループが表示され、右ペインに選択したロールとアクセス グループが表示されます。

## Horizon Console での管理者の削除

管理者ユーザーまたはグループを削除できます。システム内の最後のスーパー管理者は削除できません。スーパー管理者は、ルート アクセス グループに対する管理者ロールを持つ管理者です。

### 手順

- Horizon Console で、[設定] - [管理者] の順に移動します。
- [管理者とグループ] タブで、管理者ユーザーまたはグループを選択し、[ユーザーまたはグループの削除] をクリックして、[OK] をクリックします。

[管理者とグループ] タブに管理者ユーザーまたはグループが表示されなくなります。

## 権限の管理と確認

Horizon Console を使用して、特定の管理者ユーザーとグループ、ロール、アクセス グループの権限を追加、削除、確認できます。

### ■ Horizon Console での権限の追加

特定の管理者ユーザーまたはグループ、特定のロール、または特定のアクセス グループを含む権限を追加できます。

### ■ Horizon Console での権限の削除

特定の管理者ユーザーまたはグループ、特定のロール、または特定のアクセス グループを含む権限を削除できます。

### ■ Horizon Console での権限の確認

特定の管理者またはグループ、特定のロール、または特定のアクセス グループを含む権限を確認できます。

## Horizon Console での権限の追加

特定の管理者ユーザーまたはグループ、特定のロール、または特定のアクセス グループを含む権限を追加できます。

## 手順

- 1 Horizon Console で、[設定] - [管理者] の順に移動します。
- 2 権限を作成します。

オプション	アクション
特定の管理者ユーザーまたはグループを含む権限を作成します。	<ol style="list-style-type: none"> <li>a [管理者とグループ] タブで、管理者またはグループを選択し、[権限を追加] をクリックします。</li> <li>b ロールを選択します。</li> <li>c ロールをアクセス グループに適用しない場合、[終了] をクリックします。</li> <li>d ロールをアクセス グループに適用する場合は、[次へ] をクリックし、1 つ以上のアクセス グループを選択して [終了] をクリックします。ロールには、アクセス グループに適用する少なくとも 1 つのオブジェクト固有権限が含まれている必要があります。</li> </ol>
特定のロールを含む権限を作成します。	<ol style="list-style-type: none"> <li>a [ロールの権限] タブでロールを選択し、[権限] をクリックし、[権限を追加] をクリックします。</li> <li>b [追加] をクリックして、1 つ以上の検索条件を選択し、[検索] をクリックして検索条件に一致する管理者ユーザーまたはグループを検索します。</li> <li>c 権限に含める管理者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。Ctrl + Shift キーを押すと、複数のユーザーやグループを選択できます。</li> <li>d ロールをアクセス グループに適用しない場合、[終了] をクリックします。</li> <li>e ロールをアクセス グループに適用する場合は、[次へ] をクリックし、1 つ以上のアクセス グループを選択して [終了] をクリックします。ロールには、アクセス グループに適用する少なくとも 1 つのオブジェクト固有権限が含まれている必要があります。</li> </ol>
特定のアクセス グループを含む権限を作成します。	<ol style="list-style-type: none"> <li>a [アクセス グループ] タブで、アクセス グループを選択し、[権限を追加] をクリックします。</li> <li>b [追加] をクリックして、1 つ以上の検索条件を選択し、[検索] をクリックして検索条件に一致する管理者ユーザーまたはグループを検索します。</li> <li>c 権限に含める管理者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。Ctrl + Shift キーを押すと、複数のユーザーやグループを選択できます。</li> <li>d [次へ] をクリックし、ロールを選択して [終了] をクリックします。ロールには、アクセス グループに適用する少なくとも 1 つのオブジェクト固有権限が含まれている必要があります。</li> </ol>

## Horizon Console での権限の削除

特定の管理者ユーザーまたはグループ、特定のロール、または特定のアクセス グループを含む権限を削除できます。

管理者ユーザーまたはグループの最後の権限を削除すると、その管理者ユーザーまたはグループも削除されます。少なくとも 1 人の管理者がルート アクセス グループの Administrators（管理者）ロールを持つ必要があるため、その管理者が削除されるような権限の削除を行うことはできません。継承された権限は削除できません。

## 手順

- 1 Horizon Console で、[設定] - [管理者] の順に移動します。

## 2 削除する権限を選択します。

オプション	アクション
特定の管理者またはグループに適用される権限を削除します。	[管理者とグループ] タブで管理者またはグループを選択します。
特定のロールに適用される権限を削除します。	[ロール] タブでロールを選択します。
特定のアクセス グループに適用される権限を削除します。	[アクセス グループ] タブでフォルダを選択します。

## 3 権限を選択し、[権限を削除] をクリックします。

# Horizon Console での権限の確認

特定の管理者またはグループ、特定のロール、または特定のアクセス グループを含む権限を確認できます。

### 手順

- 1 Horizon Console で、[設定] - [管理者] の順に移動します。
- 2 権限を確認します。

オプション	アクション
特定の管理者またはグループを含む権限を確認する。	[管理者とグループ] タブで管理者またはグループを選択します。
特定のロールを含む権限を確認する。	[ロールの権限] タブでロールを選択して、[アクセス権限] をクリックします。
特定のアクセス グループを含む権限を確認する。	[アクセス グループ] タブでフォルダを選択します。

# アクセス グループの管理と確認

Horizon Console を使用して、アクセス グループを追加または削除したり、特定のアクセス グループ内のデスクトップ プールとマシンを確認したりできます。

### ■ [Horizon Console でアクセス グループを追加する](#)

アクセス グループを作成することにより、特定のマシン、デスクトップ プールまたはファームの管理を委任できます。デフォルトでは、デスクトップ プール、アプリケーション プールおよびファームは、ルート アクセス プールにあります。

### ■ [Horizon Console での別のアクセス グループへのデスクトップ プールまたはファームの移動](#)

アクセス グループの作成後、自動デスクトップ プール、手動プールまたはファームを新しいアクセス グループに移動できます。

### ■ [Horizon Console でのアクセス グループの削除](#)

オブジェクトが含まれていないアクセス グループは削除できます。ルート アクセス グループは削除できません。

#### ■ アクセス グループ内のデオブジェクトの確認

Horizon Console で、特定のアクセス グループのデスクトップ プール、アプリケーション プール、ファーム、パーシステント ディスクを確認できます。

#### ■ アクセス グループ内の vCenter 仮想マシンの確認

Horizon Console で特定のアクセス グループ内の vCenter Server 仮想マシンを表示できます。vCenter 仮想マシンは、そのプールからアクセス グループを継承します。

## Horizon Console でアクセス グループを追加する

アクセス グループを作成することにより、特定のマシン、デスクトップ プールまたはファームの管理を委任できます。デフォルトでは、デスクトップ プール、アプリケーション プールおよびファームは、ルート アクセス プールにあります。

ルート アクセス グループを含む最大 100 のアクセス グループを保持できます。

### 手順

- 1 Horizon Console で、[アクセス グループ] ダイアログ ボックスに移動します。

オプション	アクション
デスクトップから	<ul style="list-style-type: none"> <li>■ [インベントリ] - [デスクトップ] の順に選択します。</li> <li>■ [アクセス グループ] ドロップダウン メニューから、[新しいアクセス グループ] を選択します。</li> </ul>
ファームから	<ul style="list-style-type: none"> <li>■ [インベントリ] - [ファーム] の順に選択します。</li> <li>■ [アクセス グループ] ドロップダウン メニューから [新しいアクセス グループ] を選択します。</li> </ul>

- 2 アクセス グループの名前と説明を入力し、[OK] をクリックします。

説明はオプションです。

### 次のステップ

- 1 つ以上のオブジェクトをアクセス グループに移動します。

## Horizon Console での別のアクセス グループへのデスクトップ プールまたはファームの移動

アクセス グループの作成後、自動デスクトップ プール、手動プールまたはファームを新しいアクセス グループに移動できます。

### 手順

- 1 Horizon Console で、[インベントリ] - [デスクトップ] の順に選択するか、[インベントリ] - [ファーム] の順に選択します。
- 2 プールまたはファームを選択します。
- 3 [アクセス グループ] ドロップダウン メニューから [アクセス グループを変更] を選択します。

4 アクセス グループを選択し、[OK] をクリックします。

Horizon Console が、選択したアクセス グループにプールまたはファームを移動します。

## Horizon Console でのアクセス グループの削除

オブジェクトが含まれていないアクセス グループは削除できます。ルート アクセス グループは削除できません。

### 前提条件

アクセス グループにオブジェクトが含まれている場合は、オブジェクトを別のアクセス グループまたはルート アクセス グループに移動します。 [Horizon Console での別のアクセス グループへのデスクトップ プールまたはファームの移動](#)を参照してください。

### 手順

- 1 Horizon Console で、[設定] - [管理者] の順に移動します。
- 2 [アクセス グループ] タブでアクセス グループを選択して、[アクセス グループを削除] をクリックします。
- 3 [OK] をクリックしてアクセス グループを削除します。

## アクセス グループ内のデオブジェクトの確認

Horizon Console で、特定のアクセス グループのデスクトップ プール、アプリケーション プール、ファーム、パーシステント ディスクを確認できます。

### 手順

- 1 Horizon Console で、オブジェクトのメイン ページに移動します。

オブジェクト	アクション
デスクトップ プール	[インベントリ] - [デスクトップ] の順に選択します。
アプリケーション プール	[インベントリ] - [アプリケーション] の順に選択します。
ファーム	[インベントリ] - [ファーム] の順に選択します。
通常ディスク	[インベントリ] - [パーシステント ディスク] の順に選択します。

デフォルトでは、すべてのアクセス グループ内のオブジェクトが表示されます。

- 2 メイン ウィンドウ ペインの [アクセス グループ] ドロップダウン メニューから、アクセス グループを選択します。

選択したアクセス グループ内のオブジェクトが表示されます。

## アクセス グループ内の vCenter 仮想マシンの確認

Horizon Console で特定のアクセス グループ内の vCenter Server 仮想マシンを表示できます。vCenter 仮想マシンは、そのプールからアクセス グループを継承します。

### 手順

- 1 Horizon Console で、[インベントリ] - [マシン] の順に移動します。



- 2 [vCenter 仮想マシン] タブを選択します。

デフォルトでは、すべてのアクセス グループ内の vCenter 仮想マシンが表示されます。

- 3 [アクセス グループ] ドロップダウン メニューからアクセス グループを選択します。

選択したアクセス グループ内の vCenter 仮想マシンが表示されます。

## カスタム ロールの管理

Horizon Console を使用して、カスタム ロールを追加、変更、および削除できます。

- [Horizon Console でのカスタム ロールの追加](#)

定義済みの管理者ロールがニーズを満たしていない場合、Horizon Console で特定の権限を組み合わせで独自のロールを作成できます。

- [Horizon Console でのカスタム ロールの権限の変更](#)

カスタム ロール内の権限を変更できます。定義済みの管理者ロールを変更することはできません。

- [Horizon Console でのカスタム ロールの削除](#)

権限に含まれていない場合は、カスタム ロールを削除できます。定義済みの管理者ロールを削除することはできません。

## Horizon Console でのカスタム ロールの追加

定義済みの管理者ロールがニーズを満たしていない場合、Horizon Console で特定の権限を組み合わせで独自のロールを作成できます。

### 前提条件

カスタム ロールの作成に使用できる管理者権限について理解しておきます。[定義済みのロールと権限](#)を参照してください。

---

**注:** カスタム管理者ロールを作成するときに、カスタム管理者ユーザーにグローバル権限を付与できません。クラウド ポッド アーキテクチャ 環境でグローバル資格を管理できるグローバル権限があるのは、事前定義の管理者ロールだけです。

---

### 手順

- 1 Horizon Console で、[設定] - [管理者] の順に移動します。
- 2 [ロールの権限] タブで [ロールを追加] をクリックします。
- 3 新しいロールの名前と説明を入力し、1 つ以上の権限を選択して、[OK] をクリックします。  
左ペインに新しいロールが表示されます。

## Horizon Console でのカスタム ロールの権限の変更

カスタム ロール内の権限を変更できます。定義済みの管理者ロールを変更することはできません。

### 前提条件

カスタム ロールの作成に使用できる管理者権限について理解しておきます。[定義済みのロールと権限](#)を参照してください。

### 手順

- 1 Horizon Console で、[設定] - [管理者] の順に移動します。
- 2 [ロールの権限] タブでロールを選択します。
- 3 ロールの権限を表示して、[編集] をクリックします。
- 4 権限を選択または選択解除します。
- 5 [OK] をクリックして変更を保存します。

## Horizon Console でのカスタム ロールの削除

権限に含まれていない場合は、カスタム ロールを削除できます。定義済みの管理者ロールを削除することはできません。

### 前提条件

ロールが権限に含まれる場合は、権限を削除します。[Horizon Console での権限の削除](#)を参照してください。

### 手順

- 1 Horizon Console で、[設定] - [管理者] の順に移動します。
- 2 [ロールの権限] タブで、ロールを選択し、[ロールを削除] をクリックします。  
[ロールを削除] ボタンは、定義済みロールや、権限に含まれるカスタム ロールに対しては使用できません。
- 3 [OK] をクリックしてロールを削除します。

## 定義済みのロールと権限

Horizon Console には、管理者ユーザーおよびグループに割り当てることができる定義済みのロールがあります。選択した権限を組み合わせることで独自の管理者ロールを作成することもできます。

- [定義済みの管理者ロール](#)

定義済みの管理者ロールは、一般的な管理タスクの実行に必要な個別の権限をすべて組み合わせたものです。定義済みのロールを変更することはできません。

- [グローバル権限](#)

グローバル権限は、グローバル設定の表示や変更などシステム全体の操作を制御します。グローバル権限のみを含むロールはアクセス グループに適用できません。

- [オブジェクト固有の権限](#)

オブジェクト固有権限は、特定のタイプのインベントリ オブジェクトの操作を制御します。オブジェクト固有の権限を含むロールは、アクセス グループに適用することができます。

## ■ 内部権限

一部の定義済みの管理者ロールには、内部権限が含まれています。カスタム ロールを作成するときに内部権限を選択することはできません。

## 定義済みの管理者ロール

定義済みの管理者ロールは、一般的な管理タスクの実行に必要な個別の権限をすべて組み合わせたものです。定義済みのロールを変更することはできません。

**注:** 事前定義ロールまたはカスタム ロールの組み合わせをユーザーに割り当てると、個々の事前定義ロールまたはカスタム ロールで実行できない操作が可能になります。

次の表で定義済みロールについて説明し、ロールをアクセス グループに適用できるかどうかを示します。

表 7-6. Horizon Console の事前定義ロール

ロール	ユーザーが可能な操作	アクセス グループに適用
管理者	<p>すべての管理者の操作を実行する（追加の管理者ユーザーおよびグループの作成を含む）。クラウド ポッド アーキテクチャ環境では、このロールを持つ管理者は、ポッド フェデレーションの構成と管理およびリモート ポッド セッションの管理を行うことができます。</p> <p>ルート アクセス グループに対する管理者ロールを持つ管理者は、システムのすべてのインベントリ オブジェクトに対するフル アクセス権を持つことから、スーパー ユーザーと呼ばれます。Administrators（管理者）ロールにはすべての権限が含まれるため、限られたユーザーに割り当てるようにしてください。最初に、Connection Server ホスト上のローカル管理者グループのメンバーに、ルート アクセス グループに対するこのロールが付与されます。</p> <p><b>重要:</b> 次のタスクを実行するためには、管理者がルート アクセス グループに対する管理者ロールを備えている必要があります。</p> <ul style="list-style-type: none"> <li>■ アクセス グループを追加および削除する。</li> <li>■ Horizon Console で ThinApp アプリケーションおよび設定を管理する。</li> <li>■ vdmadmin、vdmimport および lmvutil コマンドを使用する。</li> </ul>	はい
管理者（読み取り専用）	<ul style="list-style-type: none"> <li>■ グローバル設定とインベントリ オブジェクトを表示する（変更はできない）。</li> <li>■ ThinApp アプリケーションおよび設定を表示する（変更はできない）。</li> <li>■ すべての PowerShell コマンドやコマンドライン ユーティリティ（vdmexport など。vdmadmin、vdmimport および lmvutil は除く）を実行する。</li> </ul> <p>クラウド ポッド アーキテクチャ環境では、このロールを持つ管理者は、グローバル データ レイヤでインベントリ オブジェクトと設定を表示できます。</p> <p>管理者がアクセス グループに対してこのロールを持つ場合、そのアクセス グループ内のインベントリ オブジェクトのみを表示できます。</p>	はい
エージェント登録管理者	物理システム、スタンドアロン仮想マシン、RDS ホストなどの管理対象外のマシンを登録する。	いいえ
グローバル構成およびポリシー管理者	グローバル ポリシーと設定（管理者ロールと権限を除く）および ThinApp アプリケーションと設定を表示し、変更する。	いいえ
グローバル構成およびポリシー管理者（読み取り専用）	グローバル ポリシーと設定（管理者ロールと権限を除く）および ThinApp アプリケーションと設定を表示する（変更はできない）。	いいえ

ロール	ユーザーが可能な操作	アクセス グループに適用
ヘルプデスク管理者	<p>シャットダウン、リセット、再起動など、デスクトップやアプリケーションで操作を実行したり、ユーザーのデスクトップまたはアプリケーションのプロセス終了など、リモート アシスタントの操作を実行します。Horizon Help Desk Tool にアクセスするには、管理者にルート アクセス グループの権限が必要です。</p> <ul style="list-style-type: none"> <li>■ Horizon Help Desk Tool に対する読み取り専用アクセス。</li> <li>■ グローバル セッションを管理します。</li> <li>■ Horizon Console にログインできます。</li> <li>■ すべてのマシンおよびセッション関連のコマンドを実行します。</li> <li>■ リモートのプロセスとアプリケーションを管理します。</li> <li>■ 仮想デスクトップまたは公開デスクトップのリモート アシスタント。</li> </ul>	いいえ
ヘルプデスク管理者 (読み取り専用)	<p>ユーザーとセッションの情報を表示し、ドリルダウンでセッションの詳細情報を表示します。Horizon Help Desk Tool にアクセスするには、管理者にルート アクセス グループの権限が必要です。</p> <ul style="list-style-type: none"> <li>■ Horizon Help Desk Tool に対する読み取り専用アクセス。</li> <li>■ Horizon Console にログインできます。</li> </ul>	いいえ
インベントリ管理者	<ul style="list-style-type: none"> <li>■ すべてのマシン、セッション、およびプール関連の操作を実行する。</li> <li>■ 通常ディスクを管理します。</li> <li>■ リンク クローン プールを再同期、更新、再調整し、デフォルトのプール イメージを変更する。</li> <li>■ 自動ファームを管理します。</li> </ul> <p>管理者がアクセス グループに対してこのロールを持つ場合、そのアクセス グループ内のインベントリ オブジェクトに対してのみこれらの操作を実行できます。このロールを持つ管理者は、手動ファームまたは管理対象外の手動プールを作成できません。また、ファームまたは管理対象外の手動プールに RDS ホストの追加や削除を行うこともできません。</p>	はい
インベントリ管理者 (読み取り専用)	<p>インベントリ オブジェクトを表示する (変更はできない)。</p> <p>管理者がアクセス グループに対してこのロールを持つ場合、そのアクセス グループ内のインベントリ オブジェクトのみを表示できます。</p>	はい
ローカル管理者	<p>すべてのローカル管理者操作を実行する (追加の管理者ユーザーおよびグループの作成を除く)。クラウド ポッド アーキテクチャ環境では、このロールを持つ管理者は、グローバル データ レイヤで操作を実行したり、リモート ポッドでセッションを管理することはできません。</p> <p><b>注:</b> ローカル管理者ロールを持つ管理者は、Horizon Help Desk Tool にアクセスできません。CPA 以外の環境の管理者にグローバル セッションの管理権限はありません。Horizon Help Desk Tool でタスクを実行するには、この権限が必要です。</p>	はい
ローカル管理者 (読み取り専用)	<p>管理者 (読み取り専用) ロールと同じ (グローバル データ レイヤでのインベントリ オブジェクトおよび設定の表示を除く)。このロールを持つ管理者は、ローカル ポッドでのみ読み取り専用の権限を持ちます。</p> <p><b>注:</b> ローカル管理者 (読み取り専用) ロールを持つ管理者は、Horizon Help Desk Tool にアクセスできません。CPA 以外の環境の管理者にグローバル セッションの管理権限はありません。Horizon Help Desk Tool でタスクを実行するには、この権限が必要です。</p>	はい

## グローバル権限

グローバル権限は、グローバル設定の表示や変更などシステム全体の操作を制御します。グローバル権限のみを含むロールはアクセス グループに適用できません。

次の表で、グローバル権限について説明し、各権限を含む定義済みのロールを示します。

表 7-7. グローバル権限

権限	ユーザーが可能な操作	定義済みロール
コンソール操作	Horizon Console にログインして使用します。	管理者 管理者（読み取り専用） インベントリ管理者 インベントリ管理者（読み取り専用） グローバル構成およびポリシー管理者 グローバル構成およびポリシー管理者（読み取り専用） ヘルプデスク管理者 ヘルプデスク管理者（読み取り専用） ローカル管理者 ローカル管理者（読み取り専用）
直接操作	すべての PowerShell コマンドやコマンドライン ユーティリティ（vdmadmin および vdmimport 以外）を実行する。  vdmadmin、vdmimport、および lmvutil コマンドを使用する管理者には、ルート アクセス グループに対する管理者ロールが必要です。	管理者 管理者（読み取り専用）
グローバル構成とポリシーを管理	グローバル ポリシーおよび設定（管理者ロールおよび権限を除く）を表示し、変更する。	管理者 グローバル構成およびポリシー管理者
グローバル セッションを管理	グローバル セッションはクラウド ポッド アーキテクチャ環境で管理します。	管理者
ロールと権限を管理	管理者ロールおよび権限を作成、変更、削除する。	管理者
エージェントを登録	物理システム、スタンドアロン仮想マシン、RDS ホストなどの管理対象外のマシンに Horizon Agent をインストールする。  Horizon Agent のインストール時に、管理者ログイン認証情報を指定し、Connection Server インスタンスに管理対象外のマシンを登録する必要があります。	管理者 エージェント登録管理者

## オブジェクト固有の権限

オブジェクト固有権限は、特定のタイプのインベントリ オブジェクトの操作を制御します。オブジェクト固有の権限を含むロールは、アクセス グループに適用することができます。

次の表に、オブジェクト固有の権限を示します。定義済みのロール Administrators（管理者）および Inventory Administrators（インベントリ管理者）にはこれらのすべての権限が含まれます。

表 7-8. オブジェクト固有の権限

権限	ユーザーが可能な操作	オブジェクト
ファームおよびデスクトップ プールを有効にする	デスクトップ プールを有効または無効にする。	デスクトップ プール、ファーム
デスクトップおよびアプリケーション プールに資格を割り当てる	ユーザーの資格を追加または削除する。	デスクトップ プール、アプリケーション プール
Composer デスクトップ プールイメージを管理	リンク クローン プールを再同期、更新、再調整し、デフォルトのプール イメージを変更する。	デスクトップ プール
マシンを管理	すべてのマシンおよびセッション関連の操作を実行します。	マシン
通常ディスクを管理	Horizon Composer パーシステント ディスクの操作を実行します (パーシステント ディスクの接続、接続解除、インポートなど)。	通常ディスク
ファーム、デスクトップおよびアプリケーション プールを管理	ファームを追加、変更、削除します。デスクトップおよびアプリケーション プールの追加、変更、削除、資格割り当てを行います。マシンを追加および削除します。	デスクトップ プール、アプリケーション プール、ファーム
セッションを管理	セッションを切断してログオフし、ユーザーにメッセージを送信します。	セッション
再起動操作を管理	仮想マシンをリセットしたり、仮想デスクトップを再起動したりします。	マシン

## 内部権限

一部の定義済みの管理者ロールには、内部権限が含まれています。カスタム ロールを作成するときに内部権限を選択することはできません。

次の表で、内部権限について説明し、各権限を含む定義済みのロールを示します。

表 7-9. 内部権限

権限	説明	定義済みロール
フル (読み取り専用)	すべての設定への読み取り専用アクセス権を付与します。	管理者 (読み取り専用)
Manage Inventory (Read only) (インベントリの管理 (読み取り専用))	インベントリ オブジェクトへの読み取り専用アクセス権を付与します。	インベントリ管理者 (読み取り専用)
Manage Global Configuration and Policies (Read only) (グローバル構成とポリシーの管理 (読み取り専用))	設定およびグローバル ポリシー (管理者とロールを除く) への読み取り専用アクセス権を付与します。	グローバル構成およびポリシー管理者 (読み取り専用)

## 一般的なタスクに必要な権限

多くの一般的な管理者タスクには、調整された一連の権限が必要です。一部の操作では、操作対象のオブジェクトへのアクセスに加えて、ルート アクセス グループでの権限が必要です。

## プール管理のための権限

管理者が Horizon Console でプールを管理するためには、特定の権限が必要です。

次の表に、一般的なプール管理タスクの一覧と、各タスクを実行するために必要となる権限を示します。

表 7-10. プール管理タスクと権限

タスク	必要な権限
デスクトップ プールを有効または無効にする。	ファームおよびデスクトップ プールを有効にする
プールに対する資格をユーザーに付与する、または資格を取り消す。	デスクトップおよびアプリケーション プールに資格を割り当てる
プールを追加する。	ファーム、デスクトップおよびアプリケーション プールを管理  <b>注:</b> 管理対象外のデスクトップ プールを追加する場合は適用されません。管理者は、このタスクを実行するためのグローバル設定およびポリシー管理者 (読み取り専用) ロールを持っている必要があります。
プールを変更または削除する。	ファーム、デスクトップおよびアプリケーション プールを管理  <b>注:</b> 管理対象外のデスクトップ プールを削除する場合は適用されません。管理者は、このタスクを実行するためのグローバル設定およびポリシー管理者 (読み取り専用) ロールを持っている必要があります。
プールにデスクトップを追加またはプールからデスクトップを削除する。	ファーム、デスクトップおよびアプリケーション プールを管理  <b>注:</b> デスクトップ プールで管理対象外の仮想デスクトップを追加または削除する場合は適用されません。管理者は、このタスクを実行するためのグローバル設定およびポリシー管理者 (読み取り専用) ロールを持っている必要があります。
デフォルトの Horizon Console イメージを更新、再構成、再調整または変更する。	Composer デスクトップ プール イメージを管理
アクセス グループを変更する。	ソースおよびターゲット アクセス グループでの [ファーム、デスクトップおよびアプリケーション プールを管理]。

## マシン管理のための権限

管理者が Horizon Console でマシンを管理するためには、特定の権限が必要です。

次の表に、一般的なマシン管理タスクの一覧と、各タスクを実行するために必要な権限を示します。

表 7-11. マシン管理タスクと権限

タスク	必要な権限
仮想マシンを削除する。	マシンを管理 または [ファーム、デスクトップおよびアプリケーション プールを管理]  <b>注:</b> デスクトップ プールまたはファームから管理対象外のデスクトップまたは RDS ホストを削除する場合は適用されません。管理者は、このタスクを実行するためのグローバル設定およびポリシー管理者 (読み取り専用) ロールを持っている必要があります。
仮想マシンをリセットする。	再起動操作を管理
仮想デスクトップを再起動する。	再起動操作を管理

タスク	必要な権限
ユーザー所有権を割り当てるか、削除する。	マシンを管理
メンテナンス モードに切り替えるか、メンテナンス モードを終了する。	マシンを管理
セッションから切断またはログオフする。	セッションを管理

## 通常ディスク管理のための権限

管理者が Horizon Console でパーシステント ディスクを管理するためには、特定の権限が必要です。

次の表に、一般的な通常ディスクの管理タスクの一覧と、各タスクを実行するために必要な権限を示します。これらのタスクは Horizon Console の [パーシステント ディスク] ページで実行します。

表 7-12. 通常ディスク管理タスクと権限

タスク	必要な権限
ディスクを接続解除する。	ディスクに対する通常ディスクを管理、およびプールに対するファーム、デスクトップおよびアプリケーション プールを管理。
ディスクを接続する。	マシンに対する通常ディスクを管理、およびマシンに対するファーム、デスクトップおよびアプリケーション プールを管理。
ディスクを編集する。	ディスクに対する通常ディスクを管理、および選択したプールに対するファーム、デスクトップおよびアプリケーション プールを管理。
アクセス グループを変更する。	ソースおよびターゲットのアクセス グループに対する通常ディスクを管理。
デスクトップを再作成する。	ディスクに対する通常ディスクを管理、最後のプールに対するファーム、デスクトップおよびアプリケーション プールを管理。
vCenter Server からインポートする。	フォルダに対する通常ディスクを管理、およびプールに対するプールの管理。
ディスクを削除する。	ディスクに対する通常ディスクを管理。

## ユーザーと管理者の管理のための権限

管理者が Horizon Console でユーザーと管理者を管理するためには、特定の権限が必要です。

次の表に、一般的なユーザーと管理者の管理タスクの一覧と、各タスクの実行に必要な権限を示します。ユーザーの管理は Horizon Console の [ユーザーとグループ] ページで行います。管理者の管理は Horizon Console の [グローバル管理者ビュー] ページで行います。

表 7-13. ユーザーと管理者の管理タスクと権限

タスク	必要な権限
全般的なユーザー情報を更新する。	グローバル構成とポリシーを管理
ユーザーにメッセージを送信する。	マシン上のリモート セッションの管理。
管理者ユーザーまたはグループを追加する。	ロールと権限を管理
管理者の権限を追加、変更または削除する。	ロールと権限を管理
管理者ロールを追加、修正または削除する。	ロールと権限を管理



## Horizon Help Desk Tool タスクの権限

Horizon Help Desk Tool の管理者には、Horizon Console でトラブルシューティング タスクを実行するため、特定の権限が必要です。

次の表に、Horizon Help Desk Tool の管理者が実行できる一般的なタスクと、各タスクの実行に必要な権限を示します。

表 7-14. Horizon Help Desk Tool タスクと権限

タスク	必要な権限
Horizon Help Desk Tool に対する読み取り専用アクセス。	[ヘルプデスクを管理 (読み取り専用)]
グローバル セッションを管理します。	[グローバル セッションを管理]
Horizon Console にログインできます。	[コンソール操作]
すべてのマシンおよびセッション関連のコマンドを実行します。	[マシンを管理]
マシンをリセットまたは再起動します。	[再起動操作を管理]
セッションから切断してログオフします。	[セッションを管理]
リモートのプロセスとアプリケーションを管理します。	[リモートのプロセスとアプリケーションを管理]
仮想デスクトップまたは公開デスクトップのリモート アシスタント。	[リモート アシスタンス]
グローバル セッションの切断、ログアウト、リセット、再起動操作。	[ヘルプデスクを管理 (読み取り専用)]、[グローバル セッションを管理]
ローカル セッションのリセットと再起動操作。	[ヘルプデスクを管理 (読み取り専用)]、[再起動操作を管理]
リモート アシスタンス操作。	[ヘルプデスクを管理 (読み取り専用)]、[リモート アシスタンス]
リモートのプロセスとアプリケーションを終了します。	[ヘルプデスクを管理 (読み取り専用)]、[リモートのプロセスとアプリケーションを管理]
Horizon Help Desk Tool で、すべてのタスクを実行します。	[ヘルプデスクを管理 (読み取り専用)]、[グローバル セッションを管理]、[再起動操作を管理]、[リモート アシスタンス]、[リモートのプロセスとアプリケーションを管理]
リモート アシスタンス操作とリモートのプロセスとアプリケーションの終了。	[ヘルプデスクを管理 (読み取り専用)]、[リモート アシスタンス]、[リモートのプロセスとアプリケーションを管理]
ローカル セッションの切断とログアウト操作。	[ヘルプデスクを管理 (読み取り専用)]、[セッションを管理]

## 一般的な管理タスクと管理コマンドのための権限

管理者が一般的な管理タスクを実行したりコマンド ライン ユーティリティを実行したりするには、特定の権限が必要です。

次の表に、一般的な管理タスクやコマンド ライン ユーティリティを実行するために必要な権限を示します。

表 7-15. 一般的な管理タスクと管理コマンドのための権限

タスク	必要な権限
アクセス グループを追加または削除する	ルート アクセス グループに対する管理者ロールが必要。
Horizon Administrator で ThinApp アプリケーションおよび設定を管理する	ルート アクセス グループに対する管理者ロールが必要。

タスク	必要な権限
物理システム、スタンドアロン仮想マシン、RDS ホストなどの管理対象外のマシンに Horizon Agent をインストールする	エージェントを登録
Horizon Administrator で設定（管理者向けを除く）を表示または修正する	グローバル構成とポリシーを管理
すべての PowerShell コマンドやコマンドライン ユーティリティ（vdmadmin および vdmimport 以外）を実行する。	直接操作
vdmadmin および vdmimport コマンドを使用する	ルート アクセス グループに対する管理者ロールが必要。
vdmexport コマンドを使用する	ルート アクセス グループに対する管理者ロールまたは管理者（読み取り専用）ロールが必要。

## 管理者ユーザーおよびグループに関するベスト プラクティス

Horizon 7 環境のセキュリティと管理性を高めるために、管理者ユーザーおよびグループを管理するときのベスト プラクティスに従うようにしてください。

- Active Directory に新しいユーザー グループを作成して、作成したグループに管理者ロールを割り当てます。Horizon 7 権限を持つ必要のない、または持つべきではないユーザーが含まれる可能性があるため、Windows のビルトイン グループやその他の既存グループは使用しないようにします。
- Horizon 7 管理権限を持つユーザーの数は最小限にします。
- 管理者ロールにはすべての権限が含まれるため、日常的な管理に管理者ロールを使用しないでください。
- 目につきやすく推測が容易なため、管理者ユーザーおよびグループを作成するときは Administrator という名前の使用を避けます。
- アクセス グループを作成して、機密情報を扱うデスクトップとファームを分離します。それらのアクセス グループの管理を限られたユーザーに委任します。
- グローバル ポリシーと Horizon 7 設定を変更できる管理者を別途作成します。

# Horizon Console でのポリシーの設定

Horizon Console 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。

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:** 公開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。公開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。

---

この章には、次のトピックが含まれています。

- **グローバル ポリシーの設定**

## グローバル ポリシーの設定

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。

### 手順

- 1 Horizon Console で、[設定] - [グローバル ポリシー] の順に選択します。

[グローバル ポリシー] ペインには、すべてのクライアント セッション、デスクトップ プールまたはユーザーに影響する設定が表示されます。

表 8-1. Horizon 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ようにするには、安全なネットワークで 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>

2 [ポリシーを編集] をクリックして設定を変更します。

3 [OK] をクリックして変更を保存します。

# Horizon 7 コンポーネントのメンテナンス

# 9

Horizon 7 コンポーネントが常に使用でき、実行し続けるように、さまざまなメンテナンス タスクを実行できます。

この章には、次のトピックが含まれています。

- [Horizon 7 構成データのバックアップと復元](#)
- [Horizon Connection Server と Horizon Composer の構成データのリストア](#)
- [Horizon Composer データベースのデータのエクスポート](#)
- [Horizon Console での製品ライセンス キーまたはライセンス モードの変更](#)
- [ライセンス使用量の監視](#)
- [カスタマ エクスペリエンス向上プログラム](#)

## Horizon 7 構成データのバックアップと復元

Horizon Console で自動バックアップをスケジュールリングするか実行して、Horizon 7 と Horizon Composer の構成データをバックアップできます。Horizon 7 構成をリストアするには、バックアップした View LDAP ファイルと Horizon Composer データベース ファイルを手動でインポートします。

バックアップと復元機能を使用して、Horizon 7 構成データを保持および移行できます。

## Horizon Connection Server と Horizon Composer のデータのバックアップ

Connection Server の初期構成が完了したら、Horizon 7 と Horizon Composer の構成データの定期的なバックアップをスケジュールリングする必要があります。Horizon Console を使用すると、Horizon 7 と Horizon Composer のデータを保持できます。

Horizon 7 は、Connection Server の構成データを View LDAP リポジトリに保存します。Horizon Composer は、Horizon Composer データベースにリンク クローン デスクトップの設定データを保存します。

Horizon Console を使用してバックアップを実行すると、Horizon 7 が View LDAP 構成データと Horizon Composer データベースをバックアップします。両方のバックアップ ファイル セットは同じ場所に保存されます。View LDAP データは暗号化された LDAP データ交換形式 (LDIF) でエクスポートされます。View LDAP の説明については、『Horizon 7 の管理』の「View LDAP ディレクトリ」を参照してください。

バックアップは複数の方法で実行できます。

- Horizon 7 構成バックアップ機能を使用して自動バックアップをスケジュール設定します。

- Horizon Console の [今すぐバックアップ] 機能を使用してすぐにバックアップを開始します。
- `vdmexport` ユーティリティを使用して、手動で View LDAP データをエクスポートします。このユーティリティは、Connection Server の各インスタンスで提供されます。

`vdmexport` ユーティリティは、View LDAP データを暗号化された LDIF データ、プレーン テキスト、パスワードなどの秘密データが削除されたプレーン テキストとしてエクスポートできます。

---

**注:** `vdmexport` ツールは View LDAP データのみをバックアップします。このツールは Horizon Console データベース情報はバックアップしません。

---

`vdmexport` の詳細については、[Horizon Connection Server からの構成データのエクスポート](#)を参照してください。

次のガイドラインは、Horizon 7 構成データのバックアップに適用されます。

- Horizon 7 は任意の Connection Server インスタンスから構成データをエクスポートできます。
- 複製されたグループに複数の Connection Server インスタンスがある場合は、1 つのインスタンスのデータをエクスポートするだけで済みます。複製されたすべてのインスタンスに同じ構成データが含まれています。
- Connection Server の複製されたインスタンスを使用しているからといって、バックアップ メカニズムが機能していると考えないでください。Horizon 7 が Connection Server の複製されたインスタンスのデータの同期を実行するとき、1 つのインスタンスで何らかのデータが失われていると、グループのすべてのメンバーでそのデータが失われる可能性があります。
- Connection Server が複数の Horizon Composer サービスで複数の vCenter Server インスタンスを使用する場合、Horizon 7 は vCenter Server インスタンスに関連付けられているすべての Horizon Composer データベースをバックアップします。

## Horizon 7 構成バックアップのスケジュール

Horizon 7 構成データを定期的にバックアップするようにスケジュールを設定できます。Horizon 7 は、Connection Server インスタンスが構成データを格納する View LDAP リポジトリの内容をバックアップします。

構成をすぐにバックアップするには、Connection Server インスタンスを選択し、[今すぐバックアップ] をクリックします。

### 前提条件

バックアップ設定について理解しておきます。[Horizon 7 構成バックアップ設定](#)を参照してください。

### 手順

- 1 Horizon Console で、[設定] - [サーバ] の順に選択します。
- 2 [Connection Server] タブで、バックアップ対象の Connection Server インスタンスを選択して [今すぐバックアップ] をクリックします。
- 3 [バックアップ] タブで、Horizon 7 構成バックアップ設定を指定して、バックアップの頻度、バックアップの最大数、バックアップ ファイルのフォルダの場所を設定します。

- 4 (オプション) データ リカバリのパスワードを変更します。
  - a [データ リカバリのパスワードを変更] をクリックします。
  - b 新しいパスワードを 2 回入力します。
  - c (オプション) パスワードを忘れた場合のヒントを入力します。
  - d [OK] をクリックします。
- 5 [OK] をクリックします。

## Horizon 7 構成バックアップ設定

Horizon 7 では、Connection Server と Horizon Composer の構成データを定期的にバックアップできます。Horizon Console で、バックアップ処理の頻度とその他の側面を設定できます。

表 9-1. Horizon 7 構成バックアップ設定

設定	説明
Automatic backup frequency (自動バックアップの頻度)	Every Hour (1 時間ごと) : 1 時間ごとにバックアップを行います。 Every 6 Hours (6 時間ごと) : 午前 0 時、午前 6 時、午後 0 時、午後 6 時にバックアップを行います。 Every 12 Hours (12 時間ごと) : 午前 0 時と午後 0 時にバックアップを行います。 Every Day (毎日) : 毎日午前 0 時にバックアップを行います。 Every 2 Days (2 日ごと) : 土曜日、月曜日、水曜日、金曜日の午前 0 時にバックアップを行います。 Every Week (毎週) : 毎週、土曜日の午前 0 時にバックアップを行います。 Every 2 Weeks (2 週ごと) : 隔週の土曜日の午前 0 時にバックアップを行います。 Never (バックアップしない) : 自動バックアップを行いません。
バックアップ時間	バックアップをスケジュールリングする時間。
バックアップ時間のオフセット	スケジュールされたバックアップの時間のオフセット。
Max number of backups (バックアップの最大数)	Connection Server インスタンスに格納できるバックアップ ファイル数です。この数には、0 より大きい整数を指定する必要があります。 最大数に達すると、Horizon 7 は最も古いバックアップ ファイルを削除します。 この設定は、[今すぐバックアップ] を使用した場合に作成されるバックアップ ファイルにも適用されます。
フォルダの場所	Connection Server が実行されているコンピュータでバックアップ ファイルが保存されるデフォルトの場所 : C:\Programdata\VMWare\VDM\backups [今すぐバックアップ] を使用した場合も、Horizon 7 ではこの場所にバックアップ ファイルを保存します。

## Horizon Connection Server からの構成データのエクスポート

View LDAP リポジトリの内容をエクスポートして、Horizon Connection Server インスタンスの構成データをバックアップできます。

`vdmexport` コマンドを使用して、View LDAP 構成データを暗号化された LDIF ファイルにエクスポートします。  
`vdmexport -v` (逐語的) オプションを使用してデータをプレーン テキスト LDIF ファイルにエクスポートすること  
 も、`vdmexport -c` (クレンジング) オプションを使用してデータをパスワードなどの秘密データが削除されたプレーン テキストとしてエクスポートすることもできます。

任意の Connection Server インスタンスで `vdmexport` コマンドを実行できます。複製されたグループに複数の Connection Server インスタンスがある場合は、1 つのインスタンスのデータをエクスポートするだけで済みます。複製されたすべてのインスタンスに同じ構成データが含まれています。

---

**注:** `vdmexport.exe` コマンドは View LDAP データのみをバックアップします。このコマンドは Horizon Composer データベース情報はバックアップしません。

---

#### 前提条件

- Connection Server とともにインストールされている `vdmexport.exe` コマンドの実行可能ファイルを次のフォルトパスで見つけます。

`C:\Program Files\VMware\VMware View\Server\tools\bin`

- Administrators（管理者）または Administrators (Read Only)（管理者（読み取り専用））ロールのユーザーとして Connection Server インスタンスにログインします。

#### 手順

- 1 [スタート]-[コマンド プロンプト] を選択します。
- 2 コマンド プロンプトで `vdmexport` コマンドを入力し、出力をファイルにリダイレクトします。例：

```
vdmexport > Myexport.LDF
```

デフォルトでは、エクスポートされるデータは暗号化されています。

出力ファイル名を `-f` オプションの引数として指定できます。例：

```
vdmexport -f Myexport.LDF
```

`-v` オプションを使用することで、データをプレーン テキスト形式（逐語的）でエクスポートできます。例：

```
vdmexport -f Myexport.LDF -v
```

`-c` オプションを使用することで、データをパスワードなどの秘密データが削除されたプレーン テキスト形式（クレンジング データ）でエクスポートできます。例：

```
vdmexport -f Myexport.LDF -c
```

---

**注:** View LDAP 構成を復元するためにクレンジング バックアップ データの使用は検討しないでください。クレンジング構成データでは、パスワードなどの重要な情報が欠落しています。

---

`vdmexport` コマンドの詳細については、『Horizon 7 の統合』を参照してください。

#### 次のステップ

`vdmimport` コマンドを使用して、Connection Server の構成情報を復元または転送できます。

LDIF ファイルのインポートの詳細については、[Horizon Connection Server と Horizon Composer の構成データのリストア](#)を参照してください。



# Horizon Connection Server と Horizon Composer の構成データのリストア

Horizon 7 によってバックアップされた Connection Server LDAP 構成ファイルおよび Horizon Composer データベース ファイルを手動でリストアできます。

個別のユーティリティを手動で実行して、Connection Server と Horizon Composer の構成データをリストアします。

構成データをリストアする前に、Horizon Console で構成データをバックアップしたことを確認します。[Horizon Connection Server と Horizon Composer のデータのバックアップ](#)を参照してください。

`vdmimport` ユーティリティを使用して、Connection Server データを LDIF バックアップ ファイルから Connection Server インスタンス内の View LDAP リポジトリにインポートします。

`SviConfig` ユーティリティを使用すると、Horizon Composer データを `.svi` バックアップ ファイルから Horizon Composer SQL データベースにインポートできます。

---

**注:** 場合によっては、Connection Server インスタンスの現在のバージョンをインストールし、Connection Server の LDAP 構成ファイルをインポートして既存の Horizon 7 構成を復元しなければならないことがあります。既存の Horizon 7 構成で 2 番目のデータセンターをセットアップするときなどは、ビジネス継続性とディザスタ リカバリ (BC/DR) 計画の一環としてこの手順が必要になる場合があります。詳細については、『Horizon 7 のインストール』を参照してください。

---

## Horizon Connection Server への構成データのインポート

LDIF ファイルに格納されているデータのバックアップ コピーをインポートして、Connection Server インスタンスの構成データを復元できます。

`vdmimport` コマンドを使用して、LDIF ファイルのデータを Connection Server インスタンス内の View LDAP リポジトリにインポートします。

Horizon Console またはデフォルトの `vdmexport` コマンドを使用して View LDAP 構成をバックアップした場合、エクスポートされた LDIF ファイルは暗号化されています。LDIF ファイルの暗号化を解除してからでないと、インポートできません。

エクスポートされた LDIF ファイルがプレーン テキスト形式の場合、ファイルの暗号化を解除する必要はありません。

---

**注:** クレンジング形式の LDIF ファイルをインポートしないでください。この形式では、パスワードなどの秘密データが削除されたプレーン テキストになっています。インポートすると、復元された View LDAP リポジトリから重要な構成情報が失われます。

---

View LDAP リポジトリのバックアップの詳細については、[Horizon Connection Server と Horizon Composer のデータのバックアップ](#)を参照してください。

### 前提条件

- Connection Server とともにインストールされている `vdmimport` コマンドの実行可能ファイルを次のデフォルト パス配下で探します。

C:\Program Files\VMware\VMware View\Server\tools\bin

- 管理者ロールのユーザーとして Connection Server インスタンスにログインします。
- データ リカバリ パスワードを知っていることを確認します。パスワード リマインダが構成されていた場合、パスワード オプションを付けずに `vdmimport` コマンドを実行することでリマインダを表示できます。

#### 手順

- 1 Horizon Composer が実行されているサーバで VMware Horizon Composer Windows サービスを停止し、Horizon Composer のすべてのインスタンスを停止します。
- 2 Horizon Connection Server のすべてのインスタンスをアンインストールします。  
VMware Horizon Connection Server と AD LDS Instance VMwareVDMDS の両方をアンインストールします。
- 3 1 つの Connection Server インスタンスをインストールします。
- 4 Windows サービスの VMware Horizon Connection Server を停止して、Connection Server インスタンスを停止します。
- 5 [スタート]-[コマンド プロンプト] の順にクリックします。
- 6 LDIF ファイルの暗号化を解除します。  
  
コマンド プロンプトで、`vdmimport` コマンドを入力します。-d オプション、-p オプションとデータ リカバリ パスワード、-f オプションと既存の暗号化された LDIF ファイルを指定し、次に暗号化を解除された LDIF ファイルの名前を指定します。例：  
  
データ リカバリ パスワードを覚えていない場合は、-p オプションを使用せずにコマンドを入力します。ユーティリティでパスワード リマインダが表示され、パスワードを入力するように要求されます。
- 7 暗号化が解除された LDIF ファイルをインポートし、View LDAP 構成を復元します。  
  
-f オプションと暗号化を解除された LDIF ファイルを指定します。例：
- 8 Connection Server をアンインストールします。  
  
VMware Horizon Connection Server パッケージのみをアンインストールします。
- 9 Connection Server を再インストールします。
- 10 Horizon Console にログインして、構成が正しいかどうかを検証します。
- 11 Horizon Composer インスタンスを開始します。
- 12 レプリカ サーバインスタンスを再インストールします。

`vdmimport` コマンドは、Connection Server 内の View LDAP リポジトリを LDIF ファイルの構成データで更新します。`vdmimport` コマンドの詳細については、『Horizon 7 のインストール』を参照してください。

**注:** リストアされる構成が、vCenter Server および Horizon Composer（使用されている場合）に認識される仮想マシンと一致することを確認します。必要に応じて、Horizon Composer の構成をバックアップからリストアします。[Horizon Composer データベースのリストア](#)を参照してください。Horizon Composer 構成のバックアップによって vCenter Server 内の仮想マシンが変更された場合は、Horizon Composer 構成をリストアした後に不整合を手動で解決する必要があります。

## Horizon Composer データベースのリストア

Horizon Composer 構成のバックアップ ファイルを、リンク クローン情報が格納された Horizon Composer データベースにインポートできます。

`SviConfig restoredata` コマンドを使用して、システムの障害の発生後に Horizon Composer データベースデータをリストアしたり、Horizon Composer 構成を以前の状態に戻したりすることができます。

**重要:** `SviConfig` ユーティリティは、熟練した Horizon Composer 管理者のみが使用する必要があります。このユーティリティは、Horizon Composer サービスに関連する問題を解決するためのものです。

### 前提条件

Horizon Composer データベース バックアップ ファイルの場所を確認します。デフォルトでは、Horizon 7 はバックアップ ファイルを Connection Server コンピュータの C: ドライブ (C:\Programdata\VMware\VDM\backups) に格納します。

Horizon Composer バックアップ ファイルは日付スタンプと `.svi` サフィックスが付く命名規則を使用します。

`Backup-YearMonthDayCount-vCenter Server Name_Domain Name.svi`

例: `Backup-20090304000010-foobar_test_org.svi`

`SviConfig restoredata` パラメータについて理解しておく必要があります。

- `DsnName` - データベースに接続するために使用される DSN。`DsnName` パラメータは必須で、空の文字列にすることはできません。
- `Username` - データベースに接続するために使用されるユーザー名。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` - データベースに接続するために使用されるパスワード。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。
- `BackupFilePath` - Horizon Composer バックアップ ファイルへのパス。

`DsnName` および `BackupFilePath` パラメータは必須で、空の文字列にすることはできません。`Username` および `Password` パラメータはオプションです。

## 手順

- 1 Horizon Composer バックアップ ファイルを、Connection Server コンピュータから、VMware Horizon Composer サービスがインストールされているコンピュータからアクセス可能な場所にコピーします。
- 2 Horizon Composer がインストールされているコンピュータで、VMware Horizon Composer サービスを停止します。
- 3 Windows のコマンド プロンプトを開き、SviConfig 実行可能ファイルに移動します。

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

- 4 SviConfig restoredata コマンドを実行します。

```
sviconfig -operation=restoredata
          -DsnName=target_database_source_name_(DSN)
          -Username=database_administrator_username
          -Password=database_administrator_password
          -BackupFilePath=path_to_View_Composer_backup_file
```

例：

```
sviconfig -operation=restoredata -dsnname=LinkedClone
          -username=Admin -password=Pass
          -backupfilepath="C:\Program Files (x86)\VMware\VMware View
Composer\Backup-20090304000010-foobar_test_org.SVI"
```

- 5 VMware Horizon Composer サービスを開始します。

## 次のステップ

SviConfig restoredata コマンドの出力結果コードについては、[Horizon Console データベースのリストアの結果コード](#)を参照してください。

## Horizon Console データベースのリストアの結果コード

Horizon Console データベースをリストアすると、SviConfig restoredata コマンドで結果コードが表示されます。

表 9-2. restoredata の結果コード

コード	説明
0	操作は正常に終了しました。
1	指定された DSN が見つかりませんでした。
2	無効なデータベース管理者認証情報が指定されました。
3	データベースのドライバがサポートされていません。
4	予期しない問題が発生し、コマンドは完了できませんでした。

コード	説明
14	別のアプリケーションが VMware Horizon Console サービスを使用しています。コマンドを実行する前にサービスをシャットダウンしてください。
15	復元処理中に問題が発生しました。詳細については、画面のログ出力を参照してください。

## Horizon Composer データベースのデータのエクスポート

Horizon Composer データベースからデータをファイルにエクスポートできます。

**重要:** 熟練した Horizon Composer 管理者である場合に限り、SviConfig ユーティリティを使用してください。

### 前提条件

デフォルトでは、Horizon 7 はバックアップ ファイルを Connection Server コンピュータの C: ドライブ (C:\Programdata\VMWare\VDM\backups) に格納します。

SviConfig exportdata パラメータについて理解しておく必要があります。

- DsnName - データベースに接続するために使用される DSN。指定しなければ、DSN 名、ユーザー名、およびパスワードは、サーバの構成ファイルから取得されません。
- Username - データベースに接続するために使用されるユーザー名。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 - データベースに接続するために使用されるパスワード。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。
- OutputFilePath - 出力ファイルへのパス。

### 手順

- 1 Horizon Composer がインストールされているコンピュータで、VMware Horizon Composer サービスを停止します。
- 2 Windows のコマンド プロンプトを開き、SviConfig 実行可能ファイルに移動します。

このファイルは、Horizon Composer アプリケーションと同じ場所にあります。

*Horizon-Composer-installation-directory\sconfig.exe*

- 3 SviConfig exportdata コマンドを実行します。

```
sviconfig -operation=exportdata
          -DsnName=target_database_source_name_(DSN)
          -Username=database_administrator_username
          -Password=database_administrator_password
          -OutputFilePath=path_to_Horizon_Composer_output_file
```

例：

```
sviconfig -operation=exportdata -dsnname=LinkedClone
-username=Admin -password=Pass
-outputfilepath="C:\Program Files\VMware\VMware View
Composer\Export-20090304000010-foobar_test_org.SVI"
```

#### 次のステップ

SviConfig exportdata コマンドのエクスポート結果コードについては、[Horizon Composer データベースのエクスポートの結果コード](#)を参照してください。

## Horizon Composer データベースのエクスポートの結果コード

Horizon Composer データベースをエクスポートすると、SviConfig exportdata コマンドで終了コードが表示されます。

表 9-3. Exportdata ExitStatus コード

コード	説明
0	データのエクスポートが問題なく終了しました。
1	指定された DSN 名が見つかりません。
2	指定した証明書は無効です。
3	サポートされないドライバがデータベースに提供されました。
4	予期しない問題が発生しました。
18	データベース サーバに接続できません。
24	出力ファイルを開くことができません。

## Horizon Console での製品ライセンス キーまたはライセンス モードの変更

システムに対する現在のライセンスの有効期限が切れる場合や、現在ライセンスされていない Horizon 7 機能にアクセスする必要がある場合は、Horizon Console を使用して製品のライセンス キーを変更できます。VMware Horizon Cloud Service の Horizon 7 デプロイに基づいて、Horizon 7 の無期限ライセンスまたはサブスクリプション ライセンスのいずれかを取得できます。Horizon Console を使用して、ポッドのライセンス モードをサブスクリプション ライセンスから無期限ライセンスに変更できます（その逆の変更も可能）。

Horizon 7 の実行中に Horizon 7 にライセンスを追加できます。システムを再起動する必要はなく、デスクトップおよびアプリケーションへのアクセスは中断されません。

#### 前提条件

- Horizon 7 と、Horizon Composer や公開アプリケーションなどのアドオン機能を正常に動作させるため、有効な製品のライセンス キーを入手してください。

- サブスクリプション ライセンスを使用するには、サブスクリプション ライセンスで Horizon 7 を有効にしていることを確認します。『Horizon 7 のインストール』を参照してください。[ライセンス] パネルには、Horizon 7 ポッドのサブスクリプション ライセンスに関する情報が表示されます。

#### 手順

- 1 Horizon Console で、[設定] - [製品のライセンスと使用状況] の順に選択します。  
現在のライセンス キーの最初と最後の 5 文字は、[ライセンス] パネルに表示されます。
- 2 ライセンス キーを編集するには、[ライセンスを編集] をクリックして、ライセンスのシリアル番号を入力し、[OK] をクリックします。  
更新されたライセンス情報が [ライセンスの設定] パネルに表示されます。
- 3 (オプション) Horizon 7 ポッドをサブスクリプション ライセンスから無期限ライセンスに変更するには、[無期限ライセンスを使用する] をクリックして [OK] をクリックします。  
更新されたライセンス情報が [ライセンスの設定] パネルに表示されます。
- 4 (オプション) Horizon 7 ポッドを無期限ライセンスからサブスクリプション ライセンスに変更するには、[サブスクリプション ライセンスを使用する] をクリックして [OK] をクリックします。これで、VMware Horizon Cloud Service 管理者はサブスクリプション ライセンスで Horizon 7 ポッドを有効にできます。  
更新されたライセンス情報が [ライセンスの設定] パネルに表示されます。
- 5 ライセンスの有効期限の日付を確認します。
- 6 お持ちの製品のライセンスによって使用資格が付与されている VMware Horizon 7 のエディションに基づいて、デスクトップ、アプリケーションのリモート処理、Horizon Composer ライセンスが有効または無効になっていることを確認します。  
エディションによっては、VMware Horizon 7 の一部の機能を使用できません。各エディションの機能セットの比較については、<http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf> を参照してください。
- 7 ライセンスの使用状況モデルが製品ライセンスで使用しているモデルと一致することを確認します。  
使用状況は、製品ライセンスのエディションおよび使用状況の取り決めによって、指定ユーザーまたは同時ユーザーの数でカウントされます。

## ライセンス使用量の監視

Horizon Console では、Horizon 7 に同時接続しているアクティブなユーザーを監視できます。[使用量の設定] パネルには、現在の使用量と過去の最も高い使用量が表示されます。これらの数値を使用して、製品ライセンスの使用状況を追跡できます。履歴使用状況データをリセットして、現在のデータで始めからやり直すこともできます。

Horizon 7 では、指定ユーザーのライセンス使用モデルと、同時ユーザーのライセンス使用モデルの 2 つを使用できます。Horizon 7 は、製品ライセンスのエディションや使用モデルの契約にかかわらず、環境内の指定ユーザーと同時ユーザーをカウントします。

指定ユーザーの場合、Horizon 7 は、Horizon 7 環境にアクセスした固有ユーザーの数をカウントします。指定ユーザーが複数の単一ユーザー デスクトップ、公開デスクトップおよび公開アプリケーションを実行すると、このユーザーは 1 回だけカウントされます。

指定ユーザーの場合、[使用量の設定] パネルの [現在] 列には、Horizon 7 環境を最初に構成してからのユーザー数、または指定ユーザー数を最後にリセットしてからのユーザー数が表示されます。[最高] 列は、指定ユーザーには該当しません。

同時ユーザーの場合、Horizon 7 は、セッションあたりの単一ユーザー デスクトップ接続数をカウントします。同時ユーザーが複数の単一ユーザー デスクトップを実行している場合、接続された各デスクトップ セッションは個別にカウントされます。

同時ユーザーの場合、公開デスクトップとアプリケーションの接続はユーザーごとにカウントされます。同時ユーザーが複数の公開デスクトップ セッションおよびアプリケーションを実行すると、このユーザーは 1 回だけカウントされます。各公開デスクトップやアプリケーションが別々の RDS ホストでホストされている場合であってもユーザーがカウントされるのは 1 回です。同時ユーザーが 1 台の単一ユーザー デスクトップの他に、さらに公開デスクトップとアプリケーションを実行していても、このユーザーがカウントされるのは 1 回だけです。

同時接続ユーザーの場合、[使用量の設定] パネルの [最大] 列には、並列デスクトップ セッションの最大数、公開デスクトップとアプリケーションのユーザー数が表示されます。カウントは Horizon 7 環境を最初に構成した時点、または最大数を最後にリセットした時点からのカウント数になります。

共同作業セッション数、およびセッションに接続していた共同作業ユーザー数を監視できます。

- アクティブ - 共同作業セッション：セッション オーナーが複数のユーザーにセッションへの参加を招待した場合のセッション数です。例：John が 2 人のユーザーを自分のセッションに招待し、Mary が 1 人のユーザーを自分のセッションに招待しました。この行の値は 2 になります。招待されたユーザーがセッションに参加したかどうかは関係ありません。
- アクティブ - 共同作業者の合計：共同作業セッションに接続したユーザーの合計数です。セッション オーナーおよびすべての共同作業ユーザーが含まれます。例：John は 2 人のユーザーを招待し、1 人だけがセッションに参加しました。Mary は 1 人のユーザーを招待しましたが、このユーザーはセッションには参加しませんでした。この行の値は 3 になります。John の共同作業セッションにはオーナーが 1 人と参加者が 1 人いました。Mary の共同作業セッションにはオーナーが 1 人で参加者はいませんでした。セッション オーナーがカウントされるため、共同作業者の合計数は、常に共同作業セッションの合計数と同等またはそれ以上になります。

## ライセンス使用量データのリセット

Horizon Console で、製品使用量データの履歴をリセットして、現在のデータからやり直すこともできます。

グローバル構成とポリシーを管理 権限を備えた管理者は、[最大数をリセット] 設定と [指定ユーザー数をリセット] 設定を選択できます。これらの設定へのアクセスを制限するには、指定した管理者にのみこの権限を付与してください。

### 前提条件

製品ライセンスの使用状況について理解しておきます。[ライセンス使用量の監視](#)を参照してください。

### 手順

- 1 Horizon Console で、[設定] - [製品のライセンスと使用状況] の順に選択します。



- 2 (オプション) [用途] ペインで [最大数をリセット] を選択します。  
履歴同時接続数の最高値が、現在の数値にリセットされます。
- 3 (オプション) [用途] ペインで [指定ユーザー数をリセット] を選択します。

## カスタマ エクスペリエンス向上プログラム

本製品は、VMware カスタマー エクスペリエンス向上プログラム (CEIP) に参加しています。この製品の CEIP に参加することも、参加を取り消すこともできます。

CEIP を通して収集されるデータおよび VMware のその使用目的に関する詳細は、信頼と確実性センター (<http://www.vmware.com/trustvmware/ceip.html>) に記載されています。

### 手順

- 1 Horizon Console で、[設定] - [製品のライセンスと使用状況] の順に選択します。
- 2 [カスタマー エクスペリエンス プログラム] タブで、[編集設定] をクリックします。
- 3 CEIP に参加するには、[VMware カスタマ エクスペリエンス向上プログラムに参加する] を選択します。  
このオプションを選択しないと、CEIP に参加できません。
- 4 (オプション) 組織の地理的な場所、業種、従業員数を選択します。
- 5 [OK] をクリックします。

# Horizon Console での仮想デスクトッププールの作成

# 10

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。仮想マシンと物理マシンにデスクトップを展開できます。マスター 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。マスター イメージは、基本イメージまたはゴールド イメージともいいます。

基本イメージやゴールド イメージを作成する方法、クローン作成用に仮想マシンを構成する方法については、『Horizon 7 での仮想デスクトップのセットアップ』ドキュメントを参照してください。

Horizon Console では、インスタント クローン デスクトップ プールまたはフル仮想マシンを含む自動デスクトップ プールを作成できます。

この章には、次のトピックが含まれています。

- [インスタントクローン デスクトップ プールの作成](#)
- [フル仮想マシンを含む自動デスクトップ プールの作成](#)
- [Horizon Console でのリンク クローン デスクトップ プールの作成](#)
- [Horizon Console での手動デスクトップ プールの作成](#)
- [デスクトップ プールの構成](#)
- [Horizon Console でのデスクトップ プールと仮想デスクトップの管理](#)
- [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](#)

## 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。

インスタントクローン デスクトップ プールは、vCenter Server の親仮想マシン（マスター イメージ）に基づいています。インスタント クローン デスクトップの場合、親仮想マシンは、Horizon 7 が作成して維持する内部仮想マシンであり、マスター イメージに基づいて作成されます。この内部親仮想マシンは変更できません。ただし、マスター イメージは変更できます。

インスタント クローン デスクトップ プールの作成とメンテナンスの詳細については、『Horizon 7 での仮想デスクトップのセットアップ』ドキュメントを参照してください。

## Horizon Console でインスタント 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 プールを作成するときに、特定のオプションを設定できます。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、vCenter Server で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、vCenter Server で親仮想マシンをシャットダウンする必要があります。スナップショットは、vCenter Server のクローンのマスター イメージです。

**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 10-1. 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	<p>[フローティング] または [専用] を選択します。</p> <p>フローティング ユーザー割り当てでは、ユーザーはプールからランダムに選択され、デスクトップに割り当てられます。</p> <p>専用ユーザー割り当てでは、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がユーザーに返されます。ログインからログアウトまでの間、同じデスクトップでコンピュータ名と MAC アドレスが保持されます。ユーザーがデスクトップに行った他の変更は保持されません。</p>	
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	<p>プールを識別する一意の名前。</p> <p>複数の Connection Server 構成が存在する場合、同じプール ID を使用する Connection Server 構成が存在していないことを確認します。Connection Server 構成は、1 台の Connection Server、または複数の Connection Server による構成が可能です。</p>	
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	<p>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。</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。</p> <p><b>注:</b> 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。</p>	
状態	<p>[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。</p> <p>[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。</p>	
Connection Server の制限	<p>プールへのアクセスを特定の Connection Server に制限するには、[参照] をクリックして、1 台以上の Connection Server 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 Connection Server 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>	
カテゴリ フォルダ	Windows クライアント デバイスのデスクトップ プール資格に、スタート メニューのショートカットを含むカテゴリ フォルダの名前を指定します。	

オプション	説明	値をここに記入
切断後に自動的にログオフ	<ul style="list-style-type: none"> <li>■ [直後] : ユーザーは切断時にログアウトします。</li> <li>■ [なし] : ユーザーはログオフされません。</li> <li>■ [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。</li> </ul> <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 Horizon 7 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/再起動を許可	<p>ユーザーが仮想マシンをリセットしたり、仮想デスクトップを再起動できるかどうかを指定します。</p> <p>リセット操作を行うと、仮想マシンがリセットされます。オペレーティング システムのグレースフル再起動は実行されません。この操作は、vCenter Server 仮想マシンが含まれる自動プールまたは手動プールにのみ適用されます。</p> <p>再起動操作を行うと、仮想マシンが再起動されます。オペレーティング システムのグレースフル再起動が実行されます。この操作は、vCenter Server 仮想マシンが含まれる自動プールまたは手動プールにのみ適用されます。</p>	
Refresh OS disk after logoff (ログオフ後に OS ディスクを更新)	<p>OS ディスクを更新するかどうかを選択します。</p> <ul style="list-style-type: none"> <li>■ [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。</li> <li>■ [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。</li> </ul> <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デスクトップが更新されます。</p> <ul style="list-style-type: none"> <li>■ [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。インスタント 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。</li> <li>■ [なし] : OS ディスクは更新されません。</li> </ul>	
仮想マシン ディスク容量を再利用	<p>効率の良いディスク フォーマットで作成されたインスタント クローンの未使用ディスク容量を ESXi ホストが再利用できるかどうかを指定します。領域再利用機能により、インスタント 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>	
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>容量再利用のトリガーとなる、インスタント 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容量の最小量 (GB) を入力します。未使用ディスク容量がこのしきい値を超過すると、Horizon 7 は ESXi ホストに OS ディスク上の容量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、Horizon 7 はそのマシンで領域再利用プロセスを開始します。</p> <p>デフォルト値は 1 GB です。</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	<p>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。</p>	
デフォルト表示プロトコル	<p>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。</p>	

オプション	説明	値をここに記入
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。 表示プロトコルの選択をユーザーに許可しません。	
3D レンダラー	<p>デスクトップに 3D グラフィックス レンダリングを選択します。</p> <p>3D レンダリングは、仮想ハードウェア バージョン 8 以降の仮想マシンを実行する Windows 7 以降のゲストでサポートされています。ハードウェアベースのレンダリングは、vSphere 5.1 環境の仮想ハードウェア バージョン 9 以降でサポートされています。ソフトウェア レンダリングは、vSphere 5.0 環境の仮想ハードウェア バージョン 8 以降でサポートされています。</p> <p>ESXi 5.0 ホストの場合、レンダリングに最大 128MB の VRAM を使用できます。ESXi 5.1 以降のホストの場合、VRAM の最大サイズは 512MB です。vSphere 6.0 のハードウェア バージョン 11 (HWv11) の仮想マシンでは、VRAM 値 (ビデオ メモリ) が変更されています。vSphere Web Client で [vSphere Client を使用して管理] オプションを選択して、これらのマシンのビデオ メモリを設定します。詳細については、『vSphere 仮想マシン管理』ガイドの「3D グラフィックスの構成」を参照してください。</p> <p>デフォルトの表示プロトコルに Microsoft RDP を選択し、ユーザーに表示プロトコルの選択を許可しない場合、3D レンダリングは無効になります。</p> <ul style="list-style-type: none"> <li>■ [NVIDIA GRID vGPU] : 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。このオプションを選択すると、vSphere Distributed Resource Scheduler (DRS) は使用できません。</li> </ul> <p>インスタント クローン デスクトップ プールに、NVIDIA GRID vGPU の表示プロトコルとして PCoIP または VMware Blast を選択できます。</p> <ul style="list-style-type: none"> <li>■ [vSphere Client を使用して管理]。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。Horizon 7 は 3D レンダリングを制御しません。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、Horizon Console で設定した場合と同じ効果を持ちます。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。[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]、[モニターの最大数]、[特定のモニターの最大解像度] の設定が Horizon Console 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。</li> <li>■ [無効化] : 3D レンダリングが非アクティブです。デフォルトでは無効になっています。</li> </ul>	
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、『VMware Horizon HTML Access のインストールとセットアップ ガイド』を参照してください。</p> <p>VMware Identity Manager で HTML Access を使用するには、『Horizon 7 の管理 管理ガイド』の説明に従って Connection Server 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、Connection Server で使用するために構成する必要があります。</p>	
セッション共同作業を許可	デスクトップ プールのユーザーに、リモート デスクトップ セッションへの他のユーザーの招待を許可するには、[有効] を選択します。セッション オーナーとセッション共同作業者は、VMware Blast プロトコルを使用する必要があります。	
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 Horizon 7 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。	
名前付けパターン	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 Horizon 7 で使用するパターンを指定します。	

オプション	説明	値をここに記入
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。	
オンデマンドでマシンをプロビジョニング	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。	
マシンの最小数	■ [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、Horizon 7 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。	
全マシンを事前にプロビジョニング	■ [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、Horizon 7 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	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。 このオプションを選択すると、1 つ以上のインスタントクローン データストアまたはレプリカ ディスク データストアを選択するオプションを選択できます。	
vCenter の親仮想マシン	プールに vCenter Server 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）	これらのパラメータを親仮想マシンで設定してスナップショットを取得し、インスタント クローン デスクトップ プールのモニター数と解像度を指定します。必要な vRAM サイズは、仕様に基づいて計算されます。プールのマスター 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。スナップショットに基づいてインスタント クローン デスクトップ プールが作成され、これらのメモリ設定が継承されます。vSphere Client のビデオメモリの設定方法については、vSphere ドキュメントの『vSphere 単一ホスト管理』ガイド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 プールの解像度を変更する方法については、VMware ナレッジベース（KB）の記事 <a href="http://kb.vmware.com/kb/2151745">http://kb.vmware.com/kb/2151745</a> を参照してください。 スナップショットには次の詳細が含まれます。 ■ モニター数 ■ VRAM サイズ ■ 解像度	
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。	
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	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。 [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。  <b>注:</b> インスタント クローンと Storage vMotion には互換性があります。Storage DRS データストアにインスタント クローン デスクトップ プールを作成する場合、Storage DRS クラスタがデータストアのリストに表示されません。ただし、個々の Storage DRS のデータストアは選択できます。	

オプション	説明	値をここに記入
レプリカ ディスク データストア	<p>インスタントクローンを格納するレプリカ ディスク データストアを 1 つ以上選択します。このオプションは、レプリカとオペレーティング システム ディスクで別々のデータストアを選択する場合に表示されます。</p> <p>[ファームを追加] ウィザードの [レプリカ ディスクのデータストアを選択します] 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、インスタントクローンを格納するための十分な大きさがあるレプリカ ディスク データストアを特定するのに役立ちます。</p>	
ネットワーク	<p>インスタント クローン デスクトップ プールに使用するネットワークを選択します。複数の vLAN ネットワークを選択して、大規模な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。デフォルト設定では、現在のマスター イメージのネットワークが使用されます。</p> <p>[ネットワークの選択] ウィザードの表には、使用可能なネットワーク、ポート、およびポート バインドが表示されます。複数のネットワークを使用するには、[現在の親仮想マシン イメージのネットワークを使用します] の選択を解除し、インスタントクローン ファームで使用するネットワークを選択する必要があります。</p>	
vGPU プロファイル	<p>プールの vGPU プロファイルは、選択したスナップショットの vGPU プロファイルになります。プールは、このプロファイルを継承します。プールの作成中に、このプロファイルを編集することはできません。</p> <p>プールがプロビジョニングされたら、イメージを公開して vGPU プロファイルを変更できます。</p> <p>任意の数の ESXi ホストを含む 1 つの vSphere クラスタの場合、vGPU プロファイルの混在がサポートされています。</p> <p>vCenter Server バージョン 6.0 の場合、サポートされるパフォーマンス モードの vGPU プロファイルは 1 つだけです。</p> <p>vCenter Server バージョン 6.5 以降では、複数の vGPU プロファイルを使用できます。次のガイドラインに従ってください。</p> <ul style="list-style-type: none"> <li>■ クラスタ内のすべての GPU ホストに [GPU 統合] 割り当てポリシーを使用して、複数の vGPU プロファイルを使用できます。</li> <li>■ GPU 対応ホストと非対応ホストのクラスタを混在できます。</li> <li>■ [GPU 統合] 割り当てポリシーが設定されたホストのクラスタと [GPU パフォーマンス] 割り当てポリシーが設定されたホストの混在は推奨されません。</li> </ul> <p>すべての vGPU デスクトップのパフォーマンスを 1 つのプロファイルで向上させるには、クラスタ内のすべての GPU ホストの GPU 割り当てポリシーを [最適なパフォーマンス] に設定する必要があります。</p>	
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。	
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 : <b>CN=Computers</b></p> <p>[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。コンテナで Active Directory ツリー パスのコピー、貼り付けまたは入力を行うことができます。</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>このオプションは、新しいインスタント クローンの仮想マシン名が既存のコンピュータ アカウント名に一致するときに、Active Directory にある既存のコンピュータ アカウントを使用する場合に選択します。</p> <p>インスタント クローンの作成時に、既存の Active Directory コンピュータ アカウント名がインスタント クローン仮想マシン名に一致すると、Horizon 7 はパスワードをリセットしてから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。インスタント クローンを削除しても、Horizon 7 は対応するコンピュータ アカウントを削除しません。</p> <p>既存のコンピュータ アカウントが、Active Directory コンテナの設定で指定する Active Directory コンテナに配置されている必要があります。</p> <p>このオプションを無効にした場合、Horizon 7 がインスタント クローンを作成するときに、新しい Active Directory コンピュータ アカウントが作成されます。既存のコンピュータ アカウントが見つかった場合、Horizon 7 はパスワードをリセットしてから既存のコンピュータ アカウントを使用します。インスタント クローンを削除すると、Horizon 7 は対応するコンピュータ アカウントも削除します。このオプションは、デフォルトで無効になっています。</p>	
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

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。

### 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。
- マスター イメージが準備完了であることを確認します。詳細については、『Horizon 7 での仮想デスクトップのセットアップ』ドキュメントの「仮想マシンの作成および準備」を参照してください。
- プールの構成情報を収集します。[Horizon Console でインスタント クローン デスクトップ プールを作成するためのワークシート](#)を参照してください。
- Horizon 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。『Horizon 7 での仮想デスクトップのセットアップ』ドキュメントの「インスタント クローンのドメイン管理者の追加」を参照してください。

### 手順

- 1 Horizon Console で、[インベントリ] - [デスクトップ] の順に選択します。
- 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] を選択して、[次へ] をクリックします。
- 4 [インスタント クローン] を選択して、vCenter Server インスタンスを選択し、[次へ] をクリックします。



## 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。

### 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。 [Horizon Console での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。

## Horizon Console でのインスタント クローン デスクトップ プールのイメージの変更

インスタントクローン デスクトップ プールのイメージを変更して、変更を適用したり、以前のイメージに戻したりできます。新しいイメージには任意の仮想マシンから任意のスナップショットを選択できます。

プールがプロビジョニングされた後は vGPU プロファイルを編集できません。つまり、プールを編集したり、プールのイメージを変更することはできません。インスタント クローン プールに新しいイメージをプッシュする場合には、新しいイメージの vGPU プロファイルが前のイメージと一致していることを確認する必要があります。一致していないと、イメージのプッシュ操作が失敗する可能性があります。インスタント クローン プールの vGPU プロファイルを変更するには、プールを削除して、必要な vGPU プロファイルを使用して新しいプールを作成してください。

### 手順

- 1 Horizon Console で、[インベントリ] - [デスクトップ] の順に選択します。
- 2 プール ID をクリックします。
- 3 [サマリ] タブで、[メンテナンス] - [スケジュール] の順にクリックします。

[[イメージ プッシュをスケジュール]] ウィンドウが開きます。

- 4 プロンプトに従ってください。

タスクを今すぐ開始するようにスケジュールすることも、後で開始するようにスケジュールすることもできます。ユーザー セッションのあるクローンの場合、ユーザーを強制的にログアウトするか、待機するかを指定できます。ユーザーがログアウトすると、Horizon 7 はクローンを再作成します。

- 5 [終了] をクリックします。

この操作を開始すると、新しいイメージがすぐに公開されます。クローンの再作成は、[[イメージ プッシュをスケジュール]] ウィザードで指定した時から開始されます。

## Horizon Console でのプッシュイメージ操作のモニタリング

インスタント クローン デスクトップ プールでプッシュ イメージ操作の進行をモニタリングできます。

### 手順

- 1 Horizon Console で、[インベントリ] - [デスクトップ] の順に選択します。
- 2 プール ID をクリックします。

[サマリ] タブには、現在のイメージおよび保留中イメージの情報が表示されます。

### 3 [タスク] タブをクリックします。

プッシュイメージ操作に関連するタスクのリストが表示されます。

## Horizon Console でのプッシュイメージ操作の再スケジュールまたはキャンセル

インスタント クローン デスクトップ プールでプッシュイメージ操作の再スケジュールまたはキャンセルができます。

### 手順

1 Horizon Console で、[インベントリ] - [デスクトップ] の順に選択します。

2 プール ID をクリックします。

[サマリ] タブには、現在のイメージおよび保留中イメージの情報が表示されます。

3 [メンテナンス] - [再スケジュール] の順に選択するか、[メンテナンス] - [キャンセル] の順に選択します。

4 プロンプトに従ってください。

クローンの作成の進行中にプッシュイメージ操作をキャンセルした場合、新しいイメージのあるクローンがプールに残ります。新しいイメージのあるクローンと古いイメージのあるクローンがプールに混在することになります。すべてのクローンが同じイメージを持っていることを確認するために、クローンをすべて削除できます。Horizon 7 は、同じイメージのクローンを再作成します。

## 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、Horizon 7 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。

自動デスクトップ プールを作成するために、Horizon 7 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。Horizon 7 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、Horizon 7 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デスクトップ プールの作成とメンテナンスに必要な構成情報については、『Horizon 7 での仮想デスクトップのセットアップ』ドキュメントを参照してください。

## Horizon Console でフル仮想マシンを含む自動プールを作成するためのワークシート

自動デスクトップ プールを作成するときに、特定のオプションを設定できます。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。

表 10-2. 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"> <li>■ 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。</li> <li>■ フローティング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。</li> </ul>	
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する必要があります。</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>Horizon 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>Connection Server 構成は、スタンドアロンの Connection Server 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。</p> <p><b>注：</b> 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>フローティング 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><b>注：</b> 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>	
デスクトップ プールの設定	デスクトップの状態や、仮想マシンが使用中でないときの電源ステータス（表示プロトコルなど）を決定する設定。	

オプション	説明	値をここに記入
エラーによりプロビジョニングを停止	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 Horizon 7 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。	
仮想マシンの名前付け	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。	
名前を手動で指定	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。	
名前付けパターン	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。	
マシンの最大数	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。  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。	
スベアの（パワーオン状態の）マシンの数	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。  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。	
マシンの最小数	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。  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。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。	
VMware vSAN の使用	使用可能な場合は、VMware vSAN を使用するかどうかを指定します。vSAN は Software-Defined Storage 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。	
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。	
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。	
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>データストアの種類を選択します。</p> <ul style="list-style-type: none"> <li>■ [個々のデータストア]。デスクトップ プールを格納する個々のデータストアを選択します。</li> <li>■ [Storage DRS]。共有またはローカル データストアを含む Storage Distributed Resource Scheduler (DRS) クラスタを選択します。Storage DRS は、使用可能なデータストアにストレージ ワークロードを割り当て、移動するロード バランシング ユーティリティです。</li> </ul> <p>デスクトップ プールを Horizon 7 バージョン 7.1 から Horizon 7 バージョン 7.2 にアップデートした後で、Storage DRS クラスタを使用するようにプールを変更する場合には、既存のデータストアの選択を解除してから Storage DRS を選択する必要があります。</p> <p><b>注:</b> vSAN を使用する場合、データストアを 1 つのみ選択します。</p>	
View Storage Accelerator を使用	<p>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 バンド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><b>注:</b> 停電期間を追加または削除して View Storage Accelerator を無効にすると、Horizon Console は停電期間を保存しません。</p>	

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 Horizon 7 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><b>注:</b> 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。選択できるのは、テンプレートのゲスト OS に一致するカスタマイズ仕様だけです。</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。Horizon 7 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

- Horizon 7 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 7 はテンプレートにインストールされる必要があります。Horizon 7 での仮想デスクトップのセットアップ ドキュメントの「仮想マシンの作成および準備」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。 [Horizon Console でフル仮想マシンを含む自動プールを作成するためのワークシート](#)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。『Horizon 7 での仮想デスクトップのセットアップ』ドキュメントで「すべてデスクトップ プール タイプのデスクトップとプールの設定」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、Horizon 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、Horizon 7 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 Horizon Console で、[インベントリ] - [デスクトップ] の順に選択します。
- 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] を選択して、[次へ] をクリックします。
- 4 [フル仮想マシン] を選択して、vCenter Server インスタンスを選択し、[次へ] をクリックします。
- 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。

#### 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。

## Horizon Console での完全クローン デスクトップ プールの仮想マシンの再構築

仮想マシンを新しい仮想マシンで置き換え、マシン名を再利用する場合、完全クローン デスクトップ プールで仮想マシンを再構築します。エラー状態の仮想マシンを再構築し、エラーのない仮想マシンと同じ名前でも置き換えることができます。仮想マシンを再構築すると、仮想マシンが削除され、同じ仮想マシン名のクローンが作成されて、Active Directory コンピュータ アカウントが再利用されます。前の仮想マシンのユーザー データと設定はすべて失われ、デスクトップ プールのテンプレートを使用して新しい仮想マシンが作成されます。

#### 前提条件

- 完全クローンの自動デスクトップ プールを作成します。[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。

#### 手順

- 1 Horizon Console で、[インベントリ] - [デスクトップ] の順に選択します。
- 2 再構築する仮想マシンを含むデスクトップ プールを選択して、[インベントリ] タブをクリックします。
- 3 再構築する仮想マシンを選択して、[再構築] を選択します。

vCenter Server で、仮想マシンが削除され、同じ名前のクローンが作成されたことを確認できます。Horizon Console で再構築された仮想マシンのステータスを確認するには、[削除中] - [プロビジョニング] - [カスタマイズ] - [使用可能] の順に移動します。

## Horizon Console でのリンク 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、Horizon 7 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。Horizon Composer サービスは、vCenter Server に各デスクトップ用のリンク クローン仮想マシンを動的に作成します。

Horizon 7 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。

## Horizon Console でのリンク 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、特定のオプションを設定できます。このワークシートを使用して、リンク クローン デスクトップ プールを作成する前に設定オプションを準備します。

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。Horizon 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 10-3. 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
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。	
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"> <li>■ 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。</li> <li>■ フローティング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。</li> </ul>	
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>	



オプション	説明	値をここに記入
通常ディスク	<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 Horizon Composer パーシステント 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> <ul style="list-style-type: none"> <li>■ [Windows プロファイルをパーシステント ディスクにリダイレクト]。このオプションは、別個の Horizon Composer パーシステント ディスクにデータを格納する場合に選択します。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。Horizon Composer の更新、再構成、再調整操作は、パーシステント 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。</li> <li>■ [ディスク サイズ]。別個の Horizon Composer パーシステント 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 サイズを MB 単位で指定します。</li> <li>■ [ドライブ文字]。別個の Horizon Composer パーシステント 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、ドライブ文字を指定します。</li> </ul> <hr/> <p><b>注:</b> 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> <hr/> <ul style="list-style-type: none"> <li>■ [Windows プロファイルをリダイレクトしない]。このオプションは、OS ディスクに Windows プロファイルを格納する場合に選択します。ユーザー データと設定は、更新、再構成、再調整操作時に削除されます。</li> </ul>	

オプション	説明	値をここに記入
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パーシステント ディスク以外の別のディスクにリダイレクトするかどうかを選択します。</p> <ul style="list-style-type: none"> <li>■ [ディスポーザブル ファイルをパーシステント ディスク以外にリダイレクト]。このオプションは、ゲスト OS のページング ファイルと一時ファイルをパーシステント ディスク以外の別のディスクにリダイレクトする場合に選択します。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。</li> <li>■ [ディスク サイズ]。パーシステント ディスク以外のディスクにディスポーザブル ファイルをリダイレクトする場合は、ディスク サイズを MB 単位で指定します。</li> </ul> <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。ページング ファイルのサイズを確認する方法については、『Horizon 7 での仮想デスクトップのセットアップ』の「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。ディスポーザブル ファイル ディスクのサイズを設定する場合は、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、Horizon Console で指定した値よりわずかに小さいことに注意してください。</p> <ul style="list-style-type: none"> <li>■ [ドライブ文字]。パーシステント ディスク以外のディスクにディスポーザブル ファイルをリダイレクトする場合は、ドライブ文字を指定します。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、Horizon 7 でドライブ文字を割り当てます。</li> <li>■ [ディスポーザブル ファイルをリダイレクトしない]。このオプションは、ゲスト OS のページング ファイルや一時ファイルをリダイレクトしない場合に選択します。</li> </ul> <p><b>注:</b> 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>	
VMware vSAN の使用	<p>使用可能な場合は、VMware vSAN を使用するかどうかを指定します。vSAN は Software-Defined Storage 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、『Horizon 7 での仮想デスクトップのセットアップ』の「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 vSAN 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>(vSAN 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>(vSAN または Virtual Volumes を使用しない場合にのみ使用可能)</p> <p>レプリカ (マスター) 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、『Horizon 7 での仮想デスクトップのセットアップ』を参照してください。</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>	
デスクトップ プール ID	<p>プールを識別する一意の名前。</p> <p>環境内で複数の Connection Server 構成を実行している場合は、別の Connection Server 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>Connection Server 構成は、スタンドアロンの Connection Server 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	<p>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。</p>	
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、『Horizon 7 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><b>注:</b> 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>	
プロビジョニングを有効にする	<p>このオプションは、デスクトップ プールに仮想マシンをプロビジョニングする場合に選択します。</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 Horizon 7 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、<a href="#">Horizon Console での手動によるマシンの名前付けまたは名前付けパターンの指定</a>を参照してください。</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>	

オプション	説明	値をここに記入
名前付けパターン	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、その後各マシンを識別するための一意の番号を付けます。 詳細については、 <a href="#">自動デスクトップ プールでの名前付けパターンの使用</a> を参照してください。	
マシンの最大数	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。 プールの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。	
スベアの（パワーオン状態の）マシンの数	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、 <a href="#">Horizon Console での手動によるマシンの名前付けまたは名前付けパターンの指定</a> を参照してください。 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。	
Horizon 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	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、Horizon 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。 この設定を使用すると、Horizon 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。 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] より小さくしなければなりません。 詳細については、『Horizon 7 での仮想デスクトップのセットアップ』を参照してください。	
オンデマンドでマシンをプロビジョニング または 全マシンを事前にプロビジョニング	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。 ■ [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	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。 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。	
親仮想マシン	プールの親仮想マシンを選択します。	

オプション	説明	値をここに記入
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、Horizon Composer のメンテナンス操作も必要です。</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。	
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>vSAN データストア（vSphere 5.5 Update 1 の機能）では、最大 20 台までの 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 台までの 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 パ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。『Horizon 7 での仮想デスクトップのセットアップ』の「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>	
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
リンク クローン 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>[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、『Horizon 7 での仮想デスクトップのセットアップ』の「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」を参照してください。</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。詳細については、『Horizon 7 での仮想デスクトップのセットアップ』の「ローカル データストアへのリンク クローンの保存」を参照してください。</p> <p>vSAN データストア (vSphere 5.5 Update 1 の機能) では、最大 20 台までの 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 台までの ESXi ホストを持つクラスタを選択できます。</p> <p>リンク クローンに作成されたディスクの詳細については、『Horizon 7 での仮想デスクトップのセットアップ』の「リンク クローンのデータ ディスク」を参照してください。</p> <p><b>注:</b> vSAN を使用する場合、データストアを 1 つのみ選択します。</p>	
レプリカ ディスク データストア	<p>レプリカを格納するレプリカ ディスク データストアを選択します。</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。『Horizon 7 での仮想デスクトップのセットアップ』の「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>	
ログオフ時にマシンを削除または更新	<p>フローティング 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><b>注:</b> 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>	
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、『Horizon 7 での仮想デスクトップのセットアップ』の「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、<a href="#">Horizon Console でのリンク 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</a>を参照してください。</p> <p>電源ポリシーと自動プールの詳細については、『Horizon 7 での仮想デスクトップのセットアップ』の「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>	

オプション	説明	値をここに記入
Horizon 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 Horizon Storage Accelerator を使用するかどうかを指定します。Horizon Storage Accelerator を使用することで、多数の起動とアンチウイルス 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、『Horizon 7 での仮想デスクトップのセットアップ』を参照してください。</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、『Horizon 7 での仮想デスクトップのセットアップ』の「リンク クローン仮想マシンのストレージのオーバー コミットメント レベルの設定」を参照してください。</p> <p><b>注:</b> vSAN を使用する場合、この設定は効果がありません。</p>	
ネイティブ NFS スナップショット (VAAI) を使用	<p>(vSAN 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、『Horizon 7 での仮想デスクトップのセットアップ』を参照してください。</p>	
仮想マシン ディスク容量を再利用	<p>(vSAN または Virtual Volumes を使用しない場合にのみ使用可能) 容量効率の高いディスク フォーマットで作成されたリンク クローンの未使用ディスク容量を ESXi ホストが再利用できるかどうかを指定します。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、『Horizon 7 での仮想デスクトップのセットアップ』の「リンク クローン仮想マシンのディスク領域を再利用する」を参照してください。</p>	

オプション	説明	値をここに記入
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>(vSAN または Virtual Volumes を使用しない場合にのみ使用可能)</p> <p>容量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容量の最小量 (GB) を入力します。</p> <p>未使用ディスク容量がこのしきい値を超過すると、Horizon 7 は ESXi ホストに OS ディスク上の容量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、Horizon 7 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: <b>2 GB</b>。</p> <p>デフォルト値は 1 GB です。</p>	
停電期間	<p>Horizon 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、『Horizon 7 での仮想デスクトップのセットアップ』の「仮想マシンにおける ESXi 操作の停電期間の設定」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 Horizon 7 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><b>注:</b> 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>Horizon 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 Horizon Composer 設定を構成するときに指定します。Horizon 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>	



オプション	説明	値をここに記入
AD コンテナ	Active Directory コンテナの相対識別名を指定します。 例: <b>CN=Computers</b> [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。	
既存のコンピュータ アカウントの再利用を許可	Horizon 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。 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 Active Directory 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、Horizon 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。 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。 このオプションが無効になっていると、Horizon 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 Active Directory 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。 詳細については、『Horizon 7 での仮想デスクトップのセットアップ』の「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」を参照してください。	
Use QuickPrep or a customization specification (Sysprep) (QuickPrep またはカスタマイズ仕様 (Sysprep) を使用)	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。 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。 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。 詳細については、『Horizon 7 での仮想デスクトップのセットアップ』の「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。	
Power-off script (パワーオフ スクリプト)	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。 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。	
同期後スクリプト	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。 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。	

## Horizon Console でのリンク 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

Horizon 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フローティング 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。

次の表に、専用ユーザー割り当てを使用するリンク クローン プールおよびフローティング 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、『Horizon 7 での仮想デスクトップのセットアップ』の「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 10-4. 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、フローティング割り当て
状態	はい	はい
Connection Server の制限	はい	はい
カテゴリ フォルダ (* Horizon Administrator でサポート)	はい	はい
リモート マシンの電源ポリシー	はい	はい
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/再起動を許可	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 (モニターの最大数)	はい	はい
Max resolution of any one monitor (特定のモニターの最大解像度)	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

## Horizon Console でのリンク 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。Horizon 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。

### 前提条件

- Horizon 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、Horizon Composer データベースが構成されていることを確認します。『Horizon 7 のインストール』ドキュメントを参照してください。
- vCenter Server の Horizon Composer 設定が Horizon Administrator で構成されていることを確認します。『Horizon 7 の管理』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。『Horizon 7 での仮想デスクトップのセットアップ』の「クローン作成のための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。Horizon 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。 [Horizon Console でのリンク 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。『Horizon 7 での仮想デスクトップのセットアップ』の「すべてデスクトップ プール タイプのデスクトップとプールの設定」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、Horizon Console 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、Horizon 7 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。Horizon 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 Horizon Console で、[インベントリ] - [デスクトップ] の順に選択します。
- 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] を選択して、[次へ] をクリックします。
- 4 [View Composer のリンク クローン] を選択して、vCenter Server インスタンスを選択し、[次へ] をクリックします。
- 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。

Horizon Console で、[インベントリ] - [デスクトップ] の順に選択すると、プールに追加されているマシンを確認できます。

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、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。

Horizon Composer は、リンク クローンのプロビジョニング用のマスター 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、Horizon 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。 [Horizon Console での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。

## Horizon Console での手動デスクトップ 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。

Horizon 7 の手動プールでは、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。

## Horizon Console での手動デスクトップ 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、特定のオプションを設定できます。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。

**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 10-5. 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"> <li>■ 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。</li> <li>■ フローティング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。</li> </ul> <p>詳細については、<a href="#">Horizon Console でのデスクトップ プールでのユーザー割り当て</a>を参照してください。</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"> <li>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管理対象外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。</li> <li>2 デスクトップ プールに含める、vCenter Server 仮想マシンまたは管理対象外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。</li> <li>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。</li> </ol> <p>管理対象外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><b>注:</b> Horizon Console で Windows Server デスクトップを有効にすると、Horizon Console は使用可能なすべての Windows Server マシン（接続サーバなどの Horizon 7 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 Horizon 7 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、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 Horizon 7 ソフトウェア コンポーネントと同じ仮想マシンまたは物理マシンにインストールすることはできません。</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、Horizon Console 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、<a href="#">Horizon Console でのすべてのデスクトップ プール タイプのデスクトップ プールの設定</a>を参照してください。</p> <p>手動プールに適用される設定のリストについては、<a href="#">Horizon Console での手動プールのデスクトップ プール設定</a>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 Horizon 7 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><b>注:</b> 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>	

## Horizon Console での手動デスクトップ 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、ユーザーがスベア マシンに接続できるように、Horizon 7 は必ず 1 台のスベア 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 によって管理される仮想マシンを準備する方法については、『Horizon 7 での仮想デスクトップのセットアップ』の「仮想マシンの作成および準備」を参照してください。

管理対象外の仮想マシンと物理コンピュータを準備する方法については、『Horizon 7 での仮想デスクトップのセットアップ』の「管理対象外のマシンの準備」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。 [Horizon Console での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。 [Horizon Console での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の設定](#)を参照してください。

#### 手順

- 1 Horizon Console で、[インベントリ] - [デスクトップ] の順に選択します。
- 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 vCenter Server によって管理される仮想マシンを選択するか、vCenter Server によって管理されていない管理対象外の仮想マシンを選択して、[次へ] をクリックします。

オプション	説明
vCenter Server 仮想マシン	vCenter Server で管理される仮想マシン仮想マシンが配置されている vCenter Server を選択します。
その他のソース	物理コンピュータまたは vCenter Server によって管理されていない仮想マシン

- 5 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。
フローティング	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。

- 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。

Horizon Console で、[インベントリ] - [デスクトップ] の順に選択すると、プールに追加されているマシンを確認できます。

#### 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。 [Horizon Console での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。

## Horizon Console での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。

手動デスクトップ プールの設定には、次のプロパティが設定されている手動デスクトップ プールに適用される設定が表示されます。

- 専用ユーザー割り当て
- フローティング ユーザー 割り当て
- 管理対象マシン (vCenter Serve 仮想マシン)
- 管理対象外のマシン

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、[Horizon Console でのすべてのデスクトップ プール タイプのデスクトップ プールの設定](#)を参照してください。

表 10-6. 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、フローティング割り当て	手動の管理対象外のプール、専用割り当て	手動の管理対象外のプール、フローティング割り当て
状態	はい	はい	はい	はい
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		
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/再起動を許可	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 による管理対象外のマシンで 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 による管理対象外のマシンで 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		



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、フローティング割り当て	手動の管理対象外のプール、専用割り当て	手動の管理対象外のプール、フローティング割り当て
Max number of monitors (モニターの最大数)	はい	はい		
Max resolution of any one monitor (特定のモニターの最大解像度)	はい	はい		
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

## デスクトップ プールの構成

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。

## Horizon Console でのデスクトップ プールでのユーザー割り当て

デスクトップ プールのデスクトップに、フローティングまたは専用ユーザー割り当てを選択できます。

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。ログインからログアウトまでの間、同じデスクトップでコンピュータ名と MAC アドレスが保持されます。ユーザーがデスクトップに行った他の変更は保持されません。

フローティング割り当ての場合、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。

フローティング 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。

フローティング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。

## Horizon Console での手動によるマシン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、Horizon 7 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。

次の表では、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 10-7. 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、 <a href="#">自動デスクトップ プールでの名前付けパターンの使用</a> 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、 <a href="#">Horizon Console でのマシン名のリストの指定</a> 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、 <a href="#">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</a> 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。 Horizon 7 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。 Horizon 7 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。 Horizon 7 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、Horizon 7 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、Horizon 7 は選択されたカスタマイズ仕様を実行できます。
専用マシンの手動カスタマイズ	インスタント クローンでは利用不可。 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。	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。 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、 <a href="#">マシンの手動でのカスタマイズ</a> を参照してください。

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
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>フローティング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><b>注:</b> インスタントクローン プールは、フローティング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>Horizon 7 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>Horizon 7 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、Horizon 7 はスベア マシンの作成を停止します。</p> <p>Horizon 7 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><b>注:</b> 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>Horizon 7 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>Horizon 7 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>Horizon 7 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フローティング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>専用割り当ておよびフローティング割り当てプールに対してマシン名を指定できます。</p> <p><b>注:</b> フローティング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。フローティング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>

## Horizon Console での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:** フローティング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。フローティング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 [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 Horizon Console では、[プールを追加] ウィザードを起動して、フル仮想マシンを含む自動デスクトップ 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、[名前の入力] 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。
- 5 [送信] をクリックします。
- 6 (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。

- 7 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。

Horizon 7 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、Horizon 7 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。[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。

#### 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、Horizon 7 は、パターンをすべてのマシン名のプリ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 10-8. 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、Horizon 7 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。

Horizon 7 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、Horizon 7 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 10-9. 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 Horizon Console 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、[Horizon Console での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 Horizon Console 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。

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:** フローティング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。フローティング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、フル仮想マシンの自動デスクトップ プールを作成していることを確認します。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、[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 Horizon Console で、[インベントリ] - [デスクトップ] の順に選択します。
- 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。
- 8 [送信] をクリックします。
- 9 [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。

Horizon Console で、[インベントリ] - [デスクトップ] の順に選択すると、デスクトップ プールに追加されているマシンを確認できます。

## Horizon Console で名前付けパターンに従ってプロビジョニングされる自動プールのサイズを変更する

名前付けパターンを使用して自動デスクトップ プールをプロビジョニングする場合は、マシンの最大数を変更してプールのサイズを増やしたり減らしたりすることができます。

### 前提条件

- 名前付けパターンを使用してデスクトップ プールをプロビジョニングしたことを確認します。
- デスクトップ プールが自動であることを確認します。

### 手順

- 1 Horizon Console で、[インベントリ] - [デスクトップ] の順に選択します。
- 2 デスクトップ プール ID をクリックして、[編集] をクリックします。
- 3 [プロビジョニングの設定] タブで、[マシンの最大数] テキスト ボックスにデスクトップ プール内の新しいマシン数を入力します。

デスクトップ プール サイズを増やした場合は、新しいマシンを最大数までプールに追加できます。

フローティング割り当てプールのサイズを減らした場合は、未使用のマシンが削除されます。新しい最大数よりも多くのユーザーがプールにログインしている場合は、ユーザーがログオフした後にプール サイズが減少します。

専用割り当てプールのサイズを減らした場合は、未割り当てのマシンが削除されます。新しい最大数よりも多くのユーザーがマシンに割り当てられている場合は、ユーザーの割り当てを解除した後にプール サイズが減少します。

---

**注:** デスクトップ プールのサイズを減らした場合、[マシンの最大数] で指定した値よりも多くのユーザーがマシンにログインしているか、またはマシンに割り当てられている場合は、マシンの実際の数が [マシンの最大数] より多くなることがあります。

---

## 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、Horizon 7 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。フル仮想マシンの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。

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。Horizon 7 は、すべてのマシンにカスタマイズを展開します。

---

**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。

---



## Horizon Console のメンテナンス モードでの既存マシンのカスタマイズ

デスクトップ プールの作成後、個々のマシンをメンテナンス モードにしてカスタマイズ、変更、またはテストすることができます。マシンがメンテナンス モードの場合、ユーザーは仮想マシン デスクトップにアクセスできません。

既存のマシンを 1 度に 1 つずつメンテナンス モードにします。1 回の操作で、複数のマシンのメンテナンス モードを終了できます。

デスクトップ プールの作成時に、マシン名を手動で指定すると、プール内のすべてのマシンをメンテナンス モードで起動できます。

### 手順

- 1 Horizon Console で、[インベントリ] - [デスクトップ] の順に選択し、プール ID をダブルクリックして、[インベントリ] タブを選択します。
- 2 マシンを選択します。
- 3 [その他のコマンド] ドロップダウン メニューから [メンテナンス モードを開始] を選択します。
- 4 仮想マシン デスクトップをカスタマイズ、変更、またはテストします。
- 5 [手順 2](#) から [手順 4](#) を繰り返します。
- 6 カスタマイズされたマシンを選択し、[その他のコマンド] ドロップダウン メニューから [メンテナンス モードを終了] を選択します。

変更した仮想マシン デスクトップをユーザーが使用できるようになります。

## Horizon Console での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 Horizon Console で、[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 [プールを追加] ウィザードを完了して、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 Horizon Console で、[インベントリ] - [マシン] の順に選択します。
- 7 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] の順にクリックします。

### 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。

## Horizon Console でのすべてのデスクトップ プール タイプのデスクトップ プールの設定

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、およびインスタント クローン 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 10-10. 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"> <li>■ [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。</li> <li>■ [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。</li> </ul> <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>
Connection Server の制限	<ul style="list-style-type: none"> <li>■ [なし]。デスクトップ プールには、すべての Connection Server インスタンスがアクセスできます。</li> <li>■ [タグ付き]: 1 つ以上の Connection Server タグを選択して、これらのタグを持つ Connection Server 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。</li> </ul> <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 Connection Server 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>
カテゴリ フォルダ	Windows クライアント デバイスのデスクトップ プール資格に、スタート メニューのショートカットを含むカテゴリ フォルダの名前を指定します。詳細については、『Horizon 7 での公開されたデスクトップとアプリケーションのセットアップ』の「デスクトップ プールとアプリケーション プールのスタート メニュー ショートカットの設定」を参照してください。この機能は、Horizon Administrator で利用できます。
セッション タイプ	<p>デスクトップ プールでサポートされているセッション タイプを選択することにより、デスクトップ プールに基づいてアプリケーション プールを作成できます。</p> <ul style="list-style-type: none"> <li>■ [デスクトップ]。デスクトップのみがサポートされます。</li> <li>■ [アプリケーション]。アプリケーションのみがサポートされます。</li> <li>■ [デスクトップとアプリケーション]。デスクトップとアプリケーションの両方がサポートされます。</li> </ul>
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 オプションの説明については、『Horizon 7 での仮想デスクトップのセットアップ』の「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>自動プールに対する電源ポリシーの影響については、『Horizon 7 での仮想デスクトップのセットアップ』の「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>
切断後に自動的にログオフ	<ul style="list-style-type: none"> <li>■ [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。</li> <li>■ [なし]: ユーザーはログオフされません。</li> <li>■ [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。</li> </ul> <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>

設定	オプション
ユーザーによるマシンのリセット/再起動を許可	<p>ユーザーによるデスクトップのリセットまたは再起動を許可します。</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	<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> <p><b>注:</b> 複数セッションは、デスクトップ プールで実行されているアプリケーションでサポートされません。この設定は、デスクトップ プールから作成されたアプリケーションに適用されません。</p>
ログオフ後にマシンを削除	<p>フローティング割り当て、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"> <li>■ [[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。</li> <li>■ [[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。</li> </ul> <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>フローティング割り当てのリンク 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"> <li>■ [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。</li> <li>■ [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。</li> <li>■ [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。</li> </ul> <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>
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"> <li>■ [なし]: OS ディスクは更新されません。</li> <li>■ [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。</li> <li>■ [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。</li> </ul> <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 <b>3</b> 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"> <li>■ [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。</li> </ul> <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>

設定	オプション
デフォルト表示プロトコル	<p>Connection Server 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> <p><b>VMware Blast</b> 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。</p> <p><b>PCoIP</b> 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。</p> <p><b>Microsoft RDP</b> 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。</p>
ユーザーがプロトコルを選択できるようにする	<p>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。</p>
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、『Horizon 7 での仮想デスクトップのセットアップ』の「デスクトップ用の 3D レンダリングの設定」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る VRAM の量を構成できます。モニターの最大数は 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ー数を構成する必要があります。モニターの解像度に応じて、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 つのモニターを選択できます。</p> <p><b>注:</b> 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> <p>インスタント クローン デスクトップ プールの場合、3D レンダラー オプションで使用できるのは NVIDIA GRID vGPU だけです。</p>

設定	オプション
Max number of monitors (モニターの最大数)	<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 [モニターの最大数] を選択できます。</p> <p>最大で 4 つのモニターを選択できます。</p> <p>[3D レンダラー] 設定が選択されていない場合、[モニターの最大数] 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。モニター数を増やすと、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 台のモニターが 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 台のモニターが 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 台のモニターが 3840x2160 の解像度でサポートされます。モニター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ーの数を少なくします。</p> <p><b>注:</b> 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>
Max resolution of any one monitor (特定のモニターの最大解像度)	<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、[各モニターの最大解像度] を指定する必要があります。</p> <p>デフォルトでは、[各モニターの最大解像度] 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、[特定のモニターの最大解像度] 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 台のモニターが 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 台のモニターが 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 台のモニターが 3840x2160 の解像度でサポートされます。モニター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ーの数を少なくします。</p> <p><b>注:</b> 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>
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、<a href="https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html">https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html</a> 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、『Horizon 7 の管理 管理ガイド』の説明に従って Connection Server 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、Connection Server で使用するために構成する必要があります。</p>
セッション共同作業を許可	<p>プールのユーザーに、リモート デスクトップ セッションへの他のユーザーの招待を許可するには、[有効] を選択します。セッション オーナーとセッション共同作業者は、VMware Blast 表示プロトコルを使用する必要があります。</p>

# Horizon Console でのデスクトップ プールと仮想デスクトップの管理

Horizon Console では、デスクトップ プール、仮想マシンベースのデスクトップ、物理マシンベースのデスクトップ、デスクトップ セッションを管理できます。

## デスクトップ プールの管理

デスクトップ プールに対する管理タスク（プールのプロパティの編集やプールの有効化、無効化、削除など）を実行できます。

### デスクトップ プールの編集

既存のデスクトップ プールを編集して、スเปア マシン数、データストア、カスタマイズ仕様などの設定を構成できます。

#### 前提条件

デスクトップ プールの作成後に変更可能または変更不可能なデスクトップ プール設定について理解しておきます。『Horizon 7 での仮想デスクトップのセットアップ』ドキュメントで「既存のデスクトップ プールの設定の変更」と「既存のデスクトップ プールの固定設定」を参照してください。

#### 手順

- 1 Horizon Console で、[インベントリ] - [デスクトップ] の順に選択します。
- 2 デスクトップ プールを選択し、[編集] をクリックします。
- 3 [編集] ダイアログ ボックス内のタブをクリックし、デスクトップ プール オプションを再構成します。
- 4 [OK] をクリックします。

インスタントクローン デスクトップ プールのイメージを変更すると、画像の公開操作が即座に開始されます。Horizon Administrator では、デスクトップ プールのサマリ ページには保留イメージの状態が 公開 と表示されません。

インスタントクローン デスクトップ プールのクラスタを変更すると、新しいレプリカおよび親仮想マシンが新しいクラスタに作成されます。同じイメージを使用してイメージ プッシュを開始し、新しいクラスタに新しいクローンを作成できます。ただし、クローン作成プロセスで使用するテンプレート仮想マシンは古いクラスタに残ります。テンプレート仮想マシンがある ESXi ホストをメンテナンス モードにすることはできますが、テンプレート仮想マシンを移行することはできません。新しいイメージを使用してイメージ プッシュを開始すると、テンプレート仮想マシンを含むすべてのインフラストラクチャ仮想マシンを古いクラスタから完全に削除できます。

### デスクトップ プールの削除

デスクトップ プールを削除すると、ユーザーはプール内の新規リモート デスクトップを起動できなくなります。

デスクトップ プールのタイプに応じて、Horizon 7 で通常ディスク、vCenter Server フル仮想マシン、ユーザーのアクティブ セッションを処理するためのさまざまなオプションが用意されています。

デフォルトでは、デスクトップ マシンがプールに存在している場合でも、デスクトップ プールを削除できます。詳細については、『Horizon 7 での仮想デスクトップのセットアップ』ドキュメントの「デスクトップ プールの削除設定」を参照してください。この設定を構成している場合、プールを削除するには、デスクトップ プールに含まれるすべてのマシンを削除する必要があります。

インスタント クローンの自動デスクトップ プールを使用すると、Horizon 7 は常にディスクから仮想マシンを削除します。

**重要:** Horizon Console でデスクトップ プールを削除する前に vCenter Server の仮想マシンを削除しないでください。このアクションによって、Horizon 7 コンポーネントが不整合な状態になる可能性があります。

#### 手順

- 1 Horizon Console で、[インベントリ] - [デスクトップ] の順に選択します。
- 2 デスクトップ プールを選択し、[削除] をクリックします。
- 3 デスクトップ プールの削除方法を選択します。

プール	オプション
通常ディスクを含まないインスタント クローンの自動デスクトップ プール。	使用できるオプションはありません。Horizon 7 はディスクからすべての仮想マシンを削除します。リモート デスクトップへのユーザー セッションは終了します。
フル仮想マシンの自動デスクトップ プール。	vCenter Server の仮想マシンを維持するか削除するかを選択します。
RDS デスクトップ プール。 フル仮想マシンの自動デスクトップ プール。	リモート デスクトップに接続しているユーザーがいる場合は、ユーザーのセッションをアクティブなままにするか終了するかを選択します。接続サーバは、アクティブなセッションを追跡しません。

デスクトップ プールを削除すると、フル仮想マシンのコンピュータ アカウントは Active Directory に残ります。これらのアカウントを削除するには、Active Directory から手動で削除する必要があります。

インスタントクローン デスクトップ プールを削除する場合は、Horizon 7 が vCenter Server から内部仮想マシンを削除するのにしばらく時間がかかることがあります。内部仮想マシンがすべて削除されたことを確認するまでは、Horizon Console から vCenter Server を削除しないでください。

## デスクトップ プールの無効化または有効化

デスクトップ プールを無効にすると、プールがユーザーに表示されなくなり、プールのプロビジョニングが停止します。ユーザーはプールにアクセスできません。プールを無効にした後、再度有効にすることができます。

#### 前提条件

デスクトップ プールを無効にすると、デスクトップの使用を準備する間に、ユーザーがリモート デスクトップにアクセスできないようにすることができます。デスクトップ プールが必要でなくなった場合は、無効化機能を使用してアクティブな使用を取り消すことができます。Horizon 7 からデスクトップ プールの定義を削除する必要はありません。

#### 手順

- 1 Horizon Console で、[インベントリ] - [デスクトップ] の順に選択します。



- 2 デスクトップ プールを選択し、そのプールのステータスを変更します。

オプション	アクション
プールを無効にする	[ステータス] ドロップダウン メニューから [デスクトップ プールを無効にする] を選択します。
プールを有効にする	[ステータス] ドロップダウン メニューから [デスクトップ プールを有効にする] を選択します。

- 3 [OK] をクリックします。

## デスクトップ プールのプロビジョニングの無効化または有効化

自動デスクトップ プールのプロビジョニングを無効にすると、Horizon 7 がプールの新しい仮想マシンのプロビジョニングを停止します。プロビジョニングを無効にした後、再度有効にすることができます。

プールの構成を変更する前にプロビジョニングを無効にして、以前の構成で新しいマシンが作成されないことを確認します。さらにプロビジョニングを無効にして、プールの使用可能な領域が不足している状態のときに Horizon 7 が追加のストレージを使用しないようにすることもできます。

### 手順

- 1 Horizon Console で、[インベントリ] - [デスクトップ] の順に選択します。
- 2 デスクトップ プールを選択し、そのプールのステータスを変更します。

オプション	アクション
プロビジョニングを無効にする	[ステータス] ドロップダウン メニューから [プロビジョニングを無効にする] を選択します。
プロビジョニングを有効にする	[ステータス] ドロップダウン メニューから [プロビジョニングを有効にする] を選択します。

- 3 [OK] をクリックします。

## 仮想マシンベースのデスクトップの管理

仮想マシンベースのデスクトップは、vCenter Server 仮想マシンが含まれる自動または手動のデスクトップ プールのデスクトップです。

### Horizon Console でのユーザーへのマシンの割り当て

専用割り当てプールでは、リモート デスクトップをホストする仮想マシンの所有者になるユーザーを割り当てることができます。割り当てられたユーザーのみがそのリモート デスクトップにログインして接続できます。

Horizon Console は、次の状況でマシンをユーザーに割り当てます。

- デスクトップ プールの作成時に、[自動割り当てを許可] 設定を選択した場合

**注:** [自動割り当てを許可] 設定を選択した場合でも、手動でマシンをユーザーに割り当てることができます。

- 自動プールの作成時に [名前を手動で指定] 設定を選択して、ユーザー名とマシン名を指定した場合

専用割り当てプールのいずれかの設定を選択しなければ、ユーザーは仮想デスクトップにアクセスできません。手動でマシンを各ユーザーに割り当てする必要があります。



また、`vdmadmin` コマンドを使用してマシンをユーザーに割り当てることもできます。`vdmadmin` コマンドの詳細については、『Horizon 7 の管理』ガイドを参照してください。

#### 前提条件

- 仮想マシンが専用割り当てプールに属していることを確認します。Horizon Console で、デスクトップ プールの割り当てが [デスクトップ プール] ページの [ユーザーの割り当て] 列に表示されます。

#### 手順

- 1 Horizon Console で、[インベントリ] - [デスクトップ] の順に選択し、プール ID をダブルクリックして、[インベントリ] タブをクリックします。
- 2 マシンを選択します。
- 3 [その他のコマンド] ドロップダウン メニューから [ユーザーを割り当てる] を選択します。
- 4 ユーザーとグループのどちらを検索するかを選択して、[名前] または [説明] テキスト ボックスに検索文字列を入力します。
- 5 ユーザーまたはグループ名を選択し、[OK] をクリックします。

### Horizon Console での専用マシンからのユーザーの割り当て解除

専用割り当てプールでは、ユーザーへのマシン割り当てを削除できます。

また、`vdmadmin` コマンドを使用して、ユーザーへのマシン割り当てを削除することもできます。`vdmadmin` コマンドの詳細については、『Horizon 7 の管理』ガイドを参照してください。

#### 手順

- 1 Horizon Console で、[インベントリ] - [デスクトップ] の順に選択し、プール ID をダブルクリックして、[インベントリ] タブをクリックします。
- 2 マシンを選択します。
- 3 [その他のコマンド] ドロップダウン メニューから [ユーザーの割り当てを解除] を選択します。
- 4 [OK] をクリックします。

マシンを別のユーザーが使用できるようになり、別のユーザーに割り当てることができます。

### Horizon Console での仮想マシン デスクトップの削除

仮想マシン デスクトップを削除すると、ユーザーはそのデスクトップにアクセスできなくなります。

vCenter Server の仮想マシンを維持した場合、現在アクティブなセッションのユーザーは、フル仮想マシン デスクトップを使用し続けることができます。ユーザーのログオフ後、ユーザーは削除された仮想マシン デスクトップにアクセスできなくなります。

インスタント クローンを使用すると、vCenter Server は常にディスクから仮想マシンを削除します。

---

**注:** Horizon Console で仮想マシン デスクトップを削除する前に vCenter Server で仮想マシンを削除しないでください。このアクションによって、Horizon 7 コンポーネントが不整合な状態になる可能性があります。

---

## 手順

- 1 Horizon Console で、[インベントリ] - [マシン] の順に選択します。
- 2 [vCenter 仮想マシン] タブを選択します。
- 3 1 つ以上のマシンを選択し、[削除] をクリックします。
- 4 仮想マシン デスクトップの削除方法を選択します。

オプション	説明
フル仮想マシン デスクトップを含むプール	vCenter Server の仮想マシンを維持するか削除するかを選択します。 ディスクから仮想マシンを削除する場合、アクティブなセッションのユーザーはデスクトップから切断されます。 vCenter Server の仮想マシンを維持する場合は、アクティブなセッションのユーザーがデスクトップに接続し続けるか、切断されるかを選択します。
通常ディスクを含まないインスタント クローン プール	vCenter Server はインスタント クローン仮想マシンをディスクから削除します。現在アクティブなセッションのユーザーはリモート デスクトップから切断されます。

## Horizon Console での外部ファイルへの Horizon 7 情報のエクスポート

Horizon Console で、Horizon 7 表情報を外部ファイルにエクスポートできます。ユーザーとグループ、プール、マシン、View Composer 通常ディスク、ThinApp アプリケーション、イベント、および VDI セッションが表示された表をエクスポートできます。スプレッドシートや別のツールで情報を表示し、管理できます。

たとえば、複数の接続サーバ インスタンスまたは複製された接続サーバ インスタンスのグループによって管理されるマシンに関する情報を収集できます。各 Horizon Console インターフェイスからマシン表をエクスポートし、それをスプレッドシートで表示できます。

Horizon Console 表をエクスポートすると、Microsoft Excel Open XML Format Spreadsheet (XLSX) ファイルとして保存されます。この機能では、個々のページではなく表全体がエクスポートされます。

## 手順

- 1 Horizon Console で、エクスポートする表を表示します。  
たとえば、[インベントリ] - [マシン] の順にクリックして、マシン表を表示します。
- 2 表の右上の [エクスポート] アイコンをクリックします。  
アイコンにマウスをポイントすると、テーブルの内容をエクスポート ヒントが表示されます。
- 3 [ダウンロード場所の選択] ダイアログ ボックスで、XLSX ファイルのファイル名を入力します。
- 4 ファイルを保存する場所を参照します。
- 5 [保存] をクリックします。

## 次のステップ

スプレッドシートまたは他のツールを開き、XLSX 形式のファイルを表示します。

## Horizon Composer リンク クローン デスクトップ仮想マシンの管理

Horizon Composer のリンク クローン デスクトップ マシンの更新、オペレーティング システム データのサイズの削減、データストア間でのマシンの再調整を行うことができます。さらに、リンク クローンに関連付けられている通常ディスクを管理できます。

### Horizon Console でのマシンの更新によるリンク クローン サイズの削減

マシンの更新操作により、各リンク クローンのオペレーティング システム ディスクを元の状態とサイズに復元し、ストレージ コストを削減します。

可能であれば、オフピーク時に更新操作をスケジュール設定します。

ガイドラインについては、[マシンの更新操作](#)を参照してください。

#### 前提条件

- 更新操作のスケジュールを決定します。デフォルトで、Horizon Composer はすぐに操作を開始します。  
特定のリンク クローンに対し、一度にスケジュール設定できる更新操作は 1 回だけです。更新操作がさまざまなリンク クローンに影響する場合は、複数の更新操作をスケジュール設定できます。
- 操作が開始されたらすべてのユーザーを強制的にログオフさせるか、各ユーザーがログオフするのを待機してからそのユーザーのリンク クローン デスクトップを更新するかを決定します。  
ユーザーを強制的にログオフさせる場合、Horizon 7 は切断する前にユーザーに通知するため、ユーザーはアプリケーションを閉じてログオフすることができます。  
ユーザーを強制的にログオフさせる場合、ログオフが必要なリモート デスクトップ上の同時更新操作の最大数は [最大同時 View Composer メンテナンス操作数] 設定の値の半分にになります。たとえば、この設定を 24 にし、ユーザーを強制的にログオフさせる場合、ログオフが必要なリモート デスクトップ上の同時更新操作の最大数は 12 になります。
- レプリケートされた Connection Server インスタンスが展開環境内に含まれる場合は、すべてのインスタンスが同一バージョンであることを確認します。

#### 手順

- 1 Horizon Console で、[インベントリ] - [マシン] の順に選択します。
- 2 リンク クローン仮想マシンを選択します。
- 3 [インベントリ] タブで、1 台の仮想マシンを更新するのか、複数の仮想マシンを更新するのかを選択します。
  - 1 台の仮想マシンを更新するには、仮想マシン仮想マシンを選択して、[View Composer] ドロップダウンメニューから [更新] を選択します。
  - 複数の仮想マシンを更新するには、複数の仮想マシン仮想マシンを選択して、[View Composer] ドロップダウンメニューから [更新] を選択します。
- 4 ウィザードの手順に従います。

OS ディスクが元のサイズに縮小されます。

vCenter Server で、リンク クローン仮想マシンの更新操作の進捗を監視できます。

Horizon Console では、[インベントリ] - [デスクトップ] の順に選択してプール ID をクリックし、[タスク] タブをクリックすることで、操作を監視できます。[タスクを一時停止]、[タスクをキャンセル] または [タスクをレジューム] をクリックし、タスクを一時停止したり、タスクをキャンセルしたり、中断したタスクを再開したりできます。

## マシンの更新操作

ユーザーがリンク クローンを操作するたびに、クローンの OS ディスクが大きくなります。マシンの更新操作によって、OS ディスクが元の状態とサイズに復元され、ストレージ コストが削減されます。

更新操作は Horizon Composer パーシステント ディスクには影響しません。

リンク クローンは、完全な OS データを格納する親の仮想マシンに比べ使用するストレージ領域が少なくなります。ただし、クローンの OS ディスクはゲスト OS 内からデータが書き込まれるたびに拡大していきます。

Horizon Composer はリンク クローンの作成時に、クローンの OS ディスク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では、リンク クローン仮想マシンが一意に識別されます。更新操作によって、OS ディスクがそのスナップショットに戻されます。

Horizon Composer は、クローンを削除して再作成する場合にかかる時間のわずかに半分の時間で、リンク クローンを更新できます。

更新では以下のガイドラインが適用されます。

- デスクトップ プールの更新は、必要に応じて、スケジュール設定されたイベントとして、または OS データが指定サイズに達したときに実行できます。

特定のリンク クローンに対し、一度にスケジュール設定できる更新操作は 1 回だけです。更新操作をただちに開始した場合、以前にスケジュール設定されたすべてのタスクが上書きされます。

更新操作がさまざまなリンク クローンに影響する場合は、複数の更新操作をスケジュール設定できます。

新しい更新操作をスケジュール設定する前に、以前にスケジュール設定したすべてのタスクをキャンセルする必要があります。

- 専用割り当てプールとフローティング割り当てプールを更新できます。
- 更新は、ユーザーがリンク クローン デスクトップから切断される場合にのみ実行できます。
- 更新では、QuickPrep または Sysprep によって設定された一意のコンピュータ情報が保持されます。更新後に、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 SID または GUID を復元するために Sysprep を再実行する必要はありません。
- リンク クローンを再構成すると、Horizon 7 によって、リンク クローンの OS ディスクの新しいスナップショットが作成されます。その後の更新操作では、リンク クローンが最初に作成されたときに作成された元のスナップショットではなく、その新しいスナップショットによって OS データが復元されます。

ネイティブ NFS スナップショット (VAAI) テクノロジを使用してリンク クローンを生成する場合は、特定ベンダーの NAS デバイスによって、リンク クローンの OS ディスクの更新時にレプリカ ディスクのスナップショットが作成されます。これら NAS デバイスは、各クローンの OS ディスクのスナップショットを直接作成することとはサポートしていません。

- ユーザーが更新操作中に接続できる状態を保つ作動可能なプロビジョニングされたデスクトップの最小数を設定できます。

**注:** ページング ファイルとシステム一時ファイルを一時ディスクにリダイレクトすることによって、リンク クローンの拡大を抑えることができます。リンク クローンがパワーオフされると、Horizon 7 は一時ディスクを、Horizon Composer がリンク クローン プールで作成した元の一時的ディスクのコピーに置き換えます。この操作によって、一時ディスクが元のサイズに縮小されます。

このオプションは、リンク クローン デスクトップ プールの作成時に構成できます。

## Horizon Console でのリンク クローン デスクトップの更新

親仮想マシンで新しい基本イメージを作成し、再構成機能を使用して、リンク クローン仮想マシンを更新し、更新済みのイメージをリンク クローンに配布できます。

### リンク クローンの再構成のための親仮想マシンの準備

リンク クローン デスクトップ プールを再構成する前に、リンク クローンの基本イメージとして使用した親仮想マシンを更新する必要があります。

Horizon Composer では、あるオペレーティング システムを使用するリンク クローンを、別のオペレーティング システムを使用する親仮想マシンに再構成することはできません。たとえば、Windows 8 親仮想マシンのスナップショットを使用して、Windows 7 のリンク クローンを再構成することはできません。

### 手順

- 1 vCenter Server で、再構成のために親仮想マシンを更新します。
  - 親仮想マシンで、OS パッチまたはサービス パック、新しいアプリケーション、アプリケーションの更新をインストールするか、またはその他の変更を行います。
  - または、再構成時に新しい親として選択する別の仮想マシンを準備します。
- 2 vCenter Server で、更新済みまたは新しい親仮想マシンをパワーオフします。
- 3 vCenter Server で、親仮想マシンのスナップショットを作成します。

### 次のステップ

リンク クローン デスクトップ プールを再構成します。

### Horizon Console でのリンク クローン仮想マシンの再構成

マシンの再構成は、親仮想マシンに関連付けられているすべてのリンク クローン仮想マシンを同時に更新します。

可能であれば、オフピーク時に再構成をスケジュール設定します。

### 前提条件

- 親仮想マシンのスナップショットがあることを確認します。 [リンク クローンの再構成のための親仮想マシンの準備](#)を参照してください。
- 再構成のガイドラインについて理解しておきます。 [再構成によるリンク クローンの更新](#)を参照してください。
- 再構成のスケジュールを決定します。デフォルトで、Horizon Composer はすぐに再構成を開始します。

特定のリンク クローンに対し、一度にスケジュール設定できる再構成は 1 回だけです。再構成がさまざまなリンク クローンに影響する場合は、複数の再構成をスケジュール設定できます。

- 再構成が開始されたらただちにすべてのユーザーを強制的にログオフさせるか、各ユーザーがログオフするのを待機してからそのユーザーのリンククローン デスクトップを再構成するかを決定します。

ユーザーを強制的にログオフさせる場合、Horizon 7 は切断する前にユーザーに通知するため、ユーザーはアプリケーションを閉じてログオフすることができます。

- 最初のエラーでプロビジョニングを停止するかどうかを決定します。このオプションを選択し、Horizon Composer がリンク クローンをプロビジョニング中にエラーが発生すると、デスクトップ プール内のすべてのクローンに対するプロビジョニングが停止します。このオプションを選択することにより、ストレージなどのリソースが不必要に消費されるのを防ぐことができます。

[最初のエラーで停止] オプションを選択しても、カスタマイズには影響を与えません。リンク クローン上でカスタマイズ エラーが発生しても、他のクローンのプロビジョニングとカスタマイズは続行されます。

- デスクトップ プールのプロビジョニングが有効になっていることを確認します。デスクトップ プールのプロビジョニングが無効にされている場合、Horizon 7 によってデスクトップは再構成後にカスタマイズされないようになります。
- レプリケートされた Horizon Connection Server インスタンスがデプロイ内に含まれる場合は、すべてのインスタンスが同一バージョンであることを確認します。

## 手順

- 1 デスクトップ プール全体を再構成するか、単一マシンを再構成するかを選択します。

オプション	アクション
デスクトップ プール内のすべての仮想マシンを再構成する	<ol style="list-style-type: none"> <li>a Horizon Console で、[インベントリ] - [デスクトップ] の順に選択します。</li> <li>b プール ID をクリックして、再構成するデスクトップ プールを選択します。</li> <li>c [インベントリ] タブで [マシン] をクリックします。</li> <li>d 左の列から、すべてのマシン ID を選択します。</li> <li>e [Horizon Composer] ドロップダウン メニューから [再構成] を選択します。</li> </ol>
選択した仮想マシンを再構成する	<ol style="list-style-type: none"> <li>a Horizon Console で、[インベントリ] - [マシン] の順に選択します。</li> <li>b 左の列の [マシン ID] をクリックして、再構成するマシンを選択します。</li> <li>c [サマリ] タブで、[Horizon Composer] ドロップダウン メニューから [再構成] を選択します。</li> </ol>

- 2 ウィザードの手順に従います。

このデスクトップ プールの親仮想マシンとして使用する新しい仮想マシンを選択できます。

[設定内容の確認] ページで [詳細の表示] をクリックすると、再構成されるリンク クローン デスクトップを表示できます。

リンククローン仮想マシンが更新されます。OS ディスクが元のサイズに縮小されます。

専用割り当てプールでは、未割り当てのリンク クローンが削除され、再作成されます。指定した数のスペアの仮想マシンが保持されます。

フローティング割り当てプールでは、選択したすべてのリンク クローンが再構成されます。

vCenter Server で、リンククローン仮想マシンの再構成の進捗を監視できます。

Horizon Console では、[インベントリ] - [デスクトップ] の順に選択してプール ID をクリックし、[タスク] タブをクリックすることで、操作を監視できます。[タスクを一時停止]、[タスクをキャンセル] または [タスクをレジューム] をクリックし、タスクを一時停止したり、タスクをキャンセルしたり、中断したタスクを再開したりできます。

**注:** デスクトップ プールの作成時に、Sysprep カスタマイズ仕様を使用してリンク クローンをカスタマイズした場合、再構成された仮想マシンに対して新しい SID が作成されることがあります。

### 再構成によるリンク クローンの更新

再構成では、デスクトップ プール内のすべてのリンク クローンで、オペレーティング システムのパッチを提供したり、アプリケーションをインストールまたは更新したり、仮想マシン ハードウェア設定を変更したりすることができます。

リンク クローン仮想マシンを再構成するには、vCenter Server で親仮想マシンを更新するか、新しい親になる別の仮想マシンを選択します。次に、新しい親仮想マシンの構成のスナップショットを作成します。

リンク クローンは、親に直接リンクされているのではなく、レプリカにリンクされているため、リンク クローンに影響を与えることなく親仮想マシンを変更できます。

次に、デスクトップ プールの新しい基本イメージとして使用するスナップショットを選択して、再構成を開始します。Horizon Composer は新しいレプリカを作成し、再構成した OS ディスクをリンク クローンにコピーし、リンク クローンを新しいレプリカに関連付けます。

再構成によって、リンク クローンも更新され、OS ディスクのサイズが削減されます。

デスクトップの再構成は、Horizon Composer パーシステント ディスクには影響しません。

再構成では以下のガイドラインが適用されます。

- 専用割り当てデスクトップ プールとフローティング割り当てデスクトップ プールを再構成できます。
- デスクトップ プールの再構成は、必要に応じて、またはスケジュール設定されたイベントとして実行できます。  
特定のリンク クローンに対し、一度にスケジュール設定できる再構成は 1 回だけです。新しい再構成をスケジュール設定する前に、以前にスケジュール設定したすべてのタスクをキャンセルしたり、以前の操作が完了するまで待機したりする必要があります。新しい再構成をすぐに開始する前に、以前にスケジュール設定したすべてのタスクをキャンセルする必要があります。

再構成がさまざまなリンク クローンに影響する場合は、複数の再構成をスケジュール設定できます。

- デスクトップ プール内の選択したリンク クローンまたはすべてのリンク クローンを再構成できます。
- デスクトップ プール内のさまざまなリンク クローンが、基本イメージのさまざまなスナップショットやさまざまな基本イメージに基づいている場合、デスクトップ プールには複数のレプリカが含まれます。
- 再構成は、ユーザーがリンク クローン デスクトップからログオフしている場合にのみ実行できます。
- あるオペレーティング システムを使用するリンク クローンを、別のオペレーティング システムを使用する新しい、または更新された親仮想マシンに再構成することはできません。

- 現在のバージョンよりも低いハードウェア バージョンにリンク クローンを再構成することはできません。たとえば、ハードウェア バージョン 7 の親仮想マシンにハードウェア バージョン 8 のクローンを再構成することはできません。
- 再構成操作時に、ユーザーが引き続き接続できるプロビジョニングされた作動可能なデスクトップの最小数を設定できます。

---

**注:** デスクトップ プールの作成時に、Sysprep カスタマイズ仕様を使用してリンク クローンをカスタマイズした場合、再構成された仮想マシンに対して新しい SID が作成されることがあります。

---

## 失敗した再構成の修正

失敗した再構成を修正できます。さらに、使用するつもりであった基本イメージと異なる基本イメージを使用して、誤ってリンク クローンを再構成した場合も対処できます。

### 問題

再構成に失敗した結果、仮想マシンはエラーのある状態または古い状態になります。

### 原因

再構成中に、vCenter Server ホスト、vCenter Server、またはデータストアでシステム障害や問題が発生していた可能性があります。

あるいは、再構成で、元の親仮想マシンのオペレーティング システムとは別のオペレーティング システムの仮想マシンのスナップショットが使用された可能性があります。たとえば、Windows 7 のリンク クローンを再構成するために Windows 8 のスナップショットを使用した可能性があります。

### 解決方法

- 1 成功した最後の再構成で使用したスナップショットを選択します。

新しいスナップショットを選択し、リンク クローンを新しい状態に更新することもできます。

このスナップショットでは、元の親仮想マシンのスナップショットと同じオペレーティング システムを使用している必要があります。

- 2 デスクトップ プールを再構成します。

Horizon Composer はスナップショットから基本イメージを作成し、リンク クローン OS ディスクを再作成します。

再構成中に、ユーザー データおよび設定が保存された Horizon Composer パーシステント ディスクは保持されます。

誤った再構成の状況によっては、リンク クローンの再構成に加えて、それらを更新または再分散できます。

---

**注:** Horizon Composer パーシステント ディスクを構成しない場合は、再構成によって、リンク クローン仮想マシンでユーザーが生成した変更は削除されます。

---

## Horizon Console でのリンク クローン仮想マシンの再調整

再分散操作は、リンククローン仮想マシンを使用可能なデータストア間で均等に再分散します。



可能であれば、再分散操作をオフピーク時にスケジュール設定します。

#### 前提条件

- 再分散操作について理解しておきます。[#unique\\_185](#) を参照してください。
- 再分散操作のスケジュールを決定します。デフォルトで、Horizon Composer はすぐに操作を開始します。  
特定のリンク クローンに対し、一度にスケジュール設定できる再分散操作は 1 回だけです。再分散操作がさまざまなリンク クローンに影響する場合は、複数の再分散操作をスケジュール設定できます。
- 操作が開始されたらただちにすべてのユーザーを強制的にログオフさせるか、各ユーザーがログオフするのを待機してからそのユーザーのリンククローン デスクトップを再分散するかを決定します。  
ユーザーを強制的にログオフさせる場合、Horizon 7 は切断する前にユーザーに通知するため、ユーザーはアプリケーションを閉じてログオフすることができます。  
ユーザーを強制的にログオフさせると、ログオフが必要なリモート デスクトップ上の同時再調整操作の最大数は、[最大同時 Horizon Composer メンテナンス操作数] 設定値の半分になります。たとえば、この設定を 24 に構成し、ユーザーを強制的にログオフさせた場合、ログオフが必要なリモート デスクトップ上の同時再分散操作の最大数は 12 です。
- デスクトップ プールのプロビジョニングが有効になっていることを確認します。プールのプロビジョニングが無効にされている場合、Horizon 7 によって仮想マシンは再分散後にカスタマイズされないようになります。
- レプリケートされた Connection Server インスタンスが展開環境内に含まれる場合は、すべてのインスタンスが同一バージョンであることを確認します。

#### 手順

- 1 デスクトップ プール全体を再調整するか、単一マシンを再調整するかを選択します。

オプション	アクション
デスクトップ プール内のすべての仮想マシンを再調整する	<ol style="list-style-type: none"> <li>a Horizon Console で、[インベントリ] - [デスクトップ] の順に選択します。</li> <li>b プール ID をクリックして、再調整するデスクトップ プールを選択します。</li> <li>c [インベントリ] タブで [マシン] をクリックします。</li> <li>d 左の列から、すべてのマシン ID を選択します。</li> <li>e [View Composer] ドロップダウン メニューから、[再分散] を選択します。</li> </ol>
選択した仮想マシンを再調整する	<ol style="list-style-type: none"> <li>a Horizon Console で、[インベントリ] - [マシン] の順に選択します。</li> <li>b 左の列の [マシン ID] をクリックして、再調整するマシンを選択します。</li> <li>c [サマリ] タブの [View Composer] ドロップダウン メニューから [再調整] を選択します。</li> </ol>

- 2 ウィザードの手順に従います。

リンククローン仮想マシンが更新され、再分散されます。OS ディスクが元のサイズに縮小されます。

Horizon Console では、[インベントリ] - [デスクトップ] の順に選択してプール ID をダブルクリックし、[タスク] タブをクリックすることで、操作を監視できます。[タスクを一時停止]、[タスクをキャンセル] または [タスクをレジューム] をクリックし、タスクを一時停止したり、タスクをキャンセルしたり、中断したタスクを再開したりできます。

## 論理ドライブ間のリンク クローンの再分散

再分散操作は、リンク クローン仮想マシンを使用可能な論理ドライブ間で均等に再分配します。これによって、過負荷のドライブ上のストレージ領域が節約され、十分に使用されないドライブがなくなります。

大きなリンク クローン デスクトップ プールを作成し、複数の LUN (Logical Unit Number) を使用する場合、最初のサイズ設定が正確でないと、領域が効率的に使用されないことがあります。ストレージのオーバーコミット レベルを高く設定すると、リンク クローンが急速に拡大し、データストアのすべての空き領域が使用される可能性があります。

仮想マシンによって、データストアの 95% の領域が使用されると、Horizon 7 は警告ログ エントリを生成します。

再分散によって、リンク クローンも更新され、OS ディスクのサイズが削減されます。Horizon Composer パーシステント ディスクには影響しません。

再分散では以下のガイドラインが適用されます。

- 専用割り当てデスクトップ プールとフローティング割り当てデスクトップ プールを再分散できます。
- 選択したリンク クローンまたはプール内のすべてのクローンを再分散できます。
- デスクトップ プールの再分散は、必要に応じて、またはスケジュール設定されたイベントとして実行できます。

特定のリンク クローンに対し、一度にスケジュール設定できる再分散操作は 1 回だけです。再分散操作をただちに開始した場合、以前にスケジュール設定されたすべてのタスクが上書きされます。

再分散操作がさまざまなリンク クローンに影響する場合は、複数の再分散操作をスケジュール設定できます。

新しい再分散操作をスケジュール設定する前に、以前にスケジュール設定したすべてのタスクをキャンセルする必要があります。

- 再分散できるのは、スケジュールや保留中のキャンセルがない、Available (使用可能)、Error (エラー)、または Customizing (カスタマイズ) 状態の仮想マシンだけです。
- ベスト プラクティスとしては、同じデータストアに、リンク クローン仮想マシンと他のタイプの仮想マシンを混在させるのは避けてください。この場合、Horizon Composer はデータストアのすべての仮想マシンを再調整することができます。
- プールを編集し、ホストまたはクラスタ、およびリンク クローンが格納されているデータストアを変更した場合、新しく選択されたホストまたはクラスタが元のデータストアと新しいデータストアの両方へのフル アクセス権を持つ場合にのみ、リンク クローンを再分散できます。新しいクラスタのすべてのホストが元のデータストアと新しいデータストアへのアクセス権を持つ必要があります。

たとえば、スタンドアロン ホストにリンク クローン デスクトップ プールを作成し、クローンを保存するローカル データストアを選択したとします。デスクトップ プールを編集し、クラスタと共有データストアを選択した場合、クラスタ内のホストが元のローカル データストアにアクセスできないため、再分散操作は失敗します。

- 再分散操作時も接続したままにできる最小限の仮想マシンを設定できます。この仮想マシンは、すぐに使えるようにプロビジョニングされています。

---

**重要:** vSAN データストアを使用する場合、再分散操作は、デスクトップ プールのすべての仮想マシンを vSAN データストアから他のタイプのデータストアへ移行、またはその逆を行う場合にのみ使用できます。デスクトップ プールで vSAN データストアを使用する場合、vSAN では、ロード バランシング機能が提供され、ESXi クラスタ内のリソース使用が最適化されます。

---

## 再分散操作の後のリンク クローン ディスクのファイル名

リンク クローン仮想マシンを再調整すると、vCenter Server は、新しいデータストアに移動されたリンク クローン内の Horizon Composer パーシステント ディスクと破棄可能データ ディスクのファイル名を変更します。

元のファイル名によってディスクの種類が識別されます。名前が変更されたディスクには識別ラベルが含まれていません。

元のパーシステント ディスクのファイル名には、`user-disk` ラベルが含まれています (例: `desktop_name-vdm-user-disk-D-ID.vmdk`)。

元の破棄可能データ ディスクのファイル名には `disposable` ラベルが含まれています (例: `desktop_name-vdm-disposable-ID.vmdk`)。

再調整操作によってリンク クローンが新しいデータストアに移動された後、vCenter Server は、両方のディスクの種類に共通のファイル名構文 `desktop_name.n.vmdk` を使用します。

## Horizon Composer パーシステント ディスクの管理

Horizon Composer パーシステント ディスクをリンク クローン仮想マシンから接続解除し、別のリンク クローンに接続することができます。この機能により、ユーザー情報をリンク クローン仮想マシンから切り離して管理できます。

### Horizon Composer パーシステント ディスク

Horizon Composer を使用して、OS データとユーザー情報をリンク クローン仮想マシンの別々のディスクに構成できます。Horizon Composer は OS データの更新または再調整時に、パーシステント ディスク上のユーザー情報を保持します。

Horizon Composer パーシステント ディスクには、ユーザー設定とユーザーが生成したその他のデータが格納されます。リンク クローン デスクトップ プールを作成する場合は、通常ディスクを作成します。

リンク クローン仮想マシンから通常ディスクを切断し、その元のデータストアまたは別のデータストアにディスクを保存できます。ディスクを切断すると、リンク クローン仮想マシンが削除されます。切断された通常ディスクはどの仮想マシンにも関連付けられていません。

複数の方法を使用して、切断された通常ディスクを別のリンク クローン仮想マシンに接続できます。この柔軟性を利用して次のことが可能です。

- リンク クローンの削除時に、ユーザー データを保持できます。
- 従業員が退職する際に、別の従業員が離職する従業員のユーザー データにアクセスできます。
- 複数のリモート デスクトップを使用しているユーザーは、1 つのリモート デスクトップにユーザー データを統合できます。
- vCenter Server で仮想マシンにアクセスできなくなったが、通常ディスクが損傷していない場合、通常ディスクをインポートして、そのディスクを使用して新しいリンク クローンを作成できます。

---

**注:** 通常ディスクは、作成されたときに使用されていたオペレーティング システムに再接続する必要があります。たとえば、Windows 7 のリンク クローンから通常ディスクを切断し、その通常ディスクを Windows 8 のリンク クローンに再作成または接続することはできません。

---

## Horizon Console での Horizon Composer パーシステント ディスクの接続解除

Horizon Composer パーシステント ディスクをリンク クローン仮想マシンから接続解除したときに、ディスクが保存され、リンク クローンが削除されます。通常ディスクを切断することによって、別の仮想マシンでユーザー固有の情報を保存し再利用できます。

### 手順

- 1 Horizon Console で、[インベントリ] - [パーシステント ディスク] の順に選択します。
- 2 切断する通常ディスクを選択し、[切り離す] をクリックします。
- 3 通常ディスクを保存する場所を選択します。

オプション	説明
現在のデータストアを使用	通常ディスクを現在それが存在するデータストアに格納します。
次のデータストアを使用	通常ディスクを格納する新しいデータストアを選択します。[参照] をクリックし、下向き矢印をクリックして、[データストアの選択] メニューから新しいデータストアを選択します。 フィルタリングされた結果から、互換性のある非 vSAN データストアを選択し、接続解除されたパーシステント ディスクを格納できます。または、[すべてのデータストアを表示 (ローカルデータストアを含む)] を選択して、共有データストアや vSAN データストアを含むすべてのデータストアを表示します。vSAN データストアは使用できません。

Horizon Composer パーシステント ディスクがデータストアに保存されます。リンク クローン仮想マシンは削除され、Horizon Console に表示されません。

## Horizon Console での別のリンク クローンへの Horizon Composer パーシステント ディスクの接続

切断された通常ディスクを別のリンク クローン仮想マシンに接続できます。通常ディスクを接続すると、他の仮想マシンのユーザーがディスク内のユーザー設定および情報を使用できるようになります。

切断された通常ディスクを、選択したリンク クローン仮想マシン上のセカンダリ ディスクとして接続します。リンク クローンの新しいユーザーは、セカンダリ ディスクと既存のユーザー情報および設定にアクセスできます。

vSAN 以外のデータストアに格納されている通常ディスクは、vSAN データストアに格納されている仮想マシンに接続できません。同様に、vSAN に格納されているディスクは vSAN 以外に格納されている仮想マシンに接続できません。Horizon Console では、vSAN データストアと vSAN 以外のデータストアにまたがる仮想マシンを選択できません。

パーシステント ディスクを接続するリンク クローン デスクトップ プールにパーシステント ディスクのデータストアがない場合、デスクトップ プールの [マシン (View Composer の詳細)] タブと [パーシステント ディスク] タブにパーシステント ディスクの情報が表示されます。

### 前提条件

- 選択した仮想マシンが、通常ディスクが作成されたリンク クローンと同じオペレーティング システムを使用していることを確認します。

### 手順

- 1 Horizon Console で、[インベントリ] - [パーシステント ディスク] の順に選択します。
- 2 [切り離し済み] タブで通常ディスクを選択して、[接続] をクリックします。

- 3 通常ディスクを接続するリンク クローン仮想マシンを選択します。
- 4 パーシステント ディスクの接続先にするマシンを選択します。
- 5 [OK] をクリックします。

#### 次のステップ

リンク クローンのユーザーが、接続されたディスクを使用するための適切な権限を持っていることを確認します。たとえば、元のユーザーが通常ディスクに対する特定のアクセス権を持っており、その通常ディスクが新しいリンク クローン上のドライブ D として接続された場合、リンク クローンの新しいユーザーはドライブ D に対して元のユーザーのアクセス権を持っている必要があります。

リンク クローンのゲスト OS に管理者としてログインし、新しいユーザーに適切な権限を割り当てます。

#### Horizon Console での Horizon Composer パーシステント ディスクのプールまたはユーザーの編集

Horizon 7 から元のデスクトップ プールまたはユーザーが削除された場合は、接続解除された Horizon Composer パーシステント ディスクを新しいデスクトップ プールまたはユーザーに割り当てることができます。

切断された通常ディスクは、元のデスクトップ プールとユーザーに関連付けられたままです。そのデスクトップ プールまたはユーザーが Horizon 7 から削除された場合は、その通常ディスクを使用してリンク クローン仮想マシンを再作成することはできません。

そのデスクトップ プールとユーザーを編集することにより、切断された通常ディスクを使用して、新しいデスクトップ プール内に仮想マシンを再作成できます。その仮想マシンは、新しいユーザーに割り当てられます。

新しいデスクトップ プール、新しいユーザー、またはその両方を選択できます。

#### 前提条件

- 通常ディスクのデスクトップ プールまたはユーザーが Horizon 7 から削除されたことを確認します。
- 新しいデスクトップ プールが、通常ディスクが作成されたデスクトップ プールと同じオペレーティング システムを使用していることを確認します。

#### 手順

- 1 Horizon Console で、[インベントリ] - [パーシステント ディスク] の順に選択します。
- 2 ユーザーまたはデスクトップ プールが削除された通常ディスクを選択し、[編集] をクリックします。
- 3 (オプション) リストからリンク クローン デスクトップ プールを選択します。
- 4 (オプション) 通常ディスクのユーザーを選択します。

Active Directory のドメインとユーザー名を参照できます。

#### 次のステップ

切断された通常ディスクを使用してリンク クローン仮想マシンを再作成します。

## Horizon Console での接続解除されたパーシステント ディスクによるリンク クローンの再作成

Horizon Composer パーシステント ディスクを接続解除すると、リンク クローンが削除されます。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して、元のユーザーが、切断されたユーザー設定および情報にアクセスできるようにすることができます。

**注:**すでに最大サイズに達しているデスクトップ プール内にリンク クローン仮想マシンを再作成した場合も、再作成された仮想マシンがそのデスクトップ プールにそのまま追加されます。デスクトップ プールのサイズが大きくなり、未割り当てのマシンを削除するとサイズが小さくなります。

通常ディスクの元のデスクトップ プールまたはユーザーが Horizon 7 から削除された場合は、その通常ディスクに新しいデスクトップ プールまたはユーザーを割り当てることができます。 [Horizon Console での Horizon Composer パーシステント ディスクのプールまたはユーザーの編集](#)を参照してください。

新しい仮想マシンが vSAN データストアに格納されている場合、Horizon 7 は、vSAN 以外のデータストアに格納されている通常ディスクによる仮想マシンの再作成をサポートしません。同様に、vSAN に通常ディスクが格納されている場合、Horizon 7 は、vSAN 以外での仮想マシンの再作成をサポートしません。

切断された通常ディスクを vSAN 以外から vSAN に移動する場合は、vSAN 以外のデータストアに格納された仮想マシンでディスクを再作成して、仮想マシンのデスクトップ プールを vSAN データストアに再分散できます。

### 手順

- 1 Horizon Console で、[インベントリ] - [パーシステント ディスク] の順に選択します。
- 2 [切り離し済み] タブで通常ディスクを選択して、[マシンを再作成] をクリックします。  
複数の通常ディスクを選択して、各ディスクのリンク クローン仮想マシンを再作成できます。
- 3 [OK] をクリックします。

Horizon 7 によって、選択した通常ディスクごとにリンク クローン仮想マシンが作成され、元のデスクトップ プールにその仮想マシンが追加されます。

通常ディスクはそれらが格納されていたデータストアに残ります。

## Horizon Console での vSphere からのパーシステント ディスクのインポートによるリンク クローンのリストア

Horizon 7 でリンク クローン仮想マシンにアクセスできなくなった場合、Horizon Composer パーシステント ディスクで仮想マシンが構成されていれば、仮想マシンをリストアできます。vSphere データストアから Horizon 7 へ通常ディスクをインポートできます。

Horizon 7 で、パーシステント ディスク ファイルを、接続解除されたパーシステント ディスクとしてインポートします。Horizon 7 で、切断されたディスクを既存の仮想マシンに接続するか、または元のリンク クローンを再作成することができます。

### 手順

- 1 Horizon Console で、[インベントリ] - [パーシステント ディスク] の順に選択します。
- 2 [切り離し済み] タブで、[vCenter からインポートする] をクリックします。
- 3 vCenter Server インスタンスを選択します。
- 4 ディスク ファイルが存在するデータセンターを選択します。

- 5 リンク クローン デスクトップ プールを選択します。

**注:** デスクトップ プールの選択後に選択できるのは、デスクトップ プールのデータストアを基にしたパーシステント ディスクだけです。たとえば、vSAN データストアのあるデスクトップ プールを選択した場合、vSAN データストアからパーシステント ディスクを選択できます。

- 6 アクセス グループを選択します。
- 7 [通常ディスク ファイル] テキスト ボックスで、[参照] をクリックし、下向き矢印をクリックして、[データストアの選択] メニューからデータストアを選択します。
- 8 ローカル データストアからパーシステント ディスクをインポートするには、[すべてのデータストアを表示 (ローカル データストアを含む)] を選択します。
- 9 ディスク ストレージ ファイルと仮想マシン ファイルを表示するデータストア名をクリックします。
- 10 インポートするパーシステント ディスク ファイルを選択して、[OK] をクリックします。
- 11 [ユーザー] テキスト ボックスで、[参照] をクリックし、仮想マシンに割り当てるユーザーを選択して、[OK] をクリックします。
- 12 [送信] をクリックします。

ディスク ファイルが、切断された通常ディスクとして Horizon 7 にインポートされます。

#### 次のステップ

リンク クローン仮想マシンを復元するために、元の仮想マシンを再作成するか、または切断された通常ディスクを別の仮想マシンに接続することができます。

詳細については、[Horizon Console での接続解除されたパーシステント ディスクによるリンク クローンの再作成](#)および [Horizon Console での別のリンク クローンへの Horizon Composer パーシステント ディスクの接続](#)を参照してください。

#### Horizon Console での接続解除された Horizon Composer パーシステント ディスクの削除

切断された通常ディスクを削除する場合は、Horizon 7 からはディスクを削除するがデータストアには残すことも、Horizon 7 とデータストアからディスクを削除することもできます。

#### 手順

- 1 Horizon Console で、[インベントリ] - [パーシステント ディスク] の順に選択します。
- 2 [切り離し済み] タブで通常ディスクを選択して、[削除] をクリックします。
- 3 Horizon Console からディスクを削除した後に、それをデータストアから削除するか、データストア上に残すかを選択します。

オプション	説明
[View Manager からのみ削除]	削除後、通常ディスクは Horizon 7 でアクセスできなくなりますが、データストアには残ります。
[ディスクから削除]	削除後、通常ディスクが存在しなくなります。



- 4 [OK] をクリックします。

## Horizon Console での管理対象外のマシンと登録済みマシンの管理

Horizon Console では、管理対象外のマシンと登録済みのマシンを Horizon 7 から削除できます。

管理対象外のマシンには、vCenter Server により管理されていない物理コンピュータ、RDS ホスト、仮想マシンが含まれます。したがって、管理対象外のマシンをデスクトップ プールに追加する前に、接続サーバ インスタンスに登録する必要があります。

Horizon 7 には [RDS ホスト] と [その他] の 2 つのタイプの登録済みのマシンがあります。管理対象外のマシンはその他のカテゴリに含まれます。管理対象外のマシンを使用して、vCenter Server 仮想マシンを含まないデスクトップ プールが形成されます。

管理対象外のマシンに影響を与える設定を再構成する場合は、新しい設定が有効になるまでに 10 分程度かかることがあります。たとえば、プールの [切断後に自動的にログアウト] の設定を変更すると、Horizon 7 が影響を受ける管理対象外のマシンを再構成するまでに 10 分ほどかかる場合があります。

### Horizon Console でのデスクトップ プールからの管理対象外マシンの削除

管理対象外のマシンをプールから削除することによって、デスクトップ プールのサイズを減らすことができます。

#### 手順

- 1 Horizon Console で、[インベントリ] - [マシン] の順に選択します。
- 2 [その他] タブを選択します。
- 3 削除する管理対象外のマシンを選択します。
- 4 [削除] をクリックします。
- 5 [OK] をクリックします。

管理対象外のマシンがプールから削除されます。

### Horizon Console での登録済みマシンの削除

登録済みマシンを再度使用する予定がない場合は、Horizon 7 から削除できます。

削除した登録済みのマシンは、Horizon 7 で使用できなくなります。マシンを再度使用できるようにするには、Horizon Agent を再インストールする必要があります。

#### 前提条件

削除する登録済みマシンが、どのデスクトップ プールでも使用されていないことを確認します。

#### 手順

- 1 Horizon Console で、[設定] - [登録済みのマシン] の順に選択します。
- 2 [RDS ホスト] タブをクリックします。
- 3 1 つ以上のマシンを選択し、[削除] をクリックします。

選択できるマシンは、デスクトップ プールで使用されていないものだけです。



4 [OK] をクリックして確定します。

## 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

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。

### Horizon Console での問題のあるマシンの表示

動作が疑わしいとして Horizon 7 によって検出されたマシンのリストを表示できます。

Horizon Console 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 Horizon Console で、[インベントリ] - [マシン] の順に選択します。
- 2 [vCenter Server] タブで、[マシン] ドロップダウン メニューから [問題のあるマシン] をクリックします。

#### 次のステップ

必要なアクションは、Horizon Console が各マシンについて報告した問題によって異なります。

- 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。
- 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 プールのユーザー割り当ての確認

専用ユーザー割り当ての場合、仮想マシンに割り当てられているユーザーが仮想デスクトップに接続しているユーザーかどうかを確認できます。

### 前提条件

- 仮想マシンが専用割り当てプールに属していることを確認します。Horizon Console で、デスクトップ プールの割り当てが [デスクトップ プール] ページの [ユーザーの割り当て] 列に表示されます。
- ユーザーにデスクトップ プールに対する資格を付与していることを確認します。

### 手順

- 1 Horizon Console で、[インベントリ] - [マシン] の順に選択します。
- 2 [vCenter Server] タブで、割り当てられたユーザーまたは接続しているユーザーを表示します。

オプション	説明
[割り当てられたユーザー]	<p>[割り当てられたユーザー] 列に、デスクトップ プールに割り当てられているユーザーが表示されます。</p> <p><b>注:</b> [割り当てられたユーザー] 列に、フローティング デスクトップ プールのユーザーは表示されません。</p>
[接続しているユーザー]	<p>[接続しているユーザー] 列に、仮想マシンに接続しているユーザーが表示されます。通常、割り当てられたユーザーがデスクトップに接続している場合、[接続しているユーザー] と [割り当てられているユーザー] には同じユーザーが表示されます。それ以外の場合、管理者が仮想マシンに接続していれば、[接続しているユーザー] 列に管理者が表示されます。</p>

## Horizon Console でのデスクトップの再起動と仮想マシンのリセット

仮想デスクトップで再起動操作を実行すると、仮想マシンのオペレーティング システムのグレースフル再起動が実行されます。仮想マシンでリセット操作を実行すると、オペレーティング システムのグレースフル再起動は実行されず、仮想マシンのパワーオフとパワーオンが即時実行されます。

表 10-11. リセット機能と再起動機能

プールタイプ	リセット機能 (プール、マシン、セッション、Horizon Client)	再起動機能 (プール、マシン、セッション、Horizon Client)
完全クローン プール (専用プールとフローティング プール、[ログオフ時に削除] オプションは無効)	仮想マシンのリセット (仮想マシンのパワーオフとパワーオン)	仮想マシンの再起動 (OS のグレースフル再起動)
インスタント クローン プール (フローティング プール)	[仮想マシンのパワーオフ] - [仮想マシンの削除] - [新規仮想マシンの作成] - [パワーオン]	[OS のグレースフル シャットダウン] - [仮想マシンの削除] - [新規仮想マシンの作成] - [パワーオン]
公開されたデスクトップ プール	NA (未サポート)	NA (未サポート)

**注:** 再起動機能は、Horizon Client 4.4 以降で使用できます。

#### 手順

- 1 Horizon Console で、[インベントリ] - [マシン] の順に選択します。
- 2 [vCenter Server] タブで、仮想デスクトップの再起動または仮想マシンのリセットを選択します。

オプション	説明
デスクトップの再起動	仮想マシンを再起動します。オペレーティング システムのグレースフル再起動が実行されます。この操作は、vCenter Server 仮想マシンが含まれる自動プールまたは手動プールにのみ適用されます。
仮想マシンをリセット	仮想マシンをリセットします。オペレーティング システムのグレースフル再起動は実行されません。この操作は、vCenter Server 仮想マシンが含まれる自動プールまたは手動プールにのみ適用されます。

- 3 [OK] をクリックします。

## Horizon Console でのデスクトップ 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 Horizon Console で、[インベントリ] - [デスクトップ] の順にクリックします。
- 2 プール ID をクリックし、[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。

## Horizon Console での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、『Horizon 7 管理ガイド』を参照してください。

### 手順

- 1 Horizon Console で、[インベントリ] - [マシン] の順に選択します。
- 2 [その他のコマンド] - [資格のないマシンの表示] の順に選択します。
- 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] の順に選択するか、[その他のコマンド] - [資格のないポリシーを表示] の順に選択します。
- 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。

# Horizon Console での公開デスクトップとアプリケーションの作成

# 11

Horizon 7 では、Windows リモート デスクトップ サービス (RDS) ホストのグループであるファームに関連付けられる公開デスクトップを作成できます。アプリケーション プールを作成することによって、公開アプリケーションを多くのユーザーに提供することもできます。アプリケーション プール内の公開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。

この章には、次のトピックが含まれています。

- [Horizon Console でのファームの作成](#)
- [Horizon Console での公開デスクトップ プールの作成](#)
- [Horizon Console でのアプリケーション プールの作成](#)
- [Horizon Console でのファームの管理](#)
- [Horizon Console でのアプリケーション プールの管理](#)
- [Horizon Console での RDS ホストの管理](#)
- [Horizon Console での公開デスクトップ セッションとアプリケーション セッションの管理](#)

## Horizon Console でのファームの作成

ファームは、Windows リモート デスクトップ サービス (RDS) ホストのグループです。ファームに関連付けられている公開デスクトップを作成できます。アプリケーション プールを作成することによって、公開アプリケーションを多くのユーザーに提供することもできます。アプリケーション プール内の公開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。

ファームを使用すると、エンタープライズ内の RDS ホスト、公開デスクトップ、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 のインスタント クローン仮想マシンである RDS ホストで構成されます。

接続サーバは、ファームの作成時に指定したパラメータに基づいてインスタントクローン仮想マシンを作成します。インスタント クローンは、親仮想マシンの仮想ディスクを共有するため、フル仮想マシンよりも使用するストレージは少なくなります。さらに、インスタント クローンは親仮想マシンのメモリを共有し、vmFork テクノロジーを使用して作成されます。

アプリケーション プールまたは公開デスクトップ 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。ファーム内の公開ホストは、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。ファームでは公開デスクトップ 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。

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

## Horizon Console でファームを手動で作成するためのワークシート

手動ファームを作成するときに、特定のファーム設定を行うことができます。

表 11-1. ワークシート：手動ファームを作成するための設定

設定	説明	値をここに記入
ID	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	ファームに対するアクセス グループを選択するか、ファームをデフォルトのルート アクセス グループに残します。	
デフォルト表示プロトコル	[VMware Blast]、[PCoIP]、または [Microsoft RDP] を選択します。Microsoft 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。[Microsoft 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、公開デスクトップ 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 から公開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。	
事前起動セッションのタイムアウト (アプリケーションのみ)	事前起動が設定されたアプリケーションが開かれたままにする時間を決定します。デフォルトは [10 分] です。  エンドユーザーが Horizon Client の任意のアプリケーションを起動しない場合、アイドル状態のセッションがタイムアウトになるか、事前起動セッションがタイムアウトになると、アプリケーション セッションが切断されます。  タイムアウト後に事前起動セッションを終了するには、[切断されたセッションからのログオフ] オプションを [直後] に設定する必要があります。	
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] または [直後] を選択するか、分単位で数字を設定します。デフォルトは [1 分後] です。[直後] を選択すると、30 秒以内にセッションがログオフまたは切断します。  Horizon Agent がインストールされている RDS ホストのレジストリ キーを編集すると、セッションのログオフまたは切断時間をさらに短縮できます。 HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\wssm\applaunchmgr\Params に移動し、WindowCheckInterval の値を設定します。デフォルト値は 20000 です。この場合、空のセッションの確認が 20 秒ごとに行われます。最後のアプリケーション セッションが終了してからセッションがログオフするまでの最大時間は 40 秒に設定されます。この値は 2500 に変更できます。この場合、空のセッションの確認が 2.5 秒ごとに行われます。最後のアプリケーションが終了してからセッションがログオフするまでの最大時間は 5 秒に設定されます。	

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に比較的時間がかかります。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	公開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] ボックスをチェックして、公開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。	
セッション共同作業を許可	このファームをベースにするデスクトップ プールのユーザーに、リモート デスクトップセッションへの他のユーザーの招待を許可するには、[有効] を選択します。セッション オーナーと共同作業者は、VMware Blast プロトコルを使用する必要があります。	

## Horizon Console での手動ファームの作成

公開アプリケーションまたは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。『Horizon 7 での公開されたデスクトップとアプリケーションのセットアップ』ドキュメントの「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。Horizon Console で、[設定] - [登録済みのマシン] の順に選択し、[RDS ホスト] タブで各 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。 [Horizon Console でファームを手動で作成するためのワークシート](#)を参照してください。

### 手順

- 1 Horizon Console で、[インベントリ] - [ファーム] の順に選択します。
- 2 [追加] をクリックします。
- 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 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。
- 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。

## 次のステップ

公開アプリケーションまたはデスクトップ プールを作成します。

## Horizon Console で自動インスタント クローン ファームを作成するためのワークシート

自動インスタント クローン ファームを作成するときに、特定の設定を行うことができます。

表 11-2. ワークシート：自動インスタントクローン ファームを作成するための設定

設定	説明	値をここに記入
ID	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	ファームに対するアクセス グループを選択するか、ファームをデフォルトのルート アクセス グループに残します。	
デフォルト表示プロトコル	[VMware Blast]、[PCoIP]、または [Microsoft RDP] を選択します。Microsoft 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。[Microsoft 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、公開デスクトップ 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 から公開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。	



設定	説明	値をここに記入
3D レンダラー	<p>デスクトップに 3D グラフィックス レンダリングを選択します。</p> <p>3D レンダリングは、仮想ハードウェア バージョン 11 以降の仮想マシンを実行する Windows 2008、Windows 2012、Windows 2016 のゲストでサポートされています。ハードウェアベースのレンダリングは、vSphere 6.0 U1 以降の環境の仮想ハードウェア バージョン 11 以降でサポートされています。ソフトウェア レンダリングは、vSphere 6.0 U1 以降の環境の仮想ハードウェア バージョン 11 以降でサポートされています。</p> <p>ESXi 5.0 ホストの場合、レンダリングに最大 128MB の VRAM を使用できます。ESXi 5.1 以降のホストの場合、VRAM の最大サイズは 512MB です。vSphere 6.0 のハードウェア バージョン 11 (HWv11) の仮想マシンでは、VRAM 値 (ビデオ メモリ) が変更されています。vSphere Web Client で [vSphere Client を使用して管理] オプションを選択して、これらのマシンのビデオ メモリを設定します。詳細については、『vSphere 仮想マシン管理』ガイドの「3D グラフィックスの構成」を参照してください。</p> <p>デフォルトの表示プロトコルに Microsoft RDP を選択し、ユーザーに表示プロトコルの選択を許可しない場合、3D レンダリングは無効になります。</p> <ul style="list-style-type: none"> <li>■ [NVIDIA GRID vGPU]: 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。このオプションを選択すると、vSphere Distributed Resource Scheduler (DRS) は使用できません。</li> </ul> <p>インスタント クローン デスクトップ プールに NVIDIA GRID vGPU を使用する場合には、プロトコルとして VMware Blast を選択し、ユーザーに独自の表示プロトコルを選択させないことを推奨します。</p> <ul style="list-style-type: none"> <li>■ [vSphere Client を使用して管理]。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。Horizon 7 は 3D レンダリングを制御しません。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、Horizon Console で設定した場合と同じ効果を持ちます。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。[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]、[モニターの最大数]、[特定のモニターの最大解像度] の設定が Horizon Console 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。</li> <li>■ [無効化]: 3D レンダリングが非アクティブです。デフォルトでは無効になっています。</li> </ul>	
事前起動セッションのタイムアウト (アプリケーションのみ)	<p>事前起動が設定されたアプリケーションが開かれたままにする時間を決定します。デフォルトは [10 分] です。</p> <p>エンドユーザーが Horizon Client の任意のアプリケーションを起動しない場合、アイドル状態のセッションがタイムアウトになるか、事前起動セッションがタイムアウトになると、アプリケーション セッションが切断されます。</p> <p>タイムアウト後に事前起動セッションを終了するには、[切断されたセッションからのログオフ] オプションを [直後] に設定する必要があります。</p>	

設定	説明	値をここに記入
空のセッションのタイムアウト（アプリケーションのみ）	<p>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] または [直後] を選択するか、分単位で数字を設定します。デフォルトは [1 分後] です。[直後] を選択すると、30 秒以内にセッションがログオフまたは切断します。</p> <p>Horizon Agent がインストールされている RDS ホストのレジストリ キーを編集すると、セッションのログオフまたは切断時間をさらに短縮できます。</p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\wssm\applaunchmgr\Params に移動し、WindowCheckInterval の値を設定します。デフォルト値は 20000 です。この場合、空のセッションの確認が 20 秒ごとに行われます。最後のアプリケーション セッションが終了してからセッションがログオフするまでの最大時間は 40 秒に設定されます。この値は 2500 に変更できます。この場合、空のセッションの確認が 2.5 秒ごとに行われます。最後のアプリケーションが終了してからセッションがログオフするまでの最大時間は 5 秒に設定されます。</p>	
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。	
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	公開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] ボックスをチェックして、公開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。	
セッション共同作業を許可	このファームをベースにするデスクトップ プールのユーザーに、リモート デスクトップセッションへの他のユーザーの招待を許可するには、[有効] を選択します。セッション オーナーとセッション共同作業者は、VMware Blast 表示プロトコルを使用する必要があります。	
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	<p>プリフィックスまたは名前の形式を指定します。Horizon 7 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、プ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=&lt;number of digits&gt;}] を指定することもできます。[fixed=&lt;number of digits&gt;] 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。</p> <p><b>注:</b> 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。</p>	

設定	説明	値をここに記入
マシンの最大数	プロビジョニングするマシンの数。	
インスタント クローン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、接続サーバがファームの仮想マシンのメンテナンス操作を行っている間、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。この設定は、即時メンテナンスをスケジュールする場合には適用されません。	
VMware vSAN の使用	使用可能な場合は、VMware vSAN を使用するかどうかを指定します。vSAN は Software-Defined Storage 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。	
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>(vSAN を使用しない場合にのみ使用可能) 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。</p> <p>このオプションを選択すると、1 つ以上のインスタントクローン データストアまたはレプリカ ディスク データストアを選択するオプションを選択できます。</p>	
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のわかる命名規則を使用することをお勧めします。	
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、ファーム内のインスタント 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 イメージから今後インスタント 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インスタント 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、接続サーバのメンテナンス操作も必要です。</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。	
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>vSAN データストア (vSphere 5.5 Update 1 の機能) では、最大 20 台までの 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 台までの 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 [インスタント 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、インスタント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> <p><b>注:</b> vSAN を使用する場合、データストアを 1 つのみ選択します。</p>	

設定	説明	値をここに記入
レプリカ ディスク データストア	<p>インスタントクローンを格納するレプリカ ディスク データストアを 1 つ以上選択します。このオプションは、レプリカとオペレーティング システム ディスクで別々のデータストアを選択する場合に表示されます。</p> <p>[ファームを追加] ウィザードの [レプリカ ディスクのデータストアを選択します] 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、インスタントクローンを格納するための十分な大きさがあるレプリカ ディスク データストアを特定するのに役立ちます。</p>	
ネットワーク	<p>自動インスタントクローン ファームに使用するネットワークを選択します。複数の vLAN ネットワークを選択して、大規模な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。デフォルト設定では、現在の親仮想マシンのイメージのネットワークが使用されます。</p> <p>[ネットワークの選択] ウィザードの表には、使用可能なネットワーク、ポート、およびポート バインドが表示されます。複数のネットワークを使用するには、[現在の親仮想マシン イメージのネットワークを使用します] の選択を解除し、インスタントクローン ファームで使用するネットワークを選択する必要があります。</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>接続サーバには、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、インスタントクローン マシンをカスタマイズするために ClonePrep によって使用されます。</p> <p>このユーザーは、vCenter Server のための接続サーバ設定を構成するときに指定します。接続サーバ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。</p> <p>[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>	
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: <b>CN=Computers</b></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。コンテナ名は、カット、コピー、またはペーストできます。</p>	
既存のコンピュータ アカウントの再利用を許可	<p>このオプションは、新しいインスタント クローンの仮想マシン名が既存のコンピュータ アカウント名に一致するときに、Active Directory にある既存のコンピュータ アカウントを使用する場合に選択します。</p> <p>インスタント クローンの作成時に、既存の Active Directory コンピュータ アカウント名がインスタント クローン仮想マシン名に一致すると、Horizon 7 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 コンテナの設定で指定する Active Directory コンテナに配置されている必要があります。</p> <p>このオプションを無効にした場合、Horizon 7 がインスタント クローンを作成するときに、新しい Active Directory 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>	

設定	説明	値をここに記入
ClonePrep を使用	<p>仮想マシンをカスタマイズするための ClonePrep カスタマイズ仕様を指定します。</p> <ul style="list-style-type: none"> <li>■ [パワーオフ スクリプト名]。インスタントクローン マシンがパワーオフになる前に ClonePrep が実行するカスタマイズ スクリプトの名前。親仮想マシン上のスクリプトのパスを指定します。</li> <li>■ [パワーオフ スクリプト パラメータ]。インスタントクローン マシンをパワーオフする前に、ClonePrep がこれらのマシンでカスタマイズ スクリプトを実行するために使用できるパラメータを提供します。たとえば、p1 を使用します。</li> <li>■ [同期後スクリプト名]。インスタントクローン マシンが作成された後、またはイメージがこれらのマシンにプッシュされた後に、インスタントクローン マシンで ClonePrep が実行するカスタマイズ スクリプトの名前。親仮想マシン上のスクリプトのパスを指定します。</li> <li>■ [同期後スクリプト パラメータ]。インスタントクローン マシンが作成された後、またはイメージがこれらのマシンにプッシュされた後に、インスタントクローン マシンで ClonePrep が実行するスクリプトのパラメータを提供します。たとえば、p2 を使用します。</li> </ul>	
設定内容の確認	自動インスタントクローン ファームの設定を確認します。	

## Horizon Console での自動インスタント クローン ファームの作成

公開アプリケーションまたは公開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、自動インスタント クローン ファームを作成します。

### 前提条件

- Connection Server がインストールされていることを確認します。『Horizon 7 のインストール』ドキュメントを参照してください。
- vCenter Server の Connection Server 設定が Horizon Administrator で構成されていることを確認します。『Horizon 7 の管理』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。
- 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。『Horizon 7 での公開されたデスクトップとアプリケーションのセットアップ』ドキュメントで「自動ファーム用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。Connection Server 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。
- 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。 [Horizon Console で自動インスタント クローン ファームを作成するためのワークシート](#)を参照してください。

### 手順

- 1 Horizon Console で、[インベントリ] - [ファーム] の順に選択します。
- 2 [追加] をクリックします。

- 3 [自動ファーム] を選択します。
- 4 [インスタント クローン] を選択します。
- 5 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。

#### 次のステップ

公開アプリケーション プールまたは公開デスクトップ プールを作成します。 [Horizon Console での公開デスクトップ プールの作成](#)または [Horizon Console でのアプリケーション プールの作成](#)を参照してください。

## Horizon Console での自動リンク クローン ファーム作成用ワークシート

自動リンク クローン ファームを作成するときに、特定の設定を行うことができます。

表 11-3. ワークシート：自動リンククローン ファームを作成するための構成

設定	説明	値をここに記入
ID	Horizon Console 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、『Horizon 7 の管理』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。	
事前起動セッションのタイムアウト (アプリケーションのみ)	事前起動が設定されたアプリケーションが開かれたままにする時間を決定します。デフォルトは [10 分] です。 エンドユーザーが Horizon Client の任意のアプリケーションを起動しない場合、アイドル状態のセッションがタイムアウトになるか、事前起動セッションがタイムアウトになると、アプリケーション セッションが切断されます。 タイムアウト後に事前起動セッションを終了するには、[切断されたセッションからのログオフ] オプションを [直後] に設定する必要があります。	

設定	説明	値をここに記入
空のセッションのタイムアウト（アプリケーションのみ）	<p>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] または [直後] を選択するか、分単位で数字を設定します。デフォルトは [1 分後] です。[直後] を選択すると、30 秒以内にセッションがログオフまたは切断します。</p> <p>Horizon Agent がインストールされている RDS ホストのレジストリ キーを編集すると、セッションのログオフまたは切断時間をさらに短縮できます。</p> <p>HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\Plugins\wssm\applaunchmgr\Params に移動し、WindowCheckInterval の値を設定します。デフォルト値は 20000 です。この場合、空のセッションの確認が 20 秒ごとに行われます。最後のアプリケーション セッションが終了してからセッションがログオフするまでの最大時間は 40 秒に設定されます。この値は 2500 に変更できます。この場合、空のセッションの確認が 2.5 秒ごとに行われます。最後のアプリケーションが終了してからセッションがログオフするまでの最大時間は 5 秒に設定されます。</p>	
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。	
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。	
セッション共同作業を許可	このファームをベースにするデスクトップ プールのユーザーに、リモート デスクトップセッションへの他のユーザーの招待を許可するには、[有効] を選択します。セッション オーナーとセッション共同作業者は、VMware Blast プロトコルを使用する必要があります。	
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	<p>プリフィックスまたは名前の形式を指定します。Horizon 7 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、プ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=&lt;number of digits&gt;}] を指定することもできます。[fixed=&lt;number of digits&gt;] 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。</p> <p><b>注:</b> 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。</p>	



設定	説明	値をここに記入
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。	
VMware vSAN の使用	使用可能な場合は、VMware vSAN を使用するかどうかを指定します。vSAN は Software-Defined Storage 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、『Horizon 7 での仮想デスクトップのセットアップ』の「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 vSAN 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	(vSAN を使用しない場合にのみ使用可能) 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。	
スナップショット	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。  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。	
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。	
クラスタ	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。  vSAN データストア (vSphere 5.5 Update 1 の機能) では、最大 20 台までの 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 台までの ESXi ホストを持つクラスタを選択できます。  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。  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。	
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。	



設定	説明	値をここに記入
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、『Horizon 7 での仮想デスクトップのセットアップ』の「インスタントクローンおよびリンククローン デスクトップ プールのストレージ サイズ設定」を参照してください。</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。詳細については、『Horizon 7 での仮想デスクトップのセットアップ』の「ローカル データストアへのリンク クローンの保存」を参照してください。</p> <p><b>注:</b> vSAN 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、『Horizon 7 での仮想デスクトップのセットアップ』の「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」を参照してください。</p> <p><b>注:</b> vSAN を使用する場合、この設定は効果がありません。</p>	
ネイティブ NFS スナップショット (VAAI) を使用	<p>(vSAN 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、『Horizon 7 での仮想デスクトップのセットアップ』の「View Composer リンク クローン用の VAAI ストレージの使用」を参照してください。</p>	
仮想マシン ディスク容量を再利用	<p>(vSAN または Virtual Volumes を使用しない場合にのみ使用可能) 容量効率の高いディスク フォーマットで作成されたリンク クローンの未使用ディスク容量を ESXi ホストが再利用できるかどうかを指定します。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、『Horizon 7 での仮想デスクトップのセットアップ』の「リンク クローン仮想マシンのディスク領域を再利用する」を参照してください。</p>	

設定	説明	値をここに記入
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>(vSAN または Virtual Volumes を使用しない場合にのみ使用可能) 容量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容量の最小量 (GB) を入力します。未使用ディスク容量がこのしきい値を超過すると、Horizon 7 は ESXi ホストに OS ディスク上の容量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、Horizon 7 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: <b>2 GB</b>。</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、『Horizon 7 での仮想デスクトップのセットアップ』の「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。</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)、[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 Horizon 7 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><b>注:</b> 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 の設定については、『Horizon 7 の管理』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: <b>CN=Computers</b></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>	

設定	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、『Horizon 7 での仮想デスクトップのセットアップ』の「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」を参照してください。</p>	
カスタマイズ仕様 (Sysprep) を使用	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。	

## Horizon Console での自動リンク クローン ファームの作成

公開アプリケーションまたは公開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、自動リンク クローン 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。『Horizon 7 のインストール』ドキュメントを参照してください。
- vCenter Server の View Composer が設定されていることを確認します。『Horizon 7 の管理』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。『Horizon 7 の管理』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 ファーム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。 [Horizon Console での自動リンク クローン 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 Horizon Console で、[インベントリ] - [ファーム] の順に選択します。
- 2 [追加] をクリックします。
- 3 [自動ファーム] を選択します。
- 4 [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、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。

Horizon Console で、[インベントリ] - [ファーム] の順に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

公開アプリケーション プールまたは公開デスクトップ プールを作成します。 [Horizon Console での公開デスクトップ プールの作成](#)または [Horizon Console でのアプリケーション プールの作成](#)を参照してください。

# Horizon Console での公開デスクトップ 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、公開デスクトップ プールを作成します。公開デスクトップ プールは、RDS ホストのファームで実行されます。このプロパティを使用すると、リモート デスクトップ環境の特定の要件を満たすことができます。

公開デスクトップ プールのプロパティの詳細については、『Horizon 7 での公開されたデスクトップとアプリケーションのセットアップ』ドキュメントを参照してください。

## 公開デスクトップ プール作成用のワークシート

RDS ホストのファームで実行される公開デスクトップ プールを作成するときに、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。これらは、公開デスクトップ プールに固有の設定です。

表 11-4. 公開デスクトップ プールの設定

設定	説明	デフォルト値
状態	<ul style="list-style-type: none"> <li>■ [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。</li> <li>■ [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。</li> </ul> <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>	有効
接続サーバの制限	<p>デスクトップ 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の制限を構成すると、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>	なし
カテゴリ フォルダ	Windows クライアント デバイスのデスクトップ プール資格に、スタート メニューのショートカットを含むカテゴリ フォルダの名前を指定します。	無効
クライアントの制限	<p>資格を付与されたデスクトップ プールへの特定のクライアント コンピュータからのアクセスを制限するかどうかを選択します。</p> <p>デスクトップ プールへのアクセスを許可するコンピュータの名前を Active Directory セキュリティ グループに追加する必要があります。デスクトップ プール資格にユーザーまたはグループを追加するときに、このセキュリティ グループを選択できます。</p>	無効

## Horizon Console での公開デスクトップ プールの作成

RDS ホストのファームで実行されるデスクトップへのアクセス権を付与するときに、公開デスクトップ 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。『Horizon 7 での公開されたデスクトップとアプリケーションのセットアップ』ドキュメントの「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。 [Horizon Console でのファームの作成](#)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。『Horizon 7 での公開されたデスクトップとアプリケーションのセットアップ』ドキュメントで「RDS デスクトップ プールのデスクトップ プールの設定」を参照してください。

## 手順

- 1 Horizon Console で、[インベントリ] - [デスクトップ] の順に選択します。
- 2 [追加] をクリックします。
- 3 [RDS デスクトップ プール] を選択して、[次へ] をクリックします。
- 4 プール ID、表示名、および説明を指定します。

プール ID は、Horizon 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。

## 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。

# Horizon Console でのアプリケーション 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タスクの 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。

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 ホストのファームまたはデスクトップ プールで実行されます。

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 プールには 1 つのアプリケーションがあり、1 つのファームまたはデスクトップ プールと関連付けられています。エラーを避けるため、ファームまたはデスクトップ プールのすべての 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。

Horizon 7 では、アプリケーション プールを作成すると、ファームまたはデスクトップ プールのすべての RDS ホストの [開始] 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、Horizon 7 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。公開アプリケーションとデスクトップ プールについては、ファームまたはデスクトップ プール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 PCoIP および VMware Blast 表示プロトコルをサポートします。HTML Access を有効にする方法については、『VMware Horizon HTML Access のインストールとセットアップ ガイド』ドキュメントを参照してください。

## Horizon Console でアプリケーション プールを手動で作成するためのワークシート

アプリケーション プールを作成してアプリケーションを手動で指定する場合、アプリケーションの情報を追加できます。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。

表 11-5. 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
RDS ファームまたはデスクトップ プールを選択	サポートされるセッション タイプが「アプリケーション」か「アプリケーションとデスクトップ」のデスクトップのリストから、ファームまたはデスクトップ プールを選択します。	
ID	Horizon 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。	
事前起動	<p>このオプションは、ユーザーが Horizon Client でアプリケーションを開く前にアプリケーション セッションを開始するように公開アプリケーションを設定する場合に選択します。公開アプリケーションを起動するときに、Horizon Client でより速くアプリケーションを開始できます。</p> <p>このオプションを有効にすると、Horizon Client からサーバーへの接続方法に関係なく、ユーザーが Horizon Client でアプリケーションを開く前に、構成済みのアプリケーション セッションが起動されます。</p> <p><b>注:</b> この設定は、デスクトップ プールに基づくアプリケーションではサポートされません。</p> <p><b>注:</b> アプリケーション ファームを追加または編集するときに [事前起動セッションのタイムアウト (アプリケーションのみ)] オプションが設定されていると、アプリケーション セッションが切断されます。</p>	

プロパティ	説明	値をここに記入
Connection Server の制限	<p>アプリケーション プールへのアクセスを特定の Connection Server に制限するには、[参照] をクリックして、1 台以上の Connection Server 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 Connection Server の制限を構成すると、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>	
カテゴリ フォルダ	<p>Windows クライアント デバイスのアプリケーション プール資格に、スタート メニューのショートカットを含むカテゴリ フォルダの名前を指定します。</p>	



プロパティ	説明	値をここに記入
-------	----	---------

クライアントの制限	<p>資格を付与されたアプリケーション プールへの特定のクライアント コンピュータからのアクセスを制限するかどうかを選択します。</p> <p>アプリケーション プールへのアクセスを許可するコンピュータの名前を Active Directory セキュリティ グループに追加する必要があります。アプリケーション プール資格にユーザーまたはグループを追加するときに、このセキュリティ グループを選択できます。</p>	
-----------	---	--

複数セッション モード	<p>公開アプリケーションのセッションは次のモードで開始できます。</p> <p>単一セッション：クライアント A でユーザーが公開アプリケーションを単一セッション モードで開き、クライアント B で同じ公開アプリケーションまたは同じファームの別の公開アプリケーションを開くと、クライアント A のセッションが切断し、クライアント B に再接続します。</p> <p>複数セッション：クライアント A でユーザーが公開アプリケーションを複数セッション モードで開き、クライアント B で同じ公開アプリケーションまたは同じファームの別の公開アプリケーションを開くと、クライアント A の公開アプリケーションは開いたまま、クライアント B で公開アプリケーションの新しいセッションが開きます。これらのセッションは切断時にログオフされます。複数セッション モードを有効にした場合、セッションの事前起動機能は有効にできません。</p> <p>複数セッション モードには、次の値を設定します。</p> <ul style="list-style-type: none"> <li>■ [無効] - 複数セッション モードはサポートされません。</li> <li>■ [有効 (デフォルトはオフ)] - 複数セッション モードはサポートされていますが、デフォルトで無効になっています。複数セッション モードを使用するには、Horizon Client 4.10 以降で、[マルチ起動] の設定を有効にする必要があります。Horizon Client の以前のバージョンを使用している場合、アプリケーションは常に単一セッション モードで起動します。</li> <li>■ [有効 (デフォルトはオン)] - 複数セッション モードはサポートされ、デフォルトで有効になっています。複数セッション モードを無効にするには、Horizon Client 4.10 以降で、[マルチ起動] の設定を無効にします。Horizon Client の以前のバージョンを使用している場合、アプリケーションは常に単一セッション モードで起動します。</li> <li>■ [有効 (適用)] - 複数セッション モードが常に有効になります。Horizon Client のどのバージョンでも、ユーザーはこれを無効にできません、アプリケーションは常に複数セッション モードで起動します。ユーザーが Horizon Client の以前のバージョンを使用している場合、「このアプリケーションは、要求された起動モードをサポートしていません。」というエラー メッセージが表示されます。</li> </ul> <p>複数セッション モードが有効になっている場合、[最大セッション数] も設定できます。これは、異なるクライアント デバイスから同じ公開アプリケーションを同時に開始できるセッションの最大数が設定されます。</p>	
-------------	---	--

## Horizon Console でのアプリケーション プールの作成

RDS ホストまたはデスクトップ プール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。『Horizon 7 での公開されたデスクトップとアプリケーションのセットアップ』ドキュメントの「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。 [Horizon Console でのファームの作成](#)を参照してください。
- 手動または自動デスクトップ プールを作成します。 [10 章 Horizon Console での仮想デスクトップ 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。 [Horizon Console でアプリケーション プールを手動で作成するためのワークシート](#)を参照してください。

### 手順

- 1 Horizon Console で、[インベントリ] - [アプリケーション] の順に選択します。
- 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。Horizon Console 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。

### 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。

公開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 Connection Server 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 プールにアンチアフィニティ ルールを設定します。

---

**注:** デスクトップ プールで実行されるアプリケーションの場合、アンチアフィニティ ルールはフローティング デスクトップ プールから作成されたアプリケーションでのみサポートされます。専用デスクトップ プールから作成されたアプリケーションではサポートされません。

---

[Horizon Console で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。

## Horizon Console で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

アプリケーション プールのアンチアフィニティ ルールを構成すると、Horizon 接続サーバはアプリケーションを実行するのに十分なリソースを持つ RDS ホストのみでアプリケーションを起動するように試みます。この機能は、大量の CPU またはメモリ リソースを消費するアプリケーションを制御するのに役立ちます。

アンチアフィニティ ルールは、アプリケーション一致パターンと最大数で構成されます。たとえば、アプリケーション一致パターンは `autocad.exe` で最大数は 2 の可能性があります。

接続サーバは、RDS ホスト上の Horizon Agent にアンチアフィニティ ルールを送信します。プロセス名がアプリケーション一致パターンと同じであるアプリケーションが RDS ホストで実行されている場合、Horizon Agent はこれらのアプリケーションのインスタンスの現在数を数え、その数を最大数と比較します。最大数を超えた場合、接続サーバは RDS ホストの選択時にその RDS ホストをスキップしてアプリケーションの新規セッションを実行します。

#### 前提条件

- アプリケーション プールを作成します。[Horizon Console でのアプリケーション プールの作成](#)を参照してください。
- アンチアフィニティ機能の制約についてよく理解します。[アンチアフィニティ機能の制約](#)を参照してください。

#### 手順

- 1 Horizon Console で、[インベントリ] - [アプリケーション] の順に選択します。
- 2 変更するプールを選択し、[編集] をクリックします。
- 3 [アンチアフィニティ パターン] テキスト ボックスに、RDS ホストで実行されている他のアプリケーションのプロセス名に一致するパターンのカンマ区切りリストを入力します。

パターン文字列には、アスタリスク (\*) と疑問符 (?) をワイルドカード文字として含むことができます。アスタリスクは 0 文字以上に一致し、疑問符は任意の 1 文字に一致します。

たとえば、**\*pad.exe, \*notepad.???** は `wordpad.exe`、`notepad.exe`、および `notepad.bat` に一致しますが、`wordpad.bat` または `notepad.script` には一致しません。

---

**注:** Horizon 7 は、1 つのセッションのアプリケーションについて一致する複数のパターンを 1 つの一致としてカウントします。

---

- 4 [アンチアフィニティの数] テキスト ボックスに、RDS ホストが新しいアプリケーション セッションについて拒否されるまでに RDS ホストで実行できる他のアプリケーションの最大数を入力します。

最大数は 1 から 20 までの整数です。

- 5 [送信] をクリックして、変更を保存します。

### アンチアフィニティ機能の制約

アンチアフィニティ機能には一定の制約があります。

- アンチアフィニティ ルールは、新規のアプリケーション セッションにのみ影響を及ぼします。ユーザーが以前にアプリケーションを実行したセッションが含まれる RDS ホストは、必ず同じアプリケーションで再利用されます。この動作は、レポートされるロード設定およびアンチアフィニティ ルールに優先します。
- アンチアフィニティ ルールは、RDS デスクトップ セッション内からのアプリケーションの起動には影響を及ぼしません。
- RDS セッションの制限により、アンチアフィニティ ルールに関係なく、アプリケーション セッションを作成できなくなります。

- 特定の状況では、RDS ホストにおけるアプリケーションのインスタンスが指定した最大数に制約されない場合があります。たとえば、他の保留中のセッションの他のアプリケーションが起動中の場合、Horizon 7 は正確なインスタンス数を判断できません。
- アプリケーション間のアンチアフィニティ ルールはサポートされません。たとえば、Autocad や Visual Studio インスタンスなどの大規模なアプリケーション クラスは 1 つのルールではカウントできません。
- エンドユーザーがモバイル クライアントで Horizon Client を使用する環境では、アンチアフィニティ ルールを使用しないでください。アンチアフィニティ ルールにより、エンド ユーザーの同一ファーム内で複数のセッションが開始されることがあります。モバイル クライアントで複数のセッションに再接続すると、動作が不安定になる場合があります。
- アンチアフィニティ ルールでは、ロード バランシングのセッション接続数のみが考慮されます。ただし、RDS ホストのロード バランシングでは、ロード バランシングで接続中のセッション数、保留中のセッション数、切断されたセッション数の合計が考慮されます。

## Horizon Console でのファームの管理

Horizon Console で、ファームを追加、編集、削除、有効、無効にできます。

ファームの作成後、RDS ホストを追加または削除して、サポートするユーザーを増やしたり減らしたりできます。

## Horizon Console でのファームの編集

既存のファームの設定を変更できます。

### 前提条件

ファームの設定を理解します。

### 手順

- 1 Horizon Console で、[インベントリ] - [ファーム] の順に選択します。
- 2 ファームを選択し、[編集] をクリックします。
- 3 ファームの設定を変更します。
- 4 [OK] をクリックします。

## Horizon Console でのファームの削除

ファームがなくなっただけの場合、または別の RDS ホストで新しいファームを作成する場合、ファームを削除できます。削除できるのは、公開デスクトップ プールまたはアプリケーション プールに関連付けられていないファームのみです。

### 前提条件

ファームが公開デスクトップ プールまたはアプリケーション プールに関連付けられていないことを確認します。

### 手順

- 1 Horizon Console で、[インベントリ] - [ファーム] の順に選択します。

- 2 1 つ以上のファームを選択し、[削除] をクリックします。
- 3 [OK] をクリックして確定します。

## Horizon Console でのファームの無効化または有効化

ファームを無効化すると、ファームに関連付けられている公開デスクトップ プールやアプリケーション プールから公開デスクトップまたはアプリケーションを起動できなくなります。ユーザーは現在開いているアプリケーションと公開デスクトップを引き続き使用できます。

ファーム内の RDS ホストまたはファームに関連付けられている公開デスクトップ プールやアプリケーション プールでメンテナンスを行う計画がある場合は、ファームを無効化できます。ファームを無効化した後、一部のユーザーが、ファームを無効化する前に開いた公開デスクトップ プールまたはアプリケーションをまだ使用していることがあります。

### 手順

- 1 Horizon Console で、[インベントリ] - [ファーム] の順に選択します。
- 2 1 つ以上のファームを選択して [その他のコマンド] をクリックします。
- 3 [有効化] または [無効化] をクリックします。
- 4 [OK] をクリックして確定します。

プールのステータスを表示するには、[インベントリ] - [デスクトップ] の順に選択するか、[インベントリ] - [アプリケーション] の順に選択します。

## Horizon Console での自動インスタント クローン ファームのメンテナンス スケジュール

メンテナンス操作で、自動インスタントクローン ファームのすべての RDS ホストに定期的または即時メンテナンスをスケジュールリングできます。各メンテナンス サイクル中に、すべての RDS ホストが親仮想マシンから更新されます。

メンテナンスでは現在の親仮想マシンのスナップショットが使用されるため、RDS ホストのインスタント クローンに影響を及ぼさずに親仮想マシンに変更を行うことができます。自動ファームに作成されたインスタント クローンは、システム構成に親仮想マシンの情報を使用します。

自動ファームのメンテナンスをスケジュールリングすることはできますが、ファーム内の RDS ホストに個別にスケジュールリングすることはできません。

可能であれば、オフピーク時にメンテナンス操作を実行し、ピーク時にすべての RDS ホストが使用可能な状態になっているようにスケジュールリングしてください。

### 前提条件

- メンテナンス操作のスケジュールを決定します。デフォルトでは、接続サーバはすぐに操作を開始します。  
ファームには、即時メンテナンス、定期的なメンテナンスまたはその両方のスケジュールを設定できます。メンテナンス操作のスケジュールは、複数のファームに同時に設定できます。

- メンテナンス操作の開始後すぐにすべてのユーザーを強制的にログオフさせるか、各ユーザーがログオフしてからそのユーザーのマシンを更新するのかを決定します。

ユーザーを強制的にログオフさせる場合、Horizon 7 は切断する前にユーザーに通知するため、ユーザーはアプリケーションを閉じてログオフすることができます。

- ファームの最小サイズを決定します。ファームの最小サイズは、ユーザーがファームの使用を継続できるように常に使用可能にしておく RDS ホスト数です。たとえば、ファーム サイズが 10 で、最小サイズが 2 の場合、メンテナンスは 8 個の RDS ホストに実行されます。各 RDS ホストが再度使用可能になると、別のホストでメンテナンスが実行されます。すべての RDS ホストは個別に管理されます。1 台のホストが使用可能になると、残りのホストの 1 つでメンテナンスが実行されます。

ただし、即時メンテナンスをスケジュールリングした場合には、ファームのすべての RDS ホストでメンテナンスが実行されます。

すべての RDS ホストにポリシーが適用されます。設定したポリシーに応じて、ユーザーのログオフを待機するか、ユーザーを強制的にログオフします。

- 最初のエラーでプロビジョニングを停止するかどうかを決定します。このオプションを選択した場合、接続サーバがインスタント クローンをプロビジョニング中にエラーが発生すると、プロビジョニングが停止します。このオプションを選択することにより、ストレージなどのリソースが不必要に消費されるのを防ぐことができます。

[最初のエラーで停止] オプションを選択しても、カスタマイズには影響を与えません。インスタント クローン上でカスタマイズ エラーが発生しても、他のクローンのプロビジョニングとカスタマイズは続行されます。

- そのプロビジョニングが有効になっていることを確認します。プロビジョニングが無効の場合、Horizon 7 は、マシンが更新後にカスタマイズされないようにします。
- レプリケートされた接続サーバ インスタンスが展開環境内に含まれる場合は、すべてのインスタンスが同一バージョンであることを確認します。

#### 手順

- 1 Horizon Console で、[インベントリ] - [ファーム] の順に選択します。
- 2 メンテナンスをスケジュールリングするファームのプール ID をクリックします。
- 3 [メンテナンス] - [スケジュール] の順にクリックします。

## 4 [定期的なメンテナンスのスケジュール] ウィザードで、メンテナンス モードを選択します。

オプション	アクション
[定期的]	<p>ファーム内にあるすべての RDS ホスト サーバに定期的メンテナンスをスケジュールリングします。</p> <ul style="list-style-type: none"> <li>■ メンテナンスが有効になる日付と時刻を選択します。</li> <li>■ メンテナンス期間を選択します。メンテナンス期間には、毎日、毎月または毎週を選択できます。</li> <li>■ メンテナンス操作の繰り返し期間を日数で選択します。</li> </ul> <p>ファームで即時メンテナンスがスケジュールリングされている場合、即時メンテナンスの日付が定期的メンテナンスの有効日になります。即時メンテナンスをキャンセルすると、現在の日付が定期的メンテナンスの有効日になります。</p>
[直後]	<p>ファーム内にあるすべての RDS ホスト サーバに即時メンテナンスをスケジュールリングします。即時メンテナンスの場合、即時または近い将来実施する 1 回のメンテナンスをスケジュールリングできます。即時メンテナンスは、緊急のセキュリティ パッチを適用するために、新しい親仮想マシン イメージまたはスナップショットを使用してファームを更新する場合に実施します。</p> <p>即時メンテナンスの構成を選択します。</p> <ul style="list-style-type: none"> <li>■ メンテナンス操作をすぐに開始するには、[今すぐ開始] を選択します。</li> <li>■ メンテナンス操作を近い将来に実施するには、[開始日時] を選択します。日付と Web ブラウザのローカル時刻を入力します。</li> </ul> <p><b>注:</b> 即時メンテナンスが完了するまで、定期的メンテナンスは延期されます。</p>

5 [次へ] をクリックします。

6 (オプション) [変更] をクリックし、親仮想マシンを変更します。

7 スナップショットを選択します。

[現在の親仮想マシン イメージを使用] チェックボックスをオフにするまで、別のスナップショットは選択できません。

8 (オプション) [スナップショットの詳細] をクリックすると、スナップショットに関する詳細が表示されます。

9 [次へ] をクリックします。

10 (オプション) ユーザーを強制的にログオフさせるのか、ユーザーがログオフするのを待つのかを指定します。

デフォルトでは、ユーザーを強制的にログオフさせるオプションが選択されています。

11 (オプション) 最初にエラーが発生したときにプロビジョニングを停止するかどうかを指定します。

このオプションはデフォルトで選択されています。

12 [次へ] をクリックします。

[設定内容の確認] ページが表示されます。

13 [終了] をクリックします。

## Horizon Console でのアプリケーション プールの管理

Horizon Console でアプリケーション プールの追加、編集、削除、またはアプリケーション プールへの資格付与を行うことができます。

### Horizon Console でのアプリケーション プールの編集

既存のアプリケーション プールを編集して、表示名、バージョン、パブリッシャ、パス、開始フォルダ、パラメータ、説明などの設定を構成できます。アプリケーション プールの ID やアクセス グループは変更できません。

#### 前提条件

- アプリケーション プールの設定について理解しておきます。
- 接続サーバがアプリケーションの実行に必要なリソースを持つ RDS ホストでのみアプリケーションを起動するため、アンチアフィニティ ルールの構成が必要になる場合があります。

#### 手順

- 1 Horizon Console で、[インベントリ] - [アプリケーション] の順に選択します。
- 2 プールを選択し、[編集] をクリックします。
- 3 プールの設定を変更します。
- 4 [OK] をクリックします。

### Horizon Console でのアプリケーション プールの削除

アプリケーション プールを削除すると、ユーザーはプール内のアプリケーションを起動できなくなります。

ユーザーが現在アプリケーションにアクセスしていても、アプリケーション プールを削除できます。ユーザーがアプリケーションを終了した後は、アプリケーションにアクセスできなくなります。

#### 手順

- 1 Horizon Console で、[インベントリ] - [アプリケーション] の順に選択します。
- 2 1 つ以上のアプリケーション プールを選択して [削除] をクリックします。
- 3 [OK] をクリックして確定します。

### 公開アプリケーションのアイコンの変更

エンドユーザーの公開アプリケーションのアイコンをカスタマイズできます。公開アプリケーションのアイコンを変更すると、エンドユーザーの公開デスクトップに新しいアプリケーション アイコンが表示されます。

#### 前提条件

- アイコンが .PNG 形式になっていることを確認します。

#### 手順

- 1 Horizon Console で、[インベントリ] - [アプリケーション] の順に選択します。



- 2 1つまたは複数のアプリケーション プールを選択して、[アプリケーション アイコン] - [アプリケーション アイコンの関連付け] の順にクリックします。
- 3 アイコンをアップロードするには、[アイコン ファイルのアップロード] をクリックして、.PNG 形式のアイコンを選択します。

アイコン ファイルは、16 x 16 ピクセルから 256 x 256 ピクセルの間にする必要があります。

- 4 [OK] をクリックします。

公開デスクトップに公開アプリケーションのアイコンが表示されます。

## 公開アプリケーションのアイコンの削除

公開アプリケーションのアイコンを削除して、別のアイコンに置き換えることができます。公開アプリケーションのアイコンを削除すると、公開アプリケーションは公開デスクトップのデフォルトのアイコンに置き換えられます。すべての公開アプリケーションで同じアイコンが使用されている場合にのみ、複数の公開アプリケーションからアイコンを削除できます。異なるアイコンの公開アプリケーションを複数選択して、アイコンを削除することはできません。

### 手順

- 1 Horizon Console で、[インベントリ] - [アプリケーション] の順に選択します。
- 2 1つまたは複数のアプリケーション プールを選択して、[アプリケーション アイコン] - [アプリケーション アイコンの削除] の順にクリックします。

公開アプリケーションは、公開デスクトップのデフォルトのアイコンに置き換えられます。

## Horizon Console での RDS ホストの管理

手動で設定した RDS ホストと、自動ファームの追加時に自動的に作成された RDS ホストを管理できます。

RDS ホストを手動で設定すると、設定した RDS ホストは自動的に Horizon 接続サーバに登録されます。RDS ホストを接続サーバに手動で登録することはできません。手動で設定した RDS ホストに対しては、以下の管理タスクを実行できます。

- RDS ホストを編集する。
- 手動ファームに RDS ホストを追加する。
- ファームから RDS ホストを削除する。
- RDS ホストを有効にする。
- RDS ホストを無効にする。

自動ファームの追加時に自動的に作成された RDS ホストに対しては、以下の管理タスクを実行できます。

- ファームから RDS ホストを削除する。
- RDS ホストを有効にする。
- RDS ホストを無効にする。

## Horizon Console での RDS ホストの編集

RDS ホストでサポートできる接続数を変更できます。この設定は、変更可能な唯一の設定です。デフォルト値は 150 で、任意の正の数値または無制限に設定できます。

編集できる RDS ホストは、手動で設定したものに限られます。自動ファーム内の RDS ホストは編集できません。

### 手順

- 1 Horizon Console で、[設定] - [登録済みのマシン] の順に選択します。
- 2 RDS ホストを選択し、[編集] をクリックします。
- 3 [接続数] 設定の値を指定します。
- 4 [OK] をクリックします。

## Horizon Console で手動ファームに RDS ホストを追加する

ファームの規模を拡大するなどの理由で、手動で設定した RDS ホストを手動ファームに追加することができます。RDS ホストは手動ファームにしか追加できません。

### 手順

- 1 Horizon Console で、[インベントリ] - [ファーム] の順に選択します。
- 2 ファーム ID をクリックします。
- 3 [RDS ホスト] タブを選択します。
- 4 [追加] をクリックします。
- 5 1 つ以上の RDS ホストを選択します。
- 6 [OK] をクリックします。

## Horizon Console でのファームからの RDS ホストの削除

手動ファームの規模の縮小、RDS ホストのメンテナンスの実行などの理由で、手動ファームから RDS ホストを削除できます。ベスト プラクティスとして、ホストをファームから削除する前に、RDS ホストを無効にしてユーザーがアクティブなセッションからログオフしていることを確認します。

削除するホスト上にユーザーのアプリケーション セッションやデスクトップ セッションがある場合、セッションはアクティブなままですが、Horizon 7 はセッションをトラッキングしません。セッションから切断されたユーザーは再度接続することができず、未保存のデータが失われることがあります。

自動ファームから RDS ホストを削除することもできます。考えられる理由の 1 つは、RDS ホストが回復不能なエラー状態にあることです。

### 手順

- 1 Horizon Console で、[インベントリ] - [ファーム] の順に選択します。
- 2 ファーム ID をクリックします。
- 3 [RDS ホスト] タブを選択します。

- 4 1 つ以上の RDS ホストを選択します。
- 5 [ファームから削除] をクリックします。
- 6 [OK] をクリックします。

## Horizon 7 からの RDS ホストの削除

手動で設定し、使用する予定がなくなった RDS ホストは、Horizon 7 から削除できます。現在、手動ファームには、このような RDS ホストは存在してはなりません。

### 前提条件

RDS ホストがファームに属していないことを確認します。

### 手順

- 1 Horizon Console で、[設定] - [登録済みのマシン] の順に選択します。
- 2 RDS ホストを選択し、[削除] をクリックします。
- 3 [OK] をクリックします。

RDS ホストを削除した後、その RDS ホストを再び使用するには、Horizon Agent を再インストールする必要があります。

## Horizon Console での RDS ホストの無効化または有効化

RDS ホストを無効化すると、Horizon 7 により新しい公開デスクトップまたはアプリケーションをホストするのに使用されなくなります。ユーザーは現在開いているアプリケーションと公開デスクトップを引き続き使用できます。

### 手順

- 1 Horizon Console で、[インベントリ] - [ファーム] の順に選択します。
- 2 ファーム ID をクリックします。
- 3 [RDS ホスト] タブを選択します。
- 4 RDS ホストを選択し、[その他のコマンド] をクリックします。
- 5 [有効化] または [無効化] をクリックします。
- 6 [OK] をクリックします。

RDS ホストを有効化すると、[有効] 列にチェックマークが表示され、[ステータス] 列に [使用可能] が表示されます。RDS ホストを無効化すると、[有効] 列は空白で、[ステータス] 列に [無効] が表示されます。

## Horizon Console での RDS ホストのモニタリング

Horizon Console で RDS ホストのステータスをモニタリングし、プロパティを表示できます。

## 手順

- ◆ Horizon Console で、必要なプロパティが表示されるページへ移動します。

プロパティ	アクション
DNS 名、タイプ、イメージ、保留中のイメージ、タスク、最大接続数、セッション、エージェントバージョン、有効、ステータス	<ul style="list-style-type: none"> <li>■ Horizon Console で、[インベントリ] - [ファーム] の順に選択します。</li> <li>■ ファームを選択して、[RDS ホスト] タブをクリックします。</li> </ul>
RDS ホスト、ファーム、デスクトップ プール、エージェントバージョン、セッション、ステータス	<ul style="list-style-type: none"> <li>■ Horizon Console で、[インベントリ] - [マシン] の順に選択します。</li> <li>■ [RDS ホスト] タブをクリックします。</li> </ul>
DNS 名、タイプ、RDS ファーム、接続の最大数、セッション、エージェントバージョン、有効、ステータス	<ul style="list-style-type: none"> <li>■ Horizon Console で、[設定] - [登録済みのマシン] の順に選択します。</li> <li>■ [RDS ホスト] タブをクリックします。</li> </ul>

表示されるプロパティには、次の意味があります。

プロパティ	説明
RDS ホスト	RDS ホスト名。
ファーム	RDS ホストが属しているファーム。
デスクトップ プール	ファームに関連付けられている公開デスクトップ プール。
エージェントバージョン	RDS ホストで実行される Horizon Agent のバージョン。
セッション	クライアント セッション数。
DNS 名	RDS ホストの DNS 名。
Type	RDS ホストで実行される Windows Server のバージョン。
RDS ファーム	RDS ホストが属しているファーム。
イメージ	ファームの RDS ホストのイメージ。
保留中イメージ	ファーム上の RDS ホストの保留中のイメージ。
タスク	ファームの RDS ホストで実行されているタスク。
接続の最大数	RDS ホストでサポートされる接続の最大数。
有効	RDS ホストが有効になっているか。
ステータス	RDS ホストの状態。取りうる状態の説明は、 <a href="#">Horizon Console での RDS ホストのステータス</a> を参照してください。

## Horizon Console での RDS ホストのステータス

RDS ホストは、初期化された時点からその状態がさまざまに変化します。ベスト プラクティスとして、RDS ホストに対してタスクの実行や操作を行う前と後に、それらのホストが予期される状態にあるかをチェックします。

表 11-6. RDS ホストのステータス

ステータス	説明
スタートアップ	Horizon Agent は RDS ホスト上で起動されましたが、表示プロトコルなどの他の必要なサービスがまだ起動中です。エージェントの起動期間に、プロトコル サービスなどの他のプロセスも起動できます。
無効化が進行中	ホストでセッションがまだ実行されているときに RDS ホストの無効化が進行しています。セッションが終了する時点でステータスは無効に変わります。
無効	RDS ホストの無効化プロセスが完了しています。
検証しています	接続サーバが初めて RDS ホストを認識した後（一般に接続サーバが起動または再起動した後）と、RDS ホスト上の Horizon Agent との初めての正常な通信の前に発生します。通常、この状態は一時的なものです。この状態は、通信の問題を示すエージェントに到達できない状態と同じではありません。
エージェントが無効です	接続サーバが Horizon Agent を無効にすると発生します。この状態では、新しいデスクトップまたはアプリケーション セッションが RDS ホストで起動できません。
エージェントに到達できません	接続サーバは、RDS ホスト上の Horizon Agent と通信を確立できません。
無効な IP	サブネット マスク レジストリ設定は RDS ホストで構成され、構成された範囲内に IP アドレスを持つアクティブ ネットワーク アダプタは存在しません。
エージェントを再起動する必要があります	Horizon 7 コンポーネントがアップグレードされました。RDS ホストを再起動して、アップグレードされたコンポーネントで操作することを Horizon Agent に許可する必要があります。
プロトコル障害	RDP 表示プロトコルが正常に動作していません。RDP が動作しておらず、PCoIP が動作している場合、クライアントは RDP または PCoIP を使用して接続できません。ただし、RDP が動作し、PCoIP が動作していない場合、クライアントは RDP を使用して接続できます。
ドメイン障害	RDS ホストでドメインへの到達の問題が発生しました。ドメイン サーバがアクセス可能でないか、ドメイン認証が失敗しました。
構成エラー	サーバで RDS ロールが有効になっていません。
不明	RDS ホストは不明な状態にあります。
使用可能	RDS ホストは使用可能な状態です。ホストがファーム内に存在し、そのファームが公開デスクトップまたはアプリケーション プールと関連付けられている場合、ホストは公開デスクトップまたはアプリケーションをユーザーに配布するために使用されます。

## Horizon Console での公開デスクトップ セッションとアプリケーション セッションの管理

ユーザーが公開デスクトップまたはアプリケーションを起動すると、セッションが作成されます。管理者は、セッションの切断とログオフ、クライアントへのメッセージの送信、仮想マシンのリセットと再起動などを行うことができます。

## 手順

- 1 Horizon Console で、セッション情報が表示される場所に移動します。

セッションのタイプ	ナビゲーション
リモート デスクトップ セッション	<p>[インベントリ] - [デスクトップ] の順に選択し、プール ID をクリックして [セッション] タブをクリックします。[セッション] 列は、すべてのデスクトップの [デスクトップ プール] ページに表示されます。</p> <p>[インベントリ] - [ファーム] の順に選択し、ファーム ID をクリックして [セッション] タブをクリックします。[セッション] 列は、すべてのデスクトップの [ファーム] ページに表示されます。</p> <p>[設定] - [登録済みのマシン] の順に選択し、[セッション] 列を表示します。</p>
リモート 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	[監視] - [セッション] の順に選択します。
ユーザーまたはユーザー グループに関連付けられたセッション	<ul style="list-style-type: none"> <li>■ [ユーザーとグループ] を選択します。</li> <li>■ ユーザーの名前またはユーザー グループの名前をクリックします。</li> <li>■ [セッション] タブをクリックします。</li> </ul>

- 2 セッションを選択します。

ユーザーにメッセージを送信する場合、複数のセッションを選択できます。その他の操作は、一度に 1 つのセッションでのみ実行できます。ログオフ操作は、vSphere コンソールから接続していないセッションでのみ実行できます。

- 3 切断、ログオフ、メッセージの送信、デスクトップの再起動、仮想マシンのリセットのうち、いずれかの操作を選択します。

オプション	説明
セッションを切断	ユーザーをセッションから切断します。
Logoff Session (セッションのログオフ)	ユーザーをセッションからログオフさせます。保存されていないデータは失われます。
メッセージを送信	Horizon Client にメッセージを送信します。メッセージに、[情報]、[警告]、または [エラー] のラベルを付けることができます。
デスクトップの再起動	仮想デスクトップで再起動操作を実行すると、仮想マシンのオペレーティング システムのグレースフル再起動が実行されます。
仮想マシンをリセット	仮想マシンでリセット操作を実行すると、オペレーティング システムのグレースフル再起動は実行されず、仮想マシンのパワーオフとパワーオンが即時実行されます。

- 4 [OK] をクリックします。

# Horizon Console でユーザーとグループに資格を付与する

# 12

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 Horizon Connection Server 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 デスクトップや公開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。

クラウド ポッド アーキテクチャ 環境でグローバル資格を設定する方法については、『Horizon 7 でのクラウド ポッド アーキテクチャの管理』を参照してください。

---

**注:** 手動プールまたはリンク クローンデスクトップ プールに資格の追加、削除、確認を行うことはできません。

---

この章には、次のトピックが含まれています。

- [Horizon Console での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](#)
- [Horizon Console での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](#)
- [資格のあるプールのショートカットの設定](#)
- [デスクトップとアプリケーション プールへのクライアント制限の実装](#)

## Horizon Console での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	アクション
デスクトップ プールに対する資格の追加	Horizon Console で、[インベントリ] - [デスクトップ] の順に選択し、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 プールに対する資格の追加	Horizon Console で、[インベントリ] - [アプリケーション] の順に選択し、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:** 非認証アクセスのユーザーは、検索結果から除外されます。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。

## Horizon Console での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	アクション
デスクトップ プールに対する資格の追加	Horizon Console で、[インベントリ] - [デスクトップ] の順に選択し、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 プールに対する資格の追加	Horizon Console で、[インベントリ] - [アプリケーション] の順に選択し、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 Horizon Console 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	アクション
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	[デスクトップに対する資格] 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	[アプリケーションに対する資格] をクリックします。

## 資格のあるプールのショートカットの設定

資格のあるプールにショートカットを設定できます。資格のあるユーザーが Windows クライアントから接続サーバ インスタンスに接続すると、Horizon Client for Windows によりユーザーのクライアント デバイスのスタートメニューやデスクトップにこれらのショートカットが配置されます。プールを作成または変更する際に、ショートカットを設定できます。

ショートカットを設定するときに、カテゴリ フォルダまたはルート (/) フォルダを選択する必要があります。カテゴリ フォルダを追加し、独自の名前を付けることもできます。最大で 4 つのフォルダ レベルを設定できます。たとえば、Office をという名前のカテゴリ フォルダを追加し、そのフォルダを Microsoft Office や Microsoft PowerPoint など、仕事に関連するアプリケーション用に選択できます。

Windows 7 クライアント デバイスのスタート メニュー ショートカットの場合、Horizon Client によりスタート メニューの VMware アプリケーション フォルダ内にカテゴリ フォルダとショートカットが配置されます。ショートカットにルート (/) フォルダを選択した場合、Horizon Client は VMware Applications フォルダの直下にショートカットを配置します。Windows 8 および Windows 10 クライアント デバイスの場合、Horizon Client は、カテゴリ フォルダとショートカットをアプリケーション リストに配置します。ショートカットにルート (/) フォルダを選択した場合、Horizon Client はアプリケーション リストの直下にショートカットを配置します。

ショートカットの作成後、Horizon Administrator と Horizon Console でプールの [アプリのショートカット] 列にチェック マークが表示されます。

デフォルトでは、資格のあるユーザーが最初にサーバに接続したときに、Horizon Client for Windows はプロンプトを表示し、ショートカットをインストールするように指示します。[Horizon Server の設定時にショートカットを自動的にインストールする] グループ ポリシー設定を変更すると、ショートカットを自動的にインストールしたり、ショートカットをインストールしないように Horizon Client for Windows を設定できます。詳細については、『VMware Horizon Client for Windows のインストールとセットアップ ガイド』を参照してください。

デフォルトでは、ユーザーがサーバに接続するたびに、ショートカットに対する変更がユーザーの Windows クライアント デバイスと同期されます。Windows ユーザーは、Horizon Client でショートカット同期機能を無効にできます。詳細については、『VMware Horizon Client for Windows のインストールとセットアップ ガイド』を参照してください。

この機能を Windows で使用するには、クライアント システムに Horizon Client for Windows 4.6 以降が必要です。この機能を Mac で使用するには、クライアント システムに Horizon Client for Mac 4.10 以降が必要です。

グローバル資格を作成または変更する際にもショートカットを設定できます。グローバル資格の設定方法については、『Horizon 7 でのクラウド ポッド アーキテクチャの管理』を参照してください。

## Horizon Console でのデスクトップ プールのショートカットの作成

Horizon Console では、使用資格のあるデスクトップ プールのショートカットを作成できます。ショートカットを作成すると、ユーザーの Windows クライアント デバイスの Windows デスクトップ、Windows の [スタート] メニューまたはその両方デスクトップ プールが表示されます。ショートカットには最大 4 つのカテゴリ フォルダ レベルを指定できます。デスクトップ プールを作成するときに、ショートカットを作成できます。デスクトップ プールを編集するときにも、ショートカットを作成したり、変更できます。

### 前提条件

作成するデスクトップ プールのタイプに基いてプールの設定方法を決定します。

### 手順

- 1 Horizon Console で、[インベントリ] - [デスクトップ] の順にクリックし、[追加] をクリックします。
- 2 [プールを追加] ウィザードで、作成するデスクトップ プールのタイプを選択し、[次へ] をクリックします。
- 3 ウィザードの指示に従い、[デスクトップ プールの設定] ページに移動します。
- 4 デスクトップ プールにショートカットを作成します。

- a [カテゴリ フォルダ] の [参照] ボタンをクリックします。
- b [フォルダ リストからカテゴリ フォルダを選択してください] オプションを選択します。
- c [カテゴリ フォルダを選択してください。あるいは、クライアント デバイスに新しいフォルダを作成して、このプールのショートカットを配置してください] テキスト ボックスにフォルダ名を入力します。

フォルダ名の長さは最大 64 文字です。サブフォルダを指定するには、バックスラッシュ (\) 文字を入力します。たとえば、dir1\dir2\dir3\dir4 と入力します。最大で 4 つのフォルダ レベルを入力できます。フォルダ名の先頭または末尾にバックスラッシュは使用できません。また、バックスラッシュを重ねて使用することもできません。たとえば、\dir1、dir1\dir2\、dir1\\dir2、dir1\\\dir2 は無効です。Windows の予約キーワードは入力できません。

- d ショートカットの作成方法を選択します。

いずれか、または両方を選択できます。

オプション	説明
スタート メニュー/ランチャー	Windows クライアント デバイスに Windows のスタート メニューのショートカットを作成します。
デスクトップ	Windows クライアント デバイスのデスクトップにショートカットを作成します。

- e 変更内容を保存するには、[送信] をクリックします。
- 5 ウィザードの指示に従って [設定内容の確認] ページに移動し、[このウィザードの終了後にユーザーに資格を割り当てる] を選択して [送信] をクリックします。

- 6 [資格を追加] ウィザードで [追加] をクリックして、1 つ以上の検索条件を選択します。[検索] をクリックして、条件に一致するユーザーまたはグループを検索します。プール内のデスクトップの使用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。

[デスクトップ プール] ページで、デスクトップ プールの [アプリケーション ショートカット] 列にチェック マークが表示されます。

## Horizon Console でのアプリケーション プールのショートカットの作成

Horizon Console では、使用資格のあるアプリケーションのショートカットを作成できます。ショートカットを作成すると、ユーザーの Windows クライアント デバイスの Windows デスクトップ、Windows [スタート] メニューまたはその両方にショートカットが表示されます。ショートカットには最大 4 つのカテゴリ フォルダ レベルを指定できます。アプリケーション プールを作成するときに、ショートカットを作成できます。アプリケーション プールを編集するときにも、ショートカットを作成できます。

Mac クライアントで、ローカル システムの アプリケーション フォルダから公開アプリケーションを実行し、サーバからフォルダ設定を許可するように Horizon Client for Mac が設定されている場合、カテゴリ フォルダが Mac クライアント デバイスの アプリケーション フォルダに表示されます。詳細については、『VMware Horizon Client for Mac のインストールとセットアップ ガイド』を参照してください。

### 前提条件

- RDS ホストをセットアップします。『Horizon 7 でのデスクトップ プールとアプリケーション プールの設定』ドキュメントの「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。 [Horizon Console でのファームの作成](#)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。 [Horizon Console でアプリケーション プールを手動で作成するためのワークシート](#)を参照してください。
- クライアント デバイスに Horizon Client for Windows 4.6 以降をインストールします。

### 手順

- 1 Horizon Console で、[インベントリ] - [アプリケーション] の順にクリックし、[追加] をクリックします。
- 2 作成するアプリケーション プールのタイプを選択します。

オプション	説明
[アプリケーション プールを手動で追加]	アプリケーションの情報を入力します。 <a href="#">Horizon Console でアプリケーション プールを手動で作成するためのワークシート</a> を参照してください。
[インストールされているアプリケーションを選択]	アプリケーションを名前、インストール パスまたは種類でフィルタリングするか、インストール済みのアプリケーションのリストから選択します。他のオプションの設定方法については、 <a href="#">Horizon Console でアプリケーション プールを手動で作成するためのワークシート</a> を参照してください。

- 3 [アプリケーション プールを追加] ウィザードで、RDS ファームを選択して、プール ID とアプリケーションのフルパス名を入力します。

#### 4 アプリケーション プールのショートカットを作成します。

- a [カテゴリ フォルダ] の [参照] ボタンをクリックします。
- b [フォルダ リストからカテゴリ フォルダを選択してください] オプションを選択します。
- c リストからカテゴリ フォルダを選択するか、[カテゴリ フォルダを選択してください。あるいは、クライアント デバイスに新しいフォルダを作成して、このプールのショートカットを配置してください] テキスト ボックスにフォルダ名を入力します。

フォルダ名の長さは最大 64 文字です。サブフォルダを指定するには、バックスラッシュ (\) 文字を入力します。たとえば、dir1\dir2\dir3\dir4 と入力します。最大で 4 つのフォルダ レベルを入力できます。フォルダ名の先頭または末尾にバックスラッシュは使用できません。また、バックスラッシュを重ねて使用することもできません。たとえば、\dir1、dir1\dir2\、dir1\\dir2、dir1\\\dir2 は無効です。Windows の予約キーワードは入力できません。

**注:** Windows 以外のクライアントの場合、必要に応じてバックスラッシュをスラッシュに置き換えてください。

- d ショートカットの作成方法を選択します。

いずれか、または両方を選択できます。

オプション	説明
スタート メニュー/ランチャー	Windows クライアント デバイスに Windows のスタート メニューのショートカットを作成します。
デスクトップ	Windows クライアント デバイスのデスクトップにショートカットを作成します。

- e 変更内容を保存するには、[送信] をクリックします。

#### 5 [このウィザードの終了後にユーザーに資格を割り当てる] を選択します。

- 6 [資格を追加] ウィザードで [追加] をクリックして、1 つ以上の検索条件を選択します。[検索] をクリックして、条件に一致するユーザーまたはグループを検索します。プール内のアプリケーションの使用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。

[アプリケーション プール] ページで、アプリケーション プールの [アプリケーション ショートカット] 列にチェック マークが表示されます。

## デスクトップとアプリケーション プールへのクライアント制限の実装

特定のクライアント コンピュータに対して、使用資格のある公開デスクトップとアプリケーション プールへのアクセスを制限することができます。アクセスを制限するには、Active Directory セキュリティ グループ内の公開デスクトップまたはアプリケーションへのアクセスを許可するクライアント コンピュータの名前を追加し、このグループにプールの使用資格を付与する必要があります。Active Directory セキュリティ グループには、任意の AD 組織単位 (OU) またはデフォルトのコンピュータ コンテナに属しているクライアント コンピュータを含めることができます。

クライアント制限機能には、特定の要件と制限事項があります。

- 公開デスクトップまたはアプリケーション プールを作成または変更するときに、クライアント制限ポリシーを有効にする必要があります。デフォルトでは、クライアント制限ポリシーは無効になっています。公開デスクトップ プールの設定については、[公開デスクトップ プール作成用のワークシート](#)を参照してください。アプリケーション プールの設定については、[Horizon Console でアプリケーション プールを手動で作成するためのワークシート](#)を参照してください。
- 公開デスクトップまたはアプリケーション プールの使用資格を作成または変更するときに、公開デスクトップまたはアプリケーション プールへのアクセスを許可するクライアント コンピュータの名前を含む Active Directory セキュリティ グループを追加する必要があります。
- クライアント制限機能を使用すると、特定のクライアント コンピュータにのみ、公開デスクトップとアプリケーション プールへのアクセスを許可できます。使用資格のないデスクトップやアプリケーション プールに対するアクセス権はユーザーに付与されません。たとえば、ユーザーまたはユーザー グループのメンバーとしてアプリケーション プールの使用資格が付与されていないユーザーは、アプリケーション プールの使用資格のある Active Directory セキュリティ グループにユーザーのクライアント コンピュータが含まれている場合でも、アプリケーション プールにアクセスできません。
- クライアント制限機能は、このリリースの Windows クライアント コンピュータでのみサポートされます。クライアント コンピュータに Horizon Client 4.6 for Windows 以降が必要です。
- 公開デスクトップまたはアプリケーション プールにクライアント制限ポリシーが有効になっている場合、Windows 以外のクライアント、Horizon Client for Windows の 4.6 以前のバージョンを実行している Windows クライアント、HTML Access クライアントは、制限付きプールからデスクトップまたはアプリケーションを起動できません。
- クライアント制限機能で制限されるのは、Windows クライアントからの新しいセッションのみです。この機能では、前のユーザー セッションの既存アプリケーション セッションの接続は制限されません。
- Horizon Client for Windows バージョン 5.0 では、Active Directory セキュリティ グループに属するクライアント コンピュータがデフォルトの Active Directory のロケーション (CN=Computers) に存在する必要があります。

# JMP Integrated Workflow スタートガイド

# 13

JMP Integrated Workflow 概念の概要を理解し、JMP Integrated Workflow 機能を使用するために必要な作業をよく理解してください。

この章には、次のトピックが含まれています。

- [JMP Integrated Workflow のバージョン情報](#)
- [JMP 統合ワークフローの開始](#)

## JMP Integrated Workflow のバージョン情報

VMware Horizon JMP (Just-in-Time Management Platform) の統合ワークフロー機能を使用すると、ユーザーまたはユーザー グループのデスクトップ ワークスペースを 1 つのコンソールで定義し、管理することができます。

デスクトップ ワークスペースを作成するには、VMware Horizon デスクトップ プール、VMware App Volumes AppStacks、VMware User Environment Manager の設定などを含む JMP の割り当てを定義します。JMP 割り当てを送信すると、JMP 自動化エンジンが Horizon 7、App Volumes、User Environment Manager システムと通信を行い、デスクトップの使用資格をユーザーに付与します。

既存の JMP 割り当ては、Horizon Console の [割り当て (JMP)] タブで管理できます。各コンポーネントの割り当ては、それぞれの JMP コンポーネントのコンソールで変更できます。たとえば、JMP 割り当てで定義されたデスクトップ プールを変更するには、Horizon Console で [インベントリ] - [デスクトップ] の順に選択します。

Horizon Console で JMP 割り当てを開くと、JMP 割り当ての各コンポーネントが予測される状態であることが確認されます。違いがあると、影響を受ける領域がコンソールで強調表示されます。現在の状態を受け入れることも、割り当てを変更して必要な状態にし、ユーザーの資格を再度付与することもできます。

VMware Horizon JMP Server をインストールして構成すると、Horizon Console で JMP Integrated Workflow 機能が使用可能になります。詳細については、[JMP 統合ワークフローの開始](#)と『VMware Horizon JMP Server のインストールとセットアップ ガイド』を参照してください。

---

**注:** App Volumes が VMware Cloud をサポートしていないため、JMP Integrated Workflow 機能は AWS の VMware Cloud<sup>®</sup> をサポートしていません。

---

## JMP 統合ワークフローの開始

JMP Integrated Workflow 機能を使用するには、JMP Server をインストールして設定し、JMP を構成する必要があります。

## 前提条件

インストールするすべてのテクノロジー コンポーネントの前提条件とシステム要件を確認します。

## 手順

- 1 必要であれば、管理者ユーザーおよびグループを Active Directory で設定します。  
『Horizon 7 のインストール』ドキュメントの「Active Directory の準備」を参照してください。JMP を構成するには、Active Directory の情報が必要です。
- 2 Microsoft SQL Server を設定し、JMP Server のインストールで使用するログイン認証情報が作成されていることを確認します。詳細については、『VMware Horizon JMP Server のインストールとセットアップ ガイド』ドキュメントの「JMP Server のデータベース要件」を参照してください。
- 3 VMware Horizon7 バージョン 7.5 以降をインストールして設定します。  
『Horizon 7 のインストール』ドキュメントを参照してください。
- 4 (オプション) VMware App Volumes 2.14 以降をインストールして設定します。これにより、アプリケーションをリアルタイムで提供できます。  
詳細については、『VMware App Volumes インストール ガイド』ドキュメントを参照してください。
- 5 (オプション) コンテキスト ポリシーを管理するには、VMware User Environment Manager 9.2.1 以降をインストールして設定します。  
『VMware User Environment Manager のインストールと設定』ドキュメントを参照してください。
- 6 JMP Server が組織のネットワーク内にある他のサーバと安全に通信できるように、CA 署名付きの SSL 証明書を取得します。
- 7 JMP Integrated Workflow 機能に必要な他のサーバと通信できるように、JMP Server をインストールして JMP Server に SSL 証明書を設定します。  
詳細については、『VMware Horizon JMP Server のインストールとセットアップ ガイド』を参照してください。
- 8 初めての場合は、JMP を構成します。詳細については、[JMP の初期構成](#)を参照してください。

## 次のステップ

前のタスクが正常に終了すると、JMP 割り当ての作成をすぐに始めることができます。詳細については、[JMP 割り当ての作成](#)を参照してください。



## JMP 設定の管理

JMP Server をインストールしたら、JMP 割り当てを作成したり、JMP Integrated Workflow の機能を使用する前に、JMP の設定で必要な資格情報を設定する必要があります。必要であれば、JMP 設定を編集し、新しい設定情報を追加できます。

この章には、次のトピックが含まれています。

- JMP の初期構成
- JMP 設定の管理

### JMP の初期構成

JMP 割り当てを作成する前に、Horizon Console を使用して JMP を構成する必要があります。ユーザーまたはグループへのデスクトップワークスペースの割り当てで使用する Active Directory ドメインの認証情報を入力する必要があります。JMP 割り当ての作成で App Volumes AppStack と User Environment Manager 設定共有を使用するときに、認証情報を含めることもできます。

#### 前提条件

- VMware Horizon JMP Server が正常にインストールされ、その URL があることを確認します。詳細については、『VMware Horizon JMP Server のインストールとセットアップガイド』を参照してください。
- JMP Server で使用する Horizon 7 バージョン 7.5 以降の管理者アカウントの認証情報を取得します。
- JMP Server で使用する Active Directory 認証情報を取得します。
- JMP 割り当てにアプリケーションを割り当てる場合は、使用する VMware App Volumes Manager インスタンスの URL と管理者アカウントの認証情報があることを確認します。ロード バランサで App Volumes Manager インスタンスを管理する場合は、ロード バランサの URL を取得し、App Volumes Manager 情報を設定するときに使用します。
- VMware User Environment Manager 設定共有を使用する場合は、その UNC パスとアクセスに必要な管理者アカウントの認証情報を取得します。

#### 手順

- 1 Horizon Console で、[JMP 設定] をクリックします。
- 2 JMP Server の情報を入力します。
  - a [JMP Server] タブで、[JMP Server の追加] をクリックします。
  - b `https://jmp.yourcompany.com` の形式で JMP Server の URL を入力します。
  - c [保存] をクリックします。



JMP Server URL が検証されます。JMP Server が到達不能というメッセージを受信した場合は、正しい URL を入力していることを確認します。また、JMP Server が正しく構成され、JMP Server が到達可能であることを確認します。

- 3 JMP Server で使用する Horizon 7 Connection Server バージョン 7.5 以降のアカウント情報を入力します。
  - a [Horizon 7] タブをクリックします。
  - b 自動入力されていない場合は、[Connection Server URL] の値を入力します。この URL は、Horizon Console が接続している Horizon 7 Connection Server の URL と同じです。
  - c Horizon 7 サービス アカウントのユーザー名とパスワードを入力します。
  - d [サービス アカウント ドメイン] テキスト ボックスに、作成中の JMP 割り当てで使用する有効な名前を入力して、[Enter] を押します。
  - e [保存] をクリックします。
- 4 JMP 割り当てで使用する Active Directory の情報を入力します。
  - a [Active Directory] タブをクリックします。
  - b [新規] をクリックします。
  - c [NETBIOS 名] テキスト ボックスで、使用可能な NetBIOS ドメイン名のリストから選択します。  
[DNS ドメイン名] テキスト ボックスと [コンテキスト] テキスト ボックスにデフォルト値が表示されます。
  - d [DNS ドメイン名] テキスト ボックスに追加されたデフォルト値が正しい値かどうか確認します。必要であれば、別の Active Directory の完全修飾ドメイン名を入力します。例 : **mycompany.com**
  - e [プロトコル] セクションで、Active Directory のプロトコルを選択します。
  - f [バインド ユーザー名] と [バインド パスワード] テキスト ボックスに、バインド識別名 (DN) のユーザー アカウントの認証情報を入力します。例 : **administrator**
  - g デフォルトとは異なる値を使用する場合は、[コンテキスト] テキスト ボックスの値を変更します。  
この値は、Active Directory データ検索のルートとして使用されます。
  - h (オプション) [詳細プロパティ] をクリックして、ポート番号のデフォルト値を変更します。  
デフォルトのポート値は、以前に選択したプロトコルに基づいて設定されます。ポート値を変更することも、テキスト ボックスを空白にすることもできます。
  - i [ドメイン コントローラ] テキスト ボックスに、Active Directory トラフィックの処理に使用する 1 つ以上のホスト名または IP アドレスを入力できます。  
例 : **adserver.mycompany.com**, **10.111.XXX.XXX** テキスト ボックスを空白にすると、[DNS ドメイン名] テキスト ボックスに値が使用されます。
  - j [保存] をクリックします。

- 5 JMP 割り当ての作成で App Volumes Appstack を使用する場合は、使用する App Volumes Manager を構成します。

- a [App Volumes] タブをクリックします。
- b [新規] をクリックします。
- c App Volumes インスタンスに割り当てる名前を [名前] テキスト ボックスに入力します。テキスト ボックスを空白にすると、[App Volumes サーバ URL] テキスト ボックスに入力した値が使用されます。
- d JMP Server ポッドを関連付ける App Volumes Manager に有効な URL を入力します。

---

**重要:** 使用する App Volumes Manager をロード バランサが管理する場合は、そのロード バランサの URL を入力します。

---

- e App Volumes Manager またはロード バランサの管理者アカウントの認証情報を入力します。この認証情報は、JMP Server が App Volumes Manager にアクセスするときに使用します。
- f JMP 割り当てに使用される App Volumes Manager サービス アカウントのドメイン名を入力します。
- g (オプション) 1 つ以上の App Volumes Manager を登録する場合は、切り替えボタンを使用して、追加する App Volumes Manager が JMP 割り当ての作成で使用するデフォルトのサーバかどうかを示します。JMP 割り当ての作成時に使用するインスタンスは変更できます。
- h [保存] をクリックします。

- 6 JMP 割り当てを作成するときに User Environment Manager 構成共有を使用する場合は、JMP 設定にその情報を追加します。

- a [UEM] タブをクリックします。
- b [新規] をクリックします。
- c [ファイル共有の UNC パス] テキスト ボックスに、`\\fileserver-name\UEM-configuration-share-pathname` という形式で値を入力します。例: `\\FileServer\UEMConfig`。

---

**重要:** 入力するファイル共有の UNC パスに `General` は含めないでください。

---

- d User Environment Manager 構成共有への接続に使用する User Environment Manager 管理者アカウントの認証情報を入力します。
- e [Active Directory] リストから、User Environment Manager 構成共有で使用するドメイン名を選択します。

---

**注:** Active Directory に 1 つの User Environment Manager 構成共有を関連付けることができます。

---

- f [保存] をクリックします。

#### 次のステップ

JMP の初期設定が完了すると、JMP 割り当てを作成できます。詳細については、[JMP 割り当ての作成](#)を参照してください。

## JMP 設定の管理

Horizon Console では、JMP 設定の情報を変更、追加、削除できます。

- 特定の JMP 設定を変更するために、必要な情報を準備する必要があります。
- JMP 設定を変更するには、適切な管理者権限が必要です。

### JMP Server の設定の編集

既存の JMP Server 設定を変更するには、Horizon Console を使用します。

#### 前提条件

- 特定の JMP Server 設定を変更するために、必要な情報を準備する必要があります。
- Horizon Console にログインして JMP Server の設定を変更するには、適切な管理者権限が必要です。

#### 手順

- 1 Horizon Console で、[JMP 設定] を選択します。
- 2 [JMP 設定] ペインで、[JMP Server] タブをクリックします。
- 3 [編集] をクリックします。
- 4 [JMP Server の URL] に新しい URL を入力します。
- 5 [保存] をクリックします。

新しい JMP Server URL が検証されます。無効な場合、エラー メッセージが表示されます。

### Horizon 7 認証情報の編集

既存の Horizon 7 Connection Server の資格情報を変更するには、Horizon Console を使用します。

#### 手順

- 1 Horizon Console で、[JMP 設定] をクリックします。
- 2 [Horizon 7] タブをクリックします。
- 3 [認証情報の編集] をクリックします。
- 4 必要であれば、[サービス アカウント ユーザー名] に新しいユーザー名を入力します。
- 5 必要であれば、[サービス アカウント パスワード] に新しいパスワードを入力します。
- 6 必要であれば、[サービス アカウント ドメイン] の値を変更します。
- 7 [保存] をクリックします。

### Horizon 接続サーバ URL の編集

既存の JMP 割り当てに別の Horizon Connection Server に関連付けるには、JMP 割り当てに関連付けられている JMP Server の設定で登録済みの Horizon Connection Server URL を変更する必要があります。

Horizon Console には、Horizon Connection Server の情報を変更できるユーザー インターフェイスがありません。JMP の設定で既存の Horizon Connection Server ホスト URL を変更するには、SQL Server Management Studio を使用する必要があります。

#### 前提条件

- SQL Server Management Studio セッションにログインし、JMP Server に作成した SQL Server データベースにアクセスするには、適切なシステム管理者権限が必要です。
- データベースの変更を行う前に、SQL Server データベースをバックアップします。

#### 手順

- 1 現在、Horizon Console セッションにログインしている場合は、ログアウトします。
- 2 sysadmin (SA) として SQL Server Management Studio セッションにログインするか、SA 権限を持つユーザー アカウントにログインします。
- 3 置換する Horizon Connection Server ホスト URL が別の JMP Server インスタンスに登録されていないことを確認します。

たとえば、置換する Horizon Connection Server ホスト URL が `new-horizon-host.com` の場合、次の SQL ステートメントを使用して、登録されていないことを確認します。

```
SELECT * from xms_services
WHERE xms_services.host = "new-horizon-host.com"
```

- 4 前の SQL ステートメントが結果を返さない場合は、次の手順に進みます。それ以外の場合は、次のステートメントを使用して、既存の Horizon Connection Server ホストの情報を削除します。

```
DELETE from xms_services
WHERE xms_services.host = "new-horizon-host.com"
```

- 5 次のステートメントを使用して、既存の JMP Server の設定を更新します。`new-horizon-server-host.com` は、置換する Horizon Connection Server ホストの URL です。`old-horizon-host.com` は、現在登録されている Horizon Connection Server ホストの URL です。

```
UPDATE xms_service_endpoints
SET host = 'new-horizon-host.com', is_available = 1
WHERE service_id = (SELECT id FROM xms_services WHERE service_type = 'horizon'
    AND host = 'old-horizon-host.com')
AND host = 'old-horizon-host.com'

UPDATE xms_services
SET [name] = 'horizon-https://new-horizon-host.com', host = 'new-horizon-host.com'
WHERE service_type = 'horizon'
AND host = 'old-horizon-host.com'
```

- 6 新しい Horizon Connection Server URL を使用して Horizon Console にログインして、新しい Horizon Connection Server ホストが古い Horizon Connection Server ホストの JMP 割り当てに関連付けられたことを確認します。

## Active Directory ドメインの追加

最初の Active Directory ドメインを設定した後、別のドメインを追加する場合は、Horizon Console を使用します。

### 手順

- 1 Horizon Console で、[JMP 設定] をクリックします。
- 2 [Active Directory] タブをクリックし、[追加] をクリックします。
- 3 [NETBIOS 名] テキスト ボックスで、使用可能な NetBIOS ドメイン名のリストから選択します。  
[DNS ドメイン名] テキスト ボックスと [コンテキスト] テキスト ボックスにデフォルト値が表示されます。
- 4 NETBIOS 名の更新後に、[DNS ドメイン名] テキスト フィールドにデフォルト値が追加されていることを確認します。必要であれば、別の Active Directory の完全修飾ドメイン名を入力します。例：mycompany.com
- 5 [プロトコル] セクションで、Active Directory のプロトコルを選択します。
- 6 [バインド ユーザー名] と [バインド パスワード] テキスト フィールドに、バインド識別名 (DN) のユーザー アカウント (Administrator など) の認証情報を入力します。
- 7 デフォルトとは異なる値を使用する場合は、[コンテキスト] テキスト フィールドの値を変更します。
- 8 (オプション) [詳細プロパティ] をクリックして、ポート番号のデフォルト値を変更します。  
デフォルトのポート値は、以前に選択したプロトコルに基づいて設定されます。ポート値を変更することも、テキスト フィールドを空白にすることもできます。
- 9 [ドメイン コントローラ] テキスト フィールドに、Active Directory トラフィックの処理に使用する 1 つ以上のホスト名または IP アドレスを入力できます。
- 10 [保存] をクリックします。

Active Directory のテーブルに、新しく追加された Active Directory ドメインの情報が表示されます。

## Active Directory ドメイン情報の編集

JMP の設定を最初に構成した後、特定の情報が変更されている場合は、Horizon Console を使用して Active Directory ドメインの設定情報を変更します。

### 手順

- 1 Horizon Console で、[JMP 設定] をクリックします。
- 2 [Active Directory] タブをクリックします。
- 3 Active Directory ドメインのテーブルで 1 つの行を選択し、[編集] をクリックします。
- 4 更新する必要がある Active Directory 情報を変更します。
- 5 [保存] をクリックします。

## Active Directory ドメイン情報の削除

既存の Active Directory (AD) ドメインの設定情報を削除するには、Horizon Console を使用します。

登録済みの Active Directory ドメインが既存の JMP 割り当てで使用されていない場合、このドメインの情報を JMP の設定から削除できます。

#### 手順

- 1 Horizon Console で、[JMP 設定] をクリックします。
- 2 [Active Directory] タブをクリックします。
- 3 テーブルで、JMP 設定から削除する Active Directory ドメインの行を選択します。
- 4 削除確認のダイアログが表示されたらメッセージを確認し、[削除] をクリックして、この Active Directory ドメイン情報の削除を確認します。

Active Directory ドメインを使用する JMP 割り当てがない場合、ドメインが削除されます。

Active Directory ドメインが JMP 割り当てで使用されている場合、警告のダイアログボックスが表示されます。警告メッセージに、Active Directory ドメインを使用している JMP 割り当てのリストが表示されます。ドメインを JMP 割り当てから削除するか、ドメインを使用している JMP 割り当てを削除した場合にのみ、ドメイン情報を削除できます。

## App Volumes 情報の追加

Horizon Console で App Volumes Manager の情報を追加し、JMP 割り当ての作成時に使用できます。

#### 手順

- 1 Horizon Console で、[JMP 設定] をクリックします。
- 2 [App Volumes] タブをクリックし、[追加] をクリックします。  
[App Volumes インスタンスの追加] ダイアログボックスが表示されます。
- 3 App Volumes インスタンスに割り当てる一意の名前を [名前] テキストボックスに入力します。テキストボックスを空白にすると、[App Volumes サーバ URL] テキストボックスに入力した値が使用されます。
- 4 [App Volumes サーバ URL] テキストボックスに、JMP Server に関連付ける App Volumes Manager に有効な URL を入力します。追加する App Volumes Manager をロード バランサが管理する場合は、そのロード バランサの URL を入力します。

---

**注:** 追加した App Volumes Manager が別の SQL データベースに接続している場合、追加した App Volumes Manager の情報が App Volumes タブに表示されます。App Volumes Manager が同じ SQL データベースに接続している場合は、以前に登録した App Volumes Manager の情報のみが App Volumes タブに表示されます。

---

- 5 JMP Server が App Volumes Manager へのアクセスで使用する App Volumes 管理者のユーザー名とパスワードを入力します。
- 6 JMP 割り当てに使用される App Volumes サービス アカウントのドメイン名を入力します。

- 7 追加する App Volumes Manager を JMP 割り当ての作成時にデフォルトで使用する App Volumes Manager サーバにするには、切り替えボタンをクリックします。JMP 割り当ての作成時に使用するサーバは変更できません。

切り替えボタンが青色に変わり、[はい] というラベルが表示されます。

- 8 [保存] をクリックします。

## App Volumes インスタンス情報の編集

JMP 割り当てで使用する App Volumes インスタンスの情報を変更する場合は、Horizon Console で 情報を変更します。

### 手順

- 1 Horizon Console で、[JMP 設定] をクリックします。
- 2 [App Volumes] タブをクリックして、変更する App Volumes のインスタンスのテーブル行を選択します。
- 3 [編集] をクリックします。

[App Volumes インスタンスの追加] ダイアログ ボックスが表示されます。

- 4 更新する必要がある App Volumes インスタンス情報を変更します。
- 5 [保存] をクリックします。

## App Volumes インスタンス情報の削除

App Volumes インスタンスの既存の設定を削除する場合は、Horizon Console を使用します。

登録済みの App Volumes インスタンスが JMP 割り当てで使用されていない場合、このインスタンスの情報を JMP の設定から削除できます。

### 手順

- 1 Horizon Console で、[JMP 設定] をクリックします。
- 2 [App Volumes] タブをクリックします。
- 3 JMP の設定から削除する App Volumes インスタンス情報の行を選択します。
- 4 [削除] をクリックして、この App Volumes インスタンス情報の削除を確認します。

App Volumes インスタンスを使用する JMP 割り当てがない場合、インスタンスが削除されます。

App Volumes インスタンスが JMP 割り当てで使用されている場合は、警告のダイアログ ボックスが表示されます。警告メッセージに、App Volumes インスタンスを使用している JMP 割り当てのリストが表示されます。App Volumes インスタンスを JMP 割り当てから削除するか、インスタンスを使用している JMP 割り当てを削除した場合にのみ、インスタンス情報を削除できます。

## User Environment Manager 構成共有情報の追加

最初の User Environment Manager 構成共有情報を設定した後に別の共有情報を追加する場合は、Horizon Console を使用します。

Active Directory ドメインごとに 1 つの User Environment Manager 構成共有を追加できます。追加する構成共有に、JMP Server 設定の構成共有と同じ IP アドレスまたは DNS アドレスを設定することはできません。

#### 手順

- 1 Horizon Console で、[JMP 設定] をクリックします。
- 2 [UEM] タブをクリックして、[追加] をクリックします。  
[UEM ファイル共有の追加] ダイアログ ボックスが表示されます。
- 3 [ファイル共有の UNC パス] テキスト ボックスに、`\\server-name\UEM-configuration-share-pathname` という形式で値を入力します。  
  
たとえば、構成共有の場所が `\\<IP-address>\uemshare\config\general\FlexRepository\..` の場合、[ファイル共有の UNC パス] テキスト ボックスに `\\<IP-address>\uemshare\config` を入力する必要があります。
- 4 User Environment Manager 構成ファイル共有への接続で使用する User Environment Manager のユーザー名とパスワードを入力します。
- 5 [Active Directory] リストから、User Environment Manager 構成ファイル共有を使用するドメイン名を選択します。

---

**注:** Active Directory に 1 つの User Environment Manager 構成ファイル共有を関連付けることができません。

---

- 6 [保存] をクリックします。

User Environment Manager 構成ファイル共有の情報が JMP 設定に追加され、[UEM] タブのテーブルに新しい行が追加されます。

## User Environment Manager 構成ファイルの共有情報の編集

JMP 割り当てで使用されている User Environment Manager 構成ファイル共有の情報を変更するには、Horizon Console を使用します。

#### 手順

- 1 Horizon Console で、[JMP 設定] をクリックします。
- 2 [UEM] タブをクリックして、既存の情報が保存されているテーブルで、変更する User Environment Manager 構成ファイル共有の行を選択します。
- 3 [編集] をクリックします。  
[UEM ファイル共有の編集] ダイアログ ボックスが表示されます。
- 4 更新する必要がある User Environment Manager 構成ファイル共有の情報を変更します。
- 5 [保存] をクリックします。



## User Environment Manager 構成共有情報の削除

User Environment Manager 構成共有の既存の設定を削除する場合は、Horizon Console を使用します。

登録済みの User Environment Manager 構成共有が JMP 割り当てで使用されていない場合、この構成共有を JMP 設定から削除できます。

### 手順

- 1 Horizon Console で、[JMP 設定] をクリックします。
- 2 [UEM] タブをクリックします。
- 3 JMP の設定から削除する User Environment Manager 構成共有情報の行を選択します。
- 4 [削除] をクリックして、この User Environment Manager 構成共有情報の削除を確認します。

User Environment Manager 構成共有を使用する JMP 割り当てがない場合、構成共有が削除されます。

User Environment Manager 構成共有が JMP 割り当てで使用されている場合は、警告のダイアログ ボックスが表示されます。警告メッセージに、User Environment Manager 構成共有を使用している JMP 割り当てのリストが表示されます。User Environment Manager 構成共有を JMP 割り当てから削除するか、構成共有を使用している JMP 割り当てを削除した場合にのみ、その構成共有情報を削除できます。

## JMP 割り当ての管理

JMP Server をインストールして JMP の構成を行うと、JMP Integrated Workflow 機能を使用して JMP 割り当ての作成、変更、複製、削除を行うことができます。

まず、JMP 割り当ての作成を開始する前に、JMP Server をインストールして JMP の構成を行う必要があります。詳細については、『VMware Horizon JMP Server のインストールとセットアップガイド』および [JMP の初期構成](#) を参照してください。

JMP 割り当てを作成、編集、複製または削除する前に、次の前提条件が満たされていることを確認します。

- JMP の設定で登録されている Horizon 7 インスタンスが起動し、実行されていることを確認します。
- 1 つ以上の Active Directory ドメインが JMP の設定で登録されていることを確認します。
- JMP の設定で登録されている App Volumes インスタンスが起動し、実行されていることを確認します。
- JMP 設定で定義されている User Environment Manager 構成共有が起動し、実行されていることを確認します。

---

**注:** グローバル資格はサポートされていません。

---

JMP 割り当ての作成、編集、複製または削除を行っているときに、「アクションが正常に完了しませんでした」というメッセージが表示される場合があります。たとえば、基盤となる JMP テクノロジー コンポーネントの 1 つに接続を試みたときに問題が発生し、割り当ての検証に失敗する場合があります。JMP 割り当てのサマリ画面で、次のオプションのいずれかを選択し、問題を修正を行います。

- 問題を手動で修正するには、[編集] をクリックします。
- 現在の JMP 割り当てで見つかった問題を JMP Server が修正するように設定するには、[修復] をクリックします。
- JMP 割り当てを完全に削除するには、[強制的に削除] をクリックします。

この章には、次のトピックが含まれています。

- [JMP 割り当ての作成](#)
- [JMP 割り当ての編集](#)
- [JMP 割り当ての複製](#)
- [JMP 割り当ての削除](#)

## JMP 割り当ての作成

Horizon Console では、ユーザーまたはユーザー グループのデスクトップ ワークスペースの作成で使用する JMP 割り当てを作成できます。

JMP 割り当てを定義するには、Horizon デスクトップ プール、App Volumes Appstack、User Environment Manager の設定を選択します。

### 前提条件

[15 章 JMP 割り当ての管理](#)に記載されている前提条件を満たしていることを確認します。

### 手順

- 1 Horizon Console で、[割り当て (JMP)] をクリックします。
- 2 [新規] をクリックします。
- 3 [新しい割り当て] ウィザードの [ユーザー] タブで、[Active Directory] ドロップダウン リストの横に 2、3 文字入力し、新しい JMP 割り当てに追加するユーザーまたはユーザー グループを選択します。  
選択した項目が [選択したユーザー/グループ] セクションに追加されます。
- 4 [次へ] をクリックします。
- 5 [デスクトップ] タブで、JMP 割り当てに追加するデスクトップ プールを選択し、[次へ] をクリックします。
- 6 [アプリケーション] タブで、JMP 割り当てに追加するアプリケーション名の横にあるチェック ボックスをクリックします。選択が終了したら、[次へ] をクリックします。
- 7 [ユーザー環境] タブで、使用可能なユーザー環境設定で JMP 割り当てを設定するかどうかを決めます。
  - [UEM の設定を無効にしますか?] を [いいえ] に設定して [スキップ] をクリックすると、User Environment Manager の割り当てファイルが User Environment Manager の構成共有に保存されません。User Environment Manager のすべての設定が、現在作成している JMP 割り当てを使用するユーザーの仮想デスクトップ ワークスペースに適用されます。
  - [UEM の設定を無効にしますか?] を [いいえ] に設定した場合は、作成している JMP 割り当てに適用するユーザー環境設定を選択します。[次へ] をクリックすると、選択したユーザー環境設定で User Environment Manager の割り当てファイルが作成されます。選択した設定が、現在作成している JMP 割り当てを使用するユーザーの仮想デスクトップ ワークスペースに適用されます。
  - [UEM の設定を無効にしますか?] を [はい] に設定すると、使用可能なユーザー環境設定のリストがビューから消えます。[次へ] をクリックすると、空の割り当てファイルが、User Environment Manager の構成共有に書き込まれます。User Environment Manager の設定を無効にすると、現在作成している JMP 割り当てを使用するユーザーの仮想デスクトップ ワークスペースにユーザー環境設定が適用されません。
- 8 [定義] タブで、JMP 割り当てのデフォルト名をそのまま使用するか、別の名前で置き換えます。また、必要に応じて説明を追加します。
- 9 [AppStack の接続] ドロップダウン リストで、AppStack が JMP 割り当てに接続するタイミングを選択し、[次へ] をクリックします。

- 10 [サマリ] タブで、新しい割り当ての詳細を確認します。問題がなければ、[送信] をクリックします。変更を行う必要がある場合は、[戻る] をクリックして調整します。

新しい JMP 割り当てがキューに入り、JMP データベースへの保存待ち状態になります。また、[JMP 割り当て] ペインの割り当てリストに追加されます。JMP 割り当てが JMP データベースに正常に追加されると、ステータスが保留状態から変わります。これは JMP 割り当てリストで選択可能になり、編集、複製、削除を行うことができます。

また、次の情報を使用すると、新しい JMP 割り当てに作成された割り当てまたは資格を確認できます。

- JMP 割り当てに作成された Horizon デスクトップ プールの情報を確認するには、Horizon Console を使用します。[インベントリ] - [デスクトップ] の順に選択し、JMP Server によって作成されたデスクトップ プールを検索します。
- JMP Server によって新しい JMP 割り当てに作成された AppStack の情報を表示するには、App Volumes Manager コンソールを使用します。[ボリューム] - [AppStack] の順に選択し、JMP Server によって作成された AppStack を検索します。
- JMP 割り当てに設定したユーザー環境設定を確認するには、User Environment Manager 管理コンソールを使用して [ユーザー環境] タブをクリックします。左側のペインから JMP 割り当てで使用するユーザー環境設定を選択します。ユーザー環境設定の JMP 割り当て情報が表示されたダイアログ ボックスから、[割り当て] タブをクリックします。

## JMP 割り当ての編集

JMP 割り当ての定義に使用されたコンポーネントが変更されると、その割り当ての変更が必要になる場合があります。JMP 割り当てを変更するには、Horizon Console を使用します。

### 前提条件

- [15 章 JMP 割り当ての管理](#)に記載されている前提条件を満たしていることを確認します。
- 保留状態の JMP 割り当てでは編集できません。

### 手順

- 1 Horizon Console で、[割り当て (JMP)] をクリックします。
- 2 チェック ボックスをクリックするか、リストで JMP 割り当ての名前をクリックして、編集する JMP 割り当てを選択します。
- 3 [編集] をクリックします。
- 4 [割り当ての編集] ウィザードで、現在の設定を変更します。

編集を中止するには、[キャンセル] をクリックします。

- a 現在選択されているユーザーまたはグループを削除するには、削除アイコン ([X]) をクリックします。
- b [次へ] をクリックします。
- c [デスクトップ] タブで、JMP 割り当てに追加するデスクトップ プールを選択します。[次へ] をクリックします。

- d [アプリケーション] タブで、JMP 割り当てに追加するアプリケーションを選択するか、すでに選択されているアプリケーションの選択を解除します。[次へ] をクリックします。
- e [ユーザー環境] タブで、使用可能なユーザー環境設定で JMP 割り当てを設定するかどうかを決めます。
  - [UEM の設定を無効にしますか?] を [いいえ] に設定して [スキップ] をクリックすると、User Environment Manager の割り当てファイルが User Environment Manager の構成共有に保存されません。User Environment Manager のすべての設定が、現在編集している JMP 割り当てを使用するユーザーの仮想デスクトップ ワークスペースに適用されます。
  - [UEM の設定を無効にしますか?] を [いいえ] に設定した場合は、作成している JMP 割り当てに適用するユーザー環境設定を選択します。[次へ] をクリックすると、選択したユーザー環境設定で User Environment Manager の割り当てファイルが作成されます。選択した設定が、現在編集している JMP 割り当てを使用するユーザーの仮想デスクトップ ワークスペースに適用されます。
  - [UEM の設定を無効にしますか?] を [はい] に設定すると、使用可能なユーザー環境設定のリストがビューから消えます。[次へ] をクリックすると、空の割り当てファイルが、User Environment Manager の構成共有に書き込まれます。User Environment Manager の設定を無効にすると、現在編集している JMP 割り当てを使用するユーザーの仮想デスクトップ ワークスペースにユーザー環境設定が適用されません。
- f 必要であれば、[定義] タブで、[名前]、[説明]、JMP 割り当てに AppStack を接続するタイミングを変更します。
- g [次へ] をクリックします。
- h 変更内容を確認して [送信] をクリックし、変更を保存します。

成功すると、変更が保存されます。問題が検出されると、追加情報と実行可能なアクションが表示されます。

## JMP 割り当ての複製

作成する JMP 割り当てに類似した割り当てを複製すると、JMP 割り当てをより簡単に作成できます。

### 前提条件

- [15 章 JMP 割り当ての管理](#)に記載されている前提条件を満たしていることを確認します。
- 保留またはエラー状態の JMP 割り当ては複製できません。

### 手順

- 1 Horizon Console で、[割り当て (JMP)] を選択します。
- 2 複製する JMP 割り当てを選択して、[複製] をクリックします。
- 3 [新しい割り当て] ウィザードを使用して、複製された JMP 割り当てを必要に応じて変更します。
  - a 新しいユーザーまたはグループを選択するか、現在選択されているユーザーまたはグループを削除します。[次へ] をクリックします。
  - b [デスクトップ] ペインで、新しいデスクトップ プールを選択します。あるいは、複製された JMP 割り当てに含まれているデスクトップ プールを削除します。[次へ] をクリックします。

- c すでに選択されているアプリケーションの選択を解除し、新しい JMP 割り当てに追加するアプリケーションを選択します。[次へ] をクリックします。
- d [ユーザー環境] ペインで、新しい JMP 割り当てに適用する User Environment Manager の設定を選択します。[次へ] をクリックします。
- e 必要であれば、[定義名] でデフォルトの名前を置き換えます。説明を追加し、AppStack に新しい JMP 割り当てを関連付けるタイミングを指定します。
- f [次へ] をクリックして、新しい JMP 割り当てのサマリを確認します。
- g 問題がなければ、[送信] をクリックします。それ以外の場合は、[戻る] をクリックして、修正を行います。

新しい JMP 割り当てが検証されます。検証に時間がかかる場合があります。検証に成功すると、新しく作成した JMP 割り当てが [JMP 割り当て] ペインのリストに追加されます。名前の上にマウス ポイントを置くと、保留状態であることが通知されます。この状態は、JMP データベースに正常に保存するまで続きます。JMP 割り当てが保留状態でなくなると、割り当てに別のアクションを実行できます。

## JMP 割り当ての削除

Horizon Console を使用して、JMP 割り当てを削除します。

JMP 割り当てを削除すると、Horizon プールの資格、AppStack の割り当て、JMP 割り当てに関連付けられている UEM 資格が削除されます。ただし、Horizon プールの資格や JMP 割り当てで使用されている AppStack 割り当てが JMP 割り当ての作成前から存在していた場合、これらの資格や割り当ては削除されません。JMP 割り当てを削除すると、この割り当てはユーザーまたはデスクトップに適用されなくなります。

### 前提条件

- [15 章 JMP 割り当ての管理](#)に記載されている前提条件を満たしていることを確認します。
- 保留状態の JMP 割り当ては削除できません。

### 手順

- 1 Horizon Console で、[割り当て (JMP)] をクリックします。
- 2 [JMP 割り当て] ペインで、1 つ以上の JMP 割り当てを選択して [削除] をクリックします。
- 3 確認のダイアログ ボックスで、[削除] をクリックし、割り当てを完全に削除することを確認します。

成功すると、Horizon プールの資格が JMP データベースと [JMP 割り当て] ペインのリストから削除されます。

削除操作の一部が失敗すると、JMP 割り当ては削除されません。ステータス インジケータをクリックすると、削除操作が失敗した原因の詳細が表示されます。

# Horizon Console でのイベント レポートの設定

# 16

イベント データベースを作成し、Horizon 7 イベントについての情報を記録することができます。さらに、Syslog サーバを使用する場合、イベントを Syslog サーバに送信するか、Syslog 形式で記述されたイベントのフラット ファイルを作成するように Connection Server を構成できます。

この章には、次のトピックが含まれています。

- Horizon Console で Horizon 7 イベント用のデータベースとデータベース ユーザーを追加する
- Horizon Console で SQL Server データベースをイベント レポート用に準備する
- Horizon Console でのイベント データベースの設定
- Horizon Console での Syslog サーバのイベント ログの設定
- Horizon 7 でのイベントの監視

## Horizon Console で Horizon 7 イベント用のデータベースとデータベース ユーザーを追加する

イベント データベースは、既存のデータベース サーバに追加する方法で作成します。続いて、レポート ソフトウェアを使用して、そのデータベース内のイベントを分析できます。

イベント データベース用のデータベース サーバは、専用のサーバにデプロイします。これは、プロビジョニングおよび Horizon 7 のデプロイに対して重要な他のアクティビティにイベントのログ アクティビティが影響を与えないようにするためです。

---

**注:** このデータベースのために ODBC データ ソースを作成する必要はありません。

---

### 前提条件

- サポートされている Microsoft SQL Server または Oracle データベース サーバが、Connection Server インスタンスでアクセスできるシステム上に存在することを確認します。

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

- データベースとユーザーをデータベース サーバに作成するために必要なデータベース権限があることを確認します。

- Microsoft SQL Server データベース サーバにデータベースを作成する手順に慣れていない場合は、『Horizon 7 のインストール』の「View Composer データベースを SQL Server に追加する」を参照してください。
- Oracle データベース サーバにデータベースを作成する手順に慣れていない場合は、『Horizon 7 のインストール』の「View Composer データベースを Oracle 12c または 11g に追加する」を参照してください。

#### 手順

- 1 サーバにデータベースを追加し、HorizonEvents のようなわかりやすい名前をこのデータベースに付けます。  
Oracle 12c または Oracle 11g データベースの場合は、Oracle システム識別子 (SID) も指定します（この識別子は Horizon Console でイベント データベースを構成する際に使用します）。
- 2 テーブル、ビュー、Oracle トリガとシーケンスの作成権限とこれらのオブジェクトの読み書き権限を持っているユーザーをこのデータベースに追加します。  
Microsoft SQL Server データベースの場合、統合 Windows 認証セキュリティ モデルの認証方法は使用しないでください。認証に SQL Server 認証を使用していることを確認します。

データベースは作成されますが、Horizon Console でデータベースを構成するまでスキーマはインストールされません。

#### 次のステップ

以下の説明に従います。[Horizon Console でのイベント データベースの設定](#)

## Horizon Console で SQL Server データベースをイベント レポート用に準備する

Horizon Console を使用して Microsoft SQL Server にイベント データベースを設定する前に、正しい TCP/IP プロパティを設定し、サーバが SQL Server 認証を使用していることを確認する必要があります。

#### 前提条件

- イベント レポート用に SQL Server データベースを作成します。[Horizon Console で Horizon 7 イベント用のデータベースとデータベース ユーザーを追加する](#)を参照してください。
- データベースを構成するために必要なデータベース権限があることを確認します。
- データベース サーバが SQL Server 認証の認証方法を使用していることを確認します。Windows 認証は使用しないでください。

#### 手順

- 1 SQL Server 構成マネージャを開き、[SQL Server YYYY ネットワークの構成] を展開します。
- 2 [server\_name のプロトコル] を選択します。
- 3 プロトコルのリストで [TCP/IP] を右クリックし、[P プロパティ] を選択します。
- 4 [有効化] プロパティを [はい] に設定します。



- 5 ポートが割り当てられていることを確認し、必要であれば割り当てます。

静的および動的なポートおよびポートを割り当てる方法については、SQL Server 構成マネージャのオンラインヘルプを参照してください。

- 6 このポートがファイアウォールによってブロックされないことを確認します。

#### 次のステップ

Horizon Console を使用して、データベースを Connection Server に接続します。以下の説明に従います。

[Horizon Console でのイベント データベースの設定](#)

## Horizon Console でのイベント データベースの設定

イベント データベースには、Horizon 7 のイベントに関する情報が、ログ ファイルではなくデータベースのレコードとして格納されます。

Connection Server インスタンスをインストールした後で、イベント データベースを構成します。Connection Server グループ内で構成する必要があるホストは 1 台だけです。グループの他のホストは自動的に構成されます。

---

**注:** Connection Server インスタンスと外部データベース間のデータベース接続のセキュリティは、管理者の責任ですが、イベント トラフィックは Horizon 7 環境の 健全性に関する情報に制限されます。さらに慎重を期すのであれば、IPSec などの手段を使用してこのチャンネルを保護するか、データベースを Connection Server コンピュータ上でローカルに展開することができます。

---

データベース テーブル内のイベントを調べるには、Microsoft SQL Server または Oracle データベース レポート ツールを使用できます。詳細については、Horizon 7 の統合を参照してください。

また、Horizon 7 イベントを Syslog 形式で生成すると、他社製分析ソフトウェアからイベント データにアクセスできます。vdmadmin コマンドと -I オプションを使用して、Horizon 7 イベント メッセージを Syslog 形式でイベント ログ ファイルに記録します。『Horizon 7 の管理』ドキュメントで、「-I オプションを使用した Syslog 形式での Horizon 7 イベント ログ メッセージの生成」を参照してください。

#### 前提条件

イベント データベースを構成するには、次の情報が必要です。

- データベース サーバの DNS 名または IP アドレス。
- データベース サーバの種類 (Microsoft SQL Server または Oracle)。
- データベース サーバへのアクセスに使用するポート番号。デフォルトは、Oracle の場合は 1521、SQL Server の場合は 1433 です。SQL Server では、データベース サーバが名前付きインスタンスの場合、または SQL Server Express を使用している場合は、ポート番号の特定が必要になる場合があります。SQL Server の名前付きインスタンスへの接続については、Microsoft のサポート技術情報 (KB) の記事 <http://support.microsoft.com/kb/265808> を参照してください。
- データベース サーバに作成したイベント データベースの名前。 [Horizon Console で Horizon 7 イベント用のデータベースとデータベース ユーザーを追加する](#)を参照してください。

Oracle 12c または 11g データベースの場合、Horizon Console でイベント データベースを設定するときに Oracle System Identifier (SID) をデータベース名として使用する必要があります。

- このデータベース用に作成したユーザーのユーザー名とパスワード。Horizon Console で [Horizon 7 イベント用のデータベースとデータベース ユーザーを追加する](#)を参照してください。

このユーザーに対しては SQL Server 認証を使用します。統合 Windows 認証セキュリティ モデルの認証方法は使用しないでください。

- イベント データベースのテーブルのプレフィックス (VE\_ など)。プリフィックスを使用することで、Horizon 7 の複数のインストール間でデータベースを共有できます。

---

**注:** 使用しているデータベース ソフトウェアで有効な文字を入力する必要があります。ダイアログ ボックスを終了するときにプレフィックスの構文はチェックされません。使用しているデータベース ソフトウェアで有効でない文字を入力した場合、Connection Server がデータベース サーバへの接続を試行したときにエラーが発生します。ログ ファイルにはすべてのエラーが記録され、このエラーや、データベース名が無効な場合にデータベース サーバから返されるその他すべてのエラーも含まれます。

---

#### 手順

- 1 Horizon Console で、[設定] - [イベント設定] の順に選択します。
- 2 [イベント データベース] セクションで、[編集] をクリックし、提示されるフィールドに情報を入力して、[OK] をクリックします。

イベント データベース情報をクリアするには、[クリア] をクリックします。

- 3 (オプション) イベントの設定 ウィンドウで、[編集] をクリックし、イベントを表示する時間の長さ、およびイベントを新規として分類する日数を変更し、[OK] をクリックします。

これらの設定は、イベントが Horizon Console インターフェイスに表示される期間に関係します。この時間が経過すると、イベントは履歴データベース テーブルにのみ表示されます。

- 4 [Monitoring (監視)] - [イベント] を選択し、イベント データベースに正常に接続できることを確認します。

接続できない場合は、エラー メッセージが表示されます。SQL Express を使用している場合、または SQL Server の名前付きインスタンスを使用している場合は、前提条件にあるように、正しいポート番号の特定が必要な場合があります。

## Horizon Console での Syslog サーバのイベント ログの設定

Horizon 7 イベントを Syslog 形式で生成すると、分析ソフトウェアからイベント データにアクセスできます。

Connection Server グループ内で構成する必要があるホストは 1 台だけです。グループの他のホストは自動的に構成されます。

イベントのファイル ベースのログ記録を有効にすると、イベントはローカル ログ ファイルに蓄積されます。ファイル共有を指定すると、これらのログ ファイルはその共有に移動されます。

- ローカル ファイルは、構成中（多くの場合はイベント データベースが構成される前）に素早くトラブルシューティングできるようにイベントを確認するためにのみ使用します。

イベント ログのローカル ディレクトリの最大サイズは、最も古いファイルが削除される前に閉じられたログ ファイルを含めて 300 MB です。Syslog 出力のデフォルトの出力先は %PROGRAMDATA%\VMware\VDM\events\ です。

- Syslog サーバがない場合、または現在の Syslog サーバではニーズが満たせない場合は、UNC パスを使用して長期的なイベントのレコードのログ ファイルを保存します。

別の方法として、vdmadmin コマンドを使用してイベントのファイル ベースのログを Syslog 形式で構成できます。『Horizon 7 の管理』ドキュメントで、vdmadmin コマンドの -I オプションを使用した Syslog 形式での Horizon 7 イベント ログ メッセージの生成に関するトピックを参照してください。

**重要:** Syslog データはソフトウェア ベースの暗号化なしにネットワーク間で送信され、ユーザー名などの機密データが含まれている場合があります。VMware は、IPSEC などのリンク レイヤ セキュリティを使用して、こうしたデータがネットワーク上でモニターリングする可能性を回避することを推奨します。

#### 前提条件

イベントを Syslog 形式で記録できるようにするか、Syslog サーバに送信できるようにする、またはその両方を実現できるように Connection Server を構成するには、以下の情報が必要です。

- Syslog サーバを使用して UDP ポートで Horizon 7 イベントをリッスンする予定にしている場合、Syslog サーバの DNS 名または IP アドレスと UDP ポート番号が必要です。デフォルトの UDP ポート番号は 514 です。
- フラット ファイル形式でログを収集する予定にしている場合は、ログ ファイルを格納するファイル共有およびフォルダまでの UNC パスが必要で、ファイル共有に書き込む権限を持つアカウントのユーザー名、ドメイン名、パスワードが必要です。

#### 手順

- 1 Horizon Console で、[設定] - [イベント設定] の順に選択します。
- 2 (オプション) [Syslog] 領域で、イベントを Syslog サーバに送信するように Connection Server を設定するには、[Syslog サーバに送信] の下にある [追加] をクリックし、サーバ名または IP アドレスと UDP ポート番号を入力します。
- 3 (オプション) ログ ファイルで Horizon 7 イベント ログ メッセージを Syslog 形式で生成して格納できるようにするには、[ファイルに記録: 有効化] チェック ボックスを選択します。

ログ ファイルは、ファイル共有までの UNC パスを指定しない限り、ローカルで保持されます。

- 4 (オプション) Horizon 7 イベント ログ メッセージをファイル共有に保存するには、[場所にコピー] の下にある [追加] をクリックして、ログ ファイルを保存するファイル共有またはフォルダまでの UNC パスを入力し、ファイル共有に書き込み権限を持つアカウントのユーザー名、ドメイン名、パスワードを入力します。

以下は、UNC パスの例です。

```
\\syslog-server\folder\file
```

## Horizon 7 でのイベントの監視

イベント データベースは、Connection Server ホストまたはグループ、Horizon Agent、Horizon Console で発生したイベントの情報を格納し、ダッシュボードでイベントの数をユーザーに通知します。[イベント] ページでイベントの詳細を調べることができます。

**注:** イベントは、一定の時間、Horizon Console インターフェイスに一覧表示されます。この時間が経過すると、イベントは履歴データベース テーブルにのみ表示されます。データベース テーブル内のイベントを調べるには、Microsoft SQL Server または Oracle データベース レポート ツールを使用できます。詳細については、Horizon 7 の統合を参照してください。

**注:** イベント データベースが使用できない場合、Horizon 7 がイベントの監査証跡を維持し、データベースが使用可能になると、これらの監査証跡をイベント データベースに保存します。これらのイベントを Horizon Console インターフェイスに表示するには、イベント データベースと Connection Server を再起動する必要があります。

Horizon Console でのイベントの監視に加えて、イベント データが分析ソフトウェアからアクセスできるように、Horizon 7 イベントを Syslog 形式で生成できます。[Horizon Console での Syslog サーバのイベント ログの設定](#)と『Horizon 7 のインストール』の「I オプションを使用した Syslog 形式での Horizon 7 イベント ログ メッセージの生成」を参照してください。

複数の Connection Server にイベント データベースを設定すると、Horizon Console の [イベント] ページにすべての Connection Server のイベントが表示されます。Horizon Console では、実行するタスクに基づいてイベントがフィルタリングされます。これらのイベントは、[デスクトップ プール] や [アプリケーション プール] など、関連するページに表示されます。

### 前提条件

イベント データベースを作成して設定します。『Horizon 7 のインストール』ドキュメントを参照してください。

### 手順

- 1 Horizon Console で、[監視] - [イベント] の順に選択します。
- 2 (オプション) [イベント] ページでは、イベントの時間範囲を選択し、イベントにフィルタリングを適用し、一覧表示されたイベントを 1 つ以上の列で並べ替えることができます。

### 次のステップ

特定のイベントを表示するには、Horizon Console でデスクトップまたはアプリケーション プール、仮想マシン、パーシステント ディスク、ユーザーまたはグループに移動し、[イベント] タブをクリックします。

## Horizon 7 イベント メッセージ

Horizon 7 では、システムの状態が変更されるか、システムに問題が発生した場合は、常にイベントが報告されます。それらのイベント メッセージの情報をを使用して、適切な処置を取ることができます。

次の表に、Horizon 7 が報告するイベントのタイプを示します。

表 16-1. Horizon 7 が報告するイベントのタイプ

イベントのタイプ	説明
監査失敗または監査成功	管理者またはユーザーが Horizon 7 の動作または構成に対して行った変更の成否を報告します。
エラー	失敗した Horizon 7 の動作を報告します。
情報	Horizon 7 内の正常な動作を報告します。
警告	時間の経過とともにより深刻な問題を引き起こす可能性がある、動作または設定の小さな問題を報告します。

監査失敗、エラー、または警告イベントに関連付けられたメッセージが表示された場合は、何らかの処置が必要になることがあります。監査成功または情報イベントについては、処置は必要ありません。

# Horizon Console での Horizon Help Desk Tool の使用

# 17

Horizon Help Desk Tool は、Horizon 7 ユーザー セッションのステータスを取得し、トラブルシューティングとメンテナンス操作を行う Web アプリケーションです。

Horizon Help Desk Tool では、トラブルシューティングを行うためにユーザー セッションを確認し、デスクトップの再起動やリセットなどのデスクトップ メンテナンス操作を実行できます。

Horizon Help Desk Tool を設定するには、次の要件を満たす必要があります。

- Horizon 7 の Horizon Enterprise Edition ライセンスまたは Horizon Apps Advanced Edition ライセンス正しいライセンスがあることを確認するには、『Horizon 7 の管理』ドキュメントを参照してください。
- Horizon 7 コンポーネントの情報を保存するイベント データベースイベント データベースの設定の詳細については、『Horizon 7 のインストール』ドキュメントを参照してください。
- Horizon Help Desk Tool にログインするヘルプデスク管理者ロールまたはヘルプデスク管理者（読み取り専用）ロールこれらのロールの詳細については、『Horizon 7 の管理』ドキュメントを参照してください。
- ログイン セグメントを表示するには、各接続サーバ インスタンスでタイミング プロファイラを有効にします。

各接続サーバ インスタンスでタイミング プロファイラを有効にするには、次の `vdmadmin` コマンドを使用します。

```
vdmadmin -I -timingProfiler -enable
```

管理ポートを使用している接続サーバ インスタンスでタイミング プロファイラを有効にするには、次の `vdmadmin` コマンドを使用します。

```
vdmadmin -I -timingProfiler -enable -server {ip/server}
```

この章には、次のトピックが含まれています。

- [Horizon Console で Horizon Help Desk Tool を開始します。](#)
- [Horizon Help Desk Tool でのユーザーのトラブルシューティング](#)
- [Horizon Help Desk Tool のセッションの詳細](#)
- [Horizon Help Desk Tool のセッション プロセス](#)
- [Horizon Help Desk Tool のアプリケーション ステータス](#)
- [Horizon Help Desk Tool でのデスクトップまたはアプリケーション セッションのトラブルシューティング](#)

## Horizon Console で Horizon Help Desk Tool を開始します。

Horizon Help Desk Tool は、Horizon Console に統合されています。Horizon Help Desk Tool のトラブルシューティングを行うユーザーを検索できます。

### 手順

- 1 Horizon Console で、ユーザーの検索フィールドにユーザー名を入力します。

Horizon Console では、検索結果にユーザーのリストが表示されます。最大で 100 個までの検索結果が返されます。

- 2 ユーザー名を選択します。

ユーザー カードにユーザー情報が表示されます。

### 次のステップ

問題のトラブルシューティングを行うには、ユーザー カードで関連するタブをクリックします。

## Horizon Help Desk Tool でのユーザーのトラブルシューティング

Horizon Help Desk Tool のユーザー カードを使用すると、ユーザーの基本情報を確認できます。ユーザー カードのタブをクリックすると、特定のコンポーネントの詳細が表示されます。

ユーザーの詳細が表に表示されることがあります。これらのユーザーの詳細は、表の列を使って並べ替えることができます。

- 列を昇順で並べ替えるには、列を 1 回クリックします。
- 列を降順で並べ替えるには、列を 2 回クリックします。
- 列を並べ替えない場合は、列を 3 回クリックします。

### ユーザーの基本情報

ユーザーのユーザー名、電話番号、メールアドレス、ユーザーの接続状態などのユーザーの基本情報が表示されます。ユーザーにデスクトップまたはアプリケーション セッションがある場合、ユーザーは接続状態になります。ユーザーにデスクトップまたはアプリケーション セッションがない場合、ユーザーは切断状態になります。

メールアドレスをクリックすると、ユーザーにメッセージを送信できます。

また、電話番号をクリックすると、Skype for Business セッションが開きます。ユーザーとともにトラブルシューティングを行うことができます。

---

**注:** Linux デスクトップ ユーザーには、Skype for Business の情報は表示されません。

---

### セッション

[セッション] タブには、ユーザーが接続しているデスクトップまたはアプリケーションの情報が表示されます。

[フィルタ] テキスト ボックスを使用すると、デスクトップまたはアプリケーション セッションをフィルタリングできます。

**注:** [セッション] タブには、Microsoft RDP 表示プロトコルを使用するセッションや、vSphere Client または ESXi からの仮想マシンにアクセスするセッションの情報は表示されません。

[セッション] タブには、次の情報が表示されます。

表 17-1. [セッション] タブ

オプション	説明
状態	<p>デスクトップまたはアプリケーション セッションの状態が表示されます。</p> <ul style="list-style-type: none"> <li>■ セッションが接続されている場合、緑色が表示されます。</li> <li>■ セッションがローカル セッションか、ローカルのポッドで実行されているセッションの場合、L が表示されます。</li> </ul>
コンピュータ名	<p>デスクトップまたはアプリケーション セッションの名前。名前をクリックすると、カードにセッション情報が表示されます。</p> <p>セッション カードでタブをクリックすると、次の追加情報が表示されます。</p> <ul style="list-style-type: none"> <li>■ [詳細] タブには、仮想マシン、CPU またはメモリ使用量などのユーザー情報が表示されます。</li> <li>■ [プロセス] タブには、CPU およびメモリ関連のプロセスに関する情報が表示されます。</li> <li>■ [アプリケーション] タブには、実行中のアプリケーションの詳細が表示されます。</li> </ul> <p><b>注:</b> Linux デスクトップ セッションでは、[アプリケーション] タブにアクセスできません。</p>
プロトコル	デスクトップまたはアプリケーション セッションの表示プロトコル。
Type	デスクトップの種類（公開デスクトップ、仮想マシン デスクトップまたはアプリケーション）が表示されます。
接続時間	セッションが接続サーバに接続した時間。
セッションの期間	セッションが接続サーバに接続していた期間。

## デスクトップ

[デスクトップ] タブには、ユーザーに使用資格が付与されている公開デスクトップまたは仮想デスクトップの情報が表示されます。

表 17-2. デスクトップ

オプション	説明
状態	<p>デスクトップ セッションの状態が表示されます。</p> <ul style="list-style-type: none"> <li>■ セッションが接続されている場合、緑色が表示されます。</li> </ul>
デスクトップ プール名	セッションのデスクトップ プールの名前。Linux デスクトップ セッションのデスクトップ プールとして Linux が表示されます。



オプション	説明
デスクトップ タイプ	<p>デスクトップの種類（公開デスクトップまたは仮想マシン デスクトップ）が表示されます。</p> <p><b>注:</b> セッションでポッド フェデレーションの別のポッド実行されている場合、情報は表示されません。</p>
Type	<p>デスクトップの資格のタイプが表示されます。</p> <p>■ ローカル資格の場合には、Local が表示されます。</p>
vCenter	<p>vCenter Server の仮想マシンの名前が表示されます。</p> <p><b>注:</b> セッションでポッド フェデレーションの別のポッド実行されている場合、情報は表示されません。</p>
デフォルトのプロトコル	<p>デスクトップまたはアプリケーション セッションのデフォルトの表示プロトコル。</p>

## アプリケーション

[アプリケーション] タブには、ユーザーに使用資格が付与されている公開アプリケーションの情報が表示されます。

**注:** Linux デスクトップ セッションでは、[アプリケーション] タブにアクセスできません。

表 17-3. アプリケーション

オプション	説明
状態	<p>アプリケーション セッションの状態が表示されます。</p> <p>■ セッションが接続されている場合、緑色が表示されます。</p>
アプリケーション	<p>アプリケーション プールの公開アプリケーションの名前が表示されます。</p>
ファーム	<p>セッションが接続している RDS ホストを含むファームの名前。</p> <p><b>注:</b> グローバル アプリケーション資格の場合、この列にはグローバル アプリケーション資格のファーム数が表示されます。</p>
Type	<p>アプリケーションに対する資格のタイプが表示されます。</p> <p>■ ローカル資格の場合には、Local が表示されます。</p>
パブリッシャ	<p>公開アプリケーションのソフトウェア メーカー名。</p>

## アクティビティ

[アクティビティ] タブには、ユーザーのアクティビティに関するイベント ログ情報が表示されます。過去 12 時間、過去 30 日間などの期間や管理者の名前でアクティビティをフィルタリングできます。[ヘルプデスク イベントのみ] をクリックすると、Horizon Help Desk Tool アクティビティでのみフィルタリングできます。[更新] アイコンをクリックして、イベント ログを更新します。[エクスポート] アイコンをクリックして、イベント ログをファイルにエクスポートします。

**注:** クラウド ポッド アーキテクチャ環境のユーザーのイベント ログ情報は表示されません。

表 17-4. アクティビティ

オプション	説明
[時間]	時間範囲を選択します。デフォルトは、過去 12 時間です。 <ul style="list-style-type: none"> <li>■ [過去 12 時間]</li> <li>■ [過去 24 時間]</li> <li>■ [過去 7 日間]</li> <li>■ [過去 30 日間]</li> <li>■ [すべて]</li> </ul>
[管理者]	管理者ユーザーの名前。
[メッセージ]	ユーザーまたは管理者が実行したアクティビティに固有のユーザーまたは管理者のメッセージが表示されます。
[リソース名]	アクティビティの実行対象のデスクトップ プールまたは仮想マシン名に関する情報が表示されます。

## Horizon Help Desk Tool のセッションの詳細

[セッション] タブで [コンピュータ名] オプションのユーザー名をクリックすると、セッションの詳細が [詳細] タブに表示されます。Horizon Client、仮想または公開デスクトップ、CPU とメモリの詳細を確認できます。

### Horizon Client

Horizon Client のタイプに応じて情報が表示されます。ユーザー名、Horizon Client のバージョン、クライアントマシンの IP アドレス、クライアント マシンのオペレーティング システムなどの詳細が表示されます。

**注:** Horizon Agent をアップグレードした場合、Horizon Client も最新バージョンにアップグレードする必要があります。それ以外の場合、Horizon Client のバージョンは表示されません。Horizon Client のアップグレードの詳細については、『Horizon 7 のアップグレード』ドキュメントを参照してください。

### 仮想マシン

仮想デスクトップまたは公開デスクトップに関する情報が表示されます。

表 17-5. 仮想マシンの詳細

オプション	説明
[コンピュータ名]	デスクトップまたはアプリケーション セッションの名前。
[エージェント バージョン]	Horizon Agent のバージョン。
[OS バージョン]	オペレーティング システムのバージョン。
[接続サーバ]	セッションが接続している接続サーバ。
[プール]	デスクトップまたはアプリケーション プールの名前。Linux デスクトッププールの Linux を表示します。
[vCenter Server]	vCenter Server の IP アドレス。

オプション	説明
[セッション状態]	<p>デスクトップまたはアプリケーション セッションの状態。セッションの状態は、アイドル、アクティブまたは切断です。ユーザーが 1 分間非アクティブ状態になると、セッションのステータスがアイドル状態になります。アイドル状態の場合、ステータス アイコンは緑の輪郭で表示されます。アクティブ状態の場合は緑色、切断状態は灰色で表示されます。</p> <p><b>注:</b> Linux デスクトップ セッションの場合、アイドル状態のステータスは表示されません。</p>
[セッションの期間]	セッションが接続サーバと接続していた期間。
[状態の継続期間]	セッションが同じ状態を継続した時間。
[ログイン時間]	セッションにログインしたユーザーのログイン時間。
[ログインの継続期間]	ユーザーがセッションにログインしていた期間。
[ゲートウェイ/プロキシ名]	セキュリティ サーバ、Unified Access Gateway アプライアンスまたはロード バランサの名前。この情報の表示には、セッション接続後、30 ～ 60 秒ほどかかる場合があります。
[ゲートウェイ/プロキシ IP アドレス]	セキュリティ サーバ、Unified Access Gateway アプライアンスまたはロード バランサの IP アドレス。この情報の表示には、セッション接続後、30 ～ 60 秒ほどかかる場合があります。
[ファーム]	公開デスクトップまたはアプリケーション セッションの RDS ホストのファーム。

## ユーザー操作性の評価基準

PCoIP または VMware Blast 表示プロトコルを使用する仮想または公開デスクトップ セッションのパフォーマンスの詳細が表示されます。これらのパフォーマンスの詳細を表示するには、[詳細] をクリックします。これらの詳細を更新するには、更新アイコンをクリックします。

表 17-6. PCoIP 表示プロトコルの詳細

オプション	説明
[Tx バンド幅]	PCoIP セッションの転送バンド幅（キロビット/秒単位）
[フレーム レート]	PCoIP セッションのフレーム率（1 秒あたりのフレーム数）
[パケット ロス]	PCoIP セッションのパケット ロス率。
[Skype の状態]	<p>PCoIP セッションでの Skype for Business のステータス。</p> <ul style="list-style-type: none"> <li>■ 最適化済み</li> <li>■ フォールバック</li> <li>■ 最適化済み（バージョン不一致）</li> <li>■ フォールバック（バージョン不一致）</li> <li>■ 接続中</li> <li>■ 切断されました</li> <li>■ 未定義</li> </ul> <p>Linux デスクトップ セッションの場合、このオプションは N/A と表示されます。</p>

表 17-7. Blast 表示プロトコルの詳細

オプション	説明
[フレーム レート]	Blast セッションのフレーム率 (1 秒あたりのフレーム数)。
[Skype の状態]	<p>Blast セッションでの Skype for Business のステータス。</p> <ul style="list-style-type: none"> <li>■ 最適化済み</li> <li>■ フォールバック</li> <li>■ 最適化済み (バージョン不一致)</li> <li>■ フォールバック (バージョン不一致)</li> <li>■ 接続中</li> <li>■ 切断されました</li> <li>■ 未定義</li> </ul> <p>Linux デスクトップセッションの場合、このオプションは N/A と表示されます。</p>
[Blast セッション カウンタ]	<ul style="list-style-type: none"> <li>■ [推定バンド幅 (アップリンク)]。アップリンク シグナルの推定バンド幅。</li> <li>■ [パケット損失 (アップリンク)]。アップリンク シグナルのパケット損失率。</li> </ul>
[Blast イメージング カウンタ]	<ul style="list-style-type: none"> <li>■ [送信バイト]。Blast セッションで転送されたイメージング データの合計バイト数。</li> <li>■ [受信バイト]。Blast セッションで受信したイメージング データの合計バイト数。</li> </ul>
[Blast オーディオ カウンタ]	<ul style="list-style-type: none"> <li>■ [送信バイト]。Blast セッションで転送されたオーディオ データの合計バイト数。</li> <li>■ [受信バイト]。Blast セッションで受信したオーディオ データの合計バイト数。</li> </ul>
[Blast CDR カウンタ]	<ul style="list-style-type: none"> <li>■ [送信バイト]。Blast セッションで転送されたクライアント ドライブ リダイレクトの合計バイト数。</li> <li>■ [受信バイト]。Blast セッションで受信したクライアント ドライブ リダイレクトの合計バイト数。</li> </ul>

## CPU とメモリ使用量、ネットワークとディスクのパフォーマンス

仮想/公開デスクトップまたはアプリケーションの CPU とメモリの使用量や、PCoIP または Blast 表示プロトコルのネットワークまたはディスク パフォーマンスがグラフで表示されます。

**注:** Horizon Agent デスクトップの起動または再起動後すぐに、パフォーマンス グラフにタイムラインが表示されない場合があります。数分後にタイムラインが表示されます。

表 17-8. CPU 使用率

オプション	説明
[セッションの CPU]	現在のセッションの CPU 使用率。
[ホストの CPU]	セッションが割り当てられている仮想マシンの CPU 使用率。

表 17-9. メモリ使用率

オプション	説明
[セッションのメモリ]	現在のセッションのメモリ使用量。
[ホストのメモリ]	セッションが割り当てられている仮想マシンのメモリ使用量。

表 17-10. ネットワークのパフォーマンス

オプション	説明
[遅延]	<p>PCoIP または Blast セッションの遅延がグラフで表示されます。</p> <p>Blast 表示プロトコルの場合、遅延時間はラウンドトリップ時間（ミリ秒単位）です。この遅延時間を追跡するパフォーマンス カウンタは、[VMware Blast セッション カウンタ] - [RTT] です。</p> <p>PCoIP 表示プロトコルの場合、遅延時間はラウンドトリップ遅延時間（ミリ秒単位）です。この遅延時間を追跡するパフォーマンス カウンタは、[PCoIP セッション ネットワーク統計情報] - [ラウンド トリップ遅延時間] です。</p>

表 17-11. ディスクのパフォーマンス

オプション	説明
[読み取り]	1 秒あたりの読み取りの入出力 (I/O) 操作の数。
[書き込み]	1 秒あたりの書き込み I/O 操作の数。
[ディスクの遅延時間]	ディスク遅延のグラフが表示されます。ディスク遅延は、Windows パフォーマンス カウンタから取得した入出力操作/秒 (IOPS) データの時間（ミリ秒）時間です。
[平均読み取り]	1 秒あたりのランダム読み取り I/O 操作の平均数。
[平均書き込み]	1 秒あたりのランダム書き込み I/O 操作の平均数。
[平均の遅延時間]	Windows パフォーマンス カウンタから取得した IOPS データの平均遅延時間（ミリ秒）。

## セッション ログイン セグメント

ログインの継続時間とログイン時に作成されたセグメントが表示されます。

表 17-12. セッション ログイン セグメント

オプション	説明
[ログインの継続期間]	ユーザーがデスクトップまたはアプリケーション プールをクリックしてから Windows エクスプローラが起動するまでの時間。
[セッション ログイン時間]	ユーザーがセッションにログインしていた期間。
[ログイン セグメント]	<p>ログイン時に作成されたセグメントが表示されます。</p> <ul style="list-style-type: none"> <li>■ [仲介]。接続サーバがセッションの接続または再接続を処理する時間の合計。ユーザーがデスクトップ プールをクリックしてからトンネル接続が確立するまでの時間で計算されます。ユーザー認証、マシンの選択、トンネル接続を確立に必要なマシンの準備など、接続サーバのタスクの所要時間が含まれます。</li> <li>■ [GPO のロード]Windows グループ ポリシーの処理時間の合計。グローバル ポリシーが設定されていない場合、0 が表示されます。</li> <li>■ [プロファイルのロード]Windows ユーザー プロファイルの処理時間の合計。</li> <li>■ [インタラクティブ]。Horizon Agent がセッションの接続または再接続を処理する時間の合計。PCoIP または Blast Extreme がトンネル接続を使用してから Windows エクスプローラが起動するまでの時間で計算されます。</li> <li>■ [プロトコルの接続]。ログインで PCoIP または Blast プロトコル接続の完了にかかった合計時間。</li> <li>■ [ログイン スクリプト]。ログイン スクリプトが開始してから完了するまでの合計時間。</li> <li>■ [認証]。接続サーバがセッションの認証にかかった合計時間。</li> <li>■ [仮想マシンの開始]。仮想マシンの起動にかかった合計時間。この時間には、オペレーティング システムの起動、サスペンド状態のマシンの再開、Horizon Agent が接続準備完了通知の送信にかかる時間が含まれます。</li> </ul>

トラブルシューティングでログイン セグメントの情報を使用する場合には、次のガイドラインに従ってください。

- セッションが新しい仮想デスクトップ セッションの場合、すべてのログイン セグメントが表示されます。グローバル ポリシーが設定されていない場合、[GPO のロード] のログイン セグメントの時間は 0 になります。
- 切断されたセッションから仮想デスクトップ セッションが再接続された場合には、[ログインの継続期間]、[インタラクティブ]、[仲介] のログイン セグメントが表示されます。
- セッションが公開デスクトップ セッションの場合には、[ログインの継続期間]、[GPO ロード]、[プロファイルのロード] のログイン セグメントが表示されます。新しいセッションの場合には、[GPO ロード] と [プロファイルのロード] のログイン セグメントが表示されます。これらのログイン セグメントが新しいセッションで表示されない場合には、RDS ホストを再起動する必要があります。
- セッションが Linux デスクトップ セッションの場合、[GPO のロード] と [プロファイルのロード] のセグメントは表示されません。
- デスクトップ セッションに接続した直後は、ログイン データが使用できない場合があります。数分後にログイン データが表示されます。

## Horizon Help Desk Tool のセッション プロセス

[セッション] タブで [コンピュータ名] オプションのユーザー名をクリックすると、セッション プロセスが [プロセス] タブに表示されます。

### プロセス

セッションごとに、CPU やメモリ関連プロセスの詳細情報を表示できます。たとえば、セッションの CPU やメモリ使用率が異常に高い場合、[プロセス] タブでプロセスの詳細を確認できます。

RDS ホスト セッションの場合、現在のユーザーまたはシステム プロセスが開始した RDS ホスト セッション プロセスが [プロセス] タブに表示されます。

表 17-13. セッション プロセスの詳細

オプション	説明
プロセス名	セッション プロセスの名前。たとえば、chrome.exe。
CPU	プロセスの CPU 使用率 (%)。
メモリ	プロセスのメモリ使用量 (KB)。
ディスク	メモリのディスク IOPS。次の式で計算されます。 (現在の時刻の I/O バイト数の合計) - (現在時刻より 1 秒前の I/O バイト数の合計)。 タスク マネージャに正の値が表示されている場合、この計算結果は 1 秒あたり 0 KB と表示されます。
ユーザー名	プロセスを所有するユーザーの名前。
ホストの CPU	セッションが割り当てられている仮想マシンの CPU 使用率。
ホストのメモリ	セッションが割り当てられている仮想マシンのメモリ使用量。
プロセス	仮想マシン内のプロセス数
更新	更新アイコンをクリックすると、プロセスのリストが更新されます。
プロセスの終了	<p>実行中のプロセスを終了します。</p> <p><b>注:</b> プロセスを終了するには、ヘルプデスク管理者ロールが必要です。</p> <p>プロセスを終了するには、プロセスを選択して [プロセスの終了] ボタンをクリックします。</p> <p>Windows コアのプロセスなどの重要なプロセスは終了できません。これらのプロセスも [プロセス] タブに表示される場合があります。重要なプロセスを終了しようすると、Horizon Help Desk Tool はメッセージを表示し、システム プロセスを終了できないことを通知します。</p>

## Horizon Help Desk Tool のアプリケーション ステータス

[セッション] タブの [コンピュータ名] オプションでユーザー名をクリックすると、[アプリケーション] タブでアプリケーションのステータスと詳細を確認できます。Linux デスクトップ セッションでは、[アプリケーション] タブにアクセスできません。

## アプリケーション

アプリケーションごとに、現在のステータスとその他の詳細を表示できます。

エンド ユーザーのアプリケーション プロセスを終了できます。アプリケーション プロセスを終了するには、[アプリケーションの終了] をクリックし、変更内容を確認して [OK] をクリックします。

**注:** データ保存などのユーザー操作の保留中や、その他の例外が発生した場合、アプリケーション プロセスを終了できないことがあります。ただし、アプリケーションの終了時に Horizon Help Desk Tool は成功または失敗を通知するメッセージを表示しません。

表 17-14. アプリケーションの詳細

オプション	説明
アプリケーション	アプリケーションの名前。
説明	アプリケーションの説明。
ステータス	アプリケーションのステータス。アプリケーションが実行中かどうかが表示されます。
ホストの CPU	セッションが割り当てられている仮想マシンの CPU 使用率。
ホストのメモリ	セッションが割り当てられている仮想マシンのメモリ使用量。
アプリケーション	実行されているアプリケーションのリスト。
更新	更新アイコンをクリックすると、アプリケーションのリストが更新されます。

## Horizon Help Desk Tool でのデスクトップまたはアプリケーション セッションのトラブルシューティング

Horizon Help Desk Tool では、ユーザーの接続状態に基づいて、デスクトップまたはアプリケーション セッションのトラブルシューティングを行うことができます。

### 前提条件

- Horizon Help Desk Tool を開始します。

### 手順

- 1 ユーザー カードで、[セッション] タブをクリックします。

パフォーマンス カードに CPU とメモリの使用量と、Horizon Client、仮想デスクトップ、公開デスクトップに関する情報が表示されます。



## 2 トラブルシューティングのオプションを選択します。

オプション	アクション
[メッセージを送信]	<p>公開デスクトップまたは仮想デスクトップのユーザーにメッセージを送信します。警告、情報、エラーなどのメッセージの重要度を選択します。</p> <p>[メッセージの送信] をクリックし、重要度とメッセージの詳細を入力して、[送信] をクリックします。</p>
[リモート アシスタンス]	<p>接続されているデスクトップまたはアプリケーション セッションのリモート アシスタント チケットを生成できます。管理者は、リモート アシスタンス チケットを使用してユーザーのデスクトップを操作し、トラブルシューティングを行うことができます。</p> <p><b>注:</b> Linux デスクトップ ユーザーは、この機能を使用できません。</p> <p>[リモート アシスタンス] をクリックして、ヘルプ デスク チケット ファイルをダウンロードします。チケットを開きます。リモート デスクトップでユーザーがチケットを承認するまで待機します。チケットは、Windows デスクトップでのみ開くことができます。ユーザーがチケットを承認すると、ユーザーとチャットを行い、ユーザーのデスクトップの操作を要求できます。</p> <p><b>注:</b> ヘルプ デスクのリモート アシスタンス機能は Microsoft Remote Assistance をベースにしています。公開デスクトップに Microsoft Remote Assistance をインストールし、リモート アシスタンス機能を有効にする必要があります。Microsoft Remote Assistance で接続またはアップグレードの問題が発生すると、ヘルプ デスクのリモート アシスタンスが開始しない場合があります。詳細については、Microsoft の Web サイトで Microsoft Remote Assistance のドキュメントを参照してください。</p>
[再起動]	<p>仮想デスクトップで Windows の再起動プロセスを開始します。この機能は、公開デスクトップまたはアプリケーション セッションで使用できません。</p> <p>[VDI の再起動] をクリックします。</p>
[切断]	<p>デスクトップまたはアプリケーション セッションを切断します。</p> <p>[詳細] - [切断] の順にクリックします。</p>
[ログオフ]	<p>公開デスクトップまたは仮想デスクトップでログオフ プロセスを開始します。あるいは、アプリケーション セッションでログオフ プロセスを開始します。</p> <p>[詳細] - [ログオフ] の順にクリックします。</p>
[リセット]	<p>仮想マシンのリセットを開始します。この機能は、公開デスクトップまたはアプリケーション セッションで使用できません。</p> <p>[詳細] - [仮想マシンのリセット] の順にクリックします。</p> <p><b>注:</b> 保存していない作業は失われます。</p>