

# VMware Horizon 7 バージョン 7.12 リリースノート

2020 年 3 月 17 日リリース

本リリース ノートには、次のトピックが含まれています。

- [本リリースの新機能](#)
- [ご使用前の注意事項](#)
- [利用可能な言語](#)
- [互換性に関する注意](#)
- [サポートされている Windows 10 オペレーティング システム](#)
- [Red Hat Enterprise Linux Workstation のサポート](#)
- [Horizon 7 の以前のリリース](#)
- [既知の問題](#)
- [解決した問題](#)

## 本リリースの新機能

VMware Horizon 7 バージョン 7.12 には次の新機能および機能拡張が含まれています。これらの情報をインストール可能なコンポーネント別に提供します。

- [製品の機能強化](#)
- [オンプレミスの Horizon Connection Server](#)
- [Horizon Agent for Linux](#)
- [Horizon Agent](#)
- [Horizon GPO Bundle](#)
- [Horizon Client](#)
- [Horizon 7 Cloud Connector](#)
- [VMware Cloud on AWS に展開された Horizon 7](#)

このリリースで解決された問題の詳細については、[解決した問題](#)を参照してください。

### 製品の機能強化

VMware Horizon 7 バージョン 7.12 リリースには、Horizon Connection Server および Horizon Agent の多くの新機能と拡張機能が含まれています。Horizon Console の機能パリティを構築し続けているのも含まれています。HTML5 ベース Web コンソールである Horizon Console は継続的なビルドが行われ、最終的に Horizon Administrator と入れ替わります。Horizon Administrator は 2020 年初めに廃止される予定です。

### オンプレミスの Horizon Connection Server

- [Horizon Console \(HTML5 ベースの Web インターフェイス\)](#)  
Horizon Console に、いくつかの機能強化が行われています。具体的には、次の機能が強化されています。
  - リモート セッションのタイムアウト後に行われる 2 要素認証を設定できます。『VMware Horizon Console の管理』の「[Horizon Console でのクライアント セッションのグローバル設定](#)」を参照してください。

- Horizon Console で任意のリンクをクリックすると、別の Web ブラウザ タブで Horizon Console を開くことができます。『VMware Horizon Console の管理』の「[Horizon Console へのログイン](#)」を参照してください。
  - Horizon Console ダッシュボードで、ゲートウェイとゲートウェイ以外のプロトコル セッションの数を Connection Server ごとに表示できます。『VMware Horizon Console の管理』の「[Horizon Connection Server の負荷ステータスの監視](#)」を参照してください。
  - Horizon Console ダッシュボードに、ダッシュボード統計のサマリ情報が表示されます。『VMware Horizon Console の管理』の「[Horizon 7 コンポーネントの監視](#)」を参照してください。
  - 公開アプリケーションの使用資格を持つユーザーの合計数を表示できます。『VMware Horizon Console の管理』の「[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。
  - 専用のユーザー割り当てを使用して、デスクトップ プールの各マシンに複数のユーザーを割り当てることができます。これは、フル仮想マシンを含む自動プール、手動デスクトップ プール、インスタント クローン デスクトップ プールに適用されます。詳細については、『[Horizon Console 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。
  - Horizon Client にログインするときに、デスクトップ プールの表示名ではなく、割り当てられたマシンのホスト名を表示できます。これは、すべてのデスクトップ プール タイプとグローバル資格に適用されます。詳細については、『[Horizon Console 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。
- **クラウド ポッド アーキテクチャ**
    - Horizon Console ダッシュボードの [クラウド ポッド アーキテクチャ セッション] ペインに、すべてのクラウド ポッド アーキテクチャ セッションに関する情報を表示できます。「[Horizon Console でのデスクトップとアプリケーション セッションの表示](#)」を参照してください。
    - グローバル デスクトップ資格を作成するときに [割り当て済みのマシン名を表示] を選択すると、Horizon Client にグローバル資格名ではなく、割り当てられたマシンのホスト名を表示できます。「[グローバル資格構成用ワークシート](#)」を参照してください。
    - `lmvutil --createGlobalEntitlement` コマンドと `--updateGlobalEntitlement` コマンドを使用する場合、`--displayAssignedHostName` オプションを使用すると、グローバル資格名ではなく、割り当てられたマシンのホスト名を Horizon Client に表示できます。`lmvutil --updateGlobalEntitlement` コマンドを使用する場合、`--disableDisplayAssignedHostName` オプションを使用すると、割り当てられたマシンのホスト名を Horizon Client に表示しないことを指定できます。「[グローバル資格の作成](#)」と「[グローバル資格の変更](#)」を参照してください。
    - `vdmexport.exe` を使用してグローバル LDAP をバックアップするコマンドラインが変更され、サポートされるオプションが増えました。既存のスクリプトは変更せずに使用できます。「[LDAP 構成データのエクスポート](#)」を参照してください。
  - **公開されたデスクトップおよびアプリケーション**
    - 事前起動オプションを有効にすると、ユーザーが Horizon Client でアプリケーションを開く前に、デスクトップ プールでアプリケーション セッションを起動できます。「[アプリケーション プールの手動作成用ワークシート](#)」を参照してください。
  - **仮想デスクトップ**
    - 事前プロビジョニングでのフローティング インスタント クローン デスクトップ プールの再同期または更新で MAC アドレスが保持されます。「[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。この MAC アドレスは、RDSH ファームの再同期または更新時も保持されます。
    - VMware Cloud on AWS でのシングル ホスト SDDC のサポート。「[シングル ホスト SDDC でのデスクトップ プールの作成](#)」を参照してください。
    - vSphere 7.0 での `vmCrypt` とインスタント クローンのサポート
  - **Horizon Help Desk Tool**
    - Horizon Help Desk Tool で、検索フィルタのテキスト ボックスにセッション プロセスまたはアプリケーションの名前を入力して、セッション プロセスまたはアプリケーションを名前で見つけます。「[Horizon Help Desk Tool のセッション プロセス](#)」または「[Horizon Help Desk Tool のアプリケーション ステータス](#)」を参照してください。
  - **オペレーティング システム サポート**
    - Windows 1903 以降の物理 PC のサポート。

## Horizon Agent for Linux

- サポートされている新しいディストリビューション  
Horizon Agent for Linux は、Linux リモート デスクトップでの次のオペレーティング システムを新たにサポートします。詳細については、「[Horizon 7 for Linux のシステム要件](#)」を参照してください。
  - RHEL 8.1
  - CentOS 8.1
- KDE でのセッション共同作業  
KDE デスクトップ環境を使用する RHEL 7.5 デスクトップで、セッション共同作業がサポートされるようになりました。詳細については、「[Horizon Linux デスクトップの機能](#)」を参照してください。

## Horizon Agent

- リモート エクスペリエンス
  - VMware Integrated Printing 機能が、Horizon Client for Chrome と HTML Access で機能するようになりました。「[VMware Integrated Printing の設定](#)」を参照してください。
  - VMware Integrated Printing 機能を使用すると、UPD プリンタでメディア タイプを設定できなくなります。UPD プリンタのメディア タイプを変更するには、プリンタ プロパティのパーシステンスを無効にする グループ ポリシー設定を有効にして、クライアント プリンタのメディア タイプの設定を変更します。「[VMware Integrated Printing の設定](#)」を参照してください。
  - RDSH エージェントのプリンタ名 グループ ポリシーを使用して、VMware Integrated Printing 機能で公開デスクトップと公開アプリケーションにリダイレクトされるクライアント プリンタの名前を設定できます。「[VMware Integrated Printing ポリシー設定](#)」を参照してください。
  - URL コンテンツ リダイレクト機能が、Horizon Client 5.4 for Linux 以降で動作するようになりました。Linux クライアントで URL コンテンツ リダイレクト機能を使用するには、VMware Horizon URL リダイレクト拡張機能がインストールされ、有効になっている Firefox ブラウザを使用する必要があります。「[URL コンテンツ リダイレクトの要件](#)」を参照してください。
  - URL のプロトコルについて、URL コンテンツ リダイレクト機能が Windows でサポートするアプリケーションを設定できます。「[URL コンテンツ リダイレクトのグループ ポリシー設定](#)」で URL リダイレクトのホワイトリストの構成グループ ポリシー設定を参照してください。
  - NVidia GPU を使用するプールの GPU 使用率が減少しました。

## Horizon GPO Bundle

- VMware View Agent 設定 ADMX テンプレート ファイル vdm\_agent.admx に、次の新しい設定が追加されました。
  - ウォームアップ セッションの時間制限
- VMware Horizon Client 設定 ADMX テンプレート ファイル vdm\_client.admx に、次の新しい設定が追加されました。
  - 同じサーバに接続するときに既存のクライアント インスタンスを使用する
- VMware Blast ADMX テンプレート ファイル vdm\_blast.admx に、次の新しい設定が追加されました。
  - HEVC ハイカラー精度
  - UDP プロトコル設定がセッションのログイン/ログアウト時に有効になります。以前は、この設定を有効にするために再起動が必要でした。
- VMware Integrated Printing ADMX テンプレート ファイル printerRedirection.admx に、次の新しい設定が追加されました。
  - デスクトップ以外のクライアントでプリンタ リダイレクトを無効にする
  - RDSH エージェントのプリンタ名
- URL コンテンツ リダイレクト ADMX テンプレート ファイル urlRedirection.admx に、次の新しい設定が追加されました。
  - URL リダイレクトのホワイトリストの構成

## Horizon Client

HTML Access 5.4 を含む Horizon Client 5.4 の新機能については、[Horizon Client のドキュメント](#) にあるリリースノートを参照してください。

## Horizon 7 Cloud Connector

これは VMware Horizon ユニバーサル ライセンス ユーザー向けの情報です。Horizon 7 バージョン 7.6 以降で、Horizon Cloud Service を使用して Horizon 7 ポッドを管理する場合、Horizon Cloud Connector 仮想アプライアンスが必須コンポーネントになります。

## VMware Cloud on AWS に展開された Horizon 7

VMware Cloud on AWS でサポートされる Horizon 7 の機能については、[VMware のナレッジベースの記事 KB58539](#) を参照してください。

## ご使用前の注意事項

- **VMware View Composer のインストールに関する重要事項**

View Composer 7.2 以降をインストールまたはアップグレードする場合には、Microsoft .NET Framework をバージョン 4.6.1 にアップグレードする必要があります。アップグレードしない場合は、インストールに失敗します。

- **VMware Tools のインストールに関する重要事項**

vSphere で提供されているデフォルトのバージョンではなく、VMware 製品のダウンロード ページからダウンロードされた VMware Tools バージョンをインストールする予定の場合は、その VMware Tools バージョンがサポートされていることを確認してください。サポートされる VMware Tools バージョンを特定するには、[VMware 製品の相互運用性マトリックス](#) にアクセスし、ソリューションで「VMware Horizon View」およびバージョン番号を選択してから、「VMware Tools (downloadable only)」を選択します。

- View Composer をサイレント インストールする場合、VMware のナレッジベースの記事

KB2148204「[Microsoft Windows Installer Command-Line Options for Horizon Composer](#)」を参照してください。

- この Horizon 7 リリースには、以前のリリースの一部と異なる新しい構成要件が採用されています。アップグレード手順については、『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。

- Horizon 6.2 より前の環境を Horizon 7 にアップグレードする場合、および Connection Server、セキュリティサーバ、または View Composer Server がデフォルトでインストールされた自己署名証明書を使用する場合、アップグレードを実行する前に既存の自己署名証明書を削除する必要があります。既存の自己署名証明書が残っていると、接続が機能しない場合があります。アップグレード中に、インストーラは、既存の証明書を置き換えません。古い自己署名証明書を削除すると、新しい証明書が確実にインストールされます。このリリースの自己署名証明書では、6.2 より前のリリースと比べて、より長い RSA 鍵（1024 ビットではなく、2048 ビット）と、より強力な署名（SHA-1 と RSA の組み合わせではなく、SHA-256 と RSA の組み合わせ）が使用されています。自己署名証明書は安全ではないため、できる限り速やかに CA によって署名された証明書に置き換える必要があります。また、SHA-1 はすでに安全とはみなされておらず、SHA-2 証明書に置き換える必要があります。

VMware の推奨に従い、実稼動環境で使用するためにインストールした、CA で署名された証明書は削除しないでください。CA で署名された証明書は、このリリースにアップグレードした後も引き続き機能します。

- フレッシュ インストールを実行するか、すべての Connection Server を Horizon 7 バージョン 7.2 以降にアップグレードした後は、LDAP データの保護に使用されるキーが変更されたため、Horizon 7 バージョン 7.2 より前のバージョンに Connection Server インスタンスをダウングレードすることはできません。Horizon 7 バージョン 7.2 以降へのアップグレードを計画するとき、Connection Server インスタンスをダウングレードする可能性がある場合には、アップグレードの開始前に LDAP のバックアップを実行する必要があります。Connection Server インスタンスをダウングレードする場合は、すべての Connection Server インスタンスをダウングレードし、最後にダウングレードした Connection Server に LDAP のバックアップを適用する必要があります。
- Horizon Agent のインストールで [スキャナ リダイレクト] セットアップ オプションを選択すると、ホスト

統合率に大きな影響を与えることがあります。ホスト統合を最適にするには、必要とするユーザーに対してのみ [スキャナ リダイレクト] セットアップ オプションが選択されるようにします。(デフォルトでは、Horizon Agent のインストール時に [スキャナ リダイレクト] オプションは選択されていません)。スキャナ リダイレクト機能を必要とするユーザーの場合は、個別のデスクトップ プールを設定し、そのプールでのみセットアップ オプションを選択します。

- Horizon 7 では、TLSv1.1 および TLSv1.2 のみが使用されます。FIPS モードでは TLSv1.2 のみが使用されません。vSphere パッチを適用していない場合は、vSphere に接続できないことがあります。TLSv1.0 を再度有効にする方法については、『Horizon 7 のアップグレード』ドキュメントの「[Connection Server から vCenter 接続で TLSv1 を有効にする](#)」および「[View Composer から vCenter および ESXi 接続で TLSv1 を有効にする](#)」を参照してください。
- FIPS モードは、6.2 より前のリリースではサポートされません。Windows で FIPS モードを有効にし、Horizon Composer または Horizon Agent を Horizon View 6.2 より前のリリースから Horizon 7 バージョン 7.2 以降にアップグレードすると、FIPS モード オプションが表示されません。Horizon 7 バージョン 7.2 以降を FIPS モードでインストールする代わりに、フレッシュ インストールを実行する必要があります。
- Linux デスクトップは、VMware Blast 表示プロトコル向けにポート 22443 を使用します。
- Horizon 7 バージョン 7.2 以降では、Connection Server で暗号化スイートの順序付けを適用することができます。詳細については、『Horizon 7 のセキュリティ』を参照してください。
- Horizon 7 バージョン 7.2 から、Connection Server が同じポッド内の他の Connection Server との通信にポート 32111 を使用します。インストールまたはアップグレードでこのトラフィックがブロックされると、インストールが失敗します。
- Horizon 7 バージョン 7.3.2 以降では、ポート 443 の TLS ハンドシェイクが 10 秒以内に完了します。スマート カード認証が有効な場合には、100 秒以内に完了します。以前のリリースの Horizon 7 では、どの状況でもポート 443 の TLS ハンドシェイクに 100 秒が許可されました。handshakeLifetime 設定プロパティを使用すると、ポート 443 の TLS ハンドシェイクの時間を調整できます。TLS ハンドシェイクに時間がかかるクライアントをブラックリストに自動的に追加することもできます。ブラックリストにあるクライアントからの新しい接続は、処理が開始するまでに一定期間延期され、他のクライアントからの接続が優先されます。この延期期間は変更可能です。この機能を有効にするには、secureHandshakeDelay 設定プロパティを使用します。設定プロパティの詳細については、『Horizon 7 のセキュリティ』ドキュメントを参照してください。
- リモート デスクトップ サービス ロールがない場合、Horizon Agent インストーラは、Horizon Agent を RDS モードまたはデスクトップ モードでインストールするように求めるプロンプトを表示します。

## 利用可能な言語

Horizon Administrator と Horizon Console のユーザー インターフェイス、Horizon Administrator と Horizon Console のオンライン ヘルプ、Horizon 7 製品ドキュメントは、日本語、フランス語、ドイツ語、スペイン語、中国語 (簡体字)、中国語 (繁体字)、韓国語でご利用いただけます。詳細については、[VMware Horizon 7 ドキュメント センター](#)を参照してください。

## 互換性に関する注意

- シングル ユーザー マシンおよび RDS ホストの Horizon Agent でサポートされるゲスト オペレーティング システムについては、VMware のナレッジベースの記事 KB2150295 「[Supported Windows Versions for Remote Desktop Systems for Horizon Agent](#)」を参照してください。
- 6.2 より前のバージョンの View Agent を使用する Horizon 7 サーバを使用する場合は、PCoIP 接続向けに TLSv1.0 を有効にする必要があります。バージョン 6.2 よりも古い View Agent では、PCoIP 向けのセキュリティ プロトコル TLSv1.0 のみがサポートされます。Connection Server およびセキュリティ サーバを含め、Horizon 7 サーバではデフォルトで TLSv1.0 が無効になっています。VMware のナレッジベースの記事 KB2130798 「[Configure security protocols for PCoIP for Horizon 6 version 6.2 and later, and Horizon Client 3.5 and later](#)」の操作手順に従って、これらのサーバの PCoIP 接続で TLSv1.0 を有効にできます。
- Horizon Agent でサポートされる Linux ゲスト OS については、『Horizon 7 for Linux デスクトップのセットアップ』ドキュメントの「[Horizon 7 for Linux のシステム要件](#)」を参照してください。

- Connection Server、セキュリティ サーバ、View Composer 対応のオペレーティング システムについては、『Horizon 7 のインストール』ドキュメントの「[サーバ コンポーネントのシステム要件](#)」を参照してください。
- Horizon 7 機能は、このリリースで更新された一連の Horizon Client で強化されています。たとえば、VMware Blast Extreme の接続には Horizon Client 4.0 以降が必要です。サポートされる Horizon Client については、[VMware Horizon Client ドキュメント](#) ページを参照してください。
- インスタント クローン機能には vSphere 6.0 Update 1 以降が必要です。
- Windows 7 および Windows 10 ではインスタント クローンがサポートされますが、Windows 8 または Windows 8.1 ではサポートされません。
- Horizon 7 と vSphere の現在のバージョンおよび以前のバージョンとの互換性については、『[VMware 製品の相互運用性マトリックス](#)』を参照してください。
- 対応している Active Directory Domain Services (AD DS) ドメイン機能レベルについては、『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。
- Horizon Administrator 対応のブラウザなどのシステム要件については、『Horizon 7 のインストール』ドキュメントを参照してください。
- RFC 7465 の「Prohibiting RC4 Cipher Suites」、RFC 7568 の「Deprecating Secure Sockets Layer Version 3.0」、PCI-DSS 3.1 の「Payment Card Industry (PCI) Data Security Standard」、および SP800-52r1 の「Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations」に従い、Horizon 7 コンポーネントでは RC4、SSLv3、TLSv1.0 がデフォルトで無効になっています。Connection Server、セキュリティ サーバ、View Composer または Horizon Agent マシンの RC4、SSLv3 または TLSv1.0 を再度有効にする必要がある場合には、『Horizon 7 のセキュリティ』ドキュメントの「[View で無効化された古いプロトコルと暗号化方式](#)」を参照してください。
- PCoIP 接続用に PCoIP Secure Gateway (PSG) がデプロイされている場合、バージョン 4.0 以降のゼロ クライアント ファームウェアが必要です。
- クライアント ドライブ リダイレクト (CDR) を使用しているときは、Horizon Client 3.5 以降と View Agent 6.2 以降をデプロイし、CDR データが暗号化仮想チャネル経由で外部クライアント デバイスから PCoIP セキュリティ サーバ、およびセキュリティ サーバからリモート デスクトップに送信されるようにします。これより古いバージョンの Horizon Client または Horizon Agent を展開した場合、PCoIP セキュリティ サーバへの外部接続は暗号化されますが、企業ネットワーク内でセキュリティ サーバからリモート デスクトップに送信されるデータは暗号化されません。Active Directory で Microsoft リモート デスクトップ サービス グループ ポリシーを設定すると、CDR を無効にできます。詳細については、『Horizon 7 でのリモート デスクトップ機能の構成』ドキュメントの「[クライアント ドライブ リダイレクトへのアクセスの管理](#)」を参照してください。
- Horizon Agent インストーラの [USB リダイレクト] セットアップ オプションは、デフォルトでは選択解除されています。USB リダイレクト機能をインストールするには、このオプションを選択する必要があります。USB リダイレクトを安全に使用するためのガイダンスについては、『Horizon 7 のセキュリティ』ドキュメントの「[安全な View 環境での USB デバイスの展開](#)」を参照してください。
- グローバル ポリシーのマルチメディア リダイレクト (MMR) はデフォルトで拒否に設定されます。MMR を使用するには、Horizon Administrator を開いてグローバル ポリシーを編集し、この値を明示的に許可に設定します。MMR へのアクセスを制御するために、グローバルに、または個々のプールまたはユーザーに対してマルチメディア リダイレクト (MMR) ポリシーを有効または無効にできます。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。
- Horizon Administrator で透過的なページ共有 (TPS) のレベルを設定する前に、セキュリティに与える影響について理解しておくことをお勧めします。ガイダンスについては、VMware ナレッジベース (KB) の記事 2080735、「[セキュリティの考慮事項および仮想マシン間透過的なページ共有の禁止](#)」を参照してください。
- vSphere 5.5 以降の環境で View Storage Accelerator を使用するには、デスクトップ仮想マシンは 512GB 以下でなければなりません。View Storage Accelerator は、512GB を超える仮想マシンでは無効になります。仮想マシンのサイズは、合計 VMDK 容量で定義されます。たとえば、1 つの VMDK ファイルが 512GB であるか、複数の VMDK ファイルの合計が 512GB となる場合です。この要件は、以前の vSphere リリースで作成され、vSphere 5.5 にアップグレードされた仮想マシンにも適用されます。

- Horizon 7 は vSphere Flash Read Cache (旧名は vFlash) をサポートしません。
- Horizon (with View) バージョン 6.0 以降のリリースの場合、View PowerCLI cmdlets Get-TerminalServer、Add-TerminalServerPool、および Update-TerminalServerPool は非推奨になっています。
- vSphere 6.0 以降で作成された仮想マシンでは、デフォルトで画面の DMA が無効になっています。View では画面の DMA を有効にする必要があります。画面の DMA が無効になっている場合、ユーザーがリモートデスクトップに接続すると画面が黒く表示されます。Horizon 7 でデスクトップ プールがプロビジョニングされる時、プール内の vCenter Server の管理対象となるすべての仮想マシンについて、画面の DMA が自動的に有効になります。ただし、Horizon Agent が管理対象外モード (VDM\_VC\_MANAGED\_AGENT=0) で仮想マシンにインストールされる場合、画面の DMA は有効になりません。画面の DMA を手動で有効にする方法については、VMware ナレッジベース (KB) の記事 2144475、「[仮想マシンで画面の DMA を手動で有効にする](#)」を参照してください。
- vSphere 2016 以降では、vGPU 対応のインスタント クローン デスクトップ プールがサポートされます。
- Microsoft Windows Server では、Horizon 7 環境のすべての Connection Server 間で、動的なポート範囲を指定して、ポートを開く必要があります。Microsoft Windows では、これらのポートはリモート プロシージャコール (RPC) および Active Directory レプリケーションの通常の動作で必要になります。動的ポート範囲の詳細については、『Microsoft Windows Server』のドキュメントを参照してください。
- Horizon 7 バージョン 7.2 以降の viewDBChk ツールは、vCenter Server または View Composer の認証情報にアクセスできません。この情報が必要な場合、プロンプトが表示されます。
- このリリースでは、Connection Server インスタンスとセキュリティ サーバが受信した HTTP 要求の転送ルールが変更されました。locked.properties にカスタム frontMapping エントリを定義している場合には、このエントリを削除してからアップグレードしてください。特定の Connection Server インスタンスに対する管理者接続を許可しない場合には、カスタム frontMapping エントリを定義せずに、このエントリを locked.properties に追加してください。

```
frontServiceWhitelist =
```

```
tunnel|ajp:broker|ajp:portal|ajp:misc|moved:*|file:docroot
```

セキュリティ サーバでは、このエントリが自動的に適用されるので、locked.properties に設定する必要はありません。

- Horizon Persona Management は、UIA + プロファイル テンプレートで作成されたユーザー書き込み可能ポリシーと互換性がありません。
- Horizon 7 バージョン 7.0.3 以降では、内部検証により、インスタント クローンと内部テンプレートに有効な IP アドレスが設定され、ネットワーク接続が確立しているかどうか確認されます。プロビジョニングで仮想マシンの NIC に IP アドレスが割り当てられないと、インスタントクローンのプロビジョニングに失敗します。
- Horizon 7 でサポートされている NVIDIA GPU カード モデルの詳細については、<https://docs.nvidia.com/grid/9.0/product-support-matrix/index.html> を参照してください。
- AMD v340 グラフィック カードがサポートされます。
- IPv6 環境で Real-Time Audio-Video (RTAV) がサポートされます。
- Horizon 7 と最新バージョンの VMware Unified Access Gateway、VMware Identity Manager、VMware App Volumes、VMware Dynamic Environment Manager、VMware Tools の互換性については、[VMware 製品の相互運用性マトリックス](#)を参照してください。
- JMP Server は VMware App Volumes 2.14 以降をサポートしていますが、App Volumes 4.0 はサポートしていません。JMP Server を使用するには、バージョン 2.14 以降の App Volumes 2.xx をインストールする必要があります。
- IPv6 環境の RDSH インスタント クローン プールで PCoIP はサポートされません。PCoIP は、IPv6 環境のリモート デスクトップでサポートされます。
- バージョン 18.2.7 から、Avi ネットワーク (VMware NSX Advanced Load Balancer) で Connection Server、Unified Access Gateway アプライアンス、App Volumes Manager のロード バランシングがサポートされません。
- Windows 10 2004 の Horizon では、True SSO とスマートカード ベースの SSO/ログインはサポートされていません。

# サポートされている Windows 10 オペレーティング システム

サポートされる Windows 10 オペレーティング システムの最新のリストについては、VMware のナレッジベースの記事 KB2149393「[Supported Versions of Windows 10 on Horizon 7](#)」を参照してください。

Windows 10 オペレーティング システムのアップグレード要件の詳細については、VMware のナレッジベースの記事 KB2148176「[Upgrade Requirements for Windows 10 Operating Systems](#)」を参照してください。

## Red Hat Enterprise Linux Workstation のサポート

Horizon Agent for Linux は、Red Hat Enterprise Linux Workstation を実行するシステムへのインストールをサポートします。Red Hat Enterprise Linux サーバはサポートされていません。

『[Horizon 7 for Linux デスクトップのセットアップ](#)』で、Red Hat Enterprise Linux と RHEL はすべて Red Hat Enterprise Linux Workstation を意味します。

Red Hat Enterprise Linux Workstation のサポート対象バージョンについては、[Horizon 7 for Linux のシステム要件](#)を参照してください。

## Horizon 7 の以前のリリース

以前のリリースで導入された機能は、各リリースのリリース ノートに既存の既知の問題と一緒に記載されています。

## 解決した問題

解決した問題の前に付いている番号は、VMware 内部の問題追跡システムの番号を表しています。

- Horizon Administrator で、vCenter Server から開始したリモート セッションの [セッションのログアウト] ボタンと [セッションを切断] ボタンが無効になっていません。
- Horizon Console で手動デスクトップ プールを作成するときに、[セッションのタイプ] オプションが「アプリケーション」か「アプリケーションとデスクトップ」になっていると、[空のセッションのタイムアウト (アプリケーションのみ)] フィールドが更新されません。
- VMware Cloud on AWS コンソールでセグメント名が変更されていると、インスタント クローン デスクトップ プールまたはファームを選択するときに、ポート グループまたはセグメントの新しい名前が Horizon Console に表示されません。
- 2467168：ログアウト時に個人設定の同期が完了しませんでした。
- 2485807：スナップショットの作成中に個人設定の同期が停止します。
- 2487211：個人設定ドライバ VMWVvpfsd.sys のメモリリーク。
- 2490882：共通ログ ファイル システム (CLFS) ファイルが破損している場合、C1F5 バグチェックで個人設定ドライバが失敗します。
- 2487199：メモリ不足の状態ではファイル情報を変更すると、個人設定でエラーが発生します。

## 既知の問題

既知の問題には次のトピックが含まれます。

- [Horizon Persona Management](#)
- [View Composer](#)
- [Horizon Connection Server](#)
- [Horizon Agent for Linux](#)
- [Horizon Agent](#)
- [Horizon GPO Bundle](#)
- [Horizon Client](#)
- [Horizon JMP Server と JMP Integrated Workflow 機能](#)
- [Horizon Cloud Connector](#)

## Horizon Persona Management

- ログインした後に毎回、「v6」バージョンのユーザー プロファイルを使用するゲスト OS で、最初のユーザー個人設定を個人設定管理がレプリケートするのに時間がかかります。
- 個人設定プロファイルを使用して Windows 10 LTSB マシンにログインし、クイック アクセスから Downloads や My Documents などの制限付きのフォルダにアクセスすると、次のエラーが発生します。

C:\Users\vdiuser7\Downloads を使用できません。フォルダを追加する API やクイック アクセス用のファイルは Microsoft から提供されていません。

回避策：なし

- 個人設定管理が構成された仮想マシンに 2 回目にログインすると、Microsoft Edge ブラウザがクラッシュし、OneDrive アプリケーションが使用できないことを通知するエラー メッセージが表示されます。また、ファイルとフォルダが正しくレプリケートされません。この問題は、Windows 10 ビルド 1703 以降で発生します。

回避策：個人設定管理の設定で [ローカル設定フォルダを移動] を無効にします。この設定を無効にすると、Microsoft Edge ブラウザは正常に動作しますが、最初にログインしたときだけ OneDrive アプリケーションを使用できます。

- Horizon Persona Management の設定が有効になっていると、Windows Server 2012 仮想マシンのファイルにオフライン アイコンが表示されません。

回避策：なし。

- Windows 10 バージョン 1703 CBB システムに Horizon Agent がインストールされ、Persona Management が有効になっている仮想マシンで最初のログインに成功した後、次のログイン以降で「OneDrive - 無効なイメージ エラー」というメッセージが表示されます。

回避策： Windows 10 バージョン 1703 CBB システムで OneDrive を使用しないでください。グループポリシー管理エディタで、[コンピュータの構成] > [ポリシー] > [管理テンプレート] > [VMware View Agent の構成] > [個人設定管理] > [移動と同期] フォルダの順に移動し、「ローカル設定フォルダを移動」の設定を無効にします。

- 個人設定がインストールされている Windows 10 2004 (64 ビット/32 ビット) マシンで、[スタート] メニューが機能しません。

回避策：詳細は、[KB78047](#) を参照してください。

## View Composer

- 最新の Windows 更新が適用された Windows Server 2016 で、コマンド ラインから View Composer インストーラを実行すると、Microsoft .NET 4.6 Framework エラーが発生します。CLI インストーラが Microsoft .NET 4.7 の最新バージョンを認識できないため、この問題が発生します。

回避策：View Composer インストーラのインターフェイスを使用して、インストーラを実行します。

- Windows 10 オペレーティング システムのビルド 1511 からビルド 1607 に親仮想マシンをアップグレードすると、デスクトップ プールの作成や再構成が失敗します。ビルド 1607 は、Windows 10 Anniversary Update オペレーティング システムです。

**回避策：**

- オプション 1。親仮想マシンで Windows 10 ビルド 1607 を新規にインストールします。
- オプション 2。デスクトップ プール作成ウィザードで [ディスポーザブル ファイルをリダイレクトする] を選択しないでください。

- viewdbchk.cmd -findMachine コマンドを実行すると、View Composer に接続できません。

**回避策：** View Composer の自己署名証明書を Connection Server のキーストアにインポートするか、カスタム CA 証明書を使用します。

- vSphere 6.7 のゲスト カスタマイズ ユーティリティに最近行われた変更が原因で、Horizon 7 バージョン 7.5 へのアップグレードを行う際、旧バージョンの Horizon Agent の View Composer 7.5 では Sysprep のカスタマイズ メソッドを使用したリンク クローン プールのプロビジョニングおよび再構成はできません。プロビジョニングまたは再構成を行うと、リンク クローン デスクトップおよびファームが永久にカスタマイズ状態になり、スタックします。

**回避策：** VMware Tools を最新バージョンにアップグレードし、親仮想マシンで Horizon Agent をバージョン 7.5 にアップグレードして、アップグレードした親仮想マシンのスナップショットを取ります。次に、vSphere 6.7 で Sysprep のカスタマイズ メソッドを使用して、リンク クローン デスクトップ プールのプロビジョニングまたは再構成を行います。

- Win2k12 Standard と Datacenter バージョンで、リンク クローンがカスタマイズ状態になり、スタックします。

**回避策：** この問題の修正方法については、VMware ナレッジベースの記事

<https://kb.vmware.com/s/article/57348> を参照してください。

## Horizon Connection Server

- インスタントクローンのデスクトップ プールをプロビジョニングしているときにデータ ストアに十分な空き容量がない場合、Horizon Administrator には「仮想マシン <仮想マシン名> のクローン作成が失敗しました - VC\_FAULT\_FATAL: スワップ ファイルを 0 KB から 2097152 KB に拡張できませんでした。」というエラー メッセージが表示されます。このメッセージは問題の根本原因を明確に示していません。

**回避策：** データストアの容量を増やします。

- Horizon Administrator で、[カタログ] > [デスクトップ プール] の順に移動してインスタントクローン デスクトップ プールをダブルクリックし、[インベントリ] タブに移動して [マシン (インスタント クローンの詳細)] をクリックすると、ウィンドウにインスタント クローンの詳細が表示されます。ただし、OS ディスク データ ストアの列には情報が表示されません。

**回避策：** なし

- 大規模な環境では、インスタントクローン デスクトップ プールのデスクトップの一部が無効な IP 状態になることがあります。

**回避策：** Horizon Administrator で、[プール インベントリ] に移動し、[無効な IP] 状態のデスクトップを選択して [リカバリ] をクリックします。

- デスクトップ プールにエンド ユーザー セッションが存在する仮想マシンを vCenter Server または Windows オペレーティング システムのメニューから再起動あるいはリセットすると、仮想マシンが再起動されますが、Horizon Administrator で仮想マシンのステータスが [すでに使用されています] と表示される場合があります。

この問題は、次のプール タイプで発生する場合があります。

- インスタントクローン デスクトップ プール
- [ログオフ時に削除] が有効なリンククローン フローティング デスクトップ プール。
- [ログオフ時に更新] が有効なリンククローン フローティング デスクトップ プール。
- [ログオフ時に削除] が有効なフル クローン フローティング デスクトップ プール。

**回避策：** Horizon Administrator または Horizon Client を使用して、インスタントクローン デスクトップ プール内の仮想マシンを再起動またはリセットします。仮想マシンが [すでに使用されています] の状態になっている場合は、仮想マシンを削除します。この操作では、プール プロビジョニング設定に基づいて新

しい仮想マシンが自動的に作成されます。

- ローカル データストアにインスタント クローンをプロビジョニングする場合、該当するホストをメンテナンス モードに切り替えることができません。移行されないように内部仮想マシンとインスタント クローンがローカル データストアに格納されているため、この問題が発生します。  
回避策：インスタントクローン デスクトップ プールを削除します。これにより、関連する仮想マシンが削除され、対応するホストをメンテナンス モードに切り替えることができます。
- インスタントクローンの親仮想マシンがパワーオン状態のホストに存在すると、VUM を使用する ESXi ホストの修正が失敗します。  
回避策：詳細については、VMware のナレッジベースの記事 KB2144808 [ [Entering and exiting maintenance mode for an ESXi host that has Horizon instant clones](#) ] を参照してください。
- Windows Server 2016 および Windows Server 2019 RDS ホストで、ユニバーサル Windows プラットフォーム (UWP) アプリケーションを公開アプリケーションとして使用できません。
- True SSO のため、Connection Server インスタンスと登録サーバの間の接続ステータスは、Horizon Administrator にアクセスするために使用している Connection Server のシステム健全性ステータス ダッシュボードにのみ表示されます。たとえば、Horizon Administrator に <https://server1.example.com/admin> を使用している場合、登録サーバの接続ステータスは [server1.example.com](https://server1.example.com) Connection Server についてのみ収集されます。次のメッセージのいずれかが表示されることがあります。
  - この Connection Server でのセッションを管理するためにプライマリ登録サーバと通信できません。
  - この Connection Server でのセッションを管理するためにセカンダリ登録サーバと通信できません。登録サーバ 1 つをプライマリとして構成する必要があります。セカンダリ登録サーバの構成はオプションです。登録サーバが 1 台のみの場合、最初のメッセージ (エラー) のみが表示されます。プライマリとセカンダリの登録サーバがあり、両方に接続の問題が発生している場合は、両方のメッセージが表示されます。
- それぞれに異なるテンプレートがセットアップされた CA と SubCA を含む環境で真の SSO をセットアップするときは、CA または SubCA からのテンプレートと別の CA または SubCA の組み合わせを使用して真の SSO を構成できます。その結果、ダッシュボードには真の SSO のステータスが緑色で表示されることがあります。ただし、真の SSO を使用しようとするとう失敗します。
- 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場合、Horizon Help Desk Tool にポッド名が表示されません。  
回避策：Horizon Help Desk Tool にポッド名が表示されるように、クラウド ポッド アーキテクチャ環境を設定します。
- Workspace ONE のレプリカ サーバでは、Workspace ONE モードの設定は反映されません。  
回避策：Connection Server で Workspace ONE モードを設定します。
- フル クローン デスクトップ プールを作成すると、キャッシュの問題により、不正なテンプレートが表示され、有効なテンプレートが表示されない場合があります。  
回避策：Connection Server を再起動します。
- SAML 認証を Horizon Administrator に追加しようとする、[SAML 認証子の管理] ページの [追加] ボタンが無効になります。  
回避策：管理者またはローカル管理者のロールが付与されたユーザーとして Horizon Administrator にログインします。
- クラウド ポッド アーキテクチャ環境の場合、Horizon Administrator で [インベントリ] > [セッションを検索] の順に選択しても、グローバル アプリケーション資格から事前起動されたアプリケーション セッションが表示されません。  
回避策：事前起動のセッション情報を確認するには、ホスティングするポッドの Connection Server インスタンスで Horizon Administrator ユーザー インターフェイスにログインし、[監視] > [イベント] の順に選択してください。
- Intel vDGA については、Haswell および Broadwell シリーズの Intel 内蔵 GPU のみがサポートされます。

Broadwell 内蔵 GPU は、vSphere 6 Update 1b 以降でのみサポートされます。Haswell 内蔵 GPU は、vSphere 5.5 以降でサポートされます。GPU が ESXi に認識されるには、まず BIOS で有効にする必要があります。詳細については、特定の ESXi ホストのドキュメントを参照してください。Intel 社は、BIOS のグラフィカル メモリ設定をデフォルト値の設定のままにしておくことを推奨しています。設定を変更する必要がある場合は、アパチャーの設定をデフォルト (256M) のままにします。

- NVIDIA GRID vGPU を使用するように設定された View Composer デスクトップ プールに基づいた仮想マシンのプロビジョニングが失敗し、次のエラーが表示されます。操作のために親リソース プールで利用可能なグラフィック リソースが不足しています。

**回避策：** クラスタ内の 3D レンダリングのために設定されたすべての仮想デスクトップに対して単一の vGPU プロファイルを使用します。

- vCenter Server 6.5 を含む vCenter Server 6.0 U3 以降で エラー発生時に内部親仮想マシンが別のホストに移行されます。この移行は、ターゲット ホストに不要な親仮想マシンがある場合に発生します。

**回避策：** これらの親仮想マシンを手動で削除します。詳細については、『Horizon 7 での仮想デスクトップのセットアップ』を参照してください。

- メモリ不足の可能性を低減するため、フレーム バッファが 512 MB 以下の vGPU プロファイルの場合、Windows 10 ゲスト OS でサポートされる仮想ディスプレイ ヘッドは 1 つだけです。

フレーム バッファが 512 MB 以下の vGPU プロファイルは次のとおりです。

- Tesla M6-0B、M6-0Q
- Tesla M10-0B、M10-0Q
- Tesla M60-0B、M60-0Q
- GRID K100、K120Q
- GRID K200、K220Q

**回避策：** 複数の仮想ディスプレイ ヘッドに対応し、フレーム バッファが 1 GB 以上のプロファイルを使用します。

- クライアント制限機能が有効で、一方向の Active Directory 信頼が設定されているドメインの使用資格がある場合、公開デスクトップとアプリケーション プールが起動しません。

**回避策：** なし

- アップグレード後、「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」（オブジェクト固有の権限）を含むロールが設定されていると、ファームの追加オプションが灰色になります。

**回避策：** 「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」権限を含むロールを編集するか、再度作成します。これにより、「グローバル構成とポリシーを管理」権限も追加されます。

- アップグレード後に、Workspace ONE にブックマークが表示されません。

**回避策：** Workspace ONE のカタログからブックマークを再度追加します。

- ネットワーク ケーブルを取り外して再度接続した後、クライアント マシンで [切断してログオフ] をクリックすると、リモート デスクトップが切断されず、ログオフしません。

**回避策：** 手動でリモート デスクトップのウィンドウを閉じて、リモート セッションから切断します。

- Horizon Administrator でフル仮想マシンを含む自動プールのクローンを作成しているときに、[設定内容の確認] で多くのフィールドに値が表示されません。ただし、クローン作成処理は成功します。

**回避策：** なし。

- Sysprep カスタマイズを使用してリンク クローンとフル クローンを作成すると、Windows 10 ゲスト OS でカスタマイズとドメインへの参加に失敗する場合があります。

**回避策：** これは、Microsoft Windows の問題が原因で発生します。この問題を解決するには、Microsoft ナレッジベース (KB) の次の記事にある手順に従ってください。 <https://support.microsoft.com/en-us/help/2769827>

- Horizon 7 ライセンスが設定されていないと、Horizon Console でリンク クローン デスクトップ プールまたはフォームを作成できません。  
回避策：Horizon 7 ライセンスがない場合は、Horizon Administrator でリンク クローン デスクトップ プールまたはファームを作成します。
- Internet Explorer ブラウザから Horizon Console にログインすると、アイコンではなくキーワードのみが表示されます。この問題は、DNS 名ではなく IP アドレスを使用して Connection Server またはセキュリティ サーバに接続すると発生します。  
回避策：接続するときに、IP アドレスではなく DNS 名を使用します。詳細については、VMware のナレッジベースの記事 KB2150307 (<https://kb.vmware.com/s/article/2150307>) を参照してください。
- Web ブラウザとして Safari バージョン 10.1.1 を使用し、完全修飾ドメイン名で Horizon Console にログインすると、ユーザー インターフェイスで問題が発生します。たとえば、下のパネルに何も表示されません。  
回避策：Safari バージョン 10.1.1 は、Horizon Console でサポートされる Web ブラウザではありません。バージョン 10.1.1 より前またはバージョン 11.0.2 以降の Safari を使用して Horizon Console にログインしてください。
- クラウド ポッド アーキテクチャ環境のグローバル Linux セッションで Horizon Help Desk Tool を使用すると、ユーザー インターフェイスに次の問題が発生します。
  - [詳細] タブでセッションの詳細をクリックすると、「内部エラーが発生しました」というメッセージが表示され、Skype for Business のステータスが表示されません。また、オペレーティング システムのバージョンが「-」と表示されます。
  - [リモート アシスタンス] をクリックすると、「リモート アシスタンス チケットを取得できませんでした」というメッセージが表示されます。
  - [アプリケーション] タブをクリックすると、「内部エラーが発生しました」というメッセージが表示されます。
 回避策：なし。Horizon ヘルプ デスクは、Linux デスクトップの次のユーザー インターフェイス機能をサポートしていません。Skype for Business のステータス、リモート アシスタンス、[アプリケーション] タブ、セッション アイドル状態のステータス。
- vSphere バージョン 6.7 で、VMFS6 を自動 UNMAP 機能を使用している場合、Horizon Administrator が vCenter Server の容量再利用の情報を更新しません。  
回避策：なし。
- Horizon 7 バージョン 7.5 にアップグレードした後で、インストールした最初の Connection Serverだけが登録サーバに接続できます。  
回避策：Horizon Connection Server サービスを停止し、VMware Horizon View 証明書ストアから vdm.ec というフレンドリ名を含む証明書を削除し、Horizon Connection Server サービスを再起動します。
- Firefox、Google Chrome、Microsoft Edge または Safari Web ブラウザで IP アドレスを使用して Horizon Console にログインしようとする、Horizon Console にログインできません。  
回避策：完全修飾ドメイン名 (FQDN) を使用して Horizon Console にログインします。FQDN で Web アプリケーションにログインする方法については、『Horizon 7 のセキュリティ』ドキュメントを参照してください。
- Horizon Administrator の [ユーザーとグループ] ページで、次のユーザーのユーザー名列に null/null が表示されます。Account Operators、Incoming Forest Trust Builders、Terminal Server License Servers、Windows Authorization Access Group、Server Operators、Pre-Windows 2000 Compatible Access。  
回避策：なし。
- vSphere 6.7 にアップグレードした後、バージョン 6.7 より前の vSphere で作成したカスタム仕様を使用できません。  
回避策：vSphere 6.7 にアップグレードした後、新しいカスタム仕様を作成して、その仕様をプールのプロビジョニングに使用します。

- Horizon Help Desk Tool に、仲介ポッドとホスティングするポッドの両方のログイン時間が表示されますが、これ以外のポッドのログイン時間が表示されません。仲介ポッドがリモートポッドの場合、ホスティングしているポッドのログイン時間が数分遅れて Horizon Help Desk Tool に表示されます。  
回避策：ホスティングしているポッドのログイン時間が Horizon Help Desk Tool に表示されない場合は、セッションの詳細が表示されているページを閉じます。7、8分後に [詳細] タブに移動し、セッションの詳細を再度表示します。
- VMware Identity Manager がデスクトップの起動に失敗する場合があります。Connection Server で SAML が有効になっている VMware Identity Manager に SAML 構成の詳細を初めて保存した場合、デスクトップが起動しません。  
回避策：プロファイルを再度保存し、新しいプロファイルで同期操作を実行します。同期操作は、管理者の設定に応じて 1 時間または 1 日ごとに実行されます。
- シークレットモードの Chrome で Horizon Administrator を使用しているときに、表のコンテンツを CSV 形式でエクスポートしようとする、次のエラーが表示されます。同じ名前のファイルが現在開かれているため、ファイルをエクスポートできません。ファイルを閉じて操作をやり直さか、別のファイル名を使用してください。  
回避策：通常モードの Chrome で Horizon Administrator を使用して、表をエクスポートします。
- vCenter Server 6.7 で、Sysprep を使用して Windows 10 リンク クローンをカスタマイズしているときに、プロビジョニングまたは再構成を行うと、リンク クローン デスクトップが永久にカスタマイズ状態になり、スタックします。  
回避策：vCenter Server 6.5 U2 以前を使用します。vCenter Server 6.7 が必要な場合は、Quickprep を使用してカスタマイズしてください。
- Horizon Administrator でリモート アクセス ユーザーを非認証アクセス ユーザーとして追加することはできませんが、非認証アクセス ユーザーが外部ゲートウェイからのリモート アクセスを取得することはできません。ユーザーは仮想デスクトップにアクセスできなくなり、非認証アクセス ユーザーとしてアプリケーションの起動しかできなくなります。ユーザーが通常のアクセスでログインしようすると、「Incorrect authentication type requested」エラー メッセージが表示されます。  
回避策：なし。
- 信頼認証の範囲設定を「認証の選択をします」に設定すると、Horizon シングル サインオンが実行できません。  
回避策：この問題を解決するには、次の回避方法のいずれかを行ってください。
  - ドメイン全体認証を使用します。
  - 「認証を選択をします」セキュリティ設定を引き続き使用しますが、Horizon Connection Server ホスト（ローカル システム）アカウントそれぞれに、信頼しているドメインやフォレストにあるコンピュータ オブジェクト（リソースのコンピュータ）のすべてのドメイン コントローラで、「認証を許可」権限を明示的に付与します。「認証を許可」権限を付与する方法については、Microsoft の記事『Grant the Allowed to Authenticate permission on computers in the trusting domain or forest』を参照してください。
- 混在モードのライセンス環境でクラウド ポッド アーキテクチャ機能を使用すると、RDS ライセンス サーバが同じクライアントに複数の永久ライセンスを発行する場合があります。  
回避策：なし。これはサードパーティの問題で、Horizon 7 を使用していない場合でも発生します。この問題は、Microsoft RDS ライセンス サーバがライセンスを発行する方法に関係しています。
- Horizon Administrator で、リンク クローン プールのクローンまたは vSAN データストアで作成したフル仮想マシンを含む自動プールのクローンを作成するとき、「ストレージの最適化」に「VMware Virtual vSAN を使用する」オプションが表示されません。ただし、クローン作成処理は成功します。  
回避策：なし。
- フル仮想マシンを含む自動デスクトップ プールを編集しているときにデータストアを参照すると、次の問題が発生します。

- [vCenter Server の設定] タブで [データストアを参照] をクリックすると、推奨される最小 GB 値が表示されます。
- [プロビジョニング設定] タブでマシンの最大数を増やし、[vCenter Server の設定] タブを選択して [データストアを参照] をクリックします。推奨される最小 GB 値は増えますが、この値が既存の値に追加されます。
- 3 台のマシンを含むデスクトップ プールで、1 台が使用可能な状態で、1 台がカスタマイズまたはプロビジョニング段階のときに、デスクトップ プールを編集し、[vCenter Server の設定] タブを選択して [データストアを参照] をクリックします。3 台のマシンの合計に対して推奨される最小 GB 値が表示されます。

**回避策：**フル仮想マシンを含む自動デスクトップ プールを編集するときに、推奨される最小 GB 値の正しい値を取得するには、Horizon Administrator を使用してデータストア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 プールを編集しているときにデータストアを参照すると、次の問題が発生します。
  - インスタントクローン デスクトップ プール内のすべてのマシンが使用可能な状態になった後で、デスクトップ プールを編集し、[vCenter Server の設定] タブで [データストアを参照] をクリックします。推奨される最小値 (GB)、推奨される最大値 (GB)、50% の使用率の値が正の値で表示されません。
  - インスタントクローン デスクトップ プール内のすべてのマシンが使用可能な状態になった後で、デスクトップ プールを編集し、[プロビジョニング設定] タブでマシンの最大数を増やし、[vCenter Server の設定] タブで [データストアを参照] をクリックします。推奨される最小値 (GB)、推奨される最大値 (GB)、50% の使用率の値が増えますが、これらの値が既存の値に追加されます。
  - 3 台のマシンを含むデスクトップ プールで、1 台が使用可能な状態で、1 台がカスタマイズまたはプロビジョニング段階のときに、デスクトップ プールを編集し、[vCenter Server の設定] タブを選択して [データストアを参照] をクリックします。3 台すべてのマシンに対して推奨される最小値 (GB)、推奨される最大値 (GB)、50% の使用率の値が表示されます。

**回避策：**インスタントクローン デスクトップ プールを編集しているときに、推奨される最小値 (GB)、推奨される最大値 (GB)、50% の使用率に正しい値が表示されるようにするには、Horizon Administrator を使用してデータストアを参照してください。

- フル仮想マシンを含む自動デスクトップ プールを作成するときに、2 つ以上の名前を指定し、「パワーオン状態の未割り当てのマシン数」の値にその数より少ない値を設定した場合、後でプールを編集するときに、プール作成時に指定した名前の合計数と等しい値を「パワーオン状態の未割り当てのマシン数」フィールドに入力できず、間違ったエラー メッセージが表示されます。

**回避策：**2 つ以上の名前を持つフル仮想マシンを含む自動デスクトップ プールを編集する場合は、Horizon Administrator を使用して「パワーオン状態の未割り当てのマシン数」フィールドの値を正しく更新してください。

- 多くの場合、追加の設定を行っていないブラウザで IP アドレスまたは CNAME を使用して HTML Access ポータルまたは管理コンソールの 1 つに接続を試みると、接続に失敗します。この問題が発生すると、ほとんどの場合、エラーがレポートされますが、空のエラー メッセージが表示されることがあります。

**回避策：**この問題を解決するには、『Horizon 7 のセキュリティ』の「オリジンの確認」を参照してください。

- Skype for Business を設定するときに、仲介サーバを迂回するメディア バイパスを有効にするオプションを選択できます。

Skype for Business では、PSTN ユーザーとの通話を最適化するため、メディア バイパスが有効かどうかに関係なく、メディアは常に仲介サーバを介してルーティングされます。

**回避策：**なし。メディア バイパスは Virtualization Pack for Skype for Business でサポートされていません。<https://kb.vmware.com/s/article/56977> を参照してください。

- クラウド ポッド アーキテクチャ環境で、ペアリングが必要な両方の Connection Server ポッドに同じユーザーが存在すると、Horizon Administrator で「ソース ポッド」の値が 2 と表示され、両方のポッドのユーザーがソースとなります。管理者は、両方のポッドのユーザーを編集できますが、ハイブリッド ログイン時にユーザー設定に不整合が生じることがあります。また、ユーザーのハイブリッド ログインは無効にできません。

回避策：両方のポッドからユーザーを削除し、ユーザーを再作成して、ハイブリッド ログインに設定します。

- ネストされた ESXi またはネストされた仮想 ESXi に Virtual Volumes データストアを追加すると、コアダンプ エラー メッセージが生成されます。

回避策：なし。

- vSAN データストアを検索してパーシステント ディスクをインストールするときに、Horizon Administrator と Horizon Console の両方で、実際のフォルダ名ではなく内部フォルダ名が表示されます。

回避策：なし。

- Horizon Administrator と Horizon Console の両方で、「ヘルプデスクを管理（読み取り専用）」権限のあるカスタム ロールが、グループへのアクセスに使用可能なロールとして表示されます。

回避策：なし。

- 管理者（読み取り専用）ロールを持つユーザーが、Horizon Administrator で [View 構成] > [クラウド ポッド アーキテクチャ] を表示できません。

回避策：Horizon Console を使用します。

- Horizon Administrator で、vSAN データストアを使用するリンク クローン ファームを追加または編集すると、[停電期間] が無効になります。

回避策：Horizon Console で、vSAN データストアを使用するリンク クローン ファームに停電期間を設定します。

- Horizon Administrator で、フル仮想マシンを含む自動デスクトップ プールのマシンのサマリ画面にある [再構築] ボタンが機能しません。

回避策：Horizon Administrator で、[マシン] > [vCenter Server] の順に移動して再構築機能を使用します。

- 既存の PowerShell スクリプトを使用して vCenter Server を Connection Server に追加すると、次のエラーメッセージが表示されます。「Failed to add vc instance: No enum constant com.vmware.vdi.commonutils.Thumbprint.Algorithm.SHA-1。」この問題は、Horizon 7 バージョン 7.8 で自己署名証明書の証明書オーバーライドを示す certificateEncoding プロパティが追加されたことが原因で発生します。このため、無効な SHA-1 値を使用している以前のバージョンの VMware PowerCLI スクリプトは失敗します。

回避策：SHA-1 ではなく、プロパティ値 DER\_BASE64\_PEM を使用するように PowerShell スクリプトを更新します。たとえば、set \$certificate\_override.sslCertThumbprintAlgorithm = 'DER\_BASE64\_PEM' を使用します。

- ユニバーサル Windows プラットフォーム (UWP) アプリケーションをアップグレードすると、バージョンを含むパスが変更され、元のパスでアプリケーションにアクセスできなくなります。Horizon Administrator で、アプリケーションのステータスが「使用不可」になり、ユーザーはアプリケーションを起動できません。

回避策：アップグレード後に Horizon Administrator でアプリケーションのパスを更新し、アプリケーションのステータスが「使用可能」になっていることを確認します。あるいは、アプリケーションのアップグレードを行わないでください。

- クライアント ドライブ リダイレクト機能にデバイス フィルタリングが設定されているときに、ユーザーが RDP 表示プロトコルを使用して接続すると、デバイス フィルタリングが機能しません。

**回避策：**クライアント ドライブ リダイレクトにデバイス フィルタリングが設定されている場合は、RDP 接続を許可しないように Connection Server を設定します。

- True SSO デスクトップのロック解除機能は、PCoIP および Blast プロトコルでサポートされていますが、Remote Desktop Protocol (RDP) ではサポートされません。
- 次の場合、ドメインの信頼問題が原因で、Horizon Console にユーザーまたはグループのサマリが読み込まれません。
  - ユーザーとグループが一方向の信頼ドメインに属し、ログインしている管理者が一方向の信頼ドメインから必要な権限を取得している場合。
  - ユーザーとグループが双方向の信頼ドメインに属し、ログインしている管理者が双方向の信頼ドメインから必要な権限を取得している場合。
  - ユーザーとグループが一方向または双方向の信頼ドメインに属し、必要な権限を持っている管理者が子ドメインからログインしている場合。

**回避策：**Horizon Administrator を使用して、ユーザーまたはグループのサマリにアクセスします。

- Connection Server のタイムゾーンに対して Connection Server の時間が正しく設定されていないため、Horizon Console で一部のイベントが表示されないことがあります。

**回避策：**すべてのイベントを表示するには、Horizon Administrator を使用します。

- アクティブなセッションを使用して、インスタントクローン仮想マシンをリカバリできます。この状況は、Horizon Administrator と Horizon Console の両方で発生します。

**回避策：**なし。

- Horizon Administrator と Horizon Console で、パーシステント ディスクの接続を解除した vCenter Server を削除すると、その vCenter Server から接続を解除したディスクが Horizon Administrator に表示されます。ただし、ディスクの操作はできません。Horizon Console には、接続解除されたディスクは表示されませんが、内部エラーのバナーが表示されます。

**回避策：**回避策はありません。削除する前に、vCenter Server から接続解除されたディスクがないことを確認します。

- vSphere Client for vSphere 7 で Windows 2019 OS を選択して Windows 2019 をインストールした仮想マシンが Horizon 7 で表示されないか、サポートされません。

**回避策：**vSphere Client で Windows 2016 OS バージョンを選択して、仮想マシンに Windows 2019 をインストールします。

- Horizon 7 Administrator コンソールのアイコンをクリックするか、ブラウザのアドレス バーに `https://localhost/admin` または `https://localhost/newadmin` を入力して Horizon Administrator を起動すると、`https://127.0.0.1/admin` にリダイレクトされます。この場合、IP アドレスへのリダイレクトで認証エラーが発生することがあります。詳しくは、VMware ナレッジベースの記事 KB2150307([Cannot login to a VMware Web application such as Horizon Administrator or Horizon Help Desk Tool](#)) を参照してください。

**回避策：**IP アドレスへのリダイレクトを防ぐには、ブラウザのアドレス バーに `https://localhost/admin/` を入力します (URL の最後に / を付けてください) 。

- Horizon Console で、ネイティブ NFS スナップショット テクノロジーを使用するリンク クローン デスクトッププールを複製するときに、選択した vCenter Server でディスク容量再利用が有効になっていると、最適化の詳細設定で選択した [ネイティブ NFS スナップショット (VAAI) を使用] がプールの複製ウィザードに表示されません。

**回避策：**プールの複製ウィザードで、[ネイティブ NFS スナップショット (VAAI) を使用] オプションを手動で選択します。

- グローバル アプリケーション資格に [事前起動] と [ホーム サイトを使用する] オプションを一緒に使用できません。グローバル アプリケーション資格を作成するときに、[事前起動] と [ホーム サイトを使用する] オプションの両方を有効にすると、事前起動セッションがホーム サイトから作成されないことがあります。この問題は、同じセッションが後続のアプリケーションの起動に使用され、これらのセッションがホーム サイトから起動されないことが原因で発生します。

回避策：なし。

- Connection Server のインストールまたはアンインストール中に、次のエラー メッセージが表示される場合があります。「インストール ログ ファイルを開く際にエラーが発生しました。指定したログ ファイルの場所が存在し、書き込み可能であることを確認してください。」このエラーは、サードパーティ Microsoft 製品のエラーが原因で発生します。詳細については、以下を参照してください。<https://support.microsoft.com/en-in/help/2564571/error-opening-installation-log-file-verify-that-the-specified-location>
- 回避策：Connection Server がインストールされている仮想マシンを再起動します。

## Horizon Agent for Linux

このセクションでは、Linux デスクトップの構成時または Horizon Agent for Linux で発生する可能性がある問題について説明します。

- リモート デスクトップに接続して、共同作業の UI アイコンをクリックした後で、[共同作業] ウィンドウが表示されないことがあります。

回避策：デスクトップ ウィンドウのサイズを変更するか、リモート デスクトップに再接続します。

- 2560x1600 の解像度で 4 台のモニターを vSphere 6.0 の RHEL 6.6 や CentOS 6.6 仮想マシンで構成することはサポートされていません。

回避策：2048x1536 の解像度を使用するか、この構成を vSphere 5.5 に展開します。

- [キーボード入力方法システム] が fcitx に設定されている場合、Linux エージェントのキーボード レイアウトおよびロケールはクライアントと同期しません。

回避策：[キーボード入力方法システム] を iBus に設定します。

- SSSD (System Security Services Daemon) を使用するドメインを追加すると、RHEL/CentOS 7.2 デスクトップでシングル サインオン (SSO) が機能しません。

回避策：SSSD を使用するドメインを追加した後で、VMware のナレッジベースの記事 KB2150330 [SSO configuration changes required when using SSSD to join AD on RHEL/CentOS 7.2 Desktops] の情報に従って `/etc/pam.d/password-auth` ファイルを変更します。

- スマート カード リダイレクトで認証を行ったクライアント ユーザーが Ubuntu 18.04/16.04 または SLED/SLES 12 SP 3 デスクトップに接続し、PIN を入力する前にスマート カードを取り外して再度挿入すると、デスクトップで変更が認識されません。

デスクトップでスマート カードの状態変更が検出されるのは、ユーザーが PIN の入力を求めるプロンプトを閉じた後になります。

回避策：プロンプトでスマート カードの PIN を入力し、[OK] をクリックします。または、[キャンセル] をクリックして、PIN を入力せずにプロンプトを閉じます。

- Ubuntu 16.04 では、管理者が `/etc/vmware/config` 構成ファイルで `VVC.ScRedir.Enable` を `FALSE` に設定してスマート カード リダイレクトを無効にすると、デスクトップがログイン画面でハングします。

- クライアント ユーザーが Ubuntu 18.04/16.04、SLED/SLES 12 SP 3 デスクトップに接続すると、ログイン画面に「Error 2306: No suitable token available」というメッセージが表示されます。このエラー メッセージは、クライアント システムからスマート カードが取り外されたことを意味します。ユーザーは、パスワードを入力するか、スマート カードを再度挿入して、デスクトップにログインできます。

- Ubuntu 16.04 デスクトップに接続し、スマート カード認証で誤った PIN を入力すると、スマート カードの PIN ではなく、パスワードの入力を求めるログイン プロンプトが表示されます。クライアント ユーザーは、[OK] をクリックしてパスワード入力のプロンプトを閉じることができます。新しいプロンプトが表示され、スマート カードの PIN を入力するように求められます。

- Ubuntu 18.04/16.04 と SLED/SLES 12 SP3 で、ユーザーがクライアント システムからスマート カードを取り外すと、デスクトップのスクリーンセーバーが正常に機能せず、画面がロックされません。

デフォルトでは、クライアント ユーザーがデスクトップへの認証に使用するスマート カードを取り外しても、デスクトップがスクリーンセーバーでロックされません。この条件でスクリーンセーバーを機能させるには、デスクトップに pkcs11\_eventmgr を設定する必要があります。

**回避策：**スマート カード イベントに対するスクリーンセーバーの正しい動作を pkcs11\_eventmgr に指定します。

- RHEL 7.0 デスクトップで、-m パラメータに [yes] を設定してスマート カード リダイレクトを有効にした Horizon Agent をインストール後、Horizon Administrator、Horizon Console または vSphere で黒い画面が表示されます。スマート カード リダイレクトは、RHEL 7.1 以降が実行されているデスクトップでサポートされます。この機能は RHEL 7.0 デスクトップでサポートされていません。

**回避策：**RHEL 7.1 以降が実行されているデスクトップで、スマート カード リダイレクトを有効にして Horizon Agent をインストールします。

- 解像度の異なる 2 台のモニターが構成されており、1 次画面の解像度が 2 次画面よりも低い場合は、画面の特定の領域にマウスを移動したり、アプリケーション ウィンドウをドラッグしたりできないことがあります。

**回避策：**1 次モニターの解像度が 2 次モニターと同じかそれ以上であることを確認します。

- RHEL 7 デスクトップでスマート カードを使用し、カードの取り外し時に画面をロックするオプションを有効にしていると、ユーザーがスマート カードでログインした直後に画面がロックされる場合があります。これは、RHEL 7 の既知の問題です。

**回避策：**デスクトップにアクセスするには、スマート カードでログインした後に画面のロックを解除します。

- Ubuntu デスクトップで、オペレーティング システムが gnome-shell バイナリを自動的に更新すると、シングル サインオン (SSO) が正しく機能しません。Ubuntu のデフォルト ポリシーでは、OS のアップデートが自動的にダウンロードされ、インストールされます。

**回避策：**OS のアップデートのダウンロードとインストールを自動的にではなく手動で行うように、Ubuntu のポリシーを変更します。

- エンド ユーザーがスマート カードを使用して RHEL 8.0/8.1 デスクトップにログインするときに、スマート カードの PIN ではなく、ユーザーのパスワードの入力を求めるメッセージが表示されることがあります。ネットワーク遅延が大きい場合、この問題が発生する可能性が高くなります。

**回避策：**この問題の発生を減らすには、/etc/sss/sss.conf ファイルを編集し、[pam] セクションの p11\_child\_timeout の値を大きくします。デスクトップを再起動します。

## Horizon Agent

- FIPS モードでは Horizon Agent を Connection Server とペアにできず、Horizon Agent が C ドライブ以外のドライブにインストールされている場合はプールのステータスを利用できません。

**回避策：**FIPS モードで運用する場合は、Horizon Agent を C ドライブにインストールします。

- Windows Server 2016 で Horizon Agent をアンインストールすると、使用中のアプリケーションに関する警告メッセージが表示されます。

**回避策：**Windows の [プログラムの追加と削除] を使用して Horizon Agent をアンインストールするときに

表示されるダイアログ ボックスで [無視] をクリックします。コマンド ラインから Horizon Agent をアンインストールする場合は、コマンド `msiexec /x {GUID of Agent}` の代わりにコマンド `msiexec /x /qn {GUID of Agent}` を使用します。

- Horizon Agent をアンインストールすると、マウスの速度が遅くなり、動作が不安定になります。Horizon Agent をアンインストールすると、`vmkbd.sys` ドライバも削除されます。  
回避策：Horizon Agent 仮想マシンで VMware Tools を修復します。

- Windows 7 ゲスト OS システムで Horizon Agent 7.1 から Horizon Agent 7.2 にアップグレードすると、「使用中のファイル」ダイアログが表示されます。セットアップで更新するファイルが VMware Horizon Agent アプリケーションによって使用されていることが通知されます。

回避策：[無視] をクリックして、アップグレードを続行してください。

- 「ログオフ時にマシンを削除または更新」ポリシーが有効になっていると、プロファイル管理がユーザーデータの同期を完了する前に、デスクトップが更新または削除されます。

回避策：なし

- 32 ビット版 Windows 10 で Horizon Agent インストールを実行すると、「引数が不正です」という例外がスローされ、[OK] をクリックするとインストールは続行します。このエラーは、印刷スプーラ サービスが無効の場合に発生します。

回避策：インストールを正しく実行するには、印刷スプーラ サービスを有効にします。

- 共同作業セッションで、MMR を使用して高速化している動画をセッション オーナーが表示している場合、共同作業者に動画ではなく、黒い画面が表示されます。

回避策：セッション オーナーとして共同作業セッションで動画を再生する場合、Windows Media Player または Internet Explorer で動画を再生しないでください。あるいは、共同作業が有効になっているプールで MMR を無効にしてください。

- 共同作業者がマルチモニター セッションに参加し、クライアントで相対マウス モードを有効にすると、共同作業者から見えないセカンダリ モニターにマウスが移動する可能性があります。

回避策：マウスを画面に戻します。あるいは、マルチモニター セッションで相対マウス モードを使用しないでください。

- Chrome で URL コンテンツ リダイレクトを使用しているときに、フィルタリング ルールの `https` プロトコルに `*.google.*` を設定し、Chrome のホーム ページに Google を設定すると、新しいタブを開くたびに `google.com` にリダイレクトされます。

回避策：ホーム ページまたはフィルタリング ルールを変更します。

- 共同作業セッションをセットアップするときに、双方向の信頼ドメインのメール アドレスで共同作業者を追加できません。

回避策：「ドメイン\ユーザー」の形式で共同作業者を追加します。

- HTML5 マルチメディア リダイレクトは、1803 より前の Windows 10 仮想デスクトップの Edge で機能しますが、17133 などの最新の Windows 10 1803 バージョンにアップデートすると、リダイレクトが機能しなくなります。特に、`youtube.com` などの自動再生を使用している Web サイトでこの問題が発生します。

回避策：Windows 10 仮想デスクトップを強制的に再起動します。

- クライアント セッションがアイドル状態の場合、Idle Session Timeout が GPO または GPO 以外のメソッドを使用して `MaxIdleTime` に設定されていても、公開アプリケーションは切断されません。切断警告メッセージは表示されますが、アプリケーションは切断されません。

- マルチメディア リダイレクトを使用してストリーミング メディアのシーク操作を実行すると、オーディオとビデオがスムーズに再生されません。

回避策：数分待つか、現在のストリーミング メディアを再度開きます。

- ユーザーが HTML5 マルチメディア リダイレクト機能を使用して Edge ブラウザで YouTube ビデオを再生しているときに、ビデオのバッファリングが継続し、イメージやサウンドが再生されないことがあります。

回避策：画面を更新します。

- リアルタイム オーディオビデオ機能が有効になっているときに、リモート デスクトップに接続すると、次のメッセージが表示されることがあります。「Your PC needs to be restarted to finish setting up this device: *devicename* (VDI).」

回避策：デバイスがリモート デスクトップで使用できるので、このメッセージは無視してかまいません。Windows の設定通知をオフにして、メッセージが表示されないようにすることもできます。

- 複数の高解像度モニター (4K) を使用してデスクトップに接続しているときに、新しい Blast コーデックを使用してビデオを全画面表示で再生すると、再生が低パフォーマンス (低フレーム レート) になることがあります。

回避策：全画面表示でビデオを再生する場合は、H.264 を使用します。

- エージェント グループ ポリシー設定の COM ポートの隔離モードが完全隔離 (デフォルト) に設定されているときに、Horizon Agent を RDS ホストにインストールすると、シリアル ポート リダイレクト機能でシリアル プリンタを使用できません。この問題は、Windows と Linux の両方のクライアントに影響します。この問題は、仮想デスクトップでは発生しません。

回避策：COM ポートの隔離モード グループ ポリシー設定を編集して、モードを隔離無効に変更し、Horizon Agent を再起動します。詳細については、『Horizon 7 でのリモート デスクトップ機能の構成』で「シリアル ポート リダイレクトのグループ ポリシー設定」を参照してください。

- VMware Integrated Printing 機能を使用しているときに、Windows 7 クライアント マシンから Windows 10 エージェント マシンに接続し、リダイレクトされたプリンタからデルタ フォントを含むドキュメントを出力すると、フォントが正しく表示されません。

回避策：なし。これはサードパーティの問題です。

- Windows 10 1903、Windows 10 1909 (32 ビット/64 ビット) ゲスト OS を含むリンク クローンとフル クローンの sysprep が次のエラーで失敗します。SYSRP Sysprep\_Clean\_Validate\_Opk: Audit mode can't be turned on if there is an active scenario.;; hr = 0x800F0975

回避策：次の手順をマスター イメージに適用してから、デスクトップをプロビジョニングします。<https://social.technet.microsoft.com/Forums/ja-JP/0dcdbf32-05a1-4edc-8f22-287998d30de5/sysprep-problem-audit-mode-canamp39t-be-turned-on-if-there-is-an-active-scenario?forum=win10itprosetup>

- ファイル タイプの関連付けを使用して RDSH アプリケーションを起動するには、エージェント マシンにクライアント ドライブ リダイレクト機能がインストールされ、有効になっている必要があります。

- OS を Windows 1809 から 1903 にアップデートすると、Horizon Agent に黒い画面が表示されることがあります。

回避策：この[ナレッジベースの記事](#)の手順を OS イメージに適用します。

- Horizon Agent が RDS ホストにインストールされ、VMware Integrated Printing 機能の RDSH エージェントのプリンタ名 グループ ポリシー設定でサフィックスとしてのクライアント マシン名の使用が有効になっている場合、英語のクライアント マシン名のみがサポートされます。クライアント マシン名に英語以外の文字が含まれていると、公開デスクトップと公開アプリケーションで VMware Integrated Printing 機能を使用できません。

回避策：なし。

- 5K ディスプレイ モニターのホストでバージョン 7.12 以前の Horizon Agent を実行している場合、全画面表示モードで PCoIP または Blast プロトコルを使用してリモート デスクトップに接続し、デスクトップ ウィンドウのサイズを 4K より大きくすると、リモート セッションのディスプレイがモニター画面またはウィンドウ サイズに合わせて自動的に調整されません。

回避策：デスクトップ ウィンドウのサイズを 4K より小さくします。Retina ディスプレイをサポートするデバイスの場合は、全画面表示モードを終了し、通常ディスプレイに切り替えます。

## Horizon GPO Bundle

- 再起動を必要とするコンピュータベースのグローバル ポリシー オブジェクト (GPO) がインスタント クローンに適用されません。  
回避策：VMware のナレッジベースの記事 [KB2150495](#) を参照してください。
- 第 1 レベルのデスクトップ (Horizon Client と Horizon Agent がインストールされているマシン) が仮想デスクトップで、第 2 レベルのデスクトップが公開デスクトップのネスト モード構成の場合、第 1 レベルの仮想デスクトップで「クライアント プリンタのリダイレクトに適用するフィルタを指定」グループ ポリシー設定を使用しても、第 2 レベルのデスクトップには適用されません。

回避策：第 2 レベルのデスクトップでプリンタをフィルタリングする場合には、第 2 レベルのデスクトップで「クライアント プリンタのリダイレクトに適用するフィルタを指定」グループ ポリシーを設定します。

## Horizon Client

このセクションでは、Horizon Client または HTML Access を使用してリモート デスクトップまたはアプリケーションに接続するときに発生する可能性がある問題について説明します。特定の Horizon Client プラットフォームでのみ発生する問題については、[Horizon Clients のドキュメント ページ](#)で Horizon Client リリース ノートを参照してください。

- RDS ホストで複数のユーザー セッションが実行されているときに、プロファイル データが見つかりません。セッションが切断状態でも、これらのセッションが RDS ホストのタスク マネージャに表示されていると、この問題が発生します。  
回避策：RDS ホストからセッションを削除するか、公開デスクトップまたはアプリケーションからユーザーをログオフします。
- Workspace ONE にログインしても、アプリケーションの事前起動セッションが開始しません。事前起動セッションは、Horizon Client から Connection Server へのログインに成功した場合にのみ開始します。  
回避策：事前起動が有効になっているアプリケーションを開始するには、Workspace ONE からアプリケーションまたはデスクトップを手動で開始します。
- VMware Blast 表示プロトコルを使用し、かつ Blast Secure Gateway (BSG) が無効な場合、Horizon Client は、短時間 (約 1 分) ネットワーク停止からリカバリできない場合があり、デスクトップへの接続が切断されます。この問題は、BSG が有効な場合は発生しません。  
回避策：セッションを再接続します。
- RDS ホストが、セッションで最初に起動したアプリケーションのアプリケーション データのみを保存します。後続のアプリケーションの起動データは保存されません。  
回避策：セッションからログアウトして、別のアプリケーションを起動し、そのアプリケーションのデータを保存してください。
- Windows 10 クライアント オペレーティング システムで、Internet Explorer または Microsoft Edge から HTML Access 経由で Connection Server、セキュリティ サーバまたはレプリカ サーバに接続すると、デスクトップの起動に失敗します。この問題は、Windows 10 N、Windows 10 KN、Windows 7 N、Windows 7 KN ゲスト オペレーティング システムを使用しているデスクトップに影響を及ぼします。  
回避策：Firefox または Google Chrome で HTML Access を使用します。

- Intel vDGA については、複数モニターのサポートは最大 3 台のモニターに制限されます。Intel ドライバは、解像度が最大 3840 X 2160 のモニター 3 台までしかサポートしません。4 台のモニターに接続しようとすると、1 台の画面のみが機能し、3 台には黒い画面が表示されます。
- VDI デスクトップがリモートの場所に存在し、ネットワーク遅延が大きくなると、スマート カード認証による再帰的なロック解除が機能しない場合があります。  
回避策：デスクトップのロックを手動で解除します。

- Windows 8 リモート デスクトップのユーザーが Kerberos 認証を使用してログインする場合、デスクトップはロックされ、Windows 8 がデフォルトでユーザーを表示するデスクトップのロックを解除するためのユーザー アカウントは、Kerberos ドメインからのオリジナル アカウントではなく、関連する Windows Active Directory アカウントとなります。このユーザーにはログインしたアカウントは表示されません。これは Windows 8 の問題であり、Horizon 7 自体の問題ではありません。この問題は、Windows 7 でまれに発生する場合があります。

回避策：ユーザーは「他のユーザー」を選択することでデスクトップのロックを解除する必要があります。これで Windows は正しい Kerberos ドメインを表示し、ユーザーは Kerberos ID を使用してログインできます。

- Ambir ImageScan Pro 490i を使用して、リモート デスクトップやアプリケーションでスキャンを実行するときに、ダイアログ ボックスには「Scanning… (スキャン中…)」と常に表示され、スキャンが完了しません。  
回避策：クライアントでスキャンを実行します。クライアントをスキャンすると、スキャナがキャリブレーションされます。キャリブレーション操作が終了したら、キャリブレーション ファイルを保存して、ProgramData\AmbirTechnology\ImageScanPro490i に展開します。
- Horizon 7 for Linux デスクトップの HTML Access では、Unicode キーボード入力が正しく機能しません。

回避策：なし。

- Linux デスクトップに接続するとき、一部のキーボード入力が機能しません。たとえば、クライアント デバイスとリモート デスクトップの両方で、英語以外の IME を使用している場合は、一部の英語以外のキーは正しく表示されません。  
回避策：クライアント デバイスで英語の IME を設定して、リモート デスクトップで英語以外の IME を設定します。
- Skype から Skype for Business への音声通話が正常に開始しない場合があります。Skype for Business クライアントでコールの状態が「通話を接続中…」になります。

回避策：なし。

- 非永続デスクトップ内で Skype for Business を使用すると、Skype for Business のデバイス証明書の制限 (16) を超える場合があります。この制限に達してから Skype for Business にログインを試みると、新しい証明書が発行され、最初に割り当てられた証明書が失効します。

回避策：なし。

- FIPS モードを有効にして Horizon Client 4.8 for Linux 以前を起動し、FIPS モードが有効な Horizon Agent 7.6 または Horizon Connection Server 7.6 以降に接続すると、次のエラー メッセージが表示されます。[Invalid license info for rds-license: Missing client id]

回避策：FIPS モードが有効になっている Horizon Client for Linux を使用して、FIPS モードが有効な Horizon Agent 7.6 以降または Horizon Connection Server 7.6 以降に接続する場合は、Horizon Client 4.9 for Linux 以降を使用してください。

- Unified Access Gateway、Horizon Connection Server およびセキュリティ サーバで生成されるデフォルトの自己署名 TLS サーバ証明書が、macOS 10.15、iOS 13、Chrome OS 76 で実行されている Chrome ブラウザ、Safari ブラウザまたは VMware Horizon Client で使用できない場合があります。Apple がこれらの OS バージョンで信頼済み TLS サーバ証明書の要件を変更したため、この問題が発生する可能性があります。現在、デフォルトの自己署名証明書はこの新しい要件を満たしていません。クライアントから Horizon への接続が中間のロード バランサまたは TLS を終了するプロキシを経由する場合は、これらのデバイスでも新しい証明書の要件を満たす必要があります。macOS 10.15 で Horizon Client for Mac を実行しているときに、自己署名証明書の確認が必要になり、「信頼されていないサーバに接続する前に警告する」モードを続行できないことがあります。その場合、[信頼されていないサーバ接続] ダイアログ ボックスが開き、「VMware Horizon Client は接続を確認できません。管理者にお問い合わせください」というエラー メッセージが表示され、[証明書を表示] ボタンと [接続しない] ボタンのみが使用可能になります。

**回避策：**これらの製品のデフォルトの自己署名 TLS サーバ証明書をその環境の信頼済み CA の署名付き証明書に置き換えることをお勧めします。セキュリティの面でも、この操作を行うことを推奨します。この変更を行った場合、信頼済み CA の署名付き証明書が Apple の新しい要件を満たしている限り、この問題は発生しません。macOS および iOS の Horizon Client に対する別の回避策として、サーバ証明書を検証しないように SSL 構成を行う方法もあります。Apple 証明書の要件については、<https://support.apple.com/ja-jp/HT210176> を参照してください。

## Horizon JMP Server と JMP Integrated Workflow 機能

- 複数の JMP Server がインストールされている環境で、複数の JMP Server が同じ User Environment Manager 構成共有を参照しているときに JMP 割り当てを作成または削除すると、競合が発生する場合があります。

**回避策：**なし。

- 1 つの VMware App Volumes Manager のみを使用するように JMP を構成している場合、この App Volumes Manager を参照していない Horizon Agent を含むデスクトップ プールを JMP 割り当ての作成で選択すると、このデスクトップ プールの Horizon Agent が参照する App Volumes Manager インスタンスから AppStack を選択できません。また、複数の App Volumes Manager インスタンスを使用するように JMP を構成している場合、これらの App Volumes Manager インスタンスを参照する Horizon Agent を含むデスクトップ プールを選択しても、JMP 設定に定義された別の App Volumes Manager インスタンスから AppStack を選択できます。ただし、デスクトップ プールを起動すると、他の App Volumes Manager から選択された AppStack が使用不能になります。

**回避策：**なし。

- 既存の JMP 割り当てが現在使用している AppStack の名前を App Volumes Manager で変更したり、JMP 割り当てを編集して名前を変更すると、既存の JMP 割り当てのサマリ ページに新しい AppStack 名が表示されません。

**回避策：**なし。

- 2 つの Horizon 7 インスタンスを同じ JMP Server インスタンスに登録し、同じ App Volumes Manager を使用している場合、1 つの Horizon 7 インスタンスから JMP 割り当てを削除すると、もう 1 つの Horizon 7 インスタンスの別の JMP 割り当てが使用している AppStack 割り当てが削除される可能性があります。

**回避策：**なし。

- [JMP 設定] ページで Active Directory の情報を追加または編集するときに、[バインド ユーザー名] に入力した値に 30 範囲の 3 バイト文字の中国語（「試」など）が含まれていると、Active Directory の認証でエラーが発生し、操作が失敗します。

**回避策：**管理者権限があり、30 範囲の 3 バイト文字の中国語（「試」など）を含まない別のバインド ユーザー名を Active Directory から選択します。

- [JMP 設定] ページで App Volumes Manager インスタンスの情報を追加または編集するときに、[サービス アカウント ユーザー名] に入力した値に 30 範囲の 3 バイト文字の中国語（「試」など）が含まれていると、App Volumes Manager インスタンスの認証が失敗します。

回避策：管理者権限があり、30 範囲の 3 バイト文字の中国語（「試」など）を含まない別のバインド ユーザー名を App Volumes Manager インスタンスから選択します。

- Windows 10 1703 デスクトップ プールを起動すると、VMware Dynamic Environment Manager バージョン 9.2.1 でマッピングしたドライブ マッピングの設定が表示されません。

回避策：Windows 10 1703 デスクトップ プールを起動した後、次のコマンドを実行します。

```
C:\Program Files\Immidio\Flex Profiles\FlexEngine.exe -UemRefreshDrives
```

詳細については、VMware のナレッジベースの記事 KB2113657 (<https://kb.vmware.com/s/article/2113657>) を参照してください。

- localhost を使用して Horizon Console にアクセスすると、Horizon Console の [JMP 設定] ペインに「現在、JMP Server には接続できません」というエラー メッセージが表示されます。

回避策：localhost ではなく、完全修飾ドメイン名 (FQDN) で Horizon Console にアクセスします。

- 新しい JMP 割り当てを作成しているときに、[アプリケーション] タブに次の警告メッセージが表示される場合があります。「選択したデスクトップ プールに関連付けられている App Volumes インスタンスは、登録されているいずれの App Volumes インスタンスとも一致しません。」この問題は、次のいずれかの場合に発生します。

- デスクトップ プールで使用されている App Volumes Agent が完全修飾ドメイン名 (FQDN) ではなく IP アドレスでインストールされている。
- デスクトップ プールで使用されている App Volumes Agent は FQDN でインストールされているが、App Volumes Manager インスタンスの IP アドレスが JMP 設定に登録されている。

回避策：FQDN を使用して App Volumes Agent を再インストールし、[設定 (JMP)] > [App Volumes] タブで App Volumes Manager インスタンスを登録するときに FQDN を使用します。

- VMware Horizon JMP Server のインストールで、McAfee Antivirus が NSSM.EXE を脅威として検出し、JMP Server インストーラが続行できなくなります。

回避策：JMP Server をインストールする前に、McAfee Antivirus の除外リストに次のファイルを追加します。

```
C:\Program Files (x86)\VMware\JMP\nssm-2.24\nssm-2.24\win32\nssm.exe
```

```
C:\Program Files (x86)\VMware\JMP\com\xmp\node_modules\winser\bin\nssm.exe
```

- Horizon 7 Connection Server のインストールで [ローカルの Administrator グループを許可する] オプションを選択すると、<domainName>\Administrator ではなく BUILTIN\Administrators グループが作成されます。このため、Horizon Console で JMP Server の情報を追加すると、「Horizon 権限が不足しています」というエラー メッセージが表示されます。

回避策：Horizon Administrator を使用して、フル アクセス管理者として <domainName>\administrator を登録します。 Horizon Console に再度ログインして JMP Server の情報を追加します。

- JMP 割り当ての作成中、マウスをインスタントクローン でデスクトップ プールの上に移動させると、3D レンダラ オプションに表示される値は、[vSphere Client を使用して管理] ではなく、[無効]になります。

回避策：なし。

- 信頼認証の範囲設定が「認証の選択をします」に設定されていると、JMP Server を登録できません。

**回避策：**この問題を解決するには、次の回避方法のいずれかを行ってください。

- ドメイン全体認証を使用します。
  - 「認証を選択します」セキュリティ設定を引き続き使用しますが、Horizon Connection Server ホスト（ローカル システム）アカウントそれぞれに、信頼しているドメインやフォレストにあるコンピュータ オブジェクト（リソースのコンピュータ）のすべてのドメイン コントローラで、「認証を許可」権限を明示的に付与します。「認証を許可」権限を付与する方法については、Microsoft の記事 [『Grant the Allowed to Authenticate permission on computers in the trusting domain or forest』](#) を参照してください。
- デスクトップ プールで使用されている App Volumes Manager と JMP Server で使用されている User Environment Manager のバージョンに関する情報を判定できなかったため、JMP 割り当てが期待通りに機能しません。

**回避策：**デスクトップ プールを設定するときに、[プロビジョニング設定] ペインの [デスクトップ プールのサイジング] セクションで [スペアの（パワーオンされた）マシンの数] の値を 1 以上に設定します。さらに、[プロビジョニングのタイミング] セクションで [オンデマンドでマシンをプロビジョニング] オプションをオンにした場合は、[マシンの最小数] の値を 1 以上に設定します。

- JMP Server バージョン 1.0.0.516 がインストールされているホストで JMP Server バージョン 1.0.2.x のインストーラ ファイルを実行すると、インストール プロセスが続行しません。

**回避策：**[コントロール パネル] を使用して、JMP Server バージョン 1.0.0.516 をアンインストールします。JMP Server バージョン 1.0.2.x のインストール ファイルを実行し、ウィザードに従ってインストールを完了します。インストール中に同じ SQL Server データベース情報を指定し、JMP Server バージョン 1.0.0.516 のインストールで使用したデータを保持します。

- 次の場合、JMP Server インストーラ バージョン 1.1.0.xxx で環境のアップグレードに失敗してロールバックされた後、JMP Server インスタンスが使用不能になります。
  - JMP Server 環境に SQL Server データベース証明書がなく、アップグレードで [SSL の有効化] チェックボックスが選択された。
  - Windows 認証の接続モードを選択して JMP Server のアップグレードが実行されたが、SQL Server ログイン アカウントが JMP Server ホスト システムに作成されていない。
  - [キャンセル] をクリックして、アップグレードがキャンセルされた。

**回避策：**JMP Server インストーラ バージョン 1.1.0.xxx を再度実行して、アップグレードを再度やり直してください。前の JMP Server バージョンのインストールで使用した SQL Server データベース情報を再度入力する必要があります。アップグレードに成功したら、JMP Server に設定したすべての証明書がそのまま残っていることを確認します。インストールが失敗したり、キャンセルされた場合、証明書が変更されている可能性があります。

- Dynamic Environment Manager (DEM) 構成共有を追加しようとする、次のエラーが発生する場合があります。  
runOne] Error running file\_share.createFileShare { code: 400,\n took: 221,\n data: {},\n error: 'Unable to create file share <fileshare-unc-path>.'

DEM 共有構成のパスワードに、次のいずれかの文字が含まれていると、DEM 構成共有に失敗します。 “ #+;,<>=^`

**回避策：**次の使用可能な文字をパスワードに使用します。 !\$%&'()\*-./:?@[^\_`{|}

## Horizon Cloud Connector

- HTML5 ベースの vSphere Web Client を使用して、Horizon Cloud Connector 仮想アプライアンスの OVA ファイルをデプロイすると、次のエラーが発生します。「プロパティ proxySsl の指定された値 [false] が無効です。OVF パッケージのデプロイに失敗しました。」

**回避策：**Flex ベースまたは Flash ベースの vSphere Web Client を使用して、Horizon Cloud Connector 仮想アプライアンスの OVA ファイルをデプロイします。

- Horizon Cloud Connector を起動すると、`[[FAILED] Failed to start Wait for Network to be Configured.See 'systemctl status systemd-networkd-wait-online.service' for details.]` というメッセージが表示されます。

このメッセージは誤って表示されています。ネットワークに問題は発生していません。メッセージを無視して、通常どおり Horizon Cloud Connector を使用できます。