



VMware Horizon 6 バージョン 6.2.3 リリースノート

リリース日：2016 年 7 月 21 日

最終更新日：2017 年 4 月 18 日

本リリース ノートには、次のトピックが含まれています。

- [このリリースの Horizon 6 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](#)
- [解決した問題](#)
- [既知の問題](#)

このリリースの Horizon 6 の新機能

- VMware Horizon View 6.2.3 はメンテナンス リリースです。前のリリースのいくつかの既知の問題が解決されています。詳細については、[解決した問題](#)を参照してください。
- [ユーザー名を記憶する] のチェックボックスを非表示にして、管理者のログイン名を記憶しないように View Administrator を設定できます。詳細については、[KB 2145405：ログイン名を記憶しないように View Administrator を構成](#)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 6.2.3 をインストールまたはアップグレードする場合は、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。
- Horizon 6 リリースには、過去のリリース版とは別の新しい構成要件が採用されています。『[Readme](#)』ドキュメントをお読みください。この短い概要は、このリリースのインストールまたはアップグレード時に起こる可能性のある潜在的なトラブルを防ぐのに役立ちます。『View アップグレード』ドキュメントにはアップグレード手順が説明されています。
- View 6.2 より前のバージョンのインストール環境をアップグレードする場合、およびデフォルトでインストールされた自己署名証明書の Connection Server、セキュリティ サーバ、または View Composer サーバを使用する場合、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。自己署名の証明書を削除するには、VMware ナレッジベース (KB) の記事 2146256、[「Removing a Self-Signed Certificate in View \(View における自己署名証明書の削除\)」](#) のガイドラインに従ってください。

- Virtual SAN 6.1、GRID vGPU、Virtual Volumes などの Horizon 6 の機能を利用するには、vSphere 6.0 およびそれ以降のパッチリリースをインストールしてください。
- デバイスの Client Access License (CAL) 別 RDS を使用する展開の場合、エンドユーザーが RDS のデスクトップとアプリケーションへの接続を開始する前に、KB 2076660、[「View のデバイス CAL 別 RDS 管理」](#) の構成ガイドラインに従います。
- 今回のリリースにアップグレードするときは、『View アップグレード』ドキュメントに記載されているように、View Agent をアップグレードする前に、ポッドにあるすべての View Connection Server インスタンスをアップグレードしてください。
- このリリースのダウンロード ページには、VADC (View Agent Direct-Connection) を使用して HTML Access をサポートする Web サーバの静的なコンテンツを提供する Horizon View HTML Access Direct-Connection ファイルがあります。HTML Access の VADC 向けのセットアップの詳細については、『View Agent Direct Connection プラグイン管理』ガイドの[「HTML Access のセットアップ」](#)を参照してください。
- View 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、View 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特定のユーザーには、別のデスクトップ プールを構成し、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。
- 今回のリリースに含まれる View Agent インストーラから、[変更] オプションが削除されました。この View Agent バージョンをインストールした後でカスタム セットアップ オプションを変更するには、View Agent をアンインストールしてから再インストールする必要があります。パッチおよびアップグレードの場合、前のバージョンをアンインストールすることなく、新しい View Agent インストーラを実行して、新しいオプション セットを選択できます。
- FIPS モードでは、TLS 1.2 を使用する必要があります。FIPS モードで View をインストールすると、TLS 1.2 をサポートしない vSphere 5.x に接続できなくなります。
- 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 モードを有効にしており、6.2 より前のリリースの View Composer または View Agent を、6.2.3 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。View 6.2.3 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。
- このリリースでは、Linux デスクトップで Blast プロトコルに使用されるポートが 22443 になります。Horizon View 6.1.1 以前では、このポートは 5443 でした。

利用可能な言語

View Administrator ユーザー インターフェイス、View Administrator オンライン ヘルプ、Horizon 6 製品ドキュメントは、日本語、フランス語、ドイツ語、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 6 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 View Agent でサポートされているゲスト OS については、『View のインストール』ドキュメントの[「View Agent でサポートされるオペレーティング システム」](#)を参照してください。
- View Agent 6.1.x などの古いバージョンの View Agent と一緒に Horizon 6.2.3 サーバを使用しており、View Administrator で PCoIP Secure Gateway が有効になっている場合には、サーバの PCoIP 接続で TLS 1.0 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、セキュリティ プロトコル TLS 1.0 のみがサポートされます。Connection Server およびセキュリティ サーバを含む Horizon 6.2.3 サーバでは、PCoIP 接続について TLS 1.0 がデフォルトで無効になっています。KB 2130798 の「[Horizon 6 バージョン 6.2 以降および Horizon Client 3.5 以降向けの PCoIP のセキュリティプロトコルの構成](#)」の操作手順に従ってこれらのサーバで PCoIP 接続について TLS 1.0 を有効にできます。

- デフォルトでは、View コンポーネントの TLS 1.1 および TLS 1.2 が有効です。TLS 1.0 は、vSphere 5.x をサポートするために送信接続で有効になっていますが、受信接続では無効です。vSphere のバージョンが 6.x、または 5.5 U4 以降である場合、送信接続では TLS 1.0 を無効にすることをお勧めします。『View セキュリティ』ドキュメントの「[View Connection Server インスタンスまたはセキュリティ サーバでのセキュリティ プロトコルおよび暗号化スイートの構成](#)」を参照してください。
- TLS 1.2 が有効になっていない Horizon Client を使用する場合は、TLS 1.2 を有効にできます。『Horizon Client および Agent のセキュリティ』ドキュメントの「[セキュリティ プロトコルと暗号化スイートの構成](#)」を参照してください。クライアントを簡単にはアップグレードまたは再設定できない場合は、View Connection Server またはセキュリティ サーバへの受信接続で TLS 1.0 を再度有効にできます。『View セキュリティ』ドキュメントの「[View Connection Server インスタンスまたはセキュリティ サーバでのセキュリティ プロトコルおよび暗号化スイートの構成](#)」を参照してください。
- View コンポーネントでは、RC4 と SSLv3 がデフォルトで無効になっています。これは、RFC 7465 の「RC4 暗号スイートの使用禁止」および RFC 7568 の「Secure Sockets Layer バージョン 3.0 の非推奨」に従うものです。View Connection Server、セキュリティ サーバ、View Composer、または View Agent マシンの、RC4 または SSLv3 を再度有効にする必要がある場合は、『View 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。
- View Agent でサポートされる Linux ゲスト OS については、『Horizon 6 for Linux デスクトップのセットアップ』ドキュメントの「[Horizon 6 for Linux のシステム要件](#)」を参照してください。
- View Connection Server、セキュリティ サーバ、および View Composer でサポートされるゲスト OS については、『View 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 6 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、IPv6、および RDS デスクトップおよびホスト型アプリケーションへのストレージ デバイスの USB リダイレクトには、Horizon Client 3.3 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。
- View と VMware 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。vSphere 5.5 および 5.1 では、次の特定の最小 Express パッチが推奨されます。
 - Express パッチ 4 以降を適用済みの vSphere 5.5 Update 1a
 - Express パッチ 5 以降を適用済みの vSphere 5.1 Update 2
- サポートされる Active Directory Domain Services (AD DS) ドメイン機能レベルについては、『View 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。
- View Administrator と View Portal でサポートされるブラウザなどのシステム要件については、『View のインストール』ドキュメントを参照してください。
- 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 View Agent をデプロイすると、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データがセキュリティ サーバからリモート デスクトップに送信されるときに、暗号化が行われません。
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、『View でのデスクトップ プールとアプリケーション プールの設定』ドキュメントの「[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。
- View 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、『View セキュリティ』ドキュメント

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、View Administrator を開き、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。
- View 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、KB 記事「[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 \(2080735\)](#)」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 6 は vSphere Flash Read Cache (旧名は vFlash) をサポートしません。
- 今回のリリースの Workspace Portal で、製品名が Workspace Portal から VMware Identity Manager に変更されます。Horizon 6 バージョン 6.2 のドキュメントでは Workspace Portal として参照されますが、VMware Identity Manager もサポートされます。
- 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。
- キオスク モードのクライアントは、クラウド ポッド アーキテクチャの実装ではサポートされません。

以前のリリースの View

以前のリリースの View 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

今回のリリースでは、次の問題が解決されています。

- 6.2.3 より前の Horizon View 6.x リリースでは、Trend Micro の OfficeScan がインストールされていて個人設定管理が有効になっているデスクトップで、ユーザーの初回ログイン後、以降のログインが長時間よろこ画面で停止する問題が発生します。この問題は、リリース 6.2.3 以降では解決されています。ただし、View が 6.2.3 にアップグレードされる前にデスクトップにログインしたことがあるユーザーは、View が 6.2.3 にアップグレードされた後初めてログインするときに、引き続き長い遅延が発生することになります。この状態は、初回ログイン時に発生します。以降のすべてのログインでは、遅延は発生しません。この問題は、リリース 6.2.3 よりも前のデスクトップにログインしたことがないユーザーには影響しません。
- VMware Identity Manager を使用して、Microsoft ネットワーク ロード バランサで設定した View 環境から仮想デスクトップを起動すると、認証エラーが発生します。
- VMware View Persona Management バージョン 6.2 がインストールされている物理ワークステーションまたは仮想マシンで、ネットワーク共有フォルダから実行 (.exe) ファイルを管理者権限で実行すると、エラーメッセージが表示されます。
- クライアント ドライブ リダイレクト (CDR) 機能を使用して Horizon Client からデスクトップにファイルをコピーすると、コピーしたファイルでデータが破損する場合があります。
- 信頼するフォレストの子ドメインにデスクトップが含まれている場合、信頼するフォレスト アカountのシングル サインオン (SSO) が失敗します。
- 再構成後、デスクトップ仮想マシンは、予期せずにメンテナンス モードになり、それが継続され、ユーザーはデスクトップが使用できなくなります。

- 安全なトンネルを有効にしてクライアント ドライブ リダイレクト (CDR) またはファイル関連付けを使用すると、Horizon Client とリモート デスクトップ マシン間で CDR データを転送するときにパフォーマンスの問題が発生する場合があります (ファイル関連付けは、リモート アプリケーションでローカル ファイルを開く機能です)。
- AMD vDGA では、クライアント ウィンドウのサイズが解像度 640x480 未満に変更されると Autofit 機能が機能しなくなります。
- Windows Media MMR は、ビデオ メモリのリードバック パフォーマンスが遅い特定の AMD モデルなど、特定のグラフィック カードでは適切に動作しません。
- RHEL デスクトップまたは CentOS デスクトップがスクリーンセーバ モードの場合、スクリーンセーバ設定でロック画面が無効になっていると、View SSO が無効になり、Horizon Client や View Administrator から切断およびログオフできません。この問題が起きるのは、[システム] -> [環境設定] -> [スクリーンセーバ] を選択してから、[コンピュータがアイドルのときはスクリーン セーバを有効にする] を選択し、[スクリーン セーバが有効のときは画面をロックする] を選択解除したときです。
- C ドライブ以外のドライブで FIPS モードを有効にして View Connection Server 6.2.2 をインストールすると、View Administrator Web ページに、ページを表示できないというエラーが表示されます。
- View Persona Management で Windows 2012 R2 サーバの共有フォルダの場所を検証しようとする、64 ビット Windows 10 ゲスト OS へのログインが停止する場合があります。
- 「Disable synchronization of data with Google (Google とのデータの同期を無効にする)」という Google グループ ポリシーが有効な場合、ユーザーのプロファイルをレプリケートできないことがあります。
- Horizon View Client にログインしてから 55 分～ 1 時間後に、クライアント ドライブ リダイレクトのドライブが表示されなくなり、Windows エクスプローラーでこれらのドライブにアクセスできなくなります。ドライブにアクセスするには、Windows エクスプローラーを閉じてから再び開く必要があります。
- View 6.1.1 から View 6.2.1 にアップグレードした後に、Blast Secure Gateway が有効になっている場合、NodeJS が変更されたために、複数のユーザーがデスクトップから切断される場合あり、その場合でも Horizon Client にはエラー メッセージが表示されません。
- Delphi でコーディングされたリモート アプリケーションを最小化すると、そのアプリケーションが Windows タスクバーに表示されなくなります。「Send updates for empty or offscreen windows (空またはオフスクリーンウィンドウの更新を送信)」という名前のホスト型アプリケーション GPO を有効にすると、この問題が解決されます。
- デスクトップでの再構成または更新操作が完了するまで時間がかかるか失敗し、Universal File Access (UFA) サービスがシャットダウン状態のままになります。
- PCoIP または Blast 表示プロトコルを使用してリボン スタイル アプリケーションをリモート アプリケーションとして起動すると、アプリケーションが最小化後に表示されなくなる、ドロップダウン メニューが完全にはレンダリングされないなど、表示の不整合が発生します。
- View 6.0.2 および 6.2 では、ThinPrint ドライバが原因で、印刷したドキュメントにフォーマットやフォントの問題が発生します。
- 仮想マシンを通常のデスクトップ プールに追加すると、View Administrator に仮想マシンのステータスが「エージェントの待機」と表示され、このステータスが変更されません。
- View Persona Management フォルダのファイル パスがすべて大文字に変更され、大文字と小文字を区別するアプリケーションが正しく機能しなくなります。
- View Persona Management プロファイルが同期されていてフォルダ リダイレクトが有効な 32 ビットまたは 64 ビットの Windows 10 デスクトップにエンド ユーザーがログインすると、マイ ドキュメント フォルダのフォルダ リダイレクトが失敗します。
- Active Directory の単一の AltSecuristyIdentities エントリは View と Outlook Web Access などの Microsoft アプリケーションの両方で同時に使用することはできません。これは、スマート カード証明書の [サブジェクト] や [発行者] フィールドに Surname や GivenName 属性が表示される場合、Microsoft アプリケーションによってマップされる同じ文字列に、これらの属性がマップされないためです。
- Horizon 6 の以前のリリースでは、Windows 10 は ThinApp のゲスト OS としてサポートされていませんでした。現在 Windows 10 は ThinApp 5.2.2 のゲスト OS としてサポートされています。

既知の問題

既知の問題には次のトピックが含まれます。

- 操作のインストール、アップグレード、アンインストール
- RDS のデスクトップとアプリケーション
- Access Point
- 構成および View Administrator
- Horizon Client およびリモート デスクトップ エクスペリエンス
- Horizon 6 for Linux デスクトップ
- Windows Media MMR
- 3D グラフィックス アクセラレーション
- スマート カード
- クライアント ドライブ リダイレクト
- スキャナ リダイレクト
- シリアル ポート リダイレクト
- View Persona Management
- vSphere プラットフォームのサポート
- View Composer
- Windows 10 および Windows 8.x のサポート
- Windows Server デスクトップの使用
- Workspace Portal の統合
- Virtual SAN と Virtual Volumes
- クラウド ポッド アーキテクチャ
- その他

操作のインストール、アップグレード、アンインストール

- Windows Server 2012 または 2012 R2 で稼動している RDS ホストで View Agent 6.1.1 を View Agent 6.2.x にアップグレードすると、「内部エラー 25030」というメッセージが表示され、アップグレードが失敗します。

回避策：View Agent 6.1.1 をアンインストールして、RDS ホストを再起動し、View Agent 6.2.x をインストールします。

- View Agent を手動デスクトップ プールのデスクトップにインストールすると、USB HUB デバイス ドライバが正しくインストールされない場合があります。View Agent インストールの際、USB HUB デバイス ドライバが完全にインストールされる前にシステムを再起動すると、この問題が起こる可能性があります。

回避策：View Agent をインストールし、システムの再起動を促すダイアログが表示された場合、USB HUB デバイス ドライバ ソフトウェアのインストールが実行されていないか、システム トレイを調べてください。デバイス ドライバ ソフトウェアのインストールが完了（通常 30 秒程度）するまで、システムを再起動しないでください。

コマンドライン スクリプトを使用して View Agent をサイレント インストールする場合、システムを再起動する前に、ドライバのインストールが完了するようにスクリプトを十分待機またはスリープさせるようにしてください。

View Agent をインストールした後もこの問題が解決しない、またはサイレント インストールでシステムの再起動をディレイできない場合、以下の手順で USB HUB デバイス ドライバをアップデートしてください。

1. デバイス マネージャの [その他のデバイス] で、[VMware View 仮想 USB ハブ] を右クリックします。

2. [ドライバ ソフトウェアのアップデート] > [ドライバ ソフトウェアをコンピュータで参照する] をクリックします。

3. C:\Program Files\VMware\VMware View\Agent\bin\drivers にアクセスし、[Next (次へ)] をクリックすると、Windows がドライバをインストールします。

- Windows 8 から Windows 8.1 にデスクトップをアップグレードするには、View Agent をアンインストールし、Windows 8 から Windows 8.1 にオペレーティング システムをアップグレードして、View Agent を再インストールします。代わりに、Windows 8.1 を新規インストールしてから View Agent をインストールできます。

- 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。
- View Agent 5.1.x 以前から現行の View Agent バージョンにマスター イメージをアップグレードすると、リンク クローン イメージで USB リダイレクトが失敗します。View Agent 5.2 以降から現行バージョンにアップグレードした場合、この問題は発生しません。
回避策：「[KB 2062215: View Agent 5.3 にアップグレードした後に、リンク クローン イメージで USB リダイレクトが失敗する](#)」を参照してください。
- View Agent インストーラを Windows 8 の仮想マシンで実行しているときに、ビデオ ドライバをインストールすると、Windows デスクトップに何も表示されなくなります。インストールが正常に完了する前に Windows デスクトップが数分間黒い画面になる場合があります。
回避策：View Agent をインストールする前に、2013 年 5 月の Windows 8.0 のロールアップを適用します。[Microsoft 社のサポート技術情報 2836988](#) を参照してください。
- Windows 8.1 または Windows Server 2012/2012 R2 仮想マシン（RDS ホストまたは VDI デスクトップとして展開された）で View インストーラを実行すると、インストーラの処理が完了するまで膨大な時間がかかる場合があります。仮想マシンのドメイン コントローラまたは階層内にある他のドメイン コントローラが応答していない、またはこれらのコントローラに接続できない場合に、この問題が発生します。
回避策：ドメイン コントローラに最新のパッチが適用済みで、十分な空きディスク領域があり、互いに通信できることを検証します。
- RDS ホストから View Agent をアンインストールすると、エラー ダイアログが表示され、アンインストール操作を完了できません。このダイアログには、アンインストール操作で RDS ビデオ ドライバを停止できなかったと表示されます。この問題は、切断したデスクトップ セッションが RDS ホストでまだ実行されているときに発生します。
回避策：RDS ホストを再起動し、View Agent のアンインストールを完了します。ベスト プラクティスとしては、すべての RDS セッションをログオフしてから View Agent をアンインストールします。
- View 6.2.x の View Connection Server のホット パッチをデプロイするときに、コントロール パネルの [プログラムと機能] アプレットで VMware Horizon 6 HTML Access の正しい VMware アイコンではなく汎用のアイコンが表示されます。これは表示上の問題であり、HTML Access の機能には影響はありません。
回避策：Connection Server の以前のバージョンをアンインストールしてから、ホット パッチをインストールします。
- Windows Server 2008 を実行している RDS ホストで View Agent 6.2 を View Agent 6.2.x にアップグレードするときに、VMware Horizon View Agent および Server Manager アプリケーションを閉じてから [再試行] をクリックして続行するように求めるメッセージが表示される場合があります。このメッセージを無視して、[再試行] をクリックしても問題はありません。アップグレードは、正常に実行されます。
回避策：不要。
- View Agent のサイレント インストールでは、Flash URL リダイレクト機能をインストールできません。
回避策：View Agent インストーラが Flash URL リダイレクト機能をインストールできるようにするには、サイレント インストールに `VDM_FLASH_URL_REDIRECTION=1` プロパティを含める必要があります。
例：`VMware-viewagent-x86_64-6.2.1-3284564.exe /a /s /v"/qn VDM_VC_MANAGED_AGENT=1 VDM_FLASH_URL_REDIRECTION=1 ADDLOCAL=Core,SVIAgent,ThinPrint,USB,HTMLAccess,FlashURLRedirection,RTAV"`
- 転送プロトコルとして TLS 1.2 をサポートする View Composer データベースを使用している場合、View Composer 6.2.3 のインストールに失敗します。
回避策：View Composer をインストールするマシンで、TLS 1.2 をサポートするデータベース クライアント パッチを適用します。
- FIPS モードでは View Agent を View Connection Server とペアにできず、View 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、View Agent を C ドライブにインストールします。

RDS のデスクトップとアプリケーション

- RDS ロールが有効な Windows Server 2012 親仮想マシンから、自動化されたファームをデプロイすると、デプロイされたリンク クローン仮想マシンで Sysprep カスタマイズが失敗します。このサードパーティの

問題は、RDS ロールが有効な他のバージョンの Windows Server では発生しません。

回避策：<https://support.microsoft.com/en-us/kb/3020396> で入手可能な Microsoft ホットフィックスを Windows Server 2012 親仮想マシンに適用します。

- 単一の RDS ホストに対して複数の接続を連続して確立すると、何人かのユーザー（たとえば、120 ユーザーのうちの 1 ユーザーまたは 2 ユーザー）が RDS デスクトップ セッションの起動や再起動を行えなくなることがあります。

回避策：RDS ホストの vCPU 数と RAM サイズを増やします。

- RDS ロールが RDS ホストに構成されてからの日数が 120 日を超えていて、これまで接続をしたことがない場合、RDS デスクトップまたはアプリケーションへの最初の接続が失敗します。この問題は RDP のみで発生します。

回避策：数秒待ってから再度 RDS デスクトップまたはアプリケーションに接続します。

- Microsoft の推奨に従って、場所ベースのプリンタの永続設定が、プリンタ ドライバの DEVMODE の拡張部分ではなく、プライベート領域に保存されている場合、設定はサポートされません。

回避策：ユーザー環境設定がプリンタ ドライバの DEVMODE 部分に保存されたプリンタを使用してください。

- View Agent は、物理マシンである RDS ホストに仮想印刷機能をインストールできません。仮想マシンである RDS ホストに View Agent がインストールされている場合は、RDS デスクトップで仮想印刷がサポートされます。

回避策：仮想マシンに RDS ホストを構成し、View Agent をインストールします。

- PCoIP で RDS デスクトップに接続する単一クライアント デスクトップは、デバイスの Client Access License (CAL) ごとに複数の RDS を使用することがあります。この問題は、ユーザー CAL 別の RDS が使用される展開の場合、クライアントが RDP を介して View に接続する場合、あるいはライセンス サーバを 1 つだけ展開し、すべての RDS ホストが同じゲスト オペレーティング システムで実行される場合には発生しません。

回避策：エンドユーザーが RDS のデスクトップとアプリケーションへの接続を開始する前に、KB 2076660、「[View のデバイス CAL 別 RDS の管理](#)」の構成ガイドラインに従います。

- Windows Server 2008 R2 SP1 RDS ホストで実行されているデスクトップ セッションでは、Windows Media Player で H.264 ビデオ ファイルやビデオ ファイルのある AAC オーディオを再生できません。これは既知のサードパーティの問題です。

回避策：[Microsoft KB 記事 2483177](#) にアクセスし、Windows Server 2008 R2 のデスクトップ エクスプレス デコーダー更新パッケージをダウンロードします。

- Windows Server 2012 R2 RDS ホストで実行されているデスクトップ セッションで Chrome ブラウザを使って YouTube を再生すると、動画の表示が乱れることがあります。たとえば、黒い箱がブラウザ ウィンドウに表示されます。この問題は他のブラウザや Windows Server 2008 R2 SP1 RDS ホストでは発生しません。

回避策：Chrome ブラウザで、[Chrome] > [設定] > [詳細設定表示] > [システム] の順に選択し、[ハードウェア アクセラレーションが使用可能な場合は使用する] の選択を解除します。

- Windows 2008 R2 SP1 物理 RDS ホストで実行されているデスクトップでビデオを再生し、メインのモニターから別のモニターにビデオの表示を移す場合、ビデオの再生が停止、または映像フレームの更新が停止します（音声は引き続き再生されることがあります）。この問題は仮想マシン RDS ホストまたはシングル モニター構成では発生しません。また、Windows Server 2008 R2 SP1 でのみ発生します。

回避策：ビデオはメイン モニターでのみ再生します。または、RDS デスクトップ プールを仮想マシン RDS ホスト上に構成します。

- リモート アプリケーションを起動して応答しなくなったので別のアプリケーションを起動すると、2 つ目のアプリケーションのアイコンがクライアント デバイスのタスクバーに追加されません。

回避策：最初のアプリケーションが応答するまで待機します。（たとえば、大量のファイルが読み込まれている場合、アプリケーションが応答しないことがあります。）最初のアプリケーションが応答しないようであれば、RDS 仮想マシンでアプリケーション プロセスを強制終了します。

- 2013 年 2 月の更新プログラムがインストールされておらず、Windows Server 2012 R2 を実行中の RDS ホストでホストされているアプリケーション Lync 2013 は、起動すると、「Microsoft Lync は動作を停止しました」というエラー メッセージが表示された後、すぐにクラッシュします。これは、Lync 2013 の既知の問題です。

回避策：Lync の 2013 年 2 月の更新プログラムを適用してください。更新プログラムは、[Microsoft 社の](#)

Access Point

- スマート カード認証の Access Point 2.0 は、テック プレビュー機能です。つまり、テスト環境でスマート カード認証を使用できますが、本番環境では使用できません。また、このテック プレビュー機能ではテクニカル サポートを利用できません。
スマート カード認証を使用する場合、スマート カードは必須です。スマート カードをオプションとして設定すると機能しません。
- Access Point がスマート カード認証を使用するように構成され、View Connection Server のアイドル セッション タイムアウトも設定されている場合、アイドル セッション タイムアウト時間が経過した後、再ログインができなくなります。たとえば、アイドル セッション タイムアウトが 3 分に設定され、3 分を超えてセッションをアイドル状態のまま放置した場合、セッション タイムアウト ダイアログ ボックスが表示されて、[続行] をクリックすると、スマート カードの PIN ではなく Active Directory の認証情報の入力を求められます。Active Directory の認証情報を入力しても、ステータスが「認証しています...」と表示され、フリーズします。
回避策：スマート カード認証を使用する予定の場合は、アイドル セッション タイムアウトを構成しないでください。
- View Administrator を使用してログイン前メッセージを構成した場合、スマート カード認証は機能しません。View Administrator でログイン前メッセージを構成した場合、スマート カード認証を使用してログインし、ログイン前メッセージを確認するように求められたとき、メッセージの確認後にログイン前メッセージが再表示されます。
回避策：スマート カード認証を使用する予定の場合は、ログイン前メッセージを構成しないでください。
- Access Point REST 管理 API の使用時、「/v1/config/settings」リソースを使用して認証設定を更新できません。
回避策：特定の認証方式用のリソースを使用します（「/v1/config/authmethod/certificate-auth」など）。
- コマンドラインの VMware OVF Tool またはデプロイ ウィザードを使用して Access Point アプライアンスをデプロイするとき、DNS アドレスは 1 つだけ入力する必要があります。複数のアドレスを入力すると、DNS 解決が機能しません。
- View Edge 設定「blastEnabled」を False に設定した場合、HTML Access を使用してリモート デスクトップおよびアプリケーションにアクセスできなくなります。一般的に、Access Point は DMZ にデプロイされているため、「blastEnabled」オプションを True に設定するとこの問題は発生しません。
回避策：「blastEnabled」を False に設定して HTML Access も使用する場合は、「proxyPattern」オプションも「/1/portal(.*)」に設定する必要があります。
- Horizon 6 バージョン 6.2.3 では、View Connection Server で SAML 認証を有効にした後は、SAML メタデータは生成されません。次のような View Connection Server のサービス プロバイダ メタデータの URL にアクセスするときに、「404 ページが見つかりません」というエラーが表示されます。
`https://connectionserver.example.com/SAML/metadata/sp.xml`。
回避策：サービス プロバイダの SAML メタデータを生成するには、VMware ナレッジベース (KB) の記事 2146390、「[Service Provider Metadata Generation fails for Horizon 6 version 6.2.3 \(Horizon 6 バージョン 6.2.3 でサービス プロバイダのメタデータの生成が失敗する\)](#)」に記載されているガイドラインに従ってください。

構成および View Administrator

- Firefox ブラウザから View Administrator を使用するとき、韓国語 IME (Input Method Editor) を使用してテキスト フィールドにハングル文字を入力する場合、ハングル文字が正しく表示されません。この問題は Firefox のみで発生します。これはサードパーティの問題です。
回避策：別のブラウザを使用します。引き続き Firefox を使用するのであれば、ハングル文字を 1 文字ずつ入力します。
- View Connection Server インスタンスで VMware View Blast Secure Gateway (absg.log) のログ レベルを

Info から Debug に変更すると、ログ レベルは Info のままになります。(View Connection Server インスタンスの Set View Connection Server Log Levels (View Connection Server ログ レベルの設定) を開き、absg ログ レベルを変更し、VMware View Blast Secure Gateway サービスを再起動して、ログ レベルを変更します。) Debug から Info へのログ レベルの変更は、正常に機能します。

回避策：なし。

- View PCoIP ADM (pcoip.adm) グループ ポリシー設定 [Configure SSL connections to satisfy Security Tools (Security Tools を満たすために SSL 接続を構成)] はこのリリースの View ではサポートされません。このグループ ポリシー設定で特定のオプションの実装を試みると、View 展開で予期しない結果が発生する場合があります。

回避策：このリリースの View ではこの設定を使用しないでください。

- [Configure the TCP port to which PCoIP Server binds and listens (PCoIP Server がバインドおよびリッスンする TCP ポートを構成)] または [Configure the UDP port to which PCoIP Server binds and listens (PCoIP Server がバインドおよびリッスンする UDP ポートを構成)] グループ ポリシーを構成中にリトライ ポート範囲のサイズを 0 に設定すると、PCoIP ディスプレイ プロトコルでデスクトップにユーザーがログインする時に接続に失敗します。Horizon Client から「このデスクトップの表示プロトコルは現在使用できません。システム管理者にお問い合わせください」というエラー メッセージが返されます。グループ ポリシーのヘルプ テキストに、ポート範囲は 0 ～ 10 であると間違って表示されます。

注：RDS ホストでは、デフォルト ベースの TCP と UDP ポートは 4173 です。PCoIP が RDS ホストで使用されるとき、ユーザー接続ごとに別個の PCoIP ポートが使用されます。リモート デスクトップ サービスによって設定されるデフォルトのポート範囲は、同時ユーザー接続の予想される最大数に対応できる十分な大きさです。

回避策：

シングルユーザー マシンの PCoIP：リトライ ポート範囲を 1 ～ 10 の範囲で設定します。(正しいポート範囲は、1 ～ 10 です)。

RDS ホストの PCoIP：ベスト プラクティスとして、これらのポリシー設定を利用して RDS ホストのデフォルト ポート範囲を変更しないでください。また、TCP や UDP のポート値をデフォルトの 4173 から変更しないでください。最も重要なことは、TCP または UDP ポート値を 4172 に設定しません。この値を 4172 にリセットすると、RDS セッションの PCoIP のパフォーマンスに悪影響を与えます。

- イベント データベースのシステム健全性ステータスが、「存在しないか、権限がないため、'VE_user_events' 表示をドロップできません」というエラー メッセージと共に、View Administrator のダッシュボードに赤色で表示されることがまれにあります。この状態は、実際のエラーを示しているわけではないため、少し時間が経った後に自然に解決されます。

回避策：なし。

Horizon Client およびリモート デスクトップ エクスperiエンス

- Linux クライアント 2.3.4 が Horizon 6.0.1 View Agent に接続しており、リモート デスクトップの状態が「使用可能」である場合（「切断」でない）、デスクトップとクライアントの間のクリップボード リダイレクトは機能しません。この問題は、「View PCoIP の一般的なセッション変数」グループ ポリシーの設定 [クリップボード リダイレクトの構成] が、「どちらの方向も有効」に設定されている場合でも発生します。

回避策：デスクトップから切断してから再接続するか、Linux クライアントをバージョン 3.1 にアップグレードします。

- View Connection Server のサーバ名または FQDN (完全修飾ドメイン名) に ASCII 以外の文字が使用されている場合、Horizon Client は View Connection Server に接続できません。

回避策：なし。

- デスクトップが PCoIP を使用して接続され、複数のモニターを使用するよう構成されている場合、ユーザーが Microsoft PowerPoint 2010 または 2007 でスライド ショーを再生すると（解像度を指定し、2 台目のモニターでスライドを再生する）、各スライドの一部分が各モニターに表示されます。

回避策：ホスト クライアント システムで、2 台目のモニターの画面解像度を希望する解像度にサイズ変更します。View デスクトップに戻り、2 台目のモニターでスライド ショーを開始します。

- デスクトップが PCoIP を使用して接続されている場合、ユーザーが Microsoft PowerPoint 2010 または 2007 でスライド ショーを再生し、解像度を指定すると、スライドは指定した解像度で再生され、現在の解像度に合わせて拡大・縮小されません。

回避策：再生解像度で「現在の解像度を使用」を選択します。

- 仮想印刷機能は、View Agent からインストールしたときのみサポートされます。VMware Tools でインストールしてもサポートされません。
- デスクトップの Windows Media Player でビデオを再生する場合、PCoIP 切断が特定の状況で発生する場合があります。

回避策：デスクトップで、Windows レジストリを開いて、64 ビット Windows では

HKLM\Software\Wow6432Node\Policies\Teradici\PCoIP\pcoip_admin_defaults レジストリ キー、または 32 ビット Windows では

HKLM\Software\Policies\Teradici\PCoIP\pcoip_admin_defaults レジストリ キーに移動します。pcoip.enable_tera2800 DWORD レジストリ値を追加して、その値を 1 に設定します。

- RDS ホストでホストされている Windows 2008 R2 SP1 デスクトップ プールでは、言語同期設定（クライアントからゲストまで）がデフォルトでオンになっており、オフにすることはできません。そのため、View Agent の「PCoIP ユーザー デフォルト入力言語の同期をオンにする」グループ ポリシーを無効にしても、影響はありません。リモート デスクトップ言語はクライアント システムで使用される言語と常に同期します。

回避策：なし。

Horizon 6 for Linux デスクトップ

- ゲスト OS のログイン プロセスが完了する前に Linux デスクトップから切断する場合、デスクトップ プール設定「切断後に自動的にログオフ」が「直後」または 5 分未満の待機時間が設定されていても、View Agent for Linux は 5 分以上経ってからログオフします。

回避策：ログイン プロセスが完了してから Linux デスクトップから切断します。

- RHEL デスクトップまたは CentOS デスクトップをスクリーンセーバ モードのときにサイズ変更すると、黒い画面が表示され、「[ロック解除] ダイアログが表示されません。

回避策：ESC キーを押します。

- 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。

- 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。

- vDGA 環境にある RHEL 6.6 仮想マシンで 2560x1600 の解像度の 2 台以上のモニターを構成する場合、デスクトップのパフォーマンスが低下します。たとえば、アプリケーション ウィンドウがスムーズに移動しなくなります。この問題は、RHEL のデスクトップ効果を有効にしている場合に発生します。

回避策：[System（システム）] > [Preference（環境設定）] > [Desktop Effects（デスクトップ効果）] に移動し、[Standard（標準）] を選択して、[Desktop Effects（デスクトップ効果）] を無効にします。

Windows Media MMR

- Windows Media MMR が Windows 10 デスクトップで機能しません。

回避策：なし

- リダイレクトされたビデオを Internet Explorer で再生しているときに、ブラウザのタブを切り替えと、ビデオ ウィンドウの一部が、ブラウザ ウィンドウの後ろまたは横で表示され続けます。この問題が発生するのは、Windows 7 デスクトップのみです。

回避策：Windows 8.1 デスクトップを使用してください。または、リダイレクトされたビデオを再生しているときに、別のタブに切り替えしないでください。

3D グラフィックス アクセラレーション

- 3D レンダリングと vSGA が有効なマシンで 4K モニターが構成されている場合、Windows Media Player ウィンドウの移動、サイズ変更、または全画面表示モードへの切り替えが非常に遅くなる場合があります。

す。この問題は、2D、ソフトウェア 3D レンダリング、または解像度が 2560x1440 のモニターでは発生しません。

回避策：なし

- デスクトップ プールをデプロイするために親またはテンプレートとして使用する仮想マシンに NVIDIA ドライバがインストールされている場合、この仮想マシンを ESXi ホストの非 NVIDIA GRID ハードウェアにデプロイすると、デスクトップ セッションを正常に開始できない場合があります。この問題は、仮想マシンが以前 NVIDIA GRID vGPU デプロイで使用されていた場合に起きることがあります。

回避策：仮想マシンから NVIDIA ドライバを削除した後、スナップショットまたはテンプレートを作成して、デスクトップ プールをデプロイします。

- NVIDIA ドライバ バージョン 347.25 を使用するように構成された Windows 7 仮想マシン上で vDGA が有効になっていると、デスクトップ セッションが切断されることがあります。この問題は、Windows 8.1.x クライアントまたは他の NVIDIA ドライバ バージョンでは発生しません。

回避策：NVIDIA ドライバ バージョン 347.25 を使用しないでください。

- Windows 8/8.1 デスクトップで、3D スクリーンセーバーが [3D レンダラー] 設定が無効な場合でも動作し、正しく表示されません。この問題は Windows 7 デスクトップでは発生しません。

回避策：エンドユーザーが 3D スクリーンセーバーを使用したり、デスクトップ プールの [3D レンダラー] 設定を有効にしたりすることがないようにしてください。

スマート カード

- スマート カードを使用して RDS デスクトップにログインすると、シングルユーザーの VDI デスクトップの場合よりも時間がかかります。この問題は、Windows クライアントでは他のクライアントに比べて深刻ではありません。

回避策：なし。

- Windows 7 クライアント マシンで、スマート カードの削除ポリシーがトリガーされたときに、Horizon Client が終了します。
- View Client 5.4.2（実行ファイルは wswc.exe）を実行しているユーザーは、スマート カード認証を使用してログオンできません。

回避策：Horizon Client 3.0 以降をインストールし、実行します。

クライアント ドライブ リダイレクト

- Microsoft リモート デスクトップ サービス グループ ポリシー設定でクライアント ドライブ リダイレクトを無効にしても（[ドライブのリダイレクトを許可しない] を選択しても）、Horizon Client で [オプション] > [フォルダを共有] オプションを選択して、共有ドライブを選択できます。ドライブは共有されず、リモート デスクトップには表示されません。View Agent をインストールするときにクライアント ドライブ リダイレクト オプションをインストールしていない場合、この問題は発生しません。

回避策：なし。

スキャナ リダイレクト

- スキャナ リダイレクトを Windows 10 デスクトップで使用すると、Microsoft の [Windows Fax とスキャン] が機能しません。

回避策：別のスキャン アプリケーションを Windows 10 デスクトップで使用するか、他のデスクトップ プラットフォームに変更します。

- View 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。デフォルトでは、View 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。

回避策：ほとんどのユーザーで [スキャナ リダイレクト] セットアップ オプションが選択解除されていることを確認します。スキャナ リダイレクト機能を必要とする特定のユーザーには、別のデスクトップ プールを構成し、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。

- スキャナ設定が WIA スキャナで有効にならないことがあります。たとえば、グレースケール モードを選択して、元画像の領域の一部を選択すると、スキャナはカラーを使用して、画像全体をスキャンすることがあります。

回避策：TWAIN スキャナを使用してください。

- 一部の環境では、別の WIA スキャナに切り替えると、元のスキャナから画像がスキャンされ続けることがあります。

回避策：View デスクトップ セッションからログオフしてください。新しいデスクトップ セッションを起動して、選択したスキャナを使用してスキャンを実行します。

- スキャナ リダイレクト機能がインストールされた状態で View Agent をアンインストールすると、実行中のアプリケーションをすべて閉じるようにアンインストール プロセスによって指示されます。

回避策：なし。View Agent のアンインストールを続行する前に、表示されたアプリケーションを閉じる必要があります。

シリアル ポート リダイレクト

- バンド幅制限のグループ ポリシー設定が有効になりません。この設定でユーザーが入力した値は無視され、既存のバンド幅がシリアル ポートのリダイレクトで使用されます。消費されるバンド幅は、同時に使用されるシリアル ポート デバイスの数と、各デバイスで使用するボーレートによって異なります。

回避策：なし。

View Persona Management

- View Persona Management では、デスクトップ仮想マシンのディスク容量が非常に少なくなっている場合、ユーザーの個人設定が中央リポジトリに正しくレプリケートされない可能性があります。
- View Persona Management を使用すれば、グループ ポリシー設定を使用して、ユーザー プロファイル フォルダをネットワーク共有にリダイレクトできます。フォルダがリダイレクトされると、ユーザー セッション中にすべてのデータがネットワーク共有に直接保存されます。Windows のフォルダ リダイレクトには [ユーザーに *folder-name* に対する排他的権限を与える] というチェックボックスがあり、リダイレクトされるフォルダにユーザー固有の排他的権限を与えます。セキュリティ対策のため、このチェックボックスはデフォルトで選択されています。このチェックボックスを選択すると、管理者はリダイレクトされたフォルダにアクセスできません。管理者がユーザーのリダイレクトされたフォルダに対するアクセス権を強制的に変更しようとする、そのユーザーに対して View Persona Management が機能しなくなります。

回避策：「[KB 2058932: View Persona Management のためにリダイレクトされたフォルダへのアクセスをドメイン管理者に与える](#)」を参照してください。

- View Persona Management は、RDS ホストで実行されているセッションベースのデスクトップ プールではサポートされません。

回避策：シングルユーザー マシンで実行される自動または手動のデスクトップ プールに View Persona Management をインストールします。

- まれに、個人設定管理が有効になっていると、ユーザーがログインした後にクイック起動ツールバーのアイコンが正しく表示されません。

回避策：ログアウトして再びログインします。

vSphere プラットフォームのサポート

- View Storage Accelerator が、大きな仮想ディスク（たとえば、100 GB の仮想ディスク）のダイジェスト ファイルを生成または再生成するのに長時間かかる場合があります。その結果、デスクトップは予想より長い時間に渡ってアクセスできなくなることがあります。

回避策：ダイジェスト再生成操作が許可されている場合、ブラックアウト期間を使用して制御してください。また、これらの操作の頻度を削減するためにダイジェストの再作成間隔を使用してください。代わりに、非常に大きい仮想マシンが含まれるデスクトップ プールの View Storage Accelerator を無効にしてください。

- リンク クローン プールが vSphere 5.5 仮想マシンで構成されている場合、View Composer 再調整操作は `FileAlreadyExists` エラーで失敗する場合があります。この問題は、View Composer デスクトップ プールで OS ディスクとユーザー データ ディスクに異なるデータストアが使用され、View Composer 再調整操作の実行前にユーザー データ ディスク用に選択されていたデータストアが変更された場合に限って発生します。

回避策：`FileAlreadyExists` エラーがあるリンク クローン デスクトップから通常ディスクを切り離し

ます。後で、アーカイブしたディスクを新しい仮想マシンに接続してリンク クローン デスクトップを再作成するか、セカンダリ ディスクとして既存のリンク クローン デスクトップに接続できます。OS ディスクとユーザー データ ディスクを同じデータストアに保持するか、View Composer 再調整操作の前にデータストアの選択を変更しないことにより、この問題の発生を回避できます。

- vSphere 5.5 にアップグレードした後に、領域を効率的に利用する仮想ディスクを使用し、1 台の ESXi ホストにつき 200 以上のリンク クローン仮想マシンがある場合、ヒープ サイズ エラーが発生する場合があります。例: Error: Heap seSparse could not be grown by 12288 bytes for allocation of 12288 bytes(エラー: 12288 バイトの割り当てに対して、ヒープ seSparse を 12288 バイト拡張できませんでした)

回避策: 領域を効率的に利用する仮想ディスクを使用するリンク クローン仮想マシンの数を ESXi ホスト 1 台につき 200 未満に減らします。

View Composer

- 何千ものデスクトップを含むリンク クローン プールを View Administrator がプロビジョニングすると、いくつかのマシン (1,000 台あたり 1 ~ 2 台) が失敗し、「カスタマイズがタイムアウトになりました」というエラーが表示される場合があります。自動リカバリが有効の場合は (実稼動環境の推奨設定)、エラーが発生したマシンが自動的に再作成され、プロビジョニングされます。回避策は必要ありません。
回避策: 自動リカバリが無効の場合は、View Administrator で、エラーが発生したマシンを手動で削除します。View Administrator は、通常のプール管理の一環として新しいマシンをプロビジョニングします。
- 大きなデスクトップ プールを削除すると、.hlog ファイルが含まれる多くのフォルダと、.sdd.sf という名前の空のサブフォルダが削除されずに残る場合があります。
回避策: 削除操作の後に残ったフォルダを手動で削除します。手順については、VMware KB [\[Rebalance operation leaves VM folders in previous datastores \(2108928\)\]](#) のソリューションを参照してください。
- IDE コントローラを備えた仮想マシンを Windows XP から Windows 7 へアップグレードする場合、仮想マシンのスナップショットを作成し、リンク クローン プールを作成すると、リンク クローンがカスタマイズできず、プールが作成できません。
回避策: SCSI コントローラとディスクを仮想マシンに追加します。次に VMware Tools を起動し、仮想マシンに VMware SCSI コントローラ ドライバをインストールします。スナップショットを作成して、リンク クローン プールを作成します。
- Sysprep でカスタマイズされたリンク クローン デスクトップをプロビジョニングする場合、一部のデスクトップではカスタマイズされないことがあります。
回避策: デスクトップを更新します。それでも一部のデスクトップがカスタマイズできない場合、再度更新します。
- 親の仮想マシンで VMware View Composer Guest Agent Server サービスのログイン アカウントを変更しないでください。デフォルトでは、これはローカル システム アカウントです。このアカウントを変更すると、この親から作成されたリンク クローンは起動しなくなります。
- デスクトップ プールのプロビジョニングが失敗して、次のエラー メッセージが表示されます。「ポーリング処理のエラー: View Composer Server <https://machine-name:18443> に接続できません: java.net.ConnectException: 接続が拒否されました: 接続。)」
回避策: VMware vCenter Server サーバを再起動してから、デスクトップ プールを再度プロビジョニングします。

Windows 10 および Windows 8.x のサポート

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 [\[Supported Versions of Windows 10 on Horizon View\]](#) 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 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。

- Windows 8.1 デスクトップから Windows 10 にアップグレードした場合、デスクトップにログインした場合、およびログイン画面でキーを押した場合、Windows の表示画面が黒くなり、デスクトップが使用できなくなります。
回避策: 次の手順を実行します。

1. Horizon Client からではなく、vSphere Web Client コンソールまたは RDP からマシンに接続し、画面
上のキーボードを使用して Windows 10 ゲスト OS にログインします。
 2. デバイス マネージャを開き、プロンプトが表示されたら、管理者の認証情報を入力してログインし
ます。
 3. [キーボード] を選択します。
 4. 表示されたキーボード デバイスを右クリックし、[プロパティ] を選択します。
 5. [ドライバー] タブをクリックします。現在のドライバを Lenovo ThinkPad PS/2 キーボード ドライバ
にします。
 6. Microsoft キーボード ドライバを再び使用するには、[ドライバーを元に戻す] をクリックします。
 7. Windows 10 システムを再起動します。
- View Administrator の [登録済みのマシン] ページで Windows 10 管理対象外のマシンが Windows 8 として
表示されます。手動デスクトップ プール内にある vCenter Server の管理対象 Windows 10 マシンと、自動
プール内にある Windows 10 マシンは、Windows 10 として正しく表示されます。
回避策：なし
 - 場合によっては、Windows 8.x デスクトップ セッションに再接続したときに、デスクトップ ディスプレイ
がすぐに表示されないことがあります。最大 20 秒間、黒い画面が表示される場合があります。
回避策：なし
 - Windows 8.x リンク クローン仮想マシンに領域再利用を実行したとき、システム処理可能ディスクとユー
ザー通常ディスクのサイズが最大容量まで増えることがあります。この領域増加は、最初の領域再利用を
完了したときにのみ発生します。OS ディスクに関しては、領域再利用は期待どおりに動作し、未使用領
域を再利用します。この問題は、システム処理可能ディスクとユーザー通常ディスクを使用しない View
Composer デスクトップに影響を与えません。
回避策：Windows 8 または 8.1 仮想マシンで View Composer デスクトップを構成し、領域再利用を有効に
するとき、システム処理可能ディスクまたはユーザー通常ディスクを構成しません。
 - 高品質かつ積極的なスロットルを用いた Adobe Flash 最適化設定は、Windows 8 または Windows 8.1 デス
クトップで Internet Explorer 10 または Internet Explorer 11 をエンド ユーザーが使用する場合は完全に有効
にはなりません。
回避策：なし。
 - Windows 8 デスクトップでは、View Persona Management 設定である [ログオフ時にローカルの個人設定を削除]
を有効にした場合に、ユーザーが PDF ファイルを作成し、デスクトップをログオフして再びログインする
と、ユーザーはオフラインの PDF ファイルを開くことができなくなります。Windows 8 Reader がオフライ
ン PDF コンテンツをダウンロードできなくなるためです。
回避策：ファイルを右クリックして手動でダウンロードし、[プロパティ] を選択するか、[Adobe Reader
で開く] を選択します。
 - Windows 8 以降のコンピュータで Internet Explorer 10 または 11 を使用している場合、ブラウザのローケ
ルを繁体字中国語に設定して View Administrator にログインすると、ナビゲーション パネルが簡体字中国
語で表示されることがあります。
回避策：別のブラウザを使用して View Administrator にログインしてください。
 - Windows 8 View 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、View 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。
 - vSphere 5.1 環境で 64 ビットまたは 32 ビットの Windows 8 デスクトップをプロビジョニングすると、
Sysprep カスタマイズが失敗する場合があります。デスクトップは、**カスタマイズがタイムアウトしました**というエ
ラー メッセージでエラー状態になります。この問題は、親仮想マシンまたはテンプレートでアンチウイルス
ソフトウェアがインストールされている場合に発生します。この問題は、フル クローンおよびリンク
されたクローン デスクトップに適用されます。この問題は QuickPrep でカスタマイズしたリンク クローン
デスクトップには該当しません。

回避策：親仮想マシンまたはテンプレートのアンチウイルス ソフトウェアをアンインストールし、プールを再作成します。

- Windows 8.1 デスクトップの再構成中、Sysprep のカスタマイズが失敗し、「カスタマイズ操作がタイムアウトしました」というエラー メッセージが表示される場合があります。この問題は、使用されていない機能を削除することによってディスク領域を確保する Windows 8.1 の計画されたメンテナンス作業によって発生します。

回避策：次のコマンドを使用して、セットアップ完了直後にメインテナンス作業を無効にしてください。Schtasks.exe /change /disable /tn

"\Microsoft\Windows\AppxDeploymentClient\Pre-staged app cleanup"

- 通常ディスクを使用して再構成、更新、または再調整操作を行った後、Windows 10 デスクトップが起動に失敗するか、[スタート] メニューに表示されなくなる場合があります。Windows アプリケーションには、Windows ストア、ネイティブ アプリケーション、Edge ブラウザ、Cortana 検索などのアプリケーションが含まれます。この問題は、Windows 10 アプリケーションの特性が原因で発生します。この問題は、次のデスクトップ タイプに影響します。
 - 通常ディスクのあるリンク クローン専用のデスクトップ。
 - 通常ディスクをローカル ディスクとして使用し、個人設定管理の[ローカル設定フォルダの移動]が有効になっている個人設定管理が有効なリンク クローン フローティング デスクトップ。

この問題は、フローティングまたは専用リンク クローンの Windows 10 バージョン 1607 デスクトップ プールでは発生しません。このデスクトッププールでは、Persona Management が有効または無効でもユーザー プロファイルがネットワーク共有にリダイレクトされます。個人設定管理が有効になっている場合、ユーザー プロファイルは VMware Persona GPO 設定を使用して移動するように設定されます。

- Horizon View 6.2.3 で、Agent のオペレーティング システムが Windows 10 1607 CBB の場合、プリンタのアイコンが[デバイスとプリンタ]フォルダに表示されません。

回避策：デバイス サービスを再起動して、プリンタを再度追加してください。詳細については、VMware ナレッジベースの記事 KB2149788「[Printer icons are not visible in Devices and Printers folder when Agent operating system is Windows 10 1607 CBB in Horizon View 6.2.3 or 6.2.4](#)」を参照してください。

Windows Server デスクトップの使用

- Horizon Client を初めて利用する場合、接続したデスクトップが使用可能な状態になっていても、Windows Server 2008 R2 SP1 デスクトップに接続できないことやブラック スクリーンになることがあります。

回避策：Windows Server 2008 R2 SP1 仮想マシンをシャットダウンし、電源を入れ直してください。デスクトップが使用可能な状態になった時点で、再接続してください。注：仮想マシンを再設定または再起動しても、この問題は解決できません。仮想マシンを最初にシャットダウンしてからパワーオンします。

Workspace Portal の統合

- View Connection Server のインスタンスまたはセキュリティ サーバのデフォルト HTTPS ポート 443 を変更した場合に、Horizon ユーザーが Horizon User Portal からデスクトップの開始を試みると、デスクトップの起動が失敗します。この問題は、ユーザーが Horizon Client または HTML Access のいずれかで Horizon Workspace 経由でデスクトップにアクセスを試みると発生します。

回避策：デフォルト HTTPS ポート 443 をそのままにします。

- View Administrator で SAML 認証子を追加すると、メタデータ URL が Windows 証明書ストアの[信頼されたルート証明機関]フォルダに信頼された証明書をポイントしているときでも、[無効な証明書が検出されました]ウィンドウが表示されます。この問題は、信頼された証明書が Windows 証明書ストアに追加されたときに、自己署名証明書を持つ既存の SAML 認証子が同じメタデータ URL を使用していた場合に発生します。

回避策：

1. Windows 証明書ストアの[信頼されたルート証明機関]フォルダからメタデータ URL 用の信頼された証明書を削除します。
2. 自己署名した証明書がある SAML 認証子を削除します。
3. Windows 証明書ストアの[信頼されたルート証明機関]フォルダにメタデータ URL 用の信頼された証明書を追加します。

- 4. SAML 認証子を再び追加します。

Virtual SAN と Virtual Volumes

- ハイブリッド vSAN 環境で約 3% の仮想マシンが View Storage Accelerator を使用しない可能性があります。これらのマシンは、起動時間が数秒長くなります。
回避策：View Storage Accelerator を使用しなかった仮想マシンを削除してから再作成します。
- このリリースでは、Virtual Volume データストアで View Storage Accelerator はサポートされません。
回避策：なし
- 一部の Virtual Volumes ストレージ アレイでは、View Composer リンク クローンのプロビジョニングが失敗します。次のメッセージが表示されます。「Error creating disk Error creating VVol Object.This may be due to insufficient available space on the datastore or the datastore's inability to support the selected provisioning type. (ディスク作成中にエラーが発生しました。VVol オブジェクトを作成中にエラーが発生しました。原因として、データストアの空き容量が不足しているか、選択されたプロビジョニング タイプをデータストアでサポートできないことが考えられます)」View Composer は、他のすべてのリンク クローン ディスクがシン プロビジョニングを使用している場合でも、シックプロビジョニング形式で小さな内部ディスクを作成します。この問題は、サードパーティの Virtual Volumes ストレージ アレイがデフォルトではシックプロビジョニングされたディスクをサポートしていない場合に発生します。
回避策：Virtual Volumes でシックプロビジョニングされたディスクを作成できるようにするには、ストレージ アレイ上のシック プロビジョニングを有効にします。
- Virtual SAN データストア上に保存されている View Composer 通常ディスクを接続するか再作成すると、vCenter Server の仮想ディスクのストレージ ポリシーは「期限切れ」として表示されます。元のストレージ プロファイルは保持されません。
回避策：vSphere Web Client で、ストレージ ポリシーを仮想ディスクに再適用します。
- Virtual SAN データストアには、Virtual SAN クラスタに属するホストからのみアクセスできます。別のクラスタに属するホストからはアクセスできません。そのため、1 つの Virtual SAN データストアから別のクラスタ内の別の Virtual SAN データストアにプールを再分散することはできません。
- ONTAP 8.2.x 以前を実行している NetApp ストレージ システムに常駐している Virtual デスクトップは Volumes データストア上に、大規模な VDI デスクトップ プール（たとえば、2,000 デスクトップ）が作成されている環境では、「VVol ターゲットでベンダー固有のエラーが発生しました」というエラーメッセージが表示され、少数のデスクトップの再構成操作が失敗することがあります。
回避策：NetApp ストレージ システムを ONTAP 8.3 以降にアップグレードします。

クラウド ポッド アーキテクチャ

- View Administrator ログイン中、他の View 管理者によって行われたクラウド ポッド アーキテクチャ構成の変更は、現在の View Administrator セッションに表示されません。
回避策：View Administrator からログアウトし、再度ログインして変更を確認します。

その他

- フローティング割り当てまたは自動化されたファームを使用して自動リンク クローン プールからマシンを削除している間、ViewDbChk ユーティリティが「通常ディスクのアーカイブ中...」というメッセージを表示する場合があります。
回避策：なし。
- ハードウェア バージョン 8 の仮想マシンでは、使用可能な最大ビデオ RAM は 128MB です。ハードウェア バージョン 9 以降の仮想マシンでは、許可される最大ビデオ RAM は 512MB です。仮想マシンのハードウェア バージョンのビデオ RAM 制限を超える値を View Administrator から構成すると、vSphere Client の [Recent Tasks] 画面にエラーが表示され、構成操作がループします。この問題は、vSphere Client からではなく、View Administrator （プール設定ページ）からビデオ メモリ値を構成した場合に限って発生します。
回避策：vSphere Client の仮想マシンのハードウェア バージョンをアップグレードするか、View Administrator を使用して、現在の仮想マシンのハードウェア バージョンに基づくビデオ メモリに適切な値を設定してください。

