

Horizon 7 のセキュリティ

2018 年 12 月 13 日

VMware Horizon 7 7.7



vmware®

VMware Web サイトで最新の技術ドキュメントをご確認いただけます。

<https://docs.vmware.com/jp/>

VMware の Web サイトでは、最新の製品アップデートを提供しています。

本書に関するご意見、ご要望をお寄せください。フィードバック送信先：

docfeedback@vmware.com

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

ヴィエムウェア株式会社
105-0013 東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

Copyright © 2009–2018 VMware, Inc. All rights reserved. [著作権および商標](#).

内容

Horizon 7 セキュリティ 5

1 Horizon 7 のアカウント、リソース、およびログ ファイル 6

Horizon 7 アカウント 6

Horizon 7 のリソース 7

Horizon 7 ログ ファイル 8

2 Horizon 7 のセキュリティ設定 10

Horizon Administrator のセキュリティ関連のグローバル設定 10

Horizon Administrator のセキュリティ関連のサーバ設定 12

View LDAP のセキュリティ関連の設定 13

3 ポートとサービス 15

Horizon 7 の TCP ポートと UDP ポート 15

Horizon 7 TrueSSO ポート 20

Horizon 7 Cloud Connector 仮想アプライアンスのポート 21

接続サーバ ホスト上のサービス 22

セキュリティ サーバ上のサービス 22

4 証明書のサムプリントの検証と証明書の自動生成 24

5 接続サーバ 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 26

セキュリティ プロトコルと暗号化スイートのデフォルトのグローバル ポリシー 26

グローバルな承諾ポリシーと提案ポリシーの構成 27

各サーバでの承諾ポリシーの構成 29

リモート デスクトップでの提案ポリシーの構成 30

Horizon 7 で無効化された古いプロトコルと暗号化方式 31

6 Blast Secure Gateway のセキュリティ プロトコルと暗号化スイートの構成 33

Blast Secure Gateway (BSG) のセキュリティ プロトコルと暗号化スイートの構成 33

7 PCoIP Secure Gateway のセキュリティ プロトコルと暗号化スイートの設定 35

PCoIP Secure Gateway (PSG) のセキュリティ プロトコルと暗号化スイートの設定 35

8 保護された Horizon 7 環境での USB デバイスの展開 36

すべてのタイプのデバイスに対する USB リダイレクトの無効化 36

特定のデバイスに対する USB リダイレクトの無効化 38

9 接続サーバおよびセキュリティ サーバでの HTTP による保護手段 40

Internet Engineering Task Force 標準 40

World Wide Web Consortium 標準 41

他の保護手段 45

HTTP 保護対策の設定 49

Horizon 7 セキュリティ

『Horizon 7 セキュリティ』では、VMware Horizon 7 のセキュリティ機能について簡潔に参照できます。

- 必要なシステムおよびデータベース ログイン アカウント。
- セキュリティに関連する構成オプションおよび設定。
- セキュリティ関連の構成ファイルおよびパスワード、およびセキュリティ操作について推奨されるアクセス制御など、保護される必要があるリソース。
- ログ ファイルの場所とその目的。
- Horizon 7 を正しく操作するために開くまたは有効にする必要がある外部インターフェイス、ポート、サービス。

対象読者

本マニュアルの情報は、IT の意思決定者、アーキテクト、管理者、および Horizon 7 のセキュリティ コンポーネントに精通する必要があるその他の読者を対象としています。

Horizon 7 のアカウント、リソース、およびログ ファイル

1

特定コンポーネントに別のアカウントを使用すると、個人に必要以上のアクセスと権限を与えることを防ぐことができます。構成ファイルおよび機密データが含まれるその他のファイルの場所を把握しておく、さまざまなホストシステムに対するセキュリティのセットアップに役立ちます。

注: Horizon 7.0 から、View Agent が Horizon Agent という名前に変更されました。

この章には、次のトピックが含まれています。

- [Horizon 7 アカウント](#)
- [Horizon 7 のリソース](#)
- [Horizon 7 ログ ファイル](#)

Horizon 7 アカウント

Horizon 7 コンポーネントを管理するには、システム アカウントおよびデータベース アカウントを設定する必要があります。

表 1-1. Horizon 7 のシステム アカウント

Horizon のコンポーネント	必要なアカウント
Horizon Client	リモート デスクトップおよびアプリケーションへのアクセス権があるユーザーについて、Active Directory でユーザー アカウントを構成します。ユーザー アカウントは、リモート デスクトップユーザー グループのメンバーである必要がありますが、このアカウントには、Horizon 管理者権限は不要です。
vCenter Server	Horizon 7 をサポートするために必要な vCenter Server での操作を実行するための権限を持つユーザー アカウントを Active Directory で構成します。 必要な権限については、『Horizon 7 のインストール』ドキュメントを参照してください。

表 1-1. Horizon 7 のシステム アカウント (続き)

Horizon のコンポーネント	必要なアカウント
View Composer	<p>AD operations account. View Composer で使用するユーザー アカウントを Active Directory で作成します。View Composer では、リンク クローン デスクトップを Active Directory ドメインに参加させるためにこのアカウントが必要です。Active Directory 操作アカウントの View Composer ユーザーを Horizon 管理者アカウントにすることはできません。このアカウントには、指定された Active Directory コンテナ内のコンピュータ オブジェクトを追加および削除するために必要な最小限の権限を付与します。たとえば、このアカウントにはドメイン管理者権限は必要ありません。</p> <p>Standalone control account. vCenter Server と同じマシンに View Composer をインストールすると、Horizon 7 は同じユーザー アカウントで vCenter Server と View Composer サービスの両方にアクセスします。スタンドアローン マシンに View Composer をインストールする場合は、Horizon 7 が View Composer にアクセスできるように、個別のユーザー アカウントを構成します。</p> <p>Active Directory 操作アカウントとスタンドアローン制御アカウントに必要な権限については、『Horizon 7 のインストール』を参照してください。</p>
接続サーバ	<p>Horizon 7 をインストールすると、Horizon 管理者として特定のドメイン ユーザー、ローカル管理者グループ、特定のドメイン ユーザー グループを指定できます。Horizon 管理者の専用ドメイン ユーザー グループを作成することを推奨します。デフォルトは、現在ログインしているドメイン ユーザーです。</p> <p>Horizon Administrator では、[View 構成] - [管理者] を使用して、Horizon 管理者のリストを変更できます。</p> <p>必要な権限については、『Horizon 7 の管理』ドキュメントを参照してください。</p>

表 1-2. Horizon のデータベース アカウント

Horizon のコンポーネント	必要なアカウント
View Composer データベース	<p>SQL Server または Oracle データベースに View Composer データが格納されます。View Composer ユーザー アカウントに関連付けることができるデータベースの管理者アカウントを作成します。</p> <p>View Composer データベースの設定については、『Horizon 7 のインストール』ドキュメントを参照してください。</p>
Horizon 接続サーバにより使用されるイベント データベース	<p>SQL Server または Oracle データベースに Horizon イベント データが格納されます。Horizon Administrator がイベント データにアクセスするのに使用できるデータベースの管理者アカウントを作成します。</p> <p>View Composer データベースの設定については、『Horizon 7 のインストール』ドキュメントを参照してください。</p>

セキュリティ脆弱性のリスクを軽減するために、次のアクションを実行します。

- 組織が使用する他のデータベース サーバとは別のサーバで Horizon 7 データベースを構成します。
- 1 人のユーザーが複数のデータベースにアクセスすることを許可しないようにします。
- View Composer とイベント データベースにアクセスするアカウントは別々に構成します。

Horizon 7 のリソース

Horizon 7 には、いくつかの構成ファイルと、保護する必要がある同じようなリソースが含まれます。

表 1-3. Horizon 接続サーバおよびセキュリティ サーバのリソース

リソース	場所	保護
LDAP 設定	適用なし	LDAP データは、ロール ベースのアクセス制御の一環として自動的に保護されます。
LDAP バックアップ ファイル	%ProgramData%\VMWare\VDM\backups	アクセス制御により保護されます。

表 1-3. Horizon 接続サーバおよびセキュリティ サーバのリソース (続き)

リソース	場所	保護
locked.properties (セキュア ゲートウェイ の構成ファイル)	<install_directory>\VMware\VMware View\Server\sslgateway\conf	Horizon 管理者以外のユーザーからのアクセ スに対して、このファイルを確実に保護でき るようにします。
absg.properties (Blast Secure Gateway の構成ファイル)	<install_directory>\VMware\VMware View\Server\appblastgateway	Horizon 管理者以外のユーザーからのアクセ スに対して、このファイルを確実に保護でき るようにします。
ログ ファイル	「 Horizon 7 ログ ファイル 」を参照してください。	アクセス制御により保護されます。
web.xml (Tomcat 構成ファイル)	<install_directory>\VMware View\Server\broker\web apps\ROOT\Web INF	アクセス制御により保護されます。

Horizon 7 ログ ファイル

Horizon 7 により、そのコンポーネントのインストールおよび操作を記録するログ ファイルが作成されます。

注: Horizon 7 のログ ファイルは、VMware サポートによって使用されることを目的としています。VMware では、Horizon 7 を監視するために、イベント データベースを構成して使用することを推奨します。詳細については、『Horizon 7 のインストール』 および 『Horizon 7 の統合』 ドキュメントを参照してください。

表 1-4. Horizon 7 のログ ファイル

Horizon のコンポーネント	ファイル パスその他の情報
すべてのコンポーネント (イン ストール ログ)	<%TEMP%>\vminst.log_<日付>_<タイムスタンプ> <%TEMP%>\vmmsi.log_<日付>_<タイムスタンプ>
Horizon Agent	<<ドライブ文字>>:\ProgramData\VMware\VDM\logs <<ドライブ文字>>:\ProgramData\VMware\VDM\logs に格納されている Horizon 7 ログ ファイルに アクセスするには、管理者特権を使用してプログラムからログを開く必要があります。プログラム ファイルを右 クリックして、[管理者として実行] を選択します。 ユーザー データ ディスク (UDD) が構成されている場合、<<Drive Letter>> がその UDD に対応する場合が あります。 PCoIP のログの名前は、pcoip_agent*.log および pcoip_server*.log です。
公開されたアプリケーション	SQL Server または Oracle データベース サーバで構成された Horizon イベント データベースを表示します。 Windows アプリケーションのイベント ログ。デフォルトで無効になっています。
View Composer	リンク クローン デスクトップにある <%system_drive%>\Windows\Temp\vmware-viewcomposer- ga-new.log。 View Composer ログには、QuickPrep および Sysprep スクリプトの実行に関する情報が含まれます。このロ グには、スクリプト実行の開始と終了時刻、および出力またはエラー メッセージが記録されます。

表 1-4. Horizon 7 のログ ファイル (続き)

Horizon のコンポーネント	ファイル パスとその他の情報
接続サーバまたはセキュリティ サーバ	<p><<ドライブ文字>>:\ProgramData\VMware\VDM\logs。</p> <p>このログ ディレクトリは、Common の構成 ADMX テンプレート ファイル (<code>vdm_common.admx</code>) のログ設定で、構成可能です。</p> <p>PCoIP Secure Gateway のログは、PCoIP Secure Gateway サブディレクトリの SecurityGateway_*.log という名前のファイルに書き込まれます。</p> <p>Blast Secure Gateway のログは、Blast Secure Gateway サブディレクトリの absg*.log という名前のファイルに書き込まれます。</p>
Horizon のサービス	<p>SQL Server または Oracle データベース サーバで構成された Horizon イベント データベースを表示します。</p> <p>Windows システムのイベント ログ。</p>

Horizon 7 のセキュリティ設定

Horizon 7 には、構成のセキュリティを調整するために使用できるいくつかの設定が含まれています。必要に応じて、Horizon Administrator または ADSI Edit ユーティリティを使用して、これらの設定にアクセスできます。

注: Horizon Client および Horizon Agent のセキュリティ設定については、『Horizon Client および Agent のセキュリティ』ドキュメントを参照してください。

この章には、次のトピックが含まれています。

- [Horizon Administrator のセキュリティ関連のグローバル設定](#)
- [Horizon Administrator のセキュリティ関連のサーバ設定](#)
- [View LDAP のセキュリティ関連の設定](#)

Horizon Administrator のセキュリティ関連のグローバル設定

クライアント セッションおよび接続のセキュリティ関連のグローバル設定には、Horizon Administrator の [View 構成] - [グローバル設定] でアクセス可能です。

表 2-1. セキュリティ関連のグローバル設定

設定	説明
[データ リカバリのパスワードを変更]	<p>パスワードは、View LDAP 構成が暗号化されたバックアップから復元する場合に必要です。</p> <p>接続サーババージョン 5.1 以降をインストールするときに、データ リカバリ パスワードを指定します。インストール後、このパスワードは Horizon Administrator で変更できます。</p> <p>接続サーバをバックアップすると、View LDAP 構成が暗号化された LDIF データとしてエクスポートされます。暗号化されたバックアップを vdmimport ユーティリティで復元するには、データ リカバリ パスワードを指定する必要があります。パスワードは 1 文字から 128 文字の間にする必要があります。安全なパスワードの生成に関する組織のベスト プラクティスに従ってください。</p>
[メッセージセキュリティ モード]	<p>Horizon 7 コンポーネント間で JMS メッセージが渡される場合に使用するセキュリティ メカニズムを決定します。</p> <ul style="list-style-type: none"> ■ [無効化] に設定すると、メッセージ セキュリティ モデルが無効になります。 ■ [有効] に設定すると、レガシー メッセージへの署名と JMS メッセージの検証が行われます。Horizon 7 コンポーネントは未署名のメッセージを拒否します。このモードは、TLS とプレーン JMS 接続の混在をサポートします。 ■ [拡張済み] に設定されている場合、TLS は全 JMS 接続に使用され、すべてのメッセージを暗号化します。アクセス制御は、Horizon 7 コンポーネントがメッセージを送信する、およびメッセージを受信する JMS トピックを制限するためにも有効化されます。 ■ [混在] に設定すると、メッセージ セキュリティ モードは有効になりますが、View Manager 3.0 より前の Horizon 7 コンポーネントでは強制されません。 <p>新しくインストールする場合のデフォルトの設定は、[拡張済み] です。前のバージョンからアップグレードする場合は、前のバージョンで使用されていた設定が維持されます。</p> <p>重要: VMware は、すべての接続サーバインスタンス、セキュリティ サーバ、および Horizon 7 デスクトップをこのリリースにアップグレード後、メッセージセキュリティ モードを [拡張済み] に設定することを強く推奨します。[拡張済み] 設定にすると、多くの重要なセキュリティ向上と MQ (メッセージ キュー) の更新が提供されます。</p>
[拡張セキュリティのステータス] (読み取り専用)	<p>[メッセージセキュリティ モード] が [有効] から [拡張済み] に変更された場合に表示される読み取り専用フィールド。変更は段階的に行われるため、このフィールドにはフェーズを通じた進捗が表示されます。</p> <ul style="list-style-type: none"> ■ [MessageBus の再起動待機中] が最初のフェーズです。この状態は、手動でポッド内のすべての接続サーバインスタンスを再起動するか、ポッド内のすべての接続サーバホストの VMware Horizon Message Bus Component サービスを再起動するまで、表示されます。 ■ 次の段階は [拡張の保留] です。すべての Horizon Message Bus コンポーネント サービスが再起動されると、すべてのデスクトップサーバおよびセキュリティサーバに対して、システムはメッセージ セキュリティ モードを [拡張済み] に変更する処理を開始します。 ■ 最後の段階は [拡張済み] であり、すべてのコンポーネントが [拡張済み] メッセージセキュリティ モードを使用するようになったことを示します。
[ネットワークへの割り込み後に安全なトンネル接続を再認証する]	<p>Horizon Client が Horizon 7 デスクトップおよびアプリケーションへのセキュアなトンネル接続を使用する場合、ネットワークの中断後にユーザー認証情報を再認証する必要があるかどうかを決定します。</p> <p>この設定により、セキュリティが強化されます。たとえば、ラップトップが盗まれて別のネットワークに移動された場合、ネットワーク接続が一時的に中断されたことにより、ユーザーは Horizon 7 デスクトップおよびアプリケーションに自動的にアクセスできなくなります。</p> <p>デフォルトでは、この設定は無効になっています。</p>
[ユーザーの強制切断]	<p>ユーザーが Horizon 7 にログインしてから指定した時間 (分) が経過すると、すべてのデスクトップとアプリケーションが切断されます。すべてのデスクトップとアプリケーションは、ユーザーがそれらをいつ開いたかにかかわらず同時に切断されます。</p> <p>デフォルトは 600 分です。</p>

表 2-1. セキュリティ関連のグローバル設定 (続き)

設定	説明
[アプリケーションをサポートするクライアント。] [ユーザーがキーボードとマウスを使用しなくなった場合に、アプリケーションを切断し、SSO 認証情報を破棄する]	クライアント デバイスで、キーボードやマウスが使用されなくなった場合にアプリケーション セッションを保護します。[経過時間...分] に設定した場合、指定された時間 (分) ユーザーのアクティビティがないと、Horizon 7 により、すべてのアプリケーションが切断され、SSO 認証情報は破棄されます。デスクトップ セッションは切断されます。ユーザーは、再度ログインして切断されたアプリケーションに再接続するか、新しいデスクトップまたはアプリケーションを起動する必要があります。 [なし] に設定すると、ユーザーのアクティビティがなくても、Horizon 7 によるアプリケーションの切断や SSO 認証情報の破棄は行われません。 デフォルトは [なし] です。
[その他のクライアント。] [SSO 認証情報の破棄]	一定の期間後に SSO 認証情報を破棄します。この設定は、アプリケーションのリモート処理をサポートしていないクライアント用です。[経過時間...分] に設定した場合、クライアント デバイスでのユーザー アクティビティにかかわらず、Horizon 7 へログイン後指定時間 (分) が経過したら、ユーザーはデスクトップへ再度ログインしてデスクトップに接続する必要があります。 デフォルトは、[15 分後] です。
[セキュリティ サーバのペアリングのために IPsec を有効化]	セキュリティ サーバと Horizon 接続サーバインスタンス間の接続に Internet Protocol Security (IPsec) を使用するかどうかを決定します。FIPS モードでセキュリティ サーバをインストールする前に、この設定を無効にする必要があります。無効にしないと、ペアリングが失敗します。 デフォルトでは、セキュリティ サーバ接続に IPsec が有効となっています。
[View Administrator セッション タイムアウト]	セッションがタイムアウトする前にアイドル状態の Horizon Administrator セッションがどれだけ続くかを決定します。 重要: Horizon Administrator セッション タイムアウトを長い分数に設定すると、Horizon Administrator が不正に使用されるリスクが増します。アイドル状態のセッションを長時間許可する場合は用心してください。 デフォルトでは、Horizon Administrator セッション タイムアウトは 30 分です。セッション タイムアウトは 1 分から 4320 分の間で設定できます。

これらの設定およびセキュリティに与える影響の詳細については、『Horizon 7 の管理』を参照してください。

注: Horizon 7 に対するすべての Horizon Client 接続および Horizon Administrator 接続には、TLS が必要です。Horizon 7 の展開でロード バランサまたはその他のクライアントが接続する中間サーバが使用されている場合、TLS をそれらにオフロードしてから、それぞれの接続サーバインスタンスおよびセキュリティ サーバで非 TLS 接続を構成できます。『Horizon 7 の管理』ドキュメントの「TLS 接続を中間サーバにオフロードする」を参照してください。

Horizon Administrator のセキュリティ関連のサーバ設定

セキュリティ関連のサーバ設定には、Horizon Administrator の [View 構成] - [サーバ] でアクセス可能です。

表 2-2. セキュリティ関連のサーバ設定

設定	説明
[マシンへの PCoIP 接続に PCoIP Secure Gateway を使用する]	<p>ユーザーが PCoIP 表示プロトコルを使用して Horizon 7 デスクトップおよびアプリケーションに接続するときに、Horizon Client は接続サーバはセキュリティ サーバ ホストへの安全な接続を追加で行うかどうかを決定します。</p> <p>この設定が無効になっている場合は、デスクトップまたはアプリケーション セッションが、接続サーバまたはセキュリティ サーバ ホストをバイパスして、クライアントと Horizon 7 デスクトップまたはリモート デスクトップ サービス (RDS) ホストとの間で直接確立されるようになります。</p> <p>デフォルトでは、この設定は無効になっています。</p>
[マシンへの安全なトンネル接続を使用する]	<p>ユーザーが Horizon 7 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、Horizon Client が接続サーバまたはセキュリティ サーバ ホストへの HTTPS 接続をさらに行うかどうかを決定します。</p> <p>この設定が無効になっている場合は、デスクトップまたはアプリケーション セッションが、接続サーバまたはセキュリティ サーバ ホストをバイパスして、クライアントと Horizon 7 デスクトップまたはリモート デスクトップ サービス (RDS) ホストとの間で直接確立されるようになります。</p> <p>デフォルトでは、この設定は有効になっています。</p>
[Blast Secure Gateway を使用してマシンに Blast 接続する]	<p>Web ブラウザまたは Blast Extreme 表示プロトコルでデスクトップにアクセスするクライアントが Blast Secure Gateway を使用して接続サーバへのセキュアなトンネルを確立するかどうかを決定します。</p> <p>有効にしない場合、Blast Extreme セッションを使用するクライアント、および Web ブラウザによって、接続サーバをバイパスした Horizon 7 デスクトップへの直接接続が行われます。</p> <p>デフォルトでは、この設定は無効になっています。</p>

これらの設定およびセキュリティに与える影響の詳細については、『Horizon 7 の管理』を参照してください。

View LDAP のセキュリティ関連の設定

View LDAP では、オブジェクトパス

cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int にセキュリティ関連の設定があります。ADSI Edit ユーティリティを使用して、接続サーバ インスタンスに関するこれらの設定値を変更できます。グループ内にある他のすべての接続サーバ インスタンスに、この変更内容が自動的に伝わります。

表 2-3. View LDAP のセキュリティ関連の設定

名前と値のペア	説明
[cs-allowunencryptedstartsession]	<p>属性は、pae-NameValuePair です。</p> <p>この属性は、リモート ユーザー セッションの開始中に、セキュアなチャネルが接続サーバインスタンスとデスクトップ間で必要かどうかを制御します。</p> <p>View Agent 5.1 以降または Horizon Agent 7.0 以降がデスクトップ コンピュータにインストールされている場合、この属性は効果がなく、セキュアなチャネルが常に必要となります。View Agent 5.1 より古いバージョンがインストールされている場合、デスクトップ コンピュータが接続サーバインスタンスのドメインと双方向の信頼があるドメインのメンバーでないと、セキュアなチャネルは確立できません。この場合、この属性は、リモート ユーザー セッションがセキュア チャネルなしで開始できるかどうかを決定するために重要になります。</p> <p>すべての場合、ユーザー認証情報および認証チケットは静的キーで保護されます。セキュア チャネルは、動的キーを使用して機密性をさらに確実なものにします。</p> <p>[0] に設定すると、リモート ユーザー セッションはセキュア チャネルが確立できなければ開始されません。この設定は、すべてのデスクトップが信頼されているドメインにあるか、すべてのデスクトップに View Agent 5.1 以降のバージョンがインストールされている場合に適しています。</p> <p>[1] に設定すると、リモート ユーザー セッションは、セキュア チャネルが確立できない場合であっても開始できます。この設定は、一部のデスクトップに古い View Agent がインストールされて、それらが信頼されていないドメインにある場合に適しています。</p> <p>デフォルトの設定は [1] です。</p>

ポートとサービス

Horizon 7 コンポーネントが互いに通信できるように、特定の UDP および TCP ポートを開く必要があります。各タイプの View Server で実行される Windows サービスを把握することは、Horizon 7 Server に属さないサービスの識別に役立ちます。

この章には、次のトピックが含まれています。

- [Horizon 7 の TCP ポートと UDP ポート](#)
- [Horizon 7 TrueSSO ポート](#)
- [Horizon 7 Cloud Connector 仮想アプライアンスのポート](#)
- [接続サーバ ホスト上のサービス](#)
- [セキュリティ サーバ上のサービス](#)

Horizon 7 の TCP ポートと UDP ポート

Horizon 7 では、そのコンポーネント間のネットワーク アクセスに TCP および UDP ポートが使用されます。

インストール中に、Horizon 7 ではオプションで Windows ファイアウォール ルールを構成し、デフォルトで使われるポートを開くことができます。インストール後にデフォルトのポートを変更した場合、手動で Windows ファイアウォール ルールを再構成して更新されたポートへのアクセスを許可する必要があります。『Horizon 7 のインストール』の「Horizon 7 サービスのデフォルト ポートの置換」を参照してください。

TrueSSO ソリューションに関連する証明書ログインで Horizon 7 が使用するポートのリストについては、[「Horizon 7 TrueSSO ポート」](#)を参照してください。

表 3-1. Horizon 7 で使用される TCP および UDP ポート

送信元	ポート	送信先	ポート	プロトコル	説明
セキュリティ サーバ、接続サーバ、または Unified Access Gateway アプライアンス	55000	Horizon Agent	4172	UDP	PCoIP Secure Gateway が使用されている場合の PCoIP (SALSA20 ではありません)。
セキュリティ サーバ、接続サーバ、または Unified Access Gateway アプライアンス	4172	Horizon Client	*	UDP	PCoIP Secure Gateway が使用されている場合の PCoIP (SALSA20 ではありません)。 <u>注:</u> 受信元のポートが異なるため、この表の下にある注意を参照してください。
セキュリティ サーバ	500	接続サーバ	500	UDP	IPsec ネゴシエーション トラフィック。
セキュリティ サーバ	*	接続サーバ	4001	TCP	JMS トラフィック。
セキュリティ サーバ	*	接続サーバ	4002	TCP	JMS SSL トラフィック。
セキュリティ サーバ	*	接続サーバ	8009	TCP	IPsec を使用していない場合、AJP13 で転送される Web トラフィック。
セキュリティ サーバ	*	接続サーバ	*	ESP	NAT なしで IPsec を使用している場合、AJP13 で転送される Web トラフィック。
セキュリティ サーバ	4500	接続サーバ	4500	UDP	NAT デバイスを通じて IPsec を使用している場合、AJP13 で転送される Web トラフィック。
セキュリティ サーバ、接続サーバ、または Unified Access Gateway アプライアンス	*	Horizon Agent	3389	TCP	トンネル接続が使用される場合の Horizon 7 デスクトップへの Microsoft RDP トラフィック。
セキュリティ サーバ、接続サーバ、または Unified Access Gateway アプライアンス	*	Horizon Agent	9427	TCP	トンネル接続が使用されている場合、Windows Media MMR リダイレクトとクライアント ドライブ リダイレクト。
セキュリティ サーバ、接続サーバ、または Unified Access Gateway アプライアンス	*	Horizon Agent	32111	TCP	トンネル接続が使用される場合の USB のリダイレクトとタイムゾーンの同期。

表 3-1. Horizon 7 で使用される TCP および UDP ポート (続き)

送信元	ポート	送信先	ポート	プロトコル	説明
セキュリティ サーバ、接続サーバ、または Unified Access Gateway アプライアンス	*	Horizon Agent	4172	TCP	PCoIP Secure Gateway が使用されている場合の PCoIP。
セキュリティ サーバ、接続サーバ、または Unified Access Gateway アプライアンス	*	Horizon Agent	22443	TCP	Blast Secure Gateway が使用されている場合の VMware Blast Extreme。
セキュリティ サーバ、接続サーバ、または Unified Access Gateway アプライアンス	*	Horizon Agent	22443	TCP	Blast Secure Gateway が使用される場合の HTML Access。
Horizon Agent	4172	Horizon Client	*	UDP	PCoIP Secure Gateway が使用されていない場合の PCoIP。 注: 受信元のポートが異なるため、この表の下にある注意を参照してください。
Horizon Agent	4172	接続サーバ、セキュリティ サーバ、または Unified Access Gateway アプライアンス	55000	UDP	PCoIP Secure Gateway が使用されている場合の PCoIP (SALSA20 ではありません)。
Horizon Agent	4172	Unified Access Gateway アプライアンス	*	UDP	PCoIP。Horizon 7 デスクトップおよびアプリケーションは、UDP ポート 4172 から Unified Access Gateway アプライアンスに PCoIP データを送り返します。 送信先の UDP ポートは、受信した UDP パケットのソース ポートとなり、これは返信データであるため、通常は、これに明示的なファイアウォール ルールを追加する必要はありません。
Horizon Agent (管理対象外)	*	接続サーバインスタンス	389	TCP	管理対象外エージェントのインストールで AD LDS にアクセスします。 注: このポートを他の目的で使用する場合は、この表の下にある注を参照してください。
Horizon Client	*	接続サーバ、セキュリティ サーバ、または Unified Access Gateway アプライアンス	80	TCP	デフォルトで TLS (HTTPS アクセス) は、クライアント接続で有効になってますが、ポート 80 (HTTP アクセス) は特定のケースで使用できます。 「Horizon 7 での HTTP リダイレクト」 を参照してください。

表 3-1. Horizon 7 で使用される TCP および UDP ポート (続き)

送信元	ポート	送信先	ポート	プロトコル	説明
Horizon Client	*	接続サーバ、セキュリティ サーバ、または Unified Access Gateway アプライアンス	443	TCP	Horizon 7 にログインするための HTTPS。(このポートはトンネル接続が使用される場合のトンネリングにも使用されます。)
Horizon Client	*	接続サーバ、セキュリティ サーバ、または Unified Access Gateway アプライアンス	4172	TCP と UDP	PCoIP Secure Gateway が使用されている場合の PCoIP。
Horizon Client	*	Horizon Agent	3389	TCP	トンネル接続の代わりに直接接続が使用される場合の Horizon 7 デスクトップへの Microsoft RDP トラフィック。
Horizon Client	*	Horizon Agent	9427	TCP	トンネル接続の代わりに直接接続が使用されている場合、Windows Media MMR リダイレクトとクライアント ドライブ リダイレクト。
Horizon Client	*	Horizon Agent	32111	TCP	トンネル接続の代わりに直接接続が使用される場合の USB のリダイレクトとタイム ゾーンの同期。
Horizon Client	*	Horizon Agent	4172	TCP と UDP	PCoIP Secure Gateway が使用されていない場合の PCoIP。 注: 送信先のポートが異なるため、この表の下にある注意を参照してください。
Horizon Client	*	Horizon Agent	22443	TCP と UDP	VMware Blast
Horizon Client	*	接続サーバ、セキュリティ サーバ、または Unified Access Gateway アプライアンス	4172	TCP と UDP	PCoIP Secure Gateway が使用されている場合の PCoIP (SALSA20 ではありません)。 注: 送信先のポートが異なるため、この表の下にある注意を参照してください。
Web ブラウザ	*	セキュリティ サーバまたは Unified Access Gateway アプライアンス	8443	TCP	HTML Access。
接続サーバ	*	接続サーバ	48080	TCP	接続サーバ コンポーネント間の内部通信の場合。
接続サーバ	*	vCenter Server または View Composer	80	TCP	vCenter Server または View Composer へのアクセスで TLS が無効になっている場合の SOAP メッセージ。
接続サーバ	*	vCenter Server	443	TCP	vCenter Server へのアクセスで TLS が有効になっている場合の SOAP メッセージ。
接続サーバ	*	View Composer	18443	TCP	View Composer へのアクセスで TLS が有効になっている場合の SOAP メッセージ。

表 3-1. Horizon 7 で使用される TCP および UDP ポート (続き)

送信元	ポート	送信先	ポート	プロトコル	説明
接続サーバ	*	接続サーバ	4100	TCP	JMS ルータ間トラフィック。
接続サーバ	*	接続サーバ	4101	TCP	JMS TLS ルーター間トラフィック。
接続サーバ	*	接続サーバ	8472	TCP	クラウド ポッド アーキテクチャでのポッド間通信の場合。
接続サーバ	*	接続サーバ	22389	TCP	クラウド ポッド アーキテクチャでのグローバル LDAP レプリケーションの場合。
接続サーバ	*	接続サーバ	22636	TCP	クラウド ポッド アーキテクチャでの安全なグローバル LDAP レプリケーションの場合。
接続サーバ	*	接続サーバ	32111	TCP	キー共有トラフィック。
接続サーバ	*	認証局	*	HTTP、HTTPS	CRL または OCSP のクエリ
Unified Access Gateway アプライアンス	*	接続サーバまたはロード バランサ	443	TCP	HTTPS アクセス。Unified Access Gateway アプライアンスは、TCP ポート 443 で接続し、複数の接続サーバインスタンスの前にある 1 つの接続サーバインスタンスまたはロード バランサと通信します。
View Composer サービス	*	ESXi ホスト	902	TCP	View Composer 内部ディスク、および指定される場合には通常ディスクとシステム廃棄可能ディスクを含むリンク クローンディスクが、View Composer によりカスタマイズされるときに使用されます。

注: PCoIP 用にクライアントが使用する UDP ポート番号は変更できます。ポート 50002 が使用されている場合、クライアントは 50003 を選択します。ポート 50003 が使用されている場合、クライアントは 50004 を選択し、このような処理が続きます。表にアスタリスク (*) が示されている項目については、ANY を使用してファイアウォールを構成する必要があります。

注: Microsoft Windows Server では、Horizon 7 環境のすべての接続サーバ間で、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。

注: 接続サーバ インスタンスでは、ポート 389 は不定期でアドホックな接続でアクセスされます。表のように、このポートは管理対象外エージェントのインストールでアクセスされます。また、LDAP エディタを使用してデータベースを直接編集するときや、readmin などのツールでコマンドを発行する場合にアクセスされます。AD LDS がインストールされている場合、これらの目的でファイアウォール ルールが作成されますが、ポートへのアクセスが必要な場合は無効にできます。

Horizon 7 での HTTP リダイレクト

Horizon Administrator への接続を除いて、HTTP への接続は HTTPS にサイレントでリダイレクトされます。HTTP リダイレクトは、最近の Horizon クライアントでは HTTPS がデフォルトになっているので不要ですが、たとえば、Horizon Client のダウンロードなど、Web ブラウザでユーザーが接続する場合に役立ちます。

HTTP リダイレクトの問題は、セキュアでないプロトコルにあります。ユーザーがアドレス バーに **https://** を入力する習慣がない場合、期待するページが正しく表示されている場合であっても、攻撃者は Web ブラウザに危害を加えたり、マルウェアをインストールしたり、証明書を盗むことができます。

注: 外部接続用の HTTP リダイレクトは、外部ファイアウォールがインバウンドトラフィックを TCP ポート 80 に許可するように構成されている場合に限って実行できます。

Horizon Administrator への HTTP 上での接続はリダイレクトされません。代わりに、エラーメッセージが返され、HTTPS を使用する必要があることが示されます。

すべての HTTP 接続の試行のリダイレクトを防ぐには、『Horizon 7 のインストール』の「接続サーバへのクライアント接続で HTTP リダイレクトを防止」を参照してください。

接続サーバインスタンスまたはセキュリティサーバのポート 80 への接続は、TLS クライアント接続を中間デバイスにオフロードする場合も実行できます。『Horizon 7 の管理』ドキュメントの「TLS 接続を中間サーバにオフロードする」を参照してください。

TLS ポート番号が変更されたときに HTTP リダイレクトを許可するには、『Horizon 7 のインストール』の「接続サーバへの HTTP リダイレクト用のポート番号を変更」を参照してください。

Horizon 7 TrueSSO ポート

Horizon 7 は、通信パス（ポートおよびプロトコル）とセキュリティ制御に TrueSSO ポートを使用します。これらのポートは、Horizon Connection Server 間で証明書を転送する場合や、仮想デスクトップや公開アプリケーションが TrueSSO ソリューションと関連する証明書でログインする場合に使用します。

表 3-2. Horizon 7 によって使用される TrueSSO ポート

Source	送信先	ポート	プロトコル	説明
Horizon Client	VMware Identity Manager アプライアンス	TCP 443	HTTPS	SAML アサーションとアーティファクトを生成する VMware Identity Manager アプライアンスから Horizon 7 を起動します。
Horizon Client	Horizon Connection Server	TCP 443	HTTPS	Horizon Client を起動します。
Horizon Connection Server	VMware Identity Manager アプライアンス	TCP 443	HTTPS	接続サーバが、VMware Identity Manager と SAML の解決を実行します。VMware Identity Manager がアーティファクトを検証し、アサーションを返します。
Horizon Connection Server	Horizon 登録サーバ	TCP 32111		登録サーバを使用します。

表 3-2. Horizon 7 によって使用される TrueSSO ポート (続き)

Source	送信先	ポート	プロトコル	説明
登録サーバ	ADCS			<p>登録サーバは、Microsoft 証明書認証局 (CA) から証明書を要求し、短時間有効な一時的な証明書を生成します。</p> <p>登録サービスは、認証局 (CA) との初期通信に TCP 135 RPC を使用します。以降は、1024 ~ 5000 と 49152 ~ 65535 からランダムにポートを選択します。https://support.microsoft.com/en-us/help/832017#method4 の「証明書サービス」を参照してください。</p> <p>また、登録サーバはドメイン コントローラーに接続して、関連するすべてのポートを使用して DC を検出し、Active Directory にパイノドしてクエリを実行します。</p> <p>[https://support.microsoft.com/en-us/help/832017#method1 および https://support.microsoft.com/en-us/help/832017#method12] を参照してください。</p>
Horizon Agent	Horizon Connection Server	TCP 4002	TLS 経由での JMS	Horizon Agent は、ログインの証明書を要求し、受信します。
仮想デスクトップまたは公開アプリケーション	Active Directory DC			Windows では、Active Directory を使用して証明書の信頼性を検証します。多くのポートが必要になる場合もあります。Microsoft のドキュメントで、ポートとプロトコルの一覧を確認してください。
Horizon Client	Horizon Agent (プロトコル セッション)	TCP/UDP 22443	Blast	Windows デスクトップまたはアプリケーションにログインします。Horizon Client でリモート セッションが開始します。
Horizon Client	Horizon Agent (プロトコル セッション)	UDP 4172	PCoIP	Windows デスクトップまたはアプリケーションにログインします。Horizon Client でリモート セッションが開始します。

Horizon 7 Cloud Connector 仮想アプライアンスのポート

Horizon 7 は、ポートを使用して別の Horizon 7 Cloud Connector 仮想アプライアンスからのアップグレード、VMware Horizon Cloud Service とのペアリング、認証、通信を待機します。

表 3-3. Horizon 7 Cloud Connector のポート

送信元	ポート	送信先	ポート	プロトコル	説明
Horizon 7 Cloud Connector	*	VMware Horizon Cloud Service	443	HTTPS	VMware Horizon Cloud Service とペアリングしてデータを転送します。
Horizon 7 Cloud Connector	*	接続サーバ	443	HTTPS	接続サーバへの API 呼び出し。
新しい Horizon 7 Cloud Connector	*	既存の Horizon 7 Cloud Connector	22	SSH	アップグレード プロセスの開始要求を待機します。
Web ブラウザ	*	Horizon 7 Cloud Connector	443	HTTPS	ペアリング プロセスの開始を待機します。
Horizon 7 Cloud Connector	*	認証局	*	HTTP、HTTPS	CRL または OCSP のクエリ

接続サーバ ホスト上のサービス

Horizon 7 の処理は、接続サーバ ホストで実行しているいくつかのサービスに依存しています。

表 3-4. Horizon 接続サーバ ホスト サービス

サービス名	スタートアップの種類	説明
VMware Horizon View Blast Secure Gateway	自動	安全な HTML Access サービスと Blast Extreme サービスを提供します。クライアントが Blast Secure Gateway を介して接続サーバに接続する場合には、このサービスを実行する必要があります。
VMware Horizon View 接続サーバ	自動	コネクション ブローカー サービスを提供します。このサービスは常に実行する必要があります。このサービスを開始または停止すると、Framework、Message Bus、Security Gateway、および Web サービスも開始または停止されます。このサービスでは、VMwareVDMDS サービスまたは VMware Horizon View スクリプト ホスト サービスは開始または停止されません。
VMware Horizon View Framework コンポーネント	Manual	イベント ログ、セキュリティ、および COM+ Framework サービスを提供します。このサービスは常に実行する必要があります。
VMware Horizon View Message Bus コンポーネント	Manual	Horizon 7 コンポーネント間のメッセージング サービスを提供します。このサービスは常に実行する必要があります。
VMware Horizon View PCoIP Secure Gateway	Manual	PCoIP Secure Gateway サービスを提供します。クライアントが PCoIP Secure Gateway を介して接続サーバに接続する場合には、このサービスを実行する必要があります。
VMware Horizon View スクリプト ホスト	無効	仮想マシンを削除する場合に実行するサードパーティ スクリプトをサポートします。デフォルトでは、このサービスは無効になっています。スクリプトを実行する場合、このサービスを有効にする必要があります。
VMware Horizon View Security Gateway コンポーネント	Manual	一般的なゲートウェイ サービスを提供します。このサービスは常に実行する必要があります。
VMware Horizon View Web コンポーネント	Manual	Web サービスを提供します。このサービスは常に実行する必要があります。
VMwareVDMDS	自動	LDAP ディレクトリ サービスを提供します。このサービスは常に実行する必要があります。Horizon 7 のアップグレード中、このサービスにより既存のデータが正しく移行されます。

セキュリティ サーバ上のサービス

Horizon 7 の動作は、セキュリティ サーバで実行しているいくつかのサービスに依存しています。

表 3-5. セキュリティ サーバ サービス

サービス名	スタートアップの種類	説明
VMware Horizon View Blast Secure Gateway	自動	安全な HTML Access サービスと Blast Extreme サービスを提供します。クライアントが Blast Secure Gateway を介してこのセキュリティ サーバに接続する場合には、このサービスを実行する必要があります。
VMware Horizon View セキュリティ サーバ	自動	セキュリティ サーバ サービスを提供します。このサービスは常に行うする必要があります。このサービスを開始または停止すると、Framework および Security Gateway サービスも開始または停止されます。
VMware Horizon View Framework コンポーネント	手動	イベント ログ、セキュリティ、および COM+ Framework サービスを提供します。このサービスは常に行う必要があります。
VMware Horizon View PCoIP Secure Gateway	手動	PCoIP Secure Gateway サービスを提供します。クライアントが PCoIP Secure Gateway を介してこのセキュリティ サーバに接続する場合には、このサービスを実行する必要があります。
VMware Horizon View Security Gateway コンポーネント	手動	一般的なゲートウェイ サービスを提供します。このサービスは常に行う必要があります。

証明書のサムプリントの検証と証明書の自動生成

4

Horizon 7 は、多くの公開キー証明書を使用します。これらの証明書の一部は、信頼できるサードパーティが関与するメカニズムで検証されていますが、これにより、必要な精度や速度、柔軟性が提供されるとは限りません。Horizon 7 は、いくつかの状況でサムプリントの検証というメカニズムを使用します。

サムプリントの検証では、個々の証明書フィールドを検証したり、信頼チェーンを構築することはありません。証明書をトークンとして扱い、バイトシーケンス全体（またはその暗号ハッシュ）と事前共有のバイトシーケンスまたはハッシュと比較します。これは通常、別の信頼チャンネルとジャストインタイムで共有されるため、サービスから提示された証明書が、予期した証明書と完全に一致するかどうか検証することができます。

Horizon Message Bus は、接続サーバ間の通信だけでなく、Horizon Agent と接続サーバインスタンス間の通信でも使用されます。セットアップチャンネルはメッセージごとの署名とペイロード暗号化を使用しますが、メインチャンネルは TLS 相互認証で保護されています。TLS チャンネルでチャンネルを保護している場合、クライアントとサーバの両方の認証で TLS 証明書とサムプリントの検証が行われます。Horizon Message Bus の場合、サーバが常にメッセージルーターになります。メッセージルーターがこのようにメッセージを共有しているため、クライアントがメッセージルーターになる場合もあります。ただし、クライアントは、接続サーバインスタンス、セキュリティサーバまたは Horizon Agent のいずれかです。

最初の証明書のサムプリントとセットアップメッセージの署名キーは、さまざまな方法で提供されます。たとえば、セキュリティサーバのペアリング時に、この情報が接続サーバと交換されます。ただし、この最初の交換が発生すると、署名キーと証明書サムプリントの以降のロールオーバーはセットアップチャンネル経由で行われます。接続サーバでは、証明書のサムプリントが LDAP に保存されます。このため、Horizon Agent が任意の接続サーバに接続し、すべての接続サーバが相互に通信を行うことができます。Horizon Message Bus のサーバとクライアントの証明書は自動的に生成され、定期的に交換されます。失効した証明書は自動的に削除されるため、手動で操作を行う必要はありません。メインチャンネルの両端の証明書はスケジュールに従って自動的に生成され、セットアップチャンネルで交換されます。これらの証明書を自分で置きかえることはできません。期限切れの証明書は自動的に削除されます。

同様のメカニズムがポッド間通信にも適用されます。

他の通信チャンネルではユーザー提供の証明書を使用できますが、デフォルトは証明書の自動生成です。これには、セキュアトンネル、登録サーバ、Composer、vCenter Server との接続、表示プロトコル、補助チャンネルなどが含まれます。これらの証明書を交換する方法の詳細については、『Horizon 7 の管理』を参照してください。デフォルトの証明書はインストール時に生成されますが、PCoIP を除き、自動的に更新されることはありません。公開鍵基盤 (PKI) で生成された証明書を PCoIP で使用できない場合、スタートアップ時に新しい証明書を自動的に生成します。公開鍵基盤 (PKI) で生成された証明書を使用する場合でも、これらのチャンネルの大半にサムプリントの検証を使用できます。

Composer と vCenter Server 証明書の検証では、複数の技術が使用されます。接続サーバインスタンスは常に、受信した証明書の検証で 公開鍵基盤 (PKI) を使用します。この検証に失敗した場合、証明書の確認後、Horizon 7 管理者は接続の続行を許可できます。接続サーバはサムプリント検証を使用して、証明書の暗号化ハッシュを記憶し、ユーザー不在時に使用します。

接続サーバ インスタンスまたはセキュリティ サーバでのセキュリティ プロトコルおよび暗号化スイートの構成

5

接続サーバによって承認されるセキュリティ プロトコルおよび暗号化スイートを構成できます。複製されたグループ内のすべての 接続サーバ インスタンスに適用されるグローバルな承諾ポリシーを定義することも、それぞれの接続サーバ インスタンスおよびセキュリティ サーバについて承諾ポリシーを定義することもできます。

また、接続サーバ インスタンスが vCenter Server および View Composer に接続するときに提案するセキュリティ プロトコルおよび暗号化スイートを構成することもできます。複製されたグループ内のすべての接続サーバ インスタンスに適用されるグローバルな提案ポリシーを定義できます。グローバルな提案ポリシーを免除される個別のインスタンスは定義できません。

注: 接続サーバのセキュリティ設定は Blast Secure Gateway (BSG) に適用されません。BSG のセキュリティを個別に構成する必要があります。 [章 6 「Blast Secure Gateway 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。

Oracle の Unlimited Strength Jurisdiction Policy ファイルが標準として含まれており、デフォルトで 256 ビットのキーを利用できます。

この章には、次のトピックが含まれています。

- [セキュリティ プロトコルと暗号化スイートのデフォルトのグローバル ポリシー](#)
- [グローバルな承諾ポリシーと提案ポリシーの構成](#)
- [各サーバでの承諾ポリシーの構成](#)
- [リモート デスクトップでの提案ポリシーの構成](#)
- [Horizon 7 で無効化された古いプロトコルと暗号化方式](#)

セキュリティ プロトコルと暗号化スイートのデフォルトのグローバルポリシー

グローバルな承諾ポリシーと提案ポリシーによって、特定のプロトコルと暗号化スイートがデフォルトで有効になります。

表 5-1. デフォルトのグローバルな承諾ポリシー

デフォルトのセキュリティ プロトコル	デフォルトの暗号化スイート
<ul style="list-style-type: none"> ■ TLS 1.2 ■ TLS 1.1 	<ul style="list-style-type: none"> ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

表 5-2. デフォルトのグローバルな提案ポリシー

デフォルトのセキュリティ プロトコル	デフォルトの暗号化スイート
<ul style="list-style-type: none"> ■ TLS 1.2 ■ TLS 1.1 	<ul style="list-style-type: none"> ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 ■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA ■ TLS_RSA_WITH_AES_128_CBC_SHA ■ TLS_RSA_WITH_AES_256_CBC_SHA

パフォーマンス上の理由から、GCM 暗号はデフォルトでは有効になりません。

グローバルな承諾ポリシーと提案ポリシーの構成

グローバルな承諾ポリシーと提案ポリシーは、View LDAP 属性で定義されます。これらのポリシーは、複製されたグループ内のすべての接続サーバ インスタンスおよびセキュリティ サーバに適用されます。グローバルなポリシーを変更するには、任意の View 接続サーバ インスタンスで LDAP を編集できます。

各ポリシーは、View LDAP の場所

(cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int) にある単一値の属性です。

View LDAP で定義されたグローバルな承諾ポリシーと提案ポリシー

グローバルな承諾ポリシーと提案ポリシーを定義する View LDAP 属性は編集できます。

グローバルな承諾ポリシー

次の属性でセキュリティ プロトコルを一覧にしています。最新のプロトコルが先頭になるようにリストを並び替える必要があります。

```
pae-ServerSSLSecureProtocols = \LIST:TLSv1.2,TLSv1.1,TLSv1
```

次の属性で暗号化スイートを一覧にしています。この例は、省略したリストを示しています。

```
pae-ServerSSLCipherSuites
= \LIST:TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
```

次の属性は、暗号化スイートの順序を制御します。通常、サーバでの暗号化スイートの順序は重要ではなく、クライアントの順序が使用されます。サーバの暗号化スイートの順序を使用するには、次の属性を設定します。

```
pae-ServerSSLHonorClientOrder = 0
```

グローバルな提案ポリシー

次の属性でセキュリティ プロトコルを一覧にしています。最新のプロトコルが先頭になるようにリストを並び替える必要があります。

```
pae-ClientSSLSecureProtocols = \LIST:TLSv1.2,TLSv1.1,TLSv1
```

次の属性で暗号化スイートを一覧にしています。このリストは、優先順位の順序になっている必要があります。最も優先順位の高い暗号化スイートを先頭に、次に優先順位の高いスイートを次に、といった順序にしてください。この例は、省略したリストを示しています。

```
pae-ClientSSLCipherSuites
= \LIST:TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
```

グローバルな承諾ポリシーと提案ポリシーの変更

セキュリティ プロトコルおよび暗号化スイートのグローバルな承諾ポリシーと提案ポリシーを変更するには、ADSI Edit ユーティリティを使用して View LDAP 属性を編集します。

前提条件

- 承諾ポリシーと提案ポリシーを定義する View LDAP 属性について理解しておきます。[\[View LDAP で定義されたグローバルな承諾ポリシーと提案ポリシー\]](#) を参照してください。
- お使いのバージョンの Windows Server オペレーティングシステムでの ADSI Edit ユーティリティの使用方法については、Microsoft TechNet Web サイトを参照してください。

手順

- 1 View 接続サーバ コンピュータ上で ADSI Edit ユーティリティを起動します。
- 2 コンソール ツリーで、[接続] を選択します。
- 3 [識別名または命名規則を選択または入力] テキスト ボックスに、識別名「**DC=vdi, DC=vmware, DC=int**」を入力します。
- 4 [ドメインまたはサーバを選択または入力] テキスト ボックスで、**localhost:389** を選択または入力するか、View 接続サーバ コンピュータの完全修飾ドメイン名 (FQDN) を入力し、続いてポート 389 を入力します。
例: **localhost:389** または **mycomputer.mydomain.com:389**
- 5 [ADSI Edit] ツリーを展開し、[OU=Properties] を展開して [OU=Global] を選択し、右ペインで [OU=Common] を選択します。
- 6 オブジェクト [CN=Common, OU=Global, OU=Properties] で変更する各属性を選択して、セキュリティ プロトコルまたは暗号化スイートの新しいリストを入力します。

- 7 **pae-ServerSSLSecureProtocols** を変更した場合は、各接続サーバ インスタンスとセキュリティ サーバで Windows サービス VMware Horizon View Security Gateway Component を再起動します。

pae-ClientSSLSecureProtocols を変更した後にサービスを再起動する必要はありません。

各サーバでの承諾ポリシーの構成

各接続サーバ インスタンスまたはセキュリティ サーバでローカルな承諾ポリシーを指定するには、プロパティを **locked.properties** ファイルに追加する必要があります。**locked.properties** ファイルがまだサーバにない場合は、作成する必要があります。

構成する各セキュリティ プロトコルについて、**secureProtocols.<n>** エントリを追加します。次の構文を使用します。**secureProtocols.<n>=<security protocol>**。

構成する各暗号化スイートについて、**enabledCipherSuite.<n>** エントリを追加します。次の構文を使用します。**enabledCipherSuite.<n>=<cipher suite>**。

変数 **<n>** は、エントリの各タイプに連続的に追加する整数（1、2、3）です。

honorClientOrder エントリを追加して、暗号化スイートの順序を制御します。通常、サーバでの暗号化スイートの順序は重要ではなく、クライアントの順序が使用されます。サーバの暗号化スイートの順序を使用する場合には、次の構文を使用します。

```
honorClientOrder=false
```

locked.properties ファイルのエントリの構文が正しく、暗号化スイートやセキュリティ プロトコルの名前が正しい綴りになっていることを確認してください。このファイルに誤りがあると、クライアントとサーバ間のネゴシエーションに失敗する場合があります。

手順

- 1 接続サーバ ホストまたはセキュリティ サーバ コンピュータ上で、TLS/SSL ゲートウェイ構成フォルダ内の **locked.properties** ファイルを作成または編集します。

例：<install_directory\VMware\VMware View\Server\sslgateway\conf\>
- 2 **secureProtocols.<n>** と **enabledCipherSuite.<n>** エントリに、関連するセキュリティ プロトコルと暗号化スイートを含めて追加します。
- 3 **locked.properties** ファイルを保存します。
- 4 変更を反映するため、VMware Horizon View 接続サーバ サービスまたは VMware Horizon View セキュリティサーバ サービスを再起動してください。

例：各サーバでのデフォルトの承諾ポリシー

次の例は、デフォルトのポリシーを指定するために必要な **locked.properties** ファイルのエントリを示しています。

```
# The following list should be ordered with the latest protocol first:

secureProtocols.1=TLSv1.2
secureProtocols.2=TLSv1.1

# This setting must be the latest protocol given in the list above:

preferredSecureProtocol=TLSv1.2

# The order of the following list is unimportant unless honorClientOrder is false:

enabledCipherSuite.1=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
enabledCipherSuite.2=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
enabledCipherSuite.3=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
enabledCipherSuite.4=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

# Use the client's ordering of cipher suites (ignores the ordering given above):

honorClientOrder=true
```

リモート デスクトップでの提案ポリシーの構成

Windows を実行しているリモート デスクトップで提案ポリシーを構成して、接続サーバへのメッセージ バス接続のセキュリティを制御できます。

接続の問題を回避するため同じポリシーを受け入れるように接続サーバが構成されていることを確認します。

手順

- 1 リモート デスクトップで Windows レジストリ エディタを起動します。
- 2 HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\Configuration レジストリ キーに移動します。
- 3 新しい文字列 (REG_SZ) 値 **ClientSSLSecureProtocols** を追加します。
- 4 [\LIST:<protocol_1>,<protocol_2>,...] の形式で暗号化スイートのリストに値を設定します。

最も新しいプロトコルを最初にしてプロトコルを表示します。例：

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

- 5 新しい文字列 (REG_SZ) 値 **ClientSSLCipherSuites** を追加します。

6 [LIST:<cipher_suite_1>,<cipher_suite_2>,...] の形式で暗号化スイートのリストに値を設定します。

ここでは優先される順番で表示する必要があり、最も利用したい暗号化スイートを最初に表示します。例：

```
\LIST:TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
```

Horizon 7 で無効化された古いプロトコルと暗号化方式

いくつかの古いプロトコルと暗号化方式は安全ではないと見なされて、Horizon 7 においてデフォルトで無効になっています。必要な場合には、これらを手動で有効にできます。

DHE 暗号化スイート

詳細については、<http://kb.vmware.com/kb/2121183> を参照してください。DSA 証明書に準拠する暗号化スイートは、Diffie-Hellman 短期鍵を使用しており、Horizon 6 バージョン 6.2 から、これらのスイートはデフォルトでは無効になっています。

接続サーバのインスタンス、セキュリティ サーバ、および Horizon 7 デスクトップでは、View LDAP データベース、**locked.properties** ファイル、またはレジストリをこのガイドの説明に従って編集し、これらの暗号化スイートを有効にすることができます。「グローバルな承諾ポリシーと提案ポリシーの変更」、「各サーバでの承諾ポリシーの構成」、および「リモート デスクトップでの提案ポリシーの構成」を参照してください。次の 1 つまたは複数のスイートを含む暗号化スイートのリストを、この順番で定義できます。

- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (TLS 1.2 のみ、FIPS は対象外)
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (TLS 1.2 のみ、FIPS は対象外)
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (TLS 1.2 のみ)
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (TLS 1.2 のみ)
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA

View Composer および View Agent Direct-Connection (VADC) マシンでは、『Horizon 7 のインストール』ドキュメントの「View Composer および Horizon Agent マシンにおける SSL/TLS での強度の低い暗号化方式の無効化」の手順に従って操作するときに、暗号化方式のリストに以下を追加することで、DHE 暗号化スイートを有効にできます。

```
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
```

注： ECDSA 証明書のサポートは、有効にできません。これらの証明書は、これまで一度もサポートされたことはありません。

SSLv3

Horizon 7 では、SSL バージョン 3.0 が削除されました。

詳細については、<http://tools.ietf.org/html/rfc7568> を参照してください。

RC4

詳細については、<http://tools.ietf.org/html/rfc7465> を参照してください。

接続サーバのインスタンス、セキュリティ サーバ、および Horizon 7 デスクトップについては、構成ファイル **C:\Program Files\VMware\VMware View\Server\jre\lib\security\java.security** を編集して、接続サーバ、セキュリティ サーバ、または Horizon Agent マシンで RC4 を有効にできます。ファイルの最後は、**jdk.tls.legacyAlgorithms** と呼ばれる複数行のエントリになっています。**RC4_128** とその後のコメントをこのエントリから削除して、接続サーバ、セキュリティ サーバ、または Horizon Agent マシンを場合によって再起動します。

View Composer および View Agent Direct-Connection (VADC) マシンでは、『Horizon 7 のインストール』ドキュメントの「View Composer および Horizon Agent マシンにおける SSL/TLS での強度の低い暗号化方式の無効化」の手順に従って操作するときに、暗号化方式のリストに以下を追加することで、RC4 を有効にできます。

```

TLS_RSA_WITH_RC4_128_SHA

```

TLS 1.0

Horizon 7 のデフォルトでは、TLS 1.0 は無効になっています。

詳細は、https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf および <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf> を参照してください。TLS 1.0 を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「接続サーバからの vCenter Server 接続に対する TLSv1 の有効化」および「View Composer からの vCenter Server および ESXi 接続に対する TLSv1 の有効化」を参照してください。

Blast Secure Gateway のセキュリティ プロトコルと暗号化スイートの構成

6

接続サーバのセキュリティ設定は Blast Secure Gateway (BSG) に適用されません。BSG のセキュリティを個別に構成する必要があります。

Blast Secure Gateway (BSG) のセキュリティ プロトコルと暗号化スイートの構成

absg.properties ファイルを編集すると、BSG のクライアントサイド リスナによって承認されるセキュリティ プロトコルと暗号化スイートを構成できます。

許可されるプロトコルは、低いものから高いものの順序で、tls1.0、tls1.1、tls1.2 です。SSLv3 以前のような古いプロトコルは許可されません。2 つのプロパティ **localHttpsProtocolLow** と **localHttpsProtocolHigh** により、BSG リスナによって承認されるプロトコルの範囲が決まります。たとえば、**localHttpsProtocolLow=tls1.0** と **localHttpsProtocolHigh=tls1.2** を設定すると、リスナは、tls1.0、tls1.1、tls1.2 を承認します。デフォルト設定は **localHttpsProtocolLow=tls1.1** と **localHttpsProtocolHigh=tls1.2** です。BSG の **absg.log** ファイルを調べると、特定の BSG インスタンスで有効になっている値がわかります。

暗号化方式のリストは、<https://www.openssl.org/docs/manmaster/man1/ciphers.html> の「CIPHER LIST FORMAT」で定義されている形式で指定する必要があります。デフォルトの暗号化方式リストを次に示します。

```
!aNULL:kECDH+AESGCM:ECDH+AESGCM:kECDH+AES:ECDH+AES
```

手順

- 1 接続サーバインスタンスで **<install_directory>\VMware\VMware View\Server\appblastgateway\absg.properties** ファイルを編集します。

デフォルトのインストール ディレクトリは **<%ProgramFiles%>** です。

- 2 プロパティ **localHttpsProtocolLow** と **localHttpsProtocolHigh** を編集して、プロトコルの範囲を指定します。

次に例を示します。

```
localHttpsProtocolLow=tls1.0  
localHttpsProtocolHigh=tls1.2
```

プロトコルを 1 つのみ有効にするには、**localHttpsProtocolLow** と **localHttpsProtocolHigh** の両方に同じプロトコルを指定します。

- 3 **localHttpsCipherSpec** プロパティを編集して、暗号化スイートのリストを指定します。

次に例を示します。

```
localHttpsCipherSpec=!aNULL:kECDH+AESGCM:ECDH+AESGCM:kECDH+AES:ECDH+AES
```

- 4 Windows サービス VMware HorizonHorizon 7 Blast Secure Gateway を再起動します。

PCoIP Secure Gateway のセキュリティ プロトコルと暗号化スイートの設定

7

接続サーバのセキュリティ設定は PCoIP Secure Gateway (PSG) に適用されません。PSG のセキュリティを個別に設定する必要があります。

PCoIP Secure Gateway (PSG) のセキュリティ プロトコルと暗号化スイートの設定

レジストリを編集すると、PSG のクライアントサイド リスナーによって承認されるセキュリティ プロトコルと暗号化スイートを設定できます。必要な場合、このタスクを RDS ホスト上で実行することもできます。

許可されるプロトコルは、低いものから高いものの順序で、tls1.0、tls1.1、tls1.2 です。SSLv3 以前のような古いプロトコルは許可されません。

デフォルトの暗号化方式リストを次に示します。

```
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:AES256-SHA256:AES256-SHA:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES128-SHA:@STRENGTH
```

手順

- 1 接続サーバ インスタンス、セキュリティ サーバまたは RDS ホストで、レジストリ エディタを開き、**HKLM\Software\Teradici\SecurityGateway** に移動します。
- 2 REG_SZ レジストリ値 **SSLProtocol** を追加または編集して、プロトコルのリストを指定します。

次に例を示します。

```
tls1.2:tls1.1
```

- 3 REG_SZ レジストリ値 **SSLCipherList** を追加または編集して、暗号化スイートのリストを指定します。

次に例を示します。

```
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256
```

保護された Horizon 7 環境での USB デバイスの展開

8

USB デバイスは BadUSB と呼ばれるセキュリティ脅威に対して脆弱である可能性があり、一部の USB デバイスではファームウェアがハイジャックされたり、マルウェアに置き換えられたりする場合があります。たとえば、ネットワークトラフィックをリダイレクトしたり、キーボードをエミュレートしてキーストロークを取得したりするデバイスを作成できます。このようなセキュリティ上の脆弱性から Horizon 7 の展開が保護されるように USB リダイレクト機能を構成できます。

USB リダイレクトを無効にすることで、すべての USB デバイスがユーザーのリモート デスクトップやアプリケーションにリダイレクトされないようにできます。あるいは、特定の USB デバイスのリダイレクト機能を無効にすることで、ユーザーが自分のリモート デスクトップやアプリケーションで特定のデバイスにしかアクセスできないようにすることができます。

組織のセキュリティ要件に従って、このような設定を施すかどうかを決定してください。これらの設定は必須ではありません。Horizon 7 の展開で、USB リダイレクトをインストールし、すべての USB デバイスでその機能を有効なままにしておくこともできます。少なくとも、組織がこのセキュリティ上の脆弱性に晒される可能性をどの程度まで限定する必要があるかについて、慎重に検討してください。

この章には、次のトピックが含まれています。

- [すべてのタイプのデバイスに対する USB リダイレクトの無効化](#)
- [特定のデバイスに対する USB リダイレクトの無効化](#)

すべてのタイプのデバイスに対する USB リダイレクトの無効化

一部の非常にセキュリティ要件が厳しい環境では、ユーザーがクライアント デバイスに接続した可能性のあるすべての USB デバイスがリモート デスクトップおよびアプリケーションにリダイレクトされるのを回避する必要があります。すべてのデスクトップ プール、特定のデスクトップ プール、またはデスクトップ プール内の特定のユーザーの USB リダイレクトを無効にすることができます。

状況に応じて、次に示す方法の中から任意のものを使用してください。

- Horizon Agent をデスクトップ イメージまたは RDS ホストでインストールする場合、[USB リダイレクト] セットアップ オプションを選択解除してください。(このオプションはデフォルトで選択されていません)。この手法では、デスクトップ イメージまたは RDS ホストから展開されるすべてのリモート デスクトップおよびアプリケーションで、USB デバイスへのアクセスが回避されます。

- Horizon Administrator で、特定のプールに対する [USB アクセス] ポリシーを編集して、アクセスを拒否または許可します。この手法では、デスクトップイメージを変更する必要はなく、特定のデスクトップおよびアプリケーション プールで USB デバイスへのアクセスを制御できます。

公開デスクトップおよびアプリケーション プールには、グローバル [USB アクセス] ポリシーのみを使用できます。個々の公開デスクトップまたはアプリケーション プールに対してこのポリシーを設定することはできません。

- Horizon Administrator で、デスクトップまたはアプリケーション プール レベルでポリシーを設定した後、[ユーザー上書き] 設定を選択し、ユーザーを選択することで、プール内の特定のユーザーに対するポリシーを上書きできます。
- Horizon Agent 側またはクライアント側で、必要に応じて **Exclude All Devices** ポリシーを **true** に設定する。
- スマート ポリシーを使用して、[USB リダイレクト] Horizon ポリシー設定を無効にするポリシーを作成します。この手法により、特定の条件が満たされる場合に特定のリモート デスクトップでの USB リダイレクトを無効化できます。たとえば、ユーザーが企業のネットワーク以外からリモート デスクトップに接続している場合は USB リダイレクトを無効にするポリシーを設定できます。

Exclude All Devices ポリシーを **true** に設定すると、Horizon Client はどの USB デバイスもリダイレクトされないようにします。その他のポリシー設定を使用して、特定のデバイスまたはデバイス ファミリがリダイレクトされるように変更できます。このポリシーを **false** に設定すると、Horizon Client は、その他のポリシー設定でブロックされているものを除き、すべての USB デバイスがリダイレクトされるようにします。このポリシーは、Horizon Agent と Horizon Client の両方に設定できます。次の表は、Horizon Agent と Horizon Client に設定できる **Exclude All Devices** ポリシーを組み合わせ、クライアント コンピュータに効果的なポリシーを作成する方法を示しています。デフォルトでは、ブロックされていない限り、すべての USB デバイスがリダイレクトされるようになっています。

表 8-1. Exclude All Devices（すべてのデバイスを除外する）ポリシーの組み合わせた場合の効果

Horizon Agent での Exclude All Devices (すべてのデバイスを除外する) ポリシー	Horizon Client での Exclude All Devices (すべてのデバイスを除外する) ポリシー	組み合わせた場合の効果的な Exclude All Devices (すべてのデバイスを除外する) ポリ シー
false または未定義 (すべての USB デバイ スを含む)	false または未定義 (すべての USB デバイ スを含む)	すべての USB デバイスを含む
false (すべての USB デバイスを含む)	true (すべての USB デバイスを除外する)	すべての USB デバイスを除外する
true (すべての USB デバイスを除外する)	いずれか、または未定義	すべての USB デバイスを除外する

Disable Remote Configuration Download ポリシーを **true** に設定すると、Horizon Agent での **Exclude All Devices** の値が Horizon Client に渡されませんが、Horizon Agent と Horizon Client は **Exclude All Devices** のローカル値を適用します。

これらのポリシーは、Horizon Agent の構成 ADMX テンプレート ファイル (**vdm_agent.admx**) に含まれています。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』の「Horizon Agent の構成 ADMX テンプレートの USB 設定」を参照してください。

特定のデバイスに対する USB リダイレクトの無効化

ユーザーの中には、ローカル側で接続された特定の USB デバイスをリダイレクトして、リモート デスクトップまたはアプリケーションでそれらのデバイスがタスクを実行できるようにする必要のあるユーザーもいます。たとえば、医師は Dictaphone USB デバイスを使用して、患者の医療情報を記録しなければならない場合があります。このような場合、すべての USB デバイスへのアクセスを無効にすることはできません。グループ ポリシー設定を使用して、特定のデバイスに対して USB リダイレクトを有効または無効にすることができます。

特定のデバイスに対して USB リダイレクトを有効にする前に、会社内のクライアント マシンに接続される物理デバイスを信用できることを確認してください。サプライ チェーンを信用できることを確認します。可能であれば、USB デバイスの加工および流通過程の管理体制を追跡します。

また、従業員に不明な発行元からのデバイスを接続しないように周知します。可能な場合は、環境内のデバイスを署名付きファームウェア更新のみ、つまり FIPS 140-2 レベル 3 認定のものに限定し、現場で更新可能なすべての種類のファームウェアをサポートしないようにします。このようなタイプの USB デバイスは発行元を特定するのが困難であり、デバイスの要件によっては検出不可能である可能性があります。このような選択肢は実用的ではないかもしれませんが、検討する価値はあります。

各 USB デバイスにはコンピュータにそれ自体を認識させるためのベンダー ID と製品 ID が付けられています。Horizon Agent 構成のグループ ポリシー設定を構成することで、既知のデバイス タイプを含めるポリシーを設定できます。この手法により、不明なデバイスが環境内で使用されるリスクをなくすることができます。

たとえば、既知のデバイス ベンダー ID および製品 ID である **vid/pid=0123/abcd** を除くすべてのデバイスがリモート デスクトップまたはアプリケーションにリダイレクトされるのを回避できます。

ExcludeAllDevices	Enabled
IncludeVidPid	o:vid-0123_pid-abcd

注: この例の構成では保護することはできませんが、感染したデバイスによって何らかの vid/pid が報告される可能性があるため、攻撃の可能性は依然としてあります。

デフォルトで、Horizon 7 は特定のデバイス ファミリがリモート デスクトップまたはアプリケーションにリダイレクトされるのをブロックします。たとえば、HID（ヒューマン インターフェイス デバイス）やキーボードなどはゲスト内への表示がブロックされます。出回っている一部の BadUSB コードは USB キーボード デバイスをターゲットにしています。

特定のデバイス ファミリがリモート デスクトップまたはアプリケーションにリダイレクトされるのを回避できます。たとえば、すべてのビデオ、オーディオ、および大規模ストレージ デバイスをブロックできます。

ExcludeDeviceFamily	o:video;audio;storage
----------------------------	------------------------------

反対に、ホワイトリストを作成し、すべてのデバイスがリダイレクトされないようにしても特定のデバイス ファミリののみは使用できるようにすることもできます。たとえば、ストレージ デバイスを除くすべてのデバイスをブロックできます。

ExcludeAllDevices	Enabled
IncludeDeviceFamily	o:storage

リモート ユーザーがデスクトップまたはアプリケーションにログインして、それを感染させる場合、別のリスクが発生する可能性があります。会社のファイアウォールの外側から行われたすべての Horizon 7 接続への USB アクセスを回避できます。USB デバイスは内的には使用できますが、外的には使用できなくなります。

TCP ポート 32111 をブロックして USB デバイスへの外部アクセスを無効にすると、タイム ゾーン同期が動作しなくなります。これは、タイム ゾーン同期でもポート 32111 が使用されているためです。ゼロ クライアントの場合、USB トラフィックは UDP ポート 4172 の仮想チャネル内に組み込まれます。ポート 4172 は USB リダイレクトの他にディスプレイ プロトコルにも使用されるため、ポート 4172 をブロックすることはできません。必要な場合は、ゼロ クライアントに対して USB リダイレクトを無効に設定できます。詳細については、ゼロ クライアント製品パンフレットを参照するか、ゼロ クライアント ベンダーにお問い合わせください。

特定のデバイス ファミリまたは特定のデバイスをブロックするポリシーを設定すると、BadUSB マルウェアによって感染させられるリスクを軽減できる可能性があります。これらのポリシーによってすべてのリスクが軽減されるわけではありませんが、全体的なセキュリティ戦略の一部として有効に機能する可能性があります。

これらのポリシーは、Horizon Agent の構成 ADMX テンプレート ファイル (**vdm_agent.admx**) に含まれています。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」を参照してください。

接続サーバおよびセキュリティ サーバ での HTTP による保護手段

9

Horizon 7 は特定の手段により、HTTP プロトコルを使用する通信を保護します。

この章には、次のトピックが含まれています。

- [Internet Engineering Task Force 標準](#)
- [World Wide Web Consortium 標準](#)
- [他の保護手段](#)
- [HTTP 保護対策の設定](#)

Internet Engineering Task Force 標準

接続サーバとセキュリティ サーバは、一定の Internet Engineering Task Force (IETF) 標準に準拠します。

- RFC 5746 Transport Layer Security (TLS) – Renegotiation Indication Extension (安全な再ネゴシエーションとも呼ばれる) は、デフォルトで有効になっています。

注: クライアントが開始する再ネゴシエーションは、接続サーバとセキュリティサーバにおいてデフォルトで無効になっています。有効にするには、レジストリ値 `[HKLM\SOFTWARE\VMware, Inc.\VMware VDM\plugins\wsnm\TunnelService\Params]JvmOptions` を編集して、文字列から `-Djdk.tls.rejectClientInitiatedRenegotiation=true` を削除します。

- RFC 6797 HTTP Strict Transport Security (HSTS) (トランスポート セキュリティとも呼ばれる) は、デフォルトで有効になっています。この設定を無効にすることはできません。
- RFC 7034 HTTP Header Field X-Frame-Options (カウンター クリックジャッキングとも呼ばれる) は、デフォルトで有効になっています。無効にするには、ファイル `locked.properties` にエントリ `x-frame-options=OFF` を追加します。ファイル `locked.properties` にプロパティを追加する方法については、[\[HTTP 保護対策の設定\]](#) を参照してください。

注: Horizon 7 バージョン 7.2 より前のリリースでは、このリストを変更しても HTML Access との接続に影響はありません。

- RFC 6454 のオリジンの確認は、デフォルトで有効になっています。これは、クロスサイト リクエスト フォージェリからの保護を提供します。無効にするには、**locked.properties** にエントリ **checkOrigin=false** を追加します。詳細については、「[クロスオリジン リソース共有](#)」を参照してください。

注: 以前のリリースでは、この保護はデフォルトで無効になっていました。

World Wide Web Consortium 標準

接続サーバとセキュリティ サーバは、特定の World Wide Web Consortium (W3C) 標準に準拠しています。

- クロスオリジン リソース共有 (CORS) は、クライアント側のクロスオリジン リクエストを制限します。この機能を有効にするには、**locked.properties** に **enableCORS = true** エントリを追加します。無効にするには、**enableCORS = false** エントリを追加します。
- コンテンツ セキュリティ ポリシー (CSP)。さまざまなコンテンツ インジェクションの脆弱性を回避します。デフォルトでは、有効になっています。無効にするには、**locked.properties** に **enableCSP=false** エントリを追加します。

クロスオリジン リソース共有

クロスオリジン リソース共有 (CORS) 機能は、ポリシー ステートメントをオンデマンドでクライアントに提供し、リクエストがポリシーに準拠しているかどうか確認することで、クライアント側のクロスオリジン リクエストを制限します。この機能は、必要なときに構成し、有効にできます。

ポリシーには、許可される HTTP メソッドのセット、リクエストの送信元、有効なコンテンツ タイプが記述されています。これらはリクエスト URL によって異なり、**locked.properties** ファイルにエントリを追加することで必要に応じて再設定できます。

プロパティ名の後の省略記号は、プロパティでリストを使用できることを示します。

表 9-1. CORS プロパティ

プロパティ	値の種類	マスター デフォルト	他のデフォルト値
enableCORS	true false	false	n/a
acceptContentType ...	http-content-type	application/x-www-form-urlencoded,application/xml,text/xml	admin=application/x-amf newadmin=application/json,application/text,application/x-www-form-urlencoded portal=application/json sso-redirect=application/x-amf view-vlsi-rest=application/json
acceptHeader...	http-header-name	*	n/a
exposeHeader...	http-header-name	*	n/a
filterHeaders	true false	true	n/a

表 9-1. CORS プロパティ (続き)

プロパティ	値の種類	マスター デフォルト	他のデフォルト値
checkOrigin	true false	true	n/a
checkReferer	true false	false	n/a
allowCredentials	true false	false	admin=true broker=true misc=true newadmin=true portal=true saml=true sso-redirect=true tunnel=true view-vlsi=true view-vlsi-rest=true
allowMethod...	http-method-name	GET,HEAD,POST	misc=GET,HEAD saml=GET,HEAD sso-redirect=GET,HEAD
allowPreflight	true false	true	n/a
maxAge	cache-time	0	n/a
balancedHost	load-balancer-name	OFF	n/a
portalHost...	gateway-name	OFF	n/a
chromeExtension..	chrome-extension-hash	ppkfnjlimknmjoaemnpidmdlfchhehel	n/a

注: この値は、Horizon Client for Chrome の Chrome 拡張機能 ID になります。

locked.properties ファイルを使用して、CORS プロパティの使い方を説明します。

```
enableCORS = true
allowPreflight = true
checkOrigin = true
checkOrigin-misc = false
allowMethod.1 = GET
allowMethod.2 = HEAD
allowMethod.3 = POST
allowMethod-saml.1 = GET
```

```
allowMethod-saml.2 = HEAD
acceptContentType.1 = application/x-www-form-urlencoded
acceptContentType.2 = application/xml
acceptContentType.3 = text/xml
```

オリジンの確認

オリジンの確認は、デフォルトで有効になっています。有効な場合、リクエストが受け入れられるのは、オリジンがない場合か、オリジンが外部 URL に指定されたアドレス、**balancedHost** アドレス、**portalHost** アドレス、**chromeExtension** ハッシュ、**null** または **localhost** に一致している場合だけです。オリジンがこのいずれかでない場合、「予期しないオリジン」エラーがログに記録され、ステータス 404 が返されます。

注: ブラウザによっては、Origin ヘッダーが提供されません、また、まったく提供されない場合もあります。Origin ヘッダーがない場合は、リクエストの Referer ヘッダーをチェックすることもできます。Referer ヘッダーでは、ヘッダー名に「r」が 1 つ含まれています。Referer ヘッダーを確認するには、**locked.properties** ファイルに次のプロパティを追加します。

```
checkReferer=true
```

複数の接続サーバ ホストやセキュリティ サーバがロード バランシングされている場合、**locked.properties** ファイルに **balancedHost** エントリを追加して、ロード バランサのアドレスを指定する必要があります。このアドレスについては、ポート 443 が前提となります。

Unified Access Gateway アプライアンスまたは別のゲートウェイを介してクライアントが接続する場合、**portalHost** エントリを **locked.properties** ファイルに追加し、すべてのゲートウェイ アドレスを指定する必要があります。これらのアドレスについては、ポート 443 が前提となります。外部 URL が指定された名前と異なる名前で接続サーバ ホストまたはセキュリティ サーバにアクセスするには、**portalHost** エントリの指定も必要です。

Chrome 拡張クライアントは、最初のオリジンに独自の ID を設定します。接続を許可するには、**locked.properties** ファイルに **chromeExtension** エントリを追加して、拡張機能を登録します。例：

```
chromeExtension.1=bpifadopbphhpkkcfohecfadckmpjmjd
```

コンテンツ セキュリティ ポリシー

コンテンツ セキュリティ ポリシー (CSP) 機能は、準拠しているブラウザに対するポリシー ディレクティブを提供します。これにより、クロス サイト スクリプティング (XSS) などのコンテンツ インジェクションの脆弱性を回避できます。この機能は、デフォルトで有効になっています。**locked.properties** にエントリを追加すると、ポリシー ディレクティブを再設定できます。

表 9-2. CSP プロパティ

プロパティ	値の種類	マスター デフォルト	他のデフォルト値
enableCSP	true false	true	n/a
content-security-policy	directives-list	default-src 'self';script-src 'self' 'unsafe- inline' 'unsafe-eval' data:;style-src 'self' 'unsafe- inline';font-src 'self' data:;frame- ancestors 'none'	newadmin = default-src 'self';script-src 'self' 'unsafe- inline' 'unsafe-eval' data:;style- src 'self' 'unsafe-inline';font-src 'self' data:;img-src 'self' data:;connect-src 'self' https;;frame-ancestors 'none' portal = default-src 'self';script-src 'self' 'unsafe- inline' 'unsafe-eval' data:;style- src 'self' 'unsafe-inline';font-src 'self' data:;img-src 'self' data: blob;;media-src 'self' blob;;connect-src 'self' wss;;frame-src 'self' blob;;child- src 'self' blob;;object-src 'self' blob;;frame-ancestors 'self'
x-content-type-options	OFF specification	nosniff	n/a
x-frame-options	OFF specification	deny	portal = sameorigin
x-xss-protection	OFF specification	1; mode=block	n/a

CSP プロパティを **locked.properties** ファイルに追加できます。CSP プロパティの例：

```
enableCSP = true
content-security-policy = default-src 'self';script-src 'self' 'unsafe-inline' 'unsafe-eval'
data:;style-src 'self'
'unsafe-inline';font-src 'self' data:
content-security-policy-newadmin = default-src 'self';script-src 'self' 'unsafe-inline'
'unsafe-eval' data:;style-src 'self'
'unsafe-inline';font-src 'self' data:;img-src 'self' data:;connect-src 'self' https:
content-security-policy-portal = default-src 'self';script-src 'self' 'unsafe-inline'
'unsafe-eval' data:;style-src 'self'
'unsafe-inline';font-src 'self' data:;img-src 'self' data: blob;;media-src 'self'
blob;;connect-src 'self' wss;;frame-src
'self' blob;;child-src 'self' blob;;object-src 'self' blob:
x-content-type-options = nosniff
x-frame-options = deny
x-frame-options-portal = sameorigin
x-xss-protection = 1; mode=block
```

他の保護手段

Internet Engineering Task Force 標準と W3 標準の他にも、Horizon 7 は HTTP プロトコルを使用する通信を保護するための手段を採用しています。

MIME タイプのセキュリティ リスクの軽減

デフォルトでは、MIME タイプを悪用した攻撃を回避する攻撃を防止するため、Horizon 7 は HTTP 応答でヘッダ **x-content-type-options: nosniff** を送信します。

ファイル **locked.properties** に次のエントリを追加して、この機能を無効にできます。

```
x-content-type-options=OFF
```

クロスサイト スクリプティング攻撃の緩和

デフォルトでは、Horizon 7 は XSS (クロスサイト スクリプティング) フィルタ機能を使用し、HTTP 応答でヘッダ **x-xss-protection=1; mode=block** を送信するクロスサイト スクリプティング攻撃を緩和します。

ファイル **locked.properties** に次のエントリを追加して、この機能を無効にできます。

```
x-xss-protection=OFF
```

コンテンツ タイプの確認

デフォルトでは、Horizon 7 は宣言されたコンテンツ タイプが以下である要求のみを受け入れます。

- application/x-www-form-urlencoded
- application/xml
- text/xml

注: 以前のリリースでは、この保護はデフォルトで無効になっていました。

View が受け入れるコンテンツ タイプを制限するには、**locked.properties** ファイルに次のエントリを追加します。

```
acceptContentType.1=<content-type>
```

例:

```
acceptContentType.1=x-www-form-urlencoded
```

別のコンテンツ タイプを受け入れるには、エントリ **acceptContentType.2=<content-type>** を追加するなどします。

宣言されたコンテンツ タイプを使用する要求を受け入れるには、**acceptContentType=***を指定します。

注: Horizon 7 バージョン 7.2 より前のリリースでは、このリストを変更しても Horizon Administrator との接続に影響はありません。

クライアント動作のモニタリング

接続サーバがクライアントからの要求に使用できるリソースは限られています。誤動作したクライアントがこれらのリソースを占有してしまうと、他のクライアントが要求を処理できなくなります。クライアント動作をモニタリングすることで、誤動作を検出し、回避することができます。

ハンドシェイクの監視

ポート 443 の TLS ハンドシェイクは設定された期間内に完了する必要があります。完了できなかった場合には、強制的に終了されます。デフォルトの期間は 10 秒間です。スマート カード認証が有効になっている場合、ポート 443 の TLS ハンドシェイクは 100 秒以内に完了する必要があります。

必要であれば、**locked.properties** ファイルに次のプロパティを追加して、ポート 443 での TLS ハンドシェイクの時間を調整できます。

```
handshakeLifetime = lifetime_in_seconds
```

例：

```
handshakeLifetime = 20
```

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。詳細については、「[クライアントのブラックリスト登録](#)」を参照してください。

要求受信のモニタリング

HTTP 要求は 30 秒以内に完全に受信する必要があります。それ以外の場合、接続が強制的に終了します。

要求の送信に時間がかかるクライアントを自動的にブラックリストに追加することもできます。詳細については、「[クライアントのブラックリスト登録](#)」を参照してください。

要求数

1 つのクライアントから 1 分あたり 100 を超える HTTP 要求が送信されることは想定されていません。しかしながら、デフォルトでは、このしきい値を超えても何も起こりません。

このしきい値を超えたクライアントを自動的にブラックリストに追加することもできます。詳細については、「[クライアントのブラックリスト登録](#)」を参照してください。

クライアントのブラックリスト登録が有効になっている場合、要求数しきい値の設定が必要になる場合があります。

次のプロパティを **locked.properties** ファイルに追加すると、クライアントあたりの HTTP 要求送信の最大数を調整できます。

```
requestTallyThreshold = max_served_requests_in_30_seconds
```

例：

```
requestTallyThreshold = 100
```

次のプロパティを **locked.properties** ファイルに追加すると、クライアントあたりの HTTP 要求失敗の最大数を調整できます。

```
tarPitGraceThreshold = max_failed_requests_in_30_seconds
```

例：

```
tarPitGraceThreshold = 5
```

クライアントのブラックリスト登録

このタイプの保護機能は、正しく設定していないとパフォーマンスが低下したり、ユーザーに不快感を与えるため、デフォルトでは無効になっています。Unified Access Gateway アプライアンスなどのゲートウェイを使用している場合は、すべてのクライアント接続が同じ IP アドレスで表されるため、クライアントのブラックリスト登録を有効にしないでください。

有効にすると、ブラックリストに登録されたクライアントからの接続は、一定の期間が経過するまで処理が延期されます。同じクライアントからの多くの接続が同時に遅延すると、そのクライアントからの以降の接続は拒否されます。このしきい値は設定可能です。

この機能を有効にするには、**locked.properties** ファイルに次のプロパティを追加します。

```
secureHandshakeDelay = delay_in_milliseconds
```

例：

```
secureHandshakeDelay = 2000
```

HTTPS 接続のブラックリスト登録を無効にするには、**secureHandshakeDelay** エントリを削除するか、0 に設定します。

TLS ハンドシェイクが過剰に発生すると、**handshakeLifetime** と **secureHandshakeDelay** の合計に等しい時間が経過するまで、そのクライアントの IP アドレスがブラックリストに追加されています。

上記の例では、誤動作したクライアントの IP アドレスは 22 秒間ブラックリストに追加されています。

```
(20 * 1000) + 2000 = 22 seconds
```

同じ IP アドレスからの接続が誤動作するたびに、この最小期間は延長されます。最小期間が経過し、この IP アドレスから最後の遅延接続が処理されると、IP アドレスがブラックリストから削除されます。

クライアントがブラックリストに追加されていなくても、TLS ハンドシェイクに時間がかかる場合があります。たとえば、接続が繰り返し切断されたり、存在しない URL に繰り返し接続するなど、一連の要求が同じエラーで終了する場合などがあります。これらのトリガは、ブラックリストの最小期間が異なります。ポート 80 に対する追加トリガの監視を延長するには、**locked.properties** ファイルに次のエントリを追加します。

```
insecureHandshakeDelay = delay_in_milliseconds
```

例：

```
insecureHandshakeDelay = 1000
```

HTTP 接続のブラックリスト登録を無効にするには、**insecureHandshakeDelay** エントリを削除するか、0 に設定します。

動作モニタリングのプロパティ

これらのプロパティを使用すると、クライアントの動作をモニタリングできます。これらのプロパティには、誤動作を検出して回避するためのプロパティが含まれます。

表 9-3. 動作モニタリングのプロパティ

プロパティ	説明	デフォルト値	動的
handshakeLifetime	TLS ハンドシェイクの最大の時間 (秒)。	10 または 100 (「 ハンドシェイクの監視 」を参照)	いいえ
secureHandshakeDelay	ブラックリストに登録されている場合の TLS ハンドシェイクの遅延時間 (ミリ秒)。	0 (ブラックリスト登録が無効の場合)	いいえ
insecureHandshakeDelay	ブラックリストに登録されている場合の TLS 以外のハンドシェイクの遅延時間 (ミリ秒)。	0 (ブラックリスト登録が無効の場合)	いいえ
requestTallyThreshold	30 秒間に処理された HTTP 要求の数 (クライアントのブラックリスト登録)	50	いいえ
tarPitGraceThreshold	30 秒間に処理されなかった HTTP 要求の数 (クライアントのブラックリスト登録)	3	いいえ
secureBlacklist...	ブラックリストに登録されている場合に、ポート 443 ですぐに拒否される IP アドレスのリスト。	なし	はい
insecureBlacklist...	ブラックリストに登録されている場合に、ポート 80 ですぐに拒否される IP アドレスのリスト。	なし	はい
secureWhitelist...	ポート 443 でブラックリストから除外される IP アドレスのリスト。	なし	はい
insecureWhitelist...	ポート 80 でブラックリストから除外される IP アドレスのリスト。	なし	はい

動的のエントリに対する変更はすぐに反映されます。サービスを再起動する必要はありません。

ユーザー エージェントのホワイトリスト登録

ホワイトリストを設定して、Horizon 7 に接続できるユーザー エージェントを制限します。デフォルトでは、すべてのユーザー エージェントが許可されます。

注: 厳密にいうと、これはセキュリティ機能ではありません。ユーザー エージェントの検出は、接続を要求するクライアントのユーザー エージェント リクエスト ヘッダーで行いますが、このヘッダーは偽装される可能性があります。一部のブラウザは、リクエスト ヘッダーの変更をユーザーに許可しています。

ユーザー エージェントは名前と最小バージョンで指定します。例：

```
clientWhitelist-portal.1 = Chrome-14
clientWhitelist-portal.2 = Safari-5.1
```

これは、HTML Access を使用して接続できるのが、Google Chrome バージョン 14 以降と Safari バージョン 5.1 以降であることを意味します。他のサービスには、どのブラウザも接続できます。

認識されている次のユーザー エージェント名を入力できます。

- Android
- Chrome
- Edge
- IE
- Firefox
- Opera
- Safari

注: 他のユーザー エージェントは、Horizon 7 でサポートされていません。例を示します。

HTTP 保護対策の設定

HTTP 保護対策を設定するには、接続サーバまたはセキュリティ サーバ インスタンスの SSL ゲートウェイ設定フォルダにある **locked.properties** ファイルを作成または編集する必要があります。

例：<install_directory>\VMware\VMware
View\Server\sslgateway\conf\locked.properties

- **locked.properties** でプロパティを設定するには、次の構文を使用します。

```
myProperty = newValue
```

- プロパティ名は、常に大文字と小文字が区別されます。プロパティ値では区別されない場合もあります。=記号の前後のスペースは省略可能です。

- CORS と CSP プロパティには、サービス固有の値とマスター値を設定できます。たとえば、管理サービスが Horizon Administrator の要求を処理するため、プロパティ名の後に **-admin** を付けると、他のサービスに影響を及ぼさずに、このサービスにプロパティを設定できます。

```
myProperty-admin = newValueForAdmin
```

- マスター値とサービス固有の値の両方が指定されている場合、サービス固有の値は名前付きのサービスに適用され、マスター値はそれ以外のすべてのサービスに適用されます。唯一の例外は、「OFF」という特別な値です。プロパティのマスター値が「OFF」に設定されている場合、このプロパティのサービス固有の値はすべて無視されます。

例：

```
myProperty = OFF
myProperty-admin = newValueForAdmin ; ignored
```

- 一部のプロパティは、値のリストを取得できます。

単一の値を設定するには、次のプロパティを入力します。

```
myProperty = newValue
myProperty-admin = newValueForAdmin
```

リストの値を取得できるプロパティに複数の値を設定するには、1 行に 1 つの値を指定します。

```
myProperty.1 = newValue1
myProperty.2 = newValue2
myProperty-admin.1 = newValueForAdmin1
myProperty-admin.2 = newValueForAdmin2
```

- サービス固有の設定を作成するときに、使用するサービス名を特定するには、デバッグ ログで以下のシーケンスを含む行を確認します。

```
(ajp:admin:Request21) Request from abc.def.com/10.20.30.40: GET /admin/
```

この例のサービス名は **admin** です。次のような一般的なサービス名を使用できます。

- **admin**(Horizon Administrator)
- **newadmin** for Horizon Console
- **broker** (接続サーバ)
- **docroot** (ローカル ファイル サービス)
- **portal**(HTML Access)
- **saml** (SAML 通信 (vIDM))
- **tunnel** (セキュアなトンネル)
- **view-vlsi**(View API)

- misc (その他)