

# Horizon Client および Agent のセキュリティ

Horizon Client 3.x/4.x および View Agent 6.2.x/Horizon Agent 7.0.x

2016 年 9 月

VMware Horizon 7 7.0



vmware®

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

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

ヴァイエルムウェア株式会社  
105-0013 東京都港区浜松町 1-30-5  
浜松町スクエア 13F  
[www.vmware.com/jp](http://www.vmware.com/jp)

Copyright © 2015 年、2016 年 VMware, Inc. All rights reserved. [著作権および商標情報](#)。

# 目次

## Horizon Client および View Agent のセキュリティ 5

### 1 外部ポート 6

View 通信プロトコルの概要 6

Horizon Agent のファイアウォール ルール 7

クライアントとエージェントで使用する TCP および UDP ポート 7

### 2 インストールされるサービス、デーモン、およびプロセス 11

Windows マシンで View Agent または Horizon Agent のインストーラによってインストールされるサービス 11

Windows クライアントにインストールされるサービス 12

その他のクライアントと Linux デスクトップにインストールされたデーモン 12

### 3 保護するリソース 14

クライアント システムのセキュリティを保護するためのベスト プラクティスの実装 14

構成ファイルの場所 14

アカウント 15

### 4 クライアントとエージェントのセキュリティ設定 17

証明書確認の構成 17

View Agent または Horizon Agent 構成テンプレートのセキュリティ関連の設定 18

Linux デスクトップでの構成ファイルのオプション設定 20

HTML Access のグループ ポリシー設定 23

Horizon Client の構成テンプレートのセキュリティ設定 24

Horizon Client 証明書検証モードの構成 28

### 5 セキュリティ プロトコルと暗号化スイートの構成 30

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ポリシー 30

特定のクライアント タイプのセキュリティ プロトコルおよび暗号化スイートの構成 39

SSL/TLS における強度の弱い暗号化方式の無効化 39

HTML Access Agent のセキュリティ プロトコルと暗号化スイートの構成 40

View デスクトップでの提案ポリシーの構成 41

### 6 クライアントとエージェントのログ ファイルの場所 42

Windows 版 Horizon Client のログ 42

Horizon Client for Mac のログ 44

Linux 版 Horizon Client のログ 45

モバイル デバイス上の Horizon Client のログ 46

Windows マシンの View Agent または Horizon Agent のログ 47

Linux デスクトップのログ 48

## 7 セキュリティ パッチの適用 50

View Agent または Horizon Agent へのパッチの適用 50

Horizon Client のパッチの適用 51

# Horizon Client および View Agent のセキュリティ

『Horizon Client および Agent のセキュリティ』では、VMware Horizon Client<sup>®</sup> および Horizon Agent (Horizon 7) または VMware View Agent<sup>®</sup> (Horizon 6) のセキュリティ機能を簡単に参照できます。このガイドは『View セキュリティ』の関連ガイドであり、VMware Horizon<sup>™</sup> 6 および Horizon 7 のすべてのメジャーバージョンとマイナーバージョンについて制作されています。『Horizon Client および Agent のセキュリティ』ガイドは、クライアントおよびエージェントソフトウェアの四半期ごとのリリースに合わせて四半期ごとに更新されます。

Horizon Client は、エンド ユーザーがクライアント デバイスから起動してリモートのアプリケーションまたはデスクトップに接続するためのアプリケーションです。View Agent (Horizon 6) または Horizon Agent (Horizon 7) は、リモート デスクトップのオペレーティング システム、またはリモート アプリケーションを提供する Microsoft RDS ホストで稼動するエージェント ソフトウェアです。このガイドには次の情報が含まれています。

- 必要なシステム ログイン アカウント。システムのインストールまたはブートストラップ中に作成されるアカウントのログオン ID およびデフォルトを変更する方法についての指示。
- 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。
- サービス ユーザーに適用される権限。
- クライアントとエージェント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、およびサービス。
- お客様が最新のセキュリティ更新プログラムまたはパッチを取得して適用する方法に関する情報。

## 対象読者

本ドキュメントの情報は、クライアントとエージェントなどの、Horizon 6 や 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、IT の意思決定者、アーキテクト、管理者、その他の読者を対象としています。

## VMware の技術ドキュメントの用語集

VMware の技術ドキュメントには、専門的な用語などを集約した用語集があります。VMware の技術ドキュメントで使用されている用語の定義については、<http://www.vmware.com/support/pubs> をご覧ください。

# 外部ポート

製品を適切に動作させるため、また使用する機能によって、さまざまなポートを開いて、クライアントとリモート デスクトップ上のエージェントが相互に通信できるようにする必要があります。

この章には、次のトピックが含まれています。

- [View 通信プロトコルの概要](#)
- [Horizon Agent のファイアウォール ルール](#)
- [クライアントとエージェントで使用される TCP および UDP ポート](#)

## View 通信プロトコルの概要

View のコンポーネントは、複数の異なるプロトコルを使用してメッセージをやりとりします。

[表 1-1. デフォルト ポート](#) に、各プロトコルで使用されるデフォルト ポートを示します。必要に応じて、組織のポリシーに準拠するか競合を回避するために、どのポート番号が使用されるかを変更できます。

表 1-1. デフォルト ポート

プロトコル	ポート
JMS	TCP ポート 4001 TCP ポート 4002
HTTP	TCP ポート 80
HTTPS	TCP ポート 443
MMR/CDR	マルチメディア リダイレクトとクライアント ドライブ リダイレクトでは、TCP ポート 9427
RDP	TCP ポート 3389
PCoIP	リモート デスクトップまたはアプリケーションのポート 4172 への Horizon Client の任意の TCP ポート。 PCoIP は、リモート デスクトップまたはアプリケーションのポート 4172 への Horizon Client の UDP ポート 50002（または PCoIP Secure Gateway の UDP ポート 55000）も使用します。
USB リダイレクト	TCP ポート 32111。このポートはタイム ゾーンの同期にも使用されます。
VMware Blast Extreme	リモート デスクトップまたはアプリケーションのポート 22443 への、または Blast Secure Gateway が使用されている場合、View 接続サーバ、セキュリティ サーバ、Access Point アプライアンスのポート 8443 への Horizon Client の任意の TCP または UDP ポート。
HTML Access	接続サーバおよびセキュリティ サーバ上の HTML Access Gateway では、TCP ポート 8443 View Agent または Horizon Agent の接続では TCP ポート 22443

## Horizon Agent のファイアウォール ルール

Horizon Agent インストール プログラムはファイアウォールの特定の TCP ポートを開きます。これらのポートは、特に記述のない限り受信ポートです。

表 1-2. エージェントのインストール時に開かれる TCP ポート

プロトコル	ポート
RDP	3389
USB リダイレクト	32111 (このポートはタイム ゾーン同期にも使用されます。)
MMR (マルチメディア リダイレクト) と CDR (クライアント ドライブ リダイレクト)	9427
PCoIP	4172 (TCP および UDP)
VMware Blast Extreme	22443 (TCP および UDP)
HTML Access	22443

エージェント インストール プログラムによって、ホスト オペレーティング システムの現在の RDP ポート (通常は 3389) に合わせて受信 RDP 接続のローカル ファイアウォール ルールが構成されます。インストール後にこの RDP ポート番号を変更する場合は、関連するファイアウォール ルールも変更する必要があります。

エージェント インストール プログラムでリモート デスクトップのサポートを有効にしない場合、ポート 3389 および 32111 が開かれないため、それらのポートを手動で開く必要があります。

仮想マシン テンプレートをデスクトップ ソースとして使用する場合は、そのテンプレートがデスクトップ ドメインのメンバーである場合にのみ、デプロイされたデスクトップにファイアウォールの例外が継承されます。Microsoft のグループ ポリシー設定を使用して、ローカルでのファイアウォールの例外を管理できます。詳細については、Microsoft のサポート技術情報 (KB) の記事 875357 を参照してください。

## クライアントとエージェントで使用される TCP および UDP ポート

View Agent (Horizon 6 の場合)、Horizon Agent (Horizon 7 の場合)、および Horizon Client は、互いのネットワーク アクセスや各種 View server 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 ポートを使用します。

Windows クライアントおよびリモート デスクトップおよび RDS ホストのインストール中に、インストーラではオプションで Windows ファイアウォール ルールを構成し、デフォルトで使用さ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。『View のインストール』の「View 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。

表 1-3. View Agent または Horizon Agent 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
Horizon Client	*	View Agent/ 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 View デスクトップへの Microsoft RDP トラフィック。
Horizon Client	*	View Agent/ 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	*	View Agent/ 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	*	View Agent/ Horizon Agent	4172	TCP と UDP	PCoIP Secure Gateway が使用されていない場合の PCoIP。  <b>注:</b> 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	トンネル接続の代わりに直接接続が使用される場合の VMware Blast Extreme。
ブラウザ	*	View Agent/ Horizon Agent	22443	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 HTML Access。
セキュリティ サーバ、 View 接続サーバ、または Access Point アプリ アンス	*	View Agent/ Horizon Agent	3389	TCP	トンネル接続が使用される場合の View 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、 View 接続サーバ、または Access Point アプリ アンス	*	View Agent/ 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、 View 接続サーバ、または Access Point アプリ アンス	*	View Agent/ 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。
セキュリティ サーバ、 View 接続サーバ、または Access Point アプリ アンス	55000	View Agent/ 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、 View 接続サーバ、または Access Point アプリ アンス	*	View Agent/ 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、 View 接続サーバ、または Access Point アプリ 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、 View 接続サーバ、または Access Point アプリ アンス	*	View Agent/ Horizon Agent	22443	TCP	Blast Secure Gateway が使用されている場合の HTML Access。



送信元	ポート	送信先	ポート	プロトコル	説明
View Agent/Horizon Agent	*	View 接続サーバ	4001、4002	TCP	JMS SSL トラフィック。
View Agent/Horizon Agent	4172	Horizon Client	*	UDP	PCoIP Secure Gateway が使用されていない場合の PCoIP。  <b>注:</b> 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。
View Agent/Horizon Agent	4172	View 接続サーバ、セキュリティ サーバ、または Access Point 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)。

**注:** PCoIP 用にエージェントが使用する 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、エージェントは 50003 を選択します。ポート 50003 が使用されている場合、エージェントは 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。

RDS ホストの Horizon Agent に関する Windows ファイアウォール ルールでは、256 個の連続した UDP ポート ブロックが受信トラフィック用に開いていることが示されます。このポート ブロックは、VMWare Blast Extreme が Horizon Agent 内部で使用します。RDS ホストにある Microsoft が署名した特別なドライバによって、外部ソースからこれらのポートへの受信トラフィックがブロックされる場合があります。Microsoft が署名したドライバによって、これらのポートが Windows ファイアウォールによって開かないようになります。

表 1-4. Horizon Client 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
Horizon Client	*	View 接続サーバ、セキュリティ サーバ、または Access Point アプライアンス	443	TCP	View 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	*	View Agent/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 View デスクトップへの Microsoft RDP トラフィック。
Horizon Client	*	View Agent/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レダイレクト。
Horizon Client	*	View Agent/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	*	View Agent/Horizon Agent	4172	TCP と UDP	PCoIP Secure Gateway が使用されていない場合の PCoIP。  <b>注:</b> 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。

送信元	ポート	送信先	ポート	プロトコル	説明
Horizon Client	*	View 接続サーバ、セキュリティ サーバ、または Access Point 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)。  <b>注:</b> 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。
View Agent/Horizon Agent	4172	Horizon Client	*	UDP	PCoIP Secure Gateway が使用されていない場合の PCoIP。  <b>注:</b> 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、View 接続サーバ、または Access Point 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)。  <b>注:</b> 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 Client	*	View 接続サーバ、セキュリティ サーバ、または Access Point アプライアンス	8443	TCP	Blast Secure Gateway が使用されている場合の HTML Access および VMware Blast Extreme。
Horizon Client	*	View 接続サーバ、セキュリティ サーバ、または Access Point アプライアンス	8443	UDP	Blast Secure Gateway が使用されている場合の VMware Blast Extreme。  <b>注:</b> このポートは、Linux デスクトップによって使用されません。

**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。

# インストールされるサービス、デーモン、およびプロセス

## 2

クライアントまたはエージェントのインストーラを実行すると、複数のコンポーネントがインストールされます。

この章には、次のトピックが含まれています。

- Windows マシンで View Agent または Horizon Agent のインストーラによってインストールされるサービス
- Windows クライアントにインストールされるサービス
- その他のクライアントと Linux デスクトップにインストールされたデーモン

## Windows マシンで View Agent または Horizon Agent のインストーラによってインストールされるサービス

リモート デスクトップとアプリケーションの操作は、いくつかの Windows サービスによって決まります。

表 2-1. View Agent（Horizon 6 の場合）または Horizon Agent（Horizon 7 の場合）のサービス

サービス名	スタートアップの種類	説明
VMware Blast	自動	HTML Access と VMware Blast Extreme プロトコルを使用してネイティブ クライアントと接続するためのサービスを提供します。
VMware Horizon View Agent	自動	View Agent/Horizon Agent にサービスを提供します。
VMware Horizon View Composer Guest Agent Server	自動	仮想マシンが View Composer リンク クローン デスクトップ プールの一部である場合、サービスを提供します。
VMware Horizon View Persona Management	機能が有効である場合は自動、その他の場合は無効	VMware の個人設定管理機能にサービスを提供します。
VMware Horizon View スクリプト ホスト	無効	セッション開始スクリプトがある場合はそれを実行し、デスクトップセキュリティ ポリシーを構成してからデスクトップ セッションを開始することがサポートされます。 ポリシーは、クライアント デバイスとユーザーの場所に基づきます。
VMware Netlink Supervisor Service	自動	スキャナ リダイレクト機能およびシリアル ポート リダイレクト機能をサポートするため、カーネル プロセスとユーザー空間プロセスの間で情報を転送する監視サービスを提供します。
VMware Scanner Redirection Client Service	自動	（View Agent 6.0.2 以降）スキャナ リダイレクト機能にサービスを提供します。

サービス名	スタートアップの種類	説明
VMware Serial Com Client Service	自動	(View Agent 6.1.1 以降) シリアル ポート リダイレクト機能にサービスを提供します。
VMware スナップショット プロバイダ	手動	クローン作成に使用される仮想マシンのスナップショットにサービスを提供します。
VMware Tools	自動	ホスト オペレーティング システムとゲスト オペレーティング システムの間でオブジェクトを同期して、仮想マシンのゲスト オペレーティング システムのパフォーマンスを強化し、仮想マシンの管理を改善することがサポートされます。
VMware USB Arbitration Service	自動	クライアントに接続している、さまざまな USB デバイスを列挙し、どのデバイスをクライアントに接続して、どのデバイスをリモート デスクトップに接続するかを判断します。
VMware View USB	自動	USB リダイレクト機能にサービスを提供します。

## Windows クライアントにインストールされるサービス

Horizon Client の操作は、いくつかの Windows サービスによって決まります。

表 2-2. Horizon Client のサービス

サービス名	スタートアップの種類	説明
VMware Horizon Client	自動	Horizon Client のサービスを提供します。
VMware Netlink Supervisor Service	自動	スキャナ リダイレクト機能およびシリアル ポート リダイレクト機能をサポートするため、カーネル プロセスとユーザー空間プロセスの間で情報を転送する監視サービスを提供します。
VMware Scanner Redirection Client Service	自動	(Horizon Client 3.2 以降) スキャナ リダイレクト機能にサービスを提供します。
VMware Serial Com Client Service	自動	(Horizon Client 3.4 以降) シリアル ポート リダイレクト機能にサービスを提供します。
VMware USB Arbitration Service	自動	クライアントに接続している、さまざまな USB デバイスを列挙し、どのデバイスをクライアントに接続して、どのデバイスをリモート デスクトップに接続するかを判断します。
VMware View USB	自動	USB リダイレクト機能にサービスを提供します。

## その他のクライアントと Linux デスクトップにインストールされたデーモン

セキュリティ上の理由により、Horizon Client によってデーモンまたはプロセスがインストールされているかどうかを知ることが重要です。

表 2-3. Horizon Client によってクライアント タイプごとにインストールされたサービス、プロセス、またはデーモン

タイプ	サービス、プロセス、またはデーモン
Linux クライアント	<ul style="list-style-type: none"> <li>■ <b>vmware-usbarbitrator</b>。クライアントに接続されているさまざまな USB デバイスを列挙し、クライアントに接続するデバイスとリモート デスクトップに接続するデバイスを決定します。</li> <li>■ <b>vmware-view-used</b>。USB リダイレクト機能のサービスを提供します。</li> </ul> <p><b>注:</b> これらのデーモンは、インストール時に [インストール後にサービスを登録して起動する] チェック ボックスをクリックすると自動的に開始されます。これらのプロセスはルートとして動作します。</p>
Mac クライアント	Horizon Client はデーモンを作成しません。
Chrome クライアント	Horizon Client は 1 つの Android プロセスで動作します。Horizon Client はデーモンを作成しません。
iOS クライアント	Horizon Client はデーモンを作成しません。
Android クライアント	Horizon Client は 1 つの Android プロセスで動作します。Horizon Client はデーモンを作成しません。
Windows ストア クライアント	Horizon Client はシステム サービスの作成やトリガを行いません。
Linux デスクトップ	<ul style="list-style-type: none"> <li>■ <b>StandaloneAgent</b>。root 権限で実行され、Linux システムの稼動時に開始されます。StandaloneAgent。View 接続サーバと通信し、リモート デスクトップのセッション管理（セッションのセットアップや分解を行い、View 接続サーバのプロローカーに対するリモート デスクトップ ステータスの更新）を実行します。</li> <li>■ <b>VMwareBlastServer</b>。StartSession 要求が View 接続サーバから受信されると StandaloneAgent によって開始されます。VMwareBlastServer デーモンは vmwblast (Linux Agent のインストール時に作成されるシステム アカウント) 権限で実行されます。StandaloneAgent との通信には内部の MKSControl チャネルを使用し、Horizon Client との通信には Blast プロトコルを使用します。</li> </ul>

## 保護するリソース

これらのリソースには、関連する構成ファイル、パスワード、アクセス制御が含まれます。

この章には、次のトピックが含まれています。

- クライアント システムのセキュリティを保護するためのベスト プラクティスの実装
- 構成ファイルの場所
- アカウント

### クライアント システムのセキュリティを保護するためのベスト プラクティスの実装

クライアント システムのセキュリティを保護するためのベスト プラクティスを実装する必要があります。

- クライアント システムが、一定期間動作していない場合にスリープ状態になり、コンピュータをアクティブにする前にユーザーがパスワードを入力する必要があるように構成されていることを確認してください。
- クライアント システムの起動時に、ユーザーはユーザー名とパスワードを入力する必要があります。クライアント システムで自動ログインを許可するように構成しないでください。
- Mac クライアント システムの場合、キーチェーンとユーザー アカウントに異なるパスワードを設定することを考慮してください。パスワードが異なる場合、システムが自動的にパスワードを入力する前に、ユーザーに入力が要求されます。さらに、FileVault 保護を有効にすることも考慮してください。

### 構成ファイルの場所

保護する必要があるリソースには、セキュリティ関連の構成ファイルが含まれます。

表 3-1. 各クライアント タイプの構成ファイルの場所

タイプ	ディレクトリパス
Linux クライアント	<p>Horizon Client の起動時、各場所で構成設定が次の順序で処理されます。</p> <ol style="list-style-type: none"> <li>1 /etc/vmware/view-default-config</li> <li>2 ~/.vmware/view-preferences</li> <li>3 /etc/vmware/view-mandatory-config</li> </ol> <p>設定が複数の場所で定義されている場合、使用される値は、読み取られた最後のファイルまたはコマンドライン オプションの値になります。</p>
Windows クライアント	<p>個人情報が含まれる場合があるユーザー設定は、次のファイルにあります。</p> <p>C:\Users\user-name\AppData\Roaming\VMware\VMware Horizon View Client\prefs.txt</p>
Mac クライアント	<p>Mac クライアントの起動後に生成される、一部の構成ファイル。</p> <ul style="list-style-type: none"> <li>■ \$HOME/Library/Preferences/com.vmware.horizon.plist</li> <li>■ \$HOME/Library/Preferences/com.vmware.vmr.plist</li> <li>■ \$HOME/Library/Preferences/com.vmware.horizon.keyboard.plist</li> <li>■ /Library/Preferences/com.vmware.horizon.plist</li> </ul>
Chrome クライアント	<p>セキュリティ関連の設定は、構成ファイルではなく、ユーザー インターフェイスに表示されます。構成ファイルは、どのユーザーに対しても表示されません。</p>
iOS クライアント	<p>セキュリティ関連の設定は、構成ファイルではなく、ユーザー インターフェイスに表示されます。構成ファイルは、どのユーザーに対しても表示されません。</p>
Android クライアント	<p>セキュリティ関連の設定は、構成ファイルではなく、ユーザー インターフェイスに表示されます。構成ファイルは、どのユーザーに対しても表示されません。</p>
Windows ストア クライアント	<p>セキュリティ関連の設定は、構成ファイルではなく、ユーザー インターフェイスに表示されます。構成ファイルは、どのユーザーに対しても表示されません。</p>
View Agent または Horizon Agent (Windows オペレーティングシステムを 搭載したリモート デスクトップ)	<p>セキュリティ関連の設定は、Windows レジストリのみに表示されます。</p>
Linux デスクトップ	<p>テキスト エディタを使用して次の構成ファイルを開き、SSL 関連の設定を指定できます。</p> <p>/etc/vmware/viewagent-custom.conf</p>

## アカウント

Client ユーザーには Active Directory のアカウントが必要です。

### Horizon Client ユーザー アカウント

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。RDP プロトコルを使用する計画がある場合、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にする必要があります。

通常、エンド ユーザーは View 管理者にしないでください。View 管理者がユーザーの使用環境を確認する必要がある場合は、別のテスト アカウントを作成して資格を与えます。デスクトップでは、View のエンド ユーザーを管理者などの特権グループのメンバーにしないでください。エンド ユーザーが、ロック ダウンされた構成ファイルおよび Windows のレジストリを変更できるようになってしまいます。

## インストール中に作成されるシステム アカウント

Horizon Client アプリケーションでは、どの種類のクライアントにもサービス ユーザー アカウントは作成されません。Horizon Client for Windows で作成されるサービスでは、ログオン ID が Local System になります。

Mac クライアントでは、最初の起動時に、ユーザーが Local Admin アクセス権を付与して、USB および仮想印刷 (ThinPrint) サービスを起動する必要があります。これらのサービスを初めて起動した後で、標準ユーザーにこれらのサービスの実行アクセス権が与えられます。同じように、Linux クライアントでは、インストール中に [インストール後にサービスを登録して起動する] チェック ボックスをオンにすると、`vmware-usbarbitrator` デーモンと `vmware-view-used` デーモンが自動的に起動します。これらのプロセスはルートとして動作します。

Windows デスクトップでは、View Agent または Horizon Agent でサービス ユーザー アカウントは作成されません。Linux デスクトップでは、システム アカウント `vmwblast` が作成されます。Linux デスクトップの場合、`StandaloneAgent` デーモンはルート権限で動作し、`VmwareBlastServer` デーモンは `vmwblast` 権限で動作します。



# クライアントとエージェントのセキュリティ設定

# 4

クライアントとエージェントの設定をいくつか使用して、構成のセキュリティを調整できます。グループ ポリシー オブジェクトを使用したり、Windows レジストリ設定を編集したりして、リモート デスクトップと Windows クライアントの設定にアクセスできます。

ログ収集に関する構成設定については、[6 章 クライアントとエージェントのログ ファイルの場所](#)を参照してください。セキュリティ プロトコルと暗号化スイートに関連する構成設定については、[5 章 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。

この章には、次のトピックが含まれています。

- [証明書確認の構成](#)
- [View Agent または Horizon Agent 構成テンプレートのセキュリティ関連の設定](#)
- [Linux デスクトップでの構成ファイルのオプション設定](#)
- [HTML Access のグループ ポリシー設定](#)
- [Horizon Client の構成テンプレートのセキュリティ設定](#)
- [Horizon Client 証明書検証モードの構成](#)

## 証明書確認の構成

管理者は、証明書検証モードを構成し、たとえば、完全な検証を常に実行するようにすることができます。管理者は、サーバの証明書の確認が失敗した場合にクライアント接続を拒否するかどうかについて、エンド ユーザーが選択できるかどうかを設定することもできます。

証明書確認は、View Server と Horizon Client 間の SSL/TLS 接続に対して実行されます。管理者は、次のいずれかの方法を使用するように検証モードを構成できます。

- エンド ユーザーに検証モードの選択を許可します。このリストのこれ以降では、3 つの検証モードを説明します。
- (検証なし) 証明書確認は実行されません。
- (警告) 自己署名証明書がサーバによって提示されると、エンド ユーザーに警告が通知されます。ユーザーは、このタイプの接続を許可するかどうかを選択できます。
- (フル セキュリティ) フル検証が実行され、フル検証をパスしない接続は拒否されます。

証明書検査では、次のような検査が行われます。

- 証明書は失効しているか。
- 証明書の目的は、送信側の ID 検証やサーバ通信の暗号化以外にあるか。つまり、証明書のタイプは正しいか。
- 証明書は期限切れになっているか、また有効なのは未来のみか。つまり、証明書はコンピュータの時刻に応じて有効になっているか。
- 証明書上の共通名は、それを送信するサーバのホスト名と一致しているか。ロード バランサが Horizon Client を、Horizon Client で入力したホスト名と一致しない証明書を持つサーバにリダイレクトした場合、不一致が発生する可能性があります。クライアントにホスト名ではなく IP アドレスを入力した場合でも、不一致の原因となる可能性があります。
- 不明なまたは信頼されていない証明機関 (CA) によって署名された証明書か。自己署名された証明書は、信頼されていない CA の証明書タイプの 1 つです。

チェックをパスするには、証明書のトラスト チェーンが、デバイスのローカル証明書ストアでルートになっている必要があります。

特定のタイプのクライアントの証明書確認を構成する方法については、そのクライアントに関する『VMware Horizon Client の使用』ドキュメントを参照してください。このドキュメントは [https://www.vmware.com/support/viewclients/doc/viewclients\\_pubs-archive.html](https://www.vmware.com/support/viewclients/doc/viewclients_pubs-archive.html) の Horizon Client ドキュメント ページから入手できます。また、これらのドキュメントには、自己署名証明書の使用に関する情報も含まれています。

## View Agent または Horizon Agent 構成テンプレートのセキュリティ関連の設定

View Agent または Horizon Agent の ADM テンプレート ファイル (vdm\_agent.adm) には、セキュリティ関連の設定があります。特に記述のない限り、これらの設定にはコンピュータの構成の設定のみが含まれます。

セキュリティ設定は、HKLM\Software\VMware, Inc.\VMware VDM\Agent\Configuration にあるゲストマシンのレジストリに保存されます。

表 4-1. View Agent（Horizon 6 の場合）または Horizon Agent（Horizon 7 の場合）の構成テンプレートのセキュリティ関連の設定

設定	説明
AllowDirectRDP	<p>Horizon Client デバイス以外のクライアントが RDP を使用してリモート デスクトップに直接接続できるかどうかを指定します。この設定が無効になっていると、エージェントでは、Horizon Client 経由での View によって管理される接続のみが許可されます。</p> <p>Horizon Client for Mac からリモート デスクトップに接続する場合は、AllowDirectRDP の設定を無効にしないでください。この設定を無効にすると、Access is denied(アクセスが拒否されました) エラーが発生して接続に失敗します。</p> <p>デフォルトの設定の場合、ユーザーは、View デスクトップ セッションにログイン中に RDP を使用して、View の外側から仮想マシンに接続できます。RDP 接続によって View デスクトップ セッションが終了し、View ユーザーの保存されていないデータや設定は失われます。View ユーザーは、外部の RDP 接続が開かれるまで、デスクトップにログインできません。この状況を回避するには、AllowDirectRDP 設定を無効にします。</p> <hr/> <p><b>重要:</b> View を正しく動作させるために、Windows リモート デスクトップ サービスが各デスクトップのゲスト OS で実行されている必要があります。この設定を使用して、ユーザーが自分のデスクトップに直接 RDP 接続を作成することを不可にできます。</p> <hr/> <p>デフォルトでは、この設定は有効になっています。</p> <p>これに相当する Windows レジストリの値は AllowDirectRDP です。</p>
AllowSingleSignon	<p>シングル サインオン (SSO) を使用して、ユーザーをデスクトップおよびアプリケーションに接続するかどうかを決定します。この設定が有効になっていると、ユーザーはサーバにログインするときに、自分の認証情報を 1 回入力するだけで済みます。この設定を無効にすると、ユーザーはリモート接続の確立時に再認証する必要があります。</p> <p>デフォルトでは、この設定は有効になっています。</p> <p>これに相当する Windows レジストリの値は AllowSingleSignon です。</p>
CommandsToRunOnConnect	<p>セッションに初めて接続するときに実行されるコマンドまたはコマンド スクリプトのリストを指定します。</p> <p>デフォルトではリストは指定されていません。</p> <p>これに相当する Windows レジストリの値は CommandsToRunOnConnect です。</p>
CommandsToRunOnDisconnect	<p>セッションが切断されたときに実行されるコマンドまたはコマンド スクリプトのリストを指定します。</p> <p>デフォルトではリストは指定されていません。</p> <p>これに相当する Windows レジストリの値は CommandsToRunOnReconnect です。</p>
CommandsToRunOnReconnect	<p>セッションが切断された後、再接続されるときに実行されるコマンドまたはコマンド スクリプトのリストを指定します。</p> <p>デフォルトではリストは指定されていません。</p> <p>これに相当する Windows レジストリの値は CommandsToRunOnDisconnect です。</p>

設定	説明
ConnectionTicketTimeout	<p>View 接続チケットが有効な時間（秒）を指定します。</p> <p>Horizon Client デバイスは、エージェントに接続するときに、検証とシングル サインオンのために接続チケットを使用します。セキュリティ上の理由から、接続チケットは限られた期間のみ有効です。ユーザーがリモート デスクトップに接続するときは、接続チケットのタイムアウト期間内に認証を行う必要があります。そうでないとセッションがタイムアウトになります。この設定が構成されていない場合、デフォルトのタイムアウト期間は 900 秒になります。</p> <p>これに相当する Windows レジストリの値は VdmConnectionTicketTimeout です。</p>
CredentialFilterExceptions	<p>エージェントの CredentialFilter のロードを許可されていない実行可能ファイルを指定します。ファイル名にパスまたはサフィックスを含めることはできません。複数のファイル名を区切るにはセミコロンを使用します。</p> <p>デフォルトではリストは指定されていません。</p> <p>これに相当する Windows レジストリの値は CredentialFilterExceptions です。</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、『View 管理ガイド』を参照してください。

## Linux デスクトップでの構成ファイルのオプション設定

/etc/vmware/config ファイルまたは /etc/vmware/viewagent-custom.conf ファイルにエントリを追加して、特定のオプションを構成できます。

インストーラは、View Agent または Horizon Agent のインストール中に、2 つの構成テンプレート ファイル config.template と viewagent-custom.conf.template を /etc/vmware にコピーします。/etc/vmware/config ファイルと /etc/vmware/viewagent-custom.conf ファイルが存在しない場合、インストーラは config.template を config に、viewagent-custom.conf.template を viewagent-custom.conf にコピーします。テンプレート ファイルではすべての構成オプションがリストされていて、詳細な説明があります。オプションを設定するには、コメントを削除して値を適切に変更します。

構成を変更したら、Linux を再起動して変更を有効にしてください。

### /etc/vmware/config の構成オプション

VMwareBlastServer およびその関連プラグインでは、構成ファイル /etc/vmware/config が使用されます。

表 4-2. /etc/vmware/config の構成オプション

オプション	値	デフォルト	説明
WC.ScRedir.Enable	TRUE または FALSE	TRUE	スマート カード リダイレクトを無効にします。
WC.logLevel	FATAL、ERROR、WARN、INFO、DEBUG、または TRACE	INFO	このオプションを使用して、WC プロキシ ノードのログ レベルを設定します。
WC.RTAV.Enable	TRUE または FALSE	TRUE	このオプションを設定してオーディオ入力を無効にします。

オプション	値	デフォルト	説明
Clipboard.Direction	0、1、2、3	2	このオプションにより、クリップボード リダイレクト ポリシーが決定されます。 <ul style="list-style-type: none"> <li>■ 0 - クリップボード リダイレクトを無効にします。</li> <li>■ 1 - クリップボード リダイレクトを両方向で有効にします。</li> <li>■ 2 - クリップボード リダイレクトをクライアントからリモート デスクトップのみで有効にします。</li> <li>■ 3 - クリップボード リダイレクトをリモート デスクトップからクライアントのみで有効にします。</li> </ul>
mksVNCServer.useXExtButtonMapping	TRUE または FALSE	FALSE	このオプションを設定して SLED 11 SP3 での左手用マウスのサポートを有効または無効にします。
mksvhan.clipboardSize	INTEGER	1024	このオプションを使用して、クリップボードの最大サイズをコピーおよび貼り付けます。
RemoteDisplay.maxBandwidthKbps	INTEGER	4096000	VMware Blast セッションの最大帯域幅をキロビット/秒 (kbps) 単位で指定します。この帯域幅には、イメージ、オーディオ、仮想チャネル、および VMware Blast 制御のすべてのトラフィックが含まれます。最大値は、4 Gbps (4096000) です。
RemoteDisplay.maxFPS	INTEGER	60	画面更新の最大レートを指定します。この設定を使用して、ユーザーが使用する平均帯域幅を管理します。有効値は 3 から 60 までの間にする必要があります。デフォルトは 1 秒あたり 60 回の更新です。
RemoteDisplay.enableStats	TRUE または FALSE	FALSE	帯域幅、FPS、RTT などでは、Blast protocol statistics を mks ログで有効または無効にします。
RemoteDisplay.allowH264	TRUE または FALSE	TRUE	H.264 エンコードを有効または無効にするようにこのオプションを設定します。
vdpservice.log.logLevel	FATAL、ERROR、WARN、INFO、DEBUG、または TRACE	INFO	このオプションを使用して、vdpservice のログ レベルを設定します。
RemoteDisplay.qpmaxH264	利用可能な値の範囲：0 ~ 51	36	このオプションを使用して、H264minQP 量子化パラメータを設定します。このパラメータは、H.264 エンコードを使用するように構成されたリモート ディスプレイの最高イメージ品質を指定します。RemoteDisplay.qpminH264 に設定した値よりも大きな値を設定します。
RemoteDisplay.qpminH264	利用可能な値の範囲：0 ~ 51	10	このオプションを使用して、H264maxQP 量子化パラメータを設定します。このパラメータは、H.264 エンコードを使用するように構成されたリモート ディスプレイの最低イメージ品質を指定します。RemoteDisplay.qpmaxH264 に設定した値よりも小さな値を設定します。
RemoteDisplay.minQualityJPEG	利用可能な値の範囲：1 ~ 100	25	JPEG/PNG エンコードを使用する場合のデスクトップ ディスプレイのイメージ品質を指定します。低品質設定は、スクロール発生時など、頻繁に変化する画面の領域に適しています。

オプション	値	デフォルト	説明
RemoteDisplay.midQualityJPEG	利用可能な値の範囲：1～100	35	JPEG/PNG エンコードを使用する場合のデスクトップ ディスプレイのイメージ品質を指定します。デスクトップ ディスプレイの中程度の品質を設定するために使用します。
RemoteDisplay.maxQualityJPEG	利用可能な値の範囲：1～100	90	JPEG/PNG エンコードを使用する場合のデスクトップ ディスプレイのイメージ品質を指定します。高品質設定は、より静的な画面の領域に適していて、イメージ品質がより高くなります。

## /etc/vmware/viewagent-custom.conf の構成オプション

Java Standalone Agent では、構成ファイル `/etc/vmware/viewagent-custom.conf` が使用されます。

表 4-3. `/etc/vmware/viewagent-custom.conf` の構成オプション

オプション	値	デフォルト	説明
サブネット	NULL、または IP アドレス/CIDR 形式のネットワークアドレスとマスク	NULL	<p>異なるサブネットを持つ複数のローカル IP アドレスがある場合、このオプションを使用して、Linux エージェントが View 接続サーバに提供するサブネットを設定します。</p> <p>Linux エージェント マシンで複数のサブネット構成が検出される場合、Linux エージェントが使用する適切なサブネットを指定するために、このオプションが必要です。たとえば、Docker を Linux マシンにインストールした場合、Docker は仮想ネットワーク アダプタとして導入されます。Linux エージェントが仮想ネットワーク アダプタとして Docker を使用しないようにするには、このオプションを設定し、実際の物理ネットワーク アダプタを使用する必要があります。</p> <p>IP アドレス/CIDR 形式で値を指定する必要があります。例： Subnet=192.168.1.0/24</p> <p>NULL は、Linux エージェントがランダムに IP アドレスを選択することを意味します。</p>
SSOEnable	TRUE または FALSE	TRUE	シングル サインオン (SSO) を無効にします。
SSOUserFormat	テキスト文字列	[username]	<p>シングル サインオンのログイン名の形式を指定します。デフォルトはユーザー名のみです。ドメイン名も要求する場合は、このオプションを設定します。一般的にログイン名では、ドメイン名と特殊文字にユーザー名を続けます。特殊文字をバックスラッシュにする場合は、別のバックスラッシュを使用してエスケープする必要があります。ログイン名の形式の例を次に挙げます。</p> <ul style="list-style-type: none"> <li>■ SSOUserFormat=[domain]\\[username]</li> <li>■ SSOUserFormat=[domain]+[username]</li> <li>■ SSOUserFormat=[username]@[domain]</li> </ul>
StartBlastServerTime out	整数	20	VMwareBlastServer プロセスで初期化に使用する時間を秒単位で決めます。このタイムアウト値以内にプロセスの準備ができない場合、ユーザーのログインは失敗します。
SSLCiphers	テキスト文字列	!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES	暗号化のリストを指定します。 <a href="https://www.openssl.org/docs/manmaster/apps/ciphers.html">https://www.openssl.org/docs/manmaster/apps/ciphers.html</a> で定義されている形式を使用する必要があります。

オプション	値	デフォルト	説明
SSLProtocols	テキスト文字列	TLSv1_1:TLSv1_2	セキュリティ プロトコルを指定します。サポートされるプロトコルは、TLSv1.0、TLSv1.1、TLSv1.2 です。
SSLCipherServerPreference	TRUE または FALSE	TRUE	オプション SSL_OP_CIPHER_SERVER_PREFERENCE を有効または無効にします。詳細については、 <a href="https://www.openssl.org/docs/manmaster/ssl/SSL_CTX_set_options.html">https://www.openssl.org/docs/manmaster/ssl/SSL_CTX_set_options.html</a> を参照してください。
LogCnt	整数	-1	このオプションを使用して、/tmp/vmware-root に保持するログ ファイルの数を設定します。 <ul style="list-style-type: none"> <li>■ -1 - すべて保持</li> <li>■ 0 - すべて削除</li> <li>■ &gt; 0 - 保持するログの数。</li> </ul>
RunOnceScript			このオプションを使用して、クローン作成された仮想マシンを Active Directory へ再参加させます。  ホスト名の変更後、RunOnceScript を設定します。指定されたスクリプトは、最初のホスト名の変更後、一度だけ実行されます。Agent サービスが開始され、ホスト名が Agent のインストール後に変更された場合、スクリプトは root 権限として実行されます。  たとえば、winbind ソリューションでは、winbind でベース仮想マシンを Active Directory に参加させ、このオプションをスクリプトパスに設定する必要があります。これには、ドメインへ再度参加させるコマンド /usr/bin/net ads join -U <ADUserName> %<ADUserPassword> が含まれている必要があります。仮想マシンのクローン作成後、オペレーティング システムのカスタマイズによってホスト名が変更されます。Agent サービスが開始されると、クローン作成された仮想マシンを Active Directory へ参加するスクリプトが実行されます。
RunOnceScriptTimeout		120	このオプションを使用して、RunOnceScript オプションのタイムアウト値を秒数で設定します。  たとえば、RunOnceScriptTimeout=120 のように設定します。

**注:** 3つのセキュリティ オプション、SSLCiphers、SSLProtocols、SSLCipherServerPreference は VMwareBlastServer プロセス用です。VMwareBlastServer プロセスが開始されると、Java Standalone Agent はこれらのオプションをパラメータとして渡します。Blast Secure Gateway (BSG) が有効であるとき、これらのオプションは BSG と Linux デスクトップの間の接続に影響します。BSG が無効であるとき、これらのオプションはクライアントと Linux デスクトップの間の接続に影響します。

## HTML Access のグループ ポリシー設定

HTML Access のグループ ポリシー設定は、テンプレート ファイル `vdm_blast.adm` で指定されます。このテンプレートは、HTML Access が使用する唯一の表示プロトコルである VMware Blast 表示プロトコル用です。

HTML Access 4.0 および Horizon 7.0 の VMware Blast グループ ポリシー設定については、『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「VMware Blast ポリシー設定」で説明されています。

次の表は、HTML Access 3.5 以前および Horizon 6.2.x 以前を使用している場合に HTML Access に適用されるグループ ポリシー設定について示しています。Horizon 7.0 以降では、さらに多くの VMware Blast グループ ポリシー設定を利用できます。

表 4-4. HTML Access 3.5 以前のグループ ポリシー設定

設定	説明
空の画面	<p>リモート仮想マシンが、HTML Access セッション中に View の外から見ることを制御します。たとえば、管理者は vSphere Web クライアントを使用して、ユーザーが HTML Access を介してデスクトップに接続されている間に仮想マシンでコンソールを開く場合があります。</p> <p>この設定が有効になっているか構成されていない場合で、HTML Access セッションがアクティブである間に誰かが View の外からリモート仮想マシンにアクセスを試みる場合、リモート仮想マシンは空の画面を表示します。</p>
セッションのガーベッジ コレクション	<p>破棄されたリモート セッションのガーベッジ コレクションを制御します。この設定を有効にすると、ガーベッジ コレクションの間隔としきい値を構成できます。</p> <p>間隔はガーベッジ コレクタが実行される頻度を制御します。ミリ秒単位で間隔を設定します。</p> <p>しきい値は、セッションが破棄された後でそれが削除候補となる前までに必要となる経過時間を決定します。秒単位でしきい値を設定します。</p>
クリップボード リダイレクトの構成	<p>クリップボード リダイレクトを許可する方向を決定します。テキストのみをコピーおよび貼り付けできます。次のいずれかの値を選択できます。</p> <ul style="list-style-type: none"> <li>■ [クライアントからサーバの方向のみ有効] (すなわち、クライアント システムからリモート デスクトップにのみ、コピーおよび貼り付けを許可します。)</li> <li>■ [どちらの方向も無効]</li> <li>■ [どちらの方向も有効]</li> <li>■ [サーバからクライアントの方向のみ有効] (すなわち、リモート デスクトップからクライアント システムにのみ、コピーおよび貼り付けを許可します。)</li> </ul> <p>この設定は View Agent または Horizon Agent にのみ適用されます。</p> <p>この設定が無効または構成されていない場合、デフォルト値は [クライアントからサーバの方向のみ有効] です。</p>
HTTP サービス	<p>Blast Agent サービス用のセキュアな (HTTPS) TCP ポートに変更可能です。デフォルトのポートは 22443 です。</p> <p>この設定を有効にしてポート番号を変更します。この設定を変更する場合は、影響を受けるリモート デスクトップ (View Agent または Horizon Agent のインストール先) のファイアウォールの設定も更新する必要があります。</p>

## Horizon Client の構成テンプレートのセキュリティ設定

Horizon Client の ADM テンプレート ファイル (vdm\_client.adm) のセキュリティ セクションとスクリプト定義 セクションには、セキュリティ関連の設定があります。特に注記のない限り、これらの設定にはコンピュータの構成の設定のみが含まれます。ユーザーの構成の設定が利用可能であり、値を定義している場合には、同等のコンピュータの構成の設定は上書きされます。

次の表では、ADM テンプレート ファイルにおけるセキュリティ セクションの設定について説明します。



表 4-5. Horizon Client の構成テンプレート：セキュリティ設定

設定	説明
Allow command line credentials ([コンピュータの構成] 設定)	<p>Horizon Client のコマンドライン オプションでユーザー認証情報を指定できるかどうかを指定します。この設定が無効になっていると、ユーザーがコマンドラインから Horizon Client を実行するときに smartCardPIN および password オプションは使用できません。</p> <p>デフォルトでは、この設定は有効になっています。</p> <p>これに相当する Windows レジストリの値は AllowCmdLineCredentials です。</p>
Servers Trusted For Delegation ([コンピュータの構成] 設定)	<p>ユーザーが [Log in as current user (現在のユーザーとしてログイン)] チェック ボックスを選択すると渡されるユーザー ID と認証情報を受け付ける View 接続サーバインスタンスを指定します。View 接続サーバインスタンスを指定しない場合は、すべての View 接続サーバインスタンスがこの情報を受け付けます。</p> <p>View 接続サーバ インスタンスを追加するには、次のいずれかの形式を使用します。</p> <ul style="list-style-type: none"> <li>■ domain\system\$</li> <li>■ system\$@domain.com</li> <li>■ View 接続サーバ サービスのサービス プリンシパル名 (SPN)</li> </ul> <p>これに相当する Windows レジストリの値は BrokersTrustedForDelegation です。</p>
Certificate verification mode ([コンピュータの構成] 設定)	<p>Horizon Client で実行される証明書確認のレベルを構成します。次のいずれかのモードを選択できます。</p> <ul style="list-style-type: none"> <li>■ No Security. View は、証明書確認を実行しません。</li> <li>■ Warn But Allow. View が自己署名証明書を提示すると、警告が表示されます。ただし、ユーザーは View 接続サーバへの接続を継続できます。証明書名は、Horizon Client のユーザーによって提供される View 接続サーバ名と一致する必要はありません。その他の証明書エラーが発生すると、View でエラー ダイアログ ボックスが表示され、ユーザーは View 接続サーバに接続できません。Warn But Allow はデフォルト値です。</li> <li>■ Full Security. 証明書に関する何らかのエラーが発生すると、ユーザーは View 接続サーバに接続できなくなります。View で証明書エラーが表示されます。</li> </ul> <p>このグループ ポリシー設定が構成されると、ユーザーは選択した証明書検証モードを Horizon Client で確認できますが、設定を構成することはできません。ユーザー向けの SSL 構成に関するダイアログ ボックスには、管理者が設定をロックしたことが表示されます。</p> <p>この設定が未構成が無効になっている場合、Horizon Client ユーザーは証明書検証モードを選択できます。</p> <p>グループ ポリシーとして証明書検証設定を構成したくない場合は、さらに、Windows レジストリ設定を修正して証明書検証を有効にできます。</p>
Default value of the 'Log in as current user' checkbox ([コンピュータおよびユーザー構成] 設定)	<p>Horizon Client 接続ダイアログ ボックスの [現在のユーザーとしてログイン] チェックボックスのデフォルトの値を指定します。</p> <p>この設定により、Horizon Client インストール中に指定したデフォルトの値が上書きされます。ユーザーがコマンドラインから Horizon Client を実行し、logInAsCurrentUser オプションを指定すると、この設定はその値によって上書きされます。</p> <p>[現在のユーザーとしてログイン] チェック ボックスをオンにすると、ユーザーがクライアント システムにログインするときに入力した ID と認証情報が、View 接続サーバインスタンスに、そして最終的にはリモート デスクトップに渡されます。チェック ボックスをオフにすると、ユーザーはリモート デスクトップにアクセスするまでに ID と認証情報を何回も入力する必要があります。</p> <p>デフォルトでは、この設定は無効になっています。</p> <p>これに相当する Windows レジストリの値は LogInAsCurrentUser です。</p>

設定	説明
<b>Display option to Log in as current user</b> ([コンピュータおよびユーザー構成] 設定)	<p>[現在のユーザーとしてログイン] チェックボックスは Horizon Client 接続ダイアログ ボックスで表示できるかどうかを指定します。</p> <p>チェック ボックスを表示すると、ユーザーはそれをオンまたはオフにして、デフォルト値を上書きできます。チェック ボックスを表示しないと、ユーザーは Horizon Client の接続ダイアログ ボックスからデフォルト値をオーバーライドできません。</p> <p>Default value of the 'Log in as current user' checkbox のポリシー設定を使用することで、[現在のユーザーとしてログイン] チェック ボックスのデフォルト値を指定できます。</p> <p>デフォルトでは、この設定は有効になっています。</p> <p>これに相当する Windows レジストリの値は <code>LogInAsCurrentUser_Display</code> です。</p>
<b>Enable jump list integration</b> ([コンピュータの構成] 設定)	<p>Windows 7 以降のシステムのタスクバーにある Horizon Client アイコンにジャンプ リストを表示するかどうかを決定します。ユーザーはこのジャンプ リストを使用して、最近使った View 接続 サーバ インスタンスおよびリモート デスクトップに接続できます。</p> <p>Horizon Client が共有されている場合、最近使用したデスクトップの名前を他のユーザーに見られたくないことがあります。この設定を無効にすると、ジャンプ リストを非表示にできます。</p> <p>デフォルトでは、この設定は有効になっています。</p> <p>これに相当する Windows レジストリの値は <code>EnableJumplist</code> です。</p>
<b>Enable SSL encrypted framework channel</b> ([コンピュータおよびユーザー構成] 設定)	<p>SSL を View 5.0 以前のデスクトップで有効にするかどうかを決定します。View 5.0 以前では、ポート TCP 32111 経由でデスクトップに送信されるデータが暗号化されませんでした。</p> <ul style="list-style-type: none"> <li>■ [有効化] : SSL を有効にしますが、リモート デスクトップで SSL がサポートされていない場合は、非暗号化接続に戻ることを許可します。たとえば、View 5.0 以前のデスクトップでは SSL がサポートされていません。[有効化] はデフォルトの設定です。</li> <li>■ [無効化] : SSL を無効にします。この設定は推奨されませんが、デバッグする場合、またはチャネルがトンネリングされず、WAN アクセラレータ製品によって最適化される可能性がある場合に便利ことがあります。</li> <li>■ [強制] : SSL を有効にし、SSL がサポートされていないデスクトップへの接続を拒否します。</li> </ul> <p>これに相当する Windows レジストリの値は <code>EnableTicketSSLAuth</code> です。</p>

設定	説明
<b>Configures SSL protocols and cryptographic algorithms</b> ([コンピュータおよびユーザー構成] 設定)	<p>SSL 暗号化接続を確立する前に、特定の暗号化アルゴリズムとプロトコルの使用を制限する暗号リストを構成します。暗号リストは、コロンで区切られた 1 つ以上の暗号文字列で構成されています。</p> <p><b>注:</b> すべての暗号文字列では、大文字と小文字が区別されます。</p> <ul style="list-style-type: none"> <li>■ Horizon Client 4.2 のデフォルト値は、[!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES] になります。</li> <li>■ Horizon Client 4.0.1 と 4.1 のデフォルト値は、[TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH] になります。</li> <li>■ Horizon Client 4.0 のデフォルト値は、[TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH] になります。</li> <li>■ Horizon Client 3.5 のデフォルト値は、[TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH] になります。</li> <li>■ Horizon Client 3.3 および 3.4 のデフォルト値は、[TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH] になります。</li> <li>■ Horizon Client 3.2 以前の値は [SSLv3:TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH] になります。</li> </ul> <p>つまり、Horizon Client 4.0.1 と 4.1 では、TLSv1.0、TLSv1.1、および TLSv1.2 は有効です。(SSL v2.0 および v3.0 は削除されました)。TLSv1.0 とサーバの互換性が必要な場合、TLSv1.0 を無効にできます。Horizon Client 4.0 では、TLS v1.1、および TLS v1.2 は有効になっています (TLS v1.0 は無効です。SSL v2.0 および v3.0 は削除されました)。Horizon Client 3.5 では、TLS v1.0、TLS v1.1、および TLS v1.2 は有効になっています (SSL v2.0 および v3.0 は無効になります)。Horizon Client 3.3 および 3.4 では、TLS v1.0 および TLS v1.1 が有効になっています (SSL v2.0、SSL v3.0、TLS v1.2 は無効になっています)。Horizon Client 3.2 以前では、SSL v3.0 も有効になっています。(SSL v2.0 および TLS v1.2 は無効になります。)</p> <p>暗号化スイートは 128 ビットまたは 256 ビット AES を使用し、匿名 DH アルゴリズムを削除して、現在の暗号リストを暗号化アルゴリズムのキー長の順にソートします。</p> <p>構成の参照リンク : <a href="http://www.openssl.org/docs/apps/ciphers.html">http://www.openssl.org/docs/apps/ciphers.html</a></p> <p>これに相当する Windows レジストリの値は SSLCipherList です。</p> <p>この設定をグループ ポリシーとして構成したくないときは、クライアント コンピュータの次のレジストリ キーのいずれかに、SSLCipherList 値の名前を追加することにより、証明書検証を有効にできます。</p> <ul style="list-style-type: none"> <li>■ 32 ビット Windows の場合: HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security</li> <li>■ 64 ビット Windows の場合 : HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security</li> </ul>
<b>Enable Single Sign-On for smart card authentication</b> ([コンピュータの構成] 設定)	<p>スマート カード認証に対してシングル サインオンを有効にするかどうかを指定します。シングル サインオンを有効にすると、Horizon Client は、スマート カードの暗号化された PIN を、一時的なメモリに格納してから View 接続サーバに送信します。シングル サインオンを無効にすると、Horizon Client でカスタム PIN ダイアログは表示されません。</p> <p>これに相当する Windows レジストリの値は EnableSmartCardSSO です。</p>
<b>Ignore bad SSL certificate date received from the server</b> ([コンピュータの構成] 設定)	<p>(View 4.6 以前のリリースのみ) 無効なサーバ証明書の日付に関連するエラーを無視するかどうかを指定します。これらのエラーは、サーバが日付の過ぎた証明書を送信した場合に発生します。</p> <p>これに相当する Windows レジストリの値は IgnoreCertDateInvalid です。</p>

設定	説明
Ignore certificate revocation problems ([コンピュータの構成] 設定)	(View 4.6 以前のリリースのみ) 失効したサーバ証明書に関連するエラーを無視するかどうかを指定します。これらのエラーは、サーバが失効した証明書を送信した場合や、クライアントが証明書の失効ステータスを確認できない場合に発生します。  デフォルトでは、この設定は無効になっています。  これに相当する Windows レジストリの値は <code>IgnoreRevocation</code> です。
Ignore incorrect SSL certificate common name (host name field) ([コンピュータの構成] 設定)	(View 4.6 以前のリリースのみ) 正しくないサーバ証明書の共通名に関連するエラーを無視するかどうかを指定します。これらのエラーは、証明書の共通名がそれを送信したサーバのホスト名と一致していない場合に発生します。  これに相当する Windows レジストリの値は <code>IgnoreCertCnInvalid</code> です。
Ignore incorrect usage problems ([コンピュータの構成] 設定)	(View 4.6 以前のリリースのみ) サーバ証明書の不適切な使用に関連するエラーを無視するかどうかを指定します。これらのエラーは、サーバが送信者の ID の検証およびサーバ通信の暗号化以外の目的で証明書を送信した場合に発生します。  これに相当する Windows レジストリの値は <code>IgnoreWrongUsage</code> です。
Ignore unknown certificate authority problems ([コンピュータの構成] 設定)	(View 4.6 以前のリリースのみ) サーバ証明書の不明な証明機関 (CA) に関連するエラーを無視するかどうかを指定します。これらのエラーは、サーバが信頼されないサードパーティの CA によって署名された証明書を送信した場合に発生します。  これに相当する Windows レジストリの値は <code>IgnoreUnknownCa</code> です。

次の表では、ADM テンプレート ファイルにおけるスクリプトの定義セクションの設定について説明します。

表 4-6. スクリプト定義セクションのセキュリティ関連の設定

設定	説明
Connect all USB devices to the desktop on launch	デスクトップの起動時に、クライアント システム上の使用可能なすべての USB デバイスをデスクトップに接続するかどうかを指定します。  デフォルトでは、この設定は無効になっています。  これに相当する Windows レジストリの値は <code>connectUSBOnStartup</code> です。
Connect all USB devices to the desktop when they are plugged in	USB デバイスがクライアント システムにプラグインされたときに、それらの USB デバイスをデスクトップに接続するかどうかを指定します。  デフォルトでは、この設定は無効になっています。  これに相当する Windows レジストリの値は <code>connectUSBOnInsert</code> です。
Logon Password	Horizon Client がログイン時に使用するパスワードを指定します。このパスワードは、Active Directory によってテキスト形式で格納されます。  デフォルトでは、この設定は定義されていません。  これに相当する Windows レジストリの値は <code>Password</code> です。

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、『Windows 版 VMware Horizon Client の使用』を参照してください。

## Horizon Client 証明書検証モードの構成

`CertCheckMode` の値の名前を、Windows クライアント コンピュータのレジストリ キーに追加すると、Horizon Client 証明書検証モードを構成できます。

32 ビットの Windows の場合、レジストリ キーは、HKEY\_LOCAL\_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security です。64 ビットの Windows の場合、レジストリ キーは、HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security です。

レジストリ キーには、次の値のいずれかを使用します。

- 0 - [サーバ ID 証明書を確認しない] オプションを実装。
- 1 - [信頼されないサーバに接続する前に警告する] オプションを実装。
- 2 - [信頼されていないサーバに接続しない] オプションを実装。

さらに、証明書検証モードグループ ポリシー設定を構成すると、Horizon Client の証明書検証モードも構成できます。グループ ポリシー設定とレジストリ キーの CertCheckMode 設定の両方を構成すると、グループ ポリシー設定の方がレジストリ キーでの設定よりも優先されます。

グループ ポリシー設定またはレジストリ設定が構成されると、ユーザーは選択した証明書検証モードを Horizon Client で確認できますが、設定を構成することはできません。

証明書検証モードグループ ポリシー設定の構成の詳細については、[Horizon Client の構成テンプレートのセキュリティ設定](#) を参照してください。

# セキュリティ プロトコルと暗号化スイートの構成

Horizon Client、View Agent/Horizon Agent、および View server のコンポーネントの間で承認と提案が行われるセキュリティ プロトコルおよび暗号化スイートを構成できます。

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ポリシー](#)
- [特定のクライアント タイプのセキュリティ プロトコルおよび暗号化スイートの構成](#)
- [SSL/TLS における強度の弱い暗号化方式の無効化](#)
- [HTML Access Agent のセキュリティ プロトコルと暗号化スイートの構成](#)
- [View デスクトップでの提案ポリシーの構成](#)

## 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。

次の表に、Windows、Linux、Mac、iOS、Android、および Chrome のクライアント システムの Horizon Client 4.2、4.1、4.0.1、4.0、および 3.x に対してデフォルトで有効になっているプロトコルと暗号化スイートを示します。Windows 版、Linux 版、および Mac 版の Horizon Client 3.1 以降では、これらの暗号化スイートとプロトコルを使用して、USB チャンネル（USB サービス デーモンと View Agent または Horizon Agent の間の通信）を暗号化することもできます。Horizon Client 4.0 以前のバージョンでは、USB サービス デーモンは、リモート デスクトップへの接続時に、RC4（:RC4-SHA: +RC4）を暗号化制御文字列の末尾に追加します。Horizon Client 4.0 以降では、RC4 は追加されません。

## Horizon Client 4.2

表 5-1. Horizon Client 4.2 でデフォルトで有効になるセキュリティ プロトコルおよび暗号化スイート

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
TLS 1.2	<ul style="list-style-type: none"> <li>■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)</li> <li>■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)</li> <li>■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)</li> <li>■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)</li> <li>■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</li> <li>■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)</li> </ul>
■ TLS 1.1	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
■ TLS 1.0	<ul style="list-style-type: none"> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</li> <li>■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)</li> </ul>

Horizon Client が VMware Horizon Air サーバに確実に接続できるように、TLS 1.0 はデフォルトで有効になっています。デフォルトの暗号文字列は、「!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES」になります。サーバと TLS 1.0 に互換性がない場合、TLS 1.0 を無効にできます。



## Horizon Client 4.0.1、および 4.1

表 5-2. Horizon Client 4.0.1、および 4.1 でデフォルトで有効なセキュリティ プロトコルおよび暗号化スイート

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
TLS 1.2	<ul style="list-style-type: none"> <li>■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)</li> <li>■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)</li> <li>■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)</li> <li>■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)</li> <li>■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</li> <li>■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)</li> </ul>
■ TLS 1.1	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
■ TLS 1.0	<ul style="list-style-type: none"> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</li> <li>■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)</li> </ul>

Horizon Client が VMware Horizon Air サーバに確実に接続できるように、TLS 1.0 はデフォルトで有効になっています。デフォルト暗号文字列は、TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH になります。サーバと TLS 1.0 に互換性がない場合、TLS 1.0 を無効にできます。

## Horizon Client 4.0

表 5-3. Horizon Client 4.0 でデフォルトで有効になるセキュリティ プロトコルおよび暗号化スイート

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
TLS 1.2	<ul style="list-style-type: none"> <li>■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)</li> <li>■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)</li> <li>■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)</li> <li>■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)</li> <li>■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</li> <li>■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)</li> </ul>
■ TLS 1.1	<ul style="list-style-type: none"> <li>■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</li> <li>■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)</li> </ul>

---

**重要:** TLS 1.0 はデフォルトで無効です。SSL 3.0 は削除されています。

---

## Horizon Client 3.5

表 5-4. Horizon Client 3.5 でデフォルトで有効になるセキュリティ プロトコルおよび暗号化スイート

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
TLS 1.2	<ul style="list-style-type: none"> <li>■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)</li> <li>■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)</li> <li>■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)</li> <li>■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)</li> <li>■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</li> <li>■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)</li> </ul>
■ TLS 1.1	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
■ TLS 1.0	<ul style="list-style-type: none"> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</li> <li>■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)</li> </ul>

## Horizon Client 3.3 および 3.4

表 5-5. Horizon Client 3.3 および 3.4 でデフォルトで有効なセキュリティ プロトコルおよび暗号化スイート

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
■ TLS 1.1	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
■ TLS 1.0	■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
	■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
	■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
	■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
	■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
	■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)
	■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
	■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
	■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
	■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

**注:** TLS 1.2 もサポートされていますが、デフォルトでは無効になっています。TLS 1.2 を有効にするには、[VMware KB 2121183](#) の説明に従います。この手順により [表 5-4. Horizon Client 3.5 でデフォルトで有効になるセキュリティ プロトコルおよび暗号化スイート](#) にリストされた暗号化スイートがサポートされます。

## Horizon Client 3.0、3.1、および 3.2

表 5-6. Horizon Client 3.0、3.1、および 3.2 でデフォルトで有効なセキュリティ プロトコルおよび暗号化スイート

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
■ TLS 1.1	■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
■ TLS 1.0	■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
■ SSL 3.0 (Windows クライアントでのみ有効)	■ TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA (0xc022)
	■ TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA (0xc021)
	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
	■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
	■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
	■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
	■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
	■ TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA (0xc01f)
	■ TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA (0xc01e)
	■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
	■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)
	■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
	■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

**注:** TLS 1.2 もサポートされていますが、デフォルトでは無効になっています。TLS 1.2 を有効にするには、[VMware KB 2121183](#) の説明に従います。この手順により [表 5-4. Horizon Client 3.5 でデフォルトで有効になるセキュリティ プロトコルおよび暗号化スイート](#) にリストされた暗号化スイートがサポートされます。

## 特定のクライアント タイプのセキュリティ プロトコルおよび暗号化スイートの構成

クライアントのタイプごとに、使用するプロトコルおよび暗号化スイートを構成する方法が異なります。

View server で現在の設定がサポートされていない場合にのみ、Horizon Client のセキュリティ プロトコルを変更してください。クライアントの接続先である View server で有効になっていないセキュリティ プロトコルを Horizon Client に対して構成すると、TLS/SSL エラーが発生して接続に失敗します。

プロトコルおよび暗号化方式をデフォルト値から変更する場合は、クライアント固有の方法を使用します。

- Windows クライアント システムの場合、グループ ポリシー設定または Windows レジストリ設定のいずれかを使用できます。詳細については、『VMware Horizon Client for Windows の使用』を参照してください。
- Linux クライアント システムの場合、構成ファイル プロパティまたはコマンドライン オプションを使用できます。詳細については、『VMware Horizon Client for Linux の使用』を参照してください。
- Mac クライアント システムでは、Horizon Client の [環境設定] の設定を使用できます。詳細については、『VMware Horizon Client for Mac の使用』を参照してください。
- iOS、Android、および Chrome OS クライアント システムでは、Horizon Client 設定の [SSL 詳細オプション] 設定を使用できます。詳細については、『VMware Horizon Client for iOS の使用』、『VMware Horizon Client for Android の使用』または『VMware Horizon Client for Chrome OS の使用』の該当するドキュメントを参照してください。

このドキュメントは [https://www.vmware.com/support/viewclients/doc/viewclients\\_pubs-archive.html](https://www.vmware.com/support/viewclients/doc/viewclients_pubs-archive.html) の Horizon Client ドキュメント ページから入手できます。

## SSL/TLS における強度の弱い暗号化方式の無効化

より強固なセキュリティを実現するため、View Agent または Horizon Agent を実行する Windows ベースのマシンが SSL/TLS プロトコルによる通信で弱い暗号化方式を使用しないように、ドメイン ポリシーの GPO（グループ ポリシー オブジェクト）を構成できます。

### 手順

- 1 Active Directory サーバで、[スタート] - [管理ツール] - [グループ ポリシー管理] を選択し、その GPO を右クリックし、[編集] を選択して GPO を編集します。
- 2 グループ ポリシー管理エディタで、[コンピュータの構成] - [ポリシー] - [管理用テンプレート] - [ネットワーク] - [SSL 構成設定] に移動します。
- 3 [SSL 暗号の順位] をダブルクリックします。
- 4 [SSL 暗号の順位] ウィンドウで [有効] をクリックします。
- 5 [オプション] ペインで、[SSL 暗号] テキスト ボックスの内容全体を次の暗号リストに置き換えます。

```
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,
```

```
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA
```

上記に示した暗号化スイートは、読みやすいように複数の行に分割されています。このリストをテキストボックスに追加するときは、カンマの後にスペースを入れずに 1 行の暗号化スイートとして貼り付ける必要があります。

- 6 グループ ポリシー管理エディタを閉じます。
- 7 View Agent または Horizon Agent マシンを再起動して、新しいグループ ポリシーを有効にします。

## HTML Access Agent のセキュリティ プロトコルと暗号化スイートの構成

View Agent 6.2 からは、Windows レジストリを編集して、HTML Access Agent によって使用される暗号化スイートを構成できます。View Agent 6.2.1 からは、使用されるセキュリティ プロトコルも構成できます。グループ ポリシー オブジェクト (GPO) で構成を指定することもできます。

View Agent 6.2.1 以降のリリースでは、HTML Access Agent で TLS 1.1 と TLS 1.2 のみが使用されます。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、TLS 1.0、TLS 1.1、TLS 1.2 です。SSLv3 以前のような古いプロトコルは許可されません。レジストリ値 `SslProtocolLow` と `SslProtocolHigh` により、HTML Access Agent 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、`SslProtocolLow=tls_1.0` と `SslProtocolHigh=tls_1.2` を設定すると、HTML Access Agent は、TLS 1.0、TLS 1.1、TLS 1.2 を承認します。デフォルト設定は `SslProtocolLow=tls_1.1` と `SslProtocolHigh=tls_1.2` です。

暗号化方式のリストは、<http://openssl.org/docs/manmaster/apps/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。

```
ECDHE-RSA-AES256-SHA:AES256-SHA:HIGH:!AESGCM:!CAMELLIA:!3DES:!EDH:!EXPORT:!MD5:!PSK:!RC4:!SRP:!aNULL:!eNULL
```

### 手順

- 1 Windows レジストリ エディタを開始します。
- 2 `HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config` レジストリ キーに移動します。
- 3 2 つの新しい文字列 (REG\_SZ) 値、`SslProtocolLow` と `SslProtocolHigh` を追加して、プロトコルの範囲を指定します。

レジストリ値のデータは、`tls_1.0`、`tls_1.1`、`tls_1.2` のいずれかにする必要があります。プロトコルを 1 つのみ有効にするには、両方のレジストリ値に同じプロトコルを指定します。2 つのレジストリ値のいずれかが存在しないか、データが 3 つのうちのいずれかのプロトコルに設定されていない場合は、デフォルトのプロトコルが使用されます。



- 新しい文字列 (REG\_SZ) 値、SslCiphers を追加して、暗号化スイートのリストを指定します。

レジストリ値のデータ フィールドに暗号化スイートのリストを入力するか貼り付けます。次に例を示します。

```
ECDHE-RSA-AES256-SHA:HIGH:!AESGCM:!CAMELLIA:!3DES:!EDH:!EXPORT:!MD5:!PSK:!RC4:!SRP:!aNULL:!eNULL
```

- Windows サービスの VMware Blast を再起動します。

デフォルトの暗号化リストを使用するように戻すには、SslCiphers レジストリ値を削除して、Windows サービスの VMware Blast を再起動します。値のデータ部分を単に削除しないでください。データ部分を削除すると、HTML Access Agent は、OpenSSL 暗号化リスト形式の定義に従って、すべての暗号化を許可しなくなります。

HTML Access Agent が起動すると、ログ ファイルにプロトコルと暗号化の情報が書き込まれます。ログ ファイルを調べると、有効になっている値を判断できます。

デフォルトのプロトコルと暗号化スイートは、VMware でネットワーク セキュリティのベスト プラクティスが進展することに伴い、今後変更されることがあります。

## View 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 View デスクトップで提案ポリシーを構成して、View 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 View 接続サーバが構成されていることを確認します。

### 手順

- View デスクトップで Windows レジストリ エディタを起動します。
- HKEY\_LOCAL\_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\Configuration レジストリ キーに移動します。
- 新しい文字列 (REG\_SZ) 値 ClientSSLSecureProtocols を追加します。
- [\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
```

- 新しい文字列 (REG\_SZ) 値 ClientSSLCipherSuites を追加します。
- [\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
```

# クライアントとエージェントのログファイルの場所

クライアントとエージェントにより、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。

この章には、次のトピックが含まれています。

- [Windows 版 Horizon Client のログ](#)
- [Horizon Client for Mac のログ](#)
- [Linux 版 Horizon Client のログ](#)
- [モバイル デバイス上の Horizon Client のログ](#)
- [Windows マシンの View Agent または Horizon Agent のログ](#)
- [Linux デスクトップのログ](#)

## Windows 版 Horizon Client のログ

ログ ファイルにより、インストール、表示プロトコル、さまざまな機能コンポーネントの問題をトラブルシューティングできます。グループ ポリシー設定を使用して、一部のログ ファイルの場所、詳細度、保持期間を構成できます。

### ログの場所

次の表のファイル名では、YYYYは年、MMは月、DDは日、XXXXXXは番号を表します。

表 6-1. Windows 版 Horizon Client のログ ファイル

ログのタイプ	ディレクトリパス	ファイル名
インストール手順	C:\Users\%username%\AppData\Local\Temp	vminst.log_XXXXXX_XXXXXX.txt vmmsi.log_XXXXXX_XXXXXX.txt
PCoIP クライアント vmware-remotemks.exe プロセスから	C:\Users\%username%\AppData\Local\Temp	pcoip_client_YYYY_MM_DD_XXXXXX.txt  <b>注:</b> GPO を使用して、ログ レベルを 0 から 3（最も詳細）で構成できます。View PCoIP クライアントのセッション変数 ADM テンプレート ファイル (pcoip.adm) を使用してください。この設定は、[PCoIP イベントログの詳細度の構成] と呼ばれます。

ログのタイプ	ディレクトリパス	ファイル名
Horizon Client のユーザー インターフェイス  vmware-view.exe プロセスから	C:\Users\%username%\AppData\Local\VMware\VDM\Logs	vmware-horizon-viewclient-YYYY-MM-DD-XXXXXX.txt  <b>注:</b> GPO を使用してログの場所を構成できます。 View Common の構成 ADM テンプレート ファイル (vdm_common.adm) を使用してください。
Horizon Client のログ  vmware-view.exe プロセスから	C:\Users\%username%\AppData\Local\Temp\vmware-username-XXXXXX	vmware-crtbora-XXXXXX.log
メッセージ フレームワーク	C:\Users\%username%\AppData\Local\VMware\VDM\Logs	log-YYYY-MM-DD-XXXXXX.txt debug-YYYY-MM-DD-XXXXXX.txt
リモート MKS (マウス、キーボード、画面) ログ  vmware-remotemks.exe プロセスから	C:\Users\%username%\AppData\Local\Temp\vmware-username	ViewMP-Client-XXXXXX.log vmware-mks-XXXXXX.log vmware-rdeSvc-XXXXXX.log vmware-vvaClient-XXXXXX.log
Tsdr クライアント  vmware-remotemks.exe プロセスから	C:\Users\%username%\AppData\Local\Temp\vmware-username	vmware-ViewTsdr-Client-XXXXXX.log
Tsmmr クライアント  vmware-remotemks.exe プロセスから	C:\Users\%username%\AppData\Local\Temp\vmware-username	vmware-ViewTsmmr-Client-XXXXXX.log
VdpService クライアント  vmware-remotemks.exe プロセスから	C:\Users\%username%\AppData\Local\Temp\vmware-username	vmware-vdpServiceClient-XXXXXX.log
WSNM サービス  wsnm.exe プロセスから	C:\ProgramData\VMware\VDM\logs	debug-yyyy-mm-dd-XXXXXX.txt  <b>注:</b> GPO を使用してログの場所を構成できます。 View Common の構成 ADM テンプレート ファイル (vdm_common.adm) を使用してください。
USB リダイレクト  vmware-view-usbd.exe プロセスから	C:\ProgramData\VMware\VDM\logs	debug-yyyy-mm-dd-XXXXXX.txt  <b>注:</b> GPO を使用してログの場所を構成できます。 View Common の構成 ADM テンプレート ファイル (vdm_common.adm) を使用してください。
シリアル ポート リダイレクト  vmwsprrdpws.exe プロセスから	C:\ProgramData\VMware\VDM\Logs	Serial*.txt Netlink*.txt
スキャナ リダイレクト  ftscanmgr.exe プロセスから	C:\ProgramData\VMware\VDM\Logs	Scanner*.txt Netlink*.txt

## ログ構成

グループ ポリシー設定を使用して、一部の構成を変更できます。

- PCoIP クライアント ログでは、ログ レベルを 0 から 3（最も詳細）で構成できます。View PCoIP クライアントのセッション変数 ADM テンプレート ファイル (pcoip.adm) を使用してください。この設定は、[PCoIP イベントログの詳細度の構成] と呼ばれます。
- クライアント ユーザー インターフェイス ログでは、ログの場所、詳細度、保持ポリシーを構成します。View Common の構成 ADM テンプレート ファイル (vdm\_common.adm) を使用してください。
- USB リダイレクト ログでは、ログの場所、詳細度、保持ポリシーを構成します。View Common の構成 ADM テンプレート ファイル (vdm\_common.adm) を使用してください。
- WSNM サービス ログでは、ログの場所、詳細度、保持ポリシーを構成します。View Common の構成 ADM テンプレート ファイル (vdm\_common.adm) を使用してください。

コマンドラインのコマンドを使用して、詳細レベルを設定することもできます。C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT ディレクトリに移動して、次のコマンドを入力してください。

```
support.bat loglevels
```

新しいコマンド プロンプト ウィンドウが表示され、詳細レベルを選択するように求められます。

## ログバンドルの収集

クライアント ユーザー インターフェイス またはコマンドラインのコマンドを使用し、ログを .zip ファイルに収集して、VMware テクニカル サポートに送信できます。

- [Horizon Client] ウィンドウの [オプション] メニューから [サポート情報] を選択し、表示されるダイアログ ボックスで [サポート データの収集] をクリックします。
- コマンド ラインから C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT ディレクトリに移動して、コマンド support.bat を入力してください。

## Horizon Client for Mac のログ

ログ ファイルにより、インストール、表示プロトコル、さまざまな機能コンポーネントの問題をトラブルシューティングできます。構成ファイルを作成して、詳細度レベルを構成できます。

### ログの場所

表 6-2. Horizon Client for Mac のログ ファイル

ログのタイプ	ディレクトリ パス	ファイル名
Horizon Client のユーザー インターフェイス	~/Library/Logs/VMware Horizon Client	
PCoIP クライアント	~/Library/Logs/VMware Horizon Client	

ログのタイプ	ディレクトリパス	ファイル名
リアルタイム オーディオビデオ	~/Library/Logs/VMware	vmware-RTAV-pid.log
USB リダイレクト	~/Library/Logs/VMware	
VChan	~/Library/Logs/VMware Horizon Client	
リモート MKS (マウス、キーボード、画面) ログ	~/Library/Logs/VMware	
Crtbora	~/Library/Logs/VMware	

## ログ構成

Horizon Client 3.1 以降では、Horizon Client で Mac クライアント上の ~/Library/Logs/VMware Horizon Client ディレクトリにログ ファイルが生成されます。管理者は、Mac クライアントの /Library/Preferences/com.vmware.horizon.plist ファイルにキーを設定すると、ログ ファイルの最大数とログ ファイルを保存する最大日数を構成できます。

表 6-3. ログ ファイル収集の plist キー

キー	説明
MaxDebugLogs	ログ ファイルの最大数。最大値は 100 です。
MaxDaysToKeepLogs	ログ ファイルを保存する最大日数。この値に制限はありません。

これらの条件と一致しないファイルは、Horizon Client を起動するときに削除されます。

MaxDebugLogs キーまたは MaxDaysToKeepLogs キーが com.vmware.horizon.plist ファイルに設定されていない場合、ログ ファイルのデフォルト数は 5 個で、ログ ファイルを保存するデフォルトの日数は 7 日間です。

## Linux 版 Horizon Client のログ

ログ ファイルにより、インストール、表示プロトコル、さまざまな機能コンポーネントの問題をトラブルシューティングできます。構成ファイルを作成して、詳細度レベルを構成できます。

## ログの場所

表 6-4. Linux 版 Horizon Client のログ ファイル

ログのタイプ	ディレクトリパス	ファイル名
インストール手順	/tmp/vmware-root/	.vmware-installer-pid.log vmware-vmis-pid.log
Horizon Client のユーザー インターフェイス	/tmp/vmware-username/	vmware-horizon-client-pid.log
PCoIP クライアント	/tmp/teradici-username/	pcoip_client_YYYY_MM_DD_XXXXXX.log
リアルタイム オーディオビデオ	/tmp/vmware-username/	vmware-RTAV-pid.log

ログのタイプ	ディレクトリパス	ファイル名
USB リダイレクト	/tmp/vmware-root/	vmware-usbarb-pid.log vmware-view-usbd-pid.log
VChan	/tmp/vmware-username/	VChan-Client.log  <b>注:</b> このログは、 「export VMW_RDPVC_BRIDGE_LOG_ENABLED=1」を設定して RDPVCBridge ログを有効にすると作成されます。
リモート MKS (マウス、キーボード、画面) ログ	/tmp/vmware-username/	vmware-mks-pid.log vmware-MKSVchanClient-pid.log vmware-rdeSvc-pid.log
VdpService クライアント	/tmp/vmware-username/	vmware-vdpServiceClient-pid.log
Tsdr クライアント	/tmp/vmware-username/	vmware-ViewTsdr-Client-pid.log

## ログ構成

構成プロパティ (view.defaultLogLevel) を使用して、クライアント ログの詳細度レベルを 0 (すべてのイベントを収集) から 6 (致命的なイベントのみを収集) で設定できます。

USB 固有のログでは、次のコマンドラインのコマンドを使用できます。

```
vmware-usbarbitrator --verbose
vmware-view-usbd -o log:trace
```

## ログバンドルの収集

ログコレクタは /usr/bin/vmware-view-log-collector にあります。ログコレクタを使用するには実行権限が必要です。権限を設定するには、Linux コマンドラインから次のコマンドを入力します。

```
chmod +x /usr/bin/vmware-view-log-collector
```

ログコレクタを実行するには、Linux コマンドラインから次のコマンドを入力します。

```
/usr/bin/vmware-view-log-collector
```

## モバイルデバイス上の Horizon Client のログ

モバイルデバイスで、ログファイルが保存されているディレクトリに移動するために、サードパーティ製プログラムをインストールする必要がある場合があります。モバイルクライアントには、ログバンドルを VMware に送信する構成設定があります。ログ記録がパフォーマンスに影響することがあるため、ログの有効化は、問題をトラブルシューティングする必要がある場合のみ行ってください。

## iOS クライアントのログ

iOS クライアントの場合、*User Programs/Horizon/* の tmp ディレクトリと Documents ディレクトリにログファイルがあります。これらのディレクトリに移動するには、最初に iFunbox などのサードパーティ製アプリケーションをインストールする必要があります。

Horizon Client 設定で [ログ記録] 設定をオンにすると、ログを有効にすることができます。この設定が有効になっていると、クライアントが予期せずに終了したり、クライアントを終了してから再起動したりすると、ログファイルは結合されて 1 つの GZ ファイルに圧縮されます。そのバンドルを VMware に電子メールで送信できます。デバイスが PC または Mac に接続されている場合は、iTunes を使用してログファイルを取得することもできます。

## Android クライアントのログ

Android クライアントでは、ログファイルは *Android/data/com.vmware.view.client.android/files/* ディレクトリにあります。このディレクトリに移動するには、最初に File Explorer や My Files などのサードパーティ製アプリをインストールする必要があります。

デフォルトでは、ログが作成されるのは、アプリケーションが予期せずに終了した後のみです。このデフォルトを変更するには、Horizon Client 設定で [ログの有効化] 設定をオンにします。ログバンドルを VMware に電子メールで送信するには、クライアントの全般設定で [ログの送信] 設定を使用します。

## Chrome クライアントのログ

Chrome クライアントでは、ログは JavaScript コンソールのみで使用可能です。

## Windows ストア クライアントのログ

Windows 版 Horizon Client ではなくて Windows ストア版 Horizon Client がインストールされている Windows ストア クライアントでは、ログファイルは *C:\Users\%username%\AppData\Local\Packages\VMwareInc.VMwareViewClient\_23chmsjxv380w\LocalState\logs* ディレクトリに配置されます。

ログを有効にするには、クライアントの全般設定で [詳細なログ記録を有効にする] 設定をオンにしてから [サポート情報の収集] ボタンを使用します。ログ用のフォルダを選択するように求められます。このフォルダは、その他のフォルダと同じように圧縮できます。

## Windows マシンの View Agent または Horizon Agent のログ

ログファイルにより、インストール、表示プロトコル、さまざまな機能コンポーネントの問題をトラブルシューティングできます。グループポリシー設定を使用して、一部のログファイルの場所、詳細度、保持期間を構成できます。

### ログの場所

次の表のファイル名では、YYYY は年、MM は月、DD は日、XXXXXX は番号を表します。

表 6-5. Windows 版 Horizon Client のログ ファイル

ログのタイプ	ディレクトリパス	ファイル名
インストール手順	C:\Users\%username%\AppData\Local\Temp	vminst.log_XXXXXX_XXXXXX.txt vmmsi.log_XXXXXX_XXXXXX.txt
View Agent (Horizon 6 の場合) または Horizon Agent (Horizon 7 の場合)	<ドライブ文字>:\ProgramData\VMware\VDM\logs	pcoip_agent_YYYY_MM_DD_XXXXXX.txt pcoip_agent_YYYY_MM_DD_XXXXXX.txt vmware-vdpServiceServer-XXXXXX.log Serial*.txt Scanner*.txt Netlink*.txt debug-yyyy-mm-dd-XXXXXX.txt
<b>注:</b> GPO を使用してログの場所を構成できます。View Common の構成 ADM テンプレート ファイル (vdm_common.adm) を使用してください。		

## ログ構成

ログ オプションを構成する方法はいくつかあります。

- グループ ポリシー設定を使用して、ログの場所、冗長性、および保持のポリシーを構成できます。View Common の構成 ADM テンプレート ファイル (vdm\_common.adm) を使用してください。
- コマンド ライン コマンドを使用して冗長性のレベルを設定できます。C:\Program Files\VMware\VMware View\Agent\DCT ディレクトリに移動して、次のコマンドを入力します。support.bat loglevels  
新しいコマンド プロンプト ウィンドウが表示され、詳細レベルを選択するように求められます。
- vdmadmin コマンドと -A オプションを使用して、View Agent または Horizon Agent によるログの記録を構成できます。手順については、『View 管理』ドキュメントを参照してください。

## ログ バンドルの収集

コマンド ライン コマンドを使用してログを収集し、VMware のテクニカル サポートに送信できる .zip ファイルにできます。コマンドラインで C:\Program Files\VMware\VMware View\Agent\DCT ディレクトリに移動して、次のコマンドを入力します。support.bat

## Linux デスクトップのログ

ログ ファイルにより、インストール、表示プロトコル、さまざまな機能コンポーネントの問題をトラブルシューティングできます。構成ファイルを作成して、詳細度レベルを構成できます。



## ログの場所

表 6-6. Linux デスクトップのログ ファイル

ログのタイプ	ディレクトリパス
インストール手順	/tmp/vmware-root
View Agent (Horizon 6 の場合) または Horizon Agent (Horizon 7 の場合)	/var/log/vmware
View Agent (Horizon 6 の場合) または Horizon Agent (Horizon 7 の場合)	/usr/lib/vmware/viewagent/viewagent-debug.log

## ログ構成

/etc/vmware/config ファイルを編集してログを構成します。

## ログバンドルの収集

マシンの構成情報を収集して圧縮した tar ボールに記録するデータ収集ツール (DCT) バンドルを作成できます。Linux デスクトップでコマンド プロンプトを開いて、`dct-debug.sh` スクリプトを実行します。

```
sudo /usr/lib/vmware/viewagent/bin/dct-debug.sh
```

tar ボールは、スクリプトが実行されたディレクトリ（現在の作業ディレクトリ）に生成されます。ファイル名にはオペレーティング システム、タイムスタンプ、およびその他の情報が含まれます。例：`ubuntu-12-vdm-sdct-20150201-0606-agent.tgz`

このコマンドは /tmp/vmware-root ディレクトリと /var/log/vmware ディレクトリからログ ファイルを収集し、次のシステム ログと構成ファイルも収集します。

- /var/log/messages\*
- /var/log/syslog\*
- /var/log/boot\*.log
- /proc/cpuinfo、/proc/meminfo、/proc/vmstat、/proc/loadavg
- /var/log/audit/auth.log\*
- /etc/hosts
- /etc/resolv.conf
- /etc/nsswitch.conf
- /var/log/Xorg\*
- /etc/X11/xorg.conf
- /usr/lib/vmware/viewagent のコア ファイル
- /var/crash/\_usr\_lib\_vmware\_viewagent\* のクラッシュ ファイル

## セキュリティ パッチの適用

パッチ リリースには、View Composer、View 接続サーバ、View Agent または Horizon Agent、および、さまざまなクライアントの View コンポーネントのインストーラ ファイルが含まれている場合があります。適用する必要があるパッチ コンポーネントは、View のデプロイで必要されるバグ修正によって異なります。

必要とされるバグ修正によっては、次の順番で該当する View コンポーネントをインストールします。

- 1 View Composer
- 2 View 接続サーバ
- 3 View Agent (Horizon 6 の場合) または Horizon Agent (Horizon 7 の場合)
- 4 Horizon Client

サーバ コンポーネントにパッチを適用する方法については、『View アップグレード』を参照してください。

この章には、次のトピックが含まれています。

- [View Agent または Horizon Agent へのパッチの適用](#)
- [Horizon Client のパッチの適用](#)

### View Agent または Horizon Agent へのパッチの適用

パッチを適用するには、パッチ バージョンのインストーラをダウンロードして実行します。

次の手順は、リンク クローン デスクトップ プールについては親仮想マシンで、完全なクローン プールでは各仮想マシン デスクトップで、1 つの仮想マシン デスクトップのみを含むプールについては個々のデスクトップ仮想マシンで、実行する必要があります。

#### 前提条件

パッチ インストーラの実行に使用するホスト上に管理者権限のあるドメイン ユーザー アカウントがあることを確認します。

#### 手順

- 1 すべての親仮想マシン、完全クローンのテンプレートに使用される仮想マシン、プールにある完全クローン、手動で追加された個々の仮想マシンで、View Agent (Horizon 6) または Horizon Agent (Horizon 7) のパッチ バージョンのインストーラ ファイルをダウンロードします。

このダウンロードに関する手順については、VMware の担当者までお問い合わせください。

- 2 View Agent または Horizon Agent のパッチ リリース用にダウンロードしたインストーラを実行します。

エージェント インストーラの実行については、『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』を参照してください。

---

**注:** Horizon 6 バージョン 6.2 以降のリリースでは、パッチをインストールする前に、前バージョンをアンインストールする必要はありません。

---

- 3 View Composer へのパッチ適用の準備作業で新規仮想マシンのプロビジョニングを無効にした場合は、再度プロビジョニングを有効にします。
- 4 リンク クローン デスクトップ プールを作成するために使用される親仮想マシンについては、仮想マシンのスナップショットを取得します。  
  
スナップショットの作成の詳細については、vSphere Client のオンライン ヘルプを参照してください。
- 5 リンク クローン デスクトップ プールでは、作成したスナップショットを使用してデスクトップ プールを再構成します。
- 6 パッチが適用されたデスクトップ プールに Horizon Client を使用してログインできることを確認します。
- 7 いずれかのリンク クローン デスクトップ プールについて更新または再構成の操作をキャンセルした場合は、再度作業をスケジュールします。

## Horizon Client のパッチの適用

デスクトップ クライアントデバイスでパッチを適用するには、パッチ バージョンのインストーラをダウンロードして実行します。モバイル クライアントでパッチを適用する場合には、Google Play、Windows ストア、または Apple App Store などのアプリを販売する Web サイトから更新をインストールします。

### 手順

- 1 各クライアント システムで、Horizon Client のパッチ バージョンのインストーラ ファイルをダウンロードします。

このダウンロードに関する手順については、VMware の担当者までお問い合わせください。または、クライアント ダウンロード ページ <http://www.vmware.com/go/viewclients> でご確認ください。すでに述べたように、一部のクライアントについては、アプリ ストアからパッチ リリースを入手できます。

- 2 クライアント デバイスが Mac または Linux デスクトップまたはラップトップである場合は、デバイスから現在のバージョンのクライアント ソフトウェアを削除します。

各デバイス特有の方法でアプリケーションを削除してください。

---

**注:** Windows 版 Horizon Client 3.5 以降のリリースでは、Windows クライアントのパッチをインストールする前に、前バージョンをアンインストールする必要はありません。Windows 版 Horizon Client 4.1 以降のリリースでは、アップグレード Horizon Client オンライン機能を有効にして、Windows クライアントの Horizon Client をオンラインでアップグレードできます。詳細については、Windows 版『VMware Horizon Client の使用』を参照してください。

---

- 3 必要な場合には、Horizon Client のパッチ リリース用にダウンロードしたインストーラを実行します。

Apple App Store や Google Play からパッチを入手した場合には、アプリは、通常ダウンロードしたときにインストールされるため、インストーラを実行する必要はありません。

- 4 パッチが適用されたデスクトップ プールに新しくパッチが適用された Horizon Client でログインできることを確認します。