

View セキュリティ

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/>) でご確認ください。このドキュメントに関するご意見およびご感想は、docfeedback@vmware.com までお送りください。

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

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

Copyright © 2009 ~ 2016 VMware, Inc. All rights reserved. [著作権および商標情報](#)。

目次

View セキュリティ	5
1 View のアカウント、リソース、およびログ ファイル	6
View アカウント	6
View のリソース	7
View のログ ファイル	8
2 View のセキュリティ設定	9
View Administrator のセキュリティ関連のグローバル設定	9
View Administrator のセキュリティ関連のサーバ設定	11
View LDAP のセキュリティ関連の設定	12
3 ポートとサービス	14
View の TCP および UDP ポート	14
View での HTTP リダイレクト	17
View 接続サーバ ホスト上のサービス	18
セキュリティ サーバ上のサービス	19
4 View 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	20
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	20
グローバルな承諾ポリシーと提案ポリシーの構成	21
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	21
グローバルな承諾ポリシーと提案ポリシーの変更	22
各 View Server での承諾ポリシーの構成	22
View デスクトップでの提案ポリシーの構成	23
View で無効化された古いプロトコルと暗号化方式	24
5 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	26
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	26
6 保護された View 環境での USB デバイスの展開	28
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	28
特定のデバイスに対する USB リダイレクトの無効化	30
7 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	32
Internet Engineering Task Force 標準	32
オリジンの確認	32

他の保護手段 33

MIME タイプのセキュリティ リスクの軽減 33

クロスサイト スクリプティング攻撃の緩和 33

コンテンツ タイプの確認 34

View セキュリティ

『View 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。
- View 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 View 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。

View 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、と、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。

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

View アカウント

View 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. View のシステム アカウント

View 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、View 管理者権限は不要です。
vCenter Server	View 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、『View のインストール』を参照してください。

View コンポーネント	必要なアカウント
View Composer	<p>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。</p> <p>このユーザー アカウントは、View 管理者のアカウントにしないでください。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>必要な権限については、『View のインストール』を参照してください。</p>
View 接続サーバ	<p>View をインストールすると、ドメイン ユーザー、ローカル管理者グループを指定できます。また、View 管理者としてドメイン ユーザー グループを指定できます。View 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ています。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>View Administrator では、[View 構成] - [管理者] を使用して、View 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、『View 管理者ガイド』を参照してください。</p>

表 1-2. View のデータベース アカウント

View 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、『View のインストール』を参照してください。</p>
View 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 View イベント データが格納されます。View 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、『View のインストール』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 View 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。

View のリソース

View 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. View 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。
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	View 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	View 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。

リソース	場所	保護
ログ ファイル	View のログ 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)	<code>install_directory\VMware View\Server\broker\web apps\ROOT\Web INF</code>	アクセス制御により保護されます。

View のログ ファイル

View 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: View 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。View 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、『View のインストール』および『VMware View の統合』ドキュメントを参照してください。

表 1-4. View のログ ファイル

View コンポーネント	ファイル パスとその他の情報
すべてのコンポーネント (インストール ログ)	<code>%TEMP%\vminst.log_ 日付_ タイムスタンプ</code> <code>%TEMP%\vmmsi.log_ 日付_ タイムスタンプ</code>
Horizon Agent	<p><ドライブ文字>:\ProgramData\VMware\VDM\logs</p> <p><ドライブ文字>:\ProgramData\VMware\VDM\logs に格納されている View 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。</p> <p>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。</p> <p>PCoIP のログの名前は、<code>pcoip_agent*.log</code> および <code>pcoip_server*.log</code> です。</p>
View アプリケーション	<p>SQL Server または Oracle データベース サーバで構成されたイベント データベースを表示します。</p> <p>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。</p>
View Composer	<p>リンク クローン デスクトップにある <code>%system_drive%\Windows\Temp\vmware-viewcomposer-ga-new.log</code>。</p> <p>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。</p>
View 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、View Common の構成 ADM テンプレート ファイル (<code>vdm_common.adm</code>) のログ構成設定で、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 <code>SecurityGateway_*.log</code> 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 <code>absbg*.log</code> という名前のファイルに書き込まれます。</p>
View 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>

View のセキュリティ設定

View 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、View 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。

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

View 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、View 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 構成を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>View 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 View Administrator で変更できます。</p> <p>View 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 <code>vdmimport</code> 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>View 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。View 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、SSL 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、SSL 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、View 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 View 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 View 接続サーバ インスタンス、セキュリティ サーバ、および View 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 View 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 View 接続サーバ ホストの VMware Horizon View Message Bus コンポーネント 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 View 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 View デスクトップおよびアプリケーションへの安全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 View 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 View 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>

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、View 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、View 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、View ヘ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 View 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 View Administrator セッションがどれだけ続くかを決定します。 重要: View Administrator セッション タイムアウトを長い分数に設定すると、View 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、View 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、『View 管理ガイド』を参照してください。

注: View に対するすべての Horizon Client 接続および View Administrator 接続には、SSL が必要です。View のデプロイでロード 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、SSL をそれらにオフロードしてから、それぞれの View 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 SSL 接続を構成できます。『View 管理ガイド』の「SSL 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。

View 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、View 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 View 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 View 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、View 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 View 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 View 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 View 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、View 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 View 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 View 接続サーバへの安全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、View 接続サーバをバイパスした View 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、『View 管理ガイド』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、View 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 View 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、<code>pae-NameValuePair</code> 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 チャネルが View 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 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 View 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 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

View 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、View 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。

- View の TCP および UDP ポート
- View 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

View の TCP および UDP ポート

View 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、View 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 3-1. View 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、View 接続サーバ、または Access Point 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、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)。 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。
セキュリティ サーバ	500	View 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	*	View 接続サーバ	4001	TCP	JMS トラフィック。
セキュリティ サーバ	*	View 接続サーバ	4002	TCP	JMS SSL トラフィック。

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	*	View 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	*	View 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	View 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、View 接続サーバ、または Access Point 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 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、View 接続サーバ、または Access Point 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。
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	*	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、View 接続サーバ、または Access Point 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	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)。

送信元	ポート	送信先	ポート	プロトコル	説明
Horizon Agent	4172	Access Point アプライアンス	*	UDP	PCoIP。View 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 Access Point 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 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	80	TCP	デフォルトで SSL (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。 View での HTTP リダイレクト 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	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 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。
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 View 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	*	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)。 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 Access Point アプライアンス	8443	TCP	HTML Access。
View 接続サーバ	*	View 接続サーバ	48080	TCP	View 接続サーバ コンポーネント間の内部通信の場合。

送信元	ポート	送信先	ポート	プロトコル	説明
View 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 SSL が無効になっている場合の SOAP メッセージ。
View 接続サーバ	*	vCenter Server	443	TCP	vCenter Server へのアクセスで SSL が有効になっている場合の SOAP メッセージ。
View 接続サーバ	*	View Composer	18443	TCP	View Composer へのアクセスで SSL が有効になっている場合の SOAP メッセージ。
View 接続サーバ	*	View 接続サーバ	4100	TCP	JMS ルータ間トラフィック。
View 接続サーバ	*	View 接続サーバ	4101	TCP	JMS SSL ルータ間トラフィック。
View 接続サーバ	*	View 接続サーバ	8472	TCP	Cloud Pod アーキテクチャでのポッド間通信の場合。
View 接続サーバ	*	View 接続サーバ	22389	TCP	Cloud Pod 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。
View 接続サーバ	*	View 接続サーバ	22636	TCP	Cloud Pod 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。
Access Point アプライアンス	*	View 接続サーバまたはロード バランサ	443	TCP	HTTPS アクセス。Access Point アプライアンスは、TCP ポート 443 で接続し、複数の View 接続サーバ インスタンスの前にある 1 つの View 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。

View での HTTP リダイレクト

View 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り実行できます。

View 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、『View 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。

View 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、SSL 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。『View 管理ガイド』の「SSL 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。

SSL 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、『View 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。

View 接続サーバ ホスト上のサービス

View の動作は、View 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 3-2. View 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 View 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 ブロッカー 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	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実行する必要があります。
VMware Horizon View Message Bus コンポーネント	手動	View 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	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 View 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	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実行する必要があります。
VMware Horizon View Web コンポーネント	手動	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。View 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

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

表 3-3. 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 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実行する必要があります。
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実行する必要があります。

View 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

View 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 View 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 View 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、View 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 View 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: View 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。 [5 章 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 View Server での承諾ポリシーの構成](#)
- [View デスクトップでの提案ポリシーの構成](#)
- [View 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 4-1. デフォルトのグローバル 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
■ TLS 1.2	■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
■ TLS 1.1	■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
■ TLS 1.0	■ 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

接続しているすべてのクライアントが、TLS 1.1 または TLS 1.2 あるいはその両方をサポートしている場合には、承諾ポリシーから TLS 1.0 を削除できます。

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 View 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 View 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。暗号化スイートの順序は重要ではありません。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
```

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 View Server での承諾ポリシーの構成

各 View 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 View server にはない場合は、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。

`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 View 接続サーバまたはセキュリティ サーバ コンピュータ上で、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
secureProtocols.3=TLSv1

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

preferredSecureProtocol=TLSv1.2

# The order of the following list is unimportant:

enabledCipherSuite.1=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
enabledCipherSuite.2=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
enabledCipherSuite.3=TLS_RSA_WITH_AES_128_CBC_SHA256
enabledCipherSuite.4=TLS_RSA_WITH_AES_128_CBC_SHA
```

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

- 1 View 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
```

View 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、View 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 View 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 View Server での承諾ポリシーの構成](#)、および [View 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、『View 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 View 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 とその後のコンマ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、『View 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 では、TLS 1.0 はデフォルトで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、『View 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

5

View 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。

この章には、次のトピックが含まれています。

- 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

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

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

保護された View 環境での USB デバイスの展開

6

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 View 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 View 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。View 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。

- View 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。

RDS 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 RDS 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。

- View 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。
- 必要に応じて、Horizon Agent 側またはクライアント側で **Exclude All Devices** ポリシーを **true** に設定します。
- 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なります。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 6-1. 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 ADM テンプレート ファイル (`vdm_agent.adm`) に含まれています。詳細については、『View でのデスクトップ プールとアプリケーション プールの設定』の「Horizon Agent の構成 ADM 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すが、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、View 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 View 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 の仮想チャン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 ファミリー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 ADM テンプレート ファイル (`vdm_agent.adm`) に含まれています。詳細については、『View でのデスクトップ プールとアプリケーション プールの設定』の「Horizon Agent の構成 ADM テンプレートの USB 設定」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

7

View 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](#)
- [他の保護手段](#)

Internet Engineering Task Force 標準

View 接続サーバと View 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。
- 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、[各 View Server での承諾ポリシーの構成](#)を参照してください。

このオプションを変更しても、HTML Access への接続には影響しません。

オリジンの確認

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。

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。

ファイル `locked.properties` に次のエントリを追加して、この保護を無効にできます。

```
checkOrigin=false
```

複数の接続サーバやセキュリティ サーバがロード バランシングされている場合、ファイル `locked.properties` に次の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。

```
balancedHost=load-balancer-name
```

クライアントが Access Point を通じて接続される場合は、`locked.properties` ファイルに Access Point 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。例：

```
portalHost.1=access-point-name-1
portalHost.2=access-point-name-2
```

外部 URL に指定されたものとは異なる名前により、接続サーバまたはセキュリティ サーバへのアクセスを提供する場合も、同様に操作します。

このオプションが有効な場合、外部 URL で指定されたアドレス、`balancedHost` アドレス、`portalHost` アドレス、または `localhost` に対してのみ View への接続を行うことができます。

他の保護手段

Internet Engineering Task Force 標準の他にも、View 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 タイプの混乱を引き起こす攻撃を防止するため、View 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、View 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、View は次の宣言されたコンテンツ タイプのみを使用する要求を受け入れます。

- 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。

このリストを変更しても、View Administrator への接続には影響しません。