VMware View Security

View 5.0
View Manager 5.0
View Composer 2.7

このドキュメントは新しいエディションに置き換わるまで、ここで書いてある各製品と後続のすべてのバージョンをサポートします。このドキュメントの最新版をチェックするには、http://www.vmware.com/jp/support/pubs を参照してください。

JA-000575-00

vmware®

最新の技術ドキュメントは VMware の Web サイト（http://www.vmware.com/jp/support/pubs/）にあります
VMware の Web サイトでは最新の製品アップデートも提供されています。
このドキュメントに関するご意見およびご感想がある場合は、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

目次

VMware View Security

VMware View Security では、VMware View™ 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。
- VMware 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、およびサービス

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 VMware 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。本リファレンス ガイドは、『VMware View Hardening Guide』およびその他の VMware View のマニュアルと一緒に使用する必要があります。

VMware View Security リファレンス

安全な View 環境を構成するために、設定を変更し、いくつかの分野で調整を行って、システムを保護できます。

- VMware View のアカウント (P. 8)

  VMware 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。

- VMware View のセキュリティ設定 (P. 9)

  VMware 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 を使用して、グループ プロファイルを編集して、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。

- VMware View のリソース (P. 16)

  VMware 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。

- VMware View のログ ファイル (P. 17)

  VMware View ソフトウェアにより、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。

- VMware View の TCP および UDP ポート (P. 18)

  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。適切なポートでアクセスを許可するには、ファイアウォールを再構成する必要がある場合があります。

- View Connection Server ホスト上のサービス (P. 23)

  View Manager の動作は、View Connection Server 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。これらのサービスの操作を調整する場合は、まず、これらのサービスについて理解しておく必要があります。

- セキュリティ サーバ上のサービス (P. 23)

  View Manager 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。これらのサービスの操作を調整する場合は、まず、これらのサービスについて理解しておく必要があります。

- View Transfer Server ホスト上のサービス (P. 24)

  ローカル デスクトップの転送操作は、View Transfer Server ホスト上で実行されるサービスに依存しています。これらのサービスの操作を調整する場合は、まず、これらのサービスについて理解しておく必要があります。

VMware View のアカウント

VMware 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. VMware View システムのアカウント

VMware View のコンポーネント	必要なアカウント
View Client	View デスクトップ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。
View Client with Local Mode	ローカル モードで View デスクトップ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。このユーザー アカウントには、View 管理者権限は不要です。 デスクトップの標準的なベスト プラクティスとして、 ローカル モードで使用する予定の各 View デスクトップ上の ローカル管理者アカウントに必ず一意のパスワードを 作成するようにします。
vCenter Server	View Manager 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、『VMware View のインストール』を参照してください。
View Composer	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。 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。 必要な権限については、『VMware View のインストール』を参照してください。
View Connection Server、セキュリティ サーバ、または View Transfer Server	最初は、View Connection Server コンピュータのローカル Administrators グループ（BUILTIN\Administrators）のメンバーであるユーザー全員が、View Administrator へのログインを許可されています。 View Administrator では、 [View Configuration（View の構成）] - [Administrators（管理者）] を使用して、View 管理者のリストを変更できます。 必要な権限については、『VMware View 管理者ガイド』を参照してください。

表 2. VMware View データベースのアカウント

VMware View のコンポーネント	必要なアカウント
View Composer データベース	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。 View Composer データベースの設定については、『VMware View のインストール』を参照してください。
View Connection Server により使用されるイベント データベース	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。 View Composer データベースの設定については、『VMware View のインストール』を参照してください。

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。

VMware View のセキュリティ設定

VMware 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 を使用して、グループ プロファイルを編集して、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。

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は、View Administrator の [View Configuration（View の構成）] - [Global Settings（グローバル設定）] からアクセスできます。

表 3. セキュリティ関連のグローバル設定

設定	説明
[Disable Single Sign-on for Local Mode operations（ローカル モードの操作でシングル サインオンを無効にする）]	ユーザーがローカル デスクトップにログインするときにシングル サインオンを有効にするかどうかを指定します。 デフォルトでは、この設定は無効になっています。
[Enable automatic status updates（自動ステータス更新を有効にする）]	View Manager が、View Administrator にあるグローバル ステータス ペインとダッシュボードを定期的に更新するかどうかを指定します。この設定を有効にすると、View Administrator にログインしているどのユーザーに対しても、アイドル状態のセッションがタイムアウトになりません。 デフォルトでは、この設定は無効になっています。
[Message security mode（メッセージ セキュリティ モード）]	View Manager コンポーネント間で渡される JMS メッセージの署名と検証が行われるかどうかを指定します。 [Disabled（無効にする）] 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。 [Enabled（有効にする）] に設定すると、View コンポーネントは未署名のメッセージを拒否します。 [Mixed（混在する）] 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、iew Manager 3.0 より前の View コンポーネントでは強制されません。 デフォルトの設定は [Disabled（無効にする）] です。
[Reauthenticate secure tunnel connections after network interruption（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）]	View デスクトップへの安全なトンネル接続を View Client で使用する場合、ネットワークへの割り込み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指定します。 デフォルトでは、この設定は有効になっています。
[Require SSL for client connections and View Administrator（クライアント接続と View Administrator で SSL を必要とする）]	View Connection Server と View デスクトップ クライアントの間、および View Connection Server と View Administrator にアクセスするクライアントの間で安全な SSL 通信チャネルを使用するかどうかを指定します。 デフォルトでは、この設定は有効になっています。
[Session timeout（セッション タイムアウト）]	ユーザーが View Connection Server にログインした後にセッションを開いておくことができる時間を指定します。 デフォルトは 600 分です。

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、『VMware View 管理ガイド』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は、View Administrator の [View Configuration（View の構成）] - [Servers（サーバ）] からアクセスできます。

表 4. セキュリティ関連のサーバ設定

設定	説明
[Connect using SSL（SSL を使用して接続）]	有効になっている場合、View は SSL 暗号化を使用して vCenter Server と通信します。 デフォルトでは、この設定は有効になっています。
[Use PCoIP Secure Gateway for PCoIP connections to desktop（デスクトップへの PCoIP 接続に PCoIP Secure Gateway を使用）]	有効になっている場合は、ユーザーが Microsoft RDP 表示プロトコルを使用して View デスクトップに接続するときに、View Client は View Connection Server またはセキュリティ サーバ ホストへの安全な接続を追加で作成します。 無効になっている場合は、デスクトップ セッションが、View Connection Server ホスト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 システムと View デスクトップ仮想マシンとの間で直接確立されるようになります。 デフォルトでは、この設定は無効になっています。
[Use secure tunnel connection to desktop（デスクトップへの安全なトンネル接続を使用する）]	有効になっている場合は、View デスクトップに接続するときに、View Client は View Connection Server またはセキュリティ サーバ ホストへの HTTPS 接続をさらに作成します。 無効になっている場合は、デスクトップ セッションが、View Connection Server ホスト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 システムと View デスクトップ仮想マシンとの間で直接確立されるようになります。 デフォルトでは、この設定は有効になっています。
[Use secure tunnel connection for Local Mode operations（ローカル モード操作に安全なトンネル接続を使用する）]	有効になっている場合は、ローカル デスクトップはトンネリングされた通信を使用します。ネットワーク トラフィックは、View Connection Server またはセキュリティ サーバ（構成されている場合）を介してルーティングされます。 無効になっている場合は、ローカル デスクトップと、データセンター内の対応するリモート デスクトップの間で、データが直接転送されます。 デフォルトでは、この設定は無効になっています。
[Use SSL for Local Mode operations（ローカル モードの操作に SSL を使用する）]	有効になっている場合は、クライアント コンピュータとデータセンターとの通信およびデータ転送に SSL 暗号化が使用されます。対象となる操作には、デスクトップのチェックインとチェックアウト、およびクライアント コンピュータからデータ センターへのデータのレプリケーションが含まれますが、View Composer 基本イメージの転送は含まれません。 デフォルトでは、この設定は無効になっています。
[Use SSL when provisioning desktops in Local Mode（ローカル モードのデスクトップのプロビジョニングに SSL を使用する）]	有効になっている場合は、Transfer Server リポジトリからクライアント コンピュータへの View Composer 基本イメージ ファイルの転送に SSL 暗号化が使用されます。 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、『VMware View 管理ガイド』を参照してください。

View Agent の構成テンプレートのセキュリティ関連の設定

View 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\Policies\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 5. View Agent の構成テンプレートのセキュリティ関連の設定

設定	レジストリ値の名前	説明
AllowDirectRDP	AllowDirectRDP	View 以外のクライアントが RDP を使用して View 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、View Agent では、View 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。 **重要** View を正しく動作させるために、Windows Terminal Services 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。 デフォルトでは、この設定は有効になっています。
AllowSingleSignon	AllowSingleSignon	シングル サインオン（SSO）を使用して、ユーザーを View デスクトップに接続するかどうかを指定します。この設定が有効になっていると、ユーザーは View Client に接続するときに、自分の認証情報を入力するだけで済みます。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。 デフォルトでは、この設定は有効になっています。
CommandsToRunOnConnect	CommandsToRunOnConnect	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。 デフォルトではリストは指定されていません。
CommandsToRunOnReconnect	CommandsToRunOnReconnect	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。 デフォルトではリストは指定されていません。
ConnectionTicketTimeout	VdmConnectionTicketTimeout	View 接続チケットが有効な時間（秒）を指定します。 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 120 秒になります。
CredentialFilterExceptions	CredentialFilterExceptions	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。 デフォルトではリストは指定されていません。

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、『VMware View 管理ガイド』を参照してください。

View Client の構成テンプレートのセキュリティ設定

View Client の ADM テンプレート ファイル（**vdm_client.adm**）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。

セキュリティ設定は、**HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client\Security** にあるホスト マシンのレジストリに保存されます。

表 6. View Client の構成テンプレートのセキュリティ設定

設定	レジストリ値の名前	説明
Allow command line credentials（コマンド ラインの認証情報を許可する）	AllowCmdLineCredentials	View 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。この設定が有効になっていると、ユーザーがコマンド ラインから View 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。 デフォルトでは、この設定は有効になっています。
Brokers Trusted For Delegation（委任に対して信頼されるブローカー）	BrokersTrustedForDelegation	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 Connection Server インスタンスを指定します。View Connection Server インスタンスを指定しない場合は、すべての View Connection Server インスタンスがこの情報を受け付けます。 View Connection Server 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。 ■ **domain¥** ■ **system$@domain.com** ■ View Connection Server サービスのサービス プリンシパル名（SPN）

表 6. View Client の構成テンプレートのセキュリティ設定 (続き)

設定	レジストリ値の名前	説明
Certificate verification mode(証明書検証モード)	CertCheckMode	View Client で実行される証明書チェック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。 ■ No Security(セキュリティなし):View で証明書チェックは実行されません。 ■ Warn But Allow(警告するが許可する):次のようなサーバ証明書問題が発生した場合、警告が表示されますが、ユーザーは View Connection Server に接続し続けることができます。 ■ 自己署名証明書が View で提供される。この場合、証明書名が、View Client で ユーザーが提供した View Connection Server 名と一致しなければ問題ありません。 ■ 展開内で構成された検証可能な証明書が、期限切れになったか、まだ有効になっていない。 証明書に関してこれら以外のエラー状況が生じると、View はエラー ダイアログを表示し、ユーザーが View Connection Server に接続しないようにします。 Warn But Allow(警告するが許可する) はデフォルト値です。 ■ Full Security(フル セキュリティ):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 Connection Server に接続できなくなります。View はユーザーに証明書エラーを表示します。 View Client で何らかの証明書チェックを実行できるようにするには、View Administrator のグローバル設定で [Require SSL for client connections and View Administrator(クライアント接続と View Administrator で SSL を必要とする)] を選択する必要があります。 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 View 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。 この設定が未構成か無効になっている場合は、View Client ユーザーが SSL を構成し、証明書検証モードを選択できます。 Windows クライアントの場合、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 キーに CertCheckMode 値の名前を追加することでも、証明書検証を有効にすることができます。 HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security レジストリ キーでは次の値を使用します。 ■ 0 は、No Security(セキュリティなし) を実装します。 ■ 1 は、Warn But Allow(警告するが許可する) を実装します。 ■ 2 は、Full Security(フル セキュリティ) を実装します。 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。

表 6. View Client の構成テンプレートのセキュリティ設定 (続き)

設定	レジストリ値の名前	説明
Default value of the 'Log in as current user' checkbox([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)	LogInAsCurrentUse	View Client の接続ダイアログ ボックスの [Log in as current user（現在のユーザーとしてログイン）] チェック ボックスのデフォルト値を指定します。 この設定は、View Client のインストール時に指定されたデフォルト値を上書きします。 ユーザーが View Client をコマンド ラインから実行し、**logInAsCurrentUser** オプションを指定した場合、この設定はオプションの指定によって上書きされます。 [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 Connection Server インスタンスに、そして最終的には View 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 View 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。 コンピュータの構成の設定の他に、ユーザーの構成の設定が利用できます。 デフォルトでは、これらの設定は無効です。
Display option to Log in as current user(現在のユーザーとしてログインするためのオプションを表示する)	LogInAsCurrentUser_Display	[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 View Client の接続ダイアログ ボックスに表示するかどうかを指定します。 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 View Client の接続ダイアログ ボックスからデフォルト値を上書きできません。 [Log in as current user（現在のユーザーとしてログイン）] チェック ボックスのデフォルト値は、**Default value of the 'Log in as current user' checkbox([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)** ポリシー設定を使用して指定できます。 コンピュータの構成の設定の他に、ユーザーの構成の設定が利用できます。 デフォルトでは、これらの設定は有効です。
Enable jump list integration(ジャンプ リストの統合を有効にする)	EnableJumplist	Windows 7 以降のシステムのタスクバーにある View Client アイコンに、ジャンプ リストを表示するかどうかを指定します。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 Connection Server インスタンスおよび View デスクトップに接続できます。 View 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。 デフォルトでは、この設定は有効になっています。
Enable Single Sign-On for smart card authentication(スマート カード認証のシングル サインオンを有効にする)	EnableSmartCardSSO	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、View 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 Connection Server に送信します。シングル サインオンを無効にすると、View Client はカスタム PIN ダイアログを表示しません。 デフォルトでは、この設定は無効になっています。
Ignore bad SSL certificate date received from the server(サーバから受信した不正な SSL 証明書日付を無視する)	IgnoreCertDateInvalid	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。 デフォルトでは、この設定は有効になっています。 この設定は、View 4.6 以前のリリースにのみ適用されます。

表 6. View Client の構成テンプレートのセキュリティ設定 (続き)

設定	レジストリ値の名前	説明
Ignore certificate revocation problems(証明書失効の問題を無視する)	IgnoreRevocation	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。 この設定は、View 4.6 以前のリリースにのみ適用されます。
Ignore incorrect SSL certificate common name (不正な SSL 証明書の共通名(ホスト名フィールド)を無視する)	IgnoreCertCnInvalid	不正な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。 デフォルトでは、この設定は無効になっています。 この設定は、View 4.6 以前のリリースにのみ適用されます。
Ignore incorrect usage problems(不正使用の問題を無視する)	IgnoreWrongUsage	サーバ証明書の不正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。 デフォルトでは、この設定は無効になっています。 この設定は、View 4.6 以前のリリースにのみ適用されます。
Ignore unknown certificate authority problems(不明な証明機関の問題を無視する)	IgnoreUnknownCa	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。 デフォルトでは、この設定は無効になっています。 この設定は、View 4.6 以前のリリースにのみ適用されます。

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、『VMware View 管理ガイド』を参照してください。

View Client 構成テンプレートのスクリプト定義セクションにあるセキュリティ関連の設定

View Client の ADM テンプレート ファイル (vdm_client.adm) の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。特に記述のない限り、これらの設定にはコンピュータの構成およびユーザーの構成の設定の両方が含まれます。ユーザーの構成の設定を定義している場合は、同等のコンピュータの構成の設定は上書きされます。

スクリプト定義の設定は、HKLM\Software\Policies\VMware, Inc.\VMware VDM\Client にあるホスト マシンのレジストリに保存されます。

表 7. 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	レジストリ値の名前	説明
Connect all USB devices to the desktop on launch(すべての USB デバイスを起動時にデスクトップに接続する)	connectUSBOnStartup	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。
Connect all USB devices to the desktop when they are plugged in(すべての USB デバイスをプラグインされたときにデスクトップに接続する)	connectUSBOnInsert	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。
Logon Password(ログオン パスワード)	Password	View 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、『VMware 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 Connection Server 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 Connection Server インスタンスに、この変更内容が自動的に伝わります。

表 8. View LDAP のセキュリティ関連の設定

名前と値のペア	属性	説明
[cs-allowunencryptedstartsession]	`pae-NameValuePair`	セキュリティ サポート プロバイダ インターフェイス（SSPI）ネゴシエーションがサポートされている、信頼できるドメインに含まれていない デスクトップへのシングル サインオンに対する、静的なキーによる保護の使用を許可します。静的なキーによる保護は、 SSPI よりも安全ではないといわれています。 [0] に設定すると、静的なキーによる保護は許可されません。すべてのデスクトップが信頼できるドメインにある場合には、この設定が適しています。SSPI ネゴシエーションが失敗する場合、セッションは開始しません。 [1] に 設定すると、 SSPI ネゴシエーションが失敗した場合に、静的なキーによる保護が使用されますいくつかのデスクトップが信頼できるドメインにない場合には、この設定が適しています。 デフォルトの設定は [1] です。
	`pae-OVDIKeyCipher`	ユーザーがローカル デスクトップをチェックインまたはチェックアウトするとき、View Connection Server が仮想ディスク（`.vmdk`）ファイルを暗号化するのに使用する暗号化キーの暗号方式を指定します。 暗号化キー暗号方式の値は [AES-128] 、 [AES-192] 、または [AES-256] に設定できます。 デフォルト値は [AES-128] です。
	`pae-SSOCredentialCacheTimeout`	ユーザーのシングル サインオン（SSO）認証情報が有効ではなくなった後の SSO タイムアウト上限を分単位で設定します。 デフォルト値は [15] です。 値 [-1] は、SSO タイムアウト制限が設定されていないことを意味します。 値 [0] に設定すると、SSO が無効になります。

VMware View のリソース

VMware 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 9. View Connection Server 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	`<<ドライブ文字>>:\Programdata\VMWare\VDM\backups` (Windows Server 2008) `<<ドライブ文字>>:\Documents and Settings\All Users\Application Data\VMWare\VDM\backups` (Windows Server 2003)	アクセス制御により保護されます。
`locked.properties` (証明書プロパティ ファイル)	`<インストール ディレクトリ>\VMware\VMware View\Server\sslgateway\conf`	アクセス制御により保護が可能です。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。

表 9. View Connection Server およびセキュリティ サーバのリソース (続き)

リソース	場所	保護
ログ ファイル	<%ALLUSERSPROFILE%>\Application Data\VMware\VDM\logs <<ドライブ文字>>:\Documents and Settings\All Users\Application Data\VMware\VDM\logs	アクセス制御により保護されます。
web.xml (Tomcat 構成ファイル)	<インストール ディレクトリ>\VMware View\Server\broker\web apps\ROOT\Web INF	アクセス制御により保護されます。

表 10. View Transfer Server のリソース

リソース	場所	保護
httpd.conf (Apache 構成ファイル)	<インストール ディレクトリ>\VMware\VMware View\Server\httpd\conf	アクセス制御により保護が可能です。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。
ログ ファイル	<<ドライブ文字>>:\ProgramData\VMware\VDM\logs (Windows Server 2008 R2) <%ALLUSERSPROFILE%>\Application Data\VMware\VDM\logs (Windows Server 2003 および Windows Server 2003 R2) <<ドライバ文字>>:\Program Files\Apache Group\Apache2\logs (Apache Server)	アクセス制御により保護されます。

VMware View のログ ファイル

VMware View ソフトウェアにより、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。

注意 VMware 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、『VMware View のインストール』および『VMware View Integration（VMware View 統合ガイド）』を参照してください。

表 11. VMware View のログ ファイル

VMware View のコンポーネント	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）	<%TEMP%>\vminst.log_<date>_<timestamp> <%TEMP%>\vmmsi.log_<date>_<timestamp>
View Agent	Windows XP ゲスト OS: <<ドライブ文字>>:\Documents and Settings\All Users\Application Data\VMware\VDM\logs Windows Vista および Windows 7 ゲスト OS: <<ドライブ文字>>:\ProgramData\VMware\VDM\logs ユーザー データ ディスク（UDD）が 構成されている場合、<<ドライブ文字>> がその UDD に対応する場合があります。 PCoIP のログの名前は、pcoip_agent*.log および pcoip_server*.log です。
View アプリケーション	SQL Server または Oracle データベース サーバで構成されたイベント データベースを表示します。 Windows アプリケーションのイベント ログ。デフォルトで無効になっています。

表 11. VMware View のログ ファイル (続き)

VMware View のコンポーネント	ファイル パスとその他の情報

View Client with Local Mode	Windows XP ホスト OS:
	`C:\Documents and Settings\<%username%>\Local Settings\Application Data\VMware\VDM\Logs\`
	Windows Vista および Windows 7 ホスト OS:
	`C:\Users\<%username%>\AppData\VMware\VDM\Logs\`

View Composer	リンク クローン デスクトップにある <%system_drive%>`\Windows\Temp\vmware-viewcomposer-ga-new.log` View Composer ログには、QuickPrep および Sysprep スクリプトの実行に関する情報が含まれます。 このログには、スクリプト実行の開始と終了時刻、および出力またはエラー メッセージが記録されます。
View Connection Server またはセキュリティ サーバ	サーバにある <%ALLUSERSPROFILE%>`\Application Data\VMware\VDM\logs\*.txt` サーバでの `<<ドライブ文字>>:\Documents and Settings\All Users\Application Data\VMware\VDM\logs\*.txt` 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 (`vdm_common.adm`) のログ構成設定で、構成可能です。 PCoIP Secure Gateway のログは、セキュリティ サーバのログ ディレクトリにある `PCoIP Secure Gateway` サブディレクトリの `SecurityGateway_*.log` という名前のファイルに書き込まれます。
View サービス	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。 Windows システムのイベント ログ。

View Transfer Server	Windows Server 2008 R2:
	`<<ドライブ文字>>:\ProgramData\VMware\VDM\logs\*.txt`
	Windows Server 2003 および Windows Server 2003 R2:
	<%ALLUSERSPROFILE%>`\Application Data\VMware\VDM\logs\*.txt`
	Apache Server:
	`<<ドライブ文字>>:\Program Files\Apache Group\Apache2\logs\error.log`

VMware 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。適切なポートでアクセスを許可するには、ファイアウォールを再構成する必要がある場合があります。

表 12. View により使用される TCP および UDP ポート (ローカル モードを除く)

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	4172	View Agent 4.5 以前	50002 (グループ ポリシーにより変更可能)	UDP	PCoIP Secure Gateway が使用されている場合の PCoIP (AES-128-GCM のみ)。
セキュリティ サーバ	4172	View Agent 4.6 以降	4172	UDP	PCoIP Secure Gateway が使用されている場合の PCoIP (AES-128-GCM のみ)。
セキュリティ サーバ	4172	View Client 4.5 以前	50002 (変更不可)	UDP	PCoIP Secure Gateway が使用されている場合の PCoIP (AES-128-GCM のみ)。

表 12. View により使用される TCP および UDP ポート (ローカル モードを除く) (続き)

送信元	ポート	送信先	ポート	プロトコル	説明
セキュリティ サーバ	4172	View Client 4.6 以降	4172	UDP	PCoIP Secure Gateway が使用されている場合の PCoIP（AES-128-GCM のみ）。
セキュリティ サーバ	*	View Connection Server	4001	TCP	JMS トラフィック。
セキュリティ サーバ	*	View Connection Server	8009	TCP	AJP13 で転送される Web トラフィック。
セキュリティ サーバ	*	View デスクトップ	3389	TCP	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 デスクトップ	9427	TCP	Wyse MMR リダイレクト。
セキュリティ サーバ	*	View デスクトップ	32111	TCP	USB リダイレクト。
セキュリティ サーバ	*	View デスクトップ 4.5 以前	50002 (グループ ポリシーにより変更可能)	TCP	PCoIP Secure Gateway が使用されている場合の PCoIP（HTTPS）。
セキュリティ サーバ	*	View デスクトップ 4.6 以降	4172	TCP	PCoIP Secure Gateway が使用されている場合の PCoIP（HTTPS）。
View Agent 4.5 以前	50002 (グループ ポリシーにより変更可能)	View Client 4.5 以前	50002（変更不可）	UDP	PCoIP Secure Gateway が使用されていない場合の PCoIP（AES-128-GCM または SALSA20）。
View Agent 4.5 以前	50002（グループ ポリシーにより変更可能）	View Client 4.6 以降	4172	UDP	PCoIP Secure Gateway が使用されていない場合の PCoIP（AES-128-GCM または SALSA20）。
View Agent 4.6 以降	4172	View Client 4.5 以前	50002（変更不可）	UDP	PCoIP Secure Gateway が使用されていない場合の PCoIP（AES-128-GCM または SALSA20）。
View Agent 4.6 以降	4172	View Client 4.6 以降	4172	UDP	PCoIP Secure Gateway が使用されていない場合の PCoIP（AES-128-GCM または SALSA20）。
View Agent 4.5 以前	50002（グループ ポリシーにより変更可能）	View Connection Server またはセキュリティ サーバ	4172	UDP	PCoIP Secure Gateway が使用されている場合の PCoIP（AES-128-GCM のみ）。
View Agent 4.6 以降	4172	View Connection Server またはセキュリティ サーバ	4172	UDP	PCoIP Secure Gateway が使用されている場合の PCoIP（AES-128-GCM のみ）。
View Client	*	View Connection Server またはセキュリティ サーバ	80	TCP	SSL がクライアント接続で無効になっている場合の HTTP アクセス。
View Client	*	View Connection Server またはセキュリティ サーバ	443	TCP	SSL がクライアント接続で有効になっている場合の HTTPS アクセス。
View Client	*	View Connection Server またはセキュリティ サーバ	4172	TCP	PCoIP Secure Gateway が使用されている場合の PCoIP（HTTPS）。

表 12. View により使用される TCP および UDP ポート (ローカル モードを除く) (続き)

送信元	ポート	送信先	ポート	プロトコル	説明
View Client	*	View デスクトップ	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。
View Client	*	View デスクトップ	9427	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 Wyse MMR リダイレクト。
View Client	*	View デスクトップ	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 リダイレクト。
View Client 4.5 以前	*	View Agent 4.5 以前	50002（グループ ポリシーにより変更可能）	TCP	PCoIP Secure Gateway が使用されていない場合の PCoIP（HTTPS）。
View Client 4.5 以前	50002（変更不可）	View Agent 4.5 以前	50002（グループ ポリシーにより変更可能）	UDP	PCoIP Secure Gateway が使用されていない場合の PCoIP（AES-28-GCM または SALSA20）。
View Client 4.5 以前	*	View Agent 4.6 以降	4172	TCP	PCoIP Secure Gateway が使用されていない場合の PCoIP（HTTPS）。
View Client 4.5 以前	50002（変更不可）	View Agent 4.6 以降	4172	UDP	PCoIP Secure Gateway が使用されていない場合の PCoIP（AES-28-GCM または SALSA20）。
View Client 4.5 以前	50002（変更不可）	View Connection Server またはセキュリティ サーバ	4172	UDP	PCoIP Secure Gateway が使用されている場合の PCoIP（AES-128-GCM のみ）。
View Client 4.6 以降	*	View Agent 4.5 以前	50002（グループ ポリシーにより変更可能）	TCP	PCoIP Secure Gateway が使用されていない場合の PCoIP（HTTPS）。
View Client 4.6 以降	4172	View Agent 4.5 以前	50002（グループ ポリシーにより変更可能）	UDP	PCoIP Secure Gateway が使用されていない場合の PCoIP（AES-28-GCM または SALSA20）。
View Client 4.6 以降	*	View Agent 4.6 以降	4172	TCP	PCoIP Secure Gateway が使用されていない場合の PCoIP（HTTPS）。
View Client 4.6 以降	4172	View Agent 4.6 以降	4172	UDP	PCoIP Secure Gateway が使用されていない場合の PCoIP（AES-28-GCM または SALSA20）。
View Client 4.6 以降	4172	View Connection Server またはセキュリティ サーバ	4172	UDP	PCoIP Secure Gateway が使用されている場合の PCoIP（AES-128-GCM のみ）。
View Connection Server	*	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。

表 12. View により使用される TCP および UDP ポート (ローカル モードを除く) (続き)

送信元	ポート	送信先	ポート	プロトコル	説明
View Connection Server	*	vCenter Server または View Composer	443	TCP	vCenter Server または 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 Connection Server	4172	View Agent 4.5 以前	50002（グループ ポリシーにより変更可能）	UDP	View Connection Server 経由で PCoIP Secure Gateway が使用されている場合の PCoIP（AES-128-GCM のみ）。
View Connection Server	4172	View Agent 4.6 以降	4172	UDP	View Connection Server 経由で PCoIP Secure Gateway が使用されている場合の PCoIP（AES-128-GCM のみ）。
View Connection Server	4172	View Client 4.5 以前	50002（変更不可）	UDP	View Connection Server 経由で PCoIP Secure Gateway が使用されている場合の PCoIP（AES-128-GCM のみ）。
View Connection Server	4172	View Client 4.6 以降	4172	UDP	View Connection Server 経由で PCoIP Secure Gateway が使用されている場合の PCoIP（AES-128-GCM のみ）。
View Connection Server	*	View Connection Server	4100	TCP	JMS ルータ間トラフィック。
View Connection Server	*	View デスクトップ	3389	TCP	View Connection Server 経由でトンネル接続が使用されている場合の View デスクトップへの Microsoft RDP トラフィック。
View Connection Server	*	View デスクトップ	4172	TCP	View Connection Server 経由で PCoIP Secure Gateway が使用されている場合の PCoIP（HTTPS）。
View Connection Server	*	View デスクトップ	9427	TCP	View Connection Server 経由でトンネル接続が使用されている場合の Wyse MMR リダイレクト。
View Connection Server	*	View デスクトップ	32111	TCP	View Connection Server 経由でトンネル接続が使用されている場合の USB リダイレクト。
View デスクトップ	*	View Connection Server インスタンス	4001	TCP	JMS トラフィック。
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。

ローカル モード機能では、正しく操作するために、追加のポートを開く必要があります。

表 13. ローカル モードで使用される TCP および UDP ポート

送信元	Port（ポート）	送信先	Port（ポート）	プロトコル	説明
セキュリティ サーバ	*	View Transfer Server	80	TCP	トンネル接続が使用され、ローカル モードの操作で SSL が無効になっている場合の View デスクトップ ダウンロードおよびデータのレプリケーション
セキュリティ サーバ	*	View Transfer Server	443	TCP	トンネル接続が使用され、ローカル モードの操作で SSL が有効になっている場合の View デスクトップ ダウンロードおよびデータのレプリケーション
View Client with Local Mode	*	View Transfer Server	80	TCP	トンネル接続の代わりに直接接続が使用され、ローカル モードの操作で SSL が無効になっている場合の View デスクトップ ダウンロードおよびデータのレプリケーション
View Client with Local Mode	*	View Transfer Server	443	TCP	トンネル接続の代わりに直接接続が使用され、ローカル モードの操作で SSL が有効になっている場合の View デスクトップ ダウンロードおよびデータのレプリケーション
View Connection Server	*	ESX ホスト	902	TCP	ローカル デスクトップのチェックアウトのときに使用されます。
View Connection Server	*	View Transfer Server	80	TCP	View Connection Server 経由のトンネル接続が使用され、ローカル モードの操作で SSL が無効になっている場合の View デスクトップ ダウンロードおよびデータのレプリケーション
View Connection Server	*	View Transfer Server	443	TCP	View Connection Server 経由のトンネル接続が使用され、ローカル モードの操作で SSL が有効になっている場合の View デスクトップ ダウンロードおよびデータのレプリケーション
View Connection Server	*	View Transfer Server	4001	TCP	ローカル モードをサポートする JMS トラフィック。
View Transfer Server	*	ESX ホスト	902	TCP	ローカル モードの View Composer パッケージの公開。

View Connection Server ホスト上のサービス

View Manager の動作は、View Connection Server 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。これらのサービスの操作を調整する場合は、まず、これらのサービスについて理解しておく必要があります。

表 14. View Connection Server 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 View Connection Server	自動	コネクション ブローカー サービスを提供します。View Manager の正しい動作のために、このサービスが実行されている必要があります。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 View Script Host サービスは開始または停止されません。
VMware View Framework コンポーネント	手動	View Manager のイベント ログ、セキュリティ、および COM+ Framework サービスを提供します。View Manager の正しい動作のために、このサービスが実行されている必要があります。
VMware View Message Bus Component	手動	View Manager 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。View Manager の正しい動作のために、このサービスが実行されている必要があります。
VMware View PCoIP Secure Gateway	手動	PCoIP セキュア ゲートウェイ サービスを提供します。クライアントが PCoIP セキュリア ゲートウェイを介して View Connection Server 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 View スクリプト ホスト	自動（有効になっている場合）	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 View Security Gateway Component	手動	View Manager の安全なトンネル サービスを提供します。View Manager の正しい動作のために、このサービスが実行されている必要があります。
VMware View Web Component	手動	View Manager の Web サービスを提供します。View Manager の正しい動作のために、このサービスが実行されている必要があります。
VMwareVDMDS	自動	View Manager の LDAP ディレクトリ サービスを提供します。View Manager の正しい動作のために、このサービスが実行されている必要があります。また、既存のデータが正しく移行されるように、このサービスが VMware View のアップグレード中にも実行されている必要があります。

セキュリティ サーバ上のサービス

View Manager 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。これらのサービスの操作を調整する場合は、まず、これらのサービスについて理解しておく必要があります。

表 15. 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 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。セキュリティ サーバの正しい動作のために、このサービスが実行されている必要があります。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 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。セキュリティ サーバの正しい動作のために、このサービスが実行されている必要があります。

表 15. セキュリティ サーバ サービス (続き)

サービス名	スタートアップの種類	説明
VMware View PCoIP Secure Gateway	手動	PCoIP セキュア ゲートウェイ サービスを提供します。クライアントが PCoIP セキュア ゲートウェイを介してセキュリティ 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 View Security Gateway Component	手動	安全な トンネル サービスを提供します。セキュリティ サーバの正しい動作のために、このサービスが実行されている必要があります。

View Transfer Server ホスト上のサービス

ローカル デスクトップの転送操作は、View Transfer Server ホスト上で実行されるサービスに依存しています。これらのサービスの操作を調整する場合は、まず、これらのサービスについて理解しておく必要があります。

View Manager でのローカル デスクトップの正しい操作のためには、View Transfer Server にインストールされているすべてのサービスが実行されている必要があります。

表 16. View Transfer Server 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 View Transfer Server	自動	View Transfer Server に関連したサービスを調整するサービスを提供します。このサービスを開始または停止すると、View Transfer Server Control サービスと Framework サービスも開始または停止されます。
VMware View Transfer Server Control サービス	手動	View Transfer Server のための管理機能を提供するとともに、View Connection Server との通信を処理します。
VMware View Framework Component	手動	View Manager のイベント ログ、セキュリティ、および COM+ Framework サービスを提供します。
Apache2.2 サービス	自動	View デスクトップをローカル モードで実行するクライアント コンピュータのためのデータ転送機能を提供します。 Apache2.2 サービスは、View Transfer Server を View Manager に追加すると開始されます。

インデックス