

View Agent Direct Connect プラグイン管理

VMware Horizon 6 6.2



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

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

Copyright © 2019 VMware, Inc. All rights reserved. [著作権および商標情報](#)。

目次

View Agent Direct-Connection プラグイン管理	4
1 View Agent Direct-Connection プラグインのインストール	5
View Agent Direct-Connection プラグインのシステム要件	5
View Agent Direct-Connection プラグインのインストール	5
View Agent Direct-Connection プラグインのサイレントインストール	6
2 View Agent Direct-Connection プラグインの詳細構成	8
View Agent Direct-Connection プラグイン	8
SSL/TLS における強度の弱い暗号化方式の無効化	11
デフォルトの自己署名 SSL サーバ証明書の置き換え	12
Horizon Client のデスクトップおよびアプリケーションへのアクセスの許可	12
ネットワーク アドレス変換とポート マッピングの使用	13
高度なアドレス方式	15
Windows 証明書ストアへの認証局の追加	16
3 HTML Access のセットアップ	17
HTML Access 用 View Agent のインストール	17
静的なコンテンツ配信の設定	18
信頼される CA 署名付き SSL サーバ証明書の設定	19
Windows 10 デスクトップでの HTTP/2 プロトコルの無効化	20
4 リモート デスクトップ サービス ホストでの View Agent Direct-Connection の設定	21
リモート デスクトップ サービス (RDS) ホスト	21
RDS デスクトップおよびアプリケーションに資格を割り当てる	22
5 View Agent Direct-Connection プラグインのトラブルシューティング	23
不適切なグラフィック ドライバがインストールされている	23
ビデオ RAM の不足	24
トレース情報とデバッグ情報を含めるために完全なログ記録を有効にする	24

View Agent Direct-Connection プラグイン管理

『View Agent Direct Connect プラグイン管理』では、View Agent Direct-Connection プラグインのインストールと構成について説明しています。このプラグインが View Agent にインストール可能なエクステンションで、これにより Horizon Client は View 接続サーバを使用せずに仮想マシン ベースのデスクトップ、Remote Desktop Services (RDS) デスクトップ、またはアプリケーションに直接接続できます。デスクトップとアプリケーションの機能はすべて、ユーザーが View 接続サーバ経由で接続する場合と同じように機能します。

対象読者

この情報は、仮想マシン ベースのデスクトップまたは RDS ホストに対して View Agent Direct-Connection プラグインのインストール、アップグレード、または構成を行う管理者を対象にしています。このガイドは、仮想マシン テクノロジーやデータセンターの運用に精通している Windows システム管理者向けに記述されています。

View Agent Direct-Connection プラグインのインストール

1

View Agent Direct-Connection (VADC) プラグインにより、Horizon Client は仮想マシンベース デスクトップ、RDS デスクトップ、またはアプリケーションに直接接続できます。VADC プラグインは View Agent のエクステンションで、仮想マシンベース デスクトップまたは RDS ホストに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。

- [View Agent Direct-Connection プラグインのシステム要件](#)
- [View Agent Direct-Connection プラグインのインストール](#)
- [View Agent Direct-Connection プラグインのサイレント インストール](#)

View Agent Direct-Connection プラグインのシステム要件

View Agent Direct-Connection (VADC) プラグインは、View Agent がすでにインストールされているマシンにインストールされます。View Agent でサポートされているオペレーティング システムのリストについては、『View のインストール』の「View Agent でサポートされるオペレーティング システム」を参照してください。

VADC プラグインには、次の追加の要件があります。

- VADC プラグインがインストールされている仮想マシンまたは物理マシンで PCoIP を適切に機能させるには、128 MB 以上のビデオ RAM が必要です。
- 仮想マシンでは、View Agent をインストールする前に VMware Tools をインストールする必要があります。
- 物理マシンでは、Teradici ホスト カードが必要です。VMware Tools のインストールは不要です。

注: VADC をサポートする仮想マシンベースのデスクトップは、Microsoft Active Directory のドメインに参加したり、ワークグループのメンバーになることができます。

View Agent Direct-Connection プラグインのインストール

View Agent Direct-Connection (VADC) プラグインは、VMware Web サイトからダウンロードしてインストールできる Windows インストーラ ファイルにパッケージ化されています。

前提条件

- View Agent がインストールされていることを確認します。環境に View 接続サーバが含まれていない場合、コマンドラインから View Agent をインストールし、View Agent に View 接続サーバに登録しないように指示するパラメータを指定します。[HTML Access 用 View Agent のインストール](#)を参照してください。

手順

- 1 VMware ダウンロード ページ (<http://www.vmware.com/go/downloadview>) から、VADC プラグイン インストーラ ファイルをダウンロードします。

インストーラ ファイル名は、VMware-viewagent-direct-connection-x86_64-y.y.y-xxxxxx.exe for 64-bit Windows または VMware-viewagent-direct-connection--y.y.y-xxxxxx.exe for 32-bit Windows です。y.y.y はバージョン番号、xxxxxx はビルド番号です。

- 2 インストーラ ファイルをダブルクリックします。

- 3 (オプション) TCP のポート番号を変更します。

デフォルトのポート番号は 443 です。

- 4 (オプション) Windows ファイアウォール サービスを構成する方法を選択します。

デフォルトでは、[Windows ファイアウォールを自動的に構成する] が選択されており、インストーラは必要なネットワーク接続を許可するよう Windows ファイアウォールを構成します。

- 5 (オプション) SSL 3.0 を無効化するかどうかを選択します。

デフォルトでは、[SSLv3 のサポートを自動的に無効にします (推奨)] が選択されており、インストーラが SSL 3.0 をオペレーティング システム レベルで無効にします。SSL 3.0 がレジストリ内ですでに明示的に有効または無効になっている場合、このオプションは表示されず、インストーラは何もアクションを実行しません。このオプションが選択解除された場合も、インストーラは何もアクションを実行しません。

- 6 指示に従ってインストールを終了します。

View Agent Direct-Connection プラグインのサイレント インストール

Microsoft Windows インストーラ (MSI) のサイレント インストール機能を使用して、View Agent Direct-Connection (VADC) プラグインをインストールできます。サイレント インストールはコマンドラインを使用するため、ウィザードのプロンプトに応える必要はありません。

サイレント インストールでは、大規模エンタープライズに VADC プラグインを効率よく展開できます。Windows インストーラの詳細については、『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「Microsoft Windows インストーラ コマンド ライン オプション」を参照してください。VADC プラグインは次の MSI プロパティをサポートします。

表 1-1. View Agent Direct-Connection プラグインのサイレント インストールのための MSI プロパティ

MSI プロパティ	説明	デフォルト値
LISTENPORT	リモート接続を受け入れるために VADC プラグインが使用する TCP ポート。デフォルトでは、インストーラはこのポートのトラフィックを許可するように Windows ファイアウォールを構成します。	443
MODIFYFIREWALL	1 に設定すると、インストーラは LISTENPORT のトラフィックを許可するように Windows ファイアウォールを構成します。0 に設定すると、インストーラはこのように処理しません。	1
DISABLE_SSLV3	SSL 3.0 がレジストリですでに明示的に有効または無効になっている場合、インストーラはこのプロパティを無視します。そうでない場合、このプロパティが 1 に設定されている場合はインストーラがオペレーション システム レベルで SSL 3.0 を無効化し、このプロパティが 0 に設定されている場合はインストーラが何もアクションを実行しません。	1

前提条件

- View Agent がインストールされていることを確認します。環境に View 接続サーバが含まれていない場合、コマンドラインから View Agent をインストールし、View Agent に View 接続サーバに登録しないように指示するパラメータを指定します。[HTML Access 用 View Agent のインストール](#)を参照してください。

手順

- 1 Windows コマンド プロンプトを開きます。
- 2 サイレント インストールを指定するコマンドライン オプションを使用して VADC プラグイン インストーラ ファイルを実行します。必要に応じて MSI プロパティをさらに指定できます。

次の例では、デフォルトのオプションを指定して VADC プラグインがインストールされます。

```
VMware-viewagent-direct-connection--y.y.y-xxxxxx.exe /s
```

次の例では、VADC プラグインがインストールされ、リモート接続のために VADC がリスンする TCP ポートが指定されます。

```
VMware-viewagent-direct-connection--y.y.y-xxxxxx.exe /s /v"/qn LISTENPORT=9999"
```

View Agent Direct-Connection プラグインの詳細構成

2

View Direct-Connection プラグインの構成設定は、デフォルトのまま使用することも、Windows Active Directory のグループ ポリシー オブジェクト (GPO) を使用するかまたは個々の Windows レジストリ設定を変更することによってカスタマイズすることもできます。

この章には、次のトピックが含まれています。

- View Agent Direct-Connection プラグイン
- SSL/TLS における強度の弱い暗号化方式の無効化
- デフォルトの自己署名 SSL サーバ証明書の置き換え
- Horizon Client のデスクトップおよびアプリケーションへのアクセスの許可
- ネットワーク アドレス変換とポート マッピングの使用
- Windows 証明書ストアへの認証局の追加

View Agent Direct-Connection プラグイン

View Agent Direct-Connection プラグインのすべての構成設定は、ローカルのレジストリに格納されます。この ADM ファイルのポリシー設定を Active Directory のグループ ポリシ オブジェクト (GPO) に追加し、Group Policy Object Editor の設定を構成することができます。

このレジストリ値は、レジストリ キー HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Agent \Configuration\XMLAPI に置かれています。

表 2-1. View Agent Direct-Connection プラグイン

設定	レジストリセッティ	タイプ	説明
無効なポート番号です。	httpsPortNumber	REG_SZ	プラグインが、Horizon Client からの受信 HTTPS リクエストをリスンする TCP ポート。この値が変更された場合、Windows のファイアウォールに対応する変更を行い、トラフィックが入るのを許可します。
セッション タイムアウト	sessionTimeout	REG_SZ	ユーザーが View 接続サーバ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。時間は分単位で設定します。デフォルトは 600 分です。タイムアウトになりました。すべてのユーザーのデスクトップとアプリケーションのセッションが切断されます。

設定	レジストリセッティ	タイプ	説明
免責条項が有効	disclaimerEnabled	REG_SZ	この値には、TRUE または FALSE を指定できます。TRUE に設定された場合、ログイン時のユーザー承諾の disclaimer text が表示されます。 .テキストは、「免責条項テキスト」から表示されるか（このテキストが作成されている場合）、次の GPO から表示されます： Configuration\Windows Settings\Security Settings\Local Policies\Security Options: Interactive logon. disclaimerEnabled のデフォルト設定は FALSE です。
免責条項テキスト	disclaimerText	REG_SZ	Horizon View Client がログイン時に使用するユーザー名を指定します。免責事項有効ポリシーは TRUE に設定する必要があります。このテキストが指定されていない場合、デフォルトでは Windows ポリシー Configuration\Windows Settings\Security Settings\Local Policies\Security Options にある値が使用されます。
クライアント設定 : AlwaysConnect	AlwaysConnect	REG_SZ	この値には、TRUE または FALSE を指定できます。常に接続設定は、Horizon Client に送信されます。このポリシーが TRUE に設定されている場合、保存されているすべての設定が上書きされます。デフォルトではリストは指定されていません。このポリシーを有効にすると、値が TRUE に設定されます。このポリシーを無効にすると、値が FALSE に設定されます。
外部 PColP ポート	externalPColPPort	REG_SZ	TCP/UD プロトコルで使用するターゲット TCP/UDP ポート番号の Horizon Client に送信されるポート番号番号の前の A + 文字は、HTTPS で使用されたポート番号からの関連番号を示します。外部に公開されているポート番号がサービスがリスンしているポートと一致しない場合にのみこの値を設定します。ポート番号が「%1\$s」で指定されていません。0A デフォルトではリストは指定されていません。
外部 Blast ポート	externalBlastPort	REG_SZ	The port number sent to Horizon Client for the destination TCP/UDP port number that is used for the PColP protocol.番号の前の A + 文字は、HTTPS で使用されたポート番号からの関連番号を示します。外部に公開されているポート番号がサービスがリスンしているポートと一致しない場合にのみこの値を設定します。ポート番号が「%1\$s」で指定されていません。0A デフォルトではリストは指定されていません。
外部 RDP ポート	externalRDPPort	REG_SZ	The port number sent to Horizon Client for the destination TCP/UDP port number that is used for the PColP protocol.番号の前の A + 文字は、HTTPS で使用されたポート番号からの関連番号を示します。外部に公開されているポート番号がサービスがリスンしているポートと一致しない場合にのみこの値を設定します。ポート番号が「%1\$s」で指定されていません。0A デフォルトではリストは指定されていません。
IP アドレス	externalIPAddress	REG_SZ	The port number sent to Horizon Client for the destination TCP/UDP port number that is used for the PColP protocol.Only set this value if the externally exposed port number does not match the port that the service is listening on.ポート番号が「%1\$s」で指定されていません。0A デフォルトではリストは指定されていません。

設定	レジストリセッティ	タイプ	説明
外部フレームワーク チャネル ポート	externalFrameworkChannelPort	REG_SZ	The port number sent to Horizon Client for the destination TCP/UDP port number that is used for the PCoIP protocol.番号の前の A + 文字は、HTTPS で使用されたポート番号からの関連番号を示します。Only set this value if the externally exposed port number does not match the port that the service is listening on.ポート番号が「%1\$s」で指定されていません。!0A デフォルトではリストは指定されていません。
USB が有効	usbEnabled	REG_SZ	この値には、TRUE または FALSE を指定できます。デスクトップがクライアントシステムに接続されている USB デバイスを使用できるかどうかを指定します。デフォルト値は 20 です。セキュリティ上の理由のため、外部デバイスを使用できないようにするには、設定を FALSE に変更します。
クライアント設定 : USB AutoConnect	usbAutoConnect	REG_SZ	この値には、TRUE または FALSE を指定できます。このポリシーが dilato it protected entry_1 に設定された場合、保存されたクライアント設定が上書きされます。デフォルトではリストは指定されていません。
リセットが有効	resetEnabled	REG_SZ	この値には、TRUE または FALSE を指定できます。TRUE に設定された場合、認証された Horizon client クライアントは、操作システム レベルの再起動を行えます。デフォルトでは、この設定は無効 (FALSE) になっています。
PCoIP クライアントイメエ ジキャッシュ	clientCredentialCacheTimeout	REG_SZ	Horizon client でユーザーが保存されたパスワードを使用できる期間(分単位)。0 オヨビ-1Horizon Client により、ユーザーはこの設定が有効な値に設定された場合、パスワードを保存することができます。デフォルトは 0 分です。
セッションタイムアウト	userIdleTimeout	REG_SZ	Horizon client でユーザーの活動がこの期間ない場合、ユーザーのデスクトップとアプリケーションのセッションが切断されます。値は秒単位で設定します。デフォルトは 900 秒 (15 分) です。
スマート カード サポート	x509CertAuth	REG_SZ	次の値に基づいて、スマート カード認証がどのようにサポートされるかを示します。 ■ 0 : 不許可 ■ 1 : オプション ■ 2 : 必須 デフォルト値は 0 です。
スマート カードの証明書の 発行元	x509SSLCertAuth	REG_SZ	スマート カードの証明書が SSL ネゴシエーションから取得されることを示します。x509CertAuth が 1 または 2 に設定されている場合、この値は TRUE に設定する必要があります。デフォルト値は FALSE です。この設定を変更するには、View Agent サービスを再起動する必要があります。
クライアント構成の名前/値 のペア	BioMetricsTimeout	REG_SZ	生体認証がサポートされているかどうかを示し、サポートされている場合は、使用できる時間を示します。0 は、生体認証がサポートされていないことを意味します。-1 は、生体認証がサポートされていて、制限時間がないことを意味します。正の数値は、使用可能な時間 (分) を意味します。デフォルトは 0 (サポートされていない) です。

Network Address Translation (NAT) およびポートマッピング サポートで使用されている外部ポート番号および外部 IP アドレスの値。詳細については、[ネットワーク アドレス変換とポート マッピングの使用](#) を参照してください。

この ADM ファイルのポリシー設定を Active Directory のグループ ポリシー オブジェクト (GPO) に追加し、Group Policy Object Editor の設定を構成することができます。ポリシー設定は、通常のレジストリ設定より優先されます。GPO テンプレート ファイルがポリシーの構成用に提供されています。.ViewView Agent およびプラグインがデフォルトの場所にインストールされたとき、デフォルト ファイルは次の場所に格納されます。

C:\Program Files\VMware\VMware View\Agent\extras\view_agent_direct_connection.adm

このファイルを Active Directory サーバにコピーし、グループ ポリシー管理エディタを使用してこの管理テンプレートを追加する必要があります。ポリシー管理の詳細については、Microsoft Policy Editor および GPO ハンドリングドキュメントを参照してください。レジストリ キーでは次の値を使用します。

HKEY_LOCAL_MACHINE Software\Policies\VMware, Inc.\VMware VDM\Agent\Configuration\XMLAPI

スマート カード認証を使用する場合、スマート カード証明書にサインする認証局 (CA) が Windows 証明書ストアに存在する必要があります。認証局の追加方法の詳細については、「[Windows 証明書ストアへの認証局の追加](#)」を参照してください。

注: ユーザーがスマート カードを使用して Windows 7 または Windows Server 2008 R2 マシンにログインしようとするときに、スマート カードの証明書が中間 CA によって署名されている場合、Windows は中間 CA の名前を含まない信頼された発行者リストをクライアントに送信する可能性があるため、その試行は失敗することがあります。この状況が発生すると、クライアントは適切なスマート カードの証明書を選択できなくなります。この問題を回避するために、レジストリ キー HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL でレジストリの値 SendTrustedIssuerList (REG_DWORD) を 0 に設定します。このレジストリ値が 0 に設定されていると、Windows は信頼された発行者リストをクライアントに送信しなくなるため、スマート カードから有効なすべての証明書を選択できるようになります。

SSL/TLS における強度の弱い暗号化方式の無効化

セキュリティを強化するために、ドメイン ポリシー GPO (グループ ポリシー オブジェクト) を構成し、Horizon Client と仮想マシンベースのデスクトップや RDS ホスト間の通信で SSL/TLS プロトコルを必ず使用し、強度の低い暗号化方式を許可しないようにすることができます。

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 VADC 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。

注: 仮想デスクトップ OS でサポートされているいずれかの暗号化方式をサポートするように Horizon Client が構成されていない場合は、TLS/SSL ネゴシエーションは失敗し、クライアントは接続できません。

Horizon Client でサポートされる暗号化スイートの構成についての詳細は、https://www.vmware.com/support/viewclients/doc/viewclients_pubs.html で公開されている Horizon Client ドキュメントを参照してください。

デフォルトの自己署名 SSL サーバ証明書の置き換え

自己署名 SSL サーバ証明書は、改ざんや盗聴の脅威から Horizon Client を十分に保護することができません。デスクトップをこれらの脅威から保護するには、生成された自己署名証明書を置き換える必要があります。

インストール後に View Agent Direct-Connection プラグインを初めて起動すると、自己署名 SSL サーバ証明書が自動的に生成され、Windows 証明書ストアに置かれます。SSL プロトコル ネゴシエーション中に SSL サーバ証明書が Horizon Client に提示され、このデスクトップについての情報がクライアントに示されます。このデフォルトの自己署名 SSL サーバ証明書が、このデスクトップについて保証するには、クライアントに信用され、Horizon Client 証明書確認によって完全に検証済みの、証明書機関 (CA) が署名した証明書によって置き換えられる必要があります。

この証明書を Windows 証明書ストアに保存する手順、および適切な CA 署名の証明書で置き換える手順は、View 接続サーバ (バージョン 5.1 以降) で使用する手順と同じです。この証明書の置き換え手順の詳細については、『View のインストール』の「View Server 用の SSL 証明書の構成」を参照してください。

サブジェクトの別名 (SAN) を持つ証明書およびワイルドカード証明書はサポートされません。

注: View Agent Direct-Connection プラグインを使用して CA 署名の SSL サーバ証明書を多数のデスクトップに配布するには、Active Directory 登録を使用して証明書を各仮想マシンに配布します。詳細については、以下を参照してください。 <http://technet.microsoft.com/en-us/library/cc732625.aspx>.

Horizon Client のデスクトップおよびアプリケーションへのアクセスの許可

ユーザーがデスクトップおよびアプリケーションに直接アクセスすることを許可する認証メカニズムは、[View Agent Direct-Connection ユーザー] と呼ばれるローカルのオペレーティング システム グループ内で制御されます。

ユーザーがこのグループのメンバーである場合、ユーザーは仮想マシンベースのデスクトップ、RDS デスクトップまたはアプリケーションに接続することが許可されます。プラグインが最初にインストールされると、このローカルグループが作成されて、認証済みユーザーグループが含まれます。プラグインにより正常に認証されたすべてのユーザーはデスクトップまたはアプリケーションにアクセスすることが許可されます。

このデスクトップまたは RDS ホストへのアクセスを制限するには、このグループのメンバーシップを変更して、ユーザーおよびユーザーグループのリストを指定します。これらのユーザーは、ローカルまたはドメインユーザー、またはユーザーグループとなります。ユーザーがこのグループにいない場合、この仮想マシンベースのデスクトップ、またはこの RDS ホストにホストされている RDS デスクトップおよびアプリケーションにアクセスする資格がないというメッセージが認証後に表示されます。

ネットワーク アドレス変換とポート マッピングの使用

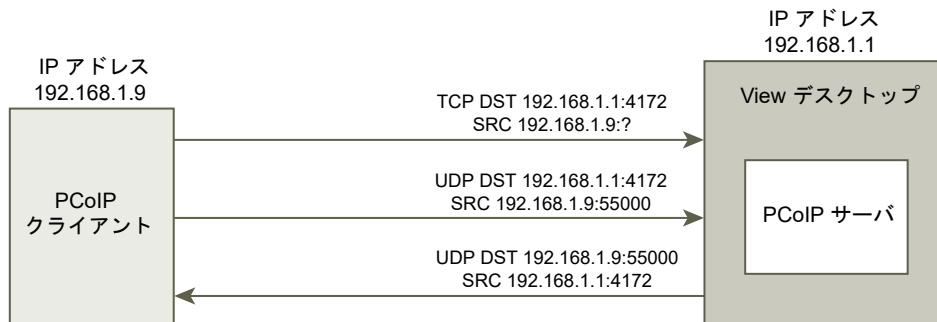
Horizon Client が複数のネットワーク上の仮想マシンベースのデスクトップに接続する場合は、ネットワークアドレス変換 (NAT) とポート マッピングの構成が必要です。

ここに示している例の場合、デスクトップで外部アドレス情報を設定する必要があります。これにより Horizon Client は、この情報を参照し、NAT またはポート マッピング デバイスを使用してデスクトップに接続できます。この URL は、View 接続サーバと View セキュリティ サーバにある [外部 URL] と [PCoIP 外部 URL] の設定と同じです。

Horizon Client が別のネットワーク上に存在し、NAT デバイスが Horizon Client とプラグインを実行しているデスクトップとの間に存在する場合は、NAT またはポート マッピングの構成が必要です。たとえば、Horizon Client とデスクトップとの間にファイアウォールが存在する場合、このファイアウォールは NAT デバイスまたはポート マッピング デバイスとして機能しています。

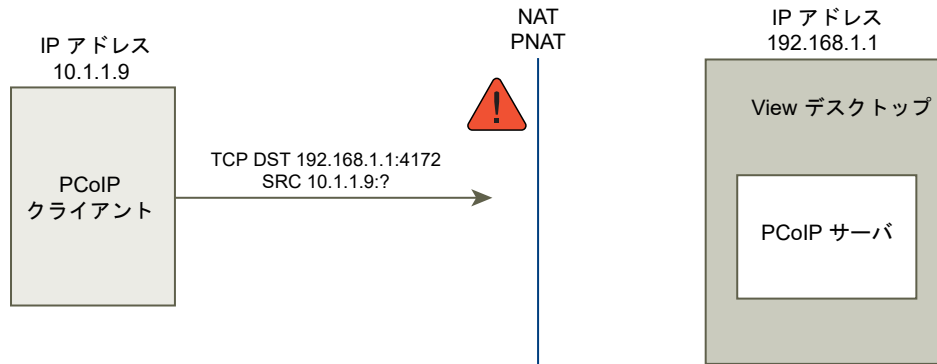
IP アドレス 192.168.1.1 のデスクトップの展開例は、NAT とポート マッピングの構成を示しています。同じネットワーク上の、IP アドレス 192.168.1.9 の Horizon Client システムは、TCP と UDP を使用して PCoIP 接続を確立します。この接続は、NAT もポート マッピングも構成されない直接接続です。

図 2-1. 同じネットワーク上のクライアントからの直接 PCoIP



クライアントとデスクトップが異なるアドレス空間で稼働し、プラグインに構成上の変更をしないようにクライアントとデスクトップの間に NAT デバイスを追加した場合、PCoIP パケットは正しくルーティングされず、失敗します。この例では、クライアントが異なるアドレス空間を使用しており、クライアントの IP アドレスは 10.1.1.9 です。このクライアントはデスクトップのアドレスを使用して TCP および UDP PCoIP パケットを送信するため、このセットアップは失敗します。送信先アドレス 192.168.1.1 は、クライアント ネットワークからは機能しません。このアドレスが原因となって、クライアントの画面に何も表示されなくなる可能性があります。

図 2-2. エラーを表示する NAT デバイス経由のクライアントからの PColP

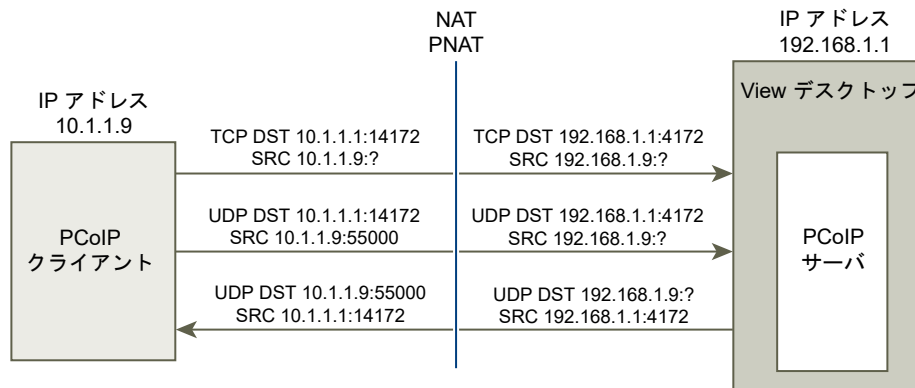


この問題を解決するには、外部 IP アドレスを使用するようにプラグインを構成する必要があります。このデスクトップで `externalIPAddress` がこのデスクトップで 10.1.1.1 として構成されている場合、このデスクトップにデスクトッププロトコル接続をする場合、プラグインはこのクライアントに IP アドレス 10.1.1.1 を提供します。PCoIP の場合、このセットアップのデスクトップで PCoIP Secure Gateway サービスが開始されなければなりません。

ポートマッピングの場合、デスクトップは標準の PCoIP ポート 4172 を使用するが、クライアントはポートマッピングデバイスでポート 4172 にマッピングされる別の送信先ポートを使用する必要があるときには、管理者はこのセットアップ用にプラグインを構成する必要があります。ポートマッピングデバイスによってポート 14172 が 4172 にマッピングされる場合、クライアントは PCoIP に送信先ポート 14172 を使用する必要があります。管理者は、PCoIP 用にこのセットアップを構成する必要があります。プラグインの `externalPCoIPPort` を 14172 に設定します。

NAT とポートマッピングを使用する構成では、`externalIPAddress` を 10.1.1.1 (192.168.1.1 にネットワーク変換される) に設定し、`externalPCoIPPort` を 14172 (4172 にポートマップされる) に設定します。

図 2-3. NAT デバイスおよびポートマッピング経由のクライアントからの PColP



PCoIP の外部 PCoIP TCP/UDP ポート構成と同様に、RDP ポート (3389) またはフレームワークチャネルポート (32111) のポートマッピングが行われる場合は、`externalRDPPort` と `externalFrameworkChannelPort` を構成し、ポートマッピングデバイス経由によるこれらの接続にクライアントが使用する TCP ポート番号を指定する必要があります。

高度なアドレス方式

仮想マシン ベースの複数のデスクトップを、NAT および同じ外部 IP アドレス上のポート マッピング デバイスを介してアクセスできるように構成する場合、各デスクトップに一意のポート番号を指定する必要があります。これでクライアントは同じ送信先 IP アドレスを使用できますが、特定の仮想デスクトップに接続をダイレクトする場合は HTTPS 接続用の一意の TCP ポート番号を使用します。

たとえば同じ送信先 IP アドレスを使用して、HTTPS ポート 1000 はある 1 つのデスクトップにダイレクトし、HTTPS ポート 1005 はもう 1 つのデスクトップにダイレクトするとします。この場合、デスクトップ プロトコル 接続のためにすべてのデスクトップに一意の外部ポート番号を構成するのは、あまりにも複雑です。このような理由から、プラグイン設定の `externalPCoIPPort`、`externalRDP`、および `externalFrameworkChannelPort` に静的な値ではなく関係式を指定して、クライアントが使用するベースの HTTPS ポート番号に相対的なポート番号を定義できます。

ポート マッピング デバイスが HTTPS でポート番号 1000 を使用する場合は TCP 443 にマップされ、RDP のポート番号 1001 では TCP 3389 に、PCoIP のポート番号 1002 では TCP および UDP 4172 に、フレームワーク チャネルのポート番号 1003 では TCP 32111 にマップされます。構成を簡素化するために、外部ポート番号は `externalRDP`、`externalPCoIP`、および `externalFrameworkChannelPort` に設定できます。HTTPS 送信先ポート番号 1000 を使用したクライアントから HTTPS 接続が行われるとき、外部ポート番号がこのポート番号 1000 に対して相対的に自動計算され、それぞれ 1001、1002、および 1003 が使用されます。

もう 1 つの仮想デスクトップを展開するために、ポート マッピング デバイスが HTTPS でポート番号 1005 を使用する場合は TCP 443 にマップされ、RDP のポート番号 1006 では TCP 3389 に、PCoIP のポート番号 1007 では TCP および UDP 4172 に、フレームワーク チャネルのポート番号 1008 では TCP 32111 にマップされます。デスクトップ (+1、+2、+3 など) の外部ポート構成が全く同じであれば、HTTPS 送信先ポート番号 1005 を使用したクライアントから HTTPS 接続が行われるときに、外部ポート番号がこのポート番号 1005 に対して相対的に自動計算され、それぞれ 1006、1007、および 1008 が使用されます。

この方式を使用すると、すべてのデスクトップを同一に構成できるほか、同じ外部 IP アドレスを共有できます。ベースの HTTPS ポート番号を 5 つずつ増やして(1000、1005、1010 ...) ポート番号を割り当てると、12,000 を超える仮想デスクトップが同じ IP アドレスでアクセスできるようになります。ベースのポート番号を使用すると、ポート マッピング デバイス構成に基づいて、接続のルーティング先となる仮想デスクトップを判断できます。すべての仮想デスクトップで `externalIPAddress=10.20.30.40`、`externalRDP`、`externalPCoIP`、および `externalFrameworkChannelPort` が設定されている場合、仮想デスクトップへのマッピングは NAT およびポート マッピングの表で示すとおりです。

表 2-2. NAT およびポート マッピングの値

VM#	デスクトップ IP アドレス	HTTPS	RDP	PCOIP (TCP および UDP)	フレームワーク チャネル
0	192.168.0.0	10.20.30.40:1000 -> 192.168.0.0:443	10.20.30.40:1001 -> 192.168.0.0:3389	10.20.30.40:1002 -> 192.168.0.0:4172	10.20.30.40:1003 -> 192.168.0.0:32111
1	192.168.0.1	10.20.30.40:1005 -> 192.168.0.1:443	10.20.30.40:1006 -> 192.168.0.1:3389	10.20.30.40:1007 -> 192.168.0.1:4172	10.20.30.40:1008 -> 192.168.0.1:32111

VM#	デスクトップ IP アドレス	HTTPS	RDP	PCOIP (TCP および UDP)	フレームワーク チャネル
2	192.168.0.2	10.20.30.40:1010 -> 192.168.0.2:443	10.20.30.40:1011 -> 192.168.0.2:3389	10.20.30.40:1012 -> 192.168.0.2:4172	10.20.30.40:1013 -> 192.168.0.2:32111
3	192.168.0.3	10.20.30.40:1015 -> 192.168.0.3:443	10.20.30.40:1016 -> 192.168.0.3:3389	10.20.30.40:1017 -> 192.168.0.3:4172	10.20.30.40:1018 -> 192.168.0.3:32111

この例では、Horizon Client は IP アドレス 10.20.30.40 および HTTPS 送信先ポート番号 ($1000 + n * 5$) に接続します。ここで n はデスクトップ番号です。デスクトップ 3 に接続するには、クライアントは 10.20.30.40:1015 に接続します。このアドレス指定方式により、各デスクトップの構成設定が大幅に簡素化されます。すべてのデスクトップは、同一の外部アドレスとポート構成で構成されます。NAT およびポート マッピング構成は、この一貫したパターンで NAT およびポート マッピング デバイス内で行われ、すべてのデスクトップは 1 つのパブリック IP アドレスでアクセスできます。クライアントは通常、この IP アドレスを解決する 1 つのパブリック DNS 名を使用します。

Windows 証明書ストアへの認証局の追加

スマート カード認証を使用する場合、スマート カード証明書にサインする認証局 (CA) が Windows 証明書ストアに常駐する必要があります。常駐していない場合、Windows 証明書ストアに CA を追加できます。

前提条件

Microsoft 管理コンソール (MMC) に証明書のスナップインがあることを確認します。『View のインストール』の「MMC への証明書スナップインの追加」を参照してください。

手順

- 1 MMC を開始します。
- 2 MMC コンソールで、[証明書 (ローカル コンピュータ)] ノードを展開し、[信頼されたルート証明機関] - [証明書] フォルダに移動します。
ルート証明書があり、証明書チェーンに中間証明書がなければ、MMC を終了します。
- 3 [信頼されたルート証明機関] - [証明書] フォルダを右クリックし、[すべてのタスク] - [インポート] をクリックします。
- 4 [証明書のインポート] ウィザードで、[次へ] をクリックしてルート CA 証明書が保存されている場所を参照します。
- 5 ルート CA 証明書ファイルを選択し、[開く] をクリックします。
- 6 [次へ] をクリックし、[次へ] をクリックし、そして [終了] をクリックします。
- 7 スマート カード証明書が中間 CA によって発行されている場合、証明書チェーンのすべての中間証明書をインポートします。
 - a [証明書 (ローカル コンピュータ)] - [中間証明機関] - [証明書] フォルダに移動します。
 - b 各中間証明書に対して、手順 3 から 6 を繰り返します。

HTML Access のセットアップ

View Agent Direct-Connection (VADC) プラグインは、仮想マシンベースのデスクトップおよび RDS デスクトップへの HTML Access をサポートしています。RDS アプリケーションへの HTML Access はサポートしていません。

この章には、次のトピックが含まれています。

- [HTML Access 用 View Agent のインストール](#)
- [静的なコンテンツ配信の設定](#)
- [信頼される CA 署名付き SSL サーバ証明書の設定](#)
- [Windows 10 デスクトップでの HTTP/2 プロトコルの無効化](#)

HTML Access 用 View Agent のインストール

HTML Access をサポートするために、特別なパラメータを使用して仮想マシンベース デスクトップに View Agent をインストールする必要があります。

前提条件

- VMware ダウンロード ページ (<http://www.vmware.com/go/downloadview>) から、View Agent インストーラ ファイルをダウンロードします。

インストーラのファイル名は、32 ビット Windows の場合は `VMware-viewagent-y.y.y-xxxxxx.exe`、64 ビット Windows の場合は `VMware-viewagent-x86_64-y.y.y-xxxxxx.exe` です。y.y.y はバージョン番号、xxxxxx はビルド番号です。

手順

- ◆ コマンド ラインから View Agent をインストールし、View Agent を View 接続サーバに登録しないようにパラメータを指定します。

この例では 32 ビット バージョンの View Agent をインストールします。

```
VMware-viewagent-y.y.y-xxxxxx.exe /v VDM_SKIP_BROKER_REGISTRATION=1
```

次のステップ

View Agent Direct-Connection プラグインをインストールします。[View Agent Direct-Connection プラグインのインストール](#)を参照してください。

静的なコンテンツ配信の設定

HTML Access クライアントをデスクトップで提供する必要がある場合には、デスクトップでセットアップ タスクをいくつか実行する必要があります。この作業により、ユーザーはブラウザで直接デスクトップをポイントできるようになります。

前提条件

- VMware ダウンロード ページ (<http://www.vmware.com/go/downloadview>) から View HTML Access の portal.war zip ファイルをダウンロードします。

ファイル名は、VMware-Horizon-View-HTML-Access-y.y.y-xxxxxx.zip です (y.y.y はバージョン番号、xxxxxx はビルド番号)。

手順

- 1 [コントロール パネル] を開きます。
- 2 [プログラムと機能] - [Windows の機能の有効化または無効化] の順に移動します。
- 3 [インターネット インフォメーション サービス] チェック ボックスを選択し、[OK] をクリックします。
- 4 [コントロール パネル] で、[管理ツール] - [インターネット インフォメーション サービス (IIS) マネージャー] の順に移動します。
- 5 左ペインにある項目を展開します。
- 6 [既定の Web サイト] を右クリックし、[バインドの編集...] を選択します。
- 7 [追加] をクリックします。
- 8 [https]、[すべて未使用]、およびポート [443] を指定します。
- 9 [SSL 証明書] フィールドで、正しい証明書を選択します。

オプション	アクション
証明書 [vdm] が存在します。	[vdm] を選択し、[OK] をクリックします。
証明書 [vdm] が存在しません。	[vdmdefault] を選択し、[OK] をクリックします。

- 10 [サイト バインド] ダイアログで、[http ポート 80] のエントリを削除し、[閉じる] をクリックします。
- 11 [既定の Web サイト] をクリックします。
- 12 [MIME の種類] をダブルクリックします。
- 13 [ファイル名拡張子] .json が存在しない場合は、[アクション] ペインで、[追加...] をクリックします。存在する場合は、次の 2 つの手順はスキップします。
- 14 [ファイル名拡張子] に [.json] と入力します。
- 15 [MIME の種類] に [text/h323] と入力し、[OK] をクリックします。
- 16 VMware-Horizon-View-HTML-Access-y.y.y-xxxxxx.zip を一時フォルダにコピーします。

17 VMware-Horizon-View-HTML-Access-y.y.y-xxxxxx.zip を解凍します。

この結果、portal.war というファイルが表示されます。

18 portal.war を portal.zip という名前に変更します。

19 portal.zip をフォルダ C:\inetpub\wwwroot に解凍します。

必要に応じてフォルダのアクセス許可を調整し、ファイルを追加できるようにします。

フォルダ C:\inetpub\wwwroot\portal が作成されます。

20 [Notepad] を開きます。

21 次のコンテンツが入ったファイル C:\inetpub\wwwroot\Default.htm を作成します（<デスクトップの IP アドレスまたは DNS 名> をデスクトップの実際の IP アドレスまたは DNS 名に置き換えてください）。

```
<HEAD>
<noscript>
  <meta HTTP-EQUIV="REFRESH" content="0; url=https://<IP address or DNS name of desktop>/portal/
webclient/index.html">
</noscript>
</HEAD>
<script>
  var destination = 'https://<IP address or DNS name of desktop>/portal/webclient/index.html';
  var isSearch = !!window.location.search;
  window.location.href = destination + (isSearch ? window.location.search + '&' : '?') +
'vadc=1' + (window.location.hash || '');
</script>
```

信頼される CA 署名付き SSL サーバ証明書の設定

信頼される CA 署名付き SSL サーバ証明書を設定して、クライアントとデスクトップ間のトラフィックが不正でないことを保証します。

前提条件

- デフォルトの自己署名 SSL サーバ証明書を信頼される CA 署名付き SSL サーバ証明書で置き換えます。[デフォルトの自己署名 SSL サーバ証明書の置き換え](#)を参照してください。これにより、フレンドリ名の値 **vdm** を持つ証明書が作成されます。
- クライアントの静的コンテンツがデスクトップにより提供される場合、静的コンテンツの配布を設定します。[静的なコンテンツ配信の設定](#)を参照してください。
- Windows 証明書ストアについて理解しておきます。『View のインストール』の「新しい SSL 証明書を使用するように View 接続サーバ、セキュリティ サーバ、または View Composer を構成する」を参照してください。

手順

- 1 Windows 証明書ストアで、[個人 > 証明書] に移動します。
- 2 フレンドリ名 [vdm] を持つ証明書をダブルクリックします。
- 3 [詳細] タブをクリックします。

- 4 [サムプリント] の値をコピーします。
- 5 Windows レジストリ エディタを開始します。
- 6 レジストリ キー HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config に移動します。
- 7 新しい文字列 (REG_SZ) 値 SslHash をこのレジストリ キーに追加します。
- 8 SslHash 値を [サムプリント] 値に設定します。

Windows 10 デスクトップでの HTTP/2 プロトコルの無効化

一部の Web ブラウザでは、Windows 10 VADC デスクトップにアクセスするときに、ERR_SPDY_PROTOCOL_ERROR というエラーが発生することがあります。このエラーを回避するには、デスクトップの HTTP/2 プロトコルを無効にします。

手順

- 1 Windows レジストリ エディタを開始します。
- 2 レジストリ キー HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\HTTP\Parameters に移動します。
- 3 2つの新しい REG_DWORD 値 EnableHttp2Tls および EnableHttp2Cleartext をこのレジストリ キーに追加します。
- 4 両方の値を [0] に設定します。
- 5 デスクトップを再起動します。

リモート デスクトップ サービス ホストでの View Agent Direct-Connection の設定

4

View では、ユーザーが Horizon Client からアクセス可能な RDS デスクトップやアプリケーションを提供するリモート デスクトップ サービス (RDS) ホストをサポートしています。RDS デスクトップは、RDS ホストへのデスクトップセッションに基づいています。標準的な View 展開では、クライアントは View 接続サーバを使用してデスクトップやアプリケーションに接続します。ただし、RDS ホストに View Agent Direct-Connection プラグインをインストールすると、クライアントは View 接続サーバを使用せずに RDS デスクトップやアプリケーションに直接接続できます。

この章には、次のトピックが含まれています。

- リモート デスクトップ サービス (RDS) ホスト
- RDS デスクトップおよびアプリケーションに資格を割り当てる

リモート デスクトップ サービス (RDS) ホスト

リモート デスクトップ サービス (RDS) ホストは、リモート アクセスのためのアプリケーションおよびデスクトップをホストするサーバ コンピュータです。

View 展開では、RDS ホストは、Microsoft リモート デスクトップ サービス ロール、Microsoft リモート デスクトップ セッション ホスト サービスおよび View Agent がインストールされている Windows サーバです。RDS ホストでは、VADC プラグインがインストールされていれば、View Agent Direct Connection (VADC) がサポートされます。RDS ホストの設定と View Agent のインストールに関する情報については、『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「リモート デスクトップ サービス ホストの設定」を参照してください。VADC プラグインのインストールについては、[1 章 View Agent Direct-Connection プラグインのインストール](#)を参照してください。

注: View Agent をインストールするときに、インストーラで、View Agent の接続先になる View 接続サーバのホスト名または IP アドレスの入力が求められます。パラメータを使用してインストーラを実行すると、この手順を省略できます。

```
VMware-viewagent-x86_64-y.y.y-xxxxxx.exe /v "VDM_SKIP_BROKER_REGISTRATION=1"
```

RDS ホストの設定と VADC プラグインのインストールを行った後に、RDS デスクトップとアプリケーションに資格を付与する必要があります。[RDS デスクトップおよびアプリケーションに資格を割り当てる](#)を参照してください。

RDS デスクトップおよびアプリケーションに資格を割り当てる

ユーザーがデスクトップおよびアプリケーションにアクセスする前に、ユーザーに RDS デスクトップおよびアプリケーションに対する資格を割り当てる必要があります。

RDS ホストで Windows Server 2008 R2 SP1 が実行している場合、[RemoteApp マネージャ]を実行して資格を構成します。

RDS ホストで Windows Server 2012 または 2012 R2 が実行している場合、[Server Manager] を実行して [リモート デスクトップ サービス] に移動し、資格を構成します。

デスクトップに対する資格

ユーザーに RDS デスクトップを起動する資格を割り当てるには、次の手順を実行します。

- ユーザーがローカル グループ [View Agent Direct-Connection ユーザー] のメンバーであることを確認します。デフォルトでは、すべての認証されたユーザーはこのグループのメンバーです。
- Windows Server 2008 R2 SP1 では、[RemoteApp マネージャ] で、RD セッション ホスト サーバが [リモート デスクトップ接続を RD Web Access のこの RD セッション ホスト サーバに示す] に構成されていることを確認します。
- Windows 2012 または 2012 R2 の場合、[Server Manager] を実行して [リモート デスクトップ サービス] に移動し、資格を構成します。

アプリケーションに対する資格

ユーザーに アプリケーションを起動する資格を割り当てるには、次の手順を実行します。

- ユーザーがローカル グループ [View Agent Direct-Connection ユーザー] のメンバーであることを確認します。デフォルトでは、すべての認証されたユーザーはこのグループのメンバーです。
- Windows Server 2008 R2 SP1 では、[RemoteApp マネージャ] で、アプリケーションが [RemoteApp プログラム] の下にリストされて、[RD Web Access] 用に設定され、すべてのユーザー、このユーザー、またはユーザーがメンバーであるグループに対して設定されたユーザー割り当てがあることを確認します。
- Windows 2012 または 2012 R2 の場合、[Server Manager] を実行して [リモート デスクトップ サービス] に移動し、資格を構成します。

View Agent Direct-Connection プラグインのトラブルシューティング

5

View Agent Direct-Connection プラグインを使用する場合、既知の問題が発生することがあります。

View Agent Direct-Connection プラグインに関する問題を調査する場合、正しいバージョンがインストールされ実行されていることを確認してください。

VMware に関するサポートの問題を提起する必要がある場合は、必ず完全なログを有効にし、問題を再現してから、データ収集ツール (DCT) ログ セットを生成してください。こうすることで、VMware テクニカル サポートはこれらのログを分析できます。DCT ログ セットの生成の詳細については、VMware View の診断情報の収集に関するナレッジベースの記事 (<http://kb.vmware.com/kb/1017939>) 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。

- [不適切なグラフィック ドライバがインストールされている](#)
- [ビデオ RAM の不足](#)
- [トレース情報とデバッグ情報を含めるために完全なログ記録を有効にする](#)

不適切なグラフィック ドライバがインストールされている

PCoIP が正常に機能するには、適切なバージョンのグラフィック ドライバがインストールされている必要があります。

問題

ユーザーが PCoIP を使用してデスクトップまたはアプリケーションに接続すると、ブラック スクリーンが表示されます。

原因

不適切なバージョンのグラフィック ドライバが動作しています。View Agent のインストール後に不適切なバージョンの VMware Tools がインストールされると、この問題が発生する場合があります。

解決方法

- ◆ View Agent 再度インストールしてください。

ビデオ RAM の不足

PCoIP をサポートするには、デスクトップまたは RDS ホストを実行する仮想マシンには、128MB 以上のビデオ RAM が必要です。

問題

ユーザーが PCoIP を使用してデスクトップまたはアプリケーションに接続すると、ブラック スクリーンが表示されます。

原因

この仮想マシンには、十分なビデオ RAM がありません。

解決方法

- ◆ 各仮想マシンには、128MB 以上のビデオ RAM を構成してください。

トレース情報とデバッグ情報を含めるために完全なログ記録を有効にする

View Agent Direct-Connection プラグインでは、ログ エントリを標準の View Agent ログに書き込みます。トレースおよびデバッグ情報は、デフォルトではログに含まれません。

問題

View Agent ログにはトレースおよびデバッグ情報は含まれません。

原因

完全なログは有効になっていません。View Agent ログにトレースおよびデバッグ情報を含めるには、完全なログを有効にする必要があります。

解決方法

- 1 コマンド プロンプトを開いて、C:\Program Files\VMware\VMware View\Agent\DCT\support.bat loglevels を実行します。
- 2 完全なログの場合は **3** を入力します。

デバッグ ログ ファイルは %ALLUSERSPROFILE%\VMware\VDM\logs にあります。ファイル debug*.log には View Agent とプラグインからログに記録された情報が含まれます。プラグインのログ行を見つけるには、wsnm_xmlapi を検索します。

View Agent が起動されると、プラグインのバージョンがログに記録されます。

```
2012-10-01T12:09:59.078+01:00 INFO (09E4-0C08) <logloaded> [MessageFramework] Plugin
'wsnm_xmlapi - VMware View Agent XML API Handler Plugin' loaded, version=e.x.p build-
855808, buildtype=release
```

```
2012-10-01T12:09:59.078+01:00 TRACE (09E4-06E4) <PluginInitThread> [wsnm_xmlapi] Agent XML
API Protocol Handler starting
```