VMware Horizon View Agent Direct-Connection プラグイン管理

Horizon View 5.3
View Agent 5.3

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-001290-00

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/）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 Horizon View Agent Direct-Connection プラグイン管理

VMware Horizon View Agent Direct-Connection プラグイン管理は、 VMware Horizon View Agent Direct-Connection プラグインのインストールおよび構成についての情報を提供します。 このプラグインは、View Agent へのインストール可能な拡張で、 View 接続サーバを使用せずにデスクトップに直接接続することを View Client に許可します。

仮想デスクトップで動作している VMware Horizon View Agent Direct-Connection プラグインで、クライアントは 仮想デスクトップに直接接続できます。PCoIP、HTML5 Access、RDP、USB リダイレクト、およびセッション管理のすべての View デスクトップ機能は、 View 接続サーバを介してユーザーが接続した場合と同じ方法で動作します。

対象ユーザー

この情報は、VMware 仮想デスクトップに VMware Horizon View Agent Direct-Connection プラグインをインストール、アップグレードまたは使用するすべての人を 対象にしています。ガイドは、仮想マシン技術およびデータセンター操作を熟知している Windows システム管理者向けに 書かれています。

VMware Horizon View Agent Direct-Connection プラグインのセットアップおよびインストール

1

Horizon View Agent Direct-Connection プラグインのインストールには、View デスクトップが特定のシステム要件を満たし、仮想マシンでプラグイン インストーラが動作していることを確認する作業が含まれます。

この章では次のトピックについて説明します。

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

Horizon View Agent Direct-Connection プラグインは、以下のソフトウェア要件を満たす View 仮想デスクトップにインストールする 必要があります。

表 1-1. Horizon View Agent Direct-Connection プラグインのシステム要件

vSphere バージョン	オペレーティング システム バージョン	ソフトウェア
定められた View Agent バージョンがサポートするすべての vSphere バージョン。 重要　すべての仮想デスクトップは、vSphere 5.x ESXi ホストでホストされる必要があります。	定められた View Agent バージョンがサポートするすべてのオペレーティング システム バージョン。	■ View Agent 5.3 以降 ■ VMware Tools をインストール後に Horizon View Agent をインストールする必要があります。

重要　各 View 仮想デスクトップは、正しく機能するために PCoIP に少なくとも 128 MB のビデオ RAM を 構成する必要があります。

仮想デスクトップは、Microsoft Active Directory Domain に参加するか、ワークグループのメンバーに なることができます。

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

View Agent が動作している Windows 仮想マシンに Horizon View Agent Direct-Connection プラグインをインストールする必要があります。

開始する前に

仮想マシンが View Agent のサポートされたバージョンを実行していること、構成された十分なビデオ RAM 量があること、ESXi のサポートされたバージョンで動作していることを確認します。「VMware Horizon View Agent Direct-Connection プラグインのシステム要件 (P. 7)」を参照してください。

手順

1 管理者として仮想マシンにログインし、ユーザーのオペレーティング システムに適切なインストーラを起動します。

オペレーティング システム	インストーラ
Windows 64 ビット	VMware-viewagent-direct-connection-x86_64-x.y.z-nnnnnn.exe
Windows 32 ビット	VMware-viewagent-direct-connection-x.y.z-nnnnnn.exe

インストーラは、Windows オペレーティング システムおよび View Agent の正しいバージョンがインストールされることを確認します。

2 オプションで、[構成情報] ダイアログ ボックスに View Client からの HTTPS 要求を着信するためにリッスンするためにプラグインによって使用される TCP ポート番号を入力します。

デフォルトの TCP ポート番号は 443 で、ほとんどの場合変更すべきではありませんが、必要に応じてインストール後にポート番号を変更できます。

[[Windows ファイヤウォールを自動的に構成する]] チェックボックスがデフォルトで選択されます。この選択は、この TCP ポートのファイヤウォール規則を追加して、View Client からの接続を許可します。Windows ファイヤウォールが動作していて、この規則が作成されていない場合、View Client は接続できなくなります。

次に進む前に

この仮想マシンにアクセスするために View Client を使用して完了したインストールをテストしてください。View Client では、View 接続サーバ インスタンスまたはセキュリティ サーバの名前または IP アドレスを指定する代わりに、このプラグインを動作している View デスクトップの名前または IP アドレスを指定します。ユーザーは通常として認証し、デスクトップを選択および接続するためのユーザー エクスペリエンスは、View 接続サーバからの接続と同じです。

VMware Horizon View Agent Direct-Connection プラグインのアンインストール

他の Windows アプリケーションと同じように Horizon View Agent Direct-Connection プラグインをアンインストールできます。

手順

1 [[コントロール パネル] > [プログラムと機能]] を選択します。

2 [[VMware View Agent Direct-Connection プラグイン]] を選択します。

3 [[アンインストール]] を選択します。

Horizon View Agent Direct-Connection プラグインが削除され、View Agent が再起動されます。

VMware Horizon View Agent Direct-Connection プラグインの詳細構成 2

デフォルトの Horizon View Direct-Connection プラグイン構成設定を使用するか、 Windows Active Directory グループ ポリシー (GPO) を介するか、または特定の Windows レジストリ設定を使用してカスタマイズすることができます。

この章では次のトピックについて説明します。

VMware Horizon View Agent Direct-Connection プラグイン構成設定

Horizon View Agent Direct-Connection プラグインのすべての構成設定は、 各 View デスクトップのローカル レジストリに保存されます。Windows Active Directory グループ ポリシー (GPO)、ローカル ポリシー エディタを介して、またはレジストリを直接変更して、これらの設定を管理できます。

プラグインはデフォルト値で動作します。 ただし、このデフォルトは変更できます。これらのレジストリ値はレジストリキーで設定できます:

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

表 2-1. Direct-Connection プラグイン 構成設定

設定	レジストリ値	タイプ	説明
HTTPS ポート番号	httpsPortNumber	REG_SZ	View Client からの着信 HTTPS 要求をプラグインがリッスンする TCP ポート番号。 この値を変更する場合、Windows ファイヤウォールに対応する変更を行い、新しい値が許可されるようにする必要があります。
Session timeout（セッション タイムアウト）	sessionTimeout	REG_SZ	View Client でログイン後にユーザーがセッションを開いたままにできる期間。 時間は分単位で設定します。このポリシーが 構成されていないか無効である場合、デフォルトは 600 分です。デスクトップ セッションがタイム アウトすると、セッションは終了して View Clinet は デスクトップから切断されます。

表 2-1. Direct-Connection プラグイン 構成設定 (続き)

設定	レジストリ値	タイプ	説明
免責条項を有効	disclaimerEnabled	REG_SZ	値は TRUE または FALSE に設定されます。 TRUE に設定すると、ログインでユーザーが承諾する免責条項のテキストが表示されます。 このテキストは、記述されている場合は「免責条項テキスト」から表示されるか、GPO `Configuration\Windows Settings\Security Settings\Local Policies\Security Options: Interactive logon` から表示されます。disclaimerEnabled のデフォルト設定は FALSE です。
免責条項テキスト	disclaimerText	REG_SZ	ログインで View Client ユーザーに表示される免責条項テキスト。 免責条項を有効ポリシーは TRUE に設定する必要があります。テキストが指定されていない場合、デフォルトは Windows ポリシー `Configuration\Windows Settings\Security Settings\Local Policies\Security Options` からの値を使用します。 .
クライアント設定: AlwaysConnect	alwaysConnect	REG_SZ	値は TRUE または FALSE です。AlwaysConnect 設定は View Client に送付されます。 このポリシーが TRUE に設定されると、保存されているクライアント設定は上書きされます。 デフォルトでは値は設定されていません。このポリシーを有効にする場合は、値を TRUE に設定します。このポリシーを無効にする場合は、値を FALSE に設定します。
外部 PCoIP ポート	externalPCoIPPort	REG_SZ	PCoIP プロトコルで使用される送信先 TCP/UDP ポート番号の View Client に送信されるポート番号。 番号の先頭の A + 文字は、HTTPS で使用されるポート番号からの相対番号を示します。 外部に示されたポート番号が、サービスがリッスンしているポートと一致しない場合に限って、この値を設定します。 通常は、このポート番号は NAT 環境にあります。 デフォルトでは値は設定されていません。
外部 Blast ポート	externalBlastPort	REG_SZ	HTML5/Blast プロトコルで使用される送信先 TCP ポート番号の View Client に送信されるポート番号。 番号の先頭の A + 文字は、 HTTPS で使用されるポート番号からの相対番号を示します。外部に示されたポート番号が、サービスがリッスンしているポートと一致しない場合に限って、この値を設定します。 通常は、このポート番号は NAT 環境にあります。 デフォルトでは値は設定されていません。
外部 RDP ポート	externalRDPPort	REG_SZ	RDP プロトコルで使用される送信先 TCP ポート番号の View Client に送信されるポート番号。 番号の先頭の A + 文字は、HTTPS で使用されるポート番号からの相対番号を示します。外部に示されたポート番号が、サービスがリッスンしているポートと一致しない場合に限って、この値を設定します。 通常は、このポート番号は NAT 環境にあります。 デフォルトでは値は設定されていません。
外部 IP アドレス	externalIPAddress	REG_SZ	セカンダリ プロトコル（RDP、PCoIP、 フレームワーク チャネルなど）で使用される送信先 IP アドレスの View Client に送付される IP v4 アドレス。外部に示されたアドレスがデスクトップ マシンのアドレスと一致しない場合に限ってこの値を設定します。 通常は、このアドレスは NAT 環境にあります。 デフォルトでは値は設定されていません。

表 2-1. Direct-Connection プラグイン 構成設定 (続き)

設定	レジストリ値	タイプ	説明
外部フレームワーク チャネル ポート	externalFrameworkChannelPort	REG_SZ	フレームワーク チャネル プロトコルで使用される送信先 TCP/UDP ポート番号の View Client に送信されるポート番号。 番号の先頭の A + 文字は、 HTTPS で使用されるポート番号からの相対番号を示します。外部に示されたポート番号が、サービスがリッスンしているポートと一致しない場合に限って、この値を設定します。 通常は、このポート番号は NAT 環境にあります。 デフォルトでは値は設定されていません。
USB 有効化	usbEnabled	REG_SZ	値は **TRUE** または **FALSE** に設定します。デスクトップがクライアント システムに接続された USB デバイスを使用できるかどうかを判断します。 デフォルト値は有効です。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、 設定を無効 (**FALSE**) に変更します。
クライアント設定: USB AutoConnect	usbAutoConnect	REG_SZ	値は **TRUE** または **FALSE** に設定します。USB デバイスがプラグインされるときに、USB デバイスをデスクトップに接続します。 このポリシーが設定されている場合、保存されているすべてのクライアント設定は上書きされます。 デフォルトでは値は設定されていません。
有効化をリセット	resetEnabled	REG_SZ	値は **TRUE** または **FALSE** に設定します。 **TRUE** に設定されると、認証された View Client はオペレーティング システム レベルの再起動を実行できます。 デフォルトでは、この設定は無効になっています (**FALSE**)。
クライアント証明書キャッシュ タイムアウト	clientCredentialCacheTimeout	REG_SZ	保存されたパスワードを View Client がユーザーに使用許可する時間（分）。 0 は許可しないという意味で、-1 は永久に許可するという意味です。View Client は、この設定が有効値に設定されている場合、パスワードの保存オプションをユーザーに提供します。 デフォルトは 0 分（許可しない）です。

View Client 設定は、プラグインの動作を変更しません。 これらの設定は、解釈のために View Client に送付されます。

外部ポート番号および外部 IP アドレス値は、ネットワーク アドレス変換（NAT）および ポート マッピング サポートで使用されます。詳細については、を参照してください。★xml で調整必要：このセグメントの外にある 「ネットワーク アドレス変換 とポート マッピングの使用 (P. 13)」.

ローカル ポリシー エディタを使用するか、Active Directory でグループ ポリシー オブジェクト（GPO）を使用して、これらのレジストリ設定を上書きするポリシーを 設定できます。ポリシー設定は、通常のレジストリ設定よりも優先されます。 GPO テンプレート ファイルはポリシーを構成するために共有されます。 View 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ると、テンプレート ファイルは以下の場所に置かれます:

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

このテンプレート ファイルを Active Directory またはローカル グループ ポリシー エディタにインポートして、 これらの構成設定の管理を簡素化できます。この方法でポリシー設定を管理する詳細については、Microsoft ポリシー エディタおよび GPO 取り扱いマニュアルを参照してください。 プラグインのポリシー設定は、レジストリ キーに保存されます:

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

SSL/TLS で弱い暗号を無効

SSL/TLS プロトコルを使用する View Client と View デスクトップ間の通信が、この View デスクトップの硬化手順を使用して弱い暗号化文字を許可しないことを保証できます。

弱い暗号化を無効にするための構成は、Windows レジストリに保存されます。これらの設定の変更は、View Agent Direct-Connection プラグインを実行するすべてのデスクトップ オペレーティング システムで行う必要があります。

注意　これらの設定は、オペレーティング システムでの SSL/TLS のすべての使用に影響します。

INTERNET-DRAFT `56-bit Export Cipher Suites For TLS draft-ietf-tls-56-bit-ciphersuites-00.txt` がある SSL 3.0 および TLS 1.0 (RFC2246) の両方が、異なる文字スイートを使用するオプションを提供します。各文字スイートは、SSL/TLS セッション内で使用されるキー交換、認証、暗号化、および MAC アルゴリズムを決定します。

開始する前に

`Regedt32.exe` レジストリ エディタを使用して Windows レジストリ キーの編集を経験する必要があります。

手順

- レジストリ エディタ `Regedt32.exe` を起動して、このレジストリ キーを指定します:`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL`

次に進む前に

表 2-2. 文字スイートの更新

Windows XP SP3	Windows Vista 以降
1 subkey`\Ciphers\DES 56/56` で、DWORD 値 `Enabled` を `0x0` の値で追加します。 2 subkey`\Hashes\MD5` で、DWORD 値 `Enabled` を `0x0` の値で追加します。 これらの更新は、以下の文字だけが Windows XP SP3 で使用できることを保証します: ■ SSLv3 168 ビット DES-CBC3-SHA ■ SSLv3 128 ビット RC4-SHA ■ TLSv1 168 ビット DES-CBC3-SHA ■ TLSv1 128 ビット RC4-SHA	1 subkey `\Hashes` で subkey `MD5` を作成します。 2 subkey `\Hashes \MD5` で、DWORD 値 `Enabled` を `0x0` の値で追加します。 これらの更新は、以下の文字だけが Windows Vista 以降で使用できることを保証します: ■ SSLv3 168 ビット DES-CBC3-SHA ■ SSLv3 128 ビット RC4-SHA ■ TLSv1 256 ビット AES256-SHA ■ TLSv1 128 ビット AES128-SHA ■ TLSv1 168 ビット DES-CBC3-SHA ■ TLSv1 128 ビット RC4-SHA

デフォルトの自己署名 SSL サーバ証明書の置換

自己署名 SSL サーバ証明書は、改ざんや盗聴の脅威に対して十分な保護を View Client に 与えることができません。これらの脅威からデスクトップを保護するには、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。

View Agent Direct-Connection プラグインをインストール後に初めて起動すると、 自動的に自己署名 SSL サーバ証明書を生成して、Windows Certificate Store にそれを配置します。 SSL サーバ証明書が SSL プロトコルのネゴシエーション中に View Client に提示され、 この View デスクトップについての情報がクライアントに提供されます。このデフォルトの自己署名 SSL サーバ証明書は、 クライアントによって信用され、View Client 証明書チェックによって完全に証明されている Certificate Authority (CA) によって署名された証明書と置き換えない限り、このデスクトップについて保証を与えることはできません。

Windows Certificate Store でこの証明書を保存する手続きおよび 適切な CA によって署名された証明書で置き換える手続きは、View 接続サーバ（バージョン 5.1 以降）で使用される手続きと同じです。 この証明書の置き換え手続きの詳細は、『VMware Horizon View インストール ガイド』の「View サーバの SSL 証明書を構成」 を参照してください。

Subject Alternative Name (SAN) 付きの証明書とワイルドカード証明書がサポートされます。

注意　View Agent Direct-Connection プラグインを使用して多くの View デスクトップに CA 署名 SSL 証明書を配布するには、 Active Directory Enrollment を使用して、各仮想マシンに証明書を配布します。 詳細については、を参照してください。★xml で調整必要：このセグメントの外にある
http://technet.microsoft.com/en-us/library/cc732625.aspx

View Client を View デスクトップにアクセス認証

View Client のユーザーが View デスクトップに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 Users] と呼ばれるローカル オペレーティング システム グループ内で直接制御されます。

ユーザーがこのグループのメンバーである場合、そのユーザーはデスクトップに直接接続することが認証されます。プラグインを最初にインストールする場合、このローカル グループが作成され、認証されたユーザー グループが含まれます。プラグインによって認証されたすべての人がデスクトップにアクセスするために認証されます。

このデスクトップへのアクセスを制限する場合、ユーザーおよびユーザー グループのリストを指定するためのこのグループのメンバーシップを変更できます。これらのユーザーは、ローカルまたはドメイン ユーザーおよびユーザー グループが可能です。View Client ユーザーがこのグループに存在しなければ、ユーザーはこのデスクトップにアクセスする資格がない旨の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

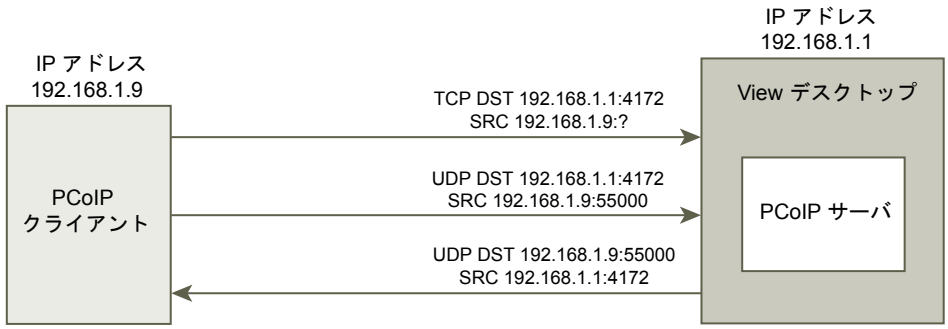
View Client が異なるネットワークの View デスクトップに接続する場合、ネットワーク アドレス変換 （NAT） とポート マッピングの構成が必要となります。

この例では、 View デスクトップの外部アドレス情報を構成し、 View Client がこの情報を使用し、NAT またはポート マッピング デバイスを使用して View デスクトップに 接続できるようにする必要があります。この URL は、View Connection Server とセキュリティ サーバにある外部 URL と PCoIP 外部 URL の設定と同じです。

View Client が別のネットワークにあり、 NAT デバイスが View Client とプラグインを実行している View 仮想デスクトップ間にある場合は、 NAT またはポート マッピング構成が必要となります。 たとえば、View Client と View 仮想デスクトップ間にファイアウォールがある場合、 このファイアウォールは NAT またはポート マッピング デバイスとして動作します。

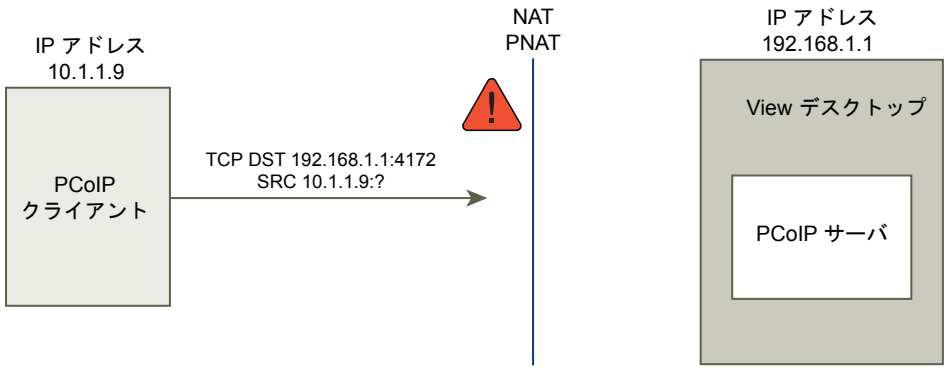
IP アドレスが 192.168.1.1 の View デスクトップ の導入例における NAT と ポート マッピングを示します。同じネットワークにある IP アドレスが 192.168.1.9 の View Client システムは、 TCP および UDP を使用して PCoIP 接続を確立します。この 接続は、NAT やポート マッピング構成のないダイレクトの接続になります。

図 2-1. 同じネットワークのクライアント からのダイレクト PCoIP



NAT デバイスをクライアントとデスクトップ間に追加して、異なるアドレス空間で 稼働するようにしており、プラグインに構成上の変更を行わない場合 PCoIP パケットは正しくルーティングされずに、 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、 IP アドレスが 10.1.1.9 になっています。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。送信先の アドレスである 192.168.1.1 は、クライアント ネットワークからは機能せず、クライアント の画面には何も表示されない場合があります。

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の PCoIP

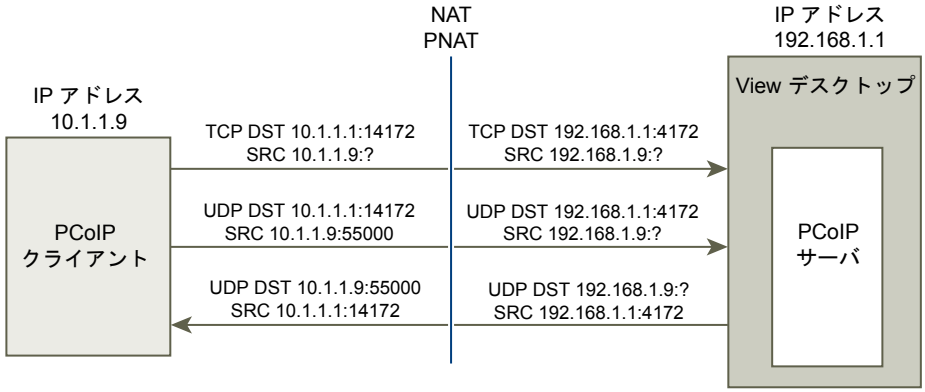


この問題を解決するためには、 外部 IP アドレスを使用するようにプラグインを構成する必要があります。 もし、 `externalIPAddress` がこのデスクトップで 10.1.1.1 として構成されている場合、 このデスクトップにデスクトップ プロトコル接続をする場合、 プラグインはこのクライアントに IP アドレス 10.1.1.1 を提供します。 PCoIP の場合、PCoIP Secure Gateway サービスをこのセットアップ環境のデスクトップで開始する必要があります。

ポート マッピングについては、 デスクトップが標準の PCoIP ポート 4172 を使用するものの、クライアントが、ポート マッピング デバイスのポート 4172 にマッピングされて いる別の送信先ポートを使用する必要がある場合、 このセットアップ環境では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 デバイスがポート 14172 を 4172 にマッピングする場合、 クライアントは、PCoIP で送信先ポート 14172 を使用する必要があります。PCoIP では、このセットアップ環境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 使用し、 `externalIPAdress` が 10.1.1.1 に設定されている構成では、ネットワークは 192.168.1.1 に変換され、 `externalPColPPort` が 14172 に設定され、ポートは 4172 にマッピングされます。

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の PCoIP



PCoIP の外部 PCoIP TCP/UDP ポート 構成と同様、RDP ポート （3389） または Framework Channel ポート （32111） がポート マッピングされる場合、 `externalRDPPort` および `externalFrameworkChannelPort` を構成し、クライアントがポート マッピング デバイスを介して接続を行うために使用する TCP ポート番号を指定する必要があります。

高度なアドレッシング スキーム

いくつかの View デスクトップを NAT および同じ外部 IP アドレスでデバイスを割り当てるポートを介してアクセスできるように構成する場合、各 View デスクトップにポート番号の一意的なセット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付先 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直接接続するには HTTPS 接続用の一意の TCP ポート番号を使用してください。

アドレッシング スキームの例

この例では、両方が同じ送付先 IP アドレスを使用して、HTTPS ポート 1000 は 1 つのデスクトップに向かい、HTTPS ポート 1005 は他に向かいます。このケースでは、デスクトップ プロトコル接続用のすべての View デスクトップに対して一意の外部ポート番号を構成することは複雑すぎます。この理由のため、プラグイン設定の `externalPCoIPPort`、`externalRDPPort`、および `externalFrameworkChannelPort` は、クライアントで使用されるベースの HTTPS ポート番号に相対するポート番号を定義するために静的値の代わりに、オプションの関係式を取ることができます。

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 は TCP 3389 にマップされ、PCoIP のポート番号 1002 は TCP および UDP 4172 にマップされ、フレームワーク チャネルのポート番号 1003 は TCP 32111 にマップされ、構成を簡素化するために、外部ポート番号は `externalRDPPort`=+1、`externalPCoIPPort`=+2 および `externalFrameworkChannelPort`=+3 に構成できます。1000 の HTTPS 送付先ポート番号を使用したクライアントから HTTPS 接続が来ている場合、外部ポート番号は 1000 のこのポート番号に対して自動的に計算され、それぞれ 1001、1002、および 1003 を使用します。

別の仮想デスクトップを導入するには、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 にマップされ、PCoIP のポート番号 1007 では TCP および UDP 4172 にマップされ、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。これは、HTTPS 接続が 1005 の HTTPS 送付先ポート番号を使用したクライアントから来ている場合にデスクトップ (+1、+2、+3、など) の全く同じ外部ポート構成で、これらの外部ポート番号は、自動的に 1005 のこのポート番号に対して計算され、それぞれ 1006、1007、および 1008 を使用します。

このスキーマによってすべてのデスクトップは個別に構成できると同時に、同じ外部 IP アドレスで共有できます。したがって、ベース HTTPS ポート番号の 5 つの (1000、1005、1010 …) の増分で割り当てているポート番号は、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することを許可します。そして、ベース ポート番号を使用して、ポート マッピング デバイス構成に基づいて、接続をルートする仮想デスクトップを判断します。すべての仮想デスクトップで構成された `externalIPAddress`=10.20.30.40、`externalRDPPort`=+1、`externalPCoIPPort`=+2 および `externalFrameworkChannelPort`=+3 では、仮想デスクトップへのマッピングは、NAT およびマッピング テーブルに説明されている通りです。

表 2-3. NAT およびポートのマッピング値

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
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

View Client は IP アドレス 10.20.30.40 および <n> が View デスクトップ番号である HTTPS 送付先ポート番号 (1000 +< n> * 5) に接続します。View 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。このアドレッシング スキームは、各 View デスクトップの構成設定を大幅に簡素化します。すべてのデスクトップは、同一の外部アドレスおよびポート構成で構成されます。NAT およびマッピング構成は、この一定のパターンで 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 View デスクトップは単一のパブリック IP アドレスでアクセスできます。クライアントは、一般的にこの IP アドレスを解決する単一のパブリック DNS 名を使用します。

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

3

Horizon View Agent Direct-Connection プラグインを使用する場合、いくつかの既知の問題が発生する可能性があり、それらを解決する必要があります。

Horizon View Agent Direct-Connection プラグインの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て動作していることを確認します。上記の例では、プラグイン バージョンの詳細は、`version=e.x.p build-855808, buildtype=release` です。プラグイン名 VMware View Agent XML API ハンドラー プラグインがログされています。

VMware でサポート問題を取り上げる必要がある場合、問題を再現し、Data Collection Tool (DCT) ログ セットを作成します。VMware のテクニカル サポートはこれらのログを分析できます。DCT ログ セットの作成についての詳細は、VMware View KB 記事 http://kb.vmware.com/kb/1017939 の診断情報の収集を参照してください。

トレースおよびデバッグ情報を含むフル ロギングを有効

Horizon View Agent Direct-Connection プラグインは、標準の View Agent ログにログ エントリを書き込みます。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

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

原因

フル ロギングは有効にされていません。View Agent ログにトレースおよびデバッグ情報を含めるためにフル ロギン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 フル ロギングでは **3** を入力します。

デバッグ ログ ファイルは、`%ALLUSERSPROFILE%\VMware\VDM\logs` に置かれます。`debug*.log` ファイルには、View Agent およびプラグインからログされた情報があります。プラグイン ログ行を見つけるためには `wsnm_xmlapi` を検索します。

View Agent が起動すると、プラグイン バージョンが記録されます:

```
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
```

仮想マシンに構成されたビデオ RAM が不十分

適正量のビデオ RAM を仮想マシンに構成する必要があります。

問題

PCoIP を使用すると黒い画面が表示されます。

原因

16 MB または 32 MB などの不十分なビデオ RAM が仮想マシンに構成されていました。

解決方法

- 各仮想マシンには少なくとも 128 MB のビデオ RAM を構成してください。

不正なグラフィックス ドライバがインストールされる

Horizon View Agent グラフィックス ドライバの正しいバージョンをインストールする必要があります。 グラフィックス ドライバは、Horizon View Agent がインストールされた後にダウングレードされた可能性があります。 これは、VMware Tools の不正なバージョンが Horizon View Agent の後にインストールされると発生します。

問題

ダウングレードされたグラフィックス ドライバのため、PCoIP を使用すると黒い画面が表示されます。

原因

グラフィックス ドライバの不正なバージョンがインストールされました。

解決方法

- Horizon View Agent を再インストールしてください。

インデックス