VMware Horizon Client para o Windows Guia de Instalação e Configuração

VMware Horizon Client for Windows 2111

vmware®

Você pode encontrar a documentação técnica mais atualizada no site da VMware, em:

https://docs.vmware.com/br/

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

VMware Brasil
Rua Surubim, 504 4º andar CEP 04571-050
Cidade Monções
São Paulo
SÃO PAULO: 04571-050
Brasil
Tel: +55 11 55097200
Fax: + 55. 11. 5509-7224
www.vmware.com/br

Conteúdo

VMware Horizon Client para o Windows Guia de Instalação e Configuração

Este guia descreve como instalar, configurar e usar o software VMware Horizon® Client™ em um sistema cliente Microsoft Windows.

Estas informações destinam-se a administradores que precisam configurar uma implantação do Horizon que inclui sistemas cliente Microsoft Windows, como desktops e laptops. As informações foram escritas para administradores de sistema experientes que estão familiarizados com a tecnologia de máquinas virtuais e as operações do centro de dados.

Se você for um usuário final, consulte o documento *VMware Horizon Client para o WindowsGuia do Usuário* ou visualize o Horizon Client para obter a ajuda on-line do Windows.

Requisitos do sistema e configuração para clientes baseados em Windows

1

Os sistemas que executam componentes Horizon Client devem atender a determinados requisitos de hardware e software.

O Horizon Client em sistemas Windows usa as configurações de Internet do Microsoft Internet Explorer, incluindo configurações de proxy, ao se conectar a um servidor. Verifique se as configurações do Internet Explorer estão corretas e se você pode acessar a URL do servidor por meio do Internet Explorer.

Leia os seguintes tópicos:

- Requisitos de hardware e software para sistemas cliente Windows
- Requisitos de autenticação de cartão inteligente
- Requisitos de autenticação do certificado do dispositivo cliente
- Requisitos de integração do OPSWAT
- Requisitos do sistema para áudio e vídeo em tempo real
- Requisitos do sistema para redirecionamento do scanner
- Requisitos do sistema para redirecionamento de porta serial
- Requisitos para usar o redirecionamento de conteúdo de URL
- Requisitos do sistema para redirecionamento de multimídia HTML5
- Requisitos do sistema para redirecionamento de navegador
- Requisitos do sistema para redirecionamento de multimídia (MMR)
- Configurar os serviços E911 para Microsoft Teams
- Requisitos do sistema para redirecionamento de geolocalização
- Requisitos do sistema para o recurso de colaboração de sessão
- Requisitos do sistema para Skype for Business
- Sistemas operacionais de desktop compatíveis

Requisitos de hardware e software para sistemas cliente Windows

Você pode instalar o Horizon Client para Windows em PCs e laptops que usam um sistema operacional Microsoft Windows compatível.

O PC ou laptop no qual você instala o Horizon Client e os periféricos que ele usa devem atender a determinados requisitos do sistema.

Modelos

Todos os dispositivos x86-64 Windows

Memória

Pelo menos 1 GB de RAM

Sistemas operacionais

Horizon Client é compatível com os seguintes sistemas operacionais.

SO	Versão	Service Pack ou Opção de Manutenção	Edições compatíveis
Windows 11	64 bits	N/A	Home, Pro, Pro para Workstations, Enterprise, Internet das Coisas (IoT) Enterprise e Education
Windows 10	64 bits	Versão 21H2 SAC Versão 21H1 SAC Versão 20H2 SAC Enterprise 2021 LTSC Enterprise 2019 LTSC	Home, Pro, Pro para Workstations, Enterprise, Internet das Coisas (IoT) Enterprise e Education
Windows Server 2012 R2	64 bits	Atualização mais recente	Padrão e Datacenter
Windows Server 2016	64 bits	Atualização mais recente	Padrão e Datacenter
Windows Server 2019	64 bits	Atualização mais recente	Padrão e Datacenter

Windows Server 2012 R2, Windows Server 2016 e Windows Server 2019 são compatíveis com a finalidade de executar Horizon Client no modo aninhado. Para obter informações sobre os recursos compatíveis com o modo aninhado, consulte o VMware artigo da Base de conhecimento (KB) 67248.

Importante Às vezes, novos sistemas operacionais Windows são compatíveis após a publicação deste documento. Para obter as informações de suporte do sistema operacional mais atualizadas, consulte o VMware artigo da Base de conhecimento (KB) 58096.

Servidor de Conexão e Horizon Agent

Versão de manutenção mais recente do Horizon 7 versão 7.5 e versões posteriores.

Se os sistemas cliente se conectarem de fora do firewall corporativo, use um appliance do Unified Access Gateway para que os sistemas cliente não exijam uma conexão VPN. Se a sua empresa tiver uma rede sem fio interna para fornecer acesso roteável a áreas de trabalho remotas que os dispositivos podem usar, você não precisa configurar o Unified Access Gateway ou uma conexão VPN.

Exibir protocolos

- PCoIP
- VMware Blast
- RDP

Protocolos de rede

- IPv4
- IPv6

Durante uma instalação personalizada do Horizon Client, você pode ativar a seleção automática do protocolo da Internet. Para obter mais informações, consulte Ativando a seleção automática de protocolo de Internet. Para obter informações sobre como usar o Horizon em um ambiente IPv6, consulte o documento *Instalação Horizon*.

Requisitos de hardware para PCoIP e VMware Blast

- Processador baseado em x86 com extensões SSE2, com uma velocidade de processador de 800 MHz ou mais rápida.
- RAM disponível acima dos requisitos do sistema para oferecer suporte a várias configurações de monitor. Use a fórmula a seguir como um guia geral. A unidade de medida é pixels.

```
20 MB + (24 * (# monitors) * (monitor width) * (monitor height))
```

Em geral, você pode usar os seguintes cálculos.

```
1 monitor: 1600 x 1200: 64 MB
2 monitors: 1600 x 1200: 128 MB
3 monitors: 1600 x 1200: 256 MB
```

Requisitos de hardware para RDP

- Processador baseado em x86 com extensões SSE2, com uma velocidade de processador de 800 MHz ou mais rápida.
- 128 MB de RAM.

Requisitos de software para RDP

- Para o Windows 10, use o RDP 10.0.

- O instalador do agente configura a regra de firewall local para conexões RDP de entrada para corresponder à porta RDP atual do sistema operacional do host, que normalmente é 3389. Se você alterar o número da porta RDP, deverá alterar as regras de firewall associadas.

Você pode baixar versões do Cliente de Área de Trabalho Remota do Centro de Download da Microsoft.

Requisitos de vídeo e gráficos

- Placa gráfica compatível com vídeo Direct3D 11.
- Drivers de placa de vídeo e de vídeo mais recentes.

Requisitos do .NET Framework

O instalador do Horizon Client requer o .NET Framework versão 4.5 ou posterior. O instalador verifica se o .NET Framework versão 4.5 ou posterior está instalado antes da instalação. Se a máquina cliente não atender a esse pré-requisito, o instalador baixará a versão mais recente do .NET Framework automaticamente.

Para usar o Horizon Client, é necessário o .NET Desktop Runtime para Windows x86 versão 5.0 ou posterior. O instalador do Horizon Client instala uma versão recente do Desktop Runtime. Depois de instalar o Horizon Client, você pode atualizar o Desktop Runtime em https://dotnet.microsoft.com/download/dotnet/5.0/runtime.

Requisitos de autenticação de cartão inteligente

Os dispositivos cliente que usam um cartão inteligente para autenticação do usuário devem atender a determinados requisitos.

Requisitos de hardware e software do cliente

Cada dispositivo cliente que usa um cartão inteligente para autenticação do usuário deve ter o seguinte hardware e software.

- Horizon Client
- Cartões inteligentes e leitores de cartão inteligente que usam um provedor PKCS#11 ou Microsoft CNG API/CryptoAPI.
- Drivers de aplicativo específicos do produto

Os usuários que se autenticam com cartões inteligentes devem ter um cartão inteligente ou token de cartão inteligente USB, e cada cartão inteligente deve conter um certificado de usuário.

Antes de emitir um certificado, você deve criar o modelo de certificado. Você deve selecionar **Key Storage Provider** ou **Legacy Cryptographic Service Provider**.

Para criar um modelo de certificado KSP, selecione **Windows Server 2008** ou posterior para a Autoridade de certificação na guia **Compatibilidade (Compatibility)** e selecione **Provedor de armazenamento de chaves (Key Storage Provider)** na guia **guia Criptografia (Cryptography)**.

Se você estiver usando um modelo de certificado KSP para emitir o certificado, para o CSP especificado no modelo de emissão do certificado, selecione **Microsoft Smart Card Key Storage Provider** ou um KSP de cartão inteligente de terceiros que ofereça suporte a RSA com SHA- 256 algoritmos. Se você estiver usando um modelo de certificado CSP herdado, selecione **Microsoft Base Smart Card Crypto Provider** ou um CSP de cartão inteligente de terceiros que ofereça suporte a RSA com algoritmos SHA-256.

Requisitos de inscrição do cartão inteligente

Para instalar certificados em um cartão inteligente, um administrador deve configurar um computador para atuar como uma estação de inscrição. Esse computador deve ter autoridade para emitir certificados de cartão inteligente para usuários e deve ser membro do domínio para o qual você está emitindo certificados.

Ao inscrever um cartão inteligente, você pode selecionar o tamanho da chave do certificado resultante. Para usar cartões inteligentes com áreas de trabalho locais, você deve selecionar um tamanho de chave de 1.024 bits ou 2.048 bits ao inscrever o cartão inteligente. Não há suporte para certificados com chaves de 512 bits.

O site do Microsoft TechNet inclui informações detalhadas sobre como planejar e implementar a autenticação de cartão inteligente para sistemas Windows.

Requisitos de software de aplicativo publicado e de área de trabalho remota

Um administrador do Horizon deve instalar drivers de aplicativo específicos do produto nas áreas de trabalho virtuais ou no host RDS.

Habilitando a caixa de texto User Name Hint em Horizon Client

Em alguns ambientes, os usuários de smart card podem usar um único certificado de smart card para autenticar várias contas de usuário. Os usuários inserem seus nomes de usuário na caixa de texto **Dica de nome de usuário (Username hint)** quando fazem login com um cartão inteligente.

Para que a caixa de texto **Sugestão de nome de usuário (Username hint)** apareça na caixa de diálogo de login Horizon Client, você deve ativar o recurso de dicas de nome de usuário de smart card no Servidor de Conexão. Para obter informações sobre como ativar o recurso de dicas de nome de usuário do cartão inteligente, consulte o documento *Administração Horizon*.

Se o seu ambiente usar um appliance do Unified Access Gateway para acesso externo seguro, você deverá configurar o appliance do Unified Access Gateway para oferecer suporte ao recurso de dicas de nome de usuário do cartão inteligente. O recurso de dicas de nome de usuário do cartão inteligente é compatível apenas com o Unified Access Gateway 2.7.2 e versões posteriores. Para obter informações sobre como ativar o recurso de dicas de nome de usuário do cartão inteligente em Unified Access Gateway, consulte o documento *Implantação e configuração do VMware Unified Access Gateway*.

Horizon Client continua a oferecer suporte a certificados de cartão inteligente de conta única, mesmo quando o recurso de dicas de nome de usuário do cartão inteligente está ativado.

Requisitos adicionais de autenticação de cartão inteligente

Além de atender aos requisitos de cartão inteligente para sistemas Horizon Client, outros componentes do Horizon devem atender a determinados requisitos de configuração para oferecer suporte a cartões inteligentes.

Servidor de conexão e hosts do servidor de segurança

Um administrador deve adicionar todas as cadeias de certificados de Autoridade de Certificação (CA) aplicáveis a todos os certificados de usuário confiável a um arquivo de armazenamento confiável do servidor no host do Servidor de Conexão ou, se um servidor de segurança for usado, no host do servidor de segurança. Essas cadeias de certificados incluem certificados raiz e, se uma autoridade de certificação intermediária emitir o certificado de cartão inteligente do usuário, também deverá incluir certificados intermediários.

Para obter informações sobre como configurar o Servidor de Conexão para oferecer suporte ao uso de smart card, consulte o documento *Administração Horizon*.

Unified Access Gateway dispositivos

Para obter informações sobre como configurar a autenticação de cartão inteligente em um appliance do Unified Access Gateway, consulte o documento *Implantação e configuração do VMware Unified Access Gateway*.

Active Directory

Para obter informações sobre tarefas que um administrador pode precisar executar em Active Directory para implementar a autenticação de cartão inteligente, consulte o documento *Administração Horizon*.

Requisitos de autenticação do certificado do dispositivo cliente

Com o recurso de autenticação de certificado do dispositivo cliente, você pode configurar a autenticação de certificado para dispositivos cliente. Unified Access Gateway autentica os dispositivos cliente. Os Serviços de Certificados da Microsoft, com o Active Directory, gerenciam a criação e a distribuição de certificados para os dispositivos cliente. Após a autenticação bem-sucedida do dispositivo, o usuário ainda deve realizar a autenticação do usuário.

Esse recurso tem os seguintes requisitos.

- Unified Access Gateway 2.6 ou posterior
- Horizon 7 versão 7.5 ou posterior
- Um certificado instalado no dispositivo cliente que Unified Access Gateway aceita

Para obter informações sobre como configurar o Unified Access Gateway, consulte a documentação do Unified Access Gateway.

Antes de emitir um certificado, você deve criar o modelo de certificado. Você deve selecionar **Key Storage Provider** ou **Legacy Cryptographic Service Provider**.

Para criar um modelo de certificado KSP, selecione **Windows Server 2008** ou posterior para a Autoridade de certificação na guia **Compatibilidade (Compatibility)** e selecione **Provedor de armazenamento de chaves (Key Storage Provider)** na guia **guia Criptografia (Cryptography)**.

Se você estiver usando um modelo de certificado KSP para emitir o certificado, selecione **Microsoft Software Key Storage Provider** ou um KSP de cartão inteligente de terceiros que ofereça suporte a RSA com algoritmos SHA-256. Se você estiver usando um modelo de certificado CSP herdado, selecione **Microsoft Enhanced RSA and AES Cryptographic Provider**, que oferece suporte a RSA com algoritmos SHA-256 e TLS1.2.

Para obter uma lista de provedores de serviços de criptografia CryptoAPI, vá para https://docs.microsoft.com/en-us/windows/win32/seccertenroll/cryptoapi-cryptographic-service-providers.

Requisitos de integração do OPSWAT

Em algumas empresas, um administrador pode integrar o Unified Access Gateway ao aplicativo OPSWAT MetaAccess de terceiros. Essa integração, que normalmente é usada em dispositivos não gerenciados em ambientes corporativos BYOD (traga seu próprio dispositivo), permite que as organizações definam políticas de aceitação de dispositivos para Horizon Client dispositivos.

Por exemplo, um administrador pode definir uma política de aceitação de dispositivo que exija que os dispositivos cliente sejam protegidos por senha ou tenham uma versão mínima do sistema operacional. Os dispositivos cliente que estão em conformidade com a política de aceitação do dispositivo podem acessar áreas de trabalho remotas e aplicativos publicados por meio de Unified Access Gateway. Unified Access Gateway nega o acesso a recursos remotos de dispositivos cliente que não estão em conformidade com a política de aceitação do dispositivo.

Para obter mais informações, consulte o documento *Implantando e configurando o VMware Unified Access Gateway*.

Requisitos do sistema para áudio e vídeo em tempo real

O Áudio-Vídeo em Tempo Real funciona com dispositivos de webcam padrão, áudio USB e áudio analógico. O recurso também funciona com aplicativos de conferência padrão. Para oferecer suporte a áudio e vídeo em tempo real, sua implantação do Horizon deve atender a determinados requisitos de software e hardware.

Áreas de trabalho virtuais

Para usar mais de uma webcam ou microfone em uma área de trabalho virtual, o Horizon Agent 7.10 ou posterior deve estar instalado.

Ao usar o Microsoft Teams com áudio e vídeo em tempo real, as áreas de trabalho virtuais devem ter no mínimo 4 vCPUs e 4 GB de RAM.

Horizon Client computador ou dispositivo de acesso para cliente

- O Áudio-Vídeo em Tempo Real é compatível com todos os sistemas operacionais que executam Horizon Client para Windows. Para obter informações, consulte Requisitos de hardware e software para sistemas cliente Windows.
- Os drivers da webcam e do dispositivo de áudio devem estar instalados, e a webcam e o dispositivo de áudio devem estar operáveis no computador cliente. Você não precisa instalar os drivers de dispositivo na máquina em que o agente está instalado.

Exibir protocolos

- PCoIP
- VMware Blast

Requisitos do sistema para redirecionamento do scanner

Os usuários finais podem verificar informações em suas áreas de trabalho remotas e aplicativos com scanners conectados aos seus sistemas clientes locais. Para usar esse recurso, as áreas de trabalho remotas e os computadores cliente devem atender a determinados requisitos do sistema.

Áreas de trabalho remotas

As áreas de trabalho remotas devem ter o Horizon Agent instalado com a opção de configuração Redirecionamento do scanner selecionada nas máquinas virtuais pai ou modelo ou hosts RDS. Nos sistemas operacionais Windows desktop e Windows Server guest, a opção de configuração Horizon Agent Redirecionamento do scanner está desmarcada por padrão.

Para obter informações sobre quais sistemas operacionais convidados têm suporte para áreas de trabalho virtuais e hosts RDS, e para obter informações sobre como configurar o redirecionamento do scanner em áreas de trabalho remotas e aplicativos publicados, consulte "Configurar o redirecionamento do scanner" no documento *Configurando recursos de área de trabalho remota no Horizon*.

Horizon Client computador ou dispositivo de acesso para cliente

O redirecionamento do scanner é compatível com o Windows 10. Os drivers de dispositivo do scanner devem ser instalados, e o scanner deve ser operável, no computador cliente. Você não precisa instalar os drivers de dispositivo do scanner no sistema operacional da área de trabalho remota em que o agente está instalado.

Padrão do dispositivo de digitalização

TWAIN ou WIA

Exibir protocolos

- PCoIP
- VMware Blast

O redirecionamento do scanner não é compatível com sessões de área de trabalho RDP.

Requisitos do sistema para redirecionamento de porta serial

Com o recurso de redirecionamento de porta serial, os usuários finais podem redirecionar portas seriais (COM) conectadas localmente, como portas RS232 integradas ou adaptadores USB para Serial, para suas áreas de trabalho remotas e aplicativos publicados. Para oferecer suporte ao redirecionamento de porta serial, sua implantação do VMware Horizon deve atender a determinados requisitos de software e hardware.

Áreas de trabalho virtuais

Horizon Agent deve ser instalado com a opção de configuração Redirecionamento de Porta Serial selecionada. Essa opção de configuração está desmarcada por padrão.

Os seguintes sistemas operacionais têm suporte em áreas de trabalho virtuais.

- 64 bits Windows 7
- 64 bits Windows 8.x
- 64 bits Windows 10
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Observação Horizon Agent 2006 e versões posteriores não são compatíveis com Windows 7, Windows 8.x, Window Server 2008 R2 e Windows Server 2012 R2.

Os drivers de dispositivo de porta serial não precisam ser instalados na área de trabalho virtual.

Áreas de trabalho publicadas e aplicativos publicados

Os hosts RDS devem ter o Horizon Agent 7.6 ou posterior instalado com a opção de configuração Redirecionamento de porta serial selecionada. Essa opção de configuração está desmarcada por padrão.

Os seguintes sistemas operacionais são compatíveis com áreas de trabalho e aplicativos publicados publicados.

- Windows Server 2008 R2

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Observação Horizon Agent 2006 e versões posteriores não são compatíveis com Windows Server 2008 R2 e Windows Server 2012 R2.

Os drivers de dispositivo de porta serial não precisam ser instalados no host RDS.

O redirecionamento de porta serial está disponível com áreas de trabalho completas e não é compatível com aplicativos publicados em hosts RDS.

Horizon Client computador ou dispositivo de acesso para cliente

O redirecionamento de porta serial é compatível com Windows 10 sistemas cliente. Todos os drivers de dispositivo de porta serial necessários devem ser instalados e a porta serial deve ser operável.

Exibir protocolos

- PCoIP
- VMware Blast

O redirecionamento de porta serial não é compatível com sessões de área de trabalho RDP.

Para obter informações sobre como configurar o redirecionamento de porta serial, consulte "Configurando o redirecionamento de porta serial" no documento *Configurando recursos de área de trabalho remota no Horizon*.

Requisitos para usar o redirecionamento de conteúdo de URL

Com o recurso Redirecionamento de Conteúdo de URL, o conteúdo de URL pode ser redirecionado da máquina cliente para uma área de trabalho remota ou aplicativo publicado (redirecionamento de cliente para agente) ou de uma área de trabalho remota ou aplicativo publicado para a máquina cliente redirecionamento).

Por exemplo, um usuário final pode clicar em um link no aplicativo nativo do Microsoft Word no cliente e o link é aberto no aplicativo remoto do Internet Explorer, ou um usuário final pode clicar em um link no aplicativo remoto do Internet Explorer e o link é aberto em um navegador nativo na máquina cliente. Qualquer número de protocolos pode ser configurado para redirecionamento, incluindo HTTP, mailto e callto.

Um administrador do Horizon também deve definir configurações que especifiquem como o Horizon Client redireciona o conteúdo da URL do cliente para uma área de trabalho remota ou um aplicativo publicado, ou como o Horizon Agent redireciona o conteúdo da URL de uma área de trabalho remota ou um aplicativo publicado para o cliente.

Para obter informações completas, consulte o tópico "Configurando o redirecionamento de conteúdo de URL" no documento *Configurando recursos de área de trabalho remota no Horizon*.

Requisitos do sistema para redirecionamento de multimídia HTML5

Horizon Agent e Horizon Client, e as áreas de trabalho remotas e os sistemas cliente nos quais você instala o agente e o software cliente, devem atender a determinados requisitos para oferecer suporte ao recurso Redirecionamento de Multimídia HTML5.

Com o redirecionamento multimídia HTML5, se um usuário final usar o navegador Google Chrome ou Microsoft Edge em uma área de trabalho remota, o conteúdo multimídia HTML5 será enviado para o sistema do cliente. O sistema do cliente reproduz o conteúdo multimídia, o que reduz a carga no host ESXi, e o usuário final tem uma melhor experiência de áudio e vídeo.

Área de trabalho remota

- Horizon Agent deve ser instalado na área de trabalho virtual ou no host RDS para áreas de trabalho publicadas com a opção de configuração personalizada HTML5 Multimedia Redirection selecionada. A partir do Horizon Agent 7.10, a opção de configuração personalizada HTML5 Multimedia Redirection é removida e o HTML5 Multimedia Redirection é instalado por padrão. Para obter mais informações, consulte os tópicos sobre como instalar o Horizon Agent nos documentos *Configurando áreas de trabalho virtuais no Horizon* e *Configurando áreas de trabalho e aplicativos publicados no Horizon*.
- As configurações de política de grupo do redirecionamento multimídia HTML5 devem ser definidas no servidor Active Directory. Consulte os tópicos sobre como configurar o redirecionamento multimídia HTML5 no documento *Configurando recursos de área de trabalho remota no Horizon*.
- O navegador Google Chrome, Microsoft Edge ou Microsoft Edge (Chromium) deve estar instalado.
- A extensão de redirecionamento de multimídia HTML5 VMware Horizon deve ser instalada no navegador. Consulte os tópicos sobre como configurar o redirecionamento multimídia HTML5 no documento *Configurando recursos de área de trabalho remota no Horizon*.

Sistema do cliente

- A opção de configuração personalizada Suporte para redirecionamento de multimídia HTML5 e redirecionamento de navegador deve ser selecionada quando você instalar o Horizon Client. Essa opção é selecionada por padrão.

Protocolo de exibição para a sessão remota

- PCoIP

- VMware Blast

Porta TCP

O redirecionamento de multimídia HTML5 usa a porta 9427.

Requisitos do sistema para redirecionamento de navegador

As áreas de trabalho remotas e os sistemas cliente nos quais você instala o agente e o software cliente devem atender a determinados requisitos para oferecer suporte ao recurso Redirecionamento do navegador.

Com o redirecionamento do navegador, quando um usuário final abre um site no navegador Chrome em uma área de trabalho remota, a página da Web é renderizada no sistema do cliente, em vez do sistema do agente, e é exibida na janela de visualização do navegador remoto. A viewport é a parte da janela do navegador que contém o conteúdo da página da Web.

Áreas de trabalho remotas

- Horizon Agent A versão 7.10 ou posterior deve ser instalada na área de trabalho virtual ou no host RDS para áreas de trabalho publicadas. Consulte os tópicos sobre como instalar o Horizon Agent nos documentos *Configurando áreas de trabalho virtuais no Horizon* e *Configurando áreas de trabalho e aplicativos publicados no Horizon*.
- As configurações de política de grupo de redirecionamento VMware Browser devem ser definidas no servidor Active Directory. Consulte os tópicos sobre como configurar o redirecionamento do navegador no documento *Configurando recursos de área de trabalho remota no Horizon*.
- O navegador Chrome ou o navegador Microsoft Edge (Chromium) deve estar instalado.
- A extensão de redirecionamento do navegador VMware Horizon deve ser instalada no navegador. Consulte os tópicos sobre como configurar o redirecionamento do navegador no documento *Configurando recursos de área de trabalho remota no Horizon*.

Protocolo de exibição para a sessão remota

- PCoIP
- VMware Blast

Requisitos do sistema para redirecionamento de multimídia (MMR)

Com o redirecionamento de multimídia (MMR), o fluxo de multimídia é decodificado no sistema do cliente. O sistema do cliente reproduz o conteúdo de mídia para que a carga no host ESXi seja reduzida.

Áreas de trabalho remotas

Para obter informações sobre os requisitos do sistema operacional e outros requisitos de software e definições de configuração, consulte os tópicos sobre Windows Media Redirecionamento de multimídia no documento *Configurando recursos de área de trabalho remota no Horizon*.

Horizon Client computador ou dispositivo de acesso para cliente

Windows 10

Formatos de mídia compatíveis

Formatos de mídia compatíveis com Windows Media Player, por exemplo: M4V; MOV; MP4; MPEG-4 Parte 2; WMV 7, 8 e 9; WMA; AVI; ACE; MP3.

MP3 não é compatível com o uso de MMS e RTSP.

Observação O conteúdo protegido por DRM não é redirecionado por meio do Windows Media MMR.

Configurar os serviços E911 para Microsoft Teams

Para permitir os serviços E911 para o recurso Otimização de Mídia para Microsoft Teams, você deve habilitar manualmente os serviços de localização Windows para Horizon Client. Esses serviços fornecem informações de geolocalização do cliente para Microsoft Teams em execução em uma área de trabalho remota para roteamento baseado em localização durante chamadas de emergência.

Observação Os serviços E911 exigem o Horizon Agent 2111 ou posterior.

Para ativar os serviços de localização para Horizon Client em Windows, siga as etapas abaixo.

1. Na caixa de diálogo Configurações, navegue até **Privacidade e segurança (Privacy & Security)**.
2. Em Permissões do aplicativo, clique na guia **Local (Location)**.
3. Defina **Serviços de localização (Location services)** como **Ativado (On)**.
4. Defina **Permitir que os aplicativos acessem sua localização (Let apps access your location)** como **Ativado (On)**.

Requisitos do sistema para redirecionamento de geolocalização

Horizon Agent e Horizon Client, bem como a área de trabalho virtual ou o host RDS e a máquina cliente nos quais você instala o agente e o software cliente, devem atender a determinados requisitos para oferecer suporte ao recurso Redirecionamento de geolocalização.

A origem das informações de geolocalização é o sistema operacional do dispositivo local usando Horizon Client. Essas informações podem ser redirecionadas pelo cliente para áreas de trabalho remotas ou aplicativos publicados. As definições de configuração do sistema host e do agente podem restringir a disponibilidade do recurso.

Com o redirecionamento de geolocalização, as informações de geolocalização são enviadas do sistema do cliente para a área de trabalho remota ou o aplicativo publicado.

Área de trabalho virtual ou host RDS

- A configuração do Windows **Serviço de localização (Location service)** deve estar **Ativado (On)** em **Configurações (Settings) > Privacidade (Privacy) > Local (Location)** .
- O recurso Redirecionamento de geolocalização é compatível com os seguintes aplicativos de área de trabalho remota.

Aplicativo	Plataforma
Google Chrome (versão mais recente)	Todos os desktops virtuais ou hosts RDS
Internet Explorer 11	Todos os desktops virtuais ou hosts RDS
Microsoft Edge (Cromo)	Todos os desktops virtuais ou hosts RDS
Microsoft Edge, Mapas, Meteorologia e outros aplicativos Win32 e UWP	Windows 10

- A configuração de permissão **Local (Location)**, se houver, deve ser ativada individualmente em cada navegador compatível.
- O Horizon Agent 7.6 ou posterior deve ser instalado com a opção de configuração personalizada Redirecionamento de geolocalização selecionada. Essa opção não está selecionada por padrão. Consulte os tópicos sobre como instalar o Horizon Agent nos documentos *Configurando áreas de trabalho virtuais no Horizon* e *Configurando áreas de trabalho e aplicativos publicados no Horizon*.
- As configurações de política de grupo VMware Redirecionamento de geolocalização devem ser definidas no servidor Active Directory. Consulte os tópicos sobre como configurar o redirecionamento de geolocalização no documento *Configurando recursos de área de trabalho remota no Horizon*.
- Para o Internet Explorer 11, o plug-in do IE de geolocalização VMware Horizon deve estar ativado para hosts RDS. Você não precisa ativar o plug-in do IE de redirecionamento de geolocalização do VMware Horizon para Windows 10 áreas de trabalho virtuais. O Internet Explorer é compatível com Windows 10 áreas de trabalho virtuais com o driver de redirecionamento de geolocalização VMware. Consulte os tópicos sobre como configurar o redirecionamento de geolocalização no documento *Configurando recursos de área de trabalho remota no Horizon*.
- Para o Chrome e o Microsoft Edge (Chromium), a extensão Chrome de redirecionamento de geolocalização do VMware Horizon deve ser instalada. Consulte os tópicos sobre como configurar o redirecionamento de geolocalização no documento *Configurando recursos de área de trabalho remota no Horizon*.

Sistema do cliente

- Para compartilhar as informações de localização do sistema do cliente, você deve definir as configurações de **Geolocalização (Geolocation)** em Horizon Client.
- Para sistemas cliente de Windows 10, a configuração do Windows **Serviço de localização (Location service)** deve estar **Ativado (On)** em **Configurações (Settings) > Privacidade (Privacy) > }Localização (Location)** para que o Horizon acesse sua localização.

Protocolo de exibição para a sessão remota

PCoIP ou VMware Blast

Requisitos do sistema para o recurso de colaboração de sessão

Com o recurso Colaboração de Sessão, os usuários podem convidar outros usuários para ingressar em uma sessão de área de trabalho remota existente. Para oferecer suporte ao recurso de Colaboração de Sessão, sua implantação do Horizon deve atender a determinados requisitos.

Colaboradores da sessão

Para ingressar em uma sessão colaborativa, um usuário deve ter o Horizon Client para Windows, Mac ou Linux instalado no sistema cliente ou deve usar HTML Access.

Windows áreas de trabalho remotas

O recurso de Colaboração de Sessão deve ser habilitado no pool de áreas de trabalho ou no nível do farm. Para obter informações sobre como habilitar o recurso Colaboração de Sessão para pools de áreas de trabalho, consulte o documento *Configurando áreas de trabalho virtuais no Horizon*. Para obter informações sobre como habilitar o recurso Colaboração de Sessão para um farm, consulte o documento *Configurando áreas de trabalho e aplicativos publicados no Horizon*.

Você pode usar as configurações de política de grupo Horizon Agent para configurar o recurso Colaboração de Sessão. Para obter informações, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.

Áreas de trabalho remotas do Linux

Para obter os requisitos da área de trabalho remota do Linux, consulte o documento *Configuração de desktops Linux no Horizon*.

Servidor de conexão

O recurso de Colaboração de Sessão requer que a instância do Servidor de Conexão use uma licença Enterprise.

Exibir protocolos

VMware Blast

O recurso de Colaboração de Sessão não oferece suporte a sessões de aplicativo publicadas.

Requisitos do sistema para Skype for Business

Um usuário final pode executar o Skype for Business dentro de uma área de trabalho virtual sem afetar negativamente a infraestrutura virtual e sobrecarregar a rede. Durante Skype chamadas de áudio e vídeo, todo o processamento de mídia ocorre na máquina cliente, e não na área de trabalho virtual.

Para usar esse recurso, você deve instalar o recurso Pacote de Virtualização para Skype for Business na máquina cliente quando o Horizon Client para Windows estiver instalado. Para obter informações, consulte Capítulo 2 Instalando e atualizando Horizon Client para Windows.

Um administrador do Horizon também deve instalar o recurso VMware Virtualization Pack para Skype for Business na área de trabalho virtual quando o Horizon Agent estiver instalado. Para obter informações sobre como instalar o Horizon Agent, consulte o documento *Configurando áreas de trabalho virtuais no Horizon*.

Para obter os requisitos completos, consulte "Configurar Skype for Business" no documento *Configurando recursos de área de trabalho remota no Horizon*.

Sistemas operacionais de desktop compatíveis

Um administrador do Horizon cria máquinas virtuais que têm um sistema operacional convidado e instala o software do agente no sistema operacional convidado. Os usuários finais podem fazer login nessas máquinas virtuais a partir de um dispositivo cliente.

Para obter uma lista dos sistemas operacionais guest Windows compatíveis, consulte o documento *Instalação Horizon*.

Alguns sistemas operacionais guest Linux também são compatíveis. Para obter informações sobre os requisitos do sistema, a configuração de máquinas virtuais Linux e uma lista de recursos compatíveis, consulte o documento *Configuração de desktops Linux no Horizon*.

Instalando e atualizando Horizon Client para Windows

2

Você pode obter o instalador do Horizon Client baseado em Windows no site do VMware ou em uma página de acesso do Web fornecida pelo Connection Server. Você pode definir várias opções de inicialização para usuários finais após a instalação do Horizon Client. Você pode atualizar o Horizon Client online.

Leia os seguintes tópicos:

Ativando o modo FIPS no Windows sistema operacional do cliente

Se você planeja instalar o Horizon Client com criptografia compatível com o Federal Information Processing Standard (FIPS), deverá habilitar o modo FIPS no sistema operacional do cliente antes de executar o instalador do Horizon Client.

Quando o modo FIPS está ativado no sistema operacional do cliente, os aplicativos usam apenas algoritmos criptográficos compatíveis com FIPS-140 e com os modos de operação aprovados pelo FIPS. Você pode habilitar o modo FIPS habilitando uma configuração de segurança específica, na Política de Segurança Local ou como parte da Política de Grupo, ou editando uma chave do Registro Windows.

Para obter mais informações sobre a conformidade com o FIPS, consulte o documento *Instalação Horizon*.

Definindo a propriedade de configuração FIPS

Para habilitar o modo FIPS no sistema operacional cliente, você pode usar uma configuração de política de grupo Windows ou uma configuração de Registro Windows para o computador cliente.

- Para usar a configuração de política de grupo, abra o Editor de Política de Grupo, navegue até `Configuração do Computador\Windows\} Configurações\Configurações de Segurança\Políticas Locais\Opções de Segurança` e ative a opção **Criptografia do sistema: usar compatível com FIPS algoritmos para criptografia, hashing e configuração de assinatura (System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing)**.
- Para usar o Registro Windows, vá para `HKLM\System\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy\Enabled` e defina **Enabled** como 1.

Para obter mais informações sobre o modo FIPS, vá para https://support.microsoft.com/en-us/kb/811833.

Importante Se você não ativar o modo FIPS antes de executar o instalador Horizon Client, a opção do instalador para usar a criptografia compatível com FIPS não aparecerá durante uma instalação personalizada. A criptografia compatível com FIPS não é habilitada durante uma instalação típica. Se você instalar o Horizon Client sem a opção de criptografia compatível com FIPS e depois decidir usar a opção, deverá desinstalar o cliente, ativar o modo FIPS no sistema operacional do cliente e executar o instalador do Horizon Client novamente.

Ativando a seleção automática de protocolo de Internet

Ao realizar uma instalação personalizada do Horizon Client, você pode ativar a seleção automática do protocolo da Internet. Com a seleção automática, o Horizon Client verifica a rede atual e se conecta por IPv4 ou IPv6 automaticamente.

Quando a seleção automática está ativada, os seguintes recursos são compatíveis com o Unified Access Gateway 3.3 e posterior com o protocolo de exibição VMware Blast.

- Faça login como usuário atual
- Saída de áudio
- Coleta de dados do Programa de Aperfeiçoamento da Experiência do Usuário
- Impressão virtual
- VMware Integrated Printing (requer Horizon 7 versão 7.7 ou posterior)
- Redirecionamento de multimídia HTML5
- VMware vídeo
- Redirecionamento USB

- Áudio e vídeo em tempo real (RTAV)

Instalar Horizon Client para Windows

Você pode executar um arquivo de instalador baseado em Windows para instalar todos os componentes Horizon Client.

Este procedimento descreve como instalar o Horizon Client usando um assistente de instalação interativo. Para instalar o Horizon Client a partir da linha de comando, consulte Instalar o Horizon Client a partir da linha de comando. Para instalar o recurso Redirecionamento de Conteúdo de URL, você deve executar o instalador a partir da linha de comando.

Observação Você pode instalar o Horizon Client na máquina virtual de área de trabalho remota. As empresas podem usar essa estratégia de instalação quando seus usuários finais acessarem aplicativos publicados de Windows dispositivos thin client.

Pré-requisitos

- Verifique se o sistema do cliente usa um sistema operacional compatível. Consulte Requisitos de hardware e software para sistemas cliente Windows.
- Verifique se você tem a URL de uma página de download que contém o instalador Horizon Client. Essa URL pode ser a página VMware Downloads em http://www.vmware.com/go/viewclients ou pode ser a URL de uma instância do Servidor de Conexão.
- Verifique se você pode fazer login como administrador no sistema do cliente.
- Verifique se os controladores de domínio têm os patches mais recentes, espaço livre em disco suficiente e se podem se comunicar entre si.
- Se você planeja instalar o Horizon Client com criptografia compatível com FIPS, ative o modo FIPS no sistema operacional do cliente. Consulte Ativando o modo FIPS no Windows sistema operacional do cliente.
- Se você planeja selecionar o protocolo IPv6 ou a seleção automática de protocolo da Internet, consulte o documento *Instalação Horizon* para obter informações sobre os recursos que não estão disponíveis em um ambiente IPv6.
- Se você planeja ativar a seleção automática de protocolo de Internet, consulte Ativando a seleção automática de protocolo de Internet para obter informações sobre os recursos compatíveis.
- Se você planeja instalar o componente **Redirecionamento USB (USB Redirection)**, realize as seguintes tarefas:
  - Determine se a pessoa que usa o dispositivo cliente tem permissão para acessar dispositivos USB conectados localmente a partir de uma área de trabalho remota. Se o acesso não for permitido, não instale o componente **Redirecionamento USB (USB Redirection)** ou instale o componente e desative-o usando uma configuração de

política de grupo. Se você usar a política de grupo para desativar o redirecionamento de USB, não precisará reinstalar o Horizon Client se posteriormente decidir ativar o redirecionamento de USB para um cliente. Para obter mais informações, consulte Usando configurações de política de grupo para configurar Horizon Client.

- Verifique se o recurso Atualização Automática Windows não está desativado no computador cliente.

- Decida se deseja usar o recurso que permite que os usuários finais façam login em Horizon Client e na área de trabalho remota como o usuário conectado no momento. As informações de credenciais que o usuário digitou ao fazer login no sistema do cliente são passadas para a instância do Servidor de Conexão e, por fim, para a área de trabalho remota. Alguns sistemas operacionais cliente não oferecem suporte a esse recurso.
- Se você não quiser que os usuários finais forneçam o nome de domínio totalmente qualificado (FQDN) da instância do Servidor de Conexão, determine o FQDN para que você possa fornecê-lo durante a instalação.

Procedimentos

1. Faça login no sistema do cliente como administrador.
2. Navegue até a página VMware Downloads em http://www.vmware.com/go/viewclients.
3. Faça download do arquivo do instalador, por exemplo, `VMware-Horizon-Client-`*`YYMM`*`-`*`y.y.y`*`-`*`xxxxxx`*`.exe`.

   YYMM é o número da versão de marketing, *y.y.y* é o número da versão interna e *xxxxxx* é o número da compilação.
4. Clique duas vezes no arquivo do instalador para iniciar a instalação.

5 Selecione um tipo de instalação e siga os prompts.

Opção	Ação
Instalação típica	Clique em **Agree & Install**. O instalador configura o cliente para usar o protocolo de Internet IPv4 e instala os seguintes recursos. ■ Redirecionamento USB ■ Faça login como usuário atual, incluindo a exibição da opção de menu **Fazer login como usuário atual (Log in as current user)**. ■ Pacote de virtualização para Skype for Business ■ Suporte para redirecionamento de multimídia HTML5 e redirecionamento de navegador ■ Otimização de mídia para Microsoft Teams
Instalação personalizada	Clique em **Personalizar instalação (Customize Installation)** e selecione os recursos a serem instalados. Você deve selecionar essa opção para instalar os seguintes recursos. ■ Especifique um local de instalação não padrão. ■ Use o protocolo de Internet IPv6 ou a seleção automática. Se você ativar a seleção automática, o Horizon Client verificará a rede atual e se conectará por IPv4 ou IPv6 automaticamente. ■ Defina o comportamento de login padrão como **Fazer login como usuário atual (Log in as current user)**. ■ Especifique uma instância padrão do Servidor de Conexão. ■ Habilite a criptografia compatível com FIPS. As opções de instalação personalizada de criptografia compatível com FIPS estarão disponíveis no instalador somente se o modo FIPS estiver ativado no sistema operacional do cliente.

Resultados

Alguns recursos exigem que você reinicie o sistema do cliente.

O instalador instala os serviços do Windows, incluindo o VMware Horizon Client (`horizon_client_service`) e o VMware Serviço de Arbitragem USB (`VMUSBArbService`).

Próximo passo

Inicie o Horizon Client e verifique se você pode fazer login na área de trabalho remota ou no aplicativo publicado correto. Consulte Conectar-se a uma Área de Trabalho Remota ou Aplicativo Publicado.

Instalar o Horizon Client a partir da linha de comando

Você pode instalar o Horizon Client a partir da linha de comando digitando o nome do arquivo do instalador e especificando os comandos e as propriedades de instalação. Você pode instalar o Horizon Client silenciosamente a partir da linha de comando.

A tabela a seguir descreve os comandos de instalação do Horizon Client.

Tabela 2-1. Horizon Client Comandos de instalação

Comando	Descrição
`/?` ou `/help`	Lista os comandos e as propriedades de instalação do Horizon Client.
`/silent`	Instala o Horizon Client silenciosamente. Você não precisa responder aos prompts do assistente.
`/install`	Instala o Horizon Client interativamente. Você deve responder aos prompts do assistente.
`/uninstall`	Desinstala Horizon Client.
`/repair`	Reparos Horizon Client.
`/norestart`	Suprime todas as reinicializações e solicitações de reinicialização durante o processo de instalação.
`/x /extract`	Extrai os pacotes do instalador para o diretório `%TEMP%`.
`/l` ou `/log`	Especifica uma pasta e um padrão de nomenclatura para arquivos de log de instalação. Por exemplo, se você especificar o seguinte comando, o instalador do Horizon Client criará arquivos de log com o prefixo `Test` na pasta chamada `C:\Temp`. `/log "C:\Temp\Test"`

A tabela a seguir descreve as propriedades de instalação do Horizon Client.

Tabela 2-2. Horizon Client Propriedades de instalação

Propriedade	Descrição	Padrão
`INSTALLDIR`	Caminho e pasta em que o Horizon Client está instalado. Por exemplo: `INSTALLDIR=""D:\abc\my folder""` Os conjuntos de aspas duplas que incluem o caminho permitem que o instalador interprete o espaço como uma parte válida do caminho.	`%ProgramFiles%VMware\VMware Horizon View Client\}`
`VDM_IP_PROTOCOL_USAGE`	Versão do IP (Protocolo da Internet) que os componentes do Horizon Client usam para comunicação. Os valores válidos são os seguintes: ■ IPv4 ■ IPv6 ■ Duplo Se você especificar Dual, o Horizon Client verificará a rede atual e se conectará por IPv4 ou IPv6 automaticamente.	IPv4

Tabela 2-2. Horizon Client Propriedades de instalação (continuação)

Propriedade	Descrição	Padrão
VDM_FIPS_ENABLED	Determina se o Horizon Client deve ser instalado com criptografia compatível com FIPS. Um valor de 1 instala Horizon Client com criptografia compatível com FIPS. Um valor de 0 instala o Horizon Client sem criptografia compatível com FIPs. **Observação** Antes de definir essa propriedade como 1, você deve ativar o modo FIPS no sistema operacional do cliente Windows. Consulte Ativando o modo FIPS no Windows sistema operacional do cliente.	0
VDM_SERVER	Nome de domínio totalmente qualificado (FQDN) da instância do Servidor de Conexão à qual Horizon Client os usuários se conectam por padrão. Por exemplo: `VDM_Server=cs1.companydomain.com` Se você configurar essa propriedade, os usuários do Horizon Client não precisarão fornecer esse FQDN.	Nenhum
LOGINASCURRENTUSER_DISPLAY	Determina se **Fazer login como usuário atual (Log in as current user)** aparece no menu **Opções (Options)** na barra de menus Horizon Client. Os valores válidos são 1 (ativado) ou 0 (desativado).	1
LOGINASCURRENTUSER_DEFAULT	Determina se **Fazer login como usuário atual (Log in as current user)** está selecionado por padrão no menu **Opções (Options)** na barra de menus Horizon Client. Os valores válidos são 1 (ativado) e 0 (desativado). Quando fazer login como usuário atual é o comportamento de login padrão, as informações de identidade e credencial que os usuários fornecem quando fazem login no sistema do cliente são passadas para a instância do Servidor de Conexão e, finalmente, para a área de trabalho remota. Quando efetuar login como usuário atual não for o comportamento de login padrão, os usuários deverão fornecer informações de identidade e credenciais várias vezes antes de poderem acessar uma área de trabalho remota ou um aplicativo. **Observação** Se você alterar esse valor para a interface do usuário, Horizon Client ignorará a configuração de política de grupo padrão relacionada.	0

Tabela 2-2. Horizon Client Propriedades de instalação (continuação)

Propriedade	Descrição	Padrão
ADDLOCAL	Especifica os recursos a serem instalados. Os valores válidos são os seguintes: ■ ALL - Instala todos os recursos disponíveis, exceto o redirecionamento de conteúdo de URL. ■ TSSO - Instala o recurso Fazer login como usuário atual. ■ USB - Instala o recurso Redirecionamento de USB. Para especificar recursos individuais, digite uma lista de nomes de recursos separados por vírgula. Não use espaços entre nomes. Por exemplo, para instalar o Horizon Client com o recurso Redirecionamento de USB, mas sem o recurso Fazer login como usuário atual, digite o seguinte comando: VMware-Horizon-Client-*y.y.y*-*xxxxxx*.exe ADDLOCAL=USB	Nenhum
INSTALL_SFB	Determina se o recurso Pacote de Virtualização do VMware para Skype for Business está instalado. Um valor de 1 instala o recurso. Um valor de 0 não instala o recurso.	1
INSTALL_HTML5MMR	Determina se o recurso Suporte para redirecionamento de multimídia e redirecionamento de navegador HTML5 está instalado. Um valor de 1 instala o recurso. Um valor de 0 não instala o recurso.	1
REMOVER	Especifica os recursos que não devem ser instalados. Os valores válidos são os seguintes: ■ Scanner - Não instala o recurso de redirecionamento do scanner. ■ FolderRedirection - Não instala o recurso de redirecionamento de pasta. ■ SerialPort - Não instala o recurso de redirecionamento de porta serial. Para especificar vários recursos, digite uma lista de nomes de recursos separados por vírgula. Não use espaços entre nomes. Por exemplo, o seguinte comando não instala o recurso de redirecionamento do scanner: VMware-Horizon-Client-*y.y.y*-*xxxxxx*.exe REMOVE=Scanner	Nenhum

Tabela 2-2. Horizon Client Propriedades de instalação (continuação)

Propriedade	Descrição	Padrão
DESKTOP_SHORTCUT	Determina se um atalho na área de trabalho deve ser criado para Horizon Client. Um valor de 0 não cria um atalho na área de trabalho. Um valor de 1 cria um atalho na área de trabalho.	1
STARTMENU_SHORTCUT	Determina se um atalho do menu Iniciar para Horizon Client deve ser criado. Um valor de 0 não cria um atalho do menu Iniciar. Um valor de 1 cria um atalho do menu Iniciar.	1
URL_FILTERING_ENABLED	Determina se o recurso Redirecionamento de Conteúdo de URL está instalado. Um valor de 1 instala o recurso. Um valor de 0 não instala o recurso. Quando você define essa propriedade como 1 em uma instalação interativa, a caixa de seleção **Redirecionamento de Conteúdo de URL (URL Content Redirection)** aparece em Recursos adicionais na caixa de diálogo de instalação personalizada e é selecionada por padrão. A caixa de seleção não aparece a menos que você defina essa propriedade como 1. **Observação** A propriedade ADDLOCAL=ALL não inclui o recurso Redirecionamento de Conteúdo de URL.	0
AUTO_UPDATE_ENABLED	Determina se o recurso de atualização online está ativado. Um valor de 1 ativa o recurso. Um valor de 0 desativa o recurso. Para obter mais informações, consulte Atualização do Horizon Client on-line.	1
INSTALL_TEAMS_REDIRECTION	Determina se o recurso Otimização de Mídia para Microsoft Teams está ativado. Um valor de 1 ativa o recurso. Um valor de 0 desativa o recurso. Para obter mais informações sobre esse recurso, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.	1

Pré-requisitos

- Verifique se o sistema do cliente usa um sistema operacional compatível. Consulte Requisitos de hardware e software para sistemas cliente Windows.
- Verifique se você pode fazer login como administrador no sistema do cliente.
- Verifique se os controladores de domínio têm os patches mais recentes, espaço livre em disco suficiente e se podem se comunicar entre si.

- Se você planeja instalar o Horizon Client com criptografia compatível com FIPS, ative o modo FIPS no sistema operacional do cliente. Consulte Ativando o modo FIPS no Windows sistema operacional do cliente.
- Decida se deseja usar o recurso que permite que os usuários finais façam login em Horizon Client e na área de trabalho remota como o usuário conectado no momento. As informações de credenciais que o usuário digitou ao fazer login no sistema do cliente são passadas para a instância do Servidor de Conexão e, por fim, para a área de trabalho remota. Alguns sistemas operacionais cliente não oferecem suporte a esse recurso.
- Familiarize-se com os comandos de instalação do Horizon Client.
- Familiarize-se com as propriedades de instalação do Horizon Client.
- Determine se os usuários finais devem acessar dispositivos USB conectados localmente a partir de suas áreas de trabalho remotas. Caso contrário, defina a propriedade de instalação `ADDLOCAL` como a lista de recursos e omita o recurso USB.
- Se você não quiser que os usuários finais forneçam o nome de domínio totalmente qualificado (FQDN) da instância do Servidor de Conexão, determine o FQDN para que você possa fornecê-lo durante a instalação.

Procedimentos

1. Faça login no sistema do cliente como administrador.
2. Navegue até a página VMware Downloads em http://www.vmware.com/go/viewclients.
3. Faça download do arquivo de instalação do , `por exemplo, VMware-Horizon-Client-YYMM-y.y.y-xxxxxx`.exeHorizon Client .

   YYMM é o número da versão de marketing, *y.y.y* é o número da versão interna e *xxxxxx* é o número da compilação.
4. Abra um prompt de comando no computador cliente Windows.
5. Digite o nome do arquivo do instalador, os comandos de instalação e as propriedades de instalação em uma linha.

   `VMware-Horizon-Client-YYMM-y.y.y-xxxxxx.exe [commands] [properties ]`

Resultados

O instalador instala o Horizon Client de acordo com os comandos de instalação e as propriedades que você especificar. Se você especificar o comando de instalação `/silent`, os prompts do assistente não aparecerão.

O instalador instala os serviços do Windows, incluindo o VMware Horizon Client (`horizon_client_service`) e o VMware Serviço de Arbitragem USB (`VMUSBArbService`).

Exemplo: Comandos de instalação de amostra

O comando a seguir instala o Horizon Client interativamente e ativa o recurso Redirecionamento de Conteúdo de URL.

```
VMware-Horizon-Client-YYMM-y.y.y-xxxxxx.exe URL_FILTERING_ENABLED=1
```

O comando a seguir instala o Horizon Client silenciosamente e suprime todas as reinicializações e prompts de reinicialização durante o processo de instalação.

```
VMware-Horizon-Client-YYMM-y.y.y-xxxxxx.exe /silent /norestart
```

Próximo passo

Se você ativou o recurso Redirecionamento de Conteúdo de URL ao instalar o Horizon Client, verifique se o recurso está instalado. Consulte Verificar a instalação do redirecionamento de conteúdo da URL.

Inicie o Horizon Client e verifique se você pode fazer login na área de trabalho remota ou no aplicativo publicado correto. Consulte Conectar-se a uma Área de Trabalho Remota ou Aplicativo Publicado.

Verificar a instalação do redirecionamento de conteúdo da URL

Se você ativou o recurso Redirecionamento de Conteúdo de URL ao instalar o Horizon Client, verifique se o recurso foi instalado.

Pré-requisitos

Especifique a propriedade de instalação `URL_FILTERING_ENABLED=1` ao instalar o Horizon Client. Consulte Instalar o Horizon Client a partir da linha de comando.

Procedimentos

1. Faça login na máquina cliente.
2. Verifique se os arquivos `vmware-url-protocol-launch-helper.exe` e `vmware-url-filtering-plugin.dll` estão instalados no diretório `%PROGRAMFILES%\VMware\}\VMware Horizon View Client\}\\}` diretório.
3. Verifique se o complemento VMware Horizon View URL Filtering Plugin está instalado e ativado no Internet Explorer.

Atualização do Horizon Client on-line

Você pode atualizar o Horizon Client online.

Por padrão, um ícone verde aparece no menu **Opções (Options)** para indicar que uma nova versão do Horizon Client está disponível.

Durante o processo de atualização, por padrão, você pode marcar ou desmarcar a caixa de seleção **Verificar atualizações e mostrar notificação de emblema (Check for updates and show badge notification)** para especificar se o Horizon Client verificará se há atualizações automaticamente e exibirá a notificação da nova versão.

Você pode controlar o comportamento do recurso de atualização online definindo as seguintes configurações de política de grupo.

- **Ative a Horizon Clientatualização online**, que ativa ou desativa o recurso de atualização online.
- **URL para Horizon Clientatualização online**, que especifica uma URL alternativa da qual Horizon Client pode recuperar atualizações.
- **Verificar atualizações automaticamente (Automatically check for update)**, que controla a caixa de seleção **Verificar atualizações e mostrar notificação de emblema (Check for updates and show badge notification)**.
- **Atualizar mensagem pop-up (Update message pop-up)**, que controla a caixa de seleção **Mostrar mensagem pop-up quando houver uma atualização (Show pop-up message when there is an update)**. A caixa de seleção **Mostrar mensagem pop-up quando houver uma atualização (Show pop-up message when there is an update)** terá efeito somente se a caixa de seleção **Verificar atualizações e mostrar notificação de emblema (Check for updates and show badge notification)** estiver marcada.
- **Permitir que o usuário ignore a Horizon Clientatualização**, que controla o botão **Ignorar (Skip)**.

Para obter informações completas sobre essas configurações de política de grupo, consulte Usando configurações de política de grupo para configurar Horizon Client.

Você também pode desativar o recurso de atualização online definindo a propriedade `AUTO_UPDATE_ENABLED` como 0 ao instalar o Horizon Client a partir da linha de comando. Para obter mais informações, consulte Instalar o Horizon Client a partir da linha de comando.

Pré-requisitos

- Salve seu trabalho antes de atualizar Horizon Client. A atualização pode iniciar uma reinicialização do sistema.
- Verifique se você pode fazer login como administrador no sistema do cliente.

Procedimentos

1. Faça login no sistema do cliente como administrador.
2. Inicie Horizon Client, clique em **Opções (Options)** na barra de menus e selecione **Atualizações de software (Software Updates)**.
3. Para verificar se há atualizações disponíveis, clique em **Verificar atualizações (Check for Updates)**.

   Horizon Client indica se uma atualização está disponível.

4 Para iniciar o processo de atualização se uma nova versão estiver disponível, clique em **Fazer download e instalar (Download and Install)**.

   Como alternativa, você pode clicar em **Ignorar (Skip)** (se disponível) ou clicar em **Lembrar-me mais tarde (Remind Me Later)** para instalar a atualização novamente. Se você clicar em **Ignorar (Skip)**, não verá outra notificação de atualização até que a próxima versão Horizon Client esteja disponível. Você ainda pode clicar em **Atualizações de software (Software Updates)** para verificar manualmente se há uma atualização.

5 Para instalar a atualização após Horizon Client baixá-la, clique em **OK**.

   O assistente de instalação interativo Horizon Client é aberto.

Configurando o Horizon Client para usuários finais

3

A configuração do Horizon Client para usuários finais pode envolver a configuração de URIs para iniciar o Horizon Client, a configuração do modo de verificação de certificado, a definição de opções avançadas de TLS, a personalização dos menus do Horizon Client e o uso de políticas de grupo para definir configurações personalizadas.

Leia os seguintes tópicos:

Preparando o servidor de conexão para Horizon Client

Antes que os usuários finais possam se conectar a um servidor e acessar uma área de trabalho remota ou um aplicativo publicado, um administrador do Horizon deve definir determinadas configurações do Servidor de Conexão.

Unified Access Gateway e servidores de segurança

Se a sua implantação do VMware Horizon incluir um appliance do Unified Access Gateway, configure o Servidor de Conexão para funcionar com o Unified Access Gateway. Consulte o documento *Implantação e configuração do VMware Unified Access Gateway*. Os dispositivos Unified Access Gateway executam a mesma função que os servidores de segurança.

Se a sua implantação do VMware Horizon incluir um servidor de segurança, verifique se você está usando as versões de manutenção mais recentes do Connection Server 7.5 e Security Server 7.5 ou versões posteriores. Para obter mais informações, consulte o documento de instalação da sua versão do Horizon.

Observação Os servidores de segurança não são compatíveis com o VMware Horizon 2006 e versões posteriores.

Conexão de túnel segura

Se você planeja usar uma conexão de túnel seguro para dispositivos cliente e se a conexão segura estiver configurada com um nome de host DNS para uma instância do Servidor de Conexão ou um servidor de segurança, verifique se o dispositivo cliente pode resolver esse nome DNS. .

Pools de desktops e aplicativos

Use a seguinte lista de verificação ao configurar pools de área de trabalho e de aplicativos.

- Verifique se uma área de trabalho ou um pool de aplicativos foi criado e se a conta de usuário que você planeja usar tem o direito de acessar o pool. Para obter mais informações, consulte os documentos *Configurando áreas de trabalho virtuais no Horizon* e *Configurando áreas de trabalho e aplicativos publicados no Horizon*.
- Se os usuários finais tiverem uma tela de alta resolução e usarem a configuração de cliente **Modo de alta resolução (High Resolution Mode)** ao visualizar suas áreas de trabalho remotas no modo de tela cheia, verifique se vRAM suficiente está alocada para cada Windows área de trabalho remota. A quantidade de vRAM depende da resolução da tela e do número de monitores configurados para os usuários finais.

Autenticação do usuário

Use a seguinte lista de verificação ao configurar a autenticação do usuário.

- Para fornecer aos usuários finais acesso não autenticado a aplicativos publicados em Horizon Client, você deve habilitar esse recurso na instância do Servidor de Conexão. Para obter mais informações, consulte os tópicos sobre acesso não autenticado no documento *Administração Horizon*.
- Para usar a autenticação de dois fatores, como a autenticação RSA SecurID ou RADIUS, com o Horizon Client, você deve habilitar o recurso de autenticação de dois fatores para a instância do Servidor de Conexão. A partir do Horizon 7 versão 7.11, você pode personalizar os rótulos na página de login de autenticação do RADIUS. A partir do Horizon 7 versão 7.12, você pode configurar a autenticação de dois fatores para ocorrer após o tempo limite de uma sessão remota. Para obter mais informações, consulte os tópicos sobre autenticação de dois fatores no documento *Administração Horizon*.
- Para permitir que a instância do Servidor de Conexão aceite a identidade do usuário e as informações de credencial que são passadas quando os usuários selecionam **Fazer login como usuário atual (Log in As Current User)** no menu **Opções (Options)** na barra de menus Horizon Client, ative a opção Configuração **Aceitar logon como usuário atual (Accept logon as current user)** para a instância do Servidor de Conexão. Essa configuração está disponível no Horizon 7 versão 7.8 e posterior. Para obter mais informações, consulte o documento *Administração Horizon*.

  Você pode usar as configurações de política de grupo Horizon Client para configurar o recurso Fazer login como usuário atual, incluindo a especificação de uma lista de instâncias do Servidor de Conexão que podem aceitar as informações de autenticação Fazer login como usuário atual. Para obter informações sobre essas configurações do lado do cliente, consulte Usando configurações de política de grupo para configurar Horizon Client.
- Para ocultar a URL do servidor em Horizon Client, ative a configuração global **Ocultar informações do servidor na interface do usuário do cliente (Hide server information in client user interface)**. Para obter mais informações, consulte o documento *Administração Horizon*.
- Para ocultar o menu suspenso **Domínio (Domain)** em Horizon Client, ative a configuração global **Ocultar lista de domínios na interface do usuário do cliente (Hide domain list in client user interface)**. A partir do Horizon 7 versão 7.8, essa configuração é ativada por padrão. Para obter mais informações, consulte o documento *Administração Horizon*.
- Para enviar a lista de domínios para Horizon Client, ative a configuração global **Enviar lista de domínios (Send domain list)** em Horizon Console. Essa configuração está disponível no Horizon 7 versão 7.8 e posterior e é desativada por padrão. Versões Horizon 7 anteriores enviam a lista de domínios. Para obter mais informações, consulte o documento *Administração Horizon*.

A tabela a seguir mostra como as configurações globais **Enviar lista de domínios (Send domain list)** e **Ocultar lista de domínios na interface do usuário do cliente (Hide domain list in client user interface)** determinam como os usuários podem fazer login no servidor.

Configuração de Enviar lista de domínios	Ocultar lista de domínios na configuração da interface do usuário do cliente	Como os usuários fazem login
Desativado (padrão)	Ativado	O menu suspenso **Domínio (Domain)** está oculto. Os usuários devem digitar um dos seguintes valores na caixa de texto **Nome de usuário (User name)**. ■ Nome de usuário (não permitido para vários domínios) ■ ***domínio\\}nome de usuário*** ■ ***nome de usuário@domínio.com***
Desativado (padrão)	Desativado	Se um domínio padrão estiver configurado no cliente, o domínio padrão aparecerá no menu suspenso **Domínio (Domain)**. Se o cliente não conhecer um domínio padrão, `*DefaultDomain*` aparecerá no menu suspenso **Domínio (Domain)**. Os usuários devem digitar um dos seguintes valores na caixa de texto **Nome de usuário (User name)**. ■ Nome de usuário (não permitido para vários domínios) ■ ***domínio\\}nome de usuário*** ■ ***nome de usuário@domínio.com***
Ativado	Ativado	O menu suspenso **Domínio (Domain)** está oculto. Os usuários devem digitar um dos seguintes valores na caixa de texto **Nome de usuário (User name)**. ■ Nome de usuário (não permitido para vários domínios) ■ ***domínio\\}nome de usuário*** ■ ***nome de usuário@domínio.com***
Ativado	Desativado	Os usuários podem digitar um nome de usuário na caixa de texto **Nome de usuário (User name)** e, em seguida, selecionar um domínio no menu suspenso **Domínio (Domain)**. Como alternativa, os usuários podem digitar um dos seguintes valores na caixa de texto **Nome de usuário (User name)**. ■ ***domínio\\}nome de usuário*** ■ ***nome de usuário@domínio.com***

Definições de configuração comuns

O Horizon Client fornece vários mecanismos de configuração que simplificam a experiência de login e seleção de área de trabalho remota para usuários finais e impõem políticas de segurança.

A tabela a seguir mostra apenas algumas das definições de configuração que você pode definir de uma ou mais maneiras.

Tabela 3-1. Definições de configuração comuns

Configuração	Mecanismos de configuração
Endereço do servidor	URI, Política de Grupo, Linha de Comando, Windows Registro
Active Directory nome de usuário	URI, Política de Grupo, Linha de Comando, Windows Registro

Tabela 3-1. Definições de configuração comuns (continuação)

Configuração	Mecanismos de configuração
Nome de domínio	URI, Política de Grupo, Linha de Comando, Windows Registro
Nome de exibição da área de trabalho remota	URI, Política de Grupo, Linha de Comando
Tamanho da janela	URI, Política de Grupo, Linha de Comando
Exibir protocolo	URI, linha de comando
Configurando a verificação de certificado	Política de Grupo, Windows Registro
Configurando protocolos TLS e algoritmos criptográficos	Política de Grupo, Windows Registro

Usando URIs para configurar Horizon Client

Você pode usar identificadores uniformes de recursos (URIs) para criar links de página da Web ou de e-mail nos quais os usuários finais podem clicar para iniciar o Horizon Client, conectar-se a um servidor ou abrir uma área de trabalho remota ou um aplicativo publicado.

Você cria esses links construindo URIs que fornecem algumas ou todas as informações a seguir, para que os usuários finais não precisem fornecê-las.

- Endereço do servidor
- Número da porta do servidor
- Active Directory nome de usuário
- nome de usuário RADIUS ou RSA SecurID, se diferente do nome de usuário Active Directory
- Nome de domínio
- Área de trabalho remota ou nome de exibição do aplicativo publicado
- Tamanho da janela
- Ações, incluindo redefinir, fazer logout e iniciar sessão
- Exibir protocolo
- Opções para redirecionar dispositivos USB

Para construir um URI, use o esquema de URI `vmware-view` com Horizon Client partes de caminho e consulta específicas.

Para usar URIs para iniciar o Horizon Client, o Horizon Client já deve estar instalado nos computadores clientes.

Sintaxe para criar URIs do vmware-view

A sintaxe do URI inclui o esquema de URI `vmware-view`, uma parte do caminho para especificar a área de trabalho remota ou o aplicativo publicado e, opcionalmente, uma consulta para especificar as ações ou opções de configuração da área de trabalho remota ou do aplicativo publicado.

Especificação de URI

Use a seguinte sintaxe para criar URIs para iniciar Horizon Client.

```
vmware-view://[authority-part][/path-part][?query-part]
```

O único elemento necessário é o esquema de URI, `vmware-view`. Como o nome do esquema faz distinção entre maiúsculas e minúsculas para algumas versões de alguns sistemas operacionais cliente, digite `vmware-view`.

Importante Em todas as partes, os caracteres não ASCII devem primeiro ser codificados de acordo com UTF-8 [STD63] e, em seguida, cada octeto da sequência UTF-8 correspondente deve ser codificado por porcentagem para ser representado como caracteres URI.

Para obter informações sobre a codificação de caracteres ASCII, consulte a referência de codificação de URL em http://www.utf8-chartable.de/.

authority-part

O endereço do servidor e, opcionalmente, um nome de usuário, um número de porta não padrão ou ambos. Não há suporte para sublinhados (_) em nomes de servidor. Os nomes de servidor devem estar em conformidade com a sintaxe do DNS.

Para especificar um nome de usuário, use a seguinte sintaxe.

```
user1@server-address
```

Você não pode especificar um endereço UPN, que inclui o domínio. Para especificar o domínio, você pode usar a parte de consulta `domainName` no URI.

Para especificar um número de porta, use a seguinte sintaxe.

```
server-address:port-number
```

path-part

O nome para exibição da área de trabalho remota ou do aplicativo publicado. O nome para exibição é especificado em Horizon Console quando o pool de áreas de trabalho ou o pool de aplicativos é criado. Se o nome para exibição contiver um espaço, use o mecanismo de codificação **`%20`** para representar o espaço.

Como alternativa, você pode especificar uma ID de área de trabalho ou aplicativo, que é uma cadeia de caracteres de caminho que inclui a ID da área de trabalho

ou do pool de aplicativos. Para encontrar uma ID de área de trabalho ou de aplicativo, abra o ADSI Edit no host do Servidor de Conexão, navegue até `DC=vdi,dc=vmware,dc=int` e selecione o nó `OU=Applications` . Todos os pools de desktops e aplicativos são listados. O atributo `distinguishedName` especifica o valor do ID. Você deve codificar o valor da ID antes de especificá-lo em um URI, por exemplo, `cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`.

Se você especificar uma ID de área de trabalho ou de aplicativo, deverá usar apenas letras minúsculas, mesmo se a ID de área de trabalho ou de aplicativo contiver letras maiúsculas no ADSI Edit.

Observação Mais de uma área de trabalho remota ou aplicativo publicado pode ter o mesmo nome de exibição, mas a ID da área de trabalho e do aplicativo é exclusiva. Para especificar uma determinada área de trabalho remota ou aplicativo publicado, use a ID da área de trabalho ou do aplicativo em vez do nome para exibição.

query-part

As opções de configuração a serem usadas ou as ações da área de trabalho remota ou do aplicativo publicado a serem executadas. As consultas não diferenciam maiúsculas de minúsculas. Para usar várias consultas, use um e comercial (&) entre as consultas. Se as consultas entrarem em conflito, Horizon Client usará a última consulta na lista. Use a seguinte sintaxe.

```
query1=value1[&query2=value2...]
```

Consultas compatíveis

As consultas a seguir são compatíveis com esse tipo de Horizon Client. Se você estiver criando URIs para vários tipos de clientes, como clientes de área de trabalho e clientes móveis, consulte o guia de instalação e configuração para cada tipo de sistema do cliente para obter a lista de consultas com suporte.

ação

Tabela 3-2. Valores que podem ser usados com a ação Consultar

Valor	Descrição
`browse`	Exibe uma lista de áreas de trabalho remotas disponíveis e aplicativos publicados hospedados no servidor especificado. Você não é obrigado a especificar uma área de trabalho remota ou um aplicativo publicado ao usar esta ação.
`start-session`	Abre a área de trabalho remota ou o aplicativo publicado especificado. Se nenhuma consulta de ação for fornecida e o nome da área de trabalho remota ou do aplicativo publicado for fornecido, `start-session` será a ação padrão.
`reset`	Desliga e reinicia a área de trabalho remota ou o aplicativo publicado especificado. Os dados não salvos são perdidos. Redefinir uma área de trabalho remota é o mesmo que pressionar o botão Redefinir em um PC físico.

Tabela 3-2. Valores que podem ser usados com a ação Consultar (continuação)

Valor	Descrição
`restart`	Desliga e reinicia a área de trabalho remota especificada. Reiniciar uma área de trabalho remota é o mesmo que o comando de reinicialização do sistema operacional Windows. O sistema operacional geralmente solicita que o usuário salve os dados não salvos antes de ser reiniciado.
`logoff`	Desconecta o usuário do sistema operacional convidado na área de trabalho remota. Se você especificar um aplicativo publicado, a ação será ignorada ou o usuário final verá a mensagem de aviso "Ação de URI inválida".

argumentos

Especifica os argumentos de linha de comando a serem adicionados quando o aplicativo publicado é iniciado. Use a sintaxe `args=`*value*, em que *value* é uma string. Use a codificação de porcentagem para os seguintes caracteres:

- Para dois-pontos (:), use **`%3A`**
- Para uma barra invertida (\), use **`%5C`**
- Para um espaço ( ), use **`%20`**
- Para aspas duplas ("), use **`%22`**

Por exemplo, para especificar o nome de arquivo "`Meu novo arquivo.txt`" para o aplicativo Notepad++, use **`%22My%20new%20file.txt%22`**.

appProtocol

Para aplicativos publicados, os valores válidos são **`PCOIP`** e **`BLAST`**. Por exemplo, para especificar PCoIP, use a sintaxe **`appProtocol=PCOIP`**.

connectUSBOnInsert

Conecta um dispositivo USB à área de trabalho remota em primeiro plano ou ao aplicativo publicado quando você conecta o dispositivo. Essa consulta será definida implicitamente se você especificar a consulta `unattended` para uma área de trabalho remota. Para usar essa consulta, você deve definir a consulta `action` como **`start-session`** ou não terá uma consulta `action`. Os valores válidos são **`true`** e **`false`**. Um exemplo da sintaxe é **`connectUSBOnInsert=true`**.

connectUSBOnStartup

Redireciona todos os dispositivos USB que estão conectados no momento ao sistema cliente para a área de trabalho remota ou o aplicativo publicado. Essa consulta será definida implicitamente se você especificar a consulta `unattended` para uma área de trabalho remota. Para usar essa consulta, você deve definir a consulta `action` como **`start-session`** ou não terá uma consulta `action`. Os valores válidos são **`true`** e **`false`**. Um exemplo da sintaxe é **`connectUSBOnStartup=true`**.

desktopLayout

Define o tamanho da janela da área de trabalho remota. Para usar essa consulta, você deve definir a consulta `action` como **`start-session`** ou não ter uma consulta `action`.

Tabela 3-3. Valores válidos para a consulta desktopLayout

Valor	Descrição
`fullscreen`	Tela cheia em um monitor. Esse valor é o padrão.
`multimonitor`	Tela cheia em todos os monitores.
`windowLarge`	Grande janela.
`windowSmall`	Janela pequena.
*W*x*H*	Resolução personalizada, em que você especifica a largura por altura, em pixels. Um exemplo da sintaxe é **`desktopLayout=1280x800`**.

desktopProtocol

Para áreas de trabalho remotas, os valores válidos são **`RDP`**, **`PCOIP`** e **`BLAST`**. Por exemplo, para especificar PCoIP, use a sintaxe **`desktopProtocol=PCOIP`**.

domainName

Especifica o nome de domínio NETBIOS associado ao usuário que está se conectando à área de trabalho remota ou ao aplicativo publicado. Por exemplo, você pode usar `mycompany` em vez de `mycompany.com`.

filePath

Especifica o caminho para o arquivo no sistema local que você deseja abrir com o aplicativo publicado. Você deve especificar o caminho completo, incluindo a letra da unidade. Use a codificação de porcentagem para os seguintes caracteres:

- Para dois-pontos (:), use **`%3A`**
- Para uma barra invertida (\), use **`%5C`**
- Para um espaço ( ), use **`%20`**

Por exemplo, para representar o caminho do arquivo `C:\test file.txt`, use **`C%3A%5Ctest%20file.txt`**.

launchMinimized

Inicia Horizon Client no modo minimizado. Horizon Client permanece minimizado até que a área de trabalho remota ou o aplicativo publicado especificado seja iniciado. A sintaxe é **`launchMinimized=true`**. Você não pode usar essa consulta com a consulta **autônoma (unattended)**.

tokenUserName

Especifica o nome de usuário RSA ou RADIUS. Use essa consulta somente se o nome de usuário RSA ou RADIUS for diferente do nome de usuário Active Directory. Se você não especificar essa consulta e a autenticação RSA ou RADIUS for necessária, Horizon Client usará o nome de usuário Windows. A sintaxe é **tokenUserName=*name***.

autônomo

Cria uma conexão de servidor com uma área de trabalho remota no modo de quiosque. Se você usar essa consulta, não especifique as informações do usuário se tiver gerado o nome da conta do endereço MAC do dispositivo do cliente. Se você tiver criado nomes de conta personalizados no ADAM, como nomes que começam com "personalizado-", deverá especificar as informações da conta.

useExistente

Se essa opção for definida como **true**, apenas uma instância Horizon Client poderá ser executada. Se os usuários tentarem se conectar a um segundo servidor, eles deverão fazer logout do primeiro servidor, fazendo com que as sessões de área de trabalho remota e de aplicativo publicado sejam desconectadas. Se essa opção for definida como **false**, várias instâncias de Horizon Client poderão ser executadas e os usuários poderão se conectar a vários servidores ao mesmo tempo. O padrão é **true**. Um exemplo da sintaxe é **useExisting=false**.

unauhenticatedAccessEnabled

Se essa opção for definida como **true**, o recurso Acesso não autenticado será ativado por padrão. A opção **Acesso não autenticado (Unauthenticated Access)** fica visível na interface do usuário e está selecionada. Se essa opção for definida como **false**, o recurso Acesso não autenticado será desativado. A configuração **Acesso não autenticado (Unauthenticated Access)** está oculta e desativada. Quando essa opção é definida como **""**, o recurso Acesso não autenticado é desativado e a configuração **Acesso não autenticado (Unauthenticated Access)** é ocultada da interface do usuário e desativada. Um exemplo da sintaxe é **unauthenticatedAccessEnabled=true**.

não autenticadoAccessAccount

Se o recurso Acesso não autenticado estiver ativado, define a conta a ser usada. Se o Acesso não autenticado estiver desativado, essa consulta será ignorada. Um exemplo de sintaxe usando a conta de usuário **anonymous1** é **unauthenticatedAccessAccount=anonymous1**.

Exemplos de URIs do vmware-view

Você pode usar o esquema de URI `vmware-view` para criar links ou botões de hipertexto e incluir esses links no e-mail ou em uma página Web. Por exemplo, um usuário final pode clicar em um link de URI para iniciar uma área de trabalho remota com as opções de inicialização que você especificar.

Cada exemplo de URI é seguido por uma descrição do que o usuário final vê depois de clicar no link do URI.

1 `vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session`

Horizon Client inicia e se conecta ao servidor `view.mycompany.com`. A caixa de diálogo de logon solicita ao usuário um nome de usuário, um nome de domínio e uma senha. Após um login bem-sucedido, o cliente se conecta à área de trabalho remota que tem o nome de exibição `Área de Trabalho Primária`, e o usuário é conectado ao sistema operacional convidado.

Observação Neste exemplo, o protocolo de exibição padrão e o tamanho da janela são usados. O protocolo de exibição padrão é PCoIP e o tamanho padrão da janela é tela cheia.

2 `vmware-view://view.mycompany.com/cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`

Horizon Client inicia e se conecta ao servidor `view.mycompany.com`. A caixa de diálogo de logon solicita ao usuário um nome de usuário, um nome de domínio e uma senha. Após um login bem-sucedido, o cliente se conecta à área de trabalho remota que tem a ID de área de trabalho `CN=win7-32,OU=Applications,DC=vdi,DC=vmware,DC=int` (valor codificado `cn%3Dwin7-32%2Cou%3Dapplications%2Cdc%3Dvdi%2Cdc%3Dvmware%2Cdc%3Dint`).

3 `vmware-view://view.mycompany.com:7555/Primary%20Desktop`

Esse URI tem o mesmo efeito que o exemplo anterior, exceto que ele usa a porta não padrão de 7555 para a instância do Servidor de Conexão. (A porta padrão é 443.) Como um identificador de área de trabalho remota é fornecido, a área de trabalho remota é aberta, mesmo que a ação `start-session` não esteja incluída no URI.

4 `vmware-view://fred@view.mycompany.com/Finance%20Desktop?desktopProtocol=PCOIP`

Horizon Client inicia e se conecta ao servidor `view.mycompany.com`. Na caixa de diálogo de login, a caixa de texto **Nome de usuário (User name)** é preenchida com `fred`. O usuário deve fornecer o nome de domínio e a senha. Após um login bem-sucedido, o cliente se conecta à área de trabalho remota que tem o nome de exibição `Finance Desktop`, e o usuário é conectado ao sistema operacional convidado. A conexão usa o protocolo de exibição PCoIP.

5 `vmware-view://view.mycompany.com/Calculator?action=start-session&appProtocol=BLAST`

Horizon Client inicia e se conecta ao servidor `view.mycompany.com`. Na caixa de diálogo de logon, o usuário deve fornecer o nome de usuário, o nome de domínio e a senha. Após um login bem-sucedido, o cliente se conecta ao aplicativo publicado que tem o nome de exibição `Calculadora`. A conexão usa o protocolo de exibição VMware Blast.

6 `vmware-view://fred@view.mycompany.com/Finance%20Desktop?domainName=mycompany`

Horizon Client inicia e se conecta ao servidor `view.mycompany.com`. Na caixa de diálogo de login, a caixa de texto **Nome de usuário (User name)** é preenchida com `fred`, e a caixa de texto **Domínio (Domain)** é preenchida com `minha empresa`. O usuário deve fornecer apenas uma senha. Após um login bem-sucedido, o cliente se conecta à área de trabalho remota que tem o nome de exibição `Finance Desktop`, e o usuário é conectado ao sistema operacional convidado.

7
```
vmware-view://view.mycompany.com/
```

Horizon Client é iniciado e o usuário é levado ao prompt de login para se conectar ao servidor `view.mycompany.com`.

8
```
vmware-view://view.mycompany.com/Primary%20Desktop?action=reset
```

Horizon Client inicia e se conecta ao servidor `view.mycompany.com`. A caixa de diálogo de logon solicita ao usuário um nome de usuário, um nome de domínio e uma senha. Após um login bem-sucedido, Horizon Client redefine a área de trabalho especificada.

Observação Essa ação estará disponível somente se um administrador do Horizon tiver ativado o recurso de redefinição para a área de trabalho remota.

9
```
vmware-view://view.mycompany.com/Primary%20Desktop?action=restart
```

Horizon Client inicia e se conecta ao servidor `view.mycompany.com`. A caixa de diálogo de logon solicita ao usuário um nome de usuário, um nome de domínio e uma senha. Após um login bem-sucedido, Horizon Client reinicia a área de trabalho especificada.

Observação Essa ação estará disponível somente se um administrador do Horizon tiver ativado o recurso de reinicialização para a área de trabalho remota.

10
```
vmware-view://view.mycompany.com/Primary%20Desktop?action=start-
session&connectUSBOnStartup=true
```

Esse URI tem o mesmo efeito que o primeiro exemplo, e todos os dispositivos USB conectados ao sistema do cliente são redirecionados para a área de trabalho remota.

11
```
vmware-view://
```

Se Horizon Client não estiver em execução, ele será iniciado. Se Horizon Client já estiver em execução, ele será exibido em primeiro plano.

12
```
vmware-view://10.10.10.10/My%20Notepad++?args=%22My%20new%20file.txt%22
```

Inicia o My Notepad++ no servidor 10.10.10.10 e passa o argumento `Meu novo arquivo.txt` no comando de início do aplicativo publicado. Espaços e aspas duplas usam o escape de porcentagem. O nome do arquivo está entre aspas porque contém espaços.

Você também pode digitar esse comando no prompt de linha de comando Windows usando a seguinte sintaxe:

```
vmware-view.exe --serverURL 10.10.10.10 --appName "My Notepad++" --args "\"my new.txt\""
```

Neste exemplo, as aspas duplas são escapadas usando os caracteres \".

13
```
vmware-view://10.10.10.10/Notepad++%2012?args=a.txt%20b.txt
```

Inicia o Notepad++ 12 no servidor 10.10.10.10 e passa o argumento `a.text b.txt` no comando de início do aplicativo publicado. Como o argumento não está entre aspas, um espaço separa os nomes dos arquivos e os dois arquivos são abertos separadamente no Notepad++.

Observação Os aplicativos publicados podem diferir na maneira como usam argumentos de linha de comando. Por exemplo, se você passar o argumento `a.txt b.txt` para o WordPad, o WordPad abrirá apenas um arquivo, `a.txt`.

14
```
vmware-view://view.mycompany.com/Notepad?
unauthenticatedAccessEnabled=true&unauthenticatedAccessAccount=anonymous1
```

Horizon Client inicia e se conecta ao servidor `view.mycompany.com` usando a conta de usuário **`anonymous1`**. O aplicativo Bloco de Notas é iniciado sem solicitar que o usuário forneça as credenciais de login.

Exemplos de código HTML

Você pode usar URIs para criar links de hipertexto e botões para incluir em e-mails ou em páginas Web. Os exemplos a seguir mostram como usar o URI do primeiro exemplo de URI para codificar o link de hipertexto rotulado **Test Link** e um botão rotulado **TestButton**.

```
<html>
<body>

<a href="vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session">Test Link</
a><br>

<form><input type="button" value="TestButton" onClick="window.location.href=
'vmware-view://view.mycompany.com/Primary%20Desktop?action=start-session'"></form> <br>

</body>
</html>
```

Configurando o modo de verificação de certificado em Horizon Client

A verificação do certificado do servidor ocorre para conexões entre Horizon Client e um servidor. Um certificado é uma forma digital de identificação, semelhante a um passaporte ou carteira de motorista.

A verificação do certificado do servidor inclui as seguintes verificações:

- O certificado foi revogado?
- O certificado destina-se a um propósito diferente de verificar a identidade do remetente e criptografar as comunicações do servidor? Ou seja, esse é o tipo correto de certificado?
- O certificado expirou ou é válido apenas no futuro? Ou seja, o certificado é válido de acordo com o relógio do computador?
- O nome comum no certificado corresponde ao nome do host do servidor que o envia? Uma incompatibilidade poderá ocorrer se um balanceador de carga redirecionar Horizon Client para um servidor que tenha um certificado que não corresponda ao nome do host inserido em Horizon Client. Outro motivo pelo qual uma incompatibilidade pode ocorrer é se você inserir um endereço IP em vez de um nome de host no cliente.
- O certificado é assinado por uma autoridade de certificação (CA) desconhecida ou não confiável? Certificados autoassinados são um tipo de CA não confiável. Para passar nessa verificação, a cadeia de confiança do certificado deve estar enraizada no repositório de certificados local do dispositivo.

Para obter informações sobre como distribuir um certificado raiz autoassinado a todos os sistemas cliente Windows em um domínio, consulte "Adicionar o certificado raiz a autoridades de certificação raiz confiáveis" no documento *Instalação Horizon*.

Para definir o modo de verificação de certificado, inicie Horizon Client e selecione **Configurações (Settings) > Segurança (Security)**. Você pode selecionar uma das seguintes opções. Observe que você não pode configurar a verificação de certificado no modo FIPS.

- **Nunca se conecte a servidores não confiáveis (Never connect to untrusted servers)**. Essa configuração significa que você não poderá se conectar ao servidor se qualquer uma das verificações de certificado falhar. Uma mensagem de erro lista as verificações que falharam.
- **Avisar antes de se conectar a servidores não confiáveis (Warn before connecting to untrusted servers)**. Essa configuração significa que você pode clicar em **Continuar (Continue)** para ignorar o aviso se uma verificação de certificado falhar porque o servidor usa um certificado autoassinado. Para certificados autoassinados, o nome do certificado não é necessário para corresponder ao nome do servidor que você digitou em Horizon Client. Você também poderá receber um aviso se o certificado expirar.
- **Não verifique os certificados de identidade do servidor (Do not verify server identity certificates)**. Essa configuração significa que nenhuma verificação de certificado ocorre.

Se um administrador instalar posteriormente um certificado de segurança de uma autoridade de certificação confiável e todas as verificações de certificado forem aprovadas quando você se conectar, essa conexão confiável será lembrada para esse servidor específico. No futuro, se esse servidor apresentar um certificado autoassinado novamente, a conexão falhará. Depois que um determinado servidor apresenta um certificado totalmente verificável, ele sempre deve fazer isso.

Importante Se você usou anteriormente a política de grupo para configurar os sistemas cliente da sua empresa para usar uma criptografia específica, como ao definir as configurações de política de grupo SSL Cipher Suite Order, agora você deve usar uma configuração de segurança de política de grupo Horizon Client. Consulte Usando configurações de política de grupo para configurar Horizon Client. Como alternativa, você pode usar a configuração de registro `SSLCipherList` no sistema do cliente. Consulte Usando o Windows Registry para configurar o Horizon Client.

Você pode configurar o modo de verificação de certificado padrão e impedir que os usuários finais o alterem em Horizon Client. Para obter mais informações, consulte Configurando o modo de verificação de certificado para usuários finais.

Usando um servidor proxy SSL

Se você usar um servidor proxy SSL para inspecionar o tráfego enviado do ambiente do cliente para a Internet, ative a configuração **Permitir conexão por meio de um proxy SSL (Allow connection via an SSL Proxy)**. Essa configuração permite a verificação de certificado para conexões secundárias por meio de um servidor proxy SSL e se aplica às conexões do Blast Secure Gateway e do túnel seguro. Se você usar um servidor proxy SSL e ativar a verificação de certificado, mas não ativar a configuração **Permitir conexão por meio de um proxy SSL (Allow connection via an SSL Proxy)**, as conexões falharão devido a impressões digitais incompatíveis. A configuração **Permitir conexão por meio de um proxy SSL (Allow connection via an SSL Proxy)** não estará disponível se você ativar a opção **Não verificar certificados de identidade do servidor (Do not verify server identity certificates)**. Quando a opção **Não verificar certificados de identidade do servidor (Do not verify server identity certificates)** está ativada, Horizon Client não verifica o certificado ou a impressão digital e um proxy SSL é sempre permitido.

Você pode usar a configuração de política de grupo **Configura o comportamento de verificação de certificado do Proxy SSL do Horizon Client** para definir se a verificação de certificado para conexões secundárias deve ser permitida por meio de um servidor proxy SSL. Para obter mais informações, consulte Usando configurações de política de grupo para configurar Horizon Client.

Para permitir conexões VMware Blast por meio de um servidor proxy, consulte Configurar opções do VMware Blast.

Configurando o modo de verificação de certificado para usuários finais

Você pode configurar o modo de verificação de certificado para usuários finais. Por exemplo, você pode configurar para que a verificação completa seja sempre realizada. A verificação de certificado ocorre para conexões TLS entre um servidor e Horizon Client.

Você pode configurar uma das seguintes estratégias de verificação de certificado para usuários finais.

- Os usuários finais têm permissão para selecionar o modo de verificação de certificado em Horizon Client.
- (Sem verificação) Nenhuma verificação de certificado é executada.
- (Aviso) Se o servidor apresentar um certificado autoassinado, os usuários finais serão avisados. Os usuários podem determinar se permitem esse tipo de conexão.
- (Segurança total) A verificação completa é executada e as conexões que não passam na verificação completa são rejeitadas.

Se você usar um servidor proxy SSL para inspecionar o tráfego enviado do ambiente do cliente para a Internet, poderá configurar a verificação de certificado para conexões secundárias por meio do servidor proxy SSL. Esse recurso se aplica às conexões do Blast Secure Gateway e do túnel seguro. Você também pode permitir o uso do servidor proxy para conexões VMware Blast.

Para obter informações sobre os tipos de verificações de certificado que podem ser realizadas, consulte Configurando o modo de verificação de certificado em Horizon Client.

Você pode usar as configurações de política de grupo Horizon Client para definir o modo de verificação de certificado, permitir o uso de proxy SSL, restringir o uso de determinados algoritmos e protocolos criptográficos antes de estabelecer uma conexão TLS criptografada e habilitar o uso de proxy para conexões VMware Blast. Para obter mais informações, consulte Usando configurações de política de grupo para configurar Horizon Client.

Se você não quiser configurar o modo de verificação de certificado como uma política de grupo, poderá habilitar a verificação de certificado adicionando o nome do valor `CertCheckMode` a uma das seguintes chaves do Registro no computador cliente:

- Para Windows de 32 bits: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\}\VMware\} VDM\Client\Security`
- Para Windows de 64 bits: `HKLM\SOFTWARE\WOW6432Node\VMware, Inc.\}\VMware\} VDM\Client\Security`

Use os seguintes valores na chave do Registro:

- **0** implementa `Do not verify server identity certificates.`
- **1** implementa `Warn before connecting to untrusted servers.`
- **2** implementa `Never connect to untrusted servers.`

Se você definir a configuração da política de grupo e a configuração `CertCheckMode` na chave do Registro, a configuração da política de grupo terá precedência sobre o valor da chave do Registro.

Configurando opções avançadas de TLS

Você pode selecionar os protocolos de segurança e os algoritmos criptográficos que são usados para criptografar as comunicações entre Horizon Client e servidores e entre Horizon Client e o agente em uma área de trabalho remota.

Essas opções de segurança também são usadas para criptografar o canal USB.

Com a configuração padrão, os conjuntos de codificação usam AES de 128 bits ou 256 bits, removem algoritmos DH anônimos e classificam a lista de codificação atual na ordem do comprimento da chave do algoritmo de criptografia.

Por padrão, o TLS v1.1 e o TLS v1.2 estão ativados. SSL v2.0, SSL v3.0 e TLS v1.0 não são compatíveis.

Se você configurar um protocolo de segurança para Horizon Client que não esteja ativado no servidor ao qual o cliente se conecta, ocorrerá um erro de TLS e a conexão falhará.

Importante Pelo menos um dos protocolos que você habilita em Horizon Client também deve estar habilitado na área de trabalho remota ou os dispositivos USB não podem ser redirecionados para a área de trabalho remota.

No sistema cliente, você pode usar uma configuração de política de grupo ou uma configuração de Registro Windows para alterar as codificações e os protocolos padrão. Para obter informações sobre como usar uma configuração de política de grupo, consulte a configuração **Configura protocolos SSL e algoritmos criptográficos (Configures SSL protocols and cryptographic algorithms)** em Usando configurações de política de grupo para configurar Horizon Client. Para obter informações sobre como usar a configuração SSLCipherList no Windows Registry, consulte Usando o Windows Registry para configurar o Horizon Client.

Personalizando os menus do Horizon Client

Você pode usar políticas de grupo do Horizon Client para ocultar alguns itens em determinados menus na interface do usuário do Horizon Client.

Para obter informações sobre como usar as políticas de grupo que controlam os menus Horizon Client, consulte as descrições de **Ocultar itens no menu de contexto do aplicativo (Hide items in application context menu)**, **Ocultar itens no menu de contexto da área de trabalho (Hide items in desktop context menu)**, **Ocultar itens na barra de ferramentas da área de trabalho (Hide items in desktop toolbar)**, **Ocultar itens no menu da bandeja do sistema (Hide items in system tray menu)** e **Ocultar itens no menu da barra de ferramentas do cliente (Hide items in the client toolbar menu)** agrupam configurações de política em Usando configurações de política de grupo para configurar Horizon Client.

Personalizando as Horizon Client mensagens de erro

Você pode usar a configuração de política de grupo Horizon Client **Rodapé de tela de erro personalizado (Custom error screen footer)** para adicionar texto de ajuda personalizado à parte inferior de todas as mensagens de erro que aparecem na interface do usuário do Horizon Client. Por exemplo, seu texto de ajuda pode informar aos usuários como entrar em contato com o suporte técnico da sua empresa.

Você deve criar um arquivo de texto simples (`.txt`) no sistema do cliente local para conter o texto de ajuda. O arquivo de texto pode conter até 2.048 caracteres, incluindo caracteres de controle. Há suporte para a codificação ANSI e Unicode. Você especifica o caminho completo para esse arquivo de texto ao definir a configuração de política de grupo **Rodapé de tela de erro personalizado (Custom error screen footer)**.

Para obter informações detalhadas sobre como usar a configuração de política de grupo **Rodapé de tela de erro personalizado (Custom error screen footer)**, consulte Usando configurações de política de grupo para configurar Horizon Client.

Configurando a manipulação de eventos do cursor

Você pode otimizar a manipulação de eventos de cursor definindo as configurações no arquivo `C:\ProgramData\VMware\}\VMware Horizon View\}\config.ini` no sistema cliente Windows.

Observação Para usar a manipulação de eventos de cursor, o Horizon Agent 2006 ou posterior deve estar instalado na área de trabalho remota.

Configuração	Descrição
`RemoteDisplay.allowCursorWarping`	Ativa ou desativa o recurso de distorção do cursor. Quando esse recurso está ativado e o mouse está no modo absoluto, o agente remoto detecta movimentos repentinos do cursor e os reflete para o cliente movendo o cursor local. Quando esse recurso está desativado, o cliente ignora movimentos repentinos do cursor no agente remoto. Os valores válidos são TRUE ou FALSE. O valor padrão é TRUE.
`RemoteDisplay.allowCursorEventsOnLowLatencyChannel`	Determina se o canal de baixa latência é usado para atualizações do cursor. Os valores válidos são TRUE ou FALSE. O valor padrão é TRUE.

Você pode configurar a latência máxima permitida ao unir movimentos do mouse definindo a configuração de política de grupo **Configurar latência máxima para união do mouse (Configure maximum latency for mouse coalescing)**. Para obter mais informações, consulte Usando configurações de política de grupo para configurar Horizon Client.

Você também pode configurar a manipulação de eventos de cursor na máquina do agente. Por exemplo, você pode usar a configuração de política de grupo **Distorção do cursor (Cursor Warping)** do lado do agente para definir a distorção do cursor e pode modificar as configurações do Registro Windows na máquina do agente para habilitar ou desabilitar eventos de movimento do mouse agrupados e a baixa -canal de latência. As configurações no cliente e no agente devem corresponder para que o recurso seja ativado. Para obter informações sobre as configurações do lado do agente, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.

Usando configurações de política de grupo para configurar Horizon Client

Horizon Client inclui um arquivo de modelo ADMX de política de grupo que você pode usar para configurar os recursos e o comportamento do Horizon Client. Você pode otimizar e proteger a área de trabalho remota e as conexões de aplicativos publicados adicionando as configurações de política no arquivo de modelo ADMX a um GPO novo ou existente em Active Directory.

O arquivo de modelo contém as políticas de grupo Configuração do Computador e Configuração do Usuário.

- As políticas de Configuração do Computador definem políticas que se aplicam a Horizon Client, independentemente de quem está executando o cliente no host.
- As políticas de Configuração do Usuário definem políticas Horizon Client que se aplicam a todos os usuários que estão executando o Horizon Client e às configurações de conexão RDP. As políticas de Configuração do Usuário substituem as políticas equivalentes de Configuração do Computador.

Horizon Client aplica políticas quando áreas de trabalho remotas e aplicativos publicados são iniciados e quando os usuários fazem login.

O Horizon Client arquivo de modelo ADMX de configuração (`vdm_client.admx`) e todos os arquivos de modelo ADMX que fornecem configurações de política de grupo estão disponíveis em `VMware-Horizon-Extras-Bundle-` *`YYMM`*`-x.x.x-yyyyyyy.zip`, em que *YYMM* é o número da versão de marketing, *x.x.x* é o número interno o número da versão e *yyyyyyy* é o número da compilação. Você pode baixar esse arquivo ZIP do VMware site Downloads em https://my.vmware.com/web/vmware/downloads. Você deve copiar o arquivo para o servidor Active Directory e usar o Editor de Gerenciamento de Política de Grupo para adicionar os modelos administrativos. Para obter instruções, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.

Configurações de definição de script para GPOs de cliente

Você pode definir políticas de grupo para muitas das mesmas configurações que podem ser definidas ao executar Horizon Client na linha de comando, incluindo o tamanho da janela da área de trabalho remota, o nome de usuário de logon e o nome de domínio de logon.

A tabela a seguir descreve as configurações de definição de script no arquivo de modelo VMware Horizon Client Configuration ADMX. Esse arquivo de modelo fornece uma versão de Configuração do Computador e uma Configuração do Usuário de cada configuração de definição de script. A definição de Configuração do Usuário substitui a definição equivalente de Configuração do Computador. As configurações aparecem na pasta **VMware Horizon Client Configuração > Definições de script (Scripting definitions)** no Editor de Gerenciamento de Política de Grupo.

Tabela 3-4. VMware Horizon Client Modelo de configuração: definições de script

Configuração	Descrição
`Automatically connect if only one launch item is entitled`	Se um usuário tiver direito a apenas uma área de trabalho remota, conecte-o a essa área de trabalho remota. Essa configuração evita que o usuário tenha que selecionar uma área de trabalho remota em uma lista que contém apenas uma área de trabalho remota.
`Connect all USB devices to the desktop or remote application on launch`	Determina se todos os dispositivos USB disponíveis no sistema cliente estão conectados à área de trabalho remota ou ao aplicativo publicado quando a área de trabalho remota ou o aplicativo publicado é iniciado.
`Connect USB devices to the desktop or remote application when they are plugged in`	Determina se os dispositivos USB estão conectados à área de trabalho remota ou ao aplicativo publicado quando os dispositivos são conectados ao sistema do cliente.
`DesktopLayout`	Especifica o layout da janela Horizon Client que os usuários veem quando fazem login em uma área de trabalho remota. As opções de layout são as seguintes: ■ `Full Screen` ■ `Multimonitor` ■ `Window - Large` ■ `Window - Small` Essa configuração está disponível somente quando o `DesktopName to select setting` também está definido.
`DesktopName to select`	Especifica a área de trabalho remota padrão que Horizon Client usa durante o login.
`Disable 3rd-party Terminal Services plugins`	Determina se o Horizon Client verifica plug-ins de Serviços de Terminal de terceiros que estão instalados como plug-ins RDP normais. Se você não definir essa configuração, o Horizon Client verificará plug-ins de terceiros por padrão. Essa configuração não afeta os plug-ins específicos do Horizon, como o redirecionamento de USB.
`Locked Guest Size`	Se a exibição for usada em um monitor, especifica a resolução da tela da área de trabalho remota. Essa configuração não funcionará se você definir a exibição da área de trabalho remota como **Todos os monitores (All Monitors)**. Depois de ativar essa configuração, a funcionalidade de ajuste automático da área de trabalho remota é desativada e a opção **Permitir dimensionamento de exibição (Allow Display Scaling)** fica oculta na interface do usuário do Horizon Client.
`Logon DomainName`	Especifica o domínio NetBIOS que Horizon Client usa durante o logon.

Tabela 3-4. VMware Horizon Client Modelo de configuração: definições de script (continuação)

Configuração	Descrição
`Logon Password`	Especifica a senha que Horizon Client usa durante o login. A senha é armazenada em texto simples por Active Directory. Para maior segurança, não especifique essa configuração. Os usuários podem digitar a senha de forma interativa.
`Logon UserName`	Especifica a senha que Horizon Client usa durante o login. A senha é armazenada em texto simples por Active Directory.
`Server URL`	Especifica a URL que Horizon Client usa durante o login, por exemplo, `https://view1.example.com`.
`Suppress error messages (when fully scripted only)`	Determina se as mensagens de erro Horizon Client são ocultas durante o login. Essa configuração se aplica somente quando o processo de logon é totalmente com script, por exemplo, quando todas as informações de logon necessárias são pré-preenchidas por meio da política de grupo. Se o login falhar devido a informações de login incorretas, os usuários não serão notificados e o processo Horizon Client será encerrado.
`Disconnected application session resumption behavior`	Determina como os aplicativos publicados em execução se comportam quando os usuários se reconectam a um servidor. As escolhas são as seguintes: ■ Pedir para se reconectar a aplicativos abertos ■ Reconectar automaticamente para abrir aplicativos ■ Não pergunte e não reconecte automaticamente Quando essa configuração está habilitada, os usuários finais não podem configurar o comportamento de reconexão do aplicativo publicado em Horizon Client. Quando essa configuração está desativada, os usuários finais podem configurar o comportamento de reconexão do aplicativo publicado em Horizon Client. Essa configuração está desativada por padrão.
`Enable Unauthenticated Access to the server`	Determina se os usuários precisam inserir credenciais para acessar seus aplicativos publicados quando usam Horizon Client. Quando essa configuração está ativada, a configuração **Acesso não autenticado (Unauthenticated Access)** em Horizon Client fica visível, desativada e selecionada. O cliente poderá fazer fallback para outro método de autenticação se o Acesso não autenticado não estiver disponível. Quando essa configuração está desativada, os usuários sempre precisam inserir suas credenciais para fazer login e acessar seus aplicativos publicados. A configuração **Acesso não autenticado (Unauthenticated Access)** em Horizon Client está oculta e desmarcada. Os usuários podem ativar o Acesso não autenticado em Horizon Client por padrão. A configuração **Acesso não autenticado (Unauthenticated Access)** está visível, ativada e desmarcada.

Tabela 3-4. VMware Horizon Client Modelo de configuração: definições de script (continuação)

Configuração	Descrição
`Account to use for Unauthenticated Access`	Especifica a conta de usuário do Acesso não autenticado que Horizon Client usa para fazer login anonimamente no servidor se a configuração de política de grupo `Enable Unauthenticated Access to the server` estiver habilitada ou se um usuário habilitar o Acesso não autenticado selecionando **Acesso não autenticado (Unauthenticated Access)** em Horizon Client . Se o Acesso não autenticado não for usado para uma conexão específica a um servidor, essa configuração será ignorada. Os usuários podem selecionar uma conta por padrão.
`Use existing client instance when connect to same server`	Determina se uma conexão é adicionada à instância Horizon Client existente com a qual o usuário já está conectado ao mesmo servidor. Essa configuração é desativada por padrão quando não está configurada.

Configurações de segurança para GPOs de cliente

As configurações de segurança incluem políticas de grupo para certificados, credenciais de logon e o recurso de logon único.

A tabela a seguir descreve as configurações de segurança no arquivo de modelo Horizon Client Configuration ADMX. Esta tabela mostra se as configurações incluem as configurações de Configuração do Computador e do Usuário ou apenas as configurações de Configuração do Computador. Para as configurações de segurança que incluem os dois tipos de configurações, a configuração do Usuário substitui a configuração equivalente da Configuração do Computador. Essas configurações aparecem na pasta **VMware Horizon Client Configuração > Configurações de segurança (Security Settings)** no Editor de Gerenciamento de Política de Grupo.

Tabela 3-5. Horizon Client Modelo de configuração: configurações de segurança

Configuração	Computador	Usuário	Descrição
`Allow command line credentials`	X		Determina se as credenciais do usuário podem ser fornecidas com as opções de linha de comando Horizon Client. Se essa configuração estiver desativada, as opções `smartCardPIN` e `password` não estarão disponíveis quando os usuários executarem Horizon Client a partir da linha de comando. Essa configuração é habilitada por padrão. O valor de Registro Windows equivalente é `AllowCmdLineCredentials`.
`Configures the SSL Proxy certificate checking behavior of the Horizon Client`	X		Determina se a verificação de certificado para conexões secundárias deve ser permitida por meio de um servidor proxy SSL para conexões de gateway seguro do Blast e de túnel seguro. Quando essa configuração não está definida (o padrão), os usuários podem alterar a configuração do proxy SSL em Horizon Client manualmente. Consulte Configurando o modo de verificação de certificado em Horizon Client. Por padrão, Horizon Client bloqueia conexões de proxy SSL para conexões de gateway seguro do Blast e de túnel seguro.
`Servers Trusted For Delegation`	X		Especifica as instâncias do Servidor de Conexão que aceitam as informações de identidade e credencial do usuário que são transmitidas quando um usuário seleciona **Fazer login como usuário atual (Log in as current user)** no menu **Opções (Options)** na barra de menus Horizon Client. Se você não especificar nenhuma instância do Servidor de Conexão, todas as instâncias do Servidor de Conexão aceitarão essas informações, a menos que a configuração de autenticação **Permitir logon como usuário atual (Allow logon as current user)** esteja desativada para a instância do Servidor de Conexão em Horizon Console. Para adicionar uma instância do Servidor de Conexão, use um dos seguintes formatos: ■ `domínio\sistema$` ■ `system$@domain.com` ■ O Nome da Entidade de Serviço (SPN) do serviço do Servidor de Conexão. O valor de Registro Windows equivalente é `BrokersTrustedForDelegation`.

Tabela 3-5. Horizon Client Modelo de configuração: configurações de segurança (continuação)

Configuração	Computador	Usuário	Descrição
`Certificate verification mode`	X		Configura o nível de verificação de certificado que Horizon Client executa. Você pode selecionar um destes modos: ■ `No Security`. Nenhuma verificação de certificado ocorre. ■ `Warn But Allow`. Se uma verificação de certificado falhar porque o servidor usa um certificado autoassinado, os usuários verão um aviso, que eles poderão ignorar. Para certificados autoassinados, o nome do certificado não é necessário para corresponder ao nome do servidor que os usuários inserem em Horizon Client. Se ocorrer qualquer outra condição de erro de certificado, Horizon Client mostrará um erro e impedirá que os usuários se conectem ao servidor. `Warn But Allow` é o valor padrão. ■ `Full Security`. Se ocorrer algum tipo de erro de certificado, os usuários não poderão se conectar ao servidor. Horizon Client exibe erros de certificado para o usuário. Quando essa configuração é definida, os usuários podem visualizar o modo de verificação de certificado selecionado em Horizon Client, mas não podem definir a configuração. A caixa de diálogo do modo de verificação de certificado informa aos usuários que um administrador bloqueou a configuração. Quando essa configuração está desativada, os usuários do Horizon Client podem selecionar um modo de verificação de certificado. Essa configuração está desativada por padrão. Para permitir que um servidor realize a seleção de certificados fornecidos por Horizon Client, o cliente deve fazer conexões HTTPS com o Servidor de Conexão ou o host do servidor de segurança. A verificação de certificado não terá suporte se você descarregar o TLS para um dispositivo intermediário que faz conexões HTTP com o Servidor de Conexão ou o host do servidor de segurança. Se você não quiser definir essa configuração como uma política de grupo, também poderá habilitar a verificação de certificado adicionando o nome do valor `CertCheckMode` a uma das seguintes chaves do Registro no computador cliente: ■ Para Windows de 32 bits: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\} \VMware\} VDM\Client\Security` ■ Para Windows de 64 bits: `HKLM\SOFTWARE\WOW6432Node\VMware, Inc.\} \VMware\} VDM\Client\Security`

Tabela 3-5. Horizon Client Modelo de configuração: configurações de segurança (continuação)

Configuração	Computador	Usuário	Descrição
			Use os seguintes valores na chave do Registro: ■ **0** implementa `No Security`. ■ **1** implementa `Warn But Allow`. ■ **2** implementa `Full Security`. Se você definir a configuração da política de grupo e a configuração `CertCheckMode` na chave do Registro Windows, a configuração da política de grupo terá precedência sobre o valor da chave do Registro. **Observação** Em uma versão futura do Horizon Client, talvez não haja suporte para o uso do Registro Windows para definir essa configuração, e a configuração de política de grupo deve ser usada.
`Default value of the 'Log in as current user' checkbox`	X	X	Especifica o valor padrão de **Fazer login como usuário atual (Log in as current user)** no menu **Opções (Options)** na barra de menus Horizon Client. Essa configuração substitui o valor padrão especificado durante a instalação do Horizon Client. Se um usuário executar Horizon Client na linha de comando e especificar a opção `logInAsCurrentUser`, esse valor substituirá essa configuração. Quando **Fazer login como usuário atual (Log in as current user)** é selecionado no menu **Opções (Options)**, as informações de identidade e credencial que o usuário forneceu ao fazer login no sistema do cliente são passadas para a instância do Servidor de Conexão e, finalmente, à área de trabalho remota ou ao aplicativo publicado. Quando a opção **Fazer login como usuário atual (Log in as current user)** está desmarcada, os usuários devem fornecer informações de identidade e credenciais várias vezes antes de poderem acessar uma área de trabalho remota ou um aplicativo publicado. Essa configuração está desativada por padrão. O valor de Registro Windows equivalente é `LogInAsCurrentUser`.

Tabela 3-5. Horizon Client Modelo de configuração: configurações de segurança (continuação)

Configuração	Computador	Usuário	Descrição
`Display option to Log in as current user`	X	X	Determina se **Fazer login como usuário atual (Log in as current user)** está visível no menu **Opções (Options)** na barra de menus Horizon Client. Quando **Fazer login como usuário atual (Log in as current user)** estiver visível, os usuários poderão marcá-lo ou desmarcá-lo e substituir seu valor padrão. Quando **Fazer login como usuário atual (Log in as current user)** está oculto, os usuários não podem substituir seu valor padrão no menu Horizon Client **Opções (Options)**. Você pode especificar o valor padrão para **Fazer login como usuário atual (Log in as current user)** usando a configuração de política `Default value of the 'Log in as current user' checkbox`. Essa configuração é habilitada por padrão. O valor de Registro Windows equivalente é `LogInAsCurrentUser_Display`.
`Enable jump list integration`	X		Determina se uma lista de atalhos aparece no ícone Horizon Client na barra de tarefas dos sistemas Windows 7 e posteriores. A lista de atalhos permite que os usuários se conectem a servidores recentes, áreas de trabalho remotas e aplicativos publicados. Se Horizon Client for compartilhado, talvez você não queira que os usuários vejam os nomes das áreas de trabalho recentes e dos aplicativos publicados. Você pode desativar a lista de atalhos desativando essa configuração. Essa configuração é habilitada por padrão. O valor equivalente do Windows Registry é `EnableJumplist`.
`Enable SSL encrypted framework channel`	X	X	Determina se o TLS está habilitado para áreas de trabalho remotas do View 5.0 e versões anteriores. Antes do View 5.0, os dados enviados pela porta TCP 32111 para a área de trabalho remota não eram criptografados. ■ **Ativar (Enable)**: ativa o TLS, mas permite o fallback para a conexão não criptografada anterior se a área de trabalho remota não tiver suporte para TLS. Por exemplo, as áreas de trabalho remotas do View 5.0 e versões anteriores não têm suporte a TLS. **Ativar (Enable)** é a configuração padrão. ■ **Desativar (Disable)**: desativa o TLS. Essa configuração pode ser útil para depuração ou se o canal não estiver sendo encapsulado e puder ser otimizado por um produto acelerador de WAN. ■ **Aplicar (Enforce)**: ativa o TLS e se recusa a se conectar a áreas de trabalho remotas que não têm suporte a TLS . O valor equivalente do Windows Registry é `EnableTicketSSLAuth`.

Tabela 3-5. Horizon Client Modelo de configuração: configurações de segurança (continuação)

Configuração	Computador	Usuário	Descrição
`Configures SSL protocols and cryptographic algorithms`	X	X	Configura a lista de codificação para restringir o uso de determinados algoritmos e protocolos criptográficos antes de estabelecer uma conexão TLS criptografada. A lista de codificação consiste em uma ou mais cadeias de caracteres de codificação separadas por dois-pontos. A cadeia de caracteres de codificação faz distinção entre maiúsculas e minúsculas. O valor padrão é **TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES** Essa cadeia de caracteres de codificação significa que o TLS v1.1 e o TLS v1.2 estão ativados e o SSL v.2.0, SSL v3.0 e TLS v1.0 estão desativados. SSL v2.0, SSL v3.0 e TLS v1.0 não são mais os protocolos aprovados e estão permanentemente desativados. Os conjuntos de codificação usam ECDHE, ECDH e RSA com AES de 128 bits ou 256 bits. O modo GCM é o preferido. Para obter mais informações, consulte http://www.openssl.org/docs/apps/ciphers.html. O valor equivalente do Windows Registry é `SSLCipherList`.
`Enable Single Sign-On for smart card authentication`	X		Determina se o logon único está habilitado para autenticação de cartão inteligente. Quando o single sign-on está ativado, o Horizon Client armazena o PIN do smart card criptografado na memória temporária antes de enviá-lo ao Servidor de Conexão. Quando o single sign-on está desativado, o Horizon Client não exibe uma caixa de diálogo PIN personalizado. O valor de Registro Windows equivalente é `EnableSmartCardSSO`.

Tabela 3-5. Horizon Client Modelo de configuração: configurações de segurança (continuação)

Configuração	Computador	Usuário	Descrição
`Ignore certificate revocation problems`	X	X	Determina se o status de revogação do certificado deve ser verificado. Quando esse GPO estiver habilitado, o Horizon Client tratará o certificado do servidor como válido, mesmo que o certificado enviado pelo servidor tenha sido revogado ou a verificação de revogação de certificado seja impossível, por exemplo, se a conexão com a Internet for limitada. Essa configuração está desativada por padrão. **Observação** Quando essa configuração está habilitada, o cliente só pode usar uma URL armazenada em cache durante a verificação do certificado do servidor. Os tipos de informações de URL armazenadas em cache podem ser Ponto de Distribuição de CRL (CDP) e Acesso a Informações de Autoridade (métodos de acesso de emissor de OCSP e CA).
`Unlock remote sessions when the client machine is unlocked`	X	X	Determina se o recurso Desbloqueio Recursivo está ativado. O recurso Desbloqueio Recursivo desbloqueia todas as sessões remotas após o desbloqueio da máquina cliente. Esse recurso se aplica somente depois que um usuário faz login no servidor com o recurso Fazer login como usuário atual. Essa configuração é habilitada por padrão.

As configurações a seguir aparecem na pasta **VMware Horizon Client Configuração > Configurações de segurança (Security Settings) > Configurações NTLM (NTLM Settings)** no Editor de Gerenciamento de Política de Grupo.

Tabela 3-6. Horizon Client Modelo de configuração: configurações de segurança, configurações de autenticação NTLM

Configuração	Computador	Usuário	Descrição
`Allow NTLM Authentication`	X		Quando essa configuração está ativada, a autenticação NTLM é permitida com o recurso **Fazer login como usuário atual (Log in as current user)**. Quando essa configuração está desativada, a autenticação NTLM não é usada para nenhum servidor. Quando essa configuração está ativada, você pode selecionar **Sim (Yes)** ou **Não (No)** no menu suspenso **Permitir fallback de Kerberos para NTLM (Allow fallback from Kerberos to NTLM)**. ■ Se você selecionar **Sim (Yes)**, a autenticação NTLM poderá ser usada sempre que o cliente não conseguir recuperar um tíquete Kerberos para o servidor. ■ Se você selecionar **Não (No)**, a autenticação NTLM será permitida apenas para servidores listados na configuração de política de grupo **Sempre usar servidores NTLM (Always use NTLM servers)**. Quando essa configuração não está definida, a autenticação NTLM é permitida para os servidores listados na configuração de política de grupo **Sempre usar servidores NTLM (Always use NTLM servers)**. Para usar a autenticação NTLM, o certificado SSL do servidor deve ser válido e as políticas Windows não devem restringir o uso de NTLM. Para obter informações sobre como configurar o fallback de Kerberos para NTLM em uma instância do Servidor de Conexão, consulte "Usando o recurso Fazer login como usuário atual disponível com Horizon Client com base em Windows" no documento *VMware Horizon Console Administração*.
`Always use NTLM for servers`	X		Quando essa configuração está ativada, o recurso **Fazer login como usuário atual (Log in as current user)** sempre usa a autenticação NTLM para os servidores listados. Para criar a lista de servidores, clique em **Mostrar (Show)** e digite o nome do servidor na coluna **Valor (Value)**. O formato de nomenclatura para servidores é o nome de domínio totalmente qualificado (FQDN).

Configurações de RDP para GPOs de cliente

Você pode definir as configurações de política de grupo para opções como o redirecionamento de áudio, impressoras, portas e outros dispositivos ao usar o protocolo de exibição Microsoft RDP.

A tabela a seguir descreve as configurações do Protocolo de Área de Trabalho Remota (RDP) no arquivo de modelo Horizon Client Configuração ADMX. Todas as configurações de RDP são definições de Configuração do Usuário. As configurações aparecem na pasta **VMware Horizon Client Configuração > Configurações de RDP (RDP Settings)** no Editor de Gerenciamento de Política de Grupo.

Tabela 3-7. Horizon Client Modelo administrativo de configuração: configurações de RDP

Configuração	Descrição
`Audio redirection`	Determina se as informações de áudio reproduzidas na área de trabalho remota são redirecionadas. Selecione uma das seguintes configurações: ■ **Desativar áudio (Disable Audio)**: o áudio está desativado. ■ **Reproduzir na VM (necessário para suporte a VoIP USB)**: o áudio é reproduzido na área de trabalho remota. Essa configuração requer um dispositivo de áudio USB compartilhado para fornecer som no cliente. ■ **Redirecionar para o cliente (Redirect to client)**: o áudio é redirecionado para o cliente. Essa configuração é o modo padrão. Essa configuração se aplica somente ao áudio RDP. O áudio redirecionado por meio do MMR é reproduzido no cliente.
`Enable audio capture redirection`	Determina se o dispositivo de entrada de áudio padrão é redirecionado do cliente para a sessão remota. Quando essa configuração está ativada, o dispositivo de gravação de áudio no cliente aparece na área de trabalho remota e pode gravar a entrada de áudio. A configuração padrão é desativada.
`Bitmap cache file size in` *unidade* `for` *número* `bpp bitmaps`	Especifica o tamanho do cache de bitmap, em kilobytes ou megabytes, a ser usado para configurações de cor de bitmap de bits por pixel (bpp) específicas. São fornecidas versões separadas dessa configuração para as seguintes combinações de unidade e bpp: ■ MB/8bpp ■ MB/16bpp ■ MB/24bpp ■ MB/32bpp
`In-memory bitmap cache size in KB for 8bpp bitmaps`	Especifica o tamanho, em kilobytes, do cache de bitmap de RAM a ser usado para a configuração de cor de 8 bits por pixel. Se ScaleBitmapCachesByBPP for true (o padrão), esse tamanho de cache será multiplicado pelos bytes por pixel para determinar o tamanho real do cache de RAM. Quando essa configuração estiver habilitada, insira um tamanho em kilobytes.
`Bitmap caching/cache persistence active`	Determina se o cache de bitmap persistente é usado (ativo). O armazenamento em cache persistente de bitmaps pode melhorar o desempenho, mas requer espaço em disco adicional.
`Color depth`	Especifica a profundidade de cor da área de trabalho remota. Selecione uma das configurações disponíveis: ■ 8 bits ■ 15 bits ■ 16 bits ■ 24 bits ■ 32 bits

Tabela 3-7. Horizon Client Modelo administrativo de configuração: configurações de RDP (continuação)

Configuração	Descrição
`Cursor shadow`	Determina se uma sombra aparece sob o ponteiro na área de trabalho remota.
`Desktop background`	Determina se o plano de fundo da área de trabalho aparece quando os clientes se conectam a uma área de trabalho remota.
`Desktop composition`	Determina se a composição da área de trabalho está habilitada na área de trabalho remota. Quando a composição da área de trabalho está habilitada, as janelas individuais não são mais desenhadas diretamente na tela ou no dispositivo de exibição principal, como acontecia nas versões anteriores do Microsoft Windows. Em vez disso, o desenho é redirecionado para superfícies fora da tela na memória de vídeo, que são renderizadas em uma imagem da área de trabalho e apresentadas na tela.
`Enable compression`	Determina se os dados RDP são compactados. Essa configuração é habilitada por padrão.
`Enable RDP Auto-Reconnect`	Determina se o componente do cliente RDP tenta se reconectar a uma área de trabalho remota após uma falha de conexão do protocolo RDP. Essa configuração não terá efeito se a opção **Usar conexão de túnel seguro com a área de trabalho (Use secure tunnel connection to desktop)** estiver ativada em Horizon Console. Essa configuração está desativada por padrão.
`Font smoothing`	Determina se a suavização de serrilhado é aplicada às fontes na área de trabalho remota.
`Menu and window animation`	Determina se a animação para menus e janelas é habilitada quando os clientes se conectam a uma área de trabalho remota.
`Redirect clipboard`	Determina se as informações da área de transferência local são redirecionadas quando os clientes se conectam à área de trabalho remota.
`Redirect drives`	Determina se as unidades de disco locais são redirecionadas quando os clientes se conectam à área de trabalho remota. Por padrão, as unidades locais são redirecionadas. Habilitar essa configuração, ou deixá-la sem configuração, permite que os dados na unidade redirecionada na área de trabalho remota sejam copiados para a unidade no computador cliente. Desabilite essa configuração se permitir que os dados passem da área de trabalho remota para os computadores cliente dos usuários representar um possível risco de segurança na sua implantação. Outra abordagem é desabilitar o redirecionamento de pastas na máquina virtual de área de trabalho remota habilitando a configuração de política de grupo da Microsoft Windows, `Do not allow drive redirection`. A configuração `Redirect drives` se aplica somente ao RDP.
`Redirect printers`	Determina se as impressoras locais são redirecionadas quando os clientes se conectam à área de trabalho remota.
`Redirect serial ports`	Determina se as portas COM locais são redirecionadas quando os clientes se conectam à área de trabalho remota.
`Redirect smart cards`	Determina se os cartões inteligentes locais são redirecionados quando os clientes se conectam à área de trabalho remota. **Observação** Essa configuração se aplica a conexões RDP e PCoIP.

Tabela 3-7. Horizon Client Modelo administrativo de configuração: configurações de RDP (continuação)

Configuração	Descrição
`Redirect supported plug-and-play devices`	Determina se os dispositivos plug-and-play e de ponto de venda locais são redirecionados quando os clientes se conectam à área de trabalho remota. Esse comportamento é diferente do redirecionamento que o componente Redirecionamento USB do agente gerencia.
`Shadow bitmaps`	Determina se os bitmaps estão sombreados. Essa configuração não tem efeito no modo de tela inteira.
`Show contents of window while dragging`	Determina se o conteúdo da pasta aparece quando os usuários arrastam uma pasta para um novo local.
`Themes`	Determina se os temas aparecem quando os clientes se conectam a uma área de trabalho remota.
`Windows key combination redirection`	Determina onde as combinações de teclas Windows são aplicadas. Essa configuração permite que você envie combinações de teclas para a máquina virtual remota ou aplique combinações de teclas localmente. As combinações de teclas são aplicadas localmente por padrão.
`Enable Credential Security Service Provider`	Especifica se a conexão da área de trabalho remota usa a Autenticação no Nível da Rede (NLA). Se o sistema operacional convidado exigir NLA para conexões de área de trabalho remota, você deverá habilitar essa configuração ou Horizon Client poderá não se conectar à área de trabalho remota. Além de habilitar essa configuração, você também deve verificar se as seguintes condições são atendidas: ■ Os sistemas operacionais cliente e convidado oferecem suporte a NLA. ■ As conexões de cliente diretas são habilitadas para a instância do Servidor de Conexão. As conexões em túnel não são compatíveis com o NLA.

Configurações gerais para GPOs de cliente

As configurações gerais incluem opções de proxy, encaminhamento de fuso horário, aceleração de multimídia e outras configurações de exibição.

A tabela a seguir descreve as configurações gerais no arquivo de modelo Horizon Client Configuration ADMX. As configurações gerais incluem as configurações de Configuração do Computador e Configuração do Usuário. A definição de Configuração do Usuário substitui a definição equivalente de Configuração do Computador. As configurações aparecem na pasta **VMware Horizon Client Configuração** no Editor de Gerenciamento de Política de Grupo.

Tabela 3-8. Horizon Client Modelo de configuração: configurações gerais

Configuração	Computador	Usuário	Descrição
`Allow Blast connections to use operating system proxy settings`	X		Configura o uso do servidor proxy para conexões VMware Blast. Quando essa configuração está ativada, VMware Blast pode se conectar por meio de um servidor proxy. Quando essa configuração está desativada, VMware Blast não pode usar um servidor proxy. Quando essa configuração não está definida (o padrão), os usuários podem definir se as conexões do VMware Blast podem usar um servidor proxy na interface do usuário do Horizon Client. Consulte Configurar opções do VMware Blast.
`Allow data sharing`	X		Quando essa configuração está ativada, a configuração do modo de compartilhamento de dados na interface do usuário do Horizon Client é definida como Ativado e os usuários finais não podem alterar a configuração. Quando essa configuração está desativada, a configuração do modo de compartilhamento de dados na interface do usuário do Horizon Client é definida como Desativada e os usuários finais não podem alterar a configuração. Quando essa configuração não está definida (o padrão), os usuários finais podem alterar a configuração do modo de compartilhamento de dados na interface do usuário do Horizon Client.
`Allow display scaling`	X	X	Quando essa configuração está habilitada, o recurso de dimensionamento de vídeo é habilitado para todas as áreas de trabalho remotas e aplicativos publicados. Quando essa configuração está desativada, o recurso de dimensionamento de exibição é desativado para todas as áreas de trabalho remotas e aplicativos publicados. Se essa configuração não estiver definida (a configuração padrão), os usuários finais poderão ativar e desativar o dimensionamento de exibição na interface do usuário do Horizon Client. Você também pode ocultar a preferência de dimensionamento de exibição na interface do usuário do Horizon Client ativando a configuração de política de grupo **Tamanho do convidado bloqueado (Locked Guest Size)**.
`Allow H.264 Decoding`	X		Configura a decodificação H.264 para o protocolo VMware Blast. Quando essa configuração está ativada, a decodificação H.264 se torna a opção preferencial. Quando essa configuração está desativada, a decodificação H.264 nunca é usada. Quando essa configuração não está definida, os usuários podem optar por habilitar a decodificação H.264. Consulte Configurar opções do VMware Blast.

Tabela 3-8. Horizon Client Modelo de configuração: configurações gerais (continuação)

Configuração	Computador	Usuário	Descrição
`Allow H.264 high color accuracy`	X		Configura o modo de alta precisão de cores para H.264. Essa configuração terá efeito somente se a decodificação H.264 estiver ativada. Quando essa configuração não está definida, os usuários podem optar por ativar o modo de alta precisão de cores. Consulte Configurar opções do VMware Blast.
`Allow HEVC Decoding`	X		Configura a decodificação HEVC (também conhecida como H.265) para o protocolo VMware Blast. Quando essa configuração está habilitada, a decodificação HEVC se torna a opção preferida. Quando essa configuração está desativada, a decodificação HEVC nunca é usada. Quando essa configuração não está definida, os usuários podem optar por habilitar a decodificação HEVC. Consulte Configurar opções do VMware Blast.
`Allow user to skip Horizon Client update`	X		Especifica se os usuários podem clicar no botão **Ignorar (Skip)** na janela de atualização Horizon Client. Se os usuários clicarem em **Ignorar (Skip)**, eles não verão outra notificação de atualização até que a próxima versão Horizon Client esteja disponível.
`Always hide the remote floating language (IME) bar for Hosted Apps`	X	X	Força a desativação da barra de idioma flutuante para sessões do aplicativo. Quando essa configuração está habilitada, a barra de idioma flutuante nunca é mostrada em uma sessão de aplicativo publicada, independentemente de o recurso IME local estar habilitado. Quando essa configuração está desativada, a barra de idiomas flutuante é mostrada somente se o recurso IME local estiver desativado. Essa configuração está desativada por padrão.
`Always on top`		X	Determina se a janela Horizon Client é sempre a janela mais alta. A ativação dessa configuração evita que a barra de tarefas Windows oculte uma janela Horizon Client de tela inteira. Essa configuração está desativada por padrão.
`Automatic input focus in a virtual desktop window`	X	X	Quando essa configuração está ativada, o Horizon Client envia a entrada para a área de trabalho remota automaticamente quando um usuário traz a área de trabalho remota para a frente. Em outras palavras, o foco não está no quadro da janela e o usuário não precisa clicar dentro da janela da área de trabalho remota para mover o foco.
`Automatically check for updates`	X		Especifica se as atualizações de software de Horizon Client devem ser verificadas automaticamente. Essa configuração controla a caixa de seleção **Verificar atualizações e mostrar notificação de emblema (Check for updates and show badge notification)** na janela de atualização Horizon Client. Essa configuração é habilitada por padrão.

Tabela 3-8. Horizon Client Modelo de configuração: configurações gerais (continuação)

Configuração	Computador	Usuário	Descrição
`Automatically install shortcuts when configured on the Horizon server`	X	X	Quando os atalhos do aplicativo publicado e da área de trabalho remota são configurados em uma instância do Servidor de Conexão, essa configuração especifica como e se os atalhos são instalados em máquinas cliente quando os usuários se conectam ao servidor. Quando essa configuração está habilitada, os atalhos são instalados nas máquinas cliente. Os usuários não são solicitados a instalar os atalhos. Quando essa configuração está desativada, os atalhos nunca são instalados nas máquinas cliente. Os usuários não são solicitados a instalar os atalhos. Os usuários são solicitados a instalar os atalhos por padrão.
`Automatically synchronize the keypad, scroll and caps lock keys`	X		Quando essa configuração está habilitada, os estados de alternância das teclas Num Lock, Scroll Lock e Caps Lock são sincronizados do dispositivo do cliente para uma área de trabalho remota. Em Horizon Client, a caixa de seleção da configuração **Sincronizar automaticamente o teclado, as teclas de rolagem e as teclas cap lock (Automatically synchronize the keypad, scroll and cap lock keys)** está marcada, e a configuração fica esmaecida. Quando essa configuração está desativada, os estados de alternância da tecla de bloqueio são sincronizados da área de trabalho remota para o dispositivo cliente. No Horizon Client, a caixa de seleção da configuração **Sincronizar automaticamente o teclado, as teclas de rolagem e as teclas cap lock (Automatically synchronize the keypad, scroll and cap lock keys)** está desmarcada e a configuração está esmaecida. Quando essa configuração está ativada ou desativada, os usuários não podem modificar a configuração **Sincronizar automaticamente o teclado, as teclas de rolagem e as teclas cap lock (Automatically synchronize the keypad, scroll and cap lock keys)** em Horizon Client. Quando essa configuração não está definida, um usuário pode ativar ou desativar a sincronização da tecla de bloqueio para uma área de trabalho remota definindo a configuração **Sincronizar automaticamente o teclado, as teclas de rolagem e as teclas de bloqueio de cap (Automatically synchronize the keypad, scroll and cap lock keys)** em Horizon Client. Consulte Configurar a sincronização da chave de bloqueio. Essa configuração não é definida por padrão.

Tabela 3-8. Horizon Client Modelo de configuração: configurações gerais (continuação)

Configuração	Computador	Usuário	Descrição
`Block multiple Horizon Client instances per Windows session`	X		Impede que um usuário inicie várias instâncias Horizon Client durante uma sessão Windows. Quando essa configuração está ativada, o Horizon Client é executado no modo de instância única e um usuário não pode iniciar várias instâncias do Horizon Client em uma sessão do Windows. Quando essa configuração está desativada, um usuário pode iniciar várias instâncias do Horizon Client em uma sessão do Windows. Essa configuração está desativada por padrão.
`Configure maximum latency for mouse coalescing`	X		Define a latência máxima permitida, em milissegundos, ao unir eventos de movimento do mouse. Os valores válidos são de 0 a 50. Um valor de 0 desativa o recurso. A união de eventos de movimento do mouse pode reduzir o uso de largura de banda do cliente para o agente, mas pode adicionar uma latência menor ao movimento do mouse. Essa configuração está desativada por padrão.
`Custom error screen footer`	X		Permite adicionar texto de ajuda personalizado na parte inferior de todas as Horizon Client mensagens de erro. Você deve fornecer o texto de ajuda em um arquivo de texto simples (`.txt`) no sistema do cliente local. O arquivo de texto pode conter até 2.048 caracteres, incluindo caracteres de controle. Há suporte para a codificação ANSI e Unicode. Quando essa configuração está ativada, você especifica o caminho completo para o arquivo que contém o texto de ajuda personalizado na caixa de texto fornecida, por exemplo, `C:\myDocs\errorFooter.txt`. Essa configuração está desativada por padrão.
`Default value of the "Hide the selector after launching an item" check box`	X	X	Define se a caixa de seleção **Ocultar o seletor após iniciar um item (Hide the selector after launching an item)** está marcada por padrão. Essa configuração está desativada por padrão.
`Disable desktop disconnect messages`	X	X	Especifica se as mensagens que normalmente são exibidas após a desconexão da área de trabalho remota estão desativadas. Essas mensagens são exibidas por padrão.

Tabela 3-8. Horizon Client Modelo de configuração: configurações gerais (continuação)

Configuração	Computador	Usuário	Descrição
`Disable sharing files and folders`		X	Especifica se a funcionalidade de redirecionamento de unidade do cliente está disponível em Horizon Client. Quando essa configuração está habilitada, toda a funcionalidade de redirecionamento de unidade do cliente é desativada em Horizon Client, incluindo a capacidade de abrir arquivos locais com aplicativos publicados. Além disso, os seguintes elementos estão ocultos na interface do usuário do Horizon Client: ■ Painel Compartilhamento na caixa de diálogo Configurações. ■ item **Compartilhar pastas (Share Folders)** no menu **Opção (Option)** em uma área de trabalho remota. ■ Item **Compartilhando (Sharing)** para Horizon Client na bandeja do sistema. ■ A caixa de diálogo Compartilhamento que aparece na primeira vez que você se conecta a uma área de trabalho remota ou aplicativo depois de se conectar a um servidor. Quando essa configuração está desativada, o recurso de redirecionamento de unidade do cliente fica totalmente funcional. Essa configuração está desativada por padrão.
`Disable time zone forwarding`	X		Determina se a sincronização de fuso horário entre a área de trabalho remota e o cliente conectado está desativada.
`Disable toast notifications`	X	X	Determina se as notificações do sistema devem ser desabilitadas de Horizon Client. Habilite essa configuração se não quiser que o usuário veja notificações do sistema no canto da tela. **Observação** Se você habilitar essa configuração, o usuário não verá um aviso de cinco minutos quando a função Tempo limite da sessão estiver ativa.
`Disallow passing through client information in a nested session`	X		Especifica se Horizon Client é impedido de transmitir informações do cliente em uma sessão aninhada. Quando ativado, se Horizon Client estiver em execução dentro de uma sessão remota, ele enviará as informações reais do cliente físico em vez das informações do dispositivo da máquina virtual. Essa configuração se aplica às seguintes informações do cliente: nome e domínio do dispositivo, tipo de cliente, endereço IP e endereço MAC. Essa configuração é desativada por padrão, o que significa que a passagem de informações do cliente em uma sessão aninhada é permitida.

Tabela 3-8. Horizon Client Modelo de configuração: configurações gerais (continuação)

Configuração	Computador	Usuário	Descrição
`Display modifier function key`	X	X	Especifica a combinação de modificador de alternância e tecla de função que um usuário pode pressionar que, ao capturar e injetar entrada em uma sessão de PCoIP ou de área de trabalho remota VMware Blast, altera a configuração de exibição na máquina cliente. Quando essa configuração não está definida (a configuração padrão), o usuário final deve usar o mouse para soltar a área de trabalho remota e pressionar a tecla de logotipo Windows + P para selecionar um modo de exibição de apresentação. Essa configuração não se aplica a sessões de aplicativo publicadas.
`Disable opening local files in hosted applications`		X	Especifica se Horizon Client registra manipuladores locais para as extensões de arquivo compatíveis com os aplicativos hospedados. Quando essa configuração está ativada, Horizon Client não registra nenhum manipulador de extensão de arquivo e não permite que o usuário substitua a configuração. Quando essa configuração está desativada, Horizon Client sempre registra manipuladores de extensão de arquivo. Por padrão, os manipuladores de extensão de arquivo são registrados, mas os usuários podem desativar o recurso na interface do usuário do Horizon Client usando a configuração **Ativar a capacidade de abrir um arquivo local com um aplicativo remoto do sistema de arquivos local (Turn on the ability to open a local file with a remote application from the local file system)** no painel Compartilhamento na caixa de diálogo Configurações. Para obter mais informações, consulte Compartilhar pastas e unidades locais. Essa configuração está desativada por padrão.
`Don't check monitor alignment on spanning`		X	Por padrão, a área de trabalho do cliente não abrange vários monitores se as telas não formarem um retângulo exato quando combinadas. Ative essa configuração para substituir o padrão. Essa configuração está desativada por padrão.
`Enable multi-media acceleration`		X	Determina se o redirecionamento de multimídia (MMR) está ativado no cliente. O MMR não funcionará corretamente se o hardware de exibição de vídeo Horizon Client não tiver suporte para sobreposição.
`Enable relative mouse`	X	X	Ativa o mouse relativo ao usar o protocolo de exibição PCoIP. O modo de mouse relativo melhora o comportamento do mouse para determinados aplicativos gráficos e jogos. Se a área de trabalho remota não oferecer suporte ao mouse relativo, essa configuração não será usada. Essa configuração está desativada por padrão.

Tabela 3-8. Horizon Client Modelo de configuração: configurações gerais (continuação)

Configuração	Computador	Usuário	Descrição
`Enable the shade`		X	Determina se a barra de menus de sombra na parte superior da janela Horizon Client está visível. Essa configuração é habilitada por padrão. **Observação** A barra de menus da cortina está desativada por padrão para o modo de quiosque.
`Enable Horizon Client online update`	X		Habilita o recurso de atualização online. Essa configuração é habilitada por padrão. **Observação** Você também pode desativar o recurso de atualização online definindo a propriedade `AUTO_UPDATE_ENABLED` como 0 ao instalar o Horizon Client a partir da linha de comando. Para obter mais informações, consulte Instalar o Horizon Client a partir da linha de comando.
`Enable Split Mks Window`	X		Essa configuração fornece uma solução temporária para problemas de exibição de vários monitores encontrados ao usar o Horizon Client para o Windows 2106 ou posterior com aplicativos de comunicações unificadas (UC), como Cisco WebEx e Zoom. Essa configuração é habilitada por padrão. Se o seu fornecedor de UC ainda não tiver fornecido uma atualização de aplicativo que corrija o problema de exibição, você poderá implementar uma solução temporária desativando essa configuração. Desativar essa configuração desativa a hierarquia de janelas padrão e faz com que as janelas sejam exibidas em relação à caixa delimitadora de todos os monitores em uma configuração de vários monitores. Para obter mais informações, consulte o VMware artigo da Base de conhecimento (KB) 85400. **Observação** Use esta solução alternativa apenas como uma correção temporária até que você possa instalar a versão atualizada do aplicativo de UC que corrige o problema de exibição permanentemente. Depois de instalar o aplicativo de UC atualizado, ative a hierarquia padrão do Windows novamente ativando essa configuração no GPO.

Tabela 3-8. Horizon Client Modelo de configuração: configurações gerais (continuação)

Configuração	Computador	Usuário	Descrição
`Hide items in application context menu`	X	X	Use essa configuração para ocultar itens no menu de contexto que aparece quando você clica com o botão direito do mouse em um aplicativo publicado na área de trabalho e na janela do seletor de aplicativos. Quando essa configuração está ativada, você pode configurar as seguintes opções: ■ **Ocultar configurações (Hide Settings)** -- Selecione **Sim (Yes)** para ocultar o item **Configurações (Settings)** no menu de contexto. ■ **Ocultar Criar atalho para a área de trabalho (Hide Create Shortcut to Desktop)** -- Selecione **Sim (Yes)** para ocultar o item **Criar atalho para a área de trabalho (Create Shortcut to Desktop)** no menu de contexto. ■ **Ocultar Adicionar ao menu Iniciar (Hide Add to Start Menu)** -- Selecione **Sim (Yes)** para ocultar o item **Adicionar ao menu Iniciar (Add to Start Menu)** no menu de contexto. ■ **Ocultar marcar como favorito (Hide Mark as Favorite)** -- Selecione **Sim (Yes)** para ocultar o item **Marcar como favorito (Mark as Favorite)** no menu de contexto. Essa configuração está desativada por padrão.
`Hide items in desktop context menu`	X	X	Use essa configuração para ocultar itens no menu de contexto que aparece quando você clica com o botão direito do mouse em uma área de trabalho remota na área de trabalho e na janela do seletor de aplicativos. Quando essa configuração está ativada, você pode configurar as seguintes opções: ■ **Ocultar área de trabalho redefinida (Hide Reset Desktop)** -- Selecione **Sim (Yes)** para ocultar o item **Redefinir área de trabalho (Reset Desktop)** no menu de contexto. ■ **Ocultar reinicialização da área de trabalho (Hide Restart Desktop)** -- Selecione **Sim (Yes)** para ocultar o item **Reiniciar área de trabalho (Restart Desktop)** no menu de contexto. ■ **Ocultar exibição (Hide Display)** -- Selecione **Sim (Yes)** para ocultar o item **Exibir (Display)** no menu de contexto. ■ **Ocultar configurações (Hide Settings)** -- Selecione **Sim (Yes)** para ocultar o item **Configurações (Settings)** no menu de contexto. ■ **Ocultar Criar atalho para a área de trabalho (Hide Create Shortcut to Desktop)** -- Selecione **Sim (Yes)** para ocultar o item **Criar atalho para a área de trabalho (Create Shortcut to Desktop)** no menu de contexto. ■ **Ocultar Adicionar ao menu Iniciar (Hide Add to Start Menu)** -- Selecione **Sim (Yes)** para ocultar o item **Adicionar ao menu Iniciar (Add to Start Menu)** no menu de contexto. ■ **Ocultar marcar como favorito (Hide Mark as Favorite)** -- Selecione **Sim (Yes)** para ocultar o item **Marcar como favorito (Mark as Favorite)** no menu de contexto. Essa configuração está desativada por padrão.

Tabela 3-8. Horizon Client Modelo de configuração: configurações gerais (continuação)

Configuração	Computador	Usuário	Descrição
`Hide items in desktop toolbar`	X	X	Use essa configuração para ocultar itens na barra de menus em uma janela da área de trabalho remota. Quando essa configuração está habilitada, você pode configurar as seguintes opções. ■ **Ocultar ajuda (Hide Help)** -- Selecione **Sim (Yes)** para ocultar o item **Ajuda (Help)** no menu **Opções (Options)**. ■ **Ocultar Redefinir área de trabalho (Hide Reset Desktop)** -- Selecione **Sim (Yes)** para ocultar o item **Redefinir área de trabalho (Reset Desktop)** do menu **Opções (Options)**. ■ **Ocultar reinicialização da área de trabalho (Hide Restart Desktop)** -- Selecione **Sim (Yes)** para ocultar o item **Reiniciar área de trabalho (Restart Desktop)** do menu **Opções (Options)**. ■ **Ocultar dispositivo USB conectado (Hide Connect USB Device)** -- Selecione **Sim (Yes)** para ocultar o menu **Conectar dispositivo USB (Connect USB Device)** na barra de menus. Essa configuração está desativada por padrão.
`Hide items in system tray menu`	X	X	Use essa configuração para ocultar itens no menu de contexto que aparece quando você clica com o botão direito do mouse no ícone Horizon Client na bandeja do sistema no sistema do cliente local. Quando essa configuração está habilitada, você pode configurar as seguintes opções. ■ **Ocultar configurações (Hide Settings)** -- Selecione **Sim (Yes)** para ocultar o item Horizon Client **Configurações (Settings)**. Essa configuração está desativada por padrão.
`Hide items in the client toolbar menu`	X	X	Use essa configuração para ocultar itens na barra de ferramentas na parte superior da área de trabalho e na janela do seletor de aplicativos. Quando essa configuração está habilitada, você pode configurar as seguintes opções. ■ **Alternar Ocultar Favoritos (Hide Favorites Toggle)** -- Selecione **Sim (Yes)** para ocultar o ícone **Mostrar Favoritos (Show Favorites)** (estrela). ■ **Ocultar engrenagem de configurações (Hide Settings Gear)** -- Selecione **Sim (Yes)** para ocultar o ícone **Configurações (Settings)** (engrenagem). Essa configuração está desativada por padrão.
`Hotkey combination to grab input focus`	X	X	Configura uma combinação de teclas de atalho para obter o foco de entrada para a última sessão de PCoIP ou de área de trabalho remota VMware Blast usada. A tecla de atalho consiste em uma ou duas teclas modificadoras e uma tecla de letra. Quando essa configuração está desativada ou não é configurada, o usuário pode obter o foco clicando dentro da janela da área de trabalho remota. Essa configuração não é definida por padrão.

Tabela 3-8. Horizon Client Modelo de configuração: configurações gerais (continuação)

Configuração	Computador	Usuário	Descrição
`Hotkey combination to release input focus`	X	X	Configura uma combinação de teclas de atalho para liberar o foco de entrada de uma sessão de PCoIP ou VMware Blast de área de trabalho remota. A tecla de atalho consiste em uma ou duas teclas modificadoras e uma tecla de função. Quando a caixa de seleção **Minimizar a área de trabalho virtual em tela cheia após liberar o foco de entrada (Minimize the fullscreen virtual desktop after release input focus)** está marcada, os usuários podem pressionar qualquer tecla de atalho configurada para liberar o foco de entrada (por exemplo, Ctrl+Shift+F5) para minimizar a área de trabalho remota quando a área de trabalho remota estiver no modo de tela inteira. Por padrão, Ctrl+Shift+F5 minimiza a janela da área de trabalho remota quando a área de trabalho está no modo de tela inteira sem nenhuma configuração. Quando essa configuração está desativada ou não configurada, o usuário pode liberar o foco pressionando Ctrl+Alt ou clicando fora da janela da área de trabalho remota. Essa configuração não é definida por padrão.
`Pin the shade`		X	Determina se o pino na cortina na parte superior da janela Horizon Client está ativado e a ocultação automática da barra de menus não ocorre. Essa configuração não terá efeito se a sombra estiver desativada. Essa configuração é habilitada por padrão.
`Save resolution and DPI to server`	X		Determina se Horizon Client salva a resolução de exibição personalizada e as configurações de dimensionamento de exibição no servidor. Para obter informações sobre como personalizar a resolução da tela e as configurações de dimensionamento da tela para uma área de trabalho remota, consulte Personalizar a resolução de vídeo e o dimensionamento de vídeo para uma área de trabalho remota. Quando essa configuração está habilitada e a resolução ou o dimensionamento da tela foi personalizado para uma área de trabalho remota, sempre que um usuário abre a área de trabalho remota, as configurações personalizadas são aplicadas automaticamente, independentemente do dispositivo cliente que o usuário usa para fazer login no a área de trabalho remota. Essa configuração está desativada por padrão.
`Tunnel proxy bypass address list`	X		Especifica uma lista de endereços de túnel. O servidor proxy não é usado para esses endereços. Use um ponto-e-vírgula (;) para separar várias entradas.
`Update message pop-up`	X		Especifica se a mensagem pop-up de atualização será exibida automaticamente para os usuários finais quando uma nova versão do Horizon Client estiver disponível. Essa configuração controla a caixa de seleção **Mostrar mensagem pop-up quando houver uma atualização (Show pop-up message when there is an update)** na janela de atualização Horizon Client. Essa configuração está desativada por padrão.

Tabela 3-8. Horizon Client Modelo de configuração: configurações gerais (continuação)

Configuração	Computador	Usuário	Descrição
`URL for Horizon Client online help`	X		Especifica uma URL alternativa da qual Horizon Client pode recuperar páginas de ajuda. Essa configuração deve ser usada em ambientes que não podem recuperar o sistema de ajuda hospedado remotamente porque não têm acesso à Internet.
`URL for Horizon Client online update`	X		Especifica uma URL alternativa da qual Horizon Client pode recuperar atualizações. Essa configuração deve ser usada em um ambiente que define seu próprio centro de atualizações privado/pessoal. Se não estiver ativado, o servidor de atualização oficial VMware será usado.

Configurações USB para GPOs de cliente

Você pode definir as configurações de política de USB para Horizon Agent e Horizon Client. Na conexão, Horizon Client baixa as configurações de política USB de Horizon Agent e usa essas configurações, juntamente com as configurações de política USB Horizon Client, para determinar quais dispositivos estão disponíveis para redirecionamento da máquina host.

A tabela a seguir descreve cada configuração de política para dividir dispositivos USB compostos no arquivo de modelo Horizon Client Configuração ADMX. As configurações se aplicam no nível do computador. As configurações do GPO no nível do computador têm precedência sobre o registro em `HKLM\Software\Policies\VMware, Inc.\}\VMware\} VDM\Client\USB`. As configurações aparecem na pasta **VMware Horizon Client Configuração > Exibir configuração USB (View USB Configuration)** no Editor de Gerenciamento de Política de Grupo.

Para obter mais informações sobre como usar políticas para controlar o redirecionamento de USB, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.

Tabela 3-9. Horizon Client Modelo de configuração: Configurações de divisão USB

Configuração	Descrição
`Allow Auto Device Splitting`	Permitir a divisão automática de dispositivos USB compostos. O valor padrão é indefinido, o que equivale a **`false`**.
`Exclude Vid/Pid Device From Split`	Exclui da divisão um dispositivo USB composto especificado pelo fornecedor e pelas IDs do produto. O formato da configuração é `_pid-`*xxx1*`;vid-`*yyy2*`[_pid-`*xxx2*`vid-`*yyy2*`]..`. Você deve especificar os números de ID em hexadecimal. Você pode usar o caractere curinga (**`*`**) no lugar de dígitos individuais em uma ID. Por exemplo: **`vid-0781_pid-55**`** O valor padrão é indefinido.
`Split Vid/Pid Device`	Trata os componentes de um dispositivo USB composto especificado pelo fornecedor e as IDs do produto como dispositivos separados. O formato da configuração é xxxx`(exintf:`aaaa`;exintf:`zz`)[vid-`*ww*`]_pid-` Você pode usar a palavra-chave `exintf` para excluir componentes do redirecionamento especificando seu número de interface. Você deve especificar os números de ID em hexadecimal e os números de interface em decimal, incluindo qualquer zero à esquerda. Você pode usar o caractere curinga (**`*`**) no lugar de dígitos individuais em uma ID. Por exemplo: **`vid-0781_pid-554c(exintf:01;exintf:02)`** **Observação** O Horizon não inclui automaticamente os componentes que você não excluiu explicitamente. Você deve especificar uma política de filtro como `Include Vid/Pid Device` para incluir esses componentes. O valor padrão é indefinido.

A tabela a seguir descreve as configurações de política no Horizon Client arquivo de modelo ADMX de configuração para filtrar dispositivos USB. As configurações se aplicam no nível do computador. As configurações do GPO no nível do computador têm precedência sobre o registro em `HKLM\Software\Policies\VMware, Inc.\}\VMware\} VDM\Client\USB`.

Para obter mais informações sobre como definir as configurações de política de filtro para redirecionamento de USB, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.

Tabela 3-10. Horizon Client Modelo de configuração: Configurações de filtragem USB

Configuração	Descrição
`Allow Audio Input Devices`	Permite que os dispositivos de entrada de áudio sejam redirecionados. O valor padrão é indefinido, o que equivale a **`true`**. Essa configuração aparece na pasta **VMware Horizon Client Configuração > Exibir configuração USB (View USB Configuration)** no Editor de Gerenciamento de Política de Grupo.
`Allow Audio Output Devices`	Permite que os dispositivos de saída de áudio sejam redirecionados. O valor padrão é indefinido, o que equivale a **`false`**. Essa configuração aparece na pasta **VMware Horizon Client Configuração > Exibir configuração USB (View USB Configuration)** no Editor de Gerenciamento de Política de Grupo.

Tabela 3-10. Horizon Client Modelo de configuração: Configurações de filtragem USB (continuação)

Configuração	Descrição
`Allow HID-Bootable`	Permite que dispositivos de entrada que não sejam teclados ou mouses que estejam disponíveis no momento da inicialização (também conhecidos como dispositivos de inicialização oculta) sejam redirecionados. O valor padrão é indefinido, o que equivale a **`true`**. Essa configuração aparece na pasta **VMware Horizon Client Configuração > Exibir configuração USB (View USB Configuration)** no Editor de Gerenciamento de Política de Grupo.
`Allow Device Descriptor Failsafe Behavior`	Permite que os dispositivos sejam redirecionados mesmo se o Horizon Client falhar ao obter os descritores de configuração/dispositivo. Para permitir um dispositivo, mesmo que ele falhe no config/desc, inclua-o nos filtros Include, como `IncludeVidPid` ou `IncludePath`. O valor padrão é indefinido, o que equivale a **`false`**. Essa configuração aparece na pasta **VMware Horizon Client Configuração > Exibir configuração USB (View USB Configuration) > Configurações não configuráveis pelo agente (Settings not configurable by Agent)** no Editor de gerenciamento de política de grupo.
`Allow Other Input Devices`	Permite que dispositivos de entrada que não sejam dispositivos de inicialização oculta ou teclados com dispositivos apontadores integrados sejam redirecionados. O valor padrão é indefinido, o que equivale a **`true`**. Essa configuração aparece na pasta **VMware Horizon Client Configuração > Exibir configuração USB (View USB Configuration)** no Editor de Gerenciamento de Política de Grupo.
`Allow Keyboard and Mouse Devices`	Permite que teclados com dispositivos apontadores integrados (como mouse, trackball ou touch pad) sejam redirecionados. O valor padrão é indefinido, o que equivale a **`false`**. Essa configuração aparece na pasta **VMware Horizon Client Configuração > Exibir configuração USB (View USB Configuration)** no Editor de Gerenciamento de Política de Grupo.
`Allow Smart Cards`	Permite que os dispositivos de cartão inteligente sejam redirecionados. O valor padrão é indefinido, o que equivale a **`false`**. Essa configuração aparece na pasta **VMware Horizon Client Configuração > Exibir configuração USB (View USB Configuration)** no Editor de Gerenciamento de Política de Grupo.
`Allow Video Devices`	Permite que os dispositivos de vídeo sejam redirecionados. O valor padrão é indefinido, o que equivale a **`true`**. Essa configuração aparece na pasta **VMware Horizon Client Configuração > Exibir configuração USB (View USB Configuration)** no Editor de Gerenciamento de Política de Grupo.
`Disable Remote Configuration`	Desabilita o uso das configurações do agente ao realizar a filtragem do dispositivo USB. O valor padrão é indefinido, o que equivale a **`false`**. Essa configuração aparece na pasta **VMware Horizon Client Configuração > Exibir configuração USB (View USB Configuration) > Configurações não configuráveis pelo agente (Settings not configurable by Agent)** no Editor de gerenciamento de política de grupo.

Tabela 3-10. Horizon Client Modelo de configuração: Configurações de filtragem USB (continuação)

Configuração	Descrição
`Exclude All Devices`	Exclui todos os dispositivos USB do redirecionamento. Se definido como **`true`**, você poderá usar outras configurações de política para permitir que dispositivos ou famílias de dispositivos específicos sejam redirecionados. Se definido como **`false`**, você poderá usar outras configurações de política para evitar que dispositivos ou famílias de dispositivos específicos sejam redirecionados. Se você definir o valor de `Exclude All Devices` como **`true`** no agente e essa configuração for passada para Horizon Client, a configuração do agente substituirá a configuração Horizon Client. O valor padrão é indefinido, o que equivale a **`false`**. Essa configuração aparece na pasta **VMware Horizon Client Configuração > Exibir configuração USB (View USB Configuration)** no Editor de Gerenciamento de Política de Grupo.

`Exclude Automatically Connection Device Family`	Exclui famílias de dispositivos do encaminhamento automático. Use a seguinte sintaxe:
	`family-name[;...]`
	Por exemplo:
	`storage;hid`

`Exclude Automatically Connection Vid/Pid Device`	Exclui os dispositivos que têm IDs de fornecedor e produto específicos de serem encaminhados automaticamente. Use a seguinte sintaxe:
	`vid-xxxx_pid-xxxx|*[;...]`
	Por exemplo:
	`vid-0781_pid-554c;vid-0781_pid-9999`

`Exclude Device Family`	Exclui famílias de dispositivos do redirecionamento. O formato da configuração é *family_name_1*[*; family_name_2*]... Por exemplo: **`bluetooth;smart-card`** Se você tiver ativado a divisão automática de dispositivos, o Horizon examinará a família de dispositivos de cada interface de um dispositivo USB composto para decidir quais interfaces serão excluídas. Se você tiver desativado a divisão automática de dispositivos, o Horizon examinará a família de dispositivos de todo o dispositivo USB composto. O valor padrão é indefinido. Essa configuração aparece na pasta **VMware Horizon Client Configuração > Exibir configuração USB (View USB Configuration)** no Editor de Gerenciamento de Política de Grupo.
`Exclude Vid/Pid Device`	Exclui o redirecionamento de dispositivos com IDs de fornecedor e produto específicos. O formato da configuração é `_pid-`*xxx1*`;vid-`*yyy2*[`_pid-`*xxx2*`vid-`*yyy2*].. . Você deve especificar os números de ID em hexadecimal. Você pode usar o caractere curinga (**`*`**) no lugar de dígitos individuais em uma ID. Por exemplo: **`vid-0781_pid-****;vid-0561_pid-554c`** O valor padrão é indefinido. Essa configuração aparece na pasta **VMware Horizon Client Configuração > Exibir configuração USB (View USB Configuration)** no Editor de Gerenciamento de Política de Grupo.

Tabela 3-10. Horizon Client Modelo de configuração: Configurações de filtragem USB (continuação)

Configuração	Descrição
`Exclude Path`	Excluir dispositivos em caminhos de porta ou hub especificados do redirecionamento. O formato da configuração é `;bus-`*x1*`[/`*y1*`]…/port-`*z1*`[bus-`*x2*`{[/`*y2*`]…/port-`*z2*`]…` Você deve especificar os números de barramento e porta em hexadecimal. Você não pode usar o caractere curinga em caminhos. Por exemplo: **bus-1/2/3_port-02;bus-1/1/1/4_port-ff** O valor padrão é indefinido. Essa configuração aparece na pasta **VMware Horizon Client Configuração > Exibir configuração USB (View USB Configuration) > Configurações não configuráveis pelo agente (Settings not configurable by Agent)** no Editor de gerenciamento de política de grupo.
`Include Device Family`	Inclui famílias de dispositivos que podem ser redirecionados. O formato da configuração é *family_name_1*`[;`*family_name_2*`]…` Por exemplo: **armazenamento** O valor padrão é indefinido. Essa configuração aparece na pasta **VMware Horizon Client Configuração > Exibir configuração USB (View USB Configuration)** no Editor de Gerenciamento de Política de Grupo.
`Include Path`	Incluir dispositivos em um hub especificado ou caminhos de porta que podem ser redirecionados. O formato da configuração é `;bus-`*x1*`[/`*y1*`]…/port-`*z1*`[bus-`*x2*`{[/`*y2*`]…/port-`*z2*`]…` Você deve especificar os números de barramento e porta em hexadecimal. Você não pode usar o caractere curinga em caminhos. Por exemplo: **bus-1/2_port-02;bus-1/7/1/4_port-0f** O valor padrão é indefinido. Essa configuração aparece na pasta **VMware Horizon Client Configuração > Exibir configuração USB (View USB Configuration) > Configurações não configuráveis pelo agente (Settings not configurable by Agent)** no Editor de gerenciamento de política de grupo.
`Include Vid/Pid Device`	Especifica os dispositivos USB que têm um fornecedor e uma ID de produto especificados que podem ser redirecionados. O formato da configuração é `_pid-`*xxx1*`;vid-`*yyy2*`[_pid-`*xxx2*`vid-`*yyy2*`]… .` Você deve especificar os números de ID em hexadecimal. Você pode usar o caractere curinga (*****) no lugar de dígitos individuais em uma ID. Por exemplo: **vid-0561_pid-554c** O valor padrão é indefinido. Essa configuração aparece na pasta **VMware Horizon Client Configuração > Exibir configuração USB (View USB Configuration)** no Editor de Gerenciamento de Política de Grupo.

Em um cenário de modo aninhado ou de salto duplo, um usuário se conecta do sistema cliente físico a uma área de trabalho remota, inicia Horizon Client dentro da área de trabalho remota (a sessão aninhada) e se conecta a outra área de trabalho remota. Para que o dispositivo funcione conforme o esperado na sessão aninhada, você deve definir as configurações de política USB da mesma maneira na máquina cliente física e na sessão aninhada.

VMware Browser Configurações de redirecionamento para GPOs de cliente

Você pode definir as configurações de política de grupo para o recurso Redirecionamento de Navegador.

A tabela a seguir descreve as configurações de redirecionamento do navegador no arquivo de modelo Horizon Client Configuration ADMX. Todas as configurações de redirecionamento do navegador são configurações do computador. As configurações aparecem na pasta **VMware Horizon Client Configuração > VMware Browser Redirecionamento** no Editor de Gerenciamento de Política de Grupo.

Para obter informações sobre as configurações de redirecionamento de navegador do lado do agente, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.

Tabela 3-11. Horizon Client Modelo de configuração: VMware Browser Configurações de redirecionamento

Configuração	Descrição
`Enable WebRTC camera and microphone access for browser redirection`	Quando essa configuração está ativada, as páginas redirecionadas que usam WebRTC têm acesso à câmera e ao microfone do sistema do cliente. Essa configuração é habilitada por padrão.
`Ignore certificate errors for browser redirection`	Quando essa configuração está habilitada, os erros de certificado que ocorrem na página redirecionada são ignorados e a navegação continua. Essa configuração está desativada por padrão.
`Enable cache for browser redirection`	Quando essa configuração está ativada, o histórico de navegação, incluindo cookies, é armazenado no sistema do cliente. **Observação** A desativação dessa configuração não limpa o cache. Se você desabilitar e reabilitar essa configuração, o cache será reutilizado. Essa configuração é habilitada por padrão.

VMware Integrated Printing Configurações para GPOs de cliente

Você pode definir as configurações de política de grupo para o recurso VMware Integrated Printing.

A tabela a seguir descreve as configurações VMware Integrated Printing no arquivo de modelo Horizon Client Configuration ADMX. A tabela mostra se as configurações incluem as definições de Configuração do Computador e de Configuração do Usuário ou apenas as definições de Configuração do Computador. Para as configurações que incluem os dois tipos de configurações, a configuração do Usuário substitui a configuração equivalente da Configuração do Computador. As configurações aparecem na pasta **VMware Horizon Client Configuração > VMware Integrated Printing** no Editor de Gerenciamento de Política de Grupo.

Para obter informações sobre as configurações do VMware Integrated Printing do lado do agente, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.

Tabela 3-12. Horizon Client Modelo de configuração: VMware Integrated Printing Configurações

Configuração	Computador	Usuário	Descrição
`Do not redirect client printer(s)`	X	X	Determina se as impressoras do cliente são redirecionadas. Quando essa configuração está ativada, nenhuma impressora cliente é redirecionada. Quando essa configuração está desativada ou não é definida, todas as impressoras cliente são redirecionadas. Essa configuração não é definida por padrão.
`Allow to redirect L1 local printers to inner session`	X	X	Determina se as impressoras locais L1 devem ser redirecionadas para a sessão interna. VMware é compatível com a execução de Horizon Client dentro de uma área de trabalho remota. Essa configuração, comumente chamada de modo aninhado, envolve três camadas e dois saltos, da seguinte forma: ■ L0 (endpoint) - máquina física em que Horizon Client está instalado. ■ L1 (primeiro salto da área de trabalho remota) - a área de trabalho remota em que Horizon Client e Horizon Agent estão instalados. ■ L2 (área de trabalho publicada do segundo salto ou aplicativo publicado) - a área de trabalho publicada ou o aplicativo publicado ao qual o cliente de segundo salto se conecta. Quando essa configuração está habilitada, as impressoras locais L1 são redirecionadas para a sessão interna. Quando essa configuração não está definida ou desativada, as impressoras locais L1 não são redirecionadas para a sessão interna. Essa configuração não é definida por padrão.

Variáveis de sessão do PCoIP Client Configurações do modelo ADMX

O arquivo de modelo ADMX de Variáveis de Sessão do Cliente PCoIP (`pcoip.client.admx`) contém configurações de política relacionadas ao protocolo de exibição PCoIP. Você pode configurar os valores padrão do computador que um administrador pode substituir ou pode definir as configurações do usuário que um administrador não pode substituir. As configurações que podem ser substituídas aparecem na pasta **Variáveis de sessão do cliente PCoIP (PCoIP Client Session Variables) > Padrões substituíveis do administrador (Overridable Administrator Defaults)** no Editor de Gerenciamento de Política de Grupo. As configurações que não podem ser substituídas aparecem na pasta **Variáveis de sessão do cliente PCoIP (PCoIP Client Session Variables) > Configurações não substituíveis (Not Overridable Settings)** no Editor de Gerenciamento de Política de Grupo.

Os arquivos ADMX estão disponíveis em `VMware-Horizon-Extras-Bundle-`*`YYMM`*`-x.x.x-`*`yyyyyyyy`*`.zip`, que pode ser baixado do site VMware } Site de downloads em https://my.vmware.com/web/vmware/downloads. Em Desktop & End-User Computing, selecione o download VMware Horizon, que inclui o Pacote GPO que contém o arquivo ZIP.

Tabela 3-13. Variáveis de sessão do PCoIP Client

Configuração	Descrição
`Configure PCoIP client image cache size policy`	Controla o tamanho do cache de imagem do cliente PCoIP. O cliente usa o cache de imagem para armazenar partes da exibição que foram transmitidas anteriormente. O armazenamento em cache de imagens reduz a quantidade de dados que são retransmitidos. Quando essa configuração está desativada, o PCoIP usa um tamanho padrão de cache de imagem do cliente de 250 MB. Ao habilitar essa configuração, você pode configurar um tamanho de cache de imagem do cliente de um mínimo de 50 MB a um máximo de 300 MB. O valor padrão é 250 MB. Essa configuração está desativada por padrão.
`Configure PCoIP event log cleanup by size in MB`	Habilita a configuração da limpeza do log de eventos PCoIP por tamanho em MB. Quando essa configuração é definida, ela controla a limpeza do arquivo de log por tamanho em MB. Por exemplo, para uma configuração diferente de zero de *m*, os arquivos de log maiores que *m* MB são excluídos silenciosamente. Uma configuração de 0 indica que não há limpeza de arquivo por tamanho. Quando essa configuração está desativada, a configuração padrão de limpeza do log de eventos por tamanho em MB é 100. Essa configuração está desativada por padrão.
`Configure PCoIP event log cleanup by time in days`	Habilita a configuração da limpeza do log de eventos PCoIP por hora em dias. Quando essa configuração é definida, ela controla a limpeza do arquivo de log por hora em dias. Por exemplo, para uma configuração diferente de zero de *n*, os arquivos de log com mais de *n* dias são excluídos silenciosamente. Uma configuração de 0 indica que não há limpeza de arquivo por hora. Quando essa política está desativada, a configuração padrão de limpeza do log de eventos por hora em dias é 7. Essa configuração está desativada por padrão. A limpeza do arquivo de log é realizada uma vez, quando a sessão é iniciada. Qualquer alteração na configuração não será aplicada até a próxima sessão.
`Configure PCoIP event log verbosity`	Define o detalhamento do log de eventos do PCoIP. Os valores variam de 0 (menos detalhado) a 3 (mais detalhado). Quando essa configuração está habilitada, você pode definir o nível de detalhamento de 0 a 3. Quando a configuração está desativada, o nível de detalhamento padrão do log de eventos é 2. Essa configuração está desativada por padrão. Quando essa configuração é modificada durante uma sessão PCoIP ativa, a nova configuração entra em vigor imediatamente.
`Configure PCoIP session encryption algorithms`	Controla os algoritmos de criptografia anunciados pelo endpoint PCoIP durante a negociação da sessão. Marcar uma das caixas de seleção desativa o algoritmo de criptografia associado. Você deve habilitar pelo menos um algoritmo. Essa configuração se aplica ao agente e ao cliente. Os endpoints negociam o algoritmo de criptografia de sessão real usado. Se o modo aprovado pelo FIPS140-2 estiver ativado, o valor **Desativar a criptografia AES-128-GCM (Disable AES-128-GCM encryption)** será substituído se a criptografia AES-128-GCM e a criptografia AES-256-GCM estiverem desativadas. Se a configuração `Configure SSL Connections` estiver desativada, os algoritmos Salsa20-256round12 e AES-128-GCM estarão disponíveis para negociação por esse endpoint. Essa configuração está desativada por padrão. Os algoritmos de criptografia compatíveis, em ordem de preferência, são SALSA20/12-256, AES-GCM-128 e AES-GCM-256. Por padrão, todos os algoritmos de criptografia com suporte estão disponíveis para negociação por esse endpoint.

Tabela 3-13. Variáveis de sessão do PCoIP Client (continuação)

Configuração	Descrição
`Configure PCoIP virtual channels`	Especifica os canais virtuais que podem e não podem operar em sessões PCoIP. Essa configuração também determina se o processamento da área de transferência deve ser desativado no host PCoIP. Os canais virtuais usados em sessões PCoIP devem aparecer na lista de autorização de canais virtuais. Os canais virtuais que aparecem na lista de canais virtuais não autorizados não podem ser usados em sessões PCoIP. Você pode especificar no máximo 15 canais virtuais para uso em sessões PCoIP. Separe os nomes de vários canais com o caractere de barra vertical (|). Por exemplo, a sequência de autorização do canal virtual para permitir os canais virtuais mksvchan e vdp_rdpvcbridge é **`mksvchan|vdp_rdpvcbridge`**. Se o nome de um canal contiver a barra vertical ou o caractere de barra invertida (\), insira um caractere de barra invertida antes dele. Por exemplo, digite o nome do canal awk|ward\channel como **`awk\\|ward\\channel`**. Quando a lista de canais virtuais autorizados está vazia, todos os canais virtuais não são permitidos. Quando a lista de canais virtuais não autorizados está vazia, todos os canais virtuais são permitidos. A configuração de canais virtuais se aplica ao agente e ao cliente. Os canais virtuais devem ser ativados no agente e no cliente para que os canais virtuais sejam usados. A configuração de canais virtuais fornece uma caixa de seleção separada que permite desativar o processamento remoto da área de transferência no host PCoIP. Esse valor se aplica somente ao agente. Por padrão, todos os canais virtuais estão ativados, incluindo o processamento da área de transferência.
`Configure SSL cipher list`	Configura uma lista de codificação TLS/SSL para restringir o uso de conjuntos de codificação antes de estabelecer uma conexão TLS/SSL criptografada. A lista consiste em uma ou mais cadeias de caracteres do conjunto de cifras separadas por dois-pontos. Todas as cadeias de caracteres do conjunto de cifras não diferenciam maiúsculas de minúsculas. O valor padrão é ECDHE-RSA-AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:ECDHE-RSA-AES128-GCM-SHA256:AES128-SHA256:AES128-SHA:@STRENGTH. Se essa configuração estiver definida, a caixa de seleção **Aplicar AES-256 ou cifras mais fortes para negociação de conexão SSL (Enforce AES-256 or stronger ciphers for SSL connection negotiation)** na configuração `Configure SSL connections to satisfy Security Tools` será ignorada. Essa configuração deve ser aplicada ao servidor PCoIP e ao cliente PCoIP.
`Configure SSL connections to satisfy Security Tools`	Especifica como as conexões de negociação de sessão TLS são estabelecidas. Para satisfazer as ferramentas de segurança, como scanners de porta, ative essa configuração e faça o seguinte: 1 Armazene o certificado da Autoridade de Certificação que assinou qualquer certificado de Servidor a ser usado com PCoIP no repositório de certificados Raiz Confiável. 2 Configure o agente para carregar certificados somente do Repositório de Certificados. Se o repositório Pessoal para a Máquina Local for usado, deixe o nome do repositório do Certificado de CA inalterado com o valor ROOT, a menos que um local de repositório diferente tenha sido usado na etapa 1. Se essa configuração estiver desativada, o conjunto de codificação AES-128 não estará disponível e o endpoint usará certificados de Autoridade de Certificação do repositório MEU da conta de máquina e certificados de Autoridade de Certificação do repositório ROOT. Essa configuração está desativada por padrão.

Tabela 3-13. Variáveis de sessão do PCoIP Client (continuação)

Configuração	Descrição
`Configure SSL protocols`	Configura o protocolo OpenSSL para restringir o uso de determinados protocolos antes de estabelecer uma conexão TLS criptografada. A lista de protocolos consiste em uma ou mais sequências de protocolos OpenSSL separadas por dois-pontos. Todas as cadeias de caracteres de codificação não diferenciam maiúsculas de minúsculas. O valor padrão é `TLS1.1:TLS1.2`, o que significa que o TLS v1.1 e o TLS v1.2 estão ativados e o SSL v2.0, SSLv3.0 e TLS v1.0 estão desativados. Se essa configuração for definida no cliente e no agente, a regra de negociação do protocolo OpenSSL será seguida.
`Configure the Client PCoIP UDP port`	Especifica a porta do cliente UDP usada pelos clientes PCoIP de software. O valor da porta UDP especifica a porta UDP base a ser usada. Se a porta base não estiver disponível, o valor do intervalo de portas UDP determinará quantas portas adicionais tentar. O intervalo vai da porta base até a soma da porta base e do intervalo de portas. Por exemplo, se a porta base for 50002 e o intervalo de portas for 64, o intervalo abrangerá de 50002 a 50066. Essa configuração se aplica somente ao cliente. Por padrão, a porta base é 50002 e o intervalo de portas é 64.
`Configure the maximum PCoIP session bandwidth`	Especifica a largura de banda máxima, em kilobits por segundo, em uma sessão PCoIP. A largura de banda inclui todas as imagens, áudio, canal virtual, USB e tráfego PCoIP de controle. Defina esse valor como a capacidade geral do link ao qual seu endpoint está conectado, considerando o número esperado de sessões PCoIP simultâneas. Por exemplo, com uma configuração de VDI de usuário único (uma única sessão PCoIP) que se conecta por meio de uma conexão de Internet de 4 Mbit/s, defina esse valor como 4 Mbit ou 10% menos que esse valor para deixar alguma margem para outro tráfego de rede. Quando você espera que várias sessões PCoIP simultâneas compartilhem um link, incluindo vários usuários de VDI ou uma configuração de RDS, convém ajustar a configuração adequadamente. No entanto, a redução desse valor restringirá a largura de banda máxima para cada sessão ativa. Definir esse valor impede que o agente tente transmitir a uma taxa mais alta do que a capacidade do link, o que causaria perda excessiva de pacotes e uma experiência do usuário inferior. Esse valor é simétrico. Ele força o cliente e o agente a usar o menor dos dois valores definidos no lado do cliente e do agente. Por exemplo, definir uma largura de banda máxima de 4 Mbit/s força o agente a transmitir a uma taxa mais baixa, mesmo que a configuração esteja definida no cliente. Quando essa configuração está desativada em um endpoint, o endpoint não impõe restrições de largura de banda. Quando essa configuração está habilitada, a configuração é usada como a restrição máxima de largura de banda do endpoint em kilobits por segundo. O valor padrão é 900.000 kilobits por segundo. Essa configuração se aplica ao agente e ao cliente. Se os dois endpoints tiverem configurações diferentes, o valor mais baixo será usado.

Tabela 3-13. Variáveis de sessão do PCoIP Client (continuação)

Configuração	Descrição
`Configure the PCoIP session bandwidth floor`	Especifica um limite inferior, em kilobits por segundo, para a largura de banda que a sessão PCoIP reserva. Essa configuração define a taxa de transmissão de largura de banda mínima esperada para o endpoint. Quando você usa essa configuração para reservar largura de banda para um endpoint, o usuário não precisa aguardar a largura de banda ficar disponível, o que melhora a capacidade de resposta da sessão. Certifique-se de não subscrever em excesso a largura de banda reservada total para todos os endpoints. Certifique-se de que a soma dos pisos de largura de banda para todas as conexões em sua configuração não exceda a capacidade da rede. O valor padrão é 0, o que significa que nenhuma largura de banda mínima está reservada. Quando essa configuração está desativada, nenhuma largura de banda mínima é reservada. Essa configuração está desativada por padrão. Essa configuração se aplica ao agente e ao cliente, mas afeta apenas o endpoint no qual ela está configurada. Quando essa configuração é modificada durante uma sessão PCoIP ativa, a alteração entra em vigor imediatamente.
`Configure the PCoIP session MTU`	Especifica o tamanho da Unidade Máxima de Transmissão (MTU) para pacotes UDP para uma sessão PCoIP. O tamanho da MTU inclui cabeçalhos de pacote IP e UDP. O TCP usa o mecanismo de descoberta de MTU padrão para definir a MTU e essa configuração não a afeta. O tamanho máximo da MTU é de 1500 bytes. O tamanho mínimo da MTU é de 500 bytes. O valor padrão é 1300 bytes. Normalmente, você não precisa alterar o tamanho da MTU. Altere esse valor se você tiver uma configuração de rede incomum que cause a fragmentação do pacote PCoIP. Essa configuração se aplica ao agente e ao cliente. Se os dois endpoints tiverem configurações de tamanho de MTU diferentes, o tamanho mais baixo será usado. Se essa configuração estiver desativada ou não for definida, o cliente usará o valor padrão na negociação com o agente.

Tabela 3-13. Variáveis de sessão do PCoIP Client (continuação)

Configuração	Descrição
`Configure the PCoIP transport header`	Configura o cabeçalho de transporte PCoIP e define a prioridade da sessão de transporte. O cabeçalho de transporte PCoIP é um cabeçalho de 32 bits que é adicionado a todos os pacotes UDP PCoIP (somente se o cabeçalho de transporte estiver ativado e ambos os lados o suportarem). O cabeçalho de transporte PCoIP permite que os dispositivos de rede tomem melhores decisões de priorização/QoS ao lidar com o congestionamento da rede. O cabeçalho de transporte é habilitado por padrão. A prioridade da sessão de transporte determina a prioridade da sessão PCoIP relatada no cabeçalho de transporte PCoIP. Os dispositivos de rede tomam melhores decisões de priorização/QoS com base na prioridade da sessão de transporte especificada. Quando a configuração `Configure the PCoIP transport header` está habilitada, as seguintes prioridades de sessão de transporte estão disponíveis: ■ **Alto (High)** ■ **Médio (Medium)** (valor padrão) ■ **Baixa (Low)** ■ **Indefinido (Undefined)** O agente PCoIP e o cliente negociam o valor de prioridade da sessão de transporte. Se o agente PCoIP especificar um valor de prioridade de sessão de transporte, a sessão usará a prioridade de sessão especificada pelo agente. Se apenas o cliente tiver especificado uma prioridade de sessão de transporte, a sessão usará a prioridade de sessão especificada pelo cliente. Se nem o agente nem o cliente especificaram uma prioridade de sessão de transporte, ou se **Prioridade indefinida (Undefined Priority)** for especificada, a sessão usará o valor padrão, prioridade **Média (Medium)**.
`Enable/disable audio in the PCoIP session`	Determina se o áudio está ativado em sessões PCoIP. Ambos os endpoints devem ter o áudio ativado. Quando essa configuração está ativada, o áudio PCoIP é permitido. Quando está desativado, o áudio PCoIP é desativado. O áudio é ativado por padrão.

Executando o Horizon Client da linha de comando

Você pode executar o Horizon Client a partir da linha de comando ou de scripts. Convém executar o Horizon Client a partir da linha de comando se estiver implementando um aplicativo baseado em quiosque que concede aos usuários finais acesso a aplicativos de área de trabalho remota.

Para executar o Horizon Client a partir da linha de comando, use o comando `vmware-view.exe`. O comando `vmware-view.exe` inclui opções que você pode especificar para alterar o comportamento de Horizon Client.

Horizon Client Uso do comando

A sintaxe do comando `vmware-view` controla a operação de Horizon Client.

Use a seguinte forma do comando `vmware-view` em um prompt de comando Windows.

```
vmware-view [command_line_option [argument]] ...
```

O caminho padrão para o arquivo executável do comando `vmware-view` depende do sistema do cliente. Você pode adicionar esse caminho à variável de ambiente *PATH* no sistema do cliente.

- Sistemas de 64 bits: `C:\Program Files\VMware\}\VMware Horizon View Client\}\\}`
- Sistemas de 64 bits no ARM: `C:\Program Files (x86)\VMware\}\VMware Horizon View Client\}\\}`

A tabela a seguir mostra as opções de linha de comando que você pode usar com o comando `vmware-view`.

Tabela 3-14. Horizon Client Opções de linha de comando

Opção	Descrição
`/?`	Exibe a lista de opções de comando.
`-appName` *application_name*	Especifica o nome do aplicativo publicado conforme ele aparece na janela de seleção da área de trabalho e do aplicativo. O nome é o nome para exibição que foi especificado para o pool de aplicativos no assistente de criação do pool.
`-appProtocol` *protocolo*	Especifica o protocolo de exibição do aplicativo publicado a ser usado, se disponível. Os protocolos válidos são os seguintes: ■ **Explosão** ■ **PCoIP**
`-appSessionReconnectionBehavior` *argumento*	Especifica a configuração do comportamento de reconexão do aplicativo publicado. Os argumentos válidos são os seguintes: **always** — Implementa a configuração **Reconectar automaticamente para abrir aplicativos (Reconnect automatically to open applications)**. **never** — Implementa a configuração **Não pedir para reconectar e não reconectar automaticamente (Do not ask to reconnect and do not automatically reconnect)**. **ask** — Implementa a configuração **Pedir para se reconectar a aplicativos abertos (Ask to reconnect to open applications)**. Quando você usa essa opção, as configurações de reconexão do aplicativo publicado são desativadas em Horizon Client.
`-args` *argumento*	Especifica os argumentos de linha de comando a serem adicionados quando um aplicativo publicado é iniciado. Por exemplo: `vmware-view.exe -serverURL 10.10.10.10 -appName "My Notepad++" -args "\"my new.txt\""`
`-connectUSBOnStartup`	Quando definido como `true`, redireciona todos os dispositivos USB conectados ao host para a área de trabalho remota ou o aplicativo publicado. Essa opção será definida implicitamente se você especificar a opção `-unattended` para uma área de trabalho remota. O padrão é `false`.

Tabela 3-14. Horizon Client Opções de linha de comando (continuação)

Opção	Descrição
`-connectUSBOnInsert`	Quando definido como `true`, conecta um dispositivo USB à área de trabalho remota em primeiro plano ou ao aplicativo publicado quando você conecta o dispositivo. Essa opção será definida implicitamente se você especificar a opção `-unattended` para uma área de trabalho remota. O padrão é `false`.
`-desktopLayout` *window_size*	Especifica como exibir a janela da área de trabalho remota. Os valores de tamanho de janela válidos são os seguintes: **`fullscreen`** Exibição em tela cheia. **`multimonitor`** Exibição de vários monitores. **`windowLarge`** Grande janela. **`windowSmall`** Janela pequena. **`length X width`** Tamanho personalizado, por exemplo, 800 X 600.
`-desktopName` *desktop_name*	Especifica o nome da área de trabalho remota conforme aparece na janela de seleção da área de trabalho e do aplicativo. O nome é o nome para exibição que foi especificado para o pool no assistente de criação de pool. **Importante** Não especifique essa opção para clientes no modo de quiosque. Essa opção não tem efeito quando a área de trabalho remota é executada no modo de quiosque. Para o modo de quiosque, a conexão é feita com a primeira área de trabalho remota na lista de áreas de trabalho remotas autorizadas.
`-desktopProtocol` *protocolo*	Especifica o protocolo de exibição a ser usado conforme aparece na janela de seleção da área de trabalho e do aplicativo. Os protocolos de exibição válidos são os seguintes: ■ **Explosão** ■ **PCoIP** ■ **RDP**
`-domainName` *domain_name*	Especifica o domínio NETBIOS que o usuário final usa para fazer login em Horizon Client. Por exemplo, use `mycompany` em vez de `mycompany.com`.
`-file` *file_path*	Especifica o caminho de um arquivo de configuração que contém opções de comando e argumentos adicionais.
`-h`	Mostra as opções de ajuda.
`-hideClientAfterLaunchSession`	Quando definido como `true`, oculta a janela do seletor de área de trabalho e de aplicativo. Quando definido como `false`, mostra a janela do seletor de área de trabalho e de aplicativo.

Tabela 3-14. Horizon Client Opções de linha de comando (continuação)

Opção	Descrição

`-installShortcutsThenQuit`	Use essa opção para instalar atalhos da área de trabalho e de aplicativos configurados no servidor. Quando você usa essa opção com informações suficientes de autenticação do servidor, o Horizon Client se conecta silenciosamente ao servidor, instala os atalhos e fecha. Se a autenticação do servidor falhar, o Horizon Client será encerrado silenciosamente.
	Para instalar atalhos no sistema cliente automaticamente, crie um script que seja executado quando o sistema cliente for inicializado. Por exemplo:
	`vmware-view.exe -serverURL serverurl -userName user -domainName domain -password password -installShortcutsThenQuit`
	`vmware-view.exe -serverURL serverurl -loginAsCurrentUser true -installShortcutsThenQuit`
	Para obter informações sobre atalhos criados pelo servidor, consulte Configurar atualizações de atalhos do menu Iniciar.

`-languageId` *Locale_ID*	Fornece suporte à localização para diferentes idiomas em Horizon Client. Se uma biblioteca de recursos estiver disponível, especifique a ID de localidade (LCID) a ser usada. Para o inglês dos EUA, insira o valor 0x409.
`-launchMinimized`	Inicia Horizon Client no modo minimizado. Se você fornecer a opção `-appName` ou `-desktopName`, Horizon Client permanecerá minimizado até que o aplicativo publicado ou a área de trabalho remota especificado seja iniciado. Você não pode usar essa opção com a opção `-unattended` ou `-nonInteractive`.

`-listMonitors`	Lista valores de índice e exibe informações de layout para os monitores conectados. Por exemplo:
	`1: (0, 0, 1920, 1200)`
	`2: (1920, 0, 3840, 1200)`
	`3: (-900, -410, 0, 1190)`
	Você usa esses valores de índice na opção `-monitors`.

`-loginAsCurrentUser`	Quando definido como `true`, usa as informações de credencial que o usuário final fornece ao fazer login no sistema do cliente para fazer login no servidor e, finalmente, na área de trabalho remota. O padrão é `false`.
`"n[,n,n,n]"-monitors` *n*	Especifica os monitores a serem usados em uma configuração de vários monitores, em que *n* é o valor de índice de um monitor. Você pode usar a opção `-listMonitors` para determinar os valores de índice dos monitores conectados. Você pode especificar até quatro valores de índice, separados por vírgulas. Por exemplo: `-monitors "1,2"` Essa opção não tem efeito, a menos que `-desktopLayout` esteja definido como `multimonitor`.

Tabela 3-14. Horizon Client Opções de linha de comando (continuação)

Opção	Descrição
`-nonInteractive`	Suprime caixas de mensagens de erro ao iniciar o Horizon Client a partir de um script. Essa opção será definida implicitamente se você especificar a opção `-unattended`. **Observação** Se você fizer login em um servidor no modo não interativo, não será solicitado que você instale os atalhos do menu **Iniciar (Start)** (se disponíveis), e os atalhos são instalados por padrão.
`-noVMwareAddins`	Impede o carregamento de canais virtuais específicos de VMware, como impressão virtual.
`-password` *senha*	Especifica a senha que o usuário final usa para fazer login em Horizon Client. A senha é processada em texto sem formatação pelo console de comando ou por qualquer ferramenta de script. Se você gerar a senha automaticamente, não precisará especificar essa opção para clientes no modo de quiosque. Para maior segurança, não especifique essa opção. Os usuários podem digitar a senha de forma interativa.
`-printEnvironmentInfo`	Exibe o endereço IP, o endereço MAC e o nome da máquina do dispositivo cliente.
`-serverURL` *connection_server*	Especifica a URL, o endereço IP ou o FQDN do servidor.
`-shutdown`	Desliga todas as áreas de trabalho remotas e aplicativos publicados e os componentes relevantes da interface do usuário.
`-singleAutoConnect`	Se o usuário tiver direito a apenas uma área de trabalho remota ou aplicativo publicado, o conectará a essa área de trabalho remota ou aplicativo publicado depois que o usuário for autenticado no servidor. Essa configuração evita que o usuário selecione uma área de trabalho remota ou um aplicativo publicado em uma lista que contém apenas um item.
`-smartCardPIN` *PIN*	Especifica o PIN quando um usuário final insere um cartão inteligente para fazer login.
`-usernameHint` *user_name*	Especifica o nome da conta a ser usado como a dica de nome de usuário.
`-standalone`	Inicia uma segunda instância de Horizon Client que pode se conectar ao mesmo servidor ou a um servidor diferente. Essa opção é compatível com a compatibilidade com versões anteriores. A especificação de `-standalone` não é necessária, pois esse é o comportamento padrão do cliente. Para várias conexões de área de trabalho remota com o mesmo servidor ou com um servidor diferente, há suporte para o uso do túnel seguro. **Observação** A segunda conexão de área de trabalho remota pode não ter acesso ao hardware local, como dispositivos USB, smart cards, impressoras e vários monitores.
`-supportText` *file_name*	Especifica o caminho completo de um arquivo de texto. O conteúdo do arquivo é exibido na caixa de diálogo Sobre.

Tabela 3-14. Horizon Client Opções de linha de comando (continuação)

Opção	Descrição
`-unattended`	Inicia o Horizon Client em um modo não interativo adequado para clientes no modo de quiosque. Você também deve especificar as seguintes informações: ■ O nome da conta do cliente, se você não tiver gerado o nome da conta do endereço MAC do dispositivo do cliente. O nome deve começar com a cadeia de caracteres “custom-” ou um prefixo alternativo que você configurou no ADAM. ■ A senha do cliente, caso você não tenha gerado uma senha automaticamente ao configurar a conta para o cliente. A opção `-unattended` define implicitamente as opções `-nonInteractive`, `-connectUSBOnStartup`, `-connectUSBOnInsert` e `-desktopLayout multimonitor`.
`-unauthenticatedAccessAccount`	Especifica uma conta de usuário de Acesso não autenticado a ser usada para fazer login anonimamente no servidor quando o Acesso não autenticado está habilitado. Se o Acesso não autenticado não estiver ativado, essa opção será ignorada. Por exemplo: `vmware-view.exe -serverURL view.mycompany.com -unauthenticatedAccessEnabled true -unauthenticatedAccessAccount anonymous1`
`-unauthenticatedAccessEnabled`	Quando definido como `true`, ativa o Acesso não autenticado. Se o Acesso não autenticado não estiver disponível, o cliente poderá fazer fallback para outro método de autenticação. A configuração **Acesso não autenticado (Unauthenticated Access)** está visível, desativada e selecionada em Horizon Client. Quando definido como `false`, exige que você insira suas credenciais para fazer login e acessar seus aplicativos. A configuração **Acesso não autenticado (Unauthenticated Access)** está oculta e desmarcada em Horizon Client. Se você não especificar essa opção, poderá habilitar o Acesso não autenticado em Horizon Client. A configuração **Acesso não autenticado (Unauthenticated Access)** está visível, ativada e desmarcada.

Tabela 3-14. Horizon Client Opções de linha de comando (continuação)

Opção	Descrição

`-useExisting`	Permite iniciar várias áreas de trabalho remotas e aplicativos publicados a partir de uma única sessão Horizon Client.
	Quando você especifica essa opção, Horizon Client determina se existe uma sessão com o mesmo nome de usuário, domínio e URL do servidor e, se existir, reutiliza essa sessão em vez de criar uma sessão.
	Por exemplo, no comando a seguir, user-1 inicia o aplicativo Calculadora e uma nova sessão é criada.
	`vmware-view.exe -userName user-1 -password secret -domainName domain -appName Calculator -serverURL view.mycompany.com -useExisting`
	No comando seguinte, user1 inicia o aplicativo Paint com o mesmo nome de usuário, domínio e URL do servidor, e a mesma sessão é usada.
	`vmware-view.exe -userName user-1 -password secret -domainName domain -appName Paint -serverURL view.mycompany.com -useExisting`

`-userName` *user_name*	Especifica o nome da conta que o usuário final usa para fazer login em Horizon Client. Se você gerar o nome da conta a partir do endereço MAC do dispositivo do cliente, não precisará especificar essa opção para clientes no modo de quiosque.

Você pode especificar todas as opções por Active Directory políticas de grupo, exceto `-file`, `-languageId`, `-printEnvironmentInfo`, `-smartCardPIN` e `-unattended`.

Observação As configurações de política de grupo têm precedência sobre as configurações que você especifica na linha de comando. As opções de linha de comando diferenciam maiúsculas de minúsculas.

Horizon Client Arquivo de configuração

Você pode ler as opções de linha de comando para Horizon Client de um arquivo de configuração.

Você pode especificar o caminho do arquivo de configuração como um argumento para a opção `-file` *file_path* do comando `vmware-view`. O arquivo deve ser um arquivo de texto Unicode (UTF-16) ou ASCII.

Exemplo: Exemplo de um arquivo de configuração para um aplicativo não interativo

O exemplo a seguir mostra o conteúdo de um arquivo de configuração para um aplicativo não interativo.

```
-serverURL https://view.yourcompany.com
-userName autouser
-password auto123
```

```
-domainName companydomain
-desktopName autodesktop
-nonInteractive
```

Exemplo: Exemplo de um arquivo de configuração para um cliente no modo de quiosque

O exemplo a seguir mostra um cliente no modo de quiosque em que o nome da conta é baseado no endereço MAC do cliente. O cliente tem uma senha gerada automaticamente.

```
-serverURL 145.124.24.100
-unattended
```

Usando o Windows Registry para configurar o Horizon Client

Você pode definir as configurações padrão para Horizon Client no Registro Windows em vez de especificar essas configurações na linha de comando. As configurações de política de grupo têm precedência sobre as Windows configurações do Registro, e as Windows configurações do Registro têm precedência sobre a linha de comando.

Observação Em uma versão futura do Horizon Client, as configurações de registro do Windows podem não ser suportadas e as configurações de política de grupo devem ser usadas.

A tabela a seguir lista as configurações do Registro para fazer login em Horizon Client. Essas configurações estão localizadas em `HKEY_CURRENT_USER\Software\VMware, Inc.\} \VMware\} VDM\Client\\}` no registro. Esse local é específico para um usuário específico. As configurações de `HKEY_LOCAL_MACHINE`, descritas na tabela a seguir, são configurações de todo o computador e pertencem a todos os usuários locais e a todos os usuários do domínio que têm permissão para fazer login no computador em um ambiente de domínio Windows.

Tabela 3-15. Horizon Client Configurações do Registro para Credenciais

Configuração do Registro	Descrição
`Senha`	Senha padrão.
`Nome de usuário`	Nome de usuário padrão.

A tabela a seguir lista as configurações do Registro para Horizon Client que não incluem credenciais de logon. A localização dessas configurações depende do tipo de sistema da seguinte forma:

- Para Windows de 32 bits: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\}\VMware\} VDM\Client\\}`

- Para Windows de 64 bits: `HKLM\SOFTWARE\WOW6432Node\VMware, Inc.\}\VMware\} VDM\Client\\}`

Tabela 3-16. Horizon Client Configurações do Registro

Configuração do Registro	Descrição
`DomainName`	Nome de domínio NETBIOS padrão. Por exemplo, você pode usar `mycompany` em vez de `mycompany.com`.
`AtivarShade`	Determina se a barra de menus (sombreada) na parte superior da janela Horizon Client está ativada. A barra de menus é ativada por padrão, exceto para clientes no modo de quiosque. Um valor de **`false`** desativa a barra de menus. **Observação** Essa configuração é aplicável somente quando você tem o layout de exibição definido como **Todos os monitores (All Monitors)** ou **Tela inteira (Fullscreen)**.
`ServerURL`	URL, endereço IP ou FQDN da instância padrão do Servidor de Conexão.
`EnableSoftKeypad`	Se definido como **`true`** e uma janela Horizon Client estiver em foco, os eventos de teclado físico, teclado virtual, mouse e teclado de escrita manual serão enviados para a área de trabalho remota ou aplicativo publicado, mesmo se o mouse ou o teclado virtual estiver fora da janela Horizon Client. O padrão é **`false`**.

A tabela a seguir mostra as configurações de segurança que você pode adicionar. A localização dessas configurações depende do tipo de sistema da seguinte forma:

- Para Windows de 32 bits: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\}\VMware\} VDM\Client\Security`
- Para Windows de 64 bits: `HKLM\SOFTWARE\WOW6432Node\VMware, Inc.\}\VMware\} VDM\Client\Security`

Tabela 3-17. Configurações de segurança

Configuração do Registro	Descrição e valores válidos
`CertCheckMode`	Modo de verificação de certificado. Os valores válidos são os seguintes: ■ **0** implementa `Do not verify server identity certificates.` ■ **1** implementa `Warn before connecting to untrusted servers.` ■ **2** implementa `Never connect to untrusted servers.`
`SSLCipherList`	Configura a lista de codificação para restringir o uso de determinados algoritmos e protocolos criptográficos antes de estabelecer uma conexão TLS criptografada. A lista de codificação consiste em uma ou mais cadeias de caracteres de codificação separadas por dois-pontos. Todas as cadeias de caracteres de codificação diferenciam maiúsculas de minúsculas. O valor padrão é **TLSv1.1:TLSv1.2:!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES**. O valor padrão significa que o TLS v1.1 e o TLS v1.2 estão ativados e o SSL v.2.0, SSL v3.0 e TLS v1.0 estão desativados. SSL v2.0, SSL v3.0 e TLS v1.0 não são mais os protocolos aprovados e estão permanentemente desativados. Os conjuntos de codificação usam AES de 128 bits ou 256 bits, removem algoritmos DH anônimos e classificam a lista de codificação atual na ordem do comprimento da chave do algoritmo de criptografia. Para obter informações de referência sobre a configuração, consulte http://www.openssl.org/docs/apps/ciphers.html .

A tabela a seguir mostra as configurações de VMware Integrated Printing que você pode definir. A localização dessas configurações depende do tipo de sistema da seguinte forma:

- Para Windows de 32 bits: `HKEY_LOCAL_MACHINE\Software\VMware, Inc.\}\VMware\}VDM\Client\PrintRedir`
- Para Windows de 64 bits: `HKLM\SOFTWARE\WOW6432Node\VMware, Inc.\}\VMware\}VDM\Client\PrintRedir`

Tabela 3-18. VMware Integrated Printing Configurações

Configuração do Registro	Descrição e valores válidos
`EnableActualSizePrinting`	Determina se os arquivos devem ser impressos de uma área de trabalho remota dimensionando e ajustando o conteúdo do arquivo ao tamanho da página impressa ou imprimindo o conteúdo do arquivo no tamanho real. Os valores válidos são os seguintes: ■ **`true`** imprime o conteúdo do arquivo em seu tamanho real. ■ **`false`** dimensiona e ajusta o conteúdo do arquivo ao tamanho da página impressa. O valor padrão é **`true`**.

Limpando o último nome de usuário usado para fazer login em um servidor

Quando os usuários finais fazem login em uma instância do Servidor de Conexão para a qual a configuração global **Ocultar lista de domínios na interface do usuário do cliente (Hide domain list in client user interface)** está ativada, o menu suspenso **Domínio (Domain)** fica oculto em Horizon Client e os usuários fornecem informações de domínio na caixa de texto Horizon Client **Nome de usuário (User name)**. Por exemplo, os usuários devem digitar o nome de usuário no formato ***domínio\\}nome de usuário*** ou ***nome de usuário@domínio{*** .

Em um sistema cliente Windows, uma chave do Registro determina se o último nome de usuário será salvo e exibido na caixa de texto **Nome de usuário (User name)** na próxima vez que um usuário fizer login no servidor. Para evitar que o último nome de usuário seja exibido na caixa de texto **Nome de usuário (User name)** e exponha informações de domínio, você deve definir o valor da propriedade `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\} \CurrentVersion\Policies\ Chave de Registro System\dontdisplaylastusername` para 1 no sistema do cliente Windows.

Para obter informações sobre como ocultar informações de segurança em Horizon Client, incluindo o menu suspenso **Domínio (Domain)** e informações de URL do servidor, consulte os tópicos sobre configurações globais no documento *Administração Horizon*.

Configurar opções do VMware Blast

Você pode configurar as opções do VMware Blast para a área de trabalho remota e as sessões de aplicativos publicados que usam o protocolo de exibição VMware Blast.

Você pode permitir a decodificação H.264 e a codificação de vídeo de alta eficiência (HEVC). H.264 é um padrão do setor para compactação de vídeo, que é o processo de conversão de vídeo digital em um formato que ocupa menos capacidade quando armazenado ou transmitido. Quando a decodificação H.264 é permitida, você também pode permitir maior fidelidade de cores.

A resolução máxima com suporte, e se o HEVC é compatível, depende da capacidade da unidade de processamento gráfico (GPU) no cliente. Uma GPU que pode oferecer suporte à resolução de 4K para JPEG/PNG pode não oferecer suporte à resolução de 4K para H.264. Se uma resolução para H.264 não for compatível, Horizon Client usará JPEG/PNG em vez disso.

Se o seu ambiente usar um servidor proxy, você poderá especificar se deseja permitir VMware Blast conexões a um servidor proxy do sistema operacional.

Para um servidor proxy SSL, você também precisa configurar a verificação de certificado para conexões secundárias por meio do servidor proxy SSL. Para obter mais informações, consulte Configurando o modo de verificação de certificado em Horizon Client.

Você pode configurar as opções do VMware Blast antes ou depois de se conectar a um servidor.

Pré-requisitos

Para usar a codificação de vídeo de alta eficiência (HEVC), o Horizon Agent 7.7 ou posterior deve estar instalado. Para maior precisão de cores com YUV 4:4:4, o Horizon Agent 7.11 ou posterior deve ser instalado. Além disso, o sistema cliente deve ter uma GPU que ofereça suporte à decodificação HEVC.

A configuração de política de grupo **Permitir que conexões Blast usem as configurações de proxy do sistema operacional (Allow Blast connections to use operating system proxy settings)** do lado do cliente determina se as conexões VMware Blast podem se conectar por meio de um servidor proxy e se os usuários podem alterar a configuração do servidor proxy VMware Blast no Horizon Client } interface do usuário. Para obter mais informações, consulte Usando configurações de política de grupo para configurar Horizon Client.

Dependendo da versão do Horizon Agent que está instalada, um administrador do Horizon pode usar as configurações de política de grupo do lado do agente para habilitar ou desativar recursos do VMware Blast, incluindo alta precisão de cores H.264 e HEVC. Para obter informações, consulte "VMware Blast Configurações de política" no documento *Configurando recursos de área de trabalho remota no Horizon*.

Procedimentos

1. Inicie Horizon Client.
2. Clique em **Configurações (Settings)** (ícone de engrenagem) no canto superior direito da barra de menus e selecione **VMware Blast**.
3. Para permitir a decodificação H.264 em Horizon Client, ative a opção **Permitir decodificação H.264 (Allow H.264 Decoding)**.

   Quando essa opção está ativada (a configuração padrão), o Horizon Client usará a decodificação H.264 se o agente oferecer suporte à codificação de hardware ou software H.264. Se o agente não for compatível com a codificação de software ou hardware H.264, o Horizon Client usará a decodificação JPG/PNG (com o Horizon Agent 7.x) ou a decodificação Blast Codec (com o Horizon Agent 2006 e posterior). Quando essa opção está desmarcada, o Horizon Client usa a decodificação JPG/PNG (com o Horizon Agent 7.x) ou a decodificação Blast Codec (com o Horizon Agent 2006 e posterior).
4. Para permitir maior fidelidade de cores quando a decodificação H.264 é permitida em Horizon Client, marque a caixa de seleção **Permitir alta precisão de cores (reduz a vida útil da bateria e o desempenho)**.

   Quando essa opção é selecionada, o Horizon Client usa alta precisão de cores, mas somente se o agente oferecer suporte a alta precisão de cores. A seleção dessa opção pode reduzir a vida útil da bateria e o desempenho. Esse recurso é desativado por padrão.

5 Para permitir o HEVC, ative a opção **Permitir decodificação de vídeo de alta eficiência (HEVC)**.

Quando essa opção é selecionada, o desempenho e a qualidade da imagem são aprimorados se a máquina cliente tiver uma GPU que ofereça suporte à decodificação HEVC. Esse recurso é ativado por padrão.

Se essa opção for selecionada, mas a máquina cliente não tiver uma GPU que ofereça suporte à decodificação HEVC, ou o agente não for compatível com a codificação HEVC, Horizon Client usará a decodificação H.264 se H.264 estiver selecionado. Horizon Client usará a decodificação Blast Codec se H.264 não estiver selecionado.

6 Para ativar a decodificação de intervalo dinâmico alto, marque a caixa de seleção **Permitir decodificação de intervalo dinâmico alto (HDR)**.

Essa opção estará disponível somente se você ativar a configuração **Permitir decodificação de vídeo de alta eficiência (HEVC)**.

7 Para permitir VMware Blast conexões por meio de um servidor proxy, ative a opção **Permitir que conexões Blast usem as configurações de proxy do sistema operacional (Allow Blast connections to use operating system proxy settings)**.

Resultados

As alterações entrarão em vigor na próxima vez que um usuário se conectar a uma área de trabalho remota ou aplicativo publicado e selecionar o protocolo de exibição VMware Blast. Suas alterações não afetam VMware Blast sessões existentes.

Usando as configurações de proxy do Internet Explorer

Horizon Client usa as configurações de proxy definidas no Internet Explorer.

Ignorando as configurações de proxy

Horizon Client usa as configurações de desvio de proxy do Internet Explorer para ignorar conexões HTTPS a um host do Servidor de Conexão, servidor de segurança ou appliance do Unified Access Gateway.

Se o túnel seguro estiver ativado no host do Servidor de Conexão, no servidor de segurança ou no appliance do Unified Access Gateway, você deverá usar a configuração de política de grupo `Lista de endereços de proxy de túnel` no arquivo de modelo Horizon Client Configuração ADM ou ADMX para especificar uma lista de endereços para ignorar a conexão de túnel. O servidor proxy não é usado para esses endereços. Use um ponto-e-vírgula (;) para separar várias entradas. Essa configuração de política de grupo cria a seguinte chave do Registro:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\VMware, Inc.\VMware VDM\Client\TunnelProxyBypass
```

Você não pode usar essa configuração de política de grupo para conexões diretas. Se a aplicação da configuração de política de grupo não funcionar conforme o esperado, tente ignorar o proxy para endereços locais. Para obter mais informações, consulte https://blogs.msdn.microsoft.com/askie/2015/10/12/how-to-configure-proxy-settings-for-ie10-and-ie11-as-iem- não está disponível/.

Failover do proxy

O Horizon Client oferece suporte ao failover de proxy com a configuração **Usar script de configuração automática (Use automatic configuration script)** em **Configuração automática (Automatic configuration)** em **Opções da Internet > Conexões > Configurações de LAN (Internet Options > Connections > LAN settings)** no Internet Explorer. Para usar essa configuração, você deve criar um script de configuração automática que retorne vários servidores proxy.

Configurar o compartilhamento de dados do Horizon Client

Se um administrador do Horizon tiver optado por participar do VMware Programa de Aperfeiçoamento da Experiência do Cliente (CEIP), o VMware coletará e receberá dados anônimos de sistemas cliente por meio do Servidor de Conexão. Você pode configurar se deseja compartilhar esses dados de cliente com o Servidor de Conexão.

Para obter informações sobre como configurar o Horizon para ingressar no CEIP, consulte o documento *Administração Horizon*.

O compartilhamento de dados é ativado por padrão em Horizon Client. Você deve definir a configuração de compartilhamento de dados antes de se conectar a um servidor. A configuração é aplicada a todos os servidores. Você não pode alterar a configuração de compartilhamento de dados do Horizon Client depois de se conectar a um servidor.

Você pode usar a configuração de política de grupo **Permitir compartilhamento de dados (Allow data sharing)** para ativar ou desativar o compartilhamento de dados e impedir que os usuários alterem a configuração em Horizon Client. Para obter mais informações, consulte Usando configurações de política de grupo para configurar Horizon Client.

VMware coleta dados sobre sistemas cliente para priorizar a compatibilidade de hardware e software. Se o administrador do Horizon tiver optado por participar do programa de aprimoramento da experiência do cliente, o VMware coletará dados anônimos sobre sua implantação para responder melhor aos requisitos do cliente. VMware não coleta dados que identificam sua organização. As informações de Horizon Client são enviadas primeiro para a instância do Servidor de Conexão e depois para VMware, juntamente com dados sobre o Servidor de Conexão, pools de áreas de trabalho e áreas de trabalho remotas.

As informações são criptografadas quando estão em trânsito para a instância do Servidor de Conexão. As informações no sistema do cliente são registradas sem criptografia em um diretório específico do usuário. Os logs não contêm informações de identificação pessoal.

Um administrador do Horizon pode selecionar se deseja participar do VMware programa de aprimoramento da experiência do cliente ao instalar o Servidor de Conexão ou definindo uma opção em Horizon Console após a instalação.

Tabela 3-19. Dados coletados do Horizon Clients para o programa de aprimoramento da experiência do cliente

Descrição	Este campo é anônimo?
Empresa que produziu o aplicativo Horizon Client	Não
Nome do produto	Não
Versão do produto do cliente	Não
Arquitetura binária do cliente	Não
Nome da compilação do cliente	Não
Sistema operacional do host	Não
Kernel do sistema operacional do host	Não
Arquitetura do sistema operacional do host	Não
Modelo do sistema host	Não
CPU do sistema host	Não
Número de núcleos no processador do sistema host	Não
MB de memória no sistema host	Não
Número de dispositivos USB conectados	Não
Máximo de conexões simultâneas de dispositivos USB	Não
ID do fornecedor do dispositivo USB	Não
ID do produto do dispositivo USB	Não
Família de dispositivos USB	Não
Contagem de uso do dispositivo USB	Não

Procedimentos

1. Inicie Horizon Client.
2. Clique em **Configurações (Settings)** (ícone de engrenagem) no canto superior direito da barra de menus e selecione **Compartilhamento de dados (Data Sharing)**.
3. Ative ou desative a opção **Modo de compartilhamento de dados (Data sharing mode)**.

Lista de negações de endereços MAC

Horizon Client relata o endereço MAC do hardware local do usuário em vez do endereço MAC da VPN usando uma lista de negações codificada de endereços MAC.

Os seguintes endereços MAC estão incluídos na lista de negações.

```
000000000000
00059a3c7800
00059a3c7a00
00090faa0001
00090ffe0001
001c42000008
001c42000009
005056c00001
005056c00008
00ff091cb893
00ff10404c08
00ff39c549ca
00ff5ab2e94a
00ff5d79fab3
00ffa43eb222
00ffc7cd3234
02004c4f4f50
0205857feb80
025041000001
080027000443
080027000c04
0800270014be
080027002049
08002700281e
080027003494
0800270034f0
080027004816
08002700509c
0800270074bd
08002700802d
08002700ac25
08002700c4be
08002700c84c
08002700c84e
08002700d49e
08002700e41d
08002700e4a0
08002700e843
08002700e865
08002700e8d3
08002700f061
08002700f091
08002700f4eb
0a0027000000
0a0027000002
0a0027000003
0a002700000d
```

```
1e85de8f5e73
2e85de8f5e73
```

Além disso, o seguinte endereço MAC é usado para a Touch Bar em muitos laptops MacBook.

```
acde48001122
```

Gerenciando a Área de Trabalho Remota e as Conexões de Aplicativos Publicados

4

Os usuários finais podem usar o Horizon Client para se conectar a um servidor, fazer login ou logoff de áreas de trabalho remotas e usar aplicativos publicados. Para fins de solução de problemas, os usuários finais também podem reiniciar e redefinir áreas de trabalho remotas e redefinir aplicativos publicados.

Dependendo de como você configura as políticas, os usuários finais podem realizar muitas operações em suas áreas de trabalho remotas e aplicativos publicados.

Leia os seguintes tópicos:

Conectar-se a uma Área de Trabalho Remota ou Aplicativo Publicado

Para se conectar a uma área de trabalho remota ou a um aplicativo publicado, você deve fornecer o nome de um servidor e as credenciais da sua conta de usuário.

Antes de permitir que os usuários finais acessem suas áreas de trabalho remotas e aplicativos publicados, teste se você pode se conectar a uma área de trabalho remota ou a um aplicativo publicado a partir de um dispositivo cliente. Pode ser necessário especificar um servidor e fornecer credenciais para sua conta de usuário.

Pré-requisitos

- Obtenha credenciais de login, como nome de usuário e senha, RSA SecurID nome de usuário e código de acesso, RADIUS credenciais de autenticação ou número de identificação pessoal (PIN) do cartão inteligente.
- Obtenha o nome de domínio NETBIOS para fazer login. Por exemplo, você pode usar `mycompany` em vez de `mycompany.com`.
- Execute as tarefas administrativas descritas em Preparando o servidor de conexão para Horizon Client.
- Se você estiver fora da rede corporativa e precisar de uma conexão VPN para acessar áreas de trabalho remotas e aplicativos publicados, verifique se o dispositivo do cliente está configurado para usar uma conexão VPN e ative essa conexão.
- Verifique se você tem o nome de domínio totalmente qualificado (FQDN) do servidor que fornece acesso à área de trabalho remota ou ao aplicativo publicado. Não há suporte para sublinhados (_) em nomes de servidor. Se a porta não for 443, você também precisará do número da porta.
- Se você planeja usar o protocolo de exibição RDP para se conectar a uma área de trabalho remota, verifique se a configuração de política de grupo do agente AllowDirectRDP está habilitada. Para obter informações, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.
- Configure o modo de verificação de certificado para o certificado apresentado pelo servidor. Para determinar qual modo usar, consulte Configurando o modo de verificação de certificado em Horizon Client.

Procedimentos

1. Se uma conexão VPN for necessária, ative a VPN.
2. Inicie Horizon Client.
3. (Opcional) Para fazer login como o usuário do domínio Windows conectado no momento, clique no menu **Opções (Options)** (ícone...) no canto superior direito da barra de menus e selecione **Fazer login como usuário atual{ (Log in As Current User)**.

   Essa configuração estará disponível somente se o recurso **Fazer login como usuário atual (Log in as current user)** estiver instalado no sistema do cliente.

4 Conecte-se a um servidor.

Opção	Ação
Conectar-se a um novo servidor	Clique no botão **+ Adicionar servidor (+ Add Server)** ou clique em **+ Adicionar servidor (+ Add Server)** na barra de menus, digite o nome de um servidor e clique em **Conectar (Connect)**. **Observação** Para especificar um endereço IPv6 ao adicionar um servidor, você deve colocar o endereço entre colchetes.
Conectar-se a um servidor existente	Clique duas vezes no ícone do servidor ou clique com o botão direito do mouse no ícone do servidor e selecione **Conectar (Connect)**.

As conexões entre Horizon Client e o servidor sempre usam TLS. A porta padrão para conexões TLS é 443. Se o servidor não estiver configurado para usar a porta padrão, use o formato *servername*:*port*, por exemplo, **view.company.com:1443** .

Você pode ver uma mensagem que você deve confirmar antes que a caixa de diálogo de logon apareça.

5 Se você for solicitado a fornecer RSA SecurID credenciais ou RADIUS credenciais de autenticação, insira as credenciais e clique em **Continuar (Continue)**.

6 Insira as credenciais de um usuário com direito a usar pelo menos uma área de trabalho remota ou um aplicativo publicado, selecione o domínio e clique em **Login**.

Se você digitar o nome de usuário como **username@domain**, Horizon Client o tratará como um nome principal do usuário (UPN) e o menu suspenso **Domain** será desativado.

Se o menu suspenso **Domínio (Domain)** estiver oculto, você deverá digitar o nome de usuário como ***nome de usuário*@*domínio*** ou ***}domínio**}nome de usuário***.

7 Se Horizon Client solicitar que você crie atalhos para aplicativos publicados ou áreas de trabalho remotas no menu **Iniciar (Start)** ou na área de trabalho remota, clique em **Sim (Yes)** ou **Não (No)**.

Esse prompt pode aparecer na primeira vez que você se conectar a um servidor no qual os atalhos foram configurados para aplicativos publicados ou áreas de trabalho remotas. Se você clicar em **Sim (Yes)**, os atalhos do menu **Iniciar (Start)** ou da área de trabalho serão instalados no sistema cliente para esses aplicativos publicados ou áreas de trabalho remotas, se você tiver direito a usá-los. Se você clicar em **Não (No)**, o menu **Iniciar (Start)** ou os atalhos da área de trabalho não serão instalados.

Um administrador do Horizon pode definir a configuração de política de grupo **Instalar atalhos automaticamente quando configurado no servidor Horizon (Automatically install shortcuts when configured on the Horizon server)** para solicitar que os usuários finais instalem atalhos (o padrão), instalem atalhos automaticamente ou nunca instalem atalhos.

8 (Opcional) Para definir as configurações de exibição para uma área de trabalho remota, clique com o botão direito do mouse no ícone da área de trabalho remota e selecione **Configurações (Settings)**.

Opção	Ação
Selecionar um protocolo de exibição	Se um administrador do Horizon tiver permitido, use o menu suspenso **Conectar via (Connect Via)** para selecionar o protocolo de exibição.
Selecionar um layout de exibição	Use o menu suspenso **Exibir (Display)** para selecionar um tamanho de janela ou usar vários monitores.

9 Para se conectar a uma área de trabalho remota ou aplicativo publicado, clique duas vezes no ícone da área de trabalho remota ou do aplicativo publicado na janela de seleção da área de trabalho e do aplicativo.

Se você estiver se conectando a uma área de trabalho publicada RDSH e a área de trabalho publicada já estiver definida para usar um protocolo de exibição diferente, não será possível se conectar imediatamente. Horizon Client solicita que você use o protocolo definido entre RDP e Blast/PCoIP ou faça logoff para que Horizon Client possa se conectar a um protocolo de exibição diferente.

Resultados

Depois que você estiver conectado, a área de trabalho remota ou o aplicativo publicado será aberto.

Se você tiver direito a mais de uma área de trabalho remota ou aplicativo publicado no servidor, a janela do seletor de área de trabalho e aplicativo permanecerá aberta para que você possa se conectar a várias áreas de trabalho remotas e aplicativos publicados.

Se o recurso de redirecionamento de unidade do cliente estiver ativado, a caixa de diálogo Compartilhamento será exibida e você poderá permitir ou negar o acesso a arquivos no sistema de arquivos local. Para obter mais informações, consulte Compartilhar pastas e unidades locais.

Na primeira vez que você se conecta a um servidor, o Horizon Client salva um atalho para o servidor na janela inicial do Horizon Client. Você pode clicar duas vezes nesse atalho de servidor na próxima vez que precisar se conectar ao servidor.

Se a autenticação no servidor falhar ou se o cliente não puder se conectar à área de trabalho remota ou ao aplicativo publicado, execute as seguintes tarefas:

- Verifique se o certificado do servidor está funcionando corretamente. Caso contrário, em Horizon Console, você também poderá ver que o agente em áreas de trabalho remotas está inacessível. Esses sintomas indicam problemas de conexão adicionais causados por problemas de certificado.
- Verifique se as tags definidas na instância do Servidor de Conexão permitem conexões desse usuário. Consulte o documento *Administração Horizon*.

- Verifique se o usuário tem autorização para acessar essa área de trabalho remota ou aplicativo publicado. Consulte o documento *Configurando áreas de trabalho virtuais no Horizon* ou *Configurando áreas de trabalho e aplicativos publicados no Horizon*.
- Se você estiver usando o protocolo de exibição RDP para se conectar a uma área de trabalho remota, verifique se o sistema operacional da área de trabalho remota permite conexões de área de trabalho remota.

Próximo passo

Defina as configurações de inicialização. Se você não quiser exigir que os usuários finais forneçam o nome do host do servidor ou se quiser definir outras configurações de inicialização, use uma opção de linha de comando para criar um atalho na área de trabalho remota. Consulte Executando o Horizon Client da linha de comando.

Usar o acesso não autenticado para se conectar a aplicativos publicados

Se você tiver uma conta de usuário Acesso não autenticado, poderá fazer login em um servidor anonimamente e se conectar aos seus aplicativos publicados.

Antes de permitir que os usuários finais acessem um aplicativo publicado com o recurso Acesso não autenticado, teste se você pode se conectar ao aplicativo publicado a partir de um dispositivo cliente. Pode ser necessário especificar um servidor e fornecer credenciais para sua conta de usuário.

Por padrão, os usuários selecionam a configuração **Acesso não autenticado (Unauthenticated Access)** no menu **Opções (Options)** e selecionam uma conta de usuário para fazer login anonimamente. Um administrador do Horizon pode definir as configurações de política de grupo para pré-selecionar a configuração **Acesso não autenticado (Unauthenticated Access)** e fazer login dos usuários com uma conta de usuário Acesso não autenticado específica.

Pré-requisitos

- Execute as tarefas administrativas descritas em Preparando o servidor de conexão para Horizon Client.
- Configure os usuários do Acesso Não Autenticado na instância do Servidor de Conexão. Para obter informações, consulte "Fornecendo acesso não autenticado para aplicativos publicados" no documento *Administração Horizon*.
- Se você estiver fora da rede corporativa, verifique se o dispositivo do cliente está configurado para usar uma conexão VPN e ative essa conexão.
- Verifique se você tem o nome de domínio totalmente qualificado (FQDN) do servidor que fornece acesso ao aplicativo publicado. Não há suporte para sublinhados (_) em nomes de servidor. Se a porta não for 443, você também precisará do número da porta.

- Configure o modo de verificação de certificado para o certificado apresentado pelo servidor em Horizon Client. Para determinar qual modo usar, consulte Configurando o modo de verificação de certificado em Horizon Client.
- (Opcional) Defina as configurações de política de grupo **Conta a ser usada para acesso não autenticado (Account to use for Unauthenticated Access)** e **Ativar acesso não autenticado ao servidor (Enable Unauthenticated Access to the server)** para alterar o comportamento padrão de Acesso não autenticado. Para obter informações, consulte Usando configurações de política de grupo para configurar Horizon Client.

Procedimentos

1. Se uma conexão VPN for necessária, ative a VPN.
2. Inicie Horizon Client.
3. Clique em **Opções (Options)** na barra de menus e selecione **Acesso não autenticado (Unauthenticated Access)**.

   Dependendo de como o sistema do cliente está configurado, essa configuração pode ser pré-selecionada.
4. Conecte-se ao servidor no qual você tem acesso não autenticado.

Opção	Ação
Conectar-se a um novo servidor	Clique no botão **+ Adicionar servidor (+ Add Server)** ou clique no botão **+ Adicionar servidor (+ Add Server)** na barra de menus, digite o nome do servidor e clique em **Conectar (Connect)**.
Conectar-se a um servidor existente	Clique duas vezes no ícone do servidor na janela inicial Horizon Client.

   As conexões entre Horizon Client e o servidor sempre usam TLS. A porta padrão para conexões TLS é 443. Se o servidor não estiver configurado para usar a porta padrão, use o formato mostrado neste exemplo: `view.company.com:1443`.

   Você pode ver uma mensagem que deve ser confirmada antes que a caixa de diálogo Logon seja exibida.
5. Quando a caixa de diálogo Login for exibida, selecione uma conta no menu suspenso **Conta de usuário (User account)**, se necessário.

   Se apenas uma conta de usuário estiver disponível, o menu suspenso será desativado e a conta de usuário será pré-selecionada.
6. (Opcional) Se a caixa de seleção **Sempre usar esta conta (Always use this account)** estiver disponível, marque-a para ignorar a caixa de diálogo Login na próxima vez que você se conectar ao servidor.

   Para desmarcar essa configuração antes de se conectar ao servidor da próxima vez, clique com o botão direito do mouse no ícone do servidor na janela inicial Horizon Client e selecione **Esquecer a conta de acesso não autenticado salva (Forget the saved Unauthenticated Access account)**.

7 Clique em **Login** para fazer login no servidor.

A janela do seletor de aplicativos é exibida.

8 Para iniciar um aplicativo publicado, clique duas vezes no ícone do aplicativo publicado.

Compartilhar informações de localização

Este tópico descreve como compartilhar informações de localização de um sistema cliente.

Ao se conectar a uma área de trabalho remota ou aplicativo publicado, você pode compartilhar as informações de localização do sistema cliente usando o recurso Redirecionamento de geolocalização ou com a Otimização Microsoft Teams. Para o redirecionamento de geolocalização, você deve ativar o recurso. Para o Microsoft Teams Optimization, o compartilhamento de informações de localização (E911) é ativado por padrão. Além de compartilhar as informações do sistema do cliente, você também deve definir uma configuração em Horizon Client.

Pré-requisitos

Para o recurso Redirecionamento de Geolocalização, um administrador do Horizon deve configurar o recurso Redirecionamento de Geolocalização para a área de trabalho remota ou o aplicativo publicado. Conclua as seguintes etapas para esta tarefa:

- Ative o recurso Redirecionamento de geolocalização ao instalar o Horizon Agent.
- Defina políticas de grupo para configurar os recursos de redirecionamento de geolocalização.
- Ative o plug-in do IE de redirecionamento de geolocalização VMware Horizon.

Para obter os requisitos completos, consulte Requisitos do sistema para redirecionamento de geolocalização.

Para usar a Otimização do Microsoft Teams, você deve ativar esse recurso. A ativação da Otimização Microsoft Teams também ativa o E911 (compartilhamento de localização). Para obter os requisitos completos, consulte Configurar os serviços E911 para Microsoft Teams.

Procedimentos

1 Usando Horizon Client, conecte-se a um servidor e abra **Configurações (Settings)**.

   - Clique no ícone **Configurações (Settings)** (engrenagem) no canto superior direito da área de trabalho e da janela do seletor de aplicativos.
   - Clique com o botão direito do mouse em uma área de trabalho remota ou em um aplicativo publicado na janela do seletor de área de trabalho e aplicativos e selecione **Configurações (Settings)**.

2 Defina as configurações de geolocalização e clique em**Voltar (Back)**(<).

Opção	Ação
Compartilhar as informações de localização do sistema cliente com áreas de trabalho remotas e aplicativos publicados	Ative a opção **Compartilhar sua localização (Share your location)**.
Não mostrar a caixa de diálogo Geolocalização quando você se conectar a uma área de trabalho remota ou aplicativo publicado	Marque a caixa de seleção **Não mostrar a caixa de diálogo ao conectar uma área de trabalho ou aplicativo (Do not show dialog when connecting a desktop or application)**. A caixa de diálogo Geolocalização pergunta se você deseja compartilhar informações de localização com uma área de trabalho remota ou um aplicativo publicado. Se essa caixa de seleção estiver desmarcada, a caixa de diálogo Geolocalização aparecerá na primeira vez que você se conectar a uma área de trabalho remota ou aplicativo publicado. Por exemplo, se você fizer login em um servidor e se conectar a uma área de trabalho remota, verá a caixa de diálogo Localização geográfica. Se você se conectar a outra área de trabalho remota ou aplicativo publicado, não verá a caixa de diálogo novamente. Para ver a caixa de diálogo novamente, você deve se desconectar do servidor e fazer login novamente.

Ocultar a janela VMware Horizon Client

Você pode ocultar a janela VMware Horizon Client depois de abrir uma área de trabalho remota ou um aplicativo publicado.

Você pode usar uma configuração de política de grupo para definir se a janela ficará sempre oculta depois que uma área de trabalho remota ou um aplicativo publicado for aberto. Para obter mais informações, consulte Usando configurações de política de grupo para configurar Horizon Client.

Procedimentos

- Para ocultar a janela VMware Horizon Client depois de abrir uma área de trabalho remota ou um aplicativo publicado, clique no botão **Fechar (Close)** no canto da janela VMware Horizon Client.
- Para definir uma configuração que sempre oculte a janela VMware Horizon Client após a abertura de uma área de trabalho remota ou de um aplicativo publicado, antes de você se conectar a um servidor, clique em **Opções (Options)** na barra de menus e selecione **Ocultar seletor após a inicialização{ (Hide Selector After Launching)**.
- Para mostrar a janela VMware Horizon Client após ela ter sido ocultada, clique com o botão direito do mouse no ícone VMware Horizon Client na bandeja do sistema e selecione **Mostrar VMware Horizon Client**.

Reconectando-se a uma Área de Trabalho Remota ou Aplicativo Publicado

Por motivos de segurança, um administrador do Horizon pode definir tempos limite para efetuar logoff de um servidor e bloquear um aplicativo publicado após algum período de inatividade.

Por padrão, você deve fazer login novamente se tiver o Horizon Client aberto e estiver conectado a um servidor específico por mais de 10 horas. Esse tempo limite se aplica às conexões de área de trabalho remota e de aplicativo publicado.

Você recebe um aviso 30 segundos antes de um aplicativo publicado ser bloqueado automaticamente. Se você não responder, o aplicativo publicado será bloqueado. Por padrão, o tempo limite ocorre após 15 minutos de inatividade, mas um administrador do Horizon pode alterar o período de tempo limite.

Por exemplo, se você tiver um ou mais aplicativos publicados abertos e se afastar do computador, as janelas do aplicativo publicado poderão não estar mais abertas quando você retornar uma hora depois. Em vez disso, você pode ver uma caixa de diálogo solicitando que você clique em **OK** para autenticar novamente no servidor para que as janelas de aplicativos publicados apareçam novamente.

Para definir essas configurações de tempo limite em Horizon Console, selecione **Configurações (Settings) > Configurações globais (Global Settings)**, clique na guia **Configurações gerais (General Settings)** e clique em **Editar (Edit)**.

Criar um atalho na área de trabalho do cliente Windows ou no menu Iniciar

Você pode criar um atalho para uma área de trabalho remota ou um aplicativo publicado. O atalho aparece na área de trabalho do sistema do cliente, assim como os atalhos para aplicativos instalados localmente. Você também pode criar um atalho do menu Windows Iniciar.

Procedimentos

1. Inicie Horizon Client e faça login no servidor.
2. Na janela do seletor de área de trabalho e aplicativo, clique com o botão direito do mouse em uma área de trabalho remota ou em um aplicativo publicado e selecione **Criar atalho para a área de trabalho (Create Shortcut to Desktop)** ou **Adicionar ao menu Iniciar (Add to Start Menu)** no menu de contexto.

Resultados

Dependendo do comando selecionado, o Horizon Client cria um atalho na área de trabalho ou no menu Iniciar do Windows no sistema do cliente.

Próximo passo

Você pode renomear, excluir ou executar qualquer ação em um atalho que pode ser executada em atalhos para aplicativos instalados localmente. Se você ainda não estiver conectado ao servidor quando usar o atalho, Horizon Client solicitará que você faça login antes que a área de trabalho remota ou o aplicativo publicado seja aberto.

Configurar atualizações de atalhos do menu Iniciar

Um administrador do Horizon pode configurar o menu Iniciar ou os atalhos da área de trabalho para determinadas áreas de trabalho remotas e aplicativos publicados. Você pode configurar se as alterações feitas na área de trabalho remota e nos atalhos de aplicativos publicados no servidor serão aplicadas ao sistema do cliente quando você se conectar ao servidor.

Se você tiver direito a uma área de trabalho remota ou aplicativo publicado que tenha atalhos, o Horizon Client colocará os atalhos no menu Iniciar, na área de trabalho ou em ambos, no sistema do cliente quando você se conectar ao servidor.

Em Windows 10 sistemas, Horizon Client coloca atalhos na lista Aplicativos. Se um administrador do Horizon criar uma pasta de categoria para um atalho, a pasta de categoria aparecerá na pasta VMware Aplicativos ou como uma categoria na lista Aplicativos.

Você pode usar uma configuração de política de grupo para definir se o Horizon Client instala atalhos automaticamente, solicita aos usuários finais antes de instalar atalhos ou nunca instala atalhos. Para obter mais informações, consulte a configuração de política de grupo **Instalar atalhos automaticamente quando configurado no servidor Horizon (Automatically install shortcuts when configured on the Horizon server)** em Usando configurações de política de grupo para configurar Horizon Client.

Você pode usar o comando `vmware-view` com a opção `-installShortcutsThenQuit` para criar um script que é executado quando o sistema do cliente é inicializado e instala atalhos automaticamente. Para obter mais informações, consulte Executando o Horizon Client da linha de comando .

Se você ainda não estiver conectado ao servidor quando clicar em um atalho criado pelo servidor, Horizon Client solicitará que você faça login antes que a área de trabalho remota ou o aplicativo publicado seja aberto.

Se um administrador do Horizon modificar os atalhos da área de trabalho remota e do aplicativo publicado no servidor, por padrão, os atalhos serão atualizados no sistema do cliente na próxima vez que você se conectar a esse servidor. Você pode alterar o comportamento padrão de atualização do atalho em Horizon Client. Para obter mais informações, consulte Configurar atualizações de atalhos do menu Iniciar.

Para remover os atalhos criados pelo servidor do sistema do cliente, você pode excluir o servidor da janela de seleção do servidor Horizon Client ou desinstalar o Horizon Client.

Observação Os usuários não são solicitados a instalar atalhos criados pelo servidor, e os atalhos criados pelo servidor não são criados, em clientes no modo de quiosque.

Pré-requisitos

Você não pode alterar a configuração de atualização de atalhos a menos que tenha instalado anteriormente um atalho de um servidor.

Procedimentos

1. Inicie Horizon Client e conecte-se a um servidor.
2. Abra a caixa de diálogo **Configurações (Settings)** e selecione **Atalhos (Shortcuts)**.
   - Clique no ícone **Configurações (Settings)** (engrenagem) no canto superior direito da área de trabalho e da janela do seletor de aplicativos.
   - Clique com o botão direito do mouse no ícone da área de trabalho remota ou do aplicativo publicado e selecione **Configurações (Settings)**.
3. Ative ou desative a opção **Atualizar automaticamente a lista de atalhos de aplicativos e da área de trabalho (Automatically update list of application and desktop shortcuts)**.

Configurar o recurso de conexão automática para uma área de trabalho remota

Você pode configurar um servidor para abrir uma determinada área de trabalho remota automaticamente quando se conectar a esse servidor. Você não pode configurar um servidor para abrir um aplicativo publicado automaticamente.

Pré-requisitos

Obtenha credenciais para se conectar ao servidor, como nome de usuário e senha, RSA SecurID nome de usuário e código de acesso, RADIUS nome de usuário e código de acesso de autenticação ou número de identificação pessoal (PIN) do cartão inteligente.

Procedimentos

1. Inicie Horizon Client e conecte-se ao servidor.
2. Na janela do seletor de área de trabalho e aplicativo, selecione a área de trabalho remota, selecione **Configurações (Settings)** (ícone de engrenagem) no canto superior direito da janela e alterne a opção **Conexão automática a esta área de trabalho (Autoconnect to this desktop)** para ligado.
3. Desconecte-se do servidor.
4. Reconecte-se ao servidor.

   Horizon Client inicia a área de trabalho remota automaticamente.

5 (Opcional) Se você precisar desativar o recurso de conexão automática para a área de trabalho remota, na janela do seletor de área de trabalho e aplicativo, selecione a área de trabalho remota, selecione **Configurações (Settings)** (ícone de engrenagem) no canto superior direito da janela e alterne para desative a opção **Conexão automática a esta área de trabalho (Autoconnect to this desktop)**.

Fazer logoff ou desconectar

Se você se desconectar de uma área de trabalho remota sem fazer logoff, os aplicativos na área de trabalho remota poderão permanecer abertos. Você também pode se desconectar de um servidor e deixar os aplicativos publicados em execução.

Você pode fazer logoff de uma área de trabalho remota mesmo se a área de trabalho remota não estiver aberta. Esse recurso tem o mesmo resultado que enviar Ctrl+Alt+Del para a área de trabalho remota e clicar em **Log Off**.

Observação A combinação de teclas Windows Ctrl+Alt+Del não é compatível com áreas de trabalho remotas. Em vez disso, clique no botão **Enviar Ctrl+Alt+Delete (Send Ctrl+Alt+Delete)** na barra de menus. Como alternativa, você pode pressionar Ctrl+Alt+Insert.

Procedimentos

- Desconecte-se de uma área de trabalho remota sem fazer logoff.

Opção	Ação
Na janela da área de trabalho remota	Execute uma das seguintes ações: ■ Clique no botão **Fechar (Close)** no canto da janela da área de trabalho remota. ■ Selecione **Opções (Options)** na barra de menus da janela da área de trabalho remota e selecione **Desconectar (Disconnect)**.
Na janela do seletor de aplicativos e área de trabalho	No canto superior esquerdo da área de trabalho e da janela do seletor de aplicativos, clique no ícone **Desconectar deste servidor (Disconnect from this server)** e clique em **OK** na caixa de diálogo de aviso. Se você tiver direito a várias áreas de trabalho remotas ou aplicativos publicados no servidor, a janela do seletor de área de trabalho e aplicativos será aberta.

Observação Um administrador do Horizon pode configurar áreas de trabalho remotas para fazer logoff quando forem desconectadas. Nesse caso, todos os aplicativos abertos na área de trabalho remota são fechados.

- Faça logoff e desconecte-se de uma área de trabalho remota.

Opção	Ação
De dentro da área de trabalho remota	Use o menu Windows **Iniciar (Start)** para fazer logoff.
Na barra de menus	Selecione **Opções (Options)** e selecione **Logoff da área de trabalho (Logoff Desktop)**. Se você usar esse procedimento, os arquivos abertos na área de trabalho remota serão fechados sem serem salvos primeiro.

- Desconecte-se de um aplicativo publicado.

Opção	Ação
Desconectar-se do aplicativo publicado, mas não do servidor	Saia do aplicativo publicado da maneira usual, por exemplo, clique no botão **Fechar (Close)** no canto da janela do aplicativo.
Desconectar-se do aplicativo publicado e do servidor	No canto superior esquerdo da janela do seletor de aplicativos, clique no ícone **Desconectar deste servidor (Disconnect from this server)** e clique em **OK** na caixa de diálogo de aviso.
Feche a janela do seletor de aplicativos, mas deixe o aplicativo publicado em execução	Clique no botão **Fechar (Close)**. A janela do seletor de aplicativos é fechada.

- Faça logoff quando você não tiver uma área de trabalho remota aberta.

  Se você usar esse procedimento, os arquivos abertos na área de trabalho remota serão fechados sem serem salvos primeiro.

  a Inicie o Horizon Client, conecte-se ao servidor que fornece acesso à área de trabalho remota e forneça as credenciais de autenticação.

  b Clique com o botão direito do mouse no ícone da área de trabalho remota e selecione **Logoff**.

Desconectando de um servidor

Depois de terminar de usar uma área de trabalho remota ou um aplicativo publicado, você poderá se desconectar do servidor.

Para se desconectar de um servidor, clique no ícone **Desconectar deste servidor (Disconnect from this server)** no canto superior esquerdo da janela Horizon Client.

Trabalhando em uma Área de Trabalho Remota ou em um Aplicativo Publicado

5

O Horizon Client para Windows fornece um ambiente de área de trabalho e aplicativo personalizado e familiar. Os usuários finais podem acessar o USB e outros dispositivos conectados ao computador Windows local, enviar documentos para qualquer impressora que o computador local possa detectar, usar cartões inteligentes para autenticar e usar vários monitores.

Leia os seguintes tópicos:

Suporte a recursos para clientes Windows

Certos sistemas operacionais convidados e recursos de área de trabalho remota exigem versões Horizon Agent específicas. Use essas informações ao planejar quais recursos serão disponibilizados para os usuários finais.

Áreas de trabalho virtuais Windows compatíveis

As áreas de trabalho virtuais Windows são máquinas virtuais de sessão única.

Esta versão do Horizon Client funciona com Windows áreas de trabalho virtuais que têm o Horizon Agent 7.5 ou posterior instalado. Os sistemas operacionais guest compatíveis incluem Windows 7, Windows 8.x e Windows 10, Windows Server 2012 R2, Windows Server 2016 e Windows Server 2019, com as seguintes limitações:

- Windows Server As áreas de trabalho virtuais de 2019 exigem o Horizon Agent 7.7 ou posterior.
- As áreas de trabalho virtuais Windows 7 e Windows 8.x não são compatíveis com o Horizon Agent 2006 e versões posteriores.

Áreas de trabalho publicadas com suporte em hosts RDS

Hosts RDS são computadores servidor que têm o Windows Serviços de Área de Trabalho Remota e o Horizon Agent instalado. Vários usuários podem ter sessões de área de trabalho publicadas em um host RDS simultaneamente. Um host RDS pode ser uma máquina física ou uma máquina virtual.

Esta versão do Horizon Client funciona com hosts RDS que têm o Horizon Agent 7.5 ou posterior instalado. Os sistemas operacionais guest compatíveis incluem Windows Server 2012, Windows Server 2012 R2, Windows Server 2016 e Windows Server 2019, com as seguintes limitações:

- Windows Server Os hosts RDS de 2019 exigem o Horizon Agent 7.7 ou posterior.
- Os hosts RDS do Windows Server 2012 não são compatíveis com o Horizon Agent 2006 e versões posteriores.

Requisitos para recursos específicos da área de trabalho remota

A maioria dos recursos da área de trabalho remota funciona com o Horizon Agent 7.5, mas alguns recursos exigem versões posteriores do Horizon Agent.

Recurso	Requisitos
Arrastar texto e imagens	Horizon Agent 7.9 ou posterior
Arrastar arquivos e pastas	Horizon Agent 7.7 ou posterior
Redirecionamento de geolocalização	Horizon Agent 7.6 ou posterior
Redirecionamento do navegador	Horizon Agent 7.10 ou posterior
VMware Integrated Printing e impressão baseada em localização	Horizon Agent 7.7 ou posterior

Esta versão do Horizon Client para Windows não é compatível com os seguintes recursos de área de trabalho remota, que são compatíveis com as versões do Horizon Agent 7.x:

- Impressão virtual (também conhecida como ThinPrint)
- Redirecionamento de URL Flash
- Redirecionamento de Flash

Desktops Linux compatíveis

Para obter uma lista de sistemas operacionais convidados Linux compatíveis e informações sobre os recursos compatíveis, consulte o documento *Configuração de desktops Linux no Horizon*.

Redimensionando a janela da Área de Trabalho Remota

Se um administrador do Horizon tiver bloqueado o tamanho do convidado ou se você estiver usando o protocolo de exibição RDP, não será possível alterar a resolução da janela da área de trabalho remota.

Se você tiver vários monitores, poderá selecionar os monitores nos quais exibir uma janela da área de trabalho remota. Para obter mais informações, consulte Selecionar monitores específicos para exibir uma área de trabalho remota. Você também pode configurar a janela da área de trabalho remota para abrir em um único monitor. Para obter mais informações, consulte Exibir uma área de trabalho remota em um único monitor em uma configuração de vários monitores.

Configurações de vários monitores compatíveis

Horizon Client é compatível com as seguintes configurações de vários monitores.

- Com o protocolo de exibição VMware Blast, começando com o Horizon 7 versão 7.8, há suporte para seis monitores com resolução de 2560 X 1600 com áreas de trabalho virtuais que estão executando o Windows 10 versão 1703 ou posterior. As especificações de exibição do Windows atualizadas exigem o Windows 10 versão 1803 ou posterior para suporte a seis monitores no Horizon 7 versão 7.9 e posterior.
- Com os pools de desktops de clone instantâneo, o número máximo de monitores é quatro com resolução de 4K.
- Com dois ou mais monitores, os monitores não precisam estar no mesmo modo. Por exemplo, se você estiver usando um laptop conectado a um monitor externo, o monitor externo poderá estar no modo retrato ou paisagem.
- Com a versão de hardware 13 ou anterior, os monitores podem ser colocados lado a lado, empilhados dois a dois ou empilhados verticalmente somente se você estiver usando dois monitores e a altura total for inferior a 4096 pixels.
- Para usar o recurso de vários monitores seletivos, você deve usar o protocolo de exibição VMware Blast ou o protocolo de exibição PCoIP. Para obter mais informações, consulte Selecionar monitores específicos para exibir uma área de trabalho remota e Selecionar monitores específicos para exibir aplicativos publicados.
- Para usar o recurso de renderização 3D do vSGA, você deve usar o protocolo de exibição VMware Blast ou o protocolo de exibição PCoIP. Você pode usar até dois monitores, com resolução de até 1920 X 1200. Para uma resolução de 4K (3840 X 2160), apenas um monitor é compatível.

- Para vGPU ou outros modos de passagem de GPU, o hardware e os drivers do fornecedor determinam o número de monitores e a resolução máxima. Para obter mais informações, consulte o *Guia do usuário da GPU virtual NVIDIA GRID* ou acesse o site do fornecedor.
- Se você estiver usando cinco ou mais monitores e se conectar a uma sessão remota com VMware Blast, se usar as mesmas credenciais de usuário para se conectar à sessão com PCoIP de um dispositivo diferente (sem fazer logoff da sessão original), o falha na conexão com a nova sessão.
- Com o protocolo de exibição VMware Blast, há suporte para uma resolução de tela de área de trabalho remota de 8 K (7680 x 4320). Dois monitores de 8K são suportados. A versão de hardware da máquina virtual da área de trabalho deve ser 14 (ESXi 6.7 ou posterior). Você deve alocar recursos de sistema suficientes na máquina virtual para oferecer suporte a uma exibição de 8K. Para obter informações sobre as configurações de monitor compatíveis com desktops baseados em GRID e para perfis de vGPU da NVIDIA, consulte o *Guia do usuário do software GPU virtual* no site da NVIDIA. Esse recurso é compatível apenas com o cliente Windows.
- Com o protocolo de vídeo VMware Blast ou o protocolo de vídeo PCoIP, há suporte para uma resolução de tela de área de trabalho remota de 4K (3840 x 2160). O número de monitores 4K com suporte depende da versão do hardware da máquina virtual da área de trabalho e da versão Windows.

Versão do hardware	Versão Windows	Número de monitores 4K compatíveis
10 (ESXi compatível com 5.5.x)	7, 8, 8.x, 10	1
11 (ESXi compatível com 6.0)	7 (recurso de renderização 3D desativado e Windows Aero desativado)	3
11	7 (recurso de renderização 3D ativado)	1
11	8, 8.x, 10	1
13 ou 14	7, 8, 8.x, 10 (recurso de renderização 3D ativado)	1
13 ou 14	7, 8, 8.x, 10	4

Para obter o melhor desempenho, a máquina virtual deve ter pelo menos 2 GB de RAM e 2 vCPUs. Esse recurso pode exigir boas condições de rede, como uma largura de banda de 1.000 Mbps com baixa latência de rede e uma baixa taxa de perda de pacotes.

Observação Quando a resolução de tela da área de trabalho remota está definida como 3840 x 2160 (4K), os itens na tela podem parecer menores, e talvez você não consiga usar a caixa de diálogo Resolução da Tela na área de trabalho remota para aumentar o texto e outros itens. Nesse cenário, você pode definir o DPI da máquina cliente com a configuração adequada e habilitar o recurso Sincronização de DPI para redirecionar a configuração de DPI da máquina cliente para a área de trabalho remota.

- Se você usar o Microsoft RDP 7, o número máximo de monitores que você pode usar para exibir uma área de trabalho remota é 16.
- Se você usar o protocolo de exibição Microsoft RDP, deverá ter o Microsoft Remote Desktop Connection (RDC) 6.0 ou posterior instalado na área de trabalho remota.

Selecionar monitores específicos para exibir uma área de trabalho remota

Se você tiver dois ou mais monitores, poderá selecionar os monitores nos quais exibir uma janela da área de trabalho remota. Por exemplo, se você tiver dois monitores, poderá especificar que a janela da área de trabalho remota apareça em apenas um desses monitores.

A partir do Horizon 7 versão 7.8, você pode selecionar até seis monitores adjacentes com áreas de trabalho virtuais que estejam executando o Windows 10 versão 1703 e posterior. A partir do Horizon 7 versão 7.9, você pode selecionar até seis monitores adjacentes com áreas de trabalho virtuais que estejam executando o Windows 10 versão 1803 e posterior. Os monitores podem estar lado a lado ou empilhados verticalmente. Por exemplo, você pode configurar duas linhas de três monitores cada. Com outras versões do Windows ou versões anteriores do VMware Horizon, você pode usar até quatro monitores adjacentes.

Pré-requisitos

Você deve ter dois ou mais monitores.

Procedimentos

1. Inicie Horizon Client e conecte-se a um servidor.
2. Abra a caixa de diálogo Configurações da área de trabalho remota.
   - Clique no ícone **Configurações (Settings)** (engrenagem) no canto superior direito da janela de seleção da área de trabalho e do aplicativo e selecione a área de trabalho remota no painel esquerdo.
   - Clique com o botão direito do mouse na área de trabalho remota na janela de seleção de área de trabalho e aplicativo e selecione **Configurações (Settings)**.
3. Selecione **PCoIP** ou **VMware Blast** no menu suspenso **Conectar via (Connect Via)**.

   O menu suspenso **Conectar via (Connect Via)** só aparecerá se um administrador do Horizon o tiver ativado.
4. No menu suspenso **Exibir (Display)**, selecione **Tela cheia - Todos os monitores (Fullscreen - All Monitors)**.

   As miniaturas dos monitores que estão conectados no momento ao sistema cliente aparecem em Configurações de vídeo. A topologia de exibição corresponde às configurações de exibição no sistema do cliente.

5 Para marcar ou desmarcar um monitor no qual a janela da área de trabalho remota será exibida, clique em uma miniatura.

Quando você seleciona um monitor, sua miniatura muda de cor. Se você violar uma regra de seleção de exibição, uma mensagem de aviso será exibida.

6 Para salvar suas alterações, clique em **Aplicar (Apply)**.

7 Conecte-se à área de trabalho remota.

Suas alterações são aplicadas imediatamente quando você se conecta à área de trabalho remota. Horizon Client salva as configurações de exibição em um arquivo de preferências para a área de trabalho remota depois que você sai do Horizon Client.

Exibir uma área de trabalho remota em um único monitor em uma configuração de vários monitores

Se você tiver dois ou mais monitores, mas quiser que uma janela da área de trabalho remota apareça em apenas um monitor, poderá configurar a janela da área de trabalho remota para abrir em um único monitor.

Pré-requisitos

Você deve ter dois ou mais monitores.

Procedimentos

1 Inicie Horizon Client e conecte-se a um servidor.

2 Abra a caixa de diálogo Configurações da área de trabalho remota.

- Clique no ícone **Configurações (Settings)** (engrenagem) no canto superior direito da janela de seleção da área de trabalho e do aplicativo e selecione a área de trabalho remota no painel esquerdo.
- Clique com o botão direito do mouse na área de trabalho remota na janela de seleção de área de trabalho e aplicativo e selecione **Configurações (Settings)**.

3 No menu suspenso **Conectar via (Connect Via)**, selecione **VMware Blast**, **PCoIP** ou **Microsoft RDP**.

4 No menu suspenso **Tela (Display)**, selecione **Tela inteira - Monitor único (Fullscreen - Single Monitor)**, **Janela - Grande (Window - Large)**, **Janela - Pequena (Window - Small)** ou **Personalizado (Custom)**.

Janela - Grande (Window - Large) maximiza o tamanho da janela. **Janela - Pequena (Window - Small)** define o tamanho da janela como 640 x 480 pixels em 100 por cento de dimensionamento. Se você selecionar **Personalizado (Custom)**, poderá selecionar um tamanho de janela específico.

Resultados

Por padrão, a janela da área de trabalho remota é aberta no monitor principal. Você pode arrastar a janela da área de trabalho remota para um monitor não primário e, na próxima vez que abrir a área de trabalho remota, a janela da área de trabalho remota aparecerá nesse mesmo monitor. A janela é aberta, fica centralizada no monitor e usa o tamanho da janela que você selecionou para o modo de exibição, não um tamanho que você pode ter criado arrastando a janela para redimensioná-la.

Selecionar monitores específicos para exibir aplicativos publicados

Se você tiver dois ou mais monitores, poderá selecionar os monitores nos quais exibir as janelas de aplicativos publicados. Por exemplo, se você tiver dois monitores, poderá especificar que as janelas de aplicativos publicados apareçam em apenas um desses monitores.

Você pode selecionar até quatro monitores adjacentes. Os monitores podem estar lado a lado, empilhados dois a dois ou empilhados verticalmente. No máximo dois monitores podem ser empilhados verticalmente.

Pré-requisitos

Você deve ter dois ou mais monitores.

Procedimentos

1 Inicie Horizon Client e conecte-se a um servidor.

2 Abra a caixa de diálogo Configurações para aplicativos publicados.

- Clique no ícone **Configurações (Settings)** (engrenagem) no canto superior direito da janela de seleção da área de trabalho e do aplicativo e selecione **Aplicativos (Applications)**.
- Clique com o botão direito do mouse em um aplicativo publicado na área de trabalho e na janela de seleção de aplicativo e selecione **Configurações (Settings)**.

3 Em Configurações de Vídeo, marque ou desmarque um monitor no qual a janela do aplicativo publicado será exibida.

   Quando você seleciona um monitor, sua miniatura muda de cor. Se você violar uma regra de seleção de exibição, uma mensagem de aviso será exibida.

4 Para salvar suas alterações, clique em **Aplicar (Apply)**.

Usar dimensionamento de exibição

Os usuários com problemas de visão ou telas de alta resolução, como monitores 4K, geralmente têm o dimensionamento ativado definindo o DPI (pontos por polegada) no sistema do cliente como superior a 100%. A configuração de DPI controla o tamanho do texto, dos aplicativos e dos

ícones. Uma configuração de DPI mais baixa faz com que pareçam menores e uma configuração mais alta faz com que pareçam maiores. Com o recurso Display Scaling, as áreas de trabalho remotas e os aplicativos publicados oferecem suporte à configuração de dimensionamento do sistema cliente e aparecem em tamanho normal, em vez de muito pequenos.

Horizon Client compara a configuração de DPI que recebe da área de trabalho remota ou do aplicativo publicado com a configuração de DPI do sistema do cliente. Se as configurações de DPI não corresponderem e o recurso Escala de Exibição estiver ativado, Horizon Client calculará o fator de escala. Por exemplo, se a configuração de DPI de uma área de trabalho remota for 100 por cento e a configuração de DPI do sistema cliente for 200 por cento, Horizon Client dimensionará a configuração de DPI da área de trabalho remota por um fator de 2 (200 / 100 = 2) .

Horizon Client salva a configuração de dimensionamento de exibição para cada área de trabalho remota separadamente. Para aplicativos publicados, a configuração de dimensionamento de exibição se aplica a todos os aplicativos publicados que estão disponíveis para o usuário conectado no momento.

Em uma configuração de vários monitores, o uso do dimensionamento de exibição não afeta o número de monitores e as resoluções máximas compatíveis com Horizon Client. Quando o dimensionamento de exibição é permitido e está em vigor, o dimensionamento é baseado na configuração de DPI do sistema do cliente.

Você pode ocultar a configuração de dimensionamento de exibição ativando a configuração de política de grupo Horizon Client **Tamanho do convidado bloqueado (Locked Guest Size)**.

Você pode ativar ou desativar o dimensionamento de exibição para todas as áreas de trabalho remotas e aplicativos publicados definindo a configuração de política de grupo **Permitir dimensionamento de exibição (Allow display scaling)**. Para obter informações, consulte Usando configurações de política de grupo para configurar Horizon Client. **Permitir dimensionamento de exibição (Allow display scaling)** está ativado por padrão e a opção está ativada na interface do usuário.

Procedimentos

1 Inicie Horizon Client e conecte-se a um servidor.

2 Na janela do seletor de área de trabalho e aplicativo, clique com o botão direito do mouse na área de trabalho remota ou no aplicativo publicado e selecione **Configurações (Settings)**.

3 Ative a opção **Permitir dimensionamento de exibição (Allow display scaling)**.

   Se um administrador tiver pré-configurado o dimensionamento de exibição, a caixa de seleção estará esmaecida. Se um administrador tiver ocultado a configuração de dimensionamento de vídeo, a caixa de seleção não aparecerá.

Como usar a sincronização de DPI

O recurso Sincronização de DPI garante que a configuração de DPI em uma área de trabalho remota ou aplicativo publicado corresponda à configuração de DPI do sistema do cliente.

Assim como o recurso Display Scaling, o recurso DPI Synchronization pode melhorar a legibilidade do texto e dos ícones em displays de alto DPI. Ao contrário do recurso Display Scaling, que aumenta o tamanho de fontes e imagens e pode torná-las desfocadas, o recurso DPI Synchronization aumenta o tamanho de fontes e imagens, mantendo-as nítidas. Por esse motivo, o recurso Sincronização de DPI geralmente é o preferido para uma experiência ideal do usuário.

Se o recurso Sincronização de DPI e o recurso Dimensionamento de Exibição estiverem ativados, apenas um recurso entrará em vigor a qualquer momento.

A configuração de política de grupo do agente de **Sincronização de DPI (DPI Synchronization)** determina se o recurso Sincronização de DPI está ativado. O recurso é ativado por padrão.

Comportamento da sincronização de DPI com áreas de trabalho remotas

O comportamento padrão da sincronização de DPI depende da versão do Horizon Agent que está instalada na máquina do agente.

A partir de Horizon Agent 2012, a configuração de DPI por monitor do cliente é sincronizada com o agente e as alterações entram em vigor imediatamente durante uma sessão remota por padrão. Esse recurso é controlado pela configuração de política de grupo do agente **Sincronização de DPI por monitor (DPI Synchronization Per Monitor)**. O recurso Sincronização de DPI por Monitor é compatível por padrão para áreas de trabalho virtuais e áreas de trabalho físicas. Não há suporte para áreas de trabalho publicadas.

Com versões anteriores do Horizon Agent, o Horizon Client oferece suporte à sincronização somente com a configuração de DPI do sistema. A sincronização de DPI ocorre durante a conexão inicial, e o dimensionamento de exibição funciona em caso de reconexão, se necessário. Quando a Sincronização de DPI funciona e a configuração de DPI do sistema cliente corresponde à configuração de DPI da área de trabalho remota, o Dimensionamento de vídeo não pode ter efeito, mesmo se você ativar a opção **Permitir dimensionamento de vídeo (Allow Display Scaling)** na interface do usuário. Windows não permite que os usuários alterem a configuração de DPI no nível do sistema para a sessão do usuário atual, e a sincronização de DPI ocorre somente quando eles fazem login e iniciam uma sessão remota. Se os usuários alterarem a configuração de DPI durante uma sessão remota, eles deverão fazer logout e login novamente para que a configuração de DPI da área de trabalho remota corresponda à nova configuração de DPI do sistema do cliente.

A configuração de DPI do agente está localizada no registro Windows em `Computador\HKEY_CURRENT_USER\Control Panel\Desktop: logPixels`.

Observação A configuração de DPI do sistema pode não ser a mesma que a configuração de DPI do monitor principal. Por exemplo, se você fechar o monitor principal e o sistema alternar para um monitor externo com uma configuração de DPI diferente do monitor principal, a configuração de DPI do sistema ainda será a mesma do monitor principal fechado anteriormente.

Esta versão do Horizon Client não é compatível com a configuração de política de grupo do agente **Sincronização de DPI por conexão (DPI Synchronization Per Connection)**, que é fornecida com o Horizon Agent versões 7.8 a 2006.

Para obter mais informações sobre as configurações de política de grupo de sincronização de DPI, consulte o documento *Configurando recursos de área de trabalho remota no Horizon* para sua versão do Horizon Agent.

Sistemas operacionais convidados compatíveis com desktops virtuais

Para áreas de trabalho virtuais, o recurso Sincronização de DPI é compatível com os seguintes sistemas operacionais guest:

- 32 bits ou 64 bits Windows 7
- 32 bits ou 64 bits Windows 8.x
- 32 bits ou 64 bits Windows 10
- 32 bits ou 64 bits Windows 11
- Windows Server 2008 R2 configurado como um desktop
- Windows Server 2012 R2 configurado como um desktop
- Windows Server 2016 configurado como um desktop
- Windows Server 2019 configurado como um desktop
- Windows Server 2022 configurado como um desktop

Observação Para máquinas servidor Windows configuradas como uma área de trabalho, o recurso Sincronização de DPI por monitor só é compatível com o servidor Windows 2022.

Hosts RDS com suporte para áreas de trabalho publicadas e aplicativos publicados

Para áreas de trabalho e aplicativos publicados publicados, o recurso Sincronização de DPI é compatível com os seguintes hosts RDS:

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

Observação Para hosts RDS, o recurso Sincronização de DPI por Monitor não é compatível. Essa limitação não se aplica a aplicativos publicados que são executados em pools de áreas de trabalho com o recurso Aplicativos Hospedados por VM.

Alterar o modo de exibição de uma área de trabalho remota

Você pode alterar o modo de exibição, como do modo **Tela inteira - Todos os monitores (Fullscreen - All Monitors)** para o modo **Tela inteira - Monitor único (Fullscreen - Single Monitor)**, antes ou depois de se conectar a uma área de trabalho remota. Esse recurso não é compatível com aplicativos publicados.

Procedimentos

1 Inicie Horizon Client e conecte-se a um servidor.

2 Abra a caixa de diálogo Configurações da área de trabalho remota.

- Clique no ícone **Configurações (Settings)** (engrenagem) no canto superior direito da janela de seleção da área de trabalho e do aplicativo e selecione a área de trabalho remota no painel esquerdo.
- Clique com o botão direito do mouse na área de trabalho remota na janela de seleção de área de trabalho e aplicativo e selecione **Configurações (Settings)**.

3 No menu suspenso **Exibir (Display)**, selecione o modo de exibição.

Opção	Descrição
Tela cheia - Todos os monitores	Exibe a janela da área de trabalho remota em vários monitores. A janela da área de trabalho remota aparece em todos os monitores por padrão.
Tela cheia - Monitor único	Faz com que a janela da área de trabalho remota preencha a tela.
Janela - Grande	Maximiza a janela da área de trabalho remota.
Janela - Pequena	Define o tamanho da janela da área de trabalho remota como 640 x 480 pixels em 100 por cento de dimensionamento.
Personalizado	Exibe um controle deslizante que você pode usar para configurar um tamanho personalizado da janela da área de trabalho remota.

Resultados

Se você estiver conectado à área de trabalho remota, suas alterações serão aplicadas imediatamente. Se você não estiver conectado à área de trabalho remota, suas alterações serão aplicadas quando você se conectar a ela. Horizon Client salva as configurações de exibição em um arquivo de preferências para a área de trabalho remota depois que você sai do Horizon Client.

Se você usar o modo **Tela inteira - Todos os monitores (Fullscreen - All Monitors)** e clicar no botão **Minimizar (Minimize)**, se você maximizar a janela, a janela voltará para o modo **Tela inteira - Todos os monitores (Fullscreen - All Monitors)** . Da mesma forma, se você usar o modo **Tela inteira - Monitor único (Fullscreen - Single Monitor)** e minimizar a janela, se você maximizar a janela, a janela voltará para o modo **Tela inteira - Monitor único (Fullscreen - Single Monitor)** em um monitor.

Observação Se Horizon Client usar todos os monitores e você maximizar uma janela de aplicativo publicada, a janela se expandirá para a tela inteira apenas do monitor que a contém.

Personalizar a resolução de vídeo e o dimensionamento de vídeo para uma área de trabalho remota

Você pode usar Horizon Client para personalizar a resolução de exibição e o dimensionamento de exibição para uma área de trabalho remota. A resolução da tela determina a clareza do texto e das imagens. Em resoluções mais altas, como 1600 x 1200 pixels, os itens aparecem mais nítidos. A escala de exibição, que é representada como uma porcentagem, aumenta ou diminui o tamanho do texto, dos ícones e dos elementos de navegação.

Por padrão, as configurações personalizadas de resolução de vídeo e dimensionamento de vídeo são armazenadas apenas no sistema do cliente local. Um administrador pode usar a configuração de política de grupo **Salvar resolução e DPI no servidor (Save resolution and DPI to server)** para salvar essas configurações no servidor para que elas sejam sempre aplicadas, independentemente do dispositivo cliente usado para fazer login na área de trabalho remota. Para obter mais informações, consulte Usando configurações de política de grupo para configurar Horizon Client.

Esse recurso tem as seguintes limitações e considerações.

- Não há suporte para a personalização da resolução de exibição e do dimensionamento para uma área de trabalho remota no modo de vários monitores.
- Se você selecionar uma resolução personalizada superior ou inferior à resolução do cliente, Horizon Client redimensionará a janela da área de trabalho remota para caber na janela do cliente.
- Se você personalizar a resolução de vídeo durante uma sessão de área de trabalho remota, suas alterações entrarão em vigor imediatamente. Se você personalizar o dimensionamento da exibição durante uma sessão de área de trabalho remota, deverá fazer logout e login novamente para que as alterações entrem em vigor.
- A configuração de política de grupo Horizon Client **Tamanho do convidado bloqueado (Locked guest size)** tem precedência sobre a personalização da resolução da tela. Para obter mais informações, consulte Usando configurações de política de grupo para configurar Horizon Client.

Procedimentos

1 Inicie Horizon Client e conecte-se a um servidor.

2 Na janela do seletor de área de trabalho e aplicativos, clique com o botão direito do mouse na área de trabalho remota e selecione **Configurações (Settings)**.

3 No menu **Conectar via (Connect Via)**, selecione **VMware Blast** ou **PCoIP**.

4 No menu suspenso **Exibir (Display)**, selecione **Tela inteira - Todos os monitores (Fullscreen - All Monitors)**, **Tela inteira - Monitor único (Fullscreen - Single Monitor)**, **Janela - Grande (Window - Large)**, **Janela - Pequena (Window - Small)** ou **Personalizada (Custom)**.

5 Para personalizar a resolução da tela, selecione uma resolução no menu suspenso **Resolução (Resolution)**.

   Se você selecionar **Automático (Automatic)** (a configuração padrão), Horizon Client ajustará a área de trabalho remota ao tamanho da janela do cliente. Se a área de trabalho remota não oferecer suporte à resolução de vídeo selecionada, ela usará a configuração padrão.

6 Para personalizar o dimensionamento da exibição, selecione um tamanho de dimensionamento no menu suspenso **Escalonamento (Scaling)**.

   Se você selecionar **Automático (Automatic)** (a configuração padrão), Horizon Client sincronizará o dimensionamento de exibição do sistema cliente com a área de trabalho remota.

Usar dispositivos USB

Com o recurso de redirecionamento de USB, você pode usar dispositivos USB conectados localmente, como pen drives, em uma área de trabalho remota ou em um aplicativo publicado.

Quando você usa o recurso de redirecionamento de USB, a maioria dos dispositivos USB que estão conectados ao sistema do cliente local ficam disponíveis nos menus em Horizon Client. Você pode usar esses menus para conectar e desconectar os dispositivos.

Para obter informações sobre os requisitos e as limitações do dispositivo USB para redirecionamento de USB, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.

Você pode conectar dispositivos USB a uma área de trabalho remota ou aplicativo publicado de forma manual ou automática.

Este procedimento descreve como usar o Horizon Client para configurar a conexão automática de dispositivos USB a uma área de trabalho remota ou aplicativo publicado. Você também pode configurar a conexão automática usando a interface de linha de comando Horizon Client ou configurando uma política de grupo.

Para obter informações sobre a interface da linha de comando, consulte Executando o Horizon Client da linha de comando. Para obter informações sobre como configurar políticas de grupo, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.

Pré-requisitos

- Para usar dispositivos USB com uma área de trabalho remota ou um aplicativo publicado, um administrador do Horizon deve habilitar o recurso de redirecionamento de USB.

  Essa tarefa inclui a instalação do componente Redirecionamento de USB de Horizon Agent e pode incluir a configuração de políticas relacionadas ao redirecionamento de USB. Para obter mais informações, consulte o documento *Configurando recursos de área de trabalho remota no Horizon* e Usando configurações de política de grupo para configurar Horizon Client.

- O componente Redirecionamento USB deve ser instalado em Horizon Client. Se você não tiver incluído esse componente na instalação, desinstale o Horizon Client e execute o instalador novamente para incluir o componente Redirecionamento USB.

  Para obter instruções de instalação, consulte o documento *VMware Horizon Client para o WindowsGuia de Instalação e Configuração*.

- Familiarize-se com o Limitações de redirecionamento de USB.

Procedimentos

- Conecte manualmente o dispositivo USB a uma área de trabalho remota.

  a Conecte o dispositivo USB ao sistema do cliente local.

  b Na barra de menu VMware Horizon Client da área de trabalho remota, clique em **Dispositivos USB (USB Devices)**.

  c Ative a opção do dispositivo USB.

  O dispositivo é redirecionado manualmente do sistema local para a área de trabalho remota.

- Conecte o dispositivo USB a um aplicativo publicado.

  a Conecte o dispositivo USB ao sistema do cliente local.

  b Inicie o Horizon Client e conecte-se ao aplicativo publicado.

  c Clique no ícone **Configurações (Settings)** (engrenagem) no canto superior direito da área de trabalho e da janela do seletor de aplicativos e clique em **Dispositivos USB (USB Devices)**.

  d No painel direito, selecione o aplicativo publicado e ative a opção do dispositivo USB.

  Horizon Client conecta o dispositivo USB ao aplicativo publicado que você selecionou. O dispositivo USB também está disponível para outros aplicativos no mesmo farm que o aplicativo selecionado.

  e (Opcional) Para configurar o Horizon Client para conectar o dispositivo USB automaticamente ao aplicativo publicado quando o aplicativo for iniciado, marque a caixa de seleção **Conectar automaticamente na inicialização (Automatically Connect at Startup)**.

f (Opcional) Para configurar o Horizon Client para conectar o dispositivo USB automaticamente ao aplicativo publicado quando você conectar o dispositivo ao sistema local, marque a caixa de seleção **Conectar automaticamente ao ser inserido (Automatically Connect when Inserted)**.

O aplicativo publicado deve estar ativado e em primeiro plano para que esse comportamento tenha efeito.

g Quando terminar de usar o aplicativo publicado, abra a caixa de diálogo Configurações novamente, selecione **Dispositivos USB (USB Devices)** e desative a opção do dispositivo USB.

Você deve liberar o dispositivo USB para poder acessá-lo do seu sistema local.

- Configure o Horizon Client para conectar dispositivos USB automaticamente a uma área de trabalho remota ao conectá-los ao sistema local.

  Use o recurso de conexão automática se você planeja conectar dispositivos que usam drivers MTP, como smartphones e tablets Samsung baseados em Android.

  a Antes de conectar o dispositivo USB, inicie o Horizon Client e conecte-se à área de trabalho remota.

  b Na barra de menus VMware Horizon Client na área de trabalho remota, selecione **Dispositivos USB (USB Devices) > Conectar automaticamente quando inserido (Automatically Connect when Inserted)**.

  c Conecte o dispositivo USB.

  Os dispositivos USB que você conecta ao seu sistema local depois de iniciar o Horizon Client são redirecionados para a área de trabalho remota.

- Configure o Horizon Client para conectar dispositivos USB automaticamente a uma área de trabalho remota quando o Horizon Client for iniciado.

  a Na barra de menus VMware Horizon Client na área de trabalho remota, selecione **Dispositivos USB (USB Devices) > Conectar-se automaticamente na inicialização (Automatically Connect at Startup)**.

  b Conecte o dispositivo USB e reinicie Horizon Client.

  Os dispositivos USB que estão conectados ao sistema do cliente local quando você inicia o Horizon Client são redirecionados para a área de trabalho remota.

Resultados

O dispositivo USB aparece na área de trabalho remota ou no aplicativo publicado. Um dispositivo USB pode levar até 20 segundos para aparecer na área de trabalho remota ou no aplicativo publicado. Na primeira vez que você conectar o dispositivo a uma área de trabalho remota, poderá ser solicitado a instalar drivers.

Se o dispositivo USB não aparecer na área de trabalho remota ou no aplicativo publicado após vários minutos, desconecte e reconecte o dispositivo ao computador cliente.

Próximo passo

Se você tiver problemas com o redirecionamento de USB, consulte o tópico sobre como solucionar problemas de redirecionamento de USB no documento *Configurando recursos de área de trabalho remota no Horizon*.

Limitações de redirecionamento de USB

O recurso de redirecionamento USB tem algumas limitações.

- Quando você acessa um dispositivo USB de um menu em Horizon Client e usa o dispositivo em uma área de trabalho remota ou aplicativo publicado, não é possível acessar o dispositivo USB no dispositivo local.
- Os dispositivos USB que não aparecem no menu, mas estão disponíveis em uma área de trabalho remota ou em um aplicativo publicado, incluem dispositivos de interface humana, como teclados e dispositivos apontadores. A área de trabalho remota ou o aplicativo publicado e o dispositivo local usam esses dispositivos ao mesmo tempo. Às vezes, a interação com esses dispositivos USB pode ser lenta devido à latência da rede.
- Unidades de disco USB grandes podem levar vários minutos para aparecer na área de trabalho remota ou no aplicativo publicado.
- Alguns dispositivos USB requerem drivers específicos. Se um driver necessário ainda não estiver instalado, você poderá ser solicitado a instalá-lo quando conectar o dispositivo USB à área de trabalho remota ou ao aplicativo publicado.
- Se você planeja conectar dispositivos USB que usam drivers MTP, como smartphones e tablets Samsung baseados em Android, configure o Horizon Client para que ele conecte dispositivos USB à área de trabalho remota ou ao aplicativo publicado automaticamente. Caso contrário, se você tentar redirecionar manualmente o dispositivo USB usando um item de menu, o dispositivo não será redirecionado, a menos que você desconecte o dispositivo e conecte-o novamente.
- Não se conecte a scanners usando o menu **Dispositivos USB (USB Devices)**. Para usar um dispositivo de scanner, use o recurso de redirecionamento do scanner. Consulte Como usar scanners.
- O redirecionamento de dispositivos de áudio USB depende do estado da rede e não é confiável. Alguns dispositivos exigem uma alta taxa de transferência de dados, mesmo quando estão ociosos. Os dispositivos de entrada e saída de áudio funcionam bem com o recurso Áudio e Vídeo em Tempo Real. Você não precisa usar o redirecionamento USB para esses dispositivos.
- Não é possível formatar uma unidade USB redirecionada em uma área de trabalho publicada, a menos que você se conecte como usuário administrador.
- Um aplicativo publicado se conecta automaticamente na inicialização e quando os recursos inseridos não funcionam com direitos globais de aplicativo.

- O recurso de redirecionamento de USB não é compatível com controladores USB que não sejam PCI no sistema cliente, como o Controlador Fresco Logic F-One. Se você usar esse controlador no sistema cliente, o redirecionamento USB poderá falhar para todos os dispositivos USB no sistema cliente.

Observação Não redirecione dispositivos USB, como dispositivos Ethernet USB e dispositivos de tela sensível ao toque, para uma área de trabalho remota ou um aplicativo publicado. Se você redirecionar um dispositivo Ethernet USB, o sistema do cliente perderá a conectividade de rede. Se você redirecionar um dispositivo de tela sensível ao toque, a área de trabalho remota ou o aplicativo publicado receberá a entrada de toque, mas não a entrada do teclado. Se você tiver definido a área de trabalho remota ou o aplicativo publicado para conectar dispositivos USB automaticamente, poderá configurar uma política para excluir dispositivos específicos.

Como usar webcams e microfones

Com o recurso Áudio e Vídeo em Tempo Real, você pode usar a webcam ou o microfone do sistema cliente local em uma área de trabalho remota ou em um aplicativo publicado. O Áudio-Vídeo em Tempo Real é compatível com aplicativos de conferência padrão e aplicativos de vídeo baseados em navegador. Ele é compatível com webcams padrão, dispositivos USB de áudio e entrada de áudio analógica.

Para obter informações sobre como configurar o recurso Áudio e Vídeo em Tempo Real na máquina do agente, incluindo a configuração da taxa de quadros e da resolução da imagem, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.

Quando você pode usar uma webcam com o recurso de áudio e vídeo em tempo real

Se um administrador do Horizon tiver configurado o recurso Áudio e Vídeo em Tempo Real, você poderá usar uma webcam integrada ou conectada ao computador cliente em uma área de trabalho remota ou aplicativo publicado. Você pode usar a webcam em aplicativos de conferência, como Skype, Webex ou Google Hangouts.

Durante a configuração de um aplicativo como Skype, Webex ou Google Hangouts em uma área de trabalho remota, você pode selecionar dispositivos de entrada e saída nos menus do aplicativo.

Para áreas de trabalho virtuais que têm o Horizon Agent 7.9 ou anterior instalado e para áreas de trabalho e aplicativos publicados publicados, o Áudio-Vídeo em Tempo Real pode redirecionar apenas uma webcam, e a webcam é denominada VMware Webcam Virtual nos aplicativos. Para áreas de trabalho virtuais que têm o Horizon Agent 7.10 ou posterior instalado, o áudio e vídeo em tempo real pode redirecionar mais de uma webcam, e o nome da webcam redirecionada é o nome real do dispositivo com (VDI) anexado, por exemplo, C670i FHD Webcam (VDI).

Para muitos aplicativos, você não precisa selecionar um dispositivo de entrada.

Quando o computador cliente usa a webcam, a sessão remota não pode usá-la ao mesmo tempo. Além disso, quando a sessão remota usa a webcam, o computador cliente não pode usá-la ao mesmo tempo.

Importante Se você usar uma webcam USB, não a conecte a partir do menu **Conectar dispositivo USB (Connect USB Device)** em Horizon Client. Fazer isso roteará o dispositivo por meio do redirecionamento USB, e o desempenho não poderá ser usado para bate-papo por vídeo.

Se mais de uma webcam estiver conectada ao computador cliente, você deverá configurar uma webcam preferencial para uso em sessões remotas para áreas de trabalho e aplicativos publicados e para áreas de trabalho virtuais que não oferecem suporte a várias webcams.

Para obter mais informações, consulte Selecionar uma webcam ou microfone preferido em um sistema cliente Windows.

Selecionar uma webcam ou microfone preferido em um sistema cliente Windows

Com o recurso Áudio e Vídeo em Tempo Real, se várias webcams ou microfones estiverem conectados ao sistema do cliente, você poderá especificar qual webcam ou microfone é o preferido definindo as configurações de Áudio e Vídeo em Tempo Real em Horizon Client.

Com o recurso Áudio-Vídeo em Tempo Real, os dispositivos de vídeo, de entrada de áudio e de saída de áudio funcionam sem exigir o uso de redirecionamento de USB, e a quantidade de largura de banda de rede necessária é bastante reduzida. Dispositivos de entrada de áudio analógico também são suportados.

Se estiver disponível, a webcam ou o microfone preferido será usado na área de trabalho remota ou no aplicativo publicado. Se a webcam ou o microfone preferido não estiver disponível, outra webcam ou microfone será usado.

Observação Se você estiver usando uma webcam ou microfone USB, não o conecte a partir do menu **Conectar dispositivo USB (Connect USB Device)**em Horizon Client. Fazer isso encaminha o dispositivo por meio do redirecionamento USB, e o dispositivo não pode usar o recurso Áudio e Vídeo em Tempo Real.

Para áreas de trabalho virtuais com o Horizon Agent 7.10 ou posterior instalado, o recurso Áudio e Vídeo em Tempo Real é compatível com vários dispositivos de webcam e microfone.

Pré-requisitos

- Verifique se uma webcam USB ou um microfone USB, ou outro tipo de microfone, está instalado e funcionando no sistema do cliente.
- Verifique se você está usando o protocolo de exibição VMware Blast ou o protocolo de exibição PCoIP para a área de trabalho remota ou o aplicativo publicado.
- Conecte-se a um servidor.

Procedimentos

1 Abra a caixa de diálogo **Configurações (Settings)** e selecione **Áudio-Vídeo em tempo real (Real-Time Audio-Video)** no painel esquerdo.

   - Clique no ícone **Configurações (Settings)** (engrenagem) no canto superior direito da área de trabalho e da janela do seletor de aplicativos.
   - Clique com o botão direito do mouse em uma área de trabalho remota ou em um aplicativo publicado na janela do seletor de área de trabalho e aplicativos e selecione **Configurações (Settings)**.

2 Para configurar uma webcam preferencial, selecione-a no menu suspenso **Webcam preferencial (Preferred webcam)**.

3 Para configurar um microfone preferencial, selecione um microfone específico ou **Todos (All)** no menu suspenso **Microfone preferido (Preferred microphone)**.

   Se a área de trabalho remota oferecer suporte a vários dispositivos com o recurso Áudio e Vídeo em Tempo Real e você selecionar um microfone específico, somente o microfone e os dispositivos de webcam selecionados serão redirecionados para a área de trabalho remota. Se você selecionar **Todos (All)**, todos os dispositivos de microfone e webcam disponíveis serão redirecionados para a área de trabalho remota.

Como usar vários dispositivos com o recurso de áudio e vídeo em tempo real

Se mais de uma webcam ou microfone estiver conectado ao computador cliente e a área de trabalho remota oferecer suporte ao redirecionamento de vários dispositivos com o recurso Áudio e Vídeo em Tempo Real, você poderá usar todas as webcams e microfones conectados ao computador cliente na área de trabalho remota.

Esse recurso é compatível apenas com áreas de trabalho virtuais que têm o Horizon Agent 7.10 ou posterior instalado. Ele não é compatível com áreas de trabalho publicadas ou aplicativos publicados. Para obter os requisitos completos do sistema, consulte Requisitos do sistema para áudio e vídeo em tempo real.

Veja a seguir dicas para usar mais de uma webcam ou microfone com o recurso Áudio e Vídeo em Tempo Real.

- Quando você se conecta a uma área de trabalho remota, o recurso Áudio e Vídeo em Tempo Real redireciona todas as webcams e microfones atualmente conectados ao computador cliente. A área de trabalho remota decide qual webcam e microfone são o dispositivo padrão. Você não precisa configurar uma webcam ou microfone preferencial em Horizon Client.
- Se você quiser usar o mesmo microfone por padrão em aplicativos como Skype for Business, deverá configurar um microfone padrão. Caso contrário, todos os microfones serão redirecionados e você deverá selecionar um microfone sempre que usar o aplicativo. Para obter mais informações, consulte Selecionar uma webcam ou microfone preferido em um sistema cliente Windows.

- Se você desconectar uma webcam ou um microfone do computador cliente e o dispositivo não estiver sendo usado em um aplicativo na área de trabalho remota, o recurso Áudio-Vídeo em tempo real excluirá o dispositivo da área de trabalho remota imediatamente. Se o dispositivo estiver sendo usado por um aplicativo na área de trabalho remota, o recurso Áudio e Vídeo em Tempo Real excluirá o dispositivo depois que o aplicativo o liberar.
- O nome de exibição de um dispositivo redirecionado é o nome real do dispositivo, mas com (VDI) anexado, por exemplo, C670i FHD Webcam (VDI).
- Você pode usar vários dispositivos redirecionados simultaneamente em uma área de trabalho remota.

Selecionar um alto-falante preferido para uma área de trabalho remota

Se vários alto-falantes estiverem conectados ao sistema cliente, você poderá especificar qual alto-falante é o preferido em uma área de trabalho remota. Você também pode selecionar todos os alto-falantes disponíveis.

Esse recurso é compatível apenas com áreas de trabalho virtuais. Ele não é compatível com áreas de trabalho e aplicativos publicados publicados.

Se você selecionar um alto-falante específico e, em seguida, adicionar ou remover um alto-falante do sistema cliente durante uma sessão remota, as alterações não terão efeito na sessão remota. Se você selecionar todos os alto-falantes disponíveis, os dispositivos serão atualizados dinamicamente durante uma sessão remota.

Pré-requisitos

- Verifique se vários alto-falantes estão instalados e operacionais no sistema do cliente.
- Verifique se você está usando o protocolo de exibição VMware Blast para se conectar à área de trabalho remota. Esse recurso não funciona com nenhum outro protocolo de exibição.
- Verifique se o Horizon Agent 2012 ou posterior está instalado na área de trabalho remota. Para versões anteriores do Horizon Agent, o áudio é reproduzido no dispositivo de áudio padrão conectado ao sistema do cliente.
- Conecte-se ao servidor.

Procedimentos

1 Abra a caixa de diálogo **Configurações (Settings)** e selecione **Áudio-Vídeo em tempo real (Real-Time Audio-Video)** no painel esquerdo.

   - Clique no ícone **Configurações (Settings)** (engrenagem) no canto superior direito da área de trabalho e da janela do seletor de aplicativos.
   - Clique com o botão direito do mouse na área de trabalho remota na janela do seletor de área de trabalho e aplicativo e selecione **Configurações (Settings)**.

2 Selecione um alto-falante no menu suspenso **Alto-falante preferido (Preferred speaker)**.

Observação Esse recurso é independente do recurso Áudio-Vídeo em Tempo Real, embora apareça na página**Áudio-Vídeo em Tempo Real (Real-Time Audio-Video)**.

Se você selecionar um alto-falante específico, somente o alto-falante selecionado será redirecionado para a área de trabalho remota. Se você selecionar **Todos (All)**, todos os alto-falantes disponíveis serão redirecionados para a área de trabalho remota. Se você selecionar **Padrão (Default)**, o áudio será reproduzido no dispositivo de áudio padrão conectado ao sistema cliente.

Compartilhando sessões de área de trabalho remota

Com o recurso Colaboração de Sessão, você pode convidar outros usuários para ingressar em uma sessão de área de trabalho remota existente. Uma sessão de área de trabalho remota compartilhada dessa maneira é chamada de sessão colaborativa. O usuário que compartilha uma sessão com outro usuário é chamado de proprietário da sessão, e o usuário que ingressa em uma sessão compartilhada é chamado de colaborador da sessão.

Um administrador do Horizon deve habilitar o recurso Colaboração de Sessão.

Para desktops Windows, essa tarefa inclui a ativação do recurso Colaboração de Sessão no pool de desktops ou no nível do farm. Ele também pode incluir o uso de políticas de grupo para configurar os recursos de Colaboração de Sessão, como os métodos de convite disponíveis. Para obter os requisitos completos, consulte Requisitos do sistema para o recurso de colaboração de sessão.

Para obter informações sobre como ativar o recurso Colaboração de Sessão para desktops Windows, consulte o documento *Configurando áreas de trabalho virtuais no Horizon*. Para obter informações sobre como habilitar o recurso Colaboração de Sessão para um farm, consulte o documento *Configurando áreas de trabalho e aplicativos publicados no Horizon*. Para obter informações sobre como usar as configurações de política de grupo para configurar o recurso Colaboração de Sessão, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.

Para obter informações sobre como ativar o recurso Colaboração de Sessão para desktops Linux, consulte o documento *Configuração de desktops Linux no Horizon*.

Convidar um usuário para ingressar em uma sessão de área de trabalho remota

Com o recurso Colaboração de Sessão, você pode convidar usuários para ingressar em uma sessão de área de trabalho remota enviando convites de colaboração por e-mail, em uma mensagem instantânea (Windows somente áreas de trabalho remotas) ou copiando um link para a área de transferência e encaminhando o link para os usuários .

Você pode convidar apenas usuários que pertencem a um domínio que o servidor permite para autenticação. Você pode convidar até cinco usuários por padrão. Um administrador do Horizon pode alterar o número máximo de usuários que você pode convidar.

O recurso de Colaboração de Sessão tem as seguintes limitações.

- Se você tiver vários monitores, somente o monitor primário será mostrado aos colaboradores da sessão.
- Você deve selecionar o protocolo de exibição VMware Blast ao criar uma sessão de área de trabalho remota para compartilhar. O recurso Colaboração de Sessão não oferece suporte a sessões PCoIP ou RDP.
- A codificação de hardware H.264 não é suportada. Se o proprietário da sessão estiver usando a codificação de hardware e um colaborador ingressar na sessão, ambos retornarão para a codificação de software.
- A colaboração anônima não é suportada. Os colaboradores da sessão devem ser identificáveis por meio de mecanismos de autenticação compatíveis com o Horizon.
- Os colaboradores da sessão devem ter o Horizon Client para Windows, Mac ou Linux instalado ou devem usar HTML Access.
- Se um colaborador da sessão tiver uma versão não compatível do Horizon Client, uma mensagem de erro será exibida quando o usuário clicar em um link de colaboração.
- Você não pode usar o recurso Colaboração de Sessão para compartilhar sessões de aplicativo publicadas.

Pré-requisitos

- O recurso de Colaboração de Sessão deve ser ativado e configurado.
- Para usar o método de convite por e-mail, um aplicativo de e-mail deve estar instalado.
- Para usar o método de convite de IM para uma área de trabalho remota Windows, o Skype for Business deve estar instalado e configurado.

Procedimentos

1. Conecte-se a uma área de trabalho remota para a qual o recurso Colaboração de Sessão esteja ativado.

   Você deve usar o protocolo de exibição VMware Blast.

2. Na bandeja do sistema da área de trabalho remota, clique no ícone **VMware Horizon Colaboração**, por exemplo,  .

   O ícone de colaboração pode ter uma aparência diferente, dependendo da versão do sistema operacional.

3 Quando a caixa de diálogo VMware Horizon Colaboração for aberta, digite o nome de usuário (por exemplo, **`usuário-teste`** ou **`domínio\usuário-teste`**) ou o endereço de e-mail do usuário do qual você deseja ingressar no controle remoto sessão de área de trabalho.

   Na primeira vez que você digitar o nome de usuário ou o endereço de e-mail de um determinado usuário, deverá clicar em **Procurar "*usuário*"**, digitar uma vírgula (,) ou pressionar a tecla **Digite a tecla (Enter)** para validar o usuário. Para áreas de trabalho remotas do Windows, o recurso Colaboração de Sessão lembrará o usuário na próxima vez que você inserir o nome de usuário ou o endereço de e-mail do usuário.

4 Selecione um método de convite.

   Nem todos os métodos de convite podem estar disponíveis.

Opção	Ação
E-mail	Copia o convite de colaboração para a área de transferência e abre uma nova mensagem de e-mail no aplicativo de e-mail padrão. Um aplicativo de e-mail deve ser instalado para usar esse método de convite.
IM	(Windows somente áreas de trabalho remotas) Copia o convite de colaboração para a área de transferência e abre uma nova janela em Skype for Business. Pressione Ctrl+V para colar o link na janela Skype for Business. Skype for Business deve ser instalado e configurado para usar esse método de convite.
Copiar Link	Copia o convite de colaboração para a área de transferência. Você deve abrir manualmente outro aplicativo, como o Bloco de Notas, e pressionar Ctrl+V para colar o convite.

Resultados

Depois de enviar um convite, o ícone VMware Horizon Colaboração também aparece na área de trabalho e a interface do usuário de Colaboração de Sessão se transforma em um painel que mostra o estado atual da sessão de colaboração e permite que você execute determinadas ações.

Quando um colaborador de sessão aceita seu convite para ingressar em uma sessão de Windowsárea de trabalho remota, o recurso Colaboração de Sessão notifica você e um ponto vermelho aparece no ícone de Colaboração VMware Horizon na bandeja do sistema. Quando um colaborador da sessão aceita seu convite para ingressar em uma sessão de área de trabalho remota do Linux, uma notificação é exibida na área de trabalho da sessão principal.

Próximo passo

Gerencie a sessão de área de trabalho remota na caixa de diálogo VMware Horizon Colaboração. Consulte Gerenciar uma sessão de área de trabalho remota compartilhada.

Gerenciar uma sessão de área de trabalho remota compartilhada

Depois de enviar um convite de colaboração de sessão, a interface do usuário de Colaboração de Sessão se transforma em um painel que mostra o estado atual da sessão de área de trabalho remota compartilhada (sessão colaborativa) e permite que você execute determinadas ações.

Um administrador do Horizon pode impedir a transferência do controle para um colaborador da sessão. Para áreas de trabalho remotas Windows, consulte a configuração de política de grupo **Permitir controle passando para colaboradores (Allow control passing to collaborators)** no documento *Configurando recursos de área de trabalho remota no Horizon*. Para áreas de trabalho remotas do Linux, consulte o parâmetro `collaboration.enableControlPassing` no documento *Configuração de desktops Linux no Horizon*.

Pré-requisitos

Inicie uma sessão colaborativa. Consulte Convidar um usuário para ingressar em uma sessão de área de trabalho remota.

Procedimentos

1 Na área de trabalho remota, clique no ícone **VMware Horizon Colaboração** na bandeja do sistema.

Os nomes de todos os colaboradores da sessão aparecem na coluna Nome e seus status aparecem na coluna Status.

2 Use o painel Colaboração de sessão do VMware Horizon para gerenciar a sessão colaborativa.

Opção	Ação
Revogar um convite ou remover um colaborador	Clique em **Remover (Remove)** na coluna Status.
Entregar o controle a um colaborador da sessão	Depois que o colaborador da sessão ingressar na sessão, alterne a chave na coluna Controle para **Ativado (On)**. Para retomar o controle da sessão, clique duas vezes ou pressione qualquer tecla. O colaborador da sessão também pode devolver o controle alternando a chave na coluna Controle para **Desativado (Off)** ou clicando no botão **Devolver controle (Give Back Control)**.
Adicionar um colaborador	Clique em **Adicionar colaboradores (Add Collaborators)**.
Encerrar a sessão colaborativa	Clique em **Encerrar colaboração (End Collaboration)**. Todos os colaboradores ativos estão desconectados. Em Windows áreas de trabalho remotas, você também pode encerrar a sessão colaborativa clicando no botão **Parar (Stop)** ao lado do ícone **VMware Horizon Colaboração de sessão**. O botão **Parar (Stop)** não está disponível em áreas de trabalho remotas do Linux.

Ingressar em uma Sessão de Área de Trabalho Remota

Com o recurso Colaboração de Sessão, você pode clicar no link em um convite de colaboração para ingressar em uma sessão de área de trabalho remota. O link pode estar em um e-mail ou mensagem instantânea, ou em um documento que o proprietário da sessão encaminha para você. Como alternativa, você pode fazer login no servidor e clicar duas vezes no ícone da sessão na área de trabalho remota e na janela do seletor de aplicativos.

Este procedimento descreve como ingressar em uma sessão de área de trabalho remota a partir de um convite de colaboração.

Observação Em um ambiente do Cloud Pod Architecture, você não pode ingressar em uma sessão colaborativa fazendo login no servidor, a menos que faça login no pod do proprietário da sessão.

Ao ingressar em uma sessão de área de trabalho remota com o recurso Colaboração de Sessão, você não pode usar os seguintes recursos na sessão de área de trabalho remota.

- Redirecionamento USB
- Áudio e vídeo em tempo real (RTAV)
- Redirecionamento de multimídia
- Redirecionamento de unidade do cliente
- Redirecionamento de cartão inteligente
- VMware Integrated Printing
- Redirecionamento do Microsoft Lync
- Redireccionamento de ficheiros e funcionalidade Keep in Dock
- Redirecionamento da área de transferência

Você também não pode alterar a resolução da área de trabalho remota na sessão da área de trabalho remota.

Pré-requisitos

Para ingressar em uma sessão de área de trabalho remota com o recurso Colaboração de Sessão, você deve ter o Horizon Client para Windows, Mac ou Linux instalado no sistema cliente ou deve usar HTML Access.

Procedimentos

1 Clique no link no convite de colaboração.

  Horizon Client é aberto no sistema do cliente.

2 Digite suas credenciais para fazer login em Horizon Client.

   Depois que você for autenticado com êxito, a sessão colaborativa começará e você poderá ver a área de trabalho remota do proprietário da sessão. Se o proprietário da sessão transferir o controle do mouse e do teclado para você, você poderá usar a área de trabalho remota.

3 Para retornar o controle do mouse e do teclado ao proprietário da sessão, clique no ícone **VMware Horizon Colaboração** na bandeja do sistema e alterne a chave na coluna Controle para **Desativado (Off)** ou clique no botão **botão }Devolver controle (Give Back Control)**.

4 Para sair da sessão colaborativa, clique em **Opções (Options) > Desconectar (Disconnect)**.

Compartilhar pastas e unidades locais

Com o recurso de redirecionamento de unidade do cliente, você pode compartilhar pastas e unidades no sistema do cliente local com áreas de trabalho remotas e aplicativos publicados.

As unidades compartilhadas podem incluir unidades mapeadas e dispositivos de armazenamento USB. As unidades mapeadas podem ter caminhos UNC (Convenção Universal de Nomenclatura).

O comprimento máximo do nome de uma pasta compartilhada é de 117 caracteres.

O recurso de redirecionamento de unidade do cliente não é compatível com o compartilhamento do Microsoft OneDrive, do Google Drive e do armazenamento de arquivos corporativos.

Em uma área de trabalho remota Windows, as pastas e unidades compartilhadas aparecem na pasta **Este PC (This PC)** ou na pasta **Computador (Computer)**, dependendo da versão do sistema operacional Windows. Em um aplicativo publicado, como o Bloco de Notas, você pode procurar e abrir um arquivo em uma pasta ou unidade compartilhada.

As configurações de redirecionamento de unidade do cliente se aplicam a todas as áreas de trabalho remotas e aplicativos publicados.

Pré-requisitos

Para compartilhar pastas e unidades com uma área de trabalho remota ou aplicativo publicado, o recurso de redirecionamento de unidade do cliente deve estar instalado em Horizon Agent. O recurso de redirecionamento de unidade do cliente é instalado por padrão.

Você pode ocultar o recurso de redirecionamento de unidade do cliente em Horizon Client ativando uma configuração de política de grupo. Para obter mais informações, consulte **Desativar compartilhamento de arquivos e pastas (Disable sharing files and folders)** em Usando configurações de política de grupo para configurar Horizon Client.

Com o Horizon Agent 7.8 e versões posteriores, você pode configurar o comportamento da letra de unidade para unidades redirecionadas pelo recurso de redirecionamento de unidade do cliente definindo a configuração de política de grupo **Exibir dispositivo redirecionado com letra de unidade (Display redirected device with drive letter)**. Para obter mais informações, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.

Com o Horizon Agent 7.9 e versões posteriores, você pode incluir ou excluir pastas em dispositivos que têm IDs de fornecedor e produto especificados de serem redirecionados usando **Incluir dispositivo Vid/Pid (Include Vid/Pid Device)** e **Excluir dispositivo Vid/Pid{ (Exclude Vid/Pid Device)** configurações de política de grupo. Para obter mais informações, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.

Com o Horizon Agent 7.10 e posterior, você pode configurar como as letras de unidade são mapeadas usando as configurações de política de grupo **Configurar modo de mapeamento de letra de unidade (Configure drive letter mapping mode)** e **Definir tabela de mapeamento de letra de unidade (Define drive letter mapping table)**. Para obter mais informações, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.

Se o túnel seguro estiver ativado na instância do Servidor de Conexão, configurar o navegador no sistema cliente para usar um servidor proxy poderá causar um desempenho ruim no redirecionamento da unidade do cliente. Para obter o melhor desempenho de redirecionamento da unidade do cliente, configure o navegador para não usar um servidor proxy ou detectar as configurações de LAN automaticamente.

Procedimentos

1 Abra a caixa de diálogo Configurações e exiba o painel Compartilhamento de unidade.

Opção	Descrição
Na janela do seletor de aplicativos e área de trabalho	Clique com o botão direito do mouse em uma área de trabalho remota ou no ícone de um aplicativo publicado, selecione **Configurações (Settings)** e selecione **Compartilhamento de unidade (Drive Sharing)** no painel esquerdo da janela exibida.
Na caixa de diálogo Compartilhamento exibida quando você se conecta a uma área de trabalho remota ou aplicativo publicado	Clique no link **Configurações (Settings) > Compartilhamento do Drive (Drive Sharing)** na caixa de diálogo.
De dentro de uma área de trabalho remota	Selecione **Opções (Options) > Configurações (Settings) > Compartilhamento do Drive (Drive Sharing)** na barra de menus.

2 Defina as configurações de redirecionamento da unidade do cliente.

Opção	Ação
Compartilhar uma pasta ou unidade específica com áreas de trabalho remotas e aplicativos publicados	Clique no botão **Adicionar (Add)**, procure e selecione a pasta ou unidade a ser compartilhada. **Observação** Se um dispositivo USB já estiver conectado a uma área de trabalho remota ou aplicativo publicado com o recurso de redirecionamento de USB, você não poderá compartilhar uma pasta no dispositivo USB. Além disso, não ative o recurso de redirecionamento de USB que conecta dispositivos USB automaticamente na inicialização ou quando o dispositivo é inserido. Se você fizer isso, na próxima vez que você iniciar o Horizon Client ou conectar o dispositivo USB, o dispositivo se conectará com o recurso de redirecionamento de USB em vez de com o recurso de redirecionamento de unidade do cliente. Se o mapeamento de letra de unidade estiver configurado, as pastas configuradas na lista de compartilhamento não serão redirecionadas. Para obter mais informações, consulte "Usar a política de grupo para configurar o comportamento da letra de unidade" no documento *Configurando recursos de área de trabalho remota no Horizon*.
Interromper o compartilhamento de uma pasta ou unidade específica	Selecione a pasta ou unidade na lista Pastas e clique no botão **Remover (Remove)**.
Conceder a áreas de trabalho remotas e aplicativos publicados acesso a arquivos em seu diretório de usuários local	Ative a opção **Compartilhar seus arquivos locais *nome de usuário***.

Opção	Ação
Compartilhar dispositivos de armazenamento USB com áreas de trabalho remotas e aplicativos publicados	Ative a opção **Permitir acesso automático ao armazenamento removível (Allow auto access to removable storage)**. O recurso de redirecionamento de unidade do cliente compartilha automaticamente todos os dispositivos de armazenamento USB inseridos no sistema do cliente e todas as unidades externas FireWire e conectadas por Thunderbolt. Não é necessário selecionar um dispositivo específico para compartilhar. **Observação** Os dispositivos de armazenamento USB já conectados a uma área de trabalho remota ou aplicativo publicado com o recurso de redirecionamento USB não são compartilhados. Se você estiver usando um pen drive USB criptografado, deverá iniciar o Horizon Client antes de conectar o dispositivo USB para que o Horizon Client possa detectar o dispositivo. Se essa opção estiver desativada, você poderá usar o recurso de redirecionamento USB para conectar dispositivos de armazenamento USB a áreas de trabalho remotas e aplicativos publicados.
Não mostrar a caixa de diálogo Compartilhamento ao se conectar a uma área de trabalho remota ou aplicativo publicado	Marque a caixa de seleção **Não mostrar a caixa de diálogo ao conectar-se a uma área de trabalho ou aplicativo (Do not show dialog when connecting to a desktop or application)**. Se essa caixa de seleção estiver desmarcada, a caixa de diálogo Compartilhamento aparecerá na primeira vez que você se conectar a uma área de trabalho remota ou aplicativo publicado. Por exemplo, se você fizer login em um servidor e se conectar a uma área de trabalho remota, verá a caixa de diálogo Compartilhamento. Se você se conectar a outra área de trabalho remota ou aplicativo publicado, não verá a caixa de diálogo. Para ver a caixa de diálogo novamente, você deve se desconectar do servidor e fazer login novamente.

Próximo passo

Verifique se você pode ver as pastas compartilhadas de dentro da área de trabalho remota ou do aplicativo publicado.

- Em uma área de trabalho remota do Windows, abra o Explorador de Arquivos e procure na pasta **Este PC (This PC)** ou abra o Windows Explorer e procure na pasta **Computador (Computer)**, dependendo do Windows versão do sistema operacional.
- Em um aplicativo publicado, selecione **Arquivo (File) > Abrir (Open)** ou **Arquivo (File) > Salvar como (Save As)** e navegue para a pasta ou unidade.

As pastas e unidades que você selecionou para compartilhamento podem usar uma (ou mais) das seguintes convenções de nomenclatura.

Convenção de nomenclatura	Exemplo
folder-name em *desktop-name*	jsmith em JSMITH-W03
folder-name (*drive-number*:)	jsmith (Z:)
folder-name em *desktop-name* (*drive-number*:)	jsmith em JSMITH-W03 (Z:)

Para algumas versões do Horizon Agent, uma pasta redirecionada pode ter duas entradas, como em **Dispositivos e unidades (Devices and drives)** e **Locais de rede (Network locations)** em Windows 10, e ambas as entradas podem aparecer na mesma tempo. Se todos os rótulos de volume (de A: a Z:) já estiverem em uso, a pasta redirecionada terá apenas uma entrada.

Abrir arquivos locais em aplicativos publicados

Você pode ativar a capacidade de abrir arquivos locais em aplicativos publicados diretamente do sistema de arquivos local.

Com esse recurso, o menu **Abrir com (Open with)** no sistema cliente lista os aplicativos publicados disponíveis quando você clica com o botão direito do mouse em um arquivo local.

Você também pode definir que os arquivos sejam abertos automaticamente em aplicativos publicados ao clicar duas vezes no arquivo. Com esse recurso, todos os arquivos no sistema de arquivos local que têm determinadas extensões de arquivo são registrados no servidor no qual você está conectado. Por exemplo, se o Microsoft Word for um aplicativo publicado no servidor, você poderá clicar com o botão direito do mouse em um arquivo `.docx` no sistema de arquivos local e abrir o arquivo com o aplicativo publicado do Microsoft Word.

Pré-requisitos

Para abrir arquivos locais em aplicativos publicados, um administrador do Horizon deve instalar o recurso de redirecionamento de unidade do cliente em Horizon Agent. O recurso de redirecionamento de unidade do cliente é instalado por padrão. Para obter mais informações, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.

Você pode ocultar o recurso de redirecionamento de unidade do cliente em Horizon Client ativando uma configuração de política de grupo. Para obter mais informações, consulte **Desativar compartilhamento de arquivos e pastas (Disable sharing files and folders)** em Usando configurações de política de grupo para configurar Horizon Client.

Procedimentos

1 Conecte-se a um servidor.

2 Abra a caixa de diálogo Configurações e exiba o painel Aplicativos.

Opção	Descrição
Na janela do seletor de aplicativos e área de trabalho	Clique com o botão direito do mouse em uma área de trabalho remota ou no ícone de um aplicativo publicado, selecione **Configurações (Settings)** e selecione **Aplicativos (Applications)** no painel esquerdo da janela exibida.
No menu de contexto do ícone da bandeja do sistema quando você se conecta a uma área de trabalho remota ou aplicativo publicado	Clique no link **Configurações (Settings) > Compartilhamento (Sharing)** na caixa de diálogo.
De dentro de uma área de trabalho remota	Selecione **Opções (Options) > Configurações (Settings)** na barra de menus da área de trabalho remota e selecione **Aplicativos (Applications)** no painel esquerdo da janela exibida.

3 Marque a caixa de seleção **Abrir arquivos locais em aplicativos hospedados (Open local files in hosted applications)**.

   Quando essa opção está habilitada, você pode clicar com o botão direito do mouse em um arquivo no sistema de arquivos local e selecionar para abrir o arquivo em um aplicativo publicado. Você também pode alterar as propriedades do arquivo para que todos os arquivos com essa extensão de arquivo sejam abertos com o aplicativo publicado por padrão, como quando você clica duas vezes no arquivo. Por exemplo, você pode clicar com o botão direito do mouse em um arquivo, selecionar **Propriedades (Properties)** e clicar em **Alterar (Change)** para selecionar o aplicativo publicado para abrir arquivos desse tipo.

Copiando e colando

Por padrão, você pode copiar e colar do sistema cliente para uma área de trabalho remota ou um aplicativo publicado.

Se você usar o protocolo de exibição VMware Blast ou o protocolo de exibição PCoIP, um administrador do Horizon poderá configurar esse recurso para que as operações de copiar e colar sejam permitidas somente do sistema do cliente para uma área de trabalho remota ou aplicativo publicado, ou apenas de uma área de trabalho remota ou aplicativo publicado para o sistema do cliente, ou ambos, ou nenhum.

Os formatos de dados a seguir são compatíveis.

- CF_BITMAP
- CF_DIB
- CF_HDROP (tipo de arquivo)
- CF_UNICODETEXT
- Biff12
- Art::GML ClipFormat
- Formato HTML
- RTF (Rich Text Format)

Um administrador do Horizon configura a capacidade de copiar e colar definindo políticas de grupo do agente. Dependendo da versão do servidor e do agente do Horizon, um administrador do Horizon também poderá usar políticas de grupo para restringir os formatos da área de transferência durante operações de copiar e colar ou usar Políticas Inteligentes para controlar o comportamento de copiar e colar em áreas de trabalho remotas. Para obter mais informações, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.

Copiando e colando texto e imagens

Por padrão, você pode copiar e colar do sistema cliente para uma área de trabalho remota ou um aplicativo publicado. Você também poderá copiar e colar de uma área de trabalho remota ou aplicativo publicado para o sistema cliente ou entre duas áreas de trabalho remotas ou aplicativos publicados, se um administrador do Horizon habilitar esses recursos.

Por exemplo, para copiar texto no sistema do cliente, selecione o texto e pressione Ctrl+C. Para colar o texto em uma área de trabalho remota, pressione Ctrl+V na área de trabalho remota.

Esse recurso tem as seguintes limitações.

- Se você estiver copiando texto formatado, alguns dos dados serão texto e outros serão informações de formatação. Se você copiar uma grande quantidade de texto ou texto formatado e uma imagem, ao tentar colar o texto e a imagem, poderá ver parte ou todo o texto sem formatação, mas nenhuma formatação ou imagem. Esse problema ocorre porque os três tipos de dados às vezes são armazenados separadamente. Por exemplo, dependendo do tipo de documento, as imagens podem ser armazenadas como imagens ou como dados RTF.
- Se o texto e os dados RTF juntos usarem menos do que o tamanho máximo da área de transferência, o texto formatado será colado. Muitas vezes, os dados RTF não podem ser truncados, de modo que, se o texto e a formatação usarem mais do que o tamanho máximo da área de transferência, os dados RTF serão descartados e o texto sem formatação será colado.
- Se não for possível colar todo o texto e imagens formatados que você selecionou em uma operação, talvez seja necessário copiar e colar quantidades menores em cada operação.

Copiando e colando arquivos e pastas

Por padrão, você pode copiar e colar arquivos e pastas do sistema do cliente em uma área de trabalho remota ou em um aplicativo publicado. Você também poderá copiar e colar arquivos e pastas de uma área de trabalho remota ou aplicativo publicado no sistema cliente se um administrador do Horizon habilitar esses recursos.

Por exemplo, para copiar um arquivo no sistema do cliente, selecione o arquivo e pressione Ctrl+C. Para colar o arquivo em uma área de trabalho remota, pressione Ctrl+V na área de trabalho remota.

Esse recurso requer o Horizon Agent 2012 ou posterior na máquina do agente.

O recurso de redirecionamento de unidade do cliente deve ser instalado na máquina do agente para usar esse recurso. Para obter mais informações, consulte o documento *Configurando áreas de trabalho virtuais no Horizon* ou *Configurando áreas de trabalho e aplicativos publicados no Horizon*.

Você pode desativar esse recurso ativando as configurações **Filtrar arquivos e pastas dos dados da área de transferência de entrada (Filter files and folders from incoming clipboard data)** e **Filtrar arquivos e pastas dos dados da área de transferência de saída (Filter files and folders from outgoing clipboard data)** nas **Configurar formatos de redirecionamento da área de transferência (Configure clipboard redirection formats)** configuração de política de grupo para a máquina do agente. Para obter informações sobre as configurações de política de grupo do agente que controlam esse recurso, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.

Esse recurso tem as seguintes limitações.

- Pode não funcionar para algumas pastas especiais, como a pasta da área de trabalho ou uma pasta de lista de arquivos acessada recentemente, quando você tenta copiar e colar vários arquivos, pois a pasta pode mostrar arquivos e pastas que não estão na mesma pasta pai. Esse recurso só pode copiar e colar arquivos e pastas que estejam na mesma pasta pai.
- Pode não funcionar para determinados aplicativos, como o WordPad e o PowerPoint.
- Somente uma operação de copiar e colar é permitida por vez. Operações adicionais de copiar e colar são ignoradas.

Log da atividade de copiar e colar

Quando você ativa o recurso de auditoria da área de transferência, o Horizon Agent registra informações sobre a atividade de copiar e colar em um log de eventos na máquina do agente. O recurso de auditoria da área de transferência está desativado por padrão.

Esse recurso se aplica somente à cópia e colagem de texto e imagens. Ela não se aplica à cópia e colagem de arquivos e pastas.

Para ativar o recurso de auditoria da área de transferência, você deve definir a configuração de política de grupo **Configurar auditoria da área de transferência (Configure clipboard audit)**.

Se o Horizon Agent 7.6 estiver instalado na máquina do agente, somente as informações sobre os dados da área de transferência copiados da máquina do agente para a máquina do cliente serão registradas no log de eventos. Se o Horizon Agent 7.7 ou posterior estiver instalado na máquina do agente, você poderá configurar o recurso de auditoria da área de transferência para registrar informações apenas sobre os dados copiados da máquina cliente para a máquina agente, somente sobre os dados copiados da máquina agente para a máquina cliente ou sobre dados copiados em ambas as direções.

Você também pode definir a configuração de política de grupo **Se bloquear o redirecionamento da área de transferência para o lado do cliente quando o cliente não oferecer suporte à auditoria (Whether block clipboard redirection to client side when client doesn't support audit)** para especificar se o redirecionamento da área de transferência deve ser bloqueado para clientes que não oferecem suporte ao recurso de auditoria da área de transferência.

Para obter mais informações sobre as configurações de política de grupo para redirecionamento da área de transferência, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.

O log de eventos em que as informações sobre a atividade de copiar e colar são registradas é denominado VMware Horizon Auditoria de RX. Para visualizar o log de eventos na máquina do agente, use o visualizador de eventos Windows. Para visualizar o log de eventos de um local centralizado, configure o VMware Log Insight ou o Windows Coletor de Eventos. Para obter informações sobre Log Insight, vá para https://docs.vmware.com/br/vRealize-Log-Insight/index.html. Para obter informações sobre o Windows Event Collector, consulte a documentação da Microsoft.

Configurando o tamanho da memória da área de transferência do cliente

O tamanho da memória da área de transferência é configurável para o servidor e o cliente.

Esse recurso se aplica somente à cópia e colagem de texto e imagens. Ela não se aplica à cópia e colagem de arquivos e pastas.

Quando uma sessão PCoIP ou VMware Blast é estabelecida, o servidor envia o tamanho da memória da área de transferência para o cliente. O tamanho efetivo da memória da área de transferência é o menor dos valores de tamanho de memória da área de transferência do servidor e do cliente.

Para definir o tamanho da memória da área de transferência do cliente, modifique o valor de registro Windows `HKLM\Software\VMware, Inc.\VMware VDPService\Plugins\MKSVchan\ClientClipboardSize`. O tipo de valor é REG_DWORD. O valor é especificado em KB. Se você especificar 0 ou não especificar um valor, o tamanho padrão da memória da área de transferência do cliente será de 8192 KB (8 MB).

Um tamanho grande de memória da área de transferência pode afetar negativamente o desempenho, dependendo da sua rede. VMware recomenda que você não defina o tamanho da memória da área de transferência para um valor superior a 16 MB.

Para transferir grandes quantidades de dados, use o recurso de redirecionamento de unidade do cliente.

Arrastar e soltar

O recurso de arrastar e soltar funciona de forma diferente dependendo da versão do Horizon Agent e de como ela está configurada.

Com o Horizon Agent 7.9 e posterior, você pode arrastar e soltar arquivos, pastas, texto, rich text e imagens entre o sistema do cliente e as áreas de trabalho remotas e os aplicativos publicados. Com o Horizon Agent 7.7 e 7.8, você pode arrastar e soltar somente arquivos e pastas entre o sistema do cliente e as áreas de trabalho remotas e os aplicativos publicados. As versões anteriores do Horizon Agent não suportam arrastar e soltar.

Os formatos de dados a seguir são compatíveis.

- Formato HTML
- Formato Rich Text (RTF)
- CF_BITMAP
- CF_DIB
- CF_UNICODETEXT
- FileGroupDescriptorW
- FileGroupDescriptor
- FileContents

Dependendo da versão do Horizon Agent, um administrador do Horizon pode usar determinadas configurações de política de grupo ou Políticas inteligentes para configurar o comportamento de arrastar e soltar. Para obter informações completas sobre como configurar o recurso de arrastar e soltar, consulte o documento *Configurando recursos de área de trabalho remota no Horizon* para sua versão do VMware Horizon.

Arrastar texto e imagens

Com o Horizon Agent 7.9 e posterior, você pode arrastar texto, imagens e outros formatos de dados do sistema cliente para um aplicativo aberto em uma área de trabalho remota ou um aplicativo publicado. Por exemplo, você pode arrastar texto de um navegador no sistema cliente e soltá-lo no aplicativo WordPad em uma área de trabalho remota. Dependendo de como o recurso de arrastar e soltar estiver configurado, você também poderá arrastar texto, imagens e outros formatos de dados de um aplicativo aberto em uma área de trabalho remota ou um aplicativo publicado para o sistema cliente.

Um administrador do Horizon pode configurar o comportamento de arrastar e soltar definindo as configurações de política de grupo. Com o Horizon Agent 7.9 e o Dynamic Environment Manager 9.8 e posterior, um administrador do Horizon também pode usar Políticas inteligentes para configurar o comportamento de arrastar e soltar, incluindo a desativação de todo o recurso de arrastar e soltar. Para obter mais informações, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.

Arrastar arquivos e pastas

Com o Horizon Agent 7.7 e posterior, você pode arrastar e soltar arquivos e pastas entre o sistema cliente do Windows e as áreas de trabalho remotas e os aplicativos publicados. Você pode arrastar e soltar vários arquivos e pastas ao mesmo tempo. Uma barra de progresso mostra o status da operação de arrastar e soltar.

Se você arrastar um arquivo ou uma pasta entre o sistema cliente e uma área de trabalho remota, o arquivo ou a pasta aparecerá no sistema de arquivos do sistema de destino. Se você arrastar um arquivo e soltá-lo em um aplicativo aberto, como o Bloco de Notas, o texto aparecerá no aplicativo. Se você arrastar um arquivo para uma nova mensagem de e-mail, o arquivo se tornará um anexo da mensagem de e-mail.

Por padrão, arrastar e soltar do sistema cliente para áreas de trabalho remotas e aplicativos publicados está ativado, e arrastar e soltar de áreas de trabalho remotas e aplicativos publicados para o sistema cliente está desativado. Um administrador do Horizon pode controlar a direção de arrastar e soltar definindo as configurações de política de grupo.

Arrastar e soltar arquivos, pastas e conteúdo de arquivos requer que o recurso de redirecionamento de unidade do cliente esteja instalado em Horizon Agent. O recurso de redirecionamento de unidade do cliente é instalado por padrão. Para obter informações completas sobre como configurar o recurso de arrastar e soltar, incluindo os requisitos do recurso, consulte o documento *Configurando recursos de área de trabalho remota no Horizon* para sua versão do VMware Horizon.

Dicas para usar o recurso Arrastar e Soltar

Ao usar o recurso de arrastar e soltar, siga estas dicas.

Observação Dependendo da versão do Horizon Agent, algumas dicas podem não se aplicar ao seu ambiente.

- Você deve usar o protocolo de exibição VMware Blast ou PCoIP.
- Se o recurso de mouse relativo estiver ativado (selecione **Configurações (Settings) > Ativar mouse relativo (Enable Relative Mouse)** depois de se conectar a uma área de trabalho remota que suporte esse recurso), você só poderá arrastar e soltar do sistema cliente para uma área de trabalho virtual.
- Quando uma operação de arrastar e soltar está em andamento, você não pode iniciar uma nova operação de arrastar e soltar até que a primeira operação de arrastar e soltar seja concluída.
- Você não pode usar o recurso de arrastar e soltar no modo aninhado.
- Ao arrastar e soltar, você deve usar o botão principal do mouse (por padrão, o botão esquerdo). Não há suporte para usar o botão secundário do mouse (por padrão, o botão direito) e pressionar Ctrl+Shift+Alt mais o botão principal do mouse.
- Você não pode arrastar e soltar entre áreas de trabalho remotas.
- Não é possível arrastar e soltar entre aplicativos publicados de farms diferentes.

- Se você arrastar e soltar um arquivo ou uma pasta entre o sistema cliente e uma área de trabalho remota, o arquivo ou a pasta aparecerá no sistema de arquivos do sistema de destino. Se você arrastar um arquivo e soltá-lo em um aplicativo aberto, como o Bloco de Notas, o texto aparecerá no aplicativo. Se você arrastar um arquivo para uma nova mensagem de e-mail, o arquivo se tornará um anexo da mensagem de e-mail.
- Você pode arrastar e soltar vários arquivos e pastas ao mesmo tempo. Uma barra de progresso mostra o status da operação de arrastar e soltar.
- Por padrão, arrastar e soltar do sistema cliente para áreas de trabalho remotas e aplicativos publicados está ativado, e arrastar e soltar de áreas de trabalho remotas e aplicativos publicados para o sistema cliente está desativado.
- Se você estiver arrastando texto formatado, alguns dos dados serão texto e outros serão informações de formatação. Se você arrastar uma grande quantidade de texto formatado ou texto e uma imagem, ao tentar soltar o texto e a imagem, poderá ver parte ou todo o texto sem formatação, mas nenhuma formatação ou imagem. Esse problema ocorre porque os três tipos de dados às vezes são armazenados separadamente. Por exemplo, dependendo do tipo de documento, as imagens podem ser armazenadas como imagens ou como dados RTF.
- Se você estiver arrastando dados de texto sem formatação e RTF, e o tamanho total dos dados for menor que o limite de tamanho de arrastar e soltar, o texto formatado será copiado. Como os dados RTF não podem ser truncados, se o tamanho total dos dados for maior que o limite de tamanho de arrastar e soltar, os dados RTF serão descartados e somente o texto sem formatação (ou parte do texto sem formatação) será copiado.
- Se não for possível arrastar todo o texto e imagens formatados em uma operação, talvez seja necessário arrastar quantidades menores em cada operação.
- Quando você arrasta um arquivo do sistema cliente e o solta em um aplicativo publicado, não pode clicar em **Salvar como (Save as)** para copiar o arquivo de volta para um arquivo diferente no sistema cliente. Você pode clicar em **Salvar (Save)** para copiar o arquivo de volta para o mesmo arquivo no sistema do cliente.
- Se você arrastar um arquivo do sistema do cliente para um aplicativo em uma área de trabalho remota, o arquivo será copiado para a área de trabalho remota e você só poderá editar a cópia do arquivo.
- Em uma máquina Windows de 64 bits, se você não conseguir arrastar de Horizon Client para um aplicativo local de 64 bits, tente usar a versão de 32 bits do aplicativo local.
- Se o aplicativo local de destino não aceitar o objeto arrastado, tente arrastar o objeto para o sistema de arquivos local e, em seguida, arrastá-lo para o aplicativo local de destino do sistema de arquivos local.
- Existe um mecanismo de tempo limite interno para tolerância a falhas.

Dicas para usar aplicativos publicados

Os aplicativos publicados parecem aplicativos que estão instalados no sistema do cliente local. Ao usar aplicativos publicados, siga estas dicas.

- Você pode minimizar e maximizar um aplicativo publicado por meio do aplicativo publicado. Quando um aplicativo publicado é minimizado, ele aparece na barra de tarefas do sistema cliente. Você também pode minimizar e maximizar o aplicativo publicado clicando em seu ícone na barra de tarefas.
- Você pode encerrar um aplicativo publicado por meio do aplicativo publicado ou clicando com o botão direito do mouse em seu ícone na barra de tarefas.
- Você pode pressionar Alt+Tab para alternar entre aplicativos publicados abertos.
- Se um aplicativo publicado criar um item da Bandeja do Sistema Windows, esse item também aparecerá na bandeja do sistema no sistema cliente. Por padrão, os ícones da bandeja do sistema aparecem apenas para mostrar notificações. Você pode personalizar esse comportamento da mesma forma que personaliza aplicativos instalados nativamente.

  Observação Se você abrir o Painel de Controle para personalizar os ícones da área de notificação, os nomes dos ícones dos aplicativos publicados serão listados como VMware Horizon Client - *nome do aplicativo*.

Reconectar-se a aplicativos publicados após se desconectar

A execução de aplicativos publicados pode permanecer aberta após você se desconectar de um servidor em Horizon Client. Você pode configurar como os aplicativos publicados em execução se comportam ao se reconectar ao servidor em Horizon Client.

Você pode desativar as configurações de comportamento de reconexão do aplicativo publicado em Horizon Client, na linha de comando ou definindo uma configuração de política de grupo. A configuração da política de grupo tem precedência sobre a configuração da linha de comando. Para obter mais informações, consulte a opção `-appSessionReconnectionBehavior` em Instalar o Horizon Client a partir da linha de comando ou a configuração de política de grupo **Comportamento de retomada de sessão do aplicativo desconectado (Disconnected application session resumption behavior)** em Usando configurações de política de grupo para configurar Horizon Client.

Procedimentos

1. Na janela Horizon Client do seletor de área de trabalho e aplicativo, clique com o botão direito do mouse em um aplicativo publicado e selecione **Configurações (Settings)**.

2 No painel Aplicativos, selecione uma configuração de comportamento de reconexão do aplicativo.

Opção	Descrição
Pedir para se reconectar para abrir aplicativos publicados	Horizon Client notifica que você tem um ou mais aplicativos publicados em execução quando você se reconecta ao servidor. Você pode clicar em **Reconectar aos aplicativos (Reconnect to applications)** para reabrir as janelas do aplicativo publicado ou em **Agora não (Not Now)** para não reabrir as janelas do aplicativo publicado.
Reconectar automaticamente para abrir aplicativos publicados	Windows para executar aplicativos publicados reabra quando você se reconecta ao servidor.
Não peça para reconectar e não reconectar automaticamente	Horizon Client não solicita que você reabra os aplicativos publicados em execução, e as janelas de aplicativos publicados em execução não reabrem quando você se reconecta ao servidor.

Resultados

A configuração terá efeito na próxima vez que Horizon Client se conectar ao servidor.

Usar várias sessões de um aplicativo publicado de diferentes dispositivos cliente

Quando o modo de várias sessões está ativado para um aplicativo publicado, você pode usar várias sessões do mesmo aplicativo publicado ao fazer logon no servidor de diferentes dispositivos cliente.

Por exemplo, se você abrir um aplicativo publicado no modo de várias sessões no cliente A e, em seguida, abrir o mesmo aplicativo publicado no cliente B, o aplicativo publicado permanecerá aberto no cliente A e uma nova sessão do aplicativo publicado será aberta no cliente B. Em comparação, quando o modo de várias sessões está desativado (modo de sessão única), a sessão do aplicativo publicado no cliente A é desconectada e reconectada no cliente B.

O recurso do modo de várias sessões tem as seguintes limitações.

- O modo de várias sessões não funciona para aplicativos que não oferecem suporte a várias instâncias, como Skype for Business.
- Se a sessão do aplicativo for desconectada enquanto você estiver usando um aplicativo publicado no modo de várias sessões, você será desconectado automaticamente e todos os dados não salvos serão perdidos.

Pré-requisitos

Um administrador do Horizon deve habilitar o modo de várias sessões para o pool de aplicativos. Os usuários não podem modificar o modo de várias sessões para um aplicativo publicado, a menos que um administrador do Horizon permita. Consulte *Configurando áreas de trabalho e aplicativos publicados no Horizon*. Esse recurso requer o Horizon 7 versão 7.7 ou posterior.

Procedimentos

1 Conecte-se a um servidor.

2 Abra a caixa de diálogo Configurações e selecione **Multi-Launch** no painel esquerdo.

   - Clique no ícone **Configurações (Settings)** (engrenagem) no canto superior direito da janela de seleção da área de trabalho e do aplicativo.
   - Clique com o botão direito do mouse em uma área de trabalho remota ou em um aplicativo publicado na janela de seleção de área de trabalho e aplicativo e selecione **Configurações (Settings)**.

   Se nenhum aplicativo publicado estiver disponível para uso no modo de várias sessões, a configuração **Multi-Launch** não aparecerá.

3 Selecione os aplicativos publicados que você deseja usar no modo de várias sessões e ative ou desative a opção **Multi-Launch**.

   Se um administrador do Horizon tiver imposto o modo de várias sessões para um aplicativo publicado, você não poderá alterar essa configuração.

Usar um IME local com aplicativos publicados

Se você usar teclados e códigos de idioma que não sejam o inglês, poderá usar um IME (editor de método de entrada) instalado no sistema do cliente local para enviar caracteres que não sejam do inglês para aplicativos publicados.

Você pode usar teclas de atalho e ícones na área de notificação (bandeja do sistema) do sistema do cliente local para alternar para um IME diferente. Você não precisa instalar um IME no servidor que hospeda o aplicativo publicado.

Quando esse recurso está ativado, o IME local é usado. Se um IME estiver instalado e configurado no servidor que hospeda o aplicativo publicado, esse IME remoto será ignorado.

Esse recurso está desativado por padrão. Ao habilitar ou desabilitar esse recurso, você deve se desconectar do servidor e fazer login novamente antes que a alteração entre em vigor.

Pré-requisitos

- Verifique se um ou mais IMEs estão instalados no sistema do cliente.
- Verifique se o idioma de entrada no sistema do cliente local corresponde ao idioma usado no IME.

Procedimentos

1 Inicie Horizon Client e conecte-se a um servidor.

2 Na janela do seletor de área de trabalho e aplicativo, clique com o botão direito do mouse em um aplicativo publicado e selecione **Configurações (Settings)**.

3 No painel **Aplicativos (Applications)**, ative a opção **Estender o IME local para aplicativos hospedados (Extend the local IME to hosted applications)**.

4 Reinicie a sessão.

Opção	Ação
Faça logoff do servidor	Desconecte-se do servidor, faça login novamente e reconecte-se ao aplicativo publicado. Você pode retomar os aplicativos publicados, que foram desconectados, mas não fechados, e quaisquer áreas de trabalho remotas.
Redefinir os aplicativos	Clique com o botão direito do mouse em um aplicativo publicado, selecione **Configurações (Settings)** e clique em **Redefinir (Reset)**. Quando você usa essa opção, as áreas de trabalho remotas abertas não são desconectadas, mas todos os aplicativos publicados são fechados e devem ser reiniciados.

A configuração terá efeito somente depois que você reiniciar a sessão. A configuração se aplica a todos os aplicativos publicados no servidor.

5 Use o IME local, pois você pode usá-lo com aplicativos instalados localmente.

Resultados

A designação do idioma e um ícone para o IME aparecem na área de notificação (bandeja do sistema) do sistema do cliente local. Você pode usar as teclas de atalho para alternar para um idioma ou IME diferente. As combinações de teclas que realizam determinadas ações, como CTRL+X para recortar texto e Alt+Seta para a direita para mover para uma guia diferente, funcionam corretamente.

Observação Em sistemas Windows 8.x, você pode especificar teclas de atalho para IMEs usando a caixa de diálogo **Serviços de texto e idiomas de entrada**, que está disponível em **Painel de controle (Control Panel) > }Região e idioma (Region and Language) > Guia Teclados e idiomas (Keyboards and Languages tab) > Botão Alterar teclados (Change Keyboards button) > Serviços de texto e idiomas de entrada (Text Services and Input Languages) > Guia Configurações avançadas de teclas (Advanced Key Settings tab)**).

Usar um IME Local com uma Área de Trabalho Remota

Se você usar teclados e códigos de idioma que não sejam o inglês, poderá usar um IME (editor de método de entrada) instalado no sistema do cliente local para enviar caracteres que não sejam do inglês para uma área de trabalho remota. O Horizon Client é compatível com chinês simplificado, chinês tradicional, japonês e coreano. As opções de clique com o botão direito do mouse são compatíveis com japonês e coreano.

Esse recurso está desativado por padrão. Quando esse recurso está ativado, você pode usar teclas de atalho e ícones na área de notificação (bandeja do sistema) do sistema do cliente local para alternar para um IME diferente.

Pré-requisitos

- Verifique se um ou mais IMEs estão instalados no sistema do cliente.

Você não precisa instalar um IME na área de trabalho remota. Se um IME estiver instalado e configurado na área de trabalho remota, ele será ignorado.

- Verifique se o idioma de entrada no sistema do cliente local corresponde ao idioma usado no IME.

Procedimentos

1. Inicie Horizon Client e conecte-se a um servidor.
2. Abra a caixa de diálogo **Configurações (Settings)** da área de trabalho remota.
   - Clique no ícone **Configurações (Settings)** (engrenagem) no canto superior direito da janela de seleção da área de trabalho e do aplicativo e selecione a área de trabalho remota no painel esquerdo.
   - Clique com o botão direito do mouse na área de trabalho remota na janela de seleção de área de trabalho e aplicativo e selecione **Configurações (Settings)**.
3. Selecione **Estender o IME local para esta área de trabalho (Extend the local IME to this desktop)**.
4. Inicie a área de trabalho remota e use o IME local, pois você pode usá-lo com aplicativos instalados localmente.

Resultados

Um novo VMware IME é ativado automaticamente na área de trabalho remota, e o status de conversão do IME é sincronizado em cada direção entre o sistema do cliente local e a área de trabalho remota.

A designação do idioma e um ícone para o IME aparecem na área de notificação (bandeja do sistema) do sistema do cliente local. Você pode usar as teclas de atalho para alternar para um idioma ou IME diferente. As combinações de teclas que realizam determinadas ações, como CTRL+X para recortar texto e Alt+Seta para a direita para mover para uma guia diferente, funcionam corretamente.

Observação Em sistemas Windows 8.x, você pode especificar teclas de atalho para IMEs usando a caixa de diálogo **Serviços de texto e idiomas de entrada**, que está disponível em **Painel de controle (Control Panel) > }Região e idioma (Region and Language) > Guia Teclados e idiomas (Keyboards and Languages tab) > Botão Alterar teclados (Change Keyboards button) > Serviços de texto e idiomas de entrada (Text Services and Input Languages) > Guia Configurações avançadas de teclas (Advanced Key Settings tab)**).

Imprimindo de uma Área de Trabalho Remota ou Aplicativo Publicado

Com o recurso VMware Integrated Printing, você pode imprimir em uma impressora de rede ou em uma impressora conectada localmente a partir de uma área de trabalho remota ou de um aplicativo publicado.

Para obter informações sobre como instalar o recurso VMware Integrated Printing, consulte o documento *Configurando áreas de trabalho virtuais no Horizon* ou *Configurando áreas de trabalho e aplicativos publicados no Horizon*.

Para obter informações sobre como configurar o recurso VMware Integrated Printing, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.

Para obter informações sobre os tipos de áreas de trabalho remotas que oferecem suporte ao recurso VMware Integrated Printing, consulte Suporte a recursos para clientes Windows.

Definir preferências de impressão para o recurso VMware Integrated Printing

Você pode definir as preferências de impressão em uma área de trabalho remota para o recurso VMware Integrated Printing. Com o recurso VMware Integrated Printing, você pode usar impressoras locais ou de rede a partir de uma área de trabalho remota sem precisar instalar drivers de impressora adicionais na área de trabalho remota Windows. Para cada impressora disponível por meio desse recurso, você pode definir preferências para compactação de dados, qualidade de impressão, impressão nos dois lados, cor e outras configurações.

Em uma área de trabalho de máquina virtual de usuário único, cada impressora virtual aparece como *<printer_name>*(*vdi*) por padrão. Em uma área de trabalho ou aplicativo publicado publicado, cada impressora virtual aparece como *<printer_name>*(v*<session_ID>*) por padrão.

A partir do Horizon Agent 7.12, você pode usar a política de grupo para modificar a convenção de nomenclatura para impressoras cliente redirecionadas. Para obter informações, consulte o documento *Configurando recursos de área de trabalho remota no Horizon* para sua versão do Horizon Agent.

Você pode usar o Windows Registry para definir as configurações padrão VMware Integrated Printing para Horizon Client. Consulte Usando o Windows Registry para configurar o Horizon Client.

Pré-requisitos

Para usar o VMware Integrated Printing, um administrador do Horizon deve instalar o recurso VMware Integrated Printing na área de trabalho remota. Essa tarefa envolve a ativação da opção **VMware Integrated Printing** no instalador do Horizon Agent. Para obter informações sobre como instalar o Horizon Agent, consulte o documento *Configurando áreas de trabalho virtuais no Horizon* ou *Configurando áreas de trabalho e aplicativos publicados no Horizon*. Para obter informações sobre como configurar o recurso VMware Integrated Printing, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.

Para determinar se o recurso VMware Integrated Printing está instalado em uma área de trabalho remota, verifique se o arquivo `C:\Program Files\Common Files\VMware\}\Remote Experience\x64\vmware-print-redir-server.exe` } e os arquivos `C:\Program Files\Common Files\VMware\}\Remote Experience\x64\vmware-print-redir-service.exe` existem no sistema de arquivos da área de trabalho remota.

Esse recurso requer o Horizon Agent 7.7 ou posterior.

Procedimentos

1. Na área de trabalho remota Windows, vá para **Painel de controle (Control Panel) > Hardware e som (Hardware and Sound) > Dispositivos e impressoras (Devices and Printers)**.
2. Na janela **Dispositivos e Impressoras**, clique com o botão direito do mouse na impressora virtual e selecione **Propriedades da impressora (Printer properties)** no menu de contexto.
3. Na guia **Geral (General)**, clique em **Preferências (Preferences)**.
4. Na caixa de diálogo Preferências de impressão, selecione as diferentes guias e especifique as configurações a serem usadas.
5. Para salvar suas alterações, clique em **OK**.

Imprimindo de uma área de trabalho remota para uma impressora USB local

Uma impressora USB é uma impressora conectada a uma porta USB no sistema do cliente local. Você pode enviar trabalhos de impressão para uma impressora USB conectada ao sistema do cliente local a partir de uma área de trabalho remota.

Você pode usar o recurso de redirecionamento USB ou o recurso VMware Integrated Printing para imprimir em uma impressora USB a partir de uma área de trabalho remota. Impressoras USB redirecionadas e impressoras virtuais podem trabalhar juntas sem conflito.

Usando o recurso de redirecionamento USB

Para usar o recurso de redirecionamento USB para conectar uma impressora USB a uma porta USB virtual em uma área de trabalho remota, os drivers de impressora necessários devem estar instalados na área de trabalho remota, bem como no sistema cliente.

Quando você usa o recurso de redirecionamento USB para redirecionar uma impressora USB, a impressora USB não está mais conectada logicamente à porta USB física no sistema do cliente local e não aparece na lista de impressoras locais no sistema do cliente local. Você pode imprimir na impressora USB a partir da área de trabalho remota, mas não pode mais imprimir na impressora USB a partir do sistema cliente local.

Em uma área de trabalho remota, as impressoras USB redirecionadas aparecem como *<printer_name>*.

Usando o recurso VMware Integrated Printing

Ao usar o recurso VMware Integrated Printing para enviar trabalhos de impressão para uma impressora USB, você pode imprimir na impressora USB a partir da área de trabalho remota e do sistema cliente local e não precisa instalar drivers de impressora na área de trabalho remota.

Para usar o recurso VMware Integrated Printing, o recurso deve ser ativado quando você instalar o Horizon Agent. Para obter informações de instalação, consulte o documento *Configurando áreas de trabalho virtuais no Horizon* ou *Configurando áreas de trabalho e aplicativos publicados no Horizon*.

Para obter mais informações, consulte Definir preferências de impressão para o recurso VMware Integrated Printing.

Melhorar o desempenho do mouse em uma área de trabalho remota

Se você usar o protocolo de exibição VMware Blast ou o protocolo de exibição PCoIP ao usar aplicativos 3D em uma área de trabalho remota, o desempenho do mouse melhorará quando você ativar o recurso de mouse relativo.

Na maioria das circunstâncias, se você estiver usando aplicativos que não exigem renderização em 3D, o Horizon Client transmitirá informações sobre os movimentos do ponteiro do mouse usando coordenadas absolutas. Usando coordenadas absolutas, o cliente renderiza os movimentos do mouse localmente, o que melhora o desempenho, especialmente se você estiver fora da rede corporativa.

Para trabalhos que exigem o uso de aplicativos com muitos gráficos, como o AutoCAD, ou para jogar videogames 3D, você pode melhorar o desempenho do mouse ativando o recurso de mouse relativo, que usa coordenadas relativas, em vez de absolutas.

Quando o recurso de mouse relativo está ativado, o desempenho pode ser lento se você estiver fora da rede corporativa, em uma WAN.

Pré-requisitos

Um administrador do Horizon deve ativar a renderização em 3D para o pool de desktops. Para obter informações sobre as configurações do pool e as opções disponíveis para renderização em 3D, consulte o documento *Configurando áreas de trabalho virtuais no Horizon* ou *Configurando áreas de trabalho e aplicativos publicados no Horizon*.

Procedimentos

1. Inicie Horizon Client e faça login no servidor.
2. Clique com o botão direito do mouse na área de trabalho remota e selecione **VMware Blast** ou **PCoIP**.
3. Conecte-se à área de trabalho remota.

4 Na caixa de diálogo Configurações, ative a opção **Ativar mouse relativo (Enable Relative Mouse)**.

Para desativar o recurso de mouse relativo, desative a opção **Ativar mouse relativo (Enable Relative Mouse)**.

Observação Se você usar Horizon Client no modo de janela em vez do modo de tela inteira e o recurso de mouse relativo estiver ativado, talvez não seja possível mover o ponteiro do mouse para as opções de menu Horizon Client ou mover o ponteiro para fora do Horizon Client janela. Para resolver essa situação, pressione Ctrl+Alt.

Como usar scanners

Com o recurso de redirecionamento do verificador, você pode verificar informações em áreas de trabalho remotas e aplicativos publicados com verificadores conectados ao sistema do cliente local. Esse recurso redireciona os dados de verificação com uma largura de banda significativamente menor do que a que pode ser obtida usando o redirecionamento USB.

O redirecionamento do scanner oferece suporte a dispositivos de digitalização padrão que são compatíveis com os formatos TWAIN e WIA (Windows Aquisição de Imagem). Você deve instalar os drivers de dispositivo do scanner no sistema cliente local. Você não precisa instalar os drivers do dispositivo do scanner em uma área de trabalho remota.

Se um administrador do Horizon tiver configurado o recurso de redirecionamento do verificador e você usar o protocolo de exibição VMware Blast ou o protocolo de exibição PCoIP, um verificador conectado ao sistema do cliente local poderá ser usado em uma área de trabalho remota ou em um aplicativo publicado.

Importante Não conecte um scanner a partir do menu **Conectar dispositivo USB (Connect USB Device)** em Horizon Client. O desempenho será inutilizável.

Quando a verificação de dados é redirecionada para uma área de trabalho remota ou um aplicativo publicado, você não pode acessar o verificador no computador cliente local. Por outro lado, quando um scanner está em uso no computador cliente local, você não pode acessá-lo na área de trabalho remota ou no aplicativo publicado.

Um administrador do Horizon pode definir as configurações de política de grupo para controlar as opções disponíveis na caixa de diálogo VMware Horizon Preferências de redirecionamento do scanner. Para obter mais informações, consulte o documento *Configurando recursos de área de trabalho remota no Horizon*.

Observação Se um administrador do Horizon configurar o redirecionamento do verificador para usar um verificador específico e esse verificador não estiver disponível, o redirecionamento do verificador não funcionará.

Dicas para usar o recurso de redirecionamento do scanner

- Para alterar as configurações de redirecionamento do scanner, clique no ícone do scanner () na bandeja do sistema ou na área de notificação da área de trabalho remota. Em um aplicativo publicado, o ícone da bandeja do sistema é redirecionado para o computador cliente local.

  Observação Você não precisa usar o menu que aparece quando você clica no ícone do scanner. O redirecionamento do scanner funciona sem qualquer configuração adicional. Se o menu não listar nenhum scanner, um scanner incompatível está conectado ao sistema do cliente local. Se o ícone do scanner não aparecer, o recurso de redirecionamento do scanner está desativado ou não está instalado na área de trabalho remota. O ícone do scanner também não aparece em sistemas cliente locais que não oferecem suporte a esse recurso.

- Se você quiser que a caixa de diálogo Propriedades de digitalização TWAIN apareça mesmo se um aplicativo de digitalização não exibir a caixa de diálogo de digitalização, clique na opção **Preferências (Preferences)** no menu do ícone do scanner e selecione a opção **Forçar as propriedades de digitalização TWAIN caixa de seleção dialog (Force the TWAIN Scanning Properties dialog)**.
- Para exibir os nomes reais do scanner em vez do scanner VMware Virtual *nnn*, clique na opção **Preferências (Preferences)** no menu do ícone do scanner e selecione a opção **Usar nomes definidos pelo fornecedor para scanners TWAIN{ (Use vendor defined names for TWAIN scanners)** caixa de seleção.
- Para selecionar opções para controlar a compactação da imagem ou determinar como selecionar o scanner padrão, clique na opção **Preferências (Preferences)** no menu do ícone do scanner e selecione a guia **Compressão (Compression)** ou **Padrões (Defaults)** .
- Se você planeja usar o recurso Áudio e Vídeo em Tempo Real para redirecionar webcams conforme recomendado por VMware, clique na opção **Preferências (Preferences)** no menu do ícone do scanner e selecione a opção **Ocultar dispositivos de imagem do tipo webcam{ (Hide webcam type imaging devices)** caixa de seleção.
- A maioria dos scanners TWAIN exibe uma caixa de diálogo de configurações do scanner por padrão, mas alguns não. Para os scanners que não exibem opções de configurações, você pode usar a opção **Preferências (Preferences)** no menu do ícone do scanner e selecionar a opção **Forçar a caixa de diálogo Propriedades de digitalização TWAIN (Force the TWAIN Scanning Properties dialog)**.

- Para exibir a caixa de diálogo Propriedades do scanner TWAIN na área de trabalho remota, clique na opção **Preferências (Preferences)** no menu do ícone do scanner e marque a caixa de seleção **Agente (VMware caixa de diálogo Propriedades de digitalização)**. Para exibir a caixa de diálogo Propriedades do scanner TWAIN no sistema cliente local, marque a caixa de seleção **Cliente (caixa de diálogo Propriedades da digitalização nativa, se compatível)**.

  Observação Na caixa de diálogo Propriedades do Scanner TWAIN do lado do agente, algumas opções menos comuns podem não estar incluídas. Para usar essas opções menos comuns, marque a caixa de seleção **Cliente (caixa de diálogo Propriedades de verificação nativa, se compatível)**.

- A digitalização de uma imagem muito grande ou com uma resolução muito alta pode não funcionar. Nesse caso, você pode ver o indicador de progresso da verificação congelar ou o aplicativo do scanner pode fechar inesperadamente. Se você minimizar a área de trabalho remota, uma mensagem de erro poderá aparecer no sistema do cliente local, notificando que a resolução está definida como muito alta. Para resolver esse problema, reduza a resolução ou corte a imagem para um tamanho menor e digitalize novamente.

Redirecionando portas seriais

Com o recurso de redirecionamento de porta serial, você pode redirecionar portas seriais conectadas localmente (COM), como portas RS232 integradas e adaptadores USB para serial. Dispositivos como impressoras, leitores de código de barras e outros dispositivos seriais podem ser conectados a essas portas e usados em áreas de trabalho remotas.

Se um administrador do Horizon tiver configurado o recurso de redirecionamento de porta serial e se você usar o protocolo de exibição VMware Blast ou o protocolo de exibição PCoIP, o redirecionamento de porta serial funcionará na área de trabalho remota sem configurações adicionais. Por exemplo, a COM1 no sistema do cliente local é redirecionada como COM1 na área de trabalho remota. A COM2 é redirecionada como COM2. Se a porta COM já estiver em uso, ela será mapeada para evitar conflitos. Por exemplo, se COM1 e COM2 existirem na área de trabalho remota, a COM1 no sistema cliente será mapeada para COM3 por padrão.

Você deve ter os drivers de dispositivo necessários instalados no sistema cliente local, mas não precisa instalar os drivers de dispositivo na área de trabalho remota. Por exemplo, se você usar um adaptador USB para serial que exija que drivers de dispositivo específicos funcionem no sistema cliente local, instale esses drivers, mas somente no sistema cliente.

Importante Se você estiver usando um dispositivo que se conecta a um adaptador USB para serial, não conecte o dispositivo do menu **Conectar dispositivo USB (Connect USB Device)** em Horizon Client. Isso roteará o dispositivo por meio do redirecionamento USB e ignorará o recurso de redirecionamento de porta serial.

Dicas para usar o recurso de redirecionamento de porta serial

- Clique no ícone da porta serial ( ) na bandeja do sistema ou na área de notificação da área de trabalho remota para conectar, desconectar ou personalize as portas COM mapeadas.

  Quando você clica no ícone da porta serial, o menu de contexto **Redirecionamento COM Serial para VMware Horizon** é exibido. Se um administrador tiver bloqueado a configuração, os itens no menu de contexto ficarão esmaecidos. O ícone aparecerá somente se um administrador do Horizon tiver configurado o recurso de redirecionamento de porta serial e todos os requisitos forem atendidos. Para obter mais informações, consulte Requisitos do sistema para redirecionamento de porta serial.

- No menu de contexto, os itens de porta são listados como ***port* mapeada para *port***, por exemplo, **COM1 mapeada para COM3 (COM1 mapped to COM3)**. A primeira porta, que é COM1 neste exemplo, é a porta física ou o adaptador USB para serial no sistema do cliente local. A segunda porta, que é COM3 neste exemplo, é a porta usada na área de trabalho remota.
- Para selecionar o comando **Propriedades da Porta (Port Properties)**, clique com o botão direito do mouse em uma porta COM.

  Na caixa de diálogo Propriedades COM, você pode configurar uma porta para se conectar automaticamente quando uma sessão de área de trabalho remota for iniciada ou pode ignorar o DSR (sinal de pronto para conjunto de dados), que é necessário para alguns modems e outros dispositivos.

  Você também pode alterar o número da porta que a área de trabalho remota usa. Por exemplo, se a porta COM1 no sistema cliente estiver mapeada para COM3 na área de trabalho remota, mas o aplicativo que você estiver usando exigir COM1, você poderá alterar o número da porta para COM1. Se COM1 existir na área de trabalho remota, você poderá ver **COM1 (Sobreposto)**. Você ainda pode usar essa porta sobreposta. A área de trabalho remota pode receber dados seriais por meio da porta do servidor e também do sistema do cliente.
- Conecte-se a uma porta COM mapeada antes de tentar iniciar um aplicativo que exija acesso à porta. Por exemplo, clique com o botão direito do mouse em uma porta COM e selecione **Conectar (Connect)** para usar a porta na área de trabalho remota. Quando você inicia o aplicativo, o aplicativo abre a porta serial.

  Quando uma porta COM redirecionada é aberta e está em uso em uma área de trabalho remota, você não pode acessar a porta no computador local. Por outro lado, quando uma porta COM está em uso no computador local, você não pode acessar a porta na área de trabalho remota.
- Na área de trabalho remota, você pode usar a guia Windows Gerenciador de dispositivos **Configurações de porta (Port Settings)** para definir a taxa de transmissão padrão para uma determinada porta COM. Use as mesmas configurações no Windows Gerenciador de dispositivos no sistema do cliente. As configurações dessa guia serão usadas somente se o aplicativo não especificar as configurações de porta.

- Antes de desconectar a porta COM, você deve fechar a porta no aplicativo ou fechar o aplicativo. Em seguida, você pode selecionar o comando **Desconectar (Disconnect)** para desconectar e disponibilizar a porta COM física para uso no computador cliente.
- Se você configurar uma porta serial para se conectar automaticamente, iniciar um aplicativo que abre a porta serial e, em seguida, desconectar e reconectar a sessão da área de trabalho remota, o recurso de conexão automática não funcionará. Você também não pode se conectar usando a opção de menu do ícone da bandeja do sistema da porta serial. Na maioria dos casos, o aplicativo não pode mais usar a porta serial. Você deve interromper o aplicativo, desconectar a sessão da área de trabalho remota e reconectar-se novamente para resolver o problema.

Atalhos de teclado para foco de entrada

Você pode usar as configurações de política de grupo **Combinação de teclas de atalho para obter o foco de entrada (Hotkey combination to grab input focus)** e **Combinação de teclas de atalho para liberar o foco de entrada (Hotkey combination to release input focus)** para configurar atalhos de teclado para foco de entrada.

Você pode usar a configuração de política de grupo **Foco automático de entrada em uma janela de área de trabalho virtual (Automatic input focus in a virtual desktop window)** para enviar entradas para a área de trabalho remota automaticamente quando um usuário traz a área de trabalho remota para a frente. Esses recursos são úteis para usuários que não podem usar cliques do mouse para capturar e liberar uma área de trabalho remota. Para obter mais informações, consulte Usando configurações de política de grupo para configurar Horizon Client

Sincronização de idioma de origem de entrada do teclado

Quando você se conecta a uma área de trabalho remota, o idioma de origem de entrada do teclado no sistema cliente é sincronizado na área de trabalho remota.

Esse recurso é compatível com os seguintes idiomas de origem de entrada do teclado no sistema cliente.

- Inglês
- francês
- alemão
- Japonês
- Coreano
- Espanhol
- Chinês simplificado
- Chinês tradicional

A sincronização não ocorrerá se o idioma de origem de entrada do teclado não for compatível.

A sincronização do idioma de origem de entrada do teclado é controlada pela configuração de política de grupo **Sincronização de localidade do teclado (Keyboard locale synchronization)** do lado do agente. Para obter mais informações, consulte "VMware Blast Configurações de Política de Grupo" no documento *Configurando recursos de área de trabalho remota no Horizon*.

Configurar a sincronização da chave de bloqueio

Você pode configurar o Horizon Client para sincronizar os estados de alternância das teclas Num Lock, Scroll Lock e Caps Lock do sistema do cliente para uma área de trabalho remota ativando uma configuração em Horizon Client. Essa configuração está desativada por padrão.

Você também pode usar a configuração de política de grupo Horizon Client **Sincronizar automaticamente o teclado, as teclas de rolagem e as teclas caps lock (Automatically synchronize the keypad, scroll and caps lock keys)** para configurar a sincronização da tecla de bloqueio. Quando essa configuração de política de grupo está habilitada ou desabilitada, os usuários não podem alterar a configuração de sincronização da tecla de bloqueio na interface do usuário do Horizon Client. Para obter mais informações, consulte Usando configurações de política de grupo para configurar Horizon Client.

Se a configuração de política de grupo **Sincronizar automaticamente o teclado, as teclas de rolagem e as teclas caps lock (Automatically synchronize the keypad, scroll and caps lock keys)** estiver desativada ou não estiver configurada, ou a configuração de sincronização da tecla de bloqueio Horizon Client não estiver selecionada (a configuração padrão), a tecla de bloqueio será alternada state é sincronizado da área de trabalho remota para o sistema cliente por padrão.

Procedimentos

1. Inicie Horizon Client e conecte-se a um servidor.
2. Abra a caixa de diálogo Configurações da área de trabalho remota.
   - Clique no ícone **Configurações (Settings)** (engrenagem) no canto superior direito da janela de seleção da área de trabalho e do aplicativo e selecione a área de trabalho remota no painel esquerdo.
   - Clique com o botão direito do mouse na área de trabalho remota na janela de seleção de área de trabalho e aplicativo e selecione **Configurações (Settings)**.
3. Para ativar o recurso de sincronização da tecla de bloqueio, ative a opção **Sincronizar automaticamente o teclado, as teclas de rolagem e as teclas de bloqueio (Automatically synchronize the keypad, scroll and cap lock keys)**.

Solução de problemas Horizon Client

6

Você pode resolver a maioria dos problemas com o Horizon Client reiniciando ou redefinindo áreas de trabalho remotas ou aplicativos publicados, ou reinstalando o Horizon Client.

Leia os seguintes tópicos:

Reiniciar uma Área de Trabalho Remota

Se o sistema operacional da área de trabalho remota parar de responder, talvez seja necessário reiniciar uma área de trabalho remota. Reiniciar uma área de trabalho remota é semelhante a usar o comando de reinicialização do sistema operacional Windows. O sistema operacional de área de trabalho remota geralmente solicita que você salve todos os dados não salvos antes de ser reiniciado.

Você só poderá reiniciar uma área de trabalho remota se um administrador do Horizon tiver habilitado o recurso de reinicialização para a área de trabalho remota e a área de trabalho remota estiver ligada. Você pode reiniciar apenas uma área de trabalho remota por vez.

Para obter informações sobre como ativar o recurso de reinicialização da área de trabalho, consulte o documento *Configurando áreas de trabalho virtuais no Horizon* ou *Configurando áreas de trabalho e aplicativos publicados no Horizon*.

Procedimentos

- Use o comando **Reiniciar a área de trabalho (Restart Desktop)**.

Opção	Ação
De dentro da área de trabalho remota	Selecione **Opções (Options) > Reiniciar a área de trabalho (Restart Desktop)** na barra de menus.
Na janela do seletor da área de trabalho	Clique com o botão direito do mouse no ícone da área de trabalho remota e selecione **Reiniciar área de trabalho (Restart Desktop)**.

  Horizon Client solicita que você confirme a ação de reinicialização.

Resultados

O sistema operacional na área de trabalho remota é reiniciado e o cliente desconecta e faz logoff da área de trabalho remota.

Próximo passo

Aguarde um tempo adequado para que o sistema seja reiniciado antes de tentar se reconectar à área de trabalho remota.

Se reiniciar a área de trabalho remota não resolver o problema, talvez seja necessário redefinir a área de trabalho remota. Consulte Redefinir áreas de trabalho remotas ou aplicativos publicados.

Redefinir áreas de trabalho remotas ou aplicativos publicados

Talvez seja necessário redefinir uma área de trabalho remota se o sistema operacional da área de trabalho parar de responder e reiniciar a área de trabalho remota não resolver o problema.

Redefinir uma área de trabalho remota é o mesmo que pressionar o botão Redefinir em um PC físico para forçar a reinicialização do PC. Todos os arquivos abertos na área de trabalho remota são fechados e não são salvos.

A redefinição de aplicativos publicados encerra todos os aplicativos abertos.

Você só poderá redefinir uma área de trabalho remota se um administrador do Horizon tiver ativado o recurso de redefinição para a área de trabalho remota e se a área de trabalho remota estiver ligada. Você pode redefinir apenas uma área de trabalho remota por vez.

Para obter informações sobre como ativar o recurso de redefinição da área de trabalho, consulte o documento *Configurando áreas de trabalho virtuais no Horizon* ou *Configurando áreas de trabalho e aplicativos publicados no Horizon*.

Procedimentos

1 Para redefinir uma área de trabalho remota, use o comando **Redefinir área de trabalho (Reset Desktop)**.

Opção	Ação
De dentro da área de trabalho remota	Selecione **Opções (Options) > Redefinir área de trabalho (Reset Desktop)** na barra de menus.
Na janela do seletor de aplicativos e área de trabalho	Clique com o botão direito do mouse no ícone da área de trabalho remota e selecione **Redefinir área de trabalho (Reset Desktop)**.

2 Para redefinir aplicativos publicados, use o botão **Redefinir (Reset)** na área de trabalho e na janela do seletor de aplicativos.

   a Clique no botão **Configurações (Settings)** (ícone de engrenagem) na barra de menus.

   b Selecione **Aplicativos (Applications)** no painel esquerdo, clique no botão **Redefinir (Reset)** no painel direito e clique em **OK**.

Resultados

Quando você redefine uma área de trabalho remota, o sistema operacional na área de trabalho remota é reiniciado e o cliente desconecta e faz logoff da área de trabalho remota. Quando você redefine aplicativos publicados, os aplicativos publicados são encerrados.

Próximo passo

Aguarde um tempo adequado para que o sistema seja reiniciado antes de tentar se reconectar à área de trabalho remota ou ao aplicativo publicado.

Reparar Horizon Client para Windows

Às vezes, você pode resolver problemas com o Horizon Client reparando o Horizon Client.

Pré-requisitos

- Verifique se você pode fazer login como administrador no sistema do cliente.
- Verifique se você tem o instalador Horizon Client. Você não poderá reparar o Horizon Client se não tiver o instalador.

Procedimentos

- Para reparar Horizon Client interativamente, execute uma das seguintes tarefas.
  - Clique duas vezes no instalador do Horizon Client e clique em **Reparar (Repair)**.
  - Execute o instalador do Horizon Client na linha de comando e digite o comando `/repair`.

    Por exemplo, no prompt de comando, digite o seguinte comando:

    ```
    VMware-Horizon-Client-y.y.y-xxxxxx.exe /repair
    ```

y.y.y é o número da versão e *xxxxxx* é o número da compilação.

- Para reparar o Horizon Client silenciosamente, execute o instalador do Horizon Client na linha de comando e digite os comandos `/silent` e `/repair`.

  Por exemplo, na linha de comando, digite o seguinte comando:

  ```
  VMware-Horizon-Client-y.y.y-xxxxxx.exe /silent /repair
  ```

  y.y.y é o número da versão e *xxxxxx* é o número da compilação.

Desinstalar Horizon Client para Windows

Se reparar o Horizon Client não resolver o problema, talvez seja necessário desinstalar e reinstalar o Horizon Client.

Este procedimento mostra como desinstalar o Horizon Client quando você tem o instalador do Horizon Client.

Se você não tiver o instalador do Horizon Client, poderá desinstalar o Horizon Client da mesma forma que desinstala outros aplicativos no sistema do Windows. Por exemplo, em um sistema do Windows 10, você pode usar o sistema operacional **> >** Windows).

Pré-requisitos

Verifique se você pode fazer login como administrador no sistema do cliente.

Procedimentos

- Para desinstalar o Horizon Client interativamente, execute uma das seguintes tarefas.
  - Clique duas vezes no instalador do Horizon Client e clique em **Remover (Remove)**.
  - Execute o instalador do Horizon Client na linha de comando e digite o comando `/uninstall`.

    Por exemplo, no prompt de comando, digite o seguinte comando:

    ```
    VMware-Horizon-Client-y.y.y-xxxxxx.exe /uninstall
    ```

    y.y.y é o número da versão e *xxxxxx* é o número da compilação.
- Para desinstalar o Horizon Client silenciosamente, execute o instalador do Horizon Client na linha de comando e digite os comandos `/silent` e `/uninstall`.

  Por exemplo, no prompt de comando, digite o seguinte comando:

  ```
  VMware-Horizon-Client-y.y.y-xxxxxx.exe /silent /uninstall
  ```

  y.y.y é o número da versão e *xxxxxx* é o número da compilação.

Próximo passo

Reinstale Horizon Client. Consulte Capítulo 2 Instalando e atualizando Horizon Client para Windows.

Problemas com a entrada do teclado

Quando você digita em uma área de trabalho remota ou em um aplicativo publicado, nenhuma das teclas pressionadas parece funcionar.

Problema

Quando você está conectado a uma área de trabalho remota ou aplicativo publicado, nenhum caractere aparece quando você digita. Outro sintoma pode ser que uma única chave continua se repetindo.

Causa

Alguns softwares de segurança, como o Norton 360 Total Security, incluem um recurso que detecta o software de log de pressionamentos de tecla e bloqueia o log de pressionamentos de tecla. Esse recurso de segurança destina-se a proteger o sistema contra spyware que rouba senhas e números de cartão de crédito. Esse software de segurança pode impedir que Horizon Client envie pressionamentos de tecla para a área de trabalho remota ou o aplicativo publicado.

Solução

- No sistema do cliente, desative o recurso de detecção de registro de pressionamento de tecla do seu software antivírus ou de segurança.

O que fazer se o Horizon Client for encerrado inesperadamente

Horizon Client é encerrado mesmo que você não o feche.

Problema

Horizon Client encerra inesperadamente. Dependendo da configuração do servidor, você pode ver uma mensagem como `Não há conexão segura com o Servidor de Conexão do View`. Às vezes, uma mensagem não aparece.

Causa

Esse problema ocorre quando a conexão com o servidor é perdida.

Solução

- Reinicie Horizon Client. Você poderá se conectar com êxito quando o servidor estiver em execução novamente. Se os problemas de conexão persistirem, entre em contato com o administrador do sistema ou com o Suporte da VMware.

Conectando-se a um servidor no modo Workspace ONE

Você não pode se conectar a um servidor diretamente por meio de Horizon Client ou seus direitos de área de trabalho remota e de aplicativo publicado não estão visíveis em Horizon Client.

Problema

- Quando você tenta se conectar ao servidor diretamente por meio de Horizon Client, Horizon Client redireciona você para o portal Workspace ONE.
- Quando você abre uma área de trabalho remota ou um aplicativo publicado por meio de um URI ou atalho, ou quando abre um arquivo local por meio da associação de arquivos, a solicitação redireciona você para o portal Workspace ONE para autenticação.
- Depois de abrir uma área de trabalho remota ou um aplicativo publicado por meio de Workspace ONE e o Horizon Client for iniciado, você não poderá ver ou abrir outras áreas de trabalho remotas ou aplicativos publicados autorizados em Horizon Client.

Causa

Um administrador do Horizon pode habilitar o modo Workspace ONE em uma instância do Servidor de Conexão. Esse comportamento é normal quando o modo Workspace ONE está ativado em uma instância do Servidor de Conexão.

Solução

Use Workspace ONE para se conectar a um servidor habilitado para Workspace ONE e acessar suas áreas de trabalho remotas e aplicativos publicados.