Métodos Aprovados do CallManager para o acesso remoto do Suporte técnico de Cisco

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Métodos aprovados do Acesso remoto
Cisco CallManager
VNC
WTS (Desktop remoto)
Luzes integradas para fora (ILO)
MeetingPlace de Cisco
Fixe conexões de rede
Como usar um VPN
Informações Relacionadas

Introdução

Além do que os procedimentos de Acesso remoto alistou em instalar o sistema operacional no servidor de aplicativos do Cisco IP Telephony, este documento alista os métodos usados pelo Suporte técnico de Cisco aos sistemas de acesso remotamente. Isto aumenta extremamente a capacidade do coordenador para diagnosticar e resolver edições do sistema. Embora não se exige, os clientes são incentivados altamente fornecer algum tipo do acesso para propósitos de Troubleshooting.

Éa responsabilidade do cliente fornecer todo o software requerido.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- CallManager da Cisco 3.x(x) e mais atrasado

- Virtual Network Computing (VNC)
- Serviço do Windows Terminal (WTS) (igualmente chamado Desktop remoto)
- MeetingPlace de Cisco

O WTS não é fornecido por Cisco.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Métodos aprovados do Acesso remoto

Cisco CallManager

Para obter informações adicionais sobre do Acesso remoto do CallManager da Cisco, refira o maio onde eu uso serviços terminal, o VNC, ou o ILO neste server durante o capítulo da elevação de *instalar o sistema operacional no servidor de aplicativos do Cisco IP Telephony, versão 2000.2.6*.

VNC

O VNC envia agora com o CallManager da Cisco instala o CD e é apoiado para o Acesso remoto ao CallManager da Cisco. Para obter mais informações sobre do VNC, refira o local de RealVNC .

O VNC é o único método apoiado do Acesso remoto para instalações de software e elevações.

Se você quer usar o Virtual Network Computing (VNC) para promover remotamente um servidor do CallManager da Cisco, refira a página de documentação do sistema operacional do Cisco IP Telephony para obter a versão a mais atrasada do documento VNC.

Para mais informação, refira o melhoramento da revisão do CallManager da Cisco 4.1.2.

Caution: Se você instalou o VNC mas não o planeia o usar para executar a elevação, desabilite-a para impedir o Acesso remoto ao server. Se você não desabilita o VNC e um usuário/acessos de administrador o server na altura da elevação, a elevação falha.

WTS (Desktop remoto)

Cisco instala serviços terminal. Consequentemente, o Suporte técnico de Cisco pode executar a administração remota e tarefas de Troubleshooting. O Windows Terminal Services é apoiado e preferido para a administração e o acesso de servidor remoto para o Suporte técnico de Cisco.

Limitações WTS

A instalação ou as elevações do software não são apoiadas no CallManager da Cisco.

Caution: Antes que a elevação, Cisco recomende que você desabilita serviços terminal e recarregue imediatamente o server para impedir o Acesso remoto ao server. Se você alcança o server com os serviços terminal, faz com às vezes que a elevação falhe.

Depois que você promove o server, você deve permitir serviços terminal.

Para obter mais informações sobre do WTS, refira o local WTS de Microsoft .

Luzes integradas para fora (ILO)

Não use o ILO para executar tarefas da elevação ou da instalação. Cisco apoia o ILO para o Gerenciamento remoto e as tarefas de configuração somente.

Para obter mais informações sobre do ILO, refira aproximadamente o ILO.

MeetingPlace de Cisco

O MeetingPlace de Cisco é uma ferramenta original usada pelo Suporte técnico para Conferências web. Permite o acesso aos sistemas com o HTTP. Enquanto há um acesso ao Internet do servidor do CallManager da Cisco, este é o método preferido.

Note: À revelia, o internet explorer abre os links novos nos indicadores existentes. Consequentemente, você pode facilmente perder sua conferência via web quando você clica sobre um link. Para impedir este comportamento do internet Explorer, as **ferramentas** seletas **> as opções de internet > avançaram** e desmarcam **indicadores da reutilização para atalhos de lançamento**.

Abra a porta TCP 1627 a fim compartilhar do desktop. Se a porta TCP 1627 é obstruída pelo Firewall, as mensagens estão escavadas um túnel através da porta TCP 80. O MeetingPlace de Cisco igualmente apoia o Tunelamento usando HTTPS (SSL). O SSL exige um certificado SSL. Para permitir o apoio para o SSL, a porta 443 deve estar aberta na rede. Para obter informações sobre do aplicativo de conferência pela Web, refira a conferência na Web com o Cisco MeetingPlace.

Note: Quando você inicia uma sessão do serviço terminal ao servidor do CallManager da Cisco, lance um navegador de lá ao MeetingPlace de Cisco, compartilhe do desktop, e minimize então esta sessão do serviço terminal, a conferência via web com gelos do Suporte técnico. Cisco recomenda que você compartilha do desktop de seu PC local, fazer logon ao MeetingPlace de Cisco do console de servidor diretamente, ou não minimiza sua sessão do serviço terminal ao CallManager da Cisco.

Para a informação de produto adicional, refira o MeetingPlace de Cisco.

Se você precisa de estabelecer uma sessão com um engenheiro de suporte técnico, vá à página do MeetingPlace TAC.

Desta página, incorpore o número de ID exclusivo de reunião que o engenheiro de suporte técnico atribui para esta reunião. Se você é um usuário da primeira vez, selecione o link de teste do navegador para assegurar a compatibilidade. Se você já não os tem, a página do navegador do teste alerta-o instalar componentes de algumas Javas. Este é um processo de uma vez. Não se exige a próxima vez que você conecta a Cisco o MeetingPlace.

Uma vez que você assina dentro como um convidado, você pode compartilhar de todo o aplicativo com o engenheiro de suporte técnico e permitir o controle do coordenador.

Note: Quando você usa o MeetingPlace para conferência pela Web de Cisco, o processo do navegador de Internet usa uma parcela de recursos do CPU. Este é um comportamento esperado.

Fixe conexões de rede

Os clientes são responsáveis para a conectividade de rede segura para o acesso. As conexões do Cisco Virtual Private Network (VPN) são o método preferido.

Como usar um VPN

Um VPN é uma rede privada que use linhas de telefone público (ou em alguns casos um modem a cabo). A privacidade é mantida com a criptografia e o uso de protocolos seguros. Quando você usa um VPN para alcançar o CallManager da Cisco com um Firewall, você pode usar o CallManager da Cisco como se você era dentro da rede.

O VPN é exigido nestas circunstâncias:

- Quando você precisar o acesso ao Web site do CallManager da Cisco (servidor do CallManager name>/ccmadmin do <Cisco de http://) de um computador remoto fora de seu firewall de rede.

Note: Se você não usa o VPN para o Acesso remoto, refira a site do microsoft para obter informações sobre de configurar o modelo de objeto de componente distribuído (DCOM) com um Firewall.

Discuta estabelecido de um VPN com seu administrador de LAN.

Informações Relacionadas

- Suporte à Tecnologia de Voz
- Suporte de Produtos de Comunicação de Voz e de IP
- Troubleshooting da Telefonia IP Cisco
- Suporte Técnico - Cisco Systems