Guia de planejamento e requisitos do sistema do Cisco WebEx Meetings Server versão 2.8

Primeira publicação: 01 de Novembro de 2016

Última modificação: 14 de Abril de 2017

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

AS ESPECIFICAÇÕES E INFORMAÇÕES REFERENTES AOS PRODUTOS DESTE GUIA ESTÃO SUJEITAS A ALTERAÇÕES SEM AVISO PRÉVIO. TODAS AS DECLARAÇÕES, INFORMAÇÕES E RECOMENDAÇÕES DESTE GUIA SÃO PRECISAS, MAS SÃO APRESENTADAS SEM NENHUM TIPO DE GARANTIA EXPLÍCITA OU IMPLÍCITA. OS USUÁRIOS DEVEM ASSUMIR RESPONSABILIDADE TOTAL PELA APLICAÇÃO DE QUAISQUER PRODUTOS.

A LICENÇA DE SOFTWARE E A GARANTIA LIMITADA QUE ACOMPANHAM O PRODUTO SÃO ESTABELECIDAS NO PACOTE DE INFORMAÇÕES FORNECIDO COM O PRODUTO E SÃO INCORPORADAS NESTE DOCUMENTO POR ESTA REFERÊNCIA. SE NÃO FOR POSSÍVEL LOCALIZAR A LICENÇA DE SOFTWARE OU A GARANTIA LIMITADA, ENTRE EM CONTATO COM O REPRESENTANTE DA CISCO PARA OBTER UMA CÓPIA.

A implementação de compactação de cabeçalho TCP da Cisco é uma adaptação de um programa desenvolvido pela University of California, Berkeley (UCB) como parte da versão de domínio público da UCB do sistema operacional UNIX. Todos os direitos reservados. Copyright © 1981, Regents of the University of California.

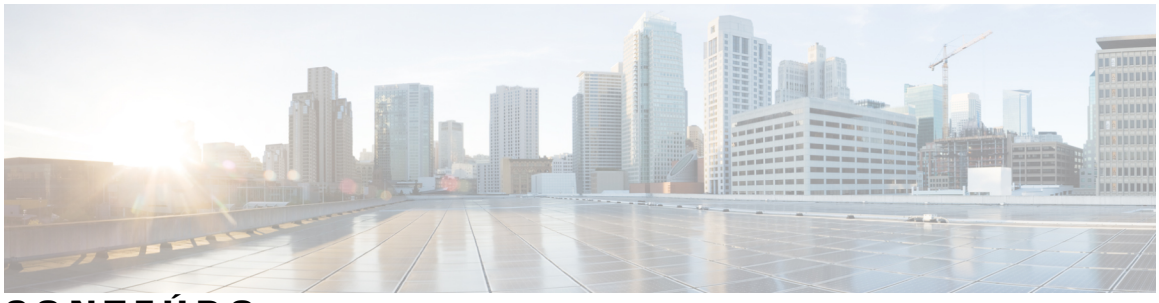
NÃO OBSTANTE QUALQUER OUTRA GARANTIA AQUI REFERIDA, TODOS OS ARQUIVOS DE DOCUMENTOS E SOFTWARE DESTES FORNECEDORES SÃO FORNECIDOS "COMO ESTÃO" COM TODAS AS FALHAS. A CISCO E OS FORNECEDORES MENCIONADOS ANTERIORMENTE ISENTAM-SE DE TODAS AS GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, MAS NÃO SE LIMITANDO A, GARANTIAS DE COMERCIALIZAÇÃO, ADEQUAÇÃO A UM PROPÓSITO ESPECÍFICO E NÃO VIOLAÇÃO OU RESULTANTE DE QUALQUER DISTRIBUIÇÃO, USO OU PRÁTICA COMERCIAL.

SOB NENHUMA CIRCUNSTÂNCIA A CISCO OU SEUS FORNECEDORES SERÃO RESPONSÁVEIS POR DANOS INDIRETOS, ESPECIAIS, CONSEQUENCIAIS OU INCIDENTAIS, INCLUINDO, MAS NÃO SE LIMITANDO A, PERDA DE LUCROS OU DANOS A DADOS RESULTANTES DO USO OU INCAPACIDADE DE USO DESTE GUIA, MESMO QUE A CISCO OU SEUS FORNECEDORES TENHAM ADVERTIDO SOBRE A POSSIBILIDADE DE TAIS DANOS.

Quaisquer números de telefone e endereços IP (Internet Protocol – Protocolo de Internet) usados neste documento não se destinam a ser endereços e números de telefone reais. Todos os exemplos, saída de exibição de comando, diagramas de topologia de rede e outras figuras incluídas no documento são mostrados apenas para fins ilustrativos. Qualquer uso de endereços IP ou números de telefone reais em conteúdo ilustrativo é não intencional e coincidente.

Cisco e o logotipo da Cisco são marcas comerciais ou registradas da Cisco Systems, Inc. e/ou de suas afiliadas nos Estados Unidos e em outros países. Para ver uma lista das marcas comerciais da Cisco, acesse a URL: http://www.cisco.com/go/trademarks. Todas as marcas de terceiros citadas pertencem a seus respectivos proprietários. O uso do termo "parceiro" não implica uma relação de sociedade entre a Cisco e qualquer outra empresa. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.



CONTEÚDO

Requisitos Gerais do sistema 1

- Práticas Recomendadas do Cisco WebEx Meetings Server 6
- Ferramentas de produtividade WebEx 8
- Usuários 8
- Tamanhos de implantação para seu sistema 8
- Requisitos para corresidência com vCenter 9
- Máquinas Virtuais em seu sistema 9
- Requisitos Mínimos de Hardware 10
  - Recursos consumidos pelo CWMS e o organizador ESXi 12
  - Sistema de 50 usuários 12
  - Sistema de 250 usuários 16
  - Sistema de 800 usuários 19
  - Sistema de 2000 usuários 22
- Capacidade do sistema matriz 27
- Caminhos de Atualização Suportados 31
- Caminhos de Atualização Suportados 33

Introdução do Cisco WebEx Meetings Server 37

- Informações para os clientes do Cisco Unified MeetingPlace 39
- Implantação de um centro de dados único 39
- Registrando centros de dados únicos para criar um sistema com (MDC) 39
- Usando O Vmware vSphere Com Seu Sistema 40
  - Vantagens de implantar um sistema no VMware vSphere 40
- Desempenho do Sistema IOPS e de Armazenamento 42
- Instalar o VMware vSphere ESXi e Configurar o Armazenamento 44
- Participar de Reuniões 45

Layout da Máquina Virtual em sua Rede 47

- Diferentes tipos de topologia de rede para seu sistema 48
- Topologia de rede do proxy reverso da internet (IRP) interna 48
- Topologia de Rede Sem Split-Horizon 49

Todas as Topologias de Rede Internas 50
Topologia de Rede Split-Horizon 51
Redundância nas implantações HA ou MDC 53
Considerações de Rede para o Proxy Reverso da Internet 54
Requisitos da Largura de Banda de Rede 56
Requisitos de rede para vários centros de dados 60
NIC Teaming para Agregação de Largura de Banda 61
Balanceamento de carga 62
Lista de verificação de rede para o sistema 63
O checklist da Rede para uma Instalação ou Expansão com uma Implantação Automática e Acesso Público 64
O checklist da rede para uma instalação ou expansão com uma implantação manual, acesso público e todas as máquinas virtuais internas 67
O checklist da rede para uma instalação ou expansão com uma implantação automática, acesso público e um DNS sem split-horizon 70
O checklist da rede para uma instalação ou expansão com uma implantação manual, acesso público e um DNS sem split horizon 72
O checklist da rede para uma instalação ou expansão com uma implantação automática, acesso público e um DNS split-horizon 75
O checklist da rede para uma instalação ou expansão com uma implantação manual, acesso público e um DNS split-horizon 78
O checklist da Rede para uma Instalação ou Expansão com Implementação Automática e Nenhum Acesso Público 81
Checklist de Rede Para uma Instalação ou Expansão Com Implementação Manual e Acesso Não Público 83
As URLs do Site WebEx e da Administração Webex 86
Porta de acesso quando todas as máquinas virtuais estão na rede interna 87
Porta de acesso com um proxy reverso da Internet na rede DMZ 88
Porta de Acesso no Firewall Externo 88
Porta de Acesso no Firewall Interno 89
Portas VMware vCenter 93
Portas do Cisco WebEx Meeting Center 94
Usar NAT com seu sistema 94
Projeções proxies 97
Configurar o Cisco Unified Communications Manager (CUCM) 99

CUCM em um ambiente MDC 100
Antes de Começar 100
Teleconferência segura CUCM em um ambiente MDC 101
Checklist da configuração CUCM do centro de multidados 101
Checklist da configuração CUCM com ou sem alta disponibilidade 102
Configurando CUCM em um sistema com CWMS 102
Configurando o CUCM em um sistema com de 250 ou 800 usuários 103
Configurando o CUCM em um sistema com para 2000 usuários 104
Configurar CUCM para sistemas de alta disponibilidade e sem alta disponibilidade 105
Configurando o CUCM nos sistemas de 50, 250 e 800 usuários sem alta disponibilidade 105
Configurando o CUCM nos sistemas de 50, 250 e 800 usuários com alta disponibilidade 106
Configurar o CUCM em um sistema de 2000 usuários sem alta disponibilidade 107
Configurando o CUCM em um sistema de 2000 usuários com alta disponibilidade 108
Configurar um perfil de segurança de tronco SIP 109
Configurar um Perfil de Segurança de Tronco SIP para um Ponto Balanceador de Carga 109
Configurar um Perfil de Segurança de Tronco SIP para um Ponto de Aplicativo 110
Configurar um perfil SIP 111
Configurar um perfil SIP padrão 111
Configurar um perfil TLS SIP 111
Configure um perfil SIP IPv6 112
Gerenciamento de certificados CUCM usando TLS 112
Carregue os certificados do Cisco WebEx Meetings Server 113
Instalando um Certificado CUCM de Terceiros 113
Baixar os certificados CUCM 114
Gerando uma Solicitação de Assinatura de Certificado (CSR) para a Versão 2.6 e superior 115
Gerando uma solicitação de assinatura de certificado (CSR) Versão 2.5 e inferior 116
Configurar um tronco SIP 118
Configurar um Tronco SIP em um Ponto Balanceador de Carga 119
Configurar um Tronco SIP para um Ponto de Aplicativo 120
Configurar um grupo de rota 121
Configurar uma lista de rota 122
Configurar um Padrão de Rota 123
Configurar um padrão de rota SIP 123
Compatibilidade de recursos e de suporte do CUCM 124
Compatibilidade de extremidade de áudio 126

Sobre os downloads de aplicativos 129

Fazer download de aplicativos no site da Administração 130

Conteúdo dos arquivos ZIP de aplicação 131

Chave do idioma de aplicação 131

Conteúdo do arquivo ZIP das ferramentas de produtividade 131

Conteúdo do arquivo ZIP do cliente WebEx Meetings 132

Conteúdo do arquivo ZIP do reprodutor de gravação de rede 133

Desenvolvimento em massa de Ferramentas de produtividade Cisco WebEx 134

Instalação silenciosa das Ferramentas de Produtividade utilizando a linha de comando 134

Remoção silenciosa das Ferramentas de Produtividade usando a interface da linha de comando 135

Limitações para a instalação silenciosa de aplicativos CWMS ao usar SMS 135

Anunciando as Ferramentas de Produtividade WebEx usando o programa automático por sistema de SMS 136

Remoção dos componentes das Ferramentas de produtividade usando o programa automático por sistema de SMS 137

Adicionando Ferramentas de Produtividade usando o programa automático por sistema de SMS 138

Desinstalando as Ferramentas de produtividade usando o programa de desinstalação por sistema de SMS 139

Publicidade do programa para atualizar para a nova versão das Ferramentas de produtividade WebEx 139

Criar um pacote a partir de uma definição 140

Implantação em massa do aplicativo de reuniões 141

Instalar o Cisco WebEx Meetings 141

Desinstalar Cisco WebEx Meetings Localmente 141

Instalação silenciosa do aplicativo Meetings usando a linha de comando 142

Remoção silenciosa do aplicativo Meetings usando a interface da linha de comando 143

Limitações para a instalação silenciosa de aplicativos CWMS ao usar SMS 143

Anúncio do CWMS usando o programa automático por sistema de SMS 143

Desinstalando o aplicativo Cisco WebEx Meetings usando o programa de desinstalação por sistema de SMS 145

Implantação em massa do reprodutor de gravações de rede 145

Instalar o reprodutor de gravações de rede 145

Instalação silenciosa do reprodutor de gravações usando a linha de comando 146

Desinstalação silenciosa do reprodutor de gravações usando a interface da linha de comando 146
Instalação de aplicativos CWMS usando o Microsoft Systems Management Server 2003 (SMS) 147
Limitações para a instalação silenciosa de aplicativos CWMS ao usar SMS 147
Anuncie o reprodutor de gravações de rede Cisco WebEx usando o programa automático por sistema de SMS 147
Desinstale o reprodutor de gravações de rede Cisco WebEx usando o programa de desinstalação automático por sistema de SMS 148
Reconfigurar suas configurações depois de realizar uma atualização 149
Visão geral do registro único 151
Benefícios de Registro Único 152
Visão geral da configuração SAML 2.0 de registro único 153
SAML de SSO para Início de Sessão da Administração e do Usuário Final 154
O registro único SAML 2.0 diferencia entre os serviços de reunião WebEx com base em nuvem e o WebEx Meetings Server 154
Atributos de declarações SAML 160
Atributos de declarações SAML suportados 160
Parâmetros Opcionais 164
Valores de fuso horário 165
Valores de código de país 168
Valores das Regiões 178
Valores dos Idiomas 179
Códigos de idiomas 179
Requisitos de armazenamento para gravações de reuniões 181
Requisitos de armazenamento para arquivos de backup do sistema 182
MIBs SNMP Suportados 183
Informações MIBS do sistema CWMS 183
MIBs relacionadas a CPU 184
Informações de memória do CWMS 187
Uso do Disco 187
Interceptações SNMP Suportadas 188
Notificação de Eventos 188
Dados de Interceptação 189
Requisitos do sistema PC comum 191

Requisitos do sistema operacional para Windows 192
Requisitos do sistema operacional para Mac 195
Requisitos dos sistemas operacionais para dispositivos móveis 196
Suporte à Citrix XenDesktop e XenApp 196
Matriz de Compatibilidade das Ferramentas de Produtividade e Aplicativos Cisco WebEx Meetings 197
Sobre as licenças do organizador 199
Integração do Cisco Unified Communications Manager (CUCM) 201
Integração do Session Manager Edition (SME) 201
Compatibilidade de extremidade de áudio 202

CAPÍTULO 1

Requisitos Gerais do sistema

O Cisco WebEx Meetings Server (CWMS) é compatível com os servidores Cisco UCS que atendem ou excedem as especificações apresentadas nesta seção.

Importante Quando você faz uma *atualização* para uma versão principal do CWMS, como a Versão 2.0 ou Versão 2.5 da Versão 1.x, os organizadores ESXi (servidor UCS da Cisco) onde a máquina virtual de Administração está localizada requerem um mínimo de 1,5 TB de espaço livre em disco. Consulte a seção neste documento que descreve os sistemas de usuários de tamanhos diferentes, que começa com o Sistema de 50 usuários, na página 12. Durante a atualização, haverá dois conjuntos de máquinas virtuais na sua rede ao mesmo tempo; as máquinas virtuais *originais* executando a Versão 1.x e as máquinas virtuais de *atualização* para suportar a nova versão. Para obter mais detalhes, consulte a seção "Atualizando o Sistema" no Guia de Administração do CWMS em http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

Módulo	Notas dos Requisitos
Servidor do organizador e processadores	• Servidor rack UCS da Cisco da *Série C* ou equivalente ao servidor blade da *Série B*. • Suporte de conjunto de instruções AES-NI. • Velocidade do clock do processador de 2.4 GHz ou mais rápido. **Observação** Hardware de terceiros não é compatível.

Módulo	Notas dos Requisitos
Interfaces de rede NICs entre os organizadores ESXi (para as máquinas virtuais do Cisco WebEx Meetings Server) e o comutador Ethernet (não para a interface de rede externa).	• Mínimo 1 NIC físico para uma configuração não redundante. Consulte a Sistema de 50 usuários, na página 12 seção para necessidades especiais, onde o proxy reverso da internet (IRP) e a máquina virtual de Administração compartilham um organizador. • As configurações redundantes devem ter todas as interfaces NIC duplicadas (*unidas* ou *ligadas*) e conectadas à matriz de comutação independente. • Um NIC adicional para a rede de gerenciamento VMware (opcional).
[1]Armazenamento interno (DAS) para organizadores ESXi onde as máquinas virtuais internas são implantadas	• Mínimo de 4 drives em uma configuração RAID 10 ou RAID 5 • Mínimo de 1,5 TB de armazenamento utilizável para novas atualizações ou implantações de sistema. • Quando você atualiza para o CWMS versão 2.X da versão 1.X, os organizadores ESXi requerem de 172 a 1118 GB de espaço livre em disco, dependendo do tamanho do seu sistema e das máquinas virtuais. Consulte a seção desde documento que descreve os sistemas de usuários de tamanhos diferentes, que começa com o Sistema de 50 usuários, na página 12. • Segunda matriz opcional para ESXi **Observação** As máquinas virtuais devem utilizar o thick provisioning para armazenamento.
Armazenamento interno (DAS) para organizadores ESXi onde as máquinas virtuais de IRP são implantadas	• Mínimo de 2 unidades em uma configuração RAID-1 • Mínimo de 300 GB de armazenamento utilizável • Pode usar as mesmas configurações que as máquinas virtuais internas **Observação** As máquinas virtuais devem utilizar o thick provisioning para armazenamento.

Módulo	Notas dos Requisitos
Armazenamento SAN	• Pode ser usado como um substituto para o DAS. (Recomendamos alocar a mesma quantidade de espaço de armazenamento.) • Os servidores blade série B possuem apenas duas unidades de disco rígido. Se você estiver usando servidores blade UCS da Cisco da série B e planeja atualizar para o CWMS Versão 2.x, você deve usar o armazenamento SAN para atender as 4 unidades de disco rígido em uma configuração RAID 5 ou RAID 10. • Recomendado apenas para implantações onde a equipe de suporte tem experiência no monitoramento e ajuste de desempenho SAN. **Observação** Você assume a responsabilidade por adicionar armazenamento adicional nas novas exigências do VMware e no crescimento futuro do sistema. • Apenas Fiber Channel (FC) ou Fiber Channel acima de Ethernet (FCoE) de 10 GB. • Os requisitos de desempenho são os mesmos como para a DAS. • A latência total máxima admissível, conforme medida pelo vSphere, é de 20 ms. Para obter mais informações, consulte a seção *Armazenamento* em http://docwiki.cisco.com/wiki/UC_Virtualization_Supported_Hardware#Storage. • Espaço total necessário para as máquinas virtuais: A soma dos recursos de armazenamento reservados para cada máquina virtual do sistema CWMS. **Observação** As máquinas virtuais devem utilizar o thick provisioning para armazenamento.

Módulo	Notas dos Requisitos
[2]Armazenamento NAS	• Pode ser usado como um substituto para o DAS ou SAN. (Recomendamos a alocação da mesma quantidade de espaço de armazenamento.) • Recomendamos o uso dos servidores de armazenamento NAS com os servidores rack da Série C UCS da Cisco. • Recomendado apenas para implantações onde a equipe de suporte tem experiência no monitoramento e ajuste de desempenho SAN. Você assume a responsabilidade por adicionar armazenamento adicional nas novas exigências do VMware e no crescimento futuro do sistema. • Apenas Fiber Channel (FC), Sistema de arquivos de rede (NFS) ou SCSI. Para obter mais informações, consulte http://docwiki.cisco.com/wiki/UC_Virtualization_Storage_System_Design_Requirements#General_Guidelines_for_SAN.2FNAS. • Os requisitos de desempenho são os mesmos como para a DAS. • A latência total máxima admissível, conforme medida pelo vSphere, é de 20 ms. Para obter mais informações, consulte http://docwiki.cisco.com/wiki/UC_Virtualization_Supported_Hardware#Storage. • Espaço total necessário para as máquinas virtuais: A soma dos recursos de armazenamento reservados para cada máquina virtual do sistema CWMS. • O servidor de arquivos deve suportar o vStorage APIs for Array Integration (VAAI) e usar o thick provisioning. **Observação** Embora o esquema de provisionamento padrão para o armazenamento NAS seja thin provisioning, as máquinas virtuais devem utilizar o thick provisioning para armazenamento. (O thin provisioning não é suportado.) Para habilitar o thick provisioning para implantação com armazenamento NAS, o plug-in fornecido pelo fornecedor de armazenamento para VAAI deve ser instalado em todos os servidores UCS usados na implantação do Cisco WebEx Meetings Server.

Módulo	Notas dos Requisitos
Hipervisor	As versões ESXi e as licenças vSphere estão descritas na seção Requisitos Mínimos de Hardware, na página 10. O VMware vSphere é necessário e é o único produto suportado; outros produtos hipervisores não são suportados. vCenter Server 5.0, 5.0 Update 1, 5.0 Update 2, 5.1, 5.1 Update 1, 5.5 e 6.0 (CWMS 2.6MR1 e superior) As licenças vSphere são descritas na seção Requisitos Mínimos de Hardware. Uma licença VMware por soquete de processador. Corresidência: • O vCenter pode ser corresidente com o CWMS, proporcionando os requisitos de memória e de processador que são adicionados aos requisitos do sistema. • As configurações corresidentes do vCenter são compatíveis apenas em sistemas de 50 e 250 de usuários. • A corresidência com os produtos Cisco Unified Communications no mesmo host ESXi físico não é compatível. • A corresidência com as máquinas virtuais sem CWMS no mesmo host ESXi físico não é compatível. Recursos avançados do VMware vSphere, como o Distributed Resource Scheduler (DRS), Clonagem, Tolerância de Falhas (FT) e vMotion ou Storage vMotion, enquanto o sistema está ligado, não são suportados.
Servidor de e-mail	• Nome de domínio totalmente qualificado (FQDN) do servidor de e-mail que o sistema usa para enviar e-mails. • Número de porta — o valor padrão do número de porta SMTP é 25 ou 465 (número de porta SMTP seguro). • Para usar um servidor de e-mail habilitado para TLS com certificados de terceiros, você deve importar os certificados para o sistema. Para obter mais informações consulte "Gerenciando Certificados" no guia de administração em http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

Módulo	Notas dos Requisitos
Licenças	Licenças MCD—Uma licença MCD é necessária para cada centro de dados em um sistema com vários centros de dados. Uma licença MCD não é exigida para um sistema com um único centro de dados. Licença de organizador — Cada usuário que deve organizar uma reunião precisa ter uma licença de Organizador para iniciar uma reunião Web WebEx, Áudio WebEx, discagem múltipla ou de conferência pessoal. Para obter mais informações sobre as licenças de organizador, consulte Sobre as licenças do organizador, na página 199.

1 Se a sua organização tem experiência no gerenciamento de uma rede de área de armazenamento (SAN), recomendamos a SAN sobre o armazenamento de conexão direta (DAS). As SANs podem ser mais confiáveis do que as matrizes de disco locais.

2 Certifique-se de que um sistema de arquivos de rede (NFS) tenha capacidade de armazenamento suficiente para armazenar backups automáticos regulares do seu banco de dados e gravações de reuniões. (CWMS suporta as versões NFS 2, 3 e 4.)

- Práticas Recomendadas do Cisco WebEx Meetings Server, página 6
- Ferramentas de produtividade WebEx, página 8
- Usuários, página 8
- Tamanhos de implantação para seu sistema, página 8
- Requisitos para coresidência com vCenter, página 9
- Máquinas Virtuais em seu sistema, página 9
- Requisitos Mínimos de Hardware, página 10
- Capacidade do sistema matriz, página 27
- Caminhos de Atualização Suportados, página 31
- Caminhos de Atualização Suportados, página 33

Práticas Recomendadas do Cisco WebEx Meetings Server

O seguinte é uma lista de práticas recomendadas que você deve consultar ao configurar e manter o sistema Cisco WebEx Meetings Server:

- Ligue os organizadores de máquinas virtuais usando uma fonte de alimentação ininterrupta (UPS) para minimizar as interrupções de energia. Repetidas falhas de energia podem danificar os sistemas do organizador e as máquinas virtuais.
- Sempre coloque seu sistema no modo de manutenção antes de desligar o sistema operacional de um convidado.
- Para eventos agendados e outras situações que exigem um desligamento do sistema, desligue suas máquinas virtuais desligando o sistema operacional do convidado.
- O sistema é projetado para reparar-se quando necessário e reiniciar pode interromper este processo. Nós não recomendamos que você reinicie o sistema para corrigi-lo. Se o seu sistema está em um estado

insalubre, entre em contato com o TAC da Cisco. Desligue o sistema apenas quando instruído a fazê-lo ou durante eventos agendados, como a manutenção do centro de dados.

- Configure a redundância de rede para minimizar falhas na rede. Consulte "Adicionar um Sistema de Alta Disponibilidade" no *Guia de Administração do Cisco WebEx Meetings Server* para obter mais informações.
- Utilizar fotos instantâneas nas suas máquinas virtuais pode prejudicar o desempenho do sistema de maneiras que afetam a experiência do usuário, mesmo quando o sistema for levemente carregado de outra forma.
- Se seu sistema estiver com problemas, certifique-se de verificar o ambiente VMware vCenter para determinar se a rede ou as condições no vCenter estão causando o problema.
- Configure a alta disponibilidade para aumentar a probabilidade de o sistema continuar a funcionar se uma falha ocorrer.
- Se você tem um sistema de alta disponibilidade e seu sistema secundário falhar, você pode repará-lo removendo o sistema secundário existente (consulte "Removendo um Sistema de Alta Disponibilidade" no *Guia de Administração do Cisco WebEx Meetings Server*) e adicionando um novo sistema secundário (consulte "Adicionando um Sistema de Alta Disponibilidade" no *Guia de Administração do Cisco WebEx Meetings Server*). Se o sistema primário em um sistema de alta disponibilidade falhar, você não pode repará-lo usando este procedimento. Recomendamos que você restaure o sistema primário usando o procedimento de recuperação de desastres e, em seguida, adicione um novo sistema secundário. Até que você adicione um novo sistema secundário, a implantação estará operando sem redundância total. Este procedimento ajuda a evitar interrupções não planejadas se qualquer uma das máquinas virtuais secundárias falhar. Consulte "Utilizar o Recurso de Recuperação de Desastres" no *Guia de Administração do Cisco WebEx Meetings Server* para obter mais informações.
- Uma vez que o sistema só mantém o backup mais recente do sistema no NFS e remove os anteriores a cada dia, recomendamos que você mantenha vários backups recentes em outras mídias.

Restrição Não crie manualmente os arquivos ou diretórios no compartilhamento NFS usado pelo Cisco WebEx Meetings Server, uma vez que ele executa vários scripts em arquivos e diretórios NFS. O servidor de armazenamento NFS deve ser de uso exclusivo do Cisco WebEx Meetings Server.

- Use seu painel para monitorar o estado de saúde do NFS, da CPU e do armazenamento. Recomendamos ativar os alarmes do painel para armazenamento e CPU.
- Se você planeja usar a integração de diretórios, consulte a seção Configurando a Integração de Diretórios no capítulo "Gerenciar Usuários" do *Guia de administração do Cisco WebEx Meetings Server* para mais informações.
- Ao usar o Cisco WebEx Meeting Server, o tronco SIP relacionado no CUCM na interface do serviço CallManager deve ter a caixa de seleção **Ponto de término de mídia necessário** desmarcada na página **Configuração do tronco**. Consulte Configurar um Tronco SIP em um Ponto Balanceador de Carga, na página 119 e Configurar um Tronco SIP para um Ponto de Aplicativo, na página 120 para obter mais detalhes.
- Se você estiver executando o Cisco WebEx Meetings Server versão 2.0 ou superior e usando os servidores blade da série B, será necessário usar o armazenamento SAN para cumprir os requisitos do disco rígido. Consulte Requisitos Gerais do sistema, na página 1 para obter mais informações sobre os requisitos SAN.

Ferramentas de produtividade WebEx

As Ferramentas de Produtividade WebEx permitem que os usuários iniciem, agendem ou participem de sessões WebEx Meetings a partir dos aplicativos, como o Microsoft® Outlook®. Os usuários podem encontrar mais informações sobre as Ferramentas de Produtividade Cisco WebEx em http://www.webex.com/support/productivity-tools.html.

O Cisco WebEx Meetings Server suporta a versão mais recente de aplicativos WebEx, disponíveis na página **Configurações** > **Downloads**. Se os usuários estiverem executando uma versão mais antiga das Ferramentas de Produtividade WebEx após você realizar uma atualização do sistema, eles poderão agendar, iniciar e participar de reuniões, mas os recursos mais recentes não estarão disponíveis. Recomendamos que você mova silenciosamente as últimas Ferramentas de Produtividade WebEx .msi para uma ótima experiência. Consulte Matriz de Compatibilidade das Ferramentas de Produtividade e Aplicativos Cisco WebEx Meetings, na página 197.)

Usuários

O sistema suporta um máximo de tempo de vida de 400.000 contas de usuário. Este número representa o total de contas de usuário ativa e desativada. Este número máximo de tempo de vida é grande o suficiente para acomodar o crescimento esperado no banco de dados do usuário.

Os administradores não podem excluir usuários do sistema. Em vez disso, os usuários são desativados. Este projeto permite que os administradores reativem contas de usuários anteriormente desativadas, mesmo após longos períodos de inatividade do usuário. As reuniões do usuário e outros conteúdos (incluindo gravações) são restaurados.

Tamanhos de implantação para seu sistema

Ao determinar o tamanho de seu sistema, considere quantos usuários você acredita que usarão o sistema a qualquer momento. Por exemplo, em um sistema de 50 usuários, o número máximo de usuários participando simultaneamente em reuniões é de 50. Se mais de 50 usuários tentarem participar de uma reunião, uma mensagem de erro é exibida a todos os usuários que tentarem participar de uma reunião depois que o número máximo de usuários tiver excedido, e o sistema impede que esses usuários participem da reunião.

- Sistema de 50 usuários, na página 12
- Sistema de 250 usuários, na página 16
- Sistema de 800 usuários, na página 19
- Sistema de 2000 usuários, na página 22

Aqui estão algumas questões à serem consideradas ao determinar o tamanho do seu sistema:

- Determine o maior número de usuários que você prevê que irão participar de uma reunião em algum momento dado, incluindo ocasiões raras ou incomuns.
- Você pode expandir o tamanho do sistema para um tamanho maior a qualquer momento, desde que seu hardware atenda ou exceda os requisitos mínimos para o sistema de tamanho maior; caso contrário, você deve comprar hardware adicional.

- Se você planeja adicionar Alta disponibilidade (HA) ou Vários centros de dados (MDC) ao seu sistema, inclua as máquinas virtuais adicionais necessárias para suportar o sistema HA ou MCD quando você adquirir seu hardware.
-

Requisitos para coresidência com vCenter

O VMware vCenter Server ou o vCenter Server Appliance podem residir com outras máquinas virtuais ou com as máquinas virtuais Cisco WebEx Meetings Server (CWMS) em alguns casos.

Em um sistema com 50 ou 250 usuários, o VMware vCenter pode residir no mesmo host com o CWMS. No entanto, RAM adicional deve ser solicitada ou instalada com o servidor UCS da Cisco. Para a quantidade exata de RAM necessária, consulte os requisitos para esse tamanho de sistema em Requisitos Mínimos de Hardware.

Máquinas Virtuais em seu sistema

Estas são as máquinas virtuais criadas para o seu sistema. Algumas funções são combinadas em uma máquina virtual para os tamanhos mais pequenos do sistema.

- Admin—*Nó central* do sistema. Inclui o banco de dados do sistema e fornece funções administrativas.
- Mídia: fornece serviços de mídia (funções de áudio e vídeo, telefonia e serviços de reuniões).

  Incluído na Máquina virtual de administração, em um sistema com 50 usuários simultâneos.
- Web—Oferece serviços web (lista de reuniões e gravações). Permite o usuário agendar reuniões futuras.

  Incluídas na Máquina virtual de administração, em um sistema com 50, 250 ou 800 usuários simultâneos.

  Os usuários finais iniciam sessão no site WebEx. Os administradores iniciam sessão no site da Administração.
- Proxy Reverso da Internet (IRP)—Fornece acesso público, habilitando os usuários a organizar ou participar de reuniões da Internet e por meio de dispositivos móveis. O proxy reverso da Internet é necessário para que a sua mão de obra móvel participe de reuniões.

Observação Apenas o IRP fornecido com este produto pode ser usado neste sistema. Os proxies reversos da Internet ou os balanceadores de carga da web, fornecidos por outros fornecedores, não são compatíveis. O IRP fornecido com este produto é otimizado para lidar com o tráfego web em tempo real, áudio e compartilhamento de dados de usuários externos que entram em reuniões da Internet.

Observação Nesta documentação, usamos o termo *máquinas virtuais internas* para se referir à máquina virtual de administração, e se for o caso, às máquinas virtuais de mídia e web.

O IRP situa-se na rede DMZ (topologias de rede split-horizon e sem split-horizon) ou na rede interna (todas as topologias de rede interna).

- Topologia de Rede Sem Split-Horizon, na página 49
- Topologia de Rede Split-Horizon, na página 51
- Topologia de rede do proxy reverso da internet (IRP) interna, na página 48

Requisitos Mínimos de Hardware

Esta seção lista alguns dos servidores UCS da Cisco que você pode utilizar para cada tamanho de sistema. Para os requisitos específicos de cada sistema, consulte:

- Sistema de 50 usuários
- Sistema de 250 usuários
- Sistema de 800 usuários
- Sistema de 2000 usuários

Também consulte o "Guia de Solicitações do Cisco WebEx Meetings Server" em http://www.cisco.com/c/en/us/products/conferencing/webex-meetings-server/sales-resources-listing.html.

Tabela 1: Versão ESXi e tipos de licenças

Tamanho do sistema	Versão ESXi	Tipo de licença vSphere
50 ou 250	5.0, 5.0 Update 1, 5.1, 5.5 ou 6.0	Edição Standard , Edição Enterprise, Edição Enterprise Plus
800 ou 2000	5.0 ou 5.0 Update 1	Somente a Edição Enterprise Plus
	5.1 a 5.5[3]	Enterprise Edition, Enterprise Plus Edition
	5.5 ou superior[1]	Edição Standard , Edição Enterprise, Edição Enterprise Plus
	6.0	Edição Standard , Edição Enterprise, Edição Enterprise Plus

[3] "Ou superior" faz referência à atualizações, não versões completas. Por exemplo, 5.5 Update 1 ou 5.1 Update 2.

Tabela 2: Modelos de organizador

Tamanho da Implantação	Exemplo de modelo UCS
50 Usuários	• UCS C220 M3 • UCS B200 M3 • UCS C220 M4S • C240 M4S2
250 usuários	• UCS C220 M3 • UCS B200 M3 • UCS C220 M4S • C240 M4S2
800 Usuários	• UCS C460 M2 • UCS B440 M2 • UCS B420 M3 (2.0 e superior)
2000 usuários	• UCS C460 M2 • UCS B440 M2 • UCS B420 M3 (2.0 e superior)

A co-residência com o vCenter é suportada com implantações de sistemas de 50 e 250 usuários somente. A coresidência com produtos Cisco Unified Communications no mesmo organizador físico não é suportada.

É possível utilizar modelos mais antigos do hardware UCS com o seu sistema, mas para uma melhor experiência do usuário, utilize o hardware listado na tabela. Por exemplo, você pode utilizar o UCS C220 M3 em um sistema de 250 usuários se você já tiver o hardware disponível.

Ao atualizar para o Cisco WebEx Meetings Server versão 2.0 ou superior, é possível usar os servidores blade B200 M3 UCS da Cisco com discos rígidos locais 2x, desde que o sistema atualizado use o armazenamento SAN para suas máquinas virtuais. Usar o armazenamento SAN com os servidores blade série B permite que o sistema atenda as 4 unidades de disco rígido em um requisito de configuração RAID 5 ou RAID 10 do Cisco WebEx Meetings Server.

Observação Para sistemas de 800 e 2000 usuários executando 2.0 e superior, não recomendamos implantar máquinas virtuais adicionais em um host DMZ. Isto pode resultar num aumento de perda de pacotes e latência notável nos conectores de mídia.

Recursos consumidos pelo CWMS e o organizador ESXi

O Cisco WebEx Meetings Server é implantado em uma ou mais máquinas virtuais em organizadores ESXi. Os recursos de memória e CPU e o espaço de armazenamento são consumidos pelo Cisco WebEx Meetings Server (CWMS) e pelo ESXi (Componente VMware que permite a virtualização no servidor físico UCS da Cisco). Dependendo do tamanho do sistema, o vCenter e várias máquinas virtuais podem funcionar no mesmo servidor UCS da Cisco.

O CWMS usa a *reserva de recursos* em suas máquinas virtuais para garantir a escalabilidade do sistema. Outras cargas de trabalho do VMware não tiram a CPU e outros recursos fora das máquinas virtuais. Os requisitos mínimos para cada tamanho de sistema inclui recursos suficientes para suportar:

- Qualidade contínua de serviço do CWMS no pico de uso do sistema (capacidade máxima).
- VMware ESXi.
- VMware vCenter (quando co-residente).

  Para os requisitos do vCenter Server, consulte Base de Conhecimento e procure por "Melhores práticas para instalar o vCenter Server 5.0" ou "Melhores práticas para instalar o vCenter Server 5.1" ou "Melhores práticas para instalar o vCenter Server 5.5", respectivamente.
- Fotos instantâneas VMware da máquina virtual (exclua estas o mais breve possível, caso contrário, você pode experimentar grave degradação de desempenho).

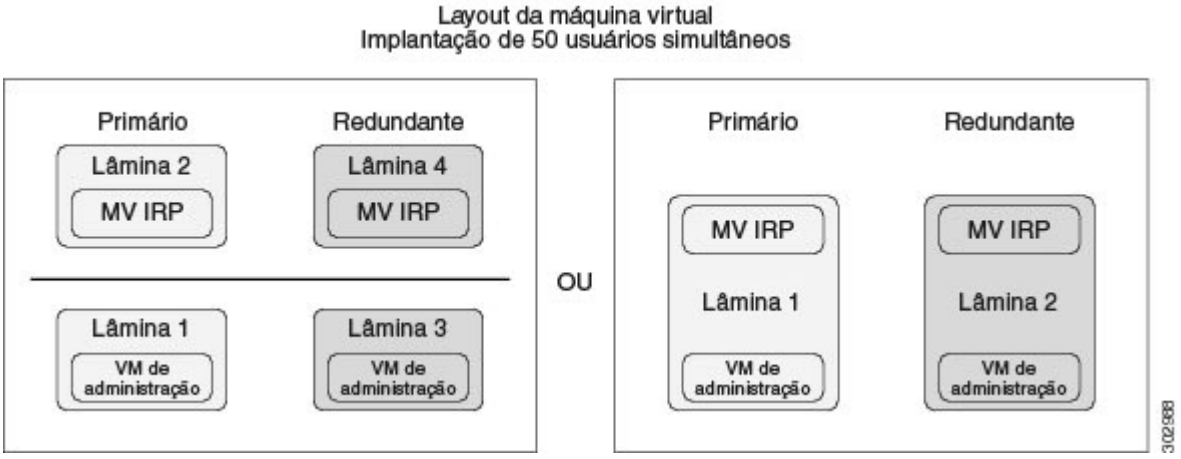
  Espaço extra de disco é necessário para as fotos instantâneas, uma vez que algumas fotos instantâneas podem ser tão grandes como a máquina virtual original. Em alguns casos, o vSphere pode excluir as fotos instantâneas para criar espaço de armazenamento, comprometendo a capacidade de reverter para as fotos instantâneas anteriores.
- Utilização do Servidor UCS da Cisco ao longo do ciclo de vida normal do servidor.

Os requisitos de hardware especificados no arquivo OVA são os requisitos mínimos que são necessários para implantar o Cisco WebEx Meetings Server. Estes requisitos *não incluem* qualquer CPU, memória ou requisitos de armazenamento do VMware vCenter ou do ESXi.

Cuidado A co-residência, outra além das configurações listadas nas tabelas neste documento, não é suportada. Se você ignorar os requisitos do nosso sistema, as máquinas virtuais talvez não consigam inicializar. A implantação das máquinas virtuais pode parar a partir das primeiras telas do produto durante a implantação do OVA vCenter.

Sistema de 50 usuários

Um sistema de 50 usuários também é descrito como um *micro* sistema. (Múltiplos Centro Dados (MCD) não está disponível para micro sistemas.) O diagrama ilustra duas versões de uma implantação de 50 usuários. (As máquinas virtuais "Redundantes" demonstram suporte para a Alta Disponibilidade (HA).)



A tabela lista os requisitos mínimos de hardware para os organizadores ESXi (servidores UCS da Cisco) no seu sistema. As duas últimas colunas mostram a quantidade de espaço em disco necessária para as novas instalações do Cisco WebEx Meeting Server e o espaço livre em disco necessário quando você usa a Atualização automática para atualizar o Cisco WebEx Meeting Server versão 1.5MR3 para a versão 2.X usando os servidores existentes UCS da Cisco. Para obter mais informações, consulte Requisitos Gerais do sistema.

Para obter informações sobre os requisitos de largura de banda, consulte Requisitos da Largura de Banda de Rede, na página 56.

Observação Para obter informações, consulte .Vantagens de implantar um sistema no VMware vSphere, na página 40

A co-residência com o vCenter é compatível com uma implantação de sistema de 50 usuários como configurada na tabela a seguir.

Máquinas Virtuais no organizador ESXi (Servidor UCS da Cisco)	Núcleo do processador	Memória (GB)	Portas Ethernet	Requisitos de Armazenamento em Disco Rígido para Novas Instalações	Espaço livre para armazenamento em disco rígido requerido para atualizar automaticamente da 1.5MR3 para a 2.X[4]
Admin	4 (ESXi 5.0) 6 (ESXi 5.1 e acima)	24	2 para a máquina virtual de administração, incluindo 1 se o NIC teaming for usado para redundância 1 recomendado para o gerenciamento de rede ESXi	1,5 TB, mínimo de 7.200 RPM	1118 GB para uma instalação automática.

Máquinas Virtuais no organizador ESXi (Servidor UCS da Cisco)	Núcleo do processador	Memória (GB)	Portas Ethernet	Requisitos de Armazenamento em Disco Rígido para Novas Instalações	Espaço livre para armazenamento em disco rígido requerido para atualizar automaticamente da 1.5MR3 para a 2.X[4]
Admin e vCenter (corresidentes)	6 (ESXi 5.0) 8 (ESXi 5.1 e acima)	36	2 para a máquina virtual de administração, incluindo 1 se o NIC teaming for usado para redundância 1 para o vCenter 1 recomendado para o gerenciamento de rede ESXi	1,5 TB, mínimo de 7.200 RPM	1078 GB Este quadro está baseado no pressuposto de que você tenha configurado vCenter com 40 GB.
Proxy reverso de Internet (IRP)	4 (ESXi 5.0) 6 (ESXi 5.1 e acima)	12	2 para a máquina virtual de IRP, incluindo 1 se o NIC teaming for usado para redundância 1 recomendado para o gerenciamento de rede ESXi	300 GB; mínimo de 7.200 RPM	172 GB
Admin e IRP (corresidentes)	8	36	2 para a máquina virtual de administração, incluindo 1 se o NIC teaming for usado para redundância 2 para a máquina virtual de IRP, incluindo 1 se o NIC teaming for usado para redundância 1 recomendado para o gerenciamento de rede ESXi	1,5 TB, mínimo de 7.200 RPM	990 GB

Máquinas Virtuais no organizador ESXi (Servidor UCS da Cisco)	Núcleo do processador	Memória (GB)	Portas Ethernet	Requisitos de Armazenamento em Disco Rígido para Novas Instalações	Espaço livre para armazenamento em disco rígido requerido para atualizar automaticamente da 1.5MR3 para a 2.X[4]
Admin e IRP e vCenter (todos corresidentes)	12	40	2 para a máquina virtual de administração, incluindo 1 se o NIC teaming for usado para redundância 2 para a máquina virtual de IRP, incluindo 1 se o NIC teaming for usado para redundância 1 para o vCenter 1 recomendado para o gerenciamento de rede ESXi	1,5 TB, mínimo de 7.200 RPM	950 GB Este quadro está baseado no pressuposto de que você tenha configurado vCenter com 40 GB.

4 Se você escolher Atualização Manual, onde você implanta manualmente todas as máquinas virtuais, e você estiver utilizando o mesmo hardware, você é obrigado a ter o dobro do espaço livre como é necessário para a atualização automática.

Observação Se você pretende utilizar um sistema de Alta Disponibilidade (HA), duplique os requisitos de hardware e a quantidade do sistema primário para suportar ambos os sistemas.

Recursos Reservados pelas Máquinas Virtuais em um Sistema de 50 Usuários

Esta seção ilustra quanta mídia as máquinas virtuais usam e é dirigida para aqueles com conhecimento avançado em VMware. Os recursos da CPU são especificados como vCPUs (núcleos) e MHz (ciclos de CPU). O VMware VMkernel utiliza ciclos MHz para controlar o agendamento da CPU.

Os recursos de memória são especificados pelo máximo de memória e pela memória reservada. A memória reservada não é compartilhada com outras máquinas virtuais no mesmo servidor físico UCS da Cisco.

Os recursos de disco (armazenamento) são controlados em duas áreas distintas. Durante a compilação OVA, os tamanhos das partições do sistema de arquivos do CentOS determinam o tamanho mínimo do disco. Em segundo lugar, o vCenter controla o máximo de espaço em disco disponível.

Se você tentar implantar uma máquina virtual sem o número mínimo de vCPUs, a implantação OVA da máquina virtual irá falhar. Se você tentar implantar uma máquina virtual sem a velocidade mínima total do processador MHz, a máquina virtual não ligará.

Importante Os números nesta tabela não incluem os recursos para o VMware ESXi e vCenter. Consulte Recursos consumidos pelo CWMS e o organizador ESXi, na página 12.

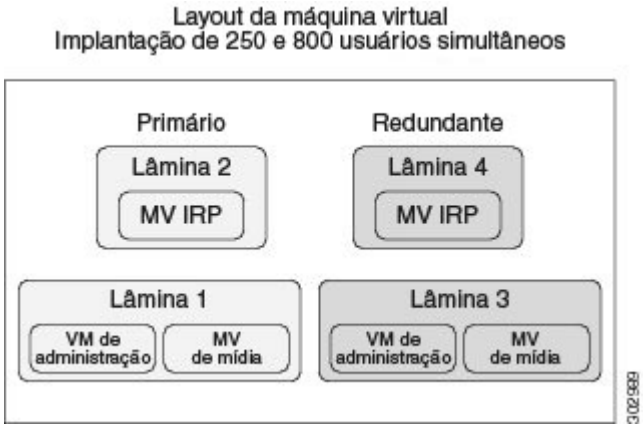
Tipo de Máquina Virtual	CPU Virtual (vCPU)	CPU[5] (MHz)	Memória Reservada/Memória Total[6] (GB)	Discos (GB)
Admin	4	8000	12/14	418
Proxy Reverso da Internet	4	8000	4/4	128

5 Número obtido pela multiplicação do número de CPUs físicas com a velocidade do chip da CPU (MHz). O hyperthreading não está incluído neste cálculo. (A CPU física deve ter uma velocidade de clock de 2.4 GHz ou mais rápido).

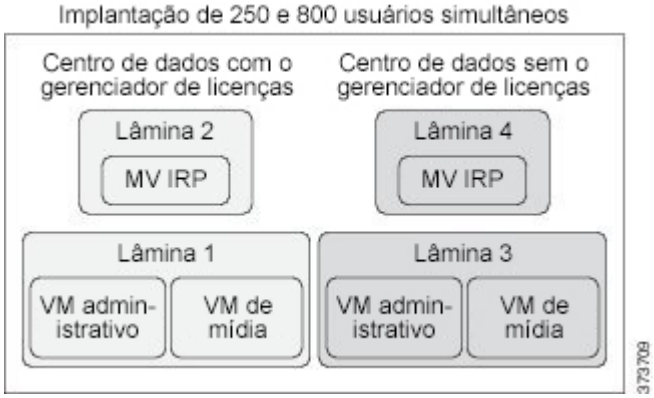
6 As máquinas virtuais com funcionalidade de mídia têm memória adicional, não reservada; Memória = Reservada/Total

Sistema de 250 usuários

Um sistema de 250 usuários também é descrito como um sistema *pequeno*. O diagrama ilustra duas versões de uma implantação de 250 usuários. As máquinas virtuais "Redundantes" demonstram suporte para a Alta Disponibilidade (HA). Se o sistema não inclui suporte HA, então somente implemente o sistema **Primário**.



Este diagrama mostra o layout de um sistema de 250 usuários com dois centros de dados que formam um sistema com (MDC) com suporte de Proxy Reverso da Internet (IRP). O Gerenciador de Licenças é executado em apenas um centro de dados.



A tabela lista os requisitos mínimos de hardware para os organizadores ESXi (servidores UCS da Cisco) no seu sistema. As duas últimas colunas mostram a quantidade de espaço em disco necessária para as novas instalações do Cisco WebEx Meeting Server e o espaço livre em disco necessário quando você usa a Atualização automática para atualizar o Cisco WebEx Meeting Server versão 1.5MR3 para a versão 2.X usando os servidores existentes UCS da Cisco. Para obter mais informações, consulte Requisitos Gerais do sistema.

Para obter informações sobre os requisitos de largura de banda, consulte Requisitos da Largura de Banda de Rede, na página 56.

Para obter informações, consulte .Vantagens de implantar um sistema no VMware vSphere, na página 40

A co-residência com o vCenter é compatível com uma implantação de sistema de 250 usuários como configurada na tabela a seguir.

Máquinas Virtuais no organizador ESXi (Servidor UCS da Cisco)	Núcleo do processador	Memória (GB)	Portas Ethernet	Requisitos de Armazenamento em Disco Rígido para Novas Instalações	Espaço livre para armazenamento em disco rígido requerido para atualizar automaticamente da 1.5MR3 para a 2.X[7]
Administração e mídia	12	52	• 2 para Mídia e Administração, incluindo 1 se o NIC teaming for usado para redundância • 1 recomendado para o gerenciamento de rede ESXi	1,5 TB, mínimo de 7.200 RPM	990 GB

Máquinas Virtuais no organizador ESXi (Servidor UCS da Cisco)	Núcleo do processador	Memória (GB)	Portas Ethernet	Requisitos de Armazenamento em Disco Rígido para Novas Instalações	Espaço livre para armazenamento em disco rígido requerido para atualizar automaticamente da 1.5MR3 para a 2.X[7]
(Admin e mídia) e vCenter (corresidentes)	16	56	• 2 para Mídia e Administração, incluindo 1 se o NIC teaming for usado para redundância • 1 recomendado para o gerenciamento de rede ESXi • 1 para o vCenter	1,5 TB, mínimo de 7.200 RPM	950 GB (Esta figura está baseada no pressuposto de que você configurou o vCenter com 40 GB.)
Proxy reverso de Internet (IRP)	12	36	• 2 para IRP, incluindo 1 se o NIC teaming for usado para redundância • 1 recomendado para o gerenciamento de rede ESXi	300 GB; mínimo de 7.200 RPM	172 GB

7 Se você escolher Atualização Manual, onde você implanta manualmente todas as máquinas virtuais, e você estiver utilizando o mesmo hardware, você é obrigado a ter o dobro do espaço livre como é necessário para a atualização automática.

Observação Se você pretende utilizar um sistema de HA, adquira o mesmo hardware e quantidades do sistema HA como você fez com o sistema primário.

Recursos Reservados pelas Máquinas Virtuais em um Sistema de 250 Usuários

Esta seção ilustra quanta mídia as máquinas virtuais usam e é dirigida para aqueles com conhecimento avançado em VMware. Os recursos da CPU são especificados como vCPUs (núcleos) e MHz (ciclos de CPU). O VMware VMkernel utiliza ciclos MHz para controlar o agendamento da CPU.

Os recursos de memória são especificados pelo máximo de memória e pela memória reservada. A memória reservada não é compartilhada com outras máquinas virtuais no mesmo servidor físico UCS da Cisco.

Os recursos de disco (armazenamento) são controlados em duas áreas distintas. Durante a compilação OVA, os tamanhos das partições do sistema de arquivos do CentOS determinam o tamanho mínimo do disco. Em segundo lugar, o vCenter controla o máximo de espaço em disco disponível.

Se você tentar implantar uma máquina virtual sem o número mínimo de vCPUs, a implantação OVA da máquina virtual irá falhar. Se você tentar implantar uma máquina virtual sem a velocidade mínima total do processador MHz, a máquina virtual não ligará.

Importante Os números nesta tabela não incluem os recursos para o VMware ESXi e vCenter. Consulte Recursos consumidos pelo CWMS e o organizador ESXi.

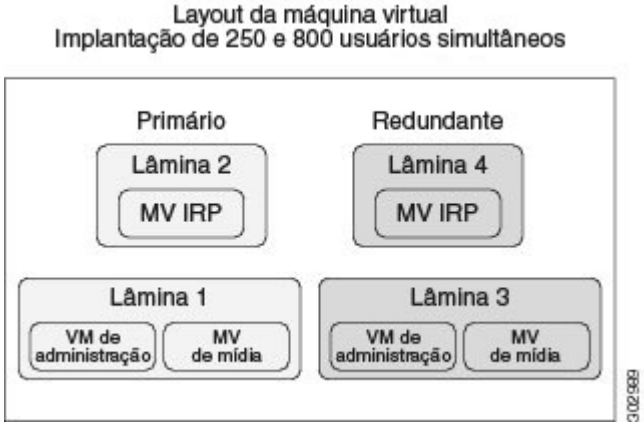
Tipo de Máquina Virtual	CPU Virtual (vCPU)	CPU[8] (MHz)	Memória Reservada/Memória Total[9] (GB)	Discos (GB)
Admin	4	8000	16/16	418
Mídia	8	16.480	13/23	128
Proxy Reverso da Internet	8	16.480	6/6	128

8 Número obtido pela multiplicação do número de CPUs físicas com a velocidade do chip da CPU (MHz). O hyperthreading não está incluído neste cálculo. (A CPU física deve ter uma velocidade de clock de 2.4 GHz ou mais rápido).

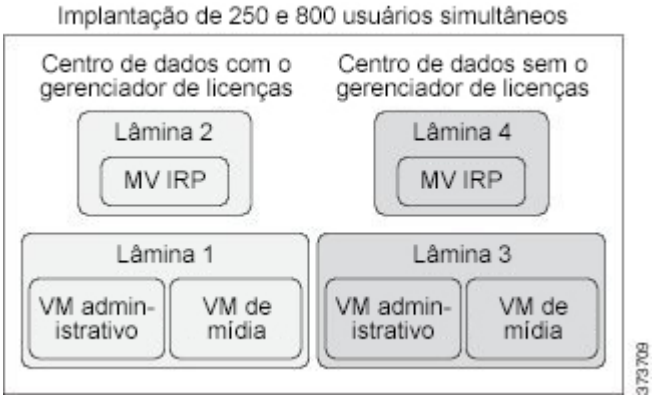
9 As máquinas virtuais com funcionalidade de mídia têm memória adicional, não reservada; Memória = Reservada/Total

Sistema de 800 usuários

Um sistema de 800 usuários também é descrito como um sistema *médio*. Este diagrama ilustra duas versões de uma implantação de 800 usuários. As máquinas virtuais "Redundantes" demonstram suporte para a Alta Disponibilidade (HA).



Este diagrama mostra o layout de um sistema de 800 usuários com dois centros de dados que formam um sistema com (MDC) com suporte de Proxy Reverso da Internet (IRP). O Gerenciador de Licenças é executado em apenas um centro de dados.



A tabela lista os requisitos mínimos de hardware para os organizadores ESXi (servidores UCS da Cisco) no seu sistema. As duas últimas colunas mostram a quantidade de espaço em disco necessária para as novas instalações do Cisco WebEx Meeting Server e o espaço livre em disco necessário quando você usa a Atualização automática para atualizar o Cisco WebEx Meeting Server versão 1.5MR3 para a versão 2.X usando os servidores existentes UCS da Cisco. Para obter mais informações, consulte Requisitos Gerais do sistema.

Para obter informações sobre os requisitos de largura de banda, consulte Requisitos da Largura de Banda de Rede, na página 56.

Observação A co-residência com o vCenter não é compatível com uma implantação de sistema de 800 usuários.

Para obter informações, consulte .Vantagens de implantar um sistema no VMware vSphere, na página 40

Máquinas Virtuais no organizador ESXi (Servidor UCS da Cisco)	Núcleo do processador	Memória (GB)	Portas Ethernet	Requisitos de Armazenamento em Disco Rígido para Novas Instalações	Espaço livre para armazenamento em disco rígido requerido para atualizar automaticamente da 1.5MR3 para a 2.X[10]
Administração e mídia (combinado)	40	80	• 2 para Mídia e Administração, incluindo 1 se o NIC teaming for usado para redundância • 1 recomendado para o gerenciamento de rede ESXi	1,5 TB; mínimo de 10.000 RPM	990 GB

Máquinas Virtuais no organizador ESXi (Servidor UCS da Cisco)	Núcleo do processador	Memória (GB)	Portas Ethernet	Requisitos de Armazenamento em Disco Rígido para Novas Instalações	Espaço livre para armazenamento em disco rígido requerido para atualizar automaticamente da 1.5MR3 para a 2.X[10]
Proxy reverso de Internet (IRP)	40	36	• 2 para IRP, incluindo 1 se o NIC teaming for usado para redundância • 1 recomendado para o gerenciamento de rede ESXi	300 GB; mínimo de 7.200 RPM	172 GB

10 Se você escolher Atualização Manual, onde você implanta manualmente todas as máquinas virtuais, e você estiver utilizando o mesmo hardware, você é obrigado a ter o dobro do espaço livre como é necessário para a atualização automática.

Observação Se você pretende usar um sistema de HA, compre os mesmos requisitos e quantidades de hardware como o sistema primário.

Para sistemas com 800 usuários, não recomendamos implantar máquinas virtuais adicionais em um organizador DMZ. Isto pode resultar num aumento de perda de pacotes e latência notável nos conectores de mídia.

Recursos reservados pelas máquinas virtuais em um sistema de 800 usuários

Esta seção ilustra quanta mídia as máquinas virtuais usam e é dirigido para aqueles com conhecimento avançado em VMware. Os recursos da CPU são especificados como vCPUs (núcleos) e MHz (ciclos de CPU). O VMware VMkernel utiliza ciclos MHz para controlar o agendamento da CPU.

Os recursos de memória são especificados pelo máximo de memória e pela memória reservada. A memória reservada não é compartilhada com outras máquinas virtuais no mesmo servidor físico UCS da Cisco.

Os recursos de disco (armazenamento) são controlados em duas áreas distintas. Durante a compilação OVA, os tamanhos das partições do sistema de arquivos do CentOS determinam o tamanho mínimo do disco. Em segundo lugar, o vCenter controla o máximo de espaço em disco disponível.

Se você tentar implantar uma máquina virtual sem o número mínimo de vCPUs, a implantação OVA da máquina virtual irá falhar. Se você tentar implantar uma máquina virtual sem a velocidade mínima total do processador MHz, a máquina virtual não ligará.

Importante Os números nesta tabela não incluem recursos para o VMware ESXi. Consulte Recursos consumidos pelo CWMS e o organizador ESXi, na página 12.

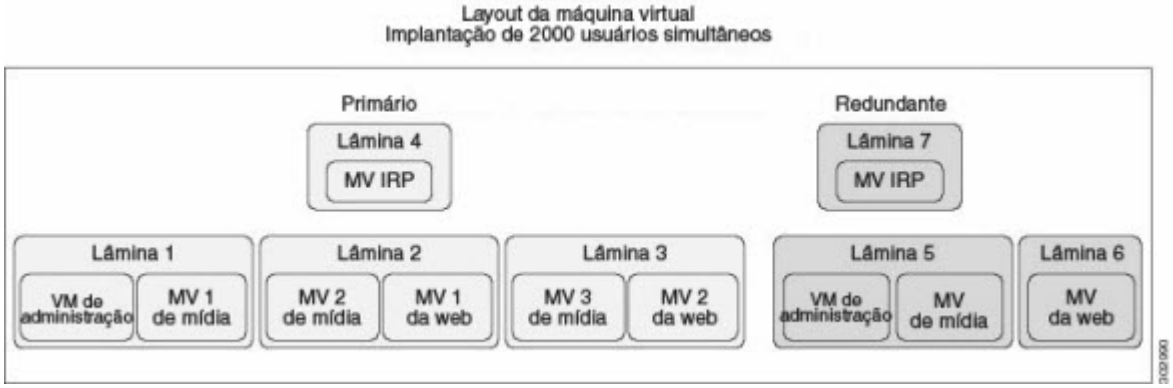
Tipo de Máquina Virtual	CPU Virtual (vCPU)	CPU[11] (MHz)	Memória Reservada/Memória Total[12] (GB)	Discos (GB)
Admin	10	20.600	16/16	418
Mídia	30	60.800	14/44	128
Proxy Reverso da Internet	20	41.200	10/10	128

11 Número obtido pela multiplicação do número de CPUs físicas com a velocidade do chip da CPU (MHz). O hyperthreading não está incluído neste cálculo. (A CPU física deve ter uma velocidade de clock de 2.4 GHz ou mais rápido).

12 As máquinas virtuais com funcionalidade de mídia têm memória adicional, não reservada; Memória = Reservada/Total

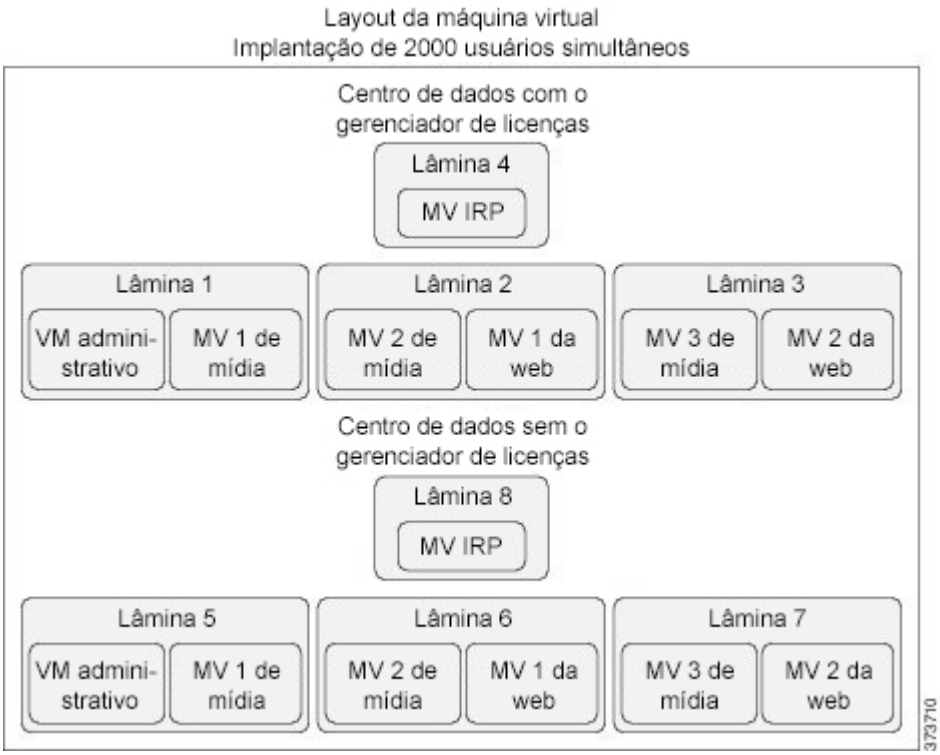
Sistema de 2000 usuários

Um sistema de 2000 usuários também é descrito como um sistema *grande*. Este diagrama mostra um sistema de 2000 usuários com Alta Disponibilidade (HA) e suporte de Proxy Reverso da Internet (IRP). As máquinas virtuais HA são mostradas como as máquinas virtuais **Redundantes**. Se o sistema não inclui suporte HA, então somente implemente o sistema **Primário**.



Este diagrama mostra uma implementação de 2000 usuários com dois centros de dados que formam um sistema de Múltiplos Centros de Dados (MDC) com suporte do Proxy Reverso da Internet (IRP). O Gerenciador de

Licenças é executado em apenas um centro de dados.



Importante Recomendamos que você implemente todas as máquinas virtuais mostradas no diagrama. Ao implantar diferentes tipos de máquinas virtuais em um servidor físico, você pode evitar melhor um desligamento do sistema em caso de falha de hardware. Por exemplo, colocar uma mídia e uma máquina virtual da web em um único servidor físico é mais resistente do que se você colocar duas máquinas virtuais da Web no mesmo servidor físico.

Em um grande sistema, há uma exclusão da regra de balanceamento de carga igual (consulte Balanceamento de carga, na página 62 para obter mais informações), onde há balanceadores de carga de tronco SIP na Mídia 1 e Mídia 2, e onde Mídia 3 e opcionalmente Mídia HA não têm balanceamento de carga. Se houver uma falha de ambas as Mídias 1 e 2 no sistema primário, todo o serviço de telefonia no CWMS será perdido. Se o sistema é uma implementação HA, a redundância atenua a falha de uma única máquina virtual.

A tabela lista os requisitos mínimos de hardware para os organizadores ESXi (servidores UCS da Cisco) no seu sistema. As duas últimas colunas mostram a quantidade de espaço em disco necessária para as novas instalações do Cisco WebEx Meeting Server e o espaço livre em disco necessário quando você usa a Atualização automática para atualizar o Cisco WebEx Meeting Server versão 1.5MR3 para a versão 2.X usando os servidores existentes UCS da Cisco. Para obter mais informações, consulte Requisitos Gerais do sistema.

Para obter informações sobre os requisitos de largura de banda, consulte Requisitos da Largura de Banda de Rede, na página 56.

Se você planeja adicionar um sistema de HA, as máquinas virtuais são exibidas como as máquinas virtuais "redundantes". Se você não quer HA, apenas implante o sistema primário.

Observação A co-residência com o vCenter não é compatível com uma implantação de sistema de 2000 usuários.

Observação Para obter informações, consulte .Vantagens de implantar um sistema no VMware vSphere, na página 40

Máquinas Virtuais no organizador ESXi (Servidor UCS da Cisco)	Núcleo do processador	Memória (GB)	Portas Ethernet	Requisitos de Armazenamento em Disco Rígido para Novas Instalações	Espaço livre para armazenamento em disco rígido requerido para atualizar automaticamente da 1.5MR3 para a 2.X[13]
Mídia1 e administração (combinado)	40	80	• 2 para Mídia1 e Administração, incluindo 1 se o NIC teaming for usado para redundância • 1 recomendado para o gerenciamento de rede ESXi	1,5 TB; mínimo de 10.000 RPM	990 GB
Mídia2 e web1 (combinado)	40	80	• 2 para Mídia2 e Web1, incluindo 1 se o NIC teaming for usado para redundância • 1 recomendado para o gerenciamento de rede ESXi	1 TB; mínimo de 10.000 RPM	768 GB

Máquinas Virtuais no organizador ESXi (Servidor UCS da Cisco)	Núcleo do processador	Memória (GB)	Portas Ethernet	Requisitos de Armazenamento em Disco Rígido para Novas Instalações	Espaço livre para armazenamento em disco rígido requerido para atualizar automaticamente da 1.5MR3 para a 2.X[13]
Mídia3 e web2 (combinado)	40	80	• 2 para Mídia3 e Web2, incluindo 1 se o NIC teaming for usado para redundância • 1 recomendado para o gerenciamento de rede ESXi	1 TB; mínimo de 10.000 RPM	768 GB
Proxy reverso de Internet (IRP)	40	36	• 2 para IRP, incluindo 1 se o NIC teaming for usado para redundância • 1 recomendado para o gerenciamento de rede ESXi	300 GB; mínimo de 7.200 RPM	172 GB
Mídia e administração (combinado) para HA	40	80	• 2 para Mídia e Administração, incluindo 1 se o NIC teaming for usado para redundância • 1 recomendado para o gerenciamento de rede ESXi	1,5 TB; mínimo de 10.000 RPM	990 GB

Máquinas Virtuais no organizador ESXi (Servidor UCS da Cisco)	Núcleo do processador	Memória (GB)	Portas Ethernet	Requisitos de Armazenamento em Disco Rígido para Novas Instalações	Espaço livre para armazenamento em disco rígido requerido para atualizar automaticamente da 1.5MR3 para a 2.X[13]
Web para HA	40	80	• 2 para Web, incluindo 1 se o NIC teaming for usado para redundância • 1 recomendado para o gerenciamento de rede ESXi	1 TB; mínimo de 10.000 RPM	896 GB
IRP para HA	40	36	• 2 para IRP, incluindo 1 se o NIC teaming for usado para redundância • 1 recomendado para o gerenciamento de rede ESXi	300 GB; mínimo de 7.200 RPM	172 GB

13 Se você escolher Atualização Manual, onde você implanta manualmente todas as máquinas virtuais, e você estiver utilizando o mesmo hardware, você é obrigado a ter o dobro do espaço livre como é necessário para a atualização automática.

Observação Para sistemas com 2000 usuários, não recomendamos implantar máquinas virtuais adicionais em um organizador DMZ. Isto pode resultar num aumento de perda de pacotes e latência notável nos conectores de mídia.

Recursos Reservados pelas Máquinas Virtuais em um Sistema de 2000 Usuários

Esta seção ilustra quanta mídia as máquinas virtuais usam e é dirigido para aqueles com conhecimento avançado em VMware. Os recursos da CPU são especificados como vCPUs (núcleos) e MHz (ciclos de CPU). O VMware VMkernel utiliza ciclos MHz para controlar o agendamento da CPU.

Os recursos de memória são especificados pelo máximo de memória e pela memória reservada. A memória reservada não é compartilhada com outras máquinas virtuais no mesmo servidor físico UCS da Cisco.

Os recursos de disco (armazenamento) são controlados em duas áreas distintas. Durante a compilação OVA, os tamanhos das partições do sistema de arquivos do CentOS determinam o tamanho mínimo do disco. Em segundo lugar, o vCenter controla o máximo de espaço em disco disponível.

Se você tentar implantar uma máquina virtual sem o número mínimo de vCPUs, a implantação OVA da máquina virtual irá falhar. Se você tentar implantar uma máquina virtual sem a velocidade mínima total do processador MHz, a máquina virtual não ligará.

Importante Os números nesta tabela não incluem recursos para o VMware ESXi. Consulte Recursos consumidos pelo CWMS e o organizador ESXi.

Tipo de Máquina Virtual	CPU Virtual (vCPU)	CPU[14](MHz)	Memória Reservada/Memória Total[15](GB)	Discos (GB)
Admin	10	20.600	16/16	418 Para as versões 2.6 e superiores, novos sistemas implantados usando um arquivo OVA devem ser 513.
Mídia	30	60.800	14/44	128
Web	10	20.600	16/16	128
Proxy Reverso da Internet	20	41.200	10/10	128

14 Número obtido pela multiplicação do número de CPUs físicas com a velocidade do chip da CPU (MHz). O hyperthreading não está incluído neste cálculo. (A CPU física deve ter uma velocidade de clock de 2.4 GHz ou mais rápido).

15 As máquinas virtuais com funcionalidade de mídia têm memória adicional, não reservada; Memória = Reservada/Total

Capacidade do sistema matriz

Pontos Chave:

- Um dos pressupostos básicos para a informação apresentada nesta seção é de que haja pelo menos duas pessoas que participem de uma reunião.
- As conexões de reuniões simultâneas são definidas como o número de pessoas participando de uma reunião em um determinado momento. Por exemplo, em um sistema de 50 usuários, o máximo de conexões de reuniões simultâneas pode ser composto de cinco reuniões simultâneas, em que cada uma tem um total de 10 pessoas na reunião (ou seja, um organizador e nove participantes).
- Depois que o número máximo de participantes da reunião for alcançado em qualquer momento, o sistema não permite que outros usuários iniciem ou participem das reuniões. Deste número máximo de

participantes da reunião (2000, 800, 250 ou 50 pessoas), apenas metade desses usuários pode usar o vídeo. O vídeo é definido como enviando ou recebendo, ou seja, os usuários podem estar utilizando o vídeo da webcam WebEx ou a opção de compartilhamento de arquivos de vídeo que permite que os usuários compartilhem um vídeo.

- O compartilhamento do desktop não é considerado vídeo. Isso significa que, com um sistema de 250 usuários, 250 pessoas podem compartilhar os seus desktops durante as reuniões em um determinado momento.
- A adição de Alta Disponibilidade ou de não aumenta a capacidade do sistema de realizar reuniões; um sistema com 800 usuários ainda é um sistema com 800 usuários.

Os números na tabela abaixo representam a capacidade de concepção para o sistema Cisco WebEx Meetings Server. Operar o sistema em uma capacidade maior do que essas especificadas pode resultar em uma experiência de usuário degradada e pode resultar em instabilidade no sistema. A Cisco se reserva o direito de reforçar os limites de capacidade nesses níveis.

Observação Estes valores na tabela a seguir permanecem os mesmos, independentemente se o sistema é composto por um único centro de dados ou é um sistema com .

Tabela 3: Matriz de capacidade do sistema da versão 2.5 e superior

Capacidade do sistema	sistema de 2000 usuários	sistema de 800 usuários	sistema de 250 usuários	sistema de 50 usuários	Notas
Máximo de Conexões Simultâneas de Reunião (Áudio, vídeo e os usuários da Internet)	2000	800	250	50	O número de pessoas que participam em reuniões simultâneas em um determinado momento.
Máximo de conexões simultâneas de áudio (Chamadas telefônicas de teleconferência e conexão de voz utilizando o computador dos clientes da reunião)	2000	800	250	50	A capacidade do sistema é a mesma como exibida no lado esquerdo, independentemente de quais combinações das seguintes características são usadas: • Codecs de áudio G.711, G.722, G.729 • Teleconferência IPv4 ou IPv6 • Criptografia de áudio TLS/SRTP

Capacidade do sistema	sistema de 2000 usuários	sistema de 800 usuários	sistema de 250 usuários	sistema de 50 usuários	Notas
Número Máximo de Vídeos Simultâneos e Usuários Compartilhando Arquivos de Vídeo	1000[16]	400	125	25	Estes números mostram o número máximo de conexões simultâneas de reunião (ou participantes) autorizado a usar o compartilhamento de vídeo ao mesmo tempo. Quando o número de usuários compartilhando vídeo em reuniões simultâneas atingir esse limite, os usuários restantes convidados para as reuniões simultâneas poderão participar das reuniões, mas as janelas de vídeo serão desativadas. **Observação** Se um participante em uma reunião utiliza vídeo, então todos os outros usuários na mesma reunião serão contados como usuários de vídeo, mesmo que eles não estejam utilizando o vídeo. **Observação** O compartilhamento do desktop não é considerado vídeo.
Número Máximo de Participantes em uma Reunião	500	500	250	50	Esses números mostram o número máximo de participantes que podem participar de uma reunião.
Número máximo de reuniões que podem ser gravadas simultaneamente	100	40	13	3	Este é o número total de reuniões que podem usar a funcionalidade Gravação ao mesmo tempo.
Número Máximo de Sessões Simultâneas de Reprodução de Gravação	500	200	63	12	Este é o número total de sessões de reprodução de gravação que podem ocorrer simultaneamente. Refere-se as gravações que estão salvas no seu sistema de armazenamento e não inclui as gravações que são baixadas para os desktops dos usuários. **Observação** Essas sessões de reprodução não estão incluídas nas conexões de reuniões simultâneas no sistema.
Número máximo de perfis de usuários	400,000	400,000	400,000	400,000	Esse número inclui usuários ativos e desativados.
Número máximo de reuniões simultâneas	1000	400	125	25	O número de reuniões separadas que pode estar ativas ao mesmo tempo.

Capacidade do sistema	sistema de 2000 usuários	sistema de 800 usuários	sistema de 250 usuários	sistema de 50 usuários	Notas
Taxa Máxima de Chamada (chamadas/por segundo)	20	8	3	1	Este é o número médio de usuários que pode discar para uma reunião durante um período de tempo de um segundo. Depois que o sistema chegar a esse número, os próximos usuários a discarem na reunião podem enfrentar uma espera de alguns segundos adicionais antes de se conectarem à reunião.
Número Máximo de Registros Únicos Simultâneos	20 pessoas por segundo	8 pessoas por segundo	3 pessoas por segundo	1 pessoa por segundo	Este é o número médio de usuários que pode iniciar sessão simultaneamente no site WebEx durante um período de tempo de um segundo. Depois que o sistema chegar a esse número, os próximos usuários que iniciarem a sessão no site WebEx podem enfrentar uma espera de alguns segundos adicionais antes de poderem participar de uma reunião.
Número máximo agregado de utilização da largura de banda	5 Gbps	2 Gbps	625 Mbps	125 Gbps	Utilizando o nosso sistema de teste na sua largura de banda máxima, esta é a máxima largura de banda que o sistema de teste pode lidar. Para mais informações sobre a utilização de largura de banda, consulte a seção Requisitos de largura de banda de rede no capítulo *Topologia de rede para o sistema* do Guia de Planejamento. Você também pode consultar o Documento sobre largura de banda de rede WebEx.

16 800 nos Padrões de Processamento de Informações Federais (ambientes FIPS)

Observação Para novas instalações do Cisco WebEx Meetings Server Versão 2.0 e superior, os requisitos de armazenamento são:

- O espaço em disco pode ser local (DAS) ou externo (SAN ou NAS).
- Os organizadores ESXi (servidor Cisco UCS) com a máquina virtual de Administração requerem 1.5 TB de espaço no disco.
- Os organizadores ESXi (servidor Cisco UCS) sem uma máquina virtual de Administração requerem 1 TB de espaço no disco.
- Ao atualizar o Cisco WebEx Meetings Server usando os servidores Cisco UCS existentes, os organizadores ESXi requerem 1118 GB de espaço livre no disco caso o servidor UCS possua apenas a máquina virtual de Administração (sistema primário ou HA) ou 990 GB de espaço livre no disco se o servidor UCS possui uma máquina virtual de Administração e uma de Mídia (sistema primário ou HA).

Para obter detalhes completos, consulte a seção **Recursos usados pelo Cisco WebEx Meetings Server e o organizador ESXi** nos http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html.

Dica O duração máxima de uma reunião é de 24 horas para todas as implantações de sistema com qualquer número de usuários.

Observação Ao considerar uma atualização, planeje o aumento do tamanho dos armazenamentos de dados, uma vez que o sistema original e o sistema atualizado compartilham armazenamentos de dados até o teste do sistema atualizado estar completo e o sistema original removido.

Para obter informações sobre os requisitos da largura de banda de rede para os sistemas de usuários de diferentes tamanhos, consulte a seção "Requisitos da Largura de Banda de Rede" no capítulo Topologia de Rede para seu Sistema neste livro.

Caminhos de Atualização Suportados

Esta versão do Cisco WebEx Meetings Server suporta as atualizações da versão 1.x à 2.8. Os seguintes pontos se aplicam:

- Uma atualização é definida como uma substituição do sistema para implantar grandes modificações que fizemos ao sistema.
- Uma atualização é definida como uma modificação incremental do sistema. As atualizações implementam correções e pequenas melhorias.
- Uma atualização retém todos os dados do sistema original. Uma atualização mantém todos os dados do sistema original, exceto para os registros.
- Ao atualizar, você não pode pular uma versão principal do software e ir diretamente para a versão de manutenção de companhia (MR).

Por exemplo, para atualizar da versão 1.5MR5 para a 2.8MR, *atualize* da 1.5MR5 para a 2.8 e, em seguida, *atualize* para a 2.8MR.

Observação Todas as atualizações exigem tempo de inatividade. Para Vários centros de dados, você atualiza ambos os centros de dados simultaneamente.

Cuidado Não clique em **Reiniciar** em um centro de dados até que a atualização do outro esteja completa e ambos exibam o botão **Reiniciar**. Quando você atualizar da versão 2.5MR6 ou posterior para a 2.8, reinicie um centro de dados antes que a atualização seja concluída para a replicação de outros intervalos.

Use a tabela a seguir para determinar como atualizar o Cisco WebEx Meetings Server versão 2.8.

Versão instalada	Para a versão	Caminho
1.0 para 1.1	2.8	**1** Atualizar para 1.5. **2** Atualize para o 1.5MR5 Patch 2 ou posterior. **3** Atualizar para 2.8.
1.5 para 1.5MR4	2.8	**1** Atualize para o 1.5MR5 Patch 2 ou posterior. **2** Atualizar para 2.8.
1.5 MR5	2.8	**1** Atualize para o 1.5MR5 Patch 2 ou posterior. **2** Atualizar para 2.8.
1.5MR5 Patch 2 ou posterior	2.8	Atualizar para 2.8.
2.0 para 2.0MR8	2.8	**1** Atualizar para 2.0MR9. **2** Atualizar para 2.8.
2.0MR9 ou posterior	2.8	Atualizar para 2.8.
2.5 para 2.5MR5	2.8	**1** Atualizar para 2.5MR6. **2** Atualizar para 2.8.
2.5MR6	2.8	Atualizar para 2.8.

Versão instalada	Para a versão	Caminho
2.6 para 2.6MR2	2.8	1 Atualizar para 2.6MR3 2 Atualizar para 2.8
2.6MR3 ou posterior	2.8	Atualizar para 2.8.
2.7 ou qualquer 2.7MR	2.8	Atualizar para 2.8.
2.8 ou qualquer 2.8MR	Qualquer 2.8MR	Atualizar para 2.8MR.

Importante Não é possível alterar o tipo de criptografia de áudio (Criptografia de áudio - AE/Áudio não criptografado - AU) para o sistema durante uma atualização. Após a implantação, a única forma de alterar um sistema de um tipo de criptografia de áudio para outro é implantar um novo sistema.

Para obter mais informações, consulte os seguintes documentos:

- *Guia de administração do Cisco WebEx Meetings Server versão 2.8*: http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html
- *Requisitos do sistema e guia de planejamento do Cisco WebEx Meetings Server versão 2.8*: http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html

Caminhos de Atualização Suportados

Esta versão do Cisco WebEx Meetings Server suporta as atualizações da versão 1.x à 3.0. Os seguintes pontos se aplicam:

- Uma atualização é definida como uma substituição do sistema para implantar grandes modificações que fizemos ao sistema.
- Uma atualização é definida como uma modificação incremental do sistema. As atualizações implementam correções e pequenas melhorias.
- Uma atualização retém todos os dados do sistema original. Uma atualização mantém todos os dados do sistema original, exceto para os registros.
- Ao atualizar, você não pode pular uma versão principal do software e ir diretamente para a versão de manutenção de companhia (MR).

  Por exemplo, para atualizar da versão 1.5MR5 para a 3.0MR, *atualize* da 1.5MR5 para a 3.0 e, em seguida, *atualize* para a 3.0MR.

Observação Todas as atualizações exigem tempo de inatividade. Para Vários centros de dados, você atualiza ambos os centros de dados simultaneamente.

Cuidado Não clique em **Reiniciar** em um centro de dados até que a atualização do outro esteja completa e ambos exibam o botão **Reiniciar**. Quando você atualizar da versão 2.5MR6 ou posterior para a 3.0, reinicie um centro de dados antes que a atualização seja concluída para a replicação de outros intervalos.

Use a tabela a seguir para determinar como atualizar o Cisco WebEx Meetings Server versão 3.0.

Versão instalada	Para a versão	Caminho
1.0 para 1.1	2.8	**1** Atualizar para 1.5. **2** Atualize para o 1.5MR5 Patch 2 ou posterior. **3** Atualizar para 2.8.
1.5 para 1.5MR4	2.8	**1** Atualize para o 1.5MR5 Patch 2 ou posterior. **2** Atualizar para 2.8.
1.5 MR5	2.8	**1** Atualize para o 1.5MR5 Patch 2 ou posterior. **2** Atualizar para 2.8.
1.5MR5 Patch 2 ou posterior	2.8	Atualizar para 2.8.
2.0 para 2.0MR8	3.0	**1** Atualizar para 2.0MR9. **2** Atualizar para 3.0.
2.0MR9 ou posterior	3.0	Atualizar para 3.0.
2.5 para 2.5MR5	3.0	**1** Atualizar para 2.5MR6. **2** Atualizar para 3.0.
2.5MR6	3.0	Atualizar para 3.0.
2.6 ou qualquer 2.6MR	3.0	Atualizar para 3.0.
2.7 ou qualquer 2.7MR	Qualquer 3.0MR	Atualizar para 3.0MR.

Importante Não é possível alterar o tipo de criptografia de áudio (Criptografia de áudio - AE/Áudio não criptografado - AU) para o sistema durante uma atualização. Após a implantação, a única forma de alterar um sistema de um tipo de criptografia de áudio para outro é implantar um novo sistema.

Para obter mais informações, consulte os seguintes documentos:

- *Guia de administração do Cisco WebEx Meetings Server versão 3.0*: http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html
- *Requisitos do sistema e guia de planejamento do Cisco WebEx Meetings Server versão 3.0*: http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-and-configuration-guides-list.html

CAPÍTULO 2

Introdução do Cisco WebEx Meetings Server

O Cisco Webex Meetings Server (CWMS) é uma solução de conferência de nuvem privada (no local) segura, totalmente virtualizada que combina áudio, vídeo e internet para reduzir os custos de conferência e ampliar seus investimentos nas Comunicações Unificadas da Cisco.

Assim como outros produtos Cisco WebEx, ele oferece ferramentas de colaboração em tempo real, incluindo compartilhamento de documentos, aplicativos e desktop, ferramentas de anotação, controle de organizador completo para gerenciamento efetivo de reuniões, uma lista de participantes integrada com falante ativo e comutação, gravação e reprodução de vídeo. Este produto utiliza vídeo de alta qualidade, por isso a experiência de compartilhamento de vídeo é nítida e clara.

Você pode implantar e gerenciar esta solução de conferência na sua nuvem privada, atrás do firewall em seu centro de dados. Ele é projetado para servidores UCS da Cisco e para o VMware vSphere. (Para obter requisitos específicos, consulte Requisitos Mínimos de Hardware, na página 10). Possui uma rápida implantação virtual e ferramentas poderosas para que os administradores configurem e gerenciem o sistema, e vejam as métricas principais do sistema.

Além disso, os usuários móveis podem assistir e participar nas reuniões. Para os dispositivos suportados, consulte Requisitos dos sistemas operacionais para dispositivos móveis, na página 196.

Considerações importantes para o sistema

Observe o seguinte:

- Projeções proxies—não é recomendável, mas você pode usá-las com restrições. Para obter detalhes completos, consulte o *Guia de Solução de Problemas do Cisco WebEx Meetings Server*.
- Proxies reversos—apenas o servidor de proxy reverso da internet incluído com este produto é suportado.
- NAT—suportada quando atende aos requisitos para este sistema. Para obter detalhes completos, consulte Usar NAT com seu sistema.
- Centros de dados único — implantações dentro de um único centro de dados são suportadas por todas as versões do Cisco WebEx Meetings Server. Para obter detalhes completos, consulte Implantação de um centro de dados único.
- Vários centros de dados—os centros de dados que executam o Cisco WebEx Meetings Server versão 2.5 ou superior podem ser unidos para criar um sistema composto por vários centros de dados. Para obter detalhes completos, consulte *Sobre o Centro de multidados* no Guia de administração do Cisco WebEx Meetings Server.

- Servidor de armazenamento — Cada centro de dados em um sistema com deve ter um servidor de armazenamento separado. O mesmo servidor de armazenamento não pode suportar mais de um centro de dados.
- Sistema de alta disponibilidade—definido como um sistema com máquinas virtuais redundantes que executam a mesma versão do Cisco WebEx Meetings Server. Se o sistema primário (em um sistema com centro de dados único) falhar, o sistema de alta disponibilidade continua em serviço. As máquinas virtuais redundantes de alta disponibilidade devem ser co-localizadas no mesmo centro de dados com as máquinas virtuais primárias. As máquinas virtuais do sistema de alta disponibilidade e primário devem também estar na mesma VLAN ou subrede.

  Você não pode unir sistemas de alta disponibilidade para criar um ambiente de .
- Servidor de proxy reverso da internet (IRP)—é definido como uma máquina virtual colocada como um proxy entre a internet externa e a rede interna de uma empresa para fornecer acesso público ao CWMS. É necessário um servidor de proxy reverso da internet para permitir que os usuários agendem e participem de reuniões de dispositivos móveis ou para fornecer acesso seguro ao site WebEx da internet. Não é necessário um servidor de proxy reverso da internet se você limitar o acesso ao Cisco WebEx Meetings Server para sua rede interna. (Implante uma máquina virtual IRP usando o mesmo arquivo OVA que você usou para implantar sua máquina virtual de administração. A máquina virtual IRP deve estar na mesma subrede que o endereço IP virtual público.)
- Endereço IP virtual (VIP)—usado para se comunicar com as máquinas virtuais de administração, mídia e web dentro de um centro de dados.
- Endereço IP virtual privado (VIP)—configurado na máquina virtual de administração e está associado à URL do site de administração. O VIP privado também pode ser associado à URL do site WebEx se o endereço estiver configurado no servidor DNS interno em uma implantação DNS split-horizon ou em implantações sem um servidor de proxy reverso da internet.
- Endereço IP virtual público (VIP)—configurado na máquina virtual de proxy reverso da internet e está associado apenas à URL do site WebEx. A URL do site WebEx nos servidores DNS externos deve ser resolvida para o endereço de IP Virtual Público para fornecer aos usuários acesso ao site WebEx a partir da Internet. Um endereço de IP virtual público não é configurado no sistema se não houver um servidor de proxy reverso da Internet.

Cuidado Se você ignorar as nossas recomendações e exigências ao implantar um sistema, você não irá receber suporte da Cisco. A Cisco não é responsável por quaisquer problemas que possam ocorrer como resultado de não seguir nossa orientação.

Recursos Novos e Alterados para o Cisco WebEx Meetings Server

Para uma lista de recursos novos e alterados, consulte "Recursos novos e alterados do Cisco WebEx Meetings Server" nas *Notas de versão para o Cisco WebEx Meetings Server* em Notas de versão.

- Informações para os clientes do Cisco Unified MeetingPlace, página 39
- Implantação de um centro de dados único, página 39
- Registrando centros de dados únicos para criar um sistema com (MDC), página 39
- Usando O Vmware vSphere Com Seu Sistema, página 40
- Desempenho do Sistema IOPS e de Armazenamento, página 42

- Instalar o VMware vSphere ESXi e Configurar o Armazenamento, página 44
- Participar de Reuniões, página 45

Informações para os clientes do Cisco Unified MeetingPlace

Por causa de diferenças de arquitetura, não há caminho de migração (para contas de usuários existentes, personalizações e reuniões) do Cisco Unified MeetingPlace para o Cisco WebEx Meetings Server. Estes são dois produtos distintos.

Você pode facilitar a transição para os usuários, continuando a suportar tanto o Cisco Unified MeetingPlace quanto o Cisco WebEx Meetings Server enquanto incentiva seus usuários a mudar para o novo sistema.

Implantação de um centro de dados único

O Cisco WebEx Meeting Server (CWMS) pode ser implantado como um sistema de Centro de dados único (SDC) e, opcionalmente, como um sistema de alta disponibilidade (HA) ou um sistema com (MDC) (consulte Redundância nas implantações HA ou MDC, na página 53). Um sistema SDC (incluindo um sistema com suporte HA) requer apenas licenças de Organizadores após um período de teste. Um sistema MDC exige um mínimo de duas licenças de recursos do MDC, licenças de Organizadores e não há período de teste do MDC.

Registrando centros de dados únicos para criar um sistema com (MDC)

Você pode entrar em dois centros de dados que estão executando o Cisco WebEx Meeting Server versão 2.5 ou superior para formar um único sistema com vários centros de dados (MDC). Um máximo de dois centros de dados podem ser unidos. A diferença entre um sistema com vários centros de dados e um de Alta disponibilidade é que um sistema de Alta disponibilidade deve ser colocalizado e funciona como um sistema de backup. Em um sistema MDC, os centros de dados podem ser localizados em diferentes localizações geográficas e ambos os centros de dados contribuem para o processamento do sistema. Consulte Redundância nas implantações HA ou MDC, na página 53. Uma licença deve ser adquirida para cada centro de dados CWMS em um sistema MDC. As licenças MDC devem ser compradas antes de tentar implantar um sistema MDC. (Um sistema com um único centro de dados não precisa de uma licença de recurso.) Para obter detalhes sobre como preparar os centros de dados a serem unidos, o processo de Registro e como executar os dados de um centro de dados para outro quando o processo de Registro estiver completo, consulte o capítulo "Registrando centros de dados para criar um sistema com vários centros de dados (MDC)" no *Guia de administração do Cisco WebEx* (http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html).

Usando O Vmware vSphere Com Seu Sistema

Importante Este produto só instala em uma plataforma de virtualização VMWare vSphere. As ferramentas VMWare para o CWMS são instaladas automaticamente durante a implantação do sistema e não devem ser atualizadas manualmente. Consulte docwiki.cisco.com/wiki/VMWare_Tools para obter mais informações sobre as ferramentas VMWare.

- O Cisco WebEx Meetings Server é projetado para funcionar em qualquer servidor UCS equivalente da Cisco que atende ou excede os requisitos do sistema. No entanto, para poupar tempo, recomendamos o uso de servidores Cisco UCS padrão. Para obter detalhes completos sobre os requisitos de hardware e VMWare, consulte Requisitos Mínimos de Hardware, na página 10.
- É necessário adquirir o VMWare vSphere 5.0, 5.0 Update 1, 5.0 Update 2, 5.1, 5.1 Update 1, 5.5 ou 6.0 para usar como a plataforma do hipervisor do Cisco WebEx Meetings Server.

  Observação Por razões de segurança, o 5.1 deve ser a versão 1900470 ou posterior.

  Complete um dos seguintes:

  - Compre o vSphere diretamente da Cisco no GPL (Lista de Preços Global). A Cisco é um parceiro aprovado e distribuidor do VMWare.
  - Compre o vSphere diretamente do VMWare através de acordos corporativos que você tem com o VMWare.

Vantagens de implantar um sistema no VMware vSphere

Esta seção explica porque o VMware vSphere e o vCenter usam integralmente este produto Cisco WebEx e lista algumas considerações.

Implantação do Sistema

- Este produto é embalado como um aparelho virtual OVA compatível com o VMware vSphere e não como uma coleção de pacotes de software em um DVD. Você deve ter o vCenter para implantar o OVA ou o produto não instalará.
- Ao embalar como um utensílio virtual, habilitamos a implantação rápida; em alguns casos, em menos de uma hora.
- Para facilitar instalações rápidas com o dispositivo virtual OVA, você poderá selecionar a implantação automática do sistema para a maioria dos tamanhos de sistema. Basta fornecer as credenciais do vCenter e implantaremos todas as máquinas virtuais em seu sistema, sem intervenção manual. Esta inovação minimizará seus custos de trabalho e tempo.

Observação O modelo OVA cria dois NICs virtuais para cada máquina virtual. No entanto, apenas as máquinas virtuais de admin usam os dois NICs virtuais. Para todas as outras máquinas virtuais do Cisco WebEx Meetings Server (CWMS), apenas um NIC virtual é usado e o outro é desligado.

- CWMS requer que você execute o VMware ESXi ou o VMware ESXi correspondente instalável da Imagem ISO da Cisco. Ambas as edições contém os drivers necessários para suportar os servidores UCS da Cisco que são exigidos pelo Cisco WebEx Meetings Server. Para obter mais informações, consulte http://www.cisco.com/en/US/docs/unified_computing/ucs/release/notes/OL_26617.pdf.

Fácil recuperação de erros do sistema

Se a mudança não atender às suas expectativas, usando o VMware Data Recovery você pode reverter as alterações que afetam os sistemas de forma rápida e sem uma reimplantação do sistema.

Considerações vSphere

Observe as seguintes considerações:

- Você pode mover sua máquina virtual para outro organizador ESXi. No entanto, você deve manter a disposição das máquinas virtuais no novo organizador ESXi. Em outras palavras, se você planeja mover uma máquina virtual de mídia que seja corresidente com uma máquina virtual da Web, você deverá movê-la para um host ESXi separado (onde seja a única máquina virtual) ou movê-la para um host ESXi que já tenha uma máquina virtual da Web.

Observação O organizador ESXi de destino deverá obedecer aos mesmos requisitos do sistema como o organizador ESXi de origem.

Os seguintes recursos do VMware não são suportados com o CWMS:

- VMotion e Storage VMotion (Embora você possa mover as máquinas virtuais, você não pode fazer isso usando estas ferramentas.)
- Programação de Recursos Distribuídos (DRS) do Vmware
- Alta Disponibilidade (HA) do vSphere
- Agrupamento e compartilhamento de recursos vSphere
- Clonando uma máquina virtual

Melhores Práticas vSphere

- Recomendamos que você não use instantâneos de máquinas virtuais. Se você decidir usar fotos instantâneas, então depois de confirmar as mudanças do sistema, ou comprometa as fotos instantâneas ou remova-as o mais rápido possível. Manter uma foto instantânea por algum período de tempo irá resultar em grave degradação do desempenho.
- Para ambientes de SAN, implante imagens de disco para uma SAN com números IOPS elevados.

Para um sistema com 800 usuários, a média do IOPS para uma implantação com o OVA é de 506 (máx IOPS é de 855) para a máquina virtual de Administração e de 475 (máx IOPS é de 652) para uma máquina virtual de Mídia. Uma vez que estas máquinas virtuais são criadas e ativadas, então você poderá inserir a URL maiúsculas/minúsculas e continuar a implantação do sistema em um navegador da web. A média do IOPS para um sistema primário é de 108 (máx IOPS é de 1558) e de 163 (máx IOPS é de 1736) para um sistema secundário.

- Certifique-se de que há espaço livre suficiente em sua SAN. As fotos instantâneas são armazenadas na mesma SAN.
- Implante uma rede de 10 GB para rápida implantação e banda larga para o crescimento futuro.
- Recomendamos que você gerencie todas as máquinas virtuais utilizando o mesmo vCenter. Isto permite uma recuperação mais fácil se você precisar recuperar seu sistema.

Para obter mais informações sobre a largura de banda de rede, consulte Requisitos da Largura de Banda de Rede, na página 56.

Requisitos do vCenter Server

Além do vSphere, o vCenter Server também é necessário.

- Para implantar este dispositivo virtual, você também deve usar o vCenter para implantar e gerenciar as máquinas virtuais em seu sistema. Este produto não funcionará sem vCenter Server.
- A Cisco recomenda backups e fotos instantâneas do sistema à frente de importantes operações de impacto do sistema. Criar backups permite que você reverta as alterações no caso da atualização não atender às suas expectativas. Você pode automatizar backups e fotos instantâneos usando o vCenter.
- O CWMS suporta o vSphere Standard Edition.

Edição vSphere para os Sistemas de 800 e 2000 Usuários

- Os sistemas de 800 e 2000 usuários compreendem máquinas virtuais que requerem entre 30 e 40 vCPUs. Estas máquinas virtuais utilizam estes vCPUs para executar tarefas de computação muito intensivas, tais como a codificação ou descodificação SSL, misturando fluxos de áudio, e assim por diante.

  Para obter informações completas sobre os requisitos vCPU, consulte Recursos consumidos pelo CWMS e o organizador ESXi, na página 12.
- No mínimo, você deve comprar a edição vSphere 5.0 Enterprise Plus ou a edição vSphere 5.1 Enterprise Plus, uma vez que as edições vSphere de menor efeito não suportam o número de vCPUs necessários.

Desempenho do Sistema IOPS e de Armazenamento

IOPS e Taxa de Transferência máxima esperadas

A tabela a seguir mostra a IOPS máxima esperada e os valores de transferência para a carga máxima no sistema de uma única máquina virtual.

Tamanho do sistema	Máquinas Virtuais	Operações máximas de entrada/saída (IOPS)	Leitura máxima de megabytes por segundo	Gravação máxima de megabytes por segundo
sistema de 50 usuários	Admin	450	1	15
	DMZ	70	0.3	0.3
sistema de 250 usuários	Admin	1400	1	25
	Mídia	150	1	10
	DMZ	110	0.4	0.6
sistema de 800 usuários	Admin	1400	3	50
	Mídia	300	1	30
	DMZ	150	1	1.5
sistema de 2000 usuários	Admin	1600	2.5	60
	Mídia	300	1	25
	Web	200	3	1.5
	DMZ	200	1.5	3

IOPS para a reinicialização do sistema de um sistema de 2000 usuários

A tabela a seguir mostra as informações IOPS de um sistema de 2000 usuários para o processo de inicialização (reinicialização).

Máquinas virtuais em um sistema de 2000 usuários	IOPS para inicialização do sistema (reinicialização)	IOPS para atualização mínima
Admin	2300	3000
Mídia	2000	2000
Web	1500	2000
Web	1000	2000

IOPS para backup de um sistema de 2000 usuários

A tabela a seguir mostra as informações IOPS de um sistema de 2000 usuários para um backup feito durante as horas de folga.

Máquina virtual de administração para um sistema de 2000 usuários	IOPS para backup	Leitura máxima de megabytes por segundo	Gravação máxima de megabytes por segundo
1 GB de backup	2000	220	300
12 GB de backup	5000	320	600

Instalar o VMware vSphere ESXi e Configurar o Armazenamento

O Cisco WebEx Meetings Server é uma solução baseada em software. Não é uma combinação de pacote de hardware/software. Você tem escolhas sobre como comprar e fornecer suas plataformas de hardware, desde que o hardware atenda ou exceda os requisitos de armazenamento, memória e CPU.

Você pode implantar o Cisco WebEx Meetings Server em Servidores UCS da Cisco que atendam nossas especificações mínimas. Ou você pode optar por implementar este produto em Servidores UCS mais novos e de maior efeito que excedam nossas especificações mínimas.

Múltiplos controladores RAID e opções de rede estão disponíveis. Você pode optar por usar o armazenamento SAN, em vez do RAID local. Nós não fornecemos detalhes sobre cada tipo de configuração de armazenamento que você pode escolher.

No entanto, como o Cisco WebEx Meetings Server é implantado em Servidores UCS da Cisco, consulte o *Guia RAID de Servidores UCS da Cisco* em http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/raid/configuration/guide/RAID_GUIDE.html.

- Para instalar o VMware vSphere ESXi em um Servidor Back UCS de Série B, consulte http://www.cisco.com/en/US/docs/unified_computing/ucs/os-install-guides/vmware/b_B-Series_VMware_Install.html.
- Para instalar o VMware vSphere ESXi em um Servidor Rack UCS de Série C, consulte http://www.cisco.com/en/US/docs/unified_computing/ucs/os-install-guides/vmware/b_C-Series_VMware_Install.html.

Consulte também docwiki.cisco.com/wiki/VMware_Tools para obter mais informações.

Configurando o Cache de Gravação em um Controlador RAID

Para um melhor desempenho do sistema, você deve verificar a configuração da Gravação Padrão no seu controlador RAID. Você pode definir a Gravação Padrão para três configurações: *Write Back com BBU*, *Write Through* ou *Write Back Sempre*. Algumas diretrizes para selecionar a configuração apropriada para Gravação Padrão nos seus Servidores UCS da Cisco são:

- **Write Back com BBU** - use essa configuração se você instalou uma unidade de backup da bateria no seu controlador RAID. No caso de uma perda de energia do sistema, a unidade de backup da bateria preserva o conteúdo da memória de cache do controlador.

  No caso da unidade de backup da bateria falhar ou ficar off-line a um ciclo de reaprendizagem, a configuração Write Back com BBU falha no cache **Write Through** automaticamente. Sem uma unidade de backup da bateria funcionando, a configuração Write Through é mais segura, embora você possa observar a degradação do desempenho do subsistema I/O da máquina do organizador.

- **Write Through** - utilize esta configuração e habilite o cache expressamente (utilizando a opção de Cache em Disco) se você precisar remover a unidade de backup da bateria para reparos. Esta configuração deve proporcionar a você um melhor desempenho, mas não o ideal. Depois de substituir a bateria defeituosa, você pode retornar com segurança a configuração de Gravação Padrão para o modo Write Back com BBU.
- **Write Back Sempre** - utilize esta configuração se o organizador que hospeda o controlador RAID está conectado a uma fonte de alimentação ininterrupta.

Participar de Reuniões

A experiência do usuário final com o Cisco WebEx Meetings Server é de um site que os usuários acessam para agendar e entrar em reuniões. Este site inclui elementos de conferência em tempo real que facilitam as reuniões on-line. Os usuários podem participar de reuniões através de um navegador ou de um cliente nos desktops.

Para detalhes completos sobre a experiência do usuário final, inicie a sessão no site WebEx e selecione **Ajuda**.

Usuários do Windows

O seguinte assume que um usuário tem privilégios de administrador do Windows no seu PC o suficiente para permitir que entre nas reuniões WebEx. Se isso não é verdade, os administradores do sistema podem mover o cliente do aplicativo WebEx Meetings para um usuário usando software de gerenciamento de desktop, como o IBM Tivoli. Consulte Fazer download de aplicativos no site da Administração, na página 130.

- Os usuários do Microsoft Internet Explorer podem instalar um controle ActiveX ou plugin Java, baixar o instalador do aplicativo WebEx Meetings ou executar o aplicativo em uma pasta temporária do sistema (como TFS). A primeira vez que o usuário participa de uma reunião, o software do cliente é baixado e instalado automaticamente.
- Os usuários do Google Chrome e Mozilla Firefox podem instalar um plugin Java, baixar o aplicativo WebEx Meetings ou executar o aplicativo em uma pasta temporária do sistema. O software do cliente é baixado e instalado automaticamente a primeira vez que o usuário participar de uma reunião.

Não é necessário alterar qualquer um dos instaladores de aplicativos ActiveX, plugin Java, WebEx Meetings ou configurações TFS.

Usuários do Mac

- Se o Java estiver habilitado, o software do cliente será baixado e instalado automaticamente na primeira vez que o usuário entrar em uma reunião. (O Java está desativado por padrão no Mac OS X Lion versão 10.7 e no OS X Mountain Lion versão 10.8.)
- Se o Java estiver desativado, o usuário pode baixar e instalar o aplicativo WebEx Meetings.

Usuários do sistema de

Se o site WebEx usa certificados autoassinados em vez de certificados de uma autoridade de certificação bem conhecida, depois que o centro de dados é unido a outro centro de dados, os usuários devem instalar um certificado para cada centro de dados no armazenamento de Autoridades de Certificação de Raiz Confiável antes de iniciarem ou entrarem em uma reunião.

Usando navegadores Chrome e FireFox

Se você estiver usando o Chrome 32 e posterior ou Firefox 27[17]e posterior, você poderá ver uma solicitação para instalar o plugin Cisco WebEx. Selecione **Baixar** e siga as instruções para instalar o plugin necessário.

Observação Depois de instalar o plugin, pode ser necessário habilitá-lo.

- Se você estiver usando Chrome, selecione o ícone de plug-in que aparece no canto superior direito da sua página, marque a opção **Permitir sempre plug-ins...** e selecione **Concluído**.
- Se você estiver usando Firefox, selecione o ícone de plug-in que aparece no início de sua URL (antes do https:) e selecione **Permitir e lembrar**.

Se a reunião não iniciar automaticamente, atualize a página.

Se você estiver usando o navegador Chrome 38 e posterior para iniciar uma reunião WebEx ou reproduzir uma gravação WebEx, você pode ser requerido a concluir a seguinte instalação de uma só vez para adicionar a extensão Cisco WebEx no seu navegador Chrome:

1. Selecione **Adicionar WebEx ao Chrome**.
2. Selecione **Gratuito** na caixa de diálogo Extensão Cisco WebEx.
3. Selecione **Adicionar** para adicionar a extensão Cisco WebEx no seu navegador Chrome.
4. Abra o arquivo Cisco_WebEx_Add-on.exe e selecione **Executar**.
5. A página será atualizada quando a instalação estiver concluída. Se a reunião não iniciar automaticamente, atualize a página.

17 As versões exatas do Chrome e Firefox que são impactadas por essa política não foram finalizadas até a publicação deste documento.

CAPÍTULO 3

Layout da Máquina Virtual em sua Rede

O Cisco WebEx Meetings Server (CWMS) compreende dois grupos de máquinas virtuais: as máquinas virtuais internas e as máquinas virtuais de proxy reverso da internet (IRP) opcionais. O IRP é necessário para os sistemas onde é permitido que os usuários externos organizem ou participem de reuniões através da Internet sem o uso de VPN ou usando dispositivos móveis CDMA. Sem o IRP, apenas os usuários internos e VPN podem organizar ou participar de reuniões. Para obter mais informações sobre o IRP, consulte Considerações de Rede para o Proxy Reverso da Internet, na página 54.

Máquinas Virtuais Internas

Para máquinas virtuais internas consulte a Máquina virtual de Administração e, se aplicável, as máquinas virtuais de mídia e Web.

- As máquinas virtuais internas *devem* estar em uma única VLAN comum ou sub-rede. Durante a implantação do sistema, você verá mensagens de erro se as atribuições de endereços de IP violarem esta regra. O design do sistema pressupõe que todas as máquinas virtuais internas, incluindo as máquinas virtuais de Alta Disponibilidade (HA), estão conectadas através de uma LAN que oferece alta largura de banda, perda de pacotes insignificante e uma latência de menos de 4 ms.

  Voz, dados, vídeo e SAN, todos dependem da banda larga de rede. É fundamental implantar uma rede que consiga lidar com a carga pretendida.

- A Cisco recomenda colocar todas as máquinas virtuais internas no mesmo comutador Ethernet. No entanto, ao provisionar um sistema HA, recomendamos que você implemente dois comutadores Ethernet para garantir a redundância da rede.

- Se você decidir colocar as máquinas virtuais em comutadores Ethernet diferentes dentro do mesmo centro de dados, então a rede *deve atender* aos requisitos específicos de largura de banda e latência de rede, conforme descritos em Requisitos da Largura de Banda de Rede, na página 56. Nessa situação, o tronco comutador-para-comutador deverá atender às mesmas exigências de rede que a latência L3 e a taxa de transferência, para um único comutador físico.

Para obter informações adicionais sobre os sistemas com HA, consulte Redundância nas implantações HA ou MDC, na página 53.

- Diferentes tipos de topologia de rede para seu sistema, página 48
- Topologia de rede do proxy reverso da internet (IRP) interna, página 48
- Topologia de Rede Sem Split-Horizon, página 49

- Todas as Topologias de Rede Internas, página 50
- Topologia de Rede Split-Horizon, página 51
- Redundância nas implantações HA ou MDC, página 53
- Considerações de Rede para o Proxy Reverso da Internet, página 54
- Requisitos da Largura de Banda de Rede, página 56
- NIC Teaming para Agregação de Largura de Banda, página 61
- Balanceamento de carga, página 62

Diferentes tipos de topologia de rede para seu sistema

Este produto suporta as seguintes topologias de rede:

- Topologia de rede do proxy reverso da internet (IRP) interna, na página 48
- Topologia de Rede Sem Split-Horizon, na página 49
- Todas as Topologias de Rede Internas, na página 50
- Topologia de Rede Split-Horizon, na página 51

Observação Se a topologia de rede inclui projeções proxies, ela deve cumprir requisitos específicos para que o proxy reverso da Internet funcione corretamente. Consulte o *Guia de Solução de Problemas do Cisco WebEx Meetings Server* para obter detalhes completos.

Topologia de rede do proxy reverso da internet (IRP) interna

Esta seção descreve a topologia de rede quando todas as máquinas virtuais no seu sistema, incluindo a máquina virtual de Proxy Reverso da Internet, estão na mesma rede interna.

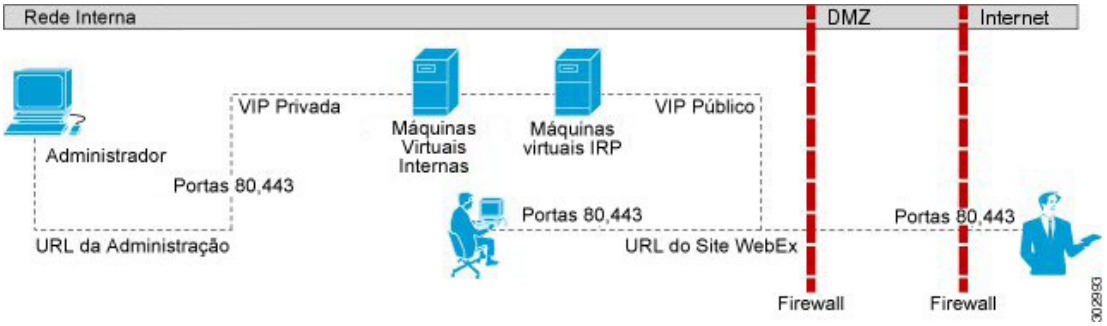
Esta configuração permite aos usuários iniciar sessão e entrar nas reuniões de forma segura a partir da Internet sem uma conexão VPN.

Se você estiver usando implantação automática, então os organizadores ESXi de todas as máquinas virtuais (incluindo o IRP) devem ser gerenciados a partir do mesmo VMware vCenter. Esta informação do vCenter é necessária durante uma implantação de sistema automático.

Observação Essa configuração suporta o acesso móvel.

Você irá definir a URL da Administração, a URL do site WebEx, o endereço VIP privado e o endereço VIP público durante a implantação do sistema. Para obter mais informações sobre estes termos, e quando fornecê-los, consulte a seção de instalação do *Guia de Administração do Cisco WebEx Meetings Server*.

Este é um diagrama de Toda a topologia de rede IRP interna.



Para obter uma lista completa das portas de acesso necessárias para essa implantação, consulte Porta de acesso quando todas as máquinas virtuais estão na rede interna, na página 87.

Vantagens de Todas as topologias de rede IRP internas

Em comparação com a topologia de rede sem split-horizon, não há máquinas virtuais na DMZ, e o tráfego de rede para usuários internos não está conectado através da DMZ para organizar ou participar de reuniões.

Desvantagens de Todas as topologias de rede IRP internas

O acesso público (permitindo que os usuários externos acessem o sistema) requer a abertura de portas de entrada (80 e 443) diretamente da Internet para a rede interna.

Para obter mais informações sobre o IRP, consulte Considerações de Rede para o Proxy Reverso da Internet, na página 54 e Adicionando acesso público ao seu sistema utilizando IRP.

Topologia de Rede Sem Split-Horizon

Esta seção descreve a topologia de rede quando estiver usando uma DNS Non-Split-Horizon. As máquinas virtuais internas (Administração e, se aplicável, mídia e web) estão na rede interna e o proxy reverso da Internet está na rede DMZ.

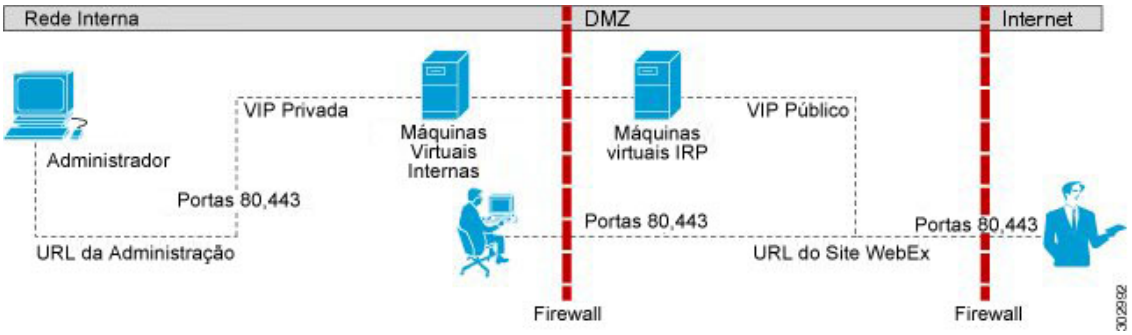
Observação Esta configuração permite aos usuários iniciar sessão e entrar nas reuniões de forma segura a partir da Internet sem uma conexão VPN.

Observação Essa configuração suporta o acesso móvel.

Para este produto, a principal diferença entre uma topologia de rede split-horizon e uma sem split-horizon é que para um sistema split-horizon, os usuários internos acessam a URL do site WebEx usando o endereço VIP privado. Os usuários externos (fora do firewall) acessam a URL do site WebEx usando o endereço VIP público. Para uma rede sem split-horizon, todos os usuários (internos e externos) acessam a URL do site WebEx usando o endereço VIP público.

Você irá definir a URL da Administração, a URL do site WebEx, o endereço VIP privado e o endereço VIP público durante a implantação do sistema. Para obter mais informações sobre estes termos, e quando fornecê-los, consulte a seção de instalação do *Guia de Administração do Cisco WebEx Meetings Server*.

Este é um esquema de diagrama de topologia de rede non-split-horizon.



Observação Para obter uma lista completa das portas de acesso necessárias para essa implantação, consulte Porta de acesso com um proxy reverso da Internet na rede DMZ, na página 88.

Vantagens de uma Topologia de Rede Sem Split-Horizon

- Controle apertado sobre o tráfego que entra e sai de uma rede.
- Endereços mais comuns, requisitos simples de rede de DNS.

Desvantagens de uma Topologia de Rede Sem Split-Horizon

- Configuração complexa, mas não tão complexa como a topologia de rede split-horizon.
- Tráfego interno é direcionado para a rede DMZ. Todo o tráfego de rede da Internet, assim como da interna (rede privada) irá para o Proxy Reverso da Internet na rede DMZ e, em seguida, volta para as máquinas virtuais internas.
- Requer mais portas a serem abertas no firewall entre a rede interna e DMZ do que toda a topologia de rede interna.
- A implantação automática do sistema (apenas sistemas para 50, 250 ou 800 usuários simultâneos) requer uma configuração mais detalhada no vCenter.
- Das três topologias de rede, essa é a configuração que mais afeta o desempenho de rede, já que todos os carregamentos de reuniões são por meio do Proxy Reverso de Internet. Como existem vários saltos, a latência da rede também é afetada.

Observação Consulte a Requisitos da Largura de Banda de Rede, na página 56 para obter detalhes sobre os requisitos de velocidade NIC para implantações DNS sem split-horizon.

Todas as Topologias de Rede Internas

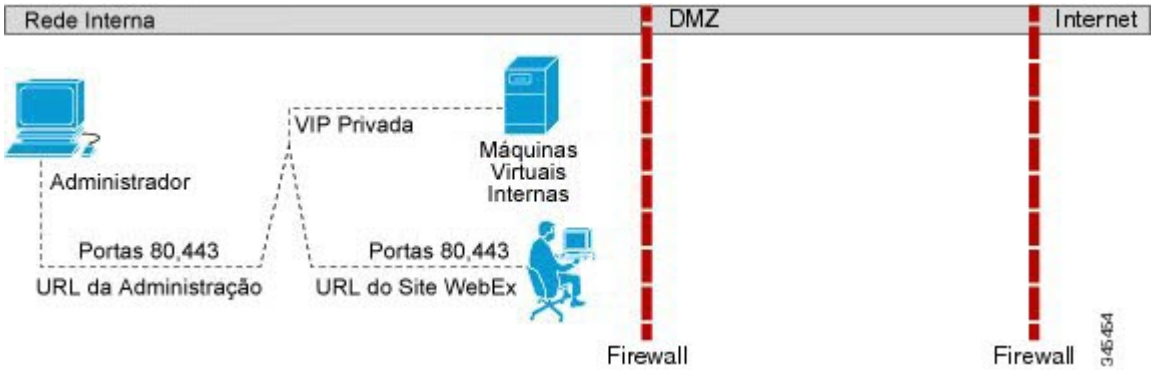
Esta seção descreve a topologia de rede, quando todas as máquinas virtuais no sistema estão na mesma rede interna. Não há acesso público; apenas usuários internos e de VPN podem organizar ou participar de reuniões.

Observação Se você estiver usando implantação automática, então os organizadores do ESXi de todas as máquinas virtuais devem ser gerenciados a partir do mesmo VMware vCenter. Esta informação do vCenter é necessária durante uma implantação de sistema automático.

Observação Esta configuração não suporta o acesso móvel.

Você irá definir a URL da Administração, a URL do site WebEx e o endereço VIP privado durante a implantação do sistema. Para obter mais informações sobre estes termos, e quando fornecê-los, consulte a seção de instalação do *Guia de Administração do Cisco WebEx Meetings Server*.

Este é um esquema de diagrama de Toda a topologia de rede interna.



Vantagens de um esquema sobre Todas as Topologias de Rede Internas

- Fornece baixa latência, pois há menos saltos de rede entre as máquinas virtuais.

Desvantagens de um esquema sobre Todas as Topologias de Rede Internas

- Não há acesso público (permitindo que os usuários externos acessem o sistema) e nem acesso para usuários móveis.

Topologia de Rede Split-Horizon

Esta seção descreve a topologia de rede quando você tem uma DNS split-horizon. As máquinas virtuais internas (Administração e, se aplicável, mídia e web) estão na rede interna e o proxy reverso da Internet está na rede DMZ.

Observação Esta configuração permite aos usuários iniciar sessão e entrar nas reuniões de forma segura a partir da Internet sem uma conexão VPN.

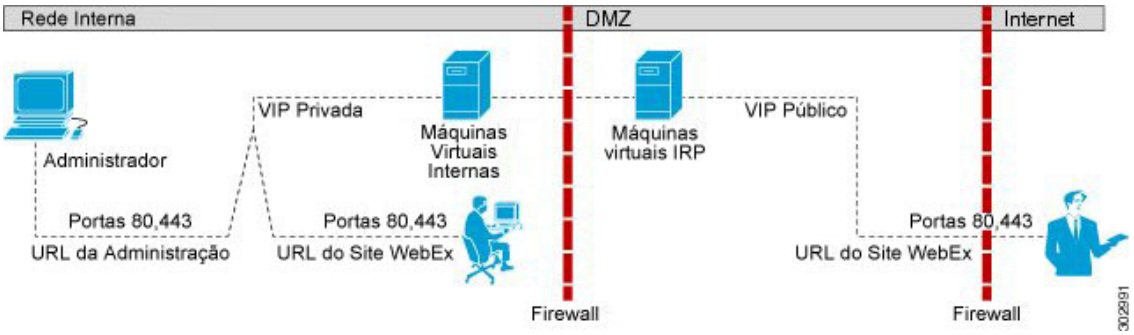
Observação Esta configuração pode suportar apenas acessos móveis a partir de uma rede IP pública (internet). O acesso móvel não é suportado em uma rede interna (intranet).

Em uma implantação split-horizon, o tráfego de origem da Internet (incluindo os usuários móveis que empregam uma rede de dados de celular) vai para o proxy reverso da Internet. O tráfego de origem interna (incluindo usuários móveis que empregam Wi-Fi local) vai diretamente para as máquinas virtuais internas.

Para este produto, a principal diferença entre uma topologia de rede split-horizon e uma sem split-horizon é que para um sistema split-horizon, os usuários internos acessam a URL do site WebEx usando o endereço VIP privado. Os usuários externos (fora do firewall) acessam a URL do site WebEx usando o endereço VIP público. Para uma rede sem split-horizon, todos os usuários (internos e externos) acessam a URL do site WebEx usando o endereço VIP público.

Você irá definir a URL da Administração, a URL do site WebEx, o endereço VIP privado e o endereço VIP público durante a implantação do sistema. Para obter mais informações sobre estes termos, e quando fornecê-los, consulte a seção de instalação do *Guia de Administração do Cisco WebEx Meetings Server*.

Este é um esquema de diagrama de uma topologia de rede split-horizon.



Observação Para obter uma lista completa das portas de acesso necessárias para essa implantação, consulte Porta de acesso com um proxy reverso da Internet na rede DMZ, na página 88.

Vantagens de uma Topologia de Rede Split-Horizon

- Controle apertado sobre o tráfego que entra e sai de uma rede.
- Existe uma separação de tráfego de rede, carregando o sistema e permitindo uma maior distribuição da carga.

  O tráfego de entrada da Internet irá para o Proxy Reverso da Internet. O tráfego interno (rede privada) irá diretamente para as máquinas virtuais internas (Admin e, se aplicável, mídia e Web).
- O desempenho e a latência de rede são melhores em relação à DNS non-split-horizon, mas piores do que toda a topologia de rede interna.

Desvantagens de uma Topologia de Rede Split-Horizon

- Das três topologias de rede diferentes, essa é a que apresenta uma configuração mais complexa.
- Requer mapeamento sofisticado de DNS.

- Requer mais portas a serem abertas no firewall entre a rede interna e DMZ do que toda a topologia de rede interna.
- A implantação automática do sistema (apenas sistemas para 50, 250 ou 800 usuários simultâneos) requer uma configuração mais detalhada no vCenter.
- Devido ao redirecionamento da Web para usuários internos, a URL do site WebEx é substituída pela URL do hostname da máquina virtual, que contém os serviços Web, bem como as máquinas virtuais de mídia.

Consulte a Requisitos da Largura de Banda de Rede, na página 56 para obter detalhes sobre os requisitos de velocidade NIC para implantações DNS split-horizon.

Redundância nas implantações HA ou MDC

Alta Disponibilidade (HA) fornece redundância através do failover de um sistema defeituoso primário do Cisco WebEx Meetings Server (CWMS) para um sistema HA do CWMS de backup no mesmo local físico.

(MDC) do CWMS implementam e depois os unem em um único sistema CWMS. O failover é semelhante a um sistema HA, exceto que os centros de dados do sistema MDC são pares para ambos os usuários que atendem e não são geograficamente limitados. Na verdade, a implantação de geograficamente próximos aos usuários melhora o desempenho da rede. Um sistema CWMS não pode suportar a HA e o MDC.

As condições para a redundância são:

- As máquinas virtuais HA devem ser co-localizadas no mesmo centro de dados que as máquinas virtuais primárias. Todas essas máquinas virtuais devem estar na mesma VLAN ou sub-rede. Os requisitos de velocidade e latência para conectividade entre os componentes primários e de HA são os mesmos conforme definidos anteriormente para as máquinas virtuais primárias. Dividir os componentes primários e HA do sistema entre os centros de dados não é suportado.

  As máquinas virtuais MDC não precisam ser colocalizadas no mesmo centro de dados.
- A conectividade entre todas as máquinas virtuais internas deve ser completamente redundante, de modo que a falha de um link de rede ou comutação não irá romper a conectividade entre os componentes primários e HA ou MDC. Para alcançar esta redundância, cada servidor organizador deve ter conexões redundantes para vários comutadores Ethernet.
- As máquinas virtuais primárias e HA de proxy reverso da internet (IRP) devem estar em uma mesma VLAN ou sub-rede (normalmente não na mesma sub-rede que as máquinas virtuais internas). A conectividade entre as máquinas virtuais de proxy reverso da internet deve ser totalmente redundante, da mesma maneira que as máquinas virtuais internas.

  Depois de entrar nos centros de dados em um sistema MDC, o IRP pode ser ativado ou desativado nos centros de dados. A configuração IRP de todo o centro de dados no sistema CWMS MDC deve corresponder; não pode haver uma incompatibilidade.

A adição de um sistema HA ou MDC não aumenta a capacidade total do sistema. Se você implantar um sistema de 800 usuários com ou sem o HA, a capacidade total do sistema permanece o mesma, o número máximo de conexões simultâneas de áudio é de 800.

O sistema HA ou MDC compreende máquinas virtuais redundantes para cada tipo de máquina virtual em sua implantação. (Para uma descrição de cada tipo de máquina virtual, consulte Máquinas Virtuais em seu sistema, na página 9.) Por exemplo:

- Um sistema de 50 usuários consiste em uma máquina virtual de administração e, opcionalmente, uma máquina virtual de Proxy Reverso da Internet (IRP) para acesso público. Se você adicionar um sistema HA (MDC não está disponível), o sistema combinado de 50 usuários compreende duas máquinas virtuais de administração e duas máquinas virtuais IRP.
- Um sistema primário de 250 ou 800 usuários consiste em uma máquina virtual de administração, uma máquina virtual de Mídia e, opcionalmente, uma máquina virtual IRP. Se você adicionar um sistema HA ou MDC, o sistema combinado de 250 ou 800 usuários compreende duas máquinas virtuais de administração, duas máquinas virtuais de mídia e duas máquinas virtuais IRP.
- Um sistema primário de 2000 usuários consiste em uma máquina virtual de administração, três máquinas virtuais de Mídia, duas máquinas virtuais da Web e, opcionalmente, uma máquina virtual IRP. Se você adicionar um sistema HA ou MDC, o sistema combinado de 2000 usuários compreende duas máquinas virtuais de administração, quatro (três mais uma redundante) máquinas virtuais de mídia, três (duas mais uma redundante) máquinas virtuais da web e duas máquinas virtuais IRP.

Em um sistema HA ou MDC, o endereço VIP público e o endereço VIP privado são compartilhados com o sistema primário. (O endereço VIP público e o endereço VIP privado são diferentes e não são compartilhados.) Quando uma máquina virtual está desligada, a outra máquina virtual usa o mesmo endereço VIP. Devido a este comportamento, uma falha da máquina virtual é transparente para os usuários enquanto as reuniões continuam sem colocar demandas incomuns na infraestrutura de DNS. No entanto, um endereço VIP compartilhado só pode ser implantado em um único segmento de rede ou VLAN; dividir uma VLAN por dois centros de dados cria muitos problemas.

Requeremos que a conectividade entre as máquinas virtuais internas primária e HA esteja dentro do mesmo centro de dados, reduzindo o problema de distinguir entre uma falha da máquina virtual e uma falha da rede. Permitir uma divisão de rede pode resultar em divisão de conexões de reuniões e atualizações conflitantes do banco de dados. É mais prático construir um segmento de rede HA verdadeiro dentro de um único centro de dados do que entre .

Em um sistema MDC, os dados são replicados nos centros de dados (exceto para o Gerenciador de Licenças). Portanto, se um centro de dados falhar ou a conectividade da rede for perdida, o centro de dados sobrevivente continua a servir os usuários, independentemente da localização geográfica.

A melhor maneira de construir um sistema tolerante a falhas é quando a maioria dos componentes do sistema operam como "todos ativos". No entanto, alguns componentes essenciais, especialmente os serviços de banco de dados, são "ativo/modo de espera". (Os servidores da web e os componentes de mídia no sistema de HA dependem dos componentes do sistema primário. Qualquer interrupção ou latência nas conexões resulta em atrasos para os usuários, especialmente ao entrarem em reuniões. A latência entre os componentes de serviços de mídia aumenta a latência de áudio e vídeo para alguns usuários durante as reuniões. (Para o Cisco WebEx Meetings Server, 1 ms de latência de rede é aceitável entre as máquinas virtuais internas. Para obter mais detalhes, consulte Layout da Máquina Virtual em sua Rede, na página 47).

Considerações de Rede para o Proxy Reverso da Internet

As máquinas virtuais do Proxy Reverso da Internet compartilham os mesmos requisitos gerais de rede, em relação às máquinas virtuais internas. Para as configurações de DNS non-split-horizon e split-horizon, as máquinas virtuais do Proxy Reverso da Internet são implantadas em sua rede DMZ e não na rede interna.

Restrição Mesmo que os Servidores UCS da Cisco sejam configurados com dois NICs, o Cisco WebEx Meetings Server não suporta apontar um NIC para a Internet e o outro NIC para a Intranet. Esta restrição se aplica independentemente dos mapeamentos entre os NICs físicos e os NICs virtuais usados pelo vSphere (e o proxy reverso da Internet).

A máquina virtual de proxy reverso da Internet sempre se conecta a uma única VLAN externa, independentemente do número ou NICs que você utiliza. Se você utilizar vários NICs físicos e eles estiverem conectados a diferentes comutadores ou roteadores, os NICs ainda devem estar conectados à mesma VLAN.

Portanto, você não pode usar o proxy reverso da Internet para colmatar o tráfego entre dois segmentos de rede separados (com um apontando para a Internet e o outro apontando para a Intranet). A próxima seção descreve como você pode atingir este objetivo.

Latência entre as Máquinas Virtuais Internas e o Proxy Reverso da Internet

A latência máxima aceitável no caminho de ida e volta entre o NIC no proxy reverso da Internet e o NIC em quaisquer das máquinas virtuais internas deve ser estabelecida em menos de 4 ms. O excesso de latência neste caminho irá limitar a largura de banda que pode ser usada por usuários finais para áudio, vídeo, e o compartilhamento de desktop. Se a latência aumenta de 4 ms para 8 ms, por exemplo, a largura de banda utilizável irá cair pela metade, com a experiência se degradando progressivamente com o aumento da latência.

Observação O limite de 4 ms de latência não se aplica para o caminho entre quaisquer componentes do Cisco WebEx Meetings Server e as extremidades dos usuários finais.

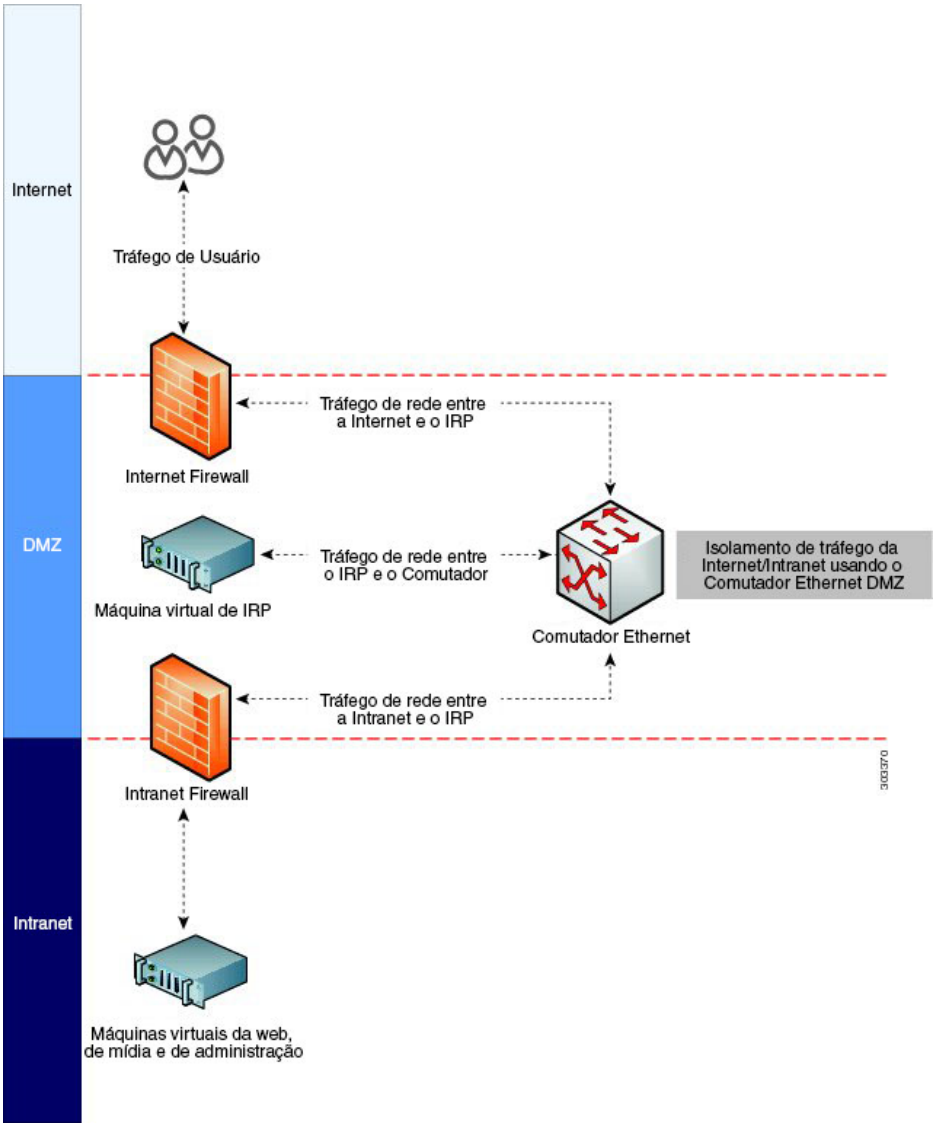
Observação Potenciais graves atrasos em conexões do usuário final que passam pelo proxy reverso da Internet no Cisco WebEx Meetings Server podem acontecer quando a latência exceder os 4 ms entre o IRP e as máquinas virtuais internas.

Isolamento do Tráfego de Rede

Você pode configurar o isolamento do tráfego de rede entre a Internet e sua rede interna, usando um comutador Ethernet DMZ. O diagrama e o procedimento a seguir ilustram um exemplo:

1. Conecte o proxy reverso da Internet a um comutador de processamento ou roteador e use esse comutador ou roteador para dividir a o tráfego da Intranet e da Internet.
2. Uma vez que o comutador ou o roteador dividir o tráfego, você poderá então canalizar esses dois padrões de tráfego a duas portas físicas separadas do comutador ou do roteador. Uma porta aponta para a Internet e a outra porta aponta para a Intranet.

Aqui está um diagrama de um exemplo de topologia de rede:



Para obter informações sobre os requisitos de largura de banda de rede, consulte Requisitos da Largura de Banda de Rede, na página 56.

Requisitos da Largura de Banda de Rede

Esta seção descreve os requisitos da largura de banda para sistemas de 50, 250, 800 e 2000 usuários. Cumprir os requisitos da largura de banda descritos na seção irá fornecer uma qualidade de experiência do usuário final para os usuários que organizam e participam de reuniões WebEx, e ajudará a garantir que a sua rede poderá suportar as demandas de tráfego a partir do compartilhamento de vídeo, de áudio e da web.

Estimativa de Largura de Banda para Sessões do Usuário Final

É importante estimar a largura de banda de rede para suportar as demandas de tráfego do compartilhamento de vídeo, de áudio e da web para o tamanho do sistema do usuário. Os requisitos da banda larga para este

produto são fundamentalmente os mesmos que para os serviços de nuvem do Cisco WebEx. Se você deseja otimizar seus provisionamento de rede, o uso de largura de banda de serviços de nuvem do Cisco WebEx é apresentado no Documento de Largura de Banda de Rede WebEx.

As informações contidas na tabela a seguir mostram a largura de banda esperada para compartilhamento de web, áudio e vídeo.

Componente do WebEx Meeting	Agregar Largura de Banda da Sessão do Usuário Final
Vídeo (360p + 6 miniaturas)	1,5 Mb/s
Áudio	0,1 Mb/s
Compartilhamento Web (Este valor assume que você vira um slide a cada 30 segundos.)	0,6 Mb/s
Total máximo de largura de banda	2,2 Mb/s

Apesar de 2,2 Mb/s ser a largura de banda máxima esperada para uma conexão de um único usuário, a Cisco recomenda o uso da largura de banda máxima esperada de 1,5 Mb/s ao calcular os requisitos da largura de banda. Como apenas metade do número máximo de usuários pode empregar o compartilhamento de vídeo, de áudio e da web, enquanto os demais usuários devem usar apenas o compartilhamento de áudio e da web, este produz uma largura de banda média de cerca de 1,5 Mb/s por conexão de usuário.

Se você consultar o*Documento de Largura de Banda de Rede WebEx*, você irá notar que os valores da largura de banda na tabela anterior são baseados nas condições dos piores casos de tráfego. A utilização da largura de banda média é *muito* menor, mas a Cisco recomenda o uso dos números dos piores casos, pelas seguintes razões:

- Usando os números dos piores casos para o seu cálculo deverá ajudá-lo a fornecer a largura de banda necessária para evitar uma experiência de usuário degradada como resultado de uso pesado.
- O Cisco WebEx Meetings Server envia os mesmos dados simultaneamente para todos os participantes em uma reunião. Quando um organizador WebEx vira uma página em uma apresentação, uma imagem daquela página (possivelmente compreendendo vários megabytes) é enviada separadamente para cada extremidade, ao mesmo tempo, e tão rapidamente quanto possível.

Largura de Banda nos Caminhos de Rede

Use o seguinte processo para determinar a largura de banda necessária nos diversos caminhos de rede.

1. Determine a largura de banda média para uma sessão de usuário usando a tabela fornecida na seção anterior.
2. Determine o número máximo de usuários que você espera conectar simultaneamente nesse link.
3. Multiplique a largura de banda total pelo número máximo de usuários.

Exemplos de cenários:

- Se você espera um máximo de 100 usuários para se conectar simultaneamente a partir da Internet, você provavelmente precisará de 1,5 Mb/s x 100 = 150 Mb/s de largura de banda disponível na sua conexão ISP e através do firewall externo para o proxy reverso da Internet. Para obter mais detalhes sobre o Proxy Reverso da Internet, consulte Considerações de Rede para o Proxy Reverso da Internet, na página 54

- Suponha que você tenha um sistema de 2000 usuários, com todas as conexões passando pelo proxy reverso da Internet. Neste cenário, você precisa assumir que o tráfego para todos os 2000 usuários irá se conectar ao proxy reverso da Internet e depois do proxy reverso da Internet para as máquinas virtuais internas. A largura de banda agregada entrando no proxy reverso da Internet a partir de outras partes da rede será 2000 x 1,5 Mb/s = 3 Gb/s. Para obter mais detalhes sobre o sem split horizon, consulte Topologia de Rede Sem Split-Horizon, na página 49.

Observação O mesmo 3 Gb/s de tráfego passa da entrada e saída através do proxy reverso da Internet, exigindo que o NIC no proxy reverso da Internet lide com 6 Gb/s de tráfego de usuário. Consulte a próxima seção para obter mais informações sobre os requisitos de largura de banda para o NIC no proxy reverso da Internet.

- Suponha que você tenha um sistema de 2000 usuários em uma implantação de DNS split horizon. Neste cenário, os usuários da Internet ligarão para o proxy reverso Internet, enquanto os usuários da intranet ligarão diretamente para as máquinas internas virtuais. Suponha que 10 por cento dos seus usuários se conectam a uma reunião usando a Internet versus 90 por cento dos usuários que se conectam a suas reuniões através da Intranet. O resultado é que a largura de banda agregada entrando no proxy reverso da Internet passará a ser de cerca de 300 Mb/s (10 por cento dos 2000 usuários vezes 1,5 Mb/s é igual a 300 Mb/s). Se esses mesmos 300 Mb/s de tráfego passar do proxy reverso da Internet, o NIC no proxy reverso da Internet pode ser necessário para lidar com 600 Mb/s de tráfego de usuário. Esta é uma exigência da largura de banda drasticamente menor do que com a implantação de DNS sem split-horizon descrita no cenário anterior. A redução no tráfego de rede tem relação direta com as recomendações para o NIC ou com a velocidade da interface do comutador (consulte a próxima seção), que pode possibilitar que você implemente NICs de 1 Gb/s mais baratos no Servidor UCS da Cisco para o proxy reverso da Internet ou para a Infraestrutura do Comutador Ethernet de 1 Gigabite na rede DMZ. Para obter mais detalhes sobre o split horizon, consulte Topologia de Rede Split-Horizon, na página 51.

Observação Você pode ser obrigado a implantar NICs Ethernet de 1 Gigabite configurados para o NIC Teaming se o uso do proxy reverso da internet estiver ligeiramente próximo do limite de 1000 Mb/s.

Consulte NIC Teaming para Agregação de Largura de Banda, na página 61 para obter mais detalhes.

Largura de Banda em Interfaces de Rede do Cisco WebEx Meetings Server

Para interfaces diretas entre sua arquitetura de comutação e seu sistema, recomendamos o provisionamento dos NICs da interface para as velocidades máximas indicadas na tabela a seguir. Estas velocidades se aplicam à conectividade entre os Servidores UCS da Cisco e as portas nos comutadores de processamento na sua infraestrutura de comutação local. Estas são as velocidades recomendadas necessárias para suportar os requisitos dos piores casos de tráfego.

Capacidade do sistema	Velocidade da Interface do Comutador ou do NIC
sistema de 50 usuários	1 Gb/s
sistema de 250 usuários	1 Gb/s
sistema de 800 usuários	10 Gb/s[1819]

Capacidade do sistema	Velocidade da Interface do Comutador ou do NIC
sistema de 2000 usuários	10 Gb/s[20]

18 Como opção, você pode optar por reduzir os custos de infraestrutura de rede com a implantação do NIC Teaming usando dois ou mais NICs Ethernet de Gigabite no servidor UCS e no NIC Teaming no comutador de processamento.

19 Para sistemas de 800 usuários, se a sua implantação está utilizando armazenamento DAS interno, você pode opcionalmente optar por reduzir os custos de infraestrutura de rede com a implantação NIC Teaming utilizando duas ou mais NICs Ethernet de Gigabite no Servidor UCS e NIC Teaming no comutador de processamento. No entanto, se a sua implantação está utilizando armazenamento SAN ou NAS, você precisará de um link Ethernet de 10 Gigabites.

20 Se você tem uma implantação de DNS sem split-horizon, o requisito de 10 Gb/s pertence ao IRP e as máquinas virtuais internas. Se você tem uma implantação de DNS split-horizon, você pode reduzir as demandas da infraestrutura de rede em seu IRP (e rede DMZ), o que pode resultar em você ser capaz de implantar NICs de 1 Gb/s mais baratos no Servidor UCS da Cisco para o proxy reverso da Internet ou Infraestrutura de Comutador Ethernet de 1 Gigabite na rede DMZ, como descrito na seção "Largura de Banda nos Caminhos de Rede". No entanto, o requisito de velocidade de 10 Gb/s é válido para as máquinas virtuais internas (e rede interna).

Consulte a seguinte seção "Considerações sobre largura de banda para implantações DNS split-horizon" para obter mais informações sobre o uso de NICSs de 1 Gb/s e comutadores Ethernet para uma implantação de DNS split-horizon.

Pressupostos para cálculos de velocidade NIC:

- A largura de banda agregada da sessão do usuário final (1,5 Mb/s) foi utilizada para calcular as velocidades de NIC mostradas na tabela anterior.
- O tráfego de controle da máquina virtual interna deve estar livre de congestionamento. Isso se aplica especialmente para sistemas de 2000 usuários e qualquer sistema provisionado para alta disponibilidade. O congestionamento grave em links de máquinas virtuais pode resultar em instabilidade do sistema e consequênte interrupção do serviço.
- As conexões para armazenamento NAS, utilizadas para backup de gravação e banco de dados, não devem estar congestionadas.
- As ineficiências da implementação e os protocolos gerais resultam na largura de banda do link utilizável que é significativamente menor do que os registros de velocidade de 1 Gb/s ou 10 Gb/s.
- Se uma grande porcentagem do tráfego atingir o proxy reverso da Internet quando os usuários iniciarem sessão nas reuniões, é preciso lembrar que cada conexão do usuário passa duas vezes através do NIC no proxy reverso da Internet (entrada e saída). Usando o sistema de 2.000 usuários como um exemplo, isso significa que o NIC no Proxy Reverso da Internet pode ser necessário para lidar com 6 Gb/s de tráfego de usuário (2.000 usuários vezes 1,5 Mb/s é igual a 3 Gb/s, vezes dois para tráfego de entrada e saída é igual a 6 Gb/s).

Conservadoramente, pedimos que as conexões locais não sejam mais de 60 por cento utilizadas para o tráfego de mídia do usuário final, permitindo que os 40 por cento restantes estejam disponíveis para outro tráfego, rajadas de tráfego incomuns e sobrecarga da rede. Usando o sistema de 800 usuários como exemplo, estimamos o tráfego do usuário final em 1,2 Gb/s para as máquinas virtuais de mídia e administração e 2,4 Gb/s para a máquina virtual de proxy reverso da internet. Aplicando a regra dos 60 por cento, queremos que o NIC seja capaz de lidar com 2 Gb/s para as máquinas virtuais de Mídia e de Administração (tráfego de usuários estimado em 1,2 Gb/s para as máquinas virtuais de Mídia e de Administração dividido por 60 por cento do consumo de largura de banda estimada normal igual a 2,0 Gb/s) e 4 Gb/s para a máquina virtual de Proxy Reverso da Internet.

Observação As velocidades NIC mostradas na tabela anterior não contam para a largura de banda utilizada para acessar o armazenamento SAN. Se a Fibre Channel sobre o Ethernet (FCoE) é usada para uma conexão de SAN, ela deve ser provisionada para usar uma interface de rede independente.

Considerações sobre Largura de Banda para Implantações DNS Split-Horizon

Com uma implantação de DNS split-horizon, alguns de seus usuários irão iniciar sessão em reuniões a partir da Internet e aquele tráfego atingirá o proxy reverso da Internet, enquanto que a maioria dos usuários que estão na rede interna irão iniciar sessão em reuniões sem atingir o proxy reverso da Internet. Com uma implantação de DNS split-horizon, se você acelerar a rede e dividir o tráfego para que a maioria do tráfego permaneça dentro da rede interna (em oposição a atingir o proxy reverso da Internet), você pode potencialmente usar o NIC Teaming e provisionar um NIC de menor efeito (NIC de 1 Gb/s) no Proxy reverso da Internet e provisionar a infraestrutura de comutação entre o proxy reverso da Internet e a Internet para serem 1 Gb/s ou pelo menos menor do que o recomendado de 10 Gb/s, para um sistema de 2000 usuários.

Por exemplo, se uma empresa tem 100 usuários que querem acessar um sistema de porta de 2000 usuários da Internet ao mesmo tempo, você precisaria de uma largura de banda de 150 Mb/s (1,5 Mb/s de largura de banda de sessão de usuário agregada * 100 usuários = 150 Mb/s). Isto implica que uma infraestrutura de rede da rede DMZ para o proxy reverso da Internet pode ser de comutadores Ethernet de 1 Gb/s, e a interface de rede Ethernet no proxy reverso da Internet pode ser de 1 Gb/s, ao contrário do requisito da interface declarada de 10 Gb/s. Mesmo quando você leva em conta que o proxy reverso da Internet vê o dobro do tráfego (ou seja, sua NIC teria que lidar com 300 Mb/s de tráfego de usuários), aplicando a regra de 60 por cento (explicado na seção "Largura de banda das interfaces de rede do Cisco WebEx Meetings Server") se traduz a 500 Mb/s. Um link de 1 Gb/s ainda é suficiente, mas não seria suficiente se assumíssemos 250 usuários, em vez de 100 usuários.

Observação A otimização da largura de banda é aplicável apenas para o NIC no proxy reverso da Internet em implantações DNS split-horizon.

Para implantações DNS sem split-horizon, você deve implantar comutadores Ethernet de 10 Gb/s e interfaces NIC Ethernet no proxy reverso da Internet.

Requisitos de rede para vários centros de dados

Requisitos para um link de rede entre dois centros de dados:

- Largura de banda garantida de 4,5 Mbps para comunicações essenciais entre centros de dados.
- Menos de 200 ms de latência (atraso de tempo de ida e volta).

Requisitos de rede do centro de dados para reuniões em cascata entre centros de dados:

- Cada reunião em cascata com áudio e Web requer 0,16 Mbps.
- Cada reunião em cascata com vídeo LQ em 180p, áudio e Web requer 0,66 Mbps.
- Cada reunião em cascata com vídeo HQ em 360p, áudio e Web requer 1,20 Mbps.
- Menos de 200 ms de latência (atraso de tempo de ida e volta).

Por exemplo, o pior caso de um sistema de 2000 usuários (número máximo de 1000 reuniões são em cascata. Metade delas pode ter vídeo e metade não:

- *Vídeo HQ :* 500 x 1,2 + 500 x 0,16 = 680 Mbps
- *Vídeo LQ:* 500 x 0,66 + 500 x 0,16 = 410 Mbps

Para um sistema de 800 usuários:

- *Vídeo de alta qualidade:* 680 / 2000 x 800 = 272 Mbps
- *Vídeo LQ:* 410 / 2000 x 800 = 164 Mbps

Para um sistema de 250 usuários:

- *Vídeo de alta qualidade:* 680 / 2000 x 250 = 85 Mbps
- *Vídeo LQ:* 410 / 2000 x 250 = 51,25 Mbps

Informações adicionais podem ser encontradas em http://www.cisco.com/c/en/us/products/conferencing/webex-meeting-center/white-paper-listing.html.

NIC Teaming para Agregação de Largura de Banda

Configurar o NIC Teaming em seus servidores UCS que contêm o organizador ESXi com as máquinas virtuais internas oferece duas vantagens: O carregamento NIC Teaming equilibra o tráfego de rede entre as redes físicas e virtuais e fornece failover em caso de uma falha de hardware ou uma queda de rede. Além disso, para implementações onde a infraestrutura de 10 Gb/s não está disponível, pode ser possível para você juntar múltiplas NICs de 1 Gb/s para alcançar um resultado equivalente.

Observação Para obter mais informações sobre as velocidades NIC necessárias para sistemas de usuários de diferentes tamanhos, consulte a seção "Largura de Banda nas Interfaces de Rede do Cisco WebEx Meetings Server" neste capítulo.

A Cisco suporta o NIC Teaming para balanceamento de carga da largura de banda para todos os tamanhos de sistemas de usuários--sistemas de 50, 250, 800 e 2000 usuários - mas é mais útil para os clientes que estão tentando otimizar custos de rede para um sistema de 800 usuários. Se a sua implantação estiver usando um armazenamento DAS interno, os requisitos da largura de banda agregada para e dos Servidores UCS da Cisco e os comutadores de processamento para um sistema de 800 usuários são projetados para serem semelhantes ao uso dos NICs Ethernet Dual de 1 Gigabites (ou NICs Ethernet Quad de 1 Gigabites em um sistema com HA) para suportar requisitos de tráfego nos piores casos, aliviando assim a necessidade de provisionar os Servidores UCS com NICs Ethernet de 10 Gigabites (ou comutadores central de distribuição Ethernet de 10 Gigabite).

Observação Se a implantação estiver utilizando armazenamento SAN ou NAS, os requisitos de largura de banda agregada para e dos Servidores UCS da Cisco e os comutadores de processamento para um sistema de 800 usuários será de Ethernet de 10 Gigabites.

Observação Para obter informações sobre a configuração do NIC teaming no VMware, consulte a documentação do VMware em http://kb.vmware.com e procure por "NIC teaming no ESXi/ESX".

Considerando o uso de interfaces de rede tradicionais e comutadores Ethernet, você pode fornecer redundância usando o NIC teaming e comutadores duplicados, conforme descrito no seguinte processo:

- Configure um comutador Ethernet que suporta IEEE 802.3ad/IEEE 802.1ax Link Aggregation Control Protocol (LACP).
- Usando o vCenter, conecte o grupo de porta da máquina virtual associada com as máquinas virtuais do Cisco WebEx Meetings Server para ambos os adaptadores físicos.
- Conecte ambos os adaptadores físicos para o comutador.
- Provisionar o comutador para estaticamente provisionar as duas portas como uma equipe.
- Ao usar o VMware vSphere, defina o NIC Teaming para Ativo/Ativo para permitir o rendimento em ambas as interfaces NIC.

Por exemplo, para uma implantação de 800 usuários, dois links de 1 Gb/s podem ser substituídos por cada link de 10 Gb/s no organizador ESXi com as máquinas virtuais internas, e quatro links de 1 Gb/s podem ser substituídos por cada link de 10 Gb/s no Proxy Reverso da Internet. (Para obter tolerância a falhas em um sistema com HA, como descrito na seção "Conexões de Rede Redundantes para Implantações HA", é necessário dobrar o número de links). Com o organizador ESXi com as máquinas virtuais internas, conecte dois links de 1 Gb/s para o primeiro comutador Ethernet *mais* dois links de 1 Gb/s para o segundo comutador Ethernet.

Observação Os exemplos de configurações de servidores mostrados nos *Requisitos do Sistema do Cisco WebEx Meetings Server* não incluem interfaces de rede suficientes para suportar o NIC Teaming para esta finalidade.

Balanceamento de carga

O balanceamento de carga é sempre feito no CWMS, não importa o tipo de tráfego que está sendo tratado e não é configurável.

O sistema tenta balancear a carga igualmente em todos os nós da web. Quando a implantação é um sistema sem Alta Disponibilidade (HA), as conexões são balanceadas entre todos os nós da web nesse sistema. No caso de uma implantação HA, o sistema utiliza os nós da web tanto no sistema primário como no sistema HA para balanceamento de carga. No caso da falha de um, mas não de todos os nós da web, o sistema permanece ativo, mas a capacidade é reduzida.

O nó do Proxy reverso da internet (IRP) é um ponto de entrada e a maioria das decisões de balanceamento de carga são feitas lá. Apenas um nó IRP está ativo em um sistema. Um sistema sem implantação HA tem apenas um nó IRP. Um sistema com a implantação HA tem dois nós IRP, um IRP está ativo, enquanto o outro está inativo. Dependendo da configuração do DNS, o IRP servirá todo o tráfego externo (e todo o tráfego interno em caso de DNS sem split).

Se houver uma falha envolvendo vários organizadores, a funcionalidade e a capacidade podem ser afetadas.

CAPÍTULO 4

Lista de verificação de rede para o sistema

A lista de verificação de rede lista as alterações de rede necessárias para seu sistema, dependendo da configuração DNS e se você habilita ou não o acesso público (usuários podem organizar ou participar de reuniões na Internet ou por meio de um dispositivo móvel).

Escolha a lista de verificação apropriada, dependendo se você está usando a implantação automática do sistema (recomendado para 50, 250 ou 800 implantações de usuário) ou a implantação manual do sistema (exigido para 2.000 implantações de usuário).

- Todas as máquinas virtuais, incluindo o Proxy Reverso da Internet, estão na sua rede interna (configuração mais fácil)
  - O checklist da Rede para uma Instalação ou Expansão com uma Implantação Automática e Acesso Público, na página 64
  - O checklist da rede para uma instalação ou expansão com uma implantação manual, acesso público e todas as máquinas virtuais internas, na página 67
- DNS sem split-horizon (a configuração de DNS mais comum)
  - O checklist da rede para uma instalação ou expansão com uma implantação automática, acesso público e um DNS sem split-horizon, na página 70
  - O checklist da rede para uma instalação ou expansão com uma implantação manual, acesso público e um DNS sem split horizon, na página 72
- DNS Split-horizon
  - O checklist da rede para uma instalação ou expansão com uma implantação automática, acesso público e um DNS split-horizon, na página 75
  - O checklist da rede para uma instalação ou expansão com uma implantação manual, acesso público e um DNS split-horizon, na página 78
- Sistema sem acesso público
  - O checklist da Rede para uma Instalação ou Expansão com Implementação Automática e Nenhum Acesso Público, na página 81
  - Checklist de Rede Para uma Instalação ou Expansão Com Implementação Manual e Acesso Não Público, na página 83

- O checklist da Rede para uma Instalação ou Expansão com uma Implantação Automática e Acesso Público, página 64
- O checklist da rede para uma instalação ou expansão com uma implantação manual, acesso público e todas as máquinas virtuais internas, página 67
- O checklist da rede para uma instalação ou expansão com uma implantação automática, acesso público e um DNS sem split-horizon, página 70
- O checklist da rede para uma instalação ou expansão com uma implantação manual, acesso público e um DNS sem split horizon, página 72
- O checklist da rede para uma instalação ou expansão com uma implantação automática, acesso público e um DNS split-horizon, página 75
- O checklist da rede para uma instalação ou expansão com uma implantação manual, acesso público e um DNS split-horizon, página 78
- O checklist da Rede para uma Instalação ou Expansão com Implementação Automática e Nenhum Acesso Público, página 81
- Checklist de Rede Para uma Instalação ou Expansão Com Implementação Manual e Acesso Não Público, página 83
- As URLs do Site WebEx e da Administração Webex, página 86
- Porta de acesso quando todas as máquinas virtuais estão na rede interna, página 87
- Porta de acesso com um proxy reverso da Internet na rede DMZ, página 88
- Portas VMware vCenter, página 93
- Portas do Cisco WebEx Meeting Center, página 94
- Usar NAT com seu sistema, página 94
- Projeções proxies, página 97

O checklist da Rede para uma Instalação ou Expansão com uma Implantação Automática e Acesso Público

Implementação de Máquina Virtual

Em uma implantação automática, implantamos todas as máquinas virtuais (que não seja a máquina virtual de Administração) para você. Recomendamos que você escolha uma implantação automática se você estiver implantando um sistema de 50, 250 ou 800 usuários.

- Certifique-se que a máquina virtual de mídia (se aplicável) está na mesma sub-rede da máquina virtual de administração.
- Garanta que as máquinas virtuais de Proxy Reverso da Internet estejam na sua rede interna.
- Certifique-se de que os organizadores ESXi para todas as máquinas virtuais (incluindo o Proxy Reverso da Internet) sejam gerenciados do mesmo VMware vCenter.

Endereços de IP necessários

Descrição	Local da rede	Endereço IP
Endereço de IP real da máquina virtual de administração	Interna	
Endereço de IP real da máquina virtual de mídia (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração)	
Endereço de IP real do proxy reverso da Internet	Interna (pode estar na mesma sub-rede que a máquina virtual de administração)	
URL da Administração (usada exclusivamente pelo sistema. Mapeia para o endereço VIP privado)	Interna (mesma sub-rede que a máquina virtual de administração)	
URL do site WebEx (usada exclusivamente pelo sistema. Mapeia para o endereço VIP público)	Interna (mesma sub-rede que o proxy reverso da internet). Este endereço de IP deve ser roteável ao público.	
Endereço de IP real da máquina virtual de administração de HA (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração do sistema primário)	
Endereço de IP real da máquina virtual de mídia de HA (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração do sistema primário)	
Endereço de IP real do proxy reverso da Internet de HA (se aplicável)	Interna [mesma sub-rede que o proxy reverso da Internet do sistema primário (mas pode usar a NAT com um endereço de IP privado)]	

CONFIGURAÇÃO DNS

Atualize o servidor DNS da seguinte forma. Existem algumas limitações quanto à parte do nome do organizador em relação à URL do site WebEx e a URL do site de Administração. Para obter uma lista das palavras que você não pode usar, consulte As URLs do Site WebEx e da Administração Webex, na página 86.

Tarefa	Exemplos
Nomes dos organizadores e endereços de IP das máquinas virtuais internas: A máquina virtual de Administração e se aplicável, a máquina virtual de mídia.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

Tarefa	Exemplos
Nome do organizador e endereço de IP para a máquina virtual de Proxy Reverso da Internet.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
URL do site de Administração e endereço VIP Privado.	• <Administration-site-URL> <Private-VIP-address>
URL do site WebEx e endereço VIP Público.	• <WebEx-site-URL> <Public-VIP-address>

CONFIGURAÇÃO FIREWALL

Por razões de segurança, recomendamos que você coloque o proxy reverso da Internet em uma sub-rede separada das máquinas virtuais internas (Administração ou mídia). Consulte Porta de acesso quando todas as máquinas virtuais estão na rede interna, na página 87.

Configuração de Roteamento da Rede

Tarefa	Exemplos
Habilite o roteamento Layer 3 entre as redes DMZ e interna.	• Sub-rede Interna <internal-subnet>/24 • Sub-rede DMZ <DMZ-subnet>/24
Verifique se o endereço VIP Público e as máquinas virtuais de Proxy Reverso da Internet estão na mesma sub-rede. [Como você está implantando todas as máquinas virtuais do sistema internamente (o proxy reverso da Internet não está na DMZ), esta sub-rede deve estar na rede interna.]	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Certifique-se que o endereço VIP Privado e as máquinas virtuais internas estejam na mesma sub-rede.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

O checklist da rede para uma instalação ou expansão com uma implantação manual, acesso público e todas as máquinas virtuais internas

Implementação de Máquina Virtual

Em uma implantação manual, você cria todas as máquinas virtuais para o seu sistema usando o assistente OVA do seu cliente vSphere. Você, então, instala o sistema usando uma implantação manual.

Você deve escolher uma implantação manual se você estiver implantando um sistema de usuário 2000.

- Verifique se todas as máquinas virtuais internas adicionais (Mídia e internet, se aplicável) estão na mesma sub-rede que a máquina virtual de administração.
- Garanta que as máquinas virtuais de Proxy Reverso da Internet estejam na sua rede interna.

Endereços de IP necessários

Descrição	Local da rede	Endereço IP
Endereço de IP real da máquina virtual de administração	Interna	
Endereço de IP real da máquina virtual de mídia (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração)	
Endereço de IP real da segunda máquina virtual de mídia (somente sistema de 2000 usuários)	Interna (mesma sub-rede que a máquina virtual de administração)	
Endereço de IP real da terceira máquina virtual de mídia (somente sistema de 2000 usuários)	Interna (mesma sub-rede que a máquina virtual de administração)	
Endereço de IP real da máquina virtual da web (somente sistema de 2000 usuários)	Interna (mesma sub-rede que a máquina virtual de administração)	
Endereço de IP real da segunda máquina virtual da web (somente sistema de 2000 usuários)	Interna (mesma sub-rede que a máquina virtual de administração)	
Endereço de IP real do proxy reverso da Internet	Interna (pode estar na mesma sub-rede que a máquina virtual de administração)	
URL da Administração (usada exclusivamente pelo sistema. Mapeia para o endereço VIP privado)	Interna (mesma sub-rede que a máquina virtual de administração)	

Descrição	Local da rede	Endereço IP
URL do site WebEx (usada exclusivamente pelo sistema. Mapeia para o endereço VIP público)	Interna (mesma sub-rede que o proxy reverso da internet) **Observação** Este endereço de IP deve ser roteável ao público.	
Endereço de IP real da máquina virtual de administração de HA (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração do sistema primário)	
Endereço de IP real da máquina virtual de mídia de HA (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração do sistema primário)	
Endereço de IP real da máquina virtual da web de HA (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração do sistema primário)	
Endereço de IP real do proxy reverso da Internet de HA (se aplicável)	Interna—mesma sub-rede que o proxy reverso da Internet do sistema primário (mas pode usar a NAT com um endereço de IP privado)	

CONFIGURAÇÃO DNS

Faça as seguintes alterações em sua configuração DNS.

Observação Existem algumas limitações quanto à parte do nome do organizador em relação à URL do site WebEx e a URL do site de Administração. Para obter uma lista das palavras que você não pode usar, consulte As URLs do Site WebEx e da Administração Webex, na página 86.

Tarefa	Exemplo
Atualize o seu Servidor DNS com os nomes dos organizadores e o endereço de IP das máquinas virtuais internas: A máquina virtual de Administração e se aplicável, as máquinas virtuais de mídia e da internet.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

Tarefa	Exemplo
Atualize o seu servidor DNS com os nomes dos organizadores e o endereço de IP das máquinas virtuais do proxy reverso da internet.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Atualize o seu servidor DNS com a URL do site de Administração informações do endereço VIP Privado.	• <Administration-site-URL> <Private-VIP-address>
Atualize o seu servidor DNS com a URL do site WebEx e as informações do endereço VIP Público.	• <WebEx-site-URL> <Public-VIP-address>

CONFIGURAÇÃO FIREWALL

Por razões de segurança, a Cisco recomenda que você coloque o proxy reverso da Internet em uma sub-rede separada das máquinas virtuais internas (Administração, mídia e internet, se for o caso).

Embora não seja recomendado, nós também apoiamos colocar todas as suas máquinas virtuais (Proxy reverso da internet e interna) na mesma sub-rede. Consulte Porta de acesso quando todas as máquinas virtuais estão na rede interna, na página 87.

Configuração de Roteamento da Rede

Faça as seguintes alterações em seu roteamento de rede.

Tarefa	Compare Estes Endereços de IP
Habilitar o roteamento L3 (Layer 3) entre as redes DMZ e interna para as seguintes máquinas virtuais: A máquina virtual de Administração e se aplicável, as máquinas de mídia e virtuais da internet	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Verifique se o endereço VIP Público e as máquinas virtuais de Proxy Reverso da Internet estão na mesma sub-rede. **Observação** Como você está implantando todas as máquinas virtuais do sistema internamente (o proxy reverso da Internet não está na DMZ), então esta sub-rede deve estar na rede interna.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>

Tarefa	Compare Estes Endereços de IP
Verifique se o endereço VIP Privado e as máquinas virtuais internas (Administração, mídia e internet, se aplicável) estão na mesma sub-rede.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

O checklist da rede para uma instalação ou expansão com uma implantação automática, acesso público e um DNS sem split-horizon

Implementação de Máquina Virtual

Em uma implantação automática, implantamos todas as máquinas virtuais (que não seja a máquina virtual de Administração) para você. Recomendamos que você escolha uma implantação automática se você estiver implantando um sistema de 50, 250 ou 800 usuários.

- Certifique-se que a máquina virtual de mídia (se aplicável) está na mesma sub-rede da máquina virtual de administração.
- Garanta que as máquinas virtuais de Proxy Reverso da Internet estejam na sua rede DMZ.

Endereços de IP necessários

Descrição	Local da rede	Endereço IP
Endereço de IP real da máquina virtual de administração	Interna	
Endereço de IP real da máquina virtual de mídia (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração)	
Endereço de IP real do proxy reverso da Internet	DMZ (mas pode usar a NAT com um endereço de IP privado)	
URL da Administração (usada exclusivamente pelo sistema. Mapeia para o endereço VIP privado)	Interna (mesma sub-rede que a máquina virtual de administração)	

Descrição	Local da rede	Endereço IP
URL do site WebEx (usada exclusivamente pelo sistema. Mapeia para o endereço VIP público)	DMZ (mesma sub-rede do proxy reverso da Internet)	
Endereço de IP real da máquina virtual de administração de HA (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração do sistema primário)	
Endereço de IP real da máquina virtual de mídia de HA (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração do sistema primário)	
Endereço de IP real do proxy reverso da Internet de HA (se aplicável)	DMZ [mesma sub-rede que o proxy reverso da Internet do sistema primário (mas pode usar a NAT com um endereço de IP privado)]	

CONFIGURAÇÃO DNS

Atualize o servidor DNS da seguinte forma. Existem algumas limitações quanto à parte do nome do organizador em relação à URL do site WebEx e a URL do site de Administração. Para obter uma lista das palavras que você não pode usar, consulte As URLs do Site WebEx e da Administração Webex, na página 86.

Tarefa	Exemplo
Nomes dos organizadores e endereços de IP das máquinas virtuais internas: A máquina virtual de Administração e se aplicável, a máquina virtual de mídia.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
Nome do organizador e endereço de IP para a máquina virtual de Proxy Reverso da Internet.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
URL do site de Administração e endereço VIP Privado.	• <Administration-site-URL> <Private-VIP-address>
URL do site WebEx e endereço VIP Público.	• <WebEx-site-URL> <Public-VIP-address>

CONFIGURAÇÃO FIREWALL

Por razões de segurança, recomendamos que você coloque o proxy reverso da Internet em uma sub-rede separada das máquinas virtuais internas (Administração ou mídia). Consulte Porta de acesso quando todas as máquinas virtuais estão na rede interna, na página 87.

Configuração de Roteamento da Rede

Faça as seguintes alterações em seu roteamento de rede.

Tarefa	Compare Estes Endereços de IP
Habilite o roteamento Layer 3 entre as redes DMZ e interna.	• Sub-rede Interna <internal-subnet>/24 • Sub-rede DMZ <DMZ-subnet>/24
Verifique se o endereço VIP Público e as máquinas virtuais de Proxy Reverso da Internet estão na mesma sub-rede.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Certifique-se que o endereço VIP Privado e as máquinas virtuais internas estejam na mesma sub-rede.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

O checklist da rede para uma instalação ou expansão com uma implantação manual, acesso público e um DNS sem split horizon

Implementação de Máquina Virtual

Em uma implantação manual, você cria todas as máquinas virtuais para o seu sistema usando o assistente OVA do seu cliente vSphere. Você, então, instala o sistema usando uma implantação manual.

Você deve escolher uma implantação manual se você estiver implantando um sistema de usuário 2000.

- Verifique se todas as máquinas virtuais internas adicionais (Mídia e internet, se aplicável) estão na mesma sub-rede que a máquina virtual de administração.
- Garanta que as máquinas virtuais de Proxy Reverso da Internet estejam na sua rede DMZ.

Endereços de IP necessários

Descrição	Local da rede	Endereço IP
Endereço de IP real da máquina virtual de administração	Interna	
Endereço de IP real da máquina virtual de mídia (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração)	
Endereço de IP real da segunda máquina virtual de mídia (somente sistema de 2000 usuários)	Interna (mesma sub-rede que a máquina virtual de administração)	
Endereço de IP real da terceira máquina virtual de mídia (somente sistema de 2000 usuários)	Interna (mesma sub-rede que a máquina virtual de administração)	
Endereço de IP real da máquina virtual da web (somente sistema de 2000 usuários)	Interna (mesma sub-rede que a máquina virtual de administração)	
Endereço de IP real da segunda máquina virtual da web (somente sistema de 2000 usuários)	Interna (mesma sub-rede que a máquina virtual de administração)	
Endereço de IP real do proxy reverso da Internet	DMZ (mas pode usar a NAT com um endereço de IP privado)	
URL da Administração (usada exclusivamente pelo sistema. Mapeia para o endereço VIP privado)	Interna (mesma sub-rede que a máquina virtual de administração)	
URL do site WebEx (usada exclusivamente pelo sistema. Mapeia para o endereço VIP público)	DMZ (mesma sub-rede do proxy reverso da Internet)	
Endereço de IP real da máquina virtual de administração de HA (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração do sistema primário)	
Endereço de IP real da máquina virtual de mídia de HA (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração do sistema primário)	
Endereço de IP real da máquina virtual da web de HA (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração do sistema primário)	
Endereço de IP real do proxy reverso da Internet de HA (se aplicável)	DMZ—mesma sub-rede que o proxy reverso da Internet do sistema primário (mas pode usar a NAT com um endereço de IP privado)	

CONFIGURAÇÃO DNS

Faça as seguintes alterações em sua configuração DNS.

Observação Existem algumas limitações quanto à parte do nome do organizador em relação à URL do site WebEx e a URL do site de Administração. Para obter uma lista das palavras que você não pode usar, consulte As URLs do Site WebEx e da Administração Webex, na página 86.

Tarefa	Exemplo
Atualize o seu Servidor DNS com os nomes dos organizadores e o endereço de IP das máquinas virtuais internas: A máquina virtual de Administração e se aplicável, as máquinas virtuais de mídia e da internet.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Atualize o seu servidor DNS com os nomes dos organizadores e o endereço de IP das máquinas virtuais do proxy reverso da internet.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Atualize o seu servidor DNS com a URL do site de Administração informações do endereço VIP Privado.	• <Administration-site-URL> <Private-VIP-address>
Atualize o seu servidor DNS com a URL do site WebEx e as informações do endereço VIP Público.	• <WebEx-site-URL> <Public-VIP-address>

CONFIGURAÇÃO FIREWALL

Por razões de segurança, a Cisco recomenda que você coloque o proxy reverso da Internet em uma sub-rede separada das máquinas virtuais internas (Administração, mídia e internet, se for o caso). Consulte Porta de acesso com um proxy reverso da Internet na rede DMZ, na página 88.

Configuração de Roteamento da Rede

Faça as seguintes alterações em seu roteamento de rede.

Tarefa	Compare Estes Endereços de IP
Habilitar o roteamento L3 (Layer 3) entre as redes DMZ e interna para as seguintes máquinas virtuais: A máquina virtual de Administração e se aplicável, as máquinas de mídia e virtuais da internet	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Verifique se o endereço VIP Público e as máquinas virtuais de Proxy Reverso da Internet estão na mesma sub-rede.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Verifique se o endereço VIP Privado e as máquinas virtuais internas (Administração, mídia e internet, se aplicável) estão na mesma sub-rede.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

O checklist da rede para uma instalação ou expansão com uma implantação automática, acesso público e um DNS split-horizon

Implementação de Máquina Virtual

Em uma implantação automática, implantamos todas as máquinas virtuais (que não seja a máquina virtual de Administração) para você. Recomendamos que você escolha uma implantação automática se você estiver implantando um sistema de 50, 250 ou 800 usuários.

- Certifique-se que a máquina virtual de mídia (se aplicável) está na mesma sub-rede da máquina virtual de administração.
- Garanta que as máquinas virtuais de Proxy Reverso da Internet estejam na sua rede DMZ.

Endereços de IP necessários

Descrição	Local da rede	Endereço IP
Endereço de IP real da máquina virtual de administração	Interna	
Endereço de IP real da máquina virtual de mídia (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração)	
Endereço de IP real do proxy reverso da Internet	DMZ (mas pode usar a NAT com um endereço de IP privado)	
URL da Administração (usada exclusivamente pelo sistema. Mapeia para o endereço VIP privado)	Interna (mesma sub-rede que a máquina virtual de administração)	
URL do site WebEx (usada exclusivamente pelo sistema. Mapeia para dois endereços VIP): • usuários internos—endereço VIP privado • usuários externos—endereço VIP público	• Usuários internos—Interna (mesma sub-rede que a máquina virtual de administração) • Usuários externos—DMZ (mesma sub-rede que o proxy reverso da internet)	
Endereço de IP real da máquina virtual de administração de HA (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração do sistema primário)	
Endereço de IP real da máquina virtual de mídia de HA (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração do sistema primário)	
Endereço de IP real do proxy reverso da Internet de HA (se aplicável)	DMZ [mesma sub-rede que o proxy reverso da Internet do sistema primário (mas pode usar a NAT com um endereço de IP privado)]	

CONFIGURAÇÃO DNS

Atualize o servidor DNS da seguinte forma. Existem algumas limitações quanto à parte do nome do organizador em relação à URL do site WebEx e a URL do site de Administração. Para obter uma lista das palavras que você não pode usar, consulte As URLs do Site WebEx e da Administração Webex, na página 86.

Tarefa	Exemplo
Nomes dos organizadores e endereços de IP das máquinas virtuais internas: A máquina virtual de Administração e se aplicável, a máquina virtual de mídia.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
Nome do organizador e endereço de IP para a máquina virtual DMZ.	• <IRP-vm-FQDN> <IRP-vm-IP-address>
URL do site WebEx, URL do site de Administração e informações sobre o endereço VIP Privado.	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>
URL do site WebEx e endereço VIP Público.	• <WebEx-site-URL> <Public-VIP-address>

CONFIGURAÇÃO FIREWALL

Por razões de segurança, recomendamos que você coloque o proxy reverso da Internet em uma sub-rede separada das máquinas virtuais internas (Administração ou mídia). Consulte Porta de acesso quando todas as máquinas virtuais estão na rede interna, na página 87.

Configuração de Roteamento da Rede

Faça as seguintes alterações em seu roteamento de rede.

Tarefa	Compare Estes Endereços de IP
Habilite o roteamento Layer 3 entre as redes DMZ e interna.	• Sub-rede Interna <internal-subnet>/24 • Sub-rede DMZ <DMZ-subnet>/24
Verifique se o endereço VIP Público e as máquinas virtuais de Proxy Reverso da Internet estão na mesma sub-rede.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>

Tarefa	Compare Estes Endereços de IP
Certifique-se que o endereço VIP Privado e as máquinas virtuais internas estejam na mesma sub-rede.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

O checklist da rede para uma instalação ou expansão com uma implantação manual, acesso público e um DNS split-horizon

Implementação de Máquina Virtual

Em uma implantação manual, você cria todas as máquinas virtuais para o seu sistema usando o assistente OVA do seu cliente vSphere. Você, então, instala o sistema usando uma implantação manual.

Você deve escolher uma implantação manual se você estiver implantando um sistema de usuário 2000.

- Verifique se todas as máquinas virtuais internas adicionais (Mídia e internet, se aplicável) estão na mesma sub-rede que a máquina virtual de administração.
- Garanta que as máquinas virtuais de Proxy Reverso da Internet estejam na sua rede DMZ.

Endereços de IP necessários

Descrição	Local da rede	Endereço IP
Endereço de IP real da máquina virtual de administração	Interna	
Endereço de IP real da máquina virtual de mídia (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração)	
Endereço de IP real da segunda máquina virtual de mídia (somente sistema de 2000 usuários)	Interna (mesma sub-rede que a máquina virtual de administração)	
Endereço de IP real da terceira máquina virtual de mídia (somente sistema de 2000 usuários)	Interna (mesma sub-rede que a máquina virtual de administração)	
Endereço de IP real da máquina virtual da web (somente sistema de 2000 usuários)	Interna (mesma sub-rede que a máquina virtual de administração)	
Endereço de IP real da segunda máquina virtual da web (somente sistema de 2000 usuários)	Interna (mesma sub-rede que a máquina virtual de administração)	

Descrição	Local da rede	Endereço IP
Endereço de IP real do proxy reverso da Internet	DMZ (mas pode usar a NAT com um endereço de IP privado)	
URL da Administração (usada exclusivamente pelo sistema. Mapeia para o endereço VIP privado)	Interna (mesma sub-rede que a máquina virtual de administração)	
URL do site WebEx (usada exclusivamente pelo sistema. Mapeia para dois endereços VIP) • usuários internos—endereço VIP privado • usuários externos—endereço VIP público	• Usuários internos—Interna (mesma sub-rede que a máquina virtual de administração) • Usuários externos—DMZ (mesma sub-rede que o proxy reverso da internet)	
Endereço de IP real da máquina virtual de administração de HA (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração do sistema primário)	
Endereço de IP real da máquina virtual de mídia de HA (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração do sistema primário)	
Endereço de IP real da máquina virtual da web de HA (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração do sistema primário)	
Endereço de IP real do proxy reverso da Internet de HA (se aplicável)	DMZ—mesma sub-rede que o proxy reverso da Internet do sistema primário (mas pode usar a NAT com um endereço de IP privado)	

CONFIGURAÇÃO DNS

Faça as seguintes alterações em sua configuração DNS.

Observação Existem algumas limitações quanto à parte do nome do organizador em relação à URL do site WebEx e a URL do site de Administração. Para obter uma lista das palavras que você não pode usar, consulte As URLs do Site WebEx e da Administração Webex, na página 86.

Tarefa	Exemplo
Atualize o seu Servidor DNS (que permite a pesquisa interna) com os nomes dos organizadores e os endereços de IP das máquinas virtuais internas: A máquina virtual de Administração e se aplicável, as máquinas virtuais de mídia e da internet.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Atualize o seu Servidor DNS (que permite a pesquisa interna) com o hostname e endereço de IP para a máquina virtual interna:	• <IRP-vm-FQDN> <IRP-vm-IP-address>
Atualize o seu servidor DNS (que permite a pesquisa interna) com a URL do site WebEx, URL do site de Administração e informações de endereço VIP Privado.	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>
Atualize o servidor DNS (que permite a pesquisa externa) com a URL do site WebEx e informações de endereço VIP Público.	• <WebEx-site-URL> <Public-VIP-address>

CONFIGURAÇÃO FIREWALL

Por razões de segurança, a Cisco recomenda que você coloque o proxy reverso da Internet em uma sub-rede separada das máquinas virtuais internas (Administração, mídia e internet, se for o caso). Consulte Porta de acesso com um proxy reverso da Internet na rede DMZ, na página 88.

Configuração de Roteamento da Rede

Faça as seguintes alterações em seu roteamento de rede.

Tarefa	Compare Estes Endereços de IP
Habilitar o roteamento L3 (Layer 3) entre as redes DMZ e interna para as seguintes máquinas virtuais: A máquina virtual de Administração e se aplicável, as máquinas de mídia e virtuais da internet	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Verifique se o endereço VIP Público e as máquinas virtuais de Proxy Reverso da Internet estão na mesma sub-rede.	• <Public-VIP-address> • <IRP-vm-FQDN> <IRP-vm-IP-address>
Verifique se o endereço VIP Privado e as máquinas virtuais internas (Máquina virtual de Administração e se aplicável, as máquinas virtuais de mídia e da internet) estão na mesma sub-rede.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

O checklist da Rede para uma Instalação ou Expansão com Implementação Automática e Nenhum Acesso Público

Implementação de Máquina Virtual

Em uma implantação automática, implantamos todas as máquinas virtuais (que não seja a máquina virtual de Administração) para você. Recomendamos que você escolha uma implantação automática se você estiver implantando um sistema de 50, 250 ou 800 usuários.

Certifique-se que a máquina virtual de mídia (se aplicável) está na mesma sub-rede da máquina virtual de administração.

Endereços de IP necessários

Descrição	Local da rede	Endereço IP
Endereço de IP real da máquina virtual de administração	Interna	
Endereço de IP real da máquina virtual de mídia (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração)	
URL da Administração (usada exclusivamente pelo sistema. Mapeia para o endereço VIP privado)	Interna (mesma sub-rede que a máquina virtual de administração)	
Endereço de IP real da máquina virtual de administração de HA (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração do sistema primário)	
Endereço de IP real da máquina virtual de mídia de HA (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração do sistema primário)	
Endereço de IP real do proxy reverso da Internet de HA (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração do sistema primário)	

CONFIGURAÇÃO DNS

Atualize o servidor DNS da seguinte forma. Existem algumas limitações quanto à parte do nome do organizador em relação à URL do site WebEx e a URL do site de Administração. Para obter uma lista das palavras que você não pode usar, consulte As URLs do Site WebEx e da Administração Webex, na página 86.

Tarefa	Exemplo
Nomes dos organizadores e endereços de IP das máquinas virtuais internas: A máquina virtual de Administração e se aplicável, a máquina virtual de mídia.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>
URL do site WebEx, URL do site de Administração e informações sobre o endereço VIP Privado.	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>

CONFIGURAÇÃO FIREWALL

Tarefa	Exemplo
Configure todos os firewalls dentro da sua rede interna para permitir que os navegadores da web acessem o endereço VIP Privado.	HTTP <Private-VIP-address>:80 HTTPS <Private-VIP-address>:443

Configuração de Roteamento da Rede

Tarefa	Compare Estes Endereços de IP
Certifique-se que o endereço VIP Privado e as máquinas virtuais internas estejam na mesma sub-rede.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address>

Checklist de Rede Para uma Instalação ou Expansão Com Implementação Manual e Acesso Não Público

Implementação de Máquina Virtual

Em uma implantação manual, você cria todas as máquinas virtuais para o seu sistema usando o assistente OVA do seu cliente vSphere. Você, então, instala o sistema usando uma implantação manual.

Você deve escolher uma implantação manual se você estiver implantando um sistema de usuário 2000.

- Verifique se todas as máquinas virtuais internas adicionais (Mídia e internet, se aplicável) estão na mesma sub-rede que a máquina virtual de administração.

Endereços de IP necessários

Descrição	Local da rede	Endereço IP
Endereço de IP real da máquina virtual de administração	Interna	
Endereço de IP real da máquina virtual de mídia (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração)	
Endereço de IP real da segunda máquina virtual de mídia (somente sistema de 2000 usuários)	Interna (mesma sub-rede que a máquina virtual de administração)	

Descrição	Local da rede	Endereço IP
Endereço de IP real da terceira máquina virtual de mídia (somente sistema de 2000 usuários)	Interna (mesma sub-rede que a máquina virtual de administração)	
Endereço de IP real da máquina virtual da web (somente sistema de 2000 usuários)	Interna (mesma sub-rede que a máquina virtual de administração)	
Endereço de IP real da segunda máquina virtual da web (somente sistema de 2000 usuários)	Interna (mesma sub-rede que a máquina virtual de administração)	
URL da Administração (usada exclusivamente pelo sistema. Mapeia para o endereço VIP privado)	Interna (mesma sub-rede que a máquina virtual de administração)	
URL do site WebEx (usada exclusivamente pelo sistema. Mapeia para o endereço VIP privado)	Interna (mesma sub-rede que a máquina virtual de administração)	
Endereço de IP real da máquina virtual de administração de HA (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração do sistema primário)	
Endereço de IP real da máquina virtual de mídia de HA (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração do sistema primário)	
Endereço de IP real da máquina virtual da web de HA (se aplicável)	Interna (mesma sub-rede que a máquina virtual de administração do sistema primário)	

CONFIGURAÇÃO DNS

Faça as seguintes alterações em sua configuração DNS.

Observação Existem algumas limitações quanto à parte do nome do organizador em relação à URL do site WebEx e a URL do site de Administração. Para obter uma lista das palavras que você não pode usar, consulte As URLs do Site WebEx e da Administração Webex, na página 86.

Tarefa	Exemplo
Atualize o seu Servidor DNS (que permite a pesquisa interna) com os nomes dos organizadores e os endereços de IP das máquinas virtuais internas: A máquina virtual de Administração e se aplicável, as máquinas virtuais de mídia e da internet.	• <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>
Atualize o seu servidor DNS com a URL do site de Administração, a URL do site WebEx e informações do endereço de VIP Privado.	• <Administration-site-URL> <Private-VIP-address> • <WebEx-site-URL> <Private-VIP-address>

CONFIGURAÇÃO FIREWALL

Faça as seguintes alterações em seus firewalls.

Tarefa	Exemplo
Configure todos os firewalls dentro da sua rede interna para permitir que os navegadores da web acessem o endereço VIP Privado.	• HTTP <Private-VIP-address>:80 • HTTPS <Private-VIP-address>:443

Configuração de Roteamento da Rede

Faça as seguintes alterações em seu roteamento de rede.

Tarefa	Compare Estes Endereços de IP
Verifique se o endereço VIP Privado e as máquinas virtuais internas (Administração, mídia e internet, se aplicável) estão na mesma sub-rede.	• <Private-VIP-address> • <admin-vm-FQDN> <admin-vm-IP-address> • <media-vm-FQDN> <media-vm-IP-address> • <web-vm-FQDN> <web-vm-IP-address>

As URLs do Site WebEx e da Administração Webex

URL do Site WebEx

Usuários acessam a URL do site WebEx para agendar, organizar ou participar de reuniões. Esta URL resolve para o endereço VIP privado ou endereço VIP público, dependendo se você está ou usando um DNS split-horizon.

- Resolve para o endereço VIP público para todos os usuários, quando você não tem DNS split-horizon.
- Resolve para o endereço VIP público para os usuários externos, quando você tem DNS split-horizon.
- Resolve para o endereço VIP privado para os usuários internos, quando você tem DNS split-horizon.

Observação As portas 80 e 443 devem ser abertas para a URL do site WebEx.

URL da Administração WebEx

Os administradores acessam a URL da Administração WebEx para configurar, gerenciar e monitorar o sistema. Esta URL resolve para o endereço VIP privado.

Observação As portas 80 e 443 devem ser abertas para a URL de administração WebEx.

Nomes para as URLs do Site WebEx e da Administração WebEx.

Você pode escolher quase todos os nomes para essas URLs, compreendendo todos os caracteres minúsculos. No entanto, você não pode usar os seguintes como o nome do organizador nas URLs:

- o mesmo nome que os nomes dos organizadores para qualquer uma das máquinas virtuais no sistema

- autenticação
- client
- companylogo
- dispatcher
- docs
- elm-admin
- elm-cliente-serviços
- E-mails
- manutenção
- manager
- orion
- oriondata
- oriontemp
- NBR
- npp
- probe
- reminder
- RAIZ
- solr
- TomcatROOT
- upgradeserver
- url0107ld
- Versão
- WBXService
- WebEx

Porta de acesso quando todas as máquinas virtuais estão na rede interna

Esta seção descreve a porta de acesso necessária no firewall externo quando todas as máquinas virtuais do sistema (Admin e, se for o caso, mídia, Web e Proxy Reverso da Internet) estiverem na rede interna. Esta é a topologia de rede interna do proxy reverso da internet. (Consulte também Portas do Cisco WebEx Meeting Center, na página 94).

Verifique se o firewall ou qualquer solução de balanceamento de carga redireciona os pedidos de portas listadas abaixo para garantir que os usuários finais possam organizar e participar de reuniões com sucesso.

- Porta TCP 80 para o endereço IP virtual público (VIP)
- Porta TCP 443 para o endereço IP virtual público (VIP)

Observação O nó da Web e o nó da Administração enviam solicitações SMTP para o servidor de e-mail configurado. Se houver um firewall entre as máquinas virtuais internas da Web e de Administração e o servidor de e-mail, o tráfego SMTP pode ser bloqueado. Para garantir que a configuração do servidor de e-mail e a notificação de e-mail funcionem corretamente, a porta 25 ou 465 (número de porta SMTP segura) deve estar aberta entre o servidor de e-mail e as máquinas virtuais da Web e de Administração.

Porta de Acesso no Firewall Externo

Se você tiver ativado o acesso público, então as seguintes portas estarão abertas, da entrada diretamente da Internet para as máquinas virtuais do proxy reverso da internet na rede interna:

Porta de acesso com um proxy reverso da Internet na rede DMZ

Esta seção descreve a porta de acesso necessária nos firewalls interno e externo, quando você tem máquinas virtuais internas (Admin e, se for o caso, mídia e Web) na rede interna, e o Proxy Reverso da Internet (IRP) na rede DMZ. (Consulte também Portas do Cisco WebEx Meeting Center, na página 94).

Configurar as Listas de controle de acesso (ACLs) no interruptor que permite o tráfego das máquinas virtuais do sistema aos hosts ESXi.

Porta de Acesso no Firewall Externo

Ativado o acesso do público ao abrir a porta 80 (HTTP), além da porta 443 (HTTPS), assim os usuários podem inserir a URL do site WebEx sem ter que lembrar se é HTTP ou HTTPS. Embora a porta 80 esteja aberta, todo o tráfego de rede flui pela porta 443 (Criptografia SSL HTTPS).

Importante Verifique se o firewall ou qualquer solução de balanceamento de carga redireciona as solicitações de portas listadas abaixo para garantir que os usuários possam organizar e entrar em reuniões com sucesso.

Restrição Configure a porta TCP 64700 na máquina IRP para negar as solicitações que vêm para o endereço VIP público. No firewall externo, isso limita o acesso a esta porta para solicitações somente das máquinas virtuais de Administração.

Protocolo	Porta	Origem	Destino	Por que ela é necessária
TCP	443	Quaisquer clientes externos.	VIP público (Eth1) do IRP.	Os clientes externos acessam a URL do site WebEx usando HTTPS. As conexões TCP são iniciadas das máquinas de clientes externos para máquinas virtuais IRP.
TCP	80	Quaisquer clientes externos.	VIP público (Eth1) do IRP.	Os clientes externos acessam a URL do site WebEx usando HTTP. As conexões TCP são iniciadas das máquinas de clientes externos para máquinas virtuais IRP.
TCP	8444 (Introduzido no 2.5MR1, 2.6 e 2.0MR6HF.)	Quaisquer clientes externos.	VIP público (Eth1) do IRP.	Os clientes externos acessam as gravações WebEx usando HTTPS. As conexões TCP são iniciadas das máquinas de clientes externos para máquinas virtuais IRP.
UDP	53	IP real (Eth0) do IRP.	Servidor DNS.	Isto é necessário se você tiver um firewall entre as máquinas virtuais e o servidor DNS, para o seu sistema implantar e operar com sucesso.

Porta de Acesso no Firewall Interno

Se você tem restrições em conexões da rede interna para a rede DMZ, então a tabela nesta seção se aplica. Permita a *saída* de conexões TCP da rede interna para o segmento de rede DMZ.

Observação Nenhuma conexão TCP deve ser permitida do segmento DMZ para a rede interna para este produto funcionar corretamente.

Observação Usando o iptables ou as listas de controle de acesso (ACLs), configure o firewall para que as conexões para a porta 64616 venham apenas a partir da máquina virtual de administração.

Observação O nó da Web e o nó da Administração enviam solicitações SMTP para o servidor de e-mail configurado. Se houver um firewall entre as máquinas virtuais internas da Web e de Administração e o servidor de e-mail, o tráfego SMTP pode ser bloqueado. Para garantir que a configuração do servidor de e-mail e a notificação de e-mail funcionem corretamente, a porta 25 ou 465 (número de porta SMTP segura) deve estar aberta entre o servidor de e-mail e as máquinas virtuais da Web e de Administração.

Observação Especialmente quando o IRP está na rede DMZ, permitir que o protocolo de controle de mensagens da Internet (ICMP) ecoe as solicitações e as respostas. Caso contrário, o IRP detecta e a validação de disponibilidade do servidor DNS pode falhar se a resposta de eco do ICMP não for recebida.

Protocolo	Porta	Origem	Destino	Por que ela é necessária
TCP	64001	Todas as máquinas virtuais internas (Eth0 IP).	IP real (Eth0) das máquinas virtuais IRP.	Estabelece conexões inversas ao IRP. As conexões TCP são estabelecidas a partir das máquinas virtuais internas para as máquinas virtuais IRP.
TCP	64002	Máquinas virtuais da web e de administração (Eth0 IP).	IP real (Eth0) das máquinas virtuais IRP.	Estabelece conexões inversas ao IRP. As conexões TCP são estabelecidas a partir das máquinas virtuais internas para as máquinas virtuais IRP.
TCP	7001	Todas as máquinas virtuais internas (Eth0 IP).	IP real (Eth0) das máquinas virtuais IRP.	Estabelece conexões inversas ao IRP. As conexões TCP são iniciadas a partir das máquinas virtuais internas para as máquinas virtuais IRP.

Protocolo	Porta	Origem	Destino	Por que ela é necessária
TCP	64616	Máquinas virtuais de administração (Eth0 IP).	IP real (Eth0) das máquinas virtuais IRP.	Inicialização do IRP. As conexões TCP são iniciadas a partir de máquinas virtuais de administração para as máquinas virtuais IRP. **Observação** Usando o iptables ou as listas de controle de acesso (ACLs), configure o firewall para que as conexões para a porta 64616 venham apenas a partir da máquina virtual de administração.
TCP	64700	Máquinas virtuais de administração (Eth0 IP).	IP real (Eth0) das máquinas virtuais IRP.	Coleta registros sobre o IRP. As conexões TCP são iniciadas a partir de máquinas virtuais de administração para as máquinas virtuais IRP. Limite o acesso a esta porta em todas as máquinas virtuais do Cisco WebEx Meetings Server apenas para outras máquinas virtuais do Cisco WebEx Meetings Server com regras do firewall.
TCP	22	As máquinas de clientes internos.	IP real (Eth0) das máquinas virtuais IRP.	Solução de problemas das máquinas virtuais IRP usando uma conta de suporte remoto.
TCP	443	As máquinas de clientes internos.	VIP privada (Eth1) das máquinas virtuais de administração. IP real (Eth0) das máquinas virtuais de mídia.	Os usuários internos acessam a URL do site WebEx usando HTTPS. As conexões TCP são estabelecidas a partir da máquina do cliente interno para a máquina virtual de administração.

Protocolo	Porta	Origem	Destino	Por que ela é necessária
TCP	443	VIP privado (Eth1) das máquinas virtuais de administração e IP real (eth0) das máquinas virtuais de mídia.	VIP público (Eth1) do IRP.	
TCP	65002	As máquinas de clientes internos.	Todas as máquinas virtuais internas.	Controlam o tráfego de rede entre as máquinas virtuais internas.
TCP	65102	As máquinas de clientes internos.	Todas as máquinas virtuais internas.	Controlam o tráfego de rede entre as máquinas virtuais internas.
TCP	80	As máquinas de clientes internos.	VIP privada (Eth1) das máquinas virtuais de administração.	Os usuários internos acessam a URL do site WebEx usando HTTP. As conexões TCP são estabelecidas a partir da máquina do cliente interno para a máquina virtual de administração.
UDP	53	Todas as máquinas virtuais internas (Eth0 IP).	Servidor DNS.	Se você tiver um firewall entre as máquinas virtuais e o servidor DNS, para seu sistema implantar e operar com sucesso.
TCP	8443	Nó da Web do Cisco WebEx Meetings Server.	CUCM	Para o tráfego AXL em um sistema de Múltiplos Centros de Dados entre o Cisco WebEx Meetings Server e o CUCM para permitir o failover do CUCM LDAP.
TCP	8444	O nó da web do Cisco WebEx Meetings Server é usado para baixar arquivos de gravação.	VIP privada (Eth1) das máquinas virtuais de administração. IP real (Eth0) das máquinas virtuais de mídia.	Os usuários internos acessam a URL do site WebEx usando HTTPS. As conexões TCP são estabelecidas a partir da máquina do cliente interno para a máquina virtual de administração.

Portas VMware vCenter

Portas abertas para Implantação

Estas são algumas das portas que são utilizadas durante a implantação de um Centro de Dados Único (SDC) do Cisco WebEx Meetings Server (CWMS). Assim que a implantação estiver concluída, você poderá fechar todas as portas que foram abertas exclusivamente para a implantação.

A porta TCP 443 deve ser aberta, nos dois sentidos, entre o vCenter e a máquina virtual de administração para a gestão segura de https durante uma implantação do sistema automático. A máquina virtual de administração usa essa porta para fornecer credenciais do vCenter e implantar as máquinas virtuais automaticamente no vCenter.

As portas listadas abaixo são usadas para a comunicação entre o organizador ESXi e o vCenter. Se o organizador ESXi e o vCenter estão conectados a uma *rede de gerenciamento separada*, você pode não precisar abrir essas portas através do firewall. Para obter uma lista completa de portas usadas pelo vCenter e pelo organizador ESXi, consulte a documentação do VMware.

- Porta UDP/TCP 902 em ambas as direções entre o vCenter e os hosts ESXi para gerenciamento de vCenter
- (Opcional) Porta TCP 22 do cliente vSphere para os hosts ESXi para gerenciamento SSH
- Porta UDP 514 dos hosts ESXi para seu sistema ao syslog interno
- Porta TCP 5989 em ambas as direções entre vCenter e os hosts ESXi para gerenciamento de XML

A porta UDP padrão utilizada pelos clientes externos para transmissão de dados de áudio e vídeo é SSL (porta 443).

Portas abertas para suportar

Portas a serem abertas entre as máquinas internas	tcp 8080 tcp 8081 tcp 8082 tcp 9809 tcp 9810 tcp 9811 tcp 9812 tcp 9813 tcp 9814 tcp 9815 tcp 9816 tcp 9817 tcp 9818 tcp 9819 tcp 9820 tcp 9840 tcp 6502 tcp 12340 tcp 12342 tcp 12442 tcp 7001 tcp 7003 tcp 7004 tcp 7005 tcp:5060 tcp 5061 tcp 5062 tcp 5063 tcp 22
Portas a serem abertas entre as máquinas internas e os IPs virtuais	tcp 443 tcp 80

Portas a serem abertas entre o IPs do Proxy Reverso da Internet e as máquinas internas	tcp 7001 tcp 64001 tcp 64700 tcp 64616
Portas UDP para abrirem entre as máquinas internas	udp range:10000:19999 udp range:16000:32000 udp range:9000:9009 udp 5060 udp 5062

Portas do Cisco WebEx Meeting Center

Essas portas são utilizadas para a comunicação entre o Cisco WebEx Meeting Center e o Cisco WebEx Meetings Server.

- As portas UDP utilizadas pelos clientes internos para transmissão de dados de vídeo e áudio entre UDP e SSL incluem:
  - Para os sistemas de 50 usuários, use a porta UDP 9000
  - Para os sistemas de 250 usuários, use as portas UDP 9000, 9001, 9002, 9003
  - Para os sistemas do 800 usuários, use as portas UDP 9000, 9001, 9002, 9003, 9004, 9005, 9006, 9007, 9008, 9009
  - Para os sistemas de 2000 usuários, use as portas UDP 9000, 9001, 9002, 9003, 9004, 9005, 9006, 9007
- Com as configurações de rede adequadas, os servidores de mídia internos permitem conexões através de qualquer porta utilizada pelo Meeting Center.
- O proxy reverso da Internet só aceita conexões a partir do Meeting Center através de portas TCP 80 e 443.
- Tráfego AXL do nó da Web para o CUCM é passado através da porta 8443. (Consulte também Usando o CUCM para configurar o AXL Web Service e a sincronização de diretórios).

Usar NAT com seu sistema

A Cisco suporta a passagem de Tradução de Endereços de Rede (NAT) com este produto para os endereços de IP da máquina virtual e para os endereços de IP virtuais (VIPs públicos e privados) que são usados no sistema.

O diagrama esquemático a seguir ilustra uma típica passagem NAT para um sistema de 50 usuários sem Alta Disponibilidade (HA). Ao usar a NAT, você pode reduzir o número de *endereços de IP públicos* necessários para o produto para apenas um endereço de IP, em vez de dois (ou três, no caso de implantar HA). Você

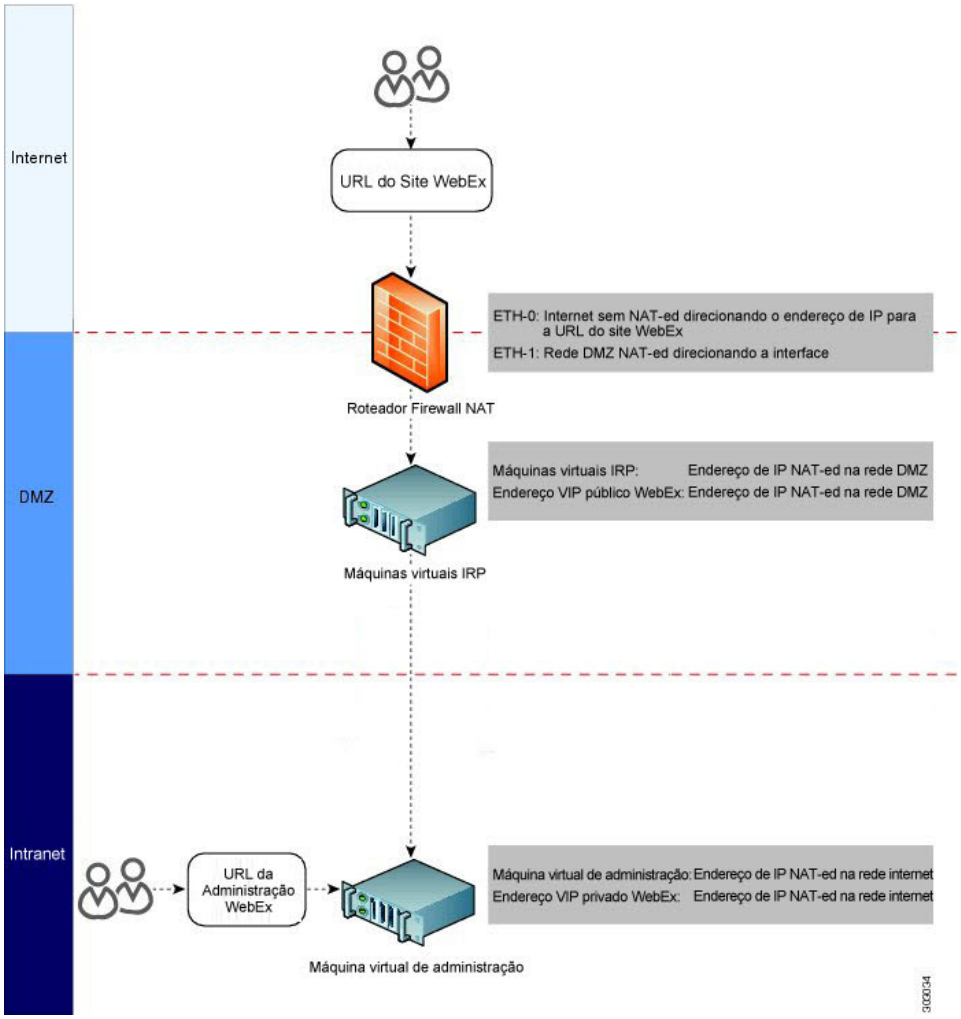
também pode implantar implantações NAT semelhantes, desde que estas satisfaçam os requisitos gerais do sistema.

Importante O uso de múltiplas NATs e firewalls tende a aumentar a latência, afetando a qualidade do tráfego em tempo real para os usuários.

Além disso, ao usar vários domínios NAT, o roteamento entre esses vários domínios NAT pode ser um desafio. Você pode usar endereços de IP NAT-ed, desde que os seguintes requisitos sejam atendidos:

- Todas as máquinas virtuais do sistema podem utilizar endereços de IP NAT-ed, com a exceção da máquina virtual de proxy reverso da internet. NAT entre a máquina virtual de administração e a máquina virtual de Proxy Reverso da Internet não é suportada. O endereço de IP da máquina virtual de proxy reverso da internet (seu endereço de IP real) deve estar acessível pela máquina virtual de administração através da rede interna.
- O endereço VIP público em si não precisa ser publicamente visível, mas deve ser traduzível a partir da Internet.
- Ao implantar o acesso público, a URL do site WebEx deve ser mapeada para um endereço de IP visível na Internet. Este endereço de IP visível na Internet deve ser acessível por usuários externos e *também* mapeado para o endereço VIP público que você configurou durante a implantação do sistema.

  Você pode optar por tornar o endereço VIP público visível da Internet. Se você optar por não fazê-lo publicamente visível, então deve ser traduzível da Internet.



No diagrama, um usuário externo acessa o site WebEx para participar ou organizar uma reunião. Após uma pesquisa de DNS, o endereço de IP do site WebEx é o endereço de IP público NAT (Eth0). Este endereço de IP público NAT é para o roteador de firewall NAT externo (Roteador firewall e NAT 1), entre a rede externa e a rede DMZ.

O roteador de firewall recebe este pedido do usuário externo e, internamente, encaminha o pedido para o endereço de IP privado NAT do roteador (Eth1, exposto à rede DMZ). O Eth1 então envia o pedido para o endereço VIP público (também um endereço de IP NAT no segmento de rede privada para o site WebEx).

Você pode usar endereços de IP NAT para o endereço VIP público e para os endereços de IP do proxy reverso da internet. O único endereço de IP público NAT é o endereço de IP Eth0 para o roteador de firewall NAT.

Observação Para garantir esse roteador de firewall NAT (entre a Internet e a rede DMZ), encaminhe o pacote recebido corretamente, defina a configuração de mapeamento de portas no dispositivo NAT, ou aplique outros mecanismos similares para garantir que o pacote seja encaminhado corretamente para o endereço VIP público e para o proxy reverso da internet.

Geralmente há um segundo roteador de firewall NAT interno entre a rede DMZ e a rede interna. Similar ao roteador de firewall NAT externo, o Eth0 é um endereço de IP privado NAT DMZ e é uma interface para a rede DMZ. O Eth1 é um endereço de IP privado NAT que é uma interface para a rede interna.

Você pode usar endereços de IP NAT para o endereço VIP privado e para os endereços de IP da máquina virtual de administração.

Para obter mais informações sobre a NAT, consulte http://www.cisco.com/c/en/us/tech/ip/ip-addressing-services/tech-tech-notes-list.html.

Projeções proxies

Se a sua topologia de rede inclui projeções proxies, ela *deve atender aos requisitos específicos* do proxy reverso da internet para funcionar corretamente. Consulte "Uso de projeções proxies no seu sistema" no *Guia de solução de problemas do Cisco WebEx Meetings Server* para detalhes completos.

CAPÍTULO 5

Configurar o Cisco Unified Communications Manager (CUCM)

Para ativar a teleconferência no Cisco WebEx Meetings Server, você deve configurar um (ou mais) sistema do Cisco Unified Communications Manager (CUCM) para gerenciar o controle de chamada. Opcionalmente, você pode configurar um segundo sistema CUCM para alta disponibilidade de áudio.

- CUCM em um ambiente MDC, página 100
- Antes de Começar, página 100
- Teleconferência segura CUCM em um ambiente MDC, página 101
- Checklist da configuração CUCM do centro de multidados, página 101
- Checklist da configuração CUCM com ou sem alta disponibilidade, página 102
- Configurando CUCM em um sistema com CWMS, página 102
- Configurar CUCM para sistemas de alta disponibilidade e sem alta disponibilidade, página 105
- Configurar um perfil de segurança de tronco SIP, página 109
- Configurar um perfil SIP, página 111
- Gerenciamento de certificados CUCM usando TLS, página 112
- Configurar um tronco SIP, página 118
- Configurar um grupo de rota, página 121
- Configurar uma lista de rota, página 122
- Configurar um Padrão de Rota, página 123
- Configurar um padrão de rota SIP, página 123
- Compatibilidade de recursos e de suporte do CUCM, página 124

CUCM em um ambiente MDC

As configurações CUCM em um ambiente com (MDC) são as mesmas que em um ambiente com Centro de dados único (SDC). Os parâmetros de configuração modificados em um centro de dados são automaticamente compensados por outro centro de dados.

No CUCM, as configurações básicas em um ambiente com (MDC) são as mesmas que em um ambiente com um Centro de dados único (SDC). No entanto, você deve configurar troncos a todos os centros de dados. Cada centro de dados pode ter um padrão de rota diferente. Se você quiser usar mais de um CUCM, cada centro de dados deve ter um tronco SIP para o CUCM nos outros centros de dados para chamadas de transferência.

Antes de Começar

Obtenha as informações do Ponto de aplicação e o Ponto balanceador de carga da página de **Áudio** do Cisco WebEx Meetings Server. Os pontos balanceadores de carga gerenciam o balanceamento de carga da chamada e os pontos de aplicativos gerenciam as chamadas, o fluxo de conferência e o controle de recursos. Os sistemas de tamanhos diferentes têm diferentes números de pontos balanceadores de carga e de pontos de aplicativos e os números não são personalizados. Inicie sessão no site da Administração e selecione **Configurações** > **Áudio** para ver estas informações.

- Tamanho (50/250/800/2000)
- Alta disponibilidade
- Tipo de transporte

Na página de **Áudio** há uma Tabela de configuração SIP que exibe as informações do ponto balanceador de carga e do ponto de aplicativo, incluindo endereços IP e portas. Esta tabela também é exibida na página **Configurando suas Configurações de Áudio pela Primeira Vez** que aparece na primeira vez que você configurar as definições de áudio.

Para fazer com que o CUCM funcione com o Cisco WebEx Meetings Server, o CUCM requer as seguintes configurações específicas e de base:

- Configuração básica

Observação Estas configurações podem ser compartilhadas com múltiplos sistemas do Cisco WebEx Meetings Server.

  - Perfil de segurança de tronco SIP
  - Perfil SIP

- Configuração específica

Observação Estas configurações devem ser feitas para sistemas individuais do Cisco WebEx Meetings Server e não podem ser compartilhadas por vários sistemas.

  - Gerenciamento de Certificados

- Tronco SIP
- Grupo de rota
- Lista de rota
- Padrão de rota
- Padrão de Rota SIP

Teleconferência segura CUCM em um ambiente MDC

Não é possível importar certificados de todos os centros de dados em um Centro de multidados (MDC) em um único Cisco Unified Call Manager (CUCM) como necessário para garantir a teleconferência quando o nome comum de ambos os certificados for o mesmo.

Por padrão, o nome comum para todos os centros de dados é a URL do site global do sistema. No entanto, para tornar o nome comum único, você pode gerar certificados usando Gerando uma Solicitação de Assinatura de Certificado (CSR) para a Versão 2.6 e superior, na página 115 para a versão 2.6 e superior ou Gerando uma solicitação de assinatura de certificado (CSR) Versão 2.5 e inferior, na página 116 para a versão 2.5 e anterior. Selecione a URL do site local em vez da URL do site global para ser utilizada no nome comum.

Os certificados autoassinados gerados durante qualquer procedimento de alteração do sistema (como alterar a URL da administração ou do site, alterar os nomes de organizadores) resultam em um certificado que tem a URL do site global no nome comum, então você deve criar manualmente os certificados com a URL do site local após este tipo de operação.

Checklist da configuração CUCM do centro de multidados

A checklist de configuração exibe o número de cada tipo de configuração do Cisco Unified Communication Manager (CUCM) que você deve configurar para o sistema com (MDC).

Tamanho do sistema	Perfis de segurança (Configuração base)	Perfis SIP (Configuração base)	Troncos SIP (Configuração específica)	Grupos de rota (Configuração específica)	Listas de rota (Configuração específica)	Padrões de rotas (Configuração específica)	Padrões de rotas SIP (Configuração específica)
250 usuários	2	1	4	1	1	N	2
800 Usuários	2	1	4	1	1	N	2
2000 usuários com HA	2	1	6	1	1	N	4

Checklist da configuração CUCM com ou sem alta disponibilidade

A checklist de configuração exibe o número de cada tipo de configuração do Cisco Unified Communication Manager (CUCM) que você deve configurar para o sistema com um Centro de dados único (SDC), com ou sem alta disponibilidade (HA).

Tamanho do sistema	Perfis de segurança (Configuração base)	Perfis SIP (Configuração base)	Troncos SIP (Configuração específica)	Grupos de rota (Configuração específica)	Listas de rota (Configuração específica)	Padrões de rotas (Configuração específica)	Padrões de rotas SIP (Configuração específica)
50 Usuários	2	1	2	1	1	N[21]	1
50 usuários com HA	2	1	4	1	1	N	2
250 usuários	2	1	2	1	1	N	1
250 usuários com HA	2	1	4	1	1	N	2
800 Usuários	2	1	2	1	1	N	1
800 usuários com HA	2	1	4	1	1	N	2
2000 usuários	2	1	5	1	1	N	3
2000 usuários com HA	2	1	6	1	1	N	4

21 N é o número dos Números de chamada de entrada de acesso que você configura no Cisco WebEx Meetings Server.

Configurando CUCM em um sistema com CWMS

Normalmente, cada site em um ambiente com (MDC) tem um grupo CUCM específico associado a ele. Os grupos CUCM são conectados usando troncos entre grupos (TIC). Cada grupo CUCM tem chamada de entrada/troncos na discagem para o site local CWMS. Session Manager Edition (SME) é suportado. CWMS pode ser configurado atrás dos grupos CUCM locais. Cada CUCM tem troncos SIP REFER de todas as máquinas virtuais de mídia no MDC.

Para redundância, cada grupo CUCM pode ter troncos INVITE para todos os centros de dados. O padrão de rota de chamada de entrada dá prioridade ao tronco INVITE associado ao centro de dados local e usa o tronco INVITE para o centro de dados remoto somente em caso de falha.

Tabela 4: Troncos CUCM SIP configurados em cada grupo CUCM

Implementação	Troncos INVITE - Balanceador de Carga (MACC)	Troncos REFER - Ponto de Aplicação (TAS)
Pequeno	2	2
Média	2	2
Grande	4	6

Configurando o CUCM em um sistema com de 250 ou 800 usuários

Configure o Cisco Unified Communication Manager (CUCM) para sistemas de 250 ou 800 usuários com vários centros de dados. Normalmente, cada centro de dados possui um cluster CUCM local.

Antes de iniciar

Informações necessárias:

- Endereço de IP de um ponto balanceador de carga para cada centro de dados
- Endereço de IP de um ponto de aplicativo para cada centro de dados
- O número de números de chamada de entrada de acesso que você irá configurar em seu sistema

Etapa 1 Reveja o perfil de segurança existente do tronco SIP e determine se satisfaz ou não o requisito de instalação do Cisco WebEx Meetings Server. Se não satisfazer, configure dois perfis de segurança do tronco SIP.
Adicione um perfil de segurança do tronco SIP para o ponto balanceador de carga e adicione um perfil de segurança do tronco SIP para o ponto de aplicativo. Consulte Configurar um Perfil de Segurança de Tronco SIP para um Ponto Balanceador de Carga, na página 109 e Configurar um Perfil de Segurança de Tronco SIP para um Ponto de Aplicativo, na página 110.

Etapa 2 Reveja o perfil existente SIP e determine se satisfaz ou não o requisito de instalação do Cisco WebEx Meetings Server. Se não satisfazer, configure um perfil SIP.
Configure um perfil SIP conforme descrito no Configurar um perfil TLS SIP ou Configure um perfil SIP IPv6, na página 112.

Etapa 3 Configure dois troncos SIP para os pontos balanceadores de carga.
Consulte Configurar um Tronco SIP em um Ponto Balanceador de Carga.

Etapa 4 Configure dois troncos SIP para os pontos de aplicativos.
Consulte Configurar um Tronco SIP para um Ponto de Aplicativo.

Etapa 5 Configure um grupo de rotas usando o tronco SIP que você configurou para o ponto balanceador de carga.
Consulte Configurar um grupo de rota.

Etapa 6 Configure uma lista de rotas usando o grupo de rotas que você configurou na etapa anterior.
Consulte Configurar uma lista de rota.

Etapa 7 Configure *N* padrões de rotas usando a lista de rotas acima.
N é o número de números de acesso de chamadas de entrada que você configurou nas configurações de áudio no site de Administração. Consulte Configurar um Padrão de Rota.

Etapa 8 Configure dois padrões de rotas SIP para os pontos de aplicativos.
Consulte Configurar um padrão de rota SIP.

Configurando o CUCM em um sistema com para 2000 usuários

Configure o Cisco Unified Communication Manager (CUCM) para um sistemas de 2000 usuários com vários centros de dados (MDC). Normalmente, cada centro de dados possui um cluster CUCM local.

Antes de iniciar

Informações necessárias:

- Endereço de IP de três pontos balanceadores de carga para cada centro de dados
- Endereço de IP de três pontos de aplicativos para cada centro de dados
- O número de números de chamada de entrada de acesso que você irá configurar em seu sistema

Etapa 1 Reveja o perfil de segurança existente do tronco SIP e determine se satisfaz ou não o requisito de instalação do Cisco WebEx Meetings Server. Se não satisfazer, configure dois perfis de segurança do tronco SIP.
Adicione um perfil de segurança do tronco SIP para o ponto balanceador de carga e adicione um perfil de segurança do tronco SIP para o ponto de aplicativo. Consulte Configurar um Perfil de Segurança de Tronco SIP para um Ponto Balanceador de Carga, na página 109 e Configurar um Perfil de Segurança de Tronco SIP para um Ponto de Aplicativo, na página 110.

Etapa 2 Reveja o perfil existente SIP e determine se satisfaz ou não o requisito de instalação do Cisco WebEx Meetings Server. Se não satisfazer, configure um perfil SIP.
Configure um perfil SIP conforme descrito no Configurar um perfil TLS SIP ou Configure um perfil SIP IPv6, na página 112.

Etapa 3 Configure dois troncos SIP para os pontos balanceadores de carga.
Consulte Configurar um Tronco SIP em um Ponto Balanceador de Carga.

Etapa 4 Configure quatro troncos SIP para os pontos de aplicativos.
Consulte Configurar um Tronco SIP para um Ponto de Aplicativo.

Etapa 5 Configure um grupo de rotas usando o tronco SIP que você configurou para o ponto balanceador de carga.
Consulte Configurar um grupo de rota.

Etapa 6 Configure uma lista de rotas usando o grupo de rotas que você configurou na etapa anterior.
Consulte Configurar uma lista de rota.

Etapa 7 Configure *N* padrões de rotas usando a lista de rotas acima.

N é o número de números de acesso de chamadas de entrada que você configurou nas configurações de áudio no site de Administração. Consulte Configurar um Padrão de Rota.

Etapa 8 Configure quatro padrões de rotas SIP para os pontos de aplicativos.
Consulte Configurar um padrão de rota SIP.

Configurar CUCM para sistemas de alta disponibilidade e sem alta disponibilidade

As seções seguintes fornecem uma descrição das tarefas necessárias para configurar sistemas de alta disponibilidade e sem alta disponibilidade de vários tamanhos.

Configurando o CUCM nos sistemas de 50, 250 e 800 usuários sem alta disponibilidade

Configure o CUCM para sistemas de 50, 250 e 800 usuários sem Alta Disponibilidade

Antes de iniciar

Informações necessárias:

- Endereço de IP de um ponto balanceador de carga
- Endereço de IP de um ponto de aplicativo
- O número de números de chamada de entrada de acesso que você irá configurar em seu sistema

Etapa 1 Reveja o perfil de segurança existente do tronco SIP e determine se satisfaz ou não o requisito de instalação do Cisco WebEx Meetings Server. Se não satisfazer, configure dois perfis de segurança do tronco SIP.
Adicione um perfil de segurança do tronco SIP para o ponto balanceador de carga e adicione um perfil de segurança do tronco SIP para o ponto de aplicativo. Consulte Configurar um Perfil de Segurança de Tronco SIP para um Ponto Balanceador de Carga, na página 109 e Configurar um Perfil de Segurança de Tronco SIP para um Ponto de Aplicativo, na página 110.

Etapa 2 Reveja o perfil existente SIP e determine se satisfaz ou não o requisito de instalação do Cisco WebEx Meetings Server. Se não satisfazer, configure um perfil SIP.
Configure um perfil SIP conforme descrito no Configurar um perfil TLS SIP ou Configure um perfil SIP IPv6, na página 112.

Etapa 3 Configure um tronco SIP para o ponto balanceador de carga.
Consulte Configurar um Tronco SIP em um Ponto Balanceador de Carga.

Etapa 4 Configure um tronco SIP para o ponto de aplicativo.
Consulte Configurar um Tronco SIP para um Ponto de Aplicativo.

Etapa 5 Configure um grupo de rotas usando o tronco SIP que você configurou para o ponto balanceador de carga.
Consulte Configurar um grupo de rota.

Etapa 6 Configure uma lista de rotas usando o grupo de rotas que você configurou na etapa anterior.
Consulte Configurar uma lista de rota.

Etapa 7 Configure *N* padrões de rotas usando a lista de rotas acima.
N é o número de números de acesso de chamadas de entrada que você configurou nas configurações de áudio no site de Administração. Consulte Configurar um Padrão de Rota.

Etapa 8 Configure dois padrões de rotas SIP para os pontos de aplicativos.
Consulte Configurar um padrão de rota SIP.

Configurando o CUCM nos sistemas de 50, 250 e 800 usuários com alta disponibilidade

Esta seção descreve as informações necessárias e instruções detalhadas sobre como configurar o CUCM para sistemas de 50, 250 ou 800 usuários com alta disponibilidade.

Informações necessárias

- Endereço de IP de dois pontos balanceadores de carga
- Endereço de IP de dois pontos de aplicativos
- O número de números de chamada de entrada de acesso que você irá configurar em seu sistema

Procedimento de configuração

Execute as seguintes etapas:

Tarefa	Descrição	Informações detalhadas
1	Reveja o perfil de segurança existente do tronco SIP e determine se satisfaz ou não o requisito de instalação do Cisco WebEx Meetings Server. Se não satisfazer, configure dois perfis de segurança do tronco SIP.	Adicione um perfil de segurança do tronco SIP para o ponto balanceador de carga e adicione um perfil de segurança do tronco SIP para o ponto de aplicativo. Consulte Configurar um Perfil de Segurança de Tronco SIP para um Ponto Balanceador de Carga, na página 109 e Configurar um Perfil de Segurança de Tronco SIP para um Ponto de Aplicativo, na página 110.
2	Reveja o perfil existente SIP e determine se satisfaz ou não o requisito de instalação do Cisco WebEx Meetings Server. Se não satisfazer, configure um perfil SIP.	Configure um perfil SIP conforme descrito no Configurar um perfil TLS SIP ou Configure um perfil SIP IPv6, na página 112.
3	Configure dois troncos SIP para os pontos balanceadores de carga.	Consulte Configurar um Tronco SIP em um Ponto Balanceador de Carga.

Tarefa	Descrição	Informações detalhadas
4	Configure dois troncos SIP para os pontos de aplicativos.	Consulte Configurar um Tronco SIP para um Ponto de Aplicativo.
5	Configure um grupo de rotas usando o tronco SIP que você configurou para o ponto balanceador de carga na tarefa 3, acima.	Consulte Configurar um grupo de rota.
6	Configure uma lista de rotas usando o grupo de rotas que você configurou na tarefa 5, acima.	Consulte Configurar uma lista de rota.
7	Configure *N* padrões de rotas usando a lista de rotas acima. *N* é o número de números de acesso de chamadas de entrada que você configurou nas configurações de áudio no site de Administração.	Consulte Configurar um Padrão de Rota.
8	Configure dois padrões de rotas SIP para os pontos de aplicativos.	Consulte Configurar um padrão de rota SIP.

Configurar o CUCM em um sistema de 2000 usuários sem alta disponibilidade

Configure o Cisco Unified Communication Manager (CUCM) para um sistema de 2000 usuários sem Alta Disponibilidade.

Antes de iniciar

Informações necessárias:

- Endereço de IP de dois pontos balanceadores de carga
- Endereço de IP de três pontos de aplicativos
- O número de números de chamada de entrada de acesso que você irá configurar em seu sistema

Etapa 1 Reveja o perfil de segurança existente do tronco SIP e determine se satisfaz ou não o requisito de instalação do Cisco WebEx Meetings Server. Se não satisfazer, configure dois perfis de segurança do tronco SIP.
Adicione um perfil de segurança do tronco SIP para o ponto balanceador de carga e adicione um perfil de segurança do tronco SIP para o ponto de aplicativo. Consulte Configurar um Perfil de Segurança de Tronco SIP para um Ponto Balanceador de Carga, na página 109 e Configurar um Perfil de Segurança de Tronco SIP para um Ponto de Aplicativo, na página 110.

Etapa 2 Reveja o perfil existente SIP e determine se satisfaz ou não o requisito de instalação do Cisco WebEx Meetings Server. Se não satisfazer, configure um perfil SIP.
Configure um perfil SIP conforme descrito no Configurar um perfil TLS SIP ou Configure um perfil SIP IPv6, na página 112.

Etapa 3 Configure dois troncos SIP para o ponto balanceador de carga.
Consulte Configurar um Tronco SIP em um Ponto Balanceador de Carga.

Etapa 4 Configure três troncos SIP para o ponto de aplicativo.
Consulte Configurar um Tronco SIP para um Ponto de Aplicativo.

Etapa 5 Configure um grupo de rotas usando o tronco SIP que você configurou para o ponto balanceador de carga.
Consulte Configurar um grupo de rota.

Etapa 6 Configure uma lista de rotas usando o grupo de rotas que você configurou na etapa anterior.
Consulte Configurar uma lista de rota.

Etapa 7 Configure *N* padrões de rotas usando a lista de rotas acima.
N é o número de números de acesso de chamadas de entrada que você configurou nas configurações de áudio no site de Administração. Consulte Configurar um Padrão de Rota.

Etapa 8 Configure dois padrões de rotas SIP para os pontos de aplicativos.
Consulte Configurar um padrão de rota SIP.

Próximos passos

Configurando o CUCM em um sistema de 2000 usuários com alta disponibilidade

Configure o Cisco Unified Communication Manager (CUCM) para um sistema de 2000 usuários com Alta Disponibilidade.

Antes de iniciar

Informações necessárias:

- Endereço de IP de dois pontos balanceadores de carga
- Endereço de IP de quatro pontos de aplicativos
- O número de números de chamada de entrada de acesso que você irá configurar em seu sistema

Etapa 1 Reveja o perfil de segurança existente do tronco SIP e determine se satisfaz ou não o requisito de instalação do Cisco WebEx Meetings Server. Se não satisfazer, configure dois perfis de segurança do tronco SIP.
Adicione um perfil de segurança do tronco SIP para o ponto balanceador de carga e adicione um perfil de segurança do tronco SIP para o ponto de aplicativo. Consulte Configurar um Perfil de Segurança de Tronco SIP para um Ponto Balanceador de Carga, na página 109 e Configurar um Perfil de Segurança de Tronco SIP para um Ponto de Aplicativo, na página 110.

Etapa 2 Reveja o perfil existente SIP e determine se satisfaz ou não o requisito de instalação do Cisco WebEx Meetings Server. Se não satisfazer, configure um perfil SIP.
Configure um perfil SIP conforme descrito no Configurar um perfil TLS SIP ou Configure um perfil SIP IPv6, na página 112.

Etapa 3 Configure dois troncos SIP para os pontos balanceadores de carga.
Consulte Configurar um Tronco SIP em um Ponto Balanceador de Carga.

Etapa 4 Configure quatro troncos SIP para os pontos de aplicativos.
Consulte Configurar um Tronco SIP para um Ponto de Aplicativo.

Etapa 5 Configure um grupo de rotas usando o tronco SIP que você configurou para o ponto balanceador de carga.
Consulte Configurar um grupo de rota.

Etapa 6 Configure uma lista de rotas usando o grupo de rotas que você configurou na etapa anterior.
Consulte Configurar uma lista de rota.

Etapa 7 Configure *N* padrões de rotas usando a lista de rotas acima.
N é o número de números de acesso de chamadas de entrada que você configurou nas configurações de áudio no site de Administração. Consulte Configurar um Padrão de Rota.

Etapa 8 Configure dois padrões de rotas SIP para os pontos de aplicativos.
Consulte Configurar um padrão de rota SIP.

Próximos passos

Configurar um perfil de segurança de tronco SIP

Configurar um Perfil de Segurança de Tronco SIP para um Ponto Balanceador de Carga

Antes de iniciar

Se o sistema Cisco WebEx Meetings Server está configurado para TLS, você deve importar um certificado de teleconferência seguro. Para obter mais informações, consulte a seção "Importação de certificados de teleconferência seguros" no *Guia de Administração do Cisco WebEx Meetings Server* em http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html.

Etapa 1 Inicie sessão em http://ccm-server/, onde *ccm-server* é o nome de domínio totalmente qualificado ou o endereço IP do servidor Cisco Unified Communications Manager.

Etapa 2 Selecione **Cisco Unified CM Administration**.

Etapa 3 Selecione **Sistema** > **Segurança** > **Perfil de segurança de tronco SIP**.

Etapa 4 Selecione **Adicionar novo**.

Etapa 5 Configure os seguintes campos.

- Nome—Insira um nome para identificar o seu perfil de segurança de tronco SIP.
- Modo de segurança do dispositivo — Selecione **Não seguro** se você quiser que o CUCM se comunique com o Cisco WebEx Meetings Server usando UDP/TCP. Selecione **Criptografado** se você quiser que o CUCM se comunique com o Cisco WebEx Meetings Server usando TLS.

- Nome do assunto X.509 — Insira seu nome de certificado se você quiser que o CUCM se comunique com o Cisco WebEx Meetings Server usando TLS.

  Observação Se você quiser que o CUCM se comunique com o Cisco WebEx Meetings Server usando TLS, um sistema diferente do Cisco WebEx Meetings Server não poderá compartilhar o mesmo perfil de segurança de tronco SIP, porque cada sistema deve ter um certificado diferente. Obtenha o nome do certificado do Cisco WebEx Meetings Server no site da administração. Para obter mais informações, consulte "Gerenciando certificados" no *Guia de administração*.

- Porta de entrada— Insira 5060 se você deseja que o CUCM se comunique com o Cisco WebEx Meetings Server usando UDP/TCP. Insira 5061 se você deseja que o CUCM se comunique com o Cisco WebEx Meetings Server usando TLS.

Observação Não configure nenhum dos outros campos da página, mantenha as configurações padrão.

Etapa 6 Selecione **Salvar**.

Configurar um Perfil de Segurança de Tronco SIP para um Ponto de Aplicativo

Antes de iniciar

Se o sistema Cisco WebEx Meetings Server está configurado para TLS, você deve importar um certificado de teleconferência seguro. Para obter mais informações, consulte a seção "Importação de certificados de teleconferência seguros" no *Guia de Administração do Cisco WebEx Meetings Server* em http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html.

Etapa 1 Inicie sessão em http://ccm-server/, onde *ccm-server* é o nome de domínio totalmente qualificado ou o endereço IP do servidor Cisco Unified Communications Manager.

Etapa 2 Selecione **Cisco Unified CM Administration**.

Etapa 3 Selecione **Sistema** > **Segurança** > **Perfil de segurança de tronco SIP**.

Etapa 4 Selecione **Adicionar novo**.

Etapa 5 Configure os seguintes campos:

- Nome—Insira um nome para identificar o seu perfil de segurança de tronco SIP.
- Modo de segurança do dispositivo — Selecione **Não seguro** se você quiser que o CUCM se comunique com o Cisco WebEx Meetings Server usando UDP/TCP. Selecione **Criptografado** se você quiser que o CUCM se comunique com o Cisco WebEx Meetings Server usando TLS.
- Nome do assunto X.509 — Insira seu nome de certificado se você quiser que o CUCM se comunique com o Cisco WebEx Meetings Server usando TLS.

  Observação Se você quiser que o CUCM se comunique com o Cisco WebEx Meetings Server usando TLS, um sistema diferente do Cisco WebEx Meetings Server não poderá compartilhar o mesmo perfil de segurança de tronco SIP, porque cada sistema deve ter um certificado diferente. Obtenha o nome do certificado do Cisco WebEx Meetings Server no site da administração. Para obter mais informações, consulte "Gerenciando certificados" no *Guia de administração*.

- Porta de entrada— Insira 5062 se você deseja que o CUCM se comunique com o Cisco WebEx Meetings Server usando UDP/TCP. Insira 5063 se você deseja que o CUCM se comunique com o Cisco WebEx Meetings Server usando TLS.

Observação Não configure nenhum dos outros campos da página, mantenha as configurações padrão.

Etapa 6 Selecione **Salvar**.

Configurar um perfil SIP

Configurar um perfil SIP padrão

O perfil do Protocolo de Iniciação de Sessão (SIP) padrão utiliza as configurações padrão e não requer etapas adicionais de configuração.

Configurar um perfil TLS SIP

Etapa 1 Inicie sessão em http://ccm-server/, onde *ccm-server* é o nome de domínio totalmente qualificado ou o endereço IP do servidor Cisco Unified Communications Manager.

Etapa 2 Selecione **Cisco Unified CM Administration**.

Etapa 3 Selecione **Dispositivo** > **Configurações do dispositivo** > **Perfil SIP**.

Etapa 4 Selecione **Adicionar novo**.

Etapa 5 Configure os seguintes campos:

- Nome—Insira um nome para o perfil SIP.
- Redirecione por aplicação—Selecione a caixa de seleção.

Não configure quaisquer outros campos na página; deixe os campos com suas configurações padrões.

Etapa 6 Selecione **Salvar**.

Configure um perfil SIP IPv6

Etapa 1 Inicie sessão em http://ccm-server/, onde *ccm-server* é o nome de domínio totalmente qualificado ou o endereço IP do servidor Cisco Unified Communications Manager.

Etapa 2 Selecione **Cisco Unified CM Administration**.

Etapa 3 Selecione **Dispositivo** > **Configurações do dispositivo** > **Perfil SIP**.

Etapa 4 Selecione **Adicionar novo**.

Etapa 5 Configure os seguintes campos:

- Nome—Insira um nome para o perfil SIP.
- Habilitar ENAT—Selecione a caixa de seleção.

Não configure quaisquer outros campos na página; deixe os campos com suas configurações padrões.

Etapa 6 Selecione **Salvar**.

Gerenciamento de certificados CUCM usando TLS

Se você quiser que o Cisco Unified Communications Manager (CUCM) se comunique com o Cisco WebEx Meetings Server (CWMS) usando TLS, você deve executar as seguintes ações:

- Obtenha um certificado CWMS a partir do site de Administração e carregue-o para o CUCM.

Observação Se o CWMS utiliza certificados de terceiros, então todos os certificados da cadeia de certificados devem ser carregados para o CUCM.

- Baixe o certificado CUCM e depois carregue-o no site de Administração CWMS.

Observação Se CUCM utiliza certificados de terceiros, então apenas o último certificado na cadeia de certificados (Certificado de autoridade certificadora raiz (CA} precisa ser carregado para o CWMS.

Se você usar TLS para conectar todos os centros de dados em um sistema com (MDC) para o mesmo CUCM, o CWMS não pode usar a URL do site comum para o nome comum do certificado. Você deve usar cada URL do site local do centro de dados para cada nome comum do certificado, porque o CUCM 10.5 e versões mais antigas tratam vários certificados com um nome comum como o mesmo certificado. Se os nomes não são diferentes, o segundo certificado do centro de dados substitui o primeiro certificado do centro de dados depois de carregar o segundo certificado do centro de dados no CUCM.

Consulte "Gerenciamento de Certificados" no *Guia de Administração* para obter mais informações. Consulte http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html para obter mais detalhes.

Carregue os certificados do Cisco WebEx Meetings Server

Etapa 1 Faça o download e exporte o seu certificado do Cisco WebEx Meetings Server.
a) Inicie sessão no site da Administração do Cisco WebEx Meetings Server.
b) Selecione **Configurações** > **Segurança** > **Certificados**.
c) Copie o nome do certificado da seção de Certificado SSL.
d) Selecione **Mais opções** > **Exportar o certificado SSL**.
e) Salve o seu certificado para o disco rígido local.

Etapa 2 Inicie sessão em http://ccm-server/, onde *ccm-server* é o nome de domínio totalmente qualificado ou o endereço IP do servidor Cisco Unified Communications Manager.

Etapa 3 Selecione **Cisco Unified OS Administration**.

Etapa 4 Selecione **Segurança** > **Gerenciamento de certificados**.

Etapa 5 Selecione **Atualizar certificado/Cadeia de certificados**.

Etapa 6 Selecione **CallManager-confiança** no menu suspenso Nome do certificado.

Etapa 7 Selecione o botão **Procurar** e selecione o certificado que você salvou no seu disco rígido local.

Etapa 8 Clique em **Baixar Arquivo**.
O sistema exibe uma mensagem "Sucesso: Certificado carregado".

Etapa 9 (Opcional) Se o Cisco WebEx Meetings Server utiliza certificados autoassinados, repita os passos 4 a 8 para carregar o certificado intermediário e o certificado da autoridade certificadora raiz (CA) da cadeia de certificados.

Etapa 10 Selecionar **Fechar**.

Próximos passos

Para obter mais informações sobre certificados, consulte a seção "Gerenciando Certificados" no *Guia de Administração* em http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

Instalando um Certificado CUCM de Terceiros

Este procedimento explica como carregar um certificado de terceiros no seu Cisco WebEx Meetings Server.

Antes de iniciar

- Gere um Pedido de Assinatura de Certificado (CSR) e envie-o para uma autoridade certificadora de terceiros para solicitar certificados. Consulte Gerando uma Solicitação de Assinatura de Certificado (CSR) para a Versão 2.6 e superior para a versão 2.6 e superior ou Gerando uma solicitação de assinatura de certificado (CSR) Versão 2.5 e inferior, na página 116para a versão 2.5 e anterior para obter instruções.
- A autoridade certificadora enviará a você uma cadeia de certificados que pode conter o seguinte:

- Certificado 1 (usuário) - emitido a uma entidade do usuário por uma autoridade de certificação intermediária.
- Certificado 2 (intermediário) - emitido para uma autoridade de certificação intermediária por uma autoridade certificadora raiz.
- Certificado 3 (CA Raiz) - emitido pela autoridade de certificação raiz.

• Quando você receber vários certificados em uma cadeia de certificados, concatene os três certificados em um arquivo, com o certificado de usuário primeiro.

Etapa 1 Importe o arquivo de certificado de terceiros no Cisco WebEx Meetings Server, conforme descrito no *Guia de administração do Cisco WebEx Meeting Server* em http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

Etapa 2 Inicie sessão em http://ccm-server/, onde *ccm-server* é o nome de domínio totalmente qualificado ou o endereço IP do servidor Cisco Unified Communications Manager.

Etapa 3 Selecione **Cisco Unified OS Administration**.

Etapa 4 Selecione **Segurança** > **Gerenciamento de certificados**.

Etapa 5 Selecione **Atualizar certificado/Cadeia de certificados**.

Etapa 6 Selecione **CallManager-confiança** no menu suspenso Nome do certificado.

Etapa 7 Selecione o botão **Procurar** e selecione o certificado Autoridade Certificadora Raiz (CA) que você salvou no seu disco rígido local.
Este é o último certificado autoassinado da cadeia de verificação, que é utilizado para verificar o certificado `CallManager.pem`.

Observação Você pode obter o certificado CA Raiz diretamente de uma autoridade certificadora, ao mesmo tempo que o certificado `CallManager.pem` é criado.

Etapa 8 Clique em **Baixar Arquivo**.
Espere o seu sistema indicar "Êxito: Certificado carregado."

Etapa 9 Selecionar **Fechar**.

Próximos passos

Para obter mais informações sobre certificados, consulte a seção *Gerenciando certificados* no *Guia de administração do Cisco WebEx Meetings Server* em http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

Baixar os certificados CUCM

Este procedimento é necessário apenas se o CUCM utiliza certificados autoassinados. Se o CUCM utiliza certificados de terceiros, você deve carregar apenas o último certificado (certificado CA Raiz) na cadeia de certificados no Cisco WebEx Meeting Server. Contate a Autoridade Certificadora (CA) para obter informações sobre como obter um certificado CA Raiz.

Consulte a sua documentação CUCM para mais informações sobre a geração de certificados CUCM.

Etapa 1 Inicie sessão em http://ccm-server/, onde *ccm-server* é o nome de domínio totalmente qualificado ou o endereço IP do servidor Cisco Unified Communications Manager.

Etapa 2 Selecione **Cisco Unified OS Administration**.

Etapa 3 Selecione **Segurança** > **Gerenciamento de certificados**.

Etapa 4 Procure o certificado no campo "Nome do Certificado" para o certificado com o nome "CallManager". Selecione o campo ".PEM File".

Etapa 5 Selecione **Baixar** para salvar o certificado CUCM `CallManager.pem` no seu disco rígido local.

Próximos passos

Para mais informações sobre carregar certificados CUCM no Cisco WebEx Meetings Server, consulte "Gerenciando Certificados" no *Guia de administração*. Consulte http://www.cisco.com/en/US/products/ps12732/products_installation_and_configuration_guides_list.html.

Gerando uma Solicitação de Assinatura de Certificado (CSR) para a Versão 2.6 e superior

O método de hash usado para gerar uma Solicitação de Assinatura de Certificado (CSR) e a chave privada para certificados SSL no CWMS 2.5 e acima usam SHA2 (SHA256).

Etapa 1 Conectar ao site de Administração.
Em um sistema com Múltiplos Centros de Dados, o DNS determina qual Painel do centro de dados é exibido. Use este Painel para gerenciar todos os centros de dados no sistema.

Etapa 2 Selecione **Configurações** > **Segurança** > **Certificados** > **Certificados no sistema CWMS**.
Em um sistema com Vários centros de dados, continue com os **Certificados no sistema CWMS ou certificados no centro de dados *N***

Etapa 3 Selecione **Gerar CSR** para o tipo desejado de CSR.
Em 01 de novembro de 2015, as autoridades de certificação (por exemplo, VeriSign, GoDaddy, e assim por diante) pararão de emitir certificados para nomes de domínio internos (por exemplo domínio.local, domínio.interno). Antes do CWMS versão 2.0MR9, você podia carregar apenas um único certificado SSL com Nomes alternativos para todos os componentes na implantação, mas isso exigia de você a compra de certificados SAN SSL caros para uma solução completa. A partir do CWMS versão 2.5MR5, você pode comprar no SSL da URL do site WebEx um certificado da Autoridade de Certificação para uso em servidores IRP, e utilize os certificados SSL autoassinados para as máquinas virtuais de rede interna.

Etapa 4 Complete estes campos na página **Gerar CSR (Certificado de Solicitação de Entrada)**.

Opção	Descrição
Nome comum	Selecione o certificado da **URL do site local**, certificado da **URL do site global** ou certificado **Curinga**.

Opção	Descrição
Nomes Alternativos do Assunto Esta opção só aparece se você selecionar **Nome alternativo do assunto** para o seu tipo de Nome Comum.	Seu site de administração e nomes da máquina virtual. Nenhum nome alternativo de assunto são necessários se você selecionou um nome comum para o curinga.
Organização	Insira o nome da organização.
Departamento	Insira o nome do departamento.
Cidade	Insira a cidade.
Estado/Província	Insira o estado ou província.
País	Selecione o país.
Tamanho da Chave	Selecione o tamanho da chave 2048.
Algoritmo hash	Selecione o algoritmo hach SHA256.

Etapa 5 Selecione **Gerar CSR**.
A caixa de diálogo **Baixar CSR** aparece.

Etapa 6 Selecione **Baixar**.
Você recebe um arquivo ZIP que contém a CSR e a chave privada associada. O arquivo CSR é chamado de `csr.pem` e o arquivo de chave privada é chamado `csr_private_key.pem`.

Etapa 7 Faça backup do sistema usando o VMware Data Recovery ou o VMware vSphere Data Protection. Consulte Criando um backup usando o VMware vCenter.
O backup do sistema preserva a chave privada, no caso em que seja necessário restaurá-lo.

Gerando uma solicitação de assinatura de certificado (CSR) Versão 2.5 e inferior

O método de hash usado para gerar uma Solicitação de Assinatura de Certificado (CSR) e a chave privada para certificados SSL no CWMS 2.0 e versões anteriores usam SHA1. O CWMS 2.5 e acima usam SHA2 (SHA256).

Os certificados de aplicativos internos e externos e CSRs possuem as seguintes opções:

- Tipos de chaves:
  - RSA
  - EC

- Para o tipo de chave RSA, o comprimento da chave é 2048.
- Algoritmos RSA Hash:
  - SHA1
  - SHA224
  - SHA256
  - SHA384
  - SHA512
- Tamanhos de chaves e algoritmos hash dos certificados CE:
  - O tamanho da chave é 256:
    - SHA256
    - SHA384
    - SHA512
  - O tamanho da chave é 384:
    - SHA384
    - SHA512
  - O tamanho da chave é 512:
    - SHA512

Os certificados externos e internos devem ser do mesmo tipo. O certificado externo depende do certificado interno. Por exemplo, se um sistema tiver um certificado interno RSA, a página **Gerar autoassinado externo** terá apenas uma opção do tipo de chave, RSA (o mesmo que o tipo de chave do certificado externo). Você não pode gerar ou baixar certificados externos com um tipo de chave diferente do tipo de chave interna instalada.

Etapa 1 Conectar ao site de Administração.
Em um sistema com Múltiplos Centros de Dados, o DNS determina qual Painel do centro de dados é exibido. Use este Painel para gerenciar todos os centros de dados no sistema.

Etapa 2 Selecione **Configurações** > **Segurança** > **Certificados** > **Certificados no sistema CWMS**.
Em um sistema com Vários centros de dados, continue com os **Certificados no sistema CWMS ou certificados no centro de dados *N***

Etapa 3 Selecione **Gerar CSR** para o tipo desejado de CSR.
Em 01 de novembro de 2015, as autoridades de certificação (por exemplo, VeriSign, GoDaddy, e assim por diante) pararão de emitir certificados para nomes de domínio internos (por exemplo domínio.local, domínio.interno). Antes do CWMS versão 2.0MR9, você podia carregar apenas um único certificado SSL com Nomes alternativos para todos os componentes na implantação, mas isso exigia de você a compra de certificados SAN SSL caros para uma solução completa. A partir do CWMS versão 2.5MR5, você pode comprar no SSL da URL do site WebEx um certificado da

Autoridade de Certificação para uso em servidores IRP, e utilize os certificados SSL autoassinados para as máquinas virtuais de rede interna.

Etapa 4 Complete estes campos na página **Gerar CSR (Certificado de Solicitação de Entrada)**.

Opção	Descrição
Nome comum	Selecione o certificado da **URL do site local**, certificado da **URL do site global** ou certificado **Curinga**.
Nomes Alternativos do Assunto Esta opção só aparece se você selecionar **Nome alternativo do assunto** para o seu tipo de Nome Comum.	Seu site de administração e nomes da máquina virtual. Nenhum nome alternativo de assunto são necessários se você selecionou um nome comum para o curinga.
Organização	Insira o nome da sua organização.
Departamento	Insira o nome do seu departamento.
Cidade	Digite sua cidade.
Estado/Província	Insira seu Estado ou província.
País	Selecione o seu país.
Tamanho da Chave	Selecione o tamanho da chave 2048.

Etapa 5 Selecione **Gerar CSR**.
A caixa de diálogo **Baixar CSR** aparece.

Etapa 6 Selecione **Baixar**.
Você recebe um arquivo ZIP que contém a CSR e a chave privada associada. O arquivo CSR é chamado de `csr.pem` e o arquivo de chave privada é chamado `csr_private_key.pem`.

Etapa 7 Faça backup do sistema usando o VMware Data Recovery ou o VMware vSphere Data Protection. Consulte Criando um backup usando o VMware vCenter.
O backup do sistema preserva a chave privada, no caso em que seja necessário restaurá-lo.

Configurar um tronco SIP

Observação Ao implantar um sistema de 2000 usuários com Alta disponibilidade (HA) e múltiplos pontos de aplicativos e de balanceadores de carga, cada ponto de aplicativo e de balanceador de carga na solução CWMS deve ter um tronco SIP dedicado; múltiplos endereços IP de destino dentro do mesmo tronco SIP não são suportados.

Configurar um Tronco SIP em um Ponto Balanceador de Carga

Etapa 1 Inicie sessão em http://ccm-server/, onde *ccm-server* é o nome de domínio totalmente qualificado ou o endereço IP do servidor Cisco Unified Communications Manager.

Etapa 2 Selecione **Cisco Unified CM Administration**.

Etapa 3 Selecione **Dispositivo** > **Tronco**.

Etapa 4 Selecione **Adicionar novo**.

Etapa 5 No menu suspenso **Tipo de tronco**, selecione **Tronco SIP**.

Observação Não altere quaisquer outros campos nesta página; deixe os parâmetros em suas configurações padrões.

O ponto de terminação de mídia requerido deve estar desmarcado na página **Configuração de tronco** quando o CUCM estiver comunicando-se com o Cisco WebEx Meeting Server. Se você não estiver usando o Cisco WebEx Meeting Service com o áudio CUCM SIP, selecione **Ponto de terminação de mídia requerido** ao fornecer serviços telefônicos usando uma infraestrutura PBX de terceiros.

Etapa 6 Selecione **Próximo**.

Etapa 7 Configure os seguintes campos:

- Nome do dispositivo — Insira um nome para o tronco SIP.
- Pool do dispositivo — Selecione um dispositivo pool apropriado do menu suspenso.

  Para determinar qual Grupo Cisco Unified Communications Manager foi configurado nesse grupo de dispositivos, selecione **Sistema** > **Menu do grupo de dispositivos**. Para verificar quais Cisco Unified Communications Managers fazem parte deste grupo, selecione **Sistema** > **Grupo Cisco Unified CM**.

  Observação Anote os endereços de IP do servidor primário e secundário. Esses endereços IP são inseridos quando você configura as definições de áudio no Cisco WebEx Meetings Server. Consulte "Definindo as suas Configurações de Áudio pela Primeira Vez" no *Guia de administração* para obter mais detalhes. Consulte Guias de Instalação e Atualização do Cisco WebEx Meetings Server.
- Endereço de destino—Insira o endereço IPv4 do ponto balanceador de carga. Consulte a tabela de Configuração SIP na página Áudio do site da administração do endereço IP.
- Endereço de destino IPv6—Insira o endereço IPv6 do ponto balanceador de carga se você quiser ativar o IPv6 entre o CUCM e o Cisco WebEx Meetings Server.
- Porta de destino—Insira 5060 se você deseja que o CUCM se comunique com o Cisco WebEx Meetings Server usando UDP/TCP. Insira 5061 se você deseja que o CUCM se comunique com o Cisco WebEx Meetings Server usando TLS.
- Perfil de segurança do tronco SIP—Selecione seu perfil de segurança do ponto balanceador de carga a partir do menu suspenso.
- Perfil SIP — Selecione **Perfil SIP padrão** se você quiser que o CUCM se comunique com o Cisco WebEx Meetings Server usando UDP/TCP. Selecione **Prfil SIP TLS** se você quiser que o CUCM se comunique com o Cisco WebEx Meetings Server usando TLS. Selecione **Perfil SIP IPv6** se você quiser ativar o IPv6 entre o CUCM e o Cisco WebEx Meetings Server.
- Espaço de pesquisa de chamada—Selecione um Espaço de pesquisa de chamada que pode ligar para os números de telefone e os padrões de rota configurados no CUCM que você deseja que o Cisco WebEx Meetings Server chame. Selecione **Roteamento de chamada** > **Classe de controle** > **Espaço de pesquisa de chamada**. Um espaço

de pesquisa de chamada consiste de uma lista ordenada de partições de rota que normalmente é atribuída a dispositivos ou padrões de rota. Os espaços de pesquisa de chamadas determinam as partições que os dispositivos de chamadas pesquisam quando estão tentando completar uma chamada. Para obter mais informações, consulte "Configuração do Espaço de pesquisa de chamada" no *Guia de Administração do Cisco Unified Communications Manager* ou "Espaços de pesquisa de chamada e Partições" no *Guia do Sistema do Cisco Unified Communications Manager*.

- Espaço de pesquisa de chamada de reencaminhamento e Espaço de pesquisa de chamada para consulta Out-Of-Dialog—Selecione um Espaço de pesquisa de chamada e um Espaço de pesquisa de chamada para consulta Out-Of-Dialog que possuem a partição de rota que é configurada para o padrão de rota SIP. Consulte Configurar um padrão de rota SIP. Se isso for definido como **< Nenhum >**, então o sistema encaminha apenas chamadas para padrões de rota com uma partição de rota definida para **< Nenhum >**, então o padrão de rota SIP deve ter a partição de rota definida para **< Nenhum >**. Esta configuração é necessária para inserir reuniões no Cisco WebEx Meetings Server. Para obter mais informações, consulte "Configuração do Espaço de pesquisa de chamada" no *Guia de Administração do Cisco Unified Communications Manager* ou "Espaços de pesquisa de chamada e Partições" no *Guia do Sistema do Cisco Unified Communications Manager*.

Observação Não altere quaisquer outros campos nesta página; deixe os parâmetros em suas configurações padrões.

Etapa 8 Selecione **Salvar**.

Etapa 9 Selecione **Redefinir** e depois selecione **Redefinir e reiniciar** na janela pop-up.

Configurar um Tronco SIP para um Ponto de Aplicativo

Etapa 1 Inicie sessão em http://ccm-server/, onde *ccm-server* é o nome de domínio totalmente qualificado ou o endereço IP do servidor Cisco Unified Communications Manager.

Etapa 2 Selecione **Cisco Unified CM Administration**.

Etapa 3 Selecione **Dispositivo** > **Tronco**.

Etapa 4 Selecione **Adicionar novo**.

Etapa 5 No menu suspenso **Tipo de tronco**, selecione **Tronco SIP**.

Observação Não altere quaisquer outros campos nesta página; deixe os valores para suas configurações padrões.

Etapa 6 Selecione **Próximo**.

Etapa 7 Configure os seguintes campos:

- Nome do dispositivo—Insira um nome para o seu tronco SIP.
- Dispositivo pool—Selecione **Padrão** a partir do menu suspenso.
- Endereço de destino — Insira o endereço de IPv4 do servidor de aplicação.
- Endereço de destino IPv6 — Opcionalmente, insira o endereço IPv6 do servidor de aplicativos para ativar o IPv6 entre o CUCM e o Cisco WebEx Meetings Server.
- Porta de destino — Insira 5062 se você deseja que o CUCM se comunique com o Cisco WebEx Meetings Server usando UDP/TCP. Insira 5063 se você deseja que o CUCM se comunique com o Cisco WebEx Meetings Server usando TLS.

- Perfil de segurança do tronco SIP — Selecione seu perfil de segurança do servidor de aplicação a partir do menu suspenso.
- Perfil SIP — Selecione **Perfil SIP padrão** se você quiser que o CUCM se comunique com o Cisco WebEx Meetings Server usando UDP/TCP. Selecione **Perfil SIP TLS** se você quiser que o CUCM se comunique com o Cisco WebEx Meetings Server usando TLS. Selecione **Perfil SIP IPv6** se você quiser ativar o IPv6 entre o CUCM e o Cisco WebEx Meetings Server.
- Espaço de pesquisa de chamada—Selecione um Espaço de pesquisa de chamada que pode chamar para os números de telefone e os padrões de rota configurados no CUCM que você deseja que o Cisco WebEx Meetings Server chame. Selecione **Roteamento de chamada** > **Classe de controle** > **Espaço de pesquisa de chamada**. Um espaço de pesquisa de chamada consiste de uma lista ordenada de partições de rota que normalmente é atribuída a dispositivos ou padrões de rota. Os espaços de pesquisa de chamadas determinam as partições que os dispositivos de chamadas pesquisam quando estão tentando completar uma chamada. Se isso for definido como **<Nenhum>**, então isso só será capaz de chamar dispositivos ou padrões de rota com uma partição definida para **<Nenhum>**. Para obter mais informações, consulte *Configuração do Espaço de pesquisa de chamada* no *Guia de Administração do Cisco Unified Communications Manager* ou *Espaços de pesquisa de chamada e Partições* no *Guia do Sistema do Cisco Unified Communications Manager*.

Observação Não altere quaisquer outros campos nesta página; deixe os valores para suas configurações padrões.

Deixe a caixa de diálogo **Terminação de Ponto de Mídia Requerido** não selecionada na página **Configuração de Tronco** quando o CUCM estiver comunicando-se com o Cisco WebEx Meeting Server. Se você não estiver utilizando o Cisco WebEx Meeting Service com áudio CUCM SIP, você pode selecionar a caixa de diálogo **Terminação de Ponto de Mídia Requerido** enquanto estiver fornecendo serviços telefônicos que utilizem infraestrutura PBX de terceiros.

Etapa 8 Selecione **Salvar**.

Etapa 9 Selecione **Redefinir** e depois selecione **Redefinir e reiniciar** na janela pop-up.
Você deve redefinir o tronco SIP para completar a sua configuração.

Configurar um grupo de rota

Etapa 1 Inicie sessão em http://ccm-server/, onde *ccm-server* é o nome de domínio totalmente qualificado ou o endereço IP do servidor Cisco Unified Communications Manager.

Etapa 2 Selecione **Cisco Unified CM Administration**.

Etapa 3 Selecione **Roteamento de chamada** > **Rotear/Buscar** > **Grupo de rotas**.

Etapa 4 Selecione **Adicionar novo**.

Etapa 5 Configure os seguintes campos

- Nome do grupo de rotas—Insira um nome para o seu grupo de rotas.
- Algoritmo de distribuição. Selecione **Circular** no menu suspenso.

Observação Ao selecionar **Circular**, você permite que o CUCM distribua uma chamada para usuários inativos ou disponíveis a partir do membro (N+1)º de um grupo de rotas, onde o membro Nº é o membro ao qual o CUCM recentemente estendeu uma chamada. Se o membro Nº é o último membro de um grupo de rotas, o CUCM distribui uma chamada a partir da parte superior do grupo de rotas.

- Encontre dispositivos para adicionar ao grupo de rotas— Selecione **Tronco SIP do ponto balanceador de carga** na lista de dispositivos disponíveis. Em seguida, selecione **Adicionar ao grupo de rotas**.

Observação Não altere nenhum outro campo nesta página. Deixe-os em suas configurações padrão.

Etapa 6 Selecione **Salvar**.

Próximos passos

Crie uma lista de rotas para o seu grupo de rotas. Prossiga para Configurar uma lista de rota, na página 122.

Configurar uma lista de rota

Etapa 1 Inicie sessão em http://ccm-server/, onde *ccm-server* é o nome de domínio totalmente qualificado ou o endereço IP do servidor Cisco Unified Communications Manager.

Etapa 2 Selecione **Cisco Unified CM Administration**.

Etapa 3 Selecione **Roteamento de chamada** > **Rotear/Buscar** > **Lista de rotas**.

Etapa 4 Selecione **Adicionar novo**.

Etapa 5 Configure os seguintes campos

- Nome—Insira um nome para a lista de rotas.
- Grupo Cisco Unified Communications Manager—Selecione **Padrão** no menu suspenso.

Observação Não altere quaisquer outros campos nesta página; deixe os campos para suas configurações padrões.

Etapa 6 Selecione **Salvar**.

Etapa 7 Selecione **Adicionar grupo de rotas**.
A página **Configuração dos Detalhes da Lista de Rotas** é exibida.

Etapa 8 Selecione o grupo de rotas previamente configurado do menu suspenso **Grupo de rotas** e selecione **Salvar**.
A página **Configuração da lista de rotas** é exibida.

Etapa 9 Selecione **Salvar**.

Próximos passos

Configure um padrão de rota para sua lista de rotas. Prossiga para Configurar um Padrão de Rota, na página 123.

Configurar um Padrão de Rota

Etapa 1 Inicie sessão em http://ccm-server/, onde *ccm-server* é o nome de domínio totalmente qualificado ou o endereço IP do servidor Cisco Unified Communications Manager.

Etapa 2 Selecione **Cisco Unified CM Administration**.

Etapa 3 Selecione **Roteamento de chamada** > **Rotear/Buscar** > **Padrão de rotas**.

Etapa 4 Selecione **Adicionar novo**.

Etapa 5 Configure os seguintes campos

- **Padrão de rota**—Insira um nome para o padrão de rota.

  Observação Adicione um padrão de rota para cada grupo de Discagem Múltipla. Registre este nome, pois você deve inseri-lo na página de Administração **Configurações** > **Áudio** > **Grupo de discagem múltipla** ao criar um grupo de discagem múltipla.

- **Partição de rota**—Selecione uma partição de rota que é acessível através de telefones ou dispositivos que podem chamar o Cisco WebEx Meetings Server. Se isto define para **< Nenhum >**, qualquer dispositivo configurado no CUCM seria capaz de chamar o Cisco WebEx Meetings Server. Para obter mais informações, consulte "Configuração do Espaço de pesquisa de chamada" no *Guia de Administração do Cisco Unified Communications Manager* ou "Espaços de pesquisa de chamada e Partições" no *Guia do Sistema do Cisco Unified Communications Manager*.
- **Porta de entrada/Lista de rotas**—Selecione a lista de rotas previamente configurada do menu suspenso.

Observação Não altere quaisquer outros campos nesta página; deixe estes campos para suas configurações padrões.

Etapa 6 Selecione **Salvar**.

Configurar um padrão de rota SIP

Etapa 1 Inicie sessão em http://ccm-server/, onde *ccm-server* é o nome de domínio totalmente qualificado ou o endereço IP do servidor Cisco Unified Communications Manager.

Etapa 2 Selecione **Cisco Unified CM Administration**.

Etapa 3 Selecione **Roteamento de chamada** > **Padrão de rota SIP**.

Etapa 4 Selecione **Adicionar novo**.

Etapa 5 Configure os seguintes campos

- Partição de Rota—Selecione uma partição de rota que está incluída no espaço de pesquisa de chamada que está configurado como o Reencaminhamento do Espaço de Pesquisa de Chamada da seção "Configuração de um tronco SIP para um Ponto de Aplicativo" acima. Se isto define para **< Nenhum >**, então o Reencaminhamento do Espaço de Pesquisa de Chamada configurado para o tronco SIP para um ponto de aplicativo deve ser definido para **< Nenhum >**. Para obter mais informações, consulte "Configuração do Espaço de pesquisa de chamada" no *Guia de*

Administração do Cisco Unified Communications Manager ou "Espaços de pesquisa de chamada e Partições" no *Guia do Sistema do Cisco Unified Communications Manager*.

- Uso padrão—Selecione **Roteamento do endereço de IP**.
- Padrão IPv4—Insira o endereço de IP do ponto de aplicativo. Consulte a tabela de Configuração SIP na página Administração de Áudio do Site do endereço de IP.
- Tronco SIP—Selecione o tronco SIP previamente configurado para o ponto de aplicativo a partir do menu suspenso.

Observação Não altere quaisquer outros campos nesta página; deixe estes campos para suas configurações padrões.

Etapa 6 Selecione **Salvar**.

Compatibilidade de recursos e de suporte do CUCM

Compatibilidade de recursos do CUCM

O Cisco WebEx Meetings Server (CWMS) suporta o Cisco Unified Call Manager (CUCM) 8.6 ou 9.0 sem TLS/SRTP e o CUCM 9.1, 10.0, 10.5, 11.0(1a) ou 11.5(1)SU1.

Importante As conexões TLS entre o CUCM e o CWMS falham com as versões do CUCM que não suportam certificados que são assinados com um algoritmo de assinatura SHA256 com criptografia RSA.

Atualize o CUCM para uma versão que suporta este algoritmo de assinatura ou obtenha um certificado de terceiros que está assinado com SHA1 com a criptografia RSA. De acordo com a recomendação mais recente do Instituto Nacional de Padrões e Tecnologia (NIST), o SHA1 não deve mais ser usado para gerar assinatura digital, pois esta é uma vulnerabilidade da segurança.

A tabela a seguir fornece compatibilidade de recursos para as versões suportadas do CUCM. A capacidade do sistema do Cisco WebEx Meetings Server não é afetada pelas opções de configuração.

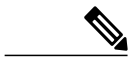
Observação O CWMS não suporta as versões CUCM não listadas ou outros aplicativos de gerenciamento proxy SIP de terceiros.

Tabela 5: Compatibilidade de recursos para as versões suportadas do CUCM

Recurso	Pré-condições/observações
Chamada de saída (IPv6)	Configure o CWMS com endereços de IPv6 durante o processo de instalação.
Chamada de entrada (IPv6)	Configure o CWMS com endereços de IPv6 durante o processo de instalação.

Recurso	Pré-condições/observações
TLS/SRTP	Configure certificados de segurança do sistema CWMS.
RFC2833	Selecione essa opção durante a configuração do tronco SIP do CUCM.
KPML	Selecione essa opção durante a configuração do tronco SIP do CUCM.
Manutenção de atividade — enviando CWMS	Realizada utilizando a mensagem de OPÇÕES SIP.
Manutenção de atividade — recebendo CWMS	Realizada utilizando a mensagem de OPÇÕES SIP.
Qualidade de serviço	Pacotes de controle.
TCP	Certifique-se de que as portas padrão sejam: 5060 para pontos balanceadores de carga de conferência; 5062 para pontos de aplicativos de conferência.
TLS	Certifique-se de que as portas padrão sejam: 5061 para pontos balanceadores de carga de conferência; 5063 para pontos de aplicativos de conferência.
UDP	Certifique-se de que as portas padrão sejam: 5060 para pontos balanceadores de carga de conferência; 5062 para pontos de aplicativos de conferência.
Certificados autoassinados	N/D
Certificados de terceiros	N/D

Recursos de chamadas telefônicas compatíveis



Observação O software do CUCM 9.0 que é parte do produto BE6K (Business Edition 6000) é suportado pelo CWMS.

- Chamada retida
- Chamada não retida
- A chamada com identificação é exibida no EP
- O nome que está chamando é exibido no EP
- Transferência de chamadas (IPv4 para IPv4)
- Transferência de chamadas (IPv6 para IPv4)
- Transferência de chamadas (IPv4 para IPv6)
- Transferência de chamadas (IPv6 para IPv6)

Recursos de mídia de telefonia

O CWMS suporta participantes com os codecs G.711, G.722 e G.729 ao mesmo tempo. Alterar a configuração codec não afeta o desempenho do sistema. Tamanhos de pacotes suportadas no CWMS:

- 10, 20 ou 30ms para codecs de áudio g.711
- 20ms para codec de áudio g.722
- 10, 20, 30, 40, 50 ou 60ms para codecs de áudio g.729

Recurso	G.711	G.722	G.729
Compressão de ruído	Sim	Sim	Sim
Ruído de conforto	Sim	Não	Não
Cancelamento de eco	Não	Não	Não
Ocultação de perda de pacotes	Sim	Sim	Não
Controle de ganho automático	Sim	Sim	Sim
Qualidade de serviço	Sim	Sim	Sim

Observação Todos os avisos de áudio personalizados, incluindo as instruções de discagem múltipla, são: 8KHz, 16-bit, 64kbps, momo, CCITT u-law (G.711).

Compatibilidade de extremidade de áudio

Você pode usar qualquer extremidade com base em padrões de áudio que se conecta ao Cisco Unified Communications Manager para participar de uma reunião WebEx. As extremidades de áudio suportadas incluem os Telefones IP da Cisco, extremidades do Telepresence e os dispositivos PSTN, como telefones celulares e telefones fixos. Muitas extremidades de áudio suportam a conectividade de áudio e de vídeo. No entanto, apenas a conectividade de áudio para o Cisco WebEx Meetings Server é suportada.

Para permitir que usuários de fora da organização participem de reuniões WebEx usando dispositivos PSTN, sua empresa deve implantar Gateways Analógicos para VoIP, tais como Roteadores de Serviços Integrados (ISR) da Cisco. Os telefones IP listados abaixo foram testados com o Cisco WebEx Meetings Server:

- Cisco 7960
- Cisco 7970
- Cisco 7971
- Cisco 7940
- Cisco 9951
- Cisco 9971

- Cisco 7980 (Tandberg)
- Cisco 7975
- Cisco E20
- Cisco Telepresence (CTS 1100)
- Cisco Ip Communicator
- Telefone com vídeo Lifesize
- Tandberg 1000
- Tandberg 1700
- Polycom
- Cisco Cius
- C20
- EX 60
- EX 90

Outros terminais compatíveis com o Cisco UC também devem funcionar normalmente. Para obter uma lista de telefones IP do Cisco Unified suportados pelo Cisco Unified Communications Manager e os pacotes de dispositivos disponíveis para cada modelo, consulte Recurso de telefone IP do Cisco Unified e Matriz de compatibilidade do pacote de dispositivos do Cisco Unified Communications Manager.

CAPÍTULO 6

Sobre os downloads de aplicativos

Você pode implantar esses aplicativos CWMS em massa usando as ferramentas disponíveis para você no site de Administração. Os aplicativos disponíveis para download incluem o seguinte:

- Aplicativo WebEx Meetings—O aplicativo principal para agendamento, atendimento ou organização de reuniões.

  A execução do aplicativo WebEx Meetings em um sistema operacional virtualizado não é suportada.

  Se um usuário não tiver o aplicativo WebEx Meetings instalado, ele será baixado ao PC na primeira vez que um usuário entrar em uma reunião. Isso pode ser configurado para ser feito sob demanda ou em silêncio. O usuário tem a opção de usar o aplicativo Cisco WebEx Meetings durante a duração da reunião e tê-lo removido quando a reunião terminar ou executar uma instalação do aplicativo para acelerar o processo de iniciar ou participar de reuniões futuras. Isso pode falhar porque o usuário não tem privilégios de administrador.

- Ferramentas de Produtividade WebEx—Fornece uma interface entre outros aplicativos, como o Microsoft™ Outlook®, permitindo o gerenciamento de reuniões, por meio desses aplicativos.

  Depois de uma atualização para um sistema, as versões antigas das ferramentas de produtividade WebEx devem ser removidas e a versão mais recente instalada.

- Reprodutor de gravações de rede WebEx—Reproduz as gravações de reuniões. Isso pode incluir qualquer material exibido durante a reunião.

No CWMS, o instalador .MSI dos aplicativos está disponível na página **Admin** > **Configurações** > **Downloads**. Consulte "Baixar aplicativos do site de administração" no Guia de planejamento CWMS para obter mais informações.

Recomendamos que você mova os aplicativos aos computadores dos usuários off-line, antes de informar a esses usuários finais que as contas foram criadas a eles. Isso garante que os usuários podem iniciar e participar de reuniões e reproduzir gravações de rede na primeira vez que iniciarem sessão.

Onde os usuários têm privilégios de administrador, você pode permitir que eles baixem os aplicativos da página **Downloads** do usuário final e permitir que eles mesmos instalem os aplicativos. Nenhuma ação adicional do administrador é necessária.

Ao **atualizar** para o Cisco WebEx Meetings Server Versão 1.5MR3 ou superior em um ambiente bloqueado onde os PCs dos usuários não têm privilégios de administrador, antes de iniciar o procedimento de atualização, mova a nova versão do aplicativo WebEx Meetings a todos os PCs dos usuários.

- Fazer download de aplicativos no site da Administração, página 130

- Conteúdo dos arquivos ZIP de aplicação, página 131
- Desenvolvimento em massa de Ferramentas de produtividade Cisco WebEx, página 134
- Implantação em massa do aplicativo de reuniões, página 141
- Implantação em massa do reprodutor de gravações de rede, página 145
- Reconfigurar suas configurações depois de realizar uma atualização, página 149

Fazer download de aplicativos no site da Administração

Você pode configurar o sistema para que os administradores possam mover os aplicativos do desktop do Cisco WebEx aos usuários ou que você possa permitir que os usuários realizem o próprio download.

Etapa 1 Conectar ao site de Administração.
Em um sistema com Múltiplos Centros de Dados, o DNS determina qual Painel do centro de dados é exibido. Use este Painel para gerenciar todos os centros de dados no sistema.

Etapa 2 Selecione **Configurações** > **Downloads**.

Etapa 3 Selecione os seus métodos de download:

- Permita que usuários baixem aplicativos da área de trabalho WebEx.
  Use esta opção para permitir que os usuários que têm permissões de administrador para seus PCs gerenciem os aplicativos de conferência.
- Mova manualmente as aplicações do desktop WebEx para o desktop do usuário.
  Use esta opção para habilitar a conferência para usuários que não têm permissões de administrador para seus PCs.

  Se você selecionou esta opção, a janela será expandida para mostrar as seções de Reuniões Cisco WebEx, Ferramentas de Produtividade e do reprodutor de gravações de rede.

Etapa 4 (Opcional) Selecione **Atualização automática das Ferramentas de Produtividade WebEx** para configurar atualizações periódicas e automáticas das Ferramentas de Produtividade WebEx. (**Padrão**: Marcado.)

Etapa 5 Se você selecionou **Mover manualmente os aplicativos do desktop WebEx para o desktop do usuário**:

a) Na seção de Reuniões WebEx, selecione **Download** e salve o arquivo ZIP no seu sistema.
b) Na seção Ferramentas de Produtividade, selecione **Download** e salve o arquivo no seu sistema.
c) Na seção do Reprodutor de gravações de rede WebEx, selecione **Download** e salve o arquivo ZIP no seu sistema.

Etapa 6 Selecione **Salvar** para salvar suas configurações de Download.
Isto é especialmente importante se você estiver permitindo aos usuários baixar aplicativos de desktop WebEx.

Etapa 7 (Opcional) Se você selecionou **Mover manualmente os aplicativos do desktop WebEx para o desktop do usuário**:

a) Execute o arquivo baixado.
b) Abra o arquivo ZIP.
   Cada arquivo ZIP contém o instalador do aplicativo para todos os idiomas suportados. Consulte Conteúdo dos arquivos ZIP de aplicação, na página 131 para obter informações sobre o instalador recomendado para uso.
c) Selecione o instalador para sua plataforma e idioma, e o extraia para uma pasta do diretório local.
   O arquivo ZIP contém instaladores MSI para a plataforma Windows em todos os idiomas disponíveis.

A versão do Aplicativo de Reuniões e Ferramentas de Produtividade que se alinha com cada versão do Cisco WebEx Meeting Server pode ser encontrada em Matriz de Compatibilidade das Ferramentas de Produtividade e Aplicativos Cisco WebEx Meetings, na página 197.

Próximos passos

Implante os instaladores MSI, conforme descrito neste capítulo.

Conteúdo dos arquivos ZIP de aplicação

Os arquivos ZIP contêm um instalador de aplicativos para cada idioma.

Chave do idioma de aplicação

O arquivo instalador de aplicativos em inglês em cada arquivo ZIP está sem um sufixo do idioma. O arquivo instalador de aplicativos para cada um dos outros idiomas contém uma abreviatura no nome do arquivo que indica o idioma do aplicativo que ele contém. A tabela lista a abreviatura usada para cada idioma:

Abreviatura	Idioma
BS	Chinês Tradicional
de	Alemão
es	Espanhol da América Latina
Sex	Francês
GB	Chinês Simplificado
it	Italiano
jp	Japonês
ko	Coreano
nl	Holandês
PT	Português
ru	Russo
SP	Espanhol

Conteúdo do arquivo ZIP das ferramentas de produtividade

O arquivo ZIP das ferramentas de produtividade contém os seguintes arquivos. Use a chave na tabela de chaves do Idioma do aplicativo para determinar o idioma de cada arquivo. Observe que não há versão do Mac das ferramentas de produtividade.

- ptools.msi
- ptools_B5.msi
- ptools_DE.msi
- ptools_ES.msi
- ptools_FR.msi
- ptools_GB.msi
- ptools_IT.msi
- ptools_JP.msi
- ptools_KO.msi
- ptools_NL.msi
- ptools_PT.msi
- ptools_RU.msi
- ptools_SP.msi

Conteúdo do arquivo ZIP do cliente WebEx Meetings

Use a chave no Chave do idioma de aplicação, na página 131 para determinar o idioma do aplicativo contido em cada arquivo Zip.

Versão 2.7 e posterior	Versão 2.6 e anterior
webexmc.msi.msi	onpremmc.msi
webexmc_allinone.msi	onpremmc_B5.msi
webexmc.msi_B5.msi	onpremmc_DE.msi
webexmc.msi_DE.msi	onpremmc_ES.msi
webexmc.msi_ES.msi	onpremmc_FR.msi
webexmc.msi_FR.msi	onpremmc_GB.msi
webexmc.msi_GB.msi	onpremmc_IT.msi
webexmc.msi_IT.msi	onpremmc_JP.msi
webexmc.msi_JP.msi	onpremmc_KO.msi
webexmc.msi_KO.msi	onpremmc_NL.msi
webexmc.msi_NL.msi	onpremmc_PT.msi

Versão 2.7 e posterior	Versão 2.6 e anterior
webexmc.msi_PT.msi	onpremmc_RU.msi
webexmc.msi_RU.msi	onpremmc_SP.msi
webexmc.msi_SP.msi	webexmc_onprem.dmg (para Mac)
webexmc_onprem.dmg (para Mac)	

Conteúdo do arquivo ZIP do reprodutor de gravação de rede

O reprodutor de gravações de rede só está disponível para a implantação de massa e download se você selecionou **Permitir que usuários baixem aplicativos do desktop WebEx** na página Downloads. Consulte *Definição das configurações de download* no *Guia de administração do Cisco WebEx Meetings Server* para obter mais informações.

O arquivo ZIP do reprodutor de gravação de rede contém os seguintes arquivos. Use a chave na tabela de chaves do Idioma do aplicativo para determinar o idioma de cada arquivo.

- nbr2player_onprem.msi
- nbr2player_onprem_B5.msi
- nbr2player_onprem_DE.msi
- nbr2player_onprem_ES.msi
- nbr2player_onprem_FR.msi
- nbr2player_onprem_GB.msi
- nbr2player_onprem_IT.msi
- nbr2player_onprem_JP.msi
- nbr2player_onprem_KO.msi
- nbr2player_onprem_NL.msi
- nbr2player_onprem_PT.msi
- nbr2player_onprem_RU.msi
- nbr2player_onprem_SP.msi
- webexnbrplayer_intel.dmg (para Mac)

Desenvolvimento em massa de Ferramentas de produtividade Cisco WebEx

Esta seção descreve as tarefas envolvidas na instalação das Ferramentas de Produtividade WebEx da Cisco usando o pacote `ptools.ms`. Instalação de um único computador e instalações de grande escala podem ser realizadas utilizando o Microsoft Systems Management Server 2003 (SMS).

A versão das Ferramentas de Produtividade que se alinha com cada versão do Cisco WebEx Meeting Server pode ser encontrada em Matriz de Compatibilidade das Ferramentas de Produtividade e Aplicativos Cisco WebEx Meetings, na página 197.

Instalação silenciosa das Ferramentas de Produtividade utilizando a linha de comando

Os administradores podem iniciar sessão no computador de um usuário e instalar as Ferramentas de Produtividade WebEx usando o modo silencioso.

Antes de iniciar

Antes de instalar uma versão de manutenção ou atualizar o sistema para uma versão mais recente, as versões anteriores das Ferramentas de Produtividade Cisco WebEx devem ser desinstaladas.

Etapa 1 Inicie a sessão no computador do usuário.

Etapa 2 Baixe o pacote MSI no disco rígido do computador.

Etapa 3 Abra o prompt de comando do Windows.
No Windows 7 ou Windows Vista, você deve usar o executar como administrador para abrir a janela do prompt.

Etapa 4 Execute o comando MSI para instalar as Ferramentas de Produtividade WebEx silenciosamente.

Exemplo:
msiexec.exe /q /i "ptools.msi" SITEURL="https://sample.webex.com" OI=1 MSN=1

Nome do parâmetro	Valor	Descrição
OI	1	Habilitar integração com o Outlook
	0 (padrão)	Desabilitar integração com o Outlook
MSN	1	Habilitar a integração do serviço de mensagens instantâneas para o Microsoft Office Communicator e Lync
MSN	0 (padrão)	Desabilitar a integração do serviço de mensagens instantâneas para o Microsoft Office Communicator e Lync

Etapa 5 Reinicie o computador.

Remoção silenciosa das Ferramentas de Produtividade usando a interface da linha de comando

Os administradores podem iniciar sessão no computador de um usuário e desinstalar as Ferramentas de Produtividade usando o modo silencioso.

Etapa 1 Inicie a sessão no computador do usuário.

Etapa 2 Baixe o pacote MSI no disco rígido do computador.

Etapa 3 Abra o prompt de comando do Windows.
No Windows 7 ou Windows Vista, você deve usar o executar como administrador para abrir a janela do prompt.

Etapa 4 Desinstale todos os componentes do pacote MSI inserindo ptools.msi o comando msiexec.exe /q /x "ptools.msi".

Limitações para a instalação silenciosa de aplicativos CWMS ao usar SMS

As seguintes limitações se aplicam quando você executa uma instalação silenciosa usando o Microsoft Systems Management Server 2003 (SMS):

- O modo de SMS por usuário não pode ser suportado.
- Se o administrador de SMS desejar adicionar um recurso para as Ferramentas de produtividade WebEx, ele deverá executar o comando **REMOVER** primeiro e, depois, executar o comando**ADDSOURCE**, mesmo que o recurso não tenha sido instalado antes.
- Se um usuário fizer logon em um computador com desktop remoto enquanto o administrador anuncia o pacote, ele deverá reiniciar o computador para que as Ferramentas de Produtividade WebEx funcionem normalmente.
- É possível realizar a implantação em massa, mas cada usuário deve inserir as informações credenciais.
- Antes de atualizar para uma versão de manutenção ou atualizar para uma versão mais recente, os usuários devem desinstalar as Ferramentas de Produtividade Cisco WebEx. Após a atualização, você pode mover manualmente as Ferramentas de Produtividade aos seus usuários ou os usuários podem baixar as Ferramentas de Produtividade da página **Downloads**.
- Se você estiver utilizando a integração Lync, depois de uma instalação silenciosa, os usuários devem reiniciar seus computadores para que todas as integrações do serviço de mensagens instantâneas funcione corretamente.

Anunciando as Ferramentas de Produtividade WebEx usando o programa automático por sistema de SMS

Após a atualização, você pode usar o site de Administração para mover manualmente as Ferramentas de Produtividade aos seus usuários ou permitir que os usuários baixem as Ferramentas de Produtividade da página **Downloads** do usuário final.

Consulte a seção "Definição das configurações de download" *no guia de administração do Cisco WebEx Meetings Server* para obter mais informações.

Se você é o administrador do Microsoft Systems Management Server 2003 (SMS), você pode anunciar as Ferramentas de Produtividade Cisco WebEx usando o programa automático por sistema de SMS.

Etapa 1 Criar um pacote a partir da definição. Consulte Criar um pacote a partir de uma definição, na página 140 para obter mais informações.

Etapa 2 Altere as opções do programa para **Automático por sistema** antes do anúncio:

a) Abra o console SMS do administrador e selecione **Banco de dados do site** > **Pacotes** > **Cisco WebEx LLC Ferramentas de Produtividade Cisco WebEx 2.82** > **Programas**.

b) Clique com o botão direito do mouse na opção Automático por sistema e selecione **Propriedades** para abrir a caixa de diálogo **Propriedades do programa automático por sistema**.

c) Selecione a **guia** Ambiente.

- Para a opção **O programa pode executar**, selecione **Somente quando o usuário está registrado em**.
- Para a opção **Modo de execução**, selecione **Executar com direitos administrativos**. (Não ativar **Permitir que os usuários possam interagir com este programa**.)

d) Selecione a aba **Geral**.

e) Adicionar um parâmetro adicional para a opção de linha de comando para especificar algumas opções para as Ferramentas de produtividade Cisco WebEx:

- SITEURL=″http://sample.webex.com″ especifica a URL do site WebEx usada pela sua empresa.
- Sinalizadores de Ferramentas de Produtividade especifica qual componente é habilitado para as Ferramentas de Produtividade WebEx. Os parâmetros devem ser maiúsculas e o valor padrão é 0 (desabilitado).

  No exemplo a seguir, a linha de comando inicial é msiexec.exe /q ALLUSERS=2 /m MSIZWPBY /i "ptools.msi".
- Acrescentar sinalizadores de Ferramentas de produtividade e parâmetros à linha de comando: msiexec.exe /q ALLUSERS=2 /m MSIZWPBY /i "ptools.msi" SITEURL="https://sample.webex.com" OI=1MSN=1.

Observação Consulte a tabela de parâmetros em Instalação silenciosa das Ferramentas de Produtividade utilizando a linha de comando, na página 134 para obter definições de parâmetros.

Etapa 3 Anuncie o programa.

a) Abra o console SMS do administrador e selecione **Banco de dados do site** > **Pacotes** > **Cisco WebEx LLC Ferramentas de Produtividade Cisco WebEx 2.82 em Inglês** > **Programs**.

b) Clique com o botão direito do mouse na opção **Automático por sistema**.

c) Selecione **Todas as tarefas** > **Distribuir software**.

d) Selecione **Avançar** no **Assistente de distribuição do programa**.

e) Selecione o servidor SMS e selecione **Avançar**.
f) Selecione a coleção e selecione **Avançar**.
g) Digite o nome do anúncio no campo **Nome** e selecione **Avançar**.
h) Especifique se o anúncio deverá se aplicar a subcoleções e selecione **Avançar**.
i) Especifique quando o programa será anunciado e selecione **Avançar**.
j) Especifique se deve ou não atribuir o programa e selecione **Próxima**.
k) Selecione **Concluir** na página **Concluindo o Assistente de distribuição do programa**.
l) Vá até o diretório \Site Database\System Status\Advertisement Status e verifique o status do anúncio.
Se você habilitar a notificação, o usuário verá uma mensagem indicando que o programa atribuído será executado após o anúncio do programa. O programa atribuído executará silenciosamente.

Remoção dos componentes das Ferramentas de produtividade usando o programa automático por sistema de SMS

Execute o seguinte procedimento para remover as Ferramentas de Produtividade utilizando o Microsoft Systems Management Server 2003 (SMS):

Etapas de Resumo

1. Crie um novo programa e copie todas as opções do "programa automático por sistema", como descrito em Anunciando as Ferramentas de Produtividade WebEx usando o programa automático por sistema de SMS, na página 136 e, em seguida, atualize a linha de comando:
2. Anuncie o programa para a coleção especificada de máquinas de trabalho no domínio. Consulte Limitações para a instalação silenciosa de aplicativos CWMS ao usar SMS, na página 135 para obter mais informações.

Etapas Detalhadas

Etapa 1 Crie um novo programa e copie todas as opções do "programa automático por sistema", como descrito em Anunciando as Ferramentas de Produtividade WebEx usando o programa automático por sistema de SMS, na página 136 e, em seguida, atualize a linha de comando:

a) Abra o console SMS do administrador e selecione **Banco de dados do site** > **Pacotes** > **Cisco WebEx LLC Ferramentas de Produtividade Cisco WebEx 2.82** > **Programas**.
b) Clique com o botão direito do mouse na área em branco e selecione **Novo** > **Programa**.
c) Digite o nome do programa e a linha de comando padrão.
d) Na caixa de diálogo **Propriedades**, selecione a guia **Ambiente**.

- Para a opção **O programa pode executar**, selecione **Somente quando o usuário está registrado em**.
- Para a opção **Modo de execução**, selecione **Executar com direitos administrativos**. (Não ative **Permitir que os usuários possam interagir com este programa**).

e) Atualize a linha de comando na guia **Geral**.
f) Acrescentar REMOVER à linha de comando e especificar os recursos que precisam ser removidos.

Exemplo:
Se deseja remover OI, digite o seguinte comando: msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" REMOVE="OI"
O valor de PTIM é para integração do CWMS com serviços de mensagem instantânea. Exemplo: msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" REMOVE="PTIM"

Etapa 2 Anuncie o programa para a coleção especificada de máquinas de trabalho no domínio. Consulte Limitações para a instalação silenciosa de aplicativos CWMS ao usar SMS, na página 135 para obter mais informações.
As Ferramentas de Produtividade do Cisco WebEx serão atualizadas nestas máquinas silenciosamente.

Adicionando Ferramentas de Produtividade usando o programa automático por sistema de SMS

Para adicionar um componente às Ferramentas de Produtividade, você deve executar primeiro REMOVER e, em seguida, ADDSOURCE, ainda que o componente não tenha sido instalado antes.

Etapa 1 Crie um novo programa chamado `Add-phase1`, copie todas as opções do "programa automático por sistema" e, em seguida, atualize a linha de comando:

a) Abra o console SMS do administrador e selecione **Banco de dados do site** > **Pacotes** > **Cisco WebEx LLC Ferramentas de Produtividade Cisco WebEx 2.82** > **Programas**.
b) Clique com o botão direito do mouse na área em branco e selecione **Novo** > **Programa**.
c) Digite o nome do programa e a linha de comando padrão.
d) Na caixa de diálogo Propriedades, selecione a guia **Ambiente**.

- Para a opção **O programa pode executar**, selecione **Somente quando o usuário está registrado em**.
- Para a opção **Modo de execução**, selecione **Executar com direitos administrativos**. (Não ativar **Permitir que os usuários possam interagir com este programa**.)

e) Atualize a linha de comando na guia **Geral**.
f) Acrescente REMOVER à linha de comando e especifique os recursos que precisam ser adicionados.

Exemplo:
Se você quiser adicionar OI e PITM (o valor PITM é da integração WebEx para os serviços de mensagens instantâneas), você precisa REMOVÊ-LOS primeiro, mesmo que eles não estejam instalados: msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" REMOVE="OI,PTIM"

Etapa 2 Anuncie o programa para a coleção especificada de máquinas de trabalho no domínio. Consulte Limitações para a instalação silenciosa de aplicativos CWMS ao usar SMS, na página 135 para obter mais informações.

Etapa 3 Crie um segundo nome de programa, "Add-phrase2" e copie todas as opções do "programa automático por sistema" e, em seguida, atualize a linha de comando:

a) Abra o console SMS do administrador e selecione **Banco de dados do site** > **Pacotes** > **Cisco WebEx LLC Ferramentas de Produtividade Cisco WebEx 2.82** > **Programas**.

b) Clique com o botão direito do mouse na área em branco e selecione **Novo** > **Programa**.
c) Digite o nome do programa e a linha de comando padrão.
d) Na caixa de diálogo Propriedades, selecione a guia **Ambiente**.

- Para a opção **O programa pode executar**, selecione **Somente quando o usuário está registrado em**.
- Para a opção **Modo de execução**, selecione **Executar com direitos administrativos**. (Não ative **Permitir que os usuários possam interagir com este programa**).

e) Na caixa de diálogo Propriedades, selecione a guia **Avançado**.
f) Ativar **Executar outro programa primeiro** e selecionar programa **Add-phase1**.
g) Atualize a linha de comando na guia **Geral**.
h) Acrescentar ADDSOURCE à linha de comando e especificar os recursos que precisam ser adicionados.

Exemplo:
Se você quiser adicionar OI e PITM, use este comando de exemplo: msiexec.exe /q ALLUSERS=2 /m MSII5HK3 /i "ptools.msi" ADDSOURCE="OI,PTIM" OI=1 MSN=1

Etapa 4 Anuncie o programa para a coleção especificada de máquinas de trabalho no domínio. Consulte Limitações para a instalação silenciosa de aplicativos CWMS ao usar SMS, na página 135 para obter mais informações.
As Ferramentas de Produtividade Cisco WebEx são atualizadas nessas máquinas silenciosamente.

Desinstalando as Ferramentas de produtividade usando o programa de desinstalação por sistema de SMS

O administrador de SMS pode desinstalar as Ferramentas de Produtividade Cisco WebEx usando o programa de desinstalação por sistema de SMS.

Etapa 1 Use o pacote de instalação de SMS criado em Criar um pacote a partir de uma definição, na página 140.

Etapa 2 Anuncie o programa de desinstalação por sistema para desinstalar as Ferramentas de produtividade Cisco WebEx.
As Ferramentas de produtividade Cisco WebEx serão desinstaladas em estas máquinas silenciosamente.

Publicidade do programa para atualizar para a nova versão das Ferramentas de produtividade WebEx

Executar o seguinte procedimento para anunciar o programa de atualização para a nova versão das Ferramentas de produtividade Cisco WebEx.

Antes de iniciar

Antes de instalar uma versão de manutenção ou atualizar o seu sistema para uma versão mais recente, os usuários devem desinstalar as Ferramentas de Produtividade Cisco WebEx em execução nos desktops. Após a atualização, você pode usar o site de Administração para mover manualmente as Ferramentas de Produtividade aos seus usuários ou os usuários podem baixar as Ferramentas de Produtividade da página **Downloads** do usuário final.

Inicie sessão no site da Administração, selecione **Configurações** > **Downloads** e desabilite as seguintes configurações:

- **Atualização automática das ferramentas de produtividade Cisco WebEx**
- **Permitir que usuários baixem aplicativos da área de trabalho WebEx**

Etapa 1 Crie um novo pacote de instalação SMS usando o pacote MSI das Ferramentas de Produtividade WebEx.
Consulte Criar um pacote a partir de uma definição, na página 140 para obter mais informações.

Etapa 2 Alterar as opções do programa para **Automático por sistema** antes de anúncio.
Consulte Adicionando Ferramentas de Produtividade usando o programa automático por sistema de SMS, na página 138 para obter mais informações.

Etapa 3 Anuncie o programa. Consulte Adicionando Ferramentas de Produtividade usando o programa automático por sistema de SMS, na página 138 para obter mais informações.
As antigas Ferramentas de produtividade Cisco WebEx são removidas e as novas Ferramentas de produtividade Cisco WebEx serão instaladas silenciosamente.

Criar um pacote a partir de uma definição

Etapa 1 Abra o console SMS do administrador e selecione **Banco de dados do site** > **Pacote**.

Etapa 2 Clique com o botão direito do mouse em **Pacote**.

Etapa 3 Selecione **Novo** > **Pacote da definição**.

Etapa 4 No assistente **Criar pacote da definição**, selecione **Próximo**.

Etapa 5 Selecione **Procurar** para localizá-lo, selecione o pacote MSI das Ferramentas de produtividade WebEx e, em seguida, selecione **Avançar**.

Etapa 6 Selecione **Sempre obter arquivos de um diretório de origem** e, em seguida, selecione **Próximo.**

Etapa 7 Selecione a localização do diretório de origem e clique em **Próximo**.

Etapa 8 Selecione **Finalizar**.

Etapa 9 Selecione **Banco de dados do site** > **Pacotes** > **Cisco WebEx LLC Ferramentas de Produtividade Cisco WebEx 2.82 em Inglês** > **Programas**.
Há seis programas disponíveis.

Implantação em massa do aplicativo de reuniões

Esta seção foi projetada para ajudar a sua organização a entender as tarefas envolvidas na instalação do aplicativo Cisco WebEx Meetings. Esta seção é um guia exaustivo que abrange diversos tipos de instalações, incluindo uma instalação para um único computador e instalações em grande escala, usando o Microsoft Systems Management Server 2003 (SMS).

Observação "Instalação silenciosa" significa que o aplicativo pode ser implantado em silêncio, mas a configuração do usuário final é necessária.

Instalar o Cisco WebEx Meetings

Antes de iniciar

Os seguintes pré-requisitos aplicam-se à instalação do Cisco WebEx Meetings:

- Instalar o pacote MSI do Cisco WebEx requer privilégios de administrador. O pacote MSI é instalado para a pasta padrão de Programas do SO que requer privilégios de administrador para acessar.
- O pacote MSI do Cisco WebEx é desenvolvido para o Windows Installer Service 2.0 ou superior. Se a máquina local estiver configurada com uma versão mais antiga, uma mensagem de erro é exibida informando ao usuário que uma versão mais recente do Windows Installer Service é necessária. Ao executar o pacote MSI, o usuário será avisado com uma interface básica MSI.

Etapa 1 Inicie o instalador no computador do usuário.
O assistente de instalação é exibido com uma mensagem introdutória.

Etapa 2 Selecione **Próximo** nas seguintes caixas de diálogo até chegar à caixa de diálogo de instalação.

Etapa 3 Selecione **Instalar**.

Etapa 4 Selecione **Concluir** quando a instalação estiver concluída.

Desinstalar Cisco WebEx Meetings Localmente

Você pode iniciar a sessão no computador de um usuário e desinstalar o aplicativo Cisco WebEx Meetings no Painel de Controle ou na pasta WebEx no disco rígido local.

Antes de iniciar

O aplicativo Cisco WebEx Meetings está instalado no computador de um usuário.

Etapa 1 Inicie a sessão no computador do usuário.

Etapa 2 Apague o aplicativo Cisco WebEx Meeting utilizando um dos seguintes métodos:

- Selecione **Iniciar** > **Painel de controle** > **Programas e recursos**. Na lista de programas, selecione **Cisco WebEx Meetings** e então **Desinstalar/Modificar**.
- Selecione **Iniciar** > **Computador** > **Sistema (C:)** > **Pasta de dados de programa** > **Pasta WebEx**. Clique com o botão direito do mouse em **atcliun.exe** e selecione **Apagar**.

Observação Quando você desinstalada o atcliun.exe da pasta WebEx, ambas as versões local e na nuvem do aplicativo Cisco WebEx Meetings serão removidas, se ambas as versões do aplicativo foram salvas no disco rígido local do usuário. No entanto, quando você exclui o aplicativo usando o Painel de Controle, apenas a versão presencial do aplicativo é excluída.

O aplicativo Cisco WebEx Meetings está desinstalado do computador de um usuário.

Instalação silenciosa do aplicativo Meetings usando a linha de comando

Os administradores podem iniciar sessão no computador de um usuário e instalar o aplicativo WebEx Meetings usando o modo silencioso.

Etapa 1 Inicie a sessão no computador do usuário.

Etapa 2 Baixe o pacote MSI no disco rígido do computador.

Etapa 3 Abra o prompt de comando do Windows.
No Windows 7 ou Windows Vista, você deve usar o executar como administrador para abrir a janela do prompt.

Etapa 4 Insira o comando MSI para instalar aplicativos Cisco WebEx Meeting silenciosamente.

Exemplo:
Insira msiexec /i onpremmc.msi /qn.

Etapa 5 Reinicie o computador.

Remoção silenciosa do aplicativo Meetings usando a interface da linha de comando

Os administradores podem iniciar sessão no computador do usuário e desinstalar o aplicativo Meetings usando o modo silencioso.

Etapa 1 Inicie a sessão no computador do usuário.

Etapa 2 Abra o prompt de comando do Windows.
No Windows 7 ou Windows Vista, você deve usar o executar como administrador para abrir a janela do prompt.

Etapa 3 Desinstale todos os componentes do pacote MSI onpremmc.msi inserindo o comando msiexec/x onpremmc.msi/qn.

Limitações para a instalação silenciosa de aplicativos CWMS ao usar SMS

As seguintes limitações se aplicam quando você executa uma instalação silenciosa usando o Microsoft Systems Management Server 2003 (SMS):

- O modo de SMS por usuário não pode ser suportado.
- Se o administrador de SMS desejar adicionar um recurso para as Ferramentas de produtividade WebEx, ele deverá executar o comando **REMOVER** primeiro e, depois, executar o comando**ADDSOURCE**, mesmo que o recurso não tenha sido instalado antes.
- Se um usuário fizer logon em um computador com desktop remoto enquanto o administrador anuncia o pacote, ele deverá reiniciar o computador para que as Ferramentas de Produtividade WebEx funcionem normalmente.
- É possível realizar a implantação em massa, mas cada usuário deve inserir as informações credenciais.
- Antes de atualizar para uma versão de manutenção ou atualizar para uma versão mais recente, os usuários devem desinstalar as Ferramentas de Produtividade Cisco WebEx. Após a atualização, você pode mover manualmente as Ferramentas de Produtividade aos seus usuários ou os usuários podem baixar as Ferramentas de Produtividade da página **Downloads**.
- Se você estiver utilizando a integração Lync, depois de uma instalação silenciosa, os usuários devem reiniciar seus computadores para que todas as integrações do serviço de mensagens instantâneas funcione corretamente.

Anúncio do CWMS usando o programa automático por sistema de SMS

Um administrador do Microsoft Systems Management Server 2003 (SMS) pode anunciar a disponibilidade dos aplicativos Cisco WebEx Meetings usando o programa automático por sistema.

Antes de iniciar

Inicie sessão no site da Administração e configure suas configurações de Download para manualmente mover os aplicativos do desktop WebEx para o computador do usuário. Consulte a seção *Definição das configurações de download* no Guia de administração do Cisco WebEx Meetings Server para obter mais informações.

Etapa 1 Criar um pacote a partir da definição. Consulte Criar um pacote a partir de uma definição, na página 140 para obter mais informações.

Etapa 2 Altere as opções do programa para "Automático por sistema" antes de anunciar:

a) Abra o console SMS do administrador e selecione **Banco de dados do site** > **Pacotes** > **Cisco WebEx LLC Aplicativo Cisco WebEx Meetings em Inglês** > **Programas**.

b) Clique com o botão direito do mouse na opção **Automático por sistema** e selecione **Propriedades** para abrir a caixa de diálogo **Propriedades do programa automático por sistema**.

c) Selecione a **guia** Ambiente.

- Para a opção **O programa pode executar**, selecione **Somente quando o usuário está registrado em**.
- Para a opção **Modo de execução**, selecione **Executar com direitos administrativos**. Não selecione **Permitir que os usuários possam interagir com este programa**.

d) Selecione a aba **Geral**.

e) Adicione um parâmetro adicional para a opção de linha de comando para especificar algumas opções para o aplicativo Cisco WebEx Meetings:

Exemplo:
Por exemplo, a linha de comando inicial é a seguinte: msiexec /i "onpremmc.msi" /qn

Etapa 3 Agora você pode anunciar o programa.

a) Abra o console SMS do administrador e selecione **Banco de dados do site** > **Pacotes** > **Cisco WebEx LLC Aplicativo Cisco WebEx Meetings em Inglês** > **Programas**.

b) Clique com o botão direito do mouse na opção **Automático por sistema**.

c) Selecione **Todas as tarefas** > **Distribuir software**.

d) Selecione **Avançar** no **Assistente de distribuição do programa**.

e) Selecione o servidor SMS e selecione **Avançar**.

f) Selecione a coleção e selecione **Avançar**.

g) Digite o nome do anúncio no campo **Nome** e selecione **Avançar**.

h) Especifique se o anúncio deverá se aplicar a subcoleções e selecione **Avançar**.

i) Especifique quando o programa será anunciado e selecione **Avançar**.

j) Especifique se deve atribuir o programa e selecione **Avançar**.

k) Selecione **Concluir** na página **Concluindo o Assistente de distribuição do programa**.

l) Vá até o diretório \Site Database\System Status\Advertisement Status e verifique o status do anúncio.
Se você habilitar a notificação, o usuário verá uma mensagem indicando que o programa atribuído será executado após o anúncio do programa. O programa atribuído executará silenciosamente.

Desinstalando o aplicativo Cisco WebEx Meetings usando o programa de desinstalação por sistema de SMS

O administrador de SMS pode desinstalar o aplicativo Cisco WebEx Meetings usando o programa de desinstalação por sistema de SMS.

Etapa 1 Use o pacote de instalação de SMS criado em Criar um pacote a partir de uma definição, na página 140.

Etapa 2 Anuncie o programa de desinstalação por sistema para desinstalar o aplicativo Cisco WebEx Meetings. O aplicativo Cisco WebEx Meetings será desinstalado nas máquinas especificadas silenciosamente.

Implantação em massa do reprodutor de gravações de rede

Esta seção é um guia exaustivo que abrange diversos tipos de instalações, incluindo uma instalação para um único computador e instalações em grande escala, usando o Microsoft Systems Management Server 2003 (SMS).

Observação Os arquivos do reprodutor de gravações de rede maiores que 4 GB só poderão ser reproduzidos quando acessados de um navegador da Web.

Instalar o reprodutor de gravações de rede

Antes de iniciar

- Verifique se você possui privilégios de administrador no dispositivo alvo, pois o pacote MSI do Cisco WebEx está instalado na pasta Programas OS padrão que exige tal acesso.
- O pacote MSI do Cisco WebEx é desenvolvido para o Windows Installer Service 2.0 ou superior. Se a máquina local estiver configurada com uma versão mais antiga do instalador, uma mensagem de erro será exibida informando ao usuário que, a fim de instalar este pacote MSI, uma versão mais recente do Windows Installer Service será necessária. Ao executar o pacote MSI, o usuário será avisado através da interface MSI.

Etapa 1 Inicie o instalador no computador do usuário.

O assistente de instalação é exibido com uma mensagem introdutória.

Etapa 2 Selecione **Próxima** em cada uma das caixas de diálogo até que a caixa de diálogo de instalação seja exibida.

Etapa 3 Selecione **Instalar**.

Etapa 4 Selecione **Finalizar**.

Instalação silenciosa do reprodutor de gravações usando a linha de comando

Os administradores podem iniciar sessão no computador de um usuário e instalar o reprodutor de gravações WebEx usando o modo silencioso.

Etapa 1 Inicie a sessão no computador do usuário.

Etapa 2 Baixe o pacote MSI no disco rígido do computador.

Etapa 3 Abra o prompt de comando do Windows.
No Windows 7 ou Windows Vista, você deve usar o executar como administrador para abrir a janela do prompt.

Etapa 4 Insira o comando MSI para instalar o Reprodutor de gravações WebEx silenciosamente.

Exemplo:
Insira msiexec/i nbr2player_onprem.msi/qn.

Etapa 5 Reinicie o computador.

Desinstalação silenciosa do reprodutor de gravações usando a interface da linha de comando

Os administradores podem iniciar sessão no computador de um usuário e remover o reprodutor de gravações usando o modo silencioso.

Etapa 1 Inicie a sessão no computador do usuário.

Etapa 2 Baixe o pacote MSI no disco rígido do computador.

Etapa 3 Abra o prompt de comando do Windows.
No Windows 7 ou Windows Vista, você deve usar o executar como administrador para abrir a janela do prompt.

Etapa 4 Desinstale todos os componentes do pacote MSI onpremmc.msi inserindo o comando msiexec/i nbr2player_onprem.msi/qn.

Instalação de aplicativos CWMS usando o Microsoft Systems Management Server 2003 (SMS)

Limitações para a instalação silenciosa de aplicativos CWMS ao usar SMS

As seguintes limitações se aplicam quando você executa uma instalação silenciosa usando o Microsoft Systems Management Server 2003 (SMS):

- O modo de SMS por usuário não pode ser suportado.
- Se o administrador de SMS desejar adicionar um recurso para as Ferramentas de produtividade WebEx, ele deverá executar o comando **REMOVER** primeiro e, depois, executar o comando**ADDSOURCE**, mesmo que o recurso não tenha sido instalado antes.
- Se um usuário fizer logon em um computador com desktop remoto enquanto o administrador anuncia o pacote, ele deverá reiniciar o computador para que as Ferramentas de Produtividade WebEx funcionem normalmente.
- É possível realizar a implantação em massa, mas cada usuário deve inserir as informações credenciais.
- Antes de atualizar para uma versão de manutenção ou atualizar para uma versão mais recente, os usuários devem desinstalar as Ferramentas de Produtividade Cisco WebEx. Após a atualização, você pode mover manualmente as Ferramentas de Produtividade aos seus usuários ou os usuários podem baixar as Ferramentas de Produtividade da página **Downloads**.
- Se você estiver utilizando a integração Lync, depois de uma instalação silenciosa, os usuários devem reiniciar seus computadores para que todas as integrações do serviço de mensagens instantâneas funcione corretamente.

Anuncie o reprodutor de gravações de rede Cisco WebEx usando o programa automático por sistema de SMS

Se você for o administrador do SMS, execute o seguinte procedimento para anunciar o Reprodutor de Gravações de Rede do Cisco WebEx usando o programa automático por sistema de SMS.

Antes de iniciar

Registre-se no site da Administração e configure suas configurações de download para manualmente mover as aplicações do desktop WebEx para o desktop do usuário. Consulte a seção "Definição das configurações de download" no guia de administração do Cisco WebEx Meetings Server para obter mais informações.

Etapas de Resumo

1. Criar um pacote a partir da definição. Consulte Criar um pacote a partir de uma definição, na página 140 para obter mais informações.
2. Altere as opções do programa para "Automático por sistema" antes de anunciar:
3. Agora você pode anunciar o programa.

Etapas Detalhadas

Etapa 1 Criar um pacote a partir da definição. Consulte Criar um pacote a partir de uma definição, na página 140 para obter mais informações.

Etapa 2 Altere as opções do programa para "Automático por sistema" antes de anunciar:

a) Abra o console SMS do administrador e selecione **Banco de dados do site** > **Pacotes** > **Cisco WebEx LLC Reprodutor de Gravações de Rede Cisco WebEx em Inglês** > **Programas**.

b) Clique com o botão direito do mouse na opção **Automático por sistema** e selecione **Propriedades** para abrir a caixa de diálogo **Propriedades do programa automático por sistema**.

c) Selecione a **guia** Ambiente.

- Para a opção **O programa pode executar**, selecione **Somente quando o usuário está registrado em**.
- Para a opção **Modo de execução**, selecione **Executar com direitos administrativos**. Não selecione **Permitir que os usuários possam interagir com este programa**.

d) Selecione a aba **Geral**.

e) Adicione um parâmetro adicional para a opção de linha de comando para especificar algumas opções para o aplicativo Cisco WebEx Meetings:

Exemplo:
Por exemplo, a linha de comando inicial é a seguinte: msiexec /i "nbr2player_onprem.msi" /qn

Etapa 3 Agora você pode anunciar o programa.

a) Abra o console SMS do administrador e selecione **Banco de dados do site** > **Pacotes** > **Cisco WebEx LLC Reprodutor de Gravações de Rede Cisco WebEx em Inglês** > **Programas**.

b) Clique com o botão direito do mouse na opção **Automático por sistema**.

c) Selecione **Todas as tarefas** > **Distribuir software**.

d) Selecione **Avançar** no **Assistente de distribuição do programa**.

e) Selecione o servidor SMS e selecione **Avançar**.

f) Selecione a coleção e selecione **Avançar**.

g) Digite o nome do anúncio no campo **Nome** e selecione **Avançar**.

h) Especifique se o anúncio deverá se aplicar a subcoleções e selecione **Avançar**.

i) Especifique quando o programa será anunciado e selecione **Avançar**.

j) Especifique se deve atribuir o programa e selecione **Avançar**.

k) Selecione **Concluir** na página **Concluindo o Assistente de distribuição do programa**.

l) Vá até o diretório \Site Database\System Status\Advertisement Status e verifique o status do anúncio.
Se você habilitar a notificação, o usuário verá uma mensagem indicando que o programa atribuído será executado após o anúncio do programa. O programa atribuído executará silenciosamente.

Desinstale o reprodutor de gravações de rede Cisco WebEx usando o programa de desinstalação automático por sistema de SMS

O administrador de SMS pode desinstalar o reprodutor de gravações de rede Cisco WebEx usando o programa de desinstalação por sistema de SMS, realizando o seguinte procedimento.

Etapas de Resumo

1. Use o pacote de instalação de SMS criado em Criar um pacote a partir de uma definição, na página 140.
2. Anuncie o programa de desinstalação por sistema para desinstalar o reprodutor de gravações de rede Cisco WebEx.

Etapas Detalhadas

Etapa 1 Use o pacote de instalação de SMS criado em Criar um pacote a partir de uma definição, na página 140.

Etapa 2 Anuncie o programa de desinstalação por sistema para desinstalar o reprodutor de gravações de rede Cisco WebEx. O Reprodutor de gravações de rede Cisco WebEx será desinstalado nas máquinas especificadas em silêncio.

Reconfigurar suas configurações depois de realizar uma atualização

Depois de executar uma atualização do seu software Cisco WebEx Meetings Server (CWMS), você deve atualizar os caminhos para suas aplicações implantadas em massa. (Após uma atualização, o Reprodutor de gravações de rede é atualizado automaticamente na primeira vez que é usado para reproduzir uma gravação.)

Para sistemas Mac, o caminho é `/Users/(Local User)/Library/Application Support/WebEx Folder/`.

Para sistemas Windows, o caminho depende da versão, do tipo de download e do tipo de navegador web:

- Windows 7 e Windows Vista: <SystemDisk>\ProgramData\WebEx
- Das Ferramentas de Produtividade ou do WebEx Connect, utilize o caminho das Ferramentas de Produtividade ou do WebEx Connect.
- Se você estiver utilizando a instalação MSI, sempre utilize um caminho único. Seu sistema ignora o arquivo existente.
- Se você estiver utilizando o tipo de download com o Windows 7, o sistema utiliza um caminho único. No Windows XP, se o GPC pode encontrar o valor da tabela registrada, o sistema utiliza uma pasta existente. Caso contrário, o sistema irá utilizar seu próprio caminho, tal como descrito acima.

Os aplicativos de cliente em ambos os sistemas Windows e Mac são atualizados automaticamente para manter a compatibilidade com o sistema atualizado.

Em um ambiente bloqueado, você deve executar manualmente as atualizações para os sistemas Windows, mas não para os sistemas Mac.

Observação A versão do Aplicativo de Reuniões e Ferramentas de Produtividade que se alinha com a versão do Cisco WebEx Meeting Server pode ser encontrada em Matriz de Compatibilidade das Ferramentas de Produtividade e Aplicativos Cisco WebEx Meetings, na página 197.

CAPÍTULO 7

Visão geral do registro único

Os padrões de registro único (SSO) federado, como o SAML 2.0, fornecem mecanismos seguros para aprovar credenciais e informações relacionadas entre sites diferentes que tenham seus próprios sistemas de autorização e autenticação. A SAML 2.0 é um padrão aberto desenvolvido pelo Comitê Técnico de Serviços de Segurança OASIS.

O protocolo SAML 2.0 tem visto sucesso significativo, ganhando força em serviços financeiros, ensino superior, governo e outros segmentos da indústria. O suporte SAML 2.0 foi implementado por todos os principais fornecedores de gerenciamento de acesso à web. A Administração de Serviços Gerais do Governo dos EUA (GSA) exige que todos os fornecedores participem no programa E-Federação de Autenticação de Identidade dos EUA para ser compatível com SAML 2.0.

Web sites em conformidade com SAML 2.0 trocam informações de credenciais de usuários usando declarações SAML. A declaração SAML é um documento XML que contém declarações confiáveis sobre um assunto, incluindo, por exemplo, um nome de usuário e privilégios. Declarações SAML são assinadas digitalmente para garantir sua autenticidade.

Muitas grandes empresas têm implantado Sistema de Gerenciamento de Identidades e Acesso (IAM) e sistemas de fornecedor de identidade (IdP), tais como Ping Identy Ping Federate, CA SiteMinder, Open AM e Windows ADFS 2.0 em suas intranets corporativas. Estes sistemas IAM e IdP lidam com a autenticação do usuário e os requisitos de SSO para funcionários e parceiros. Os sistemas IAM e IdP usam protocolos SAML para inter-operarem com web sites parceiros fora dos seus firewalls. Os usuários podem utilizar seus sistemas IAM e IdP para autenticar automaticamente os usuários para serviços de reuniões do Cisco WebEx. Isso aumenta a eficiência, pois os usuários não precisam lembrar de seus nomes de usuários e senhas para iniciar ou participar de reuniões em seus sites Cisco WebEx.

Observação O WebEx Meetings Server suporta apenas IdPs SAML 2.0. Ele não suporta IdPs com base no antigo SAML 1.1 e WS-Federar padrões. Esta restrição está em contraste com os serviços de reuniões do Cisco WebEx baseados em nuvem, que continuam a suportar o SAML 1.1 e WS-Federate. O seguinte é uma lista de IdPs SAML 2.0 que foram validados para trabalhar com o Cisco WebEx Meetings Server:

- O Microsoft ADFS 2.0 (um complemento gratuito para o Microsoft Windows Server 2008/Windows Server 2008 R2 ou a função do servidor AD FS no Windows Server 2012)
- Microsoft ADFS 3.0 (função do servidor AD FS no Windows Server 2012)
- Ping Identity Ping Federate 6.6.0.17
- Forgerock Open AM 10.0.0
- CA SiteMinder 6.0 SP5

Como a SAML 2.0 é um padrão aberto, outros IdPs SAML 2.0 também podem operar com o Cisco WebEx Meetings Server. No entanto, outros IdPs SAML 2.0 não foram testados pela Cisco. É, portanto, de responsabilidade do administrador tornar essa integração operacional.

- Benefícios de Registro Único, página 152
- Visão geral da configuração SAML 2.0 de registro único, página 153
- SAML de SSO para Início de Sessão da Administração e do Usuário Final, página 154
- O registro único SAML 2.0 diferencia entre os serviços de reunião WebEx com base em nuvem e o WebEx Meetings Server, página 154
- Atributos de declarações SAML, página 160

Benefícios de Registro Único

O registro único (SSO) pode beneficiá-lo das seguintes formas:

- Autenticação de usuário simplificada-Fora da caixa, o Cisco WebEx Meetings Server exige que os usuários iniciem sessão usando endereços de e-mail e senhas que são específicos para o sistema do Meetings Server. Embora esta abordagem funcione bem para algumas organizações de pequeno e médio porte, as grandes organizações preferem usar credenciais corporativas, ou seja, Diretório Ativo para segurança reforçada. Você pode conseguir isso usando SAML 2.0 de SSO.

  Observação Autenticação segura-A senha de SSO nunca é enviada para ou armazenada no Cisco WebEx Meetings Server depois que o usuário é autenticado.

- Gerenciamento de usuário simplificado-Grandes organizações com mudança de mão de obra, devido a atrito normal preferem automatizar o processo de gerenciamento de usuários ao integrar com o WebEx Meetings Server. Isto significa automatizar o seguinte:
  - A criação da conta do usuário quando os funcionários participam da organização

- Atualizações da conta do usuário quando os funcionários assumem diferentes papéis dentro da organização
- Desativação da conta do usuário quando os funcionários deixam a organização

Você pode conseguir a automatização para esses eventos, configurando **Criação automática de conta** e **Atualização automática da conta** na seção de SSO do site de Administração do Cisco WebEx Meetings Server. Recomendamos que você ativar esses recursos se eles também são apoiados pelos seus IdPs SAML. As contas de usuários são criadas automaticamente e atualizadas "sob demanda" quando os usuários autenticam, eliminando a necessidade de criar contas de usuários manualmente. Da mesma forma, os usuários não podem mais iniciar a sessão em suas contas depois de deixar a organização, pois o IdP SAML 2.0 bloqueia esses usuários de iniciarem sessão depois que eles foram removidos do banco de dados, que normalmente é um proxy para o diretório corporativo subjacente.

Visão geral da configuração SAML 2.0 de registro único

Importante A menos que você ou alguém da sua organização tenha experiência com SAML 2.0 de registro único (SSO), recomendamos que você contrate os serviços de um parceiro AUC qualificado da Cisco ou Serviços Avançados da Cisco. Fazemos esta recomendação porque a configuração SAML de SSO pode ser complicada.

Cuidado Se a resposta SAML tem um retorno CR em qualquer um dos campos, então a atualização, a criação da conta e a autenticação falham. Embora o provedor SAML calcula a assinatura digital com o retorno CR, o Cisco WebEx Meetings Server remove o retorno CR fazendo com que a assinatura digital seja inválida.

Revise estas etapas gerais para a configuração SAML 2.0 de SSO:

1. Garanta que a sua infraestrutura SAML 2.0 de SSO esteja no lugar e integrada com o diretório corporativo. Isto implica a configuração SAML 2.0 do software IdP e do site de autenticação SSO. O site de autenticação é um portal onde os usuários inserem suas credenciais corporativas.
2. Garanta que os usuários possam acessar o site de autenticação SSO. Este passo é importante porque, como parte do processo de registro, o Cisco WebEx Meetings Server redireciona os usuários para o site de autenticação.

Observação Se o sistema Cisco WebEx Meetings Server está habilitado para acesso público, permitindo aos usuários iniciar sessão e entrar em reuniões da Internet, é fundamental garantir que o site de autenticação SSO também esteja acessível da Internet. Isso geralmente implica a implantação do IdP SAML 2.0 na sua DMZ. Caso contrário, os usuários verão erros "404 site não encontrado" ao iniciar a sessão no Cisco WebEx Meetings Server da Internet.

3. Conecte o WebEx Meetings Server ao IdP SAML 2.0 usando ambos os métodos:
   - Selecione **Configurações** > **Segurança** > **SSO Federado** em seu site de administração Cisco WebEx Meetings Server e defina os parâmetros IdP. (Consulte a seção Configurando as *Definições de Registro Único (SSO) Federado* no Guia de administração do Cisco WebEx Meetings Server.)

- Siga as instruções na sua documentação IdP SAML 2.0. Note que estas instruções variam de fornecedor para fornecedor. Recomendamos que você contate um parceiro AUC qualificado da Cisco ou Serviços Avançados da Cisco para ajudar a implementar a solução.

Observação Não use as instruções encontradas no Cisco Developer Network para configurar um IdP SAML 2.0. Essas instruções são destinadas a serviços de reuniões Cisco WebEx baseados em nuvem e não funcionam com o Cisco WebEx Meetings Server.

SAML de SSO para Início de Sessão da Administração e do Usuário Final

SAML de SSO normalmente é configurado apenas para fins de início de sessão no site do usuário final e não no site de Administração. Nos sites do Cisco WebEx Meetings Server integrados ao SAML 2.0, o comportamento espelha o comportamento SaaS da WebEx quando se trata da autenticação do usuário. O administrador do Cisco WebEx Meetings Server (e um administrador SaaS da WebEx) pode iniciar sessão em uma conta de usuário final usando SAML de SSO, mas deve inicar sessão em uma conta de administrador no mesmo sistema usando uma senha separada. Isso garante que, em caso de falhas catastróficas no iDP SAML de SSO, um administrador ainda poderá acessar o site da Administração. Sem essa prova de falhas, você pode encontrar uma situação em que o site da Administração se torna inacessível não por causa de uma falha de produto, mas por causa de um problema com o software IdP SAML de SSO. O software IdP SAML de SSO está em um servidor que é externo ao Cisco WebEx Meetings Server (ou SaaS da WebEx) e, portanto, fora do nosso controle.

O registro único SAML 2.0 diferencia entre os serviços de reunião WebEx com base em nuvem e o WebEx Meetings Server

Enquanto os serviços de reuniões Cisco WebEx com base em nuvem empregam IDs de usuários únicos ao criar contas de usuários, o Cisco WebEx Meetings Server usa endereços de e-mail como a base para a criação de contas de usuários. Ao implantar o registro único (SSO) SAML 2.0, note que os serviços de reuniões Cisco WebEx com base em nuvem permitem a remoção do domínio de e-mail, como "@cisco.com", do UPN (Nome principal do usuário) quando a criação automática da conta é ativada. Isto resulta na criação de uma conta de usuário que se assemelha a uma ID do usuário. Como o Cisco WebEx Meetings Server usa um endereço de e-mail completo para criar contas de usuários, você não pode remover o domínio de e-mail do UPN.

O servidor do Fornecedor de identidade (IdP) pode usar qualquer campo exclusivo do Diretório Ativo (AD), como o NameID, para uma configuração de SSO. Se você usa SSO e alterar o endereço de e-mail de um usuário ativo, altere o mapeamento para o campo NameID no servidor IdP.

Enquanto os serviços de reuniões Cisco WebEx com base em nuvem empregam IDs de usuários únicos ao criar contas de usuários, o Cisco WebEx Meetings Server usa endereços de e-mail como a base para a criação de contas de usuários. Este tem as seguintes importantes implicações ao implantar o registro único (SSO) SAML 2.0:

- É obrigatório para a Declaração SAML colocar o endereço de e-mail no campo NameID. Sem este passo, a autenticação de usuário e a criação de conta falham porque o Cisco WebEx Meetings não permite a criação de contas de usuários sem um endereço de e-mail associado.
- Os serviços de reuniões Cisco WebEx com base em nuvem permitem a remoção do domínio de e-mail, como "@cisco.com", do UPN (Nome Principal do Usuário) quando a criação automática da conta é ativada. Isto resulta na criação de uma conta de usuário que se assemelha a uma ID do usuário. Como o Cisco WebEx Meetings Server usa um endereço de e-mail completo para criar contas de usuários, você não pode remover o domínio de e-mail do UPN.

Você pode implantar o Cisco WebEx Meetings Server sem o SSO SAML 2.0 e depois da implantação, ativar o SSO. Fazer isso tem os seguintes importantes efeitos sobre a autenticação do usuário, criação automática de conta e recursos de atualização automática de conta:

Cenário	Comportamento da autenticação de usuário	Criação automática de conta (AAC) ativada	AAC desativada	Atualização automática da conta (AAU) ativada	AAU desativada
O SSO não está ativado. As contas de usuários foram criadas no sistema CWMS.	Os usuários iniciam sessão usando seus endereços de e-mail e senhas exclusivas.	N/D	N/D	N/D	N/D
Ative o SSO. Os usuários com contas existentes iniciam sessão no site WebEx, Ferramentas de Produtividade WebEx ou nos aplicativos Cisco WebEx Meetings em seus dispositivos móveis.	Os usuários são redirecionados ao site de autenticação IdP SAML 2.0 e iniciar sessão usando suas credenciais corporativas, em vez de senhas exclusivas. Se não forem usuários válidos, eles serão informados pelo IdP SAML 2.0 que não podem usar o Cisco WebEx ou que são usuários inválidos.	N/D	N/D	N/D	N/D

Cenário	Comportamento da autenticação de usuário	Criação automática de conta (AAC) ativada	AAC desativada	Atualização automática da conta (AAU) ativada	AAU desativada
O SSO está ligado. Os usuários não têm contas existentes no sistema.	Igual ao cenário anterior.	As contas de usuários no Cisco WebEx Meetings são criadas "sob demanda" depois que os usuários iniciam a sessão. Pré-requisito: A Declaração SAML contém um endereço de e-mail válido no campo NameID.	Os usuários que não possuem contas no sistema podem iniciar sessão, mas não podem acessar o Cisco WebEx. Para remediar esta situação: • Deixe a AAC ativada. • Crie contas de usuário manualmente.	N/D	N/D
O SSO está ligado. Usuários que iniciaram sessão anteriormente usando o SSO e que agora estão iniciando sessão novamente.	O mesmo que o cenário "Ativar SSO".	N/D	N/D	As contas de usuários existentes são atualizadas automaticamente com quaisquer alterações nas credenciais do usuário, desde que o NameID permaneça inalterado.	N/D

Cenário	Comportamento da autenticação de usuário	Criação automática de conta (AAC) ativada	AAC desativada	Atualização automática da conta (AAU) ativada	AAU desativada
Você desativa o SSO. (Este é um cenário incomum.) Usuários que iniciaram sessão anteriormente usando o SSO e que agora estão iniciando sessão novamente.	Se os usuários inserem suas credenciais corporativas, eles não podem iniciar sessão, pois o Cisco WebEx espera seus endereços de e-mail e senhas exclusivas. Nesta situação, educar os usuários sobre como redefinir as senhas exclusivas em suas contas Cisco WebEx e dar-lhes tempo suficiente para agir antes de desativar o SSO. Depois de redefinir suas senhas, os usuários podem iniciar sessão usando seus endereços de e-mail e senhas exclusivas.	N/D	N/D	N/D	N/D

Cenário	Comportamento da autenticação de usuário	Criação automática de conta (AAC) ativada	AAC desativada	Atualização automática da conta (AAU) ativada	AAU desativada
Caso especial: Um usuário também é um administrador de sistema. Cenário A: O usuário inicia sessão no site WebEx. Cenário B: O usuário inicia sessão no site de Administração do Cisco WebEx.		Cenário A: Mesmos resultados que o cenário anterior. Cenário B: N/A.	Cenário A: Mesmos resultados que o cenário anterior. Cenário B: N/A.	Cenário A: Mesmos resultados que o cenário anterior. Cenário B: N/A.	Cenário A: Mesmos resultados que o cenário anterior. Cenário B: N/A.

Cenário	Comportamento da autenticação de usuário	Criação automática de conta (AAC) ativada	AAC desativada	Atualização automática da conta (AAU) ativada	AAU desativada
	Cenário A: Mesmos resultados que o cenário anterior. Cenário B: Quando o usuário inicia sessão no site de Administração Cisco WebEx, ele é sempre solicitado a inserir seu endereço de e-mail e senha exclusiva; o SSO não tem efeito quando um usuário inicia sessão no site de Administração Cisco WebEx. Esta é uma medida de segurança incorporada no produto. Ela garante que os administradores dos sistemas possam sempre iniciar sessão no site de Administração Cisco WebEx. Se o site de Administração Cisco WebEx suportasse o SSO, então disfunções no IdP SAML 2.0 ou uma perda de conectividade de rede entre o				

Cenário	Comportamento da autenticação de usuário	Criação automática de conta (AAC) ativada	AAC desativada	Atualização automática da conta (AAU) ativada	AAU desativada
	Cisco WebEx Meetings Server e o IdP SAML 2.0 poderiam resultar em uma situação em que os administradores de sistemas não pudessem iniciar sessão e gerenciar o produto.				

Atributos de declarações SAML

A tabela a seguir lista os atributos de asserção SAML suportados pelo Cisco WebEx Meetings Server. Certifique-se de configurar o `sobrenome`, `nome`, `e-mail` e os atributos `updatetimestamp`. A atualização automática não funciona, a menos que o atributo `updatetimestamp` esteja configurado.

Atributos de declarações SAML suportados

Atribuir Nome	Atribuir Significado	Obrigatório para Usuário Criado Automaticamente	Faixa de Valor de Entrada	Comentários
Sobrenome		Sim		
Nome		Sim		
E-mail		Sim	Formato de e-mail válido	Sempre obrigatório, mesmo que a Criação automática de contas e a atualização estejam desabilitadas na configuração de SSO.

Atribuir Nome	Atribuir Significado	Obrigatório para Usuário Criado Automaticamente	Faixa de Valor de Entrada	Comentários
updateTimeStamp	O tempo de atualização de informações do usuário	Não	Formato de suporte **formato longo:** exemplo: System.currentTimeMillis() **Formato LDIF:** aaaaMMddHHmmss aaaa-MM-dd HH:mm:ss exemplo: 20090115213256 **Formato UTC** ("2009-10-09T06:00:32Z")	Se o updateTimeStamp está faltando, não é possível fazer atualização automática do usuário, normalmente mapeada para o item whenChanged se o IdP está conectado à AD.
optionalparams		Não		Consulte Parâmetros Opcionais, na página 164.
OPhoneCountry		Não		Escritório de códigos de telefones do país
OPhoneArea		Não		Área de telefone do escritório
OPhoneLocal		Não	Insira somente caracteres numéricos. Por exemplo, 5551212. Não insira caracteres não numéricos, como traços ou parênteses.	Escritório de telefone local
OPhoneExt		Não		Extensão de telefone do escritório
FPhoneCountry		Não		Código do país do telefone alternativo
FPhoneArea		Não		Área do telefone alternativo

Atribuir Nome	Atribuir Significado	Obrigatório para Usuário Criado Automaticamente	Faixa de Valor de Entrada	Comentários
FPhoneLocal		Não		Local do telefone alternativo
FPhoneExt		Não		Extensão de telefone alternativo
PPhoneCountry		Não		Código do país do telefone alternativo 2
PPhoneArea		Não		Área do telefone alternativo 2
PPhoneLocal		Não		Local do telefone alternativo 2
PPhoneExt		Não		Extensão de telefone alternativo 2
MPhoneCountry		Não		Código do país do telefone móvel
MPhoneArea		Não		Área do telefone móvel
MPhoneLocal		Não		Local do telefone móvel
MPhoneExt		Não		Extensão de telefone móvel
Fuso horário		Não		Consulte Valores de fuso horário, na página 165.
Endereço 1		Não		Endereço 1
Endereço 2		Não		Endereço 2
Cidade		Não		Cidade
Estado		Não		Estado
CEP		Não		CEP

Atribuir Nome	Atribuir Significado	Obrigatório para Usuário Criado Automaticamente	Faixa de Valor de Entrada	Comentários
País		Não		Consulte Valores de código de país, na página 168.
Região		Não		Consulte Valores das Regiões, na página 178.
Idioma		Não		Consulte Valores dos Idiomas, na página 179.
TC1	sequência	Não	Código de rastreamento do grupo 1 inserido pelo usuário no site da Administração	Índice 1
TC2	sequência	Não	Código de rastreamento do grupo 2 inserido pelo usuário no site da Administração	Índice 2
TC3	sequência	Não	Código de rastreamento do grupo 3 inserido pelo usuário no site da Administração	Índice 3
TC4	sequência	Não	Código de rastreamento do grupo 4 inserido pelo usuário no site da Administração	Índice 4
TC5	sequência	Não	Código de rastreamento do grupo 5 inserido pelo usuário no site da Administração	Índice 5
TC6	sequência	Não	Código de rastreamento do grupo 6 inserido pelo usuário no site da Administração	Índice 6

Atribuir Nome	Atribuir Significado	Obrigatório para Usuário Criado Automaticamente	Faixa de Valor de Entrada	Comentários
TC7	sequência	Não	Código de rastreamento do grupo 7 inserido pelo usuário no site da Administração	Índice 7
TC8	sequência	Não	Código de rastreamento do grupo 8 inserido pelo usuário no site da Administração	Índice 8
TC9	sequência	Não	Código de rastreamento do grupo 9 inserido pelo usuário no site da Administração	Índice 9
TC10	sequência	Não	Código de rastreamento do grupo 10 inserido pelo usuário no site da Administração	Índice 10

Parâmetros Opcionais

Você pode definir a configuração dos Parâmetros Opcionais como segue:

- <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic' Name="optionalparams">
- <saml:AttributeValue xsi:type="xs:string">City=Toronto</saml:AttributeValue >
- <saml:AttributeValue xsi:type="xs:string">AA=OFF</saml:AttributeValue >
- <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic' Name="City">
- <saml:AttributeValue xsi:type="xs:string">Toronto</saml:AttributeValue>
- <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic' Name="AA">
- <saml:AttributeValue xsi:type="xs:string">DESATIVADO</saml:AttributeValue>

Valores de fuso horário

Fuso horário	Valor
Ilhas Marshall(Horário de Dateline, GMT-12:00)	0
Samoa (Horário de Samoa, GMT-11:00)	1
Honolulu (Horário do Hawaii, GMT-10:00)	2
Anchorage (Horário de Verão do Alaska, GMT-08:00)	3
São Francisco (Horário de Verão do Pacífico, GMT-07:00)	4
Arizona (Horário das Montanhas, GMT-07:00)	5
Denver (Horário de Verão das Montanhas, GMT-06:00)	6
Chicago (Horário de Verão Central, GMT-05:00)	7
Cidade do México (Horário de Verão do México, GMT-05:00)	8
Saslatchewan (Horário Central, GMT-06:00)	9
Bogotá (Horário do Pacífico na América do Sul , GMT-05: 00)	10
Nova York (Horário de Verão no Leste, GMT-04:00)	11
Indiana (Horário de Verão no Leste, GMT-04:00)	12
Halifax (Horário de Verão do Atlântico, GMT-03:00)	13
La Paz (Horário do Leste na América do Sul, GMT-04:00)	14
Terra Nova (Horário de Verão da Terra Nova, GMT-02:30)	15
Brasília (Horário Padrão do Leste na América do Sul, GMT-03:00)	16
Buenos Aires (Horário do Leste na América do Sul, GMT-03: 00)	17

Fuso horário	Valor
Médio Atlântico (Hora do Médio Atlântico, GMT-02:00)	18
Açores (Horário de Verão de Açores, GMT)	19
Reiquejavique (Horário de Greenwich, GMT)	20
Londres (Horário de Verão GMT, GMT+01:00)	21
Amsterdã (Horário de Verão da Europa, GMT+02:00)	22
Paris (Horário de Verão da Europa, GMT+02:00)	23
Berlin (Horário de Verão da Europa, GMT+02:00)	25
Atenas (Horário de Verão da Grécia, GMT+03:00)	26
Cairo (Horário do Egito, GMT+02:00)	28
Pretória (Horário da África do Sul, GMT+02:00)	29
Helsinque (Horário de Verão no Norte da Europa, GMT+03:00)	30
Tel Aviv (Horário de Verão de Israel, GMT+03:00)	31
Riyadh (Horário da Arábia Saudita, GMT+03:00)	32
Moscou (Horário da Rússia, GMT+04:00)	33
Nairóbi (Horário de Nairóbi, GMT+03:00)	34
Teerã (Horário de Verão do Irã, GMT+04:30)	35
Abu Dabi, Mascate (Horário Árabe, GMT+04:00)	36
Bacu (Horário de Verão de Bacu, GMT+05:00)	37
Cabul (Horário do Afeganistão, GMT+04:30)	38
Ecaterinburgo (Horário da Ásia Ocidental, GMT+06:00)	39
Islamabade (Horário da Ásia Ocidental, GMT+05:00)	40
Mumbai (Horário da Índia, GMT+05:30)	41
Colombo (Horário de Colombo, GMT+05:30)	42

Fuso horário	Valor
Almaty (Horário da Ásia Central, GMT+06:00)	43
Bangkok (Horário de Bangkok, GMT+07:00)	44
Beijing (China Time, GMT+08:00)	45
Perth (Horário Oeste da Austrália, GMT+08:00)	46
Cingapura (Horário de Cingapura, GMT+08:00)	47
Taipei (Horário de Taipei, GMT+08:00)	48
Tóquio (Horário do Japão, GMT+09:00)	49
Seul (Horário da Coréia GMT+09:00)	50
Yakutsk (Horário de Yakutsk, GMT+10:00)	51
Adelaide (Horário Padrão Central da Austrália, GMT+09:30)	52
Darwin (Horário Central da Austrália, GMT+09:30)	53
Brisbane (Horário do Leste da Austrália, GMT+10:00)	54
Sydney (Horário Padrão Leste da Austrália, GMT+10:00)	55
Guam (Hora do Pacífico Oeste, GMT+10:00)	56
Hobart (Horário Padrão da Tasmânia, GMT+10:00)	57
Vladivostok (Horário de Vladivostok, GMT+11:00)	58
Ilhas Solomon (Horário Central do Pacífico, GMT+11:00)	59
Wellington (Horário Padrão da Nova Zelândia, GMT+12:00)	60
Fiji (Horário de Fiji, GMT+12:00)	61
Estocolmo (Horário de Verão da Suécia, GMT+02:00)	130
Tijuana (Horário de Verão no México do Pacífico, GMT-07:00)	131
Chihuahua (Horário de Verão nas Montanhas do México, GMT-06:00)	132

Fuso horário	Valor
Caracas (Horário do Leste na América do Sul, GMT-04:30)	133
Kuala Lumpur (Horário da Malásia, GMT+08:00)	134
Recife (S. do Leste na América do Sul, GMT-03: 00)	135
Casablanca (Horário de Verão do Marrocos, GMT+01:00)	136
Tegucigalpa (Horário de Honduras, GMT-06:00)	137
Nuuk (Horário de Verão da Groenlândia, GMT-02:00)	138
Amman (Horário de Verão da Jordânia, GMT+03:00)	139
Istambul (Horário de Verão do Leste Europeu, GMT+03:00)	140
Catmandu (Horário do Nepal, GMT+05:45)	141
Roma (Horário de Verão da Europa, GMT+02:00)	142
Oeste da África (Horário do Oeste da África, GMT+01:00)	143
Madri (Horário de Verão da Europa, GMT+02:00)	144

Valores de código de país

País	Código
Afeganistão	93
Albânia	355
Argélia	213
Samoa Americana	1684
Andorra	376
Angola	244
Anguila	1264

País	Código
Antártica	672_1
Antígua (incluindo Barbuda)	1268
Argentina	54
Armênia	374
Aruba	297
Ilha Ascensão	247
Austrália	61
Áustria	43
Azerbaijão	994
Bahamas	1242
Barein	973
Bangladesh	880
Barbados	1246
Bielorrússia	375
Bélgica	32
Belize	501
Benim	229
Bermuda	1441
Butão	975
Bolívia	591
Bósnia Herzegovina	387
Botsuana	267
Brasil	55
Ilhas Virgens Britânicas	1284

País	Código
Brunei	673
Bulgária	359
Burquina Faso	226
Burundi	257
Camboja	855
Camarões	237
Canadá	1_1
Ilha Cabo Verde	238
Ilhas Cayman	1_9
República Centro-Africana	236
República do Chade	235
Chile	56
China	86
Colômbia	57
Ilhas Comores	269_1
Ilhas Cook	682
Costa Rica	506
Croácia	385
Cuba	53
Chipre	357
República Checa	420
Dinamarca	45
Diego Garcia	246
Djibuti	253

País	Código
Dominica	1767
República Dominicana	1809
Equador	593
Egito, exceto Cairo	20
El Salvador	503
Guiné Equatorial	240
Eritréia	291
Estônia	372
Etiópia	251
Ilhas Faroés	298
Ilhas Falkland	500
Ilhas Fiji	679
Finlândia	358
França	33
Depts. Franceses (Oceano Índico)	262
Guiana Francesa	594
Polinésia Francesa	689
República do Gabão	241
Gâmbia	220
Geórgia	995
Alemanha	49
Gana	233
Gibraltar	350
Grécia	30

País	Código
Groenlândia	299
Granada	1473
Guadalupe	590
Guantanamo (Base naval dos EUA)	53_1
Guatemala	502
Guiné	224
Guiné Bissau	245
Guiana	592
Haiti	509
Honduras	504
Hong Kong	852
Hungria	36
Islândia	354
Índia	91
Indonésia	62
Irã	98
Iraque	964
Irlanda	353
Israel	972
Itália	39_1
Costa do Marfim	225
Jamaica	1876
Japão	81
Jordânia	962

País	Código
Cazaquistão	7_1
Quênia	254
Quiribati	686
Coréia (Norte)	850
Coréia (Sul)	82
Kuwait	965
Quirguistão	996
Laos	856
Letônia	371
Líbano	961
Lesoto	266
Libéria	231
Líbia	218
Liechtenstein	423
Lituânia	370
Luxemburgo	352
Macau	853
Macedônia	389
Madagascar	261
Malauí	265
Malásia	60
Maldivas	960
Mali	223
Malta	356

País	Código
Ilhas Marshall	692
Mauritânia	222
Maurício	230
Ilha Mayotte	269
México	52
Micronésia	691
Moldávia	373
Mônaco	377
Mongólia	976
Montserrat	1664
Marrocos	212
Moçambique	258
Miamar	95
Namíbia	264
Nauru	674
Nepal	977
Holanda	31
Antilhas Holandesas	599_2
Nova Caledônia	687
Nova Zelândia	64
Nicarágua	505
Níger	227
Niue	683
Ilha Norfolk	672

País	Código
lhas Marianas do Norte	1670
Noruega	47
Omã	968
Paquistão	92
Palau	680
Panamá	507
Papua Nova Guiné	675
Paraguai	595
Peru	51
Filipinas	63
Polônia	48
Portugal	351
Porto Rico	1787
Catar	974
Romênia	40
Rússia	7
Ruanda	250
San Marino	378
São Tomé	239
Arábia Saudita	966
República do Senegal	221
Sérvia	381
Ilhas Seychelles	248
Serra Leoa	232

País	Código
Cingapura	65
Eslováquia	421
Eslovênia	386
Ilhas Salomão	677
Somália	252
África do Sul	27
Espanha	34
Sri Lanka	94
Santa Helena	290
São Cristóvão e Neves	1869
Santa Lúcia	1758
São Pedro e Miguelão	508
São Vicente	1784
Sudão	249
Suriname	597
Suazilândia	268
Suécia	46
Suíça	41
Síria	963
Taiwan	886
Tadjiquistão	992
Tanzânia	255
Tailândia	66
Togo	228

País	Código
Ilhas Tonga	676
Trinidad e Tobago	1868
Tunísia	216
Turquia	90
Turcomenistão	993
Turks e Caicos	1649
Tuvalu	688
Uganda	256
Ucrânia	380
Emirados Árabes Unidos	971
Reino Unido	41
Estados Unidos da América	1
Uruguai	598
Uzbequistão	998
Vanuatu	678
Cidade do Vaticano	39
Venezuela	58
Vietnã	84
Ilhas Wallis e Futuna	681
Samoa Ocidental	685
Iêmen	967
Zâmbia	260
Zimbábue	263

Valores das Regiões

Região	Valor
Estados Unidos	2
Austrália	3
Canadá	4
Francês Canadense	5
China	6
França	7
Alemanha	8
Hong Kong	9
Itália	10
Japão	11
Coréia	12
Nova Zelândia	13
Espanha	14
Suíça	15
Taiwan	16
Reino Unido	17
México	18
Argentina	19
Chile	20
Colômbia	21
Venezuela	22
Brasil	23
Portugal	24

Região	Valor
Bélgica	25
Holanda	26
Rússia	28
Índia	29

Valores dos Idiomas

Idioma	Valor
Espanhol castelhano	11
Holandês	14
Inglês	1
Francês	7
Alemão	9
Italiano	10
Japonês	5
Coreano	6
Espanhol da América Latina	12
Português	15
Russo	16
Chinês Simplificado	3
Chinês Tradicional	4

Códigos de idiomas

Idioma	Código de país
Espanhol castelhano	34

Idioma	Código de país
Chinês	852, 853, 886
Holandês	31, 32
Francês	33, 242, 243
Alemão	41, 43, 49
Italiano	39
Japonês	81
Coreano	82
Espanhol da América Latina	52, 54, 56, 57, 58
Mandarim	86
Português	55, 351
Russo	7
Inglês do Reino Unido	44, 61, 64, 91
Inglês dos E.U.A	1

CAPÍTULO 8

Requisitos de armazenamento para gravações de reuniões

Você pode configurar um servidor de armazenamento de qualquer capacidade. O número de gravações Cisco WebEx salvo é dependente da quantidade de espaço de armazenamento configurada.

Quando um usuário marca uma gravação para exclusão, ela imediatamente fica indisponível na interface do usuário. Ela é mantida em armazenamento de três a seis meses. Portanto, as gravações podem ser copiadas, feito backup ou usadas por até seis meses apesar de serem marcadas para exclusão pelo usuário. (Se um usuário excluir inadvertidamente uma gravação da página de Gravações de reuniões do Cisco WebEx, mas a gravação for salva no servidor de armazenamento do Sistema de arquivos de rede (NFS), você deve entrar em contato com o Centro de Assistência Técnica (TAC) da Cisco para recuperar a gravação.)

Se as gravações em seu sistema não consomem mais de 75 por cento do espaço alocado em um período de três meses, as gravações são excluídas após seis meses. Se as gravações consomem mais de 75 por cento do espaço alocado em algum ponto em um período de três meses, o sistema automaticamente exclui os primeiros 10 arquivos que foram definidos para exclusão por um usuário.

Por exemplo, um usuário identifica dois arquivos para exclusão hoje, depois cinco arquivos amanhã, e, em seguida, nove arquivos depois de amanhã. Se o uso do armazenamento excede o limite de 75 por cento, o sistema exclui os dois primeiros arquivos depois de três meses, os próximos cinco arquivos no dia seguinte, e, em seguida, ele exclui os primeiros três dos nove arquivos marcados para exclusão no dia seguinte.

Se a organização exige que você armazene gravações de reuniões por mais de seis meses, arquive periodicamente as gravações em outra mídia.

A tabela a seguir fornece uma estimativa da quantidade de espaço de armazenamento necessária para uma hora de gravação. Use esses valores para ajudá-lo a estimar a quantidade de espaço de armazenamento necessária para o sistema para seis meses de gravações de reuniões.

Conteúdo da reunião	Espaço para armazenamento aproximado necessário para uma hora de gravação de reunião
Compartilhamento da aplicação	36 MB
Voz	30 MB
Vídeo de 180p	104 MB
Vídeo de 360p	337 MB

Os vídeos de webcam são armazenados na resolução original para a gravação da reunião. No entanto, ao reproduzir a gravação, a resolução de vídeo é restrita a vídeo de 180p.

- Requisitos de armazenamento para arquivos de backup do sistema, página 182

Requisitos de armazenamento para arquivos de backup do sistema

A recomendação geral para a quantidade de armazenamento necessário para backups do sistema, o que não inclui gravações de reuniões, é de pelo menos 900 MB ou espaço suficiente para acomodar até três arquivos de backup do sistema. O sistema exclui automaticamente os arquivos de backup mais antigos e armazena somente o backup mais recente.

Considerações ao determinar o espaço de armazenamento necessário para backups:

- O número de usuários
- O número médio de reuniões realizadas por dia
- O tamanho do seu banco de dados, que irá aumentar ao longo do tempo
- Com implantações de HA, pode haver atrasos na operação de transporte diário, devido à latência de rede ou uma alta carga do sistema durante a replicação de dados. Isto pode aumentar o tamanho de um arquivo de backup.

O Painel mostra os requisitos de armazenamento aproximados para um backup do sistema. Deixe espaço suficiente no servidor de armazenamento para, pelo menos, três vezes o tamanho do backup observado.

CAPÍTULO 9

MIBs SNMP Suportados

O SNMP MIB ftp://ftp.cisco.com/pub/mibs/v2/CISCO-WBX-MEETING-MIB.my é suportado pelo Cisco WebEx Meetings Server. Nem todas as variáveis MIB são aplicáveis ao Cisco WebEx Meetings Server ou a todos os tipos de implantação do Cisco WebEx Meetings Server. Por exemplo, os centros de dados MIB relacionados não se aplicam a sistemas Cisco WebEx Meetings Server.

- Informações MIBS do sistema CWMS, página 183
- MIBs relacionadas a CPU, página 184
- Informações de memória do CWMS, página 187
- Uso do Disco, página 187
- Interceptações SNMP Suportadas, página 188

Informações MIBS do sistema CWMS

OBJETO[22]	OID	Descrição
cwCommSystemVersion Tipo: sequência	.1.3.6.1.4.1.9.9.809.1.1.1	Versão do sistema Cisco WebEx.
cwCommSystemObjectID Tipo: Autônomo	.1.3.6.1.4.1.9.9.809.1.1.2	O sysObjectID conforme definido no SNMPv2-MIB.

22 Todos os objetos nesta tabela são somente leitura (RO).

MIBs relacionadas a CPU

OBJETO	Privilégio de Leitura/ Gravação	OID	Descrição
cwCommCPUTotalUsage Tipo: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.1	Porcentagem de uso da CPU por um componente de host. O percentual de uso total da CPU contém o uso da CPU pelo usuário, o uso da CPU pelo sistema e o uso nice da CPU. O tempo de usuário na CPU: O tempo na CPU gasto no espaço do usuário. O horário do sistema na CPU: O tempo na CPU gasto no espaço do kernel. O tempo bom da CPU: O tempo na CPU gasto em processos de baixa prioridade.
cwCommCPUUsageWindow Tipo: Gauge32	RW	.1.3.6.1.4.1.9.9.809.1.2.1.2	A duração (em segundos) antes de uma notificação (interceptação) ser enviada indicando um uso de CPU atravessou um limite normal/menor/menor e permanece no novo limite.
cwCommCPUTotalNumber Tipo: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.3	Número de CPUs no sistema.
cwCommCPUUsageTable Tipo: N/D	Não acessível	.1.3.6.1.4.1.9.9.809.1.2.1.4	Uma lista de uso da CPU registrada no dispositivo.
cwCommCPUIndex Tipo: Não registrado	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.1	Identificador de CPU único. Cada CPU possui o seu próprio uso e os valores de repartição.
cwCommCPUName Tipo: sequência	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.2	Nome da CPU. Por exemplo, Intel® Xeon™ CPU 3.00GHz.

OBJETO	Privilégio de Leitura/ Gravação	OID	Descrição
cwCommCPUUsage Tipo: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.3	Porcentagem do total de recursos usados da CPU. Normalmente é usado o GHz para medição da capacidade da CPU. Como o GHz é muito grande para medir algumas categorias de uso da CPU, o KHz é usado como a unidade de medida. A velocidade do sistema é multiplicada pela fração de cada seção da CPU (por exemplo, inativa, nice ou do usuário) para obter a velocidade da CPU em KHz de cada categoria. KHz é usada como a unidade de medida para todas as categorias de CPU nesta tabela.
cwCommCPUUsageUser Tipo: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.4	Energia da CPU executada no modo de usuário.
cwCommCPUUsageNice Tipo: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.5	Energia da CPU executada em processos de baixa prioridade. Nice é um programa encontrado no Unix e no Linux. Ele mapeia diretamente a uma chamada kernel do mesmo nome. O Nice é usado para chamar um utilitário ou um script shell com uma prioridade específica, dando assim a um processo mais ou menos tempo da CPU do que outros processos.

OBJETO	Privilégio de Leitura/ Gravação	OID	Descrição
cwCommCPUUsageSystem Tipo: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.6	Energia da CPU executada no modo kernel.
cwCommCPUUsageIdle Tipo: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.7	Energia da CPU no status de inativa.
cwCommCPUUsageIOWait Tipo: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.8	Energia da CPU usada ao esperar pela E/S de disco ser concluída.
cwCommCPUUsageIRQ Tipo: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.9	Energia da CPU usada ao lidar com uma solicitação de interrupção.
cwCommCPUUsageSoftIRQ Tipo: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.10	Energia da CPU usada ao lidar com uma solicitação de interrupção de software.
cwCommCPUUsageSteal Tipo: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.11	Energia da CPU usada em outras tarefas ao executar em um ambiente virtualizado.
cwCommCPUUsageCapacitySubTotal Tipo: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.4.1.12	Atual energia total da CPU.
cwCommCPUMonitoringStatus Tipo: sequência	RO	.1.3.6.1.4.1.9.9.809.1.2.1.5	Status de monitoramento dos recursos da CPU: • fechado (0) — Recurso não disponível. • aberto (1) — Recurso está disponível.
cwCommCPUCapacityTotal Tipo: Gauge32	RO	.1.3.6.1.4.1.9.9.809.1.2.1.6	Capacidade geral da CPU.

Informações de memória do CWMS

OBJETO[23]	OID	Descrição
cwCommMEMUsage Tipo: Gauge32	.1.3.6.1.4.1.9.9.809.1.2.2.1	Uso de memória física da máquina virtual.
cwCommMEMMonitoringStatus Tipo: sequência	.1.3.6.1.4.1.9.9.809.1.2.2.2	Status de monitoramento do recurso de memória: fechado (0) — Recurso não disponível. aberto (1) — Recurso está disponível.
cwCommMEMTotal Tipo: Gauge32	.1.3.6.1.4.1.9.9.809.1.2.2.3	Tamanho total de memória física (em KB) do host.
cwCommMEMSwapUsage Tipo: Gauge32	.1.3.6.1.4.1.9.9.809.1.2.3.1	Uso de memória física (em porcentagem) e uso de memória swap do host.
cwCommMEMSwapMonitoringStatus Tipo: sequência	.1.3.6.1.4.1.9.9.809.1.2.3.2	Este objeto fornece o status de monitoramento da memória e da memória swap. fechado (0)—O status da memória e da memória swap estão disponíveis. aberto (0)—O status da memória e da memória swap não estão disponíveis.

23 Todos os objetos nesta tabela são somente leitura (RO).

Uso do Disco

OBJETO[24]	OID	Descrição
cwCommDiskUsageCount	.1.3.6.1.4.1.9.9.809.1.2.5.1	Contagem de quantos discos (por exemplo, disco local, disco remoto e disco de gravação de reunião) estão disponíveis no sistema.
cwCommDiskUsageIndex	.1.3.6.1.4.1.9.9.809.1.2.5.2.1.1	Índice de entradas na tabela que possui informações de gerenciamento genéricas ao uso do disco.
cwCommDiskPartitionName	.1.3.6.1.4.1.9.9.809.1.2.5.2.1.2	Nome da partição de disco. Por exemplo, a partição /opt ou /dev.

OBJETO[24]	OID	Descrição
cwCommDiskUsage	.1.3.6.1.4.1.9.9.809.1.2.5.2.1.3	Uso atual de disco (em porcentagem) no host.
cwCommDiskTotal	.1.3.6.1.4.1.9.9.809.1.2.5.2.1.4	Tamanho total de espaço em disco (em MB) deste host.
cwCommDiskMonitoringStatus	1.3.6.1.4.1.9.9.809.1.2.5.3	Status de monitoramento dos recursos de disco. fechado (0) — O status da utilização do disco não está disponível. aberto (1) — O status da utilização do disco está disponível.

24 Todos os objetos nesta tabela são somente leitura (RO).

Interceptações SNMP Suportadas

As Interceptações SNMP suportadas pelo Cisco WebEx Meetings Server.

Notificação de Eventos

cwCommSystemResourceUsageNormalEvent (.1.3.6.1.4.1.9.9.809.0.1)

Notificação quando o uso de recursos de um sistema é alterado do status *normal*. O sistema pode enviar esta notificação no evento:

- O valor do `cwCommCPUUsage` de uma CPU é alterado para ser menor do que o valor do limite mínimo predefinido da CPU.
- O valor do `cwCommMEMUsage` é alterado para ser menor do que o valor de um limite mínimo predefinido da MEM.
- O valor do `cwCommMEMSwapUsage` é alterado para ser menor do que o valor do limite mínimo predefinido da MEM swap.
- O valor do `cwCommFileUsage` é alterado para ser menor do que o valor do limite mínimo do arquivo.
- O valor do `cwCommDiskUsage` em um disco é alterado para ser menor do que o valor do limite mínimo predefinido do disco.

cwCommSystemResourceUsageMinorEvent (.1.3.6.1.4.1.9.9.809.0.2)

Notificação quando o uso de recursos de um sistema é alterado do status *mínimo*. A notificação menor significa o sistema tem alguns problemas e o administrador do sistema deve resolvê-las. O sistema pode enviar esta notificação no evento:

- O valor do `cwCommCPUUsage` de uma CPU é alterado para ser maior do que ou igual ao valor do limite mínimo predefinido da CPU e menor que o valor cwCommCPUMajorThreshold.
- O valor do `cwCommMEMUsage` é alterado para ser maior do que ou igual ao valor do limite mínimo predefinido da MEM e menor que o valor do limite máximo predefinido da MEM.
- O valor do `cwCommMEMSwapUsage` é alterado para ser maior do que ou igual ao valor do limite mínimo predefinido da MEM Swap e menor que o valor do limite máximo predefinido da MEM Swap.
- O valor do `cwCommFileUsage` é alterado para ser maior do que ou igual ao valor do limite mínimo predefinido do arquivo e menor que o valor do limite máximo predefinido do arquivo.
- O valor do `cwCommDiskUsage` é alterado para ser maior do que ou igual ao valor do limite mínimo predefinido do disco e menor que o valor do limite máximo predefinido do disco.

cwCommSystemResourceUsageMajorEvent (.1.3.6.1.4.1.9.9.809.0.3)

Esta notificação indica que o uso de recursos do sistema é alterado para o status *máximo*. A notificação de máximo significa que o sistema está em estado crítico e que o administrador do sistema precisa agir imediatamente. O sistema pode enviar esta notificação no evento:

- O valor do `cwCommCPUUsage` de uma CPU é alterado para ser maior ou igual que o valor do limite máximo predefinido da CPU.
- O valor do `cwCommMEMUsage` é alterado para ser maior ou igual que o valor do limite máximo predefinido da MEM.
- O valor do `cwCommMEMSwapUsage` é alterado para ser maior ou igual que o valor do limite máximo predefinido da MEM Swap.
- O valor do `cwCommFileUsage` é alterado para ser maior ou igual que o valor do limite máximo predefinido do arquivo.
- O valor do `cwCommDiskUsage` é alterado para ser maior ou igual que o valor do limite máximo predefinido do disco.

Dados de Interceptação

Dados de interceptação suportados. Recomendamos que você defina o filtro MIB para receber apenas essas interceptações.

Nome	OID	Convenção Textual	Descrição
cwCommNotificationHostAddressType	.1.3.6.1.4.1.9.9.809.1.2.4.1	InetAddressType	Tipo do endereço de rede disponibilizado através do cwCommNotificationHostAddress.
cwCommNotificationHostAddress	.1.3.6.1.4.1.9.9.809.1.2.4.2	InetAddress	O endereço IP do organizador enviado com a notificação.

Nome	OID	Convenção Textual	Descrição
cwCommNotificationResName	.1.3.6.1.4.1.9.9.809.1.2.4.3	CiscoWebExCommSysRes	O nome do recurso do sistema enviado com a notificação. Ele indica o nome do recurso do sistema que ultrapassou os níveis de aviso predefinidos. 0. cwCommTtoalCPUUsage 1. cwCommMemUsage 2. cwCommMemSwapUsage 3. abrir o descritor de arquivo (sem os dados MIB) 4. cwCommSocketUsage 5. um dos cwCommDiskTotal
cwCommNotificationResValue	.1.3.6.1.4.1.9.9.809.1.2.4.4	Unsigned32	Valor de uso percentual de recursos do sistema com a notificação.
cwCommNotificationSeqNum	.1.3.6.1.4.1.9.9.809.1.2.4.5	Counter32	Número de sequência que rastreia o pedido das notificações.

CAPÍTULO 10

Requisitos do sistema PC comum

Requisitos do sistema Cisco WebEx Meeting Server (CWMS) comuns aos navegadores e sistemas operacionais. Os requisitos para o PC do administrador e para o PC do usuário das Ferramentas de Produtividade são os mesmos.

Requisitos do cliente e do navegador

- JavaScript e cookies habilitados
- Java 6, Java 7 ou Java 8 (para navegadores da web que suportam Java) habilitado
- Plug-ins Cisco WebEx habilitados para Chrome 32 e posterior ou Firefox 27 e posterior
- Plug-ins habilitados no Safari
- Active X habilitado e desbloqueado para Microsoft Internet Explorer (recomendado)

Observação Como a política do Google e Mozilla mudou, começando com o Chrome 32 e Firefox 27, pode ser necessário que os usuários tenham que ativar o plugin WebEx manualmente quando usarem estes navegadores[25] para participarem de uma reunião WebEx ou para reproduzirem uma gravação WebEx. Mais informações e instruções podem ser encontradas em https://support.webex.com/webex/meetings/en_US/chrome-firefox-join-faq.htm.

Se um cliente estiver usando um navegador que não seja as versões especificadas do Chrome ou Firefox e tiver Java habilitado, o aplicativo Cisco WebEx Meetings fará automaticamente o download para o sistema do cliente na primeira vez que esse cliente iniciar ou entrar em uma reunião. Recomendamos que você oriente todos os clientes a instalarem a atualização mais recente da sua versão Java.

Requisitos TLS

Configure **Configurações da internet** em todos os computadores de usuários para criptografia TLS. Por exemplo, em um PC com Windows, selecione **Painel de controle** > **Opções da internet** > **Avançado** > **Segurança** > **Usar TLS 1.1** e **Usar TLS 1.2**. Recomendamos selecionar ambas as opções para compatibilidade máxima. (**Usar TLS 1.0** não é compatível nas versões 2.7 ou superior.)

25 As versões exatas do Chrome e Firefox que são impactadas por essa política não foram finalizadas até a publicação deste documento.

Se os usuários organizarem reuniões para convidados, tais como pessoas que não trabalham para sua empresa, informe aos convidados da reunião para atualizarem manualmente os sistemas operacionais e navegadores, pois eles devem corresponder à configuração TLS antes de entrarem nas reuniões. Se eles não modificarem os sistemas, enfrentarão problemas de compatibilidade. Recomendamos que você inclua essas instruções em seus convites para reuniões. Você pode fazer isso editando os convites adequados para reuniões, disponíveis no site da Administração em **Configurações** > **E-mail** > **Modelos**.

Requisitos SSL e TLS

Configure **Configurações da Internet** em todos os computadores de usuários para utilizar criptografia SSL e TLS. Por exemplo, em um PC Windows:

- Selecione **Painel de controle** > **Opções da Internet** > **Avançado** > **Segurança** > **Usar SSL 3.0**. É recomendável selecionar essa opção para o máximo de compatibilidade.
- Selecione **Painel de controle** > **Opções da internet** > **Avançado** > **Segurança** > **Usar TLS 1.0** e **Usar TLS 1.2** para compatibilidade máxima.

Se os usuários organizarem reuniões para convidados, tais como pessoas que não trabalham para sua empresa, informe aos convidados da reunião para atualizarem manualmente os sistemas operacionais e navegadores, pois eles devem corresponder à configuração SSL ou TLS antes de entrarem nas reuniões. Se eles não executarem os passos acima, irão enfrentar problemas de compatibilidade. Recomendamos que você inclua essas instruções em seus convites para reuniões. Você pode fazer isso editando os convites adequados para reuniões, disponíveis no site da Administração em **Configurações** > **E-mail** > **Modelos.**.

- Requisitos do sistema operacional para Windows, página 192
- Requisitos do sistema operacional para Mac, página 195
- Requisitos dos sistemas operacionais para dispositivos móveis, página 196
- Suporte à Citrix XenDesktop e XenApp, página 196
- Matriz de Compatibilidade das Ferramentas de Produtividade e Aplicativos Cisco WebEx Meetings, página 197
- Sobre as licenças do organizador, página 199

Requisitos do sistema operacional para Windows

Sistemas Operacionais Windows

- Windows Vista (32 bits/64 bits)
- Windows 7 (32 bits/64 bits)
- Windows 8 (32 bits/64 bits)
- Windows 8.1 (32 bits/64 bits)
- Windows 10 (32 bits/64 bits) (CWMS 2.6MR1 e superior)
- Edge (apenas Windows 10) 20.10240.16384.0 a 38.14393.00

Observação Suporte para o Microsoft Windows 10 Redstone 1, também conhecido como Windows 10 Anniversary Update (versão 1607), foi adicionado no CWMS versão 2.7.

Requisitos de hardware do Windows

Processador Intel Core2 Duo ou AMD CPU 2.XX GHz ou superior.

Recomenda-se um mínimo de 2 GB de RAM.

Navegadores Windows suportados

- Internet Explorer: 8 - 11.103.14393.0

  IE 11 foi testado no Windows 7 SP1 e Windows 8.1
- Mozilla Firefox: 10—50

  Mozilla Firefox: 34 - 37 testado na versão 2.5MR4

  Consulte a agenda de lançamento do Firefox em https://wiki.mozilla.org/RapidRelease/Calendar
- Google Chrome: 23 - 54.0.2840.99

  Google Chrome: 39 - 42 testado na versão 2.5MR4

  Consulte a agenda de lançamentos do Chrome em http://www.chromium.org/developers/calendar

Integração com o Microsoft Outlook

- Microsoft Outlook 2007 SP2 e superior
- Microsoft Outlook 2010 (edições de 32 bits e 64 bits, todos os Service Packs)
- Microsoft Outlook 2013
- Microsoft Outlook 2016 (CWMS 2.6MR1)

A tabela a seguir descreve quais versões do Microsoft Outlook são suportadas em quais sistemas operacionais.

Versão do Microsoft Outlook (Cliente/servidor Exchange)	Vista	Windows 7	Windows 8 (somente no modo de desktop)	Windows 10
Outlook 2007/Exchange 2007	S	S	N	N
Outlook 2010/ Exchange 2007	S	S	S	S
Outlook 2010/ Exchange 2010	S	S	S	S

Versão do Microsoft Outlook (Cliente/servidor Exchange)	Vista	Windows 7	Windows 8 (somente no modo de desktop)	Windows 10
Outlook 2013/ Exchange 2010	N	S	S	S
Outlook 2010/ Exchange 365 hospedado	N	S	S	S
Outlook 2013/ Exchange 2013	N	S	S	S
Outlook 2013/ Exchange 365 hospedado	N	S	S	S
Outlook 2016/ Exchange 365 hospedado	N	S	S	S
Outlook 2010/ Exchange 2016	N	S	S	Y - suporta o window 7,8,10
Outlook 2013/ Exchange 2016	N	S	S	Y - suporta o window 7,8,10
Outlook 2016/ Exchange 2016	N	S	S	Y - suporta o window 7,8,10
Outlook 2016/ Exchange 2010	N	S	S	Y - suporta o window 7,8,10
Outlook 2016/ Exchange 2013	N	S	S	Y - suporta o window 7,8,10

Clientes de Mensagens Instantâneas Suportados

Versão do Serviço de mensagens instantâneas	Windows XP SP3	Windows 7	Windows 8
Communicator 2007	S	S	S
Communicator 2007 R2	S	S	S
Lync 2010 (32 bits)	N	S	S

Versão do Serviço de mensagens instantâneas	Windows XP SP3	Windows 7	Windows 8
Lync 2013 (32 bits)	N	S	S

Integração com o Cisco Jabber para Windows

- Cisco Jabber para Windows 9.2.6
- Cisco Jabber para Windows 9.6.1
- Cisco Jabber para Windows 9.7
- Cisco Jabber para Windows 10.5
- Cisco Jabber para Windows 11.0
- Cisco Jabber para Windows 11.5 (CWMS 2.6MR1)
- Cisco Jabber para Windows 11.6
- Suporta Cisco WebEx Meetings Server com LDAP/Diretório ativo de integração.

Restrição Jabber para Windows 9.2.6 suporta integração com Cisco WebEx Meetings Server 1.5 e sites posteriores que estão configurados para SAML 2.0 de registro único (SSO). Versões anteriores do Jabber para Windows não suportam registro único.

Nem todas as versões do Cisco Jabber ou das plataformas suportam a integração com o Cisco WebEx Meetings Server. (Por exemplo, Jabber e WebEx Communicator baseados em nuvem.) Para obter informações sobre a integração com Cisco WebEx Meetings Server, consulte o Cisco Jabber para documentação do Windows em http://www.cisco.com/en/US/products/ps12511/tsd_products_support_series_home.html.

Requisitos do sistema operacional para Mac

Sistemas operacionais suportados Mac

- Mac OS X 10.7 Lion
- SO Mac X 10.8 Mountain Lion
- Mac OS X 10.9 Mavericks
- OS X 10.11 El Capitan (CWMS 2.6MR1)
- OS X 10.12 Sierra (CWMS 2.7MR2)

Requisitos de hardware Mac

2.0 GHz ou superior CPU.

Recomenda-se um mínimo de 512 MB de RAM.

Navegadores Mac suportados

- Apple Safari: 6—9.1.3
- Google Chrome: 23— 53.0.2743.116

  Consulte a agenda de lançamentos do Chrome em http://www.chromium.org/developers/calendar
- Mozilla Firefox: 10—48.1

Integração com o Cisco Jabber para Mac

As seguintes integrações com o Cisco Jabber para Mac são suportadas para sites do Cisco WebEx Meetings Server que estão configurados para registro único (SSO) SAML 2.0 ou LDAP/Diretório Ativo.

- Cisco Jabber para Mac 11.6 suporta a integração com o Cisco WebEx Meetings Server Versão 2.6 e posterior
- Cisco Jabber para Mac 10.5 suporta a integração com o Cisco WebEx Meetings Server Versão 2.5 e posterior
- Cisco Jabber para Mac 9.6 suporta a integração com o Cisco WebEx Meetings Server Versão 2.0 e posterior

Requisitos dos sistemas operacionais para dispositivos móveis

Depois de baixar manualmente o aplicativo Cisco WebEx no iOS ou Android e o recurso móvel WebEx estar habilitado, um usuário pode utilizar o aplicativo para participar ou iniciar uma reunião. Um usuário também pode acessar o Cisco WebEx em um dispositivo móvel usando um navegador, mas isto talvez não proporcione a mesma experiência ideal para o usuário.

Cisco WebEx Meeting Server Versão 2.0 e suportes superiores:

- iPhones e iPads da Apple usando iOS 6.0 e posterior.
- Dispositivos móveis Android usando Android 2.1 e posterior.
- Jabber para iPhones e para Android 9.6 e posterior.

Observação Você não pode reproduzir a gravação no dispositivo móvel. Se você iniciou uma reunião utilizando um dispositivo móvel Android, você pode iniciar e gerenciar a gravação de uma reunião. Se você iniciou uma reunião utilizando um dispositivo móvel iOS, você não pode iniciar ou gerenciar a gravação de uma reunião no dispositivo iOS.

Suporte à Citrix XenDesktop e XenApp

O Cisco Webex Meeting Server suporta o Citrix XenDesktop 7.6, em que o sistema operacional do host e o sistema operacional virtual são Windows 7 ou Windows 8. (O sistema operacional do host é o sistema operacional instalado no computador do usuário final. O sistema operacional virtual é o sistema operacional fornecido pelo servidor.)

Problemas conhecidos e limitações

- Devido a uma limitação na arquitetura do ambiente do desktop virtual, enviar vídeo pode não ter um bom funcionamento. Além disso, ao enviar vídeo em uma reunião, a taxa de quadros pode ser baixa, resultando em uma experiência menos do que ótima do usuário.
- Alguns arquivos de vídeo não podem ser compartilhados em um ambiente de desktop virtual.
- Ao executar um Mac OS, a webcam e o microfone (externo ou integrado) podem não ser reconhecidos e estar disponíveis para uso em uma reunião.
- Remote Access e Access Anywhere não são suportados porque seus agentes são removidos automaticamente pela plataforma Citrix subjacente após o reinício do sistema operacional.
- Os usuários das Ferramentas de Produtividade não podem iniciar uma reunião One-Click ou iniciar uma reunião agendada do Outlook.

Matriz de Compatibilidade das Ferramentas de Produtividade e Aplicativos Cisco WebEx Meetings

Esta tabela lista os números de compilação para o aplicativo WebEx Meetings e as Ferramentas de Produtividade baixadas para cada versão do Cisco WebEx Meetings Server.

Versão do Cisco WebEx Meetings Server	Número ISO	Ferramentas de Produtividade Cisco WebEx	Aplicativo Cisco WebEx Meetings
1.5 MR3	1.5.1.323	2.80.501.321	27.32.151.321
1.5 MR4	1.5.1.402/1.5.1.400	2.80.501.401	27.32.151.401
1.5 MR5	1.5.1.503	2.80.501.503	27.32.151.503 (Windows) orion1.5.MR3.FCS.0.0.503 (Mac)
2.0[26]	2.0.1.2	2.82.0.1713	27.32.200.1713
2.0 MR1	2.0.1.107	2.82.0.1713	27.32.200.1713
2.0 MR2	2.0.1.205	2.82.0.1713	27.32.200.1713
2.0 MR3	2.0.1.302	2.82.1.302	27.32.200.302
2.0 MR4	2.0.1.407	2.82.1.407	27.32.200.407 orion2.0.MR4.0.0.407 (MAC OS)
2.0MR5	2.0.1.507	2.82.1.507	27.32.201.507 (Windows) orion2.0.MR5.0.0.507 (Mac)

Versão do Cisco WebEx Meetings Server	Número ISO	Ferramentas de Produtividade Cisco WebEx	Aplicativo Cisco WebEx Meetings
2.0MR6	2.0.1.611	2.82.1.606	27.32.200.606 (Windows) orion2.0.MR6.0.0.606 (Mac)
2.0MR7	2.0.1.707	2.82.1.701	27.32.201.701 (Windows) orion2.0.MR7.0.0.701 (Mac)
2.0MR8	2.0.1.809	2.82.1.701	27.32.201.701 (Windows) orion2.0.MR7.0.0.701 (Mac)
2.0MR8 Security patch 1	2.0.1.839	2.82.1.839	27.32.201.839 (Windows) orion2.0.MR8.0.0.839 (Mac)
2.0MR9	2.0.1.918	2.82.1.910	27.32.201.910 (Windows) orion2.0.MR9.0.0.910 (Mac)
2.5	2.5.1.29	2.82.500.2353	29.9.2.10085 (Windows e Mac)
2.5MR1	2.5.1.132	2.82.500.3339	29.11.3.4858 (Windows e Mac)
2.5MR2	2.5.1.227	2.82.501.10002	29.12.0.10076 (Windows e Mac)
2.5MR3	2.5.1.3009	2.82.501.10008	29.12.0.10076 (Windows e Mac)
2.5MR4	2.5.1.4378	2.82.502.8	29.13.11.10173 (Windows e Mac)
2.5MR5	2.5.1.5033	2.82.502.9	29.13.12.10182 (Windows e Mac)
2.5MR6	2.5.1.6139	2.82.502.11	29.13.41.30001 (Windows e Mac)
2.6	2.6.1.39	2.82.502.1078	30.1.0.20002 (Windows e Mac)

Versão do Cisco WebEx Meetings Server	Número ISO	Ferramentas de Produtividade Cisco WebEx	Aplicativo Cisco WebEx Meetings
2.6MR1	2.6.1.1099	2.82.6501.1082	30.5.2.10002 (Windows e Mac)
2.6MR2	2.6.1.2097	2.82.6520.1083	30.6.4.10003 (Windows e Mac)
2.6MR3	2.6.1.3096	2.82.6520.1090	30.10.1.10008 (Windows e Mac)
2.7	2.7.1.12	2.82.7000.1150	31.4.0.41 (Windows e Mac)
2.7MR1	2.7.1.1073	2.82.7000.1159	31.5.20.63 (Windows e Mac)
2.7MR2	2.7.1.2048 [27]	2.82.7000.1161	31.8.0.167 (Windows e Mac)
2.8	2.8.1.12 (Diferido. Use a versão 2.8.1.17.)	N/D	N/D
2.8	2.8.1.17	2.82.7000.1174	31.11.6.9

[26] Não está mais disponível.

[27] A atualização do software 2.7MR2 é apenas para sistemas que atualmente executam o Cisco WebEx Meetings Server versão 2.7.1.12 ou 2.7.1.1073 ou posterior.

Sobre as licenças do organizador

Este produto tem **Licenciamento baseado em organizador** que requer que você compre uma licença para cada usuário que **organiza** reuniões ou é atribuído manualmente uma licença. Um usuário não consome uma licença de Organizador participando ou agendando uma reunião em nome de terceiros. O cálculo do uso da licença para fins de relatório ocorre uma vez por mês, por exemplo, uma vez a partir de 1º a 31 de janeiro, e uma vez a partir de 1º a 28 de fevereiro, etc.

Observação Ao atualizar de uma versão anterior para a versão 2.5 ou superior, todas as licenças que estavam no sistema original são lançadas a partir da sua designação para os usuários. Os usuários podem readquirir licenças organizando reuniões ou atribuindo licenças manualmente. Isto também é verdade ao instalar um sistema de Múltiplos Centros de Dados (MDC). As licenças do organizador são perdidas no centro de dados que está no sistema MDC. Essas licenças podem ser reorganizadas no sistema MDC após o Registro.

Na página **Relatórios**, você pode pedir um relatório que fornece o número total de licenças consumidas. Além disso, recomendamos que você veja o Relatório de Resumo em PDF que mostra as tendências de consumo

de licença. Ao ver a tendência geral da licença, você pode planejar futuras aquisições de licenças de forma mais eficaz, para coincidir com a crescente adoção desse sistema na sua empresa.

CAPÍTULO 11

Integração do Cisco Unified Communications Manager (CUCM)

O Cisco WebEx Meetings Server versão 2.8 é compatível com as seguintes versões do Cisco Unified Communications Manager:

- 11.5(1)SU1
- 11.0(1a)
- 10.5.2
- 10.5
- 10.0
- 9.1
- 9.0

Observação No CWMS 2.7 e posterior, o suporte ao TLS 1.0 foi removido (CSCuu40706). O suporte ao TLS 1.2 foi introduzido no CUCM versões 10.5 e posteriores.

- Integração do Session Manager Edition (SME), página 201
- Compatibilidade de extremidade de áudio, página 202

Integração do Session Manager Edition (SME)

O CWMS suporta o Session Manager Edition (SME)

Usuários Unified MP podem escolher o Cisco WebEx como o provedor de web conferência durante o agendamento de uma reunião Unified MP. A integração do Cisco WebEx está disponível no Cisco Unified MP 6.0.2 e versões posteriores. As conferências de voz e vídeo são fornecidas pelo Unified MP. As informações de discagem de voz e vídeo devem ser fornecidas aos usuários WebEx para que eles para entrar na reunião, ou eles podem usar o recurso de out-dial que está disponível no WebEx para entrar na reunião.

Compatibilidade de extremidade de áudio

Você pode usar qualquer extremidade com base em padrões de áudio que se conecta ao Cisco Unified Communications Manager para participar de uma reunião WebEx. As extremidades de áudio suportadas incluem os Telefones IP da Cisco, extremidades do Telepresence e os dispositivos PSTN, como telefones celulares e telefones fixos. Muitas extremidades de áudio suportam a conectividade de áudio e de vídeo. No entanto, apenas a conectividade de áudio para o Cisco WebEx Meetings Server é suportada.

Para permitir que usuários de fora da organização participem de reuniões WebEx usando dispositivos PSTN, sua empresa deve implantar Gateways Analógicos para VoIP, tais como Roteadores de Serviços Integrados (ISR) da Cisco. Os telefones IP listados abaixo foram testados com o Cisco WebEx Meetings Server:

- Cisco 7960
- Cisco 7970
- Cisco 7971
- Cisco 7940
- Cisco 9951
- Cisco 9971
- Cisco 7980 (Tandberg)
- Cisco 7975
- Cisco E20
- Cisco Telepresence (CTS 1100)
- Cisco Ip Communicator
- Telefone com vídeo Lifesize
- Tandberg 1000
- Tandberg 1700
- Polycom
- Cisco Cius
- C20
- EX 60
- EX 90

Outros terminais compatíveis com o Cisco UC também devem funcionar normalmente. Para obter uma lista de telefones IP do Cisco Unified suportados pelo Cisco Unified Communications Manager e os pacotes de dispositivos disponíveis para cada modelo, consulte Recurso de telefone IP do Cisco Unified e Matriz de compatibilidade do pacote de dispositivos do Cisco Unified Communications Manager.