

Gerente unificado da interação da Web e do email: Servidor de Web em um exemplo da configuração DMZ

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Informações de Apoio](#)

[Configurar a website padrão](#)

[Instale arquivos para o servidor de arquivo](#)

[Instale arquivos para o filtro de JBoss ISAPI](#)

[Configurar a website padrão](#)

[Crie diretórios virtuais](#)

[Configurar diretórios virtuais](#)

[Crie a extensão de serviço da Web dos "jboss-iis"](#)

[Advertência conhecida](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

Os servidores de aplicativo do Cisco Unified Web Interaction Manager (WIM unificado) residem tipicamente dentro de uma rede interna dos negócios, assim que significa que um servidor de Web externo está exigido para sessões do bate-papo com os clientes no Internet. Alcance aos sistemas de arquivo compartilhado e os server do base de dados (DB) em um intranet corporativa são proibidos tipicamente dos servidores de Web externos em uma zona desmilitarizada (DMZ). Isto significa que o componente do servidor de Web para o Cisco Unified E-Mail Interaction Manager (EIM unificado) e WIM não pode ser instalado usando o instalador.

Este documento descreve como configurar manualmente um servidor de Web situado em um DMZ.

[Pré-requisitos](#)

[Requisitos](#)

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- **A instalação unificada WIM** - Todos os componentes unificados exigidos WIM devem ser instalados e verificado nos server situados dentro do intranet corporativa.
- **Exigências DNS** - Um registro externo DNS deve ser criado para os servidores de Web externos. Se há servidores de Web externos do múltiplo, o registro externo DNS deve corresponder a um equilibrador da carga.
- **Exigências do Firewall** - O firewall externo (entre o Internet e o DMZ) deve ser configurado a fim permitir o acesso na porta 80 para o hostname no registro externo DNS. O Firewall interno (entre o DMZ e o intranet corporativa) deve ser configurado a fim permitir o acesso nas portas 15006, 15007, e 15008.

Todos os componentes unificados exigidos WIM devem ser instalados e verificado nos server situados dentro do intranet corporativa.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Informações de Apoio

Para esta discussão, supõe-se que o site configurado é a “website padrão”. As etapas necessárias a fim criar um site não são incluídas neste documento.

Configurar a website padrão

Estas seções descrevem como configurar a website padrão no IIS para Cisco unificaram WIM. Estas etapas devem ser executadas em cada servidor de Web externo na instalação unificada WIM.

Instale arquivos para o servidor de arquivo

Desde que a parte do arquivo no servidor de arquivo não pode ser alcançada do DMZ, os arquivos no servidor de arquivo devem manualmente ser instalados em cada servidor de Web externo.

Conclua estes passos:

1. No servidor de arquivo, crie um arquivo zip do dobrador de `Cisco_Home > eService`.

2. Copie o arquivo zip a cada servidor de Web externo.
3. Em cada servidor de Web externo, crie um dobrador nomeado `Cisco` (por exemplo, `C:\Cisco`).
4. Em cada servidor de Web externo, abra o zíper o arquivo zip no dobrador criado em etapa 3, tais que o pathname resultante é `C:\Cisco\eservice`.

Instale arquivos para o filtro de JBoss ISAPI

Abra o zíper `jboss-iis.zip` no diretório home para a website padrão (tipicamente, `C:\inetpub\wwwroot`). Isto conduz a `C:\inetpub\wwwroot\jboss - iis`. Verifique que este dobrador contém estes arquivos:

- `isapi_redirect.dll`
- `isapi_redirect.properties`
- `uriworkermap.properties`
- `workers.properties`

Atualize `isapi_redirect.properties`

O arquivo de configuração de filtro `isapi_redirect.properties` de JBoss ISAPI contém uma propriedade que especifica onde um arquivo de registro é encontrado. O valor para esta propriedade deve ser atualizado a fim refletir o lugar deste arquivo de registro em uma unidade local.

Termine estas etapas a fim atualizar este valor:

1. Encontre a propriedade `log_file`.
2. Se for necessário, substitua `C:\Cisco` com o pathname do dobrador criado em etapa 3 de [arquivos Install para o servidor de arquivo](#).
3. Substitua `hostname.egain.net` com o hostname totalmente qualificado do servidor de Web externo.

Repita estas etapas em cada servidor de Web externo.

Atualize `workers.properties`

O arquivo de configuração de filtro `workers.properties` de JBoss ISAPI contém três propriedades que especificam o hostname totalmente qualificado para um server de aplicativo de JBoss. Cada servidor de Web externo deve ser emparelhado com um server de aplicativo diferente de JBoss. O valor para esta propriedade deve ser atualizado a fim refletir o hostname para o server de aplicativo apropriado de JBoss.

Termine estas etapas a fim atualizar estes valores:

1. Para a propriedade `worker.default.host`, substitua `appserver.egain.net` com o hostname totalmente qualificado para o server de aplicativo apropriado de JBoss.
2. Para a propriedade `worker.pushlet.host`, substitua `appserver.egain.net` com o hostname totalmente qualificado para o server de aplicativo apropriado de JBoss.
3. Para a propriedade `worker.live.host`, substitua `appserver.egain.net` com o hostname totalmente qualificado para o server de aplicativo apropriado de JBoss.

Repita estas etapas em cada servidor de Web externo.

Configurar a website padrão

Conclua estes passos:

1. Clicar com o botão direito a **website padrão**, e escolha **propriedades do** menu suspenso.
2. Na aba do diretório home, verifique os valores para estes campos: Para o caminho local, verifique que o valor é **C:\Inetpub\wwwroot**. Para o pool do aplicativo, verifique que o valor é **DefaultAppPool**.
3. Adicionar mapeamentos do aplicativo para estes Ramais na website padrão: `.controller.egain.jsp`
4. Clique a **configuração...** a fim lançar o indicador da configuração do aplicativo.
5. Para cada mapeamento do aplicativo: O clique **adiciona** a fim lançar adicionar/edita o indicador do mapeamento da extensão. Entre em **C:\Inetpub\wwwroot\jboss - os iis \ isapi_redirect.dll para o executável**. Incorpore um dos Ramais alistados acima para a extensão. Incorpore o **GET, CABEÇA, CARGO, TRAÇO** para os verbos. Certifique-se que **motor do script** está verificado. Certifique-se que **para verificar que o arquivo existe** não está verificado.
6. Na aba do site, verifique que o valor para o campo do endereço IP de Um ou Mais Servidores Cisco ICM NT é **toda Unassigned**. Isto é válido enquanto a website padrão é o único site configurado.
7. Nos filtros ISAPI catalogue, **adicionar... um** filtro ISAPI com estes valores de campo: **jboss-iis** para o nome do filtro **C:\Inetpub\wwwroot\jboss - iis \ isapi_redirect.dll para o executável**
8. Na aba dos cabeçalhos HTTP, adicionar estes MIMICAM tipos na website padrão:

Crie diretórios virtuais

Conclua estes passos:

1. Crie estes diretórios virtuais na website padrão: `<partition_name>` - O nome da separação especificado ao instalar o aplicativo (por exemplo, "padrão"). sistema jboss-iis Há um assistente que alerte para a informação exigida a fim criar um diretório virtual. O assistente é compreendido destes sequência das telas:
2. Na tela do diretório virtual aliás, dê entrada com o nome do diretório virtual que está sendo criado (por exemplo, "sistema" ou "jboss-iis").
3. Na tela do diretório de conteúdo do site, incorpore o pathname absoluto para o dobrador eService criado dentro [instalam arquivos para o servidor de arquivo](#) (por exemplo, `C:\Cisco\eService`) ao criar os diretórios virtuais do "`<partition_name>`" ou do "sistema", e entram em `C:\Inetpub\wwwroot\jboss - iis` ao criar o diretório virtual dos "jboss-iis".
4. Nas permissões de acesso do diretório virtual selecione, aceite a configuração padrão (permissão "lida" somente).

Configurar diretórios virtuais

Conclua estes passos:

1. Clicar com o botão direito no `<partition_name>`, no **sistema**, ou nos diretórios virtuais dos **jboss-iis**, e selecione **propriedades do** menu suspenso.
2. Na aba do diretório virtual, mude o valor para permissões Execute aos **scripts e executáveis**.
3. Na aba dos documentos, a lista de páginas satisfeitas do padrão deve conter somente uma entrada para os diretórios virtuais do `<partition_name>` e do sistema: `<partition_name>.asp`

- para o diretório virtual do <partition_name>**system.asp** para o diretório virtual do sistema
4. Para o diretório virtual dos jboss-iis, a lista de páginas satisfeitas do padrão deve estar vazia. Verifique que a caixa de seleção da **página satisfeita do padrão da possibilidade** não está selecionada.

[Crie a extensão de serviço da Web dos “jboss-iis”](#)

Termine estas etapas a fim criar a extensão de serviço da Web dos jboss-iis:

1. Selecione o dobrador da **extensão de serviço da Web**.
2. Selecione **adicionar um link novo da extensão de serviço da Web....**
3. Entre em **jboss-iis** para o nome da extensão.
4. Entre em **C:\inetpub\wwwroot\jboss - os iis \ isapi_redirect.dll** para os arquivos requerido.
5. Verifique o **estado da extensão do grupo** à caixa de seleção **permitida**.

[Advertência conhecida](#)

Desde que a parte do arquivo é localizada ao servidor de Web no DMZ, todas as mudanças ao aplicativo (por exemplo, os usuários que fazem mudanças ao dicionário adicionando ou suprimindo palavras) precisam de ser propagadas manualmente do sistema de arquivos a cada servidor de Web no DMZ. A mesma coisa deve ser feita quando as correções de programa são aplicadas ao servidor de arquivo.

Como um melhor prática, certifique-se de que estes diretórios são sincronizados automaticamente cada noite:

- escaninho
- config
- I10n
- META-INF
- relatórios
- Web
- webtemp

[Verificar](#)

No momento, não há procedimento de verificação disponível para esta configuração.

[Troubleshooting](#)

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

[Informações Relacionadas](#)

- [Suporte Técnico e Documentação - Cisco Systems](#)