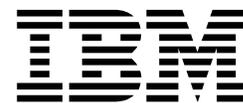


IBM Host On Demand Versão 12.0



Planejamento, Instalação e Configuração do Host On-Demand

IBM Host On Demand Versão 12.0



Planejamento, Instalação e Configuração do Host On-Demand

Nota

Antes de utilizar estas informações e o produto suportado por elas, leia as informações no Apêndice E, “Avisos”, na página 169.

Nona edição (fevereiro de 2016)

Esta edição aplica-se à Versão 12 do IBM® Host On Demand (número de programa 5724-I20) e a todas as liberações e modificações subsequentes até que seja indicado de outra forma em novas edições.

© Copyright IBM Corporation 1997, 2016.

Índice

Sobre este manual	vii
Sobre Outras Documentações do Host On-Demand	vii
Convenções Utilizadas Neste Manual	ix
Terminologia	ix
Termos relacionados ao Java	x

Parte 1. Planejamento para Host On-Demand 1

Capítulo 1. Introdução ao IBM Host On Demand 3

O que é Host On Demand?	3
Como Funciona o Host On-Demand?	3
Por que Utilizar o Host On-Demand?	5
Uma Abordagem Econômica para Conectividade	5
Gerenciamento Centralizado dos Dados de	
Configuração	5
Conexão Direta em Qualquer Servidor Telnet	5
Interface do Usuário Baseada no Navegador.	5
Suporte para Diferentes Plataformas e Ambientes	
de Rede	6
Suporte para Java.	6
Suporte para Internet Protocol Versão 6	6
Suporte para Vários Idiomas Nacionais	6
Conexões Seguras	6
Arquivos HTML Personalizados	7
Toolkit para Criar Novos Aplicativos e-business	7
Programmable Host On-Demand	7
APIs do gerenciador de sessões do Host On	
Demand	8
Suporte para o WebSphere Portal	8
Conexões com bancos de dados DB2 em	
servidores IBM System i	8
O que Há de Novo?	8
Obtendo as Informações Mais Recentes sobre o	
Host On-Demand.	8
Novas funções no Host On Demand Versão 12	9

Capítulo 2. Planejamento para Implementação 11

Compreendendo o Modelo Baseado em HTML	11
Compreendendo o Modelo Baseado em Servidor de	
Configuração	12
Compreendendo o Modelo Combinado	13
Considerações sobre a Implementação do Cliente.	14

Capítulo 3. Planejando o Java no cliente 15

Melhorias no cliente em cache para Java.	15
Limites de suporte	15
Recursos aprimorados fornecidos pelo Java.	16
Fazendo download de um cliente com o Java	16
Mac OS X com Java	17

Limitações do Mac OS X	17
Tempos de inicialização um pouco mais lentos	
com clientes Java	17
Limitações de plug-ins Java específicos	18
Limitações com applets fornecidos pelo cliente e	
Java	18
Limitações com usuários restritos e Java.	18
Navegadores e plug-ins Java	18
Navegadores ativados para Java	18
Navegadores e Plug-ins Suportados por Clientes	
Host On-Demand	18
Microsoft Internet Explorer com um plug-in Java	19
Firefox com um plug-in Java	19

Capítulo 4. Planejamento para Segurança 21

Transport Layer Security (TLS)	21
Como a segurança TLS funciona	21
TLS para o Host On Demand	23
Segurança do Servidor Web	28
Segurança da Configuração	28
O Redirecionador	28
Por que Utilizar o Redirecionador?	29
Como o Redirecionador Funciona	29
Capacidade de Carga do Redirecionador	30
Sistemas operacionais suportados pelo	
Redirecionador	30
Utilizando o Host On-Demand com um Firewall	32
Configurando Portas de Firewall	33
Conectando-se a um Sistema Host Através de um	
Servidor Proxy	35
Segurança do ID de Usuário.	36
Web Express Logon.	36
Autenticação Nativa	36
Logon de Domínio do Windows	37
Ambientes FIPS	37

Capítulo 5. Planejamento para Suporte ao Idioma Nacional 39

Idiomas Suportados	39
Páginas de Códigos do Host Suportadas.	40
Páginas de Códigos 3270 e 5250	40
Páginas de Códigos VT	43
Páginas de códigos do Gateway CICS	43
Suporte ao JIS2004 Unicode Japonês	44
Mapeamento de Caracteres Definido pelo Usuário	44
Suporte a Unicode para i/OS e OS/400	44

Parte 2. Instalando, Efetuando Upgrade e Desinstalando o Host On-Demand 45

Capítulo 6. Instalando o Servidor Host On-Demand e o Software Relacionado . 47

Instalando o Host On-Demand usando o Installation Manager	47
Links importantes	47
Antes da instalação do HOD	47
Preparando para instalação	47
Efetuando Upgrade de Versões Anteriores do Host On-Demand	48
Instalando o Host On-Demand	48
A GUI do Installation Manager	48
Assistente de Implementação	50
Fazendo upgrade de versões anteriores do Assistente de Implementação	51
Instalando o Deployment Wizard	51
Fazendo o Download da Imagem de Instalação do Deployment Wizard a partir de um Servidor Host On-Demand	52
Host Access Toolkit.	52
Fazendo upgrade de versões anteriores do Host Access Toolkit	52
Instalando o Host Access Toolkit	52
Instalando o Modo de Console	53
Sobre a instalação no Modo de Console	53
Antes de instalar o HOD no IBM iSeries.	54
Procedimento de instalação	55
Instalando o Assistente de Implementação no Modo do Console	58
Instalando o Host Access Toolkit no Modo do Console.	58
Instalando no modo silencioso	58
Procedimento de instalação	59
Instalando o Servlet de Configuração	60
Implementando o Servlet no WebSphere Application Server	60

Capítulo 7. Desinstalando o Servidor Host On-Demand 63

Desinstalando o Host On-Demand usando o modo de console do Installation Manager	63
---	----

Parte 3. Configurando o Host On-Demand 65

Capítulo 8. Configurando os clientes de emulador do Host On Demand 67

Criando Arquivos HTML do Host On-Demand	67
Configurando Sessões do Host On-Demand	68
Utilizando o Deployment Wizard	69
Distribuindo a Saída do Deployment Wizard para o Seu Servidor Host On-Demand	69

Capítulo 9. Utilizando Clientes de Novos Usuários e de Administração do Host On-Demand 71

Carregando Clientes de Administração e de Novos Usuários	71
Clientes de administração	71

Utilitário do Diretório	72
Clientes de Novos Usuários	73

Capítulo 10. Utilizando os Clientes de Emulador do Host On-Demand 75

Carregando Clientes de Emulador	75
Selecionando o cliente apropriado	76
Clientes em Cache	77
Instalando Clientes em Cache	78
Removendo o Cliente Armazenado em Cache	81
Problemas de suporte a clientes em cache ao acessar vários servidores Host On Demand.	83
Suporte a clientes em cache para Windows	83
Suporte a clientes em cache para Mac OS X (somente clientes Java)	84
Resolução de Problemas de Clientes em Cache	85
Cliente Web Start	85
Instalando o cliente Web Start	86
Configurando seu servidor da web para o Web Start.	88
Fazendo upgrade do cliente Web Start	88
Incluindo componentes do Web Start após a instalação inicial.	89
Usuários restritos do Web Start e do Windows.	89
Marcando sessões com o Web Start	89
Usando o Web Start com HTTPS	89
Removendo o cliente Web Start.	89
Clientes de Download	89
Ativando o Cliente de Download	90
Ativando o cliente de download depois de instalar o cliente em cache ou o cliente Web Start.	90
Clientes de Emulador Predefinidos	90
Reduzindo o Tamanho do Cliente de Download	91
Implementando archives e classes Java fornecidos pelo cliente	92
Usando o parâmetro HTML AdditionalArchives	92
Implementando a partir do Diretório de Publicação.	93
Dicas e sugestões para archives.	93

Capítulo 11. Utilizando Clientes Database On-Demand 95

Funções do Banco de Dados em Clientes de Emulação de Vídeo e em Macros	96
Iniciando um cliente do Database On-Demand	96
Clientes Predefinidos do Database On-Demand	97
Configurando o Database On-Demand para Usuários	97
Obtendo e Instalando um Driver JDBC	98
Formatos de Arquivo para Acesso ao Banco de Dados	98
Utilizando Várias Páginas de Códigos com o Database On-Demand	98
Páginas de Códigos do Database On-Demand Suportadas	99

Capítulo 12. Criando e Implementando Bibliotecas de Macros do Servidor 101

Implementando uma Biblioteca de Macros do Servidor para um Servidor Web	101
---	-----

Implementando uma Biblioteca de Macros do Servidor em uma Unidade Compartilhada	102
---	-----

Capítulo 13. Modificando Propriedades de Sessão

Dinamicamente	105
Configurando o Arquivo HTML Inicial	105
Definindo o Código Base	105
Incluir o Parâmetro ConfigBase	106
Substituindo Parâmetros HTML	106
Propriedades da Sessão Específicas que Podem Ser Substituídas	107
Exemplo nº1: Substituindo o Nome da LU Baseado no Endereço IP do Cliente	111
Exemplo nº2: Permitindo que o Usuário Especifique o Host de Conexão Utilizando um Formulário HTML	113

Capítulo 14. Configurando o Host On-Demand no zSeries

117	
Configurando Diretórios de Publicação e Privados de Leitura/Gravação Separados	117
Configurar um Sistema de arquivos separado para o diretório privado do Host On-Demand	117
Configurar um Diretório de Publicação do Usuário Separado	117
Considerações sobre Migração para z/OS	118
Fazendo Backup do Diretório Privado	118
Instalando o Assistente de Desenvolvimento a partir do servidor z/OS	119

Capítulo 15. Configurando o Host On-Demand no IBM System i

121	
Configurando, iniciando e parando o Gerenciador de Serviços do Host On Demand no IBM System i	121
Configurar	121
Iniciar	122
Parar	122
Trabalhar com Status do HOD Server	122
Gerenciamento de Certificados	123
Iniciar Information Bundler.	124
Criar tabela de definição de impressora HOD	124
Usando o Assistente de Implementação com o IBM System i	124
Configurando servidores IBM System i para conexão segura	125
Instalando e configurando o Host On-Demand com TLS no i/OS e OS/400	125
Configurando um Servidor Telnet para Conexão Segura.	126
Configurando o Conjunto de Chaves CustomizedCAs do Host On-Demand	126
Autenticação do Cliente	127
Configurando o Proxy OS/400 do Host On-Demand para Conexões Seguras	127
Serviço Seguro da Web	127
Suporte a Unicode para i/OS e OS/400	128
Informações Gerais	128
Informações de Programação do Host	129

Capítulo 16. Implementando o Host On-Demand com o WebSphere Portal

131	
Como o Host On-Demand Funciona com o Portal Server	131
Utilizando Clientes Host On-Demand com o Portal Server	132
Limitações de Acesso ao Host On-Demand Através de um Portlet	132
Considerações Especiais ao Utilizar um Portlet do Host On-Demand	133
Estendendo os Portlets do Host On-Demand	135

Capítulo 17. Suporte ao Eclipse-Plugin

137	
Criando Plug-ins do Host On-Demand	137
Configurando Propriedades da Sessão Dinamicamente.	139
Utilizando um Diretório de Publicação do Usuário Separado	140
Visualizar IDs Utilizados no Plugin do Host On-Demand	141
Limitações sobre o uso do Host On Demand em um ambiente Eclipse-Plugin	141

Capítulo 18. Configurando o Servidor Host On-Demand para Utilizar o LDAP

143	
Configurando o Suporte LDAP	143
Instalando as Extensões de Esquema	144
Configurando o Servidor Host On-Demand para Utilizar o LDAP como um Data Store	145

Apêndice A. Utilizando Clientes Instalados Localmente

147	
Sistemas Operacionais que Suportam Clientes Instalados Localmente	147
Instalando o Cliente Local	147
Iniciando o Cliente Local	147
Removendo o Cliente Local	147

Apêndice B. Utilizando a Interface de Linha de Comandos IKEYCMD

149	
Configuração de Ambiente para Interface da Linha de Comandos IKEYCMD	149
Sintaxe de Linha de Comandos IKEYCMD	150
Lista de Tarefas da IKEYCMD para o Host On-Demand	151
Criando um Novo Banco de Dados de Chaves	151
Definindo a Senha do Banco de Dados	152
Alterando a Senha do Banco de Dados	152
Listando CAs	153
Criando um novo par de chaves e solicitação de certificado	153
Armazenando o Certificado de Servidor	154
Recebendo um Certificado Assinado pela CA	154
Armazenando um Certificado de CA	155
Criando um Certificado Auto-assinado	155
Tornando os Certificados de Servidor Disponíveis para os Clientes	156
Adicionando a Raiz de um CA Desconhecido em CustomizedCAs.p12	156

Exportando Chaves	157
Importando Chaves	158
Mostrando a chave padrão em um banco de dados de chaves.	158
Armazenando o Banco de Dados Criptografado em um Arquivo Stash.	158
Visão Geral dos Parâmetros de Linha de Comandos IKEYCMD	159
Visão Geral das Opções de Linha de Comandos IKEYCMD	160
Chamada da Linha de Comandos	161
Arquivo de Propriedades do Usuário	163

Apêndice C. Utilitário P12 Keyring	165
Uso.	165

Opções	165
Exemplos.	166

Apêndice D. Opções da Linha de Comandos do Ativador de Plataforma Nativa	167
---	------------

Apêndice E. Avisos	169
---------------------------	------------

Apêndice F. Marcas Registradas	171
---------------------------------------	------------

Sobre este manual

O guia *Planejamento, Instalação e Configuração do Host On-Demand* ajuda a planejar, instalar e configurar o programa Host On-Demand. Este manual foi escrito para administradores. Ele contém três partes principais.

Parte 1, “Planejamento para Host On-Demand”, na página 1 fornece informações a serem consideradas sobre o Host On-Demand antes da instalação e implementação. Por exemplo, que plataforma de servidor você utilizará? Que modelo de implementação será utilizado? Como você trata da segurança?

Parte 2, “Instalando, Efetuando Upgrade e Desinstalando o Host On-Demand”, na página 45 apresenta os procedimentos passo a passo com base em cada sistema operacional.

Parte 3, “Configurando o Host On-Demand”, na página 65 descreve os diferentes modelos de configuração para especificar como as informações de configuração da sessão são definidas e gerenciadas, como modificar dinamicamente as informações de configuração, como personalizar novos clientes e como implementar o Host On-Demand para os seus usuários.

Depois de instalar e configurar o Host On-Demand, utilize a ajuda on-line para obter informações sobre como definir sessões e executar outras tarefas administrativas.

Planejando, instalando e configurando o Host On Demand também está disponível no DVD-ROM e no Knowledge Center do Host On Demand.

Sobre Outras Documentações do Host On-Demand

Além do guia *Planejamento, Instalação e Configuração do Host On-Demand*, o Host On-Demand também fornece outras fontes de informações que ajudam na utilização do produto. Para acessar a documentação descrita aqui, acesse o Knowledge Center do Host On Demand. A maior parte da documentação também está incluída no produto Host On-Demand ou no Toolkit DVD-ROMs.



O recurso MySupport permite personalizar a visualização de suporte e registrar-se para receber semanalmente notificações por e-mail com alertas sobre novos fix packs, downloads e informações de suporte técnico importantes de produtos IBM. Para registrar-se no MySupport, execute as instruções fornecidas nesta Nota Técnica.

- *Online help.* A ajuda on-line é a primeira origem de informações para administradores e usuários depois de concluída a instalação do Host On-Demand. Ela fornece etapas detalhadas sobre como executar tarefas do Host On-Demand. Um conteúdo e um índice ajudam você a localizar painéis de ajuda orientados por tarefas e painéis de ajuda conceituais. Enquanto você utiliza a GUI (Interface Gráfica com o Usuário) do Host On-Demand, os botões de ajuda ativam os painéis de ajuda no nível do painel, para a GUI.
- *Program Directory.* O diretório do programa orienta como instalar o Host On-Demand nas plataformas z/OS.

- *Readme file.* Este arquivo, `readme.html`, contém informações sobre o produto que foram descobertas muito tarde e por isso não foram incluídas na documentação do produto.
- *Web Express Logon Reference.* Esse manual fornece uma abordagem passo a passo para compreender, implementar e resolver problemas no Web Express Logon. Ele oferece uma visão geral do Web Express Logon, vários exemplos etapa por etapa para ajudar a planejar e implementar o Web Express Logon em seu ambiente, bem como várias APIs para escrever macros e plug-ins personalizados.
- *Macro Programming Guide.* Esse manual descreve como criar macros do Host On-Demand para automatizar interações do usuário com aplicativos host ou para transmitir dados entre um aplicativo host e um aplicativo nativo. Esse manual fornece informações detalhadas sobre todos os aspectos de desenvolvimento de macros e inclui informações revisadas sobre a linguagem de macro anteriormente publicada no Host Access Beans for Java Reference.
- *Host Printing Reference.* Depois de configurar as sessões do host, utilize o Host Printing Reference para permitir que os usuários imprimam informações sobre a sessão do host em um arquivo ou impressora local ou conectada à LAN.
- *Session Manager API Reference.* Este manual fornece APIs JavaScript para gerenciar sessões do host e interações baseadas em texto com sessões do host.
- *Programmable Host On-Demand.* Esse manual fornece um conjunto de APIs Java que permitem aos desenvolvedores integrar várias partes do código do cliente Host On-Demand, como terminais, menus e barras de ferramentas, em seus próprios aplicativos e applets Java personalizados.
- *Toolkit Getting Started.* Este manual explica como instalar e configurar o Host On-Demand Toolkit, que é fornecido com o Host Access Client Package, mas é instalado a partir de um DVD-ROM diferente do produto base Host On-Demand. O Host On-Demand Toolkit complementa o produto base Host On-Demand, oferecendo Java beans e outros componentes para ajudar a maximizar a utilização do Host On-Demand em seu ambiente.
- *Host Access Beans for Java Reference.* Este manual faz parte do Host On-Demand Toolkit. Utilizado como referência para programadores que desejam personalizar o ambiente do Host On-Demand utilizando Java beans e criar macros para automatizar as etapas nas sessões do emulador.
- *Programmer's Guide for the AS/400 Toolbox for Java.* O Guia do Programador para o AS/400 Toolbox para Java está localizado no DVD do Toolkit no diretório `as400`. O guia está disponível em arquivos zip para os seguintes idiomas: inglês, japonês, coreano, espanhol e russo.
- *Host Access Class Library Reference.* Este manual faz parte do Host On-Demand Toolkit. Utilizado como referência para programadores que desejam escrever applets e aplicativos Java que possam acessar informações do host no nível fluxo de dados.
- *J2EE Connector Reference.* Este manual faz parte do Host On-Demand Toolkit. Ele serve como uma referência para os programadores que desejam escrever applets e servlets que acessam aplicativos compatíveis com o Java Enterprise Edition (J2EE).

Convenções Utilizadas Neste Manual

As seguintes convenções tipográficas são utilizadas em *Planejamento, Instalação e Configuração do Host On-Demand*:

Tabela 1. Convenções Utilizadas Neste Manual

Convenção	Significado
Espaçamento Fixo	Indica o texto que você precisa inserir em um prompt de comandos e os valores que precisa usar literalmente, como comandos, funções e atributos de definição de recurso e seus valores. O espaçamento fixo também indica exemplos de código e texto da tela.
<i>Itálico</i>	Indica valores de variáveis que precisam ser fornecidos (por exemplo, você fornece o nome de um arquivo para <i>file_name</i>). Itálico também indica ênfase e os títulos dos manuais.
Return	Refere-se à tecla rotulada com a palavra Return, a palavra Enter ou a seta para a esquerda.
>	Quando utilizado para descrever um menu, mostra uma série de seleções do menu. Por exemplo, "Clique em Arquivo > Novo" significa "No menu Arquivo, clique no comando Novo." Quando utilizado para descrever uma exibição em árvore, mostra uma série de expansões da pasta ou do objeto. Por exemplo, "Expandir Servlet HODConfig > Sysplexes > Plex1 > Servidores J2EE > BBOARS2" significa: <ol style="list-style-type: none">1. Expandir a pasta Servlet HODConfig2. Expandir a pasta Sysplexes3. Expandir a pasta Plex14. Expandir a pasta Servidores J2EE5. Expandir a pasta BBOARS2



Este gráfico é utilizado para destacar as notas para o leitor.



Este gráfico é utilizado para destacar as dicas para o leitor.

Terminologia

Esta seção descreve a terminologia utilizada em todo este manual.

applet Um programa escrito em Java que é referido em um arquivo HTML. Um applet é ativado por uma JVM (Java Virtual Machine) em execução em um navegador da Web.

aplicativo

Um programa ou conjunto de programas que executam uma tarefa ou função específica.

cliente armazenado em cache

Um cliente armazenado em cache do Host On-Demand é qualquer cliente Host On-Demand cujos componentes foram armazenados em cache (armazenados localmente para acesso rápido) na unidade de disco rígido de uma estação de trabalho do cliente.

diretório de publicação padrão

O diretório de publicação padrão é o HOD do subdiretório em seu diretório de instalação do servidor Host On Demand, por exemplo, c:\Program Files\IBM\HostOnDemand\HOD\ em plataformas Windows e /opt/IBM/HostOnDemand/HOD em AIX, Linux, Solaris, /QIBM/Programs/IBM/HostOnDemand/HOD em i (as/400) e /usr/lpp/HOD/hostondemand/HOD em plataformas z/OS.

cliente de download

Os clientes de download transferem por download os arquivos de applet necessários toda vez que os usuários acessam os arquivos HTML. Os clientes de download são geralmente utilizados em ambientes conectados pela LAN, porque as conexões de rede de alta velocidade reduzem o tempo necessário para transferi-los por download a partir do servidor Web.

cliente de emulador

Um cliente de emulador é um cliente do Host On-Demand que ativa uma sessão do emulador de terminal. O Host On-Demand inclui os seguintes clientes de emuladores: cliente armazenado em cache, cliente Web Start e cliente de download.

diretório de publicação do usuário separado

Fornecer uma localização gravável separada para implementar arquivos HTML personalizados, isolando-os dos arquivos fornecidos pelo Host On-Demand. Isso mantém o diretório de publicação do Host On-Demand somente leitura e facilita a aplicação de upgrades futuros do Host On-Demand. Observe que outros arquivos modificados pelo usuário (como os applets do cliente e os programas HACL) ainda precisarão ser executados a partir do diretório de publicação do Host On-Demand.

Web Application Server

O tempo de execução para aplicativos dinâmicos da Web. O servidor de aplicativos da Web inclui suporte para servlets Java, JSP (JavaServer Pages) e outras APIs (Application Programming Interfaces) corporativas Java. Um servidor de aplicativos da Web fornece comunicação, gerenciamento de recursos, segurança, gerenciamento de transações e capacidades de persistência para aplicativos da Web. Ele geralmente também inclui uma interface de administração para gerenciar o servidor e os aplicativos implementados.

servidor Web

Um servidor na Web que serve pedidos para documentos HTTP. Um servidor da Web controla o fluxo de transações enviadas e recebidas do navegador. Ele protege a confidencialidade de transações de clientes e garante que a identidade do usuário seja transmitida de maneira protegida para o servidor.

cliente Web Start

O cliente Web Start permite que usuários executem sessões do Host On-Demand sem um navegador. Os usuários iniciam sessões do Host On-Demand a partir do Gerenciador de Aplicativos do Java Web Start.

Termos relacionados ao Java

Observe os seguintes termos e seu uso neste documento.

Java Refere-se ao Java Runtime Environment (JRE) no servidor HOD ou no cliente HOD.

Navegador ativado para Java

Um navegador da web que executa applets Java na JVM Java de um plug-in Java instalado, por exemplo, Firefox e Internet Explorer com um plug-in Java. Para obter informações adicionais, consulte o "Navegadores e plug-ins Java" na página 18.

Cliente de emulador do Java, cliente em cache do Java, cliente de download de Java Uma versão do cliente Host On-Demand. A versão Java consiste em um conjunto completo de componentes do cliente Host On Demand compilados com um compilador Java.

Parte 1. Planejamento para Host On-Demand

Capítulo 1. Introdução ao IBM Host On Demand

O que é Host On Demand?

O IBM Host On Demand fornece aos usuários acesso ao host, com base ou não no navegador, seguro e com custo reduzido em ambientes baseados na intranet e extranet. O Host On-Demand está instalado em um servidor Web, simplificando a implementação e o gerenciamento administrativos, transferido por download do applet ou do aplicativo do Host On-Demand no navegador ou estação de trabalho cliente, fornecendo conectividade do usuário a aplicativos e dados críticos do host.

O Host On-Demand suporta emulação para tipos de terminais comuns, protocolos de comunicação, gateways de comunicação e impressoras, incluindo os seguintes:

- Terminais TN3270 e TN3270E
- Terminais TN5250
- Terminais VT52, VT100, VT220, VT320 e VT420
- O SSH (Secure Shell)
- Transport Layer Security (TLS)
- FTP (File Transfer Protocol)
- CICS (Customer Information and Control System) Transaction Gateway
- Impressoras TN3270E e TN5250

Você pode utilizar o Host Access Toolkit com base no componente Java para criar aplicativos e-business personalizados. Esse Toolkit contém um excelente conjunto de bibliotecas Java e interfaces de programação de aplicativos: Host Access Class Library (HACL), Host Access Beans for Java e conectores Java Enterprise Edition (J2EE). O Host On-Demand também inclui o Database On-Demand, que fornece uma interface para enviar consultas de Linguagem de Consulta Estruturada (SQL) para bancos de dados IBM DB2 hospedados nos sistemas IBM System i7.

Como Funciona o Host On-Demand?

A figura e a explicação a seguir mostram como funciona um sistema Host On-Demand. O Host On-Demand é um sistema cliente/servidor. Os clientes Host On-Demand são applets Java que são transferidos através de download do servidor Web para um navegador da Web em um computador remoto.

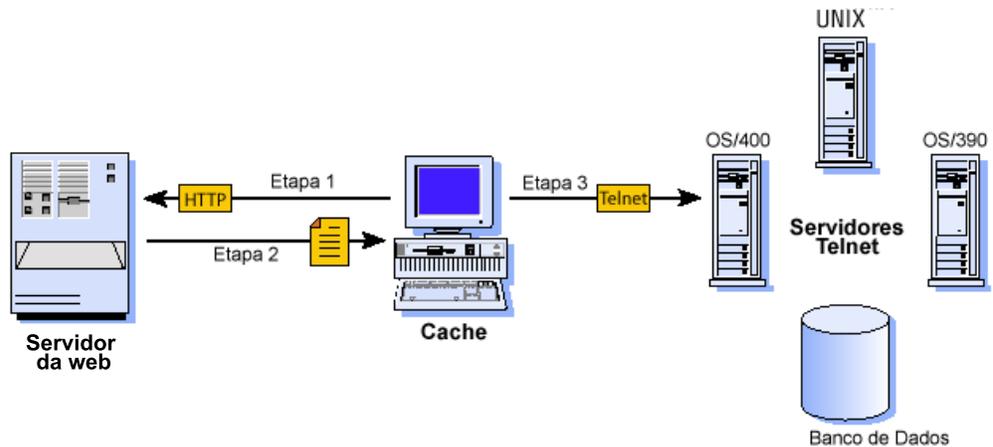


Figura 1. Como Funciona o Host On-Demand

Etapa 1. O usuário abre um navegador e clica em um hyperlink.

Etapa 2. O applet IBM Host On Demand é transferido por download para a estação de trabalho do cliente.

Etapa 3. Quando o applet é transferido por download, o IBM Host On Demand conecta-se diretamente a qualquer servidor Telnet para acessar aplicativos de host.

As informações da sessão são configuradas no arquivo HTML ou no servidor de configuração do Host On-Demand. Para obter informações adicionais sobre o servidor de configuração, consulte o Capítulo 2, "Planejamento para Implementação", na página 11.

Os applets de clientes do Host On-Demand podem ser executados como clientes de download, clientes Web Start ou clientes em cache. Os clientes de download são transferidos através de download a partir do servidor Web toda vez que são utilizados. Os clientes em cache e Web Start são transferidos por download a partir do servidor Web e armazenados no computador cliente. Após o download inicial, o cliente armazenado em cache é carregado a partir da máquina local. O cliente armazenado em cache verifica o servidor Host On-Demand quanto a novas versões do cliente e faz download da versão atualizada automaticamente.

O Host On-Demand inclui os seguintes componentes administrativos:

- O Deployment Wizard, uma ferramenta para criar arquivos HTML do cliente de emulador. O Deployment Wizard permite que os administradores gerem, de modo rápido e fácil, os arquivos HTML do Host On-Demand que são personalizados conforme as necessidades de uma organização.
- Os clientes de administração podem ser utilizados pelos administradores do sistema para definir sessões comuns, criar usuários e grupos e executar outras tarefas administrativas no servidor Host On-Demand.

Além disso, uma série de clientes predefinidos também são fornecidos com o Host On-Demand para demonstrar funções do cliente Host On-Demand para usuários e administradores (por exemplo, emulação, Database On-Demand, remoção do cliente armazenado em cache e utilitários de determinação de problemas).

Por que Utilizar o Host On-Demand?

Uma Abordagem Econômica para Conectividade

Você pode reduzir os custos de manutenção e aumentar o retorno de seu investimento instalando o Host On-Demand em um servidor Web, eliminando a necessidade de gerenciar desktops de usuários individuais.

Uma vez que os applets residem em um servidor e permitem que, quando necessário, sejam feitos download nos navegadores Web, não será mais preciso programar manutenção e atualizações. Efetue o upgrade do software no servidor e os usuários poderão receber o upgrade na próxima vez em que acessarem o applet do cliente.

Gerenciamento Centralizado dos Dados de Configuração

Os administradores podem definir e controlar centralmente todas as informações de configuração de sessão para seus usuários, incluindo opções de conexão, recursos de segurança, definições de macros, especificações do teclado e mapeamentos de cores. Além disso, os administradores têm controle total sobre quais campos o usuário pode ou não modificar e podem escolher o local para armazenar as atualizações do usuário.

Em plataformas Windows, a interface gráfica com o usuário padrão do Host On Demand é baseada no Nimbus Look and Feel fornecido pelo Java 1.6 e mais recente. O Nimbus Look and Feel para as interfaces gráficas com o usuário de administração pode ser desativado configurando o valor da variável de ambiente `SETHODNIMBUSGUI` como `false`.

Conexão Direta em Qualquer Servidor Telnet

Com o Host On-Demand, o applet do cliente contém a funcionalidade de emulação. Com o emulador residindo no cliente, o servidor de camada intermediária, tal como o IBM Communications Server ou um servidor SNA de terceiros, pode ser eliminado. Quaisquer problemas de desempenho e segurança apresentados com esta peça intermediária também serão removidos. Uma vez que o applet é prestativo para o cliente, é fácil conectá-lo diretamente em qualquer servidor Telnet padrão que forneça o melhor acesso aos dados solicitados. Você pode acessar várias sessões do host simultaneamente. Eliminando a necessidade de um servidor de nível intermediário, o Host On-Demand também minimiza restrições de capacidade. Para saber como isso funciona, consulte a Figura 1 na página 4.

Interface do Usuário Baseada no Navegador

O acesso baseado no navegador do Host On-Demand oferece a você uma maneira simples de gerenciar e implementar centralmente aplicativos e dados críticos do host. O Host On-Demand utiliza o poder da tecnologia Java para abrir as portas para seu sistema host sempre e em qualquer lugar que precisar dele, diretamente de seu navegador. Apenas clique em um hyperlink para lançar o applet Java do Host On-Demand. Esta solução de conectividade Web-para-host fornece acesso seguro do navegador da Web aos aplicativos host e aos dados do sistema através de emulação baseada em Java, dessa forma, você pode obter os aplicativos host existentes na Web sem programação. Devido ao fato do Host On-Demand ser baseado em Java, sua interface possui a mesma aparência nos vários tipos de ambientes operacionais.

Em plataformas Windows, a interface gráfica com o usuário padrão do cliente Host On Demand é baseada no Nimbus Look and Feel fornecido pelo Java 1.6 e mais recente. O Nimbus Look and Feel pode ser desativado usando o parâmetro HTML `setHODNimbusGUI` ou a variável de ambiente `SETHODNIMBUSGUI`.

Nota: Os portlets do Host On Demand herdam a aparência de seu servidor de portal.

Suporte para Diferentes Plataformas e Ambientes de Rede

Os servidores e clientes Host On-Demand são suportados em várias plataformas e podem ser utilizados através de qualquer rede TCP/IP. Isso fornece a você muita flexibilidade na configuração do sistema e permite que o Host On-Demand seja implementado no ambiente de computação sem ter que adquirir o novo hardware.

Suporte para Java

O Host On Demand é compatível com navegadores que suportam padrões Java. Além disso, alguns novos recursos do Host On Demand aproveitam os recursos oferecidos somente pelo Java.

Suporte para Internet Protocol Versão 6

O suporte para protocolo da Internet Versão 6 requer o Java 1.4 ou superior. No entanto, o Host On Demand Versão 12 suporta o Java 1.6 ou superior.

Um protocolo da Internet é um protocolo usado para rotear dados de sua origem para seu destino através de um ambiente de Internet. Um IP é um intermediário entre camadas mais altas de protocolo e a rede física.

O Protocolo da Internet Versão 6 é a substituição do Protocolo da Internet Versão 4. O Protocolo da Internet Versão 6 expande o número de endereços IP disponíveis e faz melhorias no roteamento e na configuração de rede. O Protocolo da Internet Versão 6 e o Protocolo da Internet Versão 4 foram projetados pelo Internet Engineering Task Force (IETF).

A maioria dos usuários da Internet usa atualmente o Protocolo da Internet Versão 4. Espera-se que o Protocolo da Internet Versão 6 substitua o Protocolo da Internet Versão 4 em alguns anos.



O servidor Host On-Demand também suporta o Protocolo da Internet Versão 6 para o Redirecionador. Para obter informações adicionais, consulte o “Suporte do redirecionador para IPv6” na página 31.

Suporte para Vários Idiomas Nacionais

O Host On Demand está disponível em vários idiomas, incluindo idiomas de conjunto de caracteres de byte duplo (DBCS). Também é fornecido suporte ao símbolo monetário europeu, bem como suporte ao teclado e à página de códigos para outros idiomas como árabe, hebraico e tai. Todas as versões de idiomas estão disponíveis no mesmo meio e as versões de idioma múltiplo podem ser acessadas simultaneamente.

Conexões Seguras

Usando o Transport Layer Security (TLS) versão 1.0, o Host On Demand estende o acesso seguro a dados do host para intranets, extranets e a Internet. Trabalhadores móveis acessam um Web site seguro, recebem autenticação e estabelecem

comunicação com um host corporativo seguro. Com o suporte do certificado do cliente e do servidor, o Host On Demand pode apresentar um certificado digital (X.509, Versão 3) para o servidor Telnet - como o IBM Communications Server for z/OS - para autenticação.

O Host On-Demand também pode ser configurado para ser utilizado em ambientes que incluem firewalls. As portas de firewall precisam ser abertas para as funções definidas em suas definições de sessão do Host On-Demand. Para obter informações adicionais, consulte o "Utilizando o Host On-Demand com um Firewall" na página 32.

Arquivos HTML Personalizados

O Host On Demand inclui um Assistente de Implementação que é possível usar para criar arquivos HTML customizados. Com esses arquivos, é possível customizar o conteúdo do cliente e a função necessária para atender às necessidades de grupos específicos de usuários. Para obter informações adicionais sobre o Deployment Wizard, consulte o Capítulo 8, "Configurando os clientes de emulador do Host On Demand", na página 67.

Toolkit para Criar Novos Aplicativos e-business

O Host On-Demand inclui o Host Access Toolkit, baseado no componente Java, para criar aplicativos e-business personalizados. Esse Toolkit contém um excelente conjunto de bibliotecas Java e interfaces de programação de aplicativos, incluindo o Host Access Class Library (HACL), Host Access Beans for Java e conectores Java Enterprise Edition (J2EE).

O HACL fornece uma API não-visual para interagir com máquinas host de backend que estão executando aplicativos originalmente projetados para interação humana. Os aplicativos host contam com a apresentação de caracteres legíveis, campos formatados, codificação de cores e respostas do teclado. O HACL fornece classes especializadas para as funcionalidades necessárias para imitar a interação tradicional com uma série de apresentações de tela do host (telas verdes). O HACL não contém classes de GUI (componente visível). Por exemplo, um programa Java pode estar em execução em um mainframe como um aplicativo secundário. O programa aplicativo secundário interage primeiro com outro mainframe em execução em um aplicativo de dados CICS e, em seguida, com um navegador do cliente através de páginas HTML geradas dinamicamente. O aplicativo secundário interpreta entradas do cliente em ações do terminal simuladas que são enviadas para a máquina CICS utilizando a HACL API. As telas de resposta da máquina CICS são capturadas utilizando as HACL APIs, convertidas em páginas HTML dinâmicas e enviadas novamente para o cliente.

O Host On-Demand J2EE Connector fornece um conjunto de adaptadores de Recursos que se comunicam com os hosts 3270, 5250, CICS e VT. Esses adaptadores de recursos são implementados em um servidor de aplicativos compatível, como o IBM Application Server. Os usuários podem escrever aplicativos da Web utilizando as APIs fornecidas no Host On-Demand J2EE Connector por meio do WebSphere Studio Application Developer Integration Edition.

Programmable Host On-Demand

O Programmable Host On-Demand é um conjunto de Java APIs que permite aos desenvolvedores integrarem várias partes do código do cliente Host On-Demand, como terminais, menus e barras de ferramentas, em seus próprios aplicativos e applets Java personalizados. A API fornece ao desenvolvedor controle completo

sobre o desktop Host On-Demand (o que o usuário vê) sem começar com o Host Access Java Beans encontrado no Toolkit. O código subjacente do Host On-Demand trata de toda a "fiação" dos vários componentes, incluindo salvamento de preferências do usuário, como macros, remapeamentos de teclados e remapeamentos de cores, para o sistema de arquivos locais para uso futuro. O desenvolvedor deve determinar apenas o layout do desktop do Host On-Demand. Para obter informações adicionais, consulte a Programmable Host On-Demand Reference .

APIs do gerenciador de sessões do Host On Demand

Além das APIs (Application Programming Interfaces) fornecidas com o Host Access Toolkit, o Host On-Demand fornece APIs públicas especializadas que oferecem suporte para sessões do host incorporadas em páginas da Web utilizando o JavaScript. Essas APIs baseadas em JavaScript ajudam os desenvolvedores de aplicativos gerenciar sessões de host e interações baseadas em texto com sessões de host e estão disponíveis através do Gerenciador de Sessão do Host On-Demand. Consulte a Referência da API do Gerenciador de Sessão para obter informações adicionais.

Suporte para o WebSphere Portal

O Host On-Demand pode ser executado como um portlet no Portal Server, um componente do WebSphere Portal. O Portal Server possui gerenciamento sofisticado de desktop e recursos de segurança que oferecem aos administradores mais controle sobre direitos de acesso dos usuários e controle de usuários por meio da aparência e da organização do portal desktop.

Os administradores podem criar portlets personalizados do Host On-Demand, de modo rápido e fácil, utilizando o Deployment Wizard e, em seguida, carregá-los diretamente no Portal Server.

Nota: O Portal Server é um produto separado e requer instalação independente.

Conexões com bancos de dados DB2 em servidores IBM System i

O Database On-Demand é incluído com o Host On-Demand para fornecer acesso a informações sobre o DB2 armazenadas em servidores IBM System i5 que utilizam um driver JDBC (Java Database Connectivity). O Database On-Demand é um applet Java que permite desempenhar os pedidos de SQL (Structured Query Language) para os bancos de dados do IBM System i5 através de um driver JDBC. O Database On-Demand é um applet separado do applet do Host On-Demand e é iniciado por um arquivo HTML separado. Também é possível utilizar o suporte à transferência de dados de dentro de uma sessão de emulador para executar pedidos SQL se você precisar de emulação de terminal e de suporte para consultas SQL.

O que Há de Novo?

Obtendo as Informações Mais Recentes sobre o Host On-Demand

Para obter as informações mais recentes sobre o Host On Demand Versão 12, veja o arquivo leia-me do produto.

Para obter informações atualizadas do produto, acesse o website do Host On Demand.

Para obter as últimas dicas e sugestões técnicas para o Host On-Demand, vá para o site do Host On-Demand Hints and Tips.

Para obter informações gerais de suporte de software, acesse Software Support Handbook.

Novas funções no Host On Demand Versão 12

As funções e os aprimoramentos a seguir foram incluídos no Host On Demand Versão 12:

- O administrador HOD pode escolher Java Secure Socket Extension (JSSE) para conexões seguras usando o Redirecionador.
- O Uso de chave e o Uso de chave estendida permitem que o cliente HOD envie o Certificado pessoal baseado em Uso de chave.
- O tema padrão do HOD V12.0 para clientes Windows é baseado na aparência do Nimbus do Java.
- Os usuários HOD podem selecionar o texto na tela terminal de forma desigual semelhante ao aplicativo de edição de texto, como Notepad no Windows.
- Os usuários podem fechar as sessões HOD integradas ao uso do botão fechar na guia da sessão.
- O HOD V12.0 inclui o recurso de digitação antecipada principal que permite que os usuários continuem digitando quando a entrada estiver inibida.
- O HOD V12.0 inclui uma interface gráfica para a ferramenta de linha de comandos existente DirUtil para Windows e Linux.
- Copiar como imagem permite que o usuário final copie a tela verde (espaço de apresentação) ou parte da tela verde (espaço de apresentação) como Imagem.
- O recurso Print Graphics baseado em Print Graphics do PCOMM. Ele imprime a área marcada da tela como imagem.
- O administrador HOD pode localizar a versão do servidor HOD executando um script ou arquivo de lote disponível para todos os sistemas operacionais suportados.
- Suporte do HOD V12.0 para navegadores sem plug-in Java.
- O HOD V12.0 usa o IBM Installation Manager em todas as plataformas suportadas.
- O HOD V12.0 inclui um pacote de cliente independente que funciona sem nenhuma dependência do servidor HOD.
- O HOD v12.0 pode ser instalado como um aplicativo de 64 bits em um sistema operacional de 64 bits. O HOD Service Manager é executado como um processo de 64 bits.
- O HOD V12.0 suporta o Windows 10.

Capítulo 2. Planejamento para Implementação

O Host On-Demand oferece acesso a aplicativos do host a partir de um navegador da Web. O navegador faz o download do applet Java Host On-Demand a partir do servidor Web e, em seguida, conecta-se a qualquer servidor Telnet para acessar aplicativos do host. O applet do Host On-Demand precisa de informações de configuração para determinar o host para se conectar e outras propriedades da sessão do host. Essas informações de configuração podem ser fornecidas para o applet do Host On-Demand a partir de um arquivo HTML que é utilizado para ativar o Host On-Demand ou pelo servidor de configuração do Host On-Demand. O servidor de configuração faz parte do Host On-Demand que armazena centralmente informações de configuração de sessão e preferências do usuário por IDs de usuário e grupo. Os usuários acessam então as informações da sessão e as preferências do usuário entrando em contato com o servidor de configuração. O servidor de configuração é gerenciado através do cliente de administração. Para obter informações sobre como configurar o servidor de configuração do Host On-Demand, consulte a ajuda on-line.

Você pode criar arquivos HTML do cliente personalizados utilizando o Deployment Wizard. Ao criar esses arquivos HTML, você pode escolher entre três modelos diferentes de configuração para especificar como as informações de configuração da sessão e as preferências do usuário são definidas e gerenciadas: o modelo com base em HTML, o modelo com base no servidor de configuração e o modelo combinado.

Esses modelos são descritos abaixo. Para obter informações detalhadas sobre cada modelo e os benefícios e limitações para utilizar cada um deles, consulte a ajuda on-line.

Compreendendo o Modelo Baseado em HTML

Se você escolher o modelo baseado em HTML, todas as informações de configuração da sessão estarão contidas no próprio arquivo HTML e nada mais será necessário para definir sessões do host. Portanto, não é necessário utilizar o servidor de configuração para especificar sessões, o que significa que você não tem que abrir uma porta em seu firewall. Se você permitir que usuários salvem alterações das informações de configuração da sessão do host, suas alterações serão armazenadas no sistema de arquivos local onde o navegador está sendo executado.

Não é recomendado usar a porta 8999 porque você não precisa iniciar o servidor HOD usando o modelo baseado em HTML. Neste caso, o recurso do servidor é salvo.

Esta opção para definir informações de configuração nos arquivos HTML está disponível apenas nos clientes que são criados utilizando o Deployment Wizard.

Modelo baseado em HTML

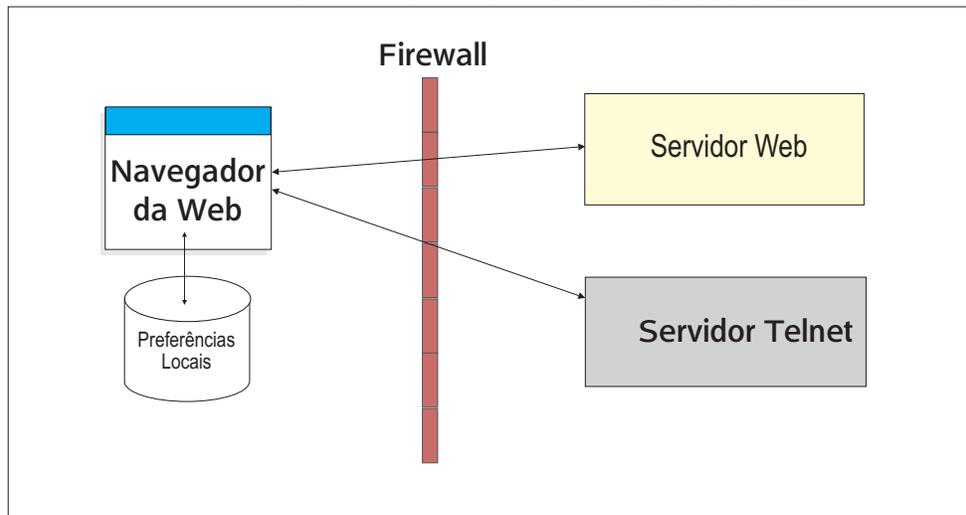


Figura 2. Modelo Baseado em HTML

Compreendendo o Modelo Baseado em Servidor de Configuração

No modelo baseado no servidor de configuração, as informações de sessão do host são mantidas no servidor de configuração através do cliente de Administração e as informações são definidas utilizando uma estrutura de usuários e grupos. Por padrão, o servidor de configuração armazena seus dados diretamente na máquina do servidor Host On-Demand, embora possa ser configurado para utilizar o LDAP. Os usuários acessam suas configurações utilizando arquivos HTML personalizados criados no Deployment Wizard ou utilizando um dentre diversos arquivos HTML que são fornecidos como parte do Host On-Demand. Os IDs de usuários são definidos no servidor de configuração e, na maioria dos casos, o usuário precisa efetuar login no servidor Host On-Demand antes da exibição das sessões. Se os administradores permitirem que os usuários salvem alterações, as preferências de usuários serão armazenadas no servidor de configuração por ID do usuário. Como as personalizações são salvas no servidor de configuração, este modelo pode ser a melhor escolha se os usuários precisarem acessar suas sessões a partir de várias máquinas.

Por padrão, o navegador da Web comunica-se diretamente com o servidor de configuração. Se você se comunicar através de um firewall, será preciso abrir a porta do servidor de configuração no firewall. Alternativamente, você pode utilizar o servlet de configuração para eliminar a necessidade de abrir a porta do servidor de configuração no firewall. O navegador da Web conecta-se com o servlet de configuração por meio de uma conexão HTTP ou HTTPS e o servlet de configuração interage com o servidor de configuração. Consulte Configurando o Servlet de Configuração para obter informações adicionais sobre como utilizar o servlet de configuração.

Modelo Baseado no Servidor de Configuração e Modelo Combinado

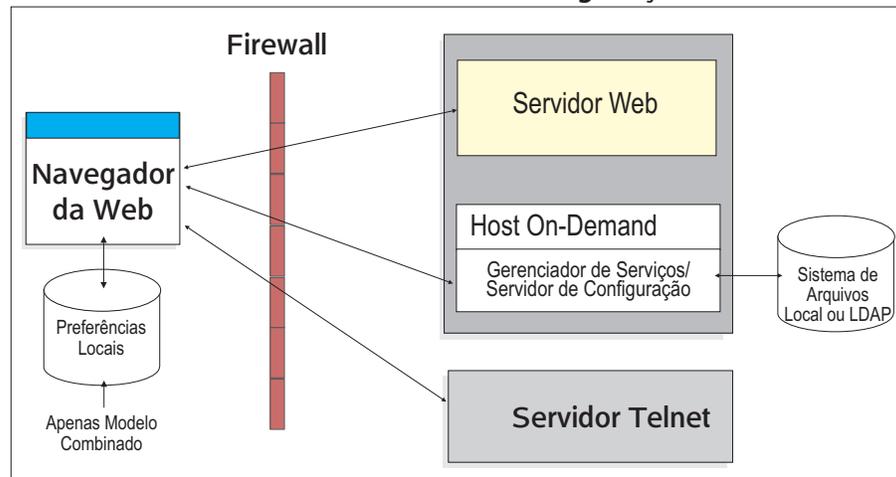


Figura 3. Modelo Baseado no Servidor de Configuração e Modelo Combinado

Modelo Baseado no Servidor de Configuração e Modelo Combinado Utilizando o Servlet de Configuração

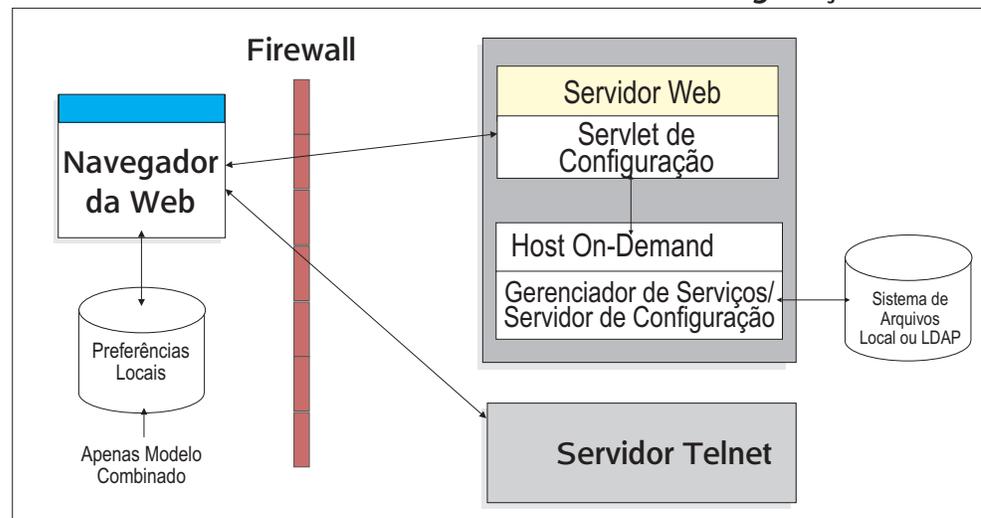


Figura 4. Modelo Baseado no Servidor de Configuração e Modelo Combinado Utilizando o Servlet de Configuração

Compreendendo o Modelo Combinado

O Host On-Demand suporta um modelo combinado, em que as informações de sessão do host são definidas no servidor de configuração (como o modelo baseado no servidor de configuração) e as atualizações do usuário são salvas na máquina do usuário (como o modelo baseado em HTML). Além disso, como o modelo baseado em HTML, os usuários do modelo combinado não precisam efetuar login no servidor Host On-Demand para exibir suas sessões.

Considerações sobre a Implementação do Cliente

Adicionalmente, para considerações de implementação do cliente, você precisa decidir pela utilização de clientes armazenados em cache, com download feito ou Web Start (consulte o Capítulo 10, “Utilizando os Clientes de Emulador do Host On-Demand”, na página 75) e qual versão do Java utilizar (consulte o Capítulo 3, “Planejando o Java no cliente”, na página 15).

Capítulo 3. Planejando o Java no cliente

Esse capítulo fornece informações detalhadas relacionadas à execução do cliente Host On Demand em um navegador ativado para Java.

- “Melhorias no cliente em cache para Java” descreve as funções do cliente em cache do Java do Host On Demand.
- “Recursos aprimorados fornecidos pelo Java” na página 16 descreve os recursos avançados do cliente Host On Demand que estão disponíveis somente com um navegador ativado para Java.
- “Mac OS X com Java” na página 17 discute os problemas envolvidos no uso do Apple Mac OS X como um cliente Host On Demand com Java.
- “Navegadores e plug-ins Java” na página 18 discute os problemas envolvidos no uso de navegadores ativados para Java e plug-ins Java.

Melhorias no cliente em cache para Java

As melhorias a seguir conduzem o cliente em cache do Java para o mesmo nível de usabilidade e flexibilidade que o cliente em cache do Java 1. Com o cliente em cache do Java, é possível fazer o seguinte:

- Instalar o cliente em cache do Java a partir uma unidade de LAN ou unidade de DVD. Para obter informações adicionais, consulte o “Instalando o Cliente em Cache a partir de uma LAN ou DVD” na página 79.
- Compartilhar o cliente em cache do Java entre mais de um usuário no Windows. Para obter informações adicionais, consulte o “Suporte a clientes em cache para Windows” na página 83.
- Remover o cliente em cache do Java em uma operação, sem limpar o cache do plug-in Java. Para obter informações adicionais, consulte o “Removendo o Cliente Armazenado em Cache” na página 81.
- Fazer upgrade do cliente em cache do Java no segundo plano.

Nota: As restrições a seguir se aplicam:

- Os usuários que fazem upgrade do cliente em cache do Host On Demand v7 para o Host On Demand v11 não podem escolher fazer upgrade dele no segundo plano.
- Não é possível fazer upgrade de alguns tipos de clientes em cache do Java no segundo plano. Consulte “Limites de suporte” para obter mais informações.

Quase todos os clientes em cache do Java do Host On Demand suportam essas melhorias. O cliente Java Web Start também suporta essas melhorias.

Limites de suporte

Os tipos a seguir de clientes em cache do Java não suportam as melhorias para o cliente em cache do Java:

- Cliente Web Start
- Janela Processar Coleta para Coleta de Tela de Impressão
- Suporte para Shell Seguro (SSH) para sessões de terminal VT e sessões seguras de File Transfer Protocol (SFTP)
- IME Automático/Conversão no Ponto

- Aperfeiçoamentos da Tela de Impressão
- Internet Protocol Versão 6 (IPv6)
- Recursos de acessibilidade
- Suporte de chave duplicada
- Keypad Pop-up Customizável
- Suporte ao Botão de Rolagem do Mouse
- Para linguagens bidirecionais, agora o suporte é fornecido para Identificadores de Conjuntos de Caracteres Codificados (CCSIDs) do OS/400 para exibir caracteres Unicode.

Recursos aprimorados fornecidos pelo Java

Usando um navegador ativado para Java com um plug-in Java, é possível aproveitar os recursos avançados a seguir oferecidos pelo cliente Host On Demand. Para obter mais informações sobre navegadores ativados para Java, consulte “Navegadores e plug-ins Java” na página 18.

- Cliente Web Start
- Janela Processar Coleta para Coleta de Tela de Impressão
- Suporte para SSH (Secure Shell) para sessões de Terminal VT e sessões seguras do SFTP (Secure File Transfer Protocol)
- IME Automático/Conversão no Ponto
- Aperfeiçoamentos da Tela de Impressão
- Internet Protocol Versão 6 (IPv6)
- Recursos de acessibilidade
- Suporte de chave duplicada
- Keypad Pop-up Customizável
- Suporte ao Botão de Rolagem do Mouse
- Para linguagens bidirecionais, o suporte é fornecido para Identificadores de Conjuntos de Caracteres Codificados (CCSIDs) do OS/400 para exibir caracteres Unicode.

Fazendo download de um cliente com o Java

As seções a seguir discutem as limitações no download de um cliente com o Java.

Impossível Fazer Download de um Componente na Lista de Pré-carregamento

Com o cliente de download de Java, um usuário não pode fazer download de um componente do cliente Host On Demand que não se encontra na lista de pré-carregamentos original. Consequentemente, é necessário especificar todos os componentes que os usuários podem requerer na lista de pré-carregamentos.

Essa limitação é causada por um conflito entre o método usado por um cliente de download para fazer download de componentes não na lista de pré-carregamentos e restrições de segurança impostas pelo plug-in Java.

Arquivos HTML Não Contêm Alguns Componentes

Com o Java, os arquivos HTML do cliente de download padrão (HOD_XX.html, em que XX é o sufixo do idioma de duas letras) não contêm os componentes do cliente a seguir:

- Transferência de dados
- Transferência de arquivos 5250

- Suporte para Impressão do Host 5250
- Importação/exportação
- SLP
- Sessões tailandesas
- Conversor de Página de Códigos do FTP
- Sessões bidirecionais
- Sessões 5250 Hindi
- Sessões DBCS utilizando definições de caracteres especificadas pelo usuário
- ZipPrint em sessões de DBCS

A IBM removeu esses componentes usados menos frequentemente da lista de pré-carregamentos dos arquivos HTML de download padrão do Java para um tempo de download menor. Entretanto, com o cliente de download de Java, qualquer componente que não esteja na lista de pré-carregamentos não pode ser transferido por download posteriormente.

Se você quiser que alguns ou todos esses componentes estejam na lista de pré-carregamento, execute uma das seguintes ações:

- Use o Assistente de Implementação para criar um arquivo HTML do Java para o cliente de download ou cliente em cache que contenha exatamente os componentes necessários.
- Use o arquivo HTML padrão para o cliente em cache (HODCached_xx.html, em que xx é o sufixo do idioma de duas letras) em vez do arquivo HTML padrão do cliente de download.
- Utilize a versão de depuração do cliente de download padrão (HODDebug_xx.html, em que xx é o sufixo de duas letras do idioma). A versão de depuração contém todos os componentes. Entretanto, essa versão de depuração do cliente de download padrão é maior que a versão sem depuração.

Mac OS X com Java

Os clientes de emulador e de banco de dados do Host On Demand Mac OS X suportam Safari, Firefox e a versão Mac do Internet Explorer. O Host On Demand não suporta os clientes de administração no Mac OS X. O Host On Demand Versão 12.0 suporta o Java 1.6 ou superior.

O recurso Suporte a Teclas Duplicadas requer um Java Plug-in de 1.4.2 ou mais recente em clientes Macintosh. No entanto, o Host On Demand Versão 11 suporta o Java 1.6 ou superior.

Limitações do Mac OS X

O Mac OS X não suporta as melhorias do cliente em cache do Java descritas em “Melhorias no cliente em cache para Java” na página 15. Para obter informações adicionais, consulte o “Suporte a clientes em cache para Mac OS X (somente clientes Java)” na página 84.

Tempos de inicialização um pouco mais lentos com clientes Java

Com um navegador ativado para Java, o cliente Host On Demand é iniciado um pouco mais lento (5 a 15 segundos mais lento, dependendo do tipo de estação de trabalho). O atraso é causado pelo sistema que está carregando o plug-in Java.

Além disso, com o navegador ativado para Java, uma sessão de host na área de trabalho do cliente Host On Demand pode levar um pouco mais de tempo para ser iniciada.

Limitações de plug-ins Java específicos

Se você estiver usando o plug-in Java da Oracle e os caracteres Hindi não forem exibidos corretamente, assegure-se de que seu nível de Sun JRE seja o mais recente.

Limitações com applets fornecidos pelo cliente e Java

Se um usuário executar um applet fornecido pelo cliente (ou seja, um applet escrito por sua empresa ou por terceiros) com uma sessão (como Exibição 3270) ativada a partir de um cliente Host On Demand do Java e esse applet requerer quaisquer permissões do Java, recomenda-se tomar uma das ações a seguir para atender os requisitos de segurança do Java:

- O applet deve ser arquivado em um arquivo .JAR do Java assinado.
- As permissões devem ter sido concedidas anteriormente na estação de trabalho usando o Java Policy Tool fornecido com o plug-in Java.

Se você não atender os requisitos de segurança do Java, o applet falhará silenciosamente.

Limitações com usuários restritos e Java

Os usuários restritos não têm a autoridade para instalar o plug-in Java. Um usuário com autoridade administrativa deve instalar o plug-in Java.

Navegadores e plug-ins Java

Esta seção discute problemas envolvidos no uso de navegadores ativados para Java e plug-ins Java.

Navegadores ativados para Java

Um navegador ativado para Java não tem uma JVM incluída nele. Ele mesmo pode exibir arquivos HTML, mas precisa de um plug-in Java separado instalado para ativar um applet Java como o cliente Host On Demand. Exemplos de navegadores ativados para Java são Firefox e Microsoft Internet Explorer com o plug-in Java instalado.

Navegadores e Plug-ins Suportados por Clientes Host On-Demand

Os usuários com estações de trabalho do cliente executando o Windows podem fazer download do plug-in IBM Java a partir de qualquer servidor Host On Demand.

Como os fornecedores de plug-ins Java como Oracle e IBM publicam novas versões de seus plug-ins Java e como a IBM estende o Host On Demand para suportar essas novas versões, a IBM anunciará suporte das novas versões no website do Host On Demand.

Microsoft Internet Explorer com um plug-in Java

Quando um plug-in Java estiver instalado e configurado corretamente em uma estação de trabalho do cliente Windows, o Microsoft Internet Explorer funcionará como um navegador ativado para Java, dependendo de como o Host On Demand escolhe ativar o cliente.

Firefox com um plug-in Java

Para executar um applet Java no Firefox, é necessário instalar um plug-in Java.

Consequentemente, o Host On Demand espera que você configure o plug-in Java para que ele *seja* o Java Runtime padrão para Firefox. Para obter instruções sobre como verificar ou mudar essa configuração, consulte o tópico Configurando o Java Runtime padrão para um navegador ativado para Java na ajuda on-line.

Nota: Os usuários restritos, como usuários restritos que compartilham um cliente em cache no Windows ou usuários restritos em uma estação de trabalho Linux ou AIX, não podem instalar o plug-in Java.

Capítulo 4. Planejamento para Segurança

Se você está simplesmente implementando o Host On-Demand dentro de sua empresa ou se está utilizando-o para fornecer acesso aos seus sistemas host sobre a Internet, a segurança é de seu interesse. Este capítulo fornece uma visão geral da segurança do Host On-Demand.

- Transport Layer Security (TLS) . Fornece criptografia, autenticação baseada em certificado e negociações de segurança em uma conexão Telnet ou FTP estabelecida. Consulte “TLS para o Host On Demand” na página 23 para obter detalhes.
- O Redirecionador. Suporta o TLS entre os clientes Host On Demand e o servidor Host On Demand. Consulte “O Redirecionador” na página 28 para obter detalhes.
- Firewalls. Você pode configurar o Host On-Demand para atravessar um firewall. Consulte “Utilizando o Host On-Demand com um Firewall” na página 32 para obter detalhes.
- Segurança do ID de usuário. Inclui Web Express Logon, Native Authentication e logon de Domínio do Windows. Consulte “Segurança do ID de Usuário” na página 36 para obter detalhes.
- Ambientes FIPS (Federal Information Processing Standards). Consulte “Ambientes FIPS” na página 37 se seu ambiente exigir que seus componentes de segurança utilizem componentes/módulos certificados pelo FIPS.

Transport Layer Security (TLS)

Como a segurança TLS funciona

O TLS é baseado no protocolo SSL. O TLS usa o protocolo de handshake inicial para estabelecer autenticação e criptografia entre cliente/servidor. Para obter informações detalhadas sobre TLS, veja a descrição de *O protocolo TLS versão 1.0*.

O protocolo TLS utiliza a tecnologia criptográfica de chave pública e chave simétrica. A criptografia de chave pública utiliza um par de chaves: uma chave pública e uma chave privativa. As informações criptografadas com uma chave podem ser decriptografadas somente com a outra chave. Por exemplo, as informações criptografadas com a chave pública podem ser decriptografadas somente com a chave privativa. Cada chave pública do servidor é publicada e a chave privativa é mantida em segredo. Para enviar uma mensagem segura ao servidor, o cliente criptografa a mensagem utilizando a chave pública do servidor. Quando o servidor recebe a mensagem, ele decriptografia a mensagem com sua chave privativa.

A criptografia de chave simétrica utiliza a mesma chave para criptografar e decriptografar mensagens. O cliente gera aleatoriamente uma chave simétrica que é utilizada para criptografar todos os dados da sessão. A chave é, então, criptografada com a chave pública do servidor e enviada ao servidor.

O TLS fornece três serviços de segurança básicos:

Exclusividade da mensagem

É atingida através de uma combinação da criptografia de chave pública e chave simétrica. Todo o tráfego entre um cliente e um servidor é

criptografado utilizando uma chamada e um algoritmo de criptografia negociado durante a configuração da sessão.

Integridade da mensagem

Assegura que o tráfego da sessão não altere a rota até o seu destino final. O TLS usa uma combinação de chaves pública/privada e funções hash para assegurar a integridade da mensagem.

Autenticação Mútua

Troca de identificação através de certificados de chave pública. As identidades do cliente e do servidor são codificadas em certificados de chave pública, os quais contêm os seguintes componentes:

- Nome distinto da pessoa
- Nome distinto do emissor
- Chave pública da pessoa
- Assinatura do emissor
- Período de validade
- Número de série

Tabela 2. Dica



Você também pode utilizar o HTTP (HTTPS) para garantir que as informações de segurança de um cliente não serão comprometidas na medida que é feito um download de um servidor.

Certificados

A segurança é controlada por certificados digitais que agem como cartões de ID eletrônicos. O objetivo de um certificado é garantir que um programa ou um usuário é seguro para permitir a conexão proposta e, se a criptografia está envolvida, para fornecer as teclas de criptografia/decriptografia necessárias. Eles são geralmente emitidos por CAs (Autoridades de Certificação), que são organizações confiáveis pela indústria como um todo e cujo negócio é a emissão de certificados de Internet. Um certificado da CA, que também é conhecido como um certificado raiz, inclui (entre outras coisas) a assinatura da CA e um período de validade.

A criptografia e a autenticação são executadas por meio de um par de chaves, uma pública e uma privativa. A chave pública é embutida em um certificado, conhecido como um certificado de site ou servidor. O certificado contém vários itens de informações, incluindo o nome do CA (Autoridade de Certificação) que emitiu o certificado, o nome e a chave pública do servidor ou do cliente, a assinatura do CA e a data e o número de série do certificado. A chave privativa é criada quando você cria um pedido de certificado de auto-assinatura ou um certificado CA e é utilizado para decriptografar mensagens dos clientes.

Uma sessão TLS é estabelecida na sequência a seguir:

1. O cliente e o servidor trocam mensagens de saudação para negociar o algoritmo de criptografia e a função hash (para integridade da mensagem) a serem utilizados para a sessão.
2. O cliente solicita um certificado X.509 do servidor para provar sua identidade. Opcionalmente, o servidor pode solicitar um certificado do cliente. Os certificados são conferidos verificando-se o formato do certificado e as datas de validade e verificando se o certificado inclui a assinatura de uma autoridade de certificado confiável (ou é auto-assinada).

3. O cliente gera aleatoriamente um conjunto de teclas que é utilizado para a criptografia. As teclas são criptografadas com a tecla pública do servidor e seguramente comunicadas para o servidor.

TLS para o Host On Demand

Há três áreas nas quais você pode configurar a segurança para o Host On-Demand: segurança da sessão, segurança do servidor Web e segurança da configuração.

Segurança da sessão

O Host On Demand Versão 12.0 usa o protocolo TLS para fornecer segurança para sessões de emulador e FTP.

O protocolo TLS fornece privacidade nas comunicações através de uma rede TCP/IP. O TLS foi projetado para evitar a espionagem, violação de mensagens ou falsificação de mensagens. Ele também oferece uma estrutura que permite que novos algoritmos criptografados sejam facilmente incorporados. O Host On Demand suporta a criptografia de sessões de emulação e FTP e autenticação de servidor/cliente de acordo com o *Protocolo TLS Versão 1.0*.

O suporte é fornecido para o seguinte:

- Criptografia de dados RSA tipo 4 em conexões entre os clientes Host On Demand e os servidores Telnet ou FTP que suportam o TLS versão 1.0, 1.1, 1.2.
- Certificados X.509.
- Algoritmos de criptografia em massa usando chaves de até 168 bits de comprimento.
- Algoritmos de autenticação usando chaves de até 2048 bits de comprimento.
- Autenticação de servidor e cliente.
- Suporte para armazenamento e uso de certificados de cliente no sistema do cliente.
- Prompt opcional do usuário para certificado do cliente quando solicitado pelo servidor.
- Indicadores de sessão segura. Um ícone de bloqueio é exibido na barra de status da sessão para indicar ao usuário que a sessão é segura. A segurança da criptografia, por exemplo, 64, 128 ou 256, também é exibida ao lado do ícone de bloqueio e quando o mouse passa sobre o ícone de bloqueio.

Para o Host On Demand, é possível usar um certificado de CA, mas também é possível criar seu próprio certificado autoassinado, conforme descrito no tópico Usando um certificado autoassinado na ajuda on-line.

Um utilitário Certificate Management gráfico (disponível em plataformas Windows e AIX) é fornecido para:

- Criar pedidos de certificado
- Receber e armazenar certificados
- Criar certificados auto-assinados

A IKEYCMD é uma ferramenta, além do utilitário Host On-Demand Certificate Management, que pode ser utilizada para gerenciar chaves, certificados e pedidos de certificado. Possui uma funcionalidade semelhante à do Certificate Management e é executada a partir da linha de comandos sem uma interface gráfica. Para obter informações adicionais, consulte o Apêndice B, "Utilizando a Interface de Linha de Comandos IKEYCMD", na página 149.

Para suportar serviços TLS, o Host On Demand usa seis bancos de dados:

HODServerKeyDb.kdb

O HODServerKeyDb.kdb é criado a primeira vez que você configura o TLS para o Redirecionador do Host On Demand. Esse banco de dados contém a chave privada e o certificado do servidor bem como uma lista de certificados CA (ou signatário). Essas CAs são consideradas *reconhecidas* e são *confiáveis* pelo servidor Host On-Demand. Você pode incluir certificados de outros CAs (CAs desconhecidas) e certificados que você cria e assina (auto-assinado) neste banco de dados. Consulte “O Redirecionador” na página 28 para obter informações adicionais.

HODServerKeyStore.jks

O redirecionador pode ser configurado para usar Java Secure Socket Extension (JSSE) em vez de GSKit. Quando configurado com JSSE, o redirecionador lê a chave privada e os certificados de HODServerKeyStore.jks. Consulte O Redirecionador para obter mais informações.

CustomizedCAs.p12

O CustomizedCAs.p12 é um arquivo de formato PKCS#12 que contém os certificados raiz de CAs desconhecidas e certificados auto-assinados que não estão na lista WellKnownTrusted. Se você usar um certificado autoassinado ou um certificado de uma autoridade desconhecida (CA), será necessário criar ou atualizar o CustomizedCAs.p12. O Host On-Demand não instala um arquivo CustomizedCAs.p12 por padrão.

O arquivo CustomizedCAs.p12 é uma versão recente do arquivo CustomizedCAs.class, que você pode ter criado com um release anterior do Host On-Demand. O arquivo CustomizedCAs.class suporta o Host On-Demand Versão 7 e clientes anteriores, e está localizado no diretório de publicação por padrão. Se você estiver executando o Windows ou AIX, quando fizer upgrade para a versão 12, a instalação do Host On Demand detectará automaticamente o arquivo CustomizedCAs.class, criará o novo arquivo CustomizedCAs.p12 e o colocará no diretório de publicação. Ambos os arquivos permanecem no diretório de publicação e estão disponíveis para clientes de diferentes versões. Se você tiver um diretório de publicação separado e não o diretório de publicação padrão, a instalação do Host On-Demand não conseguirá detectar o arquivo CustomizedCAs.class e será preciso executar a ferramenta de migração manualmente na linha de comandos.

Se você criar o arquivo CustomizedCAs.p12 pela primeira vez que estiver utilizando o utilitário Certificate Management do Host On-Demand (IKEYMAN), também deverá ter o arquivo CustomizedCAs.class mais antigo em seu diretório de publicação, para que os clientes mais antigos ainda possam funcionar com o novo servidor. Além disso, quando você atualizar subsequentemente o arquivo CustomizedCAs.p12, terá que certificar-se de que essas alterações foram selecionadas pelo arquivo CustomizedCAs.class. Para plataformas Windows, se esses arquivos estiverem no diretório de publicação padrão, c:\Program Files\IBM\HostOnDemand\HOD, toda vez que você abrir IKEYMAN para atualizar o arquivo CustomizedCAs.p12 e, em seguida, fechar IKEYMAN, o arquivo CustomizedCAs.class é automaticamente atualizado junto com o arquivo CustomizedCAs.p12. Se esses arquivos não estiverem no diretório de publicação padrão, será preciso executar manualmente a

ferramenta de migração reversa do diretório de publicação utilizando o comando a seguir. O comando aparece em três linhas, mas deve ser digitado como uma única linha.

```
..\hod_jre\jre\bin\java -cp ..\lib\sm.zip;  
com.ibm.eNetwork.HOD.convert.CVT2SSLIGHT  
CustomizedCAs.p12 hod CustomizedCAs.class
```

No AIX, para que o arquivo CustomizedCAs.class capture as mudanças feitas no arquivo CustomizedCAs.p12, é necessário executar essa ferramenta de migração reversa manualmente a partir do diretório de publicação usando o comando a seguir. O comando aparece em três linhas, mas deve ser digitado como uma única linha.

```
../hod_jre/jre/bin/java -cp ../lib/sm.zip  
com.ibm.eNetwork.HOD.convert.CVT2SSLIGHT  
CustomizedCAs.p12 hod CustomizedCAs.class
```

CustomizedCAs.class

O CustomizedCAs.class é um arquivo de classe Java que contém os certificados de CAs desconhecidas e certificados auto-assinados que não estão na lista WellKnownTrusted. Se você usar um certificado autoassinado ou um certificado de uma autoridade desconhecida (CA), será necessário atualizar o arquivo CustomizedCAs.class. Entretanto, observe que você não pode mais criar ou atualizar o arquivo CustomizedCAs.class usando o utilitário Certificate Management em plataformas Windows ou AIX. No Host On-Demand Versões 9 ou posteriores, você poderá criar apenas uma versão mais nova deste arquivo chamado CustomizedCAs.p12. Porém, todos os clientes ainda suportam o formato mais antigo. Para obter informações adicionais, consulte a descrição do CustomizedCAs.p12 acima.

WellKnownTrustedCAs.class, WellKnownTrustedCAs.p12 e WellKnownTrustedCAs.jks

O WellKnownTrustedCAs.class, WellKnownTrustedCAs.p12 e WellKnownTrustedCAs.jks são os arquivos fornecidos pelo Host On Demand que contêm os certificados públicos de todos os CAs nos quais o Host On Demand confia. Esses arquivos não devem ser modificados.

WellKnownTrustedCAs.class/WellKnownTrustedCAs.p12 e WellKnownTrustedCAs.jks, CustomizedCAs.p12 e/ou CustomizedCAs.class e CustomizedCAs.jks devem estar presentes no diretório de publicação do Host On Demand. O cliente Host On Demand usa esses arquivos para confiar no certificado do servidor durante o handshake TLS.

CustomizedCAs.jks

O arquivo CustomizedCAs.jks é diferente do arquivo CustomizedCAs.p12 que é usado para SSLite quando a configuração Usar JSSE estiver configurada como Não. É possível criar um arquivo CustomizedCAs.jks convertendo o CustomizedCAs.p12 existente para o formato JKS ou criando um novo arquivo nesse formato. É possível usar o utilitário de Gerenciamento de certificado que está instalado com o Host On Demand ou a ferramenta de linha de comandos keytool.exe, que é um Java Key and Certificate Management Tool disponível no JRE para esse propósito.

Ativação de TLS básico para clientes Host On Demand

Quando você seleciona o protocolo TLS para o cliente Host On Demand, uma sessão TLS básica é estabelecida. Durante o processo de negociação de TLS, o servidor apresenta seu certificado para o cliente. Com a ativação de TLS básico, o certificado deve ser assinado por uma autoridade na qual o cliente confia. O cliente verifica primeiro o WellKnownTrustedCAs.class/WellKnownTrustedCAs.p12 e, em

seguida, o CustomizedCAs.p12 ou o CustomizedCAs.class. Se o Host On Demand for configurado para usar o JSSE para ativação de TLS, os arquivos WellKnownTrustedCAs.jks e CustomizedCAs.jks serão usados. O cliente rejeitará a sessão se não encontrar o assinante nesses arquivos. Se o cliente encontrar o assinante nesses arquivos, a sessão será estabelecida. Esta é a Autenticação de Servidor básica. O Host On-Demand permite configurar uma forma mais avançada de Autenticação de Servidor em sua configuração de cliente. Consulte a seção seguinte para obter informações adicionais.

Autenticação do Servidor

A codificação da troca de dados entre o cliente e o servidor não garante que o cliente esteja se comunicando com o servidor correto. Para evitar este problema, você pode ativar a autenticação do servidor. Assim o cliente após ter certeza de que o certificado do servidor é confiável, verifica se o nome da Internet no certificado corresponde ao nome da Internet do servidor. Se corresponderem, a negociação de TLS continuará. Se não, a conexão termina imediatamente. Consulte autenticação do servidor na ajuda on-line para obter informações adicionais.

Autenticação do Cliente

A autenticação do cliente é semelhante à autenticação do servidor, exceto que o servidor Telnet requer um certificado do cliente para verificar se o cliente é quem ele declara ser. Nem todos os servidores suportam a autenticação do cliente, incluindo o Redirecionador do On-Demand. Para configurar a autenticação de cliente, é necessário proceder da seguinte forma:

- obter certificados para clientes
- enviar os certificados para os clientes
- configurar os clientes para utilizarem autenticação de cliente

Consulte configurando clientes para utilizar autenticação de cliente na ajuda on-line, para obter informações adicionais.

Express Logon

Há dois tipos de Express Logon:

- Web Express Logon: O Web Express Logon permite aos usuários efetuar logon em sistemas host e em aplicativos host sem precisar fornecer um ID de usuário e senha. Esse recurso funciona em conjunto com o aplicativo de segurança da rede adquirindo as credenciais de rede do usuário e mapeando-as para suas credenciais do host, sem necessidade de efetuar logon várias vezes. Dependendo do host, o processo de automatização de logon pode ser baseado na macro ou na conexão. Para obter informações adicionais, consulte a Referência de Web Express Logon.
- Certificate Express Logon: O Certificate Express Logon é baseado em macro e também permite aos usuários efetuar logon sem precisar inserir um ID de usuário e senha. Ele é funcionalmente semelhante ao Web Express Logon, embora requeira que você configure sua sessão para TLS e autenticação de cliente, e o Communications Server deve suportar e ser configurado para Express Logon. Para obter informações adicionais, consulte Express logon na ajuda on-line.

Tabela 3. Dica



A partir do Host On-Demand V9, o Web Express Logon oferece um tipo de automação de logon que utiliza certificados do lado do cliente. Esse modelo é chamado de Web Express Logon com base em certificado e é significativamente diferente do Certificate Express Logon. Com o Certificate Express Logon, os certificados de clientes são utilizados para autenticar usuários para um servidor TN3270 ativado para Express Logon que é configurado para automatizar o processo de login. Com o Web Express Logon com base em certificado, no entanto, os certificados de clientes são utilizados para autenticar usuários para um servidor da Web ou para um aplicativo de segurança da rede e o processo de login é automatizado por um plug-in e uma macro. Para obter informações adicionais, consulte a Referência de Web Express Logon.

Segurança Telnet baseada em TLS

A segurança negociada para Telnet permite que as negociações de segurança entre o cliente e o servidor Telnet sejam feitas na conexão de Telnet estabelecida. Você pode configurar a segurança negociada para Telnet para a exibição 3270 do Host On-Demand e para as sessões de impressora.

O servidor de Telnet deve suportar a segurança Telnet baseada em TLS (conforme descrito no Rascunho da Internet IETF *Segurança Telnet baseada em TLS*) para os clientes Host On Demand usarem a segurança negociada pelo Telnet. O Servidor de Comunicação para z/OS suporta a segurança Telnet baseada em TLS.

Para obter informações adicionais a respeito da segurança negociada para Telnet, consulte a Visão geral da segurança negociada para Telnet na ajuda on-line. Consulte a documentação do servidor de Telnet para obter mais informações sobre como configurar o TLS no servidor de Telnet e consulte o tópico Segurança na ajuda on-line para obter mais informações sobre como configurar um cliente para conectar-se a um servidor de Telnet seguro.

Segurança FTP baseada em TLS

O Host On Demand fornece a transferência de arquivos segura baseada em TLS para sessões FTP. A sessão FTP não suporta negociações de TLS implícitas/incondicionais para a porta 990/989. Portanto, a porta 990 não deve ser utilizada para sessões seguras de FTP. Ela suporta somente negociações TLS explícitas/condicionais (comando AUTH) para qualquer outra porta.

As propriedades de segurança da sessão FTP são independentes das propriedades de segurança da sessão de emulador. Para uma sessão FTP integrada, é necessário configurar as informações de segurança do FTP usando a nova guia Segurança nas propriedades de sessão FTP. Se você configurar uma sessão do emulador para ser segura e o Tipo de Transferência de Arquivos estiver definido para FTP, a sessão do FTP não será assegurada automaticamente. Nesta situação, a mensagem a seguir aparece ao clicar no botão OK: Se uma sessão de transferência de arquivos segura for desejada, configure as informações de segurança nos Padrões para Transferência de Arquivos.

A função FTP segura baseada em TLS é suportada pelo z/OS V1R2 ou superior.

Exemplos de quando usar a segurança de sessão

Consulte os exemplos a seguir como situações onde você pode utilizar a segurança de sessão:

- Permitindo que clientes peçam seus produtos na Internet. Nessa situação, você deseja certificar-se de que as informações que os clientes lhe fornecem, como número do cartão de crédito, sejam criptografadas para que não possam ser roubadas. Deseja certificar-se também de que a informações que você fornece aos clientes sejam protegidas.
- Concedendo aos fornecedores ou parceiros de negócios acesso a informações em seus computadores host. Você não quer que ninguém consiga acessar esses dados.
- Permitindo que sua equipe tenha acesso a informações do computador host de sites remotos ou quando estiverem viajando.
- Oferecendo aos médicos acesso a registros de pacientes de onde quer que estejam e certificando-se que pessoas não autorizadas possam acessar esses registros.

Segurança do Servidor Web

É possível configurar o servidor da web para usar TLS, para que o fluxo de dados de seu servidor da web para o navegador seja criptografado. Veja a documentação do servidor da web para obter mais informações sobre como configurar o servidor da web para TLS. Depois que o cliente for carregado em um navegador, ele se comunica diretamente com o host. É possível configurar o Host On Demand para fornecer segurança TLS para as suas sessões de host. Para obter mais informações, veja Configurando o TLS na ajuda on-line.

Segurança da Configuração

Se você utilizar o modelo HTML, suas informações de configuração de sessão serão criptografadas ao utilizar o HTTPS. Para todos os outros modelos, você precisa configurar o Host On-Demand para utilizar o servlet de configuração através do HTTPS (depois de configurar seu servidor de aplicativos da Web) para criptografar a configuração da sessão em vez de comunicar-se diretamente com o servidor de configuração. Consulte “Instalando o Servlet de Configuração” na página 60 neste guia, para obter informações sobre como instalar e configurar o servlet, e consulte configurando o servlet de configuração na ajuda on-line para obter informações sobre como configurar clientes para utilizarem o servlet de configuração.

O Redirecionador

O Redirecionador é um serviço que é executado no servidor do Host On-Demand e que permite que um cliente do Host On-Demand se comunique com um servidor de Telnet conectando-se com uma porta do Redirecionador no servidor do Host On-Demand.

Normalmente, o cliente do Host On-Demand:

- Conecta-se diretamente com o servidor do Host On-Demand para fazer download do código do cliente e para acessar arquivos HTML públicos.
- Também conecta-se diretamente com um servidor de Telnet que é executado ou está conectado com um host 3270, 5250, VT ou CICS.

No entanto, quando o Redirecionador é utilizado, o Redirecionador atua como um intermediário entre o cliente e o servidor de Telnet. O cliente, em vez de conectar-se diretamente com o servidor de Telnet, conecta-se com uma porta do Redirecionador no servidor do Host On-Demand. Em seguida, o Redirecionador envia ao servidor de Telnet os dados recebidos do cliente. Quando o servidor de

Telnet responde, o Redirecionador envia ao cliente os dados recebidos do servidor de Telnet. Esse processo continua até que a sessão seja finalizada.

Por que Utilizar o Redirecionador?

Se o servidor de Telnet não suportar TLS e você estiver executando o servidor Host On Demand em um dos sistemas operacionais nos quais o Redirecionador suporta sessões seguras (veja “Sistemas operacionais suportados pelo Redirecionador” na página 30), será possível configurar o Redirecionador do Host On Demand para fornecer suporte de TLS.

Tabela 4. Dica



Muitos servidores Telnet suportam TLS (por exemplo, IBM Communications Servers on zSeries, IBM System i, AIX ou NT). Se o seu servidor de Telnet suporta TLS, é altamente recomendável usar o servidor de Telnet. Se o seu servidor de Telnet não suporta TLS, o Redirecionador do Communications Server for AIX oferece uma alternativa mais escalável para o Redirecionador do Host On Demand.

O Redirecionador age como um proxy Telnet transparente que utiliza o remapeamento de porta para conectar o servidor Host On-Demand a outros servidores Telnet. Cada servidor definido pode configurar um conjunto de números de portas locais. Em vez de se conectar diretamente no servidor Telnet de destino, um cliente se conecta ao servidor Host On-Demand e no número da porta. O Redirecionador mapeia o número da porta local para o número da porta-host do destino e faz a conexão.

Tabela 5. Recomendação



A solução recomendada para um proxy Telnet é utilizar o Load Balancer, um recurso dos WebSphere Application Server's Edge Components, ou um produto semelhante que forneça conversão de endereço como parte da solução global de firewall, em vez do Redirecionador do Host On-Demand.

Como o Redirecionador Funciona

Figura 5 ilustra como o Redirecionador envia dados do cliente ao servidor de Telnet e envia ao cliente os dados de resposta do servidor de Telnet.

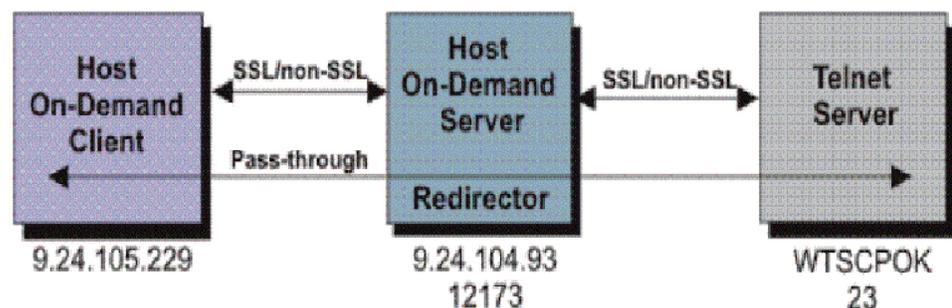


Figura 5. Como o Redirecionador Funciona

O Redirecionador pode ser configurado em qualquer um dos seguintes quatro modos:

- Passagem

- O Redirecionador comunica-se com o servidor de Telnet e com o cliente sem alterar o conteúdo dos dados.
- Lado do cliente
 - O cliente e o Redirecionador se comunicam em uma sessão segura usando TLS (o conteúdo é criptografado/decriptografado).
 - O Redirecionador e o servidor de Telnet se comunicam em uma sessão não segura.
- Lado do host
 - O cliente e o Redirecionador se comunicam em uma sessão não segura.
 - O Redirecionador e o servidor de Telnet se comunicam em uma sessão segura usando TLS (o conteúdo é criptografado/decriptografado)
- Ambos
 - O cliente e o Redirecionador se comunicam em uma sessão segura usando TLS (o conteúdo é criptografado/decriptografado).
 - O Redirecionador e o servidor de Telnet se comunicam em uma sessão segura usando TLS (o conteúdo é criptografado/decriptografado).

Antes de usar os modos Lado do cliente, Lado do servidor ou Ambos, é necessário criar o HODServerKeyDb.kdb ou HODServerKeyStore.jks (se configurado para usar JSSE) para o Redirecionador.

Você pode utilizar o modo Passagem quando não é necessária criptografia pelo Redirecionador, porque o fluxo de dados não precisa ser criptografado ou porque o fluxo de dados já é criptografado entre o cliente e o servidor de Telnet. É necessário usar o modo de Passagem se o cliente Host On Demand estiver conectando-se por meio do Redirecionador a um host que requer autenticação de cliente ou o Express Logon.

Consulte Adicionando um Host ao Redirecionador na ajuda on-line para obter informações adicionais.

Capacidade de Carga do Redirecionador

Para obter as recomendações de capacidade de carga do Redirecionador, consulte o LEIA-ME.

Sistemas operacionais suportados pelo Redirecionador

O Redirecionador agora suporta:

- Todos os sistemas operacionais suportados pelo servidor do Host On-Demand e que também suportam o IPv4 (Internet Protocol Versão 4).
- Alguns sistemas operacionais suportados pelo servidor do Host On-Demand e que também suportam o IPv6 (Internet Protocol Versão 6).

Nem todos os modos do Redirecionador são suportados em todos os sistemas operacionais. As próximas duas subseções descrevem o suporte ao Redirecionador em mais detalhes. Para obter informações adicionais sobre o IPv4 e o IPv6, consulte “Suporte para Internet Protocol Versão 6” na página 6.

Sistemas operacionais que suportam IPv4

Para sistemas operacionais que suportam o IPv4 o Redirecionador suporta o seguinte:

- Modo Passagem em todos os sistemas operacionais suportados pelo servidor do Host On-Demand.

- Outros modos (lado do cliente, lado do host e ambos) em apenas alguns dos sistemas operacionais suportados pelo servidor Host On-Demand

Tabela 6 e Tabela 7 mostram estas informações:

Tabela 6. Modos de sistemas operacionais de 32 bits e de Redirecionador para os quais o Redirecionador suporta IPv4 usando GSKit

Sistema operacional:	Passagem:	Lado do Cliente:	Lado do Host:	Ambos:
Windows	Sim	Sim	Sim	Sim
AIX	Sim	Sim	Sim	Sim
Linux	Sim	Sim	Sim	Sim
Todos os outros sistemas operacionais	Sim	Não	Não	Não

Tabela 7. Modos de sistemas operacionais de 64 bits e de Redirecionador para os quais o Redirecionador suporta IPv4 usando JSEE

Sistema operacional	Passagem:	Lado do Cliente:	Lado do Host:	Ambos:
Windows	Sim	Sim	Sim	Sim
AIX	Sim	Sim	Sim	Sim
Linux	Sim	Sim	Sim	Sim
Todos os outros sistemas operacionais	Sim	Não	Não	Não

Suporte do redirecionador para IPv6

Tabela 8 e Tabela 9 mostram os modos de sistemas operacionais e de Redirecionador para os quais o Redirecionador suporta o Internet Protocol Version 6 (IPv6):

Tabela 8. Modos de sistemas operacionais de 32 bits e de Redirecionador para os quais o Redirecionador suporta IPv6 usando GSKit

Sistema Operacional	Passagem:	Lado do Cliente:	Lado do Host:	Ambos:
Windows	Sim	Sim	Sim	Sim
Linux	Sim	Sim	Sim	Sim
AIX	Sim	Sim	Sim	Sim

Tabela 9. Modos de sistemas operacionais de 64 bits e de Redirecionador para os quais o Redirecionador suporta IPv6 usando JSEE

Sistema operacional:	Passagem:	Lado do Cliente:	Lado do Host:	Ambos:
Windows	Sim	Sim	Sim	Sim
Linux	Sim	Sim	Sim	Sim
AIX	Sim	Sim	Sim	Sim

Utilizando o Host On-Demand com um Firewall

Se você estiver configurando o Host On-Demand para passar por um firewall, recomendamos que o administrador do firewall abra apenas aquelas portas requeridas para funcionamento dos clientes. As portas Telnet permite o tráfego de sessão criptografado por TLS.

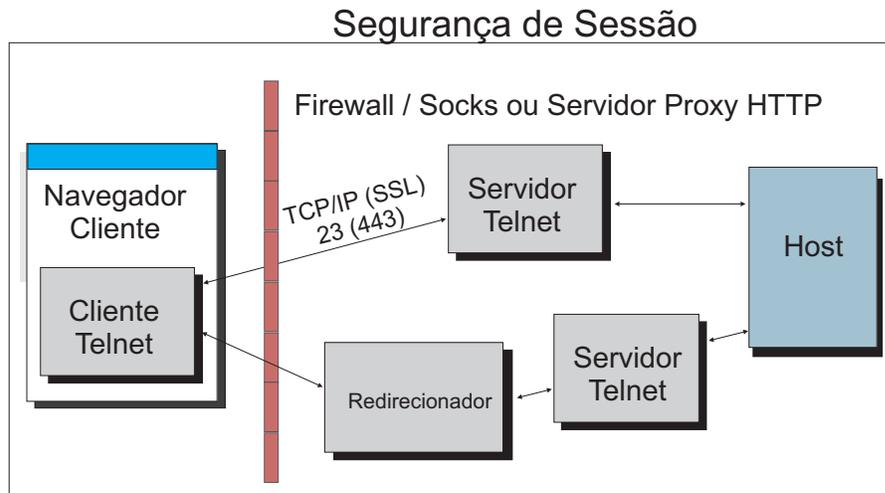


Figura 6. Segurança de Sessão Através de um Firewall ou Servidor Proxy

Se você estiver utilizando modelos com base no servidor de configuração ou combinados, o servlet de configuração do Host On-Demand permitirá que os clientes do Host On-Demand se comuniquem com o servidor de configuração por meio de HTTP ou de HTTPS.

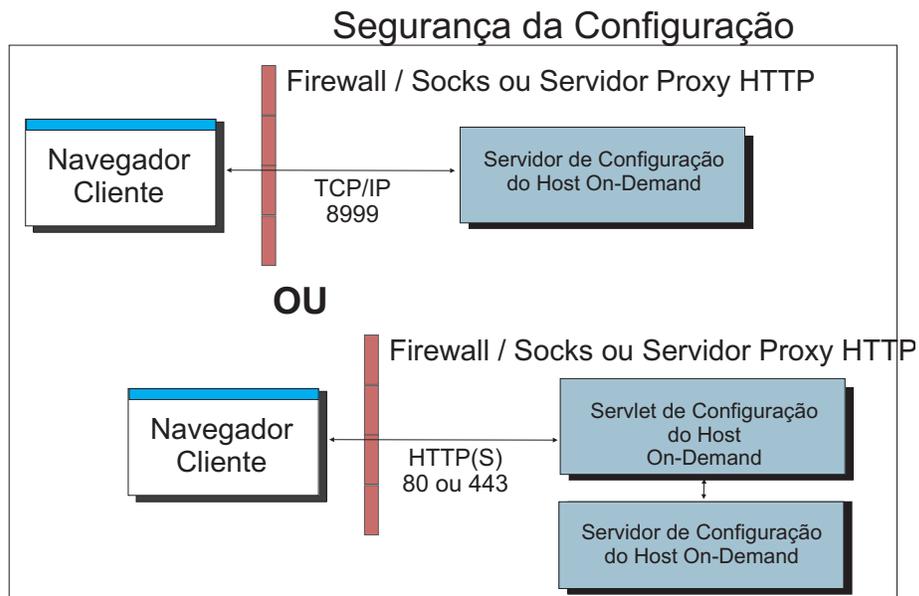


Figura 7. Segurança da Configuração, com e sem o Servlet de Configuração, Através de um Firewall ou Servidor Proxy

Para clientes Host On Demand que conectam-se a um sistema host por meio de portas abertas no firewall, veja “Configurando Portas de Firewall” na página 33 para obter detalhes. Para clientes Host On Demand que conectam-se a um sistema

host por meio de um servidor proxy Socks ou HTTP, veja “Conectando-se a um Sistema Host Através de um Servidor Proxy” na página 35 para obter detalhes.

Configurando Portas de Firewall

Se você estiver utilizando o modelo baseado no servidor de configuração ou o modelo combinado, os clientes Host On-Demand precisarão se comunicar com o servidor de configuração. Para permitir isso através de um firewall, você precisará abrir a porta do Gerenciador de Serviços do Host On-Demand ou utilizar o servlet de configuração do Host On-Demand. O Gerenciador de Serviços atende, por padrão, na porta 8999. Você pode alterar esse padrão para qualquer outro número de porta disponível. Para obter detalhes, consulte Alterando a porta do Gerenciador de Serviços na ajuda on-line. O servlet de configuração do Host On-Demand permite que os clientes Host On-Demand comuniquem-se com o servidor de configuração através de HTTP ou HTTPS. Portanto, a porta do Gerenciador de Serviços não precisará ser aberta no firewall. (Veja a Figura 4 na página 13). Consulte “Instalando o Servlet de Configuração” na página 60 e Configurando o servlet de configuração na ajuda on-line para obter detalhes sobre a utilização do servlet de configuração.

Se você estiver utilizando o modelo baseado em HTML, não há nenhum requisito para os clientes Host On-Demand acessarem o servidor de configuração e a porta do Gerenciador de Serviços não precisará ser aberta no firewall. Os clientes ainda tentarão contatar o servidor de configuração para contagem de licenças, mas falharão silenciosamente se a porta do Gerenciador de Serviços não estiver aberta. Se desejar prevenir os clientes de fazer pedidos de contagem de licença, você poderá adicionar um parâmetro Desativar com um valor de LUM na exibição em árvore Parâmetros Adicionais na janela Opções Avançadas no Deployment Wizard.

Além da porta do Gerenciador de Serviços, certifique-se de que o administrador de firewall abra quaisquer portas que estejam em uso por funções utilizadas pelos clientes. Por exemplo, se você tiver uma sessão TLS com o Redirecionador na porta 5000, a porta 5000 deverá ser aberta para o tráfego de Telnet. A tabela a seguir resume as portas que o Host On-Demand pode utilizar.

Tabela 10. Funções do Host On-Demand e as Portas que Elas Utilizam

Função do Host On-Demand	Portas Utilizadas
Emulação de terminal (3270 e VT) e Emulação de impressora 3270	23 (Telnet), 80 (HTTP) ou 443 (TLS) e 8999 (servidor de configuração) ³
Emulação de Terminal e de Impressora 5250	23 (Telnet) ou 992 ¹ (TLS) ou 80 (HTTP) ou 443 (TLS) e 8999 (servidor de configuração) ³
Transferência de arquivos 3270	23 (Telnet), 80 (HTTP) ou 443 (TLS) e 8999 (servidor de configuração) ³
Transferência de arquivos 5250 - savfile	80 (HTTP), 8999 (servidor de configuração) ³ , 21 (FTP) ⁴ , >1024 (FTP) ⁴ , 446 (drda) ⁴ , 449 (as-svrmap) ⁴ , 8470 (as-central) ^{1 2 4} , 8473 (as-file) ^{1 4} , 8475 (as-rmtcmd) ^{1 4} e 8476 (as-signon) ^{1 4}
Transferência de arquivos 5250 - banco de dados	80 (HTTP), 8999 (servidor config) ³ , 446 (drda) ⁴ , 449 (as-svrmap) ⁴ , 8470 (as-central) ^{1 2 4} , 8473 (as-file) ^{1 4} , 8475 (as-rmtcmd) ^{1 4} e 8476 (as-signon) ^{1 4}
Transferência de arquivos 5250 - arquivo de fluxo	80 (HTTP), 8999 (servidor config) ^{1 2 4} , 449 (as-svrmap) ⁴ , 8470 (as-central) ^{1 2 4} , 8473 (as-file) ^{1 4} e 8476 (as-signon) ^{1 4}

Tabela 10. Funções do Host On-Demand e as Portas que Elas Utilizam (continuação)

FTP	21 (FTP), 80 (HTTP), 8999 (servidor de configuração) ^{1 2 4} e >1024 (FTP) ⁵
CICS	2006
Database On-Demand	80 (HTTP), 8999 (servidor config) ³ , 449 (as-svrmap) ⁴ , 8470 (as-central) ^{1 2 4} , 8471 (as-database) ^{1 4} e 8476 (as-signon) ^{1 4}
LUM (License Use Management)	8999 (servidor de configuração) para contagem de uso de licença padrão utilizando o servidor de configuração
Clientes Host On-Demand	23 (Telnet), 80 (HTTP) e 8999 (servidor config) ³
Clientes de administração	80 (HTTP) e 8999 (servidor config) ³
SSH (o Secure Shell)	22

Tabela 11. Notas

Notas:

- 1 Você pode alterar os números da porta com o comando WRKSRVTBLE. Os números da porta listados são os valores padrão.
- 2 A porta para as-central é utilizada apenas se uma tabela de conversão de página de códigos precisar ser criada dinamicamente (EBCDIC para/do Unicode). Isso depende do JVM e do local do cliente.
- 3 Você pode alterar a porta do config server. A porta 8999 é a padrão.
- 4 Estas portas não precisam ser abertas no firewall se você estiver usando o suporte a servidor proxy IBM System i. Você precisará abrir a porta do servidor proxy padrão 3470. Essa porta pode ser alterada.
- 5 No modo passivo (PASV), o cliente FTP inicia ambas as conexões com o servidor, resolvendo o problema de firewalls que filtram a conexão da porta de dados de entrada para o cliente a partir do servidor. Ao abrir uma conexão de FTP, o cliente abre localmente duas portas não privilegiadas aleatoriamente (N>1024 e N+1). A primeira porta contata o servidor na porta 21, mas em vez de emitir um comando PORT e permitir que o servidor conecte-se novamente à sua porta de dados, o cliente emite o comando PASV. Como resultado, o servidor abre uma porta não privilegiada aleatória (P>1024) e envia o comando PORT P novamente para o cliente. Em seguida, o cliente inicia a conexão a partir da porta N+1 para a porta P no servidor para transferir dados.

Do ponto de vista do firewall do lado do servidor, para suportar o FTP no modo passivo, é necessário abrir as portas de comunicação a seguir:

- Porta 21 do servidor FTP a partir de qualquer lugar (o cliente inicia a conexão)
- Porta 21 do FTP para portas remotas >1024 (o servidor responde à porta de controle do cliente)
- Portas do servidor FTP >1024 a partir de qualquer lugar (o cliente inicia a conexão de dados para a porta aleatória especificada pelo servidor)
- Porta do servidor FTP >1024 para portas remotas >1024 (o servidor envia ACKs (e dados) para a porta de dados de cliente)

Se você não deseja abrir a porta 8999 no firewall, ainda pode permitir que os usuários acessem o Host On-Demand. Existem duas opções:

- Utilize o Deployment Wizard para criar arquivos HTML que contêm todas as informações de configuração. Isto elimina a necessidade de acessar o servidor de configuração. Ao criar os arquivos HTML, escolha “modelo baseado em HTML” na página Modelo de Configuração do Deployment Wizard.

- Se você deseja utilizar o servidor de configuração, pode configurar clientes para utilizar o servlet de configuração. Consulte Configurando o servlet de configuração na ajuda on-line do Host On-Demand. Esta opção estará disponível somente se o servidor Web suportar servlets.

Se você utilizar o servidor de configuração e ele estiver separado do navegador por um firewall, será necessário abrir a porta do servidor de configuração no firewall ou executar o servlet de configuração do Host On-Demand. O servlet de configuração permite que o navegador comunique-se com o servidor de configuração através de protocolos da Web padrão, como HTTP ou HTTPS. (Veja a Figura 4 na página 13).

Conectando-se a um Sistema Host Através de um Servidor Proxy

Os clientes Host On-Demand podem utilizar um servidor proxy para acessar transparentemente os sistemas host sob um firewall. Dois tipos de servidores proxy são suportados:

- Servidores proxy Socks, descritos em “Conectando-se por meio de um servidor proxy Socks”. Tanto a versão 4 como a versão 5 do Socks são suportadas.
- Servidores proxy HTTP, descritos em “Conectando-se por meio de um servidor proxy HTTP” na página 36.

Antes de conectar-se a um sistema host por meio de um servidor proxy, é necessário descobrir qual protocolo o servidor proxy suporta. Decida se você deseja especificar as definições do servidor proxy através do navegador da Web ou identificar explicitamente um servidor proxy para a sessão. Se você decidir identificar explicitamente um servidor proxy, é necessário especificar o protocolo usado pelo servidor proxy, o nome do servidor proxy e o número da porta, além de outras informações.

Em geral, se um servidor proxy Socks estiver disponível, configure as sessões do Host On-Demand para utilizá-lo. Configure as sessões para utilizar um servidor proxy HTTP se esse for o único tipo de servidor proxy suportado em seu site.

Conectando-se por meio de um servidor proxy Socks

Muitas organizações utilizam os servidores proxy Socks para proteger recursos de computação sob um firewall. Socks é um protocolo para proxies de rede com base em TCP/IP. Ele permite que os aplicativos em um lado de um servidor proxy Socks tenham acesso total aos hosts no outro lado do servidor proxy Socks, sem conexão direta com eles. Os servidores Proxy são geralmente utilizados juntamente com os firewalls. Sob o protocolo Socks, um cliente que solicita uma conexão com um sistema host através de um firewall, na verdade, conecta-se a um servidor proxy Socks. O servidor proxy Socks age como um intermediário entre o cliente e o sistema host. Ele autoriza os pedidos de comunicação, conecta-se ao host em nome do cliente e retransmite dados entre os dois sistemas.

O Host On-Demand suporta as versões 4 e 5 do protocolo Socks.

- O Socks versão 4 especifica o formato da mensagem e as convenções para permitir que os usuários do aplicativo baseado em TCP acessem através de um firewall. Ele fornece controle de acesso com base nas informações de cabeçalho do TCP, incluindo endereços IP e números de porta de origem e de destino.
- O Socks versão 5 (também conhecido como AFT (Authenticated Firewall Traversal)) é um padrão Internet aberto para proxies de rede. Ele adiciona autenticação, melhor suporte para resolver nomes de domínios, suporte para endereços IPv6 e outros recursos para a versão 4. Esses recursos são muito úteis

para clientes localizados fora de um firewall. Um ID de usuário e senha do Socks para o servidor proxy podem, opcionalmente, ser enviados através da conexão entre o cliente Host On-Demand e o servidor proxy. O ID de usuário e a senha não são criptografados. Para obter mais informações sobre a versão 5, veja *Protocolo Socks versão 5*.

O JVM (Java Virtual Machine) utilizado na maioria dos navegadores da Web suporta o Socks versão 4. Uma sessão pode acessar um servidor proxy do Socks versão 4 ou versão 5, ignorando as definições de servidor proxy no navegador da Web. Você também pode precisar negociar a sessão de conexão de um Socks versão 4, se o servidor proxy não suportar a versão 5. Para obter informações adicionais sobre as definições do servidor proxy Socks, consulte Servidor Proxy na ajuda on-line.

Conectando-se por meio de um servidor proxy HTTP

Os servidores proxy HTTP tratam de pedidos HTTP através de firewalls. Eles agem como intermediários entre as redes locais privadas e a Internet. O servidor proxy HTTP é conectado à rede local e à Internet. Os usuários locais configuram seus navegadores para transmitir pedidos HTTP através do servidor proxy HTTP, especificando o endereço IP e o número da porta TCP do servidor proxy. O servidor proxy HTTP aceita esses pedidos HTTP e os encaminha para os servidores Web reais especificados pelas URLs digitadas no navegador.

Para clientes Host On-Demand, os servidores proxy HTTP agem como agentes de encaminhamento para conexões com um sistema host. O servidor proxy HTTP abre uma conexão com o sistema host e envia os dados, de um lado para outro, entre o sistema host e o cliente. Embora um servidor proxy HTTP geralmente feche uma conexão depois de atender a um pedido HTTP, o Host On-Demand mantém a conexão aberta para o tráfego do host, utilizando o Método de Conexão HTTP (se estiver ativado para o servidor proxy).

Para utilizar uma sessão de um servidor proxy HTTP, você precisa selecionar o proxy HTTP como o tipo de proxy e especificar o nome do servidor proxy e o número da porta. Para obter informações adicionais sobre as definições do servidor proxy HTTP, consulte Servidor Proxy na ajuda on-line.

Segurança do ID de Usuário

Web Express Logon

Se você tiver um aplicativo de segurança de rede adequado e se estiver utilizando o modelo baseado no servidor de configuração, poderá selecionar o Web Express Logon no Deployment Wizard para permitir aos usuários acessar hosts e aplicativos baseados no host sem fornecer um ID de usuário e senha adicionais. Digitar a URL completa do Servidor do Mapeador de Credencial informa ao Host On-Demand onde localizar o Servlet do Mapeador de Credencial, que processa o pedido HTTPS do usuário, desempenha uma procura e retorna credenciais do usuário. As credenciais são utilizadas para desempenhar um login seguro e automatizado do Host On-Demand.

Autenticação Nativa

Se utilizar o modelo baseado no servidor de configuração, você poderá configurar os usuários do Host On-Demand para serem autenticados nativamente. Esta opção permite que os usuários efetuem logon no Host On Demand usando a mesma senha que usariam para efetuar logon no sistema operacional (AIX ou z/OS) no

qual o Host On Demand está ativo. Quando um usuário efetua logon no Host On-Demand, sua senha é validada contra a senha do sistema operacional, em vez de uma senha do Host On-Demand separada. Isso fornece ao administrador um ponto único de controle para administração da senha e ao usuário uma única senha para memorizar.

Consulte Autenticação Nativa na ajuda on-line, para obter informações adicionais sobre como ativar essa opção.

Logon de Domínio do Windows

Se os usuários tiverem efetuado logon em um domínio do Windows, esta opção (disponível com o modelo baseado no servidor de configuração no Deployment Wizard) efetuará logon dos usuários automaticamente no Host On-Demand utilizando os nomes de usuário do Windows. A janela de logon do Host On-Demand não aparece e o nome do usuário do Windows é utilizado como o ID de usuário do Host On-Demand. Se um ID de usuário do Host On-Demand ainda não existir (correspondendo ao nome do usuário do Windows), você também poderá optar por criar um ID de usuário automaticamente no grupo do Host On-Demand especificado.

Consulte Tipo de Logon na ajuda on-line, para obter informações adicionais sobre como escolher como os usuários acessam o servidor de configuração do Host On-Demand.

Ambientes FIPS

Se você estiver em um ambiente que exija ou requeira que os componentes de segurança utilizem componentes/módulos certificados pelo FIPS (Federal Information Processing Standards), considere o seguinte. Para conexões de Telnet e de FTP, o Host On-Demand utiliza módulos compatíveis com FIPS por padrão. Se seu ambiente requerer a conexão com um host IBM System i para transferência de arquivos ou transferência de dados, assegure-se de que seu sistema atenda aos requisitos a seguir:

- Você está usando um JRE Java que é certificado pelo FIPS, por exemplo, IBM 1.6.0 Liberação de Serviço 5.
- É necessário configurar o parâmetro HTML UseJSSEforiSeries na janela Opções avançadas do Assistente de Implementação e configurar seu valor como true.
- É necessário incluir o certificado do host IBM System i no armazenamento confiável do cliente Java Secure Socket Extension (JSSE) para o Java JRE. Consulte seu provedor do JRE Java para detalhes de configuração.

Quando tiver uma conexão segura com um host IBM System i e estiver acessando os recursos de transferência de arquivos, será solicitado que insira o caminho e a senha para o Armazenamento confiável JSSE. Se estiver executando a transferência de dados para um host IBM System i, também verá campos adicionais para inserir o caminho e a senha para o Armazenamento confiável JSSE.

Outra maneira de digitar o caminho e a senha é utilizar um Applet de Execução que é fornecido com o Host On-Demand. Para isso, execute as seguintes etapas:

1. No menu de uma sessão de vídeo, selecione Ações > Applet de Execução.
2. Digite `com.ibm.eNetwork.HOD.util.jsse.JSSESetup` no campo para o nome da classe.
3. Clique OK.

É necessário configurar o Armazenamento confiável do JSSE somente uma vez. Ele é uma configuração global que se aplica a todas as sessões. Depois que os valores forem inseridos, eles persistirão até que o navegador seja reiniciado.

Em versões anteriores do Host On Demand, é possível ativar a autenticação no modo FIPS por meio de um parâmetro HTML. A versão atual do Host On-Demand fornece uma opção de menu para ativar ou desativar o modo FIPS para cada sessão. Por padrão, o modo FIPS é ativado para todas as sessões.

Capítulo 5. Planejamento para Suporte ao Idioma Nacional

O Host On Demand é fornecido em vários idiomas. As janelas da sessão, os painéis de configuração, os arquivos de ajuda e a documentação foram traduzidos. Além disso, o suporte para exibição, teclado e processamento é fornecido em árabe, hebraico, tailandês e hindi. Esse suporte é totalmente explicado na ajuda on-line.

Todas as versões traduzidas são fornecidas nos DVDs e na fitas do zSeries. Ao instalar o Host On-Demand on i/OS, OS/400, Windows, AIX, Linux e Solaris usando o programa de instalação gráfica, é possível escolher quais idiomas instalar. No z/OS e Novell, todos os idiomas são sempre instalados.



O suporte ao idioma nacional é dependente do sistema operacional, assim, o suporte ao teclado e a fonte apropriada para o idioma que deseja utilizar devem estar instalados no sistema operacional. Por exemplo, se deseja utilizar o coreano como o idioma da sessão host, mas não possui a fonte coreana e o suporte ao teclado instalados, não será possível exibir os caracteres corretos.



DBCS não pode ser utilizado como nome de arquivo HTML.

Idiomas Suportados

Os idiomas nos quais o Host On-Demand foi traduzido estão listados abaixo, junto com os sufixos do idioma que você pode utilizar para carregar as versões traduzidas dos clientes Host On-Demand. Por exemplo, as páginas HTML fornecidas pela IBM possuem extensões de idioma para identificar diferentes instalações de idioma e diferentes arquivos HTML predefinidos de idioma, tal como HOD_en.html para Inglês.

Idioma	Sufixo do Idioma
Chinês Simplificado	zh
Chinês Tradicional	zh_TW
Tcheco	cs
Dinamarquês	da
Holandês	nl
Inglês	en
Finlandês	fi
Francês	fr
Alemão	de
Grego	el
Húngaro	hu
Italiano	it
Japonês	ja
Coreano	ko
Norueguês	no

Polonês	pl
Português do Brasil	pt
Português	pt_PT
Russo	ru
Esloveno	sl
Espanhol	es
Sueco	sv
Turco	tr
Catalão	Ca

Páginas de Códigos do Host Suportadas

O Host On-Demand suporta várias páginas de códigos. Estas páginas de códigos podem ser especificadas em uma base de sessão-por-sessão.

Páginas de Códigos 3270 e 5250

As páginas de códigos especificadas abaixo são suportadas pelos emuladores 3270 e 5250. Você pode selecioná-las na janela Configuração da Sessão.

País ou Região	Página de Códigos	Nota
Língua Árabe	420	
Áustria	273	
Áustria (Euro)	1141	
Bielo-Rússia	1025	
Bielo-Rússia (Euro)	1154	
Bélgica	037	
Bélgica (Euro)	1140	
Bélgica (Código Antigo)	274	
Bósnia/Herzegovina	870	
Bósnia/Herzegovina (Euro)	1153	
Brasil	037	
Brasil (Euro)	1140	
Brasil (Antigo)	275	
Bulgária	1025	
Bulgária (Euro)	1154	
Canadá	037	
Canadá (Euro)	1140	
China (Chinês Simplificado Estendido)	1388	
Croácia	870	
Croácia (Euro)	1153	
República Tcheca	870	
República Tcheca (Euro)	1153	
Dinamarca	277	

Dinamarca (Euro)	1142	
Estônia	1122	
Estônia (Euro)	1157	
Finlândia	278	
Finlândia (Euro)	1143	
França	297	
França (Euro)	1147	
Macedônia	1025	
Macedônia FYR (Euro)	1154	
Alemanha	273	
Alemanha (Euro)	1141	
Grécia	875	
Hebraico (Código Novo)	424	
Hebraico (Código Antigo)	803	
Hindi	1137	Exibição 5250 apenas
Hungria	870	
Hungria (Euro)	1153	
Islândia	871	
Islândia (Euro)	1149	
Itália	280	
Itália (Euro)	1144	
Japão (Katakana)	930	
Japão (Katakana Estendido)	930	
Japonês (Unicode Katakana Estendido; JIS2004)	1390	3270 apenas
Japão (Latim Estendido)	939	
1399 Japonês (Unicode latim estendido; JIS2004)	1399	
Cazaquistão (Euro)	1166	
Coréia (Euro)	1364	3270 apenas
Coréia (Estendido)	933	
América Latina	284	
América Latina (Euro)	1145	
Letônia	1112	
Letônia (Euro)	1156	
Lituânia	1112	
Lituânia (Euro)	1156	
Multilíngüe	500	
Multilíngüe ISO (Euro)	924	
Multilíngüe (Euro)	1148	
Holanda	037	
Holanda (Euro)	1140	

Noruega	277	
Noruega (Euro)	1142	
Edição Aberta	1047	
Polônia	870	
Polônia (Euro)	1153	
Portugal	037	
Portugal (Euro)	1140	
Romênia	870	
Romênia (Euro)	1153	
Rússia	1025	
Rússia (Euro)	1154	
Sérvia/Montenegro (Cirílico)	1025	
Sérvia/Montenegro (Cirílico; Euro)	1154	
Eslováquia	870	
Eslováquia (Euro)	1153	
Eslovênia	870	
Eslovênia (Euro)	1153	
Espanha	284	
Espanha (Euro)	1145	
Suécia	278	
Suécia (Euro)	1143	
Taiwan (Chinês Tradicional Estendido)	937	
Taiwan (Chinês Tradicional Estendido; Euro)	1371	
Tai	838	
Tai (Euro)	1160	
Turquia	1026	
Turquia (Euro)	1155	
Ucrânia	1123	
Ucrânia (Euro)	1158	
Reino Unido	285	
Reino Unido (Euro)	1146	
Estados Unidos	037	
Estados Unidos (Euro)	1140	

Notas:

- A impressão de host 3270 com uma PDT (Printer Definition Table) suporta somente as páginas de códigos Latin-1, DBCS, bidirecional e Tai. Outras páginas de códigos são suportadas na impressão Adobe PDF ou em plataformas Windows sem uma PDT.
- Para incluir mais caracteres (definidos no padrão GB18030 pelo Governo da República Popular da China), 6582 Unicode Extensão-A e 1.948 caracteres

adicionais não-Han (Mongol, Uygur, Tibetano, e Yi) foram incluídos na página de códigos 1388 de Chinês Simplificado para o Host On-Demand Versão 6.

Páginas de Códigos VT

Idioma	Página de Códigos
Árabe	ASMO 708 e ASMO 449
Britânico	1101
DEC Grego	
Hebraico DEC	
Conjunto de Caracteres de Substituição Multinacional DEC	1100
DEC Técnico	
Holandês	1102
Finlandês	1103
Francês	1104
Francês canadense	1020
Alemão	1011
Hebraico NRCS	
Grego ISO Suplementar (ISO Latim-7)	813
Hebraico Complementar ISO	
ISO Latim-1	819
Italiano	1012
Norueguês/Dinamarquês	1105
PC Dinamarquês/Norueguês	865
PC Internacional	437
PC Multilíngüe	850
PC Português	860
PRC GBK	936
PC Espanhol	220
Espanhol	1023
Sueco	1106
Suíço	1021
Estados Unidos	1100

Páginas de códigos do Gateway CICS

Página de Códigos	Conjunto de Caracteres
000	Detectar Automaticamente (padrão)
437	Latim-1
813	Grego ISO (8859_7)
819	Latim 1 ISO (8859_1)
850	Latim 1
852	Latim 2

855	Cirílico
856	Hebraico
857	Latim 5
864	Árabe
866	Cirílico
869	Grego
874	Tai
912	Latim 2 ISO (8859_2)
915	Cirílico ISO (8859_5)
920	Latim 5 ISO(8859_9)

Suporte ao JIS2004 Unicode Japonês

O suporte do JIS2004 pode agora ser ativado selecionando as páginas de códigos do host existentes 1390 japonês (Unicode Katakana Estendido) e 1399 japonês (Unicode Latino Estendido). Os seguintes recursos são suportados:

- Edição de espaço de apresentação
- Designações de teclas
- Transferência de arquivos
- Tela de impressão
- Sessão de impressora
- GDI
- Adobe PDF
- Host Access Class Library (HACL)

Funções não incluídas devido aos formatos Unicode não suportados atualmente em HOD:

- Macro
- Use Printer Definition Table (PDT) na sessão da impressora

Mapeamento de Caracteres Definido pelo Usuário

Para idiomas do DBCS (Conjunto de Caracteres de Byte Duplo), você pode utilizar o mapeamento de UDC (User Defined Character) personalizado em sua sessão (impressão do host 3270, 5250, 3270) em vez do mapeamento padrão. Você pode criar uma tabela de conversão de UDC utilizando o editor de mapeamento de UDC para armazenar mapeamento personalizado para sua sessão. Para obter instruções sobre como utilizar o editor de mapeamento UDC para alterar o mapeamento de caracteres, consulte Utilizando o editor de mapeamento UDC (User-Defined Character) na ajuda on-line.

Suporte a Unicode para i/OS e OS/400

Consulte “Suporte a Unicode para i/OS e OS/400” na página 128.

Parte 2. Instalando, Efetuando Upgrade e Desinstalando o Host On-Demand

Capítulo 6. Instalando o Servidor Host On-Demand e o Software Relacionado

Este capítulo discute a instalação dos três seguintes componentes do Host On-Demand:

- O servidor Host On-Demand, que é necessário para utilizar o Host On-Demand. Consulte “Instalando o Host On-Demand usando o Installation Manager” para obter instruções.
- O servlet de configuração do Host On-Demand, que é necessário apenas em instâncias específicas quando você está executando o Host On-Demand em conjunto com um firewall. Consulte “Instalando o Servlet de Configuração” na página 60 para obter explicação e instruções adicionais.
- O Deployment Wizard, uma ferramenta extremamente útil executada no Windows para gerar clientes Host On-Demand personalizados. A instalação do Deployment Wizard não é obrigatória, mas é altamente recomendável. Consulte “Assistente de Implementação” na página 50 para obter instruções.

Instalando o Host On-Demand usando o Installation Manager

É necessário o IBM Installation Manager para instalar o Host On-Demand. O IBM Installation Manager precisa ser instalado primeiro no Modo de Administrador no sistema em que o Host On-Demand estiver planejado para instalação. Em seguida, é possível usar o gerenciador de instalação para instalar o Host On-Demand.

O IBM Installation Manager Versão 1.8.3 ou superior é necessário para instalar o Host On-Demand.

Links importantes

Consulte as instruções em Instalando ou atualizando o Installation Manager para instalar o gerenciador de instalação. Para obter mais informações sobre o IBM Installation Manager, consulte o IBM Installation Manager Knowledge Center.

Antes da instalação do HOD

Preparando para instalação

Assegure-se de que a máquina na qual a instalação ocorrerá atenda a todos os pré-requisitos.

Os requisitos de software para Host On-Demand podem ser localizados em Relatórios de compatibilidade de produtos de software. Verifique a lista abaixo para a preparação:

- Assegure-se de que o IBM Installation Manager v1.8.3 ou superior esteja instalado.
- Sua máquina precisa de no mínimo 1,2 de espaço em disco para instalação (instalado e espaço temporário) para a arquitetura de 32 bits e um idioma. Para instalar mais de um idioma, esse valor aumenta de 4 para 8 MB para cada idioma.
- Você precisa no mínimo de 4,5 GB para o repositório de produto de multiplataforma (download e extração).

- Os usuários precisam efetuar logon com privilégios de Administrador.
- Uma versão suportada do servidor HTTP (por exemplo, IBM HTTP Server ou servidor Apache) é instalada no sistema.

Efetuando Upgrade de Versões Anteriores do Host On-Demand

Se você tiver uma versão anterior do Host On-Demand, como HOD V11.0, não haverá caminho de migração direto do HOD V11 para HOD V12.0 e versões acima. Siga estas etapas para migrar:

1. É necessário fazer backup de todos os arquivos customizados dos diretórios Host On-Demand anteriores, especificamente a partir do diretório privado e quaisquer páginas do cliente criadas com o Assistente de Implementação. Esses arquivos podem ser reutilizados no HOD V12.0.
2. Desinstale todas as instalações existentes do Host On-Demand V11.0.
3. A instalação do Host On-Demand inicial e acima requer que um caminho vazio esteja disponível. Portanto, é possível renomear ou excluir quaisquer pastas ou diretórios existentes em que uma versão anterior esteja instalada anteriormente.
4. Instale o Host On-Demand usando o IBM Installation Manager. É recomendado não clicar em **Cancelar** quando uma instalação está em andamento.
5. Restaure o diretório privado para as pastas ou diretórios do Host On-Demand.
6. Edite quaisquer clientes criados com o Assistente de Implementação com o Assistente de Implementação do Host On-Demand e implemente no servidor HOD.

Instalando o Host On-Demand

É possível instalar o Host On-Demand usando o gerenciador de instalação em todas as plataformas suportadas.

A GUI do Installation Manager

GUI do Installation Manager:

1. Inicie o Installation Manager de acordo com instruções para a plataforma.
2. Selecione **Arquivo > Preferências**.
3. Selecione **Repositórios** à esquerda. Esta opção mostra os repositórios disponíveis que foram incluídos no Installation Manager.
4. Selecione **Incluir repositório** se o Host On-Demand não estiver listado.
5. Clique em **Procurar e navegar** para o local do caminho do Host On-Demand extraído e selecione o arquivo diskTag.inf presente na pasta disk1.
6. Clique em **OK** e o novo local do repositório deverá ser listado.
7. Clique em **Testar Conexões** para assegurar que a URL do Repositório esteja disponível.
8. Na página inicial do gerenciador de instalação, clique em **Instalar**. O gerenciador de instalação procurará os repositórios definidos para pacotes disponíveis.
9. Selecione o **pacote do Host On-Demand**. Clique em **Avançar**.
10. Leia os contratos de licença. Se você concordar com os termos do contrato de licença, clique em **Eu aceito os termos do contrato de licença** e clique em **Avançar** para continuar.
11. Selecione **Criar um novo grupo de pacotes** e escolha a **Arquitetura**.

12. Se o sistema operacional for de 64 bits, é necessário selecionar *64 bits* ou *32 bits* para instalar o produto no modo de bit correspondente.
13. Clique em **Avançar**.
14. Selecione os idiomas que você deseja instalar. O padrão é *inglês*. Clique em **Avançar**.
15. Selecione o **recurso Host On-Demand 12.0**. Clique em **Avançar**.
16. Revise e especifique todas as informações sob a guia Host On-Demand 12.0.
 - a. No painel *Publicar informações* no Host On-Demand 12.0, configure o **diretório de Publicação**, especifique o alias do servidor da web e o *número da Porta do Gerenciador de Serviços*. Clique em **Avançar**.

O diretório de publicação armazena arquivos que devem estar disponíveis para os clientes. O assistente de instalação informa-o para designar seu diretório de publicação exibindo o diretório padrão. Execute as seguintes etapas:

 - 1) Especifique um alias para o diretório, o padrão é *hod*.
 - 2) Especifique a porta do Gerenciador de Serviços, através da qual clientes Host On-Demand se comunicam com o Gerenciador de Serviços. Essa comunicação é necessária pelas seguintes opções de implementação:
 - Usando o servidor de configuração para manter as informações de configuração de sessão como no servidor baseado em configuração e modelos de implementação combinados, descritos em Capítulo 2, "Planejamento para Implementação", na página 11.
 - Contagem de uso sob licença: consulte *Uso sob licença* na ajuda on-line.
 - A IBM recomenda designar *porta 8999* para esses propósitos. Verifique a documentação do servidor para ver se esta porta está sendo utilizada. Se estiver em uso, será possível mudar a porta durante ou após a instalação. Para obter informações adicionais sobre como alterar a porta do Gerenciador de Serviços, consulte *Alterando a porta de configuração do Gerenciador de Serviços* na ajuda on-line.
 - b. No painel do servidor da web em Host On-Demand 12.0, selecione a opção de servidor da web que seja apropriada para seu requisito:
 - Selecione **Sem servidor da web** quando o servidor da web estiver configurado manualmente pelo usuário. Isso é recomendado para servidores da web como IPlanet e Lotus Domino. O usuário é avisado para entrar em contato com seu administrador do servidor da web ou consultar a documentação do servidor da web para obter detalhes.
 - Selecione a opção 'Selecionar na lista de servidores da web detectados' e, em seguida, selecione o servidor da web na lista se mais de um foi detectado.
 - Selecione a opção **Selecionar manualmente o servidor da web específico**, caso um IBM HTTP Server ou servidor da web Apache esteja instalado, mas não detectado.
 - Selecione o tipo de servidor da web que está instalado em seu sistema.
 - Clique no botão **Navegar** e navegue até o arquivo de configuração (*httpd.conf*) para o servidor da web instalado em seu sistema. É possível, como alternativa, digitar no campo o caminho completo do arquivo *httpd.conf* no diretório de instalação do servidor da web.

- c. No painel do Servidor de aplicativos no Host On-Demand 12, se o programa de instalação detectar o IBM WebSphere Application Server em seu sistema, será possível configurar o Servlet de configuração. O próximo painel da guia Servidor de aplicativos se desejar configurar o Servlet de configuração de HOD no WebSphere Application Server. Consulte Instalando o servlet de configuração para obter mais informações.

Desmarque a caixa de seleção se não planejar usar o Servlet de configuração.

Se você planeja usar o Servlet de configuração, selecione o servidor de aplicativos na lista de detectados. O programa de instalação implementa automaticamente o servlet de configuração no servidor de aplicativos da Web designado e configura os clientes para acessarem o Gerenciador de Serviços através do servlet.

Nota:

- O Websphere Application Server é detectado se estiver instalado pelo mesmo programa IBM Installation Manager no sistema. As versões que podem ser detectadas são Websphere Application Server V8.0 e V8.5.2.
 - Um Servidor de aplicativos com a segurança administrativa ativada não é suportado para configuração de servlet durante a instalação.
- d. Uma vez que os painéis estejam atualizados apropriadamente, clique em **Avançar**.
17. Revise as informações de resumo e clique em **Instalar**.
18. Uma vez que a instalação esteja concluída, uma página de resumo será exibida. Revise as mensagens.
- Se a instalação for bem-sucedida, o programa exibe uma mensagem que indica que a instalação foi bem sucedida. O programa também pode exibir importantes instruções de pós-instalação. Clique em **Concluir**.
 - Se a instalação não for bem-sucedida, clique em **Visualizar Arquivo de Log** para solucionar o problema.
19. Para assegurar que a instalação seja concluída com sucesso, é possível executar as ações adicionais a seguir:
- a. Reinicie o servidor da web.
 - b. Assegure-se de que as páginas HOD estejam acessíveis no navegador. Se não, verifique a configuração do servidor da web e assegure-se de que os arquivos no diretório de publicação do Host On-Demand estejam acessíveis. Consulte a documentação do servidor da web para configurar os detalhes.

Assistente de Implementação

O Deployment Wizard é instalado automaticamente como parte da instalação do servidor Host On-Demand para Windows. Também está disponível separadamente para os clientes que não desejam instalar o servidor Host On-Demand inteiro para Windows. Os usuários podem selecionar apenas a opção do Assistente de Implementação durante a instalação.

Fazendo upgrade de versões anteriores do Assistente de Implementação

Se você tiver uma versão anterior do Assistente de Implementação, como a partir do HOD V11.0, não haverá caminho de upgrade direto do Assistente de Implementação V11.0 para o Assistente de Implementação V12.0 e versões posteriores. Execute as etapas a seguir para upgrade:

1. Faça um backup de quaisquer arquivos customizados do diretório do Assistente de Implementação. É possível reutilizá-los no Assistente de Implementação.
2. Desinstale qualquer instalação existente do Assistente de Implementação V11.0.
3. O novo Assistente de Implementação requer que um caminho vazio esteja disponível. Assim, renomeie ou exclua a pasta existente da instalação do Assistente de Implementação.
4. Instale o Assistente de Implementação usando o IBM Installation Manager.
5. Reimplante seus arquivos customizados na pasta de instalação do Assistente de Implementação.

Instalando o Deployment Wizard

Para instalar e executar o Assistente de Implementação, execute as tarefas a seguir:

1. Abra o Installation Manager.
2. Inclua o local do repositório do Host On-Demand no Installation Manager:
 - a. Na página inicial do Installation Manager, clique em **Arquivo > Preferências** e, em seguida, clique em **Repositórios**. A página Repositórios é aberta, mostrando quaisquer repositórios disponíveis, locais e status da conexão deles.
 - b. Na página Repositórios, clique em **Incluir Repositório**.
 - c. Na caixa de diálogo Incluir repositório, clique em **Procurar**.
 - d. Navegue até o local do disco 1 do Host On-Demand e selecione o arquivo diskTag.inf e, em seguida, clique em **OK**. O novo local do repositório é listado.
 - e. Clique em **Testar Conexões** para assegurar que a URL do Repositório esteja disponível.
 - f. Na página Início, clique em **Instalar**. O Installation Manager procura os pacotes disponíveis nos repositórios definidos.
 - g. Repita as etapas acima para o segundo disco. Se você continuar sem configurar o segundo disco, o Installation Manager confirmará com o usuário durante o processo de instalação.
3. Selecione o pacote do Assistente de Implementação do Host On-Demand.
4. Assegure-se de que a Versão 12.0 também esteja selecionada sob ele. Clique em **Avançar**.
5. No painel Instalar pacotes, selecione **Criar um novo pacote** e **Assistente de Implementação do IBM Host On-Demand** como o nome do Grupo de pacotes.
6. No caso da seleção Arquitetura estar configurada para 64 bits, mude a seleção para 32 bits, se necessário. Clique em **Avançar**.
7. No painel Instalar pacotes, selecione o recurso de Assistente de Implementação do Host On-Demand 12.0. As informações do disco na área inferior do painel fornece informações sobre o espaço em disco disponível e espaço em disco necessários. Clique em **Avançar**.
8. Selecione a guia para o painel Local do Assistente de Implementação do Host On-Demand e sob o título Host On-Demand Wizard 12.0 na guia esquerda. O local do servidor do Host On-Demand indica o link para o servidor do Host

On-Demand. Assegure-se de que um link válido e em funcionamento para o servidor HOD seja inserido no campo. Clique em **Avançar**.

9. No painel de resumo, revise os pacotes selecionados e seleções de instalação. Clique em **Instalar** para continuar com a instalação.

Fazendo o Download da Imagem de Instalação do Deployment Wizard a partir de um Servidor Host On-Demand

A imagem do Assistente de Implementação é enviada em todas as plataformas do servidor Host On-Demand e pode ser transferida por download a partir do servidor e instalada em qualquer máquina.

Para fazer download do Assistente de Implementação a partir de um servidor do Host On-Demand, execute as etapas a seguir:

1. Na sua máquina Windows, inicie seu navegador e aponte para o arquivo HODMain_xx.html em seu servidor do Host On-Demand, em que xx é seu sufixo de idioma de duas letras.
2. Clique na guia Administradores 3.
3. Clique no link de Assistente de Implementação para fazer download da imagem de instalação do Assistente de Implementação para sua máquina Windows.
4. Execute a instalação do Assistente de Implementação para instalar o Assistente de Implementação.
5. Uma vez que a instalação esteja concluída, é possível abrir o Assistente de Implementação no menu da área de trabalho **Iniciar > Programas**.

Host Access Toolkit

O Host Access Toolkit é instalado automaticamente como parte da instalação de servidor do Host On-Demand do Windows. Também está disponível separadamente para os clientes que não desejam instalar o servidor Host On-Demand inteiro para Windows. Os usuários podem selecionar apenas a opção Host Access Toolkit durante a instalação.

Fazendo upgrade de versões anteriores do Host Access Toolkit

Se você tiver uma versão anterior do Host Access Toolkit, como a partir do Host Access Toolkit V11.0, não há caminho de upgrade direto a partir do Host Access Toolkit V11.0 para Host Access Toolkit V12.0 e acima. Execute as etapas a seguir para upgrade:

1. Faça um backup de quaisquer arquivos customizados a partir do diretório Host Access Toolkit. É possível reutilizá-los no Host Access Toolkit.
2. Desinstale qualquer instalação existente do Host Access Toolkit V11.0.
3. O novo Host Access Toolkit requer que um caminho vazio esteja disponível. Assim, renomeie a pasta existente da instalação do Host Access Toolkit.
4. Instale o Host Access Toolkit usando o IBM Installation Manager.
5. Reimplante seus arquivos customizados na pasta de instalação do Host Access Toolkit.

Instalando o Host Access Toolkit

Execute as etapas básicas a seguir para instalar o Host Access Toolkit em um sistema Windows:

1. Abra o Installation Manager.
2. Inclua o local do repositório do Host On-Demand no Installation Manager.
 - a. Na página inicial do Installation Manager, clique em **Arquivo > Preferências** e, em seguida, clique em **Repositórios**. A página Repositórios é aberta, mostrando quaisquer repositórios disponíveis, os locais e status de conexão deles.
 - b. Na página Repositórios, clique em **Incluir Repositório**.
 - c. Na caixa de diálogo Incluir repositório, clique em **Procurar**. Navegue até o local de seu disk1 do Host On-Demand e selecione o arquivo diskTag.inf. Em seguida, clique em **OK**. O novo local do repositório é listado.
 - d. Clique em **Testar Conexões** para assegurar que a URL do Repositório esteja disponível.
 - e. Na página Início, clique em **Instalar**. O Installation Manager procura pacotes disponíveis em seus repositórios definidos.
 - f. Repita as etapas acima para o segundo disco. Se você continuar sem configurar o segundo disco, o gerenciador de instalação confirmará com você durante o processo de instalação.
3. Selecione o pacote do Host Access Toolkit.
4. Assegure-se de que a Versão 12.0 também esteja selecionada sob ele. Clique em **Avançar**.
5. No painel Instalar pacotes, selecione **Criar um novo pacote** e selecione **IBM Host Access Toolkit** como o nome do grupo de pacotes.
6. No caso de a seleção de Arquitetura ser configurada como 64 bits, mude a seleção para 32 bits, porque é a recomendada. Clique em **Avançar**.
7. Selecione os idiomas que você deseja instalar. O padrão é *inglês*. Clique em **Avançar**.
8. No painel Instalar pacotes, selecione o recurso Host Access Toolkit 12.0. As informações do disco na área inferior do painel fornece informações sobre o espaço em disco disponível e espaço em disco necessários. Clique em **Avançar**.
9. Selecione a guia para painel do Host Access Toolkit 12.0 sob o título Host Access Toolkit 12.0 na guia esquerda.
10. No painel de resumo, revise os pacotes selecionados e seleções de instalação. Clique em **Instalar** para continuar com a instalação.

Instalando o Modo de Console

Este capítulo contém instruções de uso do modo do console do Installation Manager para instalar o Host On-Demand em plataformas que não suportam uma Interface Gráfica com o Usuário.

Nota: Se você estiver instalando para IBM iSeries, será sugerida a leitura de “Antes de instalar o HOD no IBM iSeries” na página 54.

Sobre a instalação no Modo de Console

Os administradores dos sistemas Linux, UNIX e z/OS, que não suportam uma interface gráfica com o usuário (GUI), podem usar a interface baseada em console do Installation Manager para instalar o Host On-Demand.

Usando o modo do console do IBM Installation Manager, é possível trabalhar nos pacotes de instalação para concluir as tarefas a seguir:

- Tarefas de Instalação

- Efetuar upgrade
- Modify
- Recuperar
- Desinstalando

Para iniciar o modo do console do Installation Manager, use o utilitário *imcl* disponível no diretório de ferramentas do Installation Manager.

Essas etapas de instalação incluem um cenário de instalação típico usando o modo do console. Durante a sessão de instalação, os prompts do modo do console são exibidos específicos para o pacote que está sendo instalado. É possível seguir as opções conforme aparecem na tela do console para continuar com a instalação.

A interface do modo do console do Installation Manager usa essas convenções:

- [X] indica uma opção selecionada.
- [] indica uma opção que não está selecionada.
- Os comandos padrão são cercados por colchetes [].
- [N] Indica que o comando padrão é N: Avançar.

Nota: Mais informações sobre o Installation Manager e o modo do console estão disponíveis no Installation Manager Knowledge Center para a versão do Installation Manager que você instalou. Consulte o IBM Installation Manager Knowledge Center.

O Installation Manager pode ser instalado usando as informações fornecidas na documentação do Installation Manager Instalando ou atualizando o Installation Manager.

Para instalar o Host On-Demand, o Installation Manager deve ser instalado no modo de Administrador. Para obter mais informações sobre o download do Installation Manager, consulte os Requisitos de sistema para IBM Installation Manager e Packaging Utility, o nível mínimo é 1.8.3 para instalar o Host On-Demand.

Para obter mais informações sobre o uso do Installation Manager, consulte o IBM Installation Manager Knowledge Center.

Antes de instalar o HOD no IBM iSeries

A instalação do Host On-Demand em plataformas IBM iSeries é suportada por meio do modo do console do Installation Manager. O modo GUI da instalação não está disponível no IBM iSeries.

As notas adicionais antes da instalação do Host On-Demand no IBM iSeries estão listadas abaixo:

- Assegure-se de que o IBM Installation Manager V1.8.3 ou superior esteja instalado e que ele deve ser instalado no modo de Administrador. É recomendado seguir a documentação do IBM Installation Manager para obter detalhes adicionais. As informações sobre a instalação do Installation Manager V1.8.3 estão disponíveis em: instalando o Installation Manager no IBM i.
- A instalação é executada por um usuário com o administrador ou privilégios de administrador.
- A instalação remota no IBM i não está disponível no HOD V12.0 usando o Installation Manager.

Para iniciar a instalação, é necessário executar as tarefas a seguir:

1. Copie os arquivos zip ESD do Host On-Demand no IBM i a partir do FTP (Protocolo de Transferência de Arquivos) ou por qualquer meio regular e extraia o arquivo zip.
2. Abra o Installation Manager e configure um repositório fornecendo o caminho completo para o arquivo `diskTag.inf` que está no disco do Host On-Demand.
3. Continue com as etapas restantes, conforme fornecido na instalação do modo do console.

Procedimento de instalação

Para instalar o HOD no Modo de Console, execute as tarefas a seguir:

1. Inicie o IBM Installation Manager no modo do console. Abra um prompt de comandos com os privilégios de administrador e mude para a pasta `tools` no diretório de instalação do IBM Installation Manager.
2. Execute o comando a seguir no diretório de ferramentas

```
imcl -c
```

.

Em diferentes sistemas operacionais, por exemplo:

- AIX® ou Linux:
`/opt/IBM/InstallationManager/eclipse/tools/imcl -c`
- IBM i:
`/QIBM/ProdData/InstallationManager/eclipse/tools/imcl -c`
- Windows:
`\Program Files\IBM\Installation Manager\eclipse\tools\imcl.exe -c`
- z/OS:
`/InstallationManager/bin/eclipse/tools/imcl -c`

Para obter mais detalhes sobre iniciar o Installation Manager no modo do console, consulte *Iniciando o modo do console*.

3. Na janela do console, especifique o repositório do IBM Host On-Demand:
 - a. Digite *P* e, em seguida, pressione **Enter** para editar preferências.
 - b. Digite *1* e, em seguida, pressione **Enter** para especificar repositórios.
 - c. Digite *D* e, em seguida, pressione **Enter** para incluir um repositório.
 - d. Digite o caminho do repositório para o IBM Host On-Demand 12.0. Por exemplo, `<path>\HOD\disk1\diskTag.inf`.
 - e. Digite *A* e, em seguida, pressione **Enter** para salvar as informações do repositório.
 - f. Digite *R* e, em seguida, pressione **Enter** para retornar para o menu principal.
4. Selecione *1* para instalar a partir do menu principal. Se você tiver repositórios que requerem credenciais, será informado para inserir seu ID e, em seguida, a senha. Também é possível salvar as credenciais quando for solicitado. Consulte *Salvando credenciais no modo do console no Installation Manager Knowledge Center*.
5. No painel para selecionar pacotes para instalação, digite o número apropriado para selecionar o pacote do Host On-Demand 12.0.
6. No painel subsequente, digite o número apropriado para escolher a versão 12.0 para instalação e pressione **Enter**.
7. Insira *N* para continuar.

8. Revise o contrato de licença digitando o número apropriado para visualizar informações sobre licença. Para aceitar o contrato de licença, digite *A* e, em seguida, clique em **Enter**. Digite *N* e pressione **Enter** para continuar.
9. Selecione o **Diretório de recursos compartilhados do Installation Manager**. Consulte Visão geral dos grupos de pacotes e do diretório de recursos compartilhados para obter informações adicionais. Para mudar o diretório, insira *M* e, em seguida, **Enter**. Insira o caminho correto, em seguida, digite *N* para continuar.
10. O painel Local permite especificar o local do diretório de instalação do IBM Host On-Demand 12.0. Digite *M* para mudar o local do diretório de instalação. Insira o caminho correto e insira *N* para continuar.
11. A arquitetura do pacote é exibida ao instalar em um sistema operacional de 64 bits. Para novos grupos de pacotes, é possível mudar o modo de bits inserindo *T*: *mudar para arquitetura de bits*. Por exemplo, se a Arquitetura selecionada for exibida como 64 bits e a opção *T* for exibida para Mudar para arquitetura de 32 bits, digite *T* para alterar para a arquitetura de 32 bits.
12. Para aceitar os valores padrão ou continuar após inserir um diferente valor, digite *N* para continuar.
13. No painel de idioma, insira o número à esquerda do idioma para incluir ou remover o idioma da lista de idiomas para instalação. É possível selecionar apenas um idioma por vez ou *S* para selecionar todos os idiomas. O inglês é selecionado por padrão e é obrigatório. As opções de idioma se aplicam a todos os pacotes instalados no grupo de pacotes. Digite *N* para continuar.
14. O próximo painel exibe o menu Configurações, para os detalhes de configuração necessários pela instalação do Host On-Demand 12:
Geralmente, o menu de configuração do Host On-Demand 12 possui as entradas a seguir:
 - Publicar Informações
 - Servidor da web
 - a. Insira o número apropriado à esquerda da entrada Publicar informações para revisar as configurações. O painel Publicar informações exibe as informações a seguir:
 - *Diretório de destino de publicação* é o local em que os arquivos do Host On-Demand que os usuários acessam a partir da web estão instalados. Um valor padrão é mostrado no painel. Digite *1* para mudar o local, se necessário.
 - *Alias de publicação do Host On-Demand* é a configuração de alias do servidor da web para o diretório de publicação do Host On-Demand. Digite *A* para mudar o local, se necessário.
 - *Porta do Gerenciador de Serviços* é o número da porta no qual o gerenciador de serviços do Host On-Demand atende. Especifique *Porta do Gerenciador de Serviços*, por meio do qual os clientes Host On-Demand comunicam-se com o Gerenciador de Serviços. Essa comunicação é necessária pelas seguintes opções de implementação:
 - Usando o servidor de configuração para manter as informações de configuração de sessão (como no servidor baseado em configuração e modelos de implementação combinados, descritos em Capítulo 2, “Planejamento para Implementação”, na página 11).
 - Contagem de Uso de Licença (consulte Uso de Licença na ajuda on-line)

Porta 8999 é a porta padrão para Host On-Demand. Verifique com seu administrador do sistema para ver se essa porta está ocupada. Se estiver

em uso, será possível mudar a porta durante ou após a instalação. Para obter informações adicionais sobre como alterar a porta do Gerenciador de Serviços, consulte Alterando a porta de configuração do Gerenciador de Serviços na ajuda on-line.

Insira o número associado a qualquer uma dessas opções para mudar as respectivas configurações. Consulte as opções restantes na tela para navegar.

- b. Insira o número apropriado à esquerda do servidor da web para revisar suas configurações.
 - 1) O painel do servidor da web exibe as opções a seguir. É necessário selecionar a opção de servidor da web apropriada para seu requisito:
 - **Sem servidor da web:** selecione ao configurar o servidor da web manualmente ou quando não houver servidor da web. Isso é recomendado para servidores da web como IPlanet, Lotus Domino. Entre em contato com o administrador do servidor da web ou consulte a documentação do servidor da web para obter detalhes.

Nota: Selecione *Sem servidor da web* para instalações z/OS, porque o servidor da web não pode ser detectado e deve ser configurado manualmente.
 - **Selecionar na lista de servidores da web detectados:** para selecionar um servidor da web selecionado, selecione esta opção e depois o servidor da web que foi detectado.
 - **Selecionar manualmente o servidor da web específico:** selecione esta opção quando um IBM HTTP Server 8.5 ou um servidor da web Apache 2.2 está instalado, mas não detectado. É necessário inserir o caminho completo para o arquivo httpd.conf no diretório de instalação do servidor da web.
 - 2) Insira o número associado à opção necessária para mudar as respectivas configurações. Consulte as opções na tela para navegar. Insira *N* para continuar.
- c. Se o programa de instalação detectar o IBM WebSphere Application Server em seu sistema, o próximo painel acessado usando a guia Servidor de aplicativos se deseja configurar o servlet de configuração do Host On-Demand no WebSphere Application Server. Se os usuários executarem o Host On-Demand por meio de um firewall, isso eliminará a necessidade de abrir uma porta extra para comunicações do cliente com o Gerenciador de Serviços do Host On-Demand. Consulte "Instalando o Servlet de Configuração" na página 60 para obter mais informações.
 - Se você digitar o número ou letra que aparecer à esquerda da questão, o IBM Installation Manager exibirá uma lista das versões dos servidores de aplicativos, seus perfis e servidores detectados, solicitando que os usuários escolham a partir deles. O programa de instalação implementa automaticamente o servlet de configuração no servidor de aplicativos da web que designar e configura seus clientes para acessarem o Gerenciador de Serviços por meio desse servlet.
 - Se continuar sem escolher configurar o servlet, a instalação não configurará o servlet de configuração. Os clientes podem acessar o Gerenciador de Serviços diretamente na *porta 8999* (ou uma porta alternativa que você tenha especificado).

Nota:

- O Websphere Application Server é detectado se tiver sido instalado pelo mesmo programa IBM Installation Manager no sistema. As versões que podem ser detectadas são Websphere Application Server V8.0 e Websphere Application Server V8.5.
 - Um servidor com a segurança administrativa ativada não é suportado para configuração de servlet durante a instalação.
15. O próximo painel é o painel de resumo. Revise suas seleções antes de continuar com a instalação.
 16. Para gerar um arquivo de resposta, insira *G*: para gerar um arquivo de resposta de instalação.
 17. Insira o nome do arquivo de resposta e use *.xml* como a extensão do arquivo. Os arquivos de resposta são arquivos XML.
 18. Inclua um local de diretório ao inserir o nome do arquivo de resposta para salvar o arquivo em um local diferente.
 19. Insira *I* para iniciar a instalação.
 20. Quando a instalação for concluída, insira *F*: para concluir.
 21. Insira *X* para sair do Installation Manager.

Instalando o Assistente de Implementação no Modo do Console

O Deployment Wizard é instalado automaticamente como parte da instalação do servidor Host On-Demand para Windows. Também está disponível separadamente para os clientes que não desejam instalar o servidor Host On-Demand inteiro para Windows. Os usuários podem selecionar apenas a opção Assistente de Implementação durante a instalação.

Consulte “Instalando o Modo de Console” na página 53 para obter mais detalhes.

Instalando o Host Access Toolkit no Modo do Console

O Host Access Toolkit é instalado automaticamente como parte da instalação de servidor do Host On-Demand do Windows. Também está disponível separadamente para os clientes que não desejam instalar o servidor Host On-Demand inteiro para Windows. Os usuários podem selecionar apenas a opção Host Access Toolkit durante a instalação.

Consulte “Instalando o Modo de Console” na página 53 para obter mais detalhes.

Instalando no modo silencioso

Instalar o Host On-Demand em modo silencioso permite usar um script para a instalação. É necessário criar um arquivo de resposta primeiro antes de iniciar o Installation Manager usando o arquivo de resposta.

Para obter informações sobre instalar pacotes silenciosamente usando o Installation Manager versão V1.8.3, consulte os tópicos a seguir no Centro de Informações do Installation Manager:

- Roteiros de Instalação Silenciosa
- Argumentos da linha de comandos do Installation Manager para modo silencioso

Procedimento de instalação

Esta seção contém instruções de instalação do HOD em Modo Silencioso.

Execute as tarefas a seguir para instalar o HOD em Modo Silencioso:

1. Para criar um arquivo de resposta, registre um arquivo de resposta usando o IBM Installation Manager no modo do assistente em uma máquina em que a GUI esteja disponível com a opção *-record*. Para obter mais detalhes, consulte Registrar um arquivo de resposta com o Installation Manager. Por exemplo, no Windows, o registro de um arquivo de resposta é exibido como:

```
C:\Program Files
(x86)\IBM\Installation Manager\eclipse>IBMIM.exe
-record e:\recordResponse.xml
```

2. Se necessário, abra o arquivo XML gerado para visualizar e editar preferências. Para obter detalhes no arquivo, consulte Comandos de arquivo de resposta silencioso do Installation Manager.
3. Para executar a instalação silenciosa usando o arquivo de resposta gerado, use o utilitário de linha de comandos *imcl* fornecido pelo IBM Installation Manager. Os exemplos em diferentes sistemas operacionais estão listados abaixo:

- Windows:

```
imcl.exe input response_file -log log_file
```
- Linux, UNIX, IBM i, IBM z/OS e sistema operacional X

```
./imcl input response_file -log log_file
```

Para obter mais detalhes, consulte Instalando um pacote silenciosamente usando um arquivo de resposta.

Nota:

- É recomendado evitar o uso do parâmetro *-skipInstall* ao registrar um arquivo de resposta para instalação do Host On-Demand.
- Se um servidor da web, um servidor de aplicativos ou ambos forem configurados pelo Host On-Demand durante a instalação silenciosa, será necessário registrar o arquivo de resposta em uma configuração de software semelhante para que as preferências do usuário e parâmetros de software sejam registrados no arquivo de resposta apropriadamente. Por exemplo, se o HTTP Server V8.5 for configurado, é recomendado que os parâmetros a seguir correspondam para melhores resultados:

- A versão de servidor HTTP
- O caminho do local de instalação do servidor HTTP
- O caminho do local do arquivo httpd.conf no servidor HTTP

Da mesma forma, para uma instalação silenciosa em um ambiente em que o Websphere Application Server está localizado, registre o arquivo de resposta em um sistema em que uma configuração semelhante do Websphere Application Server está disponível.

Se um arquivo de resposta registrado em um ambiente em que o Websphere Application Server não está instalado, é recomendado que seja usado em ambientes em que o Websphere Application Server não está instalado.

- É recomendado e útil manter arquivos de resposta separados para diferentes cenários de implementação.
- É necessário registrar o arquivo de resposta na mesma plataforma de sistema operacional em que o Host On-demand será instalado. Por

exemplo, para uma instalação silenciosa no Linux, registre o arquivo de resposta no Linux. É útil manter arquivos de resposta separados para diferentes sistemas operacionais.

- Os pré-requisitos para o console ou o modo GUI da instalação (conforme aplicável) são relevantes no modo de instalação silenciosa também. Eles incluem (mas não se limitam a) o seguinte:
 - O usuário que efetuou login deve ter os privilégios de administrador.
 - O Installation Manager deve ter sido instalado no modo de Administrador.
 - O Installation Manager V1.8.3 ou superior está instalado para instalar o Host On-Demand. No caso em que a segurança administrativa está ativada no Websphere Application Server, a configuração do Servlet de configuração do Host On-demand não é suportada durante a instalação. É necessário configurá-la manualmente.

Instalando o Servlet de Configuração

Durante a instalação do Host On-Demand, é possível escolher ter o servlet de configuração instalado e configurado no i/OS, OS/400, Windows, AIX, Linux e Solaris para IBM Application Server.



Todos os servidores Web e mecanismos servlet são configurados de maneiras diferentes. Verifique seu servidor Web e a documentação do mecanismo servlet para obter detalhes da configuração do servlet em seu sistema operacional.

Será necessário a instalação do servlet de configuração, apenas se ambas as instruções a seguir forem verdadeiras para a implementação do Host On-Demand:

- Planeje configurar o Host On-Demand, para que a comunicação do cliente com o Gerenciador de Serviços seja necessária (como nos modelos de implementação baseados e combinados no servidor de configuração, se você ativar a Contagem de Uso de Licença ou se utilizar o Redirecionador).
- Um firewall protege o(s) servidor(es) no(s) qual(is) você pretende manter informações de configuração de sessão e não deseja abrir uma porta nesse firewall para fornecer acesso aos clientes externos para o Gerenciador de Serviços.

Por padrão, os clientes Host On-Demand utilizam a porta 8999 para acessar informações de configuração a partir do Gerenciador de Serviços. Se um dos clientes estiver fora do firewall, o administrador do firewall precisará abrir a porta 8999, interna e externamente. No entanto, você pode evitar abrir esta porta personalizando os clientes para utilizarem o servlet de configuração para acessar as informações de configuração.

Implementando o Servlet no WebSphere Application Server

Durante a instalação do Host On Demand no Windows, AIX, Linux e Solaris, o utilitário de instalação procura no sistema uma instância do WebSphere Application Server. Se ele detectar uma instância, o utilitário de instalação poderá instalar e configurar automaticamente o servlet de configuração no WebSphere Application Server versões 5.1, 6.0, 6.1 e 7.0.

Para plataformas que fornecem um programa de instalação como o System z e outros, será necessário instalar manualmente o servlet de configuração. Consulte a documentação do WebSphere Application Server para obter as etapas na instalação de aplicativos corporativos. Também é possível acessar <http://www.ibm.com/>

software/webservers/ e navegar para a página de suporte do WebSphere Application Server, na qual é possível localizar um link para a documentação da sua versão.

O arquivo EAR do servlet de configuração do Host On-Demand, `cfgservlet.ear`, está localizado no diretório `lib` de instalação do Host On-Demand.



Para WebSphere Application Server 5: Após você salvar as definições de implementação no console administrativo, é preciso iniciar o servlet de configuração do Host On-Demand na janela Aplicativos Corporativos do WebSphere Application Server. Em seguida, vá para a janela Ambiente e selecione Atualizar Plug-in do Servidor Web.

Após o servlet de configuração ser instalado, é possível configurar os clientes para usarem o servlet de configuração em vez de acessarem diretamente o Gerenciador de Serviços. Você pode utilizar o Deployment Wizard para construir as páginas do cliente HTML. O assistente define os parâmetros de applet no HTML baseado na entrada, assim, você não precisa aprender a sintaxe e os valores de parâmetros válidos. A IBM recomenda utilizar o Deployment Wizard para definir o parâmetro `ConfigServerURL` no HTML do cliente para `HODConfig/HODConfig/hod`.

Para obter informações adicionais a respeito dos parâmetros, configuração e exemplos do servlet de configuração, consulte Configurando o Servlet de Configuração na ajuda on-line.

Capítulo 7. Desinstalando o Servidor Host On-Demand

É possível usar a GUI do Installation Manager para desinstalar o Host On-Demand Versão 12. Siga as etapas abaixo para a desinstalação:

1. Pare todos os aplicativos relacionados ao Host On-Demand (por exemplo, Assistente de Implementação e Gerenciador de Serviços do IBM Host On-Demand).
2. Inicie o Gerenciador de Instalação. Clique em **Desinstalar**.
3. Selecione IBM® Host On-Demand e a versão apropriada e clique em **Avançar**.
4. Revise as informações do resumo. Clique em **Desinstalar**.
 - Se a desinstalação for bem-sucedida, o programa exibirá uma mensagem que indica o sucesso.
 - Se a desinstalação não for bem-sucedida, clique em **Visualizar log** para solucionar o problema.
5. Clique em **Concluir**.
6. Clique em **Arquivo > Sair** para fechar o Installation Manager.

Desinstalando o Host On-Demand usando o modo de console do Installation Manager

É possível usar o modo de console para desinstalar pacotes. Para desinstalar, o usuário deve ser o administrador ou efetuar login com privilégio de administrador.

Execute as etapas a seguir para desinstalar o HOD no modo do console do Installation Manager:

1. Feche todos os programas associados à instalação do Host On-Demand. Por exemplo, o Assistente de Implementação e o Gerenciador de Serviços do IBM Host On-Demand.
2. Digite o comando
: imcl -c

e pressione **Enter**
3. Insira **5** para continuar a desinstalação.
4. Digite o número que aparece à esquerda do grupo de pacotes do Host On-Demand 12.0. Pressione **Enter**.
5. Revise os detalhes do grupo de pacotes do Host On-Demand 12.0 que deve ser desinstalado. Digite **N** para *Avançar* ou pressione **Enter**. **N** é a seleção padrão.
6. Selecione o pacote Host On-Demand digitando o número que aparece à esquerda do pacote Host On-Demand 12.0. Pressione **Enter**. Insira **N** para *Avançar*.
7. Confirme o pacote a ser desinstalado. Digite **U** para *Desinstalar* e pressione **Enter**. Este painel também fornece uma opção para criar um arquivo de resposta. Pressione **G** e **Enter** para continuar a criar um arquivo de resposta. Isso inicia a desinstalação.
8. No próximo prompt, pressione **F** para *Concluir*.

Parte 3. Configurando o Host On-Demand

Capítulo 8. Configurando os clientes de emulador do Host On Demand

Depois de instalar o Host On-Demand, você precisará criar arquivos HTML e configurar sessões do Host On-Demand para os usuários.



O Host On-Demand fornece um arquivo HTML de amostra de sessões de emuladores 3270, 5250, VT e FTP prontas para uso pré-configurado com cliente de download e componentes de detecção automática Java. Essas sessões utilizam o modelo de configuração com base em HTML e são fornecidas para permitir que você tenha o Host On-Demand ativo e em execução e acesse seus sistemas host rapidamente. Para utilizar sessões de emuladores, siga as etapas a seguir:

1. Localize o arquivo `hodclients.zip` no diretório `your_publish_directory\samples\html`, em que `your_publish_directory` é o nome do diretório de publicação do Host On-Demand.
2. Verifique se o arquivo `hodclients.zip` criado pelo Assistente de Implementação está localizado no diretório no qual você deseja descompactar arquivos ZIP (seja no diretório de publicação do Host On-Demand ou em um diretório de publicação com finalidade especial). Caso contrário, copie o arquivo `.zip` para aquele diretório.
3. Utilize a ferramenta DWunzip para descompactar o conteúdo do `hodclients.zip` em seu diretório de publicação. Consulte a seção Utilizando o DWunzip para obter informações adicionais sobre como utilizar essa ferramenta.
4. Utilize seu navegador para apontar para `hodclients.html` em seu navegador da Web, por exemplo, `http://host/alias/hodclients.html`.
5. Clique com o botão direito do mouse no ícone da sessão apropriada e selecione Propriedades para abrir as propriedades da sessão. Preencha o endereço de destino, a porta e quaisquer outras propriedades corretas de conexão de seu sistema host. Clique em OK.
6. Dê um clique duplo no ícone da sessão para iniciá-la.

Você pode utilizar o Deployment Wizard para personalizar os arquivos HTML. Para obter informações adicionais, consulte o "Utilizando o Deployment Wizard" na página 69.

Criando Arquivos HTML do Host On-Demand

A melhor maneira de criar e configurar os arquivos HTML para o Host On-Demand é utilizar o Deployment Wizard. O Deployment Wizard permite criar facilmente arquivos HTML personalizados que contêm todos os recursos do Host On-Demand ajustados ao seu ambiente. Segue uma lista de alguns dos diversos recursos que podem ser configurados utilizando o Deployment Wizard:

- **Modelos de configuração.** Os modelos de configuração definem a abordagem de alto nível que você deseja seguir em relação ao lugar em que define suas sessões e o lugar em que as preferências do usuário são mantidas. Para obter informações adicionais sobre modelos de configuração, consulte o Capítulo 2, "Planejamento para Implementação", na página 11.
- **Pré-carregamentos.** O Host On-Demand é executado como um applet e deve transferir por download o código para as máquinas dos usuários. Por padrão, o cliente Host On-Demand faz os downloads de todos os componentes, mas você pode reduzir o tamanho do download removendo os componentes desnecessários.

- **Cliente armazenado em cache, Cliente Web Start ou Cliente de download.** Os clientes armazenados em cache mantêm o código na primeira vez que o usuário acessa o arquivo HTML e o armazena nas máquinas dos usuários. O cliente Web Start armazena o código do cliente armazenado em cache como o Cliente Armazenado em Cache, mas além disso, permite executar o Host On-Demand sem um navegador. Os clientes de download transferem por download os arquivos de applet necessários toda vez que os usuários acessam os arquivos HTML.
- **Aparência da página da Web (modelos HTML personalizados).** Você pode configurar facilmente um modelo que o Deployment Wizard utilizará para gerar os arquivos HTML. Esse recurso facilita a inclusão de seu próprio plano de fundo, banners, etc.
- **Opções do Cliente Armazenado em Cache/Web Start.** Ao executar o cliente armazenado em cache ou o cliente Web Start, é necessário fazer o upgrade do código quando versões mais recentes do cliente estão disponíveis. É possível usar várias opções do Assistente de Implementação para controlar os upgrades.
- **Localização da instalação do Host On-Demand (base de código).** Normalmente, os arquivos do Deployment Wizard são colocados no diretório de publicação do servidor Host On-Demand. No entanto, algumas vezes pode ser útil colocar esses arquivos em uma localização que seja independente do servidor Host On-Demand para que, por exemplo, possam receber diferentes controles de segurança ou tornar mais fáceis os upgrades do servidor Host On-Demand.
- **WebSphere Portal.** O WebSphere Portal fornece uma estrutura para conectar extensões de conteúdo conhecidas como portlets a um Web site. Os portlets são aplicativos que organizam o conteúdo de diferentes origens e o exibem em um único arquivo HTML em uma janela do navegador. Os arquivos HTML que são utilizados para ativar as sessões do Host On-Demand podem ser implementados como portlets, permitindo que os usuários acessem o Host On-Demand através de uma interface do portal.
- **Logon do domínio do Windows.** Se os usuários tiverem efetuado logon em um domínio do Windows, esta opção efetuará logon dos usuários automaticamente no Host On-Demand utilizando os nomes de usuário do Windows. Esta opção está disponível apenas ao utilizar o modelo baseado no servidor de configuração no Deployment Wizard.
- **APIs do Gerenciador de Sessão.** O Gerenciador de Sessão do Host On-Demand fornece APIs JavaScript para gerenciar sessões do host e interações baseadas em texto com sessões do host. Essas APIs fornecem suporte para incorporar sessões do host a uma página da Web utilizando o JavaScript e podem ser ativadas com o Deployment Wizard.



Para usar o cliente Web Start, é necessário usar o Assistente de Implementação. Os arquivos predefinidos para esse tipo de cliente não são fornecidos.

Configurando Sessões do Host On-Demand

Além de configurar os arquivos HTML, é necessário definir sessões para os usuários. Se estiver utilizando o modelo baseado em HTML, você irá configurar as sessões no Deployment Wizard ao mesmo tempo em que irá criar os arquivos HTML. Do contrário, se estiver utilizando o modelo baseado no servidor de configuração ou o modelo combinado, ou estiver utilizando os clientes predefinidos, você precisará criar grupos, usuários e sessões no servidor de configuração utilizando um dos clientes de administração.

Há uma faixa completa de opções disponíveis ao configurar as sessões, independentemente se precisar utilizar o Deployment Wizard ou um dos clientes de administração:

- **Propriedades da sessão.** Todas as propriedades da sessão podem ser configuradas, incluindo informações de conexão, segurança, etc. Cada um dos campos pode ser bloqueado para evitar que usuários os atualizem.
- **Opções de tempo de execução.** Ao configurar uma sessão, você pode lançar a sessão e configurar recursos, como tamanho e posicionamento da sessão, cores, personalização da barra de ferramentas e macros. Você pode configurar opções de tempo de execução no Deployment Wizard e o cliente de administração completo.
- **Desativando funções do usuário.** Você pode desativar quase todas as funções que os usuários normalmente recebem como parte de sua sessão Host On-Demand, como incluir em favoritos, criar ou executar macros, etc.

Utilizando o Deployment Wizard

O Assistente de Implementação é executado em plataformas Windows e Linux. Para iniciar o Deployment Wizard, selecione um dos seguintes caminhos:

- Se você instalou automaticamente o Assistente de Implementação como parte do servidor Host On Demand do Windows, acesse **Iniciar > Programas > IBM Host On Demand > Administração > Assistente de Implementação**.

A janela Bem-vindo ao Deployment Wizard é exibida.

O Deployment Wizard orienta-o em relação às opções de configuração e fornece ajuda abrangente para os recursos. Depois de concluir a seleção dos recursos, o Deployment Wizard cria os arquivos HTML e de suporte. Esses arquivos precisam ser colocados no servidor Host On-Demand em um diretório conhecido do servidor Web; normalmente, esse diretório é o diretório de publicação do servidor Host On-Demand.

Distribuindo a Saída do Deployment Wizard para o Seu Servidor Host On-Demand

Se seu servidor Host On-Demand estiver em uma plataforma Windows ou IBM System i, será possível gravar seus arquivos HTML e de configuração do Assistente de Implementação diretamente em seu diretório de publicação do servidor Host On-Demand. Na tela final do Deployment Wizard, você pode selecionar o local para gravar os arquivos gerados. Você pode selecionar qualquer local ou unidade de rede acessível pela máquina na qual o Deployment Wizard estiver sendo executado. Nesse caso, você direcionaria a saída do Deployment Wizard para um diretório de publicação no servidor Host On-Demand e especificaria um formato de saída *HTML*. Supondo que você já tenha definido as sessões, a página HTML estará pronta para ser acessada pelos usuários.

Do contrário, se o Deployment Wizard não puder gravar diretamente no servidor Host On-Demand, você deverá selecionar a opção para o Deployment Wizard gerar um arquivo zip para o formato de saída. O Deployment Wizard produzirá um único arquivo zip contendo todos os arquivos HTML e de suporte. Você precisará mover o arquivo zip para o servidor Host On-Demand e utilizar DWunzip para extrair o arquivo zip no diretório de publicação desejado. Supondo que você já tenha definido as sessões, a página HTML estará pronta para ser acessada pelos usuários.

Capítulo 9. Utilizando Clientes de Novos Usuários e de Administração do Host On-Demand

O Host On-Demand fornece vários clientes predefinidos para administrar o Host On-Demand e criar novas contas de usuário. Antes de acessar um cliente de emulador ou um cliente do Database On-Demand que usa os modelos de implementação baseados no servidor de configuração ou combinados, é necessário incluir usuários e configurar sessões para eles com um dos clientes de administração ou de administração completa.

Carregando Clientes de Administração e de Novos Usuários

Para carregar um cliente de administração ou de novos usuários, proceda de uma das seguintes formas:

- Especifique a URL completa do arquivo HTML em seu navegador:

`http://server_name/hod_alias/client_name.html`

em que *server_name* é o nome do host ou endereço IP do servidor Host On-Demand, *hod_alias* é o alias (ou caminho) do diretório de publicação e *client_name* é o nome do arquivo HTML do cliente de administração ou do novo usuário. Por exemplo, você pode fazer o download da versão em cache do cliente de administração a partir do servidor Web, especificando uma URL, tal como a seguinte:

`http://host.yourcompany.com/hod/HODAdminCached.html`

Para efetuar logon como o administrador na primeira vez após a instalação inicial:

1. Digite o ID do usuário padrão: admin.
 2. Digite a senha padrão: password.
 3. Clique em Efetuar Logon.
- Carregue o arquivo HODMain_xx.html, em que xx é o sufixo de seu idioma com duas letras, no seu navegador, para exibir os links para todos os clientes de administração e de novos usuários disponíveis, além de outros clientes predefinidos. HODMain_xx.html está localizado no diretório de publicação.

Clientes de administração

Os clientes de administração permitem que você execute as seguintes tarefas para os dados armazenados no servidor de configuração:

- Gerenciar usuários, grupos e sessões
- Configurar, gerenciar e rastrear o serviço do Redirecionador
- Configurar o Database On-Demand
- Ativar segurança
- Exibir rastreamento e registros de mensagens
- Desativar funções para usuários finais

Os clientes de administração executam em todas as plataformas do cliente Host On-Demand, exceto no sistema operacional Macintosh. Se você estiver criando arquivos HTML no Assistente de Implementação usando os modelos baseados no servidor de configuração ou combinados, é necessário configurar sessões no

servidor de configuração usando um cliente de administração. Consulte Etapas da Configuração Básica na ajuda on-line para obter informações mais detalhadas sobre como configurar o servidor de configuração do Host On-Demand.

O Host On-Demand fornece os seguintes clientes de administração e administração completa predefinidos:

Cliente de administração (HODAdmin.html)

Carrega a versão de download do cliente de administração.

Cliente de administração em cache (HODAdminCached.html)

Carrega a versão em cache do cliente de Administração. A vantagem de utilizar este cliente é que ele pode ser armazenado em cache juntamente com o cliente armazenado em cache no navegador.



Para marcar o cliente de Administração em cache, é necessário criar manualmente o marcador. Ele deverá apontar para o HODAdminCached.html, para que o Host On-Demand possa comparar a versão em cache com a versão do servidor. Isso permite que o Host On-Demand reconheça e notifique o usuário que uma versão mais recente do cliente de Administração em cache está disponível no servidor.

Cliente de administração em cache com determinação de problemas (HODAdminCachedDebug.html)¹

Carrega o cliente de Administração em um ambiente em cache com determinação de problemas (registro e rastreamento de sessão) ativado.

Cliente de Administração Completa (HODAdminFull.html)²

Carrega a versão de download do cliente de Administração completa. O cliente de administração completa fornece ao administrador a capacidade adicional para iniciar sessões para configurar as propriedades de tempo de execução. No entanto, o tamanho do download do cliente de administração completa é maior que o tamanho do download do cliente de administração.

Cliente de Administração Completa em cache (HODAdminCachedFull.html)²

Carrega a versão em cache do cliente de Administração completa. Como a versão em cache do cliente de Administração regular, este cliente pode ser armazenado em cache juntamente com o cliente armazenado em cache no navegador.

Cliente de Administração Completa em cache com determinação de problemas (HODAdminCachedDebugFull.html)^{1, 2}

Carrega a versão em cache do cliente de Administração Completa com determinação de problemas (registro e rastreamento de sessão) ativado.

Notas:

1. Utilize os clientes de identificação de problemas apenas se você estiver utilizando o Suporte para resolver um problema com sua instalação do Host On-Demand.
2. O cliente de Administração completa é o cliente de Administração com Iniciar Sessão ativado.
3. Se você usar um navegador ativado para Java, será necessário usar o Painel de Controle Java para remover o cliente de Administração em cache. Para obter instruções, consulte Usando o plug-in Java na ajuda on-line.

Utilitário do Diretório

O Utilitário de diretório é um aplicativo Java que o administrador pode usar para gerenciar informações de configuração de usuário, grupo ou sessão. Essas

informações são armazenadas no data store padrão do Host On-Demand ou em um diretório LDAP. Esse utilitário é útil apenas no ambiente no qual o modelo baseado no Servidor de Configuração está em uso. O Utilitário de Diretório permite incluir, excluir ou atualizar um grande número de usuários, grupos ou sessões em um ambiente de modo em lote em vez de usar o cliente de Administração. O Utilitário de diretório lê um arquivo XML ASCII que contém as ações a seguir a serem executadas em usuários, grupos ou sessões definidos para o servidor de configuração:

- Incluir, atualizar e excluir grupos
- Incluir, atualizar e excluir usuários de grupos
- Incluir, atualizar e excluir sessões de usuários ou grupos
- Listar usuários e grupos existentes nos arquivos de saída, como produtos de pesquisas exclusivas
- Listar usuários e grupos existentes nos arquivos de saída que podem ser reutilizados como entrada



Pesquisas executadas com a ação de lista são baseadas no usuário (retornando informações específicas do usuário) ou baseadas no grupo (retornando informações específicas do grupo). Os ambientes LDAP, no entanto, suportam somente pesquisas baseada no usuário.

Para obter informações adicionais, consulte Usando o Directory Utility na ajuda on-line.

Cientes de Novos Usuários

Se o administrador tiver ativado Permitir que Usuários Criem Contas na janela Usuários/Grupos, os usuários poderão utilizar os clientes predefinidos do novo usuário para criar novas contas. Veja o tópico Permitindo que os usuários criem contas na ajuda on-line para obter mais informações sobre esse cliente.

Os seguintes clientes de novos usuários são fornecidos com o Host On-Demand:

Cliente de novos usuários (NewUser.html)

Carrega a versão de download do cliente de Novo usuário.

Cliente de novos usuários em cache (NewUserCached.html)

Carrega o cliente de Novo Usuário em um ambiente em cache.

Cliente de novos usuários com determinação de problemas (NewUserCachedDebug.html)¹

Carrega o cliente de Novo Usuário em um ambiente em cache com determinação de problemas (registro e rastreamento de sessão).

Nota: Utilize os clientes de determinação de problemas apenas se você estiver trabalhando com o Suporte IBM para resolver um problema com sua instalação do Host On-Demand.

Capítulo 10. Utilizando os Clientes de Emulador do Host On-Demand

Este capítulo discute os problemas que você precisa estar ciente ao configurar e utilizar os clientes de emulador de terminal do Host On-Demand.

- “Carregando Clientes de Emulador” descreve como acessar os clientes de emulador do Host On-Demand.
- “Selecionando o cliente apropriado” na página 76 discute como decidir qual cliente é o melhor para as suas necessidades.
- “Clientes em Cache” na página 77 discute como usar clientes em cache, incluindo como instalar e removê-los, implementá-los por meio da Internet, suporte para Windows e Mac OS X e resolução de problemas.
- “Cliente Web Start” na página 85 discute como utilizar o cliente Web Start, incluindo sua instalação e remoção, a configuração do navegador da Web, a utilização do Web Start com usuários restritos do Windows e o upgrade.
- “Clientes de Download” na página 89 discute como utilizar clientes de download, incluindo a instalação e o carregamento deles depois de transferir por download um cliente armazenado em cache ou um cliente Web Start.
- “Clientes de Emulador Predefinidos” na página 90 descreve os clientes de emulador predefinidos fornecidos com o Host On-Demand.
- “Reduzindo o Tamanho do Cliente de Download” na página 91 discute estratégias para reduzir o tamanho do download dos clientes.
- “Implementando archives e classes Java fornecidos pelo cliente” na página 92 descreve como implementar Java archives e arquivos de classe em seus clientes.

Carregando Clientes de Emulador



O Host On-Demand fornece um arquivo HTML de amostra de sessões de emuladores 3270, 5250, VT e FTP prontas para uso pré-configurado com cliente de download e componentes de detecção automática Java. Essas sessões utilizam o modelo de configuração com base em HTML e são fornecidas para permitir que você tenha o Host On-Demand ativo e em execução e acesse seus sistemas host rapidamente. Para obter informações adicionais, consulte o Capítulo 8, “Configurando os clientes de emulador do Host On Demand”, na página 67.

Para carregar um cliente de emulador do Host On-Demand, um usuário inicia um navegador da Web e insere no campo Endereço a URL de um arquivo HTML do Host On-Demand. O arquivo HTML do Host On-Demand deve ser um dos seguintes:

- Um arquivo HTML que você cria com o Deployment Wizard.
- Um dos vários arquivos HTML predefinidos genéricos incluídos com o Host On-Demand.

A IBM recomenda a primeira opção. Para obter informações adicionais sobre o Deployment Wizard, consulte o tópico Deployment Wizard na ajuda on-line. Para obter informações adicionais sobre arquivos HTML predefinidos genéricos, consulte “Clientes de Emulador Predefinidos” na página 90.



Se o cliente de emulador for implementado com o modelo de implementação baseado no servidor de configuração ou combinado, será necessário incluir usuários e configurar sessões com o cliente de administração, antes de poder usar o cliente de emulador.

Para ativar arquivos HTML gerados pelo Deployment Wizard, especifique a URL completa do arquivo HTML em seu navegador:

```
http://server_name/hod_alias/client_name.html
```

em que *server_name* é o nome do host ou endereço IP do servidor Host On-Demand, *hod_alias* é o alias (ou caminho) do diretório de publicação e *client_name* é o nome de arquivo HTML do cliente. Por exemplo, se você criou um arquivo HTML no Deployment Wizard denominado 3270sessions.html, poderá fazer o download dele, especificando uma URL, tal como a seguinte:

```
http://host.yourcompany.com/hod/3270sessions.html
```

Para ativar um arquivo HTML predefinido incluído com o Host On-Demand, aponte o navegador para o arquivo HODMain_xx.html, em que *xx* é o sufixo de seu idioma com duas letras para exibir os links de todos os clientes predefinidos disponíveis. HODMain_xx.html está localizado no diretório de publicação.

Quando você acessa um cliente, um aviso de segurança aparece para notificar que o Host On-Demand foi criado pela **International Business Machines**. Os usuários devem conceder privilégios de segurança Java para esta sessão ou qualquer sessão futura clicando nos botões apropriados para que o Host On-Demand funcione corretamente.

Nota: Bloqueadores de pop-up podem impedir que as janelas de segurança Java e outras janelas de resposta sejam exibidas.

Selecionando o cliente apropriado

Os tipos de clientes Host On-Demand que você utiliza dependem de seu ambiente de computação e suas preferências pessoais.

Os clientes armazenados em cache e os clientes Web Start são armazenados localmente e carregam mais rápido do que os clientes de download (a menos que uma versão atualizada do cliente esteja sendo transferida por download a partir do servidor Web). Você pode utilizá-los igualmente bem através de conexões de rede e dial-up. Os clientes armazenados em cache e os clientes Web Start utilizam mais espaço em disco local do que os clientes de download, mas na maioria das máquinas isso não é um problema.

O cliente Web Start permite que usuários executem sessões do Host On-Demand sem um navegador. Os usuários iniciam sessões do Host On-Demand a partir do Gerenciador de Aplicativos do Java Web Start. Se um usuário fechar o desktop do Host On-Demand e houver sessões ativas em execução, ele será solicitado a se certificar de que deseja fechar todas as sessões.

Os clientes de download são geralmente utilizados em ambientes conectados pela LAN, porque as conexões de rede de alta velocidade reduzem o tempo necessário para transferi-los por download a partir do servidor Web. Não é recomendável utilizá-los através de conexões dial-up de baixa velocidade porque precisam ser transferidos através de download toda vez que são utilizados, o que leva mais tempo nessas conexões. A área de cobertura do pequeno disco de clientes de

download é especialmente bem adequada para máquinas clientes que não têm muito espaço em disco local, como máquinas NetStation.

Você pode usar clientes em cache, Web Start e de download no mesmo ambiente Host On-Demand. Consulte “Removendo o Cliente Armazenado em Cache” na página 81 para obter instruções sobre a remoção de clientes armazenados em cache.

Se você planeja usar o cliente Web Start, é necessário usar o Assistente de Implementação para gerar seu arquivo HTML. Se planeja utilizar clientes armazenados em cache ou clientes de download, a IBM recomenda que crie seus próprios clientes utilizando o Deployment Wizard em vez de um dos clientes predefinidos. Consulte “Reduzindo o Tamanho do Cliente de Download” na página 91 para obter informações adicionais.

Cientes em Cache

Um cliente armazenado em cache do Host On-Demand é qualquer cliente do Host On-Demand cujos componentes foram armazenados em cache (armazenados localmente para acesso rápido) na unidade de disco rígido de uma estação de trabalho do usuário. Quando um usuário executa pela primeira vez um cliente armazenado em cache, o código de inicialização do Host On-Demand transfere por download os componentes do cliente Host On-Demand e os armazena na unidade de disco rígido da estação de trabalho do usuário. Isso é chamado de instalação do cliente armazenado em cache.

Então, quando o usuário executa o cliente armazenado em cache, o código de inicialização do Host On-Demand transfere por download apenas um pequeno applet de inicialização a partir do servidor. O applet de inicialização por sua vez inicia o cliente Host On-Demand a partir dos componentes armazenados em cache na unidade de disco rígido.

Utilizando o cliente armazenado em cache, o usuário não precisa aguardar que os componentes do cliente Host On-Demand sejam transferidos por download, porque eles já ficam imediatamente disponíveis na unidade de disco rígido da estação de trabalho. Além disso, o cliente armazenado em cache é persistente através dos reinícios do sistema operacional e dos recarregamentos do navegador. Embora o cliente armazenado em cache tenha sido originalmente planejado para usuários com conectividade mais lenta, como linhas de telefone dial-up, nas quais a transferência por download de um applet grande levaria muito tempo, muitos clientes têm preferido utilizar o cliente armazenado em cache mesmo em linhas de alta velocidade.

Como todos os clientes Host On-Demand, o cliente armazenado em cache é iniciado (na primeira vez e subsequentemente) especificando a URL de um arquivo HTML do Host On-Demand no campo Endereço de um navegador da Web suportado. A IBM recomenda que você crie seu próprio arquivo HTML utilizando o Deployment Wizard. No entanto, é possível utilizar um dos arquivos HTML predefinidos genéricos do cliente armazenado em cache incluídos com o Host On-Demand.

O applet que inicia o cliente armazenado em cache também determina se o número da versão de qualquer componente do cliente Host On-Demand no servidor Host On-Demand é mais recente que o número de versão dos componentes correspondentes transferidos por download. Se for, então o applet fará o upgrade

do cliente armazenado em cache transferindo por download e armazenando em cache o componente mais recente a partir do servidor antes de ativar o cliente armazenado em cache.

O usuário pode então instalar vários tipos de um cliente armazenado em cache na mesma estação de trabalho. Por exemplo, um cliente de emulador, um cliente do Database On-Demand e um cliente de administração armazenados em cache poderiam ser instalados em uma única estação de trabalho. Além disso, com a versão Java do Host On Demand, o usuário pode instalar duas versões do mesmo cliente em cache: uma com determinação de problema e outra sem determinação de problema.

Instalando Clientes em Cache

Você pode instalar um cliente em cache a partir de um servidor Host On-Demand ou de uma unidade de LAN ou de DVD.

Informações instaladas para o cliente em cache

Dois tipos de informações são armazenadas na estação de trabalho do usuário quando um cliente em cache do Java está instalado:

- Componentes do Host On-Demand
Esses componentes estão no formulário de arquivos Java archive (JAR).
- Informações de controle
Essas informações incluem dados como a URL do servidor Host On-Demand e a versão de cada componente transferido por download.

Cliente em cache do Java: Várias versões do cliente em cache do Java podem existir na estação de trabalho do usuário, porque o código de inicialização do cliente em cache do Java armazena os componentes do cliente em cache em um diretório diferente do disco rígido da estação de trabalho para cada servidor a partir do qual o usuário transferiu por download um cliente em cache.

Para o cliente em cache do Java, todos os componentes do cliente transferidos por download a partir do mesmo servidor são armazenados no mesmo diretório do disco rígido do usuário. Por exemplo, se o usuário instalar um cliente de emulador do Java e um cliente do Java Database On-Demand a partir do mesmo servidor, os arquivos do componente para os dois tipos de cliente serão armazenados no mesmo diretório.

Para alguns tipos especializados de clientes em cache do Java, os componentes do cliente são armazenados no *cache permanente* do plug-in Java. Esses são os mesmos tipos de clientes armazenados em cache listados em “Limites de suporte” na página 15.

Instalando o Cliente Armazenado em Cache a partir do Servidor Host On-Demand

Para instalar o cliente armazenado em cache a partir de um servidor Host On-Demand:

1. Especifique a URL completa do arquivo HTML em seu navegador, conforme descrito em “Carregando Clientes de Emulador” na página 75.
2. Se quiser utilizar um cliente predefinido, clique no link do cliente armazenado em cache após carregar `http://server_name/hod_alias/HODMain.html`, em que *server_name* é o nome do host ou endereço IP do servidor Host On-Demand e *hod_alias* é o alias (ou caminho) do diretório de publicação.

3. O cliente armazenado em cache começa a instalação imediatamente. Uma janela mostra o progresso da instalação. A barra de progresso superior desta janela mostra o status de arquivos individuais conforme são transferidos por download, enquanto a barra de progresso inferior mostra o status da instalação global.



A janela de progresso da instalação não aparece para alguns tipos de clientes em cache do Java. Estes são os mesmos clientes em cache que estão listados em “Limites de suporte” na página 15.

4. Quando a instalação é concluída, o código de instalação ativa imediatamente o cliente em cache do Java. O usuário não precisa iniciar novamente o navegador.

Instalando o Cliente em Cache a partir de uma LAN ou DVD

Agora, alguns ou todos os usuários podem fazer download inicialmente do cliente em cache a partir de uma unidade de LAN ou de DVD. Para instalar o cliente em cache, o usuário precisa acessar a unidade de LAN ou de DVD apenas uma vez. Depois da instalação, o usuário conecta-se ao servidor do Host On-Demand normalmente.

As vantagens desse método são que os componentes do cliente armazenado em cache são instalados na estação de trabalho do usuário mais rapidamente do que seriam se tivessem de ser transferidos por download a partir do servidor da Web e que o usuário não está colocando uma carga adicional no servidor da Web ao transferir por download um conjunto inteiro de componentes do cliente armazenado em cache.

Este método é suportado na maior parte das plataformas do cliente. No entanto, vários clientes em cache do Java não suportam esse recurso. Os clientes em cache do Java que não suportam esse recurso estão listados em “Limites de suporte” na página 15.

Limitações: O arquivo HTML não pode especificar um diretório de publicação do usuário separado. (Se você especificou uma Base de Código no Deployment Wizard, o arquivo HTML não poderá ser usado para instalar o cliente em cache a partir de uma unidade de LAN ou de DVD.) Consulte o online help para obter informações adicionais sobre o diretório de publicação do usuário separado.

Etapas para o Administrador Criar a Imagem do DVD ou da LAN:

1. Utilize a janela Nome do Arquivo e Formato de Saída no Deployment Wizard para criar seus arquivos *.html personalizados (por exemplo, MyHOD.html). Se você precisar distribuir os arquivos do Deployment Wizard para outro servidor, poderá selecionar o Zip de Saída para que possa utilizar o DWunzip. Para obter informações adicionais, consulte Utilizando o DWunzip na ajuda on-line.
2. Para o cliente em cache do Java, é possível evitar ter o tipo de usuário no nome do host do servidor Host On Demand durante a instalação especificando o parâmetro HTML adicional WebServerHostname no Assistente de Implementação. Para obter informações adicionais, consulte Parâmetros HTML na ajuda on-line.
3. Depois de carregar os novos arquivos do Deployment Wizard no servidor, teste os novos arquivos para certificar-se de que funcionam conforme esperado.
4. Copie ou transfira por FTP os seguintes arquivos do diretório de publicação da instalação do servidor Host On-Demand para uma unidade de rede ou DVD (certifique-se de que tenha colocado a mesma versão do Host On-Demand na unidade de DVD ou LAN existente no servidor Host On-Demand):

- MyHOD.html
 - MyHOD.jnlp (se existir)
 - z_MyHOD.html (se existir)
 - hoddetect*.html
 - hodlogo.gif
 - hodbkgnd.gif
 - Installer.html
 - Installer2.html
 - *.jar
 - *.properties
 - *.js
5. Copie os seguintes arquivos e diretórios enquanto preserve a estrutura de diretórios:
- msgs\cached_*.properties
 - HODData\MyHOD*.*



Se esses arquivos estiverem sendo copiados de uma instalação no z/OS para uma imagem de DVD, observe que será necessário primeiramente remover a extensão de arquivo .ascii de todos os arquivos HTML, PROPERTIES, JS, JNLP e CSS. Por exemplo, um arquivo denominado *.properties.ascii deve ser copiado no DVD como *.properties.



Se você estiver usando um DVD para a instalação do cliente em cache, o DVD deverá ser distribuído com as mesmas diretrizes dos regulamentos do Contrato de Licença e de Exportação e Importação, porque ele contém tecnologia de criptografia.

Etapas para o usuário: Depois que o administrador configurar a unidade de LAN ou DVD, o usuário deverá executar as seguintes etapas para instalar o cliente em cache.

1. Prepare a máquina do cliente para a instalação fazendo o seguinte:
 - Obter acesso à unidade de LAN ou DVD.
 - Obtenha o nome e o local do arquivo HTML, como f:\myPath\MyHOD.html, que o administrador do sistema colocou na unidade de LAN ou DVD. (O arquivo HTML tem o mesmo nome e conteúdo para todos os usuários. Ele não é específico para um único usuário).
 - *Somente para o cliente em cache do Java*, localize o nome do host do servidor Host On Demand ao qual o usuário se conectará após a instalação do cliente em cache. Por exemplo, se o usuário se conectar ao `http://myHODServer/hod/MyHOD.html`, então o nome do host será myHODServer.



Para o cliente em cache do Java, o administrador do sistema pode eliminar essa etapa incluindo o parâmetro HTML WebServerHostname no arquivo HTML. Consulte Parâmetros HTML na ajuda on-line.

2. Execute o arquivo HTML:

Digite o nome e o caminho do arquivo HTML no campo de entrada de endereço do navegador, como:

```
f:/myPath/MyHOD.html
```
3. *Somente para o cliente em cache do Java*, quando solicitado pelo código de instalação, insira o nome do host do servidor Host On Demand ao qual o

usuário se conectará após a instalação do cliente em cache. Por exemplo, se o usuário ativar `http://myHODServer/hod/MyHOD.html`, então o nome do host será myHODServer.



Para o cliente em cache do Java, o administrador do sistema pode eliminar essa etapa incluindo o parâmetro HTML WebServerHostname no arquivo HTML. Consulte Parâmetros HTML na ajuda on-line.

4. Aguarde enquanto o cliente em cache do Host On-Demand é instalado a partir de uma unidade de LAN ou DVD.
5. Quando solicitado, inicie novamente o navegador e aponte-o para o arquivo HTML com o mesmo nome do servidor Host On-Demand, como:
`http://myServer/hod/MyHOD.html`

O nome do HTML no servidor Host On-Demand é igual ao nome do arquivo HTML na LAN ou DVD.

Depois de concluir essas etapas, o cliente armazenado em cache do Host On-Demand inicia da forma usual.

Removendo o Cliente Armazenado em Cache

Um método de remoção com propósito geral é discutido nas seguintes seções.

Antes de iniciar

Remover o cliente em cache significa apagar as informações que foram armazenadas no disco rígido do usuário quando o cliente em cache do Java foi instalado.

Um usuário executando a versão Java do cliente em cache tem uma versão separada do cliente em cache para cada servidor Host On Demand para o qual ele transferiu por download o cliente em cache. Para obter informações adicionais, consulte o “Informações instaladas para o cliente em cache” na página 78.

A remoção do cliente em cache do Java remove somente a versão do cliente em cache do Java transferida por download a partir do servidor que o usuário visita quando faz a remoção. Por exemplo, se o usuário visitar o servidor `http://myHODServerA/hod/HODRemove.html` para o servidor myHODServerA remover o cliente em cache do Java na estação de trabalho do usuário, somente o cliente em cache do Java que foi transferido por download a partir de myHODServerA será removido.

Finalmente, para o cliente em cache do Java, a remoção do cliente em cache remove todos os tipos de clientes em cache (como emulação, Database On-Demand e administração) associados àquela instalação.

A remoção do cliente em cache do Java de uma estação de trabalho, enquanto conectado ao servidor myHODServerA, remove o cliente em cache de emulação, o cliente em cache do Database On-Demand e o cliente em cache de administração que foram anteriormente transferidos por download a partir do servidor myHODServerA. No entanto, somente os componentes do cliente armazenado em cache transferidos por download a partir daquele servidor são removidos. Os componentes do cliente armazenado em cache de outros servidores, se houver, não serão removidos até que o usuário se conecte ao servidor e execute uma remoção.

Removendo clientes em cache do Java

O método de remoção de propósito geral remove o cliente em cache do Java. Siga estas etapas:

1. Inicie o navegador.

Inicie um navegador ativado para Java para remover um cliente em cache do Java.

2. Conecte-se ao HODMain.html no servidor Host On-Demand. Por exemplo, conecte-se à URL a seguir:

`http://myServer/HOD/HODMain.html`



Se você estiver removendo um cliente em cache do Java, é necessário conectar-se ao mesmo servidor a partir do qual instalou esse cliente para removê-lo com êxito. Para obter informações adicionais, consulte o “Antes de iniciar” na página 81.

3. Clique na seguinte entrada em Utilitários:

Remoção de Cliente no Cache

Há também uma forma alternativa e mais direta de executar essa remoção de propósito geral. Siga estas etapas:

1. Inicie o navegador.

2. Conecte-se ao HODRemove.html no servidor Host On-Demand. Por exemplo, conecte-se à URL a seguir:

`http://myServer/HOD/HODRemove.html`

Isso remove o cliente armazenado em cache.



Se você estiver removendo um cliente em cache do Java, é necessário conectar-se ao mesmo servidor a partir do qual instalou esse cliente para removê-lo com êxito. Para obter informações adicionais, consulte o “Antes de iniciar” na página 81.

Qualquer que seja o método de remoção de propósito geral usado, você será solicitado a limpar o cache do plug-in Java se tiver removido os clientes em cache do Java a seguir:

- Clientes de administração armazenados em cache
- Clientes armazenados em cache no Apple Mac OS X
- Clientes em cache de emulador com a API do Gerenciador de sessões JavaScript ativada (somente para Java Mozilla)

Uma janela aparece para notificá-lo para limpar o cache do plug-in Java. Para obter mais informações, consulte Usando o plug-in Java na ajuda on-line.

Removendo um cliente em cache compartilhado por vários usuários

Se vários usuários compartilharem um único cliente armazenado em cache e um desses usuários remover o cliente armazenado em cache, este será removido para todos os usuários. Para obter informações sobre o compartilhamento de um único cliente armazenado em cache, consulte “Suporte a clientes em cache para Windows” na página 83.

Problemas de suporte a clientes em cache ao acessar vários servidores Host On Demand

As seguintes seções detalham questões e problemas que podem surgir quando os usuários do cliente armazenado em cache acessam vários servidores Host On-Demand.

Cliente em cache do Java

Um cliente em cache do Java do Host On Demand instala uma cópia separada do código do cliente em cache para cada servidor Host On Demand que o usuário visita. No entanto, não há problema em acessar servidores em níveis de serviço diferentes. Com algumas versões do plug-in, os usuários podem precisar aumentar o tamanho do cache do Java se forem visitar muitos servidores Host On Demand.

Os problemas a seguir podem ocorrer com os clientes em cache do Java.

Problema ao usar preferências armazenadas localmente: Se estiver utilizando preferências armazenadas localmente, os arquivos HTML personalizados que são criados devem ter nomes exclusivos em sua empresa, pois os nomes de arquivos HTML são diferentes entre as preferências armazenadas localmente de diferentes sites. Utilizar nomes genéricos pode causar conflitos de preferências para os usuários.

Veja o website de suporte do Host On Demand para obter mais informações: Se você tiver problemas ao gerenciar a implementação do cliente armazenado em cache na Internet, vá para <http://www.ibm.com/software/webservers/hostondemand/support.html> para obter informações adicionais.

Suporte a clientes em cache para Windows

Em uma máquina Windows de multiusuário executando o sistema operacional Windows 7, Windows 8, Windows 10 ou Windows 2012, os usuários podem fazer download de sua própria versão independente do cliente em cache:

- Qualquer navegador suportado com um plug-in Java

Se a API JavaScript estiver ativada, o cliente em cache não poderá ser compartilhado para os navegadores Mozilla Java devido a uma limitação técnica.

Alternativamente, é possível adicionar os seguintes parâmetros utilizando a seleção de parâmetros HTML da janela Opções Avançadas do Deployment Wizard:

- `ShareCachedClient`: permite que os usuários compartilhem uma única instância do cliente armazenado em cache
- `SharedCachedDirectory`: permite que você especifique a localização do diretório em que o cliente armazenado em cache deve ser instalado

Quando o cliente armazenado em cache é compartilhado, mas você não especifica um diretório, ele é instalado no diretório padrão `\Documents and Settings\All Users\IBMHOD`. Se você especificar um diretório, por exemplo, `SharedCachedDirectory=c:\ibm`, o cliente armazenado em cache do Host On-Demand anexará `IBMHOD\HODCC` nessa cadeia e será instalado nessa nova localização, por exemplo, `c:\ibm\IBMHOD\HODCC`. Um administrador ou usuário avançado deve criar o diretório de instalação manualmente ou executar a primeira instalação do cliente armazenado em cache compartilhado. Em ambos os casos, o administrador ou usuário avançado deve alterar as definições de segurança para esse diretório para que os usuários restritos tenha acesso à Leitura, Modificação e Gravação. O Administrador pode alterar as definições de segurança e, em seguida, transferir por download o cliente armazenado em cache para o

diretório ou transferir por download o cliente armazenado em cache compartilhado para o diretório e, em seguida, alterar as definições de segurança. Se as definições de segurança não forem atualizadas e um usuário restrito tentar instalar o cliente armazenado em cache compartilhado, ele receberá uma mensagem de erro indicando que pode haver um problema com o sistema de arquivos e não conseguirá utilizar ou atualizar o cliente armazenado em cache.

Depois do administrador ou usuário avançado alterar as definições de segurança, um usuário restrito poderá efetuar logon no Windows e instalar o cliente armazenado em cache compartilhado ou utilizar (ou atualizar) uma versão anteriormente instalada desse cliente. Outros usuários restritos podem efetuar logon no Windows e utilizar o cliente armazenado em cache sem ter que fazer o download dele novamente no servidor Host On-Demand. Eles também podem efetuar upgrade do cliente armazenado em cache compartilhado, se necessário.

Se você não quiser que os usuários restritos compartilhem o cliente armazenado em cache, uma instância separada do cliente armazenado em cache será transferida através de download para o diretório de cada usuário restrito.

Se um administrador ou usuário avançado transferir por download a versão anterior do cliente armazenado em cache e você quiser permitir que usuários restritos a acessem, o administrador ou usuário avançado deverá utilizar o HODRemove.html para remover a versão anterior do cliente armazenado em cache e, em seguida, alterar as definições de segurança para o diretório do cliente armazenado em cache compartilhado para Leitura, Modificação e Gravação para usuários restritos, conforme descrito acima.

Para obter informações sobre a remoção de um cliente armazenado em cache compartilhado, consulte “Removendo um cliente em cache compartilhado por vários usuários” na página 82.

Suporte a clientes em cache para Mac OS X (somente clientes Java)

Os clientes armazenados em cache têm as seguintes limitações no Mac OS X:

- O temporário das atualizações do Host On-Demand é gerenciado em uma base por servidor.
- O pré-carregamento de clientes em cache a partir de uma unidade de DVD ou LAN não atende a nenhuma função. Quando o navegador é redirecionado para o Web site real, o plug-in considera ser um servidor Web distinto e o cliente é armazenado em cache novamente.
- O Host On-Demand é executado como um applet e deve fazer o download do código para as máquinas dos usuários. O cliente Host On-Demand transfere por download todos os componentes, mas você pode reduzir o tamanho do download removendo os componentes desnecessários. No Mac OS X, não é possível instalar componentes adicionais após o download inicial.
- Os arquivos Java do Host On Demand usados para executar o cliente em cache do Host On Demand em um navegador da web ativado para Java são armazenados no cache do Java Runtime Environment (JRE). Para remover o cliente em cache no Mac OS X, é necessário usar o Painel de Controle do Java para limpar o cache do JRE. Para obter instruções, consulte Usando o plug-in Java na ajuda on-line.
- Ao executar o cliente armazenado em cache, é necessário efetuar upgrade do código quando versões mais recentes do cliente estão disponíveis. Existe uma

série de opções do Deployment Wizard que permitem controlar a ocorrência de upgrades. Essas opções não estão disponíveis no Mac OS X.



As melhorias do cliente em cache do Java não se aplicam ao cliente em cache do Java no Mac OS X. Para obter informações adicionais, consulte o “Limites de suporte” na página 15.

Resolução de Problemas de Clientes em Cache

Se achar que não pode carregar o cliente armazenado em cache, siga as sugestões sobre resolução de problemas fornecidas a seguir.

Microsoft Internet Explorer 11.0

Depois de fazer upgrade de seu navegador para o Microsoft Internet Explorer 11.0, você poderá receber exceções de segurança no console Java. Quando você instala o Cliente Armazenado em Cache, diversos arquivos são armazenados na estrutura de diretórios do navegador. Quando você fizer upgrade do Internet Explorer para a Versão 11.0, o navegador não saberá mais sobre os arquivos CAB que contêm o código em cache do Host On Demand. Como o navegador não pode encontrar os arquivos CAB, ele tenta utilizar os arquivos de classe diretamente a partir do servidor, causando exceções de segurança. Para resolver esse problema, faça o upgrade do navegador, remova o Host On-Demand utilizando o HODRemove.html e, em seguida, reinstale o produto utilizando o HODCached.html.

Mozilla e Firefox

Com os navegadores Mozilla e Firefox, se nada acontecer quando você tentar instalar o cliente armazenado em cache ou se a tentativa de instalar o cliente armazenado em cache falhar, verifique as configurações do navegador. Certifique-se de que Mozilla e Firefox não estão configurados para suprimir as janelas pop-up que aparecem na parte superior ou sob a janela do Navegador. Essa definição evita que o cliente armazenado em cache do Host On-Demand seja instalado.

A localização dessa definição depende da versão do Mozilla:

- No Mozilla 1.2, essa definição é incluída em Editar > Preferências > Avançado > Scripts & Plug-ins.
- No Mozilla 1.3, essa definição é incluída em Editar > Preferências > Privacidade & Segurança > Janelas Pop-up.

Depois do cliente armazenado em cache ser instalado, você poderá restaurar essa definição para suprimir as janelas pop-up. Mas se for necessário instalar o cliente em cache inteiro novamente ou atualizar para uma versão mais nova no primeiro plano, será necessário configurar o Mozilla ou o Firefox novamente de forma que ele não suprima janelas pop-up.



Essa definição para suprimir janelas pop-up não impede a transferência por download de componentes adicionais que não foram incluídos no download inicial (lista de pré-carregamentos).

Cliente Web Start

O cliente Web Start permite que usuários iniciem o Host On-Demand sem um navegador. É necessário usar o Assistente de Implementação para gerar um arquivo HTML para o cliente Web Start. O arquivo HTML gerado pelo Deployment Wizard aponta para um arquivo JNLP (Java Network Launch

Protocol). O arquivo JNLP define um Aplicativo Java, incluindo os parâmetros transmitidos para o aplicativo e os arquivos que contêm arquivos de classe utilizados pelo aplicativo. O arquivo JNLP e os arquivos associados são armazenados em um servidor Web.

Quando um usuário aponta para o arquivo JNLP, o navegador ativa o aplicativo Web Start no computador cliente. Ele transfere por download os arquivos associados, verifica se o JRE mínimo requerido está presente (se especificado), armazena os arquivos na máquina do usuário, configura ícones para representar o aplicativo e ativa o aplicativo.

Os usuários podem iniciar sessões do Host On-Demand a partir do Gerenciador de Aplicativos do Java Web Start. Ao utilizar o Gerenciador de Aplicativos do Java Web Start, as sessões do Host On-Demand não dependem de um navegador. Portanto, o fechamento de um navegador não finaliza uma sessão do Host On-Demand. Se o usuário tentar fechar o desktop do Host On-Demand e houver sessões ativas em execução, ele será solicitado a se certificar de que deseja fechar todas as sessões. Se ele confirmar, as sessões serão terminadas de forma clara para evitar que ocorram problemas quando houver sessões em execução no navegador e este for fechado repentinamente.

Depois da ativação inicial do aplicativo, você poderá apontar o navegador da Web para o arquivo JNLP novamente ou clicar o mouse sobre nos ícones criados na máquina cliente. Após o Web Start ser iniciado novamente, ele verifica no servidor Web as atualizações nos arquivos e transfere por download todos os arquivos atualizados.

O Java Web Start é empacotado com o JRE 1.4.0 ou versões superiores do Java Runtime Environment. Se você utilizar o JRE 1.3, então deverá fazer o upgrade para o JRE 1.4. Para obter informações adicionais sobre o Java Web Start, consulte <http://www.javasoft.com>. O Host On Demand Versão 12 recomenda o Java 1.5 ou superior.

O cliente Web Start do Host On-Demand tem os seguintes requisitos:

- O JRE 1.4 ou posterior é requerido para utilizar o HTTPS para acessar arquivos a partir do servidor Web.
- O JRE 1.4 ou posterior é requerido para utilizar um proxy HTTP com o Web Start.
- As propriedades de sessão que indicam o uso de configurações do Navegador (como servidor proxy ou TLS) não podem ser usadas com o Web Start.

Instalando o cliente Web Start

O cliente Web Start pode ser instalado de duas maneiras. Normalmente, os usuários o instalam a partir de um servidor Host On-Demand por meio da rede, utilizando ou não um navegador da Web. Como alternativa, os usuários podem instalá-lo a partir de uma unidade de LAN ou DVD, embora isto exija um pequeno download adicional pela rede. Independentemente de como os usuários instalam o cliente Web Start, uma vez que ele esteja instalado e no Gerenciador de Aplicativos do Java Web Start, eles podem iniciá-lo clicando no ícone apropriado no Gerenciador de Aplicativos.

Instalando o cliente Web Start a partir do servidor Host On Demand

Os usuários podem instalar o cliente Web Start a partir do servidor Host On-Demand utilizando ou não um navegador.

Utilizando um Navegador da Web: Para instalar o cliente Web Start utilizando um navegador da Web, os usuários podem executar as seguintes etapas:

1. Especifique a URL completa do arquivo HTML em seu navegador, conforme descrito em “Carregando Clientes de Emulador” na página 75.

O cliente Web Start começa a instalação imediatamente. Uma janela mostra o progresso da instalação. A barra de progresso superior desta janela mostra o status de arquivos individuais conforme são transferidos por download, enquanto a barra de progresso inferior mostra o status da instalação global.

2. Quando a instalação é concluída, o código de instalação ativa imediatamente o cliente Web Start. Não é necessário reiniciar o navegador.

Sem Utilizar um Navegador da Web: Para usuários do Windows, distribua o arquivo JNLP que foi gerado a partir do Deployment Wizard (por exemplo, myhod.jnlp) para seus usuários finais. Depois que o arquivo for distribuído, os usuários poderão digitar `start myhod.jnlp` para iniciar o aplicativo Web Start e iniciar a instalação do cliente Host On-Demand. Como a extensão de arquivo '.jnlp' será registrada no aplicativo Web Start, o aplicativo Web Start irá iniciar, ler o arquivo e fazer o download de todos os arquivos archive apropriados do servidor Host On-Demand que foram especificados no arquivo JNLP gerado pelo Deployment Wizard. O cliente Web Start do Host On-Demand será iniciado quando o download for concluído.

Se você não tiver distribuído o arquivo JNLP para usuários Windows ou se os clientes estiverem executando plataformas diferentes do Windows, os usuários ainda poderão fazer o download do cliente Web Start sem um navegador da Web, iniciando o Gerenciador de Aplicativos do Java Web Start diretamente e apontando para o arquivo JNLP no servidor da Web.

Para clientes Windows, os usuários podem executar as seguintes etapas:

1. Abrir o Gerenciador de Aplicativos Java Web Start clicando duas vezes no arquivo `javaws.exe`, normalmente localizado no diretório `C:\Program Files\Java Web Start`.
2. Apontar para o arquivo JNLP no servidor da Web no endereço `http://HODServer/HODAlias/myhod.jnlp`.

Para clientes Linux, um usuário pode digitar `/javaws http://HODServer/HODAlias/myhod.jnlp` para instalar e executar a sessão do Host On-Demand. Um ícone do Host On-Demand aparece no Gerenciador de Aplicativos do Java Web Start. Os usuários podem clicar duas vezes nesse ícone para ativar o Host On-Demand.

Instalando o Cliente Web Start a partir de uma LAN ou DVD

Para reduzir o tráfego da rede e minimizar o tempo de download, algumas empresas preferem que seus usuários instalem o cliente Web Start a partir de uma LAN ou de um DVD. Como o cliente Web Start e o cliente armazenado em cache compartilham os mesmos arquivos em cache, os usuários podem instalar a maior parte do cliente Web Start utilizando o mesmo procedimento de instalação que o cliente armazenado em cache. No entanto, o cliente Web Start requer um componente adicional que deve ser instalado diretamente a partir do servidor Host On-Demand por meio de uma rede.

A instalação do cliente Web Start envolve duas etapas para o administrador seguidas por duas etapas para o usuário final.

Primeiramente o administrador deve executar as duas etapas a seguir:

1. Consultando “Etapas para o Administrador Criar a Imagem do DVD ou da LAN” na página 79 e utilize o Deployment Wizard para gerar um arquivo HTML de Cliente Armazenado em Cache.
2. Utilize o Deployment Wizard uma segunda vez para editar o arquivo HTML criado na etapa anterior, alterando o tipo de cliente de Cliente Armazenado em Cache para Cliente Web Start. (Certifique-se de que nenhuma alteração seja feita para que as sessões definidas e a lista de componentes pré-carregados permaneçam as mesmas.) Essa segunda página HTML é a que você deve publicar para acesso aos usuários.

Em segundo lugar, depois de publicar o arquivo HTML, os usuários devem executar as duas etapas a seguir:

1. Consultando a seção “Etapas para o usuário” na página 80, instale o cliente em cache que o administrador configurou na LAN ou no DVD.
2. Instale o componente adicional para o cliente Web Start seguindo as etapas para Instalação do cliente Web Start a partir do Host On-Demand Server: “Utilizando um Navegador da Web” na página 87. O código do cliente Web Start determinará se os arquivos archive do Host On-Demand já foram transferidos por download e não fará o download novamente. O componente remanescente deve ser transferido por download rapidamente e o cliente Web Start do Host On-Demand será iniciado.

Configurando seu servidor da web para o Web Start

O administrador deve registrar a extensão JNLP como um mimetype com o servidor Web para que o navegador saiba ativar o aplicativo Web Start. Por exemplo, as seguintes seções descrevem como configurar o Apache HTTP Server, o IBM HTTP Server e o Microsoft IIS.

Servidor HTTP Apache ou servidor IBM HTTP

Para configurar o Apache HTTP Server ou o IBM HTTP Server para Web Start, adicione a seguinte linha ao mime.types:

```
AddType  
Application/x-java-jnlp-file .jnlp
```

Microsoft IIS 7.0

Para configurar o Microsoft IIS para Web Start, complete as seguintes etapas:

1. No Painel de Controle > Ferramentas Administrativas > Serviços de Informação da Internet, clique em Web Site Padrão.
2. Clique na guia Cabeçalhos HTTP em Propriedades.
3. Em Mapa MIME, clique na guia Tipos de Arquivos e selecione Novo Tipo.
4. No campo Extensão, digite .jnlp.
5. No campo Tipo de Conteúdo, digite application/x-java-jnlp-file.
6. Clique em OK.

Fazendo upgrade do cliente Web Start

Depois da instalação inicial do cliente Web Start, se os usuários apontarem seus navegadores para o arquivo HTML gerado pelo Deployment Wizard e atualizações estiverem disponíveis no servidor Host On-Demand, o Host On-Demand avisará o usuário para atualizar. Se os usuários desejarem fazer a atualização, o Java Web Start transferirá por download os arquivos archive atualizados e ativará o Host On-Demand. Se os usuários rejeitarem o upgrade, o Host On-Demand os avisará novamente na próxima vez em que eles ativarem o arquivo HTML.

Incluindo componentes do Web Start após a instalação inicial

Se os usuários solicitarem uma função que não está disponível no cliente Java Web Start, o Host On-Demand solicitará a eles que instalem os componentes adicionais requeridos para aquela função. Se eles optarem por instalar os componentes adicionais, deverão reiniciar o cliente Host On-Demand para os utilizar.

Usuários restritos do Web Start e do Windows

Os Usuários Restritos do Windows com o Java Web Start 1.0.1 devem remover o JRE e o Java Web Start e reinstalar um JRE mais recente com o Java Web Start 1.2.

Marcando sessões com o Web Start

Como o cliente Web Start é executado fora de um navegador, a marcação é desativada pois ela é um recurso do navegador. Os administradores podem criar clientes Web Start que fornecem aos usuários a mesma aparência como se estivessem executando uma sessão marcada incorporada fazendo o seguinte:

1. Na janela Opções Avançadas do Deployment Wizard, adicione o parâmetro HideHODDesktop com um valor true.
2. Configure uma única sessão para inicialização automática.
3. Configure a sessão para não iniciar em uma janela separada.

Usando o Web Start com HTTPS

Se quiser utilizar o HTTPS com o cliente Web Start, a autoridade de certificação utilizada para a conexão HTTP segura deve vir de uma autoridade raiz bem conhecida. Ao utilizar o Host On-Demand como um applet e uma conexão HTTPS, você tem a oportunidade de confiar no certificado utilizado para a conexão HTTPS se a autoridade raiz não for bem conhecida pelo navegador. Como o Java Web Start é executado como um aplicativo, esse recurso do navegador não está disponível. A Java Virtual Machine utilizada pelo Java Web Start contém várias autoridades raiz confiáveis. Se o certificado que vem da conexão HTTPS tiver uma autoridade raiz de uma dessas autoridades conhecidas pela JVM, a conexão segura poderá ser estabelecida. Se você desejar usar uma autoridade de certificação diferente daquelas conhecidas pela JVM por padrão, por exemplo, um certificado autoassinado, será necessário importar o certificado para o keystore da JVM para cada um dos clientes que acessarem esse cliente Java Web Start. Isso é requerido para estabelecer a conexão HTTP segura.

Removendo o cliente Web Start

Para remover o cliente Web Start, complete as duas etapas a seguir:

1. No Gerenciador de Aplicativos do Java Web Start, realce o aplicativo e clique em Remover.
2. Lance o HODRemove.html no navegador.

Cientes de Download

Ao contrário do cliente armazenado em cache e do cliente Web Start, o cliente de download não controla como ou quando os componentes do cliente serão transferidos por download para a unidade de disco rígido da estação de trabalho. O cliente de download deixa todas as decisões de armazenamento em cache para o navegador.

Utilize o cliente de download se você atender aos *dois* requisitos a seguir:

- Você não deseja ocupar espaço em disco nas máquinas clientes instalando o cliente armazenado em cache ou o cliente Web Start.
- Seu tempo de download inicial não está em questão.

Ativando o Cliente de Download

Lance o cliente de download fazendo o download dele a partir do servidor Host On-Demand em sua janela do navegador, conforme descrito em “Carregando Clientes de Emulador” na página 75.

Ativando o cliente de download depois de instalar o cliente em cache ou o cliente Web Start

Java

Com clientes Java, é possível ativar com êxito o cliente de download depois de instalar o cliente em cache ou o cliente Web Start.

Clientes de Emulador Predefinidos

Vários arquivos HTML do cliente de emulador predefinidos são fornecidos com o Host On-Demand. Eles são incluídos para demonstrar a gama de funcionalidades do cliente Host On-Demand e para servir como exemplos para criar arquivos HTML personalizados no Deployment Wizard. Todos eles utilizam o modelo baseado no servidor de configuração. Para carregar um desses clientes, siga as instruções em “Carregando Clientes de Emulador” na página 75.



Em geral, é recomendável definir seus próprios arquivos HTML personalizados com o Deployment Wizard em vez de utilizar os arquivos HTML do cliente predefinidos.

Os seguintes arquivos HTML do cliente de emulador predefinidos são fornecidos pelo Host On-Demand:

Cliente armazenado em cache (HODCached.html)

Fornece todas as funções do cliente Host On-Demand.

Cliente armazenado em cache com determinação de problemas (HODCachedDebug.html)¹

Inicia o cliente armazenado em cache com determinação de problemas (registro e rastreamento de sessão).

Cliente de download (HOD.html)

Fornece todas as funções do cliente Host On-Demand, exceto determinação de problemas.



Com um navegador ativado para Java, o arquivo HOD.html do cliente de download predefinido omite alguns componentes do Host On Demand usados raramente. Para obter informações adicionais, incluindo uma lista de componentes excluídos e uma descrição de soluções alternativas, consulte “Arquivos HTML Não Contêm Alguns Componentes” na página 16. O acesso ao HOD.html com um navegador Java funciona com funções limitadas.

Cliente de download com determinação de problemas (HODDebug.html)¹

Carrega o cliente de download com determinação de problemas (registro e rastreamento de sessão).

Notas:

1. Utilize os clientes de determinação de problemas apenas se você estiver trabalhando com o Suporte IBM para resolver um problema com sua instalação do Host On-Demand.

Reduzindo o Tamanho do Cliente de Download

Em geral, é uma boa idéia manter o menor tamanho possível dos clientes Host On-Demand (sejam clientes de download, Web Start ou armazenados em cache). Isso acelera o tempo de download e conserva o espaço em disco nas máquinas clientes.

A melhor maneira para minimizar o tamanho dos clientes Host On-Demand é criá-los utilizando o Deployment Wizard. Os clientes predefinidos fornecidos com o Host On-Demand são geralmente maiores que os clientes personalizados criados no Deployment Wizard porque eles contêm a extensão total da funcionalidade do cliente Host On-Demand. Os clientes criados no Deployment Wizard contêm apenas as funções que você seleciona para serem pré-instaladas. Além disso, os clientes do Deployment Wizard são transferidos através de download em formato compactado. Isso reduz mais o tamanho do download.

Ao criar um cliente personalizado com o Deployment Wizard, é possível selecionar apenas as funções que você sabe que os usuários precisarão na janela Opções de Pré-carregamento no Deployment Wizard. Por exemplo, se os usuários precisarem apenas das sessões de terminal 3270 e impressora 3270, não selecione nenhum outro tipo de sessão quando estiver criando o cliente no Deployment Wizard. A inclusão de suporte para tipos de sessão não utilizados aumenta o tamanho do cliente sem melhorar sua funcionalidade.

Se você clicar em Seleção Automática na janela Opções de Pré-carregamento, o Deployment Wizard selecionará os componentes de que precisa com base na configuração da sessão.

Você também pode optar por não fazer o download dos componentes para funções que não são utilizadas com frequência. A menos que essa função seja desativada no Deployment Wizard, será solicitado ao usuário para fazer o download de quaisquer componentes necessários quando ele utilizar essa função. Se, posteriormente, você precisar de tipos de sessão adicionais, não será necessário criar um novo tipo de cliente. Você pode adicionar os novos tipos de sessão à lista de pré-carregamentos na janela Opções de Pré-carregamento.



No Mac OS X, não é possível instalar componentes adicionais após o download inicial. Para obter informações adicionais, consulte o “Suporte a clientes em cache para Mac OS X (somente clientes Java)” na página 84.

Não utilize a depuração ou determinação de problemas nos clientes predefinidos ou gerados pelo Deployment Wizard. Isso aumenta bastante o tamanho do cliente e pode reduzir o desempenho de um cliente. Os clientes de depuração e de determinação de problemas não destinam-se ao uso geral. Utilize-os apenas em conjunto com o suporte técnico do Host On-Demand para diagnosticar e resolver problemas do sistema Host On-Demand.

Implementando archives e classes Java fornecidos pelo cliente

As classes e os archives Java fornecidos pelo cliente são arquivos de classe e archives Java não incluídos como parte do cliente Host On Demand ou do Java Runtime Environment. Os exemplos de tais arquivos são classes ou archives Java que você mesmo implementou ou obteve de terceiros.

Você irá implementar tais classes ou archives para uso com o cliente de emulador nas seguintes situações:

- Você deseja que seus usuários executem macros que chamem métodos Java fornecidos pelo cliente.
- Você deseja que os usuários executem um applet fornecido pelo cliente com a sessão (iniciado automaticamente com a sessão ou ativado utilizando-se a seleção Ações > Executar Applet... no menu da janela de sessão).



Para limitações do Java na execução de applets fornecidos pelo cliente, veja “Limitações com applets fornecidos pelo cliente e Java” na página 18.

Embora vários métodos estejam disponíveis para implementar esses arquivos, cada método funciona somente sob determinadas circunstâncias. Os métodos possíveis são:

- Utilizar o parâmetro HTML AdditionalArchives no Deployment Wizard. Consulte “Usando o parâmetro HTML AdditionalArchives”.
- Copiar os arquivos para o diretório de publicação do servidor Host On-Demand. Consulte “Implementando a partir do Diretório de Publicação” na página 93.

O método de implementação escolhido depende:

- O tipo de arquivo implementado (classes Java e Java archives)
- De onde os arquivos serão implementados (servidor Host On-Demand ou estação de trabalho do cliente)
- Do tipo de plataforma de cliente e do tipo de navegador.

Os três métodos disponíveis para implementar archives e classes Java fornecidos pelo cliente estão descritos nas seguintes seções. Além disso, “Dicas e sugestões para archives” na página 93 fornece informações adicionais sobre o uso de arquivos archives.

Usando o parâmetro HTML AdditionalArchives

É possível usar esse método quando você deseja implementar archives Java em um servidor Host On Demand. Esse método funciona para o cliente de emulador armazenado em cache, o cliente de emulador de download e o cliente Web Start.

Os Java archives devem ser arquivos .JAR do Java.

A vantagem de usar o parâmetro HTML AdditionalArchives é que ele faz com que os archives Java sejam transferidos por download para a estação de trabalho do usuário automaticamente quando um de seus usuários se conecta com o arquivo HTML do cliente armazenado em cache ou do cliente de download no servidor Host On-Demand.

A desvantagem desse método é que esses archives ou arquivos de classe Java serão transferidos por download novamente sempre que o usuário se conectar àquele arquivo HTML, independentemente se você está utilizando um cliente armazenado

em cache ou um cliente transferido por download. A razão para a transferência por download dos archives sempre que o usuário se conectar é assegurar que o cliente Host On-Demand tenha as versões mais recentes dos archives ou arquivos de classe. Como resultado, esse método funciona melhor quando os archives ou arquivos de classe Java são relativamente poucos e pequenos, para que os usuários não precisem aguardar muito tempo pela transferência por download desses arquivos e para que essa transferência aos usuários não coloque uma carga pesada no servidor Web.

Para utilizar esse método, execute as seguintes etapas:

1. Coloque os archives no diretório de publicação do Host On-Demand. O diretório de publicação padrão é o HOD do subdiretório no diretório de instalação do servidor Host On-Demand, como `c:\Arquivos de programas\IBM\HostOnDemand\HOD\`.
2. Edite o arquivo HTML com o Deployment Wizard. Em seguida:
 - a. No painel Opções Avançadas, clique em Parâmetros HTML.
 - b. No campo Nome, insira `AdditionalArchives`.
 - c. No campo Valores, insira os nomes dos archives Java, separados por vírgulas, sem extensões de arquivo (.jar). Por exemplo:
`myCustomA,myCustomB,MyCustomC`

Para obter informações adicionais, consulte `AdditionalArchives` na ajuda on-line.

Implementando a partir do Diretório de Publicação

Esse método funciona na seguinte situação:

- Quando você deseja implementar arquivos de classe Java em um servidor Host On Demand. Os arquivos de classe Java não devem pertencer a nenhum pacote do Host On Demand.

Para utilizar esse método, coloque os archives no diretório de publicação do Host On-Demand. O diretório de publicação padrão é o HOD do subdiretório no diretório de instalação do servidor Host On-Demand, como `c:\Arquivos de programas\IBM\HostOnDemand\HOD\`.

Dicas e sugestões para archives

As seguintes sugestões e dicas poderão fornecer informações úteis sobre o uso de arquivos archives:

- Quando você criar o archive (.jar), verifique se o caminho de cada arquivo de classe está correto. Por exemplo, o caminho para `com.mycompany.MyClass` deve ser `com\mycompany\`. Ele *não* deve ser `C:\MyTestDirectory\com\mycompany\` e não deve ficar em branco (porque o arquivo de classe faz parte de um pacote).
- Verifique se as permissões adequadas estão definidas para os arquivos archive. Ou seja, nos sistemas operacionais que utilizam permissões de arquivo, como o Linux, AIX, Unix e z/OS, as permissões de arquivo para os arquivos archive devem ser definidas para 755 (ou seja, `rwxr-xr-x`).
- Se você tiver páginas diferentes de clientes em cache que especificam parâmetros `AdditionalArchives` diferentes, será necessário fechar e reiniciar o navegador quando alternar de uma página para outra. Caso contrário, quando você alterar de uma página para outra, o cliente armazenado em cache não será recarregado e, como resultado, o parâmetro `AdditionalArchives` não será verificado.

Capítulo 11. Utilizando Clientes Database On-Demand

O cliente do Database On-Demand é um applet Java que permite a um usuário final construir instruções SQL e instruções de File Upload, enviar essas instruções a um servidor de banco de dados remoto e recuperar os resultados de consultas SQL (instruções SQL Select) do servidor de banco de dados remoto.

O usuário pode se comunicar com um servidor de banco de dados em execução em um servidor IBM System i ou outra plataforma, contanto que o driver Java Database Connectivity (JDBC) apropriado esteja instalado na estação de trabalho do cliente Database On-Demand. Para obter informações adicionais, consulte “Obtendo e Instalando um Driver JDBC” na página 98 neste manual.

Os recursos do Database On-Demand incluem:

- Interfaces de texto e gráficas para construção de instruções SQL e de File Upload.
- A habilidade de salvar e reutilizar instruções SQL e de File Upload.
- Para instruções SQL:
 - A habilidade de executar uma instrução SQL e exibir os resultados.
 - A habilidade de salvar os resultados de uma instrução SQL em um arquivo em vários formatos de arquivo, incluindo XML (consulte “Formatos de Arquivo para Acesso ao Banco de Dados” na página 98 neste manual).
- Para instruções de File Upload:
 - A habilidade de utilizar os seguintes tipos de File Upload: create, replace, append e update.
 - A habilidade de ler arquivos de dados em vários formatos, incluindo XML (consulte “Formatos de Arquivo para Acesso ao Banco de Dados” na página 98 neste manual).

O cliente Database On-Demand está disponível apenas por meio de um de três arquivos HTML de cliente predefinidos (consulte “Clientes Predefinidos do Database On-Demand” na página 97). Não é possível utilizar o Deployment Wizard para criar um cliente Database On-Demand.

No entanto, como alternativa ao cliente Database On-Demand, agora é possível utilizar funções de banco de dados nos clientes de emulação do Host On-Demand e em macros (consulte “Funções do Banco de Dados em Clientes de Emulação de Vídeo e em Macros” na página 96).

Para obter informações adicionais, consulte Visão Geral de Acesso ao Banco de Dados na ajuda on-line do Host On-Demand.

O cliente do Database On-Demand existe em uma versão Java. Portanto:

- Um usuário final executando um navegador ativado para Java executa automaticamente a versão Java do cliente do Database On-Demand.

Esse cliente do Database On-Demand pode aproveitar os recursos avançados do plug-in Java.

Funções do Banco de Dados em Clientes de Emulação de Vídeo e em Macros

Como uma alternativa ao cliente do Database On-Demand, quase todas as funções que estão disponíveis no cliente do Database On-Demand agora estão disponíveis no cliente de emulação de vídeo, incluindo os seguintes tipos de sessão.

- Sessão de Terminal 3270
- Sessão de Terminal 5250
- Sessão de Terminal VT

Também é possível utilizar instruções SQL e instruções de File Upload em macros nas sessões do cliente de emulação de vídeo (consulte a ação SQLQuery e a ação File Upload na *Guia de Programação de Macro*).

Por exemplo, enquanto estiver conectado a um host remoto em uma sessão de Vídeo 3270, é possível ativar uma macro que lê automaticamente dados da janela da sessão de Vídeo 3270 e grava os dados em uma tabela em um banco de dados que está localizado em outro host remoto. De maneira semelhante, é possível ativar uma macro que lê automaticamente os dados de uma tabela em um banco de dados remoto e grava os dados na janela da sessão de Vídeo 3270.

Para obter informações adicionais, consulte Visão Geral de Acesso ao Banco de Dados na ajuda on-line do Host On-Demand.

Iniciando um cliente do Database On-Demand

Para iniciar um cliente do Database On-Demand em uma estação de trabalho do cliente, utilize um dos seguintes dois métodos:

- Conecte seu navegador a um arquivo HTML predefinido do Database On-Demand, digitando a URL do arquivo HTML no campo de endereço de seu navegador (ou clicando em um link que direciona o navegador para aquela URL). O formato da URL é:

```
http://server_name/hod_alias/client_name.html
```

em que *server_name* é o nome do host ou o endereço IP do servidor Host On-Demand, *hod_alias* é o alias do diretório de publicação e *client_name* é o nome do arquivo HTML. Por exemplo, assumindo-se que www.myHODServer.com é seu servidor Host On-Demand e que *hod* é o alias do diretório de publicação, a URL para a versão de download do cliente do Database On-Demand será:

```
http://www.myHODServer.com/hod/HODDatabase.html
```

- Conecte o navegador com o arquivo HTML de clientes do IBM Host On-Demand e clique no link do cliente do Database On-Demand que deseja executar. A URL do arquivo HTML de clientes é:

```
http://server_name/hod_alias/HODMain_xx.html
```

em que *server_name* e *hod_alias* possuem o mesmo significado como descrito acima. No nome do arquivo *HODMain_xx*, o *xx* é um mnemônico de duas letras do idioma que você deseja utilizar. Por exemplo, para inglês, o arquivo é denominado *HODMain_en.html* e a URL completa é (assumindo-se o mesmo servidor e alias descritos acima):

```
http://www.myHODServer.com/hod/HODMain_en.html
```

Cientes Predefinidos do Database On-Demand

O cliente do Database On-Demand está disponível por meio de qualquer um dos três arquivos HTML de clientes predefinidos. Não é possível utilizar o Deployment Wizard para criar um arquivo HTML de cliente do Database On-Demand. Os clientes predefinidos são descritos a seguir.

Cliente Database On-Demand (HODDatabase.html)

Este é o cliente de download. "Download" indica que todo o código do cliente é transferido por download para a estação de trabalho do cliente a cada vez que o usuário final iniciar o cliente do Database On-Demand.

Cliente Database On-Demand em cache (HODDatabaseCached.html)

Este é o cliente armazenado em cache. "Cached" indica que a maior parte do código do cliente é transferido por download na primeira vez que o usuário final iniciar o cliente do Database On-Demand e é armazenado na estação de trabalho do cliente. Depois do primeiro download, o cliente armazenado em cache iniciará muito mais rapidamente do que o cliente de download, porque a maior parte do código do cliente já estará disponível em sua estação de trabalho. O cliente do Database On-Demand em cache possui muitos componentes em comum com o cliente do Host On-Demand em cache.



Para o cliente em cache, se o usuário final precisar de mais de uma página de códigos, será necessário incluir o nome do arquivo archive (arquivo .jar) para cada página de código adicional para a lista de pré-carregamento no arquivo HTML predefinido. Para obter uma lista de idiomas da página de código e de nomes de arquivos correspondentes, consulte "Utilizando Várias Páginas de Códigos com o Database On-Demand" na página 98.

Cliente Database On-Demand em cache com determinação de problemas (HODDatabaseCachedDebug.html)

Este é o cliente armazenado em cache com código extra de determinação de problemas para registro da sessão de eventos da sessão e de rastreamento.



Utilize os clientes de determinação de problemas apenas se você estiver utilizando o Suporte IBM para resolver um problema com sua instalação do Host On-Demand.

Configurando o Database On-Demand para Usuários

Para configurar o Database On-Demand para usuários, siga estas etapas:

1. Utilize o Utilitário de Administração para definir grupos e usuários (consulte Gerenciando Usuários e Grupos na ajuda on-line do Host On-Demand).
2. Especifique as funções do banco de dados que deseja que os grupos e usuários executem e especifique valores padrão para alguns dos parâmetros do banco de dados em novas instruções SQL e de File Upload (consulte Opções de Grupo/Usuário do Database On-Demand na ajuda on-line do Host On-Demand).

Se deseja criar instruções SQL predefinidas e instruções de File Upload para usuários e grupos, siga estas etapas:

1. Execute o cliente do Database On-Demand como um usuário final e crie instruções SQL e de File Upload (consulte Introdução ao Database On-Demand na ajuda on-line do Host On-Demand).
2. Ative o Utilitário de Administração e copie as instruções SQL e de File Upload para outros usuários ou grupos (consulte Instruções de Grupo/Usuário do Database On-Demand na ajuda on-line do Host On-Demand).

Obtendo e Instalando um Driver JDBC

Para conectar-se com um servidor de banco de dados em execução em um host remoto, o usuário final precisa de um driver JDBC (Java Database Connectivity) instalado na estação de trabalho do cliente.

O cliente do Host On-Demand e o cliente do Database On-Demand já incluem um driver JDBC do IBM AS/400 Toolbox para Java. Esse driver permite que um cliente acesse um banco de dados DB2/400 em um IBM System i ou sistema host AS/400 configurado adequadamente. Não é necessário registrar ou implementar esse driver.

Se você precisar de um driver JDBC diferente:

1. Entre em contato com o fornecedor ou com o administrador do banco de dados remoto para obter o driver JDBC.
2. Registre o driver JDBC com o Host On-Demand ou como o Database On-Demand. Consulte Registrando um Driver JDBC na ajuda on-line do Host On-Demand.
3. Implemente o driver JDBC nas estações de trabalho de seus usuários finais. Consulte Implementando um Driver JDBC na ajuda on-line do Host On-Demand.

Formatos de Arquivo para Acesso ao Banco de Dados

O usuário final seleciona um tipo de arquivo para uma instrução SQL ou para uma instrução de File Upload na guia Saída da janela do Assistente de SQL ou na guia Arquivo da janela File Upload.

Para obter informações sobre formatos de arquivo, consulte Formatos de Arquivos para Acesso ao Banco de Dados na ajuda on-line do Host On-Demand.

Utilizando Várias Páginas de Códigos com o Database On-Demand

Se você desejar usar várias páginas de códigos com o Database On-Demand, será necessário incluir arquivos jar ou cab no arquivo HTML. Apenas as páginas de códigos que correspondem ao idioma do arquivo HTML são carregadas automaticamente. Por exemplo, se estiver executando a partir de um computador em francês, mas desejar acessar um host em holandês, será necessário fazer estas modificações.

Edite o arquivo CommonJars.js. Se você estiver utilizando um cliente de download, procure a linha que inicia com "dbaDownloadJars =" e inclua os nomes de arquivos apropriados a partir da tabela abaixo. Utilize nomes de arquivos jar, mesmo se os clientes forem utilizar o Internet Explorer (posteriormente, os nomes serão convertidos para nomes de arquivos cab). Se você estiver utilizando um cliente de cache, procure a linha que inicia com "dbaCachedComps =" e inclua o nome de componente apropriado a partir da tabela abaixo.

Páginas de Códigos do Database On-Demand Suportadas

A tabela a seguir lista os idiomas da página de código do cliente Database On-Demand, os nomes de arquivos .jar correspondentes e nomes de componentes armazenados em cache:

Idioma da Página de Código	Nome do Arquivo .JAR	Nome do Componente
Árabe	hacpar.jar	HACPAR
Tcheco, húngaro, polonês, esloveno	hacpce.jar	HACPCE
Dinamarquês, finlandês, holandês, norueguês, sueco	hacp1b.jar	HACP1B
Alemão, espanhol, francês, italiano, português, português do Brasil	hacp1a.jar	HACP1A
Grego	hacpgr.jar	HACPGR
Hebraico	hacphe.jar	HACPHE
Japonês	hacpja.jar	HACPJA
Coreano	hacpko.jar	HACPKO
Russo	hacpru.jar	HACPRU
Chinês Simplificado	hacpzh.jar	HACPZH
Tai	hacpth.jar	HACPTH
Turco	hacptr.jar	HACPTR
Chinês Tradicional	hacptw.jar	HACPTW

Capítulo 12. Criando e Implementando Bibliotecas de Macros do Servidor

As bibliotecas de macros do servidor estão disponíveis para as páginas de modelo HTML e usuários do modelo de Configuração. Para a página HTML, os usuários podem usar o Assistente de Implementação para customizar a biblioteca de macros do servidor; para o modelo de Configuração, os usuários podem usar o console de administrador do Host On Demand. A configuração baseada na GUI permite que o administrador configure para cada sessão. Para que o administrador configure para todas as sessões definidas, use o parâmetro HTML `SetServerMacroLibraryPath`.

O valor de `SetServerMacroLibraryPath` é *share path* ou *relative path*. É possível usar os valores para criar e manter um armazenador central de macros para os usuários acessarem a partir de suas sessões do Host On Demand. Essas macros são transferidas por download para a máquina do usuário somente quando necessário. Quando você faz mudanças em uma macro do servidor, os usuários obtêm automaticamente suas atualizações na próxima vez que acessarem a macro.

As bibliotecas de macros do servidor têm vários benefícios:

- Elas oferecem uma maneira conveniente de armazenar, editar e administrar macros, tudo de uma localização fácil de acessar.
- Elas permitem compartilhamento fácil de macros entre vários usuários e através de qualquer número de sessões.
- Elas eliminam a necessidade de importar macros na sessão Host On-Demand e, portanto, podem reduzir o tamanho da sessão. As macros apenas serão transferidas por download para a máquina do usuário, se e quando o usuário acessá-las.
- Você pode editar macros e substituir os arquivos na biblioteca de macros do servidor a qualquer momento, sem regenerar as sessões do Host On-Demand ou modificar os arquivos HTML. Todas as alterações feitas ficam automaticamente disponíveis na próxima vez que um usuário solicitar essa macro.

Bibliotecas de macro do servidor podem residir em um Servidor Web ou em uma unidade de rede compartilhada. Para ambos os tipos de bibliotecas, é possível controlar quais macros estão disponíveis para sessões específicas do Host On-Demand. Se você utilizar uma biblioteca de macros baseada na Web, será necessário criar um arquivo de texto que identifica as macros específicas que deseja disponibilizar para a sessão que você está configurando. Se você utilizar uma biblioteca de macros baseada na unidade compartilhada, *todos* os arquivos no diretório especificado estarão disponíveis para a sessão. Os usuários não terão permissão para gravar em uma biblioteca de macro baseada na Web, mas poderão atualizar uma biblioteca de macro baseada na unidade compartilhada se eles tiverem acesso de gravação.

Implementando uma Biblioteca de Macros do Servidor para um Servidor Web

1. Coloque as macros em um local em que os usuários possam acessar através de um servidor Web. Não precisa ser o diretório de publicação do Host On-Demand.

2. Para cada sessão que requer um conjunto de macros separadas, crie um arquivo de texto que contenha a lista de nomes de arquivos de macros. O formato do arquivo de texto pode ter apenas um nome de arquivo de macro por linha, por exemplo:

```
macro1.mac  
macro2.mac  
macro3.mac
```

Certifique-se de observar as seguintes regras:

- O nome da macro deve ser o primeiro elemento na linha, visto que tudo após o primeiro elemento é ignorado.
 - Se o primeiro elemento na linha começar com //, a linha será considerada um comentário e será ignorada.
 - Cada macro listada no arquivo de texto deve ter uma extensão .mac.
3. Coloque esse arquivo de texto na mesma localização que as macros referenciadas.
 4. No Deployment Wizard, clique no menu Configurar na janela Sessões do Host e selecione Biblioteca de macros do servidor... Marque a caixa 'Utilizar uma biblioteca de macros do servidor para esta sessão' e selecione Biblioteca de macros do servidor Web.
 5. Especifique a URL completa da lista de macros criadas na Etapa 2, por exemplo, `http://servername/hod/macrolist.txt`. Clique em OK.

Quando os usuários abrem suas sessões, eles podem utilizar as janelas Reproduzir Macro ou Macros Disponíveis para ver as macros especificadas na lista criada para a sessão. Essas macros ficam disponíveis quando os usuários selecionam Biblioteca do servidor como sua localização da macro. A localização da biblioteca do Servidor apenas ficará disponível, se você configurou a sessão para utilizar uma biblioteca de macros do servidor.

Nota: A biblioteca de macros do servidor também pode ser configurada no Cliente administrador.

Implementando uma Biblioteca de Macros do Servidor em uma Unidade Compartilhada

1. Coloque as macros em um diretório compartilhado em sua rede.
2. Na janela Sessões do Host do Deployment Wizard, selecione a sessão que deseja configurar, clique no menu Configurar e selecione Biblioteca de macros do servidor. Marque a caixa 'Utilizar uma biblioteca de macros do servidor para esta sessão' e selecione Biblioteca de macros de unidade compartilhada.
3. Especifique o caminho do diretório. Exemplos de caminhos de diretório válidos incluem os seguintes:
 - Caminhos absolutos. As letras da unidade de rede mapeadas também podem ser utilizadas no caminho absoluto. Observe que uma biblioteca de macros do servidor nunca deve apontar para uma unidade local.
 - São permitidos nomes de computadores remotos ou endereços IP, contanto que o computador do usuário já esteja conectado e autenticado remotamente no computador que está compartilhando o diretório. A seguir encontram-se dois exemplos de caminhos para bibliotecas de macros de unidades compartilhadas:
 - `\\your_host\macro_library`, em que *your_host* é o nome do host e *macro_library* é o diretório de macros.

- \\123.45.67.89\macro_library, em que 123.45.67.89 é o endereço IP do host e *macro_library* é o diretório de macros.

Se você estiver configurando uma biblioteca de macros para mais de uma sessão e se cada sessão utilizar seu próprio conjunto de macros, será necessário criar um diretório separado para cada sessão.

4. Clique em OK.

Quando os usuários abrem suas sessões, eles podem utilizar as janelas Reproduzir Macro ou Macros Disponíveis para ver uma lista de macros no diretório. Essas macros ficam disponíveis quando os usuários selecionam Biblioteca do servidor como sua localização da macro. A localização da biblioteca do Servidor apenas ficará disponível, se você configurou a sessão para utilizar uma biblioteca de macros do servidor.

Capítulo 13. Modificando Propriedades de Sessão Dinamicamente

As sessões do Host On-Demand são definidas pelo administrador e recuperadas pelo cliente Host On-Demand quando um usuário acessa um arquivo HTML do Host On-Demand. As propriedades de sessão observadas pelo usuário são valores fixos e consistem em uma combinação da configuração inicial do administrador e quaisquer atualizações do usuário. No entanto, algumas vezes seria útil com alguns arquivos HTML, ou com determinadas propriedades de sessão, definir dinamicamente um valor no momento em que o HTML é acessado. Esse tipo de controle permite definir valores de propriedades de sessão específicos com base em informações como, por exemplo, endereço IP do cliente ou a hora do dia.

Para definir dinamicamente as propriedades de sessão no momento em que o HTML é acessado, o administrador deve escrever um programa que é executado no servidor Web e modifica efetivamente o HTML antes de ser enviado para o cliente. Mesmo que as propriedades de sessão iniciais não sejam definidas no HTML, o Host On-Demand fornece a capacidade de substituir várias propriedades de sessão no HTML. Esses valores de substituição são sempre utilizados pelo cliente e têm precedência sobre as propriedades de sessão iniciais configuradas pelo administrador, bem como quaisquer atualizações da propriedade feitas pelo usuário. O valor de substituição de HTML nunca é armazenado, portanto, o cliente voltará a utilizar as definições anteriores para a propriedade sempre que o administrador remover a substituição. Além disso, a propriedade substituída é bloqueada para que não seja alterada por um usuário.

Há várias maneiras de um administrador escrever um programa para definir dinamicamente uma ou mais propriedades de sessão utilizando as substituições de HTML, como utilizar JSP (Java Server Pages), servlets, Perl, REXX ou ASP (Active Server Pages). Este capítulo apresenta alguns exemplos que focalizam problemas comuns do administrador. Esses exemplos demonstram a sintaxe e a técnica de substituição de propriedades específicas. Esses mecanismos aplicam-se a qualquer abordagem de programação escolhida pelo administrador.

Configurando o Arquivo HTML Inicial

O arquivo HTML inicial deve ser criado utilizando o Deployment Wizard que permite configurar os recursos que são importantes para você, como o tamanho do código que foi transferido por download e as funções disponíveis para os usuários. As seções seguintes descrevem os parâmetros HTML que precisarão ser incluídos. No entanto, lembre-se de que o formato exato requerido para esses parâmetros variarão, dependendo do formato do HTML. Observe que no Host On-Demand 7 e posterior, alguns dos HTMLs são gerados utilizando JavaScript, e os parâmetros HTML são especificados dentro de uma matriz JavaScript ou usando as instruções `document.write` do JavaScript. Além disso, o formato do HTML varia de acordo com o tipo de cliente (cliente em cache ou de download) selecionado.

Definindo o Código Base

Para definir o código base ao criar um HTML utilizando o Deployment Wizard, proceda da seguinte forma:

1. Na janela Opções Adicionais, clique em Opções Avançadas e vá para a ramificação Outras na exibição em árvore.
2. Digite o caminho relativo /hod/ no campo Código Base.
3. Salve o arquivo HTML no diretório de publicação do Host On-Demand padrão *your_install_directory*\HOD.

O arquivo HTML é localizado no mesmo diretório com os arquivos archives do Host On-Demand.

O código base se refere ao diretório de publicação do Host On-Demand instalado e não ao diretório onde estão publicados os arquivos do Deployment Wizard. Embora você possa inserir uma URL completa no campo Código Base, é fortemente recomendado inserir o caminho /hod/ relativo para o diretório de publicação padrão ao modificar dinamicamente as propriedades da sessão. Se você inserir uma URL completa, nenhum usuário que especifica o nome do host de maneira diferente da especificada como o Código base conseguirá acessar os arquivos, mesmo se as entradas de DNS forem determinadas para o mesmo endereço IP.

Incluir o Parâmetro ConfigBase

Inclua um parâmetro no arquivo HTML denominado ConfigBase. Semelhante à definição de /hod/ como o código base no “Definindo o Código Base” na página 105, o parâmetro ConfigBase é necessário porque eventualmente você implementará o arquivo JSP em um local que é diferente do diretório de publicação padrão e o applet do Host On-Demand precisa saber como localizar os arquivos de configuração da sessão localizados no diretório *hostondemand/HOD/HODData*. Esses arquivos são criados no momento em que você salva seu arquivo HTML do Deployment Wizard no diretório de publicação. Ao contrário do Codebase, o parâmetro ConfigBase requer uma URL completa. ConfigBase é um termo específico do Host On-Demand.



Para obter informações adicionais, consulte *Desenvolvendo Arquivos JavaServer Pages com Extensões do WebSphere*.

Substituindo Parâmetros HTML

Há várias etapas a serem seguidas para configurar dinamicamente as propriedades de sessão (os exemplos mostrados posteriormente neste capítulo ajudarão a esclarecer como alguns desses parâmetros devem ser especificados):

1. **Ativar substituições de HTML.** Por padrão, o cliente ignora as substituições de HTML. Para ativar as substituições, você precisará incluir um parâmetro HTML denominado *EnableHTMLOverrides* e defini-lo para o valor *true*.
2. **Listar as sessões a serem substituídas.** Como podem existir várias sessões associadas a um HTML, é necessário listar quais serão substituídas. Você precisará incluir um parâmetro HTML denominado *TargetedSessionList*, gerando um valor dos nomes exatos das sessões que devem aceitar substituições. O valor deve ser uma lista separada de nomes de sessão separados por vírgula, como "NomeSessão1, NomeSessão2".
3. **Especificar a própria substituição.** Para cada propriedade de sessão a ser substituída, você precisará incluir um parâmetro HTML chamado nome de propriedade, com o valor sendo a substituição desejada. O valor especificado será aplicável a todas as sessões listadas no parâmetro *TargetedSessionList*. Se você desejar substituir apenas um subconjunto das sessões no

TargetedSessionList, poderá especificar um valor no formato "NomeSessão1=valor1, NomeSessão2=valor2", por exemplo.

Propriedades da Sessão Específicas que Podem Ser Substituídas

A tabela a seguir descreve as propriedades da sessão que podem ser substituídas e fornece os valores aceitáveis para cada parâmetro:

Tabela 12. Propriedades da Sessão que Podem Ser Substituídas

Nome do Parâmetro	Descrição	Valores Válidos
Host	Nome do host ou endereço IP do servidor de destino. Aparece como "Endereço de destino" nos painéis de propriedades. Aplica-se a todos os tipos de sessão.	Nome do host ou endereço IP.
HostBackup1	Nome do host ou endereço IP do servidor de backup1. Aparece como "Endereço de destino" nos painéis de propriedades backup1on. Aplica-se a todos os tipos de sessão.	Nome do host ou endereço IP.
HostBackup2	Nome do host ou endereço IP do servidor de backup2. Aparece como "Endereço de destino" de painéis de propriedades backup2on. Aplica-se a todos os tipos de sessão.	Nome do host ou endereço IP.
Port	O número da porta na qual o servidor de destino está em escuta. Aparece como "Porta de destino" nos painéis de propriedades. Aplica-se a todos os tipos de sessão.	Qualquer número de porta TCP/IP válido.
PortBackup1	O número da porta na qual o servidor de backup1 está atendendo. Aparece como "Porta de destino" de backup1 nos painéis de propriedades. Aplica-se a todos os tipos de sessão.	Qualquer número de porta TCP/IP válido.
PortBackup2	O número da porta na qual o servidor de backup2 está atendendo. Aparece como "Porta de destino" de backup2 nos painéis de propriedades. Aplica-se a todos os tipos de sessão.	Qualquer número de porta TCP/IP válido.

Tabela 12. Propriedades da Sessão que Podem Ser Substituídas (continuação)

Nome do Parâmetro	Descrição	Valores Válidos
CodePage	A página de códigos do servidor ao qual a sessão se conectará. Aparece como "Página de Códigos do Host" nos painéis de propriedades. Aplica-se a todos os tipos de sessão, exceto FTP.	A parte numérica (por exemplo, 037) da página de códigos suportada pelo host listada no painel de propriedades de sessão.
SessionID	O nome abreviado que você deseja atribuir a esta sessão (aparece no OIA). Deve ser exclusivo para esta configuração. Aparece como "ID de Sessão" nos painéis de propriedades. Aplica-se a todos os tipos de sessão.	Um caractere: A-Z.
LUName	O nome da LU ou Conjunto de LUs, definido no servidor de destino, ao qual você deseja conectar esta sessão. Aparece como "Nome da LU ou do Conjunto" nos painéis de propriedades. Aplica-se aos tipos de sessão Terminal 3270 e Impressora 3270.	O nome de uma LU ou Conjunto de LUs.
LUNameBackup1	O nome da LU ou Conjunto de LUs, definido no servidor de backup1, ao qual você deseja conectar esta sessão. Aparece como "Nome da LU ou do Conjunto" de backup1 nos painéis de propriedades. Aplica-se aos tipos de sessão Terminal 3270 e Impressora 3270.	O nome de uma LU ou Conjunto de LUs.
LUNameBackup2	O nome da LU ou Conjunto de LUs, definido no servidor de backup2, ao qual você deseja conectar esta sessão. Aparece como "Nome da LU ou do Conjunto" de backup2 nos painéis de propriedades. Aplica-se aos tipos de sessão Terminal 3270 e Impressora 3270.	O nome de uma LU ou Conjunto de LUs.

Tabela 12. Propriedades da Sessão que Podem Ser Substituídas (continuação)

Nome do Parâmetro	Descrição	Valores Válidos
WorkstationID	O nome desta estação de trabalho. Aparece como "ID da Estação de Trabalho" nos painéis de propriedades. Aplica-se aos tipos de sessão Terminal 5250 e Impressão 5250.	Um nome exclusivo para esta estação de trabalho.
ScreenSize	Define o número de linhas e colunas na tela. Aparece como "Tamanho da Tela" nos painéis de propriedades. Aplica-se aos tipos de sessão Terminal 3270, Terminal 5250 e Terminal VT.	<ul style="list-style-type: none"> • valor=linhas x colunas • 2=24x80 (3270, 5250, VT) • 3=32x80 (3270) • 4=43x80 (3270) • 5=27x132 (3270, 5250) • 6=24x132 (VT) • 7=36x80 (VT) • 8=36x132 (VT) • 9=48x80 (VT) • 10=48x132 (VT) • 11=72x80 (VT) • 12=72x132 (VT) • 13=144x80 (VT) • 14=144x132 (VT) • 15=25x80 (VT) • 16=25x132 (VT)
SLPScope	Escopo de SLP (Service Location Protocol). Aparece como "Escopo" em "Opções de SLP" nos painéis de propriedades. Aplica-se aos tipos de sessão Terminal 3270, Impressora 3270, Terminal 5250 e Impressora 5250.	Entre em contato com o administrador para obter o valor correto para este campo.
SLPAS400Name	Conecta uma sessão a um IBM System i específico. Aparece como "Nome do iSeries (SLP)" em painéis de propriedades. Aplica-se aos tipos de sessão Terminal 5250 e Impressora 5250.	O nome completo do SNA CP (por exemplo, USIBMN.M.RAS400B).
FTPUser	Especifica o ID de usuário que a sessão utiliza ao conectar-se ao servidor FTP. Aparece como "ID do Usuário" nos painéis de propriedades. Aplica-se aos tipos de sessão FTP.	Um ID de usuário válido.

Tabela 12. Propriedades da Sessão que Podem Ser Substituídas (continuação)

Nome do Parâmetro	Descrição	Valores Válidos
FTPPassword	Especifica a senha que a sessão utiliza ao conectar-se ao servidor FTP. Aparece como "Senha" nos painéis de propriedades. Aplica-se aos tipos de sessão FTP.	Uma senha válida.
UseFTPAnonymousLogon	Ativa a sessão para efetuar login em um servidor FTP utilizando anônimo como o ID de usuário. Aparece como "Login Anônimo" nos painéis de propriedades. Aplica-se aos tipos de sessão FTP.	Sim ou Não.
FTPEmailAddress	Especifica o endereço de e-mail a ser utilizado na conexão com o servidor FTP ao utilizar o Login Anônimo. Aparece como "Endereço de e-mail" nos painéis de propriedades. Aplica-se aos tipos de sessão FTP.	Um endereço de e-mail válido.
PromptForDestinationAddress	Especifica se deve solicitar ao usuário o endereço de destino para utilizar ao conectar-se com o servidor FTP. Aparece como "Endereço de Destino" nos painéis de propriedades. Aplica-se aos tipos de sessão FTP.	sim ou não
CICSInitialTransEnabled	Permite que uma transação inicial seja iniciada quando uma sessão CICS Gateway é estabelecida.	verdadeiro ou falso
CICSInitialTrans	Especifica o nome da transação inicial a ser iniciada na conexão a um host CICS. Aplica-se apenas às sessões CICS Gateway. O parâmetro CICSInitialTransEnabled deve ser definido como true para a transação especificada ser iniciada.	Os identificadores de transação válidos são cadeias entre 1 e 128 caracteres. A cadeia identifica a transação inicial e todos os parâmetros a serem executados na conexão ao servidor. Os primeiros quatro caracteres ou os caracteres até o primeiro espaço em branco na cadeia são tidos como a transação. Os dados restantes são transmitidos para a transação em sua chamada.

Tabela 12. Propriedades da Sessão que Podem Ser Substituídas (continuação)

Nome do Parâmetro	Descrição	Valores Válidos
Netname	O nome do recurso de terminal a ser instalado ou reservado. Se este campo estiver em branco, o tipo de terminal selecionado não será previsível. Aplica-se apenas às sessões CICS.	Um nome de recurso de terminal válido.

Todos os erros encontrados no processamento dos parâmetros HTML são exibidos no Console Java.

Exemplo nº1: Substituindo o Nome da LU Baseado no Endereço IP do Cliente

Os administradores podem querer evitar especificar nomes de LU diretamente nas definições de sessão. Este exemplo mostra uma maneira simples de utilizar o endereço IP do cliente para procurar um nome de LU listado em um arquivo de texto e utilizá-lo como um valor de substituição em uma sessão.

Este exemplo foi escrito utilizando JSP. O Deployment Wizard foi utilizado para criar um arquivo HTML que contém duas sessões, denominadas Terminal 3270 e Terminal 5250. Observe que no Host On-Demand 7 e posterior, alguns dos HTMLs são gerados utilizando JavaScript, e os parâmetros HTML são especificados em uma matriz JavaScript ou utilizando as instruções document.write do JavaScript. Além disso, o formato do HTML varia de acordo com o cliente (cliente em cache ou de download) selecionado.

Este exemplo usa uma página Java em cache a ser iniciada com as mudanças necessárias para substituições HTML em negrito. Quando o Deployment Wizard é utilizado para gerar uma página Java2 armazenada em cache, ele gera os seguintes arquivos:

- Example1.html
- z_Example1.html
- Example_J2.html

Um cliente Macintosh utiliza a página Example_J2.html.

É lido um arquivo (c:\luname.table) contendo pares de endereço IP/nome da LU. O endereço IP do cliente é utilizado para procurar o nome de LU apropriado, que é substituído na sessão "3270 Display". Consulte os comentários no exemplo para obter mais detalhes. As linhas incluídas na saída do Deployment Wizard são exibidas em **negrito**.

```
<!doctype html public "-//W3C//DTD HTML 3.2 Final//EN">
<%
// Read the luname.table file into a properties variable.
// O arquivo luname.table contém linhas no seguinte formato:
//   ipAddress=luname
Properties lunames = new Properties();
lunames.load(new FileInputStream("c:\\luname.table"));
%>
<HTML>
<HEAD>
<META http-equiv="content-type" content="text/html; charset=UTF-8">
<!-- TITLE Begin -->
<TITLE>Example1 page title</TITLE>
```

```

<!-- TITLE End -->
<!-- SUMMARY Begin -->
<!--
Modelo de Configuração
Qual modelo de configuração você gostaria de usar?
-Modelo baseado em HTML
Sessões de Host
-3270 Display
-5250 Display
Opções Adicionais
-Em Cache = Cliente em cache
-Tipo Java = java2
Desativar Funções
Opções de Pré-carregamento
-Sessões 5250 = True
-Alterar Propriedades da Sessão = True
-Sessões 3270 = True
Opções Cliente em Cache/Web Start
Opções Básicas
-Depurar = False
-Altura (em pixels) = 250
-Largura (em pixels) = 550
Opções de Upgrade
-Percentual de usuários que podem fazer upgrade, por padrão = 100
-Usuário de prompt (usuário decide primeiro plano ou plano de fundo)
Opções Avançadas
Parâmetros HTML
-Nenhum
Base de código
- /hod/
Modelos HTML
-Padrão
Determinação de problema
-Depurar = False
Atualizações do usuário
-Persistir atualizações do usuário? = True
Aparência
-Cliente Padrão do Host On-Demand
Tamanho do applet
-Dimensionamento automático do navegador
API do Gerenciador de Sessão
-Ativar API JavaScript do Gerenciador de Sessão = False
Conexão do servidor
Idioma
-Código do Idioma = Usar o Código do Idioma do sistema
Sessões máximas
- 26
-->
<!-- SUMMARY End -->
</HEAD>

<BODY BACKGROUND="/hod/hodbkgnd.gif">
<CENTER>
<IMG src="/hod/hodlogo.gif" ALT="hodlogo.gif">
<P>

<SCRIPT LANGUAGE="JavaScript">
function writeAppletParameters()
{
    return "";
}
</SCRIPT>

<SCRIPT LANGUAGE="JavaScript" SRC="/hod/HODVersion.js"></SCRIPT>
<SCRIPT LANGUAGE="JavaScript" SRC="/hod/CommonJars.js"></SCRIPT>
<SCRIPT LANGUAGE="JavaScript" SRC="/hod/CommonParms.js"></SCRIPT>
<SCRIPT LANGUAGE="JavaScript" SRC="/hod/CommonJ2Parms.js"></SCRIPT>
<SCRIPT LANGUAGE="JavaScript">
var db = parent.location;
var hod_Locale = '';
var hod_AppName = '';
var hod_AppHgt = '340';
var hod_AppWid = '550';
var hod_CodeBase = '/hod/';
var hod_Comps = 'HABASE;HODBASE;HODIMG;HACP;HAFNTIB;HAFNTAP;HA3270;HODCFG;HA5250';
var hod_Archs = 'habasen.jar,hodbasen.jar,hodimg.jar,hacp.jar,hafntib.jar,hafntap.jar,
ha3270n.jar,hodcfgn.jar,ha5250n.jar';

```

```

var hod_URL = new String(window.location);
var hod_DebugOn = false;

// colocar parâmetros de applet de instalação do cliente em cache aqui
var hHod_AppletParams = nova Matriz;
hHod_AppletParams[0] = '<PARAM NAME="DebugCachedClient" VALUE="false">';
hHod_AppletParams[1] = '<PARAM NAME="ShowDocument" VALUE="parent">';
hHod_AppletParams[2] = '<PARAM NAME="CachedClient" VALUE="true">';
hHod_AppletParams[3] = '<PARAM NAME="ParameterFile" VALUE="HODData\\Example1\\params.txt">';
hHod_AppletParams[4] = '<PARAM NAME="JavaScriptAPI" VALUE="false">';
hHod_AppletParams[5] = '<PARAM NAME="BookmarkPage" VALUE="Example1.html">';

// The next 2 lines are required in order to override session properties.
// A primeira linha ativa o processamento para esta função e não
// precisa ser modificada. A segunda linha identifica as sessões que você
// deseja alterar. Neste exemplo, há duas sessões identificadas
// denominadas: "3270 Display" e "5250 Display".

hHod_AppletParams[6]='<PARAM NAME="EnableHTMLOverrides" VALUE="true">';
hHod_AppletParams[7]='<PARAM NAME="TargetedSessionList" VALUE="3270 Display,5250 Display">';

// A seguinte linha altera o parâmetro de sessão LUName para a sessão denominada
// "3270 Display". Neste exemplo, o LUName está sendo configurado como o valor
// contido no c:\luname.table para o endereço IP do cliente.
// Quando você estiver testando inicialmente suas mudanças, poderá desejar usar um valor
// constante para verificar se a sintaxe está correta, antes de inserir seus // cálculos.
hHod_AppletParams[8]='<PARAM NAME="Luname" VALUE="3270
Display=<%=lunames.get(request.getRemoteAddr())%>">';

//hHod_AppletParams[x] = '<PARAM NAME="DebugCode" VALUE="65535">';

var pg = buildJ2Page(db);
pg += writeAppletParameters();
pg += '</APPLET>';
if(hod_DebugOn) alert('J2 page complete, result = \n' + pg);
document.write(pg);
</SCRIPT>

</CENTER>
</BODY>
</HTML>

```

Exemplo nº2: Permitindo que o Usuário Especifique o Host de Conexão Utilizando um Formulário HTML

Os administradores também podem querer utilizar formulários HTML para especificar valores de substituição em vez de calculá-los. O exemplo a seguir exibe um formulário simples para entrada de um nome de host. O formulário é postado em um programa JSP que utiliza o nome do host especificado no formulário para substituir o nome do host na Sessão 3270.

Este exemplo foi escrito utilizando JSP. O Deployment Wizard foi utilizado para criar um arquivo HTML que contém duas sessões, denominadas "3270 Display" e "5250 Display". Observe que no Host On-Demand 7 e posterior, alguns dos HTMLs são gerados utilizando JavaScript, e os parâmetros HTML são especificados em uma matriz JavaScript ou utilizando as instruções document.write do JavaScript. Além disso, o formato do HTML varia de acordo com o tipo de cliente (cliente em cache ou de download) selecionado.

Na utilização de formulários, os dados do formulário precisam ser retidos através de pedidos ao programa. Isso porque os arquivos HTML do Host On-Demand se recarregam para detecção de Java e para suporte a marcadores durante a utilização de páginas do modelo baseado no servidor de configuração. Se Java 1 for selecionado e o suporte para marcadores estiver desativado se estiver sendo utilizado o modelo baseado no servidor de configuração, a página não precisará

ser recarregada e não haverá necessidade de reter os dados do formulário. Este exemplo utiliza uma sessão JSP para armazenar os dados do formulário através de recarregamentos.

Segue um formulário HTML simples que permite a entrada de um nome de host. O formulário é postado no programa JSP (example2.jsp):

```
<form method="POST" action="hod/example2.jsp">
Hostname <input name="form.hostname"><br>
<input type="submit">
</form>
```

Segue a saída modificada a partir do Deployment Wizard. Consulte os comentários no exemplo para obter mais detalhes. As linhas incluídas na saída do Deployment Wizard são exibidas em **negrito>**

```
<HTML>
<%
// Get a session or create if necessary and store the hostname
// entered in the form in the session.
HttpSession session = request.getSession(true);
String hostname = request.getParameter("form.hostname");
if (hostname!=null) {
session.putValue("session.hostname", hostname);
}
%>
<!-- HOD WIZARD HTML -->
<!-- Deployment Wizard Build : 8.0.0-B20030605 -->
<HEAD>
<META http-equiv="content-type" content="text/html; charset=UTF-8">
<TITLE>Example 2 page title</TITLE>
<SCRIPT LANGUAGE="JavaScript" SRC="/hod/CommonJars.js"></SCRIPT>
<SCRIPT LANGUAGE="JavaScript" SRC="/hod/HODJavaDetect.js"></SCRIPT>
<SCRIPT LANGUAGE="JavaScript" SRC="/hod/CommonParms.js"></SCRIPT>
<SCRIPT LANGUAGE="JavaScript">

//---- Start JavaScript variable declarations ----//
var hod_Locale = '';
var hod_jsapi=false;
var hod_AppName = '';
var hod_AppHgt = '80%';
var hod_AppWid = '80%';
var hod_CodeBase = '/hod/';
var hod_FinalFile = 'z_example2.html';
var hod_JavaType = 'java2';
var hod_Obplet = '';
var hod_jars = 'habasen.jar,hodbasen.jar,hodimg.jar,hacp.jar,hodsiggn.jar,ha3270n.jar,
               hodcfgn.jar,ha5250n.jar';

var hod_URL = new String(window.location);
var hod_DebugOn = false;
var hod_SearchArg = window.location.search.substring(1);

var hod_AppletParams = new Array;
hod_AppletParams[0] = '<PARAM NAME="ParameterFile" VALUE="HODData\\example2\\params.txt">';
hod_AppletParams[1] = '<PARAM NAME="ShowDocument" VALUE="parent">';
hod_AppletParams[2] = '<PARAM NAME="JavaScriptAPI" VALUE="' + hod_jsapi + '>';
hod_AppletParams[3] = '<PARAM NAME="PreloadComponentList" VALUE="HABASE;HODBASE;HODIMG;
                        HACP;HAFNTIB;HAFNTAP;
                        HA3270;HODCFG;HA5250">';

// The next 2 lines are required in order to override session properties.
// The first line turns on the processing for this function and does not
// need to be modified. The second line identifies the sessions that you
// want to change. In this example, there are 2 sessions identified
// named: "3270 Display" and "5250 Display".
// Be careful to increment the array index correctly.

hod_AppletParams[4] = '<PARAM NAME="EnableHTMLOverrides" VALUE="true">;
hod_AppletParams[5] = '<PARAM NAME="TargetedSessionList" VALUE="3270 Display,5250 Display">;

// The following line changes the Host or Destination Address session parameter
// for the session named "3270 Display". In this example, the Host is being set
// to the value saved in the JSP session from the HTML form.
// When you are initially testing your changes, you may want to use a constant
// value to verify that the syntax is correct before you insert your
```

```

// calculations.
// Here we override the host for the 3270 session to the value saved in the
// jsp session from the html form.

hod_AppletParams[6] = <PARAM NAME="Host" VALUE="3270
                        Display=<%=session.getValue("session.hostname")%>">;

//hod_AppletParams[x] = '<PARAM NAME="DebugCode"    VALUE="65535">';

//---- End JavaScript variable declarations ----//

function getHODMsg(msgNum) {
    return HODFrame.hodMsgs[msgNum];
}

function getHODFrame() {
    return HODFrame;
}

var lang = detectLanguage(hod_Locale);
document.writeln('<FRAMESET cols="*,10" border=0 FRAMEBORDER="0">');
document.writeln('<FRAME    src="/hod/hoddetect_' + lang + '.html" name="HODFrame">');
document.writeln('</FRAMESET>');

</SCRIPT>
</HEAD>
</HTML>

```

Capítulo 14. Configurando o Host On-Demand no zSeries

Este capítulo descreve como configurar diretórios particulares e públicos de leitura/gravação separados para configurar o Host On-Demand em um sistema zSeries.

O objetivo deste cenário de configuração é fornecer instruções para tarefas de configuração comuns do zSeries.

Configurando Diretórios de Publicação e Privados de Leitura/Gravação Separados

Configurar um Sistema de arquivos separado para o diretório privado do Host On-Demand

Quando o Host On-Demand é instalado, arquivos no diretório */usr/lpp/HOD/hostondemand/private* são atualizados em um ambiente de execução, não apenas fabricando liberações de atualização. Como esse diretório agora é atualizado durante a execução do software Host On-Demand, é recomendado que monte um Sistema de arquivos (sem serviço) separado. Você pode fazer isso de uma das seguintes formas:

- MONTE o Sistema de arquivos separado no local do diretório privado atual, como */usr/lpp/HOD/hostondemand/private*.
- Crie um link simbólico para a localização de diretório privada, da seguinte forma:
 1. Execute um TSO MKDIR para criar um ponto de montagem diferente, como */etc/HOD/private*.
 2. Renomeie, ou faça backup e exclua, seu diretório privado original.
 3. Crie um link simbólico a partir do local esperado, */usr/lpp/HOD/hostondemand/private*, para apontar para o local real, */etc/HOD/private*. Utilize o seguinte comando de link:

```
In -s /etc/HOD/private /usr/lpp/HOD/hostondemand/private
```

Se estiver usando LDAP e autenticação nativa, copie manualmente o HODrapd e o diretório */keys* no diretório */private* específico do sistema.

Quando o diretório */private* específico do sistema é montado, ele se sobrepõe, mas não destrói o diretório */private* principal. Quando as liberações de manutenção forem aplicadas, use o diretório */private* principal. Se esses arquivos forem mudados, copie-os no diretório */private* específico do sistema.

Configurar um Diretório de Publicação do Usuário Separado

Os arquivos gerados no Deployment Wizard podem ser colocados em um diretório definido pelo usuário que é separado do diretório de publicação do Host On-Demand. Isso facilita a aplicação de futuros upgrades do Host On-Demand. Esta solução mantém o diretório de publicação do Host On-Demand somente para leitura e fornece uma localização gravável separada para implementar arquivos do Deployment Wizard.

Para obter instruções sobre a implementação dos arquivos do Assistente de Implementação em um diretório de publicação do usuário separado e para obter informações sobre outros arquivos modificados pelo usuário que podem ser colocados fora do diretório de publicação, consulte a instrução de migração do assistente de implementação.

É possível criar e montar um sistema de arquivos separado para o diretório de publicação definido pelo usuário. O arquivo zip do Assistente de Implementação gerado deve ser transferido para esse diretório e descompactado em zip pelo utilitário DWUnzip. O servidor da web precisa incluir uma instrução de alias específica ao diretório de publicação definido pelo usuário.

É possível acessar a página por meio da URL que especifica o alias do local de publicação definido pelo usuário. Por exemplo, se o diretório de publicação for `/usr/lpp/HOD/publish` e o alias for `userpublish`, a URL para acessar a página do cliente seria `http://<servername>/userpublish/<pagename>.html`.

Considerações sobre Migração para z/OS

Ao fazer upgrade de um nível anterior do Host On-Demand, para o Host On-Demand V12.0, é necessário considerar a customização anterior. Diferente de migrações anteriores, não é possível instalar o HOD V12.0 sobre um nível anterior do Host On-Demand, porque o Installation Manager é usado para instalar o HOD Versão 12 e é necessário iniciar com um sistema de arquivos vazio. Após o HOD V12.0 ser instalado, é possível copiar seu diretório privado anterior no novo diretório privado para quaisquer Grupos e Usuários e sessões definidas anteriormente. Em seguida, use o comando `pax` ou `tar` para copiar seu diretório privado existente no Sistema de arquivos HOD V12.0. Consulte “Fazendo Backup do Diretório Privado”.

Quanto aos clientes anteriores criados com o Assistente de Implementação, é necessário instalar o Assistente de Implementação em um computador Windows. Em seguida, edite e reimplemente o cliente para o servidor HOD V12.0. Consulte “Instalando o Assistente de Desenvolvimento a partir do servidor z/OS” na página 119.

Fazendo Backup do Diretório Privado

O diretório privado pode ser submetido a backup usando o comando `pax` ou o comando `tar`. Suponha que o diretório privado atual para HOD V11 seja `/usr/lpp/HOD/hostondemand/private`:

1. A partir do Sistema de arquivos do Host On-Demand V11, mude o diretório para o diretório privado: `cd /usr/lpp/HOD/hostondemand/private`.
2. Arquive o diretório privado em um diretório `/tmp`. A opção `-z` compacta o arquivo; `-v` fornece uma lista de arquivos e subdiretórios que estão sendo arquivados (opcional): `pax -wzvf /tmp/private.pax.Z *`.
3. Copie o arquivo `private.tar.Z` no diretório `/tmp` no sistema para Host On-Demand V12, se for um sistema diferente.
4. No Host On-Demand V12.0 HFS, mude o diretório para o diretório privado em que o arquivo será extraído: `cd /usr/lpp/HOD/hostondemand/private`.
5. Emita o comando `pax` para extrair o arquivo `private.pax.Z`. A opção `-z` especifica um arquivo compactado; `-v` fornece uma lista de arquivos e subdiretórios que estão sendo extraídos (opcional): `pax -rzvf /tmp/private.pax.Z`.

Instalando o Assistente de Desenvolvimento a partir do servidor z/OS

O Assistente de Implementação normalmente localiza-se em uma máquina Windows durante a instalação do produto. No z/OS, um download é fornecido para que você instale o Assistente de Implementação no Windows para que possa gerar páginas de cliente para o servidor z/OS HOD. Consulte as etapas a seguir para instalar o Assistente de Implementação a partir do servidor z/OS:

1. Use FTP em binário para relocalizar este arquivo de uma estação de trabalho do Windows: */usr/lpp/HOD/hostondemand/HOD/depwiz/DW.zip*.
2. Extraia o arquivo zip para uma pasta.
3. Para iniciar a instalação, acesse *<folder>\DeploymentWizard\disk1* em Explorar.
4. Clique duas vezes em *imLauncherWindows.bat* para ativar a interface com o usuário do Installation Manager.
5. Siga as instruções para concluir a instalação.

Depois que o Assistente de Implementação está instalado, é possível ativá-lo. Acesse **Iniciar > Todos os programas > Assistente de Implementação do IBM Host On-Demand**.

Capítulo 15. Configurando o Host On-Demand no IBM System i

Após instalar o Host On-Demand na plataforma IBM System i, configure o software como a seguir:

- Para configurar o Gerenciador de Serviços, siga as instruções em “Configurando, iniciando e parando o Gerenciador de Serviços do Host On Demand no IBM System i”.
- Para usar o Assistente de Implementação com um sistema IBM System i, siga as instruções em “Usando o Assistente de Implementação com o IBM System i” na página 124.
- Para configurar a segurança, siga as instruções em “Configurando servidores IBM System i para conexão segura” na página 125.
- Para entender os requisitos para suporte Unicode utilizando os Identificadores de Conjuntos Codificados de Caracteres, consulte “Suporte a Unicode para i/OS e OS/400” na página 128.

Configurando, iniciando e parando o Gerenciador de Serviços do Host On Demand no IBM System i

É fornecido um menu para iniciar e parar o Gerenciador de Serviços do Host On-Demand. Para acessar o menu, digite o seguinte na linha de comandos do i/OS ou OS/400:

```
GO HOD
```

Os comandos a seguir podem ser usados a partir da linha de comandos do IBM iv7r1 ou OS/400.

Configurar

É possível usar o arquivo de script `NCServiceManager-OS400.sh` para configurar o Gerenciador de Serviços. `NCServiceManager-OS400.sh` está localizado no diretório a seguir no IBM System i:

```
HOD_install_directory>/lib/samples/NCServiceManager/.
```

Para definir as configurações do Gerenciador de Serviços, execute as tarefas a seguir:

1. Acesse o diretório `<HOD install directory>/lib/samples/NCServiceManager/`. Aqui, `<HOD install directory>` é o local ou caminho em que o Host On-Demand foi instalado. Por exemplo, `/QIBM/ProdData/HostOnDemand/`.
2. Abra o arquivo `NCServiceManager-OS400.sh`.
3. Verifique se as variáveis de tempo de execução estão corretas e correspondem ao seu ambiente. Altere os valores padrão das variáveis de tempo de execução se não corresponderem a seu ambiente. Estes incluem os seguintes:
 - Local do JRE: `JAVA_ENGINE`
Atualize o valor de `JAVA_ENGINE` para o caminho completo ou local do jre instalado no sistema. Ele deve ser Java V6 ou superior. Ele deve apontar para `<java_installation>/bin/java` no diretório de instalação Java.
 - Local do diretório de publicação Host On-Demand no servidor:
`MY_HOD_DIRECTORY`

Verifique e atualize, se necessário, o valor de MY_HOD_DIRECTORY para o caminho completo do diretório de instalação do HostOnDemand. Ele deve ser o diretório de instalação do Host On-Demand e o diretório contém /bin, /lib e outras pastas do Host On-Demand. Geralmente, esse valor é atualizado uma vez no momento da instalação. Por exemplo, /QIBM/ProdData/HostOnDemand.

- Caminhos de destino especificados no arquivo de comando:

MY_PUBLISHED_DIRECTORY

Verifique e atualize, se necessário, o valor de MY_PUBLISHED_DIRECTORY para o caminho completo do diretório de publicação do Host On-Demand. Geralmente, é o diretório <HOD_Installation>/HOD, em que <HOD_Installation> é o diretório de instalação do Host On-Demand.

4. Confirme se NCSERVICE_MANAGER-OS400.SH tem as permissões de execução necessárias e está autorizado a gravar em diretórios na instalação do Host On-Demand no servidor.

Iniciar

Para iniciar o Gerenciador de Serviços do Host On Demand, execute NCSERVICE_MANAGER-OS400.SH para que inicie e continue a executar em segundo plano.

Uma forma de fazer isso no IBM i Series é enviar uma tarefa chamando o IBM PASE for System i para executar o script. Entre em contato com o administrador IBM i Series para obter os detalhes sobre as melhores formas de enviar uma tarefa adequada a sua configuração e requisitos do i Series.

Um exemplo de comando que envia uma tarefa:

```
sbmjob cmd(call pgm(qp2shell) parm('/QOpenSys/usr/bin/-sh'  
'/QIBM/ProdData/HostOnDemand/lib/samples/NCSERVICE_MANAGER/NCSERVICE_MANAGER-OS400.SH'))
```

Parar

Para parar o gerenciador de serviços, termine a tarefa em Iseries. Entre em contato com seu administrador Iseries para obter detalhes sobre um método adequado para parar o serviço.

Uma forma de fazer isso é com as etapas de exemplo a seguir:

1. Digite **WRKACTJOB** para abrir uma lista de tarefas ativas.
2. No menu **Trabalhar com tarefas ativas**, a tarefa do gerenciador de serviços do Host On-Demand é listada com o nome da função *JVM-NCSERVICE_M*. Role para baixo no menu para essa entrada de tarefa e selecione a opção **Trabalhar com...**, normalmente opção 5.
3. Selecione a opção **Terminar tarefa**. Para isso, digite *41* para terminar a tarefa e pressione o botão **Enter**. Isso termina a tarefa do gerenciador de serviços e para o gerenciador de serviços.

Trabalhar com Status do HOD Server

Para determinar se o Gerenciador de Serviços está em execução, precisa ser verificado se o programa Java NCSERVICE_MANAGER, que é iniciado pelo script NCSERVICE_MANAGER-OS400.SH, está em execução ou não. Portanto, o método para verificar o status de servidor pode variar de acordo com o método usado para iniciar o gerenciador de serviços.

No exemplo acima, o Gerenciador de Serviços é iniciado enviando uma tarefa para executar o script `NCServiceManager-OS400.sh`. Assim, é possível executar as duas formas a seguir de verificar o status:

1. Use o comando `WRKACTJOB` para revisar o status:

a. Digite o comando:

```
WRKACTJOB
```

Isso fornece uma lista de tarefas ativas.

b. No menu **Trabalhar com tarefas ativas**, a tarefa do gerenciador de serviços do Host On-Demand é listada com o nome da função **JVM-NCServiceM**. Use o botão **PageDown** ou **PageUp** para rolar para baixo no menu para essa entrada de tarefa e insira o número de opção apropriado para a tarefa **Trabalhar com...**, normalmente opção 5.

c. Utilize as opções de menu para revisar o status da tarefa.

2. Consulte o status do processo na linha de comandos.

No exemplo de “Iniciar” na página 122, o script `NCServiceManager-OS400.sh` é executado chamando o IBM PASE for System i (`qp2shell`) no comando `SBMJJOB`. Assim, neste caso, as etapas a seguir também podem ajudar a verificar o status:

1. No IBM System i, efetue sign on para uma linha de comandos de tela verde.

2. b) Insira o ambiente de shell PASE. Na linha de comandos de tela verde, insira o comando a seguir:

```
call qp2term
```

.

3. No shell PASE, digite o comando a seguir:

```
ps -ef | grep NCServ
```

.

Nota: `NCServiceManager` é o nome do programa Java que executa o gerenciador de serviços.

Se o comando detectar que o Gerenciador de Serviços está em execução, ele fornecerá uma saída que se pareceria com o seguinte:

```
$
> ps -ef | grep NCServ
kushald 3146  1  0 15:23:30  -  0:00 /QIBM/ProdData/OS400/Java400/jFr
omPASE java -classpath .:sm.zip:ibmjndi.jar:jndi.jar:jsdk.jar:ods.jar:jt400.j
ar -Djava.net.preferIPv4Stack=true -DFIPS=on com.ibm.eNetwork.HODUtil.service
s.admin.NCServiceManager /QIBM/ProdData/HostOnDemand
$
```

Nota: O shell PASE faz distinção entre maiúsculas e minúsculas. Assim, é importante manter o caso correto das letras no comando (etapa c).

Gerenciamento de Certificados

Funções de gerenciamento de certificado podem ser executadas usando o utilitário `P12Keyring` fornecido pelo Host On-demand. Isso fornece uma forma fácil de criar e implementar um banco de dados de conjunto de chaves SSL. Utilize esta opção para trabalhar com certificados SSL em um dos conjuntos de chaves do Host

On-Demand. Consulte o Capítulo 4, “Planejamento para Segurança”, na página 21 para obter informações gerais sobre sessões relacionadas a SSL.

Informações sobre P12Keyring e seu uso estão disponíveis em Apêndice C. Utilitário de conjunto de chaves P12.

Alguns comandos de amostra podem ser visualizados no link Como criar, incluir ou converter certificados para o arquivo CustomizedCAs.p12 no z/OS para o Host On-Demand.

Iniciar Information Bundler

No caso de precisar entrar em contato com o IBM Support Center para obter assistência, o já disponível arquivo de script do Information Bundler pode ser usado para reunir informações sobre sua configuração do Host On-Demand.

Para obter informações sobre uso, consulte a seção Executando o Information Bundler do documento HOD V10.

Criar tabela de definição de impressora HOD

Crie uma tabela de definição de impressora customizada para sessões de impressora 3270 do Host On-Demand. Para usar esta função, consulte a seção em Compilando um PDT em uma seção do servidor iSeries.

Uma definição de impressora customizada pode ser necessária se tiver um formulário de papel especial ou se a impressora não for suportada. As opções a seguir não estão disponíveis no HOD V12.0:

Usando o Assistente de Implementação com o IBM System i

Para usar o Assistente de Implementação para implementar telas em um servidor Host On-Demand baseado em IBM System i, faça o seguinte:

1. Em uma estação de trabalho do Windows, mapeie uma unidade de rede para o diretório /qibm no sistema IBM System i que é o servidor Host On-Demand. Consulte o website IBM System i para obter mais informações.
2. Faça o download da imagem de instalação do Assistente de Implementação a partir de um servidor Host On-Demand v12 já instalado. Acesse HODMain.html (por exemplo, <http://hodserver.name.com/hod/HODMain.html>) e clique em **Imagem de instalação do Assistente de Implementação para Windows**.
3. Consulte as instruções de instalação para instalar o Assistente de Implementação. É possível executar isso sem ter que instalar o servidor Host On-Demand inteiro.
4. Projete os recursos e seleções personalizados.
5. Salve o arquivo HTML customizado na unidade de rede mapeada (por exemplo, *y:\ProdData\hostondemand\hod\myweb*).
6. Use um navegador para testar o arquivo (por exemplo, <http://iSeries.name.com/hod/myweb.html>).

Configurando servidores IBM System i para conexão segura

Se estiver usando certificados autoassinados ou certificados de uma agência de assinatura que não estejam na lista já conhecida, use o utilitário P12Keyring para configurar o conjunto de chaves CustomizedCAs. Para obter mais detalhes, consulte Apêndice C. Utilitário de conjunto de chaves P12.

Siga as etapas abaixo para configurar o conjunto de chaves CustomizedCAs:

1. Assegure-se de que o java esteja instalado no sistema.
2. Abra uma linha de comandos baseada em unix/AIX. Por exemplo, QSHELL ou shell IBM I PASE.
3. Navegue até a pasta de publicação do Host On-Demand no diretório de instalação do Host On-Demand. Geralmente, é */QIBM/ProdData/HostOnDemand/HOD/*.
4. Digite o comando

```
java -classpath .:your_install_dir/lib/sm.zip com.ibm.hod5ssligh.tools.P12Keyring CustomizedCAs connect myServer.raleigh.ibm.com:702
```

. Este comando pode levar alguns minutos para ser concluído. Se uma senha for solicitada, digite *hod* e pressione **Enter**.
5. Selecione o número do certificado que corresponde à CA (Autoridade de Certificação) que você deseja incluir no conjunto de chaves. Certifique-se de incluir o certificado CA e não o certificado do site. Se a porta não estiver respondendo, consulte Configurando servidores IBM i 7.1 para conexão segura.
6. Repita etapas 3a 5 para cada servidor de destino.

Para visualizar o conteúdo do conjunto de chaves CustomizedCAs, execute as etapas a seguir:

1. Assegure-se de que o java esteja instalado no sistema.
2. Abra um shell baseado em Linux, por exemplo, QSHELL ou shell IBM i PASE.
3. Navegue até a pasta de publicação do Host On-Demand no diretório de instalação do Host On-Demand. Geralmente, é */QIBM/ProdData/HostOnDemand/HOD/*.
4. Digite o comando

```
java -classpath .: your_install_dir/lib/sm.zip com.ibm.hod5ssligh.tools.P12Keyring CustomizedCAs list
```

.

Instalando e configurando o Host On-Demand com TLS no i/OS e OS/400

A lista a seguir fornece uma visão geral resumida das etapas necessárias para instalar e configurar o Host On Demand com TLS:

1. Verifique se todos os requisitos de software e de hardware são atendidos.
2. Instale todos os produtos de software IBM System i necessários. Consulte sua documentação do IBM System i para obter detalhes.
3. Instale todas as PTFs necessárias. As PTFs mais recentes estão localizadas no portal de suporte do IBM eServer System i.
4. Instale e configure o IBM HTTP Server ou o IBM Application Server. Consulte a documentação do produto para obter detalhes.

5. Crie um CA (Autoridade de Certificação) no Gerenciador de Certificados Digitais no IBM Administrative Server ou adquira uma CA pública. Consulte sua documentação do IBM System i para obter detalhes.
6. Configure o TLS no IBM HTTP Server ou IBM Application Server. Consulte a documentação do produto para obter detalhes.
7. Configure o Host On Demand com TLS. Consulte Configurando o TLS na ajuda on-line para obter detalhes.

Configurando um Servidor Telnet para Conexão Segura

Visite IBM System i Knowledge Center e procure *TLS* para saber as etapas necessárias para executar a fim de ativar o TLS. Pode ser necessário repetir as etapas para cada sistema IBM System i7 que desejar usar com conexões seguras.

Configurando o Conjunto de Chaves CustomizedCAs do Host On-Demand

Se estiver usando certificados autoassinados ou certificados de uma agência de assinatura que não estejam na lista já conhecida, use o utilitário P12Keyring para configurar o conjunto de chaves CustomizedCAs. Para obter mais detalhes, consulte Apêndice C. Utilitário de conjunto de chaves P12.

Execute as etapas a seguir para configurar um conjunto de chaves CustomizedCAs:

1. Assegure-se de que o java esteja instalado no sistema.
2. Abra um shell baseado em Linux, por exemplo, QSHELL ou shell IBM I PASE.
3. Navegue até a pasta de publicação do Host On-Demand no diretório de instalação do Host On-Demand. Geralmente, é */QIBM/ProdData/HostOnDemand/HOD/*.
4. Digite o comando

```
java -classpath .:your_install_dir/lib/sm.zip com.ibm.hod5ssligh.tools.P12Keyring
CustomizedCAs connect myServer.raleigh.ibm.com:702
```

Este comando pode levar alguns minutos para ser concluído. Se uma senha for solicitada, digite *hod* e pressione **Enter**.

5. Selecione o número do certificado que corresponde à CA (Autoridade de Certificação) que você deseja incluir no conjunto de chaves. Certifique-se de incluir o certificado CA e não o certificado do site. Se a porta não estiver respondendo, consulte Configurando servidores IBM System I para a conexão segura.
6. Repita etapas 3a 5 para cada servidor de destino.

Para exibir o conteúdo do conjunto de chaves CustomizedCAs, proceda da seguinte forma:

1. Assegure-se de que o java esteja instalado no sistema.
2. Abra um shell baseado em Linux, por exemplo, QSHELL ou shell IBM I PASE.
3. Navegue até a pasta de publicação do Host On-Demand no diretório de instalação do Host On-Demand. Geralmente, é */QIBM/ProdData/HostOnDemand/HOD/*.
4. Digite o comando

```
java -classpath .: your_install_dir/lib/sm.zip com.ibm.hod5ssligh.tools.P12Keyring
CustomizedCAs list
```

.



Se tiver várias máquinas IBM System i e quiser criar um único certificado que todas as máquinas poderão usar, considere a certificação cruzada. Consulte Gerenciando a segurança, APIs de serviços criptográficos e Application System/400 Cryptographic Support/400 Versão 3 para obter informações adicionais sobre a certificação cruzada.

Autenticação do Cliente

Para segurança adicional, considere usar TLS com autenticação de cliente para controlar restritamente quem pode executar Telnet para o seu sistema por meio da Internet. Por exemplo, é possível configurar o servidor Telnet para apenas permitir a autenticação se o certificado de cliente tiver sido emitido por seu IBM System i (por meio do Digital Certificate Manager).

Os certificados de cliente têm um período de validade limitado (por exemplo, 90 dias). Quando o certificado expira, o usuário deve executar um processo de Download de Certificado de Cliente para continuar. Esse processo requer um ID do usuário e senha válidos do IBM System i.



Nem todo software cliente de Telnet é capaz de autenticação de cliente. Quando ativadas, todas as conexões Telnet ativadas por TLS com o IBM System i requerem um certificado de usuário.

Consulte o website IBM System i para obter mais informações.

Configurando o Proxy OS/400 do Host On-Demand para Conexões Seguras

O proxy OS/400 pode ser configurado para criptografar transferência de arquivos e conexões do Database On-Demand. Para isso, o software adicional a seguir deve ser instalado em cada IBM System i de destino:

- IBM Cryptographic Access Provider
- IBM Client Encryption
- Servidores Host
- Digital Certificate Manager

Configurar autorizações de usuário TLS

Você precisa controlar a autorização dos usuários para os arquivos. Para ajudar a atender às responsabilidades legais de TLS, é necessário mudar a autoridade do diretório que contém os arquivos TLS para controlar o acesso de usuário aos arquivos. Para alterar a autoridade, faça o seguinte:

1. Digite o comando `wrklnk '/QIBM/ProdData/HTTP/Public/jt400/*'`
2. Selecione a opção 9 no diretório .
 - a. Assegure que *PUBLIC tenha autoridade *EXCLUDE.
 - b. Forneça aos usuários que precisam de acesso aos arquivos TLS a autoridade *RX para o diretório. Você pode autorizar usuários individuais ou grupos de usuários. Lembre-se que os usuários com autorização especial *ALLOBJ não podem ter o acesso aos arquivos TLS negado.

Serviço Seguro da Web

O servidor Host On-Demand utiliza o servidor Web para fazer download de objetos de programa para o navegador. Essas informações podem ser criptografadas, mas com um impacto considerável sobre o desempenho.

A porta padrão para o serviço da Web seguro é 443. Se essa porta não estiver ativada, a porta 80 será utilizada. Para ativar o serviço da Web seguro, execute as seguintes etapas:

1. A partir de um navegador da web, insira: `http://<server.name>:2001` (em que `<server.name>` é o nome do host TCP/IP do seu IBM System i). Se não puder se conectar, inicie o servidor HTTP com o comando i/OS e OS/400 a seguir:
`STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)`
2. Insira o perfil do usuário e a senha do i/OS ou OS/400 (quando solicitado). É necessário ter autoridades `*ALLOBJ` e `*SECADM` para concluir as atividades de configuração restantes.
3. Clique em IBM HTTP Server para AS/400.
4. Clique em Configuração e Administração.
5. Clique em Configurações.
6. Selecione a configuração CONFIG na lista.
7. Clique em Configuração de Segurança.
8. Para as seleções Permitir conexões HTTP e Permitir conexões TLS:
 - Número da porta (443)
 - Selecione Autenticação de cliente TLS, Nenhuma.
 - Selecione Aplicar.
9. Clique no botão Tarefas do AS/400 no lado esquerdo inferior da tela.
10. Clique em Digital Certificate Manager.
11. Clique em Certificados do Sistema.
12. Clique em Trabalhar com Aplicativos Seguros.
13. Clique em QIBM_HTTP_SERVER_CONFIG; em seguida, clique em Trabalhar com Certificado do Sistema.
14. Clique em Atribuir Novo Certificado.
15. Termine a instância do servidor HTTP de administração com o comando i/OS e OS/400 a seguir:
`ENDTCPSVR SERVER(*HTTP) HTTPSVR(DEFAULT)`
16. Aguarde 10 segundos para o encerramento da instância de HTTP.
17. Inicie a instância do servidor HTTP de administração com o comando i/OS e OS/400 a seguir:
`STRTCPSVR SERVER(*HTTP) HTTPSVR(DEFAULT)`
18. Em um navegador da web, insira `https://server.name/hod/hodmain.html` (em que `server.name` é o nome do host TCP/IP do seu IBM System i).

Para obter mais informações sobre uma grande variedade de tópicos do IBM System i, consulte Arquivos PDF e manuais do IBM i.

Suporte a Unicode para i/OS e OS/400

Informações Gerais

Em uma sessão de exibição 5250, o Host On-Demand suporta a exibição de dados Unicode localizados em campos marcados com CCSIDs (Coded Character Set Identifiers). Para obter mais informações, consulte Suporte a Unicode para i/OS e OS/400 usando Coded Character Set Identifiers.

Informações de Programação do Host

Para obter informações sobre programação, consulte o website IBM System i.

Capítulo 16. Implementando o Host On-Demand com o WebSphere Portal

Como uma alternativa para acessar o Host On-Demand através de um arquivo HTML, os usuários podem acessá-lo através do Portal Server, que é um componente do WebSphere Portal. O Portal Server fornece uma estrutura para conectar extensões de conteúdo conhecidas como *portlets* a um Web site. Os portlets são aplicativos que são executados no Portal Server. Eles organizam o conteúdo de diferentes origens (como Web sites, e-mail e aplicativos de negócios) e o exibem em um único arquivo HTML em uma janela do navegador. Os arquivos WAR gerados pelo Deployment Wizard utilizado para ativar sessões do Host On-Demand podem ser implementados como portlets, permitindo aos usuários acessarem o Host On-Demand através da interface do portal. Se você pretende utilizar o Host On-Demand e o Portal Server em conjunto com um firewall, consulte “Utilizando o Host On-Demand com um Firewall” na página 32. Além disso, se você estiver planejando utilizar recursos de segurança do WebSphere Portal, como o ID do Portal do usuário ou o Portal Server Credential Vault, consulte a *Referência ao Web Express Logon*.

O Host On-Demand e o Portal Server devem ser instalados para executar um portlet do Host On-Demand.

Como o Host On-Demand Funciona com o Portal Server

A Figura 8 mostra como o Host On-Demand funciona com o Portal Server.

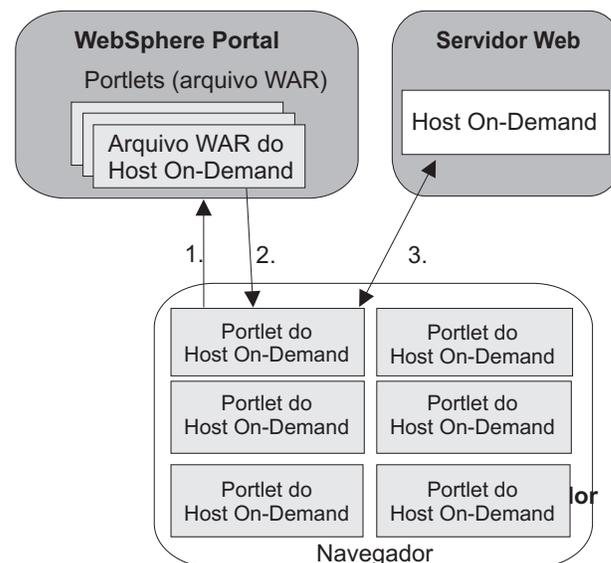


Figura 8. Como o Host On-Demand Funciona com o Portal Server

1. Um usuário efetua login no portal através de um navegador e é autenticado por um ID de usuário e senha.
2. O conjunto de portlets personalizados do usuário é transferido através de download para a máquina do usuário e é exibido no navegador.

3. Se o usuário tiver configurado um portlet do Host On-Demand, o Host On-Demand será iniciado. Isso fornece funcionalidade completa do Host On-Demand para o usuário dentro da janela do portlet, incluindo a capacidade para iniciar sessões e executar outras tarefas do Host On-Demand.

Utilizando Clientes Host On-Demand com o Portal Server

Para utilizar o Host On-Demand com o Portal Server, você precisa de um portlet do Host On-Demand. Você pode criar, de modo rápido e fácil, seus próprios portlets personalizados utilizando o Deployment Wizard. Consulte a ajuda on-line do Deployment Wizard para obter detalhes sobre como criar portlets. Também é possível fazer download dos portlets de amostra do Host On Demand a partir de Chave de serviço do Host On Demand na página de atualização de manufatura do Host On Demand sob Ferramentas e utilitários.

Depois de criar um portlet personalizado ou obter uma amostra, você pode importá-lo diretamente para o Portal Server exatamente como qualquer outro portlet. Consulte WebSphere Portal for Multiplatforms para obter mais detalhes.

Limitações de Acesso ao Host On-Demand Através de um Portlet

O ambiente do Portal suporta a funcionalidade completa do Host On-Demand com as seguintes limitações:

- Embora o Host On-Demand suporte os navegadores de clientes do Mac OS, ele não é recomendado para ambientes de Portal. Para obter mais informações sobre os navegadores suportados, consulte WebSphere Portal for Multiplatform.
- Ao executar vários portlets em uma única página do WebSphere Portal, observe o seguinte:
 - Utilize o modelo de configuração com base em HTML.
 - Use o Java ao configurar portlets como clientes em cache.
 - Configure seus portlets para serem clientes de download ou em cache, não uma mistura dos dois.
- Ao usar um navegador ativado para Java para sessões configuradas para execução em uma janela separada e que tenham o parâmetro `AssociateEmbeddedMenuBar` configurado como `false`, o menu para sessões de host 3270 e 5250 é exibido como um menu pop-up. Para sessões Host Print e FTP, por padrão, o menu pop-up não é exibido. Para exibir o menu para sessões de Host Print e FTP, é necessário configurar as sessões para que sejam iniciadas em uma janela separada.
- Para integrar a barra de menus na sessão do Host On Demand que está configurada para *não* executar em uma janela separada, é necessário ter um navegador ativado para Java e o parâmetro `AssociateEmbeddedMenuBar` configurado como `true` (o padrão). Nas seguintes circunstâncias, a barra de menus para sessões de host 3270, 5250, VT e CICS será exibida como um menu pop-up (e não será incorporada na sessão):
 - O navegador do cliente está ativado com Java e o parâmetro `AssociateEmbeddedMenuBar` está configurado como `false`.

Se a sessão do Host On-Demand estiver configurada para iniciar em uma janela separada, a barra de menus estará sempre associada à janela da sessão e não poderá ser exibida como um menu pop-up.

- Se o portlet utilizar armazenamento em cache para o Host On-Demand (conforme configurado no Deployment Wizard), cada máquina utilizada para acessar o portlet armazenará em cache o cliente Host On-Demand.

- A marcação do Host On-Demand não funciona no ambiente do portal.
- Se o tamanho do applet não for configurado no Deployment Wizard, ele assumirá como padrão o tamanho fixo, médio.
- Quando o portlet do Host On-Demand estiver em execução, você poderá ver mensagens de aviso como `java.io.FileNotFoundException` no Console Java. As mensagens são provocadas por um nome de arquivo fictício que o portlet do Host On-Demand utiliza para ativar vários portlets do Host On-Demand para execução em uma única página do portal. Essas mensagens não afetam o desempenho do portlet, portanto podem ser ignoradas.

Considerações Especiais ao Utilizar um Portlet do Host On-Demand

Ao utilizar o Host On-Demand com o Portal Server, convém considerar as seguintes questões:

- **Sessões do Host On-Demand quando o usuário efetua logout do Portal Server.** O Host On-Demand é executado como um applet na máquina do usuário e, portanto, não reconhece quando o usuário efetua logout do Portal Server. Se a sessão estiver sendo executada em uma janela separada (padrão), a sessão do Host On-Demand continuará até que o usuário feche a sessão ou feche o navegador. Se a sessão do Host On-Demand estiver sendo executada incorporada na janela do Portal Server e o usuário efetuar logout do Portal Server, a sessão pode mostrar-se encerrada, embora a conexão permaneça até que a janela do navegador seja fechada. É altamente recomendável que os usuários fechem a janela do navegador quando efetuam logout do Portal Server. Além disso, você pode configurar um tempo limite de inatividade de sessão para as suas sessões.
- **Tempo limite de inatividade de sessão.** Por padrão, o Host On-Demand não força um tempo limite nas conexões de sessão. No entanto, ao executar um portlet, pode ser vantajoso definir o tempo limite de sessões inativas para reduzir o consumo de recursos. O tempo limite de inatividade pode ser definido para a maioria dos tipos de emulador, incluindo sessões de terminal e impressora 3270, sessões de terminal e impressora 5250 e VT. Você pode ativar e definir o parâmetro de Tempo limite de Inatividade da Sessão em minutos para cada uma dessas sessões na janela Conexão de Propriedades da Sessão.
- **Instalar o WebSphere Portal e o Host On-Demand em servidores diferentes.** Se você instalar o WebSphere Portal e o Host On-Demand em servidores diferentes, determinados navegadores podem registrar uma violação de segurança ao acessar o portlet do Host On-Demand. O problema ocorre porque alguns aspectos do Host On-Demand dependem funcionalmente, de forma maciça, da interação entre o Java (do servidor Host On-Demand) e o JavaScript (do WebSphere Portal) e alguns navegadores não permitirão a interação simplesmente porque eles advêm de servidores diferentes. Uma solução é utilizar o proxy para parecer ao navegador que o WebSphere Portal e o Host On-Demand estão no mesmo servidor. Segue um exemplo das etapas a serem seguidas para configurar o proxy no servidor Apache/IBM HTTP:
 1. Configure a "URL do HOD Server" (`hodCodeBase`) do portlet do Host On-Demand para apontar para o host no qual o WebSphere Portal reside, com a raiz de contexto `/hod/` (por exemplo, `http://portal.empresa.com/hod`).
 2. Desmarque como comentário (remova o `#`) a linha no `httpd.conf` que começa com `LoadModule proxy_module`.
 3. Inclua uma regra ProxyPass no `httpd.conf` para converter o pedido de URL do HOD Server para um pedido do servidor Host On-Demand real (por exemplo, `ProxyPass /hod/ http://hod.empresa.com/hod/`).

4. Reinicie o servidor Web.

- Agora, o navegador do cliente solicitará arquivos do Host On-Demand a partir do mesmo host que o portal, mas esses pedidos serão roteados de novo internamente pelo servidor Web para a localização real da instalação do Host On-Demand.
- **Armazenamento em cache vs. não-armazenamento em cache.** A definição padrão no Deployment Wizard é armazenar em cache o Host On-Demand na máquina de cada usuário. Muitos clientes gostam desta opção com o Host On-Demand porque ela instala efetivamente todo o código necessário na máquina do usuário e não requer carregamentos de rede toda vez que o usuário acessa o portlet ou arquivo HTML. No entanto, o comportamento de armazenamento em cache pode não ser familiar para muitos usuários do Portal Server e, portanto, pode-se optar por rejeitar a opção de armazenamento em cache.
- **Escolher o modelo do Deployment Wizard.** O modelo escolhido para o portlet (Servidor de Configuração, HTML ou Combinado) refletirá o local em que as sessões serão configuradas e determinará como as alterações do usuário serão armazenadas. Embora o Host On-Demand trate os portlets da mesma maneira que os arquivos HTML, considere as seguintes características quando decidir como configurar o portlet:
 - Modelo HTML: este modelo é o modelo de configuração recomendado para portlets do Host On-Demand. Ele não tem nenhuma dependência no servidor de configuração do Host On-Demand. Se os usuários tiverem permissão para fazer atualizações, essas atualizações serão armazenadas como parte da configuração do WebSphere Portal e não na máquina local do usuário. Isso permite que os usuários mudem de uma máquina para máquina e ainda tenham acesso às atualizações.



As preferências dos usuários serão armazenadas no WebSphere Portal apenas se você tiver concedido o acesso apropriado aos usuários para o portlet e para a página da Web que acessará o portlet. Os usuários do WebSphere Portal devem possuir acesso de Usuário privilegiado, de Editor, de Gerenciador ou de Administrador. Para obter informações adicionais sobre como conceder acesso aos usuários, consulte a documentação do WebSphere Portal.

- Modelo de configuração com base no servidor: este modelo requer que os usuários acessem o servidor de configuração do Host On-Demand. Ele permite que os usuários mudem de uma máquina para outra e ainda vejam as modificações da sessão feitas por eles. No entanto, ele requer que os usuários sejam autenticados por meio do servidor de configuração do Host On-Demand e do WebSphere Portal.
- Modelo combinado: este modelo requer que os usuários tenham acesso ao servidor de configuração do Host On-Demand para obter as configurações iniciais da sessão. Como as alterações dos usuários são armazenadas como parte da configuração do WebSphere Portal e não localmente, ele permite que os usuários mudem de uma máquina para a outra e ainda vejam todas as modificações da sessão que fizeram. No entanto, ele requer que os usuários sejam autenticados pelo servidor de configuração do Host On-Demand e pelo WebSphere Portal.



As preferências dos usuários serão armazenadas no WebSphere Portal apenas se você tiver concedido o acesso apropriado aos usuários para o portlet e para a página da Web que acessará o portlet. Os usuários do WebSphere Portal V5 devem possuir acesso de Usuário Privilegiado, de Editor, de Gerenciador ou de Administrador. Para obter informações adicionais sobre como conceder acesso aos usuários, consulte a documentação do WebSphere Portal.

- **Configurando parâmetros adicionais.** Ao utilizar os portlets do Host On-Demand, você pode desejar configurar os seguintes parâmetros adicionais para obter a aparência desejada na página do portal:
 - Iniciar Automaticamente: defina esta opção como Sim na janela Preferências > Opções Iniciais das propriedades da sessão para permitir que o portlet do Host On-Demand seja iniciado automaticamente.
 - Iniciar em Janela Separada: defina essa opção como Não na janela Preferências > Opções Iniciais das propriedades da sessão para permitir que o portlet do Host On-Demand seja exibido como um portlet incorporado.
 - Ocultar o Desktop do HOD na Inicialização: selecione essa opção na janela Opções Avançadas > Aparência para ocultar o desktop do Host On-Demand.
- **Especificando nomes de portlets exclusivos no Portal Server.** Utilize o campo Título de Página na página Nome de Arquivo e Formato de Saída no Deployment Wizard, para especificar nomes de portlets exclusivos dentro do Portal Server.

Estendendo os Portlets do Host On-Demand

Em determinadas circunstâncias, você pode querer modificar a aparência ou funcionalidade dos portlets do Host On-Demand. Seguem algumas dicas e instruções para ajudar a estender os portlets:

- Os arquivos modelo do portlet estão localizados no subdiretório do portal de seu diretório de publicação do Host On-Demand (ou no diretório de instalação do Deployment Wizard, se tiverem sido instalados separadamente). A modificação desses modelos afetam todos os portlets gerados subsequentemente; portanto, faça backup desses arquivos se for modificá-los. Os arquivos-modelo incluem aqueles dos JSPs que são utilizados para exibir o applet do Host On-Demand e aqueles dos descritores XML que são utilizados para implementar os portlets no WebSphere Portal.
- Cada portlet é um archive que pode ser facilmente extraído e arquivado novamente usando um utilitário zip ou o utilitário jar empacotado com um JRE. Extraia o portlet para um diretório temporário, mantendo os nomes de diretórios. Você poderá, então, modificar os arquivos apropriados e arquivar novamente o portlet no nível superior do diretório temporário.
- Os descritores XML estão localizados no diretório de nível superior do portlet. Os arquivos JSP estão localizados no diretório /WEB-INF/hod/html do WebSphere Portal 6.
- Você pode querer incluir um arquivo de Ajuda personalizado no portlet. Para fazer isso, é necessário indicar no arquivo portlet.xml que o modo de marcação de *ajuda* é suportado. Inclua um arquivo denominado WpsHODHelp.jsp (fazendo distinção entre maiúsculas e minúsculas) contendo as informações de ajuda e o formatador HTML no diretório JSP do portlet.
- Você pode querer desenvolver um portlet personalizado que modifique dinamicamente as propriedades de sessão. Alguns dados úteis que você pode querer acessar seriam o nome do usuário do portal ou o endereço IP do cliente que está solicitando a página. Consulte as APIs do portlet para obter informações sobre como acessar esses dados. Você pode utilizar a sintaxe de

substituição de HTML descrita no Capítulo 13, “Modificando Propriedades de Sessão Dinamicamente”, na página 105 para, então, inserir dados derivados dessas informações no conjunto de parâmetros do applet.

- Consulte a documentação do WebSphere Portal instalada com o WebSphere Portal para obter informações detalhadas sobre o desenvolvimento de portlets e de APIs.

Capítulo 17. Suporte ao Eclipse-Plugin

Este capítulo descreve como configurar o Host On Demand para o IBM Eclipse-Plugin.

Nota: O Host On Demand suporta atualmente o Eclipse-Plugin somente na plataforma Windows. Verifique o LEIA-ME para obter suporte adicional já que ele será atualizado se plataformas adicionais forem incluídas.

O Eclipse-Plugin é a base para computação central de rede de próxima geração. Construído na plataforma cliente rich do Eclipse, ele fornece recursos adicionais para gerenciamento e implementação de aplicativos facilmente nos usuários finais.

No Eclipse-Plugin, todos os aplicativos são empacotados como “recursos” do Eclipse, que consistem em “plug-ins” e “fragmentos”. Os recursos do Eclipse são geralmente instalados a partir de um “site de atualização”, que é um diretório em uma máquina acessível pela Web.

Para construir o plug-in do Host On Demand para o Eclipse-Plugin, o Host On Demand fornece um applet Java chamado "Utilitário de atualização". O Utilitário do Site de Atualização converte arquivos jar do Host On-Demand em plugins e fragmentos do Eclipse e os coloca em um diretório do site de atualização novo ou existente.

Os procedimentos para instalar recursos de um site de atualização são diferentes dependendo das plataformas Eclipse-Plugin, como Workplace Managed Client (WMC) ou WebSphere Everyplace Deployment (WED). Quando WMC é utilizado, etapas de configuração extras são requeridas em sua contraparte do servidor, o WCS (Workplace Collaboration Service). O Utilitário do Site de Atualização gera um arquivo XML, que facilita as etapas de configuração no WCS.

Criando Plug-ins do Host On-Demand

Para criar e implementar estes plug-ins do Host On Demand para execução no Eclipse-Plugin, faça o seguinte:

1. Assegure que você tenha uma página do Deployment Wizard no modelo HTML que defina as sessões para seu plugin. Você pode utilizar qualquer página existente de modelo HTML ou criar uma nova.

Nota: Somente páginas de modelo HTML são suportadas para o recurso Eclipse-Plugin.

Depois da sua página ser concluída, coloque os arquivos zip de saída do Deployment Wizard descompactados no diretório de publicação do Host On-Demand.

2. Crie um diretório, por exemplo, *c:\update*, que será usado como o site de atualização do Eclipse para seu(s) plug-in(s), se caso ainda não tenha definido um. Em seguida,
3. Defina um alias para esse diretório na configuração do servidor da web e reinicie o servidor da web.
4. Agora você está pronto para criar o plugin do Host On-Demand. Na máquina do site de atualização do Eclipse, abra um navegador que esteja executando o

Java JRE (1.6 ou superior) e aponte-o para a URL do Host On Demand:
`http://<hostname>/<alias>/WCTConfig.html`.

Nota: No Linux, é necessário configurar a variável de ambiente LD_LIBRARY_PATH ao utilizar o plugin IBM 1.4.2 Java Service Release 2 e posterior.

Por exemplo, se desejar utilizar o plugin Java fornecido pelo servidor do Host On-Demand para Linux, utilize o comando de exportação para configurar a variável de ambiente LD_LIBRARY_PATH da seguinte forma:

```
export LD_LIBRARY_PATH=/opt/ibm/HostOnDemand/hod_jre/jre/bin:  
$LD_LIBRARY_PATH
```

5. Esta URL executará um applet especial do Utilitário do Site de Atualização para auxiliar na construção do plugin.
6. Preencha o painel Informações Básicas do Utilitário do Site de Atualização da seguinte forma:
 - **Diretório de Destino do Site de Atualização (Requerido)** Especifique o diretório do site de atualização Eclipse criado na Etapa 2, por exemplo `c:\updates`.
 - **Código base do HOD (requerido)** Esse campo já deve estar preenchido corretamente, se você apontou para `WCTConfig.html` conforme descrito na Etapa 3. Esse campo precisa especificar o local do diretório de publicação do Host On Demand no formato: `http://<hostname>/<alias>` O nome do servidor Host On Demand deve ser completo. Ele não pode ser um nome de URL relativa ou um nome como "host local" ou "127.0.0.1".
 - **Arquivo de Saída do Deployment Wizard (Requerido)** Especifique o nome da página do Deployment Wizard do modelo HTML criada na Etapa 1.
 - **Versão do recurso (requerido)** Especifique a sequência de versões usada no recurso gerado no formato `major.minor.service`, como `1.0.0`.
 - **Caminho de Arquivo JAR do Usuário (Opcional)** Especifique o caminho de um arquivo jar contendo o código do cliente utilizado para soluções que requerem código customizado para interagir com as sessões do Host On-Demand. É possível especificar vários arquivos separados por vírgulas (,).

Nota: Se você precisar usar o recurso **Executar applet**, será necessário empacotar seus applets em um arquivo jar e especificar o caminho de arquivo aqui.

7. É possível reduzir o tamanho do plug-in do Eclipse a ser criado desmarcando quaisquer recursos ou páginas de códigos do host desnecessários nos painéis **Códigos de tempo de execução e Páginas de códigos** do painel **Utilitário de site de atualização**.
8. Quando você tiver concluído todos os campos, selecione **Gerar e implementar plug-in**. O applet cria o plugin do Host On-Demand e o coloca no site de atualização especificado.
9. Os arquivos a seguir são criados ou modificados no diretório especificado como o Diretório de Destino do Site de Atualização:
 - **Arquivo de mapeamento do site (site.xml):** Este arquivo lista os recursos que são instaláveis a partir deste site de atualização.
 - **Arquivo de script XMLAccess:** Este arquivo é uma entrada do utilitário WebSphere Portal XMLAccess para a instalação do recurso Host On-Demand no WCS. Os nomes de arquivo são fornecidos no formato: (nome do arquivo

de saída do assistente de implementação)_DeployScript.xml. No XMLAccess, consulte Aceleradores IBM para a família WebSphere Portal.

- **subdiretório de recursos:** Este subdiretório contém os arquivos do recurso Host On-Demand.
- **subdiretório de plug-ins:** Este subdiretório contém:

Plugin do Host On-Demand	O plug-in em si. O nome do arquivo é fornecido no formato: <i>com.ibm.eNetwork.HOD.wct_(plugin version).jar</i>
Fragmento de código do Host On-Demand	O código do tempo de execução do Host On-Demand. O nome do arquivo é fornecido no formato: <i>com.ibm.eNetwork.HOD.wct.(function name)_(plugin version).jar</i>
Fragmento de Configuração	O fragmento que armazena informações de configuração. O nome do arquivo é fornecido no formato: <i>com.ibm.eNetwork.HOD.wct.configs.(deployment wizard output file name)_(feature version).jar</i>

- **subdiretório de imagens:** Este subdiretório contém um arquivo de imagem utilizado no WMC/WCS.

Para obter informações sobre a instalação do plug-in no cliente, consulte os documentos fornecidos com suas plataformas Eclipse-Plugin.

Configurando Propriedades da Sessão Dinamicamente

Na plataforma Eclipse-Plugin, as substituições de HTML não podem ser usadas para configurar dinamicamente as propriedades da sessão porque nenhum arquivo HTML é usado para executar o plug-in do Host On Demand. Se for necessário ter a funcionalidade similar, execute as seguintes etapas:

1. Implemente uma classe Java que implementa a interface *com.ibm.eNetwork.HOD.wct.IHODConfigFactory*, que é armazenada no arquivo *wct.jar*. O arquivo *wct.jar* é instalado no diretório de publicação do Host On-Demand. A interface possui dois métodos públicos:

```
public String setHodHtmlFileName()  
public Properties getHodHtmlParameters()
```

A seguir está um exemplo de tais classes Java:

```

package com.ibm.eNetwork.HOD.wct.samples;

import java.util.Properties;

import com.ibm.eNetwork.HOD.wct.IHODConfigFactory;

public class ConfigOverride implements IHODConfigFactory {
    /* (non-Javadoc)
     * @see com.ibm.eNetwork.HOD.wct.IHODConfigFactory#getHodHtmlFileName()
     */
    public String getHodHtmlFileName() {
        return "hodwmc";
    }

    /* (non-Javadoc)
     * @see com.ibm.eNetwork.HOD.wct.IHODConfigFactory#getHodHtmlParameters()
     */
    public Properties getHodHtmlParameters() {
        Properties p = new Properties();
        p.put("EnableHTMLOverrides", "true");
        p.put("TargetedSessionList", "3270 Display");
        p.put("host", "3270 Display=hostname");
        return p;
    }
}

```

Figura 9. Exemplo de classes Java

2. Empacote a classe Java em um arquivo jar.
3. Edite o arquivo HTML do Utilitário do Site de Atualização (WCTConfig.html) no diretório de publicação do Host On-Demand e configure o parâmetro showUserClass como true:


```
var showUserClass="true";
```
4. Execute o **Utilitário de site de atualização** e especifique parâmetros adicionais conforme a seguir: Caminho do arquivo JAR do usuário: o caminho do arquivo jar criado na etapa 2. Classe de factory de configuração de usuário: o nome da classe Java implementada na etapa 1 na página 139.
5. Gere um plug-in do Host On Demand e implemente-o em sua plataforma Eclipse-Plugin.

Utilizando um Diretório de Publicação do Usuário Separado

Quando você estiver utilizando um diretório de publicação do usuário separado diferente do diretório de publicação do Host On-Demand, será necessário especificar o diretório no Utilitário de Site de Atualização com o seguinte procedimento:

1. Edite o arquivo HTML do Utilitário do Site de Atualização (WCTConfig.html) no diretório de publicação do Host On-Demand e configure o parâmetro showAlternatePublishDirectory como true:


```
var showAlternatePublishDirectory ="true";
```
2. Execute o Utilitário do Site de Atualização e especifique seu diretório de publicação do usuário separado no campo de entrada Diretório de Publicação Alternativo.

Visualizar IDs Utilizados no Plugin do Host On-Demand

A seguir está a lista de IDs de visualização utilizados pelo plugin do Host On-Demand. Recomenda-se que você os conheça ao configurar o formato da página no WCS manualmente.

ID	Descrição
com.ibm.eNetwork.HOD.wct.SessionsView	Sessões Configuradas
com.ibm.eNetwork.HOD.wct.SessionLabelsView	Sessões Ativas
com.ibm.eNetwork.HOD.wct.TerminalView	Terminal (Vídeo, Impressora, FTP, etc.)

Limitações sobre o uso do Host On Demand em um ambiente Eclipse-Plugin

A seguir estão as limitações não mencionadas acima ao usar o Host On Demand em um ambiente do Eclipse-Plugin:

1. Às vezes, um diálogo modal do Host On Demand pode estar atrás da janela shell do Eclipse-Plugin. Isso ocorrerá se o Host On Demand tiver um diálogo aberto e o usuário mudar para outro aplicativo fora do Eclipse-Plugin. O usuário terá que clicar em ALT-TAB para localizar o diálogo do HOD que precisa ser conhecido.
2. “Confirmar na Saída” não funciona. A configuração “Confirmar na saída” é ignorada no ambiente do Eclipse-Plugin. Como ela não é suportada, a opção foi removida das propriedades de sessão.
3. Se uma sessão for ativada e um endereço de destino não estiver configurado, o applet do Host On-Demand estará apto para ativar o diálogo de propriedades da sessão. No ambiente do Eclipse-Plugin, os usuários recebem uma mensagem de que um endereço de destino é requerido, mas o diálogo de propriedades não abre.
4. Os elementos da GUI como Gerenciador de Macro, Teclado numérico, Barra de ferramentas, etc. não podem ser incluídos dinamicamente em uma sessão em execução. Em vez disso, esses itens devem ser ativados utilizando as propriedades existentes na seção Preferências das propriedades da sessão.
5. A opção para “Iniciar em uma Janela Separada” não tem sentido neste ambiente pois a sessão está sempre em uma área de janela do editor. Esta opção foi removida das propriedades da sessão.
6. Apenas um cliente com recursos de depuração está disponível. Não é possível reduzir os componentes de pré-carregamento utilizando as Opções de Pré-carregamento do Assistente de Implementação para tornar a área de cobertura menor (com a exceção das páginas de código do host e da Transferência de Arquivos 5250).
7. Excetuando o cliente armazenado em cache do Host On-Demand, o cliente não atualiza automaticamente para o novo nível de código. O Administrador precisa reconfigurar o Site de atualização para que a plataforma Eclipse-Plugin possa instalar o novo plug-in/fragmentos.
8. Execute tarefas do Applet apenas quando o applet estiver empacotado em um arquivo JAR e instalado em máquinas clientes.
9. O rastreo IPMON é suportado apenas no modo “normal”. O modo “automático” não é suportado. Nos modos de execução do IPMON, consulte o tópico “Visão Geral do rastreo IPMON” na ajuda on-line.

10. Quando vários recursos do Host On-Demand são instalados, o plugin do Host On-Demand exibe a lista de recursos do Host On-Demand instalados na visualização das sessões configurada para permitir que o usuário selecione um recurso entre eles. Após um recurso se selecionado uma vez, o usuário precisa reiniciar o WED para selecionar um recurso diferente.
11. Pressionar e liberar a tecla Alt emite uma exceção no console Java. Este é um problema conhecido no IBM 1.4.2 JRE e foi resolvido no IBM 1.4.2 Service Release 4.1 e posterior.

Capítulo 18. Configurando o Servidor Host On-Demand para Utilizar o LDAP

O servidor Host On-Demand é utilizado para gerenciar dados de configuração para os modelos combinados e baseados no servidor de configuração. Para o modo operacional padrão do servidor Host On-Demand, esses dados são salvos em um data store privado não compartilhado. Alguns clientes da empresa precisam gerenciar suas informações de configuração entre vários servidores Host On-Demand. Se esses clientes utilizarem o data store privado não compartilhado, seus administradores deverão gerenciar os dados para cada servidor Host On-Demand separadamente. Um diretório do servidor LDAP (Lightweight Directory Access Protocol) fornece a capacidade de compartilhar informações de configuração do usuário e do grupo em instâncias diferentes do servidor de configuração do Host On-Demand.

A utilização de um servidor do diretório LDAP para gerenciar e compartilhar suas definições através de vários servidores Host On-Demand é uma opção que deve ser cuidadosamente planejada e executada. A migração do data store privado, em específico, possui implicações sobre os dados de configuração. O LDAP permite que o cliente gerencie as informações de configuração, organizando os usuários em uma árvore hierárquica de grupos. Se os usuários existentes forem membros de mais de um grupo, algumas informações serão perdidas. Observe que os dados de configuração no data store privado não são alterados quando ocorre uma migração para o LDAP. Consulte Implicações de migração para o LDAP na ajuda on-line do Host On-Demand para obter informações mais detalhadas.

Configurando o Suporte LDAP

1. Decida qual servidor de Diretório LDAP você utilizará e, se necessário, instale-o.
2. Se estiver executando uma versão do LDAP que não suporta o esquema do Host On-Demand, instale os arquivos de extensão de esquema do Host On-Demand conforme descrito em “Instalando as Extensões de Esquema” na página 144. (Os arquivos de extensão de esquema não são requeridos para o IBM LDAP Versão 3.x ou posterior).
3. Peça ao seu administrador do LDAP um sufixo que o Host On-Demand utilizará para armazenar informações de configuração. Anote o DN (Distinguished Name) deste sufixo; você precisará desta informação para concluir a configuração do LDAP.
4. Peça ao seu administrador do LDAP um DN e uma senha de administrador para o Host On-Demand; estes serão utilizados para autenticar o servidor LDAP. O DN do administrador deve ter criado, modificado e excluído os privilégios para o sufixo mencionado na etapa anterior. Anote o DN e a senha; você precisará destas informações para concluir a configuração do LDAP.
5. Ative o LDAP na janela Serviço de Diretório no utilitário de administração. Opcionalmente, migre as informações de configuração do data store privado para o servidor do diretório LDAP. Para obter informações adicionais, consulte o Capítulo 18, “Configurando o Servidor Host On-Demand para Utilizar o LDAP”.



Os usuários e grupos que já estão definidos no LDAP para outras finalidades não são utilizados pelo Host On-Demand. Os usuários e grupos do Host On-Demand devem ser definidos separadamente, migrando as informações de configuração do data store privado ou configurando os usuários e grupos no Host On-Demand depois de ativar o LDAP.



Se você estiver utilizando o servidor IBM LDAP em plataformas Windows e AIX, e se você estiver criando um grande número de usuários, certifique-se de que o DB2 esteja configurado com o valor correto para APP_CTL_HEAP_SZ. Enquanto o valor dessa variável é dependente de instalações individuais, definir APP_CTL_HEAP_SZ como 512 é um bom valor inicial.

Para configurar o tamanho do heap do DB2 em um ambiente Windows ou AIX, emita estes comandos:

1. set DB2INSTANCE=ldapdb2
2. db2 connect to ldapdb2
3. db2 update db cfg for ldapdb2 using APP_CTL_HEAP_SZ 512
4. db2 force application all
5. db2 terminate
6. db2stop
7. db2start

Além disso, certifique-se que STMTHEAP seja grande o suficiente. O tamanho desses parâmetros são dependentes somente de configurações individuais do cliente e do número de usuários do Host On-Demand que está sendo migrado para LDAP.

Instalando as Extensões de Esquema

As extensões do Host On-Demand para o diretório de esquema do LDAP são fornecidas em vários arquivos localizados no subdiretório LDAP do diretório de publicação (por exemplo, `your_install_directory\HOD\ldap`, em que *your_install_directory* é o diretório de instalação do Host On-Demand). Estes arquivos contêm extensões para o esquema LDAP e estão armazenados no formato slapd padrão. As extensões de esquema devem entrar em vigor antes do Host On-Demand poder armazenar informações de configuração em um servidor LDAP. Entre em contato com o administrador do LDAP para instalar estas extensões de esquema.

Consulte o Diretório do Programa para obter instruções sobre como instalar as extensões de esquema para o zSeries.



O administrador do LDAP já pode ter instalado estas extensões de esquema para você por meio de outro produto IBM. Se for dessa forma, desconsidere esta etapa. Se você estiver utilizando o IBM Directory Server Versão 3.1.1 ou posterior, o esquema será pré-instalado, portanto, também será possível ignorar essas etapas.

Para instalar as extensões de esquema do Host On-Demand em um servidor do Diretório LDAP Netscape:

1. Copie os seguintes arquivos slapd do <diretório de publicação do Host On-Demand/ldap para o diretório de configuração do LDAP Netscape no servidor LDAP:

Netscape.IBM.at
Netscape.IBM.oc

2. Pare o servidor LDAP.
3. Edite o arquivo <diretório de configuração do LDAP Netscape/ slapd.conf e inclua as seguintes instruções:
userat "<Netscape LDAP config directory>/Netscape.IBM.at"
useroc "<Netscape LDAP config directory>/Netscape.IBM.oc"
4. Reinicie o servidor LDAP.

Para instalar as extensões de esquema do Host On-Demand em um servidor do Diretório LDAP IBM:

1. Copie os seguintes arquivos slapd do diretório de publicação do Host On-Demand/ldap para o <diretório de instalação/etc no servidor LDAP:
V2.1.IBM.at
V2.1.IBM.oc
2. Pare o servidor LDAP.
3. Edite o arquivo <diretório de instalação/etc/ slapd.at.conf e inclua a seguinte instrução no fim do arquivo:
include /etc/V2.1.IBM.at
4. Edite o arquivo <diretório de instalação/etc/ slapd.oc.conf e inclua a seguinte instrução no fim do arquivo:
include /etc/V2.1.IBM.oc
5. Reinicie o servidor LDAP.

Configurando o Servidor Host On-Demand para Utilizar o LDAP como um Data Store

1. Abra a janela Administração e efetue logon no Host On-Demand.
2. Clique em Serviços > Serviço de Diretório.
3. Clique na caixa Utilizar Serviço do Diretório (LDAP) e, em seguida, digite as informações do servidor LDAP.

Endereço de Destino

Digite o endereço IP do diretório LDAP. Utilize o nome do host ou o formato decimal pontilhado. O padrão é o nome do host do servidor Host On-Demand.

Porta de Destino

Digite a porta TCP/IP na qual o servidor LDAP aceitará uma conexão a partir de um cliente LDAP. A porta padrão é 389.

Nome Distinto do Administrador

Digite o DN (Distinguished Name) do administrador do diretório que permite ao Host On-Demand atualizar informações. É necessário usar a representação em sequência LDAP para nomes distintos (por exemplo, cn=Chris Smith,o=IBM,c=US).

Senha do Administrador

Digite a senha do administrador do diretório

Sufixo do Nome Distinto

Digite o DN (Distinguished Name) da entrada mais alta da DIT (Directory Information Tree) na qual as informações serão salvas. O Host On-Demand armazenará todas as informações de configuração deste sufixo no DIT. É necessário usar a representação em sequência LDAP para nomes distintos (por exemplo, cn=HOD,o=IBM,c=US).

Migrar Configuração para o Serviço do Diretório

Para migrar usuários e grupos de um armazenamento de dados privativo para o diretório LDAP, clique na caixa de opções. A migração para LDAP resulta em implicações significativas para as informações de configuração de seu grupo ou usuário. Consulte *Implicações da Migração de LDAP* na ajuda on-line para obter informações adicionais. Você pode marcar esta caixa quando trocar para o servidor do diretório ou depois de ter feito a troca.



A configuração do Redirecionador não é migrada para o servidor do diretório.



Se você tiver um problema de conexão com o LDAP e migração, tente conectar-se ao LDAP primeiro. Depois de uma conexão bem-sucedida, tente migrar.

4. Clique em Aplicar.

Quando for solicitado a autenticar-se no diretório LDAP pela primeira vez, especifique um ID de usuário "admin" e uma senha "password". Você pode alterar essa senha depois de efetuar o primeiro logon. Mesmo que possa ter alterado sua senha para o data store privado, esse ID e senha continuam a ser válidos somente para o data store privado. Para o diretório LDAP, são necessários um ID do usuário e senha separados. Para evitar confusão, você pode alterar sua senha do diretório LDAP, deixando-a igual à senha do data store privado.

As alterações feitas neste painel são imediatamente efetivadas. Visto que você trocou para o servidor LDAP, as alterações subseqüentes relacionadas ao usuário serão feitas somente no servidor LDAP, incluindo alterações administrativas para grupos, usuários ou sessões e as alterações como novas senhas, macros, alterações em teclado, etc., pelo administrador ou por um usuário.

Apêndice A. Utilizando Clientes Instalados Localmente

O cliente instalado localmente é instalado em um disco local. O applet do cliente é carregado diretamente no navegador do sistema padrão, assim, não há download de um servidor. A razão mais comum para configurar um cliente local é para usuários que se conectam remotamente sobre linhas telefônicas lentas, em que o tempo de download pode ser um problema e a conectividade ser imprevisível. Você também pode utilizar o cliente instalado localmente para testar as capacidades de acesso do host sem instalar o produto Host On-Demand completo.

Sistemas Operacionais que Suportam Clientes Instalados Localmente

O Host On-Demand pode ser instalado como um cliente nos seguintes sistemas operacionais:

- Windows 7
- Windows 8
- Windows 10
- Windows Server 2012

O cliente instalado localmente requer aproximadamente 320 MB de espaço em disco.

Instalando o Cliente Local

Para instalar o cliente local do Host On Demand em uma estação de trabalho Windows, é necessário ser um membro do grupo de Administradores.

1. Insira o DVD e execute `hodinstallwin.exe -lc` no diretório `\HODINST` do DVD.
2. Clique em Instalar.
3. Continue com o restante da janela.
4. Leia o Leia-me disponível na última janela, caso ainda não tenha feito isso.

Ao chegar ao final da instalação, o Gerenciador de Serviços do Host On-Demand será automaticamente configurado e iniciado. No Windows 7, Windows 8 e Windows 10, o Gerenciador de Serviços é instalado como um serviço.

Iniciando o Cliente Local

Para iniciar o Host On Demand como um cliente, clique em **Iniciar > Programas > IBM Host On Demand > Host On Demand**.

Removendo o Cliente Local

Para remover o cliente local, utilize Adicionar/Remover Programas do Painel de Controle.

Apêndice B. Utilizando a Interface de Linha de Comandos IKEYCMD

A IKEYCMD é uma ferramenta de linha de comandos, além do Utilitário de Gerenciamento de Certificados do Host On-Demand, que pode ser utilizada para gerenciar chaves, certificados e pedidos de certificado. Possui uma funcionalidade semelhante à do Gerenciamento de Certificados e é executada a partir da linha de comandos sem uma interface gráfica. Ela pode ser chamada a partir dos programas e scripts de shell nativos para ser utilizada quando os aplicativos preferem incluir interfaces personalizadas nas tarefas de gerenciamento de chaves e certificados. Ela pode criar arquivos de banco de dados de chaves para todos os tipos que o utilitário de Gerenciamento de Certificados suporta atualmente. Também pode criar pedidos de certificado, importar certificados assinados pela CA e gerenciar certificados auto-assinados. Ela tem como base o Java e está disponível apenas em plataformas Windows, AIX, Linux Intel e Linux zSeries.

Utilize a IKEYCMD para tarefas de configuração relacionadas à criação e ao gerenciamento de chaves públicas e privadas. Você não pode utilizar a IKEYCMD para opções de configuração que atualizam o arquivo de configuração do servidor, `httpd.conf`. Para opções que atualizam o arquivo de configuração do servidor, é necessário usar o IBM Administration Server.

Configuração de Ambiente para Interface da Linha de Comandos IKEYCMD

Configure as variáveis de ambiente para utilizar a interface de linha de comandos IKEYCMD da seguinte forma:

Para plataformas Windows, proceda da seguinte forma:

- Utilizando a interface do usuário ou modificando o `autoexec.bat` em uma janela de comando, defina/modifique a variável `PATH` para incluir a localização dos arquivos executáveis Java:

```
set PATH=c:\Program Files\IBM\HostOnDemand\hod_jre\jre\bin;%PATH%;
```

- Utilizando a interface do usuário ou modificando o `autoexec.bat` em uma janela de comando, defina/modifique a variável de ambiente `CLASSPATH` da seguinte forma:

```
set CLASSPATH=c:\Program Files\IBM\GSK7\classes\cfwk.zip;C:\  
Program Files\IBM\GSK7\classes\gsk7cls.jar;%CLASSPATH%;
```

Para plataformas AIX:

Primeiro, assegure que seus arquivos `xlC` (que constituem a biblioteca de tempo de execução para o compilador AIX C++ padrão) atendam um dos seguintes requisitos:

- no AIX 5.2: conjunto de arquivos `xlC.aix50.rte` deve estar no nível 6.0.0.3 ou posterior

Utilize o seguinte comando para confirmar sua versão:

```
lslpp -ha "xlC.aix*.rte"
```

(Se o conjunto de arquivos xLC estiver desatualizado e você iniciar o Host On-Demand ServiceManager com o Certificate Management ativo, ocorrerá erros).

Em seguida, faça as seguintes especificações:

- Defina o PATH para o local no qual o executável do JRE ou Java reside:

```
EXPORT PATH=/opt/IBM/HostOnDemand/hod_jre/jre/bin:$PATH
```

- Defina a seguinte variável de ambiente CLASSPATH:

```
EXPORT  
CLASSPATH=/usr/local/ibm/gsk7/classes/cfwk.zip:/  
usr/local/ibm/gsk7/classes/gsk7cls.jar:$CLASSPATH
```

Quando você tiver concluído essas etapas, IKEYCMD deverá ser executado de qualquer diretório. Para executar um comando IKEYCMD, utilize a seguinte sintaxe:

```
java com.ibm.gsk.ikeyman.ikeycmd  
<command>
```

Sintaxe de Linha de Comandos IKEYCMD

A sintaxe da CLI Java é

```
java  
[-Dikeycmd.properties=<properties_file>]  
com.ibm.gsk.ikeyman.ikeycmd <object> <action>  
[options]
```

em que

- `-Dikeycmd.properties` especifica o nome de um arquivo de propriedades opcional a ser utilizado para esta chamada de Java. Um arquivo de propriedades padrão, `ikminit_hod.properties`, é fornecido como um arquivo de amostra que contém as definições padrão para o Host On-Demand.
- `Object` é um dos seguintes:
 - `-keydb`: ações executadas no banco de dados de chaves (um arquivo de banco de dados de chaves CMS ou classe TLSight)
 - `-version`: exibir informações sobre a versão da IKEYCMD
- `Ação` será uma das seguintes:
 - `-cert`: ações executadas em um certificado
 - `-certreq`: ações executadas em um pedido de certificado
 - `-help`: exibir ajuda para as chamadas da IKEYCMD

`Action` é a ação específica a ser executada no objeto e `options` são as opções, obrigatórias e opcionais, especificadas para o par `object` e `action`.



As palavras-chave `object` e `action` são posicionais e devem ser especificadas na ordem selecionada. No entanto, as opções não são posicionais e podem ser especificadas em qualquer ordem, desde que sejam especificadas como um par de opção e o par operando.

Lista de Tarefas da IKEYCMD para o Host On-Demand

As tarefas da interface de linha de comandos IKEYCMD requeridas para o Host On-Demand são resumidas nas seguintes seções deste apêndice:

- “Criando um Novo Banco de Dados de Chaves”
- “Listando CAs” na página 153
- “Mostrando a chave padrão em um banco de dados de chaves” na página 158
- “Armazenando o Banco de Dados Criptografado em um Arquivo Stash” na página 158
- “Criando um novo par de chaves e solicitação de certificado” na página 153
- “Armazenando o Certificado de Servidor” na página 154
- “Criando um Certificado Auto-assinado” na página 155
- “Tornando os Certificados de Servidor Disponíveis para os Clientes” na página 156
- “Exportando Chaves” na página 157
- “Importando Chaves” na página 158

Criando um Novo Banco de Dados de Chaves

Um banco de dados de chaves é um arquivo que o servidor utiliza para armazenar um ou mais certificados e pares de chaves. Ele é obrigatório para permitir conexões seguras entre o servidor e os clientes Host On-Demand. Antes de configurar a comunicação TLS, é necessário criar o arquivo do banco de dados de chave `HODServerKeyDb.kdb` em `your_install_directory\bin` para Windows e `your_install_directory /bin` para AIX. Esse arquivo não é fornecido com o Host On Demand, portanto, é necessário criá-lo após a primeira instalação.

Em plataformas Windows, por exemplo, para criar um novo banco de dados de chaves utilizando a interface de linha de comandos IKEYCMD, digite o seguinte comando:

```
java com.ibm.gsk.ikeyman.ikeycmd -keydb -create
-db your_install_directory\bin\HODServerKeyDb.kdb
-pw <senha> -type cms -expire <dias> -stash
```

em que `your_install_directory` é seu diretório de instalação do Host On-Demand.

Observe as seguintes descrições:

- <senha>: A senha é requerida para cada operação do banco de dados de chaves. Mesmo que um banco de dados do tipo `sslslight` requeira a especificação de uma senha, esta pode ser uma cadeia NULA (especificada como "").
- -type: o `HODServerKeyDb.kdb` utilizado pelo servidor Host On-Demand é do tipo CMS.
- -expire: Dias antes da expiração da senha.
 - Se você não definir esse parâmetro, a senha não expirará.
 - **AVISO:** Se você definir esse parâmetro e se estiver utilizando o banco de dados de chaves com o Redirecionador, verifique se a execução do Redirecionador falhará depois que a senha expirar. Quando houver falha no Redirecionador, a mensagem de erro do Redirecionador *não* declarará que a senha do banco de dados de chaves expirou.
- -stash: Guarda a senha para o banco de dados de chaves. A proteção da senha é **requerida** para o IBM HTTP Server e para o servidor Host On-Demand.

Quando a opção `-stash` é especificada durante a criação do banco de dados de chaves, a senha é guardada em um arquivo com o nome de arquivo de `HODServerKeyDb.sth`

Depois de criado, o arquivo `HODServerKeyDb.kdb` armazena todas as informações de segurança necessárias ao servidor Host On-Demand. Quaisquer inclusões ou alterações são feitas no arquivo de banco de dados de chaves `HODServerKeyDb.kdb` existente.



Sempre que criar ou fizer mudanças no arquivo `HODServerKeyDb.kdb`, é necessário parar e reiniciar o Gerenciador de Serviços do Host On Demand.

Definindo a Senha do Banco de Dados

Ao criar um novo banco de dados de chaves, você especifica uma senha para o mesmo. Essa senha protege a chave privada. A chave privada é a única chave que pode assinar documentos ou decriptografar mensagens criptografadas com a chave pública. É recomendável alterar, com frequência, a senha do banco de dados de chaves.

Utilize as diretrizes a seguir quando especificar a senha:

- A senha deve ser do conjunto de caracteres Inglês (Estados Unidos).
- A senha deve ter, pelo menos, seis caracteres e conter, pelo menos, dois números não-consecutivos. Certifique-se de que a senha não consista em informações pessoais que possam ser obtidas publicamente, como as iniciais e a data de nascimento sua, de seu cônjuge ou filhos.
- Guarde a senha.



Mantenha controle das datas de expiração da senha. Se a senha expirar, uma mensagem será gravada no registro de erros. O servidor será iniciado, mas não haverá uma conexão de rede segura se a senha tiver expirado.

Alterando a Senha do Banco de Dados

Para alterar a senha do banco de dados, faça o seguinte:

Para plataformas Windows, por exemplo, digite o seguinte comando:

```
java com.ibm.gsk.ikeyman.ikeycmd -keydb -changepw  
-db your_install_directory\bin\HODServerKeyDb.kdb  
-pw <senha> -new_pw <nova_senha> -expire <dias> -stash
```

em que *your_install_directory* é seu diretório de instalação do Host On-Demand.

Observe as seguintes descrições:

- `-new_pw`: Nova senha do banco de dados de chaves; esta senha deve ser diferente da senha antiga, e esta senha não pode ser uma cadeia NULA.
- `-expire`: Dias antes da expiração da senha.
- `-stash`: Guarda a senha para o banco de dados de chaves. É necessário guardar a senha para o IBM HTTP Server e o servidor Host On-Demand.

Listando CAs

Para exibir uma lista de CAs confiáveis no banco de dados de chaves HODServerKeyDb.kdb, faça o seguinte:

Para plataformas Windows, por exemplo, digite o seguinte comando:

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -list CA
-db your_install_directory\bin\HODServerKeyDb.kdb
-pw <senha> -type cms
```

em que *your_install_directory* é seu diretório de instalação do Host On-Demand.

Por padrão, HODServerKeyDb.kdb é fornecido com os certificados de CA das seguintes CAs confiáveis reconhecidas:

- IBM World Registry CA
- Integrion CA Root (da IBM World Registry)
- VeriSign Class 1 Public Primary CA
- VeriSign Class 2 Public Primary CA
- VeriSign Class 3 Public Primary CA
- VeriSign Class 4 Public Primary CA
- VeriSign Test CA
- RSA Secure Server CA (da VeriSign)
- Thawte Personal Basic CA
- Thawte Personal Freemail CA
- Thawte Personal Premium CA
- Thawte Premium Server CA
- Thawte Server CA

Criando um novo par de chaves e solicitação de certificado

Para criar um par de chaves pública-privada e um pedido de certificado, proceda da seguinte forma:

1. Para plataformas Windows, por exemplo, digite o seguinte comando:

```
java com.ibm.gsk.ikeyman.ikeycmd -certreq -create
-db your_install_directory\bin\HODServerKeyDb.kdb
-pw <senha> -size <1024 | 512> -dn <nome_distinto>
-file <nome do arquivo> -label <etiqueta>
```

em que *your_install_directory* é seu diretório de instalação do Host On-Demand.

Observe as seguintes descrições:

- -size: tamanho de chave de 512 ou 1024
- -label: rótulo anexado ao certificado ou pedido de certificado
- -dn: nome distinto X.500. Isso é inserido como cadeia entre aspas no seguinte formato: (Apenas CN, O e C são obrigatórios; CN=common_name, O=organization, OU=organization_unit, L=location, ST=state/province, C=country).
"CN=weblinux.raleigh.ibm.com, O=ibm, OU=IBM HTTP Server, L=RTP, ST=NC, C=US"
- -file: nome do arquivo no qual o pedido de certificado será armazenado. Por padrão, o Host On-Demand utiliza o nome certreq.arm e ele deve ser

armazenado em *your_install_directory*\bin (em que *your_install_directory* é o diretório de instalação do Host On-Demand), onde HODServerKeyDb.kdb está localizado.

2. Verifique se o certificado foi criado com êxito.
 - a. Exiba o conteúdo do arquivo de pedido de certificado criado.
 - b. Certifique-se de que o banco de dados tenha gravado o pedido de certificado:

```
java com.ibm.gsk.ikeyman.ikeycmd -certreq -list  
-db <nome do arquivo> -pw <senha>
```

O rótulo recém-criado deve estar listado.
3. Envie o arquivo recém-criado para uma autoridade de certificação.

Armazenando o Certificado de Servidor

Recebendo um Certificado Assinado pela CA

Utilize este procedimento para receber um certificado enviado eletronicamente a partir de uma CA (Autoridade de Certificação), designada como CA confiável em seu servidor. Por padrão, os seguintes certificados de CA são armazenados no banco de dados de chaves HODServerKeyDb.kdb e marcados como certificados de CA confiáveis:

- IBM World Registry CA
- Integrion CA Root (da IBM World Registry)
- VeriSign Class 1 Public Primary CA
- VeriSign Class 2 Public Primary CA
- VeriSign Class 3 Public Primary CA
- VeriSign Class 4 Public Primary CA
- VeriSign Test CA
- RSA Secure Server CA (da VeriSign)
- Thawte Personal Basic CA
- Thawte Personal Freemail CA
- Thawte Personal Premium CA
- Thawte Premium Server CA
- Thawte Server CA

A Autoridade de Certificação pode enviar mais de um certificado. Além do certificado para o seu servidor, a CA também pode enviar Certificados de Assinatura adicionais ou Certificados de CA Intermediários. Por exemplo, a Verisign inclui um Certificado de CA Intermediário ao enviar um certificado de ID de Servidor Global. Antes de receber o certificado de servidor, receba quaisquer certificados de CA Intermediários adicionais. Siga as instruções em “Armazenando um Certificado de CA” na página 155 para receber Certificados de CA Intermediários.



Se a CA que emite o certificado assinado por CA não for uma CA confiável no banco de dados de chaves, é necessário primeiro armazenar o certificado de CA e designar a CA como confiável. Em seguida, você pode receber o certificado assinado pela CA no banco de dados. Não é possível receber um certificado assinado por uma CA que não seja confiável. Para obter instruções, consulte “Armazenando um Certificado de CA” na página 155

Em plataformas Windows, por exemplo, para receber o certificado assinado pela CA em um banco de dados de chaves, digite o seguinte comando:

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -receive -file <nome do arquivo>
-db
your_install_directory\bin\HODServerKeyDb.kdb
-pw <senha>
-format <ascii | binário> -default_cert <sim | não>
```

em que *your_install_directory* é seu diretório de instalação do Host On-Demand.

Observe as seguintes descrições:

- -format: A Autoridade de Certificação pode fornecer um Certificado de CA no formato ASCII ou binário
- -label: Rótulo anexado ao certificado de CA.
- -trust: Indica se esta CA pode ser confiável. Utilize opções enable quando receber um certificado CA.
- -file: Arquivo que contém o certificado de CA.

Armazenando um Certificado de CA

Em plataformas Windows, por exemplo, para armazenar um certificado de uma CA não-confiável, digite o seguinte comando:

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -add
-db your_install_directory\bin\HODServerKeyDb.kdb
-pw <senha> -label <etiqueta> -format <ascii | binário>
-trust <ativar | desativar> -file <arquivo>
```

em que *your_install_directory* é seu diretório de instalação do Host On-Demand.

Observe as seguintes descrições:

- -label: Rótulo anexado ao certificado ou pedido de certificado
- -format: As Autoridades de Certificação podem fornecer um arquivo ASCII binário
- -trust: Indica se esta CA pode ser confiável. Deve ser Yes.



É necessário parar e reiniciar o Gerenciador de Serviços do Host On Demand depois de fazer isso.

Criando um Certificado Auto-assinado

Geralmente levam-se duas ou três semanas para receber um certificado de uma CA reconhecida. Durante a espera de um certificado emitido, use IKEYCMD para criar um certificado de servidor autoassinado para ativar sessões TLS entre os clientes e o servidor. Utilize este procedimento se você estiver agindo como sua própria CA para uma rede privada da Web.

Em plataformas Windows, por exemplo, para criar um certificado auto-assinado, digite o seguinte comando:

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -create
-db your_install_directory\bin\HODServerKeyDb.kdb
-pw <senha> -size <1024 | 512> -dn <nome distinto>
-label <etiqueta> -default_cert <sim ou não>
```

em que *your_install_directory* é seu diretório de instalação do Host On-Demand.

Observe as seguintes descrições:

- -size: Tamanho de chave de 512 ou 1024
- -label: Digite um comentário descritivo utilizado para identificar a chave e o certificado no banco de dados.
- -dn: Digite um nome distinto X.500. Isso é inserido como uma cadeia entre aspas no seguinte formato (Apenas CN, O e C são obrigatórios; CN=common_name, O=organization, OU=organization_unit, L=location, ST=state, province, C=country).
"CN=weblinux.raleigh.ibm.com, O=ibm, OU=IBM HTTP Server, L=RTP, ST=NC, C=US"
- -default_cert: Digite yes, se você desejar que este certificado seja o padrão no banco de dados de chaves. Caso contrário, digite No.

Tornando os Certificados de Servidor Disponíveis para os Clientes

Todos os certificados no HODServerKeyDb.kdb estão disponíveis no servidor Host On-Demand. No entanto, em algumas configurações, um desses certificados também deve estar disponível para os clientes que acessam o servidor. Nos casos em que o servidor utiliza um certificado de uma CA desconhecida, a raiz desse certificado deve ficar disponível para o cliente. Se o servidor utilizar um certificado auto-assinado, uma cópia desse certificado deverá ficar disponível para os clientes.

Para clientes feitos download e armazenados em cache do Host On-Demand, isso é feito extraíndo o certificado em um arquivo temporário e criando ou atualizando um arquivo nomeado CustomizedCAs.p12, que deve ser apresentado no diretório de publicação do Host On-Demand.

Para criar o arquivo CustomizedCAs.p12 para clientes feitos download ou armazenados em cache, insira o seguinte comando:

```
java com.ibm.gsk.ikeyman -keydb -create -db  
CustomizedCAs.p12 -pw hod -type pkcs12
```

A senha padrão é hod.

Adicionando a Raiz de um CA Desconhecido em CustomizedCAs.p12

Primeiro, extraia o certificado raiz da CA ou um certificado auto-assinado do arquivo de banco de dados de chaves HODServerKeyDb.kdb. Para fazer isso para o Windows, por exemplo, insira o seguinte comando:

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -extract  
-db your_install_directory\bin\HODServerKeyDb.kdb  
-pw <senha> -label <etiqueta> -target cert.arm -format ascii
```

em que *your_install_directory* é seu diretório de instalação do Host On-Demand.

Observe as seguintes descrições:

- -label: Rótulo anexado ao certificado.
- -pw: Senha para abrir o arquivo de banco de dados de chaves HODServerKeyDb.kdb.
- -target: Arquivo ou banco de dados de destino. Nesse caso, é o nome do arquivo formatado Base-64 Armored ASCII com um nome de arquivo padrão cert.arm.

- -format: Pode ser ASCII ou Binário.

Agora, adicione esse certificado raiz do CA no arquivo CustomizedCAs.p12. Para adicionar um certificado raiz do CA ou um certificado auto-assinado à lista de assinantes no CustomizedCAs.p12, insira o seguinte comando:

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -add
-db CustomizedCAs.p12 -pw hod -label <etiqueta>
-file cert.arm -format ascii -trust <ativar | desativar>
```

Para clientes mais antigos, para adicionar esse certificado raiz do CA no arquivo CustomizedCAs.class, insira o seguinte comando:

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -add
-db CustomizedCAs.class -label <etiqueta>
-file cert.arm -format ascii -trust <ativar | desativar>
```

Observe as seguintes descrições:

- -label: Rótulo do certificado que está sendo incluído.
- -file: Nome do arquivo no qual o certificado foi extraído. Nesse caso, é o nome do arquivo formatado Base-64 Armored ASCII com um nome de arquivo padrão cert.arm.
- -format: Pode ser ASCII ou Binário.
- -trust: Decide se deve definir como raiz confiável. Enable irá definir a raiz da CA ou o certificado auto-assinado como uma raiz confiável. Disable não definirá a raiz da CA ou o certificado auto-assinado como raiz confiável.



Pare e inicie novamente o Gerenciador de Serviços do Host On-Demand depois de concluir esta tarefa.

Para clientes mais antigos, é necessário converter o arquivo CustomizedCAs.p12 em um arquivo CustomizedCAs.class para clientes de download ou em cache, digitando o seguinte comando. O comando aparece em três linhas, mas deve ser digitado como uma única linha.

```
..\hod_jre\jre\bin\java -cp ..\lib\sm.zip;
com.ibm.eNetwork.HOD.convert.CVT2SSLIGHT
CustomizedCAs.p12 hod CustomizedCAs.class
```

Exportando Chaves

Para exportar chaves para um outro banco de dados de chaves ou para exportar chaves para um arquivo PKCS12, digite o seguinte comando:

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -export -db <nome do arquivo>
-pw <senha> -label <etiqueta> -type <cms | jks
| jceks | pkcs12>
-target <nome do arquivo> -target_pw <senha>
-target_type <cms | jks | jceks | pkcs12> -encryption <forte |
fraca>
```

Observe as seguintes descrições:

- -label: Rótulo anexado ao certificado.
- -target: Arquivo ou banco de dados de destino.
- -target_pw: Senha para o banco de dados de chaves de destino.
- -target_type : Tipo do banco de dados especificado pelo operando -target

- -encryption: Nível de criptografia. O padrão é strong.

Importando Chaves

Para importar chaves de um outro banco de dados de chaves, digite o seguinte comando:

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -import -db <nome do arquivo>
-pw <senha> -label <etiqueta> -type <cms | jks | jceks |
pkcs12> -target
<nome do arquivo> -target_pw <senha> -target_type
<cms | jks | jceks | pkcs12>
```

Para importar chaves de um arquivo PKCS12, digite o seguinte comando:

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -import -file
<nome do arquivo>
-pw <senha> -type pkcs12 -target <nome do arquivo>
-target_pw <senha> -target_type <cms | jks | jceks | pkcs12>
```

Observe as seguintes descrições:

- -label: Rótulo anexado ao certificado.
- -target: Banco de dados de destino.
- -target_pw: Senha para o banco de dados de chaves se -target especificar um banco de dados de chaves
- -target_type: Tipo do banco de dados especificado pelo operando -target.

Mostrando a chave padrão em um banco de dados de chaves

Em plataformas Windows, por exemplo, para exibir a entrada de chave padrão, digite o seguinte comando:

```
java com.ibm.gsk.ikeyman.ikeycmd -cert -getdefault
-db your_install_directory\bin\HODServerKeyDb.kdb
-pw <senha>
```

em que *your_install_directory* é seu diretório de instalação do Host On-Demand.

Armazenando o Banco de Dados Criptografado em um Arquivo Stash

Para uma conexão de rede segura, armazene a senha de banco de dados criptografada em um arquivo escondido. Em plataformas Windows, por exemplo, para armazenar a senha enquanto um banco de dados é criado, digite o seguinte comando:

```
java com.ibm.gsk.ikeyman.ikeycmd -keydb -create
-db your_install_directory\bin\HODServerKeyDb.kdb
-pw <senha> -type cms -expire <dias> -stash
```

em que *your_install_directory* é seu diretório de instalação do Host On-Demand.

Em plataformas Windows, por exemplo, para armazenar a senha após a criação de um banco de dados, digite o seguinte comando:

```
java com.ibm.gsk.ikeyman.ikeycmd -keydb -stashpw
-db
your_install_directory\bin\HODServerKeyDb.kdb
-pw <senha>
```

em que *your_install_directory* é seu diretório de instalação do Host On-Demand.

Visão Geral dos Parâmetros de Linha de Comandos IKEYCMD

A tabela a seguir descreve cada ação que pode ser executada em um objeto especificado.

Objeto	Ação	Descrição
-keydb	-changepw	Altera a senha para um banco de dados de chaves
	-convert	Converte o banco de dados de chaves de um formato para outro
	-create	Cria um banco de dados de chaves
	-delete	Exclui o banco de dados de chaves
	-stashpw	Guardar a senha de um banco de dados de chaves em um arquivo
-cert	-add	Inclui um certificado de CA de um arquivo em um banco de dados de chaves
	-create	Cria um certificado auto-assinado
	-delete	Exclui um certificado de CA
	details	Lista as informações detalhadas de um certificado específico
	-export	Exporta um certificado pessoal e sua chave privada associada de um banco de dados de chaves para um arquivo PKCS#12 ou para outro banco de dados de chaves
	-extract	Extrai um certificado de um banco de dados de chaves
	-getdefault	Obtém o certificado pessoal padrão
	-import	Importa um certificado de um banco de dados de chaves ou arquivo PKCS#12
	-list	Lista todos os certificados
	-modify	Modifica um certificado (NOTA: Atualmente, o único campo que pode ser modificado é o campo Confiança de Certificado)
	-receive	Recebe um certificado de um arquivo em um banco de dados de chaves

	-setdefault	Define o certificado pessoal padrão
	-sign	Assina um certificado armazenado em um arquivo com um certificado armazenado em um banco de dados de chaves e armazena o certificado assinado resultante em um arquivo
-certreg	-create	Cria um pedido de certificado
	-delete	Exclui um pedido de certificado de um banco de dados de pedidos de certificado
	-details	Lista as informações detalhadas de um pedido de certificado específico
	extract	Extrai um pedido de certificado de um banco de dados de pedidos de certificado para um arquivo
	-list	Lista todos os pedidos de certificado no banco de dados de pedidos de certificado
	-recreate	Recria um pedido de certificado
-help		Exibe informações de ajuda para o comando IKEYCMD
-version		Exibe informações sobre a versão da IKEYCMD

Visão Geral das Opções de Linha de Comandos IKEYCMD

A tabela a seguir mostra cada opção que pode estar presente na linha de comandos. As opções são listadas como um grupo completo; no entanto, seu uso é independente do objeto e da ação especificados na linha de comandos.

Opção	Descrição
-db	Nome completo do caminho de um banco de dados de chaves
-default_cert	Define um certificado para ser utilizado como padrão para autenticação de cliente (yes ou no). O padrão é no.
-dn	Nome distinto X.500. Inserido como uma cadeia entre aspas no seguinte formato (apenas CN, O e C são obrigatórios): "CN=Jane Doe,O=IBM,OU=Java Development,L=Endicott,ST=NY,ZIP=13760,C=country"

-encryption	Nível de criptografia utilizado no comando de exportação do certificado (strong ou weak). O padrão é strong.
-expire	Tempo de expiração de um certificado ou de uma senha de banco de dados (em dias). Os padrões são 365 dias para um certificado e 60 dias para uma senha de banco de dados.
-file	Nome do arquivo de um certificado ou pedido de certificado (dependendo do objeto especificado)
-format	Formato de um certificado (ascii para Base64_encoded ASCII ou binário para Dados DER Binários). O padrão é ascii.
-label	Rótulo anexado a um certificado ou pedido de certificado
-new_format	Novo formato do banco de dados de chaves
-new_pw	Nova senha de banco de dados
-old_format	Formato antigo do banco de dados de chaves
-pw	Senha para o banco de dados de chaves ou arquivo PKCS#12. Consulte "Criando um Novo Banco de Dados de Chaves" na página 151.
-size	Tamanho da chave (512 ou 1024). O padrão é 1024.
-stash	Indicador para guardar a senha do banco de dados de chaves em um arquivo. Se especificado, a senha será guardada em um arquivo.
-target	Arquivo ou banco de dados de destino.
-target_pw	Senha para o banco de dados de chaves se -target especificar um banco de dados de chaves. Consulte "Criando um Novo Banco de Dados de Chaves" na página 151.
-target_type	Tipo de banco de dados especificado pelo operando -target (consulte -type).
-trust	Status de confiança de um certificado de CA (enable ou disable). O padrão é enable.
-type	Tipo de banco de dados. Os valores permitidos são cms (indica um banco de dados de chave CMS), jce (indica Java Cryptography Extension de propriedade da Sun), jceks (indica Java Cryptography Extension Key Store de propriedade da Sun) ou pkcs12 (indica um arquivo PKCS#12).
-x509version	Versão do certificado X.509 a ser criado (1, 2 ou 3). O padrão é 3.

Chamada da Linha de Comandos

Segue uma lista das chamadas de linha de comandos, com os parâmetros opcionais especificados em *itálico*.

Para simplificar, a chamada real do Java, `java com.ibm.gsk.ikeyman.ikeycmd`, é omitida em cada uma das chamadas de comando.

```
-keydb -changepw
-db <nome do arquivo> -pw <senha>
-new_pw <nova senha> -stash -expire
<dias>

-keydb -convert -db <nome do arquivo> -pw <senha>
-old_format <cms | webdb> -new_format <cms>

-keydb -create -db <nome do arquivo> -pw <senha>
-type <cms | jks | jceks | pks12>
-expire <dias> -stash

-keydb -delete -db
<nome do arquivo> -pw <senha>

-keydb -stashpw -db <nome do arquivo> -pw <senha>

-cert -add -db <nome do arquivo> -pw <senha> -label
<etiqueta>
-file <filename> -format <ascii | binary> -trust <enable | disable>

-cert -create -db <nome do arquivo> -pw <senha>
-label <etiqueta>
-dn <nome_distinto> -size <1024 | 512>
-x509version <3 | 1 | 2>
-default_cert <não | sim>

-cert -delete -db
<nome do arquivo> -pw <senha> -label <etiqueta>

-cert -details -db <nome do arquivo> -pw <senha>
-label <etiqueta>

-cert -export -db <nome do arquivo> -pw <senha>
-label <etiqueta>
-type <cms | jks | jceks | pks12> -target <nome do arquivo>
-target_pw <senha>
-target_type <cms | jks | jceks | pkcs12> -encryption <strong | weak>

-cert -extract -db <nome do arquivo> -pw
<senha> -label <etiqueta>
-target <nome do arquivo> -format <ascii |
binário>

-cert -getdefault -db <nome do arquivo> -pw <senha>

-cert -import -db <nome do arquivo> -pw <senha> -label <etiqueta>
-type <cms | jks | jceks | pks12> -target <nome do arquivo>
-target_pw <senha>
-target_type <cms | jks | jceks | pks12>

-cert
-import -file <nome do arquivo> -type <pkcs12> -target <nome do arquivo>
-target_pw <password> -target_type <cms | jks | jceks | pks12>

-cert -list <todos | pessoal | CA | site> -db
<nome do arquivo>
-pw <password> -type <cms | jks | jceks | pks12>

-cert -modify -db <nome do arquivo> -pw <senha>
-label <etiqueta>
-trust <ativar | desativar>

-cert -receive -file
<nome do arquivo> -db <nome do arquivo> -pw <senha>
-format <ascii | binary> -default_cert <no | yes>

-cert -setdefault -db <nome do arquivo> -pw
<senha> -label <etiqueta>

-cert -sign -file <nome do arquivo> -db <nome do arquivo> -pw
<senha>
-label <etiqueta> -target <nome do arquivo> -format
<ascii | binário>
-expire <dias>
```

```
-certreq -create -db  
<nome do arquivo> -pw <senha> -label <etiqueta>  
-dn <distinguished_name> -size <1024 | 512> -file <filename>  
-certreq -delete -db <nome do arquivo> -pw  
<senha> -label <etiqueta>  
-certreq -details -db <nome do arquivo> -pw <senha>  
-label <etiqueta>  
-certreq -extract -db <nome do arquivo> -pw <senha>  
-label <etiqueta>  
-target <nome do arquivo>  
-certreq -list -db <nome do arquivo>  
-pw <senha>  
-certreq -recreate -db <nome do arquivo> -pw <senha>  
-label <etiqueta>  
-target <nome do arquivo>  
-help  
-version
```

Arquivo de Propriedades do Usuário

Para eliminar um pouco de digitação nas chamadas da CLI Java, as propriedades do usuário podem ser especificadas em um arquivo de propriedades. O arquivo de propriedades pode ser especificado na chamada de linha de comandos Java através da opção Java `-Dikeycmd.properties`. Em plataformas Windows, um arquivo de propriedades de amostra, `ikminit_hod.properties`, é fornecido no `your_install_directory\bin`, em que `your_install_directory` é o diretório de instalação do Host On-Demand. Em plataformas AIX, esse arquivo é fornecido no `your_install_directory/bin`. Estes diretórios de instalação contêm a definição padrão para o Host On-Demand.

Apêndice C. Utilitário P12 Keyring

O utilitário Certificate Management gráfico (disponível em plataformas Windows e AIX) é fornecido para permitir que você crie pedidos de certificados, receba e armazene certificados e crie certificados auto-assinados. O utilitário P12 Keyring é fornecido principalmente para plataformas que não têm o Utilitário Certificate Management para criar um banco de dados do conjunto de teclas com certificados raiz de certificados auto-assinados e desconhecidos de Autoridade de Certificado. Entretanto, ele pode ser utilizado em qualquer plataforma do Host On-Demand. Esse utilitário fornece aos administradores do sistema uma maneira fácil de criar e implementar um banco de dados do conjunto de chaves TLS.

O utilitário P12 Keyring é escrito em Java. Ele obtém um certificado do servidor de um Telnet ou de um servidor FTP (ou um Redirecionador) que está configurado para TLS. Uma conexão TLS é feita para o servidor a porta TLS especificados. Se a porta não for fornecida, a porta Telnet ou FTP conhecida e segura será utilizada. O certificado do servidor será extraído e adicionado ao arquivo p12 especificado.

O acesso ao banco de dados do conjunto de teclas é protegido por senha. Um prompt de senha será fornecido antes da execução de qualquer um dos comandos. Se o arquivo do conjunto de teclas especificado não existir, ele será criado e a senha será armazenada no arquivo.



O suporte ao TLS do Host On Demand requer que a senha seja `hod`. Se você estiver adicionando um certificado particular no banco de dados do conjunto de teclas, outro prompt de senha será fornecido para o segundo arquivo p12.

Uso

```
P12Keyring p12FileName connect ipaddr[:port] [ftp]  
P12Keyring p12FileName add p12FileName2  
P12Keyring p12FileName list
```

Opções

connect - estabelece uma conexão TLS para o `ipaddr` e a porta especificados. O número da porta e a palavra-chave do `ftp` são opcionais. Se o número da porta não for especificado, a porta 442 Telnet segura padrão ou a porta 990 do FTP segura padrão será utilizada.

Se a palavra-chave **ftp** for especificada, será feita a conexão a um servidor FTP seguro configurado para segurança. Há dois tipos de opções de segurança para servidores FTP:

- Segurança implícita para a porta 990
- Segurança explícita para qualquer outra porta

Se a palavra-chave `ftp` for especificada e o número da porta não for especificado ou se ele for 990, as negociações de segurança implícita serão desempenhadas. Se a palavra-chave `ftp` for especificada e o número da porta não for 990, negociações explícitas de segurança serão feitas, emitindo primeiro o comando `AUTH TLS`.

add - adiciona um certificado de cliente particular ao banco de dados do conjunto de teclas especificado.

list - exibe uma lista de certificados armazenados no banco de dados do conjunto de teclas especificado.

Exemplos

Windows:

```
C:\your_install_dir\lib\P12Keyring
c:\ your_install_dir\HOD\CustomizedCAs
connect myServer.raleigh.ibm.com:702
```

```
C:\your_install_dir\lib\P12Keyring
c:\ your_install_dir\HOD\CustomizedCAs
connect myFTPServer.raleigh.ibm.com:5031 ftp
```

em que *your_install_dir* é o diretório de instalação do Host On-Demand.

Unix:

```
cd your_install_directory/HOD
Java -classpath
.:your_install_dir/lib/sm.zip \
com.ibm.hod5ssligh.t.tools.P12Keyring
CustomizedCAs connect
myServer.raleigh.ibm.com:702
```

em que *your_install_dir* é o diretório de instalação do Host On-Demand.

Apêndice D. Opções da Linha de Comandos do Ativador de Plataforma Nativa

Quando você insere as opções da linha de comandos a seguir com o ativador de plataforma nativa, o ativador as transmite para a instalação do Host On-Demand como parâmetros de instalação. As opções que anulam o assistente para GUI são marcadas adequadamente.

Tabela 13. Opções da Linha de Comandos

Opção	Finalidade	Uso do Exemplo
-console (Anula o assistente para GUI)	Instala o Host On-Demand no modo do console.	install.exe
-log <i>#!filename</i> em que # exibe a tela para saída padrão e <i>!filename</i> é o nome do arquivo de registro. Se você especificar ! sem um nome de arquivo, o nome de arquivo do registro padrão será utilizado.	Gera um registro do arquivo de instalação com o nome especificado.	hodinstallwin.exe -log #!\mydirectory\logfile
-options <i>filename</i>	Instala o Host On-Demand com as opções da linha de comandos que definem as propriedades especificadas para a instalação.	hodinstallwin.exe -silent -options c:\mydirectory\ responseFile
-options-record <i>filename</i>	Gera um arquivo de texto de opções gravando as respostas no assistente para instalação do Host On-Demand, estabelecendo-as como valores padrão para as variáveis de instalação.	hodinstallwin.exe -options-record responses.txt
-options-template <i>filename</i>	Gera um arquivo de texto de opções que contém os valores de instalação padrão.	hodinstallwin.exe -options-template template.txt
-silent (Anula o assistente para GUI)	Instala o Host On-Demand no modo silencioso, aceitando todos os valores de instalação padrão.	hodinstallwin.exe -silent

As opções da linha de comandos adicionais a seguir aplicam-se apenas ao processo de chamada e execução do programa de instalação. Insira-as na linha de comandos com o ativador de plataforma nativa.

Tabela 14. Opções da Linha de Comandos Específicas de Ativação

Opção	Finalidade	Uso do Exemplo
-is:log <i>filename</i>	Gera um arquivo de registro para as pesquisas JVM do ativador nativo.	hodinstallwin.exe -is:log myLogFile.txt

Tabela 14. Opções da Linha de Comandos Específicas de Ativação (continuação)

Opção	Finalidade	Uso do Exemplo
-is:silent	Previne a exibição da UI (Interface com o Usuário) do ativador, enquanto ocorrem pesquisas do JVM e outras inicializações. (Geralmente utilizado com a opção da linha de comandos <code>silent</code> .)	<pre> hodinstallwin.exe -is:silent </pre>
-is:tempdir <i>directory</i>	Define o diretório temporário utilizado pela instalação do Host On-Demand.	<pre> hodinstallwin.exe -is:tempdir "c:\temp" </pre>

Apêndice E. Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em todos os países. Consulte um representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM ou quaisquer outros direitos da IBM, poderá ser utilizado em substituição a este produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de produtos não-IBM são de responsabilidade do Cliente.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento desta publicação não garante ao Cliente nenhum direito sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

Para pedidos de licença relacionados a informações de DBCS (Conjunto de Caracteres de Byte Duplo), entre em contato com o Departamento de Propriedade Intelectual da IBM em seu país ou envie pedidos de licença, por escrito, para:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

O parágrafo a seguir não se aplica a nenhum país em que tais disposições não estejam de acordo com a legislação local: A INTERNACIONAL BUSINESS MACHINES CORPORATION FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA" SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS NÃO SE LIMITANDO A, AS GARANTIAS IMPLÍCITAS DE NÃO-INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, esta disposição pode não se aplicar ao Cliente.

Esta publicação pode conter imprecisões técnicas ou erros tipográficos. Periodicamente, são feitas alterações nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A IBM pode, a qualquer momento, aperfeiçoar e/ou alterar os produtos e/ou programas descritos nesta publicação, sem aviso prévio.

Referências nestas informações a Web sites não-IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a estes Web sites.

Os materiais contidos nestes Web sites não fazem parte dos materiais deste produto IBM e a utilização destes Web sites é de inteira responsabilidade do Cliente.

A IBM pode utilizar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Licenciados deste programa que desejam obter informações sobre este assunto com objetivo de permitir: (i) a troca de informações entre programas criados independentemente e outros programas (incluindo este) e (ii) a utilização mútua das informações trocadas, devem entrar em contato com:

Site Counsel
Av. Pasteur, 138-146
2455 South Road
Poughkeepsie, NY 12601-5400
CEP 22290-240

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriadas, incluindo em alguns casos o pagamento de uma taxa.

O programa licenciado descrito neste documento e todo o material licenciado disponível são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato de Licença do Programa Internacional IBM ou de qualquer contrato equivalente.

Tais informações podem estar disponíveis, sujeitas a termos e condições apropriadas, incluindo em alguns casos, o pagamento de uma taxa. O programa licenciado descrito neste documento e todo o material licenciado disponível são fornecidos pela IBM sob os termos do Contrato com o Cliente IBM, do Contrato de Licença do Programa Internacional IBM ou de qualquer contrato equivalente.

As informações relativas a produtos não-IBM foram obtidas junto aos fornecedores dos respectivos produtos, de seus anúncios publicados ou de outras fontes disponíveis publicamente. A IBM não testou estes produtos e não pode confirmar a precisão de seu desempenho, compatibilidade nem qualquer outra reivindicação relacionada a produtos não-IBM. Dúvidas sobre os recursos de produtos não-IBM devem ser encaminhadas diretamente a seus fornecedores.

Se estas informações estiverem sendo exibidas em cópia eletrônica, as fotografias e ilustrações coloridas podem não aparecer.

Apêndice F. Marcas Registradas

Os termos a seguir são marcas registradas da International Business Machines Corporation nos Estados Unidos e/ou em outros países: **IBM**

Java e todas as marcas comerciais e logotipos baseados em Java são marcas comerciais ou marcas registradas do Oracle Corporation nos Estados Unidos e em outros países.

Microsoft, Windows e o logotipo Windows são marcas registradas da Microsoft Corporation.

Outros nomes de empresas, produtos e serviços podem ser marcas registradas ou marcas de serviço de terceiros.



Impresso no Brasil

SC43-3082-01

